CROWDSTRIKE

RED/BLUE TEAM EXERCISE

TO DEFEND AGAINST AN ATTACK SUCCESSFULLY, YOU MUST PREPARE.

CrowdStrike Red Team
provides hands-on training of your response team, showing them real-world attacker techniques that can compromise your environment.

CrowdStrike Blue Team
incident responders will train your security personnel using your existing tools to identify, assess and respond to a simulated intrusion.

OUTCOMES

By the end of the exercise your team will be able to:

- IDENTIFY VULNERABILITIES DURING OFFENSIVE ATTACK ACTIVITIES
- DETERMINE AREAS FOR IMPROVEMENT IN DEFENSIVE INCIDENT RESPONSE PROCESSES ACROSS EVERY PHASE OF THE KILL CHAIN
- LEARN FROM FIRST-HAND EXPERIENCE AND TRAINING HOW TO HANDLE A TARGETED ATTACK
- DOCUMENT RESPONSE AND REMEDIATION ACTIVITIES TO RETURN YOUR ENVIRONMENT TO A SECURE STATUS
- IDENTIFY OPPORTUNITIES TO IMPROVE PREVENTION AND DETECTION CAPABILITIES

AN EXERCISE TRACES THE FOLLOWING PATH:

1 DELIVERY AND EXPLOITATION

THE RED TEAM WILL ATTEMPT TO COMPROMISE YOUR NETWORK USING THE SAME TACTICS AND SOFTWARE USED BY REAL-WORLD ADVERSARIE. THE BLUE TEAM, ALONGSIDE YOUR SECURITY PERSONNEL, CONDUCTS HOST- AND NETWORK-BASED ANALYSIS TO IDENTIFY THE SOURCE AND DESTINATION OF THE ATTACK.

2 COMMAND AND CONTROL

THE RED TEAM BEACONS 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.

3 OPERATIONS

THE RED TEAM ESCALATES PRIVILEGES, ENUMERATES VULNERABILITIES, EXPANDS ACCESS, AND SIMULATES DATA EXFILTRATION IN YOUR ENVIRONMENT. THE BLUE TEAM WORKS WITH YOUR PERSONNEL TO TRACK THESE ACTIONS, ASSESS THE ATTACKER'S OBJECTIVES, UNDERSTAND THE ORGANIZATIONAL RISK POSED BY THE INCIDENT, ANTICIPATE FUTURE ATTACKER ACTIVITY, AND DEVELOP CONTAINMENT AND REMEDIATION STRATEGIES.

4 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 COMPLETE, THE RED TEAM PROVIDES EVERY DETAIL OF THE ATTACK TO ENSURE A COMPLETE UNDERSTANDING OF THE CAMPAIGN. CROWDSTRIKE SERVICES CONSULTANTS ALSO FACILITATE A REVIEW OF RESPONSE ACTIVITIES AND RECORD ANY LESSONS LEARNED AND RECOMMENDATIONS FOR IMPROVEMENT.

WHY CROWDSTRIKE SERVICES?

GAIN COMPLETE VISIBILITY

WITH THE FALCON PLATFORM, THE CROWDSTRIKE SERVICES TEAM CAN QUICKLY SHOW YOUR STAFF HOW TO GAIN FULL INSIGHT INTO A INCIDENT, LOCKING DOWN CREDENTIALS, AND LIMITING ACCESS.

RECOVER FASTER AND GET BACK TO BUSINESS QUICKLY

CROWDSTRIKE SERVICES WILL SHOW YOUR TEAM HOW TO STOP AND EJECT AN ATTACKER SO WHEN A REAL RESPONSE IS NEEDED YOUR ORGANIZATION CAN RESUME BUSINESS FASTER.

LEVERAGE RELEVANT THREAT INTELLIGENCE

YOU'LL LEARN TO IDENTIFY AND UNDERSTAND THE ADVERSARIES WHO ARE MOST LIKELY TO TARGET YOUR ORGANIZATION AND YOUR INDUSTRY.

RED TEAM

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

BLUE TEAM

The CrowdStrike Blue Team is comprised of world-class incident response consultants, with extensive backgrounds in military, intelligence, law enforcement and private sectors. CrowdStrike consultants have responded to some of the largest and most consequential cybersecurity incidents in history.

LEARN HOW CROWDSTRIKE SERVICES STOPS BREACHES:

VISIT WWW.CROWDSTRIKE.COM/SERVICES

1.888.512.8906 | sales@crowdstrike.com