

BlinkOps Agentic Threat Hunting

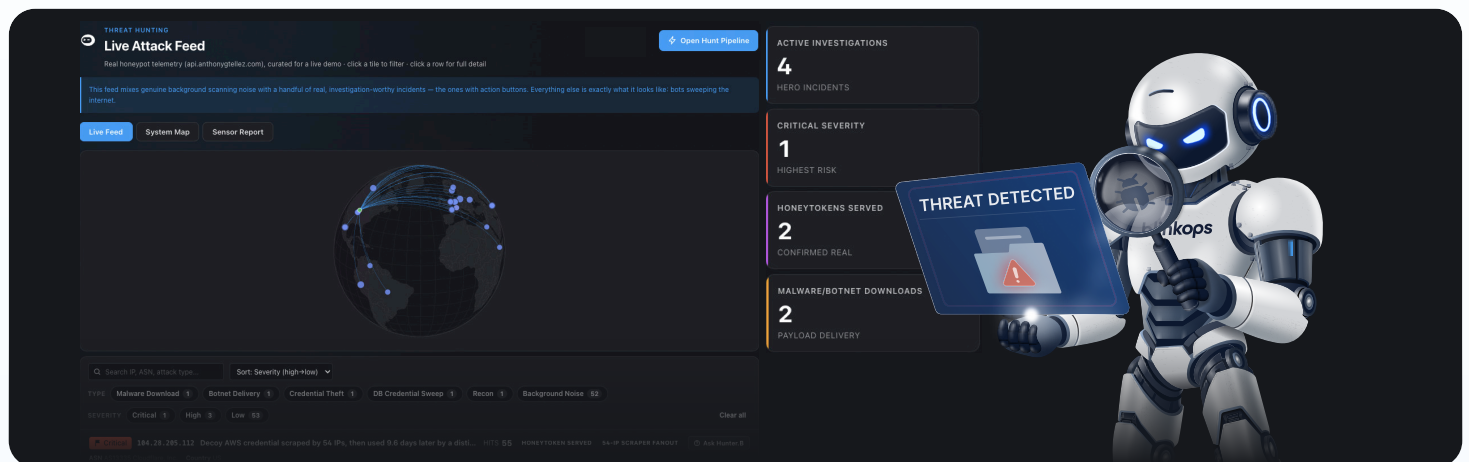
Continuously hunt for the behavior your detection rules miss

Current State

Detection rules catch behavior teams already know, but threats increasingly operate outside that coverage. Hunting for what rules miss requires senior analysts to interpret intelligence, form hypotheses, translate them into platform-specific queries, analyze results, pivot across entities, and document the outcome. That work is difficult to scale, so only a small portion of the technique surface is examined and most hunts run occasionally instead of continuously.

Blink Solution

With BlinkOps, you can deploy agentic operators that turn intelligence and observed techniques into testable hypotheses, run platform-native queries across your SIEM, EDR, and data lake, score the results, and investigate the leads. Deterministic workflows manage collection, scheduling, query execution, enrichment, and cases; AI reasons over intelligence, patterns, and investigative pivots. Analysts receive confirmed, scoped leads instead of raw results, and every hunt remains logged, repeatable, and auditable.



Threat Hunting Solutions that our customers run

Hypothesis Operator

Transforms threat intelligence and observed TTPs into scoped, testable hypotheses mapped to MITRE ATT&CK and prioritized for your environment. Each hunt starts with a clear behavioral question rather than a generic search.

Query Operator

Translates each hypothesis into the native query language and schema of the target SIEM, EDR, or data platform. It scopes fields, indexes, and time ranges around the platform's cost model so continuous hunting does not consume the search budget.

Detection Engineering Operator

Turns successful threat hunts into production-ready detections. It translates validated behavior into platform-native rules, maps them to MITRE ATT&CK, tests them against historical data, tunes thresholds to reduce noise, and routes them through your existing approval and deployment process.

Pivot Operator

Expands validated leads across related identities, endpoints, processes, and activity to build the full timeline. It opens a case, preserves every query and result, and can draft a new detection so each confirmed hunt strengthens future coverage.

Why Choose Blink

Work with top-tier security engineers

Blink's Forward Deployed Security Engineers have experience building and running threat-hunting and detection processes across complex environments. They help turn your intelligence, hypotheses, and investigative methods into repeatable solutions that strengthen security operations over time.

Agentify the entire security stack

With more than 30,000 integrations, Blink can gather intelligence and telemetry from your SIEM, EDR, data lake, threat-intelligence platforms, identity systems, and cloud environment. When a hunt finds malicious activity, Blink can create an incident and initiate response. When it reveals a coverage gap, Blink can create a new detection or improve an existing one.

Get to value fast

Start with pre-built solutions for hypothesis generation, platform-native querying, investigation, incident creation, and detection improvement. Adapt them using Workflow Studio, Agent Studio, Solution Studio, and Case Management to reflect your data sources, query languages, threat models, approval processes, and detection standards.

Customer Proof

HUMAN Security

Investigating threat intelligence across CrowdStrike, Sumo Logic, Wiz, and other tools could consume hours of an analyst's time. HUMAN built a Threat Hunting Bot that extracts indicators from security research, hunts across the environment, and returns a complete report in under 10 minutes. Across 123 investigations, only 11 required additional human analysis, and two uncovered findings that required patching—giving analysts the evidence needed to focus on what mattered.

About BlinkOps

With BlinkOps, security teams gain an operating layer that spans their entire security stack. From AI SOC, to vulnerability management, GRC, and IAM, Blink automates workflows from triage to remediation. One Agentic Security Operations Platform, infinite possibilities.