Splunk SOAR

Security Orchestration, Automation and Response (SOAR) Capabilities for the Modern SOC

- Automate alert triage and repetitive security tasks so you can work smarter and focus on mission critical objectives
- Investigate and respond to security incidents in seconds instead of hours
- Orchestrate workflows across your tools and team for increased SOC efficiency and productivity

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

The security operations center (SOC) is overwhelmed. Analysts are drowning in security alerts - too many to fully investigate and resolve each day. Security operations work is rife with monotonous, routine, repetitive tasks, especially at the Tier 1 analyst level. There is a shortage of over one million cybersecurity professionals with the necessary knowledge and expertise to adequately staff SOCs around the world. And mean time to detect, triage, and respond to threats is still too slow.

Stop being overwhelmed. Get in control. Splunk SOAR provides security orchestration, automation and response capabilities that empowers your SOC. Splunk SOAR allows security analysts to work smarter, not harder, by automating repetitive tasks; triage security incidents faster with automated detection, 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 automates alert triage, response, and manual repetitive tasks in seconds, instead of minutes or hours if performed manually. With the use of automated playbooks to orchestrate and execute actions across different point-products, security teams can eliminate analyst grunt work and increase analyst efficiency, all while freeing up time to focus on mission-critical tasks. Say goodbye to alert fatigue. Now, your team can go from overwhelmed to in-control.

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 can automate repetitive tasks, investigation and response so your security team can increase productivity and do more with the people you already have.

Make your tools work better together

Splunk SOAR orchestrates workflows and response across your IT and security stack so that each product is actively participating in your defense strategy. This strengthens your defenses by integrating existing security infrastructure together, creating a mesh of protection that is more difficult to penetrate. Splunk SOAR supports 350+ third-party tools and 2,400+ actions, so you can connect and coordinate workflows across teams and tools. This not only increases the speed of your investigation and response, but unlocks value from previous investments.

From 30 minutes to 30 seconds

Mean time to detect, triage, and respond to threats is too slow. With Splunk SOAR, respond to threats in seconds - not minutes or hours. Lower your mean time to detect (MTTD) and mean time to respond (MTTR) to threats using automated playbooks that automate security tasks across a multitude of tools at machine speed.

SOAR your own way

Deploy SOAR in a way that best supports the needs of your business, streamlines security operations, and facilitates your digital transformation. Splunk SOAR supports on-premises, cloud or hybrid deployments.

Learn more about Splunk SOAR features and functionality.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

21-14148-Splunk SOAR-PB-110