ANOMALI

White Paper

AGENTIC SOC PLATFORM

From Intelligence to Control: Threat-Informed, Identity-Aware Security Decisioning

EXECUTIVE SUMMARY

Security operations teams have invested heavily in SIEM, EDR, SOAR, identity, and vulnerability management platforms. Yet despite the proliferation of tools, outcomes have not kept pace. Alert volumes remain overwhelming, response is often delayed, and prioritization decisions lack the context required to confidently prevent or contain attacks.

The root cause is not insufficient data. It is the absence of decision-grade context at the moment controls must be applied.

This whitepaper introduces a threat-informed operating model powered by the Anomali Agentic SOC Platform. By unifying complete security telemetry, continuously enriched threat intelligence, and AI-assisted investigations, the platform enables identity-aware, intelligence-driven decisions across the attack lifecycle. The result is a shift from reactive analysis to proactive, decision-driven control that reduces breach probability, lowers operational cost, and improves measurable risk outcomes.

THE STRUCTURAL PROBLEM IN MODERN SECURITY OPERATIONS

Across SOC, CTI, identity, and vulnerability management functions, security teams encounter the same structural breakdowns:

- Decisions are made after access is granted, after execution occurs, or after exploitation is detected.
- Prioritization lacks identity, asset, and exploitation context, forcing analysts to rely on severity scores and intuition.
- Controls are applied reactively, often too late to prevent meaningful impact.
- Signals are buried in noise, overwhelming analysts and delaying response.

Adversaries exploit these conditions by abusing identities, rotating infrastructure, leveraging low-and-slow techniques, and exploiting known vulnerabilities faster than organizations can react. In this environment, detection alone does not equal defense. Security outcomes depend on whether decisions are informed, timely, and enforceable.

FROM INTELLIGENCE TO CONTROL: DEFINING THE USE CASE

“From intelligence to control” describes a security operations model in which threat intelligence, identity context, asset criticality, and telemetry directly inform enforcement decisions. Rather than treating intelligence as a reference input or post-incident artifact, this use case embeds intelligence into operational decision points across access, detection, investigation, and response.

This approach shifts security operations from alert processing to decision governance. Controls are applied earlier, with greater confidence, and with an understanding of business impact. The Agentic SOC Platform enables this shift by transforming raw data into context and translating that context into action.

HOW THE AGENTIC SOC PLATFORM POWERS THIS USE CASE

UNIFIED SECURITY DATA LAKE: DECISION-GRADE TELEMETRY

Effective control decisions require complete visibility. Traditional SIEM backends were designed for log retention, not active decisioning, forcing teams to choose between cost, performance, and coverage.

The Agentic SOC Platform's unified security data lake centralizes identity, endpoint, network, cloud, and application telemetry without retention tradeoffs. Data remains searchable, correlated, and investigation-ready across historical timelines. This foundation ensures that decisions are based on complete, unmodified evidence rather than partial snapshots.

THREATSTREAM NEXT-GEN: INTELLIGENCE THAT BECOMES CONTEXT

Threat intelligence delivers value only when it changes decisions. Static feeds and indicator lists overwhelm analysts without clarifying risk.

ThreatStream Next-Gen continuously enriches telemetry with real-world adversary, infrastructure, and campaign context. Intelligence is applied at the point of analysis to suppress irrelevant noise, elevate meaningful signals, and highlight exploitation reality. This allows teams to prioritize based on who is attacking, how they operate, and what is likely to happen next.

AGENTIC AI: FROM CONTEXT TO CONFIDENT ACTION

Even with complete data and intelligence, manual correlation slows response and introduces inconsistency.

Agentic AI reasons across telemetry, identity, and threat intelligence to support investigations and control decisions. It automates enrichment, surfaces explainable conclusions, and helps analysts determine when confidence thresholds are met for enforcement actions. This ensures that response decisions are consistent, repeatable, and defensible across SOC and CTI teams.

DECISION DOMAINS ENABLED BY THE PLATFORM

IDENTITY-AWARE DECISIONING

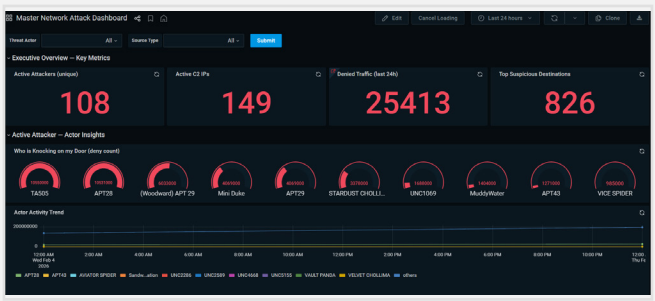
Identity is the dominant attack vector. This use case enables identity risk evaluation before access and during activity, not only after compromise. Identity-enriched investigations improve alert prioritization, while hypothesis-driven identity hunting surfaces stealthy misuse earlier.

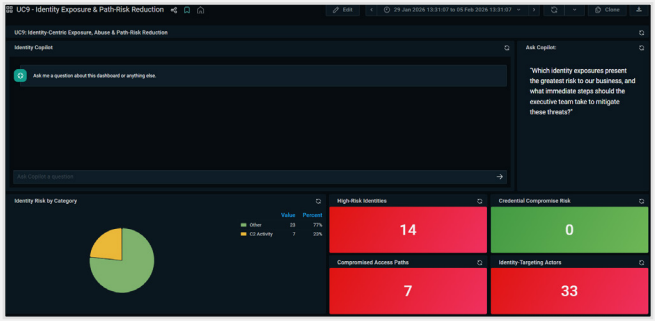
Outcome: Reduced lateral movement, earlier detection, and defensible access decisions.

INTELLIGENCE-DRIVEN SIGNAL REDUCTION

Not all alerts, vulnerabilities, or indicators carry equal risk. By embedding intelligence into operational workflows, the platform suppresses false positives, prioritizes exploitable vulnerabilities, and accelerates intelligence-to-action.

Outcome: Fewer alerts, faster decisions, and measurable reductions in analyst fatigue and SIEM cost.





THREAT-INFORMED RESPONSE ACCELERATION

Response effectiveness depends on confidence. Campaign-level context replaces reputation-only judgments, while AI-assisted investigations reduce time to certainty. Automated containment executes when thresholds are met, reducing dwell time without increasing false positives.

Outcome: Faster response, consistent enforcement, and improved SOC efficiency.

PROACTIVE AND RETROSPECTIVE COVERAGE

Security operations must operate ahead of attackers and across historical timelines. Predictive detection disrupts attacks before execution, while retrospective analysis identifies exposure beyond traditional retention limits. Intelligence updates are continuously re-evaluated against historical data.

Outcome: Fewer initial compromises and evidence-based exposure management.

BUSINESS OUTCOMES

When intelligence, identity, telemetry, and automation operate as a unified system, organizations achieve:

- Lower initial compromise rates through early-stage disruption
- Reduced attack blast radius via identity- and asset-aware controls
- Faster MTTR, trending toward pre-incident prevention
- Lower operational cost through noise suppression and prioritization
- Executive-ready reporting aligned to business risk

Security operations transition from alert handling to risk governance.

OPERATIONALIZING THE USE CASE

This model does not require wholesale platform replacement. Organizations operationalize it incrementally by integrating intelligence with identity and telemetry, applying context at decision points, and automating enforcement where confidence is high. Value is demonstrated through measurable outcomes, not tool sprawl.

FRAMEWORK AND ANALYST ALIGNMENT

This use case operationalizes established guidance from Gartner and Forrester, aligns with Zero Trust principles, and maps cleanly to NIST CSF 2.0. The Agentic SOC Platform simplifies these frameworks by unifying data, intelligence, and decisioning into a single operational plane.

CONCLUSION

Security teams may have the right tools, but can still fail if security decisions are being made without sufficient context and controls are applied too late. By unifying intelligence, identity, telemetry, and AI-assisted decisioning, the Anomali Agentic SOC Platform enables organizations to move from reactive detection to proactive control.

The outcome is not success driven by more alerts or dashboards, but by metrics that include fewer successful attacks and faster, more confident decisions.

SEE ANOMALI IN ACTION

Request a Demo