Hunters / snowflake Solution Brief

Moving Beyond SIEM

With Hunters and Snowflake

Hunters redefines threat detection, investigation and response across the enterprise.

Coupled with Snowflake's data lake, it transforms how organizations monitor, store and analyze petabytes of data they generate across environments, setting a new standard for detection and response.

THE CHALLENGE

Traditionally, security analysts have resorted to the SIEM to understand threats and look for context on alerts generated by the multiple security tools. But SIEM solutions are costly, complex and resource-consuming given that big portions of the ingestion, normalization, rules-creation and correlation fall under the analysts' responsibility. Adding to the mix, the growing number of environments and the evolution of security technologies has led to siloed detection tools, making security operations increasingly complex.

THE SOLUTION: HUNTERS AND SNOWFLAKE

Hunters is an open XDR solution that harnesses adversary expertise and machine learning to proactively detect and respond to threats across the entire attack surface - on endpoint, cloud, network, identity, and email. SaaS-delivered, Hunters seamlessly ingests petabytes of organizational data and security telemetry to search for threat signals and alerts, and automatically analyze, score and correlate them. Using a proprietary Knowledge Graph, Hunters XDR provides analysts with detailed attack stories and context for effective investigation and rapid response. It provides rich insights for containment, and streamlines response by integrating with SOAR and workflow tools. Hunters natively integrates with Snowflake, acting as both the ETL and the analytics engine on top of it, allowing security analysts to:

1. **Automatically run advanced analysis on petabytes of log data**
2. **Minimize data ownership costs**
3. **Unify threat detection across siloed tools without writing or tuning detection rules.**

BENEFITS

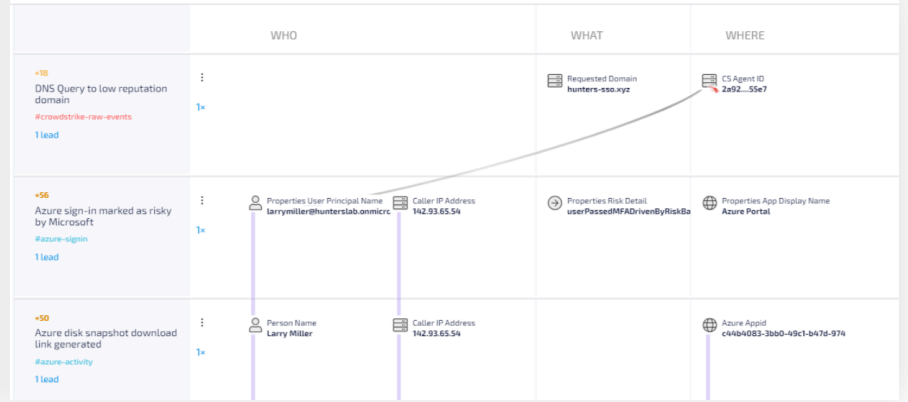
Reallocate budget from costly SIEM solutions while achieving an improved security posture

Retain more data, have it more accessible and pay less for it

Realize immediate time-to-value with Hunters' OOTB detection content and investigations, no tuning required

Detect and Respond to threats across all attack surfaces: endpoint, cloud, network, identity and email

Connect and deploy Hunters XDR in minutes with just a few clicks, no agents required



An Attack Story in Hunters' platform showing a data exfiltration from an Azure server as a result of a spear phishing, detected by Hunters' analytics for CrowdStrike events and Azure telemetry, and connected after a series of automatic investigations

MOVING BEYOND SIEM

Running on the Snowflake Data Cloud, Hunters adds intelligent out-of-the-box analysis that can quickly analyze large volumes of log data, minimize data retention costs, and consolidate formerly siloed security data sources leveraging Snowflake's virtually unlimited performance and scale.

Automated Analysis

Reduce time to detect and to respond with TTP-based detection that interconnects telemetry across: endpoint, cloud, network, identity and email. Access high-fidelity Attack Stories powered by Hunters' graph correlations and alert prioritization.

Cost Reduction

Make an efficient use of valuable analyst' time with correct prioritization, while realizing immediate time to value with OOTB detections and analytics, no tuning required. Allocate appropriate compute resources for your workloads and pay only for the computing power you use.

Unified Data

Connect all your security vendors of choice and support analytics at scale by provisioning your own data lake and using Hunters' automated threat analysis and investigation workflows against your raw data in one single interface.

It's time to move past legacy detection products and start making more out of your security data at a fraction of the cost.

HOW IT WORKS

1. **Connecting to Hunters XDR:** In Snowflake, use Partner Connect to launch Hunters.
2. **Seamless, Flexible Ingestion:** Using cloud connectors to pipe into existing security tools, or directly connecting to SIEM, Hunters XDR collects logs, events and telemetry from dozens of data sources on premises and in the cloud. This data is normalized and sent to your instance of Snowflake, where it can be combined with all other enterprise data and visualized in BI.
3. **Detection 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 onto a MITRE ATT&CK technique.
4. **Data Representation on a Multi-Dimensional Graph:** The telemetry collected from various IT and security tools is effectively connected together on a proprietary Knowledge Graph, a structured representation of all the suspicious behaviours, all the entities in the network, and the relationships between them.
5. **Automatic Investigation:** In order to understand the broader context and impact of identified weak threat signals and alerts, Hunters runs automatic investigations. It fetches all relevant information associated with those from both the source security system and from other peripheral sources, like threat intel, organizational directory, etc.
6. **Scoring and Prioritization:** Once there is enough context around threat signals and alerts, Hunters XDR leverages ML to score them, enabling easy prioritization and quick triage.
7. **Cross-Surface Correlation:** Hunters uses unsupervised learning to correlate signals and alerts across disparate areas of suspicious activity in the Graph (e.g., suspected phishing email followed by malware downloads on gateway and EDR), and surface actionable Attack Stories which include full attack summary and outline.
8. **Response and Remediation:** Streamline detection and response by escalating Attack Stories into SOAR tools and other existing workflows, enabling response automation and reducing attackers' dwell time.
9. **Advanced Analytics in Snowflake:** Perform advanced analytics directly in Snowflake using data science and ML-models.

Watch a demo of Hunters XDR and Snowflake

Hunters