IBM Newsroom

IBM Security Opens Network of Four Secure Testing Facilities Globally

X-Force Red Labs located in Atlanta, Austin, England and Australia; Team Expands with New ATM Testing Practice

PR Newswire
LAS VEGAS

LAS VEGAS, Aug. 6, 2018 /PRNewswire/ -- BLACK HAT CONFERENCE -- IBM (NYSE: IBM) Security today announced X-Force Red Labs, a network of four secure facilities dedicated to testing the security of devices and systems including consumer and industrial IoT technologies, automotive equipment, and Automated Teller Machines (ATMs). IBM X-Force Red also has launched a dedicated ATM Testing practice in response to increased demand for securing financial transaction systems.

The new Labs will be operated by X-Force Red, an autonomous team of veteran hackers within IBM Security. The X-Force Red Labs offer secure locations where X-Force Red's seasoned hackers will work to find vulnerabilities in devices (hardware and software) before and after they are deployed to customers. The four Labs will be in Austin, TX; Hursley, England; Melbourne, Australia; and Atlanta, GA.

In just two years, IBM X-Force Red has emerged as the industry's premier security testing team and has experienced tremendous growth. The team has grown its penetration testing client base by over 170 percent in the last year. This exponential growth has also led IBM Security to increase the number of X-Force Red practitioners -- doubling over the past year across multiple domains. Some of the recent additions to the X-Force Red team include: Ivan Reedman (aka the ToyMaker), Global Hardware Security Lead; Thomas MacKenzie, European and Automotive Practice Leader; and Daniel Crowley, Global Research Director for X-Force Red.

"IBM X-Force Red has one mission – hack anything to secure everything," said Charles Henderson, Global Managing Partner, IBM X-Force Red. "Via X-Force Red Labs, we have the ability to do just that, in a secure and controlled environment. Whether it's the newest smart phone that hasn't been released, an internet-connected refrigerator or a new ATM, we have the capability to test, identify, and help our clients remediate vulnerabilities before the bad guys can exploit them."

X-Force Red Labs: Hack Anything to Secure Everything

Fixing software vulnerabilities and flaws after production can cost organizations more than 29 times the cost of identifying and fixing them during the design phase, according to the Ponemon Institute[1]. IBM X-Force Red, through the new four global testing labs, assists engineers and developers with building in security throughout the development lifecycle of hardware and software, including IoT-enabled devices and ATMs.

The service includes:

- **Documenting Product Requirements:** Mapping product objectives, stakeholders and systems involved, skillsets available, and other product requirements with product engineers.
- **Technical Deep Dive:** Analysis of product design documentation, security requirements, risk management

information, and any other data to scope the penetration test.

- **Threat Modeling:** Disclosure of potential threats and risks to the product and company including threat actors likely to target their product, how and why they would compromise it, and the potential risk to the company.
- **Generating Security Requirements:** Create and implement a list of security requirements for engineers as they build products.
- **Penetrating Testing:** Hacking into products using the same methods that real-world attackers would use. Through the X-Force Red cloud-based portal, the team provides real-time updates on vulnerability findings. Since X-Force Red hackers report findings as they test, customers do not have to wait until the full test is completed to begin remediation.

The Demand for ATM Testing

With more than 300 million ATMs in the world, financial institutions need to protect these targeted machines from attackers. In early 2018, law enforcement alerted financial institutions of increased threats targeting ATMs in the U.S. that allow criminals to "jackpot" the machines and steal their contents on demand. These attacks have been known to use both malware and physical access to the ATM device to empty all of the cash from the machine. Since 2017, X-Force Red has experienced a 300 percent increase in requests for ATM testing due these emerging threats.

Many financial organizations are also still running dated operating systems on these devices that they cannot adequately patch to harden the machine. By identifying vulnerabilities in these machines in advance, before a criminal gains access, financial institutions can address and help protect against future compromise.

The X-Force Red ATM Testing service includes a global team of experienced penetration testers that can identify and help remediate physical, hardware and software vulnerabilities within banks' ATMs, before an attacker gets their hands on them. The service includes:

- **Comprehensive ATM Evaluation:** Evaluation of physical, network, application and computer system security, searching for vulnerabilities that a criminal hacker may exploit.
- **Attacker-Minded Testing:** Hacking into ATMs using the same tools and methods a criminal would use, to identify exploitable vulnerabilities.
- **Vulnerability Remediation Recommendations:** Hardening of ATM systems and defenses via comprehensive recommendation reports.
- **Compliance:** Review of ATM logs to help financial organizations stay in compliance with industry standards such as the Payment Card Industry Data Security Standard (PCI DSS).

IBM X-Force Red at Black Hat and DEF CON 2018

Members of IBM X-Force Red will be speaking at Black Hat and DEF CON. To learn more about these sessions visit: http://ibm.biz/blackhatdefcontalks

To find out more about IBM X-Force Red, go to www.ibm.com/xforcered. You can also follow 'X-Force Red in action' for the latest and greatest on all things IBM X-Force Red.

X-Force Red and other IBM Security experts will demonstrate the latest offerings at the Black Hat Networking Lounge (#2104) located in Oceanside at Mandalay Bay on August 8 & 9.

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 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 Contact:
Kelly Kane
IBM Security Media Relations
kkane@us.ibm.com
413-297-2668

[1] Source: Ponemon Institute Benchmarks on Application Security, last updated March 2018

SOURCE IBM Security

Web Site: http://www.ibm.com/security

Additional assets available online: Photos (

https://newsroom.ibm.com/2018-08-06-IBM-Security-Opens-Network-of-Four-Secure-Testing-Facilities-Globally