panther + CROWDSTRIKE

DATA SHEET

Security Analytics for CrowdStrike Falcon

Extend CrowdStrike Falcon with detection-as-code and long-term telemetry storage in a security data lake.

Challenges

As the number of connected devices grows and more people work remotely, the volume of data organizations need to collect, analyze, and retain for security and compliance has grown at an explosive rate. With older data architectures, storing all of this security data for long periods of time was costly, inefficient, and cumbersome.

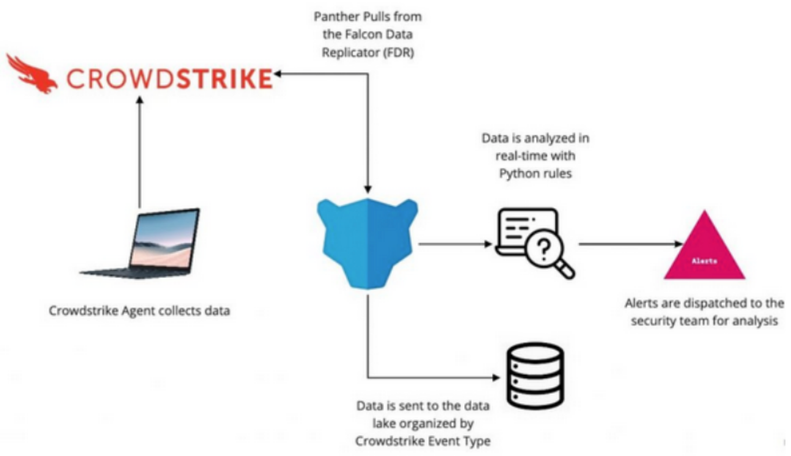
In addition to exploding data volumes, varying log schemas and formats make it difficult to correlate activity across environments and detect security vulnerabilities at scale. As more workloads migrate to the cloud, security teams need flexible tools and structured and normalized data to detect sophisticated attacks across their rapidly expanding environments.

Solution

Panther enables teams to gain additional value from their CrowdStrike Falcon event data with detection-as-code and long-term, affordable data retention in a scalable and robust security data lake.

With Panther's simple integration for CrowdStrike Falcon, teams can quickly pull raw CrowdStrike telemetry from an Amazon S3 bucket, then parse, normalize, and analyze the data historically and in real-time to trigger context-rich alerts and downstream automation. By leveraging serverless stream processing and Python-based alerting, Panther offers security teams a scalable and flexible platform for writing hardened detections that analyze high-scale CrowdStrike Falcon data and produce high-signal security alerts.

In Panther, detections run continuously against streaming event data for true real-time alerting or historically against normalized data for advanced correlation. Detection-as-code provides the flexibility, testability, and repeatability teams need to build data-driven security programs that can leverage CrowdStrike data to continually improve incident detection and response.



Key Benefits

Fast Setup

Start pulling your data quickly with Panther's native integration with CrowdStrike FDR.

Improved Security

Power more efficient incident investigations, forensics, and detection and response by storing your CrowdStrike Falcon data indefinitely.

Security Data Lake

Improve the quality of your alerts by leveraging CrowdStrike data with other data sets like AWS, Slack, Google Workspace and more.

Detection-as-Code

Apply flexible and scalable analysis to your CrowdStrike Falcon data with Python-based alert logic, test-driven development, and CI/CD workflows.

Business Value

Use Cases	Solution	Benefits
Data Retention	Panther parses, normalizes, and stores CrowdStrike Falcon logs in a high-scale security data lake for long-term retention.	End-to-end security visibility across CrowdStrike Falcon deployments, as well as additional value from the data to power forensics, alert triage, and investigations.
Monitoring DNS requests	Panther monitors activity across your CrowdStrike Falcon logs and applies Python-based detections to trigger real-time alerts.	Validate user activities in real-time across all FDR logs, CrowdStrike signatures/heuristics, Domain Name Server (DNS) data, and network connection logs to correlate data and set baseline behaviors.
Faster investigation and response	Panther ingests and normalizes your CrowdStrike data so you can leverage your logs for an additional layer of context to power high-fidelity threat detection and automated response.	Enrich CrowdStrike Falcon data and retain historic information so your security team can improve key metrics like Mean Time to Investigate (MTTI) and Mean Time to Respond (MTTD).

Key Capabilities

Improve Cloud Security Posture with Longer Data Retention

While CrowdStrike stores endpoint data temporarily, Panther enables organizations to store all of their CrowdStrike telemetry indefinitely to power more effective investigations and faster incident response.

Gain Better Insight and Security Visibility Across Cloud Services

Simply configure the Panther log-puller to gain visibility into user activity, CrowdStrike signatures/heuristics, Domain Name Server (DNS) data, and network connection logs.

Real-Time, Customized Alerting with Detection-as-Code

With Panther, security teams can use Python and test-driven development to build highly customized detections that enable advanced event analysis and high-fidelity alerts.

About Panther

Panther is a security analytics platform built to detect and respond to breaches at a cloud-scale. Security teams love using Panther for detection-as-code, extreme scalability, and low operational overhead. Trusted by Silicon Valley leaders like GitLab, Figma, Earnin, and many more. Panther comes fully integrated to CrowdStrike, and includes many other integrations, to make it easy to quickly analyze your data, triage alerts, and remediate incidents using the tools and data you have.

Request a demo

Extend CrowdStrike Falcon with detection-as-code and long-term telemetry storage in a security data lake today!

Request a Demo