



Australian Government

Assessment Requirements for ICTCLD510 Manage cloud threat detection systems

Release: 1

Assessment Requirements for ICTCLD510 Manage cloud threat detection systems

Modification History

Release	Comments
Release 1	This version first released with the Information and Communications Technology Training Package Version 8.0. Newly created unit of competency to address in-demand skills needs.

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:

- implement at least one configuration management service to enforce organisational security controls on resources created in cloud environments
- configure at least one intrusion detection system (IDS) that monitors cloud-based resources for unexpected or unwanted behaviour and changes
- centralise collection and analysis of logs from at least one cloud service, at least one network, at least one operating system and at least one application.

In the course of the above, the candidate must:

- use cloud management console, cloud software development kits and command line tools
- collect and analyse data and adjust processes as required
- produce repeatable and automated system deployments
- disseminate important information and its severity
- test log analytics by generating an event, and triggering a rule and a metric
- rectify issues according to organisational policies and procedures
- apply legislative requirements; governance, risk and compliance (GRC) measures; and organisational policies and procedures.

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:

- common threats in cloud-based organisations
- methods for collecting, analysing and extracting meaningful findings from logs from industry-recognised sources

- common procedures for presenting metrics in dashboards and reports based on log findings
- common methods to generate automated alarms based on metrics from log findings
- functions and features of cloud-based:
 - configuration management services
 - IDS
 - security information and event management (SIEM) tools
- tools for vulnerability scanning cloud-based resources
- methods for integrating third-party threat detection tools and sensors in a cloud environment
- functions and features of GRC measures
- organisational policies and procedures, and legislative requirements relating to work tasks.

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:

- cloud-based systems that may be monitored for threats
- required software and hardware to configure cloud threat detection systems
- opportunities for interaction with others
- work brief, security strategy, and organisational policies and procedures required to demonstrate the performance evidence.

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>