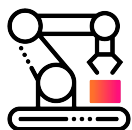


Splunk SOAR

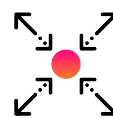
Empower your SOC with automation to speed up threat detection and boost effectiveness



Guided Automation
streamlines playbook building with real-time guidance



External prompts
engage end users and adjacent teams in collaborative incident response



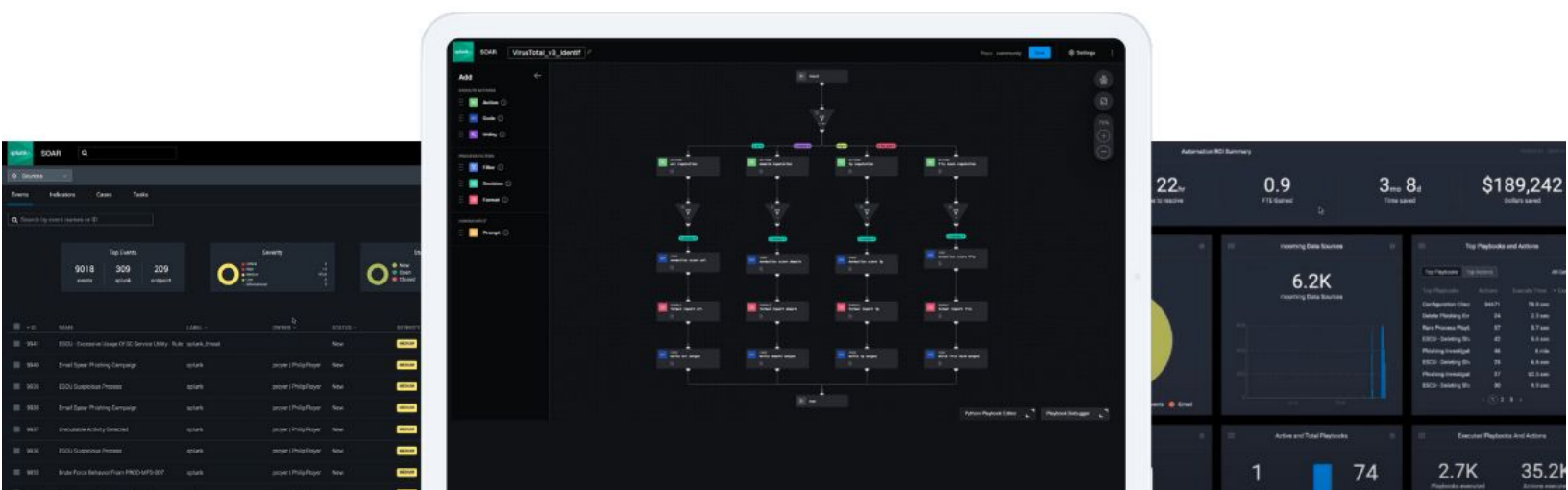
Seamless integration
with Splunk Enterprise Security empowering TDIR automation at scale

The Modern SOC Challenge

Security Operations Centers (SOCs) are facing unprecedented challenges in today's rapidly evolving threat landscape. Analysts are inundated with an overwhelming volume of security alerts, far exceeding their capacity to investigate and resolve each one effectively. Tier 1 analysts are overwhelmed by excessive, noisy alerts—spending most of their time triaging false positives and routine incidents. This alert overload leads to fatigue, increases the risk of missing real threats, and limits effective escalation to higher-tier analysts. Adding to the complexity, SOC teams must manage an ever-growing array of security tools, compounded by a persistent shortage of skilled cybersecurity professionals. This combination of analyst burnout, tool sprawl, and resource constraints makes it increasingly difficult to identify and respond to the most critical threats in a timely manner. SOC teams need a solution that simplifies workflows, enhances productivity, and delivers better security outcomes by enabling faster, more accurate threat detection and response.

The Splunk SOAR Solution

Splunk SOAR transforms the way SOC teams operate by providing security orchestration, automation, and response capabilities that empower analysts to take control of their environments. Through automation, Splunk SOAR eliminates tedious, manual tasks, enabling analysts to focus on higher-value work. By automating repetitive, low-risk tasks like alert triage and data enrichment, SOC teams can respond faster and more consistently, while reserving analyst expertise for complex or high-risk decisions. This reduces alert fatigue and maintains human oversight where it matters most. Splunk SOAR enhances operational efficiency and accuracy by seamlessly connecting security workflows across teams, tools, and processes. Additionally, it offers a comprehensive suite of features, including case management, integrated threat intelligence, collaboration tools, and detailed reporting. With Splunk SOAR, SOC teams can regain control, strengthen their defenses, and confidently navigate the ever-changing security landscape.



Recent Innovations in Splunk SOAR

Splunk SOAR continues to push the boundaries of security automation with innovative updates that empower security teams to work smarter and faster. This brief highlights key advancements from recent releases – including enhanced playbook development capabilities, seamless integration with Enterprise Security, and improved response capabilities – all designed to help teams navigate challenges with precision and efficiency.

Innovation Highlights Powering Automation at Scale

Accelerate Security with Intelligent Automation

- **Guided Automation:** Supports additional playbook blocks (Prompt, Format, Code, Utility) and includes a new Logs tab for easier testing and troubleshooting.
- **Prompt-Driven Automation:** Easily gather external approvals and inputs as part of your automated workflows.
- **Cisco Talos Integration:** Includes Cisco Talos threat intelligence and updated integrations (Webex, Secure Firewall, Secure Email and Web Manager), adding indicator intelligence and seamless orchestration to your playbooks.

Streamline Security Operations with Advanced Playbook Capabilities.

- **Conditional Filters:** Use multiple conditions and new operators to refine decision-making.
- **CrowdStrike Playbook Pack:** A newly released pack simplifies automation and enhances threat response capabilities.
- **Expanded Integration Support:** ES CMP + SOAR CMP pairing is now supported, along with ES FedRAMP High/Mod + SOAR Mod for improved flexibility and compliance.

Optimize Operational Efficiency

- **Visual Playbook Editor Shortcuts:** New copy-paste shortcuts allow quick, accurate playbook design by preserving data paths and settings.
- **Case Management and Reporting:** Comprehensive tools for tracking, collaboration, and actionable insights.
- **Azure Deployment Support:** Now supporting ES-SOAR deployments in Microsoft Azure for enhanced scalability and flexibility.



Contact us: splunk.com/asksales

splunk.com