ANOMALI

White Paper

# AGENTIC SOC PLATFORM

Identity-Enriched EDR Triage: Improving Detection Prioritization Through Identity Context

## EXECUTIVE SUMMARY

Endpoint Detection and Response platforms produce high-fidelity technical alerts, but technical accuracy alone does not determine risk. Without identity and business context, SOC teams are forced to triage endpoint alerts as isolated events, slowing response and increasing inconsistency.

This whitepaper presents an identity-enriched EDR triage model powered by the Anomali Agentic SOC Platform. By correlating endpoint detections with identity behavior, privilege context, and threat intelligence, the platform transforms EDR alerts into decision-ready signals. The result is faster prioritization, more consistent response, and a direct alignment between SOC activity and business risk.

## THE LIMITS OF EDR-ONLY TRIAGE

EDR tools are designed to answer technical questions with precision:

- What process executed
- What binary or command was involved
- What behavior occurred on the endpoint

These insights are necessary, but insufficient. In isolation, EDR alerts do not answer the questions that determine response urgency:

- Who was behind the activity
- What level of access did that identity possess
- Whether the behavior aligns with known adversary tactics

Without identity context, SOC teams must manually pivot across IAM, directory services, and intelligence tools to assess impact. This slows investigations and increases the likelihood of mis-prioritization.

## OPERATIONAL IMPACT OF MISSING IDENTITY CONTEXT

### SECURITY OPERATIONS IMPACT

When endpoint alerts lack identity context, SOC teams experience:

- High alert volumes with limited prioritization signals
- Manual enrichment that extends investigation timelines
- Inconsistent response decisions across analysts and shifts

## BUSINESS IMPACT

These operational gaps translate directly into business risk:

- Delayed containment of high-impact incidents
- Over-response to low-risk endpoint behavior
- Increased operational cost without proportional risk reduction

Over time, technically accurate alerts become operational noise.

# IDENTITY-ENRICHED EDR TRIAGE: DEFINING THE USE CASE

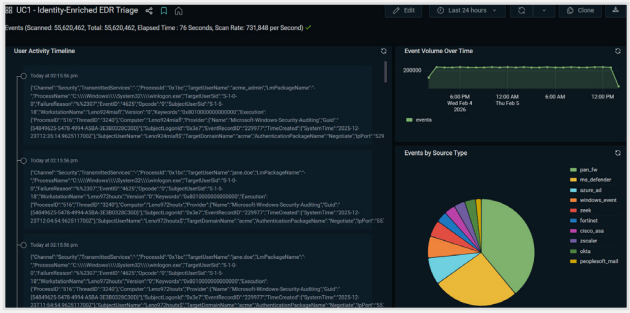
Identity-enriched EDR triage evaluates endpoint detections through the lens of identity-driven risk. Rather than treating endpoint alerts as standalone events, this model correlates each detection with the identity behind it, the privileges involved, and relevant threat intelligence.

EDR remains the detection engine. Identity provides the decision context.

The Agentic SOC Platform enables this model by unifying endpoint telemetry, identity data, and threat intelligence into a single investigation workflow, allowing analysts to prioritize alerts based on business impact rather than technical severity alone.

# HOW THE AGENTIC SOC PLATFORM POWERS THIS USE CASE

## UNIFIED SECURITY DATA LAKE: CORRELATING ENDPOINT AND IDENTITY TELEMETRY




The foundation of identity-enriched triage is complete, correlated data. The Agentic SOC Platform's unified security data lake ingests endpoint telemetry alongside identity, authentication, and access data. This enables analysts to immediately associate endpoint behavior with the user, service account, or device-bound identity responsible.

Historical telemetry remains searchable, allowing teams to evaluate whether endpoint behavior represents a deviation from established identity patterns.

## THREATSTREAM NEXT-GEN: INTELLIGENCE-DRIVEN RISK CONTEXT

Not all endpoint alerts represent real threat activity. ThreatStream Next-Gen continuously enriches endpoint detections with adversary, infrastructure, and campaign context. This intelligence helps distinguish benign anomalies from activity associated with known attacker behaviors.

By embedding intelligence directly into triage workflows, the platform suppresses low-risk noise and elevates alerts that align with active threat campaigns.

## AGENTIC AI: FASTER, MORE CONSISTENT TRIAGE DECISIONS

Manual correlation across endpoint, identity, and intelligence sources slows investigations and introduces inconsistency. Agentic AI reasons across unified telemetry and intelligence to assist analysts during triage.

AI-assisted investigations surface relevant identity attributes, privilege levels, and behavioral anomalies, helping analysts reach confident decisions faster. Explainable reasoning ensures trust while supporting consistent prioritization across the SOC.

# DECISION IMPROVEMENTS ENABLED BY IDENTITY-ENRICHED TRIAGE

## RISK-ALIGNED ALERT PRIORITIZATION

Endpoint alerts are evaluated based on who acted, what access was involved, and how that behavior aligns with known threats.

**Outcome:** High-risk alerts rise to the top of the queue.

### REDUCED INVESTIGATION TIME

Automated enrichment eliminates manual pivots across identity and intelligence systems.

**Outcome:** Faster time to decision and reduced analyst workload.

### CONSISTENT RESPONSE ACTIONS

Shared context and AI-assisted reasoning reduce subjective decision-making.

**Outcome:** More predictable, defensible response outcomes.

## BUSINESS AND SECURITY OUTCOMES

Organizations adopting identity-enriched EDR triage achieve:

- Faster prioritization of materially risky alerts
- Reduced mean time to decision during investigations
- Improved SOC efficiency without sacrificing accuracy
- Clearer alignment between technical detections and business risk

Security teams spend less time sorting alerts and more time mitigating real threats.

## OPERATIONALIZING THE USE CASE

This model integrates into existing SOC environments without replacing EDR platforms. Initial implementation focuses on:

- Correlating EDR alerts with user and service identities
- Enriching detections with privilege and entitlement data
- Applying threat intelligence for contextual risk evaluation

Value is realized quickly and expanded incrementally as additional identity and telemetry sources are integrated.

## EXPANSION AND MATURITY

As organizations mature this use case, additional context strengthens prioritization:

- IAM and PAM telemetry
- SaaS and cloud access logs
- Historical identity behavior baselines

Expansion is guided by measurable improvements in triage speed, consistency, and decision quality.

## CONCLUSION

EDR platforms are essential detection engines, but detection alone does not determine risk. Without identity context, SOC teams are forced to guess which alerts matter most.

By enriching endpoint detections with identity behavior, privilege context, and threat intelligence, the Agentic SOC Platform transforms EDR alerts into decision-ready signals. The result is faster prioritization, more consistent response, and security operations aligned to real business impact.