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: JANUARY 2024	**SESSION:** THEORY
DURATION: 2 HOURS	**MARKS: 70**

SECOND OPPORTUNITY/SUPPLEMENTARY 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

Your company's firewall has been breached and a malware has infected several systems. Describe how machine learning can assist in detecting and countering this malware in future. **[10 marks]**

QUESTION 2 — 10 marks

With increasing reports of insider threats, how would you use access analytics to mitigate such risks? **[10 marks]**

SECTION B – 50 Marks

QUESTION 3 — 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 organization. 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]**

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*******