CROWDSTRIKE

CROWDSTRIKE INCIDENT RESPONSE AND ADVISORY SERVICES

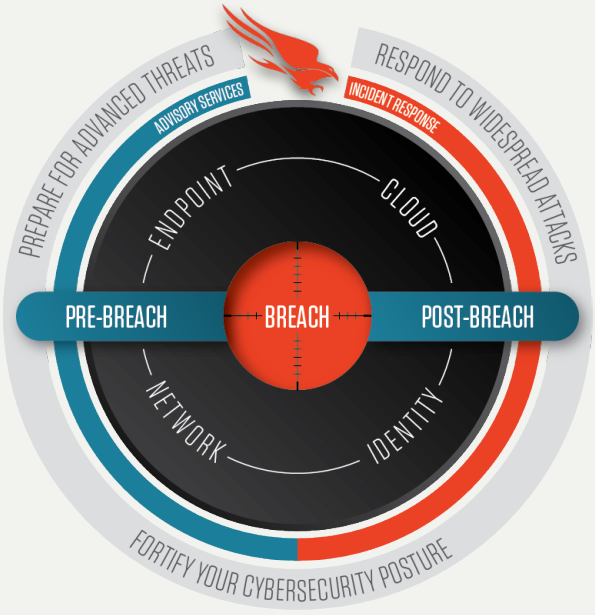
Train for, react to and remediate a breach quickly and effectively

CHOOSE THE SERVICES THAT FIT YOUR REQUIREMENTS

CrowdStrike Services includes both Incident Response (IR) and Advisory Services that play a crucial role in helping your organization mature its 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 advisory 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 Advisory 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 Advisory 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 posture:

RESPOND: Breach Services

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

PREPARE: Advisory Services

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

FORTIFY: Advisory Services

- Cybersecurity Maturity Assessment
- Technical Risk Assessment
- SOC Assessment
- AD Security Assessment
- Cybersecurity Enhancement Program
- Security Program in Depth

PLUS

- Cloud Security Services
- Identity Protection Services
- Managed Security Services
- Falcon Enablement Services
- CrowdStrike University (CSU)

Last updated: Sept. 26, 2022
22-GC-012

RESPOND: BREACH SERVICES

INCIDENT RESPONSE

- Accelerate 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 IR Services team 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 IR Services team is laser-focused on getting organizations back to business faster and reducing the impact of a cyber incident.

ENDPOINT RECOVERY

- CrowdStrike Endpoint Recovery Services helps you rapidly recover from advanced persistent threats and attacks with minimal 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 and 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

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

WHY CHOOSE CROWDSTRIKE?

DEEP HUMAN EXPERTISE
Customer Focus: CrowdStrike brings together the combined skills and expertise of its Incident Response, Threat Intelligence and Falcon OverWatch teams working together and focused on helping you stop breaches.

SUPERIOR TECHNOLOGY PLATFORM
Infinite Scale: As a recognized industry leader, CrowdStrike can deploy its CrowdStrike Security Cloud and Falcon technology platform with infinite scale to quickly identify threat actor tactics and help you recover from advanced attacks.

ADVANCED THREAT INTELLIGENCE
Elite Threat Hunting: CrowdStrike's threat intelligence and elite threat hunters deliver the visibility needed to detect, understand and contain a threat, so your environment can be surgically recovered with speed and precision.

ENTERPRISE RISK REDUCTION
Better Protection: CrowdStrike's solutions help secure the most critical areas of enterprise risk including endpoint security, cloud security, identity protection and network monitoring to stay ahead of today's threats and stop breaches.

Last updated: Sept. 26, 2022
22-GC-012

PREPARE: ADVISORY SERVICES

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 simulate a targeted attack and guide your organization — either executive or technical participants — through a realistic incident simulation, offering the experience of an attack without the attendant disruption and damage.

RED TEAM/BLUE TEAM EXERCISE

- Prepare your cybersecurity team and learn from experts as one team (red) attacks and the other team (blue) defends in your environment.
- This exercise focuses on maturing your security team's threat hunting knowledge and incident response processes through a real-world targeted attack scenario.

ADVERSARY EMULATION EXERCISE

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

PENETRATION TESTING SERVICES

- The CrowdStrike 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.

Last updated: Sept. 26, 2022
22-GC-012

FORTIFY: ADVISORY SERVICES

CYBERSECURITY MATURITY ASSESSMENT

- CrowdStrike Services asserts that being "compliant" doesn't mean you're secure. Rather than focusing solely on compliance, the CrowdStrike 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.

SOC ASSESSMENT

- An in-depth assessment helps identify gaps in your cybersecurity operations and IR program.
- Enhance the maturity level of your security operations center (SOC) and IR processes.
- Identify and prioritize actionable areas for improvement with guidance on achieving your desired future state of security operations.
- Receive a detailed and tailored report based on CrowdStrike workshops, documentation analysis and follow-up discussions.

CYBERSECURITY ENHANCEMENT PROGRAM

- Develop and implement a post-breach cybersecurity enhancement program to close security gaps and prevent further breaches.
- The CrowdStrike 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.

TECHNICAL RISK ASSESSMENT

- Proactively discover IT hygiene issues and vulnerabilities in order to safeguard your network before a breach occurs.
- The CrowdStrike Technical Risk 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.

AD SECURITY ASSESSMENT

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

SECURITY PROGRAM IN DEPTH

- Combines a wide-aperture view and detailed examination of the maturity of your information security program.
- Highlights the areas of greatest risk and helps build the business case for improvements.
- Provides a prioritized plan to reduce security risk with impactful improvements.

Last updated: Sept. 26, 2022
22-GC-012

PLUS: CLOUD SECURITY AND IDENTITY PROTECTION SERVICES

CLOUD SECURITY SERVICES

- **INCIDENT RESPONSE FOR CLOUD:** Handle critical security incidents and conduct comprehensive forensic analysis to resolve immediate cyberattacks in your cloud environment.
- **CLOUD SECURITY ASSESSMENT:** Gain actionable insights into ineffective cloud settings, cloud security misconfigurations and deviations from recommended cloud security architecture to help you prevent cloud breaches.
- **CLOUD COMPROMISE ASSESSMENT:** Identify ongoing or past attacker activity in your cloud environment and remove active threats from your network.
- **RED TEAM/BLUE TEAM EXERCISE FOR CLOUD:** Prepare your cybersecurity team and learn from experts as CrowdStrike's red team attacks and its blue team helps your team defend against a targeted attack on your cloud environment.
- **CROWDSTRIKE FALCON OPERATIONAL SUPPORT FOR CLOUD SECURITY:** Receive expert guidance and implementation support for the deployment, configuration and weaponization of your Falcon cloud security solutions, including Falcon cloud workload protection (CWP), Falcon Horizon™, Falcon Discover™ for cloud and CrowdStrike container security.

IDENTITY PROTECTION SERVICES

- **IDENTITY PROTECTION ONBOARDING:** This quick-start service deploys and operationalizes the CrowdStrike Falcon Identity Protection (IDP) solutions for detection and prevention with Zero Trust.
- **IDENTITY SECURITY ASSESSMENT:** An in-depth security assessment of your endpoints, identities and AD environment highlights major risk areas, identity best practices, and misconfigurations known to be exploited by knowledgeable threat actors.

Last updated: Sept. 26, 2022
22-GC-012

PLUS

MANAGED SECURITY SERVICES

- Falcon Complete™ managed detection and response (MDR)
- Falcon OverWatch™ managed threat hunting
- Falcon Intelligence Recon+ managed digital risk protection

FALCON ENABLEMENT SERVICES

- Falcon Gold Standard
- Falcon Operational Support
- Falcon Application Services

CROWDSTRIKE UNIVERSITY (CSU)

- Falcon Training
- Falcon Certification

SERVICES RETAINER

IR AND ADVISORY SERVICES

All of the CrowdStrike IR and Advisory 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 advisory 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
Minimum Hours	110	160	248	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

Last updated: Sept. 26, 2022
22-GC-012