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.

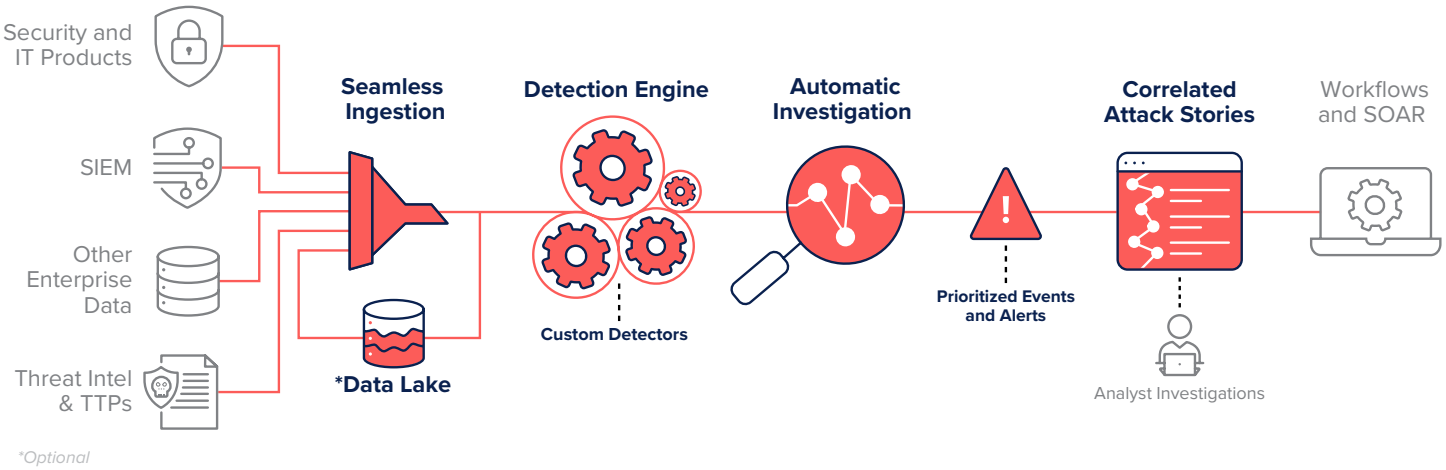
Cross-Surface Correlation

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



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