Use Case 1: File Integrity Monitoring (FIM) – Ubuntu Agent

Objective:

Detect unauthorized or unexpected modifications to critical system files on a Linux server using Wazuh File Integrity Monitoring (FIM). This simulates insider threats, privilege abuse, or persistence techniques commonly observed in real-world attacks.

Environment:

Monitored Host: Ubuntu Agent
Detection Tool: Wazuh FIM
Critical Files Monitored: /etc/passwd, /etc/shadow, /etc/sudoers, /root
Attack Source: Local modification (simulated)

Step 1: Configure FIM

Add the files or directories to monitor in the agent configuration (ossec.conf).
Ensure the FIM module is enabled and the Wazuh agent is running.
Check status with /var/ossec/bin/ossec-control status.

Step 2: Baseline Creation

Wazuh records the initial state of all monitored files.
The baseline is used to compare and detect any future changes.

Step 3: Attack Simulation

Manually modify a critical file, for example: sudo nano /etc/passwd and add a test line.
This simulates insider misuse, unauthorized administrative access, or persistence attempts.

Step 4: Detection & Alert

Wazuh detects the file modification.
An alert is generated and sent to the Wazuh Manager and Dashboard.
The alert includes the file path, type of change, timestamp, rule ID, and severity level.

Step 5: SOC Investigation

Review the alert to identify:
What changed? Critical file modification
Where? Ubuntu Agent
When? Timestamp in alert
Severity? Level assigned by Wazuh rule
Analyst determines whether the change was authorized or suspicious.

Evidence to Collect:

Screenshot of the FIM alert in the Wazuh Dashboard
Name of the modified file
Timestamp of the change
Wazuh Rule ID

MITRE ATT&CK Mapping:

T1078 – Valid Accounts (if modification attempts privilege escalation)

T1550 – Use of Alternate Authentication Material (if used for persistence)

SOC Relevance:
Demonstrates the SOC's ability to detect unauthorized file changes
Helps identify insider threats or malicious activity early
Monitors system integrity in real-time and alerts analysts before attackers escalate privileges