

Advise. Protect. Respond.

Complete security breach protection

Company
Info



OVERVIEW

As Digital Defence is the leading provider of information security services focused on preventing and responding to security breaches.

Our global clients, ranging from Fortune 500 businesses to small- and medium-sized enterprises, secure their networks and critical information by taking advantage of Digital Defence's unique capabilities:

- Our structured service delivery model ensures that IT security is aligned and customized to your specific business; reducing your total costs and ensuring a timely and effective solution
- ddCSIRT, our Computer Security Incident Response Team, provides immediate and comprehensive on-site and remote assistance in the event of a security breach
- Our people are dedicated security specialists who combine military, law enforcement, and academic backgrounds with extensive experience and leading credentials. Commensurate with the trust that is placed in them, they hold Government-issued security clearances
- Our leadership is recognized within the industry, with frequent invitations to present at national and international security conferences. We continue to shape the information security field through our leadership in organizations such as the Toronto Area Security Klatch, TASK
- We are dedicated to sharing our knowledge, providing training and mentorship to all 3 levels of government, law enforcement, corporate clients, and the academic community

Reduce corporate risks and security costs with comprehensive services aligned to your business practices.

Are Digital Defence's Security Services right for your company?

How much security risk does your business face—and how can you manage this risk?

Do you understand the regulations, laws, and best practices that govern security and privacy in an organization like yours?

Are you presently upgrading your network, or planning on implementing new technologies?

Can you prove the security of your network and its data?

What do you do when your network and data are being attacked?



We ensure that your Information Security strategy, policy and security practices are fully compliant with industry best practices and all required laws and regulations.

ADVISORY SERVICES (GOVERNANCE, RISK AND COMPLIANCE, GRC)

- Virtual CISO, an interim executive level security professional develop and implement your security strategy
- Virtual Privacy Officer, to guide an effective privacy program or ensure your incident response complies with regulations and best practices
- Compliance Management, to identify and mediate gaps in complying with PCI DSS, NERC CIP, ISO, and other standards
- Pathfinder assessment, a fixed-price and objective security snapshot that identifies security and privacy gaps, and the most effective controls

PROTECT SERVICES

- Physical Security, ensuring availability of your organization's resources
- Secure Architecture, allowing successful implementation of virtual, cloud, and other architectures end-to-end across the network
- Vulnerability Management, detecting and mediating vulnerabilities before the hackers do
- Penetration Testing, simulating an attack against the network to find all possible routes of attack
- APT Simulation, replicating the activity of persistent malware to challenge detection and response capabilities
- Application Security, from source code to implementation
- Social Engineering, providing the training employees need to identify and respond to attacks

RESPOND SERVICES

- Incident Response Program Management, ensuring you have the best possible incident response plan, including a full testing regime
- Retained Incident Response, partnering with you to respond effectively to any data incident to reduce costs and liability
- Cyber Incident Response, providing you with the single partner you need when you are experiencing an attack
- Post-Compromise Assessment, assessing your network for signs of attack and compromise to ensure that a breach of your data has not occurred
- Data Forensics, gathers the electronic data required to support criminal, civil, and regulatory litigation and ensure your success under stringent legal requirements

DigitalDefence provides unique hands-on training in penetration testing and data forensics.

Pre-certification courses for the CISSP and CISA are also available. We also provide customized training and on-site mentoring.

Contact info@digitaldefence.ca

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.



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

Disclaimer

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