RedTeam Security
THREAT PREVENTION EXPERTS

RedTeam Security Services Overview

This overview highlights our portfolio of offensive security services and how each can benefit your organization in reducing your attack surface by addressing security vulnerabilities.

www.redteamsecure.com | info@redteamsecure.com

Table of Contents

Penetration Tests

Application Security

Offensive Security

Training & Certifications

Risk Assessments

Phishing Engagements

Penetration Tests

RedTeam Security's penetration testing will identify and exploit your organization's security vulnerabilities through a systematic testing process focused on your networks, applications, physical facilities, and human assets.

Understanding and addressing cybersecurity issues can help protect your company from real-world cyber-attacks. RedTeam Security experts have the knowledge and experience to strengthen your network security and protect sensitive data. Our penetration testers act as ethical hackers to uncover security weaknesses. After completing thorough pen testing and security assessments, our security professionals will provide suggestions to remediate issues as the final product of the testing process.

Network Penetration Testing

Ethical hacking of a network environment to discover how systems will respond to a real cybersecurity threat.

Wireless Penetration Testing

Examine wireless infrastructure to uncover security flaws on wireless endpoints, hardware, and software.

Physical Penetration Testing

Assess all physical security controls through attempts to gain physical access to restricted areas and data.

Application Security

Applications are particularly vulnerable to external attacks because they are inherently designed to be accessible to the Internet. RedTeam Security's certified team of pen testers is experienced in various application testing environments, including Android applications, iOS, Windows, and other common operating systems and apps.

We take the time to understand your application's purpose and user interactions, so we can tell you that a would-be attacker would take a different time. Our penetration testers carefully consider the business logic implemented by application developers to provide a more thoughtful, comprehensive, and valuable deliverable.

Web Application Penetration Testing

Targeted testing of web applications to uncover vulnerabilities and potential points of exploit.

Mobile Application Penetration Testing

Analysis and testing of the security of a mobile environment to gain insights into the source code's vulnerabilities.

API Penetration Testing

Manual analysis of API functionality to assess the security of authentication, queries, and data transfers.

Offensive Security

Offensive security services are simulated cyber security tests with specific goals to discover and eliminate exploitable vulnerabilities and security weaknesses in an IT environment by ethical hacking or breaching the front-end and back-end servers.

Our offensive security services enable organizations with mature security postures to do next-level testing of their protections, procedures, and responses. In a standard penetration test, the testers are "allowed in" and are not actively being stopped when noticed. In an offensive security engagement, your team will have standard protections in place and may stop the attack, causing the team to reassess and pivot to achieve an agreed-upon goal.

Red Teaming

Multi-blended adversarial-based attack simulation against people, software, hardware, and facilities.

Adversary Simulation

Next-level testing designed to exercise procedures and technical protections just as a real-world attacker would.

Training & Certifications

Our security experts act as cyber-criminals to approach each engagement to gain company information. To catch a cyber-criminal, you must think like a criminal. RedTeam can create a custom cybersecurity training program for your employees and then test for weaknesses in how they handle those pretending to be employees, vendors, or business partners.

With 82% of all cybersecurity breaches caused by human error, implementing a security awareness program and testing it with physical social engineering is the best first step toward mitigating security risks. Regardless of industry type or organization size, every business will benefit from training its employees, leadership team, partners, and vendors to defend against insider threats and cyber attacks.

Cybersecurity Awareness Training
Online, self-paced training curriculum built to strengthen employee awareness of information security threats.

Physical Social Engineering
Test against real-world breaches of physical safeguards by assessing your people, processes, and procedures.

Risk Assessments

Risk Assessments are important preventative tools that analyze your systems and processes to understand security risks, ensure key controls are in place, and identify gaps in your cybersecurity preparedness.

Risk Assessments can be used for security upkeep and ongoing auditing of attack readiness or can serve as an initial analysis of security vulnerabilities. The assessments can be a vital tool in your partnership with RedTeam and will act as a starting place to launch your risk remediation efforts and align focus on the most at-risk areas.

Cloud Security Assessment
Overall evaluation and analysis of a cloud environment to identify weaknesses and potential entry points.

Vulnerability Risk Assessment
A detailed scan of your digital network to deliver a high-level overview of potential security vulnerabilities.

Active Directory Security Assessment (ADSA)
Identification and remidiation of risk-posing misconfigurations within Microsoft Active Directory.

Phishing Engagements

A key part of security preparedness is testing your employees' ability to readily recognize different malicious phishing attempts and what to do if one is received. RedTeam can actually develop a customized approach to make sure that your personnel follows company procedures and protect company assets.

Results collected during these simulations are compiled into reports which help organizations gauge their susceptibility to modern-day social engineering attacks. This valuable information is a crucial component to measuring the overall security posture and helps pinpoint where additional security awareness training might be needed.

Email Phishing
Test employees' ability to identify and report phishing emails through real-world attack scenarios.

Vishing
Vishing attackers call pretending to be clients, the IRS, or other authority figures to obtain secure information via phone.

Smishing
Simulated attacks over text message testing employees' perceptiveness of SMS threats.

Working with RedTeam Security

RedTeam Security is your dedicated offensive security partner. We help ensure your organization is ready to combat security threats from all angles. Our offensive security experts give you not only peace of mind but also the compliance to keep your organization running. Securing your business is what we do, and we look forward to working with you.

Manual Intensive Approach to Testing

At RedTeam Security, we believe that an effective and comprehensive penetration test can only be realized through rigorous manual testing techniques which is why our approach to testing consists of about 80% manual and 20% automated testing.

Dedicated Client Portal

Interact in real-time with your RedTeam Security experts on our user-friendly portal. See firsthand how our team can close in on your company data.

Comprehensive Attacker Tool Suite

To perform a comprehensive real-world assessment, RedTeam Security utilizes commercial tools, internally developed tools, and the same tools that hackers use on every assessment. Once again, we intend to assess systems by simulating a real-world attack, and we leverage the many tools at our disposal to effectively carry out that task.

Reporting and Remediation Recommendations

At the end of an engagement, our pen testers will deliver an in-depth analysis of the test findings in the form of a comprehensive report. Our reports show everything RedTeam Security found, how we found it and recommended remediation efforts to address any underlying risks.

Retesting

Our objective is to help empower our clients to remediate vulnerabilities, not just find them. As a result, remediation re-testing is provided at no additional cost for up to six findings within six months of project completion.

RedTeam Security
THREAT PREVENTION EXPERTS

Contact Us

Securing your business is what we do, and we look forward to working with you.

RedTeam Security
5200 Willson Rd. Suite 150
Edina, MN, 55424
info@redteamsecure.com
(952) 836-2770