Incident Response Plan

Detection

Use a SIEM (Security Information and Event Management)

- Collect information from devices, servers, and users in real time
- Log information in one place, organize it, and determine of a threat is imminent
- Find any common patterns or correlations to sort into common relationships quickly
- Track usual login attempts
- Use automated systems to warn security team about threats

Containment

Using smaller networks within the entire organization

- Smaller networks could help alleviate large breaches
- Prevent malware from spreading across the organization
- If one section is infected with malware, you can disconnect it from the greater network

Eradication

System Wipes

- In the event of malware breaches, wipe all the machines infected
- Wiping machines will ensure that no further damages could be done to the system
- Re-image machines to keep the integrity of physical hardware

Recovery

Backup

- Twice a month, create trusted backups of system data
- In the event of a breach, reinstall backups to servers after the hardware is wiped.
- Monitor these systems carefully before fully integrating them back to the network

DDOS

Distributed Denial of Service

- Overwhelms a network with traffic, rendering it useless.
- Some examples of this is sending large amounts of fake requests or flooding vulnerabilities within a network
- DDOS attacks prevent real users from accessing services due to the sheer amount of traffic.

Security Policy

Rules

1) Create a strict hierarchy of data access within the organization

- Categorize information as public, internal, or confidential
  - Public information can be released to the public
  - Internal information is strictly only for employees
  - Confidential information is only for certain groups of employees
- Use protocols like multi-factor authentication
- Audit security protocols often; Twice a month

2) Keep strict data encryption policies

- Use AES-256 encryption for everything

3) Regularly update software and hardware