SOC's Wazuh Checklist:

A: Wazuh Host

Supported Operating System: Linux, Windows, macOS, Solaris, AIX, and other operating systems

System Requirements:

-The minimum requirements for this type of deployment are 4 GB of RAM and 2 CPU cores,

-The recommended are 16 GB of RAM and 8 CPU cores.

- A 64-bit operating system is required.

Disk Storage Requirements - (APS = alerts per second)

Monitored endpoints	APS	Storage (GB/90 days)
Servers	0.25	3.8
Workstations	0.1	1.5
Network devices	0.5	7.6

A.1: Installation of manager

- Retrieve the package from wazuh

```
curl -o ~/unattended-installation.sh https://packages.wazuh.com/resources/4.2/open-distro/unattended-installation/unattended-installation.sh
```

- -o flag performs a health check on the host to ensure it has the system requirements to run Wazuh server

```
sudo apt-get install dirmngr
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 8B48AD6246925553
sudo apt-get update
```

```
bash ~/unattended-installation.sh
```

A.2: Change Password

Download Password Tool Script-

```
curl -so wazuh-passwords-tool.sh
https://packages.wazuh.com/resources/4.2/open-distro/tools/wazuh-passwords-tool.sh
```

Run it-

```
bash ./wazuh-passwords-tool.sh -u admin -p mypassword -v
```

B: Wazuh Agent

Supported Operating System: Linux Distributions, Windows, Apple, Oracle Solaris, HP UX, AIX

System Requirements:

- .1GB of Ram

B.1: Installation of Agent

Linux: Using APT

1) **Import GPG Key:**
   ```
   curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
   ```
2) **Add the repository:**
   ```
   echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
   ```
3) **Update package information:**

```
apt-get update
```

4) **Deploy Wazuh agent**

C.1: