

Power the SOC of the Future

Michael Spivey – Leader, Solutions Engineer

Quinlan Ferris – Solutions Engineer



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

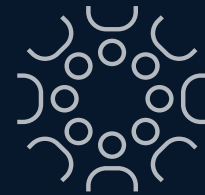
Enable seamless end-to-end connectivity to assure the delivery of applications and services

Observability

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

Security operations

Gain comprehensive threat prevention, detection, investigation, and response



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



Google

Microsoft

Amazon

Databricks

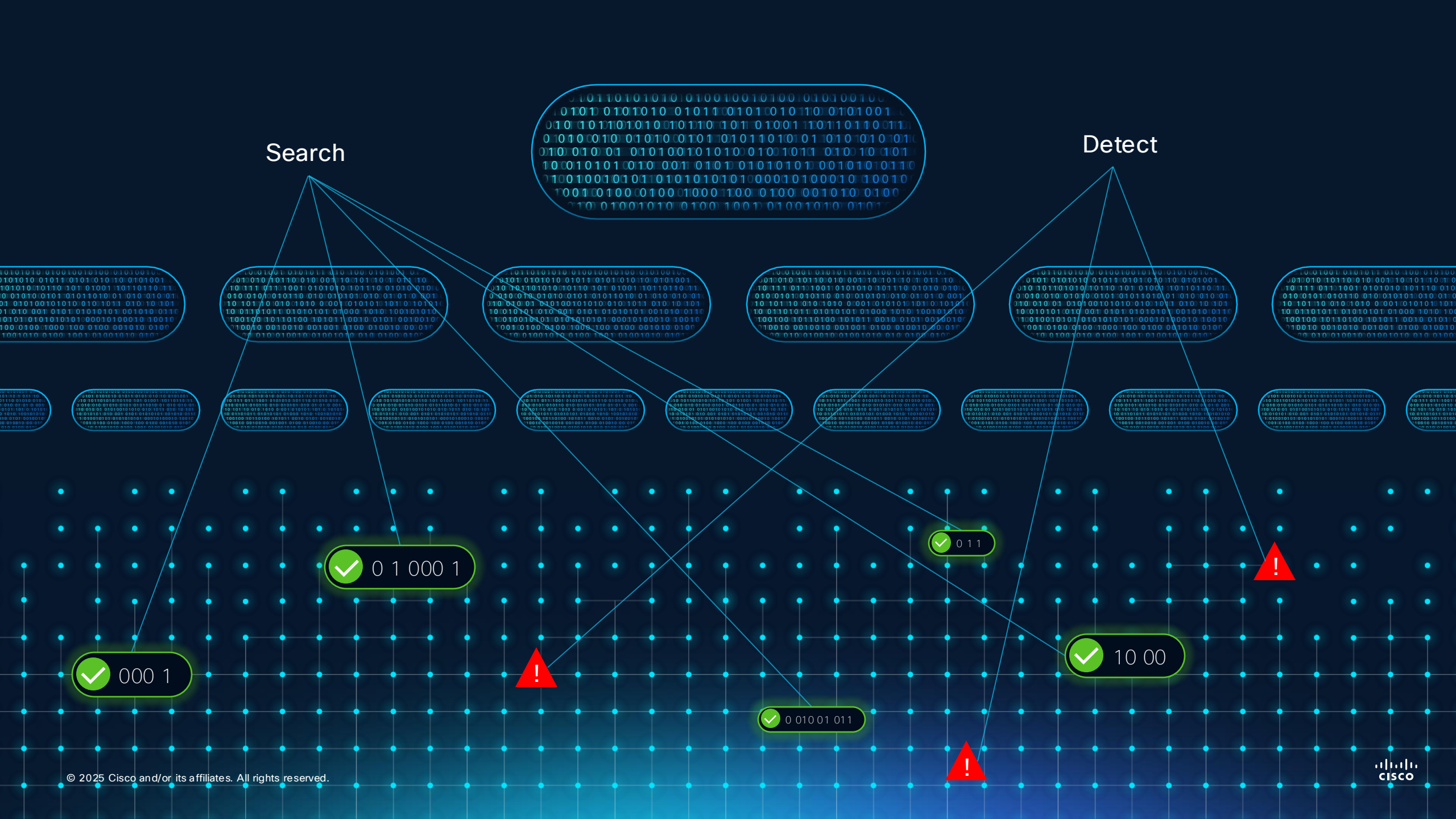
Cisco XDR

Cisco SAL

CrowdStrike

Palo Alto Networks

SentinelOne

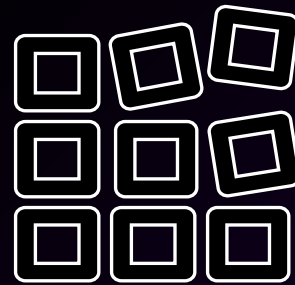


The data landscape **is changing** for the SOC

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



Data is growing exponentially.



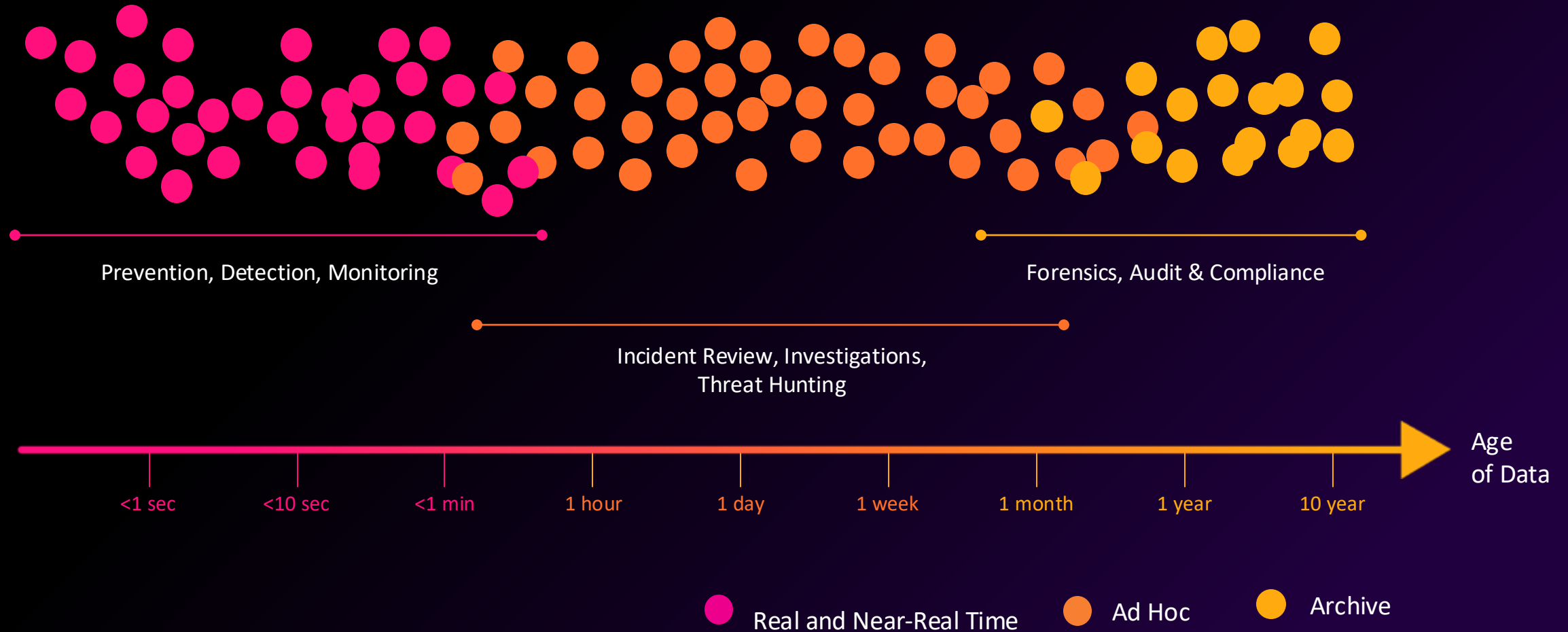
All data is not created equal.



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

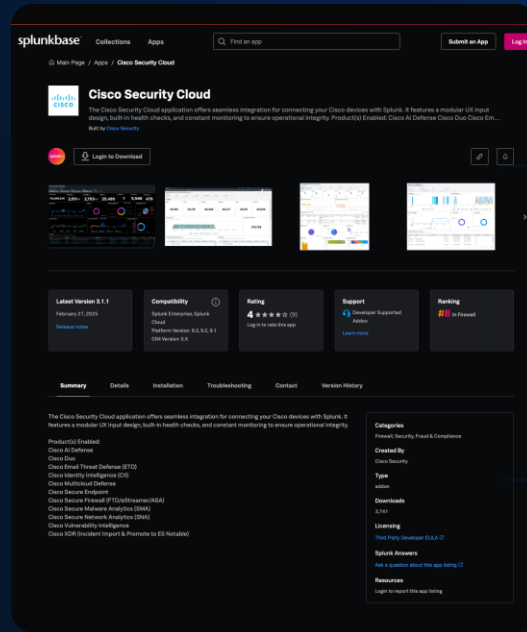
Data normalization
CIM, OCSF



Splunk Enterprise Security

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)



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

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.

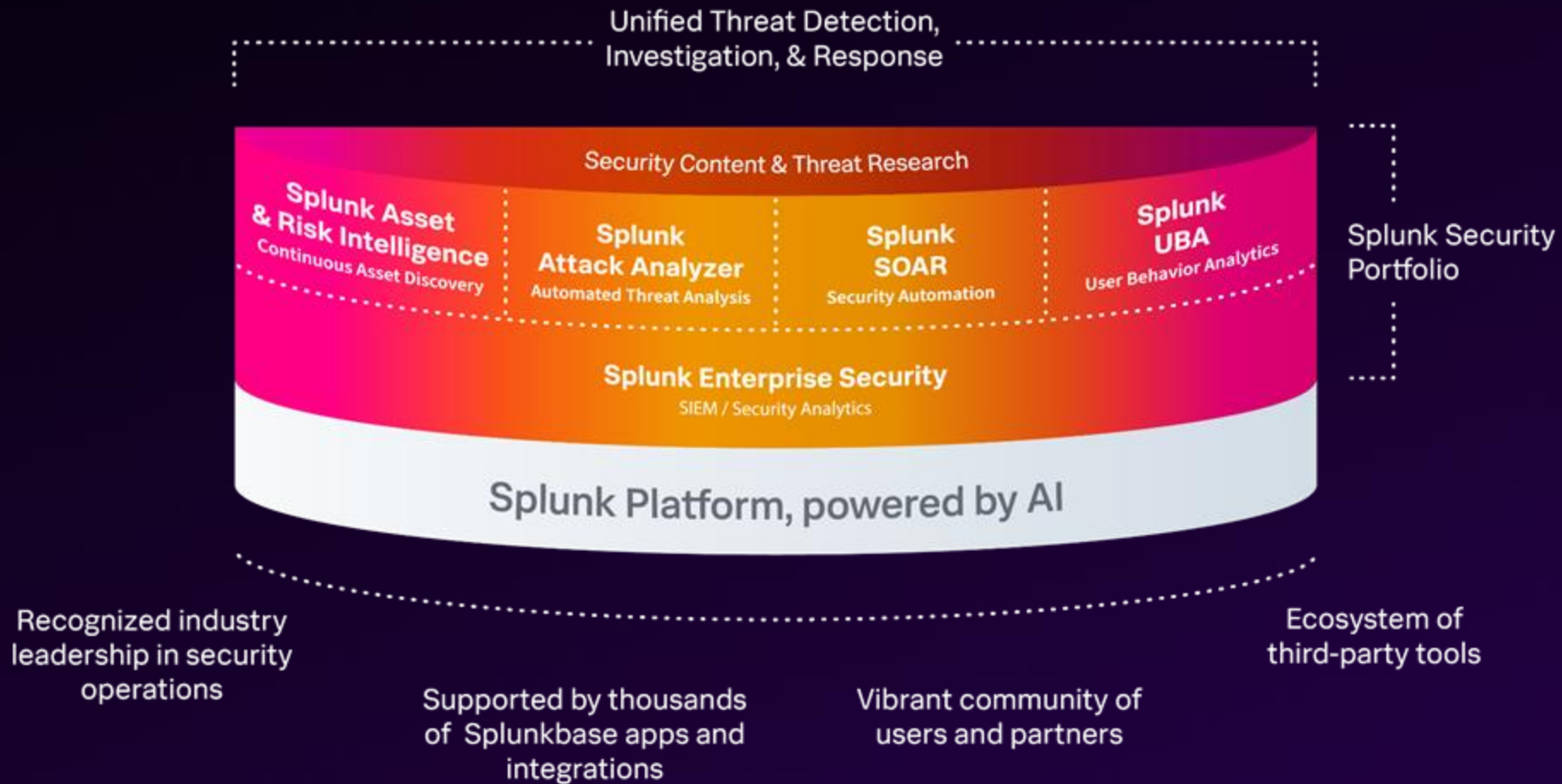
Unify Security Operations.

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.

Powering the SOC of the future with the leading TDIR solution



Splunk Enterprise Security

Power Your SOC with the SIEM of the Future

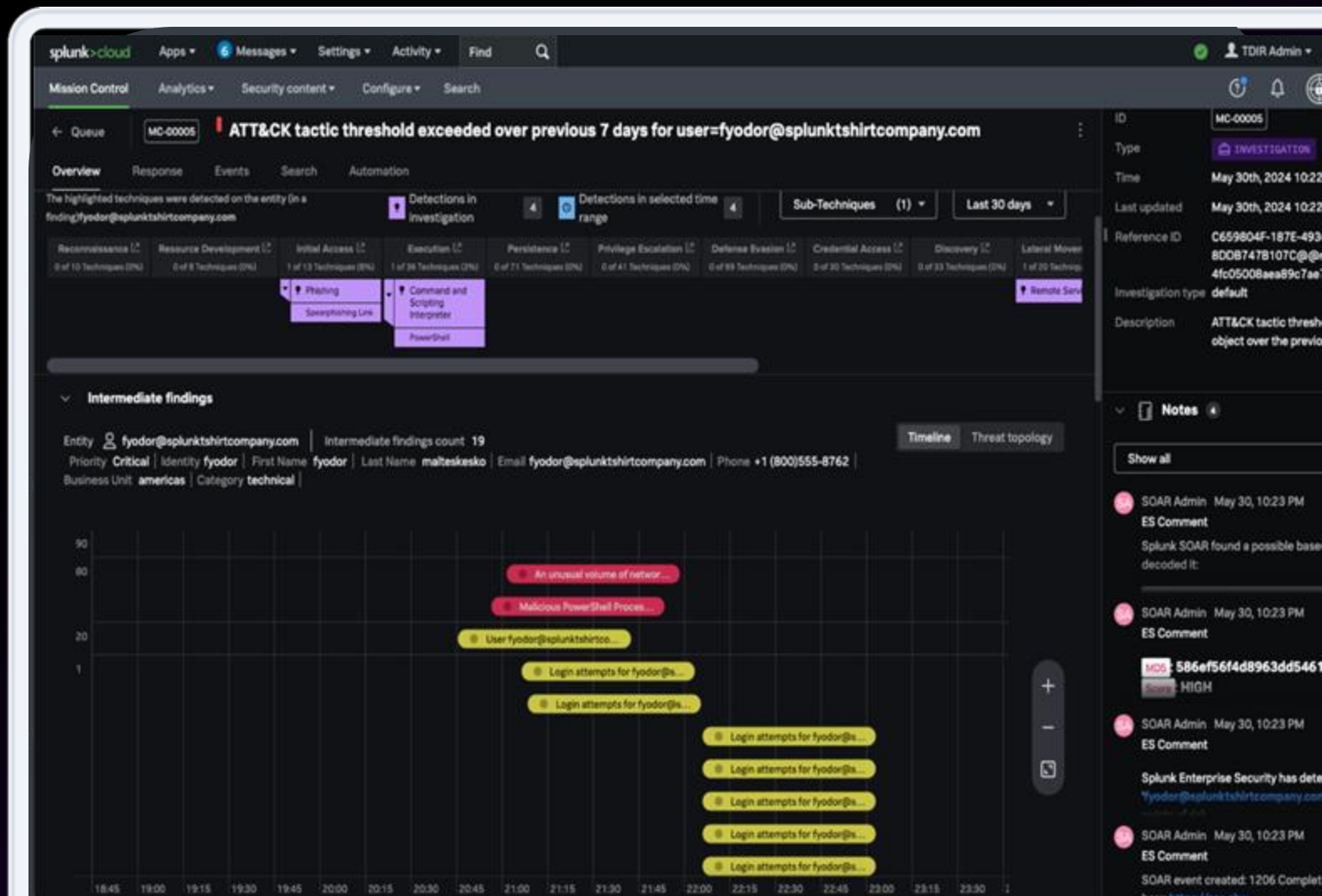
- Realize comprehensive visibility to make sense of data noise and enable fast action.
- Empower accurate detection with context to streamline investigations and increase productivity.
- Fuel operational efficiency by unifying threat detection, investigation and response (TDIR) workflows.

The screenshot displays the Splunk Enterprise Security interface. The top navigation bar includes links for Mission Control, Analytics, Security content, Configure, and Search. The main content area is titled 'Investigation of findings from the same entity [bstoll@splunkshirtcompany.com]'. It features a 'Findings' section with a table of findings, including 'Multiple findings from the same entity [bstoll@splunkshirtcompany.com]', 'ATT&CK tactic threshold exceeded over previous...', '24 hour risk threshold exceeded for entity [bstoll@splunkshirtcompany.com]', 'Malicious PowerShell process - encoded comm...', and 'Malicious PowerShell process - encoded comm...'. The 'MITRE ATT&CK map' section shows a grid of tactics and techniques, including 'Reconnaissance', 'Resource Development', 'Initial Access', 'Execution', 'Persistence', 'Privilege Escalation', and 'Defense Evasion'. The 'Custom fields' section includes 'Related Jira ticket' (ROMP-334), 'Related SNOW ticket', and 'Additional fields' (Destination, Destination category, Destination city, Destination country, Destination DNS, Destination Expected, Destination IP address, Destination NT hostname, Destination owner, Destination PCI domain, Destination requires antivirus, Destination should time synchronize). The 'Related investigations' section includes 'History' and 'Drill-down search'. The 'Notes' section includes a search bar and a list of notes, including 'Machine infected' and 'Blocked outbound network access'. The 'Files' section includes a search bar and a list of files, including 'Drop your files here or browse all file types supported'.

Empower Accurate Detection with Context

Streamline investigations
and increase productivity

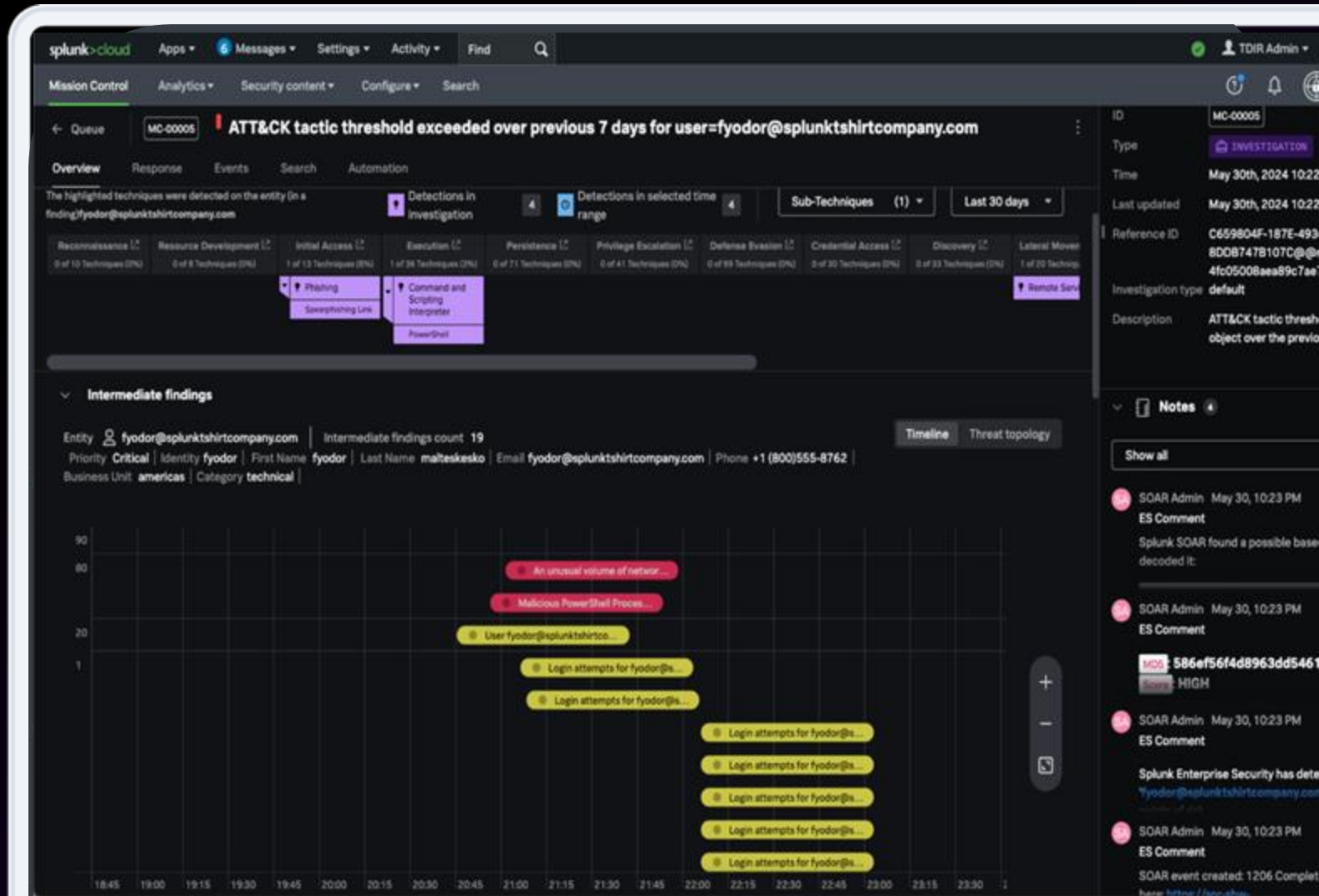
- **Drastically reduce alert volumes** by up to 90% with risk-based alerting (RBA).
- **Tap into 1,700+ out-of-the-box detections** to find and remediate threats faster.
- Easily maintain up-to-date detection content with native, **automatic detection versioning**.
- **Enhanced detection capabilities**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

- 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)

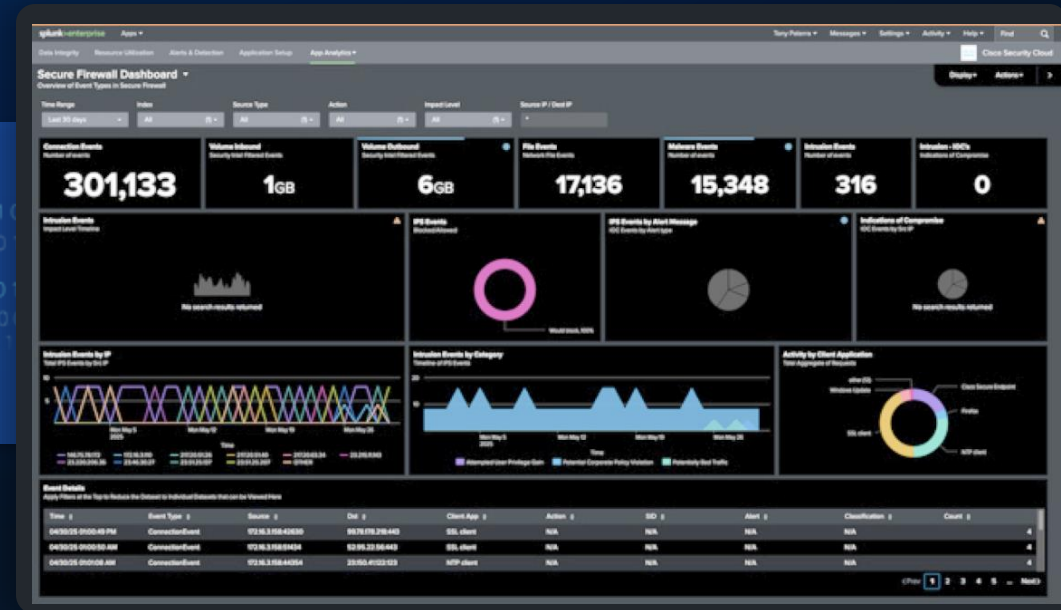


NEW

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)

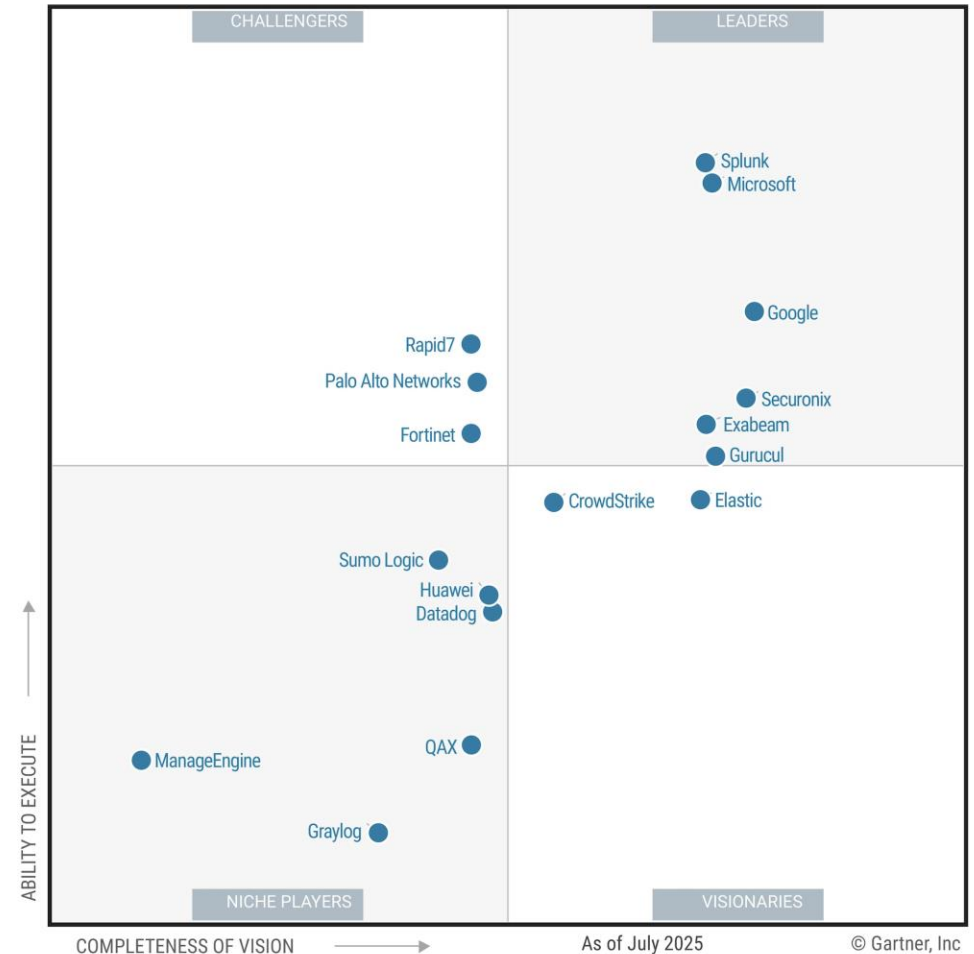
Splunk named a Leader for the 11th consecutive time

GARTNER is a registered trademark and service mark of Gartner and Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Splunk.

Figure 1: Magic Quadrant for Security Information and Event Management



Gartner

Cisco Integrations – A Deeper Dive

An abstract background featuring a gradient of blue shades, from dark navy on the left to a lighter cyan on the right. Overlaid on this gradient is a pattern of numerous small, semi-transparent blue dots of varying sizes. These dots are more densely packed in the lower half of the image, creating a sense of depth and movement, while the upper half is relatively clearer.

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

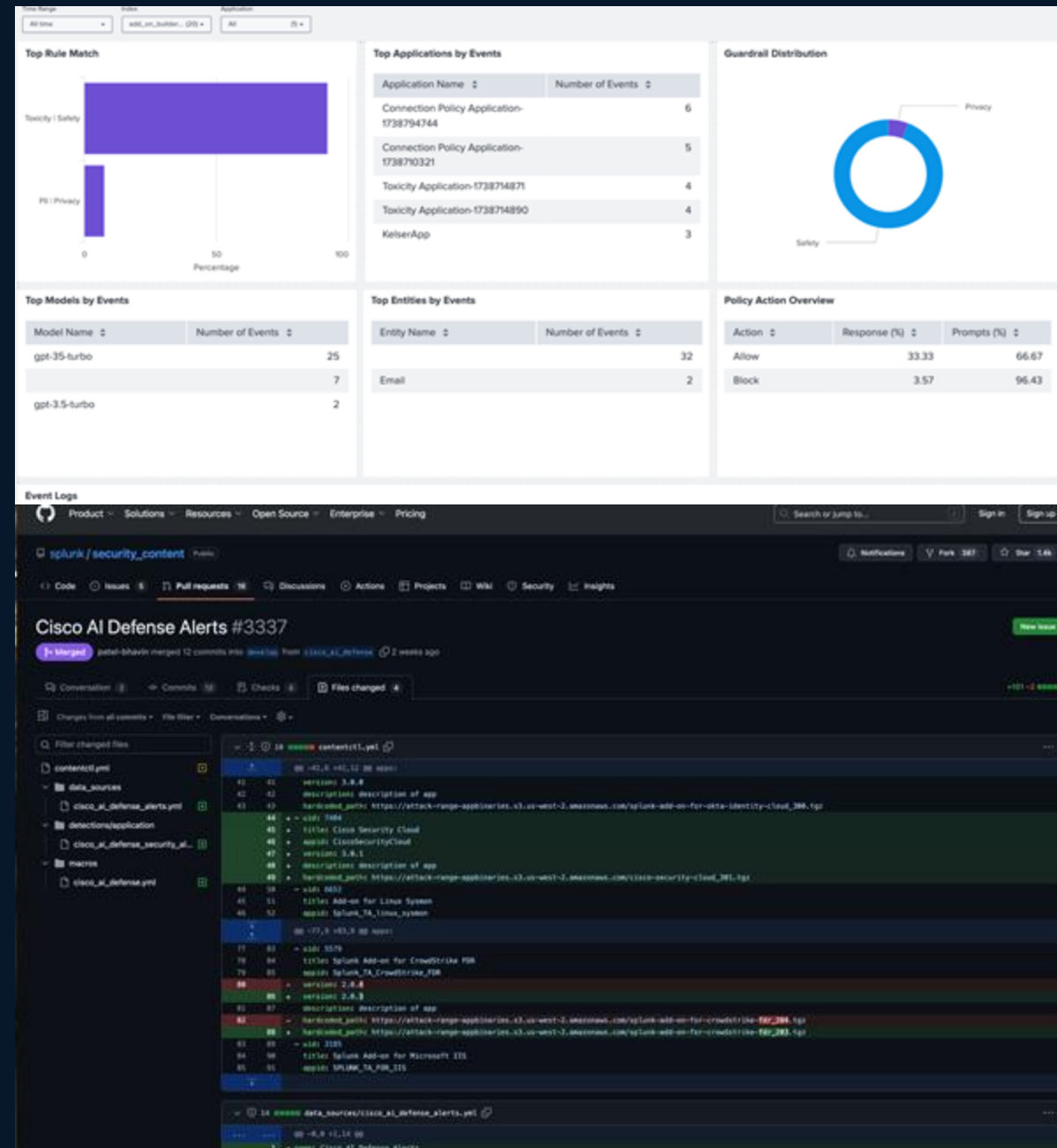
Detect and reduce AI-based
risks

*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 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

Adaptive Responses

[Talos Notable Enrichment](#)

[Notable](#)

Response	Mode	Time	User	Status
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

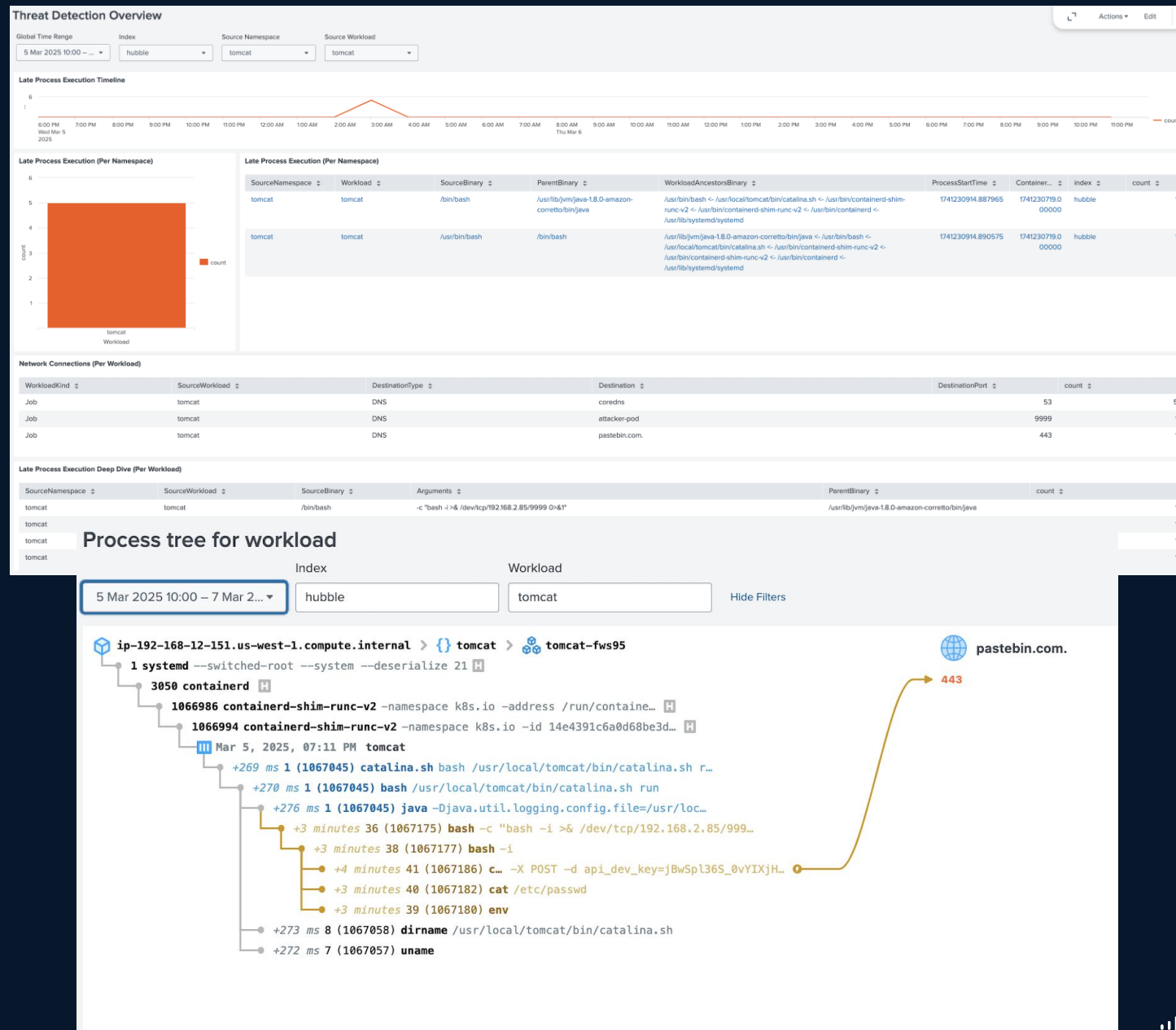
Malicious Sites Description: Sites exhibiting malicious behavior that do not necessarily fit into another, more granular, threat category.

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

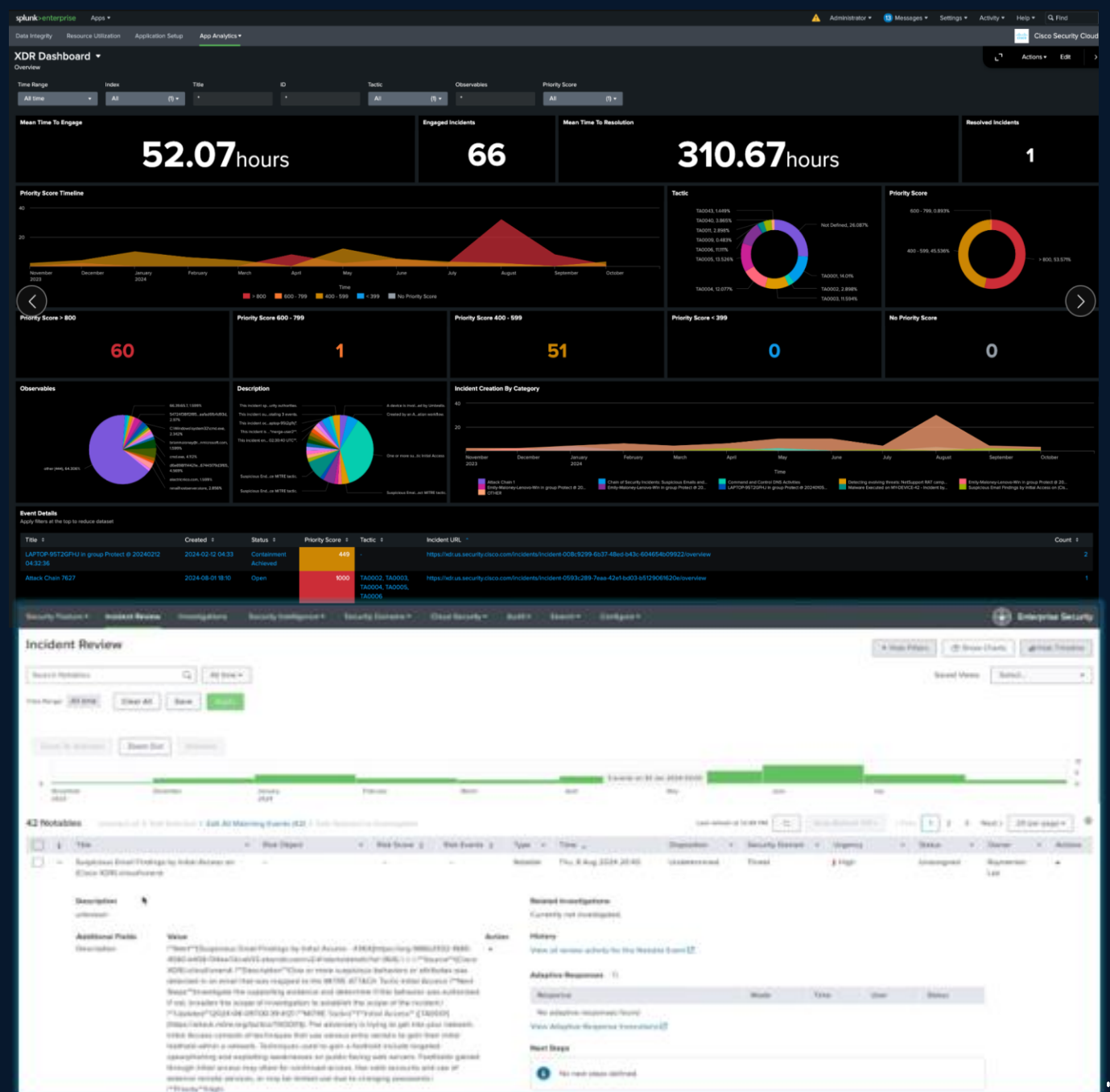
- Isovalent provides deep, kernel level runtime and network visibility into any system where the eBPF-based Tetragon agent is running on:
 - Kubernetes workloads, Linux VMs, Windows VMs
- This data supports Threat Detection and Incident Investigation Workflows via Splunk dashboards:
 - Late Process Executions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



Cisco XDR

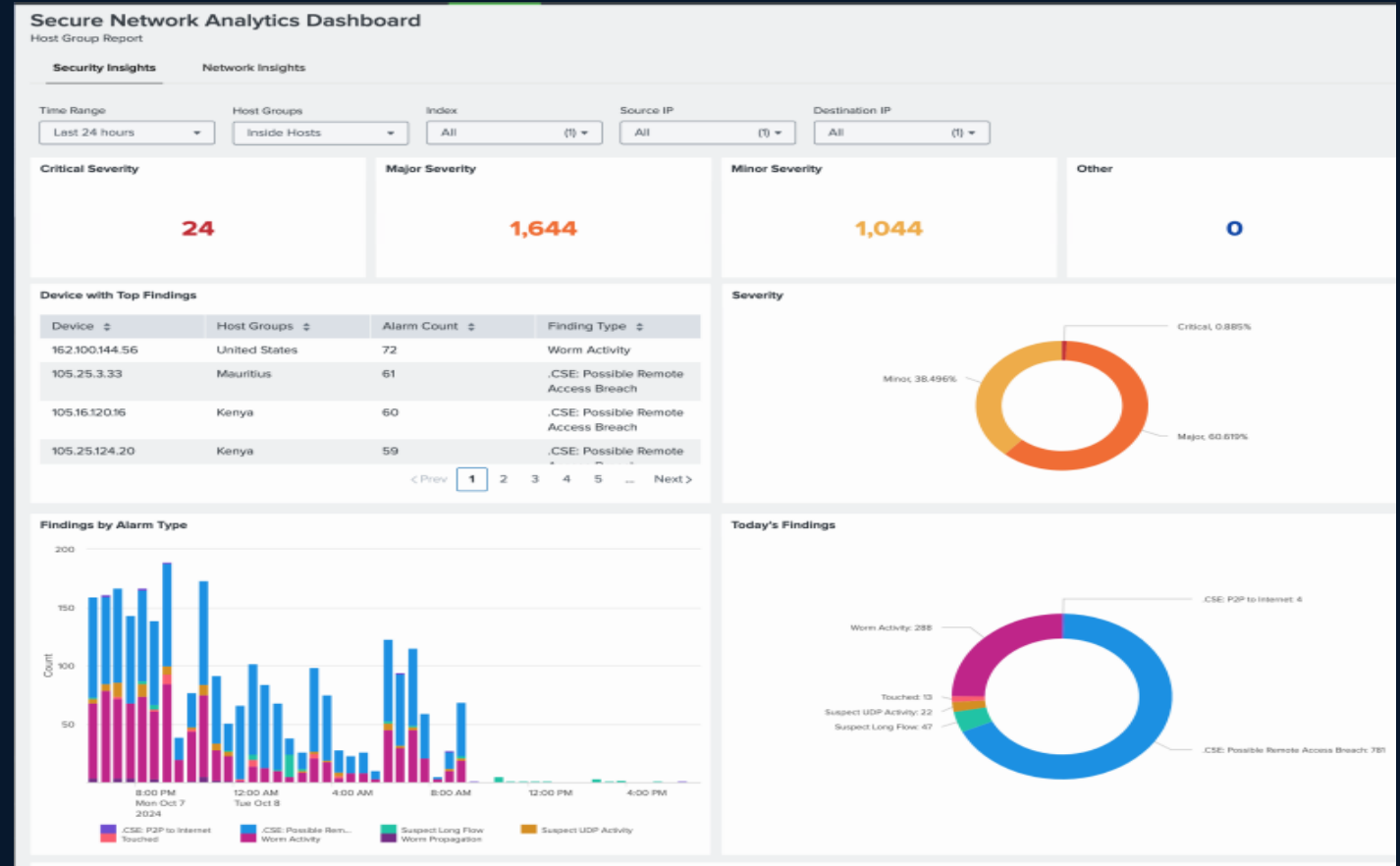
Splunk Integration

- 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



