ANOMALI

White Paper

AGENTIC SOC PLATFORM

Proactive Early-Warning Threat Detection: Disrupting Attacks Before Execution Through Predictive Threat Intelligence

EXECUTIVE SUMMARY

Most security programs remain reactive, blocking malicious infrastructure only after it has been observed in active campaigns. By the time domains or IP addresses are confirmed as malicious, attackers have often already established command-and-control, delivered malware, or initiated credential theft.

This white paper presents a proactive early-warning threat detection model powered by the Anomali Agentic SOC Platform. By applying predictive threat intelligence to DNS, network flow, and endpoint connection telemetry, the platform identifies emerging malicious infrastructure before execution occurs. Organizations can disrupt attacks earlier, reduce initial compromise rates, and decrease downstream incident response effort.

THE LIMITS OF REACTIVE INFRASTRUCTURE DEFENSE

Traditional infrastructure defense approaches rely on:

- Static blocklists
- Reputation-based domain and IP controls
- Post-compromise detection of command-and-control traffic

These techniques struggle against modern attacker behaviors, including rapidly changing infrastructure, short-lived domains, domain generation algorithms, and low-signal early-stage communications. As a result, early attacker activity frequently goes undetected or produces excessive alert noise with limited actionability.

BUSINESS AND OPERATIONAL IMPACT

SECURITY OPERATIONS IMPACT

Reactive infrastructure defense leads to:

- High volumes of DNS alerts with limited context
- Missed early-stage command-and-control communications
- Detection occurring only after malware execution or phishing success

BUSINESS IMPACT

These gaps translate into measurable risk:

- Higher initial compromise rates
- Increased downstream incident handling and investigation
- Elevated remediation cost and operational disruption

When controls engage too late, attackers gain footholds before defenses respond.

PROACTIVE EARLY-WARNING DETECTION: DEFINING THE USE CASE

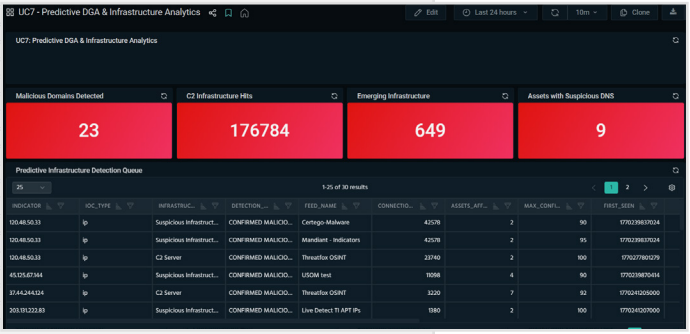
Proactive early-warning detection shifts infrastructure defense from reputation-based blocking to predictive prevention. Rather than waiting for infrastructure to be confirmed malicious, this model identifies suspicious domains and communication patterns as they emerge.

The Agentic SOC Platform enables this approach by unifying predictive threat intelligence with DNS, network, and endpoint telemetry. Early-stage signals are evaluated for likelihood of malicious use, allowing controls to be applied before attacks fully materialize.

HOW THE AGENTIC SOC PLATFORM POWERS THIS USE CASE

UNIFIED SECURITY DATA LAKE: EARLY-STAGE VISIBILITY

Effective early-warning detection requires visibility into infrastructure interactions as they occur. The Agentic SOC Platform aggregates DNS queries, network flow metadata, and endpoint connection telemetry into a unified data lake.



This allows analysts and automated controls to observe newly contacted infrastructure, identify anomalous patterns, and evaluate risk before execution stages are reached.

THREATSTREAM NEXT-GEN: PREDICTIVE INFRASTRUCTURE INTELLIGENCE

ThreatStream Next-Gen provides predictive intelligence derived from domain generation analysis, infrastructure pattern recognition, and emerging campaign indicators. Newly registered or previously unseen domains are scored based on characteristics associated with malicious use.

This intelligence enables organizations to move beyond static reputation lists and respond to attacker infrastructure as it is created.

AGENTIC AI: SCORING AND DECISION SUPPORT

Evaluating early-stage signals requires balancing prevention with precision. Agentic AI assists by correlating predictive intelligence with observed telemetry, scoring risk, and supporting consistent enforcement decisions.

AI-assisted analysis helps reduce false positives while ensuring that high-risk infrastructure is disrupted early.

EARLY-STAGE DETECTION AND DISRUPTION

Using predictive, intelligence-led analytics, organizations can:

- Score new and unknown domains at first contact
- Identify suspicious infrastructure patterns associated with pre-execution activity
- Flag early-stage communications consistent with emerging attacks
- Enforce controls before payload delivery or credential theft

This shifts defense from response to prevention.

BUSINESS AND SECURITY OUTCOMES

Organizations implementing proactive early-warning detection achieve:

- Lower initial compromise rates
- Reduced phishing and malware incidents
- Decreased SOC alert volume
- Stronger preventive security posture

Mean time to respond shifts toward pre-incident disruption rather than post-incident containment.

OPERATIONALIZING THE USE CASE

Implementation typically includes:

- Applying predictive scoring and pattern analysis to newly observed domains
- Enforcing DNS-level controls in near real time
- Automating blocklist propagation across enforcement points
- Continuously tuning thresholds to balance early detection and false positives

This approach integrates into existing network and endpoint security workflows.

CONCLUSION

Early-stage attacker activity presents the greatest opportunity for disruption. Reactive controls engage too late to prevent compromise.

By combining predictive threat intelligence with real-time infrastructure telemetry, the Anomali Agentic SOC Platform enables organizations to detect and disrupt attacks before execution. The result is reduced risk, simplified SOC operations, and a shift from reactive defense to proactive prevention.

SEE ANOMALI IN ACTION

Request a Demo

© Copyright 2026 Anomali Incorporated®. All rights reserved. ThreatStream® is a registered trademark of Anomali Inc.
vAnomali Match™ (“Match”), Anomali Lens™ (“Lens”), and Anomali Copilot are trademarks of Anomali Inc.