Understanding the features of SOAR

Main dashboard

Splunk SOAR’s main dashboard provides an overview of all your data and activity; notable events and their severity; playbooks; connections with other security tools; team workloads; and a summary of ROI from automated actions.

- To watch a video that explains this feature, click here.

Apps

Apps are the integration points between Splunk SOAR and your other security technologies. Through apps, Splunk SOAR directs your other security tools to perform “actions.” Splunk SOAR’s app model supports 300+ tools and 2000+ APIs, so you can connect and coordinate workflows across your team and tools.

- To watch a video that explains this feature, click here.
- To search available apps, click here.

Event management

Analysts are often overwhelmed with a large volume of security events. Splunk SOAR makes event management easy by consolidating all events (from multiple sources) in one place. Analysts can sort and filter events to quickly identify high fidelity notable events and prioritize action.

- To watch a video that explains this feature, click here.

Case management

Integrated case management allows you to easily promote a verified event to a case. It also allows continued access to all tools, features and data available in one interface. Case Management supports case tasks that map to your defined Standard Operating Procedures (SOPs). It also provides full access to the Splunk SOAR automation engine, allowing you to launch actions and playbooks as part of a task.

- To watch a video that explains this feature, click here.
Splunk SOAR on Splunk Mobile

Security orchestration, automation and response is available from your mobile device. Work smarter, respond faster and strengthen your defenses, all from the palm of your hand. Respond to events faster than ever because, via your mobile device, you’re reachable from anywhere. Run playbooks, triage events and collaborate with colleagues on the go.

• To watch a video that explains this feature, click here.