DIGITAL DEFENCE

Post-Compromise Assessment

Respond
Service

OVERVIEW

DigitalDefence’s Post-Compromise Assessment service allows organizations to evaluate their networks for signs of an ongoing attack, or one that has occurred in the past. This is particularly relevant at a time when advanced persistent threat are designed to stay hidden on the network, and the average lag time between compromise and discovery is more than 200 days.

The high incidence of undiscovered compromises can be attributed to a variety of factors, including:

- Organizations lack the personnel and available time to search for compromises
- Organizations lack the specific knowledge of the threats that they face – objectives, attack methodologies, and tools used
- Organizations lack specific detection tools and skills
- Organizations lack analysis skills, particularly incident response, malware analysis, and data forensics

DigitalDefence’s Compromise Assessment Service addresses these limitations to ensure you can detect and respond to a compromise of your data.

KEY BENEFITS

- Our consultants have completed hundreds of ethical penetration tests, malware analyses, and incident response investigations; this unique knowledge allows them to rapidly and effectively assess a potential compromise
- Commercial, open-source, and proprietary tools are used where necessary to complement manual testing in an investigation methodology that is customized for your organization. This provides the most effective means to identify a possible compromise

Improve corporate risk reduction with strategic security and privacy services.

Is the Post-Compromise Assessment right for your company?

- Current attack tools and methodologies used by attackers are designed to remain on the network for long periods of time—can you detect these attacks?
- Can you determine the damage that has occurred during an attack, and prevent it from re-occurring?

- An objective third party response by experienced professionals assures key clients, auditors, and management as to your organization’s commitment to security

OUR APPROACH

The DigitalDefence Post-Compromise Assessment combines our advanced knowledge of attacker methodologies and tools with our experience in responding to data security incidents. The following activities will be performed:

- Environmental review – DigitalDefence will review your organization’s network topology, especially the ingress and egress points. Typical network traffic and activities will be baselined
- Conduct endpoint analysis – Using automated tools and manual inspection, DigitalDefence will review the network, data systems, and applications against our library of Indicators of Attack (IOA; present when there is an active attack on-going) and our library of Indicators of Compromise (IOC; present when an attack has been completed).
- We will conduct an advanced search for malware, including ransomware and advanced persistent threats (APTs). Finally, we will examine the network for covert channels permitting connections of your network to unauthorized third parties
- Evidence analysis – DigitalDefence investigators will manually verify to eliminate any false-positive results. At this stage, forensic techniques may be applied, such as bit-level imaging to preserve evidence for study and litigation. Malware may be reverseengineered, especially to verify if it is targeted against the client organization. Advanced log analysis may also be completed.
- Re-Assessment - Once the relevant IOAs and IOCs have been identified and verified, the network environment (wired, wireless, backed-up data) will be re-assessed to ensure that all instances of compromise have been identified
- Targeted remediation – Once the specific threats have been identified, DigitalDefence will recommend immediate steps to eradicate the threat. These recommendations will include controls to prevent a return of the threat
- Presentation of findings – DigitalDefence will provide an executive summary and full documentation of the compromise assessment that has been completed, including major findings, and recommendations to address any remaining risks. If litigation is being pursued, additional documentation may be prepared

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

This document is for informational purposes only. DigitalDefence makes no warranties, express or implied, in this document.