TEVORA™

tevora.com

Threat Management

Internet of Things (IoT) Penetration Testing

Cybercriminals constantly evolve their attack tactics and digital attributes in order to bypass the latest security controls and exploit vulnerabilities in systems, software, and endpoints. In this challenging threat environment, you need a partner that can help you manage your risk.

Tevora IS that partner. Our certified and experienced engineers proactively **test** your IT environment to uncover security risks, **remediate** existing threats and vulnerabilities, **assess** compliance with industry security requirements and **train** users on security awareness. If you suspect a compromise, Tevora's elite team can **isolate** the threat, **clean** the system, and **build** your defenses to help protect against future attacks. ▲

The Internet of Things (IoT) is a network of connected "things" – computing devices that are embedded in everything from washing machines to automated manufacturing equipment. These devices possess complex capabilities and can connect to the Internet and to each other, allowing for tremendous efficiencies in our daily lives and opportunities for business. Unfortunately attackers have found ways to benefit, too, by leveraging the advanced functionality and often rudimentary security of these devices for malicious purposes.

Tevora's IoT Penetration Testing Process

1. Reconnaissance

- Perform static analysis of hardware and firmware
- Identify supporting platforms and services
- Perform dynamic analysis of device communication, including protocols and traffic over Bluetooth, Wi-Fi, ZigBee and other networks
- Conduct whitebox testing including reviews of
  - Documentation
  - IoT platform architecture

2. Assessment

- Perform application logic analysis
- Identify known vulnerabilities including
  - Transport security issues
  - Known vulnerable services
- Conduct input validation and fuzzing
- Develop proof-of-concept exploits to demonstrate potential IoT vulnerabilities

3. Report

- Provide a detailed findings report with recommended remediation
- Retest with validation
- Present findings to executive team
- Create an executive summary of findings for management

TEVORA™

tevora.com

Our Purpose

To protect the world from cyberthreats.

Insightful Advice
Expert Resource
Confident Delivery

About Us

Founded in 2003, Tevora is a specialized management consultancy focused on cybersecurity, risk, and compliance services. Based in Lake Forest, CA, our experienced consultants are devoted to supporting the CISO in protecting their organization's digital assets. We make it our responsibility to ensure the CISO has the tools and guidance they need to build their departments, so they can prevent and respond to daily threats.

Our expert advisors take the time to learn about each organization's unique pressures and challenges, so we can help identify and execute the best solutions for each case. We take a hands-on approach to each new partnership, and –year after year –apply our cumulative learnings to continually strengthen the company's digital defenses.

Go forward.
We've got your back.

Tevora's IoT penetration testing enables your organization to embrace the potential of IoT while keeping your organization protected. Our team applies advanced expertise, capabilities and leading tools to determine the potential risks of your IoT devices and connections, including the gateways that bridge the communications between the devices and your IT infrastructure or cloud. We can help you create forward-thinking policies that address IoT vulnerabilities before they are discovered by attackers.

Our holistic approach to IoT penetration testing includes IoT device whitebox testing and platform architecture review, static analysis of hardware and firmware and dynamic analysis of device communications including protocols and traffic over Bluetooth, Wi-Fi, ZigBee and other networks. The results of our testing enable Tevora's threat team to determine the impact a targeted IoT attack could have on your organization's core platforms and services, and provide recommendations for securing your infrastructure from the compromise of an IoT device such as the reverse engineering of hardware or impersonation of a device.