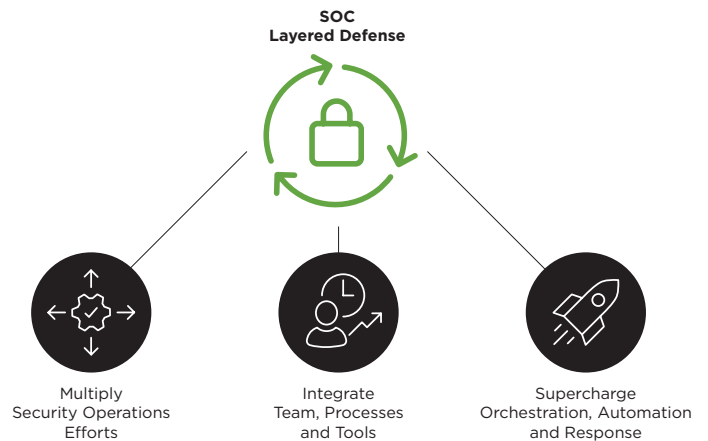


# SPLUNK® PHANTOM

Maximize your SOC efficiency with 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.** But 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 incidents, 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.

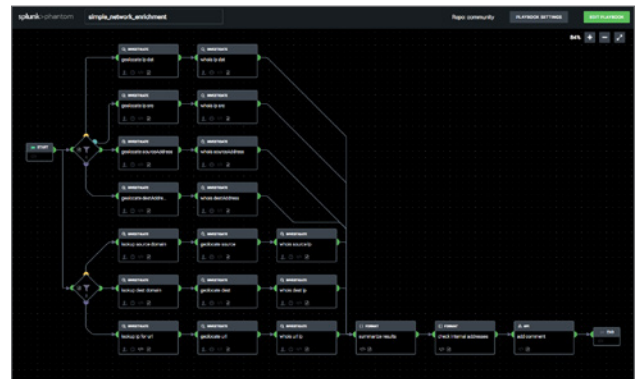
Phantom integrates security teams, processes and tools together to work smarter, respond to threats faster and strengthen defenses.



Splunk Phantom provides security orchestration, automation and response (SOAR) capabilities that allows analysts to offload repetitive tasks and focus their attention on making the most mission-critical decisions. Organizations are able to improve security and better manage risk by integrating teams, processes and tools together. With Phantom, security teams can automate tasks, orchestrate workflows and support a broad range of SOC functions including event and case management, collaboration and reporting.

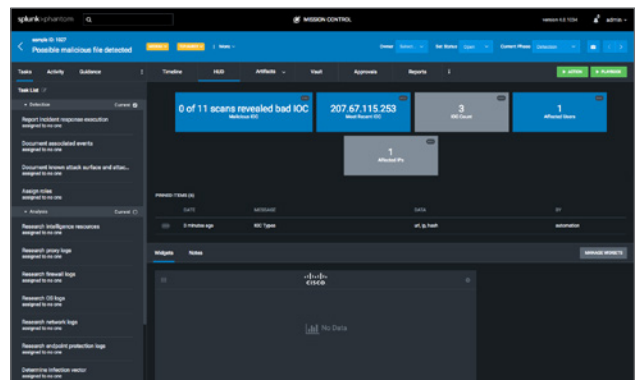
### SOC Automation

Use Phantom for event enrichment and programmatic triage to eliminate noise, pre-fetch threat intelligence at machine speed, support decision-making and prioritize the most critical events for human analysis. Conduct phishing investigations and process suspicious phishing emails in seconds. Increase security by automating repetitive steps in malware investigations and lower the overall mean time to resolve (MTTR).



### Incident Response

Phantom helps security teams investigate and respond to threats faster. Perform investigative security actions from the Mission Control interface, such as submitting files to a sandbox and query threat intelligence services without losing context of the investigation.



Use Phantom for case management to increase consistency with standard operating procedures, orchestrate human and machine tasks, and keep all case-related data and activity in one centralized location. Increase collaboration with the ability to chat with other team members about an event or case. Also use Phantom to assign events cases and tasks to the appropriate team member.

### Ready to Learn More?

Download the [free community edition](#) of Splunk Phantom and get started today



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

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