Microsoft

Workshop – Security – Security Crisis & Response Exercise

Assess

Ensuring Security Crisis Readiness

Microsoft's experienced cybersecurity professionals can help

Overview

The Security Crisis and Response Exercise provides a unique offering to customers via a 2-day custom, interactive classroom experience on understanding security crisis situations and how to respond in the event of a cybersecurity incident. Members of the elite incident response team at Microsoft, the Detection and Response Team (DART) delivers the exercise as a proactive readiness training with the objective of helping our customers prepare for incident response through practice exercises.

The simulation is based on real-life scenarios from recent cybersecurity incidents. The exercise focuses on topics such as Ransomware, Office 365 compromises, and compromises via industry-specific malware via complex backdoor software. Each scenario covers the key areas of cybersecurity: Identify, Protect, Detect, Respond, and Recover and covers a broad eco-system including supply chain vulnerabilities such as software vendors, IT service vendors, and hardware vendors.

Solution Benefits

Effectively responding to any cybersecurity incident requires your teams to be ready at any given time to minimize potential damages to your organization's data, credentials, systems and even brand image. It also requires a multi-disciplinary approach consisting of security, infrastructure, networking and other teams within your organization. In addition, recovering from such incidents as quickly as possible and getting your business back up and running depends on your organization's security posture, incident readiness and your teams' effective response.

Cybersecurity-readiness begins with understanding your IT environment and determining the level of potential cyber risks. With the Security Crisis and Response Exercise, your teams will receive tactical and strategic recommendations and knowledge of the current cloud-centric threat landscape. DART experts will detail relevant, recent case studies, including how the incidents occurred, the impact on the organizations, and where even the smallest missteps created opportunities for attackers.

The scenarios that will be covered during the 2-day exercise includes:

- Ransomware
- O365 & Azure Intrusions
- Internal APT compromise
- Industry specific commodity malware, such as trojans (i.e. banking trojans)
- CPU related vulnerabilities (i.e. Spectre/Meltdown)

How the *Security Crisis and Response Exercise* Works

The first day of the 2-day simulation includes a walk through of the chosen scenario, where the instructor details operational, logistical, and technical details of an anonymized security event. The customer will leave this phase of the simulation with a better understanding of the indicators of compromise and the tactics of attackers for the scenario.

The second day of the exercise walks customers through the simulation once more but utilizes the customer's own security and IT processes to determine the likely impact for the customer's own organization. During each stage of the simulation, we will discuss the capabilities and skill sets required to limit organizational impact of a potential compromise.

Roles that would benefit from this workshop include, but not limited to:

- Incident Response management and senior incident response engineers
- Security Operations Center management and senior analysts
- Security Engineering management and senior security engineers
- Representation from: CISO office, CTO office, networking, backup, Active Directory, messaging, systems management, helpdesk, change control, functional area system administrators and compliance officers
- Optional: Representation from executive management, PR and Legal teams for visibility and insights on incident response, disaster recovery and readiness

Period of Performance & Outcome

Security Crisis and Response Exercise is a 2-day, on-site, classroom-based training on responding to cybersecurity incidents. Upon completion of the exercise attendees will have a better understanding of incident response concepts, latest attack methods and how these attacks can lead to compromises or breaches.

Customers will also learn how to effectively respond to such attack scenarios by using their organizations security processes, configurations and policies.

Seasoned Expertise

Microsoft is a worldwide leader in providing IT products and solutions to both the public and private sectors. Microsoft has led the industry in key security initiatives such as the Trustworthy Computing initiative, the Security Development Lifecycle, botnet takedowns, and the Microsoft Malware Protection Center. The Microsoft Detection and Response Team (DART) is comprised of senior IT and IT Security leaders and experts with extensive experience in both the private sector and government. Many are former military, intelligence and law enforcement members with seasoned cybersecurity backgrounds. DART engagements are delivered by experienced cybersecurity professionals who devote 100% of their time to providing cybersecurity solutions to customers worldwide.

Microsoft's Detection and Response (DART) Team has been widely utilized by various organizations worldwide including leading defense, government, and commercial entities to help secure their most sensitive, critical environments.

Cyber security has become a crucial business risk that must be prioritized and actively addressed by all organizations today.

Overlooking a single security threat can create a serious event that could severely erode community and consumer confidence, can tarnish reputation and brand, negatively impact corporate valuations, provide competitors with an advantage, and create unwanted scrutiny.

Microsoft works with customers globally to identify risks and provide proactive solutions to help our customers manage their cyber risk especially in today's dynamic threat environment.

Microsoft