

Détection d'un mot-clé dans un fichier

Dans ce cas d'utilisation, on montre comment configurer **Wazuh SCA** pour détecter la présence d'un mot-clé dans un fichier. Le module **Wazuh SCA** déclenche une alerte lorsqu'il détecte le modèle dans le fichier.

I – Configuration du point de terminaison Linux

On suit les étapes suivantes sur le point de terminaison **Linux** pour créer le fichier **/usr/share/testfile.txt** et le surveiller avec le module **Wazuh SCA** :

1. On crée le fichier de test et ajouter du texte, y compris la phrase :

```
echo -e "config_file\nsecond line of configuration\npassword_enabled: yes" > /usr/share/testfile.txt
```

2. On vérifie que le fichier a été créé :

```
cat /usr/share/testfile.txt
```

Résultat attendu :

```
config_file
second line of configuration
password_enabled: yes
```

3. On crée un nouveau répertoire pour enregistrer les fichiers de stratégie personnalisés :

```
mkdir /var/ossec/etc/custom-sca-files/
```

4. On crée un nouveau fichier de stratégie **SCA** **/var/ossec/etc/custom-sca-files/keywordcheck.yml** et y ajouter le contenu suivant :

```
policy:
  id: "keyword_check"
  file: "keywordcheck.yml"
  name: "SCA use case: Keyword check"
  description: "Guidance for checking for a keyword or phrase in files on Ubuntu endpoints."
  references:
    - https://documentation.wazuh.com/current/user-manual/capabilities/sec-config-assessment/index.html
    - https://documentation.wazuh.com/current/user-manual/capabilities/sec-config-assessment/creating-custom-policies.html

requirements:
  title: "Check that the desired file exists on the monitored endpoints"
  description: "Requirements for running the SCA scans against endpoints with testfile.txt on them."
  condition: any
  rules:
    - 'f:/usr/share/testfile.txt'

checks:
  - id: 10000
    title: "Ensure password is disabled in the test configuration file"
    description: "Password is enabled in the test configuration file."
    rationale: "Password is considered weak for the custom test application. Threat actors can brute-force your password."
    remediation: "Disable password by setting the value of the password_enabled option to no."
    condition: none
    rules:
      - 'f:/usr/share/testfile.txt -> r:^password_enabled: yes$'
```

5. On modifie la propriété du fichier pour que **Wazuh** y ait accès :

```
chown wazuh:wazuh /var/ossec/etc/custom-sca-files/keywordcheck.yml
```

Détection d'un mot-clé dans un fichier

- On active le fichier de stratégie en ajoutant les lignes suivantes au bloc **<ossec_config>** du fichier de configuration de l'agent **Wazuh** à l'emplacement **/var/ossec/etc/ossec.conf** :

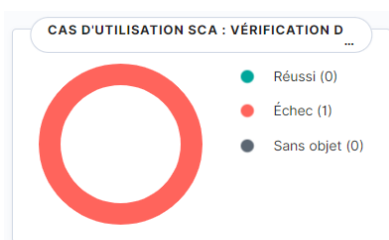
```
<sca>
<policies>
<policy enabled="yes">/var/ossec/etc/custom-sca-files/keywordcheck.yml</policy>
</policies>
</sca>
```

- On redémarre l'agent **Wazuh** pour appliquer les modifications et exécuter la nouvelle vérification **SCA** :

```
systemctl restart wazuh-agent
```

TEST :

Sur le tableau de bord **Wazuh**, accéder à l'onglet **SCA** et on sélectionne le point de terminaison **Linux** pour afficher les résultats de la vérification **SCA** personnalisée.



Cas d'utilisation SCA : vérification des mots clés ⓘ

Passé	Échoué	N'est pas applicable	Score	Terminer l'analyse
0	1	0	0%	27 mars 2024 à 12:52:01.000

Chèques (1) [Rafraîchir](#) [Exporter formaté](#)

Recherche [WQL](#)

IDENTIFIANT ↑	Titre	Cible	Résultat
10000	Assurez-vous que le mot de passe est désactivé dans le fichier de configuration de ...	Fichier : /usr/share/testfile.txt	Échoué

Lignes par page : 10 ▾ [1](#) [2](#) [3](#)

Mot de passe activé dans le fichier surveillé (password_enabled : yes)

II – Configuration du point de terminaison Windows

On suit les étapes suivantes sur le point de terminaison **Windows** pour créer le fichier et le surveiller avec le module **Wazuh SCA** :

- On exécute **PowerShell** en tant qu'administrateur et on crée le fichier de test et ajouter du texte, y compris le mot-clé :

```
New-Item "C:\Program Files\testfile.txt" -ItemType File -Value "config_file`nsecond line of configuration`npassword_enabled: no"
```

- On vérifie que le fichier a été créé :

```
Get-Content "C:\Program Files\testfile.txt"
```

Résultat attendu :

```
config_file
second line of configuration
password_enabled: no
```

Détection d'un mot-clé dans un fichier

3. On crée un nouveau répertoire pour enregistrer les fichiers de stratégie personnalisés :

```
New-Item "C:\Program Files (x86)\ossec-agent\custom-sca-files" -ItemType Directory
```

4. On ouvre le Bloc-notes en tant qu'administrateur, on crée un nouveau fichier de stratégie **SCA** avec le contenu suivant et on l'enregistre sous : **C:\Program Files (x86)\ossec-agent\custom-sca-files\keywordcheck.yml**

```
policy:
  id: "keyword_check_windows"
  file: "keywordcheck.yml"
  name: "SCA use case: Keyword check"
  description: "Guidance for checking for a keyword or phrase in files on Windows."
  references:
    - https://documentation.wazuh.com/current/user-manual/capabilities/sec-config-assessment/index.html
    - https://documentation.wazuh.com/current/user-manual/capabilities/sec-config-assessment/creating-custom-policies.html
  requirements:
    title: "Check that the desired file exists on the monitored endpoints"
    description: "Requirements for running the SCA scans against endpoints with testfile.txt on them."
    condition: any
  rules:
    - 'f:C:\Program Files\testfile.txt'
  checks:
    - id: 10001
      title: "Ensure password is disabled in the test configuration file"
      description: "Password is enabled in the test configuration file."
      rationale: "Password is considered weak for the custom test application. Threat actors can brute-force your password."
      remediation: "Disable password by setting the value of the password_enabled option to no."
      condition: none
      rules:
        - 'f:C:\Program Files\testfile.txt -> r:^password_enabled: yes$'
```

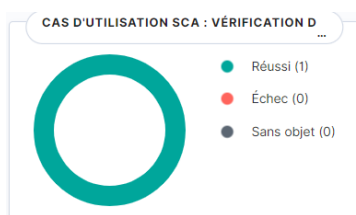
5. On active le fichier de stratégie en ajoutant les lignes suivantes au bloc **<ossec_config>** du fichier de configuration de l'agent **Wazuh** à l'emplacement **/var/ossec/etc/ossec.conf** :

```
<sca>
<policies>
  <policy enabled="yes">C:\Program Files (x86)\ossec-agent\custom-sca-files\keywordcheck.yml</policy>
</policies>
</sca>
```

6. On redémarre l'agent **Wazuh** pour appliquer les modifications et on exécute la nouvelle vérification **SCA** :

```
Restart-Service -Name WazuhSvc
```

7. Sur le tableau de bord **Wazuh**, on accède à l'onglet **SCA** et on sélectionne le point de terminaison **Windows** pour afficher les résultats de la vérification **SCA** personnalisée.



Cas d'utilisation SCA : vérification des mots clés Conseils pour rechercher un mot-clé ou une expr... 27 mars 2024 à 13:01:04.000 1 0 0 100%

Mot de passe désactivé dans le fichier surveillé (password_enabled : no)