DIGITAL DEFENCE

Cyber Incident Response

Respond
Service

OVERVIEW

All data networks come under attack by motivated hackers or disgruntled insiders; it is inevitable that –sooner or later- a security incident will occur. It is even possible that a breach, releasing confidential data to unauthorized persons, will result.

The goal of Incident Response is to stop security breaches before they happen, or to effectively respond while they are happening. A rapid response protects your Information assets and resources, and allows you to comply with regulatory requirements, avoid legal liability, prevent relay attacks against other organizations, and to minimize the potential for negative exposure to vendors, partners, and customers.

DigitalDefence has developed the Agile Incident Management, or AIM ™, program to increase the effectiveness of the incident response processes. AIM is the totality of proactive and reactive measures undertaken to help prevent and manage data security incidents across an organization.

KEY BENEFITS OF AN IMMEDIATE INCIDENT RESPONSE

- Our proprietary incident management methodology, Agile Incident Management (AIM) is designed to give the most rapid, comprehensive, and cost-effective response possible
- DigitalDefence has a deep knowledge of threat environment, including attacker objectives, methodologies, and tools. This intelligence is customized and applied specifically to the client during the investigation
- Our consultants have completed hundreds of ethical penetration tests, malware analyses, and incident response investigations; this unique knowledge allows them to rapidly and effectively assess a potential compromise

Improve corporate risk reduction with strategic security and privacy services.

Is the Cyber Incident Response Service right for your company?

- Are your employees prepared to recognize and alert you to a cyber attack?
- What do you do when your network is being attacked right now—can you respond to the incident, close it, and return to normal business operations?

- Commercial, open-source, and proprietary tools are used where necessary to complement manual testing in an investigation methodology that is customized for your organization. This provides the most effective means to identify a possible compromise
- An objective third party response by experienced professionals assures key clients, auditors, and management as to your organization's commitment to security

RESPONDING TO AN IMMEDIATE INCIDENT

DigitalDefence can provide immediate remote assistance, and can physically be at your site in as little as 4 hours. We are prepared to fully manage your incident response from start to finish. A rapid response, coupled with appropriate procedures, is critical to the success of controlling a security incident and preventing future occurrences.

When our skilled experts are deployed to your site, we will:

- Secure the scene
- Review the incident, and fully define the scope and the known timeline of events
- Reconstruct the security incident and identify potential suspects or groups of suspects
- Establish a timeline and project management framework for responding to the incident
- Isolate the probable cause using a structured root-cause analysis
- Contain the situation and eliminate the probable cause
- Preserve all evidentiary materials including live system data (physical memory, system parameters), network activity, IDS sensor output, firewall output, relevant event logs
- Conduct supplementary analysis, such as reverse-engineering of malware to determine if the organization has been targeted, or if the cyber incident was opportunistic
- Assist in recovery to a fully operational status
- Conduct a post-incident review to gather all relevant findings from key stakeholders
- Report on all findings, including investigative findings, evidence, and key recommendations.
- An executive summary will be prepared for non-technical review

About DigitalDefence

DigitalDefence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or "ethical hacking". And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss.

DigitalDefence Inc.
Toll-Free 800-385-1632 | Tel 519-771-8808
info@digitaldefence.ca | www.digitaldefence.ca