aws

Panduan Pengguna

Amazon Security Lake

Amazon Security Lake: Panduan Pengguna

Table of Contents

Apa itu Danau Keamanan Amazon?

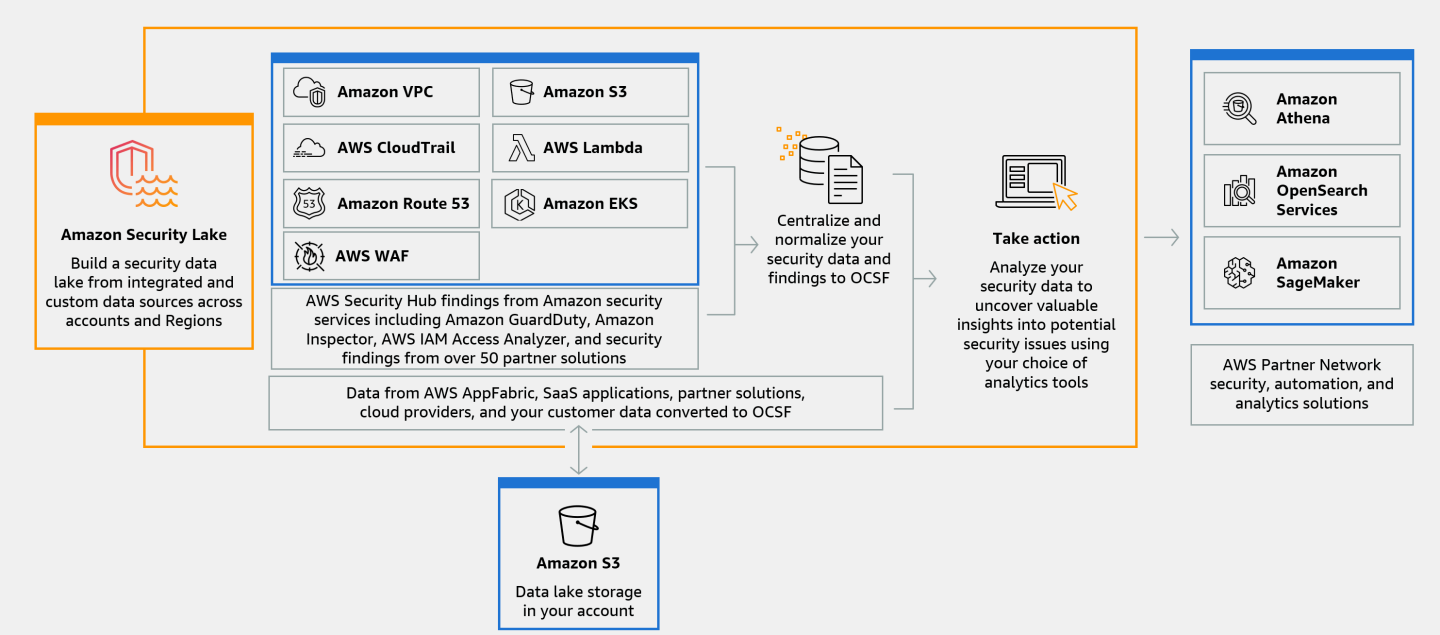
Amazon Security Lake adalah layanan danau data keamanan yang dikelola sepenuhnya. Anda dapat menggunakan Security Lake untuk secara otomatis memusatkan data keamanan dari AWS lingkungan, penyedia SaaS, di tempat, sumber cloud, dan sumber pihak ketiga ke dalam data lake yang dibuat khusus yang disimpan di tempat Anda. Akun AWS Security Lake membantu Anda menganalisis data keamanan, sehingga Anda bisa mendapatkan pemahaman yang lebih lengkap tentang postur keamanan Anda di seluruh organisasi. Dengan Security Lake, Anda juga dapat meningkatkan perlindungan beban kerja, aplikasi, dan data Anda.

Data lake didukung oleh bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3), dan Anda mempertahankan kepemilikan atas data Anda.

Security Lake mengotomatiskan pengumpulan data log dan peristiwa terkait keamanan dari layanan terintegrasi Layanan AWS dan pihak ketiga. Ini juga membantu Anda mengelola siklus hidup data dengan pengaturan retensi dan replikasi yang dapat disesuaikan. Security Lake mengubah data yang dicerna ke dalam format Apache Parquet dan skema open-source standar yang disebut Open Cybersecurity Schema Framework (). OCSF Dengan OCSF dukungan, Security Lake menormalkan dan menggabungkan data keamanan dari AWS dan berbagai sumber data keamanan perusahaan.

Layanan lain Layanan AWS dan pihak ketiga dapat berlangganan data yang disimpan di Security Lake untuk respons insiden dan analisis data keamanan.

Sekilas tentang Security Lake



Fitur Danau Keamanan

Berikut adalah beberapa cara utama Security Lake membantu Anda memusatkan, mengelola, dan berlangganan data log dan peristiwa terkait keamanan.

Agregasi data ke akun Anda

Security Lake membuat danau data keamanan yang dibuat khusus di akun Anda. Security Lake mengumpulkan data log dan peristiwa dari cloud, di tempat, dan sumber data kustom di seluruh akun dan Wilayah. Data lake didukung oleh bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3), dan Anda mempertahankan kepemilikan atas data Anda.

Berbagai sumber log dan peristiwa yang didukung

Security Lake mengumpulkan log keamanan dan peristiwa dari berbagai sumber, termasuk layanan lokal Layanan AWS, dan pihak ketiga. Setelah menelan log, apa pun sumbernya, Anda dapat mengaksesnya secara terpusat, dan mengelola siklus hidupnya. Untuk detail tentang sumber dari mana log dan peristiwa dikumpulkan oleh Security Lake, lihat Manajemen sumber di Security Lake

Transformasi dan normalisasi data

Security Lake secara otomatis mempartisi data yang masuk dari yang didukung secara native Layanan AWS dan mengubahnya menjadi format Parket yang hemat penyimpanan dan kueri. Ini juga mengubah data dari yang didukung secara native Layanan AWS ke skema open-source Open Cybersecurity Schema Framework ()OCSF. Ini membuat data kompatibel dengan penyedia lain Layanan AWS dan pihak ketiga tanpa perlu pasca-pemrosesan. Karena Security Lake menormalkan data, banyak solusi keamanan dapat menggunakan data ini secara paralel.

Berbagai tingkat akses untuk pelanggan

Pelanggan mengkonsumsi data yang disimpan di Security Lake. Anda dapat memilih tingkat akses pelanggan ke data Anda. Pelanggan dapat mengkonsumsi data hanya dari sumber, dan dalam Wilayah AWS, yang Anda tentukan. Pelanggan dapat secara otomatis diberitahu tentang objek baru saat mereka ditulis ke danau data. Atau, pelanggan dapat meminta data dari danau data. Security Lake secara otomatis membuat dan menukar kredensil yang diperlukan antara Security Lake dan pelanggan.

Manajemen data multi-akun dan Multi-wilayah

Anda dapat mengaktifkan Security Lake secara terpusat di semua Wilayah yang tersedia, dan di beberapa Akun AWS wilayah. Di Security Lake, Anda juga dapat menetapkan Wilayah rollup untuk mengkonsolidasikan log keamanan dan data peristiwa dari beberapa Wilayah. Ini dapat membantu Anda mematuhi persyaratan kepatuhan data residensi.

Dapat dikonfigurasi dan disesuaikan

Security Lake adalah layanan yang dapat dikonfigurasi dan dapat disesuaikan. Anda dapat menentukan sumber, akun, dan Wilayah mana yang ingin Anda konfigurasikan untuk koleksi log. Anda juga dapat menentukan tingkat akses pelanggan ke danau data.

Manajemen dan pengoptimalan siklus hidup data

Security Lake mengelola siklus hidup data Anda dengan pengaturan retensi yang dapat disesuaikan dan biaya penyimpanan dengan tingkatan penyimpanan otomatis. Security Lake secara otomatis mempartisi dan mengubah data keamanan yang masuk ke penyimpanan dan kueri format Parket Apache yang efisien.

Mengakses Danau Keamanan

Untuk daftar Wilayah di mana Danau Keamanan saat ini tersedia, lihatWilayah Danau Keamanan dan titik akhir. Untuk mempelajari lebih lanjut tentang Wilayah, lihat titik akhir AWS layanan di. Referensi Umum AWS

Di setiap Wilayah, Anda dapat mengakses Security Lake dengan salah satu cara berikut:

AWS Management Console

AWS Management Console Ini adalah antarmuka berbasis browser yang dapat Anda gunakan untuk membuat dan mengelola AWS sumber daya. Konsol Security Lake menyediakan akses ke akun dan sumber daya Security Lake Anda. Anda dapat melakukan sebagian besar tugas Security Lake dengan menggunakan konsol Security Lake.

Danau Keamanan API

Untuk mengakses Security Lake secara terprogram, gunakan Security LakeAPI, dan keluarkan HTTPS permintaan langsung ke layanan. Untuk informasi lebih lanjut, lihat APIReferensi Danau Keamanan.

AWS Command Line Interface (AWS CLI)

Dengan AWS CLI, Anda dapat mengeluarkan perintah di baris perintah sistem Anda untuk melakukan tugas dan AWS tugas Security Lake. Menggunakan baris perintah dapat lebih cepat dan lebih nyaman dibandingkan konsol. Alat baris perintah juga berguna jika Anda ingin membangun skrip yang melakukan tugas. Untuk informasi tentang menginstal dan menggunakan AWS CLI, lihat AWS Command Line Interface.

AWS SDKs

AWS menyediakan SDKs yang terdiri dari pustaka dan kode sampel untuk berbagai bahasa pemrograman dan platform, seperti Java, Go, Python, C ++, dan. NET. SDKsMenyediakan akses yang nyaman dan terprogram ke Security Lake dan lainnya Layanan AWS. SDK menangani tugas seperti menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba kembali permintaan secara otomatis. Untuk informasi tentang menginstal dan menggunakan AWS SDKs, lihat Alat untuk Dibangun AWS.

Layanan terkait

Berikut ini adalah yang lain Layanan AWS yang digunakan Security Lake:

- Amazon EventBridge — Security Lake digunakan EventBridge untuk memberi tahu pelanggan ketika objek ditulis ke danau data.
- AWS GlueSecurity Lake menggunakan AWS Glue crawler untuk membuat AWS Glue Data Catalog tabel dan mengirim data yang baru ditulis ke Katalog Data. Security Lake juga menyimpan metadata partisi untuk AWS Lake Formation tabel di Katalog Data.
- AWS Lake FormationSecurity Lake membuat tabel Lake Formation terpisah untuk setiap sumber yang menyumbangkan data ke Security Lake. Tabel Lake Formation berisi informasi tentang data dari setiap sumber, termasuk skema, partisi, dan informasi lokasi data. Pelanggan memiliki opsi untuk mengkonsumsi data dengan menanyakan tabel Lake Formation.
- AWS LambdaSecurity Lake menggunakan fungsi Lambda untuk mendukung mengekstrak, mengubah, dan memuat (ETL) pekerjaan pada data mentah dan untuk mendaftarkan partisi untuk data sumber di. AWS Glue
- Amazon S3 - Security Lake menyimpan data Anda sebagai objek Amazon S3. Kelas penyimpanan dan pengaturan retensi didasarkan pada penawaran Amazon S3. Security Lake tidak mendukung Amazon S3 Select.
- Amazon Simple Queue Service — Security Lake menggunakan Amazon SQS untuk mengaktifkan pemrosesan berbasis peristiwa dan mengelola notifikasi.

Security Lake mengumpulkan data dari sumber khusus selain yang berikut ini: Layanan AWS

- AWS CloudTrail manajemen dan peristiwa data (S3, Lambda)
- Log Audit Amazon Elastic Kubernetes Service (Amazon) EKS
- Log kueri Amazon Route 53 Resolver
- AWS Security Hub temuan
- Log Aliran Amazon Virtual Private Cloud (AmazonVPC)
- AWS WAF v2 Log

Untuk informasi lebih lanjut tentang sumber-sumber ini, lihatMengumpulkan data dari Layanan AWS Danau Keamanan. Anda dapat menggunakan objek Amazon S3 di danau data keamanan Anda dengan membuat pelanggan yang dapat membaca data dalam skema. OCSF Anda juga dapat melakukan kueri data dengan menggunakan Amazon Athena, Amazon Redshift, dan layanan berlangganan pihak ketiga yang terintegrasi dengannya. AWS Glue

Konsep dan terminologi

Bagian ini menjelaskan konsep dan istilah utama untuk membantu Anda menggunakan Amazon Security Lake.

Berkontribusi pada wilayah

Satu atau lebihWilayah AWS yang berkontribusi data ke Wilayah Batal.

Danau data

Data persisten Anda yang disimpan di Amazon Simple Storage Service (Amazon S3) dan dikelola oleh Security Lake. Security Lake menggunakanAWS Glue untuk mengirim data yang baru ditulis ke Katalog Data. Security Lake juga membuatAWS Lake Formation tabel untuk setiap sumber yang memberikan kontribusi data ke data lake. Danau data biasanya menyimpan yang berikut:

- Data terstruktur dan tidak terstruktur
- Data mentah dan ditransformasikan

Security Lake adalah layanan data lake yang dirancang untuk mengumpulkan log dan peristiwa terkait keamanan.

Buka Kerangka Skema Keamanan Siber (OCSF)

Skema open-source standar untuk log keamanan dan peristiwa. Ini dikembangkan olehAWS dan pemimpin industri keamanan lainnya di berbagai domain keamanan. Security Lake secara otomatis mengubah log dan peristiwa yang dikumpulkan dariLayanan AWS ke dalam skema OCSF. Sumber khusus mengubah log dan acara mereka menjadi OCSF sebelum mengirimnya ke Security Lake.

Wilayah Rollup

SebuahWilayah AWS yang mengkonsolidasikan log keamanan dan peristiwa dari satu atau beberapa Wilayah berkontribusi. Menentukan satu atau lebih Wilayah Batal dapat membantu Anda mematuhi persyaratan kepatuhan regional.

Sumber

Satu set log dan peristiwa yang dihasilkan dari satu sistem yang cocok dengan kelas peristiwa tertentu di OCSF. Danau Keamanan dapat mengumpulkan data dari sumber. Sumber mungkin merupakan layanan lainLayanan AWS atau pihak ketiga. Untuk sumber pihak ketiga, Anda harus mengonversi data ke skema OCSF sebelum mengirimkannya ke Security Lake.

Pelanggan

Layanan yang mengkonsumsi log dan acara dari Security Lake. Pelanggan mungkin merupakan layanan lainLayanan AWS atau pihak ketiga.

Memulai dengan Amazon Security Lake

Topik di bagian ini menjelaskan cara mengaktifkan dan mulai menggunakan Security Lake. Anda akan belajar cara mengkonfigurasi pengaturan data lake Anda dan mengatur pengumpulan log. Anda dapat mengaktifkan dan menggunakan Security Lake melalui AWS Management Console atau secara terprogram. Metode apa pun yang Anda gunakan, Anda harus terlebih dahulu mengatur Akun AWS dan pengguna administratif. Langkah-langkah setelah itu berbeda berdasarkan metode akses.

Konsol Security Lake menawarkan proses yang efisien untuk memulai, dan membuat semua peran AWS Identity and Access Management (IAM) yang diperlukan yang Anda butuhkan untuk membuat data lake Anda.

Jika Anda mengakses Security Lake secara terprogram, Anda perlu membuat beberapa peran AWS Identity and Access Management (IAM) untuk mengonfigurasi data lake Anda.

> **Important**
>
> Security Lake tidak mendukung penimbunan kembali peristiwa sumber log AWS mentah yang ada yang dihasilkan sebelum mengaktifkan Security Lake.

Topik

Menyiapkan Akun AWS

Sebelum Anda dapat mengaktifkan Amazon Security Lake, Anda harus memiliki file Akun AWS. Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimkan email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Aktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan MFA perangkat virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan IAM Pengguna.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat IAM Identitas.

Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat IAM Identitas, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat IAM Identitas, gunakan login URL yang dikirim ke alamat email saat Anda membuat pengguna Pusat IAM Identitas.

  Untuk bantuan masuk menggunakan pengguna Pusat IAM Identitas, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat IAM Identitas, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuk, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Identifikasi akun yang akan Anda gunakan untuk mengaktifkan Security Lake

Security Lake terintegrasi dengan AWS Organizations mengelola pengumpulan log di beberapa akun dalam suatu organisasi. Jika Anda ingin menggunakan Security Lake untuk organisasi, Anda harus menggunakan akun manajemen Organizations Anda untuk menunjuk administrator Security Lake yang didelegasikan. Kemudian, Anda harus menggunakan kredensi administrator yang didelegasikan untuk mengaktifkan Security Lake, menambahkan akun anggota, dan mengaktifkan Security Lake untuk mereka. Untuk informasi selengkapnya, lihat Mengelola banyak akun dengan AWS Organizations di Security Lake.

Atau, Anda dapat menggunakan Security Lake tanpa integrasi Organizations untuk akun mandiri yang bukan bagian dari organisasi.

Pertimbangan saat mengaktifkan Security Lake

Sebelum mengaktifkan Security Lake, pertimbangkan hal berikut:

- Security Lake menyediakan fitur manajemen lintas wilayah, yang berarti Anda dapat membuat data lake dan mengonfigurasi pengumpulan log. Wilayah AWS Untuk mengaktifkan Security Lake di semua Wilayah yang didukung, Anda dapat memilih titik akhir Regional yang didukung. Anda juga dapat menambahkan Wilayah rollup untuk mengumpulkan data dari beberapa wilayah ke satu Wilayah.
- Kami merekomendasikan untuk mengaktifkan Security Lake di semua yang didukung Wilayah AWS. Jika Anda melakukan ini, Security Lake dapat mengumpulkan data yang terhubung ke aktivitas yang tidak sah atau tidak biasa bahkan di Wilayah yang tidak Anda gunakan secara aktif. Jika Security Lake tidak diaktifkan di semua Wilayah yang didukung, kemampuannya untuk mengumpulkan data dari layanan lain yang Anda gunakan di beberapa Wilayah akan berkurang.
- Saat Anda mengaktifkan Security Lake untuk pertama kalinya di Wilayah mana pun, itu akan menciptakan peran terkait layanan untuk akun Anda yang dipanggil. `AWSServiceRoleForSecurityLake` Peran ini mencakup izin untuk menelepon orang lain Layanan AWS atas nama Anda dan mengoperasikan danau data keamanan. Untuk informasi selengkapnya tentang cara kerja peran terkait layanan, lihat Menggunakan peran terkait layanan di Panduan Pengguna. IAM Jika Anda mengaktifkan Security Lake sebagai administrator Security Lake yang didelegasikan, Security Lake akan membuat peran terkait layanan di setiap akun anggota di organisasi.
- Security Lake tidak mendukung Amazon S3 Object Lock. Saat bucket data lake dibuat, S3 Object Lock dinonaktifkan secara default. Mengaktifkan Object Lock pada bucket mengganggu pengiriman data log yang dinormalisasi ke data lake.
- Jika Anda mengaktifkan kembali Security Lake di suatu wilayah, Anda harus menghapus AWS Glue database terkait wilayah tersebut dari penggunaan Security Lake sebelumnya.

Mengaktifkan Security Lake menggunakan konsol

Tutorial ini menjelaskan cara mengaktifkan dan mengkonfigurasi Security Lake melalui AWS Management Console. Sebagai bagian dari AWS Management Console, konsol Security Lake

menawarkan proses yang efisien untuk memulai, dan menciptakan semua peran AWS Identity and Access Management (IAM) yang diperlukan yang Anda butuhkan untuk membuat data lake Anda.

Langkah 1: Konfigurasikan sumber

Security Lake mengumpulkan data log dan peristiwa dari berbagai sumber dan di seluruh Anda Akun AWS dan Wilayah AWS. Ikuti petunjuk ini untuk mengidentifikasi data mana yang ingin dikumpulkan Security Lake. Anda hanya dapat menggunakan petunjuk ini untuk menambahkan sumber yang didukung secara asli Layanan AWS . Untuk informasi tentang menambahkan sumber kustom, lihatMengumpulkan data dari sumber khusus di Security Lake.

Untuk mengkonfigurasi koleksi sumber log

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah. Anda dapat mengaktifkan Danau Keamanan di Wilayah saat ini dan Wilayah lain saat melakukan orientasi.
3. Pilih Mulai.
4. Untuk Pilih sumber log dan peristiwa, pilih salah satu opsi berikut:

    a. Menyerap AWS sumber default - Saat Anda memilih opsi yang disarankan, CloudTrail - Peristiwa data S3 tidak disertakan untuk konsumsi. Ini karena menelan volume tinggi CloudTrail - peristiwa data S3 dapat memengaruhi biaya penggunaan secara signifikan. Untuk menelan sumber ini, pilih opsi AWS sumber spesifik Ingest.

    b. Menelan AWS sumber tertentu - Dengan opsi ini, Anda dapat memilih satu atau lebih sumber log dan peristiwa yang ingin Anda konsumsi.

    > **Note**
    >
    > Saat Anda mengaktifkan Security Lake di akun untuk pertama kalinya, semua log dan sumber peristiwa yang dipilih akan menjadi bagian dari periode uji coba gratis 15 hari. Untuk informasi selengkapnya tentang statistik penggunaan, lihatMeninjau penggunaan dan perkiraan biaya.

5. Untuk Versi, pilih versi sumber data tempat Anda ingin menyerap sumber log dan peristiwa.

> **Important**
>
> Jika Anda tidak memiliki izin peran yang diperlukan untuk mengaktifkan versi baru sumber AWS log di Wilayah yang ditentukan, hubungi administrator Security Lake Anda. Untuk informasi selengkapnya, lihat Memperbarui izin peran.

6. Untuk Wilayah Terpilih, pilih apakah akan menyerap sumber log dan peristiwa dari semua Wilayah yang didukung atau Wilayah tertentu. Jika Anda memilih Wilayah Tertentu, pilih Wilayah mana untuk menyerap data.
7. Untuk akses Layanan, buat peran baru atau gunakan IAM peran yang ada yang IAM memberikan izin Security Lake untuk mengumpulkan data dari sumber Anda dan menambahkannya ke data lake Anda. Satu peran digunakan di semua Wilayah di mana Anda mengaktifkan Security Lake.
8. Pilih Berikutnya.

Langkah 2: Tentukan pengaturan penyimpanan dan rollup Regions (opsional)

Anda dapat menentukan kelas penyimpanan Amazon S3 di mana Anda ingin Security Lake menyimpan data Anda dan untuk berapa lama. Anda juga dapat menentukan Wilayah rollup untuk mengkonsolidasikan data dari beberapa Wilayah. Ini adalah langkah opsional. Untuk informasi selengkapnya, lihat Manajemen siklus hidup di Security Lake.

Untuk mengkonfigurasi pengaturan penyimpanan dan rollup

1. Jika Anda ingin mengkonsolidasikan data dari beberapa Wilayah yang berkontribusi ke Wilayah rollup, untuk Pilih Wilayah rollup, pilih Tambahkan Wilayah rollup. Tentukan Wilayah rollup dan Wilayah yang akan berkontribusi padanya. Anda dapat mengatur satu atau lebih Wilayah rollup.
2. Untuk Pilih kelas penyimpanan, pilih kelas penyimpanan Amazon S3. Kelas penyimpanan default adalah S3 Standard. Berikan periode retensi (dalam beberapa hari) jika Anda ingin data beralih ke kelas penyimpanan lain setelah waktu itu, dan pilih Tambahkan transisi. Setelah periode retensi berakhir, objek kedaluwarsa dan Amazon S3 menghapusnya. Untuk informasi selengkapnya tentang kelas penyimpanan dan retensi Amazon S3, lihat. Manajemen retensi

3. Jika Anda memilih Wilayah rollup pada langkah pertama, untuk akses Layanan, buat IAM peran baru atau gunakan peran yang ada IAM yang memberikan izin Security Lake untuk mereplikasi data di beberapa Wilayah.
4. Pilih Berikutnya.

Langkah 3: Tinjau dan buat data lake

Tinjau sumber tempat Security Lake akan mengumpulkan data dari, Wilayah rollup Anda, dan pengaturan retensi Anda. Kemudian, buat danau data Anda.

Untuk meninjau dan membuat data lake

1. Saat mengaktifkan Security Lake, tinjau sumber Log dan peristiwa, Wilayah, Wilayah Rollup, dan kelas Penyimpanan.
2. Pilih Buat.

Setelah membuat data lake Anda, Anda akan melihat halaman Ringkasan di konsol Security Lake. Halaman ini memberikan gambaran umum tentang jumlah Wilayah dan Wilayah Rollup, informasi tentang pelanggan, dan Masalah.

Menu Masalah menunjukkan ringkasan masalah dari 14 hari terakhir yang memengaruhi layanan Security Lake atau bucket Amazon S3 Anda. Untuk detail tambahan tentang setiap masalah, Anda dapat membuka halaman Masalah di konsol Security Lake.

Langkah 4: Lihat dan kueri data Anda sendiri

Setelah membuat data lake Anda, Anda dapat menggunakan Amazon Athena atau layanan serupa untuk melihat dan menanyakan data Anda dari AWS Lake Formation database dan tabel. Saat Anda menggunakan konsol, Security Lake secara otomatis memberikan izin tampilan database ke peran yang Anda gunakan untuk mengaktifkan Security Lake. Minimal, peran tersebut harus memiliki izin analis data. Untuk informasi selengkapnya tentang tingkat izin, lihat personas Lake Formation dan referensi IAM izin. Untuk petunjuk tentang pemberian *SELECT* izin, lihat Memberikan izin Katalog Data menggunakan metode sumber daya bernama di Panduan Pengembang.AWS Lake Formation

Langkah 5: Buat pelanggan

Setelah membuat data lake Anda, Anda dapat menambahkan pelanggan untuk mengkonsumsi data Anda. Pelanggan dapat menggunakan data dengan langsung mengakses objek di bucket Amazon

S3 Anda atau dengan menanyakan data lake. Untuk informasi selengkapnya tentang pelanggan, lihatManajemen pelanggan di Security Lake.

Mengaktifkan Security Lake secara terprogram

Tutorial ini menjelaskan cara mengaktifkan dan mulai menggunakan Security Lake secara terprogram. Amazon Security Lake API memberi Anda akses terprogram yang komprehensif ke akun, data, dan sumber daya Security Lake Anda. Atau, Anda dapat menggunakan alat baris AWS perintah — AWS Command Line Interfaceatau AWS Alat untuk PowerShell —atau AWS SDKsuntuk mengakses Security Lake.

Langkah 1: Buat IAM peran

Jika Anda mengakses Security Lake secara terprogram, Anda perlu membuat beberapa peran AWS Identity and Access Management (IAM) untuk mengonfigurasi data lake Anda.

> **Important**
>
> Tidak perlu membuat IAM peran ini jika Anda menggunakan konsol Security Lake untuk mengaktifkan dan mengkonfigurasi Security Lake.

Anda harus membuat peran IAM jika Anda akan mengambil satu atau beberapa tindakan berikut (pilih tautan untuk melihat informasi selengkapnya tentang IAM peran untuk setiap tindakan):

- Membuat sumber kustom — Sumber kustom adalah sumber selain yang didukung secara asli Layanan AWS yang mengirim data ke Security Lake.
- Membuat pelanggan dengan akses data — Pelanggan dengan izin dapat langsung mengakses objek S3 dari danau data Anda.
- Membuat pelanggan dengan akses kueri — Pelanggan dengan izin dapat meminta data dari Security Lake menggunakan layanan seperti Amazon Athena.
- Mengkonfigurasi Wilayah rollup — Wilayah rollup mengkonsolidasikan data dari beberapa. Wilayah AWS

Setelah membuat peran yang disebutkan sebelumnya, lampirkan AmazonSecurityLakeAdministrator AWS kebijakan terkelola untuk peran yang Anda gunakan untuk mengaktifkan Security Lake.

Kebijakan ini memberikan izin administratif yang memungkinkan kepala sekolah untuk masuk ke Security Lake dan mengakses semua tindakan Security Lake.

Lampirkan AmazonSecurityLakeMetaStoreManager AWS kebijakan terkelola untuk membuat data lake atau data kueri dari Security Lake. Kebijakan ini diperlukan untuk Security Lake untuk mendukung mengekstrak, mengubah, dan memuat (ETL) pekerjaan pada log mentah dan data peristiwa yang diterimanya dari sumber.

Langkah 2: Aktifkan Amazon Security Lake

Untuk mengaktifkan Security Lake secara terprogram, gunakan CreateDataLakeOperasi Danau API Keamanan Jika Anda menggunakan AWS CLI, jalankan create-data-lakeperintah. Dalam permintaan Anda, gunakan `region` bidang `configurations` objek untuk menentukan kode Wilayah untuk Wilayah untuk mengaktifkan Danau Keamanan. Untuk daftar kode Wilayah, lihat titik akhir Amazon Security Lake di. Referensi Umum AWS

Contoh 1

Contoh perintah berikut memungkinkan Security Lake in the `us-east-1` and `us-east-2` Regions. Di kedua Wilayah, danau data ini dienkripsi dengan kunci terkelola Amazon S3. Objek kedaluwarsa setelah 365 hari, dan objek bertransisi ke kelas penyimpanan `ONEZONE_IA` S3 setelah 60 hari. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","lifecycleConfiguration":
 {"expiration":{"days":365},"transitions":[{"days":60,"storageClass":"ONEZONE_IA"}]}},
 {"encryptionConfiguration": {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-
east-2","lifecycleConfiguration": {"expiration":{"days":365},"transitions":
[{"days":60,"storageClass":"ONEZONE_IA"}]}}]' \
--meta-store-manager-role-arn "arn:aws:iam:us-east-1:123456789012:role/service-role/
AmazonSecurityLakeMetaStoreManager"
```

Contoh 2

Contoh perintah berikut memungkinkan Security Lake in the `us-east-2` Region. Data lake ini dienkripsi dengan kunci terkelola pelanggan yang dibuat di AWS Key Management Service ()AWS KMS. Objek kedaluwarsa setelah 500 hari, dan objek beralih ke kelas penyimpanan `GLACIER` S3

setelah 30 hari. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"1234abcd-12ab-34cd-56ef-1234567890ab"},"region":"us-
east-2","lifecycleConfiguration": {"expiration":{"days":500},"transitions":
[{"days":30,"storageClass":"GLACIER"}]}}]' \
--meta-store-manager-role-arn "arn:aws:iam:us-east-1:123456789012:role/service-role/
AmazonSecurityLakeMetaStoreManager"
```

> **Note**
>
> Jika Anda telah mengaktifkan Security Lake dan ingin memperbarui pengaturan konfigurasi untuk Wilayah atau sumber, gunakan UpdateDataLakeoperasi, atau jika menggunakan AWS CLI, update-data-lakeperintah. Jangan gunakan `CreateDataLake` operasi.

Langkah 3: Konfigurasikan sumber

Security Lake mengumpulkan data log dan peristiwa dari berbagai sumber dan di seluruh Anda Akun AWS dan Wilayah AWS. Ikuti petunjuk ini untuk mengidentifikasi data mana yang ingin dikumpulkan Security Lake. Anda hanya dapat menggunakan petunjuk ini untuk menambahkan sumber yang didukung secara asli Layanan AWS . Untuk informasi tentang menambahkan sumber kustom, lihatMengumpulkan data dari sumber khusus di Security Lake.

Untuk menentukan satu atau lebih sumber koleksi secara terprogram, gunakan CreateAwsLogSourcepengoperasian Danau Keamanan. API Untuk setiap sumber, tentukan nilai unik Regional untuk `sourceName` parameter. Secara opsional gunakan parameter tambahan untuk membatasi ruang lingkup sumber ke akun tertentu (`accounts`) atau versi tertentu (`sourceVersion`).

> **Note**
>
> Jika Anda tidak menyertakan parameter opsional dalam permintaan Anda, Security Lake menerapkan permintaan Anda ke semua akun atau semua versi sumber yang ditentukan, tergantung pada parameter yang Anda kecualikan. Misalnya, jika Anda adalah administrator Security Lake yang didelegasikan untuk organisasi dan Anda mengecualikan `accounts`

parameternya, Security Lake menerapkan permintaan Anda ke semua akun di organisasi Anda. Demikian pula, jika Anda mengecualikan `sourceVersion` parameter, Security Lake menerapkan permintaan Anda ke semua versi sumber yang ditentukan.

Jika permintaan Anda menentukan Wilayah di mana Anda belum mengaktifkan Security Lake, terjadi kesalahan. Untuk mengatasi kesalahan ini, pastikan bahwa `regions` array hanya menentukan Wilayah di mana Anda telah mengaktifkan Security Lake. Atau, Anda dapat mengaktifkan Danau Keamanan di Wilayah, dan kemudian mengirimkan permintaan Anda lagi.

Saat Anda mengaktifkan Security Lake di akun untuk pertama kalinya, semua log dan sumber peristiwa yang dipilih akan menjadi bagian dari periode uji coba gratis 15 hari. Untuk informasi selengkapnya tentang statistik penggunaan, lihatMeninjau penggunaan dan perkiraan biaya.

Langkah 4: Konfigurasikan pengaturan penyimpanan dan rollup Regions (opsional)

Anda dapat menentukan kelas penyimpanan Amazon S3 di mana Anda ingin Security Lake menyimpan data Anda dan untuk berapa lama. Anda juga dapat menentukan Wilayah rollup untuk mengkonsolidasikan data dari beberapa Wilayah. Ini adalah langkah opsional. Untuk informasi selengkapnya, lihat Manajemen siklus hidup di Security Lake.

Untuk menentukan tujuan target secara terprogram saat Anda mengaktifkan Security Lake, gunakan CreateDataLakeOperasi Danau API Keamanan Jika Anda sudah mengaktifkan Security Lake dan ingin menentukan tujuan target, gunakan UpdateDataLakeoperasi, bukan `CreateDataLake` operasi.

Untuk operasi mana pun, gunakan parameter yang didukung untuk menentukan pengaturan konfigurasi yang Anda inginkan:

- Untuk menentukan Wilayah rollup, gunakan `region` bidang untuk menentukan Wilayah yang ingin Anda sumbangkan data ke Wilayah rollup. Dalam `regions` larik `replicationConfiguration` objek, tentukan kode Wilayah untuk setiap Wilayah rollup. Untuk daftar kode Wilayah, lihat titik akhir Amazon Security Lake di. Referensi Umum AWS
- Untuk menentukan pengaturan retensi untuk data Anda, gunakan `lifecycleConfiguration` parameter:
  - Untuk`transitions`, tentukan jumlah total days (`days`) yang ingin Anda simpan objek S3 di kelas `storageClass` penyimpanan Amazon S3 tertentu ().

- Untuk`expiration`, tentukan jumlah hari yang ingin Anda simpan objek di Amazon S3, menggunakan kelas penyimpanan apa pun, setelah objek dibuat. Ketika periode retensi ini berakhir, objek kedaluwarsa dan Amazon S3 menghapusnya.

Security Lake menerapkan pengaturan retensi yang ditentukan ke Wilayah yang Anda tentukan di `region` bidang `configurations` objek.

Misalnya, perintah berikut membuat data lake dengan `ap-northeast-2` sebagai Region rollup. `us-east-1`Wilayah akan menyumbangkan data ke `ap-northeast-2` Wilayah. Contoh ini juga menetapkan periode kedaluwarsa 10 hari untuk objek yang ditambahkan ke danau data.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","replicationConfiguration":
 {"regions": ["ap-northeast-2"],"roleArn":"arn:aws:iam::123456789012:role/service-
role/AmazonSecurityLakeS3ReplicationRole"},"lifecycleConfiguration": {"expiration":
{"days":10}}}]' \
--meta-store-manager-role-arn "arn:aws:iam::123456789012:role/service-role/
AmazonSecurityLakeMetaStoreManager"
```

Anda sekarang telah membuat danau data Anda. Gunakan ListDataLakespengoperasian Danau Keamanan API untuk memverifikasi pemberdayaan Danau Keamanan dan pengaturan danau data Anda di setiap Wilayah.

Jika masalah atau kesalahan muncul dalam pembuatan data lake Anda, Anda dapat melihat daftar pengecualian dengan menggunakan ListDataLakeExceptionsoperasi, dan memberi tahu pengguna tentang pengecualian dengan CreateDataLakeExceptionSubscriptionoperasi. Untuk informasi selengkapnya, lihat Memecahkan masalah status danau data.

Langkah 5: Lihat dan kueri data Anda sendiri

Setelah membuat data lake Anda, Anda dapat menggunakan Amazon Athena atau layanan serupa untuk melihat dan menanyakan data Anda dari AWS Lake Formation database dan tabel. Saat Anda mengaktifkan Security Lake secara terprogram, izin tampilan database tidak diberikan secara otomatis. Akun administrator data lake AWS Lake Formation harus memberikan SELECT izin ke IAM peran yang ingin Anda gunakan untuk menanyakan database dan tabel yang relevan. Minimal, peran tersebut harus memiliki izin analis data. Untuk informasi selengkapnya tentang tingkat izin, lihat personas Lake Formation dan referensi IAM izin. Untuk petunjuk tentang pemberian *SELECT*

izin, lihat Memberikan izin Katalog Data menggunakan metode sumber daya bernama di Panduan Pengembang.AWS Lake Formation

Langkah 6: Buat pelanggan

Setelah membuat data lake Anda, Anda dapat menambahkan pelanggan untuk mengkonsumsi data Anda. Pelanggan dapat menggunakan data dengan langsung mengakses objek di bucket Amazon S3 Anda atau dengan menanyakan data lake. Untuk informasi selengkapnya tentang pelanggan, lihatManajemen pelanggan di Security Lake.

Mengelola banyak akun dengan AWS Organizations di Security Lake

Anda dapat menggunakan Amazon Security Lake untuk mengumpulkan log keamanan dan peristiwa dari beberapa Akun AWS. Untuk membantu mengotomatiskan dan merampingkan pengelolaan beberapa akun, kami sangat menyarankan Anda mengintegrasikan Security Lake dengan. AWS Organizations

Di Organizations, akun yang Anda gunakan untuk membuat organisasi disebut akun manajemen. Untuk mengintegrasikan Security Lake dengan Organizations, akun manajemen harus menunjuk akun administrator Security Lake yang didelegasikan untuk organisasi.

Administrator Security Lake yang didelegasikan dapat mengaktifkan Security Lake dan mengkonfigurasi pengaturan Security Lake untuk akun anggota. Administrator yang didelegasikan dapat mengumpulkan log dan peristiwa di seluruh organisasi di semua Wilayah AWS tempat Security Lake diaktifkan (terlepas dari titik akhir Regional mana yang saat ini mereka gunakan). Administrator yang didelegasikan juga dapat mengonfigurasi Security Lake untuk secara otomatis mengumpulkan data log dan peristiwa untuk akun organisasi baru.

Administrator Security Lake yang didelegasikan memiliki akses ke data log dan peristiwa untuk akun anggota terkait. Dengan demikian, mereka dapat mengonfigurasi Security Lake untuk mengumpulkan data yang dimiliki oleh akun anggota terkait. Mereka juga dapat memberikan izin kepada pelanggan untuk mengkonsumsi data yang dimiliki oleh akun anggota terkait.

Untuk mengaktifkan Security Lake untuk beberapa akun dalam suatu organisasi, akun manajemen organisasi harus terlebih dahulu menunjuk akun administrator Security Lake yang didelegasikan untuk organisasi tersebut. Administrator yang didelegasikan kemudian dapat mengaktifkan dan mengkonfigurasi Security Lake untuk organisasi.

Important

Gunakan Security Lake RegisterDataLakeDelegatedAdministratorAPIuntuk memungkinkan Security Lake mengakses Organisasi Anda dan mendaftarkan administrator yang didelegasikan Organisasi.
Jika Anda menggunakan Organizations' APIs untuk mendaftarkan administrator yang didelegasikan, peran terkait layanan untuk Organizations mungkin tidak berhasil dibuat. Untuk memastikan fungsionalitas penuh, gunakan Danau KeamananAPIs.

Untuk informasi tentang menyiapkan Organizations, lihat Membuat dan mengelola organisasi di Panduan AWS Organizations Pengguna.

Pertimbangan penting bagi administrator Security Lake yang didelegasikan

Perhatikan faktor-faktor berikut yang menentukan bagaimana administrator yang didelegasikan berperilaku di Security Lake:

Administrator yang didelegasikan adalah sama di semua Wilayah.

- Saat Anda membuat administrator yang didelegasikan, administrator akan menjadi administrator yang didelegasikan untuk setiap Wilayah tempat Anda mengaktifkan Security Lake.

Sebaiknya atur akun Arsip Log sebagai administrator yang didelegasikan Security Lake.

- Akun Log Archive adalah akun Akun AWS yang didedikasikan untuk menelan dan mengarsipkan semua log terkait keamanan. Akses ke akun ini biasanya terbatas pada beberapa pengguna, seperti auditor dan tim keamanan untuk investigasi kepatuhan. Sebaiknya atur akun Arsip Log sebagai administrator yang didelegasikan Security Lake sehingga Anda dapat melihat log dan peristiwa terkait keamanan dengan pengalihan konteks minimal.

- Selain itu, kami menyarankan bahwa hanya satu set pengguna minimal yang memiliki akses langsung ke akun Arsip Log. Di luar grup pilihan ini, jika pengguna memerlukan akses ke data yang dikumpulkan Security Lake, Anda dapat menambahkannya sebagai pelanggan Security Lake. Untuk informasi tentang menambahkan pelanggan, lihatManajemen pelanggan di Security Lake.

- Jika Anda tidak menggunakan AWS Control Tower layanan ini, Anda mungkin tidak memiliki akun Arsip Log. Untuk informasi selengkapnya tentang akun Arsip Log, lihat Security OU — Akun Arsip Log di Arsitektur Referensi AWS Keamanan.

Sebuah organisasi hanya dapat memiliki satu administrator yang didelegasikan.

- Anda hanya dapat memiliki satu administrator Security Lake yang didelegasikan untuk setiap organisasi.

Akun manajemen organisasi tidak dapat menjadi administrator yang didelegasikan.

- Berdasarkan praktik terbaik AWS Keamanan dan prinsip hak istimewa terkecil, akun manajemen organisasi Anda tidak dapat menjadi administrator yang didelegasikan.

Administrator yang didelegasikan harus menjadi bagian dari organisasi yang aktif.

> Saat Anda menghapus organisasi, akun administrator yang didelegasikan tidak dapat lagi mengelola Security Lake. Anda harus menunjuk administrator yang didelegasikan dari organisasi lain atau menggunakan Security Lake dengan akun mandiri yang bukan bagian dari organisasi.

IAMizin yang diperlukan untuk menunjuk administrator yang didelegasikan

Saat menunjuk administrator Security Lake yang didelegasikan, Anda harus memiliki izin untuk mengaktifkan Security Lake dan menggunakan AWS Organizations API operasi tertentu yang tercantum dalam pernyataan kebijakan berikut.

Anda dapat menambahkan pernyataan berikut di akhir kebijakan AWS Identity and Access Management (IAM) untuk memberikan izin ini.

```
{
    "Sid": "Grant permissions to designate a delegated Security Lake administrator",
    "Effect": "Allow",
    "Action": [
        "securitylake:RegisterDataLakeDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

Menunjuk administrator Security Lake yang didelegasikan dan menambahkan akun anggota

Pilih metode akses Anda untuk menunjuk akun administrator Security Lake yang didelegasikan untuk organisasi Anda. Hanya akun manajemen organisasi yang dapat menunjuk akun administrator

yang didelegasikan untuk organisasi mereka. Akun manajemen organisasi tidak dapat menjadi akun administrator yang didelegasikan untuk organisasi mereka.

> **Note**
>
> - Akun manajemen organisasi harus menggunakan `RegisterDataLakeDelegatedAdministrator` operasi Security Lake untuk menunjuk akun administrator Security Lake yang didelegasikan. Menunjuk administrator Security Lake yang didelegasikan melalui Organizations tidak didukung.
> - Jika Anda ingin mengubah administrator yang didelegasikan untuk organisasi, Anda harus terlebih dahulu menghapus administrator yang didelegasikan saat ini. Anda kemudian dapat menunjuk administrator yang didelegasikan baru.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.

   Masuk menggunakan kredensyal akun manajemen untuk organisasi Anda.
2. - Jika Security Lake belum diaktifkan, pilih Mulai, lalu tentukan administrator Security Lake yang didelegasikan di halaman Aktifkan Danau Keamanan.
   - Jika Security Lake sudah diaktifkan, tentukan administrator Security Lake yang didelegasikan di halaman Pengaturan.
3. Di bawah Administrasi delegasi ke akun lain, pilih akun yang sudah berfungsi sebagai administrator yang didelegasikan untuk layanan AWS keamanan lainnya (disarankan). Atau, masukkan Akun AWS ID 12 digit akun yang ingin Anda tetapkan sebagai administrator Security Lake yang didelegasikan.
4. Pilih Delegasikan. Jika Security Lake belum diaktifkan, menunjuk administrator yang didelegasikan akan mengaktifkan Security Lake untuk akun tersebut di Wilayah Anda saat ini.

API

Untuk menunjuk administrator yang didelegasikan secara terprogram, gunakan RegisterDataLakeDelegatedAdministratorOperasi Danau API Keamanan Anda harus memanggil operasi dari akun manajemen organisasi. Jika Anda menggunakan AWS CLI, jalankan register-data-lake-delegated-administratorperintah dari akun manajemen organisasi. Dalam permintaan

Anda, gunakan `accountId` parameter untuk menentukan ID akun 12 digit yang akan ditetapkan sebagai akun administrator yang didelegasikan untuk organisasi. Akun AWS

Misalnya, AWS CLI perintah berikut menunjuk administrator yang didelegasikan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake register-data-lake-delegated-administrator \
--account-id 123456789012
```

Administrator yang didelegasikan juga dapat memilih untuk mengotomatiskan pengumpulan data AWS log dan peristiwa untuk akun organisasi baru. Dengan konfigurasi ini, Security Lake secara otomatis diaktifkan di akun baru saat akun ditambahkan ke organisasi di AWS Organizations. Sebagai administrator yang didelegasikan, Anda dapat mengaktifkan konfigurasi ini dengan menggunakan CreateDataLakeOrganizationConfigurationpengoperasian Danau Keamanan API atau, jika Anda menggunakan AWSCLI, dengan menjalankan create-data-lake-organization-configurationperintah. Dalam permintaan Anda, Anda juga dapat menentukan pengaturan konfigurasi tertentu untuk akun baru.

Misalnya, AWS CLI perintah berikut secara otomatis mengaktifkan Security Lake dan pengumpulan log kueri resolver Amazon Route 53, AWS Security Hub temuan, dan Log Aliran Amazon Virtual Private Cloud VPC (Amazon) di akun organisasi baru. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake create-data-lake-organization-configuration \
--auto-enable-new-account '[{"region":"us-east-1","sources":
[{"sourceName":"ROUTE53"},{"sourceName":"SH_FINDINGS"},{"sourceName":"VPC_FLOW"}]}]'
```

Setelah akun manajemen organisasi menunjuk administrator yang didelegasikan, administrator dapat mengaktifkan dan mengkonfigurasi Security Lake untuk organisasi. Ini termasuk mengaktifkan dan mengonfigurasi Security Lake untuk mengumpulkan data AWS log dan peristiwa untuk akun individu di organisasi. Untuk informasi selengkapnya, lihat Mengumpulkan data dari Layanan AWS Danau Keamanan.

Anda dapat menggunakan GetDataLakeOrganizationConfigurationoperasi untuk mendapatkan detail tentang konfigurasi organisasi Anda saat ini untuk akun anggota baru.

Menghapus administrator Security Lake yang didelegasikan

Hanya akun manajemen organisasi yang dapat menghapus administrator Security Lake yang didelegasikan untuk organisasi mereka. Jika Anda ingin mengubah administrator yang didelegasikan untuk organisasi, hapus administrator yang didelegasikan saat ini, lalu tentukan administrator yang didelegasikan baru.

> **Important**
>
> Menghapus administrator Security Lake yang didelegasikan akan menghapus data lake Anda dan menonaktifkan Security Lake untuk akun di organisasi Anda.

Anda tidak dapat mengubah atau menghapus administrator yang didelegasikan menggunakan konsol Security Lake. Tugas-tugas ini hanya dapat dilakukan secara terprogram.

Untuk menghapus administrator yang didelegasikan secara terprogram, gunakan DeregisterDataLakeDelegatedAdministratorOperasi Danau API Keamanan Anda harus memanggil operasi dari akun manajemen organisasi. Jika Anda menggunakan AWS CLI, jalankan deregister-data-lake-delegated-administratorperintah dari akun manajemen organisasi.

Misalnya, AWS CLI perintah berikut menghapus administrator Security Lake yang didelegasikan.

```
$ aws securitylake deregister-data-lake-delegated-administrator
```

Untuk menjaga penunjukan administrator yang didelegasikan tetapi mengubah pengaturan konfigurasi otomatis akun anggota baru, gunakan DeleteDataLakeOrganizationConfigurationpengoperasian Danau KeamananAPI, atau, jika Anda menggunakan AWS CLI, delete-data-lake-organization-configurationperintah. Hanya administrator yang didelegasikan yang dapat mengubah pengaturan ini untuk organisasi.

Misalnya, AWS CLI perintah berikut menghentikan pengumpulan otomatis temuan Security Hub dari akun anggota baru yang bergabung dengan organisasi. Akun anggota baru tidak akan menyumbangkan temuan Security Hub ke data lake setelah administrator yang didelegasikan memanggil operasi ini. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake delete-data-lake-organization-configuration \
```

```
--auto-enable-new-account '[{"region":"us-east-1","sources":
[{"sourceName":"SH_FINDINGS"}]}]'
```

Security Lake akses tepercaya

Setelah Anda mengatur Security Lake untuk suatu organisasi, akun AWS Organizations manajemen dapat mengaktifkan akses tepercaya dengan Security Lake. Akses tepercaya memungkinkan Security Lake untuk membuat peran IAM terkait layanan dan melakukan tugas di organisasi Anda dan akunnya atas nama Anda. Untuk informasi selengkapnya, lihat Menggunakan AWS Organizations dengan yang lain Layanan AWS di Panduan AWS Organizations Pengguna.

Sebagai pengguna akun manajemen organisasi, Anda dapat menonaktifkan akses tepercaya untuk Security Lake di AWS Organizations. Untuk petunjuk tentang menonaktifkan akses tepercaya, lihat Cara mengaktifkan atau menonaktifkan akses tepercaya di AWS Organizations Panduan Pengguna.

Sebaiknya nonaktifkan akses tepercaya jika administrator yang didelegasikan ditangguhkan, Akun AWS diisolasi, atau ditutup.

Mengelola Wilayah di Danau Keamanan

Amazon Security Lake dapat mengumpulkan log keamanan dan peristiwa Wilayah AWS di mana Anda telah mengaktifkan layanan. Untuk setiap Wilayah, data Anda disimpan di bucket Amazon S3 yang berbeda. Anda dapat menentukan konfigurasi data lake yang berbeda (misalnya, sumber dan pengaturan retensi yang berbeda) untuk Wilayah yang berbeda. Anda juga dapat menentukan satu atau beberapa Wilayah rollup untuk mengkonsolidasikan data dari beberapa Wilayah.

Memeriksa status Wilayah

Security Lake dapat mengumpulkan data di beberapa Wilayah AWS. Untuk melacak status data lake Anda, akan sangat membantu untuk memahami bagaimana setiap Wilayah saat ini dikonfigurasi. Pilih metode akses pilihan Anda, dan ikuti langkah-langkah ini untuk mendapatkan status Region saat ini.

Console

Untuk memeriksa status Wilayah

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Di panel navigasi, pilih Wilayah. Halaman Regions muncul, memberikan gambaran umum tentang Wilayah di mana Security Lake saat ini diaktifkan.
3. Pilih Wilayah, lalu pilih Edit untuk melihat detail Wilayah tersebut.

API

Untuk mendapatkan status pengumpulan log di Wilayah saat ini, gunakan GetDataLakeSourcesOperasi Danau KeamananAPI. Jika Anda menggunakan AWS CLI, jalankan get-data-lake-sourcesperintah. Untuk `accounts` parameter, tentukan satu atau lebih Akun AWS IDs sebagai daftar. Jika permintaan Anda berhasil, Security Lake mengembalikan snapshot untuk akun tersebut di Wilayah saat ini, termasuk AWS sumber mana Security Lake mengumpulkan data dan status setiap sumber. Jika Anda tidak menyertakan `accounts` parameter, respons mencakup status pengumpulan log untuk semua akun di mana Security Lake dikonfigurasi di Wilayah saat ini.

Misalnya, AWS CLI perintah berikut mengambil status pengumpulan log untuk akun yang ditentukan di Wilayah saat ini. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake get-data-lake-sources \
--accounts "123456789012" "111122223333"
```

AWS CLI Perintah berikut mencantumkan status pengumpulan log untuk semua akun dan sumber yang diaktifkan di Wilayah yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake get-data-lake-sources \
--regions "us-east-1" \
--query 'dataLakeSources[].[account,sourceName]'
```

Untuk menentukan apakah Anda telah mengaktifkan Security Lake for a Region, gunakan ListDataLakesoperasi. Jika Anda menggunakan AWS CLI, jalankan list-data-lakesperintah. Untuk `regions` parameter, tentukan kode Region untuk Region—misalnya, `us-east-1` untuk Wilayah AS Timur (Virginia N.). Untuk daftar kode Wilayah, lihat titik akhir Amazon Security Lake di. Referensi Umum AWS `ListDataLakes`Operasi mengembalikan pengaturan konfigurasi data lake untuk setiap Wilayah yang Anda tentukan dalam permintaan Anda. Jika Anda tidak menentukan Wilayah, Security Lake mengembalikan pengaturan status dan konfigurasi data lake Anda di setiap Wilayah di mana Security Lake tersedia.

Misalnya, AWS CLI perintah berikut menunjukkan pengaturan status dan konfigurasi danau data Anda di `eu-central-1` Wilayah. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake list-data-lakes \
--regions "us-east-1" "eu-central-1"
```

Mengubah pengaturan Wilayah

Pilih metode pilihan Anda, dan ikuti petunjuk ini untuk memperbarui pengaturan untuk data lake Anda dalam satu atau lebih Wilayah AWS.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Di panel navigasi, pilih Wilayah.
3. Pilih Wilayah, lalu pilih Edit.
4. Pilih kotak centang untuk Mengganti sumber untuk semua akun <Region>untuk mengonfirmasi bahwa pilihan Anda di sini mengganti pilihan sebelumnya untuk Wilayah ini.
5. Untuk Pilih kelas penyimpanan, pilih Tambahkan transisi untuk menambahkan kelas penyimpanan baru untuk data Anda.
6. Untuk Tag, secara opsional menetapkan atau mengedit tag untuk Wilayah. Tag adalah label yang dapat Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu, termasuk konfigurasi data lake untuk Anda Akun AWS di Wilayah tertentu. Untuk mempelajari selengkapnya, lihat Menandai sumber daya Danau Keamanan.
7. Untuk mengubah Region menjadi Region rollup, pilih Rollup Regions (di bawah Pengaturan) di panel navigasi. Kemudian pilih Modify. Di bagian Select rollup Regions, pilih Add rollup Region. Pilih Wilayah yang berkontribusi, dan berikan Security Lake izin untuk mereplikasi data di beberapa Wilayah. Setelah selesai, pilih Simpan untuk menyimpan perubahan Anda.

API

Untuk memperbarui pengaturan Wilayah untuk data lake Anda secara terprogram, gunakan UpdateDataLakeOperasi Danau KeamananAPI. Jika Anda menggunakan AWS CLI, jalankan update-data-lakeperintah. Untuk `region` parameternya, tentukan kode Wilayah untuk Wilayah yang ingin Anda ubah pengaturannya—misalnya, `us-east-1` untuk Wilayah AS Timur (Virginia N.). Untuk daftar kode Wilayah, lihat titik akhir Amazon Security Lake di. Referensi Umum AWS

Gunakan parameter tambahan untuk menentukan nilai baru untuk setiap setelan yang ingin Anda ubah—misalnya, kunci enkripsi (`encryptionConfiguration`) dan pengaturan retensi (). `lifecycleConfiguration`

Misalnya, AWS CLI perintah berikut memperbarui kedaluwarsa data dan pengaturan transisi kelas penyimpanan untuk Wilayah. `us-east-1` Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ update-data-lake \
--configurations '[{"region":"us-east-1","lifecycleConfiguration": {"expiration":
{"days":500},"transitions":[{"days":45,"storageClass":"ONEZONE_IA"}]}}]'
```

Mengkonfigurasi Wilayah rollup di Danau Keamanan

Wilayah rollup mengkonsolidasikan data dari satu atau lebih Wilayah yang berkontribusi. Menentukan Wilayah rollup dapat membantu Anda mematuhi persyaratan kepatuhan Regional.

Karena keterbatasan di Amazon S3, replikasi dari Customer Managed Key (CMK) data lake regional terenkripsi ke data regional terenkripsi terkelola S3 (enkripsi default) danau data regional tidak didukung.

> **Important**
>
> Jika Anda membuat sumber kustom, untuk memastikan bahwa data sumber kustom direplikasi dengan benar ke tujuan, Security Lake merekomendasikan mengikuti praktik terbaik yang dijelaskan dalam Praktik terbaik untuk menelan sumber kustom. Replikasi tidak dapat dilakukan pada data yang tidak mengikuti format jalur data partisi S3 seperti yang dijelaskan pada halaman.

Sebelum menambahkan Region rollup, Anda harus terlebih dahulu membuat dua peran berbeda di AWS Identity and Access Management ()IAM:

- IAMperan untuk replikasi data
- IAMperan untuk mendaftarkan AWS Glue partisi

> **Note**
>
> Security Lake membuat IAM peran ini atau menggunakan peran yang ada atas nama Anda saat Anda menggunakan konsol Security Lake. Namun, Anda harus membuat peran ini saat menggunakan Security Lake API atau AWS CLI.

IAMperan untuk replikasi data

IAMPeran ini memberikan izin ke Amazon S3 untuk mereplikasi log sumber dan peristiwa di beberapa Wilayah.

Untuk memberikan izin ini, buat IAM peran yang dimulai dengan awalan`SecurityLake`, dan lampirkan kebijakan contoh berikut ke peran tersebut. Anda memerlukan Amazon Resource Name

(ARN) peran saat membuat Region rollup di Security Lake. Dalam kebijakan ini, `sourceRegions` berkontribusi Wilayah, dan `destinationRegions` merupakan Wilayah rollup.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadS3ReplicationSetting",
      "Action": [
        "s3:ListBucket",
        "s3:GetReplicationConfiguration",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectRetention",
        "s3:GetObjectLegalHold"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake-[[sourceRegions]]*",
        "arn:aws:s3:::aws-security-data-lake-[[sourceRegions]]*/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:ResourceAccount": [
            "{{bucketOwnerAccountId}}"
          ]
        }
      }
    },
    {
      "Sid": "AllowS3Replication",
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateDelete",
        "s3:ReplicateTags",
        "s3:GetObjectVersionTagging"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake-[[destinationRegions]]*/*"
      ],
```

```
      "Condition": {
        "StringEquals": {
          "s3:ResourceAccount": [
            "{{bucketOwnerAccountId}}"
          ]
        }
      }
    }
  ]
}
```

Lampirkan kebijakan kepercayaan berikut ke peran Anda untuk mengizinkan Amazon S3 mengambil peran:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowS3ToAssume",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Jika Anda menggunakan kunci terkelola pelanggan from AWS Key Management Service (AWS KMS) untuk mengenkripsi data lake Security Lake, Anda harus memberikan izin berikut selain izin dalam kebijakan replikasi data.

```
{
    "Action": [
        "kms:Decrypt"
    ],
    "Effect": "Allow",
    "Condition": {
        "StringLike": {
            "kms:ViaService": [
                "s3.{sourceRegion1}.amazonaws.com",
                "s3.{sourceRegion2}.amazonaws.com"
```

```
                ],
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::aws-security-data-lake-{sourceRegion1}*",
                "arn:aws:s3:::aws-security-data-lake-{sourceRegion2}*"
            ]
        }
    },
    "Resource": [
        "{sourceRegion1KmsKeyArn}",
        "{sourceRegion2KmsKeyArn}"
    ]
},
{
    "Action": [
        "kms:Encrypt"
    ],
    "Effect": "Allow",
    "Condition": {
        "StringLike": {
            "kms:ViaService": [
            "s3.{destinationRegion1}.amazonaws.com",
            ],
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::aws-security-data-lake-{destinationRegion1}*",
            ]
        }
    },
    "Resource": [
            "{destinationRegionKmsKeyArn}"
    ]
}
```

Untuk informasi selengkapnya tentang peran replikasi, lihat Menyiapkan izin di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

IAMperan untuk mendaftarkan AWS Glue partisi

IAMPeran ini memberikan izin untuk AWS Lambda fungsi pembaru partisi yang digunakan oleh Security Lake untuk mendaftarkan AWS Glue partisi untuk objek S3 yang direplikasi dari wilayah lain. Tanpa membuat peran ini, pelanggan tidak dapat menanyakan peristiwa dari objek tersebut.

Untuk memberikan izin ini, buat peran bernama `AmazonSecurityLakeMetaStoreManager` (Anda mungkin telah membuat peran ini saat melakukan orientasi ke Security Lake). Untuk informasi selengkapnya tentang peran ini, termasuk kebijakan sampel, lihatLangkah 1: Buat IAM peran.

Di konsol Lake Formation, Anda juga harus memberikan `AmazonSecurityLakeMetaStoreManager` izin sebagai administrator danau data dengan mengikuti langkah-langkah berikut:

1. Buka konsol Lake Formation di https://console.aws.amazon.com/lakeformation/.
2. Masuk sebagai pengguna administratif.
3. Jika jendela Selamat Datang di Lake Formation muncul, pilih pengguna yang Anda buat atau pilih di Langkah 1, lalu pilih Memulai.
4. Jika Anda tidak melihat jendela Selamat Datang di Lake Formation, lakukan langkah-langkah berikut untuk mengonfigurasi Administrator Lake Formation.
    1. Di panel navigasi, di bawah Izin, pilih Peran dan tugas Administratif. Di bagian Administrator data lake di halaman konsol, pilih Pilih administrator.
    2. Di kotak dialog Kelola data lake administrator, untuk IAM pengguna dan peran, pilih AmazonSecurityLakeMetaStoreManagerIAMperan yang Anda buat, lalu pilih Simpan.

Untuk informasi selengkapnya tentang mengubah izin untuk administrator data lake, lihat Membuat administrator data lake di Panduan AWS Lake Formation Pengembang.

Menambahkan Wilayah rollup

Pilih metode akses pilihan Anda, dan ikuti langkah-langkah berikut untuk menambahkan Wilayah rollup.

> **Note**
>
> Suatu Wilayah dapat menyumbangkan data ke beberapa Wilayah rollup. Namun, Wilayah rollup tidak dapat menjadi Wilayah yang berkontribusi untuk Wilayah rollup lainnya.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.

2. Di panel navigasi, di bawah Pengaturan, pilih Rollup Regions.
3. Pilih Modify, lalu pilih Add rollup Region.
4. Tentukan Wilayah rollup dan Wilayah yang berkontribusi. Ulangi langkah ini jika Anda ingin menambahkan beberapa Wilayah rollup.
5. Jika ini adalah pertama kalinya Anda menambahkan Wilayah rollup, untuk akses Layanan, buat IAM peran baru, atau gunakan peran yang ada IAM yang memberikan izin Security Lake untuk mereplikasi data di beberapa Wilayah.
6. Setelah selesai, pilih Simpan.

Anda juga dapat menambahkan Wilayah rollup saat Anda naik ke Security Lake. Untuk informasi selengkapnya, lihat Memulai dengan Amazon Security Lake.

API

Untuk menambahkan Wilayah rollup secara terprogram, gunakan UpdateDataLakeOperasi Danau KeamananAPI. Jika Anda menggunakan AWS CLI, jalankan update-data-lakeperintah. Dalam permintaan Anda, gunakan `region` bidang untuk menentukan Wilayah yang ingin Anda sumbangkan data ke Wilayah rollup. Dalam `regions` larik `replicationConfiguration` parameter, tentukan kode Wilayah untuk setiap Wilayah rollup. Untuk daftar kode Wilayah, lihat titik akhir Amazon Security Lake di. Referensi Umum AWS

Misalnya, perintah berikut ditetapkan `ap-northeast-2` sebagai Region rollup. `us-east-1`Wilayah akan menyumbangkan data ke `ap-northeast-2` Wilayah. Contoh ini juga menetapkan periode kedaluwarsa 365 hari untuk objek yang ditambahkan ke danau data. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake update-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","replicationConfiguration":
 {"regions": ["ap-northeast-2"],"roleArn":"arn:aws:iam::123456789012:role/service-
role/AmazonSecurityLakeS3ReplicationRole"},"lifecycleConfiguration": {"expiration":
{"days":365}}}]'
```

Anda juga dapat menambahkan Wilayah rollup saat Anda naik ke Security Lake. Untuk melakukan ini, gunakan CreateDataLakeoperasi (atau, jika menggunakan AWS CLI, create-data-lakeperintah). Untuk informasi selengkapnya tentang mengonfigurasi Wilayah rollup selama orientasi, lihat. Memulai dengan Amazon Security Lake

Memperbarui atau menghapus Wilayah rollup

Pilih metode akses pilihan Anda, dan ikuti langkah-langkah ini untuk memperbarui atau menghapus Kawasan rollup di Security Lake.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Di panel navigasi, di bawah Pengaturan, pilih Rollup Regions.
3. Pilih Ubah.
4. Untuk mengubah Wilayah yang berkontribusi untuk Wilayah rollup, tentukan Wilayah kontribusi yang diperbarui di baris untuk Wilayah rollup.
5. Untuk menghapus Region rollup, pilih Remove in the row for rollup Region.
6. Setelah selesai, pilih Simpan.

API

Untuk mengonfigurasi Wilayah rollup secara terprogram, gunakan UpdateDataLakeOperasi Danau KeamananAPI. Jika Anda menggunakan AWS CLI, jalankan update-data-lakeperintah. Dalam permintaan Anda, gunakan parameter yang didukung untuk menentukan pengaturan rollup:

- Untuk menambahkan Wilayah yang berkontribusi, gunakan `region` bidang untuk menentukan kode Wilayah untuk Wilayah yang akan ditambahkan. Dalam `regions` larik `replicationConfiguration` objek, tentukan kode Wilayah untuk setiap Wilayah rollup untuk menyumbangkan data. Untuk daftar kode Wilayah, lihat titik akhir Amazon Security Lake di. Referensi Umum AWS
- Untuk menghapus Region yang berkontribusi, gunakan `region` bidang untuk menentukan kode Region untuk wilayah yang akan dihapus. Untuk `replicationConfiguration` parameter, jangan tentukan nilai apa pun.

Misalnya, perintah berikut mengonfigurasi keduanya `us-east-1` dan `us-east-2` sebagai Wilayah yang berkontribusi. Kedua Wilayah akan menyumbangkan data ke Wilayah `ap-northeast-3` rollup. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake update-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","replicationConfiguration":
 {"regions": ["ap-northeast-3"],"roleArn":"arn:aws:iam::123456789012:role/service-
role/AmazonSecurityLakeS3ReplicationRole"},"lifecycleConfiguration": {"expiration":
{"days":365}}},
{"encryptionConfiguration": {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-
east-2","replicationConfiguration": {"regions": ["ap-
northeast-3"],"roleArn":"arn:aws:iam::123456789012:role/service-role/
AmazonSecurityLakeS3ReplicationRole"}, "lifecycleConfiguration": {"expiration":
{"days":500},"transitions":[{"days":60,"storageClass":"ONEZONE_IA"}]}}]'
```

Manajemen sumber di Security Lake

Sumber adalah log dan peristiwa yang dihasilkan dari satu sistem yang cocok dengan kelas acara tertentu dalam Buka Kerangka Skema Keamanan Siber (OCSF) di Danau Keamanan skema. Amazon Security Lake dapat mengumpulkan log dan peristiwa dari berbagai sumber, termasuk sumber kustom yang didukung secara asli Layanan AWS dan pihak ketiga.

Security Lake menjalankan tugas ekstrak, transformasi, dan load (ETL) pada data sumber mentah, dan mengonversi data ke format Apache Parquet dan skema. OCSF Setelah diproses, Security Lake menyimpan data sumber di bucket Amazon Simple Storage Service (Amazon S3) di Akun AWS bucket Wilayah AWS tempat data dihasilkan. Security Lake membuat bucket Amazon S3 yang berbeda untuk setiap Wilayah tempat Anda mengaktifkan layanan. Setiap sumber mendapatkan awalan terpisah di bucket S3 Anda, dan Security Lake mengatur data dari setiap sumber dalam kumpulan tabel terpisah. AWS Lake Formation

Topik

Mengumpulkan data dari Layanan AWS Danau Keamanan

Amazon Security Lake dapat mengumpulkan log dan peristiwa dari yang didukung secara asli Layanan AWS berikut ini:

- AWS CloudTrail manajemen dan peristiwa data (S3, Lambda)
- Log Audit Amazon Elastic Kubernetes Service (Amazon) EKS
- Log kueri Amazon Route 53 Resolver
- AWS Security Hub temuan
- Log Aliran Amazon Virtual Private Cloud (AmazonVPC)
- AWS WAF log v2

Security Lake secara otomatis mengubah data ini menjadi format Buka Kerangka Skema Keamanan Siber (OCSF) di Danau Keamanan dan Apache Parquet.

> **Tip**
>
> Untuk menambahkan satu atau beberapa layanan sebelumnya sebagai sumber log di Security Lake, Anda tidak perlu mengonfigurasi pencatatan secara terpisah di layanan ini, kecuali peristiwa CloudTrail manajemen. Jika Anda memiliki log yang dikonfigurasi dalam layanan ini, Anda tidak perlu mengubah konfigurasi logging Anda untuk menambahkannya sebagai sumber log di Security Lake. Security Lake menarik data langsung dari layanan ini melalui aliran peristiwa independen dan duplikat.

Prasyarat: Verifikasi izin

Untuk menambahkan Layanan AWS sebagai sumber di Security Lake, Anda harus memiliki izin yang diperlukan. Pastikan kebijakan AWS Identity and Access Management (IAM) yang dilampirkan pada peran yang Anda gunakan untuk menambahkan sumber memiliki izin untuk melakukan tindakan berikut:

- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:GetDatabase`
- `glue:GetTable`
- `glue:UpdateTable`
- `iam:CreateServiceLinkedRole`
- `s3:GetObject`
- `s3:PutObject`

Disarankan agar peran memiliki kondisi dan ruang lingkup sumber daya berikut untuk `s3:PutObject` izin `S3:getObject` dan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUpdatingSecurityLakeS3Buckets",
            "Effect": "Allow",
```

```
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::aws-security-data-lake*",
              "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
    }
    ]
}
```

Tindakan ini memungkinkan Anda untuk mengumpulkan log dan peristiwa dari an Layanan AWS dan mengirimkannya ke AWS Glue database dan tabel yang benar.

Jika Anda menggunakan AWS KMS kunci untuk enkripsi sisi server data lake Anda, Anda juga memerlukan izin untuk. `kms:DescribeKey`

Menambahkan Layanan AWS sebagai sumber

Setelah Anda menambahkan Layanan AWS sebagai sumber, Security Lake secara otomatis mulai mengumpulkan log keamanan dan peristiwa darinya. Instruksi ini memberi tahu Anda cara menambahkan yang didukung secara asli Layanan AWS sebagai sumber di Security Lake. Untuk petunjuk tentang menambahkan sumber kustom, lihatMengumpulkan data dari sumber khusus di Security Lake.

Console

Untuk menambahkan sumber AWS log (konsol)

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Pilih Sumber dari panel navigasi.
3. Pilih Layanan AWS yang ingin Anda kumpulkan datanya, dan pilih Konfigurasi.
4. Di bagian Pengaturan sumber, aktifkan sumber dan pilih Versi sumber data yang ingin Anda gunakan untuk konsumsi data. Secara default, versi terbaru dari sumber data dicerna oleh Security Lake.

> **Important**
>
> Jika Anda tidak memiliki izin peran yang diperlukan untuk mengaktifkan versi baru sumber AWS log di Wilayah yang ditentukan, hubungi administrator Security Lake Anda. Untuk informasi selengkapnya, lihat Memperbarui izin peran.

Agar pelanggan Anda dapat menelan versi sumber data yang dipilih, Anda juga harus memperbarui pengaturan pelanggan Anda. Untuk detail tentang cara mengedit pelanggan, lihat Manajemen pelanggan di Amazon Security Lake.

Secara opsional, Anda dapat memilih untuk menelan versi terbaru saja dan menonaktifkan semua versi sumber sebelumnya yang digunakan untuk konsumsi data.

5. Di bagian Wilayah, pilih Wilayah tempat Anda ingin mengumpulkan data untuk sumbernya. Security Lake akan mengumpulkan data dari sumber dari semua akun di Wilayah yang dipilih.
6. Pilih Aktifkan.

API

Untuk menambahkan sumber AWS log (API)

Untuk menambahkan Layanan AWS sebagai sumber secara terprogram, gunakan CreateAwsLogSourcepengoperasian Danau Keamanan. API Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan create-aws-log-sourceperintah. Parameter `sourceName` dan `regions` diperlukan. Secara opsional, Anda dapat membatasi ruang lingkup sumber ke spesifik `accounts` atau spesifik`sourceVersion`.

> **Important**
>
> Bila Anda tidak memberikan parameter dalam perintah Anda, Security Lake mengasumsikan bahwa parameter yang hilang mengacu pada seluruh rangkaian. Misalnya, jika Anda tidak memberikan `accounts` parameter, perintah berlaku untuk seluruh rangkaian akun di organisasi Anda.

Contoh berikut menambahkan Log VPC Aliran sebagai sumber di akun dan Wilayah yang ditunjuk. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

> **Note**
>
> Jika Anda menerapkan permintaan ini ke Wilayah di mana Anda belum mengaktifkan Security Lake, Anda akan menerima kesalahan. Anda dapat mengatasi kesalahan dengan mengaktifkan Security Lake di Wilayah tersebut atau dengan menggunakan `regions` parameter untuk menentukan hanya Wilayah di mana Anda telah mengaktifkan Security Lake.

```
$ aws securitylake create-aws-log-source \
--sources sourceName=VPC_FLOW,accounts='["123456789012",
 "111122223333"]',regions=["us-east-2"],sourceVersion="2.0"
```

Mendapatkan status koleksi sumber

Pilih metode akses Anda, dan ikuti langkah-langkah untuk mendapatkan snapshot akun dan sumber yang pengumpulan lognya diaktifkan di Wilayah saat ini.

Console

Untuk mendapatkan status pengumpulan log di Wilayah saat ini

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Pada panel navigasi, pilih Akun.
3. Arahkan kursor ke nomor di kolom Sumber untuk melihat log mana yang diaktifkan untuk akun yang dipilih.

API

Untuk mendapatkan status pengumpulan log di Wilayah saat ini, gunakan GetDataLakeSourcespengoperasian Danau KeamananAPI. Jika Anda menggunakan AWS CLI, jalankan get-data-lake-sourcesperintah. Untuk `accounts` parameter, Anda dapat menentukan satu atau lebih Akun AWS IDs sebagai daftar. Jika permintaan Anda berhasil, Security Lake

mengembalikan snapshot untuk akun tersebut di Wilayah saat ini, termasuk AWS sumber mana Security Lake mengumpulkan data dan status setiap sumber. Jika Anda tidak menyertakan `accounts` parameter, respons mencakup status pengumpulan log untuk semua akun di mana Security Lake dikonfigurasi di Wilayah saat ini.

Misalnya, AWS CLI perintah berikut mengambil status pengumpulan log untuk akun yang ditentukan di Wilayah saat ini. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake get-data-lake-sources \
--accounts "123456789012" "111122223333"
```

Memperbarui izin peran di Security Lake

Jika Anda tidak memiliki izin peran atau sumber daya yang AWS Lambda diperlukan—fungsi baru dan antrian Amazon Simple Queue Service (SQSAmazon) —untuk menyerap data dari versi baru sumber data, Anda harus memperbarui izin peran dan membuat kumpulan sumber daya baru untuk memproses data dari sumber `AmazonSecurityLakeMetaStoreManagerV2` Anda.

Pilih metode pilihan Anda, dan ikuti petunjuk untuk memperbarui izin peran Anda dan membuat sumber daya baru untuk memproses data dari versi baru sumber AWS log di Wilayah tertentu. Ini adalah tindakan satu kali, karena izin dan sumber daya secara otomatis diterapkan ke rilis sumber data masa depan.

Console

Untuk memperbarui izin peran (konsol)

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.

   Masuk dengan kredensyal administrator Security Lake yang didelegasikan.
2. Di panel navigasi, pada Pengaturan, pilih Umum.
3. Pilih Perbarui izin peran.
4. Di bagian Akses Layanan, lakukan salah satu hal berikut:

   - Buat dan gunakan peran layanan baru — Anda dapat menggunakan peran AmazonSecurityLakeMetaStoreManager V2 yang dibuat oleh Security Lake.

- Menggunakan peran layanan yang ada — Anda dapat memilih peran layanan yang ada dari daftar nama peran Layanan.

5. Pilih Terapkan.

API

Untuk memperbarui izin peran () API

Untuk memperbarui izin secara terprogram, gunakan UpdateDataLakeOperasi Danau API Keamanan Untuk memperbarui izin menggunakan AWS CLI, jalankan update-data-lakeperintah.

Untuk memperbarui izin peran Anda, Anda harus melampirkan AmazonSecurityLakeMetastoreManagerkebijakan untuk peran.

Menghapus peran AmazonSecurityLakeMetaStoreManager

> **Important**
>
> Setelah memperbarui izin peran`AmazonSecurityLakeMetaStoreManagerV2`, konfirmasikan bahwa data lake berfungsi dengan benar sebelum Anda menghapus `AmazonSecurityLakeMetaStoreManager` peran lama. Disarankan untuk menunggu setidaknya 4 jam sebelum menghapus peran.

Jika Anda memutuskan untuk menghapus peran, Anda harus menghapus `AmazonSecurityLakeMetaStoreManager` peran terlebih dahulu AWS Lake Formation.

Ikuti langkah-langkah ini untuk menghapus `AmazonSecurityLakeMetaStoreManager` peran dari konsol Lake Formation.

1. Masuk ke AWS Management Console, dan buka konsol Lake Formation di https://console.aws.amazon.com/lakeformation/.
2. Di konsol Lake Formation, dari panel navigasi, pilih Peran dan tugas administratif.
3. Hapus `AmazonSecurityLakeMetaStoreManager` dari setiap Wilayah.

Menghapus Layanan AWS sebagai sumber dari Security Lake

Pilih metode akses Anda, dan ikuti langkah-langkah ini untuk menghapus sumber Danau Keamanan yang didukung Layanan AWS secara asli. Anda dapat menghapus sumber untuk satu atau beberapa Wilayah. Saat Anda menghapus sumbernya, Security Lake berhenti mengumpulkan data dari sumber tersebut di Wilayah dan akun yang ditentukan, dan pelanggan tidak dapat lagi mengkonsumsi data baru dari sumbernya. Namun, pelanggan masih dapat mengkonsumsi data yang dikumpulkan Security Lake dari sumbernya sebelum dihapus. Anda hanya dapat menggunakan petunjuk ini untuk menghapus sumber yang didukung secara asli Layanan AWS . Untuk informasi tentang menghapus sumber kustom, lihatMengumpulkan data dari sumber khusus di Security Lake.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Pilih Sumber dari panel navigasi.
3. Pilih sumber, dan pilih Nonaktifkan.
4. Pilih Wilayah atau Wilayah tempat Anda ingin berhenti mengumpulkan data dari sumber ini. Security Lake akan berhenti mengumpulkan data dari sumber dari semua akun di Wilayah yang dipilih.

API

Untuk menghapus Layanan AWS sebagai sumber secara terprogram, gunakan DeleteAwsLogSourcepengoperasian Danau Keamanan. API Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan delete-aws-log-sourceperintah. Parameter `sourceName` dan `regions` diperlukan. Secara opsional, Anda dapat membatasi ruang lingkup penghapusan ke spesifik `accounts` atau spesifik`sourceVersion`.

> **Important**
>
> Bila Anda tidak memberikan parameter dalam perintah Anda, Security Lake mengasumsikan bahwa parameter yang hilang mengacu pada seluruh rangkaian. Misalnya, jika Anda tidak memberikan `accounts` parameter, perintah berlaku untuk seluruh rangkaian akun di organisasi Anda.

Contoh berikut menghapus Log VPC Aliran sebagai sumber di akun dan Wilayah yang ditunjuk.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=VPC_FLOW,accounts='["123456789012",
 "111122223333"]',regions='["us-east-1", "us-east-2"]',sourceVersion="2.0"
```

Contoh berikut menghapus Route 53 sebagai sumber di akun dan Wilayah yang ditunjuk.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=ROUTE53,accounts='["123456789012"]',regions='["us-east-1", "us-east-2"]',sourceVersion="2.0"
```

Contoh sebelumnya diformat untuk Linux, macOS, atau Unix, dan mereka menggunakan karakter line-continuation backslash (\) untuk meningkatkan keterbacaan.

CloudTrail log peristiwa di Security Lake

AWS CloudTrail memberi Anda riwayat AWS API panggilan untuk akun Anda, termasuk API panggilan yang dilakukan menggunakan AWS Management Console, alat baris perintah, dan AWS layanan tertentu. AWS SDKs CloudTrail juga memungkinkan Anda untuk mengidentifikasi pengguna dan akun mana yang AWS APIs meminta layanan yang mendukung CloudTrail, alamat IP sumber tempat panggilan dibuat, dan kapan panggilan terjadi. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Security Lake dapat mengumpulkan log yang terkait dengan peristiwa CloudTrail manajemen dan peristiwa CloudTrail data untuk S3 dan Lambda. CloudTrail peristiwa manajemen, peristiwa data S3, dan peristiwa data Lambda adalah tiga sumber terpisah di Security Lake. Akibatnya, mereka memiliki nilai yang berbeda `sourceName`ketika Anda menambahkan salah satunya sebagai sumber log yang dicerna. Peristiwa manajemen, juga dikenal sebagai peristiwa bidang kontrol, memberikan wawasan tentang operasi manajemen yang dilakukan pada sumber daya di Anda Akun AWS. CloudTrail peristiwa data, juga dikenal sebagai operasi pesawat data, menunjukkan operasi sumber daya yang dilakukan pada atau di dalam sumber daya di Anda Akun AWS. Operasi ini sering kali merupakan aktivitas bervolume tinggi.

Untuk mengumpulkan acara CloudTrail manajemen di Security Lake, Anda harus memiliki setidaknya satu jejak organisasi CloudTrail Multi-wilayah yang mengumpulkan acara CloudTrail manajemen baca dan tulis. Logging harus diaktifkan untuk jejak. Jika Anda memiliki logging yang dikonfigurasi di layanan lain, Anda tidak perlu mengubah konfigurasi logging Anda untuk menambahkannya sebagai

sumber log di Security Lake. Security Lake menarik data langsung dari layanan ini melalui aliran peristiwa independen dan duplikat.

Jejak multi-wilayah mengirimkan file log dari beberapa Wilayah ke satu bucket Amazon Simple Storage Service (Amazon S3) untuk satu bucket. Akun AWS Jika Anda sudah memiliki jejak Multi-wilayah yang dikelola melalui CloudTrail konsol atau AWS Control Tower, tidak diperlukan tindakan lebih lanjut.

- Untuk informasi tentang membuat dan mengelola jejak CloudTrail, lihat Membuat jejak untuk organisasi di Panduan AWS CloudTrail Pengguna.
- Untuk informasi tentang membuat dan mengelola jejak AWS Control Tower, lihat AWS Control Tower Tindakan pencatatan dengan AWS CloudTrail di Panduan AWS Control Tower Pengguna.

Saat Anda menambahkan CloudTrail acara sebagai sumber, Security Lake segera mulai mengumpulkan log CloudTrail peristiwa Anda. Ini mengkonsumsi CloudTrail manajemen dan peristiwa data langsung dari CloudTrail melalui aliran peristiwa independen dan duplikat.

Security Lake tidak mengelola CloudTrail acara Anda atau memengaruhi CloudTrail konfigurasi yang ada. Untuk mengelola akses dan retensi CloudTrail acara Anda secara langsung, Anda harus menggunakan konsol CloudTrail layanan atauAPI. Untuk informasi selengkapnya, lihat Melihat CloudTrail peristiwa dengan riwayat peristiwa di Panduan AWS CloudTrail Pengguna.

Daftar berikut menyediakan link GitHub repositori ke referensi pemetaan untuk bagaimana Security Lake menormalkan CloudTrail peristiwa. OCSF

GitHub OCSFrepositori untuk acara CloudTrail

- Sumber versi 1 (v1.0.0-rc.2)
- Versi sumber 2 (v1.1.0)

Log EKS Audit Amazon di Danau Keamanan

Saat Anda menambahkan Log EKS Audit Amazon sebagai sumber, Security Lake mulai mengumpulkan informasi mendalam tentang aktivitas yang dilakukan pada resource Kubernetes yang berjalan di cluster Elastic Kubernetes Service () Anda. EKS EKSLog Audit membantu Anda mendeteksi aktivitas yang berpotensi mencurigakan di EKS klaster Anda dalam Amazon Elastic Kubernetes Service.

Security Lake menggunakan peristiwa Log EKS Audit langsung dari fitur pencatatan pesawat EKS kontrol Amazon melalui aliran log audit yang independen dan duplikatif. Proses ini dirancang agar tidak memerlukan pengaturan tambahan atau memengaruhi konfigurasi pencatatan bidang EKS kontrol Amazon yang ada yang mungkin Anda miliki. Untuk informasi selengkapnya, lihat pencatatan pesawat EKS kontrol Amazon di Panduan EKS Pengguna Amazon.

Log EKS audit Amazon hanya didukung di OCSF v1.1.0. Untuk informasi tentang cara Security Lake menormalkan peristiwa Log EKS AuditOCSF, lihat referensi pemetaan di GitHub OCSFrepositori untuk peristiwa EKS Amazon Audit Logs (v1.1.0).

Rute 53 log kueri resolver di Security Lake

Log kueri resolver Route 53 melacak DNS kueri yang dibuat oleh sumber daya dalam Amazon Virtual Private Cloud (Amazon) Anda. VPC Ini membantu Anda memahami bagaimana aplikasi Anda beroperasi dan menemukan ancaman keamanan.

Saat Anda menambahkan log kueri resolver Route 53 sebagai sumber di Security Lake, Security Lake segera mulai mengumpulkan log kueri resolver Anda langsung dari Route 53 melalui aliran peristiwa independen dan duplikat.

Security Lake tidak mengelola log Route 53 Anda atau memengaruhi konfigurasi pencatatan kueri resolver yang ada. Untuk mengelola log kueri resolver, Anda harus menggunakan konsol layanan Route 53. Untuk informasi selengkapnya, lihat Mengelola konfigurasi pencatatan kueri Resolver di Panduan Pengembang Amazon Route 53.

Daftar berikut menyediakan tautan GitHub repositori ke referensi pemetaan untuk bagaimana Security Lake menormalkan log Route 53. OCSF

GitHub OCSFrepositori untuk log Route 53

- Sumber versi 1 (v1.0.0-rc.2)
- Versi sumber 2 (v1.1.0)

Temuan Security Hub di Security Lake

Temuan Security Hub membantu Anda memahami postur keamanan Anda AWS dan memungkinkan Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub mengumpulkan temuan dari berbagai sumber, termasuk integrasi dengan integrasi produk

pihak ketiga lainnya Layanan AWS, dan pemeriksaan terhadap kontrol Security Hub. Security Hub memproses temuan dalam format standar yang disebut AWS Security Finding Format (ASFF).

Saat Anda menambahkan temuan Security Hub sebagai sumber di Security Lake, Security Lake segera mulai mengumpulkan temuan Anda langsung dari Security Hub melalui aliran peristiwa independen dan duplikat. Security Lake juga mengubah temuan dari ASFF ke Buka Kerangka Skema Keamanan Siber (OCSF) di Danau Keamanan (OCSF).

Security Lake tidak mengelola temuan Security Hub atau memengaruhi pengaturan Security Hub Anda. Untuk mengelola temuan Security Hub, Anda harus menggunakan konsol layanan Security HubAPI, atau AWS CLI. Untuk informasi selengkapnya, lihat Temuan AWS Security Hub di Panduan AWS Security Hub Pengguna.

Daftar berikut menyediakan tautan GitHub repositori ke referensi pemetaan untuk bagaimana Security Lake menormalkan temuan Security Hub. OCSF

GitHub OCSFrepositori untuk temuan Security Hub

- Sumber versi 1 (v1.0.0-rc.2)
- Versi sumber 2 (v1.1.0)

VPCLog Aliran di Danau Keamanan

Fitur VPC Flow Logs Amazon VPC menangkap informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di lingkungan Anda.

Saat Anda menambahkan VPC Flow Logs sebagai sumber di Security Lake, Security Lake segera mulai mengumpulkan VPC Flow Logs Anda. Ini menggunakan VPC Flow Logs langsung dari Amazon VPC melalui aliran Flow Logs yang independen dan duplikat.

Security Lake tidak mengelola Log VPC Aliran atau memengaruhi VPC konfigurasi Amazon Anda. Untuk mengelola Log Aliran, Anda harus menggunakan konsol VPC layanan Amazon. Untuk informasi selengkapnya, lihat Bekerja dengan Log Aliran di Panduan VPC Pengembang Amazon.

Daftar berikut menyediakan link GitHub repositori ke referensi pemetaan untuk bagaimana Security Lake menormalkan VPC Flow Logs. OCSF

GitHub OCSFrepositori untuk VPC Flow Logs

- Sumber versi 1 (v1.0.0-rc.2)

- Versi sumber 2 (v1.1.0)

AWS WAF log di Security Lake

Saat Anda menambahkan AWS WAF sebagai sumber log di Security Lake, Security Lake segera mulai mengumpulkan log. AWS WAF adalah firewall aplikasi web yang dapat Anda gunakan untuk memantau permintaan web yang dikirim pengguna akhir Anda ke aplikasi Anda dan untuk mengontrol akses ke konten Anda. Informasi yang dicatat mencakup waktu AWS WAF menerima permintaan web dari AWS sumber daya Anda, informasi terperinci tentang permintaan, dan detail tentang aturan yang cocok dengan permintaan tersebut.

Security Lake mengkonsumsi AWS WAF log langsung dari AWS WAF melalui aliran log independen dan duplikat. Proses ini dirancang untuk tidak memerlukan pengaturan tambahan atau memengaruhi AWS WAF konfigurasi yang ada yang mungkin Anda miliki. Untuk informasi selengkapnya tentang cara Anda dapat menggunakan AWS WAF untuk melindungi sumber daya aplikasi, lihat Cara AWS WAF kerjanya di Panduan AWS WAF Pengembang.

> **Important**
>
> Jika Anda menggunakan CloudFront distribusi Amazon sebagai tipe sumber daya AWS WAF, Anda harus memilih US East (N.Virginia) untuk menyerap log global di Security Lake.

AWS WAF log hanya didukung di OCSF v1.1.0. Untuk informasi tentang cara Security Lake menormalkan peristiwa AWS WAF logOCSF, lihat referensi pemetaan di GitHub OCSFrepositori untuk AWS WAF log (v1.1.0).

Menghapus Layanan AWS sebagai sumber

Pilih metode akses Anda, dan ikuti langkah-langkah ini untuk menghapus sumber Danau Keamanan yang didukung Layanan AWS secara asli. Anda dapat menghapus sumber untuk satu atau beberapa Wilayah. Saat Anda menghapus sumbernya, Security Lake berhenti mengumpulkan data dari sumber tersebut di Wilayah dan akun yang ditentukan, dan pelanggan tidak dapat lagi mengkonsumsi data baru dari sumbernya. Namun, pelanggan masih dapat mengkonsumsi data yang dikumpulkan Security Lake dari sumbernya sebelum dihapus. Anda hanya dapat menggunakan petunjuk ini untuk menghapus sumber yang didukung secara asli Layanan AWS . Untuk informasi tentang menghapus sumber kustom, lihatMengumpulkan data dari sumber khusus di Security Lake.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Pilih Sumber dari panel navigasi.
3. Pilih sumber, dan pilih Nonaktifkan.
4. Pilih Wilayah atau Wilayah tempat Anda ingin berhenti mengumpulkan data dari sumber ini. Security Lake akan berhenti mengumpulkan data dari sumber dari semua akun di Wilayah yang dipilih.

API

Untuk menghapus Layanan AWS sebagai sumber secara terprogram, gunakan DeleteAwsLogSourcepengoperasian Danau Keamanan. API Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan delete-aws-log-sourceperintah. Parameter `sourceName` dan `regions` diperlukan. Secara opsional, Anda dapat membatasi ruang lingkup penghapusan ke spesifik `accounts` atau spesifik`sourceVersion`.

> **Important**
>
> Bila Anda tidak memberikan parameter dalam perintah Anda, Security Lake mengasumsikan bahwa parameter yang hilang mengacu pada seluruh rangkaian. Misalnya, jika Anda tidak memberikan `accounts` parameter, perintah berlaku untuk seluruh rangkaian akun di organisasi Anda.

Contoh berikut menghapus Log VPC Aliran sebagai sumber di akun dan Wilayah yang ditunjuk.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=VPC_FLOW,accounts='["123456789012",
 "111122223333"]',regions='["us-east-1", "us-east-2"]',sourceVersion="2.0"
```

Contoh berikut menghapus Route 53 sebagai sumber di akun dan Wilayah yang ditunjuk.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=ROUTE53,accounts='["123456789012"]',regions='["us-east-1", "us-
east-2"]',sourceVersion="2.0"
```

Contoh sebelumnya diformat untuk Linux, macOS, atau Unix, dan mereka menggunakan karakter line-continuation backslash (\) untuk meningkatkan keterbacaan.

Mengumpulkan data dari sumber khusus di Security Lake

Amazon Security Lake dapat mengumpulkan log dan peristiwa dari sumber kustom pihak ketiga. Sumber kustom Security Lake adalah layanan pihak ketiga yang mengirimkan log keamanan dan peristiwa ke Amazon Security Lake. Sebelum mengirim data, sumber kustom harus mengonversi log dan peristiwa ke Open Cybersecurity Schema Framework (OCSF) dan memenuhi persyaratan sumber untuk Security Lake termasuk partisi, format file parket dan ukuran objek dan persyaratan tarif.

Untuk setiap sumber kustom, Security Lake menangani hal berikut:

- Memberikan awalan unik untuk sumber di bucket Amazon S3 Anda.
- Membuat peran dalam AWS Identity and Access Management (IAM) yang memungkinkan sumber kustom untuk menulis data ke danau data. Batas izin untuk peran ini ditetapkan oleh kebijakan AWS terkelola yang disebut. `AmazonSecurityLakePermissionsBoundary`
- Membuat AWS Lake Formation tabel untuk mengatur objek yang ditulis sumber ke Security Lake.
- Menetapkan AWS Glue crawler untuk mempartisi data sumber Anda. Crawler mengisi AWS Glue Data Catalog dengan tabel. Ini juga secara otomatis menemukan data sumber baru dan mengekstrak definisi skema.

> **Note**
>
> Anda dapat menambahkan hingga maksimal 50 sumber log kustom di akun.

Untuk menambahkan sumber khusus ke Security Lake, itu harus memenuhi persyaratan berikut. Kegagalan untuk memenuhi persyaratan ini dapat berdampak pada kinerja, dan dapat memengaruhi kasus penggunaan analitik seperti kueri.

- Tujuan — Sumber kustom harus dapat menulis data ke Security Lake sebagai satu set objek S3 di bawah awalan yang ditetapkan ke sumber. Untuk sumber yang berisi beberapa kategori data, Anda harus mengirimkan setiap kelas acara Open Cybersecurity Schema Framework (OCSF) yang

unik sebagai sumber terpisah. Security Lake membuat IAM peran yang memungkinkan sumber kustom untuk menulis ke lokasi yang ditentukan di bucket S3 Anda.

- Format - Setiap objek S3 yang dikumpulkan dari sumber kustom harus diformat sebagai file Apache Parquet.
- Skema - Kelas OCSF acara yang sama harus berlaku untuk setiap catatan dalam objek berformat Parket. Security Lake mendukung Parket versi 1.x dan 2.x. Ukuran halaman data harus dibatasi hingga 1 MB (tidak terkompresi). Ukuran grup baris tidak boleh lebih besar dari 256 MB (dikompresi). Untuk kompresi dalam objek Parket, zstandard lebih disukai.
- Partisi - Objek harus dipartisi berdasarkan wilayah, akun,. AWS eventDay Objek harus diawali dengan*source location*/region=*region*/accountId=*accountID*/eventDay=*yyyyMMdd*/.
- Ukuran dan tarif objek - File yang dikirim ke Security Lake harus dikirim secara bertahap antara 5 menit dan 1 hari acara. Pelanggan dapat mengirim file lebih sering dari 5 menit jika file berukuran lebih besar dari 256MB. Persyaratan objek dan ukuran adalah mengoptimalkan Security Lake untuk Kinerja Kueri. Tidak mengikuti persyaratan sumber kustom mungkin berdampak pada kinerja Security Lake Anda.
- Penyortiran — Dalam setiap objek yang diformat Parket, catatan harus diurutkan berdasarkan waktu untuk mengurangi biaya kueri data.

> **Note**
>
> Gunakan alat OCSF Validasi untuk memverifikasi apakah sumber kustom kompatibel dengan. `OCSF Schema`

Persyaratan partisi untuk menelan sumber khusus di Security Lake

Untuk memfasilitasi pemrosesan dan kueri data yang efisien, kami perlu memenuhi persyaratan partisi dan objek dan ukuran saat menambahkan sumber khusus ke Security Lake:

Partisi

Objek harus dipartisi berdasarkan lokasi sumber,, Wilayah AWS Akun AWS, dan tanggal.

- Jalur data partisi diformat sebagai

/ext/*custom-source-name*/region=*region*/accountId=*accountID*/eventDay=*YYYYMMDD*.

Partisi sampel dengan contoh nama bucket adalahaws-security-data-lake-*us-west-2-lake-uid*/ext/*custom-source-name*/region=*us-west-2*/accountId=*123456789012*/eventDay=*20230428*/.

Daftar berikut menjelaskan parameter yang digunakan dalam partisi jalur S3:

- Nama bucket Amazon S3 tempat Security Lake menyimpan data sumber kustom Anda.
- `source-location`— Awalan untuk sumber kustom di bucket S3 Anda. Security Lake menyimpan semua objek S3 untuk sumber tertentu di bawah awalan ini, dan awalan unik untuk sumber yang diberikan.
- `region`— Wilayah AWS ke mana data diunggah. Misalnya, Anda harus menggunakan US `East (N. Virginia)` untuk mengunggah data ke bucket Security Lake Anda di wilayah AS Timur (Virginia N.).
- `accountId`— Akun AWS ID yang berkaitan dengan catatan di partisi sumber. Untuk catatan yang berkaitan dengan akun di luar AWS, sebaiknya gunakan string seperti `external` atau`external_externalAccountId`. Dengan mengadopsi konveksi penamaan ini, Anda dapat menghindari ambiguitas dalam penamaan akun eksternal IDs sehingga tidak bertentangan dengan AWS akun IDs atau akun eksternal yang IDs dikelola oleh sistem manajemen identitas lainnya.
- `eventDay`— UTC stempel waktu rekaman, dipotong menjadi jam diformat sebagai string delapan karakter (). YYYYMMDD Jika catatan menentukan zona waktu yang berbeda dalam stempel waktu acara, Anda harus mengonversi stempel waktu menjadi UTC kunci partisi ini.

Prasyarat untuk menambahkan sumber khusus di Security Lake

Saat menambahkan sumber khusus, Security Lake membuat IAM peran yang memungkinkan sumber untuk menulis data ke lokasi yang benar di danau data. Nama peran mengikuti format`AmazonSecurityLake-Provider-{name of the custom source}-{region}`, Wilayah AWS di `region` mana Anda menambahkan sumber kustom. Security Lake melampirkan kebijakan untuk peran yang memungkinkan akses ke danau data. Jika Anda telah mengenkripsi data lake dengan AWS KMS kunci yang dikelola pelanggan, Security Lake juga melampirkan kebijakan dengan `kms:Decrypt` dan `kms:GenerateDataKey` izin ke peran

tersebut. Batas izin untuk peran ini ditetapkan oleh kebijakan AWS terkelola yang disebut. `AmazonSecurityLakePermissionsBoundary`

Topik

Memverifikasi izin

Sebelum menambahkan sumber kustom, verifikasi bahwa Anda memiliki izin untuk melakukan tindakan berikut.

Untuk memverifikasi izin Anda, gunakan IAM untuk meninjau IAM kebijakan yang dilampirkan pada IAM identitas Anda. Kemudian, bandingkan informasi dalam kebijakan tersebut dengan daftar tindakan berikut yang harus diizinkan untuk dilakukan untuk menambahkan sumber kustom.

- `glue:CreateCrawler`
- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:StopCrawlerSchedule`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `iam:DeleteRolePolicy`
- `iam:PassRole`
- `lakeformation:RegisterResource`
- `lakeformation:GrantPermissions`
- `s3:ListBucket`
- `s3:PutObject`

Tindakan ini memungkinkan Anda mengumpulkan log dan peristiwa dari sumber khusus, mengirimkannya ke AWS Glue database dan tabel yang benar, dan menyimpannya di Amazon S3.

Jika Anda menggunakan AWS KMS kunci untuk enkripsi sisi server data lake Anda, Anda juga memerlukan izin untuk,`kms:CreateGrant`, `kms:DescribeKey` dan. `kms:GenerateDataKey`

> **Important**
>
> Jika Anda berencana menggunakan konsol Security Lake untuk menambahkan sumber khusus, Anda dapat melewati langkah berikutnya dan melanjutkan keMenambahkan sumber khusus di Security Lake. Konsol Security Lake menawarkan proses yang efisien untuk memulai, dan menciptakan semua peran yang diperlukan atau menggunakan IAM peran yang ada atas nama Anda.
> Jika Anda berencana untuk menggunakan Security Lake API atau AWS CLI menambahkan sumber kustom, lanjutkan dengan langkah berikutnya untuk membuat IAM peran untuk mengizinkan akses tulis ke lokasi bucket Security Lake.

Buat IAM peran untuk mengizinkan akses tulis ke lokasi bucket Security Lake (APIdan langkah AWS CLI-only)

Jika Anda menggunakan Security Lake API atau AWS CLI menambahkan sumber kustom, tambahkan IAM peran ini untuk memberikan AWS Glue izin untuk merayapi data sumber kustom Anda dan mengidentifikasi partisi dalam data. Partisi ini diperlukan untuk mengatur data Anda dan membuat serta memperbarui tabel di Katalog Data.

Setelah membuat IAM peran ini, Anda akan memerlukan Amazon Resource Name (ARN) peran untuk menambahkan sumber kustom.

Anda harus melampirkan kebijakan yang `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole` AWS dikelola.

Untuk memberikan izin yang diperlukan, Anda juga harus membuat dan menyematkan kebijakan sebaris berikut dalam peran Anda Perayap AWS Glue untuk mengizinkan membaca file data dari sumber kustom dan membuat/memperbarui tabel di Katalog Data. AWS Glue

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3WriteRead",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::{{bucketName}}/*"
            ]
        }
    ]
}
```

Lampirkan kebijakan kepercayaan berikut untuk mengizinkan penggunaan yang dapat mengambil peran berdasarkan ID eksternal: Akun AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "glue.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Jika bucket S3 di Wilayah tempat Anda menambahkan sumber kustom dienkripsi dengan pengelola pelanggan AWS KMS key, Anda juga harus melampirkan kebijakan berikut ke peran dan kebijakan utama Anda: KMS

```
{
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey"
        "kms:Decrypt"
    ],
    "Condition": {
        "StringLike": {
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::{{name of S3 bucket created by Security Lake}"
            ]
        }
    },
    "Resource": [
        "{{ARN of customer managed key}}"
```

```
    ]
}
```

Menambahkan sumber khusus di Security Lake

Setelah membuat IAM peran untuk memanggil AWS Glue crawler, ikuti langkah-langkah berikut untuk menambahkan sumber kustom di Security Lake.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin membuat sumber kustom.
3. Pilih Sumber khusus di panel navigasi, lalu pilih Buat sumber kustom.
4. Di bagian Detail sumber kustom, masukkan nama unik global untuk sumber kustom Anda. Kemudian, pilih kelas OCSF acara yang menjelaskan jenis data yang akan dikirim sumber kustom ke Security Lake.
5. Untuk Akun AWS dengan izin untuk menulis data, masukkan Akun AWS ID dan ID Eksternal dari sumber kustom yang akan menulis log dan peristiwa ke data lake.
6. Untuk Akses Layanan, buat dan gunakan peran layanan baru atau gunakan peran layanan yang ada yang memberikan izin Security Lake untuk memanggil AWS Glue.
7. Pilih Buat.

API

Untuk menambahkan sumber khusus secara terprogram, gunakan CreateCustomLogSourcepengoperasian Danau Keamanan. API Gunakan operasi di Wilayah AWS tempat Anda ingin membuat sumber kustom. Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan create-custom-log-sourceperintah.

Dalam permintaan Anda, gunakan parameter yang didukung untuk menentukan pengaturan konfigurasi untuk sumber kustom:

- `sourceName`— Tentukan nama untuk sumbernya. Nama harus menjadi nilai Regional yang unik.
- `eventClasses`— Tentukan satu atau beberapa kelas OCSF acara untuk menggambarkan jenis data yang akan dikirim sumber ke Security Lake. Untuk daftar kelas OCSF acara yang

didukung sebagai sumber di Security Lake, lihat Open Cybersecurity Schema Framework () OCSF.

- `sourceVersion`— Secara opsional, tentukan nilai untuk membatasi pengumpulan log ke versi tertentu dari data sumber kustom.
- `crawlerConfiguration`— Tentukan Nama Sumber Daya Amazon (ARN) dari IAM peran yang Anda buat untuk memanggil AWS Glue crawler. Untuk langkah-langkah mendetail untuk membuat IAM peran, lihat Prasyarat untuk menambahkan sumber kustom
- `providerIdentity`— Tentukan AWS identitas dan ID eksternal yang akan digunakan sumber untuk menulis log dan peristiwa ke danau data.

Contoh berikut menambahkan sumber kustom sebagai sumber log di akun penyedia log yang ditunjuk di Wilayah yang ditunjuk. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake create-custom-log-source \
--source-name EXAMPLE_CUSTOM_SOURCE \
--event-classes '["DNS_ACTIVITY", "NETWORK_ACTIVITY"]' \
--configuration crawlerConfiguration={"roleArn=arn:aws:iam::XXX:role/service-role/
RoleName"},providerIdentity={"externalId=ExternalId,principal=principal"}  \
--region=[“ap-southeast-2”]
```

Menjaga data sumber kustom diperbarui AWS Glue

Setelah Anda menambahkan sumber kustom di Security Lake, Security Lake membuat AWS Glue crawler. Crawler terhubung ke sumber kustom Anda, menentukan struktur data, dan mengisi Katalog AWS Glue Data dengan tabel.

Sebaiknya jalankan crawler secara manual agar skema sumber kustom Anda tetap mutakhir dan mempertahankan fungsionalitas kueri di Athena dan layanan kueri lainnya. Secara khusus, Anda harus menjalankan crawler jika salah satu dari perubahan berikut terjadi dalam kumpulan data input Anda untuk sumber kustom:

- Kumpulan data memiliki satu atau lebih kolom tingkat atas baru.
- Kumpulan data memiliki satu atau lebih bidang baru dalam kolom dengan `struct` tipe data.

Untuk petunjuk tentang menjalankan crawler, lihat Menjadwalkan AWS Glue crawler di Panduan Pengembang.AWS Glue

Security Lake tidak dapat menghapus atau memperbarui crawler yang ada di akun Anda. Jika Anda menghapus sumber kustom, sebaiknya hapus crawler terkait jika Anda berencana membuat sumber kustom dengan nama yang sama di masa mendatang.

Kelas OCSF acara yang didukung

Kelas acara Open Cybersecurity Schema Framework (OCSF) menjelaskan jenis data yang akan dikirim sumber kustom ke Security Lake. Daftar kelas acara yang didukung adalah:

```
public enum OcsfEventClass {
    ACCOUNT_CHANGE,
    API_ACTIVITY,
    APPLICATION_LIFECYCLE,
    AUTHENTICATION,
    AUTHORIZE_SESSION,
    COMPLIANCE_FINDING,
    DATASTORE_ACTIVITY,
    DEVICE_CONFIG_STATE,
    DEVICE_CONFIG_STATE_CHANGE,
    DEVICE_INVENTORY_INFO,
    DHCP_ACTIVITY,
    DNS_ACTIVITY,
    DETECTION_FINDING,
    EMAIL_ACTIVITY,
    EMAIL_FILE_ACTIVITY,
    EMAIL_URL_ACTIVITY,
    ENTITY_MANAGEMENT,
    FILE_HOSTING_ACTIVITY,
    FILE_SYSTEM_ACTIVITY,
    FTP_ACTIVITY,
    GROUP_MANAGEMENT,
    HTTP_ACTIVITY,
    INCIDENT_FINDING,
    KERNEL_ACTIVITY,
    KERNEL_EXTENSION,
    MEMORY_ACTIVITY,
    MODULE_ACTIVITY,
    NETWORK_ACTIVITY,
    NETWORK_FILE_ACTIVITY,
    NTP_ACTIVITY,
```

```
    PATCH_STATE,
    PROCESS_ACTIVITY,
    RDP_ACTIVITY,
    REGISTRY_KEY_ACTIVITY,
    REGISTRY_VALUE_ACTIVITY,
    SCHEDULED_JOB_ACTIVITY,
    SCAN_ACTIVITY,
    SECURITY_FINDING,
    SMB_ACTIVITY,
    SSH_ACTIVITY,
    USER_ACCESS,
    USER_INVENTORY,
    VULNERABILITY_FINDING,
    WEB_RESOURCE_ACCESS_ACTIVITY,
    WEB_RESOURCES_ACTIVITY,
    WINDOWS_RESOURCE_ACTIVITY,
    // 1.3 OCSF event classes
    ADMIN_GROUP_QUERY,
    DATA_SECURITY_FINDING,
    EVENT_LOG_ACTIVITY,
    FILE_QUERY,
    FILE_REMEDIATION_ACTIVITY,
    FOLDER_QUERY,
    JOB_QUERY,
    KERNEL_OBJECT_QUERY,
    MODULE_QUERY,
    NETWORK_CONNECTION_QUERY,
    NETWORK_REMEDIATION_ACTIVITY,
    NETWORKS_QUERY,
    PERIPHERAL_DEVICE_QUERY,
    PROCESS_QUERY,
    PROCESS_REMEDIATION_ACTIVITY,
    REMEDIATION_ACTIVITY,
    SERVICE_QUERY,
    SOFTWARE_INVENTORY_INFO,
    TUNNEL_ACTIVITY,
    USER_QUERY,
    USER_SESSION_QUERY,
    // 1.3 OCSF event classes (Win extension)
    PREFETCH_QUERY,
    REGISTRY_KEY_QUERY,
    REGISTRY_VALUE_QUERY,
    WINDOWS_SERVICE_ACTIVITY
```

```
}
```

Menghapus sumber kustom dari Security Lake

Hapus sumber khusus untuk berhenti mengirim data dari sumber ke Security Lake. Saat Anda menghapus sumbernya, Security Lake berhenti mengumpulkan data dari sumber tersebut di Wilayah dan akun yang ditentukan, dan pelanggan tidak dapat lagi mengkonsumsi data baru dari sumbernya. Namun, pelanggan masih dapat mengkonsumsi data yang dikumpulkan Security Lake dari sumbernya sebelum dihapus. Anda hanya dapat menggunakan petunjuk ini untuk menghapus sumber kustom. Untuk informasi tentang menghapus dukungan asli, lihat. Layanan AWSMengumpulkan data dari Layanan AWS Danau Keamanan

Saat menghapus sumber khusus di Security Lake, Anda harus menonaktifkan setiap sumber di luar konsol Security Lake dengan sumbernya. Kegagalan untuk menonaktifkan integrasi dapat mengakibatkan integrasi sumber terus mengirim log ke Amazon S3.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menghapus sumber kustom.
3. Di panel navigasi, pilih Sumber khusus.
4. Pilih sumber kustom yang ingin Anda hapus.
5. Pilih Deregister sumber kustom dan kemudian pilih Hapus untuk mengonfirmasi tindakan.

API

Untuk menghapus sumber khusus secara terprogram, gunakan DeleteCustomLogSourcepengoperasian Danau Keamanan. API Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan delete-custom-log-sourceperintah. Gunakan operasi di Wilayah AWS tempat Anda ingin menghapus sumber kustom.

Dalam permintaan Anda, gunakan `sourceName` parameter untuk menentukan nama sumber kustom yang akan dihapus. Atau tentukan nama sumber kustom dan gunakan `sourceVersion` parameter untuk membatasi ruang lingkup penghapusan hanya versi data tertentu dari sumber kustom.

Contoh berikut menghapus sumber log kustom dari Security Lake.

Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake delete-custom-log-source \
--source-name EXAMPLE_CUSTOM_SOURCE
```

Manajemen pelanggan di Security Lake

Pelanggan Amazon Security Lake mengkonsumsi log dan peristiwa dari Security Lake. Untuk mengontrol biaya dan mematuhi praktik terbaik akses hak istimewa, Anda memberikan pelanggan akses ke data berdasarkan per sumber. Untuk informasi selengkapnya tentang sumber, lihat Manajemen sumber di Security Lake.

Security Lake mendukung dua jenis akses pelanggan:

- Akses data Pelanggan dengan akses data ke data sumber di Amazon Security Lake diberi tahu tentang objek baru untuk sumber saat data ditulis ke bucket S3. Secara default, pelanggan diberi tahu tentang objek baru melalui HTTPS titik akhir yang mereka sediakan. Atau, pelanggan dapat diberi tahu tentang objek baru dengan melakukan polling antrian Amazon Simple Queue Service (AmazonSQS).
- Akses kueri — Pelanggan dengan akses kueri dapat meminta data yang dikumpulkan Security Lake. Pelanggan ini secara langsung menanyakan tabel AWS Lake Formation di bucket S3 Anda dengan layanan seperti Amazon Athena.

Pelanggan hanya memiliki akses ke data sumber Wilayah AWS yang Anda pilih saat Anda membuat pelanggan. Untuk memberi pelanggan akses ke data dari beberapa Wilayah, Anda dapat menentukan Wilayah tempat Anda membuat pelanggan sebagai Wilayah rollup dan meminta Wilayah lain menyumbangkan data ke sana. Untuk informasi selengkapnya tentang Wilayah rollup dan Wilayah yang berkontribusi, lihat. Mengelola Wilayah di Danau Keamanan

> **Important**
>
> Jumlah maksimum sumber yang diizinkan Security Lake untuk ditambahkan per pelanggan adalah 10. Ini bisa menjadi kombinasi sumber dan AWS sumber kustom.

Topik

- Mengelola akses data untuk pelanggan Security Lake
- Mengelola akses kueri untuk pelanggan Security Lake

Mengelola akses data untuk pelanggan Security Lake

Pelanggan dengan akses data ke data sumber di Amazon Security Lake diberi tahu tentang objek baru untuk sumber saat data ditulis ke bucket S3. Secara default, pelanggan diberi tahu tentang objek baru melalui HTTPS titik akhir yang mereka sediakan. Atau, pelanggan dapat diberi tahu tentang objek baru dengan melakukan polling antrian Amazon Simple Queue Service (AmazonSQS).

Pelanggan diberitahu tentang objek Amazon S3 baru untuk sumber karena objek ditulis ke danau data Security Lake. Pelanggan dapat langsung mengakses objek S3 dan menerima pemberitahuan objek baru melalui titik akhir langganan atau dengan melakukan polling antrian Amazon Simple Queue Service (Amazon). SQS Jenis langganan ini diidentifikasi seperti `S3` pada `accessTypes` parameter CreateSubscriberAPI.

Topik

Prasyarat untuk membuat pelanggan dengan akses data di Security Lake

Anda harus menyelesaikan prasyarat berikut sebelum Anda dapat membuat pelanggan dengan akses data di Security Lake.

Memverifikasi izin

Untuk memverifikasi izin Anda, gunakan IAM untuk meninjau IAM kebijakan yang dilampirkan pada IAM identitas Anda. Kemudian, bandingkan informasi dalam kebijakan tersebut dengan daftar tindakan (izin) berikut yang harus Anda miliki untuk memberi tahu pelanggan saat data baru ditulis ke data lake.

Anda akan memerlukan izin untuk melakukan tindakan berikut:

- `iam:CreateRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:PutRolePolicy`

- lakeformation:GrantPermissions
- lakeformation:ListPermissions
- lakeformation:RegisterResource
- lakeformation:RevokePermissions
- ram:GetResourceShareAssociations
- ram:GetResourceShares
- ram:UpdateResourceShare

Selain daftar sebelumnya, Anda juga memerlukan izin untuk melakukan tindakan berikut:

- events:CreateApiDestination
- events:CreateConnection
- events:DescribeRule
- events:ListApiDestinations
- events:ListConnections
- events:PutRule
- events:PutTargets
- s3:GetBucketNotification
- s3:PutBucketNotification
- sqs:CreateQueue
- sqs:DeleteQueue
- sqs:GetQueueAttributes
- sqs:GetQueueUrl
- sqs:SetQueueAttributes

Dapatkan ID eksternal pelanggan

Untuk membuat pelanggan, selain dari Akun AWS ID pelanggan, Anda juga perlu mendapatkan ID eksternal mereka. ID eksternal adalah pengidentifikasi unik yang disediakan pelanggan kepada Anda. Security Lake menambahkan ID eksternal ke IAM peran pelanggan yang dibuatnya. Anda menggunakan ID eksternal ketika Anda membuat pelanggan di konsol Security Lake, melaluiAPI, atau AWS CLI.

Untuk informasi selengkapnya tentang eksternalIDs, lihat Cara menggunakan ID eksternal saat memberikan akses ke AWS sumber daya Anda kepada pihak ketiga dalam Panduan IAM Pengguna.

> **Important**
>
> Jika Anda berencana menggunakan konsol Security Lake untuk menambahkan pelanggan, Anda dapat melewati langkah berikutnya dan melanjutkan keMembuat pelanggan dengan akses data di Security Lake. Konsol Security Lake menawarkan proses yang efisien untuk memulai, dan menciptakan semua peran yang diperlukan atau menggunakan IAM peran yang ada atas nama Anda.
> Jika Anda berencana untuk menggunakan Security Lake API atau AWS CLI menambahkan pelanggan, lanjutkan dengan langkah berikutnya untuk membuat IAM peran untuk memanggil tujuan EventBridge API.

Buat IAM peran untuk memanggil EventBridge API tujuan (APIdan langkah AWS CLI-only)

Jika Anda menggunakan Security Lake melalui API atau AWS CLI, buat peran di AWS Identity and Access Management (IAM) yang memberikan EventBridge izin Amazon untuk memanggil API tujuan dan mengirim pemberitahuan objek ke titik akhir yang benar. HTTPS

Setelah membuat IAM peran ini, Anda akan memerlukan Amazon Resource Name (ARN) peran untuk membuat pelanggan. IAMPeran ini tidak diperlukan jika pelanggan melakukan polling data dari antrian Amazon Simple Queue Service (AmazonSQS) atau langsung menanyakan data dari. AWS Lake Formation Untuk informasi selengkapnya tentang jenis metode akses data ini (tipe akses), lihatMengelola akses kueri untuk pelanggan Security Lake.

Lampirkan kebijakan berikut ke IAM peran Anda:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowInvokeApiDestination",
            "Effect": "Allow",
            "Action": [
                "events:InvokeApiDestination"
            ],
```

```
            "Resource": [
                "arn:aws:events:{us-west-2}:{123456789012}:api-destination/
AmazonSecurityLake*/*"
            ]
        }
    ]
}
```

Lampirkan kebijakan kepercayaan berikut ke IAM peran Anda untuk mengizinkan EventBridge untuk mengambil peran:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowEventBridgeToAssume",
            "Effect": "Allow",
            "Principal": {
                "Service": "events.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Security Lake secara otomatis membuat IAM peran yang memungkinkan pelanggan membaca data dari data lake (atau peristiwa jajak pendapat dari SQS antrian Amazon jika itu adalah metode pemberitahuan yang disukai). Peran ini dilindungi dengan kebijakan AWS terkelola yang disebut `AmazonSecurityLakePermissionsBoundary`.

Membuat pelanggan dengan akses data di Security Lake

Pilih salah satu metode akses berikut untuk membuat pelanggan dengan akses ke data saat ini Wilayah AWS.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin membuat pelanggan.
3. Di panel navigasi, pilih Pelanggan.

4. Pada halaman Pelanggan, pilih Buat pelanggan.
5. Untuk detail Pelanggan, masukkan nama Pelanggan dan Deskripsi opsional.

   Wilayah terisi otomatis seperti yang Anda pilih saat ini Wilayah AWS dan tidak dapat diubah.
6. Untuk sumber Log dan acara, pilih sumber mana yang diizinkan untuk dikonsumsi pelanggan.
7. Untuk metode akses Data, pilih S3 untuk mengatur akses data bagi pelanggan.
8. Untuk kredensyal Pelanggan, berikan ID pelanggan dan Akun AWS ID eksternal.
9. (Opsional) Untuk detail Pemberitahuan, jika Anda ingin Security Lake membuat SQS antrian Amazon yang dapat dipolling pelanggan untuk pemberitahuan objek, pilih SQS antrian. Jika Anda ingin Security Lake mengirim notifikasi EventBridge ke HTTPS titik akhir, pilih Titik akhir Berlangganan.

   Jika Anda memilih titik akhir Berlangganan, lakukan juga hal berikut:

   a. Masukkan titik akhir Berlangganan. Contoh format endpoint yang valid meliputi**`http://example.com`**. Secara opsional, Anda juga dapat memberikan nama HTTPS kunci dan nilai HTTPS kunci.
   b. Untuk Akses Layanan, buat IAM peran baru atau gunakan IAM peran yang ada yang memberikan EventBridge izin untuk memanggil API tujuan dan mengirim pemberitahuan objek ke titik akhir yang benar.

      Untuk informasi tentang membuat IAM peran baru, lihat Membuat IAM peran untuk memanggil EventBridge API tujuan.
10. (Opsional) Untuk Tag, masukkan sebanyak 50 tag untuk ditetapkan ke pelanggan.

    Tag adalah label yang dapat Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Tag dapat membantu Anda mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan berbagai cara. Untuk mempelajari selengkapnya, lihat Menandai sumber daya Danau Keamanan.
11. Pilih Buat.

API

Untuk membuat pelanggan dengan akses data secara terprogram, gunakan CreateSubscriberpengoperasian Danau Keamanan. API Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah create-subscriber.

Dalam permintaan Anda, gunakan parameter ini untuk menentukan pengaturan berikut untuk pelanggan:

- Untuk`sources`, tentukan setiap sumber yang ingin diakses oleh pelanggan.
- Untuk`subscriberIdentity`, tentukan ID AWS akun dan ID eksternal yang akan digunakan pelanggan untuk mengakses data sumber.
- Untuk`subscriber-name`, tentukan nama pelanggan.
- Untuk `accessTypes`, tentukan `S3`.

Contoh 1

Contoh berikut membuat pelanggan dengan akses ke data di AWS Wilayah saat ini untuk identitas pelanggan yang ditentukan untuk sumber AWS .

```
$ aws securitylake create-subscriber \
--subscriber-identity {"accountID": 1293456789123,"externalId": 123456789012} \
--sources [{"awsLogSource": {"sourceName": VPC_FLOW, "sourceVersion": 2.0}}] \
--subscriber-name subscriber name \
--access-types S3
```

Contoh 2

Contoh berikut membuat pelanggan dengan akses ke data di AWS Wilayah saat ini untuk identitas pelanggan yang ditentukan untuk sumber kustom.

```
$ aws securitylake create-subscriber \
--subscriber-identity {"accountID": 1293456789123,"externalId": 123456789012} \
--sources [{"customLogSource": {"sourceName": custom-source-name,
 "sourceVersion": 2.0}}] \
--subscriber-name subscriber name
--access-types S3
```

Contoh sebelumnya diformat untuk Linux, macOS, atau Unix, dan mereka menggunakan karakter line-continuation backslash (\) untuk meningkatkan keterbacaan.

(Opsional) Setelah Anda membuat pelanggan, gunakan CreateSubscriberNotificationoperasi untuk menentukan cara memberi tahu pelanggan ketika data baru ditulis ke danau data untuk sumber yang Anda ingin pelanggan akses. Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan create-subscriber-notificationperintah.

- Untuk mengganti metode notifikasi default (HTTPStitik akhir) dan membuat SQS antrian Amazon, tentukan nilai untuk parameter. `sqsNotificationConfiguration`
- Jika Anda lebih suka notifikasi dengan HTTPS titik akhir, tentukan nilai untuk `httpsNotificationConfiguration` parameter.
- Untuk `targetRoleArn` bidang, tentukan IAM peran ARN yang Anda buat untuk memanggil EventBridge API tujuan.

```
$ aws securitylake create-subscriber-notification \
--subscriber-id "12345ab8-1a34-1c34-1bd4-12345ab9012" \
--configuration
 httpsNotificationConfiguration={"targetRoleArn"="arn:aws:iam::XXX:role/service-role/RoleName", "endpoint"="https://account-management.$3.$2.securitylake.aws.dev/v1/datalake"}
```

Untuk mendapatkan`subscriberID`, gunakan ListSubscriberspengoperasian Danau KeamananAPI. Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah list-subscriber.

```
$ aws securitylake list-subscribers
```

Untuk selanjutnya mengubah metode notifikasi (SQSantrian Amazon atau HTTPS titik akhir) untuk pelanggan, gunakan UpdateSubscriberNotificationoperasi atau, jika Anda menggunakan AWS CLI, jalankan perintah. update-subscriber-notification Anda juga dapat mengubah metode notifikasi dengan menggunakan konsol Security Lake: pilih pelanggan di halaman Pelanggan, lalu pilih Edit.

Contoh pesan pemberitahuan objek

Contoh berikut menunjukkan pemberitahuan acara dalam format JSON struktur untuk `CreateSubscriberNotification` operasi.

```
{
  "source": "aws.s3",
  "time": "2021-11-12T00:00:00Z",
  "account": "123456789012",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket"
```

```
  ],
  "detail": {
    "bucket": {
      "name": "amzn-s3-demo-bucket"
    },
    "object": {
      "key": "example-key",
      "size": 5,
      "etag": "b57f9512698f4b09e608f4f2a65852e5"
    },
    "request-id": "N4N7GDK58NMKJ12R",
    "requester": "securitylake.amazonaws.com"
  }
}
```

Memperbarui pelanggan data di Security Lake

Anda dapat memperbarui pelanggan dengan mengubah sumber dari mana pelanggan mengkonsumsi. Anda juga dapat menetapkan atau mengedit tag untuk pelanggan. Tag adalah label yang dapat Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu, termasuk pelanggan. Untuk mempelajari selengkapnya, lihat Menandai sumber daya Danau Keamanan.

Pilih salah satu metode akses, dan ikuti langkah-langkah ini untuk menentukan sumber baru untuk langganan yang ada.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Di panel navigasi, pilih Pelanggan.
3. Pilih pelanggan.
4. Pilih Edit, lalu lakukan salah satu hal berikut:
   - Untuk memperbarui sumber untuk pelanggan, masukkan pengaturan baru di bagian Log dan sumber acara.
   - Untuk menetapkan atau mengedit tag untuk pelanggan, ubah tag seperlunya di bagian Tag.
5. Setelah selesai, pilih Simpan.

API

Untuk memperbarui sumber akses data untuk pelanggan secara terprogram, gunakan UpdateSubscriberpengoperasian Danau Keamanan. API Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah update-subscriber. Dalam permintaan Anda, gunakan `sources` parameter untuk menentukan setiap sumber yang Anda ingin pelanggan akses.

```
$ aws securitylake update-subscriber --subscriber-id subscriber ID
```

Untuk daftar pelanggan yang terkait dengan organisasi Akun AWS atau tertentu, gunakan ListSubscribersoperasi. Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah list-subscriber.

```
$ aws securitylake list-subscribers
```

Untuk meninjau pengaturan saat ini untuk pelanggan tertentu, gunakan GetSubscriberoperasi. jalankan perintah get-subscriber. Security Lake kemudian mengembalikan nama dan deskripsi pelanggan, ID eksternal, dan informasi tambahan. Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah get-subscriber.

Untuk memperbarui metode notifikasi untuk pelanggan, gunakan UpdateSubscriberNotificationoperasi. Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan update-subscriber-notificationperintah. Misalnya, Anda dapat menentukan HTTPS titik akhir baru untuk pelanggan atau beralih dari HTTPS titik akhir ke antrian Amazon. SQS

Menghapus pelanggan data dari Security Lake

Jika Anda tidak lagi ingin pelanggan mengkonsumsi data dari Security Lake, Anda dapat menghapus pelanggan dengan mengikuti langkah-langkah ini.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Di panel navigasi, pilih Pelanggan.
3. Pilih pelanggan yang ingin Anda hapus.

4. Pilih Hapus dan konfirmasikan tindakan. Ini akan menghapus pelanggan dan semua pengaturan notifikasi terkait.

API

Berdasarkan skenario Anda, lakukan salah satu hal berikut:

- Untuk menghapus pelanggan dan semua pengaturan pemberitahuan terkait, gunakan DeleteSubscriberpengoperasian Danau API Keamanan. Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah delete-subscriber.
- Untuk mempertahankan pelanggan tetapi menghentikan notifikasi masa depan kepada pelanggan, gunakan DeleteSubscriberNotificationpengoperasian Danau Keamanan. API Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan delete-subscriber-notificationperintah run.

Mengelola akses kueri untuk pelanggan Security Lake

Pelanggan dengan akses kueri dapat meminta data yang dikumpulkan Security Lake. Pelanggan ini langsung menanyakan AWS Lake Formation tabel di bucket S3 Anda dengan layanan seperti Amazon Athena. Meskipun mesin kueri utama untuk Security Lake adalah Athena, Anda juga dapat menggunakan layanan lain, seperti Amazon Redshift Spectrum dan SQL Spark, yang terintegrasi dengan. AWS Glue Data Catalog

Pelanggan meminta data sumber dari AWS Lake Formation tabel di bucket S3 Anda dengan menggunakan layanan seperti Amazon Athena. Jenis langganan ini diidentifikasi seperti `LAKEFORMATION` pada `accessTypes` parameter CreateSubscriberAPI.

> **Note**
>
> Bagian ini menjelaskan cara memberikan akses kueri ke pelanggan pihak ketiga. Untuk informasi tentang menjalankan kueri terhadap data lake Anda sendiri, lihatLangkah 4: Lihat dan kueri data Anda sendiri.

Topik

- Prasyarat untuk membuat pelanggan dengan akses kueri di Security Lake
- Membuat pelanggan dengan akses kueri di Security Lake

- Mengedit pelanggan dengan akses kueri di Security Lake

Prasyarat untuk membuat pelanggan dengan akses kueri di Security Lake

Anda harus menyelesaikan prasyarat berikut sebelum Anda dapat membuat pelanggan dengan akses data di Security Lake.

Memverifikasi izin

Sebelum membuat pelanggan dengan akses kueri, verifikasi bahwa Anda memiliki izin untuk melakukan daftar tindakan berikut.

Untuk memverifikasi izin Anda, gunakan IAM untuk meninjau IAM kebijakan yang dilampirkan pada IAM identitas Anda. Kemudian, bandingkan informasi dalam kebijakan tersebut dengan daftar tindakan berikut yang harus Anda lakukan untuk membuat pelanggan dengan akses kueri.

- `iam:CreateRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `lakeformation:GrantPermissions`
- `lakeformation:ListPermissions`
- `lakeformation:RegisterResource`
- `lakeformation:RevokePermissions`
- `ram:GetResourceShareAssociations`
- `ram:GetResourceShares`
- `ram:UpdateResourceShare`

> **Important**
>
> Setelah Anda memverifikasi izin:
>
> - Jika Anda berencana untuk menggunakan konsol Security Lake untuk menambahkan pelanggan dengan akses kueri, Anda dapat melewati langkah berikutnya dan melanjutkan

ke[Izin administrator Grant Lake Formation](). Security Lake menciptakan semua IAM peran yang diperlukan atau menggunakan peran yang ada atas nama Anda.

- Jika Anda berencana untuk menggunakan Security Lake API atau CLI menambahkan pelanggan dengan akses kueri, lanjutkan dengan langkah berikutnya untuk membuat IAM peran untuk menanyakan data Security Lake.

Buat IAM peran untuk menanyakan data Security Lake (APIdan langkah AWS CLI-only)

Saat menggunakan Security Lake API atau AWS CLI untuk memberikan akses kueri ke pelanggan, Anda harus membuat peran bernama`AmazonSecurityLakeMetaStoreManager`. Security Lake menggunakan peran ini untuk mendaftarkan AWS Glue partisi dan memperbarui AWS Glue tabel. Anda mungkin telah membuat peran ini saat [Buat IAM peran yang diperlukan]().

Izin administrator Grant Lake Formation

Anda juga harus menambahkan izin administrator Lake Formation ke IAM peran yang Anda gunakan untuk mengakses konsol Security Lake dan menambahkan pelanggan.

Anda dapat memberikan izin administrator Lake Formation untuk peran Anda dengan mengikuti langkah-langkah berikut:

1. Buka konsol Lake Formation di https://console.aws.amazon.com/lakeformation/.
2. Masuk sebagai pengguna administratif.
3. Jika jendela Selamat Datang di Lake Formation muncul, pilih pengguna yang Anda buat atau pilih di Langkah 1, lalu pilih Mulai.
4. Jika Anda tidak melihat jendela Selamat Datang di Lake Formation, lakukan langkah-langkah berikut untuk mengonfigurasi Administrator Lake Formation.
    1. Di panel navigasi, di bawah Izin, pilih Peran dan tugas administratif. Di bagian Administrator danau data, pilih Pilih administrator.
    2. Di kotak dialog Kelola data lake administrator, untuk IAM pengguna dan peran, pilih peran administrator yang digunakan saat mengakses konsol Security Lake, lalu pilih Simpan.

Untuk informasi selengkapnya tentang mengubah izin untuk administrator data lake, lihat [Membuat administrator data lake di Panduan AWS Lake Formation]() Pengembang.

IAMPeran harus memiliki SELECT hak istimewa pada database dan tabel yang ingin Anda berikan akses kepada pelanggan. Untuk petunjuk tentang cara melakukannya, lihat Memberikan izin Katalog Data menggunakan metode sumber daya bernama di Panduan AWS Lake Formation Pengembang.

Membuat pelanggan dengan akses kueri di Security Lake

Pilih metode pilihan Anda untuk membuat pelanggan dengan akses kueri saat ini Wilayah AWS. Pelanggan dapat meminta data hanya dari Wilayah AWS yang dibuat. Untuk membuat pelanggan, Anda harus memiliki Akun AWS ID dan ID eksternal pelanggan. ID eksternal adalah pengidentifikasi unik yang disediakan pelanggan kepada Anda. Untuk informasi selengkapnya tentang eksternalIDs, lihat Cara menggunakan ID eksternal saat memberikan akses ke AWS sumber daya Anda kepada pihak ketiga dalam Panduan IAM Pengguna.

> **Note**
>
> Security Lake tidak mendukung berbagi data lintas akun Lake Formation versi 1. Anda harus memperbarui berbagi data lintas akun Lake Formation ke versi 2 atau versi 3. Untuk langkah-langkah memperbarui pengaturan versi Cross account melalui AWS Lake Formation konsol atau AWS CLI, lihat Untuk mengaktifkan versi baru di Panduan AWS Lake Formation Pengembang.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.

   Masuk ke akun administrator yang didelegasikan.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin membuat pelanggan.
3. Di panel navigasi, pilih Pelanggan.
4. Pada halaman Pelanggan, pilih Buat pelanggan.
5. Untuk detail Pelanggan, masukkan nama Pelanggan dan Deskripsi opsional.

   Wilayah terisi otomatis seperti yang Anda pilih saat ini Wilayah AWS dan tidak dapat diubah.
6. Untuk sumber Log dan peristiwa, pilih sumber mana yang ingin disertakan Security Lake saat mengembalikan hasil kueri.
7. Untuk metode akses Data, pilih Lake Formation untuk membuat akses kueri bagi pelanggan.

8. Untuk kredensi Pelanggan, berikan ID pelanggan dan Akun AWS ID eksternal.
9. (Opsional) Untuk Tag, masukkan sebanyak 50 tag untuk ditetapkan ke pelanggan.

   Tag adalah label yang dapat Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Tag dapat membantu Anda mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan berbagai cara. Untuk mempelajari selengkapnya, lihat Menandai sumber daya Danau Keamanan.
10. Pilih Buat.

API

Untuk membuat pelanggan dengan akses kueri secara terprogram, gunakan CreateSubscriberpengoperasian Danau Keamanan. API Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah create-subscriber.

Dalam permintaan Anda, gunakan parameter ini untuk menentukan pengaturan berikut untuk pelanggan:

- Untuk `accessTypes`, tentukan `LAKEFORMATION`.
- Untuk`sources`, tentukan setiap sumber yang ingin disertakan Security Lake saat mengembalikan hasil kueri.
- Untuk`subscriberIdentity`, tentukan AWS identitas dan ID eksternal yang digunakan pelanggan untuk menanyakan data sumber.

Contoh berikut membuat pelanggan dengan akses query di AWS Wilayah saat ini untuk identitas pelanggan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake create-subscriber \
--subscriber-identity {"accountID": 129345678912,"externalId": 123456789012} \
--sources [{"awsLogSource": {"sourceName": VPC_FLOW, "sourceVersion": 2.0}}] \
--subscriber-name subscriber name \
--access-types LAKEFORMATION
```

Menyiapkan berbagi tabel lintas akun (langkah pelanggan)

Security Lake menggunakan berbagi tabel lintas akun Lake Formation untuk mendukung akses kueri pelanggan. Saat Anda membuat pelanggan dengan akses kueri di konsol Security Lake, API AWS CLI, atau Security Lake membagikan informasi tentang tabel Lake Formation yang relevan dengan pelanggan dengan membuat pembagian sumber daya di AWS Resource Access Manager ()AWS RAM.

Saat Anda membuat jenis pengeditan tertentu ke pelanggan dengan akses kueri, Security Lake membuat pembagian sumber daya baru. Untuk informasi selengkapnya, lihat Mengedit pelanggan dengan akses kueri di Security Lake.

Pelanggan harus mengikuti langkah-langkah ini untuk mengkonsumsi data dari tabel Lake Formation Anda:

1. Terima pembagian sumber daya — Pelanggan harus menerima pembagian sumber daya yang memiliki `resourceShareArn` dan `resourceShareName` yang dihasilkan saat Anda membuat atau mengedit pelanggan. Pilih salah satu metode akses berikut:
   - Untuk konsol dan AWS CLI, lihat Menerima undangan berbagi sumber daya dari AWS RAM.
   - UntukAPI, panggil. GetResourceShareInvitationsAPI Filter berdasarkan `resourceShareArn` dan `resourceShareName` untuk menemukan pembagian sumber daya yang benar. Terima undangan dengan AcceptResourceShareInvitationAPI.

   Undangan berbagi sumber daya kedaluwarsa dalam 12 jam, jadi Anda harus memvalidasi dan menerima undangan dalam waktu 12 jam. Jika undangan kedaluwarsa, Anda terus melihatnya dalam `PENDING` status, tetapi menerimanya tidak akan memberi Anda akses ke sumber daya bersama. Ketika lebih dari 12 jam telah berlalu, hapus pelanggan Lake Formation dan buat ulang pelanggan untuk mendapatkan undangan berbagi sumber daya baru.
2. Buat tautan sumber daya ke database bersama — Pelanggan harus membuat tautan sumber daya ke database Lake Formation bersama di AWS Lake Formation (jika menggunakan konsol) atau AWS Glue (jika menggunakanAPI/AWSCLI). Tautan sumber daya ini mengarahkan akun pelanggan ke database bersama. Pilih salah satu metode akses berikut:
   - Untuk konsol dan AWS CLI, lihat Membuat tautan sumber daya ke database Katalog Data bersama. di Panduan AWS Lake Formation Pengembang.
   - Kami menyarankan agar pelanggan juga membuat database unik dengan tabel tautan sumber daya CreateDatabaseAPIuntuk menyimpan.

3. Kueri tabel bersama — Layanan seperti Amazon Athena dapat merujuk ke tabel secara langsung, dan data baru yang dikumpulkan Security Lake secara otomatis tersedia untuk kueri. Kueri berjalan di pelanggan Akun AWS, dan biaya yang dikeluarkan dari kueri ditagih ke pelanggan. Anda dapat mengontrol akses baca ke sumber daya di akun Security Lake Anda sendiri.

Untuk informasi selengkapnya tentang pemberian izin lintas akun, lihat Berbagi data lintas akun di Lake Formation di Panduan Pengembang.AWS Lake Formation

Mengedit pelanggan dengan akses kueri di Security Lake

Security Lake mendukung pengeditan ke pelanggan dengan akses kueri. Anda dapat mengedit nama pelanggan, deskripsi, ID eksternal, prinsipal (Akun AWS ID), dan sumber log yang dapat dikonsumsi pelanggan. Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengedit pelanggan dengan akses kueri saat ini Wilayah AWS.

> **Note**
>
> Security Lake tidak mendukung berbagi data lintas akun Lake Formation versi 1. Anda harus memperbarui berbagi data lintas akun Lake Formation ke versi 2 atau versi 3. Untuk langkah-langkah memperbarui pengaturan versi Cross account melalui AWS Lake Formation konsol atau AWS CLI, lihat Untuk mengaktifkan versi baru di Panduan AWS Lake Formation Pengembang.

Console

Berdasarkan detail yang ingin Anda edit, ikuti langkah-langkah yang disediakan untuk tindakan itu saja.

Untuk mengedit nama pelanggan

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.

   Masuk ke akun administrator yang didelegasikan.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengedit detail pelanggan.
3. Di panel navigasi, pilih Pelanggan.

4. Pada halaman Pelanggan, gunakan tombol radio untuk memilih pelanggan yang ingin Anda edit. Metode akses data untuk pelanggan yang dipilih harus LAKEFORMATION.
5. Pilih Edit.
6. Masukkan nama Pelanggan baru, dan pilih Simpan.

Untuk mengedit deskripsi pelanggan

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.

   Masuk ke akun administrator yang didelegasikan.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengedit pelanggan.
3. Di panel navigasi, pilih Pelanggan.
4. Pada halaman Pelanggan, gunakan tombol radio untuk memilih pelanggan yang ingin Anda edit. Metode akses data untuk pelanggan yang dipilih harus LAKEFORMATION.
5. Pilih Edit.
6. Masukkan deskripsi baru untuk pelanggan, dan pilih Simpan.

Untuk mengedit ID eksternal

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.

   Masuk ke akun administrator yang didelegasikan.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengedit detail pelanggan.
3. Di panel navigasi, pilih Pelanggan.
4. Pada halaman Pelanggan, gunakan tombol radio untuk memilih pelanggan yang ingin Anda edit. Metode akses data untuk pelanggan yang dipilih harus LAKEFORMATION.
5. Pilih Edit.
6. Masukkan ID Eksternal baru yang telah disediakan pelanggan, dan pilih Simpan.

   Menyimpan ID eksternal baru secara otomatis menghapus pembagian AWS RAM sumber daya sebelumnya dan membuat pembagian sumber daya baru untuk pelanggan.
7. Pelanggan harus menerima pembagian sumber daya baru dengan mengikuti langkah 1 inMenyiapkan berbagi tabel lintas akun (langkah pelanggan). Pastikan Amazon Resource

Name (ARN) yang muncul di detail pelanggan sama dengan di konsol Lake Formation. Tautan sumber daya ke tabel bersama tetap apa adanya, sehingga pelanggan tidak perlu membuat tautan sumber daya baru.

Untuk mengedit prinsipal (Akun AWS ID)

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.

   Masuk ke akun administrator yang didelegasikan.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengedit detail pelanggan.
3. Di panel navigasi, pilih Pelanggan.
4. Pada halaman Pelanggan, gunakan tombol radio untuk memilih pelanggan yang ingin Anda edit. Metode akses data untuk pelanggan yang dipilih harus LAKEFORMATION.
5. Pilih Edit.
6. Masukkan Akun AWS ID baru pelanggan, dan pilih Simpan.

   Menyimpan ID akun baru secara otomatis menghapus pembagian AWS RAM sumber daya sebelumnya sehingga prinsipal sebelumnya tidak dapat menggunakan sumber log dan peristiwa. Security Lake menciptakan pembagian sumber daya baru.
7. Dengan menggunakan kredensi prinsipal baru, pelanggan harus menerima pembagian sumber daya baru dan membuat tautan sumber daya ke tabel bersama. Ini memberi akses utama baru ke sumber daya bersama. Untuk petunjuk, lihat langkah 1 dan 2 diMenyiapkan berbagi tabel lintas akun (langkah pelanggan). Pastikan ARN yang muncul di detail pelanggan sama dengan di konsol Lake Formation.

Untuk mengedit log dan sumber peristiwa

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.

   Masuk ke akun administrator yang didelegasikan.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengedit detail pelanggan.
3. Di panel navigasi, pilih Pelanggan.
4. Pada halaman Pelanggan, gunakan tombol radio untuk memilih pelanggan yang ingin Anda edit. Metode akses data untuk pelanggan yang dipilih harus LAKEFORMATION.

5. Pilih Edit.
6. Hapus pilihan sumber yang ada atau pilih sumber yang ingin Anda tambahkan. Jika Anda membatalkan pilihan sumber, tidak ada tindakan lebih lanjut yang diperlukan dari pihak Anda. Jika Anda memilih untuk menambahkan sumber, tidak ada undangan berbagi sumber daya baru yang dibuat. Namun, Security Lake memperbarui tabel Lake Formation bersama berdasarkan sumber yang ditambahkan. Pelanggan harus membuat tautan sumber daya ke tabel bersama yang diperbarui sehingga mereka dapat menanyakan data sumber. Untuk instruksi, lihat langkah 2 diMenyiapkan berbagi tabel lintas akun (langkah pelanggan).
7. Pilih Simpan.

API

Untuk mengedit pelanggan dengan akses kueri secara terprogram, gunakan UpdateSubscriberpengoperasian Danau Keamanan. API Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah update-subscriber. Dalam permintaan Anda, gunakan parameter yang didukung untuk menentukan pengaturan berikut untuk pelanggan:

- Untuk`subscriberName`, tentukan nama pelanggan baru.
- Untuk`subscriberDescription`, tentukan deskripsi baru.
- Untuk`subscriberIdentity`, tentukan prinsipal (Akun AWS ID) dan ID eksternal yang akan digunakan pelanggan untuk menanyakan data sumber. Anda harus memberikan ID utama dan eksternal. Jika Anda ingin menjaga salah satu dari nilai-nilai ini sama, berikan nilai saat ini.
  - Memperbarui hanya ID eksternal - Tindakan ini menghapus pembagian AWS RAM sumber daya sebelumnya dan membuat pembagian sumber daya baru untuk pelanggan. Pelanggan harus menerima pembagian sumber daya baru dengan mengikuti langkah 1 inMenyiapkan berbagi tabel lintas akun (langkah pelanggan). Tautan sumber daya ke tabel bersama tetap apa adanya, sehingga pelanggan tidak perlu membuat tautan sumber daya baru.
  - Hanya memperbarui prinsipal - Tindakan ini menghapus pembagian AWS RAM sumber daya sebelumnya sehingga prinsipal sebelumnya tidak dapat menggunakan sumber log dan peristiwa. Security Lake menciptakan pembagian sumber daya baru. Dengan menggunakan kredensi prinsipal baru, pelanggan harus menerima pembagian sumber daya baru dan membuat tautan sumber daya ke tabel bersama. Ini memberi akses utama baru ke sumber daya bersama. Untuk petunjuk, lihat langkah 1 dan 2 diMenyiapkan berbagi tabel lintas akun (langkah pelanggan).

Untuk memperbarui ID eksternal dan prinsipal, ikuti langkah 1 dan 2 diMenyiapkan berbagi tabel lintas akun (langkah pelanggan).

- Untuk`sources`, hapus sumber yang ada atau tentukan sumber yang ingin Anda tambahkan. Jika Anda menghapus sumber, tidak ada tindakan lebih lanjut yang diperlukan dari pihak Anda. Jika Anda menambahkan sumber, tidak ada undangan berbagi sumber daya baru yang dibuat. Namun, Security Lake memperbarui tabel Lake Formation bersama berdasarkan sumber yang ditambahkan. Pelanggan harus membuat tautan sumber daya ke tabel bersama yang diperbarui sehingga mereka dapat menanyakan data sumber. Untuk instruksi, lihat langkah 2 diMenyiapkan berbagi tabel lintas akun (langkah pelanggan).

Pertanyaan Danau Keamanan

Anda dapat menanyakan data yang disimpan Security Lake dalam AWS Lake Formation database dan tabel. Anda juga dapat membuat pelanggan pihak ketiga di konsol Security Lake, API, atau AWS CLI. Pelanggan pihak ketiga juga dapat menanyakan data Lake Formation dari sumber yang Anda tentukan.

Administrator danau data Lake Formation harus memberikan `SELECT` izin pada database dan tabel yang relevan ke identitas IAM yang menanyakan data. Pelanggan juga harus dibuat di Security Lake sebelum dapat meminta data. Untuk informasi selengkapnya tentang cara membuat pelanggan dengan akses kueri, lihatMengelola akses kueri untuk pelanggan Security Lake.

Topik

- Kueri Security Lake untuk AWS sumber versi 1 (OCSF1.0.0-rc.2)
- Kueri Security Lake untuk versi AWS sumber 2 (OCSF1.1.0)

Kueri Security Lake untuk AWS sumber versi 1 (OCSF1.0.0-rc.2)

Bagian berikut memberikan panduan tentang kueri data dari Security Lake dan menyertakan beberapa contoh kueri untuk sumber yang didukung secara asli untuk versi AWS sumber 1. AWS Kueri ini dirancang untuk mengambil data secara spesifik. Wilayah AWS Contoh-contoh ini menggunakan us-east-1 (US East (Virginia N.)). Selain itu, contoh query menggunakan `LIMIT 25` parameter, yang mengembalikan hingga 25 record. Anda dapat menghilangkan parameter ini atau menyesuaikannya berdasarkan preferensi Anda. Untuk contoh lainnya, lihat GitHub direktori Amazon Security Lake OCSF Queries.

Tabel sumber log

Saat Anda menanyakan data Security Lake, Anda harus menyertakan nama tabel Lake Formation di mana data berada.

```
SELECT *
   FROM
 amazon_security_lake_glue_db_DB_Region.amazon_security_lake_table_DB_Region_SECURITY_LAKE_TABL
   WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
```

```
   LIMIT 25
```

Nilai umum untuk tabel sumber log meliputi yang berikut:

- `cloud_trail_mgmt_1_0`— acara AWS CloudTrail manajemen
- `lambda_execution_1_0`— peristiwa CloudTrail data untuk Lambda
- `s3_data_1_0`— peristiwa CloudTrail data untuk S3
- `route53_1_0`- Log kueri penyelesai Amazon Route 53
- `sh_findings_1_0`— AWS Security Hub temuan
- `vpc_flow_1_0`— Log Aliran Amazon Virtual Private Cloud (AmazonVPC)

Contoh: Semua temuan Security Hub dalam tabel **`sh_findings_1_0`** dari Wilayah us-east-1

```
SELECT *
   FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
   WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
   LIMIT 25
```

Database Wilayah

Saat Anda menanyakan data Security Lake, Anda harus menyertakan nama Wilayah database tempat Anda menanyakan data. Untuk daftar lengkap Wilayah basis data tempat Danau Keamanan saat ini tersedia, lihat titik akhir Amazon Security Lake.

Contoh: Daftar AWS CloudTrail aktivitas dari sumber IP

Contoh berikut mencantumkan semua CloudTrail aktivitas dari IP sumber *`192.0.2.1`* yang direkam setelah *`20230301`* (01 Maret 2023), dalam tabel *`cloud_trail_mgmt_1_0`* dari *`us-east-1`* `DB_Region`.

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay > '20230301' AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

Tanggal partisi

Dengan mempartisi data Anda, Anda dapat membatasi jumlah data yang dipindai oleh setiap kueri, sehingga meningkatkan kinerja dan mengurangi biaya. Security Lake mengimplementasikan partisi melaluieventDay,region, dan parameter. accountid eventDaypartisi menggunakan formatYYYYMMDD.

Ini adalah contoh query menggunakan eventDay partisi:

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay > '20230301'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
```

Nilai umum untuk eventDay meliputi yang berikut:

Peristiwa yang terjadi dalam 1 tahun terakhir

```
> cast(date_format(current_timestamp - INTERVAL '1' year, '%Y%m%d%H') as
varchar)
```

Peristiwa yang terjadi dalam 1 bulan terakhir

```
> cast(date_format(current_timestamp - INTERVAL '1' month, '%Y%m%d%H')
as varchar)
```

Peristiwa yang terjadi dalam 30 hari terakhir

```
> cast(date_format(current_timestamp - INTERVAL '30' day, '%Y%m%d%H') as
varchar)
```

Peristiwa yang terjadi dalam 12 jam terakhir

```
> cast(date_format(current_timestamp - INTERVAL '12' hour, '%Y%m%d%H')
as varchar)
```

Peristiwa yang terjadi dalam 5 menit terakhir

```
> cast(date_format(current_timestamp - INTERVAL '5' minute, '%Y%m%d%H')
as varchar)
```

Peristiwa yang terjadi antara 7-14 hari yang lalu

```
BETWEEN cast(date_format(current_timestamp - INTERVAL '14' day, '%Y%m%d
%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '7'
day, '%Y%m%d%H') as varchar)
```

Peristiwa yang terjadi pada atau setelah tanggal tertentu

```
>= '20230301'
```

Contoh: Daftar semua CloudTrail aktivitas dari IP sumber **192.0.2.1** pada atau setelah 1 Maret 2023 dalam tabel **cloud_trail_mgmt_1_0**

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay >= '20230301'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

Contoh: Daftar semua CloudTrail aktivitas dari sumber IP **192.0.2.1** dalam 30 hari terakhir dalam tabel **cloud_trail_mgmt_1_0**

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay > cast(date_format(current_timestamp - INTERVAL '30' day, '%Y%m%d
%H') as varchar)
```

```
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

Contoh kueri Security Lake untuk data CloudTrail

AWS CloudTrail melacak aktivitas dan API penggunaan pengguna di Layanan AWS. Pelanggan dapat meminta CloudTrail data untuk mempelajari jenis informasi berikut:

Berikut adalah beberapa contoh kueri CloudTrail data untuk AWS sumber versi 1:

Upaya yang tidak sah terhadap Layanan AWS dalam 7 hari terakhir

```
SELECT
      time,
      api.service.name,
      api.operation,
      api.response.error,
      api.response.message,
      unmapped['responseElements'],
      cloud.region,
      actor.user.uuid,
      src_endpoint.ip,
      http_request.user_agent
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND api.response.error in (
        'Client.UnauthorizedOperation',
        'Client.InvalidPermission.NotFound',
        'Client.OperationNotPermitted',
        'AccessDenied')
    ORDER BY time desc
    LIMIT 25
```

Daftar semua CloudTrail aktivitas dari sumber IP **`192.0.2.1`** dalam 7 hari terakhir

```
SELECT
      api.request.uid,
```

```
      time,
      api.service.name,
      api.operation,
      cloud.region,
      actor.user.uuid,
      src_endpoint.ip,
      http_request.user_agent
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    AND src_endpoint.ip = '127.0.0.1.'
    ORDER BY time desc
    LIMIT 25
```

Daftar semua IAM aktivitas dalam 7 hari terakhir

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND api.service.name = 'iam.amazonaws.com'
    ORDER BY time desc
    LIMIT 25
```

Contoh di mana **`AIDACKCEVSQ6C2EXAMPLE`** kredensi digunakan dalam 7 hari terakhir

```
SELECT
      actor.user.uid,
      actor.user.uuid,
      actor.user.account_uid,
      cloud.region
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND actor.user.credential_uid = 'AIDACKCEVSQ6C2EXAMPLE'
      LIMIT 25
```

Daftar CloudTrail catatan gagal dalam 7 hari terakhir

```
SELECT
      actor.user.uid,
      actor.user.uuid,
      actor.user.account_uid,
      cloud.region
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE status='failed' and eventDay BETWEEN cast(date_format(current_timestamp -
 INTERVAL '7' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp -
 INTERVAL '0' day, '%Y%m%d%H') as varchar)
    ORDER BY time DESC
    LIMIT 25
```

Contoh kueri Security Lake untuk log kueri resolver Route 53

Log kueri penyelesai Amazon Route 53 melacak DNS kueri yang dibuat oleh sumber daya di Amazon Anda. VPC Pelanggan dapat menanyakan log kueri resolver Route 53 untuk mempelajari jenis informasi berikut:

Berikut adalah beberapa contoh kueri log kueri resolver Route 53 untuk AWS sumber versi 1:

Daftar DNS pertanyaan dari CloudTrail dalam 7 hari terakhir

```
SELECT
      time,
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    ORDER BY time DESC
    LIMIT 25
```

Daftar DNS kueri yang cocok **`s3.amazonaws.com`** dalam 7 hari terakhir

```
SELECT
      time,
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode,
      answers
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    WHERE query.hostname LIKE 's3.amazonaws.com.' and eventDay BETWEEN
 cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
 cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
    ORDER BY time DESC
    LIMIT 25
```

Daftar DNS kueri yang tidak terselesaikan dalam 7 hari terakhir

```
SELECT
      time,
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode,
      answers
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    WHERE cardinality(answers) = 0 and eventDay BETWEEN
 cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
 cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
    LIMIT 25
```

Daftar DNS pertanyaan yang diselesaikan **`192.0.2.1`** dalam 7 hari terakhir

```
SELECT
      time,
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode,
```

```
      answer.rdata
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    CROSS JOIN UNNEST(answers) as st(answer)
    WHERE answer.rdata='192.0.2.1' and eventDay BETWEEN
 cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
 cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
    LIMIT 25
```

Contoh kueri Security Lake untuk temuan Security Hub

Security Hub memberi Anda pandangan komprehensif tentang status keamanan Anda AWS dan membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub menghasilkan temuan untuk pemeriksaan keamanan dan menerima temuan dari layanan pihak ketiga.

Berikut adalah beberapa contoh kueri temuan Security Hub:

Temuan baru dengan tingkat keparahan lebih besar dari atau sama dengan **`MEDIUM`** dalam 7 hari terakhir

```
SELECT
      time,
      finding,
      severity
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0_fi
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND severity_id >= 3
      AND state_id = 1
    ORDER BY time DESC
    LIMIT 25
```

Temuan duplikat dalam 7 hari terakhir

```
SELECT
    finding.uid,
    MAX(time) AS time,
    ARBITRARY(region) AS region,
```

```
    ARBITRARY(accountid) AS accountid,
    ARBITRARY(finding) AS finding,
    ARBITRARY(vulnerabilities) AS vulnerabilities
FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d
%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H')
 as varchar)
GROUP BY finding.uid
LIMIT 25
```

Semua temuan non-informasional dalam 7 hari terakhir

```
SELECT
      time,
      finding.title,
      finding,
      severity
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
    WHERE severity != 'Informational' and eventDay BETWEEN
 cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
 cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
    LIMIT 25
```

Temuan di mana sumber dayanya adalah ember Amazon S3 (tidak ada batasan waktu)

```
SELECT *
   FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
   WHERE any_match(resources, element -> element.type = 'amzn-s3-demo-bucket')
   LIMIT 25
```

Temuan dengan Common Vulnerability Scoring System (CVSS) skor lebih besar dari **1** (tidak ada batasan waktu)

```
SELECT *
   FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
   WHERE any_match(vulnerabilities, element -> element.cve.cvss.base_score > 1.0)
   LIMIT 25
```

Temuan yang cocok dengan Kerentanan Umum dan Eksposur (CVE) **CVE-0000-0000** (tidak ada batasan waktu)

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
    WHERE any_match(vulnerabilities, element -> element.cve.uid = 'CVE-0000-0000')
    LIMIT 25
```

Jumlah produk yang mengirimkan temuan dari Security Hub dalam 7 hari terakhir

```
SELECT
      metadata.product.feature.name,
      count(*)
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    GROUP BY metadata.product.feature.name
    ORDER BY metadata.product.feature.name DESC
    LIMIT 25
```

Hitungan jenis sumber daya dalam temuan dalam 7 hari terakhir

```
SELECT
      count(*),
      resource.type
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
        CROSS JOIN UNNEST(resources) as st(resource)
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    GROUP BY resource.type
    LIMIT 25
```

Paket rentan dari temuan dalam 7 hari terakhir

```
SELECT
      vulnerability
```

```
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0,
    UNNEST(vulnerabilities) as t(vulnerability)
    WHERE vulnerabilities is not null
    LIMIT 25
```

Temuan yang telah berubah dalam 7 hari terakhir

```
SELECT
    finding.uid,
    finding.created_time,
    finding.first_seen_time,
    finding.last_seen_time,
    finding.modified_time,
    finding.title,
    state
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    LIMIT 25
```

Contoh kueri Security Lake untuk Amazon VPC Flow Logs

Amazon Virtual Private Cloud (AmazonVPC) memberikan rincian tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di AndaVPC.

Berikut adalah beberapa contoh kueri Amazon VPC Flow Logs untuk AWS sumber versi 1:

Lalu lintas spesifik Wilayah AWS dalam 7 hari terakhir

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND region in ('us-east-1','us-east-2','us-west-2')
    LIMIT 25
```

Daftar aktivitas dari sumber IP **`192.0.2.1`** dan port sumber **`22`** dalam 7 hari terakhir

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND src_endpoint.ip = '192.0.2.1'
      AND src_endpoint.port = 22
    LIMIT 25
```

Hitungan alamat IP tujuan yang berbeda dalam 7 hari terakhir

```
SELECT
    COUNT(DISTINCT dst_endpoint.ip)
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    LIMIT 25
```

Lalu lintas berasal dari 198.51.100.0/24 dalam 7 hari terakhir

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    AND split_part(src_endpoint.ip,'.', 1)='198'AND split_part(src_endpoint.ip,'.',
 2)='51'
    LIMIT 25
```

Semua HTTPS lalu lintas dalam 7 hari terakhir

```
SELECT
      dst_endpoint.ip as dst,
      src_endpoint.ip as src,
      traffic.packets
```

```
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND dst_endpoint.port = 443
    GROUP BY
      dst_endpoint.ip,
      traffic.packets,
      src_endpoint.ip
    ORDER BY traffic.packets DESC
    LIMIT 25
```

Pesan berdasarkan jumlah paket untuk koneksi yang ditujukan ke port **443** dalam 7 hari terakhir

```
SELECT
      traffic.packets,
      dst_endpoint.ip
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND dst_endpoint.port = 443
    GROUP BY
      traffic.packets,
      dst_endpoint.ip
    ORDER BY traffic.packets DESC
    LIMIT 25
```

Semua lalu lintas antara IP **192.0.2.1** dan **192.0.2.2** dalam 7 hari terakhir

```
SELECT
      start_time,
      end_time,
      src_endpoint.interface_uid,
      connection_info.direction,
      src_endpoint.ip,
      dst_endpoint.ip,
      src_endpoint.port,
      dst_endpoint.port,
      traffic.packets,
      traffic.bytes
```

```
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND(
        src_endpoint.ip = '192.0.2.1'
        AND dst_endpoint.ip = '192.0.2.2')
      OR (
        src_endpoint.ip = '192.0.2.2'
        AND dst_endpoint.ip = '192.0.2.1')
    ORDER BY start_time ASC
    LIMIT 25
```

Semua lalu lintas masuk dalam 7 hari terakhir

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND connection_info.direction = 'ingress'
    LIMIT 25
```

Semua lalu lintas keluar dalam 7 hari terakhir

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND connection_info.direction = 'egress'
    LIMIT 25
```

Semua lalu lintas ditolak dalam 7 hari terakhir

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
```

```
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND type_uid = 400105
    LIMIT 25
```

Kueri Security Lake untuk versi AWS sumber 2 (OCSF1.1.0)

Bagian berikut memberikan panduan tentang kueri data dari Security Lake dan menyertakan beberapa contoh kueri untuk sumber yang didukung secara asli untuk versi AWS sumber 2. AWS Kueri ini dirancang untuk mengambil data secara spesifik. Wilayah AWS Contoh-contoh ini menggunakan us-east-1 (US East (Virginia N.)). Selain itu, contoh query menggunakan `LIMIT 25` parameter, yang mengembalikan hingga 25 record. Anda dapat menghilangkan parameter ini atau menyesuaikannya berdasarkan preferensi Anda. Untuk contoh lainnya, lihat GitHub direktori Amazon Security Lake OCSF Queries.

Anda dapat menanyakan data yang disimpan Security Lake dalam AWS Lake Formation database dan tabel. Anda juga dapat membuat pelanggan pihak ketiga di konsol Security Lake,API, atau AWS CLI. Pelanggan pihak ketiga juga dapat menanyakan data Lake Formation dari sumber yang Anda tentukan.

Administrator danau data Lake Formation harus memberikan `SELECT` izin pada database dan tabel yang relevan ke IAM identitas yang menanyakan data. Pelanggan juga harus dibuat di Security Lake sebelum dapat meminta data. Untuk informasi selengkapnya tentang cara membuat pelanggan dengan akses kueri, lihatMengelola akses kueri untuk pelanggan Security Lake.

Tabel sumber log

Saat Anda menanyakan data Security Lake, Anda harus menyertakan nama tabel Lake Formation tempat data berada.

```
SELECT *
FROM
 "amazon_security_lake_glue_db_DB_Region"."amazon_security_lake_table_DB_Region_SECURITY_LAKE_T
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Nilai umum untuk tabel sumber log meliputi yang berikut:

- `cloud_trail_mgmt_2_0`— acara AWS CloudTrail manajemen
- `lambda_execution_2_0`— peristiwa CloudTrail data untuk Lambda
- `s3_data_2_0`— peristiwa CloudTrail data untuk S3
- `route53_2_0`- Log kueri penyelesai Amazon Route 53
- `sh_findings_2_0`— AWS Security Hub temuan
- `vpc_flow_2_0`— Log Aliran Amazon Virtual Private Cloud (AmazonVPC)
- `eks_audit_2_0`— Log Audit Amazon Elastic Kubernetes Service (Amazon) EKS
- `waf_2_0`— Log AWS WAF v2

Contoh: Semua temuan Security Hub dalam tabel **`sh_findings_2_0`** dari Wilayah us-east-1

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
    WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Database Wilayah

Saat Anda menanyakan data Security Lake, Anda harus menyertakan nama Wilayah database tempat Anda menanyakan data. Untuk daftar lengkap Wilayah basis data tempat Danau Keamanan saat ini tersedia, lihat titik akhir Amazon Security Lake.

Contoh: Daftar aktivitas Amazon Virtual Private Cloud dari sumber IP

Contoh berikut mencantumkan semua VPC aktivitas Amazon dari IP sumber *`192.0.2.1`* yang direkam setelah *`20230301`* (01 Maret 2023), dalam tabel *`vpc_flow_2_0`* dari *`us-west-2`* `DB_Region`.

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
    WHERE time_dt > TIMESTAMP '2023-03-01'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time_dt desc
LIMIT 25
```

Tanggal partisi

Dengan mempartisi data Anda, Anda dapat membatasi jumlah data yang dipindai oleh setiap kueri, sehingga meningkatkan kinerja dan mengurangi biaya. Partisi bekerja sedikit berbeda di Security Lake 2.0 dibandingkan dengan Security Lake 1.0. Security Lake sekarang menerapkan partisi melaluitime_dt,, region dan. accountid Padahal, Security Lake 1.0 menerapkan partisi melaluieventDay,region, dan accountid parameter.

Kueri time_dt akan secara otomatis menghasilkan partisi tanggal dari S3, dan dapat ditanyakan seperti bidang berbasis waktu di Athena.

Ini adalah contoh kueri menggunakan time_dt partisi untuk menanyakan log setelah waktu 01 Maret 2023:

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt > TIMESTAMP '2023-03-01'
AND src_endpoint.ip = '192.0.2.1'
ORDER BY time desc
LIMIT 25
```

Nilai umum untuk time_dt meliputi yang berikut:

Peristiwa yang terjadi dalam 1 tahun terakhir

```
  WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '1' YEAR
```

Peristiwa yang terjadi dalam 1 bulan terakhir

```
  WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '1' MONTH
```

Peristiwa yang terjadi dalam 30 hari terakhir

```
  WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '30' DAY
```

Peristiwa yang terjadi dalam 12 jam terakhir

```
  WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '12' HOUR
```

Peristiwa yang terjadi dalam 5 menit terakhir

```
  WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '5' MINUTE
```

Peristiwa yang terjadi antara 7-14 hari yang lalu

```
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '14' DAY AND
CURRENT_TIMESTAMP - INTERVAL '7' DAY
```

Peristiwa yang terjadi pada atau setelah tanggal tertentu

```
WHERE time_dt >= TIMESTAMP '2023-03-01'
```

Contoh: Daftar semua CloudTrail aktivitas dari IP sumber **192.0.2.1** pada atau setelah 1 Maret 2023 dalam tabel **cloud_trail_mgmt_1_0**

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay >= '20230301'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

Contoh: Daftar semua CloudTrail aktivitas dari sumber IP **192.0.2.1** dalam 30 hari terakhir dalam tabel **cloud_trail_mgmt_1_0**

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay > cast(date_format(current_timestamp - INTERVAL '30' day, '%Y%m%d
%H') as varchar)
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

Meminta Keamanan Danau yang dapat diamati

Observables adalah fitur baru yang sekarang tersedia di Security Lake 2.0. Objek yang dapat diamati adalah elemen pivot yang berisi informasi terkait yang ditemukan di banyak tempat dalam acara tersebut. Kueri yang dapat diamati memungkinkan pengguna memperoleh wawasan keamanan tingkat tinggi dari seluruh kumpulan data mereka.

Dengan menanyakan elemen tertentu dalam observable, Anda dapat membatasi kumpulan data untuk hal-hal seperti nama Pengguna tertentu, Sumber Daya, UIDsIPs, Hash dan informasi jenis lainnya IOC

Ini adalah contoh kueri menggunakan array yang dapat diamati untuk menanyakan log di seluruh tabel VPC Flow dan Route53 yang berisi nilai IP '172.01.02.03'

```
WITH a AS
    (SELECT
    time_dt,
    observable.name,
    observable.value
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0",
    UNNEST(observables) AS t(observable)
    WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
    AND observable.value='172.01.02.03'
    AND observable.name='src_endpoint.ip'),
b as
    (SELECT
    time_dt,
    observable.name,
    observable.value
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0",
    UNNEST(observables) AS t(observable)
    WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
    AND observable.value='172.01.02.03'
    AND observable.name='src_endpoint.ip')
SELECT * FROM a
LEFT JOIN b ON a.value=b.value and a.name=b.name
LIMIT 25
```

Contoh kueri Security Lake untuk data CloudTrail

AWS CloudTrail melacak aktivitas dan API penggunaan pengguna di Layanan AWS. Pelanggan dapat meminta CloudTrail data untuk mempelajari jenis informasi berikut:

Berikut adalah beberapa contoh kueri untuk CloudTrail data untuk AWS sumber versi 2:

Upaya yang tidak sah terhadap Layanan AWS dalam 7 hari terakhir

```
SELECT
```

```
    time_dt,
    api.service.name,
    api.operation,
    api.response.error,
    api.response.message,
    api.response.data,
    cloud.region,
    actor.user.uid,
    src_endpoint.ip,
    http_request.user_agent
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND api.response.error in (
    'Client.UnauthorizedOperation',
    'Client.InvalidPermission.NotFound',
    'Client.OperationNotPermitted',
    'AccessDenied')
ORDER BY time desc
LIMIT 25
```

Daftar semua CloudTrail aktivitas dari sumber IP **`192.0.2.1`** dalam 7 hari terakhir

```
SELECT
    api.request.uid,
    time_dt,
    api.service.name,
    api.operation,
    cloud.region,
    actor.user.uid,
    src_endpoint.ip,
    http_request.user_agent
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '192.0.2.1.'
ORDER BY time desc
LIMIT 25
```

Daftar semua IAM aktivitas dalam 7 hari terakhir

```
SELECT *
```

```
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND api.service.name = 'iam.amazonaws.com'
ORDER BY time desc
LIMIT 25
```

Contoh di mana **AIDACKCEVSQ6C2EXAMPLE** kredensi digunakan dalam 7 hari terakhir

```
SELECT
      actor.user.uid,
      actor.user.uid_alt,
      actor.user.account.uid,
      cloud.region
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND actor.user.credential_uid = 'AIDACKCEVSQ6C2EXAMPLE'
LIMIT 25
```

Daftar CloudTrail catatan gagal dalam 7 hari terakhir

```
SELECT
      actor.user.uid,
      actor.user.uid_alt,
      actor.user.account.uid,
      cloud.region
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE status='failed' and time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND
 CURRENT_TIMESTAMP
ORDER BY time DESC
LIMIT 25
```

Contoh kueri untuk log kueri resolver Route 53

Log kueri penyelesai Amazon Route 53 melacak DNS kueri yang dibuat oleh sumber daya di Amazon Anda. VPC Pelanggan dapat menanyakan log kueri resolver Route 53 untuk mempelajari jenis informasi berikut:

Berikut adalah beberapa contoh kueri untuk log kueri reesolver Route 53 untuk AWS versi sumber 2:

Daftar DNS pertanyaan dari CloudTrail dalam 7 hari terakhir

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
ORDER BY time DESC
LIMIT 25
```

Daftar DNS kueri yang cocok **`s3.amazonaws.com`** dalam 7 hari terakhir

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
    answers
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0"
WHERE query.hostname LIKE 's3.amazonaws.com.' and time_dt BETWEEN CURRENT_TIMESTAMP -
 INTERVAL '7' DAY AND CURRENT_TIMESTAMP
ORDER BY time DESC
LIMIT 25
```

Daftar DNS kueri yang tidak diselesaikan dalam 7 hari terakhir

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
    answers
```

```
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0"
WHERE cardinality(answers) = 0 and time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY
 AND CURRENT_TIMESTAMP
LIMIT 25
```

Daftar DNS pertanyaan yang diselesaikan **192.0.2.1** dalam 7 hari terakhir

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
    answer.rdata
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0",
UNNEST(answers) as st(answer)
WHERE answer.rdata='192.0.2.1'
AND time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Contoh kueri Security Lake untuk temuan Security Hub

Security Hub memberi Anda pandangan komprehensif tentang status keamanan Anda AWS dan membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub menghasilkan temuan untuk pemeriksaan keamanan dan menerima temuan dari layanan pihak ketiga.

Berikut adalah beberapa contoh kueri untuk temuan Security Hub untuk AWS sumber versi 2:

Temuan baru dengan tingkat keparahan lebih besar dari atau sama dengan **MEDIUM** dalam 7 hari terakhir

```
SELECT
    time_dt,
    finding_info,
    severity_id,
    status
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
```

```
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
    AND severity_id >= 3
    AND status = 'New'
ORDER BY time DESC
LIMIT 25
```

Temuan duplikat dalam 7 hari terakhir

```
SELECT
    finding_info.uid,
    MAX(time_dt) AS time,
    ARBITRARY(region) AS region,
    ARBITRARY(accountid) AS accountid,
    ARBITRARY(finding_info) AS finding,
    ARBITRARY(vulnerabilities) AS vulnerabilities
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
GROUP BY finding_info.uid
LIMIT 25
```

Semua temuan non-informasi dalam 7 hari terakhir

```
SELECT
    time_dt,
    finding_info.title,
    finding_info,
    severity
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE severity != 'Informational' and time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7'
 DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Temuan di mana sumber dayanya adalah ember Amazon S3 (tanpa batasan waktu)

```
SELECT *
   FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE any_match(resources, element -> element.type = 'amzn-s3-demo-bucket')
LIMIT 25
```

Temuan dengan Common Vulnerability Scoring System (CVSS) skor lebih besar dari **1** (tidak ada batasan waktu)

```
SELECT
    DISTINCT finding_info.uid
    time_dt,
    metadata,
    finding_info,
    vulnerabilities,
    resource
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
UNNEST(vulnerabilities) AS t(vulnerability),
UNNEST(vulnerability.cve.cvss) AS t(cvs)
WHERE cvs.base_score > 1.0
AND vulnerabilities is NOT NULL
LIMIT 25
```

Temuan yang cocok dengan Kerentanan Umum dan Eksposur (CVE) **CVE-0000-0000** (tidak ada batasan waktu)

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE any_match(vulnerabilities, element -> element.cve.uid = 'CVE-0000-0000')
LIMIT 25
```

Jumlah produk yang mengirimkan temuan dari Security Hub dalam 7 hari terakhir

```
SELECT
    metadata.product.name,
    count(*)
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
GROUP BY metadata.product.name
ORDER BY metadata.product.name DESC
LIMIT 25
```

Hitungan jenis sumber daya dalam temuan dalam 7 hari terakhir

```
SELECT
```

```
    count(*) AS "Total",
    resource.type
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
GROUP BY resource.type
ORDER BY count(*) DESC
LIMIT 25
```

Paket rentan dari temuan dalam 7 hari terakhir

```
SELECT
    vulnerabilities
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND vulnerabilities is NOT NULL
LIMIT 25
```

Temuan yang telah berubah dalam 7 hari terakhir

```
SELECT
    status,
    finding_info.title,
    finding_info.created_time_dt,
    finding_info,
    finding_info.uid,
    finding_info.first_seen_time_dt,
    finding_info.last_seen_time_dt,
    finding_info.modified_time_dt
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Contoh kueri Security Lake untuk Amazon VPC Flow Logs

Amazon Virtual Private Cloud (AmazonVPC) memberikan rincian tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di AndaVPC.

Berikut adalah beberapa contoh kueri untuk Amazon VPC Flow Logs untuk AWS sumber versi 2:

Lalu lintas spesifik Wilayah AWS dalam 7 hari terakhir

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND region in ('us-east-1','us-east-2','us-west-2')
LIMIT 25
```

Daftar aktivitas dari sumber IP **192.0.2.1** dan port sumber **22** dalam 7 hari terakhir

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '192.0.2.1'
AND src_endpoint.port = 22
LIMIT 25
```

Hitungan alamat IP tujuan yang berbeda dalam 7 hari terakhir

```
SELECT
    COUNT(DISTINCT dst_endpoint.ip) AS "Total"
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Lalu lintas berasal dari 198.51.100.0/24 dalam 7 hari terakhir

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND split_part(src_endpoint.ip,'.', 1)='198'AND split_part(src_endpoint.ip,'.', 2)='51'
LIMIT 25
```

Semua HTTPS lalu lintas dalam 7 hari terakhir

```
SELECT
    dst_endpoint.ip as dst,
```

```
    src_endpoint.ip as src,
    traffic.packets
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND dst_endpoint.port = 443
GROUP BY
    dst_endpoint.ip,
    traffic.packets,
    src_endpoint.ip
ORDER BY traffic.packets DESC
LIMIT 25
```

Pesan berdasarkan jumlah paket untuk koneksi yang ditujukan ke port **443** dalam 7 hari terakhir

```
SELECT
    traffic.packets,
    dst_endpoint.ip
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND dst_endpoint.port = 443
GROUP BY
    traffic.packets,
    dst_endpoint.ip
ORDER BY traffic.packets DESC
LIMIT 25
```

Semua lalu lintas antara IP **192.0.2.1** dan **192.0.2.2** dalam 7 hari terakhir

```
SELECT
    start_time_dt,
    end_time_dt,
    src_endpoint.interface_uid,
    connection_info.direction,
    src_endpoint.ip,
    dst_endpoint.ip,
    src_endpoint.port,
    dst_endpoint.port,
    traffic.packets,
    traffic.bytes
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
```

```
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND(
    src_endpoint.ip = '192.0.2.1'
AND dst_endpoint.ip = '192.0.2.2')
OR (
    src_endpoint.ip = '192.0.2.2'
AND dst_endpoint.ip = '192.0.2.1')
ORDER BY start_time_dt ASC
LIMIT 25
```

Semua lalu lintas masuk dalam 7 hari terakhir

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND connection_info.direction = 'Inbound'
LIMIT 25
```

Semua lalu lintas keluar dalam 7 hari terakhir

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND connection_info.direction = 'Outbound'
LIMIT 25
```

Semua lalu lintas ditolak dalam 7 hari terakhir

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND action = 'Denied'
LIMIT 25
```

Contoh kueri Security Lake untuk log EKS audit Amazon

Aktivitas bidang kontrol trek EKS log Amazon menyediakan log audit dan diagnostik langsung dari bidang EKS kontrol Amazon ke CloudWatch Log di akun Anda. Log ini memudahkan Anda untuk

mengamankan dan menjalankan klaster Anda. Pelanggan dapat meminta EKS log untuk mempelajari jenis informasi berikut.

Berikut adalah beberapa contoh kueri untuk log EKS audit Amazon untuk versi AWS sumber 2:

Permintaan ke spesifik URL dalam 7 hari terakhir

```
SELECT
    time_dt,
    actor.user.name,
    http_request.url.path,
    activity_name
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_eks_audit_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND activity_name = 'get'
and http_request.url.path = '/apis/coordination.k8s.io/v1/'
LIMIT 25
```

Perbarui permintaan dari '10.0.97.167' selama 7 hari terakhir

```
SELECT
    activity_name,
    time_dt,
    api.request,
    http_request.url.path,
    src_endpoint.ip,
    resources
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_eks_audit_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '10.0.97.167'
AND activity_name = 'Update'
LIMIT 25
```

Permintaan dan Tanggapan terkait dengan sumber daya kube-controller-manager " selama 7 hari terakhir

```
SELECT
    activity_name,
    time_dt,
    api.request,
```

```
    api.response,
    resource.name
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_eks_audit_2_0",
UNNEST(resources) AS t(resource)
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND resource.name = 'kube-controller-manager'
LIMIT 25
```

Contoh kueri Security Lake untuk log AWS WAF v2

AWS WAF adalah firewall aplikasi web yang dapat Anda gunakan untuk memantau permintaan web yang dikirim pengguna akhir Anda ke aplikasi Anda dan untuk mengontrol akses ke konten Anda.

Berikut adalah beberapa contoh kueri untuk log AWS WAF v2 untuk versi AWS sumber 2:

Memposting permintaan dari IP sumber tertentu selama 7 hari terakhir

```
SELECT
    time_dt,
    activity_name,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method,
    http_request.http_headers
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '100.123.123.123'
AND activity_name = 'Post'
LIMIT 25
```

Permintaan yang cocok dengan jenis firewall MANAGED _ RULE _ GROUP selama 7 hari terakhir

```
SELECT
    time_dt,
    activity_name,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method,
```

```
    firewall_rule.uid,
    firewall_rule.type,
    firewall_rule.condition,
    firewall_rule.match_location,
    firewall_rule.match_details,
    firewall_rule.rate_limit
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND firewall_rule.type = 'MANAGED_RULE_GROUP'
LIMIT 25
```

Permintaan yang cocok REGEX dengan aturan firewall selama 7 hari terakhir

```
SELECT
    time_dt,
    activity_name,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method,
    firewall_rule.uid,
    firewall_rule.type,
    firewall_rule.condition,
    firewall_rule.match_location,
    firewall_rule.match_details,
    firewall_rule.rate_limit
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND firewall_rule.condition = 'REGEX'
LIMIT 25
```

Ditolak mendapatkan permintaan untuk AWS kredensional yang memicu AWS WAF aturan selama 7 hari terakhir

```
SELECT
    time_dt,
    activity_name,
    action,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
```

```
    http_request.http_method,
    firewall_rule.uid,
    firewall_rule.type
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND http_request.url.path = '/.aws/credentials'
AND action = 'Denied'
LIMIT 25
```

Dapatkan permintaan untuk AWS Kredensial, dikelompokkan berdasarkan negara selama 7 hari terakhir

```
SELECT count(*) as Total,
    src_endpoint.location.country AS Country,
    activity_name,
    action,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY
    AND CURRENT_TIMESTAMP
    AND activity_name = 'Get'
    AND http_request.url.path = '/.aws/credentials'
GROUP BY src_endpoint.location.country,
    activity_name,
    action,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method
```

Manajemen siklus hidup di Security Lake

Anda dapat menyesuaikan Security Lake untuk menyimpan data yang Anda inginkan Wilayah AWS sesuai dengan jumlah waktu yang Anda inginkan. Manajemen siklus hidup dapat membantu Anda mematuhi persyaratan kepatuhan yang berbeda.

Manajemen retensi

Untuk mengelola data Anda sehingga disimpan secara efektif, Anda dapat mengonfigurasi pengaturan retensi untuk data. Karena Security Lake menyimpan data Anda sebagai objek di bucket Amazon Simple Storage Service (Amazon S3), pengaturan retensi sesuai dengan konfigurasi Siklus Hidup Amazon S3. Dengan mengonfigurasi pengaturan ini, Anda dapat menentukan kelas penyimpanan Amazon S3 pilihan Anda dan periode waktu objek S3 untuk tetap berada di kelas penyimpanan tersebut sebelum beralih ke kelas penyimpanan yang berbeda atau kedaluwarsa. Untuk informasi selengkapnya tentang konfigurasi Siklus Hidup Amazon S3, lihat Mengelola siklus hidup penyimpanan Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Di Security Lake, Anda menentukan pengaturan retensi di tingkat Wilayah. Misalnya, Anda dapat memilih untuk mentransisikan semua objek S3 secara spesifik Wilayah AWS ke kelas penyimpanan IA Standar S3 30 hari setelah ditulis ke data lake. Kelas penyimpanan Amazon S3 default adalah Standar S3.

> **Important**
>
> Security Lake tidak mendukung Amazon S3 Object Lock. Saat bucket data lake dibuat, S3 Object Lock dinonaktifkan secara default. Mengaktifkan Kunci Objek S3 dengan mode retensi default mengganggu pengiriman data log yang dinormalisasi ke data lake.

Mengkonfigurasi pengaturan retensi saat mengaktifkan Security Lake

Ikuti petunjuk ini untuk mengonfigurasi pengaturan retensi untuk satu atau beberapa Wilayah saat Anda melakukan onboarding ke Security Lake. Jika Anda tidak mengonfigurasi pengaturan retensi, Security Lake menggunakan setelan default untuk konfigurasi Siklus Hidup Amazon S3—menyimpan data tanpa batas menggunakan kelas penyimpanan Standar S3.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Saat Anda mencapai Langkah 2: Tentukan tujuan target alur kerja orientasi, pilih Tambahkan transisi di bawah Pilih kelas penyimpanan. Kemudian pilih kelas penyimpanan Amazon S3 yang ingin Anda alihkan objek S3. (Kelas penyimpanan default yang tidak terdaftar adalah Standar S3.) Juga tentukan periode retensi (dalam beberapa hari) untuk kelas penyimpanan itu. Untuk mentransisikan objek ke kelas penyimpanan lain setelah waktu itu, pilih Tambahkan transisi dan masukkan pengaturan untuk kelas penyimpanan dan periode retensi berikutnya.
3. Untuk menentukan kapan Anda ingin objek S3 kedaluwarsa, pilih Tambahkan transisi. Kemudian, untuk kelas penyimpanan, pilih Kedaluwarsa. Untuk periode retensi, masukkan jumlah hari yang ingin Anda simpan objek di Amazon S3, menggunakan kelas penyimpanan apa pun, setelah objek dibuat. Ketika periode waktu ini berakhir, objek kedaluwarsa dan Amazon S3 menghapusnya.
4. Setelah selesai, pilih Selanjutnya.

Perubahan Anda akan berlaku untuk semua Wilayah tempat Anda mengaktifkan Security Lake selama langkah orientasi sebelumnya.

API

Untuk mengonfigurasi pengaturan retensi secara terprogram saat Anda melakukan onboarding ke Security Lake, gunakan CreateDataLakeOperasi Danau KeamananAPI. Jika Anda menggunakan AWS CLI, jalankan create-data-lakeperintah. Tentukan pengaturan retensi yang Anda inginkan dalam `lifecycleConfiguration` parameter sebagai berikut:

- Untuk`transitions`, tentukan jumlah total days (`days`) yang ingin Anda simpan objek S3 di kelas `storageClass` penyimpanan Amazon S3 tertentu ().
- Untuk`expiration`, tentukan jumlah hari yang ingin Anda simpan objek di Amazon S3, menggunakan kelas penyimpanan apa pun, setelah objek dibuat. Ketika periode waktu ini berakhir, objek kedaluwarsa dan Amazon S3 menghapusnya.

Security Lake menerapkan pengaturan ke Wilayah yang Anda tentukan di `region` bidang `configurations` objek.

Misalnya, perintah berikut memungkinkan Security Lake in the `us-east-1` Region. Di Wilayah ini, objek kedaluwarsa setelah 365 hari, dan objek bertransisi ke kelas penyimpanan `ONEZONE_IA` S3 setelah 60 hari. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","lifecycleConfiguration":
 {"expiration":{"days":365},"transitions":
[{"days":60,"storageClass":"ONEZONE_IA"}]}}]' \
--meta-store-manager-role-arn "arn:aws:securitylake:ap-
northeast-2:123456789012:data-lake/default"
```

Memperbarui pengaturan retensi

Ikuti petunjuk ini untuk memperbarui pengaturan retensi untuk satu atau beberapa Wilayah setelah mengaktifkan Security Lake.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Di panel navigasi, pilih Wilayah
3. Pilih Wilayah, lalu pilih Edit.
4. Di bagian Pilih kelas penyimpanan, masukkan pengaturan yang Anda inginkan. Untuk kelas penyimpanan, pilih kelas penyimpanan Amazon S3 yang ingin Anda alihkan objek S3. (Kelas penyimpanan default yang tidak terdaftar adalah Standar S3.) Untuk periode retensi, masukkan jumlah hari yang ingin Anda simpan objek di kelas penyimpanan tersebut. Anda dapat menentukan beberapa transisi.

   Untuk juga menentukan kapan Anda ingin objek S3 kedaluwarsa, pilih Kedaluwarsa untuk kelas penyimpanan. Kemudian, untuk periode retensi, masukkan jumlah hari yang ingin Anda simpan objek di Amazon S3, menggunakan kelas penyimpanan apa pun, setelah objek dibuat. Ketika periode waktu ini berakhir, objek kedaluwarsa dan Amazon S3 menghapusnya.
5. Setelah selesai, pilih Simpan.

API

Untuk memperbarui pengaturan retensi secara terprogram, gunakan UpdateDataLakeOperasi Danau KeamananAPI. Jika Anda menggunakan AWS CLI, jalankan update-data-lakeperintah. Dalam permintaan Anda, gunakan `lifecycleConfiguration` parameter untuk menentukan pengaturan baru:

- Untuk mengubah pengaturan transisi, gunakan `transitions` parameter untuk menentukan setiap periode waktu baru dalam days (`days`) yang ingin Anda simpan objek S3 di kelas `storageClass` penyimpanan Amazon S3 tertentu ().
- Untuk mengubah periode retensi keseluruhan, gunakan `expiration` parameter untuk menentukan jumlah hari yang ingin Anda simpan objek S3, menggunakan kelas penyimpanan apa pun, setelah objek dibuat. Ketika periode retensi ini berakhir, objek kedaluwarsa dan Amazon S3 menghapusnya.

Security Lake menerapkan pengaturan ke Wilayah yang Anda tentukan di `region` bidang `configurations` objek.

`UpdateDataLake`Pengoperasian Danau Keamanan API berfungsi sebagai operasi “upsert” yang melakukan penyisipan jika item atau catatan yang ditentukan tidak ada, atau pembaruan jika sudah ada. Security Lake menyimpan data Anda dengan aman menggunakan solusi AWS enkripsi.

Menghilangkan kunci `encryptionConfiguration` dari Wilayah yang disertakan dalam panggilan pembaruan yang saat ini digunakan KMS akan meninggalkan KMS kunci Wilayah itu di tempatnya, tetapi menentukan kunci akan mengatur ulang kunci di wilayah yang sama.

Misalnya, AWS CLI perintah berikut memperbarui pengaturan kedaluwarsa data dan pengaturan transisi penyimpanan untuk Wilayah. `us-east-1` Di Wilayah ini, objek kedaluwarsa setelah 500 hari, dan objek beralih ke kelas penyimpanan `ONEZONE_IA` S3 setelah 30 hari. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake update-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","lifecycleConfiguration":
 {"expiration":{"days":500},"transitions":
[{"days":30,"storageClass":"ONEZONE_IA"}]}}]' \
```

```
--meta-store-manager-role-arn "arn:aws:securitylake:ap-
northeast-2:123456789012:data-lake/default"
```

Wilayah Rollup

Wilayah rollup mengkonsolidasikan data dari satu atau lebih Wilayah yang berkontribusi. Ini dapat membantu Anda mematuhi persyaratan kepatuhan data regional.

Untuk petunjuk tentang mengonfigurasi Wilayah rollup, lihat. Mengkonfigurasi Wilayah rollup di Danau Keamanan

Buka Kerangka Skema Keamanan Siber (OCSF) di Danau Keamanan

Apa yang dimaksud dengan OCSF?

Open Cybersecurity Schema Framework (OCSF) adalah upaya kolaboratif dan open-source oleh AWS dan mitra terkemuka di industri keamanan siber. OCSFmenyediakan skema standar untuk peristiwa keamanan umum, mendefinisikan kriteria pembuatan versi untuk memfasilitasi evolusi skema, dan mencakup proses tata kelola sendiri untuk produsen log keamanan dan konsumen. Kode sumber publik untuk OCSF di-host di GitHub.

Security Lake secara otomatis mengonversi log dan peristiwa yang berasal dari yang didukung secara asli ke skema Layanan AWS . OCSF Setelah dikonversi keOCSF, Security Lake menyimpan data dalam bucket Amazon Simple Storage Service (Amazon S3) (satu bucket Wilayah AWS per ember) di bucket. Akun AWS Log dan peristiwa yang ditulis ke Security Lake dari sumber khusus harus mematuhi OCSF skema dan format Parket Apache. Pelanggan dapat memperlakukan log dan peristiwa sebagai catatan Parket generik atau menerapkan kelas acara OCSF skema untuk lebih akurat menafsirkan informasi yang terkandung dalam catatan.

OCSFkelas acara

Log dan peristiwa dari sumber Security Lake yang diberikan cocok dengan kelas peristiwa tertentu yang ditentukanOCSF. DNSAktivitas, SSH Aktivitas, dan Otentikasi adalah contoh kelas acara di OCSF. Anda dapat menentukan kelas acara mana yang cocok dengan sumber tertentu.

OCSFidentifikasi sumber

OCSFmenggunakan berbagai bidang untuk membantu Anda menentukan dari mana kumpulan log atau peristiwa tertentu berasal. Ini adalah nilai-nilai bidang yang relevan untuk Layanan AWS yang didukung secara asli sebagai sumber di Security Lake.

`The OCSF source identification for AWS log sources (Version 1) are listed in the following table.`

Sumber	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadata.version
CloudTrail Peristiwa Data Lambda	CloudTrail	AWS	Data	API Activity	1.0.0-rc.2
CloudTrail Manajemen Acara	CloudTrail	AWS	Management	API Activity,Authentication , atau Account Change	1.0.0-rc.2
CloudTrail Acara Data S3	CloudTrail	AWS	Data	API Activity	1.0.0-rc.2
Route 53	Route 53	AWS	Resolver Query Logs	DNS Activity	1.0.0-rc.2
Security Hub	Security Hub	AWS	Mencocokkan ProductName nilai Security Hub	Security Finding	1.0.0-rc.2
VPCLog Aliran	Amazon VPC	AWS	Flowlogs	Network Activity	1.0.0-rc.2

The OCSF source identification for AWS log sources (Version 2) are listed in the following table.

Sumber	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadata.version
CloudTrail Peristiwa Data Lambda	CloudTrail	AWS	Data	API Activity	1.1.0
CloudTrail Manajemen Acara	CloudTrail	AWS	Management	API Activity,Autation , atau Account Change	1.1.0
CloudTrail Acara Data S3	CloudTrail	AWS	Data	API Activity	1.1.0
Route 53	Route 53	AWS	Resolver Query Logs	DNS Activity	1.1.0
Security Hub	ProductName Nilai Cocokkan AWS Security Finding Format (ASFF)	CompanyName Nilai Cocokkan AWS Security Finding Format (ASFF)	Mencocokkan featureName nilai dari ASFF ProductFields	Vulnerability Finding, Compliance Finding, or Detection Finding	1.1.0
VPCLog Aliran	Amazon VPC	AWS	Flowlogs	Network Activity	1.1.0
EKSLog Audit	Amazon EKS	AWS	Elastic Kubernetes Service	API Activity	1.1.0

Sumber	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadata.version
AWS WAF v2 Log	`AWS WAF`	`AWS`	–	`HTTP Activity`	`1.1.0`

Integrasi dengan Security Lake

Amazon Security Lake terintegrasi dengan produk lain Layanan AWS dan pihak ketiga. Integrasi dapat mengirim data ke Security Lake sebagai sumber atau mengkonsumsi data di Security Lake sebagai pelanggan. Topik berikut menjelaskan produk mana Layanan AWS dan pihak ketiga yang terintegrasi dengan Security Lake.

Topik

Layanan AWS Integrasi dengan Security Lake

Amazon Security Lake terintegrasi dengan yang lain Layanan AWS. Layanan dapat beroperasi sebagai integrasi sumber, integrasi pelanggan, atau keduanya.

Integrasi sumber memiliki properti berikut:

- Kirim data ke Security Lake
- Data tiba dalam Buka Kerangka Skema Keamanan Siber (OCSF) di Danau Keamanan skema
- Data tiba dalam format Apache Parquet

Integrasi pelanggan memiliki properti berikut dapat membaca data sumber dari Security Lake pada titik HTTPS akhir atau antrian Amazon Simple Queue Service (AmazonSQS), atau dengan langsung menanyakan data sumber dari AWS Lake Formation

Bagian berikut menjelaskan Layanan AWS Security Lake mana yang terintegrasi dengan dan bagaimana setiap integrasi bekerja.

Integrasi dengan AWS AppFabric

Jenis integrasi: Sumber

AWS AppFabricadalah layanan tanpa kode yang menghubungkan aplikasi perangkat lunak sebagai layanan (SaaS) di seluruh organisasi Anda, sehingga tim TI dan keamanan dapat mengelola dan mengamankan aplikasi menggunakan skema standar dan repositori pusat.

Bagaimana Security Lake menerima AppFabric temuan

Anda dapat mengirim data log AppFabric audit ke Security Lake dengan memilih Amazon Kinesis Data Firehose sebagai tujuan dan mengonfigurasi Kinesis Data Firehose OCSF untuk mengirimkan data dalam skema dan format Apache Parquet ke Security Lake.

Prasyarat

Sebelum dapat mengirim log AppFabric audit ke Security Lake, Anda harus menampilkan log audit yang OCSF dinormalisasi ke aliran Kinesis Data Firehose. Anda kemudian dapat mengonfigurasi Kinesis Data Firehose untuk mengirim output ke bucket Amazon S3 Security Lake. Untuk informasi selengkapnya, lihat Memilih Amazon S3 untuk tujuan Anda di Panduan Pengembang Amazon Kinesis.

Kirim AppFabric temuan Anda ke Security Lake

Untuk mengirim log AppFabric audit ke Security Lake setelah menyelesaikan prasyarat sebelumnya, Anda harus mengaktifkan kedua layanan dan menambahkan AppFabric sebagai sumber khusus di Security Lake. Untuk petunjuk tentang menambahkan sumber kustom, lihatMengumpulkan data dari sumber khusus di Security Lake.

Berhenti menerima AppFabric log di Security Lake

Untuk berhenti menerima log AppFabric audit, Anda dapat menggunakan konsol Security Lake, Security LakeAPI, atau AWS CLI untuk menghapus AppFabric sebagai sumber kustom. Untuk petunjuk, silakan lihat Menghapus sumber kustom dari Security Lake.

Integrasi dengan Amazon Detective

Jenis integrasi: Pelanggan

Amazon Detective membantu Anda menganalisis, menyelidiki, dan mengidentifikasi akar penyebab temuan keamanan atau aktivitas mencurigakan dengan cepat. Detective secara otomatis mengumpulkan data log dari sumber daya Anda. AWS Kemudian menggunakan pembelajaran mesin, analisis statistik, dan teori grafik untuk menghasilkan visualisasi yang membantu Anda melakukan penyelidikan keamanan yang lebih cepat dan lebih efisien. Agregasi data Detective prebuilt, ringkasan, dan konteks membantu Anda menganalisis dan menentukan sifat dan tingkat kemungkinan masalah keamanan dengan cepat.

Saat Anda mengintegrasikan Security Lake dan Detective, Anda dapat menanyakan data log mentah yang disimpan oleh Security Lake dari Detective. Untuk informasi selengkapnya, lihat Integrasi dengan Amazon Security Lake.

Integrasi dengan Amazon OpenSearch Service

Jenis integrasi: Pelanggan

Amazon OpenSearch Service adalah layanan terkelola yang memudahkan penerapan, pengoperasian, dan skala kluster OpenSearch Layanan di. AWS Cloud Menggunakan OpenSearch Service Ingestion untuk menyerap data ke dalam kluster OpenSearch Layanan, Anda dapat memperoleh wawasan lebih cepat untuk penyelidikan keamanan yang sensitif terhadap waktu. Anda dapat merespons insiden keamanan dengan cepat, membantu Anda melindungi data dan sistem penting bisnis Anda.

OpenSearch Dasbor layanan

Setelah mengintegrasikan OpenSearch Layanan dengan Security Lake, Anda dapat mengonfigurasi Security Lake untuk mengirim data keamanan dari berbagai sumber ke OpenSearch Layanan melalui Serverless OpenSearch Service Ingestion. Untuk informasi selengkapnya tentang cara mengonfigurasi konsumsi OpenSearch Layanan untuk memproses data keamanan, lihat Menghasilkan wawasan keamanan dari data Amazon Security Lake menggunakan Amazon OpenSearch Service Ingestion.

Setelah OpenSearch Service Ingestion mulai menulis data Anda ke domain OpenSearch Layanan Anda. Untuk memvisualisasikan data menggunakan dasbor pra-bangun, navigasikan ke dasbor dan pilih salah satu dasbor yang diinstal.

OpenSearch Permintaan langsung layanan

Anda dapat menggunakan kueri langsung OpenSearch Layanan untuk menganalisis data di Amazon Security Lake. OpenSearch Layanan menyediakan ETL integrasi nol sebagai cara untuk secara langsung menanyakan data Anda di Security Lake menggunakan OpenSearch SQL atau OpenSearch Piped Processing Language (PPL) tanpa menimbulkan gesekan membangun saluran pipa konsumsi atau beralih di antara alat analitik. Pendekatan ini menghilangkan kebutuhan untuk pergerakan atau duplikasi data, memungkinkan Anda untuk menganalisis data Anda di mana ia berada menggunakan OpenSearch pengalaman Discover di OpenSearch Dasbor. Saat Anda ingin beralih dari kueri data saat istirahat ke pemantauan aktif dengan dasbor, Anda dapat membuat tampilan yang diindeks pada hasil kueri dan memasukkannya ke dalam indeks Layanan.

OpenSearch Untuk informasi selengkapnya tentang kueri langsung, lihat Bekerja dengan kueri langsung di Panduan Pengembang OpenSearch Layanan Amazon.

OpenSearch Layanan menggunakan koleksi OpenSearch Tanpa Server untuk secara langsung menanyakan data di Security Lake dan menyimpan tampilan terindeks Anda. Untuk melakukan ini, Anda membuat sumber data yang memungkinkan Anda menggunakan ETL kemampuan OpenSearch nol pada data Security Lake. Saat membuat sumber data, Anda dapat langsung mencari, mendapatkan wawasan, dan menganalisis data yang disimpan di Security Lake. Anda dapat mempercepat kinerja kueri dan menggunakan OpenSearch analitik lanjutan pada set data Security Lake tertentu menggunakan pengindeksan sesuai permintaan.

- Untuk detail tentang cara membuat integrasi sumber OpenSearch data, lihat Membuat integrasi sumber data Amazon Security Lake di Panduan Pengembang OpenSearch Layanan Amazon.
- Untuk detail tentang cara mengonfigurasi sumber data Security Lake OpenSearch, lihat Mengonfigurasi sumber data Security Lake di OpenSearch Dasbor di Panduan Pengembang OpenSearch Layanan Amazon.

Integrasi dengan Amazon QuickSight

Jenis integrasi: Pelanggan

Amazon QuickSight adalah layanan intelijen bisnis skala cloud (BI) yang dapat Anda gunakan untuk memberikan easy-to-understand wawasan kepada orang-orang yang bekerja dengan Anda, di mana pun mereka berada. Amazon QuickSight terhubung ke data Anda di cloud dan menggabungkan data dari berbagai sumber. Amazon QuickSight memberi para pengambil keputusan kesempatan untuk mengeksplorasi dan menafsirkan informasi dalam lingkungan visual yang interaktif. Mereka memiliki akses aman ke dasbor dari perangkat apa pun di jaringan Anda dan dari perangkat seluler.

QuickSight Dasbor Amazon

Untuk memvisualisasikan data Amazon Security Lake Anda di Amazon QuickSight, untuk membuat AWS objek yang diperlukan dan menyebarkan sumber data dasar, kumpulan data, analisis, dasbor, dan grup pengguna ke Amazon sehubungan QuickSight dengan Security Lake. Untuk petunjuk selengkapnya, lihat Integrasi dengan Amazon QuickSight.

Integrasi dengan Amazon SageMaker AI

Jenis integrasi: Pelanggan

Amazon SageMaker AI adalah layanan pembelajaran mesin (ML) yang dikelola sepenuhnya. Dengan Security Lake, ilmuwan dan pengembang data dapat dengan cepat dan percaya diri membangun, melatih, dan menerapkan model ML ke dalam lingkungan host yang siap produksi. Ini memberikan pengalaman UI untuk menjalankan alur kerja ML yang membuat alat SageMaker AI ML tersedia di beberapa lingkungan pengembangan terintegrasi (IDEs).

SageMaker Wawasan AI

Anda dapat menghasilkan wawasan pembelajaran mesin untuk Security Lake menggunakan SageMaker AI Studio. SageMaker AI Studio adalah lingkungan pengembangan terintegrasi web (IDE) untuk pembelajaran mesin yang menyediakan alat bagi ilmuwan data untuk mempersiapkan, membangun, melatih, dan menerapkan model pembelajaran mesin. Dengan solusi ini, Anda dapat dengan cepat menyebarkan satu set dasar notebook Python yang berfokus AWS Security Hub pada temuan di Security Lake, yang juga dapat diperluas untuk menggabungkan sumber AWS lain atau sumber data khusus di Security Lake. Untuk detail selengkapnya, lihat Menghasilkan wawasan pembelajaran mesin untuk data Amazon Security Lake menggunakan Amazon SageMaker AI.

Integrasi dengan Amazon Bedrock

Amazon Bedrock adalah layanan yang dikelola sepenuhnya yang membuat model foundation berkinerja tinggi (FMs) dari startup AI terkemuka dan Amazon tersedia untuk Anda gunakan melalui terpadu. API Dengan pengalaman tanpa server Amazon Bedrock, Anda dapat memulai dengan cepat, menyesuaikan model fondasi secara pribadi dengan data Anda sendiri, dan mengintegrasikan serta menerapkannya dengan mudah dan aman ke dalam aplikasi Anda menggunakan AWS alat tanpa harus mengelola infrastruktur apa pun.

AI generatif

Anda dapat menggunakan kemampuan AI generatif Amazon Bedrock dan input bahasa alami di SageMaker AI Studio untuk menganalisis data di Security Lake dan bekerja untuk mengurangi risiko organisasi Anda dan meningkatkan postur keamanan Anda. Anda dapat mengurangi jumlah waktu yang diperlukan untuk melakukan penyelidikan dengan secara otomatis mengidentifikasi sumber data yang sesuai, membuat dan memanggil SQL kueri, dan memvisualisasikan data dari penyelidikan Anda. Untuk detail selengkapnya, lihat Menghasilkan wawasan bertenaga AI untuk Amazon Security Lake menggunakan Amazon SageMaker AI Studio dan Amazon Bedrock.

Integrasi dengan AWS Security Hub

Jenis integrasi: Sumber

AWS Security Hubmemberi Anda pandangan komprehensif tentang keadaan keamanan Anda AWS dan membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub mengumpulkan data keamanan dari berbagai layanan Akun AWS, dan produk mitra pihak ketiga yang didukung serta membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi.

Saat Anda mengaktifkan Security Hub dan menambahkan temuan Security Hub sebagai sumber di Security Lake, Security Hub mulai mengirimkan temuan dan pembaruan baru ke temuan yang ada ke Security Lake.

Bagaimana Security Lake menerima temuan Security Hub

Di Security Hub, masalah keamanan dilacak sebagai temuan. Beberapa temuan berasal dari masalah yang terdeteksi oleh AWS layanan lain atau oleh mitra pihak ketiga. Security Hub juga menghasilkan temuannya sendiri dengan menjalankan pemeriksaan keamanan otomatis dan berkelanjutan terhadap aturan. Aturan diwakili oleh kontrol keamanan.

Semua temuan di Security Hub menggunakan JSON format standar yang disebut AWS Security Finding Format (ASFF).

Security Lake menerima temuan Security Hub dan mengubahnya menjadi. Buka Kerangka Skema Keamanan Siber (OCSF) di Danau Keamanan

Kirim temuan Security Hub Anda ke Security Lake

Untuk mengirim temuan Security Hub ke Security Lake, Anda harus mengaktifkan kedua layanan dan menambahkan temuan Security Hub sebagai sumber di Security Lake. Untuk petunjuk tentang menambahkan AWS sumber, lihatMenambahkan Layanan AWS sebagai sumber.

Jika Anda ingin Security Hub menghasilkan temuan kontrol dan mengirimkannya ke Security Lake, Anda harus mengaktifkan standar keamanan yang relevan dan mengaktifkan perekaman sumber daya secara Regional di AWS Config. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengonfigurasi AWS Config di AWS Security Hub Panduan Pengguna.

Berhenti menerima temuan Security Hub di Security Lake

Untuk berhenti menerima temuan Security Hub, Anda dapat menggunakan konsol Security Hub, Security HubAPI, atau AWS CLI.

Lihat Menonaktifkan dan mengaktifkan aliran temuan dari integrasi (konsol) atau Menonaktifkan aliran temuan dari integrasi (Security HubAPI, AWSCLI) di Panduan Pengguna.AWS Security Hub

Integrasi pihak ketiga dengan Security Lake

Amazon Security Lake terintegrasi dengan beberapa penyedia pihak ketiga. Penyedia mungkin menawarkan integrasi sumber, integrasi pelanggan, atau integrasi layanan. Penyedia mungkin menawarkan satu atau lebih jenis integrasi.

Integrasi sumber memiliki properti berikut:

- Kirim data ke Security Lake
- Data tiba dalam format Apache Parquet
- Data tiba dalam Buka Kerangka Skema Keamanan Siber (OCSF) di Danau Keamanan skema

Integrasi pelanggan memiliki properti berikut:

- Baca sumber data dari Security Lake di HTTPS titik akhir atau antrian Amazon Simple Queue Service SQS (Amazon), atau dengan langsung menanyakan data sumber dari AWS Lake Formation
- Mampu membaca data dalam format Apache Parquet
- Mampu membaca data dalam OCSF skema

Integrasi layanan dapat membantu Anda menerapkan Security Lake dan lainnya Layanan AWS di organisasi Anda. Mereka juga dapat memberikan bantuan dengan pelaporan, analitik, dan kasus penggunaan lainnya.

Untuk mencari penyedia mitra tertentu, lihat Partner Solutions Finder. Untuk membeli produk pihak ketiga, lihat AWSMarketplace.

Untuk meminta ditambahkan sebagai integrasi mitra atau menjadi mitra Security Lake, kirim email ke `<securitylake-partners@amazon.com>`.

Jika Anda menggunakan integrasi pihak ketiga yang mengirimkan temuan AWS Security Hub, Anda juga dapat meninjau temuan tersebut di Security Lake jika integrasi Security Hub untuk Security Lake diaktifkan. Untuk petunjuk tentang mengaktifkan integrasi, lihatIntegrasi dengan AWS Security Hub. Untuk daftar integrasi pihak ketiga yang mengirimkan temuan ke Security Hub, lihat Integrasi produk mitra pihak ketiga yang tersedia di AWS Security Hub Panduan Pengguna.

Sebelum mengatur pelanggan Anda, verifikasi dukungan OCSF log pelanggan Anda. Untuk detail terbaru, tinjau dokumentasi pelanggan Anda.

Integrasi kueri

Anda dapat menanyakan data yang disimpan Security Lake dalam AWS Lake Formation database dan tabel. Anda juga dapat membuat pelanggan pihak ketiga di konsol Security Lake,API, atau AWS Command Line Interface.

Administrator danau data Lake Formation harus memberikan `SELECT` izin pada database dan tabel yang relevan ke IAM identitas yang menanyakan data. Anda harus membuat pelanggan di Security Lake sebelum menanyakan data. Untuk informasi selengkapnya tentang cara membuat pelanggan dengan akses kueri, lihatMengelola akses kueri untuk pelanggan Security Lake.

Anda dapat mengonfigurasi integrasi kueri dengan Security Lake untuk mitra pihak ketiga berikut.

- Cribl – Search
- IBM – QRadar
- Palo Alto Networks – XSOAR
- Query.AI – Query Federated Search
- SOC Prime
- Splunk – Federated Analytics
- Tego Cyber

Accenture – MxDR

Jenis integrasi: Pelanggan, Layanan

Accenture's Integrasi MxDR dengan Security Lake menawarkan konsumsi data real-time dari log dan peristiwa, deteksi anomali terkelola, perburuan ancaman, dan operasi keamanan. Ini membantu analitik dan deteksi dan respons terkelola (MDR).

Sebagai integrasi layanan, Accenture juga dapat membantu Anda menerapkan Security Lake di organisasi Anda.

Dokumentasi integrasi

Aqua Security

Jenis integrasi: Sumber

Aqua Security dapat ditambahkan sebagai sumber khusus untuk mengirim acara audit ke Security Lake. Acara audit diubah menjadi OCSF skema dan format Parket.

Dokumentasi integrasi

Barracuda – Email Protection

Jenis integrasi: Sumber

Barracuda Email Protection dapat mengirim acara ke Security Lake ketika serangan email phishing baru terdeteksi. Anda dapat menerima acara ini bersama data keamanan lainnya di danau data Anda.

Dokumentasi integrasi

Booz Allen Hamilton

Jenis integrasi: Layanan

Sebagai integrasi layanan, Booz Allen Hamilton menggunakan pendekatan berbasis data untuk keamanan siber dengan menggabungkan data dan analitik dengan layanan Security Lake.

Tautan mitra

Bosch Software and Digital Solutions – AIShield

Jenis integrasi: Sumber

AIShield didukung oleh Bosch menyediakan analisis kerentanan otomatis dan perlindungan titik akhir untuk aset AI melalui integrasinya dengan Security Lake.

Dokumentasi integrasi

ChaosSearch

Jenis integrasi: Pelanggan

ChaosSearch menawarkan akses data multi-model ke pengguna dengan terbuka APIs seperti Elasticsearch danSQL, atau dengan Kibana dan Superset disertakan secara asli. UIs Anda dapat menggunakan data Security Lake Anda di ChaosSearch tanpa batas retensi untuk memantau,

waspada, dan berburu ancaman. Ini membantu Anda menghadapi lingkungan keamanan yang kompleks saat ini dan ancaman terus-menerus.

Dokumentasi integrasi

Cisco Security – Secure Firewall

Jenis integrasi: Sumber

Dengan mengintegrasikan Cisco Secure Firewall dengan Security Lake, Anda dapat menyimpan log firewall secara terstruktur dan terukur. eNcore Klien Cisco mengalirkan log firewall dari Pusat Manajemen Firewall, melakukan konversi skema ke OCSF skema, dan menyimpannya di Security Lake.

Dokumentasi integrasi

Claroty – xDome

Jenis integrasi: Sumber

Claroty xDome mengirimkan peringatan yang terdeteksi dalam jaringan ke Security Lake dengan konfigurasi minimal. Opsi penyebaran yang fleksibel dan cepat membantu xDome melindungi aset Internet of Things (XIoT) yang diperluas—yang terdiri dari IoT,, dan BMS aset—dalam jaringan AndaIIoT, sambil secara otomatis mendeteksi indikator awal ancaman.

Dokumentasi integrasi

CMD Solutions

Jenis integrasi: Layanan

CMD Solutions membantu bisnis meningkatkan kelincahan mereka dengan mengintegrasikan keamanan lebih awal dan terus menerus melalui desain, otomatisasi, dan proses jaminan berkelanjutan. Sebagai integrasi layanan, CMD Solutions dapat membantu Anda menerapkan Security Lake di organisasi Anda.

Tautan mitra

Confluent – Amazon S3 Sink Connector

Jenis integrasi: Sumber

Confluent secara otomatis menghubungkan, mengonfigurasi, dan mengatur integrasi data dengan konektor pra-bangun yang dikelola sepenuhnya. Bagian Confluent S3 Sink Connector memungkinkan Anda mengambil data mentah dan memasukkannya ke Security Lake dalam skala besar dalam format parket asli.

Dokumentasi integrasi

Contrast Security

Jenis integrasi: Sumber

Produk mitra untuk integrasi: Penilaian Kontras

Contrast Security Assess adalah IAST alat yang menawarkan deteksi kerentanan waktu nyata di aplikasi web,APIs, dan layanan mikro. Assese terintegrasi dengan Security Lake untuk membantu memberikan visibilitas terpusat untuk semua beban kerja Anda.

Dokumentasi integrasi

Cribl – Search

Jenis integrasi: Pelanggan

Anda dapat menggunakan Cribl Search untuk mencari data Security Lake.

Dokumentasi integrasi

Cribl – Stream

Jenis integrasi: Sumber

Anda dapat menggunakan Cribl Stream untuk mengirim data dari Cribl mendukung sumber pihak ketiga untuk Security Lake dalam OCSF skema.

Dokumentasi integrasi

CrowdStrike – Falcon Data Replicator

Jenis integrasi: Sumber

Integrasi ini menarik data dari CrowdStrike Falcon Data Replicator secara streaming berkelanjutan, mengubah data menjadi OCSF skema, dan mengirimkannya ke Security Lake.

Dokumentasi integrasi

CrowdStrike – Next Gen SIEM

Jenis integrasi: Pelanggan

Sederhanakan konsumsi data Security Lake dengan CrowdStrike Falcon Next-Gen SIEM konektor data yang menampilkan OCSF parser skema asli. Falcon NG SIEM merevolusi deteksi, investigasi, dan respons ancaman dengan menyatukan kedalaman dan luasnya keamanan yang tak tertandingi dalam satu platform terpadu untuk menghentikan pelanggaran.

Dokumentasi integrasi

CyberArk – Unified Identify Security Platform

Jenis integrasi: Sumber

CyberArk Audit Adapter, AWS Lambda fungsi, mengumpulkan peristiwa keamanan dari CyberArk Identity Security Platform dan mengirimkan data ke Security Lake dalam OCSF skema.

Dokumentasi integrasi

Cyber Security Cloud – Cloud Fastener

Jenis integrasi: Pelanggan

CloudFastener memanfaatkan Security Lake untuk mempermudah mengkonsolidasikan data keamanan dari lingkungan cloud Anda.

Dokumentasi integrasi

DataBahn

Jenis integrasi: Sumber

Memusatkan data keamanan Anda di Security Lake menggunakan DataBahn’s Kain Data Keamanan.

Dokumentasi integrasi (masuk ke DataBahn portal untuk meninjau dokumentasi)

Darktrace – Cyber AI Loop

Jenis integrasi: Sumber

Bagian Darktrace dan integrasi Security Lake membawa kekuatan Darktrace belajar mandiri ke Security Lake. Wawasan dari Cyber AI Loop dapat dikorelasikan dengan aliran data lain dan elemen tumpukan keamanan organisasi Anda. Log integrasi Darktrace pelanggaran model sebagai temuan keamanan.

Dokumentasi integrasi (masuk ke Darktrace portal untuk meninjau dokumentasi)

Datadog

Jenis integrasi: Pelanggan

Datadog Cloud SIEM mendeteksi ancaman real-time terhadap lingkungan cloud Anda, termasuk data di Security Lake, dan menyatukan DevOps dan tim keamanan dalam satu platform.

Dokumentasi integrasi

Deloitte – MXDR Cyber Analytics and AI Engine (CAE)

Jenis integrasi: Pelanggan, Layanan

Deloitte MXDR CAE membantu Anda dengan cepat menyimpan, menganalisis, dan memvisualisasikan data keamanan standar Anda. CAERangkaian kemampuan analitik, AI, dan ML yang disesuaikan secara otomatis memberikan wawasan yang dapat ditindaklanjuti berdasarkan model yang dijalankan terhadap data yang OCSF diformat di Security Lake.

Sebagai integrasi layanan, Deloitte juga dapat membantu Anda menerapkan Security Lake di organisasi Anda.

Dokumentasi integrasi

Devo

Jenis integrasi: Pelanggan

Bagian Devo kolektor untuk AWS mendukung konsumsi dari Security Lake. Integrasi ini dapat membantu Anda menganalisis dan mengatasi berbagai kasus penggunaan keamanan, seperti deteksi ancaman, investigasi, dan respons insiden.

Dokumentasi integrasi

DXC – SecMon

Jenis integrasi: Pelanggan, Layanan

DXC SecMon mengumpulkan peristiwa keamanan dari Security Lake dan memantaunya untuk mendeteksi dan memperingatkan potensi ancaman keamanan. Ini membantu organisasi mendapatkan pemahaman yang lebih baik tentang postur keamanan mereka dan secara proaktif mengidentifikasi dan menanggapi ancaman.

Sebagai integrasi layanan, DXC juga dapat membantu Anda menerapkan Security Lake di organisasi Anda.

Dokumentasi integrasi

Eviden – AIsaac (sebelumnya Atos)

Jenis integrasi: Pelanggan

Bagian AIsaac MDR platform mengkonsumsi VPC Flow Logs yang tertelan dalam OCSF skema di Security Lake dan menggunakan model AI untuk mendeteksi ancaman.

Dokumentasi integrasi

ExtraHop – Reveal(x) 360

Jenis integrasi: Sumber

Anda dapat meningkatkan beban kerja dan keamanan aplikasi Anda dengan mengintegrasikan data jaringan, termasuk deteksi, dari IOCs ExtraHop Reveal(x) 360, ke Security Lake dalam OCSF skema

Dokumentasi integrasi

Falcosidekick

Jenis integrasi: Sumber

Falcosidekick mengumpulkan dan mengirim acara Falco ke Security Lake. Integrasi ini mengekspor peristiwa keamanan menggunakan OCSF skema.

Dokumentasi integrasi

Fortinet - Cloud Native Firewall

Jenis integrasi: Sumber

Saat membuat FortiGate CNFcontoh di AWS, Anda dapat menentukan Amazon Security Lake sebagai tujuan keluaran log.

Dokumentasi integrasi

Gigamon – Application Metadata Intelligence

Jenis integrasi: Sumber

Gigamon Application Metadata Intelligence (AMI) memberdayakan observabilitas Anda,SIEM, dan alat pemantauan kinerja jaringan dengan atribut metadata penting. Ini membantu memberikan visibilitas aplikasi yang lebih dalam sehingga Anda dapat menentukan kemacetan kinerja, masalah kualitas, dan potensi risiko keamanan jaringan.

Dokumentasi integrasi

Hoop Cyber

Jenis integrasi: Layanan

Hoop Cyber FastStart mencakup penilaian sumber data, prioritas, orientasi sumber data dan membantu pelanggan menanyakan data mereka dengan alat dan integrasi yang ada yang ditawarkan melalui Security Lake.

Tautan mitra

HTCD – AI-First Cloud Security Platform

Jenis integrasi: Pelanggan

Dapatkan otomatisasi kepatuhan seketika, memprioritaskan temuan keamanan, dan tambalan yang disesuaikan. HTCDdapat menanyakan Security Lake untuk membantu Anda mengungkap ancaman dengan kueri bahasa alami dan wawasan berbasis AI.

Dokumentasi integrasi

IBM – QRadar

Jenis integrasi: Pelanggan

IBM Security QRadar SIEM with UAX mengintegrasikan Security Lake dengan platform analitik yang mengidentifikasi dan mencegah ancaman di cloud hybrid. Integrasi ini mendukung akses data dan akses kueri.

Dokumentasi integrasi pada AWS CloudTrail log konsumsi

Dokumentasi integrasi tentang penggunaan Amazon Athena untuk kueri

Infosys

Jenis integrasi: Layanan

Infosys membantu Anda menyesuaikan implementasi Security Lake Anda untuk kebutuhan organisasi Anda dan memberikan wawasan khusus.

Tautan mitra

Insbuilt

Jenis integrasi: Layanan

Insbuilt mengkhususkan diri dalam layanan konsultasi cloud dan dapat membantu Anda memahami cara menerapkan Security Lake di organisasi Anda.

Tautan mitra

Kyndryl – AIOps

Jenis integrasi: Pelanggan, Layanan

Kyndryl terintegrasi dengan Security Lake untuk menyediakan interoperabilitas data siber, intelijen ancaman, dan analitik bertenaga AI. Sebagai pelanggan akses data, Kyndryl mencerna Acara AWS CloudTrail Manajemen dari Security Lake untuk tujuan analitik.

Sebagai integrasi layanan, Kyndryl juga dapat membantu Anda menerapkan Security Lake di organisasi Anda.

Dokumentasi integrasi

Lacework – Polygraph

Jenis integrasi: Sumber

Lacework Polygraph® Data Platform terintegrasi dengan Security Lake sebagai sumber data dan memberikan temuan keamanan tentang kerentanan, kesalahan konfigurasi, dan ancaman yang diketahui dan tidak dikenal di seluruh lingkungan Anda. AWS

Dokumentasi integrasi

Laminar

Jenis integrasi: Sumber

Laminar mengirimkan peristiwa keamanan data ke Security Lake dalam OCSF skema, membuatnya tersedia untuk kasus penggunaan analitik tambahan, seperti respons insiden dan investigasi.

Dokumentasi integrasi

MegazoneCloud

Jenis integrasi: Layanan

MegazoneCloud mengkhususkan diri dalam layanan konsultasi cloud dan dapat membantu Anda memahami cara menerapkan Security Lake di organisasi Anda. Kami menghubungkan Security Lake dengan ISV solusi terintegrasi untuk membangun tugas khusus, dan membangun wawasan khusus yang terkait dengan kebutuhan pelanggan.

Dokumentasi integrasi

Monad

Jenis integrasi: Sumber

Monad secara otomatis mengubah data Anda menjadi OCSF skema dan mengirimkannya ke danau data Security Lake Anda.

Dokumentasi integrasi

NETSCOUT – Omnis Cyber Intelligence

Jenis integrasi: Sumber

Dengan berintegrasi dengan Security Lake, NETSCOUT menjadi sumber kustom temuan keamanan dan wawasan keamanan terperinci tentang apa yang terjadi di perusahaan Anda, seperti ancaman siber, risiko keamanan, dan perubahan permukaan serangan. Temuan ini dihasilkan di akun pelanggan oleh NETSCOUT CyberStreams and Omnis Cyber Intelligence, dan kemudian dikirim ke Danau Keamanan dalam OCSF skema. Data yang dicerna juga memenuhi persyaratan dan praktik terbaik lainnya untuk sumber Security Lake, termasuk format, skema, partisi, dan aspek terkait kinerja.

Dokumentasi integrasi

Netskope – CloudExchange

Jenis integrasi: Sumber

Netskope membantu Anda memperkuat postur keamanan Anda dengan berbagi log terkait keamanan dan informasi ancaman dengan Security Lake. Netskope Temuan dikirim ke Security Lake dengan CloudExchange Plugin, yang dapat diluncurkan sebagai lingkungan berbasis buruh pelabuhan di dalam AWS atau di pusat data lokal.

Dokumentasi integrasi

New Relic ONE

Jenis integrasi: Pelanggan

New Relic ONE adalah aplikasi pelanggan berbasis Lambda. Ini digunakan di akun Anda, dipicu oleh AmazonSQS, dan mengirimkan data ke New Relic memakai New Relic kunci lisensi

Dokumentasi integrasi

Okta – Workforce Identity Cloud

Jenis integrasi: Sumber

Okta mengirimkan log identitas ke Security Lake dalam OCSF skema melalui EventBridge integrasi Amazon. Okta System Logs dalam OCSF skema akan membantu tim ilmuwan keamanan dan data untuk menanyakan peristiwa keamanan dengan standar sumber terbuka. Membuat OCSF log standar dari Okta membantu Anda melakukan aktivitas audit dan menghasilkan laporan yang terkait dengan otentikasi, otorisasi, perubahan akun, dan perubahan entitas di bawah skema yang konsisten.

Dokumentasi integrasi

AWS CloudFormation template untuk ditambahkan Okta sebagai sumber khusus di Security Lake

Orca – Cloud Security Platform

Jenis integrasi: Sumber

Bagian Orca Platform keamanan cloud tanpa agen untuk AWS terintegrasi dengan Security Lake dengan mengirimkan peristiwa Cloud Detection and Response (CDR) dalam skema. OCSF

Dokumentasi integrasi (masuk ke Orca portal untuk meninjau dokumentasi)

Palo Alto Networks – Prisma Cloud

Jenis integrasi: Sumber

Palo Alto Networks Prisma Cloud mengumpulkan data deteksi kerentanan di VMs lingkungan cloud-native Anda dan mengirimkannya ke Security Lake.

Dokumentasi integrasi

Palo Alto Networks – XSOAR

Jenis integrasi: Suscriber

Palo Alto Networks XSOAR telah membangun integrasi pelanggan dengan XSOAR dan Security Lake.

Dokumentasi integrasi

Panther

Jenis integrasi: Pelanggan

Panther mendukung menelan log Security Lake untuk digunakan dalam pencarian dan deteksi.

Dokumentasi integrasi

Ping Identity – PingOne

Jenis integrasi: Sumber

PingOne mengirimkan peringatan modifikasi akun ke Security Lake dalam OCSF skema dan format Parket, memungkinkan Anda menemukan dan menindaklanjuti perubahan akun.

Dokumentasi integrasi

PwC – Fusion center

Jenis integrasi: Pelanggan, Layanan

PwC membawa pengetahuan dan keahlian untuk membantu klien dalam menerapkan pusat fusi untuk memenuhi kebutuhan masing-masing. Dibangun di Amazon Security Lake, pusat fusi menyediakan kemampuan untuk menggabungkan data dari berbagai sumber untuk membuat tampilan terpusat, dekat waktu nyata.

Dokumentasi integrasi

Query.AI – Query Federated Search

Jenis integrasi: Pelanggan

Query Federated Search dapat langsung menanyakan tabel Danau Keamanan apa pun melalui Amazon Athena untuk mendukung respons insiden, investigasi, perburuan ancaman, dan pencarian umum di berbagai Observable, Peristiwa, dan Objek dalam skema. OCSF

Dokumentasi integrasi

Rapid7 – InsightIDR

Jenis integrasi: Pelanggan

InsightIDR, Rapid7 SIEM/XDRsolusi, dapat menelan log di Danau Keamanan untuk deteksi ancaman dan penyelidikan aktivitas yang mencurigakan.

Dokumentasi integrasi

RipJar – Labyrinth for Threat Investigations

Jenis integrasi: Pelanggan

Labyrinth for Threat Investigations menyediakan pendekatan di seluruh perusahaan untuk eksplorasi ancaman dalam skala besar berdasarkan fusi data, dengan keamanan halus, alur kerja yang dapat disesuaikan, dan pelaporan.

Dokumentasi integrasi

Sailpoint

Jenis integrasi: Sumber

Produk mitra untuk integrasi: SailPoint IdentityNow

Integrasi ini memungkinkan pelanggan untuk mengubah data peristiwa dari SailPoint IdentityNow. Integrasi ini dimaksudkan untuk menyediakan proses otomatis untuk membawa IdentityNow aktivitas pengguna dan acara tata kelola ke Security Lake untuk meningkatkan wawasan dari insiden keamanan dan produk pemantauan peristiwa.

Dokumentasi integrasi

Securonix

Jenis integrasi: Pelanggan

Securonix Next-Gen SIEM terintegrasi dengan Security Lake, memberdayakan tim keamanan untuk menyerap data lebih cepat dan memperluas kemampuan deteksi dan respons mereka.

Dokumentasi integrasi

SentinelOne

Jenis integrasi: Pelanggan

Bagian SentinelOne Singularity™ XDR Platform memperluas deteksi dan respons real-time ke titik akhir, identitas, dan beban kerja cloud yang berjalan di infrastruktur cloud lokal dan publik, termasuk Amazon Elastic Compute Cloud (Amazon), Amazon Elastic Container Service (AmazonEC2), dan Amazon Elastic ECS Kubernetes Service (Amazon). EKS

Dokumentasi integrasi (masuk ke SentinelOne portal untuk meninjau dokumentasi)

Sentra – Data Lifecyle Security Platform

Jenis integrasi: Sumber

Setelah menerapkan Sentra infrastruktur pemindaian di akun Anda, Sentra mengambil temuan dan menelannya ke dalam SaaS Anda. Temuan ini adalah metadata yang Sentra menyimpan dan kemudian mengalirkan ke Security Lake dalam OCSF skema untuk kueri.

Dokumentasi integrasi

SOC Prime

Jenis integrasi: Pelanggan

SOC Prime terintegrasi dengan Security Lake melalui Amazon OpenSearch Service dan Amazon Athena untuk memfasilitasi orkestrasi data cerdas dan perburuan ancaman berdasarkan tonggak nol kepercayaan. SOC Prime Memberdayakan tim keamanan untuk meningkatkan visibilitas ancaman dan menyelidiki insiden tanpa volume peringatan yang berlebihan. Anda dapat menghemat waktu pengembangan dengan aturan dan kueri yang dapat digunakan kembali yang secara otomatis dapat dikonversi ke Athena dan OpenSearch Layanan dalam skema. OCSF

Dokumentasi integrasi

Splunk

Jenis integrasi: Pelanggan

Bagian Splunk AWS Add-On untuk Amazon Web Services (AWS) mendukung konsumsi dari Security Lake. Integrasi ini membantu Anda mempercepat deteksi, investigasi, dan respons ancaman dengan berlangganan data dalam OCSF skema dari Security Lake.

Dokumentasi integrasi

Stellar Cyber

Jenis integrasi: Pelanggan

Stellar Cyber mengkonsumsi log dari Security Lake dan menambahkan catatan ke Stellar Cyber danau data. Konektor ini menggunakan OCSF skema.

Dokumentasi integrasi

Sumo Logic

Jenis integrasi: Pelanggan

Sumo Logic mengkonsumsi data dari Security Lake dan menyediakan visibilitas luas di seluruh lingkungan cloud AWS, on-premise, dan hybrid. Sumo Logic memberi tim keamanan visibilitas, otomatisasi, dan pemantauan ancaman yang komprehensif di semua alat keamanan mereka.

Dokumentasi integrasi

Swimlane – Turbine

Jenis integrasi: Pelanggan

Swimlane Menyerap data dari Security Lake dalam OCSF skema, dan mengirimkan data melalui buku pedoman kode rendah dan manajemen kasus untuk memfasilitasi deteksi ancaman, investigasi, dan respons insiden yang lebih cepat.

Dokumentasi integrasi (masuk ke Swimlane portal untuk meninjau dokumentasi)

Sysdig Secure

Jenis integrasi: Sumber

Sysdig Secure's platform perlindungan aplikasi cloud-native (CNAPP) mengirimkan peristiwa keamanan ke Security Lake untuk memaksimalkan pengawasan, merampingkan investigasi, dan menyederhanakan kepatuhan.

Dokumentasi integrasi

Talon

Jenis integrasi: Sumber

Produk mitra untuk integrasi: Talon Enterprise Browser

Talon's Enterprise Browser, lingkungan titik akhir berbasis browser yang aman dan terisolasi, mengirim Talon Akses, perlindungan data, tindakan SaaS, dan peristiwa keamanan ke Security Lake menyediakan visibilitas dan opsi untuk menghubungkan peristiwa untuk deteksi, forensik, dan investigasi.

Dokumentasi integrasi (masuk ke Talon portal untuk meninjau dokumentasi)

Tanium

Jenis integrasi: Sumber

Tanium Unified Cloud Endpoint Detection, Management, and Security Platform menyediakan data inventaris ke Security Lake dalam OCSF skema.

Dokumentasi integrasi

TCS

Jenis integrasi: Layanan

Bagian TCS AWS Business Unit menawarkan inovasi, pengalaman, dan bakat. Integrasi ini didukung oleh satu dekade penciptaan nilai bersama, pengetahuan industri yang mendalam, keahlian teknologi, dan kebijaksanaan pengiriman. Sebagai integrasi layanan, TCS dapat membantu Anda menerapkan Security Lake di organisasi Anda.

Dokumentasi integrasi

Tego Cyber

Jenis integrasi: Pelanggan

Tego Cyber terintegrasi dengan Security Lake untuk membantu Anda mendeteksi dan menyelidiki potensi ancaman keamanan dengan cepat. Dengan menghubungkan beragam indikator ancaman di seluruh kerangka waktu yang luas dan sumber log, Tego Cyber mengungkap ancaman tersembunyi. Platform ini diperkaya dengan intelijen ancaman yang sangat kontekstual, memberikan presisi dan wawasan dalam deteksi dan investigasi ancaman.

Dokumentasi integrasi

Tines – No-code security automation

Jenis integrasi: Pelanggan

Tines No-code security automation membantu Anda membuat keputusan yang lebih akurat dengan memanfaatkan data keamanan yang terpusat di Security Lake.

Dokumentasi integrasi

Torq – Enterprise Security Automation Platform

Jenis integrasi: Sumber, Pelanggan

Torq terintegrasi dengan mulus dengan Security Lake sebagai sumber khusus dan pelanggan. Torq membantu Anda menerapkan otomatisasi dan orkestrasi skala perusahaan dengan platform tanpa kode sederhana.

Dokumentasi integrasi

Trellix – XDR

Jenis integrasi: Sumber, Pelanggan

Sebagai XDR platform terbuka, Trellix XDR mendukung integrasi Security Lake. Trellix XDR dapat memanfaatkan data dalam OCSF skema untuk kasus penggunaan analitik keamanan. Anda juga dapat menambah data lake Security Lake Anda dengan 1.000+ sumber peristiwa keamanan di Trellix XDR. Ini membantu Anda memperluas kemampuan deteksi dan respons untuk AWS lingkungan Anda. Data yang tertelan berkorelasi dengan risiko keamanan lainnya, memberi Anda buku pedoman yang diperlukan untuk menanggapi risiko secara tepat waktu.

Dokumentasi integrasi

Trend Micro – CloudOne

Jenis integrasi: Sumber

Trend Micro CloudOne Workload Security mengirimkan informasi berikut ke Security Lake dari instans Amazon Elastic Compute Cloud (EC2) Anda:

- DNSAktivitas kueri
- Aktivitas berkas
- Aktivitas jaringan
- Aktivitas proses
- Aktivitas Nilai Registri
- Aktivitas Akun Pengguna

Dokumentasi integrasi

Uptycs – Uptycs XDR

Jenis integrasi: Sumber

Uptycs mengirimkan banyak data dalam OCSF skema dari aset lokal dan cloud ke Security Lake. Data tersebut mencakup deteksi ancaman perilaku dari titik akhir dan beban kerja cloud, deteksi anomali, pelanggaran kebijakan, kebijakan berisiko, kesalahan konfigurasi, dan kerentanan.

Dokumentasi integrasi

Vectra AI – Vectra Detect for AWS

Jenis integrasi: Sumber

Dengan menggunakan Vectra Detect for AWS, Anda dapat mengirim peringatan kesetiaan tinggi ke Security Lake sebagai sumber khusus menggunakan templat khusus. AWS CloudFormation

Dokumentasi integrasi

VMware Aria Automation for Secure Clouds

Jenis integrasi: Sumber

Dengan integrasi ini, Anda dapat mendeteksi kesalahan konfigurasi cloud dan mengirimkannya ke Security Lake untuk analisis lanjutan.

Dokumentasi integrasi

Wazuh

Jenis integrasi: Pelanggan

Wazuh bertujuan untuk menangani data pengguna dengan aman, menyediakan akses kueri untuk setiap sumber, dan mengoptimalkan biaya kueri.

Dokumentasi integrasi

Wipro

Jenis integrasi: Sumber, Layanan

Integrasi ini memungkinkan Anda untuk mengumpulkan data dari Wipro Cloud Application Risk Governance (CARG) platform untuk memberikan pandangan terpadu tentang aplikasi cloud Anda dan postur kepatuhan di seluruh perusahaan.

Sebagai integrasi layanan, Wipro juga dapat membantu Anda menerapkan Security Lake di organisasi Anda.

Dokumentasi integrasi

Wiz – CNAPP

Jenis integrasi: Sumber

Integrasi antara Wiz Security Lake memfasilitasi pengumpulan data keamanan cloud dalam satu danau data keamanan dengan memanfaatkan OCSF skema, standar open source yang dirancang untuk pertukaran data keamanan yang dapat diperluas dan dinormalisasi.

Dokumentasi integrasi (masuk ke Wiz portal untuk meninjau dokumentasi)

Zscaler – Zscaler Posture Control

Jenis integrasi: Sumber

Zscaler Posture Control™, platform perlindungan aplikasi cloud native, mengirimkan temuan keamanan ke Security Lake dalam OCSF skema.

Dokumentasi integrasi

Keamanan di Danau Keamanan

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon Security Lake, lihat AWS Layanan dalam Lingkup menurut AWS Layanan Program Kepatuhan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Security Lake. Topik berikut menunjukkan cara mengkonfigurasi Security Lake untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Security Lake Anda.

Topik

Manajemen identitas dan akses untuk Security Lake

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. IAMadministrator mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Security Lake. IAMadalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Security Lake.

Pengguna layanan — Jika Anda menggunakan layanan Security Lake untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Security Lake untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Security Lake, lihatMemecahkan masalah identitas dan akses Amazon Security Lake.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Security Lake di perusahaan Anda, Anda mungkin memiliki akses penuh ke Security Lake. Tugas Anda adalah menentukan fitur dan sumber daya Security Lake mana yang harus diakses pengguna layanan Anda. Anda kemudian harus mengirimkan permintaan ke IAM administrator Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasarIAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM Security Lake, lihatBagaimana Security Lake bekerja dengan IAM.

IAMadministrator — Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Security Lake. Untuk melihat contoh kebijakan berbasis identitas Security Lake yang dapat Anda gunakan, lihat. IAM Contoh kebijakan berbasis identitas untuk Security Lake

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai IAM pengguna, atau dengan mengambil peranIAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (Pusat IAM Identitas), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas federasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Versi AWS Tanda Tangan 4 untuk API permintaan di Panduan IAM Pengguna.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor di Panduan AWS IAM Identity Center Pengguna dan Autentikasi AWS multi-faktor IAM di Panduan Pengguna. IAM

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan

untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensi pengguna root di IAMPanduan Pengguna.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat IAM Identitas, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat IAM Identitas, lihat Apa itu Pusat IAM Identitas? dalam AWS IAM Identity Center User Guide.

Pengguna dan grup IAM

IAMPengguna adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensi sementara daripada membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensi jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang di IAMPanduan Pengguna.

IAMGrup adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdminsdan memberikan izin grup tersebut untuk mengelola sumber dayaIAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk IAM pengguna di Panduan IAM Pengguna.

IAMperan

IAMPeran adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Untuk mengambil IAM peran sementara di dalam AWS Management Console, Anda dapat beralih dari pengguna ke IAM peran (konsol). Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustomURL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat Metode untuk mengambil peran dalam Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk penyedia identitas pihak ketiga (federasi) di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas mengkorelasikan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin

melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.

- Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.
- Peran layanan — Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam IAMPanduan Pengguna.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredensil sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instans yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di IAMPanduan Pengguna.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai JSON dokumen. Untuk

informasi selengkapnya tentang struktur dan isi dokumen JSON kebijakan, lihat Ringkasan JSON kebijakan di Panduan IAM Pengguna.

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

IAMkebijakan menentukan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Menentukan IAM izin khusus dengan kebijakan yang dikelola pelanggan di Panduan Pengguna. IAM

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan sebaris, lihat Memilih antara kebijakan terkelola dan kebijakan sebaris di IAMPanduan Pengguna.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat

dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnyaACLs, lihat Ikhtisar daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batas izin — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk IAM entitas di IAMPanduan Pengguna.
- Kebijakan kontrol layanan (SCPs) — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations danSCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.

- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah JSON kebijakan yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui IAM kebijakan yang dilampirkan ke setiap sumber daya yang Anda miliki. RCPMembatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations danRCPs, termasuk daftar dukungan Layanan AWS tersebutRCPs, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi di Panduan IAM Pengguna.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan IAM Pengguna.

Bagaimana Security Lake bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Security Lake, pelajari IAM fitur apa saja yang tersedia untuk digunakan dengan Security Lake.

IAMfitur yang dapat Anda gunakan dengan Amazon Security Lake

IAMfitur	Dukungan Security Lake
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Ya
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya

IAMfitur	Dukungan Security Lake
Kunci kondisi kebijakan	Ya
ACLs	Tidak
ABAC(tag dalam kebijakan)	Ya
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Security Lake dan AWS layanan lainnya dengan sebagian besar IAM fitur, lihat AWS layanan yang berfungsi IAM di Panduan IAM Pengguna.

Kebijakan berbasis identitas untuk Security Lake

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Menentukan IAM izin khusus dengan kebijakan yang dikelola pelanggan di Panduan Pengguna. IAM

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam JSON kebijakan, lihat referensi elemen IAM JSON kebijakan di Panduan IAM Pengguna.

Security Lake mendukung kebijakan berbasis identitas. Untuk informasi selengkapnya, lihat Contoh kebijakan berbasis identitas untuk Security Lake.

Kebijakan berbasis sumber daya dalam Security Lake

Mendukung kebijakan berbasis sumber daya: Ya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau IAM entitas di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, IAM administrator di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun IAM di Panduan IAM Pengguna.

Layanan Security Lake membuat kebijakan berbasis sumber daya untuk bucket Amazon S3 yang menyimpan data Anda. Anda tidak melampirkan kebijakan berbasis sumber daya ini ke bucket S3 Anda. Security Lake secara otomatis membuat kebijakan ini atas nama Anda.

Sumber daya contoh adalah bucket S3 dengan Amazon Resource Name (ARN) dari. `arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}` Dalam contoh ini, `region` adalah spesifik Wilayah AWS tempat Anda mengaktifkan Security Lake, dan `bucket-identifier` merupakan string alfanumerik unik Regional yang ditetapkan Security Lake ke bucket. Security Lake membuat bucket S3 untuk menyimpan data dari Wilayah itu. Kebijakan sumber daya menentukan prinsipal mana yang dapat melakukan tindakan di bucket. Berikut contoh kebijakan berbasis sumber daya (kebijakan bucket) yang dilampirkan Security Lake ke bucket:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Deny",
            "Principal": {
                "AWS": "*"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}/*",
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        },
        {
            "Sid": "PutSecurityLakeObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "securitylake.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}/*",
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{DA-AccountID}",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:securitylake:us-east-1:{DA-AccountID}:*"
                }
            }
        }
    ]
}
```

Untuk mempelajari lebih lanjut tentang kebijakan berbasis sumber daya, lihat Kebijakan berbasis identitas dan kebijakan berbasis sumber daya di Panduan Pengguna. IAM

Tindakan kebijakan untuk Security Lake

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

`Action`Elemen JSON kebijakan menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan AWS API operasi terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi yang cocok. API Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk daftar tindakan Security Lake, lihat Tindakan yang ditentukan oleh Amazon Security Lake di Referensi Otorisasi Layanan.

Tindakan kebijakan di Security Lake menggunakan awalan berikut sebelum tindakan:

```
securitylake
```

Misalnya, untuk memberikan izin kepada pengguna untuk mengakses informasi tentang pelanggan tertentu, sertakan `securitylake:GetSubscriber` tindakan dalam kebijakan yang ditetapkan kepada pengguna tersebut. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Security Lake mendefinisikan serangkaian tindakannya sendiri yang menggambarkan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "securitylake:action1",
      "securitylake:action2"
]
```

Untuk melihat contoh kebijakan berbasis identitas Security Lake, lihat. Contoh kebijakan berbasis identitas untuk Security Lake

Sumber daya kebijakan untuk Danau Keamanan

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Security Lake mendefinisikan jenis sumber daya berikut: pelanggan, dan konfigurasi data lake untuk Akun AWS dalam tertentu. Wilayah AWS Anda dapat menentukan jenis sumber daya ini dalam kebijakan dengan menggunakanARNs.

Untuk daftar jenis sumber daya Security Lake dan ARN sintaks untuk masing-masing sumber daya, lihat Jenis sumber daya yang ditentukan oleh Amazon Security Lake di Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat Anda tentukan untuk setiap jenis sumber daya, lihat Tindakan yang ditentukan oleh Amazon Security Lake di Referensi Otorisasi Layanan.

Untuk melihat contoh kebijakan berbasis identitas Security Lake, lihat. Contoh kebijakan berbasis identitas untuk Security Lake

Kunci kondisi kebijakan untuk Security Lake

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat elemen IAM kebijakan: variabel dan tag di Panduan IAM Pengguna.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan IAM Pengguna.

Untuk daftar kunci kondisi Security Lake, lihat Kunci kondisi untuk Amazon Security Lake di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat digunakan untuk menggunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Amazon Security Lake di Referensi Otorisasi Layanan. Untuk contoh kebijakan yang menggunakan kunci kondisi, lihatContoh kebijakan berbasis identitas untuk Security Lake.

Daftar kontrol akses (ACLs) di Security Lake

MendukungACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Security Lake tidak mendukungACLs, yang berarti Anda tidak dapat melampirkan ACL ke sumber daya Danau Keamanan.

Kontrol akses berbasis atribut (ABAC) dengan Security Lake

Mendukung ABAC (tag dalam kebijakan): Ya

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke IAM entitas (pengguna

atau peran) dan ke banyak AWS sumber daya. Menandai entitas dan sumber daya adalah langkah pertama dari. ABAC Kemudian Anda merancang ABAC kebijakan untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

ABACmembantu dalam lingkungan yang berkembang pesat dan membantu dengan situasi di mana manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnyaABAC, lihat Menentukan izin dengan ABAC otorisasi di IAMPanduan Pengguna. Untuk melihat tutorial dengan langkah-langkah penyiapanABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di IAMPanduan Pengguna.

Anda dapat melampirkan tag ke sumber daya Security Lake — pelanggan, dan konfigurasi data lake untuk individu. Akun AWS Wilayah AWS Anda juga dapat mengontrol akses ke jenis sumber daya ini dengan memberikan informasi tag dalam `Condition` elemen kebijakan. Untuk informasi tentang menandai sumber daya Security Lake, lihatMenandai sumber daya Danau Keamanan. Untuk contoh kebijakan berbasis identitas yang mengontrol akses ke sumber daya berdasarkan tag untuk sumber daya tersebut, lihat. Contoh kebijakan berbasis identitas untuk Security Lake

Menggunakan kredensil sementara dengan Security Lake

Mendukung kredensial sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensil sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensil sementara, lihat Layanan AWS yang berfungsi IAM di IAMPanduan Pengguna.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan link sign-on (SSO) tunggal perusahaan Anda, proses tersebut secara otomatis membuat kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi

selengkapnya tentang beralih peran, lihat Beralih dari pengguna ke IAM peran (konsol) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensil sementara menggunakan atau. AWS CLI AWS API Anda kemudian dapat menggunakan kredensil sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensi keamanan sementara di. IAM

Security Lake mendukung penggunaan kredensil sementara.

Teruskan sesi akses untuk Security Lake

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.

Beberapa tindakan Security Lake memerlukan izin untuk tindakan tambahan yang bergantung pada tindakan lain Layanan AWS. Untuk daftar tindakan ini, lihat Tindakan yang ditentukan oleh Amazon Security Lake di Referensi Otorisasi Layanan.

Peran layanan untuk Security Lake

Mendukung peran layanan: Tidak

Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam IAMPanduan Pengguna.

Security Lake tidak mengambil atau menggunakan peran layanan. Namun, layanan terkait seperti Amazon EventBridge AWS Lambda, dan Amazon S3 mengambil peran layanan saat

Anda menggunakan Security Lake. Untuk melakukan tindakan atas nama Anda, Security Lake menggunakan peran terkait layanan.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat menimbulkan masalah operasional dengan penggunaan Security Lake. Edit peran layanan hanya jika Security Lake memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Security Lake

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

Security Lake menggunakan peran IAM terkait layanan bernama. `AWSServiceRoleForAmazonSecurityLake` Peran terkait layanan Security Lake memberikan izin untuk mengoperasikan layanan danau data keamanan atas nama pelanggan. Peran terkait layanan ini adalah IAM peran yang terkait langsung dengan Security Lake. Ini telah ditentukan sebelumnya oleh Security Lake, dan itu mencakup semua izin yang diperlukan Security Lake untuk memanggil orang lain Layanan AWS atas nama Anda. Security Lake menggunakan peran terkait layanan ini di semua Wilayah AWS tempat Danau Keamanan tersedia.

Untuk detail tentang membuat atau mengelola peran terkait layanan Security Lake, lihat. Menggunakan peran terkait layanan untuk Security Lake

Contoh kebijakan berbasis identitas untuk Security Lake

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Security Lake. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan IAM berbasis identitas menggunakan contoh dokumen kebijakan ini, lihat Membuat JSON IAM kebijakan (konsol) di Panduan Pengguna. IAM

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Security Lake, termasuk format ARNs untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk Amazon Security Lake di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Security Lake
- Contoh: Izinkan pengguna untuk melihat izin mereka sendiri
- Contoh: Izinkan akun manajemen organisasi untuk menunjuk dan menghapus administrator yang didelegasikan
- Contoh: Izinkan pengguna untuk meninjau pelanggan berdasarkan tag

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Security Lake di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan AWSAWS terkelola atau kebijakan terkelola untuk fungsi pekerjaan di Panduan IAM Pengguna.
- Menerapkan izin hak istimewa paling sedikit — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang penggunaan IAM untuk menerapkan izin, lihat Kebijakan dan izin IAM di IAM Panduan Pengguna.

- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakanSSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat elemen IAM JSON kebijakan: Kondisi dalam Panduan IAM Pengguna.
- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda guna memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa IAM kebijakan () JSON dan praktik terbaik. IAM IAMAccess Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Memvalidasi kebijakan dengan IAM Access Analyzer di IAMPanduan Pengguna.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan IAM pengguna atau pengguna root di dalam Anda Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA kapan API operasi dipanggil, tambahkan MFA kondisi ke kebijakan Anda. Untuk informasi selengkapnya, lihat APIAkses aman dengan MFA di Panduan IAM Pengguna.

Untuk informasi selengkapnya tentang praktik terbaik diIAM, lihat Praktik terbaik keamanan IAM di Panduan IAM Pengguna.

Menggunakan konsol Security Lake

Untuk mengakses konsol Amazon Security Lake, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Security Lake di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau. AWS API Sebagai gantinya, izinkan akses hanya ke tindakan yang cocok dengan API operasi yang mereka coba lakukan.

Untuk memastikan bahwa pengguna dan peran dapat menggunakan konsol Security Lake, buat IAM kebijakan yang memberi mereka akses konsol. Untuk informasi selengkapnya, lihat IAMidentitas di Panduan IAM Pengguna.

Jika Anda membuat kebijakan yang memungkinkan pengguna atau peran menggunakan konsol Security Lake, pastikan kebijakan tersebut menyertakan tindakan yang sesuai untuk sumber daya yang perlu diakses pengguna atau peran tersebut di konsol. Jika tidak, mereka tidak akan dapat menavigasi ke atau menampilkan detail tentang sumber daya tersebut di konsol.

Misalnya, untuk menambahkan sumber kustom menggunakan konsol, pengguna harus diizinkan untuk melakukan tindakan ini:

- `glue:CreateCrawler`
- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:StartCrawlerSchedule`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `iam:DeleteRolePolicy`
- `iam:PassRole`
- `lakeformation:RegisterResource`
- `lakeformation:GrantPermissions`
- `s3:ListBucket`
- `s3:PutObject`

Contoh: Izinkan pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara Anda membuat kebijakan yang memungkinkan IAM pengguna melihat kebijakan sebaris dan terkelola yang dilampirkan pada identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau secara terprogram menggunakan atau. AWS CLI AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh: Izinkan akun manajemen organisasi untuk menunjuk dan menghapus administrator yang didelegasikan

Contoh ini menunjukkan cara Anda membuat kebijakan yang memungkinkan pengguna akun AWS Organizations manajemen menunjuk dan menghapus administrator Security Lake yang didelegasikan untuk organisasi mereka.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "securitylake:RegisterDataLakeDelegatedAdministrator",
```

```
                "securitylake:DeregisterDataLakeDelegatedAdministrator"
            ],
            "Resource": "arn:aws:securitylake:*:*:*"
        }
    ]
}
```

Contoh: Izinkan pengguna untuk meninjau pelanggan berdasarkan tag

Dalam kebijakan berbasis identitas, Anda dapat menggunakan kondisi untuk mengontrol akses ke sumber daya Security Lake berdasarkan tag. Contoh ini menunjukkan cara Anda membuat kebijakan yang memungkinkan pengguna meninjau pelanggan dengan menggunakan konsol Security Lake atau Security LakeAPI. Namun, izin diberikan hanya jika nilai `Owner` tag untuk pelanggan adalah nama pengguna pengguna.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewSubscriberDetailsIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:GetSubscriber",
            "Resource": "arn:aws:securitylake:*:*:subscriber/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        },
        {
            "Sid": "ListSubscribersIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:ListSubscribers",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Dalam contoh ini, jika pengguna yang memiliki nama pengguna `richard-roe` mencoba meninjau detail pelanggan individu, pelanggan harus diberi tag `Owner=richard-roe` atau. `owner=richard-roe` Jika tidak, pengguna ditolak aksesnya. Kunci tag kondisi `Owner` cocok

dengan keduanya `0wner` dan `owner` karena nama kunci kondisi tidak peka huruf besar/kecil. Untuk informasi selengkapnya tentang menggunakan kunci kondisi, lihat elemen IAM JSON kebijakan: Kondisi dalam Panduan IAM Pengguna. Untuk informasi tentang menandai sumber daya Security Lake, lihatMenandai sumber daya Danau Keamanan.

AWS kebijakan terkelola untuk Security Lake

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau API operasi baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat kebijakan AWS terkelola di Panduan IAM Pengguna.

AWS kebijakan terkelola: AmazonSecurityLakeMetastoreManager

Amazon Security Lake menggunakan AWS Lambda fungsi untuk mengelola metadata di danau data Anda. Melalui penggunaan fungsi ini, Security Lake dapat mengindeks partisi Amazon Simple Storage Service (Amazon S3) yang berisi data dan file data Anda ke dalam AWS Glue tabel Data Catalog. Kebijakan terkelola ini berisi semua izin untuk fungsi Lambda untuk mengindeks partisi S3 dan file data ke dalam tabel. AWS Glue

Detail izin

Kebijakan ini mencakup izin berikut:

- `logs`— Memungkinkan kepala sekolah untuk mencatat output fungsi Lambda ke Amazon Logs. CloudWatch
- `glue`— Memungkinkan kepala sekolah untuk melakukan tindakan penulisan khusus untuk tabel Katalog AWS Glue Data. Ini juga memungkinkan AWS Glue crawler untuk mengidentifikasi partisi dalam data Anda.
- `sqs`— Memungkinkan kepala sekolah untuk melakukan tindakan baca dan tulis tertentu untuk SQS antrian Amazon yang mengirim pemberitahuan peristiwa saat objek ditambahkan atau diperbarui di danau data Anda.
- `s3`— Memungkinkan kepala sekolah melakukan tindakan baca dan tulis tertentu untuk bucket Amazon S3 yang berisi data Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowWriteLambdaLogs",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowGlueManage",
      "Effect": "Allow",
      "Action": [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
```

```
      ],
      "Resource": [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowToReadFromSqs",
      "Effect": "Allow",
      "Action": [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes"
      ],
      "Resource": [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowMetaDataReadWrite",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid": "AllowMetaDataCleanup",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

AWS kebijakan terkelola: AmazonSecurityLakePermissionsBoundary

Amazon Security Lake membuat IAM peran bagi sumber kustom pihak ketiga untuk menulis data ke data lake dan bagi pelanggan kustom pihak ketiga untuk menggunakan data dari data lake, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izin mereka. Anda tidak perlu mengambil tindakan untuk menggunakan kebijakan ini. Jika data lake dienkripsi dengan AWS KMS kunci yang dikelola pelanggan, `kms:Decrypt` dan `kms:GenerateDataKey` izin ditambahkan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowActionsForSecurityLake",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyActionsForSecurityLake",
      "Effect": "Deny",
      "NotAction": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeBucket",
      "Effect": "Deny",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
```

```
      "NotResource": [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeSQS",
      "Effect": "Deny",
      "Action": [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "NotResource": "arn:aws:sqs:*:*:AmazonSecurityLake*"
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeKMSS3SQS",
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotLike": {
          "kms:ViaService": [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeKMSForS3",
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
```

```
        "Null": {
          "kms:EncryptionContext:aws:s3:arn": "false"
        },
        "StringNotLikeIfExists": {
          "kms:EncryptionContext:aws:s3:arn": [
            "arn:aws:s3:::aws-security-data-lake*"
          ]
        }
      }
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeKMSForS3SQS",
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "kms:EncryptionContext:aws:sqs:arn": "false"
        },
        "StringNotLikeIfExists": {
          "kms:EncryptionContext:aws:sqs:arn": [
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
        }
      }
    }
  ]
}
```

AWS kebijakan terkelola: AmazonSecurityLakeAdministrator

Anda dapat melampirkan `AmazonSecurityLakeAdministrator` kebijakan ke kepala sekolah sebelum mengaktifkan Amazon Security Lake untuk akun mereka. Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh utama ke semua tindakan Security Lake. Kepala sekolah kemudian dapat naik ke Security Lake dan kemudian mengkonfigurasi sumber dan pelanggan di Security Lake.

Kebijakan ini mencakup tindakan yang dapat dilakukan administrator Security Lake pada AWS layanan lain melalui Security Lake.

`AmazonSecurityLakeAdministrator`Kebijakan ini tidak mendukung pembuatan peran utilitas yang diperlukan oleh Security Lake untuk mengelola replikasi lintas wilayah Amazon S3, pendaftaran partisi data baru, AWS Glue menjalankan crawler Glue pada data yang ditambahkan ke sumber kustom, atau memberi tahu HTTPS pelanggan titik akhir tentang data baru. Anda dapat membuat peran ini sebelumnya seperti yang dijelaskan dalamMemulai dengan Amazon Security Lake.

Selain kebijakan `AmazonSecurityLakeAdministrator` terkelola, Security Lake memerlukan `lakeformation:PutDataLakeSettings` izin untuk fungsi orientasi dan konfigurasi. `PutDataLakeSettings`memungkinkan pengaturan IAM kepala sekolah sebagai administrator untuk semua sumber daya Lake Formation regional di akun. Peran ini harus dimiliki `iam:CreateRole permission` serta `AmazonSecurityLakeAdministrator` kebijakan yang melekat padanya.

Administrator Lake Formation memiliki akses penuh ke konsol Lake Formation, dan mengontrol konfigurasi data awal dan izin akses. Security Lake menetapkan prinsipal yang memungkinkan Security Lake dan `AmazonSecurityLakeMetaStoreManager` peran (atau peran tertentu lainnya) sebagai administrator Lake Formation sehingga mereka dapat membuat tabel, memperbarui skema tabel, mendaftarkan partisi baru, dan mengonfigurasi izin pada tabel. Anda harus menyertakan izin berikut dalam kebijakan untuk pengguna atau peran administrator Security Lake:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPutLakeFormationSettings",
            "Effect": "Allow",
            "Action": "lakeformation:PutDatalakeSettings",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": "securitylake.amazonaws.com"
                }
            }
        }
    ]
}
```

Detail izin

Kebijakan ini mencakup izin berikut.

- `securitylake`— Memungkinkan kepala sekolah akses penuh ke semua tindakan Security Lake.
- `organizations`— Memungkinkan kepala sekolah untuk mengambil informasi dari Organizations tentang akun dalam suatu AWS organisasi. Jika akun milik organisasi, maka izin ini memungkinkan konsol Security Lake menampilkan nama akun dan nomor akun.
- `iam`— Memungkinkan kepala sekolah untuk membuat peran terkait layanan untuk Security Lake,, dan AWS Lake Formation Amazon EventBridge, sebagai langkah yang diperlukan saat mengaktifkan layanan tersebut. Juga memungkinkan pembuatan dan pengeditan kebijakan untuk peran pelanggan dan sumber kustom, dengan izin peran tersebut terbatas pada apa yang diizinkan oleh kebijakan. `AmazonSecurityLakePermissionsBoundary`
- `ram`— Memungkinkan kepala sekolah untuk mengonfigurasi akses kueri Lake Formation berbasis oleh pelanggan ke sumber Security Lake.
- `s3`— Memungkinkan kepala sekolah untuk membuat dan mengelola ember Security Lake, dan membaca isi ember tersebut.
- `lambda`— Memungkinkan prinsipal untuk mengelola yang Lambda digunakan untuk memperbarui partisi AWS Glue tabel setelah pengiriman AWS sumber dan replikasi lintas wilayah.
- `glue`— Memungkinkan kepala sekolah untuk membuat dan mengelola database dan tabel Security Lake.
- `lakeformation`— Memungkinkan kepala sekolah untuk mengelola Lake Formation izin untuk tabel Security Lake.
- `events`— Memungkinkan kepala sekolah untuk mengelola aturan yang digunakan untuk memberi tahu pelanggan tentang data baru di sumber Security Lake.
- `sqs`— Memungkinkan kepala sekolah untuk membuat dan mengelola Amazon SQS antrian yang digunakan untuk memberi tahu pelanggan tentang data baru di sumber Security Lake.
- `kms`— Memungkinkan kepala sekolah memberikan akses ke Security Lake untuk menulis data menggunakan kunci yang dikelola pelanggan.
- `secretsmanager`— Memungkinkan kepala sekolah untuk mengelola rahasia yang digunakan untuk memberi tahu pelanggan tentang data baru di sumber Security Lake melalui titik akhir. HTTPS

```
{
"Version": "2012-10-17",
```

```
"Statement": [
  {
    "Sid": "AllowActionsWithAnyResource",
    "Effect": "Allow",
    "Action": [
      "securitylake:*",
      "organizations:DescribeOrganization",
      "organizations:ListDelegatedServicesForAccount",
      "organizations:ListAccounts",
      "iam:ListRoles",
      "ram:GetResourceShareAssociations"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AllowActionsWithAnyResourceViaSecurityLake",
    "Effect": "Allow",
    "Action": [
      "glue:CreateCrawler",
      "glue:StopCrawlerSchedule",
      "lambda:CreateEventSourceMapping",
      "lakeformation:GrantPermissions",
      "lakeformation:ListPermissions",
      "lakeformation:RegisterResource",
      "lakeformation:RevokePermissions",
      "lakeformation:GetDatalakeSettings",
      "events:ListConnections",
      "events:ListApiDestinations",
      "iam:GetRole",
      "iam:ListAttachedRolePolicies",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowManagingSecurityLakeS3Buckets",
    "Effect": "Allow",
    "Action": [
      "s3:CreateBucket",
```

```
      "s3:PutBucketPolicy",
      "s3:PutBucketPublicAccessBlock",
      "s3:PutBucketNotification",
      "s3:PutBucketTagging",
      "s3:PutEncryptionConfiguration",
      "s3:PutBucketVersioning",
      "s3:PutReplicationConfiguration",
      "s3:PutLifecycleConfiguration",
      "s3:ListBucket",
      "s3:PutObject",
      "s3:GetBucketNotification"
    ],
    "Resource": "arn:aws:s3:::aws-security-data-lake*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowLambdaCreateFunction",
    "Effect": "Allow",
    "Action": [
      "lambda:CreateFunction"
    ],
    "Resource": [
      "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowLambdaAddPermission",
    "Effect": "Allow",
    "Action": [
      "lambda:AddPermission"
    ],
    "Resource": [
      "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
```

```
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      },
      "StringEquals": {
        "lambda:Principal": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowGlueActions",
    "Effect": "Allow",
    "Action": [
      "glue:CreateDatabase",
      "glue:GetDatabase",
      "glue:CreateTable",
      "glue:GetTable"
    ],
    "Resource": [
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
      "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowEventBridgeActions",
    "Effect": "Allow",
    "Action": [
      "events:PutTargets",
      "events:PutRule",
      "events:DescribeRule",
      "events:CreateApiDestination",
      "events:CreateConnection",
      "events:UpdateConnection",
      "events:UpdateApiDestination",
      "events:DeleteConnection",
      "events:DeleteApiDestination",
      "events:ListTargetsByRule",
```

```
      "events:RemoveTargets",
      "events:DeleteRule"
    ],
    "Resource": [
      "arn:aws:events:*:*:rule/AmazonSecurityLake*",
      "arn:aws:events:*:*:rule/SecurityLake*",
      "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
      "arn:aws:events:*:*:connection/AmazonSecurityLake*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowSQSActions",
    "Effect": "Allow",
    "Action": [
      "sqs:CreateQueue",
      "sqs:SetQueueAttributes",
      "sqs:GetQueueURL",
      "sqs:AddPermission",
      "sqs:GetQueueAttributes",
      "sqs:DeleteQueue"
    ],
    "Resource": [
      "arn:aws:sqs:*:*:SecurityLake*",
      "arn:aws:sqs:*:*:AmazonSecurityLake*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowKmsCmkGrantForSecurityLake",
    "Effect": "Allow",
    "Action": "kms:CreateGrant",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
```

```
      },
      "StringLike": {
        "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::aws-security-data-lake*"
      },
      "ForAllValues:StringEquals": {
        "kms:GrantOperations": [
          "GenerateDataKey",
          "RetireGrant",
          "Decrypt"
        ]
      }
    }
  },
  {
    "Sid": "AllowEnablingQueryBasedSubscribers",
    "Effect": "Allow",
    "Action": [
      "ram:CreateResourceShare",
      "ram:AssociateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
      "StringLikeIfExists": {
        "ram:ResourceArn": [
          "arn:aws:glue:*:*:catalog",
          "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
          "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
        ]
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowConfiguringQueryBasedSubscribers",
    "Effect": "Allow",
    "Action": [
      "ram:UpdateResourceShare",
      "ram:GetResourceShares",
      "ram:DisassociateResourceShare",
      "ram:DeleteResourceShare"
    ],
    "Resource": "*",
```

```
    "Condition": {
      "StringLike": {
        "ram:ResourceShareName": "LakeFormation*"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowConfiguringCredentialsForSubscriberNotification",
    "Effect": "Allow",
    "Action": [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager:PutSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "lambda.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
```

```
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "lambda.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": [
          "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
          "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
        ]
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCrossRegionReplicationSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "s3.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCrossRegionReplicationS3Arn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "s3.amazonaws.com"
      },
```

```
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:s3:::aws-security-data-lake*"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "glue.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCustomSourceCrawlerGlueArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "glue.amazonaws.com"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForSubscriberNotificationSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
```

```
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "events.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:subscriber/*"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForSubscriberNotificationEventsArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "events.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:events:*:*:rule/AmazonSecurityLake*"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowOnboardingToSecurityLakeDependencies",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": [
      "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
      "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
      "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
    ],
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": [
          "securitylake.amazonaws.com",
          "lakeformation.amazonaws.com",
```

```
          "apidestinations.events.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "AllowRolePolicyActionsforSubscibersandSources",
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam:PutRolePolicy",
      "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/AmazonSecurityLake*",
    "Condition": {
      "StringEquals": {
        "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowRegisterS3LocationInLakeFormation",
    "Effect": "Allow",
    "Action": [
      "iam:PutRolePolicy",
      "iam:GetRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowIAMActionsByResource",
    "Effect": "Allow",
    "Action": [
      "iam:ListRolePolicies",
```

```
      "iam:DeleteRole"
    ],
    "Resource": "arn:aws:iam::*:role/AmazonSecurityLake*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "S3ReadAccessToSecurityLakes",
    "Effect": "Allow",
    "Action": [
      "s3:Get*",
      "s3:List*"
    ],
    "Resource": "arn:aws:s3:::aws-security-data-lake-*"
  },
  {
    "Sid": "S3ReadAccessToSecurityLakeMetastoreObject",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::security-lake-meta-store-manager-*"
  },
  {
    "Sid": "S3ResourcelessReadOnly",
    "Effect": "Allow",
    "Action": [
      "s3:GetAccountPublicAccessBlock",
      "s3:ListAccessPoints",
      "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
  }
]
}
```

AWS kebijakan terkelola: SecurityLakeServiceLinkedRole

Security Lake menggunakan peran terkait layanan bernama `AWSServiceRoleForSecurityLake` untuk membuat dan mengoperasikan danau data keamanan.

Anda tidak dapat melampirkan kebijakan `SecurityLakeServiceLinkedRole` terkelola ke IAM entitas Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Security Lake untuk melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Izin peran terkait layanan untuk Security Lake.

AWS kebijakan terkelola: SecurityLakeResourceManagementServiceRolePolicy

Security Lake menggunakan peran terkait layanan yang disebutkan `AWSServiceRoleForSecurityLakeResourceManagement` untuk melakukan pemantauan berkelanjutan dan peningkatan kinerja, yang dapat mengurangi latensi dan biaya.

Anda tidak dapat melampirkan kebijakan `SecurityLakeResourceManagementServiceRolePolicy` terkelola ke IAM entitas Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Security Lake untuk melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Izin peran terkait layanan untuk pengelolaan sumber daya.

AWS kebijakan terkelola: AWS GlueServiceRole

Kebijakan `AWS GlueServiceRole` terkelola memanggil AWS Glue crawler dan mengizinkan AWS Glue untuk meng-crawl data sumber kustom dan mengidentifikasi metadata partisi. Metadata ini diperlukan untuk membuat dan memperbarui tabel di Katalog Data.

Untuk informasi selengkapnya, lihat Mengumpulkan data dari sumber khusus di Security Lake.

Security Lake memperbarui kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Security Lake sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan RSS umpan di halaman riwayat Dokumen Security Lake.

Perubahan	Deskripsi	Tanggal
Peran terkait layanan untuk Amazon Security Lake — Peran terkait layanan baru	Kami menambahkan peran terkait layanan baru. `AWSServiceRoleForSecurityLakeResourceManagement` Peran terkait layanan ini memberikan izin kepada Security Lake untuk melakukan pemantauan berkelanjutan dan peningkatan kinerja, yang dapat mengurangi latensi dan biaya.	November 14, 2024
Peran terkait layanan untuk Amazon Security Lake - Perbarui ke izin peran terkait layanan yang ada	Kami menambahkan AWS WAF tindakan ke kebijakan AWS terkelola untuk `SecurityLakeServiceLinkedRole` kebijakan tersebut. Tindakan tambahan memungkinkan Security Lake untuk mengumpulkan AWS WAF log, ketika diaktifkan sebagai sumber log di Security Lake.	22 Mei 2024
AmazonSecurityLakePermissionsBoundary – Pembaruan ke kebijakan yang ada	Security Lake menambahkan SID tindakan ke kebijakan tersebut.	13 Mei 2024
AmazonSecurityLakeMetastoreManager – Pembaruan ke kebijakan yang ada	Security Lake memperbarui kebijakan untuk menambahkan tindakan pembersihan metadata yang memungkinkan Anda menghapus metadata di data lake Anda.	Maret 27, 2024

Perubahan	Deskripsi	Tanggal
AmazonSecurityLake Administrator – Pembaruan ke kebijakan yang ada	Security Lake memperbarui kebijakan untuk mengizinkan `iam:PassRole AmazonSecurityLakeMetastoreManagerV2` peran baru dan memungkinkan Security Lake menyebarkan atau memperbarui komponen data lake.	Februari 23, 2024
AmazonSecurityLake MetastoreManager – Kebijakan baru	Security Lake menambahkan kebijakan terkelola baru yang memberikan izin kepada Security Lake untuk mengelola metadata di data lake Anda.	23 Januari 2024
AmazonSecurityLakeAdministrator – Kebijakan baru	Security Lake menambahkan kebijakan terkelola baru yang memberikan akses penuh utama ke semua tindakan Security Lake.	30 Mei 2023
Security Lake mulai melacak perubahan	Security Lake mulai melacak perubahan untuk kebijakan yang AWS dikelola.	29 November 2022

Menggunakan peran terkait layanan untuk Security Lake

Security Lake menggunakan AWS Identity and Access Management (IAM) peran terkait layanan. Peran terkait layanan adalah IAM peran yang terkait langsung dengan Security Lake. Ini telah ditentukan sebelumnya oleh Security Lake, dan itu mencakup semua izin yang diperlukan Security Lake untuk memanggil orang lain Layanan AWS atas nama Anda dan mengoperasikan layanan danau data keamanan. Security Lake menggunakan peran terkait layanan ini di semua Wilayah AWS tempat Danau Keamanan tersedia.

Peran terkait layanan menghilangkan kebutuhan untuk menambahkan izin yang diperlukan secara manual saat menyiapkan Security Lake. Security Lake mendefinisikan izin peran terkait layanan ini, dan kecuali ditentukan lain, hanya Security Lake yang dapat mengambil peran tersebut. Izin yang ditetapkan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas lain. IAM

Anda harus mengonfigurasikan izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, menyunting, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran terkait layanan di Panduan Pengguna. IAM Anda dapat menghapus peran terkait layanan hanya setelah menghapus sumber daya terkait. Ini melindungi sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWS layanan yang bekerja dengan IAM dan cari layanan yang memiliki Ya di kolom Peran terkait layanan. Pilih Ya dengan tautan untuk meninjau dokumentasi peran terkait layanan untuk layanan tersebut.

Topik

- Izin peran terkait layanan untuk Security Lake
- Izin peran terkait layanan untuk manajemen sumber daya

Izin peran terkait layanan untuk Security Lake

Security Lake menggunakan peran terkait layanan bernama. `AWSServiceRoleForSecurityLake` Peran terkait layanan ini mempercayai `securitylake.amazonaws.com` layanan untuk mengambil peran tersebut. Untuk informasi selengkapnya tentang, kebijakan AWS terkelola untuk Amazon Security Lake, lihat AWS mengelola kebijakan untuk Amazon Security Lake.

Kebijakan izin untuk peran tersebut, yang merupakan kebijakan AWS terkelola bernama`SecurityLakeServiceLinkedRole`, memungkinkan Security Lake membuat dan mengoperasikan data lake keamanan. Ini juga memungkinkan Security Lake untuk melakukan tugas-tugas seperti berikut pada sumber daya yang ditentukan:

- Gunakan AWS Organizations tindakan untuk mengambil informasi tentang akun terkait
- Gunakan Amazon Elastic Compute Cloud (AmazonEC2) untuk mengambil informasi tentang Amazon Flow Logs VPC
- Menggunakan AWS CloudTrail tindakan untuk mengambil informasi tentang peran terkait layanan

- Gunakan AWS WAF tindakan untuk mengumpulkan AWS WAF log, saat diaktifkan sebagai sumber log di Security Lake
- Gunakan `LogDelivery` tindakan untuk membuat atau menghapus langganan pengiriman AWS WAF log.

Peran dikonfigurasi dengan kebijakan izin berikut:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "OrganizationsPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeOrganization"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "DescribeOrgAccounts",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount"
            ],
            "Resource": [
                "arn:aws:organizations::*:account/o-*/*"
            ]
        },
        {
            "Sid": "AllowManagementOfServiceLinkedChannel",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateServiceLinkedChannel",
                "cloudtrail:DeleteServiceLinkedChannel",
                "cloudtrail:GetServiceLinkedChannel",
                "cloudtrail:UpdateServiceLinkedChannel"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-
lake/*"
        },
```

```
        {
            "Sid": "AllowListServiceLinkedChannel",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:ListServiceLinkedChannels"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DescribeAnyVpc",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListDelegatedAdmins",
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "securitylake.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowWafLoggingConfiguration",
            "Effect": "Allow",
            "Action": [
                "wafv2:PutLoggingConfiguration",
                "wafv2:GetLoggingConfiguration",
                "wafv2:ListLoggingConfigurations",
                "wafv2:DeleteLoggingConfiguration"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "wafv2:LogScope": "SecurityLake"
                }
            }
```

```
        },
        {
            "Sid": "AllowPutLoggingConfiguration",
            "Effect": "Allow",
            "Action": [
                "wafv2:PutLoggingConfiguration"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-
security-lake-*"
                }
            }
        },
        {
            "Sid": "ListWebACLs",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs"
            ],
            "Resource": "*"
        },
        {
            "Sid": "LogDelivery",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": [
                        "wafv2.amazonaws.com"
                    ]
                }
            }
        }

    ]
}
```

Anda harus mengonfigurasikan izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, menyunting, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran terkait layanan di Panduan Pengguna. IAM

Membuat peran terkait layanan Security Lake

Anda tidak perlu membuat peran `AWSServiceRoleForSecurityLake` terkait layanan untuk Security Lake secara manual. Saat Anda mengaktifkan Security Lake untuk Anda Akun AWS, Security Lake secara otomatis membuat peran terkait layanan untuk Anda.

Mengedit peran terkait layanan Security Lake

Security Lake tidak mengizinkan Anda mengedit peran `AWSServiceRoleForSecurityLake` terkait layanan. Setelah peran terkait layanan dibuat, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting deskripsi peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan di IAMPanduan Pengguna.

Menghapus peran terkait layanan Security Lake

Anda tidak dapat menghapus peran terkait layanan dari Security Lake. Sebagai gantinya, Anda dapat menghapus peran terkait layanan dari IAM konsol,API, atau. AWS CLIUntuk informasi selengkapnya, lihat Menghapus peran terkait layanan di Panduan Pengguna. IAM

Sebelum dapat menghapus peran terkait layanan, Anda harus terlebih dahulu mengonfirmasi bahwa peran tersebut tidak memiliki sesi aktif dan menghapus sumber daya apa pun yang `AWSServiceRoleForSecurityLake` digunakan.

> **Note**
>
> Jika Security Lake menggunakan `AWSServiceRoleForSecurityLake` peran saat Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika itu terjadi, tunggu beberapa menit dan kemudian coba operasi lagi.

Jika Anda menghapus peran `AWSServiceRoleForSecurityLake` terkait layanan dan perlu membuatnya lagi, Anda dapat membuatnya lagi dengan mengaktifkan Security Lake untuk akun Anda. Saat Anda mengaktifkan Security Lake lagi, Security Lake secara otomatis membuat peran terkait layanan lagi untuk Anda.

Didukung Wilayah AWS untuk peran terkait layanan Security Lake

Security Lake mendukung penggunaan peran `AWSServiceRoleForSecurityLake` terkait layanan di semua Wilayah AWS tempat Security Lake tersedia. Untuk daftar Wilayah di mana Danau Keamanan saat ini tersedia, lihatWilayah Danau Keamanan dan titik akhir.

Izin peran terkait layanan untuk manajemen sumber daya

Security Lake menggunakan peran terkait layanan yang disebutkan `AWSServiceRoleForSecurityLakeResourceManagement` untuk melakukan pemantauan berkelanjutan dan peningkatan kinerja, yang dapat mengurangi latensi dan biaya. Peran terkait layanan ini mempercayai `resource-management.securitylake.amazonaws.com` layanan untuk mengambil peran tersebut. Mengaktifkan juga `AWSServiceRoleForSecurityLakeResourceManagement` akan memberinya akses ke Lake Formation dan secara otomatis mendaftarkan bucket S3 terkelola Security Lake Anda dengan Lake Formation di semua Wilayah untuk meningkatkan keamanan.

Kebijakan izin untuk peran, yang merupakan kebijakan AWS terkelola bernama`SecurityLakeResourceManagementServiceRolePolicy`, memungkinkan akses untuk mengelola sumber daya yang dibuat oleh Security Lake; termasuk mengelola metadata di data lake Anda. Untuk informasi selengkapnya tentang, kebijakan AWS terkelola untuk Amazon Security Lake, lihat kebijakan AWS terkelola untuk Amazon Security Lake.

Peran terkait layanan ini memungkinkan Security Lake memantau kesehatan sumber daya yang digunakan oleh Security Lake (S3 Bucket AWS Glue , tables, Amazon SQS Queue, Metastore Manager (MSM) Lambda Function, dan aturan) ke akun Anda. EventBridge Beberapa contoh operasi yang dapat dilakukan Security Lake dengan peran terkait layanan ini adalah:

- Pemadatan file manifes Apache Iceberg, yang meningkatkan kinerja kueri dan menurunkan waktu dan biaya pemrosesan Lambda. MSM
- Pantau status Amazon SQS untuk mendeteksi masalah konsumsi.
- Optimalkan replikasi data lintas wilayah untuk mengecualikan file metadata.

> **Note**
>
> Jika Anda tidak menginstal peran `AWSServiceRoleForSecurityLakeResourceManagement` terkait layanan, Security

Lake akan terus berfungsi tetapi sangat disarankan untuk menerima peran terkait layanan ini sehingga Security Lake dapat memantau dan mengoptimalkan sumber daya di akun Anda.

Detail izin

Peran dikonfigurasi dengan kebijakan izin berikut:

- `events`— Memungkinkan kepala sekolah untuk mengelola EventBridge aturan yang diperlukan untuk sumber log dan log pelanggan.
- `lambda`— Memungkinkan prinsipal untuk mengelola lambda yang digunakan untuk memperbarui partisi AWS Glue tabel setelah pengiriman AWS sumber dan replikasi lintas wilayah.
- `glue`— Memungkinkan kepala sekolah untuk melakukan tindakan penulisan khusus untuk tabel Katalog AWS Glue Data. Ini juga memungkinkan AWS Glue crawler untuk mengidentifikasi partisi dalam data Anda, dan memungkinkan Security Lake mengelola metadata Apache Iceberg untuk tabel Apache Iceberg Anda.
- `s3`— Memungkinkan kepala sekolah untuk melakukan tindakan baca dan tulis tertentu pada bucket Security Lake yang berisi data log dan metadata tabel Glue.
- `logs`— Memungkinkan akses baca kepala sekolah untuk mencatat output fungsi Lambda ke Log. CloudWatch
- `sqs`— Memungkinkan kepala sekolah untuk melakukan tindakan baca dan tulis tertentu untuk SQS antrian Amazon yang menerima pemberitahuan peristiwa saat objek ditambahkan atau diperbarui di danau data Anda.
- `lakeformation`— Memungkinkan kepala sekolah membaca pengaturan Lake Formation untuk memantau kesalahan konfigurasi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadEventBridgeRules",
      "Effect": "Allow",
      "Action": [
        "events:ListRules"
      ],
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "ManageSecurityLakeEventRules",
      "Effect": "Allow",
      "Action": [
        "events:PutRule"
      ],
      "Resource": "arn:aws:events:*:*:rule/AmazonSecurityLake-*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "ManageSecurityLakeLambdaConfigurations",
      "Effect": "Allow",
      "Action": [
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:PutFunctionConcurrency",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetRuntimeManagementConfig",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:PublishVersion",
        "lambda:DeleteFunctionConcurrency",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetAlias",
        "lambda:GetPolicy",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource": [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition": {
        "StringEquals": {
```

```
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowListLambdaEventSourceMappings",
      "Effect": "Allow",
      "Action": [
        "lambda:ListEventSourceMappings"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowUpdateLambdaEventSourceMapping",
      "Effect": "Allow",
      "Action": [
        "lambda:UpdateEventSourceMapping"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        },
        "StringLike": {
          "lambda:FunctionArn":
"arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
        }
      }
    },
    {
      "Sid": "AllowUpdateLambdaConfigs",
      "Effect": "Allow",
      "Action": [
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource": "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid": "ManageSecurityLakeGlueResources",
      "Effect": "Allow",
      "Action": [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:GetTables",
        "glue:UpdateTable",
        "glue:GetDatabase"
      ],
      "Resource": [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowDataLakeConfigurationManagement",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObjectAttributes",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetEncryptionConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition": {
        "StringEquals": {
```

```
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowMetaDataCompactionAndManagement",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:RestoreObject"
      ],
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "ReadSecurityLakeLambdaLogs",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetQueryResults",
        "logs:GetLogRecord"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "ManageSecurityLakeSQSQueue",
      "Effect": "Allow",
```

```
      "Action": [
        "sqs:StartMessageMoveTask",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ChangeMessageVisibility",
        "sqs:ListMessageMoveTasks",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes"
      ],
      "Resource": [
        "arn:aws:sqs:*:*:SecurityLake_*",
        "arn:aws:sqs:*:*:AmazonSecurityLakeManager-*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowDataLakeManagement",
      "Effect": "Allow",
      "Action": [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Anda harus mengonfigurasikan izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, menyunting, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran terkait layanan di Panduan Pengguna. IAM

Membuat peran terkait layanan Security Lake

Anda dapat membuat peran `AWSServiceRoleForSecurityLakeResourceManagement` terkait layanan untuk Security Lake menggunakan konsol Security Lake atau. AWS CLI

Untuk membuat peran terkait layanan, Anda harus memberikan izin berikut kepada IAM pengguna atau peran Anda. IAM IAMPeran tersebut harus menjadi administrator Lake Formation di semua Wilayah yang diaktifkan Danau Keamanan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowLakeFormationActionsViaSecurityLakeConsole",
      "Effect": "Allow",
      "Action": [
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowIamActionsViaSecurityLakeConsole",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:PutRolePolicy"
      ],
      "Resource": [
        "arn:*:iam::*:role/aws-service-role/resource-
management.securitylake.amazonaws.com/AWSServiceRoleForSecurityLakeResourceManagement",
        "arn:*:iam::*:role/*AWSServiceRoleForLakeFormationDataAccess",
        "arn:*:iam::aws:policy/service-role/AWSGlueServiceRole",
        "arn:*:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager",
        "arn:*:iam::aws:policy/aws-service-role/
SecurityLakeResourceManagementServiceRolePolicy"
      ],
      "Condition": {
```

```
        "StringLikeIfExists": {
          "iam:AWSServiceName": [
            "securitylake.amazonaws.com",
            "resource-management.securitylake.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowGlueActionsViaConsole",
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabase",
        "glue:GetTables"
      ],
      "Resource": [
        "arn:*:glue:*:*:catalog",
        "arn:*:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:*:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ]
    }
  ]
}
```

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Terima peran terkait layanan baru dengan mengklik Aktifkan peran terkait layanan di bilah informasi di halaman Ringkasan.

Setelah Anda mengaktifkan peran terkait layanan, Anda tidak perlu mengulangi proses ini untuk penggunaan Security Lake di masa mendatang.

CLI

Untuk membuat peran `AWSServiceRoleForSecurityLakeResourceManagement` terkait layanan secara terprogram, gunakan perintah berikut. CLI

```
$ aws iam create-service-linked-role
--aws-service-name resource-management.securitylake.amazonaws.com
```

Saat membuat peran `AWSServiceRoleForSecurityLakeResourceManagement` terkait layanan menggunakan AWS CLI, Anda juga harus memberikannya izin tingkat tabel Lake Formation (ALTER,DESCRIBE) ke semua tabel pada database Security Lake Glue untuk mengelola metadata tabel dan mengakses data. Jika tabel Glue di wilayah mana pun mereferensikan bucket S3 dari pengaktifan Security Lake sebelumnya, Anda harus mengizinkan ACCESS izin DATA _ LOCATION _ untuk sementara ke peran terkait layanan untuk memungkinkan Security Lake memperbaiki situasi ini.

Anda juga harus memberikan izin Lake Formation ke peran `AWSServiceRoleForSecurityLakeResourceManagement` terkait layanan untuk akun Anda.

Contoh berikut menunjukkan cara memberikan izin Lake Formation ke peran terkait layanan di Wilayah yang ditunjuk. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws lakeformation grant-permissions --region {region} --principal
 DataLakePrincipalIdentifier={AWSServiceRoleForSecurityLakeResourceManagement ARN} \
--permissions ALTER DESCRIBE --resource '{ "Table": { "DatabaseName":
 "amazon_security_lake_glue_db_{region}", "TableWildcard": {} } }'
```

Contoh berikut menunjukkan bagaimana Peran ARN akan terlihat seperti. Anda harus mengedit Peran ARN agar sesuai dengan Wilayah Anda.

```
"AWS": "arn:[partition]:iam::[accountid]:role/aws-service-
role/resource-management.securitylake.amazonaws.com/
AWSServiceRoleForSecurityLakeResourceManagement"
```

Anda juga dapat menggunakan CreateServiceLinkedRoleAPIpanggilan. Dalam permintaan, tentukan `AWSServiceName` sebagai`resource-management.securitylake.amazonaws.com`.

Setelah mengaktifkan `AWSServiceRoleForSecurityLakeResourceManagement` peran, jika Anda menggunakan AWS KMS Customer Managed Key (CMK) untuk enkripsi, Anda harus mengizinkan peran terkait layanan untuk menulis objek terenkripsi ke bucket S3 di Wilayah yang ada. AWS CMK Di AWS KMS konsol, tambahkan kebijakan berikut ke KMS kunci di AWS Wilayah tempat CMK ada. Untuk detail tentang cara mengubah kebijakan KMS utama, lihat Kebijakan utama AWS KMS di Panduan AWS Key Management Service Pengembang.

```
{
```

```
    "Sid": "Allow SLR",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:[partition]:iam::[accountid]:role/aws-service-role/resource-
management.securitylake.amazonaws.com/AWSServiceRoleForSecurityLakeResourceManagement"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::[regional-datalake-s3-
bucket-name]"
        },
        "StringLike": {
            "kms:ViaService": "s3.[region].amazonaws.com"
        }
    }
},
```

Mengedit peran terkait layanan Security Lake

Security Lake tidak mengizinkan Anda mengedit peran `AWSServiceRoleForSecurityLakeResourceManagement` terkait layanan. Setelah peran terkait layanan dibuat, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting deskripsi peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan di IAMPanduan Pengguna.

Menghapus peran terkait layanan Security Lake

Anda tidak dapat menghapus peran terkait layanan dari Security Lake. Sebagai gantinya, Anda dapat menghapus peran terkait layanan dari IAM konsol,API, atau. AWS CLIUntuk informasi selengkapnya, lihat Menghapus peran terkait layanan di Panduan Pengguna. IAM

Sebelum dapat menghapus peran terkait layanan, Anda harus terlebih dahulu mengonfirmasi bahwa peran tersebut tidak memiliki sesi aktif dan menghapus sumber daya apa pun yang `AWSServiceRoleForSecurityLakeResourceManagement` digunakan.

> **Note**
>
> Jika Security Lake menggunakan `AWSServiceRoleForSecurityLakeResourceManagement` peran saat Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika itu terjadi, tunggu beberapa menit dan kemudian coba operasi lagi.

Jika Anda menghapus peran `AWSServiceRoleForSecurityLakeResourceManagement` terkait layanan dan perlu membuatnya lagi, Anda dapat membuatnya lagi dengan mengaktifkan Security Lake untuk akun Anda. Saat Anda mengaktifkan Security Lake lagi, Security Lake secara otomatis membuat peran terkait layanan lagi untuk Anda.

Didukung Wilayah AWS untuk peran terkait layanan Security Lake

Security Lake mendukung penggunaan peran `AWSServiceRoleForSecurityLakeResourceManagement` terkait layanan di semua Wilayah AWS tempat Security Lake tersedia. Untuk daftar Wilayah di mana Danau Keamanan saat ini tersedia, lihatWilayah Danau Keamanan dan titik akhir.

Perlindungan data di Amazon Security Lake

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon Security Lake. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat Privasi Data FAQ. Untuk informasi tentang perlindungan data di Eropa, lihat Model Tanggung Jawab AWS Bersama dan posting GDPR blog di Blog AWS Keamanan.

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management ()IAM. Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan otentikasi multi-faktor (MFA) dengan setiap akun.

- GunakanSSL/TLSuntuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atau, gunakan titik akhir. API FIPS Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat Federal Information Processing Standard (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan Security Lake atau lainnya Layanan AWS menggunakan konsol,API, AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar Anda tidak menyertakan informasi kredensil dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

Enkripsi diam

Amazon Security Lake menyimpan data Anda dengan aman menggunakan solusi AWS enkripsi. Log keamanan mentah dan data peristiwa disimpan dalam bucket Simple Storage Service (Amazon S3) multi-tenant di akun yang dikelola Security Lake. Security Lake mengenkripsi data mentah ini menggunakan kunci AWS milik from AWS Key Management Service ()AWS KMS. AWS kunci yang dimiliki adalah kumpulan AWS KMS kunci yang dimiliki AWS layanan—dalam hal ini Security Lake—memiliki dan mengelola untuk digunakan di beberapa akun. AWS

Security Lake menjalankan tugas ekstrak, transformasi, dan load (ETL) pada log mentah dan data peristiwa. Data yang diproses tetap dienkripsi di akun layanan Security Lake.

Setelah ETL pekerjaan selesai, Security Lake membuat bucket S3 penyewa tunggal di akun Anda (satu ember untuk masing-masing Wilayah AWS tempat Anda mengaktifkan Security Lake). Data disimpan dalam bucket S3 multi-tenant hanya sementara sampai Security Lake dapat mengirimkan

data dengan andal ke bucket S3 penyewa tunggal. Bucket penyewa tunggal menyertakan kebijakan berbasis sumber daya yang memberikan izin Security Lake untuk menulis data log dan peristiwa ke bucket. Untuk mengenkripsi data di bucket S3, Anda dapat memilih kunci enkripsi terkelola S3 atau kunci yang dikelola pelanggan (dari). AWS KMS Kedua opsi menggunakan enkripsi simetris.

Menggunakan KMS kunci untuk enkripsi data Anda

Secara default, data yang dikirimkan oleh Security Lake ke bucket S3 Anda dienkripsi oleh enkripsi sisi server Amazon dengan kunci enkripsi yang dikelola Amazon S3 (-S3). SSE Untuk menyediakan lapisan keamanan yang Anda kelola secara langsung, Anda dapat menggunakan enkripsi sisi server dengan AWS KMS kunci (SSE-KMS) untuk data Security Lake Anda.

SSE- KMS tidak didukung di konsol Security Lake. Untuk menggunakan SSE - KMS dengan Security Lake API atauCLI, Anda terlebih dahulu membuat KMS kunci atau menggunakan kunci yang ada. Anda melampirkan kebijakan ke kunci yang menentukan pengguna mana yang dapat menggunakan kunci untuk mengenkripsi dan mendekripsi data Security Lake.

Jika Anda menggunakan kunci terkelola pelanggan untuk mengenkripsi data yang ditulis ke bucket S3, Anda tidak dapat memilih kunci Multi-wilayah. Untuk kunci yang dikelola pelanggan, Security Lake membuat hibah atas nama Anda dengan mengirimkan `CreateGrant` permintaan ke AWS KMS. Hibah AWS KMS digunakan untuk memberikan Security Lake akses ke KMS kunci di akun pelanggan.

Security Lake memerlukan hibah untuk menggunakan kunci yang dikelola pelanggan Anda untuk operasi internal berikut:

- Kirim `GenerateDataKey` permintaan AWS KMS untuk menghasilkan kunci data yang dienkripsi oleh kunci terkelola pelanggan Anda.
- Kirim `RetireGrant` permintaan ke AWS KMS. Saat Anda memperbarui data lake Anda, operasi ini memungkinkan penghentian hibah yang ditambahkan ke AWS KMS kunci untuk ETL diproses.

Security Lake tidak memerlukan `Decrypt` izin. Ketika pengguna resmi kunci membaca data Security Lake, S3 mengelola dekripsi, dan pengguna yang berwenang dapat membaca data dalam bentuk yang tidak terenkripsi. Namun, pelanggan memerlukan `Decrypt` izin untuk menggunakan data sumber. Untuk informasi selengkapnya tentang izin pelanggan, lihat. Mengelola akses data untuk pelanggan Security Lake

Jika Anda ingin menggunakan KMS kunci yang ada untuk mengenkripsi data Security Lake, Anda harus mengubah kebijakan kunci untuk KMS kunci tersebut. Kebijakan utama harus mengizinkan IAM

peran yang terkait dengan lokasi danau data Lake Formation untuk menggunakan KMS kunci untuk mendekripsi data. Untuk petunjuk tentang cara mengubah kebijakan kunci untuk KMS kunci, lihat Mengubah kebijakan kunci di Panduan AWS Key Management Service Pengembang.

KMSKunci Anda dapat menerima permintaan hibah, memungkinkan Security Lake mengakses kunci, saat Anda membuat kebijakan kunci atau menggunakan kebijakan kunci yang ada dengan izin yang sesuai. Untuk petunjuk cara membuat kebijakan kunci, lihat Membuat kebijakan kunci di Panduan AWS Key Management Service Pengembang.

Lampirkan kebijakan kunci berikut ke KMS kunci Anda:

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleRole"},
  "Action": [
    "kms:CreateGrant",
    "kms:DescribeKey",
    "kms:GenerateDataKey"
  ],
  "Resource": "*"
}
```

IAMIzin yang diperlukan saat menggunakan kunci yang dikelola pelanggan

Lihat bagian Memulai: Prasyarat untuk ikhtisar IAM peran yang perlu Anda buat untuk menggunakan Security Lake.

Saat Anda menambahkan sumber khusus atau pelanggan, Security Lake membuat IAM peran di akun Anda. Peran ini dimaksudkan untuk dibagikan dengan IAM identitas lain. Mereka mengizinkan sumber khusus untuk menulis data ke danau data dan pelanggan untuk mengkonsumsi data dari danau data. Kebijakan AWS terkelola yang disebut `AmazonSecurityLakePermissionsBoundary` menetapkan batas izin untuk peran ini.

Mengenkripsi antrian Amazon SQS

Saat Anda membuat data lake, Security Lake membuat dua antrian Amazon Simple Queue Service (SQSAmazon) yang tidak terenkripsi di akun administrator Security Lake yang didelegasikan. Anda harus mengenkripsi antrian ini untuk melindungi data Anda. Enkripsi sisi server default (SSE)

yang disediakan oleh Amazon Simple Queue Service tidak cukup. Anda harus membuat kunci terkelola pelanggan in AWS Key Management Service (AWS KMS) untuk mengenkripsi antrian dan memberikan izin utama layanan Amazon S3 untuk bekerja dengan antrian terenkripsi. Untuk petunjuk tentang pemberian izin ini, lihat Mengapa notifikasi peristiwa Amazon S3 tidak dikirimkan ke antrian SQS Amazon yang menggunakan enkripsi sisi server? di pusat AWS pengetahuan.

Karena Security Lake digunakan AWS Lambda untuk mendukung mengekstrak, mentransfer, dan memuat (ETL) pekerjaan pada data Anda, Anda juga harus memberikan izin Lambda untuk mengelola pesan di antrian Amazon Anda. SQS Untuk selengkapnya, lihat Izin peran eksekusi di Panduan AWS Lambda Pengembang.

Enkripsi bergerak

Security Lake mengenkripsi semua data dalam perjalanan antar AWS layanan. Security Lake melindungi data dalam perjalanan, saat melakukan perjalanan ke dan dari layanan, dengan secara otomatis mengenkripsi semua data antar-jaringan menggunakan protokol enkripsi Transport Layer Security (TLS) 1.2. HTTPSPermintaan langsung yang dikirim ke Security Lake APIs ditandatangani dengan menggunakan Algoritma AWS Signature Version 4 untuk membuat koneksi yang aman.

Memilih untuk tidak menggunakan data Anda untuk perbaikan layanan

Anda dapat memilih untuk tidak menggunakan data Anda untuk mengembangkan dan meningkatkan Security Lake dan layanan AWS keamanan lainnya dengan menggunakan kebijakan AWS Organizations opt-out. Anda dapat memilih untuk memilih keluar meskipun Security Lake saat ini tidak mengumpulkan data tersebut. Untuk informasi selengkapnya tentang cara memilih keluar, lihat kebijakan opt-out layanan AI di AWS Organizations Panduan Pengguna.

Saat ini, Security Lake tidak mengumpulkan data keamanan apa pun yang diproses atas nama Anda, atau data keamanan yang Anda unggah ke danau data keamanan yang dibuat oleh layanan ini. Untuk mengembangkan dan meningkatkan layanan Security Lake dan fungsionalitas layanan AWS keamanan lainnya, Security Lake dapat mengumpulkan data tersebut di masa mendatang, termasuk data yang Anda unggah dari sumber data pihak ketiga. Kami akan memperbarui halaman ini ketika Security Lake bermaksud mengumpulkan data semacam itu dan menjelaskan cara kerjanya. Anda masih akan memiliki kesempatan untuk memilih keluar kapan saja.

> **Note**
>
> Agar Anda dapat menggunakan kebijakan opt-out, AWS akun Anda harus dikelola secara terpusat oleh. AWS Organizations Jika Anda belum membuat organisasi untuk AWS akun Anda, lihat Membuat dan mengelola organisasi di Panduan AWS Organizations Pengguna.

Memilih keluar memiliki efek sebagai berikut:

- Security Lake akan menghapus data yang dikumpulkan dan disimpan sebelum Anda memilih keluar (jika ada).
- Setelah Anda memilih keluar, Security Lake tidak akan lagi mengumpulkan atau menyimpan data ini.

Validasi kepatuhan untuk Amazon Security Lake

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Kepatuhan & Tata Kelola Keamanan — Panduan implementasi solusi ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- Arsitektur untuk HIPAA Keamanan dan Kepatuhan di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat HIPAA aplikasi yang memenuhi syarat.

> **Note**
>
> Tidak semua Layanan AWS HIPAA memenuhi syarat. Untuk informasi selengkapnya, lihat Referensi Layanan yang HIPAA Memenuhi Syarat.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi ()). ISO
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCIDSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Praktik terbaik keamanan untuk Security Lake

Lihat praktik terbaik berikut untuk bekerja dengan Amazon Security Lake.

Berikan izin minimum kepada pengguna Security Lake

Ikuti prinsip hak istimewa terkecil dengan memberikan set minimum izin kebijakan akses untuk AWS Identity and Access Management (IAM) pengguna, grup pengguna, dan peran Anda. Misalnya, Anda mungkin mengizinkan IAM pengguna untuk melihat daftar sumber log di Security Lake tetapi tidak membuat sumber atau pelanggan. Untuk informasi selengkapnya, silakan lihat Contoh kebijakan berbasis identitas untuk Security Lake

Anda juga dapat menggunakan AWS CloudTrail untuk melacak API penggunaan di Security Lake. CloudTrail menyediakan catatan API tindakan yang diambil oleh pengguna, grup, atau peran di Security Lake. Untuk informasi selengkapnya, lihat Pencatatan API panggilan Security Lake menggunakan CloudTrail.

Lihat halaman Ringkasan

Halaman Ringkasan konsol Security Lake memberikan ikhtisar masalah dari 14 hari terakhir yang memengaruhi layanan Security Lake dan bucket Amazon S3 tempat data Anda disimpan. Anda dapat menyelidiki lebih lanjut masalah ini untuk membantu Anda mengurangi kemungkinan dampak terkait keamanan.

Integrasi dengan Security Hub

Integrasikan Security Lake dan AWS Security Hub untuk menerima temuan Security Hub di Security Lake. Security Hub menghasilkan temuan dari banyak integrasi yang berbeda Layanan AWS dan pihak ketiga. Menerima temuan Security Hub membantu Anda mendapatkan gambaran umum tentang postur kepatuhan Anda dan apakah Anda memenuhi praktik terbaik AWS keamanan.

Untuk informasi selengkapnya, lihat Integrasi dengan AWS Security Hub.

Hapus AWS Lambda

Saat menghapus suatu AWS Lambda fungsi, kami sarankan untuk tidak menonaktifkannya terlebih dahulu. Menonaktifkan fungsi Lambda sebelum penghapusan dapat mengganggu kemampuan kueri data dan berpotensi memengaruhi fungsi lainnya. Yang terbaik adalah menghapus fungsi Lambda secara langsung tanpa menonaktifkannya. Untuk informasi selengkapnya tentang menghapus fungsi Lambda, AWS Lambda lihat panduan pengembang.

Memantau acara Security Lake

Anda dapat memantau Security Lake menggunakan CloudWatch metrik Amazon. CloudWatch mengumpulkan data mentah dari Security Lake setiap menit dan memprosesnya menjadi metrik. Anda dapat menyetel alarm yang memicu notifikasi saat metrik cocok dengan ambang batas yang ditentukan.

Untuk informasi selengkapnya, lihat CloudWatchmetrik untuk Amazon Security Lake.

Ketahanan di Danau Keamanan Amazon

Infrastruktur global AWS dibangun di sekitar Wilayah AWS dan Availability Zone. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi yang terhubung dengan jaringan latensi rendah, throughput tinggi, dan jaringan yang sangat berlebihan. Availability Zone ini menawarkan cara efektif untuk merancang dan mengoperasikan aplikasi dan basis data. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Ketersediaan Danau Keamanan terkait dengan ketersediaan Wilayah. Distribusi di beberapa Availability Zone membantu layanan mentolerir kegagalan di Availability Zone tunggal.

Ketersediaan pesawat data Security Lake tidak terkait dengan ketersediaan Wilayah apa pun. Namun, ketersediaan pesawat kontrol Danau Keamanan terkait erat dengan ketersediaan Wilayah AS Timur (Virginia N.).

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur Global AWS.

Selain infrastruktur AWS global, Security Lake, di mana data didukung oleh Amazon Simple Storage Service (Amazon S3); menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan pencadangan Anda.

Konfigurasi siklus hidup

> Konfigurasi siklus aktif adalah serangkaian aturan yang menentukan tindakan yang diterapkan Amazon S3 pada sekelompok objek. Dengan aturan konfigurasi siklus aktif, Anda dapat memberi tahu Amazon S3 untuk melakukan transisi objek ke kelas penyimpanan yang lebih murah, mengarsipkan, atau menghapusnya. Untuk informasi selengkapnya, lihat Mengelola siklus hidup penyimpanan di Panduan Pengguna Amazon S3.

Pembuatan Versi

> Versioning adalah cara menyimpan beberapa varian objek dalam bucket yang sama. Anda dapat menggunakan versioning untuk menyimpan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan dalam bucket Amazon S3. Pembuatan versi membantu Anda pulih dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi. Untuk informasi selengkapnya, lihat Menggunakan pembuatan versi di bucket S3 di Panduan Pengguna Amazon S3.

Kelas penyimpanan

Amazon S3 menawarkan berbagai kelas penyimpanan untuk dipilih tergantung pada persyaratan beban kerja Anda. Kelas penyimpanan IA Standar S3 dan S3 One Zone-IA dirancang untuk data yang Anda akses sebulan sekali dan memerlukan akses milidetik. Kelas penyimpanan S3 Glacier Instant Retrieval dirancang untuk data arsip berumur panjang yang diakses dengan akses milidetik yang Anda akses sekitar seperempat sekali. Untuk data arsip yang tidak memerlukan akses langsung, seperti backup, Anda dapat menggunakan kelas penyimpanan S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive. Untuk informasi selengkapnya, lihat Menggunakan kelas penyimpanan Amazon S3 di Panduan Pengguna Amazon S3.

Keamanan infrastruktur di Amazon Security Lake

Sebagai layanan terkelola, Amazon Security Lake dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan API panggilan yang AWS dipublikasikan untuk mengakses Security Lake melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Transportasi (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju yang sempurna (PFS) seperti (Ephemeral Diffie-Hellman) atau DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan IAM prinsipal. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Analisis konfigurasi dan kerentanan di Security Lake

Konfigurasi dan kontrol IT merupakan tanggung jawab bersama antara AWS dan Anda, pelanggan kami. Untuk informasi selengkapnya, lihat model tanggung jawab bersama AWS.

Pemantauan Danau Keamanan Amazon

Security Lake terintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil dalam Security Lake oleh pengguna, peran, atau yang. Layanan AWS Hal ini mencakup tindakan dari konsol Security Lake dan panggilan program untuk operasi Security Lake. Dengan menggunakan informasi yang dikumpulkan olehCloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Security Lake. Untuk setiap permintaan, Anda dapat mengidentifikasi waktu permintaan itu dibuat, tempat alamat IP itu dibuat, siapa yang membuat permintaan, dan detail tambahan lainnya. Untuk informasi selengkapnya, lihat Pencatatan API panggilan Security Lake menggunakan CloudTrail.

Security Lake dan Amazon CloudWatch terintegrasi, sehingga Anda dapat mengumpulkan, dan menganalisis metrik yang dikumpulkan oleh Security Lake. CloudWatchmetrik untuk data lake Security Lake Anda secara otomatis dikumpulkan dan didorong ke CloudWatch interval satu menit. Anda juga dapat mengatur alarm untuk mengirimkan notifikasi jika ambang batas tertentu dipenuhi untuk metrik Security Lake. Untuk daftar semua metrik yang dikirim oleh Security LakeCloudWatch, lihat. Metrik dan dimensi Danau keamanan

CloudWatchmetrik untuk Amazon Security Lake

Anda dapat memantau Security Lake menggunakan AmazonCloudWatch, yang mengumpulkan data mentah setiap menit dan memprosesnya menjadi metrik yang dapat dibaca dan hampir waktu nyata. Statistik ini disimpan untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang data di danau data Anda. Anda juga dapat mengatur alarm yang memperhatikan ambang batas tertentu dan mengirim notifikasi atau mengambil tindakan saat ambang batas tersebut terpenuhi.

Topik

- Metrik dan dimensi Danau keamanan
- Melihat CloudWatch metrik untuk Security Lake
- Mengatur CloudWatch alarm untuk metrik Security Lake

Metrik dan dimensi Danau keamanan

Namespace `AWS/SecurityLake` mencakup metrik berikut.

Metrik	Deskripsi
`ProcessedSize`	Volume data dari yang didukung secara asli Layanan AWS yang saat ini disimpan di data lake Anda. Unit: Bita

Dimensi berikut tersedia untuk metrik Security Lake.

Dimensi	Deskripsi
`Account`	`ProcessedSize` metrik untuk spesifikAkun AWS. Dimensi ini hanya tersedia ketika Anda melihat `Per-Account Source Version Metrics` padaCloudWatch.
`Region`	`ProcessedSize` metrik untuk spesifikWilayah AWS.
`Source`	`ProcessedSize` metrik untuk sumber AWS log tertentu.
`SourceVersion`	`ProcessedSize` metrik untuk versi spesifik dari sumber AWS log.

Anda dapat melihat metrik untuk spesifik Akun AWS (`Per-Account Source Version Metrics`) atau untuk semua akun di organisasi (`Per-Source Version Metrics`).

Melihat CloudWatch metrik untuk Security Lake

Anda dapat memantau metrik untuk Security Lake menggunakan CloudWatch konsol, CloudWatch antarmuka baris perintah sendiri (CLI), atau secara terprogram menggunakan API. CloudWatch Pilih metode yang Anda inginkan, dan ikuti langkah-langkah untuk mengakses metrik Security Lake.

CloudWatch console

1. Buka konsol CloudWatch di https://console.aws.amazon.com/cloudwatch/.

2. Pada panel navigasi, pilih Metrik, Semua metrik.
3. Pada tab Jelajahi, pilih Danau Keamanan.
4. Pilih Metrik Versi Sumber Per Akun atau Metrik Versi Per Sumber.
5. Pilih metrik untuk melihatnya secara detail. Anda juga dapat memilih untuk melakukan hal berikut:

   - Untuk menyortir metrik, gunakan judul kolom.
   - Untuk membuat grafik metrik, pilih nama metrik, pilih opsi grafik.
   - Untuk memfilter berdasarkan metrik, pilih nama metrik dan kemudian pilih Tambahkan ke pencarian.

CloudWatch API

Untuk mengakses metrik Security Lake menggunakan CloudWatch API, gunakan `GetMetricStatistics`tindakan tersebut.

AWS CLI

Untuk mengakses metrik Security Lake menggunakanAWS CLI, jalankan `get-metric-statistics`perintah.

Untuk informasi selengkapnya tentang pemantauan menggunakan metrik, lihat Menggunakan CloudWatch metrik Amazon di CloudWatchPanduan Pengguna Amazon.

Mengatur CloudWatch alarm untuk metrik Security Lake

CloudWatchjuga memungkinkan Anda mengatur alarm bila ambang batas terpenuhi untuk suatu metrik. Misalnya, Anda dapat menyetel alarm untuk ProcessedSizemetrik, sehingga Anda diberi tahu bila volume data dari sumber tertentu melebihi ambang batas tertentu.

Untuk petunjuk tentang pengaturan alarm, lihat Menggunakan CloudWatch alarm Amazon di CloudWatchPanduan Pengguna Amazon.

Pencatatan API panggilan Security Lake menggunakan CloudTrail

Amazon Security Lake terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Security Lake. CloudTrail menangkap API panggilan untuk Security Lake sebagai acara. Panggilan yang diambil termasuk panggilan dari konsol Security Lake dan panggilan kode ke API operasi Security Lake. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Security Lake. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Security Lake, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Informasi Danau Keamanan di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Danau Keamanan, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail acara.

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk Security Lake, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi SNS notifikasi Amazon untuk CloudTrail

- Menerima file CloudTrail log dari beberapa wilayah dan Menerima file CloudTrail log dari beberapa akun

Tindakan Security Lake dicatat oleh CloudTrail dan didokumentasikan dalam APIReferensi Danau Keamanan. Misalnya, panggilan ke`UpdateDataLake`,`ListLogSources`, dan `CreateSubscriber` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Apakah permintaan dibuat dengan root atau kredensi AWS Identity and Access Management pengguna.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi lebih lanjut, lihat CloudTrail userIdentity elemen.

Memahami entri file log Security Lake

CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari API panggilan publik, sehingga tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log untuk `GetSubscriber` tindakan Security Lake.


```
{
   "eventVersion": "1.08",
   "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE:user",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/user",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
         "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
            "arn": "arn:aws:iam::123456789012:role/Admin",
            "accountId": "123456789012",
            "userName": "Admin"
         },
         "webIdFederationData": {
         },
         "attributes": {
            "creationDate": "2023-05-30T13:27:19Z",
            "mfaAuthenticated": "false"
         }
      }
   },
   "eventTime": "2023-05-30T17:29:17Z",
   "eventSource": "securitylake.amazonaws.com",
   "eventName": "GetSubscriber",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "198.51.100.1",
   "userAgent": "console.amazonaws.com",
   "requestParameters": {
      "subscriberId": "30ed17a3-0cac-4997-a41f-f5a6bexample"
   },
   "responseElements": null,
   "requestID": "d01f0f32-9ec6-4579-af50-e9f14example",
   "eventID": "9c1bff41-0f48-4ee6-921c-ebfd8example",
   "readOnly": false,
   "eventType": "AwsApiCall",
   "managementEvent": true,
   "recipientAccountId": "123456789012",
   "eventCategory": "Management"
}
```

Menandai sumber daya Danau Keamanan

Tag adalah label opsional yang dapat Anda tentukan dan tetapkan ke AWS sumber daya, termasuk jenis sumber daya Amazon Security Lake tertentu. Tag dapat membantu Anda mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Misalnya, Anda dapat menggunakan tag untuk menerapkan kebijakan, mengalokasikan biaya, membedakan sumber daya, atau mengidentifikasi sumber daya yang mendukung persyaratan kepatuhan atau alur kerja tertentu.

Anda dapat menetapkan tag ke jenis sumber daya Security Lake berikut: pelanggan, dan konfigurasi data lake untuk individu Wilayah AWS Anda Akun AWS .

Topik

Menandai dasar-dasar

Sumber daya dapat memiliki sebanyak 50 tag. Setiap tag terdiri dari kunci tag yang diperlukan dan nilai tag opsional, yang keduanya Anda tentukan. Kunci tag adalah label umum yang bertindak sebagai kategori untuk nilai tag yang lebih spesifik. Nilai tag bertindak sebagai deskriptor untuk kunci tag.

Misalnya, jika Anda menambahkan pelanggan untuk menganalisis data keamanan dari lingkungan yang berbeda (satu set pelanggan untuk data cloud dan set lain untuk data lokal), Anda dapat menetapkan kunci `Environment` tag untuk pelanggan tersebut. Nilai tag terkait mungkin `Cloud` untuk pelanggan yang menganalisis data dari Layanan AWS, dan `On-Premises` untuk yang lain.

Saat Anda menentukan dan menetapkan tag ke sumber daya Amazon Security Lake, ingatlah hal berikut:

- Setiap sumber daya dapat memiliki maksimum 50 tag.
- Untuk setiap sumber daya, setiap kunci tag harus unik dan hanya dapat memiliki satu nilai tag.

- Kunci dan nilai tanda peka huruf besar-kecil. Sebagai praktik terbaik, kami menyarankan Anda menentukan strategi untuk memanfaatkan tag dan menerapkan strategi itu secara konsisten di seluruh sumber daya Anda.
- Tombol tag dapat memiliki maksimum 128 UTF -8 karakter. Nilai tag dapat memiliki maksimal 256 UTF -8 karakter. Karakter dapat berupa huruf, angka, spasi, atau simbol berikut: _.:/= + - @
- `aws:`Awalan dicadangkan untuk digunakan oleh AWS. Anda tidak dapat menggunakannya dalam kunci tag atau nilai apa pun yang Anda tentukan. Selain itu, Anda tidak dapat mengubah atau menghapus kunci tag atau nilai yang menggunakan awalan ini. Tag yang menggunakan awalan ini tidak dihitung terhadap kuota 50 tag per sumber daya.
- Setiap tag yang Anda tetapkan hanya tersedia untuk Anda Akun AWS dan hanya Wilayah AWS di mana Anda menetapkannya.
- Jika Anda menetapkan tag ke sumber daya menggunakan Security Lake, tag hanya diterapkan ke sumber daya yang disimpan langsung di Security Lake di tempat yang berlaku Wilayah AWS. Mereka tidak diterapkan pada sumber daya pendukung terkait yang dibuat, digunakan, atau dikelola Security Lake untuk Anda di tempat lain Layanan AWS. Misalnya, jika Anda menetapkan tag ke data lake Anda, tag hanya diterapkan ke konfigurasi data lake Anda di Security Lake untuk Wilayah yang ditentukan. Aplikasi ini tidak diterapkan ke bucket Amazon Simple Storage Service (Amazon S3) yang menyimpan data log dan peristiwa Anda. Untuk juga menetapkan tag ke sumber daya terkait, Anda dapat menggunakan AWS Resource Groups atau Layanan AWS yang menyimpan sumber daya—misalnya, Amazon S3 untuk bucket S3. Menetapkan tag ke sumber daya terkait dapat membantu Anda mengidentifikasi sumber daya pendukung untuk data lake Anda.
- Jika Anda menghapus sumber daya, tag apa pun yang ditetapkan ke sumber daya juga akan dihapus.

Untuk batasan, tips, dan praktik terbaik tambahan, lihat Menandai AWS sumber daya Anda di Panduan Pengguna AWS Sumber Daya Penandaan.

> **Important**
>
> Jangan menyimpan rahasia atau jenis data sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS, termasuk AWS Billing and Cost Management. Mereka tidak dimaksudkan untuk digunakan untuk data sensitif.

Untuk menambahkan dan mengelola tag untuk sumber daya Security Lake, Anda dapat menggunakan konsol Security Lake atau Security LakeAPI.

Menggunakan tag dalam IAM kebijakan

Setelah Anda mulai menandai sumber daya, Anda dapat menentukan izin tingkat sumber daya berbasis tag dalam kebijakan (). AWS Identity and Access Management IAM Dengan menggunakan tag dengan cara ini, Anda dapat menerapkan kontrol terperinci tentang pengguna dan peran mana yang Akun AWS memiliki izin untuk membuat dan menandai sumber daya, dan pengguna dan peran mana yang memiliki izin untuk menambahkan, mengedit, dan menghapus tag secara lebih umum. Untuk mengontrol akses berdasarkan tag, Anda dapat menggunakan kunci kondisi terkait tag di elemen Kondisi kebijakan. IAM

Misalnya, Anda dapat membuat kebijakan yang memungkinkan pengguna memiliki akses penuh ke semua sumber daya Amazon Security Lake, jika `Owner` tag untuk sumber daya menentukan nama pengguna mereka:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Jika Anda menentukan izin tingkat sumber daya berbasis tag, izin akan segera berlaku. Ini berarti bahwa sumber daya Anda lebih aman segera setelah dibuat, dan Anda dapat dengan cepat mulai menerapkan penggunaan tag untuk sumber daya baru. Anda juga dapat menggunakan izin tingkat sumber daya untuk mengontrol kunci dan nilai tag mana yang dapat dikaitkan dengan sumber daya baru dan yang sudah ada. Untuk informasi selengkapnya, lihat Mengontrol akses ke AWS sumber daya menggunakan tag di Panduan IAM Pengguna.

Menambahkan tag ke sumber daya Amazon Security Lake

Untuk menambahkan tag ke sumber daya Amazon Security Lake, Anda dapat menggunakan konsol Security Lake atau Security LakeAPI.

> **Important**
>
> Menambahkan tag ke sumber daya dapat memengaruhi akses ke sumber daya. Sebelum menambahkan tag ke sumber daya, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

Console

Saat Anda mengaktifkan Security Lake untuk Wilayah AWS atau membuat pelanggan, konsol Security Lake menyediakan opsi untuk menambahkan tag ke sumber daya—konfigurasi data lake untuk Wilayah atau pelanggan. Ikuti petunjuk di konsol untuk menambahkan tag ke sumber daya saat Anda membuat sumber daya.

Untuk menambahkan satu atau beberapa tag ke sumber daya yang ada menggunakan konsol Security Lake, ikuti langkah-langkah berikut.

Untuk menambahkan tanda ke sumber daya

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Bergantung pada jenis sumber daya yang ingin Anda tambahkan tag, lakukan salah satu hal berikut:

   - Untuk konfigurasi data lake, pilih Wilayah di panel navigasi. Kemudian, di tabel Regions, pilih Region.
   - Untuk pelanggan, pilih Pelanggan di panel navigasi. Kemudian, di tabel Pelanggan saya, pilih pelanggan.

     Jika pelanggan tidak muncul di tabel, gunakan Wilayah AWS pemilih di sudut kanan atas halaman untuk memilih Wilayah tempat Anda membuat pelanggan. Tabel mencantumkan pelanggan yang ada hanya untuk Wilayah saat ini.
3. Pilih Edit.
4. Perluas bagianTag. Bagian ini mencantumkan semua tag yang saat ini ditetapkan ke sumber daya.

5. Di bagian Tag, pilih Tambahkan tag baru.
6. Di kotak Kunci, masukkan kunci tag untuk tag yang akan ditambahkan ke sumber daya. Kemudian, di kotak Nilai, secara opsional masukkan nilai tag untuk kunci tersebut.

   Kunci tag dapat berisi sebanyak 128 karakter. Nilai tag dapat berisi sebanyak 256 karakter. Karakter dapat berupa huruf, angka, spasi, atau simbol berikut: _.:/= + - @
7. Untuk menambahkan tag lain ke sumber daya, pilih Tambahkan tag baru, lalu ulangi langkah sebelumnya. Anda dapat menetapkan sebanyak 50 tag ke sumber daya.
8. Setelah selesai menambahkan tag, pilih Simpan.

API

Untuk membuat sumber daya dan menambahkan satu atau beberapa tag ke dalamnya secara terprogram, gunakan `Create` operasi yang sesuai untuk jenis sumber daya yang ingin Anda buat:

- Konfigurasi data lake — Gunakan CreateDataLakeoperasi atau, jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan create-data-lakeperintah.
- Subscriber — Gunakan CreateSubscriberoperasi atau, jika Anda menggunakan AWS CLI, jalankan perintah create-subscriber.

Dalam permintaan Anda, gunakan `tags` parameter untuk menentukan kunci tag (`key`) dan nilai tag opsional (`value`) untuk setiap tag untuk ditambahkan ke sumber daya. `tags`Parameter menentukan array objek. Setiap objek menentukan kunci tag dan nilai tag yang terkait.

Untuk menambahkan satu atau beberapa tag ke sumber daya yang ada, gunakan TagResourcepengoperasian Security Lake API atau, jika Anda menggunakan AWS CLI, jalankan perintah tag-resource. Dalam permintaan Anda, tentukan Amazon Resource Name (ARN) sumber daya yang ingin Anda tambahkan tag. Gunakan `tags` parameter untuk menentukan kunci tag (`key`) dan nilai tag opsional (`value`) untuk setiap tag yang akan ditambahkan. Seperti halnya untuk `Create` operasi dan perintah, `tags` parameter menentukan array objek, satu objek untuk setiap kunci tag dan nilai tag yang terkait.

Misalnya, AWS CLI perintah berikut menambahkan kunci `Environment` tag dengan nilai `Cloud` tag ke pelanggan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake tag-resource \
```

```
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Environment,value=Cloud
```

Di mana:

- `resource-arn`menentukan pelanggan untuk menambahkan tag ke. ARN
- *`Environment`*adalah kunci tag tag untuk ditambahkan ke pelanggan.
- *`Cloud`*adalah nilai tag untuk kunci tag yang ditentukan (*`Environment`*).

Dalam contoh berikut, perintah menambahkan beberapa tag ke pelanggan.

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Environment,value=Cloud key=CostCenter,value=12345 key=Owner,value=jane-
doe
```

Untuk setiap objek dalam `tags` array, keduanya `key` dan `value` argumen diperlukan. Namun, nilai untuk `value` argumen dapat berupa string kosong. Jika Anda tidak ingin mengaitkan nilai tag dengan kunci tag, jangan tentukan nilai untuk `value` argumen tersebut. Misalnya, perintah berikut menambahkan kunci `Owner` tag tanpa nilai tag terkait:

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

Jika operasi penandaan berhasil, Security Lake mengembalikan respons HTTP 200 kosong. Jika tidak, Security Lake mengembalikan respons HTTP 4 xx atau 500 yang menunjukkan mengapa operasi gagal.

Mengedit tag untuk sumber daya Amazon Security Lake

Untuk mengedit tag (kunci tag atau nilai tag) untuk sumber daya Amazon Security Lake, Anda dapat menggunakan konsol Security Lake atau Security LakeAPI.

> **Important**
>
> Mengedit tag untuk sumber daya dapat memengaruhi akses ke sumber daya. Sebelum Anda mengedit kunci tag atau nilai untuk sumber daya, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

Console

Ikuti langkah-langkah ini untuk mengedit tag sumber daya dengan menggunakan konsol Security Lake.

Untuk mengedit tag untuk sumber daya

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Bergantung pada jenis sumber daya yang tagnya ingin Anda edit, lakukan salah satu hal berikut:
   - Untuk konfigurasi data lake, pilih Wilayah di panel navigasi. Kemudian, di tabel Regions, pilih Region.
   - Untuk pelanggan, pilih Pelanggan di panel navigasi. Kemudian, di tabel Pelanggan saya, pilih pelanggan.

     Jika pelanggan tidak muncul di tabel, gunakan Wilayah AWS pemilih di sudut kanan atas halaman untuk memilih Wilayah tempat Anda membuat pelanggan. Tabel mencantumkan pelanggan yang ada hanya untuk Wilayah saat ini.
3. Pilih Edit.
4. Perluas bagianTag. Bagian Tag mencantumkan semua tag yang saat ini ditetapkan ke sumber daya.
5. Lakukan salah satu langkah berikut ini:
   - Untuk menambahkan nilai tag ke kunci tag yang ada, masukkan nilai di kotak Nilai di sebelah kunci tag.
   - Untuk mengubah kunci tag yang ada, pilih Hapus di sebelah tag. Kemudian pilih Tambahkan tag baru. Di kotak Kunci yang muncul, masukkan kunci tag baru. Secara opsional masukkan nilai tag terkait di kotak Nilai.

- Untuk mengubah nilai tag yang ada, pilih X di kotak Nilai yang berisi nilai. Kemudian masukkan nilai tag baru di Nilai kotak.
- Untuk menghapus nilai tag yang ada, pilih X di kotak Nilai yang berisi nilai.
- Untuk menghapus tag yang ada (kunci tag dan nilai tag), pilih Hapus di sebelah tag.

Sumber daya dapat memiliki sebanyak 50 tag. Kunci tag dapat berisi sebanyak 128 karakter. Nilai tag dapat berisi sebanyak 256 karakter. Karakter dapat berupa huruf, angka, spasi, atau simbol berikut: _.:/= + - @

6. Setelah Anda selesai mengedit tag, pilih Simpan.

API

Saat Anda mengedit tag untuk sumber daya secara terprogram, Anda menimpa tag yang ada dengan nilai baru. Oleh karena itu, cara terbaik untuk mengedit tag tergantung pada apakah Anda ingin mengedit kunci tag, nilai tag, atau keduanya. Untuk mengedit kunci tag, hapus tag saat ini dan tambahkan tag baru.

Untuk mengedit atau menghapus hanya nilai tag yang terkait dengan kunci tag, timpa nilai yang ada dengan menggunakan TagResourcepengoperasian Security LakeAPI. Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah tag-resource. Dalam permintaan Anda, tentukan Amazon Resource Name (ARN) sumber daya yang nilai tagnya ingin Anda edit atau hapus.

Untuk mengedit nilai tag, gunakan `tags` parameter untuk menentukan kunci tag yang nilai tag yang ingin Anda ubah. Juga tentukan nilai tag baru untuk kunci tersebut. Misalnya, AWS CLI perintah berikut mengubah nilai tag dari `Cloud` menjadi `On-Premises` kunci `Environment` tag yang ditetapkan ke pelanggan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Environment,value=On-Premises
```

Di mana:

- `resource-arn`menentukan ARN pelanggan.

- *Environment*adalah kunci tag yang terkait dengan nilai tag yang akan diubah.
- *On-Premises*adalah nilai tag baru untuk kunci tag yang ditentukan (*Environment*).

Untuk menghapus nilai tag dari kunci tag, jangan tentukan nilai untuk `value` argumen kunci dalam `tags` parameter. Sebagai contoh:

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

Jika operasi berhasil, Security Lake mengembalikan respons HTTP 200 kosong. Jika tidak, Security Lake mengembalikan respons HTTP 4 xx atau 500 yang menunjukkan mengapa operasi gagal.

Meninjau tag untuk sumber daya Amazon Security Lake

Anda dapat meninjau tag (kunci tag dan nilai tag) untuk sumber daya Amazon Security Lake dengan menggunakan konsol Security Lake atau Security LakeAPI.

Console

Ikuti langkah-langkah ini untuk meninjau tag sumber daya dengan menggunakan konsol Security Lake.

Untuk meninjau tag untuk sumber daya

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Bergantung pada jenis sumber daya yang tagnya ingin Anda tinjau, lakukan salah satu hal berikut:
   - Untuk konfigurasi data lake, pilih Wilayah di panel navigasi. Di tabel Regions, pilih Region, lalu pilih Edit. Kemudian perluas bagian Tag.
   - Untuk pelanggan, pilih Pelanggan di panel navigasi. Kemudian, di tabel Pelanggan saya, pilih nama pelanggan.

Jika pelanggan tidak muncul di tabel, gunakan Wilayah AWS pemilih di sudut kanan atas halaman untuk memilih Wilayah tempat Anda membuat pelanggan. Tabel mencantumkan pelanggan yang ada hanya untuk Wilayah saat ini.

Bagian Tag mencantumkan semua tag yang saat ini ditetapkan ke sumber daya.

API

Untuk mengambil dan meninjau tag untuk sumber daya yang ada secara terprogram, gunakan ListTagsForResourcepengoperasian Danau Keamanan. API Dalam permintaan Anda, gunakan `resourceArn` parameter untuk menentukan Amazon Resource Name (ARN) sumber daya.

Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan list-tags-for-resourceperintah dan gunakan `resource-arn` parameter untuk menentukan ARN sumber daya. Sebagai contoh:

```
$ aws securitylake list-tags-for-resource --resource-arn arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab
```

Dalam contoh sebelumnya, *arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab* adalah pelanggan ARN yang sudah ada.

Jika operasi berhasil, Security Lake mengembalikan `tags` array. Setiap objek dalam array menentukan tag (baik kunci tag dan nilai tag) yang saat ini ditetapkan ke sumber daya. Sebagai contoh:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Cloud"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
```

```
        }
    ]
}
```

Di mana `EnvironmentCostCenter`,, dan `Owner` merupakan kunci tag yang ditetapkan ke sumber daya. `Cloud`adalah nilai tag yang terkait dengan kunci `Environment` tag. `12345`adalah nilai tag yang terkait dengan kunci `CostCenter` tag. Kunci `Owner` tag tidak memiliki nilai tag terkait.

Menghapus tag dari sumber daya Amazon Security Lake

Untuk menghapus tag dari sumber daya Amazon Security Lake, Anda dapat menggunakan konsol Security Lake atau Security LakeAPI.

> **Important**
>
> Menghapus tag dari sumber daya dapat memengaruhi akses ke sumber daya. Sebelum Anda menghapus tag, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

Console

Ikuti langkah-langkah ini untuk menghapus satu atau beberapa tag dari sumber daya menggunakan konsol Security Lake.

Untuk menghapus tag dari sumber daya

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Bergantung pada jenis sumber daya yang ingin Anda hapus tag, lakukan salah satu hal berikut:
   - Untuk konfigurasi data lake, pilih Wilayah di panel navigasi. Kemudian, di tabel Regions, pilih Region.
   - Untuk pelanggan, pilih Pelanggan di panel navigasi. Kemudian, di tabel Pelanggan saya, pilih pelanggan.

Jika pelanggan tidak muncul di tabel, gunakan Wilayah AWS pemilih di sudut kanan atas halaman untuk memilih Wilayah tempat Anda membuat pelanggan. Tabel mencantumkan pelanggan yang ada hanya untuk Wilayah saat ini.

3. Pilih Edit.
4. Perluas bagianTag. Bagian Tag mencantumkan semua tag yang saat ini ditetapkan ke sumber daya.
5. Lakukan salah satu langkah berikut ini:

   - Untuk menghapus hanya nilai tag untuk tag, pilih X di kotak Nilai yang berisi nilai yang akan dihapus.
   - Untuk menghapus kunci tag dan nilai tag (sebagai pasangan) untuk tag, pilih Hapus di sebelah tag yang akan dihapus.
6. Untuk menghapus tag tambahan dari sumber daya, ulangi langkah sebelumnya untuk menghapus setiap tag tambahan.
7. Setelah Anda selesai menghapus tag, pilih Simpan.

API

Untuk menghapus satu atau lebih tag dari sumber daya secara terprogram, gunakan UntagResourcepengoperasian Danau Keamanan. API Dalam permintaan Anda, gunakan `resourceArn` parameter untuk menentukan Amazon Resource Name (ARN) sumber daya untuk menghapus tag. Gunakan `tagKeys` parameter untuk menentukan kunci tag tag yang akan dihapus. Untuk menghapus beberapa tag, tambahkan `tagKeys` parameter dan argumen untuk setiap tag yang akan dihapus, dipisahkan oleh ampersand (&) —misalnya,. `tagKeys=key1&tagKeys=key2` Untuk menghapus hanya nilai tag tertentu (bukan kunci tag) dari sumber daya, edit tag alih-alih menghapus tag.

Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah untag-resource untuk menghapus satu atau beberapa tag dari sumber daya. Untuk `resource-arn` parameter, tentukan ARN sumber daya untuk menghapus tag dari. Gunakan `tag-keys` parameter untuk menentukan kunci tag tag yang akan dihapus. Misalnya, perintah berikut menghapus `Environment` tag (kunci tag dan nilai tag) dari pelanggan yang ditentukan:

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
```

```
--tag-keys Environment
```

Di mana `resource-arn` menentukan ARN pelanggan untuk menghapus tag dari, dan *`Environment`* merupakan kunci tag tag untuk menghapus.

Untuk menghapus beberapa tag dari sumber daya, tambahkan setiap kunci tag tambahan sebagai argumen untuk `tag-keys` parameter. Sebagai contoh:

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment Owner
```

Jika operasi berhasil, Security Lake mengembalikan respons HTTP 200 kosong. Jika tidak, Security Lake mengembalikan respons HTTP 4 xx atau 500 yang menunjukkan mengapa operasi gagal.

Memecahkan masalah di Security Lake

Jika Anda mengalami masalah saat bekerja dengan Amazon Security Lake, gunakan sumber pemecahan masalah berikut.

Topik berikut memberikan saran pemecahan masalah untuk kesalahan dan masalah yang mungkin Anda temui terkait dengan status danau data, Lake Formation, kueri di Amazon Athena, dan. AWS Organizations IAM Jika Anda menemukan masalah yang tidak tercantum di sini, Anda dapat menggunakan `Feedback` tombol di halaman ini untuk melaporkannya.

Konsultasikan topik berikut jika Anda mengalami masalah saat menggunakan Security Lake.

Topik

- Memecahkan masalah status danau data
- Memecahkan masalah Lake Formation
- Memecahkan masalah kueri di Amazon Athena
- Memecahkan masalah Organizations
- Memecahkan masalah identitas dan akses Amazon Security Lake

Memecahkan masalah status danau data

Halaman Masalah pada konsol Security Lake menunjukkan ringkasan masalah yang memengaruhi data lake Anda. Misalnya, Security Lake tidak dapat mengaktifkan pengumpulan log untuk acara AWS CloudTrail manajemen jika Anda belum membuat CloudTrail jejak untuk organisasi Anda. Halaman Masalah mencakup masalah yang telah terjadi dalam 14 hari terakhir. Anda dapat melihat deskripsi setiap masalah dan langkah-langkah perbaikan yang disarankan.

Untuk mengakses ringkasan masalah secara terprogram, Anda dapat menggunakan ListDataLakeExceptionsOperasi Danau KeamananAPI. Jika Anda menggunakan AWS CLI, jalankan list-data-lake-exceptionsperintah. Untuk `regions` parameternya, Anda dapat menentukan satu atau beberapa kode Region—misalnya, `us-east-1` untuk Wilayah AS Timur (Virginia N.) —untuk melihat masalah yang memengaruhi Wilayah tersebut. Jika Anda tidak menyertakan `regions` parameter, masalah yang memengaruhi semua Wilayah akan dikembalikan. Untuk daftar kode Wilayah, lihat titik akhir Amazon Security Lake di. Referensi Umum AWS

Misalnya, AWS CLI perintah berikut mencantumkan masalah yang memengaruhi `us-east-1` dan `eu-west-3` Wilayah. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake list-data-lake-exceptions \
--regions "us-east-1" "eu-west-3"
```

Untuk memberi tahu pengguna Security Lake tentang masalah atau kesalahan, gunakan CreateDataLakeExceptionSubscriptionOperasi Danau KeamananAPI. Pengguna dapat diberi tahu melalui email, pengiriman ke antrian Amazon Simple Queue Service SQS (Amazon), pengiriman ke AWS Lambda fungsi, atau protokol lain yang didukung.

Misalnya, AWS CLI perintah berikut mengirimkan pemberitahuan pengecualian Security Lake ke akun yang ditentukan dengan SMS pengiriman. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake create-data-lake-exception-subscription \
--notification-endpoint "123456789012" \
--exception-time-to-live 30 \
--subscription-protocol "sms"
```

Untuk melihat detail tentang langganan pengecualian, Anda dapat menggunakan GetDataLakeExceptionSubscriptionoperasi. Untuk memperbarui langganan pengecualian, Anda dapat menggunakan UpdateDataLakeExceptionSubscriptionoperasi. Untuk menghapus langganan pengecualian dan menghentikan pemberitahuan, Anda dapat menggunakan DeleteDataLakeExceptionSubscriptionoperasi.

Memecahkan masalah Lake Formation

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Security Lake dan AWS Lake Formation database atau tabel. Untuk topik pemecahan masalah Lake Formation lainnya, lihat bagian Pemecahan Masalah pada Panduan Pengembang.AWS Lake Formation

Tabel tidak ditemukan

Anda mungkin menerima kesalahan ini saat mencoba membuat pelanggan.

Untuk mengatasi kesalahan ini, pastikan Anda telah menambahkan sumber di Wilayah. Jika Anda menambahkan sumber saat layanan Security Lake dalam rilis pratinjau, Anda harus menambahkannya lagi sebelum membuat pelanggan. Untuk informasi lebih lanjut tentang menambahkan sumber, lihatManajemen sumber di Security Lake.

400 AccessDenied

Anda mungkin menerima kesalahan ini saat menambahkan sumber khusus dan memanggil file `CreateCustomLogSource`API.

Untuk mengatasi kesalahan, tinjau izin Lake Formation Anda. IAMPeran yang memanggil API harus memiliki izin Buat tabel untuk database Security Lake. Untuk informasi selengkapnya, lihat Memberikan izin database menggunakan konsol Lake Formation dan metode sumber daya bernama di Panduan AWS Lake Formation Pengembang.

SYNTAX_ERROR: baris 1:8: SELECT * tidak diizinkan dari relasi yang tidak memiliki kolom

Anda mungkin menerima kesalahan ini saat menanyakan tabel sumber untuk pertama kalinya di Lake Formation.

Untuk mengatasi kesalahan, berikan `SELECT` izin untuk IAM peran yang Anda gunakan saat masuk ke peran Anda Akun AWS. Untuk petunjuk tentang cara memberikan `SELECT` izin, lihat Memberikan izin tabel menggunakan konsol Lake Formation dan metode sumber daya bernama di Panduan AWS Lake Formation Pengembang.

Security Lake gagal menambahkan kepala penelepon ARN ke admin danau data Lake Formation. Administrator data lake saat ini mungkin menyertakan prinsipal yang tidak valid yang tidak ada lagi.

Anda mungkin menerima kesalahan ini saat mengaktifkan Security Lake atau menambahkan Layanan AWS sebagai sumber log.

Untuk mengatasi kesalahan, ikuti langkah-langkah berikut:

1. Buka konsol Lake Formation di https://console.aws.amazon.com/lakeformation/.
2. Masuk sebagai pengguna administratif.
3. Di panel navigasi, di bawah Izin, pilih Peran dan tugas administratif.

4. Di bagian Administrator danau data, pilih Pilih administrator.
5. Hapus prinsip yang diberi label Tidak ditemukan di IAM, lalu pilih Simpan.
6. Coba operasi Danau Keamanan lagi.

Security Lake CreateSubscriber with Lake Formation tidak membuat undangan berbagi RAM sumber daya baru untuk diterima

Anda mungkin melihat kesalahan ini jika Anda berbagi sumber daya dengan berbagi data lintas akun Lake Formation versi 2 atau versi 3 sebelum membuat pelanggan Lake Formation di Security Lake. Ini karena berbagi lintas akun Lake Formation versi 2 dan versi 3 mengoptimalkan jumlah pembagian AWS RAM sumber daya dengan memetakan beberapa hibah izin lintas akun dengan satu pembagian sumber daya. AWS RAM

Pastikan untuk memeriksa bahwa nama berbagi sumber daya memiliki ID eksternal yang Anda tentukan saat membuat pelanggan dan pembagian sumber daya ARN cocok dengan `CreateSubscriber` respons. ARN

Memecahkan masalah kueri di Amazon Athena

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat menggunakan Athena untuk menanyakan objek yang disimpan di bucket Security Lake S3 Anda. Untuk topik pemecahan masalah Athena lainnya, lihat bagian Pemecahan Masalah di Athena di Panduan Pengguna Amazon Athena.

Query tidak mengembalikan objek baru di data lake

Kueri Athena Anda mungkin tidak mengembalikan objek baru di danau data Anda bahkan ketika bucket S3 untuk Security Lake berisi objek tersebut. Ini dapat terjadi jika Anda telah menonaktifkan Security Lake dan kemudian mengaktifkannya lagi. Akibatnya, AWS Glue partisi mungkin tidak mendaftarkan objek baru dengan benar.

Untuk mengatasi kesalahan, ikuti langkah-langkah berikut:

1. Buka AWS Lambda konsol di https://console.aws.amazon.com/lambda/.
2. Dari bilah navigasi, pada pemilih Wilayah, pilih Wilayah di mana Security Lake diaktifkan tetapi kueri Athena tidak mengembalikan hasil.

3. Dari panel navigasi, pilih Fungsi, dan pilih fungsi dari daftar berikut tergantung pada versi sumber:

   - `Source version 1 (OCSF 1.0.0-rc.2)` — SecurityLake _Lek_Partisi_Updater_Lambda_***#region>***fungsi.
   - `Source version 2 (OCSF 1.1.0)` – AmazonSecurityLakeMetastoreManager_***#region>***fungsi.

4. Pada tab Konfigurasi, pilih Pemicu.
5. Pilih opsi di sebelah fungsi, dan pilih Edit.
6. Pilih Aktifkan pemicu, dan pilih Simpan. Ini akan mengubah status fungsi menjadi Diaktifkan.

Tidak dapat mengakses AWS Glue tabel

Pelanggan akses kueri mungkin tidak dapat mengakses AWS Glue tabel yang berisi data Security Lake.

Pertama, pastikan bahwa Anda telah mengikuti langkah-langkah yang diuraikan. Menyiapkan berbagi tabel lintas akun (langkah pelanggan)

Jika pelanggan masih belum memiliki akses, ikuti langkah-langkah berikut:

1. Buka AWS Glue konsol di https://console.aws.amazon.com/glue/.
2. Dari panel navigasi, pilih Pengaturan Katalog Data dan Katalog.
3. Berikan izin kepada pelanggan untuk mengakses AWS Glue tabel dengan kebijakan berbasis sumber daya. Untuk informasi tentang membuat kebijakan berbasis sumber daya, lihat contoh kebijakan berbasis sumber daya di Panduan Pengembang. AWS GlueAWS Glue

Memecahkan masalah Organizations

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Security Lake dan AWS Organizations. Untuk topik pemecahan masalah Organizations lainnya, lihat bagian Pemecahan Masalah pada Panduan Pengguna.AWS Organizations

Terjadi kesalahan akses ditolak saat memanggil CreateDataLake operasi: Akun Anda harus merupakan akun administrator yang didelegasikan untuk organisasi atau akun mandiri.

Anda mungkin menerima kesalahan ini jika menghapus organisasi yang dimiliki oleh akun administrator yang didelegasikan dan kemudian mencoba menggunakan akun tersebut untuk menyiapkan Security Lake dengan menggunakan konsol Security Lake atau. CreateDataLakeAPI

Untuk mengatasi kesalahan, gunakan akun administrator yang didelegasikan dari organisasi lain atau akun mandiri.

Memecahkan masalah identitas dan akses Amazon Security Lake

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Security Lake danIAM.

Saya tidak berwenang untuk melakukan tindakan di Security Lake

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberi Anda kredensi Anda.

Contoh kesalahan berikut terjadi ketika `mateojackson` IAM pengguna mencoba menggunakan konsol untuk melihat detail tentang fiksi *`subscriber`* tetapi tidak memiliki izin `SecurityLake:`*`GetSubscriber`* fiksi.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 YOURSERVICEPREFIX:GetWidget on resource: my-example-widget
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk memungkinkannya mengakses *`subscriber`* informasi menggunakan `SecurityLake:`*`GetSubscriber`* tindakan tersebut.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Security Lake.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika IAM pengguna bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Security Lake. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Danau Keamanan saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Security Lake mendukung fitur-fitur ini, lihatBagaimana Security Lake bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke IAM pengguna lain Akun AWS yang Anda miliki di Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan IAM Pengguna.

- Untuk mempelajari cara menyediakan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna yang diautentikasi secara eksternal (federasi identitas) di Panduan Pengguna. IAM
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM

Bagaimana harga Security Lake ditentukan

Harga Amazon Security Lake didasarkan pada dua dimensi: konsumsi data dan konversi data. Security Lake juga bekerja dengan yang lain Layanan AWS untuk menyimpan dan membagikan data Anda, dan Anda mungkin dikenakan biaya terpisah untuk kegiatan ini.

Saat Anda mengaktifkan koleksi log untuk pertama kalinya di Akun AWS dalam setiap Wilayah AWS yang didukung Security Lake, akun itu secara otomatis terdaftar dalam uji coba gratis 15 hari Security Lake. Anda mungkin masih dikenakan biaya dari layanan lain selama uji coba gratis.

Untuk memahami metodologi di balik penetapan harga Security Lake, tonton video berikut: Harga Amazon Security Lake -->

Konsumsi data

Biaya-biaya ini berasal dari volume yang dicerna AWS CloudTrail log dan lainnya Layanan AWS log dan peristiwa (log kueri penyelesai Amazon Route 53, AWS Security Hub temuan, dan Amazon VPC Flow Logs).

Konversi data

Biaya-biaya ini berasal dari volume Layanan AWS log dan peristiwa yang dinormalisasi Security Lake ke Buka Kerangka Skema Keamanan Siber (OCSF) di Danau Keamanan skema dan mengonversi ke format Apache Parquet.

Biaya layanan terkait

Berikut adalah beberapa biaya yang mungkin Anda keluarkan dari yang lain Layanan AWS untuk menyimpan dan berbagi data di danau data keamanan Anda:

- Amazon S3 — Biaya ini berasal dari memelihara bucket Amazon S3 di akun Security Lake Anda, menyimpan data Anda di sana, serta mengevaluasi serta memantau bucket Anda untuk keamanan dan kontrol akses. Untuk informasi selengkapnya, lihat Harga Amazon S3.
- Amazon SQS — Biaya ini berasal dari membuat SQS antrian Amazon untuk pengiriman pesan. Untuk informasi selengkapnya, lihat SQSharga Amazon.
- Amazon EventBridge — Biaya ini berasal dari Amazon EventBridge mengirimkan pemberitahuan objek ke titik akhir berlangganan. Untuk informasi selengkapnya, lihat EventBridgeharga Amazon.

- AWS Glue — Biaya bulanan ditentukan oleh volume data log dan peristiwa yang dicerna dari AWS layanan per gigabyte. Data Anda disimpan di Amazon Simple Storage Service dan berlaku biaya Amazon S3 standar. Security Lake Lake juga mengatur AWS layanan atas nama Anda. Anda akan dikenakan biaya terpisah untuk AWS layanan yang digunakan dan sumber daya disiapkan sebagai bagian dari danau data keamanan Anda. Lihat harga untuk AWS Glue, Amazon EventBridge, AWS Lambda, Amazon SQS, dan Amazon Layanan Pemberitahuan Sederhana. Anda bertanggung jawab atas biaya yang Anda keluarkan dengan menanyakan data dari Security Lake dan menyimpan hasil kueri.

Biaya yang dikeluarkan pelanggan dengan menanyakan data dari Security Lake dan menyimpan hasil kueri adalah tanggung jawab pelanggan.

Untuk daftar lengkap biaya dan layanan tambahan, lihat harga Security Lake.

Meninjau penggunaan Security Lake dan perkiraan biaya

Halaman Penggunaan konsol Amazon Security Lake memungkinkan Anda meninjau penggunaan Security Lake saat ini, serta perkiraan penggunaan dan biaya di masa mendatang. Jika saat ini Anda berpartisipasi dalam uji coba gratis 15 hari, penggunaan Anda selama uji coba dapat membantu Anda memperkirakan biaya penggunaan Security Lake setelah uji coba gratis Anda berakhir. Untuk ikhtisar harga Security Lake, lihatBagaimana harga Security Lake ditentukan. Untuk informasi rinci dan contoh biaya, lihat Harga Amazon Security Lake.

Di Security Lake, perkiraan biaya penggunaan dilaporkan dalam Dolar AS dan hanya berlaku untuk saat ini Wilayah AWS. Biaya mencakup penggunaan Security Lake oleh semua akun di organisasi Anda dan termasuk konversi ke Open Cybersecurity Schema Framework (OCSF) dan format Apache Parquet. Namun, biaya yang diprediksi tidak termasuk biaya untuk layanan lain yang digunakan Security Lake, seperti Amazon Simple Storage Service (Amazon S3) dan AWS Glue.

Pada halaman Penggunaan, Anda memilih periode waktu untuk melihat data penggunaan dan biaya. Periode waktu default adalah 1 hari kalender terakhir. Anda harus memiliki setidaknya 1 hari penggunaan Security Lake untuk melihat proyeksi biaya.

Bagian atas halaman menunjukkan biaya yang diproyeksikan untuk semua akun. Ini adalah perkiraan biaya Security Lake Anda saat ini Wilayah AWS untuk 30 hari kalender berikutnya berdasarkan penggunaan aktual Anda selama jangka waktu yang dipilih. Penggunaan aktual dan perkiraan biaya mencerminkan semua akun di organisasi Anda.

Pada sisa halaman, data penggunaan dan biaya dibagi menjadi dua tabel sebagai berikut:

- Penggunaan dan biaya berdasarkan sumber — Ini adalah penggunaan Security Lake Anda saat ini yang dipecah berdasarkan sumber data, serta perkiraan penggunaan dan biaya untuk 30 hari kalender berikutnya berdasarkan penggunaan aktual Anda selama jangka waktu yang dipilih. Penggunaan aktual, prediksi penggunaan, dan perkiraan biaya mencerminkan semua akun di organisasi Anda. Jika Anda memilih sumber, panel terpisah akan terbuka yang menunjukkan akun mana yang menghasilkan log dan peristiwa dari sumber tersebut. Untuk setiap akun, panel split mencakup penggunaan aktual dari sumber itu dan prediksi penggunaan dan biaya.
- Penggunaan dan biaya berdasarkan akun — Ini adalah penggunaan Security Lake Anda saat ini yang dirinci berdasarkan akun, serta perkiraan penggunaan dan biaya untuk 30 hari kalender berikutnya berdasarkan penggunaan aktual Anda selama jangka waktu yang dipilih. Jika Anda memilih akun, panel terpisah akan terbuka yang menunjukkan sumber yang berkontribusi pada penggunaan akun tersebut. Untuk setiap sumber yang berkontribusi, panel terpisah mencakup penggunaan aktual dan prediksi penggunaan dan biaya.

Semua didukung AWS sumber data muncul di tabel sebelumnya, bahkan jika Anda belum menambahkan sumber tertentu di Security Lake. Kami merekomendasikan untuk menambahkan semua AWS sumber jika Anda berpartisipasi dalam uji coba gratis untuk mendapatkan perkiraan biaya untuk set lengkap log dan acara Anda. Untuk petunjuk tentang menambahkan AWS sumber, lihatMengumpulkan data dari Layanan AWS Danau Keamanan. Sumber kustom tidak termasuk dalam perhitungan penggunaan atau biaya.

Ikuti langkah-langkah ini untuk meninjau data penggunaan dan biaya Anda di konsol Security Lake.

Untuk meninjau penggunaan Security Lake dan perkiraan biaya (konsol)

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin meninjau penggunaan dan biaya Anda.
3. Di panel navigasi, pilih Pengaturan dan kemudian Penggunaan.
4. Pilih periode waktu yang ingin Anda lihat data penggunaan dan biaya. Defaultnya adalah 1 hari terakhir.
5. Pilih tab Berdasarkan sumber data atau Berdasarkan akun untuk meninjau penggunaan dan biaya secara detail.

Wilayah Danau Keamanan dan titik akhir

Untuk daftar Wilayah dan titik akhir layanan yang didukung untuk Security Lake, lihat titik akhir Amazon Security Lake di bagian. Referensi Umum AWS

Kami menyarankan Anda mengaktifkan Security Lake di semua yang didukung Wilayah AWS. Ini memungkinkan Anda menggunakan Security Lake untuk mendeteksi dan menyelidiki aktivitas yang tidak sah atau tidak biasa bahkan di Wilayah yang tidak Anda gunakan secara aktif.

Menonaktifkan Danau Keamanan

Saat Anda menonaktifkan Amazon Security Lake, Security Lake berhenti mengumpulkan log dan peristiwa dari AWS sumber Anda. Pengaturan Danau Keamanan yang ada dan sumber daya yang dibuat di Akun AWS Anda dipertahankan. Selain itu, data yang Anda simpan atau publikasikan ke orang lain Layanan AWS, seperti data sensitif dalam AWS Lake Formation tabel dan AWS CloudTrail log, tetap tersedia. Data yang disimpan di bucket Amazon Simple Storage Service (Amazon S3) tetap tersedia sesuai dengan siklus hidup penyimpanan Amazon S3 Anda.

Menonaktifkan Security Lake dari halaman Pengaturan di konsol Security Lake menghentikan pengumpulan AWS log dan peristiwa Wilayah AWS di semua tempat Security Lake saat ini diaktifkan. Anda dapat menggunakan halaman Wilayah di konsol untuk menghentikan pengumpulan log di Wilayah tertentu. Danau Keamanan API dan AWS CLI juga menghentikan pengumpulan log di Wilayah yang Anda tentukan dalam permintaan Anda.

Jika Anda menggunakan integrasi dengan AWS Organizations dan akun Anda adalah bagian dari organisasi yang mengelola beberapa akun Security Lake secara terpusat, hanya administrator Security Lake yang didelegasikan yang dapat menonaktifkan Security Lake untuk dirinya sendiri dan untuk akun anggota. Namun, meninggalkan organisasi menghentikan pengumpulan log untuk akun anggota.

Saat Anda menonaktifkan Security Lake untuk organisasi, penunjukan administrator yang didelegasikan akan dipertahankan jika Anda mengikuti instruksi penonaktifan yang disediakan di halaman ini. Anda tidak perlu menunjuk administrator yang didelegasikan lagi sebelum Anda dapat mengaktifkan kembali Security Lake.

Untuk sumber kustom, saat menonaktifkan Security Lake, Anda harus menonaktifkan setiap sumber di luar konsol Security Lake. Kegagalan untuk menonaktifkan integrasi akan mengakibatkan integrasi sumber terus mengirim log ke Amazon S3. Selain itu, Anda harus menonaktifkan integrasi pelanggan atau pelanggan masih dapat mengkonsumsi data dari Security Lake. Untuk detail tentang cara menghapus sumber kustom atau integrasi pelanggan, lihat dokumentasi masing-masing penyedia.

> **Important**
>
> Anda harus menghapus AWS Glue database sebelum mengaktifkan kembali Security Lake untuk memastikan kueri berfungsi dengan baik.

Saat Security Lake diaktifkan kembali, bucket Amazon S3 data lake baru dibuat dan data dikumpulkan di bucket S3 baru ini. Jika sebelumnya Anda telah menghapus AWS Glue tabel, satu set AWS Glue tabel baru akan dibuat.

Semua data yang dikumpulkan sebelum menonaktifkan Security Lake akan tetap berada di bucket Amazon S3 lama. Jika Anda ingin menanyakan data lama, Anda harus memindahkannya ke bucket baru menggunakan perintah Amazon S3`Sync`. Untuk detail selengkapnya, lihat perintah Sync di AWS CLI Command Reference.

Topik ini menjelaskan cara menonaktifkan Security Lake dengan menggunakan konsol Security Lake, Security LakeAPI, atau AWS CLI.

Console

1. Buka konsol Security Lake di https://console.aws.amazon.com/securitylake/.
2. Di panel navigasi, pada Pengaturan, pilih Umum.
3. Pilih Nonaktifkan Danau Keamanan.
4. Saat diminta konfirmasi, masukkan**`Disable`**, lalu pilih Nonaktifkan.

API

Untuk menonaktifkan Security Lake secara terprogram, gunakan DeleteDataLakeOperasi Danau API Keamanan Jika Anda menggunakan AWS CLI, jalankan delete-date-lakeperintah. Dalam permintaan Anda, gunakan `regions` daftar untuk menentukan kode Wilayah untuk setiap Wilayah di mana Anda ingin menonaktifkan Security Lake. Untuk daftar kode Wilayah, lihat titik akhir Amazon Security Lake di. Referensi Umum AWS

Untuk penggunaan Security Lake AWS Organizations, hanya administrator Security Lake yang didelegasikan untuk organisasi yang dapat menonaktifkan Security Lake untuk akun di organisasi.

Misalnya, AWS CLI perintah berikut menonaktifkan Security Lake in the `ap-northeast-1` and `eu-central-1` Regions. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securitylake delete-data-lake \
--regions "ap-northeast-1" "eu-central-1"
```

Riwayat dokumen untuk Panduan Pengguna Amazon Security Lake

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir Amazon Security Lake. Untuk pemberitahuan tentang pembaruan dokumentasi ini, Anda dapat berlangganan RSS umpan.

Pembaruan dokumentasi terbaru: 01 Desember 2024

Perubahan	Deskripsi	Tanggal
Fitur baru	Security Lake sekarang mendukung permintaan langsung OpenSearch Layanan untuk menganalisis data di Security Lake. Untuk detail selengkapnya, lihat Integrasi dengan OpenSearch Layanan.	Desember 1, 2024
Peran terkait layanan baru	Kami menambahkan peran terkait layanan baru. `AWSServiceRoleForSecurityLakeResourceManagement` Peran terkait layanan ini memberikan izin kepada Security Lake untuk melakukan pemantauan berkelanjutan dan peningkatan kinerja, yang dapat mengurangi latensi dan biaya.	November 14, 2024
Ketersediaan regional	Danau Keamanan sekarang tersedia di AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat). Wilayah	Juni 10, 2024

	AWS Untuk daftar lengkap Wilayah di mana Security Lake saat ini tersedia, lihat titik akhir Amazon Security Lake di Referensi Umum AWS.	
Memperbarui ke kebijakan terkelola yang ada	Kami menambahkan AWS WAF tindakan ke kebijakan AWS terkelola untuk `SecurityLakeServiceLinkedRole` kebijakan tersebut. Tindakan tambahan memungkinkan Security Lake untuk mengumpulkan AWS WAF log, ketika diaktifkan sebagai sumber log di Security Lake.	22 Mei 2024
Sumber AWS log baru	Security Lake menambahkan AWSWAFlog sebagai sumber AWS log. AWS WAF membantu Anda memantau permintaan web yang dikirim pengguna akhir ke aplikasi.	22 Mei 2024
Memperbarui ke kebijakan terkelola yang ada	Kami menambahkan SID tindakan ke `AmazonSecurityLakePermissionsBoundary` kebijakan.	13 Mei 2024

Memperbarui ke kebijakan terkelola yang ada	Kami memperbarui AmazonSecurityLake MetastoreManagerkebijakan untuk menambahkan tindakan pembersihan metadata yang memungkinkan Anda menghapus metadata di data lake Anda.	Maret 27, 2024
Versi sumber baru	Perbarui izin peran Anda untuk mencerna data dari versi sumber data baru.	Februari 29, 2024
Sumber AWS log baru	Security Lake menambahkan Log EKS Audit sebagai sumber AWS log. EKSLog Audit membantu Anda mendeteksi aktivitas yang berpotensi mencurigakan di EKS cluster Anda dalam Amazon Elastic Kubernetes Service.	Februari 29, 2024
Memperbarui ke kebijakan terkelola yang ada	Kami memperbarui kebijakan untuk mengizinkan `iam:PassRole` `AmazonSecurityLakeMetastoreManagerV2` peran baru dan memungkinkan Security Lake menyebarkan atau memperbarui komponen data lake.	Februari 23, 2024

Kebijakan terkelola baru	Kami menambahkan kebijakan AWS terkelola baru, `AmazonSecurityLakeMetastoreManager` kebijakan. Kebijakan ini memberikan izin kepada Security Lake untuk mengelola metadata di data lake Anda.	23 Januari 2024
Ketersediaan regional	Security Lake sekarang tersedia sebagai berikut Wilayah AWS: Asia Pasifik (Osaka), Kanada (Tengah), Eropa (Paris), dan Eropa (Stockholm). Untuk daftar lengkap Wilayah di mana Security Lake saat ini tersedia, lihat titik akhir Amazon Security Lake di Referensi Umum AWS.	26 Oktober 2023
Fitur baru	Anda sekarang dapat mengedit pengaturan tertentu untuk pelanggan dengan akses kueri. Anda juga dapat menetapkan tag ke sumber daya Security Lake untuk Anda Akun AWS.	Juli 20, 2023

Kebijakan terkelola baru	Security Lake menambahkan kebijakan AWS terkelola baru, `AmazonSecurityLakeAdministrator` kebijakan tersebut. Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh utama ke semua tindakan Security Lake.	30 Mei 2023
Ketersediaan umum	Danau Keamanan sekarang tersedia secara umum.	30 Mei 2023
Fitur baru	Security Lake sekarang mengirimkan metrik ke Amazon CloudWatch.	4 Mei 2023
Ketersediaan regional	Security Lake sekarang tersedia sebagai berikut Wilayah AWS: Asia Pasifik (Singapura), Eropa (London), dan Amerika Selatan (São Paulo).	22 Maret 2023
Fitur baru	Security Lake sekarang membuat peran AWS Identity and Access Management (IAM) atas nama Anda saat Anda menggunakan konsol Security Lake untuk mengaktifkan dan mulai menggunakan Security Lake.	15 Februari 2023
Rilis awal	Ini adalah rilis awal Panduan Pengguna Amazon Security Lake.	29 November 2022

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.