

IBM Invests \$200M to Help Clients Respond to Cybersecurity Incidents

Wednesday, November 16, 2016 04:00:00 PM (GMT)

CAMBRIDGE, Mass., Nov. 16, 2016 /PRNewswire/ -- IBM Security (NYSE: [IBM](#)) today announced a major expansion of its incident response capabilities, including new facilities, services and software as part of a \$200 million investment made this year. These investments include a new global security headquarters in Cambridge, Mass. which features the industry's first physical [Cyber Range](#) for the commercial sector, where participants experience preparing for and responding to cyber attacks using live malware and real-world scenarios.

IBM also expanded capabilities and capacity for its global network of IBM X-Force Command Centers which now handle over 1 trillion security events per month. These security operations centers are staffed by 1,400 security professionals who will use cognitive technologies like Watson for client services, including chat sessions and data delivery, as well as Watson for Cybersecurity to quickly address cyber security events.

As part of today's announcement, IBM launched a new elite incident response and intelligence consulting team called IBM X-Force Incident Response and Intelligence Services (IRIS). IBM's investments also includes its acquisition of Resilient Systems [earlier this year](#), a pioneer in the incident response market.

A new Ponemon Institute study on Cyber Resilience, sponsored by IBM and also [announced today](#), found 75 percent of IT and security professionals surveyed say their organization does not have a modern incident response plan applied across the entire enterprise. This lack of planning and coordination can make it difficult to respond quickly and contain the costs of an incident. For example, in 2018, companies in the UK must report data breaches to regulators within 72 hours or face fines up to 4 percent of their global annual turnover.

"Being prepared to respond is the first line of defense in making sure a cyber security incident doesn't become a crisis," said Marc van Zadelhoff, General Manager, IBM Security. "To adequately prepare for –and respond to – cyber attacks, companies need to assemble cross-functional teams that bring a strategic mix of security intelligence, technical skill, legal precision and regulatory understanding combined with a comprehensive plan of action. With our investments, we've moved IBM into a unique position in the industry with a comprehensive cybersecurity immune system for customers to build world-class capabilities for thwarting cybercrime."

IBM X-Force Command Centers and New Cyber Range

IBM Security's new headquarters in Cambridge, located at 75 Binney Street, includes a fully operational "Cyber Range," bringing together capabilities and experiences previously only available in the public sector. IBM's new X-Force Command Cambridge Cyber Range immerses people in simulated cyber attacks to train them on how properly prepare for, respond to, and manage a broad variety of threats. This experience can be leveraged by Chief Information Security Officers and their security teams, as well as those without security expertise, such as other members of the C-Suite/lines of business, board members, students and others.

IBM's Cyber Range uses live malware, ransomware and other real-world hacker tools culled from the dark web to deliver realistic cyber attack experiences. The facility features an air-gapped network of a fictitious corporation, used for simulated attacks, consisting of one petabyte of information, more than 3,000 users and a simulated version of the internet.

As part of the Cyber Range experience, IBM has designed real-world scenarios to help clients experience, defend against and shut down cyber attacks. The scenarios will also help train organizations with the necessary steps required to respond quickly in the wake of an incident, from addressing regulatory requirements that vary from country to country and state to state, to client, business partner, media and supply chain notifications and management.

As part of today's announcement, IBM also launched IBM X-Force Command Center Atlanta, a fully upgraded security operations center which IBM has operated for 15 years. The facility now handles over 35

billion security events per day – a 75 percent increase in capacity.

IBM X-Force Command Center Atlanta is a hub for the company's network of SOCs, which help protect 4,500 clients across 133 countries. Using IBM X-Force Threat Intelligence, the security operation centers bring in 200,000 new pieces of threat intelligence daily, by leveraging insights from analysis on over 100 million web pages and images, and collecting data from monitoring 270 million endpoints.

IBM also has expanded its capacity to handle security events and intelligence for IBM X-Force Command Centers in Bangalore and Poland, complemented by previously modernized IBM centers in Costa Rica and Tokyo, creating a scalable global network of defense for clients.

New IBM X-Force IRIS Team of Elite Security Consultants

IBM also launched a new incident response and intelligence consulting team called [IBM X-Force IRIS](#). Led by [Wendi Whitmore](#), Global Lead, IBM X-Force IRIS the team includes over 100 elite cybersecurity consultants positioned throughout the globe, with deep expertise in incident response and threat intelligence.

Whitmore has built the IBM X-Force IRIS team by bringing together security consultants with a [broad spectrum of experience](#), including those who have led responses to many of the largest cyber security breaches in the past decade. Their response experience has spanned retail, political and international banking networks. Many members of the new team are former security experts at federal law enforcement and intelligence agencies where they built intelligence collection and analysis capabilities which are still in use today.

The IBM X-Force IRIS team further expands IBM's incident response capabilities, building on the services announced in February. The new consulting capabilities, with the incorporation of IBM X-Force intelligence services, will help clients understand where and how cyber attacks are being launched to defend against and remediate them with greater speed and precision.

With a focus on preparedness and planning, the IBM X-Force IRIS practice helps clients test their environment, run attack scenarios, and identify key business systems and processes needing stronger security and critical to maintaining resiliency. Through an emphasis on proactive planning, IBM X-Force IRIS can help clients reduce the costs and complications of response, which can help lead to quicker containment of an incident.

The IBM X-Force IRIS's capabilities include:

- Proactive incident response planning and preparedness training
- Incident simulation and tabletop exercises, including Red Teaming / Blue Teaming
- A concurrent approach to containment, remediation and threat intelligence
- Forensic analysis
- Threat Intelligence analysis

Builds on Resilient Systems' Pioneering Incident Response Technology

Resilient, an IBM Company, provides a software platform for comprehensive incident response management and orchestration – designed to help security professionals manage and respond to incidents faster and more intelligently. The platform has agile playbooks based on National Institute of Standards and Technology and SANS Institute standards that cover potential threats from a lost laptop to malware attacks. It also has the one of the largest privacy databases with global breach notifications to help clients maintain compliance. This enables clients to mitigate cyber incidents more quickly while helping minimize their exposure.

[Resilient Systems'](#) award-winning platform is a foundational component of IBM's incident response technologies, along with IBM's [QRadar](#) Security Intelligence.

For more information on or to arrange a visit to the IBM X-Force Command Center Cyber visit:

<http://www.ibm.com/security/xforcecommand>

About IBM Security

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, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest

security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence [blog](#).

Media Contact:

Kelly Kane, IBM Security
413-297-2668
kkane@us.ibm.com

Logo - <http://photos.prnewswire.com/prnh/20090416/IBMLOGO>

To view the original version on PR Newswire, visit: <http://www.prnewswire.com/news-releases/ibm-invests-200m-to-help-clients-respond-to-cybersecurity-incidents-300364226.html>

SOURCE IBM Corporation

Countries: United States

Industries: Computer Electronics, Hardware & Software, High Tech Security, Multimedia, Internet & Wireless Technology

Languages: English

Primary Identifiers: IBM-US

Related Identifiers: IBM-US