

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

CISCO Live !

Digital Resilience

David Gamer
Principal Global Product Specialist

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?

Cisco Webex App

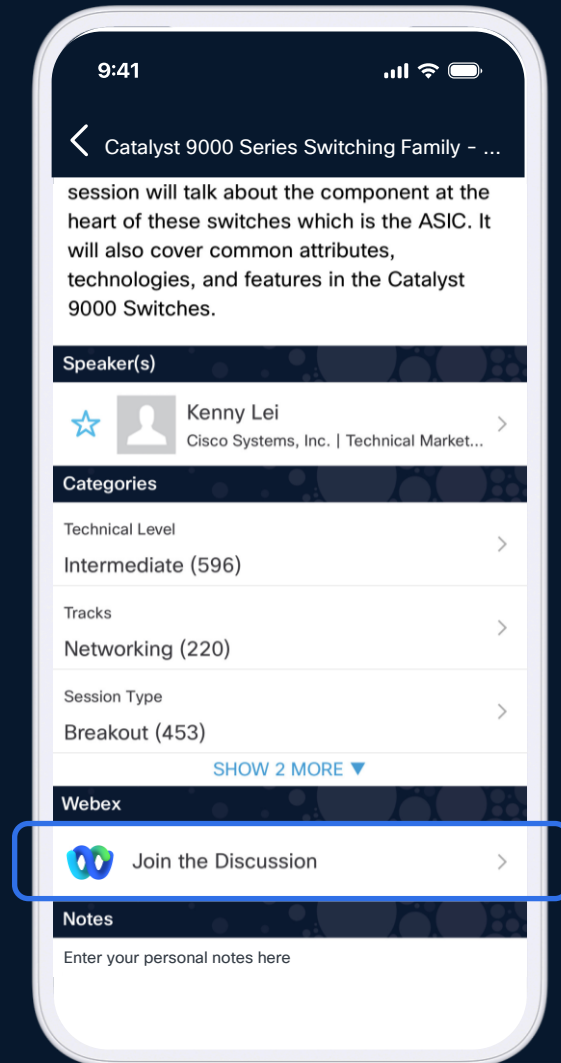
Questions?

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

How

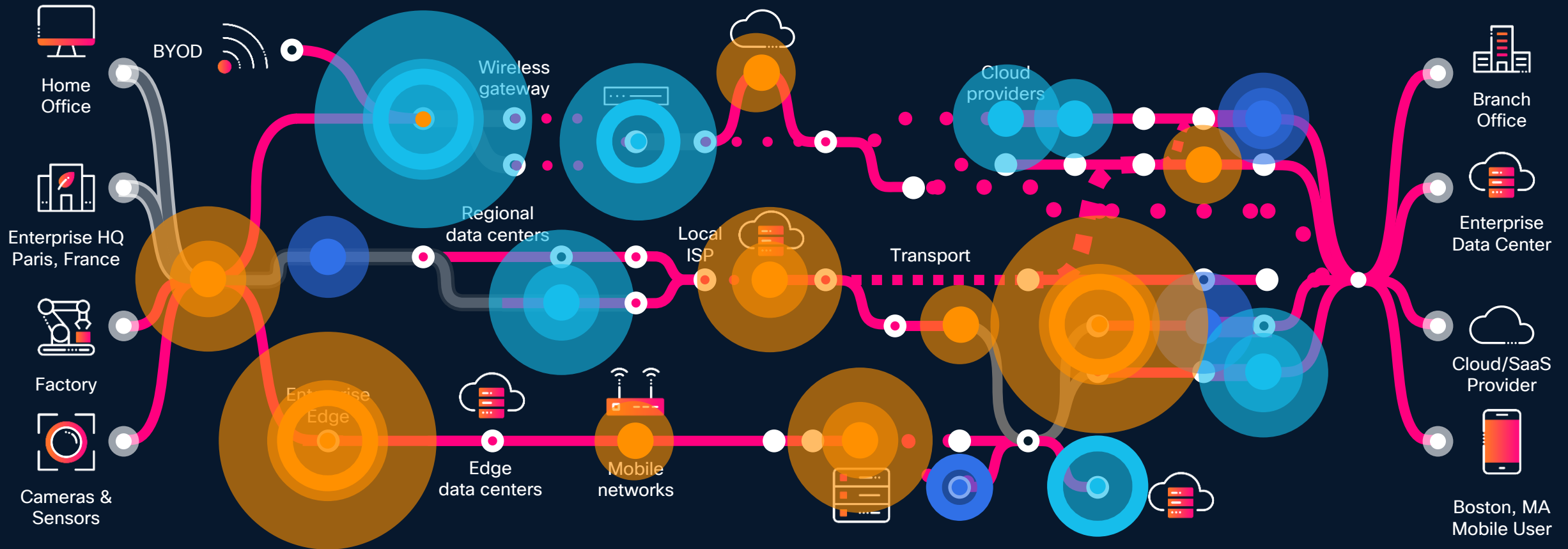
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

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



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

Complexity explosion is getting worse



AI will lift up defenders



Human-in-the Loop



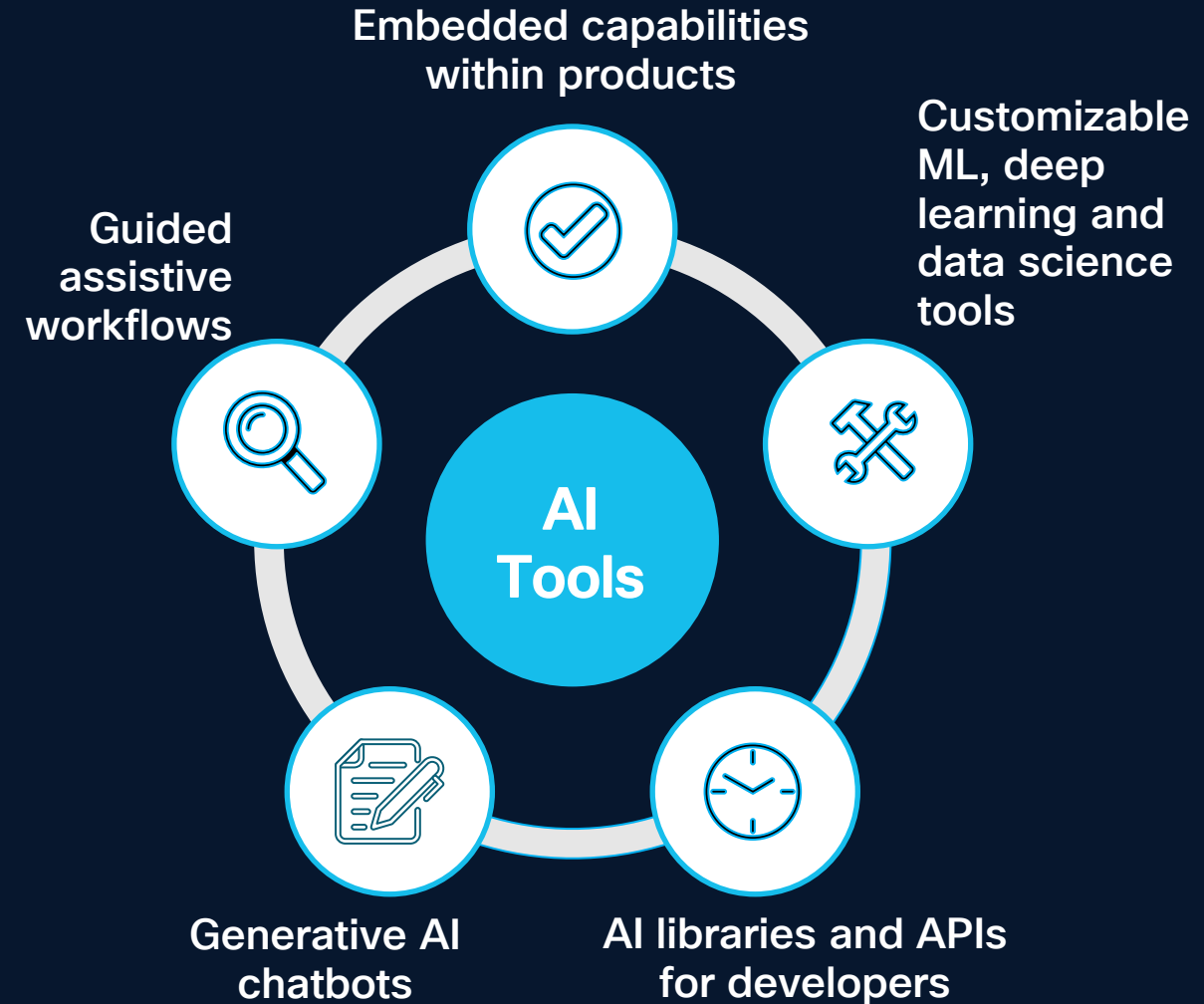
Domain-specific



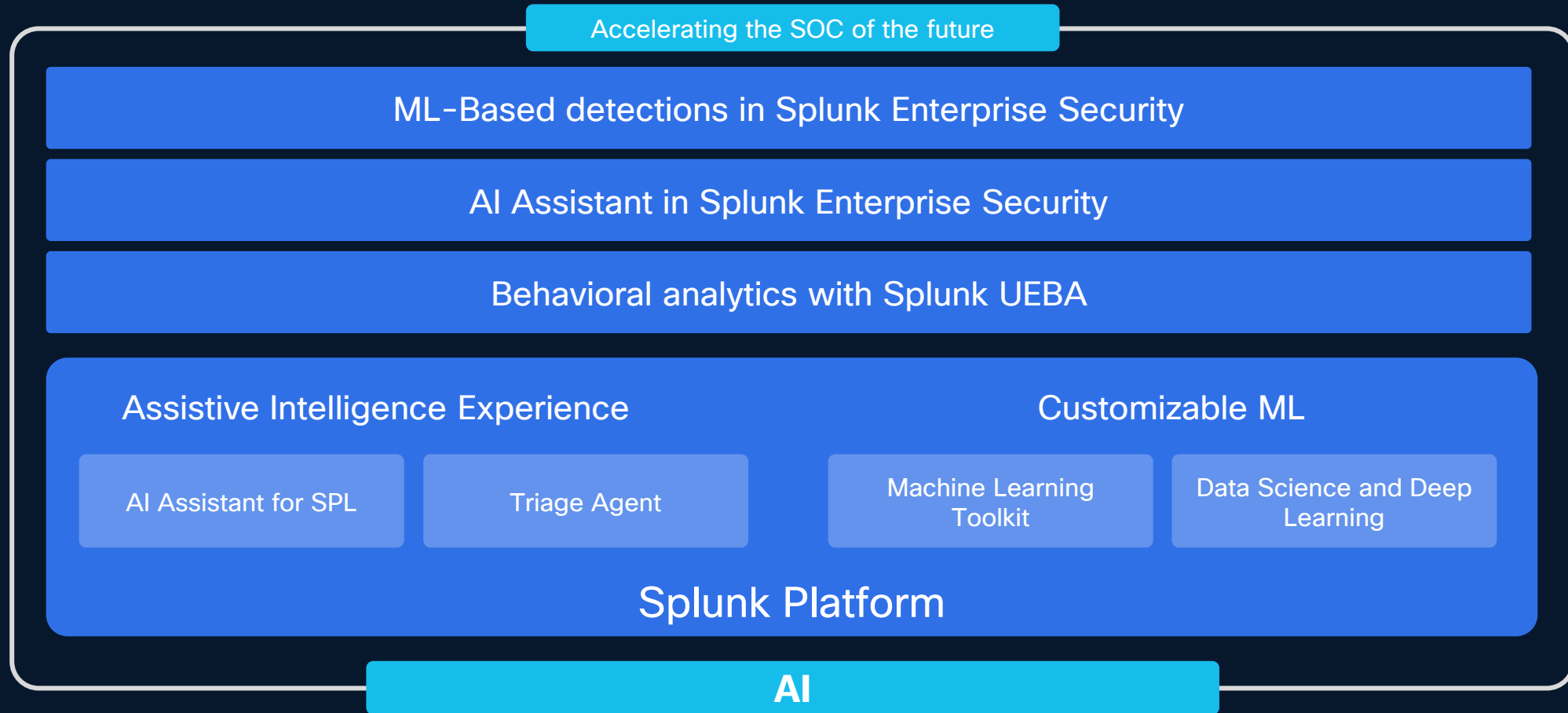
Open and Extensible

**We must unlock the value of
machine data to fuel AI**

Splunk's AI Superpower is Data



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



The background of the slide is a dark blue field filled with dynamic, flowing light streaks. These streaks are primarily in shades of bright blue and cyan, with some warmer orange and pinkish tones visible in the upper right quadrant. The lines are curved and layered, creating a sense of depth and movement, reminiscent of data flow or network connections.

Threat Detection, Investigation and Response

The SOC Operation

Initial
Triage



Incident
Response



Advanced
Response



Engineering



Management



TDIR Platform



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.



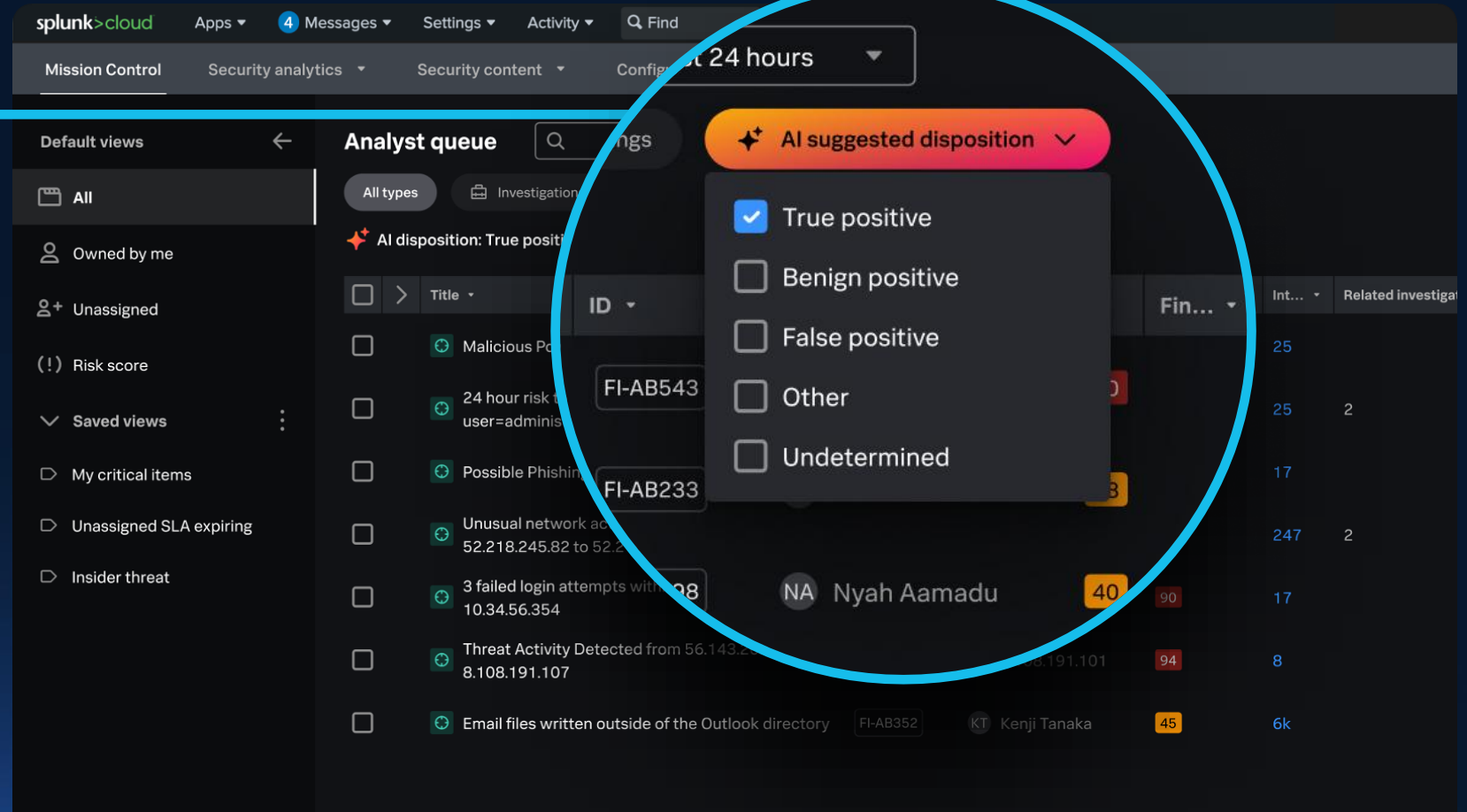
Open and Extensible

AI that is understandable and specific for each environment.

No closed boxes.

Triage Agent

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



The SOC Operation

Initial
Triage



Incident
Response



Advanced
Response



Engineering



Management



Triage
Agent

TDIR Platform

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

The screenshot displays the Splunk Security Console interface. At the top, a navigation bar includes 'Mission Control', 'Analytics', 'Security content', 'Configure', and 'Search'. Below this, a 'Queue' section shows a red alert: '24 hour risk threshold exceeded for system=win-svr1.acme.local'. The 'Overview' tab is active, showing a 'MITRE ATT&CK map' with various techniques categorized by Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, and Credential Access. Below the map, 'Intermediate findings' are listed for the entity 'win-svr1.acme.local', including 'Suspicious registry keys added', 'An instance of cmd.exe spawning...', 'An instance of powershell.exe running with pot...', and 'The Windows Firewall was disabled'. A timeline view shows these events from Thursday, May 30, to Saturday, June 1, 2024. On the right side, a chat window titled 'AI Assistant for Security' is open, showing a conversation with John Smith and the AI Assistant. The AI Assistant has responded to a query about its skills, listing two main capabilities: 'SPL Generation based on the user's Splunk environment' and 'Summarizing security findings'.

John Smith May 31, 4:01 AM
Discover AI Assistant skills

AI May 31, 4:01 AM
Sure, here are the AI Assistant skills that can be leveraged:

1. **SPL Generation based on the user's Splunk environment:**
 - This involves creating or generating Splunk Processing Language (SPL) queries according to the user's requirements and the available structure and data in the user's Splunk environment.
2. **Summarizing security findings:**

Reviewed all process activity for user bstoll
"parent_process_name","process_name",process,count,first Time,last Time
"svchost.exe","InstallAgent.exe","C:\Windows\System32\inst

John Smith May 30, 8:31 PM
Compromised user account
user account bstoll appears compromised as that user is on leave. Have quarantined the machine pending further analysis, not other activity from this account on other

John Smith May 30, 8:30 PM
Escalated to service owner
Contacted service owner to verify situation given IT user

4. **Recommending detection Security Content Update**
• This involves sugg
detections from E
various types of s
within the Splunk
environment.
These features enable efficient
reporting of security events wit
advanced analytics and AI cap

Ask me anything about 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 investigation4

Detections in selected time range0

Sub-Techniques (1)

Last 30 days

ent

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

0 of 13 Techniques (0%)

1 of 36 Techniques (3%)

0 of 71 Techniques (0%)

1 of 41 Techniques (2%)

2 of 89 Techniques (2%)

1 of 30 Techniques (3%)

0 of 33 Techniques (0%)

0 of 20 Techniques (0%)

0 of 17 Techniques

Command and Scripting Interpreter

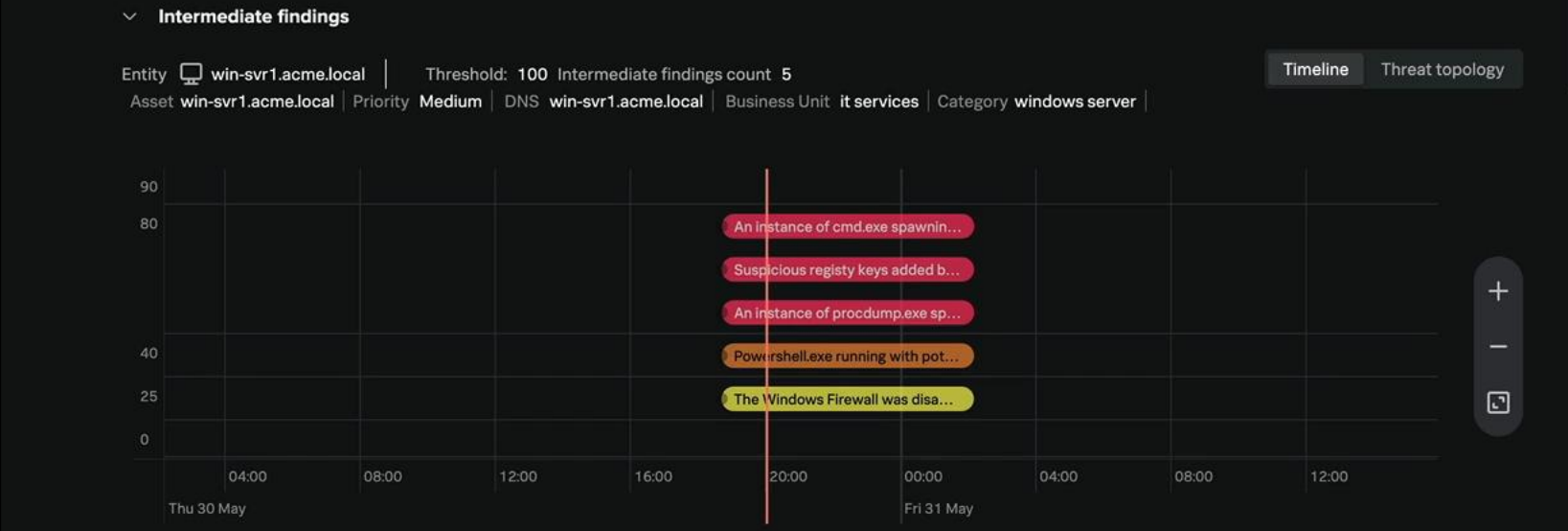
PowerShell

Abuse Elevation Control Mechanism

Abuse Elevation Control Mechanism

OS Credential Dumping

Impair Defenses



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 0

The SOC Operation

Initial
Triage



Incident
Response



Advanced
Response



Engineering



Management



Triage Agent

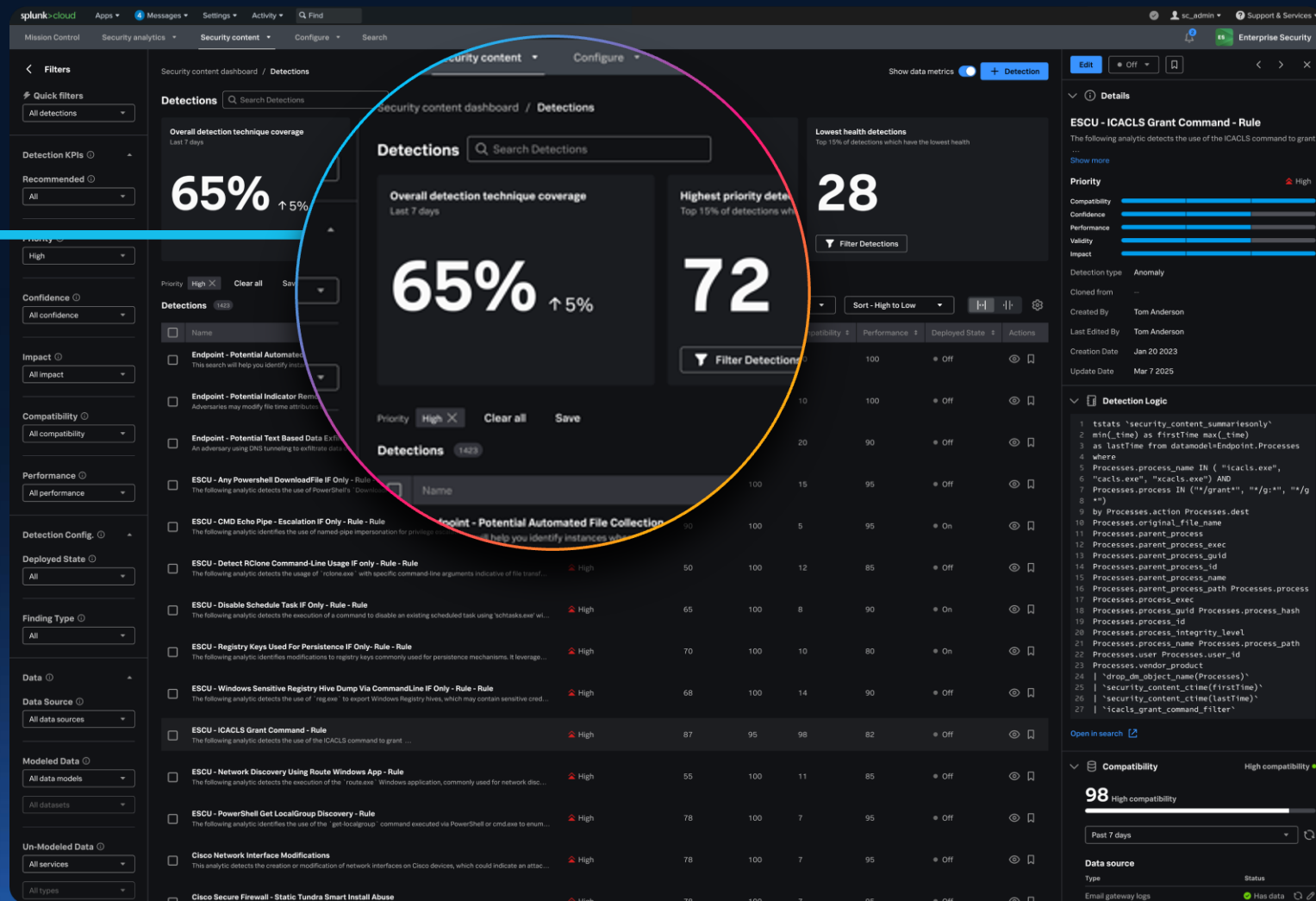
AI Assistant in Enterprise Security

TDIR Platform

Detection Studio

Powered by SnapAttack

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



The SOC Operation

Initial
Triage



Incident
Response



Advanced
Response



Engineering



Management



Triage Agent

AI Assistant in Enterprise Security

Detection Studio

TDIR Platform

The background of the slide is a dark blue field filled with dynamic, flowing light streaks. These streaks are primarily in shades of bright blue and cyan, with some warmer orange and pinkish tones visible in the upper right quadrant. The lines are curved and layered, creating a sense of depth and movement, reminiscent of data flow or network connections.

Threat Detection, Investigation and Response

The SOC Platform

Initial
Triage



Incident
Response



Advanced
Response



Engineering



Management



Triage Agent

AI Assistant in Enterprise Security

Detection Studio

TDIR Platform

The SOC Platform



Triage Agent

AI Assistant in Enterprise Security

Detection Studio

TDIR Platform

Operations

Detection

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)

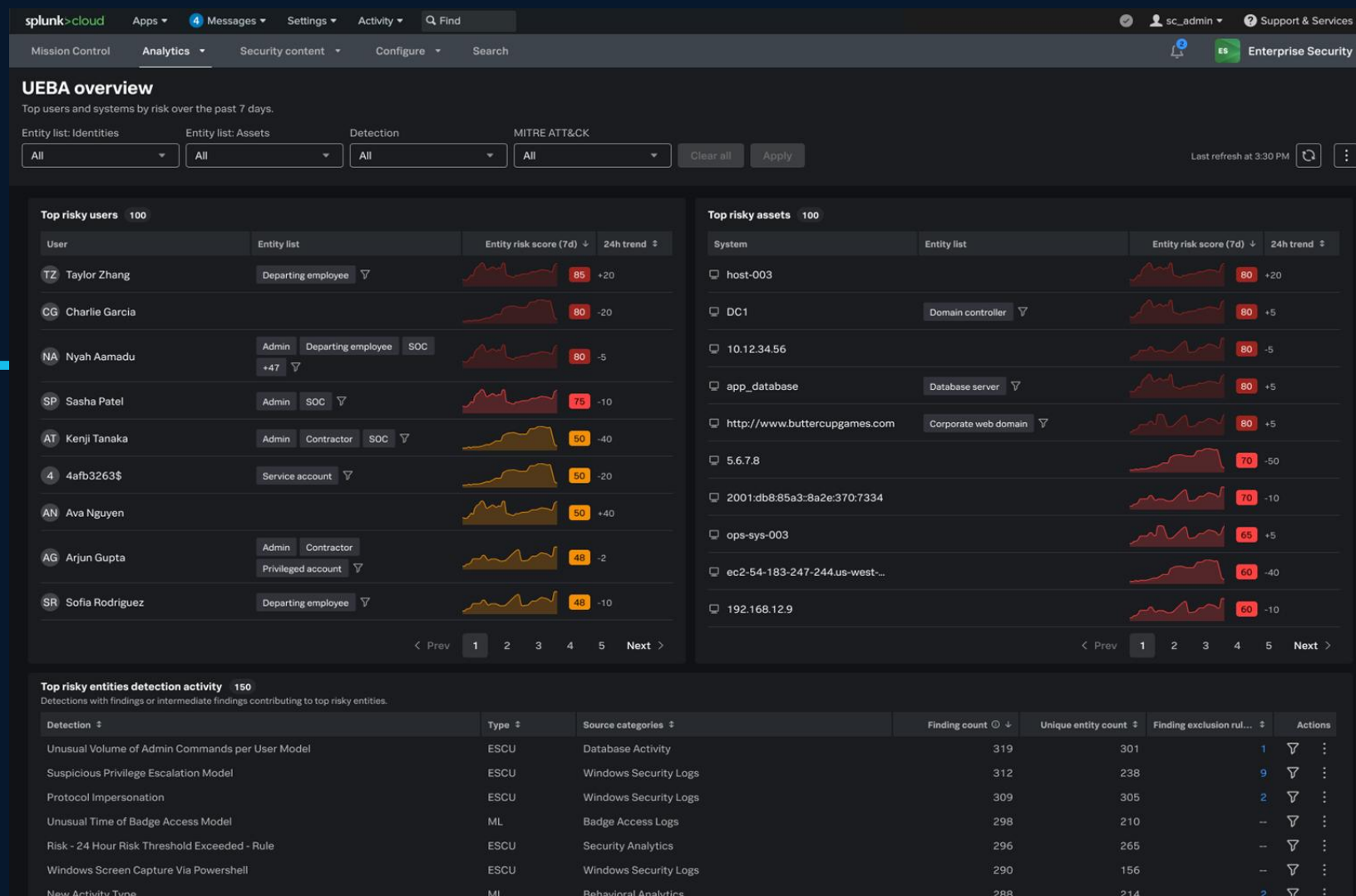
Find the signal from the noise in vast amounts of data.

• GA Nov
25

Splunk UEBA

Splunk native UEBA engines

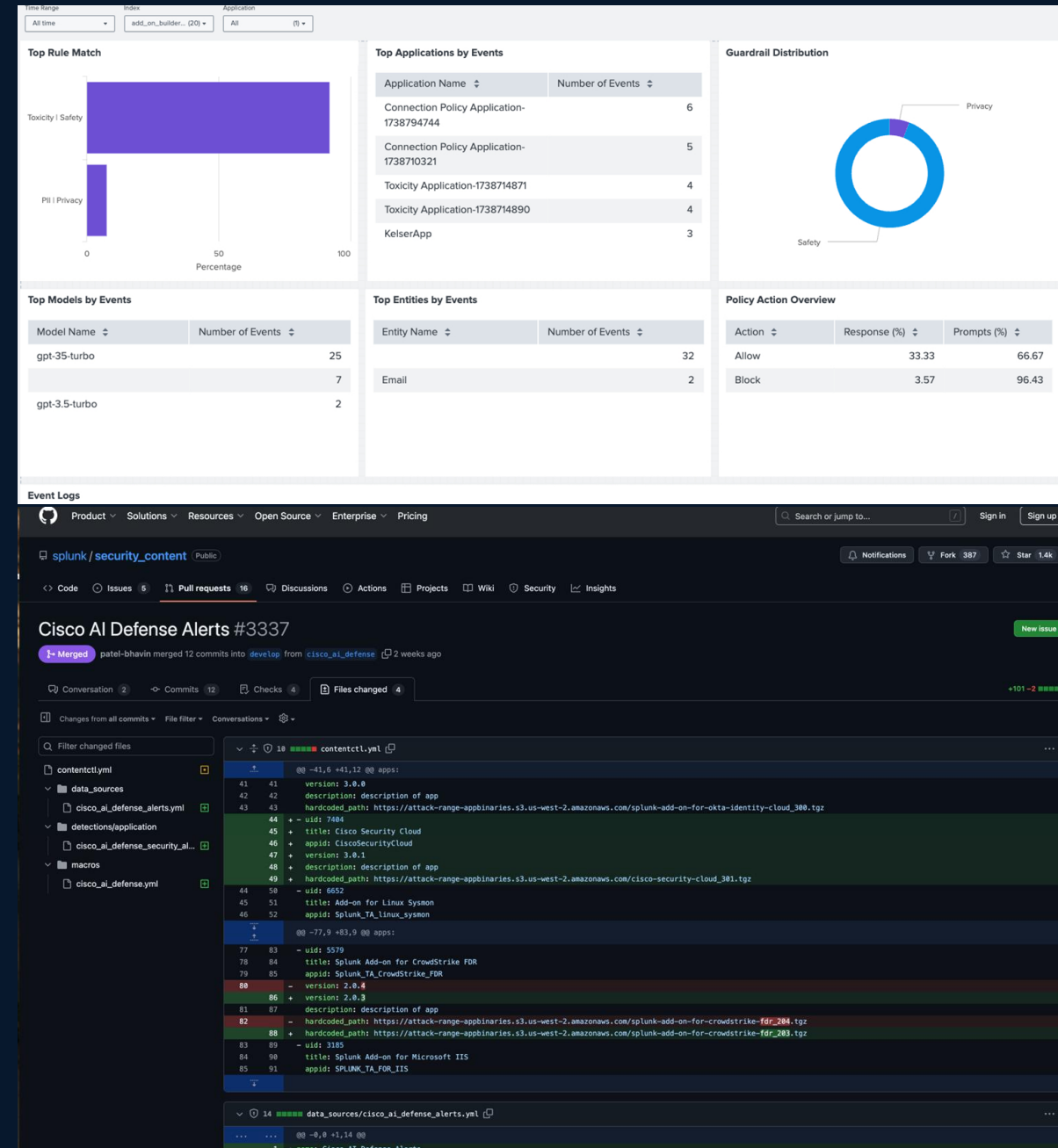
- CMP and Cloud enabled UEBA engines within ES
- Unsupervised AI and ML Behavioral baseline and detection
- Provide rich context for insider threats



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.



Malware Reversing Engine

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

SAA Attack Analyzer Recent Search All Jobs Search Forensics caseyb@splunk.com

Email.zip 100

Verdict: Phish

Malware Family: AgentTeslaXor

Phished Brands: Microsoft, Microsoft O365

Submitted: 7/9/2025, 11:06:47 AM by jcheckeye+show@splunk.com

Tenant: splunk-show

SHA256: 69e9a41020beee29616b9040081149e5...

File Type: Zip archive data, at least v2.0 to extract

File Size: 125 KB

[View AI summary of this job](#)

Resources Analyzed

- Email.zip
 - MobileActivation.eml
 - attachment → MobileLoginActiv...
 - decryption → MobileLoginActiv...
 - qrcode → https://sso.pecan-b...
 - click → https://signin.p...
 - click → https://pub-5652c...
 - download → 1...
 - 4625_76148...

Indicators of Compromise (IOCs)

 - Domains/URLs:** pecan-bank[.]com, sso.pecan-bank[.]com, signin.pecan-bank[.]com
 - Files/Files Hashes:** pub-5652c13d35fa4f6ab22a435f73ff7e0cr2.dev/1.zip
 - Files:** MobileActivation.eml, MobileLoginActivation.pdf, 1.zip, 4625_7614892678_4935.exe, kmk.exe
 - Files:** 4625_7614892678_4935.exe SHA256: 929030c5ca3c01f22c8ecbb5fc41e507dd872c8215995aa40312e8d83df4a718, 1.zip SHA256: 4aad9633d46eae9a9c4a3d284714714d034ef990a0214337b6b5b4910a7732ce, kmk.exe (dropped) SHA256: 929030c5ca3c01f22c8ecbb5fc41e507dd872c8215995aa40312e8d83df4a718

Attack vectors and techniques

 - Social engineering via a spoofed email sender and convincing PDF/QR lure.
 - Phishing page using real-looking Microsoft login form, embedded images, CSS/JS stolen or recreated from Microsoft resources.
 - JavaScript snippets to split and validate the email domain, retrieve credentials, then POST to next.php on the attacker's server.
 - Multi-stage payload download: ZIP archive → PE executable → persistence (registry Run key) → in-memory unpacking & code injection.
 - Data-stealing behaviors: keylogging, harvesting mail client profiles, stealing browser stored credentials, exfiltration of environment data.

Task: Brands Impersonated

Initial Summary: This is a malware attack

Job Duration: 1m 10s

Resources Analyzed: 1

Verdict: Phish

Malware Family: AgentTeslaXor

Phished Brands: Microsoft, Microsoft Office 365, Pecan Bank

Detections (60)

Engine	Signature / Alert	Score
Web Analyzer	> Detected Microsoft Phishing Attempt	100
Web Analyzer	> Detected Phishing Attempt	100
StaticAV	> StaticAV detected: Trojan.Ransom.Loki.BYX	100

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

The SOC Platform



Operations

Triage Agent

AI Assistant in Enterprise Security

Detection Studio

TDIR Platform

Detection

UEBA

AI Defense

Reversing Agent

AI Toolkit

The SOC Platform



Operations

Triage Agent

AI Assistant in Enterprise Security

Detection Studio

TDIR Platform

Detection

UEBA

AI Defense

Reversing Agent

AI Toolkit

Data

INTRODUCING

Cisco Data Fabric

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



- Operate on machine data at ludicrous scale



- Unlock your proprietary data for AI



- Unify experiences for humans and agents

Federated Search



ANNOUNCING

Federated search for Snowflake

A L P H A F E B R U A R Y 2 0 2 6



Machine Data Lake

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

splunk> Knowledge Hub Alpha

Dataset

Dataset Summary
Total dataset number by type

88 datasets in total

Local Index Promoted: 44, Federated Index: 28, Local Index Raw: 16

Dataset Status
Total dataset number by type

Choose Your Local Index Format

Splunk Index

Native Splunk format, optimized for fastest search performance and real-time capabilities.

- ✓ Fast search with no schematization required
- ✓ Ideal for operational dashboards and monitoring

Matched Appropriate Use Cases

- Real-time Dashboards**
Live monitoring, operational dashboards, and real-time alerting systems
- Compliance & Reporting**
Audit trails, regulatory reporting, and long-term data retention requirements

Business benefits

- Performance-first approach**
Designed for optimal query speeds and rapid data access, ensuring quick insights.
- Simple Path to Insight**
Enables fast, flexible search of machine data without requiring upfront schema design.
- Compliance & Reporting**
Audit trails, regulatory reporting, and long-term data retention requirements.
- Federated Search & Analytics**
Cross-platform queries, data lake analytics, and distributed search capabilities.
- AI/ML & Data Science**
Machine learning model training, feature engineering, and data science workflows.
- Flexible data access patterns**
Supports diverse query types and integration with various analytical tools for adaptable data consumption.
- Cost optimization priority**
Prioritizes efficient resource utilization and reduced operational costs for data storage and retrieval.

Top 3 Most Searched Datasets by Type
The most searched local index and federated index

- Local index - Promoted: main_security_index, application_logs_index, network_events_index
- Local index - Federated: main_security_index, application_logs_index, network_events_index
- Local index - Raw: main_security_index, application_logs_index, network_events_index

AI recommendations
What AI recommend to improve dataset usage

- Promote 3 high value raw datasets for security analytic user cases
- Archive 5 unused lookup tables to optimize storage and performance
- Setup automated data retention policies for 8 aging datasets
- Implement field extractions for 6 unstructured log datasets

Dataset Table

Name	Type	Owner	Size	Health
vpc_flow_logs	Local Index - Raw			
azure_ads_fed	Federated Index			
security_events	Local Index - Raw			
azure_ad_log_fed	Federated Index			
security_events	Local Index - Raw			
network_traffic	Local Index - Promoted	Rachel Green		
dns_logs	Local Index - Raw	Marcus Johnson		
aws_audit_fed	Federated Index	Jennifer Mu		
security_events	Local Index - Raw	Marcus Johnson		
network_traffic	Local Index - Promoted	Rachel Green		
security_events	Local Index - Raw	Amanda Foster		
network_traffic	Local Index - Promoted	Jennifer Mu		
security_events	Local Index - Raw	Marcus Johnson		
network_traffic	Local Index - Promoted	Jennifer Mu	1.8GB	Healthy
security_events	Local Index - Raw	Marcus Johnson	2.3GB	Healthy
gcp_audit_log2_fed	Federated Index	Robert Kim	1.8GB	Healthy
security_events	Local Index - Raw	Marcus Johnson	2.3GB	Healthy
gcp_audit_log_fed	Federated Index	Amanda Foster	1.8GB	Healthy
security_events	Local Index - Raw	Rachel Green	2.3GB	Healthy
aws_cloudtrail_fed	Federated Index	Robert Kim	1.8GB	Healthy

Cisco Data Fabric



AI-powered
data management



Federated Search
and Analytics



AI-Native Experiences
and Platform for AI



Machine Data Lake

The SOC Platform



Operations

Triage Agent

AI Assistant in Enterprise Security

Detection Studio

TDIR Platform

Detection

UEBA

AI Defense

Reversing Agent

AI Toolkit

Data

Cisco Data Fabric



AI-powered
data management



Federated Search
and Analytics



AI-Native Experiences
and Platform for AI



Machine Data Lake

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.

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

Thank you

CISCO Live !