NEWS RELEASE

Cisco Elevates the SOC with Agentic AI for Faster Threat Response and Reduced Complexity

2025-09-09

Splunk Enterprise Security Premier Edition and Essentials Edition advance unified threat detection and response

BOSTON, Sept. 9, 2025 /PRNewswire/ -- SPLUNK .CONF -- Cisco today introduced Splunk Enterprise Security Essentials Edition and Splunk Enterprise Security Premier Edition, providing customers two agentic AI-powered SecOps options that unify security workflows across threat detection, investigation, and response (TDIR). Delivered within Splunk Enterprise Security 8.2 – a market-leading SIEM solution – these advancements streamline offerings and empower customers with faster threat response and simplified security solutions. Cisco also unveiled a series of AI features that it intends to release to power the agentic Security Operations Center (SOC) of the future, enabling analysts to focus on strategic decision-making while AI handles routine tasks.

With many Cisco security products already integrated with Splunk Enterprise Security, the latest features will place agentic AI at the core of the SOC and extend security intelligence seamlessly across the network. With Splunk, AI agents do more than actively orchestrate and automate complex workflows; they transform manual tasks into proactive, autonomous security operations. This transformation streamlines comprehensive threat management, empowering security teams to act faster and more efficiently.

"Adversaries are already using AI, so defenders need to seize every possible advantage," said Mike Horn, SVP and GM for Splunk Security. "Our security offerings unify detection, investigation, and response into a single, intuitive workspace, eliminating tool fragmentation and significantly boosting efficiency. Built-in AI can help cut alert noise and reduce investigation time from hours to minutes. Now every SOC can better position to stay ahead of advanced threats and empower analysts at every level."

Powering the Agentic SOC
Many organizations drown in data but struggle to know what matters and when to act. This leads to operational blind spots and inefficiencies across SecOps, ITOps, and engineering teams. It delays timely

detection and response exposing the business to avoidable threats.

To help prevent these issues and build an agentic SOC with greater visibility and context, customers can select between two flexible solutions:

- **Splunk Enterprise Security Premier Edition:** Brings together Splunk Enterprise Security 8.2, Splunk SOAR, Splunk UEBA, and Splunk AI Assistant into a comprehensive offering with unified user experience.

- **Splunk Enterprise Security Essentials Edition:** Combines Splunk Enterprise Security 8.2 and Splunk AI Assistant in Security into a single offering with unified user experience.

"With today's increasingly sophisticated threats and sprawling attack surfaces, security teams can't afford to waste time switching between fragmented tools and operating with siloed visibility," said Michelle Abraham, Research Director, Security and Trust at IDC. "By integrating multiple security capabilities into a single, cohesive environment, security platforms empower organizations to move from reactive to proactive security, streamlining workflows, improving detection and response, and ultimately reducing risk."

Agentic AI for Security
As security challenges become more complex, organizations need integrated solutions that enhance visibility, accelerate detection, and streamline response. Additional AI-powered advancements are being released to strengthen security operations through the following:

- **Triage Agent:** AI-powered triage evaluates, prioritizes, and explains alerts—even in long-tail, low-volume cases—reducing analyst workload and surfacing what matters most.
- **Malware Reversal Agent:** AI-driven reversing explains malicious scripts line-by-line, extracts indicators of compromise, flags evasion, and groups recurring behaviors.
- **AI Playbook Authoring:** Translates natural language intent into functional, tested SOAR playbooks, with AI helping every step of the way.
- **Response Importer:** AI agents adhere to standard operating procedures (SOPs) defined by the SOC and use multi-modal LLMs to import SOPs into Enterprise Security response plans.
- **AI-Enhanced Detection Library:** Helps detections to go from hypothesis to production in minutes.
- **Personalized Detection SPL Generator:** Personalizes detections within the library to align with unique SOC environments to make them usable out of the box.

Cisco Integrations Accelerate the SOC with Agentic AI
By integrating with Cisco's security solutions, Splunk helps security teams detect, investigate, and respond to threats with greater speed and precision. Expanded offerings will include:

- **Isovalent Runtime Security (eBPF) into Splunk:** Delivers immediate, granular visibility across your workloads, quickly pinpointing potential security breaches and infrastructure anomalies.
- **Federating Cisco Firewall Data:** Integration between Splunk Cloud Platform's Federated Search for Amazon S3 and Security Analytics and Logging (SAL) will enable analysts to perform security analytics on firewall logs stored in SAL directly from Splunk Cloud Platform without the need for ingestion.

Availability

- Splunk Enterprise Security Essentials Edition is available to all global regions, and Splunk Enterprise Security Premier Edition is available in early access.
- Splunk AI Assistant in Security is available to all global regions.

- Cisco integrations and additional capabilities including Triage Agent, AI Playbook Authoring, Response Importer, AI-Enhanced Detection Library and Personalized Detection SPL Generator will be available in 2026.

For more details on all of Splunk's .conf25 announcements, please visit our newsroom. Availability dates and regions are subject to change.

About Cisco
Cisco (NASDAQ: CSCO) is the worldwide technology leader that is revolutionizing the way organizations connect and protect in the AI era. For more than 40 years, Cisco has securely connected the world. With its industry leading AI-powered solutions and services, Cisco enables its customers, partners and communities to unlock innovation, enhance productivity and strengthen digital resilience. With purpose at its core, Cisco remains committed to creating a more connected and inclusive future for all. Discover more on The Newsroom and follow us on X at @Cisco.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word 'partner' does not imply a partnership relationship between Cisco and any other company.

About Splunk LLC
Splunk, a Cisco company, helps build a safer and more resilient digital world. Organizations trust Splunk to prevent security, infrastructure and application issues from becoming major incidents, absorb shocks from digital disruptions, and accelerate digital transformation.

Splunk and the Splunk> logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word "'partner"' does not imply a partnership relationship between Cisco or its affiliates and any other company.

Futures Disclaimer: Many of the products and features mentioned are still in development and will be made available as they are finalized, subject to ongoing evolution in development and innovation. The timeline for their release is subject to change.

View original content to download multimedia:https://www.prnewswire.com/news-releases/cisco-elevates-the-soc-with-agentic-ai-for-faster-threat-response-and-reduced-complexity-302549929.html

SOURCE Cisco