

Configurer la surveillance des données de Who

En première configuration, nous avons pu voir comment configurer la surveillance de l'intégrité des fichiers.

Ici, nous montrons comment configurer la surveillance des données de **Who**.

La fonction de suivi des données avec **Who** (Qui), dans le contexte de **Wazuh**, se réfère à la surveillance des activités des utilisateurs sur un système. Cette fonctionnalité permet de suivre et d'analyser les actions effectuées par les utilisateurs, en particulier lorsqu'ils se connectent ou interagissent avec des fichiers du système.

I – Configurer whodata sur Linux

A – Installation du démon d'audit

```
apt-get install auditd
apt-get install audispd-plugins
systemctl restart auditd
```

B – Édition du fichier ossec.conf des agents Wazuh

1. On édite le fichier **ossec.conf** de l'agent **Wazuh** sur les hôtes supervisés.
2. On ajoute **whodata="yes"**, comme dans l'exemple ci-dessous :

```
<!-- File integrity monitoring -->
<syscheck>

...

<!-- Directories to check (perform all possible verifications) -->
<directories check_all="yes" realtime="yes" report_changes="yes" whodata="yes">/etc</directories>
<directories check_all="yes" realtime="yes" report_changes="yes" whodata="yes">/usr/bin</directories>
<directories check_all="yes" realtime="yes" report_changes="yes" whodata="yes">/usr/sbin</directories>
<directories check_all="yes" realtime="yes" report_changes="yes" whodata="yes">/bin</directories>
<directories check_all="yes" realtime="yes" report_changes="yes" whodata="yes">/sbin</directories>
<directories check_all="yes" realtime="yes" report_changes="yes" whodata="yes">/boot</directories>

...
</syscheck>
```

3. On quitte, enregistre le fichier et on redémarre l'agent **Wazuh** : **systemctl restart wazuh-agent**
4. On exécute la commande suivante pour vérifier si la règle d'audit de surveillance du répertoire sélectionné est appliquée :

```
sudo auditctl -l | grep wazuh_fim
```

Sortie de la commande :

```
root@test1-wazuh:~# sudo auditctl -l | grep wazuh_fim
-w /bin -p wa -k wazuh_fim
-w /boot -p wa -k wazuh_fim
-w /etc -p wa -k wazuh_fim
-w /sbin -p wa -k wazuh_fim
-w /usr/bin -p wa -k wazuh_fim
-w /usr/sbin -p wa -k wazuh_fim
```

Configurer la surveillance des données de Who

II – Test

1. Pour tester que la configuration fonctionne on se connecte avec un utilisateur autre que **root**.

Remarque : L'utilisateur doit faire partie du groupe **sudoers**. Pour l'ajouter : se connecter avec **root** puis exécuter la commande : **sudo usermod -aG sudo utest1**.

2. On édite un fichier qui fait partie des répertoires surveillés avec **sudo** : par exemple **/etc/hosts.allow**, le mot de passe de l'utilisateur sera demandé.
3. On quitte et on enregistre.
4. On se rend sur l'interface web de **Wazuh** et sur l'hôte sur lequel on a modifié le fichier (on clique sur la **petite flèche à côté du logo Wazuh**, puis sur « **Agents** », et **sur l'agent en question**, enfin, on clique sur « **More...** » et sur « **Integrity Monitoring** » et sur « **Events** »).

On peut y trouver l'alerte suivante :

> Mar 22, 2024 @ 11:49:16.781 /etc/hosts.allow

On peut ensuite développer le message pour le voir en détail :

Captures d'écran :		Description :
<pre> t agent.ip 192.168.4.42 t agent.name test1-wazuh-agent </pre>		L'adresse IP et le nom de l'hôte ou a été modifié le fichier.
<pre> t syscheck.audit.effective_user.name root t syscheck.audit.group.id 0 t syscheck.audit.group.name root t syscheck.audit.login_user.id 1000 t syscheck.audit.login_user.name clem t syscheck.audit.process.cwd /home/clem t syscheck.audit.process.id 5545 t syscheck.audit.process.name /usr/bin/nano t syscheck.audit.process.parent_cwd /home/clem t syscheck.audit.process.parent_name /usr/bin/sudo </pre>		Le nom de l'utilisateur (clem) en utilisant la commande sudo (privilège root) et en utilisant nano comme éditeur.
<pre> t syscheck.mode whodata t syscheck.mtime_after Mar 22, 2024 @ 11:49:14.000 t syscheck.mtime_before Mar 22, 2024 @ 11:26:33.000 t syscheck.path /etc/hosts.allow </pre>		La méthode syscheck (whodata), la date de la vérification avant et après modification et le fichier en question.

D'autres données sont visibles, mais celles-ci dessus sont les plus importantes.

Configurer la surveillance des données de Who

III – Configurer whodata sur Windows

Comment ça fonctionne

La fonctionnalité de surveillance des données **Who** utilise le sous-système d'audit de Microsoft Windows. Il obtient les informations relatives à qui apporte des modifications dans un répertoire surveillé. Ces modifications produisent des événements d'audit. Le module **FIM** traite ces événements et les rapporte au serveur **Wazuh**. Cette fonctionnalité n'est compatible qu'avec les systèmes d'exploitation Windows ultérieurs à **Windows Vista**.

Source : documentation.wazuh.com

1. On arrête l'agent Wazuh dans le **Gestionnaire des tâches** (Nom : **WazuhSvc**).
2. On édite le fichier **ossec.conf** qui se trouve dans : **C:\Program Files (x86)\ossec-agent** (avec le **Bloc-notes exécuté en administrateur** et cliquer sur **Fichier** et **Ouvrir** (se rendre dans le répertoire en question et sélectionner **Tous les fichiers** comme type de format)).
3. On ajoute **whodata="yes"**, comme dans l'exemple ci-dessous :

```
<!-- Spécifiez les répertoires à surveiller -->
<directories check_all="yes" realtime="yes" report_changes="yes" whodata="yes">C:\Users</directories>
<directories check_all="yes" realtime="yes" report_changes="yes" whodata="yes">C:\Windows</directories>
<directories check_all="yes" realtime="yes" report_changes="yes" whodata="yes">C:\System32</directories>
<directories check_all="yes" realtime="yes" report_changes="yes" whodata="yes">/bin</directories>
<directories check_all="yes" realtime="yes" report_changes="yes" whodata="yes">C:\Program Files</directories>
<directories check_all="yes" realtime="yes" report_changes="yes" whodata="yes">C:\Program Files (x86)</directories>
```

4. On enregistre et on quitte.
5. On redémarre l'agent **Wazuh** dans le **Gestionnaire des tâches**.

IV – Test

1. On peut rajouter un répertoire en question qui sera surveillé. Par exemple : **C:\Users*\Documents**
2. Dans le fichier **ossec.conf**, on rajoute la ligne suivante :

```
<directories check_all="yes" realtime="yes" report_changes="yes" whodata="yes">C:\Users\*\Documents</directories>
```

3. On enregistre et quitte l'éditeur puis on redémarre l'agent **Wazuh**.
4. On crée un fichier texte **audit_docu.txt** dans le dossier **Documents** à l'aide du **Bloc-notes** et on y ajoute un mot par exemple « **Salut** ».
5. On enregistre, on quitte et on regarde sur l'interface web de **Wazuh** dans la partie « **Events** » dans « **Integrity monitoring** » de l'hôte en question.