HuntersAI / CROWDSTRIKE

Extend your Threat Detection

into new surfaces with Hunters.AI & CrowdStrike Falcon

THE CHALLENGE

Enterprises are everywhere - cloud, network, endpoint, mobile. The amount of security solutions that SOC analysts need to monitor in order to secure them generates an obscene level of noise.

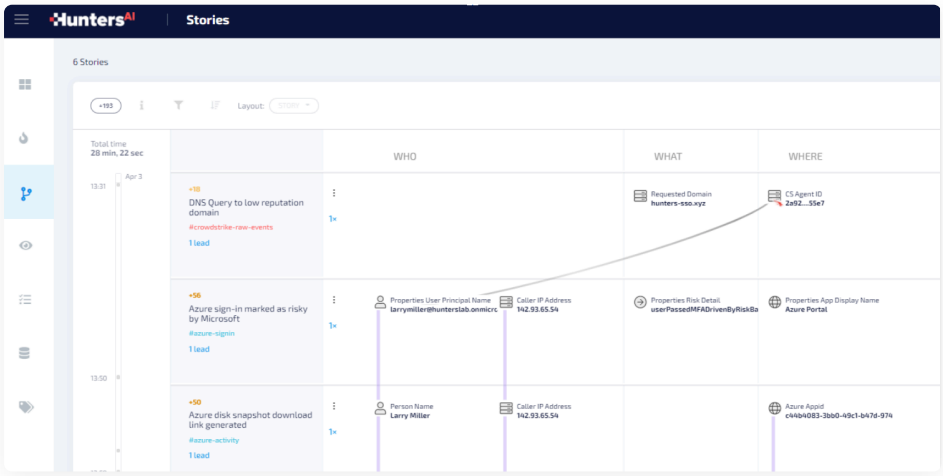
Market-leading Endpoint Security solutions like CrowdStrike Falcon enable organizations to effectively respond to endpoint threats, and yet, attackers' traces fall between the cracks of disconnected data sources across the IT security stack.

Extending detection and response to connect data across platforms and detections, a capability increasingly known as 'XDR', becomes key to effectively remediate threats.

THE SOLUTION

Hunters' open XDR solution, available on the CrowdStrike Store, extends threat detection beyond the endpoint into cloud, network, identity providers, and more. Cloud-delivered, Hunters.AI seamlessly ingests rich endpoint telemetry from the Falcon platform as well as organizational data and security telemetry from any existing data source in the organization. The solution searches for attack signals in the raw data, and automatically analyzes, scores and correlates them using a proprietary Knowledge Graph that gives the necessary context to deliver bulletproof attack stories, all across the enterprise.

With Hunters.AI, organizations can easily go from EDR to XDR, achieving higher detection efficacy while significantly reducing SOC triage and time-to-detect.



HUNTERS.AI - An Attack Story showing the correlation between a CrowdStrike event and Azure Activity

Hunters.AI grants security teams off-the-shelf enhanced security capabilities:

A. **Autonomous Analysis:** Immediate threat detections across IT environments (cloud, network, endpoint) to reduce triage time and expedite response

B. **Autonomous Response:** Enhanced investigation and forensics capabilities with Hunters' Knowledge Graph

C. **Autonomous Threat Hunting:** Automated detection of weak threat signals that bypass existing siloed organizational defenses

BENEFITS

Seamlessly transform your existing CrowdStrike endpoint telemetry into an XDR

Expedite time-to-detect and time-to-respond with data-proof attack stories

Access high fidelity scored attack stories

Detect attacks that bypass existing security controls, with cohesive threat detection across your entire IT environment (cloud, network, endpoint)

Deploy Hunters.AI in minutes with just a few clicks, no agents required

HOW IT WORKS

A. **Connecting to Hunters.AI:** Get started with Hunters.AI from the CrowdStrike Store.

B. **Cloud-based Ingestion:** Hunters.AI ingests logs and events from CrowdStrike Falcon as well dozens of additional data sources, including Cloud services providers, SaaS applications and firewalls.

C. **Extraction Engine:** Hunters.AI extracts threat signals as well as alerts from the petabytes of security data generated by the existing stack of security products. It leverages stream processing technology which enables both near real-time processing and unique complex analytical capabilities. This activity is guided by Hunters' TTP-based attack intel which is also mapped into a MITRE ATT&CK technique.

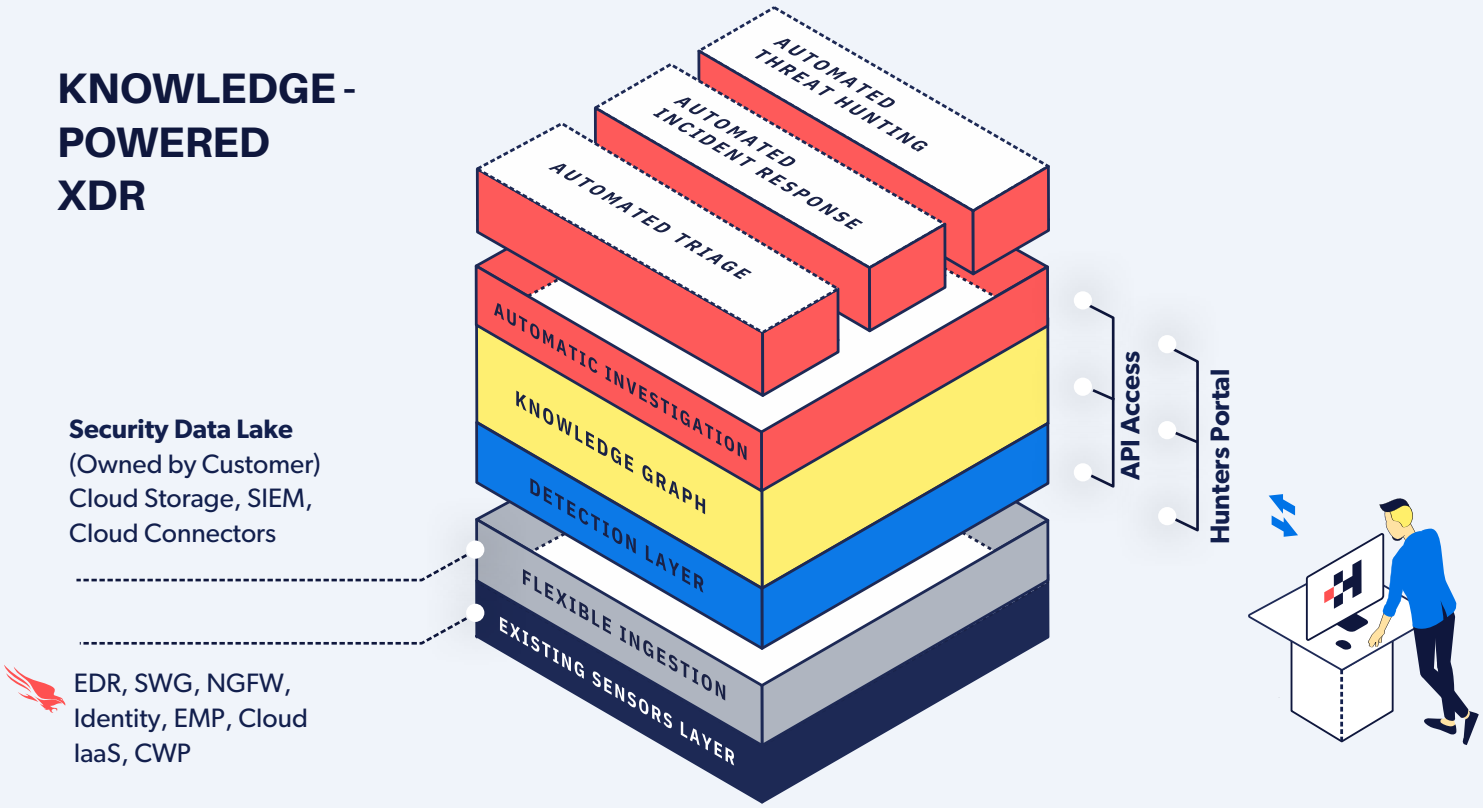
D. **Automatic Investigation and Scoring:** In order to contextualize and understand both weak and noisy threat signals and alerts, Hunters.AI performs autonomous investigations. It automatically extracts features and entities that were involved in a specific suspicious activity, and leverages ML to score them.

E. **Cross-Surface Correlation:** Hunters.AI loads investigated threat signals into a graph that is populated with related entities and relationships. It then uses unsupervised learning to correlate them across disparate areas of dense suspicious activity, all across the enterprise.

F. **Actionable Attack Stories:** Final investigation outputs from Hunters.AI are delivered as Attack Stories, which include full attack summary and outline, with details such as context, path, target and potential impact.

G. **Advanced Detection, Incident Response, and Threat Hunting:** Reduce triage time with Hunters' Attack Stories, and perform advanced forensic investigation and threat hunting quests using Hunters' Knowledge Graph.

KNOWLEDGE-POWERED XDR



Watch Hunters.AI extend your Falcon logs into an XDR!