IBM X-Force Red Launches New Service for Blockchain Security Testing

New Service Uncovers and Helps Address Security Vulnerabilities in Blockchain Design and Implementations

SAN FRANCISCO, March 5, 2019 /PRNewswire/ -- IBM (NYSE: IBM) Security's team of offensive security experts, X-Force Red, today announced the launch of a new blockchain testing service to help identify weaknesses and strengthen security of a wide range of solutions that incorporate the fast-growing technology. Leveraging the extensive security and developer expertise of X-Force Red penetration testers, the service will evaluate both the backend processes used to manage blockchain networks as well as the actual ledger environment.

With worldwide spending on blockchain solutions forecasted to reach $9.7 billion by 2021, the number of blockchain implementations will likely grow exponentially across all industries.[1] Meanwhile, the benefit of the network effect inherent to blockchain networks means they include broad, decentralized ecosystems of organizations, which in turn offers different attack vectors than traditional applications and creates opportunities for cybercriminals seeking to manipulate or monetize the data being shared on the blockchain.

IBM X-Force Red is seeing that 70 percent of solutions that incorporate blockchain rely on traditional technologies for backend processes like authentication, data processing and Application Programming Interfaces (API). The X-Force Red Blockchain Testing service will evaluate the whole implementation including chain code, public key infrastructure and hyperledgers. X-Force Red will also test backend processes, applications and physical hardware used to control access and manage blockchain networks.

"While blockchain is a breakthrough for protecting the integrity of data, that does not mean the solutions that leverage it are immune from attackers, which is why security testing is essential during development and after deployment," said Charles Henderson, Global Head of IBM X-Force Red. "If we look at mobile applications, cloud computing and even personal computers – all these innovations needed to adopt policies and techniques for security after they grew in popularity. Blockchain presents businesses with an opportunity to break that trend."

Blockchain Entering the Enterprise

While initially created as the engine behind cryptocurrencies, in a matter of years the uses for blockchain technology for business have grown exponentially. Today, there is meaningful work underway to use blockchain technology across the enterprise and organizations are seeing real efficiencies and cost savings from its use.

Blockchain solutions are most effective when networks are comprised of diverse members that contribute data. In today's distributed IT environment, where companies demand flexibility and many run workloads on a variety of different infrastructures even within their own organizations, this means that data written to the blockchain can originate from multiple different data structures, have been hosted on numerous public clouds or on-premise systems, and be subject to disparate security standards.

Blockchain enables businesses to transact with one another with greater trust and transparency. And while blockchain networks used in the enterprise take into account business-critical security considerations, the security halo does not necessarily extend beyond the blockchain itself. The same networks, applications, hardware, and personnel that can expose organizations to security vulnerabilities are still present even when blockchain technology is at the core of a technology or business solution.

Establishing hardened industry standards is a critical next phase in enabling the widespread enterprise adoption of blockchain. As an industry leader in enterprise blockchain, IBM is at the forefront of contributing

code and best practices to help build the needed technology and standards for secure, compliant and effective enterprise blockchain implementations. However, not all networks adhere to the same standards or require the same baseline levels of security, and therefore some developers can be focused on getting to market with their deployment quickly, which can lead to inadequate security. Without building critical security considerations from the ground up, the components supporting the blockchain network and its surrounding technology such as APIs, mobile apps or identity mechanisms could be at risk of a compromise.

Blockchain and X-Force Red

By working with the IBM Blockchain team, X-Force Red is able to share expertise from an architectural, operational, and deployment perspective to understand the potential security risks within the technology stack supporting blockchain networks. The skills and experience of the X-Force Red team, alongside the industry-leading IBM Blockchain business, will continue to guide clients on securing enterprise-grade implementations from network design all the way through deployment of their blockchain solution.
This includes independent testing of IBM Blockchain implementations and non-IBM affiliated implementations.

X-Force Red has changed the delivery of security testing due to the perceived gaps in security of emerging technologies such as IoT, connected cars, and now blockchain. Programmatic, scalable and continuous security testing through the entire lifecycle of products is emerging as the best way to find vulnerabilities in a proactive fashion. Blockchain adopters will now be able to leverage the security, developer, and "attacker mindset" expertise of X-Force Red to assist throughout development and deployment.

X-Force Red is comprised of hackers who can break into blockchain networks using the same tools, techniques, practices and mindsets as criminals would use. Through vulnerability assessments, vulnerability management programs, adversary simulation exercises, and manual penetration testing, X-Force Red can help organizations identify and fix vulnerabilities before criminals find them.

During a typical Blockchain Testing engagement, X-Force Red will assess:

- Identity and Access - since access can be the key to the blockchain X-Force Red will evaluate how permissions to access/add info to the blockchain are administered including password policies, susceptibility to brute force attacks, and the implementation of 2-factor authentication
- Public Key Infrastructure (PKI) – secure creation, management, and distribution of digital certificates and keys associated with a blockchain network is crucial to ensuring data integrity
- Smart Contract flaws – smart contracts, also known as "chain code," allow for trustless execution of agreements by parties on the blockchain, but proper penetration testing can find exploitable flaws in these agreements
- Software supply chain attacks - common libraries and component dependency hacking can be tested during design and implementation to ensure secure dependency signatures and a trust build pipeline

In 2017, X-Force Red introduced The Red Portal, a cloud-based communication and collaboration platform for clients and security professionals that presents an end-to-end view of security testing programs. At any point in time, clients can view the status of their testing engagements, vulnerabilities across all assets immediately after they are identified by testers, and reports of remediation recommendations. 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. Most importantly for blockchain administrators, security tests with X-Force Red can be scheduled at any time for any reason, even after the blockchain is operational, and administrators can engage directly with testers.

X-Force Red and other IBM Security experts will demonstrate the latest offerings at Booth #5759, Moscone North Hall, from March 4-8.

For more information about X-Force Red's Blockchain Security Testing Practice, click here: https://www.ibm.com/security/services/blockchain-testing

[1] New IDC Spending Guide Sees Worldwide Blockchain Spending Growing to $9.7 Billion in 2021, January 2018

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 70 billion security events per day in more than 130 countries, and has been granted more than 10,000 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

Dillon Townsel
IBM Security Media Relations
+1-512-571-3455
dillon.townsel@ibm.com

SOURCE IBM