IBM Security X-Force Threat Intelligence

Use dynamic IBM X-Force data with IBM Security QRadar to detect the latest Internet threats

Highlights

- Automatically feed IBM® X-Force® data into IBM QRadar® Security Intelligence Platform analytics
- Enrich QRadar threat analysis capabilities with up-to-the-minute data on Internet threats
- Leverage the additional threat context provided by IBM Security X-Force Threat Intelligence to gain deeper insight—and greater protection
- Prevent or minimize the impact of today's complex and serious security attacks

As security threats steadily increase in volume and sophistication, it's becoming more challenging to identify the most serious ones. Users must correlate threat information from multiple sources to make more informed decisions about which security issues pose the biggest threats to their organizations. This is particularly true on today's smarter planet, where instrumented, interconnected and intelligent businesses collect, process, use and store more information than ever before. With today's large variety of incoming attacks, it can be extremely difficult to detect and analyze ever-changing threats—much less to turn collected threat data into actionable insights that consistently identify which threats are most dangerous.

A solid security foundation designed to meet this need is IBM QRadar Security Intelligence Platform, an integrated family of products that helps detect and defend against threats by applying sophisticated analytics to more types of data. In doing so, the platform helps identify high-priority incidents that might otherwise get lost in the noise. And you can extend these comprehensive analytics still further, using IBM Security X-Force Threat Intelligence to augment QRadar intelligence capabilities by feeding it proprietary threat insights, including data on malware hosts, spam sources and anonymous proxies. Combining worldwide intelligence from IBM X-Force with security information and event management (SIEM), log management, anomaly detection, and configuration and vulnerability management capabilities from QRadar solutions provides users with additional context on security incidents, helping improve prioritization of incidents that require additional examination—and enabling organizations to prevent or minimize damaging attacks.

Address growing security threats head on

Tens of thousands of malware samples are created every day, with new classes of threats continually added to and improved upon. Sophisticated hackers use polymorphic programs to alter malware into new form factors after each delivery. And all of this is exacerbated by the proliferation of mobile devices, cloud computing and virtualization—in fact, the intersection of these technologies provides fertile new ground for threats and malware.

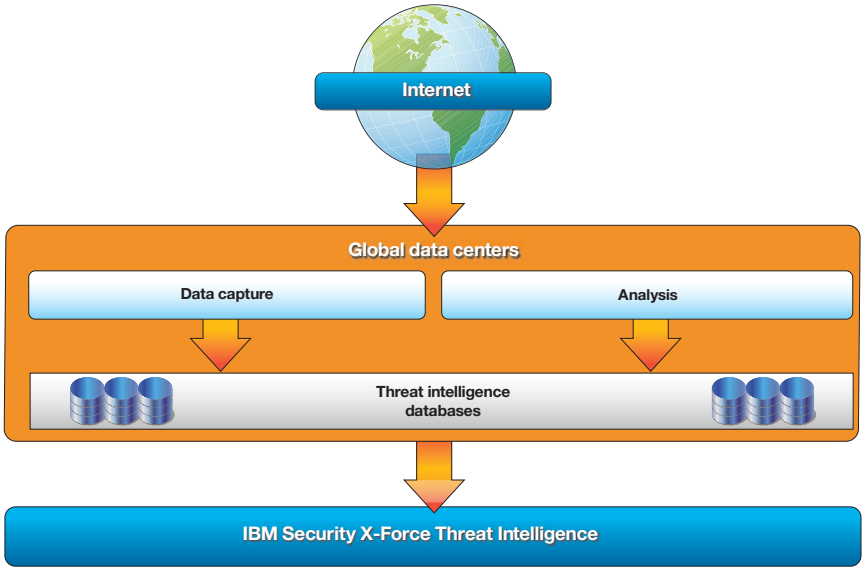
In addition, today's attacks are often not random, but targeted for maximum financial gain and impact. Rogue individuals and groups are constantly innovating new ways to attack organizations' critical data. As a result, traditional methods of dealing with Internet threats are no longer enough. Organizations need visibility into a much wider range of threat data than ever before in order to protect themselves most effectively. Adding X-Force Threat Intelligence to the QRadar Security Intelligence Platform can provide the extra intelligence required to go up against these modern-day threats.

Channel the power of IBM X-Force

X-Force Threat Intelligence is much more than just a compilation of threat data. Behind it is the power of the IBM X-Force research and development team—one of the best-known commercial security research groups in the world. This team of security experts provides the foundation for the IBM preemptive approach to Internet security by focusing their attention on researching and evaluating vulnerabilities and security issues, developing assessments and countermeasure technologies for IBM products, and educating users about emerging Internet threats and trends.

X-Force is instrumental in protecting users against the threat of attack because their knowledge base and data-collection methods are unmatched in the industry. From a vulnerability perspective, the team maintains and analyzes one of the world's most comprehensive databases of known security vulnerabilities, with more than 70,000 entries, including detailed analyses of every notable public vulnerability disclosure since 1994. From a threat perspective, the team tracks billions of security incidents daily, monitors millions of spam and phishing attacks, and has

The value of the IBM X-Force research and development team



The X-Force research and development team inspects millions of new and updated Internet sites every day, collects information, categorizes content and identifies those sites that pose a security danger to an organization.

analyzed billions of web pages and images. X-Force maintains a global research footprint that delivers unequaled security research and threat mitigation technology to IBM users.

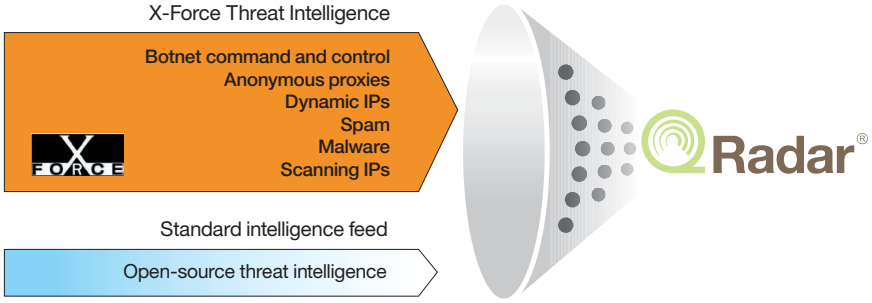
In addition to relying on their own findings, the X-Force team collects data from multiple research sources, researching all publicly disclosed vulnerabilities, consuming commercial vulnerability data and monitoring the underground for zero-day vulnerabilities. It also collaborates with the world's leading businesses and governments, vertical sector information sharing and analysis centers, global coordination centers, and other product vendors to provide complete data. Finally, from an engineering perspective, the team analyzes proof of concepts and public exploit code. By monitoring global Internet threats around the clock and updating the IBM Internet Security Systems AlertCon resource center in real time, the X-Force team helps keep IBM users abreast of the current global Internet threat level at all times.

QRadar users gain access to all of these benefits when they add the proprietary threat insights of X-Force Threat Intelligence to QRadar Security Intelligence Platform.

Enhance QRadar capabilities with X-Force

X-Force Threat Intelligence leverages the X-Force research and development team's skills and infrastructure to provide additional insight into and context for security situations that involve IP addresses of a suspicious nature. By categorizing IP addresses into segments such as malware hosts, spam sources and anonymous proxies, this IP reputation data can be incorporated into QRadar rules, offenses and events. This allows for capturing events more quickly and accurately than previously possible, as well as for capturing them in a way that provides additional understanding for further analysis.

Enhance IBM Security QRadar with IBM Security X-Force Threat Intelligence



Using X-Force Threat Intelligence with QRadar provides valuable capabilities beyond those included in the standard QRadar intelligence feed, such as frequent updates, in-house analytics, confidence ranking and comprehensive coverage.

Leveraging X-Force Threat Intelligence in conjunction with QRadar rules enables users to more precisely detect dangerous network activity.

X-Force IP reputation data is constantly updated and maintained, and the content in these feeds is given relative threat scoring. This enables QRadar users to prioritize incidents and offenses generated through this content. The data from these intelligence sources is automatically incorporated into the QRadar correlation and analysis functions and serves to greatly enrich its threat detection capabilities with up-to-the-minute Internet threat data. Any security event or network activity data seen involving these addresses is automatically flagged, adding valuable context to security incident analyses and investigations.

Users can also incorporate the latest X-Force security threat advisories and informational updates into the QRadar dashboard. This dashboard includes the current X-Force AlertCon level, which provides users with a quick and concise indicator of current Internet threat conditions.

Using X-Force Threat Intelligence with QRadar Security Intelligence Platform is simple and fast—once users have added these threat insights they will immediately begin receiving advanced threat data automatically and seamlessly.

Get the most value out of additional threat intelligence

X-Force Threat Intelligence provides vulnerability coverage across a wide range of use cases, including:

Security issue	Insight provided
A series of attempted logins from a dynamic range of IP addresses	Malicious attacker
An anonymous proxy connection to a business partner portal	Suspicious behavior
A connection from a non-mail server with a known spam host	Spam contamination
A connection between an internal endpoint and a known botnet command and control	Botnet infection
Communication between an endpoint and a known malware distribution site	Malware attack

By adding the dynamic information from X-Force Threat Intelligence to the analytical capabilities of QRadar Security Intelligence Platform, users can gain more intelligent and accurate security enforcement. This additional insight from X-Force Threat Intelligence enables QRadar users to apply this valuable data in real time to more closely monitor—and tightly secure—their environment.

Why IBM?

A preemptive security approach requires market-leading research, a keen eye for attack trends and techniques, and a streamlined and affordable platform for delivering advanced security solutions that are knowledge-based. IBM commands the extensive knowledge, innovative research methods and complex technologies required to achieve preemptive security—designed to protect your entire IT infrastructure, from the network gateway to the desktop.

For more information

To learn more about IBM Security X-Force Threat Intelligence, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

About IBM Security solutions

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 and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2013

Please Recycle

WGD03025-USEN-00