TECDT61251

Manage digital forensic activities

Overview

This standard is about managing software lifecycle management delivery projects.

This involves establishing and overseeing digital forensic policies, processes and procedures, including all tools and techniques approved for use and the need to operate ethically and professionally.

It includes making strategic technical decisions to support the organisations digital forensics capabilities, and improving the effectiveness through implementing automation as appropriate.

This standard is for those who need to manage digital forensic activities as part of their duties.

Performance criteria

You must be able to:

1.
Set the organisational policies and procedures to define digital forensic processes
2.
Maintain the organisational capability to deliver the required digital forensics services
3. Consult with senior stakeholders to agree budgets, priorities and metrics for delivering digital forensic services
4. Develop approved tools to support digital forensic data acquisition and analysis
5. Identify and implement new tools and techniques to support digital forensic process improvements
6. Lead on digital forensic data-collection, triage and analysis and investigate complex digital forensics cases
7. Manage digital forensic team training needs to maintain high levels of performance
8. Attain and maintain relevant accreditations that validate the organisations digital forensics capabilities
9. Produce and communicate reports of digital forensics metrics and investigation outcomes to appropriate stakeholders
10. Provide expert witness testimony as a digital forensics examiner on behalf of the organisation as required

Knowledge and understanding

You need to know and understand:

1. The relevant cyber security regulations and standards for digital forensics
2. The importance of providing guidance to digital forensic investigators on maintaining the integrity of the evidence and the investigative process
3. Industry best practice of security methodologies and industry standards and benchmarks
4. The industry standard digital forensic tools and techniques and how to apply them
5. That a digital forensic trace is an explicit record of digital evidence that identifies the execution of specific digital activities, communications and/or storage of specific data
6. The importance of maintaining the provenance and authenticity of digital evidence, given the ease with which digital information can be modified
7. That in the initial stages of a digital forensic investigation, it is important to triage potential digital targets to prioritise data sources for analysis
8. The accreditations required to perform the recovery or imaging of electronic data as a provider of digital forensic science services
9. The international standards and certifications that are recognised for verifying the quality and rigour of the processes followed in performing digital forensic examinations
10. That digital forensic techniques are also used to support data protection subject access requests
11. That forensic data acquisition software must reliably produce an unmodified and complete copy of the forensic targets it is designed to handle
12. The typical result of a forensic investigation is a final report and, occasionally may result in a presentation in a courtroom
13. That digital forensic tools primarily provide the means to acquire digital evidence from forensic targets, extract and reconstruct data
14. That identifying and acquiring the relevant forensic targets can be a difficult and lengthy process

15. That the desired outcome of digital forensic data extraction is a bit-level copy of the forensic target, which can then be analysed using knowledge of the structure and semantics of the data content
16. That some data can be fake and generated using anti-forensics tools in order to confuse investigation
17.
That forensic tool validation is a scientific process that subjects specific tools to systematic testing in order to establish the validity of the results produced
18.
The ethical considerations that need to be applied when conducting digital forensic investigations on personal data

TECDT61251

Manage digital forensic activities

Developed by	e-skills
Version Number	1
Date Approved	30 Mar 2022
Indicative Review Date	30 Mar 2025
Validity	Current
Status	Original
Originating Organisation	ODAG Consultants Ltd.
Original URN	TECDT61251
Relevant Occupations	Information and Communication Technology Professionals
Suite	IT and Telecoms Professional (procom)
Keywords	cyber security, digital forensics