

RESPOND Services



RESPOND
SERVICE

Improve corporate risk reduction with strategic security and privacy services.

Are the RESPOND Services right for your company?

- What do you do when your network and data are being attacked?
- Do you possess the technical knowledge to collect evidence against an attacker?
- How do you close a security 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?

Overview

No matter how much an organization prepares, a data security incident may be inevitable; therefore, the organizations that survive and flourish are those that can calmly and effectively respond to a security event. Having a plan of action before security incidents occur and having the right security partner to help when they do occur is critical.

Digital Defence's RESPOND Services are designed to give your organization the quick start and structured support to respond to any attack against your network and its data resources. Because they are directly derived from your organization's business strategy and practices - recognizing that true security is more than a technology solution.

Incident Response and Management

All data networks come under attack by motivated hackers or disgruntled insiders; it is inevitable that –sooner or later- a security incident will occur. 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** 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.

Incident Response Training

As leaders in the Incident Response field, Digital Defence shares its knowledge through a variety of workshops, including:

- Incident Response, a 5-day practical course
- Scenario-Based Incident Response and Management Training, customized to client requirements
- Data Forensics for Corporate Investigators, a 5-day practical course
- Live System Forensics, a 3-day practical workshop
- Malware Response and Analysis, a 3-day practical workshop
- Customized incident response and data forensics training specific 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

Data Forensics

Digital forensics is the rapid systematic and thorough approach used to find evidence and gather material for the support of criminal and civil actions. Digital Defence's forensics specialists are trained to respond to computer attacks and collect the electronic evidence from network devices, live systems (physical memory analysis), isolated hard drives, and analysis of malicious software ("backdoors", key loggers, etc).

After completing an analysis and documenting the relevant findings, our forensic experts can assist in preparing and presenting your case in court. We can also assist with enforcing the recovery of electronic evidence through Anton Piller orders.

eDiscovery

Electronic discovery (eDiscovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a criminal or civil legal case.

Digital Defence has developed a proactive approach to eDiscovery. By planning in advance, you can to legal challenges in a cost-effective manner that is consistent with your business practices. Because the response is planned, you can ensure regulatory compliance with legal requirements and drastically reduce your risks.

If you are already engaged in litigation, Digital Defence will identify, preserve, and document potential sources of electronic evidence in a manner that complies with legal requirements, industry standards, and industry best practices.

Activity Monitoring

As an employer, you are liable for the online activities of your employees. Activities that could create an exposure, and eventual financial or legal liability, include: theft of corporate data by employees who sell the data to a competitor, or use it to start a competing company, use of data and network resources in the commission of a fraud, inappropriate use of corporate Internet resources, including excessive personal web surfing, visiting adult sites, downloading copy write protected material, or sending inappropriate e-mails, and failure to prove compliance with regulatory requirements.

Financial and legal risks can be minimized, or even eliminated, if companies perform the due diligence of monitoring employee activities. In addition, companies can increase employee productivity by reducing non-business activity, drive rational network bandwidth and storage capacity planning, and assist in investigations of employees suspected in inappropriate activity.

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.