

Incident Response and Management



RESPOND
SERVICE

Improve corporate risk reduction with strategic security and privacy services.

Is the Incident Response and Management 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 and data are being attacked?
- How do you close an incident and return to normal business operations?
- Do you need to comply with a regulatory framework such as ISO27001:2005, PCI DSS, HIPAA, or HITECH? What about privacy requirements?

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.

DigitalDefence has pioneered the retained Incident Management, service, which brings our incident response and management expertise to small- and medium-sized companies at a reduced cost and with a rapid implementation to enhance your security as quickly as possible.

Benefits

- Verifies network and system breaches, identifies which systems have been compromised, and how the compromise took place
- Immediate 24x7 expert response; trained incident responders work collaboratively with your IT staff to establish a relationship in advance of a crisis, and to immediately respond to an event as it happens
- Comprehensive team-based approach brings together all required response and recovery specialists
- Provide direct liaison with law enforcement, other third parties
- Rapidly restores normal operations to minimize financial and reputational loss
- Demonstrates due diligence and fiduciary responsibility; preserves evidence and provides support for forensic investigation and legal remedy

Incident Management Training

Digital Defence provides unique training workshops to ensure your successful resolution of security incidents, including:

- Incident Response, a 5-day practical course focused on recognizing and responding to security incidents
- Scenario-Based Incident Response Training, customized to client requirements

About Digital Defence

Digital Defence 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

Service Description

Digital Defence's Computer Security Incident Response Team, ddCSIRT, is a "jump team" of certified incident response professionals who are available 24x7 to proactively prepare for an attack, or respond to one.

Proactive Services

DigitalDefence can augment your own response by providing specialized management and technical services in advance of a security incident by working with you to:

- Rapidly develop your customized incident response strategy, policies, standard operating procedures, and escalation criteria and procedures
- Provide 24 x 7 access to our Information Security Intelligence Service about vulnerabilities and attacks you should be aware of, and hotline support services
- Assist you in selecting and training your own in-house CSIRT team
- Provide vendor-neutral guidance in selecting and implementing technical solutions
- Create realistic training scenarios to prepare your staff to effectively respond to security incidents
- Create and implement effective security awareness training—employees will become your "first responder" to security incidents

Immediate Response Services

Digital Defence can be at your site in as little as 4 hours, and can 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:

- Review the incident
- Isolate the probable cause using a structured root-cause analysis
- Contain the situation
- Preserve all evidentiary materials
- Eliminate the probable cause
- Assist in recovery to a fully operational status, and identify any post-recovery issues

Digital Defence can also:

- Provide a trusted team of external experts to aid in your incident response (legal council, private investigation services, public relations, etc)
- Provide liaison support in dealing with law enforcement, and other third parties (ISPs, hosting companies, etc)

For more information please visit www.digitaldefence.ca



Digital Defence Inc

Toll-Free 866-677-1337 | Tel 905-681-3310
302 - 3310 South Service Road,
Burlington, Ontario L7N 3M6

Disclaimer

© 2010 Digital Defence. All rights reserved.
This document is for informational purposes only.
Digital Defence makes no warranties, express or implied, in this document.