Australian Government

Assessment Requirements for ICTCYS407 Gather, analyse and interpret threat data

Release: 1

Assessment Requirements for ICTCYS407 Gather, analyse and interpret threat data

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:

- gather, log and create dataset from a single security device or whole organisation device, including:
  - basic router info
  - firewall info
  - systems
- identify and describe at least three different inconsistencies or discrepancies within data
- document finding, recommendations and outcomes.

In the course of the above, the candidate must:

- interpret meaning from dataset and suggest action items.

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:

- data recognition software tools
- data sources, including:
  - firewalls
  - intrusion detection systems (IDS)
  - access control systems
  - security and event management systems (SIEM)
- basic troubleshooting processes related to cyber security threats
- network and cyber security features and principals
- types of attacks, including:
  - denial-of-service attack (DDOS)

  - SQL injection (SQLi)
  - cross-site scripting (XSS) attacks
  - scripted attacks
  - hardware attacks
  - attacks against Wi Fi
- legislative requirements applicable to gathering, analysing and interpreting threat data
- common cyber security threats and their impacts on business functions
- organisational policies and procedures applicable to gathering, analysing and interpreting threat data, including:
  - documentation established requirements, findings and recommendations
  - establishing security equipment and data sources
  - information collection processes
  - processes in obtaining and analysing results.

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 digital devices
- required analytic platform and applicable user instructions
- data recognition software
- single security device and whole organisation device
- legislative requirements and 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