📘 AWS SOC Project Documentation

1. Project Title

Security Operations Center (SOC) on AWS using Wazuh SIEM

2. Project Overview

This project demonstrates the deployment of a **cloud-based Security Operations Center (SOC)** on **Amazon Web Services (AWS)** using **Wazuh SIEM**.

Key components:

- **Wazuh Server** deployed on **AWS EC2 (Ubuntu 22.04 LTS)**
- **Windows Server 2025** instance as log source
- **Windows 10 Client** as test workstation
- **Ubuntu Server** as additional agent endpoint
- **Wazuh Agent** installed on all endpoints for log collection
- **File Integrity Monitoring (FIM)** and **Login Event Monitoring** rules configured
- Dashboard for **real-time monitoring and security alerts**

---

3. AWS Region Details

- **AWS Region Used**: **Asia Pacific (Mumbai) – ap-south-1**

---

4. AWS Resources Used

EC2 Instances

1. **Wazuh Server**
   - OS: Ubuntu 22.04 LTS
   - Instance Type: **t3.medium (2 vCPU, 4GB RAM)**
   - Public IP: 13.xxx.xxx.xxx
   - Security Groups:

        - Port 22 (SSH) → Admin IP only
        - Port 443 (HTTPS) → Dashboard access
        - Port 1514-1515 (TCP/UDP) → Agent communication
        - Port 55000 (TCP) → Wazuh API

2. **Windows Server 2025**
    - Instance Type: **t2.xlarge**
    - Role: Log source + Wazuh agent enrollment
3. **Windows 10 Client**
    - Instance Type: **Physical PC**
    - Role: Endpoint with Wazuh Agent installed
4. **Ubuntu Server**
    - Instance Type: **t3.Micro**
    - Role: Agent endpoint

---

5. Network Configuration

- **VPC** with default subnets
- **Security Group Rules (Inbound):**
    - 22/TCP → SSH access for admins
    - 443/TCP → HTTPS access to Wazuh Dashboard
    - 1514-1515/TCP/UDP → Agent communication
    - 55000/TCP → Wazuh API access
    - 3389/TCP → RDP Access for Windows Server

---

6. Wazuh Server Installation

1. Update Ubuntu packages:

```
sudo apt update && sudo apt upgrade -y
```

2. Install Wazuh Server & Dashboard:

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

```
sudo bash wazuh-install.sh -a
```

3. Verify service:

```
systemctl status wazuh-manager
```

4. Access dashboard:

https://<EC2_Public_IP>:443

---

7. Wazuh Agent Deployment & Registration

7.1 Windows Server & Windows 10 Agent (CLI)

1. Download Wazuh agent (Windows MSI):

https://packages.wazuh.com/4.x/windows/wazuh-agent-4.x.msi

2. Install with command:

```
msiexec /i wazuh-agent-4.x.msi /q WAZUH_MANAGER="<Wazuh_Server_Public_IP>"
WAZUH_REGISTRATION_SERVER="<Wazuh_Server_Public_IP>"
```

3. Configure agent:

- Open C:\Program Files (x86)\ossec-agent\ossec.conf
- Add Wazuh server public IP

4. Start service:

```
net start wazuh-agent
```

5. Verify in Wazuh Dashboard → **Agents Tab**

7.2 Ubuntu Agent Deployment

1. Update Ubuntu machine:

```
sudo apt update && sudo apt upgrade -y
```

2. Install Wazuh Agent:

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

```
sudo bash wazuh-install.sh -a
```

3. Start the agent:

```
sudo systemctl enable wazuh-agent
```

```
sudo systemctl start wazuh-agent
```

7.3 Register Agent Using GUI

1. **Access Wazuh Dashboard:**
   - URL: https://<Wazuh_Server_Public_IP>
   - Login with credentials
2. **Generate Agent Authentication Key:**
   - Navigate: **Agents → Manage Agents → Add Agent → New Agent Registration**
   - Copy the **authentication key** (valid for 5 minutes)
3. **Use Key to Register Agent (Ubuntu CLI):**

```
sudo /var/ossec/bin/agent-auth -m <Wazuh_Server_IP> -A <Agent_Name> -k
<Authentication_Key>
```

4. **Windows Agent Registration via GUI:**

```
msiexec /i wazuh-agent-4.x.msi /q WAZUH_MANAGER="<Wazuh_Server_IP>"
WAZUH_REGISTRATION_KEY="<Authentication_Key>"
```

5. **Verify Agent Connection:**

- Wazuh Dashboard → **Agents Tab** → Newly registered agents should appear as **Active**

---

8. Configured Monitoring Rules

8.1 File Integrity Monitoring (FIM)

Enabled by default in Wazuh:

- Watches Windows Registry

- Windows File changes in free defined locations (Open the following configuration file: C:\Program Files (x86)\ossec-agent\ossec.conf and Add the following entry inside the Directory block: <directories realtime="yes"> Location you want to monitor(Path) </directories>)
- Tracks changes in /etc/ (Linux)
- Logs visible in **Security Events → FIM**

8.2 Login Event Monitoring

- Tracks Windows and Linux login attempts and failed logins

  Windows : security Logs Via Agent

  Linux: var/log/auth.log
- Detects brute force patterns

---

9. Notifications

- **Email Alerts** configured via SMTP (optional)
- Critical events notify SOC admins in real-time

---

10. Dashboard Features

- Real-time monitoring of agents
- File integrity alerts
- Login event tracking
- Threat visualization and alerts

---

11. Security Best Practices Applied

- Private key SSH access only (no password)
- Least privilege IAM roles

- Security groups separated per server type
- CloudWatch monitoring enabled
- Agent authentication via short-lived keys

---

12. Project Summary

This AWS SOC project demonstrates:

- Deployment of Wazuh Server on **Ubuntu EC2**
- Agents installed on **Windows Server, Windows 10, and Ubuntu**
- Both **CLI and GUI-based agent registration**
- **File Integrity Monitoring** and **Login Event Monitoring** rules active
- Real-time **dashboard monitoring** and optional **email notifications**

Outcome: Centralized logging, threat monitoring, and a working SOC environment for cloud-based endpoints.