IoT & Product Security Review

Bishop Fox's Product Security Review helps fortify your devices' weaknesses by leveraging a multi-point testing methodology extending beyond known vulnerabilities to keep security issues from reaching production and avoid real-world attacks.
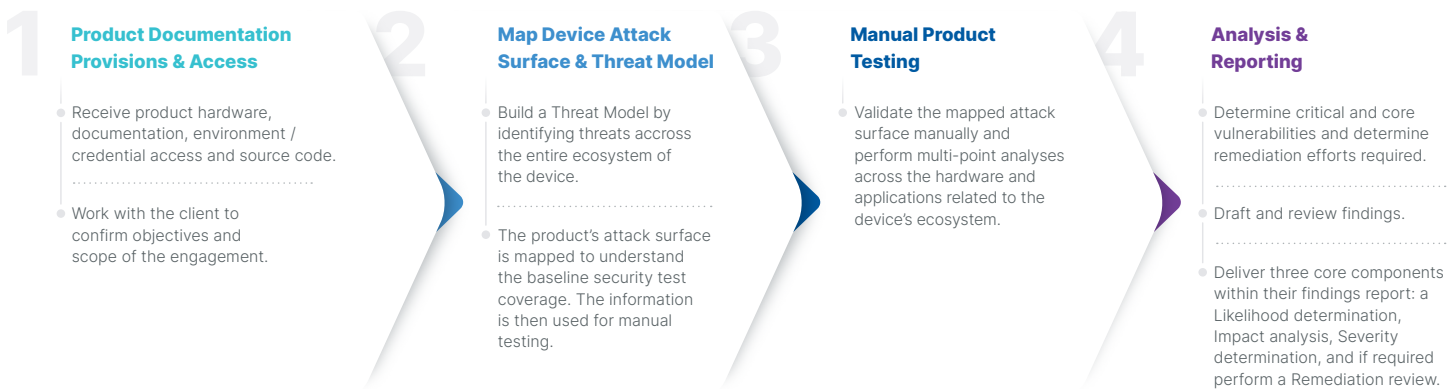
Act before impact. Don't let devices be your downfall.

Bishop Fox's Product Security Review stands alone in its depth and breadth of security testing for interconnected devices.

Accommodating an extensive range of products, our seasoned team of ethical hackers are skilled in compromising smart devices, consumer products, industrial control systems, IoT, and everything in between. Starting with a high-fidelity map of your device's complete attack surface, we deconstruct it down to the code, application, electrical components, and interdependencies that attackers could use to their advantage. Applying automation at the right places to discover known vulnerabilities, we reserve our battle-tested experts to break down those hard-to-find security issues that lie deep within product functionality. From fuzzing to in-depth code analysis, our multi-point methodology performs the same tactics, tools, and techniques your devices will likely face in a real-world attack.

This meticulous process ensures even the most obscure threats and edge-case scenarios are accounted for. Arming your team with prescriptive actions based on the likelihood and severity of exploitation, remediation can be implemented earlier in the development process ultimately helping organizations avoid costly redesigns and late-stage disruption.

1 Product Documentation Provisions & Access

- Receive product hardware, documentation, environment / credential access and source code.
- Work with the client to confirm objectives and scope of the engagement.

2 Map Device Attack Surface & Threat Model

- Build a Threat Model by identifying threats across the entire ecosystem of the device.
- The product's attack surface is mapped to understand the baseline security test coverage. The information is then used for manual testing.

3 Manual Product Testing

- Validate the mapped attack surface manually and perform multi-point analyses across the hardware and applications related to the device's ecosystem.

4 Analysis & Reporting

- Determine critical and core vulnerabilities and determine remediation efforts required.
- Draft and review findings.
- Deliver three core components within their findings report: a Likelihood determination, Impact analysis, Severity determination, and if required perform a Remediation review.

Extend Expertise to Accommodate Any Device and Its Unique Attributes

Alleviate the burden of hiring and retaining hard to find experts skilled in deconstructing devices and uncovering potential attacker pathways.

Get a Comprehensive View of Your Device's Attack Surface

From the circuit level to the cloud, uncover all vectors of attack with a complete breakdown of your product's applications, code, internal components, and connected networks.

See Your Device Through the Lens of a Skilled Attacker

Understand how a targeted adversary would search for common vulnerabilities and often missed security issues hidden deep within critical functionality.

Discover Known Vulnerabilities and Often Missed Edge Cases

Uncover the full extent of security issues using the same tactics and techniques your devices are likely to face in real-world attack scenarios.

Focus Corrective Actions Where It's Needed Most

Concentrate remediation on issues that have the greatest impact with likelihood determination and severity scoring based on threat-source motivation, nature of the vulnerability, and mitigating controls.

Address Issues Earlier in the Product Lifecycle

Avoid costly redesigns and disruptive late-stage changes with prescriptive actions that design teams can integrate earlier in the development process.

Don't let devices be your downfall.

Harden your defenses with offensive testing.

Bishop Fox takes pride in delivering a highly-skilled team of product and device experts with years of ethical hands-on hacking experience. Their multi-point testing approach is purpose-built to dig deeper, across multiple hardware, cloud and software requirements to exploit findings and uncover likely attack paths. Illuminating several issues and providing prescriptive recommendations strengthens your ability to efficiently improve the security of your products wile progressing in the product development lifecycle.

HARDWARE

AUTOMATED
- DoS
- Scanning for Exposed Network Services
- Fault Injection
- Glitching
- Fuzz Testing

MANUAL
- Identify Debugging Ports
- Testing Tamper Resistance
- Testing RF Interfaces
- Testing Firmware Update Process
- Testing for Secure Communications (RF, Networks, etc.)
- Fuzz Testing

APPLICATION

AUTOMATED
- Scanning Web Interface and Code
- Validation Bypass
- Buffer Overflow
- Cryptographic Weaknesses

MANUAL
- Exploiting Identified Vulnerabilities
- Key Binary Dissection
- Multi-point Software Testing Analysis
- Race Conditions

| EXPERTISE TO TEST ANY DEVICES ATTRIBUTES | COMPREHENSIVE VIEW OF YOUR ATTACK SURFACE | UNDERSTAND YOUR DEVICE THE WAY AN ATTACKER DOES | DISCOVER OBSCURE VULNERABILITIES AND MISSED EDGE CASES | FOCUS CORRECTIVE ACTIONS WHERE ITS NEEDED MOST | ADDRESS ISSUES EARLY ON IN THE PRODUCT LIFECYCLE |

By The Numbers

6,000+
Offensive security projects delivered

1,000+
Global customers protected

81
Net promoter score

16+
Years of experience

Trusted By Industry Leading Organizations

amazon

Google

Parrot

workplace from FACEBOOK

august

zoom

EQUIFAX

CHANGE HEALTHCARE

SONOS

Product Security Review Client Satisfaction

94%
Understand targeted outcome and objectives

100%
Replicate real-world adversaries

100%
Identify threats and weaknesses

100%
Prioritize and communicate findings

About Bishop Fox

Bishop Fox is the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments. We've worked with more than 25% of the Fortune 100, eight of the top 10 tech companies, and hundreds of other organizations to improve their security. Our Cosmos platform was named Best Emerging Technology in the 2021 SC Media Awards, and our offerings are consistently ranked as "world-class" in customer experience surveys. We're an active participant in the security community and have published more than 16 open-source tools and 50 security advisories in the last five years. Learn more at **bishopfox.com** or follow us on Twitter.