"We have millions of loyal customers. It's critical that we do everything possible to protect the data they entrust to us. Sumo Logic is a major part of how we carry out this job."

**Kashif Iqbal**
Head of Corporate Technology and Cyber Security

## Challenge

SEGA Europe sought techniques to strengthen how it safeguarded the personal details supplied by millions of loyal fans. A key aspect of this exercise was consolidating security-related machine data from the company's hybrid cloud into a single source of truth, while also establishing repeatable processes for onboarding yet-to-be-acquired game studios.

## Solution

The company chose Sumo Logic's cloud-native machine data management solution to replace its legacy Security Information and Event Management (SIEM) system. As part of this undertaking, SEGA Europe concentrated all of its log files from Amazon Web Services (AWS) and Microsoft Azure into Sumo Logic and then configured customized dashboards to address precise user needs.

## Results

SEGA Europe now has a single pane of glass to present critical security information. This resulted in significant improvements in how the company detected, escalated, and ultimately corrected potential security violations.

With an illustrious history dating back to the 1940s, SEGA's mission has always been to entertain the world with creative, innovative experiences. From its inception, the company has been a pioneer, delighting people with offerings that have included coin operated machines, home consoles, handheld devices, apps, and movies. As just one example, today tens of millions of enthusiastic fans eagerly anticipate the next Sonic The Hedgehog installment.

SEGA Europe, Ltd. is the European Distribution arm of Tokyo-based SEGA Games. SEGA Europe is headquartered in London, but wholly owns the development studios, Relic Entertainment in Vancouver, Amplitude Studios in Paris and Creative Assembly, Sports Interactive, Two Point Studios and Hardlight, all based in the UK. Every enterprise in the entertainment business must satisfy their sophisticated, demanding customers, and SEGA Europe is no exception to this rule. The company strives to stay ahead of its competition through a series of measures that range from continuously polling its fans to get their feedback and understand how they're interacting with the company's

Company
**Sega Europe, Ltd.**

Industry
**Entertainment**

Headquarters
**London, England**

Size
**1000+ (including Studios)**

Use case
**Security**

**SEGA Europe deploys Sumo Logic to protect sensitive customer information and shortens problem investigation time by 20%.**

products to launching inventive new platforms such as gaming as a service. Acquisitions are also a big part of how SEGA Europe expands its product collection to keep up with the latest market trends.

Several years ago, the company's technical leadership recognized that cloud computing could transform its entire technology architecture. SEGA Europe soon commenced its migration, and now employs a hybrid cloud framework primarily composed of Amazon Web Services (AWS) and Microsoft Azure. Sega's cloud services range from compute resources such as AWS Elastic Compute Cloud (EC2) to serverless environments. The company also continues to maintain an array of on-premise servers.

With an audience of all ages, that includes young adults and children under the age of 13, security is a persistent concern for SEGA Europe. The company routinely makes considerable investments in products and procedures to help safeguard the data that's been entrusted to it. These initiatives gain additional urgency every time a new mandate is issued, such as the recent European Union General Data Protection Regulation (GDPR). To oversee its protective activities, Sega established a dedicated team that provides services across the entire organization. Around the same time as its first foray into cloud computing, SEGA Europe began experimenting with Security Information and Event Management (SIEM) solutions in support of this group.

Although the initial SIEM ventures appeared to be promising, the company soon encountered a number of daunting drawbacks including:

- Deploying these solutions required making weighty expenditures for dedicated hardware and related infrastructure
- SEGA Europe's site-specific requirements necessitated significant outlays for customization
- The SIEM applications were overly brittle, and needed costly professional services to address errors and performance issues

It became apparent that the situation was untenable, and that failing to resolve these shortfalls could jeopardize SEGA Europe's relentless commitment to the safety and security of its customers. In response, the company began an aggressive search to identify a replacement that could also serve as a 'single source of truth' for its nascent security operations center (SOC).

SEGA Europe assembled an evaluation team to consider leading machine data management solutions such as Sumo Logic, LogRhythm, and Splunk. After a four-month appraisal, the company selected Sumo Logic based on a number of critical factors:

- It's a born-in-the-cloud solution, rather than being retrofit from an on-premise product
- It was easy to set up and use
- Cloud integration proceeded smoothly with services such as Microsoft Office 365
- It demonstrated superior scalability and elasticity at all levels of aggregation: performance wasn't negatively impacted even as the amount of ingested data grew
- Its threat intelligence capabilities were superior. This was an added benefit, since SEGA Europe desired these features but did not actively seek a standalone solution.
- It was possible to search through 30 days of archived log information

SEGA Europe conducted its Sumo Logic rollout solely with in-house personnel. With an eye towards the future—including being prepared to onboard new acquisitions more quickly—the company's implementation team invested sufficient time to fully establish a logical architecture. These efforts entailed defining consistent naming conventions and configuring data containers for anticipated growth, along with performing intensive testing. With the preparation phases complete, the company then speedily transitioned into production, beginning by ingesting machine data —from a diverse set of sources such as AWS GuardDuty, Microsoft Advanced Thread Protection, anti-virus logs, and internally-developed applications—into its new Sumo Logic instance.

> **"By providing my team with a single pane of glass for everything they need, Sumo Logic makes life much easier for all of us."**
>
> **Kashif Iqbal**
> Head of Corporate Technology and Cyber Security

The first year of SEGA Europe's Sumo Logic journey has been a success. Originally, the company aggregated 30 GB of machine data each day into Sumo Logic. However, this amount quickly ballooned to over 50 GB per day. The primary Sumo Logic user community is comprised of approximately 15 people, supporting end users throughout the entire organization as well as the company's network operations center (NOC) and security operations center (SOC). The company fields a far-reaching assortment of pre-built Sumo Logic applications and alerts meant to provide deep security insights and threat analysis across its entire technology inventory. SEGA Europe has also crafted an ever-evolving assortment of its own highly customized, specialized dashboards. This has reduced training requirements for the security team: rather than needing to gain expertise on every element in the company's technology portfolio, they can instead focus on the aggregated information presented by Sumo Logic.

The machine data that's been amassed within Sumo Logic powers a number of interesting use cases. For example, Sega's security team utilizes the well-regarded, proven Observe, Orient, Decide, and Act (OODA) loop when attempting to research and resolve incidents that may threaten the company's assets or data. The company has incorporated Sumo Logic into the playbooks that security staff consult when addressing these classes of problems. When events like this occur, Sega's operations team consults an assortment of Sumo Logic's dashboards for initial triage. These resources also supply guidance about whether the incident is a good candidate for escalation to more senior staff. By consolidating all of Sega's security-related information into an easily accessed, single source of truth, Sumo Logic has shortened the amount of time it takes to investigate and resolve a problem by 20%.

Going forward, SEGA Europe plans to deepen its involvement with Sumo Logic in a variety of ways. The company expects to gather data from additional sources (such as AWS Inspector and CrowdStrike), while continuing to build dashboards purposely tailored for its NOC and SOC. Sumo Logic's machine learning capabilities will also be a potent addition to the company's security toolbox, particularly in concert with its already-employed threat intelligence features. Finally, SEGA Europe anticipates leveraging Kubernetes—including Sumo Logic's dashboards for it—as essential tools for administering its multi-cloud portfolio.

Beginning with the original evaluation, SEGA Europe and Sumo Logic have forged a close, collaborative partnership. SEGA Europe is particularly appreciative of Sumo Logic's customer success team, which has provided extensive assistance with training and establishing product champions within the company. When paired with responsive technical support, this has laid the groundwork for future endeavors to further shield SEGA Europe's assets and information.

## About Sega

SEGA® Europe Ltd. is the European Distribution arm of Tokyo, Japan-based SEGA Games Co., Ltd., and a worldwide leader in interactive entertainment both inside and outside the home. The company develops and distributes interactive entertainment software products for a variety of hardware platforms including PC, wireless devices, and those manufactured by Nintendo, Microsoft and Sony Interactive Entertainment Europe. SEGA wholly owns the video game development studios Two Point Studios, Creative Assembly, Relic Entertainment, Amplitude Studios, Sports Interactive and HARDlight. SEGA Europe's website is located at www.sega.co.uk.

## 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. 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**