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 2025	**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: Case Study – 20 Marks

QUESTION 1 — 20 marks

ABC Enterprises has implemented an access control system to manage employee access to its resources. Recently, there have been incidents of unauthorised data access despite the access controls. The company wants to develop an analytics solution to detect anomalies in user access patterns using machine learning.

(a) Explain the concept of access analytics and its importance in detecting anomalies in user access patterns. **(5 marks)**

(b) Outline the steps you would take to develop and implement a machine learning-based access anomaly detection system. **(10 marks)**

(c) Discuss the limitations of using machine learning for access anomaly detection and suggest ways to mitigate these limitations. **(5 marks)**

SECTION B – 50 Marks

QUESTION 2 — 15 marks

(a) Describe how simulations can be used in "what-if" security scenarios to aid strategic decision-making. Provide an example related to cyber-attack response planning. **(7 marks)**

(b) Identify and discuss the challenges involved in using simulations for security process implementations, such as data accuracy and computational resources. **(8 marks)**

QUESTION 3 **15 marks**

(a) *Compare and contrast supervised and unsupervised machine learning approaches in the* context of malware detection. **(7 marks)**

(b) Propose a machine learning-based solution for detecting zero-day malware attacks. Explain how your approach would identify previously unseen malware. **(8 marks)**

QUESTION 4 **20 marks**

(a) Define security intelligence and explain its role in enhancing an organisation's risk management strategies. **(5 marks)**

(b) Discuss how security intelligence can be leveraged to detect insider threats. Specify the types of data and analytics methods that would be employed. **(10 marks)**

(c) Explain the challenges of integrating security intelligence solutions into existing security infrastructures and suggest possible solutions. **(5 marks)**

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