**Integrating Wazuh with Office365**

**Prerequisites**

* A working Wazuh server.
* Administrator access to the Office365 tenant.
* Required API permissions and credentials (Tenant ID, Client ID, and Client Secret).

**Step 1: Configure API Access in Office365**

1. Go to the [Azure Portal](https://portal.azure.com/).
2. Navigate to **Azure Active Directory** > **App registrations** > **New Registration**.
3. Provide a name for the application and select **Accounts in this organizational directory only**.
4. Click **Register**.
5. Go to **Certificates & secrets** > **Client secrets** > **New client secret**.
6. Copy the **Client Secret** and store it securely.
7. Note down the **Application (client) ID** and **Directory (tenant) ID**.

**Step 2: Configure API Permissions**

1. Go to the registered app in Azure AD.
2. Select **API permissions** > **Add a permission**.
3. Choose **Microsoft Graph** > **Application permissions**.
4. Select permissions like:
   * AuditLog.Read.All
   * Directory.Read.All
   * Reports.Read.All
5. Click **Add permissions**.
6. Select **Grant admin consent** for the permissions.

**Step 3: Configure Wazuh to Integrate with Office365**

1. On your Wazuh server, navigate to the configuration directory:
2. cd /var/ossec/etc
3. Open or create the ossec.conf file using a text editor:
4. sudo nano ossec.conf
5. Add the following configuration under the <ossec\_config> section:

<office365>

<enabled>yes</enabled>

<interval>1m</interval>

<curl\_max\_size>1M</curl\_max\_size>

<only\_future\_events>yes</only\_future\_events>

<api\_auth>

<tenant\_id>Your\_Tenant\_ID</tenant\_id>

<client\_id>Your\_Client\_ID</client\_id>

<client\_secret>Your\_Client\_Secret</client\_secret>

<api\_type>commercial</api\_type>

</api\_auth>

<subscriptions>

<subscription>Audit.SharePoint</subscription>

<subscription>Audit.AzureActiveDirectory</subscription>

<subscription>Audit.General</subscription>

<subscription>DLP.All</subscription>

<subscription>Audit.Exchange</subscription>

</subscriptions>

</office365>

1. Save and close the file by pressing CTRL+O, ENTER, and CTRL+X.

**Step 4: Restart Wazuh Manager**

1. Restart the Wazuh manager to apply the changes:

sudo systemctl restart wazuh-manager

1. Check the status to ensure it is running:

sudo systemctl status wazuh-manager

**Step 5: Verify the Integration**

1. Monitor Wazuh logs for any issues:
2. tail -f /var/ossec/logs/ossec.log
3. Confirm that Office365 logs are being ingested.

Your Wazuh server is now integrated with Office365 for monitoring and alerting. If you experience any issues, check the logs and validate your API permissions.