EXTRAHOP

5 Shifts CISOs Must Make for the Frontier AI Era

> Ultimately, it's about to become very difficult for the security community.
>
> – Anthropic[1]

The Moment We're In: Context Is the New Currency

Enterprise security has reached a critical tipping point where adversaries now identify and exploit vulnerabilities at machine speed, often outpacing human defenders.

Claude Mythos can discover long-standing vulnerabilities that survived decades of human review and millions of automated tests, and chain vulnerabilities together into critical exploit paths. Breakout time—how fast an attacker moves laterally after initial compromise—has effectively collapsed.

The modern SOC was never designed for this velocity.

Security teams have spent a decade scaling telemetry and are drowning in thousands of daily alerts, striving to find meaning among disparate clues. "Delete" has become a survival mechanism. To defend against AI-orchestrated campaigns, the SOC must evolve into a machine-speed, automation-driven operation.

The Bottom Line

Success in the frontier AI era requires a fundamental shift from visibility to real-time context. While AI can enable bad actors to stealthily access networks, it still produces observable artifacts: network traffic, authentication events, data movement, and process behavior. For agentic operations to counter machine-speed threats, organizations must have a contextualization layer that transforms raw telemetry into structured, machine-readable insight. Without it, AI agents are flying blind. They cannot reason about what they cannot understand.

Real-time context allows machine-driven decisions to be accurate, defensible, and fast.

The "Unicorn" Problem

Every enterprise environment is a unique system of relationships, behaviors, and dependencies. Because every enterprise is unique, there is no universal "normal" baseline. For an AI-enabled SOC to function, it must be able to contextualize information against the organization's unique baseline. AI defense is only as good as its ability to understand the organization's specific relationships and dependencies.

1. Assessing Claude Mythos Preview's cybersecurity capabilities, Anthropic, April 7, 2026

The Core Gap: Visibility Without Comprehension

The traditional SOC was built on:

- **Static inventories.** Periodic snapshots and manually updated CMDBs show what existed at a point in time and have little to no awareness of how assets interconnect or change in real time.
- **Isolated alerts.** Detections fire without the behavioral, historical, or sequence context needed to tell a real attack from a routine anomaly.
- **Human-paced workflows.** Analysts act as the integration layer between tools. Context is gathered during investigation, not pre-built. Scaling means hiring.

The result is alerts without context, connection, or meaning—pushing mean time to detect and mean time to respond into hours or days.

What Readiness Looks Like

In this new environment, advantage goes to organizations that can interpret and act on data first—not just collect it. These five shifts are designed to build the contextualization layer necessary for machine-speed defense.

SHIFT 1

From Asset Lists to a **Living Attack Surface**

Most organizations believe they have an inventory. In reality, they have a snapshot. Static CMDBs cannot keep up with dynamic environments that change constantly.

The modern attack surface spans:

- **Infrastructure** — cloud, on-prem, containers, serverless, AI endpoints
- **Software** — applications, APIs, dependencies
- **Identity** — human and machine, with continuously changing roles and permissions

In most global enterprises, a large share of the attack surface—legacy OT, ephemeral cloud functions, and AI model endpoints—either cannot run an EDR agent or simply does not have one. That leaves blind spots exactly where the most consequential logic now lives.

You also cannot triage a flood of software vulnerability disclosures if you do not know what you run, where it runs, or what it touches.

Without real-time visibility, you cannot answer the most basic incident response question:
“Does this affect us?”

You are no longer just securing systems—you are securing machine-driven decisions. AI systems cannot reason about what they cannot see. If the traffic looks “good,” you cannot stop a bad decision after the fact.

What's Required

A complete, continuously updated asset graph that captures:

- What exists (including shadow IT)
- The asset's typical activity
- Who and what are accessing it
- How everything connects

SHIFT 2

From Alerts to **Behavioral Understanding**

Most detections are isolated events. **Real attacks are patterns over time.**

Traditional tools miss threats that operate within legitimate access—especially AI agents. A compromised AI agent doesn't install malware. It uses authorized access in unauthorized ways.

Only behavioral analysis can detect that shift—for example:

- An agent suddenly exporting 10,000 records instead of 10
- Accessing new domains or systems outside its normal pattern

In a world where attacks unfold in seconds, waiting for signatures is too slow.

What's Required

- Behavioral baselines and real-time anomaly detection across users, systems, and agents
- Integrated contextualization that correlates disparate signals across the environment and enriches core telemetry with endpoint and identity metadata

SHIFT 3

From Analyst-Driven SOCs to **Agent-Ready Operations**

Agentic SOCs rely on autonomous systems to triage, investigate, and respond. But if your SOC depends on humans to assemble context, it cannot operate at machine speed.

Autonomous agents cannot operate effectively on raw, disconnected telemetry. They require **pre-built, structured context**—data that is already enriched, correlated, and ready for machine reasoning.

When an autonomous triage agent picks up a signal, it should not have to hunt for the full picture. It needs an immediate, high-fidelity dossier.

Context becomes the foundation of automation—not an afterthought.

The four dimensions of structured context

Asset Context

- Continuous, real-time inventory
- Criticality and sensitivity
- Expected relationships and patterns
- Software, services, and dependencies

Identity Context

- Human and non-human credentials
- Roles, privileges, and authentication events
- Peer group behavior
- Forged tickets, token misuse, and anomalies

Behavioral History

- What "normal" looks like in this environment
- Deviations from normal baseline
- Persistent memory of behaviors with the ability to learn from the past and apply it to the present
- Anomalous prompts and agent actions
- Unexpected protocols, ports, and services

Threat Relevance

- Known TTPs mapped to MITRE ATT&CK
- Blast radius and affected systems
- Timestamp, duration, sequence, velocity
- Confidence level

What's Required

- A dedicated enrichment layer that continuously correlates and contextualizes data
- Standardized, machine-readable representations of assets, identities, behaviors, and threats
- Pre-built, investigation-ready datasets (not raw telemetry) for both humans and agents
- Integration across tools so context is unified, not fragmented

SHIFT 4

From Raw Telemetry to **Efficient, Affordable Reasoning**

Raw telemetry is massive, noisy, and expensive to feed into advanced models. Large language models (LLMs) are powerful, but they are not cheap at scale.

Pointing an LLM directly at raw network exhaust, packet captures, and unfiltered logs is neither cost-effective nor operationally viable. Token budgets explode, context windows saturate, and reasoning quality degrades as signal gets buried in noise.

The solution is **high signal density**—the data is already enriched, correlated, and summarized, so the model can reason over patterns directly. Who communicated with whom, over what protocol, in what sequence, how it deviated from baseline, and whether it warrants immediate attention. Drill into supporting packet evidence only when a specific hypothesis demands it. This is the architectural pattern that makes agentic SOC economics work at all.

What's Required

Architectures that optimize for high-quality input, not maximum data volume

SHIFT 5

From One-Dimensional Data to **Multi-Layer Evidence**

Most AI security strategies underperform because they rely on the wrong data mix. Different tasks need different data types:

Data Type	What It's For
Metrics	Trends and behaviors
Metadata	Relationships and transactions
Detections	Known anomalies
Packets	Ground truth

What's Required

Build a tiered data strategy: lightweight data for continuous reasoning, with deep evidence available on demand.

The New Security Operating Model

Frontier AI doesn't just introduce new threats. It forces a new architecture for defense.

Security becomes:

- **Unified**, not fragmented
- **Adaptive**, not reactive
- **Machine-scale**, not human-scale

Organizations that make these shifts early won't just keep up—they will define what effective security looks like in the AI era.

Those who don't will be forced to react to it. In a world of machine-speed attacks, reaction is already too late.

ABOUT EXTRAHOP

ExtraHop transforms network data—one of the enterprise's most reliable sources of truth—into high-fidelity, actionable context. ExtraHop gives security and IT operations teams real-time, behavioral context across the enterprise—from legacy systems to cloud and AI environments, from privileged identities to critical systems.

For the SOC and NOC, ExtraHop delivers ground truth using deep network visibility, real-time asset inventory, application dependency mapping, and strategic decryption to detect performance issues and advanced threats.

Whether organizations are modernizing their operations or delivering more autonomous workflows, ExtraHop enables organizations to detect issues earlier, respond with confidence, and maintain resilience and security at uncompromised scale.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com