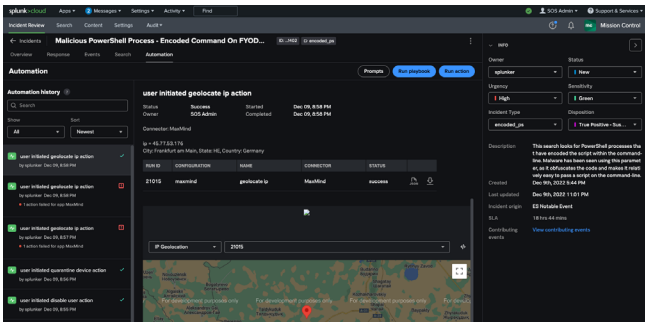
splunk>

PRODUCT BRIEF

Splunk Mission Control

Bring order to the chaos of your security operations

- **Unify** threat detection, investigation and response (TDIR) capabilities with data to take action based on prioritized insights.
- **Simplify** your security workflows by codifying your processes into response templates.
- **Modernize** and empower your security operations with the speed of security automation.



Overview

Now more than ever, your security team is faced with a wide range of challenges that span across people, process and technology. TDIR is spread across siloed tools while security insights are diffused across interfaces. This makes it difficult to achieve intelligent situational awareness or accurately assess security posture. Furthermore, security operations center (SOC) procedures and data are scattered across different systems making things difficult when investigating and responding to basic and advanced attacks.
Finally, your analysts are forced to investigate and respond manually to a continuous flood of incidents, resulting in slow incident response and reactive security operations.

It's time to bring order to the chaos of your security operations with Splunk Mission Control. Splunk Enterprise Security (ES) users can easily access Mission Control to enable a unified, simplified and modernized security operations experience for your SOC. With Mission Control, you can unify detection, investigation and response capabilities with data from any source. This helps you take action based on prioritized insights, simplify operations by codifying your processes into response templates, and modernize your SOC with security automation.

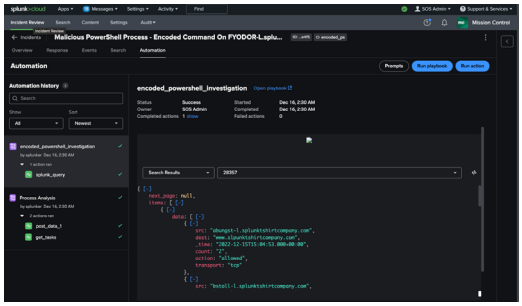
Adopting Mission Control unifies your security operations across Splunk's industry-leading security technologies and partner ecosystem within one work surface. This allows you to better understand business risk by seeing the entire picture of security insights and trends to detect what matters, investigate holistically and respond intelligently.

Capabilities

- **Security Analytics:** See a single queue of all your high fidelity incidents consisting of your prioritized Splunk ES notables and risk notables.
- **Standardized SOC Processes:** Speed up investigations with pre-built OOTB response templates that include embedded searches, actions, and playbooks to empower security analysts.
- **Orchestration, Automation and Response:** From day one, Mission Control users are able to launch playbooks to automate tasks and actions across your security stack, all from within the Mission Control interface.
- **Case Management:** Within your response templates, you may add custom notes containing intelligence data where needed and upload relevant files to document work within an incident investigation.
- **Metrics and Reporting:** Historical data from your response template tasks are stored within Mission Control allowing for detailed SOC metrics, reporting and auditability.
- **Embedded Splunk Search:** Mission Control comes equipped with native Splunk search surfaced in the Mission Control interface so you can conduct a search from within an incident without pivoting.
- **Threat Intelligence Management:** Threat Intelligence Management* provides SOC analysts with actionable intelligence and associated normalized risk scores for risk notable events.

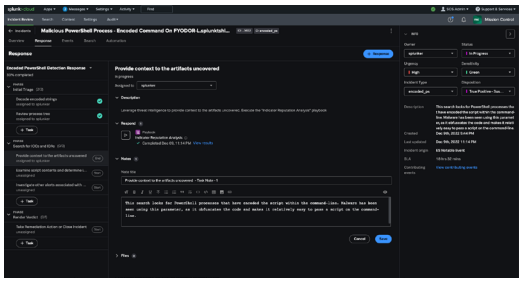
**regional limitations may apply.*

Customer outcomes



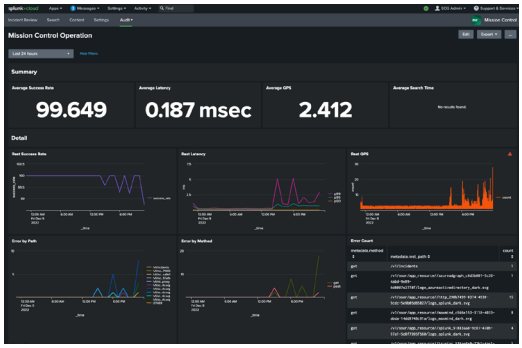
Quickly understand business risk

Mission Control allows you to determine risk faster, understand your priorities and close the right cases faster. See the entire picture of security insights and trends when you unify your SOC tools and data in a single work surface to detect what matters, investigate holistically and respond intelligently. Operate bi-directionally across Splunk ES and Splunk SOAR to pivot less between consoles and fuse threat intelligence into the process to decrease the time it takes to determine risk.



Streamline your security operations.

Improve SOC process adherence when you codify your operating procedures into pre-defined templates. Model your response plans based on pre-built templates that can be used for security use cases such as “Encoded PowerShell Response,” “Insider Threat” or “Ransomware.” Or build your own templates based on your established processes that are scattered across systems to finally achieve repeatable security operations. This allows you to rapidly initiate investigations in response to Splunk ES detections.



Be proactive and speed up by automating response

Automate manual, repetitive security processes across your integrated security stack for more proactive, empowered security operations. Ensure ES detections are responded to automatically and free up time to focus on mission-critical objectives. Run playbooks and actions directly within Mission Control to reduce console pivoting. Access Splunk’s open and broad connector ecosystem on Splunkbase to plug and play with the integrations you need across your security and IT use cases.

Ready to Learn More? Discover how **Splunk Mission Control** can unify, simplify, and modernize your security operations.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com