Achieve Full Attack Context for Stronger Prevention and Faster MTTR

Next-Generation SIEM automation for Threat Detection, Investigation, & Response

Do more with Check Point deployments

Hunters Next Generation SIEM automates threat detection, investigation, and response - freeing analysts to proactively protect their organizations. The platform automatically ingests and correlates Check Point firewall logs and alerts with data from other security tools and services to generate high fidelity detection and comprehensive attack stories. This allows for a complete overview of the attack for faster investigation and response. For example, suspicious activity observed in Check Point firewall logs is correlated with endpoint detection and response (EDR) logs to provide details about user activity on the device that generated the connection or the specific process that communicated with the Command & Control (C2) server. Hunters SIEM can then block specific traffic on the firewall and identify entities related to the same incident and remediate them.

Benefits for Check Point users

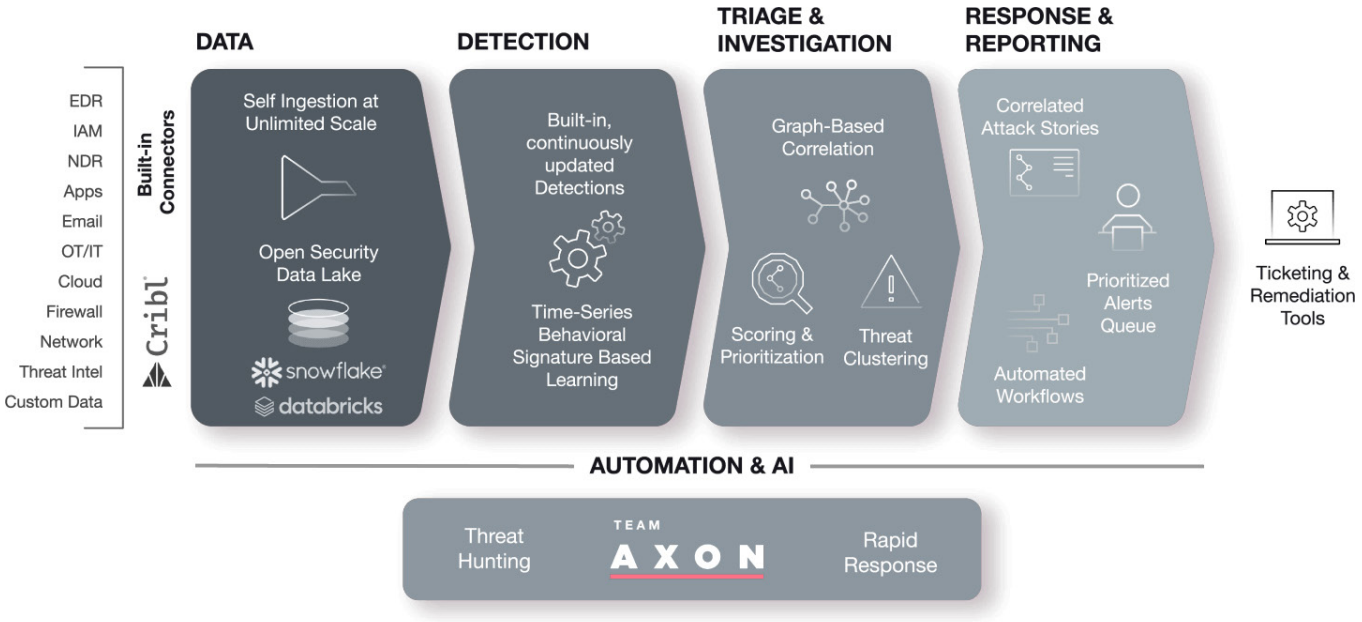
- **Faster investigation and response** - Investigate incidents in a single platform, without pivoting between tools

- **Better prevention and remediation** - Correlate data across sources for full threat context. Block a connection to an IP address on the Check Point firewall, the malware that initiated the connection and contain the compromised user

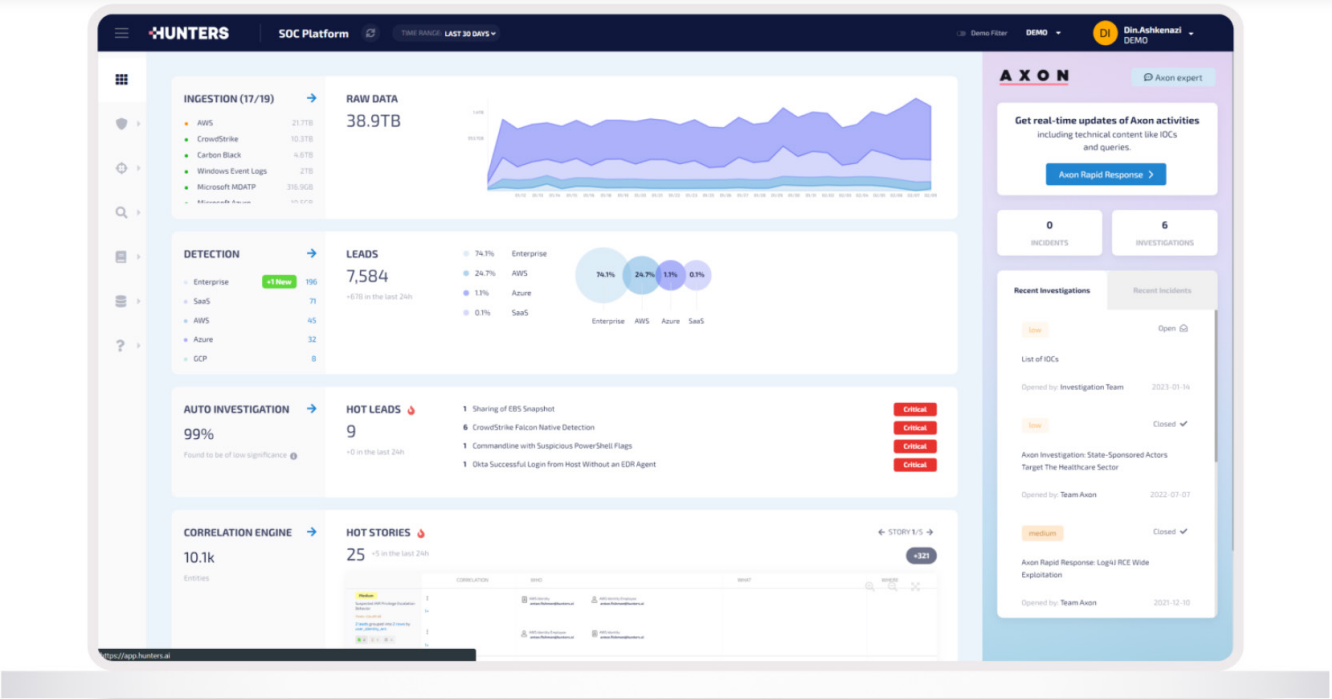
- **Noise reduction** - Focus on alerts that matter. By correlating data sources, Hunters learns the network's known IP addresses based on Check Point data, letting analysts focus on alerts with unknown and potentially malicious IP addresses

Hunters + Check Point out-of-the-box content examples:

- **Check Point Smart Defense alerts** - Hunters surfaces alerts generated by the Check Point Smart Defense module. Alerts are enriched, automatically investigated and correlated to additional data sources.
- **Data Correlation** - Traffic data and alerts ingested from Check Point appliances are correlated to the endpoint, cloud, and application data such as EDR telemetry, Windows Event logs, AWS VPC, Azure logs and more. This provides a holistic and contextual view of incidents and expedites investigations and response.
- **Log Search** - Check Point data is combined with additional network data ingested from other products, and all data is normalized and mapped to OCSF. This provides a single pane of glass for threat hunting and investigations across all log sources.
- **Out-of-the-box Detections** - Hunters provides continuously updated threat detections on top of Check Point data in addition to alerts generated by the Check Point tools.



Hunters deploys in days and eliminates repetitive work with out-of-the-box integrations and detection rules. High priority alerts are surfaced based on risk and confidence scoring, and similar alerts are clustered together, reducing alert triage by 80%. Customers can build an open, scalable data lake at a predictable cost, and bring their own data lake or leverage Hunters'.



Built-in, Always Up-to-date Detections

Hunters delivers up-to-date detections which are pre-verified on real-world customer data to remove any false positives and excessive alerting, then deployed directly to all customer tenants without requiring any action or tweaking. This dramatically reduces risk exposure and operational overhead. The threat coverage of the organization is automatically mapped to the MITRE ATT&CK framework.

Open, Scalable Security Data Lake

Hunters SOC Platform ingests, normalizes and retains data from dozens of security and IT tools, scaling to any size of environment. Customers can opt for a "bring-your-own data lake" deployment model, or leverage Hunters' embedded one. Hunters ETL (Extract, Transform & Load) and schema mapping capabilities eliminate the need to engineer, deploy and maintain ingestion pipelines.

Automated Triage and Investigation

Every alert is automatically enriched with information from various sources (e.g., user name from CrowdStrike with login records from Okta, IP addresses with threat intel information) and is displayed to the analyst for faster triage, investigation, and advanced detection and scoring purposes. The platform also clusters alerts using proprietary "threat similarity" logic, reducing redundant work for up to 90% of alerts that may happen across days and weeks.

Attack Stories

Alerts across entities and attack surfaces are automatically correlated on a graph, and are packaged as 'Attack Stories', giving a contextual view of the full incident. This capability highlights high-fidelity activity, improves investigation time, and allows leveraging low-fidelity signals that are often overlooked.

Dynamic Scoring and Prioritization

The platform continuously examines the risk level of each alert, assigning both a risk and confidence score, so analysts can prioritize the most critical to the business. For example, alerts involving sensitive assets (e.g., c-level, domain servers, etc.) are prioritized, and risk for known benign behaviors is lowered (e.g., a binary signed by Microsoft.)

IOC Search

For regulatory purposes and ad-hoc investigations, Hunters also delivers an IOC search bar to allow anyone in the SOC to search for IOCs and get results from raw data within seconds, without needing to write a SQL query.

Multi-Tenancy

Manage security operations for multiple business units from a centralized platform.

Learn More/Get Demo

About Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

About Hunters

Hunters is a group of cyber and technology experts with a mission to revolutionize security operations by combining data engineering, security expertise and layers of automation to expedite decision making, helping security teams become attack-ready. We empower security teams. Hunters infuses how attackers think and act into a platform that helps security operations see and stop attacks at their root.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com