Triage Playbooks

1. Failed RDP Logon (Rule 100010)

Investigation Steps

- Check source IP and username in the alert.
- Verify if multiple failed attempts are seen from same IP/user.
- Confirm if the user account is valid.

Escalation Criteria

- 10 failed attempts in 10 minutes.
- Login attempt from unusual country or TOR exit node.

Closure Conditions

- Single failed attempt, user confirms mistyped password.
- Source IP is internal and trusted.

Decision Flow

- Is it repeated (>10 failed attempts in 10 minutes) + external IP? → Escalate.
- Otherwise → Close.

2. GPO Modification (Rule 100014)

Investigation Steps

- Identify which GPO was modified.
- Verify the modifying user and compare against change window.

Escalation Criteria

- Modification outside scheduled change window.
- User is not part of Domain Admins/authorized change team.

Closure Conditions

- Change approved in maintenance ticket.
- Confirmed by AD admin as legitimate.

Decision Flow

- Change authorized and documented → Close
- Unauthorized or suspicious → Escalate

3. PowerShell Encoded Command (Rule 100102)

Investigation Steps

- Review command line (-enc string).
- Identify parent process launching PowerShell.
- Check if script hash matches know whitelist

Escalation Criteria

- Suspicious parent (Word, Excel, Outlook).
- User not an admin but executing encoded commands.

Closure Conditions

- Script is a known internal IT/admin script.
- User is from IT support executing routine task.

Decision Flow

- Encoded command from non-IT user → escalate.
- Known IT script → close.

4. LSASS Access Attempt (Rule 100100)

Investigation Steps

- Check process attempting to access lsass.exe.
- Compare with baseline of legitimate processes.

Escalation Criteria

- Process is Mimikatz or unknown tool.
- Multiple access attempts from same host.

Closure Conditions

- Known security product (AV, EDR) accessing LSASS.
- Admin confirms legitimate memory dump for troubleshooting.

Decision Flow

- Legitimate security tool? → Close.
- Unknown tool/process? → Escalate.

5. Shadow Copy Deletion (Rule 100104)

Investigation Steps

- Check command line for vssadmin delete shadows.
- Identify initiating user and process.

Escalation Criteria

- User not a backup admin.
- Command followed by other suspicious activity (file encryption alerts).

Closure Conditions

- Scheduled backup cleanup verified with IT.
- Legitimate storage maintenance task.

Decision Flow

- Was it expected/approved cleanup? → Close.
- Unexpected deletion → Escalate.