From Theory to Practice: Real-World AI/ML Adoption with Splunk for Security Operations

Digital Resilience

David Gamer
Principal Global Product Specialist

CISCO Live !

Session ID: BRKSEC-2545

Agenda

01 Introduction
02 Splunk AI
03 AI Assistant in ES
04 Demo
05 Cisco Cloud Security App
06 Cisco AI Defense
07 Splunk's Data Power
08 Machine Learning
08 Can You SPL?

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

Cisco Webex App

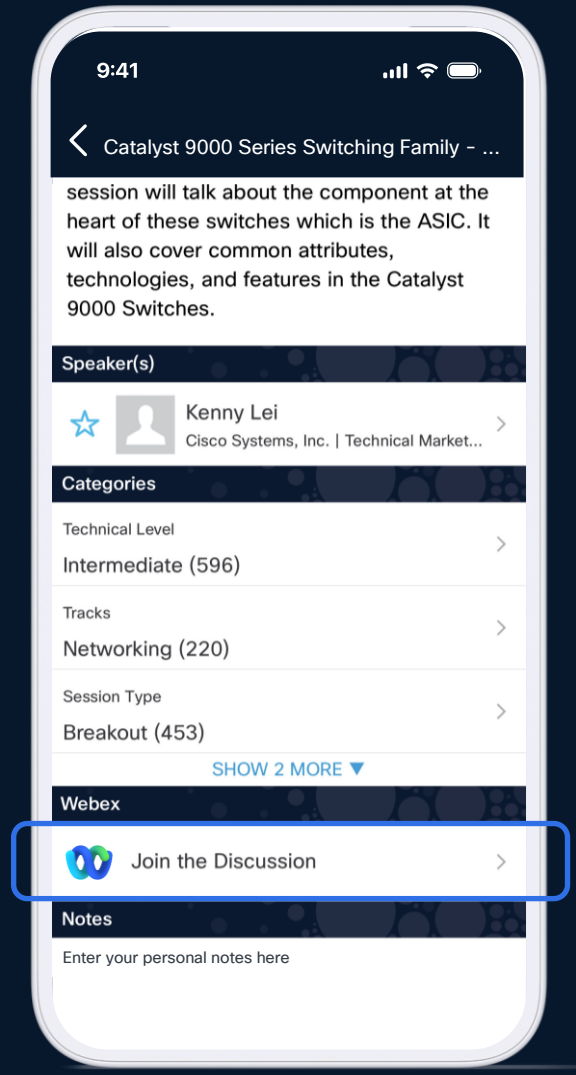
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

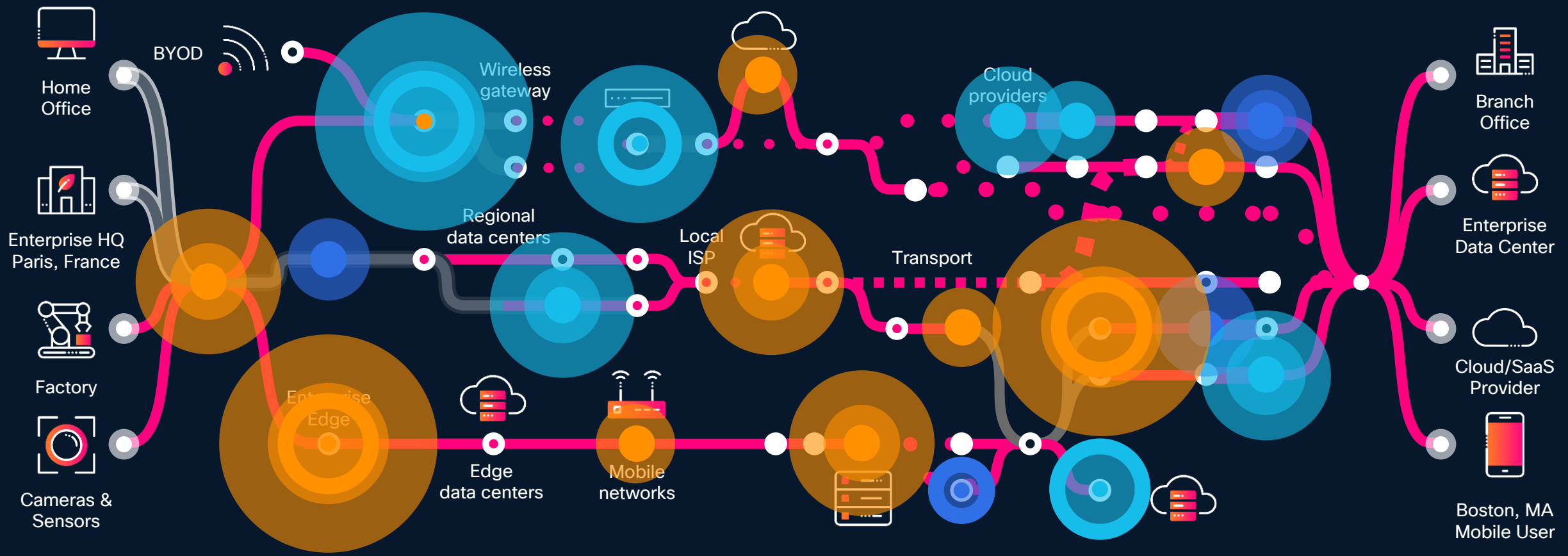
Webex spaces will be moderated by the speaker until 14 November 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKSEC-2543**

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

Complexity explosion is getting worse



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

AI will lift up defenders

Human-in-the Loop

Domain-specific

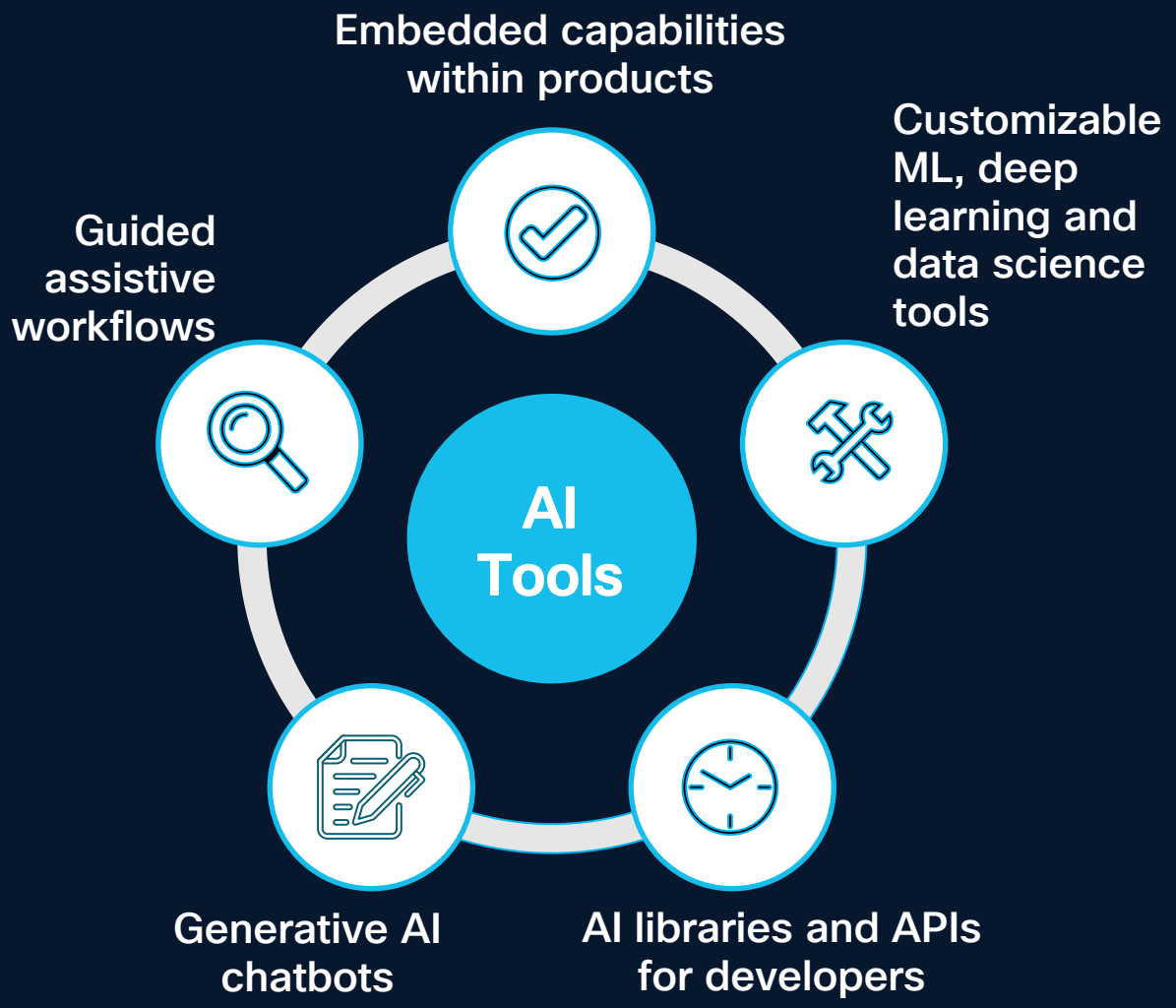
Open and Extensible

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

We must unlock the value of machine data to fuel AI

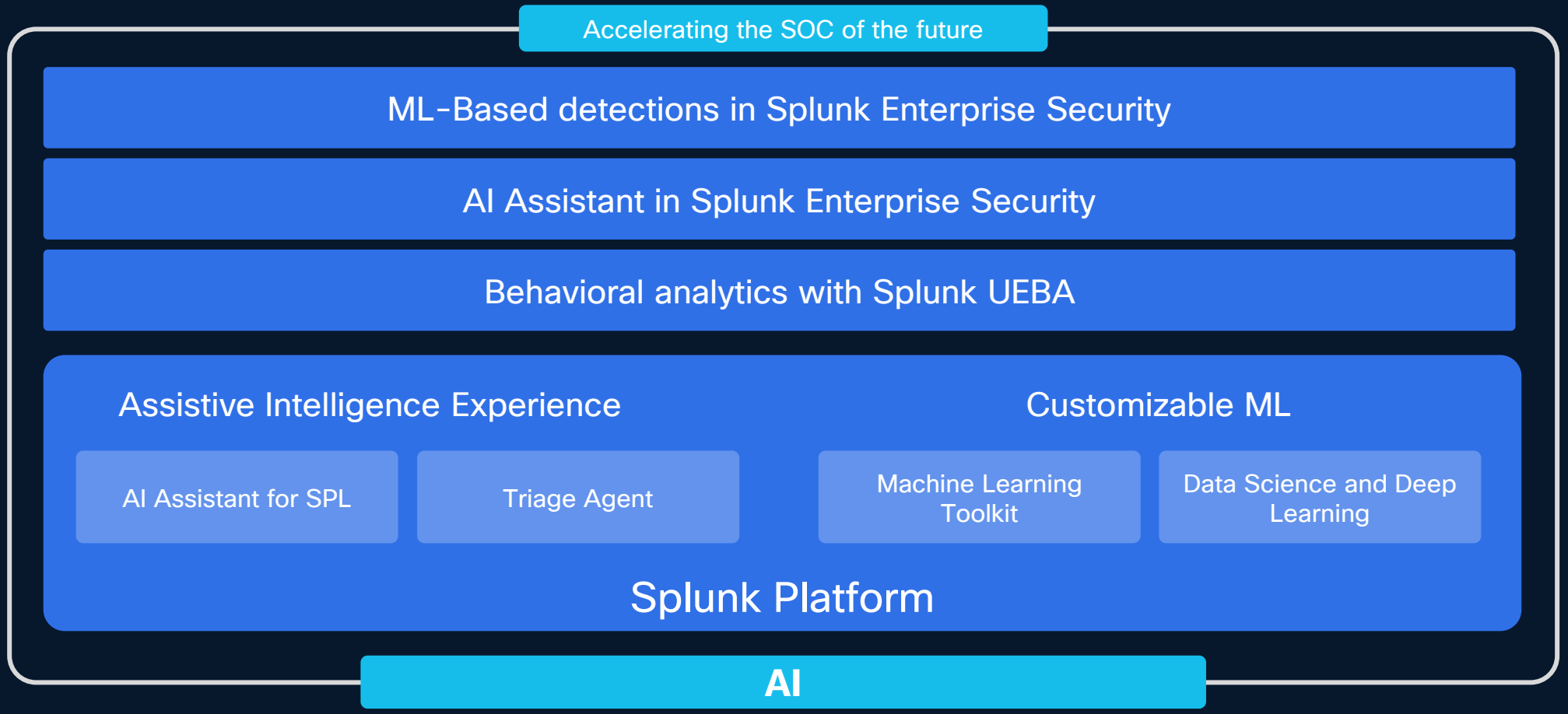
© 2025 Cisco and/or its affiliates. All rights reserved.

Splunk's AI Superpower is Data



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

Driving a new wave of maturity for the SOC Powered by Splunk's Platform



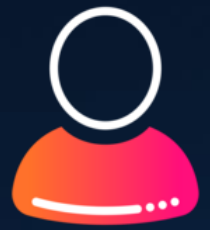
© 2025 Cisco and/or its affiliates. All rights reserved.

Threat Detection,
Investigation and Response

The SOC Operation

Initial Triage

Incident Response



Advanced Response

Engineering

Management

TDIR Platform

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

Human-in-the Loop

Simplify and distill the analyst experience.

AI to maximize the human.

Domain-specific

AI to accomplish a specific security goal.

No AI for the sake of AI.

Open and Extensible

AI that is understandable and specific for each environment.

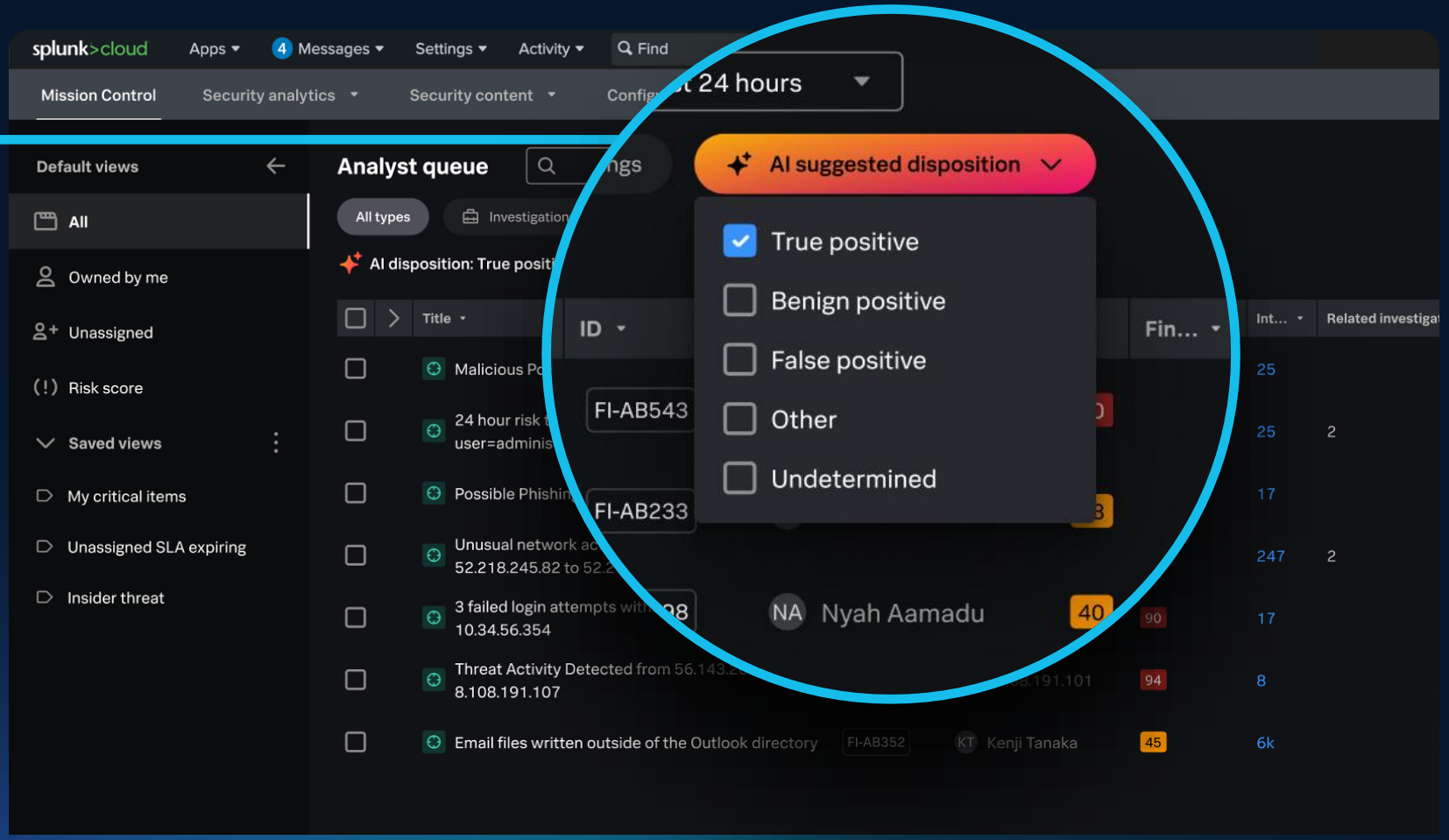
No closed boxes.

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

Alpha | Jan ‘26

Triage Agent

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

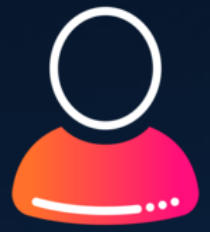


© 2025 Cisco and/or its affiliates. All rights reserved.

The SOC Operation

Initial Triage

Incident Response



Advanced Response

Engineering

Management

Triage Agent

TDIR Platform

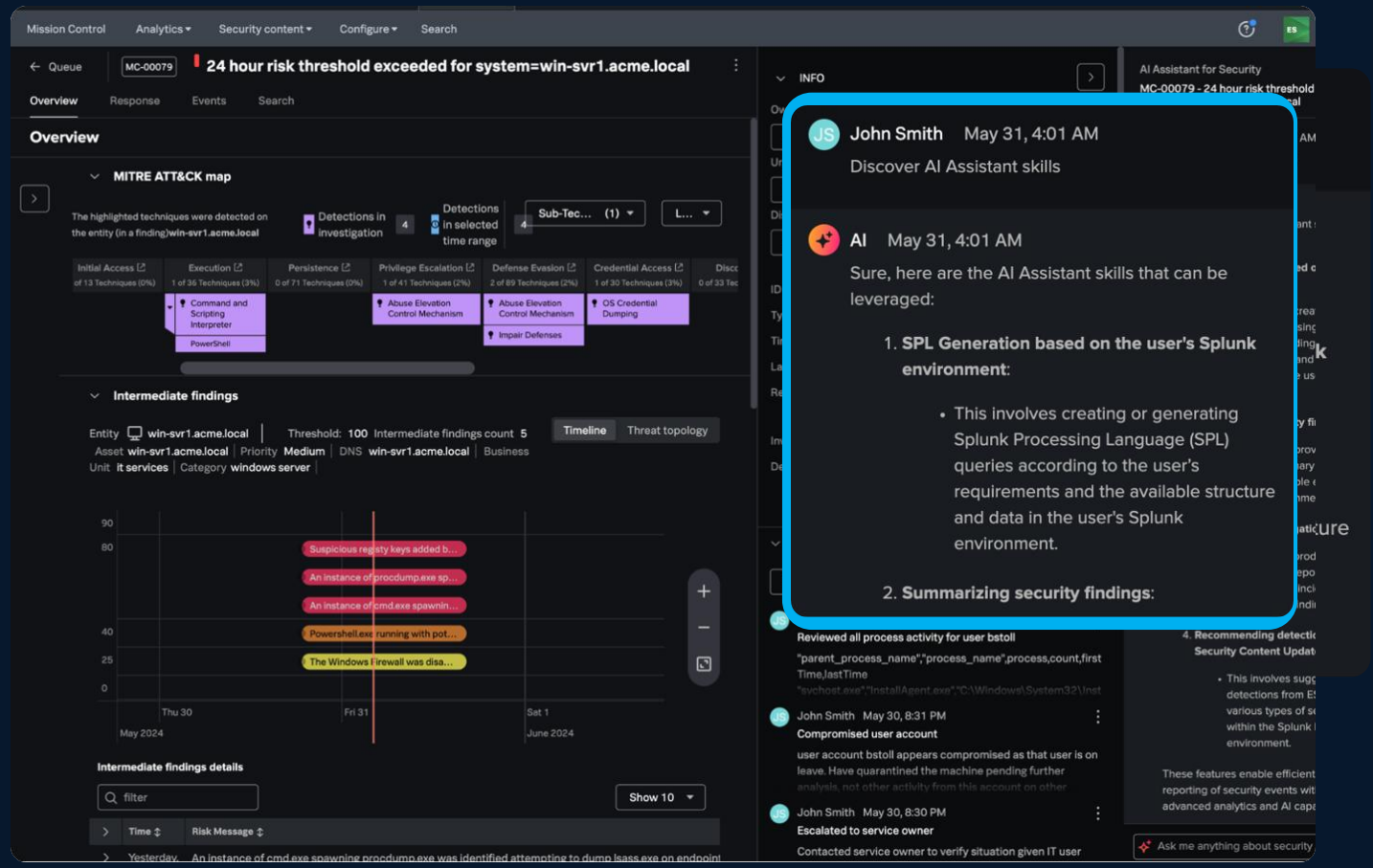
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

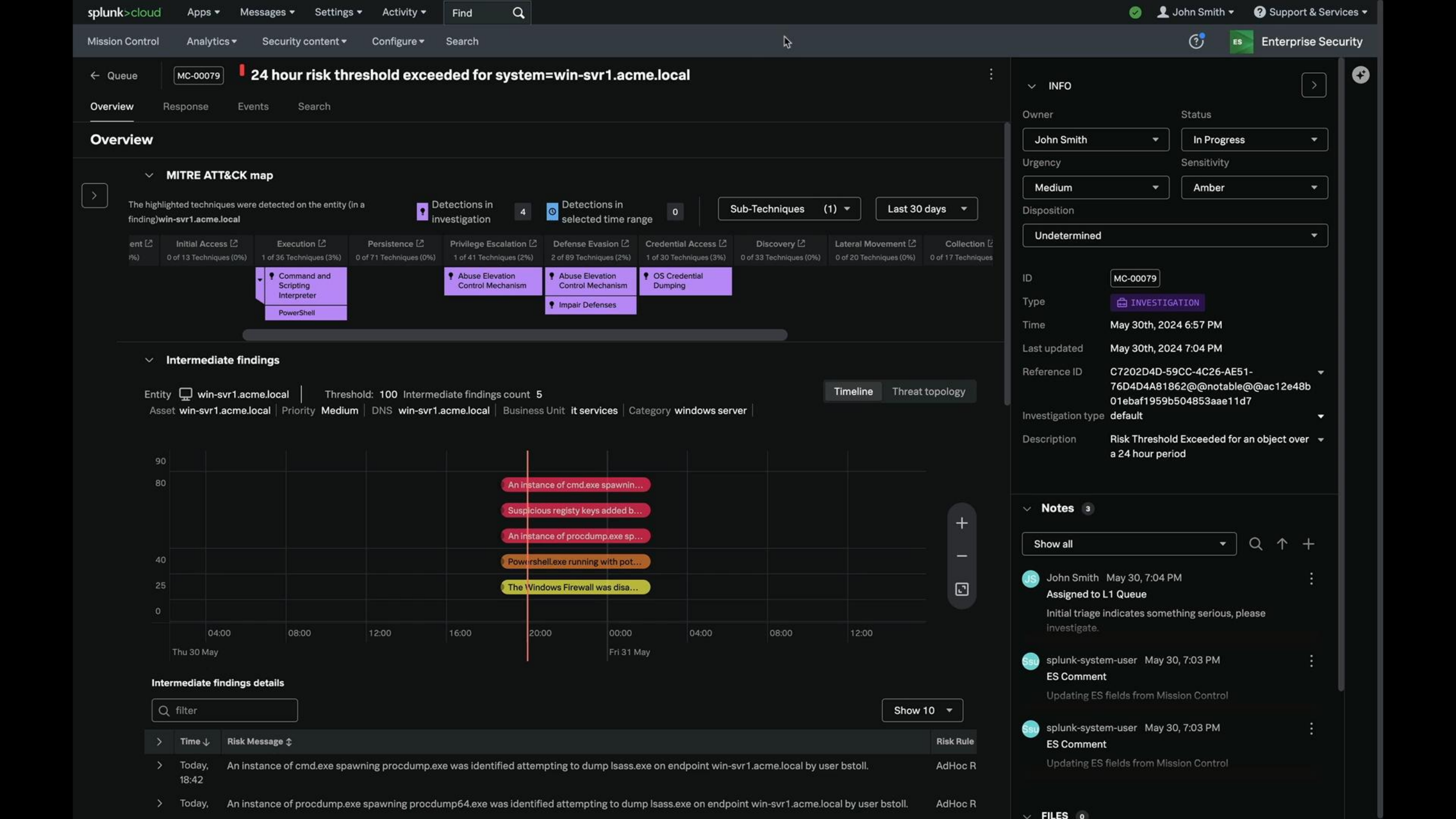
AI Assistant in Enterprise Security

Guided security workflows

- Answer analyst questions to guide investigations
- Save time by addressing threats more rapidly
- Use natural language queries to get answers during investigations



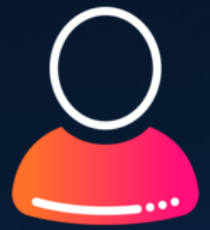
© 2025 Cisco and/or its affiliates. All rights reserved.


splunk>cloud
Apps
Messages
Settings
Activity
Find
John Smith
Support & Services
Mission Control
Analytics
Security content
Configure
Search
Enterprise Security
Queue
MC-00079
24 hour risk threshold exceeded for system=win-svr1.acme.local
Overview
Response
Events
Search
Overview
MITRE ATT&CK map
The highlighted techniques were detected on the entity (in a finding)win-svr1.acme.local
Detections in investigation 4
Detections in selected time range 0
Sub-Techniques (1)
Last 30 days
Initial Access
0 of 13 Techniques (0%)
Execution
1 of 36 Techniques (3%)
Persistence
0 of 71 Techniques (0%)
Privilege Escalation
1 of 41 Techniques (2%)
Defense Evasion
2 of 89 Techniques (2%)
Credential Access
1 of 30 Techniques (3%)
Discovery
0 of 33 Techniques (0%)
Lateral Movement
0 of 20 Techniques (0%)
Collection
0 of 17 Techniques
Command and Scripting Interpreter
PowerShell
Abuse Elevation Control Mechanism
Abuse Elevation Control Mechanism
Impair Defenses
OS Credential Dumping
Intermediate findings
Entity win-svr1.acme.local
Threshold: 100 Intermediate findings count 5
Asset win-svr1.acme.local | Priority Medium | DNS win-svr1.acme.local | Business Unit it services | Category windows server
Timeline
Threat topology
90
80
40
25
0
An instance of cmd.exe spawnin…
Suspicious registy keys added b…
An instance of procdump.exe sp…
Powershell.exe running with pot…
The Windows Firewall was disa…
04:00
08:00
12:00
16:00
20:00
00:00
04:00
08:00
12:00
Thu 30 May
Fri 31 May
Intermediate findings details
filter
Show 10
Time
Risk Message
Risk Rule
Today, 18:42
An instance of cmd.exe spawning procdump.exe was identified attempting to dump lsass.exe on endpoint win-svr1.acme.local by user bstoll.
AdHoc R
Today,
An instance of procdump.exe spawning procdump64.exe was identified attempting to dump lsass.exe on endpoint win-svr1.acme.local by user bstoll.
AdHoc R
INFO
Owner
John Smith
Status
In Progress
Urgency
Medium
Sensitivity
Amber
Disposition
Undetermined
ID
MC-00079
Type
INVESTIGATION
Time
May 30th, 2024 6:57 PM
Last updated
May 30th, 2024 7:04 PM
Reference ID
C7202D4D-59CC-4C26-AE51-76D4D4A81862@@notable@@ac12e48b01ebaf1959b504853aae11d7
Investigation type
default
Description
Risk Threshold Exceeded for an object over a 24 hour period
Notes 3
Show all
John Smith May 30, 7:04 PM
Assigned to L1 Queue
Initial triage indicates something serious, please investigate.
splunk-system-user May 30, 7:03 PM
ES Comment
Updating ES fields from Mission Control
splunk-system-user May 30, 7:03 PM
ES Comment
Updating ES fields from Mission Control
FILES

The SOC Operation

Initial Triage

Incident Response



Advanced Response

Engineering

Management

Triage Agent

AI Assistant in Enterprise Security

TDIR Platform

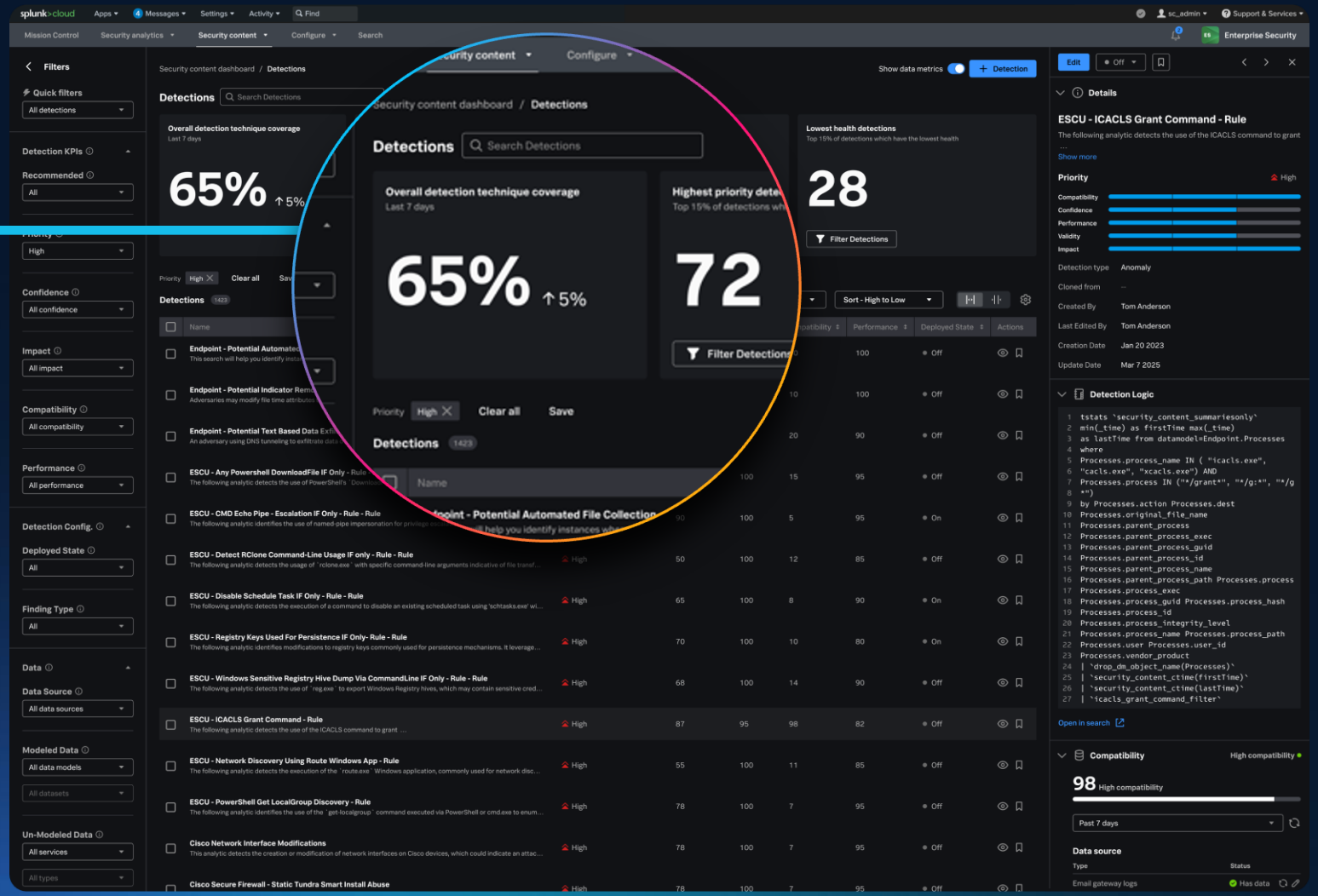
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Detection Studio

Powered by SnapAttack

- AI Guided Detection Creation
- Detection Health, Coverage and Effectiveness Visibility
- Detection-as-code lifecycle management

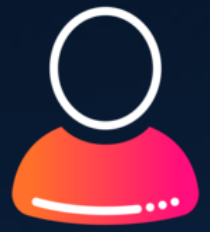


© 2025 Cisco and/or its affiliates. All rights reserved.

The SOC Operation

Initial Triage

Incident Response



Advanced Response

Engineering

Management

Triage Agent

AI Assistant in Enterprise Security

Detection Studio

TDIR Platform

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

cisco

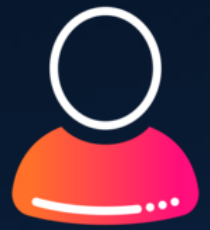
Threat Detection,
Investigation and Response

CISCO Live !

The SOC Platform

Initial Triage

Incident Response



Advanced Response

Engineering

Management

Triage Agent

AI Assistant in Enterprise Security

Detection Studio

TDIR Platform

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

cisco

The SOC Platform

Operations

Detection

Triage Agent

AI Assistant in Enterprise Security

Detection Studio

TDIR Platform

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

Focused investments

Accelerate detection, investigation and response

Rapid cybersecurity investigations and contextualization

Find the signal to improve user productivity and outcomes.

Finding Signals (detect threats)

Find the signal from the noise in vast amounts of data.

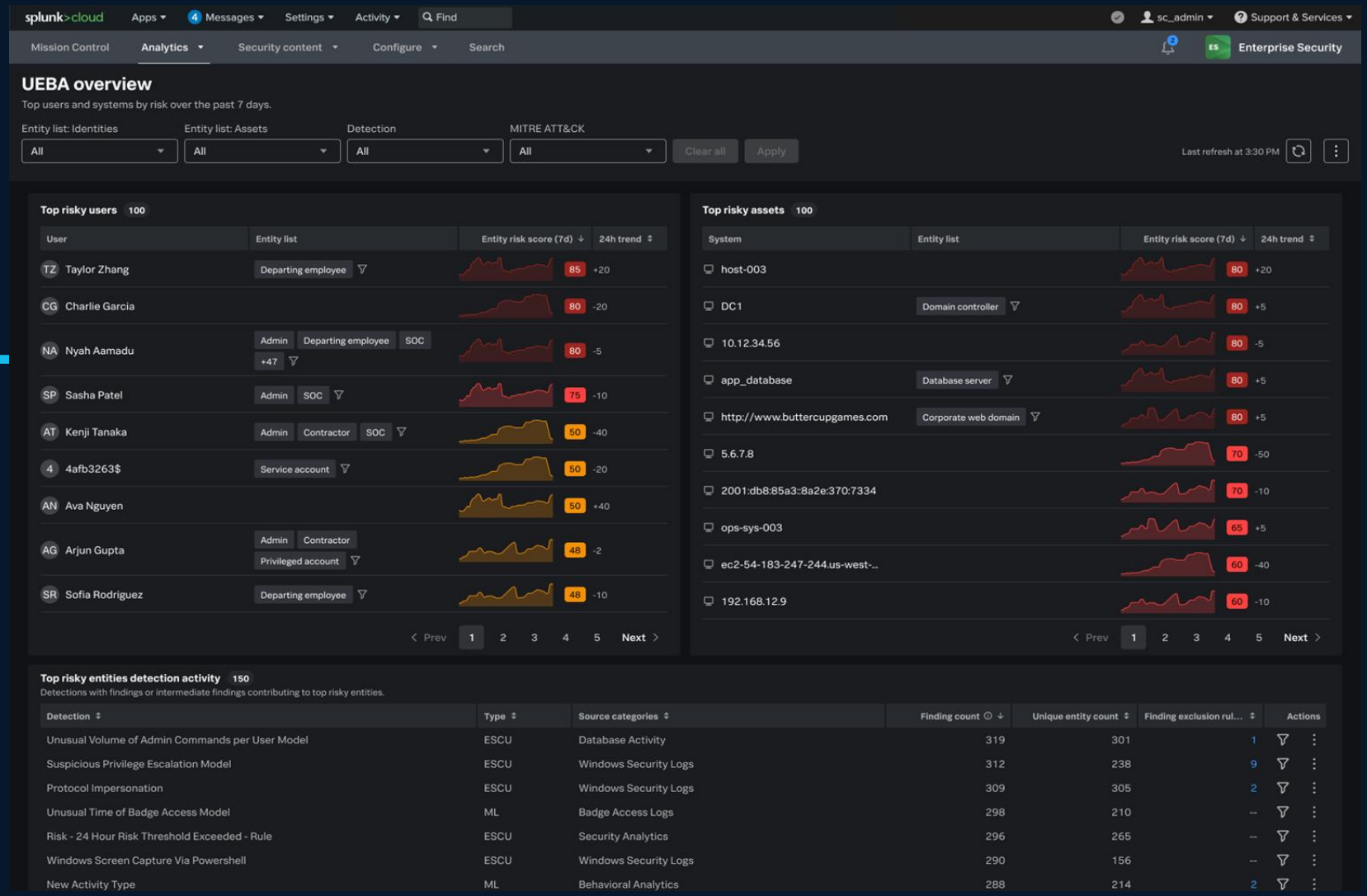
© 2025 Cisco and/or its affiliates. All rights reserved.

- GA Nov 25

Splunk UEBA

Splunk native UEBA engines

- CMP and Cloud enabled UEBA engines within ES
- Unsupervised AI and ML Behavioral baseline and detection
- Provide rich context for insider threats



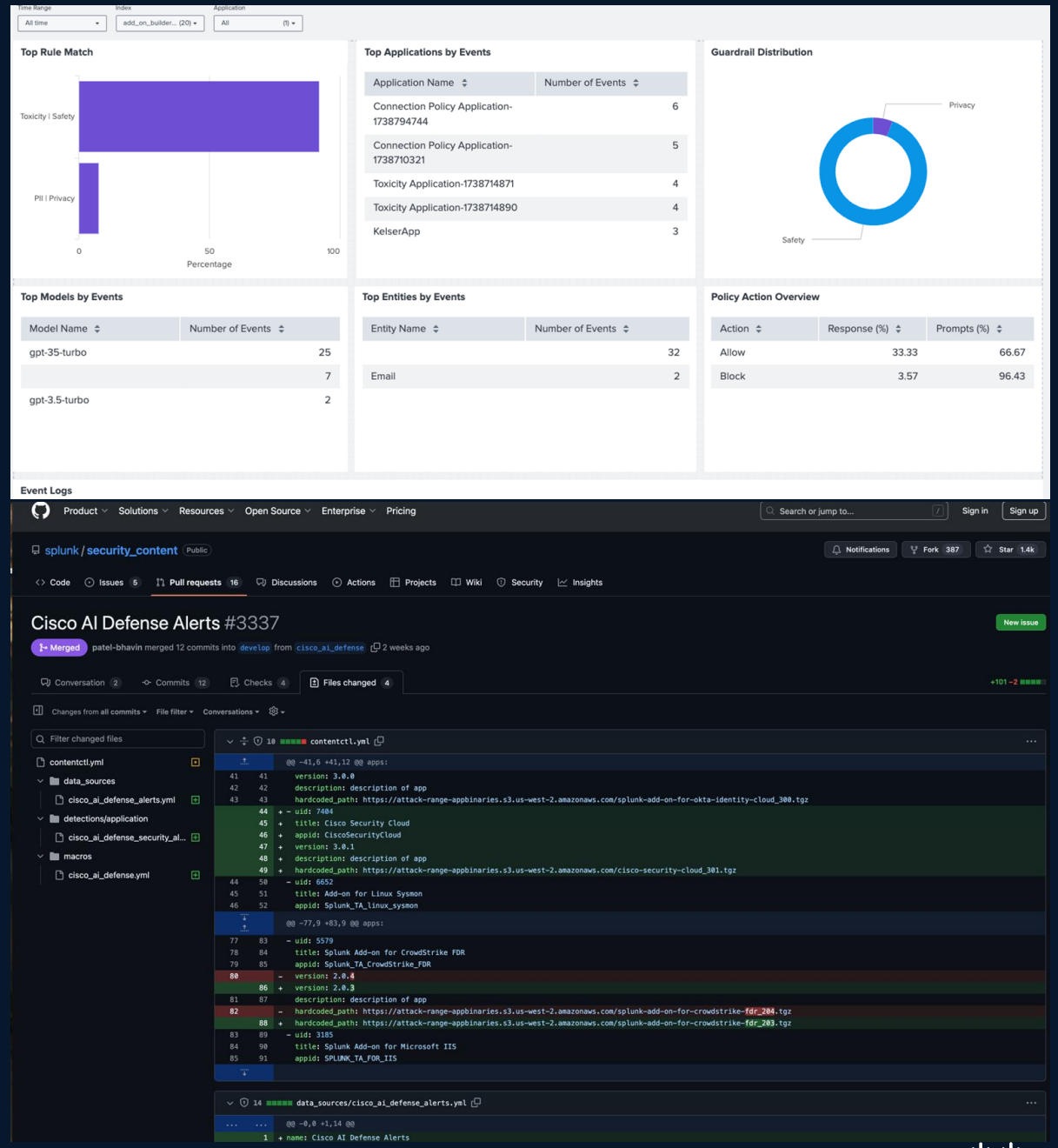
© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Cisco AI Defense

Gain visibility into emerging AI risks Integrated 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.

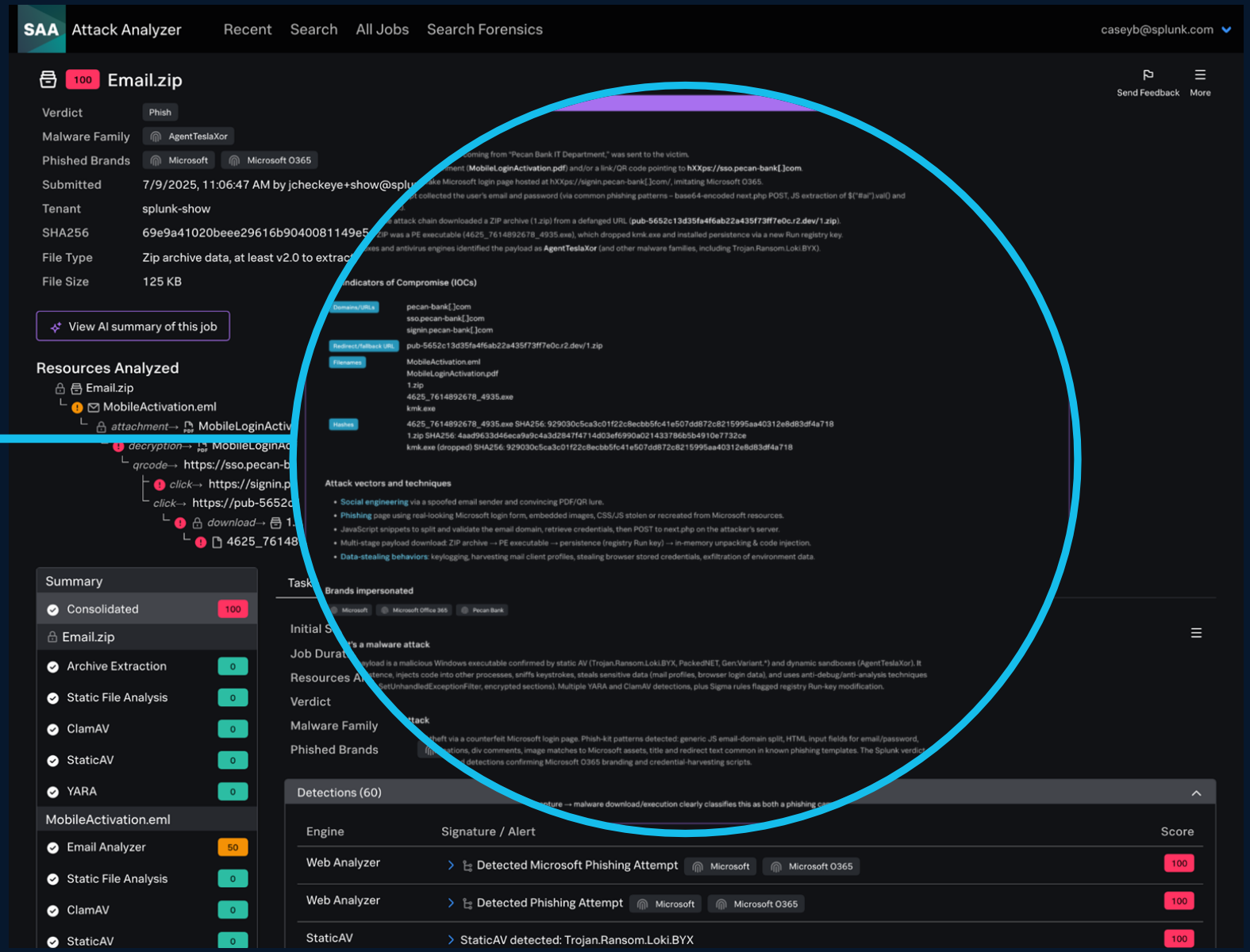


© 2025 Cisco and/or its affiliates. All rights reserved.

GA Now

Malware Reversing Engine

- Autonomous reverse engineering of all inbound payloads
- Full disposition summary and integration with ES
- Remove all manual work from payload analysis



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

AI Toolkit
Available today

- OOTB ML-powered detections: Splunk Enterprise Security Content Update (ESCU)
  - Detect DNS data exfiltration
  - Deep learning-based DGA Detection (C2)
  - Detection of risky command exploits (data exfiltration)
  - Detect suspicious DNS TXT records (bots)
  - Detect suspicious processes using RNN (malware)
  - Risky SPL detection
- Splunk Apps for Anomaly Detection & Behavioural Profiling
- Splunk Machine Learning Toolkit 5.4
- Splunk App for Deep Learning & Data Science 5.1

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

The SOC Platform

Operations

Detection

Triage Agent | AI Assistant in Enterprise Security | Detection Studio

TDIR Platform

UEBA | AI Defense | Reversing Agent | AI Toolkit

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

cisco

The SOC Platform

Operations

Detection

Data

Triage Agent	AI Assistant in Enterprise Security		Detection Studio
TDIR Platform			
UEBA	AI Defense	Reversing Agent	AI Toolkit

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

cisco

INTRODUCING

Cisco Data Fabric

A revolutionary new architecture to harness the value of machine data with AI

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

cisco

- Operate on machine data at ludicrous scale

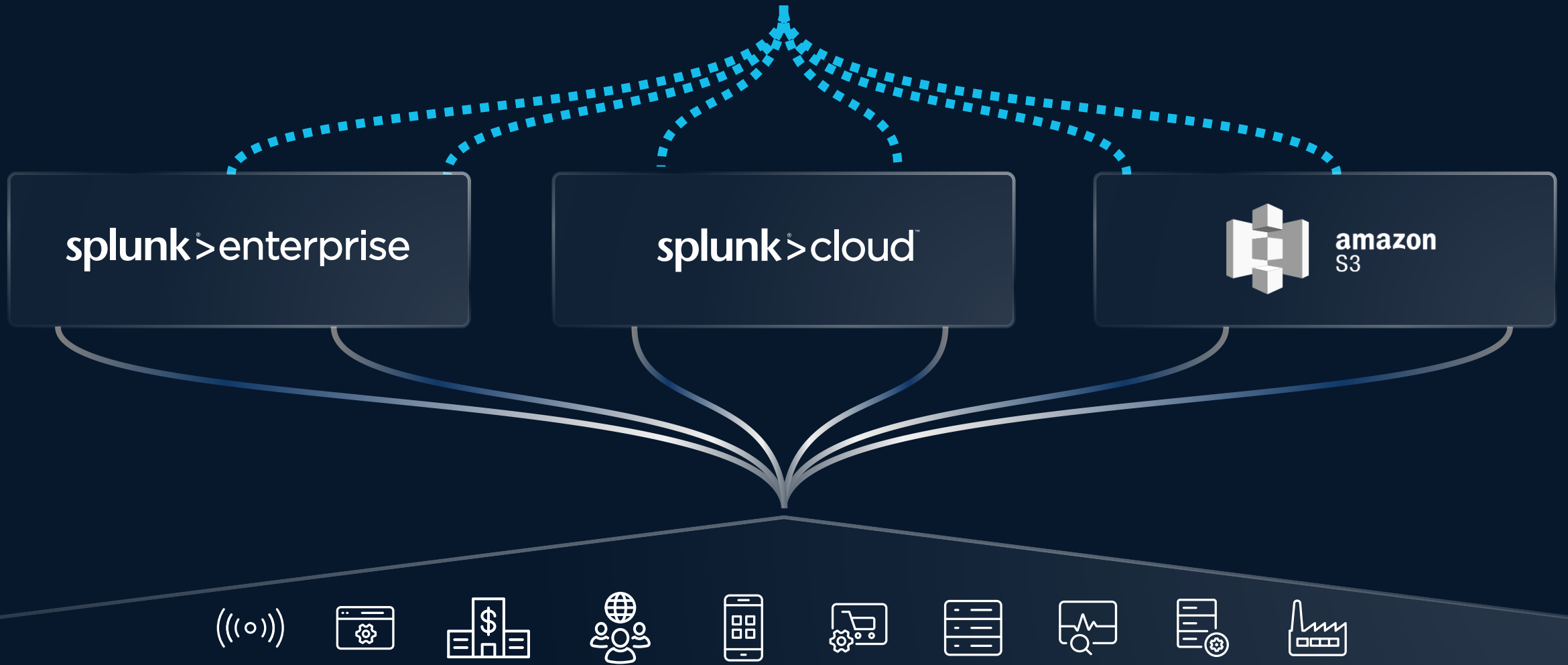
- Unlock your proprietary data for AI

- Unify experiences for humans and agents

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

© 2025 SPLUNK LLC

Federated Search



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

cisco

ANNOUNCING

Federated search for Snowflake

ALPHA FEBRUARY 2026

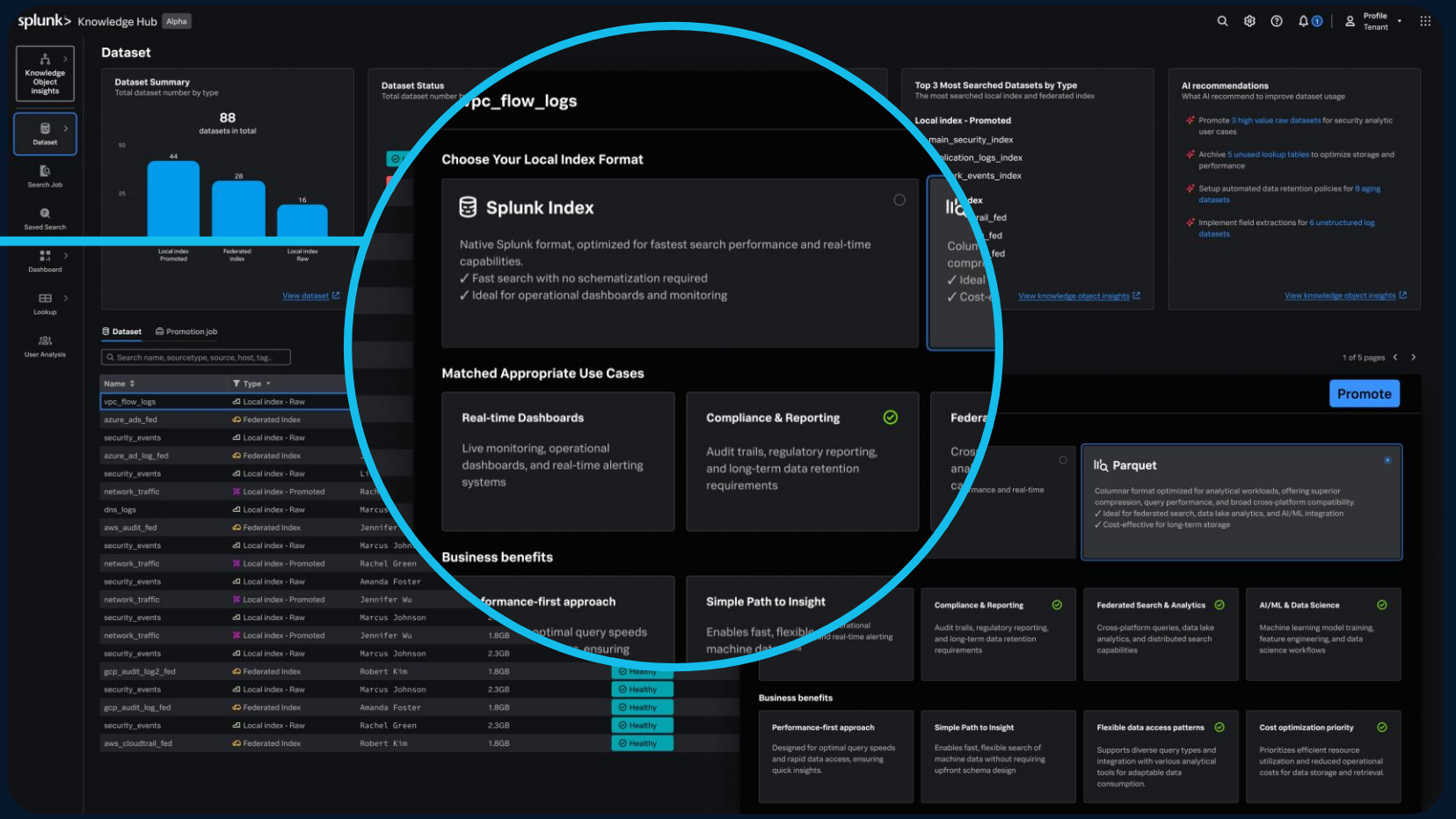
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

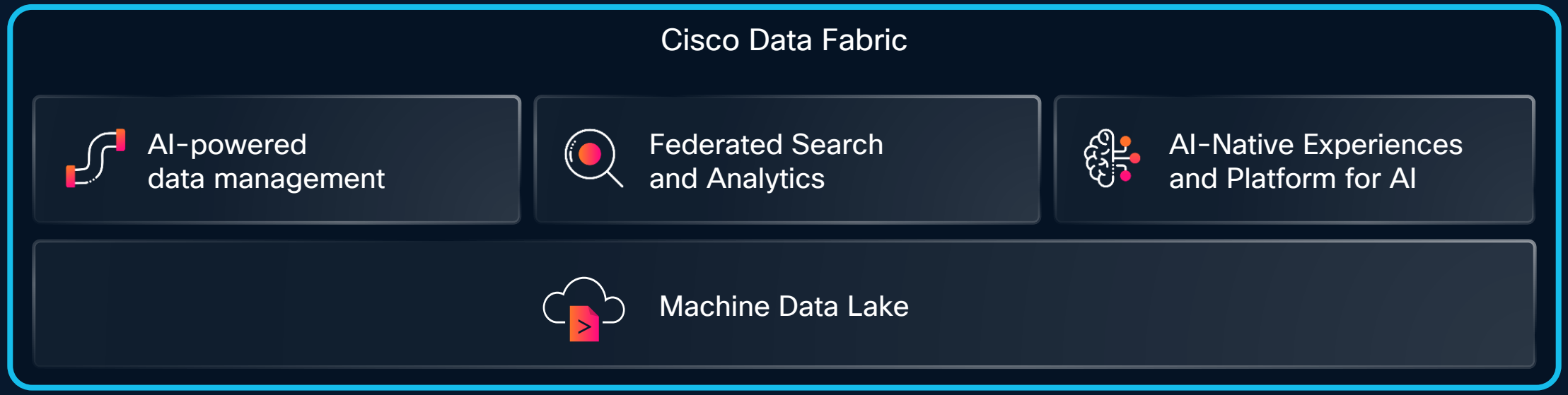
Alpha | Feb ‘26

Machine Data Lake

- Turn machine data into advantage
- Integrate for AI-ready insights
- Scalable, secured, governed



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



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

The SOC Platform

Operations

Detection

Data

Triage Agent

AI Assistant in Enterprise Security

Detection Studio

TDIR Platform

UEBA

AI Defense

Reversing Agent

AI Toolkit

Cisco Data Fabric

AI-powered data management

Federated Search and Analytics

AI-Native Experiences and Platform for AI

Machine Data Lake

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

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

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

cisco

Continue your education

Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

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

Thank you