Redefine digital resiliency with Cisco Data Fabric and Splunk Agentic SOC

Lawrence Chiang 蔣佳賓 北亞區資深售前技術總監
Sr. Leader, Solutions Engineer, Greater China
Splunk, a Cisco Company

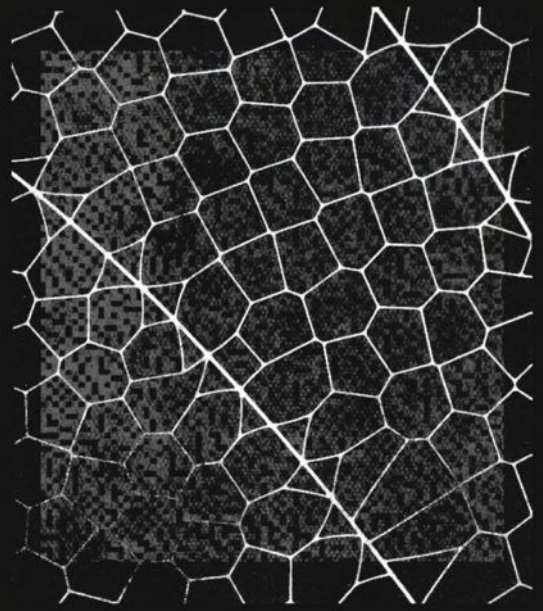
Jun Ling 凌軍 製造業首席架構師
Sr Solutions Engineer, Greater China
Cisco

July 15, 2026

ANTHROP\C

Project Glasswing

Securing critical software for the AI era



AI-Driven Vulnerability Management

Frontier AI models are creating an entirely new level of risk for every organization

> It lowers the threshold for attackers, empowering less-skilled actors to launch complex, high-impact campaigns.

Anthony Grieco
SVP and Chief Security & Trust Officer
Cisco

- More sophisticated attackers
- More personalized attacks
- More places to attack

Source: Cisco Blog, “Rising to the Era of AI-Powered Cyber Defense, ” Anthony Grieco, April 7, 2026

And we all have significantly less time to respond

THE AVERAGE TIME TO EXPLOIT VULNERABILITIES

2018
2.3 years

2023
4.2 months

2025
21.5 days

2026
38 hours

Source: zerodayclock.com, May 28, 2026

Splunk is the intelligence layer that powers agentic operations

Predict and prevent at machine speed

Unlock cross-domain insights at massive scale

Build trust in AI with end-to-end visibility

Strategical Team-up in AI era

Acquisition

splunk> a CISCO company

Armorblox now part of CISCO

MindMeld

babblelabs

PERSPICA

voicea

ACCOMPANY

Galileo

WideField

Investment

ROBUST INTELLIGENCE

DataRobot

cogniac

moogsoft Continuous Assurance

securiti

habana

scale

dremio

MISTRAL AI_

uniphore

cohere

Paxata

$1 Billion Investment Fund
AI Infrastructure and AI Software

Strategic Partnership

NVIDIA

AMD

intel

aws

Microsoft

AI Partner Certifications & Training for Channel Partners

Digital Resilince powered by Splunk AI Innovations

01 Agentic Capabilities

02 Cisco Data Fabric and Cisco Cloud Control

03 Agentic SOC

04 Observability for AI Agent (Galileo)

01 Agentic Capabilities

- AI Assistant 2.0
- Splunk AI Toolkit Agent Builder
- Demo Video

Compose AI inside Splunk – and outside it

Same person. Same data. Two ways.

INSIDE SPLUNK

Compose AI in the Splunk platform

AITK is the low/no-code AI workbench. Raj uses the AITK Agent Builder to wire AI into the place where the data already lives.

- AITK Agent Builder
- Splunk-native execution

OUTSIDE SPLUNK

Compose AI through your existing tools

The Splunk MCP Server exposes Splunk's data, search, and Skills to any agent client. Raj wires n8n to Splunk + Confluence + Jira and runs the workflow from where his business already lives.

- Splunk MCP Server
- AI Skills library (12 specialized)
- n8n, Continue, Claude Desktop, Atlassian MCPs

Splunk SRE uses both. The audience does too.

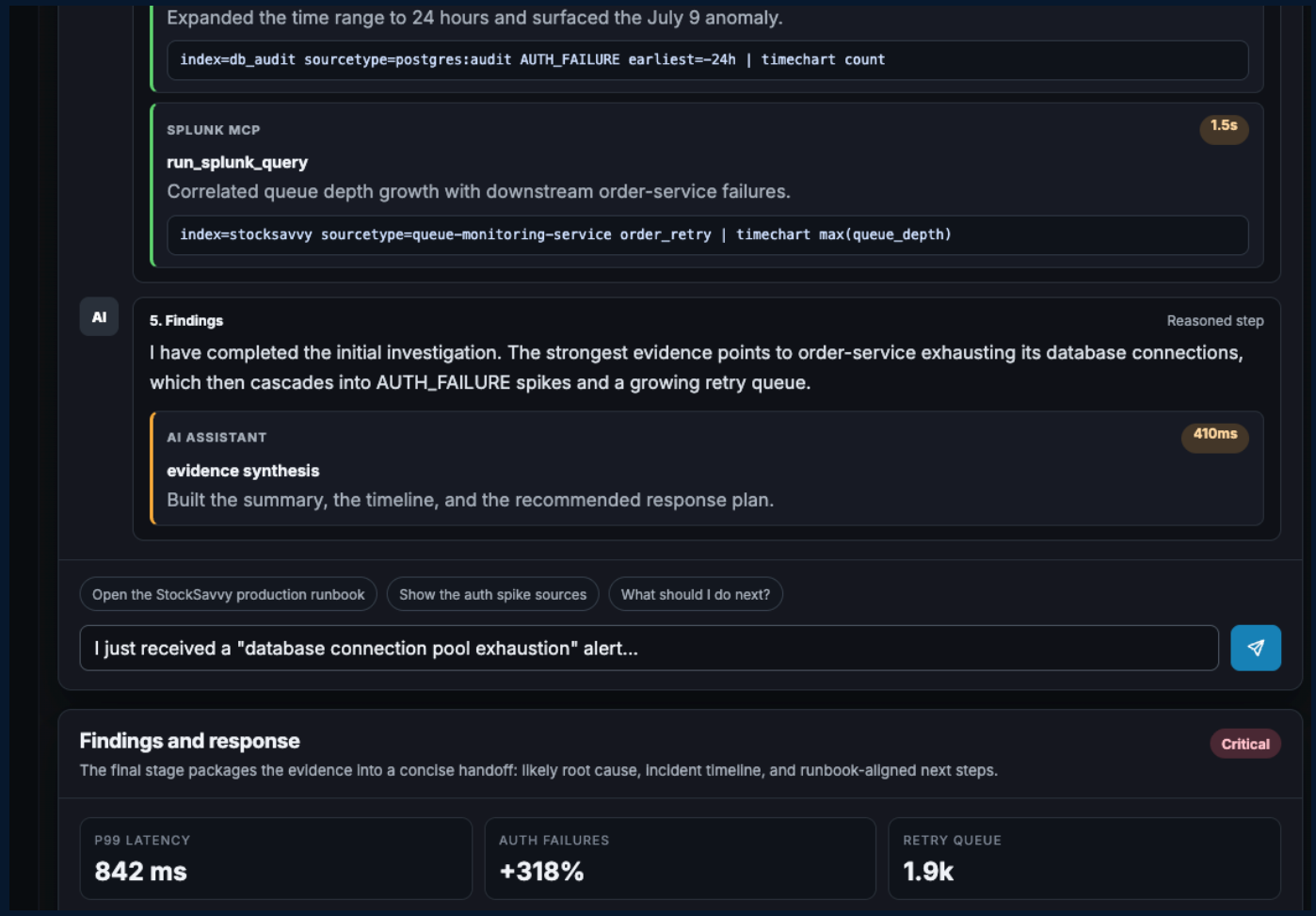
GA

Splunk MCP Server

Connect Splunk directly with your AI and agentic systems

- Integrate foundational Splunk Platform abilities including data discovery & search
- Access Splunk's tailored AI capabilities like SPL generation, optimization, and explanation
- Activate LLMs with your existing Splunk RBAC capabilities across all your users

MCP Client can be any LLM application.



02 Cisco Data Fabric and Cisco Cloud Control

- Cisco Data Fabric
- Machine Data Lake
- Cisco Cloud Control
- Demo Video

Agentic AI Era Demands New Data Strategy

Introducing

Cisco Data Fabric

A revolutionary new architecture, powered by Splunk,
to harness the value of machine data with AI

Cisco Data Fabric powered by Splunk

Workloads

Security | Observability | Network Ops | Custom Applications

Cisco Data Fabric

AI-powered data management

Federated Search and Analytics

AI-Native Experiences and Platform for AI

Machine Data Lake

Sources

Infrastructure | Applications | Security | Users & Devices

Cisco Cloud Control /C3

One platform. Every domain. The foundation everything else is built on.

The foundation everything is built on.

Meraki · ThousandEyes · Security Cloud Control · Splunk · Nexus Dashboard · Catalyst SD-WAN · Intersight · Webex · IQ · & more

Cisco Cloud Control

Cisco products

- Meraki
- Intersight
- Splunk
- ThousandEyes
- Catalyst SD-WAN
- IQ
- Catalyst Center
- Nexus Dashboard
- Security
- Nexus Hyperfabric
- Collaboration Control Hub

AgenticOps

AI Canvas
Collaborative agentic workspace

AI Assistant
Conversational entry point

Platform services

- Identity
- Inventory
- Topology
- Alerts & Notifications
- Licensing

Customize & extend

Marketplace | Agent Builder | App Builder

Cisco Data Fabric – Powered by Splunk

Our competitive advantage

Powering Cisco Cloud Control & AI Canvas

The Cisco Data Fabric & Splunk will become the engine that enables all AI analysis and insights.

- **Cisco AI Canvas**
- Meraki
- ThousandEyes
- Catalyst
- SD-WAN
- ISE
- **All Cisco Products**
- **Third-party integrations**

Cisco Cloud Control

AI Agentic Operations

the foundation

Cisco Data Fabric

powered by Splunk

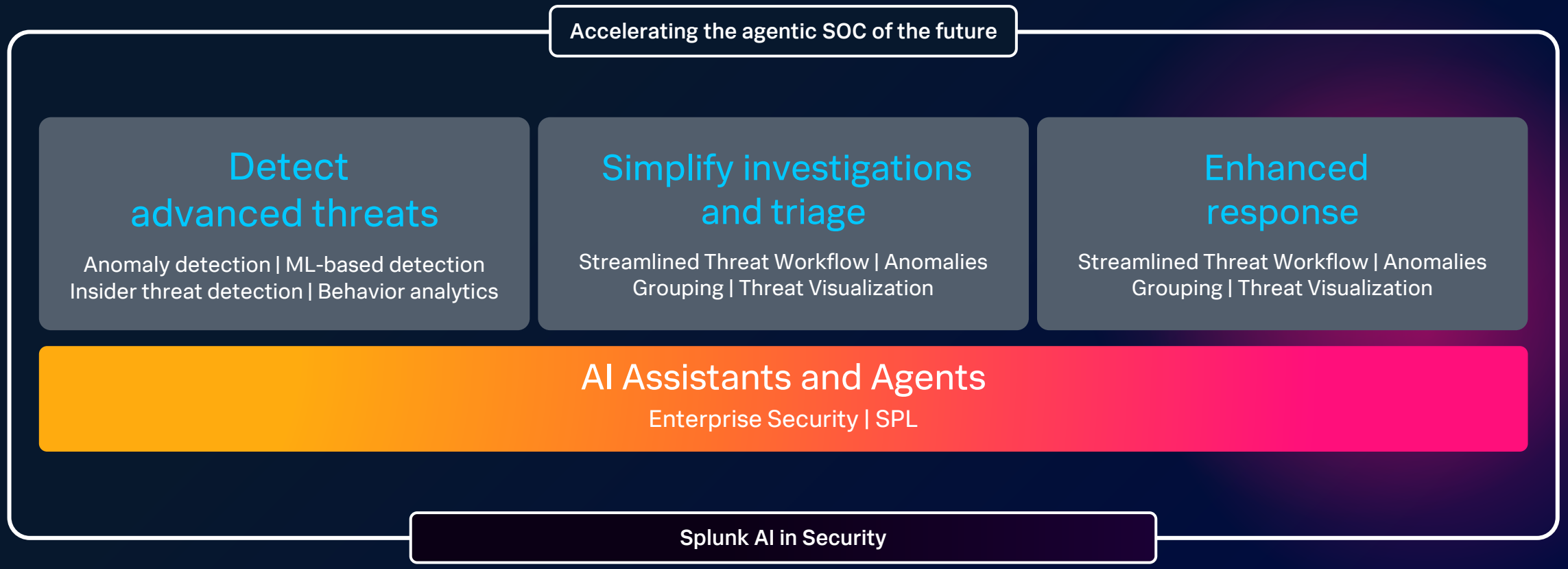
Cisco data sources

3rd-party data sources

03 Agentic SOC

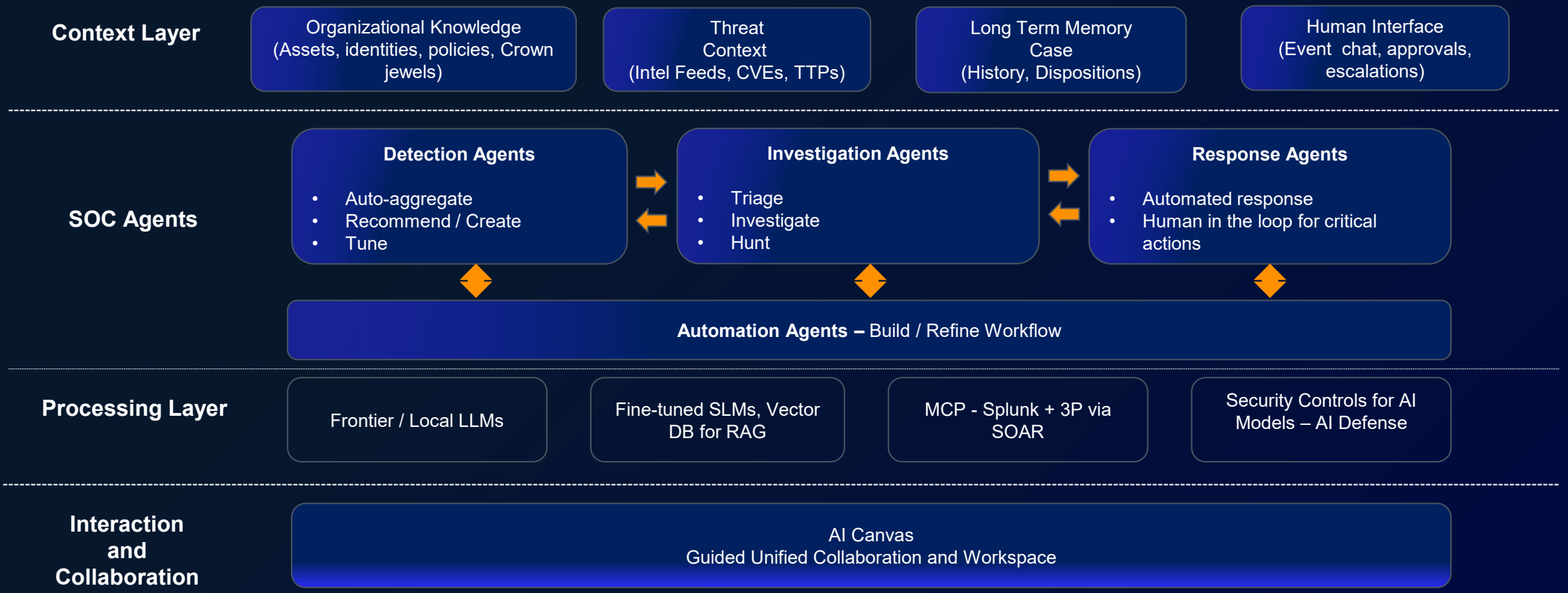
- Splunk ES update
- Streamlined SOC operations
- Specialized agents: Triage, Automation Builder, Malware Threat
- Demo Video

Driving a new wave of SOC maturity with Splunk AI in Security



For more content on Splunk AI in Security capabilities, please reference the Splunk Enterprise Security first call deck

Agentic SOC Architecture

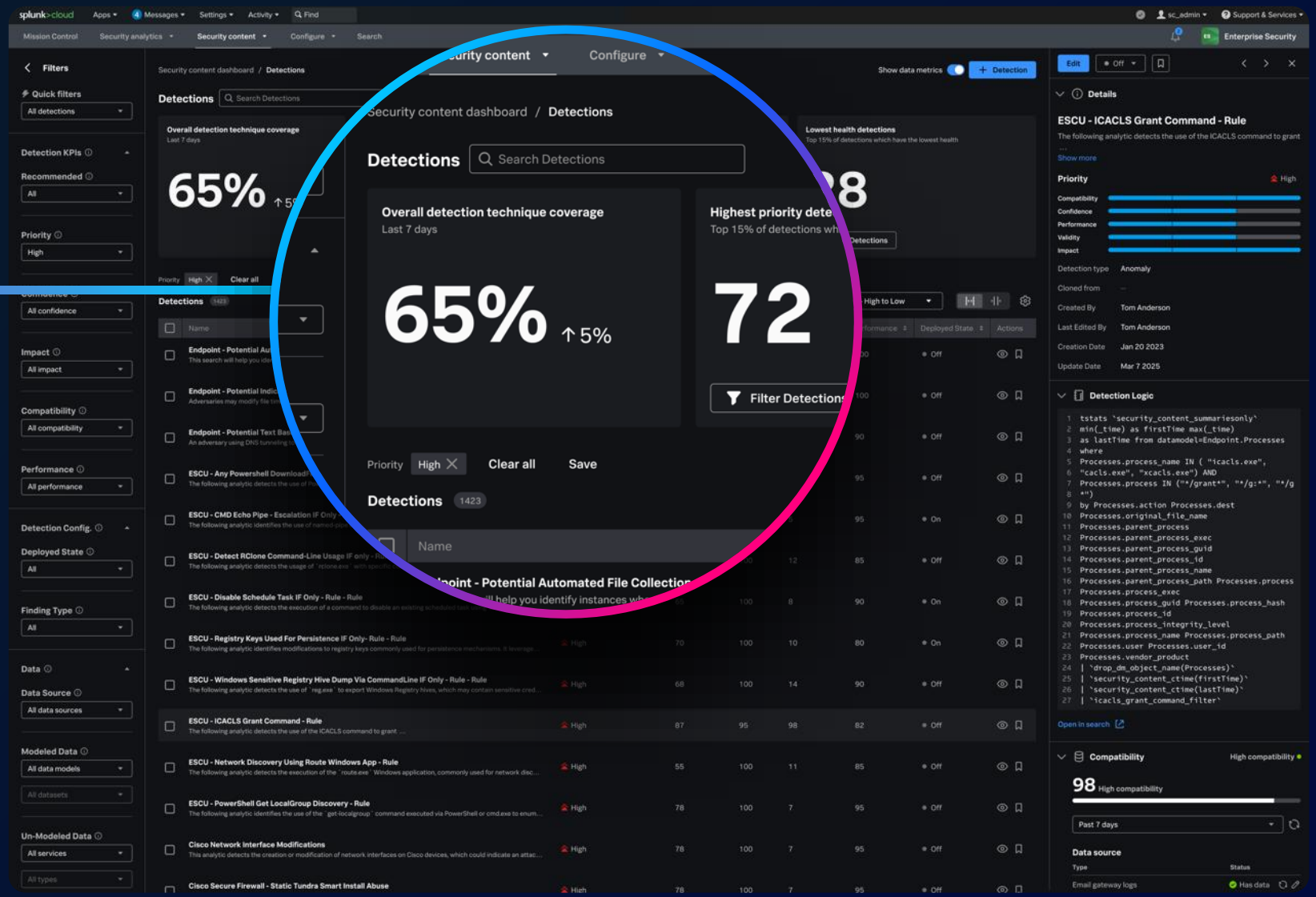


General Availability

Detection Studio

Powered by SnapAttack

- Streamline detection creation workflows
- Evaluate detection health
- Expand versioning and detection-as-code



04 Observability for AI Agent (Galileo)

We stand on the brink of an AI-driven transformation

Enterprises are building agentic teammates that can act and get work done on our behalf

>60%

have active agentic pilots today

1.3 billion

agents expected to be in operation by 2028

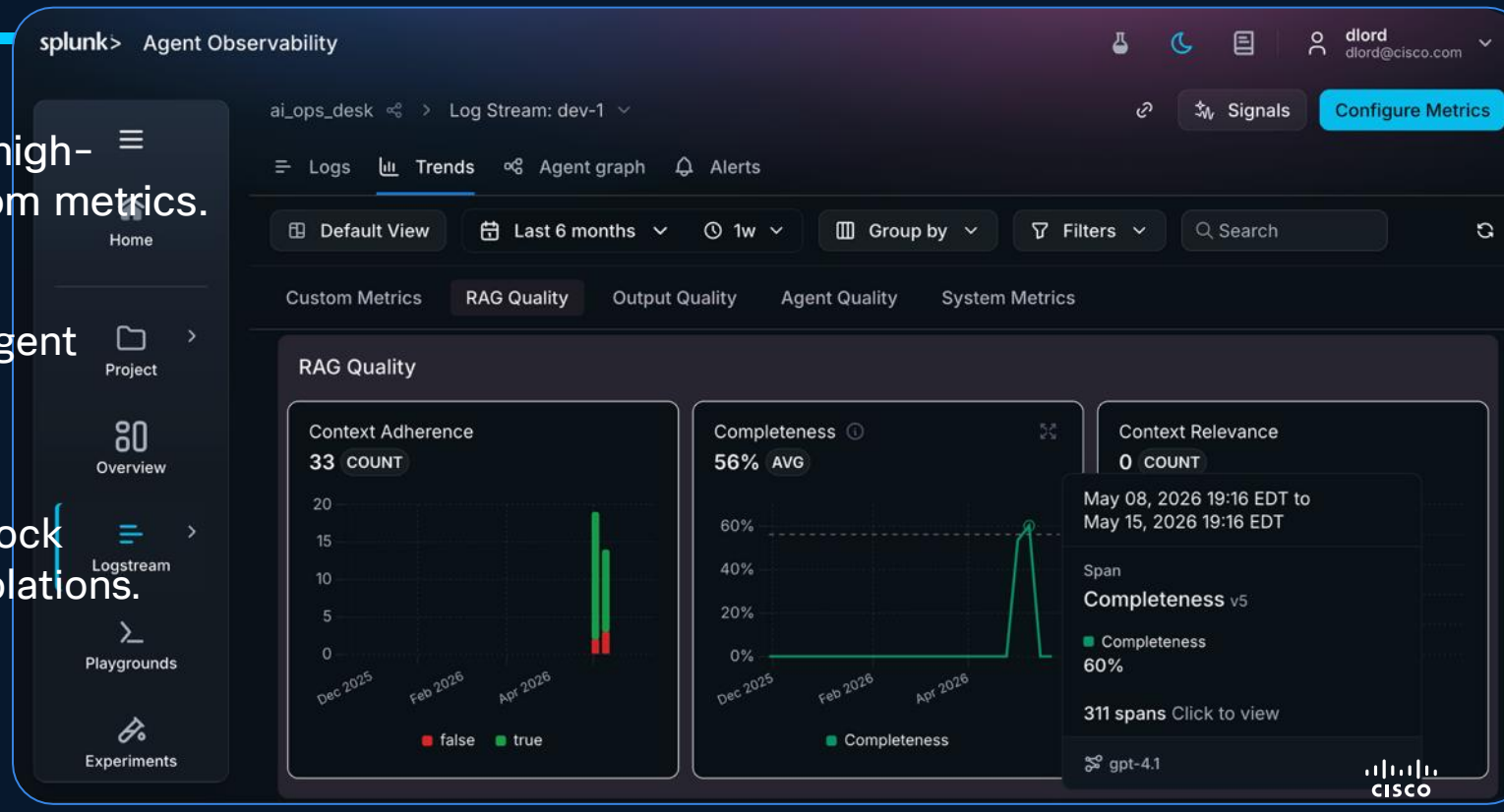
© 2026 Cisco and/or its affiliates. All rights reserved.

NEW

Splunk Agent Observability

Powered by Galileo - Observability for the agent lifecycle, from development through production

- **Accurate Evaluations**
- Evaluate agent, output, and RAG quality with high-accuracy evals and out-of-the-box and custom metrics.
- **Instant Visibility**
- See the root cause of errors in complex multi-agent workflows.
- **Runtime Guardrails**
- Leverage Luna SLMs for real-time guardrails. Block hallucinations, prompt injections, and safety violations.



Cisco + Splunk = Complete Digital Resilience

Platform Resilience

- Unified insights across the enterprise with data at massive scale

Preemptive Security

- Mitigate threats with agentic real-time threat monitoring
- Investigate and remediate threats faster with AI-powered automation

End-to-End Observability

- Observe AI with full stack, silicon to agent monitoring
- End-to-end network, application, and infrastructure monitoring

CISCO Connect

Thank you