TEVORA

One Spectrum Pointe Drive, Suite 200
Lake Forest, California 92630
t: 949.250.3290 | **e:** info@tevora.com

INTERNET OF THINGS PENETRATION TESTING

Guarding your organization's assets can be a vast undertaking. Tevora's elite threat team combines years of industry experience with exceptional outside-the-box thinking skills and industry certifications to provide you with the answers you need. By going beyond simple automation tools testing, we can help you understand whether your current controls are effective in protecting you from external and internal threats.

DEFEND A GATEWAY TO YOUR NETWORK

We live in a highly-connected world with an increasing number of devices with complex computing capabilities and network connectivity. These devices not only allow for greater efficiencies in our day-to-day lives but also create new business opportunities. As with any new model, Internet of Things (IoT), presents a new set of problems that need to be solved. For example, attackers are now leveraging the advanced functionality, and often rudimentary security, of these devices for malicious purposes.

Most businesses are acutely aware and increasingly overwhelmed by the challenges of securing devices and protecting critical assets. Tevora's elite threat team has the knowledge and experience to understand key exploits and the ability to test for new vulnerabilities to help protect your systems from harm. Understanding the potential threats at an early stage can empower your business to create forward-thinking policies addressing IoT vulnerabilities before they are discovered by attackers.

SECURING YOUR PLATFORMS

Tevora's elite threat team offers holistic testing of IoT devices to determine the impact a targeted attack could have on your organization's core platforms and services. We help ensure you are protected from compromise in the event of reverse engineering of hardware or attacker impersonation of devices.

1 RECON

- Static analysis of hardware and firmware
- Identification of supporting platforms and services
- Dynamic analysis of device communication, including network traffic, bluetooth, wireless and zigbee
- Whitebox testing including documentation review and IoT platform architecture review

2 ASSESS

- Application logic analysis
- Identification of known vulnerabilities, including transport security issues and identification of known vulnerable services
- Input validation and fuzzing
- Proof of concept exploits

3 REPORT

- Executive summary for management
- Detailed findings report with recommended remediation
- Retesting with validation
- Executive presentation