HUNTERS

CROWDSTRIKE

DATA SHEET

HUNTERS SOC PLATFORM AND CROWDSTRIKE

Do more with CrowdStrike Falcon deployments

Hunters SOC Platform is a SIEM replacement, delivering data ingestion, built-in and always up-to-date threat detection and automating correlation and investigation processes to reduce risk, cost and complexity for SOC teams.

Organizations are leveraging Hunters SOC Platform's unique detection capabilities to do more with CrowdStrike Falcon by connecting its telemetry data, such as running processes, network connections and file creations, with other data sources across the IT security stack to attain full attack insight for faster response times.

Leverage unique Hunters SOC Platform detection capabilities to attain greater attack insight

Detect logins to cloud applications like AWS, Okta, Azure

Analyze logins from a malicious IP address detected by CrowdStrike Falcon with SaaS application login logs to detect attacks on cloud applications like AWS, Okta and Azure.

Identify devices without CrowdStrike Falcon installed

Identify devices without an EDR agent installed by correlating CrowdStrike Falcon telemetry with SaaS and identity provider logs.

Attain greater insight into host vulnerabilities

Integrate data from vulnerability management platforms, including CrowdStrike Spotlight, AlienVault Open Threat Exchange and Anomali, and CrowdStrike Falcon to enrich host information with vulnerabilities related to it.

Use graph correlation to obtain full attack stories

Leverage graph correlation to combine alerts on the same attack from different IT security tools to deliver a full attack story on the who, what, when and where of an incident without pivoting between tools.

Uncover IOCs across all security data

Conduct IOC searches in seconds across all security data, including firewall, proxy, AWS, CrowdStrike and Okta logs, stored in a cloud-native, scalable data lake.

Helping companies move beyond SIEM

Replace endless rule creation on your SIEM with an always up-to-date detection engine

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

Understand the who, what, when, where of an incident with a full attack story

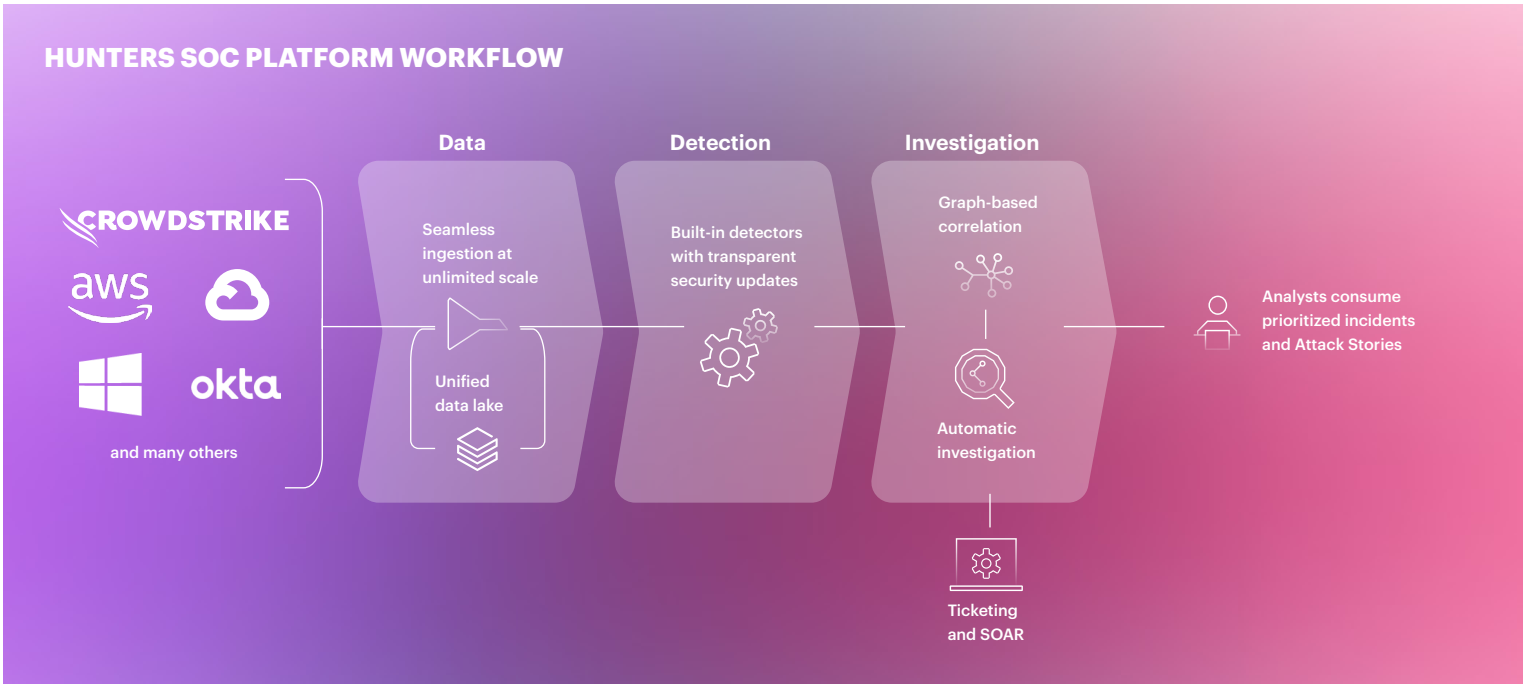
Enable security teams to focus on threats that matter by reducing alerts, false positives

Helping leading companies achieve the most out of their CrowdStrike Falcon deployments

snowflake Booking.com Solaris CLUMIO GONG cimpress

"One thing that very much stood out for us in our initial POC was that we were able to get our CrowdStrike and AWS cloudtrail logs into the Hunters platform extremely fast and start receiving contextualized alerts from day one."

CISO, major mortgage provider



Unlimited Ingestion
Hunters SOC Platform ingests, normalizes and retains data from dozens of IT and security tools, including CrowdStrike Falcon, in a cloud-native, scalable data lake. Hunters automatically applies structure to raw data, allowing security teams to spend less time converting data into a vendor-specified format.

Built-in, continuously updated detections ready from day one
Hunters offers continuously updated, built-in, pre-configured detectors that are ready to use out-of-the-box. Ingest data and start detecting threats on day one instead of spending months fine-tuning and rewriting detections to make them operational.

Automatic Investigation
Alerts are automatically enriched with information from various sources, including CrowdStrike, for faster investigation and triage.

Graph Correlation
Alerts across entities and attack surfaces are automatically correlated on a graph to reveal relationships previously undiscovered. This information is packaged in an easy to follow Attack Story that provides analysts with context on an entire incident, including the path an attacker took.

Dynamic Scoring and Prioritization
The platform continuously examines the risk level of alerts, assigning both a risk and confidence score so analysts can prioritize the most critical alerts.

IOC Search
Use a search bar to look for IOCs in all security data stored in a cloud-native, scalable data lake and get results without having to write an SQL query.