TECIS60653

Manage digital forensic examination activities

Overview

Digital forensic examination procedures are used to uncover and interpret electronic data to aid the investigation of information security issues. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events. The context is most often for usage of data in a court of law, though digital forensics can be used in other instances.

This standard defines the competencies required to lead all aspects of digital forensic examination. Including managing resources, activities and deliverables. This includes specifying the policies and processes for undertaking digital forensic examinations to determine the nature of the issue and to identify those responsible, as well as defining and implementing organisational policies and standards concerning digital forensic examination.

Performance criteria

You must be able to:

1. manage digital forensic examiners in the analysis and interpretation of computer data to investigate the root cause of information security issues
2. identify and preserve evidence in its most original form while performing a structured digital forensic investigation
3. review and apply the legislation, strategy, and policies, relating to digital forensic activities
4. develop, implement and maintain procedures, and techniques for undertaking digital forensic examinations
5. make recommendations on which digital forensic techniques and tools are approved for use in digital forensic examinations in line with organisational requirements
6. act as an expert witness to present digital forensic examination findings if required for both organisational and legal proceedings
7. identify and implement appropriate training programmes to maintain the effectiveness of digital forensic examination activities
8. advise, mentor and supervise less experienced members of the digital forensic examination team
9. objectively analyse and clearly present the findings from digital forensic examinations appropriately to sponsors, stakeholders and external bodies

Knowledge and understanding

You need to know and understand:

1. how to select and acquire a range of digital forensic examination tools to examine a wide range of information security issues
2. the range of problems and challenges that may arise during digital forensic examination activities
3. how to identify and select the most appropriate tools and techniques for a particular information security issue
4. how to select digital forensic examiners to manage and take responsibility for specific digital forensic examinations
5. how to establish escalation, communication processes and lines of authority for information security issues
6. how to develop digital forensic examination plans to respond to a wide range of information security issues
7. what are the internal and external factors that may impact on digital forensic examination activities
8. what are the policies, regulations, legislation and external standards that apply to digital forensic examination activities
9. the importance of using lessons learned in order to inform future forensic examination activities
10. the need to maintain an incident log and communicate lessons learned across the digital forensic examination team
11. the need to conduct research to keep up to date with information security threats and new digital forensic tools and techniques
12. the optimum digital forensic approaches for recovering and preserving evidence

TECIS60653

Manage digital forensic examination activities

Developed by	e-skills
Version Number	1
Date Approved	March 2016
Indicative Review Date	April 2019
Validity	Current
Status	Original
Originating Organisation	The Tech Partnership
Original URN	TECIS60653
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, digital forensic analysis