HUNTERS

DATA SHEET

HUNTERS SOC PLATFORM

Move Beyond SIEM: Reduce Risk, Complexity, and Cost for the SOC

SIEM IS OBSOLETE

→ Data volumes and cost are unmanageable, leading to poor security outcomes

→ Analysts are still drowning in false positives and noisy alerts

→ Security teams need to play catch up with detection rule-writing

→ Incident investigation and triage processes are lengthy and cumbersome

Eliminate the pain of the SOC: Solve the Data, Detection, Investigation & Response challenges

Hunters SOC Platform is a SIEM alternative, delivering data ingestion, built-in and always up-to-date threat detection, and automating correlation and investigation processes to reduce risk, complexity, and cost for security teams.

Solve the challenges around data scale, cost and reliance on data engineers

Unlimited data ingestion, retention and normalization at a predictable cost

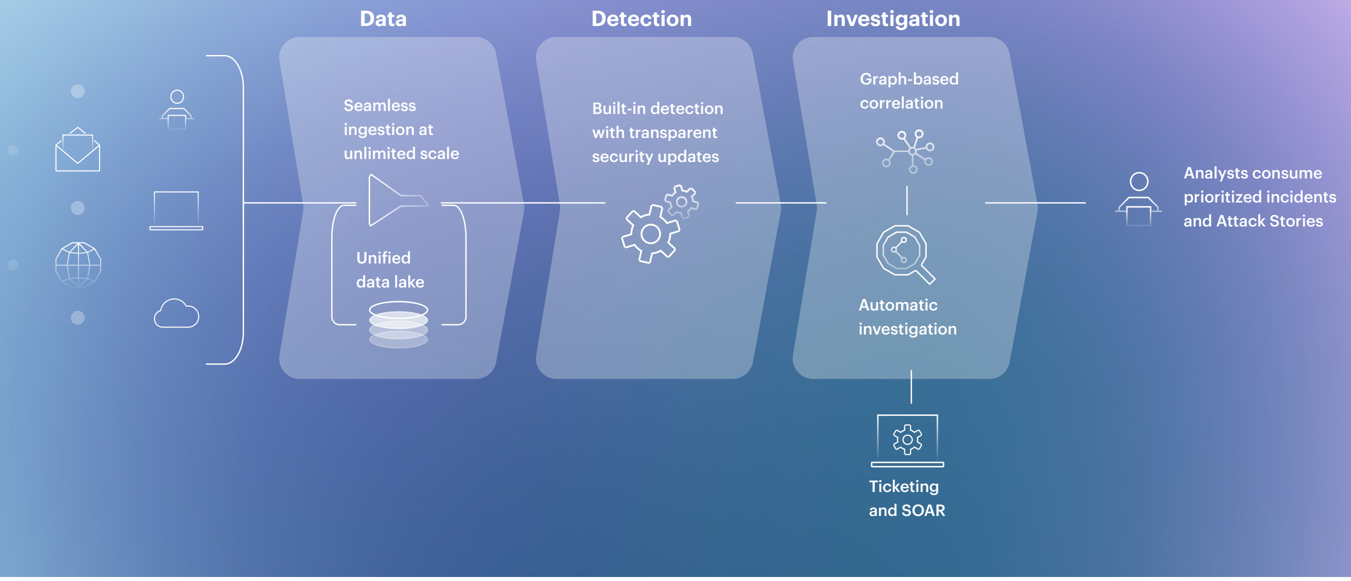
Increase threat coverage while minimizing reliance on rule-writing

Built-in, always up-to-date detection

Significantly reduce time to containment and remediation

Automating cross-correlation, triage and investigation

HUNTERS SOC PLATFORM WORKFLOW



Data

Seamless ingestion at unlimited scale

Unified data lake

Detection

Built-in detection with transparent security updates

Investigation

Graph-based correlation

Automatic investigation

Ticketing and SOAR

Analysts consume prioritized incidents and Attack Stories

HOW IT WORKS

Unlimited Ingestion

Hunters SOC Platform ingests, normalizes and retains data from dozens of security and IT tools, scaling to any size of environment. Customers can opt for a "bring-your-own data lake" deployment model, or leverage Hunters' embedded one. Hunters ETL (Extract, Transform & Load) and schema mapping capabilities eliminate the need to engineer, deploy and maintain ingestion pipelines.

Built-in, always up-to-date Detection

Hunters delivers up-to-date detections which are pre-verified on real-world customer data to remove any false positives and excessive alerting, then deployed directly to all customer tenants without requiring any action or tweaking. This dramatically reduces risk exposure while reducing operational overhead. The threat coverage of the organization is automatically mapped onto the MITRE ATT&CK framework.

Automatic Investigation

Every alert is automatically enriched with information from various sources (e.g., user name from CrowdStrike with login records from Okta, IP addresses with threat intel information) and displayed to the analyst for faster triage and investigation, as well as advanced detection and scoring purposes. The platform also clusters alerts using proprietary "threat similarity" logic, reducing redundant work for up to 90% of alerts that may happen across days and weeks.

Graph Correlation

Alerts across entities and attack surfaces are automatically correlated on a graph, and are packaged as 'Attack Stories', giving a contextual view of the full incident. This capability highlights high-fidelity activity, improves investigation time, and allows leveraging low-fidelity signals that are often overlooked.

Dynamic Scoring and Prioritization

The platform continuously examines the risk level of each alert, assigning both a risk and confidence score, so analysts can prioritize the most critical to the business. For instance, alerts involving sensitive assets (e.g., c-level, domain servers, etc.) are prioritized, and risk for known benign behaviors is lowered (e.g., a binary signed by Microsoft.)

IOC Search

For regulatory purposes and ad-hoc investigations, Hunters also delivers an IOC search bar to allow anyone in the SOC to search for IOCs and get results from raw data within seconds without needing to write an SQL query.

TEAM

AXON

Hunters' team of cybersecurity experts: Their mission is to help your security team protect your organization, through prompt and reliable cybersecurity expertise. Their services include proactive threat hunting, expert investigation assistance, and rapid response to emerging threats.

Integrations

Data Platform Partners: snowflake databricks

aws | CROWDSTRIKE | okta | Microsoft | CISCO | paloalto NETWORKS | proofpoint

Azure | Google Cloud | WIZ | mimecast | SentinelOne | zscaler The Cloud Security Company | Many more...

Trusted by market leaders

Booking.com | upwork | cimpress | Solaris | chargepoint | snowflake | Sika | GONG | CLUMIO

HUNTERS