splunk>

CASE STUDY

Splunk SOC Achieves a 7-Minute MTTD for Phishing Attacks With Splunk Attack Analyzer, Splunk SOAR

Key Challenges

Hundreds of phishing alerts overwhelmed Splunk's SOC analysts each month, who struggled with a lengthy MTTR and were limited in the number of deeper investigations they could conduct monthly.

Key Results

Splunk Attack Analyzer has given the incident response team more context as they conduct investigations, empowering them to contain threats more quickly and resolve phishing alerts 90% faster.

splunk>

Industry: Technology

Solutions: Security

Products: Splunk SOAR, Splunk Attack Analyzer

Catching every phish in the pond.

Phishing is one of the most prevalent and costliest attack vectors, and 88% of organizations surveyed in our State of Security 2024 report expect phishing to worsen in volume and effectiveness with the use of generative AI. When employees at Splunk get a suspicious email, they can report it to Splunk's detection and response team to help protect the organization from a breach. Hundreds of alerts flood the team each month. Many are false alarms, and some point to legitimate risks. In either case, analysts must conduct a thorough investigation to distinguish one from the other.

To better handle the high volume of alerts, the Splunk team decided to adopt Splunk SOAR. As email alerts came in, Splunk SOAR automated ticket creation and information extraction. This was a good starting point, but Splunk's detection and response team wanted to get MTTD down to under 7 minutes. This meant the investigation piece of the process also needed to be automated. And that's how Splunk Attack Analyzer came into play, too.

Outcomes

- Resolving phishing alerts 90% faster
- Higher accuracy of phishing detection
- Addressing and containing cybersecurity threats faster

Before, the high volume of phishing reports created a backlog of tickets waiting to be triaged by the team. After adopting Attack Analyzer, tickets were investigated and resolved 90% faster. When a potential phishing attempt is reported, SOAR opens a ticket, while the suspect email is automatically submitted to Attack Analyzer for analysis. Attack Analyzer examines the entire attack chain, then generates a score and verdict for each submission indicating the severity of the threat. Afterwards, it uploads the analysis results and relevant forensics to the ticket. All this happens in a matter of minutes, making it easy for the analyst to respond and contain the threat. Splunk's SOC can now respond to and contain threats much faster, and reduce the risk of breaches and downtime caused by phishing.

Addressing the toughest incidents out there

If you work in incident response, every judgment call had better be right. That's the expectation of every cybersecurity function in every organization. And it's especially true for Splunk's Advanced Threat Response team, which addresses the biggest and nastiest incidents the company encounters. This unit of ten individuals partners with the SOC and other internal stakeholders to keep Splunk secure. When something goes wrong, the team's job is to minimize any effects on the company's operations, finances, and reputation and allow all Splunk employees across the company to keep doing their best work.

The team recently adopted Splunk Attack Analyzer to support deeper incident investigations and conduct more analyses. It's since become the team's go-to tool for analyzing suspicious files or domains. Using Splunk Attack Analyzer has enabled them to detect incidents faster and reduce risk to the organization. "It's been helpful for the thorniest of thorny incidents," says Tony Iacobelli, senior manager on the Splunk Advanced Response team.

> Attack Analyzer is a tool that our responders love using, which is rare, and they know that they can push it to its limits, and it will still work. And when we're dealing with something weird and nebulous and unknown, Attack Analyzer is one of the first tools in the tool belt that we use to help clear up the fog."
>
> **Tony Iacobelli,** Senior Manager, Splunk Advanced Response

Having a strong automated threat analysis tool like Splunk Attack Analyzer in its arsenal means the team can expand the scope of its detections. Previously, when anything malicious popped up, the Advanced Threat Response team relied solely on its EDR solution to automatically block it from further execution. With Attack Analyzer, analysts can track patterns and get additional details (such as indicators of compromise and host-based artifacts) about the attack source to find other instances of suspicious activity the EDR may have missed. The interactive detonation modes within the tool also let the team investigate malware without running the risk of infecting their machines.

This addition to the toolbelt came at a good time. "We were expanding the number of use cases and areas we have visibility into," says Tony. "Unfortunately, we can't simply scale our people resources as we get more visibility into systems. So we need to scale our team's productivity by increasing our overall efficiency. And Attack Analyzer helped us do just that." Attack Analyzer ramped up the efficiency across Splunk's incident response teams, so much so that they achieved their goal of getting their mean time to detect on critical use cases to be under seven minutes.

24-643263-Splunk-SOC-CS-103