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 BHDS	**LEVEL:** 8
COURSE: ADVANCED INTRUSION AND LOG ANALYSIS	**COURSE CODE:** AIL811S
DATE: JULY 2023	**SESSION:** THEORY
DURATION: 2 HOURS 30 MINUTES	**MARKS:** 70

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	DR ATTLEE M. GAMUNDANI
MODERATOR:	MR NDANGI NASHIKU

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

Question 1: **[10 marks]**

A user in your organisation has reported that their email account has been hacked, and unauthorised emails have been sent from their account.

(a) What steps do you take to investigate the incident?

(b) How do you prevent similar attacks from occurring in the future?

Question 2: **[10 marks]**

Your organisation is preparing to implement a new security information and event management (SIEM) system.

(a) What factors should be considered when selecting a SIEM solution?

(b) What steps should be taken to ensure a successful implementation?

Question 3: **[10 marks]**

A vendor has notified your organisation that a hardware vulnerability exists in one of the servers you use.

(a) What steps do you take to patch the vulnerability and prevent exploitation by attackers?

Question 4: **[10 marks]**

A user in your organisation has reported that they have received a suspicious email attachment.

(a) What steps do you take to investigate the attachment?

(b) How do you prevent similar attacks from occurring in the future?

Question 5: **[10 marks]**

A security researcher has identified a vulnerability in one of your organisation's applications.

(a) What steps do you take to verify the vulnerability and remediate the issue?

Question 6: **[10 marks]**

A user in your organisation has reported that they have received a threatening email from an unknown sender.

(a) What steps do you take to investigate the email?

(b) How do you protect the user from further threats?

Question 7: **[10 marks]**

An attacker has gained access to your organisation's network and is attempting to exfiltrate sensitive data.

(a) What steps do you take to prevent the attacker from stealing the data?

(b) How do you ensure that the attacker is caught and prosecuted?

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