X-Force Red Vulnerability Assessments

Common Security Challenges

While the growth of internet-connected devices has increased productivity and flexibility, it has also increased risk. Rogue devices may connect to the network without being noticed. Data is flowing through more applications, systems and devices, making it more difficult for organizations to understand where their most valuable data lives and who interacts with it.

For small and medium-sized organizations, understanding their data and how it's being protected can be challenging.

Some can only dedicate one or two individuals to identifying security weaknesses, managing patching, deploying security controls, and developing and enforcing security policies.

Larger organizations may have more resources, however understanding the security posture of third-party contractors, who are plugging into their network on various kinds of devices, can be a challenge. If there's a merger or acquisition, understanding the security posture of the new company connecting to the network can also be difficult.

X-Force Red Vulnerability Assessments

X-Force Red offers internal and external vulnerability assessments, which are designed to be a fast, cost-effective way to deliver actionable insights. X-Force Red Vulnerability Assessments include:

Device discovery

– Scanning discovers unknown and rogue devices on the network

– Identifies unknown, malicious and non-malicious IP addresses

– Identifies unknown open servers and applications on the internet (i.e. "shadow IT")

Asset discovery

– Scanning builds an internal map of the network

– Identifies unknown applications, servers and systems, and builds profiles of assets

– Identifies misconfigurations, outdated software, and other basic vulnerabilities exposing identified assets

Third party risk evaluation

– Scanning uncovers basic vulnerabilities in acquired third party networks

– Evaluates risk posture of acquired third parties

False positive removal

– Validates identified vulnerabilities and removes false positives

Reporting and recommendations

– Produces a report of findings and recommendations for remediation

To complement its vulnerability assessments, X-Force Red offers manual penetration testing services. Learn more at **ibm.com/account/reg/us-en/signup?formid=urx-36631**