CROWDSTRIKE

CYBERSECURITY ENHANCEMENT PROGRAM

Move forward with the confidence to stop breaches

BEGIN A CYBERSECURITY ENHANCEMENT PROGRAM TO MOVE PAST A CYBER BREACH

Experiencing a cybersecurity breach is a company's worst nightmare. Experiencing a second breach would be downright catastrophic.

When a company has been the target of a cyberattack, there is an expectation from the highest levels of the organization that this must never happen again. Unfortunately, once an adversary has successfully breached your environment, they will continue to come back looking for other ways to gain access to your network.

As such, it is extremely important to implement an improvement plan that not only addresses what happened, why it happened, and who was responsible, but also aims to prevent a similar breach from occurring in the future.

DEVELOP AND EXECUTE A STRATEGIC PLAN TO PREVENT FUTURE BREACHES

The CrowdStrike® Cybersecurity Enhancement Program examines factors that may have contributed to any recent security incidents and identifies vulnerabilities or capability gaps that could contribute to future incidents. The CrowdStrike Services team identifies key areas for improvements and prioritizes them in a manner that maximizes your ability to reduce risk while continuing to work toward long-term goals.

Optionally, CrowdStrike Services can help you ensure that the implementation of the program meets the original objectives of your plan. By checking in with your team at periodic intervals, not only does the Services team help ensure that projects stay on course, it also helps reprioritize as new threats or operating conditions arise.

KEY BENEFITS

- Identify lessons learned from incident response activities
- Validate that new security controls are effective
- Identify what additional security improvements are needed and build a roadmap for implementation
- Assure executive stakeholders that the security program is moving forward and verify that improvements are reducing risk as you progress

CYBERSECURITY ENHANCEMENT PROGRAM

KEY CAPABILITIES

The road to recovery after a breach is different for each organization. It depends on the type of incident that occurred and the unique challenges and operational realities that the specific organization faces. The Cybersecurity Enhancement Program is a flexible, tailored approach for your organization and your unique circumstances and may contain the following components as required.

AFTER-ACTION REVIEW

This retrospective look at a recent incident typically consists of two elements:

- **Lessons-Learned Workshops:** This collaborative look back at the security incident helps identify areas where your internal processes were effective and where opportunities for improvement exist.
- **Security Control Validation Test:** This hands-on technical test of controls put in place to remediate the incident helps ensure they are working as intended.

PROGRAMMATIC AND TECHNICAL REVIEWS

A forward-looking evaluation of your security program and network security identifies factors that may increase the risk of another breach. These may include:

- **Cybersecurity Maturity Assessment or Security Program in Depth Assessment:** This full-spectrum review of your security program is meant to identify gaps in people, processes or technology that could open the door to future attackers. Outputs include a recommended roadmap for addressing any gaps in priority order.
- **IT Hygiene Assessment:** A hands-on technical assessment identifies potential vulnerable configurations in accessibility, account management, applications and Active Directory.
- **Compromise Assessment:** Forensic examination of areas of the network not included in the incident response ensures the compromise did not spread.

ONGOING ADVISEMENT

These periodic check-ins validate progress toward CrowdStrike's recommendations, troubleshoot issues that arise and help clarify how improvements have changed your risk exposure. Typically, the Services team performs formal check-ins on a quarterly basis and provides ad hoc support as needed between those sessions.

EXECUTIVE BRIEFINGS

Briefings to executive stakeholders provide an independent assessment of your security program and assurance of plans to enhance it. CrowdStrike typically provides two briefings: once after the programmatic and technical reviews are completed and once a year later to offer an update on how the security program has matured.

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**

WHY CHOOSE CROWDSTRIKE SERVICES?

CrowdStrike has assisted countless organizations in assessing cybersecurity programs to address the specific factors that matter in today's targeted threat landscape.

Advisory experience: It's one thing to give a customer a list of improvement opportunities. It's an entirely different level of support to help the organization successfully implement the intended risk mitigation strategies laid out in the program.

Board-level expectation management: When a breach happens, your board is going to seek answers to what happened and what happens next. The CrowdStrike Services leadership team has briefed boards and audit committees for customers in the same position and understands the questions that need answering, so that the board has confidence in the ability to stop future breaches.

Partnership with legal: Similar to the ability to work with your board, CrowdStrike also works closely with outside counsel that is typically involved in these types of assessments.

Highly skilled team: The Services team has unrivalled personnel with firsthand insight into the cybersecurity programs of organizations across all industries, sizes and geographies. CrowdStrike's deep knowledge in the tactics, techniques and procedures leveraged by today's most skilled adversaries grounds the assessment methodology in the areas likely to be exploited in the current threat landscape.

Powerful technology: The powerful CrowdStrike Falcon® platform is used to collect information from the organization's endpoints in order to gain technical hygiene insight.