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.

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.

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 adversaries.
   - 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. 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.

WHY CROWDSTRIKE SERVICES?

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.

IDENFITY VULNERABILITIES DURING OFFENSIVE ATTACK ACTIVITIES

OUTCOMES

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

- Document designs and responses to attacks to return your environment to a secure status.
- Identify opportunities to improve prevention and detection capabilities.
- Learn from first-hand experience and training how to handle a targeted attack.
- Determine improvement in defensive incident response processes across every phase of the kill chain.
- Identify opportunities to improve prevention and detection capabilities.
- Document response and remediation activities to return your environment to a secure status.
- Identify vulnerabilities during offensive attack activities.