02/04/2025

Wazuh
Le super-héros de la sécurité

UNIVERSITÉ TOULOUSE III PAUL SABATIER
Université Fédérale Toulouse Midi-Pyrénées

“


WAZUH!


Wa…quoi
?
EDR/XDR - Wazuh

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

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

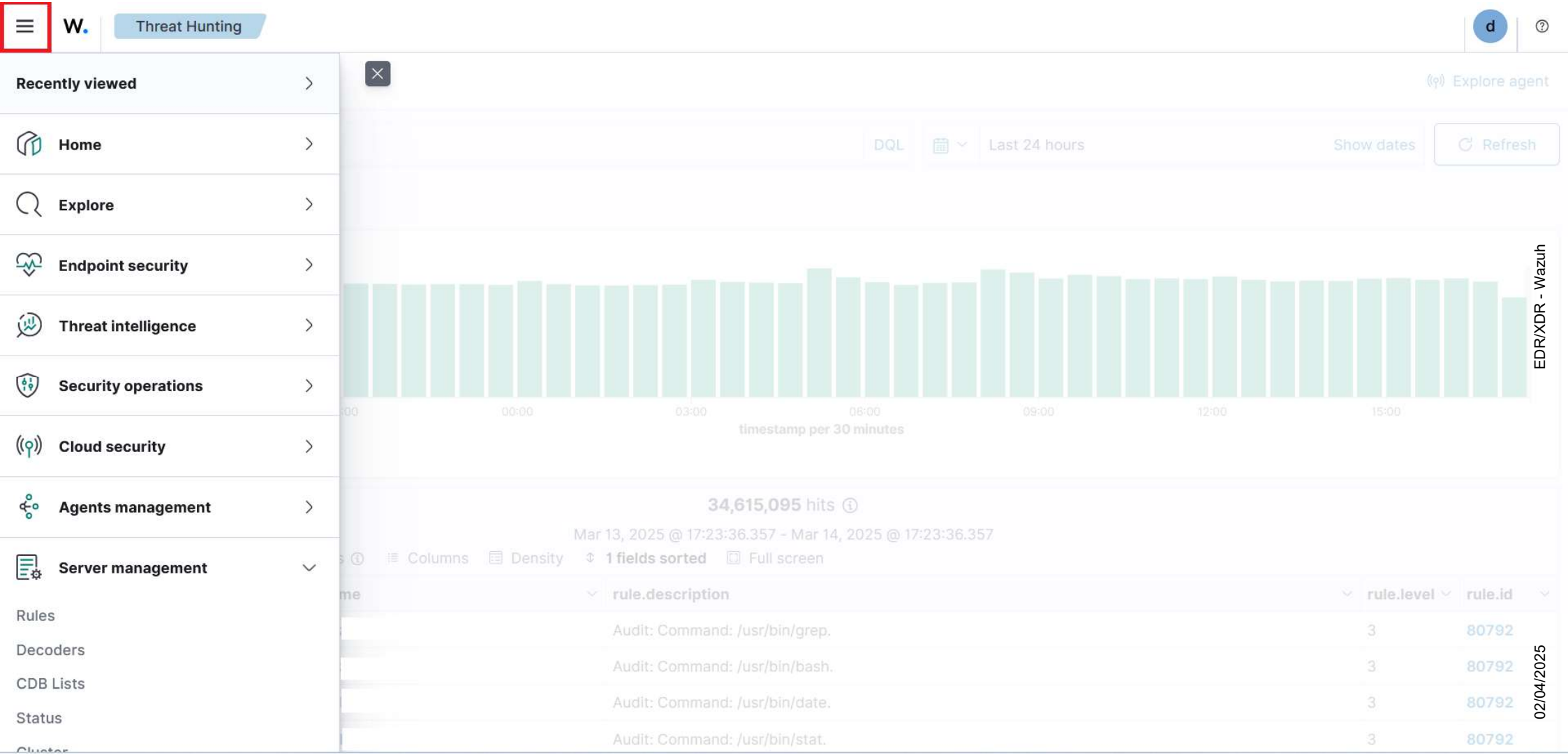
- Authentification
  - Active Directory (en LDAP)
  - MS Entra ID, Google, etc (non testé)
  - Comptes locaux

- Gestion des agents
  - Peuvent appartenir à plusieurs groupes
  - Fichier de configuration en central

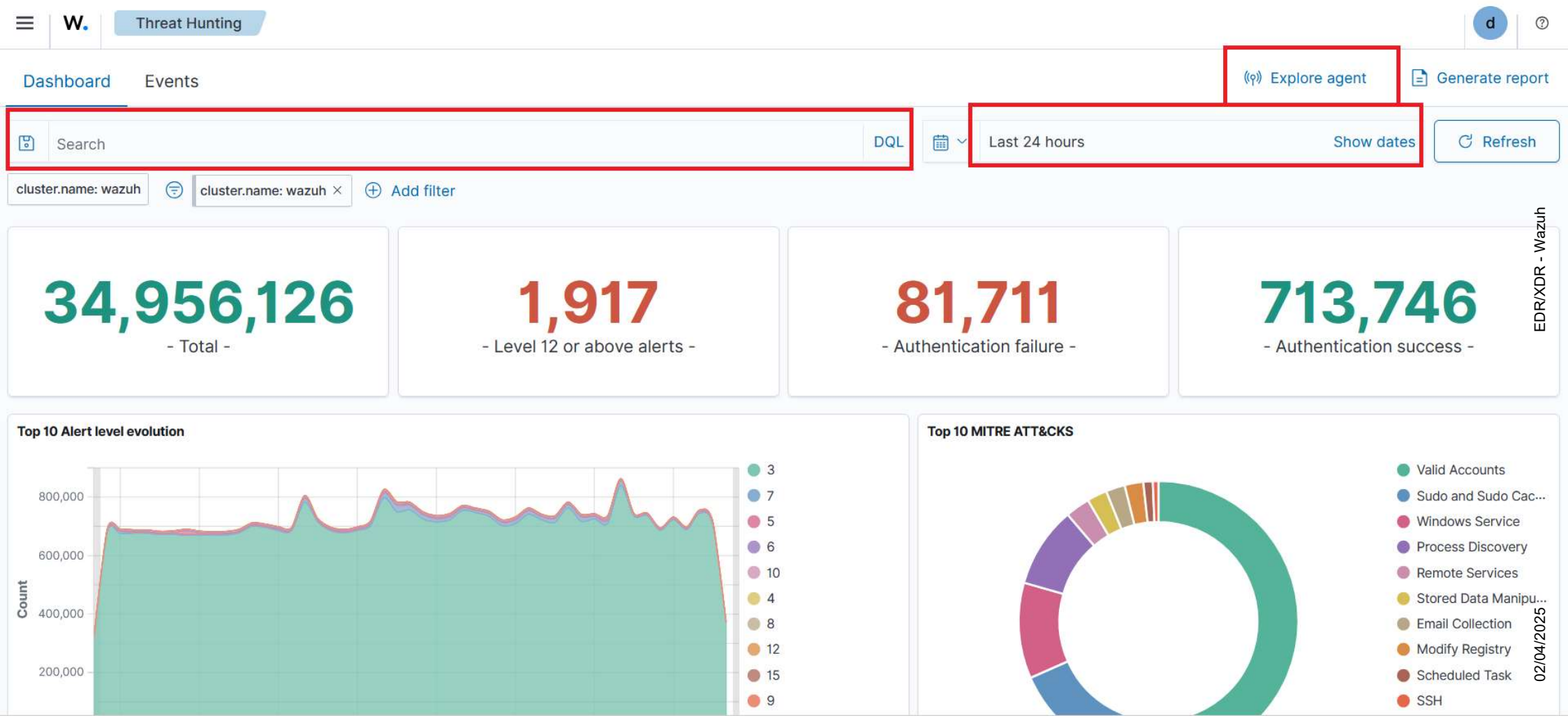
- Gestion par tenant
  - Filtrage basé sur le Document Security Level d’Opensearch
  - RBAC

Principe de fonctionnement

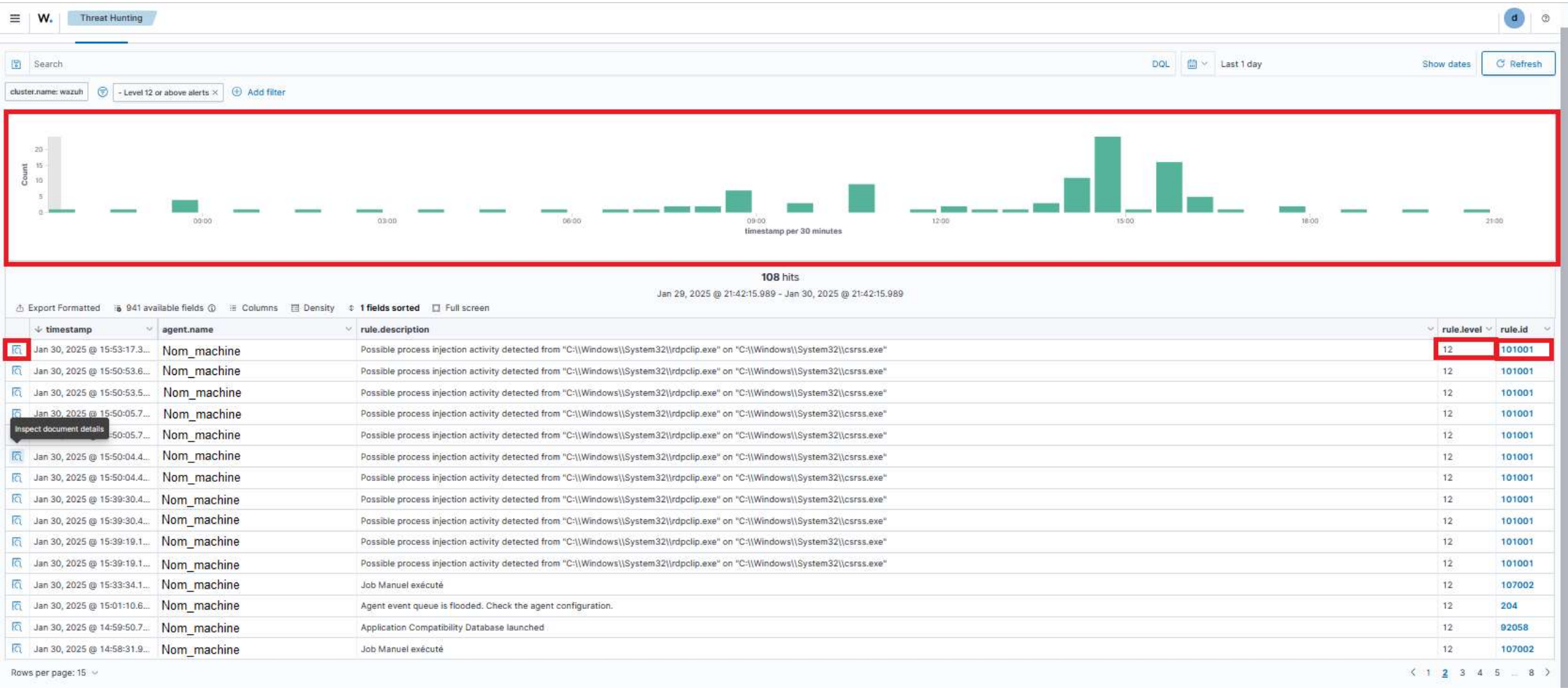
Administration



Evènements de sécurité

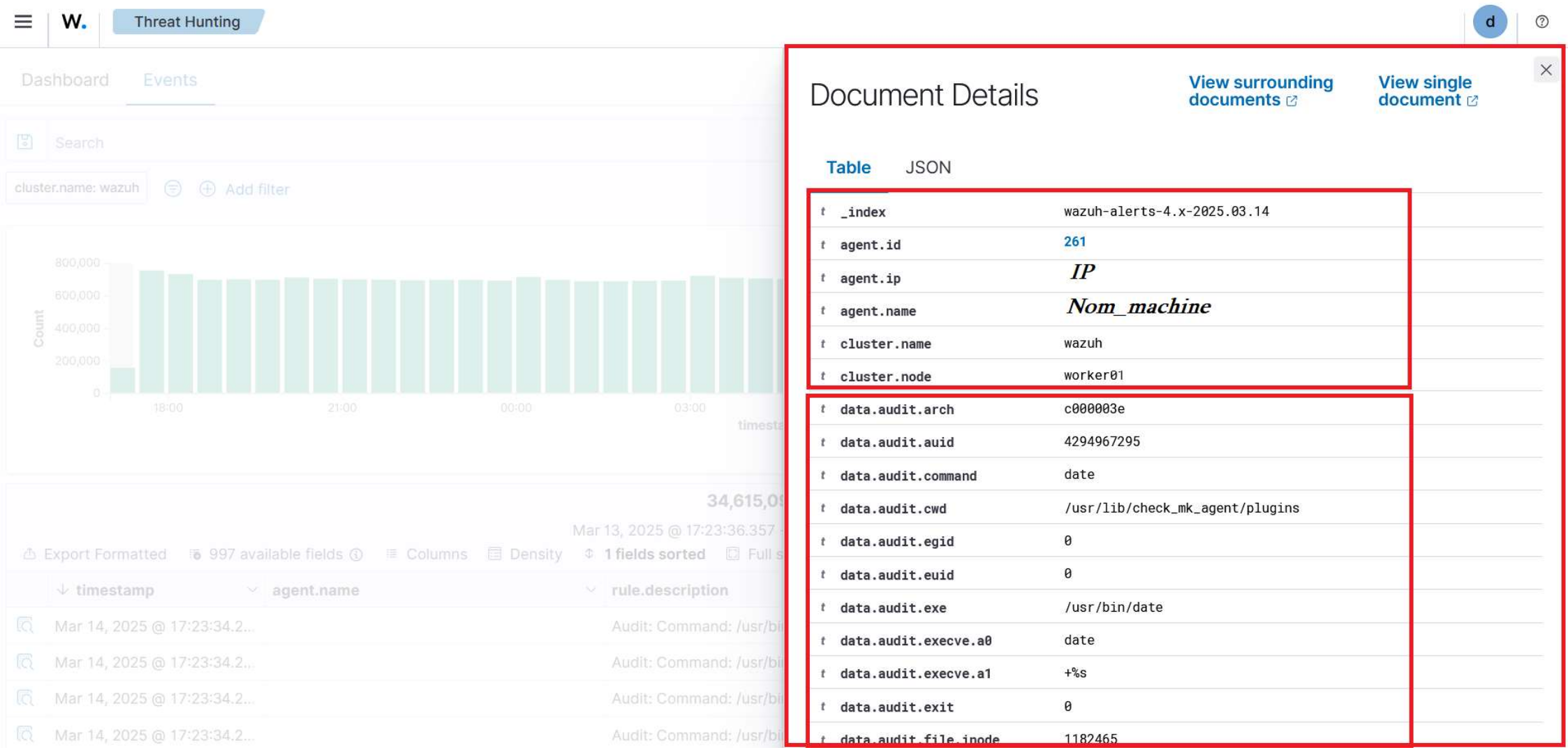


Evènements de sécurité



timestamp	agent.name	rule.description	rule.level	rule.id
Jan 30, 2025 @ 15:53:17.3...	Nom_machine	Possible process injection activity detected from "C:\\Windows\\System32\\rdpclip.exe" on "C:\\Windows\\System32\\csrss.exe"	12	101001
Jan 30, 2025 @ 15:50:53.6...	Nom_machine	Possible process injection activity detected from "C:\\Windows\\System32\\rdpclip.exe" on "C:\\Windows\\System32\\csrss.exe"	12	101001
Jan 30, 2025 @ 15:50:53.5...	Nom_machine	Possible process injection activity detected from "C:\\Windows\\System32\\rdpclip.exe" on "C:\\Windows\\System32\\csrss.exe"	12	101001
Jan 30, 2025 @ 15:50:05.7...	Nom_machine	Possible process injection activity detected from "C:\\Windows\\System32\\rdpclip.exe" on "C:\\Windows\\System32\\csrss.exe"	12	101001
Jan 30, 2025 @ 15:50:05.7...	Nom_machine	Possible process injection activity detected from "C:\\Windows\\System32\\rdpclip.exe" on "C:\\Windows\\System32\\csrss.exe"	12	101001
Jan 30, 2025 @ 15:50:04.4...	Nom_machine	Possible process injection activity detected from "C:\\Windows\\System32\\rdpclip.exe" on "C:\\Windows\\System32\\csrss.exe"	12	101001
Jan 30, 2025 @ 15:50:04.4...	Nom_machine	Possible process injection activity detected from "C:\\Windows\\System32\\rdpclip.exe" on "C:\\Windows\\System32\\csrss.exe"	12	101001
Jan 30, 2025 @ 15:39:30.4...	Nom_machine	Possible process injection activity detected from "C:\\Windows\\System32\\rdpclip.exe" on "C:\\Windows\\System32\\csrss.exe"	12	101001
Jan 30, 2025 @ 15:39:30.4...	Nom_machine	Possible process injection activity detected from "C:\\Windows\\System32\\rdpclip.exe" on "C:\\Windows\\System32\\csrss.exe"	12	101001
Jan 30, 2025 @ 15:39:19.1...	Nom_machine	Possible process injection activity detected from "C:\\Windows\\System32\\rdpclip.exe" on "C:\\Windows\\System32\\csrss.exe"	12	101001
Jan 30, 2025 @ 15:39:19.1...	Nom_machine	Possible process injection activity detected from "C:\\Windows\\System32\\rdpclip.exe" on "C:\\Windows\\System32\\csrss.exe"	12	101001
Jan 30, 2025 @ 15:33:34.1...	Nom_machine	Job Manuel exécuté	12	107002
Jan 30, 2025 @ 15:01:10.6...	Nom_machine	Agent event queue is flooded. Check the agent configuration.	12	204
Jan 30, 2025 @ 14:59:50.7...	Nom_machine	Application Compatibility Database launched	12	92058
Jan 30, 2025 @ 14:58:31.9...	Nom_machine	Job Manuel exécuté	12	107002

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 autorised 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

t cluster.node	worker01
t data.file	/dev/nul
t data.title	File present on /dev.
t decoder.name	rootcheck
t full_log	File '/dev/nul' present on /dev. Possible hidden file.
t id	1743219037.5075230536
t input.type	log
t location	rootcheck
t manager.name	wazuh.worker
t rule.description	Host-based anomaly detection event (rootcheck).

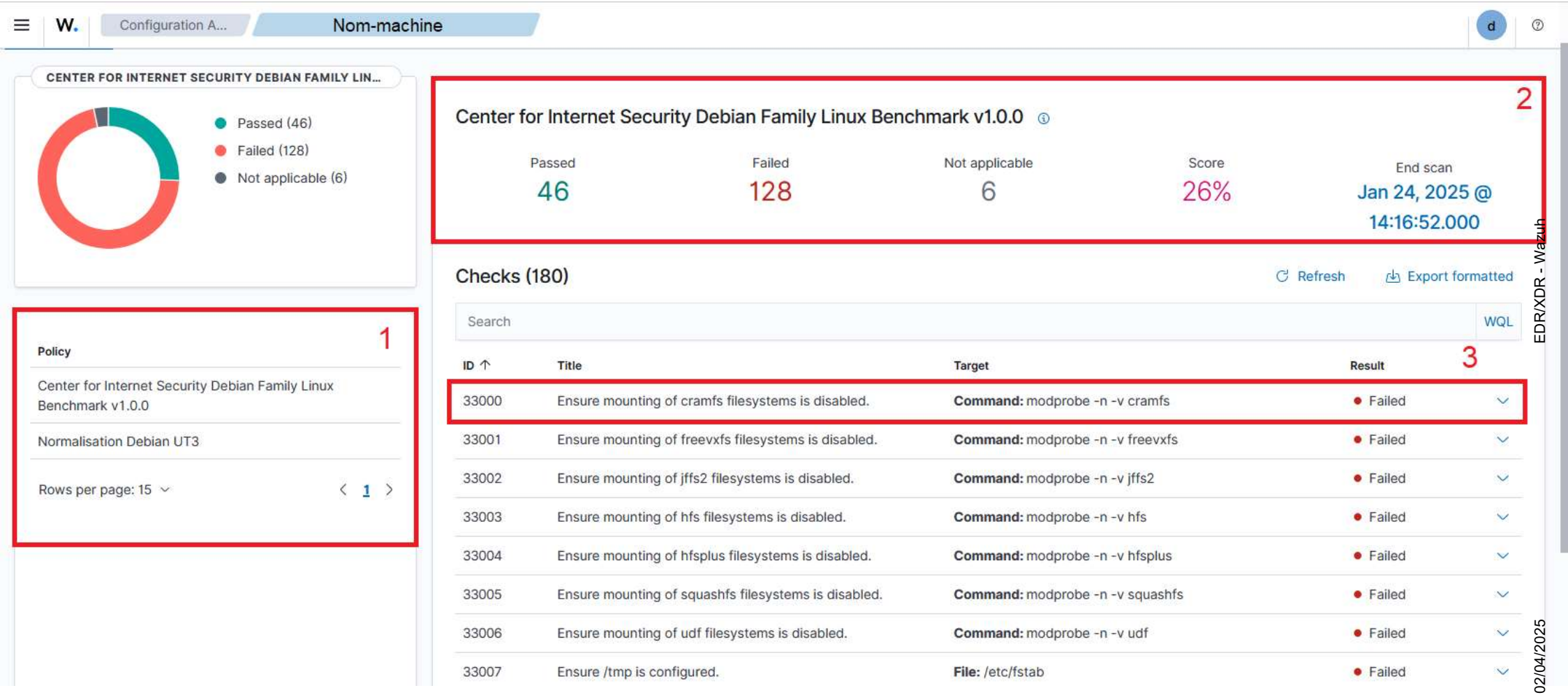
t data.title	NTFS Alternate data stream found: 'C:\Program Files\LAPS:Win32App_1'.
t decoder.name	rootcheck
t full_log	NTFS Alternate data stream found: 'C:\Program Files\LAPS:Win32App_1'. Possible hidden content.
t id	1743285819.2491494943

Malware Detection

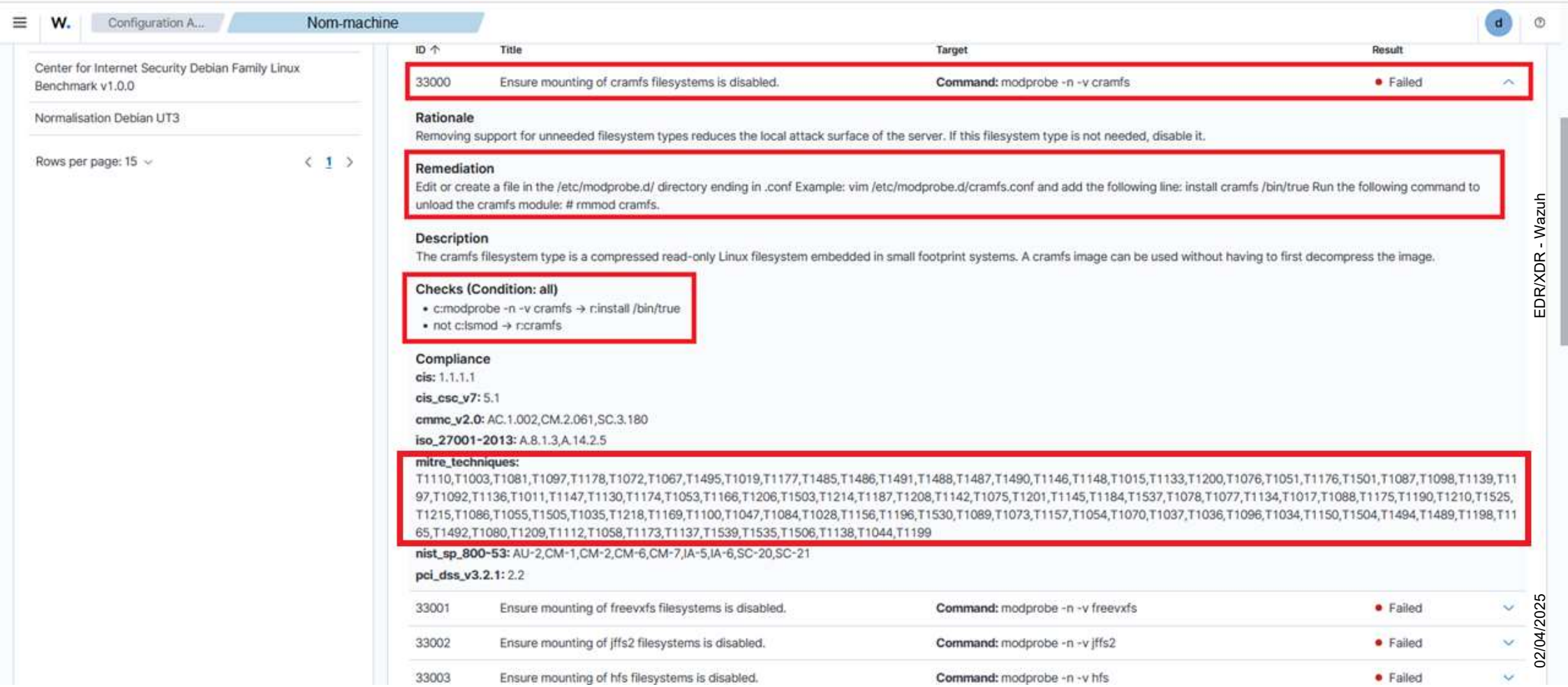
- S’appuie beaucoup sur des outils tiers

Evaluation des configurations

Exemple de conformité



Détail d'une règle de conformité



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 shell qui renvoie une valeur interprétable en regex

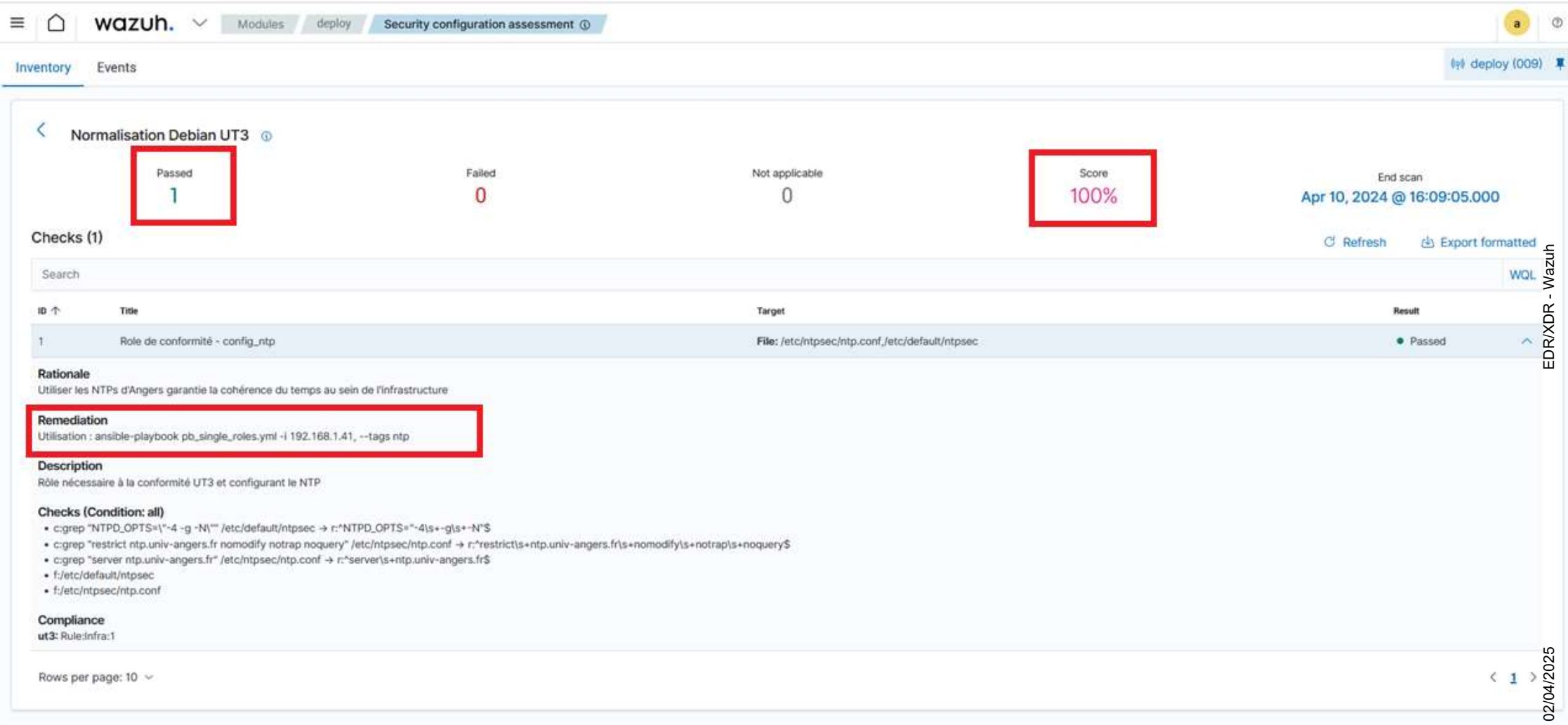
  c:[commande] -> r:^regex$

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



Security Configuration Assessment

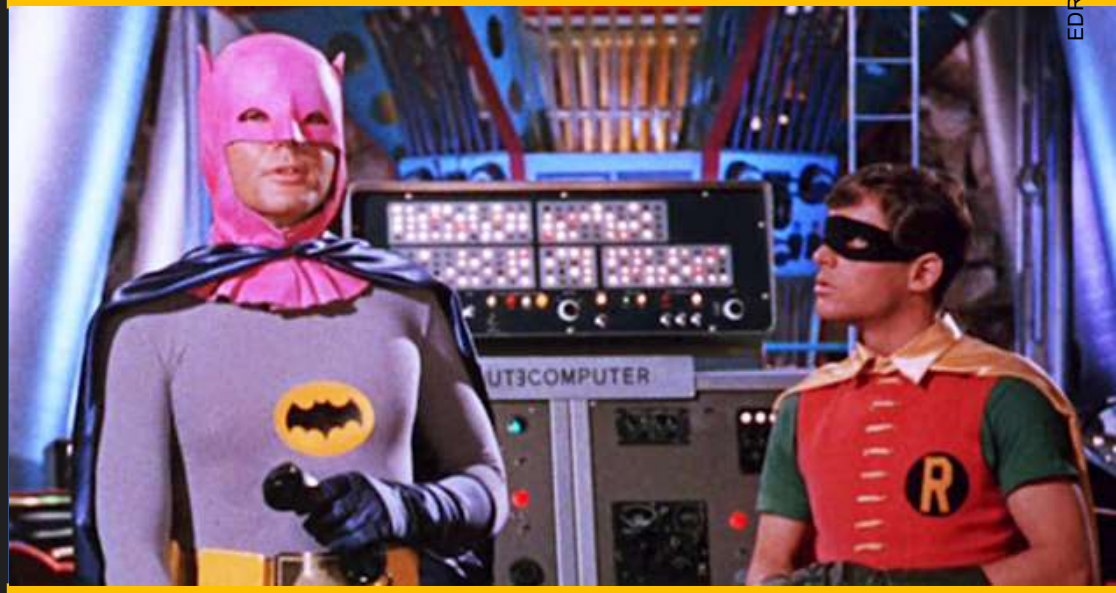
- Intérêt

→ S’assurer que la configuration est déployée et conforme
  - Personne n’a modifié les configurations clefs

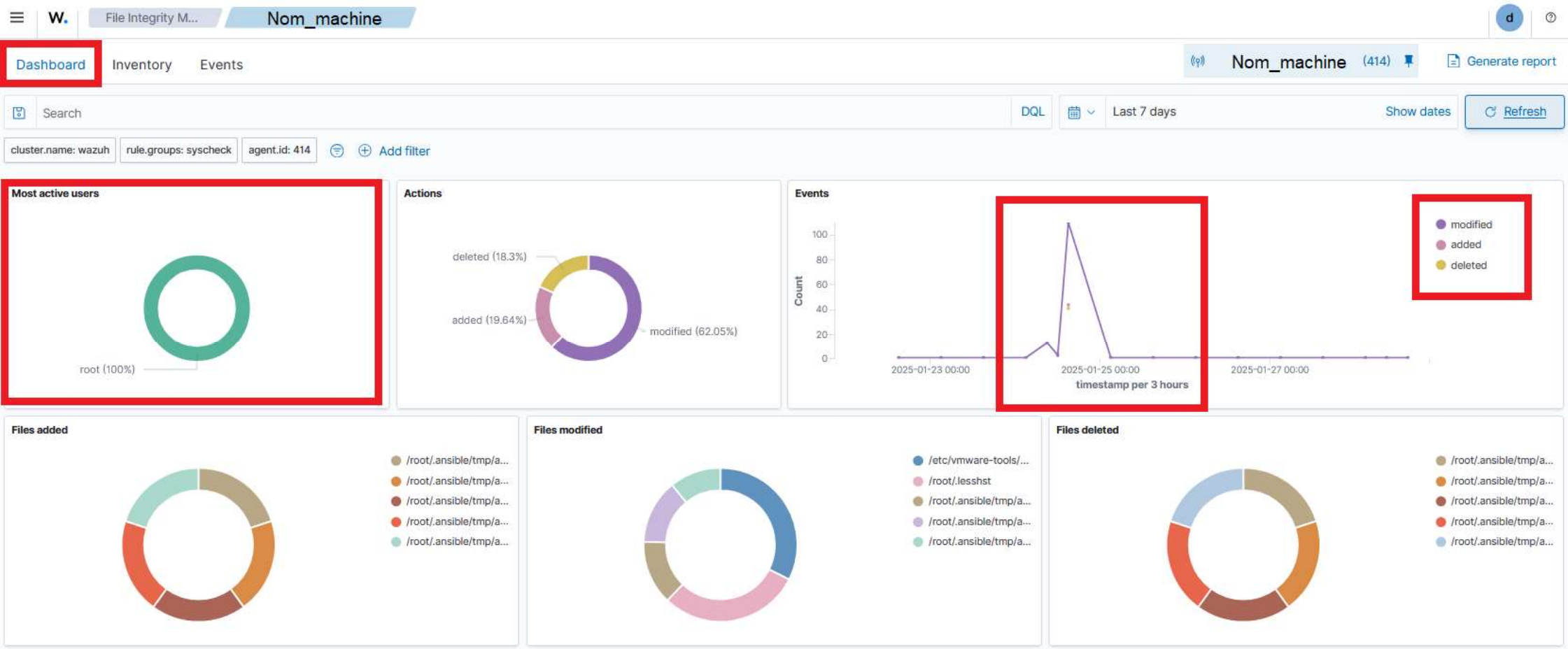
→ Conserver de la souplesse
  - Personnalisation d’un serveur

→ Aperçu de la maitrise du parc
  - Postes
  - Serveurs

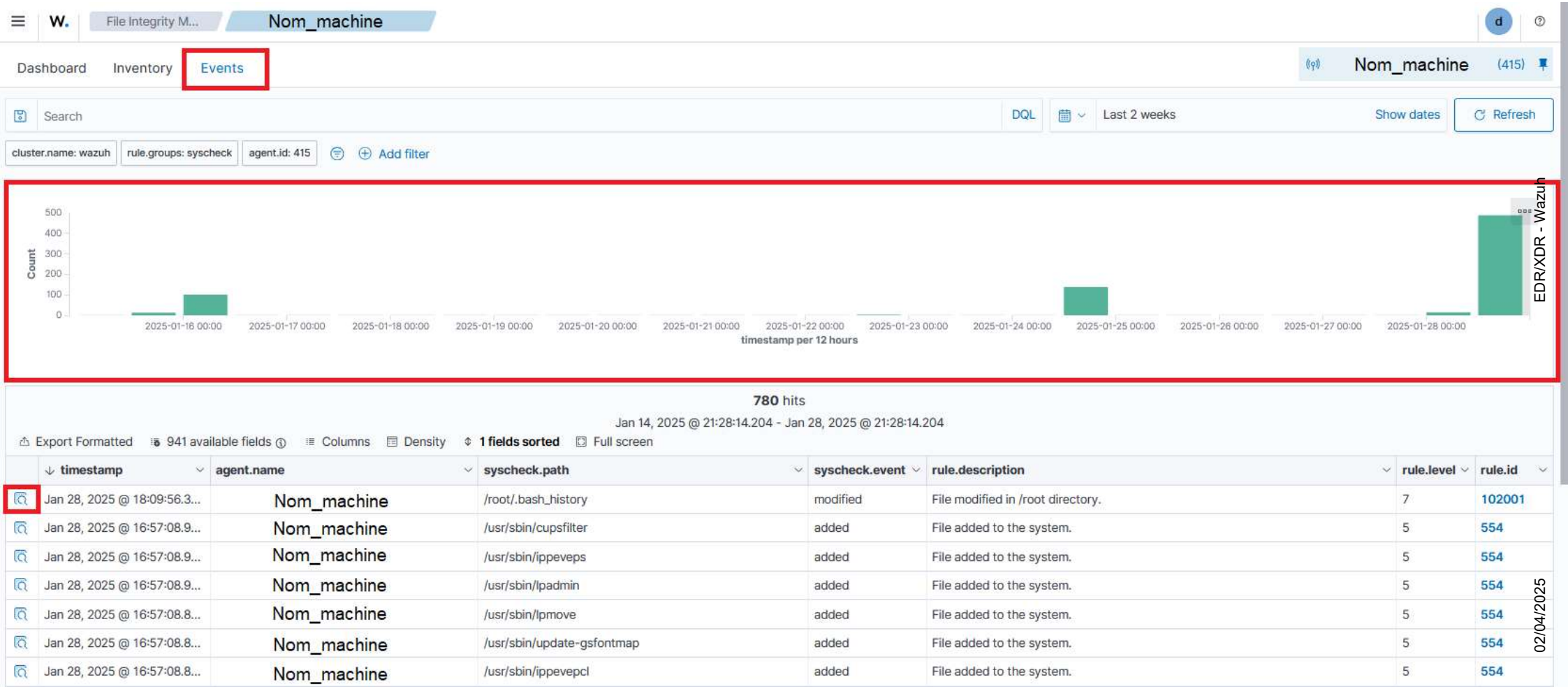
Intégrité des fichiers



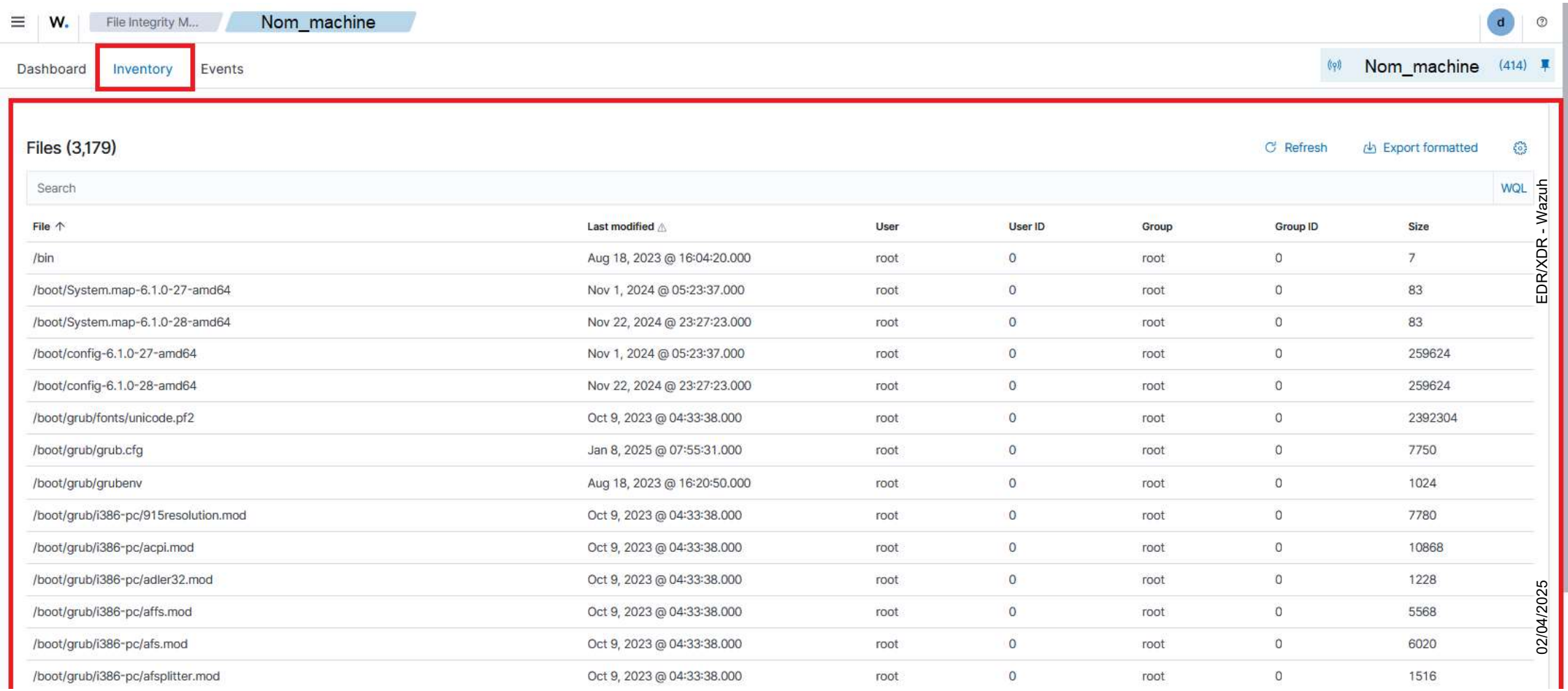
Files Integrity Monitoring : Dashboard



Files Integrity Monitoring : events



Files Integrity Monitoring : inventaire des fichiers



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 ?

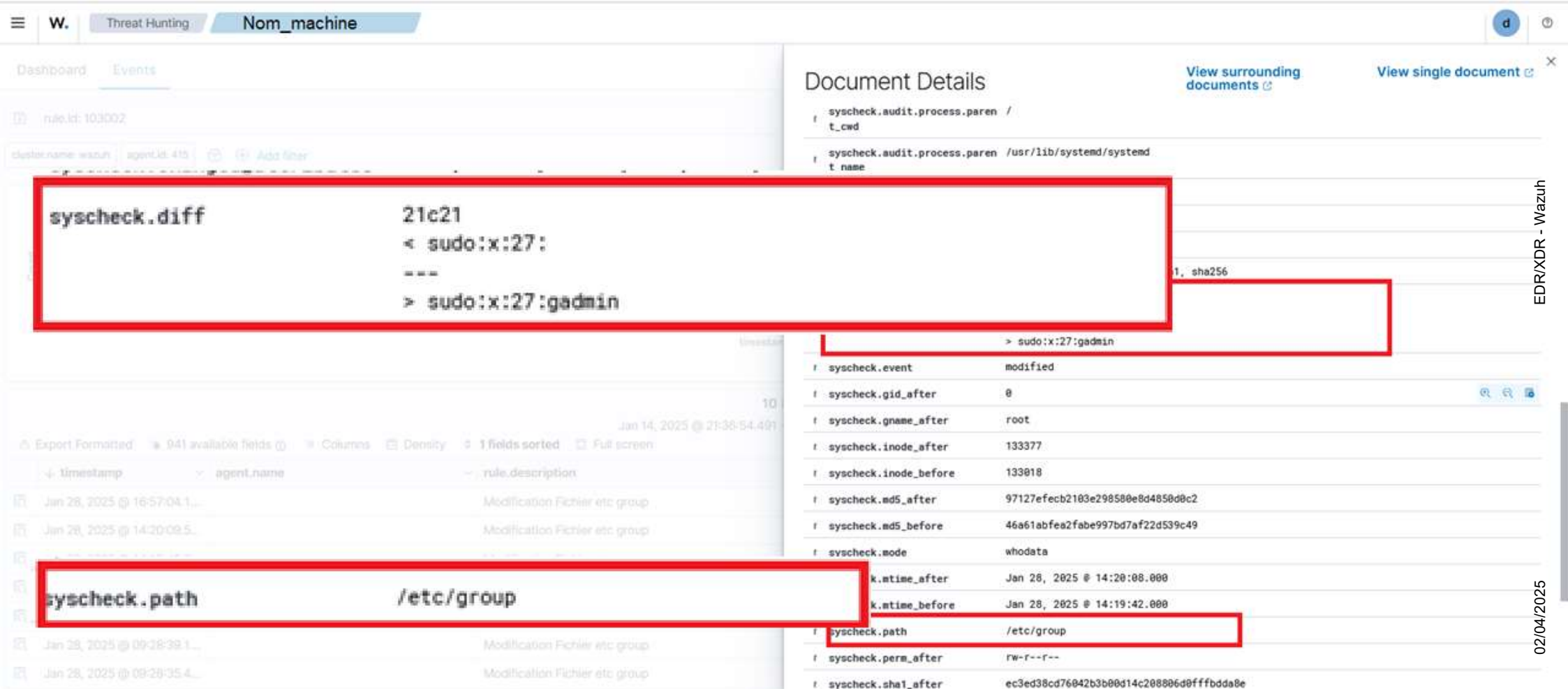
Reporting de la modification exacte

- Permet d'analyser rapidement

Bon contrôle des fichiers clés

- Rassurant

Files Integrity Monitoring : Alertes

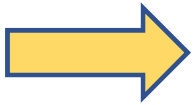


Security Configuration Assessment

- Points d’attention

Limitation du nombre de fichier à analyser

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

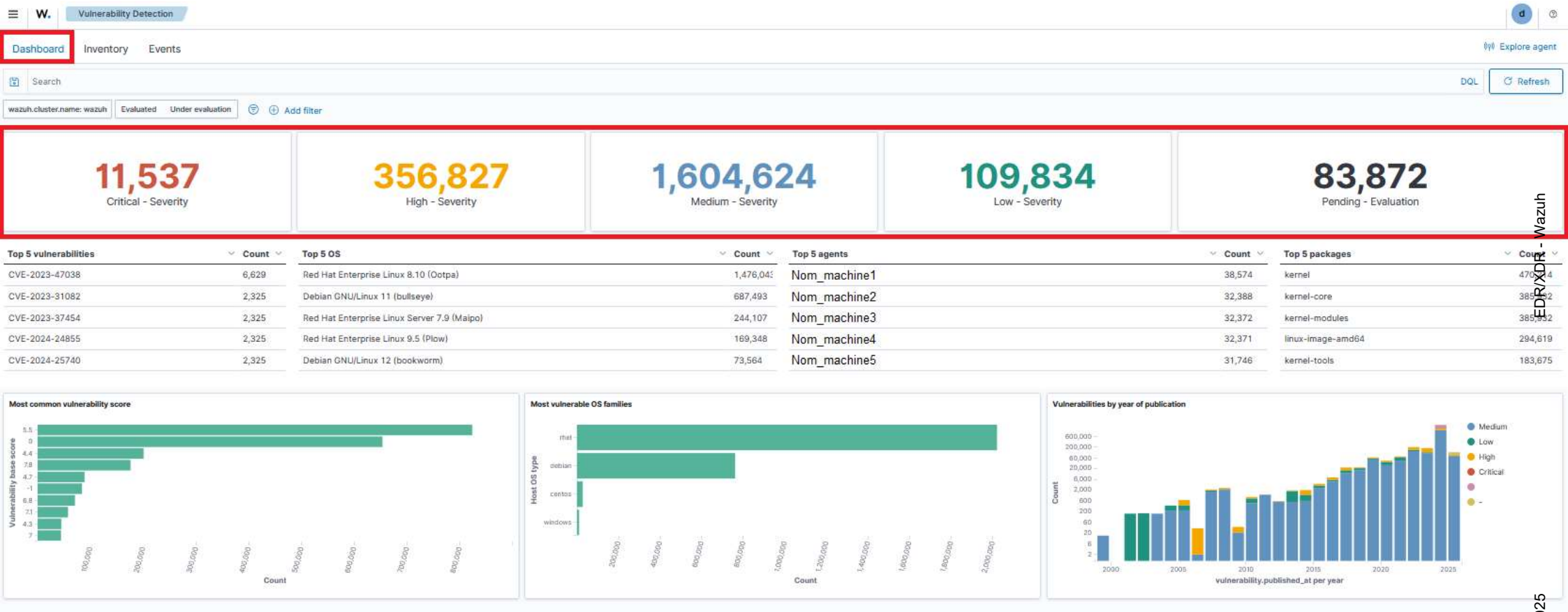


Double alerting possible

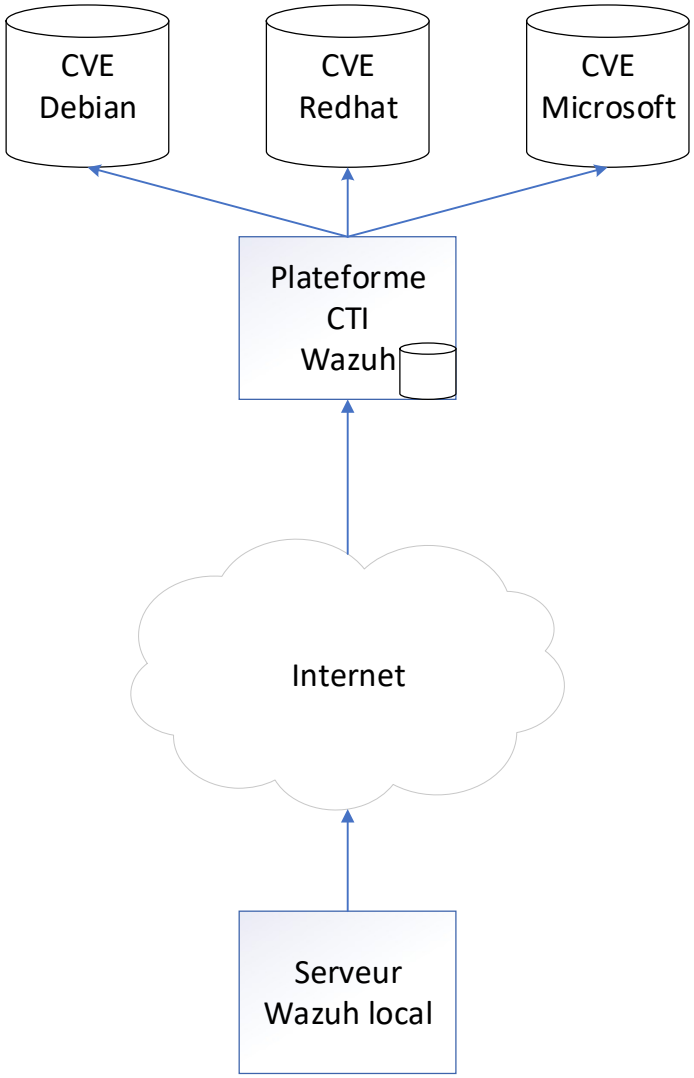
- Si temps réel + check standard du dossier

Vulnérabilités

Vulnérabilités



Vulnérabilités



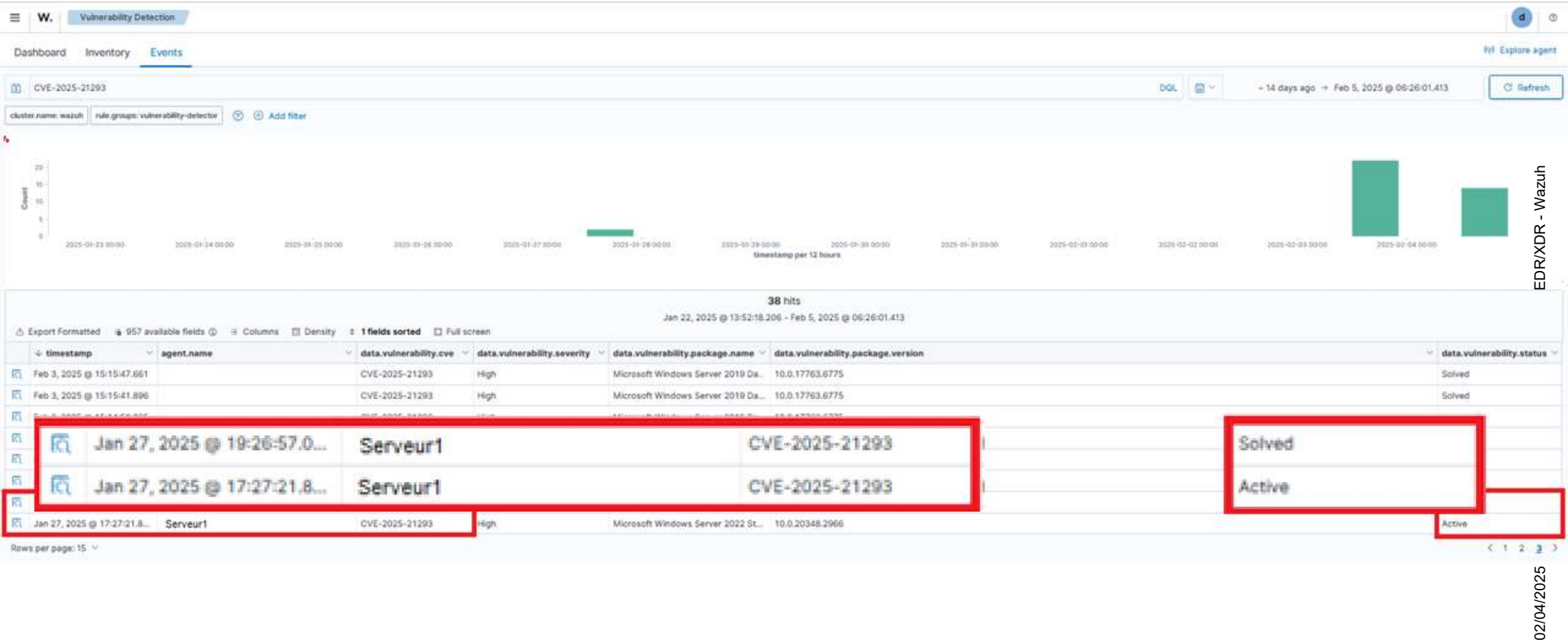
Ubuntu
Debian
RedHat
Amazon Linux
SUSE Linux Enterprise
Arch
Windows
Alma Linux
MacOs

Vulnérabilités

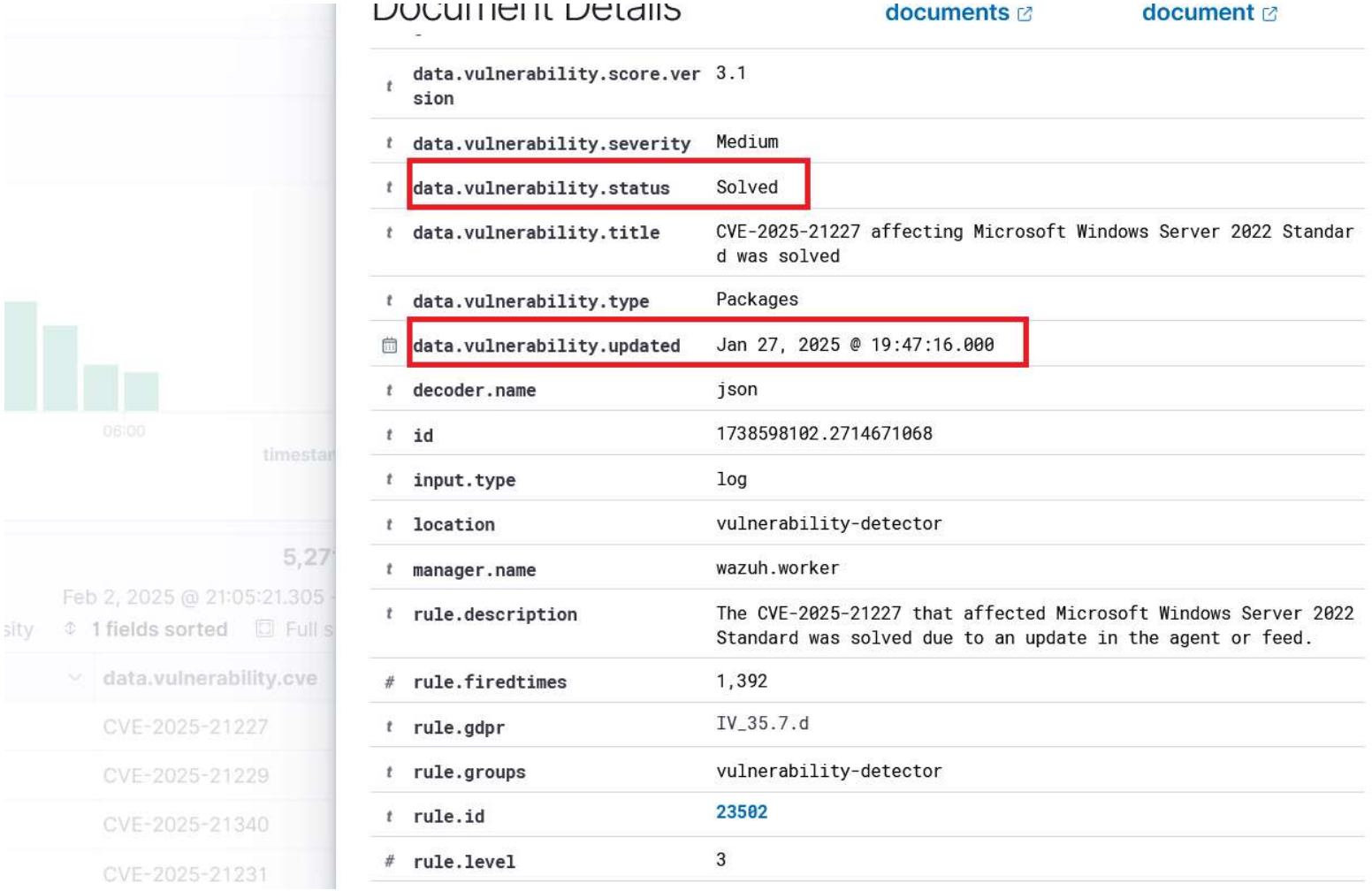
- Collecte des informations par les agents
  - Version de packages
  - Version des applications installées

- Indexation et comparaison des versions avec la base consolidée
  - Source : Les bases CVEs de Wazuh
  - Par défaut toutes les heures

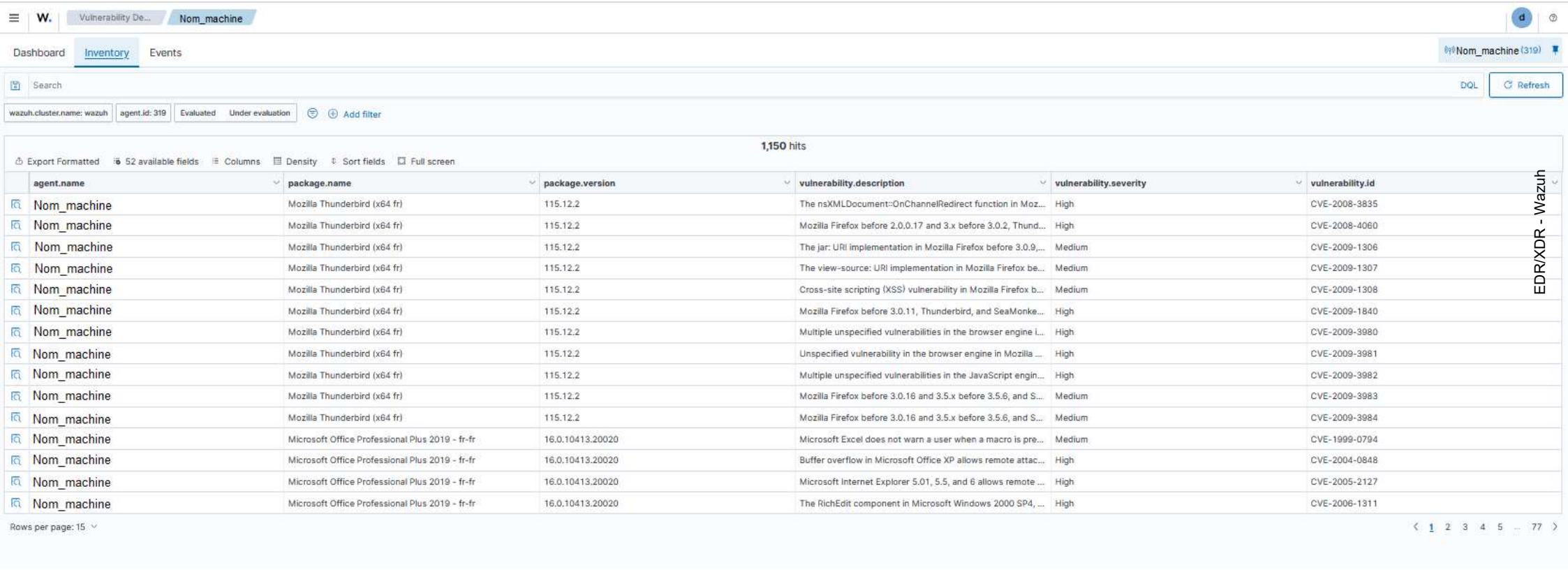
Vulnérabilités : événements



Vulnérabilités : détail



Inventaire des vulnérabilités



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 i...	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

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

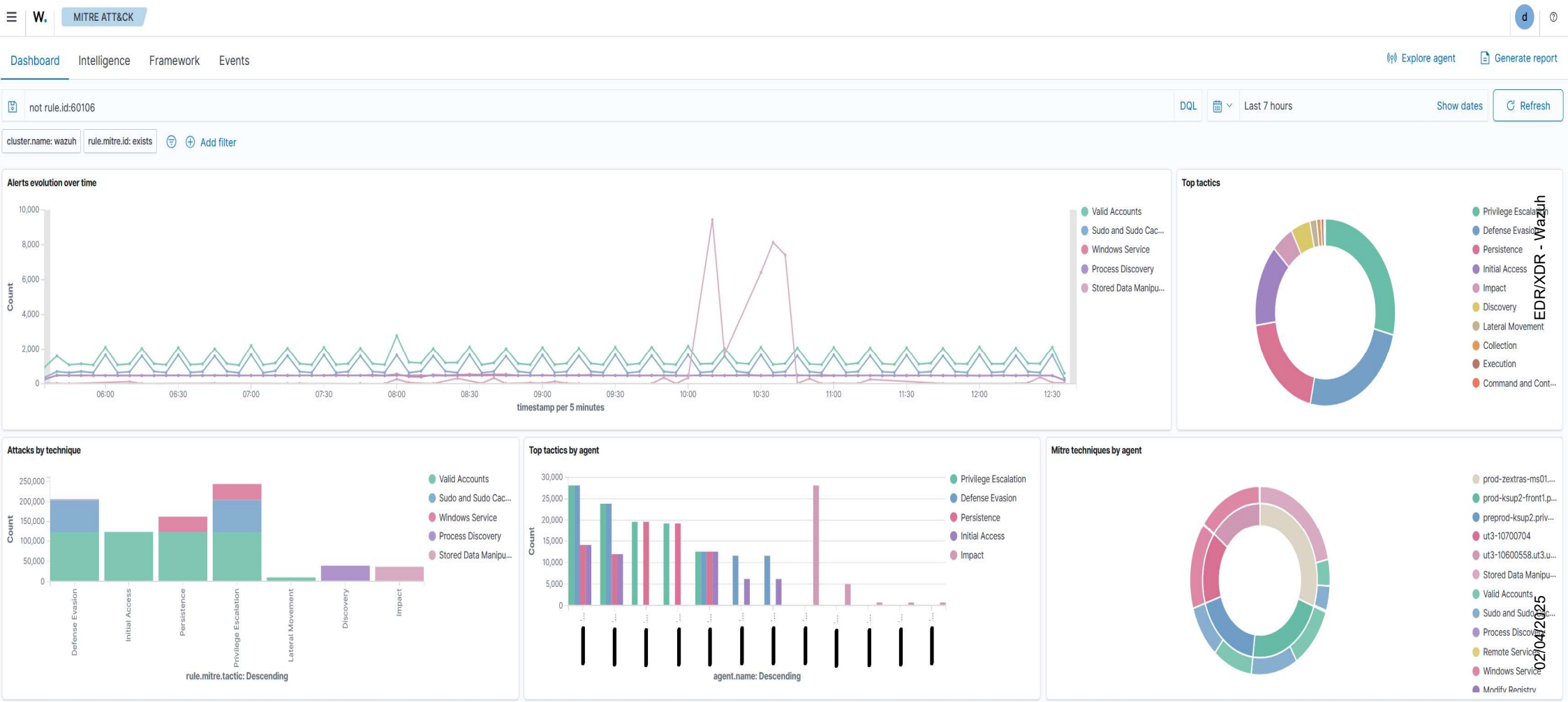
Attaques MITRE

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

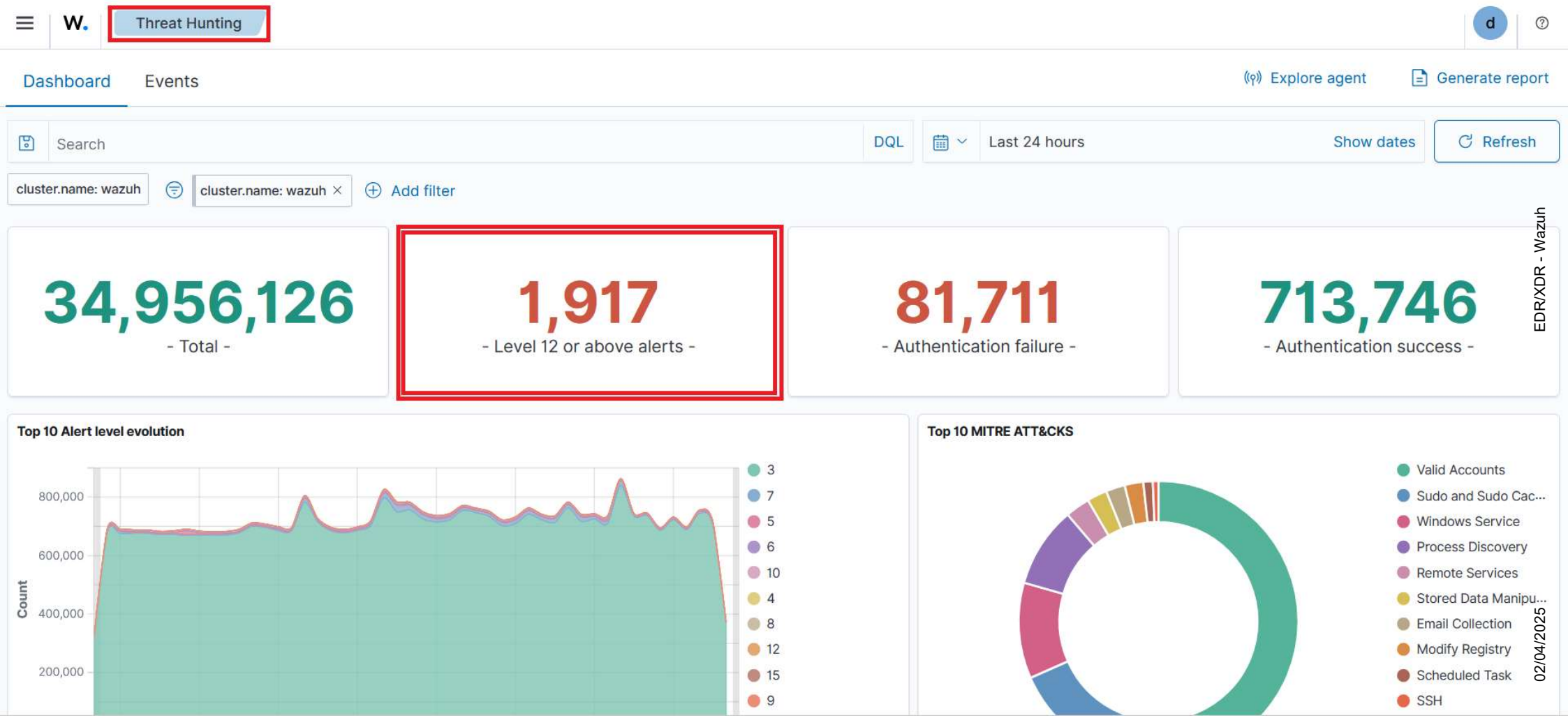
Attaques MITRE



“

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

t	data.win.eventdata.deviceDescription	HID Keyboard Device
t	data.win.eventdata.deviceId	HID\\VID_413C&PID_2113&MI_00\\9&160728ea&0&0000
t	data.win.eventdata.subjectDomainName	UT3
t	data.win.eventdata.subjectLogonId	0x3e7
t	data.win.eventdata.subjectUserName	Posteut3$
t	data.win.eventdata.subjectUserSid	S-1-5-18
t	data.win.eventdata.vendorIds	HID\\VID_413C&PID_2113&REV_0108&MI_00 HID\\VID_413C&PID_2113&MI_00 HID\\VID_413C&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: '23ffec2364efb7a684dd8eb2d2b1430bb1f189a'
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

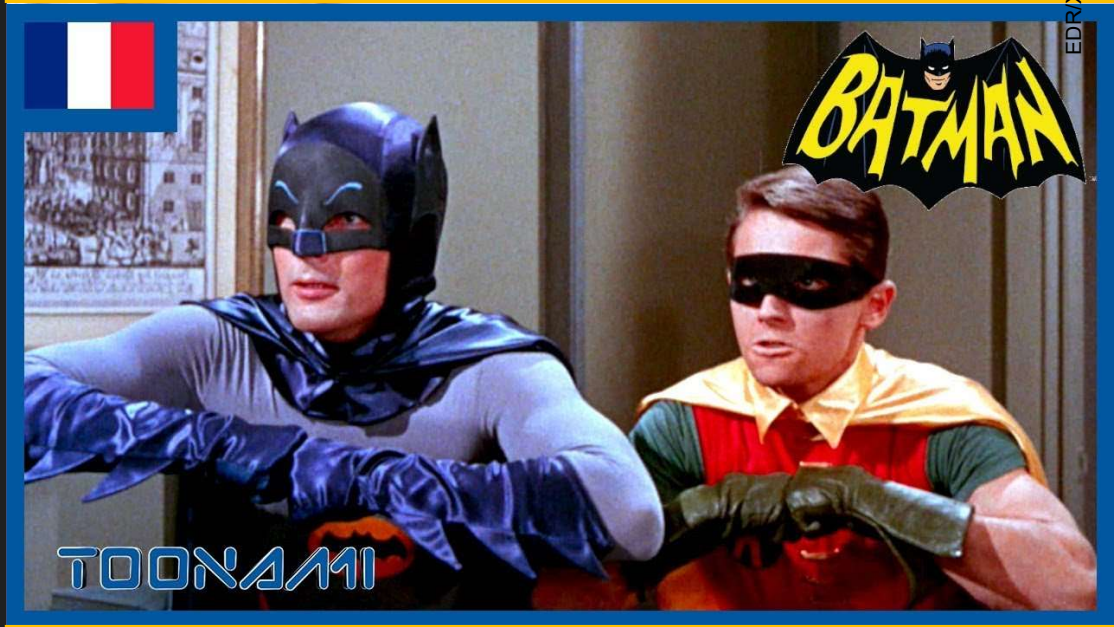
→ Télémétrie

  - Légitimité des applicatifs utilisés ?

→ Traçabilité

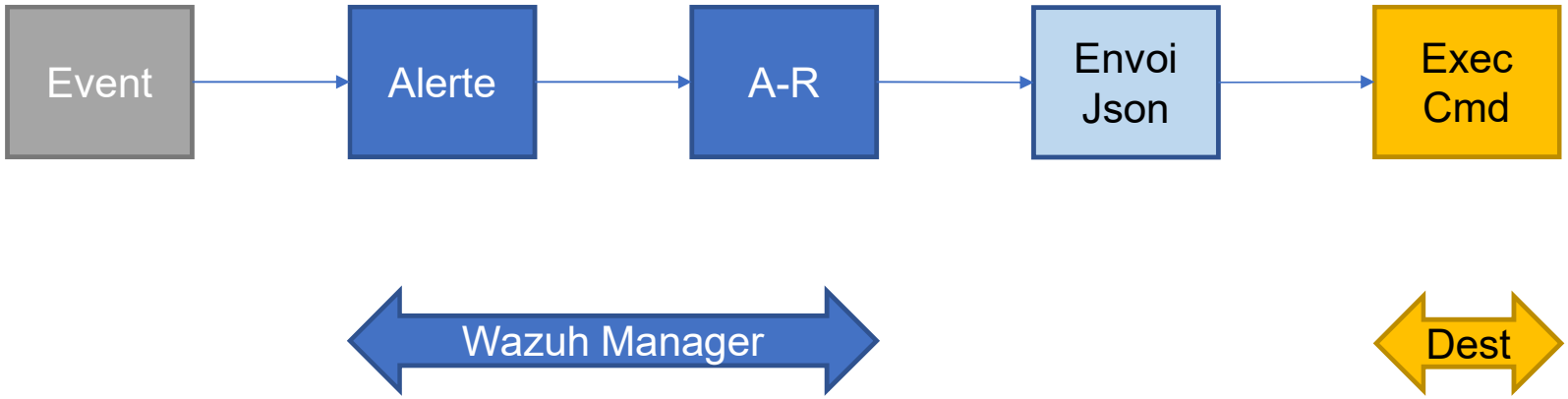
  - Conserver une trace des comportements

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

65

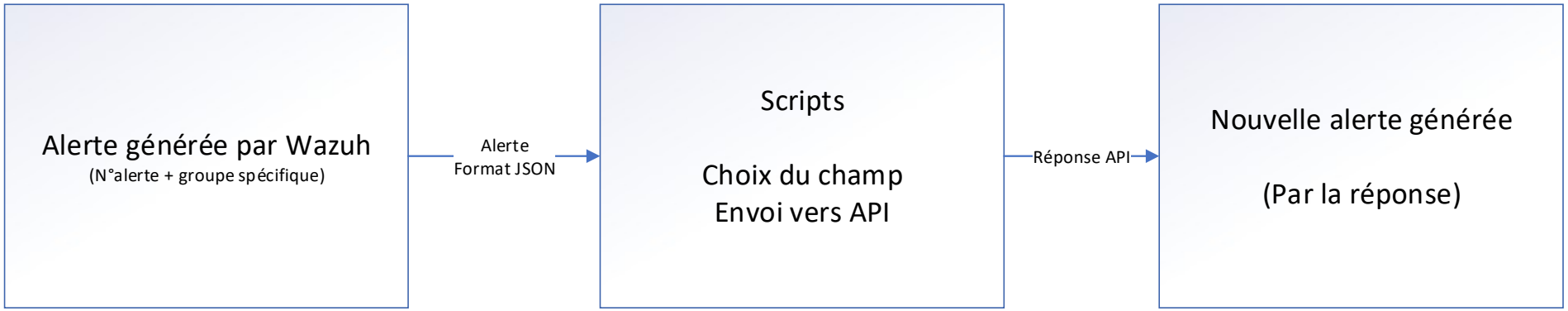
Integration

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



Sur le serveur Wazuh
/var/ossec/etc/ossec.conf :

```
<integration>
  <name>custom-opencti</name>
  <group>sysmon_eid1_detections</group>
  <rule_id>92031</rule_id>
  <alert_format>json</alert_format>
</integration>
```

Sur le serveur Wazuh
/var/ossec/integration :

custom-opencti (wrapper)
Custom-opencti.py (parsing)

Dans les règles :

```
<rule id="100625" level="12">
  <if_sid>100623</if_sid>
  <field name="opencti.id">\.+</field>
  <description>OpenCTI - IoC found in Threat Intel -
$(opencti.value)</description>
  <group>opencti,opencti_alert,</group>
  <options>alert_by_email</options>
</rule>
```

Integration : principe

- Intérêt

→ Transformer un signal faible en signal fort

→ Envoyer une alerte sur un autre outil (slack, des EDLs de parefeu…)

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