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: JANUARY 2023	**SESSION:** THEORY
DURATION: 3 HOURS	**MARKS: 90**

SECOND OPPORTUNITY/ SUPPLEMENTARY 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) **Explain the difference between Supervised Machine Learning and Unsupervised Machine Learning by giving one example of a technique for each.** **[8 marks]**

(b) **What would you summarise as the role of text mining in Security Analytics.** **[2 marks]**

Question 2 [10 Marks]

(a) **R is a full featured, object-oriented programming language, which is more than a scripting language to perform statistical calculations, besides the description provided so far, what makes R a very flexible and powerful tool for data analysts.** **[4 marks]**

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

(c) **Give and explain any two other features that makes Python more ideal for data analytics?** **[4 marks]**

Question 3 [10 marks]

The dataset $X = \{x1, \ldots, xl+u\}$ is divided into two sets, XL and XU. That is, $X = XL \cup XU$, where the points in $XL = \{x1,\ldots,xl\}$ are provided with the labels from $YL = \{y1,\ldots,yl\}$, and for the points in $XU = \{xl+1, \ldots, xl+u\}$, the labels are not known.

(a) **What Machine Learning model is presented here?** **[2 marks]**

(b) **Give two reasons why you classified the model as such in (a).** **[4 marks]**

(c) **which cybersecurity scenario would be ideal to apply the model you identified in (a) and why?** **[4 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) While deploying real-time intrusion detection and prevention defences is essential, it is not enough, why is this the case and what can security analysts do to help? [4 marks]

(b) Although there is no single standard for server log formats, there are, however, a few formats that are relatively common. Give four examples of server log formats. [4 marks]

(c) Of course, log files are not the only sources of data available for security analysis. Give any other source of data in an organisational network. [2 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]

How does VPN work? Explain with the aid of schematic diagrams. [10 marks]

Question 8 [10 marks]

(a) What is Text Mining? [2 marks]

(b) Identify and explain any two data mining styles [4 marks]

(c) Explain any two Text Mining Methods. [4 marks]

Question 9 [10 marks]

(a) There are many challenges when using security analytics, since the field is still evolving, and people are still trying to figure out how to effectively implement the techniques in their organization. Give and explain any three such challenges. [6 marks]

(b) Exploratory analysis is very valuable to increasing an organization's defences. Yet, the goal with security intelligence is to be able to conduct predictive analysis. Why is predictive analysis crucial? [4 marks]

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