Project 11

Project Objectives:

 Define the attacker type, attack method, target, and organizational context.

 Briefly outline the attack steps,referencing relevant MITRE ATTCCK .

Projects:

1. Incident Response Plan Development Objective: To create a comprehensive incident response plan that outlines procedures for identifying, managing, and mitigating security incidents effectively.

2. Incident Detection and Response Automation Objective: Automate responses to detected incidents.

3. Tabletop Exercises for Incident Response Readiness Objective: Conduct simulated incident scenarios to test readiness.

4. Real-Time Incident Monitoring and Management System

5. Threat Hunting Playbook Development Objective: Create playbooks for proactive threat hunting.

6. Daily Threat Intelligence Briefing Objective: Establish a daily briefing for the SOC team.

7. Incident Response Metrics and Reporting Objective: Measure and report on incident response effectiveness.

8. Malware Incident Response and Forensics Objective: Develop procedures for responding to malware incidents.

9. Third-Party Incident Response Management Objective: Manage incidents involving third-party vendors

10. Phishing Simulation and Training Objective: Enhance awareness of phishing threats

11. Collaboration with Other Teams Objective: Foster collaboration between SOC and other departments (e.g., IT, compliance).

Motivation

This project was chosen because it addresses a critical problem that organizations face when dealing with cybersecurity incidents. With the rise in cyberattacks and the increasing sophistication of hacking methods, organizations are becoming more vulnerable to cyber threats. The lack of an effective incident response plan or poor coordination between different teams often worsens the impact of these incidents, leading to financial losses, operational disruptions, and sensitive data breaches.

This project aims to develop a comprehensive and advanced incident response plan, automate detection and response processes, and improve coordination with internal and external teams. Implementing this project can reduce incident response time, minimize the impact of security breaches, and enhance overall preparedness for future threats.

Positive Impact on Society and Industry:

- Protect individuals’ and organizations' data from breaches.
- Strengthen customer and business trust in digital systems.
- Reduce financial losses caused by cyberattacks.
- Improve the efficiency of cybersecurity teams through training and simulations.
- Foster collaboration between departments and companies to build a safer digital environment.

Project Plan

1. Planning (Week 1):

- Define project goals.
- Analyze security requirements.
- Study MITRE ATT&CK framework.
- Assign roles and responsibilities.
- Select tools (Python, SIEM, SOAR).

2. Design (Weeks 2-3):

- Draw system architecture diagram.
- Design user interface (Wireframes).
- Prepare incident simulation scenarios.
- Design automated response playbooks.

3. Implementation (Weeks 4-6):

- Develop user interface (React).
- Build threat detection system (SIEM Integration).
- Develop automated response module (SOAR Integration).
- Create incident database.
- Set up training scenarios.

4. Testing and Evaluation (Weeks 7-8):

- Test incident detection.
- Simulate automated responses.
- Conduct incident drills.
- Evaluate performance (response time, accuracy).
- Collect feedback and improve system.