Incident Response Playbook

1. Introduction

Cybersecurity incidents are increasing rapidly due to the growth of internet usage, cloud computing, and remote work environments. Organizations face constant threats such as phishing attacks, malware infections, ransomware attacks, and unauthorized access attempts. These incidents can lead to data loss, financial damage, and reputational harm.

Incident Response (IR) is a structured approach used by organizations to detect, investigate, respond to, and recover from cybersecurity incidents. Having a well-defined Incident Response Playbook helps security teams respond quickly and effectively, minimizing damage and ensuring business continuity.

This project focuses on designing an Incident Response Playbook covering common security incidents such as phishing attacks, malware infections, and unauthorized access attempts.

2. Project Objective

- Understand Incident Response processes
- Design a structured Incident Response Playbook
- Define roles and responsibilities during incidents
- Create response procedures for common cyber attacks
- Improve incident handling and recovery strategies

3. What is Incident Response?

Incident Response is the process of identifying, managing, and resolving cybersecurity incidents. The goal is to handle incidents in a way that limits damage, reduces recovery time, and prevents future attacks.

Goals of Incident Response:

- Detect incidents quickly
- Contain and stop threats
- Remove malicious components
- Restore affected systems
- Improve security posture

4. Incident Response Lifecycle

Preparation

This phase involves preparing the organization before an incident occurs. Activities include deploying security tools, training employees, creating response policies, and setting up monitoring systems.

Identification

In this phase, security teams detect and confirm whether a security incident has occurred. Detection methods include SIEM alerts, antivirus alerts, user reports, and log monitoring.

Containment

The goal of containment is to stop the spread of the attack. Examples include isolating infected systems, blocking malicious IP addresses, and disabling compromised accounts.

Eradication

This phase removes the root cause of the incident. Examples include removing malware, patching vulnerabilities, and removing malicious files.

Recovery

Systems are restored to normal operation. Examples include restoring backups, reconnecting systems to the network, and monitoring for reinfection.

Lessons Learned

After resolving the incident, teams analyze what happened and improve security measures to prevent similar incidents in the future.

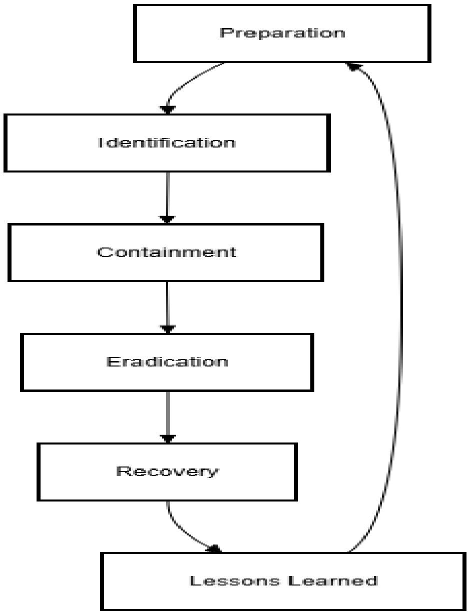

Fig. 1. Incident Response Lifecycle

5. Incident Response Team Roles

SOC Analyst: Monitor alerts and detect incidents
Incident Responder: Investigate and respond to incidents
IT Team: Restore systems and patch vulnerabilities
Management: Decision making and escalation
Legal/HR: Compliance and legal handling

6. Incident Playbook Scenarios

Phishing Attack Playbook

Identification:
- User reports suspicious email
- Email gateway detects malicious link

Containment:
- Block sender domain
- Quarantine email
- Disable compromised account

Eradication:
- Remove malicious emails
- Reset user passwords

Recovery:
- Restore user account
- Monitor login attempts

Lessons Learned:
- Improve email filters
- Conduct user awareness training

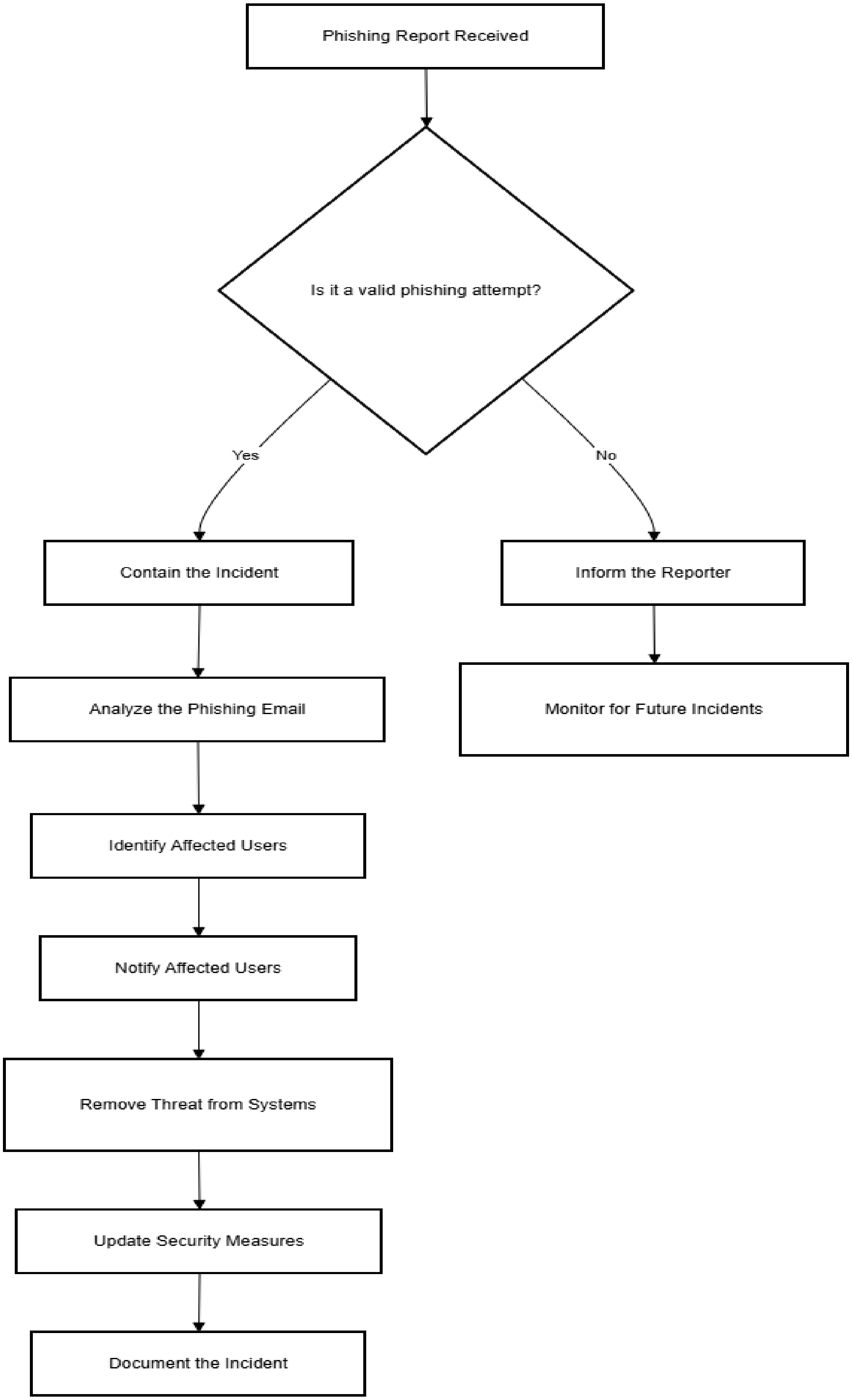

Fig. 2. Phishing Incident Response Flow

Malware Infection Playbook

Identification:
- Antivirus alert
- Unusual system behavior

Containment:
- Disconnect system from network
- Block malicious traffic

Eradication:
- Remove malware files
- Run full antivirus scan

Recovery:
- Restore system from backup
- Apply security patches

Lessons Learned:
- Update endpoint security policies

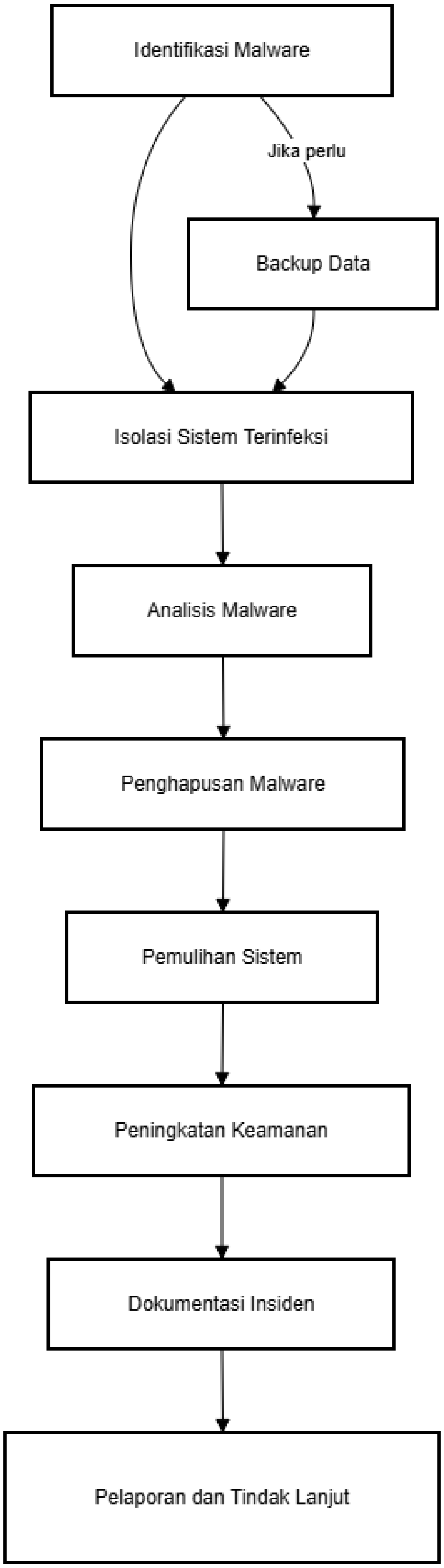

Fig. 3. Malware Incident Response Process Diagram

Unauthorized Access Playbook

Identification:
- Suspicious login alert
- Login from unknown location

Containment:
- Lock user account
- Force password reset

Eradication:
- Remove attacker access
- Check for data theft

Recovery:
- Re-enable secure access
- Monitor account activity

7. Tools Used in Incident Response

- SIEM Tools
- Endpoint Detection and Response
- Antivirus Software
- Firewalls
- Threat Intelligence Platforms

8. Communication Plan

Detection Stage: SOC Team
Confirmed Incident: IT and Management
Major Breach: Legal and Executive Management

9. Incident Severity Levels

Low: Minor issue with no major damage
Medium: Limited system impact
High: Multiple systems affected
Critical: Business operations impacted

10. Conclusion

Incident Response Playbooks are essential for organizations to handle cybersecurity incidents effectively. By following structured procedures, organizations can minimize damage, recover quickly, and strengthen their security posture. This project demonstrates how standardized response procedures can help security teams manage common cyber threats efficiently.

11. Author

Name: Anirudha G Kulkarni

Domain: Cybersecurity

Project: Incident Response Playbook