Setting the Agentic SOC into Motion

Security is no longer measured solely by its ability to reduce risk. As organizations scale AI across the enterprise, the SOC is increasingly expected to enable innovation, transformation, and growth.

Yet many security teams are struggling to keep up. Data volumes continue to grow, workflows remain fragmented, and AI-driven attacks are becoming more sophisticated. Yet, Splunk's 2025 State of Security report found that nearly half of SOC teams spend more time maintaining their existing tools than defending their organizations.

Traditional approaches to security operations weren't built for this level of speed, scale, and complexity.

The agentic SOC offers a new model. By bringing together high-quality data, advanced analytics, integrated tooling, and human-centered AI, security teams can operate with greater context, consistency, and confidence. Less time managing technology. More time advancing the business.

So where do you begin? Start with the questions that matter. Splunk and Presidio can help explore practical steps for turning the vision of the agentic SOC into an operational reality.

59%

of security leaders have moderately or significantly boosted their SOC's efficiency using AI.

Source: Splunk, State of Security 2025

Charting your course to the agentic SOC with Splunk and Presidio

The journey to an agentic SOC begins with understanding whether your organization has the data, processes, and operating model required to put AI to work effectively and responsibly.

Use the questions below to assess your readiness and identify opportunities to accelerate your progress.

Question to ask	What action should I take?
Can analysts access the data they need to investigate and respond effectively? Yes: ☐ No: ☐	☐ Identify data silos that limit visibility. ☐ Prioritize a unified data strategy across security domains. ☐ Establish consistent access to security data.
Are your tools working together without creating additional complexity? Yes: ☐ No: ☐	☐ Map analyst workflows and identify friction points. ☐ Consolidate disconnected processes where possible. ☐ Evaluate opportunities to unify detection, investigation, and response.
Can your team confidently prioritize the threats that matter most? Yes: ☐ No: ☐	☐ Assess how alerts are correlated and prioritized. ☐ Adopt risk-based approaches that reduce noise. ☐ Ensure analysts have the context needed to make decisions quickly.
Do you have a clear path toward an agentic operating model? Yes: ☐ No: ☐	☐ Define measurable outcomes for the SOC. ☐ Align people, processes, and technology around those goals. ☐ Create a roadmap for introducing agentic capabilities over time.

If you answered “no” to any of these questions, it may be time to take a closer look at your security operating model.

The path to the agentic SOC looks different for every organization. Whether you're just getting started or building on existing investments, Splunk and Presidio can help you assess your readiness, prioritize your next steps, and turn vision into action.

Presidio

SplunkSolutions@presidio.com

splunk> a CISCO company | PRESIDIO®

www.splunk.com
www.presidio.com