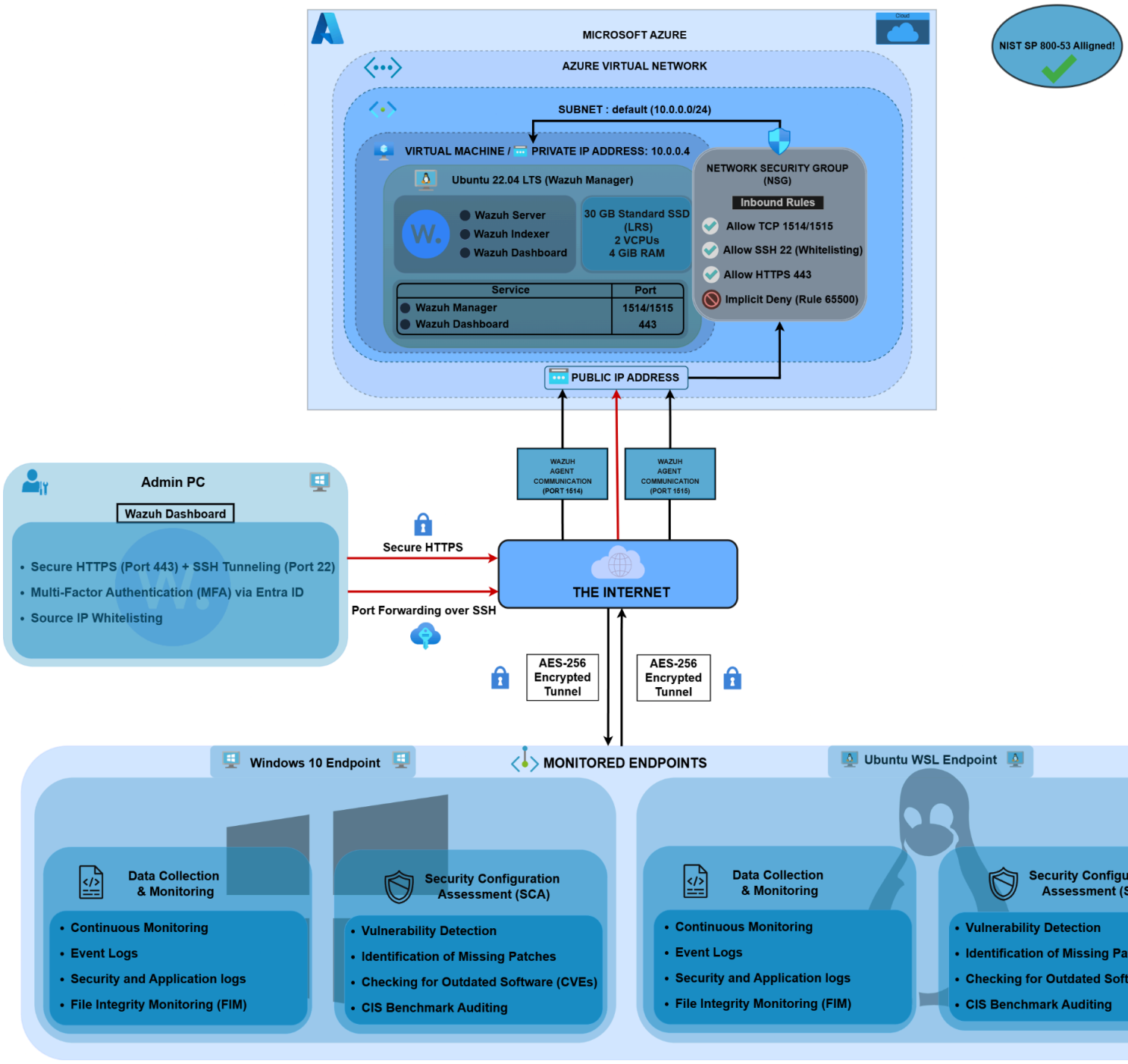
Executive Summary

Homelab Security Monitoring Project



Objective

To design and deploy a scalable, cloud-native **Security Information and Event Management (SIEM)** architecture that bridges the gap between decentralized endpoints and a centralized management system. This project was developed to simulate the real-world regulatory requirements and to help me implement governance, risk management and compliance techniques.

Architecture

The core of the environment consists of a **Wazuh Manager** hosted on an **Azure Virtual Machine (Ubuntu 22.04 LTS).** This centralized hub orchestrates security telemetry from diverse endpoints. This includes a local **Windows 10** host and a **Windows Subsystem for Linux (WSL)** instance. Communication is secured via encrypted **Wazzuh Agent** telemetry and managed through refined **Azure Network Security Group (NSG)** rules to ensure authentication and authorization.

Governance & Compliance Alignment

Beyond technical deployment, this lab serves as a functional proof-of-concept for the following compliance controls:

- **Continuous Monitoring (CA-7 / ISO 27001 A.12.4.1):** Real time visibility into unauthorized access attempts and system anomalies.
- **File Integrity Monitoring (FIM):** Tracking unauthorized changes to critical system files to ensure system Integrity and Availability.

The implementation further facilitates a comprehensive mapping of these security controls to widely recognized and relied upon industry frameworks:

- **NIST SP 800-53 (Revision 5):** Utilizing Wazuh's alerting capabilities to address the *Audit and Accountability (AU)* and *System and Information Integrity (SI)* control families, specifically providing the telemetry required for **continuous monitoring** and **incident response.**
- **ISO/IEC 27001:2022:** Supporting ***Annex A Control 8.15 (Logging)*** and ***8.16 (Monitoring Activities)*** by centralizing logs from Windows 10 and WSL endpoints into the Azure-hosted manager for analysis and retention.
- **Loi n° 05-20:** Directly aligns with **Article 7** which mandates the implementation of appropriate **monitoring and detection** mechanisms.