CROWDSTRIKE

RED TEAM SERVICES

CrowdStrike Services helps you stop the breach before it starts

RED TEAM SERVICES OVERVIEW

TEST YOUR CYBERSECURITY CAPABILITIES AGAINST ACTUAL TOOLS, TACTICS, AND PROCEDURES USED BY ADVERSARIES TARGETING YOUR INDUSTRY

CrowdStrike's Red Team offers a full suite of services and incident simulations to test your ability to defend and respond to targeted attacks. From gauging readiness to withstand an attack by the most advanced adversaries to working side-by-side with your response team to detect and react to a simulated attack, the CrowdStrike Red Team is dedicated to helping your organization to improve its security posture.

Integrated Intelligence

Crowdstrike Threat Intelligence plays a critical role in all Red Team services, from uncovering adversary motives and tactics, to predicting likely attacks.

Customized Offerings

One size does not fit all. Red Team services are tailored to meet your organization's needs, providing the best protection for your most valuable assets.

Actionable Results

Red Team services give you a better understanding of gaps in your organization's security, and provide comprehensive strategies for improvement.

THE CROWDSTRIKE DIFFERENCE

CrowdStrike's Red Team includes the most experienced testers in the security consulting business, with an average of **more than 10 years** of incident response, penetration testing, and related security activities. This expertise is reflected in a **95 percent success rate** for achieving predetermined objectives during Red Team engagements.

CrowdStrike's unique blend of best-in-class services, technology, and intelligence allows its Red Team to strategically target the areas and attack vectors most relevant to your organization, based on actual intelligence and our real-world incident response experience. Rather than relying on cookie-cutter Tactics, Techniques, and Procedures, CrowdStrike employs intelligence from the latest attacks its incident responders encounter in the field and those identified by the company's in-house threat intelligence team.

Commodity solutions are no longer sufficient. Fully patched systems and perimeter defense are essential, but they aren't enough to keep today's sophisticated adversaries at bay. CrowdStrike's Red Team helps you uncover the unseen gaps in your security posture that can allow an adversary to compromise your data, diminish your brand and impact your bottom line.

ADVERSARY EMULATION AND RED TEAM/ BLUE TEAM EXERCISE

Targeted attacks are taking a toll on organizations across every industry. Companies need to be prepared to identify, respond, and mitigate a targeted attack with speed and efficiency. CrowdStrike's Red Team service offerings bring an attacker's perspective to testing your security posture that goes far beyond simple vulnerability scans. Below are the Red Team's two primary offerings, along with supplemental offerings that complement the full Red Team suite of services.

ADVERSARY EMULATION

Adversary Emulation helps organizations gauge their readiness to withstand an attack from the most advanced adversaries. During this test, our experienced consultants mimic current attacker techniques in an attempt to gain access to your network and specific target assets.

ADVERSARY EMULATION TESTING HELPS YOU ANSWER THREE KEY QUESTIONS:

- How would a targeted attack on your environment manifest?
- What could a targeted attacker do with access to your environment?
- How effective is your current security posture at preventing, detecting, and responding to a targeted attack?

RED TEAM / BLUE TEAM EXERCISES

This exercise combines Adversary Emulation with hands-on training for your response team in tracking and responding to the attack as it unfolds.

DURING THIS EXERCISE, CROWDSTRIKE DEPLOYS TWO TEAMS OF CONSULTANTS:

- **Red Team:** Uses real-world attacker techniques to compromise your environment, giving you the experience of a real targeted attack, without the damage.
- **Blue Team:** CrowdStrike's veteran incident responders work with your security personnel and use your existing tools to identify, assess, and respond to the simulated intrusion.

PENETRATION TESTING SERVICES

In addition to Adversary Emulation and Red Team / Blue Team offerings, you can choose from a variety of testing options to meet your specific security objectives:

- **Insider Threat Penetration Testing**
- **Wireless Penetration Testing**
- **Social Engineering Assessment**
- **Web Application Penetration Testing**
- **Web Application Threat Modeling**
- **External Network Penetration Testing**
- **Mobile Device Penetration Testing**
- **Security Assessment**
- **Physical Security Testing**

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. With a complete portfolio of security consulting offerings that help organizations prepare to stop the next breach, CrowdStrike's comprehensive approach to security blends human expertise, real-time incident response technology and threat intelligence to help organizations stay ahead of would-be attackers and ensure that no threat goes undetected. Should attackers already be present in your environment, the CrowdStrike Services incident response team quickly identifies and eliminates adversaries, while the CrowdStrike Falcon platform ensures they stay out.

LEARN HOW CROWDSTRIKE STOPS BREACHES

Speak to a representative to learn how CrowdStrike Services can help your organization reduce costs associated with cyber incidents.

Phone: 1.888.512.8906
Email: sales@crowdstrike.com
Web: http://www.crowdstrike.com/services

Ver: 03-14-17