For Lab 3, Team 8 will be submitting the following documents for its document library:

Executive summary describing the document library content
This will be a single page summary of the of the documents in the document library.

Incident Response Terms and Definitions
This will be a 2-page list of cybersecurity-related terms and definitions taken both from the lecture on them and also additional topics from the internet.

Incident Response Plan
This will leverage the IR Plan template that was developed in class. The Content will include:
Section One - Introduction

- 12 Plan Overview
- 13 Objectives
- 14 Response Structure
- 15 Escalation Protocol
- 16 Recovery Support
- 17 Commitment to Principles
- 18 Alignment with Policy
- 19 Scope
- 110 Exclusions
- 111 Planning Scenarios
    - 1111 Limited or No Access to the Building
    - 1112 Loss of Data Communications, eg, WAN, Routers
    - 1113 Loss of Technology, eg, Computer Room, Network Services
    - 1114 Loss of People, eg, Illness, Death:
- 112 Recovery Objectives
- 113 Assumptions

Section Two – Incident Response and Management

- 21 Logical Sequence of Events
- 22 Local Incident Management Teams
    - 221 General Information
    - 222 Team Overview
    - 223 Local Incident Management Team
    - 224 Damage Assessment Team
    - 225 Regional Incident Management Team
    - 226 Threat Assessment Center
- 23 Incident Management Team Activities
    - 231 Local IM Team Activities
    - 232 Regional Incident Manager Activities
    - 233 Regional IM Executive Activities

Section Three – Notification, Escalation, and Declaration

- 31 Introduction
- 32 Notification Process Overview
    - 321 Initial Notification
- 33 Notification Process (Emergencies Only)
    - 331 Local IMT Notification and Notification of External Client, Vendor, and Business Partner
- 34 Incident Response Assembly Locations
- 35 Escalation Process (Emergencies Only)
- 36 Plan Authorization and Declaration
- 37 Declaration Process (Emergency Only)

Section Four – Incident Response Checklists

- 41 Key Personnel Contact List
- 42 Key Vendor Contact List
- 43 Initial Incident Response Checklist
- 44 Local Incident Management Team Task Checklist
- 441 Local Incident Management Team Meeting
- 45 Local Incident Manager Task Checklist
    - 451 Incident Response Recommended Actions
    - 452 Actions Following a Disaster Declaration
- 46 Local EOC Command Staff Task Checklist
- 47 Local EOC Operations Staff Task Checklist
- 48 Pre-Incident Preparations
    - 481 Actions Following an Incident and Prior to a Disaster Declaration Being Made
    - 483 Support for Local Incident Management Team Meeting
    - 484 Actions During and After the Disaster
    - 485 Post-Event Maintenance Activities

Section Five - Appendixes

- 51 Incident Management Forms

Incident Response Playbook

This will leverage the IR Playbook developed in class. A draft of the Playbook will include:

- Ransomware Incident Playbook
- Ransomware (Overview)
- Isolate & Contain
- Identify the Variant
- Assess Data Impact
- Notify Authorities
- Engage Legal and Communication Teams
- Backup and Restore
- Don’t Pay Ransom
- Conclusion

Threat Hunting Checklist

This will be developed based on class lectures and will include:

1 Preparation Phase:
- Identify and Document Objectives:
- Define the specific goals and objectives of the threat hunting exercise
- Assemble Threat Hunting Team:
- List the individuals and roles involved in the threat hunting process

2 Data Collection:
- Define Data Sources:
- Specify the sources of data to be monitored (logs, network traffic, etc)
- Data Aggregation:
- Detail how data will be collected and aggregated for analysis

3 Threat Intelligence Integration:
- Incorporate Threat Intelligence:
- Specify the threat intelligence feeds and sources to be used
- Determine how threat intelligence will be applied to enhance hunting

4 Tool and Technology Setup:
- Select Threat Hunting Tools:
- List the tools and technologies to be used for threat hunting
- Ensure they are properly configured and updated

5 Execution Phase:
- Continuous Monitoring:
- Outline the schedule and frequency of monitoring
- Specify the time duration for threat hunting exercises

6 Analysis Procedures:
- Behavioral Analysis:
- Describe methods for detecting abnormal behavior or deviations
- Signature-based Analysis:
- Explain how known threat signatures will be used in the analysis
- Anomaly Detection:
- Detail the approach for identifying anomalies in the data

7 Incident Response Planning:
- Incident Triage:
- Define the process for prioritizing and categorizing incidents
- Communication Plan:
- Outline how the team will communicate and escalate findings

8 Documentation and Reporting:
- Record Findings:
- Specify how identified threats and incidents will be documented

- Reporting Structure:
- Outline the structure and content of threat hunting reports
- Include key metrics and observations

9 Post-Threat Hunting Activities:

- Lessons Learned:
- Conduct a debriefing session to discuss lessons learned
- Continuous Improvement:
- Detail how the threat hunting process will be refined based on findings

10 Legal and Ethical Considerations:

- Ensure Compliance:
- Confirm that threat hunting activities comply with legal and ethical standards
- Privacy Measures:
- Detail how privacy of individuals and sensitive data will be protected

Threat intelligence with Heat Map

This will have two files to address this. One will be the pdf file of the Threat Intelligence connections to DRM, Strategic, Operational, People & Process, and Tactical from class. The other file will be information from the MITRE ATT&CK charts based on the known values from APT1, who was identified as being responsible for the RSA Security breach.

Tabletop Exercise Results

This will be driven from the class notes and execise, but the intial table of content is as follows:

1. Objective of the Tabletop Exercise:
   - Clearly state the goals and objectives of the exercise.
   - For example, testing incident response procedures or evaluating team coordination.
2. Scenario Description:
   - Develop a realistic scenario that aligns with potential threats.
   - Consider involving various departments and roles within the organization.
3. Roles and Responsibilities:
   - Define roles for participants and their responsibilities during the exercise.
   - Include the security team, IT staff, and relevant stakeholders.
4. Simulation Execution:
   - Detail the step-by-step execution of the tabletop exercise.
   - Include injects (simulated events) to prompt responses from participants.

SEIM Use Case

This will be driven from class notes, but the initial table of contents is as follows:

1. Introduction to SIEM:
   - Brief overview of SIEM (Security Information and Event Management).
   - Importance of SIEM in cybersecurity.
2. SIEM Use Cases:
   - Identify and describe specific use cases relevant to your organization.

- Examples may include:
  - Detection of abnormal login activity.
  - Anomaly detection in network traffic.
  - Malware detection and response.

3. Implementation Strategy:
   - Discuss how these use cases will be implemented in your organization.
   - Consideration of log sources, correlation rules, and incident response procedures.
4. Metrics and Key Performance Indicators (KPIs):
   - Define metrics to measure the effectiveness of each SIEM use case.
   - Establish KPIs for monitoring and improving security posture.

Incident Investigation Report

This is using the (Excel) template for an incident that was used as an earlier assignment and applying it to the incident from the class.

Incident Response Communications Plan

This communications plan will include:

1. Communications Channels:
   - Internal Communications
   - External Communications
2. Communication Protocols: Secure File Transfer
   - Escalation procedures
   - Escalation Contacts
   - Escalation Timelines
   - Escalation Criteria
3. Communication Plan
   - Internal Notification
   - Internal Communication
   - External Communications
   - Third Party Expert Engagement
   - Testing and Training

SOC Job Categories

An added document to document the expected knowledge, skills, and certifications for the new Security Operations Center.

- Tier 1 SOC Analyst
- Tier 2 SOC Responder
- Tier 3 SOC Threat Hunter
- Forensics
- Malware Reverse Engineering
- Threat Intelligence
- Engineering Support