IBM X-Force Exchange

Changing the way security analysts research, collaborate and act on threat intelligence

Highlights

- Research the latest threats through an interactive platform
- Create Collections to investigate incidents
- Collaborate with peers to identify priority threat intelligence
- Set notifications on Collections, vulnerabilities, and critical breach indicators
- Push intelligence to enforcement points to help speed time to act

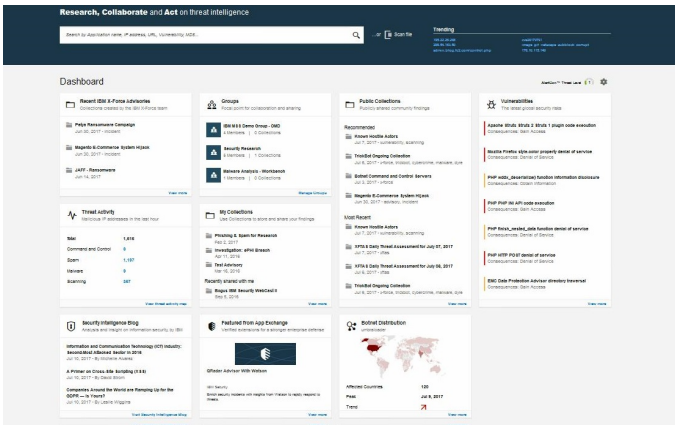
IBM® X-Force® Exchange is a cloud-based threat intelligence sharing platform that enables users to rapidly research the latest global security threats, aggregate actionable intelligence, consult with experts and collaborate with peers. IBM X-Force Exchange, supported by human- and machine- generated intelligence, leverages the scale of IBM X-Force to help users stay ahead of emerging threats.

Many enterprises use external threat intelligence to enhance their security decision making—but lack the critical support that's required to make the most of that information. Security teams use multiple sources of intelligence to identify threats, which can be time-consuming—and the sources are not always trustworthy. Too often, information cannot be processed quickly enough to make a significant impact, offering little protection.

IBM X-Force Exchange offers:

- A robust research platform with access to a wealth of threat intelligence data
- Context for threat indicators, delivered from a mix of human-and machine-generated insights
- A collaborative environment for sharing threat intelligence
- An integrated SaaS solution to help quickly discover and act on threats
- An easy-to-use interface for organizing and annotating findings
- Optional SaaS add-on features to enhance integration and analysis

Curated threat intelligence from a wide range of sources

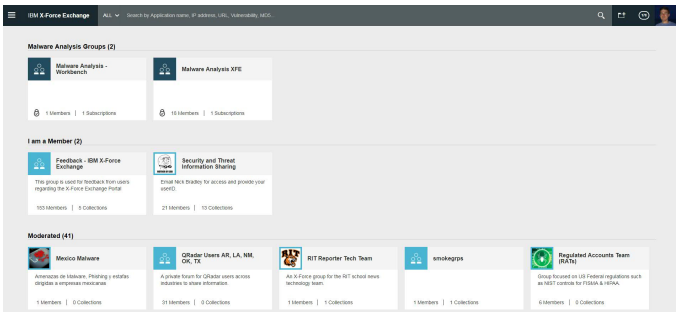


The homepage for IBM X-Force Exchange features customizable cards to show the latest vulnerabilities, advisories, botnet activity, and public Collections, as well as current security thought leadership blogs from SecurityIntelligence.com.

IBM X-Force Exchange provides timely, curated threat intelligence powered by data from crawler robots, honeypots, darknets, spamtraps, and other machine-generated threat intelligence. Thousands of malicious indicators are classified every hour, continuously refreshing threat intelligence within the platform. The data sources behind X-Force Exchange include:

- One of the world's most comprehensive databases of known security vulnerabilities
- Anonymized threat information from monitoring billions of security events daily
- Real-time global threat intelligence from millions of endpoints
- Data based on threat monitoring of billions of web pages and images
- Deep intelligence on millions of spam and phishing attacks
- Reputation data with thousands of malicious IP addresses
- Millions of malware samples, backed by a behavior-based sandbox with a continuous flow of new user-contributed samples
- Human intelligence from security experts including industry peers, IBM X-Force researchers and IBM Security professionals adds context to machine-generated data.

Collaborate and share threat intelligence with peers



Groups and Collections are key collaboration areas within IBM X-Force Exchange.

The X-Force Exchange platform facilitates making connections with industry peers to validate findings and research threat indicators. Users can engage peers, IBM Security professionals and IBM X-Force researchers, all within IBM X-Force Exchange, by sharing Collections or commenting on reports. This can add context to threats through peer collaboration to help separate the signal from the noise, aid in forensic investigations and lead to crowd-sourced intelligence.

The groups function allows users to create a private workgroup and choose the set of X-Force Exchange users with whom they wish to collaborate and share information. The group owner can add and remove users, choose those Collections for group collaboration, and assign permissions to members of the group.

Employ case file management to streamline workflow

Collections allow users to aggregate the threat intelligence that is collected during an investigation, organize information and share it with other users. In creating a Collection, users can:

- Describe the details of the investigation with text-editing features
- Add structured threat intelligence reports relevant to the investigation, with a snapshot of the information at the time it was added for proper context
- Compile other associated content, including screen shots, videos or other files
- Link Collections to create associations between related investigations
- Import threat intelligence via file, copy-and-paste or STIX format for faster upload of information

Users can create Collections in a number of ways to meet their needs. With the Quick Collection feature, new Collections can be created by adding recently viewed reports from the user sidebar. New Collections can also be created through the email inbox feature. With this capability, forwarding an email of IP addresses or md5 hashes, or even a suspicious spam email can be used to create a new Collection. There are three different ways to use the email inbox feature:

- Per user: Emails sent to this inbox generate a new private Collection for the user.
- Per group: Here, emails will create a new shared Collection for the group, which can be either public or private, based on the group access settings.
- Per Collection: Emails sent to this inbox will be added to an existing Collection.

Once a Collection is created, users can continue working with the Collection as usual and invite individual colleagues or peers to add insights, or share the Collection publicly to pass on important findings with a broad audience or gain detailed insights from other researchers.

To stay on top of the most current data, analysts can also follow a public or shared Collection to be notified of updates. Additionally, users can create a Watchlist of relevant vulnerabilities to their infrastructure so they don’t miss a critical notification.

For more information

To use the platform, visit xforce.ibmcloud.com. To learn more about this offering 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

July 2017