Wazuh - Utilisation

Sommaire

Introduction

Wazuh est une application catégorisée comme SIEM (gestion des journaux de sécurité et d'administration) et EDR (Endpoint Detection and Response) servant à détecter tous les évènements sur les machines disposant de l'agent Wazuh. Cela permet de détecter des potentielles attaques ou tentatives d'attaque sur l'infrastructure.

La force de cette application la rend également très compliquée à utiliser, en raison d'un grand nombre de menus et de sous menus menant à des fonctionnalités différentes.

Ce guide d'utilisation va couvrir les fonctionnalités les plus importantes dans l'utilisation de Wazuh pour assurer une bonne compréhension et analyse des évènements de l'infrastructure.

Accès à l'interface

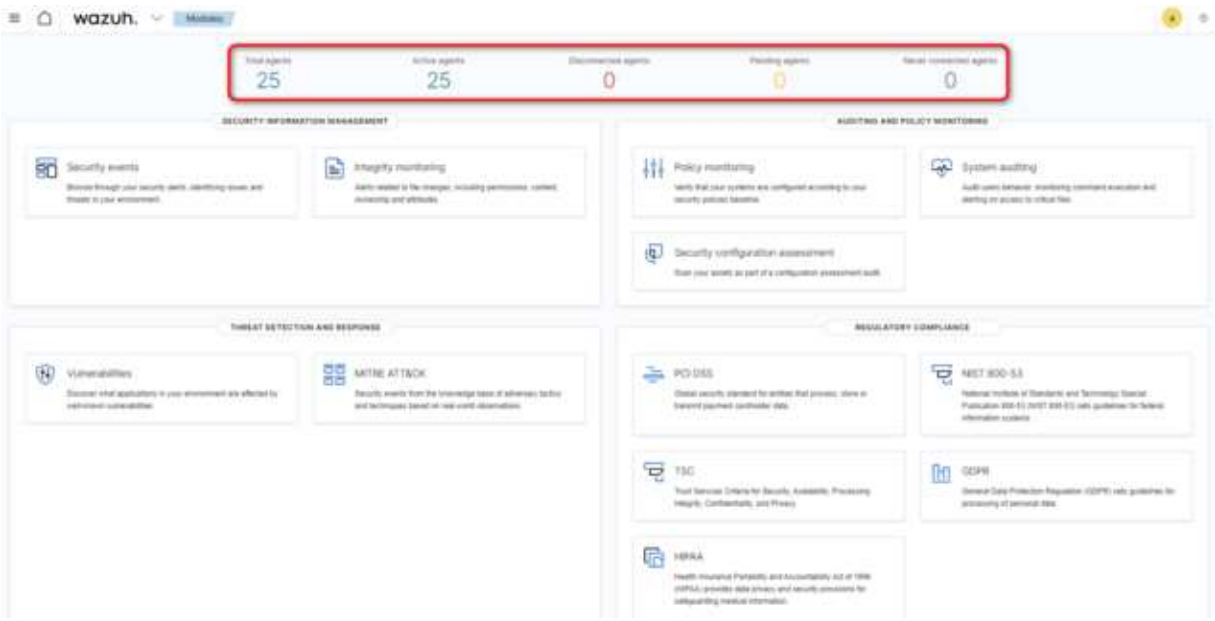
L'interface de Wazuh est accessible à l'adresse https://wazuh.crous-nantes.fr

Les identifiants administrateurs pour la connexion sont dans le KeePass Admin.

Présentation de l'interface

Tableau de bord

La page principale accessible après la connexion est le point d'accès à tous les modules qui sont décrit dans la suite de ce guide. Elle ressemble à ceci :



L'encadré en rouge indique le nombre d'agents total ainsi que leur status.

La première section nommée "Security information management" regroupe les modules concernant la visualisation et l'analyse de tous les évènements recueillis sur l'intégralité des agents.

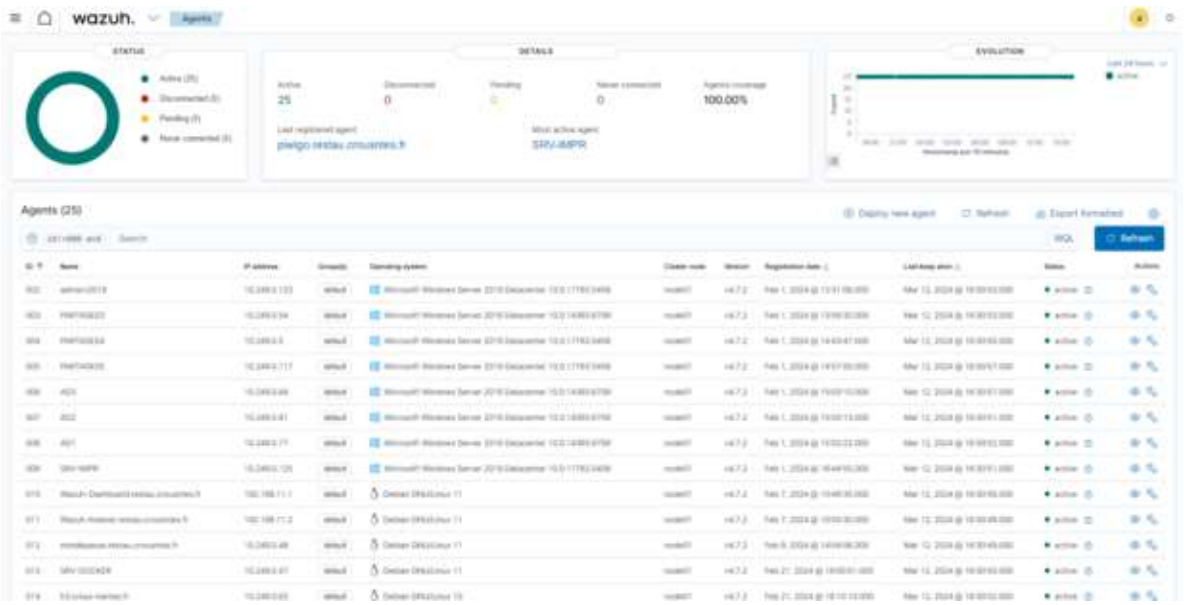
La deuxième section nommée "Auditing and policy monitoring" regroupe les modules permettant de créer des politiques de monitoring et de vérifier leur conformité.

La troisième section nommée "Threat detection and response" regroupe les modules permettant d'analyser les vulnérabilités de tous les serveurs sondés et d'accéder à la base de données MITRE qui contient un grand nombre d'informations sur les types d'attaques, les groupes d'attaquants etc..

La quatrième section permet de vérifier la conformité du système aux différents règlements de la protection des données comme RGPD, PCI DSS etc...

Vue des agents

La page d'information sur les agents est accessible via le menu déroulant puis dans Agents :



Cette page donne les détails de chaque agent, à savoir l'adresse IP de chaque machine, l'OS correspondant, la version de l'agent installé, la date d'enregistrement de l'agent, la date du dernier check et le status.

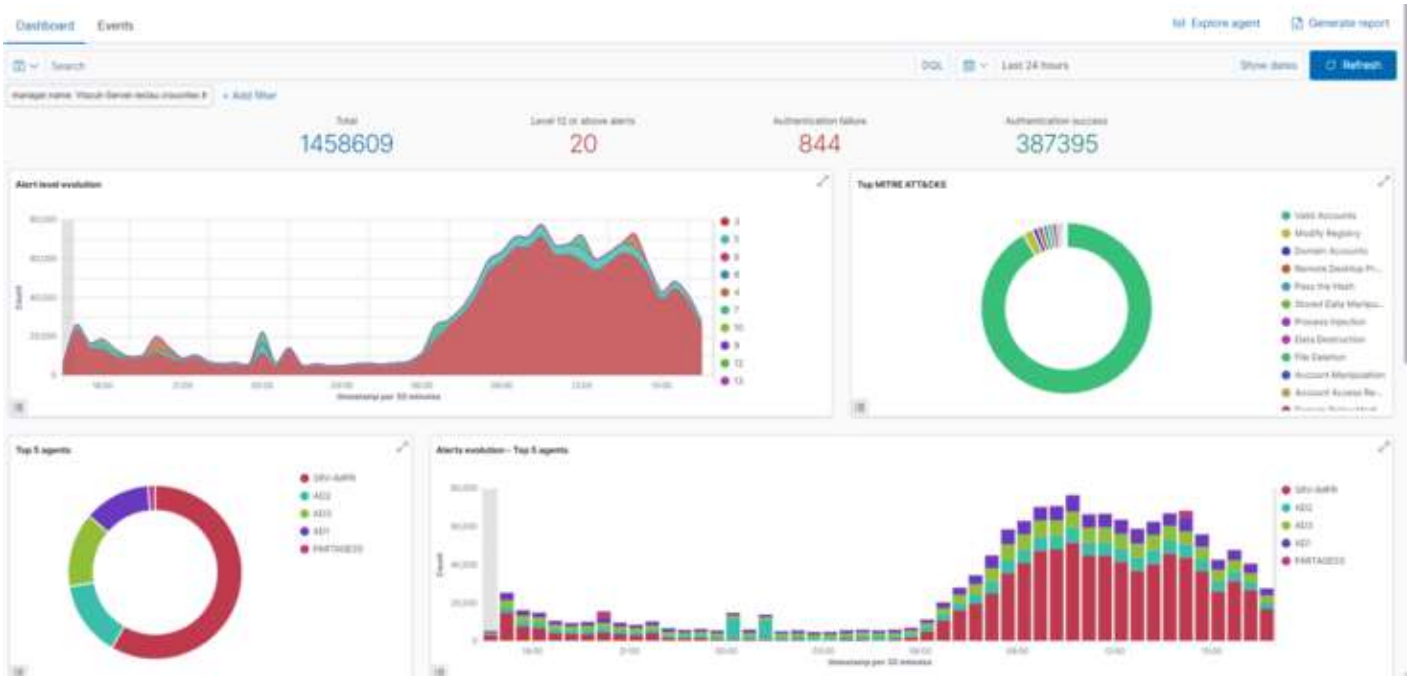
Par défaut, les agents sont triés par ID dans l'ordre croissant. Il est possible de trier par d'autres critères si besoin.

En cliquant sur un agent, on accède à la page (décrite dans les sections ci-dessous) contenant les évènements de sécurité de la machine liée à l'agent.

Présentation des modules

Management des évènements de sécurité

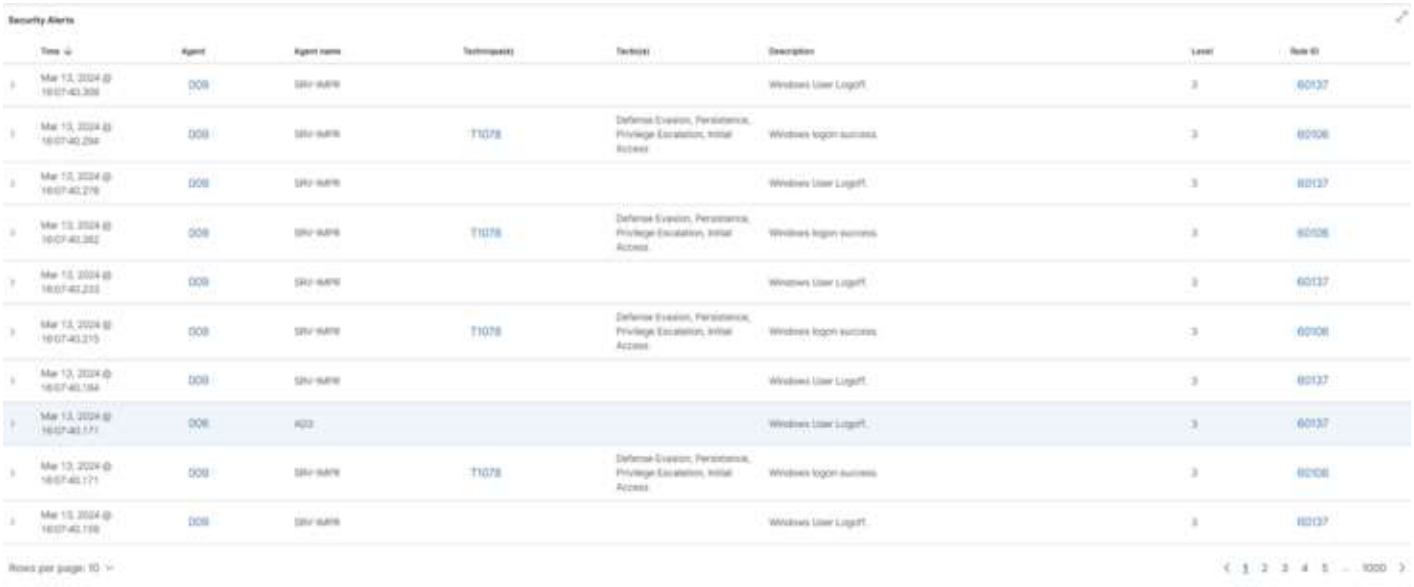
Évènements de sécurité



Cette page est un tableau de bord regroupant tous les évènements de sécurité de tous les agents enregistrés. Sans filtres ni agents épinglés, elle permet d'avoir une vision globale sur l'infrastructure grâce à des graphiques pertinents bien que compliqués à analyser.

Le premier graphique représente l'évolution en temps réel du nombre d'évènements, le deuxième représente la part de chaque type de méthode MITRE dans l'ensemble des évènements et les autres sont en lien avec l'activité des 5 agents les plus actifs.

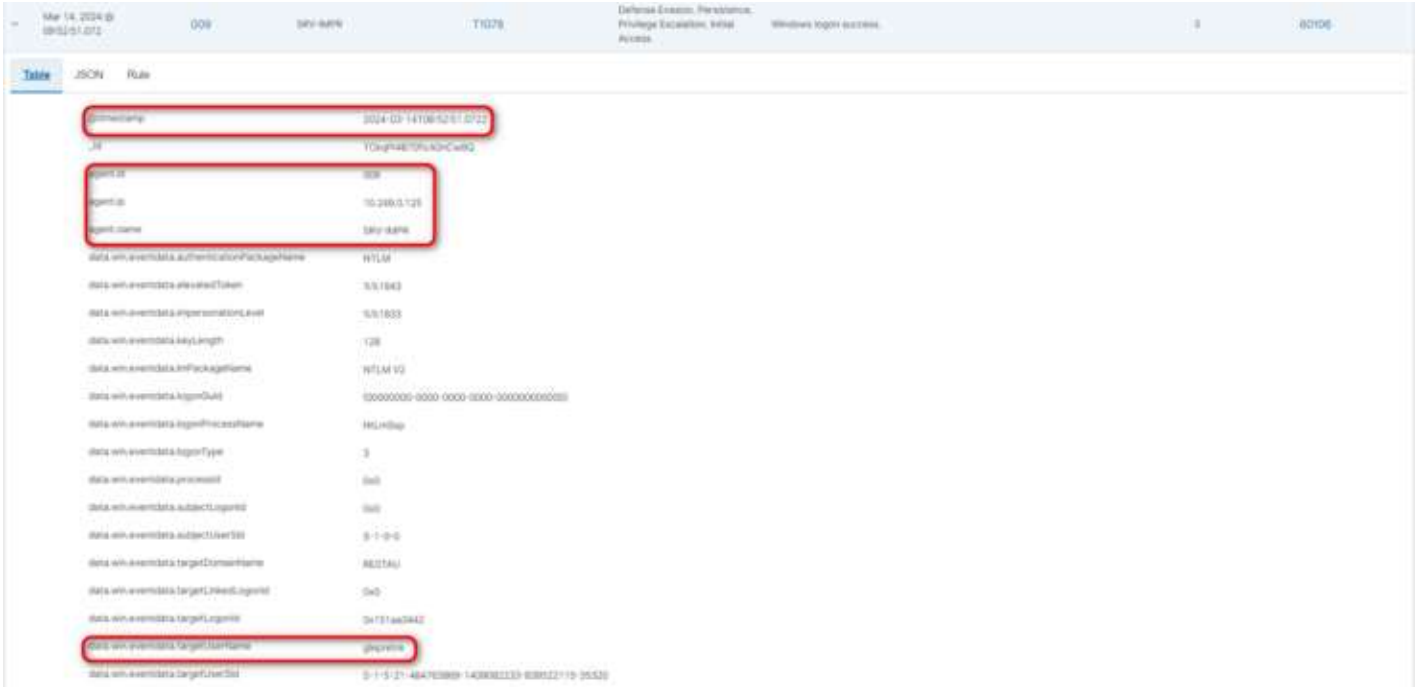
Ces graphiques permettent d'identifier rapidement l'état de l'infrastructure en constatant d'éventuelles anomalies comme un pic d'alerte à un temps donné, ou la présence d'un évènement particulier survenu très fréquemment.



La suite de la page est donc la liste des évènements remontés au serveur Wazuh. Ils apparaissent par ancienneté, et permettent d'identifier le type d'évènements (souvent des évènements de connexion d'utilisateurs), le nom et l'ID de l'agent concerné.

En cliquant sur un évènement, on a accès à un tas d'information, dont la date de l'évènement, les informations sur l'agent concerné, l'identité de l'utilisateur concerné et plein d'autres qui peuvent être utiles dans certains contextes.

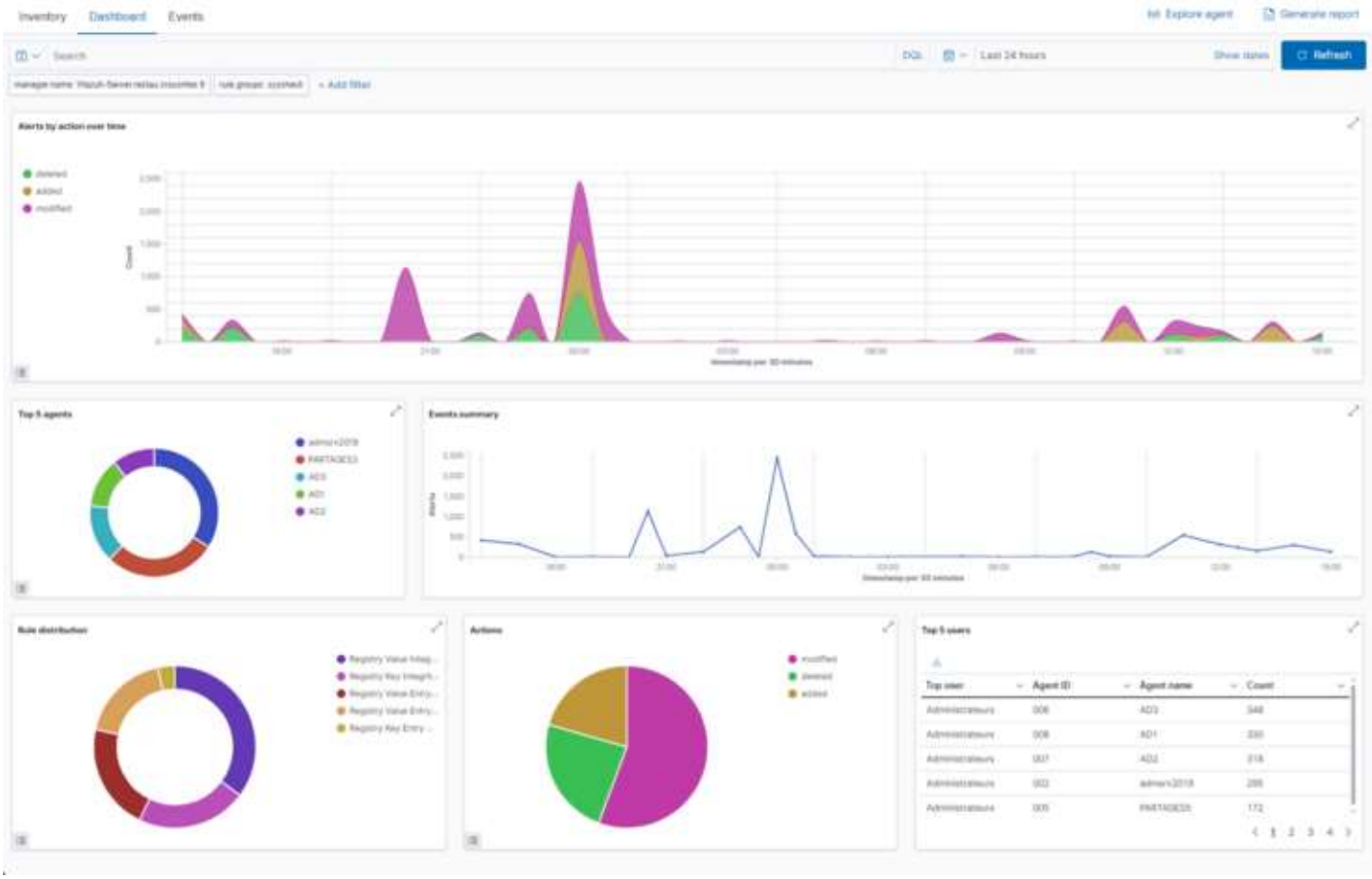
Il est possible d'exporter ces informations sous forme de fichier JSON si besoin. Cela peut être pratique pour utiliser des scripts par la suite.



Monitoring de l'intégrité des machines

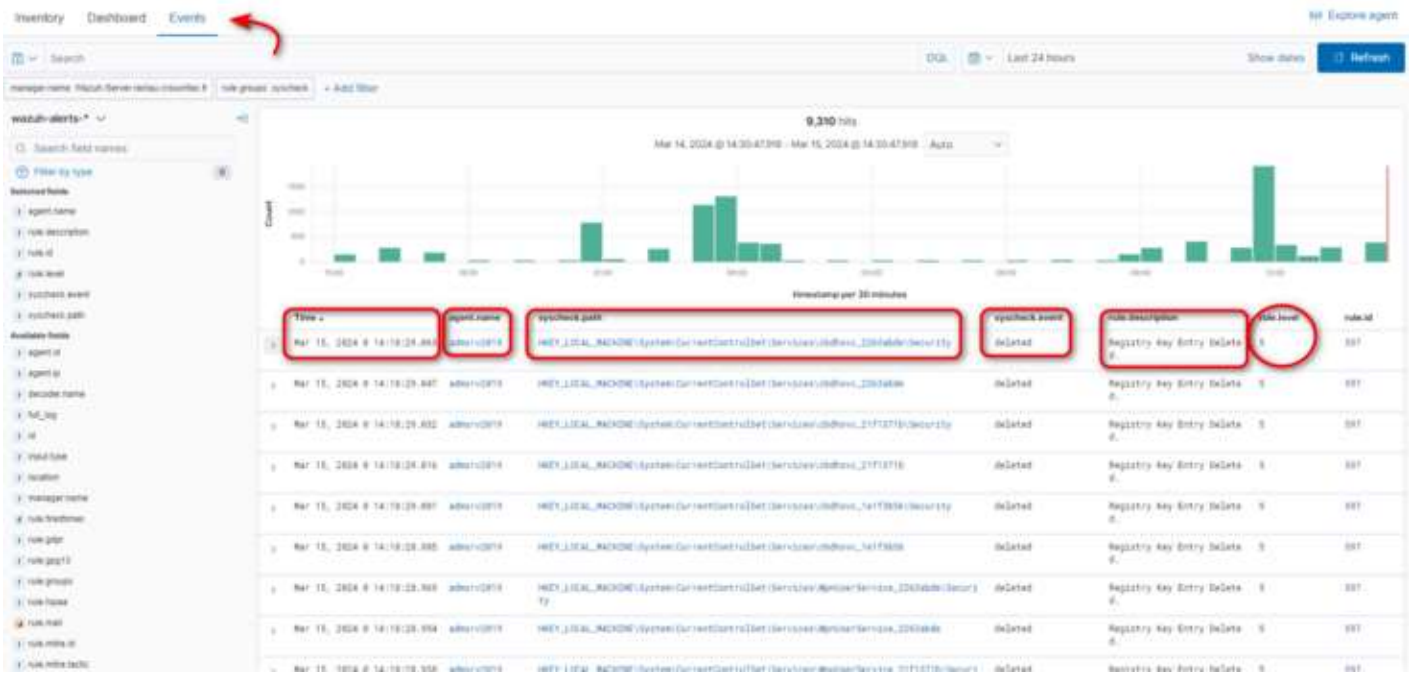
Le module de monitoring de l'intégrité des serveurs est accessible par la page d'accueil :

Ce module permet d'analyser l'intégrité des fichiers et des clés de registre sur les serveurs. La page d'accueil de ce module contient des statistiques sur ces informations sous forme de graphiques comme l'évolution des 3 types d'alerte possible (Suppression, modification, ajout) en fonction du temps.



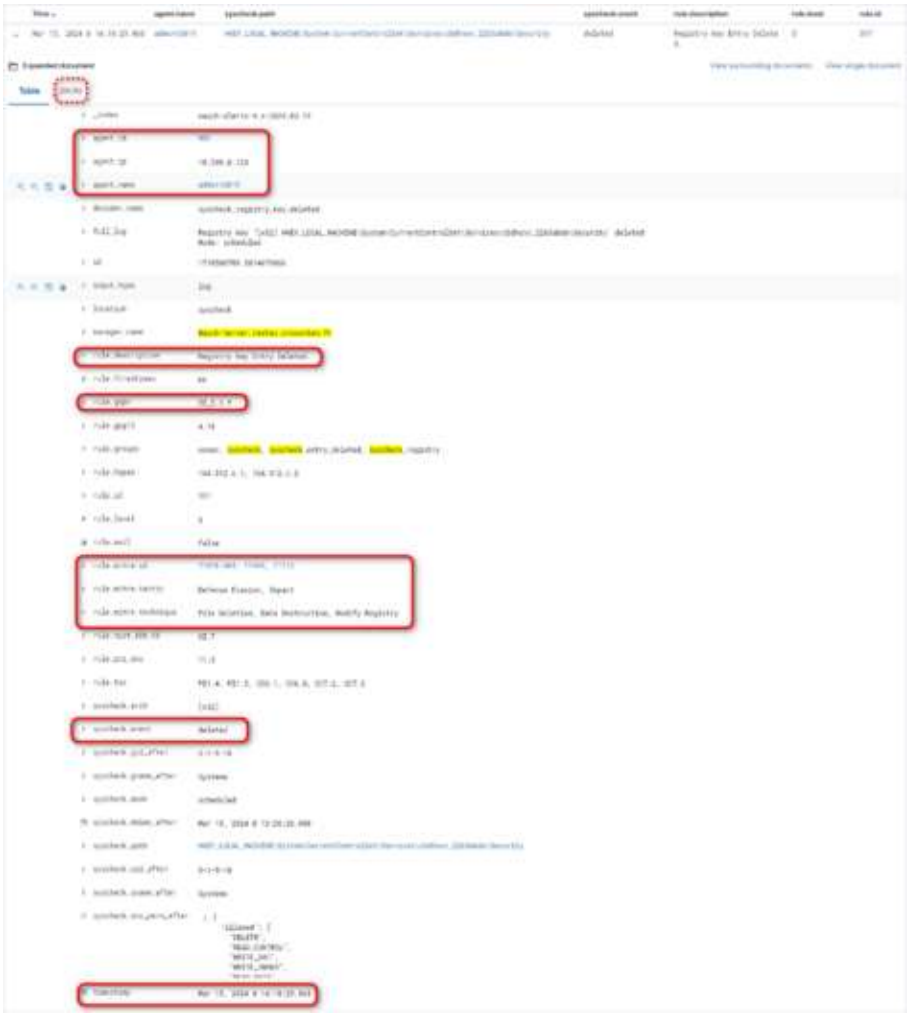
En se rendant dans l'onglet "Évènements" de ce module, on a accès à la liste de tous les évènements apparus sur l'infrastructure.

Ils sont triés par date, et filtré par défaut par agent, par type d'évènement, par description et par niveaux d'alerte :



En cliquant sur un évènement particulier, on accède à des informations plus précises sur celui-ci, notamment les informations de l'agent concerné, sa description détaillée , sa compliance RGPD (et toutes les autres normes), sa correspondance avec le registre MITRE et le timestamp précis.

Il est toujours possible d'exporter ces informations sous format JSON si besoin.



Ce module est essentiel pour couvrir les attaques du type DOS, Brute Force, Cheval de Troie etc.. puisqu'il permet de voir en temps réel les changements apportés à une machine

Politiques de sécurité et audit système

Monitoring des politiques

Audit système

Security configuration assessment

Détection de vulnérabilités et MITRE

Analyses des vulnérabilités

Registre MITRE

Compliance aux normes

RGPD (GDPR)

PCI DSS

NIST 800-53

TSC

HIPAA

La dernière modification de cette page a été faite le 15 mars 2024 à 15:07.