Fiche Reflexe Wazuh Investigation de binaires malveillants

CELLULE SOC

Août 2024

Version	Date	Propriétaire	Rédacteur / Autorité
1.0	XX/08/2024	Cellule SOC	Nicolas Clerbout
Finale			

Table des matières

1 – Utilisation basique de Wazuh

Se connecter à Wazuh

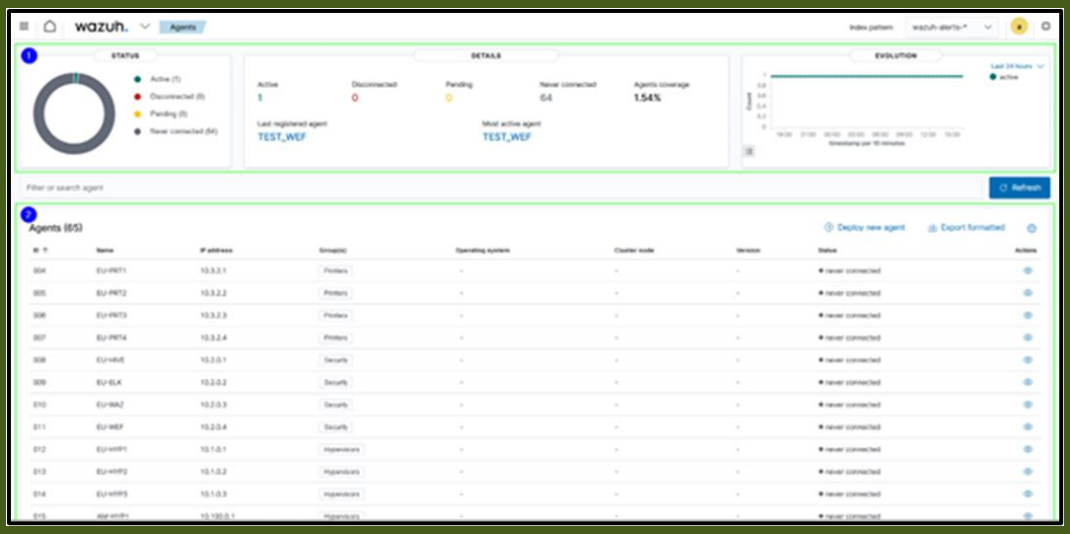
La page de connexion se trouve à l'adresse https://127.0.0.1:8443.

Une fois nos identifiants renseignés, Wazuh effectue la vérification de l'ensemble de ses services. Cette vérification prend normalement quelques secondes.

Si une ou plusieurs vérifications échouent, nous pouvons relancer manuellement le test des services en *rafraîchissant la page*. En effet, il est possible que des sauts dans la communication entre les services surviennent.

Agents

Wazuh a des *agents* monitorés et propose une vue globale sur le parc supervisé. Celle-ci est accessible en cliquant sur le menu « Agents ».



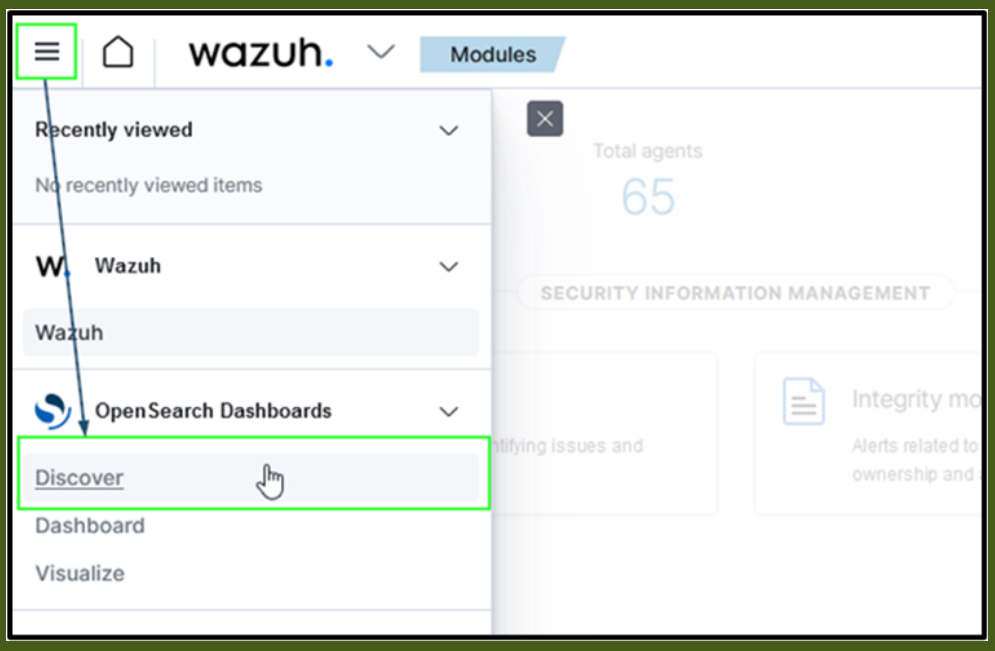
La vue « Agents » présente :

1) Des widgets informatifs sur les statuts des agents (partie supérieure de la page) ;
2) Un tableau contenant la totalité des agents.

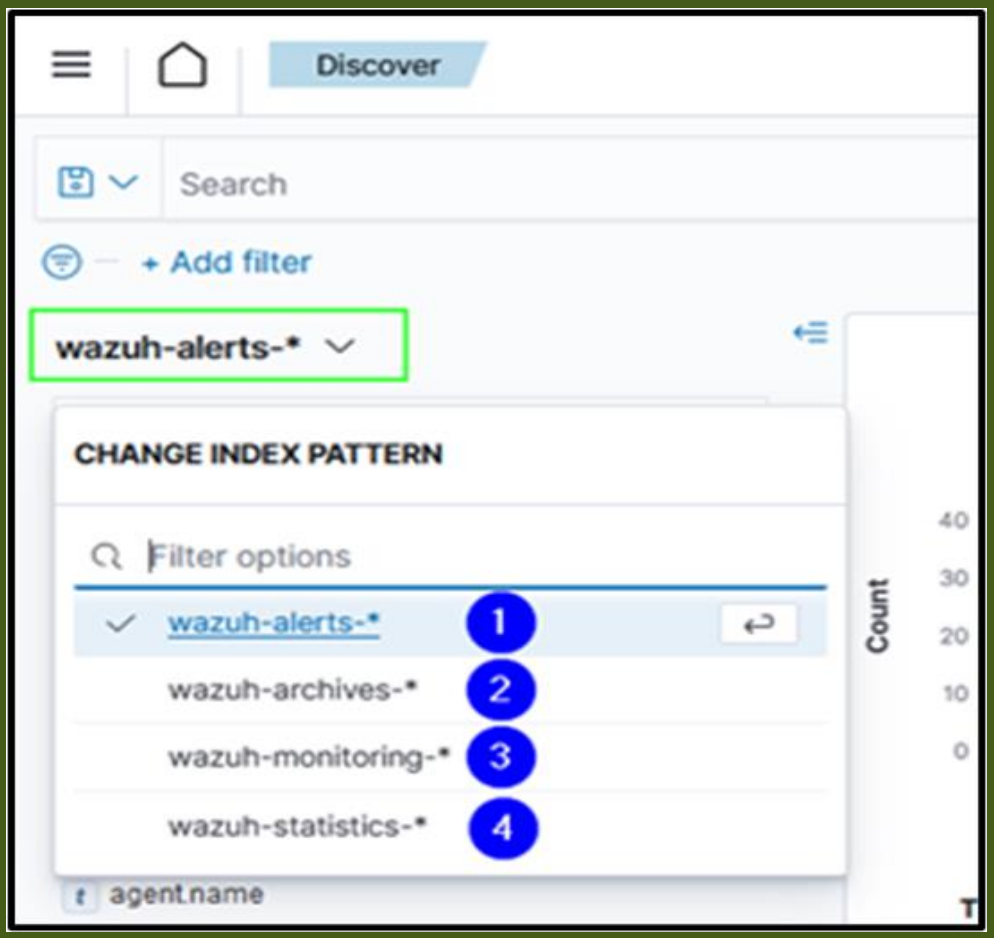
Vue Discover

La vue « Discover » nous permet d'investiguer en profondeur dans les différents index disponibles pour retrouver des informations (N.B. : c'est assez similaire à la vue « Discover » dans Elastic).

Pour y accéder :



Pour choisir l'index à explorer :

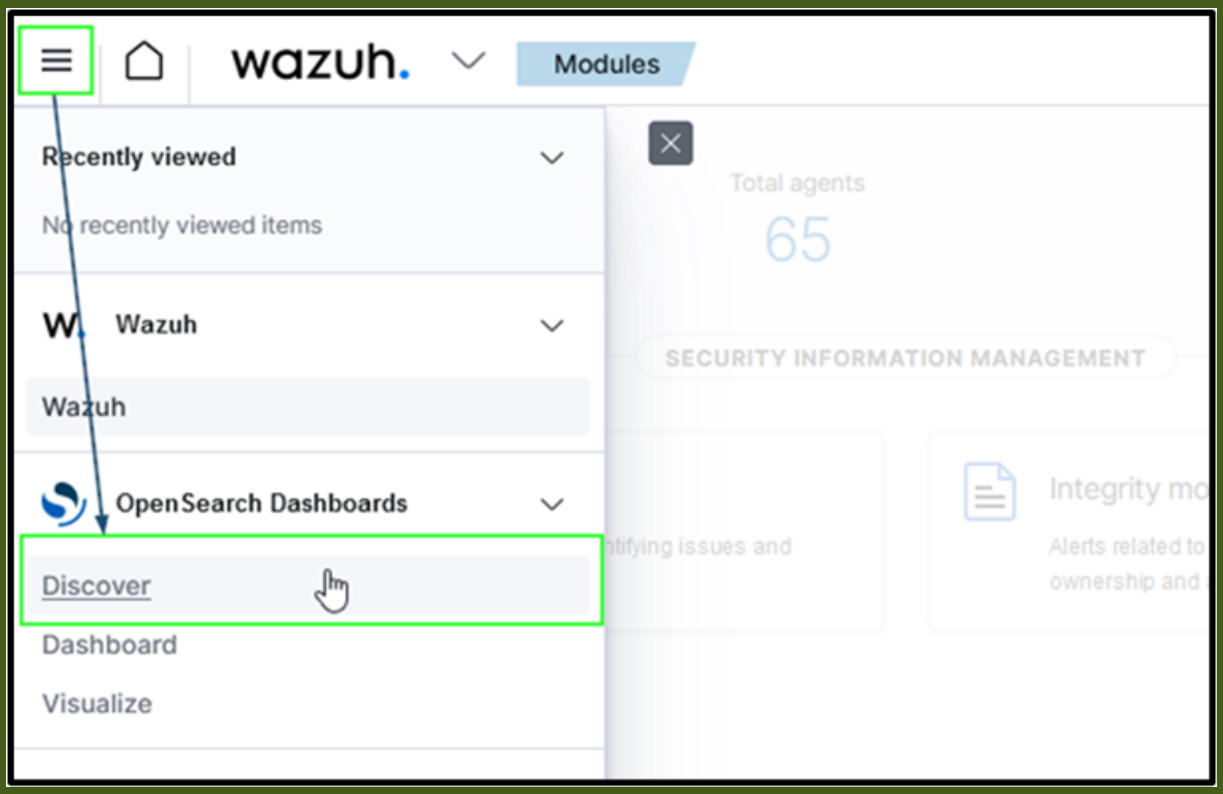


Les 4 index disponibles sont :

1) « `wazuh-alerts-*` » : contient toutes alertes générées par le processeur Wazuh. Une alerte est générée quand un ou des événements ayant eu lieu sur un terminal monitoré correspond à une règle de détection préalablement définie.
2) « `wazuh-archives-*` » : contient tous les événements générés et reçus par Wazuh y compris ceux qui ne déclenchent pas d'alerte.
3) « `wazuh-monitoring-*` » : contient l'historique des statuts de connexion des agents monitorés. A tout moment, un agent peut avoir l'un des statuts suivants : actif, déconnecté, en attente ou jamais connecté (active / disconnected / pending / never connected).
   Cet index conserve une trace des différents statuts des agents dans le temps.
4) « `wazuh-statistics-*` » : contient tous les statistiques du serveur Wazuh sur le nombre d'événements reçus et traités, le nombre d'octets reçus, les sessions TCP, etc.

2 – Investigation d'un binaire malveillant via Wazuh

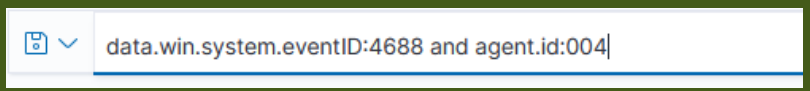
Se rendre sur la vue « Discover » :



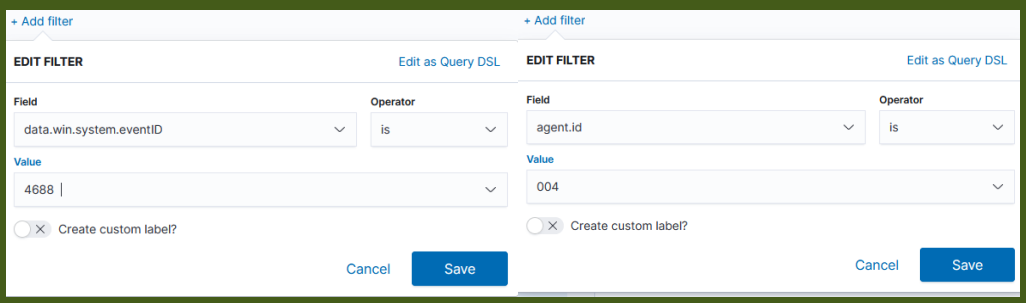
Filtres agent et Event ID

Nous nous intéressons à la création de nouveau processus, ce qui correspond à l'ID `4688` d'événement Windows (voir https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4688). Nous appliquons aussi un autre filtre, cette fois sur les agents wazuh.

Pour cela, on peut écrire une requête dans le champ de recherche ou utiliser le bouton « `Add filter` » :



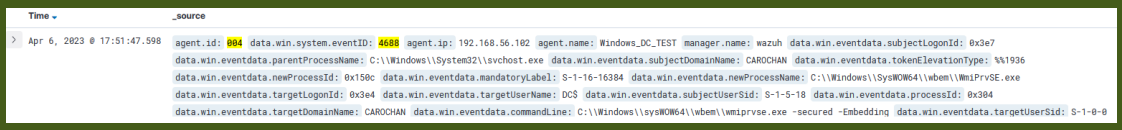
Filtrage par requête dans le champ de recherche



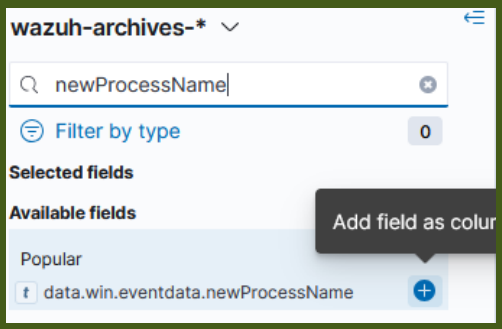
Filtrage en utilisant le bouton « Add filter »

Ajout de colonnes pertinentes pour la visualisation

Le seul filtrage par événement et `ID` de l'agent ne permet pas une visualisation claire puisque les résultats affichent un grand nombre d'informations qui ne sont pas toutes pertinentes :



Pour une meilleure visibilité, nous pouvons sélectionner les champs à afficher sous forme de colonnes. Pour cela, il faut rechercher le nom du champ qui nous intéresse dans la barre prévue à cet effet sous le nom de l'index et cliquer sur le bouton d'ajout de colonne :



Dans notre exemple, les champs `data.win.eventdata.newProcessName` et `data.win.eventdata.parentProcessName` sont affichés :

Time	data.win.eventdata.newProcessName	data.win.eventdata.parentProcessName
Apr 6, 2023 @ 17:51:47.568	C:\\Windows\\SysWOW64\\msiexec.exe	C:\\Windows\\System32\\msiexec.exe
Apr 6, 2023 @ 17:51:45.722	C:\\Windows\\System32\\msiexec.exe	C:\\Windows\\System32\\services.exe
Apr 6, 2023 @ 17:51:45.702	C:\\Windows\\System32\\msiexec.exe	C:\\Windows\\explorer.exe

Cette visualisation facilite l'analyse en nous donnant le nom et le chemin non seulement du nouveau processus créé mais aussi de son processus parent (processus qui l'a engendré). Cela permet notamment d'identifier des relations de parenté anormales entre processus telles que des instances de `powershell.exe` ou `cmd.exe` générées par un logiciel de traitement de texte par exemple.

Champs TokenElevationType et mandatoryLabel

Dans l'analyse des processus, il faut également prêter attention aux différents niveaux de privilèges qui interviennent : d'une part le niveau de privilège utilisé pour lancer le nouveau processus et d'autre part celui du processus lui-même.

Dans un premier temps, nous nous intéressons au champ `data.win.eventdata.tokenElevationType`. Celui-ci nous permet de connaître les droits de l'utilisateur en cours au moment de la création du processus. Voici les valeurs possibles :

ID	Nom Complet
%%1936	TokenElevationTypeFull (1)
%%1937	TokenElevationTypeElevated (2)
%%1938	TokenElevationTypeLimited (3)

Le type « Full » correspond au plus haut niveau de privilège (compte système local, compte de service, compte administrateur).

Le type « Elevated » suppose un utilisateur authentifié membre du groupe administrateurs (autorisé à effectuer certaines tâches comme administrateur).

Le type « Limited » correspond au niveau de privilège ne requérant pas de droits d'administration.

Ensuite, il est important de regarder aussi le champ `data.win.eventdata.mandatoryLabel`. Celui-ci permet de comprendre le niveau d'intégrité du processus. Ce niveau exprime le degré de confiance accordé au processus lui-même en déterminant les ressources auxquelles il peut accéder et ses privilèges sur le système. En fonction de sa valeur, nous pouvons donc comprendre plus précisément à quel type de processus nous avons affaire.

ID	Nom	Privilèges	Accès
S-1-16-0	Untrusted	Fortes restrictions, pas de privilèges particuliers	Accès très limité aux ressources et autres processus

S-1-16-4096	Low Integrity	Limités aux opérations non essentielles (pas de modification des fichiers systèmes ou d'installation d'applications)	Accès limité aux fichiers et répertoire temporaire utilisateur ; Accès minimal aux ressources réseau
S-1-16-8192	Medium Integrity	Suffisants pour installer des applications sans affecter les composants critiques du système	Accès aux fichiers et dossiers de l'utilisateur, aux paramètres de configuration utilisateur et aux périphériques connectés
S-1-16-12288	High Integrity	Privilèges d'administration : installation et désinstallation de logiciel, modification des paramètres de sécurité, etc.	Accès aux répertoires systèmes et aux fichiers critiques, aux outils d'administration et aux services et processus de moindre niveau d'intégrité
S-1-16-16384	System Integrity	Privilèges système complets, y compris les politiques de sécurité. Utilisé par le noyau Windows et les services essentiels	Accès illimité : ressources système et réseau, processus et services essentiels

En corrélant toutes les informations recueillies, nous pourrons déterminer si un processus est dangereux ou non. Cela nous permet du même coup de savoir s'il est nécessaire ou non de demander une suppression de fichier sur le système en question.