CISCO Connect

Splunk for SecOps: AI, Agentic AI, Optimized Workflows and Automation

Niklas Blomquist – Strategic Security Advisor

Date placeholder

Agenda

01 Splunk platform

02 Common Security Use-cases

03 Splunk Apps

04 AI Do It Yourself

05 Splunk AI Assistant for SPL

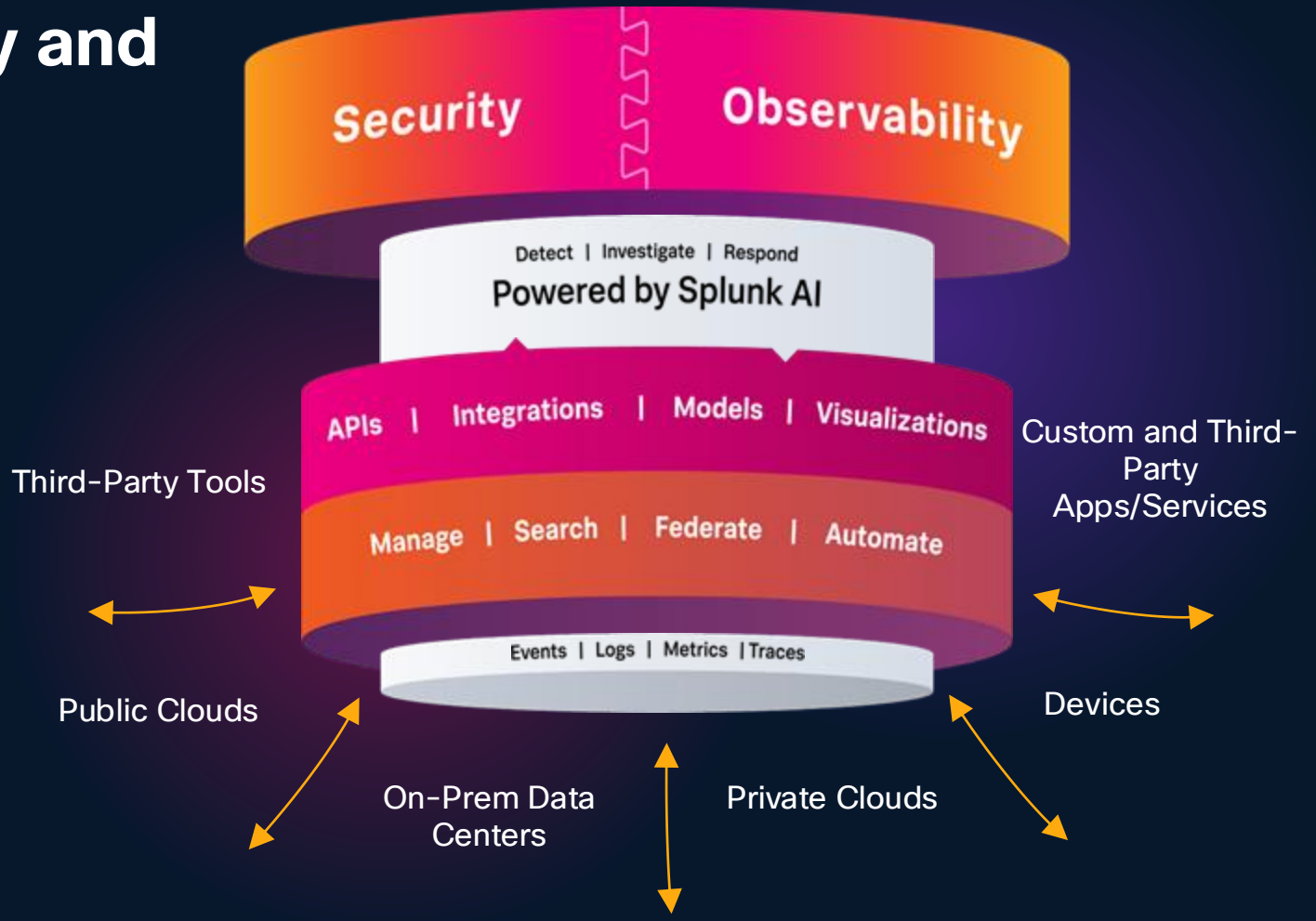
06 Splunk Premium Products

07 Splunk AI Assistant for Security

08 Splunk User and Entity Behavioral Analytics

cisco

Splunk: The Unified Security and Observability Platform



Most common Security Use Cases

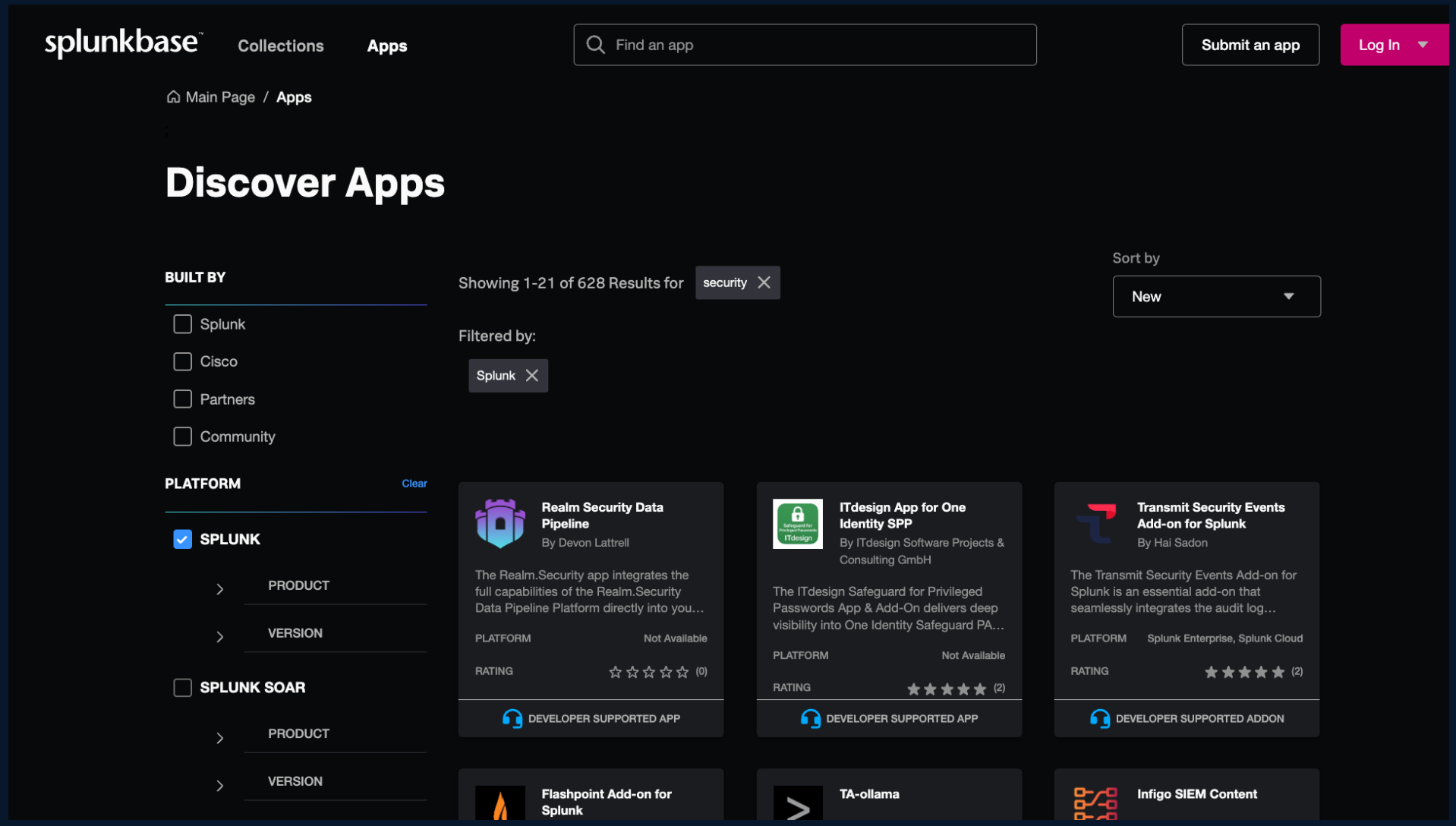
Threat Detection

Investigation

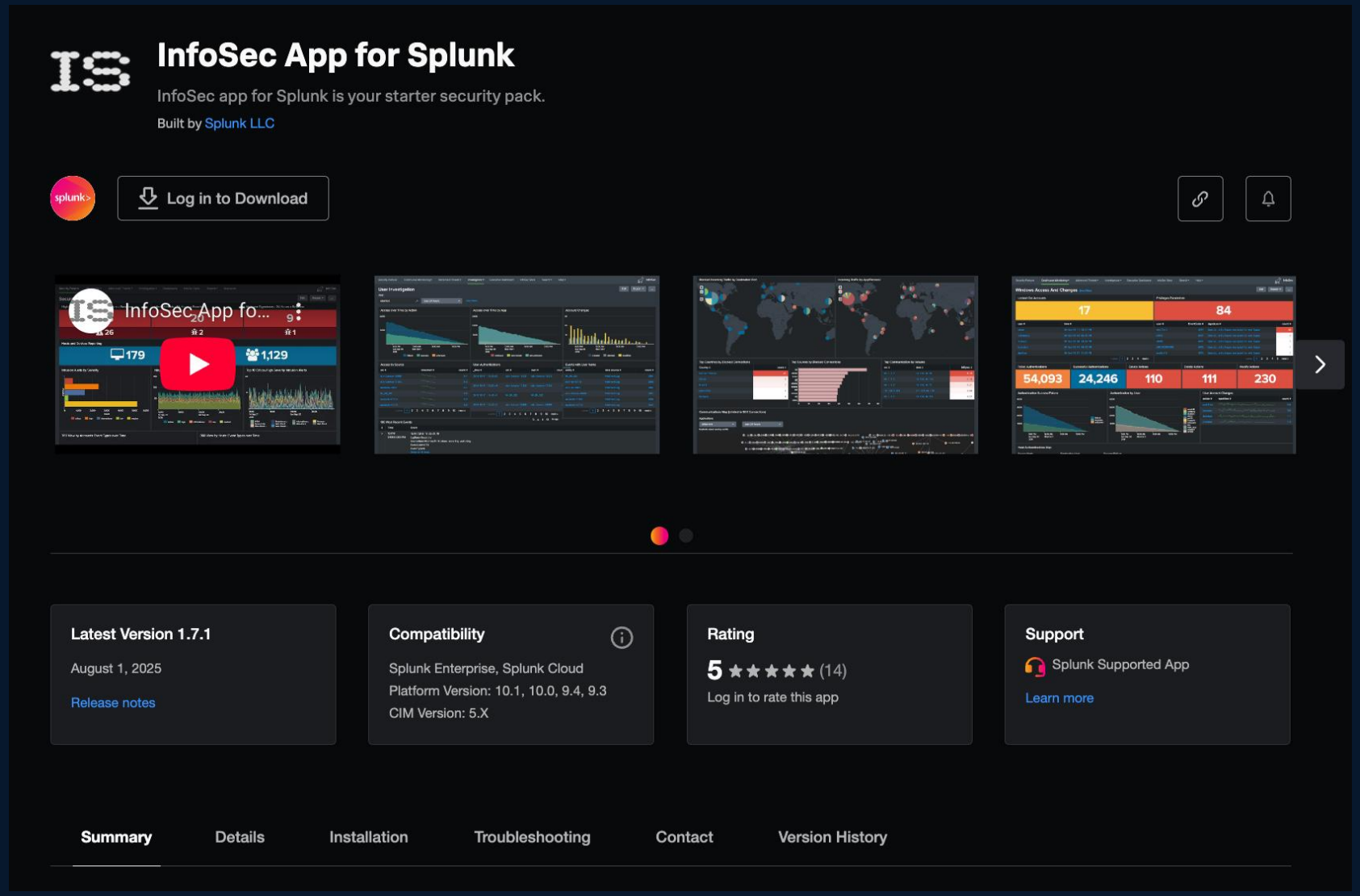
Response

Compliance

Splunkbase

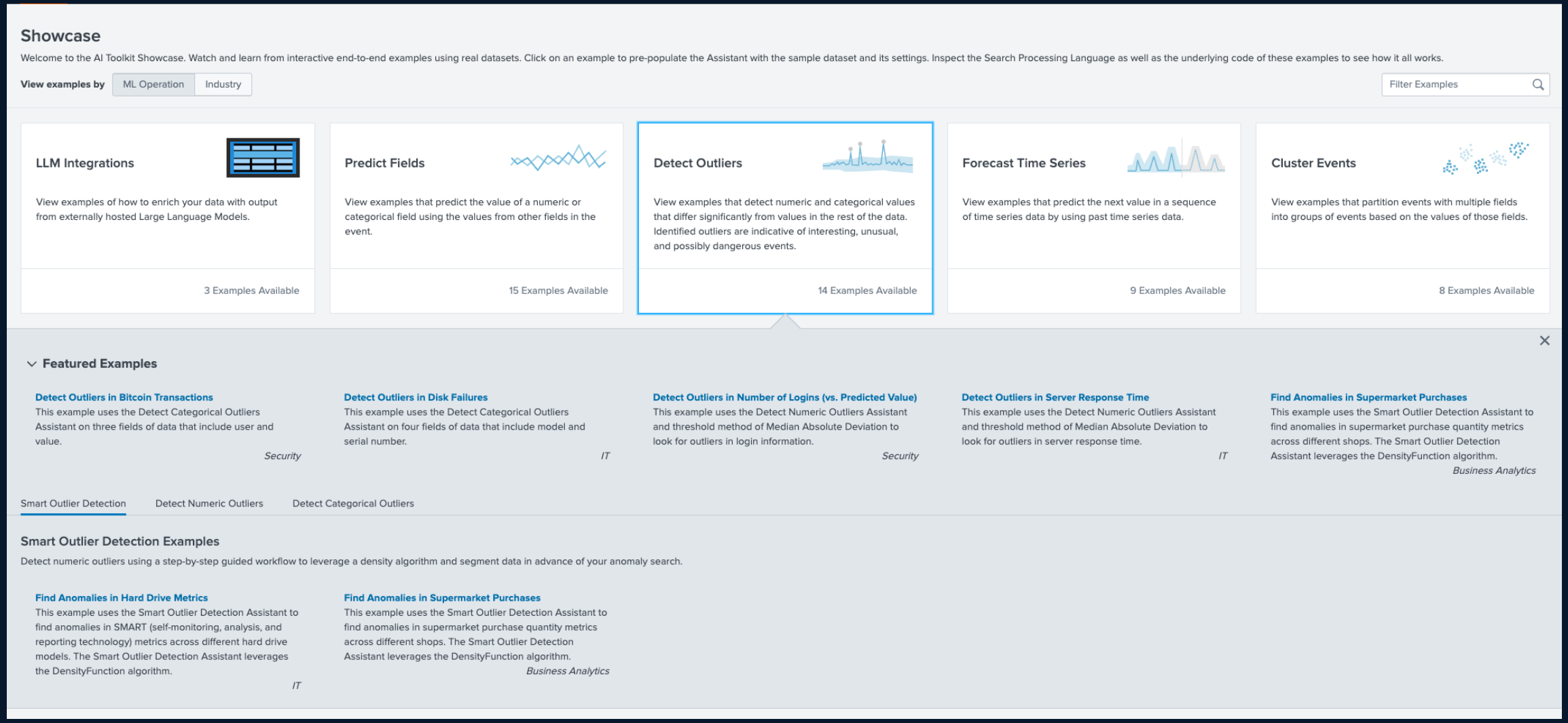


Splunk InfoSec App

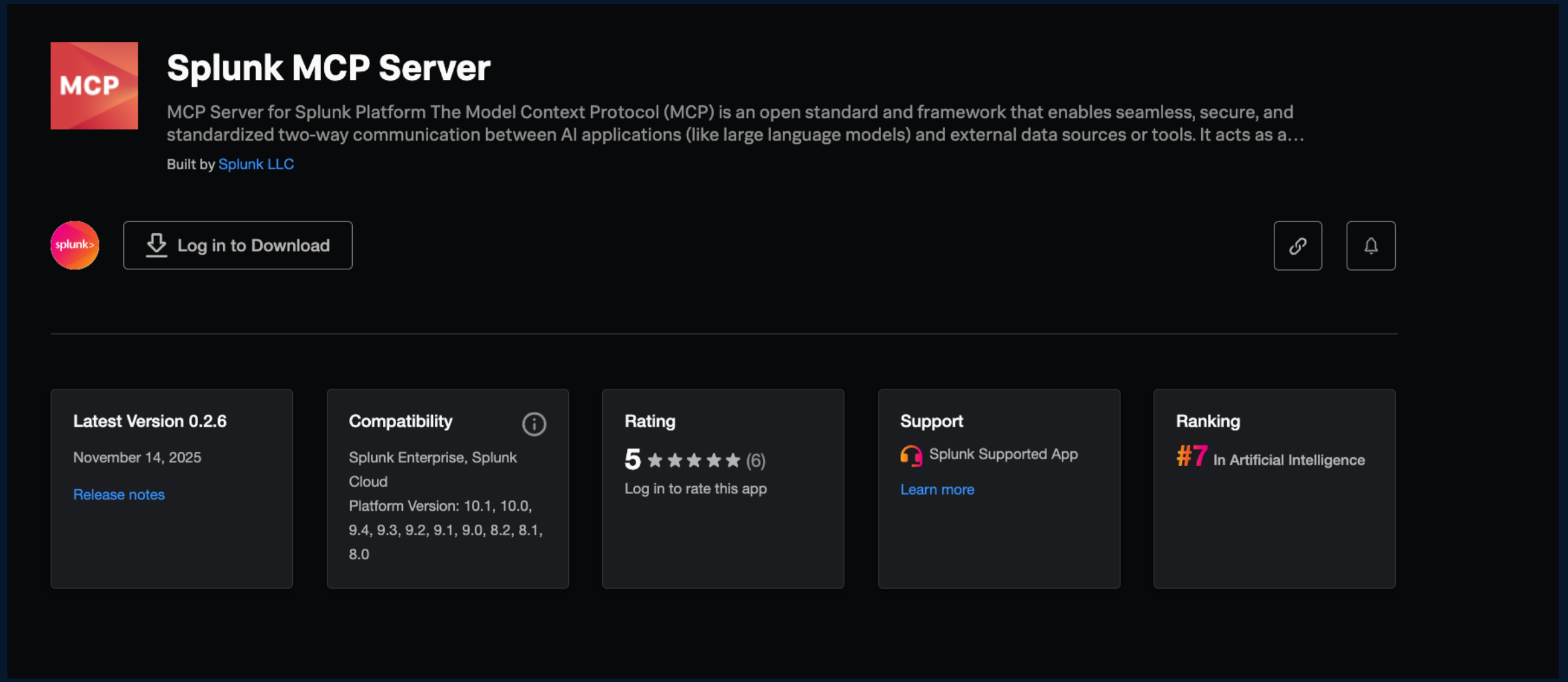


Splunk InfoSec App

Splunk AI Toolkit



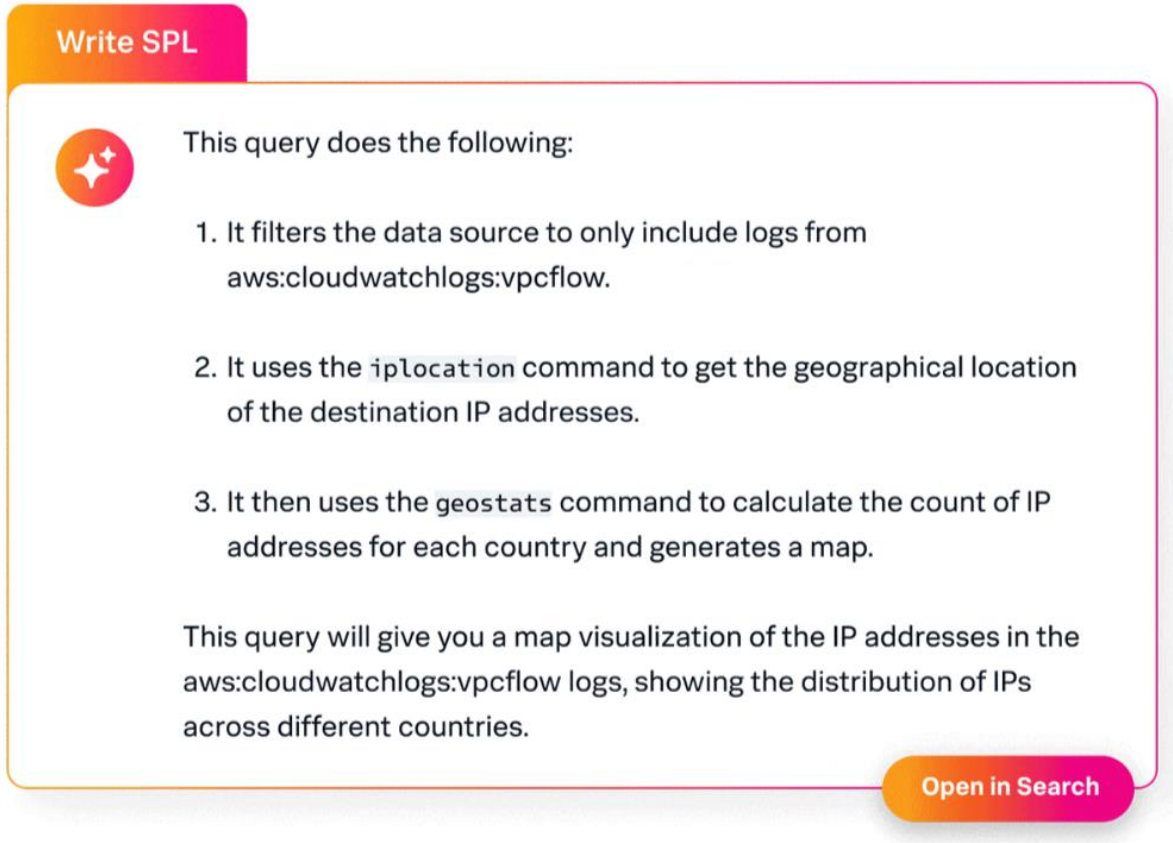
Splunk AI Toolkit



Splunk AI Assistant for SPL

Get your work done faster

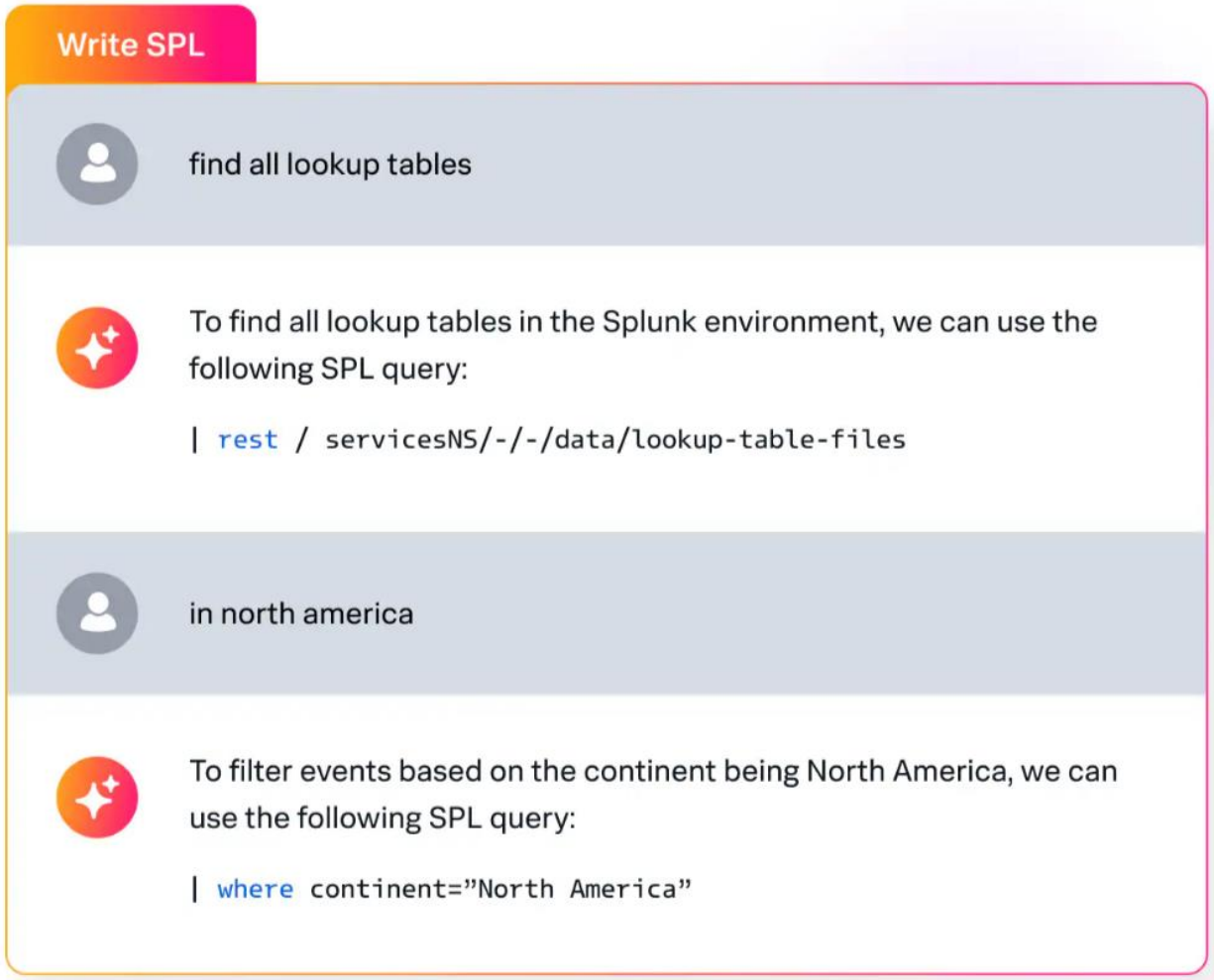
Need to create a new dashboard to troubleshoot an issue? Spend more time thinking about the problem than the technology. Use natural language to prompt Splunk AI Assistant to generate SPL and get you started quickly.



Splunk AI Assistant for SPL

Chat with your data

Analysis is an iterative process. Chat with the Splunk AI Assistant to generate SPL and drill down into your Splunk data for a deeper level of insights.



Splunk Security

Powering the SOC of the future with the leading TDIR solution

Traditional environments

Unified threat detection, investigation & response

Splunk Asset & Risk Intelligence	Splunk Attack Analyzer	Splunk SOAR	Splunk Enterprise Security
Continuous asset discovery	Automated threat analysis	Security automation	SIEM

Splunk Platform

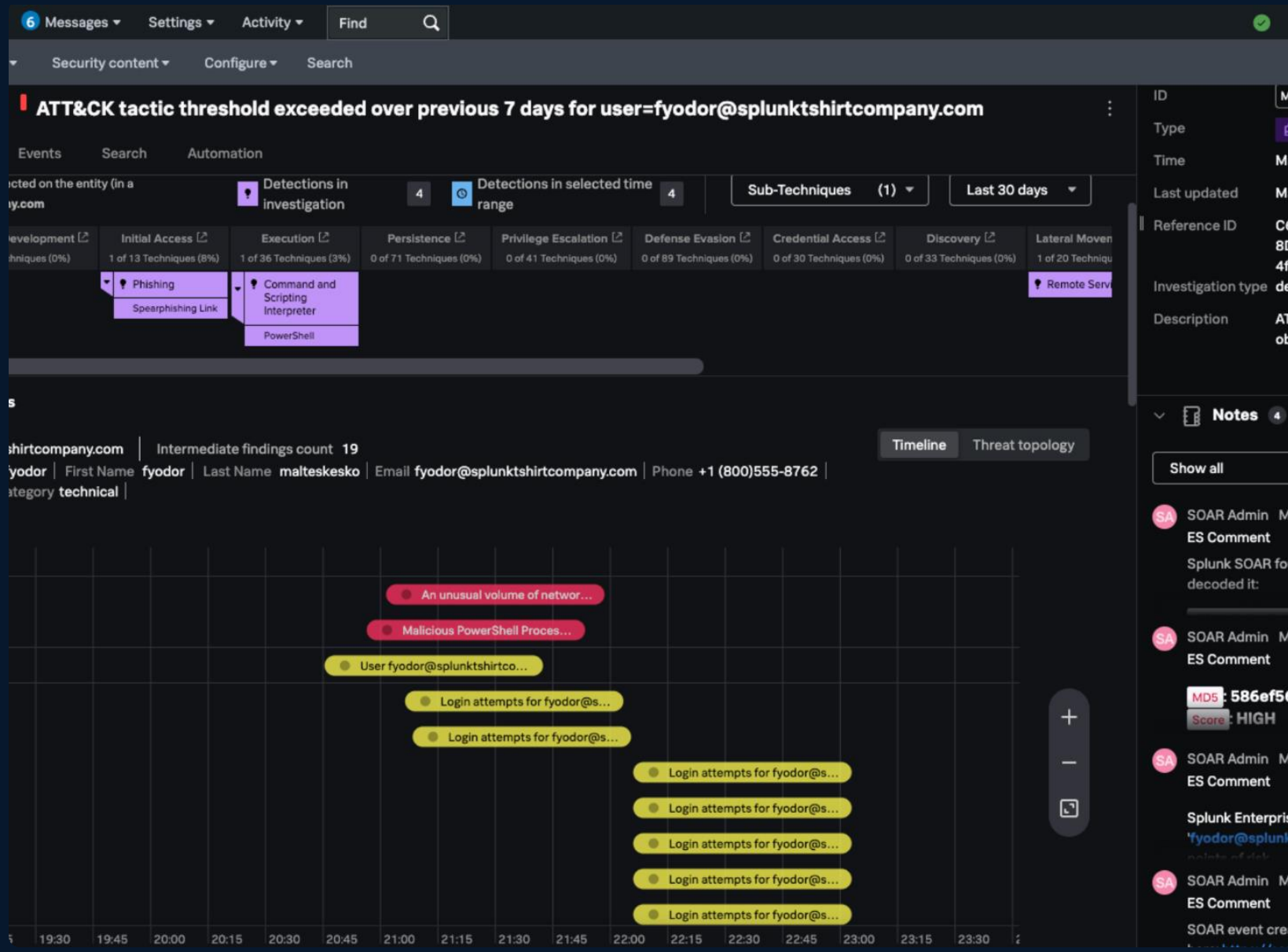
Cloud native environments

cisco

Splunk Enterprise Security

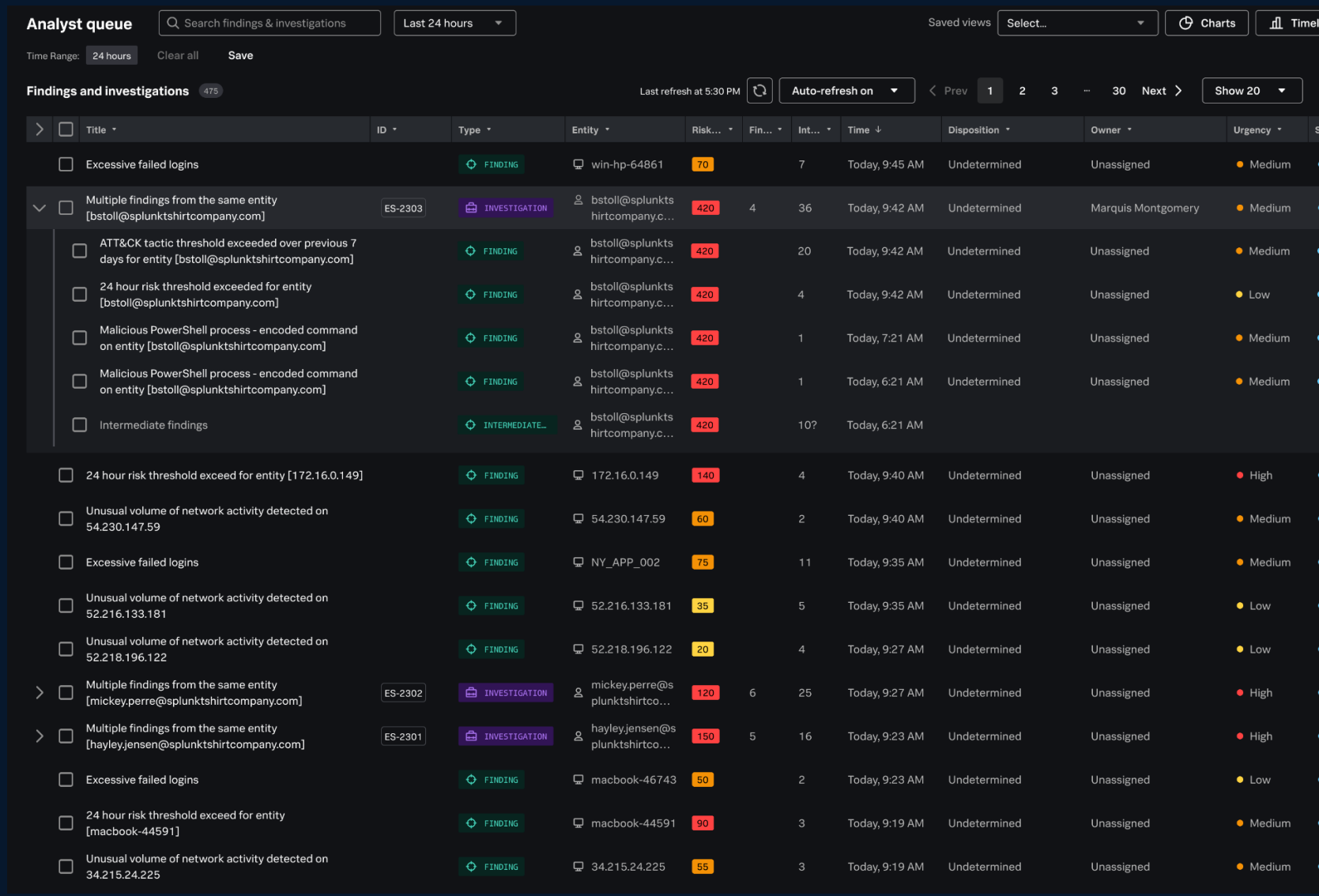
The AI Powered SecOps Platform

- **Unlock full-fidelity visibility** and control of your security data wherever it lives.
- **Deliver the best analyst experience** and tooling with unified TDIR.
- **Accelerate the SOC** with built-in AI and Agentics across every layer.



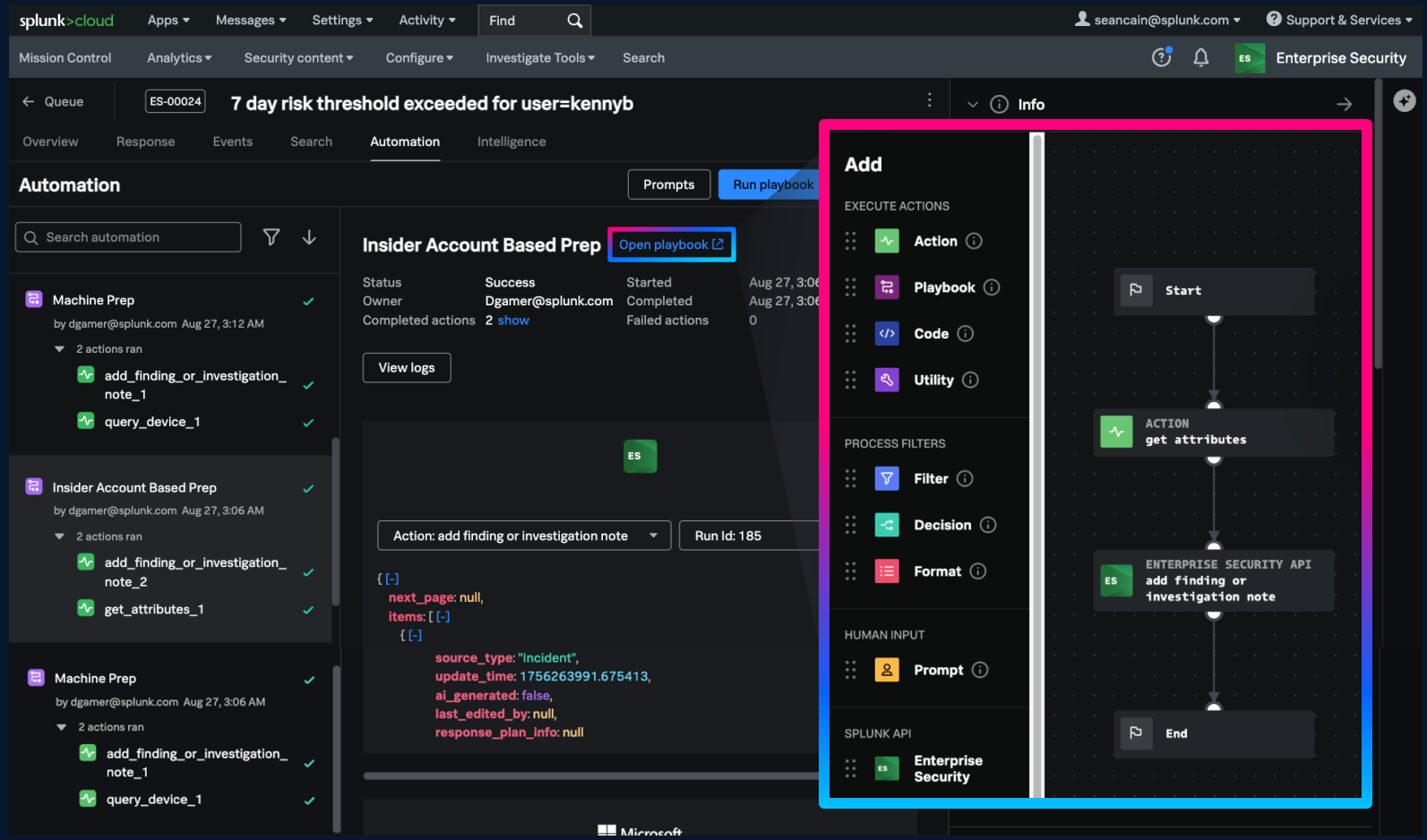
Splunk Enterprise Security

- Ingest, federate, and normalize **data from any source**, cloud, or OT for unified visibility.
- Optimize data routing, filtering, and storage to **control costs and maintain full access** for compliance and analysis.
- Enrich every alert **with integrated Cisco Talos and Splunk threat intelligence** for faster, more precise triage.
- Stay ahead with **world-class detections**—rule-based, AI-driven, and custom—continuously updated and mapped to MITRE ATT&CK.
- Deploy, test, and monitor detections faster with **Detection Studio***, enabling seamless coverage and quick gap closure.
- **Proactively address risk with RBA**, correlating weak signals, reducing false positives, and accelerating triage.



Deliver the Best Analyst Experience

- **Get integrated, end-to-end TDIR workflows** with native SIEM, SOAR, UEBA, and threat intelligence for faster value and a unified analyst experience.
- **Empower every analyst with embedded SOAR*** and case management to standardize playbooks, cut errors, and automate triage and response.
- **Detect and mitigate insider threats with UEBA***, which baselines activity and elevates risky behaviors for rapid, confident action.



Accelerate the SOC

Triage and Investigation

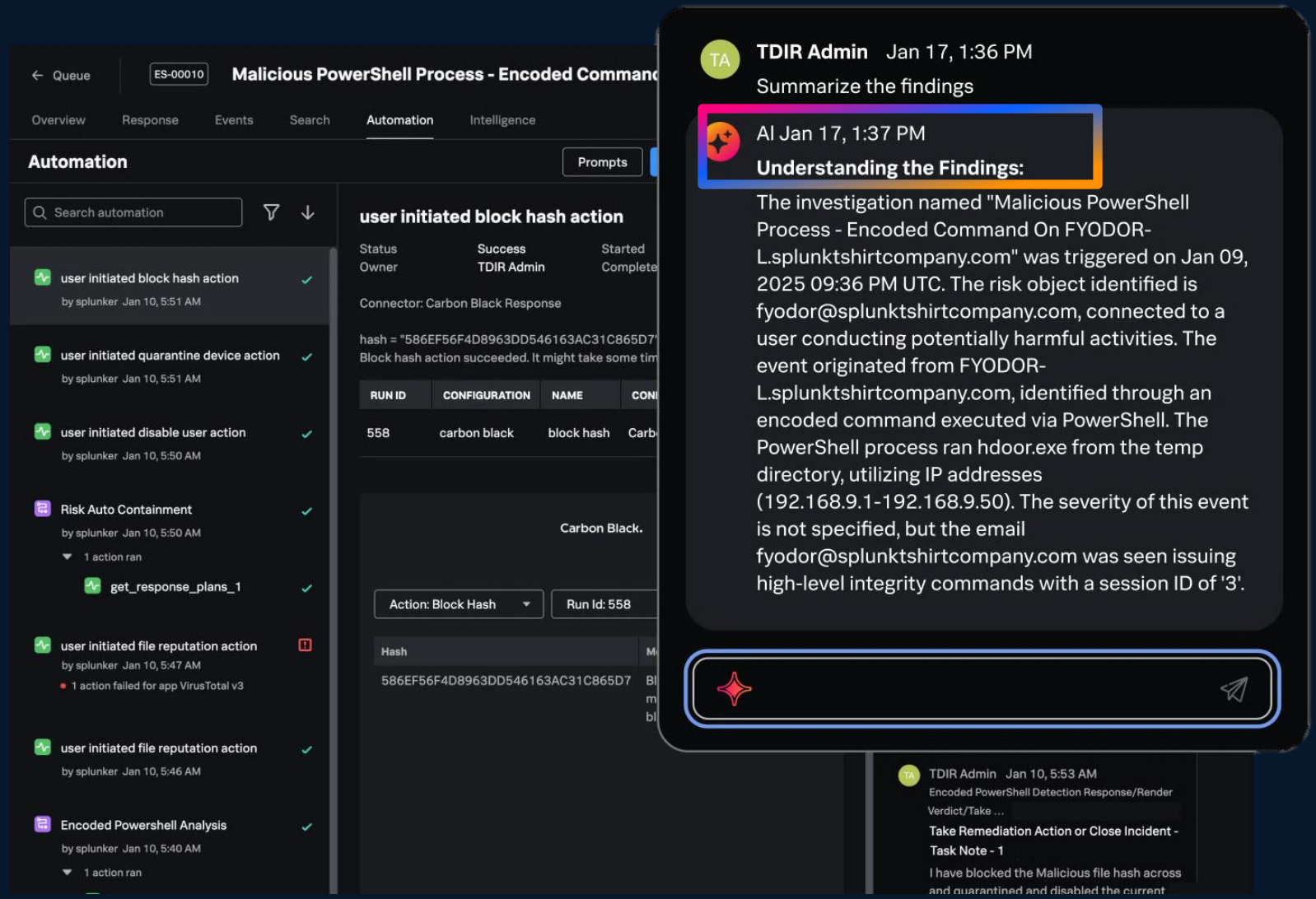
CA
- Use **AI Assistants*** to generate SPL queries, summarize findings, and provide investigation and remediation guidance from natural language.

Alpha
- Let **Triage Agents**** evaluate, prioritize, and explain alerts, reducing workload and highlighting critical issues.

Automation and Response

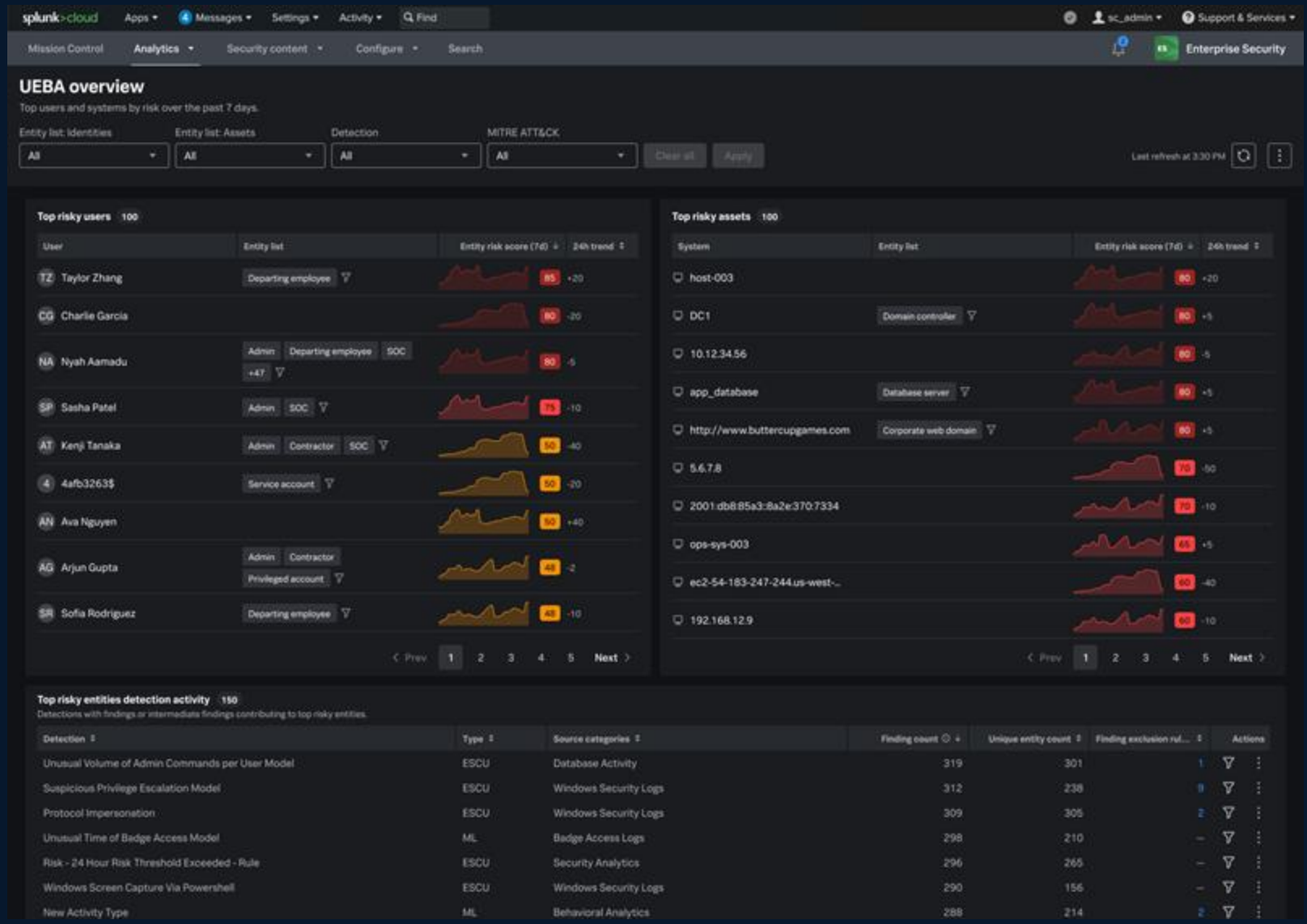
Alpha
- Accelerate automation with **AI Playbook Authoring**** that turns plain language into tested SOAR playbooks—no deep VPE expertise needed.

Alpha
- Rely on **Autonomous Response Agents**** to execute response actions in security tools based on set instructions.



Proactively detect and mitigate insider threats & advanced threats

- Establish user and entity behavior baselines to detect anomalies such as privilege abuse, lateral movement, and unauthorized access.
- Identify insider risks—including compromised accounts and data exfiltration—without relying solely on correlation rules.
- Unsupervised machine learning continuously adapts to evolving threats and insider attack tactics.



Any questions?