DIGITAL DEFENCE

Incident Response and Management:

Program Development

Respond
Service

OVERVIEW

As the number of security incidents and breaches of personal information increases, it has become a virtual certainty that organizations will have to be prepared to respond to these incidents. Unfortunately, developing this incident response capability can be costly and technically difficult.

DigitalDefence can leverage its experience in helping organizations to develop their own Incident Response Program. Once successfully implemented, an organization's incident response can be managed like other business processes.

INCIDENT RESPONSE READINESS ASSESSMENT

DigitalDefence will formally assess your incident response capabilities, evaluating:

- Do you understand the threat environment, and the objectives, methodologies and tools used by attackers?
- Do you have a documented incident response strategy and plan, and do they provide effective guidance? Do management, technical staff, and 3rd parties understand their roles and responsibilities?
- Do technical staff have the tools and training they need to recognize and respond to a security incident? Do the have a document "playbook" of pre-approved and defined responses to common threats and attacks?
- Are you prepared to coordinate with third parties in responding to an incident?
- How will your organization follow-up after the incident to determine the extent of damage, the root cause of the incident, and preventing re-occurrence?
- Are you aware of your legal and regulatory responsibilities in the event that there is a breach of your data, releasing it to the public Internet?

After assessing your capabilities, DigitalDefence will provide you with a roadmap to efficiently migrate across the gaps to the most effective practices.

Improve corporate risk reduction with strategic security and privacy services.

Is the Incident Response and Management Program Development Service right for your company?

- Is incident response in your organization a formal and managed process, or is it ad hoc?
- Is your incident response strategy and supporting practices aligned with your business strategy?
- Do you need to comply with regulations (ISO 27001, PCI DSS, NERC CIP) or fulfill a cyberinsurance requirement to have a comprehensive incident response program?

STRATEGY AND POLICY DEVELOPMENT

An effective incident response requires an organization to have a defined incident management strategy that is aligned with its business strategy and objectives. The strategy must then be made "tactical" – a policy must be created that provides the rules for how incident response will be conducted across an organization. This policy will provide the guidance and constraints for implementing all incident response activities. Finally, organizations should create specific incident "playbooks" that provide pre-approved and auditable records of technical responses to various security incidents.

DigitalDefence can assist a client in creating the strategy, policy, and supporting documents; if these have already been developed, we can provide an objective review to ensure that they meet immediate requirements, and that they will support future operations.

FIRST RESPONDERS WORKSHOP

DigitalDefence has created the "First Responders Workshop" to provide management and technical staff with the knowledge they need to launch an immediate response against a security incident. Material covered during this 2-day workshop includes:

- Introduction to attackers (external, external), and the threat environment
- Review of attacker methodologies, with hands-on demonstrations and practice in implementing the most common attacks
- Recognizing a data security incident
- Planning including resource management, responsibility and authority delegation
- The incident response process, covering development of internal standard operating procedures, the computer security incident response team (CSIRT), notification and escalation processes, internal communications and public relations, reporting, lessons learned
- Responding to common attacks (scenario-based training)
- Supporting the collection of forensic evidence and litigation preparation, including collecting data from a live system
- Relevant laws and regulations, including privacy

The workshop culminates in a Table Top Exercise that allows student to practically apply their knowledge. The workshop can be used as a stand-alone introductory training session, or as an important component of the Retained Incident Response service.

TABLE TOP AND SIMULATION EXERCISES

In incident response, it is critical that you "train as you fight, and fight as you train". Your training must actively engage your incident responders, and they should be placed in realistic scenarios that prepare them for the incidents that they will be facing.

Because many of our consultants have military or law enforcement backgrounds, we have developed a unique industry-leading approach to effective incident response training that is customized to your specific usiness. DigitalDefence can provide the following:

- Table Top Exercises – Structured walk-throughs, guiding key stakeholders in responding to incident response scenarios
- Scenario-Based Training – Once table top exercises have been completed, full scenariobased training is the most effective means of validating that all persons know how to respond to a cyber incident

Customized campaigns meet the specific needs of your organization, and your regulatory and legal environments

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