cisco Connect

GO BEYOND

#CiscoConnect

Le futur du SOC à l'ère de l'IA

Cisco XDR & Splunk ES

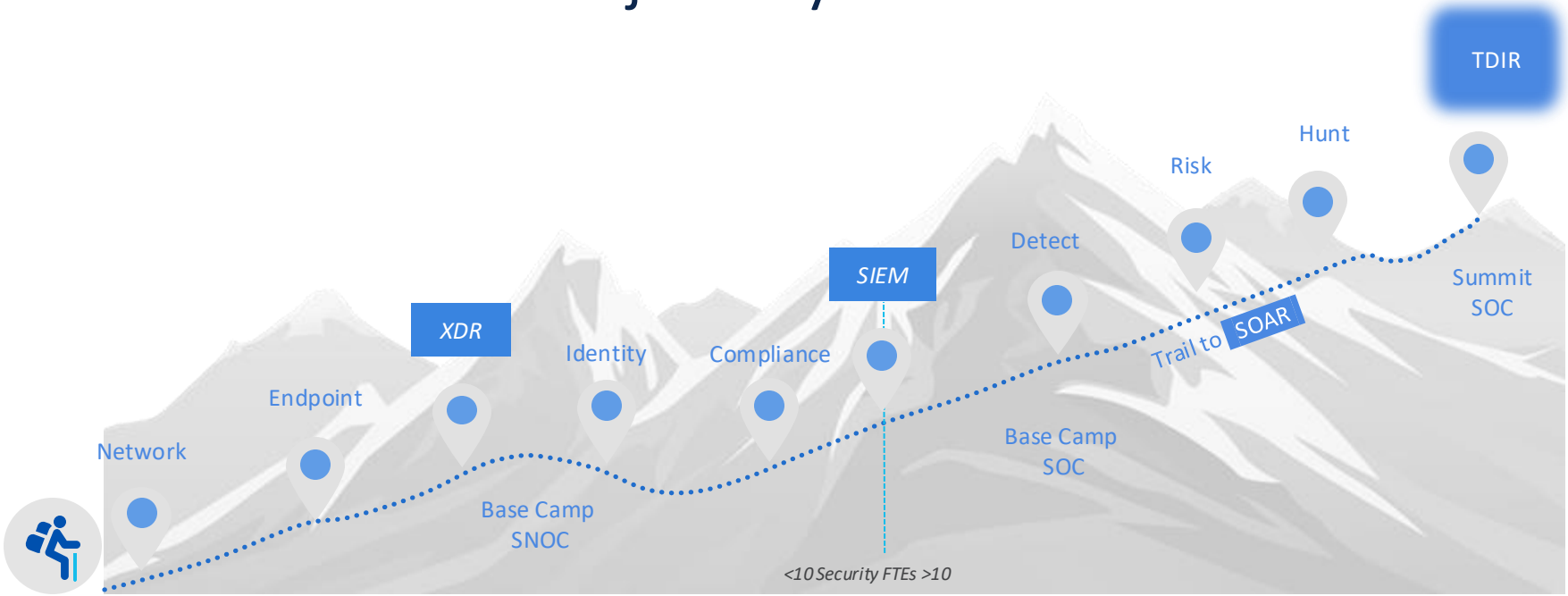
Yonathan Bleyfuesz, Solutions Engineer
ybleyfue@cisco.com

Goran Dzumhur, Solutions Engineer
gdzumhur@cisco.com

Track 3/BRK 4

cisco Connect

Disclamer : TDIR is a journey



For product demo / discussions come to our booth !

@Cisco Security *@Splunk*

Applications

|

Data

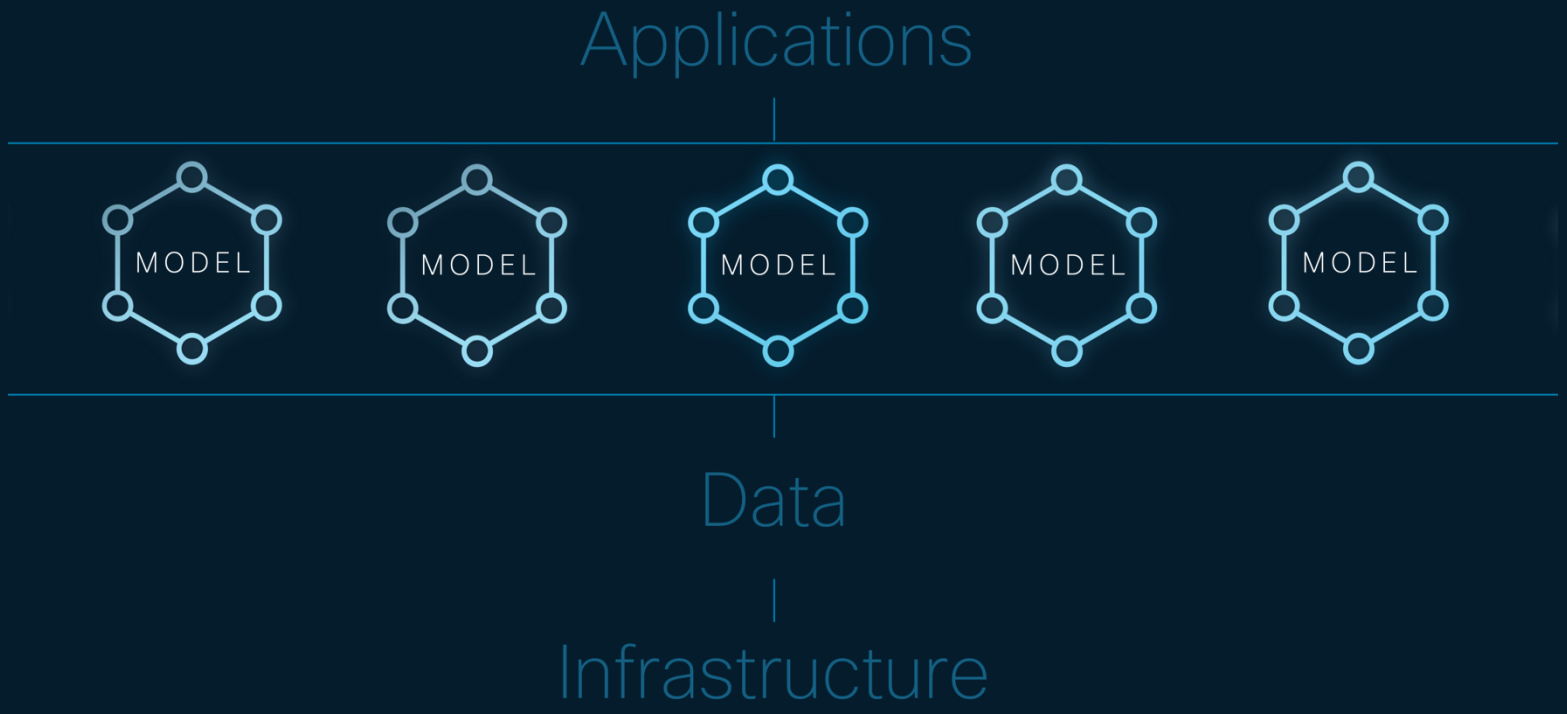
|

Infrastructure

Applications

Data

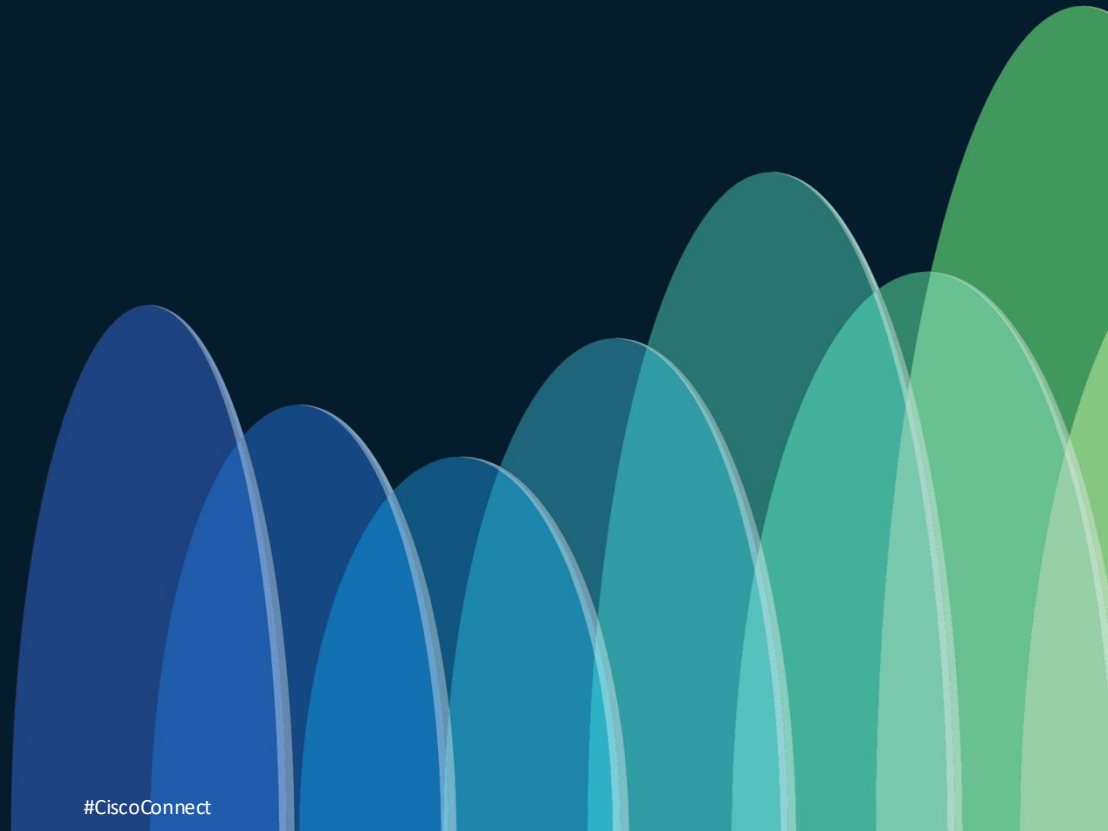
Infrastructure



(Some of) The AI Problem

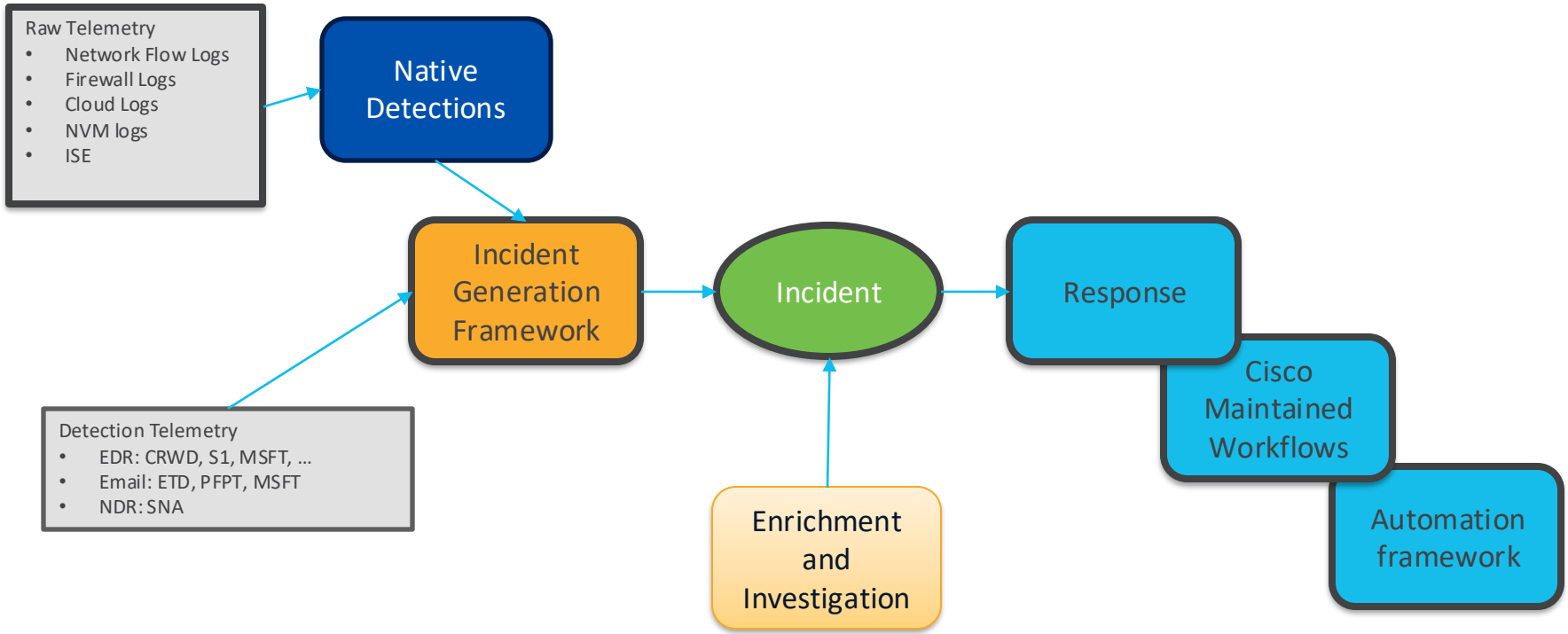
How to scale data    Hyperdistribution

Catching lateral movement with Cisco XDR

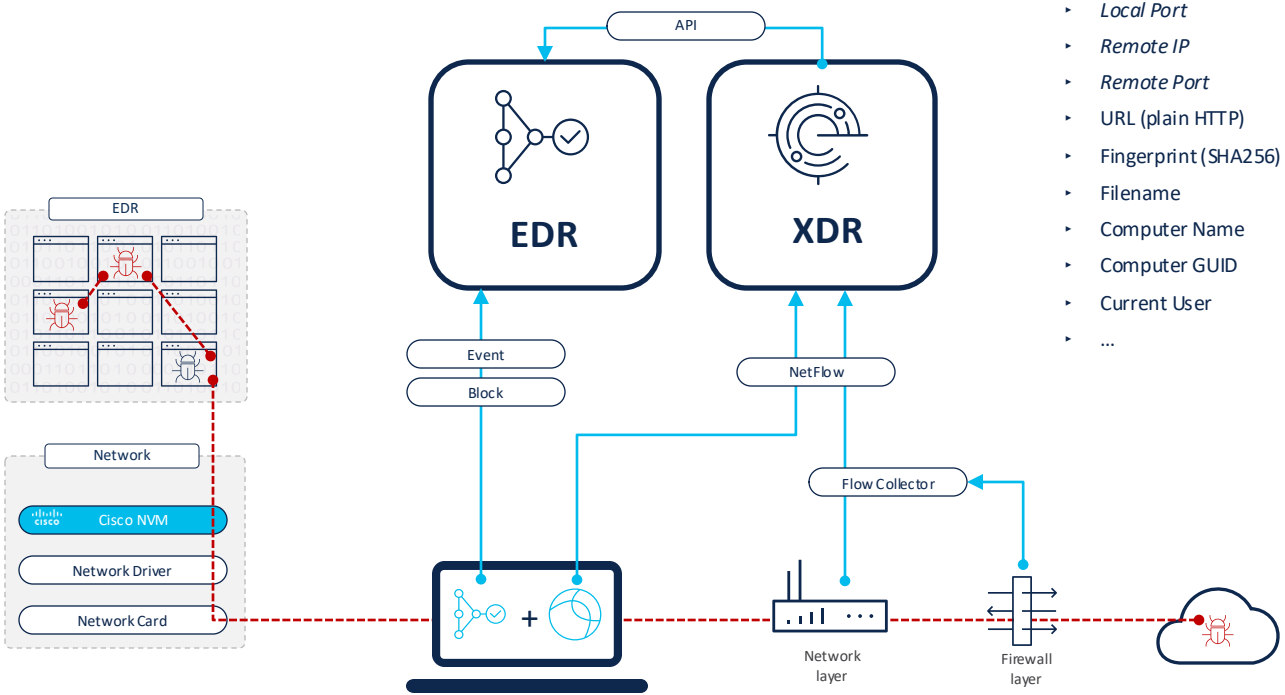


cisco Connect

Cisco XDR : Network-led, Open XDR



Network & EDR stitching



EDR Content

- *Local IP*
- *Local Port*
- *Remote IP*
- *Remote Port*
- URL (plain HTTP)
- Fingerprint (SHA256)
- Filename
- Computer Name
- Computer GUID
- Current User
- …

Flow Information

NetFlow / IPFIX

- Source IP
- Source Port
- Destination IP
- Destination Port
- Bytes sent
- Bytes Received

Added by NVM Module

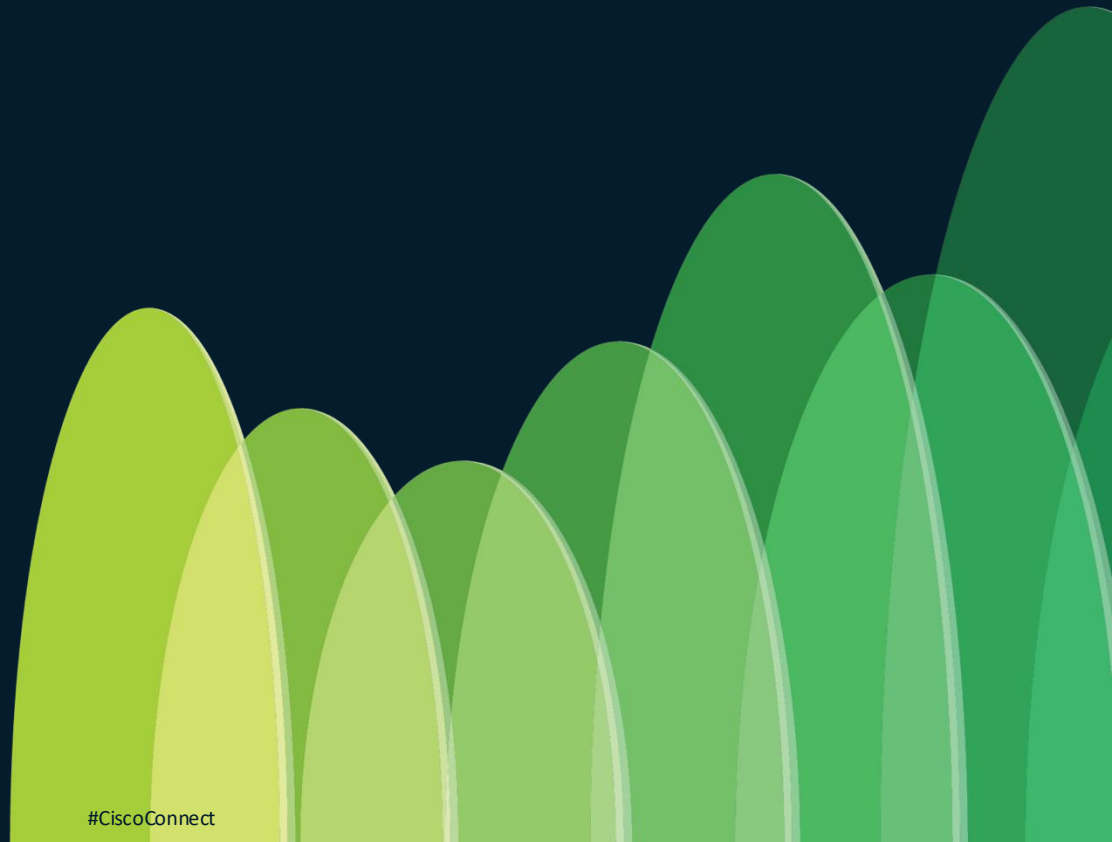
- OS Version
- OS Edition
- UDID
- Host Name
- Logged In User
- Process Name
- Process Hash
- Process Account
- Parent Process Name
- Parent Process Hash
- Parent Process Account
- DNS/Destination Hostname
- Module Hash List
- System Manufacturer
- System Type
- MAC address
- Interface Name/Type/UID

Getting the full Cisco power into the Analytics

New evolution: Use of EVE library and ETA network telemetry

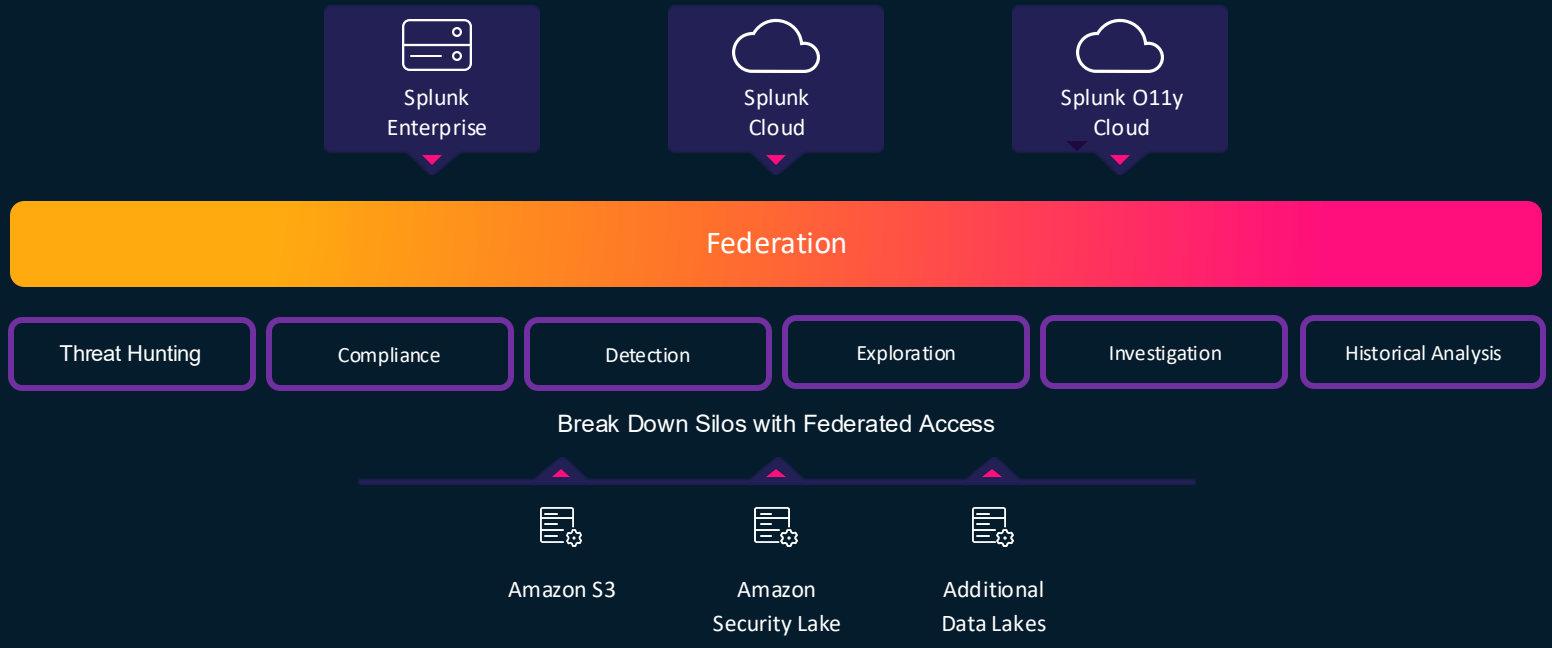
Alert Type	Observation Types	History	Priority	Cisco XDR ...	Enabled	Telemetry
	= Suspicious Network					∈ ETA
Malware Communication Identified via EVE Encrypted Visibility Engine detected communication between a process and a server that is suspected to be malware.	• Suspicious Network Activity detected by EVE	0 Days	High Default Priority: Normal		Default: Disabled	ETA
Suspicious DNS over HTTPS Activity An internal server was detected exchanging traffic with a known DNS over HTTPS server. This may indicate an attempt to evade DNS-based security.	• Watchlist Lookup • Suspicious Network Activity detected by EVE	7 Days	Normal Default Priority: Normal		Default: Enabled	ETA, Passive DNS
Use of Evasive VPN - External proxy Encrypted Visibility Engine detected use of an evasive Virtual Private Network (VPN) provider or an external proxy.	• Suspicious Network Activity detected by EVE	0 Days	Normal Default Priority: Normal		Default: Disabled	ETA
Use of Remote Access Tools Encrypted Visibility Engine detected use of remote access tools. Remote access tools may be utilized legitimately by systems administrators, but are also known to be utilized by threat actors, including Advanced Persistent Threats.	• Suspicious Network Activity detected by EVE	0 Days	Normal Default Priority: Normal		Default: Disabled	ETA

Data problem
Splunk Solution



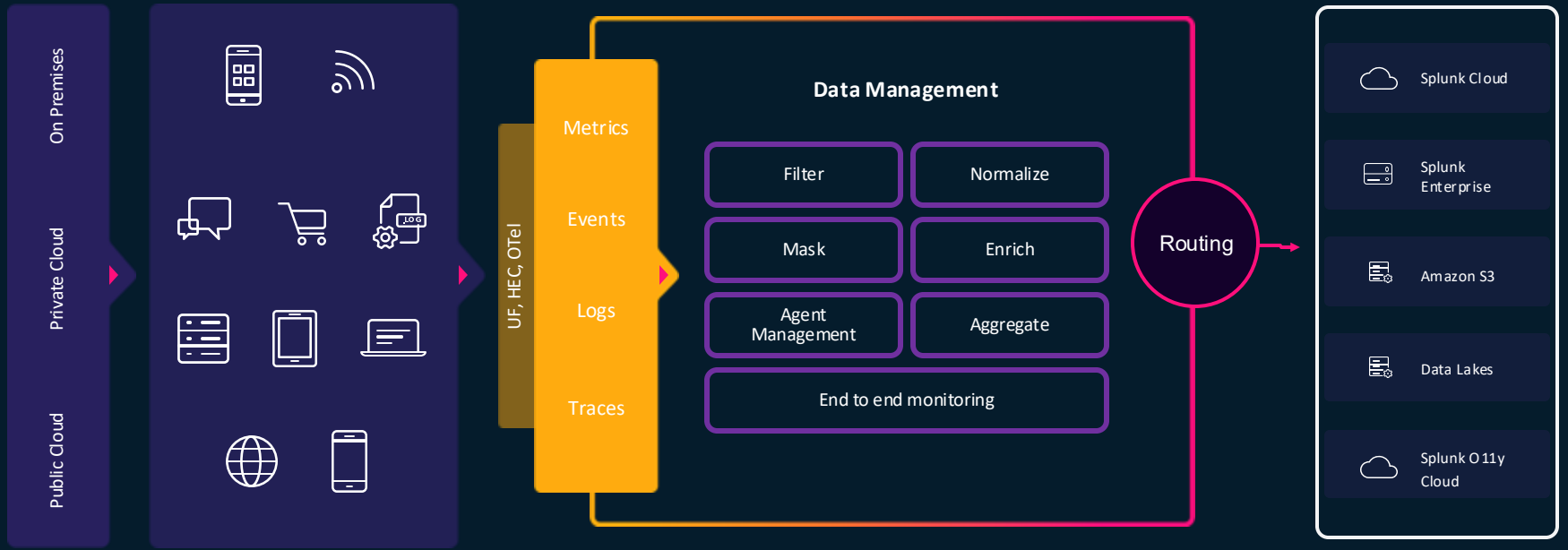
Federation

Break down silos with federated access



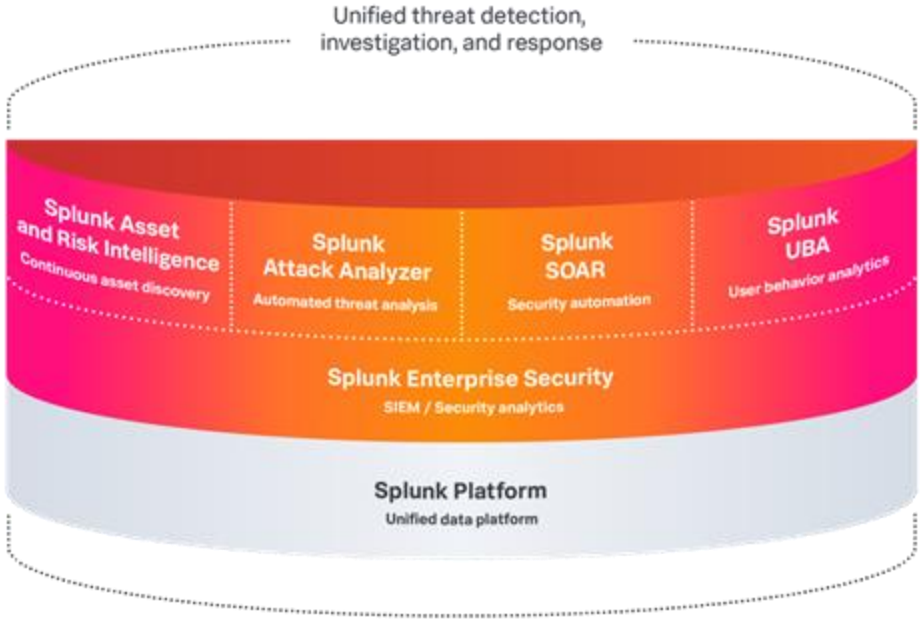
Data Management

Unified data configuration, processing, and management



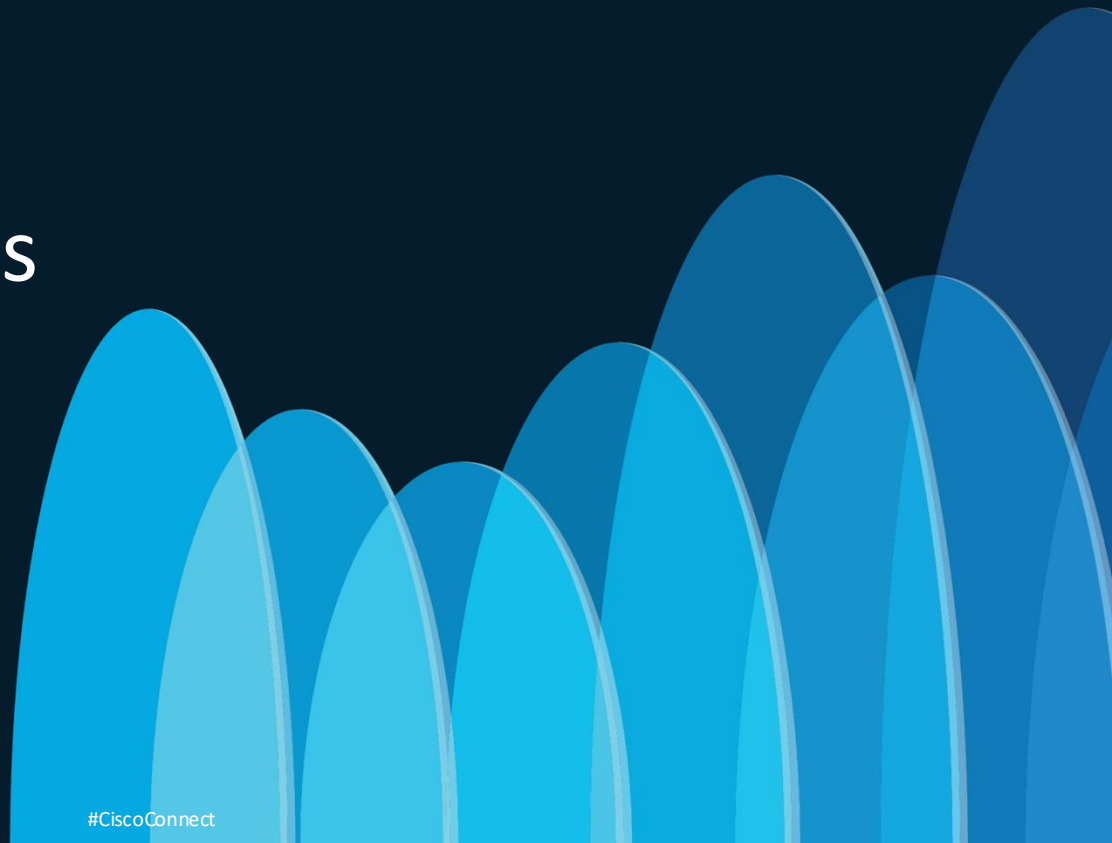
Splunk Security

Powering the SOC of the future with the leading TDIR solution



Third-party tools | Cisco User/ Cloud/ Breach/XDR | Talos | Networking | IT/OT | Applications | Clouds | Data centers

How will AI help us ?



The main SOC problems

Skills shortage

Alert fatigue

Complexity

Driving a new wave of maturity for SOC

Accelerating the SOC of the future

Detect advanced threats

Anomaly detection | ML-based detection
Insider threat detection | Behavior analytics

Simplify investigations and triage

Streamlined Threat Workflow | Anomalies Grouping | Threat Visualization

Enhanced response

Streamlined Threat Workflow | Anomalies Grouping | Threat Visualization

AI Assistants

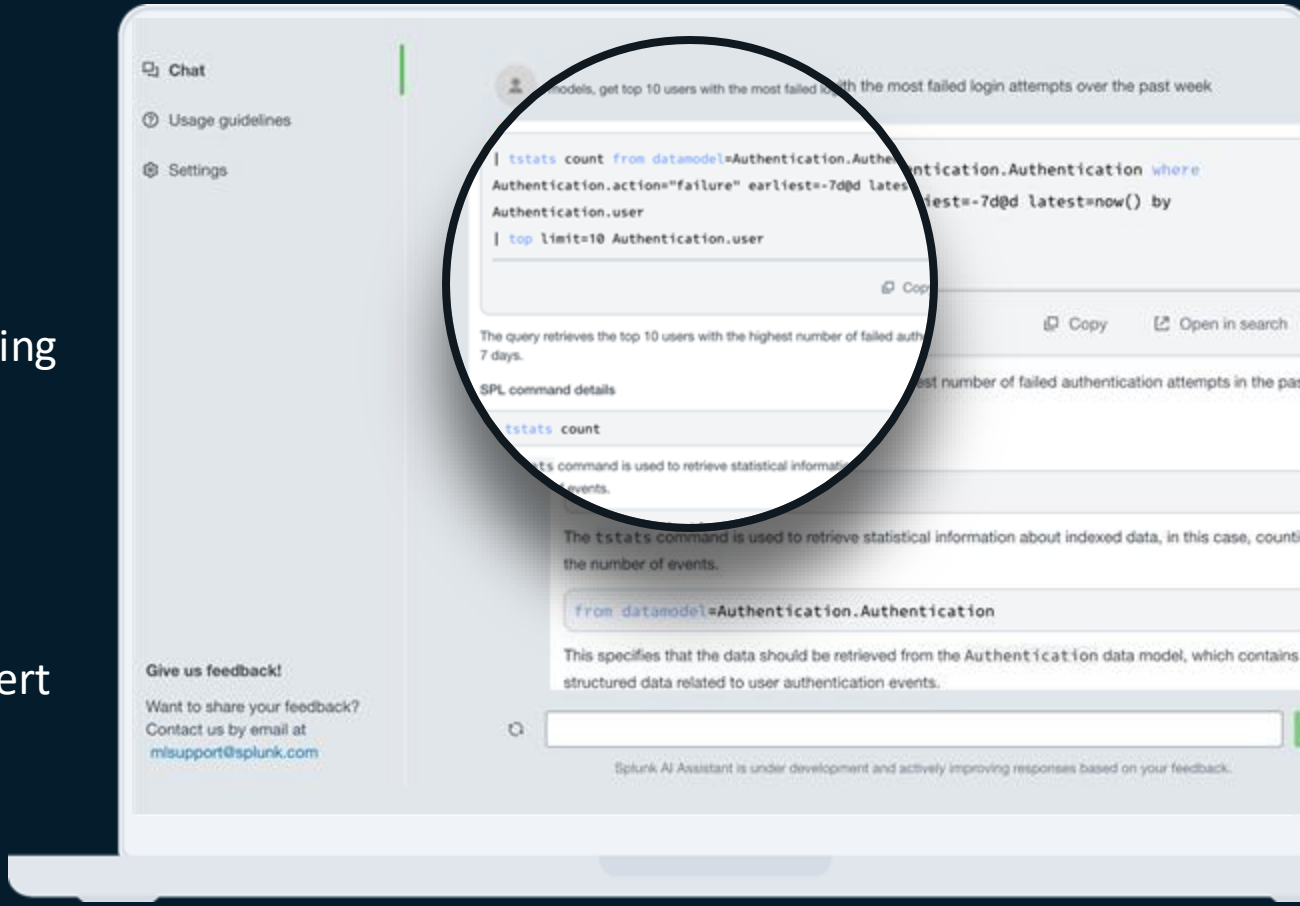
Enterprise Security | SPL

Splunk AI

AI Assistant for SPL

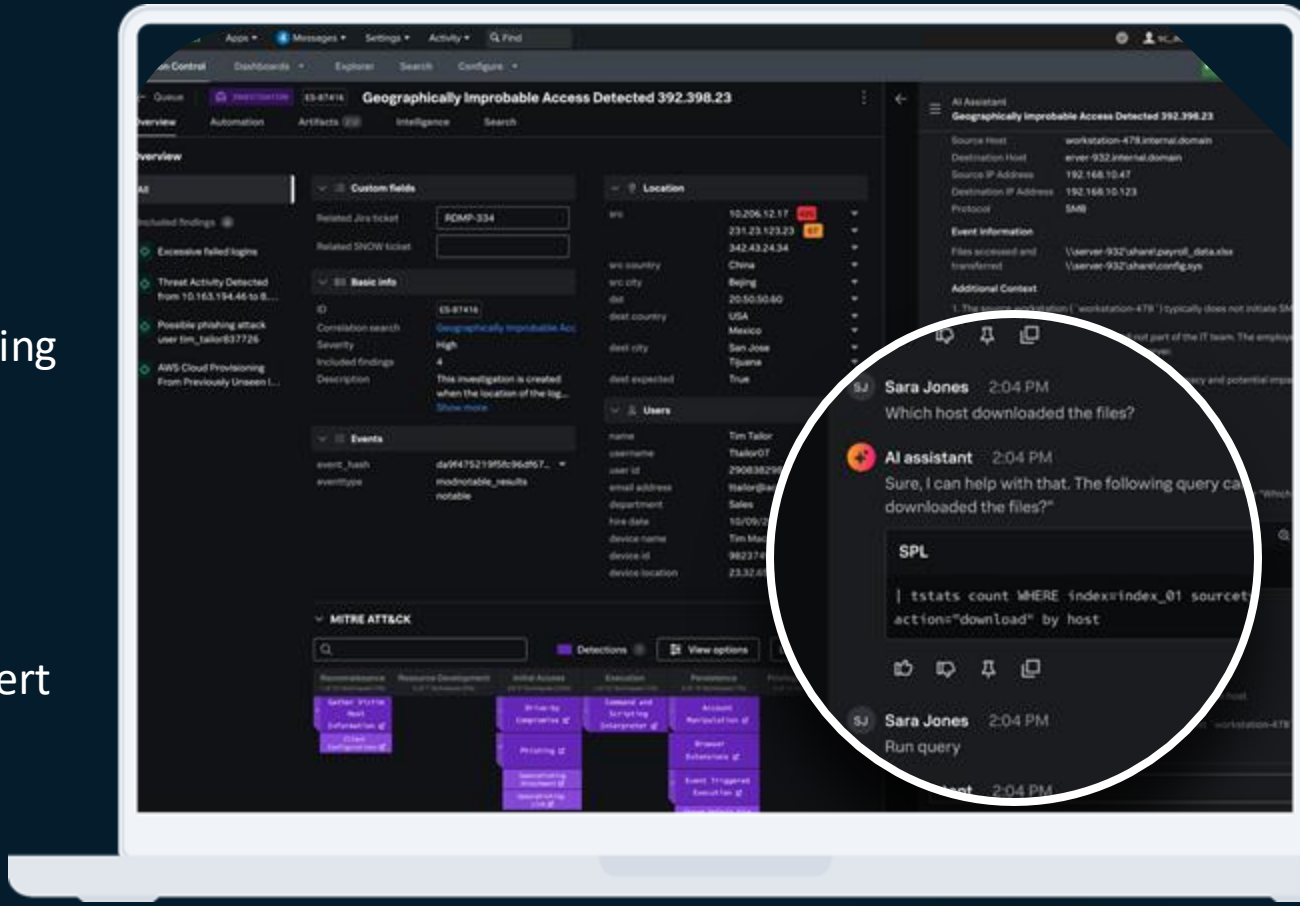
Available in Splunk Cloud

- Get your job done faster using natural language
- Chat with your data to drill down to deeper insights
- Accelerate your learning journey to become the expert



AI Assistant for Security

- Get your job done faster using natural language
- Chat with your data to drill down to deeper insights
- Accelerate your learning journey to become the expert



Our goal: To make everyone a Splunk expert

Using powerful domain-specific LLMs, in-context, to power key workflows

Faster Insights and Content

"Can you summarize the findings from this incident?"

Assisted Troubleshooting

"Write SPL to find modifications made to AWS Security Groups"

Chat with Your Data

"Search apache access logs…"

"Use ip address to filter results to north america."

RSAC 2025

New features in Cisco XDR

Clear verdict. Decisive action. AI speed.

Instant Attack Verification

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

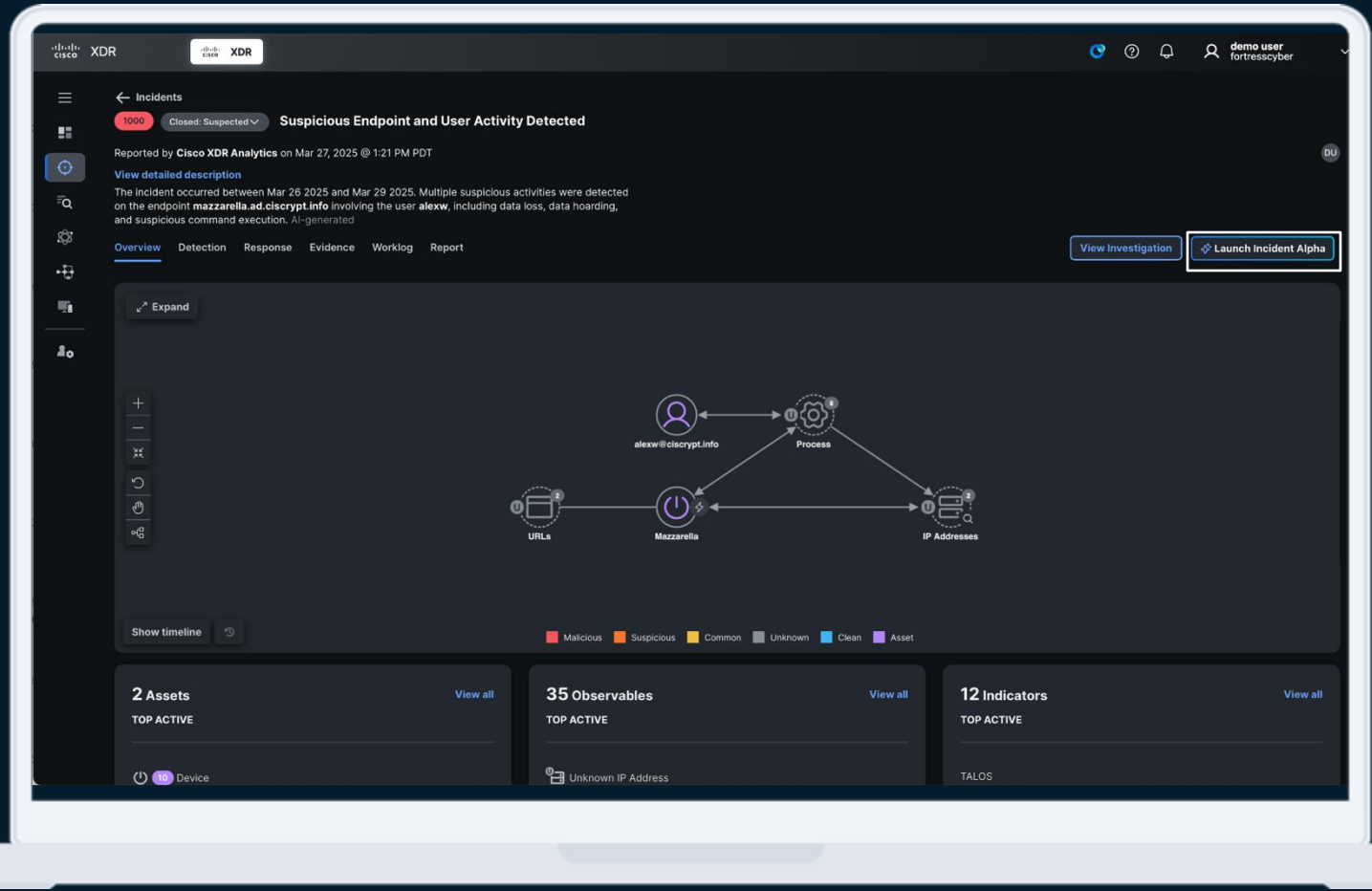
Automated Forensics

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.

Attack Storyboard

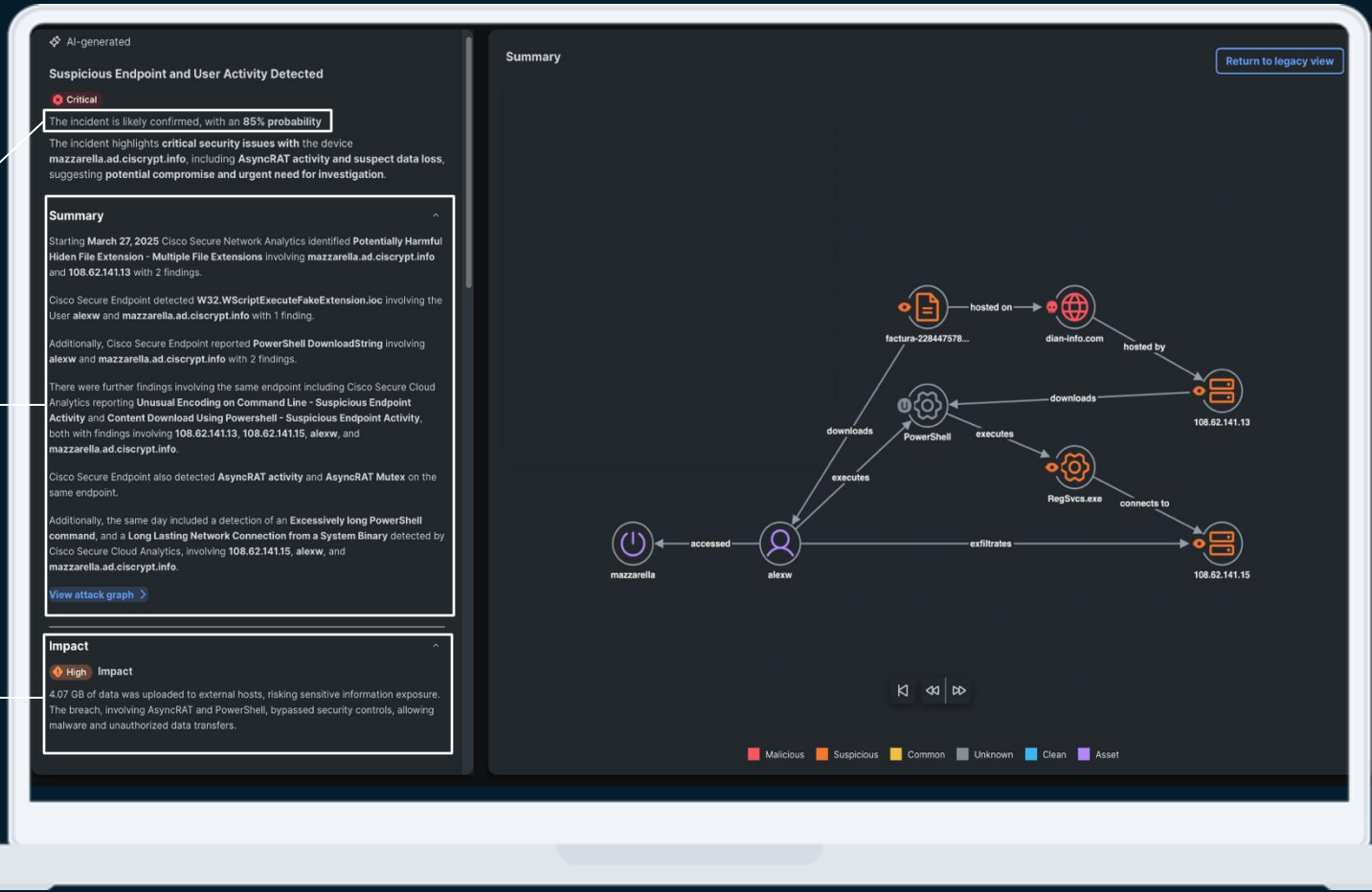


Attack Storyboard

AI Confidence Score

Investigation Summarization

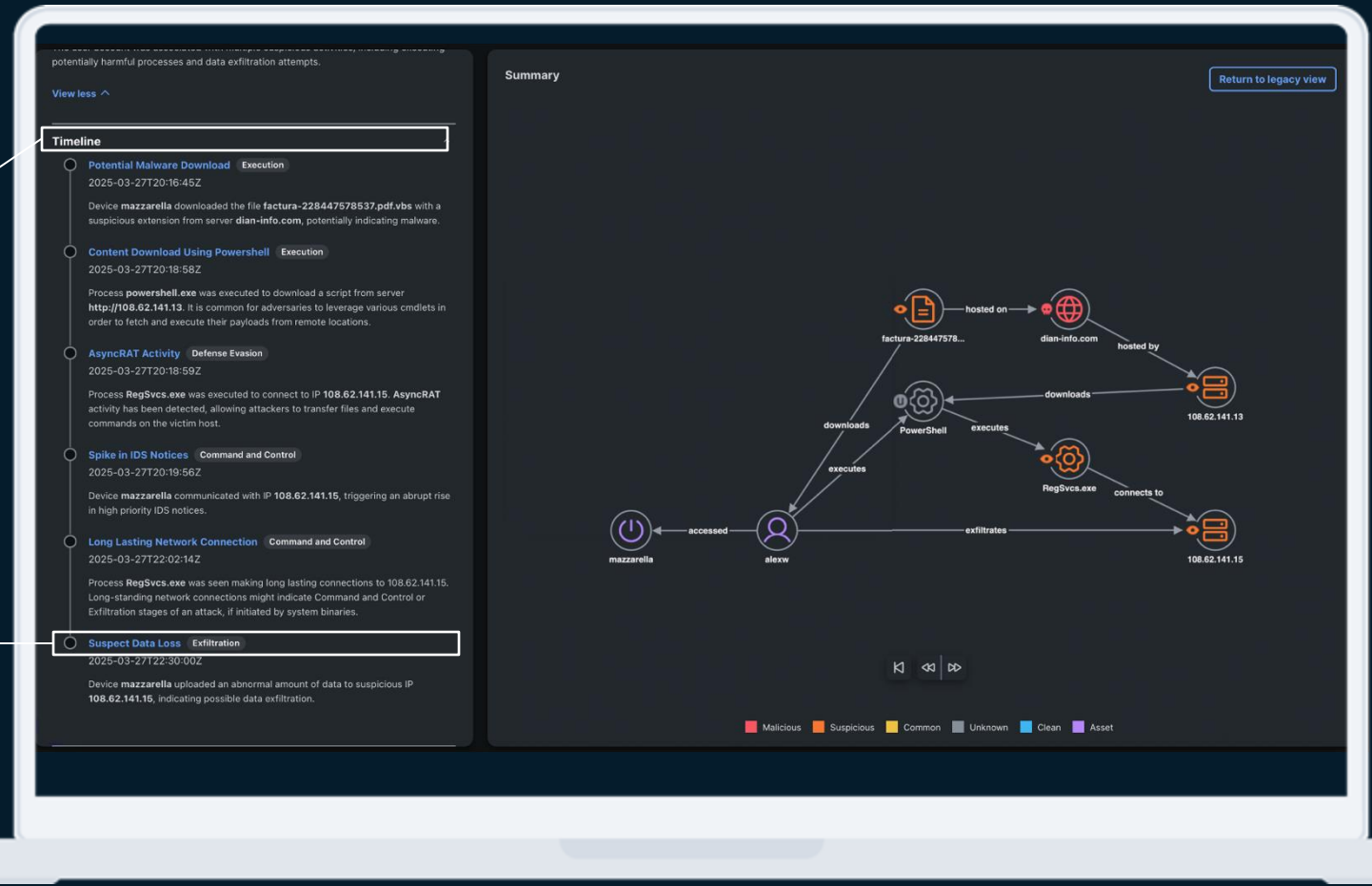
Measured impact



Attack Storyboard

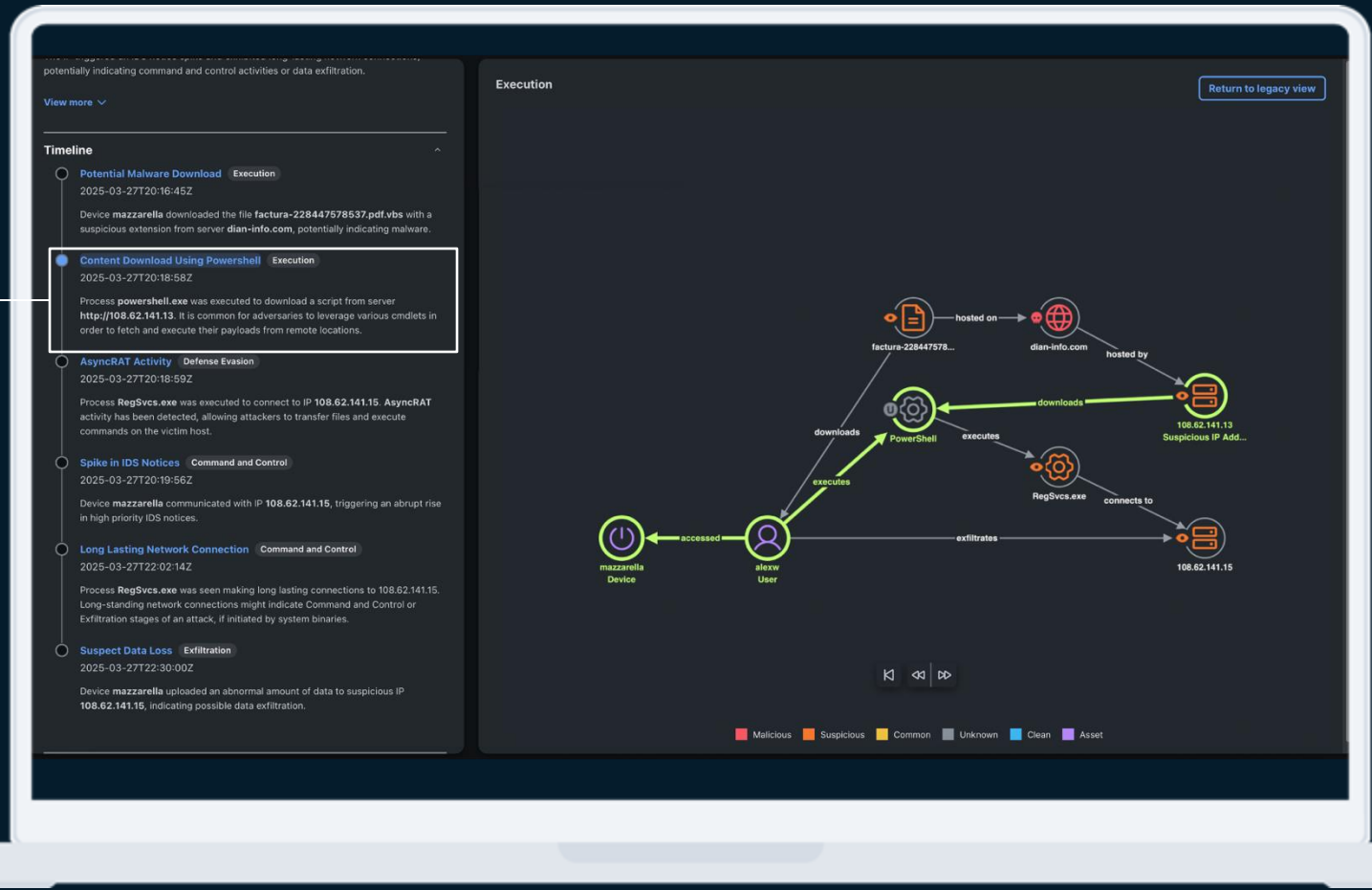
AI Generated interactive timeline

Indicator with MITRE association



Attack Storyboard

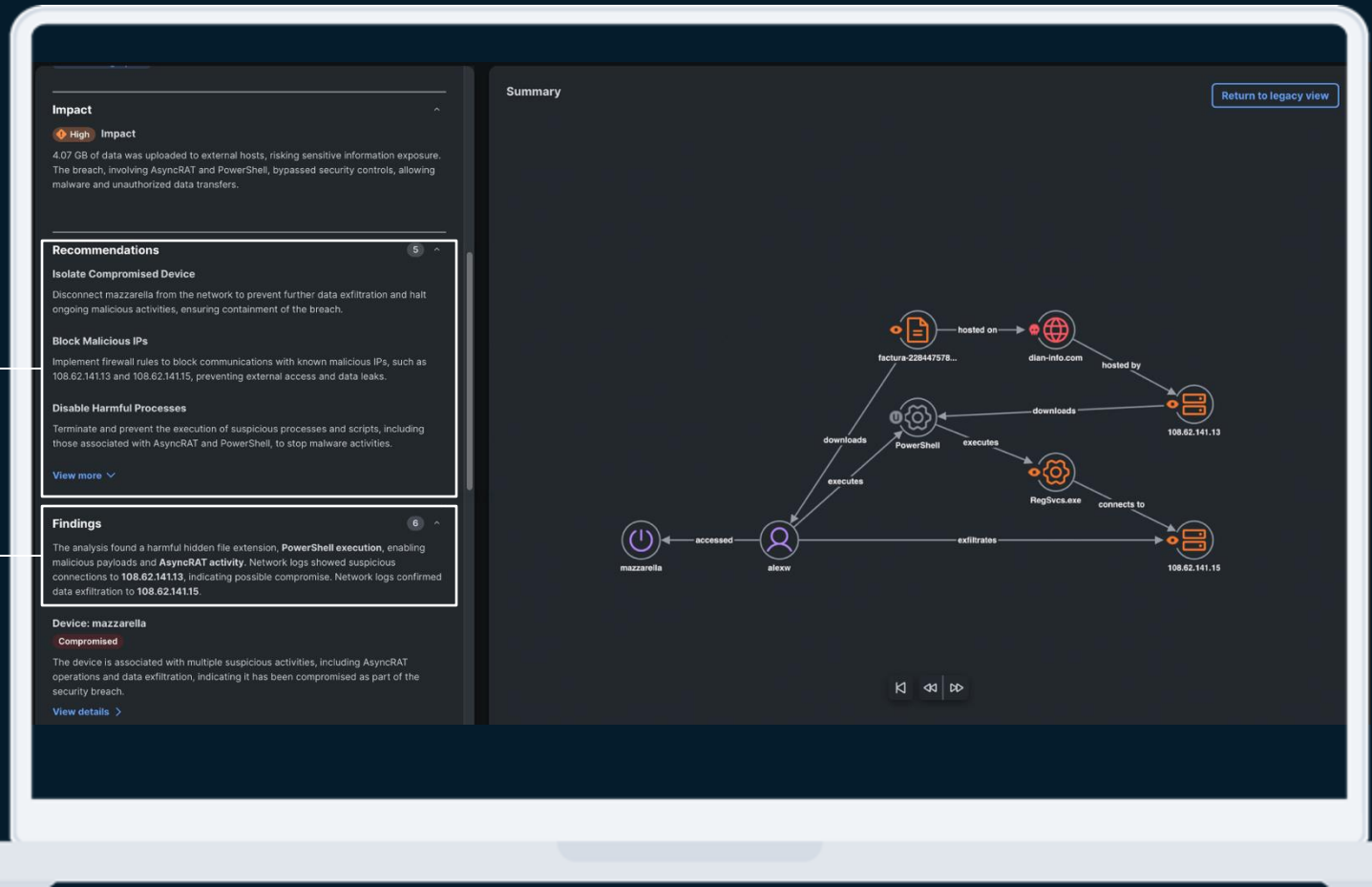
Graph Navigation using the timeline



Attack Storyboard

Generated recommendation, workflow / automation button will be present @GA

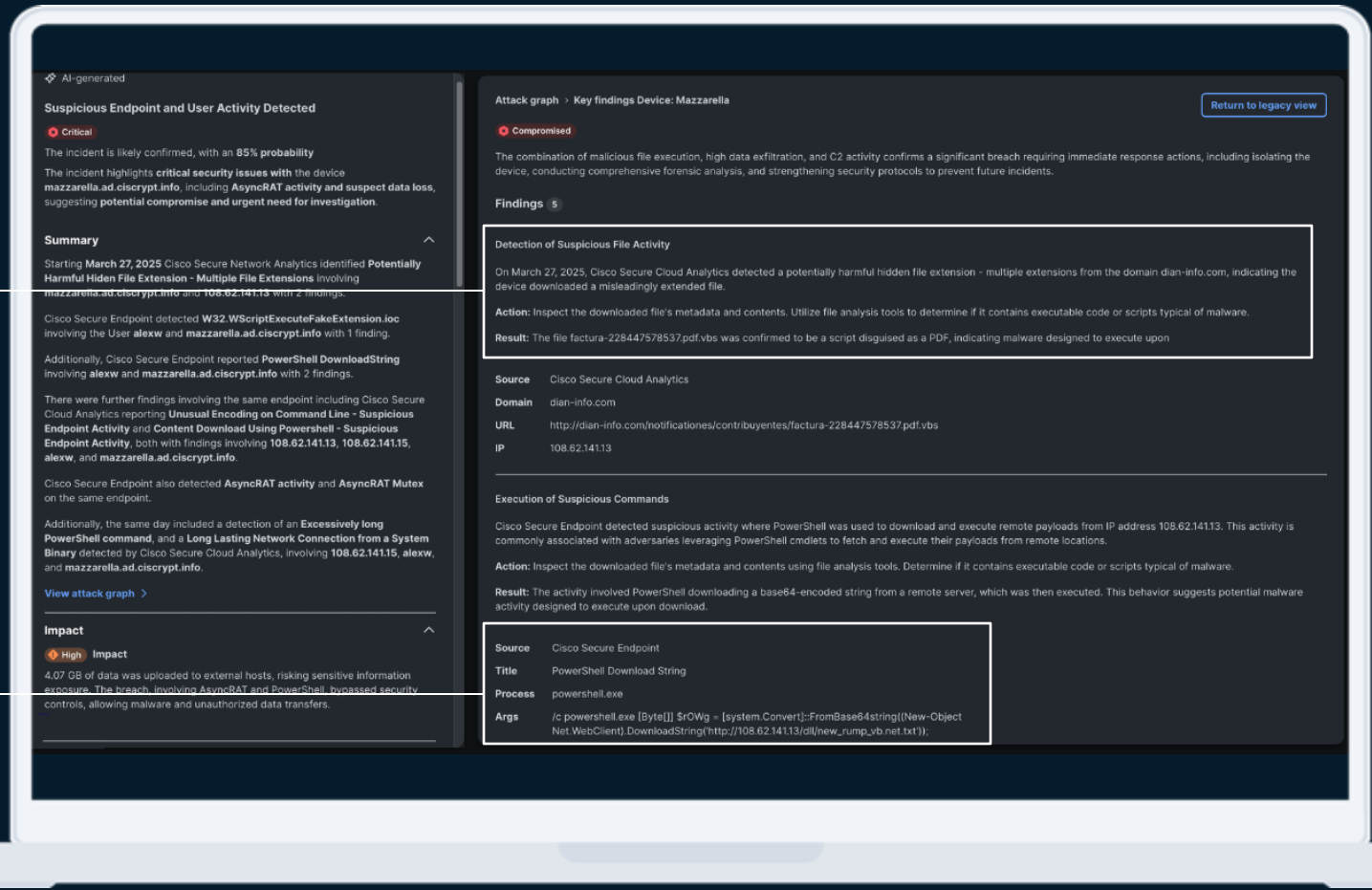
Summary of the findings the multi-agent, agentic AI used to run the investigation



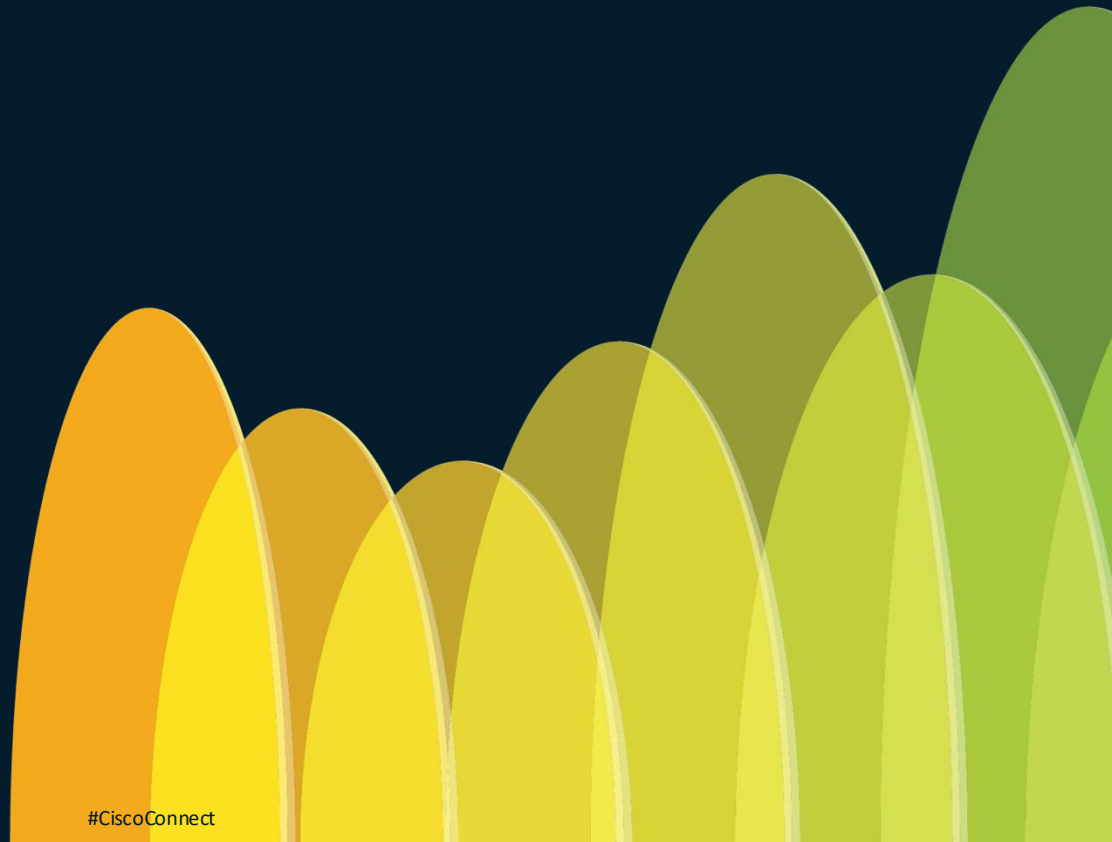
Attack Storyboard

Human formatted description

Findings properties



XDR or SIEM ?

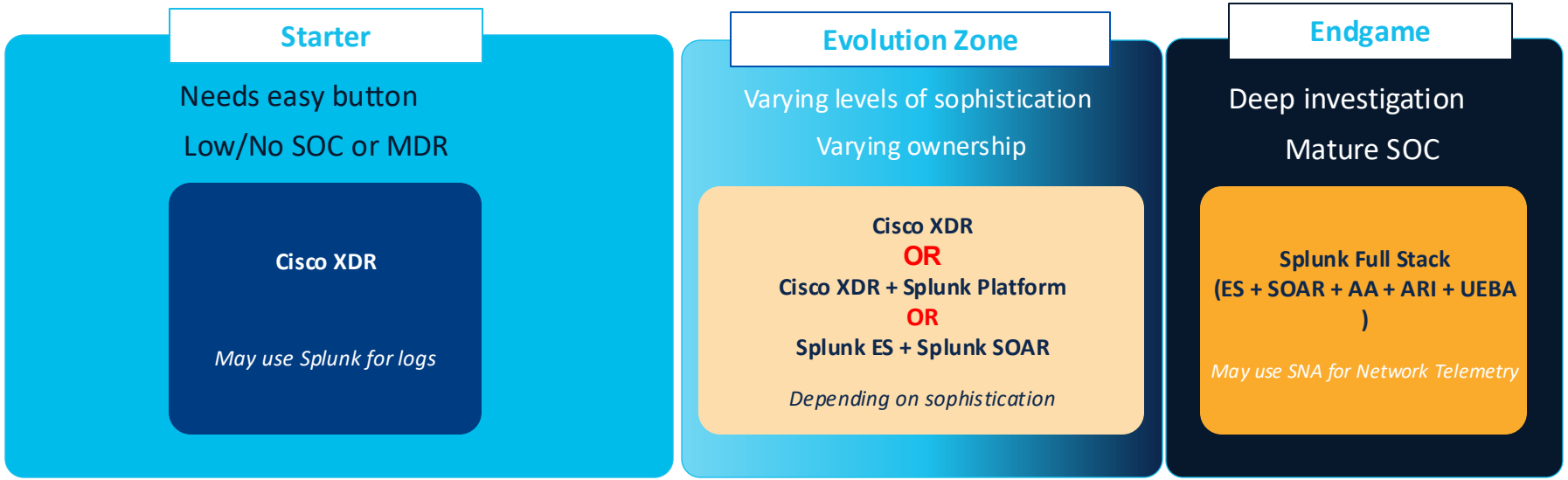


How to choose ?

Expected Outcomes :

- Asset inventory
- Automation
- Multi-Sources
- Out of the box detection
- Prioritization
- Complete Visibility
- Noise reduction
- AI Enabled
- Investigation Framework

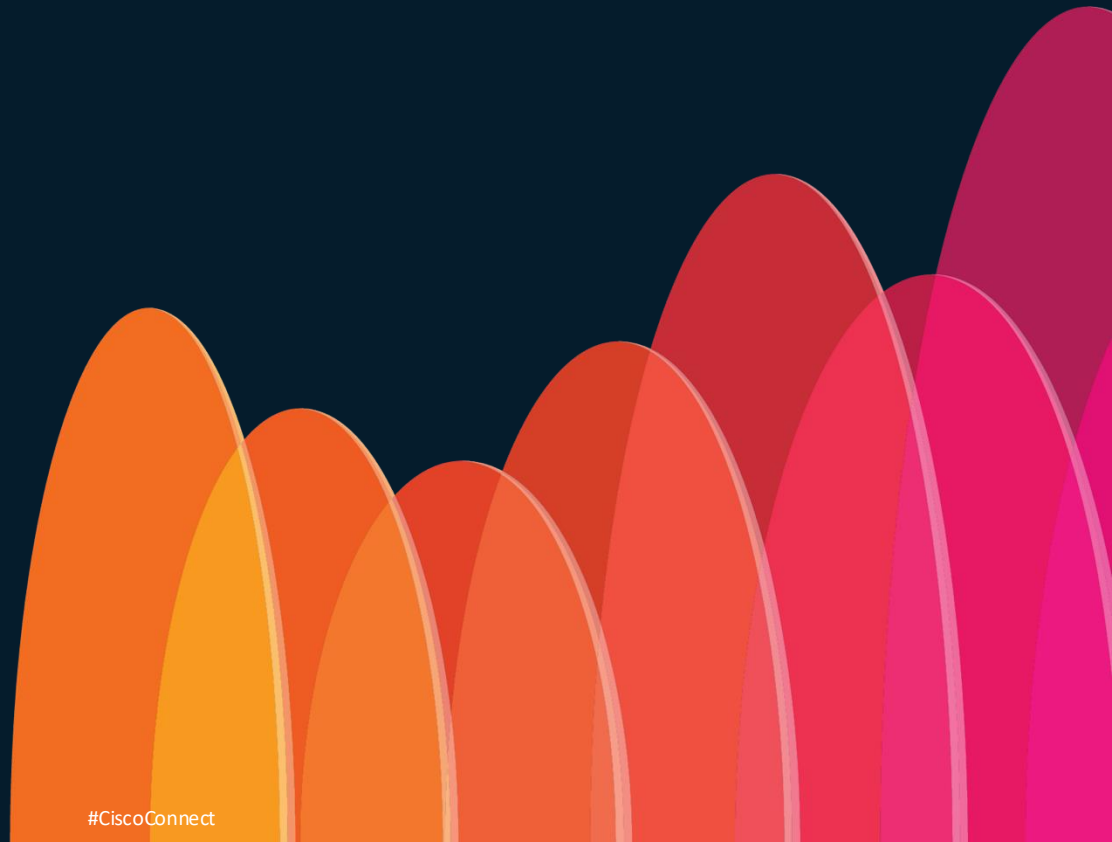
How to choose ?



Expected Outcomes :

- Asset inventory
- Automation
- Multi-Sources
- Out of the box detection
- Prioritization
- Complete Visibility
- Noise reduction
- AI Enabled
- Investigation Framework

XDR and Splunk in the wild



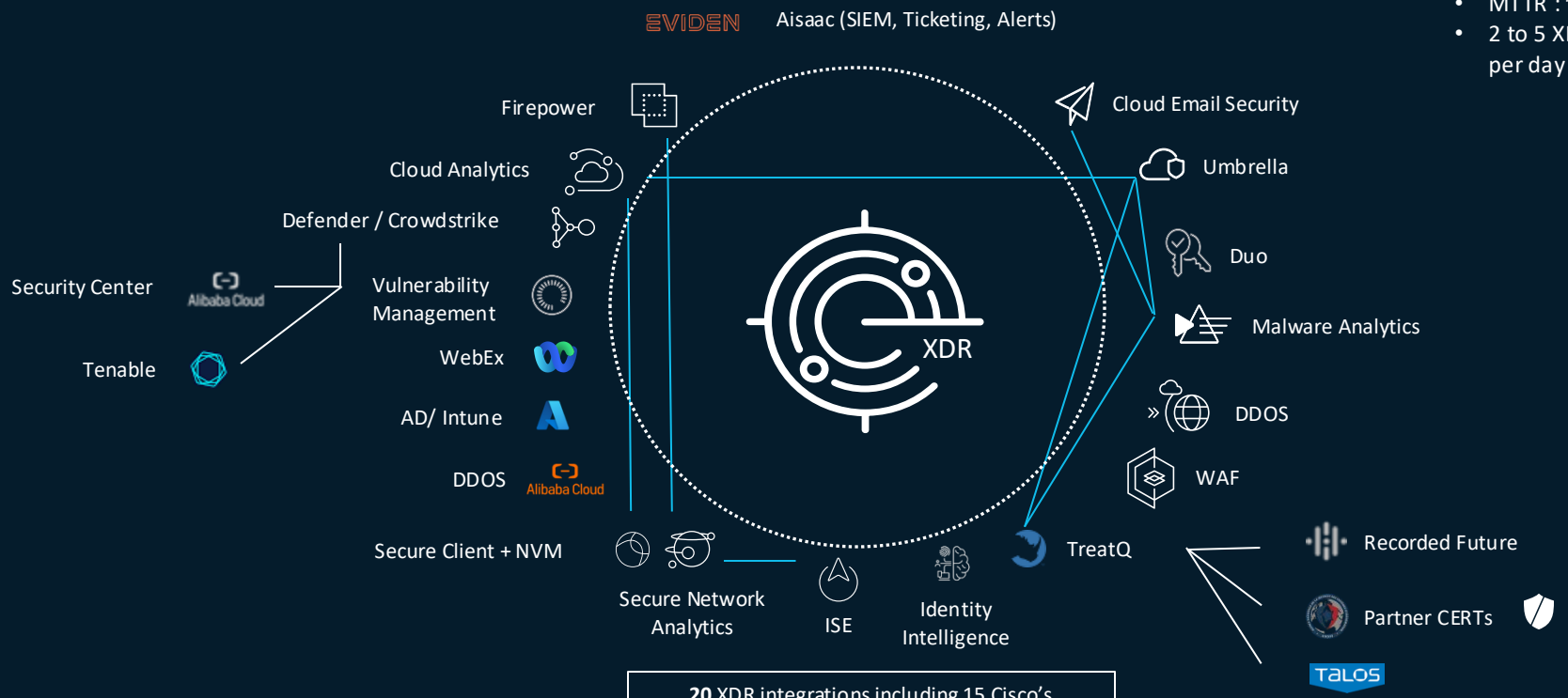
cisco Connect

Cisco XDR @Major sport event 2024

Direct Integrations

KPI :

- 55B unique events
- 1000 security tickets
- MTTR : ~19min
- 2 to 5 XDR incident per day



Cisco Event SOC Team, using XDR and Splunk

- Black Hat
- RSA
- Cisco Live
- Global Sporting Events
- Mobile World Congress
- Upcoming Major Sport Event


cisco
Thank you
cisco Connect
#CiscoConnect

cisco Connect

GO BEYOND

#CiscoConnect