HOLISTICYBER | SOLUTION BRIEF

DEFEND WHAT MATTERS

Incident Response Service

24/7 Incident Management -
Gain Containment & Get Back to Business Quickly

What is Incident Response?

Incident Response (IR) service is a tailored cybersecurity defense program, crafted by domain experts; designed to get the client back to business as quickly as possible. It consists of 24/7 incident response and management, deep-dive forensic investigations, threat removal and the implementation of proactive risk control and mitigation measures.

Our experts respond quickly to gain rapid containment and remediation, prevent further escalation and stop the attackers from reaching critical assets.

How does Incident Response work for me?

In the event of a suspected breach, we provide immediate assistance, identifying and neutralizing active threats against your organization. Whether it is an infection, compromise, or unauthorized access attempt to bypass your security controls, we are prepared to tackle it.

1. A top tear team of experts jumps in to handle the live incident, and evolving threats are met in real time by advanced detection technologies, preventative countermeasures and deceptive techniques.
2. Forensic analysis techniques are used to analyze all assets - disk, memory, and networks.
3. Infected network areas/endpoints/user IDs are isolated from the rest.
4. Attacks are stopped in their tracks.

A proactive response plan

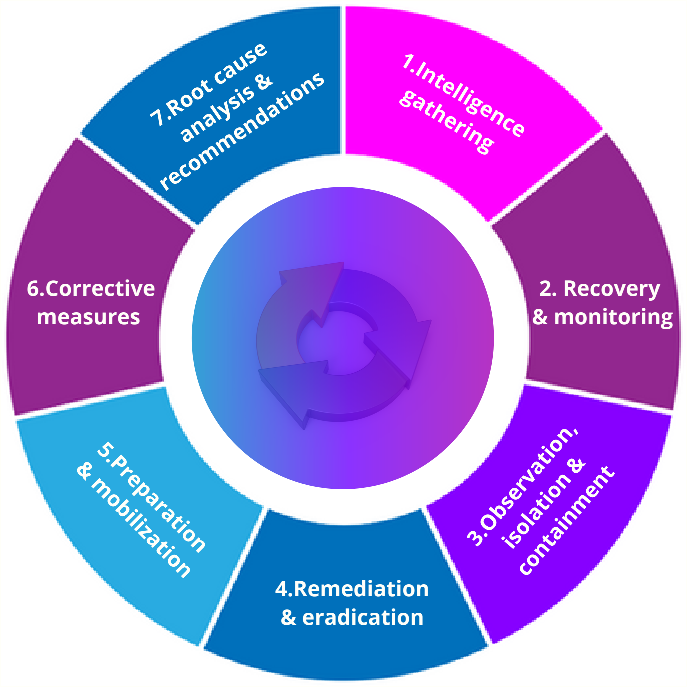
In addition to the emergency IR service, HolistiCyber offers a retainer based service that focuses on creating a customized response plan for the client. Domain experts continuously review, update and enhance the plan to meet evolving threats, while making your company unattractive to attackers, and deterring them with too much effort.

Our security experts provide a detailed threat map; identifying and categorizing your company's cyber-threat landscape both externally and internally. Based on the risks specific to your enterprise, they create a customized response plan for incidents.

In the event of a cyber-attack, your company will avoid extensive down-times, loss of data and other catastrophic results.

WHAT SHOULD YOU EXPECT?

- **Stops active cyber attacks in their tracks and monitoring**
- **24/7 real time and effective incident response**
- **Rapid triage, containment, and neutralization of active threats**
- **Multi-faceted prevention countermeasures**
- **Deceptive techniques**
- **Unique forensics analysis techniques**
- **Upgrades cyber awareness, security procedures and policies.**
- **Tailored strategy evolves quickly with changing threats.**
- **Elevates company's security posture and matures organizational cybersecurity program**


1.Intelligence gathering
2. Recovery & monitoring
3.Observation, isolation & containment
4.Remediation & eradication
5.Preparation & mobilization
6.Corrective measures
7.Root cause analysis & recommendations

Incident Response lifecycle

24/7 prevention and remediation

If a cyber attack is already under way, it should be stopped in its tracks and not be allowed to progress and spread to important areas in the organization with critical assets.

Our **nation-state grade experts** investigate cyber incidents and reveal entry points, essential attack components and the evolution of each attack. This is crucial in the first few hours of an attack as it can completely change the outcome and prevent catastrophic loses. Then, they provide focused recommendations on how to block the attackers and related route of access, as well as methods to improve security controls, counter-measures, and implementation of safeguards going forward.

Nation-state grade digital forensics

If you reached us after an attack has been launched, and we have already handled the threat, the next crucial step is to conclude which attack vector was used and how specifically it was exploited, which parts of the enterprise have been compromised (endpoints, network segments, user privileges, etc.) Digital forensics can shine a light into the gaps that were exploited and close them up for good, as well as preventing further damages from the current attack.

IR reduces risks by providing your business with a robust line of defense against attacks that would otherwise cause devastating downtimes and irrevocable financial losses.

"Our company went through a horrifying ordeal when we had a cyber attack. Everything shifted once we brought HolistiCyber to manage the event. Every aspect was handled quickly and professionally and ultimately, we had very little downtime. Plus, they left us with a strong defense plan to keep the sharks away."

CISO, Wholesale organization, USA