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.

IDENTIFY VULNERABILITIES DURING OFFENSIVE ATTACK ACTIVITIES

OUTCOMES By the end of the

exercise your team will be able to:

DETERMINE AREAS FOR IMPROVEMENT IN DEFENSIVE INCIDENT RESPONSE PROCESSES ACROSS EVERY PHASE OF THE KILL **CHAIN**

RESPONSE AND REMEDIATION ACTIVITIES TO RETURN YOUR ENVIRONMENT **TO A SECURE STATUS**

DOCUMENT

FIRST-HAND EXPERIENCE AND TRAINING HOW TO **HANDLE A TARGETED ATTACK**

LEARN FROM

OPPORTUNITIES TO IMPROVE PREVENTION AND DETECTION CAPABILITIES

IDENTIFY

AN EXERCISE TRACES THE FOLLOWING PATH:

THE RED TEAM WILL ATTEMPT TO COMPROMISE THE BLUE TEAM, ALONGSIDE YOUR SECURITY YOUR NETWORK USING THE SAME TACTICS PERSONNEL, CONDUCTS HOST- AND AND SOFTWARE USED BY NETWORK-BASED ANALYSIS TO IDENTIFY THE

DELIVERY AND EXPLOITATION

REAL-WORLD ADVERSARIE. SOURCE AND DESTINATION OF THE ATTACK. COMMAND AND CONTROL

DEVELOP CONTAINMENT AND REMEDIATION STRATEGIES.



BEACONS OUT TO IDENTIFY THIS TRAFFIC AND SEARCH FOR OTHER ITS ATTACK POTENTIAL POINTS OF COMPROMISE TO GAIN A MORE INFRASTRUCTURE. COMPREHENSIVE PICTURE OF THE ATTACKER'S ACCESS.

OPERATIONS

TEAM CONTINUES TO WORK WITH YOUR SECURITY THE ATTACK TO ENSURE A COMPLETE UNDERSTANDING OF

TEAM, CONDUCTING HOST AND NETWORK-BASED THE CAMPAIGN, CROWDSTRIKE SERVICES CONSULTANTS ALSO



AFTER-ACTION REVIEW ONCE THE ATTACK PHASES ARE COMPLETED, THE BLUE ONCE COMPLETE, THE RED TEAM PROVIDES EVERY DETAIL OF

THE RED TEAM ESCALATES PRIVILEGES, THE BLUE TEAM WORKS WITH YOUR PERSONNEL TO TRACK

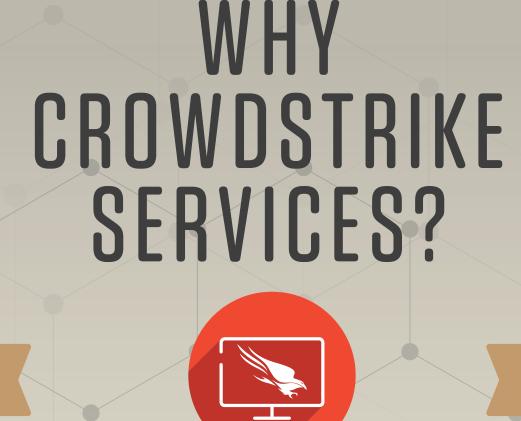
EXFILTRATION IN YOUR ENVIRONMENT. INCIDENT, ANTICIPATE FUTURE ATTACKER ACTIVITY, AND

ACCESS, AND SIMULATES DATA UNDERSTAND THE ORGANIZATIONAL RISK POSED BY THE

ENUMERATES VULNERABILITIES, EXPANDS THESE ACTIONS, ASSESS THE ATTACKER'S OBJECTIVES,

FACILITATE A REVIEW OF RESPONSE ACTIVITIES AND RECORD ANY

LESSONS LEARNED AND RECOMMENDATIONS FOR IMPROVEMENT.



THE CROWDSTRIKE SERVICES TEAM CAN QUICKLY SHOW YOUR STAFF HOW TO GAIN FULL

INSIGHT INTO A INCIDENT,

GAIN COMPLETE

VISIBILITY

WITH THE FALCON PLATFORM,

LOCKING DOWN CREDENTIALS, AND LIMITING ACCESS.

RECOVER FASTER AND GET **BACK TO BUSINESS QUICKLY** CROWDSTRIKE SERVICES WILL SHOW YOUR TEAM HOW TO STOP

NEEDED YOUR ORGANIZATION CAN RESUME BUSINESS FASTER.

AND EJECT AN ATTACKER SO WHEN A REAL RESPONSE IS



ADVERSARIES WHO ARE MOST

LIKELY TO TARGET YOUR

ORGANIZATION AND YOUR

INDUSTRY.

The CrowdStrike Red Team consists of some of the most experienced

testers in the business. Team

experience across incident

red team activities.

members average 10-plus years of

response, penetration testing and

RED TEAM

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