

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 and increased financial and reputational costs for a company. Fast and proper containment can limit the impact of damages.

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

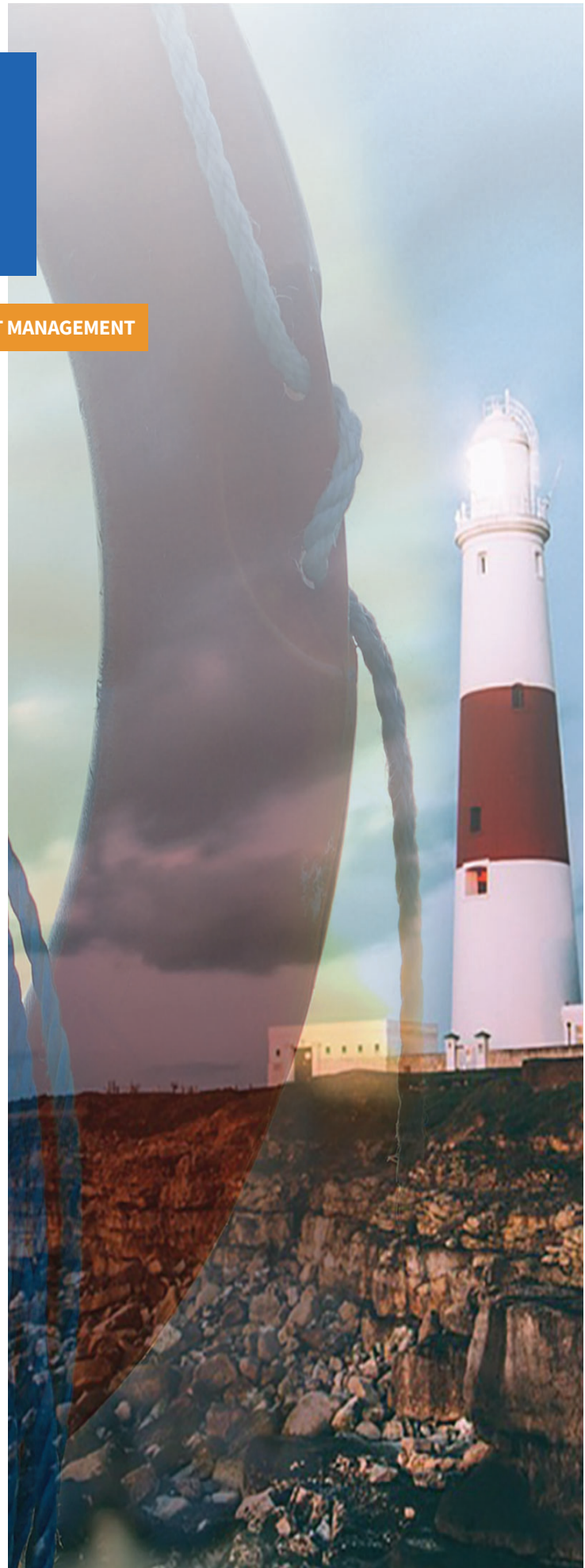
Compromise Assessment

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">IR ReadinessOrganize the CIRTRisk AssessmentPenetration TestCompromise Assessment	<ul style="list-style-type: none">Initial CallIncident Handling StrategyImagingForensicsThreat Hunting & Management	<ul style="list-style-type: none">Update IR PlanUpdate IR ExercisesUpdate Risk RegisterUpdate ContractsUpdate Policies & ProceduresExpert Testimony
REMEDATION SERVICES		
<ul style="list-style-type: none">IR Plan DevelopmentSecurity Solutions ImplementationPCI Compliance Remediation	<ul style="list-style-type: none">HIPAA Compliance DevelopmentFirst Responder TrainingIncident Manager Training	<ul style="list-style-type: none">Security Awareness TrainingIR Technology Improvements & ConfigurationSecurity EngineeringSecurity Products Reseller

INCIDENT RESPONSE READINESS SERVICES



Incident Response Plan Review

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 receive 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

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 help organizations manage executive communication, prioritize actions and contain major security incidents quickly and with minimal impact. 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.

COMPROMISE ASSESSMENT





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

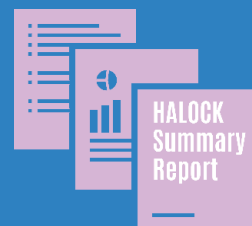
DELIVERABLES: Comprehensive report - key threats detected, status, and remediation recommendations.

MONITORING AND DETECTION

NETWORK & APPLICATION	ENDPOINT	WEB	EMAIL
Identifies applications that are in use and associate a threat rating. Real-time advanced malware security intelligence and metrics.	Software agents deployed on selected endpoints (up to 25). Evaluates activities on endpoints to determine if there is unwanted or unauthorized behaviors.	Evaluates threat activity that is occurring on Internet facing applications.	Cloud email gateway deployed for passive inspection of email content. Gateway inspects and reports on malicious and sensitive content detected .
			



HALOCK Analysis & Remediation Guidance



SECURITY THREAT MANAGEMENT

HALOCK's Security Threat Management (STM) 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, off ering you peace of mind by reducing your risk.

The key to successful information security risk management is proactive protection: services and solutions that help your organizations be on guard against potential threats and take action before cybercriminals can compromise your network.

HALOCK's STM solution delivers proactive protection through six key areas of focus:



READY. RESPONSE. REMEDIATE. RESULTS. WHY HALOCK?

HALOCK gives you the tools to properly handle a security event so you can help prevent the spread of harmful malware, and reduce data loss and legal liability. Your staff must be aware, well trained and diligent in following your response procedures to quickly and safely mitigate a security crisis.

Our professionals are experienced in cyber incident response services, including response handling, detection of advanced malware, forensic examination, criminal investigations and crisis management.

Our security experts are ready to assess your current incident response readiness and help you prepare before a security event occurs. We get involved early to help your organization navigate the complexities of a security incident and minimize the impact to your business.

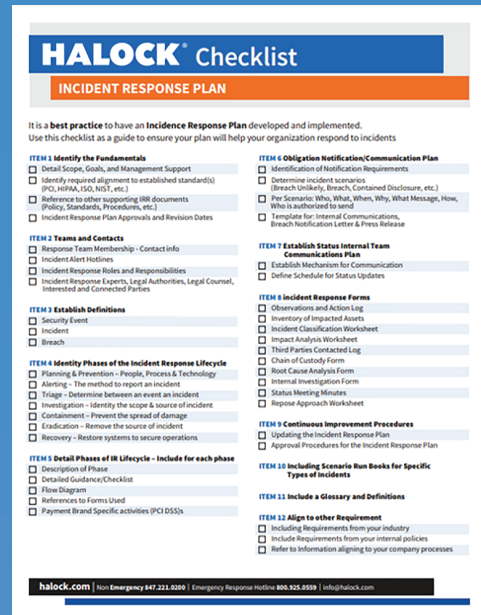


HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847-221-0200

Incident Response Hotline: 800-925-0559

halock.com

© Copyright 2019 HALOCK Security Labs. All rights reserved.



Assess your incident readiness with the Incident Response Plan Checklist

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.