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: NOVEMBER 2025	**SESSION**: THEORY
DURATION: 3 HOURS	**MARKS**: 100

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

THE QUESTION PAPER CONSISTS OF 3 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) What are the techniques for Security analytics? List them. [05 Marks]

(b) Explain how analytics is applied in cybersecurity. [05 Marks]

(c) How do simulation techniques support threat detection, risk assessment, and proactive decision-making in security analytics? [10 Marks]

Question 2

(a) Compare and contrast signature-based detection and behaviour-based detection in threat identification. [10 Marks]

(b) Describe how anomaly detection techniques help in identifying zero-day attacks. [10 Marks]

Question 3

(a) What are the goals in incident response? [05 Marks]

(b) How does an incident responder know what to fix? [05 Marks]

(c) Name the phases of Incident response? Explain the role of analytics in each phase. [10 Marks]

Question 4

(a) Differentiate between text mining and data mining. [10 Marks]

(b) Consider the scenario of the access logs of a cloud application showing multiple failed login attempts from different IPs.

1. Describe how access analytics can help identify potential brute-force or credential-stuffing attacks. [05 Marks]
2. Suggest mitigation strategies based on your analysis. [05 Marks]

Question 5

(a) What are insider threats in cybersecurity? Discuss how security intelligence can be applied to detect, prevent, and mitigate insider threats. [10 Marks]

(b) Explain the Security Intelligence Cycle, describing each phase in detail. Also, explain the basic process of security intelligence analysis. [10 Marks]

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

NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Office of the Registrar

Examinations and Assessment Administration

13 Jackson Kaujeua Street
Private Bag 13388
Windhoek
NAMIBIA

T: +264 61 207 2412
F: +264 61 207 9412
E: exams@nust.na
W: www.nust.na

MODERATOR'S REPORT: QUESTION PAPER & MEMORANDA

This report is to accompany every question paper and marking scheme/memorandum of model answers that is set and moderated.

PERSONAL INFORMATION			
Surname and Name/s	Tjikuzu Mbaunguraije		
Postal Address	PO Box 81559		
Tel Number(s)	0812020627		
Course (e.g. Economics 1)	Security Analytics	Course Code: SAS811S	
Exam Session/Date	November 2025	Signature	
Exam Type (1St/2nd Opportunity)	1st Opportunity	Date: 16/10/2025	

	Question paper		Memorandum	
CATEGORY	YES	NO	YES	NO
1. Front cover: The following information is available on the front cover				
The name of the institution	X		X	
The department within which the course falls	X		X	
The name and level of the course	X		X	
The course code	X		X	
The examination session and the year	X		X	
The duration of the paper	X		X	
The names of the Examiners and Moderator(s)	X		X	
Instructions to candidates, and such instructions are clear and unambiguous	X		X	
A list of all the material that is permissible for answering the question paper	X		X	
2. Standard of paper & memorandum				
The standard of the questions is satisfactory and appropriate to the level of the	X		X	
The question paper comprises a range of question types, i.e., recall, comprehension, analytical etc.	X		X	
The questions cover all parts of the approved syllabus.	X		X	
There is no repetition of questions	X		X	
The question paper is accompanied by a memorandum of model answers	X		X	
The model answers are of satisfactory standard and cover all aspects of the questions	X		X	
Where appropriate, alternative answers are provided	X		X	
The memorandum is designed in such a way that people other than an examiner can	X		X	
3. Language & Format Question paper & memorandum				
The instructions and the questions are clear and unambiguous	X		X	
Does the paper contain any grammatical and spelling errors		X		X
The paper is formatted clearly (e.g. questions are clearly separated)	X		X	
The marks for each question are allocated clearly in the right hand margin of the question paper & the memorandum	X		X	
The marks for each question, each section and the whole paper are calculated	X		X	

NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Office of the Registrar

Examinations and Assessment Administration

13 Jackson Kaujeua Street
Private Bag 13388
Windhoek
NAMIBIA

T: +264 61 207 2412
F: +264 61 207 9412
E: exams@nust.na
W: www.nust.na

MODERATOR'S REPORT: QUESTION PAPER & MEMORANDA

This report is to accompany every question paper and marking scheme/memorandum of model answers that is set and moderated.

PERSONAL INFORMATION					
Surname and Name/s	Tjikuzu Mbaunguraije				
Postal Address	PO Box 81559				
Tel Number(s)	0812020627				
Course (e.g. Economics 1)	Security Analytics		Course Code: SAS811S		
Exam Session/Date	December 2025		Signature		
Exam Type (1st/2nd Opportunity)	2nd Opportunity		Date: 16/10/2025		
		Question paper		Memorandum	
CATEGORY		YES	NO	YES	NO
1. Front cover: The following information is available on the front cover					
The name of the institution		X		X	
The department within which the course falls		X		X	
The name and level of the course		X		X	
The course code		X		X	
The examination session and the year			X		X
The duration of the paper		X		X	
The names of the Examiners and Moderator(s)		X		X	
Instructions to candidates, and such instructions are clear and unambiguous		X		X	
A list of all the material that is permissible for answering the question paper		X		X	
2. Standard of paper & memorandum					
The standard of the questions is satisfactory and appropriate to the level of the		X		X	
The question paper comprises a range of question types, i.e., recall, comprehension, analytical etc.		X		X	
The questions cover all parts of the approved syllabus.		X		X	
There is no repetition of questions		X		X	
The question paper is accompanied by a memorandum of model answers		X		X	
The model answers are of satisfactory standard and cover all aspects of the questions		X		X	
Where appropriate, alternative answers are provided		X		X	
The memorandum is designed in such a way that people other than an examiner can		X		X	
3. Language & Format Question paper & memorandum					
The instructions and the questions are clear and unambiguous		X		X	
Does the paper contain any grammatical and spelling errors			X		X
The paper is formatted clearly (e.g. questions are clearly separated)		X		X	
The marks for each question are allocated clearly in the right hand margin of the question paper & the memorandum		X		X	
The marks for each question, each section and the whole paper are calculated		X		X	