IBM X-Force Exchange SDK

Delivering robust threat intelligence through a feature-rich analysis framework from IBM X-Force

Highlights

- Access accurate and up-to-date information on three key types of threat intelligence: URL categorization, IP reputation, and web application profiles
- Optimized for fast access to threat intelligence for high throughput applications
- Provide access to a databases containing more than 38 billion evaluated web pages and images, 850,000 evaluated IPs, and 3,900 applications and actions
- Enable easy integration, flexible configuration, built-in licensing and customized ticket options

Threat intelligence has become a standard and essential part of the tools that security users and businesses require to provide the most accurate information on the latest threats. IBM X-Force Exchange Software Development Kit (SDK) leverages the X-Force's skills and extensive infrastructure to help deliver and maintain a set of threat intelligence focused on the areas of URL filtering, IP reputation, and web application profiles.

This same intelligence is built into the IBM X-Force Exchange collaborative threat intelligence sharing platform, and is also available for integration into third-party security products. Security vendors that want to protect their clients from potentially malicious and inappropriate web content can rely on the IBM X-Force Exchange SDK for up-to-date threat intelligence and analysis—along with an easy-to-implement application programming interface (API).

The three components of effective threat intelligence production include a robust content analysis process, a vast amount of data and the means to analyze that data. The X-Force Exchange SDK uses all three components to provide robust, effective Internet filtering, reputation scoring, and application categorization.

- IBM analysis platform classifies millions of web pages, using intelligent algorithms and massive, parallel computing
- The IBM solution continuously crawls the Internet, collecting images, binaries and other content for processing and analysis
- The platform manages multiple database clusters to cache and store information about websites' hyperlink structures, images, website text, and other important content
- As an OEM partner, you can use the X-Force Exchange SDK to add value to existing security offerings and deliver advanced technology that can help decrease the risk posed to end clients by unwanted Internet content, classified by URLs, IPs, and web applications.

URL Filtering and Categorization

Using the URL filtering capability of the SDK, you can deliver robust, ongoing content analysis for your clients. IBM employs fully automated web crawlers to scan the Internet and inspect millions of new and updated websites every day. Currently, the URL filter list contains more than 130 million entries with more than 25 billion evaluated web pages and images indexed into 73 categories. Every day, clients receive updates that encompass nearly 150,000 updated and newly categorized websites. In addition, IBM filter technology covers 45 languages and 250 countries.

Web filtering technology analyzes websites in depth, including text, images and links, to provide granular filtering of web content. IBM filtering analysis technologies available from the X-Force Exchange SDK include:

- Text classification - includes keyword search, optical character recognition for relevance and accuracy, and analysis of frequency and word combination
- Comparison of similarity and identity - determines similarity among websites based on text, images or other website elements
- Object recognition - analyzes each image for special signs, symbols, trademarks, forbidden images and so on
- Pornography and nudity detection - detects a high concentration of flesh tones in images
- Structure and Linkage Analysis - analyzes how websites link to one another in order to classify URLs; for example, if nine out of 10 links go to pornographic sites, there is high probability that the tenth link also leads to a pornographic site
- Malware detection - inspects all web pages, binaries and installation packages for malware
- Geolocation - geographically pinpoints the location of servers by IP address, lowers the reputation score of IP addresses in certain geographies known for malicious traffic, and allows administrators to f lag or block traffic from certain geographies

IP Reputation

The X-Force Exchange IP reputation capability of the SDK provides accurate information on close to one million malicious IPs with frequent and consistent analysis of this information for your clients. For example, a user can look up IP addresses for all traffic coming across the network and block any traffic that does not meet the user-defined threshold.

IP reputation technology analyzes websites in depth to provide insights on the content of an IP, its behavior, and the domains that it hosts. IBM technologies available from the X-Force Exchange IP Reputation SDK include:

- Categorization - IP categorization is focused on malicious categories including spam, anonymous proxies, dynamic IPs, malware, and botnet command & control servers.
- Reputation Score - assigns a number (on a scale from 1 to 10) to individual IP addresses to help determine the risk level for malicious activity. This reputation score is adjusted for the IP activity and behavior to accommodate the dynamic nature of IPs. For example, an IP that is categorized as sending spam will be monitored for the volume and frequency with which spam is sent; if the volume and/or frequency decreases, the reputation score will decrease accordingly.
- Multiple sources - in addition to the organic collection and analysis capabilities of the X-Force team, IBM aggregates information from both open-source and proprietary providers of threat intelligence to augment the overall information it provides to clients. By doing so, it helps provide broader coverage for the vast set of threat intelligence available.

Web Application Profile

The X-Force Exchange Web Application profile capability of the SDK provides accurate information on thousands of web applications and the user actions provided by those applications.

This capability can allow a product to filter and control the uses of web applications by users. For example, administrators can set a policy that allows users to browse Facebook but not to view or upload video.

Web application profile technology analyzes websites in depth to provide insights on the application itself as well as the actions that a user can take with that application. IBM technologies available from the X-Force Exchange web application profile SDK include:

- Web application control - recognizes the URL semantics of a wide array of web applications to enable administrators to disallow certain activity on web-based applications.
- Actions - potential actions for web application include audio/video chat, share, software updates, opening an app, stream/download, and write/post/chat.
- Regular updates - IBM monitors thousands of web applications for changes in the form and functionality to provide up-to-date information as they get updated.

Using the IBM X-Force Exchange SDK

The X-Force Exchange SDK was designed with an easy-to-implement API, allowing you to categorize URLs, define web-application policies, query for IP reputation, and configure other filtering capabilities. IBM provides two methods for accessing the threat intelligence databases: integrated filter database access for large installations and hosted filter database access with automatic load balancing. The SDK also has the capability to automate daily filter database updates, and offers a built-in software licensing system to handle subscription expiration and demo licenses. The SDK also enables OEM partners to use their own license types. Supported platforms include:

- Microsoft Windows, the import library and all source files are compatible with Microsoft Visual Studio
- Linux distributions (32 bit and 64 bit)

Choosing the right option

IBM X-Force Exchange supports both the SDK and a Commercial API to integrate threat intelligence into security operations and solutions.

IBM X-Force Exchange SDK vs API	
SDK	Commercial API
Subset of available threat intelligence information, including including IP and URL reputation, and web applications	Complete set of contextual threat intelligence, including IP and URL reputation, web applications, malware and campaign intelligence, vulnerabilities, and more
Integrated coding with a product as an OEM/ASL partnership	Developer flexibility for the language / tools of their choice
Optimized for fast access with low latency	Cloud service response times

Why IBM X-Force?

As one of the oldest and most established commercial security research groups, IBM X-Force delivers products and services that help protect against Internet threats. IBM X-Force offers a strong portfolio of content security products and software development kits for web application control, IP reputation analysis and geolocation capabilities, malware analysis, and more. IBM X-Force also maintains one of the world's largest URL databases for web and spam filtering.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

For more information

To learn more about the IBM X-Force Exchange Software Development Kit, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security/xforce.

IBM Security

75 Binney Street

Cambridge, MA 02142

Produced in the United States of America

June 2017