SIT384

Cyber security analytics

Portfolio Learning Summary Report

Kenisha Corera
DFCS|DK|62|203

Self-Assessment Details

The following checklists provide an overview of my self-assessment for this portfolio.

	Pass (D)	Credit (C)	Distinction (B)	High Distinction (A)
Self-Assessment	✓	✓	✓	✓

(Tick ✓ the box with the grade you are applying for)

(Check that you have included the minimum required details. Tick these boxes and ones for higher grades as applies.)

Self-Assessment Statement

	Included
Learning Summary Report	✓
Pass tasks complete	✓

Minimum Pass Checklist

	Included
All Credit Tasks are Complete on OnTrack	✓

Minimum Credit Checklist (in addition to Pass Checklist)

	Included
Distinction tasks are Complete	✓

Minimum Distinction Checklist (in addition to Credit Checklist)

	Included
High Distinction tasks are Complete	✓

Minimum High Distinction Checklist (in addition to Distinction Checklist)

Declaration

I declare that this portfolio is my individual work. I have not copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part of this submission been written for me by another person.

Signature: **J.K.Corera**

Portfolio Overview

Work that shows I've met every unit learning outcome for the SIT384 unit title with a high distinction level is included in this portfolio.

The work in this portfolio demonstrates that all of the Unit Learning Outcomes (ULOs) for the SIT384 Cyber Security Analytics unit have been met with a High Distinction. I knew a little bit about cybersecurity data types and analysis going into this unit. I learnt how to use a variety of data analytical methodologies to several real-world cybersecurity concerns as I developed. Additionally, I developed a great deal of experience designing and evaluating data-driven cybersecurity solutions with Python.

I have been learning about the many data formats utilised in cybersecurity systems, such as JSON, CSV, and various log formats, since the start of this course. With this assurance, I can now handle threat detection and network traffic by understanding and utilising these formats in both stored and sent data.

I have examined cybersecurity datasets using regression models, K-means clustering, and other classification techniques like as Logistic Regression and K-Nearest Neighbours. As a result, I was able to prove both technical and non-technical staff alike that I can effectively communicate complex ideas in a report or presentation by finishing multiple assignments.

Utilising Python to leverage complex data analytics solutions was one of the unit's biggest achievements. To collect and analyse data sets and create a method for separating and categorising security occurrences, I wrote code. I was able to demonstrate my problem-solving abilities when I evaluated these solutions and optimised them in reference to relevant libraries like Pandas, Scikit-learn, and Matplotlib.

I took sure to include details and justifications for my work in my portfolio so that I could assess its quality critically in comparison to the predetermined standards. I was able to demonstrate that I understood the tasks assigned to me in their entirety and that my answers were adequate by examining the accuracy and efficacy of the majority of my models. I should add that maintaining this self-control was essential to preserving my peak performance at work.

Altogether, this portfolio displays a thorough comprehension of the subject of cyber security analytics. I think that my success in getting a High Distinction was a result of my ability to stay focused, observe how and what I was teaching by going beyond the course unit, and employ fresh ways.

Reflection

The most important things I learnt:

I believe that the two most significant things I learnt in this unit were the real-world applications of machine learning techniques for cybersecurity using K-Nearest Neighbours

and logistic regression on authentic datasets. Additionally, I have a solid understanding of how data type affects security and how Python can be used to filter and alter various forms.

The things that helped me most were:

It was discovered that a directory for reviewing Python programming tutorials and data analytics was quite helpful. Classification and clustering were the most beneficial exercises for me because they helped me remember the theory underlying each tactic and gave me some practical experience using various replies.

I found the following topics particularly challenging:

The present unit's two most difficult components were fine-tuning the parameters of machine learning models, particularly Random Forest and K-Nearest Neighbours. I occasionally had trouble determining what the best parameters would be, but as I kept practicing and learnt more about the subject, I was able to increase my model's efficacy.

I found the following topics particularly interesting:

Regarding the methods, the clustering algorithms—and the K-means technique in particular—piqued my curiosity. The fact that seeming equals may be categorised without the labels needing to be considered previously or predictively startled me. This has consequences for identifying cybersecurity threats.

I feel I learnt these topics, concepts, and/or tools really well:

I am certain that my understanding of Using Python for Data Analytics has not been compromised, since I have mastered the application of clustering and classification ideas through my use of Scikit-learn. In addition, I gained proficiency in the analysis and visualization of security data, which was essential for accurately completing the unit's assignments.

I still need to work on the following areas:

Gaining a deeper understanding of deep learning and its relationship to cybersecurity data is my goal here. Though I now have a solid foundation in "shallow learning," I am not pleased with the depth of the work, and I plan to focus more on deep learning since it may provide more complex solutions to the threat detection problem.

This unit will help me in the future:

After this session, I will be able to use these abilities to my next job as a cybersecurity analyst. To better understand and handle cyber threats, security data needs to be thoroughly analyzed and then categorized. When making decisions based on data, advanced security analytics jobs can benefit from knowledge of Python and machine learning methodology.

If I did this unit again I would do the following things differently:

If I could redo this unit, I would start by studying the theory behind each algorithm rather than attempting to implement them one at a time. That would enable me to complete the tasks with a deeper comprehension and might even result in the early development of better models.