

Unify Security Operations with Splunk

CISCO Live !

Leveraging Enterprise Security, SOAR, SAA and ARI

Kacie Osora
Security Solutions Architect, Splunk

Simon O'Brien
Security Specialist, Splunk

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-1542>

Agenda

- 01 The Splunk Security platform
- 02 Splunk Enterprise Security
- 03 Splunk SOAR
- 04 Splunk Attack Analyzer
- 05 Asset and Risk Intelligence

The Splunk Security Platform



Growing compliance mandates



Expanding attack surface



Siloed tools, teams, data, and workflows

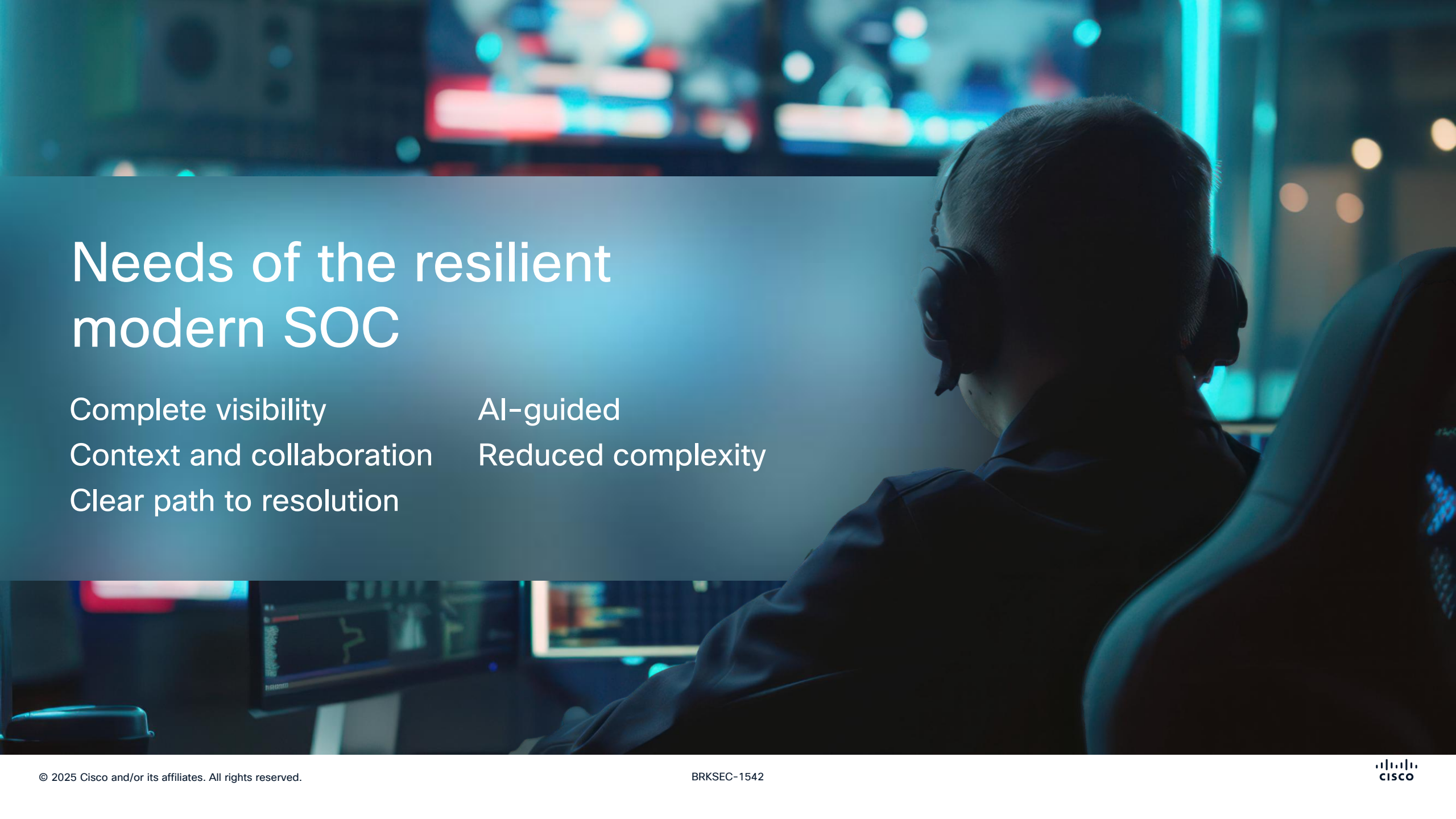


Talent and skills shortages



Growing attack volumes

SOC Challenges



Needs of the resilient modern SOC

Complete visibility

Context and collaboration

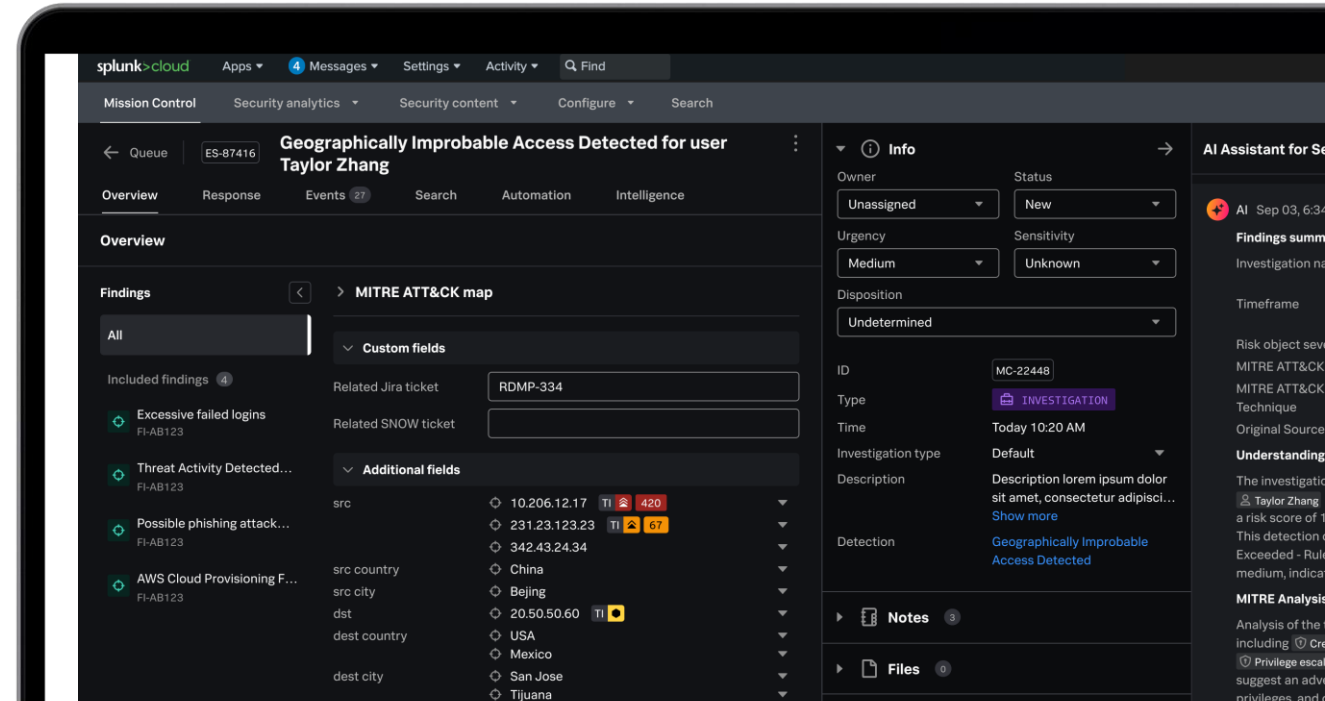
Clear path to resolution

AI-guided

Reduced complexity

Splunk Enterprise Security

Market-leading SIEM
with AI-powered
capabilities



Unmatched
visibility

Empowers
advanced detection

Fuels operational
efficiency

Splunk Recognized as a Leader

Leader in SIEM Market

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.



Source:
Magic Quadrant for
Security Information
and Event Management,
Andrew Davies, Eric
Ahlm, Angel Berrios,
Darren Livingstone.
October 8, 2025

SOC of the future

Advanced threat detections

90
PERCENT

Faster to identify root cause of threats

Real-time attack
chain detection

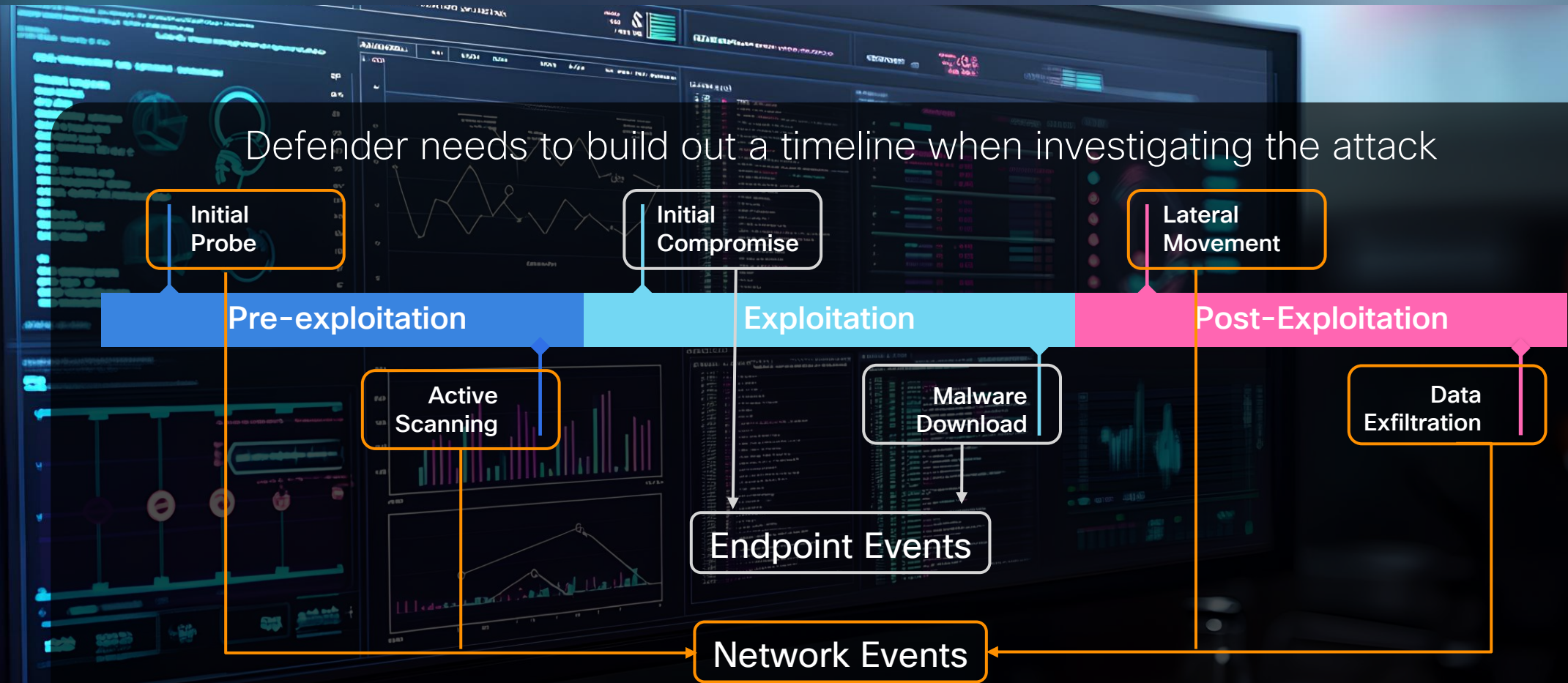
Curated and
custom detections

Automated threat
enrichment with
Cisco Talos

SOC of the future

For completeness, you need the network

Defender needs to build out a timeline when investigating the attack



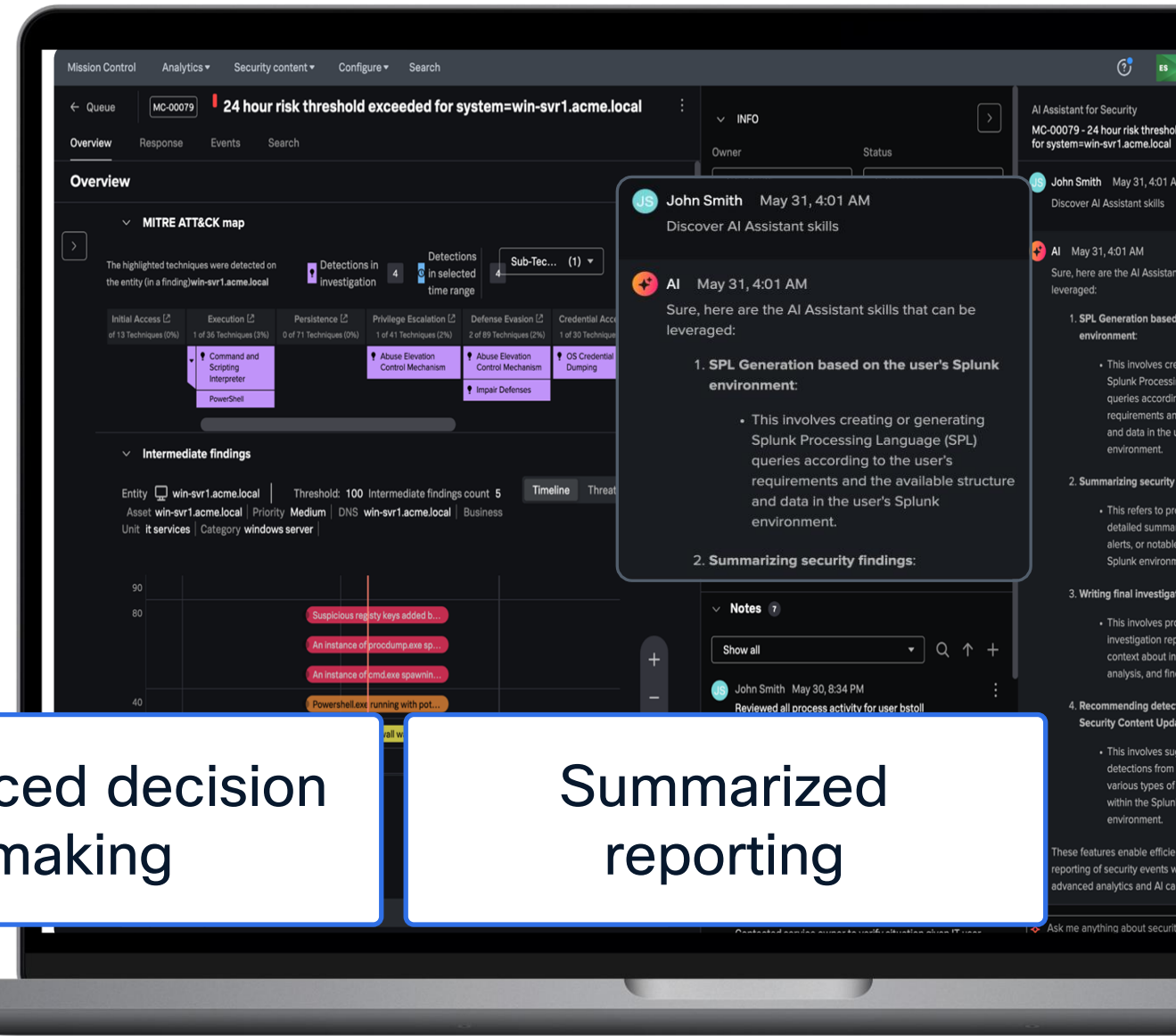
Investigate at machine scale

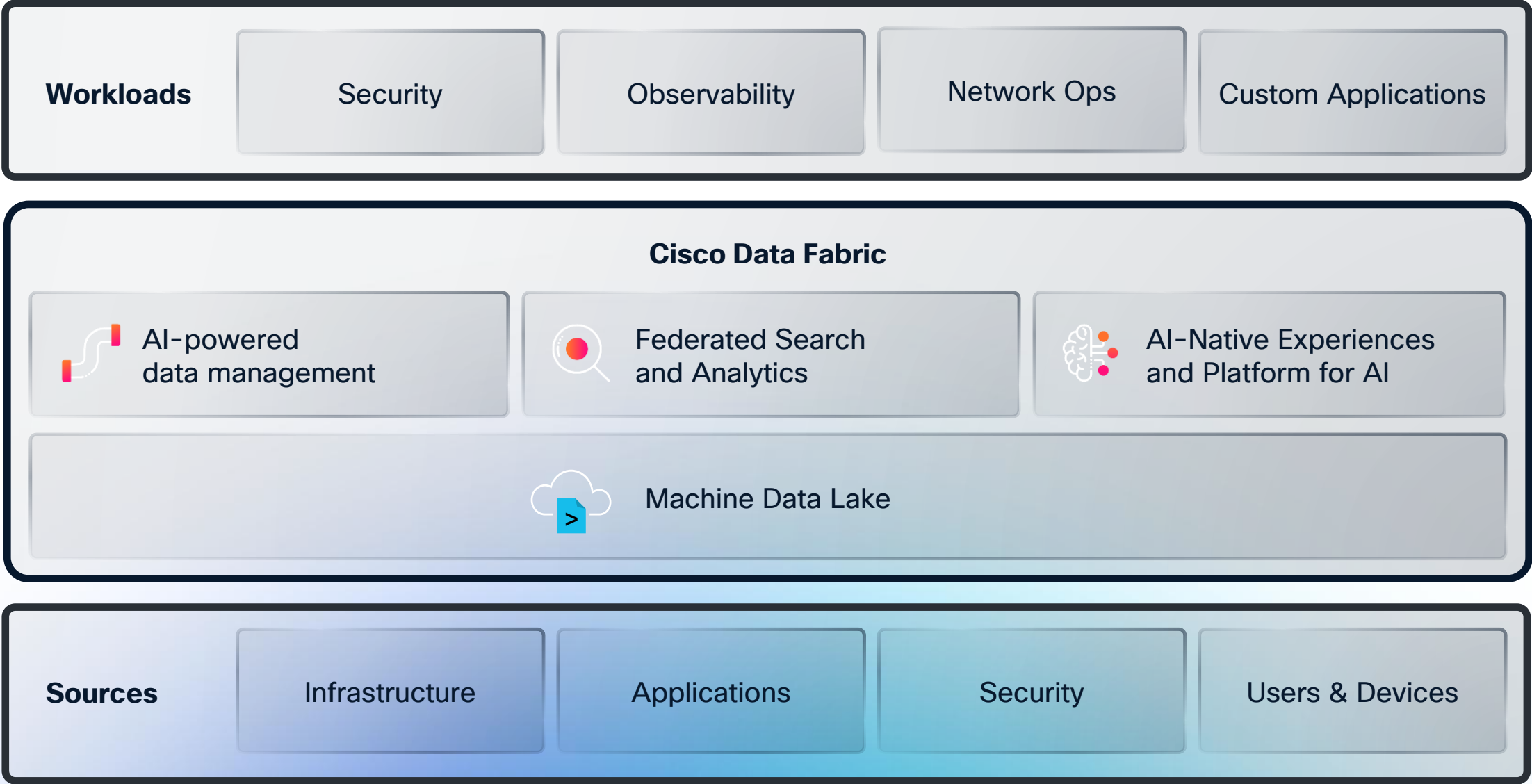
Embedded AI assistance to supercharge your work

Guided response and recommendations

Enhanced decision making

Summarized reporting





Splunk Enterprise Security

Available in two editions

GA Now

Essentials

SIEM

TIM

Controlled Availability Sep '25

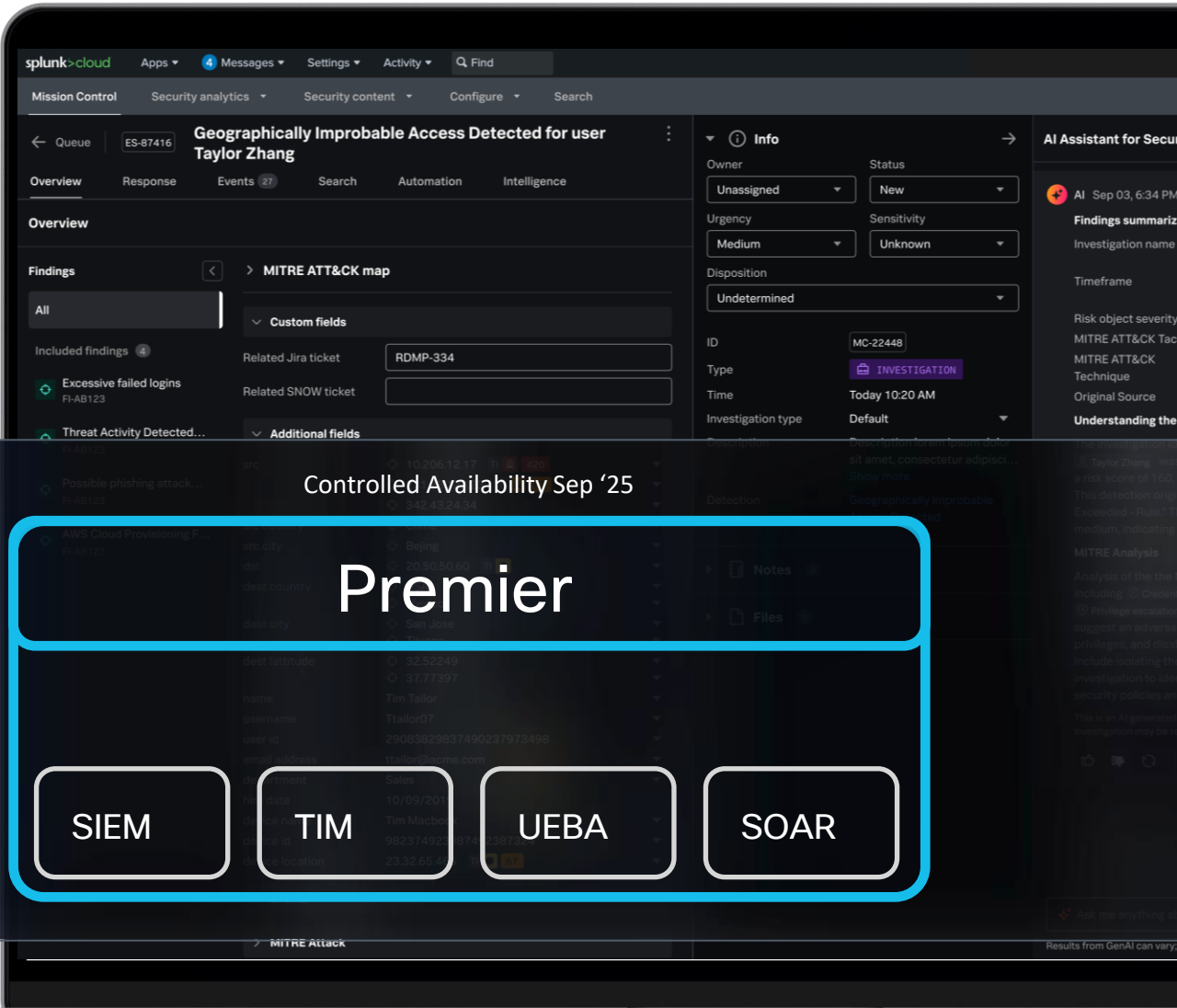
Premier

SIEM

TIM

UEBA

SOAR



DEMO

Splunk Asset and Risk Intelligence

SecOps struggle to understand their asset landscape

Rapidly evolving assets, users, devices, applications, and regulatory pressures continue to grow in scale and complexity.



Incomplete and Inaccurate Asset Data

52% manage 10,000+ assets¹



Lengthy Security Investigation

69% experienced an attack targeting unknown, or poorly managed assets²



Gaps in compliance

\$4M average revenue loss due to compliance audit failures³

1 Security Hygiene and Posture Management Survey by ESG, Oct 2021, p.12

2 Security Hygiene and Posture Management Survey by ESG, Oct 2021, p.13

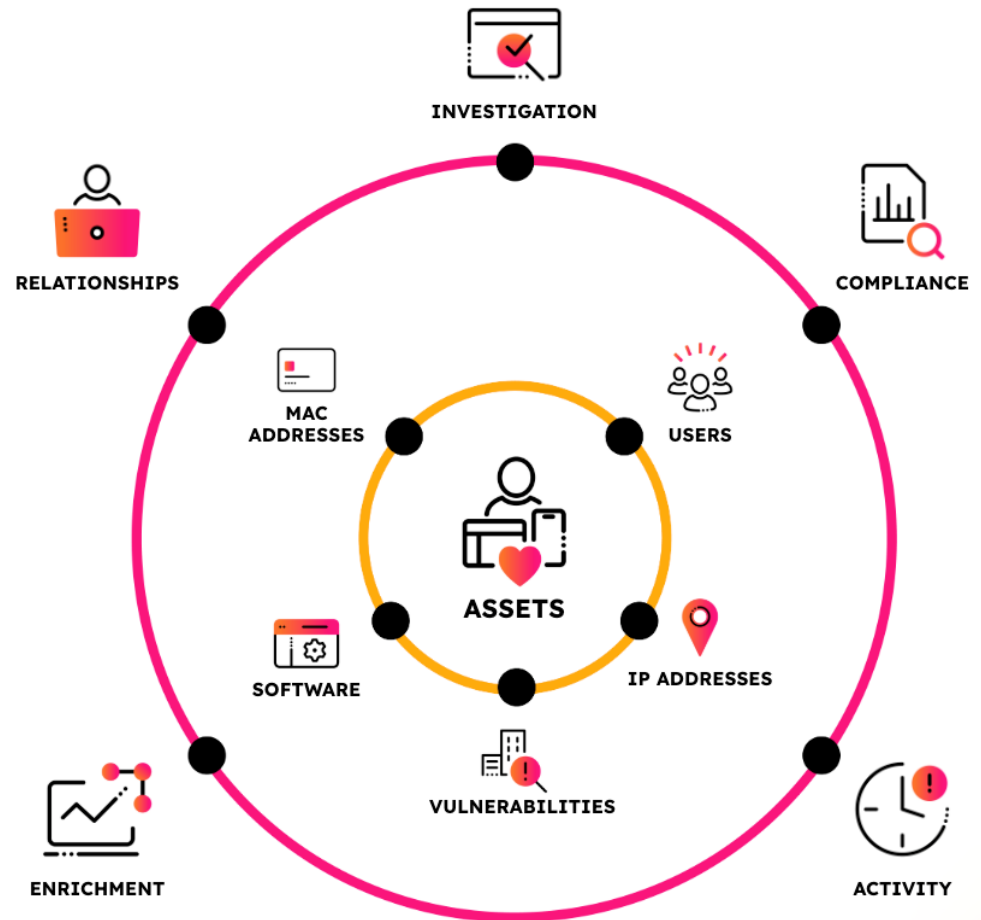
3 Whitepaper: The True Cost of Compliance, Ponemon Institute, Dec 2017, p.12

Introducing Splunk Asset and Risk Intelligence

Proactive risk mitigation through continuous asset discovery and compliance monitoring.

Continuously **discovers assets** (including devices, users, and applications) leveraging the rich data in Splunk.

Asset and Risk Intelligence identifies **compliance violations** and **gaps in security controls** using OOTB and custom frameworks, to **accelerate investigations** and **reduce risk** exposure.



The background of the slide is an abstract design featuring flowing, wavy lines in various shades of blue and white. A large, solid white rectangle is positioned on the left side of the slide, serving as a backdrop for the main text.

DEMO

Splunk Security Orchestration, Automation and Response (SOAR)

Cisco SOC of the future

Automated response

5X

Faster response time with automation

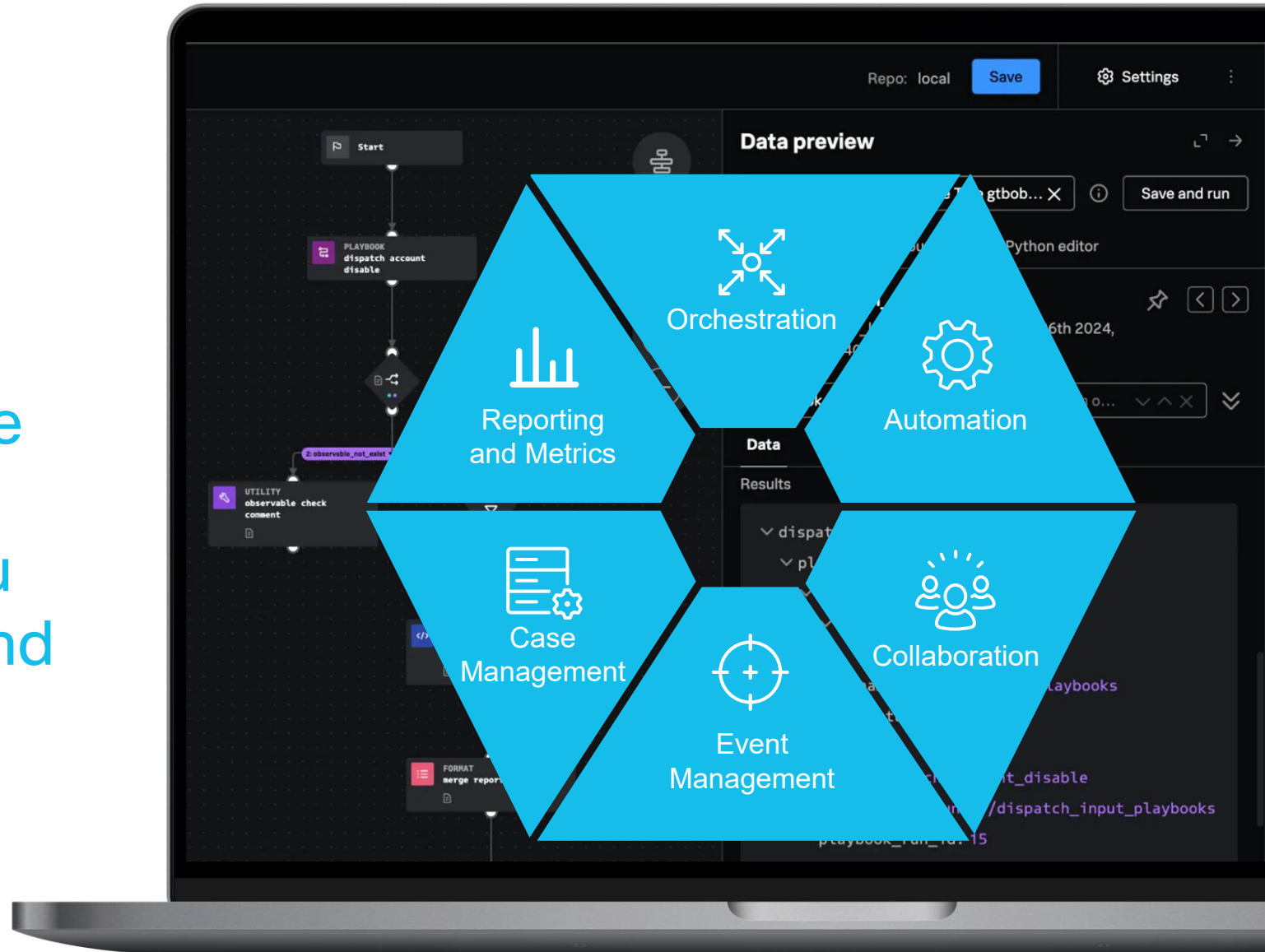
Pre-built
responses for
quick action

Comprehensive
automation and
orchestration

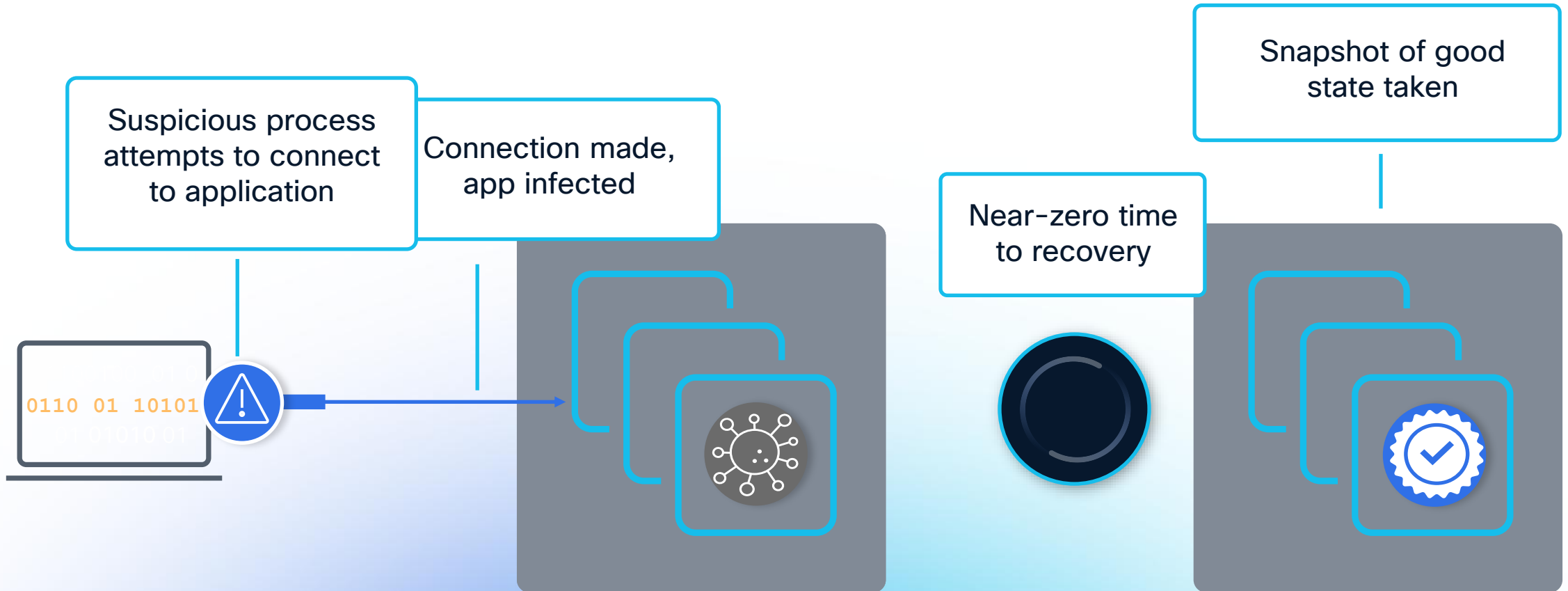
Rapid incident
response with
Cisco Talos

Automate any action, at scale

The most comprehensive automation and orchestration to help you work smarter and respond faster



Go from reactive to proactive



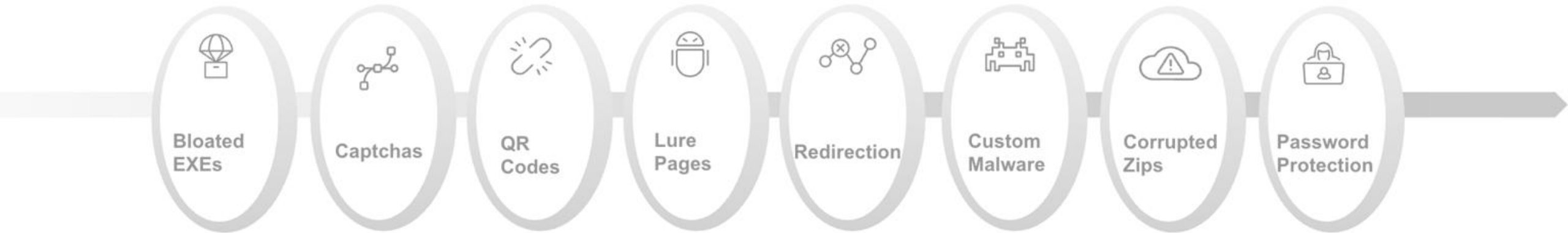
The background of the slide is an abstract design featuring flowing, wavy lines in various shades of blue and white. A large, solid white rectangle is positioned on the left side of the slide, serving as a backdrop for the main text.

DEMO

Splunk Attack Analyzer

No surprise, threats are getting through

Attackers put hoops in the way to evade detection & analysis



Introducing Splunk Attack Analyzer

Automate threat analysis of suspected malware and credential phishing threats



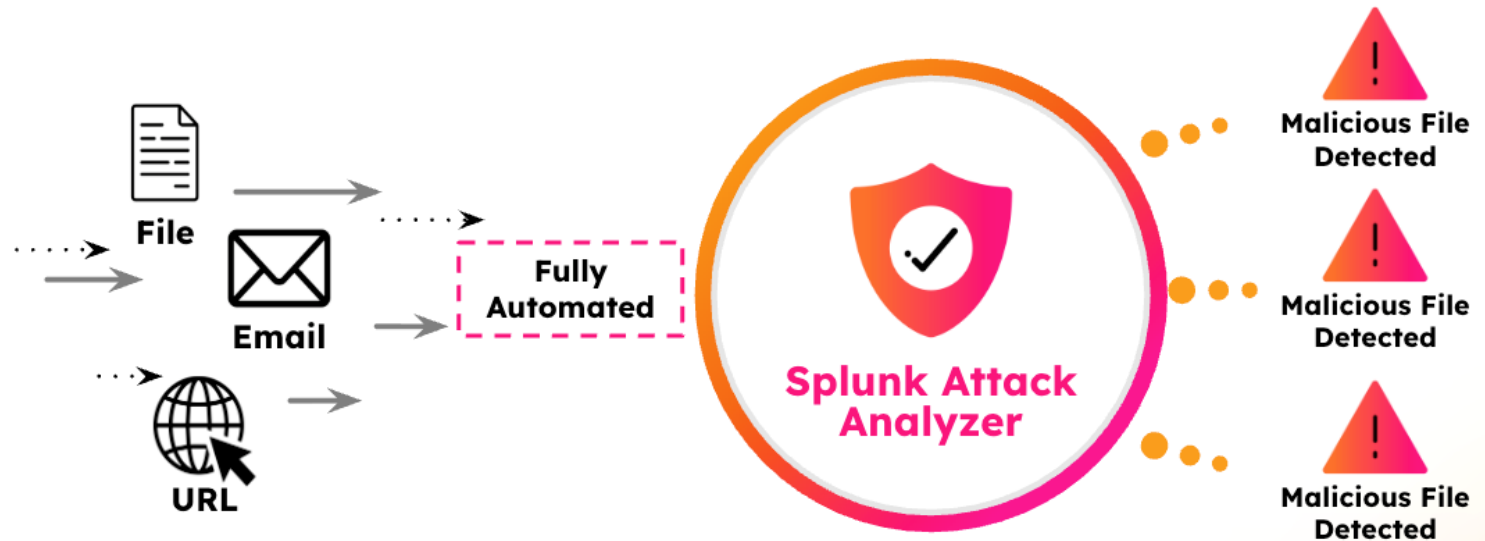
Take the **manual work out** of threat analysis



Gain **consistent, comprehensive**, high-quality threat analysis

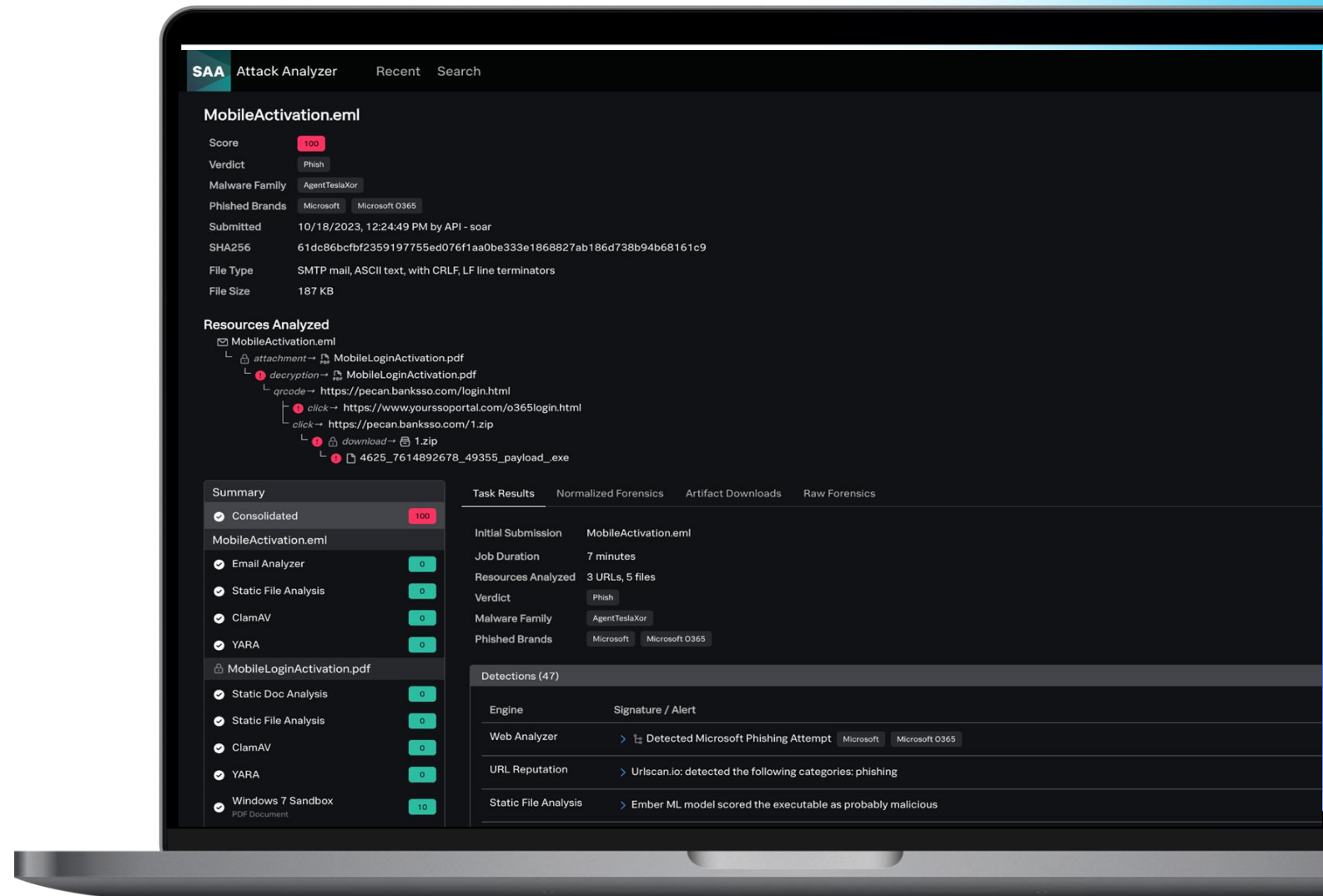


Intelligent **automation** for end-to-end threat analysis and response



Take the manual work out of threat analysis

- **Attack Chain Following** means that Splunk Attack Analyzer is going to jump through the hoops for you, think **anti-anti-analysis**.
- Attacks are **not just binaries and exploits** so your analysis platform shouldn't be, either.



DEMO

Conclusion

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 !

