splunk> a CISCO company

CUSTOMER STORY

Asurion Builds Trusted Agents with Splunk AI Assistant 2.0

Key Challenges

To modernize its security operations, Asurion needed an AI tool that understands the company's unique environment and delivers reliable outputs.

Key Results

With Splunk AI Assistant 2.0, Asurion has built the foundation for an agentic SOC, saving hours of manual work and boosting AI trust with custom, context-driven guardrails.

asurion

Industry: Technology

Products: Splunk Cloud Platform, Splunk Enterprise Security

Solutions: Platform, Security

Capabilities: Security Orchestration, Automation, and Response (SOAR), Splunk AI Assistant, Splunk Federated Search

Protecting customers' technology on the front end requires trusted AI agents on the back end.

From smartphones to tablets and from dishwashers to electric scooters, Asurion insures, repairs, and provides expert support for everyday technology. The company safeguards millions of devices worldwide, serving major telecom, e-commerce, and direct-to-consumer clients.

For over 15 years, Splunk has been central to Asurion's 24/7 SOC. The company's SIEM architecture and engineering team manages the entire data pipeline and provides expert support in threat intelligence, forensics, and security validation. To support these efforts, they rely on Splunk Enterprise Security for investigations and proactive threat hunting, alongside its Security Orchestration, Automation, and Response (SOAR) feature to streamline daily alert management.

Following a recent corporate directive to embrace AI for enhanced productivity, Bill Ouellette, senior manager of SIEM architecture and engineering for Asurion, and his team embarked on an epic AI adoption journey. Their success ultimately laid the groundwork for an agentic SOC and established Asurion as key design partners for the next generation of Splunk AI Assistant.

Outcomes

- 140 Enterprise Security notables validated in one session
- 14 saved searches flagged in a single fleet-level GEOIP catch
- Increased trust in AI outputs via the Admin Instructions feature

When building agentic trust, context is king

Ouellette began transitioning his team to an agentic framework, empowering AI to autonomously manage complex tasks. He developed an internal AI system to match the right model to each task, emphasizing the importance of context and precise prompting. "To make an agent truly useful, you must build in clear context about your environment," Ouellette explains. He goes on to say that, ultimately, his priority is trust: "When deploying an agent to end users, I must be certain that the output is grounded in verified, accurate data."

The problem was that Ouellette's original agentic systems did not have deep Splunk knowledge and often failed when applied within Asurion's Splunk environment.

Ouellette knew that to build a truly reliable model, he had to tap into Splunk's own resources, like product code and engineering documentation. That's when he called the Splunk AI Assistant team.

Transforming the environment into AI intelligence

Ouellette began sharing ideas for Splunk AI Assistant 2.0 based on his experience as a platform owner. "Splunk has been a long-term partner for us, so I made it my mission to help grow their platform alongside our internal capabilities," he says.

Now, with the new Admin Instructions feature, any user can tailor Splunk AI Assistant to fit their organization. "Admin Instructions allows you to feed in your own best practices and data, ensuring the agent understands the nuances of your environment," says Ouellette. "Critically, it allows you to stay in the driver's seat with easily defined guardrails like data sources, indexes, tags, and owners."

"We remain dedicated to a human-in-the-loop model within our SOC. Although we're rapidly expanding our AI capabilities, these tools are designed to support, not replace, human expertise," says Jordan Kramer, senior director of cyber operations and identity at Asurion. "That's why the guardrails provided by Splunk are essential. They ensure that as our workflows evolve, human oversight remains the cornerstone of our threat identification and remediation processes."

"My primary goal was to provide context to ensure accurate AI outputs," Ouellette continues. "With Splunk AI Assistant 2.0, I can establish clear context and boundaries for my AI, knowing that the responses will be trustworthy."

We remain dedicated to a human-in-the-loop model within our SOC. Although we're rapidly expanding our AI capabilities, these tools are designed to support, not replace, human expertise. That's why the guardrails provided by Splunk are essential. They ensure that as our workflows evolve, human oversight remains the cornerstone of our threat identification and remediation processes.

Jordan Kramer, Senior Director of Cyber Operations and Identity, Asurion

Asurion also made Splunk AI Assistant 2.0 more intuitive by championing natural language prompting. When he initially evaluated the tool, Ouellette found that it was primarily an SPL assistant, requiring expertise from the end-user to use. Now, instead of relying on SPL knowledge, Splunk AI Assistant 2.0 delivers an intuitive, outcome-driven experience.

"While version 1.0 was built primarily for admins and engineers, Splunk AI Assistant 2.0 functions more like a helpful chatbot, making it easy for anyone to retrieve information without needing to be a power user like me," says Ouellette. "If I could scale myself, I would. But I can't be everywhere at once."

Scaling a cloud migration from manual to machine speed

Asurion was just beginning its migration journey to Splunk Cloud Platform when Ouellette began stress-testing the new Splunk AI Assistant Agent Mode feature. He initiated a project to migrate hundreds of use cases and notables to the cloud, a tedious process that typically means manually exporting, verifying, and debugging each search.

Instead, Ouellette used Agent Mode to validate 140 notable rules in a single session — a feat that left him genuinely amazed. The efficiency continued as the team faced a fleet-level compatibility challenge. Upon discovering that GEOIP was unsupported on Splunk 10.1, Agent Mode instantly pinpointed 14 affected saved searches, turning a major operational headache into a minor hiccup.

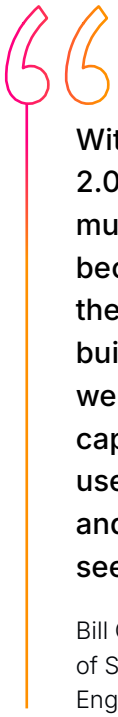
Ouellette estimates that Agent Mode compressed 50 hours of grueling validation work into just two, allowing him to focus on higher-level strategy planning. But Agent Mode really proved its worth when it caught a critical misconfiguration that a manual audit had missed. This finding secured Ouellette's confidence in the tool.

Agent Mode's ability to grasp the project scope and execute it reliably transformed Ouellette's workflow overnight: The system was fully agentic, autonomously carrying out the program from start to finish.

"With Splunk AI Assistant 2.0, we can do things much quicker," says Ouellette. "That's because we trust the product. We've built in that context; we understand its capabilities. We're able to use it to its full potential and look forward to seeing it evolve."

"Time is our biggest constraint," Ouellette admits. "But the more time we save, the more we can focus on getting alerts to the SOC and keeping our customers safe."

Welcome to the agentic era.



With Splunk AI Assistant 2.0, we can do things much quicker. That's because we trust the product. We've built in that context; we understand its capabilities. We're able to use it to its full potential and look forward to seeing it evolve.

Bill Ouellette, Senior Manager of SIEM Architecture and Engineering, Asurion

Connecting data dots without the heavy lifting

Asurion's agentic SecOps journey shows the capabilities of Cisco Data Fabric powered by the Splunk Platform, enabling Asurion to unify security data, gain better context, and build reliable, automated operations.

Ouellette appreciates that Splunk uses the Model Context Protocol (MCP) to make AI more accessible, empowering customers to build their own agents without vendor lock-in. Splunk MCP acts as a critical bridge, allowing Asurion's custom agents to access and correlate data sets that exist outside the Splunk environment. "By centralizing our MCP servers with Splunk, we now have a unified hub for our agents to gather information across different sources," says Ouellette. "We've grown our internal AI capabilities exponentially with access to much deeper insights."

The company also uses Splunk Federated Search in Transparent Mode to bridge its on-premises and Splunk Cloud environments, letting them search across both infrastructures seamlessly without a full-scale data migration. Meanwhile, Federated Search for Amazon S3 addresses the team's data retention requirements. This configuration is a gamechanger for their Enterprise Security operations, as it provides long-term S3 storage without losing the ability to query that data on demand. "We maintain consistent service levels for our internal customers through flexible, cost-effective, long-term data access and a unified search experience," Ouellette says.

Beyond seamless data access, the company realized that true agility requires syncing its cloud strategy with smart resource management. Early in Asurion's cloud migration, juggling a wide range of SKUs made it difficult to distribute resources precisely. The Splunk Cloud Flex program transformed how the company handles long-term contracts by ditching the old, rigid way of assigning resources. "With Splunk Cloud Flex, we can easily pivot resources to meet shifting business priorities," says Ouellette. To him, this flexibility provides significant peace of mind. "Offering this program — which allows us to manage our environment with greater speed and efficiency — demonstrates Splunk's commitment to its customers."

Creating an agentic future that works for everyone

"To be a design partner on Splunk AI Assistant 2.0 means Splunk genuinely values its customers and user experience," says Ouellette. "As platform users, we often identify opportunities for product evolution. The ability to engage directly with Splunk to share these ideas and receive validation — knowing they are committed to integrating that feedback — is the hallmark of a successful partnership. This collaborative approach ensures that their products continue to evolve in ways that provide lasting value for everyone."

Building on this foundation, Ouellette is already working with Splunk to advance next-gen AI Assistant capabilities, like dynamic model transitions based on real-time requirements. Drawing on his experience with task-specific model selection, the goal is to improve the AI Assistant's performance while curbing token use across the enterprise.

Ultimately, the partnership's true value stems from a shared vision: evolving the platform to drive success for every user. "Our motivation to partner with Splunk in this way extends beyond our immediate needs," Ouellette continues. "We always consider how these enhancements can benefit the broader Splunk community and contribute to everyone's long-term growth."

To Ouellette, the possibilities for tomorrow are endless. Beyond pioneering his team's agentic workflows, he's partnering with Asurion's security analysts to shape their agentic SOC strategy, training them to use Splunk AI Assistant in Enterprise Security to create trusted agents for automated playbook execution. "Integrating Splunk's built-in services with custom agents has become a cornerstone of our AI strategy," Ouellette concludes. "We've scaled further than we ever imagined."