Propelex

PENETRATION TESTING FOR TECHNOLOGY STARTUPS

Technology startups are uniquely challenged when it comes to managing information security. They have a critical need to manage a complex environment of technologies, processes, and applications, but often require all internal resources to be focused on core business operations.

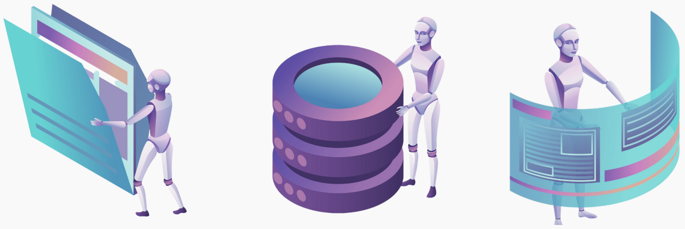
Red teaming from Propelex is the first step in supporting a more manageable, reliable, and effective security environment for technology enterprises. We deploy a manual, security expert-led methodology that is supported by AI-powered automated technologies. Our best-of-both-worlds approach delivers high-level insights, for enhanced security decision making.

RPA Startup

NAME UNDER NDA

ABOUT THE CLIENT

The Client is a technology startup that is innovating solutions in the field of robotic process automation (RPA). Their solutions collect, enrich, and organize customer data, including via their cloud software applications that leverage the power of machine learning and AI. They manage and share data with a wide variety of customers, partners, and organizations worldwide.



Secure - Robotic Process Automation

GOALS

The Client asked the Propelex pen testing team to identify security vulnerabilities and provide guidance for any necessary remediation for the following elements:

1. AWS infrastructure
2. Company website
3. Client-facing web app
4. On-premises IoT devices
5. SCADA networks
6. Physical security

RESULTS

AWS INFRASTRUCTURE

Penetration testing was performed to assess security for the Client's AWS cloud infrastructure and resources. S3 buckets, IAM roles, network access, virtualization, compliance processes, and more were evaluated in a way that was safe, effective, and complied with AWS policies (certain operations required advance notice).

SECURE & COMPLIANT

PCI DSS · HIPAA HITRUST · SOC 2 TYPE 2 · GDPR · SOX COMPLIANCE · NIST

+1 (866) 776 7352 info@propelex.com www.propelex.com

Propelex

PENETRATION TESTING FOR TECHNOLOGY STARTUPS

COMAPANY WEBSITE

Our Red Team executed a plan to audit all attack surfaces of the target website. Automated tools were used to assess response to common attack methods and known vulnerabilities. Manual operations provided a more nuanced assessment of website security and less well-known vulnerabilities.

CLIENT-FACING WEB APP

The Client's primary web app for its clients was tested, to determine its vulnerability to unauthorized access and use. Common web vulnerabilities were assessed using automated tools, while more complex attacks were attempted manually.

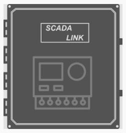
ON-PREMISES IOT DEVICES

The Client utilizes a complex ecosystem of IoT solutions and applications. We devised a red teaming methodology suitable to engage elements across a broad range of components, including communication technologies, cloud-based data management platforms, mobile applications, and data-sharing APIs.

Internet of Things

SCADA NETWORKS

Our Red Team deployed a penetration testing methodology designed to meet the unique requirements of SCADA testing, including tools appropriate for use with PLCs and RTUs. Testing was restricted to a development system, instead of the live system, to deliver the highest level of assurance for operational safety.



Programmable Logical Controller

Remote Terminal Unit

PHYSICAL SECURITY

Propelex evaluated security at Client facilities with a physical walk-through. The effectiveness of security controls and response processes was assessed for authorization and access, physical entry barriers, cameras and sensors, biometric access controls, fire detection and suppression protocols, and more.

SUCCESS STORY

RPA enterprises have unique security risks and challenges, and Propelex's penetration testing team is experienced in helping these companies assess their security environment and identify required changes. The Client was pleased that penetration testing provided enhanced visibility into their existing security frameworks, and actionable insights for improved security performance:

SECURE & COMPLIANT

PCI DSS · HIPAA HITRUST · SOC 2 TYPE 2 · GDPR · SOX COMPLIANCE · NIST

Propelex

PENETRATION TESTING FOR TECHNOLOGY STARTUPS

- Automated tools discovered basic AWS infrastructure flaws, including misconfigured S3 buckets. Manual testing was able to determine more complex issues, remediation of which helped optimize both security and performance for the Client's AWS assets.

- The penetration test of the Client's website revealed a variety of common, but potentially dangerous, vulnerabilities that were primarily the result of insufficient patching and updating. Remediation was fast and relatively simple.

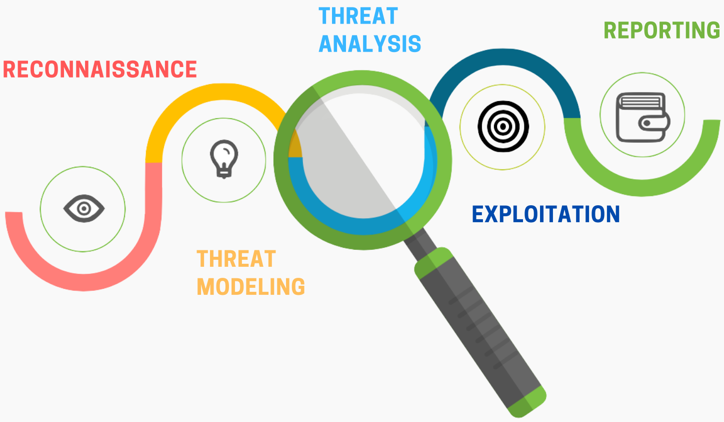
- Red teaming of the Client's web app revealed a SQL injection vulnerability that could allow exfiltration of sensitive data, among other less critical issues. Remediation operations were recommended for all vulnerabilities and the app was successfully hardened against attack.
- IoT nodes were typically located outside the Client's established security perimeter, and some represented rogue endpoint connections. Remediation focused on identifying all IoT endpoints and either securing them in a manner consistent with the Client's overall security policy, or deactivating them.

- The physical security walk-through identified several opportunities to implement improved authorization and activation controls, including more secure badges and a requirement to check-in when transiting between areas with different security levels.

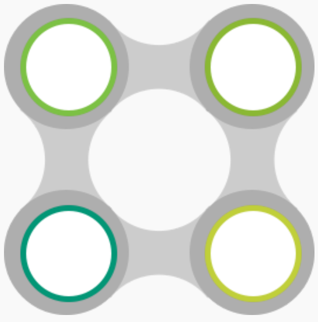
- SCADA network testing revealed several security issues, including an unchanged factory default credential, insufficient physical access restrictions to the SCADA control center, and multiple patches and updates. Recommended remediations were implemented immediately.

APPROACH

Identify organization's exploitable security vulnerabilities through a systematic process. Understand overall health of your network, application, mobile, cloud & physical controls.



RISK RATING METHODOLOGY



Threat Agent Factors
Skill Level
Motive
Opportunity
Size

Vulnerability Factors
Ease of Discovery
Ease of Exploit
Awareness
Intrusion Detection

Technical Impact Factors
Loss of Confidentiality
Loss of Integrity
Loss of Availability
Loss of Accountability

Opportunities
Financial Damage
Reputation Damage
Non-compliance
Privacy Violation

SECURE & COMPLIANT

PCI DSS · HIPAA HITRUST · SOC 2 TYPE 2 · GDPR · SOX COMPLIANCE · NIST