NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE (HONS DIGITAL FORENSICS)	
QUALIFICATION CODE: 08 BHDF	**LEVEL:** 8
COURSE: SECURITY ANALYTICS	**COURSE CODE:** SAS821S
DATE: NOVEMBER 2022	**SESSION:** THEORY
DURATION: 3 HOURS	**MARKS:** 90

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	DR ATTLEE M. GAMUNDANI
MODERATOR:	MR MBAUNGURAIJE TJIKUZU

THIS QUESTION PAPER CONSISTS OF 3 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) How does security analytics move beyond data gathering to its visualization? [2 marks]

(b) Why are tools and methods for security analytics never adequate to provide complete visualisation? [2 Marks]

(c) Identify and explain any two (2) key drivers of security analytics in today's business environment. [4 marks]

(d) What would you present as an argument for the increased hype in big data in the context of the business world today? [2 marks]

Question 2 [10 Marks]

(a) What does it mean to say Python is an interpreted programming language? [2 marks]

(b) The high-level overview of the steps for setting up and running a simulation in Arena are as follows:

1. Design and create the model,
2. Add data and parameters to the model,
3. Run the simulation, and
4. Analyse the simulation.

Explain what steps 1 and 3 entails in more detail. [8 marks]

Question 3 [10 marks]

(a) The dataset *M* consists of all possible email messages and the label is binary variable. Let the label 0 indicate a legitimate mail and the label 1 indicate a spam mail. A target function *f* (.) is required to tell us whether a particular email message *m* is a spam 1 or a legitimate mail 0. We search for a function *f* : *M* → {0, 1}, by training one of the machine learning algorithms on a set of *n* labelled messages {(*m*1,*l*1),(*m*2,*l*2),...,(*mn*,*ln*)}, where *mi* ∈*M* and *li* ∈{0,1} for 1≤*i*≤*n*.

i. What machine learning model is described here and why? [2 marks]

ii. Why is the model you indicated in (a) suitable for this typical cybersecurity application compared to its alternative? [2 marks]

iii. Which cybersecurity dataset example will not be applicable to use the model in (i) and why? [3 marks]

(b) SVM is a very popular machine learning model and is used for classification of both small- and medium-sized datasets. Identify at least three applications of SVM in cybersecurity [3 marks]

Question 4 [10 marks]

Machine learning (ML) techniques can analyse threats and respond to attacks and security incidents quickly in an automated way. Give and explain any five cybersecurity problems where ML techniques could be applied. [10 marks]

Question 5 [10 marks]

(a) Explain the meaning of an SQL injection attempt. [2 mark]

(b) Text mining techniques are particularly useful for unstructured data. Why are e-mail messages more ideal for text mining compared with network sniffers data? [4 marks]

(c) Explain any two methods of analysis you can apply for the client browser log data. [4 marks]

Question 6 [10 marks]

(a) There are a lot of interesting uses for simulations in security. One of them is evaluating the effect of security controls or mechanisms in your enterprise that otherwise would be difficult to recreate. As an Information Security Officer, who needs to evaluate different antivirus (AV) e-mail security gateway offerings. What will be the main thing you will be concerned about and in what ways will simulations help you? [6 marks]

(b) If it is possible to use simulations in security for recreating virus propagation within a network to see how fast, it will affect your enterprise. How else would you use simulations further in the same context? [4 marks]

Question 7 [10 marks]

(a) There could be scenarios whereby an attacker gains access to VPN credentials and subsequently have access to your internal resources. Give any four examples of such scenarios assuming there is no two-factor authentication. [8 marks]

(b) What is VPN? [2 marks]

Question 8 [10 marks]

(a) Explain any three Applications of Text Mining in Cybersecurity. [6 marks]

(b) What are the two key distinguishing features between Data mining and Text mining? [4 Marks]

Question 9 [10 marks]

(a) Why is Security intelligence being especially relevant in today's business world? [4 marks]

(b) Once you have your security intelligence, you have two options. Which are these two options? [2 marks]

(c) Think about how security intelligence can increase organisation XYZ's overall effectiveness and productivity. Present two arguments to organisation XYZ's management for them to take security intelligence seriously. [4 marks]

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