TECIS60663

Direct 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 covers the competencies concerned with directing information security incident management, investigation and forensics operations. Including managing resources, activities and deliverables. It includes setting the strategy and policies, and being fully accountable for successful digital forensics operations.

Performance criteria

You must be able to:

1. be fully accountable for digital forensics activities
2. define the strategy, policies and standards for digital forensics
3. lead the digital forensics research efforts in proactively monitoring information sources for evolving trends, security threats and digital forensics best practice
4. translate research findings into digital forensic practice to improve the capability of the digital forensics function
5. direct the resourcing and professional development strategy for digital forensics activities
6. monitor the quality and effectiveness of digital forensics activities, critically reviewing them and making recommendations for improvement where appropriate
7. provide timely and objective advice and guidance to others on all aspects of digital forensics activities including best practice and the application of lessons learned
8. develop and document communication processes for internal and external parties (e.g. media, law enforcement, customers) relating to digital forensics
9. prepare formal reports to senior management on the effectiveness and efficiency of digital forensics in uncovering and interpreting electronic data and preserving evidence
10. provide thought leadership on the discipline of digital forensics, contributing to internal best practice and to externally recognised forums

Knowledge and understanding

You need to know and understand:

1. how to direct the digital forensics function within the organisation
2. the need to advise and guide others on all aspects of digital forensics activities
3. how to organise, train and equip digital forensic teams to undertake digital forensic examinations
4. how lessons learned may be applied to digital forensics activities
5. the importance of research scanning for new information security threats and for new digital forensics tools and techniques
6. sources of best practice in digital forensics activities
7. the need to monitor and continually improve the effectiveness of digital forensics within the organisation
8. the importance of having effective reporting and communications on digital forensics findings to stakeholders within and external to the organisation
9. how to design and develop the strategy, policies, plans and standards for digital forensics
10. the need to ensure that timely and effective review of digital forensics procedures takes place
11. how to objectively analyse the findings from digital forensics activities and report to sponsors and stakeholders

TECIS60663

Direct 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	TECIS60663
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