Mission Control

Detect, investigate and respond to threats from one modern interface

Unify threat detection, investigation and response (TDIR) capabilities

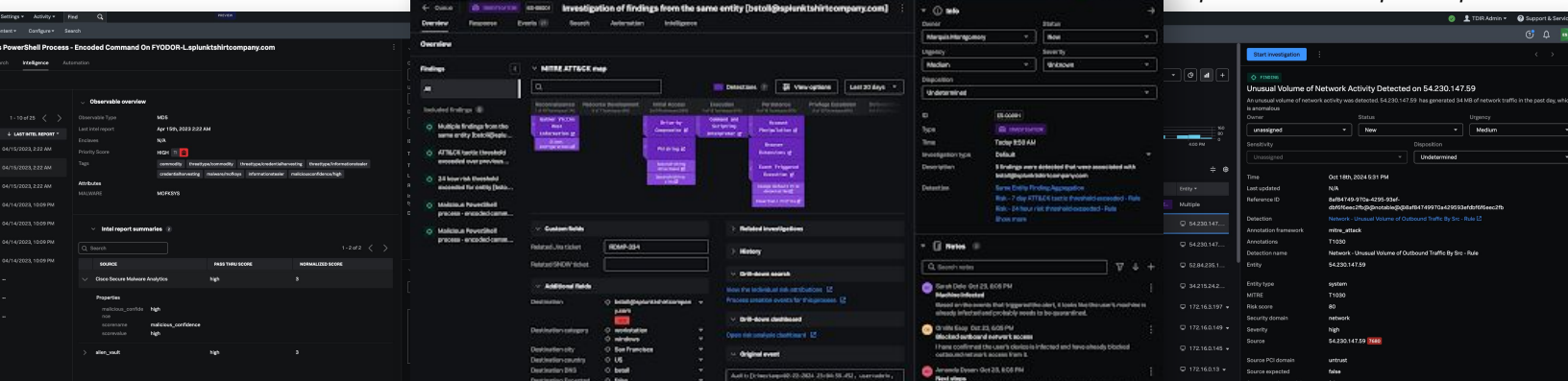
Simplify your security workflows

Modernize and empower your security operations

Security teams are 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, making it difficult to achieve intelligent situational awareness or accurately assess security posture. Security operations center (SOC) procedures and data are scattered across different systems making things difficult when investigating and responding to basic and advanced attacks. Analysts are forced to investigate and respond manually to a continuous flood of incidents, resulting in slow incident response and reactive security operations.

To enhance SOC efficiency, analysts must be equipped with a streamlined workflow experience that boosts productivity. Ensuring security analysts have access to a SIEM solution that provides the foundation to unify detection, investigation, and response to threats will bolster their confidence and efficacy in managing security risks.

As an integral feature of Splunk® Enterprise Security 8.0, Mission Control unifies your workflows across TDIR. This forever transforms how security analysts work by consolidating TDIR into a single, modern interface. Mission Control is natively integrated with Splunk's leading SOAR solution* across automated playbooks and actions, offering a unified work surface that dramatically improves both the mean time to detect (MTTD) and mean time to respond (MTTR) to incidents. Automated playbooks are infused with threat intelligence that brings together and normalizes the scoring of data sources. 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.



*Splunk SOAR subscription required

Holistic, comprehensive view: The Analyst Queue provides a centralized location that enables SOC analysts users to view Findings so that they can seamlessly prioritize and triage investigations.

Completely integrated workflow experience: One-click access to automate and orchestrate tasks within Splunk Enterprise Security. Speed up case management, alert triage, incident investigation, and incident response use cases, without leaving Splunk Enterprise Security.

Collaborate and execute incident response workflows: Response Plan templates allow users to see each phase of an incident response plan, assign key stakeholders to specific phases, and apply simple automation playbooks and workflows to tasks for quicker, more efficient remediation efforts. Add custom notes containing intelligence data where needed and upload relevant files to document work within an incident investigation.

Integrated intelligence: Threat Intelligence Management provides SOC analysts with actionable intelligence and associated normalized risk scores to better understand threat context and accelerate time to triage.

Accurate threat context: Intuitive side panel provides additional context around threats. View related information such as identified MITRE ATT&CK techniques, detections which triggered a Finding, playbooks that are automatically generated by Splunk SOAR* automation rules, review detailed notes and automation results in real-time — all in one view.

Resolve incidents in minutes: Native integration with Splunk SOAR enables analysts to contain and block threats all within Splunk Enterprise Security in a matter of clicks.*

Embedded Splunk search: Native Splunk search surfaced in the Mission Control interface so you can conduct a search from within an investigation without pivoting.

Quickly understand business risk

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 Enterprise Security and Splunk SOAR without pivoting between tools or tabs.

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.” Build your own templates based on established processes that are scattered across systems to finally achieve repeatable security operations. Rapidly initiate investigations in response to Splunk Enterprise Security detections.

Be proactive and accelerate response with automation

Automate manual, repetitive security processes across your integrated security stack for more proactive, empowered security operations. Ensure Splunk Enterprise Security 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.

**Splunk SOAR subscription required*

splunk>

Contact us: splunk.com/asksales

splunk.com