**1) Law\_Enforcement\_SOC\_Incident\_Response\_Plan.docx**

**Law Enforcement SOC Simulation Project – Incident Response Plan (Wazuh-Based)**

**Environment in scope:**  
Windows host running **Docker Desktop** (Wazuh **manager / indexer / dashboard**) + **Ubuntu 22.04 WSL** with **Wazuh agent** reporting to local manager.

**1. Preparation**

* Keep Wazuh containers healthy (manager, indexer, dashboard).
* Confirm **Ubuntu WSL agent** heartbeat daily in Dashboard → Agents.
* Record key paths for reference:
  + Agent config: /var/ossec/etc/ossec.conf
  + Agent log: /var/ossec/logs/ossec.log
* Capture baseline screenshots of the Dashboard and **Agents** page for comparison.
* Back up compose files before changes.

**2. Identification**

Use Wazuh Dashboard → **Security Events / Threat Hunting** to spot new alerts. Validate with logs:

* Manager: (dashboard events visible)
* Agent: tail -n 50 /var/ossec/logs/ossec.log

Typical indicators already observed in this lab:

* **PAM login session opened** (auth activity)
* **File integrity checksum changed** (FIM)
* **Netstat port status changed** (service/port opened/closed)
* **Partition usage 100%** (resource exhaustion)
* **CIS Benchmark results** (compliance)

Map to MITRE ATT&CK in the Dashboard to understand tactic/technique.

**3. Containment**

* If activity is suspicious, temporarily **isolate the WSL endpoint** from network (e.g., stop the process/service causing noise; block inbound where appropriate).
* Pause risky test activity on Parrot OS (if in use).
* Preserve evidence (screenshots of alerts, relevant log excerpts).

**4. Eradication & Recovery**

* Address the cause (e.g., remove misconfig, close exposed port, free disk).
* Apply package updates on Ubuntu:
* sudo apt update && sudo apt upgrade -y
* Restart agent to confirm clean state:
* sudo /var/ossec/bin/wazuh-control restart
* Verify in Dashboard → **Agents** (status **Active**) and confirm alerts stop/normalize.

**5. Lessons Learned**

* Log the incident timeline and actions in Monday.com (day comment).
* Re-run or review **CIS Benchmark** results and note improvements.
* Adjust any noisy rules/dashboards if needed.

**Evidence to attach when submitting:**  
Dashboard alert screenshots, Agents page (Active), brief log snippets, before/after CIS score.