Asia Pacific University of Technology and Innovation
Master Level
Security Operation Center and Incident Response
CT111-3-M-SOC
Assignment 1 (Group) – 50%

Course Learning Outcome:

CLO 1: Evaluate different SIEM solutions based on their embedded architectures and technologies (C5,PLO2)

CLO 2: Propose implementation of effective security operations center and incident handling procedure (A4,PLO4)

Organizations are continuously expanding their operations and opening new channels through which to serve customers and collaborate with business partners. This leads to a vast and complex array of systems, applications, data, and devices. At the same time, organizations face continuously evolving threats and an increasing set of regulatory pressures. The foundational technology of a Security Operation Center (SOC) is a **Security Information and Event Management (SIEM)** system, which aggregates system logs and events from across the organization. The SIEM uses correlation and statistical models to identify events that might constitute a security incident, alert SOC staff about them, and provide contextual information to assist investigation. A SIEM functions as a "single pane of glass" which enables the SOC to monitor enterprise systems.

Section A (Research): Submission on Week 5
Individual Component

When it comes to purchasing a SIEM solution, the market has an abundance of choice. From larger companies like IBM and Intel, to SolarWinds and SPLUNK, these solutions are made suitable for almost every size and style of company. There are also free open-source options, such as AlienVault OSSIM and Wazuh. **Each student is required to perform evaluation and research on ONE (1) SIEM solution in the current available market.** Include discussion on the embedded technologies that lie within each of the solutions.

Overview + Evaluation

Since you are working in a group, your research should then compare and contrast the selected SIEMs (with the one chosen by your team members) with rationalization on how different and advancement in technologies help in optimizing the performance of each of the solution. Include prediction on the future technology that can be embedded in a SIEM solution for the future threat and incident detection.

Comparison

Prediction

Section B (Proposal): Submission on Week 7
Group Component

Cyberattacks such as Ransomware and Distributed Denial of Service are increasingly becoming the norm. Without a functioning SOC, your organization could be at risk for major delays in detecting and responding to incidents. Keeping up with the growing rate of cybersecurity threats may seem impossible when your business is lacking in-house security resources and staff and a well-functioning Security Operations Center (SOC) can form the heart of effective detection. It can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively.

A well-designed and a truly effective SOC is also one that supports business objectives and effectively improves a company's risk posture which will provide a safe environment for the business to deliver on its core objectives in line with its strategic direction and vision.

Your task is to study the needs and requirements to have a SOC in ONE selected organization. Prepare a proposal that comprises the plan for implementation of an effective SOC in providing the best incident handling procedures to any possible cyber threats the organization might face.

Instructions:

This group assignment carries **50%** of your total assignment assessment marks. No marks will be awarded for the entire assignment if any part of it is found to be copied directly from printed materials or from another sources. All submissions should be made on or before the due date. Any late submissions after the deadline will not be entertained. **A zero (0)** mark will be awarded for late submission unless extenuating circumstances are upheld. The expected length is to be approximately 3,000 words plus diagrams and with all references clearly indicated and provided using the APA referencing convention.

Assessment Criteria:

Guidelines for the Report:

Document the results of your work in a **professional and systematic** manner, in the form of a **computerized report**. **Your completed report is to be submitted through the Online Submission Platform (Moodle)**.

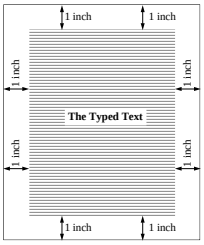
Your completed documentation should meet the following requirements:

1. Table of contents for every detailed chapter/section.
2. Introduction
3. Chapters / Sections
4. Conclusion
5. Appendices (if any)

6. Bibliography or References

In your document the report is to be written in a professional manner, paying due regard to the following aspects:

- The report should have a consistent layout and be divided into enumerated sections, sub-sections, sub-sub sections etc.
- The report should be fully referenced using the University standard.
- Your report must be typed using Microsoft Word with Times New Roman font and size 12 and it should be in 1.5 spaces.
- The report should have a one (1") margin all around the page as illustrated below:



- Every report must have a front cover. The front cover should have the following details:
  - Name
  - Intake code.
  - Subject.
  - Project Title.
  - Date Assigned (the date the report was handed out).
  - Date Completed (the date the report is due to be handed in).

Assessment Criteria:

Section A (Research) Individual:

- Documentation and Referencing 10%
- Selections of Solutions 10%
- Evaluation and Findings 20%
- Proposal for Future Technology 10%

Section B (Proposal) Group:

- Written Communication 10%
- Creativity 20%
- Ethics & Professionalism 20%

Marking Rubrics:

	1 to 2 (Fail)	3 to 5 (Pass)	6 to 8 (Merit)	9 to 10 (Distinction)
Documentation & Referencing (10)	All submission requirements were not adhered or poor writing or poor quality of contents. None, very little, or wrong usage of citation or not following proper referencing format.	Minimal submission requirements were with minimal quality of contents. Very little, with poor usage of citation or not following proper referencing format.	All submission requirements were followed with well writing and proper formatting of document along with proper quality of the content. Satisfactory format of referencing with needed citations in most required places.	All submission requirements were followed with very good writing and formatting. The quality of the content is very good. Proper, well formatted referencing with needed citations in all required places.
	1 to 2 (Fail)	**3 to 5 (Pass)**	**6 to 8 (Merit)**	**9 to 10 (Distinction)**
Selections of Solutions (10)	Poor selections of SIEM/Unable to identify the selection the appropriate SIEM solutions.	Satisfactory selections of the SIEM solutions. Minimal explanation provided on each SIEM solution.	Good selections of SIEM solutions. Satisfactory explanation and studies provided on each SIEM solution.	Excellent selections of SIEM solutions. Excellent explanation and investigation provided on each SIEM solution with outstanding research and studies has been performed.
	1 to 5 (Fail)	**6 to 10 (Pass)**	**11 to 15 (Merit)**	**16 to 20 (Distinction)**
Evaluation and Findings (20)	None or poor amount of critical evaluation presented on the selected SIEM solutions with poor or no demonstration of justification and validation presented.	Minimal critical evaluation presented on the selected SIEM solutions with satisfactory demonstration of justification and validation presented.	Good critical evaluation presented on the selected SIEM solutions with good demonstration of justification and validation presented.	Exceptional critical evaluation on the selected SIEM solutions with outstanding presentation of justification and validation presented.
	1 to 2 (Fail)	**3 to 5 (Pass)**	**6 to 8 (Merit)**	**9 to 10 (Distinction)**
Proposal for Future Technology (10)	Poor or inaccurate ideas for future technology to be embedded in a SIEM	Proposal consists of existing ideas for future technology to be embedded in a SIEM	Proposal consists of both existing and new ideas for future technology to be embedded in a SIEM	Proposal consists of fresh or new ideas for future technology to be embedded in a SIEM

	1 to 2 (Fail)	**3 to 5 (Pass)**	**6 to 8 (Merit)**	**9 to 10 (Distinction)**
Written Communication (10)	Not able to write ideas/proposal clearly	Able to write ideas/proposal with limited clarity. and require further improvements	Able to write ideas/proposal clearly. but require minor improvements.	Able to write ideas/proposal with excellent clarity and justification.
	1 to 5 (Fail)	**6 to 10 (Pass)**	**11 to 15 (Merit)**	**16 to 20 (Distinction)**
Creativity (20)	Not able to generate any new, creative idea that leads to an effective SOC.	Able to generate a few creative ideas with some help from lecturer or colleagues that leads to an effective SOC.	Able to generate a new, creative ideas that is or are relevant and appropriate that leads to an effective SOC.	Able to generate new creative ideas that have potential to be applied, has depth, quality and novel in nature that leads to an effective SOC.
	1 to 5 (Fail)	**6 to 10 (Pass)**	**11 to 15 (Merit)**	**16 to 20 (Distinction)**
Ethics & Professionalism (20)	Does not perform assigned tasks within the scope of work even with close supervision.	Perform assigned tasks within the scope of work with close supervision	Perform assigned tasks within the scope of work and meets expectation	Perform assigned tasks within by the scope of work and exceeds expectation