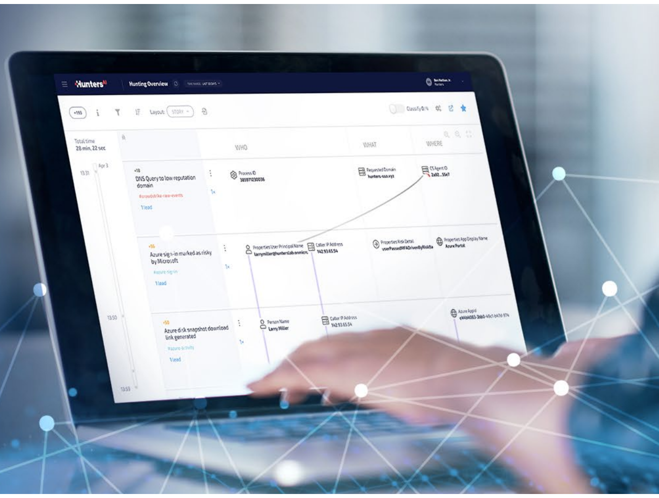
Hunters

WWW.HUNTERS.AI

Hunters XDR

DATASHEET



Hunters cloud-native, Open XDR uniquely ingests, retains and dynamically cross-correlates all security telemetry to accelerate investigations and foster confident response to incidents.

With security operations becoming a big data problem, and the ever-growing number of siloed security solutions that organizations have in place with limited or simple correlation abilities, the SOC's efficiency declined. It is no surprise that 63% of security professionals believe that security operations are more difficult today than two years ago *(ESG 2020)*.

Hunters cloud-native, vendor-agnostic, open XDR is purpose-built to help security operations teams align numerous security tools into a cohesive security incident detection, investigation and response platform. Autonomous attack analytics identify and present real incidents -with context- to drive rapid, effective SOC response.

Key XDR Use Cases

SIEM Replacement

Move past costly solutions and avoid data lock. Make the most out of your existing tools without rule-writing with Hunters' automatic investigations that reduce detection analysis and triage time to seconds instead of minutes or hours.

Security Data Lake ETL & Analytics

Unify data spread across siloed tools and automatically run advanced analysis on years of log data. Hunters XDR acts as both the ETL and the analytics engine on top of your security data lake.

Security Analytics

Identify threat signals across the environment and obtain OOTB 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

Extend Data Usability

Vendor-agnostic ingestion, normalization, cross-correlation and storage of data across the entire attack surface at cloud scale.

Gain Incident Clarity

Accelerated threat detection, understanding and response workflow with an autonomous threat management system.

Elevate Business Impact

Freed up SOC from rudimentary and repetitive tasks to focus on value added work, and freed up budget to build and improve security posture.

> "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

Seamless, Flexible Ingestion

Using cloud connectors to pipe into existing security tools, or directly connecting to SIEM, Hunters XDR collects logs, events and telemetry from dozens of data sources on premises and in the cloud, including EDRs, NDRs, Cloud service providers, Firewalls, Identity and Access Management tools, and more.

Detection Engine

Hunters XDR extracts threat signals and alerts from petabytes of existing security data using a stream processing analytics technology. It enables near real-time processing and complex analytics. Threat signal extraction is guided by Hunters' TTP-based attack intel which is also mapped onto a MITRE ATT&CK technique.

Automatic Investigation

In order to understand weak threat signals and alerts, Hunters runs automatic investigations. It fetches all relevant information associated with those, including features and entities that were involved in a specific suspicious activity, and automatically enriches them with further context.

Scoring and Prioritization

Once there is enough context around threat signals and alerts, Hunters XDR leverages ML to score them from 0 to 100, allowing for an easy prioritization and quick triage.

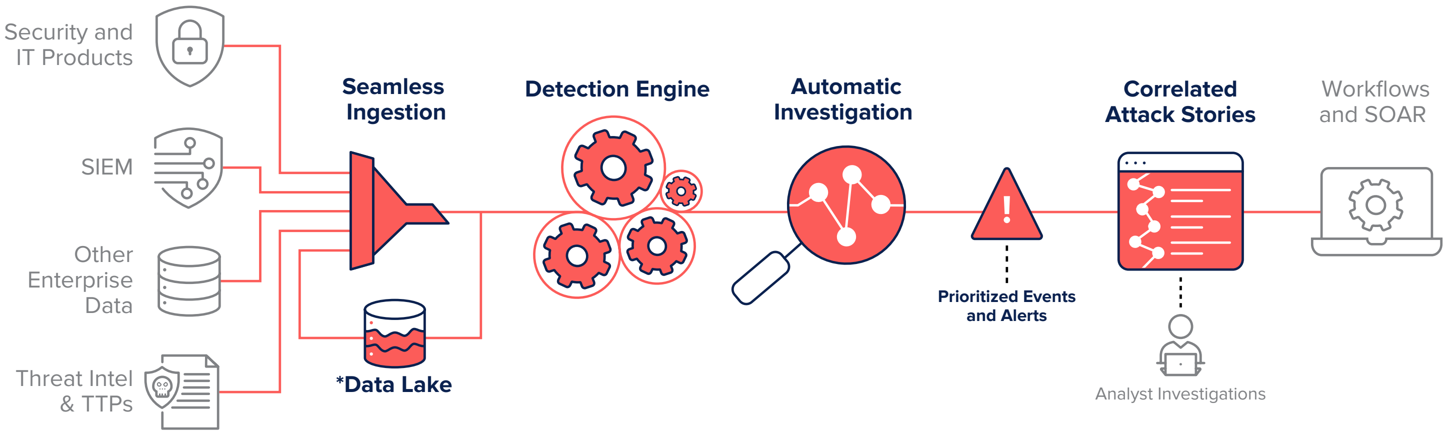
Cross-Surface Correlation

Hunters uses unsupervised learning to correlate signals and alerts across disparate areas of suspicious activity in the Graph (e.g., suspected phishing email followed by malware downloads on gateway and EDR), and surface actionable Attack Stories which include full attack summary and outline.

Response and Remediation

Streamline detection and response by escalating Attack Stories into SOAR tools and other existing workflows, enabling response automation and reducing attackers' dwell time.

GET A HUNTERS XDR DEMO



*Optional

Key Integrations

Integrations span across security products, data connectors, and workflows.

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