Communiqués de presse

IBM promeut la «Security Intelligence» afin d’aider les entreprises à combattre la montée des menaces

Afin de mieux prédire, prévenir et détecter les infractions au sein des organisations, IBM puise dans 400 sources différentes, y compris X-Force Research, pour mettre en place une sécurité analytique ainsi qu’une veille des menaces.

Paris - 22 févr. 2012: IBM annonce aujourd’hui la création d’une nouvelle plateforme de «Security Intelligence » qui combine d’importantes facultés d’analyse avec une mise à jour des données en temps réel venant de différentes sources. Elle a pour objectif de donner l’opportunité aux organisations de se protéger de façon proactive des menaces et des attaques, à la fois croissantes et complexes, qui pèsent sur leur sécurité, et qui ne cessent de grandir.

Des avancées majeures ont été intégrées dans la plateforme de sécurité, notamment :

- La toute dernière innovation en terme d’industrie intelligente. En effet, sont désormais couplées les capacités d'analyse de la plus grande base mondiale de connaissances sur les menaces, la vision des vulnérabilités fournie via la surveillance de plus de 13 milliards d'événements élémentaires quotidiens et la X-Force. Cette capacité unique permet d'identifier les APT (Advanced Persistent Threats), provenant d'équipes de pirates professionnels furtifs et les tentatives d'intrusion informatique, de contournement des défenses, qui se sophistiquent incroyablement...

- Une solution des plus complètes. Désormais, la plateforme regroupe l’ensemble des produits du framework sécurité IBM – infrastructure, gestion des identités et des accès, applications et données. Aucun autre spécialiste de sécurité ne couvre aussi bien l’éventail de ces solutions, qu’il s’agisse de solutions IBM ou non.

- Une grande précision au regard des points critiques, indispensable dans un environnement de Big Data : c’est-à-dire la capacité de couvrir et corréler les risques émanant des données même les plus élémentaires. Qu’il s’agisse d’informations périphériques d’un réseau ou de l'activité d'une base de données centrale, la sécurité doit désormais être intégrée au cœur du métier.

****

IBM Advances Security Intelligence to Help Companies Combat Increasing Threats

To help customers better predict, prevent and detect breaches across an organization, IBM taps security analytics and threat intelligence from more than 400 sources, including the X-Force threat feed

ARMONK, N.Y. – 22 Feb 2012: IBM (NYSE: IBM) today unveiled new capabilities to its security intelligence platform that combines deep analytic capabilities 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.

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, acquired by IBM last fall, is the first system to tackle this problem head-on by serving as the control center that integrates real-time security threat intelligence data from more than 400 different sources.

Major breakthroughs in the security platform include:

- **Latest Thread Intelligence**– Now linked is the intelligence from one of the world’s largest repository of threat and vulnerability insights based on the real-time monitoring of 13 billion security events per day from the IBM X-Force threat feed. This insight can flag behavior that may be associated with Advanced Persistent Threats, may emanate from teams of attackers that may access networks through stealth means.

- **Visibility into Enterprise Activity** – The platform now unites insights from products that span all four areas of organizational risk-- infrastructure, identity management, applications and data. This provides exceptional breadth of coverage for both IBM and non-IBM solutions.

- **Pinpoint Risk in an Age of Big Data** – The platform can surface and correlate risk 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 can 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 a questionable site.

Threat Intelligence

One of the significant new sources feeding the QRadar platform is IBM’s X-Force threat feed based on real-time monitoring of 13 billion security events per day, on average, for nearly 4,000 clients in more than 130 countries. This marks the first time that X-Force‘s threat intelligence is being incorporated into a security intelligence solution. The QRadar platform will now get visibility into the latest security hotspots worldwide and help protect users 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 activity with these threats and vulnerabilities in real-time using automated rules.

Broad Coverage

Here are the product integrations that allow the QRadar Security Intelligence Platform to help clients more rapidly identify attacks by connecting events from the following categories:

- **People**: Organizations should control employee access to 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 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 can 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 public 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 can now automatically alert security teams unpatched Web applications are being attacked using known application-layer vulnerabilities that have previously been identified by IBM Security AppScan. This 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 integration with IBM Endpoint Manager, 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.

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

Solutions to Analyze Big Data

In addition to the product integrations, there are new Big Data capabilities for storing and querying massive amounts of security information, and new functionality for helping to secure virtualized infrastructures, provide a new level of visibility that helps clients reduce security risk and automate their compliance processes.

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

Instant Search provides high-speed, free-text querying of both log and flow data, bringing the simplicity and speed of Internet search engines into the security intelligence solution.

The **XX24 appliance series** extends 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 enables 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 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.

New integration modules (device support modules) are included with QRadar SIEM and QRadar Log Manager at no additional cost, via automatic updates.

Availability

QRadar integration modules for IBM Guardium Database Security, as well as Big Data and cloud enhancements described above, 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.