Dataminr

Dataminr for Cyber Defense & Flashpoint

Enhance Attacker Insights and Defenses

Overview

Dataminr for Cyber Defense was specifically designed to help users understand adversaries, automate workflows, and mitigate threats faster using threat intelligence.

Flashpoint combines automation and human-driven data collection to delve into the internet's open and difficult-to-reach online spaces, providing a level of access that no other provider can. Access to this data, paired with timely, relevant, and accurate intelligence, enables organizations to take decisive actions to reduce risk and protect people, places, assets, and brand reputation.

Fully integrated, this solution enriches threat data and creates intelligence to provide insights to teams and prioritize their efforts. Dataminr for Cyber Defense provides a central place for users to see and analyze their team's data and integrate it with their security tools. With finished intelligence and technical indicators from Flashpoint, the solution delivers greater visibility than ever into threats, empowering experienced and entry-level users alike with the context they need to make better risk decisions about threats relevant to them.

The Dataminr for Cyber Defense & Flashpoint Advantage

The Flashpoint and Dataminr for Cyber Defense integration enhances investigations by centralizing access to highly relevant and actionable data and intelligence from the internet's open and difficult-to-reach sources. With access to this information within a single platform, security teams can effectively identify emerging threats, make informed decisions, and bolster their security posture.

Features

Finished Intelligence

The Finished Intelligence dataset provides access to analytical reports produced by Flashpoint subject matter experts. These human-digestible intelligence reports cover a broad spectrum of illicit, underground activity, from cybercrime & hacking to fraud, emergent malware, DDoS intelligence, hacktivism, violent extremism, and physical threats.

Technical Indicators

Enable users access to Indicators of Compromise (IoCs) and technical data across Flashpoint data sets and those included in Finished Intelligence Reports, allowing for seamless integration into users' workflows and automated tools.

Key Benefits

- **Apply Threat Intelligence for Enhanced Detection and Prevention:** Dataminr for Cyber Defense allows organizations to send threat intelligence to tools (like a SIEM or a firewall) as indicators of compromise and rules. This threat intelligence includes technical indicators from the open, deep, and dark web, and strategic insights on TTPs and threat actor activity from Finished Intelligence. Organizations can instantly see Platform ratings and observation count per indicator or incident.

- **Provide Context to Flashpoint Datasets with CAL (Collective Analytics Layer):** By distilling billions of data points from thousands of analysts and sources worldwide, Dataminr for Cyber Defense's CAL offers immediate insight into how widespread and relevant a threat is, providing global context that has never before been available. Insights from CAL provide additional context to information shared in Finished Intelligence to enable the network defender and intelligence teams to remediate and take relevant action to support their business operations.

- **Understand the Adversary with MITRE ATT&CK™:** Dataminr for Cyber Defense and Flashpoint have native MITRE ATT&CK functionality, providing organizations with a common language across the technology solutions. Intelligence is tagged with all related Techniques from the MITRE Pre-ATT&CK and Enterprise ATT&CK Datasets, enabling classification for further analysis and action.

How to Get Started

Request a demo on our website. To learn more about this particular integration, contact sales@dataminr.com. If you're an existing customer, please reach out to your customer success manager.