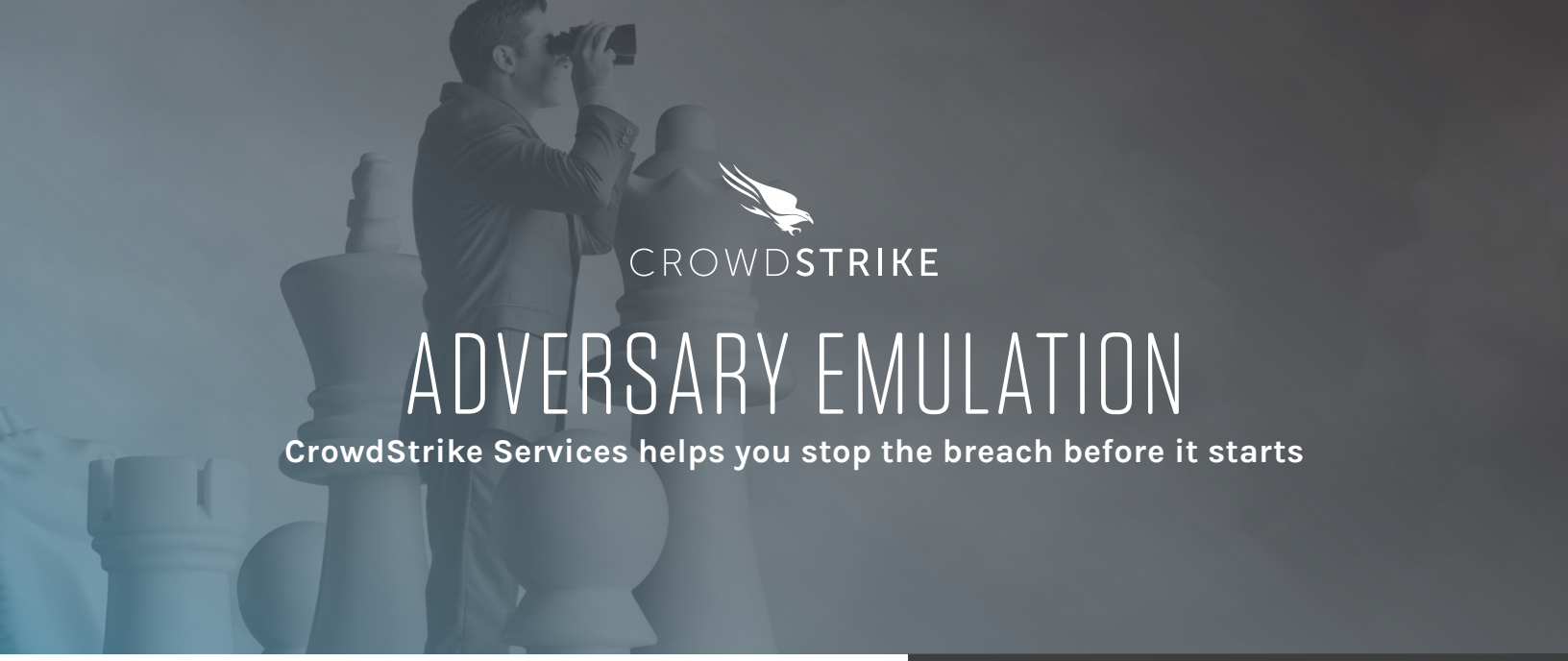

CROWDSTRIKE

ADVERSARY EMULATION

CrowdStrike Services helps you stop the breach before it starts

ADVERSARY EMULATION

CrowdStrike's premier Red Team service offering 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 an organization's network and compromise specific assets.

ADVERSARY EMULATION 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?

Our goal is to give your organization the experience of a sophisticated targeted attack, without the actual damage that accompanies a real incident. After we achieve our objective, we show you how we reached our goals and identify tactics that can help you prevent future attacks.

To make our tests as realistic as possible, we constantly update our approach to mirror the current threat landscape. We leverage CrowdStrike's Falcon Intelligence team to keep pace with changes in different adversary groups' tactics used to target similar organizations. We also leverage new attacker techniques CrowdStrike's incident responders observed in the field. The result is a test of your defenses that replicates real-world tactics, techniques, and procedures--often relying on the same tools the attackers use themselves.

HOW WE DO IT

ADVERSARY EMULATION

CrowdStrike's Red Team / Blue Team exercises begin with a review of the threat landscape your organization faces. We leverage CrowdStrike's Falcon Intelligence to understand which adversaries are likely to target your organization and the assets they would pursue. We combine this background with an understanding of your objectives for the exercise, incorporating any specific assets, tools, or processes that should be highlighted.

Once this review is complete, we select an adversary to emulate. Drawing upon our intelligence resources and what our incident responders see in the field, we identify that adversary's current tactics, techniques, and procedures (TTPs). We even acquire the adversary's tools (when non-malicious) or develop tools that closely mimic what the adversary uses. The result is an exercise that closely mirrors how an actual attack would manifest.

FOLLOWING THE KILL CHAIN

Our Red Team takes a methodical approach to emulating a realistic attack on your organization, using the kill chain to delineate each phase of the attack, starting with active reconnaissance and continuing through exploitation, command and control, and operations. But unlike an actual attack, the Red Team notifies the Blue Team before each phase begins. This allows your incident responders to use the actual tools in your environment to track and attempt to disrupt attacker activity. After each phase concludes, we review both teams' actions, identifying what responders did well, what could be improved, and whether any gaps exist.

OUR APPROACH

Our process begins by understanding our client's 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, our Red Team uses these requirements to tailor a test that specifically meets your organization's needs.

CrowdStrike's Adversary Emulation follows a kill chain methodology for conceiving of and executing each phase of an advanced attack, as follows:

1. **Reconnaissance:** The Red Team uses passive and active reconnaissance techniques to collect information about the target organization and its employees. This includes collecting information from social media and other open sources, as well as using scanning tools to survey the target network.
2. **Deliver:** The Red Team transmits the payload to a target, typically via spear phishing or removable media device.
3. **Exploit:** The recipient triggers the payload, which attempts to exploit operating system or application vulnerabilities on the target network. CrowdStrike's Red Team leverages exploits its own exploits to closely match the tools used by specific adversaries.
4. **Install:** The Red Team establishes persistent access by installing a remote access tool or backdoor.
5. **Command and Control:** The infected host beacons out to the Red Team's custom-built command and control infrastructure, establishing an encrypted communication channel and allowing the Red Team to interact directly with the target network.
6. **Privilege Escalation:** During this phase, the team enumerates the local system, looking for opportunities to extract credentials and elevate privileges to gain additional access.
7. **Lateral Movement:** Once the Red Team has compromised a system, they will try to move on to a bigger target on your internal network.
8. **Operations:** The Red Team attempts to achieve the objectives agreed upon in the preliminary conversation with the customer. If the scope permits, the Red Team may also identify other targets of opportunity that exist once persistent access has been established.

ACTIONABLE GUIDANCE AND DELIVERABLES

Once the test concludes, CrowdStrike provides:

- Documented proof of how a targeted attacker could penetrate your network and compromise sensitive assets, and/or documentation showing what defensive capabilities succeeded in preventing the simulated attack.
- An evaluation of your organization's strengths and weaknesses against the simulated attack. This is useful for prioritizing your tactical and strategic security investments.
- Opportunities to discuss your organization's detection and response activities in the context of a simulated attack.

CROWDSTRIKE'S WRITTEN DELIVERABLES MAY INCLUDE:

- A summary of the attack and results of that activity
- A summary of your identification and response to attack, if any
- Observations and findings from the test
- A summary recommendation section based on the actions we took, weaknesses we exploited, and subsequent discussions we conducted with your team

LEARN HOW CROWDSTRIKE STOPS BREACHES

VISIT WWW.CROWDSTRIKE.COM/SERVICES

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

LET'S DISCUSS YOUR NEEDS

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