Autonomous Threat Hunting

Hunters.AI is the first autonomous threat hunting solution. Scaling top-tier hunting techniques, it automatically detects cyberattacks that bypass existing security controls.

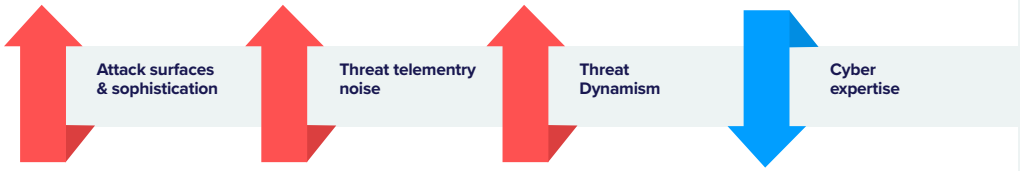
Attackers are in. Can you find them?

Cyber attackers are constantly inventing new tactics, techniques, and procedures (TTPs) to bypass organizational security defenses. While their hidden traces remain in organizational data, finding them in the massive data fog is a daunting task that requires unique domain expertise. Sadly, this is an experise that t he global ecosystem cannot sufficiently provide.

From Hunted to Hunter

In order to stand a chance against cyberattacks, today's defenders must: Become proactive, move much faster, and embrace every bit of data (and noise that often comes along with it).

In other words: to win today's threat landscape, defenders need to think like attackers, and they need to do it at scale.



Hunters.AI - Autonomous Threat Hunting

Hunters.AI is the industry's first autonomous threat hunting solution. By seamlessly connecting to raw organizational data and infusing it with TTP-based attack intelligence, it extracts threat signals, scores them, and intelligently correlates them across every attack surface. Hunters.AI delivers security operation center (SOC) teams with full attack stories to reduce response times, and reveals hidden cyber threats in the modern enterprise, at last.

BENEFITS

Threat Hunting at Scale
AI-based machine autonomously hunts threats, never not-working for you.

Leverage your Data
Utilize organizational data sources and security solutions to expose invisibile threats. No agents needed.

Interconnected Environments
Detect attacks that bypass existing security controls, with cohesive threat analysis on all: cloud, network, endpoints.

Use Findings, not Alerts
Receive data-proof attack detection stories, to significantly reduce response times.

How Does it Work?

Extracting threat signals from raw data: Hunters.AI connects to existing organizational data sources ranging from security solutions such as: EDR, Firewall, Cloud security, and more, to: cloud storage, security data lakes, and existing APIs like: Okta, ADP, Cisco Meraki, and others. Leveraging its vast repository of attack intelligence and TTP-based matrices, Hunters.AI then uses its detectors to extract threat leads across various IT environments.

Autonomous investigation and scoring: Autonomous investigation and scoring: Upon extracting threat leads, Hunters.AI:

A. Runs numerous queries on databases, comparative analyses, and more, via external APIs
B. Performs machine learning feature selection to identify risk parameters
C. Rates the risk based on the above findings - this results in scored threat leads

Detecting the attack in real-time: All scored threat leads are added on to Hunters.AI' Correlation Graph, where relevant entities like domain, identity or IP address are extracted to automatically build relationships. By now, the high relevance of detected threat leads; valid scoring; enrichment with entities; and holistic view across environments; all enable Hunters.AI' correlation graph to identify risky incidents in real-time.

Delivering attack stories to SOC: Providing security teams with concrete findings, Hunters.AI provides high fidelity attack stories. These include a full business summary as well as hunting inputs like: timeline, IOCs, data sources, and artifacts.

To complete the response cycle, Hunters.AI integrates into existing workflows like SIEM, SOAR, and others, enabling you to respond more easily and faster, based on its hunting results.

KEY FEATURES

Multi-Surface Detection & Correlation
Correlate threat signals across different platforms on cloud, network, & endpoints. Leverage Hunters' unique attack matrices along MITRE ATT&CK

Autonomous Investigations
Use Hunters' AI to proactively investigate on scored threat signals, via: hypotheses on adversarial behaviors, examination of known TTPs, and searching anomalies in known environments

Bottom-Line Attack Stories
Translate hunting outputs into actionable findings. Factual details include: timeline, location, path, context, target and potential impact

TTP-based Threat Hunting
Hunters.AI is constantly enriched with Tactics, Techniques, and Procedures (TTPs), modeled by Hunters' top-tier cyber security experts

Cloud-Based Data Connectors
Seamlessly connect to your existing data on every environment, using restful APIs, Syslog, SIEM, cloud storage connections, and more

Ready to Hunt?

START NOW