**2) Law\_Enforcement\_SOC\_Defense\_Strategy.docx**

**Layered Defense Architecture – Law Enforcement SOC Simulation Project**

**Goal:** show how multiple layers work together in your lab to reduce risk.

| **Layer** | **Tool / Mechanism** | **What it does in your project** |
| --- | --- | --- |
| Perimeter / Network | Docker network isolation; container separation | Keeps Wazuh services segmented from the host; limits blast radius. |
| Host / Endpoint | **Ubuntu 22.04 WSL agent** + File Integrity Monitoring (FIM) | Detects logins, file changes, and service/port changes on the endpoint. |
| Application / SIEM | **Wazuh Manager & Indexer** | Centralizes logs, correlates detections, stores/searches events. |
| Visibility / Analytics | **Wazuh Dashboard** (Threat Hunting, Security Events) | Lets you investigate alerts; shows MITRE ATT&CK and CIS results. |
| Threat Knowledge | **MITRE ATT&CK view** in Dashboard | Maps observed activity to adversary tactics (e.g., Defense Evasion, Priv. Esc.). |
| Compliance / Hardening | **CIS Ubuntu 22.04 Benchmark** results | Highlights misconfigs; provides a baseline to improve security posture. |
| Management / Audit | **Monday.com** + screenshots/logs | Tracks tasks, evidence, and day-to-day progress for the rubric. |

**Zero-Trust mindset (applied here):** every layer is verified and logged; the Ubuntu agent only talks to the local Wazuh manager (127.0.0.1 in your setup) and activity is validated in the dashboard.

**Outcome:** if one control falters (e.g., endpoint misconfig), other layers (SIEM correlation, ATT&CK mapping, CIS checks) still provide detection and guidance for response.