Australian Government

Assessment Requirements for ICTCYS609 Evaluate threats and vulnerabilities of IoT devices

Release: 1

Assessment Requirements for ICTCYS609 Evaluate threats and vulnerabilities of IoT devices

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

Performance Evidence

The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to:

- research and analyse an organisation's internal and external operating culture, systems and networks to evaluate threats and vulnerabilities of IoT devices and interpret findings from at least three different IoT devices.

In the course of the above, the candidate must:

- document processes and outcomes.

Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including knowledge of:

- security risks and vulnerabilities in software systems
- security risks and vulnerabilities of IoT devices
- tools used in testing a network for vulnerabilities of IoT devices
- tools used in testing a network for threats and vulnerabilities
- penetration testing methodologies required to evaluate threats and vulnerabilities of IoT devices
- risk mitigation strategies
- organisational procedures applicable to running vulnerability and threat assessments for IoT devices, including:
  - establishing goals and objectives of vulnerability assessments
  - defining scope of testing and establishment of testing regime
  - documenting established requirements
  - establishing penetration testing procedures
  - documenting findings, threats and work performed

- key organisational environments, systems and networks required to evaluate threats and vulnerabilities of IoT devices.

Assessment Conditions

Skills in this unit must be demonstrated in a workplace or simulated environment where the conditions are typical of those in a working environment in this industry.

This includes access to:

- required hardware, software and IoT devices required to evaluate threats and vulnerabilities
- required analytic platform and applicable user instructions
- data recognition software required to evaluate threats and vulnerabilities
- organisational policies and procedures applicable to gathering, analysing and interpreting threat data.

Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

Links

Companion Volume Implementation Guide is found on VETNet - https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2