NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF CYBER SECURITY

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE (HONS DIGITAL FORENSICS)	
QUALIFICATION CODE: 08 BCCS	**LEVEL: 8**
COURSE: SECURITY ANALYTICS	**COURSE CODE:** SAS821S
DATE: NOVEMBER 2023	**SESSION:** THEORY
DURATION: 2 HOURS	**MARKS: 70**

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	PROF ATTLEE M. GAMUNDANI
MODERATOR:	MR MBAUNGURAIJE TJIKUZU

THIS QUESTION PAPER CONSISTS OF 2 PAGES
(Excluding this front page)

INSTRUCTIONS

1. Answer ALL the questions.
2. Write clearly and neatly.
3. In answering questions, be guided by the allocated marks.
4. Number your answers clearly following the numbering used in this question paper.

PERMISSIBLE MATERIALS

1. None

SECTION A – 20 Marks

QUESTION 1 — 10 marks

You have been hired by a new e-commerce start-up. They have asked you to set up a security analytics framework. Describe a method you would use to analyse user activity to detect potentially fraudulent transactions. **[10 marks]**

QUESTION 2 — 10 marks

A colleague has proposed the use of unsupervised machine learning to detect anomalies in your company's web traffic. Evaluate the strengths and weaknesses of this approach. **[10 marks]**

SECTION B – 50 Marks

QUESTION 3 — 25 marks

You are provided with the results of a machine-learning analysis of user access logs for a critical application over the last three months. The results indicate the following anomalies: -

1. A 300% spike in access requests from IP addresses located in foreign countries.
2. User accounts access the system at unusual hours, predominantly between 2 AM and 4 AM.
3. Multiple failed login attempts on high-privilege accounts within a short time span.

Based on these findings: -

(a) Interpret the potential security risks associated with each of the anomalies listed. **[5 marks]**

(b) Recommend specific action steps to address and mitigate these risks. **[10 marks]**

(c) Suggest two preventive measures to avoid such anomalies in the future. **[5 marks]**

(d) How would you communicate these findings to non-technical stakeholders in the organisation? **[5 marks]**

QUESTION 4 **25 marks**

You have been given a dataset from a Security Information and Event Management (SIEM) system showing multiple high-volume traffic spikes to a particular server within the organisation. The traffic is from different IP addresses but follows a consistent pattern: high traffic for 10 minutes, then silence, repeated hourly.

(a) Interpret what kind of threat or activity this pattern might indicate. **[5 marks]**

(b) Detail an analytic approach you would use to further investigate this pattern, including specific data points you would analyse and any additional tools you would employ. **[10 marks]**

(c) Recommend at least three specific countermeasures to mitigate this potential threat. **[5 marks]**

(d) How would you ensure long-term monitoring and response to similar patterns in the future? **[5 marks]**

*******END OF EXAMINATION PAPER*******