Nov 8th, 2020

Knowledge-Powered XDR

Hunters is an open XDR platform that harnesses top-tier threat hunting techniques and ML to proactively detect threats across endpoint, cloud, network, identity, and more.

What Technology Serves your SOC?

Recent years have been increasingly challenging for SOC detection & response. While attack surfaces grew exponentially, attackers became better at blending in, and security products were layered vertically, threat detection & response evolved as a manual, slow, and siloed process.
Put simply, SOC technology wasn't there.
It is time for a generational leap in threat detection & response.

From Hunted to Hunter

To change this equation and prepare organizations for tomorrow's attacks, Hunters has built a knowledge-powered XDR platform.
Hunters' "knowledge automation" is based on four key pillars:

1. **Existing Security Detections:** cloud, network, endpoint and more.
2. **Hunters' TTPs:** adversary understanding and platform expertise.
3. **Organizational Context:** crown jewels, domain controllers, sensitive assets, etc
4. **Threat Intelligence:** feeds on current attackers' infrastructure.

Hunters - A Knowledge-Powered XDR

Hunters leverages threat hunting techniques and ML to proactively detect threats across endpoint, cloud, network, identity, and more. It ingests petabytes of organizational data and security telemetry to search for alerts and noisy attack signals, and automatically analyzes, scores and correlates threat leads. With a proprietary Knowledge Graph, Hunters' XDR gives analysts necessary context and delivers accurate attack stories, at last.

Hunters grants security teams off-the-shelf security capabilities:

A. **Triage Automation:** Use Hunters' scoring and prioritization to reduce detection analysis and triage time.
B. **Incident Response:** Uncover root cause analysis and gain unprecedent situational awareness through the power of cross-surface correlation.
C. **Threat Hunting:** Improve sophisticated threat hunting quests by leveraging Hunters' detections of weak threat signals that bypass siloed organizational defense.

BENEFITS

Flexible Ingestion
Connect security products from across network, cloud, endpoint, and even SIEM, without agents, using Hunters' cloud connectors.

Your Stack Does More
Expose invisible threats with best-of-breed security and IT products.

Interconnect Environments
Reveal noisy signals: Hunters' XDR connects security telemetry from across surfaces and enriches it with autonomous investigations.

Use Findings, not Alerts
Receive accurate attack detection stories, to significantly reduce triage and response times.

How It Works

- **A. Flexible Ingestion:** Hunters' XDR uses its cloud connectors to collects logs and events from dozens of data sources, including EDR, Cloud services providers, firewalls, and SIEMs.
- **B. Extraction 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 into a MITRE ATT&CK technique.
- **C. Automatic Investigation and Scoring:** In order to contextualize and understand weak and noisy threat signals, Hunters performs autonomous investigations. It automatically extracts features and entities that were involved in a specific suspicious activity, and leverages ML to score them.
- **D. Cross-Surface Correlation:** Hunters loads investigated threat signals into a graph populated with relevant entities and relationships. It then uses unsupervised learning to correlate them across disparate areas of dense suspicious activity (E.g., suspected phishing email followed by malware downloads on gateway and EDR).
- **E. Actionable Attack Stories:** Final investigation outputs from Hunters are delivered as Attack Stories, which include full attack summary and outline, with details such as context, path, target and potential impact. Attack stories can be escalated to SOC through existing workflows (SIEM, SOAR, Ticketing Systems, etc.)

KEY FEATURES

Cloud-Based Data Connectors across Environments

Stream Processing Analytics Engine

TTP-based Automatic Investgiations

MITRE ATT&CK Threat Mapping

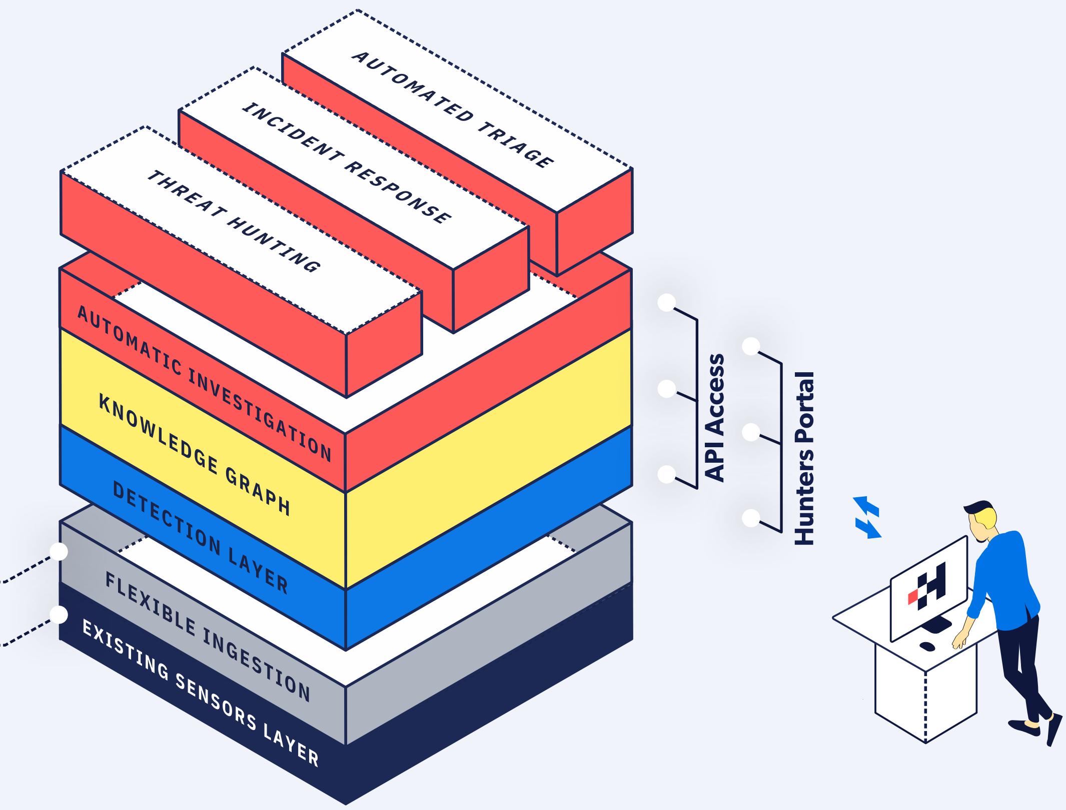
Attack Escalation via Existing Workflows

KNOWLEDGE - POWERED XDR

snowflake

Security Data Lake
(Owned by Customer)
Cloud Storage, SIEM,
Cloud Connectors

EDR, SWG, NGFW,
Identity, Email
Security Gateway,
Cloud IaaS, CWP



Ready to Hunt?

START NOW

Hunters.