Australian Government

ICTCYS407 Gather, analyse and interpret threat data

Release: 1

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.

Application

This unit describes the skills and knowledge required to gather data from various sources, analyse, and interpret information for threats, inconsistencies and discrepancies.

It applies to individuals who work in information technology security, including network and security specialists, and gather logs from devices, check abnormalities and respond accordingly. These individuals are responsible for supporting and preventing cyber threats attacking data in all business functions and in any industry context.

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
Elements describe the essential outcomes.	*Performance criteria describe the performance needed to demonstrate achievement of the element.*
1. Gather threat data	1.1 Identify legislative requirements and organisational policies and procedures to gather, analyse and interpret threat data 1.2 Identify security equipment on network and data sources 1.3 Discuss and confirm data log requirements and strategy to process data with required personnel 1.4 Collect information from alerts, logs and reported events and create a dataset according to organisational policies and procedures
2. Analyse threat data	2.1 Ingest data logs into analytic platform according to user instructions 2.2 Obtain and analyse results for reliability and consistency

ELEMENT	PERFORMANCE CRITERIA
	2.3 Check for false positives and false negative results 2.4 Detect and describe discrepancies and inconsistencies in data
3. Interpret and finalise threat data	3.1 Discuss and review threat data and results with required personnel 3.2 Discuss and assess identified threats, risks and their likelihood of occurrence and impacts of risks, 3.3 Suggest and confirm lessons learnt, action steps, recommendations and mitigation strategies with required personnel 3.4 Document results, findings and recommendations into report according to organisational procedures 3.5 Distribute documentation to required personnel and store 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
Learning	• Identifies and gathers information applicable to organisational procedures and threat data
Numeracy	• Uses tools when measuring and recording data, and interprets results through mathematical data
Reading	• Interprets information from different sources in a range of formats when identifying threat data
Writing	• Prepares complex workplace documentation detailing research findings and recommendations using required structure, layout and technical language
Planning and organising	• Uses problem solving skills when interpreting the nature and impact of threat data
Technology	• Uses required technological tools and software in gathering, analysing and interpreting threat data

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