Communiqués de presse

IBM renforce la sécurité grâce au big data

L'analytique aide les entreprises à traquer les cyber-attaques

Paris, France - 04 févr. 2013: Le paysage de la sécurité est en profonde mutation. En cause, les attaques avancées, la fraude généralisée, l'utilisation croissante des médias sociaux, la mobilité et le cloud. Alors que les entreprises doivent gérer une masse croissante de données, la façon dont la donnée d'entreprise doit être protégée change rapidement.

Pour aider à la détection des menaces furtives qui peuvent se cacher dans la masse grandissante des données, IBM annonce aujourd'hui IBM Security Analytics with Big Data qui combine la sécurité intelligente avec de grandes capacités d'analyse de données, tant pour les cyber-menaces externes que pour la détection des risques technologiques et leur prévention. IBM Security Analytics with Big Data fournit une approche complète qui permet aux analystes en matière de sécurité d'étendre leurs analyses bien au-delà des simples données de sécurité pour traquer les cyber-activités malveillantes.

Cette nouvelle solution combine la corrélation en temps réel pour une compréhension continue, l'analytique personnalisée à travers une structure de masse (comme les alertes de sécurité des terminaux, les journaux, les transactions DNS et le flux réseaux) les données non structurées (telles que les courriers électroniques, les médias sociaux et les transactions métiers) et les capacités d'analyse scientifique visant à obtenir des preuves irréfutables. Cette combinaison aide les organisations à relever les défis de sécurité les plus critiques, parmi lesquels les menaces persistantes avancées, la fraude et les menaces internes.

« *Les cybercriminels ont à leur disposition des moyens technologiques de plus en plus sophistiqués. C'est pourquoi l'industrie financière et les gouvernements doivent migrer vers un modèle axé sur le risque qui prend en compte la nature des menaces* » explique **Mark Clancy, RSSI et Responsable des risques technologiques chez Depository Trust & Clearing Corporation - DTCC**. « *Nous devons passer d'une position passive face aux alertes et aux données de sécurité, à une situation où l'on traque activement les cybercriminels sur nos réseaux. La solution IBM Security Analytics with Big Data nous donne une meilleure visibilité sur notre environnement. Nous suivons en temps réel l'état de notre sécurité et avons une vue significative de notre historique sur plusieurs années*. »

"*En tirant le meilleur parti de l'ensemble des ressources IBM, nous étendons continuellement le périmètre de nos compétences en matière de sécurité pour répondre aux besoins de nos clients*," explique **Brendan Hannigan, Directeur Général de la division IBM Security Systems Division**. "*Notre but est de fournir une compréhension exploitable de chaque bit de donnée, peu importe sa localisation sur le réseau, et d'aider les clients à apprendre de leur activité passée pour mieux sécuriser le futur*."

Pour les entreprises innovantes, à la recherche d'une connaissance poussée des risques de sécurité, la solution IBM Security Intelligence with Big Data fournit une puissance de détection sans précédent, en combinant expertise en matière de sécurité et bonne compréhension grâce à l'analytique. En élargissant le périmètre d'investigation à de nouveaux types de données, la solution aide les organisations à répondre à des questions

qu’elles ne pouvaient même pas se poser avant. L’analyse des données structurées et non structurées d’une entreprise, par la solution IBM, aide à détecter l’activité malveillante qui se cache au plus profond des données de l’organisation.

Les solutions de sécurité intelligentes et de Big Data s’appuient sur des cas concrets

La détection et l’analyse des menaces persistantes ou des fraudes nécessitent une nouvelle catégorie de solutions capables d’analyser plus de données, avec plus de flexibilité et fournissant des résultats plus précis.

Issue des laboratoires IBM, IBM Security Analytics with Big Data combine la visibilité sur la sécurité en temps réel et la détection d’anomalies grâce à la plate-forme IBM QRadar Security Intelligence avec l’analytique personnalisé et l’exploration de vastes données d’entreprise fournit par IBM Infospehere BigInsights.

Il en résulte une solution intégrée qui allie un contrôle et un système d’alerte intelligents sur un même outil de travail pour analyser, explorer la sécurité et les données d’entreprise d’une façon jusqu’à là impossible.

Principales caractéristiques :

- Corrélation et détection d’anomalies en temps réel à partir de diverses sources
- Interrogation à haute vitesse des données de sécurité intelligente
- Flexibilité de l’analyse des données structurées et non-structurées incluant la sécurité, les emails, les médias sociaux, les processus métier et autres données
- Interface graphique pour visualiser et traiter le big data
- Analyse scientifique pour une visibilité profonde dans l’activité réseau

Disponibilité

La plateforme de sécurité intelligente IBM QRadar et la plateforme IBM big data, incluant IBM InfoSphere BigInsights, sont d’ores et déjà disponibles.

A propos d’IBM Sécurité

Le portefeuille de solutions sécurité d’IBM aide les organisations à protéger leurs employés, données, applications et infrastructure. IBM offre des solutions pour la gestion des identités et des accès, la sécurité de l’information, la gestion d’évènements, la sécurité des bases de données, le développement d’applications, la gestion du risque, la gestion des terminaux, la protection contre les menaces avancées et bien plus encore.

Dans le domaine de la sécurité, IBM dispose de l’organisation de recherche et de développement la plus importante au monde, elle est composée de dix centres d'opérations (SOC), neuf centres de recherche IBM, 11 laboratoires de développement de logiciels de sécurité et l’Institute for Advanced Security. Au niveau mondial, IBM emploie des milliers d'experts spécialisés sur les questions de sécurité tels que des analystes, des consultants, des spécialistes commerciaux et techniques, ainsi que des professionnels en infogérance. IBM gère 15 milliards d’événements de sécurité par jour dans plus de 130 pays et détient 3000 brevets liés à la sécurité. IBM s’investit dans la sécurité depuis près de 50 ans, alors que la compagnie s’employait à innover en matière

de sécurité pour ses systèmes mainframe.

A propos de DTCC

La société de dépôt et de compensation (Depository Trust & Clearing Corporation – DTCC) est un acteur majeur dans la transaction de services financiers tels que la compensation et le règlement-livraison. Elle met en contact les caisses de retraite et autres gestionnaires de fonds avec leurs réseaux de distribution et traite plus de 3,6 millions de titres dans 122 pays, pour une valeur totale de 39,5 billions de dollars. Le DTCC protège les marchés et systèmes financiers en s'appuyant sur l'expertise acquise grâce à l'analytique. Cela permet d'obtenir une infrastructure plus robuste, unifiée et de promouvoir les solutions qui réduisent systématiquement les risques, améliorent le rendement d'exploitation et minimisent les coûts pour les entreprises utilisatrices de leurs services.

Pour plus d'informations sur IBM Sécurité : http://www.ibm.com/security/fr

###

IBM Announces Breakthrough with Combination of Security Intelligence and Big Data

Data analytics helps organizations hunt for cyber attacks

ARMONK, NY – 4 February 2013 – Advanced attacks, widespread fraud and the pervasive use of social media, mobile and cloud computing are drastically altering the security landscape. As organizations increasingly need to manage Big Data, the way that corporate data needs to be protected is rapidly changing.

To aid in the detection of stealthy threats that can hide in the increasing mounds of data, IBM (NYSE: IBM) today announced IBM Security Intelligence with Big Data, combining leading security intelligence with big data analytics capabilities for both external cyber security threats and internal risk detection and prevention. IBM Security Intelligence with Big Data provides a comprehensive approach that allows security analysts to extend their analysis well beyond typical security data and to hunt for malicious cyber activity.

This new solution combines real-time correlation for continuous insight, custom analytics across massive structured data (such as security device alerts, operating system logs, DNS transactions and network flows) and unstructured data (such as emails, social media content, full packet information and business transactions), and forensic capabilities for evidence gathering. The combination helps organizations address the most vexing security challenges, including advanced persistent threats, fraud and insider threats.

The Depository Trust & Clearing Corporation (DTCC) is a leading financial services transaction clearing and settlement provider linking funds and carriers with their distribution networks and handling more than 3.6 million securities from 122 countries and territories valued at US$39.5 trillion. DTCC protects the financial markets and systems as a whole, using scale and expertise with advanced data analytics to perfect a more robust, unified infrastructure and promote solutions that systematically reduce risks, amplify operating efficiency and minimize cost for the member firms.

"*As the sophistication and technological means of cyber-criminals increase, the financial industry and government need to move to a risk-based framework that incorporates the dynamic nature of the threat landscape*," said **Mark Clancy, CISO, Managing Director, Technology Risk Management, DTCC** . "*We need to move from a world where we 'farm' security data and alerts with various prevention and detection tools to a situation where we actively 'hunt' for cyber-attackers in our networks. IBM's Security Intelligence with Big Data solution gives us a practical way to gain visibility across our environment. We're gaining real-time security awareness and meaningful insight into historical activity across years of diverse data*."

"*Leveraging assets from across IBM, we are on a relentless push to expand the scope of our security intelligence capabilities for clients*," said **Brendan Hannigan, General Manager of IBM's Security Systems Division**. "*Our goal is to provide actionable insight into every bit of data, no matter where it resides across the network**,** and help clients learn from past activity to better secure the future*."

For forward-leaning organizations seeking advanced insight into security risks, IBM Security Intelligence with Big Data helps provide unprecedented powers of detection by combining deep security expertise with analytical insights on a massive scale. The solution helps organizations answer questions they could never ask before, by widening the scope of investigation to new data types. By analyzing structured, enriched security data alongside unstructured enterprise data, the IBM solution helps find malicious activity hidden deep in the masses of an organization's data.

"*Success today is too often defined as the absence of failure by the information security industry, instead of the demonstration of effectiveness. We do a lot of things in our profession that are hard to observe and hard to quantify. But any time you can measure the success or failure in a provable way, you can produce a much better outcome*," **Mark Clancy, CISO, Managing Director, Technology Risk Management, DTCC** said.

Integrated Security Intelligence and Big Data Analytics for Advanced Use Cases
Security use cases such as advanced persistent threat detection, fraud detection and insider threat analysis require a new class of solutions that can analyze more data, with more flexibility, and deliver more accurate results.

Made in IBM Labs, IBM Security Intelligence with Big Data unites the real-time security correlation and anomaly detection capabilities of the IBM QRadar Security Intelligence Platform with the custom analysis and exploration of vast business data provided by IBM InfoSphere BigInsights. The result is an integrated solution that combines intelligent monitoring and alerting with a workbench for threat and risk analysts to analyze and explore security and enterprise data in ways previously not possible.

Key capabilities include:

- Real-time correlation and anomaly detection of diverse security and network data
- High-speed querying of security intelligence data
- Flexible big data analytics across structured and unstructured data – including security, email, social media, business process, transactional, device, and other data
- Graphical front-end tool for visualizing and exploring big data

- Forensics for deep visibility into network activity

Rich Solutions with a Robust Roadmap

Included in IBM Security Intelligence with Big Data is an extensive set of pre-packaged security intelligence content, ranging from a comprehensive security data taxonomy and automated data normalization, to pre-defined rules and dashboards that codify industry best practices and accelerate time to value. IBM plans to deliver InfoSphere BigInsights Application Accelerators for specific use cases, to further accelerate deployment and enhance benefits.

The solution is additionally backed by expert professional services from IBM. These capabilities help clients kickstart their big data security initiatives through design best practices and proven implementation expertise. The solution is also supported by IBM Security Services, which helps clients manage day-to-day security operations by providing real-time management and monitoring of diverse technologies, such as SIEM, and complimentary services such as security assessments, and incident response and preparedness.

Availability
IBM QRadar Security Intelligence Platform products and IBM Big Data Platform products, including IBM InfoSphere BigInsights, are available immediately.

Related Resources

Picture Story: A Big Data Approach to Security Intelligence

YouTube video: The role big data plays in solving complex security challenges

Solutions: IBM Security Intelligence with Big Data

About IBM Security

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, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. This comprises 10 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 15 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.

All client examples cited or described are presented as illustrations of the manner in which some clients have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions.

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 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.