splunk> turn data into doing™

CASE STUDY

Automating Malware Investigation at One of the World's Leading Investment Firms

Key Challenges

Fielding 30–40 malware alerts per day, Blackstone needed a way to automate scripts across all its security vendors to consolidate response and remediation.

Key Results

By increasing automation with Splunk SOAR, Blackstone has dramatically reduced time to investigate malware alerts, driving accuracy and consistency across its incident response processes.

Blackstone

Industry: Financial Services

Solutions: Security

As one of the world's leading investment firms with more than 21 offices spanning the globe, Blackstone commonly sees up to 40 malware alerts in a single day.

Blackstone's Incident Response team investigates each malware alert as if a compromise has already occurred, a process that requires 30 to 45 minutes to address each alert fully if done manually. Considering the volume of alerts and the potential for inconsistency in any manual process, Blackstone knew there had to be a better way.

Navigating a Complex Security Landscape

Despite Blackstone's expertise in scripting and automation, developing this capability across a large set of security vendors became difficult to maintain. As each vendor changed the API for its product, the automation scripts had to change as well. To address this challenge, Blackstone began the search for a commercially available solution that could tie together its existing security products to reduce the response and remediation gap caused by limited resources, a widening attack surface and a complex technology infrastructure. Blackstone selected Splunk SOAR as its security orchestration, automation and response platform.

Data-Driven Outcomes

40 seconds
to process malware email alerts versus up to 45 minutes before Splunk

30-40
malware alerts now confidently fielded per day

21
global offices with improved security

Security Automation and Orchestration With Splunk SOAR

Using Splunk SOAR's Python-based Apps and Playbooks, Blackstone is now able to execute actions quickly, ensuring a repeatable and auditable process for investigating malware alerts. A Splunk SOAR Playbook is triggered when an email malware alert is received. Due to the lack of context in these alerts, Splunk SOAR's first order of business is to query Blackstone's security information and event management (SIEM) solution for all recipients, then Active Directory to collect context from the profiles of all affected users — business group, title and location.

Next, Splunk SOAR orchestrates a "hunt file" action in Carbon Black and queries iSightPartners' threat intelligence database before concluding with a file reputation check on VirusTotal and an assessment by Cylance's Infinity model. This information is immediately presented back to the security team in a quick-analysis format for review and action.

Starting with a well-defined manual process is essential for automation, and has allowed Blackstone to quickly implement Splunk SOAR Playbooks. Once the Blackstone team was familiar with Splunk SOAR's platform, they were able to write Playbooks in a matter of hours. Blackstone already has a roadmap for additional use cases such as automating time-consuming operational tasks and addressing additional incident response scenarios.

As a next step, Blackstone plans to create remediation Playbooks, which would allow analysts to take immediate action based on the initial Playbook result. Such actions could include additional investigation tasks, notifying users, or even isolating hosts, which would be integrated with multi-factor authentication to ensure the action is properly authorized.

> Automation with Splunk SOAR enables us to process malware email alerts in about 40 seconds versus 30 minutes or more."
>
> **Adam Fletcher,** CISO, Blackstone

Fast and Accurate Resolution of Malware Alerts

With Splunk SOAR, Blackstone has been able to dramatically reduce the time required to investigate malware alerts. By the team's estimate, the time needed to complete the manual process ranged from 30 to 45 minutes. The same process, automated with a Splunk SOAR Playbook, completes in less than one minute, freeing the team to focus on analysis and resolution.

Equally important, Splunk SOAR drives accuracy and consistency in the incident response process. In the past, as alert volume increased, analysts tended to become overwhelmed with information, potentially causing them to overlook key indicators. Similarly, experienced analysts might have been tempted to make "gut calls" based on previous incidents and incomplete information. With a Splunk SOAR Playbook, the same data is gathered for every alert, and every alert is investigated and memorialized the same way, every time.

As the first community-powered security automation and orchestration platform, Splunk SOAR gives Blackstone the flexibility to address its dynamic network. The Python-based Apps and Playbooks are easy to develop, and the Blackstone team shares those responsibilities across different integrations. The Splunk SOAR platform then ensures that both the Apps and the Playbooks integrate seamlessly with one another.

Automating incident response with Splunk SOAR has resulted in a number of improvements at Blackstone, ultimately allowing the team to spend less time performing tedious, repetitive tasks, investigate issues faster and drive consistency to ensure a fast, accurate result.

20-15387-Tier2-Blackstone-102-CS