Splunk SOAR

Empower your SOC with automation to increase productivity and respond to threats faster

Product Benefits

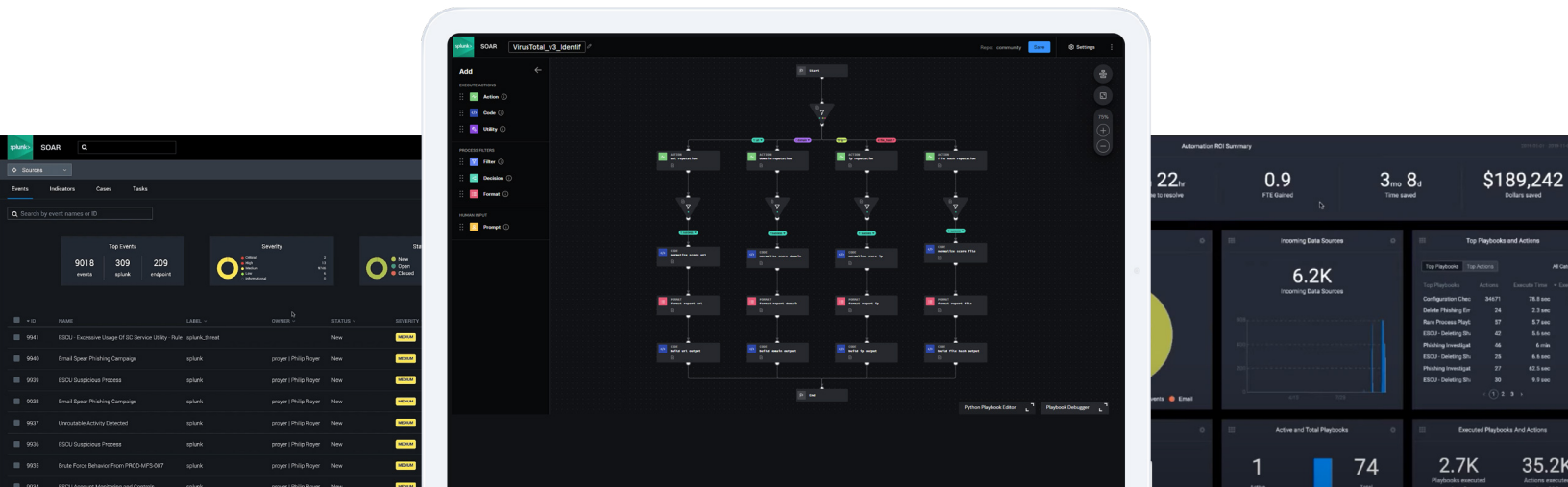
Bring order to a chaotic SOC by connecting and coordinating the tools in your security stack

Force multiply your team with the ability to prioritize alerts based on risk and reduce MTTD and MTTR

Respond with speed and accuracy through the power of automation playbooks and workflows

Security operations centers (SOCs) are overwhelmed. Analysts are drowning in a seemingly endless sea of security alerts — too many to fully investigate and resolve each day. Security operations work is rife with monotonous and repetitive tasks, especially at the Tier 1 analyst level. SOC teams not only struggle to manage an increasingly complex mix of security products, but a continued shortage of qualified cybersecurity professionals to help manage those products makes it increasingly difficult to respond to threats in an efficient and effective manner. With so many point products and alerts, SOC teams struggle to rapidly respond to the most pertinent threats. These security professionals need a way to break through the chaos and bring order to the SOC.

Splunk SOAR provides security orchestration, automation and response capabilities that empowers your SOC to go from overwhelmed to in control. Splunk SOAR allows security analysts to work smarter, not harder, by automating repetitive tasks; triage security incidents faster with automated investigation and response; increase productivity, efficiency and accuracy; and strengthen defenses by connecting and coordinating complex workflows across their team and tools. Splunk SOAR also supports a broad range of security functions including event and case management, integrated threat intelligence, collaboration tools and reporting.



Clear a vast majority of alerts and repetitive tasks with no human interaction

Splunk SOAR can streamline your response and automation processes by consolidating alerts and data from the various tools in your environment, ensuring timely and prioritized responses. Splunk's data-centric approach, backed by the power of machine learning, further amplifies its capabilities.

Force multiply your team

SOCs are short-staffed. There's a cybersecurity talent shortage. But with Splunk SOAR, you can make a team of 3 feel like a team of 10. Splunk SOAR's orchestration and automation capabilities enables teams to execute tasks quickly and efficiently, freeing up valuable time for them to focus on more strategic activities.

Get more out the security tools you have

Splunk SOAR is designed to integrate and enhance your security operations seamlessly. It orchestrates your security stack by connecting with 300+ third-party tools and supporting 2,800+ automated actions. This ensures that you can streamline complex workflows across various teams and tools without the need to massively overhaul your existing security stack.

Take prioritized action

Through better risk prioritization, Splunk SOAR helps reduce the mean time to detect critical threats and reduce threat investigation times from hours to minutes. Cutting down on threat dwell time allows for a more proactive approach. Additionally, built-in threat research and insights from the Splunk Threat Research Team help you make informed decisions and stay ahead of threats.

Automation made easy

Whether you're new to coding or a Python expert, Splunk SOAR provides you with the means to create and customize playbooks. The Visual Playbook Editor simplifies the playbook creation process by allowing you to assemble custom workflows with prebuilt code blocks and action strings. Splunk SOAR also features input playbooks for basic security and IT tasks, which can be integrated into larger playbooks and security workflows.

Read More >

Watch a Demo >

Take a Tour >

splunk>

Contact us: www.splunk.com/asksales

www.splunk.com

24-488201-Splunk-Splunk SOAR-PB-105