SUCCESS STORY

JAPAN   PROFESSIONAL SERVICES   ELASTIC SECURITY

Mitsui Fudosan built a powerful in-house monitoring capability with Elastic Security and Recorded Future, allowing it to take targeted action in real time against emerging threats

Detects and analyzes cyber attacks across the entire organization

By bringing its SIEM in-house with Elastic Security, Mitsui Fudosan performs log analysis across the business on a single platform, accelerating its responses to security events.

Reduces alert fatigue with fewer false positives, leading to 40% reduction of alerts

Mitsui Fudosan prioritizes threats in order of urgency for a more focused response.

Enables real-time responses to urgent events

Mitsui Fudosan identifies emerging external threats and takes immediate action to protect its systems.

elastic

Elastic Security gives Mitsui Fudosan full visibility of its internal systems and the external threat landscape.

As a literal brick-and-mortar industry, real estate has traditionally been far removed from the digital world. For companies like Mitsui Fudosan, one of Japan's largest real estate developers, success was built upon concrete and steel, not code and algorithms. In recent years, the company's commitment to innovation has seen it expand into the digital realm, bridging the gap between ecommerce and physical stores while investing in supply chain technologies to support the booming online marketplace.

Along with these opportunities for digital transformation came new security challenges, further extending the remit of Mitsui Fudosan's cybersecurity team, which was already tasked with protecting the entire organization in a fast-changing threat landscape. However, with its security monitoring and analysis platform previously outsourced, Mitsui Fudosan was limited in its ability to draw critical insights from security data. Mitsui Fudosan decided to bring its security monitoring platform in-house to monitor its own environment and perform its own log analysis, allowing it to respond to incidents more effectively.

"Outsourcing to a completely managed service meant we did not have a platform to do any analysis by ourselves," recalls Seungjo Jang, Engineering Manager, Digital Transformation division at Mitsui Fudosan. "We could not see anything from our end, and were only receiving analysis results, making it difficult to grasp our security situation accurately."

The company evaluated a range of security information and event management (SIEM) solutions before ultimately choosing Elastic Security for its performance and ease of use.

> ❝ Elastic is superb in its functionality as an analysis platform and is significantly more cost-effective than other products in the market. Keeping costs down allows us to allocate more of our budget and resources to other areas, which was a key factor in choosing Elastic.
>
> **Seungjo Jang**
> Engineering Manager, Digital Transformation Division,
> Mitsui Fudosan

Mitsui Fudosan also previously outsourced their threat intelligence program, limiting its visibility of the external threat landscape. Mitsui Fudosan eventually chose to implement Recorded Future alongside Elastic Security to help them better prioritize risks to their business.

elastic

Group-wide logging and analysis from one central platform

With Elastic Security, Mitsui Fudosan has a flexible platform to monitor its IT environment for potential security threats. It can track security events across a wide range of sources, including network-related logs, internal systems, and cloud services such as Microsoft 365. These sources can be seamlessly integrated using Elastic Agent, which simplifies the onboarding of new log sources with its prebuilt integrations and automated data standardization.

With the logs centralized in Elastic, the cybersecurity team can fine-tune configurations to define exactly what it wants to monitor and how. "Elastic is very flexible in terms of configuration," recalls Junichi Sawada, Engineering Leader, Digital Transformation division at Mitsui Fudosan. "We can make detailed adjustments that are difficult to achieve on other platforms and engage in detailed analysis. This capability to reach into the finer details is a considerable advantage."

Mitsui Fudosan can use Elastic Security to perform log analysis across the entire group, including subsidiaries, from one central platform. This increases efficiency by allowing for quicker investigation and response to security events, as well as strengthening the company's protection.

> With Elastic Security we have robust analytical functions for detecting cyber attacks. Being able to search and analyze across group companies means we can detect and analyze cyber attacks on a group-wide scale, which is very important for us.
>
> **Seungjo Jang**
> Engineering Manager, Digital Transformation Division,
> Mitsui Fudosan

Integrating threat intelligence and system monitoring for real-time protection

By using Elastic Security in combination with Recorded Future, Mitsui Fudosan can correlate internal security events with external threat data, enabling more accurate threat detection and faster incident response. For example, if Recorded Future identifies leaked company credentials on the dark web, the security team can quickly investigate and take action to mitigate the risk. Likewise, if Recorded Future alerts the company of a new attack method being used against another company in the industry, the cybersecurity team can use Elastic Security to implement security measures across the organization proactively, before the attack can impact Mitsui Fudosan.

elastic

> **"**
>
> We've had numerous situations where we could use Elastic to take immediate action and create monitoring rules for a particular area to mitigate against a specific risk. Without Elastic, that would be extremely difficult.

Seungjo Jang
Engineering Manager, Digital Transformation Division,
Mitsui Fudosan

Previously, the process of collecting and analyzing threat information, correlating it with system logs, and narrowing it down to high-risk items was a manual and time-consuming task. Now, thanks to the seamless integration of Elastic Security and Recorded Future, this process is fully automated, freeing up the cybersecurity team to focus on more strategic security initiatives.

Storing and accessing data in a cost-effective way

With Elastic Security's long-term data storage capabilities, Mitsui Fudosan can now store historical logs in a cost-effective way. Where cost constraints previously led the company to rely on separate platforms for analysis and long-term storage, Elastic Security's tiered storage allows Mitsui Fudosan to consolidate all its data in a single, unified platform, storing frequently accessed data on high-performance infrastructure while archiving older data on more economical tiers. "This arrangement allows us to meet our long-term retention and analysis needs while managing costs effectively, which is one of the key advantages of Elastic," Sawada explains.

Protecting an increasingly complex environment against future threats

As Mitsui Fudosan continues to expand into new digital ventures and its IT environment grows in complexity, the cybersecurity team plans to make more use of Elastic Security's automation and built-in features to streamline security tasks and protect the company from emerging threats.

In particular, it plans to use Elastic Security's machine learning for anomaly detection, such as those related to unusual network communications. It is also exploring the potential use cases of generative AI within Elastic to further automate security processes, uncover new insights, and ensure continued protection in the face of an ever-changing threat landscape.

Start your free trial

See for yourself how your business can benefit from Elastic in the Cloud, with a free 14 day trial.

Get started

elastic