splunk>

CASE STUDY

Manufacturing Company Automates With Splunk Enterprise Security SIEM

Manufacturing

Executive summary

A global contract manufacturing company headquartered in the U.S. conducts business in many parts of the world, including areas that have significant issues around cybersecurity. The company needed a security information and event management (SIEM) solution that would enable its small cybersecurity team to protect customers' intellectual property and better serve them. Since adopting Splunk Enterprise Security (ES) as its SIEM the company has seen benefits including:

- Preventing insider and external threats
- Protecting customers' sensitive data
- Automating security incident tracking to make the most of small security team

Why Splunk

Years ago, security concerns at the manufacturing company focused primarily on viruses and security attacks from outside of the organization. But over time, the company's needs grew to include identifying and determining bad actors' motives, and stopping both insider and external threats. Meanwhile, the company's data resided in silos, and the security team lacked visibility into its security posture. In addition to malicious code and bad actors that threatened the business, the company also had to contend with the speed of change and rapid deployment among its customers. As the company increased the amount of intellectual property it handled, the volume of attempts to steal that intellectual property grew.

Today, the company has a security operations center (SOC) powered by the Splunk ES data analytics security platform that enables its security team to quickly identify threats or potential threats. With Splunk ES, the organization's small security team now has a reliable SIEM solution to help ensure customer products will get to market in stealth mode. The company's security team is varied in terms of skill set and knowledge and its technical security leads have developed Identifiers of Compromise (IOCs) that tier-one analysts can use to triage incidents. This helps to onboard tier-one analysts more quickly and enables tier-two and tier-three analysts to focus on remediation and threat hunting, speeding the team's overall ability to react faster.

Industry

- Manufacturing

Splunk Use Cases

- Security
- IT operations

Challenges

- Needed to safeguard sensitive customer data
- Required SIEM to provide complete data visibility
- Needed to automate to make most of its lean but mean staff

Business Impact

- Protects customers' intellectual property
- Automation enables the company to staff team with different skill sets
- Provides single pane of glass for incident investigation and management
- Scalable solution accommodates growing volume of data

Data Sources

- Network logs
- Microsoft Windows SEP logs
- Digital Guardian Data Loss Prevention (DLP) logs
- Linux logs
- Macintosh logs

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security

By using Splunk Enterprise and Splunk ES, the team can drill down into logs for additional detail and for further correlation, investigation and analysis. Currently, Splunk ES ingests a wide variety of data sources including Microsoft Windows SEP logs, network logs, Digital Guardian Data Loss Prevention (DLP) logs, Linux logs and Macintosh logs. The team is working to bring in Windows Dynamic Host Configuration Protocol (DHCP) logs and logs from switches and other sources. Moving forward, the security team plans to continue adding additional data sources. The leadership team believes that as more data is ingested in Splunk ES it results in more effective correlation and faster investigations. The company also is looking into behavioral analytics scenarios where it can pinpoint internal bad actors and determine what is normal versus anomalous.

Single pane of glass

Today, Splunk ES is the company's single pane of glass that enables it to do incident investigation and management from one pane. To date, the company has been able to automate part of the process. For instance, Splunk ES helps the security team start a ticket for other teams to take an action, and the intent moving forward is to automate further. Because the company does not have a large security team, automation is key. The more it can automate and put in systemic controls, the more success it can show its customers. If the security team has a recurring incident or issue where they see an alert, they try to automate.

"Splunk ES is our single pane of glass that allows us to do incident management as well as investigation from one pane."

CISO, manufacturing company

Thus far, the team has focused its use of Splunk ES on IT infrastructure monitoring and cybersecurity, but moving forward the company may extend its use of Splunk into the manufacturing lines and other areas as well. For now, the ability to have fact-based analytics is critical. Using Splunk ES, the company can identify issues via visualizations that help the security team understand the scale of what it is trying to protect. As recruiting and keeping top talent is one of the most challenging issues facing security teams today, the fact that Splunk ES helps the company to optimize its security resources via automation, communication and documented best practices is critical to maintaining its security posture.

Data analytics security platform

Prior to implementing Splunk ES, the company had limited visibility into its security landscape, limiting its ability to ascertain what was normal versus an anomaly. Today, with Splunk ES alerts, visualizations and dashboards, the company has a clear understanding of how secure it is and how many vulnerabilities exist. Instead of looking at different systems that don't correlate, Splunk ES is the company's data analytics security platform that enables the security team to see the bigger picture and share its knowledge with the company's CIO and division CIOs.