FLASHPOINT

IBM QRadar
INTEGRATION

Overview

The Flashpoint App for QRadar facilitates the delivery of Flashpoint technical intelligence and associated context specifically for QRadar users.

When consumed by a QRadar instance, Flashpoint Technical Indicators are added to QRadar reference sets and can be used in search, correlation, reporting, and visualization workflows in the same manner as other data, enhancing the user's ability to uncover and monitor malicious activity within their environment, as well as add context to investigations.

The Flashpoint & IBM QRadar Advantage

Leveraging Flashpoint's technical data and intelligence reports provides QRadar users with visibility into illicit online communities in order to correlate information related to their infrastructure, therefore, gaining insights in a timely manner and leveraging the ability to prioritize alerts based on impact and severity. Users are provided the ability to correlate activity across the enterprise network, as well as apply signature- and behavior-based detection methods to expose threats.

The Flashpoint App for QRadar enables Flashpoint data to be seamlessly integrated into customers' QRadar instances in order to notify customers when a match has been made between indicators from internal log data and Flashpoint intelligence.

Integrated Flashpoint Datasets

TECHNICAL DATA

Technical Indicators: Enable users access to indicators of compromise (IOCs) and technical data across Flashpoint datasets, including those found in Flashpoint Finished Intelligence reports, allowing for seamless integration into users' workflows and automated tools.

INTELLIGENCE REPORTS

Finished Intelligence: Access to analytical reports produced by our intelligence analysts. Reports cover a wide spectrum of illicit underground activity, including crimeware, fraud, emerging malware, violent extremism, and physical threats.

Installing the Flashpoint App for QRadar

The Flashpoint App for QRadar is available on —
exchange.xforce.ibmcloud.com/hub/extension/cc1c09107df16dbd2b09c1979c89f621
QRadar users download the App, deploy, and configure it using a Flashpoint API key.

Use Cases

INCIDENT RESPONSE (IR) & DETECTION

Organizations can leverage the Flashpoint App for QRadar to quickly query across Flashpoint technical data, expediting incident response investigations, as well as detecting illicit activity. This enables teams to enrich data collected during an investigation when response time is critical. On a daily basis, organizations collect large amounts of security event data, requiring significant resources to sift through, identify, and protect against a vast number of threat indicators. The Flashpoint App for QRadar enables security operations centers (SOCs) to quickly correlate high-fidelity IOCs curated by Flashpoint intelligence analysts with the client's security event data to automatically filter through the noise and prioritize significant threats.

CYBER THREAT INTELLIGENCE (CTI)

CTI analysts are able to query against Flashpoint Technical Indicators to find data related to specific malware and threat actors. This allows analysts to generate alerts for new IOCs related to priority threat actors and groups. More specifically, it enables hunt teams to query Flashpoint technical data to identify and pivot off known threats to find additional indicators, as well as proactively uncover threats across the enterprise.

CTI teams can search malicious hashes, IPs, and domains to determine if any systems have communicated with known IOCs, as well as pivot directly to Flashpoint Finished Intelligence within QRadar to read associated Flashpoint analyses.

Key Features

REAL-TIME AND HISTORICAL THREAT DETECTION

Based on rules, IOCs and pattern-matching to find known and emerging threats

SEAMLESS INSTALLATION

The integration can be installed directly from within the IBM Security App Exchange

REFERENCE SETS AND REFERENCE TABLES

The integration can be installed directly from within the IBM Security App Exchange

ACCESS BASIC RULES

IP, Domain, URL and Hash (MD5, SHA1 and SHA256) rules are included

VIEW FLASHPOINT CONTEXT

Summary pages for offenses that are generated by Flashpoint rules

VIEW FLASHPOINT FINISHED INTELLIGENCE

Available directly in the QRadar browser without having to log into the Flashpoint Intelligence Platform

For more information on the Flashpoint App for QRadar contact: **ibmqradar_support@flashpoint-intel.com**

ABOUT FLASHPOINT

Flashpoint delivers converged intelligence and risk solutions to private and public sector organizations worldwide. As the global leader in Business Risk Intelligence (BRI), Flashpoint provides meaningful intelligence to assist organizations in combating threats and adversaries. Through sophisticated technology, advanced data collections, and human-powered analysis, Flashpoint is the only intelligence firm that can help multiple teams across an organization bolster cybersecurity, confront fraud, detect insider threats, enhance corporate and physical security, improve executive protection, address third-party risk, and support due diligence efforts.

For more information, visit **www.flashpoint-intel.com** or follow us on Twitter at **@FlashpointIntel**

ABOUT IBM SECURITY

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 70 billion security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide.

For more information, please check **www.ibm.com/security**, follow **@IBMSecurity** on Twitter or visit the IBM Security Intelligence blog at **www.securityintelligence.com**