TECIS60643

Carry out 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 conduct a digital forensic examination. It includes mastering analysis of large and complex information systems using tools to acquire and analyse systems, collect and document evidence.

Performance criteria

You must be able to:

1. collect information and preserve evidence as part of a digital forensic examination in line with organisational procedures
2. analyse digital information (including system logs, network traffic, hard disks, virtual memory, etc.) for evidence of breaches of the law and/or the organisational security policy
3. critically analyse software for installed malware products in line with organisational standards
4. examine monitoring systems to identify potential information security breaches in information systems
5. report and escalate suspicious activities related to information security in a timely manner
6. take appropriate action to secure information assets from any potential threats until threats are mitigated
7. seize digital evidence in accordance with legal and organisational guidelines
8. present digital forensics findings to managers, law enforcement organisations, and clients in a clear and understandable manner

Knowledge and understanding

You need to know and understand:

1. the purpose of digital forensic examination and its role in detecting intrusions and inappropriate access to information assets and in preventing future breaches
2. the range of methods, tools and techniques that can be used to conduct digital forensic examinations
3. the legislation and regulation that are relevant to digital forensic examination including for preservation of digital forensic evidence
4. the potential threats that pose the highest risk to the organisation and which are prioritised during digital forensic examination
5. how to access, use and analyse information and data as evidence where appropriate
6. the value and importance of digital forensic examination in identifying and classifying incidents, identifying sourcing and retaining evidence for investigation
7. the importance of using information contained in system logs, network traffic, hard disks, virtual memory as part of digital forensics activity
8. how to prioritise and escalate issues that are identified through digital forensic examination
9. that digital forensics can often requires the analysis of both transient and volatile information
10. the differences between digital forensic examination for law enforcement and within business environments

Carry out 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	TECIS60643
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