ANOMALI

White Paper

# AGENTIC SOC PLATFORM

Threat-Informed Response Acceleration: Improving Security Operations Decisions Through Intelligence-Led Context and Automation

## EXECUTIVE SUMMARY

Security operations teams are inundated with alerts but often lack the contextual clarity required to move quickly from detection to confident response. While modern security tools generate large volumes of telemetry, incidents frequently stall during investigation as analysts attempt to determine scope, confidence, and appropriate action.

This white paper presents a threat-informed response acceleration model powered by the Anomali Agentic SOC Platform. By integrating threat intelligence, security telemetry, and AI-assisted analytics, the platform enables rapid, high-confidence decision-making. Investigations shift from isolated alert review to campaign-level understanding, allowing organizations to reduce response time, improve containment accuracy, and maximize the value of existing security investments.

## THE SECURITY OPERATIONS DECISION GAP

Security operations workflows are commonly structured as a linear sequence:

- Monitor for events
- Detect suspicious activity
- Investigate impact
- Respond and mitigate

In practice, progress stalls at the investigation stage. Analysts struggle to answer fundamental questions quickly:

- Is the activity truly malicious
- Does it meaningfully affect the organization
- How confident is the assessment
- What action should be taken now

Without integrated context, analysts rely on manual correlation across tools, delaying response and increasing uncertainty.

# LIMITATIONS OF ALERT-DRIVEN INVESTIGATION

## OPERATIONAL LIMITATIONS

Alert-centric workflows create several challenges:

- Alerts lack adversary and campaign context
- Investigations focus on individual events rather than exposure scope
- Response decisions are delayed while confidence is validated

## BUSINESS IMPACT

These limitations have direct operational consequences:

- Increased dwell time for active threats
- Inconsistent containment and remediation decisions
- Higher operational cost and analyst fatigue

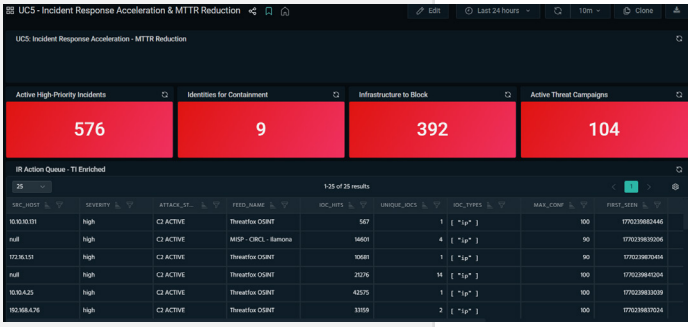
Alert volume increases, but decision quality does not.

# THREAT-INFORMED RESPONSE ACCELERATION: DEFINING THE USE CASE

Threat-informed response acceleration augments detection workflows with intelligence-led context and AI-assisted analysis. Rather than asking whether an alert is suspicious, the model focuses on decision readiness.

Key questions shift to:

- What is the scope of exposure
- How confident is the assessment
- What action is appropriate given the evidence
- Can containment be executed safely now




The Agentic SOC Platform enables this shift by unifying telemetry, threat intelligence, and AI-driven reasoning in a single operational plane.

# HOW THE AGENTIC SOC PLATFORM POWERS THIS USE CASE

## UNIFIED SECURITY DATA LAKE: COMPLETE EXPOSURE VISIBILITY

Response decisions require a complete view of activity across the environment. The Agentic SOC Platform aggregates cloud, endpoint, network, identity, email, and service telemetry into a unified data lake, preserving real-time and historical context.

Analysts can pivot across datasets to determine whether activity is isolated or widespread, enabling accurate scoping before response actions are taken.

## THREATSTREAM NEXT-GEN: CAMPAIGN-LEVEL CONTEXT

ThreatStream Next-Gen enriches events with adversary profiles, malware associations, infrastructure intelligence, and campaign context. This intelligence enables analysts to assess activity based on real-world threat behavior rather than reputation scores alone.

Campaign-level understanding provides confidence that response actions are justified and proportionate.

## AGENTIC AI: ACCELERATED INVESTIGATION AND DECISION SUPPORT

Manual correlation slows response and introduces inconsistency. Agentic AI assists analysts by reasoning across telemetry and intelligence to surface relevant relationships, prioritize investigations, and support response decisions.

AI-assisted analysis reduces time to certainty while maintaining transparency and analyst control.

## ACCELERATED INVESTIGATION AND TRIAGE

Threat-informed analytics enable analysts to:

- Identify malicious infrastructure and campaign associations
- Determine whether activity is isolated or organization-wide
- Assess related user, endpoint, and network exposure
- Move from reputation-based signals to campaign-level certainty

Investigations shift from single-event analysis to exposure-based assessment.

## BUSINESS AND SECURITY OUTCOMES

Organizations implementing threat-informed response acceleration achieve:

- Faster triage and containment
- Higher confidence response decisions
- Reduced mean time to contain
- Improved analyst efficiency and consistency

Security operations move from reactive alert handling to proactive risk mitigation.

## OPERATIONALIZING THE USE CASE

Implementation typically includes:

- Integrating security telemetry into a centralized analytics platform
- Enriching events with threat intelligence and actor context
- Applying AI-assisted investigation workflows
- Automating response actions where confidence thresholds are met

This approach complements existing SIEM, SOAR, and detection tools.

## EXPANSION AND OPTIMIZATION

As maturity increases, organizations can:

- Automate detection rules tied to threat confidence
- Trigger containment actions across integrated tools
- Monitor for recurring exposure and reinfection
- Measure response effectiveness and decision speed

Expansion is driven by improved response outcomes rather than tooling complexity.

## CONCLUSION

Effective security operations depend on fast, confident decision-making. Alert-driven workflows slow response and increase uncertainty.

By embedding threat intelligence and AI-assisted context into investigation and response workflows, the Anomali Agentic SOC Platform enables organizations to accelerate containment while improving decision quality and operational efficiency.

## SEE ANOMALI IN ACTION

Request a Demo