HITACHI
Inspire the Next

DIGITAL FORENSICS AND INCIDENCE RESPONSE

CONTACT

955 Boulevard Michèle-Bohec
#244, Blainville, Quebec
Tel: 1-800-430-8166

HITACHI
Inspire the Next

HITACHI
Inspire the Next

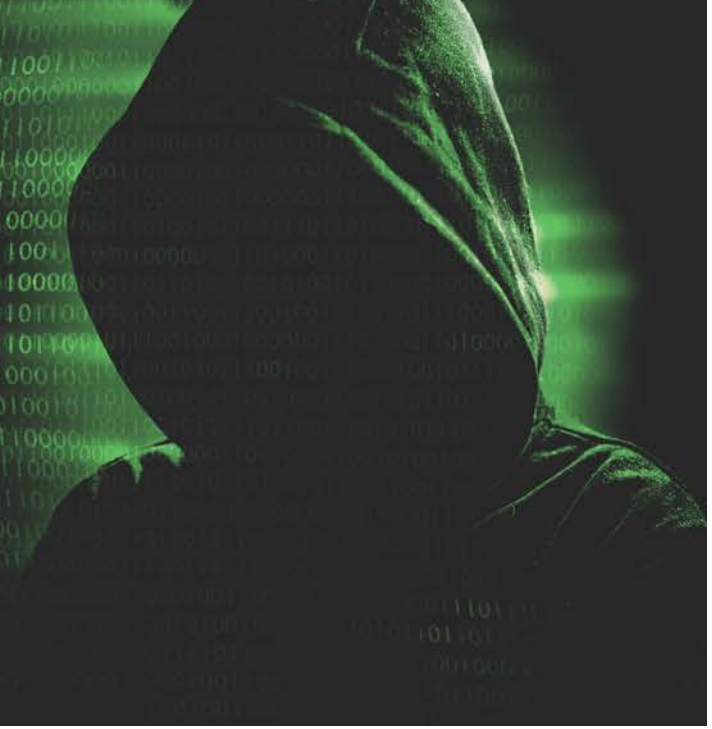
BEING PREPARED WINS THE BATTLE

Attacks are imminent. It's not a matter of when or if your system will be attacked. It's a matter of how good your incident response plan is.

A response plan should be actionable, understandable, and effective while considering all aspects of your current system, previous data breaches, and potential future gaps.

Your customized response plan will include our analysis at every angle and designed to repair existing flaws while also preparing your team to react rapidly to future attacks.

The Hitachi Systems Security difference is knowing that you have an experienced team on your side around-the-clock.



DEFINING THE ATTACK

Investigating the exact parameters of the episode, how it happened, and what it means for your company right now.

Rapid breach containment: stopping current damage from spreading and working proactively to prevent the same kind of attack from happening in the future.

INITIAL RESPONSE STEPS

Hitachi's Incident Response plan begins with an initial conversation to discuss the attack's details and what steps are needed to resolve the issue.

RESPONSE PLAN

Our white-glove service includes a complete investigation of past attacks and current security holes.

Our investigation lead will work with your company to devise a response plan that can immediately be put into action at the onslaught of an attack.

HITACHI
Inspire the Next

INCIDENT RESPONSE SERVICES IN DETAIL

- **Identification of the breach source and contributing factors**
- **Containment of the attack and reduction of the incident scope and residual effects.**
- **Localization, removal, and activity blockage of the attack**
- **Complete analysis of the incident identifying underlying causes**
- **Implementation of recovery practices and proactive solutions**
- **In-depth review of activities and discussion of the investigation and post-investigation actions**

HITACHI
Inspire the Next

OUR ONSITE AND REMOTE APPROACH TO SECURITY ATTACK

Our incident consultants have extensive experience in handling thousands of security breaches.

Add that experience to our patented threat intelligence service (TI), and the result is a rapid risk assessment that identifies risks before, during, and after they happen.

End-point Scanning: our team uses 30-different anti-virus agents combined with customized resources capable of identifying gaps on Windows, Linux, Mac, and various other systems.

Network Traffic Inspection: rapid log analyses allow us to identify how threats accessed the environment and determine if any exposed or malicious services remain.

Credentialed Internet Scans: using specific indicators of compromise, we will perform a detailed infrastructure scan.

Rapid Alerts: our detailed assessments allow us to observe any security gaps that may have existed during an impending or present attack.

Ongoing Containment Activities: our senior breach response team will work with your company to predict and contain any potential threats.

COMPLETE FORENSICS INVESTIGATION

Our consultants will provide your team with a complete forensic analysis to determine whether your system is secure.

The Hitachi forensics analysis includes the following:

Unauthorized access: was PII, personal data, confidential or proprietary information accessed without an authorization? Was this information exfiltrated?

Analysis: how was your environment accessed? How can the environment be secured in the future? Our team will provide a complete hard disk investigation via keyword search and criteria related to the incident resulting in a 360-degree analysis.

Proactive Planning: our team will provide researched and analyzed recommendations to contain and eradicate potential future threats.

Our Customized 4 Phase Methodology

Phase I: our team of specialists will compile all data, including photographs of physical assets, computer bios for file system benchmarking, verifying of data using algorithms and evidence files, and the preservation of discovered malware, related meta-data, and all log files. All data will be preserved in a non-destructive manner using industry-blocking tools.

Phase II: Evidence files will be subjected to an exhaustive series of processes, including the mounting of files, databases, archives, registries for viewing, and text indexing.

Phase III: our team will perform a complete analysis including incident response actions, network evidence for all other incidents, firewall and system logs, and an investigation into any evidence of data extraction or compromised distribution of data (email systems, open data, and unauthorized access).

Phase IV: an executive summary or formal forensic investigation report will be prepared and presented based on analysis results. Our consultants will work with your company every step of the way to explain details and execute a contingency plan.

IR (Incident Respond) Retainer

HITACHI
Inspire the Next

The Hitachi Systems Security Inc. retainer package is structured to allow HISYS-SEC MSS clients to consume hours under the master retainer package

Allocation of hours: pre-authorized and pre-paid allocation of incident response hours (TBD) to ensure incident responders promptly engage in a response scenario.

Hours to be used by HISYS-SEC's Clients at HISYS-SEC's discretion.

- Eligible services for use of hours: In addition to the IR Services, Client may use the retainer hours for Additional Services such as:
- Digital Forensics
- Incident response plan audit and/or table-top review
- Incident response plan update
- Dark Web assessment o Compromise assessment
- Vulnerability and penetration testing
- Application testing
- Security architecture
- In person security awareness training

IR (Incident Respond) Retainer

We ensure that your organization is prepared to take immediate and effective action.

Be ready for anything with full and experienced team support.

HITACHI
Inspire the Next

- Approved by many major cyber insurance carriers.
- Legal and public relations support available.
- Standard and enhanced onboarding options.
- Re-use of 50% of response hours if retainer is not triggered.
- Support for digital forensics and privacy breach advocacy.
- Discounted rates for entire response lifecycle.
- Direct access to elite response team, including Incident commander.
- Guaranteed rapid response time for cyber breaches.