TEVORA™

tevora.com

Incident Response

Emergency Incident Management and Response

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. ▲

There simply is no "good" time for a cybersecurity emergency – and certainly there is no time to waste. Our Tevora Emergency Incident Response services are available 24/7 to help you handle an active threat whenever it occurs, minimize damage, secure your system and get you back online quickly.

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

Deployment

- Identify, assess and investigate
- Analyze and scan the environment for Indicators of Compromise (IOCs), malware, suspicious activities and vulnerabilities
- Gather and investigate client-provided details of the incident
- Begin building IOCs based on attacker tactics, techniques and procedures (TTPs)

Crisis Management

- Coordinate with the organization's leadership to take appropriate action
- Contain risks, manage crisis and remove security threats immediately
- Recover systems, data and connectivity to ensure continuity

Incident Scope Review

- Review logs and monitor environment for IOCs and Indicators of Attack (IOAs)
- Investigate and review incident more thoroughly, considering all prior activity and IOCs to provide a comprehensive overview

Continued on back of page.

HITRUST Authorized CSF Assessor

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

Continued

Collaborative Analysis

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

Damage Assessment

- Clearly identify how the system was compromised and assess damage
- 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 Incident Response Services?

Tevora offers a comprehensive set of non-emergency IR services that help you plan, prepare, detect and respond to incidents within your environment. Please refer to our Incident Response Services datasheet for details. ▲

Our Computer Security Incident Response Team (CSIRT) is comprised of specialists from all areas of IR and includes incident responders, malware researchers and cyber intelligence professionals. Our IR "SWAT" team works rapidly using their dedicated IR skills as well as multiple IR and digital forensics tools to identify and locate the active threat(s), determine the incident scope and damage, isolate and contain affected systems and eradicate the threat from your environment.

Once the threat is removed, the Tevora team cleans your system and helps you return to safe, full operation. A review of the incident, including entry point, associated evidence and patterns of behavior serve as the basis for our recommendations which may include changes or enhancements to your IR plan and/or infrastructure to close identified security gaps and to strengthen your defenses against future attacks.