**IBM Advances Security Intelligence to Help Organizations Combat Increasing Threats**
**Wednesday, February 22, 2012 02:00:00 PM (GMT)**

**To help customers better predict**
**prevent and detect breaches across an organization**
**IBM to tap security analytics and threat intelligence from more than 400 sources**
**including the X-Force Threat Feed**

ARMONK, N.Y., Feb. 22, 2012 /PRNewswire/ -- IBM (NYSE: IBM) today unveiled new capabilities planned for its security intelligence platform designed to combine deep analytics with real-time data feeds from hundreds of different sources to give organizations, for the first time, the ability to help proactively protect themselves from increasingly sophisticated and complex security threats and attacks using a single platform.

(Photo: http://photos.prnewswire.com/prnh/20120222/NY57559-a )

(Photo: http://photos.prnewswire.com/prnh/20120222/NY57559-b )

(Logo: http://photos.prnewswire.com/prnh/20090416/IBMLOGO )

Organizations today are struggling to defend themselves against an onslaught of ever-evolving data breaches, such as theft of customer and employee information, credit card data and corporate intellectual property. To date, many corporations have been unable to create a security defense system because they have cobbled together technologies that don't integrate in an intelligent and automated fashion.  This patchwork approach has created loopholes that hackers can exploit.

The QRadar Security Intelligence Platform, designed by Q1 Labs and acquired by IBM last fall, tackles this problem head-on by serving as a control center that integrates real-time security intelligence data to include more than 400 different sources.

Major breakthroughs planned in the security platform include:

- **Threat Intelligence** – Intelligence from one of the world's largest repository of threat and vulnerability insights is planned to be available based on the real-time monitoring of 13 billion security events per day from the IBM X-Force Threat Intelligence Feed. This insight can flag behavior that may be associated with Advanced Persistent Threats, which may emanate from teams of attackers accessing networks through stealth means.
- **Visibility into Enterprise Activity** – The platform will unite events from IBM and non-IBM products that span four areas of organizational risk – infrastructure, people, applications and data.
- **Pinpoint Analysis in an Age of Big Data** – The platform can drill down to basic data elements to help analyze issues emanating from network access information at the periphery to database activity at the core of a business.

"Trying to approach security with a piece-part approach simply doesn't work," said Brendan Hannigan, general manager, IBM Security Systems. "By applying analytics and knowledge of the latest threats and helping integrate key security elements, IBM plans to deliver predictive insight and broader protection."

With new integrations to be made available, the analytics platform can quickly identify abnormal activity by combining the contextual awareness of the latest threats and methods being used by hackers with real-time analysis of the traffic on the corporate IT infrastructure. For example, the future integrations permit the platform to detect when multiple failed logins to a database server are followed by a successful login and access to credit card tables, followed by an upload to an unknown site.

"We chose the QRadar platform to build on and deliver our vision of a streamlined, highly intelligent platform to serve as our central nervous system for enterprise-wide monitoring," said Ken Major, Information Security Officer at AmeriCU Credit Union. "It enables us to achieve our goals, industry best practices and regulatory compliance."

## Threat Intelligence

One of the significant planned integrations for the QRadar platform is IBM's X-Force Intelligence Threat Feed based on the real-time monitoring of 13 billion security events per day, on average, for nearly 4,000 clients in more than 130 countries. The QRadar platform will have visibility into the latest security trends worldwide to help protect enterprises against emerging risks. QRadar will present current IBM X-Force threat feeds in dashboard views for users, and correlate an organization's security and network events with these threats and vulnerabilities in real-time using automated rules.

## Broad Coverage

Other planned integrations to allow the QRadar Security Intelligence Platform to help clients more rapidly identify threats by connecting events from the following categories:

- **People:** Organizations should control access to key systems and information. An employee's unauthorized access to key databases and client information can leave a firm vulnerable to security breaches. With security intelligence, security teams can quickly determine whether access patterns exhibited by a given user are consistent with the user's role and permissions within the organization. *IBM Security Identity Manager* and *IBM Security Access Manager* will integrate with the QRadar platform, complementing QRadar's existing support for enterprise directories such as Microsoft Active Directory.
- **Data:** Data is at the core of security; it is what's behind every security measure in place, and is the primary target of cyber-criminals. With *IBM Guardium Database Security* integrated with the security intelligence platform, users will be able to better correlate unauthorized or suspicious activity at the database layer – such as a database administrator accessing credit card tables during off-hours – with anomalous activity detected at the network layer, such as credit card records being sent to unfamiliar servers on the Internet.
- **Applications**: Applications are vital to day-to-day function but can also introduce new and serious vulnerabilities into company networks. Applications, because of their sensitivity, should be updated frequently. Organizations however are often unable to patch immediately due to corporate testing requirements and change control cycles. With security intelligence, companies will be able to automatically alert security teams to unpatched Web applications that risk being attacked by known application-layer exploits  that have previously been identified by *IBM Security AppScan*. This planned integration complements existing QRadar support for monitoring enterprise applications such as IBM WebSphere and SAP ERP.
- **Infrastructure**: Today, organizations struggle to secure thousands of physical devices, such as PCs and mobile phones, especially as Bring Your Own Device (BYOD) continues to grow in popularity. For this reason, companies should take extra precautions to help employees to follow secure practices in using these devices. With *IBM Endpoint Manager* integration, the security platform can provide organizations with enhanced protection of physical and virtual endpoints: servers, desktops, roaming laptops, smartphones and tablets, plus specialized equipment such as point-of-sale devices, ATMs and self-service kiosks.

QRadar integration modules are also planned for Symantec DLP, Websense Triton, Stonesoft Stonegate and other third-party products, increasing QRadar's ecosystem and continuing Q1 Labs' long-standing approach to multi-vendor heterogeneous environments.

## Solutions to Analyze Big Data

In addition, the QRadar platform has been expanded with Big Data capabilities for storing and querying massive amounts of security information, and functionality for helping to secure virtualized infrastructures and providing a new level of visibility that helps clients reduce security risk and automate their compliance processes.

The expansion of security and network data sources is complemented by advanced functionality to help organizations keep pace with their exponential data growth. The new deliverables include:

- **Instant Search** to provide high-speed, free-text querying of both log and flow data, designed to bring the simplicity and speed of Internet search engines to the security intelligence solution.
- The **XX24 appliance series** to extend the scalability and performance advantages for which QRadar solutions are well known. With the release of the QRadar 3124 SIEM appliances, QRadar 1624 Event Processor and QRadar 1724 Flow Processor – which all include 16TB of usable storage and 64GB of RAM – organizations can support more users, achieve higher performance and store data longer.

- **Intelligent data policy management** to enable users to designate which information they want to store and for how long. Less important data can be removed sooner to achieve longer retention for more important data.
- **Virtual appliances** to allow end customers and service providers to capitalize on the virtual infrastructures they have built, while benefiting from lower-priced yet fully capable security intelligence solutions.

The planned integration modules (device support modules) are expected to be included with QRadar SIEM and QRadar Log Manager at no additional cost, via automatic updates.

**Availability**

The Big Data and virtual infrastructure enhancements are available now. QRadar integration modules for IBM Guardium Database Security are planned to be available in 1Q2012.

Integration modules for IBM X-Force Threat Intelligence, IBM Security Identity Manager, IBM Security Access Manager, IBM Security AppScan and IBM Endpoint Manager are planned to be available in 2Q2012. For more information, please visit www.q1labs.com.

**About IBM**

Q1 Labs was acquired by IBM in October 2011, and serves as a cornerstone of IBM's new Security Systems division. IBM's security portfolio provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, network security and more. IBM operates the world's broadest security research and development organization and delivery organization. This comprises nine security operations centers, nine IBM Research centers, 11 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM monitors 13 billion security events per day in more than 130 countries and holds more than 3,000 security patents.

For more information on IBM security, please visit: www.ibm.com/security.

For a video on the topic of IBM Security Intelligence, please visit: http://www.youtube.com/watch?v=-YTikwDcwZ4

*IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.*

*"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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a 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 SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY. "*

Contacts:
Nicole Trager
IBM Media Relations
781-250-5829
ntrager@us.ibm.com

Colleen Haikes

IBM Media Relations
415-545-4003
chaikes@us.ibm.com

SOURCE IBM

**Countries:** United States
**Industries:** Computer Electronics, Hardware & Software, High Tech Security
**Languages:** English
**Primary Identifiers:** IBM-US
**Related Identifiers:** IBM-US
**Subjects:** New Products & Services