splunk> a CISCO company

CASE STUDY

Shunkhlai Group Accelerates Security Incident Response by 2x With Splunk Enterprise Security

Key Challenges

Security monitoring at Shunkhlai Group across its heterogeneous computing environment was reactive and decentralized, slowing incident response and lengthening downtime.

Key Results

With Splunk Enterprise and Splunk Enterprise Security delivering proactive and unified visibility into its distributed SOC operations, Shunkhlai Group responds to security incidents three times faster, while cutting downtime by up to 50%.

Shunkhlai GROUP

Industry: Energy & Utilities

Solutions: Security

Products: Splunk Enterprise, Splunk Enterprise Security

The best kind of security is proactive.

Mongolia-based Shunkhlai Group is a holding company that oversees more than 30 businesses across various sectors, including manufacturing, trade, and technology. It strives to maintain cyber vigilance and stay resilient to cyberattacks to ensure smooth operations and reliable service for its customers. As a holding company, Shunkhlai Group has a centralized cybersecurity division that implements policies, frameworks, and controls across all its subsidiaries. The Group's subsidiaries manage its respective cybersecurity processes, with guidance from the headquarters.

However, the Group's network is full of disparate and heterogeneous data sources from multi-vendor applications spread across departments. It also runs a complicated computing environment mixed with hybrid clouds and on-premises infrastructure. With Shunkhlai Group's previous security monitoring system, its teams struggled to analyze data, detect threats, and address incidents efficiently amidst a complex technology landscape.

Outcomes

2-3x
faster security incident response

2x
faster MTTD and MTTR

50%
reduction of system downtime

A team of four had to monitor security alerts manually while spending hours responding to incidents. Worst still, all these were addressed reactively. The team often couldn't detect and address security risks before they occurred, which increased the likelihood of service disruptions. Therefore, Shunkhlai Group set up a central security operations center (SOC) in 2023, adopting Splunk Enterprise and Splunk Enterprise Security to provide the data analytics to fuel their operations.

Centralized, real-time data analytics accelerates incident response and minimizes downtime

After bringing in Splunk, Shunkhlai Group shifted from a distributed security management model to a centralized one to ensure better integration, consistency, and overall management of security operations. "We chose Splunk Enterprise and Splunk Enterprise Security for their robust analytics, scalability, and comprehensive security features," says Gombodorj Munkhbat, information security manager at Shunkhlai Holding LLC. "Splunk's ability to integrate with our existing systems and provide real-time visibility into our security landscape was unmatched. It also offers us advanced threat detection, investigation, and compliance capabilities."

With Splunk, Shunkhlai Group's teams no longer need to search through disparate sources and correlate data manually to

diagnose cyberattacks. Splunk Enterprise provides a unified platform for log collection and analysis, as well as full-stack visibility into network operations. Its SOC now monitors data streams on intuitive, visualized dashboards and can discover threats, resolve issues, ensure compliance, and optimize system performance.

Splunk Enterprise Security has enhanced security monitoring with advanced threat detection based on user behavior analytics, while accelerating threat investigation and response by aggregating data and analyzing the cybersecurity landscape on a single pane of glass. All these contribute to a 50% reduction of both the mean time to detect (MTTD) and mean time to respond (MTTR), and two to three times faster incident response. The increased efficiency has become a strong foundation for Shunkhlai Group to maintain stable operations and reliable service for customers.

> Splunk enables us to detect and respond to security incidents quickly and accurately. It also provides insights that were previously unattainable, allowing us to proactively address potential issues before they escalate."
>
> **Gombodorj Munkhbat,** Information Security Manager, Shunkhlai Holding LLC

Proactive and predictive security cuts downtime by half and realizes 99.99% availability goal

With Splunk turning data into actionable insights in real time, Shunkhlai Group is better equipped to anticipate the unknowns by uncovering 50-60% more threats and mitigating security risks in a proactive manner. The combined use of the Splunk solutions and other threat intelligence tools and sensors enable Shunkhlai Group to better detect and respond to phishing attacks, malware, and other cyber threats before they impact operations.

Using Splunk's predictive analytics dashboards, analysts can detect outliers in data, spot anomalous behaviors, and track performance issues and bottlenecks in daily operations. It has successfully reduced network downtime by up to 50%, and improved the efficiency of security operations.

"Thanks to Splunk, we are able to reinforce our commitment to observing the highest standards of security and integrity, while embracing an exceptional uptime of 99.99%," Munkhbat says.

Towards a sustainable and resilient future

As a diversified holding company operating in a wide range of industry sectors, Shunkhlai Group requires a data analytics solution which is flexible enough to cope with the sustainable development of its miscellaneous business portfolios.

Munkhbat is excited that Splunk provides a customizable platform that can readily parse and process data from multiple sources, which keeps their business digitally resilient. Moreover, Splunk streamlines the Group's security operations and improves its overall security posture, raising the bar for cyber resilience.

What also impresses Munkhbat is the service quality and responsiveness of Splunk's account team. "They are always ready to help, share valuable insights, and provide solutions promptly. We also appreciate Splunk's partner Unity, which helped us deploy the solution with ease while training our engineers and providing optimal support," says Munkhbat. "Splunk will continue to be an integral part of our IT roadmap, and we plan to integrate more data sources with Splunk, while leveraging its advanced analytics to further enhance our security and operational efficiencies."