Incident Response (IR)

When cyber attacks intersect with patient care, every second counts.

[redacted]'s IR teams apply nation state-level expertise and techniques to help our clients respond quickly, minimize damage and learn from an attack. From insider threats to ransomware, [redacted] prides itself on the ability to pivot as needed at a moment's notice to help minimize impact to our clients. This is a highly intimate partnering exercise in which success is predicated on the ability to jointly decompose the incident phases of pre-incident operations, response activation, and post-breach intentions. At our core, [redacted] is a security *partner*, not a security *provider*.

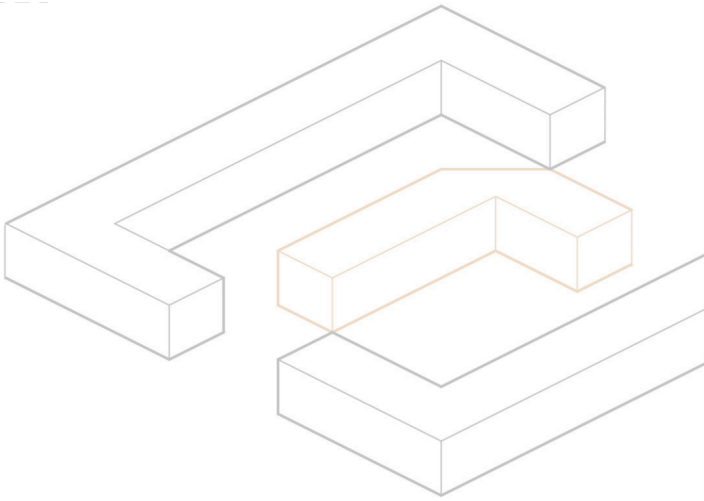
We engage with an agile mindset to rapidly test our hypotheses and adapt our techniques. We document and store our findings to preserve chain of custody. We act with urgency to ensure business continuity.

Threats evolve. So do we. So do our clients.

When called upon, the [redacted] team can validate an existing IR plan or help create one as part of a maturing cybersecurity program. We break down each of the six elements of an effective IR plan and ensure our client's plan is comprehensive and considers critical interdependencies.

Incident Handling Services

- Isolation of affected systems, platforms, and networks
- Triage
- Identification / Verification
- Categorization
- Internal/External Coordination
- Technical Aid
- Eradication / Recovery
- Operations, Maintenance, and Monitoring of IDS
- Post-Incident Consulting
- Preventative Support
- Training
- Report Assessment
- Third Party Analysis, Validation, Corrective Actions, & Reporting
- Resolution



American Hospital Association™
Preferred Cybersecurity Service

[redacted] is an American Hospital Association preferred cybersecurity service provider for Incident Response.

Case Study

Background

A client within the reproductive bioscience domain discovered their systems were infected with ransomware and initiated a same-day contract with [redacted] for assistance. Due to the sensitivity of the facility, delayed response would likely result in loss of life because of the systems affected.

The client tasked the [redacted] Incident Response (IR) team with rapid identification of the initial compromise, collection of forensic images for evaluation, development of initial recommendations to neutralize the infection, and restoration of the IT ecosystem to operational capacity. Within an hour of notification, [redacted] deployed an Incident Commander and Forensic Analysts. [redacted] personnel were on-site inside of 24 hours, managing every aspect of the identification, containment, eradication, and recovery.

Engagement

The IR team began with a compromise evaluation of the IT environment, including the collection of forensics images for analysis. The team quickly identified and segregated critical assets from the network to avoid continued spread of the infection and immediately began threat hunting activities. During this phase, [redacted] determined the client was the victim of a phishing attack, resulting in actors gaining remote access to their network and subsequently propagating malware across the network. Quickly enumerating the ransomware's presence, [redacted] determined the actor had persistent and pervasive remote access to the client's networks.

While the [redacted] IR team successfully stopped the spread and eradicated the actors, it was clear the adversary was not a typical ransomware actor, and they would return. Given the significant cost of the current clean-up combined with the possibility of future incidents, the client decided to perform a complete re-architecture, including endpoints, network and server infrastructure, configurations, development pipelines, global connectivity, and storage. In this case, [redacted] created a whole new company from an IT perspective, while working closely with the client's cyber insurance provider. During the rebuild, the team provided daily guidance on every aspect of the new architecture and incorporated best practices to properly secure the critical assets.

Outcome

[redacted] helped the client spare its most critical assets without loss of life during the incident thus protecting its prime source of revenue and, most likely, its future viability as a company. The team's expertise in security architecture and engineering resulted in a complete architectural rebuild along with several follow-on recommendations to ensure a more robust network security posture, the establishment of a new incident response plan, and proper procedures for passwords and role hygiene. [redacted] would typically engage law enforcement and offer additional pursuit capabilities to fully attribute the actors and hold them accountable, but in this case, the client declined.

healthcare@redacted.com

American Hospital Association™ Preferred Cybersecurity Service

[redacted] is an American Hospital Association preferred cybersecurity service provider for Incident Response.