

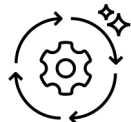
Splunk Agentic SOC Activation

A force multiplier for your security operations

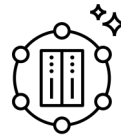
An agentic SOC functions as a significant force multiplier by transitioning security operations from manual, playbook-bound processes to an autonomous, adaptive ecosystem. By operationalizing AI agents in the Splunk Enterprise Security and SOAR environment, organizations can automate complex, multi-stage decision-making, perform real-time cross-telemetry correlation, and execute sophisticated remediation workflows at machine speed.



Reduce alert fatigue with
AI-driven prioritization



Defend autonomously to
reduce MTTD/MTTR



Activate a force
multiplier for your SOC



Shift from reactive to
proactive defense

Transform your SOC with a proactive, AI-driven agentic workforce

By activating Splunk AI Agents, you integrate cognitive automation into your security stack. These agents continuously learn from your environment, automatically triaging alerts, correlating disparate events into meaningful narratives, and providing suggested remediation paths. They function as an always-on, intelligent extension of your team that handles the heavy lifting of initial incident analysis and response.

The Splunk Agentic SOC Activation service helps you operationalize a fleet of Splunk AI Agents that act as an intelligent layer that automates the triage, correlation, and initial investigation of security events, effectively acting as a force multiplier for your security team.

AI-driven prioritization reduces alert fatigue and ensures your analysts focus on high-fidelity, high-risk incidents, significantly reducing the noise associated with false positives.

This evolution allows security teams to move beyond mere alert triaging, enabling them to handle the high velocity and volume of modern threats with consistent precision. Consequently, this architecture reduces Mean Time to Respond (MTTR) and allows for the scaling of operational capacity without requiring a proportional increase in headcount.

Shift your SOC from a reactive posture to an autonomous one, where patterns are recognized and threats are neutralized before they can impact business operations.

Benefits

- **Tuned detection content** to enhance Agent actions and outputs
- **Autonomous investigation** with pre-correlated context and automated root-cause analysis
- **Higher analyst throughput** with more time spent threat hunting and detection engineering
- **Production-ready playbook library** to automate SOAR response playbooks
- **RBAC and governance guardrails** to control access and model-selection guardrails with Human-in-the-Loop Governance, so agents operate within their authorized scope
- **Closed loop feedback** where outcomes from each case feed back into the SOP Agent and Detection Builder Agent for continuous learning and improvement

Powering the Agentic SOC

Splunk Enterprise Security expands AI from assistive productivity into purpose-built agentic workflows that help security teams detect, investigate, respond, and govern with greater speed and consistency. Together, these agents reduce repetitive work and investigation friction, giving analysts more room to focus on judgment, strategy, and high-impact response. Instead of asking analysts to manually create detections, interpret every alert, translate SOPs, or build automations from scratch, Splunk brings AI directly into the workflows where security work happens.

Splunk Security Agents

Splunk AI Assistant	The AI Assistant in Security surfaces relevant insights, automates repetitive steps, and guides analysts through everyday investigation workflows.	<ul style="list-style-type: none">• ES Essentials• ES Premier
Detection Builder Agent	The Detection Builder Agent reduces the time it takes to create, implement, and start getting value out of security detections.	<ul style="list-style-type: none">• ES Essentials• ES Premier
SOP Agent	The SOP Agent imports standard operating procedures (SOPs) into ES response plans using multi-modal LLMs to fuel agentic responses.	<ul style="list-style-type: none">• ES Essentials• ES Premier
Triage Agent	The Triage Agent evaluates, prioritizes, and explains alerts, reducing workloads and highlighting critical issues.	<ul style="list-style-type: none">• ES Premier
Malware Threat Reversing Agent	The Malware Threat Reversing Agent instantly summarizes malware threats and accelerates triage and remediation with step-by-step breakdowns of malicious scripts	<ul style="list-style-type: none">• ES Premier
Automation Builder Agent	The Automation Builder Agent turns plain language into tested SOAR playbooks — no deep Visual Playbook Editor knowledge needed.	<ul style="list-style-type: none">• ES Premier
Guided Response Agent	The Guided Response Agent provides real-time context and in-workflow actions based on standard operating procedures (SOPs) to ensure rapid, compliant resolution.	<ul style="list-style-type: none">• ES Premier

What We'll Do and Deliver

The Splunk Agentic SOC Activation offering is broken down into the phases and activities listed below. At the completion of the Design & Governance phase, our team will present the **Security AI Agent Readiness Report** and review your overall **Readiness Scorecard**. Readiness scores below 32 will require additional foundation and remediation work before proceeding with implementation.

Offering at a Glance	
Engage & Validate	<ul style="list-style-type: none">• Validate Splunk Enterprise Security (ES) environment• Perform prerequisite checks for ES Editions and licensing• Verify Splunk ES components are paired and reachable• Validate data normalization foundation and CIM compliance baseline
Discover & Assess	<div><ul style="list-style-type: none">• Conduct discovery workshops• Establish SOC transformation baseline• Review current-state SOC operating model• Map alert lifecycle stages and perform workflow assessment• Review AI readiness, Agent readiness, and data readiness• Generate AI readiness scorecard and agent readiness matrix</div> <div><p>Deliverable</p><p>Security AI Agent Readiness Report</p><ul style="list-style-type: none">• Executive Summary• Current-state SOC Assessment• Data & Splunk Platform Readiness• Target Operating Model• Use Case Library• Governance & Human-in-the-Loop• Playbook & Detection Framework• Implementation Roadmap• Appendices: Interview Notes, Work Products & Matrices</div>
Design & Governance	<ul style="list-style-type: none">• Define target-state human + AI operating models• Define governance, observability, and staffing implications• Build use case library and response playbook approach• Define governance framework and human-in-the-loop• Create implementation roadmap and executive summary
Implementation	<ul style="list-style-type: none">• Execute the implementation roadmap• Activate Splunk Agents in dependency order• Review and apply Agent best practices and prompts• Establish SOAR playbook factory• Convert manual runbooks into modular SOAR playbooks• Transfer knowledge to SOC analysts for their new agentic workforce

Readiness Score

The **Security AI Agent Readiness Report** includes your Readiness Score for implementation of the Splunk Security Agents. Readiness scores below 55 will require additional foundation and remediation work before proceeding with implementation. Additional scope can be added to the Implementation phase to have the work completed by Splunk Professional Services.

- **Score 80 - 100:** Ready for Implementation
- **Score 55 - 79:** Conditionally ready, some REMEDIATION actions required.
- **Score < 55:** Foundation work required (CIM | RBA | TUNING)

Additional Scope (as needed)

Additional foundation and remediation work may be required to maximize signal quality to ensure better agent outcomes. Below are the types of work that may be needed based on your Readiness Score.

CIM	RBA	TUNING	REMEDICATION
Review CIM (Common Information Model) compliance baseline	Enhance Risk-Based Alerting (RBA) capabilities	Review current correlation searches and alert volumes	Perform other remediation actions to Splunk environment as specified in the Security AI Agent Readiness Report
Normalize data ingest to CIM standards	Implement custom risk factors for top detections	Identify highest-volume searches with high false positive rates	
	Tune risk incident rules to reduce noise	Apply various tuning techniques to reduce alerts	
	Validate UEBA scores feed into the risk index		

Resilience, let's build it together

Splunk Customer Success provides end-to-end success capabilities at every step of your resilience journey to accelerate time to value, optimize your solutions and discover new capabilities. We offer professional services, education and training, success management and technical support, surrounding you with the expertise, guidance and self-service success resources needed to drive the right outcomes for your business. For more information contact us at sales@splunk.com.

Terms and Conditions

This Solution Guide is for informational purposes only. The services described in this solution guide are governed by the applicable fully signed ordering document and any incorporated terms and conditions.



Contact us: splunk.com/asksales

splunk.com

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2026 Splunk LLC. All rights reserved.