

02/04/2025

Wazuh Le super-héros de la sécurité



UNIVERSITÉ
TOULOUSE III
PAUL SABATIER

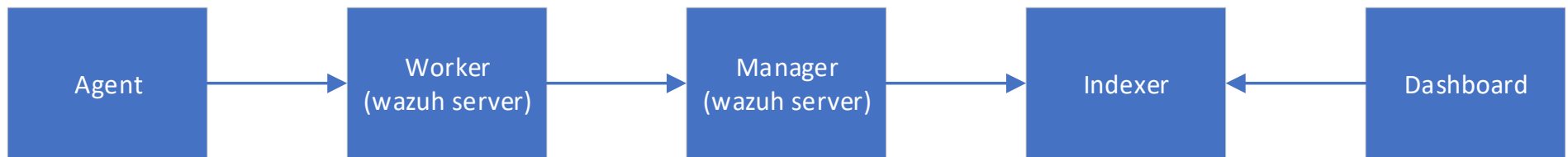


“



Qu'est ce que Wazuh ?

- Un SIEM et un XDR – Opensources (GPL et Apache Licence v2)
 - **Détection** d'incidents et **réponses**



- Worker : traitement initial, filtres, agrégation de données.
- Manager : Cohérence du cluster, groupes, agents, règles, décodeurs, CDB
- Indexer : Fork Opensearch
- Dashboard : Fork Opensearch Dashboard

Qu'est ce que Wazuh ?

- Dépends du nombre d'alertes

La théorie	Indexer	Manager/worker
RAM	16GB	4GB
CPU	8	8
Espace disque 90j		
1 server : 0,25 APS*	3,7	0,1
1 poste de travail : 0,1 APS*	1,5	0,04
1 équipement réseau : 0,5 APS*	7,4	0,2

*APS = Alerte par seconde

Qu'est ce que Wazuh ?

- Machine physique
 - Bi-Xeon E5-2650L v3
 - 2 sockets à 12 cœurs multi-threadés soit 48 processeurs
 - 256Go de RAM
 - Disques mécaniques
 - 370 serveurs + 60 postes

=> 3 indexers (10Go RAM) / 1 manager / 1 worker /1 dashboard
- Données réelles
 - 4,6Go / Serveurs / mois avec Conservation cible : 12 mois
 - Cpu 10% en moyenne, pointes à 20%
 - 48 Go Ram utilisés

Qu'est ce que Wazuh ?

- Un agent installé avec plusieurs modules
 - Collectent l'information
 - Collecteur de logs
 - Collecteur de résultats de commandes
 - Contrôle d'intégrité de fichiers
 - Security Configuration Assessment (Evaluation des configurations)
 - Malware détection
 - Inventaire (applications, processus)
 - Surveillance de conteneur docker
 - Surveillance d'infrastructure Cloud.

Linux
MacOS
Windows

Non testé

“

Installation



alamy

Image ID: A75NHJ
www.alamy.com

Installation

- Docker
 - Docker-compose fourni pour chaque élément
- Ansible
 - Pour docker
 - Pour serveurs
- Installation d'un Agent
 - Dépend de plusieurs modules (audit, rsyslog, etc.)
 - Difficultés automatisation de la configuration : pas XML Standard

Installation

- Authentication
 - Active Directory (en LDAP)
 - MS Entra ID, Google, etc (non testé)
 - Comptes locaux
- Gestion des agents
 - Peuvent appartenir à plusieurs groupes
 - Fichier de configuration en central
- Gestion par tenant
 - Filtrage basé sur le Document Security Level d'OpenSearch
 - RBAC

“

Principe de fonctionnement



Administration

W.

Threat Hunting

Recently viewed

Home

Explore

Endpoint security

Threat intelligence

Security operations

Cloud security

Agents management

Server management

Rules

Decoders

CDB Lists

Status

Cluster

DQL

▼

Last 24 hours

Show dates

Refresh

timestamp per 30 minutes

EDR/XDR - Wazuh

34,615,095 hits ⓘ

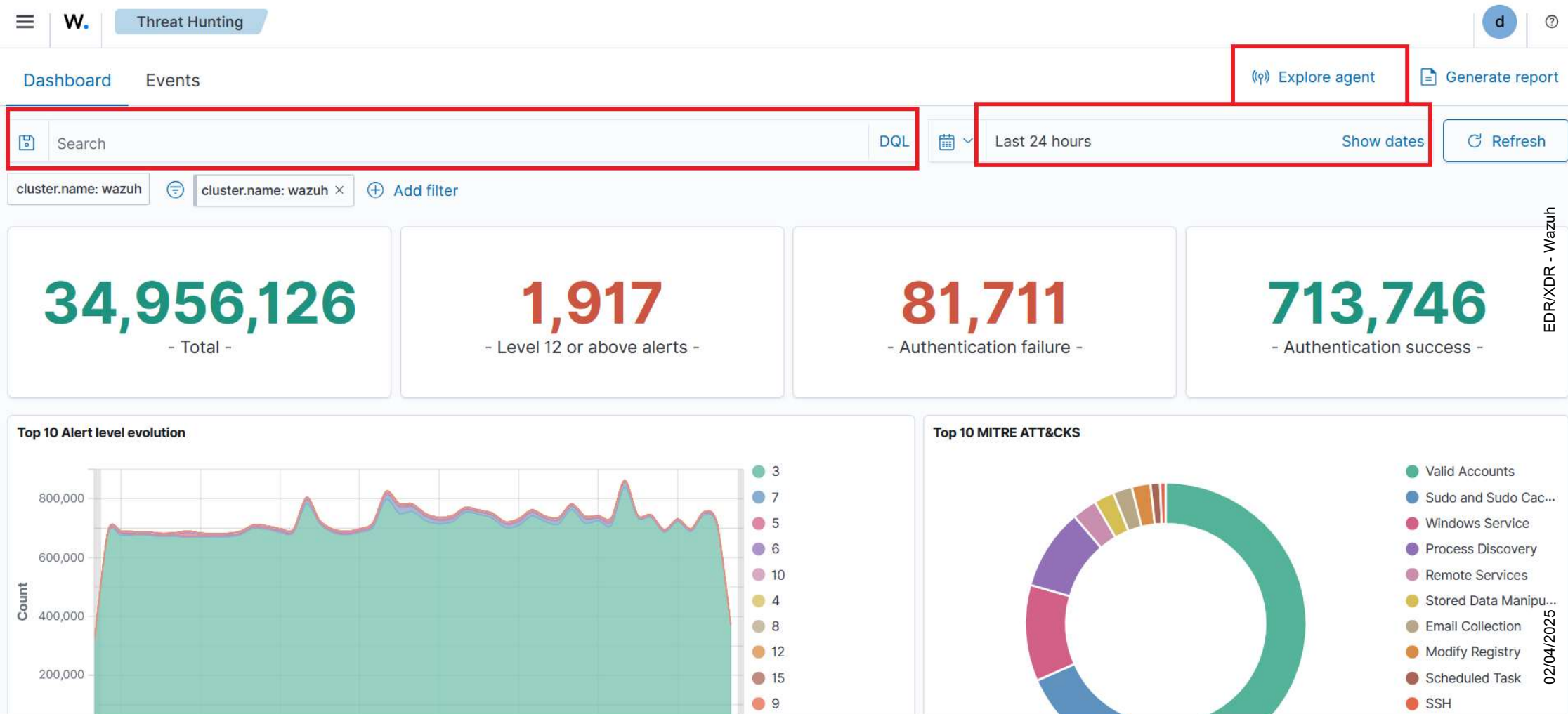
Mar 13, 2025 @ 17:23:36.357 - Mar 14, 2025 @ 17:23:36.357

Columns Density 1 fields sorted Full screen

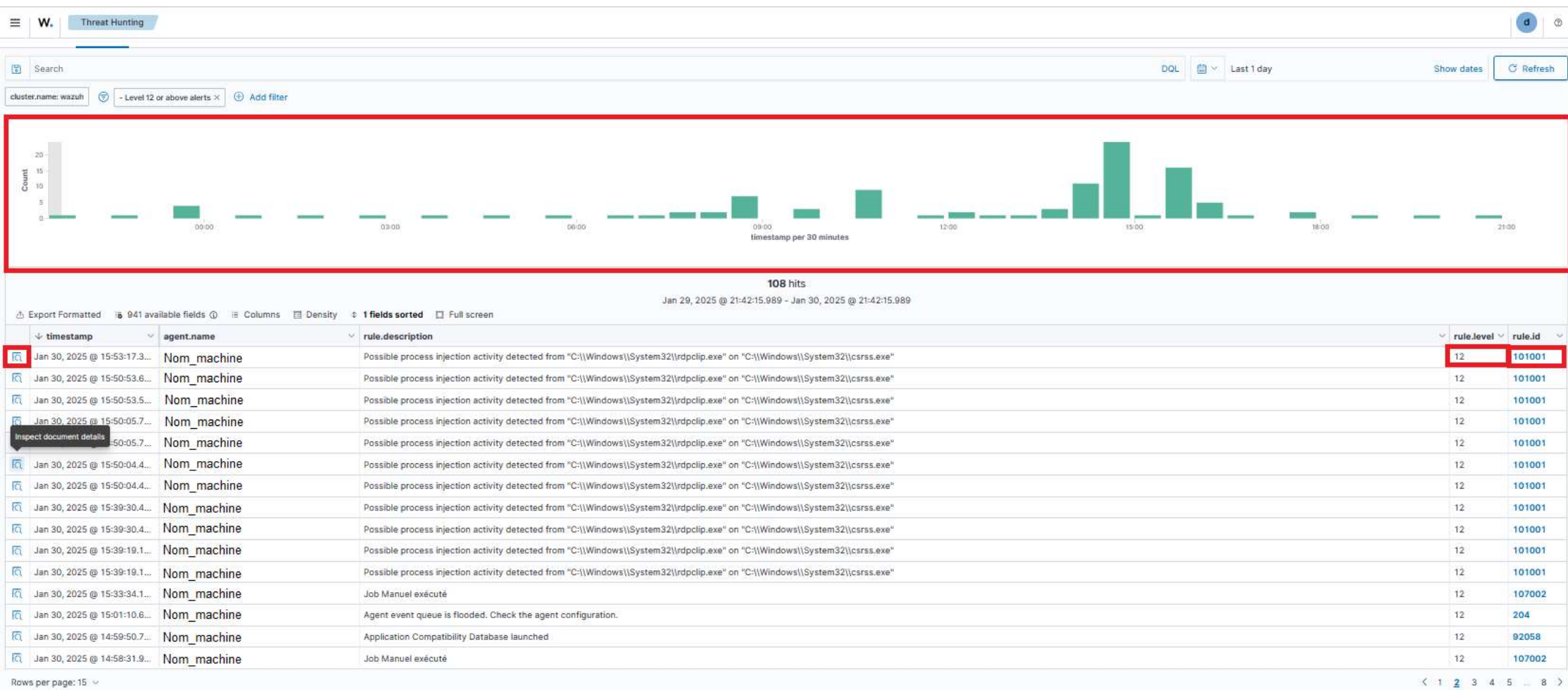
rule.description	rule.level	rule.id
Audit: Command: /usr/bin/grep.	3	80792
Audit: Command: /usr/bin/bash.	3	80792
Audit: Command: /usr/bin/date.	3	80792
Audit: Command: /usr/bin/stat.	3	80792

02/04/2025

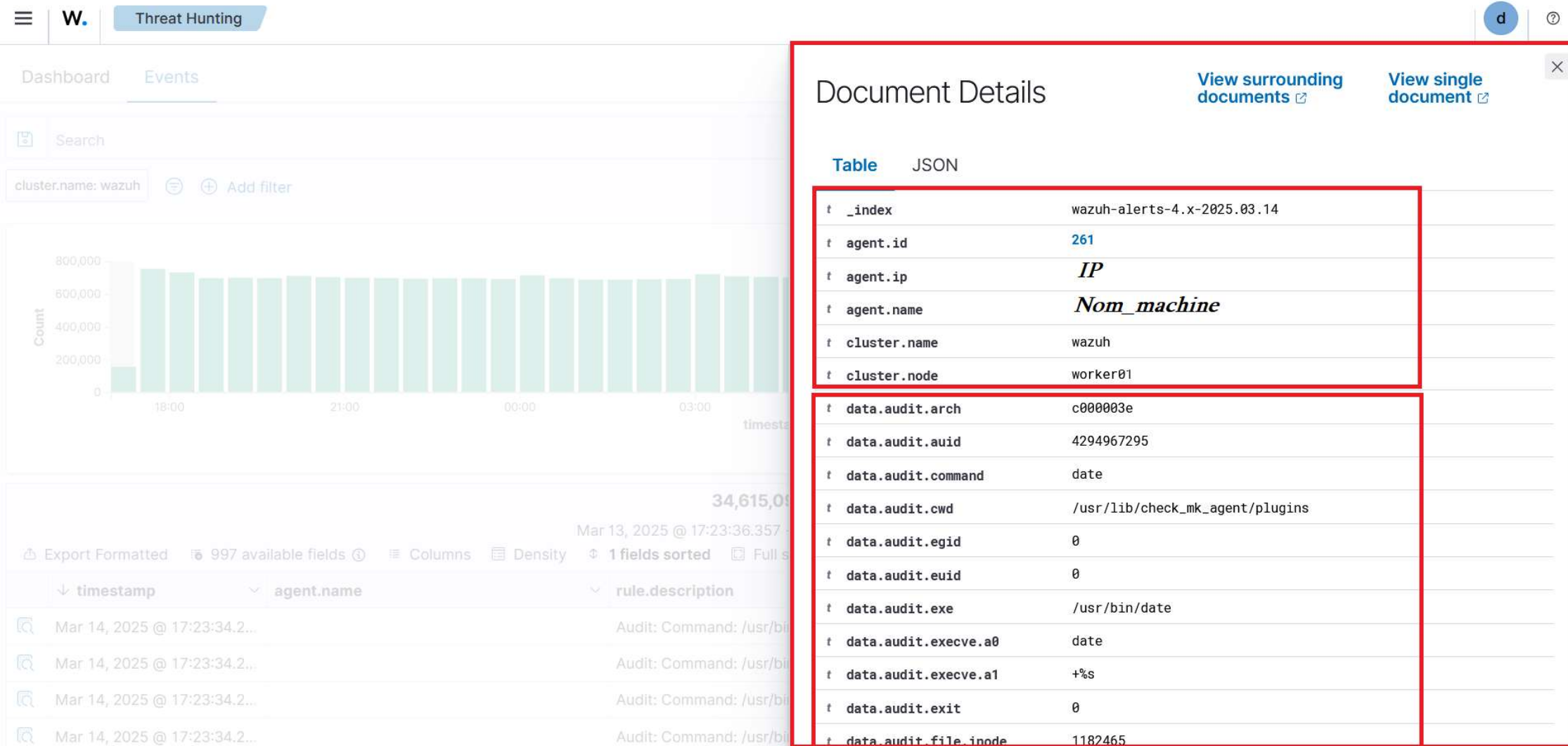
Evènements de sécurité



Evènements de sécurité



Evènements de sécurité



Security events

- Tous les évènements de sécurité de tous les modules
 - Définition d'un niveau.
 - 1 à 15 : niveau de risque
 - 0 : Ne pas stocker l'alerte
 - Envoi de mails
 - Par niveau
 - Par id

Analyse de logs

- Analyse de logs personnalisable
 - Un pré-décodeur
 - Détecte le format de logs
 - Un décodeur
 - Découpe les logs pour créer les champs
 - Des règles
 - Génère des alertes en fonction des champs

Analyse de logs

- Exemple de Décodeur

```
<decoder name="zimbra">  
  <prematch>ua=Zimbra</prematch>  
</decoder>
```

```
<decoder name="zimbra">  
  <parent>zimbra</parent>  
  <regex>^(\d+.\d+.\d+.\d+)\(\.+.cmd=(\.+);\.+.account=(\.+);\.+.protocol=(\.+);\.+.error=(\.+);</regex>  
  <order>monip,action,account,protocol,error</order>  
</decoder>
```

Pour info

192.168.2.45(nginx/1.24.0);ua=Zimbra/9.0.0_ZEXTRAS_9039;cid=21256;] security - cmd=Auth; account=cedric.chambault@univ-tlse3.fr;
protocol=imap; error=authentication failed for [cedric.chambault@univ-tlse3.fr], missing userPassword;

Analyse de logs

- Exemple de règles

```
<group name="zimbra">
  <rule id="100002" level="7">
    <decoded_as>zimbra</decoded_as>
    <field name="account">cedric.chambault@univ-tlse3.fr</field>
    <description>Connexion administrateur</description>
  </rule>
</group>

<group name="zimbra_audit,">
  <rule id="100003" level="12">
    <if_sid>100002</if_sid>
    <decoded_as>zimbra</decoded_as>
    <match>authentication failed</match>
    <description>Echec non autorisé pour un administrateur</description>
  </rule>
</group>
```

Analyse de logs

- Analyse de logs par défaut
 - **Auditd**
 - Auth.log
 - Syslog
- Possibilité d'ajouter les logs dont le format est connu
 - **Sysmon**

Security events

- Outils d'aide à la personnalisation
 - /var/ossec/bin/wazuh-logtest

```
192.168.2.45(nginx/1.24.0);ua=Zimbra/9.0.0_ZEXTRAS_9039;cid=21256;] security - cmd=Auth; account=cedric.chambault@univ-tlse3.fr; protocol=imap; error=authentication failed for [cedric.chambault@univ-tlse3.fr], missing userPassword;

**Phase 1: Completed pre-decoding.
full event: '192.168.2.45(nginx/1.24.0);ua=Zimbra/9.0.0_ZEXTRAS_9039;cid=21256;] security - cmd=Auth; account=cedric.chambault@univ-tlse3.fr; protocol=imap; error=authentication failed for [cedric.chambault@univ-tlse3.fr], missing userPassword;'

**Phase 2: Completed decoding.
name: 'zimbra'
account: 'cedric.chambault@univ-tlse3.fr'
action: 'Auth'
error: 'authentication failed for [cedric.chambault@univ-tlse3.fr], missing userPassword'
monip: '192.168.2.45'
protocol: 'imap'

**Phase 3: Completed filtering (rules).
id: '100003'
level: '12'
description: 'Echec non autorisé pour un administrateur'
groups: '['zimbra_audit']'
firedtimes: '1'
mail: 'True'

**Alert to be generated.
```

“

Malware Detection



Malware Detection

- Analyse Rootcheck
 - Processus cachés
 - Droits inhabituels (suid, write pour other mais owner root, etc.)
 - Ports cachés
 - Scan /dev
- Bases de données de rootkit et trojans
 - CDB Lists
 - Yara
 - ClamAV / Defender

Malware Detection

cluster.node	worker01
data.file	/dev/nul
data.title	File present on /dev.
decoder.name	rootcheck
full_log	File '/dev/nul' present on /dev. Possible hidden file.
id	1743219037.5075230536
input.type	log
location	rootcheck
manager.name	wazuh.worker
rule.description	Host-based anomaly detection event (rootcheck).

data.title	NTFS Alternate data stream found: 'C:\Program Files\LAPS:Win32App_1'.
decoder.name	rootcheck
full_log	NTFS Alternate data stream found: 'C:\Program Files\LAPS:Win32App_1'. Possible hidden content.
id	1743205819.2491494943

Malware Detection

 S'appuie beaucoup sur des outils tiers

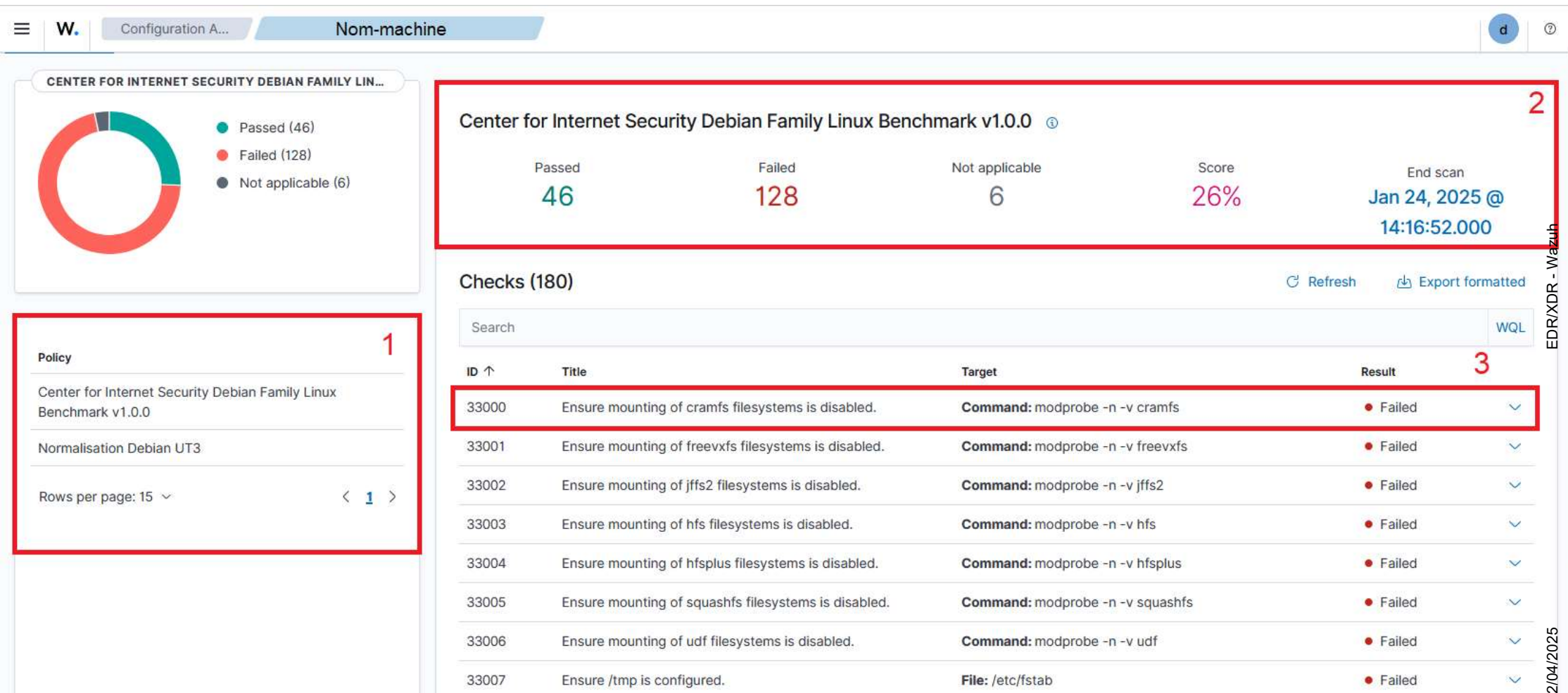
“



Evaluation des
configurations



Exemple de conformité



Détail d'une règle de conformité

W.

Configuration A...

Nom-machine

Center for Internet Security Debian Family Linux Benchmark v1.0.0

Normalisation Debian UT3

Rows per page: 15

ID ↑	Title	Target	Result
33000	Ensure mounting of cramfs filesystems is disabled.	Command: modprobe -n -v cramfs	Failed
Rationale Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it. Remediation Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/cramfs.conf and add the following line: install cramfs /bin/true Run the following command to unload the cramfs module: # rmmod cramfs. Description The cramfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A cramfs image can be used without having to first decompress the image. Checks (Condition: all) - c:modprobe -n -v cramfs → r:install /bin/true - not c:lsmod → r:cramfs Compliance cis: 1.1.1.1 cis_csc_v7: 5.1 cmmc_v2.0: AC.1.002,CM.2.061,SC.3.180 iso_27001-2013: A.8.1.3,A.14.2.5 mitre_techniques: T1110,T1003,T1081,T1097,T1178,T1072,T1067,T1495,T1019,T1177,T1485,T1486,T1491,T1488,T1487,T1490,T1146,T1148,T1015,T1133,T1200,T1076,T1051,T1176,T1501,T1087,T1098,T1139,T1197,T1092,T1136,T1011,T1147,T1130,T1174,T1053,T1166,T1206,T1503,T1214,T1187,T1208,T1142,T1075,T1201,T1145,T1184,T1537,T1078,T1077,T1134,T1017,T1088,T1175,T1190,T1210,T1525,T1215,T1086,T1055,T1505,T1035,T1218,T1169,T1100,T1047,T1084,T1028,T1156,T1196,T1530,T1089,T1073,T1157,T1054,T1070,T1037,T1036,T1096,T1034,T1150,T1504,T1494,T1489,T1198,T1165,T1492,T1080,T1209,T1112,T1058,T1173,T1137,T1539,T1535,T1506,T1138,T1044,T1199 nist_sp_800-53: AU-2,CM-1,CM-2,CM-6,CM-7,IA-5,IA-6,SC-20,SC-21 pci_dss_v3.2.1: 2.2			
33001	Ensure mounting of freevxfs filesystems is disabled.	Command: modprobe -n -v freevxfs	Failed
33002	Ensure mounting of jffs2 filesystems is disabled.	Command: modprobe -n -v jffs2	Failed
33003	Ensure mounting of hfs filesystems is disabled.	Command: modprobe -n -v hfs	Failed

Security Configuration Assessment

- Un ensemble de normes prédéfinies
 - CIS Benchmark, RGPD, HIPAA (santé), PCI DSS (Finance), NIST 800-53 et TSC (Cybersécurité)



Mesurer l'écart entre nos pratiques et les bonnes pratiques reconnues.

Security Configuration Assessment

- Personnalisation : définition de nos propres normes
 - Existence de fichiers
 - Droits
 - Hash
 - ...

Peut utiliser n'importe quel shell qui renvoie une valeur interprétable en regex
c:[commande] -> r:^regex\$

Security Configuration Assessment

• Format d'un élément

checks:

START ANSIBLE MANAGED BLOCK FOR UT3 NTP COMPLIANCE

- id: 1

title: "Role de conformité - config_ntp"

description: "Rôle nécessaire à la conformité UT3 et configurant le NTP"

rationale: "Utiliser les NTPs d'Angers garantie la cohérence du temps au sein de l'infrastructure"

remediation: "Utilisation : ansible-playbook mon_roles.yml -i 192.168.1.41, --tags ntp"

compliance:

- ut3: ["Rule:Infra:1"]

condition: all

rules:

- 'f:/etc/ntpsec/ntp.conf'

- 'f:/etc/default/ntpsec'

- c:grep "server ntp.univ-angers.fr" /etc/ntpsec/ntp.conf -> r:^server\s+ntp.univ-angers.fr\$

- c:grep "restrict ntp.univ-angers.fr nomodify notrap noquery" /etc/ntpsec/ntp.conf -> r:^restrict\s+ntp.univ-angers.fr\s+nomodify\s+notrap\s+noquery\$

- c:grep "NTPD_OPTS=\"-4 -g -N\" /etc/default/ntpsec -> r:^NTPD_OPTS=\"-4\s+-g\s+-N\"\$

END ANSIBLE MANAGED BLOCK FOR UT3 NTP COMPLIANCE

Security Configuration Assessment

Wazuh Security configuration assessment

Inventory Events

deploy (009)

Normalisation Debian UT3

Passed 1 Failed 0 Not applicable 0 Score 100%

End scan: Apr 10, 2024 @ 16:09:05.000

Refresh Export formatted

Search

ID	Title	Target	Result
1	Rôle de conformité - config_ntp	File: /etc/ntpsec/ntp.conf,/etc/default/ntpsec	Passed

Rationale
Utiliser les NTPs d'Angers garantie la cohérence du temps au sein de l'infrastructure

Remediation
Utilisation : ansible-playbook pb_single_roles.yml -i 192.168.1.41, --tags ntp

Description
Rôle nécessaire à la conformité UT3 et configurant le NTP

Checks (Condition: all)

- c:grep "NTPD_OPTS=~4 -g -N" /etc/default/ntpsec → r:"NTPD_OPTS=~4s+-g/s+-N"\$
- c:grep "restrict ntp.univ-angers.fr nomodify notrap noquery" /etc/ntpsec/ntp.conf → r:"restrict/s+ntp.univ-angers.fr/s+nomodify/s+notrap/s+noquery\$"
- c:grep "server ntp.univ-angers.fr" /etc/ntpsec/ntp.conf → r:"server/s+ntp.univ-angers.fr\$"
- f:/etc/default/ntpsec
- f:/etc/ntpsec/ntp.conf

Compliance
ut3: Rule:Infra:1

Rows per page: 10

Wazuh - Wazuh

02/04/2025

Security Configuration Assessment

- Intérêt

 S'assurer que la configuration est déployée et conforme

- Personne n'a modifié les configurations clefs

 Conserver de la souplesse

- Personnalisation d'un serveur

 Aperçu de la maitrise du parc

- Postes
- Serveurs

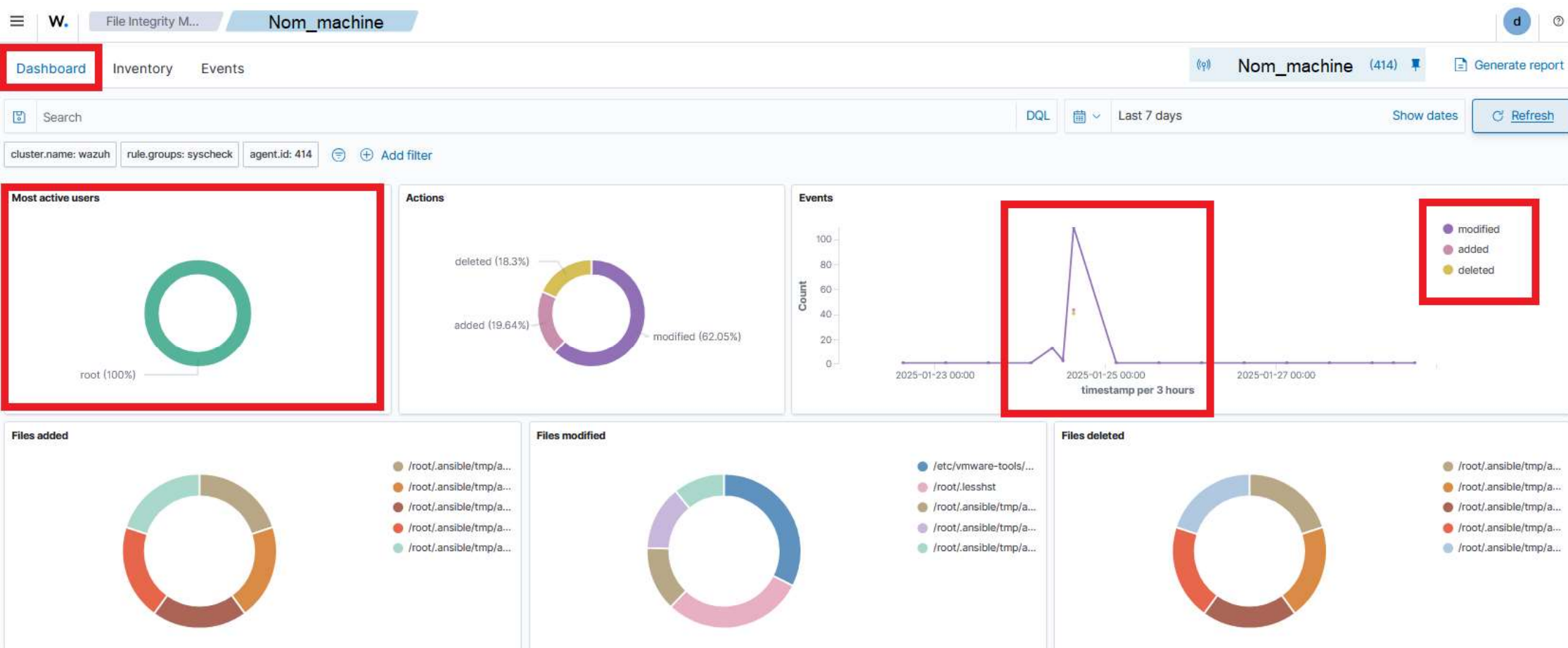
“



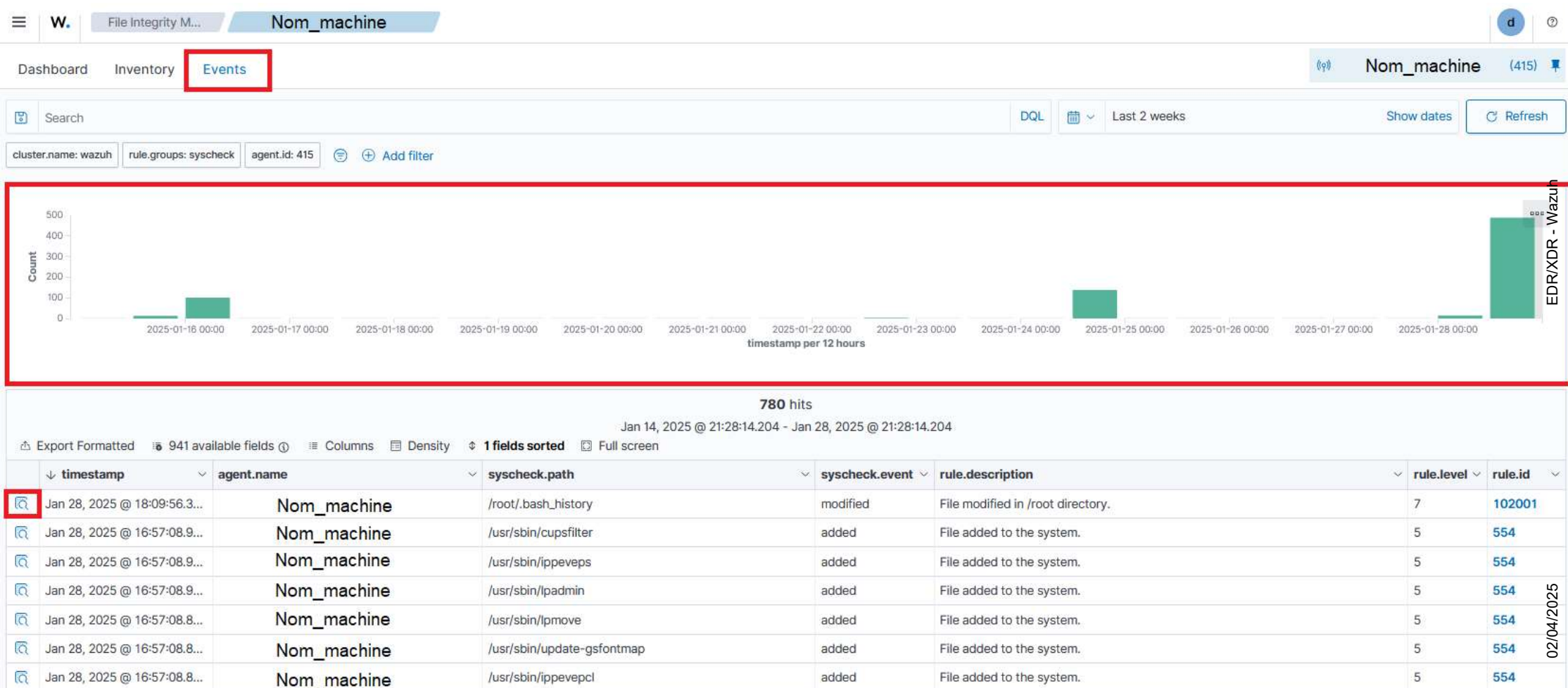
Intégrité des fichiers



Files Integrity Monitoring : Dashboard



Files Integrity Monitoring : events



Files Integrity Monitoring : inventaire des fichiers

W.	File Integrity M...	Nom_machine	d	?
Dashboard	Inventory	Events	Nom_machine (414)	

Files (3,179)							Refresh	Export formatted	
Search									WQL
File ↑	Last modified ▲	User	User ID	Group	Group ID	Size			
/bin	Aug 18, 2023 @ 16:04:20.000	root	0	root	0	7			
/boot/System.map-6.1.0-27-amd64	Nov 1, 2024 @ 05:23:37.000	root	0	root	0	83			
/boot/System.map-6.1.0-28-amd64	Nov 22, 2024 @ 23:27:23.000	root	0	root	0	83			
/boot/config-6.1.0-27-amd64	Nov 1, 2024 @ 05:23:37.000	root	0	root	0	259624			
/boot/config-6.1.0-28-amd64	Nov 22, 2024 @ 23:27:23.000	root	0	root	0	259624			
/boot/grub/fonts/unicode.pf2	Oct 9, 2023 @ 04:33:38.000	root	0	root	0	2392304			
/boot/grub/grub.cfg	Jan 8, 2025 @ 07:55:31.000	root	0	root	0	7750			
/boot/grub/grubenv	Aug 18, 2023 @ 16:20:50.000	root	0	root	0	1024			
/boot/grub/i386-pc/915resolution.mod	Oct 9, 2023 @ 04:33:38.000	root	0	root	0	7780			
/boot/grub/i386-pc/acpi.mod	Oct 9, 2023 @ 04:33:38.000	root	0	root	0	10868			
/boot/grub/i386-pc/adler32.mod	Oct 9, 2023 @ 04:33:38.000	root	0	root	0	1228			
/boot/grub/i386-pc/affs.mod	Oct 9, 2023 @ 04:33:38.000	root	0	root	0	5568			
/boot/grub/i386-pc/afs.mod	Oct 9, 2023 @ 04:33:38.000	root	0	root	0	6020			
/boot/grub/i386-pc/afsplitter.mod	Oct 9, 2023 @ 04:33:38.000	root	0	root	0	1516			

Files Integrity Monitoring

- Analyse
 - Propriétaire, groupe et droits
 - Hash (Sha1,md5,sha256)
 - Inode, attributs et date de modification
- Par défaut check toutes les 12h
 - Personnalisable
- Personnalisation des dossiers ou fichiers à contrôler
<directories>/usr/local/scripts</directories>

Files Integrity Monitoring

- Possibilité de définir une analyse temps réel sur un dossier
`<directories whodata="yes" report_changes="yes" >/etc/group</directories>`

- Intérêt



Alerting en temps quasi réel

- Mauvaise communication ou risque réel ?



Reporting de la modification exacte

- Permet d'analyser rapidement



Bon contrôle des fichiers clés

- Rassurant

Files Integrity Monitoring : Alertes

W. Threat Hunting Nom_machine

Dashboard Events

rule.id: 103002

system.name: wazuh agent.id: 415 Add filter

syscheck.diff 21c21
 < sudo:x:27:

 > sudo:x:27:gadmin

1, sha256

Export Formatted 941 available fields Columns Density 1 fields sorted Full screen

timestamp agent.name rule.description

Jan 28, 2025 @ 16:57:04.1... Modification Fichier etc group

Jan 28, 2025 @ 14:20:09.5... Modification Fichier etc group

syscheck.path /etc/group

Jan 28, 2025 @ 09:28:38.1... Modification Fichier etc group

Jan 28, 2025 @ 09:28:35.4... Modification Fichier etc group

Document Details

View surrounding documents View single document

syscheck.audit.process.paren /
 t_cwd

syscheck.audit.process.paren /usr/lib/systemd/systemd
 t_name

syscheck.event modified

syscheck.gid_after 0

syscheck.gname_after root

syscheck.inode_after 133377

syscheck.inode_before 133018

syscheck.md5_after 97127efecb2103e298580e8d4850d0c2

syscheck.md5_before 46a61abfea2fabe997bd7af22d539c49

syscheck.mode whodata

k.mtime_after Jan 28, 2025 @ 14:20:08.000

k.mtime_before Jan 28, 2025 @ 14:19:42.000

syscheck.path /etc/group

syscheck.perm_after rw-r--r--

syscheck.sha1_after ec3ed38cd76042b3b00d14c208006d0fffbdda8e

EDR/XDR - Wazuh

02/04/2025

Security Configuration Assessment

- Points d'attention



Limitation du nombre de fichier à analyser

- Maximum 100 000 fichiers par défaut
- Charge serveur si trop d'analyse temp réel



Double alerting possible

- Si temps réel + check standard du dossier

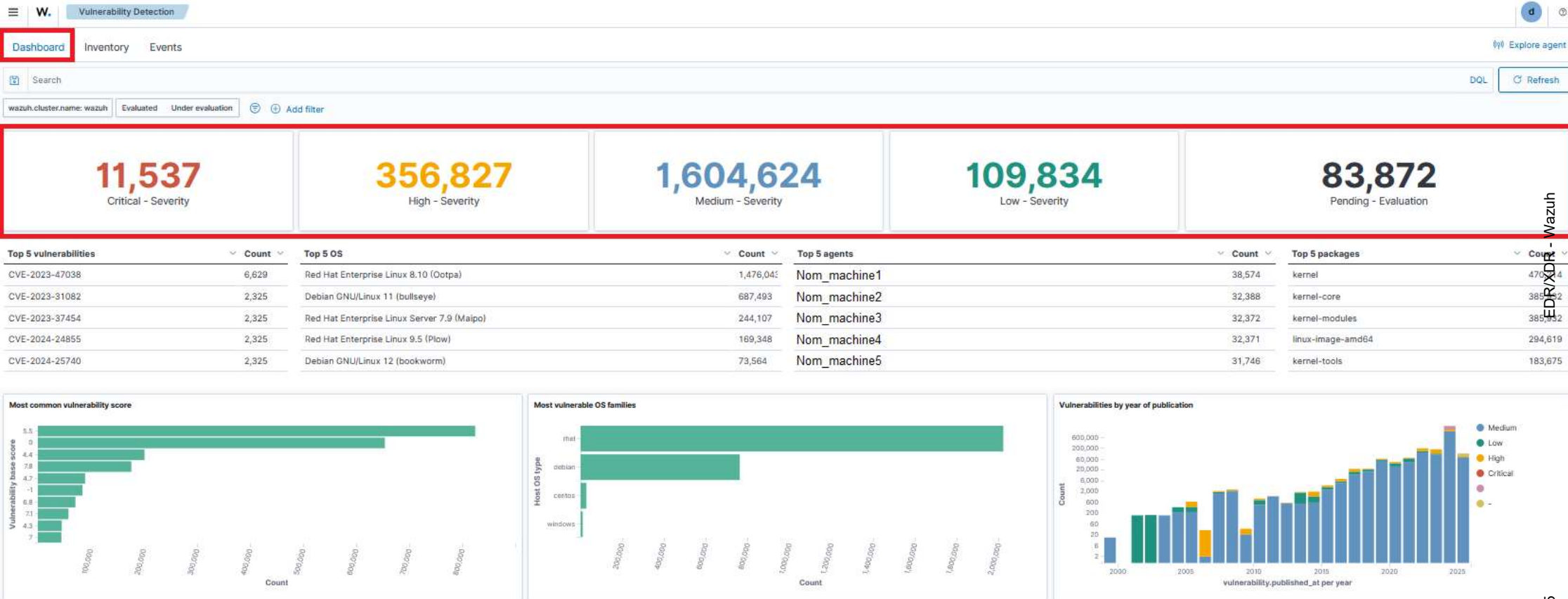
“



Vulnérabilités



Vulnérabilités



Top 5 vulnerabilities

Count

CVE-2023-470386,629

CVE-2023-310822,325

CVE-2023-374542,325

CVE-2024-248552,325

CVE-2024-257402,325

Top 5 OS

Count

Red Hat Enterprise Linux 8.10 (Ootpa)1,476,045

Debian GNU/Linux 11 (bullseye)687,493

Red Hat Enterprise Linux Server 7.9 (Maipo)244,107

Red Hat Enterprise Linux 9.5 (Plow)169,348

Debian GNU/Linux 12 (bookworm)73,564

Top 5 agents

Count

Nom_machine138,574

Nom_machine232,388

Nom_machine332,372

Nom_machine432,371

Nom_machine531,746

Top 5 packages

Count

kernel470,004

kernel-core385,932

kernel-modules385,932

linux-image-amd64294,619

kernel-tools183,675

Most common vulnerability score

Vulnerability base score

Count

Most vulnerable OS families

Host OS type

Count

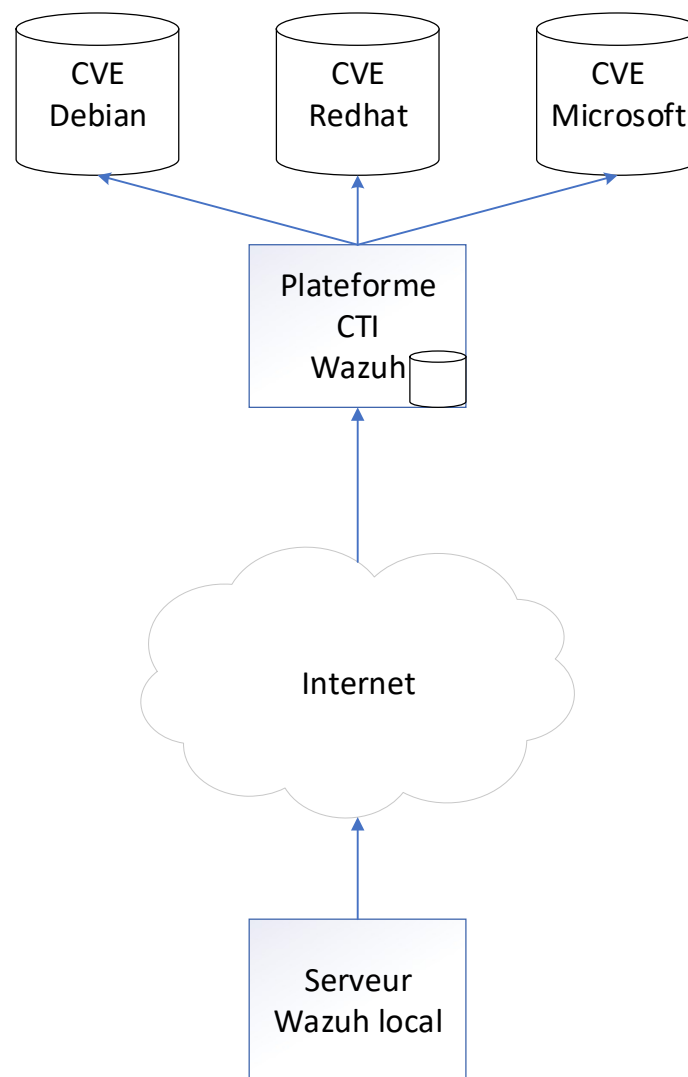
Vulnerabilities by year of publication

Count

vulnerability.published_at per year

02/04/2025

Vulnérabilités

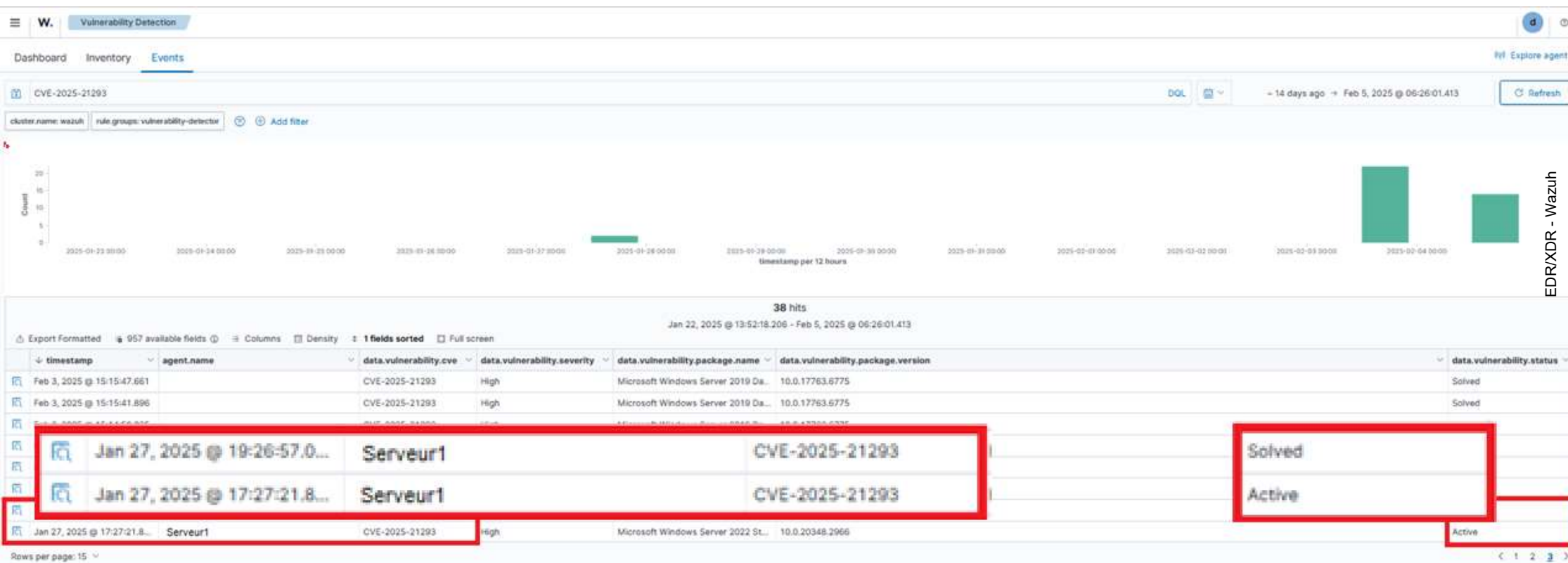


Ubuntu
Debian
RedHat
Amazon Linux
SUSE Linux Enterprise
Arch
Windows
Alma Linux
MacOs

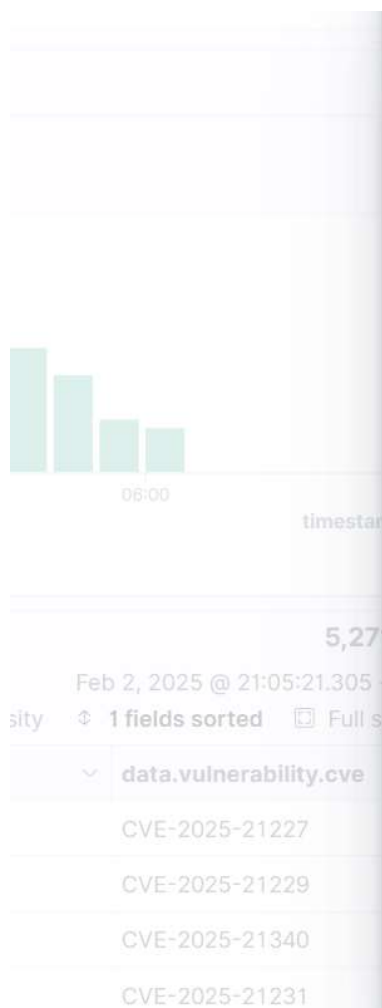
Vulnérabilités

- Collecte des informations par les agents
 - Version de packages
 - Version des applications installées
- Indexation et comparaison des versions avec la base consolidée
 - Source : Les bases CVEs de Wazuh
 - Par défaut toutes les heures

Vulnérabilités : événements



Vulnérabilités : détail



Document Details

[documents](#)
[document](#)

t	data.vulnerability.score.version	3.1
t	data.vulnerability.severity	Medium
t	data.vulnerability.status	Solved
t	data.vulnerability.title	CVE-2025-21227 affecting Microsoft Windows Server 2022 Standard was solved
t	data.vulnerability.type	Packages
t	data.vulnerability.updated	Jan 27, 2025 @ 19:47:16.000
t	decoder.name	json
t	id	1738598102.2714671068
t	input.type	log
t	location	vulnerability-detector
t	manager.name	wazuh.worker
t	rule.description	The CVE-2025-21227 that affected Microsoft Windows Server 2022 Standard was solved due to an update in the agent or feed.
#	rule.firedtimes	1,392
t	rule.gdpr	IV_35.7.d
t	rule.groups	vulnerability-detector
t	rule.id	23502
#	rule.level	3

Inventaire des vulnérabilités

W.

Vulnerability De...

Nom_machine

Dashboard

Inventory

Events

Search

Wazuh cluster name: wazuh

agent id: 319

Evaluated

Under evaluation

Add filter

1,150 hits

Export Formatted

52 available fields

Columns

Density

Sort fields

Full screen

agent.name	package.name	package.version	vulnerability.description	vulnerability.severity	vulnerability.id
Nom_machine	Mozilla Thunderbird (x64 fr)	115.12.2	The nsXMLDocument::OnChannelRedirect function in Moz...	High	CVE-2008-3835
Nom_machine	Mozilla Thunderbird (x64 fr)	115.12.2	Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thund...	High	CVE-2008-4060
Nom_machine	Mozilla Thunderbird (x64 fr)	115.12.2	The jar: URI implementation in Mozilla Firefox before 3.0.9,...	Medium	CVE-2009-1306
Nom_machine	Mozilla Thunderbird (x64 fr)	115.12.2	The view-source: URI implementation in Mozilla Firefox be...	Medium	CVE-2009-1307
Nom_machine	Mozilla Thunderbird (x64 fr)	115.12.2	Cross-site scripting (XSS) vulnerability in Mozilla Firefox b...	Medium	CVE-2009-1308
Nom_machine	Mozilla Thunderbird (x64 fr)	115.12.2	Mozilla Firefox before 3.0.11, Thunderbird, and SeaMonke...	High	CVE-2009-1840
Nom_machine	Mozilla Thunderbird (x64 fr)	115.12.2	Multiple unspecified vulnerabilities in the browser engine L...	High	CVE-2009-3980
Nom_machine	Mozilla Thunderbird (x64 fr)	115.12.2	Unspecified vulnerability in the browser engine in Mozilla ...	High	CVE-2009-3981
Nom_machine	Mozilla Thunderbird (x64 fr)	115.12.2	Multiple unspecified vulnerabilities in the JavaScript engin...	High	CVE-2009-3982
Nom_machine	Mozilla Thunderbird (x64 fr)	115.12.2	Mozilla Firefox before 3.0.16 and 3.5.x before 3.5.6, and S...	Medium	CVE-2009-3983
Nom_machine	Mozilla Thunderbird (x64 fr)	115.12.2	Mozilla Firefox before 3.0.16 and 3.5.x before 3.5.6, and S...	Medium	CVE-2009-3984
Nom_machine	Microsoft Office Professional Plus 2019 - fr-fr	16.0.10413.20020	Microsoft Excel does not warn a user when a macro is pre...	Medium	CVE-1999-0794
Nom_machine	Microsoft Office Professional Plus 2019 - fr-fr	16.0.10413.20020	Buffer overflow in Microsoft Office XP allows remote attac...	High	CVE-2004-0848
Nom_machine	Microsoft Office Professional Plus 2019 - fr-fr	16.0.10413.20020	Microsoft Internet Explorer 5.01, 5.5, and 6 allows remote ...	High	CVE-2005-2127
Nom_machine	Microsoft Office Professional Plus 2019 - fr-fr	16.0.10413.20020	The RichEdit component in Microsoft Windows 2000 SP4, ...	High	CVE-2006-1311

Rows per page: 15

<

1

2

3

4

5

...

77

>

EDR/XDR - Wazuh

Vulnérabilités

- Intérêt



Connaitre les points faibles de nos serveurs

- CVE : Quels risques / impact ?



Avoir une vision globale des packages installés

- Décider de changer d'outil si c'est possible

Vulnérabilités

- Points d'attention



Pas toutes les CVEs

- Nécessite un statut validé par le NIST

“

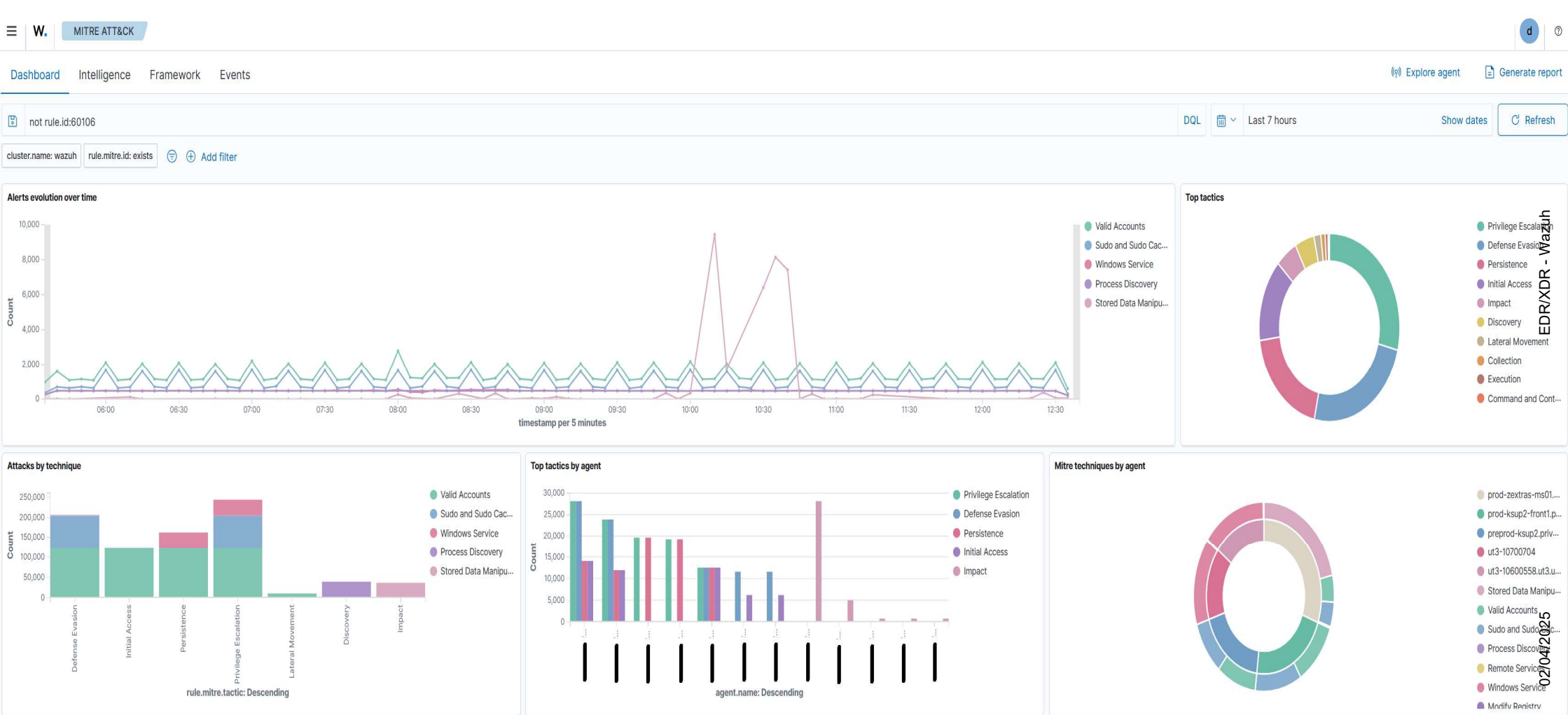
Attaques MITRE



Attaques MITRE

- Vision d'ensemble des possibles attaques
 - Distinguer les tactiques
 - Les équipements les plus concernés
- Culture de la sécurité
 - Les groupes d'attaques et leurs méthodologies
 - Les moyens de mitiger les attaques

Attaques MITRE

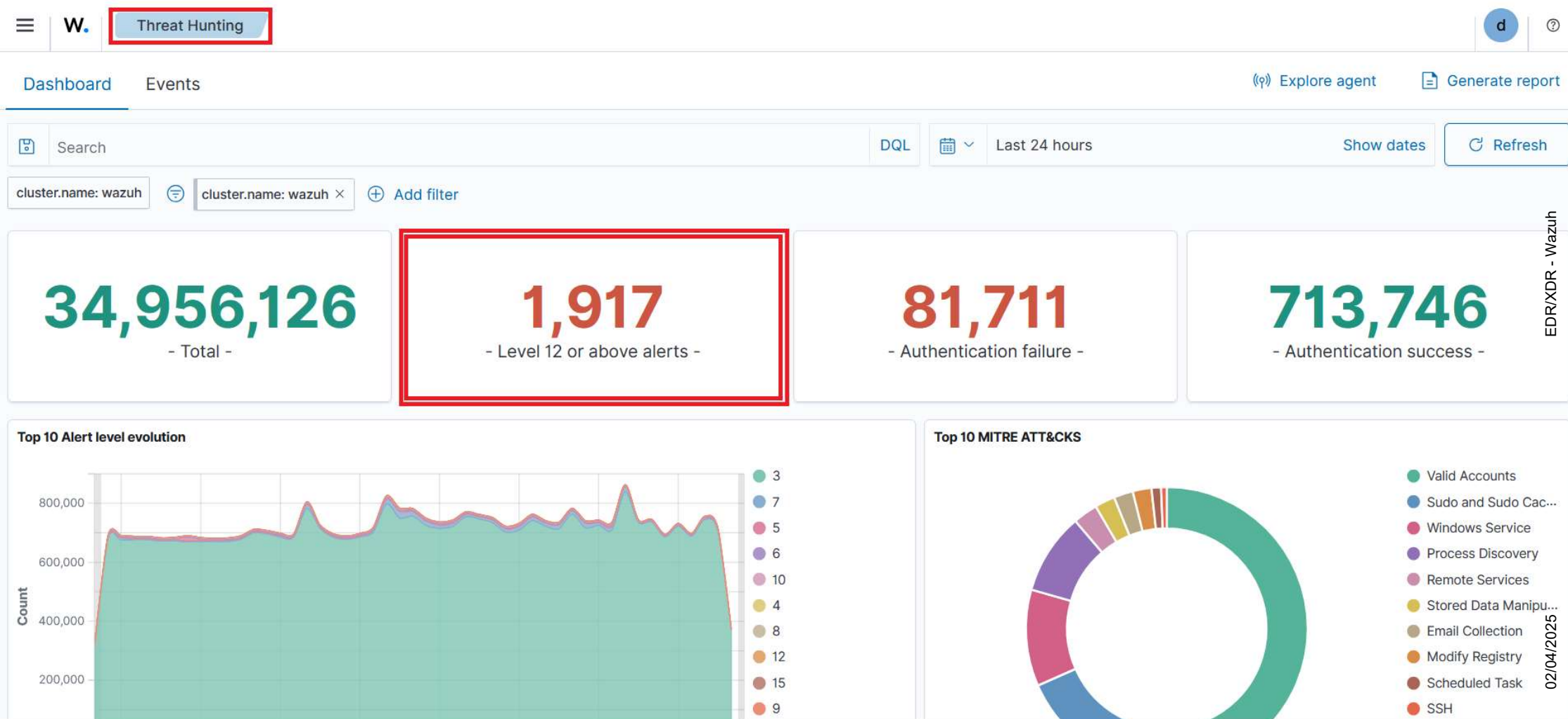


“

Threat hunting



Threat hunting



Threat hunting

- Nettoyage
 - Supprimer les alertes inutiles
 - Doublons sur un temps très court
 - Alertes qui n'apportent rien
 - Diminuer le niveau des faux positifs
 - Alertes de niveau 12 et + (non pertinents seuls)
- Si prestataire de sécurité (PASI, PRIS)
 - Adapter en fonction de leurs besoins

Threat hunting

- Ajouter des alertes
 - Ajouter ce qui contient des IOCs potentiels
 - mails
 - Requêtes DNS
 - Nom d'applicatifs connus
 - Ajouter ce qui correspond à nos procédures
 - Quel compte écrit où ?
 - Si prestataire de sécurité (PASI, PRIS)
 - Adapter en fonction de leurs besoins

Threat hunting

data.win.eventdata.deviceDescription HID Keyboard Device				
data.win.eventdata.deviceId HID\\VID_413C&PID_2113&MI_00\\9&160728ea&0&000				
data.win.eventdata.subjectDomainName UT3				  
data.win.eventdata.subjectLogonId 0x3e7				
data.win.eventdata.subjectUserPosteuteut3\$				
data.win.eventdata.subjectUserSid S-1-5-18				
data.win.eventdata.vendorIds HID\\VID_413C&PID_2113&REV_0108&MI_00 HID\\VID_413C&PID_2113&MI_00 HID\\VID_413C&PID_2113&UP:0001_U:0006 HID_DEVICE_SYSTEM_KEYBOARD HID_DEVICE_UP:0001_U:0006 HID_DEVICE				

Threat hunting

t decoder.name	syscheck_integrity_changed
t full_log	File 'c:\abcd\thumbs.db' modified mode: realtime Changed attributes: mtime,md5,sha1,sha256 Old modification time was: '1737121141', now it is '1737121145' Old md5sum was: '336562dcfcd3b1f1c628a8bc3c22406c' New md5sum is : 'acbb05a995f794dc817bb9f6468c76e3' Old sha1sum was: '23ffac2364aefb7a68a11dc8ab2d2b11300b1f180a'
t id	1737121146.3455964506
t input.type	log
t location	syscheck
t manager.name	wazuh.master
t rule.description	File modified in Shares abcd.

Threat hunting

- Intérêt



Processus non conformes, Fichiers Canaris, Claviers débranchés

- Quelqu'un n'a pas utilisé le processus standard



Télémétrie

- Légitimité des applicatifs utilisés ?



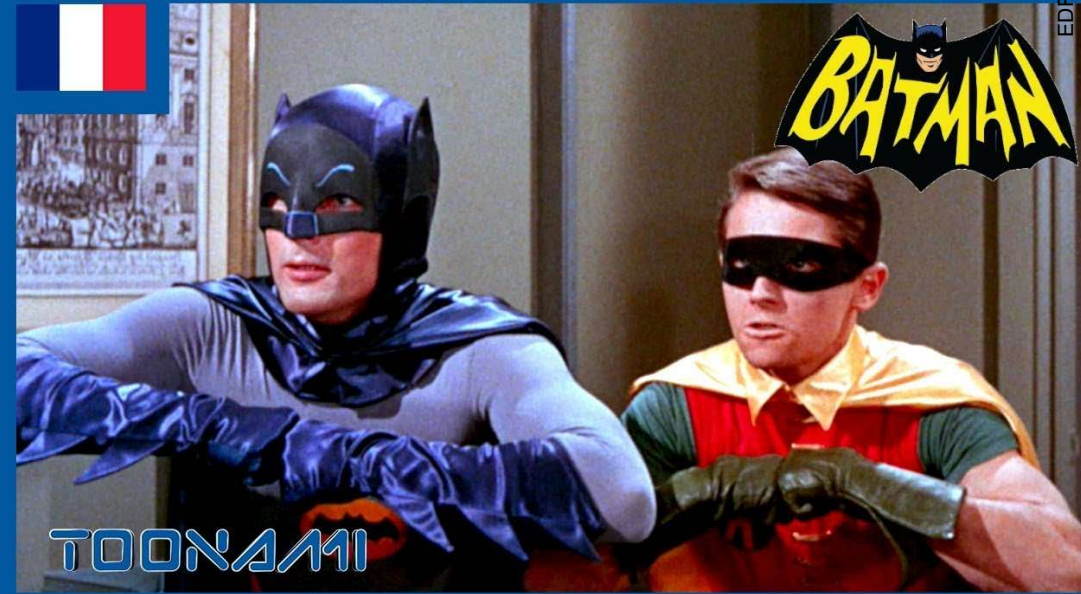
Traçabilité

- Conserver une trace des comportements

“

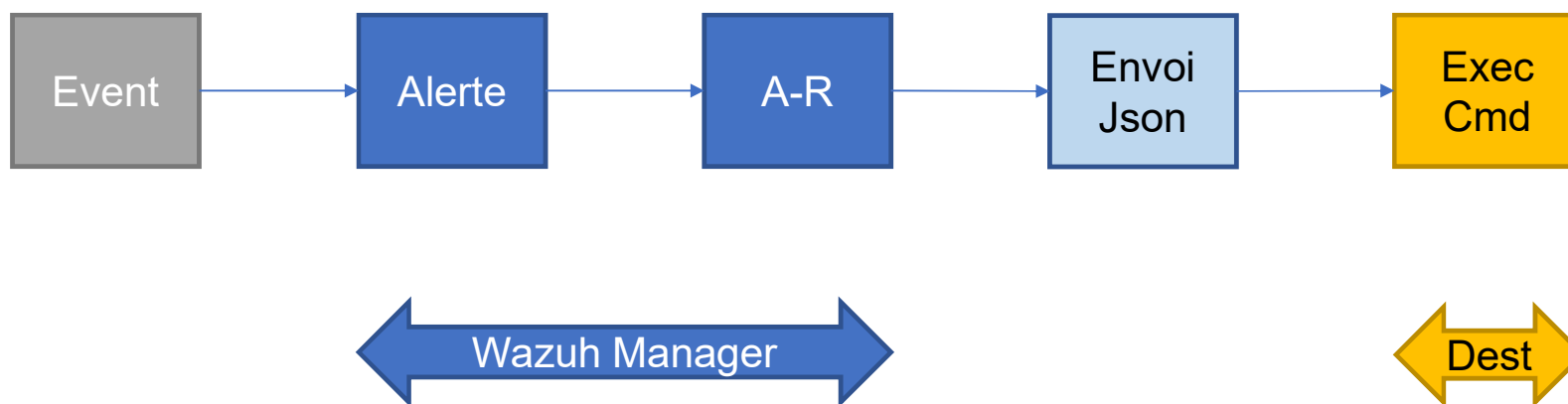


Active Response



Active Response

- Fonctionnement



Active Response

- Des commandes définies sur le serveur

<command>

<name>yara</name>

<**executable**>yara.sh</executable>

<timeout_allowed>**yes**</timeout_allowed>

</command>

Active Response

- Des active responses

```
<active-response>  
  <disabled>no</disabled>  
  <command>yara</command>  
  <location>local</location>  
  <rules_id>5763</rules_id>  
  <timeout>60</timeout>  
</active-response>
```



Local
Server
All
Defined Agent

Active Response

- Chemin des commandes sur l'agent
 - `/var/ossec/active-response/bin`
- Contrôler la configuration
 - `/var/ossec/bin/agent_control -L`
- Tester une commande
 - `/var/ossec/bin/agent_control -b 192.168.1.41 -f yara -u 001`

“



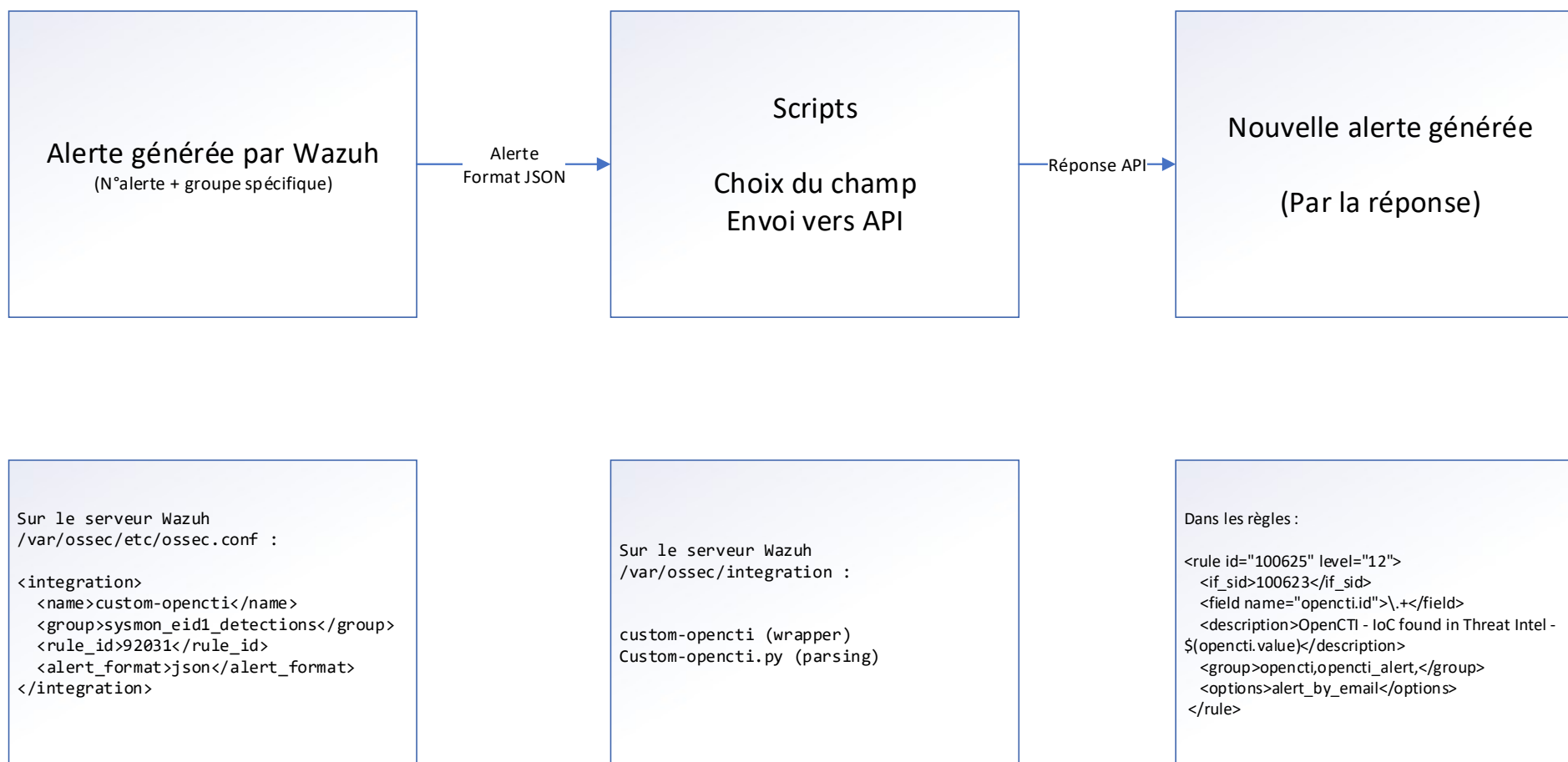
Integration



Integration : principe

- Envoyer des informations vers une API externe
 - Un ou plusieurs champs
 - Effectué par le manager
- Obtenir une réponse
 - Générer une alerte

Integration : principe



Integration : principe

- Intérêt



Transformer un signal faible en signal fort



Envoyer une alerte sur un autre outil (slack, des EDRs de parefeu...)

A photograph of a modern library or study hall with large windows. Several students are seated at long white tables, working on papers and laptops. In the foreground, a young woman with long brown hair, wearing a white t-shirt and blue jeans, is sitting at a table, looking down at a book. Next to her, another student is writing in a notebook. The room is bright and airy, with natural light coming from the windows.

FIN

- Bonne utilisation !

Références

- Wazuh
 - <https://documentation.wazuh.com/current>
- Decoders/Rules
 - <https://socfortress.medium.com/understanding-wazuh-decoders-4093e8fc242c>
 - <https://github.com/wazuh/wazuh-ruleset>
 - <https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/regex.html>
- Active Response
 - <https://documentation.wazuh.com/current/user-manual/reference/ossec-conf/commands.html>
 - <https://documentation.wazuh.com/current/user-manual/capabilities/active-response/how-to-configure.html>
- Vulnérabilités
 - <https://documentation.wazuh.com/current/user-manual/capabilities/vulnerability-detection/how-it-works.html>

Références

- Wazuh
 - <https://documentation.wazuh.com/current>
- Installation
 - Ansible
 - <https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/index.html>
 - Docker
 - <https://documentation.wazuh.com/current/deployment-options/docker/wazuh-container.html>
 - Sizing
 - <https://medium.com/@wernertie/series-wazuh-master-worker-indexer-dashboard-and-the-ainfrastructure-3a629ae2fa0d>