CROWDSTRIKE

RED / BLUE TEAM EXERCISE

CrowdStrike Services helps you stop the breach before it starts

RED TEAM / BLUE TEAM EXERCISE

CrowdStrike's Red Team / Blue Team exercise combines the simulated attack from our Adversary Emulation offering with hands-on training for your response team, who track and respond to the attack as it unfolds. 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 sit with your security personnel and use your existing tools to identify, assess and respond to the intrusion.

Our experts slow down the attacker lifecycle and guide your team through an adversary campaign with an eye toward facilitating operational growth, investigative experience, and program maturity. By the end of the exercise, we will have:

- Identified vulnerabilities as part of the offensive attack activities
- Determined areas for improvement in the defensive incident response processes across every phase of the kill chain
- Identified opportunities to improve prevention and detection capabilities
- Documented response and remediation activities to return your environment to a secure status
- Provided your response team with first-hand experience and training on how to handle a targeted attack

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 cyber 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 that should be highlighted.

A TYPICAL EXERCISE TRACES THE FOLLOWING 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 we 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 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 its 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, our 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. Our consultants also facilitate a review of response activities and record any lessons learned and recommendations for improvement.

DELIVERABLES

Following the conclusion of the exercise, written deliverables provided include:

- **Summary of the vulnerabilities exploited during the simulation**
- **Summary of the tactics, techniques, and procedures used during the simulation**
- **Observations and recommendations from the hands-on incident response training conducted during simulation pauses**
- **Recommendations on process, methodology, and technology deficiencies observed by our team during the entire simulation**

ABOUT OUR TEAMS

CrowdStrike's Red Team consists of some of the most experienced testers in the business. Our Red Team members average 10+ years of experience across incident response, penetration testing, and red team activities.

CrowdStrike's Blue Team is comprised of our world-class incident response consultants. With backgrounds in military, intelligence, law enforcement, and the private sector, our consultants have responded to some of the largest and most consequential cybersecurity incidents in history.

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

Ver: 03-14-17