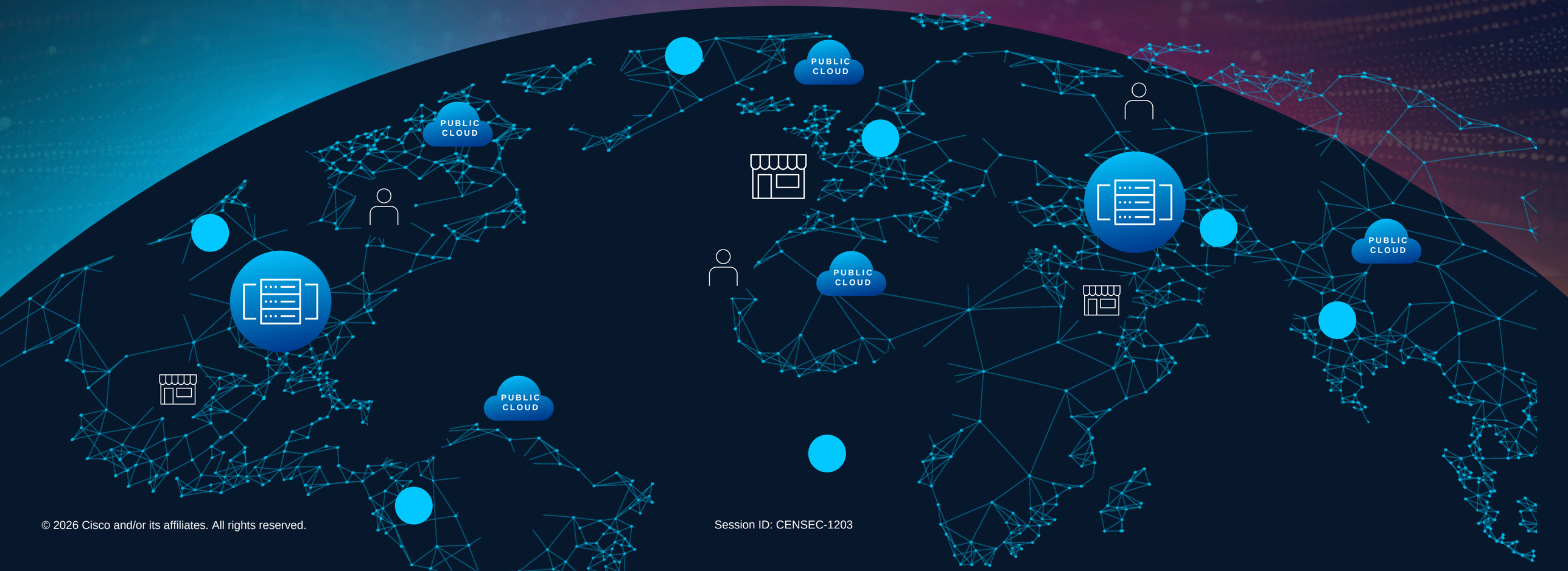
Next Level SOC und Security Roadmap

Angelo Brancato
Staff Security Specialist

January 2026

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…

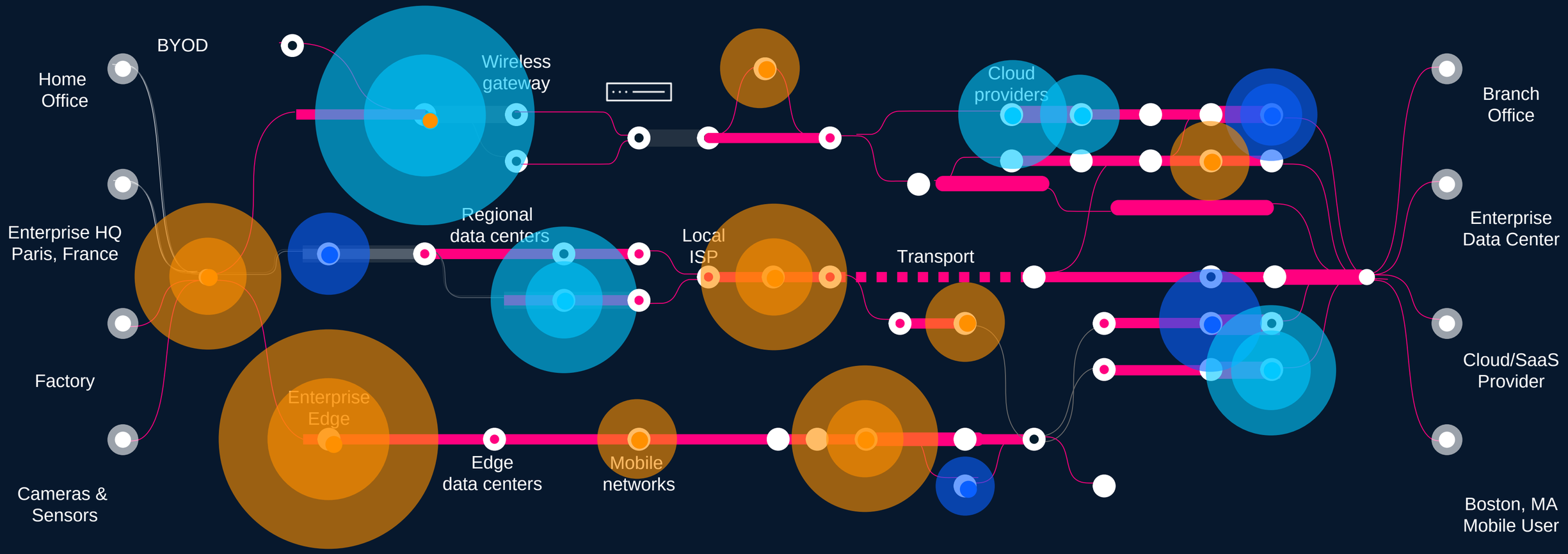
Inventory for the Next Level SOC

Easy as 1 - 2 - 3

Inventory for the Next Level SOC

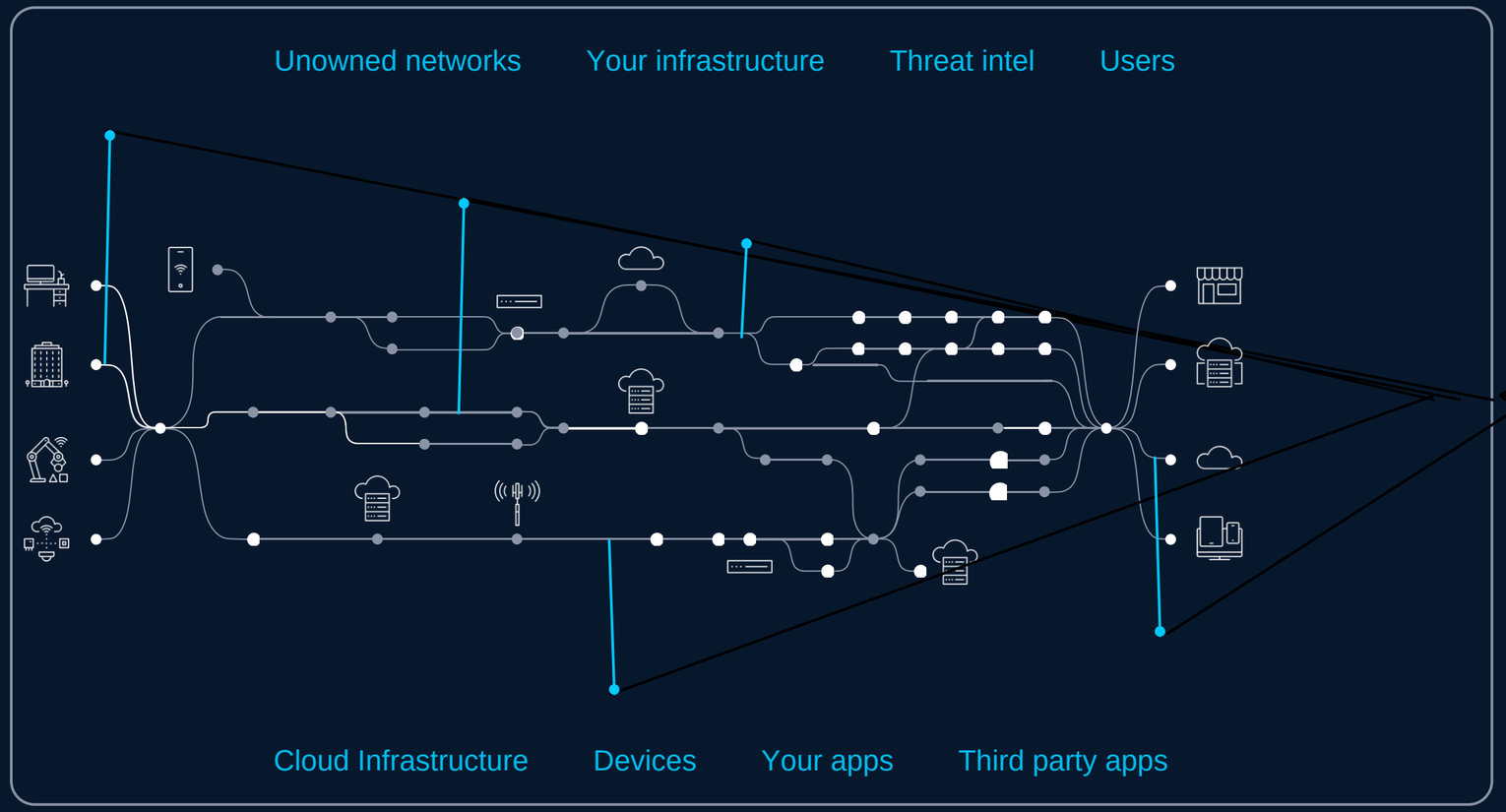
1. DATA MANAGEMENT

Complexity explosion is getting worse

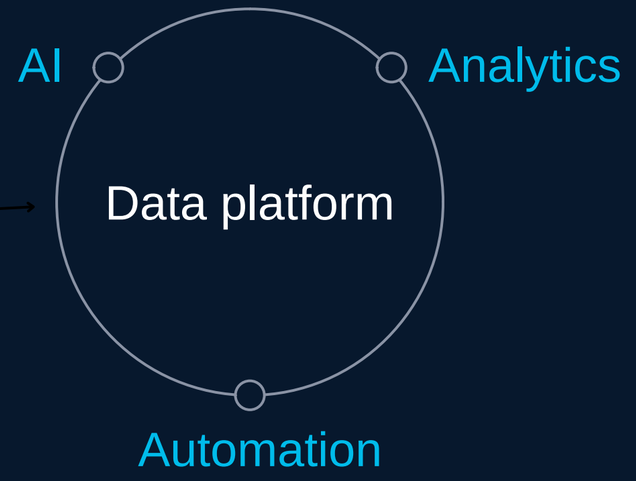


The power of Splunk and Cisco means you can unify data

across the digital footprint to drive resilience and better outcomes



Data



Security | Assurance | Observability

Workloads

Splunk / Cisco Apps

Customer / Partner / 3rd Party Apps

Open Standards (e.g. REST, MCP)

Cisco Data Fabric

AI Assistants & Agents

Machine Data Lake

Federation / Data Management

Data Sources

Logs / Events / Metrics / Traces

External Data Lakes
(e.g. Cisco Security Cloud Control, Hyperscaler, 3rd Party)

Inventory for the Next Level SOC

1. DATA MANAGEMENT

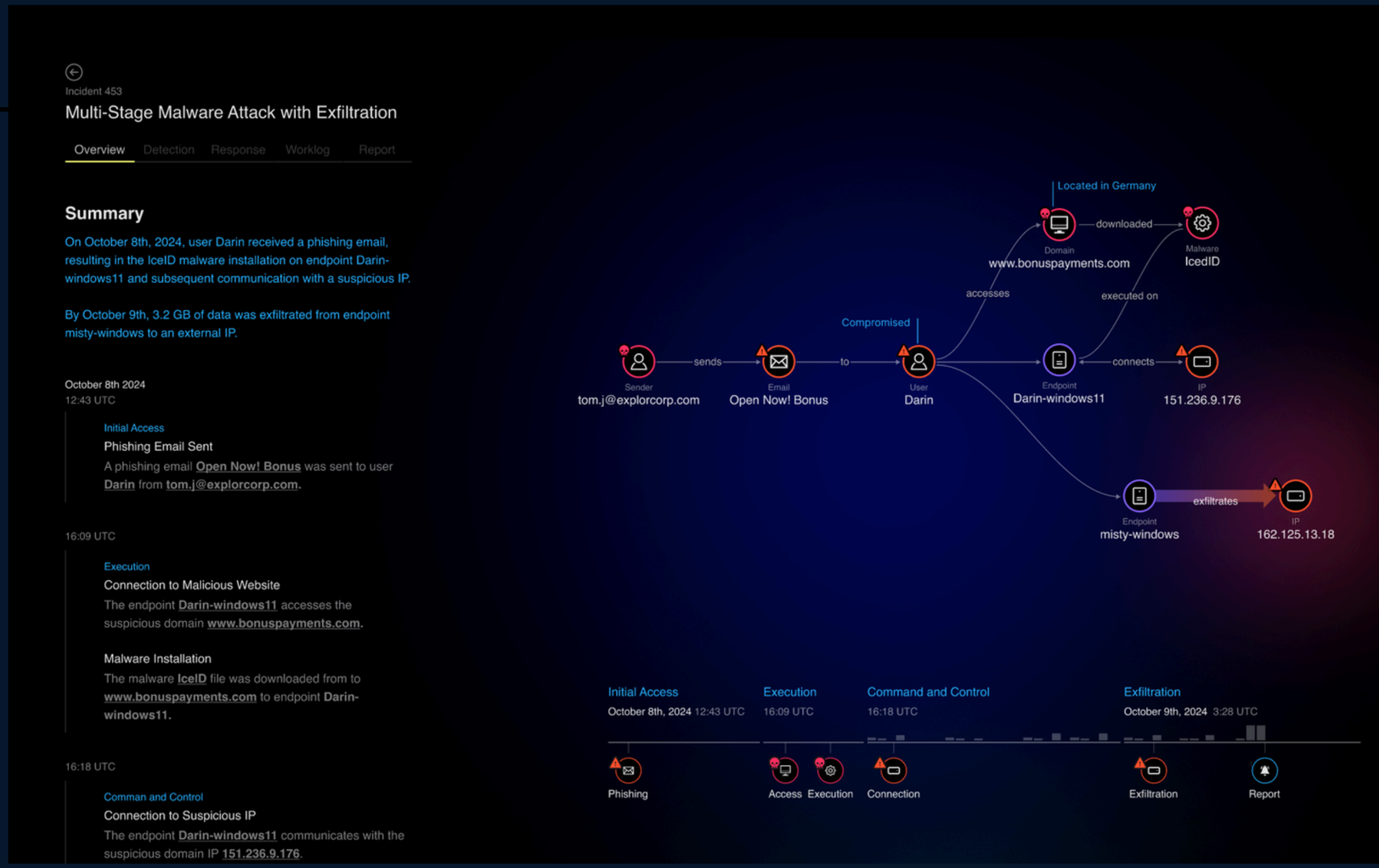
2. DETECTION CONTENT

Cisco XDR

- **Turn-Key** Solution
- **Network** at the core
- **Open** Architecture
- XDR is **Speed & Simplicity** –

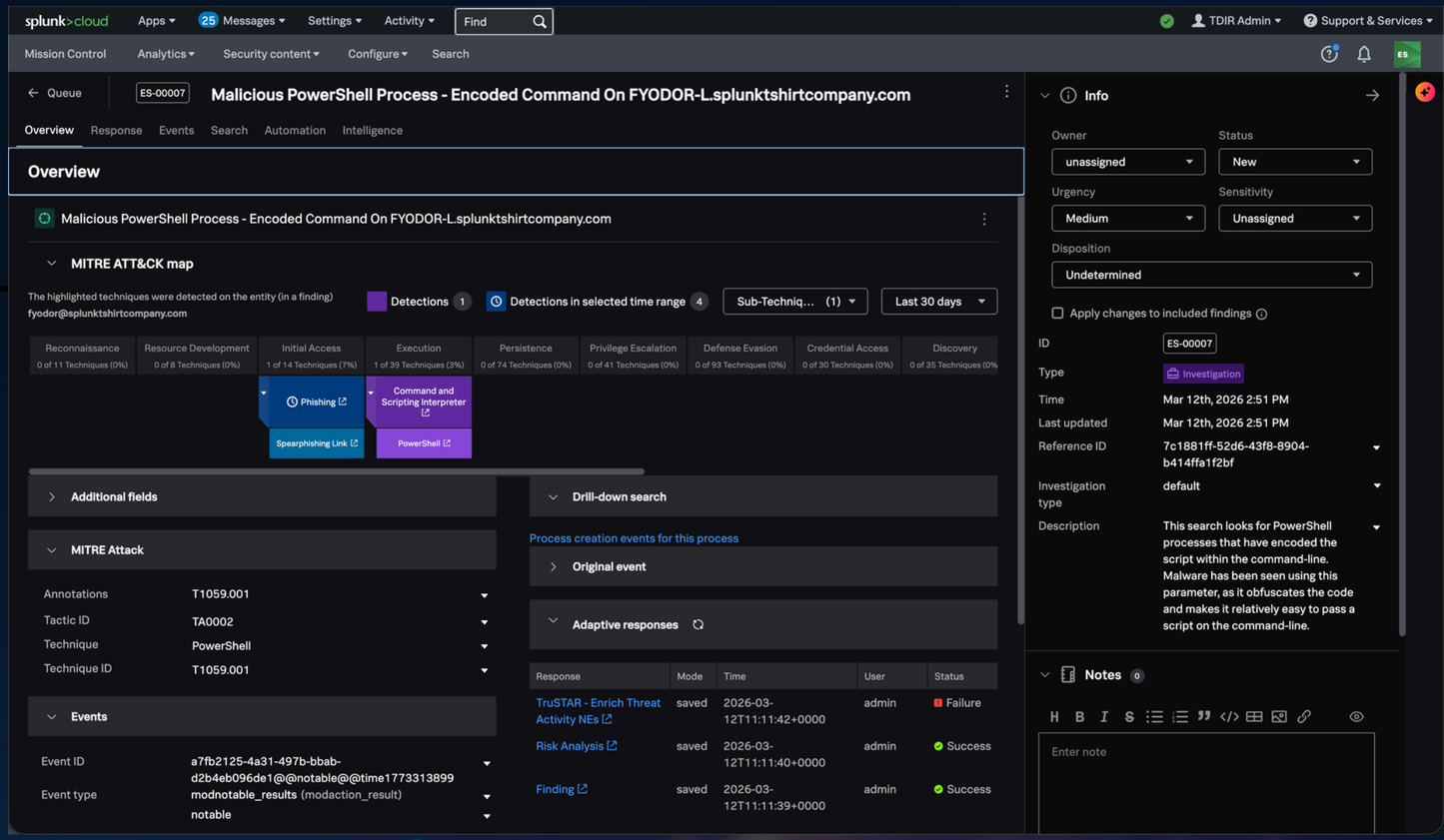
  It hands over to Splunk ES for

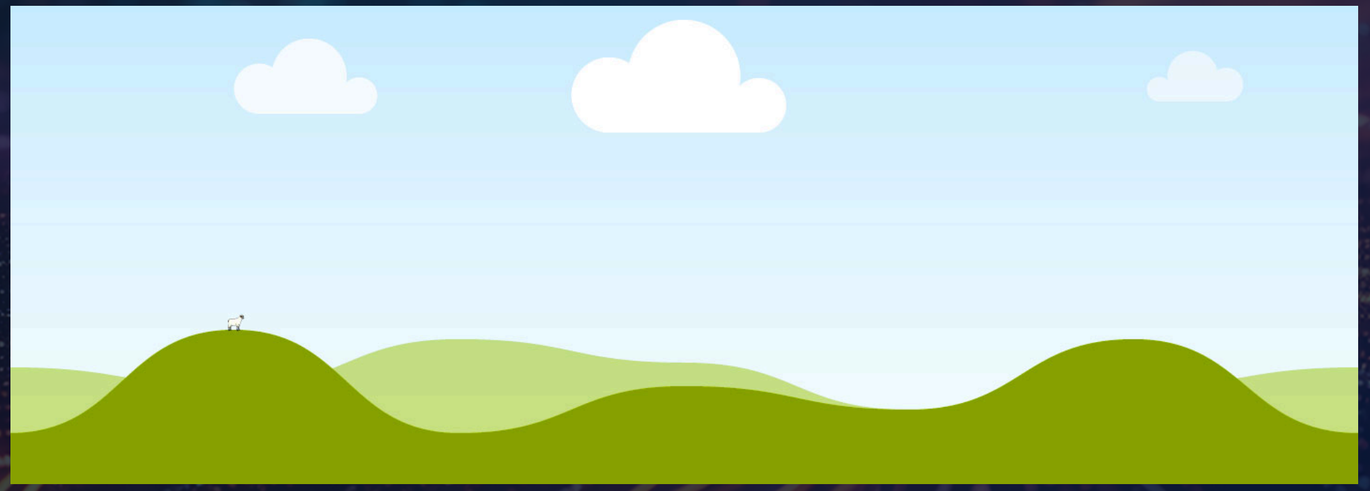
  Scale & Sophistication



Enterprise Security (ES)

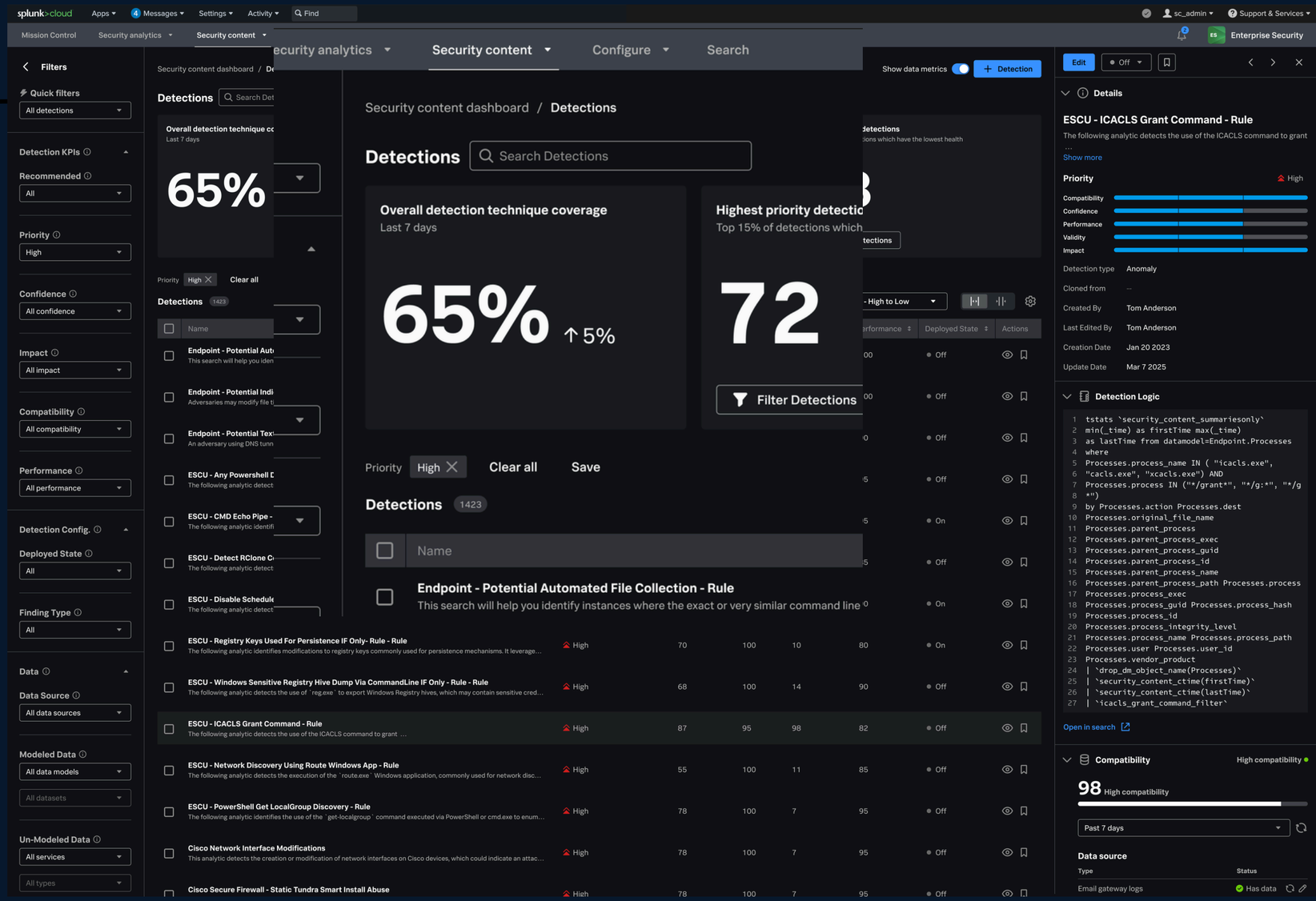
- **Best in Class Analyst Experience** and tooling with unified **TDIR**
- **Integrated** SIEM, UEBA, TIM, SOAR
- **AI Assistant** and **Agents** across every layer





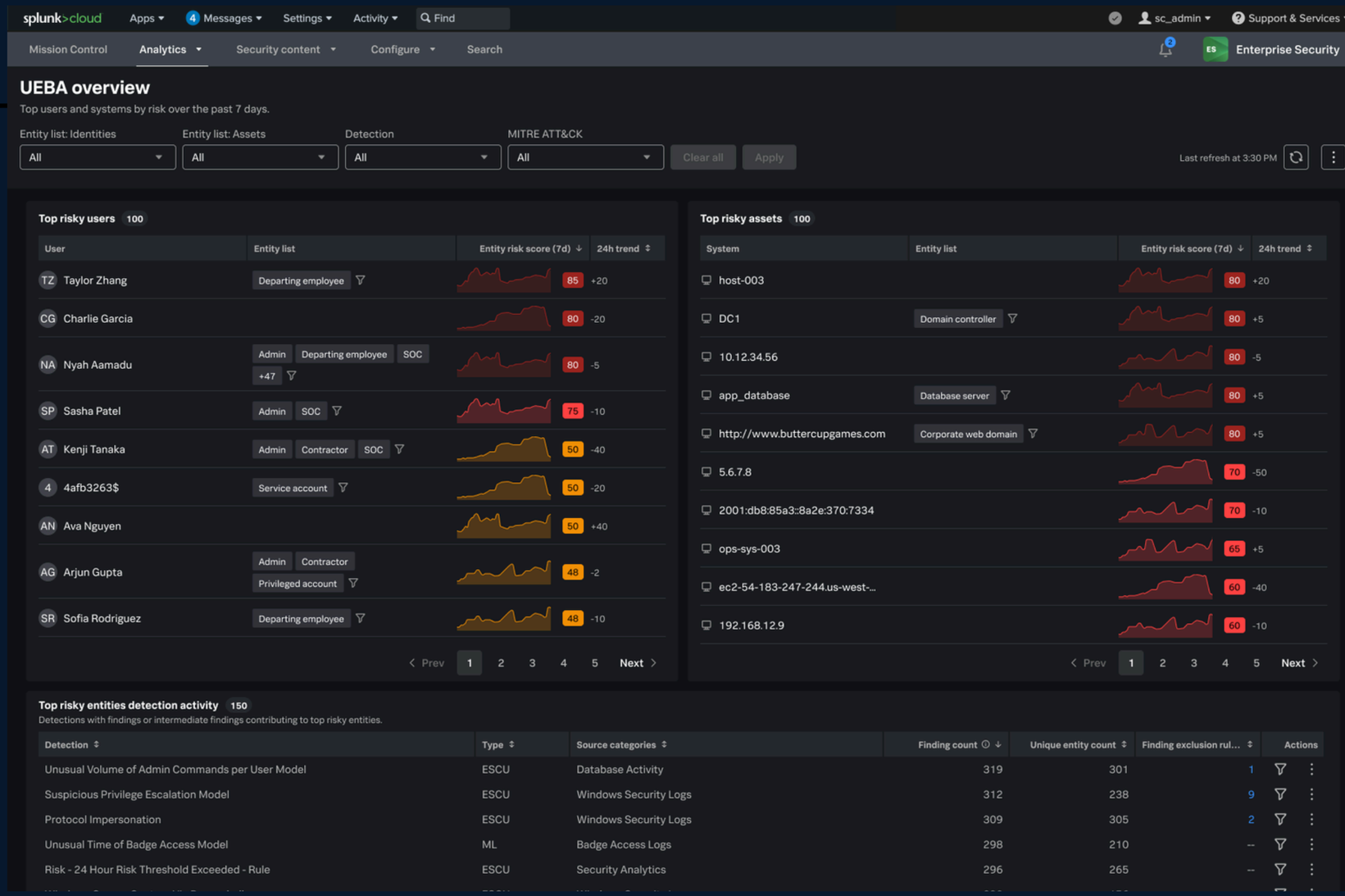
ES - Detection Studio

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



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

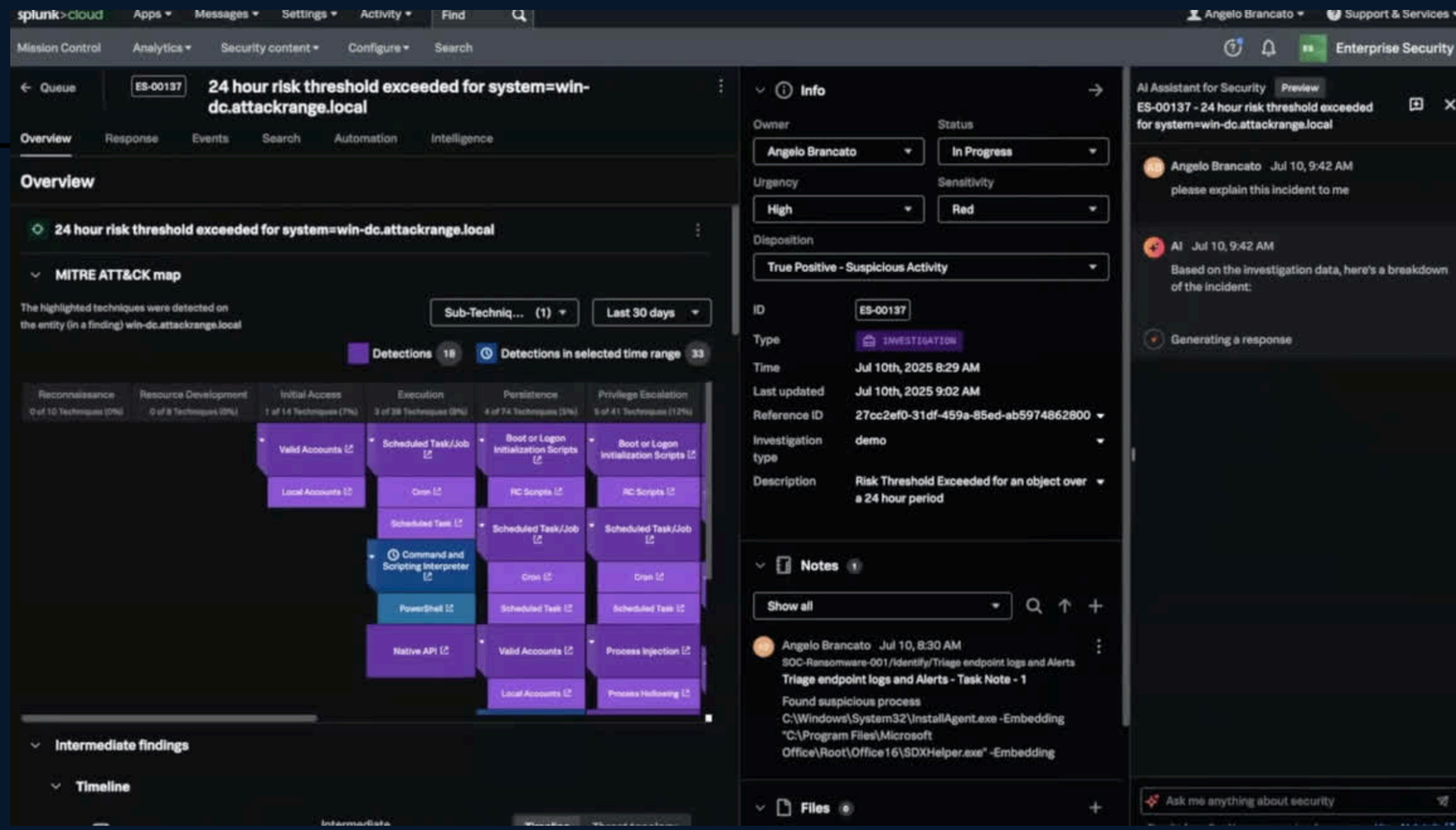
- **Continuously** discover **assets, identities** and **services** across on-prem, cloud and hybrid environments
- **Enriches** detections and investigations with **context** allowing prioritization based on actual risk
- Real-Time Risk Reports

Inventory for the Next Level SOC

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

ES - AI Assistant

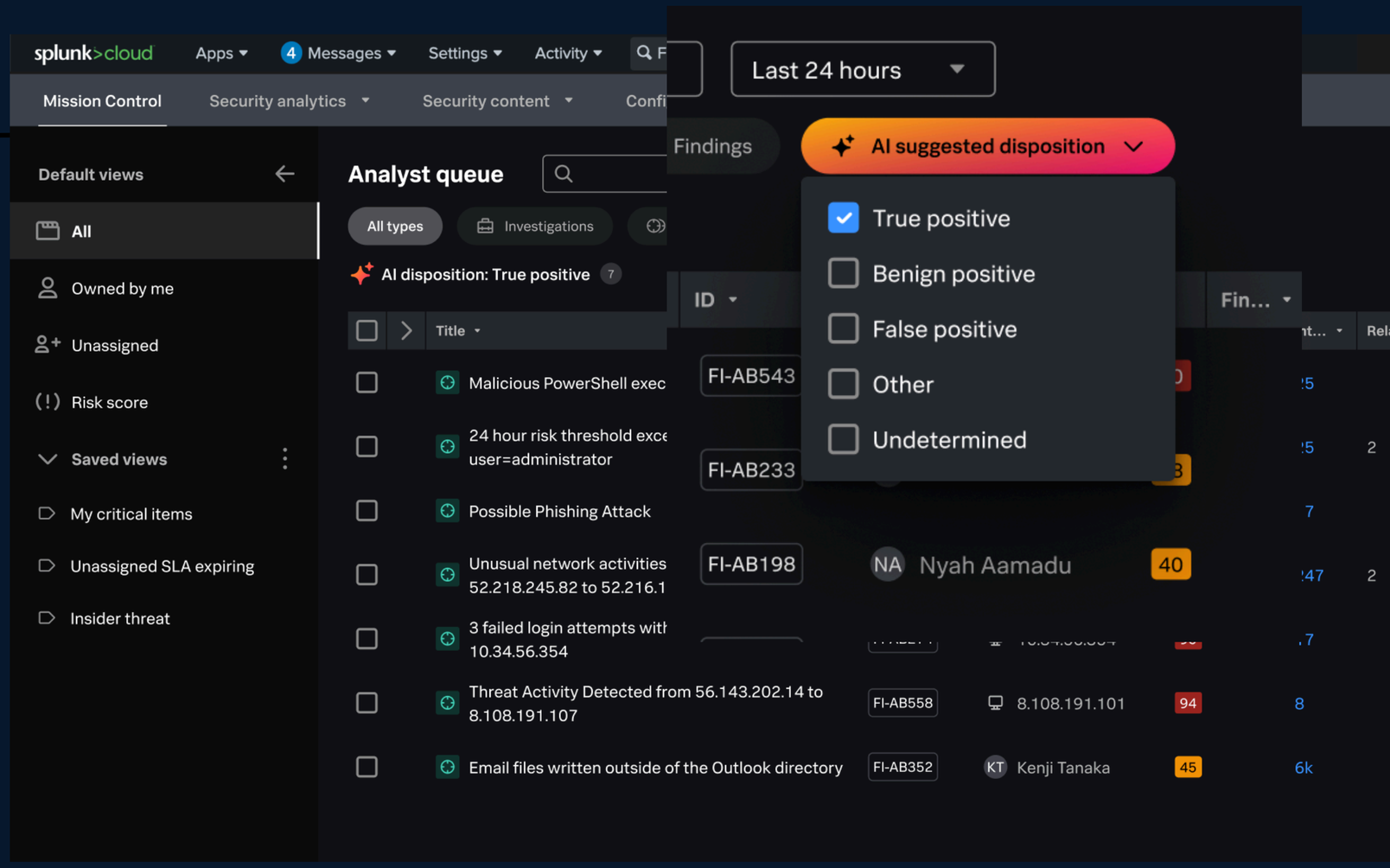
- Explain Findings & Investigations
- Suggest next steps
- Generate SPL
- Generate Investigation Report



ES - Triage Agent

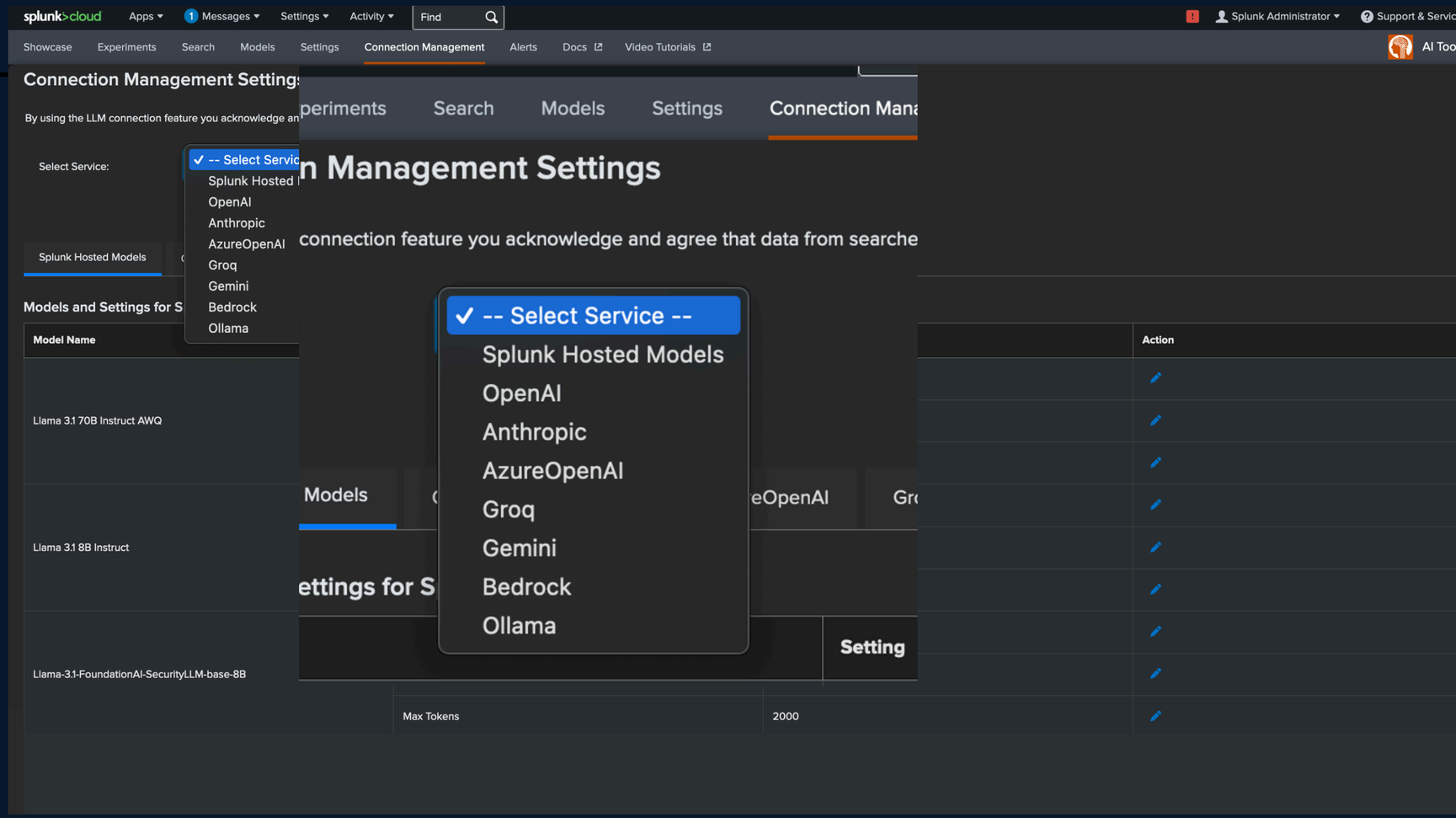
Coming Soon

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



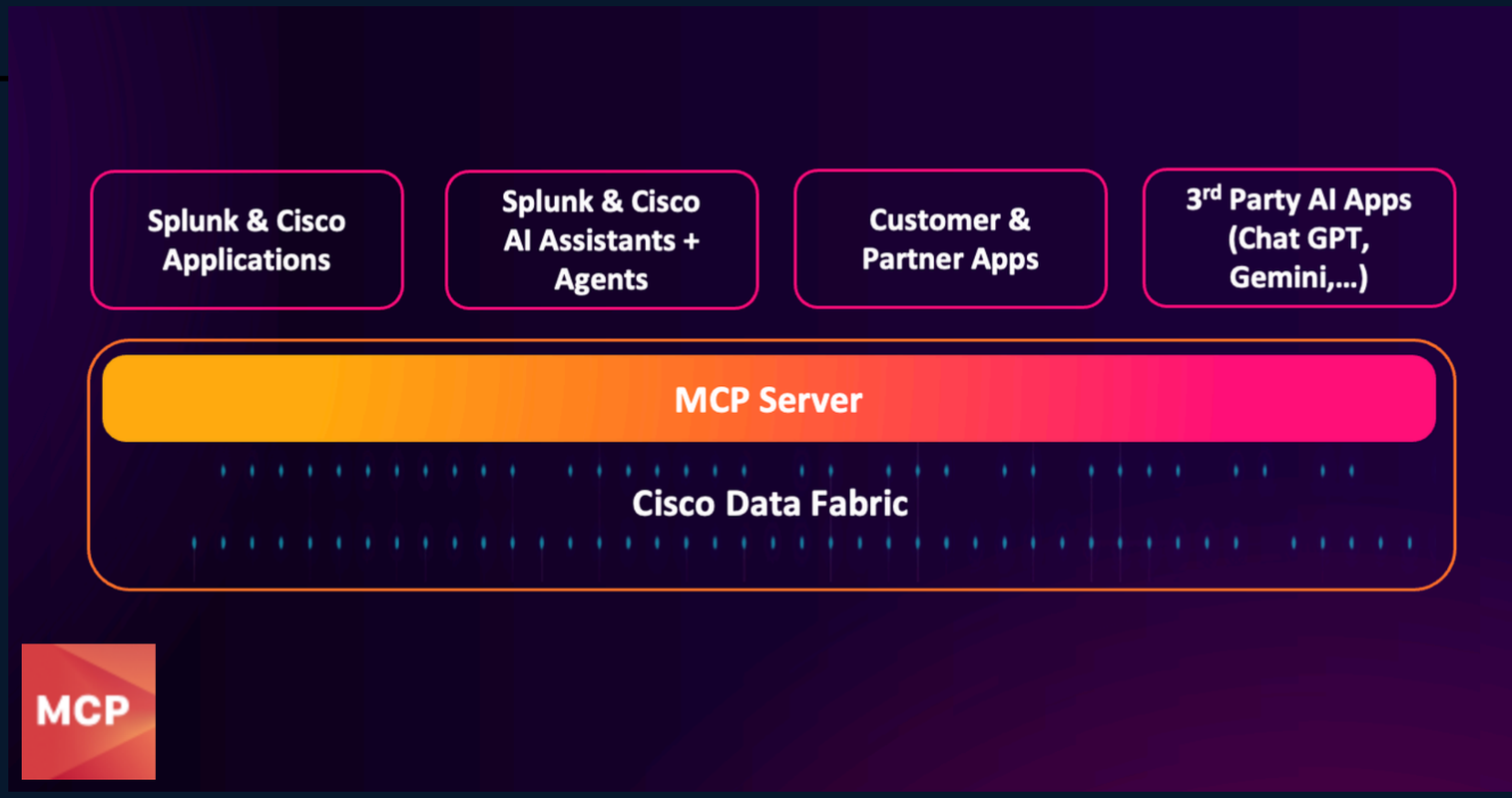
Core - AI Toolkit with LLM Integrations

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



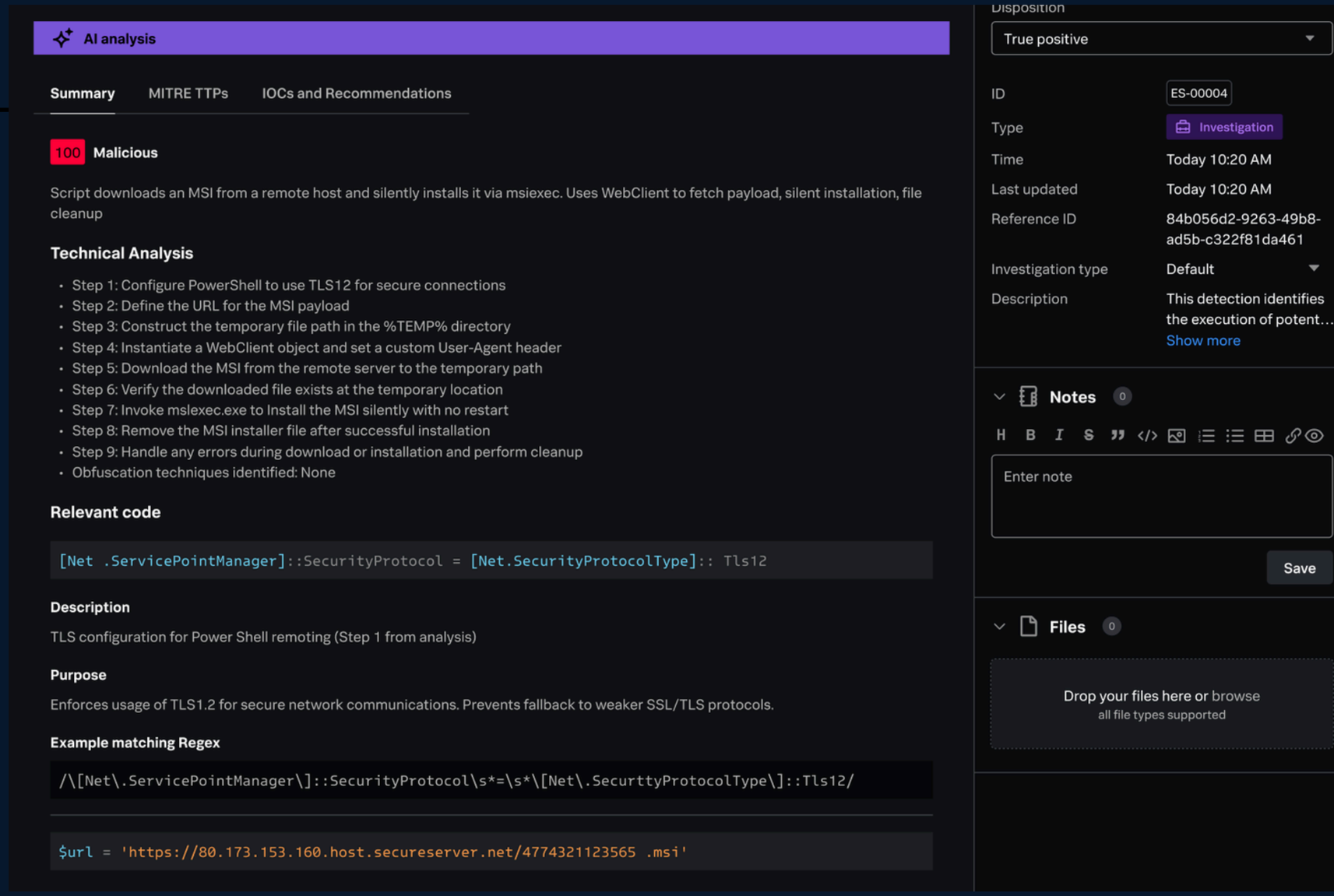
Core – MCP Server

- **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

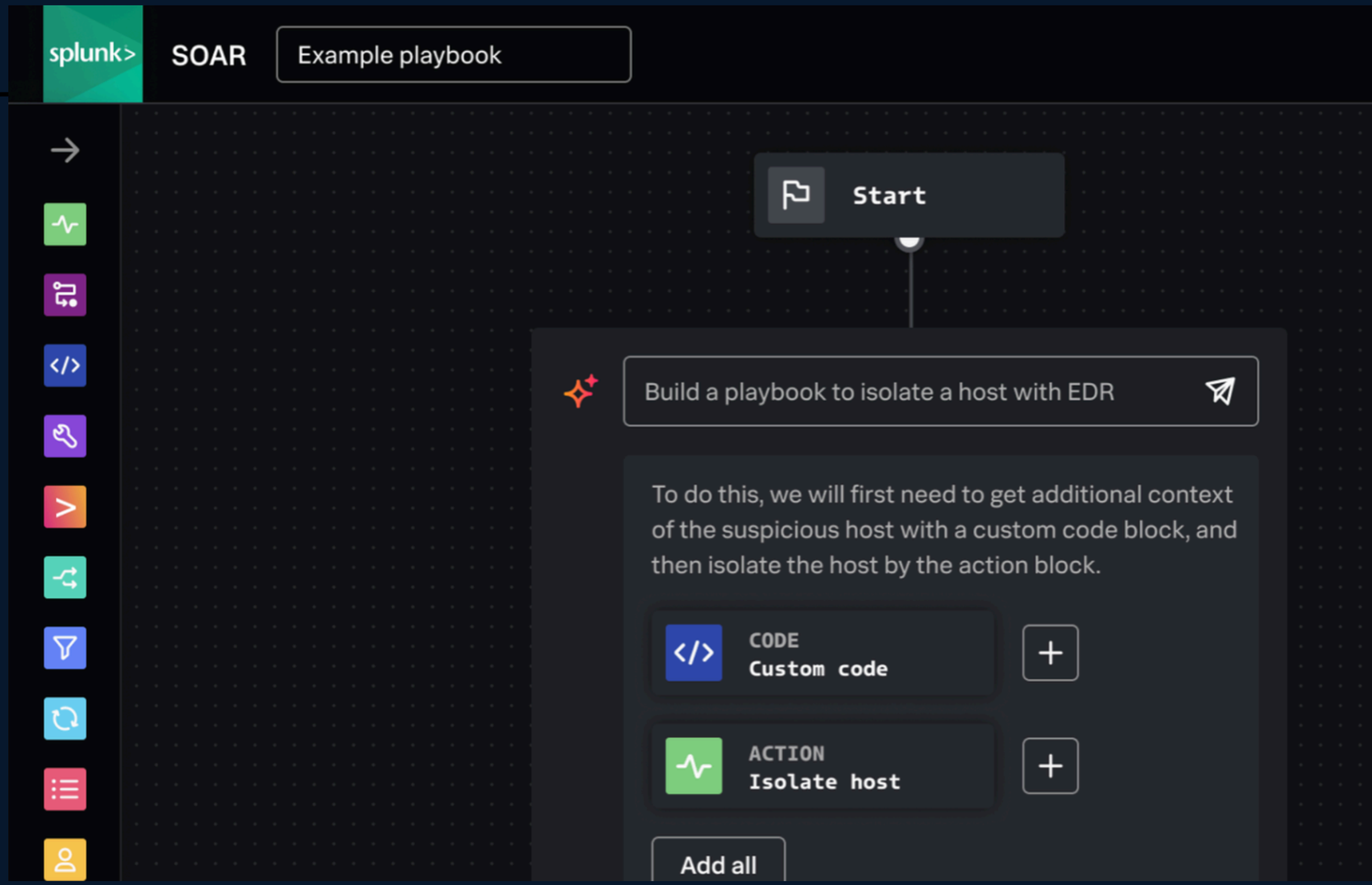
- Explains malicious scripts line-by-line
- Extracts IOCs, flags evasion, and groups recurring behaviors
- Gives analysts actionable insight in seconds, not hours.



SOAR - AI Playbook Authoring

Coming Soon

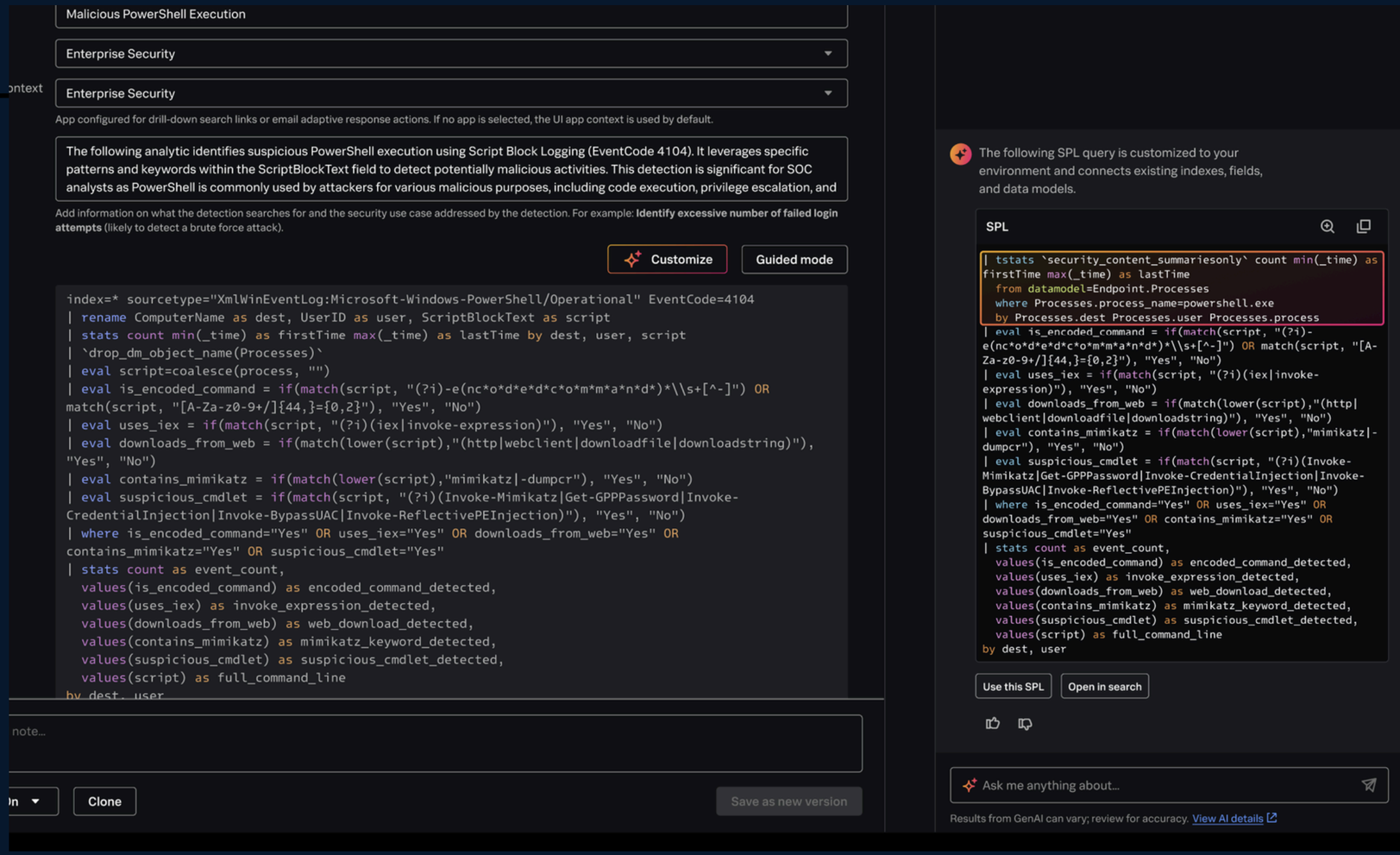
- **Accelerate time to automation**
- **Translate** natural language intent into functional building playbooks faster and easier
- Empowers security teams to automate **without dedicated developers**



ES - AI Assistant for Detection Authoring

Coming Soon

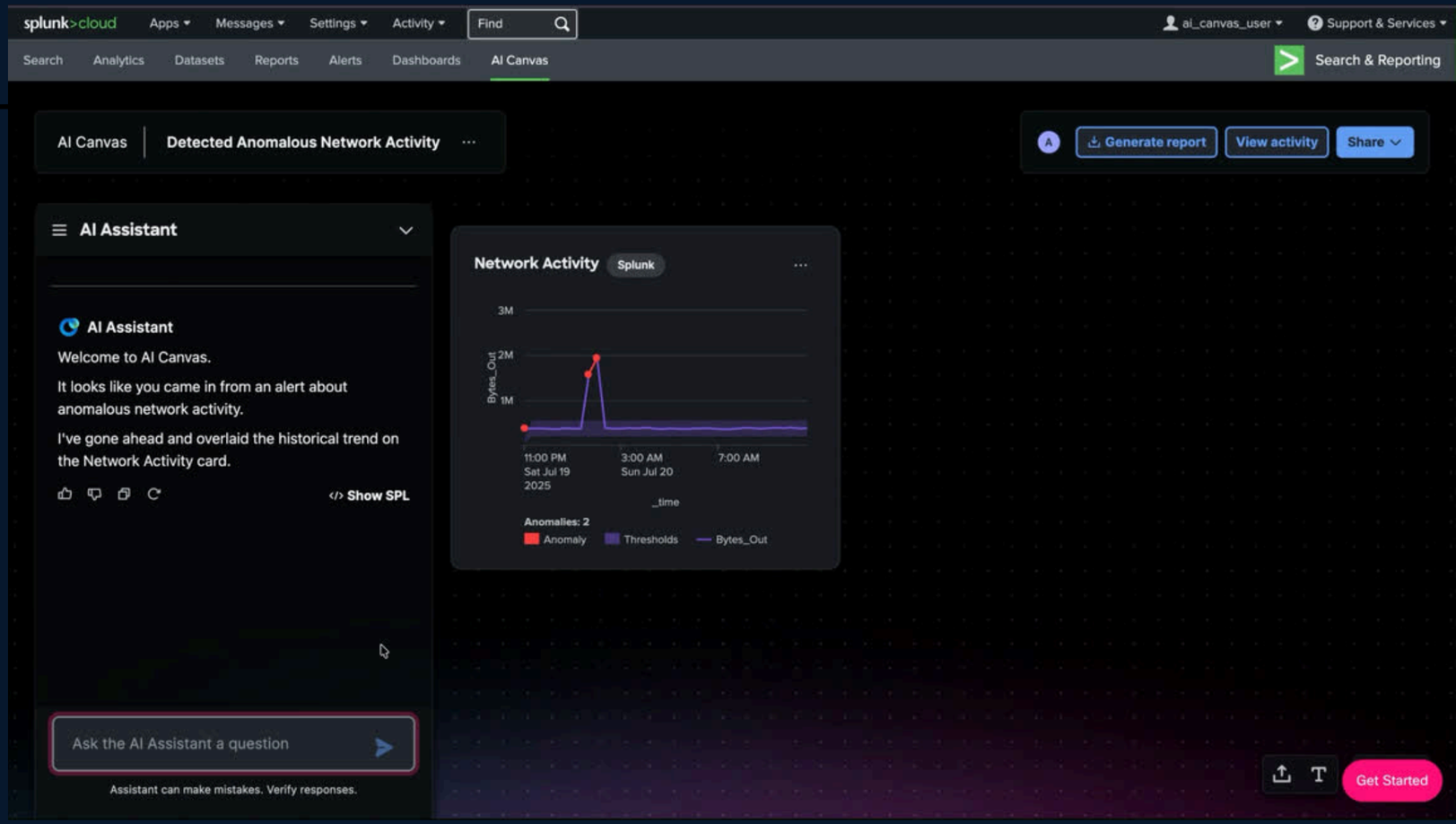
- **Generate SPL** for the detection based on natural language description
- Iterate on detection SPL to **refine detection** to be usable in your environment
- Get **detailed descriptions** and **explanations**



Core – AI Canvas

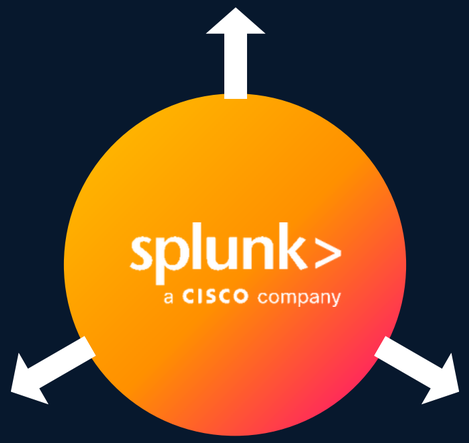
Coming Soon

- **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.



AI Assistants, LLMs & Agents in Splunk

AI Assistants

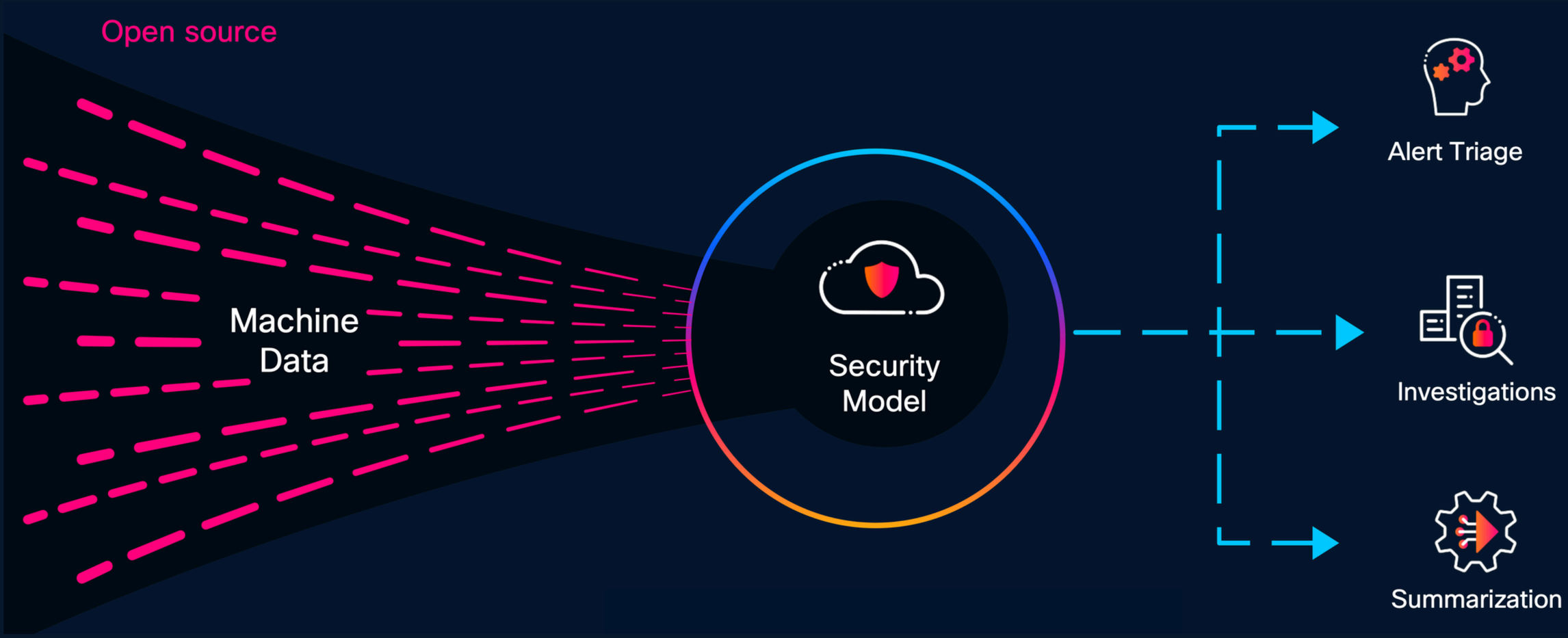


External LLMs

MCP

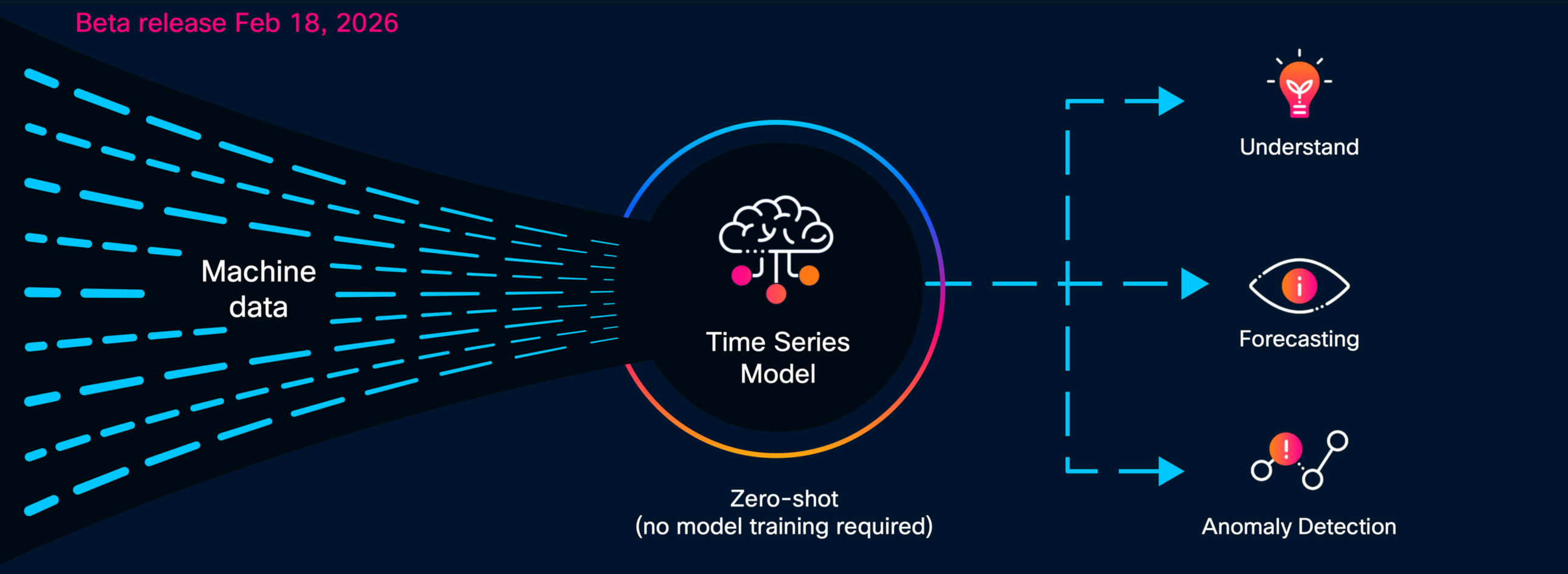
Thank you

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



Cisco Time Series Model

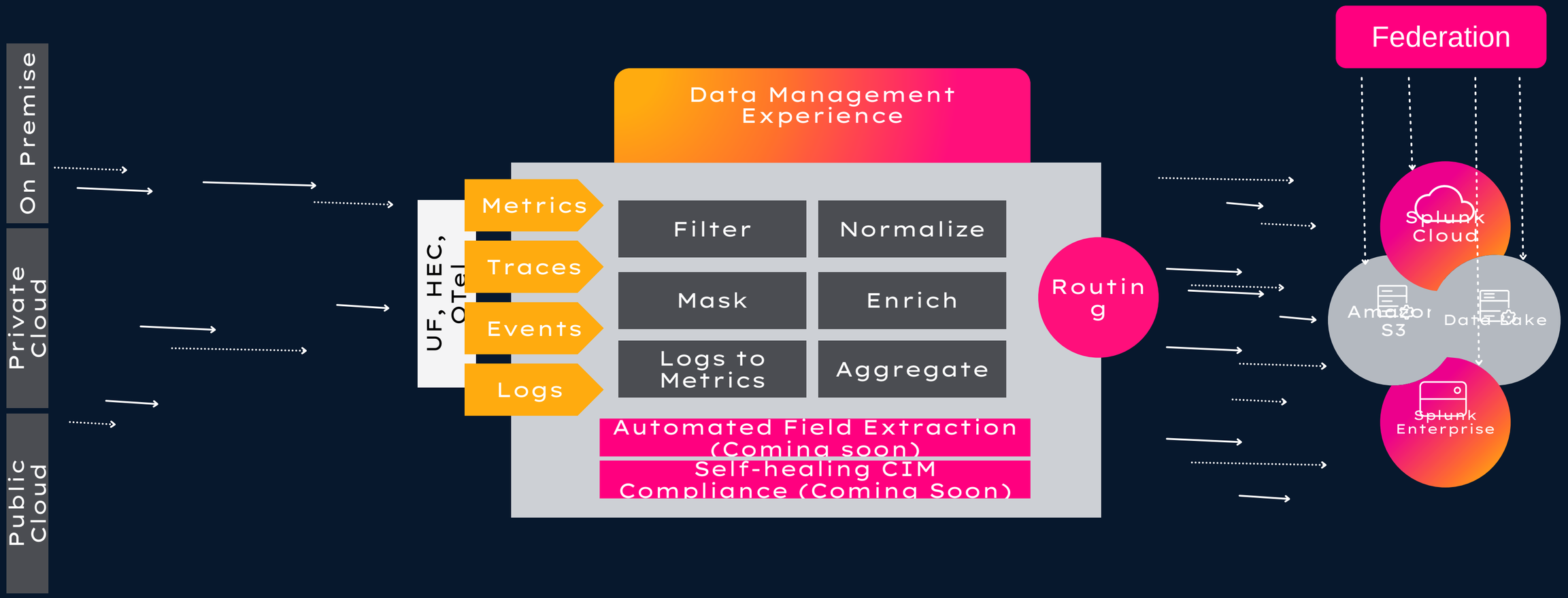
Beta release Feb 18, 2026



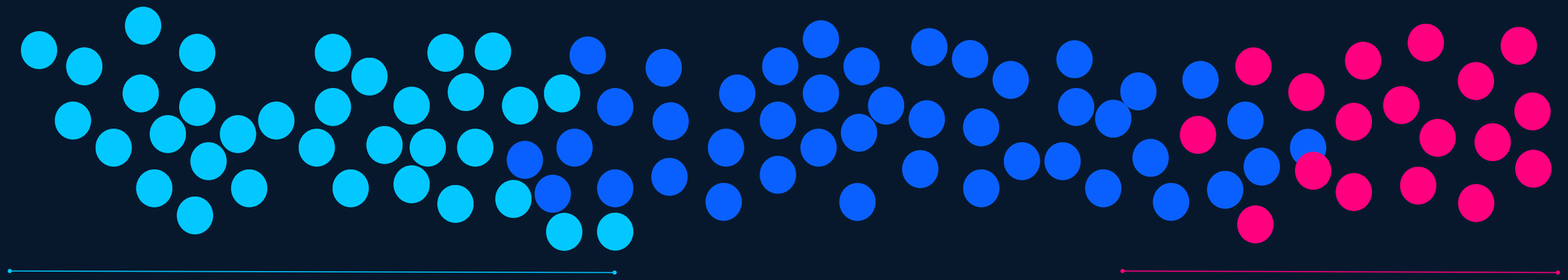
https://huggingface.co/cisco-ai/cisco-time-series-model-1.0

Splunk Data Management Experience (DMX)

Unified data configuration, processing, and management



Because not all Data is the same



Prevention, Detection, Monitoring

Forensics, Audit & Compliance

Incident Review, Investigations,
Threat Hunting

Real and Near-Real Time

Ad Hoc

Archive