CROWDSTRIKE

CROWDSTRIKE INCIDENT RESPONSE AND PROACTIVE SERVICES

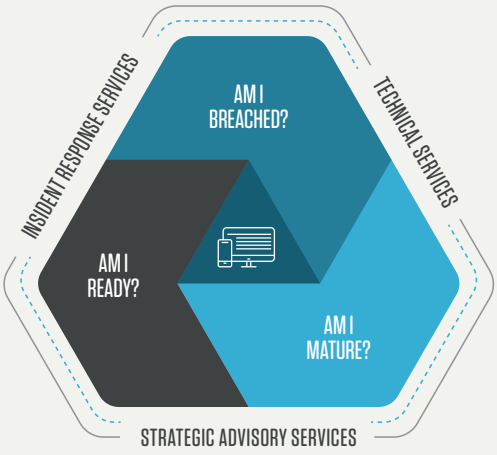
Train for, react to and remediate a breach quickly and effectively

CHOOSE THE SERVICES THAT FIT YOUR REQUIREMENTS

CrowdStrike® Services includes both incident response (IR) and proactive offerings that play a crucial role in helping your organization mature your security posture and stop a breach. These services are architected to enable organizations to react quickly and effectively to a cybersecurity incident. Customers also benefit from a range of proactive services designed to improve their overall cybersecurity readiness.

To perform this work, CrowdStrike Services brings together a team of security professionals from intelligence, law enforcement and industry; architects and engineers from the best technology companies around the globe; and security consultants who have spearheaded some of the world's most challenging intrusion investigations.

This team makes extensive use of the CrowdStrike Falcon® platform, delivering groundbreaking endpoint protection and enabling real-time incident response, detailed forensic analysis and threat intelligence to ensure no threat goes undetected. CrowdStrike Services excels at helping organizations plan for, respond to and prevent damage from a wide range of security incidents and advanced cyberattacks — and importantly, helps them defend against future attacks.



CrowdStrike IR and Proactive Services can be used individually or in combination with each other, and can be covered by a Services retainer. The retainer is flexible: If you find there is no need for CrowdStrike IR Services, you can use your available retainer hours to take advantage of Proactive Services, all of which are focused on helping to improve your overall security posture.

CROWDSTRIKE SERVICES AT A GLANCE

Crowdstrike Services offerings help organizations strengthen and mature their security postures by addressing three fundamental questions:

AM I BREACHED?

- Incident Response Services
- Endpoint Recovery Services
- Compromise Assessment
- Network Security Monitoring

AM I MATURE?

- Cybersecurity Maturity Assessment
- Active Directory Security Assessment
- Cloud Security Assessment
- Security Operations Center (SOC) Assessment
- IT Hygiene Assessment
- Cybersecurity Enhancement Program
- Security Program in Depth

AM I READY?

- Tabletop Exercise
- Live Fire Exercise
- Adversary Emulation Exercise
- Red Team / Blue Team Exercise
- Penetration Testing Services

MANAGED SERVICES, SUPPORT AND TRAINING

- Falcon Complete™
- Falcon Gold Standard
- Falcon Operational Support
- Falcon Training (CrowdStrike University)

CROWDSTRIKE INCIDENT RESPONSE AND PROACTIVE SERVICES

AM I BREACHED?

INCIDENT RESPONSE SERVICES

- Accelerate the speed of remediation when breaches occur with a comprehensive view of attacker activity to help you resume business operations faster. CrowdStrike IR Services works collaboratively with your organization to handle critical security incidents and conduct forensic analysis to resolve cyberattacks immediately and implement a long-term solution to stop recurrences.
- CrowdStrike's team of incident responders takes an intelligence-led approach to response work, blending real-world incident response, forensic investigation and remediation experience with cutting-edge technology by leveraging the unique, cloud-based Falcon platform — identifying attackers quickly and precisely, and ejecting them from the environment. The CrowdStrike team is laser-focused on getting organizations back to business faster and reducing the impact of a cyber incident.

ENDPOINT RECOVERY SERVICES

- CrowdStrike Endpoint Recovery Services helps you rapidly recover from advanced persistent threats and attacks with zero business interruption.
- This service combines CrowdStrike's industry-leading technology platform and threat intelligence with a team of highly experienced security experts to assist with the detection, analysis and remediation of known security incidents and enable rapid recovery.

COMPROMISE ASSESSMENT

- The CrowdStrike Compromise Assessment team identifies ongoing or past attacker activity in your environment to answer the critical question: "Has my organization been breached?"
- The Compromise Assessment team leverages years of experience in responding to intrusions by the most advanced attackers, combining the powerful Falcon platform, industry-leading cyber threat intelligence and 24/7 threat hunting to deliver the most comprehensive assessment of a compromise in your environment.

NETWORK SECURITY MONITORING

- This service delivers extensive network security monitoring to detect active threats present in your environment.
- It provides an extensive network security monitoring capability for detection, response and threat hunting. This service utilizes both the expertise of CrowdStrike Services threat hunters and a network appliance that detects threats present in your environment.

WHY CHOOSE CROWDSTRIKE?

Proven human expertise: Expert incident responders, malware researchers and cyber intelligence professionals provide fast incident response, forensic analysis, endpoint recovery and proactive services.

Adversary intelligence: You benefit from up-to-the-minute research and reporting on threat actors and their tactics, techniques and procedures targeting your environment.

Unrivaled threat hunting: Proactive, 24/7 hunting expands the search for adversary activity across your environment.

Superior technology: The unique CrowdStrike Falcon platform delivers next-generation endpoint protection to detect adversaries, eject them quickly and keep them out.

CROWDSTRIKE INCIDENT RESPONSE AND PROACTIVE SERVICES

AM I MATURE?

CYBERSECURITY MATURITY ASSESSMENT

- CrowdStrike Services asserts that being "compliant" doesn't mean you're secure. Rather than focusing solely on compliance, the Services team evaluates an organization's maturity level through an acute lens, tempered by years of experience in responding to threats.
- The team's methodology goes beyond a standard audit by assessing an organization's cybersecurity maturity in relation to its ability to prevent, detect and respond to the most advanced adversaries.

ACTIVE DIRECTORY SECURITY ASSESSMENT

- Receive a comprehensive review of your Active Directory (AD) configuration and policy settings to prevent exploitation of the AD infrastructure.
- CrowdStrike's Active Directory Security Assessment is uniquely designed to review AD configuration and policy settings in order to identify security configuration issues that attackers can exploit.
- The assessment involves review of documentation, discussions with your staff, execution of proprietary tools and a manual review of your AD configuration and settings. The output is a detailed report of the issues discovered and their impact, along with recommended steps for mitigation and remediation.

CLOUD SECURITY ASSESSMENT

- CrowdStrike's Cloud Security Assessment provides actionable insights into security misconfigurations and deviations from recommended cloud security architecture.
- With CrowdStrike's experience in incident response, and consultants with hands-on experience from recognized leaders in cloud security architecture, this assessment gives you the prioritized actions you need to maximize your capabilities to prevent, detect and recover from security incidents in the cloud.

IT HYGIENE ASSESSMENT

- Proactively discover vulnerabilities and safeguard your network before a breach occurs.
- CrowdStrike's IT Hygiene Assessment provides improved visibility into applications, accessibility and account management within your network, delivering comprehensive context around network traffic and security gaps. Identifying vulnerabilities and missing patches enables you to proactively safeguard your network before a breach occurs.

CYBERSECURITY ENHANCEMENT PROGRAM

- Develop and implement a cybersecurity enhancement program after a breach has occurred to close security gaps and prevent further breaches.
- CrowdStrike's Cybersecurity Enhancement Program is for organizations that recently experienced a breach and require assistance in developing a strategic cybersecurity improvement plan to prevent another breach from occurring.

ADDITIONAL OFFERINGS

Security Operations Center (SOC) Assessment: Enhance the maturity level of your SOC, and identify and prioritize areas for improvement.

Security Program in Depth: Take a deep dive into your cybersecurity processes, tools and resources to determine the maturity of your information security program.

AM I READY?

TABLETOP EXERCISE

- The CrowdStrike Services team's advanced experience in conducting IR investigations against sophisticated cyber threats provides a real-world perspective on the tabletop exercise process.
- Exercises are designed to simulate a targeted attack and guide your organization — either executive or technical participants — through a realistic incident simulation. This exercise offers the experience of an attack without the attendant disruption and damage.

LIVE FIRE EXERCISE

- This exercise is designed to test individuals within the organization to ensure they understand their roles during an incident response scenario.
- Rather than discuss a hypothetical attack as a group, the Services team leverages your tools and processes to add to the realism, providing specific information to specific individuals — just as it would occur during an actual breach investigation. The team then leaves it up to you to determine how best to manage the information. At the conclusion of the engagement, you will clearly understand the weaknesses in your process.

ADVERSARY EMULATION EXERCISE

- This test provides the benefit of experiencing a sophisticated targeted attack without the actual damage of a real incident.
- This is accomplished by having an experienced CrowdStrike consultant mimic current attacker techniques in an attempt to gain access to your organization's network and compromise specific assets. After this objective is reached, the team explains how the goal was achieved and helps you identify tactics you can employ to help prevent future attacks.

RED TEAM / BLUE TEAM EXERCISE

- Prepare your cybersecurity team and learn from experts as one team attacks (red) and one team defends (blue) in your environment.
- CrowdStrike's Red Team/Blue Team Exercise focuses on maturing your security team's threat hunting knowledge and overall incident response processes through a real-world targeted attack scenario.

PENETRATION TESTING SERVICES

- The Services team uses ethical hacking to find security gaps by conducting authorized simulation attacks and penetration tests on different components of your systems, networks and applications.
- Choose from a variety of testing options to meet your specific security objectives.

MANAGED SERVICES, SUPPORT AND TRAINING

FALCON COMPLETE™: This comprehensive endpoint protection and threat hunting solution is delivered as a turnkey, fully managed service, leveraging the power of the Falcon platform.

FALCON GOLD STANDARD: Helps you deploy, configure and manage the Falcon platform and respond to alerts for the first 90 days of your journey with CrowdStrike.

FALCON OPERATIONAL SUPPORT: Helps you deploy and configure the Falcon platform to optimize your cybersecurity operations.

FALCON TRAINING: Professional training and education services from CrowdStrike University (CSU) enhance your cybersecurity team's knowledge and help you get the most out of your investment in the Falcon platform.

SERVICES RETAINER

IR AND PROACTIVE SERVICES

All of the CrowdStrike IR and Proactive Services are available under a CrowdStrike Services Retainer agreement. The Retainer allows you to rapidly engage the team when you need IR assistance and also provides a structure to plan and deliver the proactive services that best fit your organization's needs. This gives you IR services when you need them and also provides a thoughtful plan for enhancing your cybersecurity posture and testing your readiness over the course of a year.

Retainer	Tier 1	Tier 2	Tier 3	Tier 4
IR on Demand	Yes	Yes	Yes	Yes
Response Time (Remote)	8 Hours	6 Hours	4 Hours	2 Hours
Response Time (Onsite)	2 Days	2 Days	1 Day	1 Day
Hours of Work Included	110	160	240	480

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