

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

## Blackstone

### Executive summary

As one of the world's leading investment firms with more than 21 offices spanning the globe, it's not uncommon for the security team at Blackstone to see as many as 30 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. Since deploying Splunk Phantom, Blackstone has seen benefits including:

- Processing malware email alerts in about 40 seconds versus 30 minutes or more
- Ensuring a repeatable and auditable process for investigating malware alerts

### Why Splunk Phantom

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 Phantom as its security orchestration, automation and response platform.

### Security automation and orchestration with Phantom

Using Phantom'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 Phantom Playbook is triggered when an email malware alert is received. Due to the lack of context in these alerts, Phantom'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, Phantom orchestrates a "hunt file" action in Carbon Black and queries iSightPartners' threat intelligence database before

### Industry

- Financial services

### Splunk Use Cases

- Security Orchestration, Automation and Response

### Challenges

- Difficulty maintaining automation scripts across large number of security vendors
- Needed to tie together existing security products to reduce the response and remediation gap

### Business Impact

- Dramatically reduce time to investigate malware alerts
- Drive accuracy and consistency in the incident response process
- Incident response automation enables the team to investigate issues faster

### Splunk Products

- Splunk Phantom Enterprise Edition

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 Phantom Playbooks. Once the Blackstone team was familiar with Phantom'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.

### Fast and accurate resolution of malware alerts

With Phantom, 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 Phantom Playbook, completes in less than one minute, freeing the team to focus on analysis and resolution.

---

**“Automation with Splunk Phantom enables us to process malware email alerts in about 40 seconds versus 30 minutes or more.”**

**Adam Fletcher, CISO**  
Blackstone

---

Equally important, Phantom 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 Phantom 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, Phantom 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 Phantom platform then ensures that both the Apps and the Playbooks integrate seamlessly with one another.

Automating incident response with Phantom 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.

[Download Splunk for free](#) or get started with the [free cloud trial](#). Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.



Learn more: [www.splunk.com/asksales](http://www.splunk.com/asksales)

[www.splunk.com](http://www.splunk.com)