

Incident Response Readiness Services



Offering

Tier 1

Response table
top exercise

Tier 2

Threat hunting

Tier 3

Incident response
retainer

Having your network compromised by malicious adversaries can result in substantial unplanned costs. Also the impact on day-to-day operations can be crippling. An improper data collection may lead to large penalties, sanctions, and awarded damages. Our comprehensive Incident Response Program is founded on our three-tiered approach leveraging industry and proprietary best practices that assists clients with protecting assets and their

reputation. When a critical incident occurs, you'll need a trusted advisor to help with identification, triage, remediation, and preservation. HCLTech has over 15 years of experience helping companies respond to litigation readiness events and maintain normal business operations. Our skill sets are built on field tested real-world digital forensic team experience, memory forensics, legal investigations, and defensible data handling.

Objectives



Provide an after-action debriefing to review the response and provide supplemental information and education that will improve the overall incident security program.



Perform proactive threat hunts throughout the environment focusing on common areas of intrusion and compromise that are specific to the needs of the client. All items of interest will be escalated to the client for further investigation and remediation.



Facilitate incident response-oriented tabletop security exercises to evaluate the plan and the incident response capabilities.



Provide Incident Response (IR) Retainer Services to already be there in the event of an incident.



Tier 1 & 2

Incident response tabletop exercise and threat hunting scope and approach

Using industry best practices and proprietary methodologies HCLTech delivers services in a structured approach using a three-tiered offering.



Asset/Component	Description	Covered
-----------------	-------------	---------

Tier 1 - Incident response tabletop

Subject matter experts	Identification of resources from the organization to be included in the exercises.	Security team <ul style="list-style-type: none"> • Various members from executive team • Various members from regional facilities (plant managers, etc.)
Tabletop scenarios	The incidents scenarios which will be presented	The scenarios will be defined during scope/requirements discussions
Location	Method for how tabletops will be conducted	Remote meetings
Duration	The duration of the exercise	The total effort will take 5 days. The actual tabletop exercise will be facilitated over the course of 1 day.

Tier 2 - Threat hunting

Subject matter experts	Identification of resources from the organization to be included in the exercises	Security team
Location	Method for how threat hunting will be conducted	Remote SIEM/client environment access via SSL or VPN
Duration	The duration of the exercise	The Threat Hunting Service is performed on a scheduled basis (yearly, bi-annual or quarterly) at a minimum of every 8hrs
Threat hunting objectives	Threat hunting objectives	<ul style="list-style-type: none"> • Focused threat hunting on common areas of intrusion and compromise that are specific to the needs of the client. All items of interest are escalated to the client for further investigation/remediation • HCLTech is not responsible for incident remediation or handling.

Tier 1 & 2

Incident response tabletop exercise and threat hunting project deliverables

Deliverable	Description
Tabletop exercise after-action report	Incident response tabletop exercise for the client audience, PowerPoint presentation, After-action report with observations and recommendations.
Threat hunting reports	All threat hunting reports are made available via secured email (or an agreed-upon communication tool).

Tier 3

IR retainer services scope and approach

HCLTech has a proven track record of working with clients to triage and remediate critical forensic incidents that have jeopardized their business. HCLTech has comprehensive expertise to deal with traditional digital data preservations, in addition to more advanced and sophisticated defensible data collection, processing and early case analysis. Our team combines the skills they have developed with cutting-edge forensic tools, both commercial and open-source, to quickly triage the incident, and remediate the risk of data loss with proper data culling and collection. HCLTech also provides recommendations that outline what steps can be taken to ensure defensible and admissible data, while maintaining minimal tranches of potentially relevant evidence.



Example: 100 Hours	SLA
Overview	
<ul style="list-style-type: none"> • Incident preparedness service • Block of 100 pre-paid support hours • Enhanced SLA Commitments • Ability to purchase additional hours at discounted rates • Ability to apply unused IR hours towards other HCLTech services 	See below
Incident response service	
<ul style="list-style-type: none"> • Live response analysis of the systems to identify malicious activity • Triage of the incident to restore business critical operations • Analysis of the earliest evidence of malicious activity, breach, or compromise • Correlated threat intelligence to identify potential techniques, tactics, and procedures (TTP's) of the attacker • Incident response service 	<p>Initial contact (via email or phone) established within two (2) hours of being notified.</p> <p>HCLTech first-responder assigned to your case within six (6) hours of being notified.</p> <p>Delivery of IR services to commence upon Effective Date.</p>

For more information or to get started, please contact us:

Fortius@hcl.com | hcltech.com

HCLTech | Supercharging Progress™

BI-112206304734132-EN00A11

HCLTech is a global technology company, home to 211,000+ people across 52 countries, delivering industry-leading capabilities centered around Digital, Engineering and Cloud powered by a broad portfolio of technology services and software. The company generated consolidated revenues of \$11.79 billion over the 12 months ended June 30, 2022. To learn how we can supercharge progress for you, visit hcltech.com.

hcltech.com

