

Wazuh - Utilisation

Sommaire

Introduction

Accès à l'interface

Présentation de l'interface

Tableau de bord

Vue des agents

Présentation des modules

Management des événements de sécurité

Évènements de sécurité

Monitoring de l'intégrité des machines

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

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 événements 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 événements de l'infrastructure.

Accès à l'interface

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

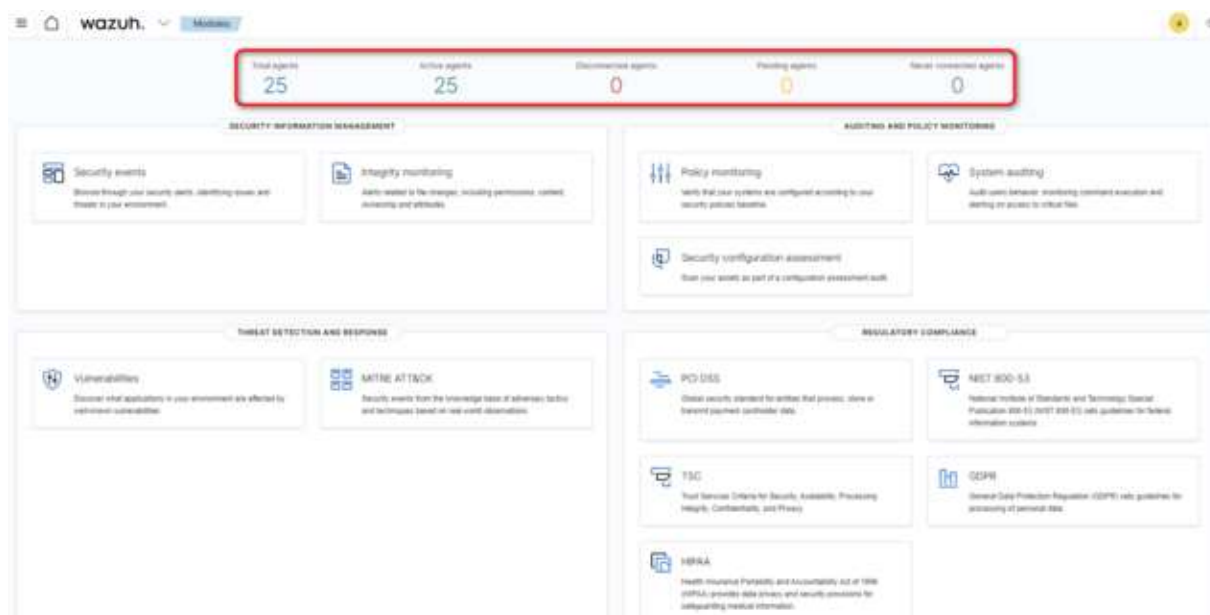


Les identifiants administrateurs pour la connexion sont dans le KeePass Admin.

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 événements 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 :

The screenshot shows the Wazuh web interface. The top navigation bar has a 'wazuh.' logo and a 'Modules' dropdown menu. The 'Agents' option is highlighted in the dropdown. The main content area displays a 'Modules directory' with various security modules. Below this, the 'Agents' page is shown, including a status overview and a table of agents.

ID	Name	IP address	OS	OS version	Agent version	Registration date	Last keep-alive	Status
001	win10-01	10.249.0.133	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
002	win10-02	10.249.0.134	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
003	win10-03	10.249.0.135	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
004	win10-04	10.249.0.136	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
005	win10-05	10.249.0.137	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
006	win10-06	10.249.0.138	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
007	win10-07	10.249.0.139	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
008	win10-08	10.249.0.140	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
009	win10-09	10.249.0.141	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
010	win10-10	10.249.0.142	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
011	win10-11	10.249.0.143	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
012	win10-12	10.249.0.144	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
013	win10-13	10.249.0.145	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
014	win10-14	10.249.0.146	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
015	win10-15	10.249.0.147	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
016	win10-16	10.249.0.148	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
017	win10-17	10.249.0.149	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
018	win10-18	10.249.0.150	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
019	win10-19	10.249.0.151	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
020	win10-20	10.249.0.152	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
021	win10-21	10.249.0.153	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
022	win10-22	10.249.0.154	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
023	win10-23	10.249.0.155	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
024	win10-24	10.249.0.156	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active
025	win10-25	10.249.0.157	Microsoft Windows Server 2016 Datacenter	10.0.17134.486	v4.7.2	Feb 1, 2024 @ 13:51:00:00	Mar 12, 2024 @ 16:00:00:00	active

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.

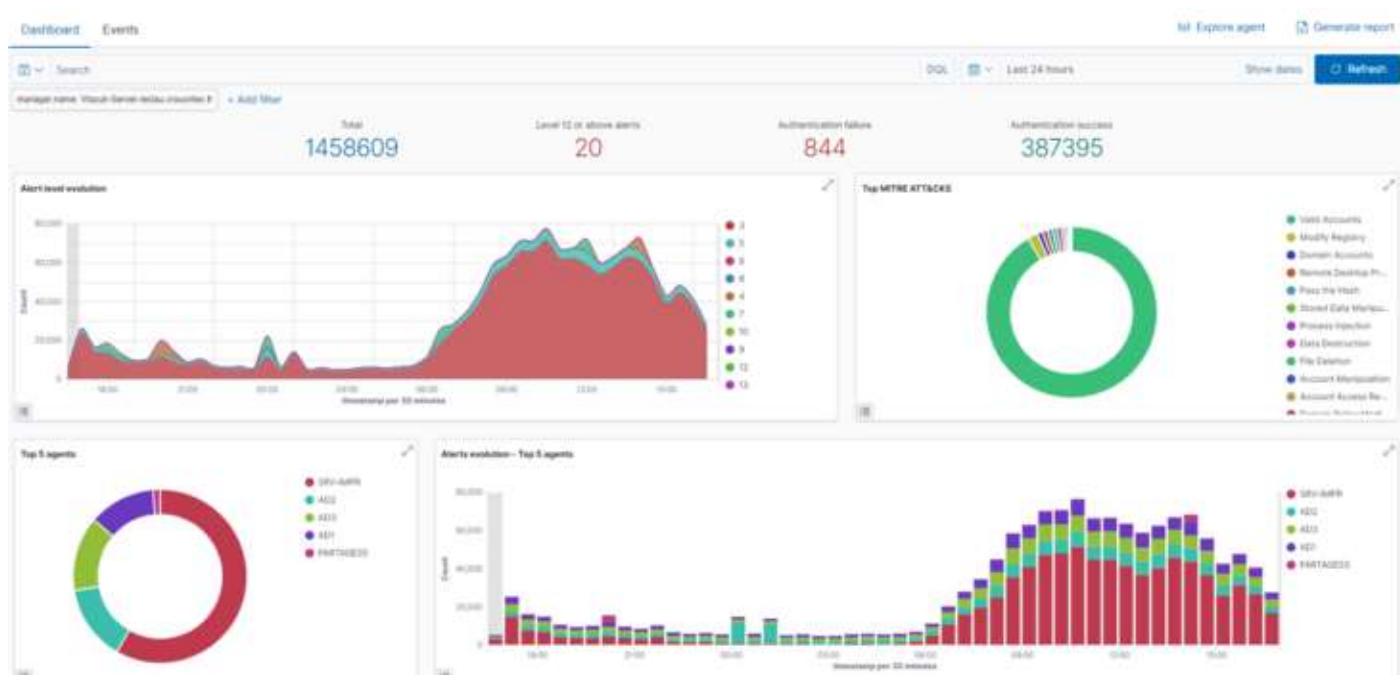
Par défaut, les agents sont triés par ID dans l'ordre croissant. Il est possible de trier par d'autres critères si besoin.

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

Présentation des modules

Management des événements de sécurité

Événements de sécurité



Cette page est un tableau de bord regroupant tous les événements 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'événements, le deuxième représente la part de chaque type de méthode MITRE dans l'ensemble des événements 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 événement particulier survenu très fréquemment.

Security Alerts								
	Time (s)	Agent	Agent name	Techniques	Tactics	Description	Level	Rule ID
1	Mar 13, 2024 @ 18:57:43.358	008	SIR-sdr6			Windows User Logoff	3	60137
2	Mar 13, 2024 @ 18:57:43.294	008	SIR-sdr6	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success	3	60106
3	Mar 13, 2024 @ 18:57:43.216	008	SIR-sdr6			Windows User Logoff	3	60137
4	Mar 13, 2024 @ 18:57:43.262	008	SIR-sdr6	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success	3	60106
5	Mar 13, 2024 @ 18:57:43.233	008	SIR-sdr6			Windows User Logoff	3	60137
6	Mar 13, 2024 @ 18:57:43.215	008	SIR-sdr6	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success	3	60106
7	Mar 13, 2024 @ 18:57:43.184	008	SIR-sdr6			Windows User Logoff	3	60137
8	Mar 13, 2024 @ 18:57:43.171	008	AG3			Windows User Logoff	3	60137
9	Mar 13, 2024 @ 18:57:43.171	008	SIR-sdr6	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success	3	60106
10	Mar 13, 2024 @ 18:57:43.158	008	SIR-sdr6			Windows User Logoff	3	60137
Rows per page: 10 ▾								
◀ 1 2 3 4 5 ... 1000								

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.

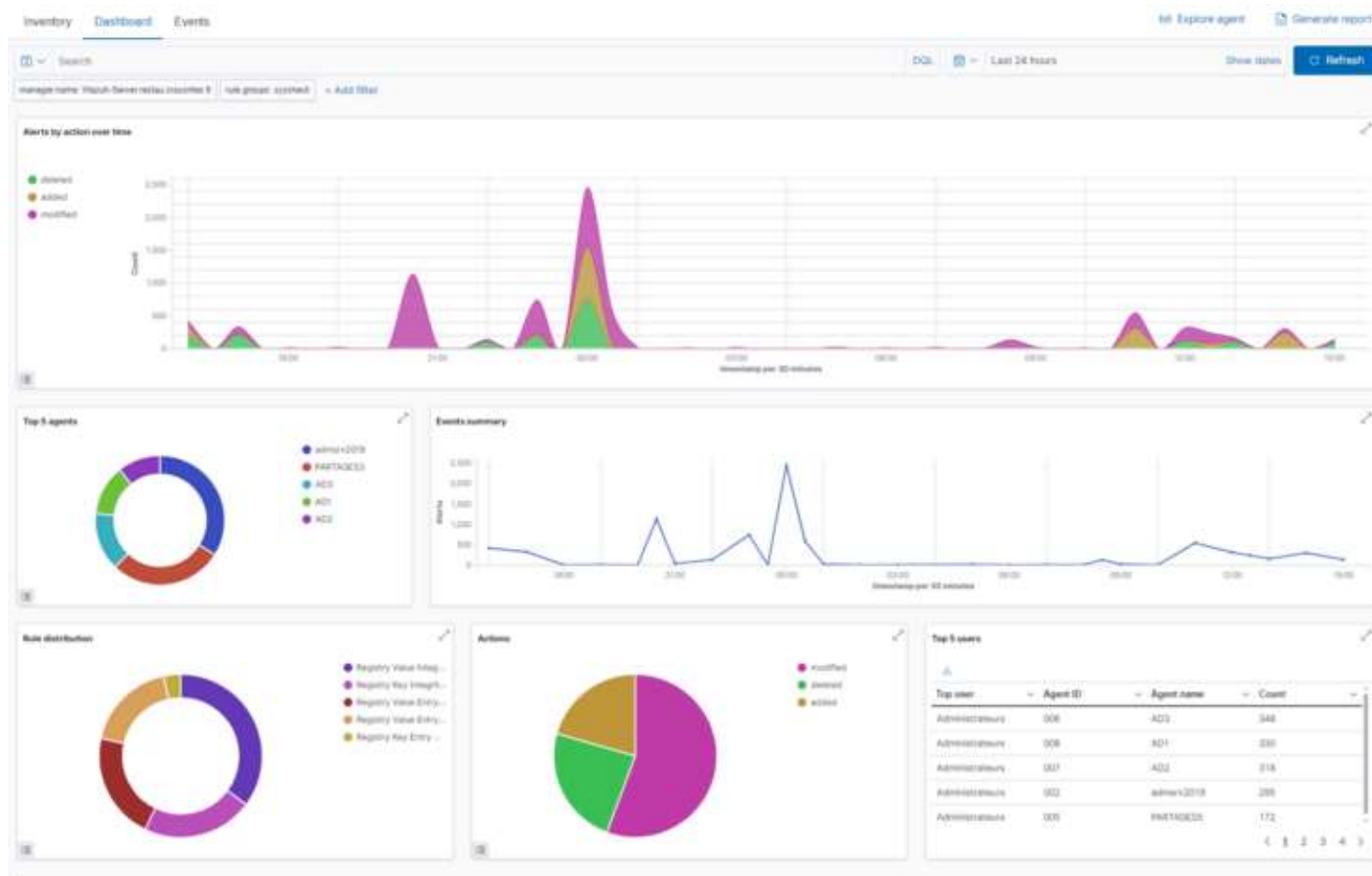
	Mar 14, 2024 @ 08:52:57.072	009	SPI-BSPN	T1078	Defense Evasion: Persistence, Privilege Escalation, Hijack Autosys	Windows login success.	3	6C1D6
Index	JSON	Rule						
	"timestamp": "2024-03-14T08:52:57.072Z"							
	"id": "TongH4B7P5hUzJnCWk9Q"							
	"agent.id": "329"							
	"agent.ip": "10.249.0.125"							
	"agent.name": "SPI-BSPN"							
	"data.win.eventdata.authenticationPackageId": "NTLM"							
	"data.win.eventdata.authenticationToken": "5/5:1843"							
	"data.win.eventdata.authenticationType": "5/5:1803"							
	"data.win.eventdata.keyLength": "128"							
	"data.win.eventdata.packageName": "NTLM V2"							
	"data.win.eventdata.loginGUID": "00000000-0000-0000-0000-000000000000"							
	"data.win.eventdata.loginProcessName": "lsass.exe"							
	"data.win.eventdata.loginType": "3"							
	"data.win.eventdata.processId": "(nil)"							
	"data.win.eventdata.subjectLogonId": "(nil)"							
	"data.win.eventdata.subjectUserSid": "S-1-5-0"							
	"data.win.eventdata.targetDomainName": "REDTEAM"							
	"data.win.eventdata.targetNameLogonId": "0x0"							
	"data.win.eventdata.targetLogonId": "0x7f1aa5442"							
	"data.win.eventdata.targetUserName": "gplmrmc"							
	"data.win.eventdata.targetUserSid": "S-1-5-21-484767889-143682113-838512119-35530"							

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 :

Inventory **Dashboard** **Events** Explore agent

Search DDL Last 24 hours Show details Refresh

manage name: Patch Server (data-source: f) rule group: syncheck + Add filter

wazuh-alerts* 9,310 hits

Search field names Filter by type

Selected fields

- agent name
- rule description
- rule id
- rule level
- timestamp
- timestamp path

Available fields

- agent id
- agent ip
- decoder name
- file_path
- file
- file size
- location
- manager name
- rule filename
- rule gid
- rule priority
- rule group
- rule name
- rule meta id
- rule meta name

Timestamp per 30 minutes

Time	agent name	syncheck path	syncheck event	rule description	rule level	rule id
Mar 15, 2024 @ 14:30:00-01	adorn-0019	WGET_1_LOCAL_MACHINE\SystemCurrentControlSet\Services\WinRM\SSDI\bin\Securty	deleted	Registry key Entry Delete	5	001
Mar 15, 2024 @ 14:30:00-02	adorn-0019	WGET_1_LOCAL_MACHINE\SystemCurrentControlSet\Services\WinRM\SSDI\bin\Securty	deleted	Registry key Entry Delete	5	001
Mar 15, 2024 @ 14:30:00-03	adorn-0019	WGET_1_LOCAL_MACHINE\SystemCurrentControlSet\Services\WinRM\SSDI\bin\Securty	deleted	Registry key Entry Delete	5	001
Mar 15, 2024 @ 14:30:00-04	adorn-0019	WGET_1_LOCAL_MACHINE\SystemCurrentControlSet\Services\WinRM\SSDI\bin\Securty	deleted	Registry key Entry Delete	5	001
Mar 15, 2024 @ 14:30:00-05	adorn-0019	WGET_1_LOCAL_MACHINE\SystemCurrentControlSet\Services\WinRM\SSDI\bin\Securty	deleted	Registry key Entry Delete	5	001
Mar 15, 2024 @ 14:30:00-06	adorn-0019	WGET_1_LOCAL_MACHINE\SystemCurrentControlSet\Services\WinRM\SSDI\bin\Securty	deleted	Registry key Entry Delete	5	001
Mar 15, 2024 @ 14:30:00-07	adorn-0019	WGET_1_LOCAL_MACHINE\SystemCurrentControlSet\Services\WinRM\SSDI\bin\Securty	deleted	Registry key Entry Delete	5	001
Mar 15, 2024 @ 14:30:00-08	adorn-0019	WGET_1_LOCAL_MACHINE\SystemCurrentControlSet\Services\WinRM\SSDI\bin\Securty	deleted	Registry key Entry Delete	5	001
Mar 15, 2024 @ 14:30:00-09	adorn-0019	WGET_1_LOCAL_MACHINE\SystemCurrentControlSet\Services\WinRM\SSDI\bin\Securty	deleted	Registry key Entry Delete	5	001
Mar 15, 2024 @ 14:30:00-10	adorn-0019	WGET_1_LOCAL_MACHINE\SystemCurrentControlSet\Services\WinRM\SSDI\bin\Securty	deleted	Registry key Entry Delete	5	001

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.

[illegible]

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

Récupérée de « https://wiki.crous-nantes.fr/index.php?title=Wazuh_-_Utilisation&oldid=45978 »

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