Workflow

1. Alert Detection (SIEM – Wazuh)

- Wazuh detects suspicious PowerShell execution on a Windows endpoint.
- Alert generated with High priority (Alert ID: 004).
- Initial metadata captured: timestamp, source IP, process name, command line.

2. Initial Triage

- Validate alert type and severity.
- Identify affected asset (Victim: 10.0.2.22).
- Identify potential source (Attack machine: 10.0.2.19).
- Check if PowerShell execution aligns with normal business activity.
- Confirm alert is not a false positive.

3. Analysis and Scope Accessment

- Review Windows Security logs.
- Analyze PowerShell command-line arguments.
- Determine whether execution was interactive or remote.

4. IOC Validation (Threat Intelligence)

- Cross-reference source IP (10.0.2.19) in VirusTotal
    - Result: No malicious verdicts.
- Cross-reference same IP in AlienVault OTX
    - Result: No confirmed malicious pulses.

5. Behavioral Analysis

- Assess technique used (PowerShell execution bypass or suspicious commands).
- Evaluate risk of fileless attack, lateral movement, or post-exploitation.
- Determine that behavior is suspicious despite clean IOC reputation.

6. Risk Assessment

- Combine SIEM alert severity + behavior analysis + internal network.
- Determine High risk due to:
    - Living-off-the-land technique
    - Internal source IP
    - High-value victim asset

7. Containment

- Isolate victim machine (10.0.2.22).
- Temporarily restrict PowerShell execution.
- Monitor attacker system (10.0.2.19) for additional suspicious activity.

8. Remediation & Recovery

- Remove any unauthorized scripts or scheduled tasks.
- Apply endpoint hardening and PowerShell logging enhancements.
- Reset credentials if compromise suspected.

9. Documentation & Closure

- Document findings in case management tool.
- Update incident status and resolution notes.
- Close alert after validation and remediation.