Outpost24

Penetration Testing and Red Teaming

Comprehensive penetration testing and in-depth assessment of your security posture

Maintaining a deep understanding of your security levels can be complex and time-consuming. Our specialist security team, Offensive Security offers comprehensive penetration testing services that cover applications, networks, mobile and more, to uncover hidden risks and provide clear insights into your current security posture while advising on ways to enhance your defenses.

Our penetration tests are conducted by our team of highly skilled and certified ethical hackers, with extensive experience across various industries, ensuring that security issues are identified to bolster your security controls and reduce risk of breach. Our penetration testing and red team assessments rigorously identify and verify exploitable vulnerabilities within your networks and systems using the latest techniques and attack scenarios as part of a Continuous Threat Exposure Management (CTEM) program.

Our Services:

Application Security

Web Application & APIs: A onetime assessment to identify vulnerabilities within a web application and API. By simulating real attacks, we will uncover potential weaknesses that could be exploited by malicious actors.

Mobile: Thorough assessment of mobile applications running on both IOS and Android to identify flaws and mobile-specific issues.

Network & Cloud Security

Cloud Infrastructure: In-depth assessments of your cloud-hosted resources, including APIs, web applications, and databases across platforms such as Azure, AWS and Google Cloud to uncover hidden risks.

Network: Comprehensive infrastructure and systems assessments to identify exploitable weaknesses, utilizing automated, manual, and proprietary tools to locate risk exposure.

Red Team & Risk Assessment

Assumed Breach: We will assess the status of your internal network and systems to spot vulnerabilities that could be exploited by a hacker including risky users and escalation paths for adversaries.

Phishing: Phishing campaigns to evaluate susceptibility to social engineering tactics, gauging the risk of attackers compromising your environment or accessing sensitive information from your workforce.

Red Teaming: Scenario-based approach in which our team will try to obtain pre-defined crown jewels, using adversarial tools, tactics and procedures relevant to uncover attack paths.

Key Use Cases

Uncover Security Blind spots
Identification of weaknesses in your environment from an attacker's perspective, enabling you to fortify your defenses, ensuring that security gaps are closed and potential breaches are preemptively mitigated.

Expert-Led Insights
Our team of highly skilled ethical hackers will review your environment utilizing the latest techniques to uncover security issues, exploitable vulnerabilities, and logic errors.

Validation
We assess the effectiveness of your existing security controls against real-world attack scenarios, helping to minimize risks and ensure that your security infrastructure can withstand targeted attacks.

Comprehensive Reporting
Our reporting provides clear insights into identified vulnerabilities and recommendations for remediation. This enables your team to prioritize and address issues effectively, enhancing overall security posture.

> *"We selected Outpost24 because it was the best option in our thorough evaluation. We were impressed with the full solution and service delivery."*
>
> IT Security Manager
> Landsbankinn

Red Team Assessment

Enhance your organization's security posture with our Red Team Assessments, where our team of highly skilled experts employs a black-box approach to emulate real-world adversary tactics. By testing your systems without prior knowledge, we ensure a thorough evaluation of your defensive capabilities, safeguarding your crown jewels and maximize your return on investment. Our comprehensive method uncovers hidden vulnerabilities across multiple dimensions—cyber, human, and physical—utilizing a diverse array of techniques from phishing to physical penetration tests and network exploitation.

Key Offerings:

Digital Footprint Assessment

We detect visible systems, leaked information, and exploitable vulnerabilities to demonstrate attack pathways. With our detailed reports and insights, you can safeguard your operations and reduce risk of breach.

Intelligence Gathering

Our specialists will gather and analyze internet data on the organization and objectives, creating a risk analysis of the target. Data includes information for phishing attacks, leaked credentials, or vulnerable systems.

Attack Scenarios

We design realistic scenarios demonstrating how adversaries might exploit collected information to launch their attack. We select the most pertinent threats and specific scenarios to execute, ensuring an effective assessment.

Physical Penetration Test

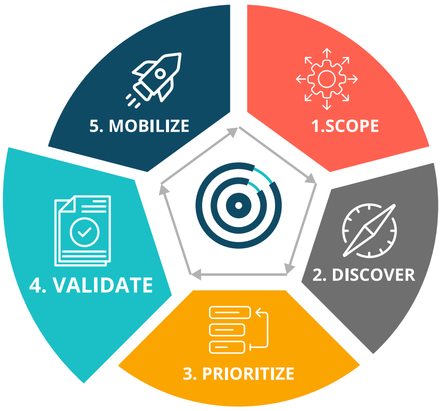
Even when cyber-elements are secured adversaries can still gain physical entry onto your premises and establish a foothold into your networks. Our team of experts will conduct a controlled red team exercise to eliminate risk of attackers looking to gain access into your offices.

Media Baiting and Phishing

Custom-printed USB drives, phishing campaigns and other media containing controlled malware to identify the level of security awareness within your organization and eliminate risk of targeted attacks on your workforce.

Network Exploitation

Internal and external network assessments to identify vulnerabilities and measure detective and responsive actions. This provides actionable insights into the effectiveness of your security measures and processes.



Embarking on or Re-energizing a CTEM program?

This solution helps with the Validation step of a Continuous Threat Exposure Management program.

By 2026, organizations that prioritize investments based on a CTEM program will be 3x less likely to suffer a breach (Gartner).

CONTACT US

About Outpost24

Outpost24 helps organizations improve cyber resilience with a complete range of exposure management solutions. Outpost24's intelligent cloud platform unifies asset management, automates vulnerability assessment, and quantifies cyber risk in business context. Executives and security teams around the world trust Outpost24 to identify and prioritize the most important security issues across their attack surface to accelerate risk reduction. Founded in 2001, Outpost24 is headquartered in Sweden and the US, with additional offices in the UK, Netherlands, Belgium, Denmark, France, and Spain. Visit https://outpost24.com/ for more information.