**playbooks/ Folder Content**

**1. Brute Force Attack Response → brute-force-playbook.md**

# 🛡️ Brute Force Attack Incident Response Playbook

## Detection

- Triggered by SIEM rule: Multiple failed logins from same IP/user within short time window.

## Triage

- Confirm if activity is from internal/external source.

- Check time pattern (short bursts vs long-term attempts).

- Review login success/failure logs.

## Containment

- Block offending IP at firewall.

- Disable affected accounts temporarily.

- Enforce MFA for exposed accounts.

## Eradication

- Reset passwords for impacted users.

- Patch vulnerable services (e.g., RDP, SSH).

## Recovery

- Re-enable accounts after securing credentials.

- Monitor for repeated attempts.

## Lessons Learned

- Implement account lockout policies.

- Review SIEM thresholds.

- Enhance monitoring for credential stuffing.

**2. Ransomware Response → ransomware-playbook.md**

# 🛡️ Ransomware Incident Response Playbook

## Detection

- Triggered by SIEM rule: Unusual file extensions (.locked, .encrypted).

- Sudden surge in file modifications.

## Triage

- Identify affected hosts and users.

- Check for suspicious processes (e.g., vssadmin delete shadows).

- Verify if encryption is still ongoing.

## Containment

- Immediately isolate infected machines from the network.

- Stop suspicious processes.

- Disable SMB shares.

## Eradication

- Remove malware from affected endpoints.

- Use clean backups to replace encrypted data.

- Apply OS and software patches.

## Recovery

- Restore data from offline backups.

- Gradually reintroduce systems to the network.

- Monitor for residual threats.

## Lessons Learned

- Strengthen email filtering.

- Conduct phishing awareness training.

- Regularly test backup and restore procedures.

**3. Suspicious DNS Requests Response → dns-playbook.md**

# 🛡️ Suspicious DNS Requests Incident Response Playbook

## Detection

- Triggered by SIEM rule: Queries to malicious or unusual TLDs (.ru, .top, .xyz).

## Triage

- Identify source IP/device.

- Validate if domain is in threat intel feeds.

- Check if traffic volume is abnormal.

## Containment

- Block malicious domains at DNS/firewall.

- Isolate compromised endpoints if C2 activity is suspected.

## Eradication

- Run malware scans on affected systems.

- Remove persistence mechanisms.

## Recovery

- Resume normal network connectivity once clean.

- Strengthen DNS filtering policies.

## Lessons Learned

- Integrate TI feeds with SIEM.

- Apply DNS sinkholing where possible.

**4. Privilege Escalation Response → privilege-escalation-playbook.md**

# 🛡️ Privilege Escalation Incident Response Playbook

## Detection

- Triggered by SIEM rule: Event ID 4672 with suspicious privileges.

## Triage

- Verify if escalation attempt was legitimate (admin activity vs attacker).

- Correlate with login times and account usage.

## Containment

- Disable suspicious accounts.

- Stop processes running with escalated privileges.

## Eradication

- Remove unauthorized accounts/roles.

- Patch vulnerabilities exploited for escalation.

## Recovery

- Reinstate services with proper accounts.

- Audit privilege assignments.

## Lessons Learned

- Enforce least privilege principle.

- Review AD privilege assignments regularly.