CISCO Connect

# Power the SOC of the Future

Michael Spivey – Leader, Solutions Engineer

Quinlan Ferris – Solutions Engineer

October 30, 2025

# Agenda

01 Introduction
02 Becoming Resilient
03 SOC Challenges
04 Splunk Security
05 SOC of the Future
06 Cisco Integrations

# Keep the organization securely up and running in the face of any disruption

## Digital resilience

### Assurance

Enable seamless end-to-end connectivity to assure the delivery of applications and services

### Observability

Prevent downtime and optimize experiences with complete visibility and insights across services

### Security operations

Gain comprehensive threat prevention, detection, investigation, and response

Google

Microsoft

Amazon

Databricks

Cisco XDR

Cisco SAL

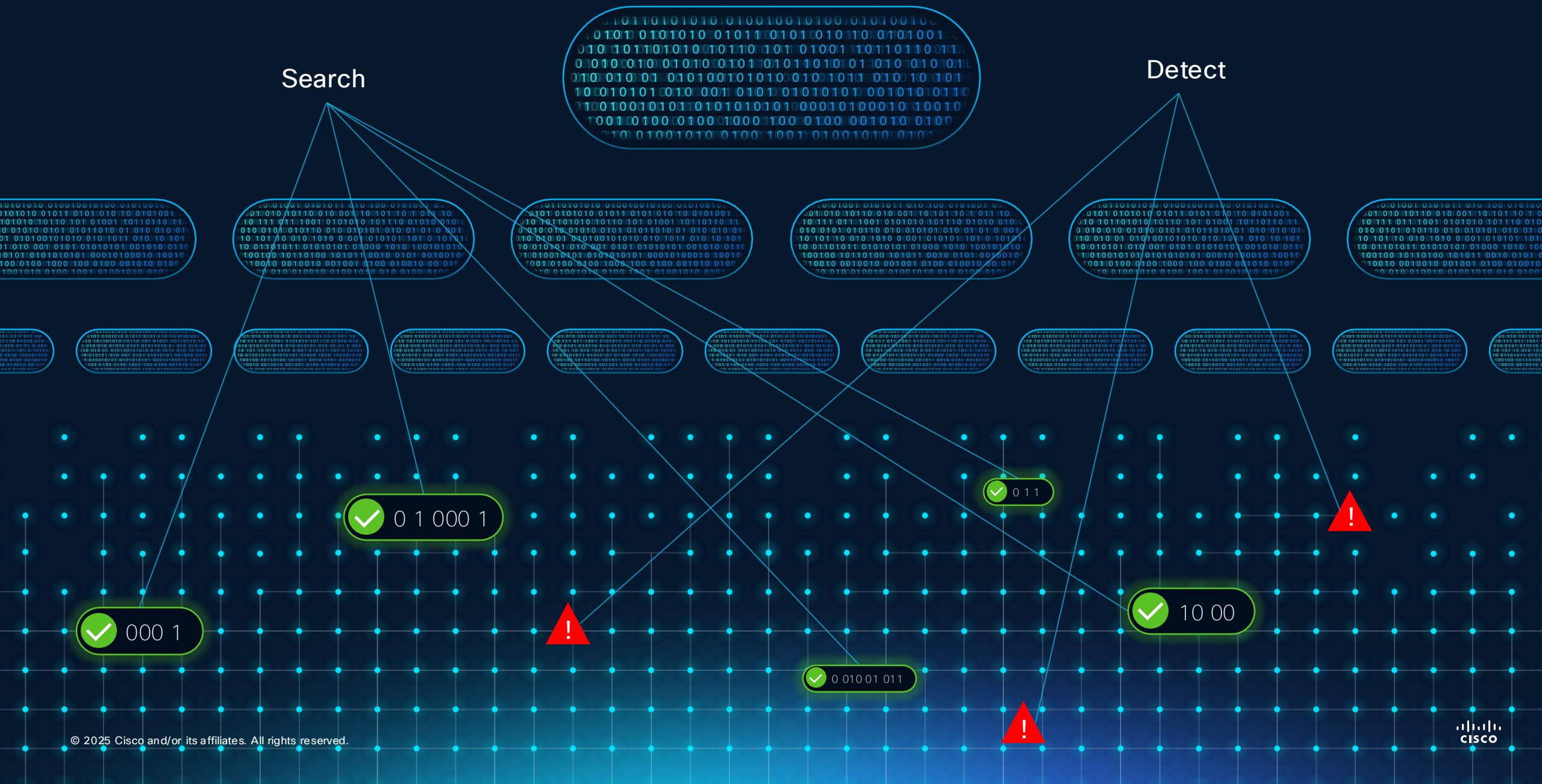
Crowdstrike

Palo Alto Networks

SentinelOne



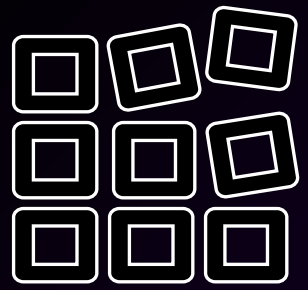
cisco



# 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

**Data management**

Filtering, Redacting & Routing

Amazon S3 | Amazon Security Lake | Additional Data Lakes

**Federation**

Search & Analytics

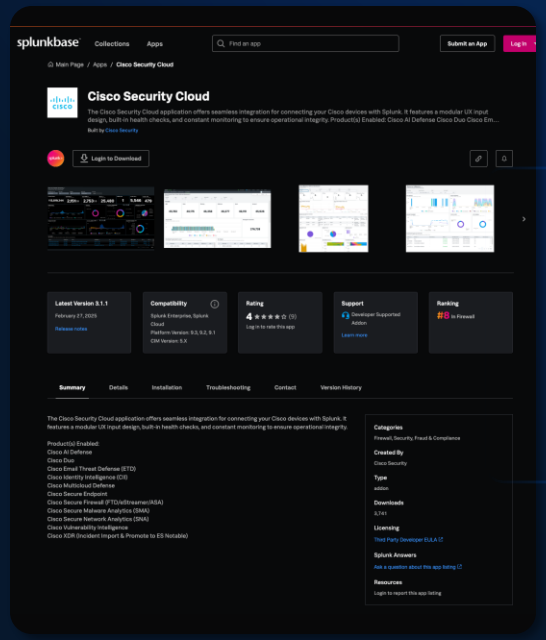
**Data normalization**

CIM, OCSF


**Splunk Enterprise Security**

# Harnessing the value of Cisco telemetry

## Cisco Security Cloud App



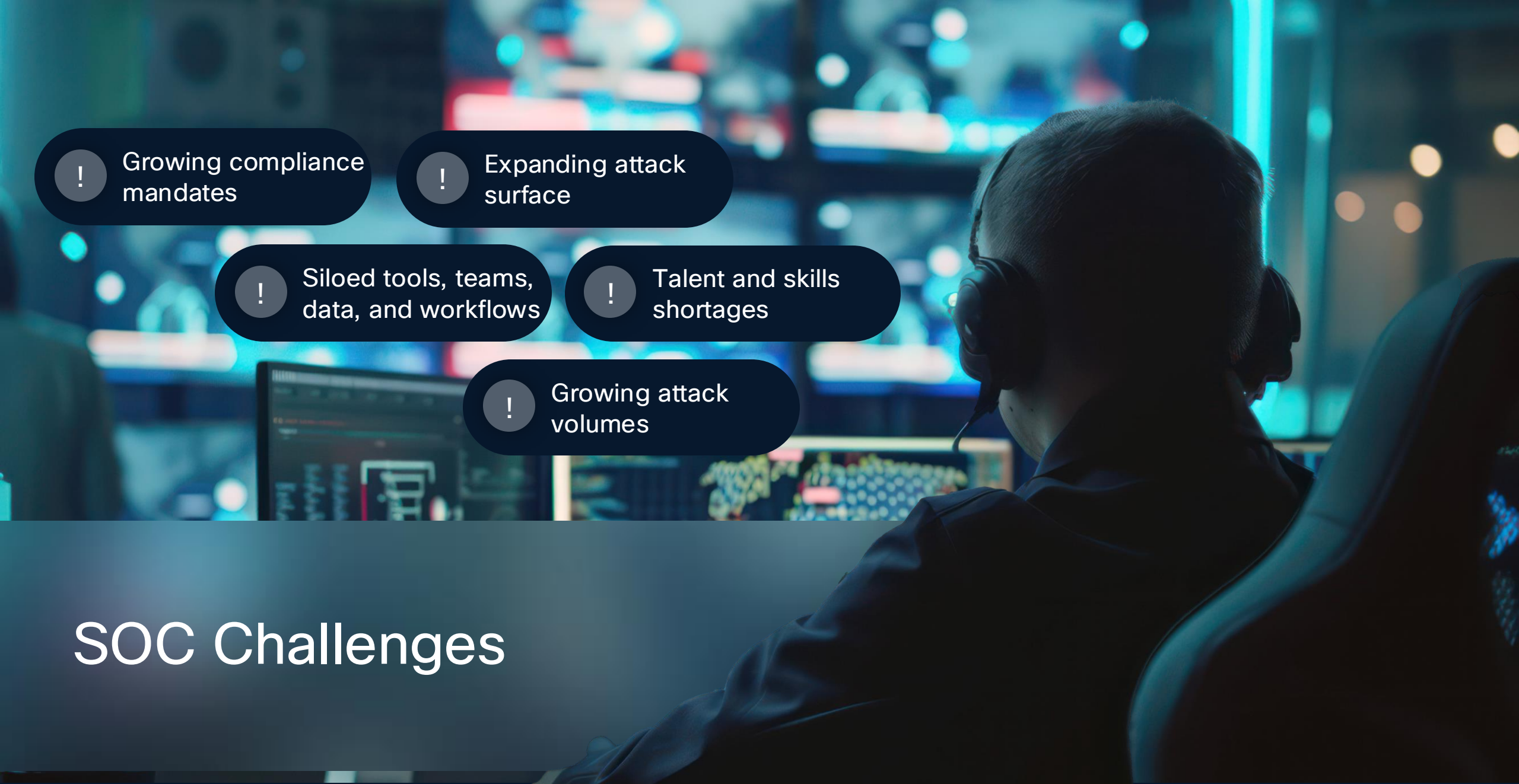

TELEMETRY
ALERTS

→ 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)




# 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

# Greater digital resilience comes from scale, speed and choice for your future proofed SOC

## Detect threats at Scale.

Gain visibility and detection at scale to reduce business risk.

## Unify Security Operations.

Unify detection, investigation and automated response for speed and efficiency.

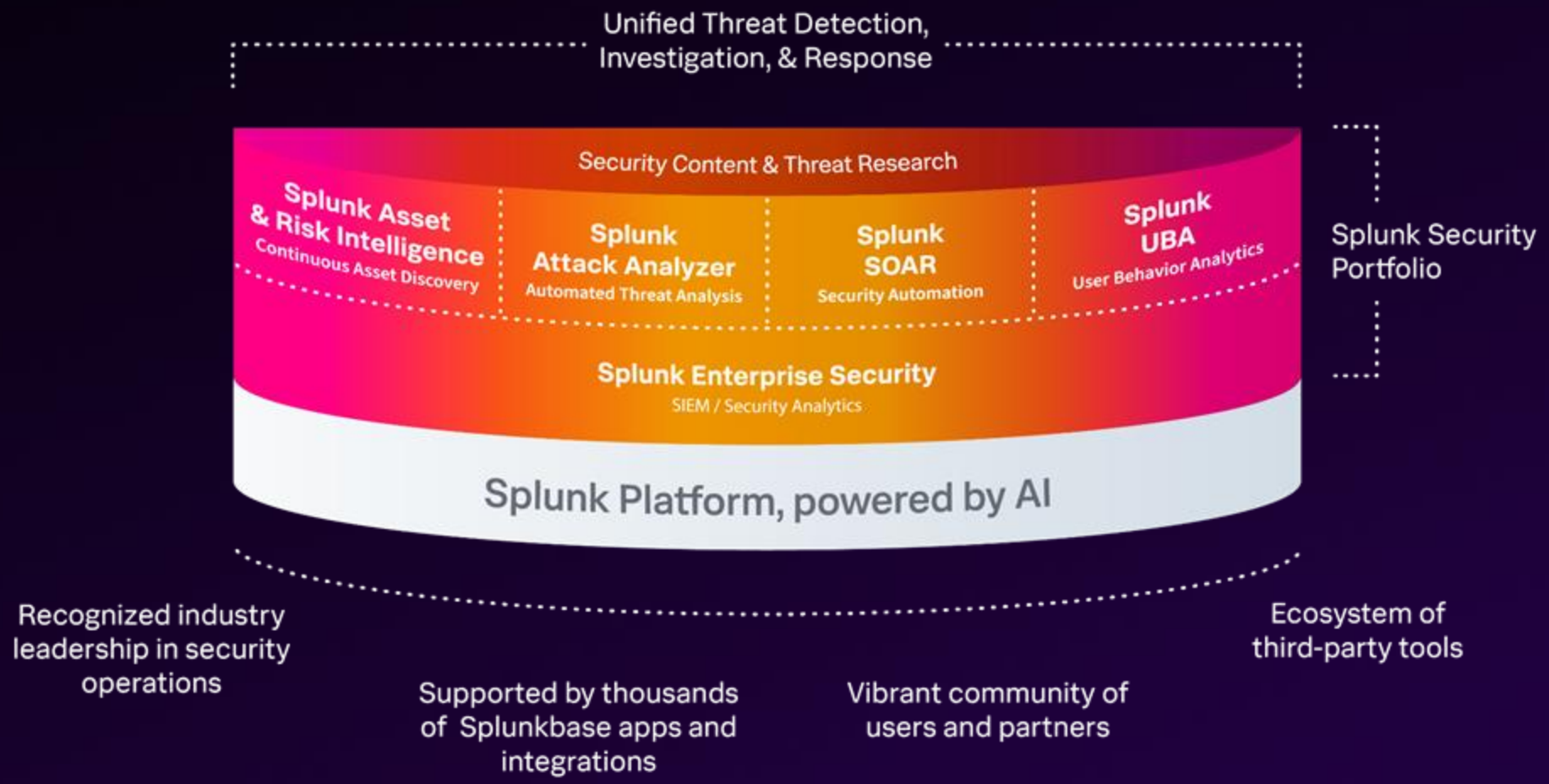
## Empower Security Innovation.

Solve any use case with a vast user community, apps, and partner ecosystem.



cisco

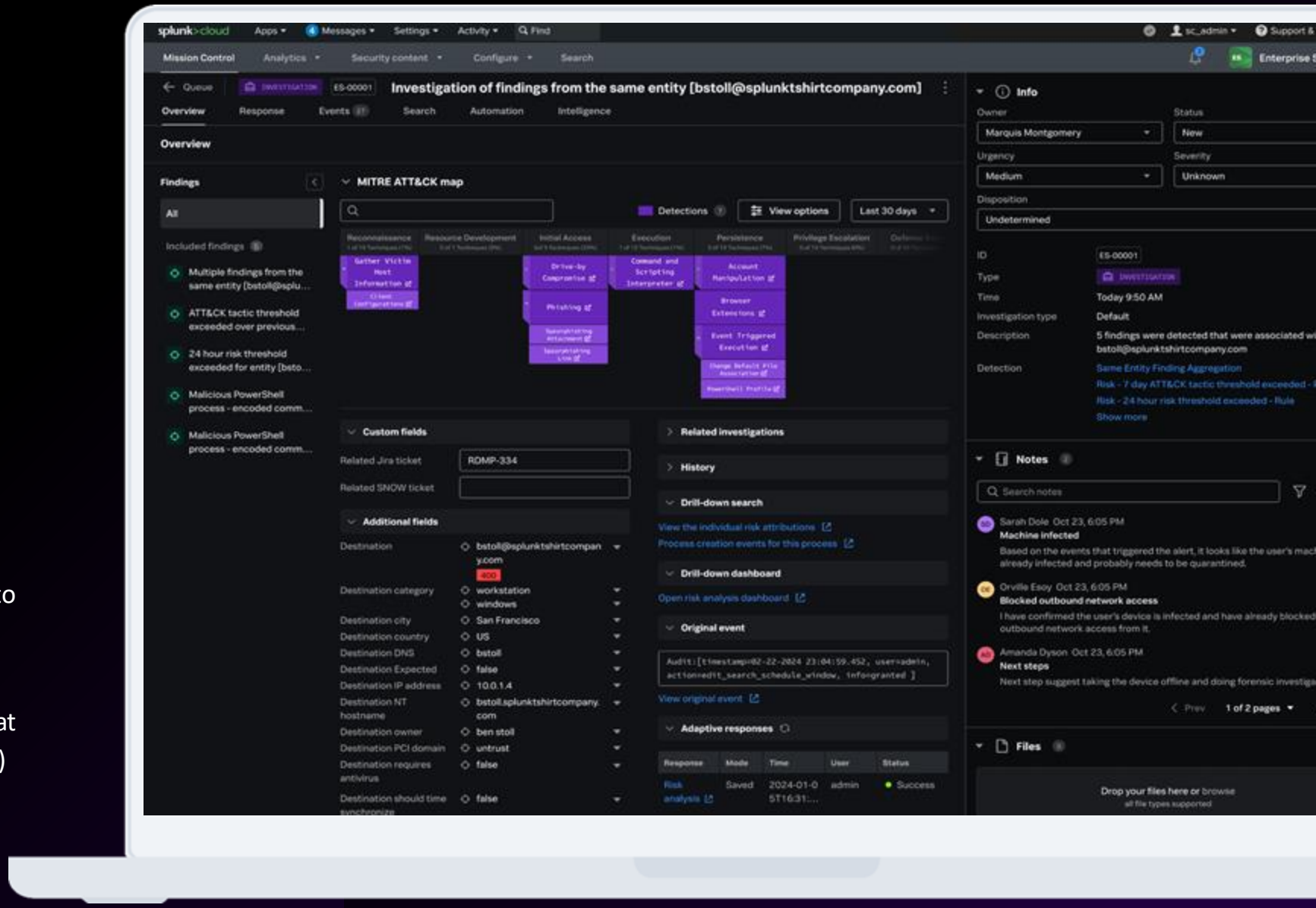
# Powering the SOC of the future with the leading TDIR solution



# 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.

New

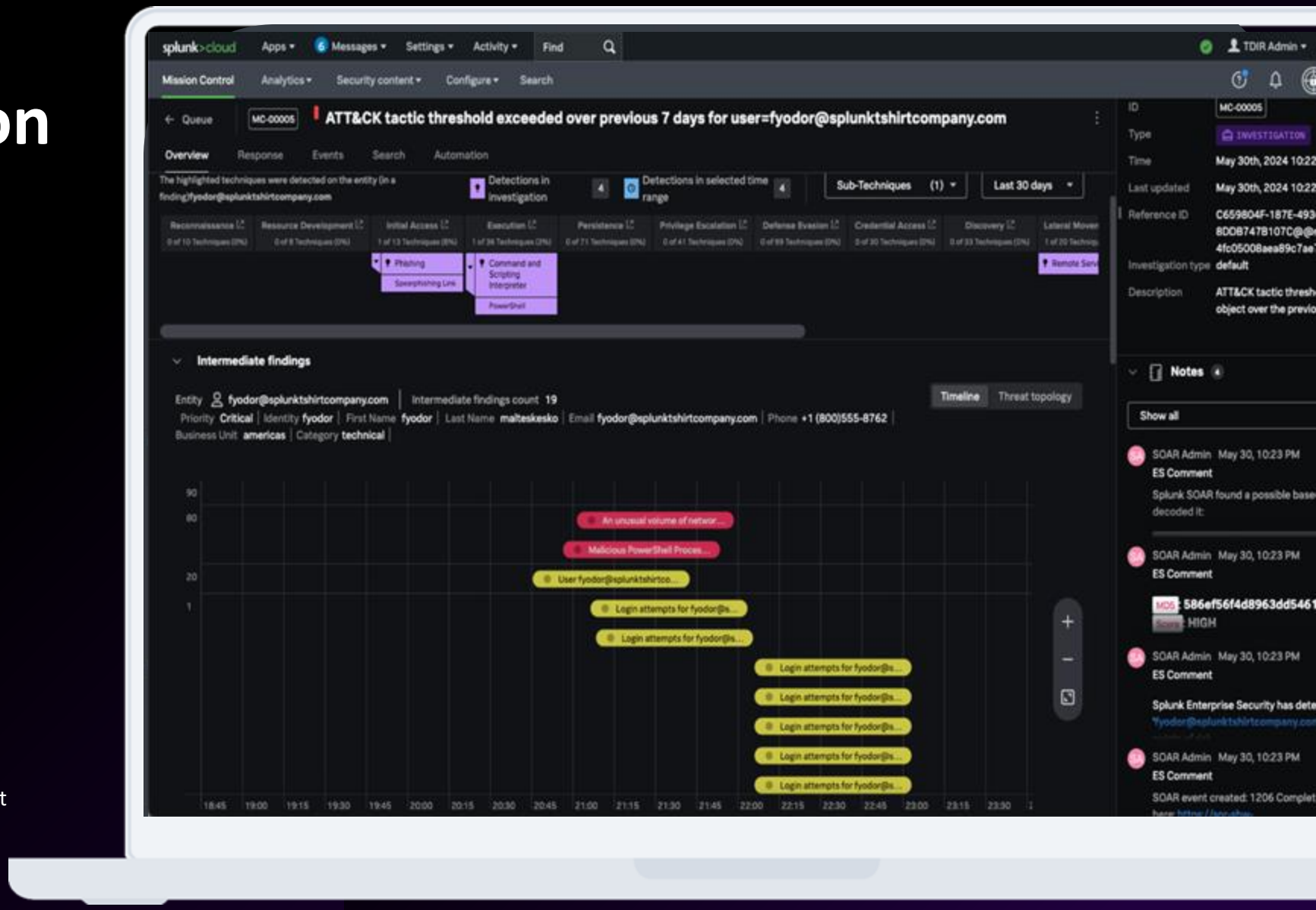
- Easily maintain up-to-date detection content with native, **automatic detection versioning.**

New

- **Enhanced detection capabilities** help analysts understand and implement a risk-based alerting detection strategy.

New

- **View all related high-fidelity findings** with a single click using **Finding Groups***, streamlining the analyst workflow



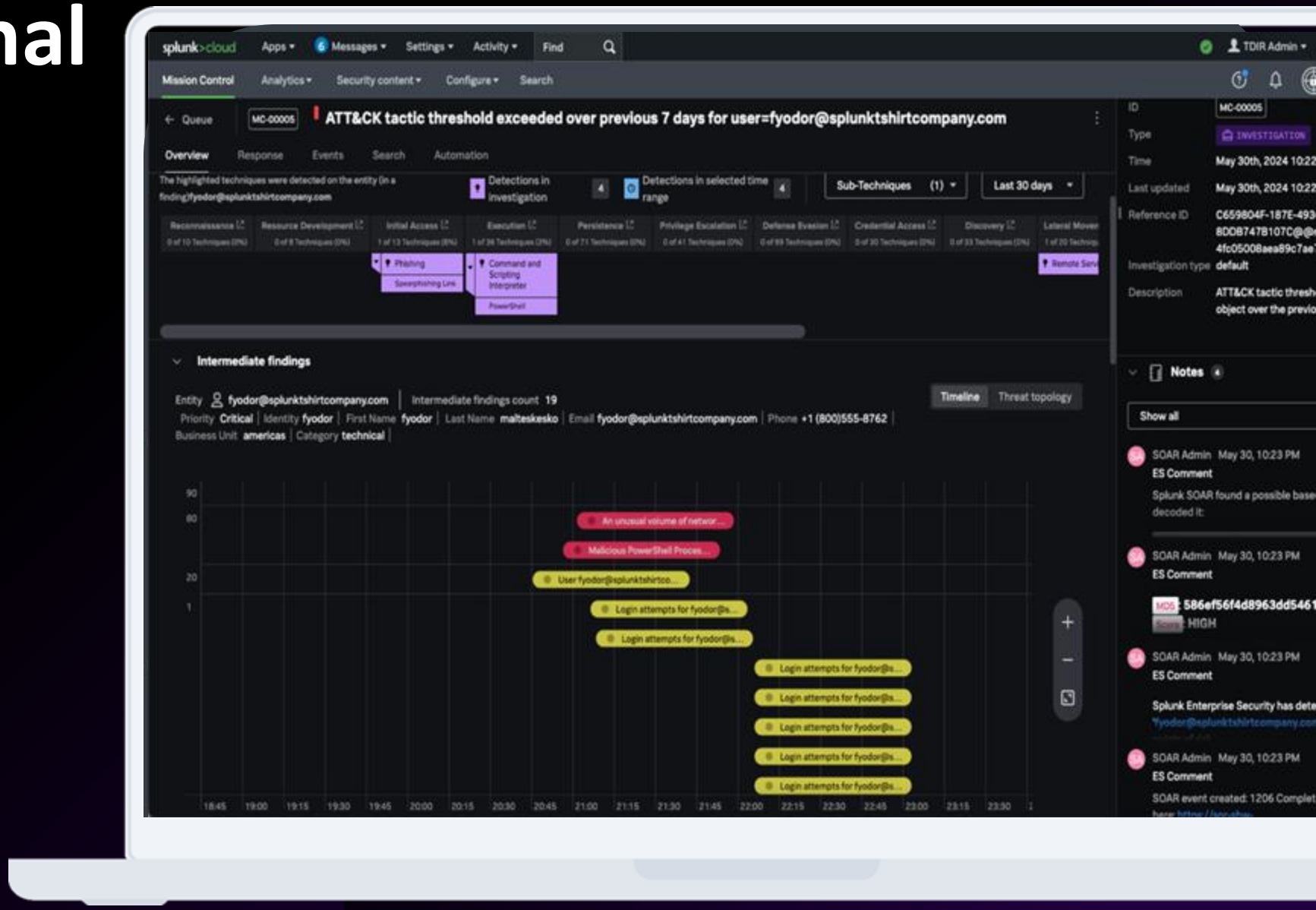
# Fuel Operational Efficiency

Unify threat detection, investigation and response (TDIR) workflows

New
- **Single, modern, unified work surface** to complete the full TDIR workflow without leaving Splunk Enterprise Security.

New
- **Native integration with Splunk SOAR*** automation playbooks and actions to optimize MTTD, MTTR and increase operational efficiency.

New
- **Execute response workflows** directly in Splunk Enterprise Security for faster, more efficient remediation.




*Splunk SOAR subscription required

# Agentic SOC of the Future

## Unified Threat Detection, Investigation & Response (TDIR)

**Cisco XDR**
Real-time Attack Detection

**Splunk Enterprise Security**
Security Analytics

**Splunk SOAR**
Security Automation

AGENTIC AI

**Splunk Platform**
Data Management and Federation

CONTENT AND THREAT RESEARCH

**Cisco Security Cloud**


Identity


Firewall


Talos


SSE


& more


Third-party tools


Clouds


Endpoints


Data centers


Applications



cisco

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

# Splunk Recognized as a Leader

2025 Gartner® Magic Quadrant™ for Security Information and Event Management (SIEM)

## Splunk named **a Leader** for the **11th consecutive time**

# Cisco Integrations – A Deeper Dive

# 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

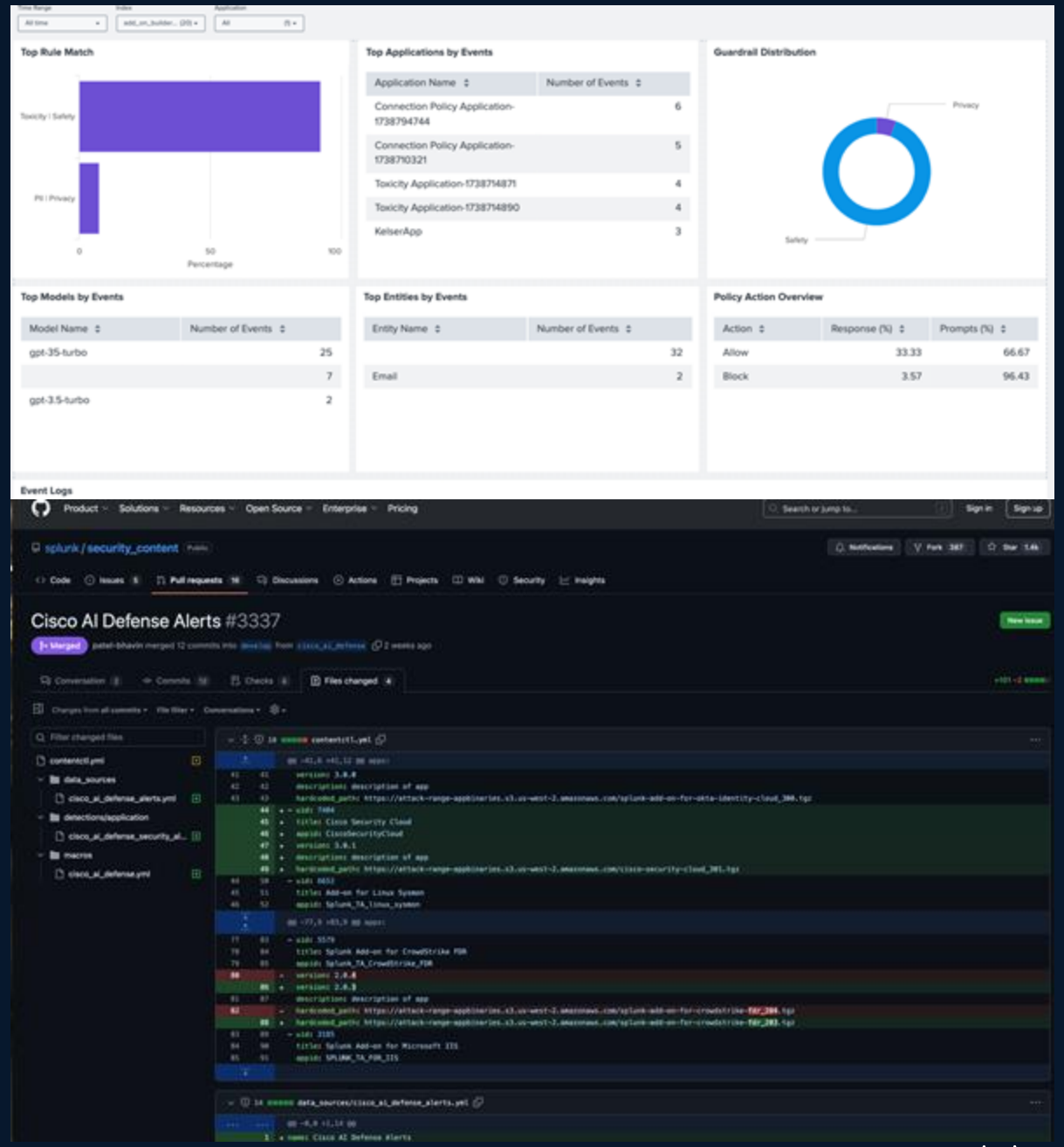
*Splunk +*
*Cisco AI Defense*

Now Available

# Cisco AI Defense

## Gain visibility into emerging AI risks with Splunk

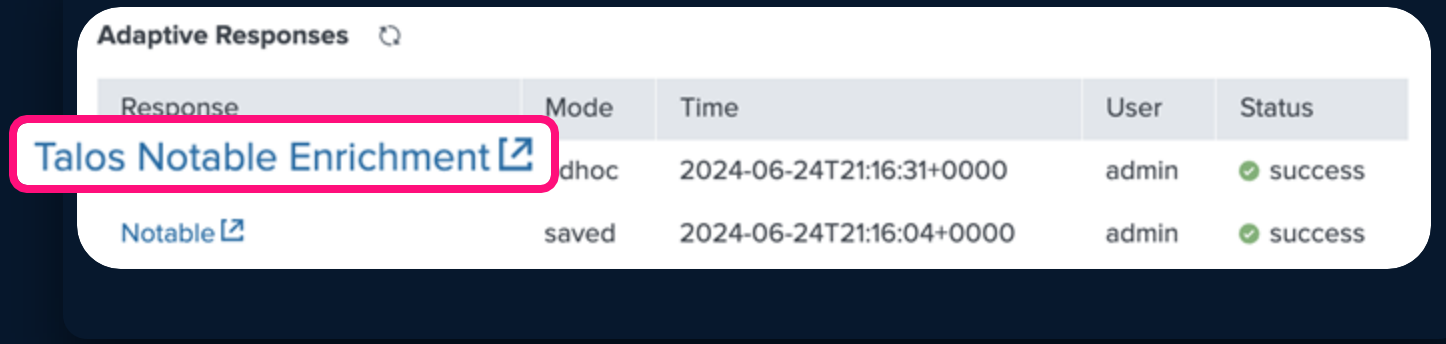
- Pulls in alerts from AI Defense and maps them to the Common Information Model (CIM), visualized in a dashboard.
- Gain visibility into risks associated with LLM models, AI apps and entities.
- Includes an out-of-the-box Enterprise Security detection that creates a search and surfaces potential attacks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

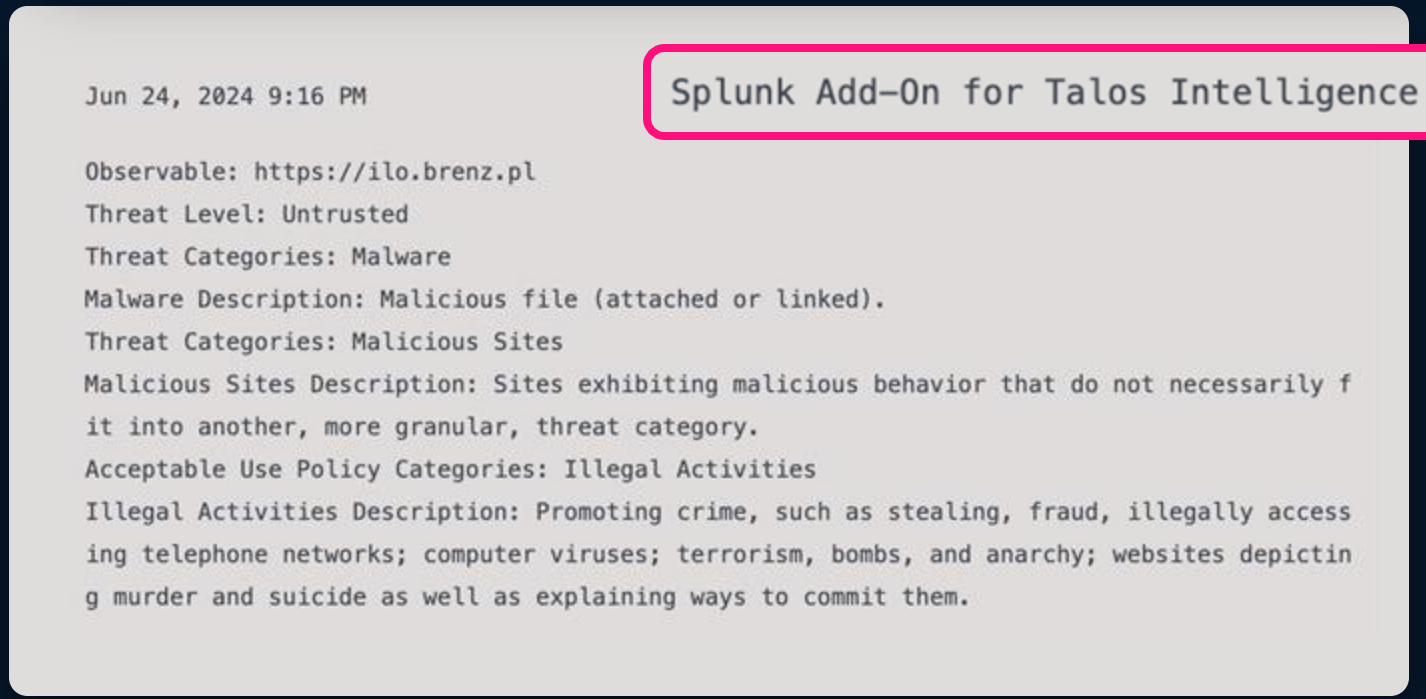


Now Available

# Splunk Add-on for Talos Intelligence

- Out-of-the-box adaptive response action
- All Splunk Enterprise Security customers have access
- Delivers rich enrichment for common IOCs

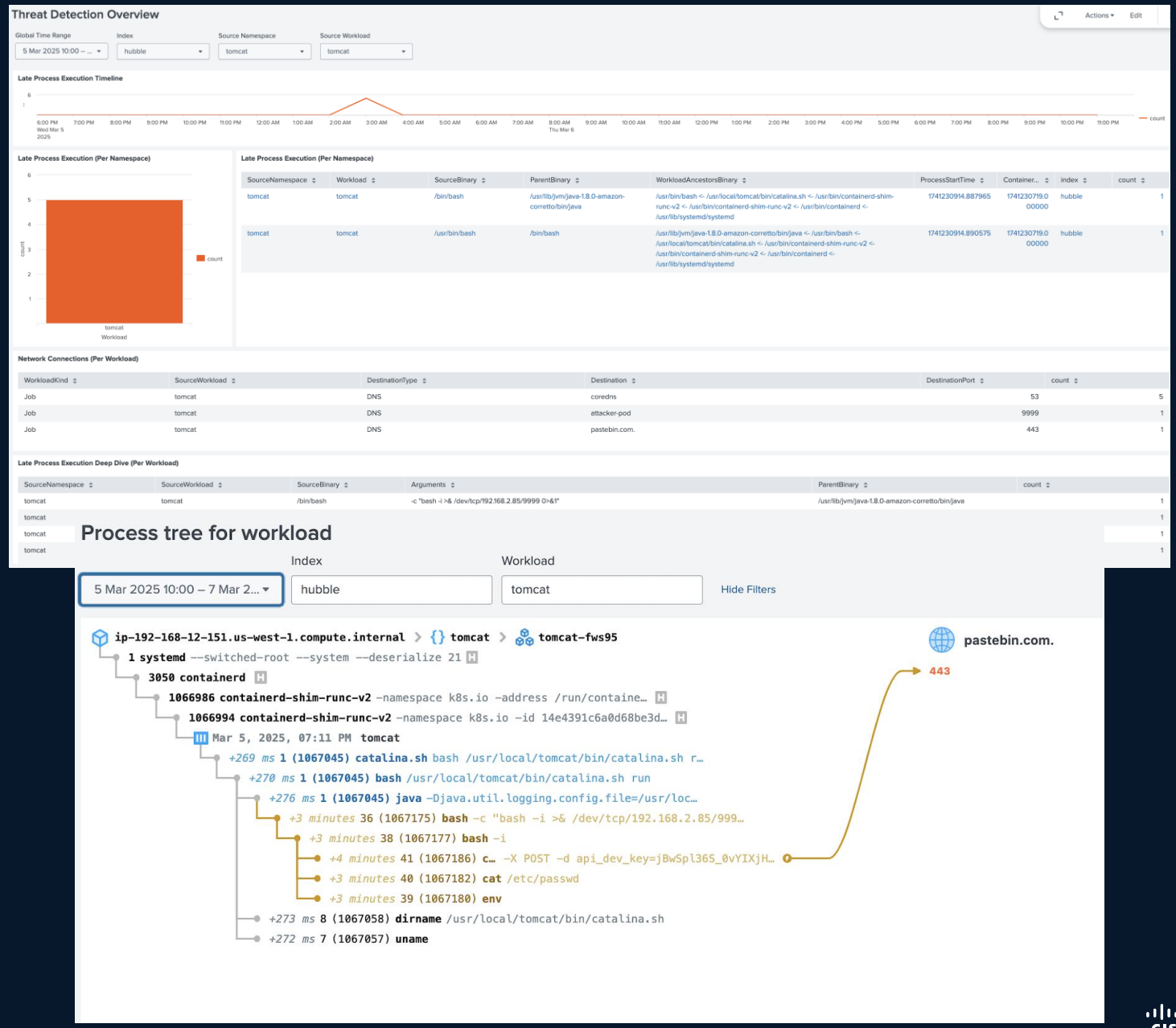


Coming Soon

# 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

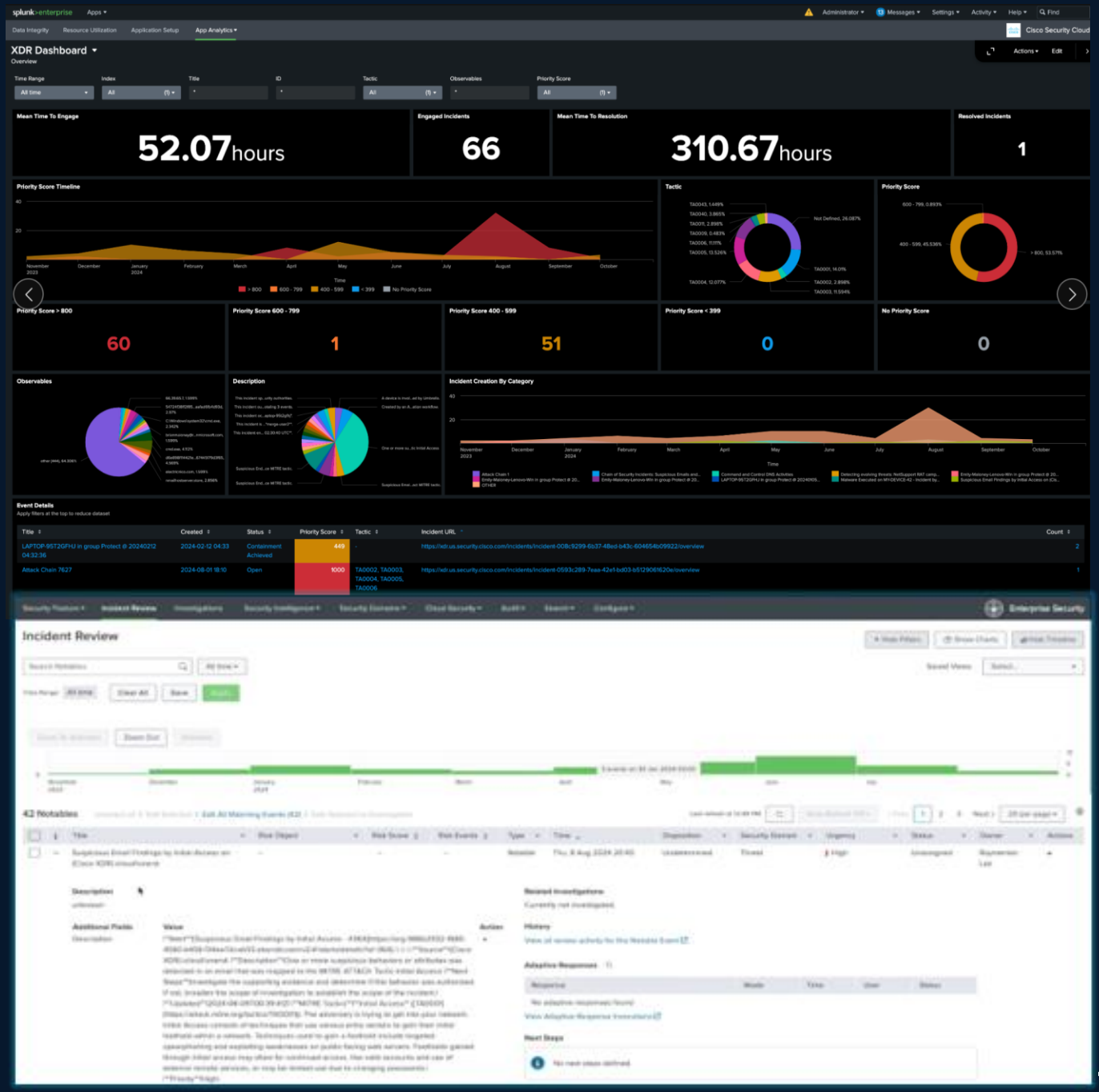


Now Available

# Cisco XDR

## Splunk Integration

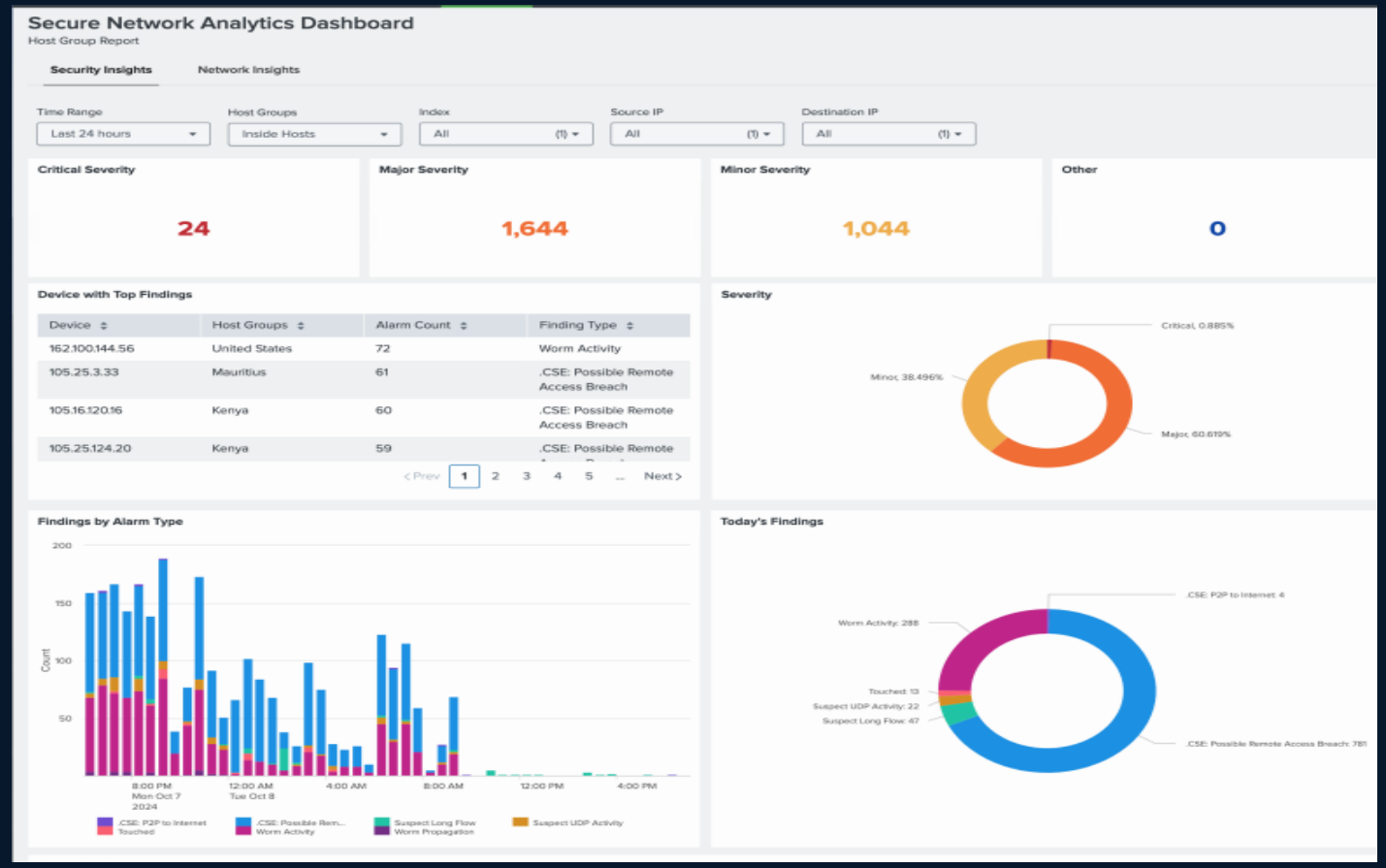
- Provides a comprehensive view of security-related threats targeting your environment across multiple security control points
- The Splunk integration ingests and maps XDR Incidents to the Alert CIM data model
- The XDR incident that is ingested contains all of the observables that were correlated together 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