sumo logic

CASE STUDY

"With hundreds of millions of customers, any security breach would be devastating. There's simply no way that we could hire enough analysts to manually carry out the hard work of protecting sensitive user information that Sumo Logic does for us automatically."

John Visneski

Director of Information Security and Data Protection Officer

Challenge

In response to the unprecedented success of the Pokémon Go app, The Pokémon Company International (Pokémon) determined that it was time to bring the game's development in-house. A major part of this venture was migrating much of the company's technology stack to Amazon Web Services (AWS), and then establishing it as a core platform to support many other usages. For this project to succeed, it was also vital that the company fashion a top-tier security operations center (SOC).

Solution

After examining a number of alternatives, the company standardized on Sumo Logic's born-in-the-cloud technologies to ingest and organize machine data from across its entire AWS portfolio. This also encompassed adopting a comprehensive set of dashboards, alerts, and other automated tools to continually monitor the threat landscape, which was bolstered by new, cooperative processes between the InfoSec team and business users.

Results

By centralizing its machine data into Sumo Logic and applying automated responses to the vast majority of potential security incidents, Pokémon substantially enhanced its reactive capabilities. Beyond strengthening the company's overall security, Sumo Logic has helped slash the amount of time necessary to conduct critical business operations.

The History

Originally launched in Japan in 1996, Pokémon has mushroomed to become a global entertainment juggernaut. Around the world, hundreds of millions of people - from toddlers to seniors - eagerly follow the exploits of more than 800 characters such as Pikachu, Charmander, Jigglypuff, and Squirtle. Pokémon was established to oversee the property outside of Asia, and carries out responsibilities such as:

Industry

Entertainment

Headquarters

Bellevue, Washington, United States

Size

501 – 1,000 employees

Use cases

Security

"We're committed to applying the OODA loop whenever possible. AWS, Sumo Logic, and other third-party tools all work together quickly and smoothly. This lets us dedicate our security analysts to scrutinize our most formidable issues, rather than wasting time on tasks that automation can address."

John Visneski

Director of Information Security and Data Protection Officer

- Brand management
- Marketing
- Licensing
- Home entertainment
- The official Pokémon website
- The animated Pokémon TV series
- The Pokémon Trading Card game

In 2016, the company unveiled Pokémon Go, an immersive augmented reality mobile app that transformed interactive gaming. Initially, the company expected that it would be downloaded between 50 and 100 million times. However, Pokémon Go quickly became an international cultural phenomenon: by early 2019 the total number of downloads surpassed one billion.

Pokémon Go was actually created by Niantic, a licensed third-party software company, but as the game continued its explosive growth Pokémon determined that the time had arrived to bring development in-house. This was to be a far bigger undertaking than merely shifting the obligations for maintaining the application. Instead, the company was committed to a thorough digital transformation that would require a fresh approach to the people, processes, and technologies that conducted its operations. For example, Pokémon's technical organization expanded by a factor of ten to include an IT team, game developers, project managers, and DevOps.

The Details

Building out a top-notch InfoSec organization was a significant part of this endeavor. Unfortunately, in far too many enterprises the InfoSec team reflexively establishes an adversarial stance towards the business and can thus usually be expected to find a way to say 'no' to any user requests that might somehow impact the organization's security. The upshot of these confrontations is that frustrated users find creative ways to cut the InfoSec team out of the loop — and thereby inadvertently introduce substantial security risks. The company selected John Visneski, an experienced information security veteran, to head up its brand-new InfoSec group. From the beginning, he wanted to follow a different path: his vision was that InfoSec should first be problem solvers and only then function as security practitioners. To bring this aspiration to life, selecting the optimal technology portfolio and instituting accompanying practices to fully leverage it was critical.

Prior to the launch of Pokémon Go, the company was already using Amazon Web Services (AWS) to host its website. As the game achieved unprecedented popularity, the organization was confronted with a massive spike in users, data, and scalability challenges. In conjunction with its plans to bring development in-house, Pokémon greatly expanded its AWS utilization to take better advantage of the platform's rich assortment of integrated technologies. This established AWS as a common foundation for everything from game development to supporting retail point of sale operations.

Throughout this period, the InfoSec's team primary mission remained the same: ensuring that the company's customer data collection was securely managed and private, regardless of whether an individual is a child or an adult. Already challenging, this job was made far more complex because of factors including:

- The explosive growth of Pokémon's user base
- Newly adopted AWS features like containers, serverless infrastructure, and alternate database platforms
- Agile software development techniques and the rise of DevOps
- An expanding mixture of stringent, far-reaching regulations such as the Children's Online Privacy Protection Act (COPPA) and the European Union's General Data Protection Regulation (GDPR)

With the entire organization embracing the cloud, it was natural that the InfoSec team also seek its own set of cloud-hosted solutions, particularly those that lent themselves to real-time, automated security responses. This would make it much easier to flexibly cope with the new AWS technologies that were being aggressively implemented by the company, as well as the perpetually evolving threat landscape. The company assembled a highly skilled group — including three former National Security Agency Red Team members — to conduct a search for the tools that would form the backbone of its platform and security operations center (SOC). The evaluation team considered numerous offerings, but eventually narrowed the quest down to products such as Splunk, Sumo Logic, and LogRhythm.

Sumo Logic won the appraisal thanks to how well it addressed a number of critical business and technical prerequisites. Most importantly, Sumo Logic's cloud-native architecture and seamless integration with AWS and third-party tooling meant that the company's technical and security ideals would be in complete alignment. Additionally, during the assessment Sumo Logic demonstrated a 'can-do', collaborative attitude, which gave the InfoSec team the confidence necessary to commit to a core long-term relationship.

The Impact

The Sumo Logic rollout proceeded quickly and immediately began to validate the founding doctrine of the company's InfoSec organization. The user community appreciated that the newly available tools, processes, and automation — backed by a culture of collaboration — provided far greater visibility into the large volumes of data that were generated every day. These fresh insights went far beyond merely protecting information; they were instrumental contributors to the company's overall success.

Consequently, other parts of the organization began clamoring for access to Sumo Logic not long after the first phase of the rollout was complete. This enthusiasm also helped the InfoSec organization to integrate their technology stack across the entire enterprise.

A methodology known as the Observe, Orient, Decide, and Act loop (OODA) is at the heart of how Pokémon's SOC operates, and has also concurrently been embraced by Sumo Logic itself. This approach — originally defined by a U.S. Air Force fighter pilot and eventual Pentagon consultant named John Boyd — relies on superior speed and agility when confronting an adversary — whether in air-to-air combat or battling an unending army of hackers. Deploying Sumo Logic in concert with AWS supplied the InfoSec team with the right set of tools, platform, and actionable guidance to shrink its OODA loop by standardizing on the most effective processes for responding to threats.

The tandem of AWS and Sumo Logic have delivered tangible benefits throughout the company. Three of the most notable examples are:

- **Automated Continuous Intelligence**. Sumo Logic aggregates and unifies all of the company's machine data and then makes it accessible via a pre-built series of security and compliance dashboards. These logs also feed its Security Information and Event Management (SIEM) and Investigation Workflows solutions. The InfoSec team has opted to use automated processes in as many circumstances as possible. This strategy frees its security analysts to concentrate on only those incidents which don't lend themselves to automation. Liberated from more mundane tasks, these specialists can use details provided by Sumo Logic to speedily pinpoint an issue, determine available options, decide on a course of action, and then implement it.
- **Process Improvement**. Ingesting machine data into Sumo Logic has enabled the company to streamline procedures that were previously much more labor intensive. In one instance, a business process that entailed 11 touchpoints spread out over five to seven business days was shaved to two touchpoints that were concluded in five minutes. Beyond saving time and money, these productivity improvements permitted employees to direct their energies toward delivering innovative products and services.
- **Data Privacy**. Users are rightfully more concerned than ever with how their confidential information is protected. Pokémon's InfoSec team has closely coordinated its ongoing data safeguarding endeavors with both AWS and Sumo Logic. The company uses details provided by these solutions to carefully consider what user data is being gathered, the business purposes for it, and how long it's being retained. This focus paid dividends in mid-2018 when the GDPR took effect, making it much easier for the company to comply with this demanding new regulation.

Sumo Logic and AWS have been instrumental in elevating both the visibility and credibility of the InfoSec organization. Business users have come to recognize that this group is sincerely interested in the company's overall success and not just fixated on risk mitigation. The result is that InfoSec is now invited to participate in the earliest phases of a new initiative, which helps "bake-in" security from the start rather than treating it as an afterthought.

At the outset, the company originally chose Sumo Logic as its machine data platform because of the product's flexibility combined with the vendor's willingness to commit to a partnership. Over time, the relationship has strengthened and deepened: along with providing attentive customer support, Sumo Logic regularly briefs Pokémon on its product roadmap and actively solicits feedback - just as AWS does. This has laid the groundwork for applying Sumo Logic's advanced analytics and automated machine learning capabilities for even more use cases going forward.

> **"From the start of our initiative, we were impressed with the investments Sumo Logic has made in our relationship. Because it's a flexible, cloud-based solution, we know that it will be able to work with other tools and platforms that we may implement over time. We're also glad that they provide such detailed access to their product roadmap."**
>
> **John Visneski**
> Director of Information Security and Data Protection Officer

About Pokémon

The Pokémon Company International, a subsidiary of The Pokémon Company in Japan, manages the property outside of Asia and is responsible for brand management, licensing and marketing, the Pokémon Trading Card Game, the animated TV series, home entertainment, and the official Pokémon website. Pokémon was launched in Japan in 1996 and today is one of the most popular children's entertainment properties in the world. For more information, visit www.pokemon.com.

About Sumo Logic

Sumo Logic is a leader in continuous intelligence, a new category of software, which enables organizations of all sizes address the data challenges and opportunities presented by digital transformation, modern applications, and cloud computing. The Sumo Logic Continuous Intelligence Platform™ automates the collection, ingestion, and analysis of application, infrastructure, security, and IoT data to derive actionable insights within seconds. More than 2,000 customers around the world rely on Sumo Logic to build, run, and secure their modern applications and cloud infrastructures. Only Sumo Logic delivers its platform as a true, multi-tenant SaaS architecture, across multiple use-cases, enabling businesses to thrive in the Intelligence Economy.

Founded in 2010, Sumo Logic is a privately held company based in Redwood City, California, and is backed by Accel Partners, Battery Ventures, DFJ Growth, Franklin Templeton, Greylock Partners, IVP, Sapphire Ventures, Sequoia Capital, Sutter Hill Ventures, and Tiger Global Management. For more information, visit www.sumologic.com.

sumo logic

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
305 Main Street, Redwood City, CA 94603

www.sumologic.com