HUNTERS

DATA SHEET

HUNTERS & SNOWFLAKE

Transform your security data and move beyond SIEM

The proliferation of security tools, the explosion of data and the increasing sophistication of the threat landscape make full access to data from the entire IT ecosystem a critical prerequisite for effective threat detection and response. Traditional logging solutions, like SIEM, are no longer viable operationally or economically, because they often force organizations to compromise on what data to include and how long to keep it to minimize costs. This results in blind spots when dealing with security threats like supply chain, insider threats, and others.

Effective security operations depends on available and usable data that fits an economical model for cloud-scale data. Snowflake and Hunters solve the data requirement for modern security operations with a solution that pairs data lake architecture with schema mapping of all available security data, designed to support the full scale and variety of data in today's organizations and enables automated threat detection, investigation and response.

Hunters and Snowflake solutions:

Hunters Security ETL for Snowflake

For organizations transitioning their security data to the Snowflake Cybersecurity workload

Hunters SOC Platform

For organizations looking to streamline and accelerate their threat detection, investigation and response with automation

GET A HUNTERS DEMO

Hunters Benefits

Cover the Entire Attack Surface

Vendor-agnostic data ingestion and normalization across all data from your security and IT tools, at a predictable cost.

Empower Security Teams

Built-in detection engineering, data correlation, and automatic investigation to overcome volume, complexity, and false positives.

Minimize Security Risk

Reduce overall security risk and compliance exposure by mitigating real threats faster and more reliably than SIEMs.

"I recommend Hunters to every CISO because they're probably experiencing the same things as I am: they're probably using the same tools as we are, and I recognize the challenges behind that. I know that Hunters can unify all the data generated from those tools and make sense out of it to help us in our fight with the intruders."

Mario Duarte, VP Security snowflake®

HUNTERS PRODUCTS

Hunters Security ETL for Snowflake

Lightweight managed extract, transform, load to unify IT and security data spread across siloed tools

The extract, transform, load (ETL) process applied to data sources is now available for your security data. Hunters Security ETL for Snowflake enables all your security data to be centralized in a repository from dozens of siloed data sources. Designed for Snowflake customers, centralized security data is now ready for query and analysis to enhance threat detection, compliance, and investigation of past incidents.

Simply select the data sources you want to centralize for security purposes and Hunters does the rest, including:

DATA COLLECTION Gather data from REST API, S3 bucket, or wherever it resides, removing worries of implementation or monitoring for changes

INFRASCTUCTURE Hunters manages the infracstructure and associated logic

DATA MAPPING Data is organized into a schema that makes it easier for you to make queries

RAW DATA Data is maintained in original format to ensure no data is lost in the process

The Hunters Security ETL for Snowflake solution is an easy and critical first step in building modern, effective security operations, and enables customers to expand to the full SOC Platform offering to add a full suite of data integrations and advanced security operations capabilities.

Hunters SOC Platform

Automated, cloud-native platform built to support the entire security operations workflow

The Hunters SOC platform empowers security teams to automatically identify and respond to incidents that matter across their entire attack surface, at a predictable cost. Through built-in detection engineering, data correlation, and automatic investigation, the platform helps teams overcome volume, complexity, and false positives. Hunters mitigates real threats faster and more reliably than SIEMs, ultimately reducing customers' overall security risk.

Core platform engines combine to deliver accuracy and efficiency across security operations workflow:

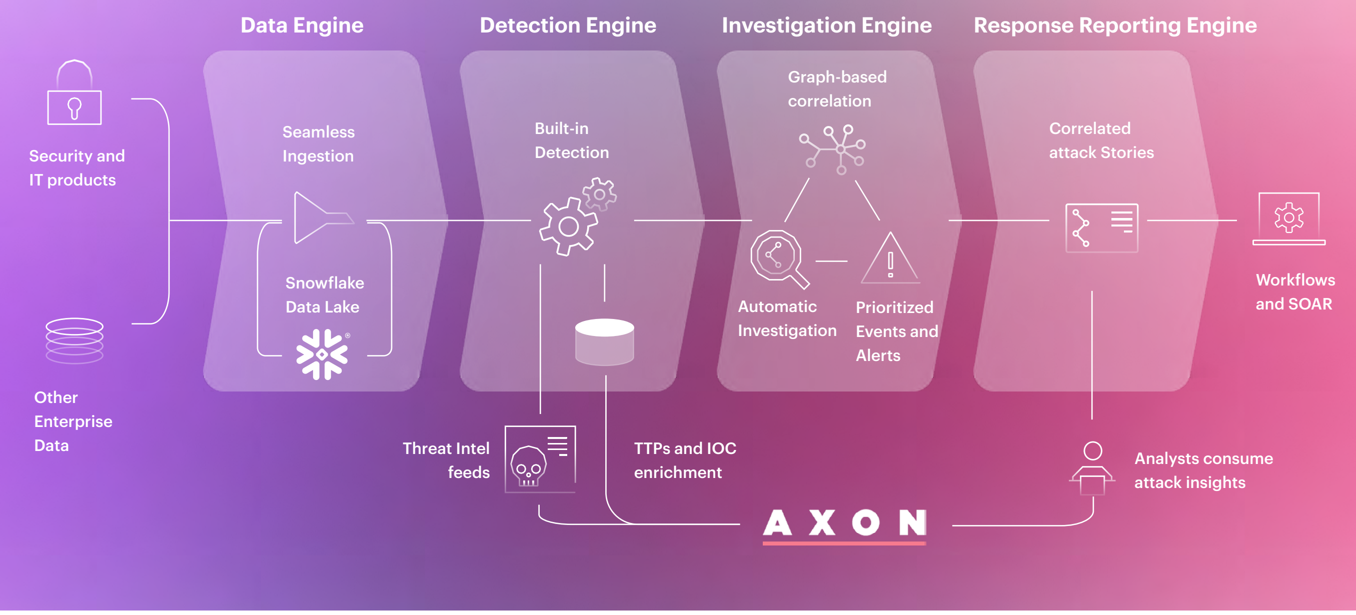
DATA ENGINE Easily ingest and retain all your data, at a predictable cost for better security outcomes

DETECTION ENGINE Offload the burden of endless rule creation and maintenance with an always up-to-date detection engine

INVESTIGATION ENGINE Leverage automation to offload manual analyst work and shorten investigations and triage processes

RESPONSE & REPORTING ENGINE Clear threat context and prioritization empower fast incident understanding and mitigation in a complete Attack Story

Hunters SOC Platform workflow


Data Engine
Detection Engine
Investigation Engine
Response Reporting Engine
Security and IT products
Other Enterprise Data
Seamless Ingestion
Snowflake Data Lake
Built-in Detection
Graph-based correlation
Automatic Investigation
Prioritized Events and Alerts
Correlated attack Stories
Workflows and SOAR
Threat Intel feeds
TTPs and IOC enrichment
AXON
Analysts consume attack insights