# Ransomware Incident Response – NIST 800-61 Scenario

## Overview
This scenario outlines the response to a ransomware attack where a workstation becomes encrypted and displays a ransom note. The attacker uses a phishing email or vulnerability exploitation to deploy ransomware across the local system.

# 1. Preparation
- Maintain offline, encrypted backups of critical systems.
- Ensure EDR tools are deployed and configured for ransomware monitoring.
- Confirm logging for:
  - Windows Event Logs
  - PowerShell Logging
  - Sysmon (if enabled)
  - File integrity monitoring
- Apply least-privilege principles for user accounts.
- Validate patch management schedule for OS and software.
- Train users on suspicious attachments and macro-enabled documents.
- Maintain IR toolkit: offline backup drives, Sysinternals, forensic imaging tools.

# 2. Detection & Analysis

## Initial Indicators
- User reports files renamed or locked.
- EDR generates alerts for:
  - Mass file modification
  - Unexpected encryption activity
  - Suspicious PowerShell commands
- System displays ransom note.
- Network share activity spikes.

## Evidence Collection
- Capture ransom note.
- Collect impacted host information (hostname, user, IP).
- Verify encryption scope:
  - Local folders
  - Network shares
  - External drives
- Obtain logs:
  - Windows Security logs

  - PowerShell transcript logs
  - Autoruns
  - Prefetch files
- Identify ransomware family via hash lookup.

## IOC Examples
Indicator Type	Value
File Extension	.locked, .crypted, .enc
File Hash	SHA256: (example placeholder)
Process	powershell.exe -enc ...
Network Activity	Outbound traffic to suspicious IP: 46.17.250.163

## Triage Severity
High — Immediate threat to data integrity and business continuity.

# 3. Containment

## Short-Term Containment
- Immediately disconnect the infected system from the network.
- Disable user account of affected workstation.
- Block associated C2 domains and IPs.
- Disable SMB for the affected machine.
- Warn IT/security team to monitor for lateral movement.

## Long-Term Containment
- Patch exploited vulnerabilities.
- Block malicious binaries or hashes via EDR.
- Disable macros enterprise-wide (if malware used Office files).
- Reset compromised credentials.

# 4. Eradication
- Remove ransomware binaries from the system.
- Kill malicious processes.
- Remove persistence mechanisms:
  - Scheduled tasks
  - Startup registry keys
  - Services created by the malware
- Reimage workstation if necessary (common practice).
- Verify full cleanup before reconnecting to network.

# 5. Recovery
- Restore data from offline backups.
- Validate integrity of restored files.
- Rejoin system to the network after EDR verification.
- Monitor impacted systems for 72 hours.
- Re-enable account access with stronger MFA and password.

# 6. Lessons Learned
- Identify vulnerabilities exploited.
- Evaluate EDR detection gaps.
- Improve patching cadence if needed.
- Update ransomware playbook with new IOCs.
- Add detection rules to SIEM for:
  - Mass file modifications
  - Shadow copy deletion
  - Unusual PowerShell usage

# MITRE ATT&CK Mapping

Technique	ID	Description
Initial Access	T1566	Phishing attachment
Execution	T1059	PowerShell-based execution
Impact	T1486	Encrypting data for impact
Privilege Escalation	T1068	Exploited OS vulnerability
Lateral Movement	T1021	SMB and RDP movement

# Final Reporting Checklist
- Infection vector identified
- Encryption scope documented
- Ransom note captured
- IOC list completed
- Containment and eradication steps recorded
- Backup restoration confirmed
- Final incident report delivered