CISCO Connect

Power the SOC of the Future with Splunk

Andrew Volkening

March 31, 2026

Agentic SOC of the Future

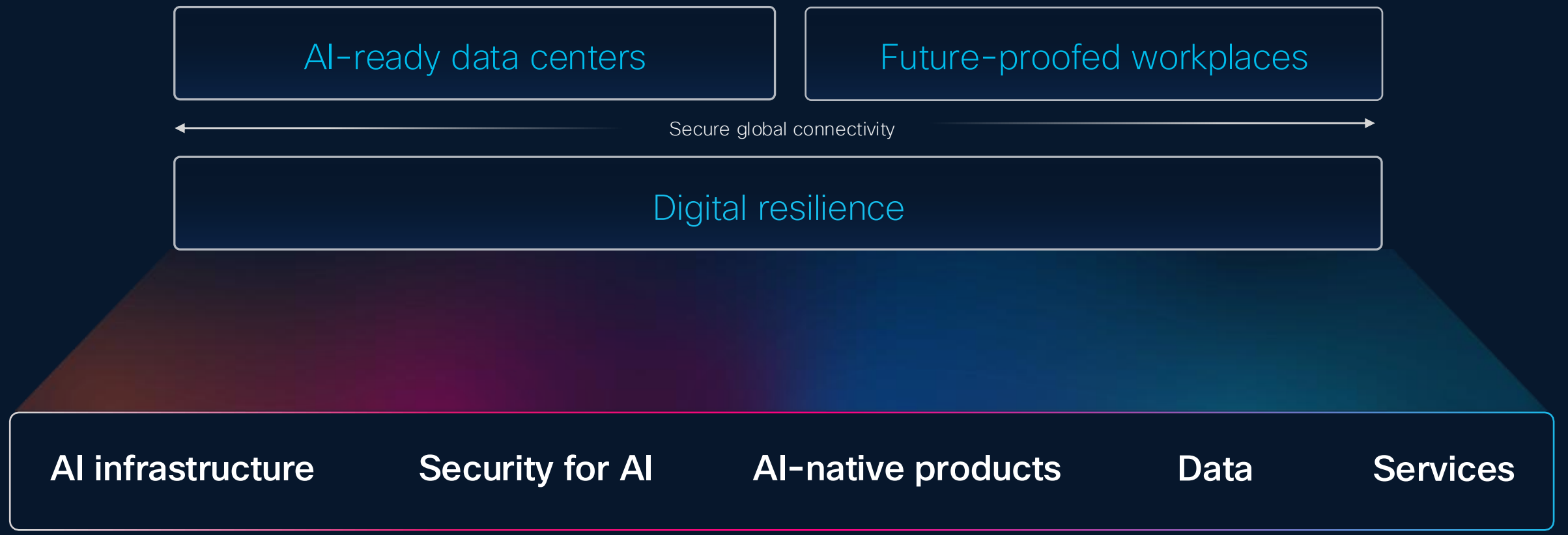
Unified Threat Detection, Investigation & Response (TDIR)

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

Cisco powers how people and technology work together across the physical and digital worlds

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

Cisco AI: Accelerating Outcomes



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

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

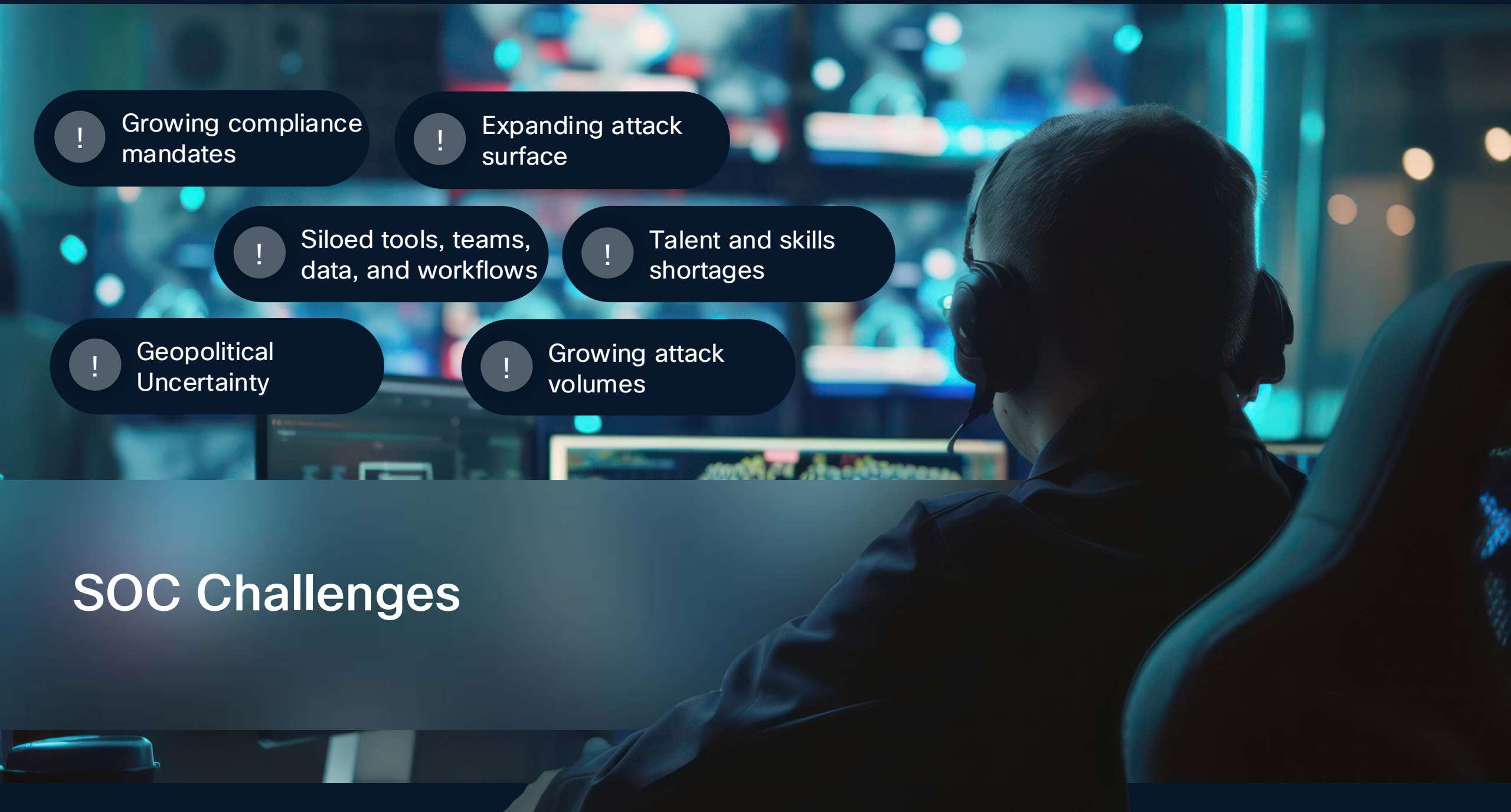
Observability

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

Security operations

Gain comprehensive threat prevention, detection, investigation, and response

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



SOC Challenges

Needs of the Resilient Modern SOC

- Complete visibility
- Context and collaboration
- Clear path to resolution
- Proactive Security Posture
- AI-powered SecOps Platform
- Extended network visibility
- Reduced complexity

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

Google

Microsoft

Amazon

Databricks

Cisco XDR

Cisco SAL

Crowdstrike

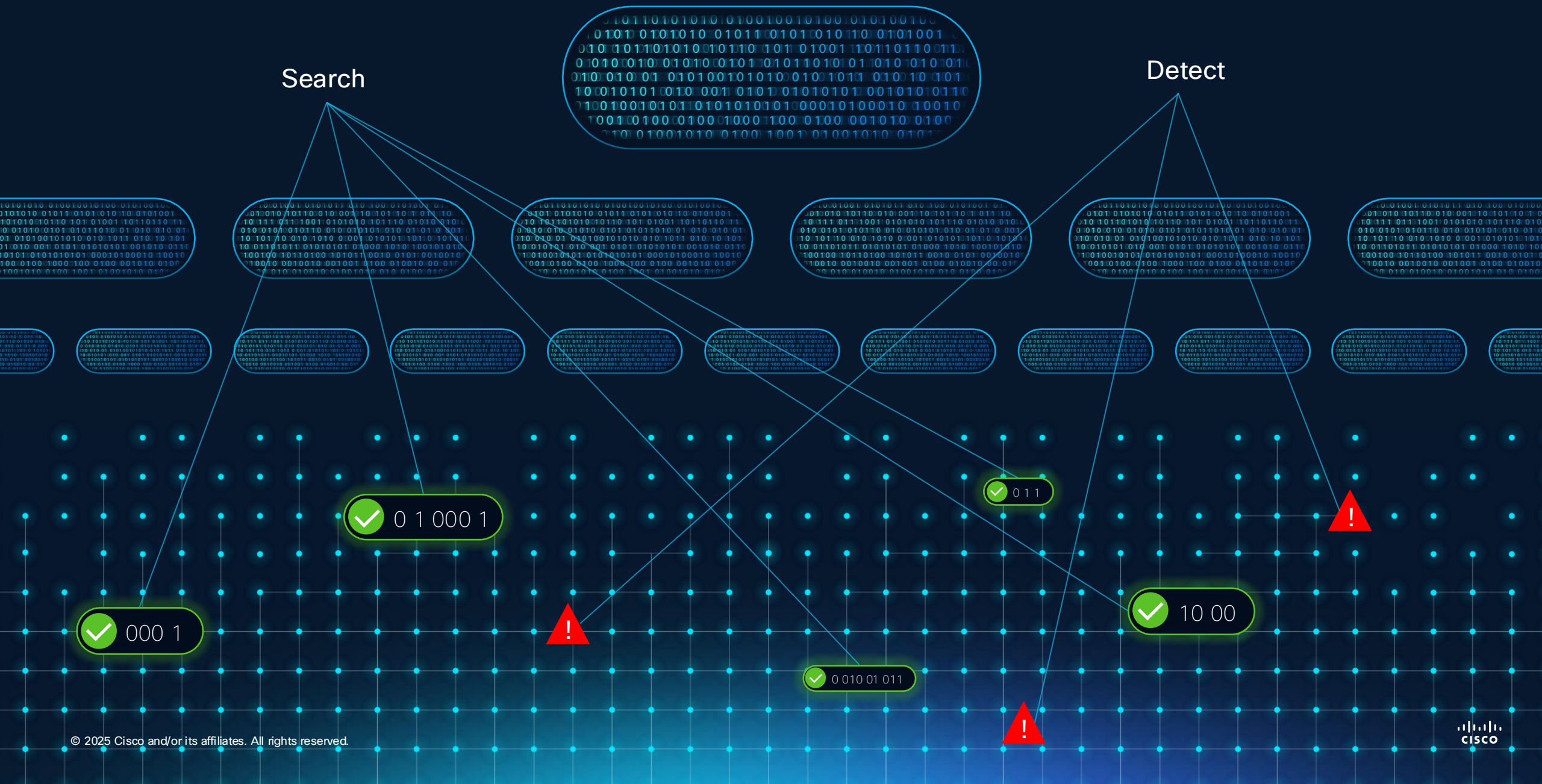
Palo Alto Networks

SentinelOne

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

cisco

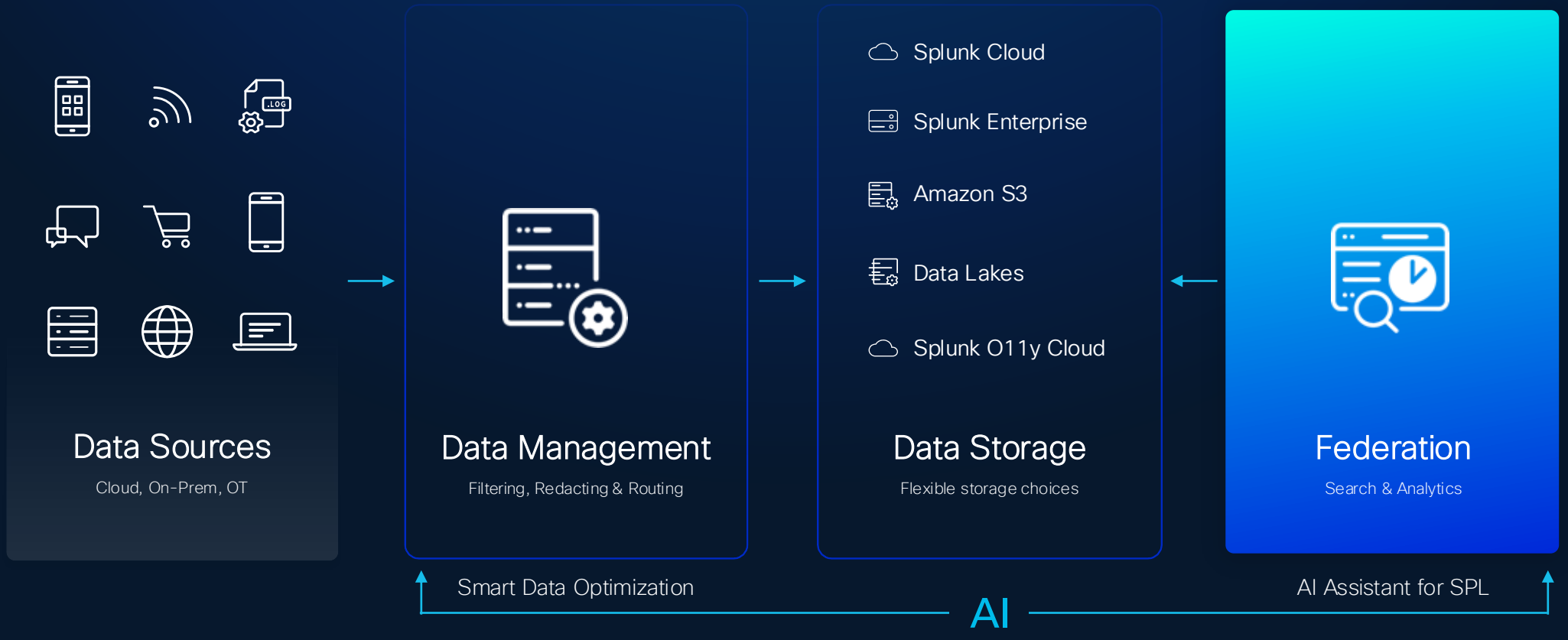
FUTURE



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

Splunk Data Management

Flexibility without sacrifice



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

Delivering More Value From Your Data

Seamless mapping to CIM

Troubleshoot data ingestion

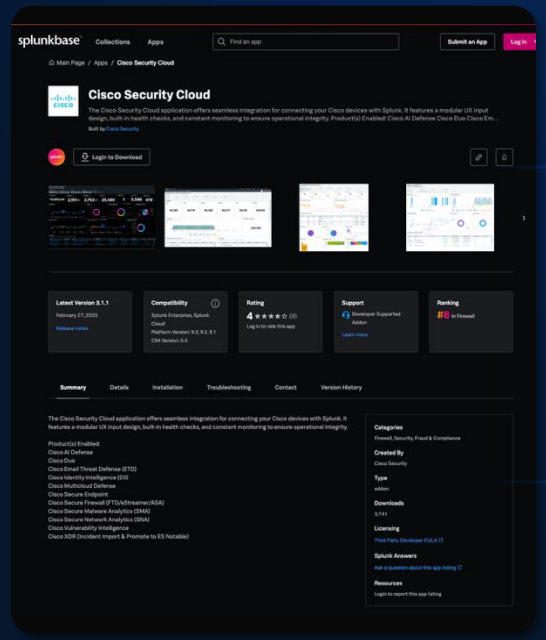
Faster time to value

Optimization of data ingestion

From Any Source

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)

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

Delivering Threat Detection, Investigation, and Response

Data Ingest

Cisco Security Cloud

AI Defense
XDR
Secure Firewall
Hypershield / Isovalent (*coming soon*)
Multicloud Defense
Secure Network Analytics
Identity Intelligence (CII)
Secure Endpoint
Secure Malware Analytics
Vulnerability Intelligence
Email Threat Defense (ETD)
Duo

Detection

Firepower Threat Defense

Unusual File Transfer Behavior
Executable Content Downloads
Blocked Connection Patterns
Anonymizing Infrastructure
Malicious Network Indicators
LOLBAS (network tools)
Malicious Behavior in Encrypted Traffic
Confirmed Exploitation Attempts Malware
File Delivery Over Web
Malicious Behavior in Encrypted Traffic

AI Defense

Investigation

Risk-based Alerting

Unusual File Transfer Behavior
Executable Content Downloads
Blocked Connection Patterns
Anonymizing Infrastructure
Malicious Network Indicators
LOLBAS (network tools)
Malicious Behavior in Encrypted Traffic
AI Defense

Cisco Talos

Response

Secure Firewall

Secure Malware Analytics + Attack Analyzer

WebEx (war room scenarios)

Cisco Talos

NEW

Security Insight, on Us

Firewall Logs at no additional cost in Splunk*

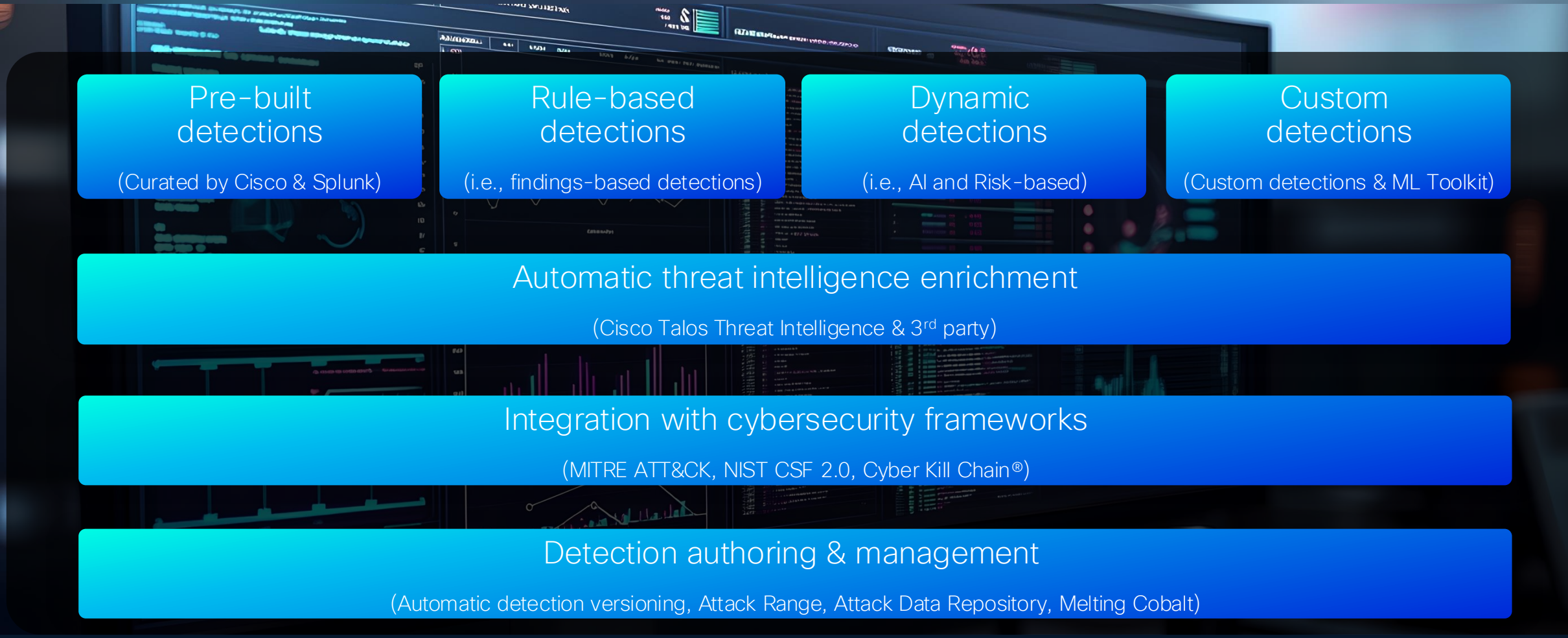
AVAILABLE
AUGUST 2025

New detections | Automated response

*Cisco Firepower (FTD) firewalls are entitled to 5GB of Splunk logging capacity with purchase or equivalent for SVC or vCPU

SOC of the Future

Comprehensive Detection Approach

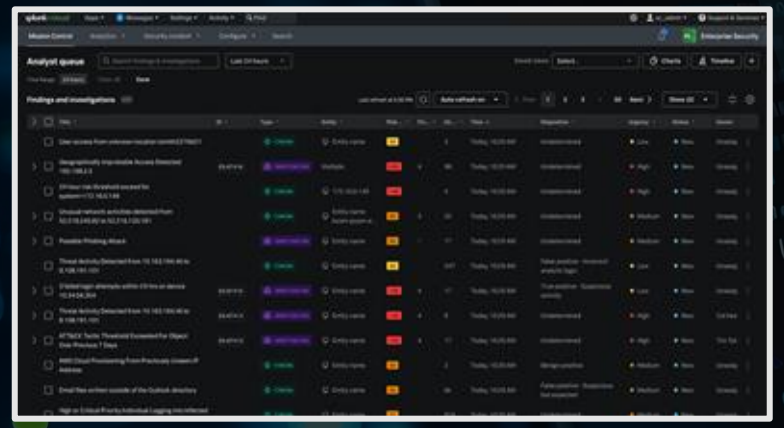


© 2025 Cisco and/or its affiliates. All rights reserved.

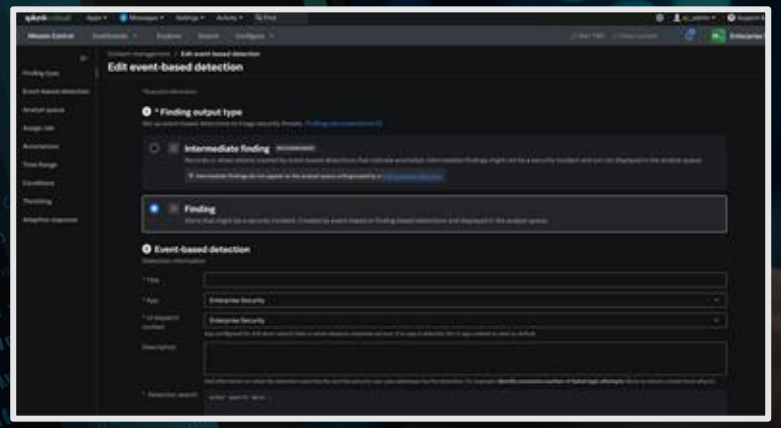
SOC of the Future

Unified Investigation Experience

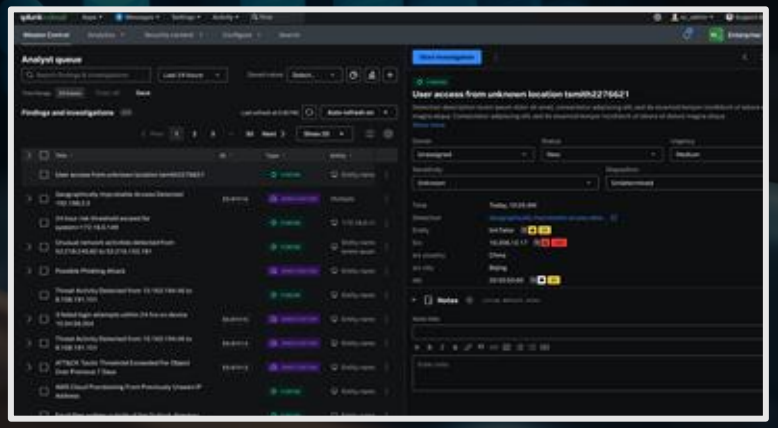
Unified
Analyst Queue



Prioritized
Risk Insights



Unified
Investigation View



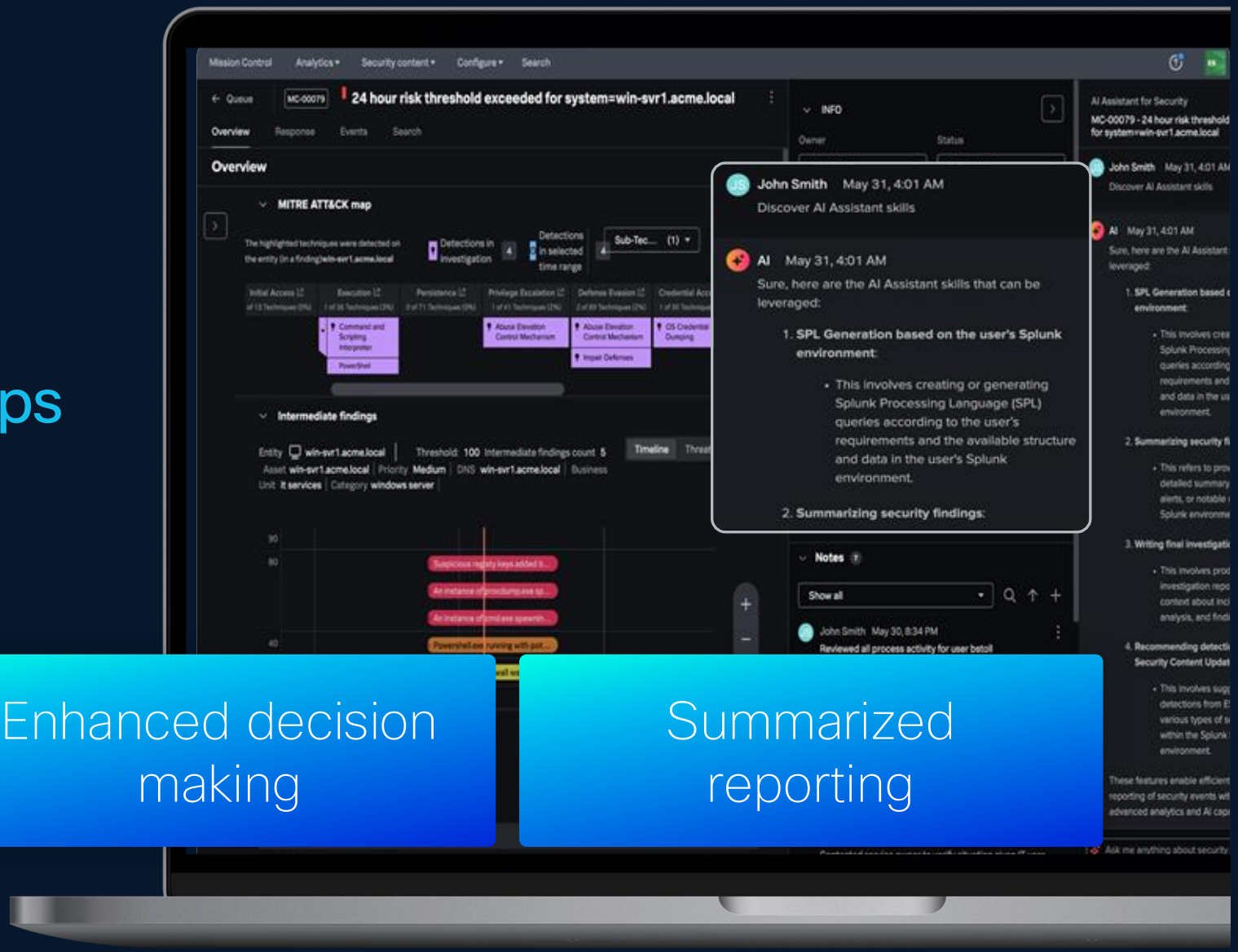
ANALYST
EXPERIENCE

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

SOC of the Future

Investigate at Machine Scale

Splunk's AI Assistant helps supercharge your workflows



Guided response and recommendations

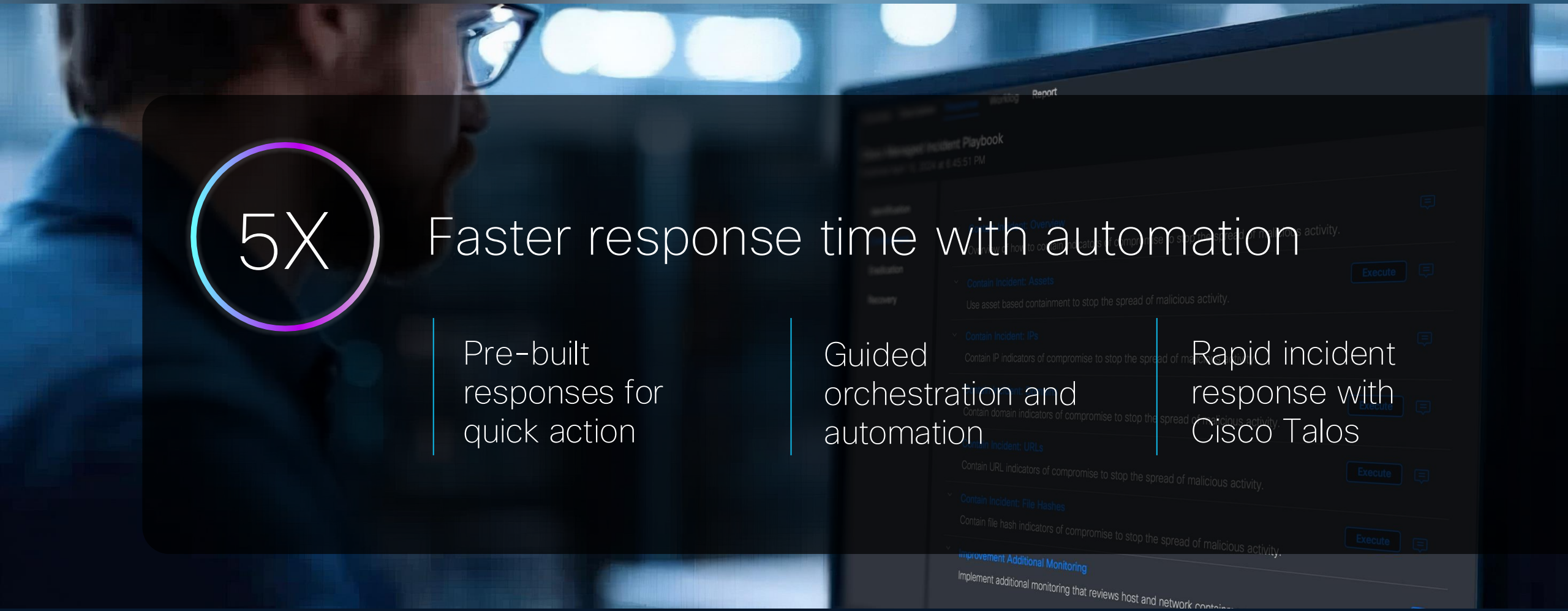
Enhanced decision making

Summarized reporting

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

SOC of the Future

Automated Response



5X

Faster response time with automation

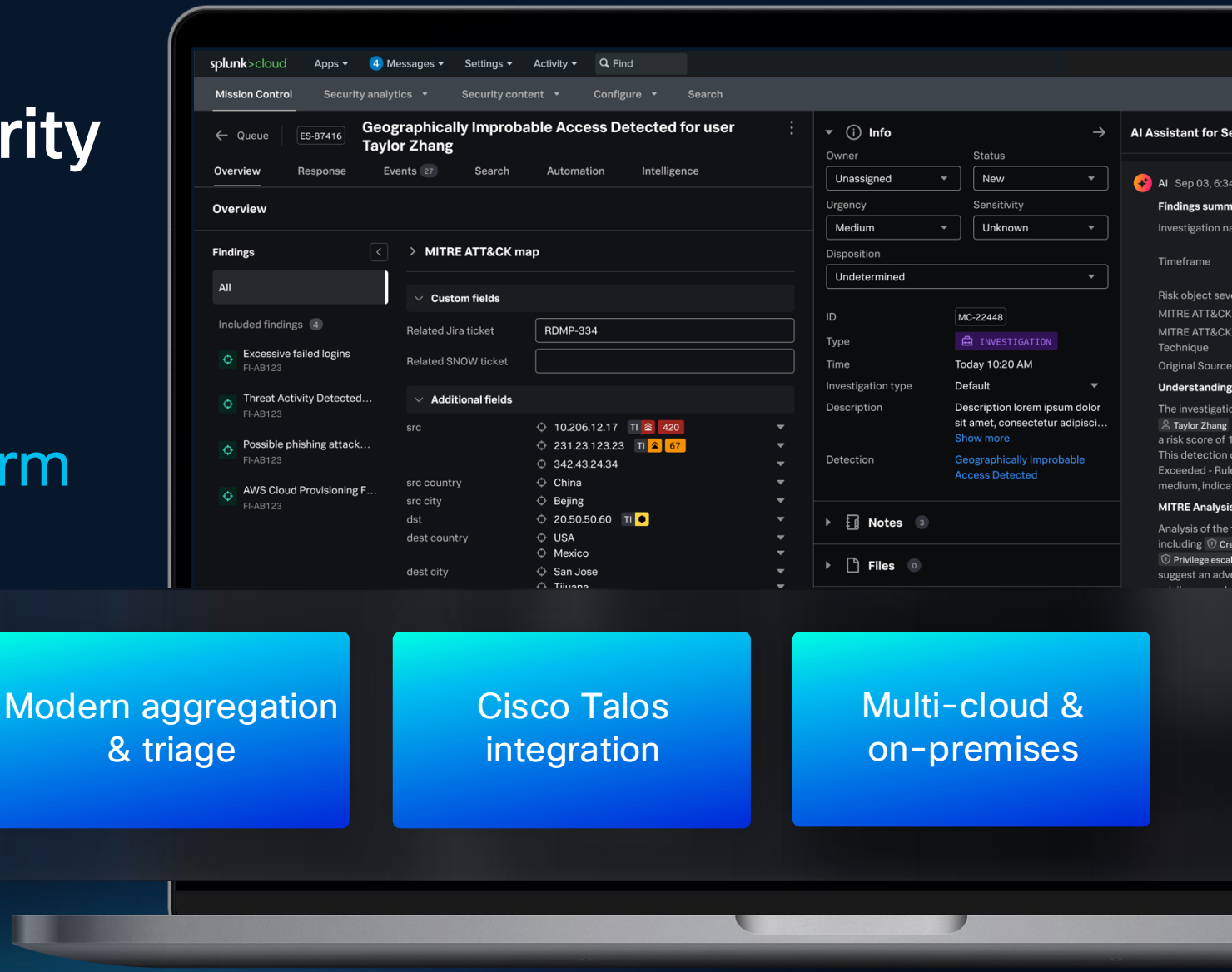
- Pre-built responses for quick action
- Guided orchestration and automation
- Rapid incident response with Cisco Talos

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

SOC of the Future

Splunk Enterprise Security

Market-leading AI-powered SecOps Platform



Natively integrated SOAR

Enhanced detection

Modern aggregation & triage

Cisco Talos integration

Multi-cloud & on-premises

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

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.

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

Agentic SOC of the Future

Unified Threat Detection, Investigation & Response (TDIR)

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

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

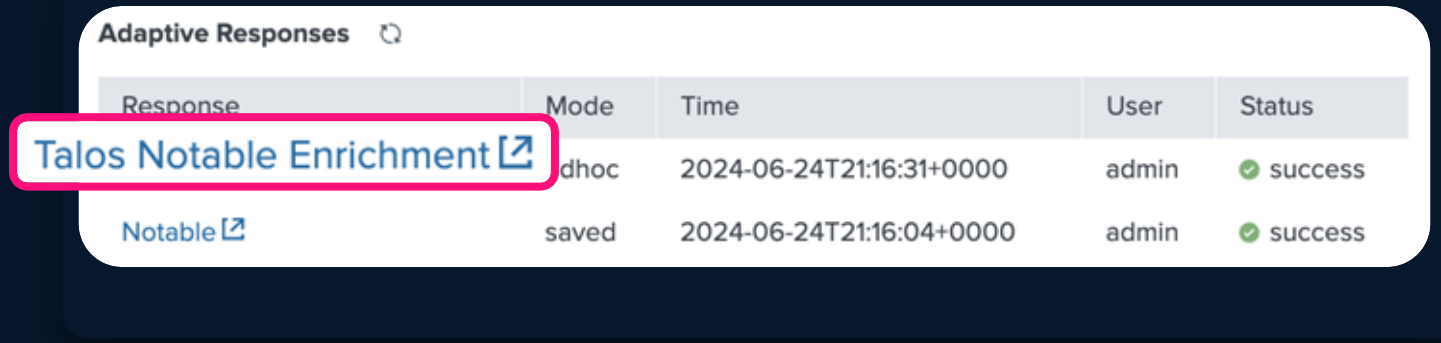
Splunk +
Cisco AI Defense

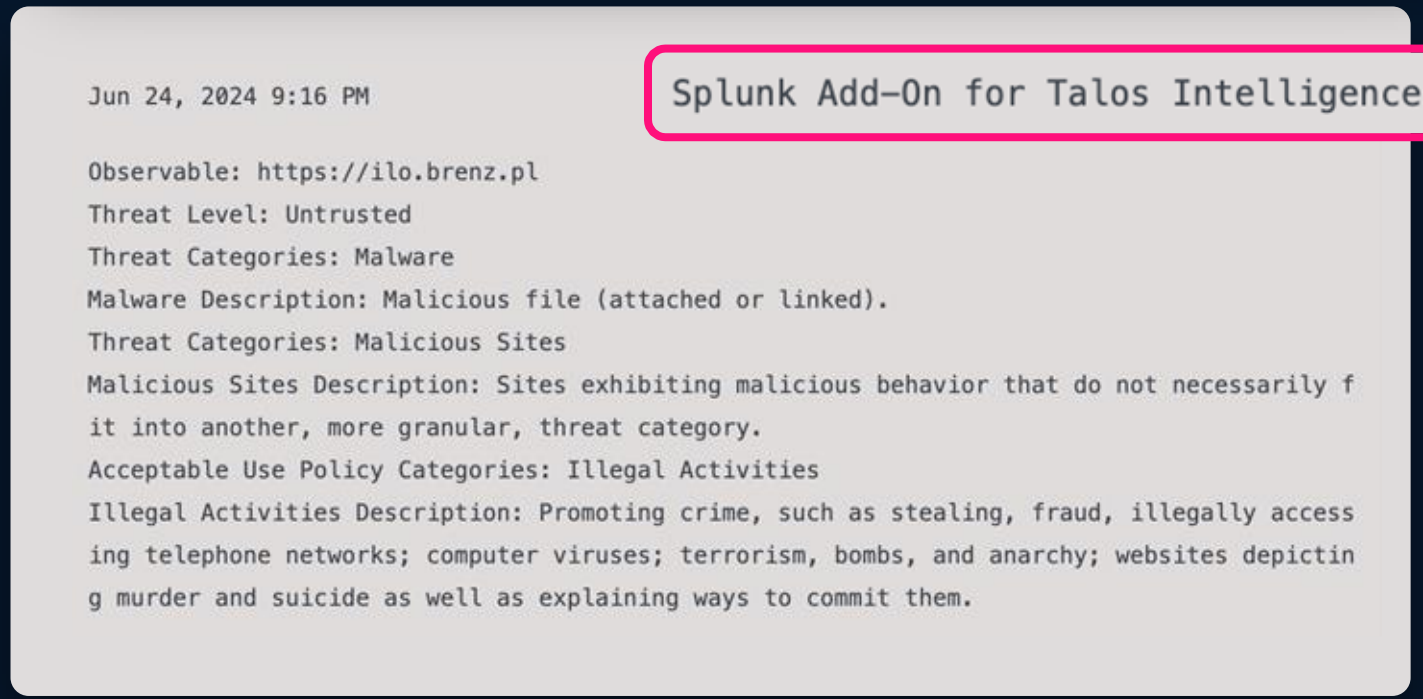
© 2025 Cisco and/or its affiliates. All rights reserved.

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





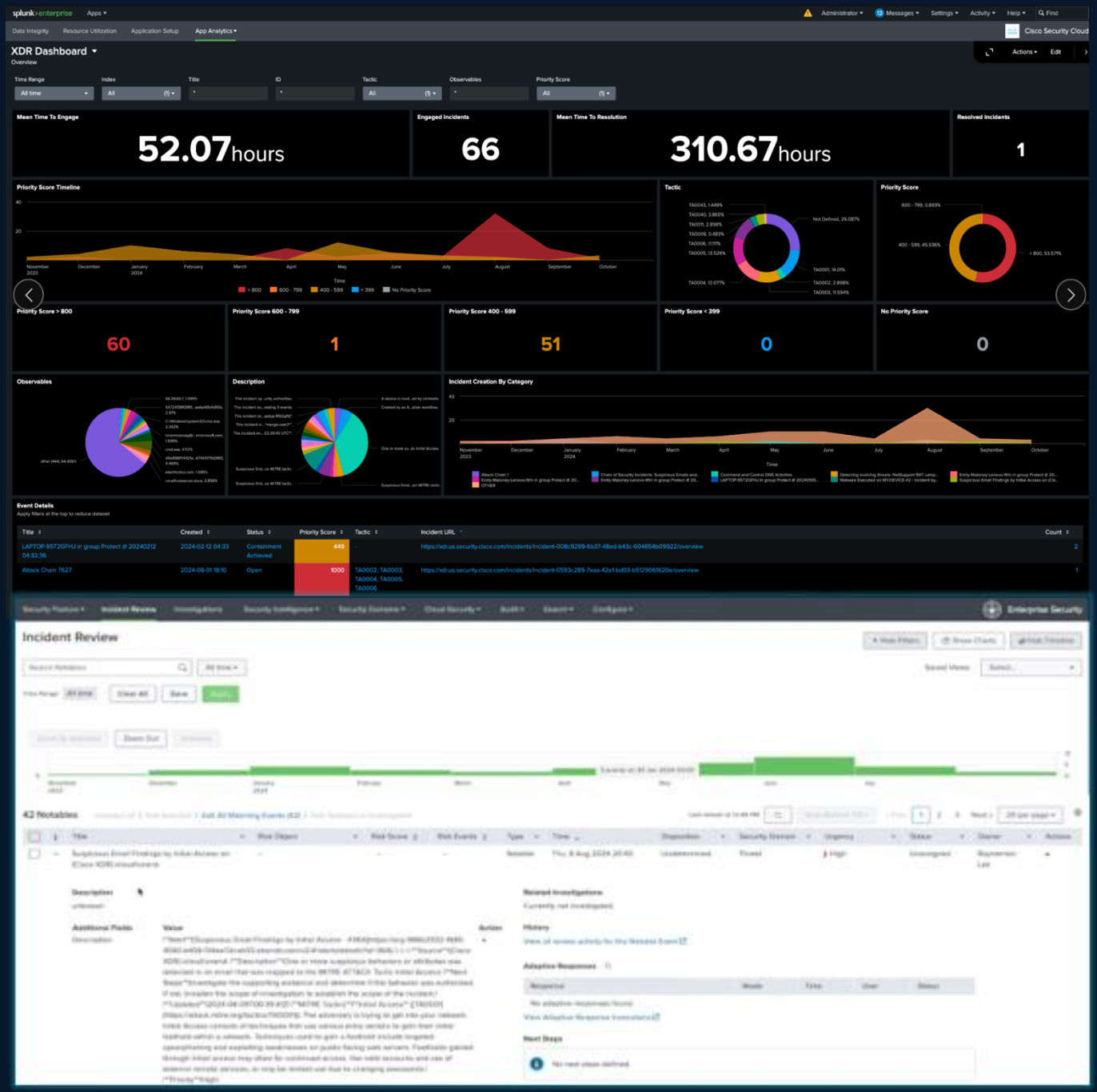
© 2025 Cisco and/or its affiliates. All rights reserved.

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.

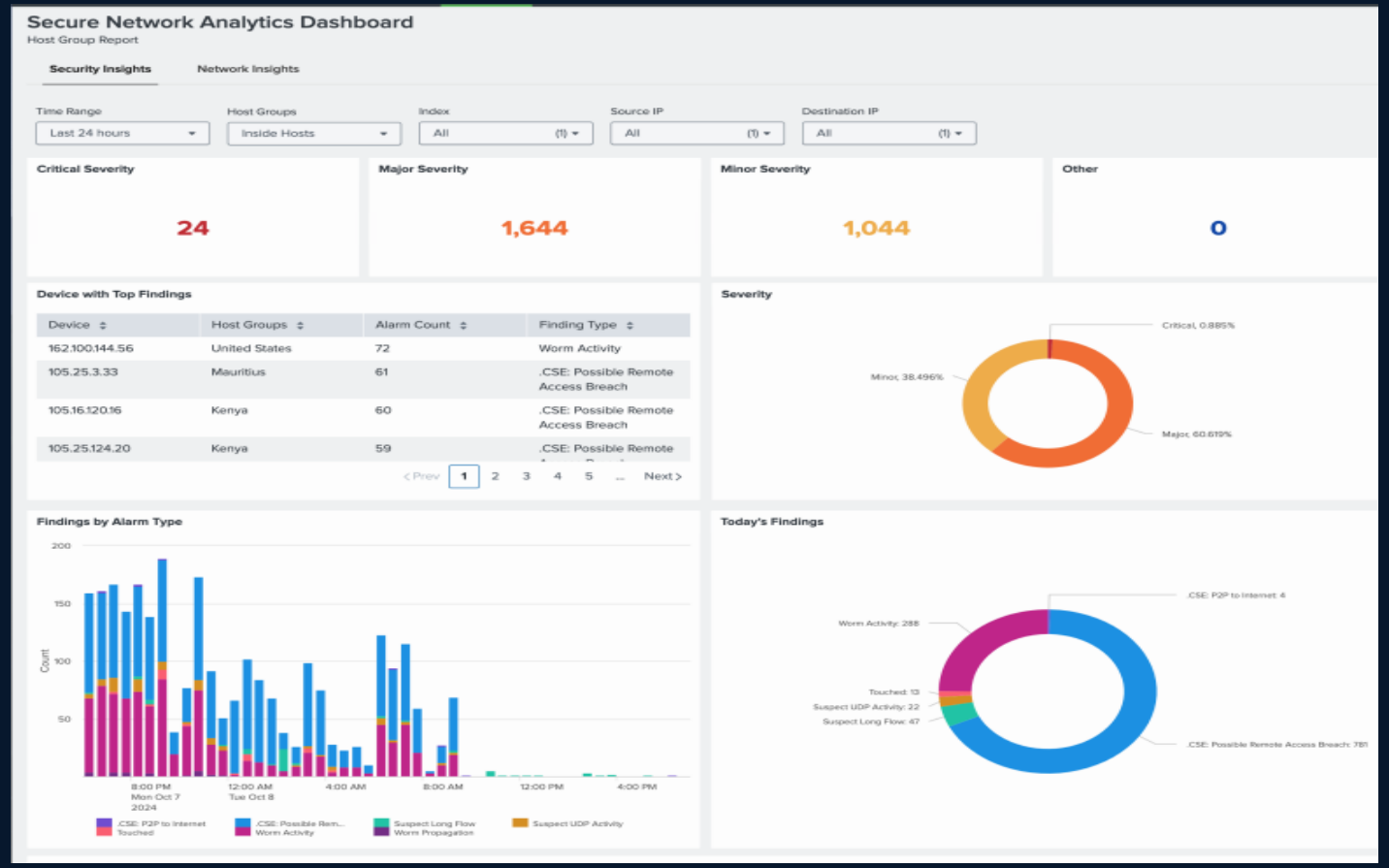


© 2025 Cisco and/or its affiliates. All rights reserved.

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



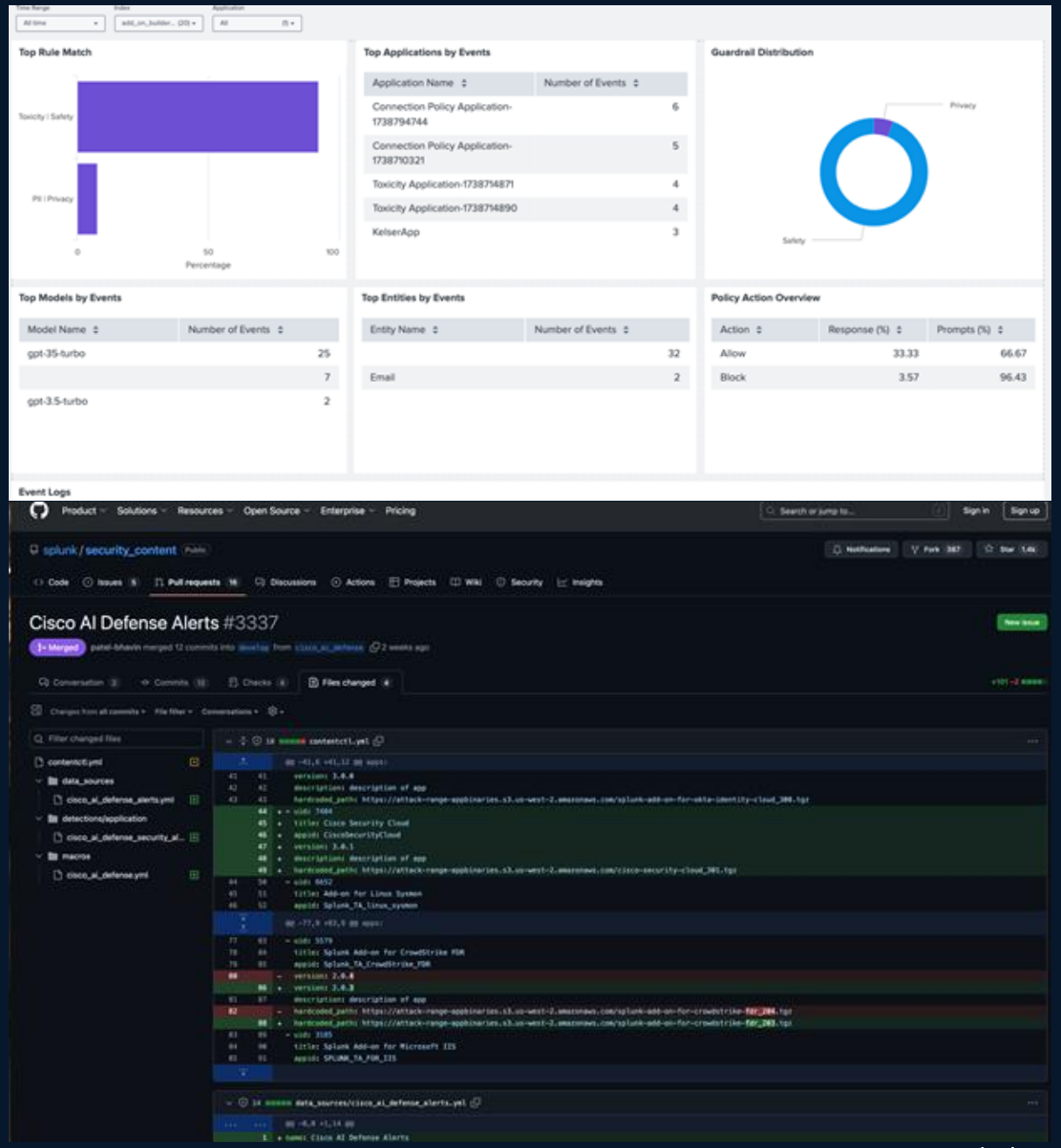
© 2025 Cisco and/or its affiliates. All rights reserved.

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, 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.

Let’s Build the SOC of the Future Together

CISCO Connect

Thank you


CISCO