



Australian Government

ICTCYS609 Evaluate threats and vulnerabilities of IoT devices

Release: 1

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.

Application

This unit describes the skills and knowledge required to gather Internet of Things (IoT) devices and data from various sources and evaluate and identify threats and vulnerabilities.

It applies to those who work as IoT developers or cyber security and risk analysts and are responsible for cyber security activities including the evaluating IoT devices for threats and vulnerabilities.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Unit Sector

Cyber security

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
1. Develop evaluation strategy	1.1 Research and determine an organisation's requirements for evaluation of IoT devices 1.2 Research organisational operations, environment and culture and determine perceived threats and vulnerabilities 1.3 Develop and document evaluation strategy according to organisational requirements, policies and procedures 1.4 Submit evaluation strategy to required personnel and seek and respond to feedback
2. Prepare to value IoT devices	2.1 Prepare devices for evaluation according to technical specifications 2.2 Secure data and networks according to technical specifications

3. Conduct evaluation	3.1 Run evaluation according to documented strategy and organisational policies and procedures 3.2 Confirm and document identified vulnerabilities and threats according to organisational policies and procedures 3.3 Document evaluation results according to organisational guidelines and requirements
4. Interpret and finalise findings	4.1 Analyse evaluation findings and determine completeness and accuracy 4.2 Categorise negative findings into threats and vulnerability and determine level of potential impact to operational activities 4.3 Develop and document recommendations to remediate threat potential and lessen vulnerabilities 4.4 Document finalised results and recommendations according to organisational requirements 4.5 Lodge documentation according to organisational policies and procedures

Foundation Skills

This section describes those language, literacy, numeracy and employment skills that are essential to performance but not explicit in the performance criteria.

SKILL	DESCRIPTION
Numeracy	• Uses mathematical formulae to determine requirements for evaluating quantitative findings
Reading	• Identifies technical, manufacturer and organisational from documentation to determine and confirm job requirements
Writing	• Prepares complex workplace documentation detailing processes and outcomes using required structure, layout and required language
Planning and organising	• Develops the operational detail in stages, regularly reviewing priorities and performance during assessment procedure, and identifies and addresses issues of non-compliance
Problem solving	• Identifies context to recognise anomalies and subtle deviations to normal expectations, focusing attention and remedying problems as they arise
Self-management	• Takes full responsibility for identifying and considering organisational protocols and requirements
Technology	• Identifies principles, concepts, language and practices associated with the digital and cyber world

Unit Mapping Information

No equivalent unit. New unit.

Links

Companion Volume Implementation Guide is found on VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>

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>