

# Incident Response & Forensic Services

INCIDENT READINESS | FORENSIC SERVICES | SECURITY THREAT MANAGEMENT

## Ensure You Have the Right Team During a Live Incident

Improper handling of information systems during a live event is the leading cause of data loss, business disruption, and increased financial and reputational costs for a company. Fast and strategic containment can limit the impact.

**HALOCK's Incident Response Team** has the specialized experience, tools and critical thinking required to handle your incident promptly and thoroughly. Our team works with your organization to resolve your incident, remove the threat and protect your critical assets.

### INCIDENT READINESS

- Incident Response Plan
- Incident Response Technology Review
- Compromise Assessment/Threat Hunting
- Incident Response Team Training
- First Responder Training

### FORENSIC SERVICES

### SECURITY THREAT MANAGEMENT



## INCIDENT RESPONSE READINESS

**INSIGHT & OUTCOME.** HALOCK's incident readiness response security experts assess the current state of your incident readiness and make recommendations for improving your security event preparedness. By leveraging our incident response and risk management experience, HALOCK evaluates your current incident readiness against standards such as NIST 800-61 and other industry best practices. Our assessments identify incident readiness gaps and suggest required remediation efforts to improve your position in the event of a security incident.

PREPARE	DETECTION & ANALYSIS CONTAIN, ERADICATE, & RECOVER	POST INCIDENT
<ul style="list-style-type: none"><li>IR Readiness</li><li>Organize the CIRT</li><li>Risk Assessment</li><li>Penetration Test</li><li>Compromise Assessment</li></ul>	<ul style="list-style-type: none"><li>Initial Call</li><li>Incident Handling Strategy</li><li>Imaging</li><li>Forensics</li><li>Threat Hunting</li><li>Threat Management</li></ul>	<ul style="list-style-type: none"><li>Update IR Plan</li><li>Update IR Exercises</li><li>Update Risk Register</li><li>Update Contracts</li><li>Update Policies &amp; Procedures</li><li>Expert Testimony</li></ul>
<b>REMEDIATION SERVICES</b>		
<ul style="list-style-type: none"><li>IR Plan Development</li><li>Security Solutions Implementation</li><li>PCI Compliance Remediation</li></ul>	<ul style="list-style-type: none"><li>HIPAA Compliance Development</li><li>First Responder Training</li><li>Incident Manager Training</li></ul>	<ul style="list-style-type: none"><li>Security Awareness Training</li><li>IR Technology Improvements &amp; Configuration</li><li>Security Engineering</li><li>Security Products Reseller</li></ul>

## INCIDENT RESPONSE READINESS SERVICES



### Incident Response Plan Review, Development, Updating

Review of your organization's documented approach to handling potential threats. HALOCK can help refine or develop a descriptive and well-documented IT incident response (IR) plan to safeguard data, protect network assets and ensure that critical services



### Incident Response Team Training

Training based upon your IR plan on processes, with a focus on notification obligations - when and what to communicate to external entities and internal employees. Training includes tabletop exercises for practice in these realistic scenarios.



### First Responder Training

Skills-based training preparing the first responder role. This 3-4 hour technical training offers best practices for forensic data acquisition for an investigation. Participants will receive forensic tools and instruction on when and how to utilize.



### Incident Response Technology Review

A review of security assets that could assist with an investigation of a breach or incident. This assessment covers deployed logging and monitoring technologies, computer and network forensic capabilities, advanced threat detection, and security architecture evaluation.



### Compromise Assessment/Threat Hunting

Identifies if there are active indicators of compromise across four attack vectors: Network & Application, Endpoint, Email, and Web Applications. Through passive appliance deployment, the Malware Threat Detection System analyzes network traffic to identify new and unknown malware threats not otherwise identifiable through penetration testing alone.

## FORENSIC SERVICES

Our forensic incident response investigators analyze your systems to determine what happened, how it happened and what information was breached. Whether the incident occurred on a PC, mobile device, server, email, network appliance, database or any combination of devices, HALOCK helps you contain the incident, eradicate any infections and recover — all while leveraging our investigative experience and technical expertise to assist you in identifying the chain of events that led to the breach.

- Incident handling and coordination
- Advanced threat visibility and analysis
- Forensic analysis of systems and data
- Containment and remediation assistance

HALOCK's security incident crisis management services work with organizations to manage executive communication, prioritize actions and contain major security incidents quickly and with minimal impact. We partner with your internal and external counsel to provide a cohesive, integrated process to help rectify your situation. Our senior crisis managers will assist you in handling even the most challenging security event — giving you guidance and assurance when you need it most.

## INCIDENT RESPONSE SOLUTIONS

Be prepared for an incident with an IR solutions that suits your specific environment. HALOCK partners with you to give you the security resources and tools you need.

INCIDENT RESPONSE SOLUTION OPTIONS	On Demand Incident Response	Basic	Premium
Contract	Quick Quote Agreement	Master Services Agreement (MSA)	Master Services Agreement (MSA)
Retainer	No	Optional*	Yes*
Service Level Agreement	No	No	Yes
Incident Response Readiness	No	No	Yes <sup>^</sup>

<sup>^</sup>Must select (1) Incident Response Plan Offering and (1) Training or Technical Review Offering



INCIDENT RESPONSE READINESS OFFERINGS		
Incident Response Plan	Training	Technical Review
Incident Response Plan Review	Incident Response Team Training	Incident Response Technology Assessment
Incident Response Plan Development	First Responder Training	Compromise Assessment
	End-User Security Awareness	

\*IR retainer hours expire after 12 months. May be used for any service for up to 18 months.

# COMPROMISE ASSESSMENT/THREAT HUNTING





Cyber security compromise assessments are purpose-built to seek and discover indicators of compromise (IoC), then determine the best course of action to remediate threats in progress. Diagnostics can be run individually or combined.

**OBJECTIVE:** Informs you what has already infiltrated your environment.

**FREQUENCY:** On demand or Ongoing program

**DELIVERABLES:** Comprehensive report - key threats detected, status, and remediation recommendations.

## MONITORING AND DETECTION

NETWORK & APPLICATION	ENDPOINT	WEB	EMAIL
<p>Identifies applications that are in use and associate a threat rating.</p> <p>Real-time advanced malware security intelligence and metrics.</p> 	<p>Software agents deployed on selected endpoints.</p> <p>Evaluates activities on endpoints to determine if there are unwanted or unauthorized behaviors.</p> 	<p>Evaluates threat activity that is occurring on Internet facing applications.</p> 	<p>Cloud email gateway deployed for passive inspection of email content.</p> <p>Gateway inspects and reports on malicious and sensitive content detected.</p> 



## HALOCK Analysis & Remediation Guidance



## SECURITY THREAT MANAGEMENT

HALOCK's Security Threat Management program continually monitors your organization — providing alerts, blocking improper access and delivering real-time cyber threat analysis. Our goal? To reduce the average time to identify and contain a breach to less than two business days, offering you peace of mind by reducing your risk.

Benefit from proactive protection including twice daily checks and a 24 hour SLA; weekly project updates on the state of your environment and summary of threat activities; performance reporting; and real-time containment and protection, with immediate reporting and support of incidents.

HALOCK's Security Threat Management solution delivers proactive protection through six key areas of focus:



**HALOCK Security Labs**  
 1834 Walden Office Square, Suite 200  
 Schaumburg, IL 60173  
 847-221-0200

Incident Response Hotline: 800-925-0559

**www.halock.com**

© Copyright 2019 HALOCK Security Labs. All rights reserved.

## About HALOCK

Founded in 1996, HALOCK Security Labs is a thought-leading information security firm, that combines strengths in strategic management consulting with deep technical expertise. HALOCK's service philosophy is to apply just the right amount of security to protect critical assets, satisfy compliance requirements and achieve corporate goals. HALOCK's services include: Security and Risk Management, Compliance Validation, Penetration Testing, Incident Response Readiness, Security Organization Development, and Security Engineering.