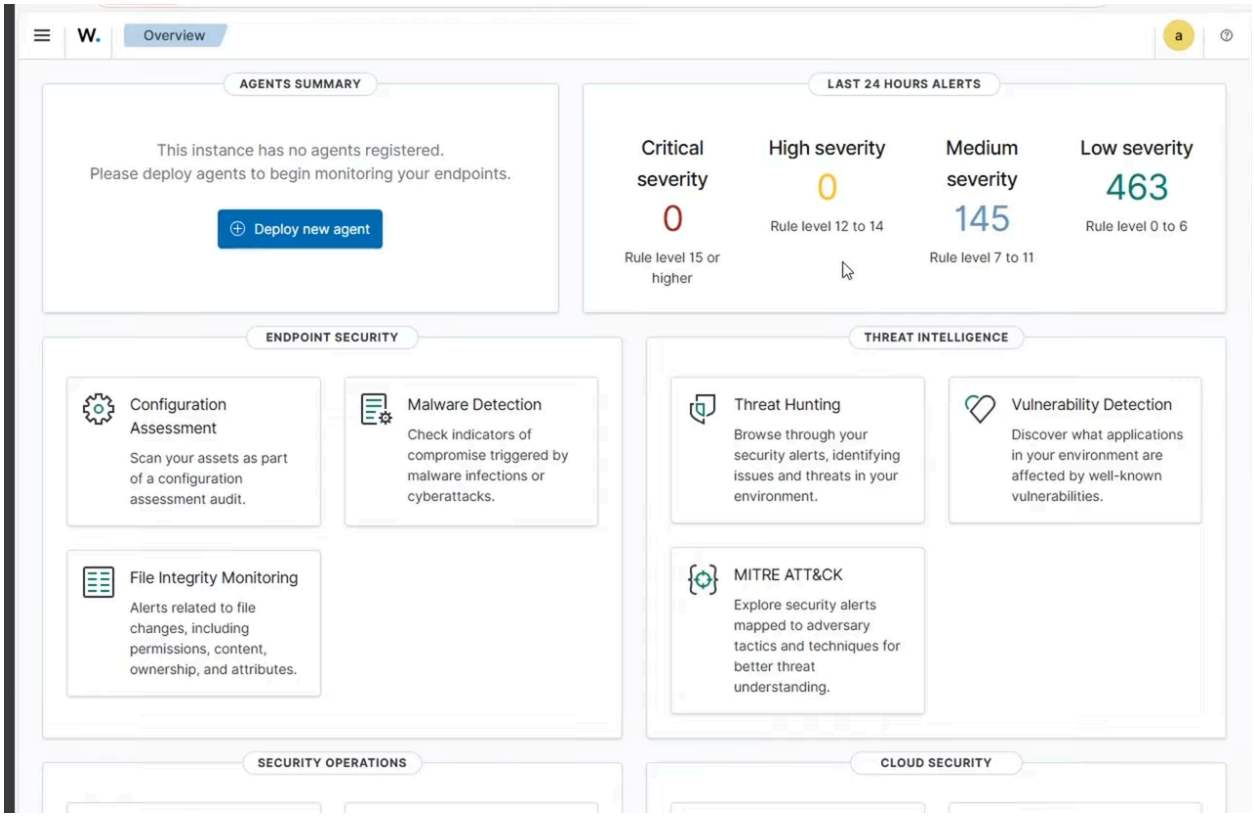
4. Wazuh SIEM Installation (Cloud VM)

Wazuh acts as the central point where all Sysmon telemetry is analyzed and correlated.



Steps:

1. Deploy a cloud VM (Ubuntu 22.04 or 24.04).
    - CPU: 2+
    - RAM: 4–8 GB
    - Open ports: 1514, 1515, 55000, 5601
2. Install Wazuh using the installation script:
   curl -s https://packages.wazuh.com/4.7/wazuh-install.sh | sudo bash
3. After installation:

- Open browser
- Navigate to https://YOUR_PUBLIC_IP
- Login with default admin credentials

Wazuh is now ready for agent enrollment.