X-Force Red

IBM **Security**

X-Force Red ATM Testing

ATM Security Challenges

With thousands to potentially millions of dollars stored inside ATMs, it's no wonder they are a top target of criminals.

Criminals typically compromise ATMs in one of two ways. They either manipulate the machine so it dispenses money without being connected to an account or exploit ATM software weaknesses to steal customer payment card or account information.

Depending on the type of ATM, attackers could be in and out in just ten minutes. Or even worse, they could remotely connect to the machine and dispense cash or steal sensitive data for as long as they want, without the bank ever noticing.

X-Force Red ATM Testing

X-Force Red's comprehensive ATM testing identifies and helps organizations fix vulnerabilities within the ATM and connected infrastructure before criminals can exploit them.

Standard or Advanced-Level Testing:

Standard:

– Testing ATM device and associated software

– Testing network traffic between ATM and other devices

– Basic analysis of backend systems

Advanced:

– Testing ATM, software, network, backend systems, entire connected infrastructure

– More complex testing methods applied (i.e. reverse engineering software)

– Extensive application-level testing of backend systems accessed by ATM software

Attacker-Minded Testing

– Exploiting vulnerabilities to validate they're real and aid in discovering others

Compliance

– Capturing and reviewing ATM logs to help organizations maintain compliance with industry standards

Remediation Recommendations and Reporting

– Report including executive summary, methodology, findings and recommendations

X-Force Red offers flat rate project-based work or subscriptions and provides on demand access to all X-Force Red security testing services. Learn more at ibm.com/account/reg/signup?formid=urx-40048