Hasan Sadiq

Task 3 (DEP)

Step 1:

Identifying Potential Security Incidents and Scenarios

Identify potential security incidents and scenarios that could impact the organization, such as:

Unauthorized access to sensitive data

Malware outbreaks

Denial of Service (DoS) attacks

Physical security breaches

Insider threats

Conduct a risk assessment to prioritize potential incidents based on likelihood and potential impact

Step 2:

Defining Roles and Responsibilities for the Response Team

Establish an incident response team (IRT) consisting of:

Incident Response Manager (IRM)

Security Analysts

IT Support Staff

Communications Specialist

Legal Representative

Define roles and responsibilities for each team member, including:

IRM: overall incident response strategy and coordination

Security Analysts: technical analysis and containment

IT Support Staff: system and network support

Communications Specialist: internal and external communication

Legal Representative: legal guidance and compliance

Step 3:

Developing Step-by-Step Response Procedures

Develop detailed, step-by-step response procedures for each identified incident scenario, including:

Initial response and containment

Incident analysis and assessment

Eradication and recovery

Post-incident activities (e.g., lessons learned, reporting)

Ensure procedures are aligned with industry best practices and regulatory requirements

Step 4:

Conducting Training and Simulation Exercises

Conduct regular training and simulation exercises to ensure the IRT is prepared to respond to incidents, including:

Tabletop exercises

Live simulations

Training on incident response tools and techniques

Review and update training programs regularly to ensure they remain relevant and effective

Step 5:

Reviewing and Updating the Plan Regularly

Review and update the incident response plan at least annually, or as needed, to ensure it remains relevant and effective

Solicit feedback from IRT members and stakeholders to identify areas for improvement

Update the plan to reflect changes in the organization, technology, or regulatory requirements

By following these key steps, the organization can develop a comprehensive incident response plan that minimizes damage and facilitates quick recovery in the event of a security incident.