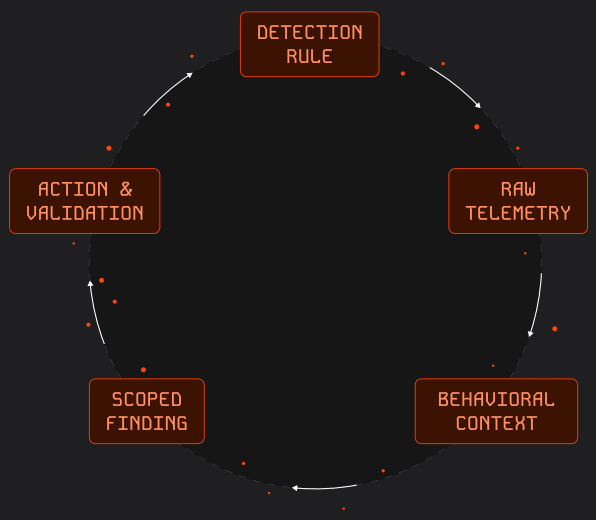
nebulock

AUTONOMOUS THREAT HUNTING

Nebulock finds false negatives across your EDR, IAM, cloud, network, and SaaS environments. By providing proactive findings, Nebulock reduces dwell time and delivers actionable inputs to SOC and SOAR workflows.

PROACTIVE, CONTEXTUAL COVERAGE ACROSS YOUR SECURITY STACK

Nebulock identifies significant behaviors that might evade current controls, providing clear, actionable insights for teams. It transforms successful investigations into repeatable detection methods and ensures improvements that last beyond an initial search. The goal is closing the loop, not more signals.



AGENTIC HUNTING

Continuous hunting across your infrastructure built for scale

Run simultaneous hunts driven by threat intelligence, hypotheses, or ad hoc investigations. Always-on hunting is event-triggered and executed by AI agents.

MEMORY

Behavioral knowledge base

Unify your data, intelligence, context, and past hunts in the platform to inform future hunts, so you never have to start from zero. Each hunt makes the next hunt better.

FINDINGS

Outcomes, not alerts

See full agent reasoning with the ability to deliver findings to your existing workflows and deploy durable detection rules for contextual coverage.

SECURITY TEAMS USE NEBULOCK TO:

DETECT INSIDER THREATS

Privileged users or AI agents with valid credentials move laterally undetected, but Nebulock agents baseline normal behavior and flag deviations in real time.

REDUCE FALSE POSITIVES

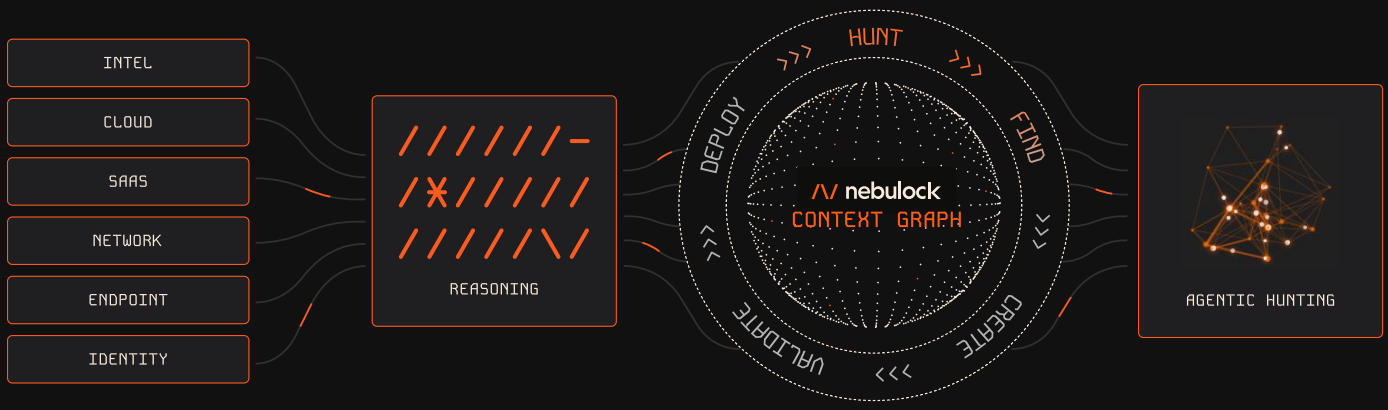
Teams spend the majority of their time chasing non-threats, while missing real ones. Continuous feedback loops cut the noise of false positives.

PREVENT DETECTION DRIFT

Custom detection rules grow stale over time. Continuous learning and evaluation by AI agents refines rules automatically.

HOW IT WORKS

Nebulock ingests raw telemetry via API from your security stack. This telemetry is distilled to surface actionable insights, enabling security teams to respond to threats faster and more effectively. Findings are shared in real time via Slack, Teams, and the Nebulock platform.



KEY INTEGRATION METHODS

01 EDR	02 IDENTITY	03 THREAT INTELLIGENCE	04 WORKFLOWS
Ingest endpoint telemetry via API from Crowdstrike, SentinelOne, Microsoft Defender, and others.	Support for Okta, Duo, and Entra ID with more options coming soon.	Leverage third party feeds or your own intelligence into hunts.	Send findings and actions to your existing SOC, SOAR, and ChatOps workflows via API.

ENDPOINT AND IDENTITY DETECTION COVERAGE

Endpoint Telemetry Collection

- Process creation and execution monitoring
- Network connection tracking
- File system activity monitoring
- Authentication and authorization event tracking
- Kernel and system integrity monitoring

Advanced Behavioral Analysis

- Detection of living-off-the-land binaries (LOLBins)
- Suspicious scripting activity (PowerShell, osascript, AppleScript)
- System preference modifications
- Unauthorized screen and camera access
- Suspicious terminal and shell activity

macOS-Specific Threat Detection

- Malware families and variants
- Suspicious LaunchAgent and Launch Daemon activity
- Unauthorized Gatekeeper bypasses
- Suspicious kernel extensions
- Privilege escalation techniques
- Keychain access anomalies

Identity and Insider Threat Detection

- Privilege escalation attempts
- Credential abuse and brute force activity
- Anomalous login activity
- Malicious insider behaviors (unexpected access or exfiltration)

Trusted by: BainCapital Cribl HEALTHEDGE Shutterfly alrSlate

STOP CHASING ALERTS. START PROACTIVELY HUNTING. VISIT NEBULOCK.IO