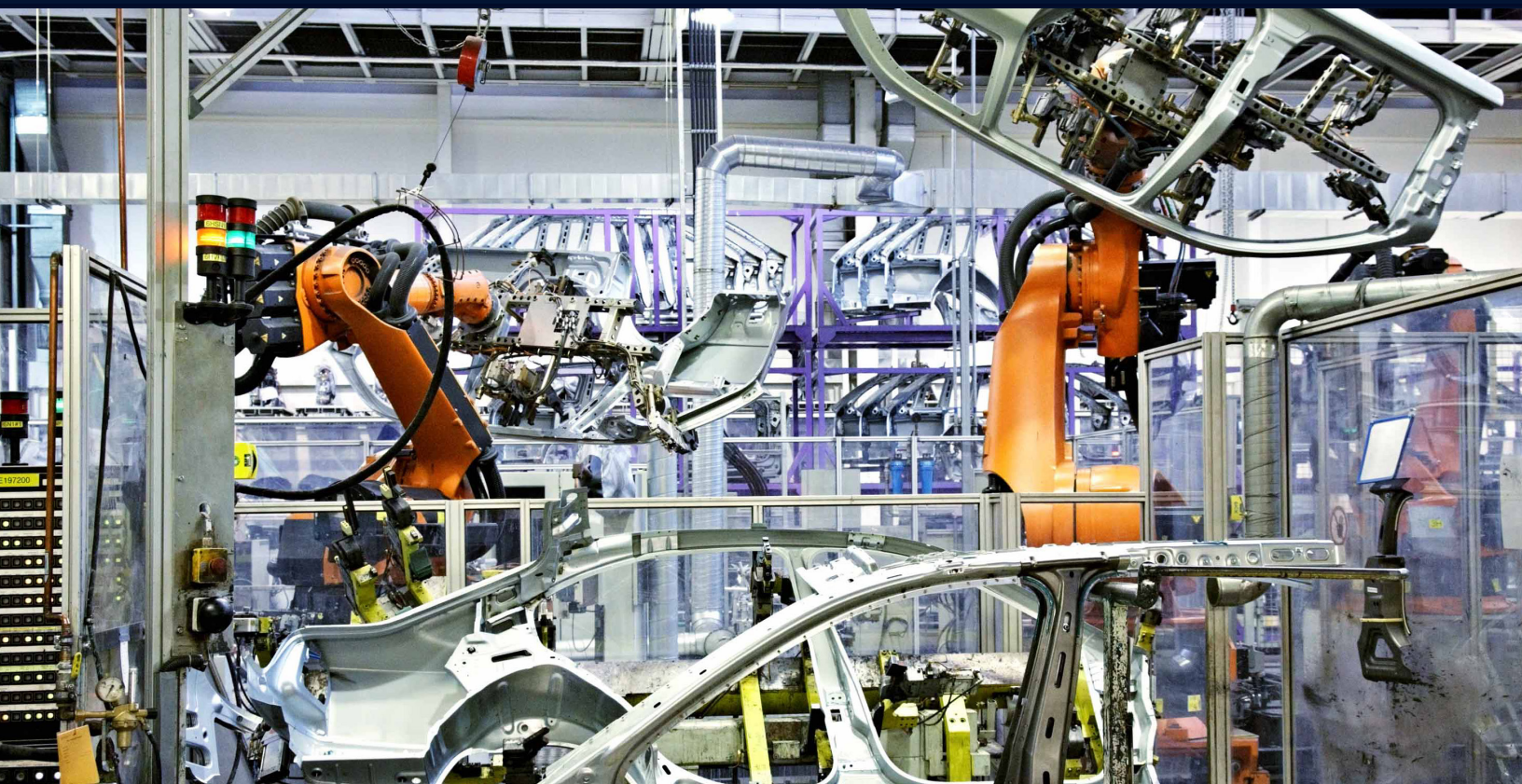
sumo logic | Continuous Intelligence Platform™

ホワイト ペーパー

製造業者の障害となる 5 つのインテリジェンス ギャップ

最適なユーザ エクスペリエンスとアプリケーションの信頼性を確保するためのリアルタイムかつ実用的なインサイト



製造企業は、ビジネスで何が起きているかをリアルタイムで把握することで、スピーディかつ的を射た対応をする必要があります。好調な製造企業は、デジタル ビジネスの成功に欠かせない 5 つの要件を満たしています。これらの企業はシステムの複雑さとデータ量の増加にうまく対処でき、デジタル ビジネスの成功を阻む 5 つのインテリジェンス ギャップを埋めることに成功しています。

成功のための位置づけ

今や、インダストリー 4.0 (第 4 次産業革命) は製造業にしっかりと根づいています。それに向けて移行を開始した製造企業では、すでにビジネス成果の改善が見られています。産業用ソフトウェア スタックにおけるイノベーションに伴い、高度な予測分析、人工知能、機械学習、接続性(Wi-Fi、RFID、5Gなど)、エッジコンピューティング、産業用モノのインターネット(IIoT)向けのアプリケーションが登場しています。これらのアプリケーションが製造企業の業績を向上させる貴重なアセットになることは明らかです。製造企業がクラウド ソリューションのパフォーマンスと可用性について今でも抱いている懸念は、5G とエッジ コンピューティングによって取り除かれます。

製造業界のリーダーたちはインダストリー 4.0 のテクノロジーをいち早く導入し、成功を収めています。これらの新しいテクノロジーを導入することで、デジタル トランスフォーメーションの技術的側面を効果的に管理するうえで前提となる、組織の硬直性の克服に成功したのです。組織の硬直を克服して、アジャイルに業務に取り組み、水準を維持し、学習する文化を確立することにより、高度なユース ケースを製造工場に導入し、バリュー チェーンをエンドツーエンドでつなげて、新たなオペレーティング システムを製造ネットワークの他の工場に拡張しています。COVID-19 の影響により、アクセスと制御を広範囲に拡げて「場所を問わずどこからでも作業できる」モデルを実現させる必要性が明らかになりました。

IIoT プラットフォームを導入すると、一元化されたリアルタイム データに必要に応じていつでもアクセスでき、最前線での問題解決とコラボレーションを強化できます。今や最前線のチームは、マシンベースのデータを自己診断して意思決定を行うことができます。新しいテクノロジーを活用すると、製造企業とバリュー チェーン パートナーが「スマートなバリュー チェーン」において連携し、注文から配送までのカスタマー エクスペリエンスを改善できます。リアルタイムでデータを交換できるので、需要の変化に迅速かつ効果的に対応できます。データ サイエンスと高度な予測型分析を使用し、これらのプロセスを共有することで、さらに最適化できます。

インダストリー 4.0 のテクノロジーを導入する際の障壁が取り除かれ、製造業でそのメリットが認識されつつある中、製造企業にとって、テクノロジーとデータを統合して高度なユース ケースを工場に導入し、エンドツーエンドでバリュー チェーンをつなげて新しいシステムを製造ネットワークの他の工場に拡張するには、今が絶好のチャンスです。つまり、製造企業が複雑さとデータ量の増加に対処し、成功の妨げとなる 5 つのインテリジェンス ギャップを解決するには、ビジネスの現状を直ちに把握してスピーディかつ的を射た対応をする必要があります。

最新型のアプリケーション アーキテクチャ

最新型のアプリケーション アーキテクチャを目指す道のりで最初のインテリジェンス ギャップ、つまりデジタル ビジネス成功の最初の要件を発生させるのは、コンポーネント化されたアプリケーションです。より迅速かつ柔軟にソフトウェアを作成してデプロイするには、最新型 IIoT アプリケーションに、リアルタイムで構築/再構築される新しいソフトウェア アーキテクチャが必要です。ワークロードが小さなコンポーネントに分かれて複数のクラウド環境に分散しているので、複雑さがさらに増します。導入されるコンポーネントの数が増えるにつれて、より多くのシステムとシグナルをコンテキストに応じて管理し分析する必要が生じます。多くの場合、開発者自身がパイプラインのモニタリングとトラブルシューティングを行う羽目になり、重要な収益源であるアプリケーション機能やリリースのための作業から時間が奪われます。DevOps チームが新しいアプリケーションと API を導入したり既存のアプリケーションを更新したりする際にマイクロサービス、Kubernetes、AWS Lambda、AWS Kinesis、その他の最新型インフラストラクチャを活用し始めるにつれて、この問題は指数関数的に増大します。Sumo Logic の Continuous Intelligence Platform を利用すると、製造企業はより迅速に品質改善を実施し、複雑な IIoT プラットフォームとサービスをより適切に管理できます。

マルチクラウドの採用

第 2 のインテリジェンス ギャップを生じさせるのは、マルチクラウド環境での操作の複雑さです。製造企業には、マルチクラウド インフラストラクチャで分散アプリケーション ワークロードを実行してスケーラビリティ、柔軟性、コスト効果を向上させ、コストを最適化する能力が必要です。ところが、マルチクラウドの採用で無秩序なデジタル拡散がさらに加速されます。その原因となっているのは、部分的な表示機能しかなく、リアルタイムで操作できず、クラウド環境のスケーラビリティもない、サイロ化されたアーキテクチャと管理ツールです。Sumo Logic Continuous Intelligence Platform は単一のペインを使用して、混合アーキテクチャ全体にわたる多数のユース ケースをリアルタイムで可視化します。これにより製造企業は問題を迅速に診断してトラブルシューティングし、サービスの中断を削減できます。

継続的セキュリティ

第 3 のインテリジェンス ギャップとなるのは、境界のないデジタル環境を保護することの複雑さです。製造企業が最新型の脅威を食い止めるには、常にデータを保護するとともに、人工知能と機械学習テクノロジーに備わる能力も必要です。境界のないデジタル フットプリント全体に攻撃領域が広がるにつれて、セキュリティの複雑さは増大します。しかし大抵の製造企業では必要なだけの熟練アナリストやクラウドネイティブなツールが不足しています。そのような状態で、この新たに生まれた分野を保護し、次々と押し寄せる最新型の巧妙な攻撃に対処し続けながら、しかも「アラート疲弊」と闘うのは至難の業です。Sumo Logic Continuous Intelligence Platform を活用すると、製造企業は脅威の検出と対応を自動化および高速化し、本当の脅威をノイズからフィルタリングできます。

「ABin Bev は世界最大規模のビール会社です。弊社で使用している最新型のインフラストラクチャは、まさにクラウドとマイクロサービスの最先端にあります。弊社がデジタル トランスフォーメーションを進める中で、Sumo Logic はセキュリティ上の懸念に対処できるよう支援してくれます。そのおかげで、グローバル セキュリティ オペレーション センター (SOC) を構築してダッシュボードとメトリクスからリアルタイムのセキュリティ インサイトを引き出すことが可能になり、組織内でセキュリティの価値を明示するのに役立っています。」

継続的コラボレーション

第 4 のインテリジェンス ギャップを生じさせるのは、分散したツールがもたらすサイロ化したデータです。これによりチームの効率的なコラボレーションが阻害されます。各チームが時代遅れのサイロ化されたシステムを使用していると、コラボレーションは大きな課題に直面します。そのようなシステムではデータを部分的にしか見られず、組織全体で何が起きているかを把握するためのリアルタイムのコンテキストが得られないからです。製造企業には、信頼できる 1 つの情報源から多数のユース ケースにコンテキストを提供する、インテリジェンスとインサイトを得る能力が必要です。これによって、コラボレーションに基づく思考や意思決定が可能になります。Sumo Logic を使用すると、製造企業のチームは、信頼できる 1 つの情報源 (最新型アプリケーション) からコンテキスト付きインサイトを得てオペレーションを行い、スピーディに意思決定できるようになります。

データ駆動型インテリジェンス

製造企業には、ログ、メトリクス、トレース、イベント、メタデータ、その他のテレメトリとして生成される大量のマシンデータからリアルタイムのインサイトとビジネス価値を引き出す能力が必要です。圧倒的な量のデータが蓄積されていく中、企業はそれを保管して保護する必要性だけでなく、そこから価値を引き出す能力の不足もしばしば実感しています。Sumo Logic Continuous Intelligence Platform を活用すると、製造企業は自社データをリアルタイムの価値に変換できます。これはビジネスの成功と競争優位に寄与し、多数のユース ケースにわたるさまざまなインテリジェンス ニーズを満たしてくれるでしょう。

製造企業向けの最新型アナリティクスとセキュリティ検出プラットフォーム

Sumo Logic は、製造企業が直面する課題に対処するマシン データ アナリティクス プラットフォームを提供しています。オンプレミス環境とハイブリッド環境にまたがるログ、イベント、パフォーマンス メトリクスなどすべてのマシン データを統合することで、Sumo Logic は IT オペレーション、DevOps、SRE、セキュリティ、エンジニアリングの各チームにリアルタイムのセキュアな統合アラートとダッシュボードを提供し、問題の特定とトラブルシューティングを加速させ、回復および解決までの時間を短縮できるようにします。Sumo Logic により、組織は新しいテクノロジーに迅速に移行してそれを導入できます。したがって、製造企業は顧客向け製品の開発に時間を割くことができ、インフラストラクチャ管理の時間を節約できます。

Sumo Logic のスケーラブルでセキュアなプラットフォームは 800 ペタバイトを超えるデータを処理/分析し、1 日に 1600 兆件を超えるレコードおよび 1 か月に 27 エクサバイトをスキャンし、2,100 社を超えるお客様にサービスを提供しています。Sumo Logic プラットフォームには以下の特長があります。

- **AWS ネイティブ:** 低 TCO、ゼロ マネジメントのセルフプロビジョニング マルチテナント SaaS。
- **スケーラブル:** ユーザ数やリアルタイム ダッシュボードの数に制限がなく、トラブルシューティング スピードを損なわない任意の量のデータの取り込みと分析。
- **高度なアナリティクスと機械学習:** 異常の検出と未知の問題の顕在化による MTTI 削減、パターン検出による迅速なトラブルシューティングと MTTR 削減。
- **価値実現までの時間の削減:** 20 以上の AWS サービスと 400 以上の一般的なテクノロジのための、すぐに使える統合と事前構築ダッシュボード
- **高度にセキュアなサービス:** PCI/DSS、ISO 27001、GDPR などにすぐに使える認証。セキュリティ キー ローテーションによる保存中および転送中のデータ暗号化。
- **柔軟なライセンス モデル:** 平均データ容量、季節変動パターン、データ関連性に基づくアナリティクスのタイプを考慮に入れたライセンス管理 (低頻度で分析される Dev/Test データには、リアルタイムまたは常時のモニタリング/アラートを利用する運用データよりも安価な料金を設定)

AWS でプラットフォームを構築している製造企業向けに、Sumo Logic はすぐに使える AWS Observability ソリューションを提供します。そのメリットを活用すると、ALB、EC2、RDS、Lambda、DynamoDB、API Gateway などの重要な AWS サービス全体にわたる統合可視性が得られます。AWS Observability ソリューションは多数の AWS アカウント、リージョン、サービスからログとメトリクスを収集し、データを自動的にタグ付けして機械学習ベースの根本原因分析を適用することで、異常を顕在化させます。これによりコンテキスト情報が得られ、ユーザは重要なログ、メトリクス、トレース データを見比べることで、発生している事象の内容、場所、原因をより少ない労力で特定できます。

製造企業のプラットフォームのサイバーセキュリティ体制を強化するため、Sumo Logic は Cloud SIEM を提供しています。これはコンテキストに応じた脅威データを優先順位づけしてセキュリティ アナリストに提供するソリューションです。Sumo Logic Cloud SIEM は、セキュリティ アナリストの効率とリスク軽減能力を妨げている一般的な技術的制限を取り除いてくれます。アラートのトリアージ処理を自動化することで、Sumo Logic はすべてのレコードを確実に分析して、インサイトを顕在化させます。インサイトはセキュリティ アナリストに知見を与える重要な出力であり、こうしてビジネス上極めて重要な脅威に時間と注意を集中できます。

ケース スタディ: Clorox

Clorox は、世界 25 か国以上で事業を展開し、83 以上の施設、33 か所の工場で約 8,800 人の従業員を抱える 60 億ドル規模のグローバルな消費財 (CPG) 企業です。同社のコンピューティング環境を構成する約 1,400 ～ 1,500 の Windows サーバでは、2003 から 2019 までさまざまなバージョンの Windows が稼働しています。各施設では約 300 台の Linux サーバがインターネット直接接続しており、ファイアウォールが導入されています。管理対象の約 7,500 台の PC のほとんどは Windows ラップトップ PC であり、約 200 台は Mac です。

Clorox は、ニーズと要件に柔軟に対応できる、最新型のセキュリティ/コンプラアンス ソリューションを求めていました。サービスの一部として SIEM を使用するマネージド セキュリティ プロバイダーから移行するにあたり、Clorox は SIEM ソリューションの中の何が不要なのか、また何が本当に必要なのかをよく理解できました。同社はクラウド SIEM 分野の大手プロバイダーをいくつか評価し、30 日以上にわたる概念実証を行いました。本番環境の実際のデータを使用した直接比較に基づいて Clorox が選択したのは、1 日あたり約 250 ギガバイトのデータを取り込んで、12 か月分のデータを保存できるよう調整された Sumo Logic の Cloud SIEM Enterprise です。さらに、同社は Sumo Logic の Special Operations サービスにもサブスクライブしました。

Sumo Logic を選択した理由

データ (次世代アンチウイルス、EDR ソリューション、シングル サインオン、ファイアウォール ログ、サーバ ログ、クラウド サービス ログ、Web プロキシ ログなど) をプラットフォームに取り込む作業は単純でした。カスタマイズしたり追加したりしたダッシュボードやメトリクスもありましたが、ほとんどはそのまま利用できたので、導入は迅速かつ簡単でした。Clorox チームはどんなデータが必要となるかを理解し、いくつかの重要な分野ですばやく価値を実現することができました。

アラート削減 - 長期間、複数テクノロジーにわたるイベントの相関付け

同社が採用していたマネージド セキュリティ ベンダーでは、すべての処理が単一イベントに基づいていました。相関はありませんでした。「偽陽性」であれ本当のアラートであれ、すべてのイベントのアラートが Clorox チームに表示されました。以前に導入していたネットワーク脅威検知 (NTD) プラットフォームでは、疑わしいログに対して、事前スコアと実際の処理後の最終スコアという 2 段階スコア付けが行われていました。初期デフォルト ルール セットは初期スコアに基づいていました。中には、1 時間で約 2,500 件のインサイトを生成する初期ルールもありました。

Sumo に移行し、Clorox チームは Sumo Logic Spec Ops を使用して SIEM とプロトタイプ ルールを調整しました。脅威インテリジェント ソースからデータを追加し、価値あるインテリジェンスを提供する優れたソースをふるいに掛けました。その結果、チームが対処すべきノイズが大幅に減り、インサイトが拡充され、アラートが管理可能な現実的な量に減りました。

異常検出

Clorox チームは、一般的なマルウェアと既知の脅威に対するアラートを受け取るだけでなく、異常検出に基づく貴重なインサイトも得られるようになりました。以前は異常を検出する適切な構造、ツール、プロセスが導入されていなかったため通常は Clorox チームが見逃していたような異常も、Sumo Logic で発見できるようになりました。たとえば、一連のイベントが発生した結果として疑わしい状況が生じると、ルールが発動され、アラートが出ることがあります。たとえば PowerShell がコマンド プロンプトを呼び出してスクリプトを実行し、そのスクリプトが Base64 エンコーディングを使って自身を隠すような状況です。

ダッシュボード機能とレポート機能

SIEM を操作して構成する中で、Clorox チームは同社のスタックから複数のダッシュボードと複数のテクノロジーを使って Sumo Logic にデータを送りました。Clorox が重点的に取り組んだことは、Sumo Logic のダッシュボード機能とレポート機能を使って 1 つの脅威管理ダッシュボードを作り、チームが関心を持つ脅威情報 (次世代アンチウイルス、Web プロキシ、NTD ソリューションなど) をそのダッシュボードに一元化することです。こうすれば、脅威管理ダッシュボードの概要情報から、Web プロキシや次世代アンチウイルスなど個々のコンポーネントに関する深いインサイトを得られるので、Clorox チームは出されたアラートのコンテキストを理解できます。

「Sumo Logic ダッシュボードを使えば、たくさんの干し草の山から針を見つけるように情報を見つけることもできます。干し草の山は 1 つではなく、たくさんです。1 つならとても簡単です。1 つ 1 つは小さな干し草の山です。」

Clorox

Gary Conner 氏
上級脅威保護担当リーダー

セキュリティを超えて

Sumo を実装する中で、Clorox チームはセキュリティ ユース ケースに留まらない直接的で大きな価値を見い出し、特に管理/運用向けのカスタム ダッシュボードを作成しました。管理向けダッシュボードでは、経営幹部が見たいと思ういくつかの特定のテクノロジーの状況が月別ビューに表示されます。これにより、レポートを毎月まとめて整理する必要がなくなったので、かなりの時間を節約できました。Sumo により、マネージャーはダッシュボードを表示してボタンをクリックするだけで、必要なデータをリアルタイムで取得できるようになりました。経営幹部も履歴データを見て、日、週、月単位で状況を把握したり、特定期間における改善状況を確認したりできます。

システムに統合されたカスタム ダッシュボード、検索機能、クエリ機能のおかげで、Clorox は特定のコンポーネントごとにルールを作成しなくても、全体的な状況をより適切に把握できるようになりました。チームはログからメトリクスへの変換を通じてカスタム メトリクスをシステムに取り込むことができるようになり、ファイアウォールのレイテンシや、ping テストでシステムがパケットをドロップしているかどうかについてインサイトが得られるようになりました。いくつかのダッシュボードとメトリックはそのまま利用できなかったので、カスタマイズして追加する必要がありましたが、Sumo Logic のプラットフォームに備わる機能を使って迅速かつ簡単に終わりました。

COVID-19 と IT オペレーション

Clorox のチームが Sumo Logic で PoC を開始したのは、COVID-19 が拡大し始めて全員がリモート作業に移行した 2020 年 2 月のことです。リモート アクセス環境がどれほどうまく動作しているかを確認する必要がありました。運用データはすでに Sumo Logic に移行されていたので、Clorox チームはファイアウォール データと VPN データを使って簡単なダッシュボードを組み立てました。運用部門と経営幹部はこのダッシュボードを使用して、システムに接続しているユーザの数と、ユーザがどのようにシステムを使用しているかを簡単に把握できるようになりました。ダッシュボードとカスタム メトリクスに基づき、Clorox チームは問題を予測し、クエリを作成してそれをサービス デスク担当員に渡すことで、問題に迅速に対処できます。

元々内在する価値と、それを超える価値

データを取り込み、そのデータから真のインサイトを引き出してアラートにコンテキストを付加できるようになった Clorox チームは、そのことに大きな、そして直接的な価値を見い出しました。Sumo Logic プラットフォームに備わる柔軟性と能力により、以前は見えなかったような情報が明らかになり、対処できるようになりました。既成の枠組みにとらわれずに考えることを目指す Clorox のセキュリティ チームは、運用担当者と連携し、Sumo Logic の継続的インテリジェンス プラットフォームを使用してセキュリティ/運用データを共有しました。

製造業者にとってのメリット

SumoLogicは継続的なインサイトを提供することで、製造企業が IIoT プラットフォームの運用上およびセキュリティ上の問題を検出、特定、解決するための時間を削減できるようにします。Sumo Logic を利用すると、製造企業には以下のメリットが得られます。

- DevSecOps のモニタリングを一元化し、プラットフォームの問題を特定して解決するための時間を削減することにより、シームレスなユーザ エクスペリエンスが確保され、ユーザ自身のためにもなります。Sumo Logic は、アプリケーションから生成される多数のログとメトリクスを分析し、ダッシュボード、アラート、機械学習によるパターン検出を提供してトラブルシューティングの時間を削減します。
- CI/CD パイプラインの信頼性を確保することにより、アプリケーションのビルドと実用開始のサイクルを加速できます。Sumo Logic はコード リポジトリ、自動化フレームワークなどのパイプライン パーツの信頼性を継続的にモニタリングすることで、エンジニアたちがインフラストラクチャの管理ではなくイノベーションに注力できるようにします。
- セキュリティ侵害をより迅速に検出してそれに対応し、脅威ハンティングを高速化し、アラートによるセキュリティ アナリストの疲弊を軽減します。Sumo Logic は AWS CloudTrail、AWS GuardDuty、その他の情報源からのセキュリティ イベントを分析し、重要な脅威を見逃さないように脅威レベルに従ってそれを分類します。
- 継続的なコンプライアンスを確保します。コンプライアンス制御をモニタリングして自動化することにより、PCI/DSS、SOC2、および GDPR の要件や監査に適合できるように支援します。Sumo Logic は、ログにしばしば誤って保存される個人識別情報（PII）を製造企業が特定して処理できるようにします。

「Sumo Logic は本当に変化を促し、当社が成長するうえで重要な役割を果たしてくれました。IoT ではユーザ数が数千から何百万、何億にも増えていくからです。当社はまず開発オペレーションで Sumo Logic を使い始めましたが、やがて広く採用し、今では 95% のユーザがダッシュボードを活用して価値を引き出し、組織内のさまざまな機能分野でデータを利用しています。」

Samsung SmartThings 社

Sumo Logic について

SumoLogicInc.(NSDQ:SUMO)は、ソフトウェアの新しいカテゴリである継続的インテリジェンスのパイオニアです。継続的インテリジェンスは、あらゆる規模の組織がデジタル トランスフォーメーション、モダン アプリケーション、およびクラウド コンピューティングによって生じるデータの課題に対応したり、それによってもたらされる機会を活用したりするのに役立ちます。Sumo Logic Continuous Intelligence Platform は、アプリケーション、インフラストラクチャ、セキュリティ、および IoT のデータの収集、取り込み、分析を自動化して、わずか数秒で実用的なインサイトを導き出します。世界中の 2,100 社を超えるお客様が、Sumo Logic を使用して最新型のアプリケーションとクラウド インフラストラクチャを構築、実行、保護しています。Sumo Logic のプラットフォームだけが、多数のユース ケースを扱う真のマルチテナント SaaS アーキテクチャです。これを活用すると企業はインテリジェンス エコノミーで成功を収められます。詳細については、www.sumologic.com/manufacturing を参照してください。

s u

Continuous Intelligence Platform™

m o

sumo logic

フリーダイヤル: 1.855.LOG.SUMO | **国際電話:** 1.650.810.8700
305 Main Street, Redwood City, CA 94603

www.sumologic.com

2021 年 03 月更新