W! O! R! M!

Malware Outbreak Attack Response Plan

The Facts Were These: A worm spreads through the internal network due to a vulnerability in an outdated service.

Below is a breakdown of each phase of the plan and a rough estimate of the timeline starting from the detection of the threat to the recovery stage.

Immediate Actions (0-30 minutes)

Detection

Endpoint detection and response (EDR) alerts.
Unusual network traffic patterns.
Multiple systems showing similar symptoms.
Antivirus alerts across multiple endpoints.

Initial Response

Isolate affected systems from network immediately.
Prevent lateral movement through network segmentation.
Activate incident response team.
Begin malware sample collection.

Containment (30 minutes - 2 hours)

Network Isolation

Segment network to prevent malware spread.
Block malicious domains and IP addresses.
Disable vulnerable services and protocols.
Quarantine affected systems.

Endpoint Protection

Deploy additional antivirus signatures.
Enable enhanced monitoring on all endpoints.
Restrict user privileges and access.
Implement application whitelisting if possible.

Investigation (2-8 hours)

Malware Analysis

Identify malware family and capabilities.
Analyze infection vectors and propagation methods.
Determine malware objectives and payload.
Assess potential data compromise.

Forensic Analysis

Preserve infected systems for analysis.
Analyze network logs for malware communication.
Review email logs for malware distribution.
Document timeline and scope of infection.

Recovery (8 hours - several days)

System Remediation

Remove malware from infected systems.
Patch vulnerabilities exploited by malware.
Rebuild severely compromised systems.
Restore data from clean backups.

Validation

Conduct comprehensive malware scans.
Verify system integrity and functionality.
Test security controls and monitoring.
Validate network segmentation and access controls.

Communication:

- **Internal**
  - Notify executive leadership and stakeholders.
  - Inform legal and compliance teams.
  - Update employees on system availability.
  - Coordinate with IT operations team.

- **External**
  - Report to law enforcement if required.
  - Notify regulatory bodies as needed.
  - Coordinate with security vendors.
  - Update customers if services are affected.

Post-Incident

Update malware detection signatures.
Implement improved endpoint protection.
Conduct security awareness training.
Review and update incident response procedures.