Australian Government

ICTCLD510 Manage cloud threat detection systems

Release: 1

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.

Application

This unit describes the skills and knowledge required to configure, detect and investigate unexpected or unwanted behaviour and changes in cloud-based systems that may threaten organisational security.

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 across cloud environments.

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.*
1. Organise data sources and data collection methods	1.1 Confirm work brief and tasks according to organisational policies and procedures 1.2 Confirm organisational security strategies and cloud security requirements 1.3 Identify and review existing cloud security strategies 1.4 Identify and analyse data sources with highest value and cost-benefit ratios 1.5 Select required data collection methods according to analysis findings

© Commonwealth of Australia, 2024 Future Skills Organisation

ELEMENT	PERFORMANCE CRITERIA
	1.6 Document selected methods and findings according to organisational policies and procedures
2. Set up resource configuration policies	2.1 Identify organisational resource configuration policies 2.2 Enable resource configuration monitoring and implement organisational policies 2.3 Enable resources out of compliance and confirm resources are identified 2.4 Reconfigure resources to meet organisational policies and confirm compliance 2.5 Document configuration according to organisational policies and procedures
3. Set up intrusion detection controls	3.1 Identify cloud-based intrusion detection system (IDS) 3.2 Deploy security sensors if required by IDS and monitor organisational resources 3.3 Enable IDS and configure controls as defined in work brief 3.4 Generate activity and test IDS according to work brief 3.5 Confirm that activity is detected by IDS 3.6 Document configuration according to organisational policies and procedures
4. Centralise security logs and configure analytics	4.1 Identify logs sources that may include security-related activity as specified in work brief 4.2 Configure centralised collection of logs and identify latest updates 4.3 Review log formats and define patterns to match and extract relevant metrics as per work brief 4.4 Test log analytics according to work brief 4.5 Analyse event management, alerting processes, dashboards, graphs and tables specified in work brief 4.6 Configure required event management, and analysis and alerting processes according to work brief 4.7 Confirm functionality of event management, and analysis and alerting processes
5. Configure monitoring dashboard	5.1 Identify cloud-based dashboard service 5.2 Identify relevant metrics and alerts from resource configuration, intrusion detection and log analysis tools 5.3 Configure dashboard and display metrics in required formats 5.4 Share dashboard with required personnel and collect feedback according to organisational policies and procedures

© Commonwealth of Australia, 2024 Future Skills Organisation

ELEMENT	PERFORMANCE CRITERIA
	5.5 Update and improve dashboard based on feedback, where required 5.6 Document configuration according to organisational policies and procedures
6. Configure alerts for security events	6.1 Identify required personnel and alert method according to work brief 6.2 Implement alarm for resource configurations and confirm alert is received for a misconfigured cloud resource 6.3 Implement alarm for IDS and confirm alert is received for a relevant event in cloud environment 6.4 Implement alarm for log metrics that reach a threshold defined in work brief, and confirm alert is received 6.5 Rectify any issues encountered in implementing and testing alerts 6.6 Document configuration 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	• Analyses and synthesises highly embedded mathematical information in a broad range of tasks and texts
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
Self-management	• Develops and implements strategies that confirm that organisational policies and procedures are being met
Technology	• Demonstrates skills that reflect sophisticated knowledge of principles, concepts, language and practices associated with cloud computing and cloud-based threats

© Commonwealth of Australia, 2024 Future Skills Organisation

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

© Commonwealth of Australia, 2024 Future Skills Organisation