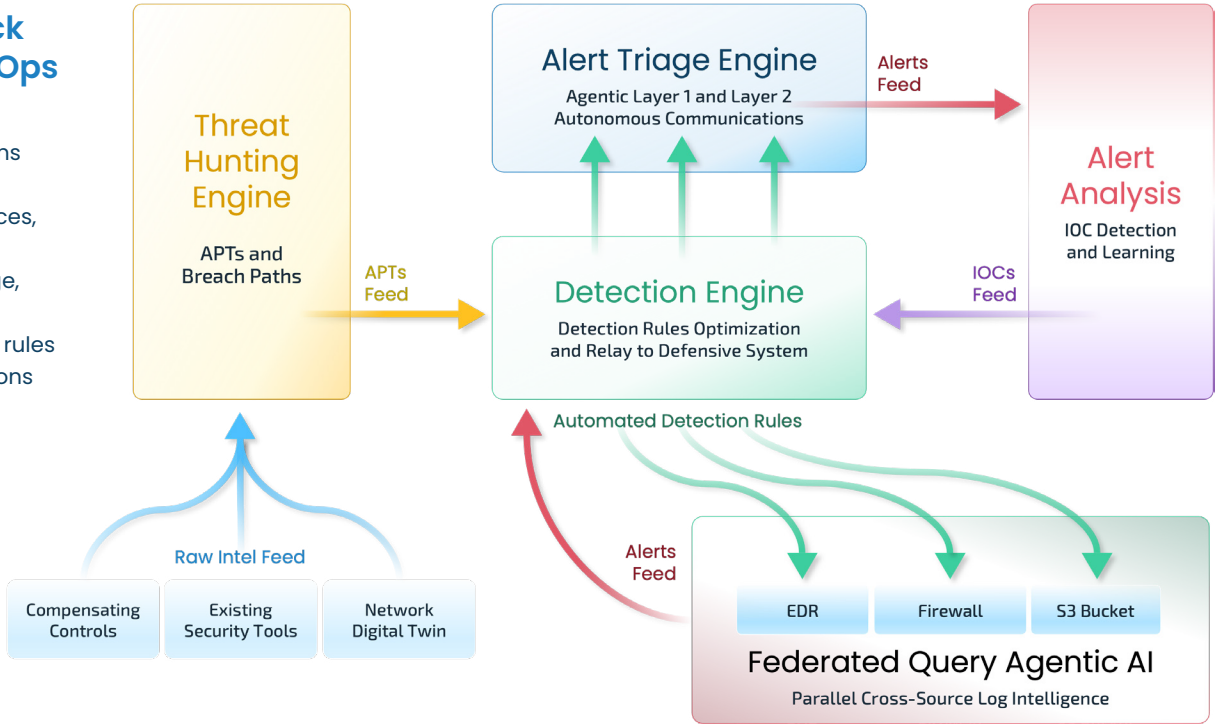
Unified Intelligence. Distributed Detection.

Tuskira™
Full Stack Agentic SecOps

Tuskira unifies intelligence across distributed security data sources without requiring costly log centralization. The platform generates detections at the source, validates them with continuous AI triage, and helps security teams reduce noise, uncover multi-stage attacks, and respond faster. The result is fewer false positives, lower SIEM overhead, and a continuously improving detection and response posture.

The Full Stack Agentic SecOps Platform

Generate detections across distributed security data sources, validate them with continuous AI triage, and continuously improve detection rules and response actions across the SOC.



SecOps Requires Four Core Functions

Every security operations team must continuously execute across four domains:

Threat Detection

Generate detections across endpoint, network, cloud, identity, and other distributed security data sources.

Alert Triage

Validate alerts, reduce false positives, and prioritize what represents real breach risk.

Threat Hunting

Identify hidden attacker behavior, APT activity, and multi-stage intrusion paths that evade static detections.

Threat Containment

Translate validated findings into targeted containment actions and defensive changes.

In most organizations, these functions are fragmented across disconnected tools, siloed data, and manual workflows. Tuskira unifies them through an AI Reasoning & Context Layer, a Security Context Graph Mesh, and a Federated Detection AI-Engine that leaves data where it lives and queries it at the source.

> *"Tuskira changed how our SOC operates. Detections are no longer static, and our analysts spend less time chasing noise and more time focused on real threats. We also started seeing value quickly, without waiting months for a large data migration."*
>
> Chief Information Security Officer
> **Global Industrial Enterprise**

Why SecOps Breaks Down

Too many tools, data silos, and no unified threat visibility

Teams operate across dozens of disconnected tools with no shared attacker, asset, or infrastructure context, making it difficult to see the full breach path.

Detection depends on expensive data centralization

Organizations pay to move massive volumes of data into centralized platforms, then still deal with reduced log coverage, stale rules, and heavy dependence on SIEM and human expertise.

Teams optimize for speed, not intelligence

Analysts are pushed to close tickets quickly, but detections, investigations, and prevention controls rarely improve through a continuous feedback loop.

How Tuskira Solves It

Federated Detection

Tuskira generates high-fidelity detections directly at the data source, eliminating costly log centralization and helping detection logic evolve faster than attacker TTPs.

Context Graph Engine

Tuskira unifies identity, endpoint, cloud, and network context into a single threat model, giving teams shared visibility into attacker behavior and full breach paths across the environment.

Autonomous SOC Agents

Tuskira applies AI-driven triage, investigation, and precision containment to help teams prioritize real breach risk, reduce noise, and improve response speed through a continuous learning loop.

What This Enables:

1. Lower SIEM and log-ingestion costs
2. Full breach-path visibility across distributed environments
3. Faster expert-level triage and containment
4. Fewer false positives and less analyst noise
5. Continuous improvement across detection, investigation, and response

Metric	Traditional SecOps	Full Stack Agentic SecOps
Alert Volume	High noise with static rules	**Reduced through federated detection and AI triage**
Investigation	Manual context gathering across tools	**Unified intelligence across distributed telemetry**
Threat Hunting	Siloed, reactive, incomplete	**Better visibility into attacker behavior and breach paths**
Containment	Reactive and temporary	**Targeted response actions pushed back into existing controls**

Experience Agentic SecOps in Action

See how Tuskira helps security teams detect threats earlier, reduce alert noise, and accelerate triage, hunting, and containment across the SOC. **Request a technical deep dive demo.**

Website: tuskira.ai
Email: Lorin@tuskira.ai

Tuskira™
Full Stack Agentic SecOps