Announcements

IBM Rolls Out Industry's First Cybersecurity Operations Center on Wheels

- Cyber "Tactical Operation Center" to Travel Globe for Events, Training and Awareness

- Part of IBM Security's Growing $200M+ investment in Incident Response Capabilities

NEW YORK, Oct. 15, 2018 /PRNewswire/ -- IBM (NYSE: IBM) Security today announced the industry's first mobile Security Operations Center, capable of traveling onsite for cybersecurity training, preparedness, and response. The IBM X-Force Command Cyber Tactical Operations Center (C-TOC) will travel around the U.S. and Europe, running incident response drills with clients, providing on-demand cybersecurity support, and building cybersecurity awareness and skills with professionals, students and consumers.

The IBM X-Force C-TOC is a fully operational Security Operations Center on wheels, modeled after Tactical Operations Centers used by the military and incident command posts used by first responders. Housed in a tractor trailer, the mobile facility provides a gesture-controlled cybersecurity "watch floor," data center and conference facilities that can accommodate two dozen operators, analysts and incident command center staff. The facility can be deployed in a variety of environments, with self-sustaining power, satellite and cellular communications, providing a sterile and resilient network for investigation and response as well as a state-of-the-art platform for cybersecurity training.

Historically, cybersecurity teams have been focused on detection and protection against cybersecurity incidents. However, as the threat landscape has evolved, organizations are now recognizing the need to plan and rehearse their response to security incidents as well. The 2018 Cost of a Data Breach Study[1] found that companies that are able to respond to incidents effectively and remediate the event within 30 days can save over $1 million on the total cost of a data breach – yet less than 25% of professionals surveyed say their company has a coordinated incident response plan applied across the organization.

The IBM C-TOC will begin its journey travelling around the U.S. and Europe, with multiple purposes:

- **Response Training and Preparedness**: With an increasing focus on improving incident response in the aftermath of major cybersecurity attacks, the C-TOC can help companies train their teams on techniques (both technical and crisis leadership) to respond to attacks while simulating real-world conditions of how hackers operate and key strategies to protect business brand and resources.
- **Onsite Cybersecurity Support**: IBM designed the C-TOC with the capabilities to deploy the mobile facility as a client-specific, on-demand Security Operation Center. One potential use-case being

explored is supporting sporting events or other large gatherings where supplemental cybersecurity resources may be needed.

- **Education and Awareness:** When the C-TOC is in between IBM client engagements, it will travel to immerse people in one of the most realistic cybersecurity experience in the industry – visiting local universities and industry events, and even reaching primary school children with awareness efforts to build interest in cybersecurity careers and help address the growing workforce shortage.

"Experiencing a major cyberattack is one of the worst crisis a company can face, and the leadership, skills and coordination required is not something you want to test out for the first time when you're facing a real attack," said Caleb Barlow, Vice President of Threat Intelligence, IBM Security. "Having a mobile facility that allows us to bring realistic cyberattack preparation and rehearsal to a larger, global audience will be a game changer in our mission to improve incident response efforts for organizations around the world."

Demand for Cybersecurity Preparation and Response Grows

IBM Security has identified incident response and preparedness as an underserved segment of the $114 billion cybersecurity market.[2] In 2016, IBM invested $200 million in new incident response facilities, services and software, including the industry's first Cyber Range for the commercial sector. Since then, IBM has taken more than 2,000 people through its immersive cybersecurity preparedness training in its facility in Cambridge, MA. With the launch of the X-Force C-TOC, this training is being taken directly to clients as well as an expanded mission to provide onsite preparedness and the potential for supplemental cybersecurity services.

To create this Cyber Range experience and the C-TOC, IBM consulted with dozens of experts from different industries, from emergency medical responders to active duty military officers. Along with IBM's own cybersecurity expertise, the C-TOC experiences train teams on the essentials of leadership in crisis – from moving out of the organizations day to day structure and into an incident command hierarchy to thinking a step ahead to anticipate the next moves of an attacker.

The C-TOC training includes a "Cyber Best Practices Laboratory" with real world examples based on experiences with customers in the Cambridge Cyber Range. It will also enable companies to participate in an immersive, gamified cyberattack which allows teams to test incident response plans under a realistic, high pressure simulation. Some examples of these attack scenarios include:

- **Ox Response Challenge**: This challenge is designed for the executive team to immerse a wide variety of stakeholders in a realistic "fusion team" environment in which players must figure out how to respond to a cyberattack as a team, across dimensions such as technical, legal, public relations and communications.
- **OpRed Escape**: Get into the mind of a cybercriminal and learn to think like a hacker; this exercise

puts participants into the "seat" of a real-world attacker, learning the ways bad guys break into networks by watching an expert and getting hands-on experience with a malicious toolset.

- **Cyber War Game**: In this hands-on scenario, participants will uncover a cyber-attack lead by a cybercrime gang targeting a fictitious corporation. Operating on the C-TOC's simulated corporate network, participants will use technical tools to identify the threats and shut them down, while also building a response plan and developing leadership and crisis management skills.

Supplemental Cybersecurity Operations

IBM also designed the C-TOC to have the potential to supplement onsite support for clients at times when their cybersecurity needs may surge. Cybercriminals are constantly on the lookout for major events and moments in time to help launch their attacks, taking advantage of increased interest, cashflow and internet activities to get higher returns on their malicious activities.

Cybersecurity at large-scale events is increasingly being considered alongside emergency services response and public safety. For these events, IBM can bring the C-TOC onsite to help not only with preparation, but to provide an isolated network, cybersecurity watch floor and incident command infrastructure.

Skills and Awareness

The cybersecurity workforce shortage is a major hurdle plaguing the industry, with an anticipated shortfall of nearly 2 million cybersecurity professionals by 2022.[3] Building awareness about security careers among younger generations, as well as helping upskill current professionals in cybersecurity, are two ways IBM Security hopes to help address the skills shortage.

When not working with clients, the C-TOC will travel to academic institutions, industry and community events for training and awareness activities. For instance, the C-TOC will travel to the National Collegiate Pentesting Competition hosted at Rochester Institute of Technology November 2 - 4, and it will also be available for events that IBM hosts to drive interest in cybersecurity and STEM careers, such as IBM Cyber Day for Girls. The C-TOC can also help improve and expand skillsets within the current cybersecurity workforce, through onsite training and hands on skills development with cybersecurity teams on critical skillsets to help them keep up with the latest cyberthreats.

C-TOC to Tour U.S. and Europe

The C-TOC will begin its tour in the U.S., travelling to client sites, schools and government facilities.

On October 18, the C-TOC will be based at the National Mall in Washington, D.C. providing cybersecurity awareness training to congressional staff and other public officials. The C-TOC will travel to Europe in January, visiting clients and events in multiple countries throughout 2019.

IBM will evaluate opportunities for additional mobile security operation centers and use-cases based on

feedback and demand.

To learn more about IBM's C-TOC and Cyber Range, go to http://ibm.com/xforcectoc.

To view and download multimedia assets, visit the following links:

- "BluePrint" Infographic with data on C-TOC
- Video b-roll for download
- Photos of the C-TOC can be downloaded by clicking the images above, or via the IBM Security Image Gallery
- Video: IBM Unveils Industry's First Security Operations Center on Wheels
- Video: First Look: Building the X-Force Command Cyber Tactical Operations Center

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 treats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 60 billion security events per day in more than 130 countries, and has been granted more than 8,000 security patents worldwide. For more information, please check www.ibm.com/security, follow IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Media Contacts:

Cassy Lalan
External Relations, IBM Security
cllalan@us.ibm.com
319-230-2232

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

[1] 2018 Cost of as Data Breach Study, sponsored by IBM and conducted by Ponemon Institute

[2] Source: Gartner, "Forecast: Information Security, Worldwide, 2016-2022, 2Q18 Update," Aug 2018

[3] Global Information Security Workforce Study 2017, ISC2 / Frost & Sullivan

SOURCE IBM

Additional assets available online: Photos (6) Video (2)