1. Objectives:

- Apply systems engineering concepts to design a robust cybersecurity system.
- Utilize UML/SysML to model the system architecture and processes.
- Implement Python automation scripts for various cybersecurity tasks.
- Integrate data analytics and machine learning for threat detection and response.
- Develop risk management and disaster recovery plans.

Team Responsibilities:

- Project Manager: Alexander Lee
- Systems Modelers: Susy Reyes / Mahsa Zarabi
- Python Developers: Ryan Rasool / Ebby Bejoy
- Data Analysts: Alicia Pongpunwattana / Raymond Le

2. Project Timeline:

Week	Date Range	Activities
5	09/30 - 10/04	Introduction to the project, group formation, and planning
6-8	10/07 - 10/25	System design and modeling using UML/SysML
9-10	10/28 - 11/08	Python scripting for automation and basic data analytics
11-12	11/11 - 11/22	Advanced data analytics and machine learning application
13	11/25 - 11/29	Risk management and disaster recovery planning
14	12/02 - 12/06	Final integration and testing
15	12/09 - 12/13	Project presentation and submission

3. Deliverables:

1. **System Design Document (Due Week 8):**

A report with UML/SysML diagrams illustrating system architecture, components, data flow, and security processes.

2. **Python Scripts and Automation (Due Week 10):**

Scripts for automating tasks such as log analysis, system monitoring, and basic threat detection.

3. **Data Analytics Report (Due Week 12):**

Analysis using real/simulated data demonstrating how the system detects and responds to threats.

4. **Risk Management Plan (Due Week 13):**

A strategy document outlining the system's risk management, incident response, and disaster recovery plans.

5. **Final Project Presentation and Submission (Due Week 15):**

A presentation summarizing system design, implementation, and findings. Submit all documentation, code, and slides.

4. Detailed Breakdown and Requirements:

Week 5: Project Kickoff and Group Formation

- **Activity:**

Introduction to the project, group formation, and initial topic discussion.

- **Output:**

Each group selects an organization type (e.g., financial, healthcare) and outlines the scope of their cybersecurity system.

- **Tasks:**
  - Form groups of 4-5 students.
  - Define the organization’s size, industry, and security challenges.
  - Create a project plan with milestones and assign roles.

Weeks 6-8: System Design and Modeling

- **Activity:**

Design the cybersecurity system using UML/SysML diagrams.

- **Output:**

System Design Document.

- **Tasks:**
    - Create use case, activity, and class diagrams using UML to model system requirements.
    - Develop block definition diagrams (BDD) and internal block diagrams (IBD) using SysML.
    - Create sequence diagrams to show data flow and control within the system.

Weeks 9-10: Python Scripting and Automation

- **Activity:**

Implement Python scripts to automate cybersecurity tasks.

- **Output:**

A set of Python scripts and a brief report explaining functionality.

- **Tasks:**
    - Create scripts for log file analysis, system performance monitoring, and alert generation.
    - Automate security checks like vulnerability scanning and network traffic monitoring.
    - Ensure error handling and logging for reliability.

Weeks 11-12: Data Analytics and Machine Learning

- **Activity:**

Integrate data analytics and machine learning into the system.

- **Output:**

Data Analytics Report and Python code.

- **Tasks:**

- Collect and preprocess relevant security data.
- Apply data analytics techniques to identify patterns and anomalies.
- Implement machine learning models for threat detection.
- Visualize findings using dashboards.

Week 13: Risk Management and Disaster Recovery

- **Activity:**

Develop a risk management plan.

- **Output:**

Risk Management Plan document.

- **Tasks:**
  - Identify potential risks and vulnerabilities.
  - Develop a risk assessment matrix.
  - Outline incident response procedures and disaster recovery plans.

Week 14: Integration and Testing

- **Activity:**

Integrate system components and conduct testing.

- **Output:**

Integrated system and test report.

- **Tasks:**
  - Integrate all components (scripts, analytics tools, etc.).
  - Perform unit, integration, and security testing.
  - Document issues and solutions.

Week 15: Project Presentation and Submission

- **Activity:**

Present the final project to the class.

- **Output:**

Presentation and final submission.

- **Tasks:**
  - Prepare a presentation summarizing system design and key findings.
  - Demonstrate system functionality through a live or recorded demo.
  - Submit all project documentation, code, and presentation slides.

5. Grading Criteria:

System Design and Modeling	25%
Python Scripting and Automation	20%
Data Analytics and Machine Learning	20%
Peer Evaluation	15%
Presentation and Integration	10%
Collaboration and Effort	10%

6. Assumptions:

- All teams will have access to necessary software (e.g., Python, data analytics tools, and UML modeling tools).
- Teams can either use real or simulated data to demonstrate the functionality of the cybersecurity system.

7. Constraints:

- The project must adhere to the outlined timeline.
- The system should address security issues relevant to the chosen organization type.

Questions for step 1)

Questionnaire for client:

- What type of threat was it?
- What was affected within the breach?
- Have the breaches resulted in data loss or corruption that couldn't be recovered?
- What was the previous level of security that was breached?
- Were firewalls implemented?
- Is this an ongoing problem?
- Who has access to this data/information? How often do the authorized personnel access/monitor the data?
- Is the data stored anywhere else/remotely?
- Is this data categorized/organized in any way?
- In person or remote attack?
- What cybersecurity tools are in place and protocols in place at the moment?
- When was the last comprehensive security audit performed on the system?
- What operating systems and software are used across the organization? Are they up to date?
- How is the organization currently responding to incidents? Is there an established incident response team or protocol?
- Have employees received regular cybersecurity training to recognize phishing, social engineering, and other types of attacks?
- How often is data backed up, and is it done in a secure, encrypted manner?
- Is there a disaster recovery plan in place (IDS/IPS)? How frequently is it tested?
- Did it pass past penetration testing?
- What improvements or upgrades are currently being considered or planned for the cybersecurity system?
- Is there a budget allocated for enhanced security measures?

- Are there any plans to adopt new technologies like artificial intelligence, machine learning, or advanced encryption for security enhancement?
- Are there any third-party vendors or partners that have access to sensitive data? If so, how is their security evaluated?

Answers:

- Meme of guy hipthrusting
- Data leak, passwords
- Yeh
- Doesnt have a clue
- Bro said mcafee
- Doesnt know
- Thumb drive but misplaced it
- Sus guy
- Mcafee again, use of python
- Poor level of security, no pen testing
- Finance loss: $3B

Planning steps:

- Secure data in a separate location to prevent further data leakage
- Locate all devices on network (Wi-Fi or LAN)
- View devices and personnel that has access to data and ability to change security settings
- Implement IDS and IPS