Australian Government

ICTCLD512 Respond to cloud security incidents

Release: 1

ICTCLD512 Respond to cloud security incidents

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.

Application

This unit describes the skills and knowledge required to respond to a range of security incidents in cloud-based environments. It includes defining response objectives and simulating security incidents.

The unit applies to individuals who may work in roles such as security engineers, cloud developers and architects, and information security officers. It also includes individuals responsible for managing operational concerns, including automation and maintaining cloud resources.

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

Unit Sector

Cloud computing

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
Elements describe the essential outcomes.	*Performance criteria describe the performance needed to demonstrate achievement of the element.*

ELEMENT	PERFORMANCE CRITERIA
1. Prepare to respond to cloud security incident	1.1 Confirm work brief, risk framework and work tasks according to organisational policies and procedures 1.2 Identify organisational IT assets, host and network security, and related risk assessments 1.3 Identify domains exposed to potential security incident according to work brief 1.4 Confirm attack vector and impact of incident in consultation with required personnel 1.5 Create cloud incident plan according to work brief
2. Detect and analyse cloud security incident	2.1 Simulate security incident according to work brief 2.2 Confirm incident detection by monitoring systems 2.3 Record security incident information according to organisational policies and procedures 2.4 Review cloud incident findings according to organisational policies and procedures 2.5 Implement log capture and replication of relevant data to secure repository with appropriate retention policy 2.6 Determine functional impact, information impact and recoverability from incident 2.7 Notify required organisational personnel of incident
3. Contain, eradicate and recover from cloud security incident	3.1 Implement containment strategy to minimise impact according to cloud incident plan 3.2 Identify and document source and method of attack 3.3 Implement plan to eradicate security threat 3.4 Confirm recovery plan, impact to services and loss of data with required personnel 3.5 Implement recovery plan for resources and data 3.6 Build automated mechanisms for programmed cloud incident triage and response
4. Complete post-incident activities	4.1 Conduct review of incident with required personnel 4.2 Identify and document opportunities for improving automated detection, containment, eradication and/or recovery for security incident 4.3 Update cloud incident response document and store in required location according to organisational policies and procedures 4.4 Recommend updates to organisational policies and procedures to reflect best practice cloud incident response methods 4.5 Present recommendations for improving organisational policies and procedures to required personnel

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
Reading	• Organises, evaluates and critiques ideas and information from a range of complex texts
Writing	• Prepares technical documentation detailing analysis, work performed and results using succinct language and logical structure
Planning and organising	• Identifies key factors that impact on decisions and their outcomes, drawing on experience, competing priorities, and decision-making strategies • Plans strategic priorities and outcomes in a flexible, efficient and effective context and diverse environment exposed to competing demands
Self-management	• Develops and implements strategies that confirm that organisational policies and procedures and regulatory requirements are being met
Technology	• Demonstrates skills that reflect sophisticated knowledge of principles, concepts, language and practices associated with cloud computing and cloud-based threats

Unit Mapping Information

No equivalent unit. Newly created unit.

Links

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