Activer la détection de vulnérabilité dans Wazuh

La détection de vulnérabilité dans **Wazuh** est une fonctionnalité qui permet d'identifier les vulnérabilités dans les applications et les systèmes d'exploitation sur les points de terminaison surveillés.

Voici comment cela fonctionne :

- Les agents **Wazuh** collectent une liste des applications installées sur les points de terminaison surveillés et l'envoient périodiquement au serveur **Wazuh**.
- Le module de détection de vulnérabilité de **Wazuh** aide les utilisateurs à découvrir les vulnérabilités dans le système d'exploitation et les applications installées sur les points de terminaison surveillés.
- Le module fonctionne en utilisant l'intégration native de **Wazuh** avec des flux de vulnérabilité externes indexés par **Canonical**, **Debian**, **Red Hat**, **Arch Linux**, **Amazon Linux Advisories Security** (**ALAS**), **Microsoft** et la **National Vulnerability Database** (**NVD**).
- Le module de détection de vulnérabilité de **Wazuh** corrèle les données d'inventaire logiciel avec les flux de vulnérabilité pour détecter les logiciels vulnérables sur un point de terminaison surveillé.
- **Wazuh** identifie les applications vulnérables et produit des rapports de risque en utilisant les informations collectées auprès des différents fournisseurs de systèmes d'exploitation et des bases de données de vulnérabilités.

Ainsi, la détection de vulnérabilité dans **Wazuh** est un processus essentiel pour renforcer la posture de sécurité globale d'un réseau en identifiant et en atténuant rapidement les vulnérabilités potentielles.

/!\ Par défaut, elle n'est pas activée dans le fichier **ossec.conf**.

Pour l'activer :

1. On édite le fichier de configuration du serveur Wazuh (**/var/ossec/etc/ossec.conf**)
2. On cherche la catégorie comme ci-dessous et on remplace **no** par **yes** :

```
<vulnerability-detector>
  <enabled>no</enabled>
  <interval>3m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

...
```

3. Juste en dessous de ces paramètres, se trouve la configuration de la détection des vulnérabilités pour différents systèmes d'exploitation, il faut l'activer en passant **<enabled>no</enabled>** à **<enabled>yes</enabled>**

Par exemple :

```
<!-- Debian OS vulnerabilities -->
  <provider name="debian">
    <enabled>yes</enabled>
    <os>buster</os>
    <os>bullseye</os>
    <os>bookworm</os>
    <update_interval>1h</update_interval>
  </provider>
```

4. On ajoute le bloc ci-dessous dans **/var/ossec/etc/shared/default/agent.conf** sur les points de terminaisons **Linux**. Juste en dessous du commentaire « <!-- Shared agent configuration here --> » :

5. Pour les points de terminaisons **Windows** : créer un fichier **agent.conf** dans **C:\Program Files (x86)\ossec-agent\wodles**.

```
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <os>yes</os>
  <packages>yes</packages>
  <hotfixes>yes</hotfixes>
</wodle>
```

6. On enregistre, on quitte et on redémarre le serveur **Wazuh** avec **systemctl restart wazuh-manager**.

7. Pour **Windows**, on redémarre le service dans le **Gestionnaire des Tâches**.

TEST :

Pour vérifier que les paramètres et la configuration ont bien été activés, il suffit de se rendre sur l'interface web de **Wazuh,** de choisir un des hôtes supervisés par **Wazuh,** puis de cliquer sur **Vulnérabilités**.

On y trouve ainsi le tableau de bord avec les données des vulnérabilités par niveau de sévérité :

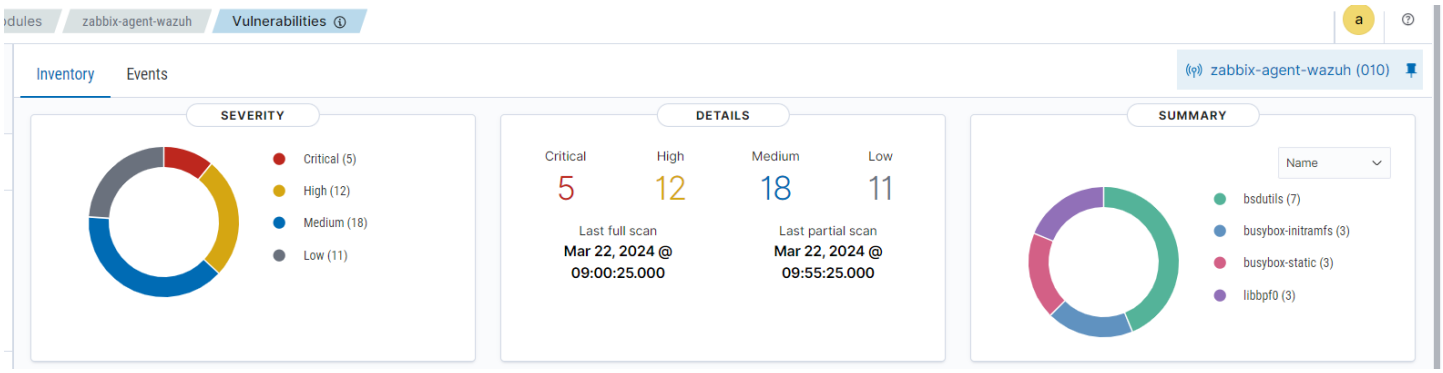

Tableau de bord à jours avec le niveau des vulnérabilités sur un point de terminaison Linux

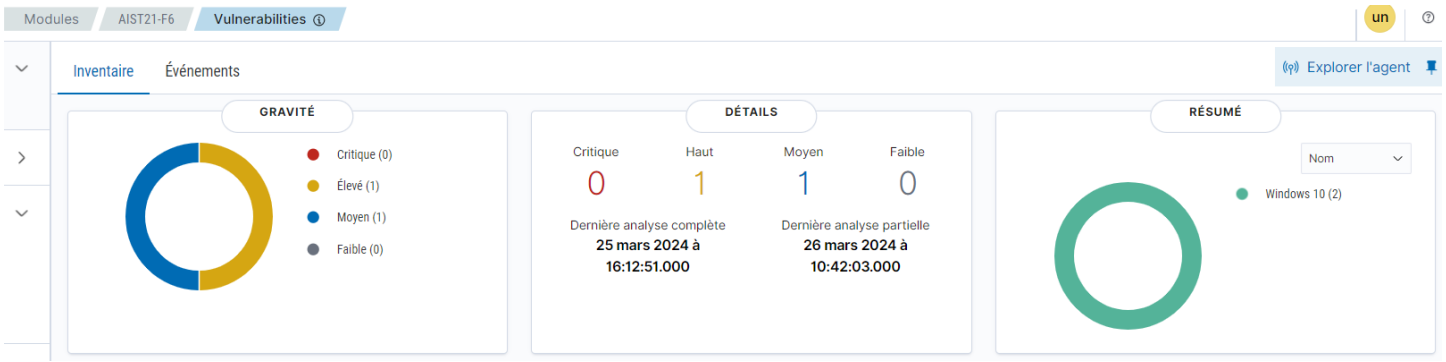

Tableau de bord à jours avec le niveau des vulnérabilités sur un point de terminaison Windows