

ADVERSARIAL CONTROLS TESTING

A customized, attack-based approach executed by our Red Team puts your email, endpoint, and network security controls to the test, so you can be confident in your security posture and strengthen defenses quickly where needed.

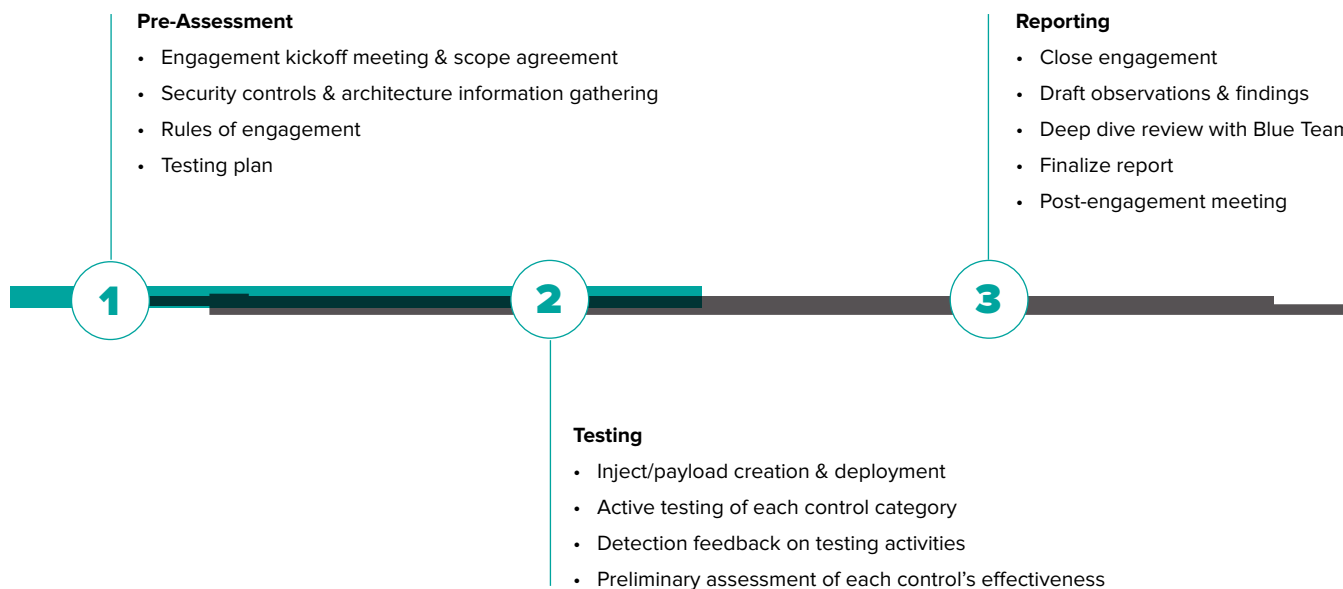
REAL-WORLD APPROACH. FAST, EFFECTIVE RESULTS.

TESTING CONTROLS THROUGH THE LENS OF AN ATTACKER

Bishop Fox's Adversarial Controls Testing is a collaborative offensive security testing service that quickly validates the effectiveness of your email, endpoint, and network security controls by simulating real-world cyberattacks. Led by Red Team experts using purpose-built automated playbooks, this service uses adversarial tactics and techniques mapped to the MITRE ATT&CK framework to assess how well your defenses can detect and prevent today's top cyber threats.

Each assessment is tailored to your organization's specific environment, ensuring that the testing is realistic and relevant, with test cases designed to simulate common attack methods such as phishing, command execution, and credential dumping. Throughout the engagement, your security team actively participates by reviewing telemetry in real time, enabling immediate feedback and adjustments.

At the conclusion of testing, Bishop Fox delivers a comprehensive report with a clear assessment of each control area, categorizing their effectiveness and providing actionable recommendations for improvement. Results are delivered quickly, typically within three weeks, giving your team the insights needed to strengthen defenses without delay and improve your organization's overall resilience.



KEY OUTCOMES



Validates the Effectiveness of Key Security Controls Against Real-World Attacks



Collaborative Approach, Customized to Your Environment



Tech-enabled Human Testers for Deep Expertise and Maximum Efficiency



Assessment Delivered in Weeks, Not Months



Actionable Findings & Recommendations

ATTACK-FOCUSED ASSESSMENT OF KEY CONTROLS

By simulating attacks on your environment, our consultants encounter your controls just like a real threat actor would. We use this attack-based approach to determine if your controls are working to detect or prevent these attack behaviors, or if we could successfully bypass and evade them. Below are examples of the types of controls that we encounter in an engagement, which will vary based on your unique environment.

ENDPOINT	NETWORK	EMAIL
SIEM		
• Overall host configuration hardening, enforced by MDM/UEM agents, endpoint-related group policy, logon scripts, etc. • EDR or "Unified Threat Management" • Endpoint DLP • Host-based firewall/IDS • Application whitelisting	• Active Directory security/hardening • Network firewall • Network IDSH • Secure Web Gateway • Network architecture controls like segmentation	• Secure Email Gateways • Usage of email authentication protocols like Sender Policy Framework • DKIM & DMARC • Anti-spam and anti-phishing filtering • Advanced threat protection • Email DLP • Secure DNS

TRUSTED BY INDUSTRY LEADING ORGANIZATIONS



SONOS

EQUIFAX

Google



CHANGE
HEALTHCARE

ABOUT BISHOP FOX

Bishop Fox is the leading expert in offensive security, providing comprehensive assessment of modern environments with continuous attack surface management, red teaming, and penetration testing for applications, cloud, network, and products. We've worked with more than 25% of the Fortune 100, half of the Fortune 10, eight of the top 10 global technology companies, and all of the top global media companies to improve their security. Our Cosmos platform won six awards for innovation in 2022 from programs including SC Media, The American Business Awards, The Globes, and Cyber Defense Magazine and was named an ASM Fast Mover and Leader in both 2022 and 2023 by GigaOm. 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](https://bishopfox.com)