# IBM Announces Security Forensics Capabilities to Help Protect Critical Data

**New analytics and automation helps any IT security team quickly identify and defend against hidden threats**

---

**ARMONK, N.Y. - 18 Feb 2014:** IBM (NYSE: IBM) today announced a powerful appliance for helping organizations diagnose and defend their critical data and enterprise networks against sophisticated external attacks and unauthorized insider activities.

Since 2010, the IBM X-Force Trend & Risk Report has been reporting on the alarming rate of how cyber attacks continue to occur. As data breaches continue to impact organizations, the need to reduce detection time and investigate these threats before they can significantly impact the business is critical. Cyber criminals often gain access to a corporate network weeks or months before actual data is compromised. According to the IBM X-Force Threat Intelligence Quarterly to be released next week, in 2013, more than half a billion records of personally identifiable information were leaked through a number of attacks against strategic targets. By detecting malicious activity earlier, organizations can more quickly stop, or reduce the potential loss of data.

IBM Security QRadar Incident Forensics, a new software product designed as a module for the QRadar Security Intelligence Platform, can help security teams retrace the step-by-step actions of sophisticated cyber criminals. By adding this forensics capture and search module to its QRadar Security Intelligence platform, IBM can further strengthen its clients' abilities to efficiently investigate security incidents and understand the impact of any suspicious activity. QRadar Incident Forensics provides a record of activity on the network, enabling organizations to retrace suspicious activity, provide alerts to growing concerns, and provide forensics search capabilities.

"Every breach is a race against time. This new forensics module further expands the breadth and depth of IBM's security intelligence capabilities," said Brendan Hannigan, general manager of IBM Security Systems. "QRadar Incident Forensics further helps IT staff prevent emerging threats and better determine the impact of any intrusion."

IBM Security QRadar Incident Forensics will help any member of an IT security team quickly and efficiently research security incidents or test for conditions associated with an observed attack pattern from an Internet threat intelligence feed such as X-Force. By using this guidance, security teams can avoid spending valuable time searching through petabytes of network traffic, and potentially discovering nothing of immediate value. With QRadar, security analysts can quickly collect security data related to an incident.

This solution is just one of IBM's new initiatives to expand its security intelligence capabilities. In the second quarter of 2014, IBM will introduce new capabilities to help organizations better understand the threat landscape. IBM Advanced Cyberthreat Intelligence Service will provide customers with insight into the threat landscape, targeted attacks and attacker tools, tactics and practices, incorporating IBM's own research with that of strategic partners specializing in threat visibility.

Additionally, IBM's Active Threat Assessment complements this ongoing threat intelligence and visibility. It leverages technical assessment capabilities and best-of-breed tools to identify previously unrealized, active threats while also modeling threats to unmitigated vulnerabilities in an enterprise environment.

IBM Security QRadar Incident Forensics, currently planned to be available in the second quarter of 2014, is an integrated module in IBM's QRadar Security Intelligence platform. Also part of this announcement, IBM is now allowing existing QRadar clients to test this solution as part of a beta program.

**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. 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.

## Contact(s) information

**Nicole Trager**
IBM Media Relations
1 (978) 621-3076
ntrager@us.ibm.com

**Tod Freeman**
IBM Media Relations
1 (415) 320-5893
tefreema@us.ibm.com