Enhance Security with Expert Penetration Testing

FINITE STATE

Take Control of Connected Device Risk

Finite State's comprehensive pen testing services are tailored for IoT device manufacturers and play a vital role in securing organizational defenses against evolving cyber threats. Our approach combines meticulous source code examination, in-depth threat modeling, and rigorous binary analysis to identify vulnerabilities, mitigate risks, and ensure compliance with global security standards. By combining advanced technology and human expertise, Finite State empowers organizations to build robust, transparent, and resilient software systems.

Finite State has built a reputation for efficacy and trustworthiness, and our operational standards and methodologies have won the respect of significant governmental agencies in the US and UK.

> 46% of companies don't do pen tests because of the significant drain on internal resources

Key Features

- **Automated & Manual Testing:** Advanced automation combined with expert manual testing provides deeper insights & identifies complex security issues for highly accurate results.
- **CI/CD Integration:** Finite State integrations support automation at scale for all firmware across business units.
- **Comprehensive Coverage:** Our broad pen-testing coverage includes hardware tampering, physical debug connectivity, network services, firmware & applications, web & API interfaces, as well as mobile & off-device management.
- **A Consolidated View of Your Security Landscape:** Results from Finite State & third-party security tools are integrated into our ongoing source code software composition analysis, static application security testing, & binary analysis to provide a unified view of aggregated data.

Benefits of Finite State's Penetration Testing

- **Regulatory Compliance** with global regulatory standards essential for international market entry, including EU CRA, NIST, Cyber Trust Mark and more.
- **Improved Public and Stakeholder Trust**
- **Accelerated Time-to-Market**
- **Cost-Effective Security Solutions** that significantly reduces the time and costs associated with security testing and optimizes internal resources.
- **Enhanced Security Posture**

A Closer Look at Finite State's Penetration Testing Process

Every penetration test is scoped to include a specific hardware revision and software builds to be tested. Based on threat modeling and the collective experience of our Red Team, Finite State can conduct the following testing activities on each device as part of the IoT ecosystem as needed:

Analysis of cloud-based authentication mechanisms, web application, & API analysis on 1st party implementations, unless prior authorization & scope expansion can be obtained for 3rd party implementations.

Analysis of firmware components to discover security configuration; binary analysis to discover previously unknown vulnerabilities, including deeper manual analysis of exploitability of findings.

Capture and analysis of network activity to determine outbound network services in use and establish network service fingerprints.

Exposure of network service discovery, fingerprinting, and interaction to identify network-facing threats from known vulnerabilities.

Interaction with debug functionality in combination with normal operation to discover undocumented features that could affect the security or functionality of the tested modules

Exposure of device-hosted web application implementation, fingerprinting, and interaction to identify network-facing threats from known and potential unknown vulnerabilities.

Service Deliverables

- Detailed Software Bills of Materials, vulnerability scan reports, and penetration test reports. These documents provide insights, context, and actionable recommendations based on our findings.
- Cryptographic hashes of the evaluated software binaries and other key files to ensure integrity and traceability of results down to the specific files that were assessed.
- Our professional assessment of its security outlining the overall testing methodology, detailed findings, and recommendations.
- 90-day access to our team of experts who can provide guidance and clarification needed to aid remediation efforts.

Secure Your IoT Future Today

Finite State's penetration testing services equip IoT manufacturers with the tools and expertise needed to navigate the complex landscape of global regulatory compliance and ever-evolving security challenges.

Partner with us today and ensure your products are compliant and secure against the threats of tomorrow.