splunk> a CISCO company

CUSTOMER STORY

ASL Reduces Security Incidents by 40% with Proactive Threat Management

Key Challenges

ASL needed to enhance real-time threat detection, automate data analytics while consolidating and correlating intelligence and insights from diverse systems without compromising operational agility.

Key Results

Splunk's centralized data and intelligence-driven monitoring platform leads to proactive threat detection and response, optimizes manpower, reduces security incidents, and safeguards critical systems.

Industry: Technology

Solutions: IT, Security

Products: Splunk Enterprise, Splunk Enterprise Security

Capabilities: SIEM / Security Analytics, Unified Security Operations, Security Incident Response, Incident Response and Automation

Enhancing customer trust with next-generation security

As a premier IT service provider and innovator, Automated Systems (H.K.) Limited (ASL) empowers businesses through cutting-edge solutions. To boost customer confidence in an era of sophisticated cyber threats, ASL made a strategic move to augment its Security Operations Center (SOC) with proactive real-time monitoring across its diverse and interconnected systems, aiming to elevate existing security protocols to new heights of speed and intelligence.

ASL states that its commitment to security is fundamental to its customer partnership. They indicate that, to address the complexities of their expanding hybrid IT environment, they are focused on transitioning beyond traditional monitoring approaches. They implemented Splunk Enterprise and Splunk Enterprise Security to build a new data and intelligence-driven monitoring platform.

Outcomes

2x
faster troubleshooting

40%
reduction in monthly security incidents

60%
fewer human resources needed for security monitoring

ASL explains that Splunk provides a unified platform that empowers them to seamlessly correlate data across various sources such as firewalls, servers, applications, and cloud resources, to convert operational challenges into strategic opportunities. They note that through the deployment of these solutions, they are able to ensure a robust security posture aligned with their clients' evolving requirements across security, productivity, and compliance domains.

Breaking bottlenecks and streamlining processes

Splunk Enterprise acts as a centralized platform to collect, index, and analyze log data generated by its diverse systems and applications. Besides simplifying data management and analysis, it also turns data into actionable insights about system performance, allowing ASL to spot anomalies and fix issues in a timely and effective manner. At the same time, Splunk Enterprise Security automatically correlates security-related data from security safeguards, including firewalls, antivirus solutions, endpoint detection and response solutions, and other security tools.

The Splunk platform ensures everything runs efficiently for enhanced security and performance. ASL is able to proactively detect malicious activities and potential threats, while responding to material security incidents around the clock. IT troubleshooting is now two times faster than before.

Moreover, the highly visualized Splunk Dashboards offer ASL a holistic visibility into the health status of all servers, network devices, storage systems, virtualization environments, and cloud resources. The team is able to customize tailored alerts and role-based dashboards to accelerate response workflows. ASL adds that they now proactively identify performance bottlenecks, capacity issues, and infrastructure-related anomalies while tracking customer behavior trends, especially during transaction spikes. This allows them to scale resources to achieve service-level agreement compliance while ensuring customers receive optimal, high-value services.

> With Splunk, our Security Operations Center is well-equipped to enhance security, accelerate incident responses, and ensure continuous monitoring with the latest threat intelligence, to reinforce the trust of our stakeholders.
>
> **Automated Systems (H.K.) Limited.**

Optimizing proactive defence in a hybrid world

With the combined use of Splunk Enterprise and Splunk Enterprise Security, ASL has successfully reduced security incidents by 40 percent per month. Besides uncovering anomalies in real time across ASL's 24/7 IT infrastructure, which lays the basis for proactive threat hunting, Splunk also automates data fusion for ASL so that it can synthesize security events from disparate sources like antivirus systems, endpoint detection and response systems, and firewalls.

ASL states that their commitment to security excellence drives them to find a solution that offers unified visibility, and Splunk stood out from others immediately. They explain that Splunk's leadership in analytics, hybrid-environment monitoring, and product innovation aligned perfectly with their vision. Most importantly, ASL emphasizes that Splunk transformed its data agility by automating correlation and delivering actionable intelligence in real time.

ASL can swiftly adapt to emerging threats and continuously enhance its security measures. They emphasize that Splunk not only meets their goals but also complements their technology team's expertise to redefine innovation, productivity, and intelligence with greater effectiveness.

Transforming data into strategic outcomes — going beyond security!

Splunk's winning factors also include its advanced analytics and machine learning features that enable ASL to trace operational patterns, perform predictive analytics, and make real-time, informed decisions to mitigate security risks and ensure the availability of IT infrastructure. For instance, ASL can now detect transaction spikes and capacity bottlenecks, ensuring SLA compliance during peak demand through proactive resource scaling.

With Splunk, ASL is now spending 60 percent less human resources on security monitoring. It can rearrange the saved resources to support other priority tasks and innovative initiatives.

Due to the versatility of the Splunk Dashboards, ASL will extend its use to more cross-functional stakeholders. While IT and security analysts remain the key users, network administrators, application developers, and compliance officers are increasingly monitoring their operational aspects through the tailored dashboards.

The expertise of ASL's talented team in utilizing Splunk has enhanced system efficiency and allowed for tailored insights, ultimately enabling ASL to provide world-class service to its customers by quickly addressing issues and optimizing performance based on real-time data.