

PENETRATION TESTING SERVICES

Test components of your environment
against the latest attack techniques

TESTING FOR SOPHISTICATED ATTACKS CAN BE DAUNTING

Testing the different components of your IT environment is a continuous and often daunting task that can include applications, networks, firewalls, wireless, mobile, insider threats — the list goes on. Yet, understanding the latest attack techniques — and testing and assessing your defenses against those types of attacks — is critical to improving your cybersecurity posture.

Identifying vulnerabilities requires more than simply running a scan of your IT environment to stop today's sophisticated attacks. It is one thing to identify that a vulnerability exists, but it is something completely different to be able to exploit that vulnerability and see how far you can penetrate into the network and systems.

MIMIC ADVANCED ATTACKS TO TEST YOUR DEFENSES

To truly protect your environment, you need to know which adversaries are more likely to target your organization so you can mimic their advanced tactics to better test your defenses.

CrowdStrike® Penetration Testing Services simulate real-world attacks on different components of your IT environment to test the detection and response capabilities of your people, processes and technology in order to identify where vulnerabilities exist in your environment.

KEY BENEFITS

Identify and mitigate vulnerabilities throughout components of your IT environment, reducing the attack surface for today's advanced threats

Gain an objective perspective, exposing blind spots and gaining visibility into security gaps that could be missed by your internal IT teams due to lack of expertise or unfamiliarity with the latest threats

Test the investments you have made in your cybersecurity tools and technology to determine if any vulnerabilities or gaps exist and whether they can stop a sophisticated attack on your organization

Prioritize your security budgets where they are needed most, saving money over the long term by preventing wasteful expenditures on issues related to the broader security landscape

KEY CAPABILITIES

CrowdStrike delivers penetration testing services to test components of your IT environment against today's sophisticated attack techniques and tactics.

There are several types of penetration tests that are designed to meet the specific goals and threat profile of an organization. Below are some of the most common types of penetration tests delivered by CrowdStrike Services:

- **Internal Pen Testing** assesses your organization's internal systems to determine how an attacker could move laterally throughout your network. The test includes system identification, enumeration, vulnerability discovery, exploitation, privilege escalation, lateral movement and objectives.
- **External Pen Testing** assesses your internet-facing systems to determine if there are exploitable vulnerabilities that expose data or allow unauthorized access to the outside world. The test includes system identification, enumeration, vulnerability discovery and exploitation.
- **Web/Mobile Application Pen Testing** evaluates your web/mobile application using a three-phase process. First is reconnaissance, where the Services team discovers information such as the operating system, services and resources in use. Second is the discovery phase, where the team attempts to identify vulnerabilities. Third is the exploitation phase, where the team leverages the discovered vulnerabilities to gain unauthorized access to sensitive data.
- **Wireless Pen Testing** identifies the risks and vulnerabilities associated with your wireless network. The team assesses weaknesses such as deauthentication attacks, misconfigurations, session reuse and unauthorized wireless devices.
- **Insider Threat Pen Testing** identifies the risks and vulnerabilities that can expose your sensitive internal resources and assets to those without authorization. The team assesses areas of escalation and bypass to identify vulnerabilities and configuration weaknesses in permissions, services and network configurations.

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging the cloud-delivered CrowdStrike Falcon® platform — including next-generation endpoint protection, cyber threat intelligence gathering and reporting operations, and a 24/7 proactive threat hunting team — the CrowdStrike Services team helps customers identify, track and block attackers in real time. This unique approach allows CrowdStrike to stop unauthorized access faster and prevent further breaches. CrowdStrike also offers proactive services so organizations can improve their ability to anticipate threats, prepare their networks, and ultimately stop breaches.

Learn more at www.crowdstrike.com/services/

WHY CHOOSE CROWDSTRIKE SERVICES?

Real-world expertise:

The CrowdStrike team has unrivaled expertise and skills drawn from their experiences in incident response, forensics and red team engagements to create attacks using real-world threat actor tools that expose vulnerabilities within your environment.

Advanced threat

intelligence: CrowdStrike uses the most advanced threat intel to understand the tactics, techniques and procedures (TTPs) that adversaries will use to penetrate your environment and disrupt your business operations.

Going beyond vulnerability

scanning: CrowdStrike engagements deliver more than just a simple vulnerability scan. These tests are designed to penetrate deep into your networks, exploit your vulnerabilities, and identify where security gaps exist and how to close them.

