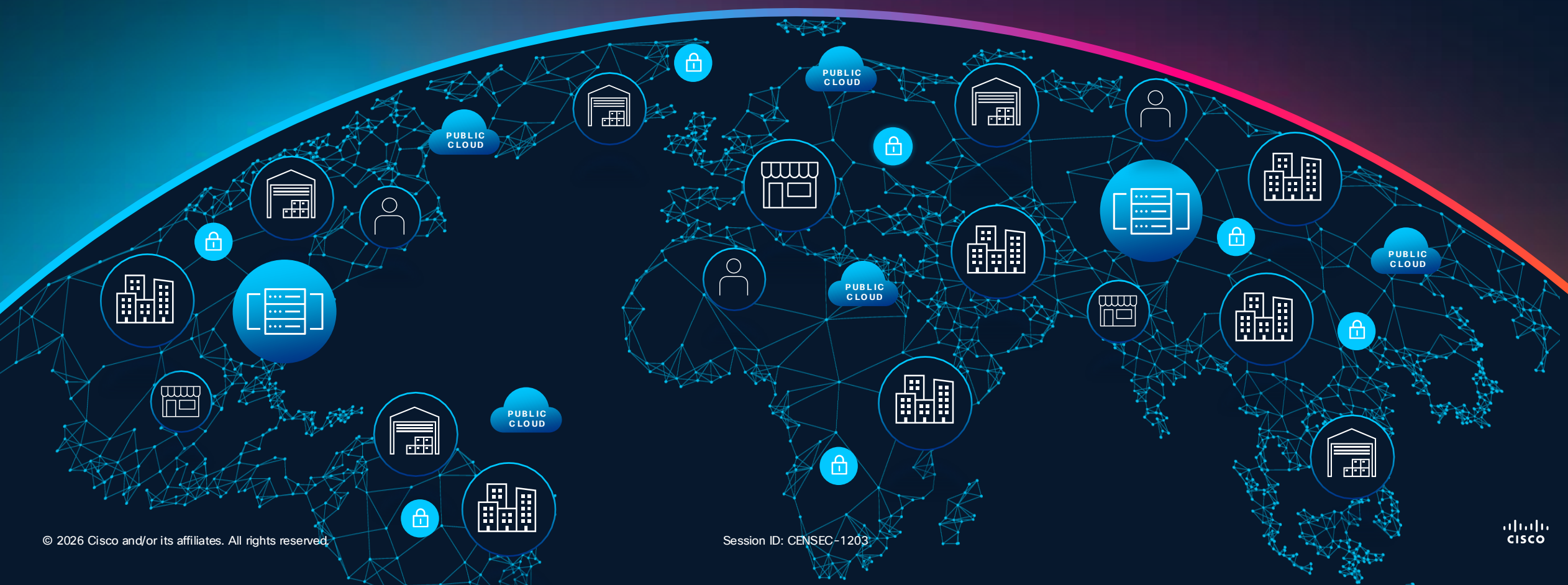
Lessons From the Agentic Frontier

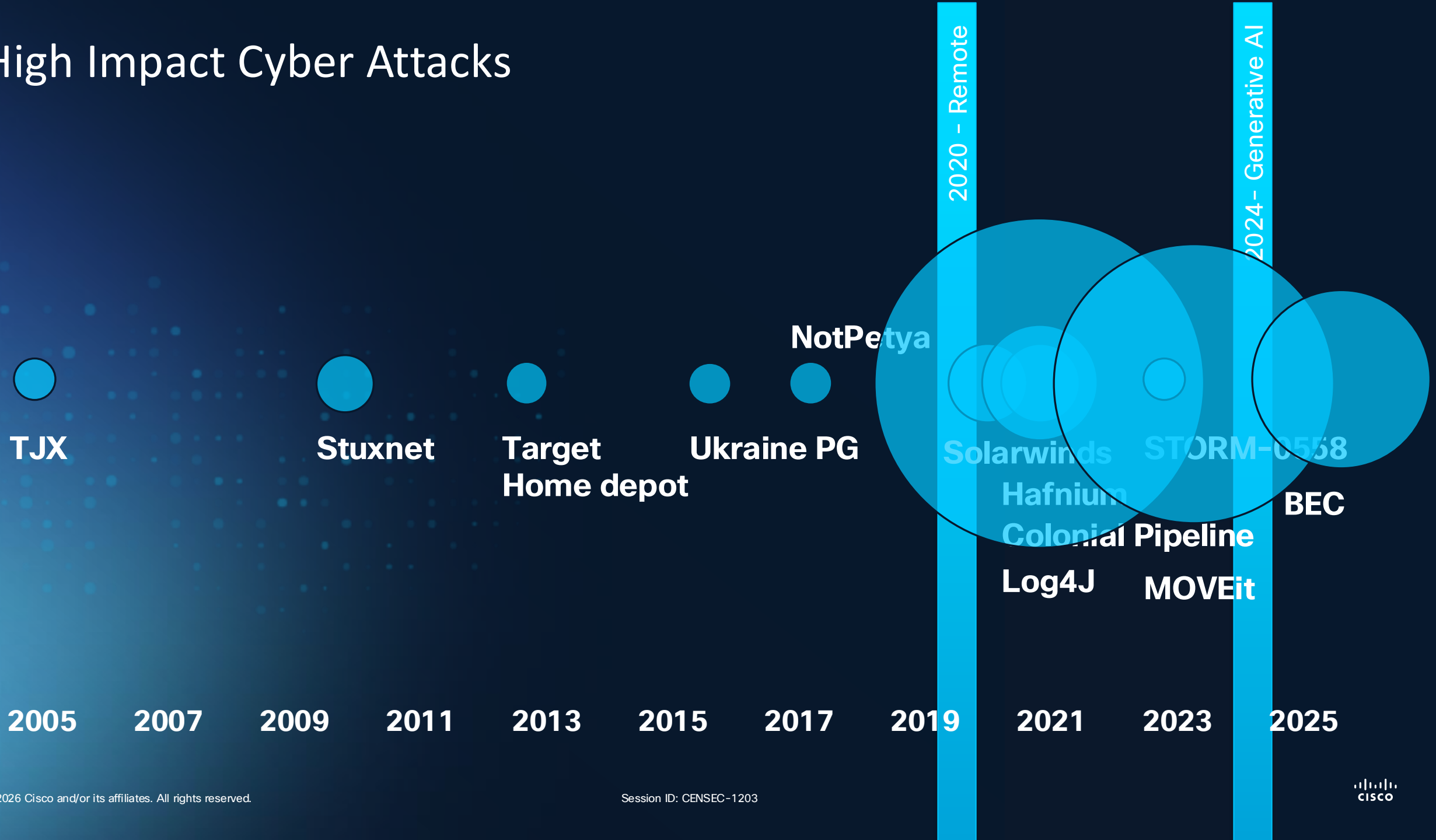
How the SOC is Winning in the AI Era

David Dalling
GVP Splunk Security Strategy

Our world has changed
and so has everything you do

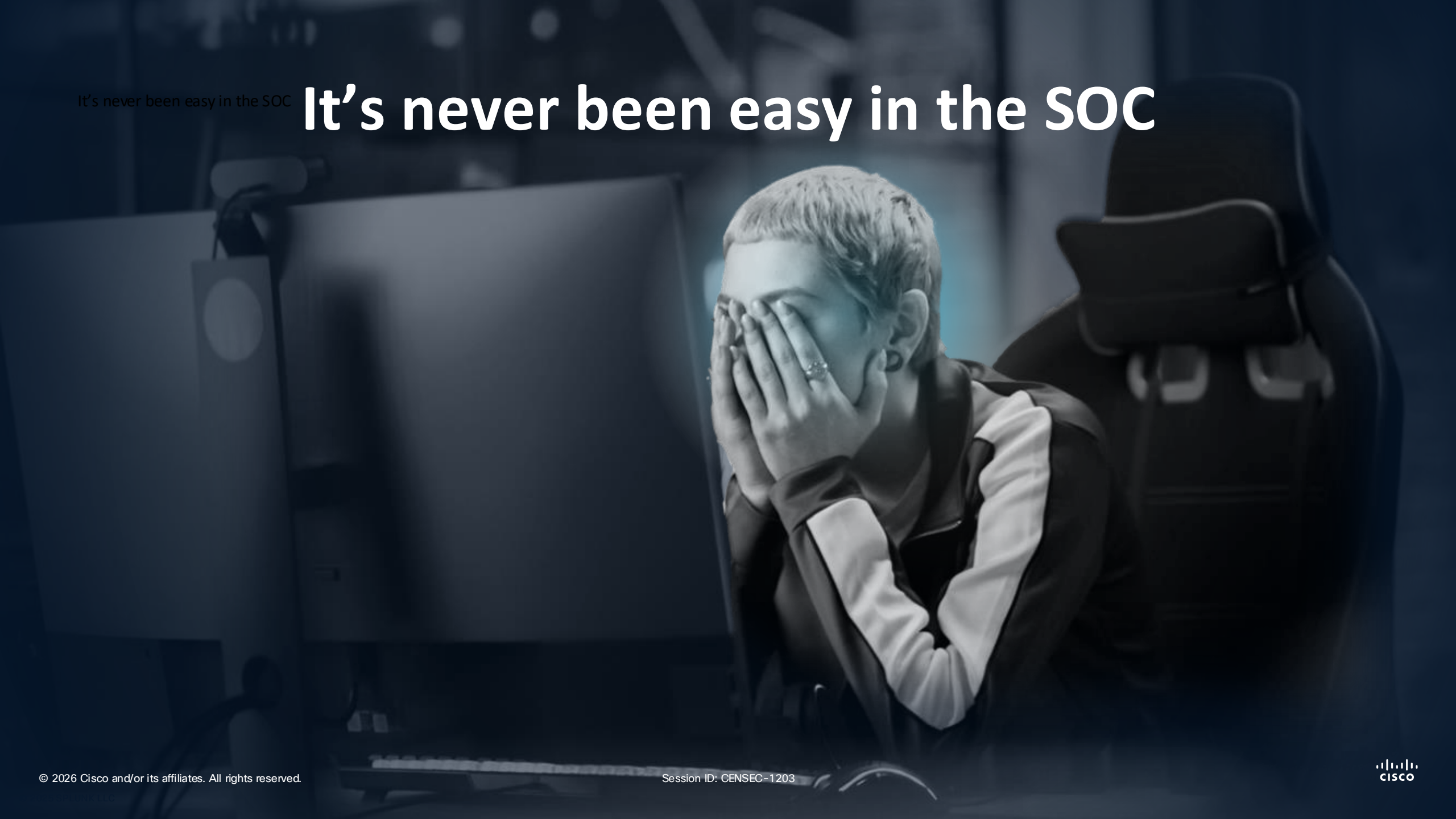


High Impact Cyber Attacks



It’s never been easy in the SOC

It’s never been easy in the SOC



Security for the Agentic Frontier

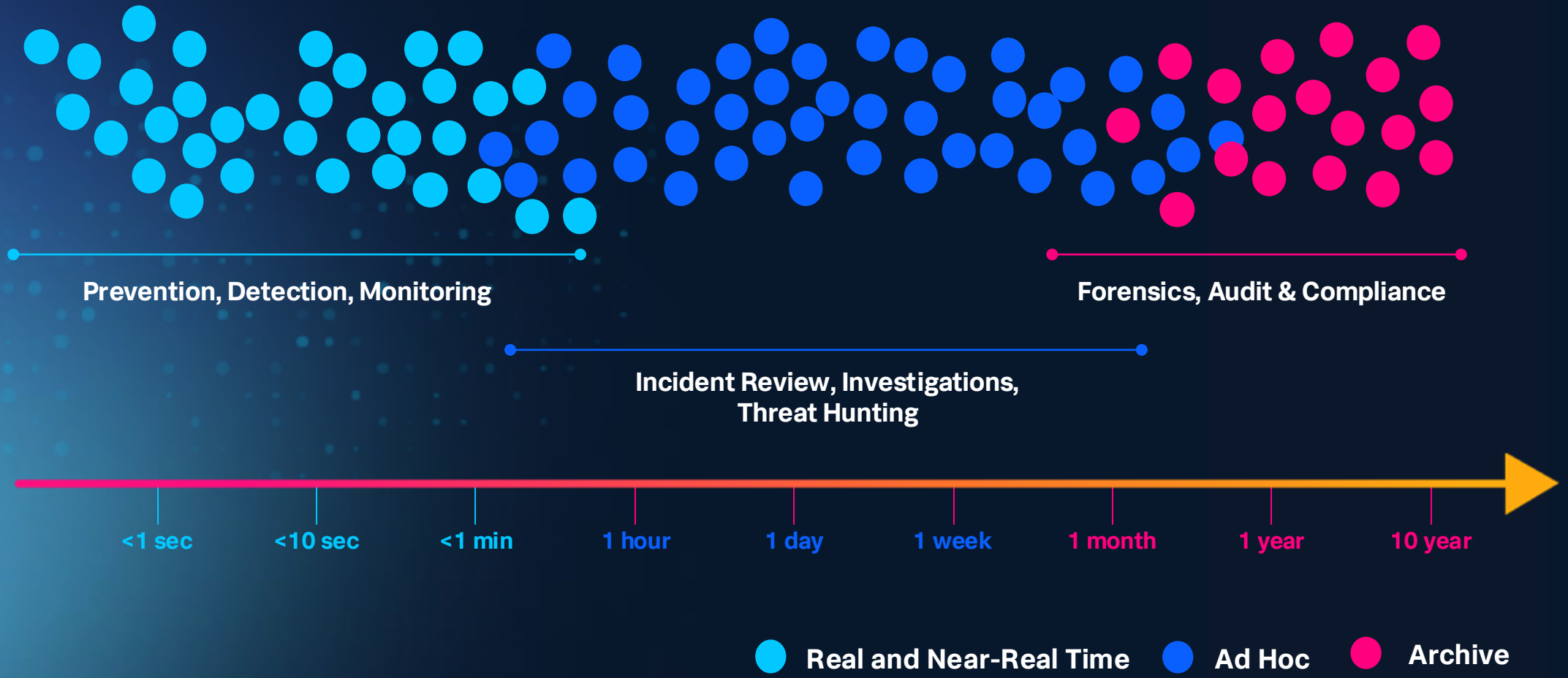
The AI transformation is here,
we must transform with it.

Traditional tools were built for yesterday’s battles. It's time to give your security team the advantage and reclaim the upper hand.

The New Security Operating Model

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

Manage your data to deliver a stronger security posture



Workloads

- Security
- Observability
- Network Ops
- Custom Applications

Cisco Data Fabric

- AI-powered data management
- Federated Search and Analytics
- AI-Native Experiences and Platform for AI

Sources

- Infrastructure
- Applications
- Security
- Users & Devices

Workloads

Security | Observability | Network Ops | Custom Applications

Cisco Data Fabric

AI-powered data management

Federated Search and Analytics

AI-Native Experiences and Platform for AI

Machine Data Lake

Sources

Infrastructure | Applications | Security | Users & Devices

We must unlock the value of data to fuel AI

Correlated detections

Agentic acceleration

Decisive actions

CISCO's Operating System for the Agentic SOC

Stop chasing incidents. Start shaping outcomes.

Surge Ahead of Attackers with AI and Automation

- AI Assisted Experiences (Human –Machine)
- Built-in Integrations & Automation (MCPs, APIs)
- Agentic Orchestration (Machine-Human)

Simplify the Analyst Experience

- Unified Work Surface
- SOAR+UEBA
- TI Enrichment
- AI-Driven Detection and Response
- Integrated Case Management

Scale Security Operations with the Cisco Data Fabric

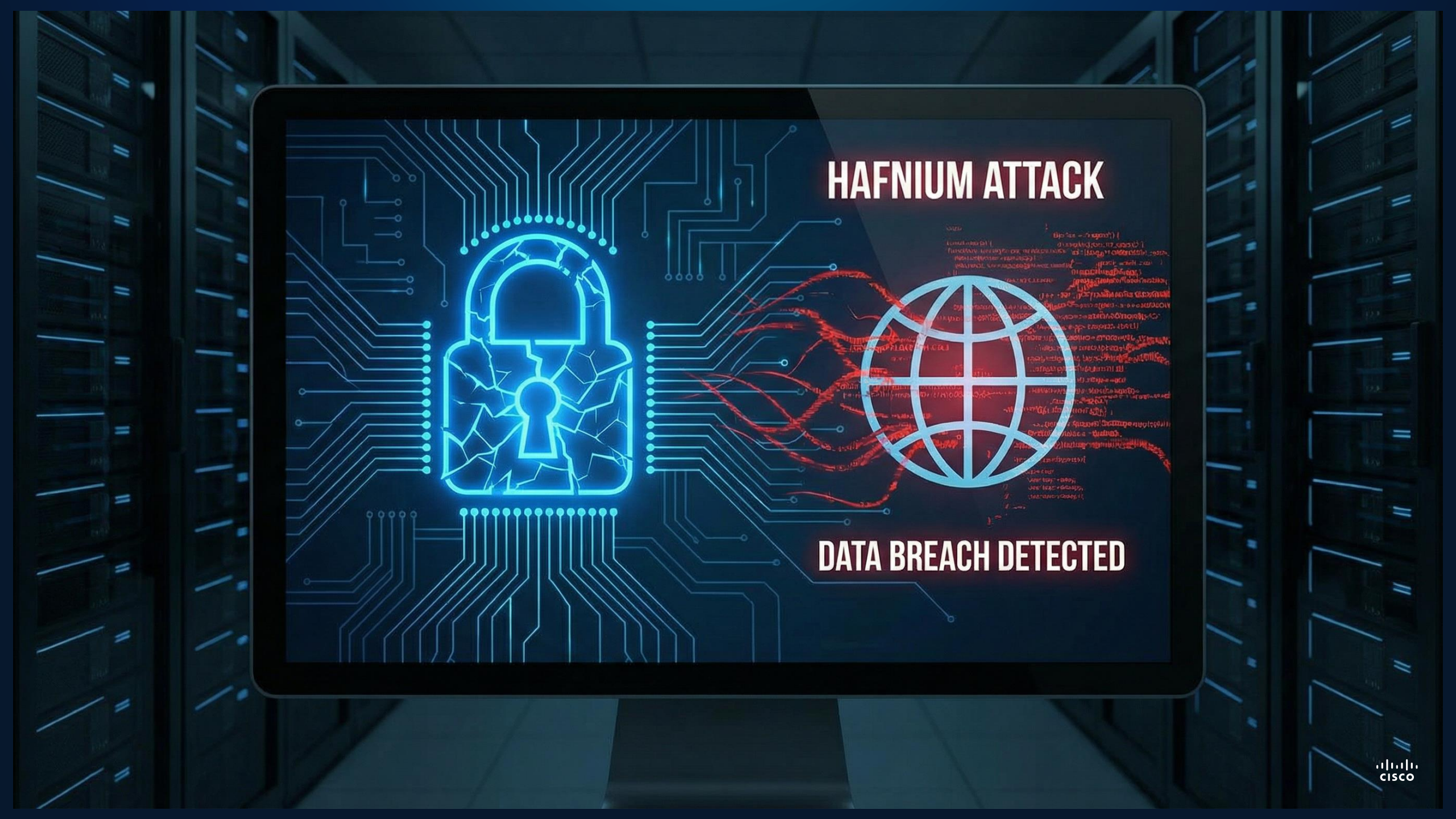
- Cost Controls
- Out-of-the-Box Content
- Detection Studio and Playbook Authoring

AI-powered Data Management

Federated Search and Analytics

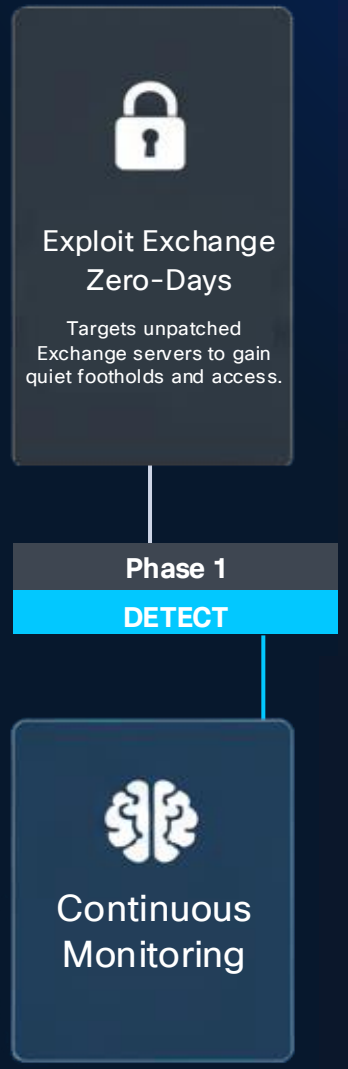
AI-Native Experiences and Platform

Machine Data Lake


HAFNIUM ATTACK
DATA BREACH DETECTED

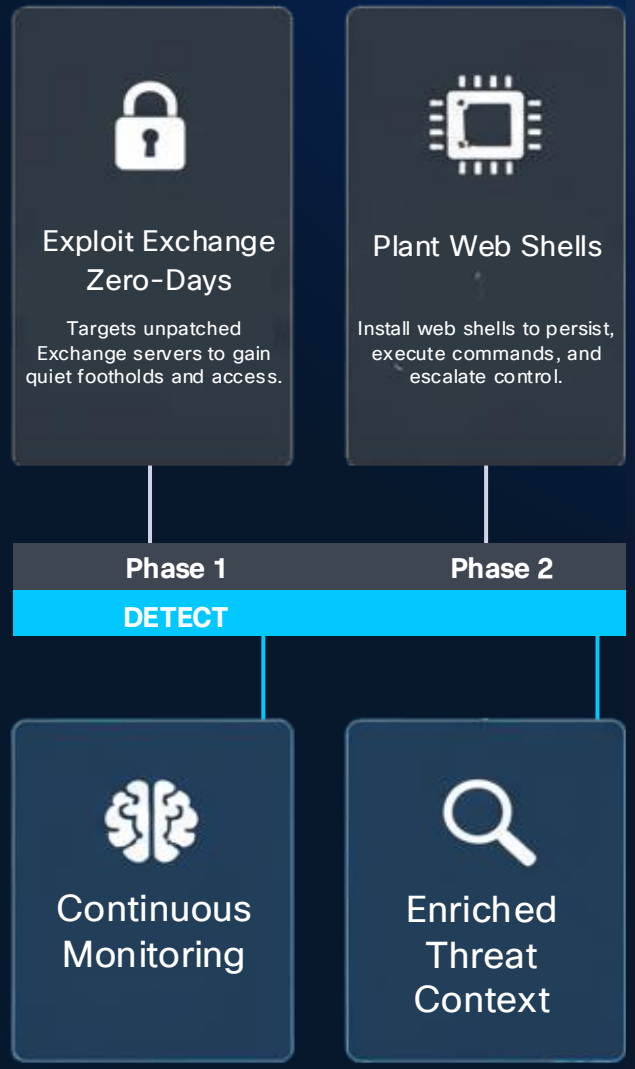
The Agentic SOC* vs. HAFNIUM

The Result: An Agentic SOC* outpaces HAFNIUM, by unifying data, analytics, tooling and AI for the analyst



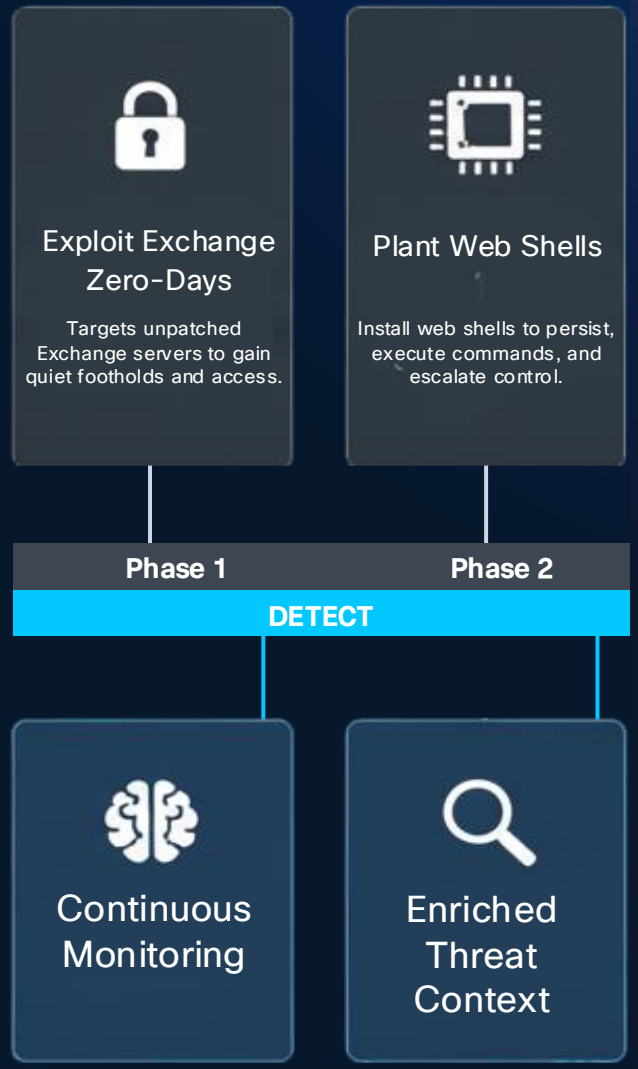
The Agentic SOC* vs. HAFNIUM

The Result: An Agentic SOC* outpaces HAFNIUM, by unifying data, analytics, tooling and AI for the analyst



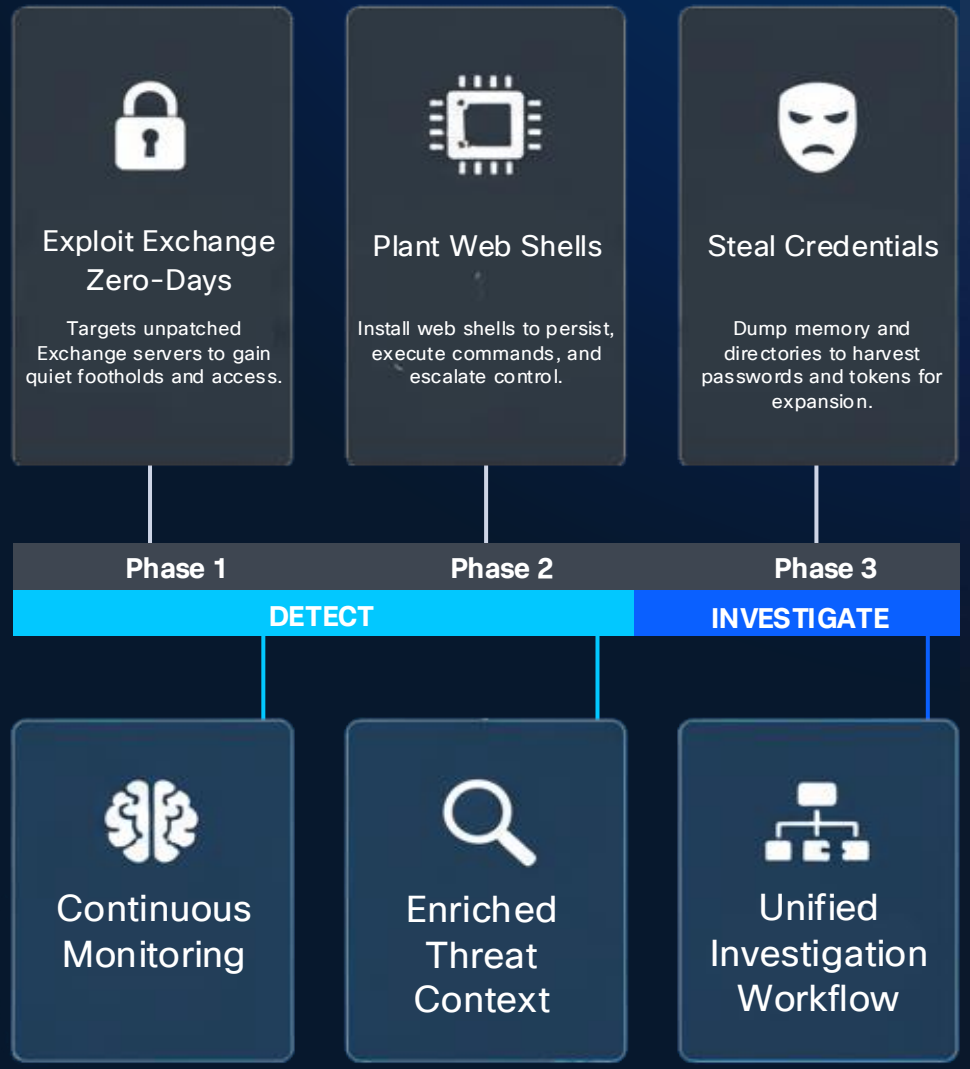
The Agentic SOC* vs. HAFNIUM

The Result: An Agentic SOC* outpaces HAFNIUM, by unifying data, analytics, tooling and AI for the analyst



The Agentic SOC* vs. HAFNIUM

The Result: An Agentic SOC* outpaces HAFNIUM, by unifying data, analytics, tooling and AI for the analyst



The Agentic SOC* vs. HAFNIUM

The Result: An Agentic SOC* outpaces HAFNIUM, by unifying data, analytics, tooling and AI for the analyst

The Agentic SOC* vs. HAFNIUM

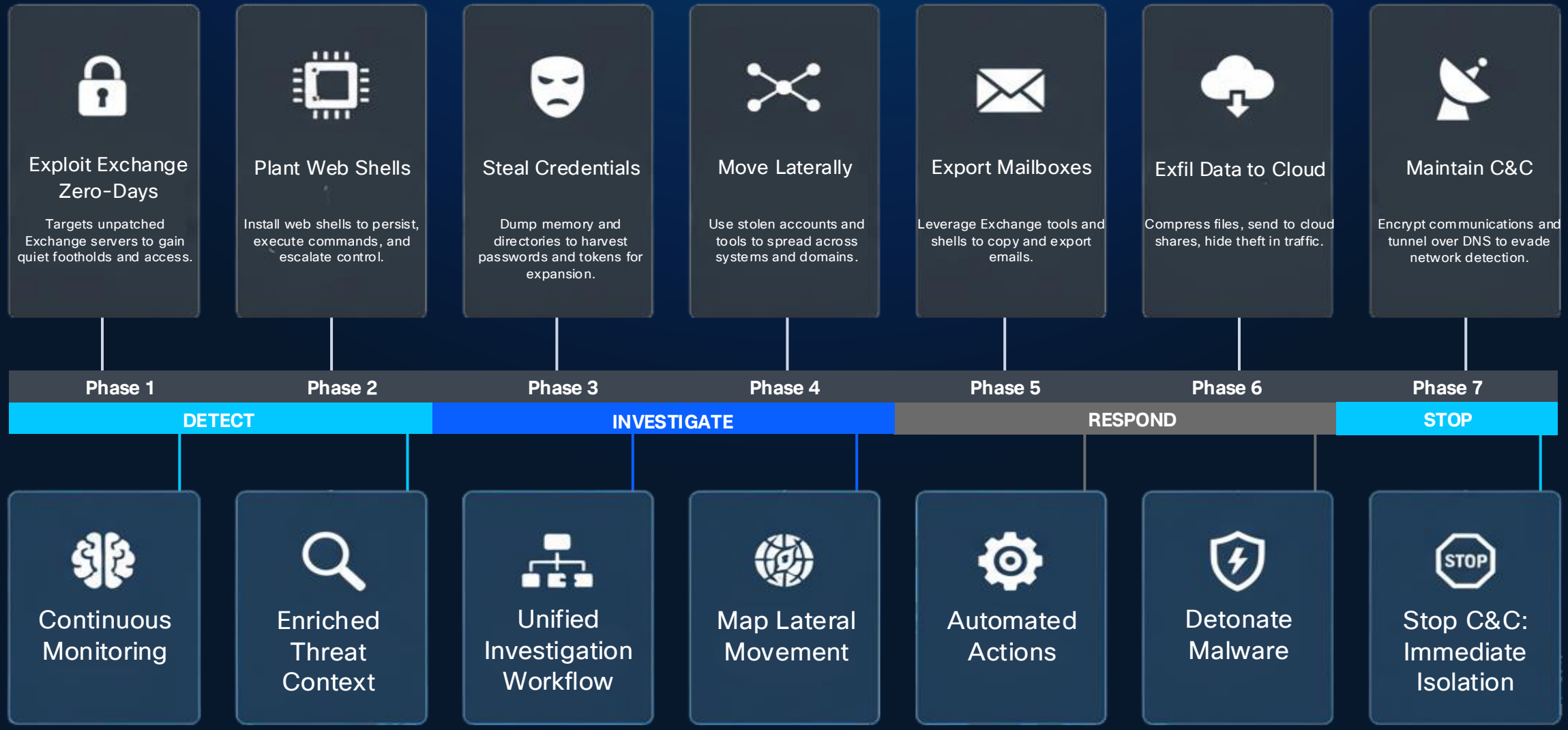
The Result: An Agentic SOC* outpaces HAFNIUM, by unifying data, analytics, tooling and AI for the analyst

The Agentic SOC* vs. HAFNIUM

The Result: An Agentic SOC* outpaces HAFNIUM, by unifying data, analytics, tooling and AI for the analyst

The Agentic SOC* vs. HAFNIUM

The Result: An Agentic SOC* outpaces HAFNIUM, by unifying data, analytics, tooling and AI for the analyst



Announcing Splunk Enterprise Security Premier

Delivering the **most complete** Agentic SOC experience on the market

Scale operations and turn high-volume data into high-fidelity visibility

Streamline detection and response to focus on what matters

Stop threats at machine speed with AI and automation

Stay ahead of attacks at machine speed

SPEED

Unified actions for humans + AI

Embedded guidance

Agentic Orchestration

SOC

X

Specialized Agents for entire security lifecycle

- Detection Builder*
- Malware Reversal
- Triage*
- Playbook Authoring
- Response*

* Slated for H2 Release

SOC Tours

February 9 - 12 **Located at WoS Pavillion, Digital Resilience Welcome Desk**

Title: **Join a Guided Security Operations Center (SOC) Tour at Cisco Live!**

Abstract: Get an exclusive, behind-the-scenes look at how Cisco detects and responds to active threats in real-time conference traffic, in collaboration with the Network Operations Center (NOC). Sign up (or book a private SOC Tour – Sales/CX and Execs).

Experience the SOC of the Future, powered by Cisco Security Cloud and Splunk Enterprise Security, with advanced protection from Firepower Threat Defense, Duo Identity, AI Defense, and Talos Intelligence. Endace continuous packet capture is fully integrated to provide comprehensive visibility and rapid response.

Monday Feb 9	Tuesday Feb 10	Wednesday Feb 11	Thursday Feb 12
3:00 – 4:00 PM	1:00 – 1:30 PM	10:30 – 11:00 AM	10:30 – 11:00 AM
4:00 – 4:30 PM	3:00 – 3:30 PM	1:00 – 1:30 PM	12:00 – 12:30 PM
	5:00 – 5:30 PM	3:00 – 3:30 PM	


CISCO