ICTCYS407

# Gather, analyse and interpret threat data

## Assessment 2 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.

## 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.

## Question 1

Describe the following threat data sources. Your answer must include:

- a description of the threat data source (Word count: 25 - 45 words)
- an outline of two (2) types of data that can be collected from each threat data source (Word count: 25 - 45 words per data source)

**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 describe each data source

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 1 – Question 1: Answer table

| Threat data source | Description of the threat data source<br>*(25-45 words)* | Two (2) types of data collected<br>*(25-45 words)* |
|---|---|---|
| A. Firewalls | Firewalls are network security devices designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between a trusted internal network and untrusted external networks (e.g., the internet). | **Firewall Logs:** These include information about incoming and outgoing network connections, source and destination IP addresses, port numbers, and actions taken (e.g., allowed, blocked).<br>**Packet Inspection Data:** Information about the contents of network packets, which may include data about application protocols, packet size, and flags. |
| B. Intrusion Detection System (IDS) | Intrusion Detection Systems are security devices or software that monitor network and system activities for signs of malicious activity or policy violations. They can be network-based or host-based. | **Alerts:** IDS generates alerts when suspicious/malicious activities are detected. These alerts include information on detected intrusions (i.e. source IP address, attack type, and severity).<br>**Packet Capture (PCAP) Data:** Detailed network traffic data captured for further analysis, including packet payloads, to understand attack patterns and methods. |
| C. Access control systems | Access control systems are used to regulate and manage physical or logical access to buildings, rooms, or digital resources. They are used to ensure only authorised individuals can access restricted areas or data. | **Access Logs:** Records of access attempts, successful and unsuccessful, which include user IDs, timestamps, access locations, and the outcome (e.g., granted or denied access).<br>**Access Permissions Data:** Information on user roles, permissions, and access levels |

| Threat data source | Description of the threat data source<br>*[25-45 words]* | Two [2] types of data collected<br>*[25-45 words]* |
|---|---|---|
| | | that define who has access to what resources. |
| D. Security and event management systems [SIEM] | SIEM systems are designed to collect, aggregate, and correlate data from various sources, including network and security devices, to provide real-time and historical insights into an organisation's security posture. | **Event Logs:** These logs contain information about various security events, such as login attempts, changes to system configurations, and other security-related actions.<br>**Correlation Data:** Data that helps SIEM systems correlate events and identify patterns or anomalies, often used to detect complex threats or incidents.<br>Other answer may include:<br>**User and Entity Behavior Analytics [UEBA] Data:** Information about user and entity behavior to detect abnormal or potentially malicious activities, helping with insider threat detection. |
| References:<br>• Students must provide a list of valid references to support their answers. | | |

## Question 2

Describe three [3] common cybersecurity threats and their impacts on business functions.

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 knowledge of common cyber threats and their impacts on business functions.

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 2 - Question 2: Answer table

| Cyber threats | Description of threat<br>*[15-45 words]* | Impacts on business functions<br>[List 2] |
|---|---|---|
| **Social engineering** | This commonly refers to the practice of attempting to convince people to divulge sensitive information. | • Theft of personal information<br>• Misuse of sensitive and business-critical data |

| Cyber threats | Description of threat<br>*(15-45 words)* | Impacts on business functions<br>(List 2) |
|---|---|---|
| Ransomware | Malware that denies access to the infected computer system and demands a person be paid in order for the restriction to be removed. | • Financial costs to restore data<br>• Unable to access organisation's operational data and systems |
| DOS Attack | An attack that prevents normal use of a computer or network by valid users. This attack can also flood a computer or the entire network with traffic until a shutdown occurs because of the overload. | • Loss of access to network resources by authorised users.<br>• Downtime causing loss in production and service operations. |

Students may choose to describe other types of threats such as:

- Phishing
- Malware
- Identity theft
- Hacking
- System and network attacks

**References:**

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

## Question 3

Outline the objective of each of the following types of attacks and how it can be identified when analysing and interpreting threat data.

Use 'Table 3' to record your answers. You must outline:

- the objective of the attack (Word count: 25-45 words per attack type)
- how the attack type can be identified when analysing and interpreting threat data (Word count: 15-35 words per attack type).

**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 listed attack types.

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 3: Answer table

| Attack type | Objective of the attack<br>*[25-45 words]* | How the attack type can be identified when analysing and interpreting threat data?<br>*[15 – 35 words]* |
|---|---|---|
| A. Denial-of-service attack (DDOS) | The objective of a Distributed Denial of Service (DDoS) attack is to degrade the performance of the system. overwhelm a target's online service, rendering it inaccessible to users, causing disruption, financial loss, and damage to reputation. | To identify it when analysing threat data, look for a sudden surge in incoming traffic or unusual traffic patterns. |
| B. SQL injection (SQLi) | The objective of an SQL injection attack is to exploit vulnerabilities in a web application's input fields, enabling unauthorised access or manipulation of a database, potentially stealing sensitive data or compromising the application's integrity. It uses malicious database query code to manipulate the backend database. | These attacks can be identified in threat data analysis by detecting unusual SQL queries, error messages, or unauthorised data retrieval attempts in web server logs. |
| C. Cross-site scripting (XSS) attacks | The objective of client-side scripting attacks is to manipulate and execute malicious code within a user's web browser, potentially compromising their data, privacy, or access to sensitive information. It uses client-side code injection to access a user's computer. | To identify these attacks in threat data, look for suspicious JavaScript or HTML code, abnormal network traffic patterns, and unauthorised access to user data. |
| D. Scripted attacks | Scripted attacks aim to exploit vulnerabilities in software or systems by using automated scripts or code to compromise security, steal data, gain unauthorised access, or disrupt services. It sends code to a computer with the intention of performing malicious acts. | They can be identified through the analysis of attack patterns, suspicious activity, and known attack vectors in threat data, along with the timely application of security patches. |
| E. Hardware attacks | Hardware attacks seek to compromise the physical components of a system or device, aiming to gain unauthorised access, steal sensitive data, or disrupt perations through manipulation or tampering. | Identifying hardware attacks involves monitoring for unusual device behaviour, hardware modifications, or unauthorised physical access in threat data analysis. |
| F. Attacks against Wi Fi | Attacks against Wi-Fi networks aim to gain unauthorised access, intercept data, or disrupt network operations, compromising confidentiality, integrity, | To identify such threats, analyse network logs for unauthorised device connections, unusual traffic patterns, and failed authentication attempts. |

| Attack type | Objective of the attack<br>*[25-45 words]* | How the attack type can be identified when analysing and interpreting threat data?<br>*[15 – 35 words]* |
|---|---|---|
| | and availability of wireless communication and connected devices. | |
| References:<br>Students must provide a list of valid references to support their answers. | | |

## Question 4

'The Hunting Loop' is a proactive cyber security approach for hunting cyber security threats. Using this approach as a guideline, explain the basic troubleshooting process for two (2) different types of threats.

(Word count: 165 - 200 words per type of threat)

**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 knowledge of basic troubleshooting processes related to cyber security threats.

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 4: Answer table**

| Type of threat | Basic troubleshooting process<br>*[165 – 200 words per type of threat]* |
|---|---|
| Malware threat | **Step 1: Data collection**<br>• Gather data from various sources, such as network logs, endpoint logs, and security event logs.<br>• Identify anomalies or suspicious activities in the data, such as unusual file downloads, system process behaviour, or communication with known malicious IP addresses.<br>**Step 2: Hypothesis generation**<br>Based on the data collected, create a hypothesis about a potential malware infection. For example, suspect a malware infection due to unusual file transfers or an increase in unauthorised access attempts.<br>**Step 3: Investigation**<br>• Begin investigating the hypothesis by analysing the suspicious files, processes, or network traffic. |

| Type of threat | Basic troubleshooting process<br>*[165 – 200 words per type of threat]* |
|---|---|
| | • Utilise threat **intelligence feeds** to check for **indicators of compromise (IoCs)** associated with known malware.<br>• Use **sandboxing** and analysis tools to execute suspicious files in a controlled environment to understand their behaviour.<br>**Step 4: Confirmation or refinement**<br>• Confirm whether the threat is indeed malware or refine the hypothesis if necessary.<br>• Identify the extent of the infection, such as the number of compromised systems and the scope of the damage.<br>**Step 5: Remediation**<br>• Develop a plan to remove the malware and its associated artifacts from the affected systems.<br>• Implement preventive measures to reduce the risk of future malware infections. |
| Insider threat | **Step 1: Data Collection**<br>• Collect data from various sources, such as user activity logs, privilege escalation logs, and access control records.<br>• Look for unusual patterns in user behaviour, such as excessive access to sensitive data or repeated failed login attempts.<br>**Step 2: Hypothesis Generation**<br>Develop a hypothesis about a potential insider threat based on the collected data. This could include suspicions of data theft, unauthorised access, or unusual privilege escalation.<br>**Step 3: Investigation**<br>• Investigate the identified users and their activities to gather more evidence.<br>• Interview relevant personnel and gather information on the user's role, access permissions, and recent behaviour.<br>• Utilise user and entity behaviour analytics (UEBA) tools to help identify abnormal user activity.<br>**Step 4: Confirmation or Refinement**<br>• Confirm whether the insider threat exists or refine the hypothesis based on new evidence.<br>• Determine the motive and intent behind the insider threat, if possible.<br>**Step 5: Remediation**<br>• Develop a response plan that may involve revoking access, monitoring the user, or involving law enforcement if necessary.<br>• Implement user and data access controls to prevent similar incidents in the future. |

| Type of threat | Basic troubleshooting process<br>*[165 – 200 words per type of threat]* |
|---|---|
| References:<br>Students must provide a list of valid references to support their answers.<br>• framework-for-threat-hunting-whitepaper.pdf (threathunting.net)<br>• The Threat Hunting Reference Model Part 2_ The Hunting Loop _ Sqrrl.pdf | |

## Question 5

List and describe the features of three (3) industry-standard software tools and how they are used to recognise threats to an organisation's network.

(Word count: 45 - 75 words for each tool)

**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 list and describe three (3) threat data recognition software tools.

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 5 - Question 5: Answer table

| Software tool | Answer:<br>*(45-75 words)* |
|---|---|
| NetFlow | NetFlow is a network protocol used for collecting and recording network traffic flow information. It aggregates data about network conversations and their characteristics. NetFlow data provides a high-level overview of network traffic, which is useful for identifying potential threats such as:<br>• unusual traffic volume or bandwidth utilisation.<br>• excessively long or short network connections.<br>• suspicious peer-to-peer or lateral movement traffic.<br>• sudden spikes in network traffic that may indicate a Distributed Denial of Service (DDoS) attack. |
| Anti-virus software | Anti-malware software is specifically designed to detect and remove malicious software, including viruses, trojans, ransomware, and spyware. Anti-malware software recognises threat data by:<br>• Scanning files and executables for known malware signatures.<br>• Identifying suspicious activities or system changes that may indicate malware.<br>• Detecting previously unknown threats based on behavior or code analysis. |
| Wireshark | Wireshark is a network protocol analyser that captures and inspects network traffic in real time. It allows you to capture packets traversing the network, |

| Software tool | Answer:<br>*(45-75 words)* |
|---|---|
| | whether wired or wireless. Wireshark can help identify various threat data, such as:<br>• communication with known malicious IPs.<br>• traffic spikes or unusual protocols that may indicate an attack.<br>• malware or exploits hidden in packet data.<br>• scanning and probing attempts by attackers. |

Other answers that students may expand upon include:

- Event log analyser software
- Access control management software
- Firewall software
- Event Viewer
- API-based analysis
- SNORT
- Sguil
- Squert

**References:**

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

Refer to the following network diagram and answer 'Question 6' and 'Question 7'.

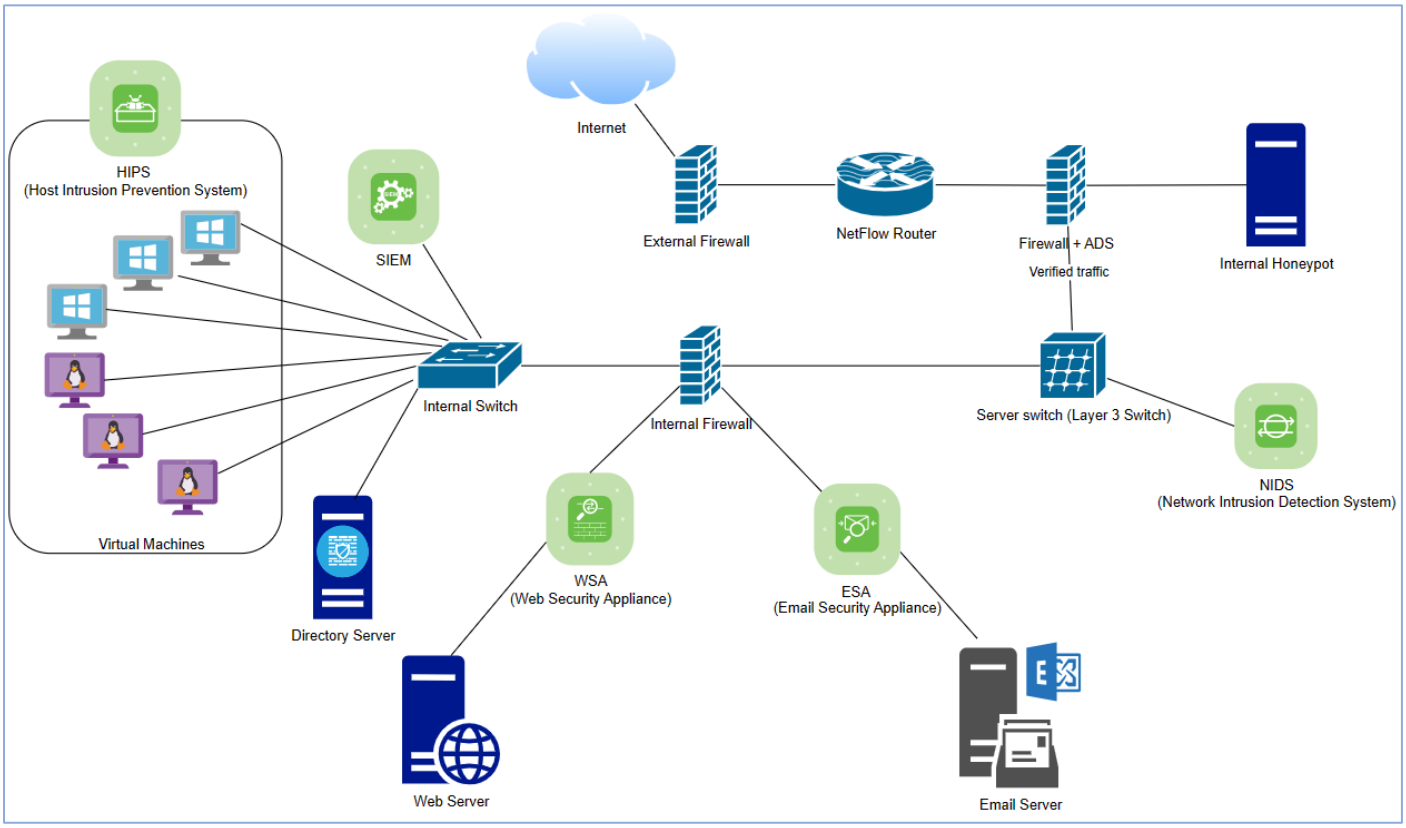


**Figure 1 - Network Diagram created using diagrams.net/draw.io (drawio.com)**

## Question 6

Identify and list five (5) types of security equipment on the given network.

**Assessor instructions:** Students must correctly identify security equipment in the given network.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

1. Web Security Appliance (WSA)
2. External and Internal firewalls
3. Host Intrusion Prevention System (HIPS)
4. Email Security Appliance (ESA)
5. Network Intrusion Detection System (NIDS)

### Question 7

Identify and list five (5) types of threat data sources on the given network.

**Assessor instructions:** Students must correctly identify threat data sources in the given network.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

1. Firewalls
2. NetFlow enabled Router logs
3. Network Intrusion detection system (NIDS)
4. Directory Server
5. Security and Event Management System (SIEM)

# 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 2!**