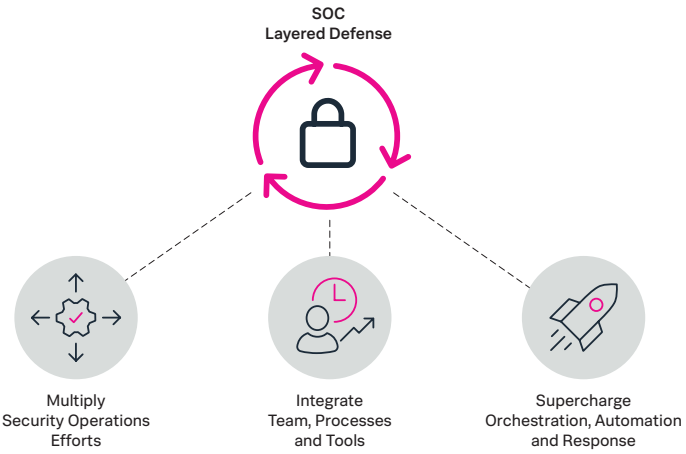
splunk> turn data into doing™

PRODUCT BRIEF

Splunk Phantom

Maximize Your SOC efficiency With Security Orchestration, Automation and Response (SOAR) Capabilities

- **Close your security skills gap** by force multiplying your security operations efforts
- **Integrate your team, processes and tools** for greater SOC efficiency
- **Supercharge your SOC** with advanced orchestration, automation and response capabilities



Security teams are working hard identifying, analyzing and mitigating threats facing their organizations.

These teams are also struggling with an endless assembly line of point products and independent static security controls with no orchestration between them. Add the fact that most companies do not have enough security personnel to analyze their volume of daily security alerts, and the result is a growing backlog of security incidents.

Organizations want to better leverage existing resources by deploying tools that maximize efficiency and scale, while creating a unified defense system that is greater than the sum of its parts.

Splunk® Phantom provides security orchestration, automation and response (SOAR) capabilities that allow analysts to improve efficiency and shorten incident response times. Phantom supercharges the scalability, performance and speed of your security automation with the ability to process 50,000 security events per hour. With Phantom, organizations are able to improve security and better manage risk by integrating teams, processes and tools together. Security teams can automate tasks, orchestrate workflows and support a broad range of security operations center (SOC) functions including event and case management, collaboration and reporting.

SOC Automation

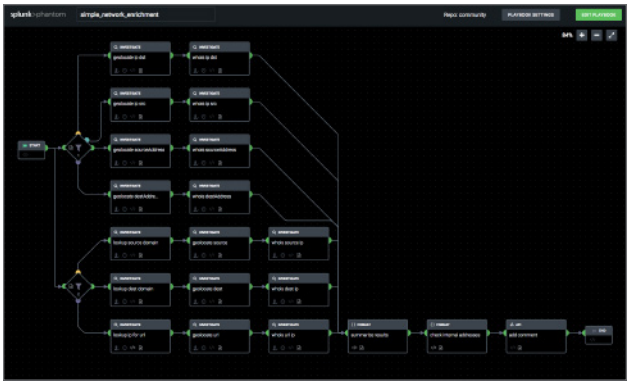
Phantom enables teams to work smarter by executing automated actions across their security infrastructure in seconds, versus hours or more if performed manually. Teams can codify workflows into Phantom's automated playbooks using the visual editor (no coding required) or the integrated Python development environment. By offloading these repetitive tasks, teams can focus their attention on making the most mission-critical decisions.

Orchestration

Phantom is the connective tissue that lets existing security tools work better together. By connecting and coordinating complex workflows across the SOC's team and tools, Phantom ensures that each part of the SOC's layered defense is actively participating in a unified defense strategy. Powerful abstraction allows teams to focus on what they need to accomplish, while the platform translates that into tool-specific actions.

Incident Response

Phantom helps security teams investigate and respond to threats faster. Using Phantom's automated detection, investigation and response capabilities, teams can execute response actions at machine speed, reduce malware dwell time and lower their overall mean time to resolve (MTTR). And now with Phantom on Splunk Mobile, analysts can use their mobile device to respond to security incidents while on-the-go. Phantom's event and case management functionality can further streamline security operations. Case-related data and activity are easily accessible from one central repository. It's easy to chat with other team members about an event or case, and assign events and tasks to the appropriate team member.



Ready to Learn More?

Download the free community edition of Splunk Phantom and get started today.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

20-14148-splunk-phantom-maximize-your-soc-efficiency-with-soar-PB-109