

RED TEAM & ADVERSARIAL EMULATION

OUR EXPERTS PUT **YOUR DEFENSES TO THE ULTIMATE TEST TO VALIDATE YOUR SECURITY** CONTROLS AND **STRENGTHEN YOUR RESILIENCE** BEFORE ADVERSARIES STRIKE.

YOUR CHALLENGE

Your organization faces a **sophisticated threat landscape**. Today's cyber adversaries are stealthy, persistent, and creative. They no longer rely solely on brute force or simple exploits. Instead, they use subtle, targeted attacks that blend technical compromise, social engineering, and physical intrusion to bypass defenses and achieve their objectives.

While vulnerability scanning and penetration testing are critical to proactively identify vulnerabilities, neither realistically represents the complex, full-scope operations of an adversary. You need to be confident that your security controls and processes will work as expected during an actual attack.

KEY OUTCOMES

Understand your ability to detect, respond, and recover from a breach—before it happens >

Validate the effectiveness of your security controls across your technical, physical, and human attack surface >

Prepare and build resilience against sophisticated attacks by the latest threat actors >

Get tailored, actionable recommendations to improve your security posture >

OUR SOLUTION

Adversarial emulation, commonly referred to as red teaming, **puts your defenses to the test** using the same tactics, techniques, and procedures (TTPs) real adversaries use, but in a controlled, low-risk environment. Unlike other forms of testing, these engagements are designed to evaluate people, processes, and technology together. With a range of approaches that simulate breach scenarios at your organization, adversary emulation is the most effective way to know if your team is prepared to detect, respond, and recover—before a real breach happens.

The effectiveness of a red team engagement is only as good as the expertise behind it. At Bishop Fox, every engagement is led by seasoned offensive security professionals who think and operate like real-world adversaries, leveraging cutting-edge tooling and proprietary methodologies anchored in the MITRE ATT&CK framework. Our Red Teamers are strategic and creative, with diverse skills and deep knowledge of the latest threats, enabling them to identify nuanced vulnerabilities and exploit complex attack paths others might overlook.

No two organizations are the same, which is **why we never take a one-size-fits-all approach or deliver generic guidance**. Engagements are tailored for your unique environment, objectives, threat actors, and the scenarios that keep you up at night. At the end of an assessment, you're armed with actionable results, detailed findings, and clear recommendations to strengthen your defenses, enhance detection, and respond faster in the face of real threats.

"The Red Teaming staff was very helpful in explaining the process and methodology they were going to use. They always communicated with us every step of the way. They are willing to go above and beyond to ensure that the engagement is to the customer's satisfaction."

— **DIRECTOR OF INFORMATION SECURITY**
FINANCIAL SERVICES

BISHOP FOX ADVERSARIAL EMULATION SERVICES

Bishop Fox offers a comprehensive portfolio of services designed to test your resilience against the most advanced skillsets and innovative attack methods, across technical, physical, and human domains. We help you validate the effectiveness of your entire security program with methodologies encompassing attack simulation and real-time collaborative testing, and support for ransomware readiness and compliance use cases.

ATTACK SIMULATION

RED TEAM – EXTERNAL BREACH

Emulates an attack targeting your perimeter to reveal how an adversary could gain initial access through exposed infrastructure, and how well your team can detect and respond to that intrusion.

RED TEAM – ASSUMED BREACH

Simulates a real-world attack scenario where the Red Team starts with an initial foothold and attempts to achieve specific objectives (e.g., sensitive data or privileged access).

PHYSICAL PENETRATION TESTING

Simulates a breach of your facility using attack tradecraft to test physical security and access controls. Assesses entry points, security protocols, and on-site personnel responses to identify security gaps.

SOCIAL ENGINEERING

Tests user awareness, process resilience, and technical controls with targeted human-focused attack techniques, such as phishing, vishing, smishing, and deepfake campaigns, with the goal of achieving defined trophies. Recommended as part of a Physical Penetration Test or broader Red Team engagement.

COLLABORATIVE TESTING & PREPAREDNESS

PURPLE TEAM

Identifies, tests, and improves your Blue Team detection capabilities through real-time collaboration with our Red Team. You receive specific feedback and actionable recommendations for immediate improvements.

ADVERSARIAL CONTROLS TESTING

Efficiently validates the effectiveness of your email, endpoint, and network security controls, in collaboration with your Blue Team.

INCIDENT RESPONSE TABLETOP EXERCISES

Tests and strengthens your incident response and crisis management capabilities through structured, discussion-based simulations with your key stakeholders. Leverages realistic threat scenarios customized for your business.

TARGETED USE CASES

RANSOMWARE READINESS

Applies the latest ransomware-specific threat intelligence around emerging variants, attacker TTPs, and industry-specific nuances to test the effectiveness of your threat detection and response.

THREAT-LED PENETRATION TESTING (TLPT)

Designed for organizations subject to regulations like DORA, CBEST, or TIBER-EU. Guided by threat intelligence and structured around realistic threat scenarios, to deliver regulator-ready reporting.

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. Learn more at bishopfox.com.