

FICHE 4 – SIEM WAZUH – CHASSE AUX MENACES

Liens officiels :

- <https://documentation.wazuh.com/current/user-manual/capabilities/vulnerability-detection/index.html>
- <https://wazuh.com/use-cases/threat-hunting/?highlight=MITRE%20ATT-CK>

SOMMAIRE

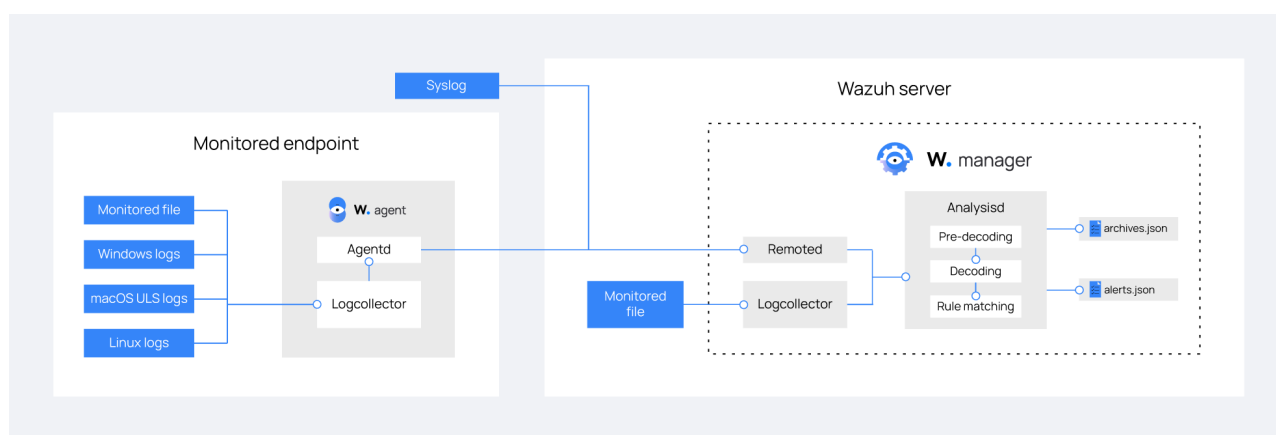
A. Analyse des données du journal.....	1
B. Archives de Wazuh.....	2
C. Détection des vulnérabilités.....	2
D. Cartographie MITRE ATT-CK.....	5

La chasse aux menaces est une **approche proactive** qui consiste à analyser de nombreuses sources de données telles que les journaux, le trafic de réseau et les données des points d'extrémité pour identifier et éliminer les cybermenaces qui ont échappé aux mesures de sécurité traditionnelles. Il vise à découvrir les **menaces potentielles** qui n'ont peut-être pas été détectées dans un environnement informatique. Le processus de chasse à la menace implique généralement plusieurs étapes : génération d'hypothèses, collecte de données, analyse et réponse.

Wazuh offre plusieurs fonctionnalités qui aident les équipes de sécurité à détecter les menaces dans leur environnement, en leur donnant les moyens de prendre des mesures rapides pour contenir la menace et prévenir d'autres dommages.

A. ANALYSE DES DONNÉES DU JOURNAL

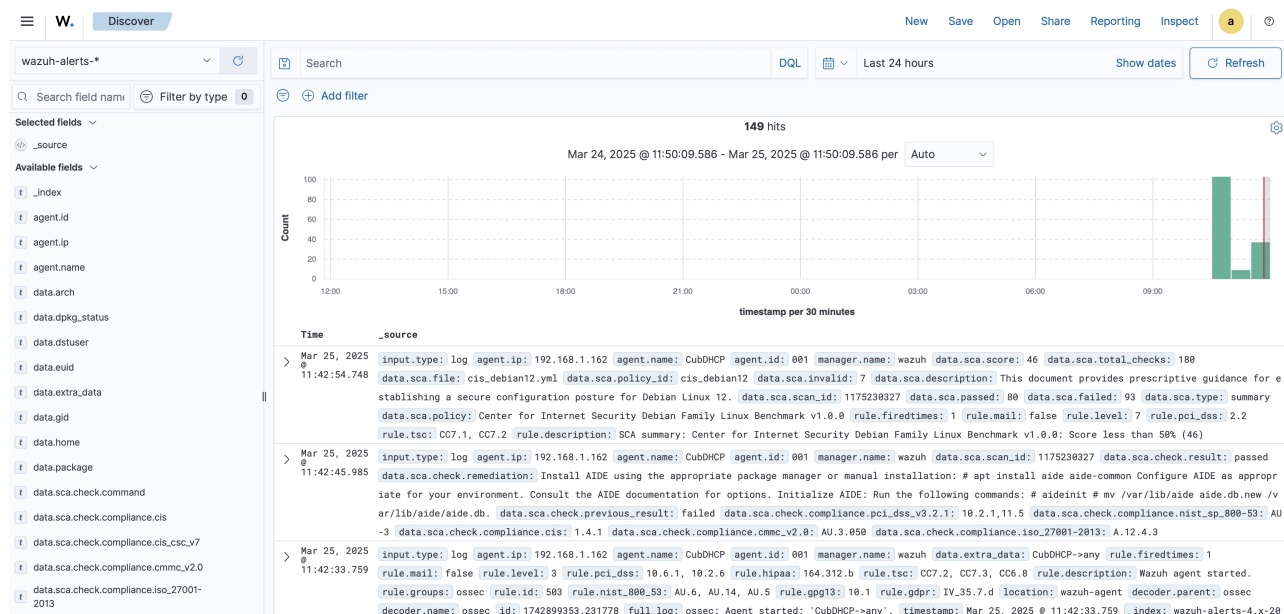
Wazuh en tant que plate-forme XDR et SIEM unifiée offre une collecte de données centralisées, permettant la collecte de données provenant de diverses sources telles que les points d'extrémité, les dispositifs de réseau et les applications. Cette approche centralisée simplifie l'analyse et réduit l'effort nécessaire pour surveiller plusieurs sources.



B. ARCHIVES DE WAZUH

Wazuh fournit un emplacement de stockage centralisé pour l'archivage de tous les journaux collectés à partir des critères d'évaluation surveillés. Les journaux d'archives Wazuh incluent ceux qui ne déclenchent pas d'alerte sur le tableau de bord de Wazuh (menu Explore / Discover).

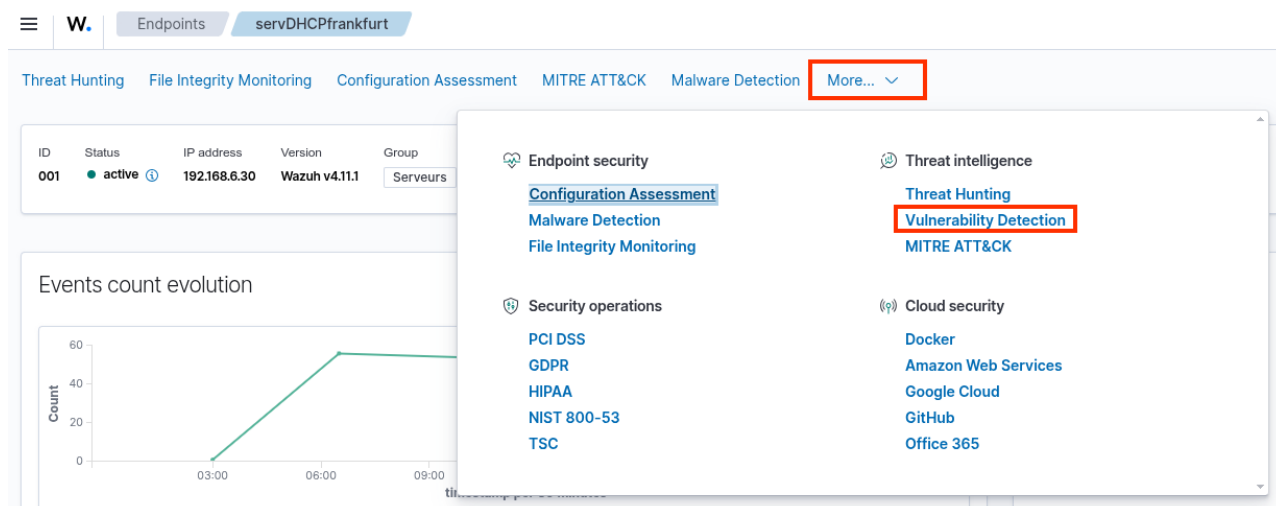
Wazuh stocke les journaux pendant de longues périodes, fournissant ainsi une piste d'audit complète des événements de sécurité. Ses fonctionnalités d'indexation et d'interrogation facilitent la recherche et l'identification rapides des problèmes potentiels et de la cause profonde des incidents de sécurité.



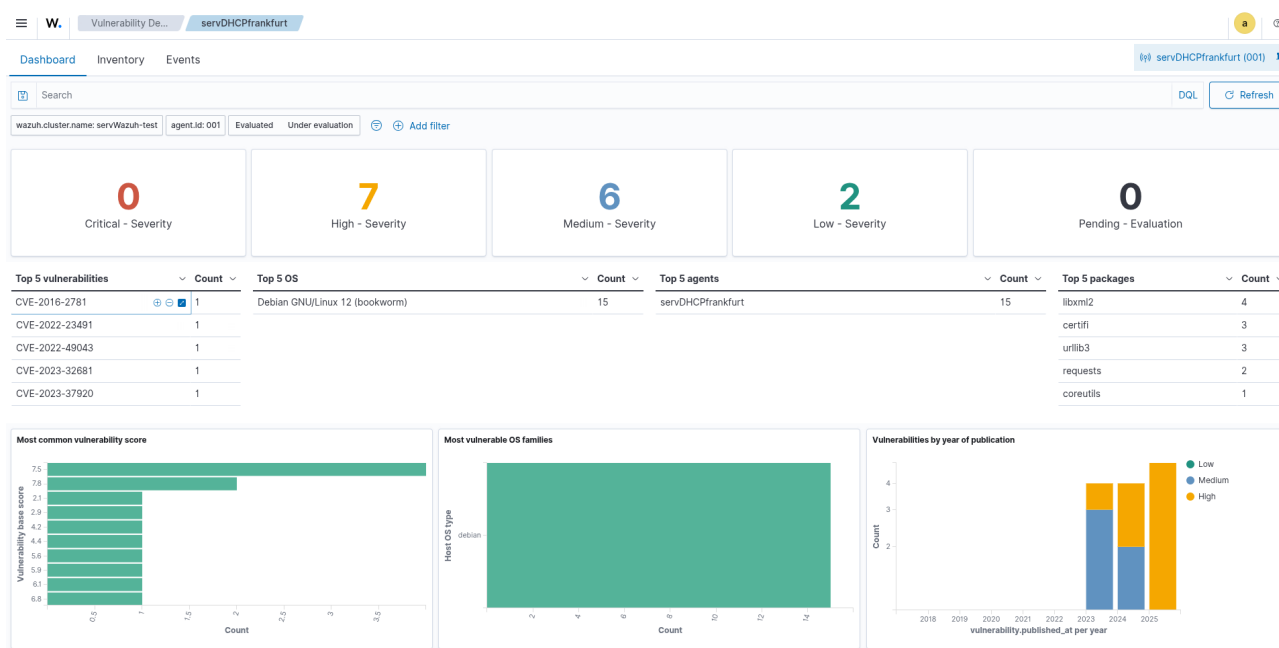
C. DÉTECTION DES VULNÉRABILITÉS

La Threat Intelligence (ou renseignement sur les menaces) correspond à l'ensemble des informations collectées, analysées et organisées, permettant à une organisation d'identifier, d'évaluer et d'anticiper des menaces informatiques potentielles.

Wazuh dispose d'un module « Vulnerability detection » qui permet d'identifier et de corriger proactivement les vulnérabilités, réduisant ainsi le risque de cyberattaque



L'interface utilisateur de Wazuh affiche toutes les vulnérabilités détectées.



Via le lien « Inventory », on obtient la liste des vulnérabilités avec les CVE associées :

agent.name	package.name	package.version	vulnerability.description	vulnerability.severity	vulnerability.id
servDHCPfrankfurt	certifi	2022.9.24	Certifi 2024.07.04 removes root certificate...	High	CVE-2024-39689
servDHCPfrankfurt	certifi	2022.9.24	Certifi 2023.07.22 removes root certificate...	High	CVE-2023-37920
servDHCPfrankfurt	idna	3.3	### Impact A specially crafted argument to...	High	CVE-2024-3651
servDHCPfrankfurt	libexpat1	2.5.0-1+deb12u1	A stack overflow vulnerability exists in the l...	High	CVE-2024-8176
servDHCPfrankfurt	libxml2	2.9.14+dfsg-1.3~deb12u1	libxml2 before 2.12.10 and 2.13.x before 2....	High	CVE-2025-24928
servDHCPfrankfurt	libxml2	2.9.14+dfsg-1.3~deb12u1	xmlXIncludeAddNode in xinclude.c in libxml...	High	CVE-2022-49043
servDHCPfrankfurt	libxml2	2.9.14+dfsg-1.3~deb12u1	libxml2 before 2.12.10 and 2.13.x before 2....	High	CVE-2024-56171

i Une CVE (Common Vulnerabilities and Exposures) est une liste publique de failles de sécurité informatique identifiées et cataloguées, permettant aux professionnels de prioriser et résoudre les vulnérabilités pour sécuriser les systèmes.

En cliquant sur la loupe, vous trouverez les détails de la CVE (description, score, etc.) ainsi que le ou les liens vers la source qui la référence et qui va potentiellement vous donner des indications pour corriger la vulnérabilité. **Il n'est ainsi pas nécessaire de sortir de l'application pour récupérer toutes les informations nécessaires.**

Vulnerability details

Table JSON

f _index	wazuh-states-vulnerabilities-servwazuh-test
f agent.id	001
f agent.name	servDHCPfrankfurt
f agent.type	Wazuh
f agent.version	v4.11.1
f host.os.full	Debian GNU/Linux 12 (bookworm)
f host.os.kernel	6.8.12-8-pve
f host.os.name	Debian GNU/Linux
f host.os.platform	debian
f host.os.type	debian
f host.os.version	12
f package.architecture	amd64
f package.description	GNOME XML library
f package.name	libxml2
# package.size	1,910,784
f package.type	deb
f package.version	2.9.14+dfsg-1.3~deb12u1
f vulnerability.category	Packages
f vulnerability.classification	CVSS
f vulnerability.description	libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a stack-based buffer overflow in xmlSprintfElements in valid.c. To exploit this, DTD validation must occur for an untrusted document or untrusted DTD. NOTE: this is similar to CVE-2017-9047.
📅 vulnerability.detected_at	Mar 21, 2025 @ 16:16:21.944
f vulnerability.enumeration	CVE
f vulnerability.id	CVE-2025-24928
📅 vulnerability.published_at	Feb 19, 2025 @ 00:15:10.000
f vulnerability.reference	https://security-tracker.debian.org/tracker/CVE-2025-24928
f vulnerability.scanner.source	Debian Security Tracker
f vulnerability.scanner.vendor	Wazuh
# vulnerability.score.base	7.8
f vulnerability.score.version	3.1
f vulnerability.severity	High
🔍 vulnerability.under_evaluation	false
f wazuh.cluster.name	servWazuh-test
f wazuh.schema.version	1.0.0

En suivant le lien, on voit que la vulnérabilité ne bénéficie d'aucun « fix » pour l'instant sur Debian 12 (bookworm)

CVE-2025-24928



Name	CVE-2025-24928
Description	libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a stack-based buffer overflow in xmlSprintfElements in valid.c. To exploit this, DTD validation must occur for an untrusted document or untrusted DTD. NOTE: this is similar to CVE-2017-9047.
Source	CVE (at NVD ; CERT , LWN , oss-sec , fulldisc , Red Hat , Ubuntu , Gentoo , SUSE bugzilla/CVE , GitHub advisories/code/issues , web search , more)
References	DLA-4064-1
Debian Bugs	1098321

Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
libxml2 (PTS)	bullseye	2.9.10+dfsg-6.7+deb11u4	vulnerable
	bullseye (security)	2.9.10+dfsg-6.7+deb11u6	fixed
	bookworm	2.9.14+dfsg-1.3~deb12u1	vulnerable
	trixie	2.12.7+dfsg+really2.9.14-0.2	vulnerable
	sid	2.12.7+dfsg+really2.9.14-0.3	vulnerable

The information below is based on the following data on fixed versions.

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
libxml2	source	bullseye	2.9.10+dfsg-6.7+deb11u6		DLA-4064-1	
libxml2	source	(unstable)	(unfixed)			1098321

Notes

<https://gitlab.gnome.org/GNOME/libxml2/-/issues/847>

<https://www.openwall.com/lists/oss-security/2025/02/18/2>

Fixed by: <https://gitlab.gnome.org/GNOME/libxml2/-/commit/8c8753ad5280ee13aee5eec9b0f6eee2ed920f57>

Fixed by: <https://gitlab.gnome.org/GNOME/libxml2/-/commit/858ca26c0689161a6b903a6682cc8a1cc10a0ea8> (v2.12.10)

D. CARTOGRAPHIE MITRE ATT&CK

Le cadre MITRE ATT&CK offre une approche normalisée pour cartographier et comprendre les tactiques, les techniques et les procédures de cyberattaques. En utilisant le module Wazuh MITRE ATT&CK, nous pouvons améliorer notre compréhension des techniques d'attaques utilisées par les acteurs de la menace et nous défendre de manière proactive contre eux.

Le module Wazuh MITRE ATT&CK cartographie les techniques d'attaques liées aux événements générés, facilitant la chasse aux menaces efficaces en identifiant rapidement les modèles de comportement des attaquants.