CROWDSTRIKE

RED TEAM / BLUE TEAM EXERCISE

Prepare your cybersecurity team to defend against targeted attacks

CYBERATTACKS ARE CONSTANTLY EVOLVING

Attack tactics, techniques and procedures (TTPs) are constantly evolving, and every organization should know how to identify, stop and prevent a breach. Many organizations have a complex suite of security tools they count on for protection. The challenge is understanding whether these tools and the associated policies and procedures implemented in them are efficient and capable of preventing a modern-day attack.

TRAIN TO DEFEND AGAINST A TARGETED ATTACK

The CrowdStrike® Red Team / Blue Team Exercise helps prepare your cybersecurity team by learning from experts, as a Red Team attacks your systems in a simulated exercise and a Blue Team helps your team defend against this targeted attack within your environment.

During this exercise, CrowdStrike deploys two teams of consultants: a Red Team that uses real-world attacker techniques to compromise your environment, and a Blue Team of incident responders who work side-by-side with your security personnel using your existing tools to identify, assess and respond to malicious activity.

KEY BENEFITS

Discover and identify misconfigurations and coverage gaps in existing security products

Focus on maturing your security team's threat hunting knowledge and overall incident response processes in a safe training environment

Enable your security staff to walk through the phases of a targeted attack and understand the mindset and methodology of a real-world threat actor and how to detect its activity within your environment

RED TEAM / BLUE TEAM EXERCISE

KEY SERVICE FEATURES

A typical exercise traces the following kill chain path:

ACTIVE RECONNAISSANCE

While the Red Team scans your public-facing infrastructure and looks for vulnerabilities, the Blue Team helps your personnel detect adversary reconnaissance and consider preventive measures that can be taken in response.

DELIVERY AND EXPLOITATION

The Red Team attempts to compromise your public-facing infrastructure using available application or system vulnerabilities, relying on tactics and software used by real-world adversaries. If the Red Team cannot gain access using the designed intrusion method, or you would prefer to not exploit live infrastructure, then a trusted agent will manually execute the tactic so that artifacts are present for investigation. The Blue Team works with your security personnel to triage the incident, conducting host and network-based analysis and identifying the source and destination of the attack, exploitation method, rogue processes, and level of privileged access.

COMMAND AND CONTROL

As the Red Team's tools beacon out to the attack infrastructure, the Blue Team helps your security personnel identify this traffic and search for other potential points of compromise to gain a more comprehensive picture of the attacker's access.

OPERATIONS

The Red Team escalates privileges, enumerates vulnerabilities, expands access and simulates data exfiltration in your environment. Meanwhile, the Blue Team works with your personnel to track these actions and assess the attacker's objectives — one of the most difficult analytic parts of incident response. By identifying the systems, data and methods the attacker used to infiltrate your environment, the response team can better understand the organizational risk posed by the incident, anticipate future attacker activity, and develop containment and remediation strategies.

AFTER-ACTION REVIEW

Once the attack phases are completed, the Blue Team continues to work with your security team, conducting host and network-based analysis and piecing together a timeline and narrative of the events that transpired. Once this is complete, the Red Team provides every detail of the attack to ensure a complete understanding of the campaign. CrowdStrike consultants also facilitate a review of response activities and record any lessons learned and recommendations for improvement.

WHY CHOOSE CROWDSTRIKE?

Real-world targeted attack scenarios: CrowdStrike's Red Teams have extensive penetration testing experience and in-depth understanding of the TTPs used in today's sophisticated attacks.

Cyber kill chain process: CrowdStrike's Red Teams incorporate the same tools and techniques that adversaries use to mirror a targeted attack that follows the steps of the cyber kill chain.

Advanced threat intelligence: CrowdStrike's Blue Teams provide insight into adversarial TTPs that specifically target your industry. The exercise helps you better understand potential threats and how to protect yourself against a targeted attack.

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**