CROWDSTRIKE INCIDENT RESPONSE AND PROACTIVE SERVICES

We are here to help
CROWDSTRIKE’S INCIDENT RESPONSE (IR) AND PROACTIVE SERVICES TEAMS PLAY A CRUCIAL ROLE IN HELPING ORGANIZATIONS MATURE THEIR SECURITY POSTURES AND STOP A BREACH SHOULD ONE OCCUR. THESE SERVICES ARE ARCHITECTED TO ENABLE ORGANIZATIONS TO REACT QUICKLY AND EFFECTIVELY TO A CYBERSECURITY INCIDENT. CUSTOMERS ALSO BENEFIT FROM THE ABILITY TO IMPLEMENT A RANGE OF PROACTIVE SERVICES DESIGNED TO IMPROVE THEIR OVERALL CYBERSECURITY READINESS.
AM I BREACHED?

INCIDENT RESPONSE

The CrowdStrike IR team works collaboratively with organizations to handle critical security incidents, resolve immediate issues and implement a long-term solution to stop recurrences. The CrowdStrike team is laser-focused on getting organizations back to business faster, while at the same time, drastically reducing the financial impact of an incident. This is accomplished by leveraging CrowdStrike’s unique cloud-based Falcon platform to identify attackers and effectively eject them from the environment. This methodology and approach cover all aspects of an incident, including providing a thorough technical investigation and ensuring containment, recovery and reporting.

COMPROMISE ASSESSMENT

The CrowdStrike Compromise Assessment (CA) is specifically designed to identify current and past attacker activity in an environment. The compromise assessment team brings years of experience in hunting and responding to the most sophisticated intrusions, by the most advanced attackers around the world. The team leverages the Falcon platform along with unmatched cyber threat intelligence (CTI) and 24/7 threat hunting.

BUSINESS EMAIL COMPROMISE (BEC)

With the rise in unauthorized access to corporate email via phishing and malware attacks, CrowdStrike has created an add-on service to the CA that addresses business email specifically, using innovative methodologies to proactively identify these attacks. This allows CrowdStrike Services to deliver the most comprehensive assessment of an organization’s IT environment, ultimately answering the critical question, “Has my organization been breached?”

FALCON NETWORK AS A SERVICE

To find the latest threats, security teams need increased visibility across their networks, including areas not covered by other tools currently in their security stacks. Falcon Network is a network monitoring security service that utilizes both the expertise of CrowdStrike Services threat hunters and a virtual network appliance that detects threats present in the environment.

To perform this work, CrowdStrike® Services brings together a team of security professionals from intelligence, law enforcement and industry; architects and engineers from the world’s best technology companies; 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, 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, it helps them defend their organizations against future attacks.

CrowdStrike’s incident response and proactive services can be used individually or in combination with each other, and can be covered by a 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 other proactive services, all of which are focused on helping to improve your overall security posture. Crowdstrike Services helps organizations secure and mature their security postures by addressing three fundamental questions: Am I breached? Am I mature? Am I ready?
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. This allows the team to assess an organization’s cybersecurity maturity in relation to its ability to prevent, detect, and respond to the most advanced adversaries.

Incident Response Policy, Plan and Playbook Development
With the ever-changing threat landscape, organizations must continuously evolve their incident response playbooks. This offering is designed to help organizations improve their incident response operations by standardizing and streamlining their processes. The services team analyzes your current plans and capabilities, then works with your team to develop relevant processes and documentation, including incident response plans, policies or playbooks.

Cloud Security Assessment
With cloud security threats on the rise, organizations continue to struggle with securing their cloud environments. CrowdStrike’s Cloud Security Assessment combines forensic analysis and penetration testing of your cloud infrastructure, to determine if the appropriate levels of security and governance have been implemented to counter inherent security challenges.

Active Directory Security Assessment
This unique offering is designed to review Active Directory (AD) configuration and policy settings in order to assess security configuration issues that attackers can leverage. The assessment involves review of documentation, discussions with staff, execution of proprietary tools and manual review of your AD configuration and settings.

AM I READY?

Cybersecurity Tabletop Exercise
CrowdStrike Services’ advanced experience in conducting IR against sophisticated cyber threats provides a real-world perspective on the tabletop exercise process. The 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.

Cybersecurity 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 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 CrowdStrike team then leaves it up to you to determine how best to manage the information. At the conclusion of the engagement, you will quickly understand the weaknesses in your process.

Adversary Emulation and Penetration Testing
This test provides the benefit of experiencing a sophisticated targeted attack without the actual damage that accompanies 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 shares with you how the goal was achieved and helps you identify tactics you can employ to help prevent future attacks.

Red Team / Blue Team Operations
During this exercise, CrowdStrike deploys two highly skilled teams of consultants: a Red Team that uses real-world attacker techniques to compromise your environment, and a Blue Team of incident responders who sit with your security personnel and use your existing tools to identify, assess and respond to the intrusion. Throughout this exercise, CrowdStrike experts slow down the attack lifecycle and guide your team in responding to an adversary campaign. This is done with an eye toward facilitating operational growth, investigative experience and program maturity.
ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging the cloud-delivered CrowdStrike Falcon® platform — next-generation endpoint protection, cyber threat intelligence gathering and reporting operations, and a 24/7 proactive threat hunting team — the CrowdStrike Services security team helps customers identify, track and block attackers in real time. This unique approach allows CrowdStrike to stop unauthorized access faster and prevent further breaches. CrowdStrike also offers proactive services so organizations can improve their ability to anticipate threats, prepare their networks, and ultimately stop breaches.

Learn more at
www.crowdstrike.com/services