SEMETS372

Performing computer system security assessments for engineering software

Overview

This standard identifies the competences you need to perform a computer system security assessment, in accordance with approved procedures. You will be given a detailed brief, and will be required to assess these requirements and to extract all necessary information in order to carry out the security assessment. You will need to select the appropriate computer systems security assessment methods to use, based on the type of computer application. You will be expected to use current British, European, international and company standards where appropriate.

Your responsibilities will require you to comply with organisational policy and procedures for computer and information security. You will be required to report any problems with the computer hardware, software, security or procedures that you cannot personally resolve, or that are outside your permitted authority, to the relevant people. You will be expected to work to verbal/written instructions and draft specifications, with a minimum of supervision, taking personal responsibility for your own actions and for the quality and accuracy of the work that you carry out.

Your underpinning knowledge will provide a good understanding of your work and will provide an informed approach to applying computer security assessment procedures. You will understand the computer system and software used, and its application, and will know about the various tools and techniques used to assess whether the computer integrity is sufficient for its intended role within a defined operational environment.

You will understand the safety precautions required when performing the security assessment. You will be required to demonstrate safe and secure working practices throughout and will understand the responsibility you owe to yourself and others in the workplace.

Performance criteria

You must be able to:

1. work safely at all times, complying with health and safety legislation, regulations, directives and other relevant guidelines
2. plan and prepare the computer system security assessment activities before you start them
3. use appropriate analysis tools to obtain the required information for the analysis activity
4. use references that follow the required conventions
5. determine the evidence required to achieve the necessary level of computer and information security
6. perform the computer security assessment
7. review the output from the security assessment
8. report your findings on the assessment performed
9. save and store the computer security assessment results as the appropriate file type and in the correct location
10. deal promptly and effectively with problems within your control, and seek help and guidance from the relevant people if you have problems that you cannot resolve

Knowledge and understanding

You need to know and understand:

1. the specific safety precautions to be taken when working with software development environment hardware (to include such items as safety guidance relating to the use of visual display unit (VDU) equipment and workstation environment; repetitive strain injury (RSI); the dangers of trailing leads and cables; how to spot faulty or dangerous electrical leads, plugs and connections)
2. how to return the work area to a safe and useable condition (such as cleaning down work surfaces; putting media, manuals and unwanted items of equipment into safe storage; leaving the work area in a safe and tidy condition)
3. the documentation required for the computer system security analysis (such as scanner analysis reports, base level security reports, relevant log extracts and other analysis reports)
4. computer system security analysis tools, and national, international and relevant company security policies, procedures, methods and tools
5. identification of the correct version of software tool, and the various techniques that are supported by the tool
6. how to use and configure the computer security analysis tools
7. how to recognise specific security vulnerabilities (such as denial of service, attacks)
8. how to access the specific security and vulnerability results
9. how to access, recognise and use a wide range of standard vulnerability libraries from the tools
10. the need for configuration control on all components (such as ensuring that completed results are verified, labelled and stored on a suitable storage device)
11. why it is necessary to be able to recall previous issues of analysis results
12. when to act on your own initiative and when to seek help and advice from others

Scope/range

1. Prepare for the computer system security assessment, by carrying out all of the following:
    1. check that the working environment is in a safe and suitable condition and that all working equipment is in a safe, tested and usable condition (such as cables undamaged, correctly connected, safely routed)
    2. identify all potential vulnerabilities which the computer system may have
    3. identify the severity of each vulnerability (such as catastrophic, severe, minor, negligible)
    4. identify the computer's worst-case contribution to the vulnerability (such as direct cause, cause in conjunction with other failure, one of several independent contributors, no contribution)
    5. identify the required standards and all relevant sources (such as customer (contractual) standards and requirements, recognised compliance agency/body's standards, corporate information security policy, industry best practice in secure computer operation)
2. Review four of the following to obtain sources of data to assess correctly the computer system security:
    1. computer network connectivity configuration
    2. computer system malware scan
    3. computer software version numbers and applied updates
    4. computer system vulnerability sweep
    5. computer service start-up configuration
    6. computer system usage logs
    7. computer peripheral connections
    8. standards reference documents
3. Carry out all of the following before performing the computer system security assessment:
    1. ensure that the data and information you have is current, complete and under configuration control
    2. confirm that the system level security identification and analysis have been performed
    3. recognise and deal with problems (such as technical issues and lack of information, or incorrect information)
4. Perform the computer system security assessment, using four of the following:
    1. security analyser (such as base level security analyser)
    2. installed virus scanner
    3. malware and spyware scanning results
    4. computer usage logs
    5. server and gateway access logs

6. record of connected devices (such as USB devices)
7. system vulnerability scanning tool
8. standards reference documents

5. Review and report on a sample of the security related evidence for all of the following:
    1. completeness
    2. traceability
    3. accuracy
    4. adequacy
6. Save and store the results in appropriate locations, to include carrying out all of the following:
    1. check that the results are correctly titled, referenced and annotated
    2. ensure that the results have been checked and that they comply with the organisation procedure
    3. save the results to an appropriate location (such as storage device, configuration database)
    4. ensure that a separate backup copy is created and placed in safe storage

SEMETS372

Performing computer system security assessments for engineering software

Developed by	Enginuity
Version Number	3
Date Approved	30 Mar 2021
Indicative Review Date	01 Mar 2024
Validity	Current
Status	Original
Originating Organisation	Enginuity
Original URN	SEMETS372
Relevant Occupations	Engineering, Engineering and Manufacturing Technologies, Engineering Technicians
Suite	Engineering Technical Support Suite 3, Advanced Manufacturing
Keywords	engineering; technical; support; security analyser; installed virus scanner; malware and spyware scanning results; computer usage logs; server and gateway access logs; system vulnerability scanning tool