SOLUTION BRIEF

Symantec Technology Partner: Splunk

Business challenge

Cyber threats are smarter, faster, and more insidious than ever. Advanced attacks can be coordinated across multiple vectors, execute at machine/network speed, employ intricate command and control structures, self-propagate, and use machine intelligence to identify and exploit weaknesses.

Combatting these threats requires an equally sophisticated, speedy, and coordinated response that includes the following:

- Indicator of compromise (IOC) enrichment
- Threat hunting and identification
- Breach mitigation
- Threat containment
- Eradication

Although modern security operations centers (SOCs) have many of these capabilities, transporting and coordinating threat information is a slow, error-prone, and labor-intensive process, a problem exacerbated by the shortage of qualified and experienced security personnel. This is arguably the most important challenge facing SOCs today.

Solution: Symantec Portfolio and Splunk's Phantom Security Operations Platform

Symantec and Splunk are working to unify our joint customers' security teams, their operations, and their SOC tools. We offer a broad range of Symantec products fully integrated with Splunk's Phantom Security Operations Platform. These include:

- Symantec Endpoint Protection (SEP)
- Symantec Advanced Threat Protection
- Symantec Content Analysis
- Symantec Security Analytics
- Symantec Data Loss Prevention

This integrated product set enables threat response processes to execute at machine speed while still allowing flexible levels of human oversight. Phantom automation and orchestration Playbooks speed the flow of accurate security event data from one Symantec product to the next. Mitigation, containment, and eradication processes run faster and are more accurate and consistent. Customers effectively execute their customized security response processes to stay well ahead of threats and attacks.

Benefits

- **Fully integrated response**—The Phantom Platform automatically orchestrates Symantec products, strengthening defenses and reducing risk.
- **Security at machine speed**—Phantom Playbooks orchestrate Symantec products at the API level, eliminating human delays.
- **Reduced dwell and response times**—Phantom translates best-practice security processes into electronic Playbooks that execute automatically, eliminating common business process delays.
- **SOC resources force multiplier**—Phantom automation frees analysts from mundane tasks, enabling SOCs to address more critical priorities.
- **Maximum ROI**—Phantom enables organizations to employ Symantec products across a broader range of integrated threat responses.

How it works

Customers use the large number of Symantec portfolio APIs, available as 'actions' in the Phantom Platform, to easily develop customized Playbooks that address security use cases reflecting their existing security procedures and processes.

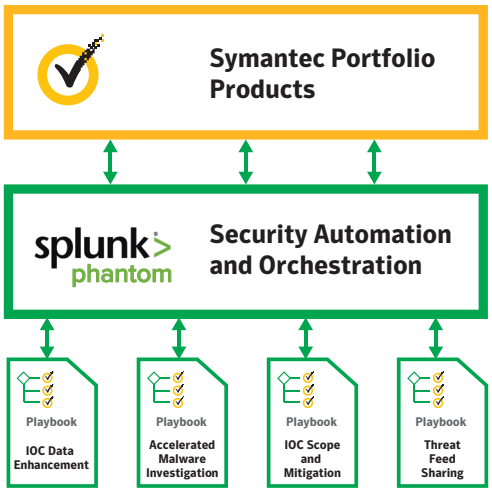
Symantec-based Phantom Playbook Examples

IOC data enhancement—When Symantec Content Analysis IOC data is handed off to the Phantom Playbook, it augments the data with threat intelligence information from third-party sources. The updated and enhanced IOC data is immediately returned to Content Analysis for further action.

Accelerated malware investigation—When Symantec Content Analysis finds a suspicious file, the Phantom Playbook automatically requests a file scan by the customer's preferred malware scanner(s). If malware is confirmed, the Playbook updates the customer's other security tools and asks security administrators to approve automated mitigation and remediation processes.

IOC scope and mitigation—When Symantec Content Analysis detects an IOC, the Phantom Playbook automatically queries the customer's endpoint detection and response (EDR) solution (including Symantec Advanced Threat Protection: Endpoint) to find endpoints that exhibit the same IOC. Affected endpoints are immediately isolated (if approved by administrators).

Threat feed sharing—When Symantec Content Analysis IOC data is handed off to the Phantom Playbook, it automatically formats and shares that data with the customer's internal threat feed systems (such as their STIX servers).



About Splunk

Splunk's Phantom Security Operations Platform helps you improve security and better manage risk by integrating your SOC team, processes, and tools. To learn more, visit the Splunk website.

About Symantec Technology Integration Partners (TIPs)

To learn more about Symantec TIPs, and the Technology Integration Partner Program, please visit the Symantec Technology Integration Partners page.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

19B192323_SB_Splunk_TIP_short