

PROTECT Services



PROTECT
SERVICE

Improve corporate risk reduction with services to protect the security and privacy of your data.

Are the PROTECT Services right for your company?

- Is your network “secure-by-design”, or is security an afterthought?
- Are you presently upgrading your network, or planning on implementing new technologies?
- Do current physical and logical controls provide adequate security for your data?
- Can you prove the security of your network and its data to an independent auditor?
- Do you have to comply with regulatory frameworks such as ISP27001:2005, PCI DSS or HIPAA / HITECH?

Overview

DigitalDefence's PROTECT services will help you to identify hidden security threats in your network, and understand their true impact on your organization. This knowledge will help you to build an effective security plan, and act before you become the victim of a security or privacy breach.

Pathfinder Assessment Service

With the Pathfinder Assessment, DigitalDefence will perform a rapid, fixed-price assessment of your organization's current security and privacy practices against the eleven domains of the international security standard ISO 27001:2005. We go beyond checklist-based reviews, reviewing your network infrastructure, and scanning your network devices and servers for vulnerabilities to create a baseline of the current security state of your organization., and a roadmap for mediation.

Physical Security and Social Engineering

It is generally accepted that if someone has physical access to any computing resource, that system can inevitably be compromised; therefore, physical security has evolved as one of the most important security controls that can be applied across the network.

DigitalDefence's Physical Security and Social Engineering service has three goals: (1) Ensure a safe working environment for all employees; (2) Ensure that physical access controls, data centres, server rooms, environmental controls, and key facilities are secure; and, (3) Ensure that employees have received the training required to recognize and respond to a social engineering attack.

Infrastructure Security: Network

Your organization's network infrastructure provides the functional support for secure business operations. We provide an objective assessment of your network's technology, people, and processes and how they impact security and privacy. Our goal is to ensure that the most appropriate controls are implemented—your business strategy is fully supported, security and manageability are enhanced, and complexity and cost are reduced.

Network Protection Training

As leaders in network and data protection services, Digital Defence shares its knowledge through a variety of workshops, including:

- Penetration Testing with the Metasploit Framework, a practical 3-day workshop on testing networks and websites using the leading open-source tool
- Network Penetration Testing, a 5-day practical course that goes beyond “ethical hacking” in teaching how to align testing to corporate objectives
- Mentored Penetration Testing, a customized course that teaches the fundamentals of penetration testing using your own network as the target
- Customized training is available for different skill levels, technologies

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

Infrastructure Security: Endpoint

One of the most significant threats to an organization’s security are the endpoints—the user-controlled devices that connect to the network (workstations, laptop computers, mobile phones and cameras, Blackberries, USB keys and portable hard drives) and specialized equipment like Point of Sale terminals.

Digital Defence provides a comprehensive program to ensure the provable security of your endpoints, and integrate them into your secure network.

Penetration Testing

A **vulnerability scan**, an automated scan of a network or device to determine if it possesses known vulnerabilities that could be exploited. Although this is the most cost-effective testing methodology, it is not accurate, and false results are common.

The most accurate testing methodology is **penetration testing**, sometimes referred to as “ethical hacking”. Using commercial, open source, and proprietary tools, skilled vulnerability researchers will use the same techniques that a hacker would use to assess your network’s security. By taking on the role of an outside hacker or a disgruntled employee, testers will: (1) demonstrate how the network was compromised, (2) prove that an actual compromise took place, and (3) provide real information on how to mediate against future attacks of this type. Digital Defence testers use both vulnerability scans and penetration testing to provide the most accurate view of network security, resilience of the network, and the survivability of your data when faced with an attack.

Digital Defence also provides training in penetration testing.

Web Services Security

Traditionally, firewalls, intrusion detection systems, and other network devices protect and secure networks. However, these safeguards cannot distinguish between legitimate and hostile traffic targeting a website.

DigitalDefence’s proprietary website and web application methodology, based on OWASP-standards, will assure you and your client’s that your web presence is not exposing your sensitive data.

Application Security

80% of all applications are vulnerable to application-layer specific attacks—how do you secure these applications in the existing threat environment?

Application security is the result of addressing underlying vulnerabilities during the Software Development Lifecycle (SDLC) - design, development, deployment, maintenance and termination of an application.

Digital Defence’s application security service aligns the technical aspects of application security to client business requirements, ensuring the delivery of a cost-effective and meaningful solution.

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.