DIGITAL DEFENCE

Vulnerability Management

Protect
Service

OVERVIEW

The modern data network contains network devices, servers, web applications, databases and other assets that are located on-premise or in a cloud environment. These networks are continually engaged in updating infrastructure and systems, installing new and updated applications, and granting access to users – each one has the potential to introduce new vulnerabilities that could be exploited by attackers. An effective response requires more than the application of patches to vulnerable systems; to secure your network, a vulnerability management program is essential. Vulnerability management refers to the managed and auditable process of:

- Discovering and prioritizing IT assets
- Scanning networks and applications for vulnerabilities
- Generating reports and prioritizing the identified vulnerabilities in the context of your organization's business priorities
- Mediating the priorities, usually by applying vendor-supplied patches and upgrades; and
- Confirming that the relevant mediation steps have been applied with no deleterious impacts on the patched system

DigitalDefence can provides assistance in developing your own vulnerability management program, or provide a managed service to address your network's vulnerabilities.

BENEFITS

- Identify security flaws in your network before they are exploited by known and emerging threats
- Regular consultations with DigitalDefence to discuss current and emerging threats and vulnerability trends; ensures that your network is always current against the latest attacks
- Leverages DigitalDefence security expertise to rapidly and effectively fix vulnerabilities, reducing your risk and reducing

Improve corporate risk reduction with strategic security and privacy services.

Is a Vulnerability Management Service right for your company?

- Have you discovered and inventoried all data resources?
- Are you using threat intelligence data that is tailored to your specific organization and its business and technical requirements
- Are you using the most cost effective approach to finding and fixing vulnerabilities on your network?

management complexity

- Ensures compliance with regulatory requirements, including ISO 27001 NERC CIP, PCI DSS

ON-DEMAND VULNERABILITY SCANNING

Many organizations have employed their own vulnerability scanning program internally; however, the reported success of such programs varies and they frequently do not meet an organization's requirements.

DigitalDefence can review your scanning program to improve its effectiveness by:

- Reviewing the network architecture and the design the vulnerability management program
- Assisting in selection of the optimum vulnerability scanning products
- Providing IT and security staff with mentoring in the use of scanning products and interpretation of the results
- Developing a verifiable mediation program with ongoing tracking, trending, and analysis

DigitalDefence can also provide ad hoc scanning to support particular events (such as regulatory compliance requirements), or deliver managed vulnerability scans at regular intervals against your internal and external networks.

CONTINUOUS VULNERABILITY SCANNING

The hackers never rest – your network is being scanned 24x7 for vulnerabilities that can be exploited. Therefore, your greatest control against an attack -vulnerability scanning- should be continuous as well.

DigitalDefence's Continuous Vulnerability Scanning is available as an internal or external service designed to identify critical changes to your infrastructure or risks posed by new vulnerabilities.

HONEYPOT AND HONEYNET DEPLOYMENT

A honeypot is a computer with no business function – it is designed to be scanned and compromised by an attacker. Its sole purpose is to provide an alert when someone is actively probing a network and seeking vulnerabilities that can be exploited. In effect, it allows you to take advantage of the vulnerability scanning that is being undertaken by an attacker. In many instances, it allows an attacker's malware to be captured and analyzed, providing attack information or even identifying the attacker.

Honeypots can be employed singly, or as a honeynet to provide for a more comprehensive early warning system. DigitalDefence has successfully deployed honeypots in cases that included:

- Capture and reverse-engineering of malware designed to target a specific company
- Identification of malicious insider who was vandalizing databases containing financial information
- Identification of malicious insider who was harassing a fellow employee
- Detection of attacks against SCADA systems

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