DIGITAL DEFENCE

Incident Response and Management:

1st Responder's Workshop

Respond
Service

DigitalDefence's 3-day workshop for First Responders is a hands-on look at how data security incidents are caused, how to recognize them, and how to resolve them with minimal financial loss and reputational damage

The First Responder in a data security incident plays a pivotal role – they will be the one who first recognizes that an attack is taking place, and will put into place the steps that will stop the attack, minimizing your financial loss and damage to your data.

DigitalDefence's workshop for 1st Responders is a practical look at how incidents are caused, how to recognize them, and how to resolve them. A core component of the program is unique scenario-based training based on real Canadian security incidents.

WHAT YOU WILL LEARN

- How to create an enterprise incident response strategy and plan in advance for a security incident, ensuring organizational readiness
- How to effectively respond to an incident, and avoid common –and costly—mistakes
- Leveraging the most up-to-date investigative techniques and tools (commercial and open source / freeware)
- How to gather the information needed for root-cause analysis and support legal action
- How to manage the response process
- How to satisfy regulatory requirements under HIPAA/HITECHI-SO 27001, PCI DSS, Sarbanes-Oxley, and other frameworks
- Become a DigitalDefence Certified Incident Responder, and will have access to pre-and post-course material , and the tools to stay current in this fast evolving field

Reduce corporate risks with focused incident response training.

Is the 1st Responder's Workshop right for your company?

- Do you need to reduce financial losses due to business downtime?
- Do you need to manage your liability and insurance costs?
- Are you prepared to recognize and respond to a data security breach?
- Should a breach occur, do you know who you have to notify, and when?
- Will your business survive and recover from a network attack?
- Are you meeting your regulatory requirements for incident response?

COURSE OVERVIEW

- The threat and attack methodologies—attackers, methodologies, tools, and types of incidents
- Legal and regulatory requirements— criminal and civil law, regulations, privacy law, mandatory breach reporting, cross-border security and privacy issues
- Agile Incident Management™ - the failure of "classical" incident response methodologies, Agile Incident Management, preparing for an incident, strategic and tactical approaches to incident response
- Documenting strategy to tactics—creating an enterprise incident response policy; creating and documenting standard operating procedures to guide a response; dealing with third parties (legal, law enforcement, cyberinsurance)
- Identifying a cyber incident—what to look for at the scene of the cybercrime, network and host attacks, conducting a rapid triage to determine attack activities and impact, rapid analysis of event logs, identifying Indicators of Attack
- Intelligence and threat handling—proactive versus reactive threat management, commercial and open source threat intelligence, risk assessments and threat modeling, identifying and hunting for Indicators of Compromise
- Recognizing and responding to physical and social engineering attacks—psychology of social engineering attacks, attack methodologies, remote and on-site attacks, effective response, addressing social engineering in policy and security awareness training
- Network and host based attacks—recognizing attacks, effective responses to the most common attack types
- Insider threat—profiles of the insider threat, attack types, responding to the insider, developing an insider threat response strategy
- Rapid malware analysis—types of malware, methodology, creating a safe analysis environment, online analysis tools, static and dynamic analysis, analysis of malicious files (MS Office, PDF), analyzing system memory for malware and attack artifacts
- Acquisition and management of electronic evidence—legal considerations, gathering evidence from live and static systems, documentation for court
- Static data forensics—the forensic process, indexing, file carving, registry analysis, operating system and event logs, email and browser forensics (Windows and Unix-based systems)
- Live system and volatile data analysis—live system triage, RAM acquisition and analysis, extraction and analysis of the registry, key file extraction and analysis (Windows and Unix-based systems)
- Making a jump bag for incident response—Selecting, testing, and validating tools, scripting the incident response

The workshop can be delivered at your site, reducing travel costs, minimizing work disruptions, and creating a private atmosphere to discuss the security of your specific business.

Who Should Attend

This workshops intended for those who need to be proficient at recognizing and responding to data security incidents, and preserving and analyzing evidence (system and network administrators, database administrators, security and privacy specialists).

This course is also pertinent for HR managers and others who conduct internal investigations.

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