splunk> a CISCO company

CASE STUDY

Johnson Matthey Fights Phishing and Closes Investigations 83% Faster With Splunk

Key Challenges

Prior to implementing Splunk, Johnson Matthey's security team faced an overwhelming number of alerts without a means to effectively filter through and prioritize the most critical ones.

Key Results

Adopting Splunk Enterprise Security, Splunk SOAR, and Splunk Attack Analyzer enhanced Johnson Matthey's alert fidelity and phishing detection accuracy, significantly boosting the overall security and protection of the organization.

Johnson Matthey
Inspiring science, enhancing life

Industry: Manufacturing

Solutions: Security

Product: Splunk Enterprise Security, Splunk SOAR, Splunk Attack Analyzer

Sustainability is everyone's responsibility

Founded in the early 1800s, Johnson Matthey is a global leader in sustainable technologies headquartered in London, U.K. Many of the world's leading energy, chemicals, and automotive companies depend on its technology and expertise to decarbonize, reduce harmful emissions, and improve their sustainability.

With a strong focus on science and innovation across multiple sectors, Johnson Matthey's business structure integrates corporate IT and operational technology (OT) functions, making cybersecurity a priority. Any data breach could impact uptime, production, and even employee safety.

The security operations center (SOC) at Johnson Matthey struggled with a high volume of alerts, lacking the context and technology needed to determine which ones were legitimate and most critical. Johnson Matthey's SOC needed a solution to provide the necessary context to investigate alerts more efficiently and keep the organization secure, allowing it to focus on its ultimate mission to address climate change.

Outcomes

- Increased alert fidelity by 30%
- Reduced case management time by 83%
- 61% of phishing cases closed by automation with SOAR

Tuning out the noise

Before using Splunk, Johnson Matthey's security team found it difficult to handle the overwhelming volume of security alerts. The team lacked the context to prioritize the alerts effectively, struggling to identify the 15-20% that required immediate attention. Finding the real threats was like finding a needle in a haystack.

After adopting Splunk Enterprise Security, the Johnson Matthey security team implemented risk-based alerting (RBA), which consolidates multiple alerts into fewer more meaningful ones that the team can focus on. Instead of receiving many separate security alerts, RBA collates them and presents the information into one alert about an asset or identity that requires immediate attention. This means all incoming data can be analyzed and used for threat hunting without inundating the SOC team with thousands of irrelevant alerts, an approach that not only improves operational efficiency, but also enhances overall security posture. Due to the enriched alerts, Johnson Matthey could expand the volume of use cases by 40-50% whilst reducing the number of alerts and false positives.

"Using risk-based alerting in Splunk Enterprise Security, we're able to fine tune precisely what we want out of the system, so all the data keeps coming for analysis, but without bombarding our SOC with irrelevant alerts," says Nathan Lowey, cybersecurity engineer at Johnson Matthey.

Teamwork makes the dream work

Because of data silos and the non-standardized nature of reporting, there were cases where multiple analysts independently worked on the same alert without collaborating. This meant there were different ways of working from one analyst to the next, not always to the same standard. Meanwhile, 90% of alerts were generated by just 20% of specific use cases. Using Splunk SOAR, Johnson Matthey started to use playbooks to streamline and standardize the alert process so that analysts' work was better organized and their reporting more uniform. This resulted in more standardized and accurate data for more proactive tuning.

Previously, when analysts recorded a threat, they had to manually create a ticket and input relevant information. Splunk SOAR has changed the process, automating repetitive tasks and enriching alerts with additional context. Case investigation used to take an average of 30 minutes, but now average five minutes. "Splunk SOAR facilitates communication," says Nathan Lowey, cybersecurity engineer at Johnson Matthey. "If one of our analysts needs to share something with someone on the OT side, with the click of a button they can extract everything from the case, sign it over to them in IT service management, and it's all protected in one single system."

> Using SOAR and Splunk Attack Analyzer has enabled us to automate part of our phishing process. Our analysts deal with fewer cases because we now automatically close the ones that aren't a real threat. We've made further enhancements so that we're certain what analysts are looking at is going to work. At this point 61% of phishing threats are analyzed and processed without us having to intervene."
>
> **Nathan Lowey,** Cybersecurity Engineer, Johnson Matthey

Addressing risks, old and new

As new and sophisticated cyber threats emerge, organizations must stay ahead of attackers. So, when teams at Johnson Matthey encountered the new threat of "quishing," a form of phishing attack that uses QR codes that standard detection systems could not distinguish from regular images, Splunk Attack Analyzer was brought in.

Adopting Splunk Attack Analyzer has boosted the accuracy of the entire phishing detection system, which had before suffered from a high rate of false alarms. Previously, every email subject line, including the words "urgent," "payment," or "report announcement" was flagged as suspicious. After using Splunk Attack Analyzer, phishing detection accuracy increased to 80%, compared to 50% originally. Approximately 61% of phishing attempts are now automatically identified as false and closed without an analyst involved. Once a malicious URL has been detected, it's automatically added to the cloud proxy.

By using Splunk Enterprise Security, Splunk SOAR, and Splunk Attack Analyzer, Johnson Matthey has simplified and enhanced its data security strategy, streamlined processes, and improved decision-making. Additionally, the once-siloed cybersecurity teams can now communicate and collaborate seamlessly, working together to keep the organization secure.