Incident Response Plan

Task:

Develop and test an incident response plan for responding to security breaches.

What is an Incident Response Plan?

An incident response plan (IRP) is a structured approach for handling security incidents effectively. It helps organizations detect, respond to, and recover from cyberattacks, minimizing damage and downtime.

Steps to Develop an Incident Response Plan

1. Identify Key Stakeholders

Define the incident response team (IRT), including IT, security, legal, and management personnel.

2. Define Incident Categories

Classify incidents (e.g., malware infection, data breach, denial-of-service) and assign response priorities.

3. Establish Detection and Reporting Procedures

Implement monitoring tools and provide employees with guidelines for reporting security incidents.

4. Develop Response Strategies

Outline step-by-step actions for containing, eradicating, and recovering from different types of security breaches.

5. Test and Update the Plan

Conduct tabletop exercises or simulations to assess effectiveness and refine the plan as needed.

6. Document and Review Lessons Learned

After incidents, analyze the response process and update policies to improve future readiness.

Incident Response Resources:

- NIST Computer Security Incident Handling Guide: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- SANS Incident Handler's Handbook: https://www.sans.org/white-papers/33901/
- FIRST Incident Response Framework: https://www.first.org/