DIGITAL DEFENCE

Pathfinder Security Assessment

Advise
Service

OVERVIEW

Often, an organization knows that they need to improve the security and privacy of their data, but they're not sure where to start. When this happens, you need an objective, rapid and cost-effective review of your security posture. It should highlight where you are, where you should be, and the best path to get from "here to there". You need a Pathfinder Audit.

With the Pathfinder Audit, DigitalDefence will perform an assessment of your organization's current security and privacy practices against the international security standard ISO 27001, and PCI DSS requirements.

We go beyond checklist-based reviews—DigitalDefence will review your physical security and data and voice network infrastructures, and scan your network devices and servers for vulnerabilities.

Unlike other assessments (vulnerability assessments, penetration tests), a Pathfinder audit is meant to support a rapid identification of the current security state of your network, and ensure that cost-effective mediation can be started as quickly as possible.

BENEFITS OF THE PATHFINDER SECURITY ASSESSMENT INCLUDE:

- Obtain an objective assessment of your current security and privacy state
- Demonstrate due diligence and fiduciary responsibility to clients, partners, and employees
- Comply with Federal and industry regulations; meet audit requirements
- Gain a significant competitive advantage against less secure organizations
- Reduce or eliminate financial and reputational costs of a data breach

Improve corporate risk reduction with strategic security and privacy services.

Is the Pathfinder Security Assessment Service right for your company?

- Are you a small– or medium sized enterprise that knows it must address security and privacy, but you're not sure where to start?
- Are business partners demanding that you meet compliance standards?
- Are you planning a security project in the future, and need to baseline your existing security policies and practices to effectively monitor improvements to your business?
- Are you recovering from a security breach?

- Obtain a high-level view of actual security and privacy exposure
- Receive a full identification and evaluation of your organization's critical networks, systems, and data
- Verified vulnerability assessment of your network, highlighting areas that must be mediated, and the means to do so

SERVICE DESCRIPTION

Upon completion of a Pathfinder audit, DigitalDefence will have performed the following tasks:

- Confirmed your existing documentation of the data and voice networks, including wired and wireless networks
- Documented your critical business assets, processes, networks, and systems
- Completed an administrative security and privacy assessment of your policies, standards, and procedures, as well as contractual provisions
- Completed a physical security assessment of the overall environment, physical access controls, and data facilities within your organization
- Completed a technical security assessment, including a review of the network architecture, security devices (firewalls, IDS/IPS), and advanced technologies such as VoIP and wireless
- Completed a vulnerability scan of the network, servers, and representative workstations from a "full knowledge" perspective. To maximize the scan's effectiveness and allow the testers to reduce false-positive results
- Assessed your organization's compliance against the ISO 27001 standard, and against the PCI DSS standard
- Developed a gap analysis to document the current state of your network versus the ideal security state
- Worked with you to create the "go forward" plan to implement changes and achieve the security and privacy demanded by your organization

The Pathfinder can be used to provide a rapid security assessment of partners who are accessing your critical data resources, ensuring that the same level of security and privacy is extended across the organization.

It has also been used to assess the security of organizations engaged in mergers or acquisitions, where it highlights potential security issues that could be expensive to mediate at a later date.

Domains of the ISO 27001 Standard

- Security policy and process
- Organization of information security
- Human resource security
- Asset management
- Asset control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationship
- Information security incident management
- Business continuity management
- Compliance with internal and external requirements

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

Disclaimer
© 2018 DigitalDefence. All rights reserved.
This document is for informational purposes only. DigitalDefence makes no warranties, express or implied, in this document.