**SCHOOL OF COMPUTING**

**DIPLOMA IN INFOCOMM SECURITY MANAGEMENT (DISM) /** **DIPLOMA IN CYBERSECURITY & DIGITAL FORENSICS (DCDF)**

**Year 2**

**ST2610 Security Policy and Incident Management (SPIM)**

Warning: Plagiarism means passing off as one's own the ideas, works, writings, etc., which belong to another person. In accordance with this definition, you are committing plagiarism if you copy the work of another person and turning it in as your own, even if you would have the permission of that person. Plagiarism is a serious offence and disciplinary action will be taken against you. If you are guilty of plagiarism, you may fail all modules in the semester, or even be liable for expulsion.

|  |  |  |
| --- | --- | --- |
| **Module Code** | : | ST2610 |
| **Module Name** | : | Security Policy and Incident Management |
| **Academic Year/Semester** | **:** | AY2024/2025 Semester 2 |
| **Assignment Title** | **:** | Assignment 1 (Proposal of SIEM) |
| **Assignment Type** | **:** | Group (4 students) Report and Presentation |
| **Weightage** | **:** | 30% |
| **Deadline** | **:** | Week 6  22 November 2024, 11:59 pm (2359 hours) |
| **Deliverables** | **:** | Group Report and Group Presentation |
| **Submission Details** | **:** | 1. Deadline: End of Week 6, 22 November 2024 at 11:59 pm (2359 hours)    * Upload the softcopy to BrightSpace by 11:59 pm (2359 hours)    * Filename format: Class\_LeaderName\_Group No\_Assignment1.zip 2. Presentation on the following week (Week 7, 25 – 29 November 2024) |
| **Late submission** | **:** | 50% of the marks will be deducted for assignments that are received within ONE (1) calendar day after the submission deadline. No marks will be given thereafter.  Exceptions to this policy will be given to students with valid LOA on medical or compassionate grounds. Students in such cases will need to inform the lecturer as soon as reasonably possible.  Students are not to assume on their own that their deadline has been  extended. |

# Requirements

**Objectives:**

1. Research and perform comparative evaluation on SIEM products, and provide a solution proposal using the chosen SIEM product to collect and analyse logs from endpoint devices and include a vulnerability analysis (minimally 2 vulnerabilities) for endpoint devices
2. Propose an Incident Response plan with necessary details (e.g. escalation matrix, runbook) for Vortex Pte Ltd to handle cybersecurity incidents.

**Background:**

Vortex Solutions Pte Ltd is an SME (Small and Medium Enterprise) specializing in providing IT support and managed services for small businesses. The company employs between 50 to 100 individuals and has an annual revenue of approximately $17 million.

Vortex Solutions manages various client infrastructures, including setting up and maintaining servers, cloud environments, and endpoint devices. They handle sensitive client data, such as login credentials and business-critical files, through remote management tools and cloud storage solutions. Please refer to the diagram below for an illustration of the company's organizational structure.

CFO

(Mr Jeffrey Ho)

VP, IT

(Mr Josh Tang)

VP, Operations (Mr Tan Hiap Seng)

VP, Sales

(Mr Lim Kim Chan)

CEO

(Mr John Williams)

Applications & Infra

IT Support

Marketing Team

Executives

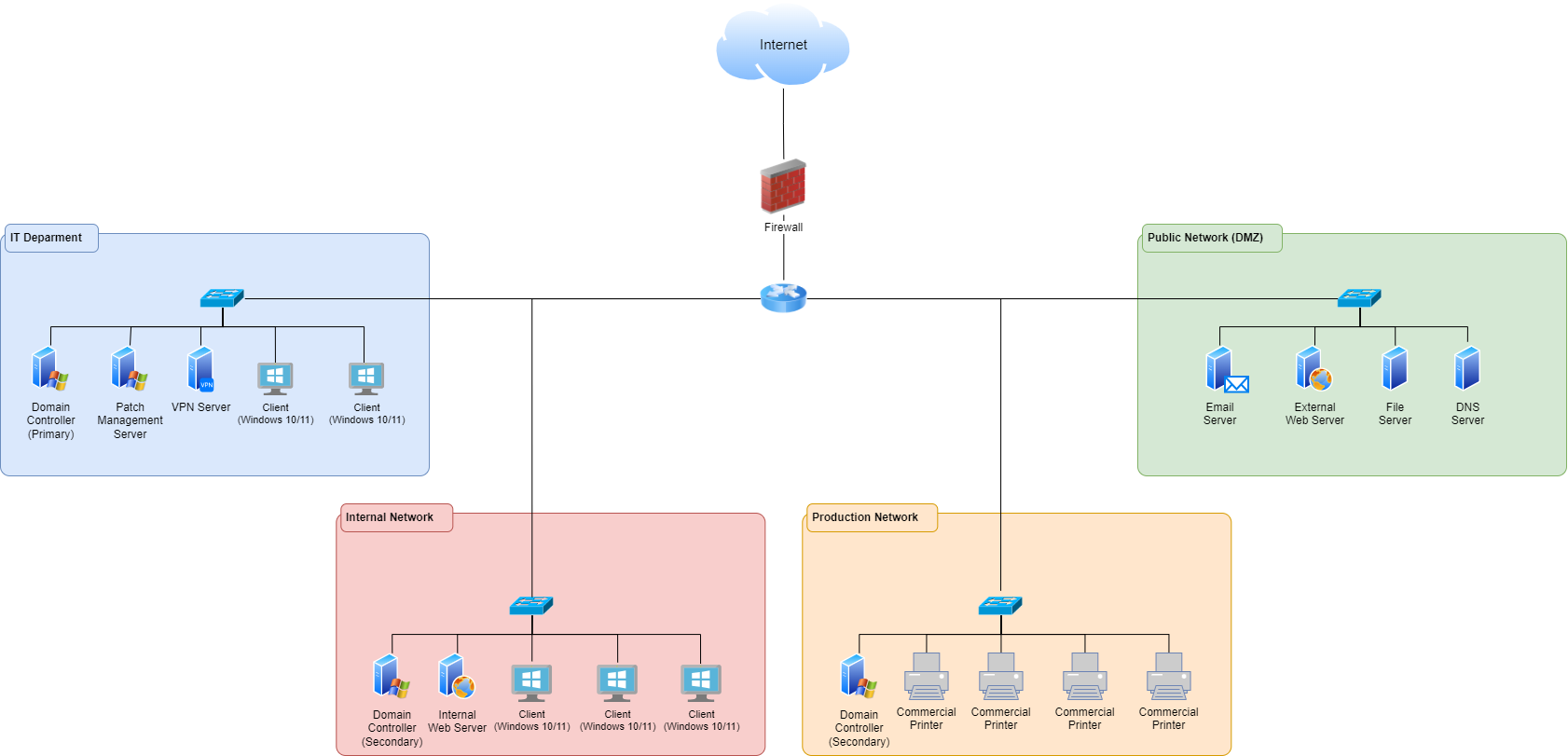
Security / CSIRT

Managed Security Product & Services

Sales Team

**Image 1**: Vortex Pte Ltd. Organization Chart

Client support requests are primarily received through their online ticketing system, but some are also received via email or USB flash drives containing diagnostic files and configuration backups from client machines. Employees often work remotely and connect to Vortex Solutions' IT network through VPN to manage clients’ systems and perform administrative tasks. The IT department's network has access to all other networks within the company. Please refer to the diagram below for a high-level overview of the company's network infrastructure.



**Image 2**: High-level overview of Vortex Pte Ltd infrastructure

You are a member of Vortex Pte Ltd's CSIRT (Computer Security Incident Response Team). Recently, the company has experienced several security incidents, including ransomware attacks, unauthorized access attempts, and malware introduced through infected USB flash drives received from clients. In one incident, a compromised USB drive led to the spread of malware across several client environments, causing significant data loss and system outages. Vortex’s lack of having an incident management plan led to chaos, panic, and in turn led them to losing customers.

Your team has been assigned the responsibility of addressing these security issues by developing and implementing a comprehensive incident response plan. You are tasked with evaluating current vulnerabilities—especially those related to external devices such as USBs—and proposing measures to detect, mitigate, and prevent future security breaches, ensuring the company’s operations remain secure.

The VP of IT has been approached by vendors regarding the adoption of a Security Information and Event Management (SIEM) solution. You and your team have been assigned the task of evaluating SIEM solutions to determine the most suitable option for Vortex and providing a recommendation.

# Deliverables

**Report (Solution Proposal)**:

The report should include a comparative evaluation of at least 4 SIEM products from Gartner’s Magic Quadrant, focusing on their design principles, architecture, functionalities, strengths, and limitations. It should propose a solution architecture for log collection and analysis of 200 endpoint devices.

The report should be at least **20 pages** (including the title page) and must include a table of contents, properly numbered sections, and APA references. Please use font size of 11. The report should have all pages numbered. All figures and tables should be numbered and captioned. There must be a title page with the names and Student IDs of group members at the beginning of the report.

**Presentation:**

You must prepare a 20-minute presentation based on your report. The presentation should be structured, and a 5-minute Q&A session will follow. Please ensure your presentation is within the

allocated time as this will count toward good time management which is part of the assessment criteria.

**Task details:**

1. As part of the security management team, your group is evaluating selected Security Information and Event Management (SIEM) products for possible procurement and implementation. You need to compare and evaluate **four or more** SIEM products listed in Gartner’s magic quadrant. Every team member should perform the assessment of at least 1 SIEM product.

Your assessment on the SIEM solutions should minimally include the following aspects:

* + **Design Principle**
    - What is the underlying design principle (e.g., scalability, ease of use, extensibility)?
    - Does it integrate well with third-party software?
  + **Architecture / Framework**
    - What are the key functional components of the product?
    - What are the resource requirements (e.g., number of servers)?
    - Can it be deployed on the cloud?
    - How does it handle data storage and event searching?
  + **Main Functionalities**
    - What are the core functionalities (e.g., Log Management, Threat Detection, User Behaviour Profiling)?
    - Are there dashboard features or analytics?
    - What data sources does it support?
    - What additional features does it offer (e.g., data collection, event correlation, real-time monitoring)?
  + **Features/Strengths/Advantages**
    - What are the product's key advantages and unique selling points?
    - How does it stand out from competitors?
  + **Limitations/Weaknesses**
    - What do users dislike or identify as shortcomings?
    - How does it compare to competitors in terms of missing features?
  + **Implementation and Deployment**
    - Propose an implementation plan based on the given infrastructure.
    - What limitations or considerations should be noted (e.g., resource management, shift rotation)?

1. As a team, you **must decide and recommend your choice of SIEM product**. Based on your choice of SIEM and knowing its capabilities, propose a solution architecture for collecting and analysing logs from **200 end point devices (which include servers, clients, network printers and network devices, etc.)** spread across the company. Your solution should minimally state:
2. How you will collect the logs from end point devices (i.e., logging component, logging frameworks, architecture etc.)?
3. How are you going to implement the proposed SIEM solution to the company’s infrastructure (i.e., proposed infrastructure of the SIEM, proposed implementation plan, resource and manpower management, etc.)?
4. What indicators of compromise will you be looking for to determine that an end point device has been compromised. You will need to do some research and gather intelligence on **2 vulnerabilities** that exist for end point devices.

Based on this, you will propose what are the rules you want to put in place to detect compromise.

1. Propose an Incident Response plan which may include the below. You may include other aspects that you deem necessary based on your research and your assessment of Vortex Pte Ltd’s needs.
2. Incident Response Team Structure
3. Incident Classification and Categorisation
4. Service Level Agreements
5. Escalation Matrix and Communications plan

Upon completion of the evaluation, your group should deliver a report on the above to the rest of the security team and the IT manager.

You must **list all reference sources in APA referencing style** for the information in your report. If the source is available o**nline,** please list the title/name, reference with the URL and date of last access.

**Remember to include the below in your report:**

1. **Task breakdown of team members based on the tables provided in Appendix A.**
2. **Declaration of Academic Integrity for each group member (repeat for each member), as provided under Appendix B. Each member must acknowledge the of use of AI tool(s) and/or other source(s) (where applicable).**

# Evaluation criteria:

|  |  |  |
| --- | --- | --- |
| **No.** | **Criteria** | **Percentage (%)** |
| 1 | Comprehensive Evaluation of SIEM Solutions | 15 |
| 2 | Insightfulness of Explanation | 15 |
| 3 | Proposed Solutions Architecture | 15 |
| 4 | Vulnerability Analysis | 10 |
| 5 | Background research | 5 |
| 6 | Proposed Incident Response Plan | 15 |
| 7 | Quality of report and presentation | 25 |

**APPENDIX A – TASK BREAKDOWN**

Summary table of research (to be included in your report submission in an appendix)

|  |  |  |  |
| --- | --- | --- | --- |
| Product Name: PRODUCT 1 | | | |
| Student Name/ID | Evaluation item | Description | Reference/Comments |
|  | Design |  |  |
|  | Architecture |  |  |
|  | Functionalities |  |  |
|  | Strength |  |  |
|  | Limitation |  |  |
|  | Other | Any other criteria (e.g. popularity, government-certified solution). |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Product Name: PRODUCT 2 | | | |
| Student Name/ID | Evaluation item | Description | Reference/Comments |
|  | Design |  |  |
|  | Architecture |  |  |
|  | Functionalities |  |  |
|  | Strength |  |  |
|  | Limitation |  |  |
|  | Other | Any other criteria (e.g. popularity, government-certified solution). |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Product Name: PRODUCT 3 | | | |
| Student Name/ID | Evaluation item | Description | Reference/Comments |
|  | Design |  |  |
|  | Architecture |  |  |
|  | Functionalities |  |  |
|  | Strength |  |  |
|  | Limitation |  |  |
|  | Other | Any other criteria (e.g. popularity, government-certified solution). |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Product Name: PRODUCT 4 | | | |
| Student Name/ID | Evaluation item | Description | Reference/Comments |
|  | Design |  |  |
|  | Architecture |  |  |
|  | Functionalities |  |  |
|  | Strength |  |  |
|  | Limitation |  |  |
|  | Other | Any other criteria (e.g. popularity, government-certified solution). |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Product Name: PRODUCT 5 | | | |
| Student Name/ID | Evaluation item | Description | Reference/Comments |
|  | Design |  |  |
|  | Architecture |  |  |
|  | Functionalities |  |  |
|  | Strength |  |  |
|  | Limitation |  |  |
|  | Other | Any other criteria (e.g. popularity, government-certified solution). |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Overall compilation of report, slides, proposed solution, incident response plan  (Please include name/id of students who are doing this) | | | |
| Student  Name/ID | Evaluation  item | Description | Comments |
|  | Report | [a section of report, or whole report] |  |
|  | Other |  |  |

**APPENDIX B – DECLARATION OF ACADEMIC INTEGRITY**

**<<*Remove this in your report.* Include the below declaration for each group member (repeat for each member). Each member must acknowledge the of use of AI tool(s) and/or other source(s) (where applicable).>>**

Declaration of Academic Integrity

Academic Integrity is a central tenet of Singapore Polytechnic. The polytechnic rules state that "Cheating in examinations and other assessed work is a very serious offence. This includes copying and using plagiarised material. Any student who cheats, attempts to cheat or breaches any rules for examinations and tests will face disciplinary action. The student is liable to be expelled."

Check **only one** of the two options below:

* I affirm that the work I submit is my own, produced without help from any AI tool(s) and/or other source(s).
* I affirm that the work I submit has been produced with the use of AI tool(s) and/or other source(s) which I have acknowledged fully in the [following section.](#_bookmark0)

By signing this form, I declare that the above affirmation made is true, and that I have read and understood the rules stated in Students Handbook on “[Plagiarism](https://www.sp.edu.sg/sp/student-services/osc-overview/student-handbook/intellectual-property-copyright-and-plagiarism)” and “[Breach of](https://www.sp.edu.sg/sp/student-services/osc-overview/student-handbook/conduct-in-examinations-breach-of-exam-rules) [Examination/Assessment Rules](https://www.sp.edu.sg/sp/student-services/osc-overview/student-handbook/conduct-in-examinations-breach-of-exam-rules)”.

|  |  |  |
| --- | --- | --- |
| Name:  Enter your name. | Student ID:  Enter your Student ID. | Class:  Enter your class. |
| Signature:  X | Date:  Click or tap to enter a date. | |

Acknowledgement of use of AI tool(s) and/or other source(s) (where applicable)

AI tool(s)

|  |  |
| --- | --- |
| **Name of AI tool** | < *For example, ChatGPT* > |
| **Input prompt** | < *Insert the question that you asked ChatGPT* > |
| **Date generated** | < *Insert the date that ChatGPT response was generated, since ChatGPT is an evolving technology* > |
| **Output generated** | < *Insert the response verbatim from ChatGPT* > |
| **Impact on submission** | < *Briefly explain which part of your submitted work was ChatGPT’s response applied* > |

Other source(s)

|  |  |
| --- | --- |
| **Source** | **Impact on submission** |
| < *Link to online source* > | < *Briefly explain which part of your submitted work the online source was applied* > |
| < *Author, Book / Article / Journal, Year, Pages* > | < *Briefly explain which part of your submitted work the Book / Article / Journal was applied* > |
| < *Student / Person name* > | < *Briefly explain which part of your submitted work the help of another student / person was applied* > |
| < *Others* > | < *Briefly explain which part of your submitted work the source was applied* > |