Workflow

1. Tools Used

- Wazuh – Alert monitoring and event visibility
- VirusTotal – File/IP/hash scanning

2. Workflow Steps

- **Identify Alert in Wazuh**
    - Log in to the Wazuh dashboard.
    - Navigate to All Alerts
    - Filter by keyword: “SSH”, “Brute-force”, or alert ID.
    - Open the alert details panel and document the alert

- **Analyze Event Details**
    - Check frequency: How many failed SSH login attempts?
    - Check destination host and user accounts targeted.
    - Review log sample included in the Wazuh alert.
    - Assess whether attempts are internal or external (LAN/WAN).
    - Check if attempts come from a known admin scanning tool (prevent false positives).

- **Threat Intelligence Validation in VirusTotal**
    - Go to: virustotal.com then IP Address Search
    - Enter: 10.0.2.19
    - Check:
        - Community score
        - Malware communications
        - Any flagged suspicious behavior

- **Decision Making**
    - **If IOC is malicious (True Positive):**
        - Escalate alert to High priority.
        - Block IP at the firewall or WAF.
        - Check for successful logins.
        - Force password reset of targeted accounts.
        - Create incident in TheHive.
    - **If IOC is genuine (False Positive):**
        - Document reason.
        - Close alert with resolution notes.
- **Documentation the incident**

3. Summary Findings

Summarise your findings.