

FICHE 3 – SIEM WAZUH – ÉVALUATION DES CONFIGURATIONS

Lien officiel de l'installation :

<https://documentation.wazuh.com/current/user-manual/capabilities/sec-config-assessment/index.html>

SOMMAIRE

A. Module évaluation de la configuration – <i>Security Configuration Assessment (SCA)</i>	1
B. Affichage des résultats de l'évaluation de la configuration.....	2
C. Interprétation des résultats de l'évaluation de la configuration.....	3
D. Mise en œuvre des mesures de remise en états.....	5

A. MODULE ÉVALUATION DE LA CONFIGURATION – SECURITY CONFIGURATION ASSESSMENT (SCA)

L'évaluation de la configuration est un processus qui vérifie si les points d'extrémité respectent un ensemble de règles prédéfinies concernant les paramètres de configuration et l'utilisation approuvée de l'application. Il s'agit de comparer la configuration actuelle aux normes industrielles et aux politiques organisationnelles établies pour identifier les vulnérabilités et les configurations erronées.

Des évaluations régulières de la configuration sont essentielles pour maintenir un environnement sûr et conforme, car elles aident les organisations à **identifier et à corriger les vulnérabilités de manière proactive**. Cette pratique renforce les contrôles de sécurité et réduit au minimum le risque d'incidents liés à la sécurité.

Wazuh propose un **module d'évaluation de la configuration de sécurité (SCA)** qui aide les équipes de sécurité à scanner et à détecter les configurations erronées dans leur environnement. L'agent Wazuh utilise des fichiers de politique pour scanner les points d'extrémité qu'il surveille. Ces fichiers contiennent des contrôles prédéfinis à effectuer sur chaque point de terminaison surveillé.

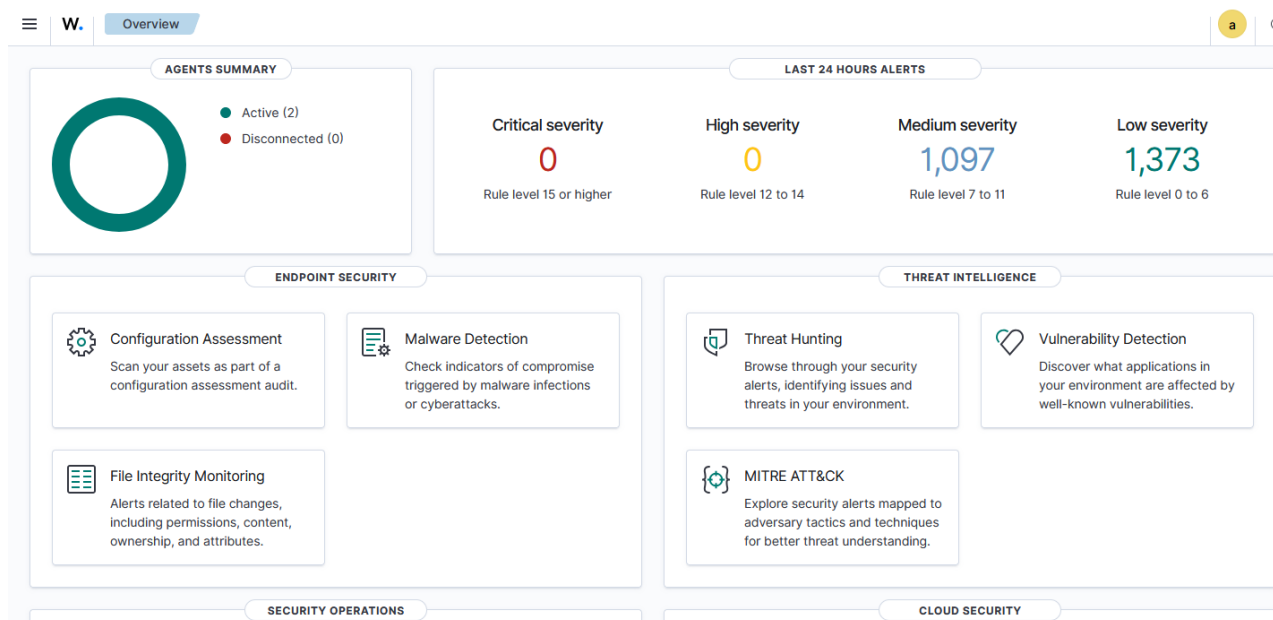
Wazuh inclut les politiques SCA originales sur la base des **critères de sécurité du Center for Internet Security (CIS)**. Ces critères servent de lignes directrices essentielles sur les meilleures pratiques pour la **protection des systèmes informatiques et des données contre les cyberattaques**. Ils fournissent des instructions claires pour établir une configuration de base sécurisée et offrent des orientations pour faire en sorte que les utilisateurs mettent en œuvre des mesures efficaces pour **protéger leurs actifs critiques et atténuer les vulnérabilités potentielles**.

Parmi les autres avantages du module Wazuh d'évaluation de la configuration - **Security Configuration Assessment (SCA)**, on peut citer :

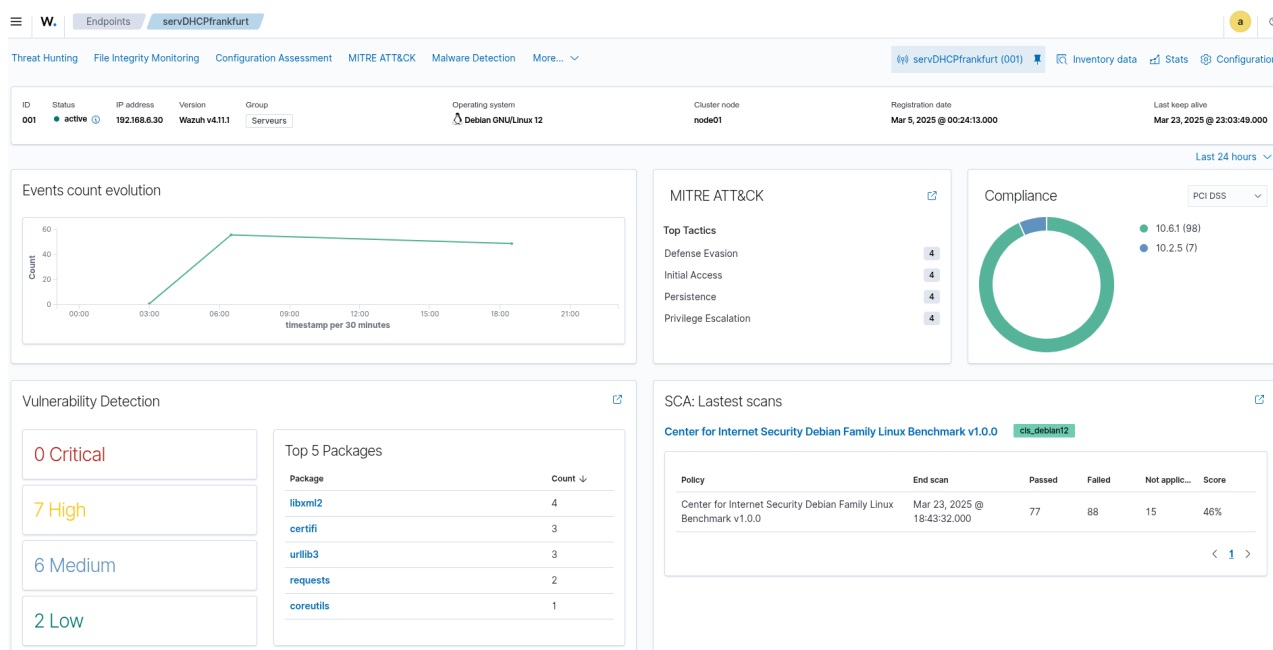
- **Gestion de la posture de sécurité** : Wazuh SCA aide les organisations à s'assurer que leurs points d'extrémité sont configurés en toute sécurité. Cela permet de minimiser les vulnérabilités résultant de mauvaises configurations et de réduire le risque d'atteintes à la sécurité.
- **Contrôle de la conformité** : Il permet aux organisations d'évaluer et de mettre en œuvre le respect des normes réglementaires, des meilleures pratiques et des politiques de sécurité intérieure.
- **Surveillance continue** : Wazuh SCA surveille en permanence la configuration des critères d'évaluation et des alertes lorsqu'il découvre des erreurs de configuration.

B. AFFICHAGE DES RÉSULTATS DE L'ÉVALUATION DE LA CONFIGURATION

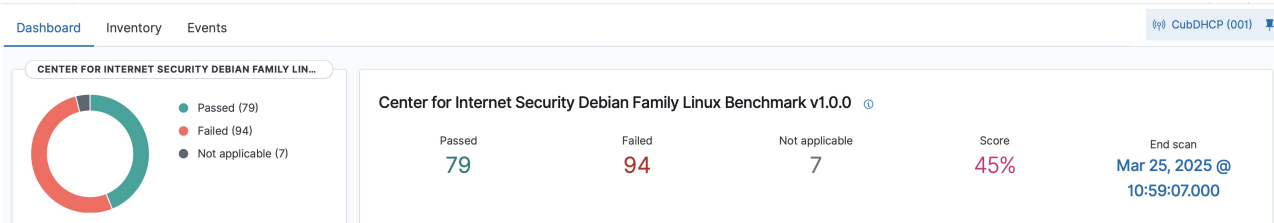
Le tableau de bord Wazuh est conçu pour fournir une vue d'ensemble des incidents et activités de sécurité dans votre environnement en temps réel. Il agrège et visualise les données provenant de différentes sources, permettant aux administrateurs et aux analystes de sécurité d'identifier et de gérer les menaces potentielles :



Pour consulter l'inventaire système de chaque terminal surveillé depuis le tableau de bord Wazuh, sélectionnez un agent et accédez au module « Données d'inventaire » comme illustré ci-dessous. La page des données d'inventaire de chaque terminal surveillé affiche son système d'exploitation, son matériel, ses processus, son interface réseau et ses packages.

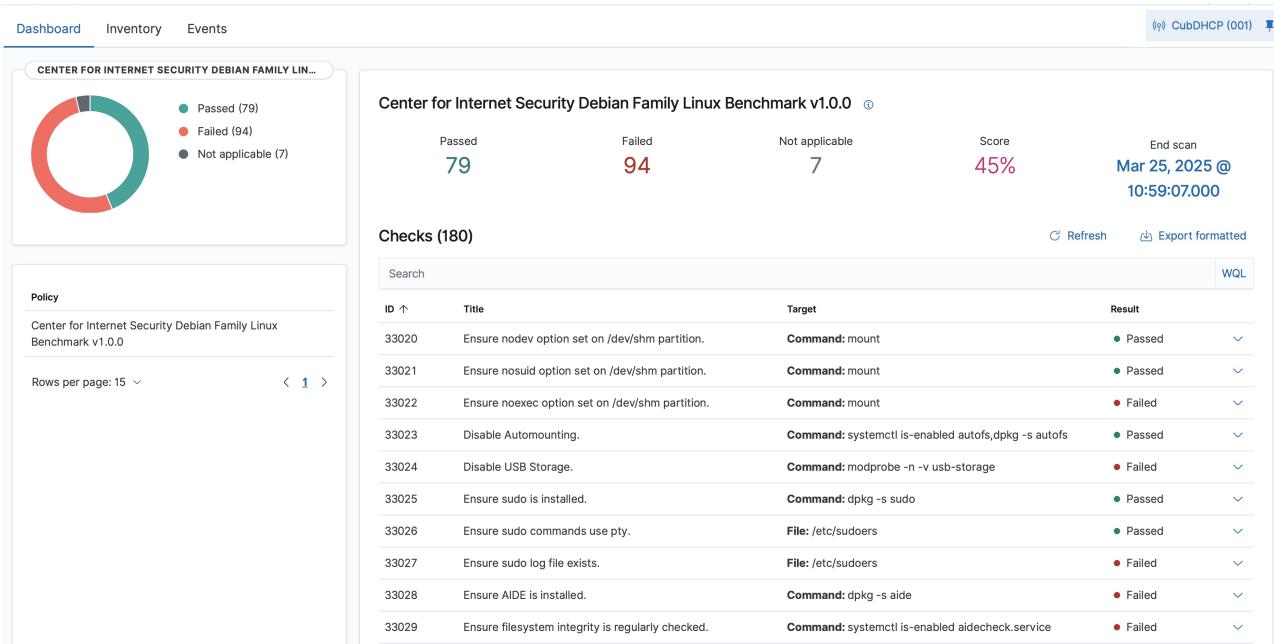


Le tableau de bord Wazuh dispose d'un module d'évaluation de la configuration (Lien « Configuration Assessment ») qui vous permet de visualiser les résultats de balayage SCA pour chaque agent.



C. INTERPRÉTATION DES RÉSULTATS DE L'ÉVALUATION DE LA CONFIGURATION

L'image ci-dessous montre la politique basée sur la référence CIS pour Debian Linux. Vous pouvez voir que 180 contrôles ont été effectués sur le point d'extrémité Debian. Sur ce nombre, 79 ont été passés, 94 ont échoué et 7 ne sont pas applicables au critère d'évaluation. Il montre également un score de 45 % qui est calculé sur la base du nombre de tests passés.



Vous pouvez cliquer sur les vérifications pour obtenir plus d'informations. Dans l'image ci-dessous, vous pouvez voir des informations telles que la raison d'être, la remédiation et une description du contrôle avec ID **33028**.

33028	Ensure AIDE is installed.	Command: dpkg -s aide	Failed	^
Rationale By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.				
Remediation Install AIDE using the appropriate package manager or manual installation: # apt install aide aide-common Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options. Initialize AIDE: Run the following commands: # aideinit # mv /var/lib/aide aide.db.new /var/lib/aide/aide.db.				
Description AIDE takes a snapshot of filesystem state including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system. Note: The prelinking feature can interfere with AIDE because it alters binaries to speed up their start up times. Run prelink -ua to restore the binaries to their prelinked state, thus avoiding false positives from AIDE.				
Checks (Condition: all) <ul style="list-style-type: none">• c:dpkg -s aide → r:Status: install ok installed• c:dpkg -s aide-common → r:Status: install ok installed				
Compliance cis: 1.4.1 cis_csc_v7: 14.9 cmmc_v2.0: AU.3.050 iso_27001-2013: A.12.4.3 nist_sp_800-53: AU-3 pci_dss_v3.2.1: 10.2.1,11.5				
33029	Ensure filesystem integrity is regularly checked.	Command: systemctl is-enabled aidecheck.service	Failed	v

Le résultat de l'analyse SCA ci-dessus montre « Failed » parce AIDE (*Advanced Intrusion Detection Environment*), qui est un outil d'intégrité des fichiers sous Linux n'est apparemment pas installé.

AIDE permet de surveiller l'état des fichiers système pour :

- Détecter les altérations causées par des erreurs accidentelles ou des modifications malveillantes (par exemple, un attaquant modifiant des binaires critiques).
- Prévenir ou limiter l'exposition en identifiant les fichiers compromis à temps.



Il est bien entendu nécessaire de faire du tri sur l'ensemble des résultats par rapport à ce qui est ce qui est nécessaire réellement à votre cas d'usage.

Par exemple, il est vérifié que certains paquets ne soient pas installés, or ce sont peut-être des services (comme apache2, cups) que vous voulez activer.

La règle qui est affichée dans cette l'image ci-dessus peut être retrouvée dans le fichier /var/ossec/ruleset/sca/cis_<distribution>.yml (exemple : /var/ossec/ruleset/sca/cis_debian12.yml).

Pour les agents Windows, les fichiers sont dans C:\Program Files (x86)\ossec-agent\ruleset\sca



Il est possible de désactiver/modifier/ajouter des règles, mais il ne faut pas modifier ces fichiers qui sont écrasés lors des mises à jour. Il n'est pas prévu de le faire dans les trois prochaines activités mais si vous voulez approfondir en autonomie, vous pouvez notamment consulter les liens suivants :

- [Comment configurer SCA](#)
- [Création de politiques SCA personnalisées](#)
- [Exemple de cas d'utilisation](#)

D. MISE EN ŒUVRE DES MESURES DE REMISE EN ÉTATS

En suivant la remédiation dans notre cas il suffit d'installer AIDE :

```
apt install aide
```

Redémarrer l'agent Wazuh pour déclencher une nouvelle analyse SCA :

```
systemctl restart wazuh-agent
```

Voici le résultat de l'analyse SCA après l'intervention :

10:59:07.000

Checks (180)

Refresh

Export formatted

Search				WQL
ID ↑	Title	Target	Result	
33020	Ensure nodev option set on /dev/shm partition.	Command: mount	Passed	▼
33021	Ensure nosuid option set on /dev/shm partition.	Command: mount	Passed	▼
33022	Ensure noexec option set on /dev/shm partition.	Command: mount	Failed	▼
33023	Disable Automounting.	Command: systemctl is-enabled autofs,dpkg -s autofs	Passed	▼
33024	Disable USB Storage.	Command: modprobe -n -v usb-storage	Failed	▼
33025	Ensure sudo is installed.	Command: dpkg -s sudo	Passed	▼
33026	Ensure sudo commands use pty.	File: /etc/sudoers	Passed	▼
33027	Ensure sudo log file exists.	File: /etc/sudoers	Failed	▼
33028	Ensure AIDE is installed.	Command: dpkg -s aide	Passed	▼
33029	Ensure filesystem integrity is regularly checked.	Command: systemctl is-enabled aidecheck.service	Failed	▼