Government of Western Australia
North Metropolitan TAFE

Assessment Task

Qualification national code and title	VU23216 Perform basic Cyber Security Analysis
Unit/s national code/s and title/s	AE780 Transition to Cyber Security Skill Set

Assessment type (☑):

☒ Questioning (Oral/Written)
☐ Practical Demonstration
☐ 3rd Party Report
☐ Other – Project/Portfolio *(please specify)*

Assessment Resources:

- Computer access
- Completion of the Splunk Search Tutorial parts 1-4

Assessment Instructions:

There are 13 questions in this assessment. This is the first of three assessments in the unit VU23216

This assessment provides evidence of understanding the underpinning knowledge of VU23216 & allows the lecturing team information about student progress so we can provide targeted help and helps us validate authenticity of work submitted so far.

Before attempting this quiz, please ensure you have completed all required Splunk Search Tutorial exercises.

This assessment should be completed in approximately 1.5 hours if possible.

If you are an online student, please coordinate with your lecturer or the online support lecturers.

You are allowed **TWO** (2) attempts by default.

Assessment Due

NOTICE: This assessment is due by session 6. This information and any updates can be found on the Learning Assessment Plan in Blackboard

However, it is strongly recommended that you complete each Search Tutorial task *during or soon after* the appropriate session.

Government of Western Australia
North Metropolitan TAFE

Assessment Task

Qualification national code and title	VU23216 Perform basic Cyber Security Analysis
Unit/s national code/s and title/s	AE780 Transition to Cyber Security Skill Set

Answering Questions

When a step includes a question, you must attempt to answer both parts. Where a code example is requested this code example should be working and include at least one line of appropriate pseudo explaining the code.

Should code be required you must include all of the code requested to complete the question.

All answers must be in complete sentences unless indicated. You must **use your own work** unless otherwise specified.

Using ChatGPT and other LLMs

If you use any form of generative AI (large language models, or LLMs) to help you answer questions, then ensure:

- The answers you place here are phrased in **your** words **not** the AI's. Failure to comply may be evidence of academic misconduct!
- Retain a history of your chat transcript with the AI, as you may be asked to show it.
- **Consider**: LLMs are not a source of truth. If you attained facts from ChatGPT, or a similar service, you may need to confirm those facts with an authoritative website (e.g. python.org).
- **Remember**: at any time, lectures may call on you to explain in your own words your answers to questions.

Reasonable Adjustment

Information on reasonable adjustment can be found in the Learning and Assessment Plan for the Unit

Recognition of Prior Learning(RPL)

Information on RPL can be found in the Learning and Assessment Plan for the Unit

Begin by completing the form below with your details…

Government of Western Australia
North Metropolitan TAFE

Assessment Task

Qualification national code and title	VU23216 Perform basic Cyber Security Analysis
Unit/s national code/s and title/s	AE780 Transition to Cyber Security Skill Set

Assessment # and title	VU23216	AT1 Knowledge Assessment
Lecturer name	*Student to fill this section out*	
Student name	*Student to fill this section out*	
Student ID number	*Student to fill this section out*	
Telephone contact number	*Student to fill this section out*	
Email	*Student to fill this section out*	

By completing and submitting this signed form to my lecturer, I am stating that:

a. The attached submission is completely my own work
b. I have correctly cited all sources of information used in this work (if required)
c. I have kept a copy of this assessment (where practicable)
d. I understand a copy of my assessment will be kept by the NMTAFE for their records.
e. I understand my assessment may be selected for use in the NMTAFE's validation and audit process to ensure student assessment meets requirements

Student Signature	*Student to fill this section out*	**Date**	*Student to fill this section out*

Assessors please note: Where verbal clarification has been sought from a student to gather additional assessment evidence from an assessment item, question/s and response/s must be recorded, signed, and dated by the assessor, against the relevant assessment item/s.

NB: Feedback will be given via Blackboard when possible.

Submission 1 ☐	Result	Satisfactory / Not Yet Satisfactory	Date	
To satisfy requirements for this assessment, you need to complete the following:		*Feedback to student…*		
Submission 2 ☐	Result	Satisfactory / Not Yet Satisfactory	Date	
To satisfy requirements for this assessment, you need to complete the following:		*Feedback to student…*		
Student Feedback		*Feedback from student…*		
Lecturer Signature		**Student Signature**		

Government of Western Australia
North Metropolitan TAFE

Assessment Task

Qualification national code and title	VU23216 Perform basic Cyber Security Analysis
Unit/s national code/s and title/s	AE780 Transition to Cyber Security Skill Set

Assessment Instrument:

Q1. What is the primary goal of data analysis, and why is it essential in Cyber Security?

Finding valuable insights in unprocessed data to aid in sound decision-making is the main objective of data analysis. Analysing system logs, network traffic, and user behaviour is crucial for cyber security since it helps detect risks, spot anomalies, and stop attacks.

Security teams can evaluate risks, bolster defences, and react swiftly to incidents with the aid of data analysis. By turning complicated security data into useful intelligence, it also guarantees regulatory compliance and improves overall data protection.

Q2. Explain the significance of exploratory data analysis (EDA) in the data analysis process. Provide an example of an EDA technique.

Prior to formal modelling, exploratory data analysis (EDA) is important because it aids in the understanding of data patterns, the detection of anomalies, and the identification of relationships. To reveal hidden patterns and enhance decision-making, it enables analysts to clean, visualize, and summarize data.

EDA is essential for identifying questionable activities in cyber security. For instance, analysing network traffic using visualization tools like heatmaps or scatter plots might highlight odd data flow spikes that could be signs of infiltration or denial-of-service (DoS) attacks.

Q3. What is a data model, and how does it contribute to the organisation and retrieval of data in a database?

A data model offers a logical framework for effectively organizing and retrieving information by defining how data is referenced, stored, and structured within a database. Data models are essential for handling massive amounts of log and event data in cyber security. They aid in standardizing data from many sources, which facilitates threat analysis, anomaly detection, and report generation.

Data models improve security monitoring, incident response, and general decision-making within an organization's security infrastructure by guaranteeing data accessibility and consistency.

Government of Western Australia
North Metropolitan TAFE

Assessment Task

Qualification national code and title	VU23216 Perform basic Cyber Security Analysis
Unit/s national code/s and title/s	AE780 Transition to Cyber Security Skill Set

Q4. Explain the significance of the Confidentiality, Integrity, and Availability (CIA) Triad in the context of database security. How does each component contribute to maintaining a secure database environment?

Database security is based on the Confidentiality, Integrity, and Availability (CIA) Triad. By using encryption and access controls, confidentiality makes sure that only authorized users can access sensitive data. Integrity guards against unauthorized changes, preserving data consistency and accuracy. By using redundancy and backups, availability guarantees that users may access data and systems whenever they're needed.

The fundamental ideas of a safe and robust Cyber Security framework are formed by these elements working together to uphold trust, guard against breaches, and guarantee dependable database operations.

Q5. List 3 common database vulnerabilities

Three major database vulnerabilities are unpatched software, which leaves systems vulnerable to known exploits; incorrect permissions, which expose sensitive information to unauthorized users; and SQL injection, which allows attackers to modify searches to access or edit data.

These flaws highlight the necessity of frequent upgrades, access control, and security monitoring because they might result in data leaks, corruption, or loss.

Q6. List two strategies for mitigating database security vulnerabilities.

Implementing strict access controls to guarantee that only authorized users can view or alter data and routinely updating and patching database software to address known security flaws are two efficient methods for reducing database security vulnerabilities.

Encrypting critical data and keeping an eye on database activities also improve defences against potential cyberthreats and unauthorized access.

Q7. What does the acronym "SIEM" stand for? Provide three examples of SIEM solutions and explain the significance of SIEM in the context of cyber security.

Security Information and Event Management is referred to as SIEM. ArcSight, IBM QRadar, and Splunk Enterprise Security are three instances of SIEM solutions. In order to identify threats and questionable activities, SIEM systems gather, examine, and correlate security events from many sources in real time. They support security teams in finding breaches, looking into occurrences, and making sure rules are followed.

Qualification national code and title	VU23216 Perform basic Cyber Security Analysis
Unit/s national code/s and title/s	AE780 Transition to Cyber Security Skill Set

SIEM is essential to cyber security because it increases visibility, automates warnings, and improves an organization's capacity to react swiftly to possible intrusions.

Q8. List four possible sources of cyber security data commonly used for monitoring and analysis.

Network traffic logs, which track data flow and identify anomalies; system and application logs, which document user actions and system events; firewall and intrusion detection/prevention system (IDS/IPS) logs, which monitor access and block threats; and endpoint security logs, which document malware activity and device health, are the four main sources of cyber security data.

When taken as a whole, these sources offer thorough visibility, facilitating proactive security monitoring, incident response, and threat identification throughout an organization.

Q9. You are tasked with analysing a cyber security dataset that contains logs from various sources. However, upon initial inspection, you notice that the dataset is messy and contains inconsistencies.

Describe three specific data cleaning challenges you might encounter in this cyber security dataset and propose appropriate data cleaning techniques to address each challenge.

Three typical issues with data cleaning in a Cyber Security dataset are: inconsistent formats, like different IP addresses or timestamp styles, which are addressed by standardization and normalization; duplicate entries, which are frequently the result of repeated logging, are resolved by deduplication; and missing values, such as absent timestamps or user IDs, can be handled by imputation or deleting incomplete records.

By using these techniques correctly, threat detection and general security monitoring are improved, and the dataset is guaranteed to be accurate, consistent, and prepared for trustworthy analysis.

Q10. Describe the concept of data transformation in the context of cyber security analysis. Provide at one example of a data transformation technique.

In cyber security analysis, data transformation is the process of transforming unstructured data into a consistent, structured format that may be used for threat identification and analysis. Easy correlation, comparison, and anomaly detection across several log sources are made possible by this procedure.

Qualification national code and title	VU23216 Perform basic Cyber Security Analysis
Unit/s national code/s and title/s	AE780 Transition to Cyber Security Skill Set

For instance, analysts can precisely sequence events and identify questionable activity patterns by standardizing timestamps from various systems. In security monitoring and incident response, data transformation guarantees dependability, consistency, and actionable insights.

Q11. Give two examples of an Exploratory Analysis Technique we use in Splunk.

Time-series visualisation, which shows log events over time to spot trends or anomalies, and correlation searches, which connect similar events from various data sources to find patterns or possible security problems, are two examples of exploratory data analysis approaches in Splunk.

Both methods assist analysts in examining unprocessed machine data, identifying anomalous activity, and obtaining useful information for monitoring and researching cyber security.

Q12. Review the SPL query below, what information is it trying to uncover?

```
index=security_logs sourcetype=firewall action=allow | stats count by src_ip
```

The SPL query counts instances aggregated by source IP (src_ip) after searching the security_logs index for firewall events with the action set to "allow." In order to assist analysts in identifying high-activity sources, possible legitimate users, or odd patterns that might point to security threats, it seeks to determine which IP addresses are producing the most permitted traffic over the firewall.

Q13. Provide at least 4 forms of data that Splunk is capable of handling.

Log files from servers and apps, network traffic data from firewalls and routers, machine-generated sensor or Internet of Things data, and structured data from databases or CSV files are just a few of the many data kinds that Splunk can manage.

Additionally, it supports JSON or XML formats and unstructured text data, allowing for thorough ingestion, indexing, and analysis for operational intelligence and cyber security monitoring.

Government of Western Australia
North Metropolitan TAFE

Assessment Task

Qualification national code and title	VU23216 Perform basic Cyber Security Analysis
Unit/s national code/s and title/s	AE780 Transition to Cyber Security Skill Set