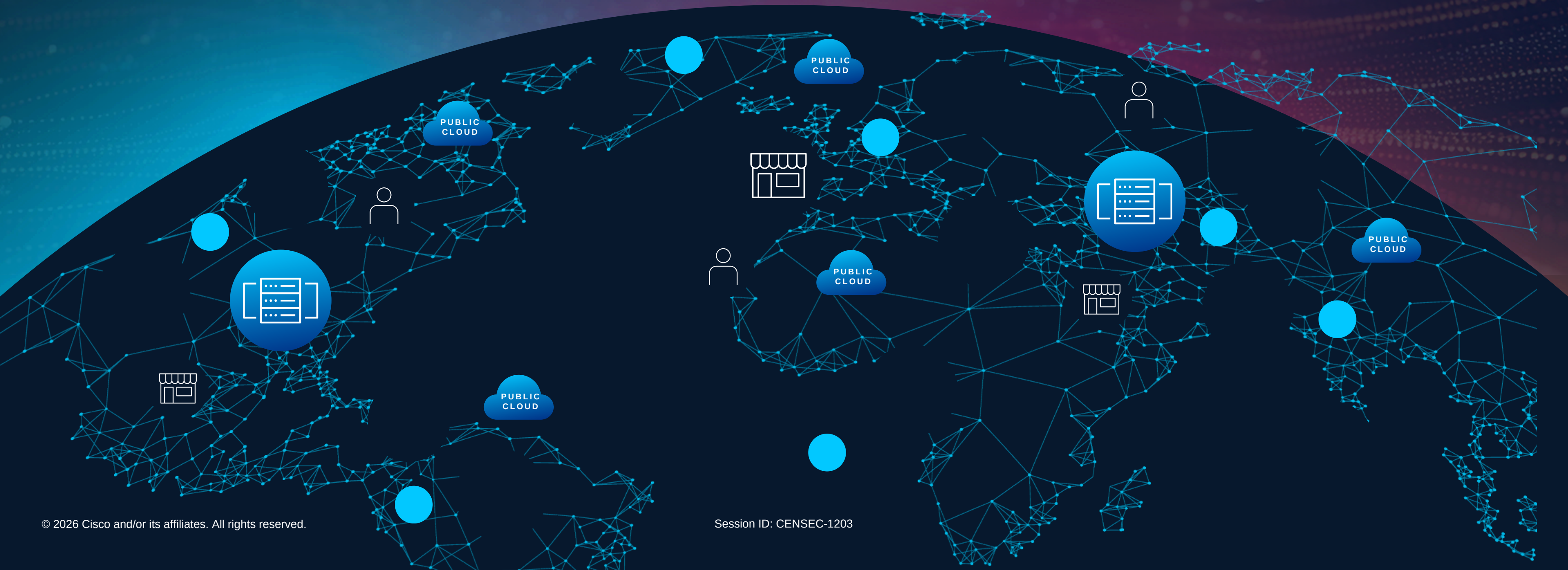


# Next Level SOC und Security Roadmap

Angelo Brancato  
Staff Security Specialist

# Our world has changed and so has everything you do





# The New Security Operating Model

Unify the data fabric, content, tooling, AI and automation in an analyst experience, to identify and stop threats before they impact the business.

Oof! That's a mouthful – let's break it down...

# Inventory for the Next Level SOC



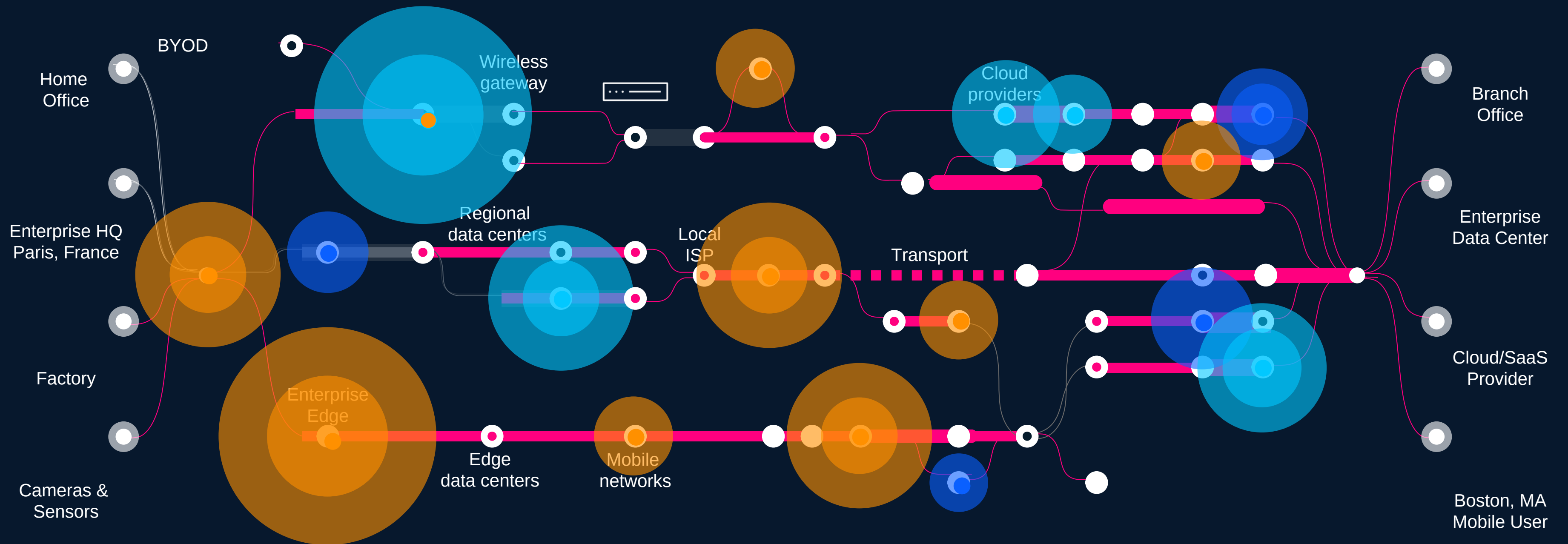
Easy as 1 - 2 - 3

# Inventory for the Next Level SOC



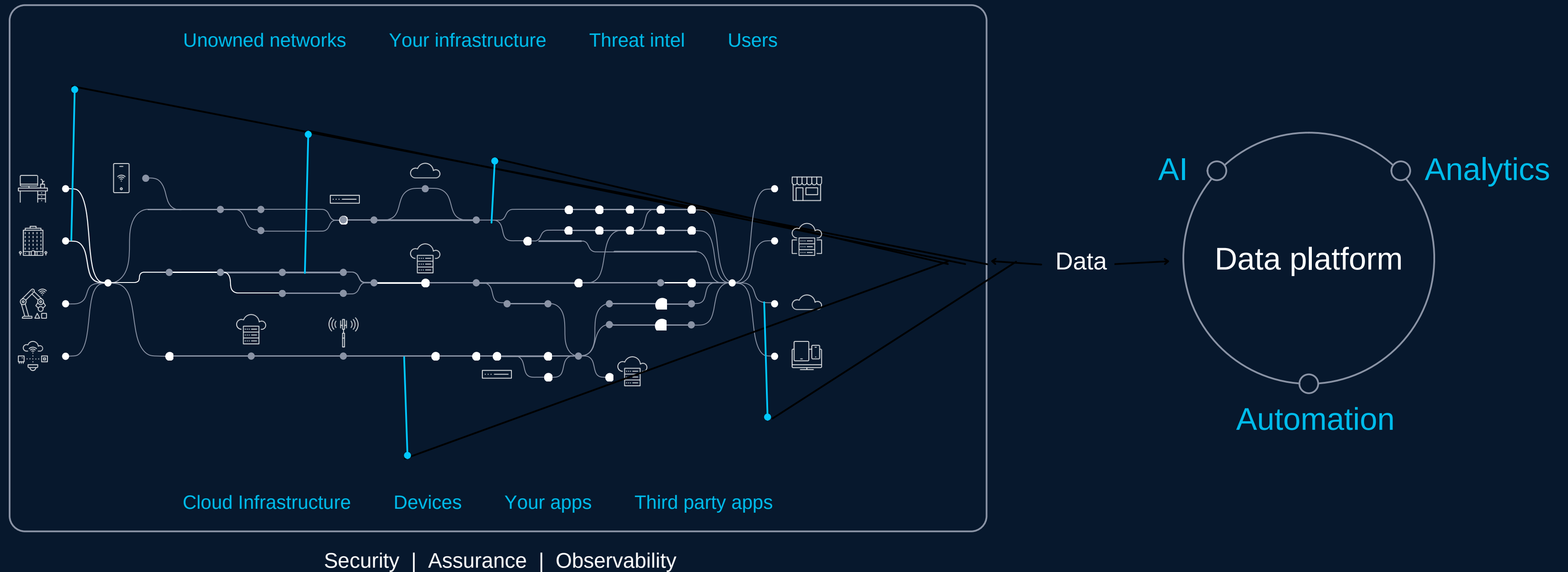
## 1. DATA MANAGEMENT

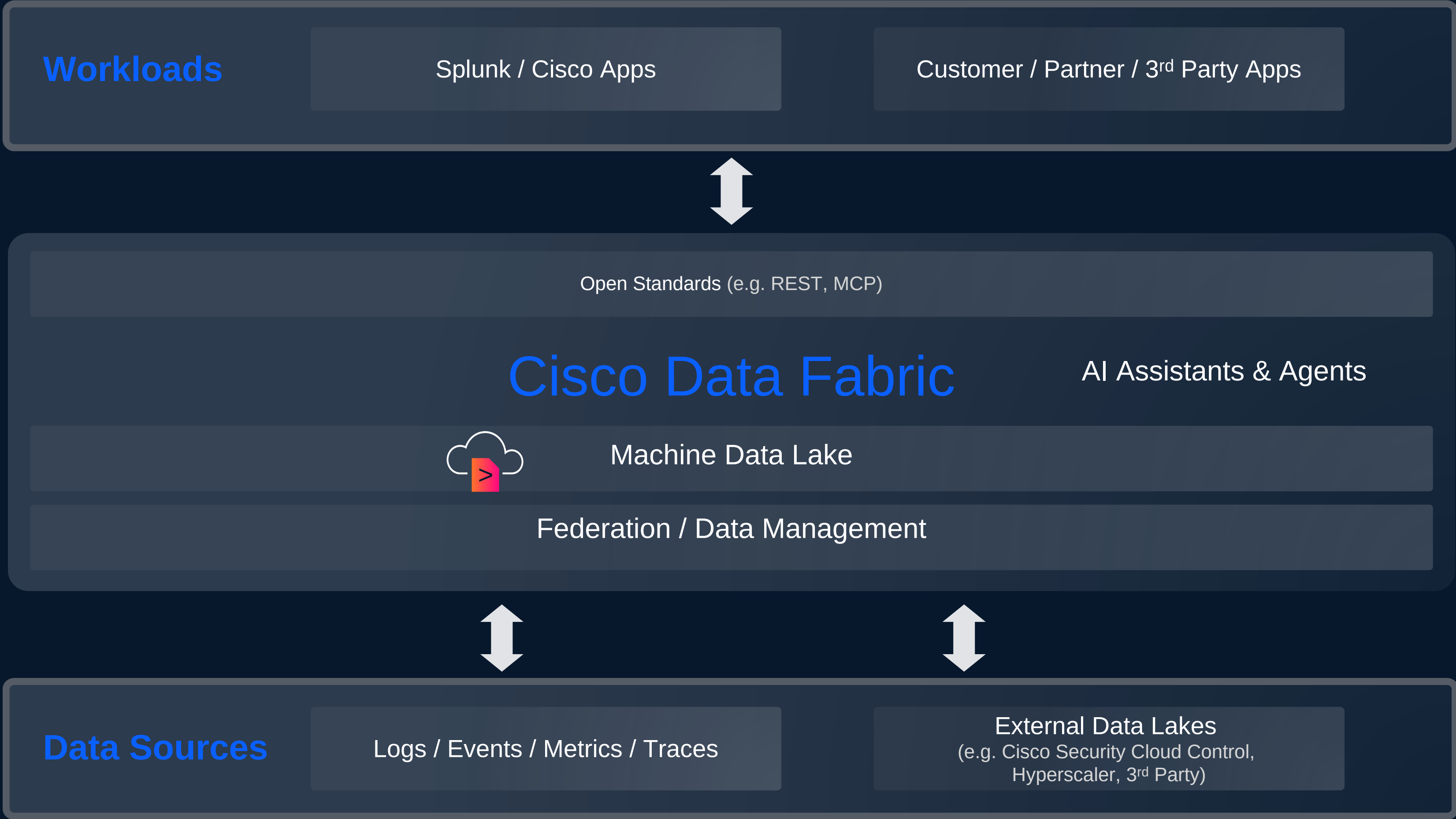
# Complexity explosion is getting worse



# The power of Splunk and Cisco means you can unify data

across the digital footprint to drive resilience and better outcomes





# Inventory for the Next Level SOC



**1. DATA MANAGEMENT**

**2. DETECTION CONTENT**

# Cisco XDR

- Turn-Key Solution
- Network at the core
- Open Architecture
- XDR is **Speed & Simplicity** – It hands over to Splunk ES for **Scale & Sophistication**



Incident 453

## Multi-Stage Malware Attack with Exfiltration

Overview Detection Response Worklog Report

### Summary

On October 8th, 2024, user Darin received a phishing email, resulting in the IcedID malware installation on endpoint Darin-windows11 and subsequent communication with a suspicious IP.

By October 9th, 3.2 GB of data was exfiltrated from endpoint misty-windows to an external IP.

October 8th 2024  
12:43 UTC

#### Initial Access

##### Phishing Email Sent

A phishing email **Open Now! Bonus** was sent to user **Darin** from **tom.j@explorcorp.com**.

16:09 UTC

#### Execution

##### Connection to Malicious Website

The endpoint **Darin-windows11** accesses the suspicious domain **www.bonuspayments.com**.

#### Malware Installation

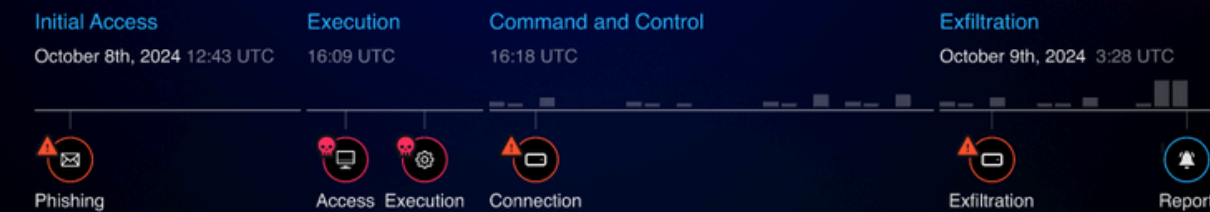
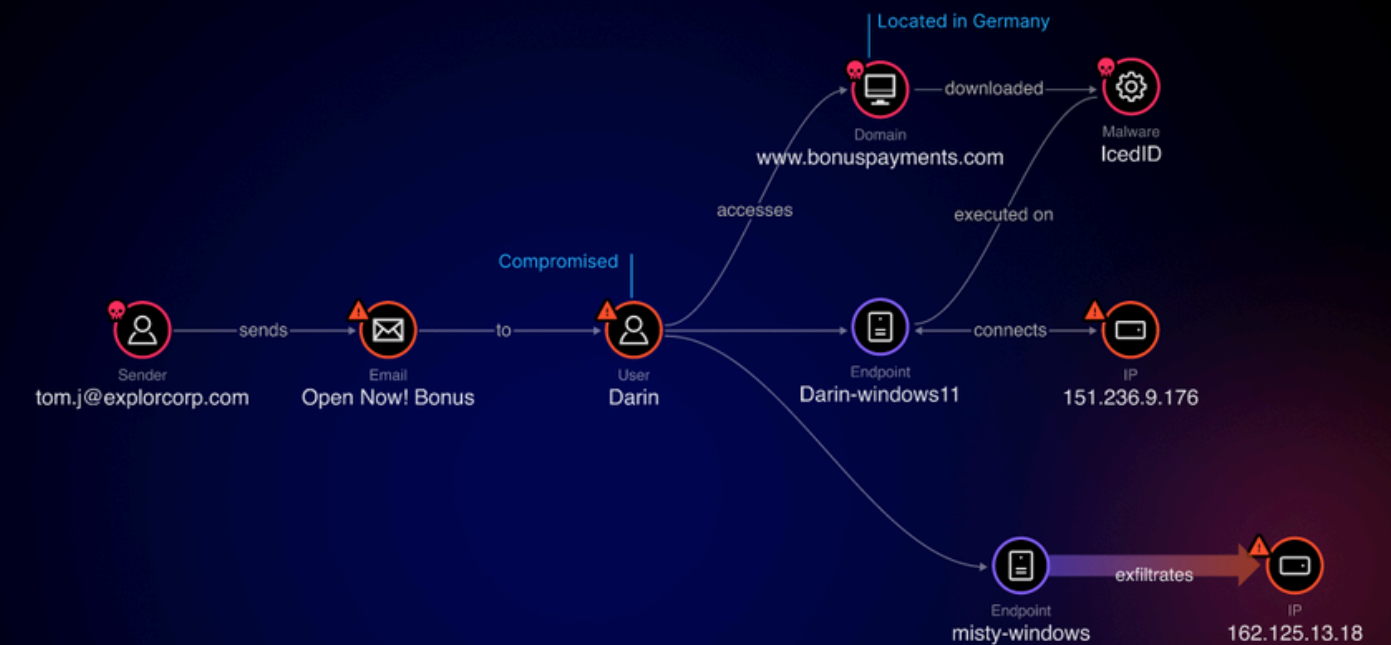
The malware **IcedID** file was downloaded from to **www.bonuspayments.com** to endpoint **Darin-windows11**.

16:18 UTC

#### Command and Control

##### Connection to Suspicious IP

The endpoint **Darin-windows11** communicates with the suspicious domain IP **151.236.9.176**.



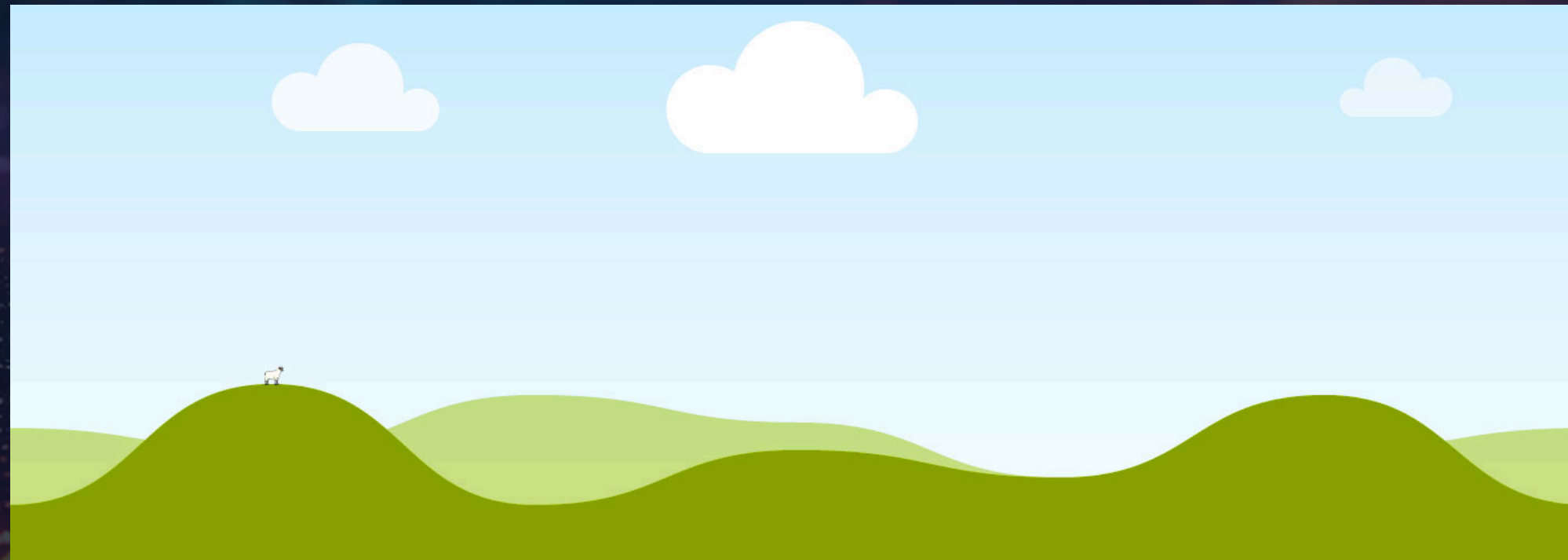
# Enterprise Security (ES)

- **Best in Class Analyst Experience** and tooling with unified TDIR
- **Integrated SIEM, UEBA, TIM, SOAR**
- **AI Assistant and Agents** across every layer

The screenshot displays the Splunk Enterprise Security (ES) interface. The main finding is titled "Malicious PowerShell Process - Encoded Command On FYODOR-L.splunkshirtcompany.com" with ID ES-00007. The interface is divided into several sections:

- Overview:** Shows the finding title and a MITRE ATT&CK map. The map highlights "Phishing" (1 of 14 techniques, 7%) and "Command and Scripting Interpreter" (1 of 39 techniques, 3%), with "PowerShell" being a sub-technique of the latter.
- MITRE Attack:** Lists annotations: T1059.001, TA0002, Technique: PowerShell, and Technique ID: T1059.001.
- Events:** Shows event details: Event ID: a7fb2125-4a31-497b-bbab-d2b4eb096de1@@notable@@time1773313899, Event type: modnotable\_results (modaction\_result), notable.
- Drill-down search:** Shows "Process creation events for this process" with an "Original event" section.
- Adaptive responses:** A table showing response actions:

Response	Mode	Time	User	Status
TruSTAR - Enrich Threat Activity NEs	saved	2026-03-12T11:11:42+0000	admin	Failure
Risk Analysis	saved	2026-03-12T11:11:40+0000	admin	Success
Finding	saved	2026-03-12T11:11:39+0000	admin	Success
- Info Panel (Right):** Contains metadata: Owner: unassigned, Status: New, Urgency: Medium, Sensitivity: Unassigned, Disposition: Undetermined, ID: ES-00007, Type: Investigation, Time: Mar 12th, 2026 2:51 PM, Last updated: Mar 12th, 2026 2:51 PM, Reference ID: 7c1881ff-52d6-43f8-8904-b414ffa1f2bf, Investigation type: default, Description: This search looks for PowerShell processes that have encoded the script within the command-line. Malware has been seen using this parameter, as it obfuscates the code and makes it relatively easy to pass a script on the command-line.



# ES - Detection Studio

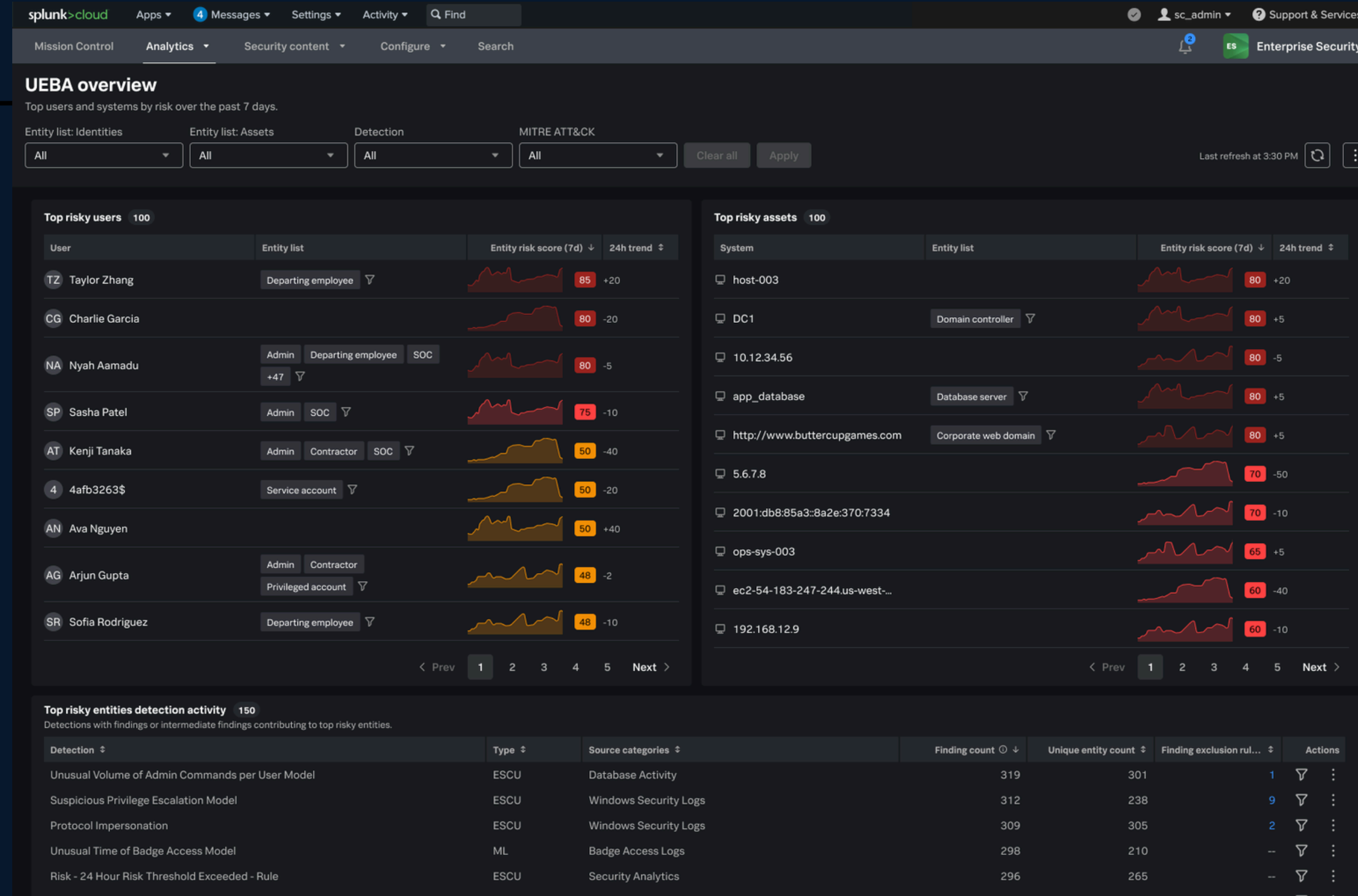
- Streamlines Detection-As-Code
- Monitors Detection-Coverage and Health
- MITRE ATT&CK coverage

The screenshot displays the Splunk ES Detection Studio interface. The top navigation bar includes 'splunk>cloud', 'Apps', 'Messages', 'Settings', 'Activity', and 'Find'. The main content area is divided into several sections:

- Filters:** A sidebar on the left with various filter categories: Quick filters (All detections), Detection KPIs (Recommended: All, Priority: High, Confidence: All confidence, Impact: All impact, Compatibility: All compatibility, Performance: All performance), Detection Config. (Deployed State: All, Finding Type: All), Data (Data Source: All data sources, Modeled Data: All data models, All datasets, Un-Modeled Data: All services, All types).
- Detections Dashboard:** A central area showing 'Overall detection technique coverage' at 65% (up 5%) and 'Highest priority detections' at 72% (Top 15% of detections). It includes a 'Filter Detections' button.
- Detections List:** A table of detection rules with columns for Name, Priority, and various metrics. The 'ESCU - ICACLS Grant Command - Rule' is highlighted.
- Details Panel:** A right-hand panel for the selected rule, showing 'ESCU - ICACLS Grant Command - Rule' with a description, priority (High), and a 'Compatibility' score of 98 (High compatibility). It also includes a 'Detection Logic' section with a list of search queries.

# ES - UEBA Insider Threat Detection

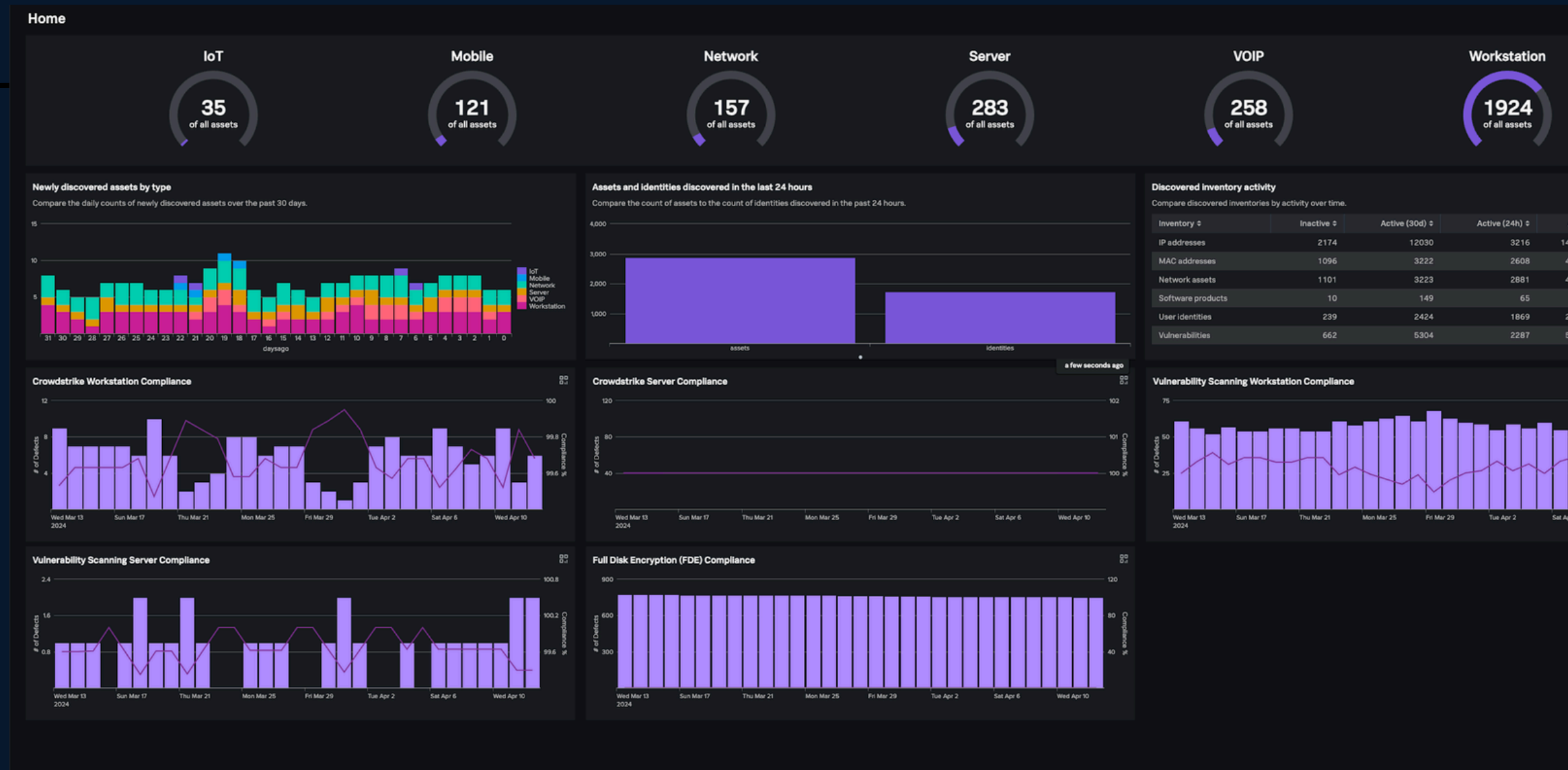
- Detects **abnormal** user and system behavior
- **Unsupervised** Machine Learning
- Identify **insider risks** — including compromised accounts, privilege misuse, lateral movement, data exfiltration etc.



# ES - Exposure Analytics

Coming Soon

- **Continuously discover assets, identities and services** across on-prem, cloud and hybrid environments
- **Enriches** detections and investigations with **context** allowing prioritization based on actual risk
- **Real-Time Risk Reports**



# Inventory for the Next Level SOC



- 1. DATA MANAGEMENT**
- 2. DETECTION CONTENT**
- 3. AUTOMATION & AI**

# ES - AI Assistant

- Explain Findings & Investigations
- Suggest next steps
- Generate SPL
- Generate Investigation Report

The screenshot displays the Splunk Enterprise Security (ES) interface. The main panel shows an investigation titled "24 hour risk threshold exceeded for system=win-dc.attackrange.local" with ID ES-00137. The interface includes a navigation bar with options like Queue, Overview, Response, Events, Search, Automation, and Intelligence. The MITRE ATT&CK map is visible, showing a grid of techniques categorized into Reconnaissance, Resource Development, Initial Access, Execution, Persistence, and Privilege Escalation. The "Execution" category is highlighted, showing techniques like "Scheduled Task/Job", "Command and Scripting Interpreter", and "PowerShell".

On the right side, there is an "Info" panel with fields for Owner (Angelo Brancato), Status (In Progress), Urgency (High), Sensitivity (Red), Disposition (True Positive - Suspicious Activity), ID (ES-00137), Type (INVESTIGATION), Time (Jul 10th, 2025 8:29 AM), Last updated (Jul 10th, 2025 9:02 AM), Reference ID (27cc2ef0-31df-459a-85ed-ab5974862800), Investigation type (demo), and Description (Risk Threshold Exceeded for an object over a 24 hour period).

At the bottom right, there is a chat window for the "AI Assistant for Security". The chat history shows a user request: "please explain this incident to me" and an AI response: "Based on the investigation data, here's a breakdown of the incident:". A "Generating a response" indicator is visible at the bottom of the chat window.

# ES - Triage Agent

Coming Soon

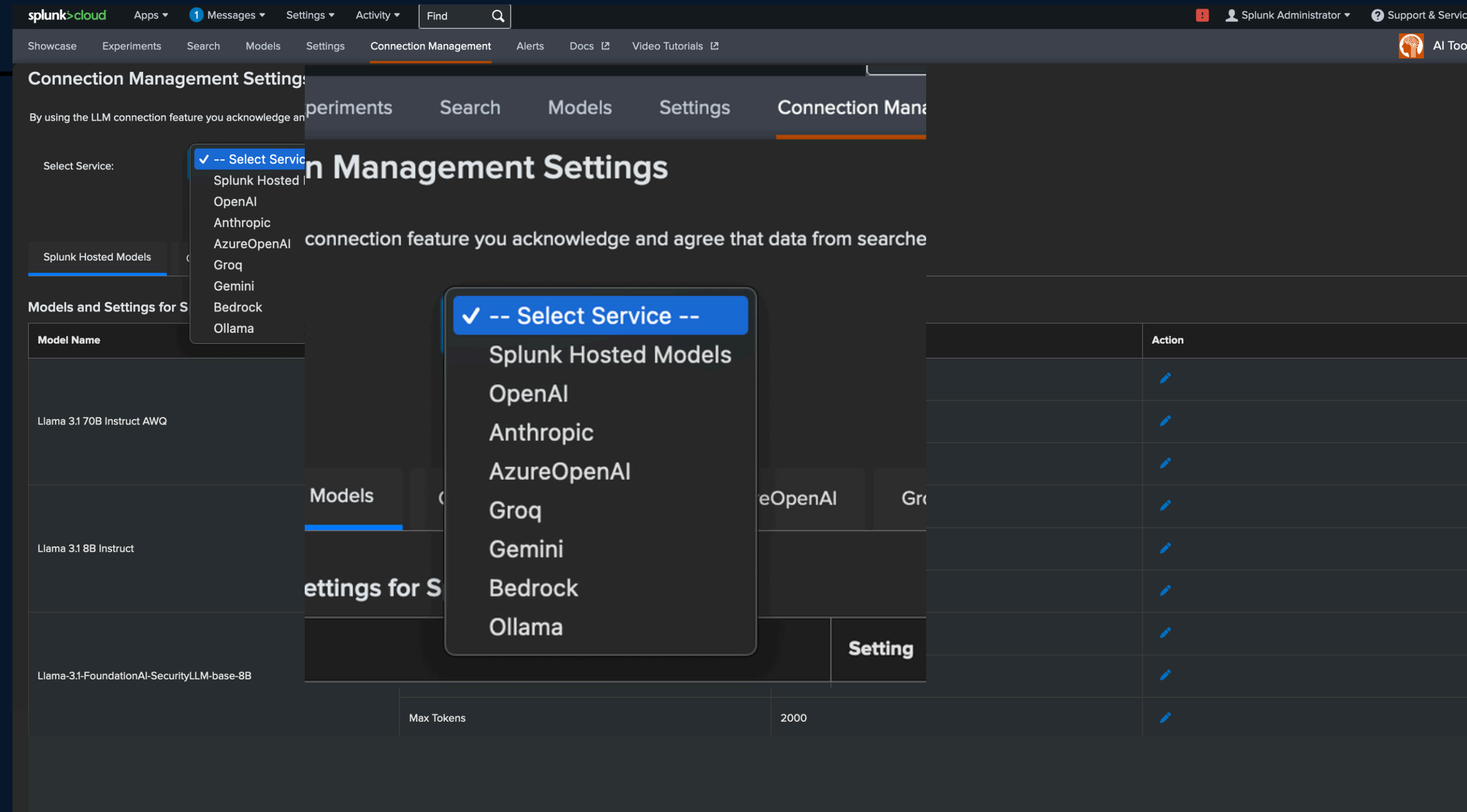
- Automatically determine alert disposition
- Streamline alert prioritization
- Plan and execute investigations
- Automate insights to reduce MTTR

The screenshot displays the Splunk Cloud Analyst Queue interface. The top navigation bar includes 'splunk>cloud', 'Apps', '4 Messages', 'Settings', and 'Activity'. The main header shows 'Mission Control', 'Security analytics', and 'Security content'. A 'Last 24 hours' filter is visible. The left sidebar lists 'Default views' with options like 'All', 'Owned by me', 'Unassigned', 'Risk score', 'Saved views', 'My critical items', 'Unassigned SLA expiring', and 'Insider threat'. The main area is titled 'Analyst queue' and shows a list of alerts with columns for 'Title', 'ID', 'Disposition', 'Owner', and 'Risk Score'. A dropdown menu for 'AI suggested disposition' is open, showing options: 'True positive' (checked), 'Benign positive', 'False positive', 'Other', and 'Undetermined'. The alert list includes items like 'Malicious PowerShell exec', '24 hour risk threshold exce user=administrator', 'Possible Phishing Attack', 'Unusual network activities', '3 failed login attempts with', 'Threat Activity Detected from 56.143.202.14 to 8.108.191.107', and 'Email files written outside of the Outlook directory'.

ID	Disposition	Owner	Risk Score
FI-AB543	True positive		5
FI-AB233	True positive		3
FI-AB198	True positive	NA Nyah Aamadu	40
FI-AB558	True positive	8,108.191.101	94
FI-AB352	True positive	KT Kenji Tanaka	45

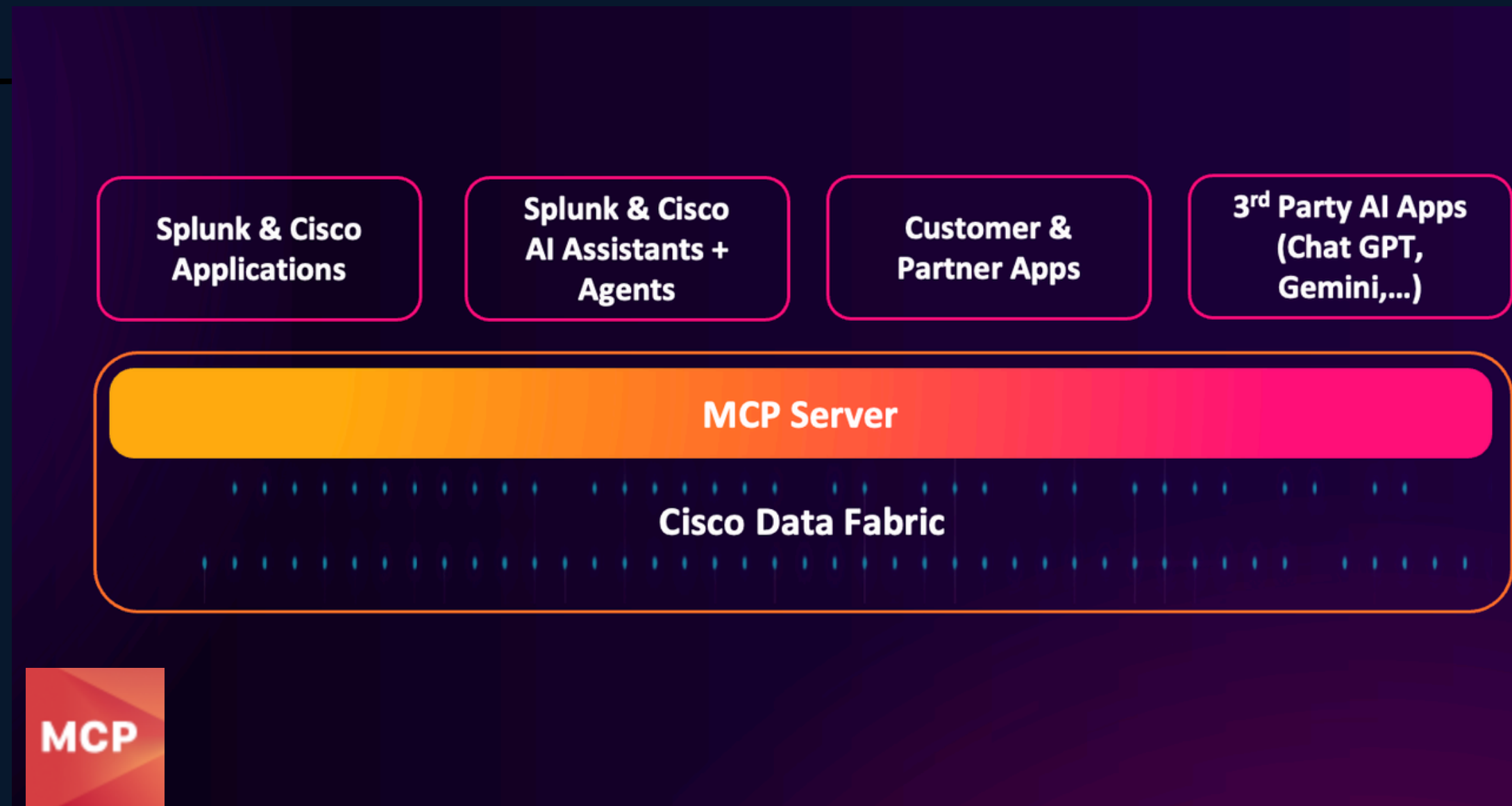
# Core - AI Toolkit with LLM Integrations

- **Build, deploy, share your own ML models**
- **Connect 3rd party LLMs**
- **Regulation (e.g. AI-Act), Data Classification or Data Sovereignty**



# Core – MCP Server

- **Natural Language Interaction** with Splunk from any AI App that speaks MCP
- **Simple integration** with your ecosystem for **Agentic Workflows**
- Delivering a new class of cross-domain **operational intelligence**



# SAA - Malware Reversing Agent

- Explains malicious scripts line-by-line
- Extracts IOCs, flags evasion, and groups recurring behaviors
- Gives analysts actionable insight in seconds, not hours.

The screenshot displays the SAA Malware Reversing Agent interface. At the top, there is a purple bar labeled "AI analysis". Below this, there are tabs for "Summary", "MITRE TTPs", and "IOCs and Recommendations". The "Summary" tab is active, showing a "100 Malicious" status. The main content area contains a description of the script, a "Technical Analysis" section with 9 steps, a "Relevant code" section with a code snippet, a "Description" section, a "Purpose" section, and an "Example matching Regex" section. On the right side, there is a "Disposition" dropdown set to "True positive", a metadata table with fields like ID, Type, Time, Last updated, Reference ID, Investigation type, and Description, a "Notes" section with a text input and a "Save" button, and a "Files" section with a "Drop your files here or browse" prompt.

AI analysis

Summary MITRE TTPs IOCs and Recommendations

**100 Malicious**

Script downloads an MSI from a remote host and silently installs it via msixec. Uses WebClient to fetch payload, silent installation, file cleanup

**Technical Analysis**

- Step 1: Configure PowerShell to use TLS12 for secure connections
- Step 2: Define the URL for the MSI payload
- Step 3: Construct the temporary file path in the %TEMP% directory
- Step 4: Instantiate a WebClient object and set a custom User-Agent header
- Step 5: Download the MSI from the remote server to the temporary path
- Step 6: Verify the downloaded file exists at the temporary location
- Step 7: Invoke mslexec.exe to Install the MSI silently with no restart
- Step 8: Remove the MSI installer file after successful installation
- Step 9: Handle any errors during download or installation and perform cleanup
- Obfuscation techniques identified: None

**Relevant code**

```
[Net .ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]:: Tls12
```

**Description**

TLS configuration for Power Shell remoting (Step 1 from analysis)

**Purpose**

Enforces usage of TLS1.2 for secure network communications. Prevents fallback to weaker SSL/TLS protocols.

**Example matching Regex**

```
/\[Net\.ServicePointManager\]::SecurityProtocol\s*=\s*\[Net\.SecurttyProtocolType\]::Tls12/
```

`$url = 'https://80.173.153.160.host.secureserver.net/4774321123565 .msi'`

Disposition: True positive

ID	ES-00004
Type	Investigation
Time	Today 10:20 AM
Last updated	Today 10:20 AM
Reference ID	84b056d2-9263-49b8-ad5b-c322f81da461
Investigation type	Default
Description	This detection identifies the execution of potent... <a href="#">Show more</a>

Notes: 0

Enter note

Save

Files: 0

Drop your files here or browse  
all file types supported

# SOAR - AI Playbook Authoring

Coming Soon

- Accelerate time to automation
- Translate natural language intent into functional building playbooks faster and easier
- Empowers security teams to automate **without dedicated developers**

The screenshot displays the SOAR AI Playbook Authoring interface. At the top, there is a navigation bar with the Splunk logo, the text 'SOAR', and a search box containing 'Example playbook'. Below the navigation bar is a vertical sidebar with various icons representing different actions or tools. The main workspace shows a 'Start' button with a folder icon. Below the 'Start' button, there is a task card with a star icon and a paper plane icon. The task card contains the text 'Build a playbook to isolate a host with EDR'. Below this text, there is a paragraph explaining the process: 'To do this, we will first need to get additional context of the suspicious host with a custom code block, and then isolate the host by the action block.' Below the paragraph, there are two blocks of actions: 'CODE Custom code' and 'ACTION Isolate host'. Each block has a plus sign icon to its right. At the bottom of the task card, there is an 'Add all' button.

# ES - AI Assistant for Detection Authoring

Coming Soon

- **Generate SPL** for the detection based on natural language description
- Iterate on detection SPL to **refine detection** to be usable in your environment
- Get **detailed descriptions and explanations**

Malicious PowerShell Execution

Enterprise Security

Enterprise Security

App configured for drill-down search links or email adaptive response actions. If no app is selected, the UI app context is used by default.

The following analytic identifies suspicious PowerShell execution using Script Block Logging (EventCode 4104). It leverages specific patterns and keywords within the ScriptBlockText field to detect potentially malicious activities. This detection is significant for SOC analysts as PowerShell is commonly used by attackers for various malicious purposes, including code execution, privilege escalation, and

Add information on what the detection searches for and the security use case addressed by the detection. For example: **Identify excessive number of failed login attempts** (likely to detect a brute force attack).

[Customize](#) [Guided mode](#)

```
index=* sourcetype="XmlWinEventLog:Microsoft-Windows-PowerShell/Operational" EventCode=4104
| rename ComputerName as dest, UserID as user, ScriptBlockText as script
| stats count min(_time) as firstTime max(_time) as lastTime by dest, user, script
| `drop_dm_object_name(Processes)`
| eval script=coalesce(process, "")
| eval is_encoded_command = if(match(script, "(?i)-e(nc*o*d*e*d*c*o*m*m*a*n*d*)*\s+[^-]") OR
match(script, "[A-Za-z0-9+/\]{44,}={0,2}"), "Yes", "No")
| eval uses_iex = if(match(script, "(?i)(iex|invoke-expression)", "Yes", "No")
| eval downloads_from_web = if(match(lower(script), "(http|webclient|downloadfile|downloadstring)", "Yes", "No")
| eval contains_mimikatz = if(match(lower(script), "mimikatz|-dumpcr"), "Yes", "No")
| eval suspicious_cmdlet = if(match(script, "(?i)(Invoke-Mimikatz|Get-GPPPassword|Invoke-
CredentialInjection|Invoke-BypassUAC|Invoke-ReflectivePEInjection)", "Yes", "No")
| where is_encoded_command="Yes" OR uses_iex="Yes" OR downloads_from_web="Yes" OR
contains_mimikatz="Yes" OR suspicious_cmdlet="Yes"
| stats count as event_count,
values(is_encoded_command) as encoded_command_detected,
values(uses_iex) as invoke_expression_detected,
values(downloads_from_web) as web_download_detected,
values(contains_mimikatz) as mimikatz_keyword_detected,
values(suspicious_cmdlet) as suspicious_cmdlet_detected,
values(script) as full_command_line
by dest, user
```

The following SPL query is customized to your environment and connects existing indexes, fields, and data models.

```
SPL
| tstats `security_content_summariesonly` count min(_time) as
firstTime max(_time) as lastTime
from datamodel=Endpoint.Processes
where Processes.process_name=powershell.exe
by Processes.dest Processes.user Processes.process
| eval is_encoded_command = if(match(script, "(?i)-
e(nc*o*d*e*d*c*o*m*m*a*n*d*)*\s+[^-]") OR match(script, "[A-
Za-z0-9+/\]{44,}={0,2}"), "Yes", "No")
| eval uses_iex = if(match(script, "(?i)(iex|invoke-
expression)", "Yes", "No")
| eval downloads_from_web = if(match(lower(script), "(http|
webclient|downloadfile|downloadstring)", "Yes", "No")
| eval contains_mimikatz = if(match(lower(script), "mimikatz|-
dumpcr"), "Yes", "No")
| eval suspicious_cmdlet = if(match(script, "(?i)(Invoke-
Mimikatz|Get-GPPPassword|Invoke-CredentialInjection|Invoke-
BypassUAC|Invoke-ReflectivePEInjection)", "Yes", "No")
| where is_encoded_command="Yes" OR uses_iex="Yes" OR
downloads_from_web="Yes" OR contains_mimikatz="Yes" OR
suspicious_cmdlet="Yes"
| stats count as event_count,
values(is_encoded_command) as encoded_command_detected,
values(uses_iex) as invoke_expression_detected,
values(downloads_from_web) as web_download_detected,
values(contains_mimikatz) as mimikatz_keyword_detected,
values(suspicious_cmdlet) as suspicious_cmdlet_detected,
values(script) as full_command_line
by dest, user
```

[Use this SPL](#) [Open in search](#)



Ask me anything about...

Results from GenAI can vary; review for accuracy. [View AI details](#)

# Core – AI Canvas

Coming Soon

- **Ask:** Type what you want to know — for example:  
“Show me recent risky logins from unmanaged devices.”
- **See:** AI Canvas builds the visualization for you — charts, tables, or timelines based on real Security data.
- **Act:** Launch SOAR-powered actions right inside the workspace — enrich an IP, get user information, or check if you’ve seen these IOCs before.
- Enable analysts to move from **question** → **insight** → **response** in a single generative workspace.

The screenshot displays the Splunk AI Canvas interface. At the top, the navigation bar includes 'splunk>cloud', 'Apps', 'Messages', 'Settings', 'Activity', and a search bar. Below this, a secondary navigation bar lists 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', 'Dashboards', and 'AI Canvas'. The main workspace is titled 'AI Canvas | Detected Anomalous Network Activity'. On the right side of the workspace, there are three buttons: 'Generate report', 'View activity', and 'Share'. The central part of the workspace is divided into two panels. The left panel, titled 'AI Assistant', contains a welcome message: 'Welcome to AI Canvas. It looks like you came in from an alert about anomalous network activity. I've gone ahead and overlaid the historical trend on the Network Activity card.' Below this message are icons for liking, commenting, and sharing, along with a 'Show SPL' link. At the bottom of this panel is a text input field with the placeholder 'Ask the AI Assistant a question' and a blue arrow button. Below the input field is a disclaimer: 'Assistant can make mistakes. Verify responses.' The right panel, titled 'Network Activity', shows a line chart with 'Bytes\_Out' on the y-axis (ranging from 0 to 3M) and time on the x-axis (from 11:00 PM Sat Jul 19 2025 to 7:00 AM Sun Jul 20 2025). The chart displays a blue line for 'Bytes\_Out', a purple line for 'Thresholds', and two red dots for 'Anomalies'. A legend at the bottom of the chart identifies these elements: 'Anomalies: 2', 'Anomaly' (red square), 'Thresholds' (purple square), and 'Bytes\_Out' (blue line). In the bottom right corner of the workspace, there are icons for a share button and a text button, followed by a pink 'Get Started' button.

# AI Assistants, LLMs & Agents in Splunk



AI Assistants



External LLMs

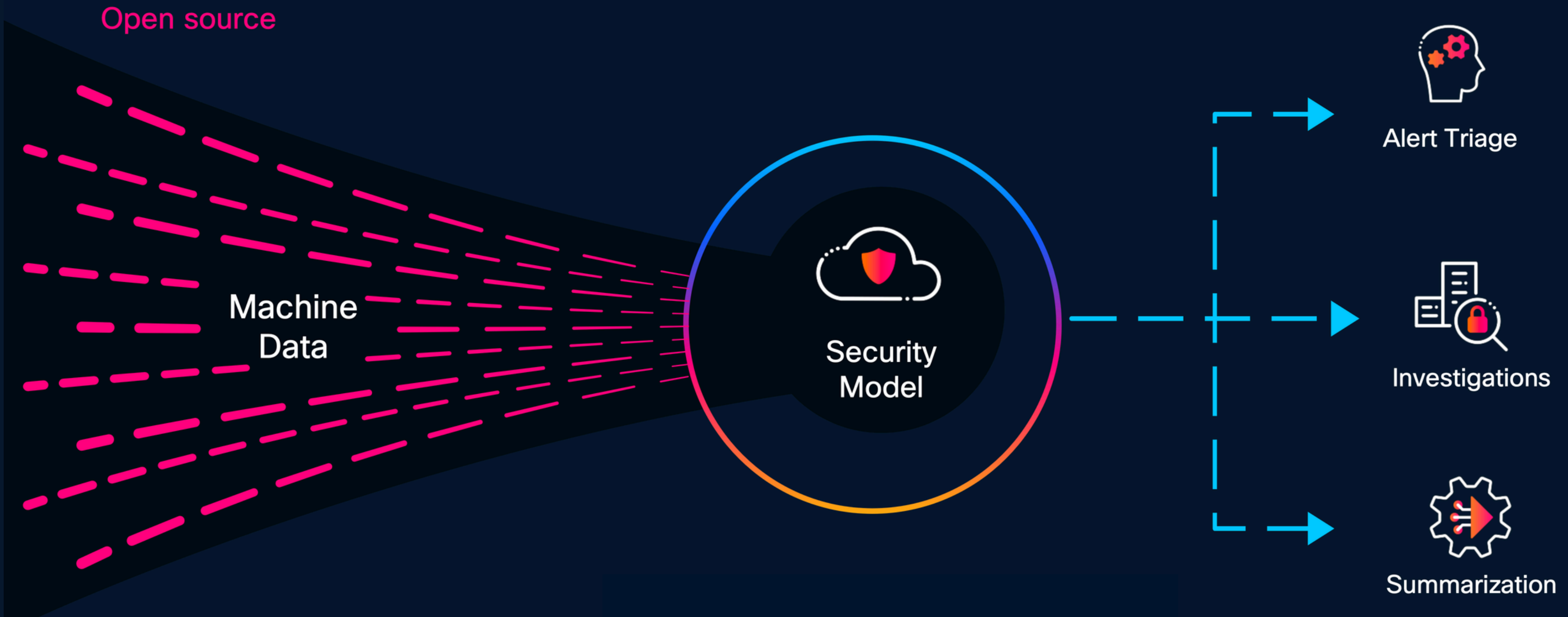


MCP

Thank you

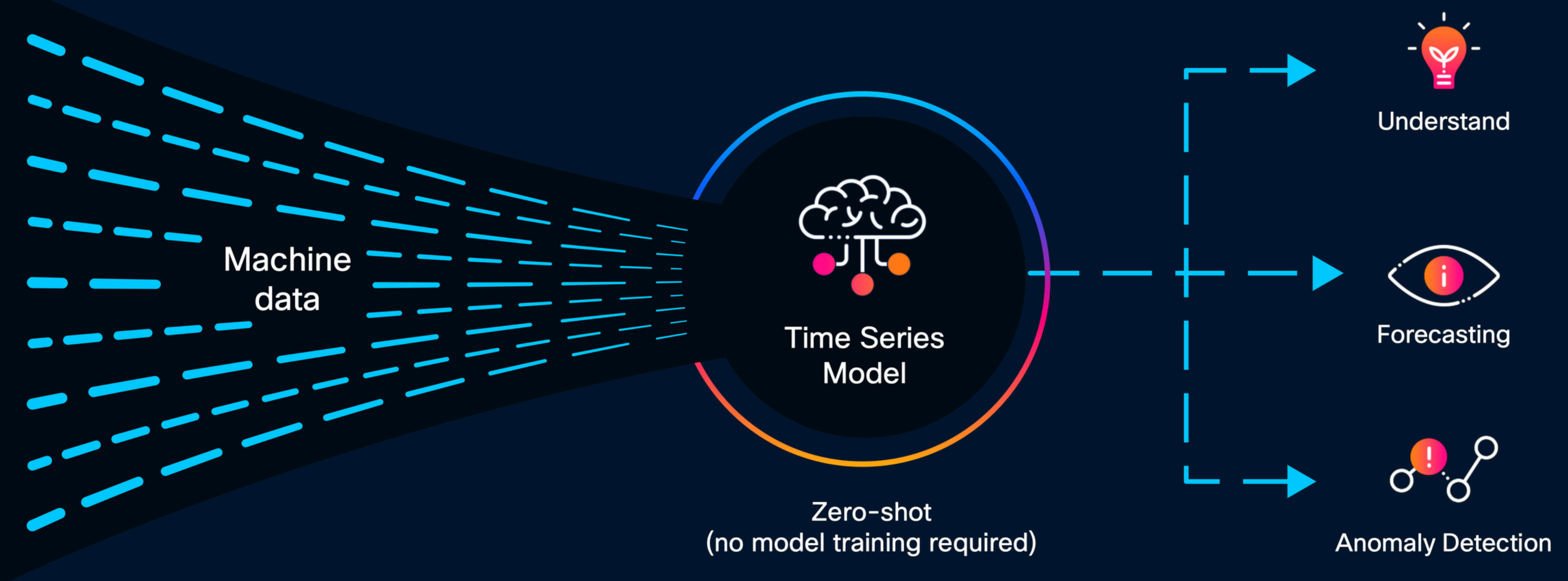


# Cisco Foundation AI Security Model (sec-1.1-8b-instruct)



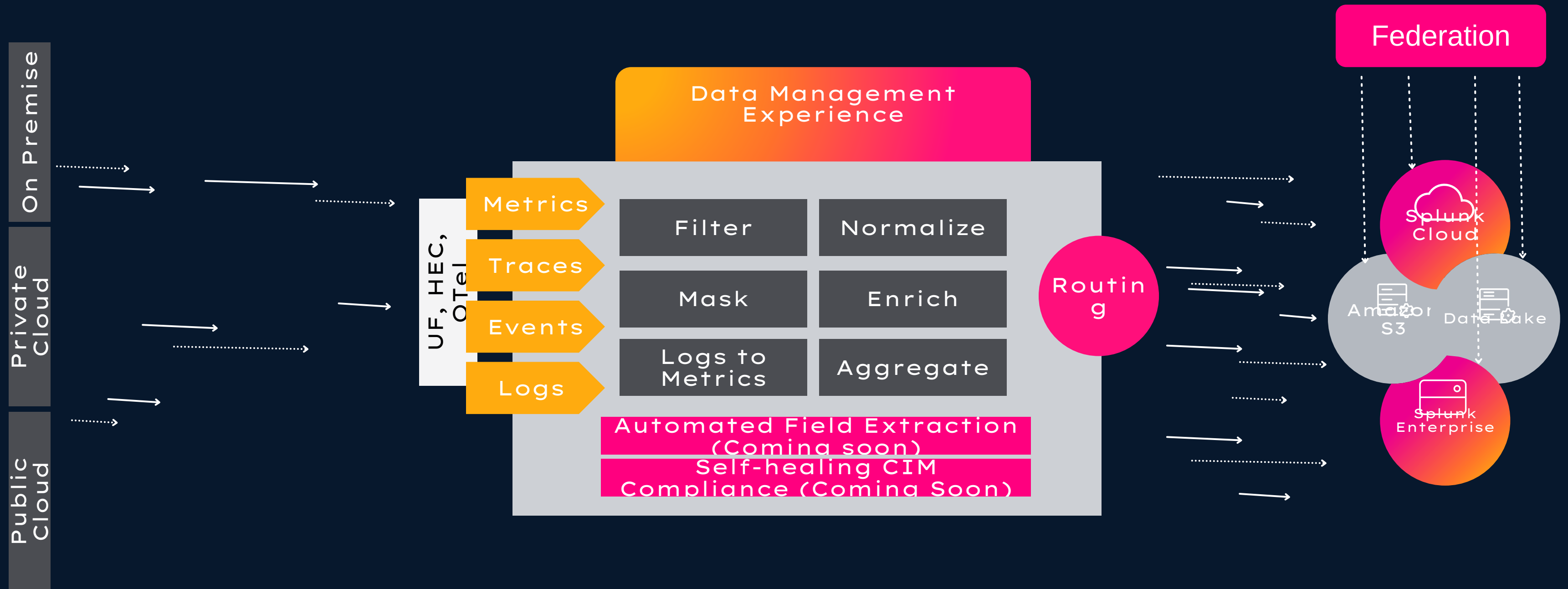
# Cisco Time Series Model

Beta release Feb 18, 2026



# Splunk Data Management Experience (DMX)

Unified data configuration, processing, and management



# Because not all Data is the same

