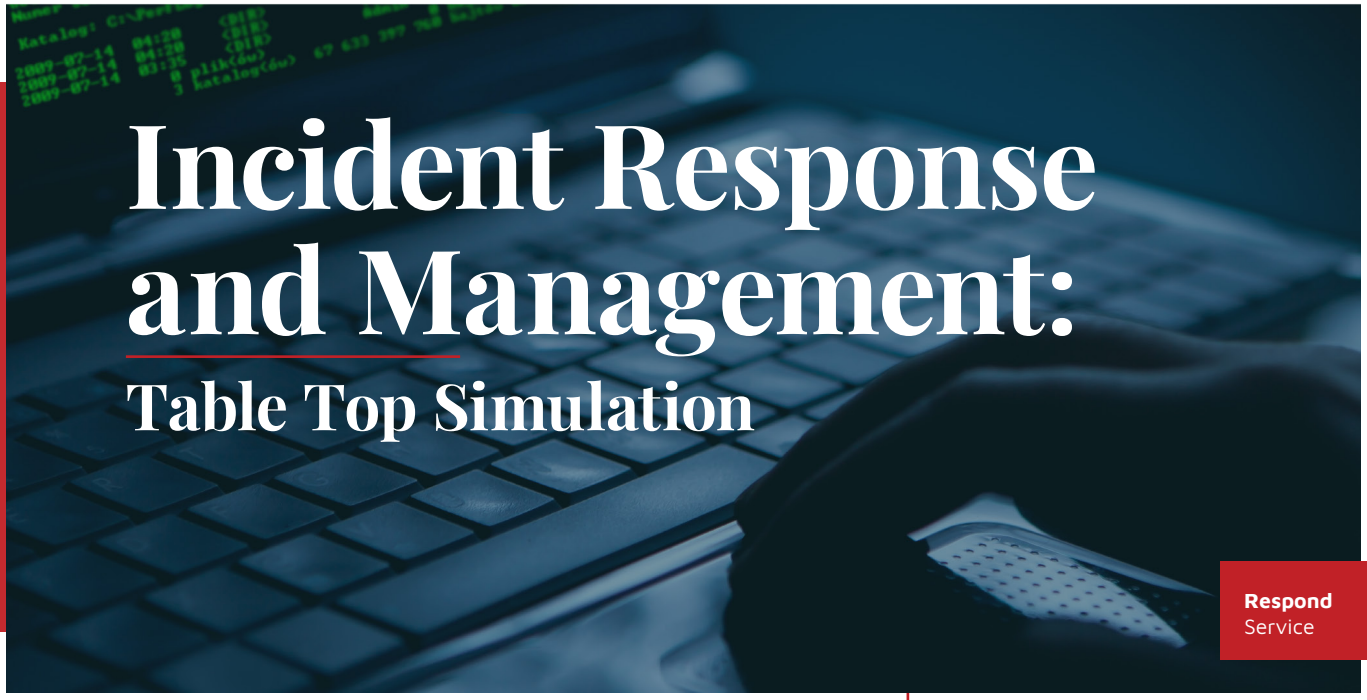
DIGITAL DEFENCE



Incident Response and Management:

Table Top Simulation

Respond
Service

OVERVIEW

All data networks come under attack by motivated hackers or disgruntled insiders; it is inevitable that –sooner or later- a ecurity incident will occur. It is even possible that a breach, releasing confidential data to unauthorized persons, will result.

The goal of Incident Response and Management is to prepare in advance to recognize and respond to a security breach, and to effectively respond to such a breach when it does occur. 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 pioneered 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.

A primary component of the AIM program is realistic training. A fundamental aspect of this training is the Table Top Simulation—an exercise that brings together executives, senior managers, and operators from the business and technical sides of the business. Under the guidance of an experienced security practitioner, the team works together to solve a simulated security breach, developing the skills to effectively respond to an actual breach.

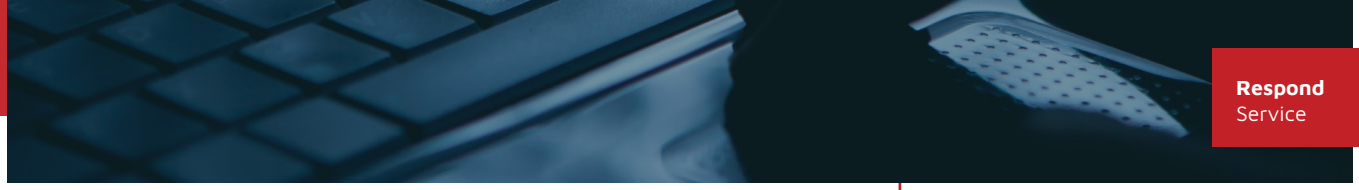
BENEFITS

- Identifies gaps or areas for improvement in existing response methodologies; results are client-specific
- On-site training in client environment ensures realistic scenario delivery and responses according to existing operational plans

Improve corporate risk reduction with strategic security and privacy services.

Is the Incident Response and Management Service—Table Top Simulation right for you?

- Are executives, senior managers, and technical staff prepared to recognize and respond to a security incident?
- Is your incident response team prepared for the speed and complexity of a cyber attack?
- Do you need to comply with a regulatory framework such as ISO27001, PCI DSS, HIPAA, or HITECH?



- Promotes cooperative thinking and Improves both individual and team-based performance in delivering the technical and "soft" skills required for resolution
- Provides real security awareness to executives, senior managers, and operational staff

SERVICE DESCRIPTION

Table top simulations assess a client's ability to respond to a common or client specific threat scenario. Common scenarios include:

- Corporate website is hacked and inflammatory messages are posted publically in association with corporate branded material
- Corporate data is disclosed when a physical device (USB key, laptop) is stolen
- Third party with access to corporate data accidentally releases data
- Automated attack is launched against the organization, usually involving malicious software designed to remain undetected on the network
- Disgruntled internal employee removes corporate data to start a competing firm, or sells data to a competing firm
- External hacker (hacker, business competitor, organized crime, activist group, government-sponsored agency) obtains corporate data; data may or may not be released to public
- Executive is extorted with the threat of release of confidential data
- Client network faces a denial of service attack

These attack scenarios can be delivered individually, or can be combined to reflect a focused attack against an organization.

The client will provide the incident response team for the exercise. The team's composition can be senior executives (CIO, Operations, Lines of Business, HR, legal), managers, or technical staff, or a mix that reflects the goals of the exercise.

A DigitalDefence practitioner, who has experience in network intrusions, incident response and management, and data forensics, will act as the facilitator during the table top exercise. They will run the scenario, and ensure that it is realistic and is aligned with client expectations. Typically, simulations will take 1 to 4 hours to complete.

DigitalDefence will ensure that the scenario is effectively played out during the exercise,. When the exercise has been completed, a post-ex review will examine strengths demonstrated during the response, and identify any areas where improvements could improve the effectiveness and efficiency of an organization's response to a security breach.

Incident Response and Management Training

DigitalDefence provides unique training sessions to ensure your successful resolution of security incidents, including:

- Table-top simulations to walk-though client responses to attack scenarios in a controlled manner
- Scenario-Based Incident Response Training, customized to client requirements
- Incident Response, a 5-day practical course focused on recognizing and responding to security incidents.

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.