CISCO Engage | Tech Day

# Detect. Investigate. Respond: How SOCs are the new UP Link


Danny Rodriguez
Security Solutions Engineer

Michael Pearson
Security Solutions Engineer

8 October 2025

# Agenda

01 Introduction

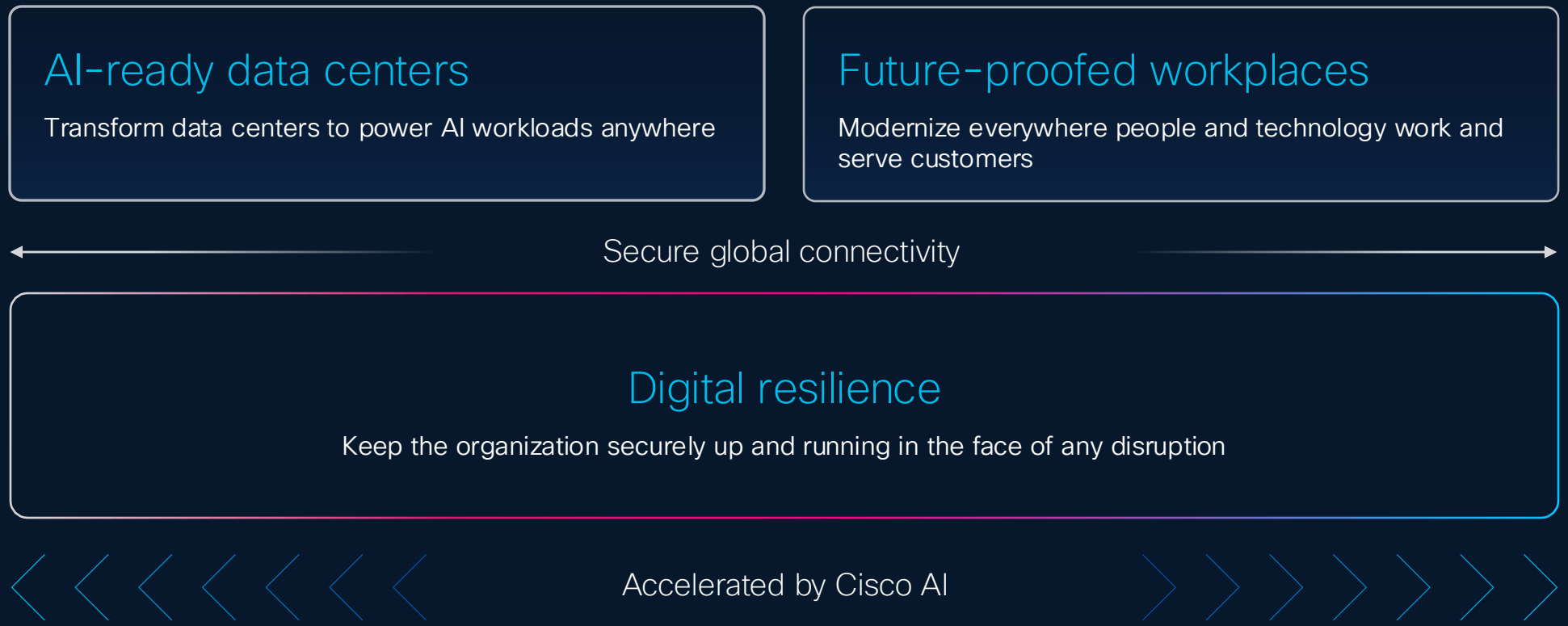
02 SOC Challenges

03 Becoming Resilient

04 SOC of the Future

05 Agentic SOC

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



# 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

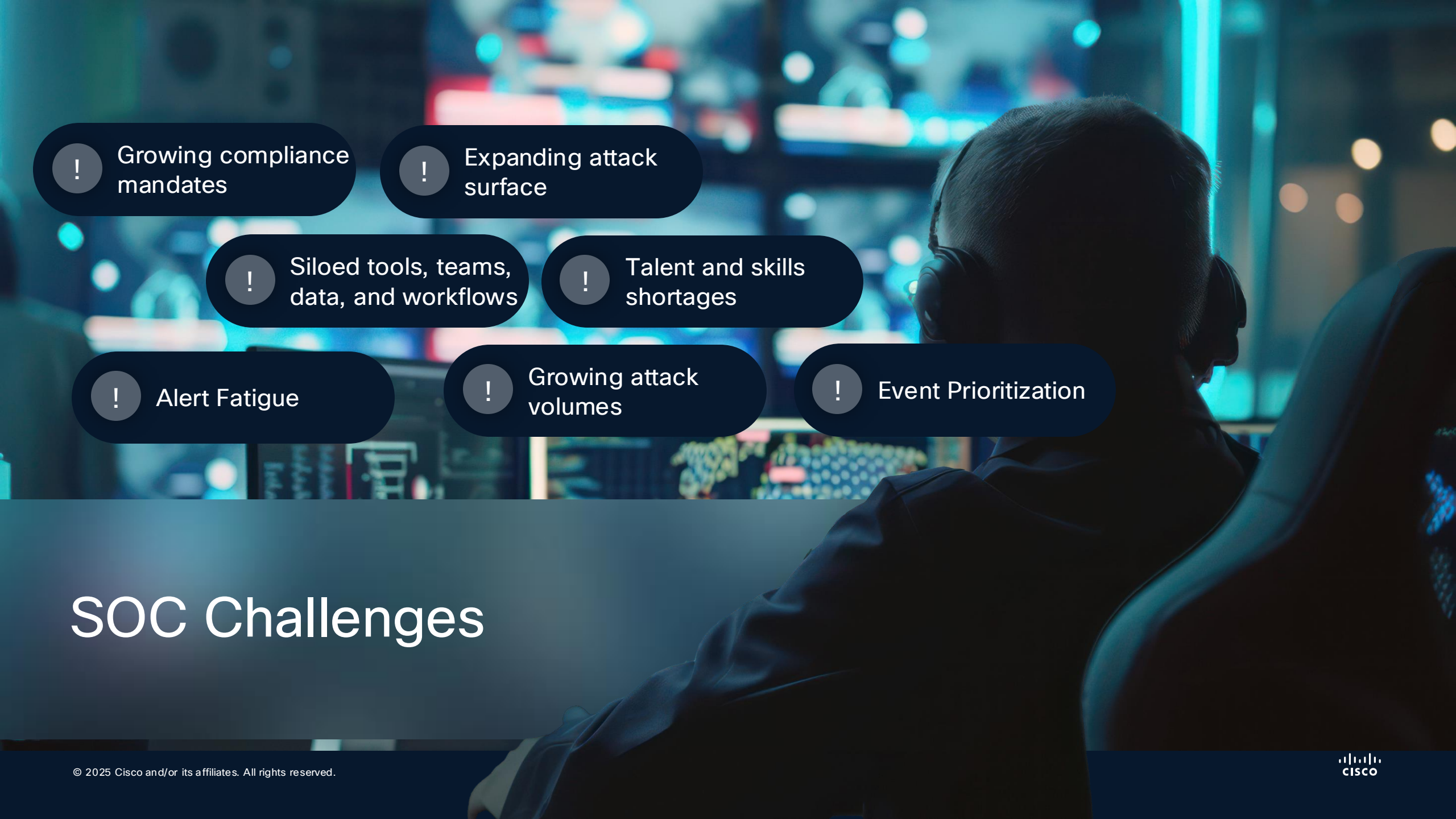
Prevent downtime and optimize experiences with complete visibility and insights across services

### Security operations

Gain comprehensive threat prevention, detection, investigation, and response



cisco



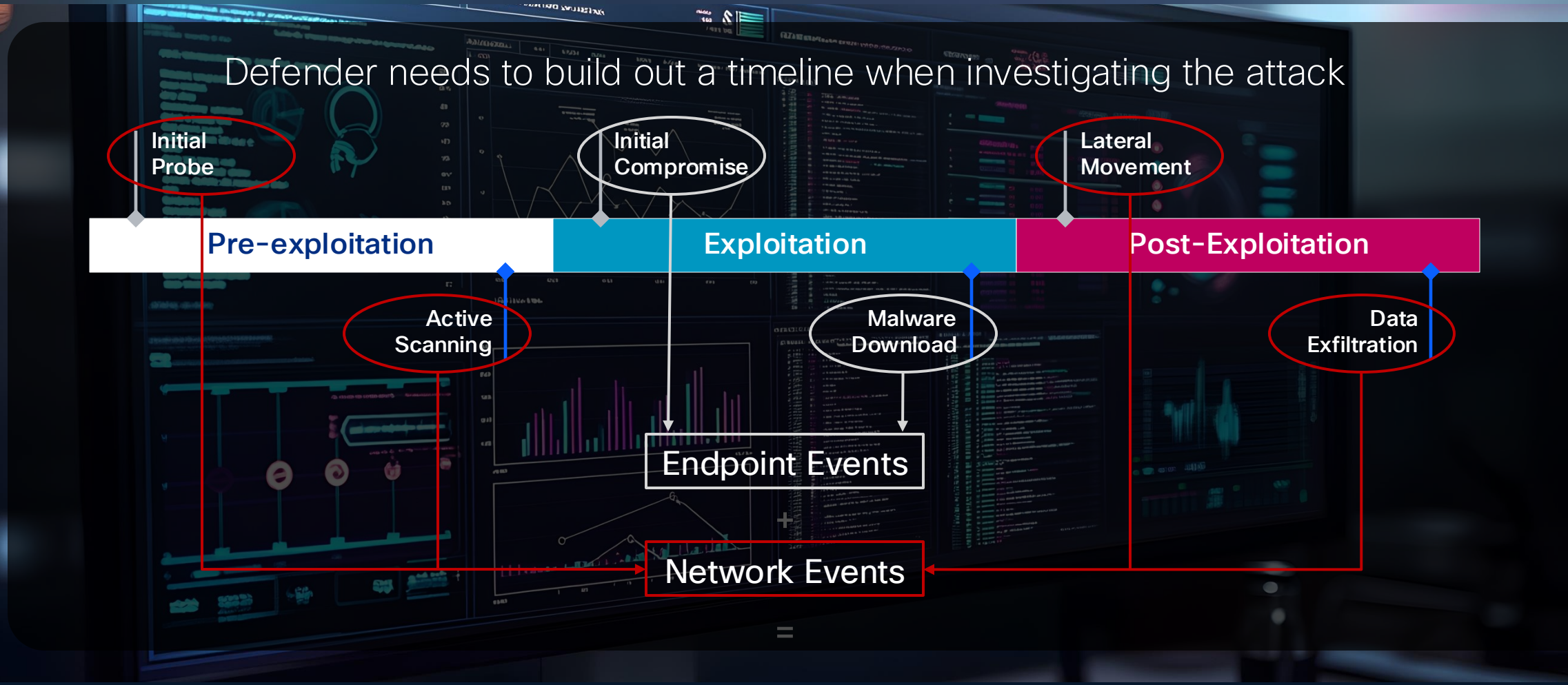

# SOC Challenges

# Needs of the resilient modern SOC

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

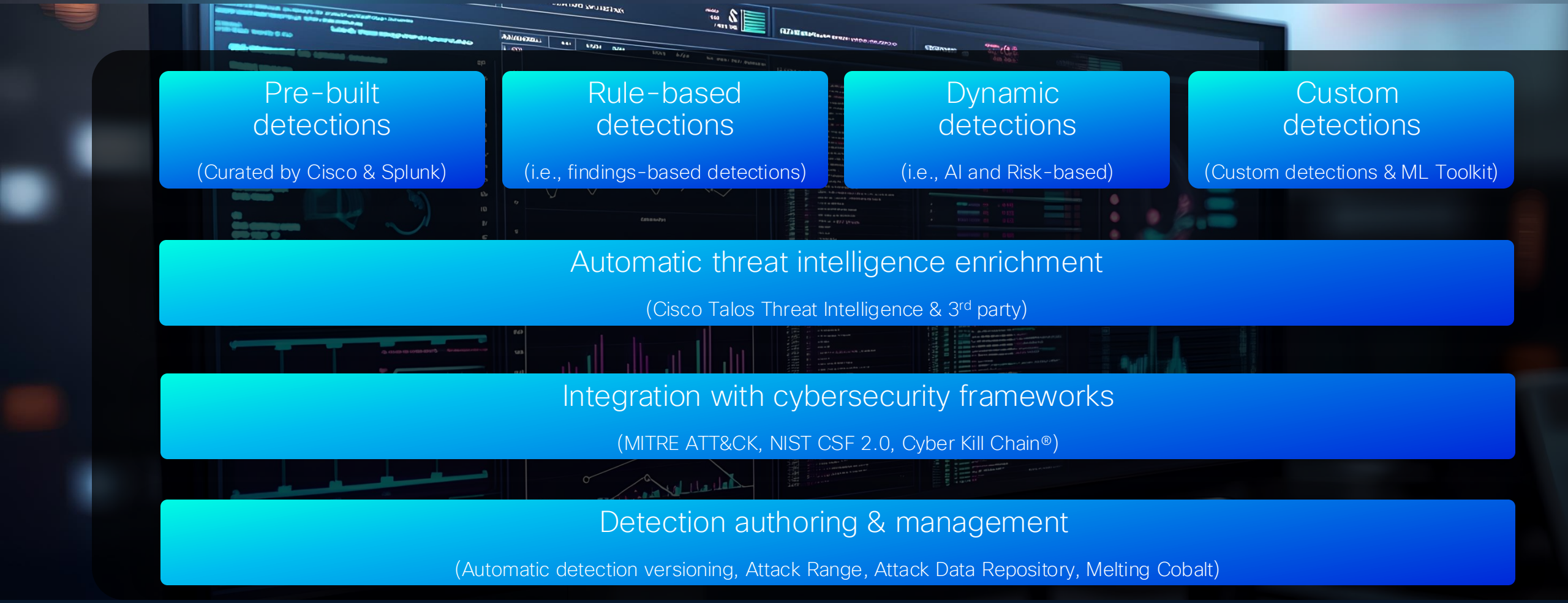
SOC of the future

# For completeness, you need the network



SOC of the future

# Comprehensive detection approach



**Pre-built detections**
(Curated by Cisco & Splunk)

**Rule-based detections**
(i.e., findings-based detections)

**Dynamic detections**
(i.e., AI and Risk-based)

**Custom detections**
(Custom detections & ML Toolkit)

**Automatic threat intelligence enrichment**
(Cisco Talos Threat Intelligence & 3rd party)

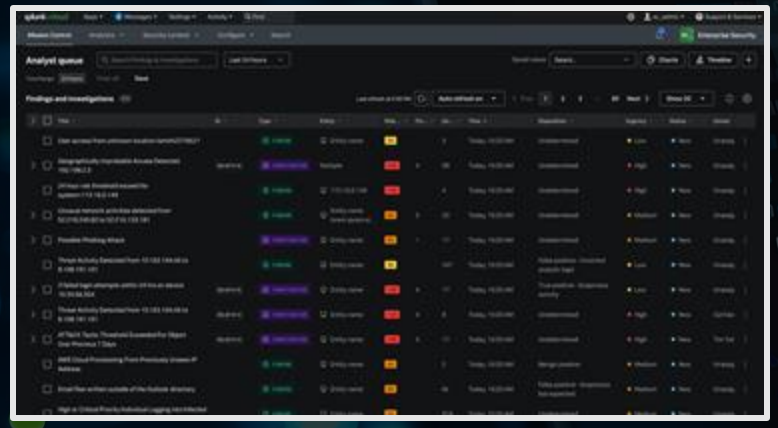
**Integration with cybersecurity frameworks**
(MITRE ATT&CK, NIST CSF 2.0, Cyber Kill Chain®)

**Detection authoring & management**
(Automatic detection versioning, Attack Range, Attack Data Repository, Melting Cobalt)

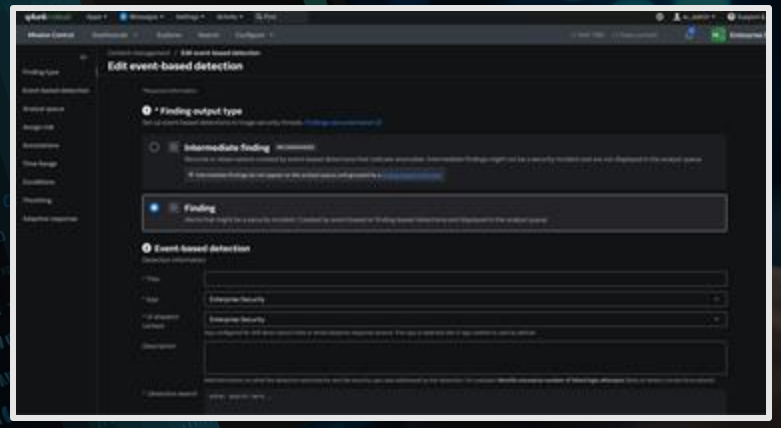
SOC of the future

# Splunk–Unified investigation experience

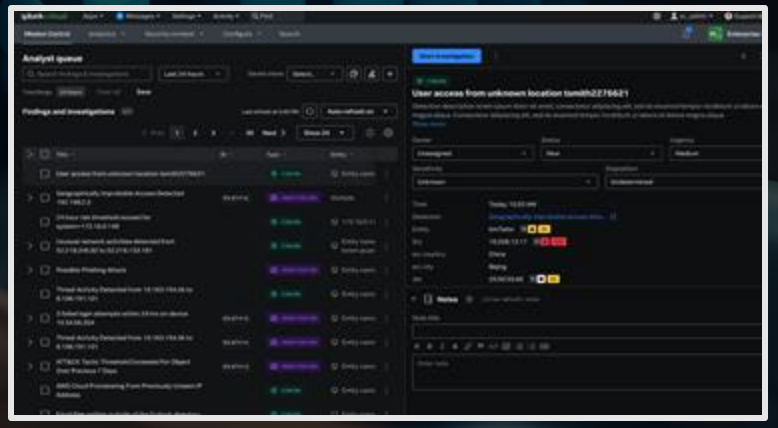
Unified
Analyst Queue



Prioritized
Risk Insights



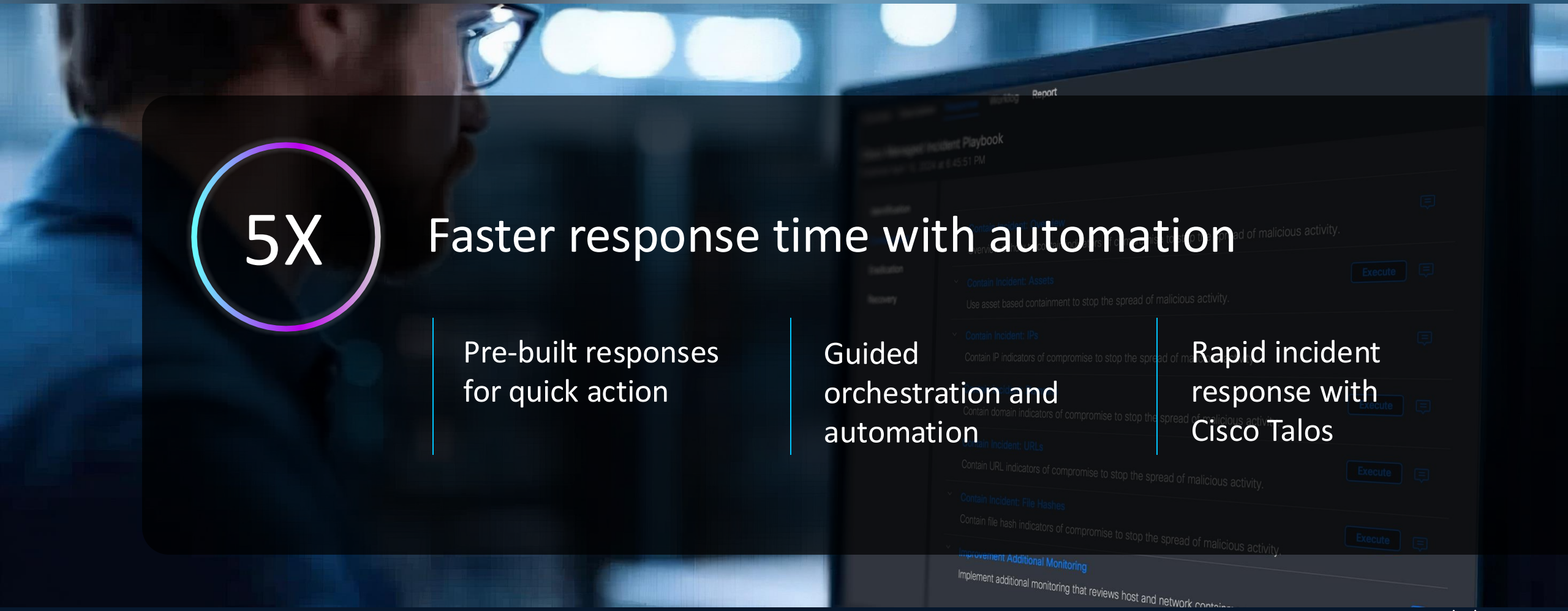

Unified
Investigation View



ANALYST
EXPERIENCE

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



cisco

# Agentic SOC of the Future

## Unified Threat Detection, Investigation & Response (TDIR)

**Cisco XDR**
Real-time Attack Detection

**Splunk Enterprise Security**
Security Analytics

**Splunk SOAR**
Security Automation

AGENTIC AI

**Splunk Platform**
Data Management and Federation

CONTENT AND THREAT RESEARCH

**Cisco Security Cloud**


Identity


Firewall


Talos


SSE


& more


Third-party tools


Clouds


Endpoints

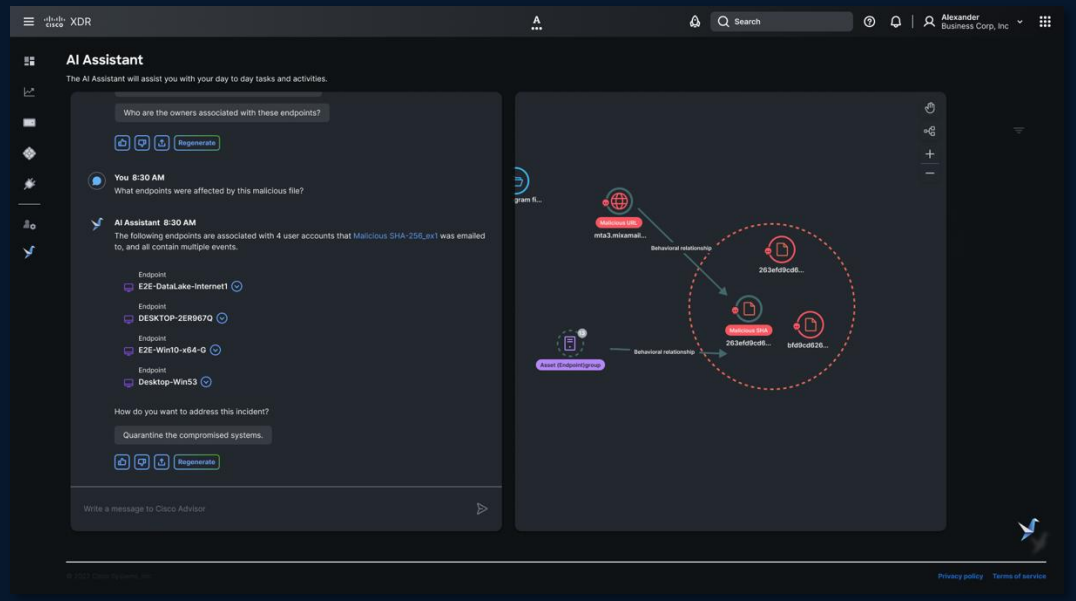

Data centers


Applications



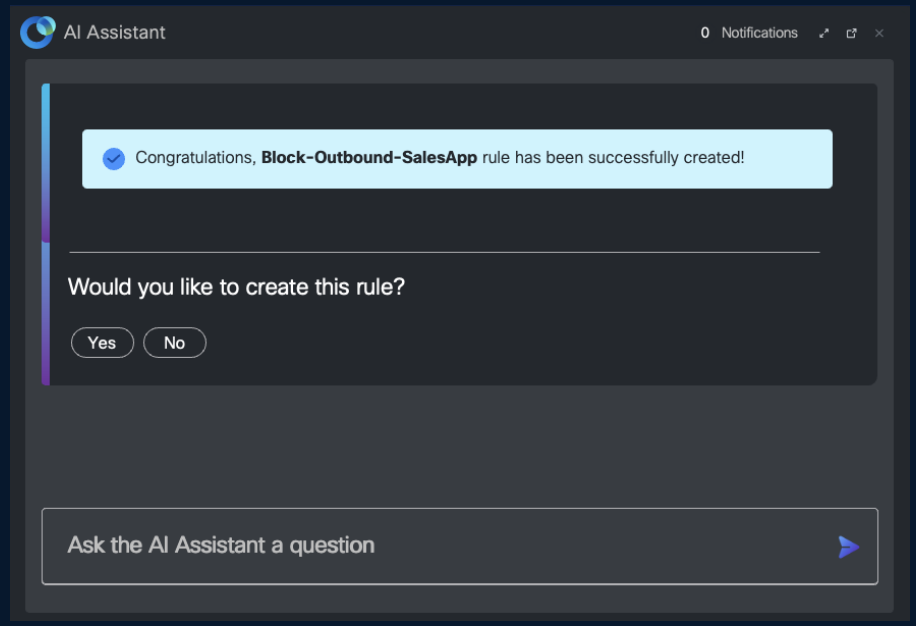
cisco

# AI Assistant




1 Detects a phishing attack that has setup a C&C and is exfiltrating data outside the network.

2 AI Assistant in XDR allows Incident Responder to request a firewall rule to be added.




3 Block any outbound exfiltration to the IP address identified from the C&C.

# Cisco XDR – Agentic AI

## Clear verdict. Decisive action. AI speed.

### Instant Attack Verification

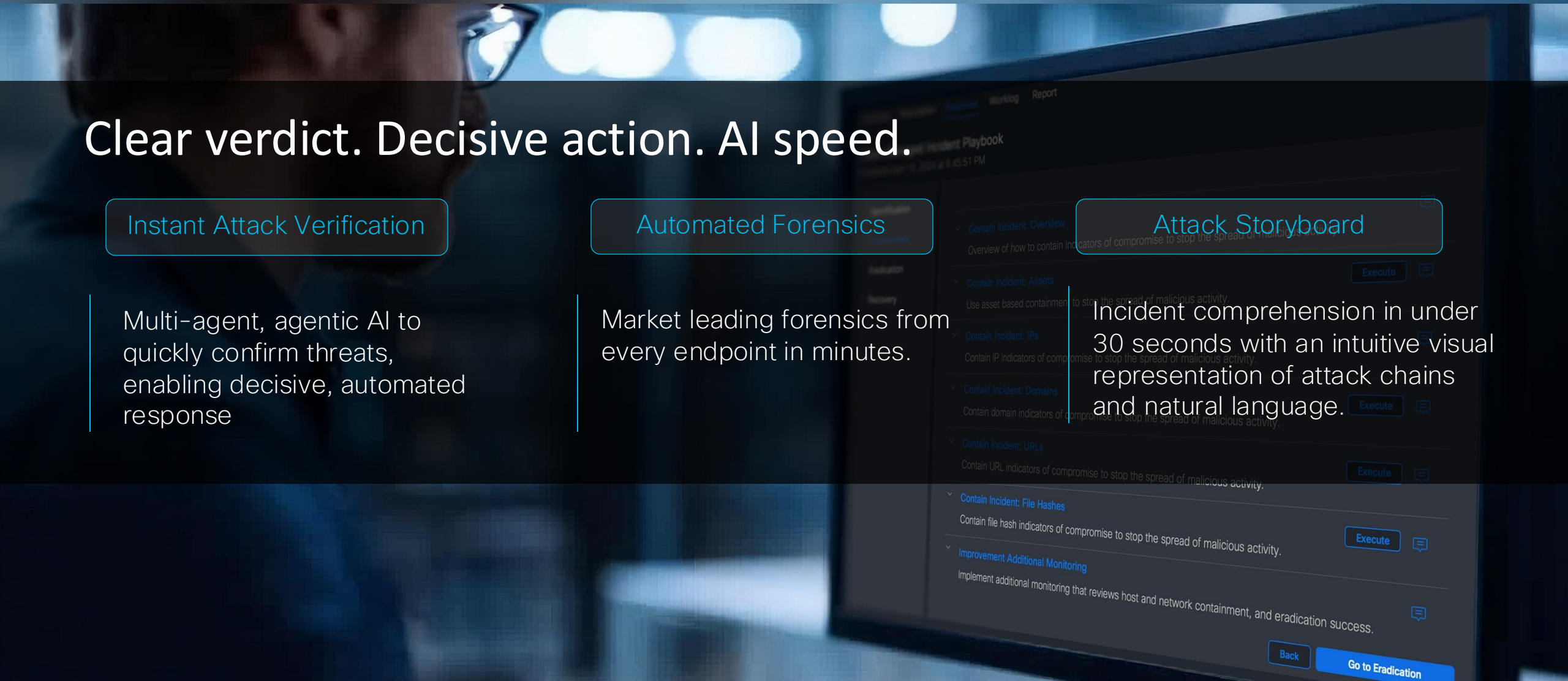
Multi-agent, agentic AI to quickly confirm threats, enabling decisive, automated response

### Automated Forensics

Market leading forensics from every endpoint in minutes.

### Attack Storyboard

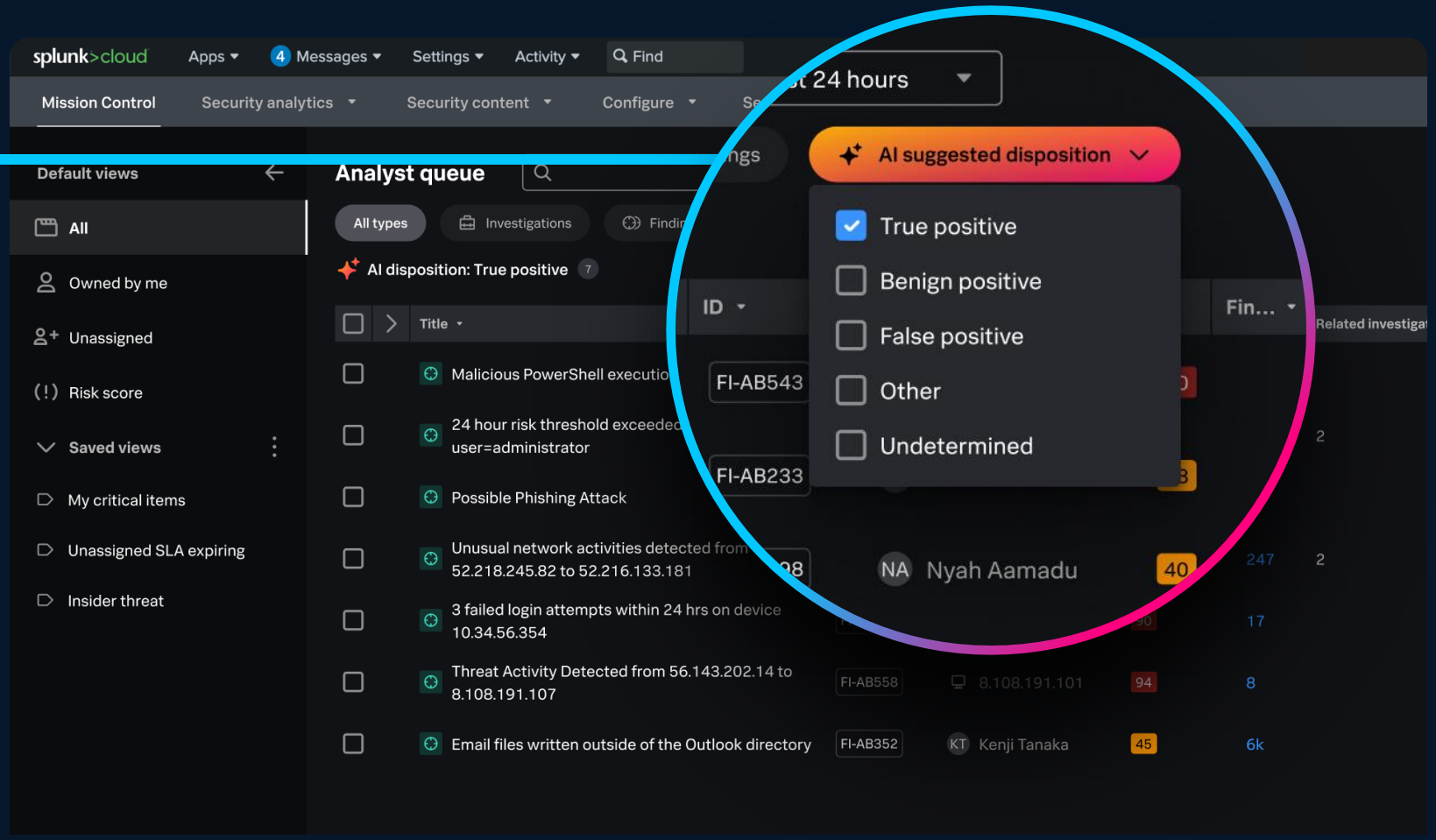
Incident comprehension in under 30 seconds with an intuitive visual representation of attack chains and natural language.



# Splunk– Agentic AI ** Alpha Early 2026

## Triage Agent

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



# Let’s build the SOC of the future together

# Thank you


CISCO