BISHOPFOX

DATA SHEET

HARDWARE PENETRATION TESTING

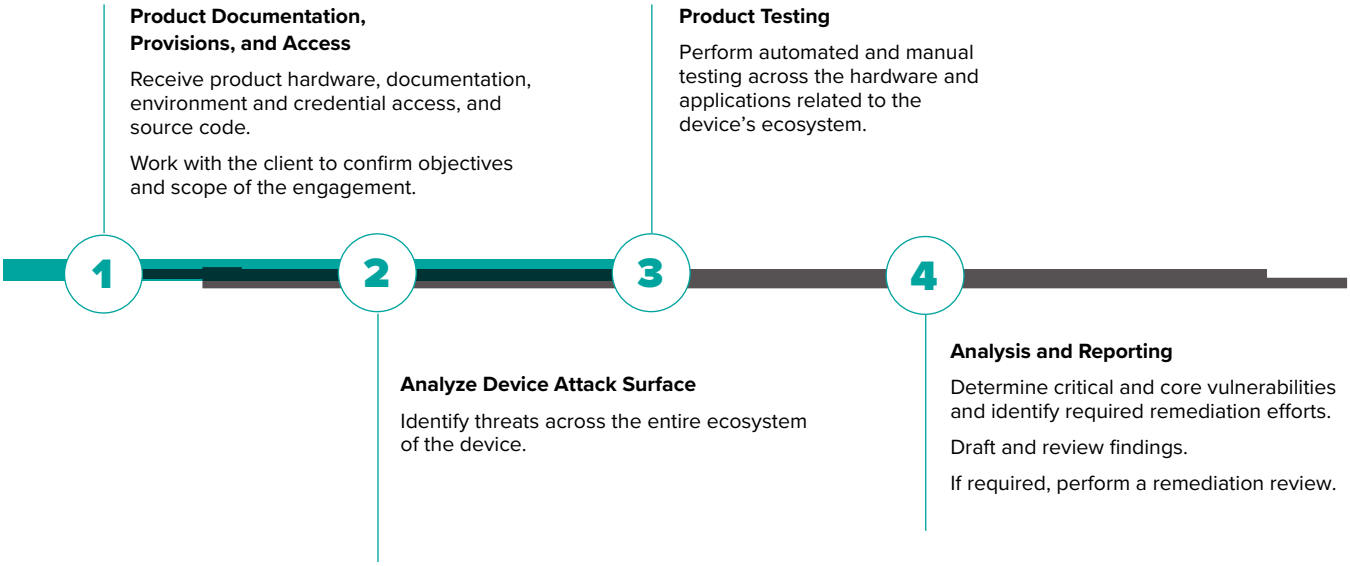
Bishop Fox's Hardware Penetration Testing helps fortify your device security with a comprehensive assessment methodology that extends beyond known vulnerabilities to keep security issues from reaching production and avoid real-world attacks.

EXPERT TESTING FOR THE CONNECTED WORLD

Bishop Fox's Hardware Penetration Testing validates that your connected products are resilient against real-world threats, protecting your users, partners, and your brand. 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.

We can deconstruct your device down to the code, electronic 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 includes the same tactics, tools, and techniques your devices will likely face in a real-world attack.

Our assessment arms your team with prescriptive actions based on the consequences of exploitation and allows you to implement remediation earlier in the development process so you can avoid costly redesigns and late-stage disruption.



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 Detailed View of Your Device's Attack Surface

From the circuit level to the cloud, uncover vectors of attack across your product's applications, code, internal components, and connected networks.

See Your Device Through the Lens of a Skilled Attacker

Understand how a motivated adversary would search for vulnerabilities and security issues hidden deep within critical functionality.

Discover Known Vulnerabilities and Often-Missed Edge Cases

Uncover 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.

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 device 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 it's needed most

↓ Address issues early in the product lifecycle

CLIENT SATISFACTION

94%
understand targeted outcome and objectives

100%
replicate real-world adversaries

100%
identify threats and weaknesses

100%
prioritize and communicate findings

TRUSTED BY INDUSTRY LEADING ORGANIZATIONS

amazon · Google · zoom · SONOS · august · Parrot · EQUIFAX · CHANGE HEALTHCARE · workplace from FACEBOOK

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've been actively contributing to and supporting the security community for almost two decades and have published more than 16 open-source tools and 50 security advisories in the last five years.

LEARN MORE AT BISHOPFOX.COM