HUNTERS

NEXT-GEN SIEM

Hunters SOC Platform

LEGACY SIEM IS OBSOLETE

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

The Modern SIEM Alternative

Hunters SOC Platform automates the entire threat detection, investigation, and response (TDIR) process, replacing repetitive human work with machine-powered ingestion, detection, enrichment, correlation, prioritization, triage and investigation, freeing analysts to proactively protect their organizations.

Complete and scalable data coverage, without relying on data engineers

Ingest, retain and normalize data from your entire security stack with hundreds of pre-built integrations

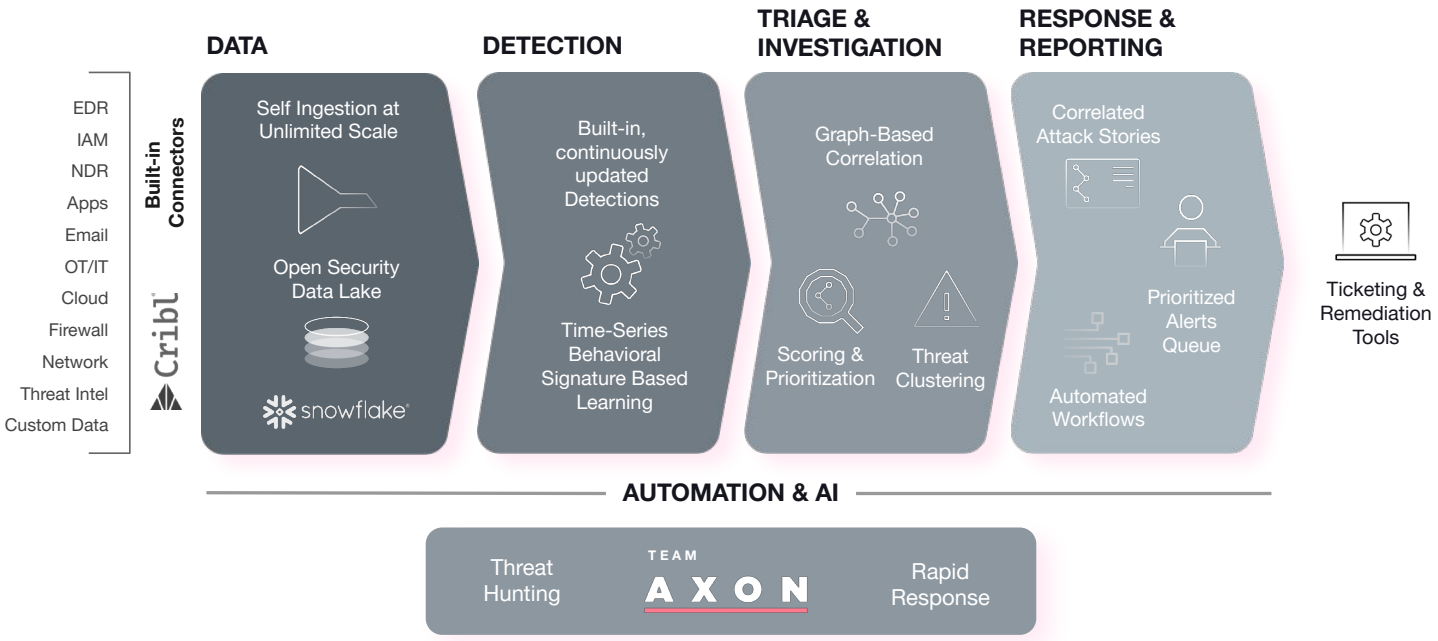
Increase threat coverage while minimizing reliance on rule-writing

Out-of-the-box detection rules mapped to the MITRE ATT&CK Framework are constantly updated and run on top of your data

Significantly reduce time to containment and remediation

Automatic, AI-powered triage, correlation and investigation

Hunters SOC Platform workflow



HOW IT WORKS

Built-in, Always Up-to-date Detections

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 and operational overhead. The threat coverage of the organization is automatically mapped to the MITRE ATT&CK framework.

Open, Scalable Security Data Lake

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.

Automated Triage and 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 is displayed to the analyst for faster triage, investigation, and 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.

Attack Stories

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 example, 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 a SQL query.

Multi-Tenancy

Manage security operations for multiple business units from a centralized platform.

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 rapid response to emerging threats, incident investigation, proactive threat hunting, and security posture and hygiene reporting.

Integrations

Data Platform Partners: snowflake, databricks

aws, CROWDSTRIKE, okta, Microsoft, CISCO, paloalto, proofpoint

Azure, Google Cloud, WIZ, mimecast, SentinelOne, zscaler, Many more...

Trusted by market leaders

Booking.com, cimpress, Solaris, chargepoint, snowflake, Sika

CLUMIO, GONG, unzer, tandem, SPOTNANA, XOXT

HUNTERS