CISCO Connect

Unleashing the Agentic SOC with Splunk



Leonard Wall
Field CISO, Cisco

September 30, 2026

Forward-looking statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.
For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to Cisco's periodic reports its other filings with the SEC, including the risk factors identified in Cisco's most recent quarterly report on Form 10-Q and annual report on Form 10-K, copies of which may be obtained by visiting the Cisco Investor Relations website at investor.cisco.com or the SEC's website at www.sec.gov. Any projections in this presentation are based on information currently available to Cisco, which is subject to change. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines or our general product direction is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in alpha or beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Copyright © 2026 Cisco and/or its affiliates. All rights reserved. Cisco, Splunk and the Cisco and Splunk logos are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to: www.cisco.com/go/trademarks. Third-party trademarks mentioned in this presentation 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.

© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Introduction

02 SOC Challenges

03 New Operating Model

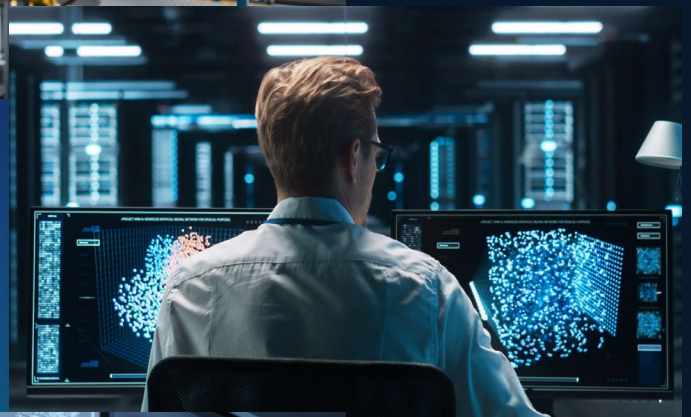
04 Delivering the Agentic SOC

05 Splunk Enterprise Security

06 Pioneering the Future

© 2025 Cisco and/or its affiliates. All rights reserved.







Security from the Agentic Frontier

The AI Transformation is here and we must transform for it

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Unrelenting Pressure on SOC Teams



Gaps in coverage

Staggering data growth, workload complexity, and costs are compounding risk



Fragmented, manual tooling

Siloed solutions, manual and reactive capabilities wear on team effectiveness



Overwhelming attack surge

Attacks, increasingly AI-fueled, are increasing in velocity, frequency and sophistication

The result: a record 50%+ of security leaders[1] and practitioners likely plan to quit their role in the next 12 months[2].

© 2025 Cisco and/or its affiliates. All rights reserved.



The way forward

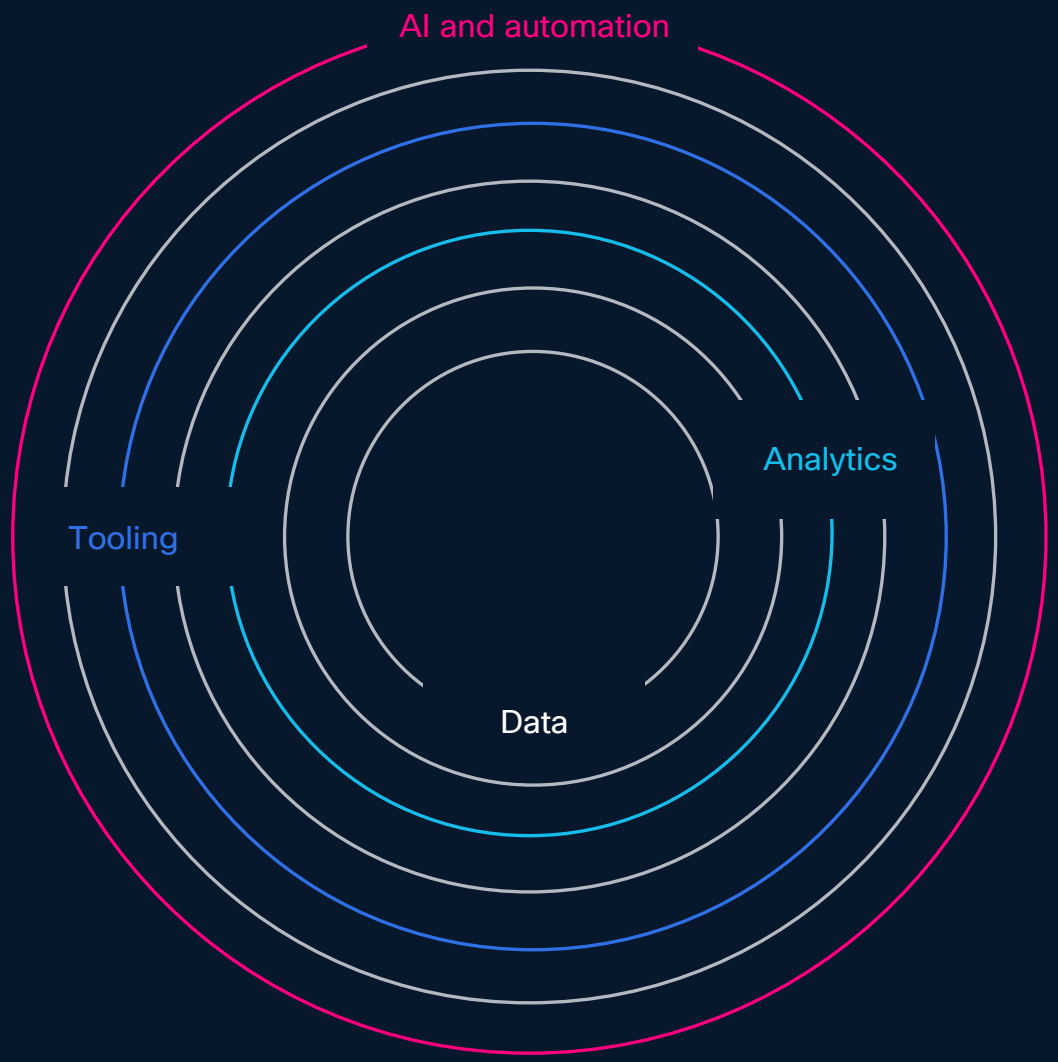
A New Operating Model

An integrated system bringing together Data, Analytics, Tooling, and AI for a powerful analyst experience.

© 2025 Cisco and/or its affiliates. All rights reserved.

Agentic SOC

- Complete visibility
- Contextual understanding
- Intuitive analyst experience
- Machine speed & scale



A Foundation of High-Fidelity Data

Data fabric
Data management
Data pipelines

Analyzed at Machine Speed

TI enrichment & context
Correlated detections
Investigation & hunting

With Intuitive SOC Tooling

Single work surface for TDIR
Team coordination
Integrated workflows

And Human-led AI & Automation

Customizable agents
Reasons and acts decisively
Prevents emerging threats

© 2025 Cisco and/or its affiliates. All rights reserved.

Why Splunk



Scale Operations

by turning high-volume data into high-fidelity visibility



Streamline detection and response

To focus on what matters



Stop threats at machine speed

With AI and automation

All to power the Agentic SOC

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

AI native data fabric for full-stack security



CROSS DOMAIN VISIBILTY

Understand the entire attack surface

AGENTIC OPS

Drive context aware action from correlated insights

AI MODELS

Unlock machine data for training and inference

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

cisco

Leverage the Fabric for secure AI

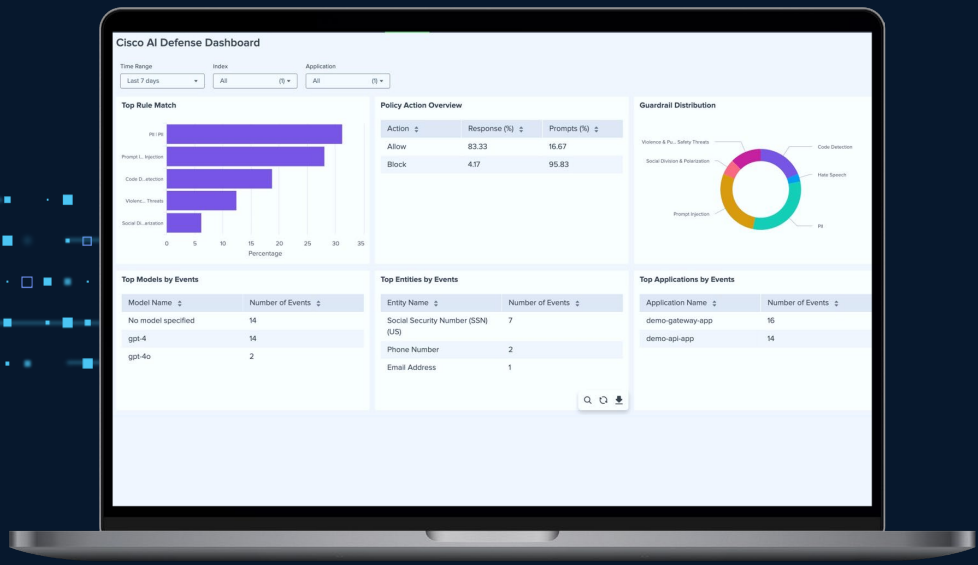
Unparalleled visibility across every AI layer

AI models, agents, and applications

AI workloads and infrastructure

CISCO DATA FABRIC

Splunk brings together disparate sources and tools for unified protection



Discover AI assets – known and unknown - in your environment

High fidelity detection across every layer of AI infrastructure

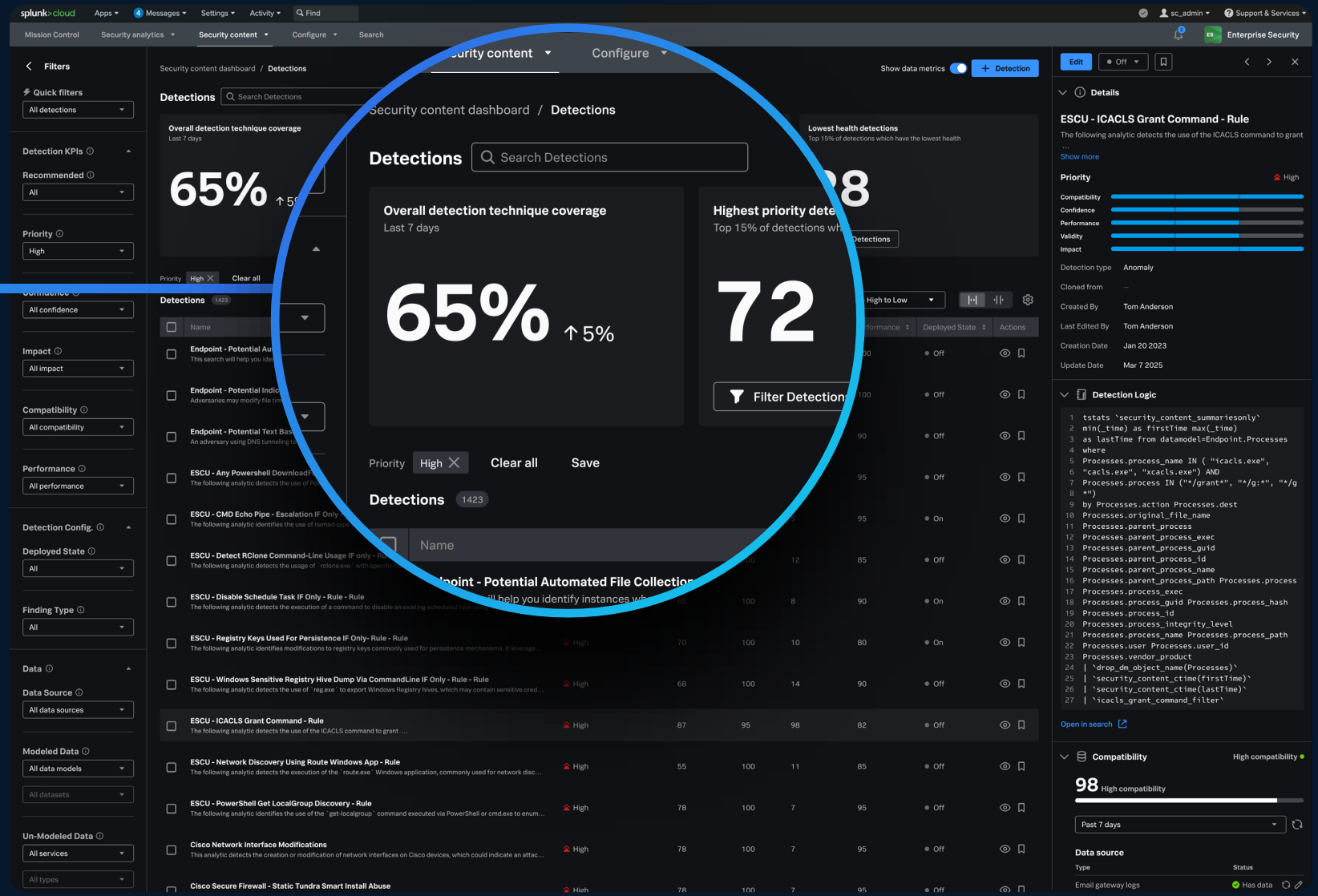
Block emergent attacks at any level

© 2025 Cisco and/or its affiliates. All rights reserved.

General Availability for Cloud

Detection Studio

Tune and author detections

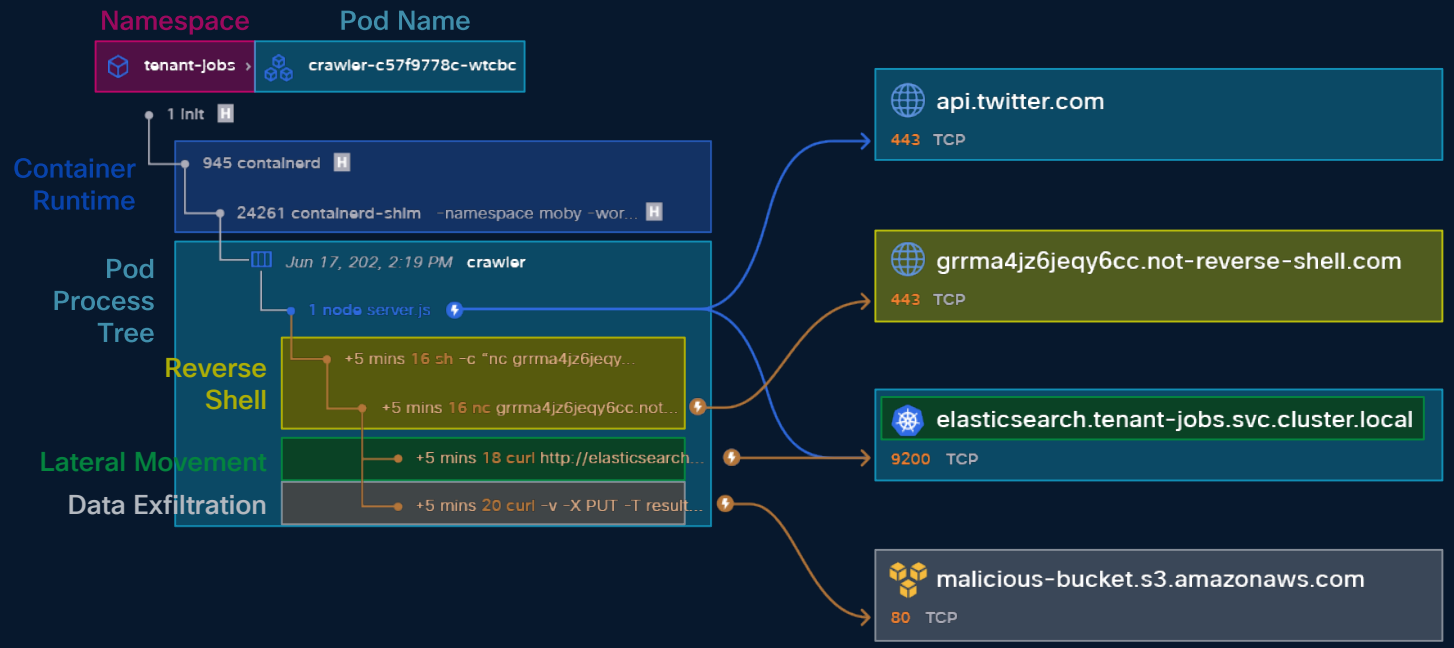


- Streamline detection creation workflows
- Evaluate detection health
- Expand versioning and detection-as-code

© 2025 Cisco and/or its affiliates. All rights reserved.

Deliver high-fidelity runtime security across cloud workloads

- Kernel Monitoring: Suspicious process detected on workload
- Splunk correlates findings and to identify lateral movement to an s3 bucket with highly sensitive data
- Guard Duty: Command and Control traffic detected
- Analyst triggers playbook to contain and remove the threat



© 2025 Cisco and/or its affiliates. All rights reserved.

Exposure Analytics



Autonomous Entity Discovery



Entity-aware Investigations



Risk based prioritization



Asset Threat Profile:

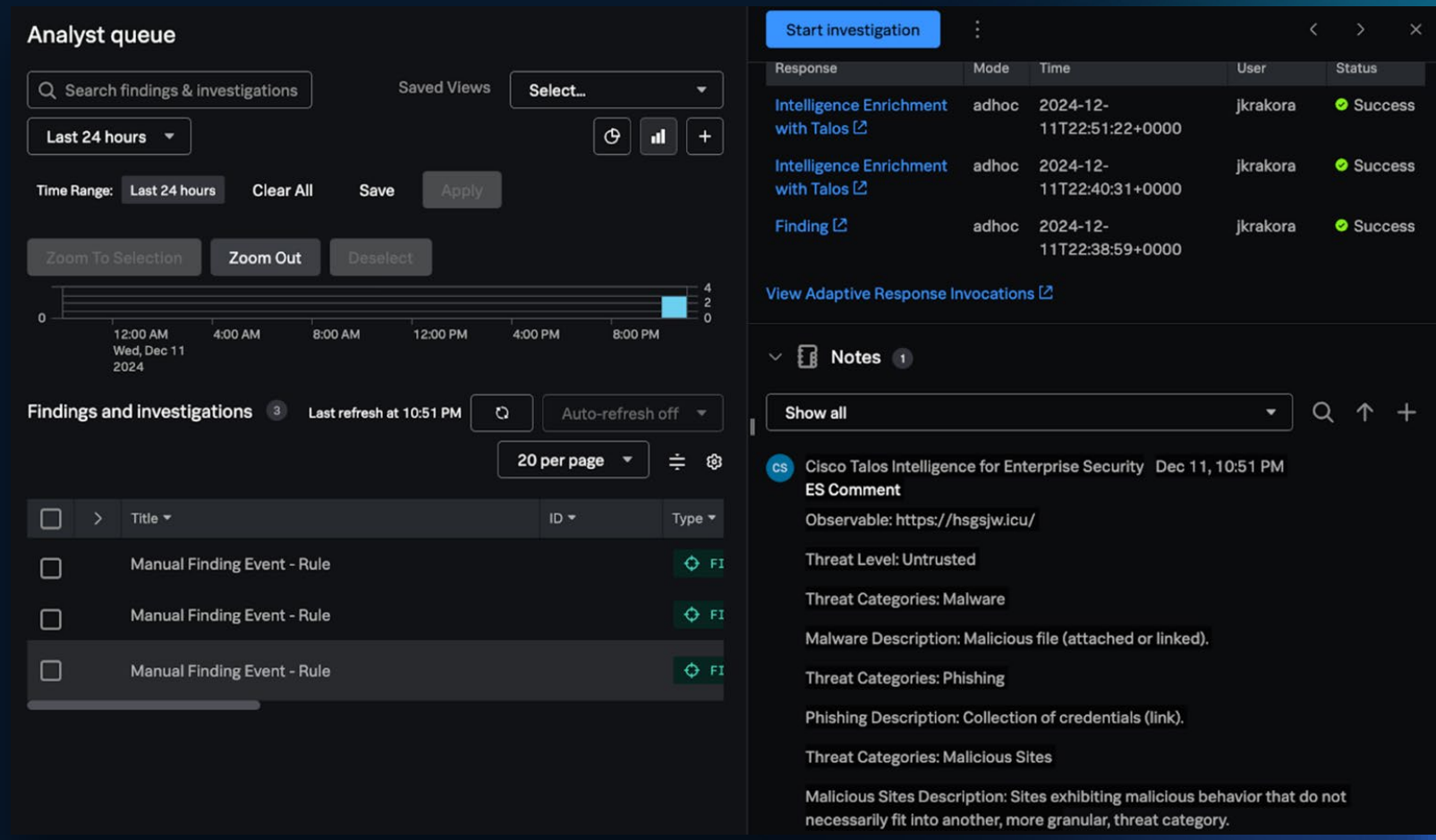
- Anomaly: Excessive Data Transfer Detected
- Process Event: Known Malicious tool execution detected
- Connection: Later Movement attempted
- Access Violation: Multiple unauthorized file reads
- Persistence: Unauthorized cron-job created

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Cisco Talos Intelligence for Enterprise Security

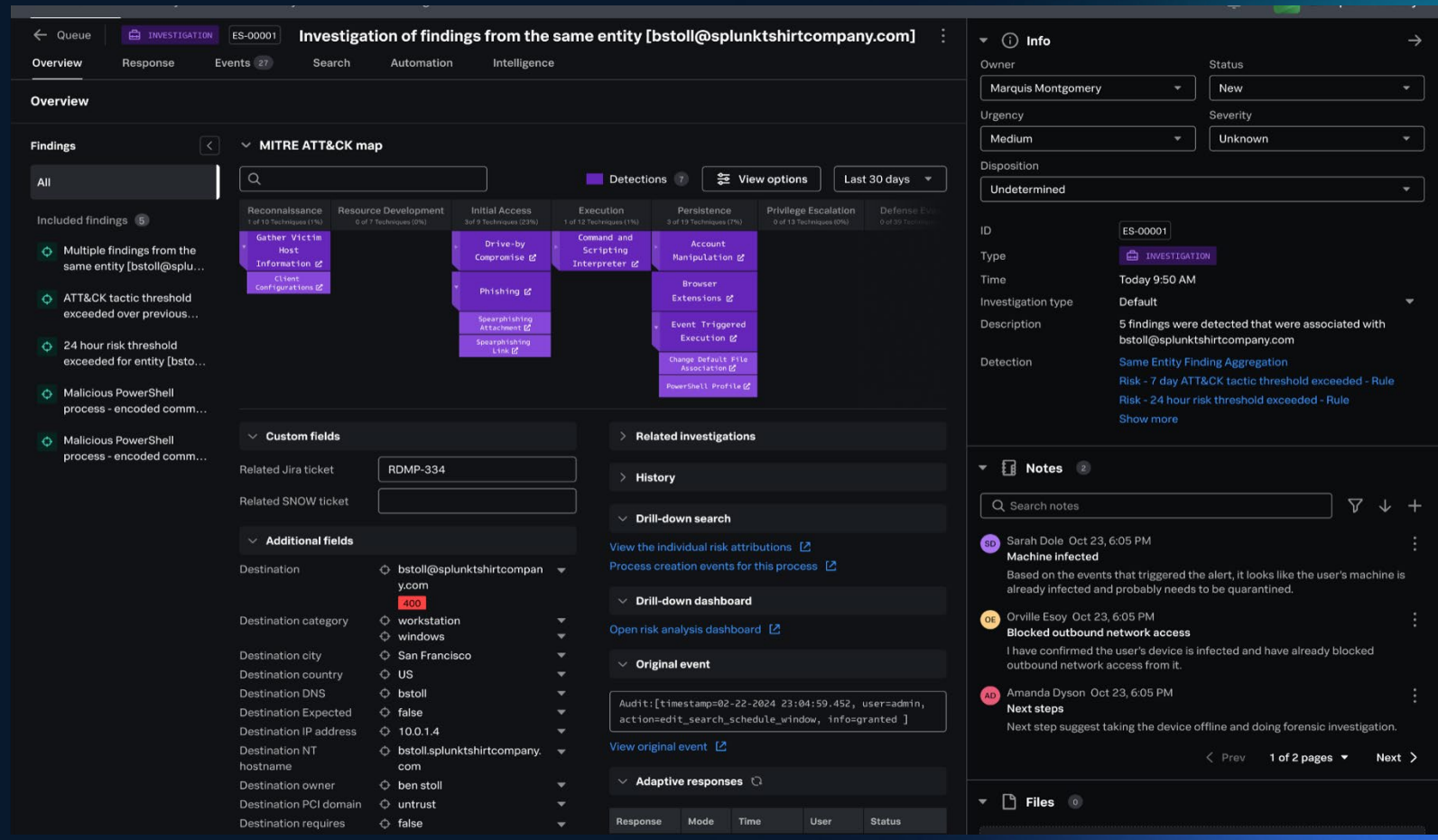
Threat Intelligence



- Native integration for all Enterprise Security cloud customers
- Enrich findings with relevant intelligence from Cisco Talos
- Helps analysts quickly understand potential threats

Fuel Operational Efficiency

SIEM



- **Single unified work surface** to complete the full TDIR workflow without leaving Splunk Enterprise Security.
- **AI Assistant in Security:** Generate SPL queries using natural language, summarize findings, generate investigation reports, and next-step/remediation guidance. New!
- **Execute response workflows** directly in ES Essentials for faster, more efficient remediation.

Dedicated and purpose-built Security AI Agents

- Detection agent
- Malware Reversing Agent
- Triage Agent
- Orchestration/ SOP Agent
- Guided Response + Automation Agents

SPEED

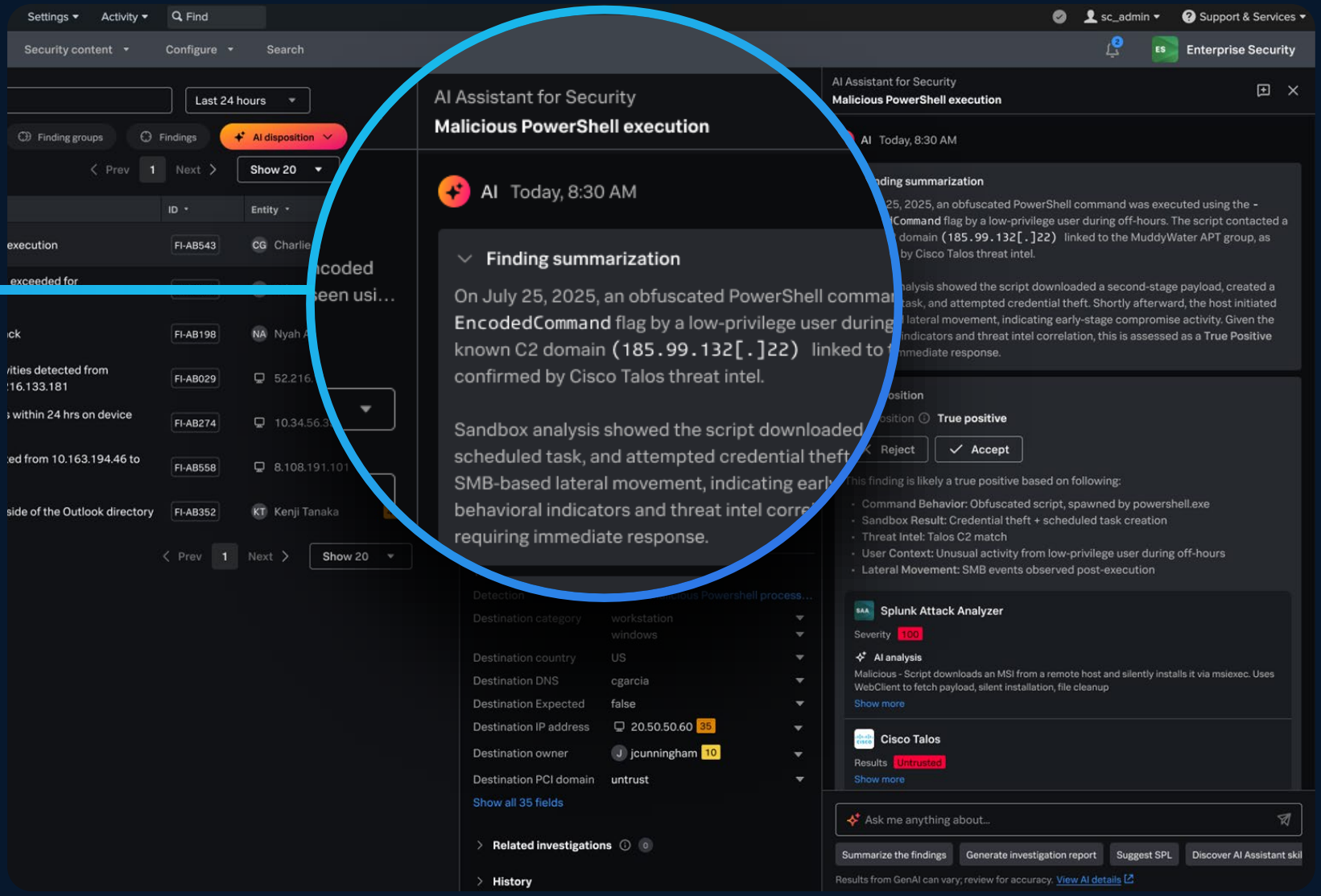
Detection → Triage → Investigation → Response

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

General Availability for Cloud

AI Assistant in Enterprise Security

- Embedded across all analyst workflows
- Guide investigations with AI-powered query generation and summarization
- Accelerate workflows with embedded, context-aware AI insights
- Empower decisions with AI-driven next step and remediation guidance



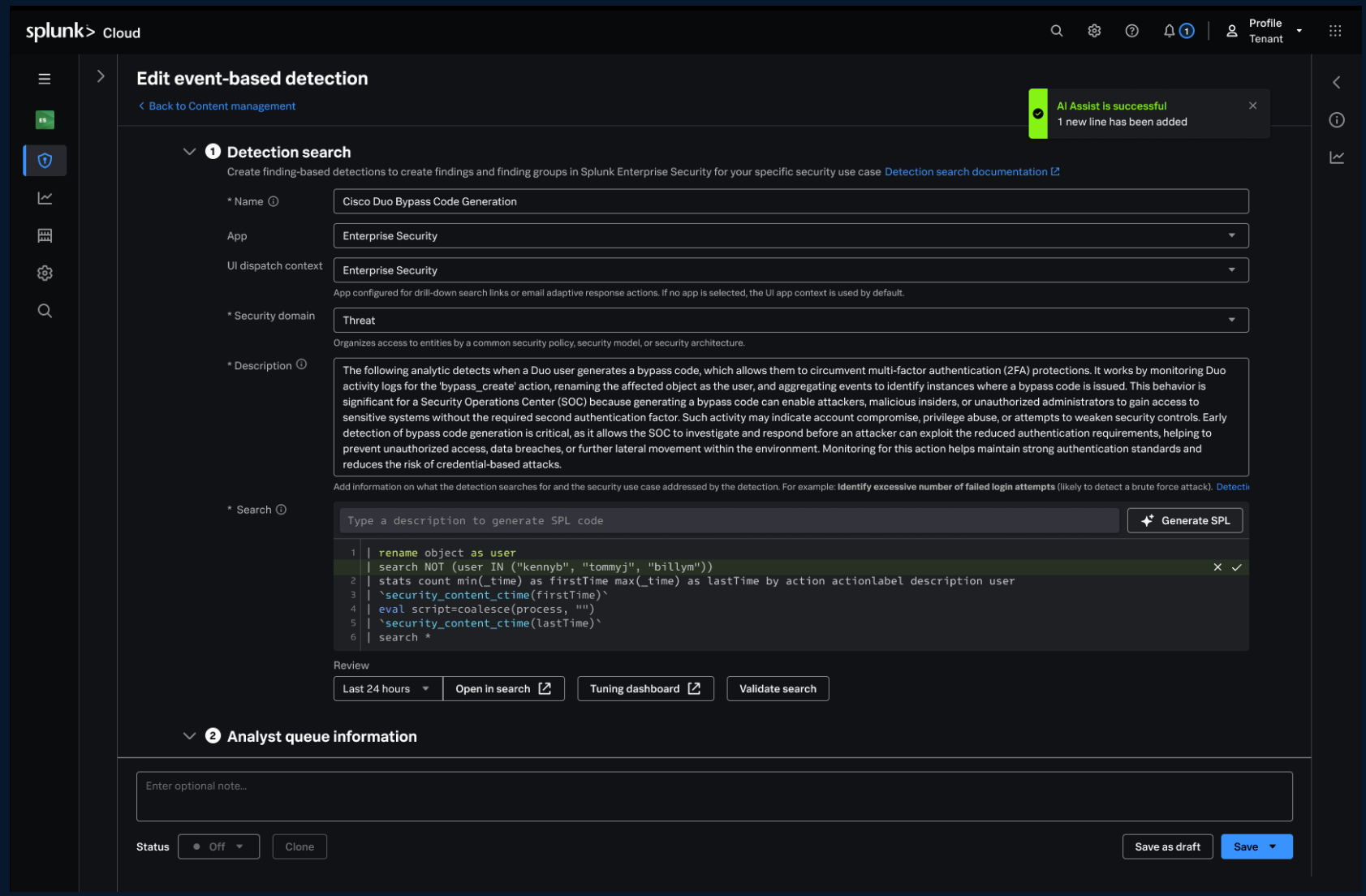
Currently available for Cloud users

© 2025 Cisco and/or its affiliates. All rights reserved.

Alpha coming soon

Detection Builder Agent

Go from detection hypothesis to production in minutes with accuracy; quickly import, tune, and tag detections; and personalize detections for your environment.

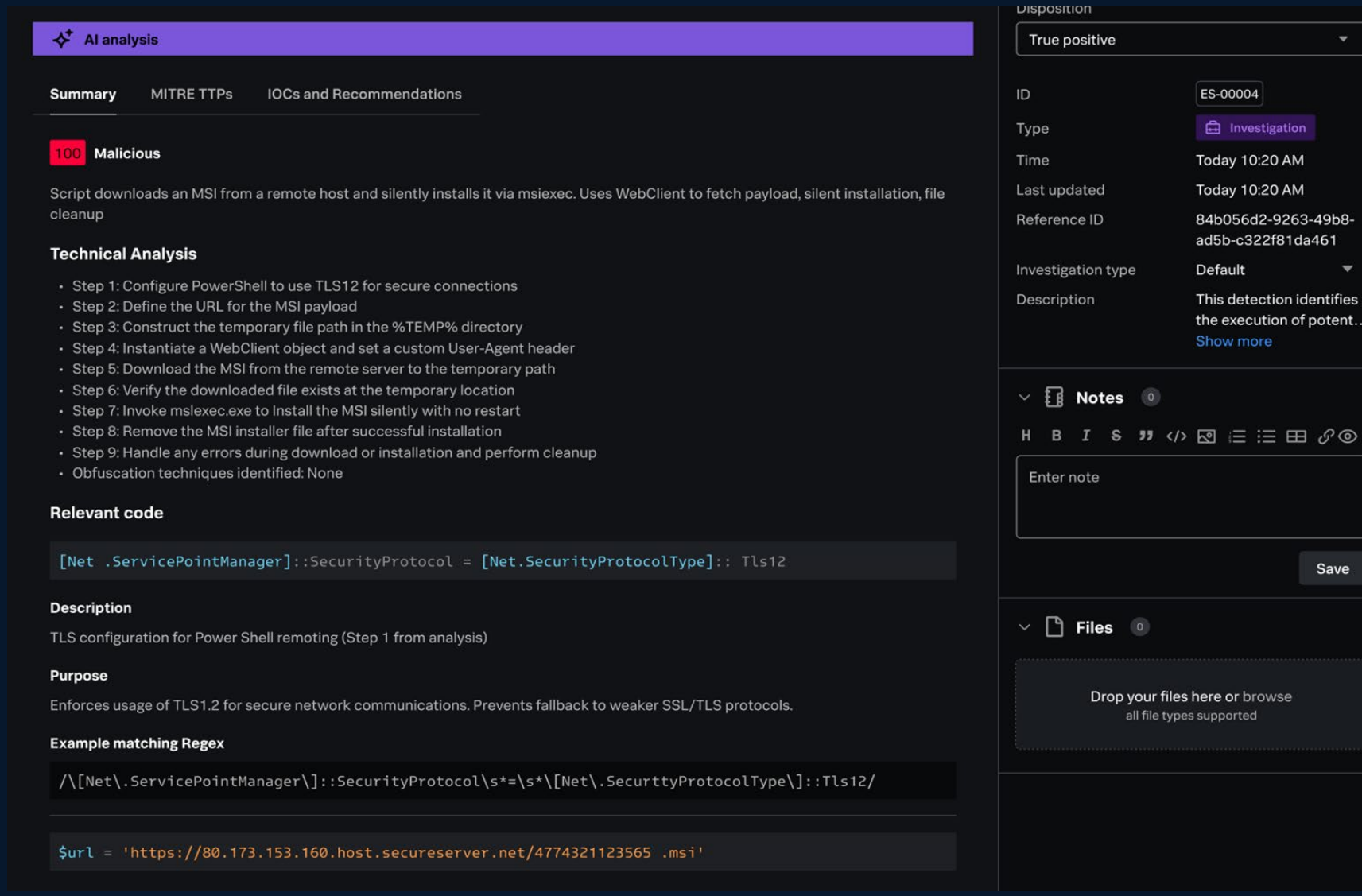


© 2025 Cisco and/or its affiliates. All rights reserved.

General Availability

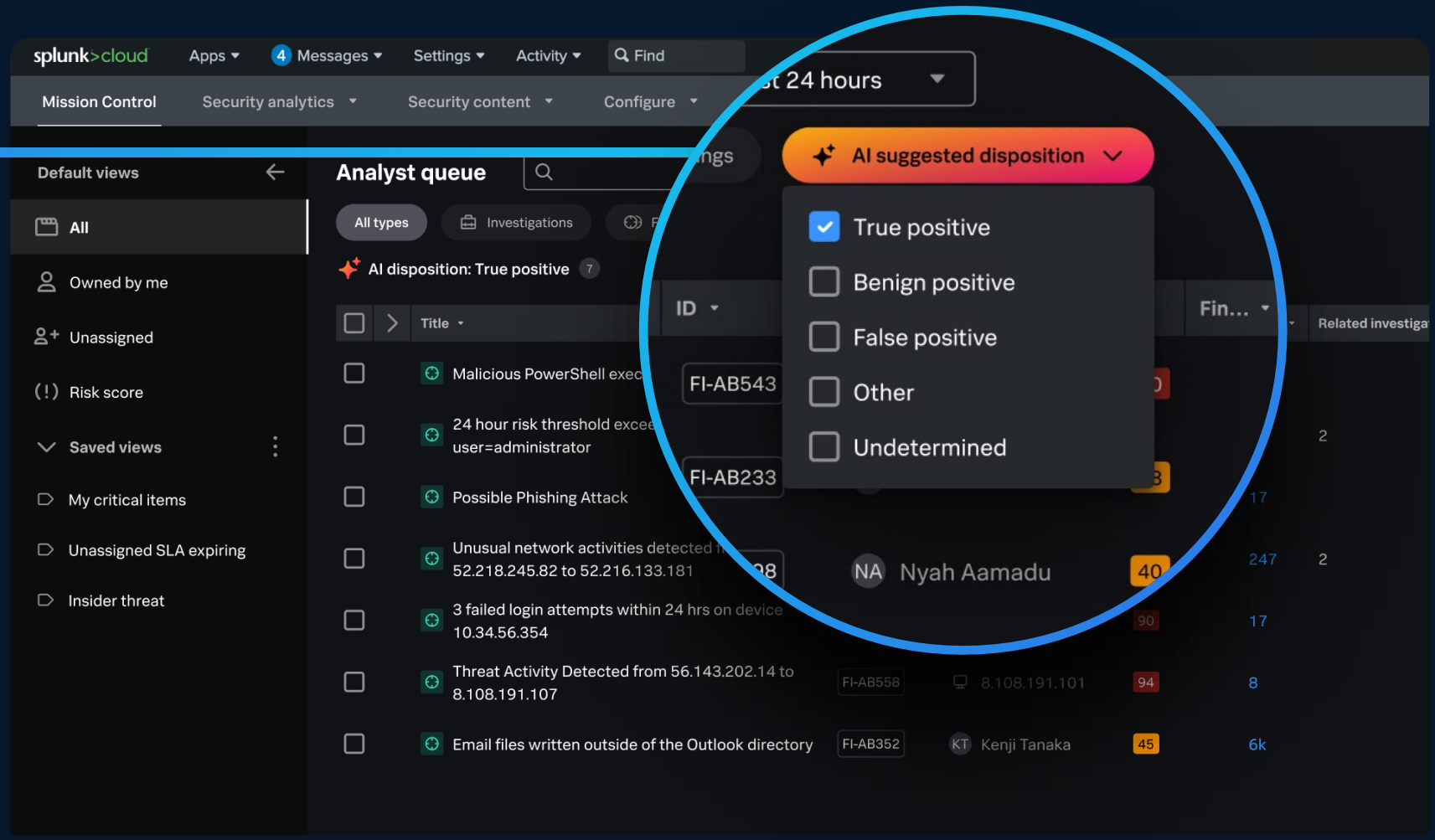
Malware Reversing Agent

- Explains malicious scripts line-by-line
- Extracts IOCs, flags evasion, and groups recurring behaviors
- Gives analysts actionable insight in seconds, not hours.



© 2025 Cisco and/or its affiliates. All rights reserved.

Triage Agent



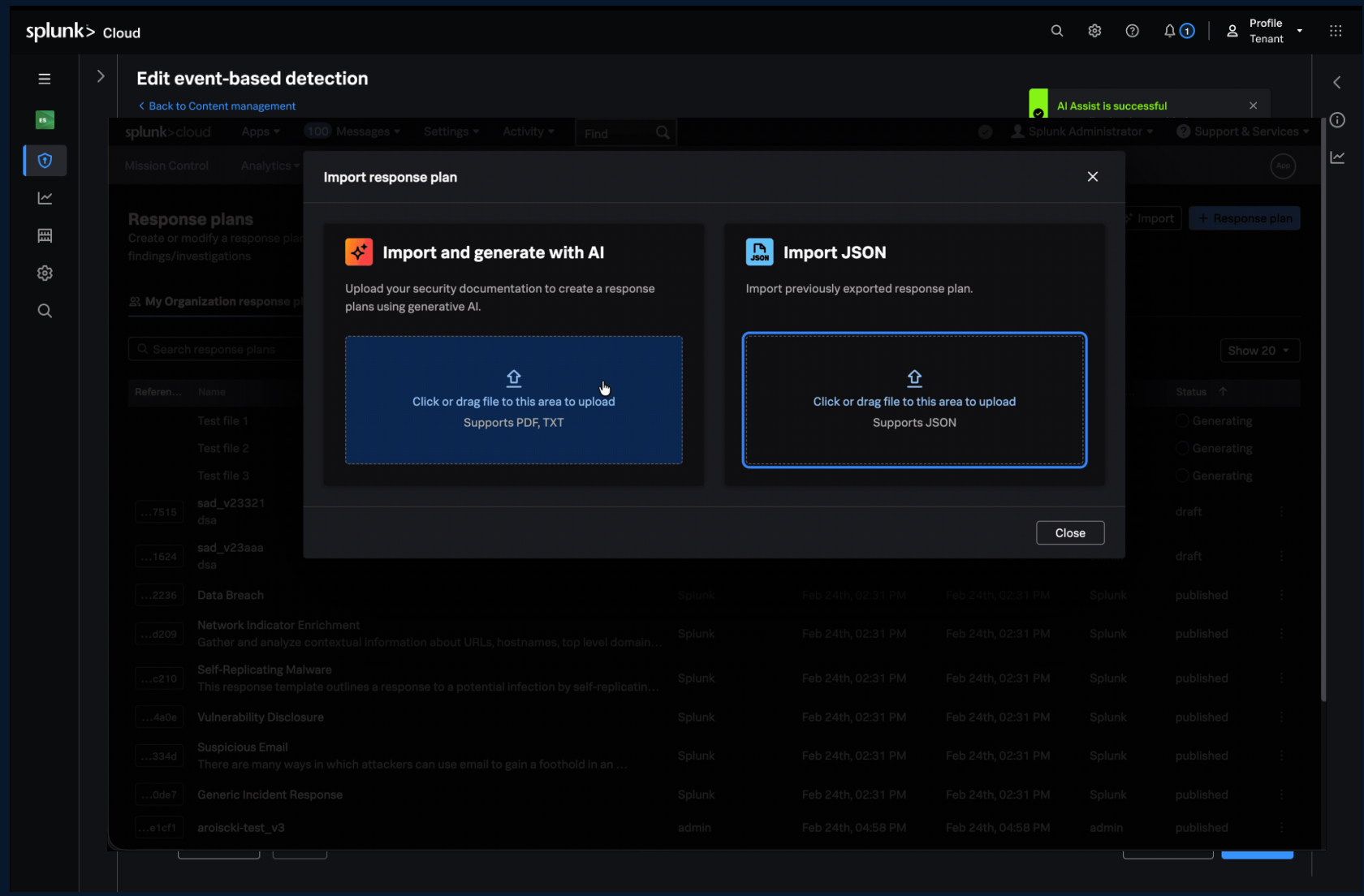
- Streamline alert prioritization
- Plan and execute investigations
- Automate insights to reduce MTTR

© 2025 Cisco and/or its affiliates. All rights reserved.

Cloud availability coming soon

SOP Agent

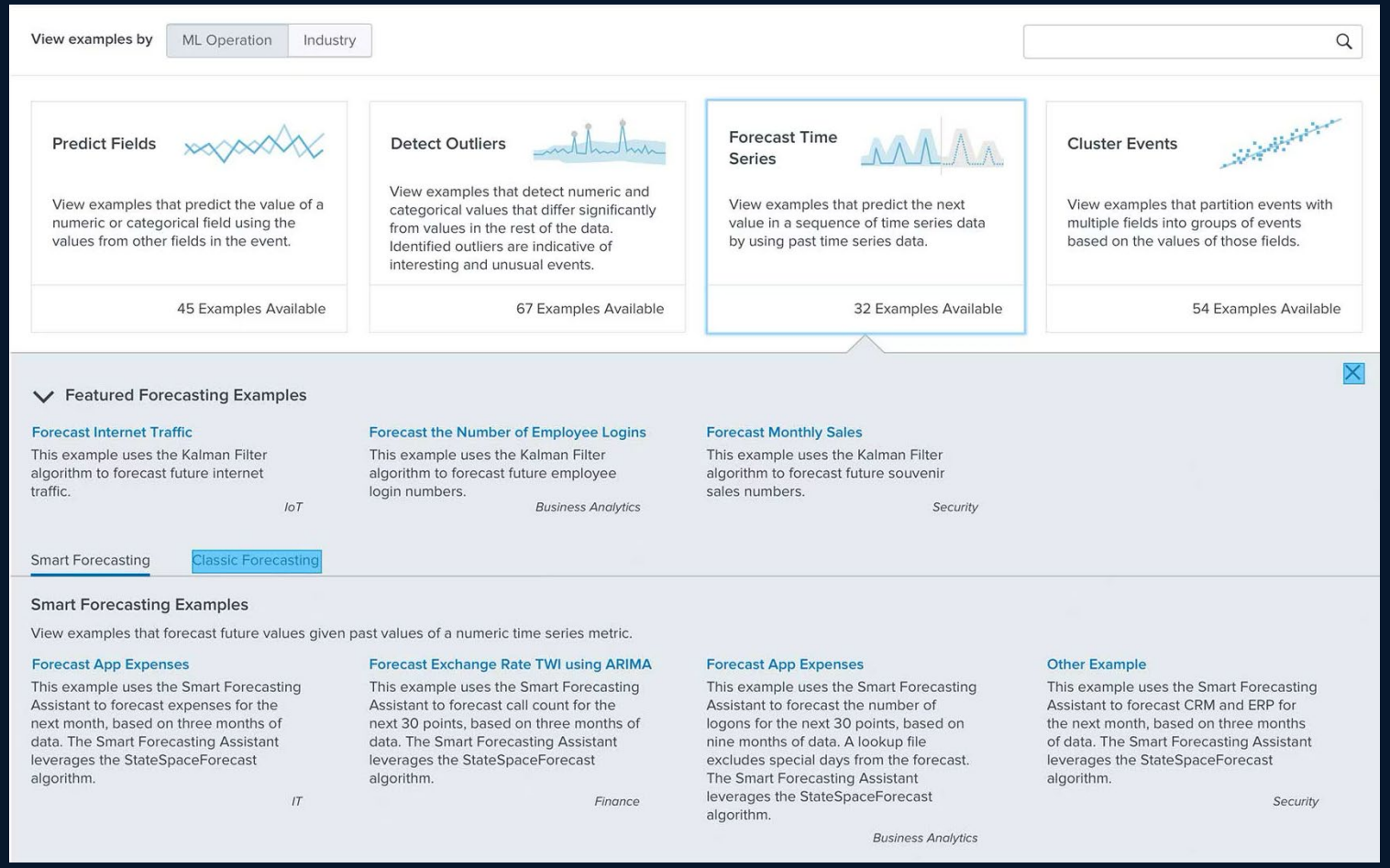
Import security standard operating procedures into Splunk Enterprise Security response plans so AI agents can act on them.



© 2025 Cisco and/or its affiliates. All rights reserved.

Splunk AI Toolkit

- Empower every user to create custom, extensible AI solutions using top LLMs over your Splunk data.



© 2025 Cisco and/or its affiliates. All rights reserved.

Delivering the Agentic SOC

Where human expertise, AI, and data work together to stop threats at machine speed.



Stop threats at machine speed **with AI & Automation (AI Assistant in ES & AI Agents)**

Scale operations by turning high-volume data into high-fidelity visibility

- Risk scoring, analysis, and prioritization
- Out-of-the-box content
- Detection & playbook authoring
- Integrated workflows
- Threat Intelligence enrichment

Streamline detection and response to focus on what matters

- SIEM / Security Analytics
- Security Automation
- Behavioral Analytics
- Exposure Analytics
- Attack Analytics

Unifying data for complete visibility with the Cisco Data Fabric



AI-powered data management



Federated Search and Analytics



AI-Native Experiences and Platform

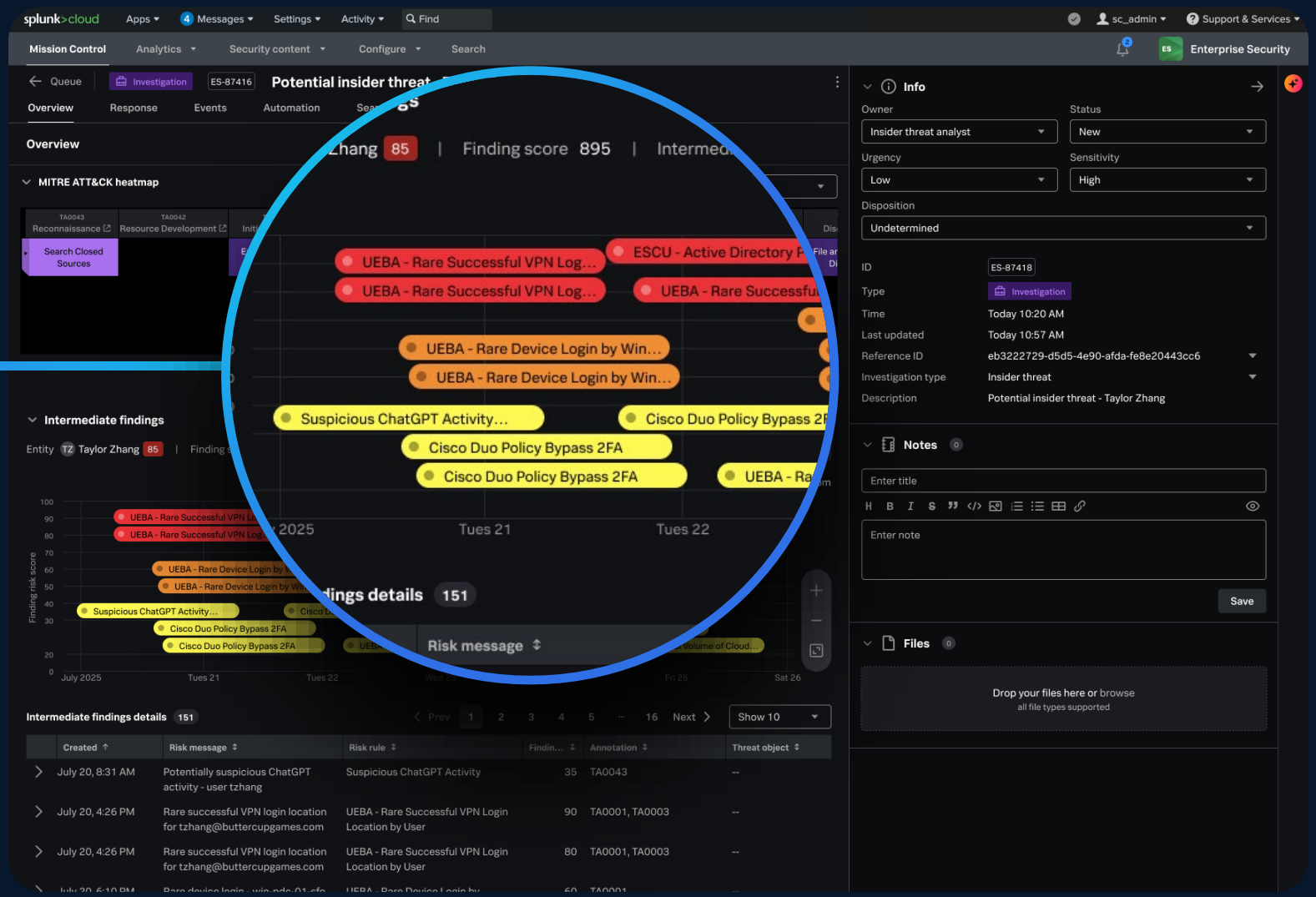


Machine Data Lake

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

The complete experience with Enterprise Security Premier



- Includes UEBA, SOAR
- Agents and AI Assistant
- Simplify your analyst experience
- Gain full visibility and control

© 2025 Cisco and/or its affiliates. All rights reserved.

Enterprise Security

Now available in two editions



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

The Agentic SOC* vs. HAFNIUM



The Result: An Agentic SOC* outpaces HAFNIUM, by unifying data, analytics, tooling and AI for the analyst

© 2025 Cisco and/or its affiliates. All rights reserved.

*Includes future capabilities

Unmatched Strengths that Set Splunk ES Apart

An open, data-native foundation data federation and a unified TDIR platform backed by the industry's deepest ecosystem

Data management and federation

Unique data management capabilities, like routing, filtering, masking, and federation to maximize performance and ROI

Architectural flexibility

Deploy on-premises, in the cloud, or in hybrid environments, with seamless IT and OT integration for broad attack surface coverage wherever you operate.

Market leadership

Splunk is the market share leader, recognized as a leader by Gartner, IDC, and Forrester. Demonstrating that our platform is trusted by a broad user base, providing confidence in your security investments.

Innovating together

With 2,200+ global security partners, thousands of partner and community-built apps, and an active user forum, Splunk delivers unmatched collaborative innovation and support.

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Splunk is a recognized leader in cybersecurity

Splunk Security provides an unparalleled foundation to power the SOC of the future

Gartner®

Eleven-Time Leader

2025 Gartner® Magic Quadrant™ for SIEM

Ranked #1 in all three Use Cases

2025 Gartner® Critical Capabilities for SIEM

FORRESTER®

Leader

Forrester Wave™: Security Analytics Platforms, Q2 2025

OMDIA

Leader

Omdia Universe: Next-Generation SIEM Solutions

IDC

Leader

2024 IDC MarketScape for SIEM for Enterprise

Ranked #1

2023 IDC Market Share for SIEM

TrustRadius

5 awards for SIEM and SOAR

PeerSpot

Leader Award SIEM and SOAR

kuppingercole ANALYSTS

A leader in SOAR

Trusted by leading organizations

Soriana · tide · TESCO · Cal Poly · REI co-op · Carnival · Singapore Airlines

Pioneering into the future

AI-Driven Risk Optimization

Proactive and Predictive Security Operations

Autonomous Resolution at Machine Speed

Adaptive and Intelligent Data Fabric

The future of security operations



Human Expertise

\+



AI

\+



Data

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

Your security team is stretched thin.

It's time for an agentic SOC platform that:

- **Automates the mundane**
- **Clarifies the complex**
- **Stops threats at machine speed**



The Evolution of the SOC Team for the AI era

© 2025 Cisco and/or its affiliates. All rights reserved.

CISCO Connect

Thank you

