CISCO Connect

Power the SOC of the Future

Kera Porter– Security Solutions Engineer

Quinlan Ferris – Solutions Engineer

April 7, 2026

Agenda

01 The Agentic Landscape

02 Becoming Resilient

03 SOC Challenges

04 Splunk Security

05 SOC of the Future

06 Cisco Integrations

AI and the Threat Landscape

AI Introduces New Opportunities and Risk

1. Rapid AI integration across industries has increased the technology's visibility and attack surface.
2. Cybercriminals are disguising malware as AI tools or installers.
3. Voidlink was first confirmation of threat actors utilizing agentic AI frameworks

Voidlink

First Evidence of AI-Assisted Development

Medium to high confidence of development with AI/LLM assistance.

Unusually fast two-month development cycle for a framework of this complexity.

Boilerplate Patterns:

Uniform API versioning (all modules are _v3).

"John Doe" placeholders in decoy response templates.

Systematic and perfectly consistent debug output across different languages.

Trae.ai LLM IDE likely used

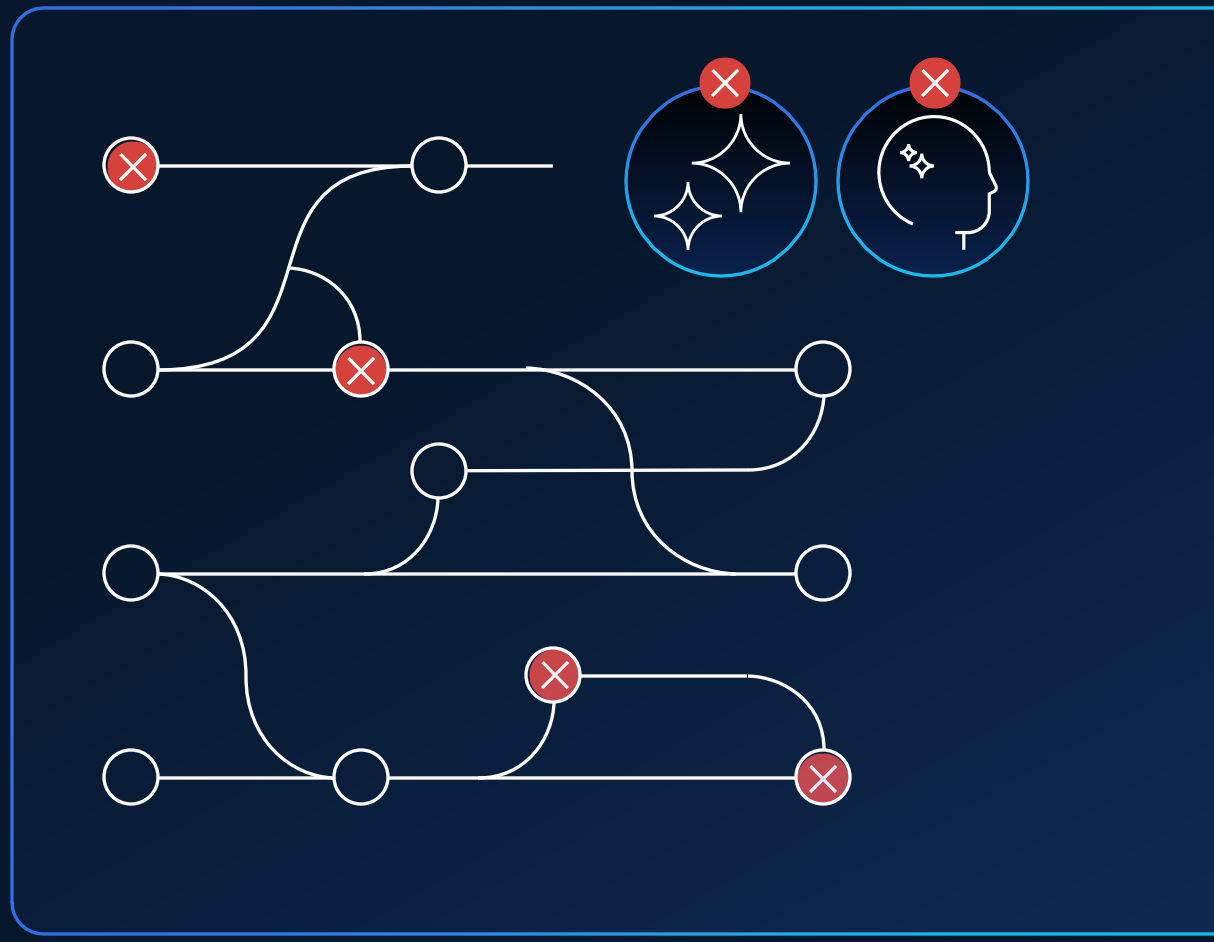
Attackers Are Using Agentic AI to Operate Faster

Emerging trends: “Vibe hacking,” “evil AI,” and Psychopathia Machinalis show attackers using AI for rapid manipulation and execution

Autonomous agents: Agentic AI tools are making decisions and acting without waiting for human input

From advice to action: These AI-enabled systems not only provide technical guidance, but hands-on operational support

Machine speed and scale: Attacks that once needed coordinated human teams can now be launched faster by a single AI-assisted operator



AI Usage Across the Kill Chain

Reconnaissance

AI automates gathering intelligence on organizations, employees, and systems.

Weaponization

AI can be used assist in the development of new malware and disguise malicious tools.

Delivery

AI generates highly convincing fake emails, messages, and websites. Providing obfuscated delivery mechanisms

Exploitation

Threat actors could use AI to uncover vulnerabilities and code flaws, leading to faster exploitation and increased risk across both the public and private sectors.

Installation

Malicious code can be hidden within AI-powered software components and plugins.

Command & Control

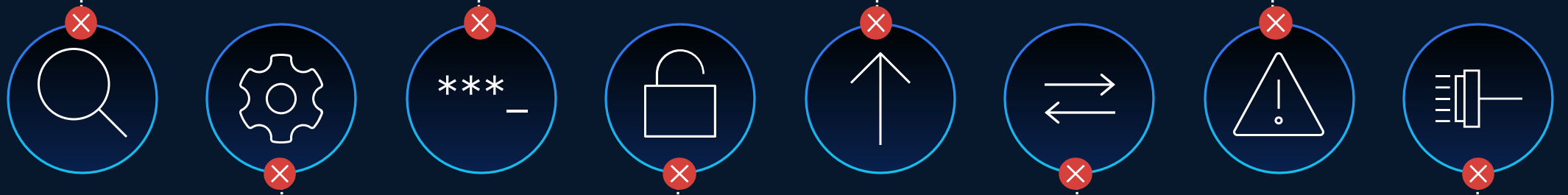
AI translates human-like instructions within malware into executable commands.

Actions on Objectives

AI can assist in the automation of data theft and the execution of the attack's final goal.

Cleanup tracks

AI helps disguise malicious activity as normal traffic to evade detection.



Securing the Agentic Workforce

Protect the agents from the world

Protect the world from the agents

Detect & respond at machine speed & scale

Google

Microsoft

Amazon

Databricks

Cisco XDR

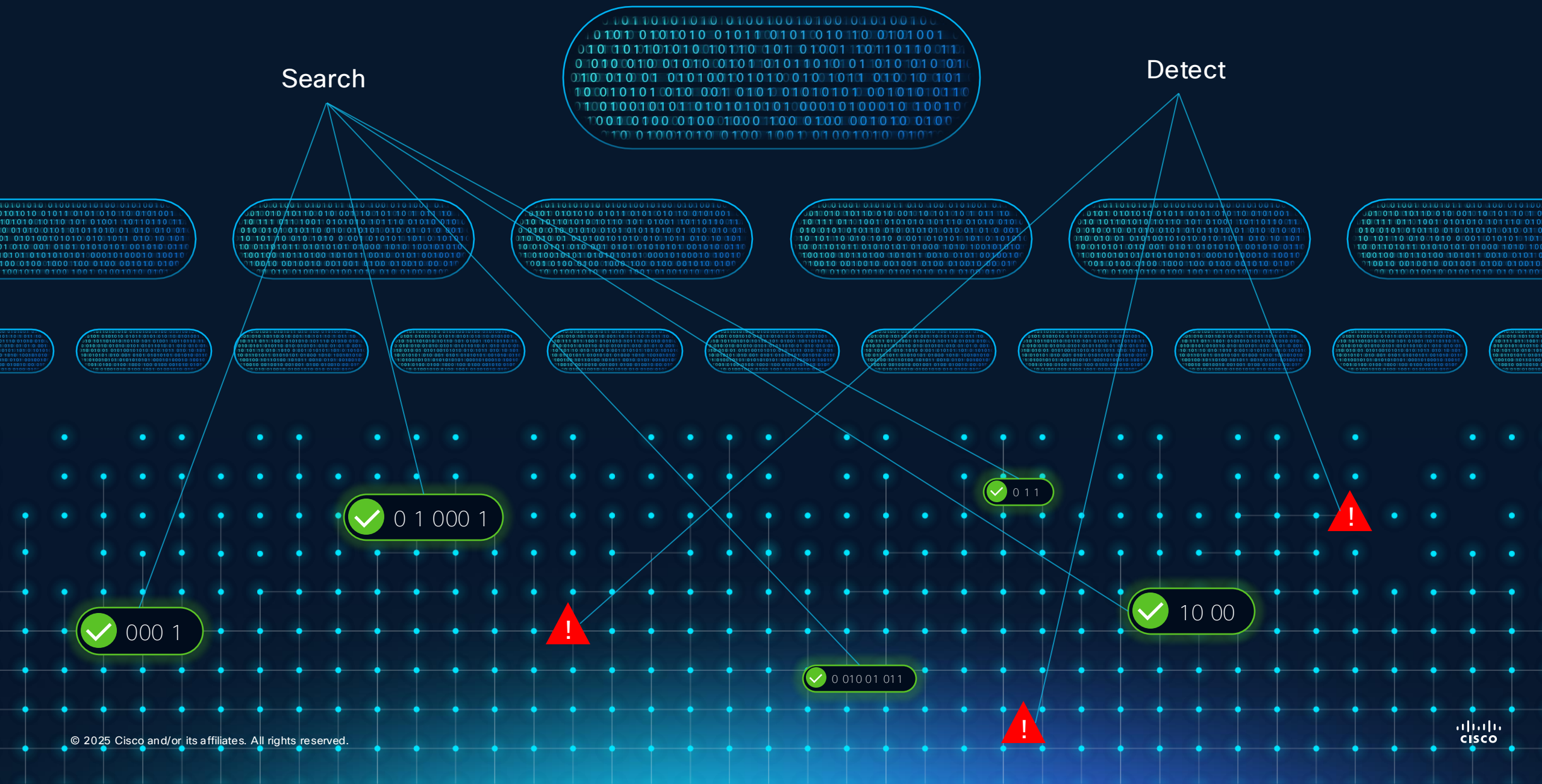
Cisco SAL

Crowdstrike

Palo Alto Networks

SentinelOne

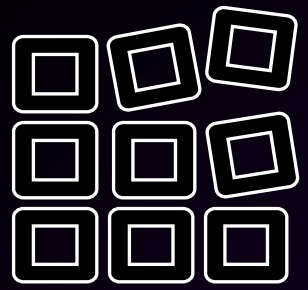
cisco



The data landscape is changing for the SOC

How do you effectively manage data for the SOC of the future?

Data is growing exponentially.



All data is not created equal.

Data may not be able to be moved within a time frame or at all.

Effectively Prioritize Data Based on Use Cases for Your SOC

Manage your data to deliver a stronger security posture

Manage SOC Data Your Way

Flexibility to manage, find and analyze actionable data in your SOC.

Filter and transform data at the Edge or in the Cloud prior to any indexing in Splunk.

Bring search and analytics to external stores without ingestion.

Public Cloud | Private Cloud | On Premises

Amazon S3 | Amazon Security Lake | Additional Data Lakes

Data management

Filtering, Redacting & Routing

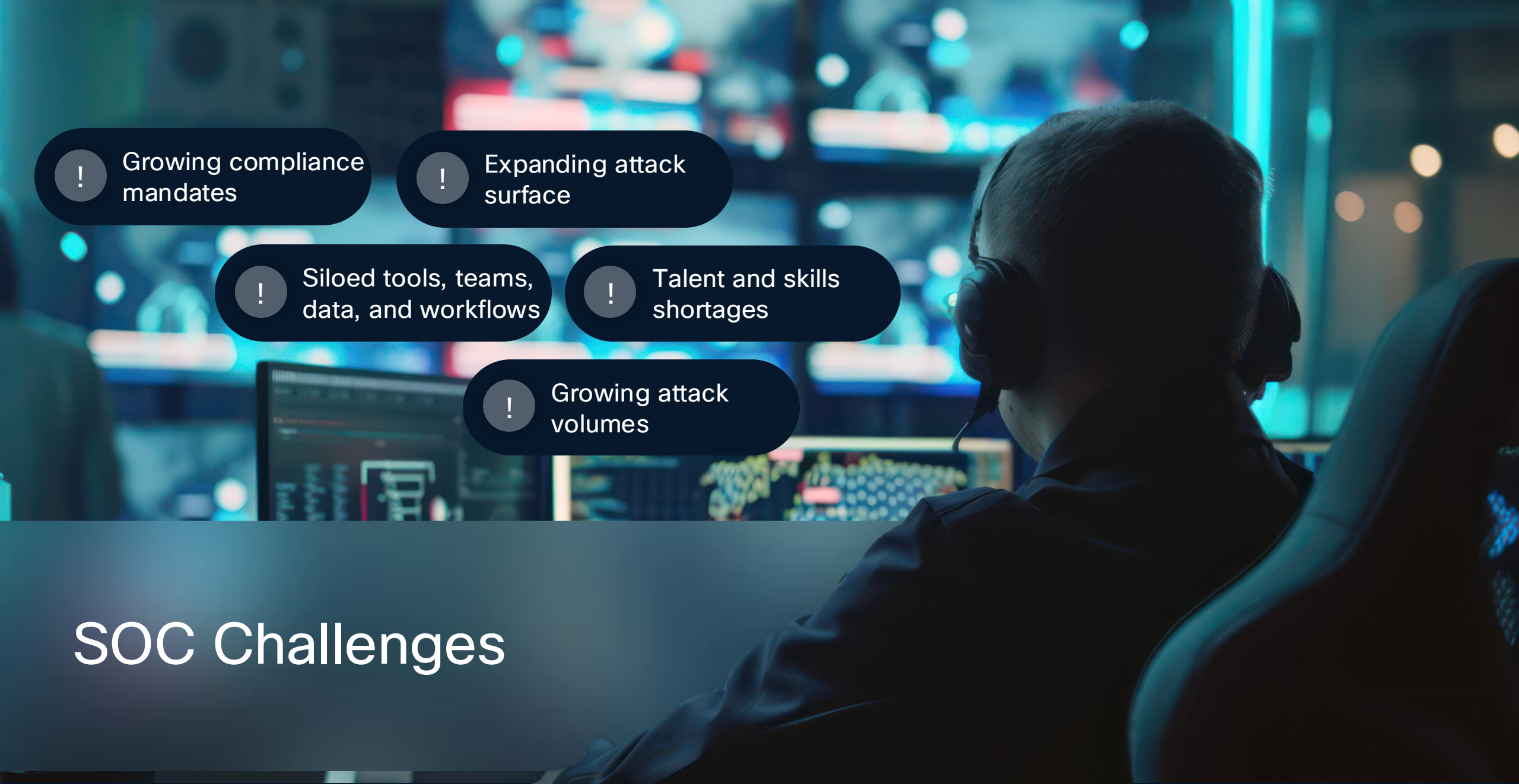
Federation

Search & Analytics

Data normalization

CIM, OCSF

Splunk Enterprise Security



SOC Challenges

Impact of Today's Security Challenges

3+

hours on average that analysts spend on alert investigations

41%

of alerts are ignored because analysts don't have the bandwidth or proper context to investigate

Up to 25+

different security tools are used in the SOC, each performing different actions across detection, investigation and response

Splunk Security Focus Areas

Powering the SOC of the future with Splunk

- Unify TDIR with Automated Workflows
- Transform Detection Engineering
- Gain Asset Visibility to Address Risk and Compliance
- Embrace Federated Data Access and Analytics
- Leverage AI for Guided Security Operations

A New Operating Model for Security

Open, AI-Native Data Platform

Leverage the Fabric for Full-Stack Security AI

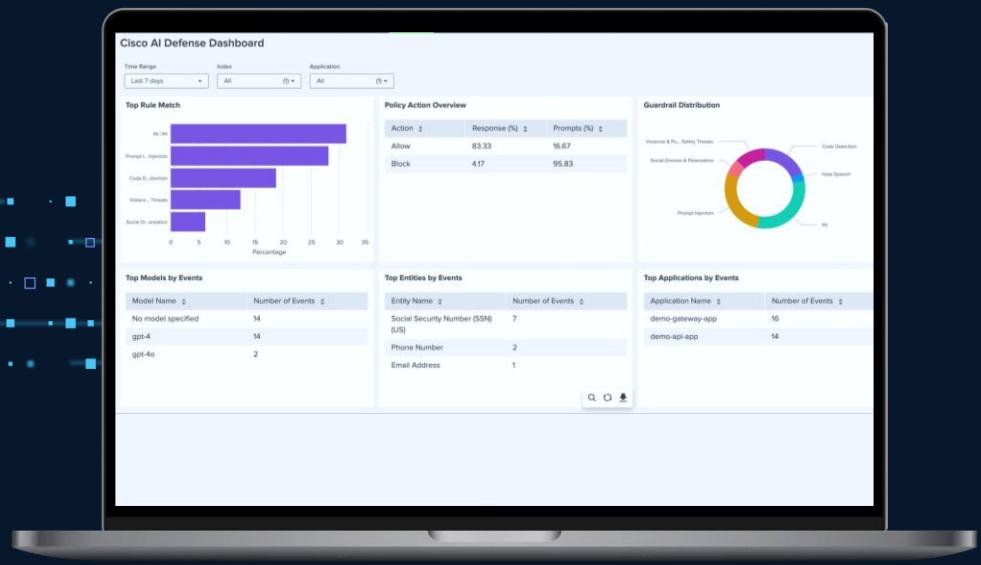
Unparalleled visibility across every AI layer

AI models, agents, and applications

AI workloads and infrastructure

CISCO DATA FABRIC

Splunk brings together disparate sources and tools for unified protection

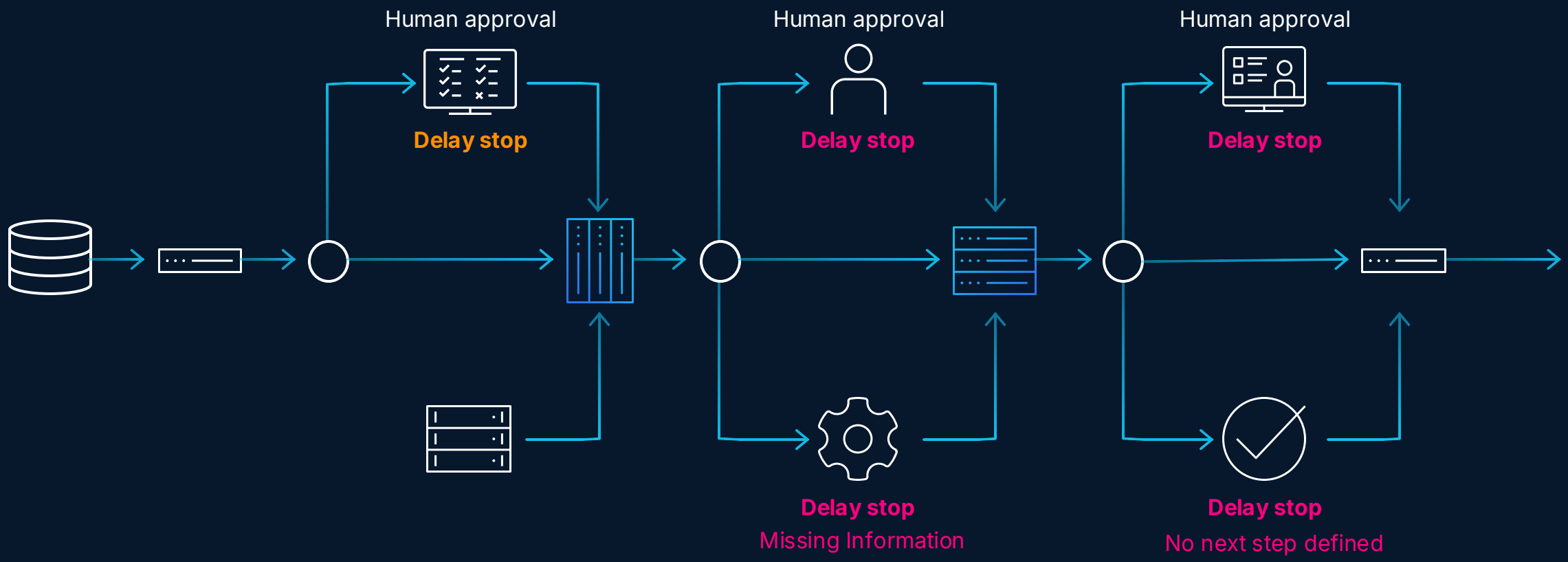


Discover AI assets – known and unknown - in your environment

High fidelity detection across every layer of AI infrastructure

Block emergent attacks at any level

The Traditional SOAR Ceiling



It is time for SOAR to evolve

Dedicated and Purpose-Built Security AI Agents

Agentic Automation

Triage Agent

ASK

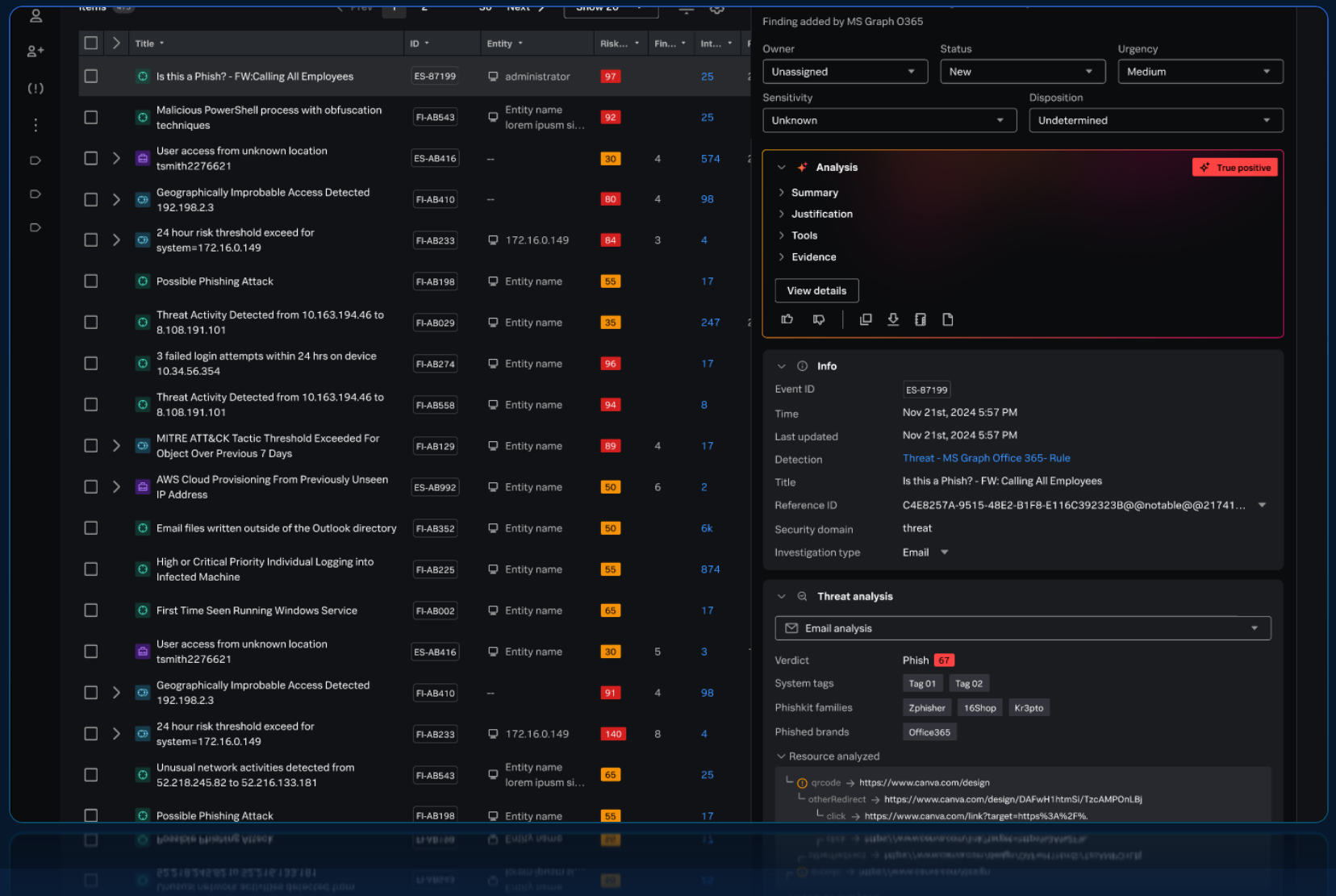
Streamline alert prioritization and disposition

SEE

Automate insights to reduce MTTR

ACT

Plan and Execute investigations



Accelerate triage from signal → context → decision with an agent built to reduce noise and surface what matters.

Human-AI Operating Model

How AI Trust is Earned : Evidence Packets

Auditable

Human Out Of The Loop (Auto)

LOW RISK

Traceable

Human On The Loop (Supervised)

MODERATE RISK

Provable

Human In The Loop (Approved)

HIGH RISK

cisco

Agentic Automation

Investigation Canvas

ASK

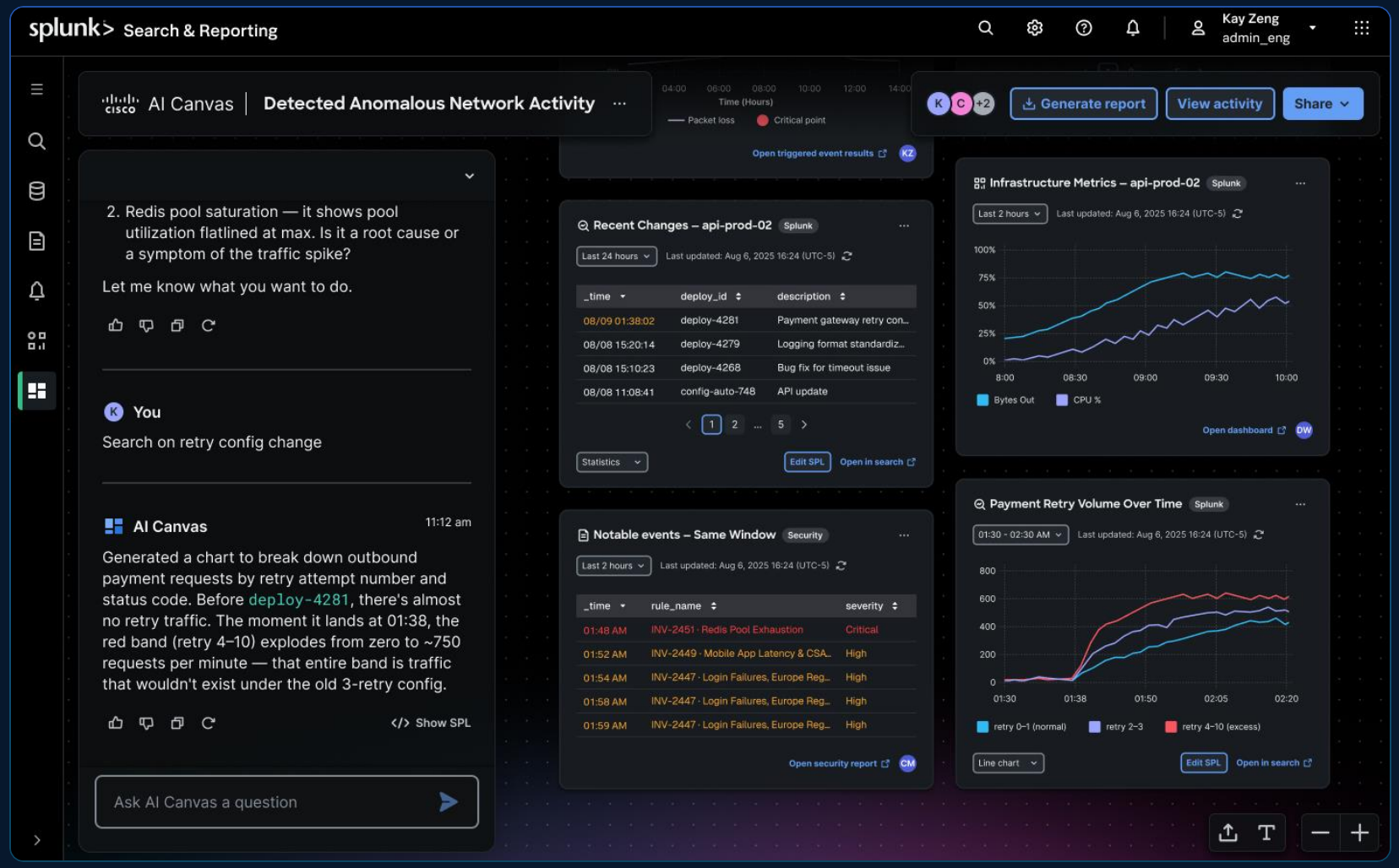
Type what you want to know

SEE

Investigation Canvas builds the visualization for you

ACT

Launch SOAR-powered actions right inside the workspace



Enable analysts to move from question → insight → response in a single generative workspace.

From Automation to Resilience

OBSERVE

Telemetry + XDR

DECIDE

Splunk correlation
+ agentic reasoning

ENFORCE

Cisco network controls
+ integrated response

VALIDATE

Splunk confirms impact
and continual monitoring

Automation executes. Resilience verifies, adapts, delivers, and overcomes

Splunk Security Product Forward-Vision

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

+

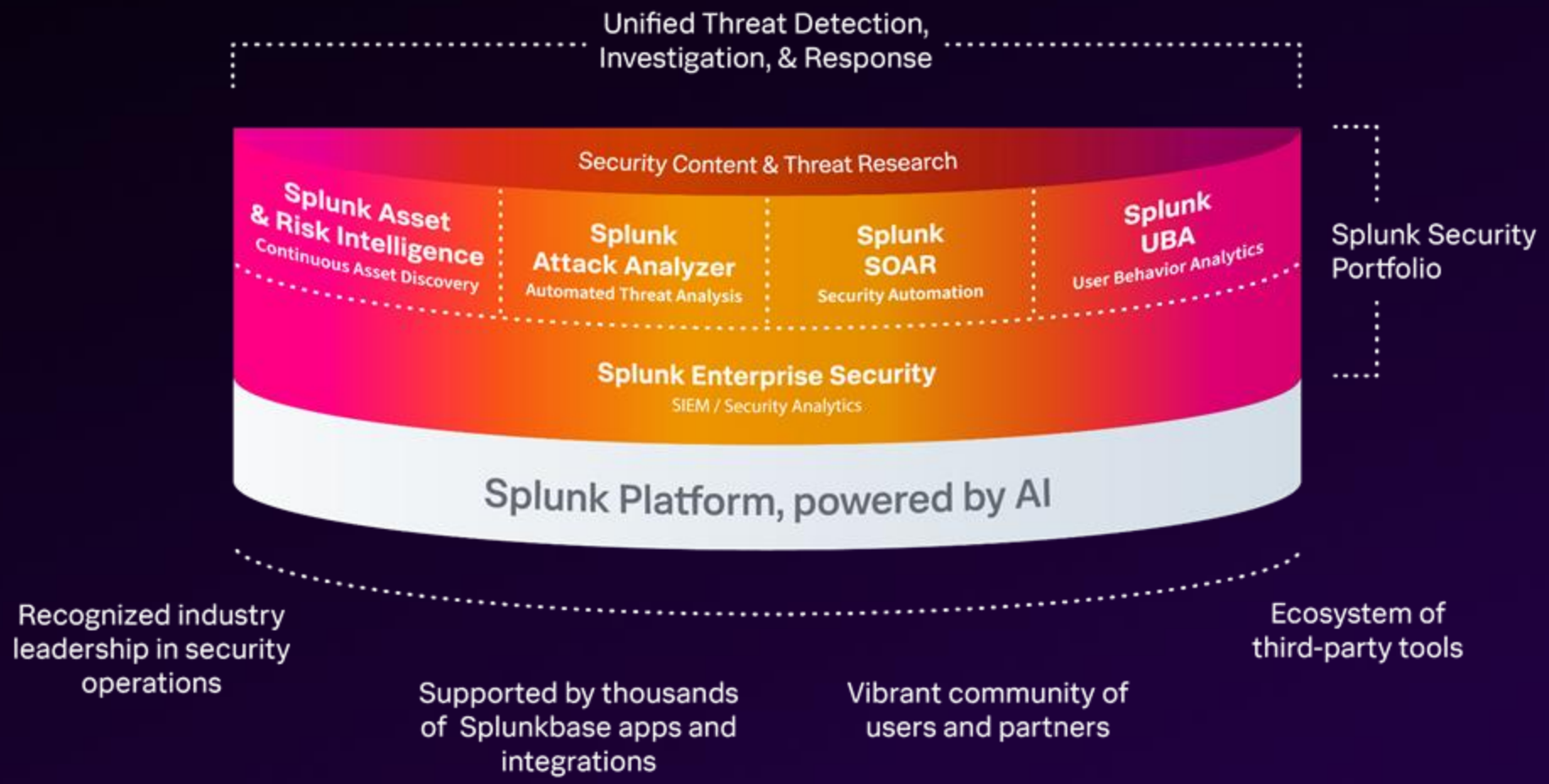
AI

+

Data

cisco

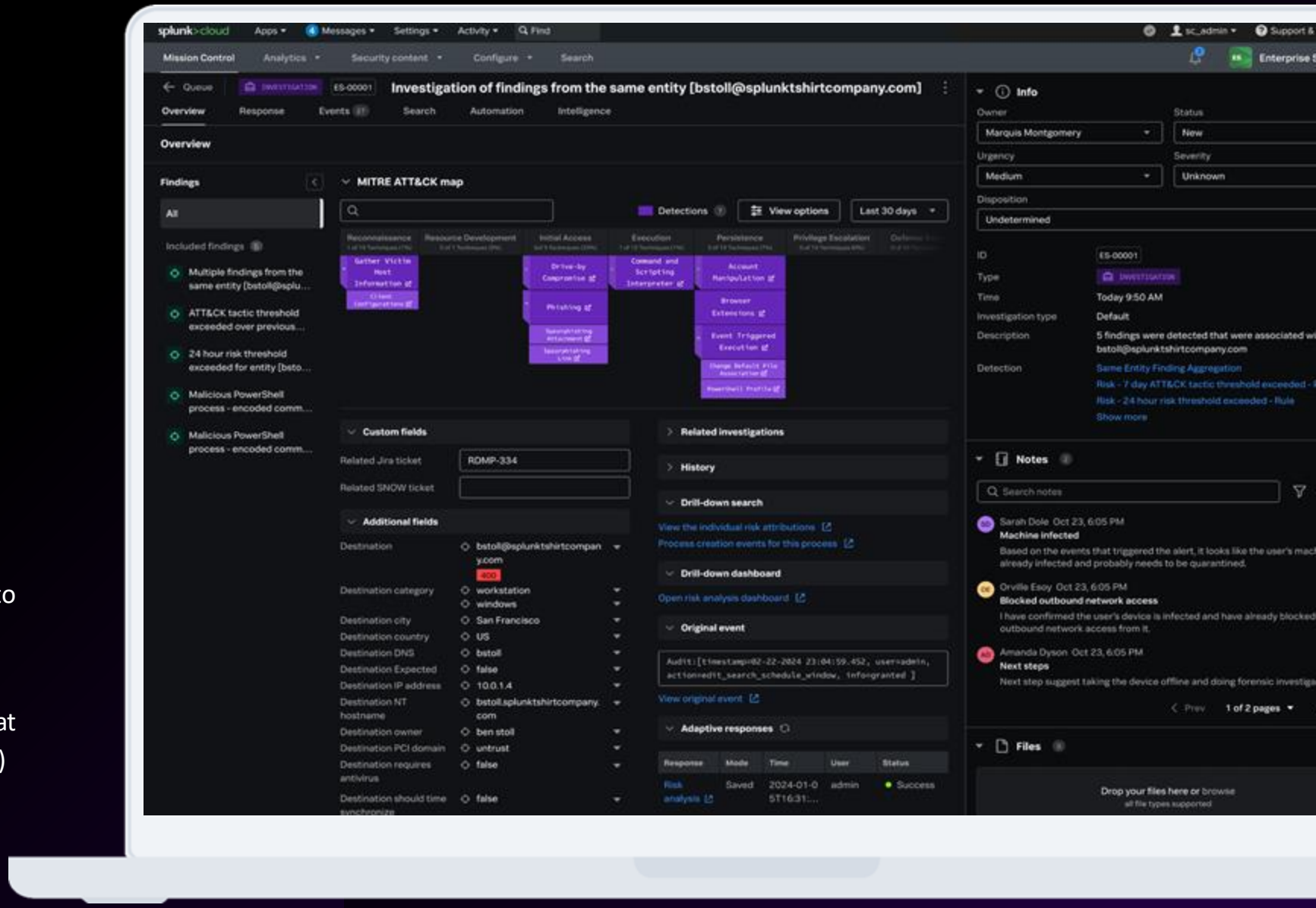
Powering the SOC of the future with the leading TDIR solution



Splunk Enterprise Security

Power Your SOC With the SIEM of The Future

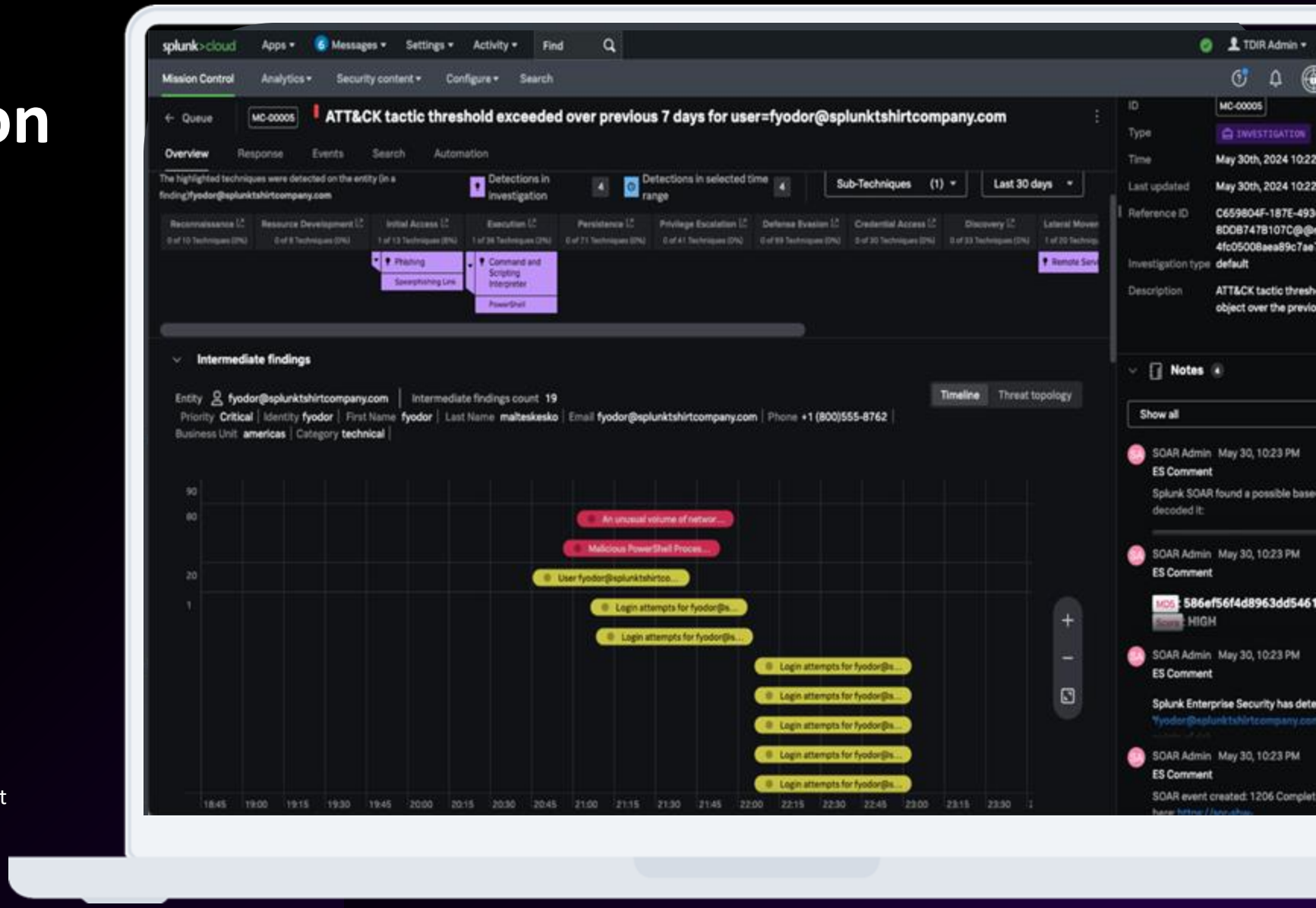
- **Realize comprehensive visibility** to make sense of data noise and enable fast action.
- **Empower accurate detection** with context to streamline investigations and increase productivity.
- **Fuel operational efficiency** by unifying threat detection, investigation and response (TDIR) workflows.



Empower Accurate Detection with Context

Streamline investigations and increase productivity

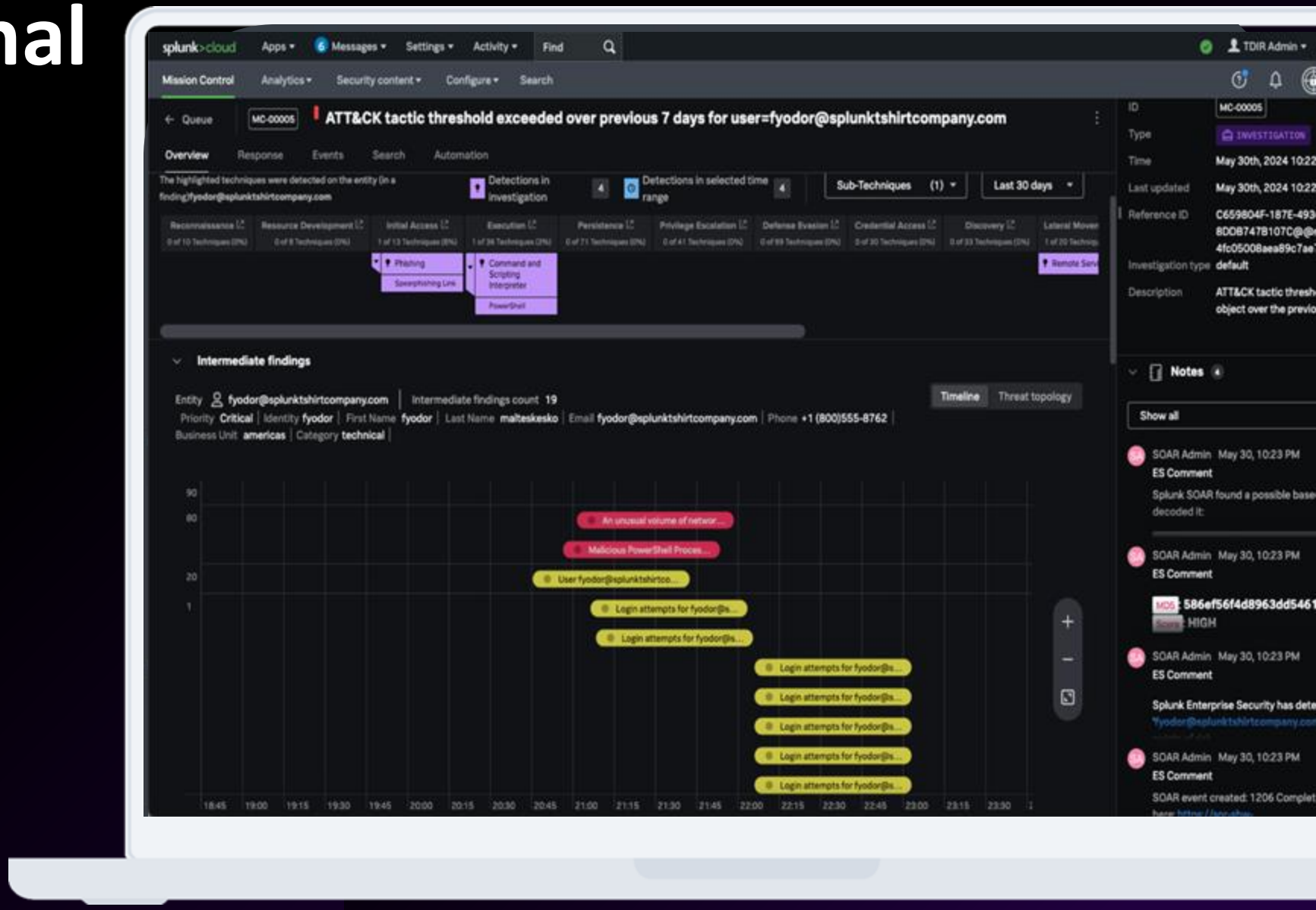
- **Drastically reduce alert volumes** by up to 90% with risk-based alerting (RBA).
- **Tap into 1,700+ out-of-the-box detections** to find and remediate threats faster.
- Easily maintain up-to-date detection content with native, **automatic detection versioning.**
- **Enhanced detection capabilities** help analysts understand and implement a risk-based alerting detection strategy.
- **View all related high-fidelity findings** with a single click using **Finding Groups***, streamlining the analyst workflow



Fuel Operational Efficiency

Unify threat detection, investigation and response (TDIR) workflows

- **Single, modern, unified work surface** to complete the full TDIR workflow without leaving Splunk Enterprise Security.
- **Native integration with Splunk SOAR*** automation playbooks and actions to optimize MTTD, MTTR and increase operational efficiency.
- **Execute response workflows** directly in Splunk Enterprise Security for faster, more efficient remediation.



*Splunk SOAR subscription required

Cisco Integrations – A Deeper Dive

NEW

Security Insight, on Us

Firewall Logs at no additional cost in Splunk*

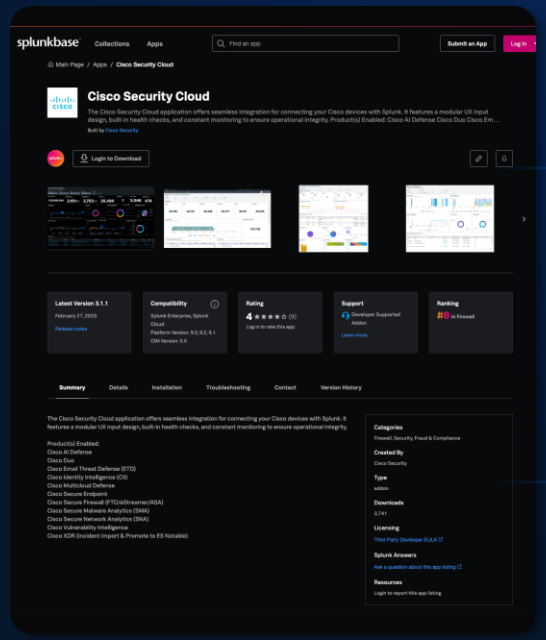
AVAILABLE
AUGUST 2025

New detections | Automated response

*Cisco Firepower (FTD) firewalls are entitled to 5GB of Splunk logging capacity with purchase or equivalent for SVC or vCPU

Harnessing the Value of Cisco Telemetry

Cisco Security Cloud App



TELEMETRY
ALERTS

Splunk

- XDR
- Secure Network Analytics
- Duo
- Email Threat Defense

- Multicloud Defense
- Secure Malware Analytics
- Secure Endpoint
- Vulnerability Management

- Identity Intelligence
- Secure Firewall
- AI Defense (new)
- Hypershield – Isovalent (July)

Integrations to Protect Your Entire Digital Footprint

Threat intelligence

Enhance defense against known and unknown threats

Splunk +
Cisco Talos

Security alerts and context

Accelerate detection, investigation and response

Splunk +
Cisco Security Cloud App

Secure AI

Detect and reduce AI-based risks

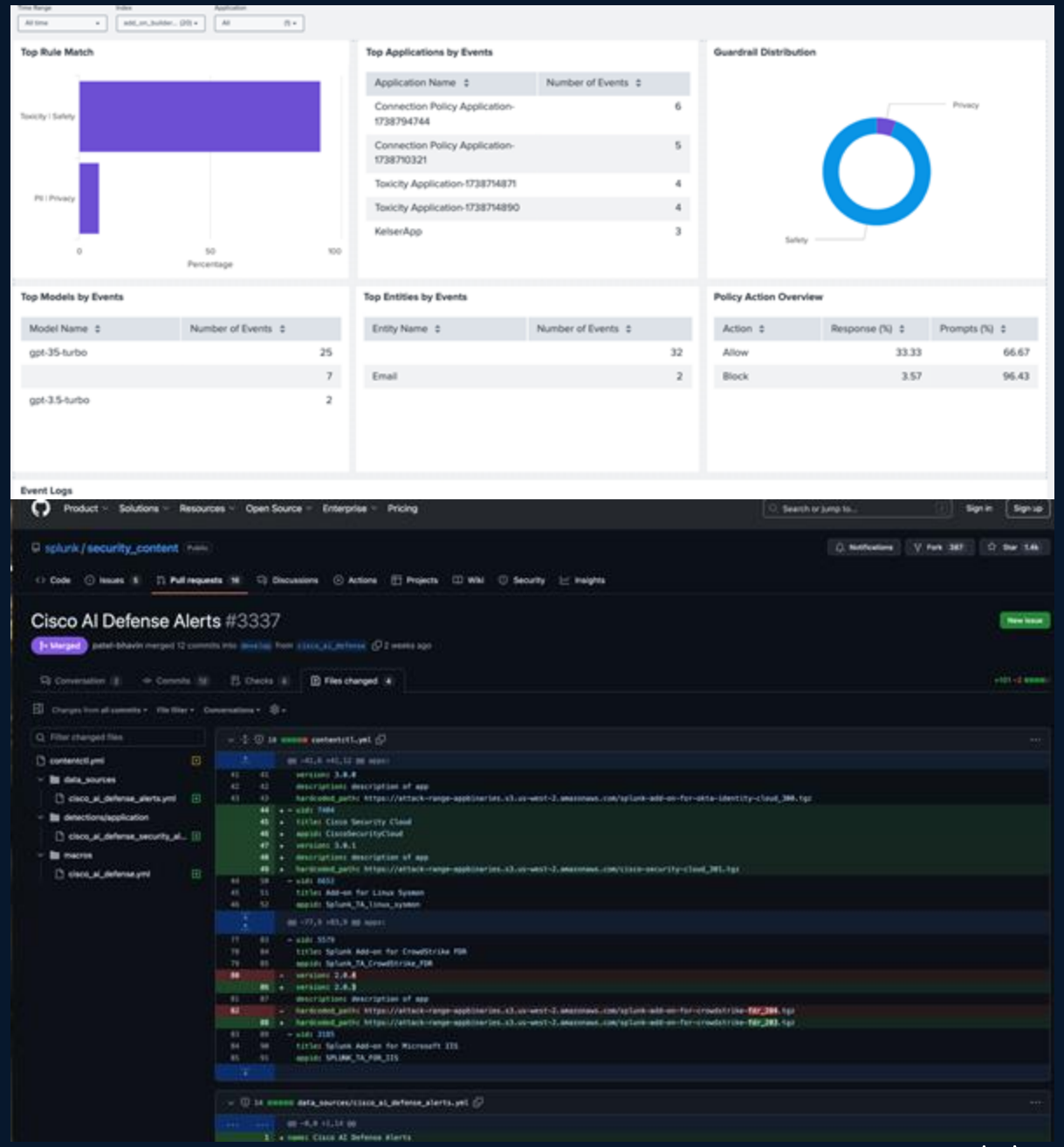
Splunk +
Cisco AI Defense

Now Available

Cisco AI Defense

Gain visibility into emerging AI risks with Splunk

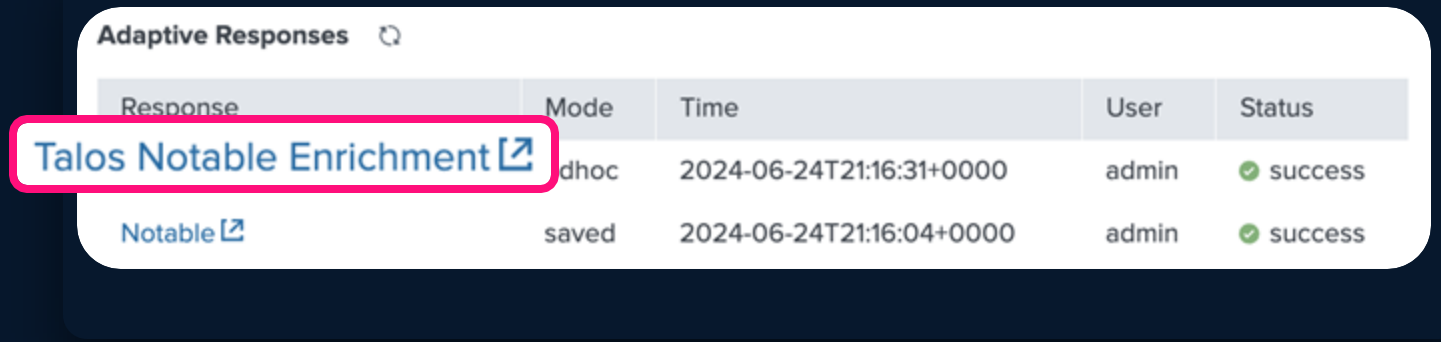
- Pulls in alerts from AI Defense and maps them to the Common Information Model (CIM), visualized in a dashboard.
- Gain visibility into risks associated with LLM models, AI apps and entities.
- Includes an out-of-the-box Enterprise Security detection that creates a search and surfaces potential attacks against the AI models running in your environment.

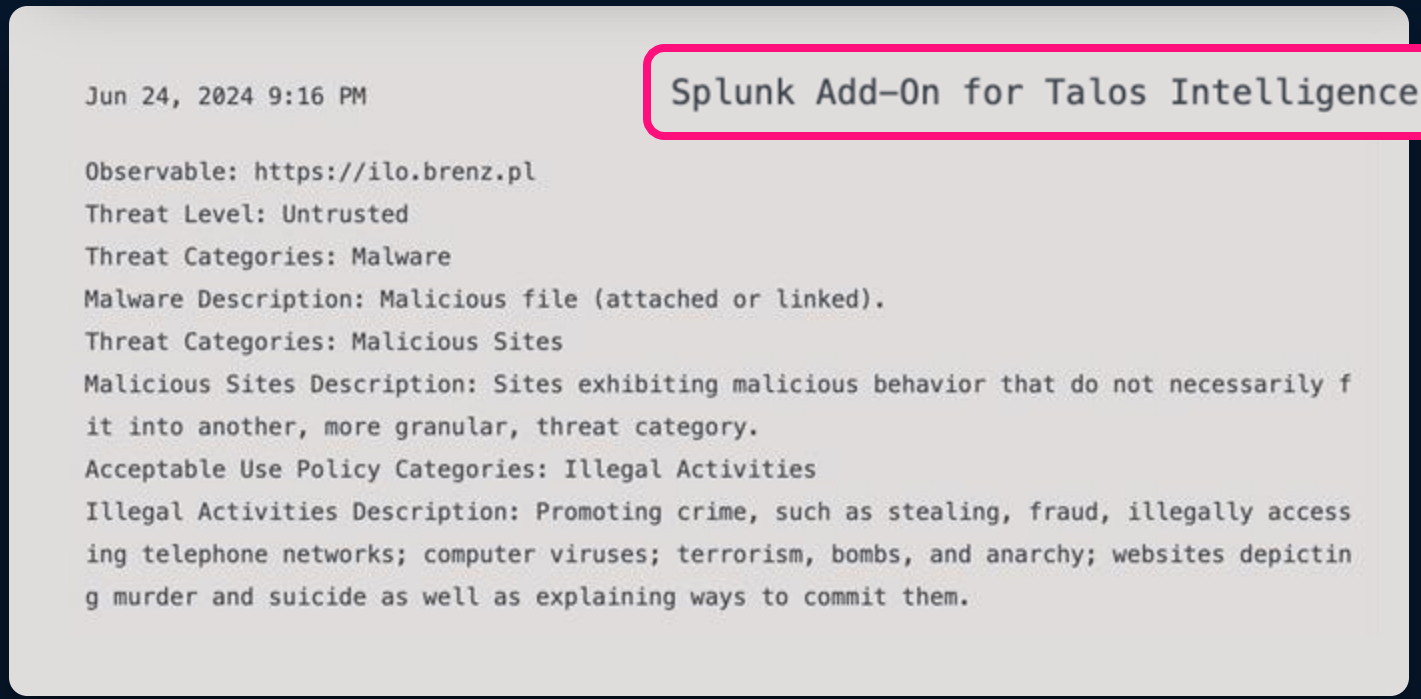


Now Available

Splunk Talos Intelligence Integration

- Out-of-the-box Enterprise Security Intel Feed
- All Splunk Enterprise Security customers have access
- Delivers automatic rich enrichment for common IOCs

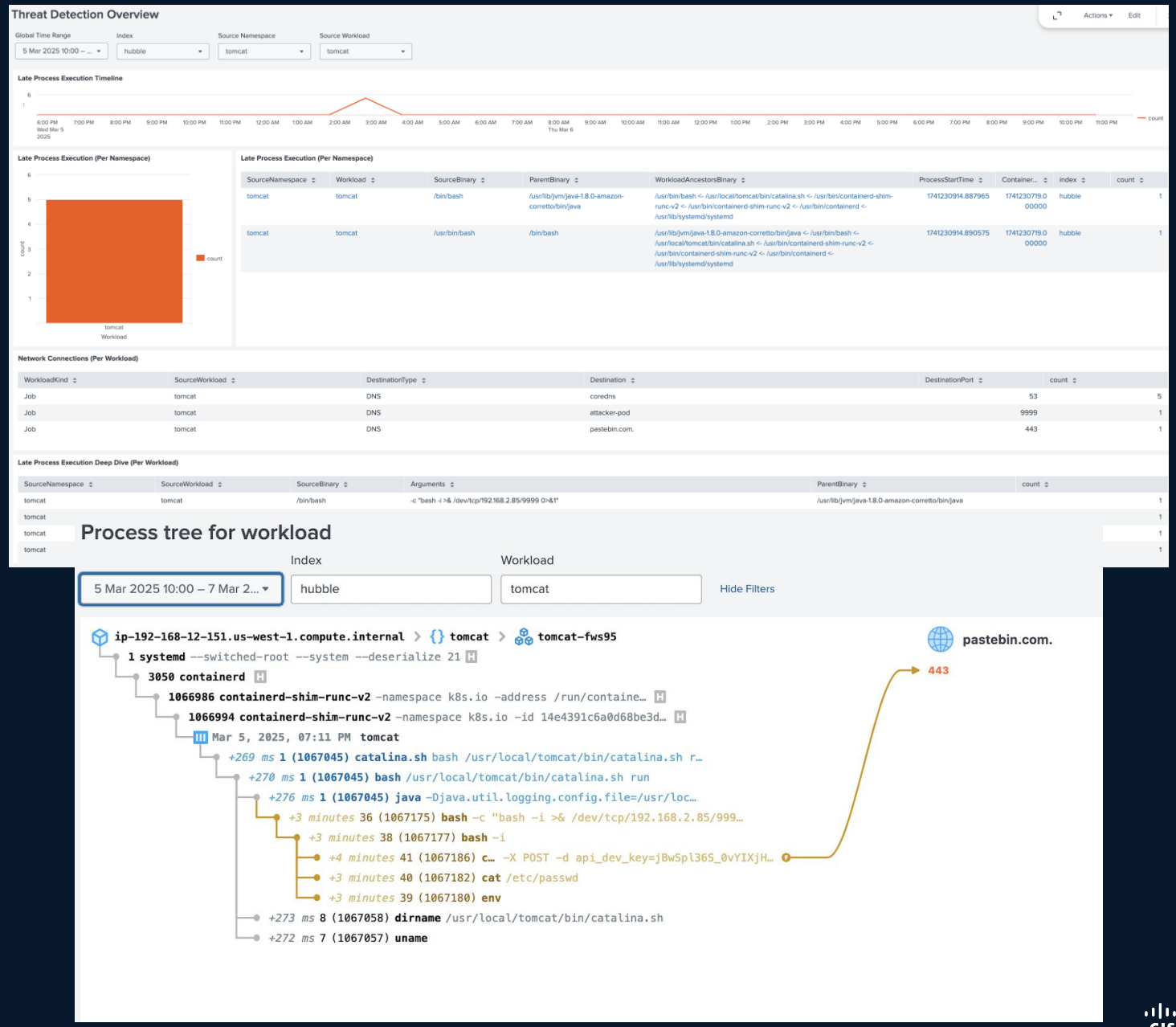




Now Available

Hypershield / Isovalent Integration

- Isovalent provides deep, kernel level runtime and network visibility into any system where the eBPF-based Tetragon agent is running on:
  - Kubernetes workloads, Linux VMs, Windows VMs
- This data supports Threat Detection and Incident Investigation Workflows via Splunk dashboards:
  - Late Process Executions
  - Shell Executions
  - Container Escapes
  - Detecting new external DNS names
- The data will be mapped to CIM Endpoint model

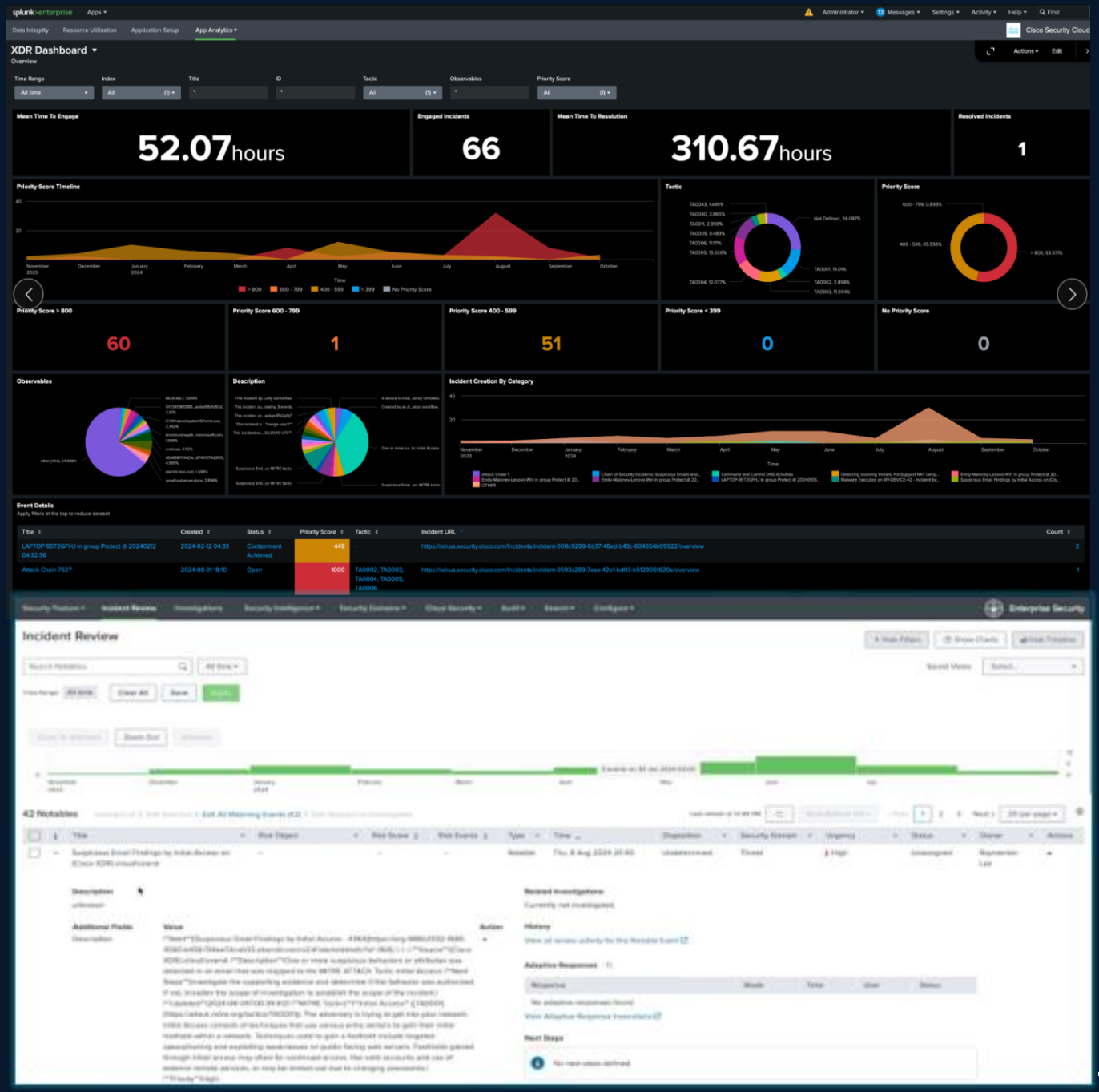


Now Available

Cisco XDR

Splunk Integration

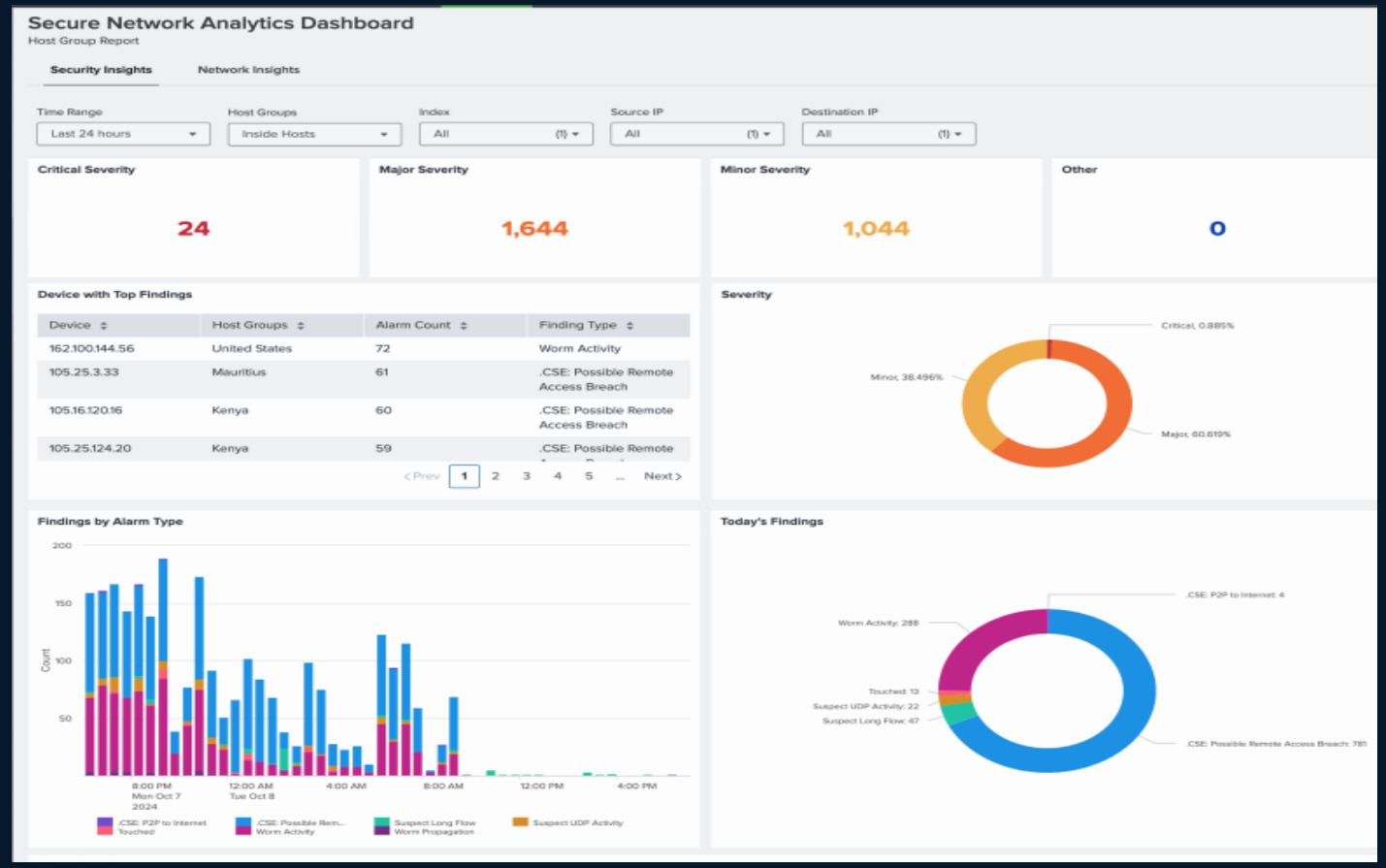
- Provides a comprehensive view of security-related threats targeting your environment across multiple security control points
- The Splunk integration ingests and maps XDR Incidents to the Alert CIM data model
- The XDR incident that is ingested contains all of the observables that were correlated together from various XDR sources
- The XDR incident can be promoted to an ES finding that will contain all of the observables and context from XDR automatically, manually or both.



Now Available

Cisco Secure Network Analytics

- Secure Network Analytics analyzes network traffic to detect threats
- The Splunk integration ingests and maps SNA events and alerts to the Alert, Network, Web CIM data model
- Ability to promote an SNA alert into an ES finding or RBA event-based criteria set by the end user on severity of alert
- Ability to filter high fidelity events in the app



Let’s Build the SOC of the Future Together

CISCO Connect

Q&A


CISCO