TECIS60552

Manage information security vulnerability assessments

Overview

Vulnerabilities provide potential entry points through which a network or application, (typically a web site) can have its functionality or data damaged, downloaded, or manipulated. A typical Web site may have many potential vulnerabilities. Malware (malicious software or code) can be installed by hackers by exploiting security weaknesses to gain access to website and install malicious code.

Vulnerability analysis, also known as vulnerability assessment, is a process that defines, identifies, and classifies the security holes (vulnerabilities) in network or communications infrastructure and in information systems applications. In addition, vulnerability analysis can forecast the effectiveness of proposed information security countermeasures and evaluate their actual effectiveness after they are put into use. Vulnerability assessment seeks to identify both instances of malware on systems as well as system and network-level vulnerabilities.

This standard defines the competencies required to manage vulnerability assessment activities. Including managing resources activities and deliverables. This includes defining and implementing organisational policies, standards and processes.

Performance criteria

You must be able to:

1. develop, implement and maintain the policies, plans, processes, procedures, methods, tools and techniques for vulnerability assessment activities and their deliverables
2. clearly and accurately define the scope of vulnerability assessments, adjusting the process to suit specific contexts
3. select and apply the most appropriate methods and tools to be used during vulnerability assessments in line with organisational requirements
4. set and maintain the resourcing and training plan for the vulnerability assessment team in line with organisational requirements
5. design, implement and report metrics for the effectiveness of information system vulnerability assessment activities
6. critically review the results of vulnerability assessments, identifying priorities for action
7. validate new potential vulnerabilities that may impact on the organisation's information assets
8. monitor the quality and effectiveness of vulnerability assessment activities, critically reviewing the vulnerability assessment processes and making recommendations for improvement where appropriate
9. advise and guide others on all aspects of vulnerability assessment activities and their deliverables
10. effectively communicate vulnerability assessment status and results to a wide range of sponsors, stakeholders and other individuals

Knowledge and understanding

You need to know and understand:

1. how to develop the policies and procedures required for effective vulnerability assessment activities
2. how to scope vulnerability assessments
3. the need to ensure that vulnerability assessments are performed on an ongoing basis
4. how to develop and implement effective vulnerability countermeasures
5. where to source information on the latest identified threats and vulnerabilities
6. the organisational, external standards, best practice frameworks and codes of conduct that vulnerability assessment should comply with
7. how to engage proactively with stakeholders to ensure that mitigation for vulnerabilities are understood and implemented in a timely manner
8. how to maintain lists of authorised or banned applications or devices for use on protective monitoring systems (white / black listing)
9. the need to critically review the results of vulnerability assessments, identifying priorities for action where appropriate
10. the detailed application of vulnerability assessment processes used to objectively determine which security controls are most appropriate
11. how to analyse information security vulnerability bulletins for their potential impact on information systems and undertake or recommends appropriate action
12. the importance of monitoring the quality and effectiveness of vulnerability assessment activities
13. how to identify and implement improvements to the vulnerability assessment processes and procedures

TECIS60552

Manage information security vulnerability assessments

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	TECIS60552
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, vulnerability assessment