BreakPoint Labs™
a Valiant Solutions Company

Reducing cyber risks to your mission by understanding your network, unique threats, and security controls.

CYBERSECURITY ASSESSMENTS

BreakPoint Labs leverages its advanced technical proficiency and decades of experience in securing complex programs to thoroughly evaluate risk factors that could impact mission success.

WHO WE ARE

Technically Proficient Experts

Our distinguished workforce comes with robust technical knowledge, real-world cybersecurity experience, and the certifications to meet your mission requirements.

A Team With A Proven Track Record of Results

We've delivered on some of the most complex missions impacting our national security — demonstrating excellence in offering effective and sustainable mission-focused security solutions.

Specialists Who Provide Flexible Solutions

Regardless of mission scale or complexity, we can develop and harness technology that meets your security needs.

Dedicated Practitioners That Go Beyond Automated Tools

Most security companies race to complete an assessment or network scan to quickly generate a report — leaving you with a mountain of false positives and incomplete risk analysis. Our team takes the extra steps to identify gaps in current defenses while demonstrating precisely how adversaries exploit your risks.

WHO WE SERVE

- Department of Defense (DoW)
- Civilian Agencies
- State & Local Governments
- Academic Institutions
- Healthcare Industry
- Commercial Enterprises

CORE COMPETENCIES: CYBERSECURITY ASSESSMENTS

We help you realize your mission on time in a secure environment by evaluating control gaps, vulnerabilities, and misconfigurations that need remediation:

Cyber Red Teaming & Threat Emulation

Demonstrating how you'd stand up against today's cyber threats, BreakPoint Labs' Red Team Operators replicate actual attacks against your security and your defensive teams detection and incident response capabilities. Using real-world adversarial tactics our experts can show you where you need to enhance your security to ensure mission success.

Penetration Testing

Through attack vectors like social engineering or exploiting your external boundary into the internal network, BreakPoint Labs simulates manual and automated techniques to exploitable vulnerabilities and critical risk within your environment.

Vulnerability Assessment

Threat actors often seek out the path of least resistance when delivering a cyber attack. BreakPoint Labs runs network vulnerability scans and risk evaluations to identify common vulnerabilities and exposures (CVE's) that an adversary can use as an attack vector to deter your mission's success.

Risk & Security Control Assessment

BreakPoint Labs provides control gap analysis across your network, applications, physical layer, and other domains to ensure your program has what it takes to protect against today's threats and meet compliance requirements. Our team also delivers robust assessments to help prioritize remediation efforts based on risk severity.

A COMPLETE CYBERSECURITY METHODOLOGY FOR ALL REQUIREMENTS

At BreakPoint Labs, we pride ourselves on leveraging industry-proven methodologies to deliver quality assessments that meet all compliance and framework needs.

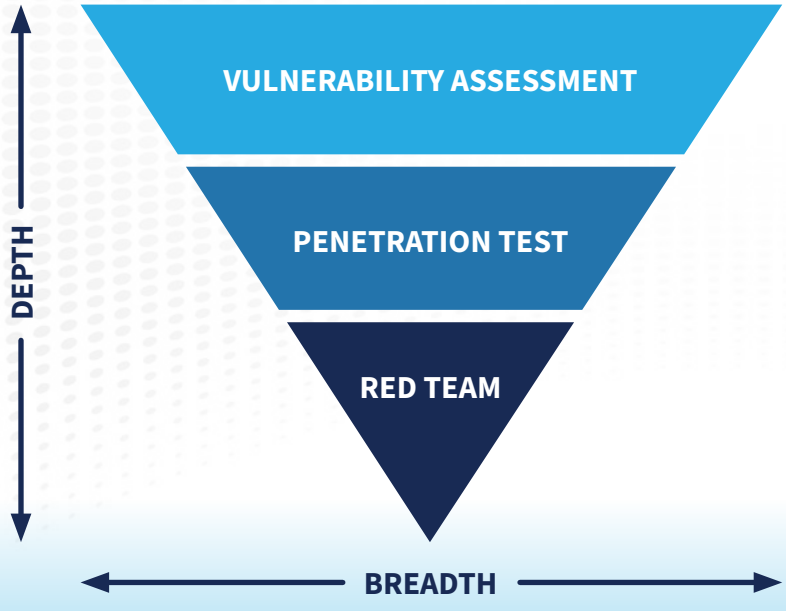
- MITRE ATT&CK Framework
- Penetration Testing Execution Standard (PTES)
- Open Web Application Security Project (OWASP) Testing Guide (OTG)
- CMMC Level 2 (C3PAO) Certified
- NIST 800-30, 800-37, 800-53/A, 800-130
- NIST 800-171 DFARS Compliance
- CNSSI 1253
- OPNAVINST N9210.3
- NIST Cybersecurity Framework (CSF)
- FISMA
- PCI Data Security Standard
- FTC Safeguards Rule

We also demonstrate a higher commitment to your mission with a comprehensive approach to cybersecurity assessments. By using manual testing techniques during penetration and vulnerability testing, in addition to automated solutions, we ensure no risk or control gap goes unnoticed.

Security Assessment Support Types

Depending on the depth and result desired by your organization, BPL can provide security assessment services from various perspectives across many domains, such as:

- Wireless Security
- Cloud Services Security
- External Security (Internet Facing)
- Application Security
- Enterprise Security (Internal Network)
- ICS/SCADA Security
- Social Engineering
- Physical Security



Vulnerability Assessment

Vulnerability Identification and Risk Review

Penetration Test

Vulnerability Identification, Exploitation and Mirror Real World Attackers

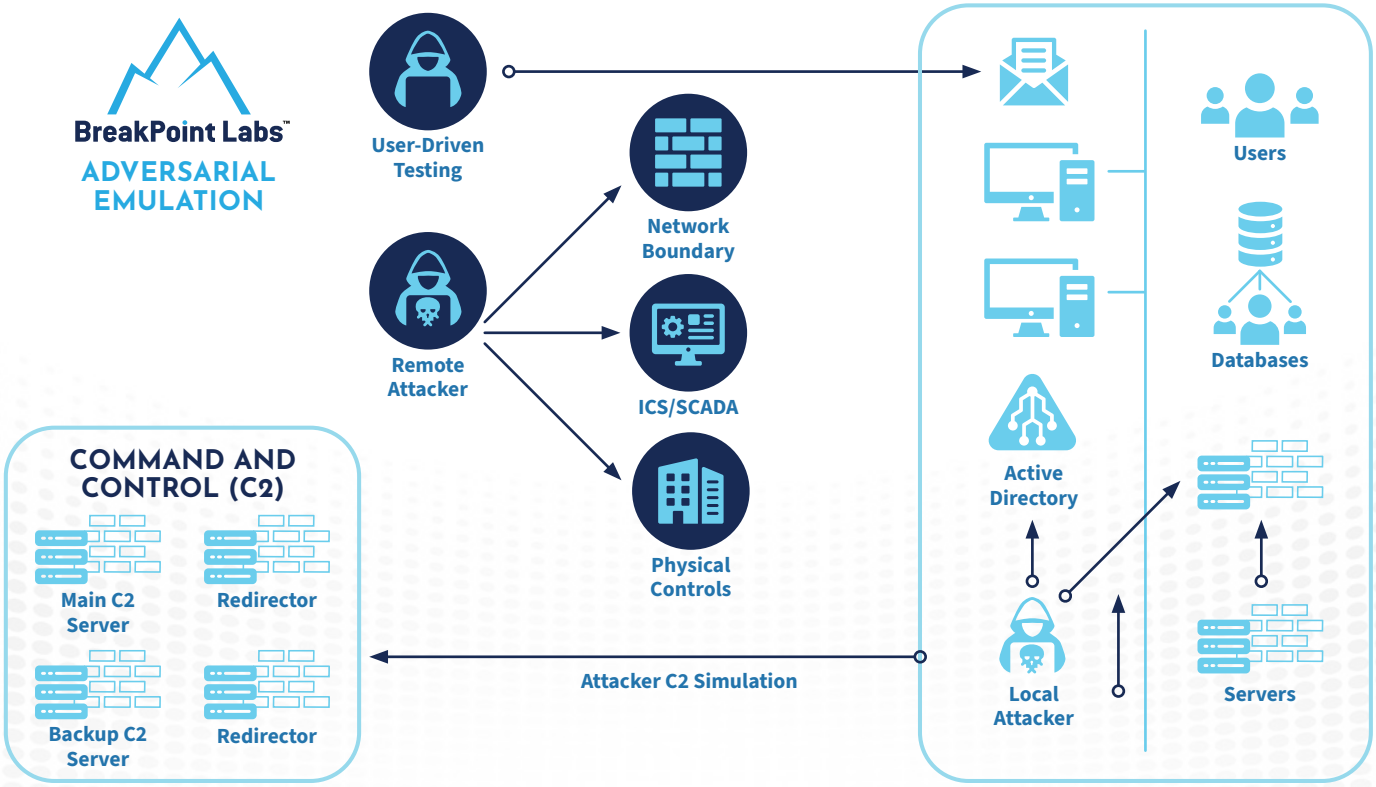
Red Team

Measuring an Organization's Defense-in-Depth while Emulating an Adversary

CYBER RED TEAMING & THREAT EMULATION

Red Team (RT) Assessments are an effective solution for organizations to gain insight into which attack paths exist within and around their environment. For an RT assessment, a stealthier approach is taken to evade and circumvent an organization's existing security controls and detection capabilities, all while the RT keeps its assessment objective(s) in mind.

BreakPoint Labs™
ADVERSARIAL EMULATION



RECON | WEAPONIZATION | DELIVERY | EXPLOITATION | INSTALLATION | COMMAND & CONTROL | OBJECTIVE

CERTIFICATIONS

BreakPoint Labs operators possess extensive expertise and qualifications necessary to conduct high-quality security assessments. We emphasize requiring hands-on technical survey qualifications from Offensive security.

- Project Management Professional (PMP)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Offensive Security Certified Professional (OSCP)
- Offensive Security Expert (OSCE)
- Offensive Security Certified Wireless Professional (OSWP)
- Offensive Security Experienced Professional (OSEP)
- Red Team Alliance Physical Red Teaming: Covert Methods of Entry (CMOE)
- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Penetration Tester (GPEN)
- GIAC Industrial Cyber Security Professional (GISCP)

PAST PERFORMANCE (Notable Projects)

Cyber Red Team Services for the U.S Army ERDC

Under contract to the U.S. Army Engineer Research and Development Center (ERDC), BreakPoint Labs delivers Cyber Red Team services across the DoD Information Network (DODIN) — emulating adversarial tactics, techniques, and procedures (TTPs) to spot the most high-impact infrastructure vulnerabilities to the program's mission.

Enterprise Penetration Testing for HHS Inspector General

Working under contract with the Office of the Inspector General (OIG) for the Department of Health and Human Services (HHS), BreakPoint Labs conducts network penetration testing across cloud service provider (CSP) environments, networking infrastructure, and web applications — assessing the effectiveness of controls for select mission-critical environments against real-world cyber attacks.

U.S. Army Corps of Engineers Security Control Assessor-Validator Services

Contracted with the U.S. Army Corps of Engineers (USACE), BreakPoint Labs is a certified Security Control Assessor-Validator (SCA-V) that delivers risk assessment and control evaluation services to the Department of Defense (DoD). They also support DoD leadership with guidance on security governance policies and technical recommendations to reduce risk.

Covert Red Teaming for the Department of Commerce Inspector General

Hired by the Department of Commerce (DOC) Office of the Inspector General (OIG), BreakPoint Labs emulated real-world attack scenarios that targeted specific mission-critical systems — providing insights into what a sophisticated attack actor could achieve with modern tactics. The BreakPoint Labs Red Team Operators successfully evaded monitoring systems, established threat persistence in the network, and eventually elevated permission levels for access to highly sensitive data.

COMPANY INFORMATION

CAGE Code: **7FZP3**
SAM UEID: **WAU7C2EAKGN9**
Small Business

BUSINESS CERTIFICATIONS

ISO 9001:2015 Certified: **Cert #14812**
ISO 27001:2022 Certified: **Cert #20297**
CMMI-SVC Level 4 Appraised
CMMC Level 2 (C3PAO) Certified
(Appraisal #77434 | Exp Oct. 17, 2028)

NAICS CODES

541330 Engineering Services
541511 Custom Computer Programming Services
541512 Computer Systems Design Services
541513 Computer Facilities Management Services
541519 Other Computer Related Services (primary)
541715 Research and Development in the Physical, Engineering, and Life Sciences (except Nanotechnology and Biotechnology)

SIC CODES

7371 Custom Computer Programming Services
7373 Computer Integrated Systems Design
7379 Computer Related Services, Nec*
7376 Computer Facilities Management
7379 Computer Related Services, Nec* (primary)

HEADQUARTERS

8116 Arlington Blvd., #255
Falls Church, VA 22042
info@breakpoint-labs.com
844-HACKME2 (844) 422-5632
https://breakpoint-labs.com

CONTRACT VEHICLES

- GSA OASIS+:
  Unrestricted: **Contract #: 47QRCA25DU054**
  Total Small Business: **Contract #: 47QRCA25DS129**
- GSA Multiple Award Schedule (MAS):
  Contract #: GS-35F-248GA
  - Highly Adaptive Cybersecurity Services (HACS)
  - Cloud Professional Services
  - IT Professional Services
- SeaPort NxG: **Contract #: N0017825F7153**
- MDA Shield IDIQ **Contract #: HQ085926DF042**
- CDAO Tradewinds Solutions Marketplace
  www.tradewindai.com
- Platform One Solutions Marketplace
  https://p1.dso.mil/marketplace

CONTACT US

Diana Orozco
Business Development Director
(210) 216-6800
dorozco@breakpoint-labs.com

Denise Cole
Contracts Administrator
(703) 495-3559
dcole@breakpoint-labs.com