ANOMALI

Guide

WHAT IS AN AGENTIC SOC PLATFORM?

A Practical Guide

WHY THE SOC NEEDS TO CHANGE

Security operations centers are under pressure from every direction. Data volumes continue to grow, threat actors move faster, and security teams are expected to deliver measurable outcomes with largely fixed budgets and staffing.

But the problem runs deeper than scale.

The legacy SIEM-centric SOC model is no longer sustainable. Next-generation platforms promised AI but delivered more alerts, not better outcomes. Analysts are drowning in noise. Budgets are strained by ingest-based pricing. The complexity of hybrid and multi-cloud environments is overwhelming already stretched teams.

Traditional SIEM-centric architectures were built for log retention and alerting, not for decision-making at scale. Threat intelligence platforms were designed for research, not operational execution. Automation without context often increases noise instead of reducing risk.

Security operations now demand an intelligence-native architecture that applies context at ingest, enables AI-ready data foundations, and drives response at machine speed with human oversight.

Without this shift, SOCs remain reactive, costly, and inconsistent.

The Anomali Intelligence-Native Agentic SOC Platform unifies a high-fidelity security data lake, next-generation ThreatStream intelligence, and true agentic AI into a single operational experience.

Rather than producing more alerts or dashboards, it focuses on turning telemetry and intelligence into guided, high-confidence security decisions.

This guide explains what an agentic SOC platform is, how it works in practice, and how Anomali's core components work together to support modern SOC and CTI workflows.

WHAT IS AN AGENTIC SOC PLATFORM?

An agentic SOC platform is an operational security platform where AI-driven agents actively assist analysts by reasoning across security data and threat intelligence to support detection, investigation, and response.

Unlike traditional analytics or automation tools, an agentic SOC platform operates at the decision layer. It does not simply generate alerts or run predefined playbooks. Instead, it continuously analyzes telemetry, enriched threat intelligence, and historical context to:

- Deliver intelligence-native detections at ingest
- Reduce alert noise and prioritize what matters
- Provide actionable investigative context
- Guide analysts toward effective response decisions
- Ensure intelligence is consistently operationalized across teams

In the Anomali Agentic SOC Platform, agentic AI works alongside human analysts. Analysts remain in control, while AI provides speed, context, and consistency at scale.

THE THREE LAYERS OF THE ANOMALI AGENTIC SOC PLATFORM

The Anomali Agentic SOC Platform is built on three tightly integrated layers. Each layer solves a specific operational problem, but the real value emerges when they work together.

1. UNIFIED SECURITY DATA LAKE: THE FOUNDATIONAL LAYER

Every SOC workflow depends on data. If telemetry is incomplete, delayed, or constrained by indexing limits, investigations stall and decisions degrade.

The Anomali Unified Security Data Lake is a modern, AI-ready, hyperscale security data architecture purpose-built for intelligence-driven operations.

Unlike legacy SIEM backends, it is designed to augment or replace existing SIEM investments, eliminating ingestion bottlenecks and unpredictable cost scaling. Key characteristics include:

- Centralized ingestion of security telemetry across cloud, endpoint, network, identity, and application sources
- Security-native normalization and correlation at ingest
- Always-searchable, investigation-ready data with no retention tradeoffs
- High-speed search and analytics across months or years of telemetry

Because telemetry is normalized and correlated as it enters the platform, downstream workflows operate on clean, consistent context. This enables analysts and agentic AI to pivot quickly across alerts, entities, and timelines without blind spots.

2. THREATSTREAM NEXT-GEN: THE INTELLIGENCE GRAPH LAYER

Telemetry alone does not explain risk. Knowing that something happened is not the same as understanding who is behind it, why it matters, or what is likely to happen next.

ThreatStream Next-Gen provides the intelligence layer of the agentic SOC. It continuously enriches security telemetry with curated, confidence-scored threat intelligence, including:

- Threat actors, campaigns, and infrastructure
- Tactics, techniques, and procedures mapped to MITRE ATT&CK
- Behavioral and indicator-of-attack context
- Asset-based contextualization tied to organizational risk

This intelligence is not static. It is automatically correlated with internal telemetry so that context travels with every alert and investigation. As a result, SOC and CTI teams can prioritize based on adversary intent and operational relevance rather than raw indicator volume.

ONE PLATFORM. THREE LAYERS.

ONE OUTCOME: FASTER, SMARTER DEFENSE

FOUNDATION LAYER

UNIFIED SECURITY DATA LAKE

Anomali's unified security data lake is the foundation of the Agentic SOC. It centralizes and retains massive volumes of security telemetry – cloud endpoint, network, identity and beyond, without the performance limits or cost penalties of legacy SIEMs.

This isn't cold storage.

It's always-on, always-searchable and built for real-time and historical analysis at scale.

INTELLIGENCE GRAPHIC LAYER

THREATSTREAM NEXT-GEN

Raw events don't explain risk.

Context does.

ThreatStream continuously enriches your data lake with real-world threat intelligence actors, infrastructure, TTPs and campaigns, so analysts understand who, why and what next not just what happened.

AGENTIC OPERATIONS LAYER

AGENTIC AI

Agentic AI brings agency to the SOC.

Instead of static dashboards or chat-only copilots, Anomali's AI-driven agents reason over your data lake and intelligence context to guide investigations, recommend next actions and automate response workflows.

The result: fewer steps, faster decisions and consistent execution without removing human control.

3. AGENTIC AI: AGENTIC OPERATIONS LAYER

Agentic AI sits above the data and intelligence layers, operating at the point where decisions are made.

Capabilities include:

- Automated enrichment and investigation of alerts
- Behavioral and IOA-based analytics focused on attacker intent
- Intelligence-ready guidance that travels with alerts and cases
- Context-aware response and mitigation recommendations
- Semantic search and natural-language interaction grounded in security context

In the Anomali platform, AI-driven agents reason across the Unified Security Data Lake and ThreatStream Next-Gen intelligence to support investigations and response. Rather than replacing analysts, agentic AI focuses on reducing manual effort and inconsistency.

This allows analysts to spend less time correlating data and more time applying judgment and taking action.

HOW AGENTIC SOC WORKFLOWS OPERATE

An agentic SOC platform is best understood through its workflows. Below is an example of how detection, investigation, and response work together in the Anomali Agentic SOC Platform.

DETECTION: FROM SIGNALS TO MEANING

Detection begins with telemetry flowing into the Unified Security Data Lake. Because data is normalized and enriched in near real time, detections are built on complete, unmodified data rather than sampled or delayed logs.

ThreatStream Next-Gen continuously enriches this telemetry with real-world threat intelligence. Agentic AI evaluates alerts using historical patterns, behavioral context, and adversary intelligence to suppress low-value signals and surface high-confidence threats.

INVESTIGATION: CONTEXT WITHOUT MANUAL CORRELATION

When an alert is escalated, agentic AI assists analysts by automatically correlating:

- Related entities and historical activity
- Threat actors, campaigns, and infrastructure
- Behavioral indicators aligned to attacker TTPs

Analysts can pivot across indicators, timelines, and threat models using semantic search and investigation workbenches. Knowledge graphs bridge natural language queries with structured security data, enabling multi-hop reasoning without complex query construction.

RESPONSE: GUIDED, CONSISTENT ACTION

Agentic AI provides context-aware response recommendations based on the specific threat scenario and environment. These recommendations are informed by intelligence, telemetry, and prior outcomes, reducing guesswork and variability.

Because intelligence and context are embedded across workflows, response actions can be executed consistently across SOC, CTI, and downstream tools such as SOAR, EDR, XDR, and ticketing systems. Response becomes consistent, intelligence-informed, and measurable.

KEY OUTCOMES OF AN AGENTIC SOC PLATFORM

Organizations adopting an agentic SOC platform aim to achieve operational outcomes rather than incremental tooling improvements.

300X FASTER DETECTION AND INVESTIGATION
Analysts pivot across years of data and intelligence in seconds.

50% ANALYST TIME SAVED WITH OPERATIONALIZED INTEL
Threat intel informs every stage of the SOC workflow, not just reports.

96% REDUCED TIME FOR THREAT INVESTIGATIONS
Context-driven prioritization reduces false positives and alert fatigue.

60% REDUCED SIEM BILL AND OPERATIONAL COST
Eliminate SIEM tax and manual effort while scaling data retention.

With the Anomali Agentic SOC Platform, teams typically focus on:

- Faster detection and triage through intelligence-driven prioritization
- Shorter investigation cycles with full historical and adversary context
- Reduced alert fatigue and analyst burnout
- More consistent, repeatable security decisions across teams
- Stronger alignment between SOC and CTI operations

These outcomes are driven by the platform's ability to move from raw data to guided action, rather than stopping at alerts or analytics.

HOW THE PLATFORM WORKS AS A SYSTEM

The defining characteristic of an agentic SOC platform is how its components work together.

- The Unified Security Data Lake ensures complete, accessible, and normalized telemetry
- ThreatStream Next-Gen transforms intelligence into operational context
- Agentic AI reasons across both layers to guide detection, investigation, and response

This integrated approach reduces tool sprawl and manual handoffs. Intelligence is no longer separate from operations, and AI is not bolted onto existing workflows. Instead, the platform functions as a single operational plane where data, intelligence, and decisions are tightly connected.

AGENTIC AI AND THE SOC: HOW TO OPERATIONALIZE AGENTIC AI ACROSS SECURITY OPERATIONS

An agentic SOC platform represents a shift in how security operations are designed. Rather than optimizing individual tools, it focuses on enabling better decisions at scale. It transforms the SOC from a reactive alert center into an intelligence-native, AI-accelerated decision engine.

The Anomali Agentic SOC Platform brings together always-on telemetry, continuously enriched threat intelligence, and agentic AI enable organization so:

- Modernize without disruptive rip-and-replace
- Augment existing SIEM investments
- Reduce cost and complexity
- Prepare for AI-driven adversaries
- Scale operations across hybrid, multi-cloud environments

For organizations looking to move beyond alert-centric security operations, an agentic SOC platform provides a practical path from information to action.

SEE ANOMALI IN ACTION

Request a Demo