Incident Response

Compromise Assessment

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. ▲

A security breach can occur in an environment in months – even years – before it is noticed. Tevora's Compromise Assessment team uncovers hidden threats within your environment and removes them before they cause further damage. We use a layered approach and multiple leading diagnostic tools to identify Indicators of Compromise (IOC) and Indicators of Attack (IOA) – the suspicious activity, behaviors and evidence that point to possible compromises in your environment.

HITRUST
Authorized CSF Assessor

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.

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. ▲

Once a hidden or potential threat is identified, the Tevora team contains the compromised host(s) and gathers data samples. We eradicate the threat, clean your environment, share the patterns of behavior found in your environment and based on the exploits found, recommend appropriate defenses, practices and architecture that will strengthen your security posture for the future. If attackers are lurking in your environment, the Tevora Compromise Assessment will sniff them out.