CROWDSTRIKE

ADVERSARY EMULATION EXERCISE

Prepare your organization for real-world targeted attacks

TODAY'S SOPHISTICATED ATTACKS CAN GO UNDETECTED

Adversaries are constantly evolving their attack tactics, techniques and procedures (TTPs), which can lead to breaches going undetected for weeks or months. At the same time, organizations are failing to detect sophisticated attacks because of ineffective security controls and gaps in their cybersecurity defenses.

Security teams need to make sure they are ready for a targeted attack, and the ability to withstand one type of attack does not mean the team has the tools and visibility to withstand a more sophisticated attack.

ARE YOU PREPARED FOR A TARGETED ATTACK ON YOUR ORGANIZATION?

The CrowdStrike® Adversary Emulation Exercise is designed to give your organization the experience of a sophisticated targeted attack by real-world threat actors — without the damage or costs of experiencing a real breach.

The CrowdStrike Services team leverages real-world threat actor TTPs derived from intelligence collected by CrowdStrike experts in the field responding to incidents and through the CrowdStrike Falcon® platform, which identifies trillions of events and millions of indicators every week.

CrowdStrike Services develops a targeted attack campaign specific to your organization and aimed at users of interest, just as an adversary would. The team takes an objective, goal-oriented approach to the attack, focusing on demonstrating access to critical information in your organization to help show the impact of a breach to your leadership without having to suffer through a real breach. This exercise will help you answer the question, **"Are we prepared for a targeted attack?"**

KEY BENEFITS

Test your security team's ability to respond to a targeted attack without the occurrence of a real incident

Test your security team against the latest attacker TTPs that pose the most risk to your industry

Focus on objective-based testing to demonstrate the effectiveness of your security controls and incident response processes

Evaluate your organization's maturity level across each phase of the MITRE ATT&CK® framework

ADVERSARY EMULATION EXERCISE

KEY SERVICE FEATURES

THE GOAL

The Services team's goal is to give your organization the experience of a sophisticated targeted attack without the actual damage that accompanies a real incident. After the Red Team achieves its objective, it shows you how it reached its goals and identifies tactics that can help you prevent future attacks.

To make this exercise as realistic as possible, the Services team constantly updates its approach to mirror the current threat landscape, leveraging CrowdStrike's Intelligence team to keep pace with changes in different adversary groups' tactics for targeting similar organizations. The team also leverages new attacker techniques that CrowdStrike's incident responders observe in the field. The result is a test of your defenses that replicates real-world attacks — often relying on the same tools the attackers themselves use.

THE APPROACH

The process begins by understanding your objectives. Whether the goals involve testing tools and visibility, security response, controls around specific assets, defenses against a specific attacker, or some combination of those, CrowdStrike's Red Team uses these requirements to tailor an exercise that specifically meets your organization's needs.

CrowdStrike's Adversary Emulation Exercise utilizes the MITRE ATT&CK framework as the basis of its methodology. The ATT&CK framework details a step-by-step approach that advanced persistent threat (APT) groups leverage during an attack.

The ATT&CK framework is divided into 11 categories that cover various tactics based on the mapped tactic category. In order to simplify the ATT&CK framework's tactic and technique mapping, CrowdStrike has grouped various TTPs into four phases.

CrowdStrike Phase	MITRE ATT&CK Framework Tactics
Gain Initial Access	Initial Access, Execution, Defense Evasion, Command and Control
Establish Foothold	Persistence, Discovery
Obtain Privileges	Privilege Escalation, Credential Access, Lateral Movement
Follow Through	Collection, Exfiltration

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services delivers Incident Response, Technical Assessments, Training, and Advisory Services that help you prepare to defend against advanced threats, respond to widespread attacks, and enhance your cybersecurity practices and controls.

We help our customers assess and enhance their cybersecurity posture, test their defenses against real-world attacks, respond to incidents, accelerate forensic investigations, and recover from a breach with speed and precision. Harnessing the power of our Security Cloud and the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike: **We stop breaches.**

Learn more at **www.crowdstrike.com/services/**
Email: **services@crowdstrike.com**

WHY CHOOSE CROWDSTRIKE?

Deep expertise:
CrowdStrike Services Red Teams have extensive adversary emulation and penetration testing experience, giving you real-world attack scenarios that highlight weaknesses in your defenses.

Threat intelligence:
The Services team leverages the CrowdStrike Falcon® platform and incident response investigations to create adversary attack emulations that employ the latest TTPs currently being used against clients in your industry.

The right approach:
CrowdStrike's Red Teams focus on objective-based testing to demonstrate the business impact of a lack of security controls, going beyond simply elevating privileges and showing what an attacker could do with that level of access.