Guide Book MS SOC PTPN Group

Jakarta, 19 Januari 2026

Disiapkan oleh :

pgn COM always reliable

Disiapkan untuk :

Perkebunan Nusantara

KERAHASIAAN

Dokumen ini bersifat **“Propietary & Confidential”** serta ditujukan hanya kepada manajemen PT Perkebunan Nusantara III (Persero) serta pihak pengambil keputusan terkait.

DAFTAR ISI

1. Standarisasi Penamaan Endpoint (Hostname per Entitas)

Agar proses monitoring, analisis insiden, dan pelaporan SOC berjalan rapi dan konsisten, setiap perangkat (endpoint) wajib menggunakan format penamaan (hostname) yang sama. Standarisasi ini membantu tim SOC untuk:

- Mengidentifikasi perangkat dengan cepat
- Mengetahui asal entitas dan lokasi perangkat
- Mempermudah penanganan insiden dan audit keamanan

Format Penamaan Hostname

Gunakan format berikut untuk seluruh endpoint:

ORG-LOC-ENV-ROLE/NAME-NUMBER

Penjelasan Setiap Bagian

a. **ORG**: Kode entitas perusahaan
   Contoh:
   PTPN-1
   PTPN-2
   ...
   PTPN-11
b. **LOC**: Lokasi kota tempat endpoint berada
   Contoh:
   Jakarta
   Riau

   Medan
   Bandung
c. **ENV**: Jenis lingkungan sistem
   Dev → Development
   Staging → Testing / Uji coba
   Prod → Production
   Personal → Workstation / desktop / laptop user
d. **ROLE / NAME**
   Untuk **server**: isi dengan fungsi server
   Contoh: Webserver, Database, Application
   Untuk **workstation/desktop/laptop**: isi dengan **nama pengguna**
e. **NUMBER**
   Nomor urut perangkat (01–100), digunakan jika:
   - Satu orang memiliki lebih dari satu perangkat
   - Terdapat lebih dari satu server dengan fungsi yang sama

Contoh Penamaan Hostname

- **Contoh untuk server:**
  PTPN-1-Jakarta-Prod-Webserver-01
- **Contoh untuk workstation / desktop / laptop:**
  PTPN-2-Riau-Personal-Wahyu-01

Catatan Penting:
Penamaan hostname yang tidak sesuai standar dapat menyulitkan proses monitoring dan penanganan insiden oleh SOC.

2. Standarisasi Timestamp & Timezone
Untuk memastikan seluruh log dan aktivitas keamanan **konsisten dan mudah dianalisis**, seluruh endpoint wajib menggunakan **zona waktu yang sama**.

Standar Timezone
Timezone yang digunakan: **Waktu Indonesia Barat (WIB) / UTC +7**
Ketentuan

a. Pengaturan timezone pada server dan workstation **harus disesuaikan ke WIB (UTC+7)**
b. Timestamp yang konsisten sangat penting untuk:
    - Korelasi log
    - Investigasi insiden
    - Pelaporan keamanan
    - Audit dan kepatuhan

Catatan:
Perbedaan timezone dapat menyebabkan kesalahan analisis waktu kejadian (timestamp mismatch).

3. Manual Book Instalasi Wazuh Agent (Windows & Linux)

Tujuan

Dokumen ini dibuat sebagai panduan sederhana untuk membantu pengguna melakukan instalasi Wazuh Agent pada perangkat Windows maupun Linux.

Wazuh Agent berfungsi untuk:

a. Memantau kondisi keamanan perangkat secara otomatis
b. Mengumpulkan log aktivitas sistem
c. Mengirimkan informasi keamanan ke Security Operation Center (SOC)

Dengan terpasangnya Wazuh Agent, perangkat Anda akan:

a. Terpantau oleh tim SOC
b. Terlindungi melalui deteksi dini terhadap aktivitas mencurigakan
c. Menjadi bagian dari sistem keamanan terpusat perusahaan

Catatan: Wazuh Agent tidak mengganggu aktivitas pengguna dan berjalan otomatis di latar belakang.

Persyaratan

Sebelum melakukan instalasi, pastikan beberapa hal berikut sudah siap.

a. Koneksi Jaringan

- Pastikan perangkat Anda:
  - ✔ Terhubung ke jaringan kantor atau jaringan yang sudah diizinkan
  - ✔ Dapat terhubung ke server **Wazuh Manager** (server SOC)
- Cara paling mudah untuk memastikan:
  - ✔ Coba lakukan **ping** ke alamat IP Wazuh Manager (akan diinformasikan oleh tim SOC)
  - ✔ **Jika ping berhasil**, berarti koneksi sudah siap
  - ✔ **Jika ping gagal**, silakan hubungi tim IT internal atau tim SOC sebelum melanjutkan instalasi.

Port yang harus terbuka
Agar Wazuh Agent dapat berkomunikasi dengan SOC, pastikan **port berikut tidak diblokir** oleh firewall:

Port	Protocol	Purpose
1514	TCP	Log and event transmission
1515	TCP	Agent enrollment

Catatan: Jika perangkat Anda berada di jaringan dengan firewall ketat, port ini mungkin perlu dibuka terlebih dahulu oleh tim IT.
Access Requirement
Untuk menginstal Wazuh Agent, dibutuhkan hak akses khusus:

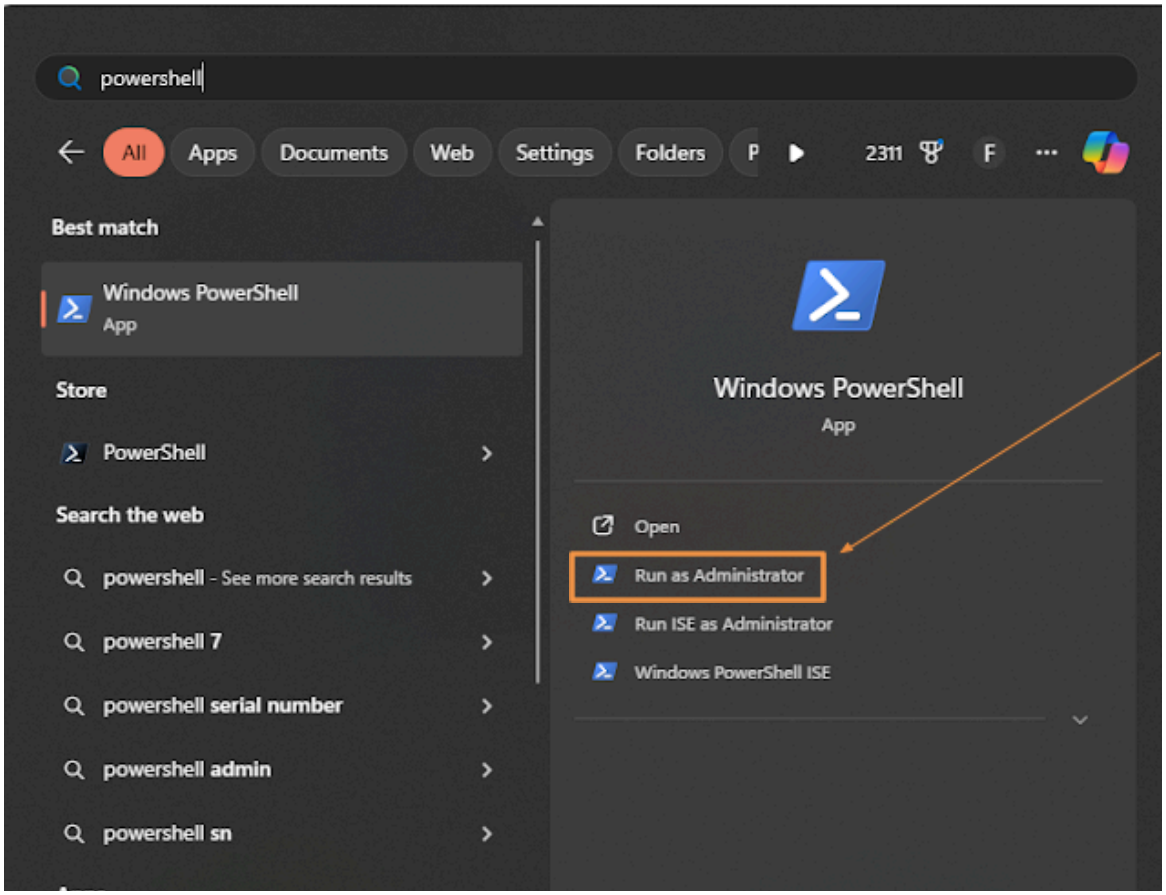
a. *Windows*
   Instalasi harus dilakukan menggunakan akun Administrator
b. *Linux*
   Instalasi harus dilakukan menggunakan akun root atau menggunakan perintah sudo

Tanpa hak akses ini, proses instalasi tidak akan berhasil.

Wazuh Agent Installation – Windows
Bagian ini menjelaskan cara menginstal **Wazuh Agent pada perangkat Windows**. Pastikan Anda mengikuti langkah-langkah di bawah ini **secara berurutan**.

I. Membuka PowerShell sebagai Administrator
II. Klik **Start Menu** Windows
III. Ketik **PowerShell**
IV. Klik kanan pada **Windows PowerShell**
V. Pilih **Run as Administrator**
VI. Jika muncul notifikasi *User Account Control (UAC)*, klik **Yes**

Catatan:
Instalasi tidak akan berhasil jika PowerShell tidak dijalankan sebagai Administrator.



Menjalankan Perintah uninstall wazuh jika sudah ada sebelumnya

I. Salin (**copy**) dan jalankan (**paste**) perintah berikut ke dalam jendela PowerShell:
msiexec.exe /x wazuh-agent-4.14.1-1.msi /qn

Menjalankan Perintah Instalasi

II. Salin (**copy**) dan jalankan (**paste**) perintah berikut ke dalam jendela PowerShell:

ptpn-1 = PT Perkebunan Nusantara I

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='103.118.111.45'
WAZUH_AGENT_GROUP='ptpn-1'
```

ptpn-2 = PT Sinergi Gula Nusantara

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='103.118.111.45'
WAZUH_AGENT_GROUP=’ptpn-2'
```

ptpn-3 = PT Perkebunan Nusantara III (HOLDING)

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='103.118.111.45'
WAZUH_AGENT_GROUP='ptpn-3'
```

ptpn-4 = PT Perkebunan Nusantara IV

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='103.118.111.45'
WAZUH_AGENT_GROUP='ptpn-4'
```

ptpn-5 = PT Riset Perkebunan Nusantara

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='103.118.111.45'
WAZUH_AGENT_GROUP='ptpn-5'
```

ptpn-6 = PT Lembaga Pendidikan Perkebunan Agro Nusantara

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='103.118.111.45'
WAZUH_AGENT_GROUP='ptpn-6'
```

ptpn-7 = PT Kharisma Pemasaran Bersama Nusantara

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='103.118.111.45'
WAZUH_AGENT_GROUP='ptpn-7'
```

ptpn-8 = PT Industri Karet Nusantara

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='103.118.111.45'
WAZUH_AGENT_GROUP="ptpn-8'
```

ptpn-9 = PT RS Sri Pamela Medika Nusantara

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='103.118.111.45'
WAZUH_AGENT_GROUP='ptpn-9'
```

ptpn-10 = PT Kawasan Industri Nusantara

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='103.118.111.45'
WAZUH_AGENT_GROUP='ptpn-10'
```

ptpn-11 = PT Bio Industri Nusantara

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='103.118.111.45'
WAZUH_AGENT_GROUP='ptpn-11'
```

- Perintah di atas akan:
  a. Mengunduh file instalasi Wazuh Agent
  b. Menginstal agent secara otomatis (tanpa tampilan)
  c. Menghubungkan agent ke Wazuh Manager (SOC)
  d. Mendaftarkan agent ke group perusahaan yang sesuai

Penjelasan Parameter (Informasi Tambahan)

a. **WAZUH_MANAGER**
   Alamat IP server SOC (Wazuh Manager)
   Contoh: 103.118.111.45
b. **WAZUH_AGENT_GROUP**
   Digunakan untuk mengelompokkan perangkat sesuai perusahaan
c. **Penting:**
   Pastikan nilai **WAZUH_AGENT_GROUP** sesuai dengan perusahaan tempat perangkat Anda berada. Jika ragu, silakan konfirmasi ke tim SOC.

Mengaktifkan Wazuh Agent

Setelah proses instalasi selesai, jalankan perintah berikut di PowerShell untuk mengaktifkan layanan Wazuh Agent:

```
NET START Wazuh
```

Jika berhasil, akan muncul pesan bahwa **service Wazuh telah berjalan**.

Verifikasi Sederhana (Opsional)

Untuk memastikan agent sudah aktif:

- Pastikan tidak ada pesan error di PowerShell
- Tunggu beberapa menit setelah service berjalan
- Tim SOC akan melakukan pengecekan dari sisi server

Catatan:

Tidak diperlukan konfigurasi tambahan dari sisi pengguna.
Seluruh proses monitoring akan dilakukan oleh tim SOC secara terpusat.

Wazuh Agent Installation – LINUX

Bagian ini menjelaskan cara menginstal **Wazuh Agent pada perangkat Linux**. Panduan dibagi berdasarkan **jenis sistem operasi dan arsitektur CPU** agar lebih mudah diikuti.

I. Membuka Terminal
II. Login ke server atau komputer Linux Anda
III. Buka **Terminal**
IV. Pastikan Anda memiliki akses **root** atau **sudo**

Catatan: *Jika menggunakan user biasa, pastikan perintah dijalankan dengan sudo.*

Menentukan Jenis Sistem Linux

Sebelum menjalankan perintah, pastikan jenis Linux yang Anda gunakan:

- **RPM (RedHat / CentOS / Rocky / AlmaLinux / Oracle Linux)**
- **DEB (Ubuntu / Debian)**

Serta arsitektur CPU:

- **amd64 / x86_64** → Server atau PC Intel / AMD (umumnya)
- **aarch64 / arm64** → Server ARM (misalnya cloud ARM atau embedded)

Jika ragu, silakan konfirmasi ke tim IT atau tim SOC.

Menjalankan Perintah uninstall wazuh jika sudah ada sebelumnya

I. Salin (**copy**) dan jalankan (**paste**) perintah berikut ke dalam jendela PowerShell:
   - *APT package manager*
     `apt-get remove --purge wazuh-agent`
   - *Yum package manager*
     `yum remove wazuh-agent`
   - *Dnf package manager*
     `dnf remove wazuh-agent`
   - *Zypp package manager*
     `zypper remove wazuh-agent`

Perintah Instalasi Wazuh Agent

A. Linux RPM – amd64 (x86_64)

Gunakan perintah berikut untuk sistem berbasis RPM dengan arsitektur amd64:

ptpn-1 = PT Perkebunan Nusantara I

```
curl -o wazuh-agent-4.14.1-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.x86_64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-1' rpm -ihv wazuh-agent-4.14.1-1.x86_64.rpm
```

ptpn-2 = PT Sinergi Gula Nusantara

```
curl -o wazuh-agent-4.14.1-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.x86_64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-2' rpm -ihv wazuh-agent-4.14.1-1.x86_64.rpm
```

ptpn-3 = PT Perkebunan Nusantara III (HOLDING)

```
curl -o wazuh-agent-4.14.1-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.x86_64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-3' rpm -ihv wazuh-agent-4.14.1-1.x86_64.rpm
```

ptpn-4 = PT Perkebunan Nusantara IV

```
curl -o wazuh-agent-4.14.1-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.x86_64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-4' rpm -ihv wazuh-agent-4.14.1-1.x86_64.rpm
```

ptpn-5 = PT Riset Perkebunan Nusantara

```
curl -o wazuh-agent-4.14.1-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.x86_64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-5' rpm -ihv wazuh-agent-4.14.1-1.x86_64.rpm
```

ptpn-6 = PT Lembaga Pendidikan Perkebunan Agro Nusantara

```
curl -o wazuh-agent-4.14.1-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.x86_64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-6' rpm -ihv wazuh-agent-4.14.1-1.x86_64.rpm
```

ptpn-7 = PT Kharisma Pemasaran Bersama Nusantara

```
curl -o wazuh-agent-4.14.1-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.x86_64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-7' rpm -ihv wazuh-agent-4.14.1-1.x86_64.rpm
```

ptpn-8 = PT Industri Karet Nusantara

```
curl -o wazuh-agent-4.14.1-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.x86_64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-8' rpm -ihv wazuh-agent-4.14.1-1.x86_64.rpm
```

ptpn-9 = PT RS Sri Pamela Medika Nusantara

```
curl -o wazuh-agent-4.14.1-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.x86_64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-9' rpm -ihv wazuh-agent-4.14.1-1.x86_64.rpm
```

ptpn-10 = PT Kawasan Industri Nusantara

```
curl -o wazuh-agent-4.14.1-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.x86_64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-10' rpm -ihv wazuh-agent-4.14.1-1.x86_64.rpm
```

ptpn-11 = PT Bio Industri Nusantara

```
curl -o wazuh-agent-4.14.1-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.x86_64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-11' rpm -ihv wazuh-agent-4.14.1-1.x86_64.rpm
```

B. Linux DEB – amd64 (x86_64)

Gunakan perintah berikut untuk Ubuntu atau Debian dengan arsitektur amd64:

ptpn-1 = PT Perkebunan Nusantara I

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_amd64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-1' dpkg -i ./wazuh-agent_4.14.1-1_amd64.deb
```

ptpn-2 = PT Sinergi Gula Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_amd64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-2' dpkg -i ./wazuh-agent_4.14.1-1_amd64.deb
```

ptpn-3 = PT Perkebunan Nusantara III (HOLDING)

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_amd64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-3' dpkg -i ./wazuh-agent_4.14.1-1_amd64.deb
```

ptpn-4 = PT Perkebunan Nusantara IV

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_amd64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-4' dpkg -i ./wazuh-agent_4.14.1-1_amd64.deb
```

ptpn-5 = PT Riset Perkebunan Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_amd64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-5' dpkg -i ./wazuh-agent_4.14.1-1_amd64.deb
```

ptpn-6 = PT Lembaga Pendidikan Perkebunan Agro Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_amd64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-6' dpkg -i ./wazuh-agent_4.14.1-1_amd64.deb
```

ptpn-7 = PT Kharisma Pemasaran Bersama Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_amd64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-7' dpkg -i ./wazuh-agent_4.14.1-1_amd64.deb
```

ptpn-8 = PT Industri Karet Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_amd64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-8' dpkg -i ./wazuh-agent_4.14.1-1_amd64.deb
```

ptpn-9 = PT RS Sri Pamela Medika Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_amd64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-9' dpkg -i ./wazuh-agent_4.14.1-1_amd64.deb
```

ptpn-10 = PT Kawasan Industri Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_amd64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-10' dpkg -i ./wazuh-agent_4.14.1-1_amd64.deb
```

ptpn-11 = PT Bio Industri Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_amd64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-11' dpkg -i ./wazuh-agent_4.14.1-1_amd64.deb
```

C. Linux RPM – aarch64 (ARM)

Gunakan perintah berikut untuk sistem RPM dengan arsitektur ARM:

ptpn-1 = PT Perkebunan Nusantara I

```
curl -o wazuh-agent-4.14.1-1.aarch64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.aarch64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-1' rpm -ihv wazuh-agent-4.14.1-1.aarch64.rpm
```

ptpn-2 = PT Sinergi Gula Nusantara

```
curl -o wazuh-agent-4.14.1-1.aarch64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.aarch64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP="ptpn-2' rpm -ihv wazuh-agent-4.14.1-1.aarch64.rpm
```

ptpn-3 = PT Perkebunan Nusantara III (HOLDING)

```
curl -o wazuh-agent-4.14.1-1.aarch64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.aarch64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-3' rpm -ihv wazuh-agent-4.14.1-1.aarch64.rpm
```

ptpn-4 = PT Perkebunan Nusantara IV

```
curl -o wazuh-agent-4.14.1-1.aarch64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.aarch64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-4' rpm -ihv wazuh-agent-4.14.1-1.aarch64.rpm
```

ptpn-5 = PT Riset Perkebunan Nusantara

```
curl -o wazuh-agent-4.14.1-1.aarch64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.aarch64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-5' rpm -ihv wazuh-agent-4.14.1-1.aarch64.rpm
```

ptpn-6 = PT Lembaga Pendidikan Perkebunan Agro Nusantara

```
curl -o wazuh-agent-4.14.1-1.aarch64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.aarch64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-6' rpm -ihv wazuh-agent-4.14.1-1.aarch64.rpm
```

ptpn-7 = PT Kharisma Pemasaran Bersama Nusantara

```
curl -o wazuh-agent-4.14.1-1.aarch64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.aarch64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-7' rpm -ihv wazuh-agent-4.14.1-1.aarch64.rpm
```

ptpn-8 = PT Industri Karet Nusantara

```
curl -o wazuh-agent-4.14.1-1.aarch64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.aarch64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-8' rpm -ihv wazuh-agent-4.14.1-1.aarch64.rpm
```

ptpn-9 = PT RS Sri Pamela Medika Nusantara

```
curl -o wazuh-agent-4.14.1-1.aarch64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.aarch64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-9' rpm -ihv wazuh-agent-4.14.1-1.aarch64.rpm
```

ptpn-10 = PT Kawasan Industri Nusantara

```
curl -o wazuh-agent-4.14.1-1.aarch64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.aarch64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-10' rpm -ihv wazuh-agent-4.14.1-1.aarch64.rpm
```

ptpn-11 = PT Bio Industri Nusantara

```
curl -o wazuh-agent-4.14.1-1.aarch64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.14.1-1.aarch64.rpm &&
sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-11' rpm -ihv wazuh-agent-4.14.1-1.aarch64.rpm
```

D. Linux DEB – aarch64 (ARM)

Gunakan perintah berikut untuk Ubuntu/Debian berbasis ARM:

ptpn-1 = PT Perkebunan Nusantara I

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_arm64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-1' dpkg -i ./wazuh-agent_4.14.1-1_arm64.deb
```

ptpn-2 = PT Sinergi Gula Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_arm64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-2' dpkg -i ./wazuh-agent_4.14.1-1_arm64.deb
```

ptpn-3 = PT Perkebunan Nusantara III (HOLDING)

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_arm64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-3' dpkg -i ./wazuh-agent_4.14.1-1_arm64.deb
```

ptpn-4 = PT Perkebunan Nusantara IV

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_arm64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-4' dpkg -i ./wazuh-agent_4.14.1-1_arm64.deb
```

ptpn-5 = PT Riset Perkebunan Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_arm64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-5' dpkg -i ./wazuh-agent_4.14.1-1_arm64.deb
```

ptpn-6 = PT Lembaga Pendidikan Perkebunan Agro Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_arm64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-6' dpkg -i ./wazuh-agent_4.14.1-1_arm64.deb
```

ptpn-7 = PT Kharisma Pemasaran Bersama Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_arm64.deb && sudo
WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-7' dpkg -i ./wazuh-agent_4.14.1-1_arm64.deb
```

ptpn-8 = PT Industri Karet Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_arm64.deb && sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-8' dpkg -i ./wazuh-agent_4.14.1-1_arm64.deb
```

ptpn-9 = PT RS Sri Pamela Medika Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_arm64.deb && sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-9' dpkg -i ./wazuh-agent_4.14.1-1_arm64.deb
```

ptpn-10 = PT Kawasan Industri Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_arm64.deb && sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-10' dpkg -i ./wazuh-agent_4.14.1-1_arm64.deb
```

ptpn-11 = PT Bio Industri Nusantara

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.1-1_arm64.deb && sudo WAZUH_MANAGER='103.118.111.45' WAZUH_AGENT_GROUP='ptpn-11' dpkg -i ./wazuh-agent_4.14.1-1_arm64.deb
```

Penjelasan Parameter

a. **WAZUH_MANAGER**
   Alamat IP server SOC (Wazuh Manager)
b. **WAZUH_AGENT_GROUP**
   Digunakan untuk mengelompokkan perangkat sesuai perusahaan
   Contoh penulisan:
   - ptpn-1
   - ptpn-2
   - …
   - ptpn-11
c. **Penting:**
   Pastikan nilai **WAZUH_AGENT_GROUP** sesuai dengan entitas perusahaan Anda.
   Jika salah, perangkat bisa masuk ke grup yang tidak sesuai.

Mengaktifkan Wazuh Agent (Linux)

Setelah proses instalasi Wazuh Agent selesai, langkah berikutnya adalah **mengaktifkan layanan Wazuh Agent** agar dapat berjalan dan terhubung ke SOC.
Langkah-langkah:

a. Buka **Terminal** pada perangkat Linux
b. Jalankan perintah berikut **secara berurutan**:
   `sudo systemctl daemon-reload`
   Perintah ini digunakan untuk menyegarkan konfigurasi service pada sistem.
   `sudo systemctl enable wazuh-agent`
   *Perintah ini memastikan Wazuh Agent **otomatis berjalan setiap kali sistem dinyalakan**.*

`sudo systemctl start wazuh-agent`
*Perintah ini digunakan untuk **menjalankan Wazuh Agent sekarang juga**.*

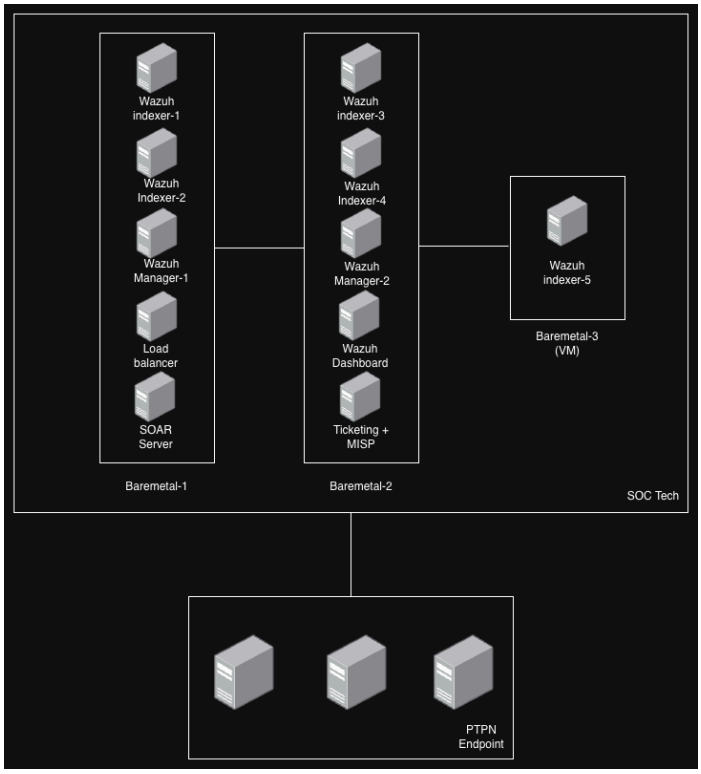
Verifikasi (Opsional)

Untuk memastikan Wazuh Agent sudah berjalan dengan normal, jalankan:
`sudo systemctl status wazuh-agent`
Jika muncul status **active (running)**, maka Wazuh Agent telah aktif dan berhasil dijalankan.
Catatan:
Setelah agent aktif, tidak diperlukan konfigurasi tambahan dari sisi pengguna.
Tim SOC akan melakukan pengecekan koneksi dan monitoring dari server pusat.

4. High Level Architecture SOC & SIEM

Bagian ini menjelaskan gambaran umum arsitektur Security Operation Center (SOC) yang digunakan untuk memantau keamanan seluruh endpoint PTPN Group.
Arsitektur ini dirancang agar:

- Aman dan terpusat
- Mampu menangani banyak endpointTetap berjalan meskipun salah satu komponen mengalami gangguan



1) Gambaran Umum Alur Sistem

a. Secara sederhana, alur kerja sistem adalah sebagai berikut:
b. **Endpoint PTPN** (server, desktop, laptop)
→ mengirimkan log dan data keamanan
c. **Wazuh Agent**
→ mengirim data ke SOC
d. **Wazuh Manager & Indexer**
→ memproses dan menyimpan data
e. **Dashboard SOC & Ticketing**
→ menampilkan informasi dan insiden keamanan
f. **Tim SOC**
→ melakukan monitoring dan penanganan insiden

*Semua proses ini berjalan **otomatis dan real-time**.*

2) Komponen Utama Arsitektur SOC

Endpoint PTPN

Endpoint adalah seluruh perangkat milik PTPN Group, seperti:

a. Server
b. Desktop
c. Laptop
d. Sistem aplikasi

Setiap endpoint:

a. Dipasang **Wazuh Agent**
b. Mengirimkan log dan aktivitas keamanan ke SOC
c. Tidak perlu dilakukan konfigurasi manual oleh user setelah instalasi

Wazuh Manager

Wazuh Manager berfungsi sebagai **otak utama SOC**, dengan tugas:

a. Menerima data dari seluruh endpoint
b. Melakukan analisis keamanan
c. Mendeteksi aktivitas mencurigakan
d. Menghasilkan alert keamanan

Pada arsitektur ini terdapat **lebih dari satu Wazuh Manager**, sehingga:

a. Beban kerja terbagi
b. Sistem tetap berjalan jika salah satu manager bermasalah

3) Wazuh Indexer

Wazuh Indexer berfungsi untuk:

a. Menyimpan log dan data keamanan
b. Memungkinkan pencarian log secara cepat
c. Mendukung analisis historis dan audit

*Indexer dibuat dalam bentuk **cluster**, artinya:*

a. Data disimpan secara terdistribusi
b. Lebih stabil dan aman
c. Tidak bergantung pada satu server saja

4) Load Balancer

Load Balancer berfungsi untuk:

a. Mengatur lalu lintas data dari endpoint ke Wazuh Manager
b. Membagi beban secara merata
c. Mencegah overload pada satu server

Dengan load balancer, sistem SOC menjadi:

a. Lebih stabil
b. Lebih responsif
c. Lebih tahan gangguan

5) Wazuh Dashboard

Wazuh Dashboard adalah **tampilan visual SOC**, yang digunakan untuk:

a. Melihat status keamanan secara real-time
b. Menampilkan alert dan insiden

c. Melihat statistik dan laporan keamanan

Dashboard ini digunakan oleh:

a. Tim SOC
b. Tim IT yang memiliki akses resmi

6) Ticketing System & MISP

Komponen ini digunakan untuk:

- Mencatat insiden keamanan dalam bentuk tiket
- Melacak status penanganan insiden
- Mengelola informasi ancaman (Threat Intelligence)

Dengan sistem ini:

- Setiap insiden terdokumentasi
- Proses penanganan lebih rapi
- Mudah diaudit dan dilaporkan

7) SOAR Server

SOAR (Security Orchestration, Automation, and Response) berfungsi untuk:

a. Mengotomatiskan respon terhadap insiden tertentu
b. Mengurangi waktu respon
c. Membantu tim SOC bekerja lebih efisien

Contoh:

a. Isolasi endpoint
b. Notifikasi otomatis
c. Eksekusi playbook keamanan

8) Infrastruktur Server (Baremetal & VM)

Arsitektur SOC dibangun menggunakan kombinasi:

a. **Baremetal Server** → untuk performa dan stabilitas tinggi
b. **Virtual Machine (VM)** → untuk fleksibilitas dan skalabilitas

Pembagian ini memastikan:

a. Sistem tetap optimal
b. Mudah dikembangkan ke depan
c. Mendukung kebutuhan jangka panjang

9) Keamanan & Ketersediaan Sistem

Arsitektur ini dirancang dengan prinsip:

a. **High Availability** → sistem tetap berjalan walaupun ada gangguan
b. **Scalability** → mudah menambah kapasitas endpoint
c. **Centralized Monitoring** → semua entitas PTPN terpantau dari satu SOC

Dari sisi pengguna (client), **tidak ada dampak ke aktivitas harian**.
Semua proses berjalan di latar belakang dan dikelola oleh tim SOC.

10) Kesimpulan

Dengan arsitektur ini:

a. Seluruh endpoint PTPN Group terpantau secara terpusat
b. Insiden keamanan dapat dideteksi lebih cepat
c. Proses respon dan pelaporan menjadi lebih terstruktur

5. Mekanisme Grouping Agent per Anak Perusahaan

Untuk memudahkan proses monitoring dan pengelolaan keamanan, setiap endpoint yang terhubung ke SOC akan **dikelompokkan berdasarkan anak perusahaan PTPN Group**.

Cara Kerja Grouping Agent

Setiap Wazuh Agent akan dimasukkan ke dalam **group sesuai entitas perusahaan**, yaitu:

- ptpn-1 = PT Perkebunan Nusantara I
- ptpn-2 = PT Sinergi Gula Nusantara
- ptpn-3 = PT Perkebunan Nusantara III (Holding)
- ptpn-4 = PT Perkebunan Nusantara IV
- ptpn-5 = PT Riset Perkebunan Nusantara
- ptpn-6 = PT Lembaga Pendidikan Perkebunan Agro Nusantara
- ptpn-7 = PT Kharisma Pemasaran Bersama Nusantara
- ptpn-8 = PT Industri Karet Nusantar
- ptpn-9 = PT RS Sri Pamela Medika Nusantara
- ptpn-10 = PT Kawasan Industri Nusantara
- ptpn-11 = PT Bio Industri Nusantara

Proses pengelompokan dilakukan:

a. **Secara otomatis** oleh sistem Wazuh berdasarkan konfigurasi saat instalasi
b. **Mengacu pada panduan Manual Book ini**, khususnya pada parameter WAZUH_AGENT_GROUP

Dengan mekanisme ini:

a. Data log antar entitas tetap terpisah
b. Akses dan monitoring dilakukan sesuai kewenangan
c. Pelaporan keamanan menjadi lebih terstruktur

Catatan:

Pengguna hanya perlu memastikan penulisan group sudah benar saat instalasi.
Proses pengelolaan selanjutnya sepenuhnya ditangani oleh tim SOC.

6. Strategi Instalasi Endpoint (PC/Laptop & Server)

Strategi instalasi Wazuh Agent dibuat **sederhana dan fleksibel**, agar tidak mengganggu operasional harian pengguna.

Ketentuan Umum Instalasi

Wazuh Agent dapat diinstal pada:

- PC
- Laptop
- Server

Tidak diperlukan konfigurasi khusus atau perubahan sistem yang kompleks.

Syarat Utama Endpoint

Agar Wazuh Agent dapat berfungsi dengan baik, endpoint hanya perlu memenuhi kondisi berikut:

a. Terhubung ke **jaringan/internet**

b. Dapat melakukan koneksi ke **Wazuh Server (SOC)**

Selama dua syarat di atas terpenuhi, instalasi dapat dilakukan tanpa hambatan.

7. Timeline Implementasi Endpoint

(Target Penyelesaian: 30 Januari 2026)

Implementasi instalasi Wazuh Agent dilakukan secara **bertahap** untuk memastikan proses berjalan stabil dan terkendali.

Tahapan Implementasi

Minggu ke-1 → 25% endpoint terpasang
Minggu ke-2 → 50% endpoint terpasang
Minggu ke-3 → 75% endpoint terpasang
Minggu ke-4 → 100% endpoint terpasang

Timeline ini mencakup:

- Instalasi agent
- Aktivasi layanan
- Verifikasi koneksi ke SOC

Catatan:

Progres implementasi akan dipantau oleh tim SOC dan dilaporkan secara berkala kepada pihak terkait.

8. Mekanisme Koordinasi & Support Implementasi
Apabila terdapat kendala, pertanyaan, atau membutuhkan bantuan selama proses **instalasi dan aktivasi Wazuh Agent**, pengguna dapat menghubungi **tim support implementasi SOC**.
Kontak Koordinasi Implementasi
Untuk kebutuhan koordinasi teknis terkait:

- Instalasi Wazuh Agent
- Koneksi agent ke SOC
- Kesalahan konfigurasi dasar
- Klarifikasi grouping atau endpoint

Silakan menghubungi:

Nama : Wahyu
Kontak : *+6285762753465*

Catatan:
Mohon menyiapkan informasi berikut sebelum menghubungi tim support agar proses bantuan lebih cepat:

a. Nama entitas (PTPN-1 s.d. PTPN-11)
b. Jenis perangkat (PC/Laptop/Server)
c. Sistem Operasi (Windows/Linux)
d. Pesan error (jika ada)

Jam Dukungan
Dukungan implementasi tersedia sesuai jam kerja dan akan dikoordinasikan lebih lanjut oleh tim SOC apabila diperlukan eskalasi lanjutan.

Penutup
Dengan mekanisme grouping yang jelas, strategi instalasi yang sederhana, serta timeline implementasi yang terukur, proses onboarding endpoint ke SOC dapat berjalan **cepat, aman, dan minim gangguan operasional**.