CrowdStrike Store

Hunters.

CROWDSTRIKE

Data Sheet

HUNTERS: KNOWLEDGE-POWERED XDR

Extend your threat protection into new surfaces with Hunters XDR and CrowdStrike Falcon

CHALLENGES

Enterprises are everywhere: cloud, network, endpoint, mobile. The amount of security solutions that security operations center (SOC) analysts need to monitor in order to secure them generates a tremendous level of noise.

Market-leading endpoint security solutions such as the CrowdStrike Falcon® platform enable organizations to effectively respond to endpoint threats, but traces of an attack can 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 remediating threats.

SOLUTION

Hunters' open XDR solution, available in the **CrowdStrike Store**, extends threat detection beyond the endpoint into cloud, network, identity providers and more. The Hunters cloud-delivered solution 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 high-fidelity attack stories, all across the enterprise.

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

BUSINESS VALUE

Use Case	Solution Benefits
Automated Triage	Use Hunters' enrichments, scoring and prioritization to reduce detection and triage time.
Incident Response	Expedite incident response with root-cause analysis, and gain unprecedented risk awareness and insights into multi-surface incidents.
Threat Hunting	Improve sophisticated threat hunting quests by leveraging Hunters' detections of weak threat signals that bypass siloed organizational defenses.

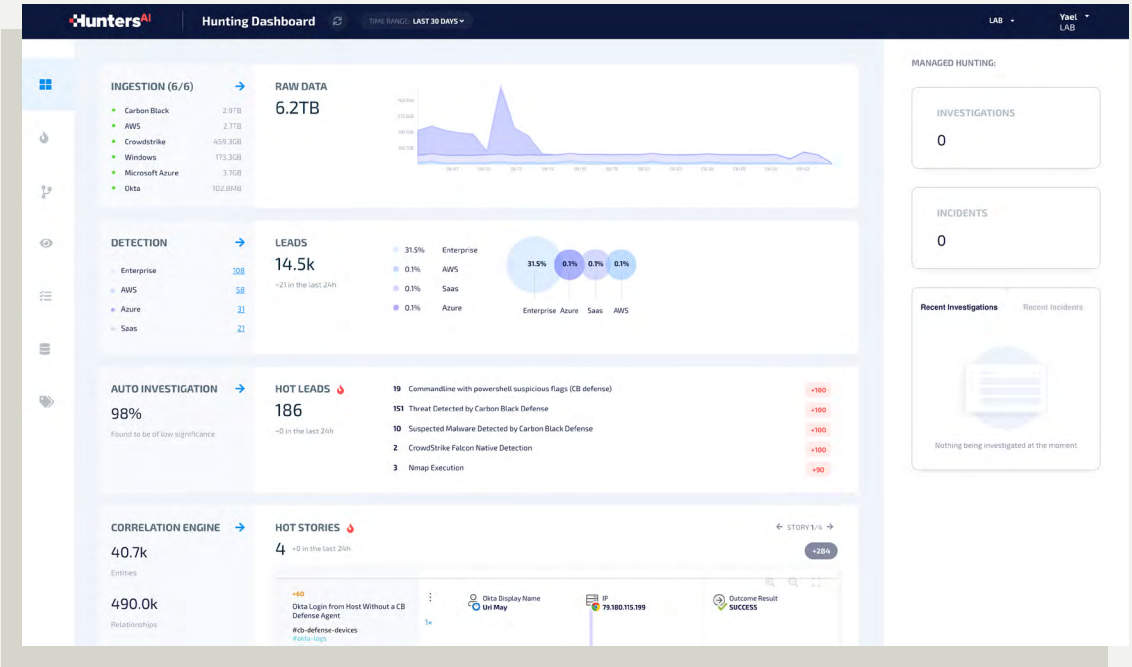
KEY BENEFITS

Extend CrowdStrike detections into new attack surfaces — go from EDR to XDR overnight

Expedite time-to-detect and time-to-respond with contextualized and correlated attack stories

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

HUNTERS: KNOWLEDGE-POWERED XDR



Hunters XDR Dashboard

TECHNICAL SOLUTION

1. **Connect to Hunters:** Get started with Hunters XDR from the **CrowdStrike Store**.
2. **Flexible ingestion:** Hunters uses its cloud connectors to ingest logs and events from CrowdStrike Falcon as well as dozens of additional data sources, including cloud services providers, SaaS applications and firewalls.
3. **Extraction engine:** Hunters 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' attack intelligence, based on tactics, techniques and procedures (TTPs) and mapped onto a MITRE ATT&CK® technique.
4. **Automatic investigation and scoring:** In order to contextualize and understand both weak and noisy threat signals and alerts, Hunters performs autonomous investigations. It automatically extracts features and entities that were involved in a specific suspicious activity and leverages machine learning (ML) to score them.
5. **Cross-surface correlation:** Investigated threat signals and alerts are loaded into Hunters' proprietary Knowledge Graph of related entities and relationships. The solution then uses unsupervised learning to correlate them across disparate areas of suspicious activity to surface "Attack Stories" all across the enterprise.
6. **Actionable Attack Stories:** Final investigation outputs from Hunters are delivered as Attack Stories, which include a full attack summary and outline with details such as context, path, target and potential impact.

HUNTERS: KNOWLEDGE-POWERED XDR

KEY CAPABILITIES

- Connects to existing data to detect overlooked threats and connect the dots between siloed areas of the organization
- Scores and correlates threat leads using a proprietary Knowledge Graph that gives the necessary context to deliver bulletproof attack stories all across the enterprise

ABOUT HUNTERS

Hunters' open XDR is built to empower SOC teams with an automated decision support system they can rely on, while optimizing on the existing security stack. Hunters flexibly integrates with your security tools to extract threat signals across endpoints, cloud, email, network and more. By leveraging a proprietary knowledge graph technology, Hunters contextualizes and correlates both high fidelity and low fidelity threat signals, into actionable findings never seen before. Hunters XDR enables analysts to answer the three biggest questions around detection and response: Is this signal malicious? What actually happened here? What did I miss?

Learn more at **Hunters.ai**.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 4 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.