TEVORA™

tevora.com

Incident Response

Tabletop Exercises

The term incident response refers to the process of handling a security breach or attack – also called an "incident." But uncovering the hidden threats in your environment and removing them before they cause further damage require skills, tools and a plan. You need a partner that is experienced in identifying, isolating and eradicating threats rapidly in order to limit the consequences and help you return your environment to normal operating conditions quickly.

Tevora IS that partner. Our comprehensive Incident Response (IR) services and team of IR specialists help you **plan**, and **prepare**, **detect** and **respond** quickly and effectively to threats in your environment. Tevora's pre- and post-IR services are focused on helping your organization survive a cyberattack – and strengthening your defenses against future incidents. ▲

Exercises that simulate real-world cyberattacks in a controlled environment can reveal a lot about an organization's ability – or inability – to handle a threat. This is the goal of Tevora's Tabletop Exercises. Our team reviews your organization's current policies, procedures, security tools and infrastructure, then builds immersive, custom threat simulations based on your specific environment.

How Tevora IR Services Help You Manage and Respond to Threats

Deployment

- Analyze and scan the environment for Indicators of Compromise (IOCs) or malicious activity
- Gather and investigate client-provided information of the incident from various departments
- Begin building IOCs based on attacker tactics, techniques and procedures (TTPs

Incident Scope Review

- Monitor the environment for attacker activity and IOCs
- Seek out evidence of similar past attacker activity and IOCs

Collaborative Analysis

- Analyze digital forensics, network traffic, logs, malware, and live response data
- Collaborate with the organization's internal team to ensure all relevant data and information is considered

Continued on back of page.

HITRUST Authorized CSF Assessor

How Tevora IR Services Help You Manage and Respond to Threats
Continued

Damage Assessment

- Identify impacted systems and/or facilities
- Ascertain if any applications were affected
- Determine the level of information exposure

Remediation

- Remediate based on best practices and organizational needs with full recovery
- Implement containment actions based on the attacker's methods and TTPs
- Formulate a strategic incident management plan to help respond to future incidents
- Perform a status check of the environment to prevent damage from future attacks

Need Emergency Incident Management and Incident Response Services?

There's no "good" time for a cybersecurity emergency, and there's no time to waste, either. The Tevora Computer Security Incident Response Team (CSIRT or CIRT) is on standby 24/7 and ready to come to your aid during an incident to secure your system and get you back online quickly. Please refer to our Emergency Incident Response datasheet for details on these services. ▲

In this low-stress environment and guided through each exercise by our IR experts, your team can review and test your established IR procedures and responses to the most severe incidents – including phishing, ransomware, and denial of service scenarios – and identify existing and potential gaps in your IR plan and infrastructure. Based on the results of the exercises, our team provides specific recommendations designed to improve your organization's ability to handle incidents. Test your team's ability to respond with Tevora Tabletop Exercises.