DATASHEET

Hunters

Hunters SOC Platform

Empower security teams to automatically identify and respond to incidents that matter, helping teams mitigate real threats faster and more reliably than SIEMs.

Today, SOCs waste time with an overwhelming amount of telemetry data to correlate, tools to manage, and false positives to chase as data is siloed across SIEMs, security and IT products, enterprise data and threat intelligence. This creates a lot of heavy lifting to keep all the data, signals and alerts from across the attack surface organized and mapped.

Meanwhile, security teams are constantly updating their own playbooks to keep up with the methodologies attackers are using. To investigate behavior, security teams need to stitch everything together, a nearly impossible task with data, staffing and expanding attack surface challenges. This means security teams are challenged to separate the “noise” from real incidents, making the attack surface more vulnerable and leaving the business at risk.

The Hunters SOC platform empowers security teams to automatically identify and respond to incidents that matter across their entire attack surface, at a predictable cost. Through built-in detection engineering, data correlation, and automatic investigation, we help teams overcome volume, complexity, and false positives. Hunters mitigates real threats faster and more reliably than SIEMs, ultimately reducing customers' overall security risk.

Key SOC Platform Solutions

SIEM Replacement

Move beyond SIEM and adopt a platform approach. Streamline your security program while achieving the automation and scale needed to accelerate how you detect, investigate and respond to threats.

Security Analytics | XDR

Apply out-of-the-box security analytics with automatic investigations and scoring to spot high fidelity threat leads from siloed systems, link them together and transform them into actionable insights.

Threat Hunting

Threat hunters can implement and automate their hunting thesis with a consolidated threat hunting platform. Pick up on weak signals and hunt across your environment with full visibility and a single interface.

Key Outcomes

Cover the Entire Attack Surface

Vendor-agnostic data ingestion and normalization across all data from your security and IT tools, at a predictable cost.

Empower Security Teams

Built-in detection engineering, data correlation, and automatic investigation to overcome volume, complexity, and false positives.

Minimize Security Risk

Reduce overall security risk and compliance exposure by mitigating real threats faster and more reliably than SIEMs.

“I recommend Hunters to every CISO because they’re probably experiencing the same things as I am: they’re probably using the same tools as we are, and I recognize the challenges behind that. I know that Hunters can unify all the data generated from those tools and make sense out of it to help us in our fight with the intruders.”

Mario Duarte, *VP Security*

snowflake

How it works

Unparalleled Data Ingest

Using cloud connectors to pipe into existing security tools, or directly connecting to SIEM at unmatched speeds, Hunters SOC Platform supports unlimited ingest of logs, events and telemetry from dozens of data sources on-premises and in the cloud.

Built-in Detection

Hunters SOC Platform extracts both raw data and alerts from existing security data using a stream processing analytics technology which enables near real-time processing and complex analytics. Threat signal extraction is guided by Hunters' TTP-based detections.

Auto-Investigation

Hunters SOC Platform runs automatic investigations on behalf of security analysts, driven by graph-based correlation, pulling all related information associated with suspicious activity and enriching it with further context.

Dynamic Prioritization

Once there is enough context around threat signals and alerts, machine learning-based algorithms are used to dynamically score them, allowing for prioritization and quick triage. As more data is ingested and analyzed, insights emerge impacting scoring and prioritization.

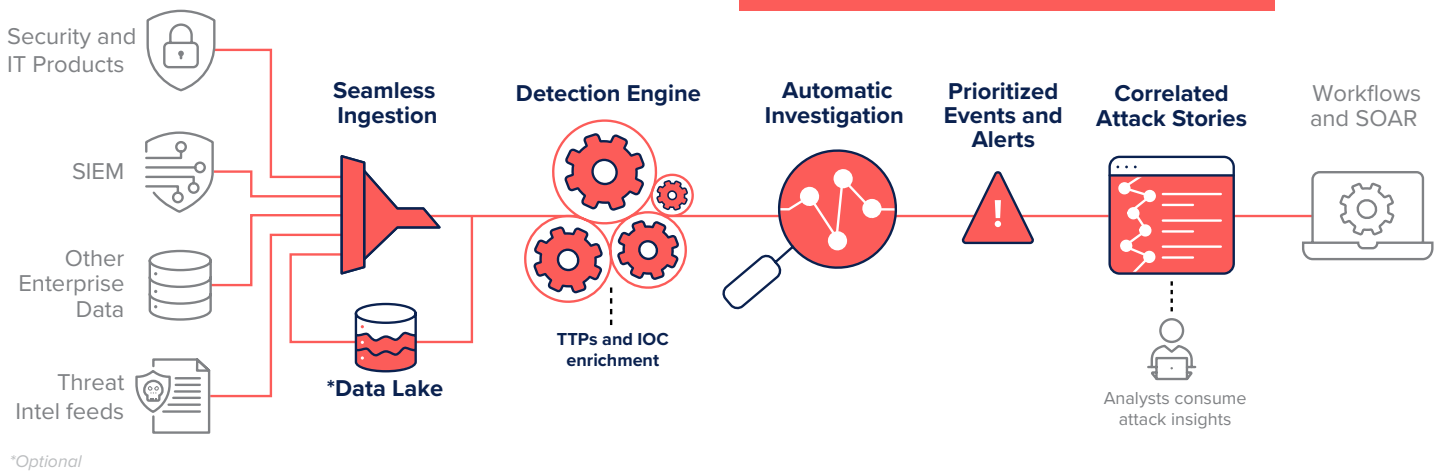
Correlated Attack Stories

Correlated signals and alerts for a given incident are automatically discovered and packaged into a contextual view of an attack story, including critical information like affected entities, users, and activities, providing analysts with a clear understanding of the attack and its impact.

Response and Remediation

With Hunters, Incident Response is accelerated as Attack Stories are streamlined into containment and remediation actions through automation, using SOAR tools and workflows to reduce the attackers' dwell time.

GET A HUNTERS SOC PLATFORM DEMO



Key Integrations

Integrations span security products, data connectors, and workflows.

Data Platform Partner: snowflake®

CROWDSTRIKE · Azure · Cisco Umbrella · Google Workspace

vmware Carbon Black · aws · paloalto NETWORKS · Office 365

Microsoft · okta · zscaler · proofpoint.

SEE ALL OF OUR INTEGRATIONS AND TECHNOLOGY PARTNERS.

Hunters

WWW.HUNTERS.AI