

IBM X-Force Red Launches New Services for Automotive Industry and IoT IBM Security Testing Group Expands with Notable Industry Hires and New Investments in Tools

LAS VEGAS, July 24, 2017 /PRNewswire/ -- IBM Security (NYSE:[IBM](#)) today announced the launch of two new security testing practice areas focused on automotive security and the Internet of Things (IoT). The new services will be delivered via an elite team of IBM X-Force Red researchers focused on testing backend processes, apps and physical hardware used to control access and management of smart systems.

The new IoT services will be delivered alongside the [Watson IoT Platform](#) to provide security services by design to organizations developing IoT solutions for all industries. With 58% of organizations testing their IoT applications only during the production phase¹, the potential for introducing vulnerabilities into existing systems remains unacceptably high. The Watson IoT Platform provides configuration and management of IoT environments, and the IBM X-Force Red services bring an added layer of security and penetration testing.

IBM X-Force Red marked its first-year anniversary with the addition of security specialists such as [Cris Thomas \(aka Space Rogue\)](#) and [Dustin Heywood \(aka Evil Mog with Team Hashcat\)](#), who add to the team's impressive roster of talent globally. To further optimize their engagements, IBM X-Force Red has also built a password cracker called "Cracken" designed to help clients improve password hygiene.

"Over the past year, we've seen security testing further emerge as a key component in clients' security programs," said Charles Henderson, Global Head of IBM X-Force Red. "Finding issues in your products and services upfront is a far better investment than the expense of letting cybercriminals find and exploit vulnerabilities. Our own investments in people, tools and expertise have more than tripled our security testing capabilities in the first year of IBM X-Force Red, making our offense our clients' best defense."

Connected Car Security is a Global Priority

Gartner estimates that the production of new automobiles equipped with data connectivity, either through a built-in communications module or by a tether to a mobile device, is forecast to reach to 61 million in 2020.² With the current and future challenges in mind, IBM X-Force Red created an automotive practice dedicated to helping clients secure hardware, networks, applications, and human interactions.

IBM X-Force Red worked with more than a dozen automotive manufacturers and third-party automotive suppliers to build expertise and programmatic penetration testing and consulting services. The formation of the automotive practice aims to help to shape and share industry best practices and standardize security protocols.

The new automotive practice is also applying some of the findings from research disclosed by IBM X-Force Red early this year that notified [consumers](#) and the [automotive industry](#) of security pitfalls inherent in connected cars. The research looked at the insecure transfer of ownership between owners of some connected cars, which may create an opportunity for a malicious takeover of the functions of the vehicle, such as locking and unlocking of doors, remote start, light and horn control, and the ability to geo-locate the current owner through a mobile app. When these findings were revealed at RSA 2017, Henderson and IBM X-Force Red also disclosed that these security loopholes were also identified across four major auto manufacturers.

The interconnected components and systems in a modern vehicle can number in the hundreds or thousands, each with their own security controls and vulnerabilities. As these components are combined and connected to mobile applications and external servers, the total amount of potential vulnerabilities for the vehicle climbs above the sum vulnerabilities of its parts. With this in mind, IBM X-Force Red performs discrete security testing of the components and solution-based security testing for the

complete system of the vehicle.

Watson IoT Platform and IBM X-Force Red

Gartner forecasts that 8.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020.³ While the insights gained from IoT data help drive revenue streams and forge lasting customer relationships, demand and shortened production cycles often leads to rushed or non-existent security testing for these new products and services.

IBM X-Force Red has changed the delivery of security testing due to the perceived gaps in security of emerging technologies such as IoT and connected cars. Programmatic and on-demand security testing through the entire lifecycle of the products is emerging as the best way to find vulnerabilities in a proactive fashion. Watson IoT Platform customers will now be able to leverage the security expertise of IBM X-Force Red to assist throughout development and deployment.

"It's not just about the technology, it is also about the global reach, investment, and collaborative approach which make IBM a trusted IoT partner for enterprise IoT solutions," said James Murphy, Offering Manager, IBM Watson IoT Platform. "With IoT technologies permeating the farthest corners of industry, IBM is bringing our Watson IoT Platform and X-Force Red security talent together to address present and future concerns."

The Watson IoT Platform approach is security by design, with security controls built-in, delivered as a [cloud-based service](#) with industry-recognized ISO27001 compliance. The Watson IoT Platform also has advanced security IoT service capabilities that extend Watson IoT Platform with Threat Intelligence for IoT. These features help customers visualize critical risks in the IoT landscape and create policy-driven automations to help prioritize operational responses for IoT incidents.

The skills and experience of the X-Force Red team alongside the Watson IoT Platform provide the vital components to help get clients off to the right start from design all the way through to go-live of their IoT solution.

Investing in Infrastructure

In February 2017, IBM X-Force launched [The Red Portal](#), a cloud-based collaboration platform for clients and security professionals that presents an [end-to-end view](#) of security testing programs. Clients can view real-time testing project milestones, vulnerabilities across all assets, reports of findings and the overall status of their managed testing program. The Red Portal centralizes and streamlines all communications with X-Force Red and provides a way to begin remediation immediately on the most critical items.

At this year's Black Hat conference, X-Force Red will unveil the newest weapon in their arsenal. Cracken is a dedicated password-cracking cluster used by X-Force Red during penetration tests and security assessments. To illustrate the importance of password length and complexity, X-Force Red will let attendees test passwords against Cracken at Booth #616 during Black Hat USA 2017.

IBM X-Force Red at Black Hat 2017 and DEF CON 2017

Charles Henderson, Global Head of IBM X-Force Red, will present his discussion of real-life penetration testing: "[Better Than Mr. Robot](#)" at Black Hat USA 2017. The session will be held in Business Hall Theater B, Mandalay Bay on Thursday, July 27 from 11:00-11:50 a.m. PT.

Chris Thompson, Red Team Ops Lead, IBM X-Force Red, will present his demonstration of advanced Red Team tactics: "[MS Just Gave the Blue Team Tactical Nukes \(and How Red Teams Need to Adapt\)](#)" at DEF CON 25. The demo will be held in the 101 Track on Saturday, July 30 from 3:00-3:45 p.m. PT.

X-Force Red and other IBM Security experts will demonstrate the latest offerings at [Booth #616](#), Level 1 Business Hall, Mandalay Bay on July 26 & 27.

¹[2017 Study on Mobile and IoT Application Security, Ponemon Institute, Arxan, & IBM Security](#)

²[Gartner, Gartner Says Connected Car Production to Grow Rapidly Over Next Five Years, September 2016](#)

³[Gartner, Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2016, December 2016.](#)

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 has been granted more than 3,000 security patents worldwide. For more information, please check www.ibm.com/security, follow [@ibmsecurity](https://twitter.com/ibmsecurity) on Twitter or visit the [IBM Security Intelligence blog](#).

Media Contact

Dillon Townsel

IBM Security Media Relations

+1-512-571-3455

dillon.townsel@ibm.com

View original content with multimedia:<http://www.prnewswire.com/news-releases/ibm-x-force-red-launches-new-services-for-automotive-industry-and-iot-300492459.html>

SOURCE IBM
