ANOMALI

White Paper

AGENTIC SOC PLATFORM

Log Source Analytics and False-Positive Suppression: Reducing Alert Noise and SIEM Cost Through Intelligence-Led Prioritization

EXECUTIVE SUMMARY

Security information and event management platforms ingest massive volumes of telemetry, yet only a small percentage of logged events represent material security risk. Most alerts generated are low-value, poorly contextualized, or operationally irrelevant, leading to analyst fatigue, inefficient investigations, and rapidly escalating SIEM ingestion and storage costs.

This white paper presents a log source analytics and false-positive suppression model powered by the Agentic SOC Platform. By correlating threat intelligence with asset criticality, identity, and telemetry at ingestion and alerting time, the platform enables intelligence-led prioritization. The result is fewer false positives, lower SIEM cost, and analyst effort focused on activity that presents genuine business risk.

THE CHALLENGE OF HIGH-VOLUME, LOW-SIGNAL LOGGING

Modern security environments generate telemetry across nearly every layer of infrastructure, including:

- Network and perimeter systems
- Endpoint and application platforms
- Identity and access services
- Cloud and SaaS environments

While comprehensive logging improves visibility, it also introduces structural challenges. Excessive event volume overwhelms detection logic, indicator matches lack context, and SIEM licensing and storage costs grow without proportional security benefit.

Without intelligence-driven prioritization, security teams spend more time managing data pipelines and alerts than reducing risk.

OPERATIONAL AND BUSINESS IMPACT OF ALERT NOISE

SECURITY OPERATIONS IMPACT

When alert volume outpaces context, SOC teams experience:

- Large volumes of low-value alerts requiring manual triage
- Reactive threat hunting driven by noise rather than intelligence
- High-confidence threats competing with background telemetry

BUSINESS IMPACT

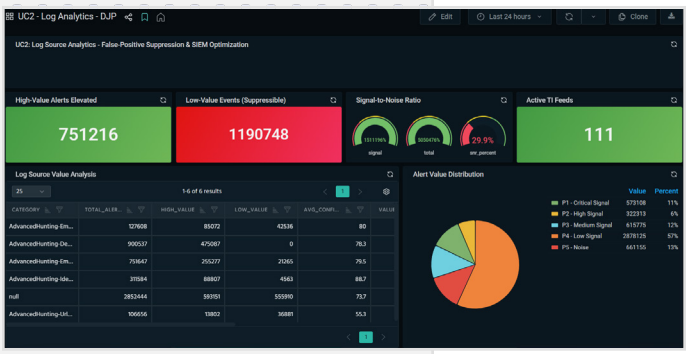
These operational inefficiencies translate into measurable business consequences:

- Rising SIEM ingestion, retention, and storage costs
- Delayed detection of threats affecting critical systems
- Difficulty demonstrating return on security investment

In this environment, more data increases complexity without improving outcomes.

LOG SOURCE ANALYTICS AND SUPPRESSION: DEFINING THE USE CASE

Log source analytics and false-positive suppression applies intelligence and asset context before alerts reach analysts. Rather than treating all telemetry equally, this use case evaluates events based on threat confidence, business criticality, and campaign relevance.



The Agentic SOC Platform enables this model by unifying log telemetry, asset inventories, identity context, and threat intelligence into a single operational plane. Alerts are generated only when evidence indicates meaningful risk, while low-value activity is automatically suppressed or deprioritized.

This shifts detection from volume-driven alerting to relevance-driven decisioning.

HOW THE AGENTIC SOC PLATFORM POWERS THIS USE CASE

UNIFIED SECURITY DATA LAKE: CORRELATING LOGS WITH BUSINESS CONTEXT

Effective suppression requires complete visibility across log sources. The Agentic SOC Platform's unified security data lake ingests network, endpoint, identity, and application telemetry at scale, preserving both real-time and historical access.

Asset inventories and criticality classifications are applied directly to log data, allowing events to be evaluated based on business impact rather than raw frequency.

THREATSTREAM NEXT-GEN: INTELLIGENCE-LED ALERT RELEVANCE

ThreatStream Next-Gen enriches log events with high-confidence indicators, adversary associations, and campaign context. This intelligence determines whether observed activity reflects active threat behavior or benign background noise.

By applying intelligence at ingestion and alerting time, the platform suppresses low-confidence matches and elevates activity tied to real-world threats.

AGENTIC AI: CONSISTENT SUPPRESSION AND PRIORITIZATION

Manual tuning of suppression rules is time-consuming and inconsistent. Agentic AI reasons across telemetry, asset context, and intelligence to assist in suppression decisions and alert prioritization.

AI-assisted analysis ensures consistent application of thresholds, adapts to changing threat pressure, and provides explainable logic for why events are promoted or suppressed.

DETECTION IMPROVEMENTS ENABLED BY THIS USE CASE

REDUCED FALSE POSITIVES

Low-confidence indicators and low-impact assets are automatically deprioritized.

Outcome: Fewer alerts reach analysts.

ASSET-AWARE ALERTING

Events affecting critical assets are surfaced immediately, even at lower volumes.

Outcome: Faster identification of high-impact threats.

COST-CONTROLLED LOGGING

Suppression reduces ingestion, retention, and storage demands without sacrificing visibility.

Outcome: Lower SIEM operating costs.

BUSINESS AND SECURITY OUTCOMES

Organizations implementing intelligence-led log analytics achieve:

- Significant reductions in false-positive alert volume
- Lower SIEM ingestion and storage costs
- Faster detection of threats affecting critical assets
- Improved analyst efficiency and decision quality

Detection relevance improves as operational cost declines.

OPERATIONALIZING THE USE CASE

This model integrates with existing SIEM and log pipelines. Initial implementation typically includes:

- Importing asset inventories and criticality classifications
- Defining alert rules tied to asset and intelligence thresholds
- Correlating log events with threat confidence and campaign data
- Visualizing outcomes through dedicated dashboards

Value is realized quickly through reduced noise and measurable cost savings.

EXPANSION AND OPTIMIZATION

As organizations v this capability, they can:

- Tune suppression thresholds based on campaign pressure
- Expand asset tagging and business impact modeling
- Automate intelligence-driven threat hunting rules
- Track cost reduction and detection efficiency over time

Expansion is justified by ongoing reductions in noise and operational expense.

CONCLUSION

High log volume does not equate to high security value. Without intelligence-led prioritization, alert noise overwhelms analysts and drives unnecessary cost.

By applying threat intelligence, asset context, and AI-assisted analytics to log telemetry, the Agentic SOC Platform enables organizations to suppress false positives, control SIEM costs, and focus security operations on threats that matter most to the business.