ICTCYS407

Gather, analyse and interpret threat data

Assessment 1 of 5

Short Answer Questions

Assessor Guide

SWINBURNE OPEN ED

Version 1

Assessment Instructions

Task Overview

This assessment task includes seven (7) short answer questions. Read each question carefully before typing your response in the space provided.

Important: Before commencing your work, you must update your *Student name* and *Student number* in the footer from **page 2** onwards.

Additional Resources and Supporting Documents

ICTCYS407_01_SAQ_Supporting documents (compressed/zipped folder) - This folder contains the following supporting documents required for completing the tasks in this assessment.

- 01_Guide-to-data-analytics-and-the-Australian-privacy-principles.pdf
- 02_NIST-Cybersecurity-Framework-Policy-Template-Guide.pdf
- 03_ISM - Cyber Security Principles (September 2023).pdf
- 04_Essential Eight Maturity Model (November 2022).pdf

Assessment Information

Submission

You are entitled to three (3) attempts to complete this assessment satisfactorily. Incomplete assessments will not be marked and will count as one of your three attempts.

All questions must be responded to correctly to be assessed as satisfactory for this assessment.

Answers must be typed into the space provided and submitted electronically via the Learning Platform. Hand-written assessments will not be accepted unless previously arranged with your assessor.

Reasonable adjustment

Students may request a reasonable adjustment for assessment tasks.

Reasonable adjustment usually involves varying:

- the processes for conducting the assessment (e.g. allowing additional time)
- the evidence gathering techniques (e.g. oral rather than written questioning, use of a scribe, modifications to equipment)

However, the evidence collected must allow the student to demonstrate all requirements of the unit.

Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

Read the following information and answer 'Question 1'.

Refer to the legislative requirements outlined in the 'Guide to Data Analytics and the Australian Privacy Principles (APPs)' by accessing:

- the online version from the Office of the Australian Information Commissioner's (OAIC's) official website at https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/guide-to-data-analytics-and-the-australian-privacy-principles

Or

- the PDF version at https://www.oaic.gov.au/privacy/guidance-and-advice?a=3086

Note: A copy of this PDF version is provided to you as an additional resource.

Question 1

Identify three (3) Australian Privacy Principles (APPs) that relate to gathering, analysing and interpreting threat data and outline the obligations of each.

Use 'Table 1' to record your answer.

(Word count: 25 - 45 words for each APP)

Assessor instructions: Students must list three (3) APPs in the answer table by correctly interpreting information from the sources provided. The descriptions provided under the column 'Obligations as it relates to gathering, analysing and interpreting threat data' are likely to include different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

Table 1 – Question 1: Answer table

#	**Australian Privacy Principle** *(Legislative requirements)*	**Obligations as it relates to gathering, analysing and interpreting threat data** *(25– 45 words)*
1	APP 3 – Collection of personal information	Organisations should be mindful to only: collect information by lawful and fair means collect sensitive information with the individual's consent (unless an exception applies).
2	APP5 – Notification	Organisations should be careful not to use personal information for a purpose other than the primary purpose it was collected for unless an exception applies.
3	APP 11 – Security of personal information	Organisations should actively take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. When personal information is no longer needed it should be destroyed or de-identified.
	Other answers include: APP10 – Quality of personal information	Organisations should take responsible steps to ensure that personal information: • collected is accurate, up-to-date and complete

#	**Australian Privacy Principle** *(Legislative requirements)*	**Obligations as it relates to gathering, analysing and interpreting threat data** *(25– 45 words)*
		• used or disclosed is having regard to the purpose of the use or disclosure is accurate, up-to-date, complete and relevant.
	APP6 – Using and disclosing personal information	Organisations should carefully consider whether the uses and disclosures of personal information for data analytics activities are compatible with the original purpose of collection (particularly when the information is collected directly from a third party).
	APP8 – Quality of personal information	Organisations should take rigorous steps to ensure the personal information collected via creation is accurate, complete and up-to-date by checking that third parties from which personal information is collected, have implemented appropriate practices, procedures and systems to ensure the quality of personal information.

Read the following information and answer 'Question 2'.

Refer to the industry-standard security policy templates and guide by accessing

- the SANS Institute official website at https://www.sans.org/information-security-policy/
- the 'NIST Cybersecurity Framework', 'Policy Template Guide' at https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/files/uploads/2021/11/NIST-Cybersecurity-Framework-Policy-Template-Guide-v21110nline.pdf

Note: A copy of this PDF document is provided as an additional resource.

Question 2

Identify organisational policies and procedures for each of the following tasks that relate to gathering, analysing and interpreting threat data.

Use 'Table 2' to record your answer. You must:

- indicate the name of a relevant policy document in the 'Policy name' column.
- describe how the policy and procedure relate to the specific task in the 'Policy and procedure description' column. (Word count: 75-100 words per task)

Assessor instructions: Students must identify and list an appropriate policy document name from SANS Institute's and/or NIST's list of policy templates and provide a description of how the policy and procedures relate to the given criteria.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

Table 2 - Question 2: Answer table

Task	Policy Name	Policy and procedure description *(75-100 words)*
A. Document established requirements, findings and recommendations	Security Assessment and Authorisation Policy	This policy defines the requirements for documenting the results of security assessments, including assessing the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements. It outlines the format for documenting findings, their severity, and recommendations (i.e. plan of action and milestones) for mitigating identified threats.
B. Establish security equipment requirements	Workstation Security (For HIPAA) Policy Other policies that students may choose to describe include: • Removable Media Policy • Router and Switch Security Policy • Acceptable Use Policy	This policy provides guidance for workstation security to ensure the confidentiality, integrity and availability of sensitive information (including protected health information – PHI) on the workstation and information the workstation may have access to is restricted to authorised users. It additionally provides guidelines to ensure that requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.
C. Established data sources	Information logging standard Other policies that students may choose to describe include: • Employee Internet Use Monitoring and Filtering Policy	Defines the specific requirements for information systems to generate appropriate audit logs that integrate with an enterprise's log management function. It identifies specific requirements that information systems must meet in order to generate appropriate audit logs and integrate them with an enterprise's log management function. This document details what information/elements should be included in the logs generated, the format of the logs and where the logs should be stored.
D. Information collection processes	Information Classification Standard Other policies that students may choose to describe include: • Cyber Security Incident Management Log • Information Security Policy • Access Control Policies	This standard outlines a classification process and provides procedures for classifying information in a manner that uniformly protects information or threat data collected. This helps identify which threat information is considered sensitive and valuable to the organisation. For example, information related to vulnerabilities, exploits, or indicators of

Task	Policy Name	Policy and procedure description *(75-100 words)*
	• Access review policy procedure	compromise (IoCs) may be classified as highly sensitive. This categorisation guides the collection and prioritisation of threat data.
E. Processes in obtaining and analysing results.	Data breach response policy Other policies that students may choose to describe include: • Risk Assessment Policy • Computer Security Threat Response Policy • Incident Response Policy	The Data breach response policy outlines the goals and the vision for the breach response process. This policy defines to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritisation of the incidents), as well as reporting, remediation, and feedback mechanisms.

Read the following information and answer 'Question 3'.

Refer to the cyber security principles *Australian Signals Directorate* by accessing:

- the cyber.gov.au official website at https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-principles
- the Information Security Manual (ISM), PDF document (Long URL: https://www.cyber.gov.au/sites/default/files/2023-09/02.%20ISM%20-%20Cyber%20Security%20Principles%20%28September%202023%29.pdf)

Note: A copy of this PDF version is provided to you as an additional resource.

Question 3

Outline the purpose of cyber security principles according to the *Information Security Manual (ISM),* and provide two(2) examples of principles relevant to gathering, analysing and interpreting threat data.

(Word count: 65-90 words)

Assessor instructions: Students must outline cyber security principles by correctly interpreting the information from the sources provided.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

The purpose of the cyber security principles is to provide strategic guidance on how organisational can protect their systems and data from cyber threats. These principles are grouped into four categories: govern, protect, detect and respond.

The following 'Detect' principles are relevant to gathering, analysing and interpreting threat data.

- D1: Event logs are collected and analysed in a timely manner to detect cyber security events.
- D2: Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents.

Read the following information and answer 'Question 4'.

Refer to the *Australian Signals Directorate* by accessing:

- the cyber.gov.au official website at https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- the 'Essential Eight Maturity Model' PDF document (Long URL: https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Essential%20Eight%20Maturity%20Model%20%28November%202022%29.pdf)

Note: A copy of this PDF version is provided to you as an additional resource.

Question 4

Outline five (5) cybersecurity features relevant to gathering, analysing and interpreting threat data according to the 'Essential Eight Maturity Model' when implementing 'Maturity Level Three'.

(Word count: 65-95 words)

Assessor instructions: Students must outline cyber security features by correctly interpreting the information from the sources provided.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

1. Allowed and blocked execution events on workstations and servers are centrally logged.
2. Event logs are protected from unauthorised modification and deletion.
3. Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.
4. An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities
5. A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.

   Other answers may include:

6. Successful and unsuccessful multi-factor authentication events are centrally logged.
7. Allowed and blocked Microsoft Office macro execution events are centrally logged.
8. Blocked PowerShell script execution events are centrally logged
9. Privileged access events are centrally logged
10. Privileged account and group management events are centrally logged

Question 5

Outline the relevance of the 'CIA Triad' when gathering, analysing and interpreting threat data.

[Word count: 100 - 125 words]

Note: To support your answer, refer to reliable sources of information such as industry-specific or vendor websites and cite your references in the 'Reference(s)' section. The reference list does not count towards the total number of words required for the answer.

Assessor instructions: Students must demonstrate their understanding of the principles of the CIA Triad, which is a fundamental cybersecurity principle/concept.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

Confidentiality:

This principle requires sensitive data to be accessible only to authorised individuals.

When gathering threat data, it's important to protect the confidentiality of sensitive information. This includes data sources, detection methods, and incident-related data. Unauthorised access to threat data can compromise security investigations.

Integrity:

This principle requires maintaining the accuracy and reliability of data and systems.

Threat data must be accurate and reliable for effective analysis. Any manipulation or tampering with the data can lead to incorrect threat assessments and ineffective security measures.

Availability:

This principle requires information and resources to be available when needed.

The availability of threat data is crucial for timely analysis and response to security incidents. Downtime or unavailability of data sources can hinder threat recognition and response efforts.

References:

- Students must provide a list of valid references to support their answers.

Question 6

Outline the following principles of networks and how they are used when gathering, analysing and interpreting threat data.

[Word count: 80-120 words per principle]

Assessor instructions: Students must demonstrate their understanding of network principles.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

Table 3 – Question 6: Answer table

#	Principles of networks	**Answer:** *(80– 120 words)*
1	Network addressing	In networking, devices are identified by IP addresses. IP addressing involves assigning unique addresses to devices on a network to facilitate communication. There are public IP addresses used on the internet and private IP addresses used within internal networks. Monitoring network traffic and collecting data on IP addresses involved in communication is essential for threat detection. Unusual patterns, unexpected connections, or communication with known malicious IP addresses can be indicators of a security threat. Analysing the source and destination IP addresses in network traffic helps identify potential threats. Other important network-addressing concepts to be aware of include: • Network Address Translation (NAT) • Port Address Translation (PAT)
2	DNS	Domain Name System (DNS) is crucial for mapping human-readable domain names to IP addresses. It's important when gathering threat data as it can help identify malicious domains or IP addresses associated with cyberattacks. Analysing DNS queries and responses can reveal signs of malware infections or suspicious activities. DNS logs can provide valuable information during the analysis of a security incident. Anomalies in DNS requests, such as frequent requests for non-existent domains or attempts to resolve known malicious domains, can be indicators of compromise. Example: DDOS
3	DMZ	DMZ is a neutral zone that separates an organisation's internal network from an external network, such as the internet. It acts as a buffer zone that adds an extra layer of security by placing certain resources (like web servers, email servers, or application servers). The DMZ serves as a first line of defense. Any malicious activity is likely to hit the DMZ first. Security measures, like firewalls and intrusion detection/prevention systems, are often deployed in the DMZ to monitor and filter incoming traffic. Threat data collected from these security measures can then be analysed to understand the nature of potential attacks. It's like having a checkpoint that screens incoming threats before they reach the heart of your network.
4	Network encryption	This involves the use of encryption protocols to secure the transmission of data over a network. When data is encrypted, it's converted into a format that can only be deciphered by someone with the appropriate decryption key. This is crucial for maintaining the confidentiality and integrity of sensitive information as it travels across networks. Example: VPNs are used to secure and encrypt network traffic, often for remote access. Monitoring VPN logs and analysing encrypted traffic are critical for detecting threats. Anomalous VPN connections can indicate unauthorised access attempts.
References: Students must provide a list of valid references to support their answers.		

Question 7

Outline the network features and functions in each layer of the OSI reference model and their relevance for gathering, analysing and interpreting threat data.

Use 'Table 4' to record your answer. You must:

- Outline the functionality of each layer [Word count: 12-25 words per layer]
- List three [3] types of data that can be collected from each layer
- List three [3] types of threat types that are typically detected at each layer.

Note: To support your answer, refer to reliable sources of information such as industry-specific or vendor websites and cite your references in the 'Reference[s]' section. The reference list does not count towards the total number of words required for the answer.

Assessor instructions: Students must demonstrate their understanding of network features.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

Table 4 – Question 7: Answer table

#	Layers of the OSI Model	Functionality of the layer: *(12-25) words)*	Type of data that can be collected	Threat types that can be detected.
1	Physical layer	The physical layer deals with the physical connection between devices and the transmission of raw binary data over a physical medium.	• Raw binary data • Electrical voltage levels • Signal strength Other answers may include: • Cable types and specifications • Device and hardware characteristics	• Physical tampering [e.g., cable cutting, equipment damage] • Cable tapping • Electromagnetic interference Other answers may include: • Power supply attacks • Unauthorised physical access
2	Data link layer	This layer is responsible for reliable point-to-point and point-to-multipoint communication over a physical network. It ensures error detection and correction.	• Frames • MAC addresses • Error detection and correction information Other answers may include: • Flow control information • Physical addresses	• MAC address spoofing • Man-in-the-middle attacks • VLAN hopping Other answers may include: • ARP spoofing • Frame eavesdropping
3	Network layer	The network layer focuses on logical addressing, routing, and forwarding of data packets between devices on different networks.	• Packets • IP addresses [source and destination] • Routing information Other answers may include: • Time-to-Live [TTL] values	• IP address spoofing • Routing attacks [e.g., route poisoning] • Network scanning Other answers may include: • Smurf attacks

#	Layers of the OSI Model	Functionality of the layer: *(12-25) words)*	Type of data that can be collected	Threat types that can be detected.
			• Subnet masks	• Fragmentation attacks
4	Transport layer	The transport layer manages end-to-end communication, ensuring reliable data transfer and error recovery.	• Segments • Source and destination ports • Sequence numbers Other answers may include: • Acknowledgment numbers • Window sizes	• Session hijacking • Denial-of-service attacks • Man-in-the-middle attacks Other answers may include: • SYN/ACK attacks • Port scanning
5	Session layer	The session layer manages sessions or dialogues between applications, allowing them to establish, maintain, and terminate connections.	• Dialogues and sessions • Session IDs • Synchronization points Other answers may include: • Dialog control information • Token management information	• Session hijacking • Session replay attacks • Token hijacking Other answers may include: • Session fixation • Denial-of-service attacks on session establishment
6	Presentation layer	Handles data translation, encryption, and compression to ensure that data is presented in a readable format between applications.	• Encoded and formatted data • Data compression information • Encryption/decryption information Other answers may include: • Character sets and encoding schemes • Syntax and semantics of data	• Data tampering • Data injection attacks • Encryption/decryption errors Other answers may include: • Compression attacks • Malformed data attacks
7	Application layer	The application layer provides network services directly to end-users and application processes.	• Messages or data specific to the application • Application layer protocols (HTTP, FTP, SMTP, etc.) • User authentication information Other answers may include: • Commands and requests • Responses and data content	• SQL injection • Cross-site scripting (XSS) • Cross-site request forgery (CSRF) Other answers may include: • Malware communication • Authentication attacks (e.g., password cracking)

References:

Students must provide a list of valid references to support their answers.

Assessment submission checklist

Students must have completed all questions within this assessment before submitting. This includes:

1	7 short answer questions completed in the spaces provided.	☐

Assessment feedback

Assessors are to indicate the assessment outcome as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:	☐ S	☐ NYS

Congratulations, you have reached the end of Assessment 1!