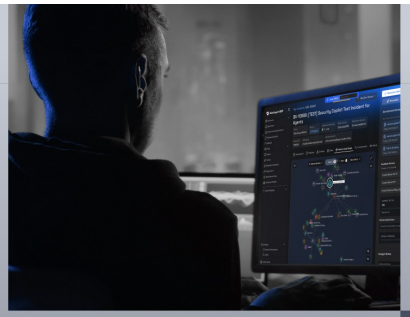
DAFITC 2026

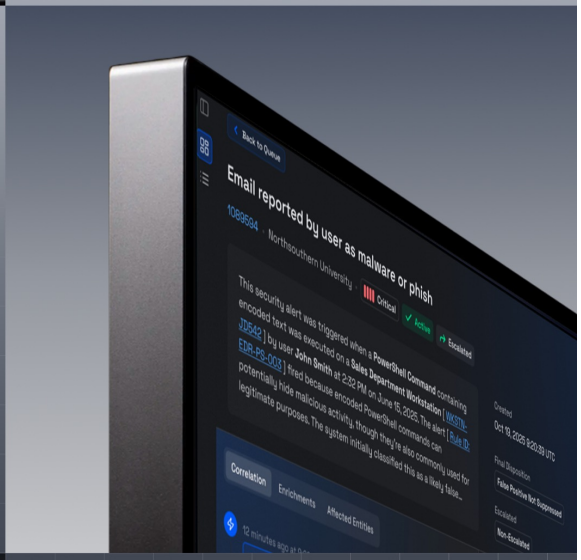
Clean Indicators, Real Mission Risk

AI-Enabled Supply Chain Context for Incident Response

BREAKOUT SESSION

THE FUTURE OF CYBER







Introductions



John Harbaugh

CIO & CISO

BlueVoyant

- **Full-Spectrum Cyber Operator** — 25+ years of public and private sector experience, including Senior Executive Service positions within the U.S. Defense and Intelligence Community
- **USAF Cyber Experience** — Helped stand up the U.S. Air Force's cyber capability and recognized as a Jimmy Doolittle Fellow for Cyber Operations
- **Scaled Advanced Capabilities** — Led major cyber organizations at Deloitte and R9B, supporting government and enterprise clients while driving innovation and growth
- **Building for the Mission Today** – Now CIO & CISO at BlueVoyant, supporting supply chain and cyber defense for USAF/USSF programs

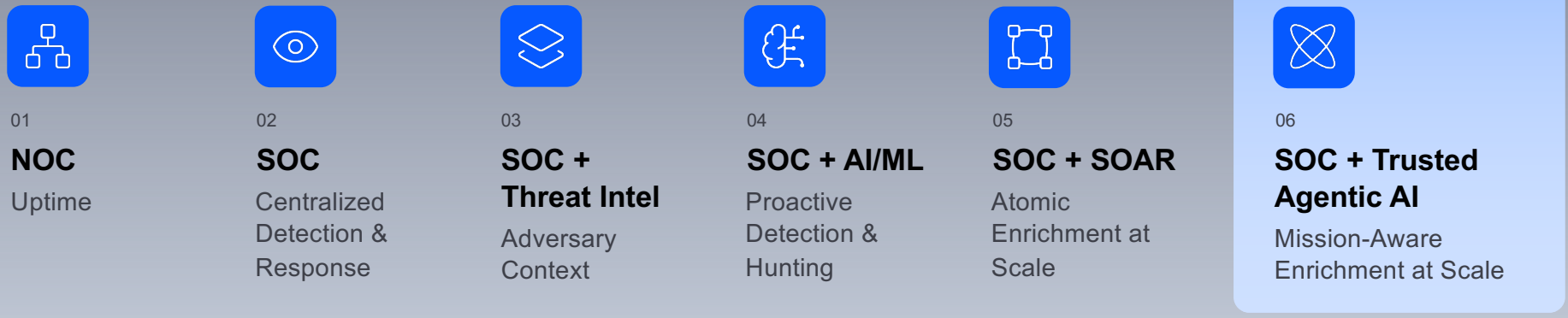
Agenda

1. What AI Changes in the SOC – and What It Does Not
2. The Supply Chain Opportunity
3. sUAS Base Defense Scenario
4. IR Framework for AI-Enabled Supply Chain Context
5. Takeaways + Q&A

THE BIG PICTURE

The SOC Was Built for Mission Defense. AI Can Make It Mission-Aware.

Government missions helped shape each major SecOps evolution — from uptime to detection, intelligence, automation, and response. The next phase is trusted AI that connects cyber activity to mission-aware response.



01
NOC
Uptime

02
SOC
Centralized Detection & Response

03
SOC + Threat Intel
Adversary Context

04
SOC + AI/ML
Proactive Detection & Hunting

05
SOC + SOAR
Atomic Enrichment at Scale

06
SOC + Trusted Agentic AI
Mission-Aware Enrichment at Scale

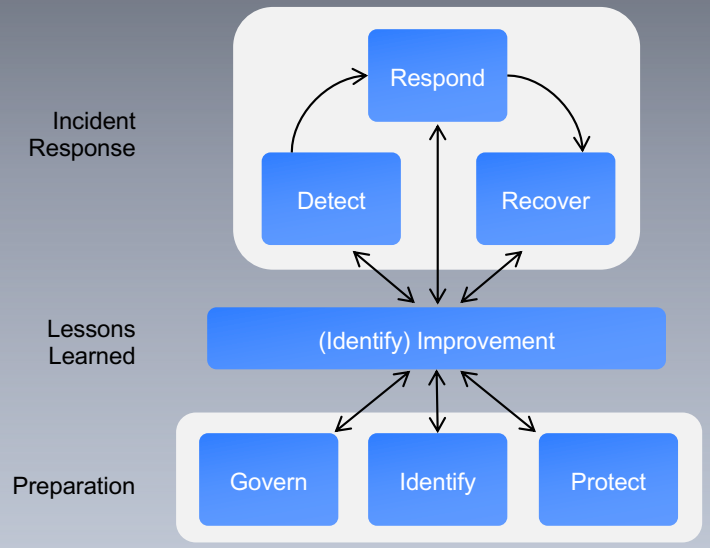
THE SHIFT

Incident Response is Part of Cybersecurity Risk Management

> “Today, incidents occur frequently and cause far more damage. Recovering from them often takes weeks or months due to their breadth, complexity, and dynamic nature.”

Source: NIST Special Publication 800-61r3 Incident Response Recommendations and Considerations for Cybersecurity Risk Management, April 2025

IR LIFECYCLE BASED ON NIST CSF 2.0



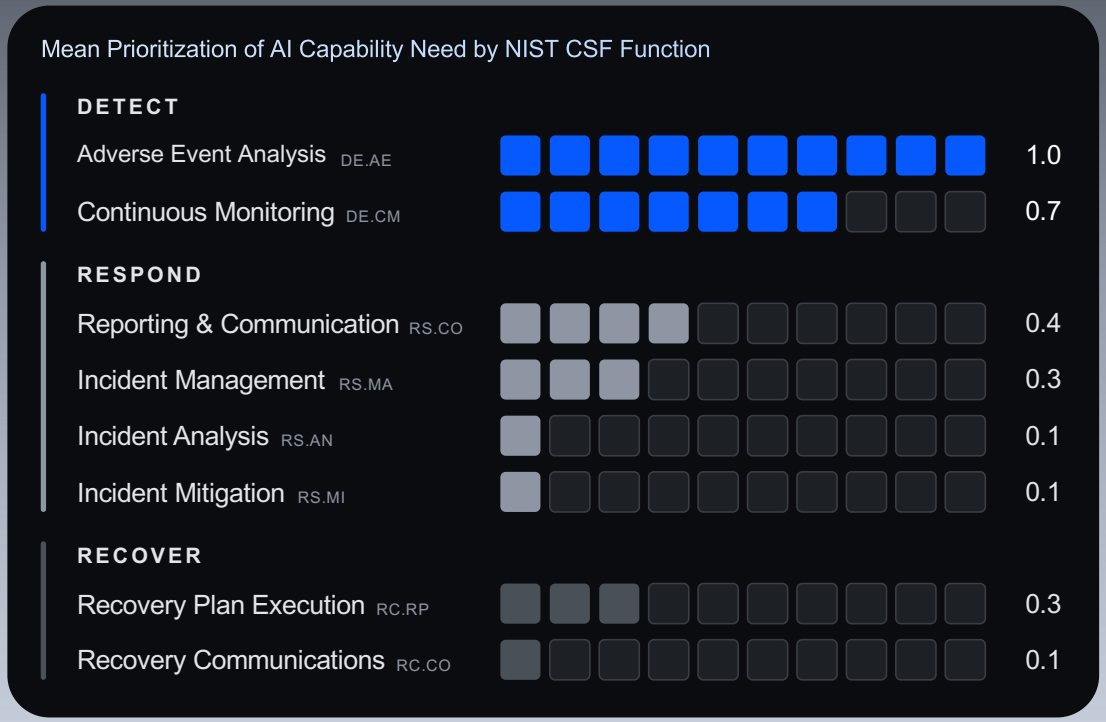
THE STATUS QUO

AI Demand is Highest in Detection – But Response Needs Context Most

AI in the SOC adoption is concentrated in detection and prioritization.

But the hardest decisions **occur after the alert**: what to isolate, what to remove, and how to restore safely without disrupting the mission.

The recent **Hugging Face incident** highlights the gap: manual incident response cannot keep pace with attacks that unfold in seconds.

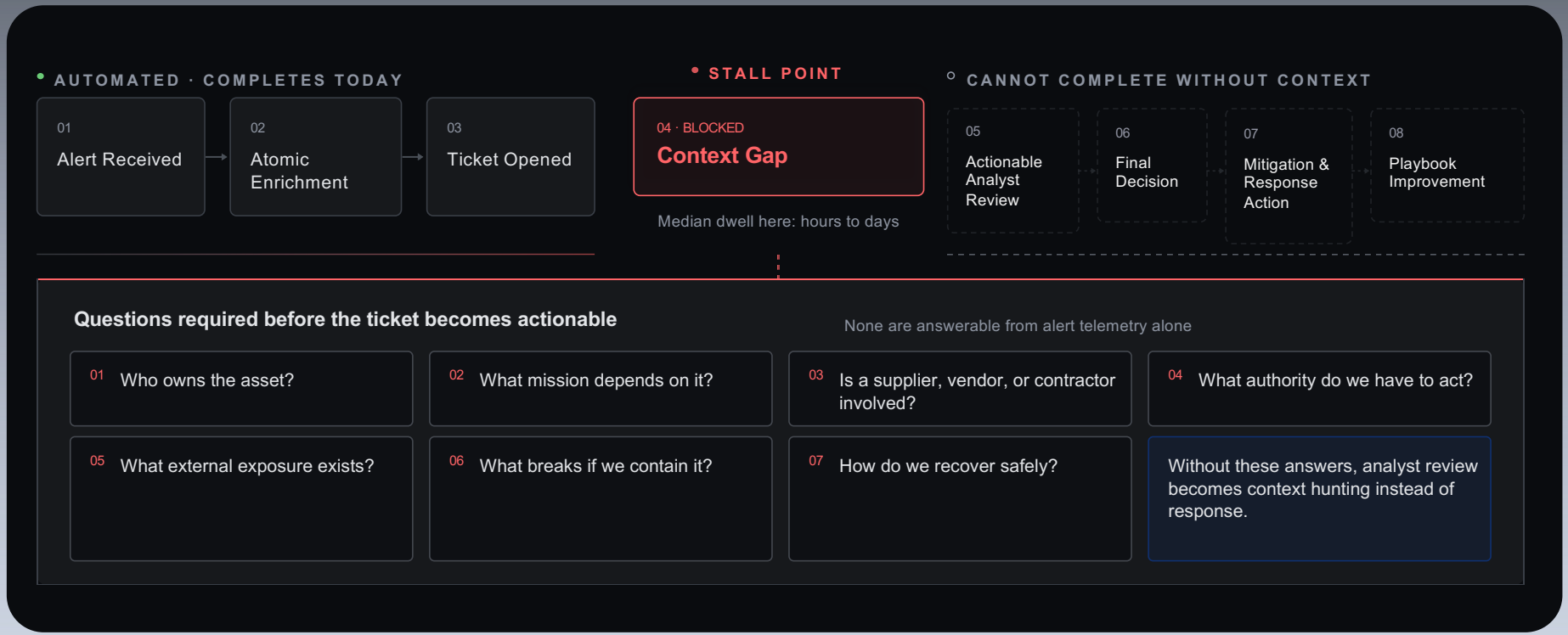


Source: NIST NCCoE Cyber AI Profile Virtual Working Session Series: Conducting AI-enabled Cyber Defense, August 2025

THE CHALLENGE

Fast Enrichment is Not Trusted Action

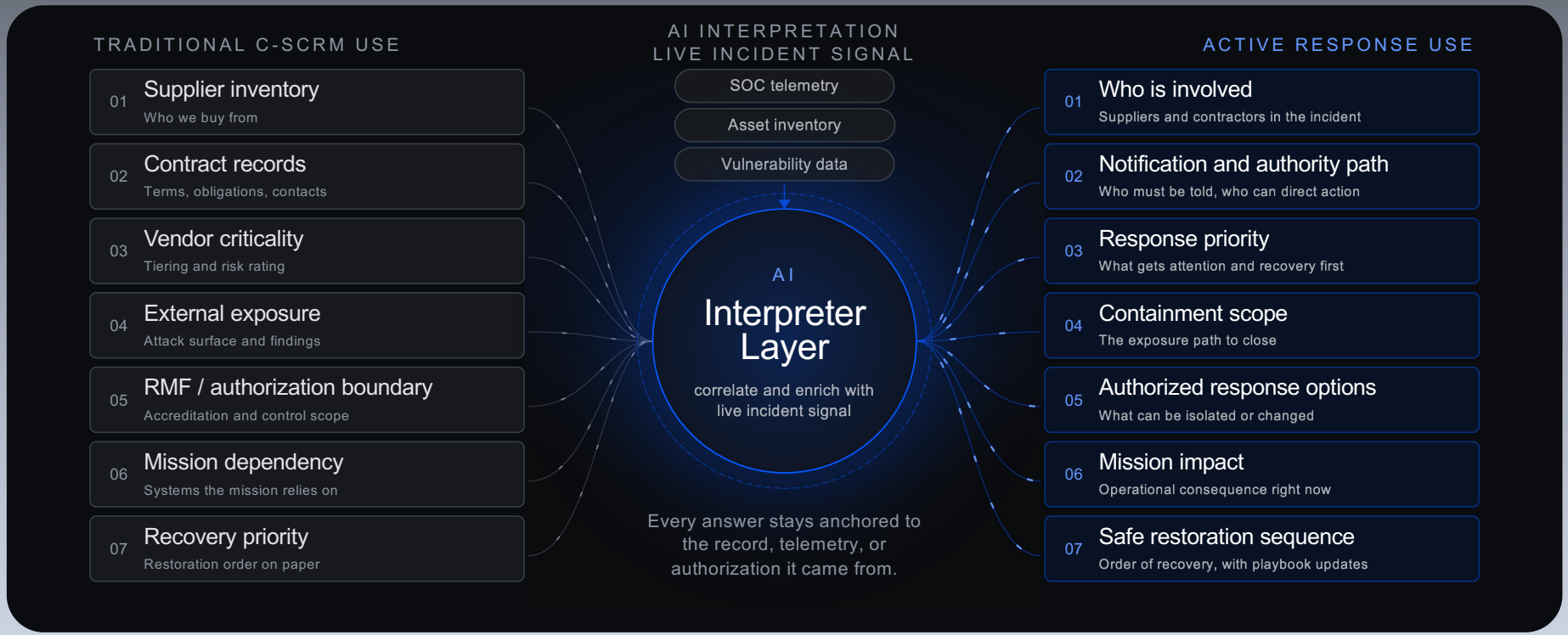
Cyber defenders don’t stall because they lack data. They stall while scrambling for decision-ready context.



THE OPPORTUNITY

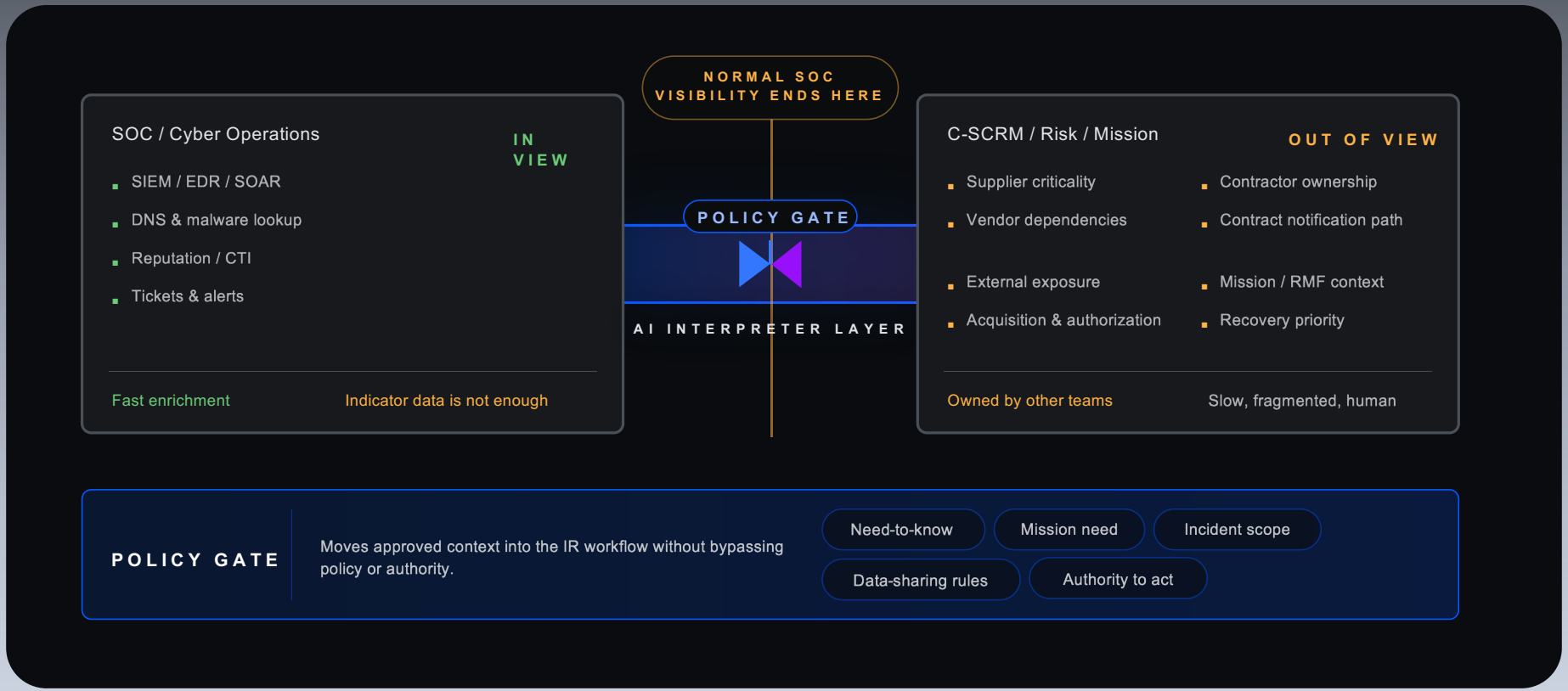
AI as the Supply Chain Context Layer for Incident Response

The C-SCRM data traditionally used for governance and risk management can be correlated with existing signal to reduce uncertainty during incident response.



THE DESIRED END STATE

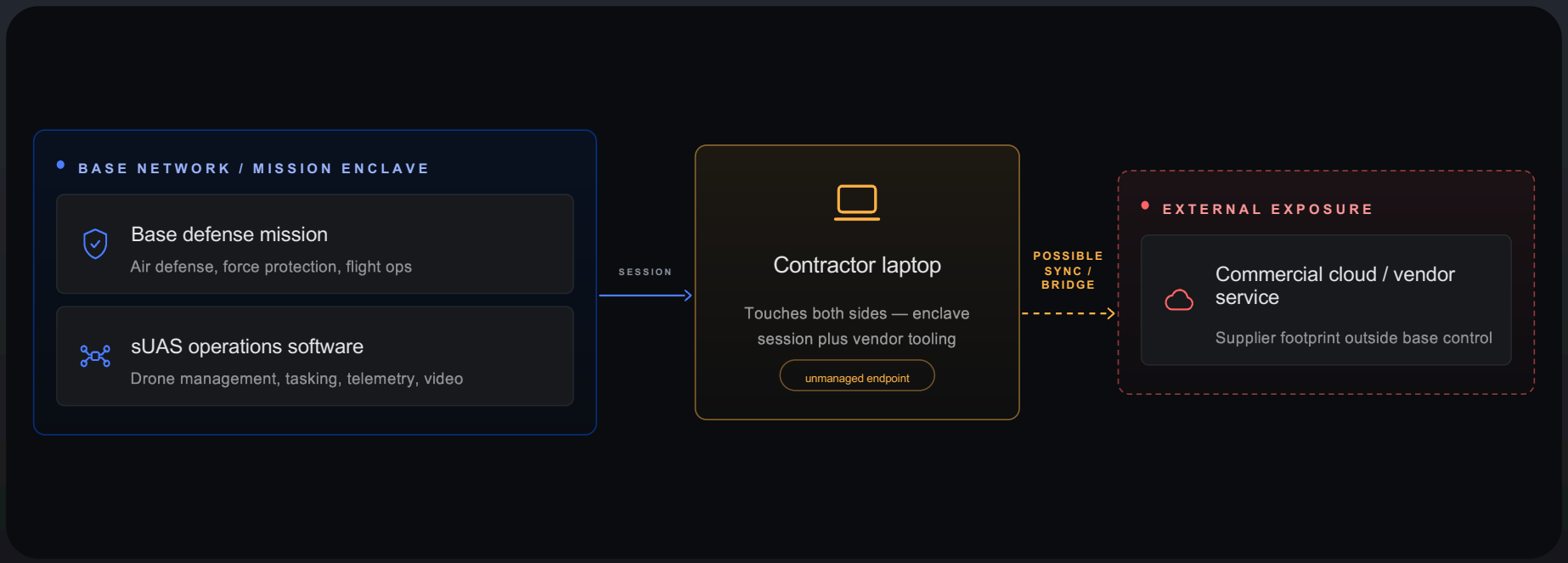
Trusted AI Can Bring this Data Where the SOC Works



SCENARIO WALKTHROUGH

sUAS Base Defense Incident Response

An unmanaged contractor laptop is detected on the base defense network running sUAS operations software. The laptop is also syncing with an external commercial vendor service that is not clearly authorized. **How do you contain exposure without disrupting operations?**



PASS 01 – ATOMIC

What the SOC can see – clean IOCs



What the defender sees:

- ✓ Domain/IP reputation: clean
- ✓ File hash: clean
- ✓ No known malware
- ✓ No threat intelligence match
- ✓ Unmanaged device on-net
- ✓ Outbound TLS to vendor cloud

Response Options

DEPRIORITIZE

BLOCK

What the defender misses:

- X Contractor ownership
- X Purpose of the device
- X Commercial drone software usage
- X Supplier cloud sync
- X Mission data flow
- X Authorization boundary issue
- X Recovery implications

PASS 02 – ENTITY CONTEXT

The records join changes what the device is – but misses connection approval



What the defender sees:

- ✓ Asset lookup
- ✓ User/account ownership
- ✓ Endpoint posture
- ✓ Vulnerability status
- ✓ Network segment
- ✓ Ticket routing
- ✓ Contractor-operated unmanaged device
- ✓ No connection approval on file

Response Options

~~DEPRIORITIZE~~

~~BLOCK~~

KILL THE PORT

What the defender misses:

- x Supplier service dependency
- x Vendor exposure
- x External attack surface
- x Contractual notification path
- x Data sync behavior
- x Mission timing
- x Recovery priority

PASS 03 – MISSION CONTEXT

Consequence and timing guide risk-informed action



What the defender sees:

- ✓ Contractor identity and relationship
- ✓ Supplier software/service footprint
- ✓ External exposure
- ✓ Known supplier vulnerabilities
- ✓ Data-flow or sync indicators
- ✓ Mission dependency
- ✓ Authorized response options
- ✓ Third-party contact path

Final Response Decision

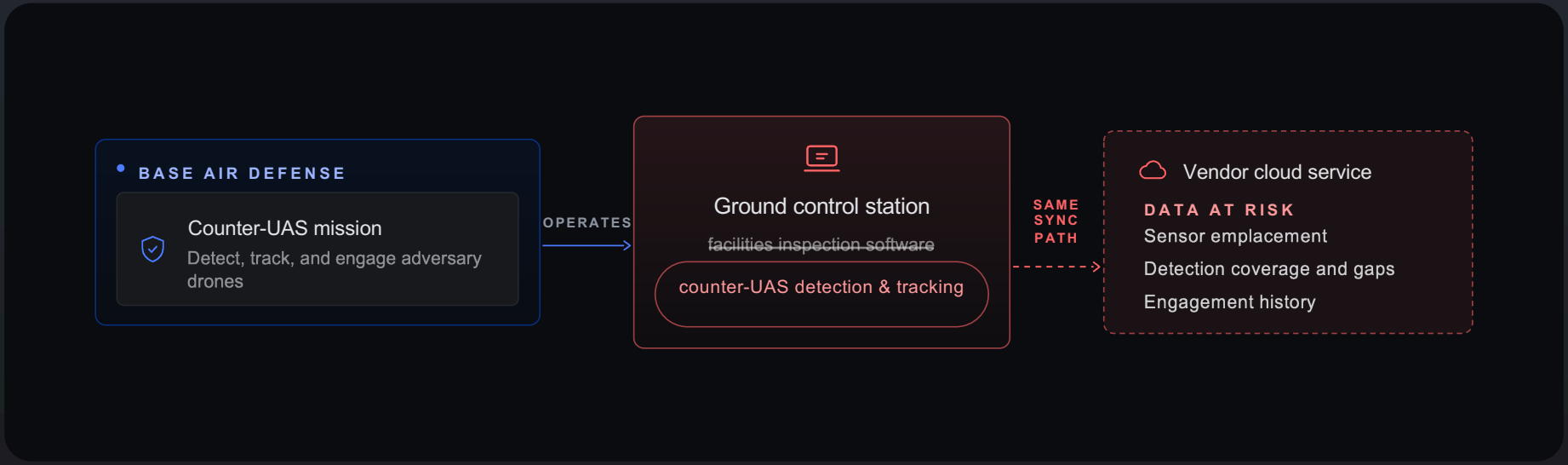
ISOLATE WITH CONTRACTING OFFICER COORINDATION

Response decisions improved:

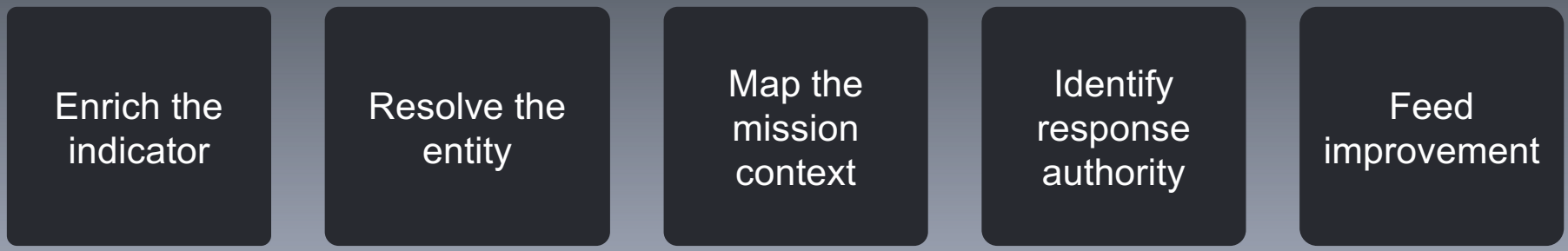
- Containment scope
- Account disablement
- System isolation
- Contractor coordination
- Recovery sequencing
- Playbook improvement

THE REVERSE

Different mission, different response



5-Step IR Framework for AI-Enabled Supply Chain Context



AI capability considerations and guardrails

- **Source grounding:** Use approved data sources and cite where context came from.
- **Policy gate:** Enforce role, need-to-know, incident scope, and data-sharing rules.
- **Human approval:** AI may recommend options; authorized personnel approve action.
- **Confidence and uncertainty:** Surface gaps, assumptions, and conflicting data.
- **Auditability:** Log prompts, sources, outputs, decisions, and actions.

TAKEAWAYS

AI isn’t changing the fundamentals of IR.

But it can change the speed, scale, and quality of context available to cyber defenders as they move through the lifecycle.

Supply chain risk data is also response data.

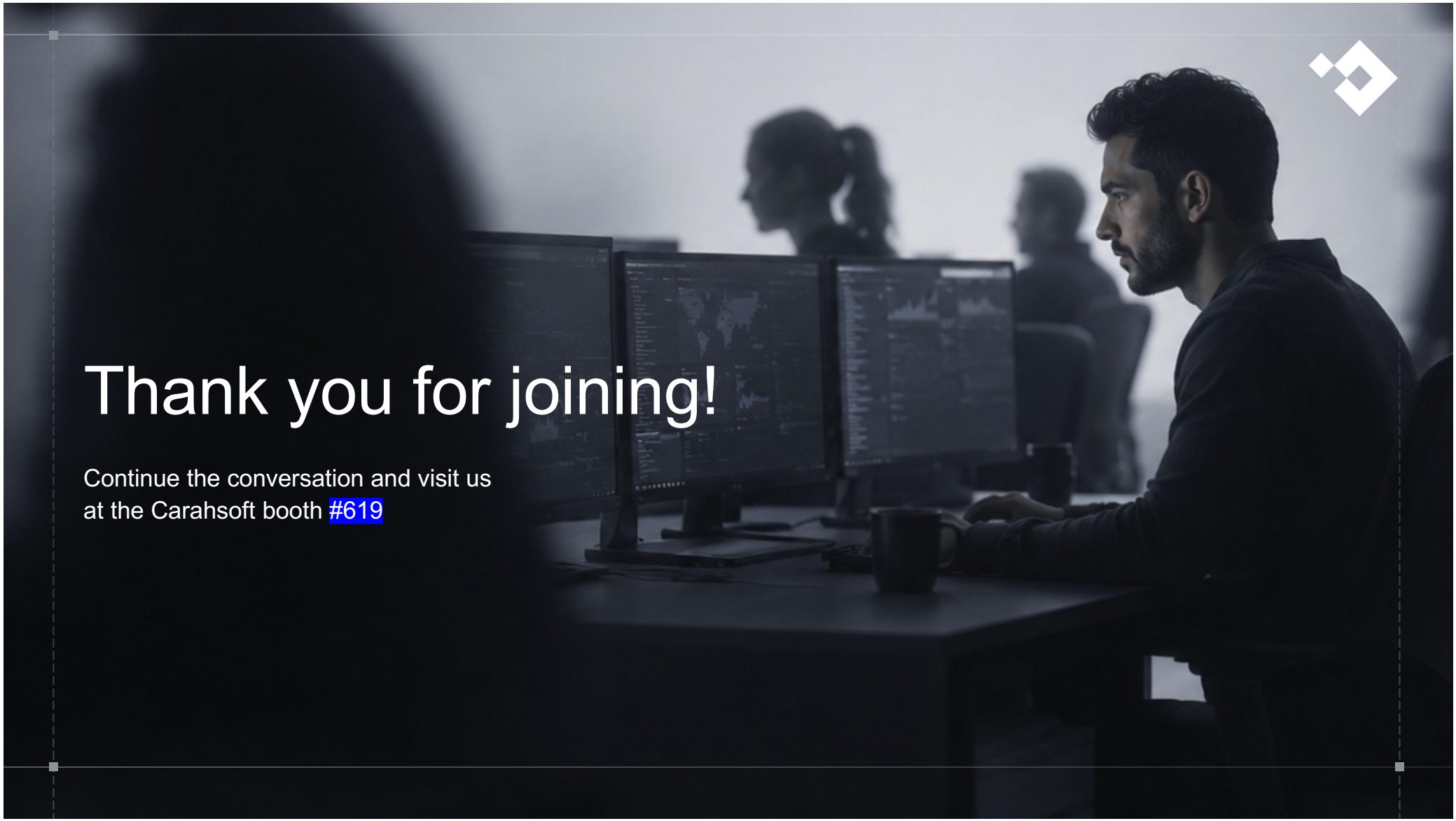
Supplier criticality, vendor dependencies, contractor ownership, and external exposure can improve containment, recovery, and third-party coordination.

Trusted AI balances machine speed with human judgment.

Automation handles the routine. Guardrails define when AI shifts to interpreter mode — providing context for authorized human decisions.

LAST CALL

Questions?


Thank you for joining!
Continue the conversation and visit us
at the Carahsoft booth #619

BlueVoyant AI Private Preview

With our recent release of BlueVoyant AI, our Agentic SecOps offering for Microsoft Security environments, we're now accepting submissions for our Private Preview program.

The Private Preview will include a 45-minute session with one of our product experts, giving you an in-depth demonstration of the offering, and time for you to engage with Q&A.

Scan the QR code

