NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY
Faculty of Computing and Informatics
School of Computing
Department of Cyber Security

13 Jackson Kaujeua Street
Private Bag 13388
Windhoek
NAMIBIA

T: +264 61 207 2052
F: +264 61 207 9052
E: dcy@nust.na
W: www.nust.na

DEPARTMENT OF CYBER SECURITY

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE (HONS DIGITAL FORENSICS)	
QUALIFICATION CODE: 08BCCS	**LEVEL**: 8
COURSE: SECURITY ANALYTICS	**COURSE CODE**: SAS821S
DATE: DECEMBER 2025	**SESSION**: THEORY
DURATION: 3 HOURS	**MARKS**: 100

SECOND OPPORTUNITY / SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER (S)	DR ARPIT JAIN
MODERATOR:	MR MBAUNGURAIJE TJIKUZU

THE QUESTION PAPER CONSISTS OF 4 PAGES
(Including 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

Question 1

(a) Describe the main objectives and benefits of implementing Security Analytics in modern organisations. [05 Marks]

(b) Explain how data collection, correlation, and visualisation enhance threat detection in security analytics. [05 Marks]

(c) Describe how machine learning and predictive modelling can be utilised to forecast cyber threats and assist in proactive defence mechanisms. [10 Marks]

Question 2

(a) What are the different kinds of features which are used in existing ML-based detection algorithms? [10 Marks]

(b) Explain how supervised and unsupervised learning techniques can be applied in detecting unknown or zero-day attacks. [10 Marks]

Question 3

(a) Explain the Incident Response Life Cycle in detail. [10 Marks]

(b) Explain the below phases of the analytics in incident response.

1. Detection and analysis [05 Marks]
2. Containment [05 Marks]

Question 4

(a) Differentiate Threat Intelligence and Security Intelligence [10 Marks]

(b) Explain the role of text mining techniques to analyse security logs, alerts, and incident reports. [10 Marks]

Question 5

Scenario:

The owners of a small start-up company found it strange when several of their programmers quit the company at the same time. When company executives "got wind" that the individuals had gone to work for a competitor, they began to ask questions about whether or not the company's intellectual property had been stolen, since these programmers were working on key pieces of their product. Since this was a small company, the management did not have a security officer, so they looked to the IT personnel to examine the problem and to look for evidence. The first area the IT personnel examined was the email of the employees. Through the email, they were able to piece together that the employees who left the company were collaborating, and they intended to steal the code they developed at this company. These emails were key evidence that the company saved to an external storage device for preservation. The company made a secondary copy so that they could review the data.

(a) Identify the type of security threat demonstrated in the case study and explain why it fits that category. [04 Marks]

(b) What are the potential risks and consequences for the company if it fails to handle the evidence properly or cannot prove intellectual property theft? [04 Marks]

(c) From an ethical and legal standpoint, was it appropriate for the IT team to access and review employee e-mails without prior consent? Explain your reasoning. [04 Marks]

(d) How can security analytics help the company detect or investigate this kind of insider threat earlier? Explain what data or tools could be used to find suspicious activity. [04 Marks]

(e) If you were appointed as a new cybersecurity advisor for this start-up, what long-term strategies would you implement to protect intellectual property and prevent insider attacks in the future? [04 Marks]

---------- **END OF EXAMINATION** ----------