ANOMALI

White Paper

AGENTIC SOC PLATFORM

Retrospective Analysis and Incident Response Scoping: Extending Threat Hunting and IR Beyond SIEM Retention Limits

EXECUTIVE SUMMARY

Most organizations retain only 60 to 90 days of searchable security data within their SIEM environments. While this window supports immediate incident response, it limits the ability to investigate long-lived vulnerabilities, low-and-slow attacker activity, and historical exposure when new threat intelligence emerges.

This whitepaper presents a retrospective analysis and incident response scoping model powered by the Anomali Agentic SOC Platform. By combining long-term, searchable telemetry with vulnerability intelligence, asset context, and AI-assisted analytics, the platform enables analysts to investigate historical activity with confidence. Security teams can scope impact accurately, prioritize remediation, and operationalize findings into repeatable detection and response workflows.

THE RETROSPECTIVE VISIBILITY GAP

Threat intelligence updates and vulnerability disclosures frequently raise retrospective questions:

- Were we exposed before this vulnerability became widely known
- Did exploitation begin months or years earlier
- Which assets and business services were most affected over time

Traditional SIEM architectures archive older data to cold storage, making retrospective investigations slow, incomplete, or impractical. Analysts are often forced to rely on assumptions rather than evidence when responding to leadership, auditors, or regulators.

BUSINESS AND OPERATIONAL IMPACT OF LIMITED RETENTION

SECURITY OPERATIONS IMPACT

When historical telemetry is unavailable or difficult to access, SOC teams face:

- Inability to detect low-and-slow attacker activity
- Reduced confidence in historical exposure assessments
- Manual, time-consuming incident response scoping

BUSINESS IMPACT

These limitations have direct consequences:

- Delayed remediation and containment decisions
- Increased residual risk from unaddressed vulnerabilities
- Reduced confidence in security posture reporting

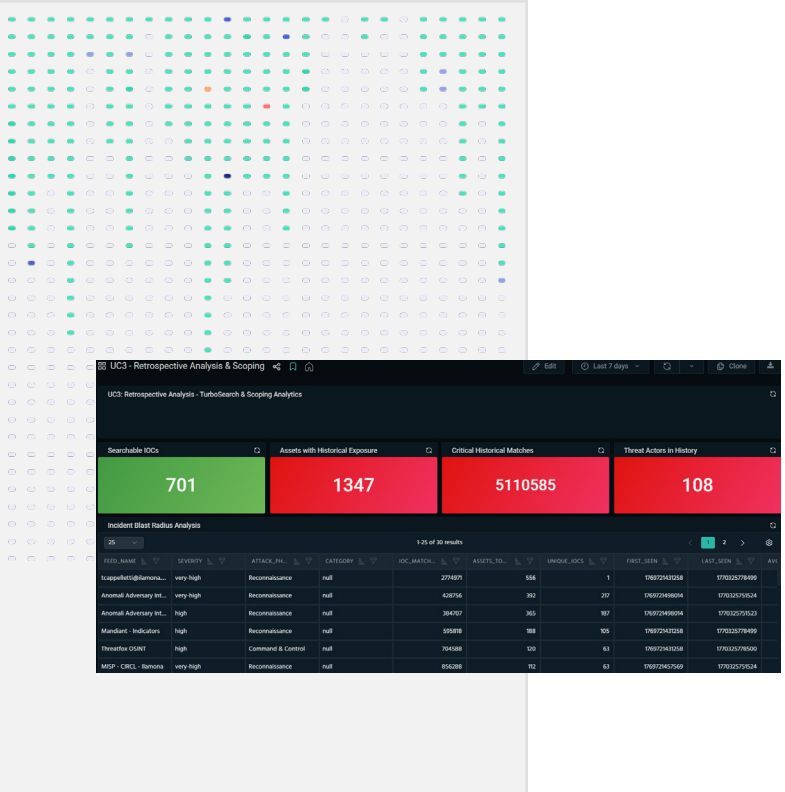
Without long-term searchable data, retrospective analysis becomes speculative rather than evidence-based.

RETROSPECTIVE ANALYSIS AND IR SCOPING: DEFINING THE USE CASE

This use case enables structured, intelligence-driven historical analysis across extended time horizons. Rather than treating retrospective investigations as ad hoc exercises, the model applies consistent analytics to identify aging exposure, scope related activity, and operationalize findings.

The Agentic SOC Platform supports this approach by unifying long-term telemetry, vulnerability intelligence, asset context, and AI-assisted analytics in a single operational plane. Analysts can pivot seamlessly across years of data to answer the questions that matter most.

HOW THE AGENTIC SOC PLATFORM POWERS THIS USE CASE



UNIFIED SECURITY DATA LAKE: LONG-TERM, SEARCHABLE TELEMETRY

The foundation of retrospective analysis is accessible history. The Agentic SOC Platform's unified security data lake retains one to multiple years of security telemetry in a searchable state, without performance degradation.

Network, endpoint, identity, and application data remain correlated and available, enabling analysts to reconstruct activity timelines and investigate historical exposure with precision.

THREATSTREAM NEXT-GEN: VULNERABILITY AND CAMPAIGN CONTEXT

ThreatStream Next-Gen enriches historical telemetry with vulnerability intelligence, exploitability data, and campaign context. CVE severity, exploitation status, and adversary associations provide critical prioritization signals during retrospective investigations.

This intelligence allows teams to focus on vulnerabilities and assets most likely to have been exploited, rather than attempting to analyze all historical exposure equally.

AGENTIC AI: ACCELERATED HISTORICAL INVESTIGATION

Manually querying years of data is slow and error-prone. Agentic AI assists analysts by converting natural-language questions into structured queries, surfacing relevant correlations, and guiding pivots across datasets.

AI-assisted analytics reduce the time required to scope historical impact while maintaining transparency and analyst control over conclusions.

INVESTIGATION WORKFLOW ENABLED BY THE PLATFORM

PHASE 1: IDENTIFY PERSISTENT EXPOSURE

Analysts query for active vulnerabilities exceeding defined age thresholds and identify assets or internal IPs with the highest cumulative exposure.

Outcome: Clear prioritization of long-lived risk.

PHASE 2: SCOPE RELATED ACTIVITY

From prioritized assets, analysts pivot to historical network, endpoint, identity, and application activity to determine whether exposure represents isolated events or sustained compromise.

Outcome: Evidence-based incident scoping.

PHASE 3: OPERATIONALIZE FINDINGS

Investigations are saved as reusable searches, alerts are scheduled for ongoing monitoring, and dashboards track remediation progress over time.

Outcome: Retrospective insights become ongoing controls.

BUSINESS AND SECURITY OUTCOMES

Organizations implementing this model achieve:

- Retrospective visibility beyond standard SIEM retention windows
- Faster and more accurate incident response scoping
- Clear prioritization of remediation efforts
- Measurable reduction in long-lived exposure

Historical analysis becomes a proactive control rather than a forensic afterthought.

OPERATIONALIZING THE USE CASE

Implementation typically includes:

- Long-term retention of searchable security telemetry
- Ingested vulnerability and asset context
- Threat intelligence enrichment for CVEs and campaigns
- Analyst workflows leveraging AI-assisted and natural-language search

This approach integrates with existing SOC, IR, and vulnerability management processes.

CONCLUSION

Understanding historical exposure is essential for managing real security risk. Without long-term searchable data, organizations are forced to speculate about impact and exposure.

By enabling retrospective analysis and structured IR scoping across extended timelines, the Anomali Agentic SOC Platform allows security teams to move from reactive investigation to continuous exposure management. The result is faster, more confident decisions grounded in evidence rather than assumptions.

SEE ANOMALI IN ACTION

Request a Demo