**Group Project Assignment for Week 5: Initial Planning**

**Assignment Description:**

This week, each group will work on initiating their group project by setting the groundwork for the system design. The tasks for the week are as follows:

1. **System Requirements**: Create a document outlining the **key requirements** for your organizational cybersecurity system. Consider aspects such as access control, incident detection, automation, and risk management.
2. **UML Diagrams**: Submit an initial **UML Activity and Use-Case Diagram** detailing your initial system design concepts. These should capture the core functions and structure of your system.
3. **Group Timeline**: Develop a detailed timeline for the project, identifying major milestones, deadlines, and responsibilities.
4. **Role Assignment**: Submit a document listing **group member roles** and a description of each person’s responsibilities. This should align with the group project agreement form.

**Deliverables:**

* **System Requirements Document** (1-2 pages)
* **UML Activity Diagram**
* **Group Project Timeline**
* **Role Assignment Document**

**Role Assignment:**

* **Project Manager:** 
  + **Kio**
* **Systems Modelers:**
  + **Milad**
  + **Markos Aklog**
* **Python Developers:**
  + **Ibrahim**
  + **Ar**
* **Data Analysts:**
  + **Denny**
  + **Mani**
  + **Sahil**

**SIT WITH YOUR GROUPS (RIP folks who did not show up)**

**Styles**

**Scenario for Group Project: Organizational Cybersecurity System**

**Your group has been hired as cybersecurity consultants by a mid-sized company in the financial services sector. The company recently experienced several cybersecurity incidents, including a data breach and unauthorized access to internal systems. Leadership is concerned about the company's overall security posture and has tasked your group with designing an organizational cybersecurity system that addresses key areas like access control, incident detection/response using data analysis, security compliance, and secure DevOps.**

**Keep in mind that, some of the systems you will need to implement for this project are:**

**• IDS/IPS**

**• DevOps pipeline**

**• Data Analysis Report**

**• Access Control**

**You will receive some initial information from the company, but much of the project will require you to ask questions and gather additional information as part of your requirements analysis. This will help you identify the specific needs of the company and tailor your system design accordingly.**

**The first group assignment will focus on initial planning, where you'll start gathering high-level requirements and mapping out the system concept using UML diagrams.**

# Functional requirements are highlighted

# Non-Functional requirements are kept the same

# Access Control

**Multi-Factor Authentication (2FA):**

* **Objective**: Enhance security by using 2FA
* **How**: Use a 2FA (Two Factor Authentication) system like Duo Security to authenticate user for extra security

**Strong Password Policies and Session Timeouts:**

* **Objective**: Enhance security by having a policy of users needing complex numbers and letters as their password. Implementing session timeouts would also drastically increase security, automatically logging the user off if inactive for a certain time to decrease the likelihood of unauthorized access.
* **How**: Use python to implement code to make users have at least 12 characters and 1 unique character.

**Access Logging and Audits:**

* **Objective**: Access log tracks who accessed the system and track actions done, this supports identifying unusual and suspicious behavior recording and tracking all data. Auditing logs helps us review and monitor our system.:

# 

# Incident detection/response

**Continuous Monitoring for Intrusions:**

* **Objective**: Detect signs of intrusion or suspicious activity in real-time.
* **How**: Use a **Security Information and Event Management (SIEM)** system like **Splunk** or **AlienVault** to continuously monitor network traffic, system logs, and user behavior for signs of suspicious activity.

**Automated Alerts:**

* **Objective**: Trigger immediate alerts to the security team when potential security incidents are detected.
* **How**: Configure real-time alerts within the **SIEM** system (e.g., **IBM QRadar** or **Splunk**) to notify the security team via email, SMS, or a centralized dashboard when predefined thresholds are crossed, such as unauthorized access attempts.

**Intrusion Detection and Prevention System (IDS/IPS):**

* **Objective**: Automatically block malicious activity and prevent suspicious IPs from accessing the network.
* **How**: Implement an **IDS/IPS** like **Snort** or **Suricata** to monitor and block suspicious network traffic in real-time. Configure the system to automatically block IP addresses linked to known malicious activities.

**Incident Response Workflow:**

* **Objective**: Ensure a structured and timely response to detected security incidents.
* **How**: Use an **Incident Response (IR) platform** like **Cortex XSOAR** or **TheHive** to automate and manage the incident response process, ensuring that steps like containment, investigation, and recovery are followed efficiently.

**Post-Incident Analysis:**

* **Objective**: Conduct a thorough analysis after incidents to understand causes and prevent recurrence.
* **How**: Use log data from the **SIEM** and **IDS/IPS** tools for root cause analysis. Generate reports with tools like **Splunk** or **Graylog** to review incidents and implement improved security measures based on findings.

# Automation

**Efficiency Through Automation:**

* **Objective:** Streamline cybersecurity operations to boost effectiveness and minimize mistakes when detecting and addressing risks.
* **How:** Utilize automated systems, for monitoring network activity that can identify behavior or indications of an attack scenario. These systems are capable of suggesting responses like notifying the team and can even take measures such as blocking an IP address or limiting access to protect the network.

**Access Control:**

* **Objective**: Manage access permissions to control who has the authority to access or alter information.   
  **How:** Utilize automated systems to check whether users possess the permissions to access files or systems effectively. If unauthorized entry is identified the system will block access, raise an alarm and eject the person from the network.

**Integration of DevOps in Automation:**

* **Objective:** Ensure that security testing is automated throughout the software development process to identify and address vulnerabilities prior, to the release date
* **How:** Utilize automated security tools that check the code for any issues while its being developed and alert the DevOps team if any vulnerabilities are detected so they can fix them before releasing the software.

**Use of Data analysis:**

* **Objective:** Automate data analysis to identify potential security risks, such as repeated failed login attempts or large data transfers that could indicate a breach.  
  **How:** By automatically detecting these risks, the system enables faster threat response, reduces overall risk, and enhances the security of the company's network.

# Risk management

**Regulatory Compliance:**

* **Objective**: Ensure the system adheres to financial sector regulations like **PCI-DSS**, **SOX**, and **GDPR**.
* **How**: Use compliance management tools such as **Tugboat Logic** or **OneTrust** to maintain regulatory standards. Regular audits with tools like **Vanta** or **LogicGate** ensure ongoing compliance.

**Vulnerability Identification and Mitigation:**

* **Objective**: Identify and fix vulnerabilities to protect the system from threats.
* **How**: Conduct regular vulnerability scans using **Nessus** or **Qualys** to find system weaknesses. Use **Microsoft WSUS** or **Chef Automate** for automated patch management, ensuring timely updates to fix vulnerabilities.

**Third-Party Vendor Security:**

* **Objective**: Manage security risks posed by third-party vendors.
* **How**: Use platforms like **SecurityScorecard** or **BitSight** to assess and monitor vendor security. Ensure vendors meet security standards through compliance checks, contractual agreements, and regular security audits.

**Proactive Security Measures:**

* **Objective**: Implement proactive measures like patch management, security audits, and multi-factor authentication (MFA) for added security.
* **How**: Use **Qualys Patch Management** for regular patching, conduct penetration testing with **Metasploit**, and deploy MFA solutions like **Duo Security** to secure high-risk systems.

**Continuous Monitoring and Automated Alerts:**

* **Objective**: Continuously monitor risks and respond to security incidents in real time.
* **How**: Deploy a **SIEM** solution like **Splunk** or **IBM QRadar** for real-time monitoring and automated alerts when threats are detected. Use platforms like **RiskWatch** for continuous risk assessments and adjustments.

****