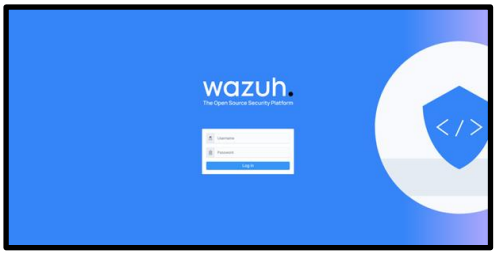
Oiseau Rouge

Fiche réflexe à mettre à jour

Utilisation de Wazuh

Se connecter à Wazuh

Sur la page de connexion, saisissez vos identifiants (admin:admin sur https://127.0.0.1:8443) :



Après avoir entré les identifiants, Wazuh va effectuer la vérification de l'ensemble de ses services, cela prend quelques secondes, le temps que toutes les vérifications soient faites.

Si une vérification échoue, vous pouvez relancer le test des services à la main en rafraîchissant la page. En effet, il se peut que des sauts dans la communication entre les services arrivent.

➢ Agents

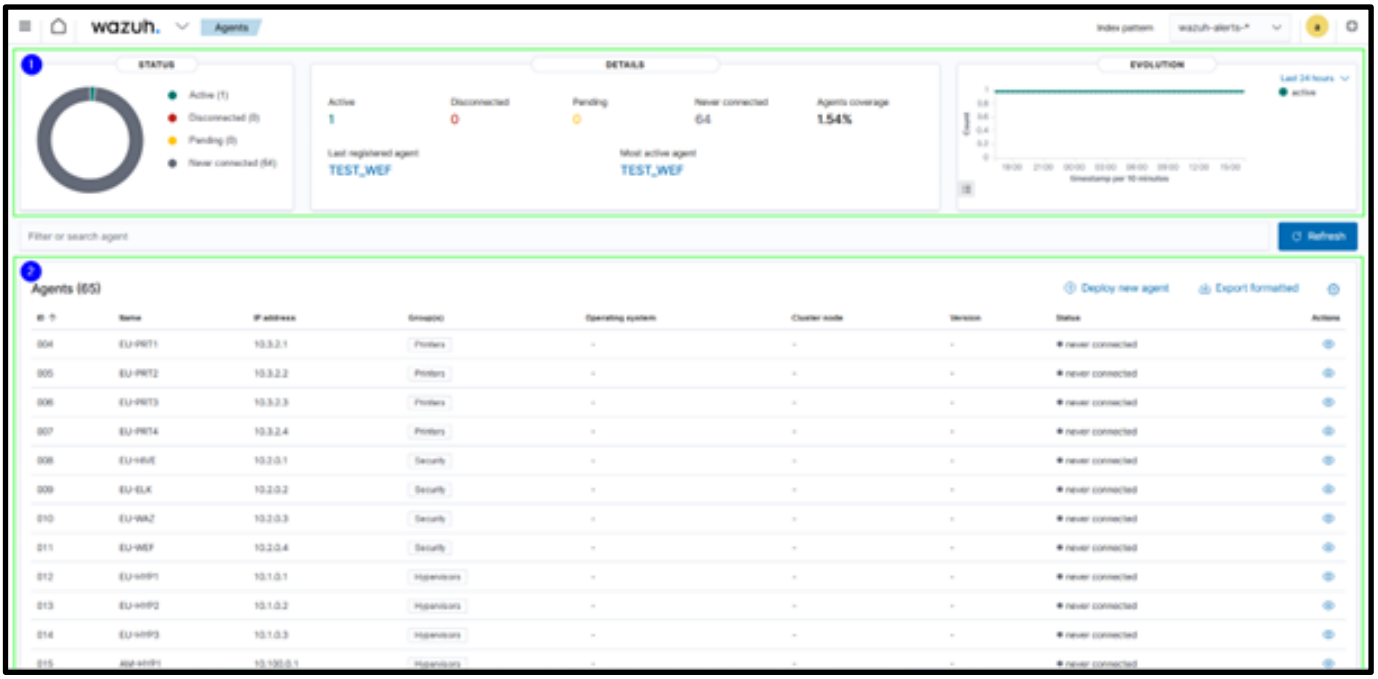
Wazuh a des agents monitorés et propose une **vue** globale sur le parc supervisé.

Pour cela, il faut cliquer sur le menu « *Agents* » :

Vous pouvez également accéder au menu directement à l'aide de ce lien :

https://<FQDN_WAZUH>/app/wazuh#/agents-preview/

La vue « Agents » s'architecture comme ci-dessous :

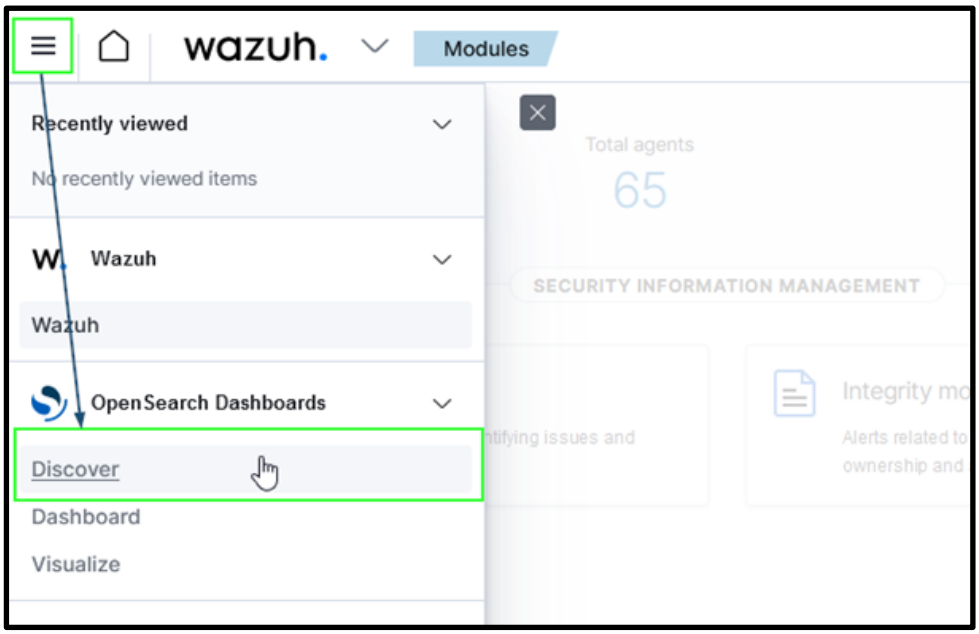


1. Des widgets informatifs sur les statuts des agents
2. Un tableau contenant la totalité des agents

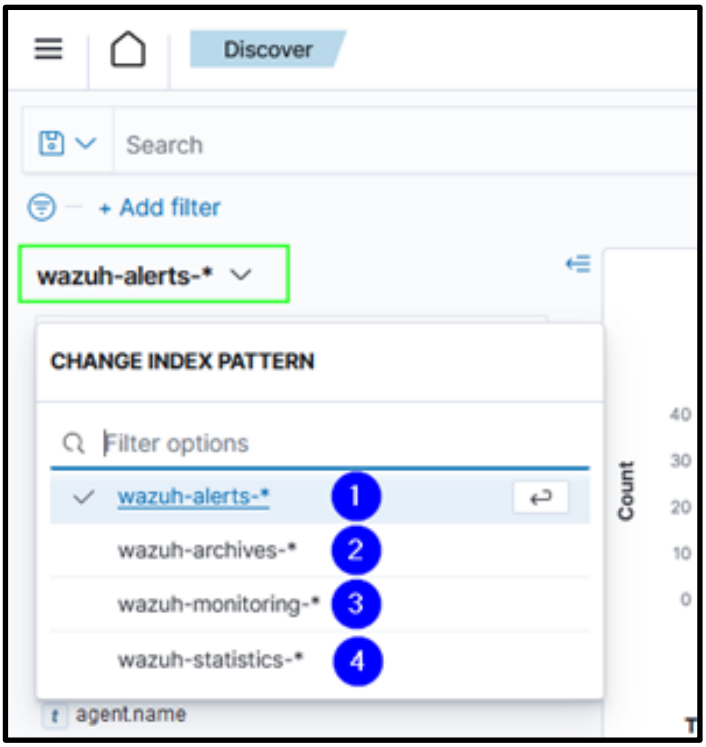
➢ Vue Discover

La vue « *Discover* », comme pour Elastic, va vous permettre d'investiguer en profondeur dans les différents index pour retrouver des informations.

Pour y accéder :



Vous allez avoir plusieurs choix d'index, comme vous pouvez le voir ci-dessous :



1. Va contenir toutes les **alertes de sécurité** générées par le processeur Wazuh.
2. Va contenir tous les **logs bruts** générés et reçu par Wazuh.

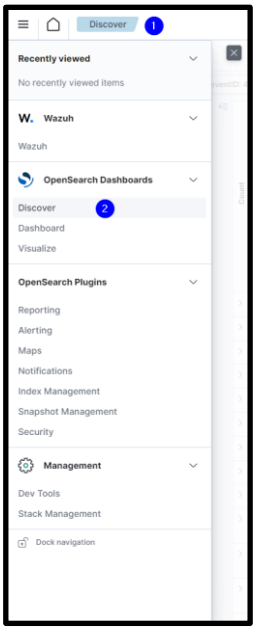
3. Va contenir le **monitoring** des agents.

4. Va contenir toutes **les statistiques globales du système** sur le nombre d'événements reçus, la taille, etc.

Ensuite, pour la partie recherche, c'est identique à la partie Elastic > Vue Discover.

Investigation d’un binaire malveillant via Wazuh

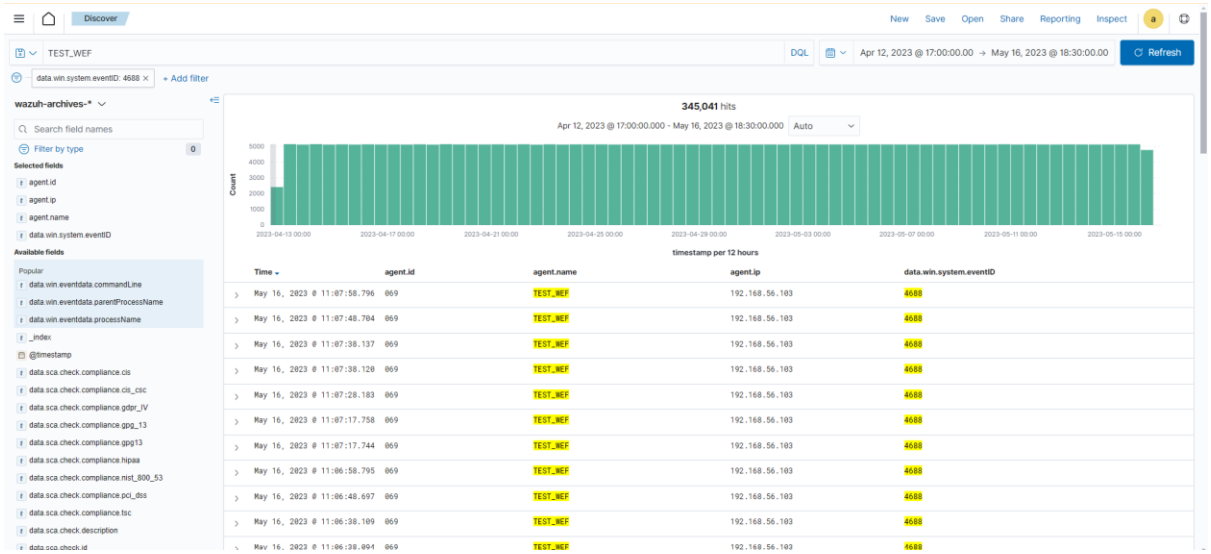
Se rendre sur la vue Discover comme ceci :



Filtrer sur l'agent souhaité, puis sur l'event ID Windows correspondant à la création de nouveaux processus (Event ID et lien vers les détails de celui-ci à compléter)

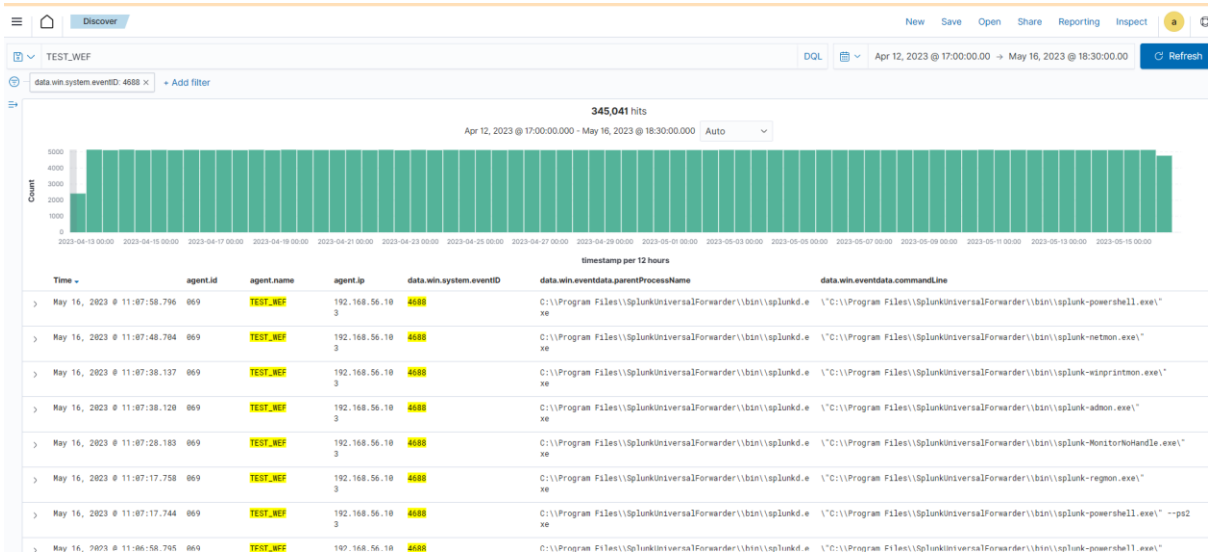
Event ID : 4688

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4688



Capture d'écran des filtres

AjouterRajouter les colonnes du chemin du processus parent et du processus fils pour avoir une meilleure visualisation des événements et des acteurs., pPar exemple ici, si je souhaite rajouter en visibilité l'ID de l'événement Windows, je fais comme ci-dessous :



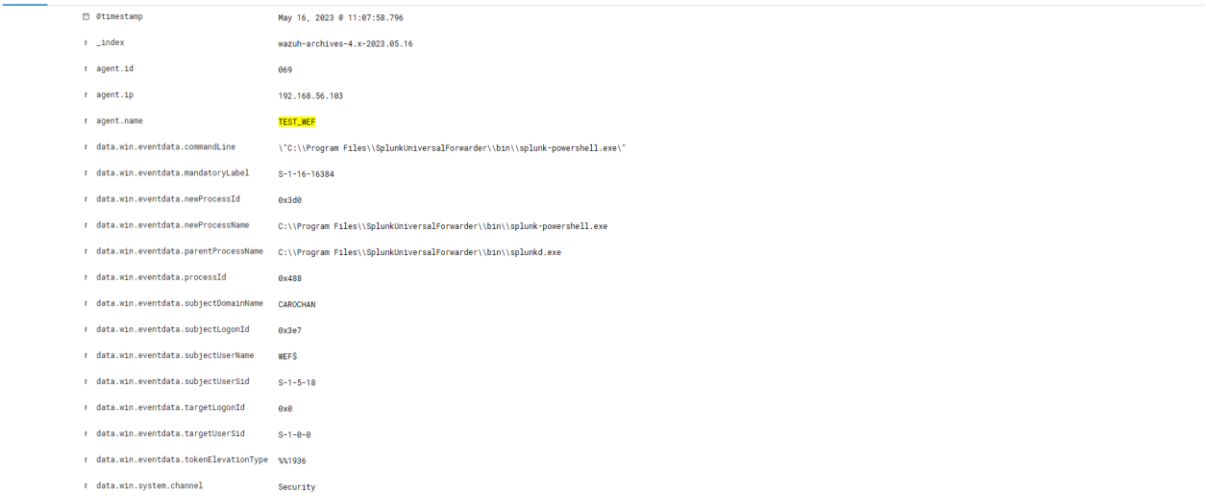
Capture d'écran montrant l'ajout d'une colonne

parentProcessName : Identifie le processus parent (splunkd.exe).

commandLine : Affiche la commande exécutée par le processus fils.

Ces colonnes aident à analyser les relations parent-fils des processus.

Une fois que nous avons les colonnes souhaitées, nous pouvons analyser plus facilement les processus et identifier, par exemple **les relations entre les processus parent et fils. Cela aide à déterminer si un processus enfant légitime est initié par un processus parent légitime ou si un comportement suspect est détecté (exemple : un processus légit déclenchant un processus malveillant)**.



@timestamp	May 16, 2023 @ 11:07:58.796
_index	wazuh-archives-4.x-2023.05.16
agent.id	069
agent.ip	192.168.56.103
agent.name	TEST_WEF
data.win.eventdata.commandLine	\"C:\\Program Files\\SplunkUniversalForwarder\\bin\\splunk-powershell.exe\"
data.win.eventdata.mandatoryLabel	S-1-16-16384
data.win.eventdata.newProcessId	0x3d0
data.win.eventdata.newProcessName	C:\\Program Files\\SplunkUniversalForwarder\\bin\\splunk-powershell.exe
data.win.eventdata.parentProcessName	C:\\Program Files\\SplunkUniversalForwarder\\bin\\splunkd.exe
data.win.eventdata.processId	0x488
data.win.eventdata.subjectDomainName	CAROCHAN
data.win.eventdata.subjectLogonId	0x3e7
data.win.eventdata.subjectUserName	WEF$
data.win.eventdata.subjectUserSid	S-1-5-18
data.win.eventdata.targetLogonId	0x0
data.win.eventdata.targetUserSid	S-1-0-0
data.win.eventdata.tokenElevationType	%%1936
data.win.system.channel	Security

Capture d’écran de l’observation

Le processus splunkd.exe (parent) a initié le processus splunk-powershell.exe (fils).

Cette relation est typique d'un fonctionnement normal dans Splunk Universal Forwarder. Par exemple, splunkd.exe utilise des modules tels que splunk-powershell.exe pour effectuer des tâches spécifiques (comme collecter des données via des scripts PowerShell).

Il est important ensuite de prêter attention à plusieurs éléments du log~~s~~, comme le "TokenElevationType", qui va permettre de savoir, en fonction de sa valeur **si le processus s'exécute avec des privilèges limités, élevés ou complets, ce qui peut indiquer un comportement suspect ou légitime**.

Voici les valeurs possibles :

ID	Nom complet
%%1936	**TokenElevationTypeDefault** → Le processus fonctionne avec **les droits standards** d'un utilisateur (pas d'élévation de privilèges).
%%1937	**TokenElevationTypeFull** → Le processus s'exécute avec **des privilèges administratifs élevés** (Exemple : un programme lancé en tant qu'administrateur).
%%1938	**TokenElevationTypeLimited** → Le processus fonctionne avec **des restrictions supplémentaires**, même si l'utilisateur est administrateur.

Ensuite, il y a le champ "mandatoryLabel", qu'il est important de regarder pour comprendre le **niveau d'intégrité associé au processus, indiquant si celui-ci est exécuté avec des droits utilisateur standards ou élevés**.. En fonction de sa valeur, on va pouvoir déterminer plus précisément à quel type de processus nous avons affaire~~à faire~~.

ID	Nom	Privilèges	Accès
S-1-16-0	Untrusted Mandatory Level	Aucun	Très restreint
S-1-16-4096	Low Mandatory Level	Accès minimal	Restreint
S-1-16-8192	Medium Mandatory Level	Accèsstandard utilisateur	Normal
S-1-16-12288	High Mandatory Level	Administrateur	Élevé
S-1-16-16384	System Mandatory Level	Complet	Total