ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ WAZUH»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Вдовиченко М.С.
(прізвище та ініціали)
Керівник Марченко В.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____ 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ
СТУДЕНТУ

Вдовиченку Максиму Сергійовичу
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технологія управління захистом кінцевих точок організації на базі рішення Wazuh»

керівник магістерської роботи Марченко Віталій Вікторович, старший викладач
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «12» жовтня 2022 року №122.

2. Строк подання студентом магістерської роботи 15.12.2022 р.

3. Вихідні дані до магістерської роботи
інформаційна система організації;
програмні комплекси управління захистом кінцевих точок;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми захисту кінцевих точок корпоративних інформаційних систем.
2. Склад та умови функціонування інформаційної системи.
3. Методи та засоби управління захистом кінцевих точок.
4. Варіант системи управління захистом кінцевих точок інформаційної системи організації.
5. Перелік графічного матеріалу

1. Тема магістерської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу складу та умов функціонування інформаційної системи організації.

4. Результати аналізу методів та засобів захисту кінцевих точок.

5. Призначення та можливості рішення Wazuh.

6. Варіант застосування системи управління захистом кінцевих точок інформаційної системи організації.

7. Рекомендації щодо застосування технології управління захистом кінцевих точок корпоративної інформаційної системи. Wazuh.

8. Висновки за результатами роботи.

6. Дата видачі завдання 26.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захисту кінцевих точок корпоративних інформаційних систем.	26.09.2022 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	….. 2022 р.	
3.	Аналіз методів та засобів захисту кінцевих точок.	….. 2022 р.	
4.	Розроблення варіант системи управління захистом кінцевих точок інформаційної системи організації.	…..2022 р.	
5.	Розроблення рекомендацій щодо застосування технології управління захистом кінцевих точок інформаційної системи організації.	…..2022 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	……2022 р.	
7.	Підготовка доповіді до захисту.	15.12.2022 р.	

Студент Вдовиченко М.С
(підпис) прізвище та ініціали

Керівник магістерської роботи Марченко В.В.
(підпис) прізвище та ініціали

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Вдовиченко М.С. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія управління захистом кінцевих точок інформаційної системи організації на базі рішення Wazuh».

Магістерська робота і рецензія додаються.

Директор інституту _____ _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Вдовиченко М.С. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2021 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту _____ Бреславська Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент ***Вдовиченко М.С.*** обрав тему роботи, метою якої було дослідити зміст технології управління захистом кінцевих точок інформаційної системи організації на базі рішення Wazuh та розробити варіант системи управління їх захистом. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Вдовиченко М.С. показав відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.
Все це дозволяє оцінити виконану магістерську роботу студента Вдовиченка Максима Сергійовича на оцінку **«відмінно»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник магістерської роботи _____ Марченко В.В.
(підпис) (прізвище та ініціали)
“____” _____ 2022 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Вдовиченко М.С.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи: 67 сторінок, 34 рисунків, 10 таблиць, 15 джерел.

Об'єкт дослідження – процес забезпечення захисту кінцевих точок організації.

Предмет дослідження – технологія управління захистом кінцевих точок організації.

Мета роботи – розробити варіант системи управління захистом кінцевих точок корпоративної інформаційної системи та рекомендації щодо застосування технології їх захисту в організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління захистом кінцевих точок організації.

В роботі проведено аналіз проблеми забезпечення кібербезпеки інформаційної системи організації та визначено мета та завдання управління захистом кінцевих точок організації. Проаналізовано існуючі технології управління захистом кінцевих точок корпоративної інформаційної системи.

Досліджено методи та засоби управління захистом кінцевих точок на прикладі рішення Wazuh. Визначено призначення, основні функції та склад програмного комплексу Wazuh.

На основі досліджень проведених в роботі розроблено варіант побудови та розгортання системи управління захистом кінцевих точок організації та рекомендації щодо застосування технології управління їх захистом в організації.

Галузь використання – кібербезпека інформаційної системи організації.

ІНФОРМАЦІЙНА СИСТЕМА ОРГАНІЗАЦІЇ, КІБЕРБЕЗПЕКА, ЗАХИСТ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК, ТЕХНОЛОГІЯ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК

ABSTRACT

Master's thesis: 67 pages, 34 figures, 10 tables, 15 sources.

Object of research – the process of ensuring the protection of endpoints of the information system of organization.

Subject of research – the technology for managing the protection of endpoints of the information system of organizaton.

The aim of research – to develop a variant of the system for managing the endpoints of the corporate information system and recommendations on how to promote the technology of their protection in the organization.

Research methods – reference to the literature on this topic, analysis of operational documentation, international standards and their alignment, modeling the process of managing the end points of the organization

The paper analyzes the problem of cybersecurity of the information system of the organization was carried out and the meta and task of managing the end points of the organization was determined. The main technologies for managing the endpoints of the corporate information system are analyzed.

The method of managing the end points on the butt of the Wazuh solution has been completed. Recognition, main functions and storage of the Wazuh software package were recognized.

On the basis of the research carried out in the robot, a variant of prompting the development of the system for managing the endpoints of the organization and recommendations for stosuvannya technology for managing the infection in the organization.

Field of use – cybersecurity of information system of organizaton.

CORPORATE INFORMATION SYSTEM, CYBER SECURITY, ENDPOINT PROTECTION, METHODS AND MEANS OF MANAGEMENT OF ENDPOINT PROTECTION FOR TECHNICS

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента Вдовиченка Максима Сергійовича

на тему: «Технологія управління захистом кінцевих точок організації на базі рішення Wazuh

Актуальність:
Управління активами корпоративної інформаційної системи стає все більш складним у зв'язку зі зростаючим числом кінцевих точок та застосовуваних інформаційних технологій. Захист та реагування кінцевих точок (Endpoint Detection and Response, EDR) є комплексним підходом для управління пристроями кінцевих точок в організації з єдиної консолі. Реалізація технології EDR в управлінні кінцевими точками створює умови забезпечення багатьох сучасних функцій захисту. Тому тема магістерської роботи є актуальною та своєчасною.

Позитивні сторони:
1. На основі проведеного аналізу, в роботі встановлено зміст проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи від новітніх загроз, визначено мета та завдання управління захистом кінцевих точок корпоративної інформаційної системи.
2. Досліджено методи та засоби управління захистом кінцевих точок корпоративної інформаційної системи на базі рішення Wazuh.
3. Запропоновано варіант технології застосування системи управління захистом кінцевих точок корпоративної інформаційної системи на базі рішення Wazuh та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:
1. У магістерській роботі бажано було б провести порівняльний аналіз рішень UEM корпоративної інформаційної системи різних виробників.
2. Запропонований системи управління захистом кінцевих точок корпоративної інформаційної системи на базі рішення Wazuh доцільно було б показати на прикладі конкретної організації.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку «**відмінно»**, а студент **Вдовиченко Максим Сергійович** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека..

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ…….. 9

ВСТУП ……..……. 10

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ…… 11

1.1. Призначення, структура, функції та умови функціонування корпоративної інформаційної системи……. 11
1.2. Аналіз проблем традиційної моделі забезпечення захисту кінцевих точок корпоративної інформаційної системи…….…. 14
1.3. Основні функціональні можливості системи захисту кінцевих точок……..…… 20
1.4. Аналіз існуючих технологій захисту кінцевих точок корпоративної інформаційної системи……. 24

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК НА БАЗІ WAZUH…… 32

2.1. Призначення, можливості та функції Wazuh ……. 32
2.2. Компоненти та архітектура Wazuh ……..……... 37
2.3. Вимоги до системи та інсталяція Wazuh…….…… 42
2.4. Можливості щодо управління Wazuh ……. 50

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ СИСТЕМИ WAZUH……. 56

3.1. Розгортання та конфігурація системи управління захистом кінцевих точок корпоративної інформаційної системи на базі Wazuh ……..... 56
3.2. Технологія управління захистом кінцевих точок з Wazuh…….. 65
3.3. Розроблення рекомендацій щодо застосування технології управління захистом кінцевих точок корпоративної інформаційної системи……..……..... 73

ВИСНОВКИ……. 75

ПЕРЕЛІК ПОСИЛАНЬ..... 76

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)..... 78

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ — Інформаційна Безпека;

ІС — Інформаційна система;

КС — Комп’ютерна система;

НСД — Несанкціонований доступ;

ПЗ — Програмне забезпечення;

EPP — Endpoint protection platform;

EDR — Endpoint detection and response;

MDR — Managed detection and response;

XDR — Extended detection and response;

FIM — File integrity monitoring;

SCA — Security configuration assesment;

MSP — Monitoring security policies;

MSC — Monitoring system calls;

SCAP — Security Content Automation Protocol;

IP — Internet Protocol;

CIS — Center for Internet Security;

CM — Command Monitoring;

DDOS — Distributed Denial of Service;

AR — Active Response;

ОС — Операційна Система;

DNS — Domain Name System;

SI — System Inventory;

HTTP — HyperText Transfer Protocol;

AM — Agentless Monitoring;

CVE — Common Vulnerabilities and Exposures;

ВСТУП

Захист підприємства, можливо, ніколи не було простим завданням, але зараз воно стало набагато складнішим, оскільки хакери стали більш креативними, а саме підприємство поширилося на віддалені місця та аж до «хмари».

З новими загрозами, зростаючим споживанням IT, кишеньковими інтелектуальними пристроями та флеш-накопичувачами на розміром з палець, безпеки в чотирьох стінах підприємства вже недостатньо. Постійне розширення кінцевих точок і зростаюча кількість і складність загроз вимагають постійного перегляду та оновлення рішень захисту кінцевих точок .

Платформа захисту кінцевої точки є важливою частиною кібербезпеки підприємства з кількох причин. Перш за все, у сучасному діловому світі, дані є найціннішим активом компанії і втрата цих даних або доступу до них може поставити весь бізнес під загрозу банкрутства. Підприємствам також доводиться стикатися не лише із зростанням кількості кінцевих точок, а і зі збільшенням їх типів та різновидів. Ці фактори самі по собі ускладнюють безпеку кінцевої точки підприємства, але додатково ускладнюються політиками віддаленої роботи та BYOD, які роблять безпеку периметра недостатньою та створюють уразливості.

Ландшафт загроз також ускладнюється: хакери завжди винаходять нові способи отримати доступ, викрасти інформацію або змусити співробітників надати конфіденційну інформацію.

У цій роботі ми розглядаємо обширний та багатофункціональний механізм захисту кінцевих точок, в результаті використання якого, будуть розроблені рекомендації по управлінням захистом кінцевих точок організації, що в свою чергу має за ціль підвищення рівня організації інформаційної безпеки підприємств.

Основною метою магістерської роботи є розробка рекомендації щодо застосування системи управління безпеки кінцевих точок розгортання технології у власному віртуальному середовищі.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

1.1. Роль, структура та функціональне призначення інформаційної системи

В наш час, де б ми не були, нас оточують інформаційно-телекомунікаційні системи. Для того щоб розглядати питання тісно пов’язані з нею, необхідно зрозуміти що вона собою являє. Її визначення можна знайти у тексті закону №81/94 Верховної Ради України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994.

Інформаційно-телекомунікаційна система – це сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле. Як сказано у визначенні, вона складається з двох ключових складових: це інформаційна система та телекомунікаційна система.

Спочатку визначимо функціональне призначення інформаційних систем. У найширшому розумінні інформаційні системи призначені для своєчасної доставки та задоволення інформаційних потреб користувачів. Наприклад, у діяльності корпорацій існує практика створення та функціонування єдиної корпоративної інформаційної системи, яка задовольняє інформаційні потреби всіх співробітників, служб, підрозділів організацій. Однак на практиці створення комплексної інформаційної системи є складним, а часом навіть нездійсненним завданням, тому на підприємствах зазвичай функціонує декілька різних систем, які вирішують окремі групи завдань: управління виробництвом, фінансово-господарською діяльністю, електронний документообіг тощо.

У зв’язку з тим, що задоволення інформаційних потреб відбувається шляхом реалізації певних інформаційних процесів, вважаємо, що основним функціональним призначенням інформаційних систем є забезпечення інформаційних процесів, зокрема створення, поширення, використання, зберігання та знищення (використання) інформації. Такий підхід до визначення

функціонального призначення інформаційних систем забезпечує інваріантність до типів інформації та інформаційних ресурсів, а також типів і видів інформаційних технологій, що використовуються для реалізації інформаційних процесів. Таким чином, стає можливим віднести інформаційні системи: видавництва, бібліотеки, архіви, ЗМІ, телекомунікації, Інтернет тощо.

За суттю інформаційна система є цілісною системою і цілком очевидно вона має всі властивості системи такого роду:

- залежно від виду і конкретного призначення інформаційна система має якості, які не можуть бути зведені до властивостей елементів, що її утворюють;
- якісні характеристики конкретної інформаційної системи залежать від якісних характеристик її елементів;
- між елементами інформаційної системи існує зв'язок, причому, коли відбувається зміна одного компонента системи, то це призводить до зміни іншого, а іноді і системи в цілому;
- інформаційну систему як цілісне утворення характеризує впорядкованість елементів, які її утворюють, а також зв'язків і відношень між ними;
- інформаційна система не існує ізольовано, ця властивість проявляється у взаємозв'язку системи з іншими системами.

Враховуючи вищесказане, можна погодитися з наступним визначенням терміна «інформаційна система» - це організований комплекс організаційно-технічних заходів (сукупність підприємств, підрозділів та спеціалістів), а також інформаційні технології та інформаційні ресурси, призначені для функціонування інформаційних процесів. розповсюдження, використання, систематизація, зберігання та знищення інформації [1].

У загальному розумінні, інформаційна система – сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів. Тобто, її завданням є здійснення пошуку, збирання, зберігання, передавання й опрацювання інформації.

Зазвичай, їх класифікують за наступними ознаками:

- Ступінь автоматизації

- Сфера призначення
- Місце діяльності
- Функціональне призначення
- Інформація що оброблюється

В свою чергу телекомунікаційна система – це комплекс програмного та апаратного обладнання, який з'єднаний один із одним в ланцюг, що здійснює передачу даних з однієї точки в іншу. Найбільш поширені такі види класифікації:

- Географічне розташування
- Структура взаємозв'язків (топологією)
- Режим комунікації
- Швидкість мережі

Прикладами такої системи може слугувати: комп'ютерна мережа, мережа INTERNET, телефонна мережа і т.д.

З розвитком інформаційних технологій, проблема несанкціонованого доступу до інформації набула велику важливість. Для збереження інформації використовуються сукупності методів і засобів що забезпечують її цілісність, конфіденційність і доступність, тобто захист інформації.

- Цілісність – це неможливість модифікації інформації неавторизованим користувачем.
- Конфіденційність – стан коли інформація не може бути отримана неавторизованим користувачем.
- Доступність – полягає в тому, що авторизований користувач може використовувати інформації відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого інтервалу часу.

Відповідно до властивостей інформації, виділяють такі загрози її безпеці:

загрози цілісності:

- знищення;
- модифікація;

загрози доступності:

- блокування;
- знищення;

загрози конфіденційності:

- несанкціонований доступ (НСД);
- витік;
- розголошення.

Кожен вид ЗІ забезпечує окремі аспекти ІБ:

Технічний — забезпечує обмеження доступу до носія повідомлення апаратно-технічними засобами (антивіруси, фаєрволи, маршрутизатори, токіни, смарт-карти тощо):

- попередження витоку по технічним каналам;
- попередження блокування ;

Інженерний — попереджує руйнування носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами:

- забезпечення фізичної стійкості носія інформації;
- забезпечення охоронно-пожежної сигналізації;
- використання обмежуючих конструкцій.

Криптографічний — попереджує доступ за допомогою математичних перетворень повідомлення:

- попередження несанкціонованої модифікації ;
- попередження несанкціонованого розголошення.

Організаційний — попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів.

- використання правил розмежування доступу;
- система відеонагляду.

1.2. Аналіз проблем традиційної моделі забезпечення захисту кінцевих точок корпоративної інформаційної системи

В будь-якій корпоративній інформаційно-телекомунікаційній системі є такий вид пристроїв, як кінцева точка або точка входу пристроїв кінцевих користувачів.

Кінцева точка – це віддалений обчислювальний пристрій, який взаємодіє з мережею, до якої він підключений. Це можуть бути такі пристрої як:

- Персональні комп’ютери;
- Ноутбуки;
- Смартфони;
- Планшети;
- Сервери;
- Системи торгових точкок(POS);
- Пристрої інтернету речей (IoT).

Кінцеві точки є ключовими вразливими точками входу для кіберзлочинців. Це саме ті місця, де зловмисники виконують код і використовують уразливості, шифрують, викрадають або експлуатують активи. Оскільки співробітники організації стають більш мобільними, підключаються до внутрішніх ресурсів із зовнішніх кінцевих точок у всьому світі, кінцеві точки стають дедалі більш сприйнятливими до атак.

Ми всі чули про «традиційний антивірус» або «захист кінцевої точки» які базуються на тому що ми вже знаємо. Файли, які містять зловмисне програмне забезпечення, заносяться в чорний список за допомогою підпису, щоб файл можна було розпізнати. Щойно новий файл знайдено, його можна розпізнати та заблокувати за допомогою сканування. Ці рішення повністю залежать від аналізу загроз виробника та регулярності оновлення сигнатурних та інших баз конкретного рішення. Оскільки щодня поширюється більше мільйона нових вірусів, зловмисного програмного забезпечення нульового дня, вкрай важко залишатися в курсі подій.

ІТ-ландшафт продовжує швидко змінюватися, як і відповідні заходи безпеки. 2016 рік був роком фішингу, зловмисного програмного забезпечення, шпигунського програмного забезпечення та нульових днів, але, зокрема, це був рік експлойтів і програм-вимагачів. Це також залишалося серйозною проблемою в

2017 році з поширенням програм - вимагачів WannaCry і PETYA . Багато виробників засобів безпеки мають проблеми з виявленням і блокуванням цих загроз до тих пір, поки не буде розпізнано визначення вірусу та не буде доступний сигнатурний запис.

Нові загрози надходять через експлойти. Експлойти використовують оновлений кіберланцюг ліквідації або кібер кіллчейн (Cyber kill chain), порівняно з традиційним шкідливим програмним забезпеченням. Цей новий ланцюг успішний, тому що він набагато складніший. І знову кінцева точка є фокусною точкою. Ми маємо справу з пристроями, які не підключені до мережі, отже не мають оптимального захисту за брандмауером або шлюзом. Ми бачимо, що завдяки новим технологіям, які використовують хакери, і більшій кількості кроків, які вони роблять, безпека кінцевої точки стає все більш важливою. Цей ланцюг виглядає наступним чином:

Рис. 1.1 Кібер кіллчейн

- Дослідження

На етапі дослідження ціль хакера всебічно досліджується, наприклад, шляхом перевірки соціальних мереж. Це також називають «соціальною інженерією». Оскільки майже всі користуються соціальними мережами, це також є чудовим засобом отримання інформації для хакерів.

- Фішинг

Після того, як мета була досліджена, розробляється фішингова кампанія. Це надсилається окремій особі, організації чи навіть сектору. Усе частіше хакери використовують spear fishing (гарпуновий фішинг), коли електронна пошта повністю адаптована до цілі. Це значно підвищує шанси на успіх.

- Переадресація

У фішинговому електронному листі ціль спонукають натиснути посилання. Клієнт часто потрапляє на сторінку хакера через те, що за легітимним веб-сайтом відкриваються інші веб-сайти але вони ретельно замасковані і їх не видно.

- Експлойт-набір

Зі свого веб-сайту хакер запускає сканування за допомогою набору експлойтів. Це сканування визначає слабкі сторони системи цілі. Це може бути стара версія Java, Adobe або Office.

- Файл-дропер

Щоб проникнути в цільову систему, хакер використовує її слабкі місця. Він робить це, надсилаючи файл дроппера. Оскільки файл дроппера надсилається в систему через SSL-з’єднання, такі речі, як брандмауери, не можуть його перехопити.

- Дзвінок додому

Файл дроппера повертається до сервера хакера, який також називають сервером команд і керування. Таким чином хакер дізнається, що його злом пройшов успішно, і тепер він може заволодіти системою за допомогою сценаріїв. При цьому використовується багато технологій, які надають доступ до пам'яті або root-права, наприклад. Оскільки це робиться через законну програму, вона не розпізнається. Деякі з цих технологій: Heap spray, SEHOP, Stack Pivot і DLL Hijacking.

- Крадіжка даних

Останнім кроком є етап, на якому хакер досягає своєї мети. Ця мета може полягати в крадіжці даних, активації програм-вимагачів або реєстрації всіх дій у системі, таким чином функціонуючи як шпигунські програми.

Думки різних фахівців збігаються в тому, що однією з найбільших проблем традиційної моделі забезпечення захисту кінцевих точок, з якою стикаються сучасні організації, є пристрій, що належить співробітникам. Традиційно організації створювали правила Bring Your Own Device (BYOD), які регулювали, як працівники можуть використовувати або не використовувати свої особисті

пристрої для роботи. Однак, саме попри віддалену роботу та розширене підключення, ці традиційні політики більше не є стійкими. Розуміння деяких ключових проблем, які викликають пристрої працівників може допомогти організаціям зменшити пов’язані з ними ризики.

Коли співробітники використовують власні пристрої, організації втрачають контроль над тим, як співробітники взаємодіють з їхніми хмарними ресурсами. Наприклад, працівник може використовувати свій пристрій для завантаження конфіденційних документів із хмарної програми. Без розширеного захисту кінцевої точки, організація не знатиме, що станеться з цією інформацією, і це проблема.

Коли організації не можуть контролювати та відстежувати потік конфіденційних даних, вони створюють нові ризики. Наприклад, якщо на пристрої працівника є шпигунське програмне забезпечення, документ може бути перехоплено, що призведе до витоку даних. Крім того, якщо організація не приділяє пильної уваги способам спільного використання цього документа, працівник може випадково передати дані або використати їх іншим неналежним чином.

Після пандемії COVID-19, дистанційна робота, ймовірно, залишиться, незважаючи на загрозу безпеці. Насправді 80 відсотків керівників планують дозволити співробітникам працювати віддалено, принаймні час від часу. Аргументація проста: працівникам це подобається, і це може заощадити гроші організації. Однак, з точки зору безпеки кінцевої точки, це пов’язано з кількома ризиками.

Незалежно від того, чи працюють співробітники вдома чи з будь-якого іншого місця, їхні пристрої, ймовірно, підключаються до загальнодоступних і персональних бездротових мереж, у яких відсутні надійні засоби контролю безпеки корпоративної мережі. Це означає, що суб’єктам загрози просто потрібно вдатися до атаки «людина посередині (MiTM)», щоб викрасти дані або облікові дані. Без захисту кінцевої точки поїздка працівника до місцевого кафе може призвести до величезних грошових втрат.

Незважаючи на те чи хочуть організації дозволити працівникам використовувати мобільні пристрої чи ні, вони залишаться. Зловмисники розумно підійшли до цього, оскільки зараз існує широкий вибір шкідливого програмного забезпечення, розробленого для будь-якого мобільного пристрою, який тільки можна уявити. На жаль, багато рішень безпеки і, в особливості, класичні політики захисту мережі не враховують цей підвищений ризик.

Оскільки багато співробітників щодня використовують свої мобільні пристрої , вони піддаються більшому ризику зараження своїх пристроїв шкідливим програмним забезпеченням. Якщо інфікований пристрій підключається до ресурсу в мережі організації, зловмисник матиме вільний шлях для отримання несанкціонованого доступу до конфіденційних даних і ресурсів. Звідти вони можуть почати сіяти хаос за допомогою більш складних атак, таких як програми-вимагачі.

Організації за своєю суттю мало контролюють додатки на персональних пристроях співробітників. На жаль, програми сторонніх розробників є вектором масової атаки. Наприклад, було виявлено, що велика кількість програм для мобільних ліхтариків містить зловмисне програмне забезпечення, а безкоштовне програмне забезпечення, завантажене на персональний ноутбук працівника, може містити безліч шкідливих програм.

Навіть якщо організація може контролювати, що співробітники встановлюють на особистих пристроях, програми можуть мати ризики, які організація не зможе зменшити. Наприклад, для нової вразливості програми може знадобитися оновлення системи безпеки. Якщо організація не може контролювати пристрій, неможливо переконатися, що користувач встановив оновлення.

Видимість ризиків є основною проблемою безпеки кінцевих точок, з якою стикаються організації. Кожна кінцева точка діє як новий вектор атаки, особливо при віддаленому підключенні до мережі. Щоб зменшити ризики, організаціям необхідно знати, де знаходиться кожна кінцева точка, а для цього необхідна повна видимість усього, що підключається до корпоративної мережі. Без видимості та контролю над усіма кінцевими точками організаційний ризик зростає.

Ландшафт кінцевих точок постійно змінюється і підприємства будь-якого розміру є привабливими цілями для кібератак. Це загальновідомо навіть серед малого бізнесу. Згідно з дослідженням проведеним Connectwise у 2020 році, 77% із 700 опитаних керівників малого та середнього бізнесу стурбовані тим, що вони стануть об’єктом атаки в найближчі шість місяців.

1.3. Основні функціональні можливості системи захисту кінцевих точок

Рішення для захисту кінцевої точки має, перш за все, пропонувати комплексний захист для кінцевої точки та корпоративної мережі. Деякі важливі функції рішення безпеки кінцевої точки включають наступне:

- Захист від зловмисного програмного забезпечення:

Рішення для захисту кінцевих точок повинні виявляти та запобігати зараженню вірусами, хробаками та іншим шкідливим програмним забезпеченням.

- Аналітика поведінки:

Програмне забезпечення – вимагач та інші варіанти зловмисного програмного забезпечення мають унікальну поведінку, завдяки якій їх можна виявити без використання підписів. Відстежуючи цю поведінку, рішення для захисту кінцевих точок можуть виявляти атаки нульового дня та реагувати на них.

- Відповідність вимогам:

Здатність забезпечити відповідність корпоративним політикам безпеки стає все більш важливою з ростом віддаленої роботи та BYOD. Рішення для кінцевих точок повинні оцінювати пристрої та дозволяти підключення до корпоративної мережі, лише якщо вони відповідають корпоративній політиці.

- Шифрування даних:

Шифрування є найефективнішим способом захисту даних від несанкціонованого доступу та можливого злому. Рішення безпеки кінцевих точок повинні пропонувати повне шифрування диска – full disk encryption і підтримувати шифрування змінних носіїв.

- Брандмауер і контроль додатків:

Сегментація мережі є важливою для управління доступом і ризиком кібербезпеки. Функції брандмауера та контролю за додатками дозволяють сегментувати мережу та блокувати трафік на основі політики безпеки та правил для окремих програм.

- Перевірка пісочниці:

Кінцеві точки можуть бути заражені зловмисним програмним забезпеченням різними способами, такими як фішинг, використання вразливості тощо. Рішення безпеки кінцевих точок повинні видобувати та перевіряти файли в ізольованому середовищі, щоб ідентифікувати та заблокувати шкідливий вміст у кінцевій точці.

- Безпечний віддалений доступ:

Безпечний віддалений доступ необхідний для співробітників, які працюють за дистанційною або гібридною моделлю. Рішення безпеки кінцевої точки повинні включати клієнт віртуальної приватної мережі (VPN) або інше безпечне рішення віддаленого доступу.

- Фільтрування URL-адрес:

Шкідливі посилання є поширеною технікою під час фішингових атак, а неналежне використання веб-сторінок на корпоративних пристроях знижує продуктивність і ставить компанію під загрозу. Фільтрування URL-адрес допомагає запобігти цим загрозам, блокуючи шкідливі та неприйнятні веб-сайти.

Інструменти безпеки кінцевих точок, які забезпечують безперервне запобігання порушенням, повинні інтегрувати такі фундаментальні елементи:

1. Профілактика: NGAV;

Традиційні антивірусні рішення виявляють менше половини всіх атак. Вони функціонують шляхом порівняння зловмисних сигнатур або фрагментів коду з базою даних, яка оновлюється учасниками щоразу, коли виявляється нова зловмисна сигнатура. Проблема полягає в тому, що зловмисне програмне забезпечення , яке ще не ідентифіковано, або невідоме зловмисне програмне забезпечення не міститься в базі даних. Існує проміжок між часом, коли зловмисне

програмне забезпечення виходить у світ, і часом, коли його можна ідентифікувати традиційними антивірусними рішеннями.

Антивірус наступного покоління усуває цю прогалину, використовуючи вдосконалені технології захисту кінцевих точок , такі як штучний інтелект і машинне навчання, щоб ідентифікувати нове зловмисне програмне забезпечення, досліджуючи більше елементів, таких як хеші файлів, URL-адреси та IP-адреси.

2. Виявлення: EDR;

Профілактики недостатньо. Жоден захист не є досконалим, і деякі атаки завжди зможуть пройти через захист і успішно проникнути в мережу. Звичайна система безпеки не може побачити, коли це відбувається, залишаючи зловмисникам вільні перебувати в середовищі протягом днів, тижнів або місяців. Компанії повинні зупинити ці «тихі збої», швидко знайшовши та усунувши зловмисників.

Щоб запобігти тихим збоям, рішення Endpoint Detection and Response (EDR) має забезпечувати постійну та повну видимість того, що відбувається на кінцевих точках у режимі реального часу. Підприємствам слід шукати рішення, які пропонують розширені можливості виявлення загроз, розслідування та реагування, включаючи пошук і розслідування даних інцидентів, сортування попереджень, перевірку підозрілих дій, полювання на загрози, виявлення та стримування зловмисної активності.

3. Керований пошук загроз;

Не всі атаки можна виявити лише за допомогою автоматизації. Для виявлення сучасних складних атак необхідний досвід фахівців із безпеки.

Кероване полювання на загрози здійснюється елітними командами, які навчаються на інцидентах, які вже відбулися, збирають краудсорсингові дані та надають вказівки щодо найкращих дій у разі виявлення зловмисної активності.

4. Інтеграція аналізу загроз;

Щоб випередити зловмисників, компаніям потрібно розуміти загрози в міру їх розвитку. Складні противники та вдосконалені постійні загрози (APT) можуть

переміщатися швидко та непомітно, а командам безпеки потрібні актуальні та точні дані, щоб гарантувати автоматичне та точне налаштування захисту.

Рішення для інтеграції аналізу загроз має включати автоматизацію для розслідування всіх інцидентів і отримання інформації за хвилини, а не години. Він повинен генерувати спеціальні індикатори компрометації (IoC) безпосередньо з кінцевих точок, щоб забезпечити проактивний захист від майбутніх атак. Також має бути людський елемент, який складається з експертів-дослідників безпеки, аналітиків загроз, культурологів і лінгвістів, які можуть зрозуміти, що виникають загрози в різних контекстах.

5. Розширений внутрішній захист;

Традиційні антивірусні програми можуть блокувати зловмисне програмне забезпечення, але вони не заважають співробітникам зберігати конфіденційні дані на USB-накопичувачі та викрадати їх з організації. Рішення для кінцевих точок забезпечують кращий захист від загроз, таких як втрата та витік даних, завдяки таким технологіям, як шифрування даних і контроль доступу до них. Це гарантує, що неавторизовані співробітники не зможуть отримати дані поза межами своїх прав доступу та викрасти чи продати їх. Захист кінцевих точок також використовує передові технології, такі як аналіз поведінки, які дозволяють підприємствам виявляти загрози на основі підозрілої поведінки із зовнішніх і внутрішніх джерел.

6. Контроль на рівні підприємства.

Традиційні антивірусні рішення зазвичай повідомляють користувача лише про виявлення загрози. Після цього ризик повинен бути проаналізований і досліджений особисто спеціалістом із безпеки. Але рішення безпеки кінцевих точок забезпечують централізований портал, який дає змогу адміністраторам відстежувати активність, установлювати, налаштовувати, виправляти та оновлювати програмне забезпечення, досліджувати будь-який підозрілий трафік і вирішувати проблеми віддалено. Це також дозволяє адміністраторам виконувати ці дії на кількох кінцевих точках одночасно, що пришвидшує вирішення проблем для співробітників і економить величезну кількість часу IT-командам і командам безпеки.

1.4. Аналіз існуючих технологій захисту кінцевих точок корпоративної інформаційної системи

Нове покоління рішень для захисту кінцевих точок є відповіддю на зростання загроз і мобільності співробітників. Інноваційні підходи до захисту від загроз, такі як EPP, EDR, MDR і DLP, витісняють або працюють разом із традиційними рішеннями безпеки кінцевих точок.

Розглянемо наведені вище рішення більш детально:

Через перехід до віддаленої роботи і ризики зв’язані з цим, уразливість кінцевих точок значно збільшилась. Організаціям необхідно розробити та впровадити комплексну стратегію безпеки кінцевих точок, здатну подолати сучасні ризики кібербезпеки, з якими стикаються кінцеві точки. Розгортання платформи захисту кінцевих точок (EPP) є ключовим компонентом цієї стратегії.

1. Рішення EPP, діючи як профілактична перша лінія захисту від кіберзагроз для кінцевої точки, визначає файлове та безфайлове зловмисне програмне забезпечення, шкідливі сценарії та зловмисне програмне забезпечення, яке працює лише в пам’яті, і блокує виконання цих загроз у системі. Оскільки зловмисне програмне забезпечення стає все складнішим і поширенішим, наявність можливостей розслідування загроз і виправлення, які надає платформа захисту кінцевих точок, має важливе значення для корпоративної кібербезпеки. Командам безпеки потрібне рішення, яке блокує багато загроз, з якими стикаються їхні кінцеві точки, і надає їм інструменти для ефективного усунення будь-яких успішних вторгнень.

Рішення EPP має забезпечувати комплексний захист кінцевих точок організації. Щоб досягти цього, рішення EPP має пропонувати певну основну функціональність.

- Запобігання всім виникаючим загрозам

Ландшафт кіберзагроз швидко розвивається, і щодня створюються нові варіанти зловмисного програмного забезпечення, щоб скористатися новими платформами та нещодавно виявленими вразливими місцями. Крім того, багато з цих варіантів

використовують різні складні методи, щоб допомогти уникнути традиційного захисту від зловмисного програмного забезпечення.

З такою швидкою зміною ландшафту загроз застарілі підходи до захисту кінцевих точок, засновані на виявленні зловмисного програмного забезпечення за допомогою сигнатур, більше не ефективні. Рішення EPP має забезпечувати захист від нових і нових загроз, а не обмежуватися виявленням і блокуванням відомих варіантів шкідливого програмного забезпечення .

- Виявлення кінцевої точки та реакція (EDR)

EPP призначений для запобігання загрозам для кінцевих точок, діючи як перша лінія захисту від кіберзагроз. Однак цей підхід, орієнтований на профілактику, може не вловити кожну потенційну загрозу.

З цієї причини EPP слід поєднувати з рішенням EDR . Рішення EDR розроблено для підтримки виявлення загроз і здійснення пошуку загроз на кінцевій точці. Рішення, яке поєднує як превентивний EPP, так і проактивний EDR, забезпечує підтримку повного спектру для виявлення та усунення кібератак на кінцеву точку.

- Інтеграції

Кінцеві точки є лише частиною IT-інфраструктури організації. Ефективний захист від кіберзагроз вимагає здатності скоординовано реагувати на кібератаки, націлені на кілька кінцевих точок у корпоративній мережі. Рішення EPP повинне мати здатність легко інтегруватися з іншими корпоративними рішеннями кібербезпеки, щоб забезпечити обмін інформацією про загрози та скоординовану автоматизовану відповідь на кіберзагрози.

- Захист будь-де, де знаходяться дані

Корпоративні мережі складаються з різноманітних кінцевих точок. Хоча багато робочих станцій користувачів працюють під керуванням Windows або macOS, організація також, ймовірно, має сервери на базі Linux. Оскільки віддалена робота стає все більш поширеною, а технологія віртуалізації вдосконалюється, використання інфраструктури віртуального робочого столу (VDI) також стало більш поширеним.

Рішення EPP має бути здатним забезпечувати послідовний захист для всіх кінцевих точок організації. Це включає підтримку всіх операційних систем, а також можливість ефективного моніторингу та захисту систем на основі VDI.

2. EDR розроблено, щоб вийти за рамки реактивного кіберзахисту на основі виявлення. Натомість він надає аналітикам безпеки інструменти, необхідні для проактивного виявлення загроз і захисту організації. EDR надає низку функцій, які покращують здатність організації керувати ризиками кібербезпеки, наприклад:

- Покращена видимість;

Рішення безпеки EDR здійснюють безперервний збір і аналітику даних і звітують до єдиної централізованої системи. Це надає групі безпеки повну видимість стану кінцевих точок мережі з однієї консолі.

- Швидкі розслідування;

Рішення EDR призначені для автоматизації збору й обробки даних, а також певних заходів реагування. Це дає змогу групі безпеки швидко отримати контекст щодо потенційного інциденту безпеки та швидко вжити заходів для його усунення.

- Автоматизація виправлення;

Рішення EDR можуть автоматично виконувати певні заходи реагування на інциденти на основі попередньо визначених правил. Це дозволяє їм блокувати або швидко виправляти певні інциденти та зменшує навантаження на аналітиків безпеки.

- Контекстуальний пошук загроз.

Безперервний збір і аналіз даних рішень EDR забезпечує глибоку видимість стану кінцевої точки. Це дозволяє мисливцям за загрозами виявляти та досліджувати потенційні ознаки наявної інфекції.

Платформи виявлення та реагування кінцевих точок (EDR) і платформи захисту кінцевих точок (EPP) мають схожі цілі, але призначені для виконання різних цілей. EPP розроблено для забезпечення захисту на рівні пристрою шляхом виявлення шкідливих файлів, виявлення потенційно зловмисної активності та надання інструментів для розслідування інцидентів і реагування.

Профілактичний характер EPP доповнює проактивний EDR. EPP діє як перша лінія захисту, відфільтровуючи атаки, які можуть бути виявлені розгорнутими рішеннями безпеки організації. EDR діє як другий рівень захисту, дозволяючи аналітикам безпеки виконувати полювання на загрози та виявляти більш непомітні загрози для кінцевої точки.

Для ефективного захисту кінцевої точки потрібне рішення, яке об'єднує можливості EDR і EPP для забезпечення захисту від кіберзагроз, не перевантажуючи групу безпеки організації.

Ключові компоненти рішення EDR:

Як випливає з назви, рішення безпеки EDR має забезпечувати підтримку як для виявлення кіберзагроз, так і для реагування на кінцевих точках організації. Щоб аналітики безпеки могли ефективно та проактивно виявляти кіберзагрози, рішення EDR повинно мати такі компоненти:

- Потік перевірки інцидентів;

Групи безпеки зазвичай переповнені сповіщеннями, великий відсоток яких є помилковими. EDR має автоматично сортувати потенційно підозрілі або зловмисні події, дозволяючи аналітику безпеки визначати пріоритети своїх розслідувань.

- Полювання на загрози;

Не всі інциденти безпеки блокуються або виявляються рішеннями безпеки організації. EDR має забезпечувати підтримку діяльності по пошуку загроз, щоб аналітики безпеки могли активно шукати потенційне вторгнення.

- Агрегація та збагачення даних;

Контекст має важливе значення для правильного розрізнення справжніх загроз і помилкових спрацьовувань. Рішення безпеки EDR повинні використовувати стільки даних, скільки доступно для прийняття обґрунтованих рішень щодо потенційних загроз.

Після виявлення загрози аналітик безпеки повинен мати можливість швидко перейти до усунення загрози. Для цього потрібні такі можливості:

- Інтегроване реагування;

Перемикання контексту погіршує здатність аналітика швидко й ефективно реагувати на інциденти безпеки. Аналітики повинні мати можливість негайно вжити заходів для реагування на інцидент безпеки після перегляду відповідних доказів.

- Кілька варіантів реагування.

Відповідна відповідь на кіберзагрозу залежить від низки факторів. Рішення безпеки EDR має надати аналітикам кілька варіантів реагування, наприклад видалення загрози або поміщення на карантин.

3. Кероване виявлення та реагування (MDR):

Кероване виявлення та реагування – це категорія пропозиції безпеки як послуги, де організація передає деякі свої операції безпеки сторонньому постачальнику. Як випливає з назви, він виходить за рамки простого виявлення загроз і працює над їх усуненням у мережі організації.

Пропозиція служби безпеки MDR зазвичай включає кілька різних функцій:

- Розслідування інциденту;

Постачальники послуг безпеки MDR розслідують сповіщення та визначать, чи це справжній інцидент чи хибний результат. Це досягається за допомогою поєднання аналізу даних, машинного навчання та людського дослідження.

- Сортування сповіщень;

не всі інциденти безпеки однакові, і ряд факторів може впливати на пріоритет різних подій. Постачальник MDR організує список подій безпеки, дозволяючи обробляти найбільш критичні в першу чергу.

- Усунення;

постачальник керованого виявлення та реагування запропонує усунення інцидентів як послугу. Це означає, що вони віддалено вживатимуть заходів для реагування на подію безпеки в мережі клієнта.

- Проактивний пошук загроз.

не всі інциденти безпеки виловлюються стеком безпеки організації. Постачальники керованого виявлення та реагування завчасно шукатимуть у мережі

та системах організації ознаки поточної атаки та, якщо таку буде виявлено, вживатимуть заходів для її усунення.

Які проблеми вирішує (кероване виявлення та реагування) MDR?

Впровадження надійної програми кібербезпеки є проблемою для багатьох організацій через кілька різних факторів. Кероване виявлення та реагування дають відповідь на багато проблем, з якими стикаються організації, які намагаються підвищити зрілість своєї безпеки та зменшити ризики кібербезпеки, наприклад:

- Кадрові обмеження;

Індустрія кібербезпеки стикається з гострою нестачею кадрів, оскільки незаповнених посад набагато більше, ніж кваліфікованих спеціалістів, які їх заповнять. Через це організаціям складно та дорого виконувати критичні ролі безпеки всередині. MDR дозволяє організації заповнювати кадрові прогалини за допомогою зовнішніх спеціалістів із безпеки.

- Обмежений доступ до досвіду;

Крім відсутності досвіду в кібербезпеці загалом, організаціям важко зайняти спеціалізовані посади, які вимагають таких навичок, як реагування на інциденти, хмарна безпека та аналіз шкідливих програм. MDR надає організації миттєвий доступ до зовнішньої експертизи з кібербезпеки, коли це необхідно, без необхідності залучати та утримувати цих талантів усередині компанії.

- Розширена ідентифікація загроз;

Вдосконалені постійні загрози (APT) та інші досвідчені кіберзлочинці розробили інструменти та методи, щоб залишатися непоміченими багатьма традиційними рішеннями кібербезпеки. MDR дозволяє організаціям виявляти та усувати ці загрози за допомогою проактивного пошуку загроз.

- Повільне виявлення загроз;

Багато інцидентів кібербезпеки залишаються непоміченими протягом значного періоду часу, що збільшує витрати та вплив на цільову організацію. Час виявлення та реагування постачальників MDR підтримується угодами про рівень обслуговування (SLA), що гарантує мінімізацію витрат організації через інцидент кібербезпеки.

- Незрілість безпеки.

Створення ефективної програми кібербезпеки може бути дорогим через необхідні інструменти, ліцензії та персонал. MDR дає змогу організації швидко розгорнути повну програму безпеки з цілодобовим виявленням загроз і реагуванням на них, при цьому багато пов’язаних витрат розподіляються між клієнтською базою постачальника MDR. Це знижує загальну вартість володіння (TCO) кібербезпеки та дає змогу організації досягти високого рівня зрілості кібербезпеки швидше, ніж це було б можливо внутрішньо.

4. Запобігання втраті даних:

Запобігання втраті даних (DLP) – це методологія кібербезпеки, яка поєднує технології та найкращі практики для запобігання розкриттю конфіденційної інформації за межами організації, особливо регульованих даних, таких як інформація, що ідентифікує особу, і дані, пов’язані з нею.

Останніми роками організації стикаються зі зростаючою кількістю міжнародних, федеральних і державних нормативних актів, призначених для захисту споживачів і контролю над розкриттям особистої інформації. У той же час компанії дедалі більше мотивуються запобігати викриттю чи неправомірному використанню запатентованої інтелектуальної власності, що може мати значні фінансові наслідки через втрату конкурентної переваги. З цих причин запобігання втраті даних стало важливим елементом арсеналу кібербезпеки.

Незалежно від того, чи йдеться про відповідність політиці, чи просто для захисту даних клієнтів, юридичних документів та інтелектуальної власності, сьогодні організації стикаються з проблемою ефективного вирішення проблеми втрати даних, не перешкоджаючи продуктивності співробітників і не перевантажуючи IT-персонал. Технологія DLP з часом розвивалася й удосконалювалася, але зрештою вона неефективна для розуміння намірів користувачів. За допомогою звичайних програм DLP не було способу відрізнити співробітника відділу маркетингу з добрих намірів, який завантажував PDF-файл на Dropbox або Google Drive, від незадоволеного співробітника фінансового відділу, який надсилав електронною поштою конфіденційні дані про грошові

потоки в конкуруючу організацію. Ще складніше було спробувати захистити конфіденційні дані без тривалого розгортання, болісного адміністрування та високих витрат, які часто пов’язані з традиційними продуктами DLP.

Успіх будь-якого бізнес-заходу значною мірою залежить від здатності обмінюватися інформацією між командами та між важливими зацікавленими сторонами. Це обов’язкова вимога, яка часто може входити в прямий конфлікт із положеннями про конфіденційність і правилами політики, або коли конфіденційні бізнес-дані потрапляють у чужі руки. Таким чином, захист конфіденційного бізнес-контенту є проблемою швидкості та обсягу. Будь-яке ефективне рішення для запобігання втраті даних має створюватися для масштабованості, продуктивності та високої доступності з основними можливостями, зокрема такими:

- Розподілене паралельне виявлення вмісту, яке знаходить неактивний вміст на тисячах робочих станцій за години, а не за дні;
- Моніторинг активності, який відстежує та контролює будь-який тип або формат конфіденційної інформації в русі, такої як електронна пошта, веб-перегляд і служби обміну файлами;
- Підходи до обробки, які вимагають лише невеликих обчислювальних навантажень і мінімізують мережевий трафік;
- Моніторинг мережі, налаштований на гігабітну швидкість захоплення та аналізу за кількома протоколами;
- Автоматичне перемикання після відмови, яке забезпечує роботу системи та захист вмісту організації 24/7/365.

Висновок до розділу 1

Забезпечення інформаційної безпеки – комплексне завдання. В ній немає неважливих або другорядних питань. Наприклад, не можна організувати захист від зовнішніх не приділяючи увагу підготовці персоналу. Також не можна сподіватись виключно на реактивні міри.

Опираючись на статистику загроз, можна зробити висновок що, ефективно протидіяти сучасним загрозам спроможні тільки ті системи, які з найраніших

стадій розробки проектувалися з урахуванням певних вимог безпеки. При цьому – це не статичний стан, а динамічний процес у рамках якого виробники адаптують свої рішення для захисту від загроз які постійно змінюються. Гнучкість налаштування IPS систем, дозволяють постійно адаптувати та модернізувати їх згідно останнім тенденціям та вимогам. Саме це дозволяє використовувати її як для забезпечення захисту в організаціях, так і для некомерційного використання.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК НА БАЗІ WAZUH

2.1. Призначення, можливості та функції Wazuh

Wazuh — це безкоштовна платформа безпеки з відкритим кодом, яка об’єднує можливості EDR і SIEM. Вона захищає робочі навантаження в локальних, віртуалізованих, контейнерних і хмарних середовищах. Wazuh допомагає організаціям і окремим особам захистити свої дані від загроз безпеки. Він широко використовується тисячами організацій по всьому світу, від малих до великих підприємств.

До можливостей Wazuh можна включити наступні пункти:

- Аналітика безпеки:

Wazuh використовується для збору, агрегування, індексування та аналізу даних безпеки, допомагаючи організаціям виявляти вторгнення, загрози та поведінкові аномалії.

Оскільки кіберзагрози стають все більш витонченими, для швидкого виявлення та усунення загроз необхідні моніторинг і аналіз безпеки в реальному часі. Легкий агент забезпечує необхідні можливості моніторингу та реагування, тоді як серверний компонент забезпечує аналіз безпеки та виконує аналіз даних.

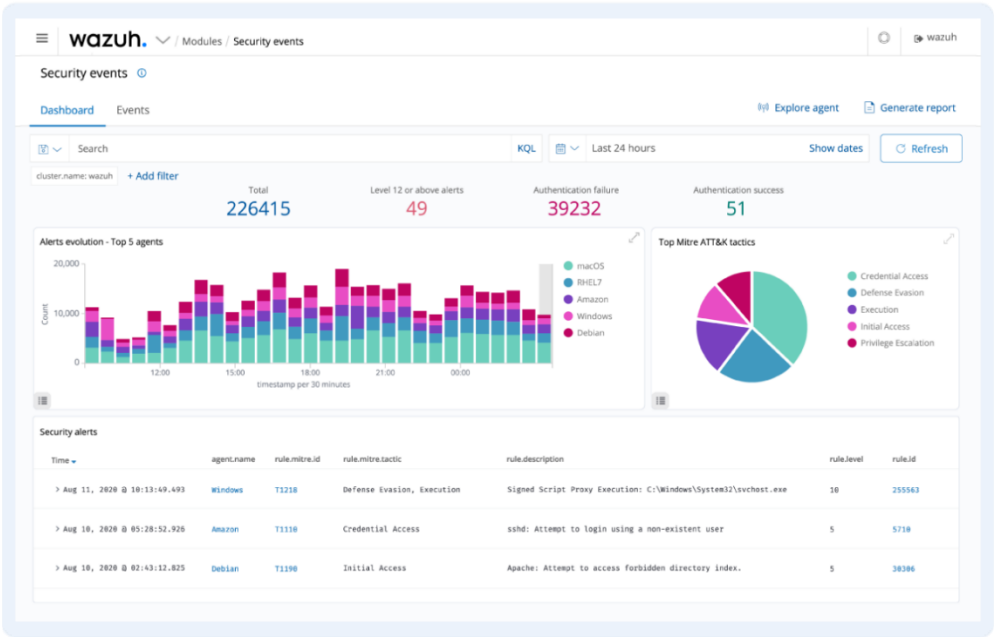

Рис. 2.1 Вікно аналітики безпеки

- Виявлення вторгнень:

Агенти Wazuh сканують контрольовані системи на наявність шкідливого програмного забезпечення, руткітів і підозрілих аномалій. Вони можуть виявляти приховані файли, замасковані процеси або незареєстровані мережеві слухачі, а також невідповідності у відповідях на системні виклики.

На додаток до можливостей агента, серверний компонент використовує підхід до виявлення вторгнень на основі сигнатур, використовуючи механізм

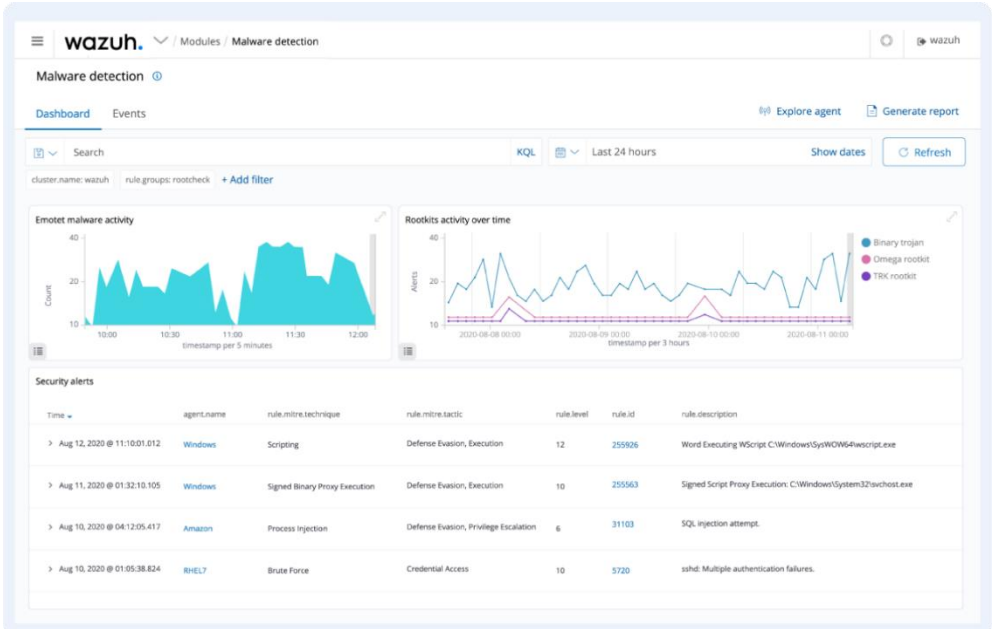

Рис. 2.2 Вікно виявлення вторгнень

регулярних виразів для аналізу зібраних даних журналу та пошуку ознак компрометації.

- Аналіз даних журналу

Агенти Wazuh читають журнали операційної системи та програм і безпечно пересилають їх до центрального менеджера для аналізу та зберігання на основі правил.

Правила Wazuh допомагають вам повідомити про помилки програми або системи, неправильні конфігурації, спроби та/або успішні зловмисні дії, порушення політики та низку інших проблем безпеки та роботи.

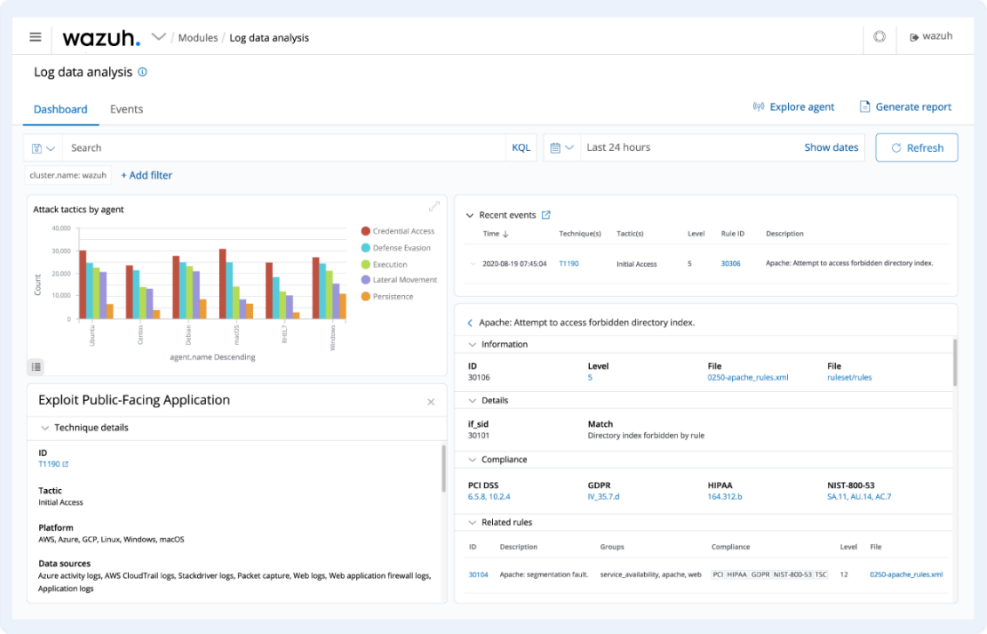

Рис. 2.3 Вікно аналізу даних журналу

- Моніторинг цілісності файлів

Wazuh відстежує файлову систему, виявляючи зміни у вмісті, дозволах, власності та атрибутах файлів, за якими потрібно стежити. Крім того, він ідентифікує користувачів і програми, які використовуються для створення або зміни файлів.

Можливості моніторингу цілісності файлів можна використовувати в поєднанні з аналізом загроз для виявлення загроз або скомпрометованих хостів. Крім того, цього вимагають деякі нормативні стандарти відповідності, наприклад PCI DSS.

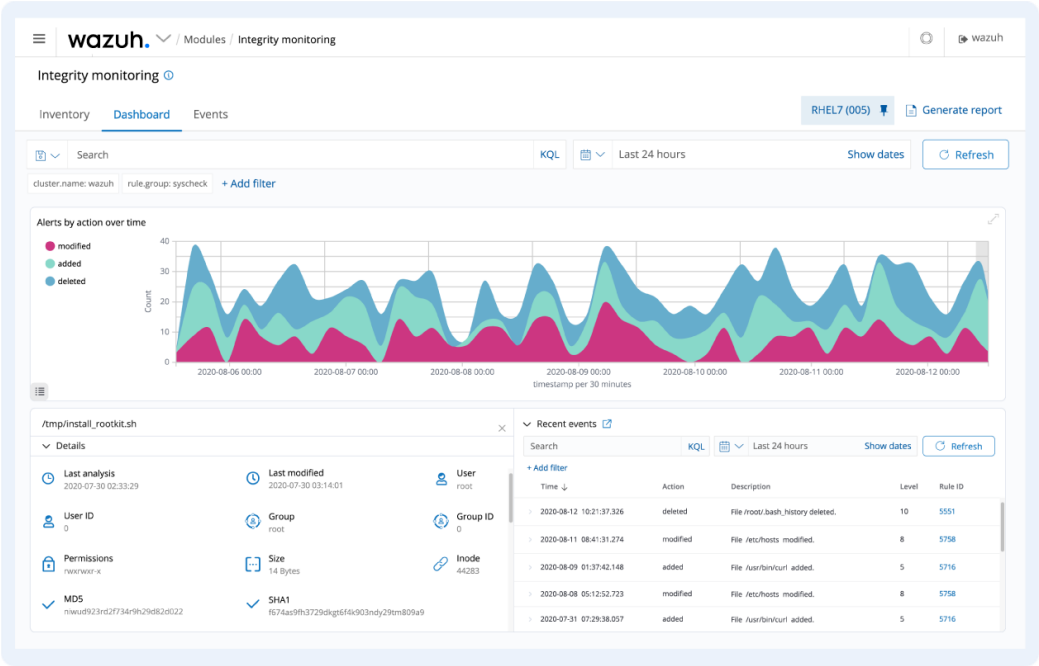

Рис. 2.4 Вікно моніторингу цілісності

- Виявлення вразливостей:

Агенти Wazuh збирають дані інвентаризації програмного забезпечення та надсилають цю інформацію на сервер, де вона співвідноситься з постійно оновлюваними базами даних CVE (Common Vulnerabilities and Exposure), щоб ідентифікувати добре відоме вразливе програмне забезпечення. Автоматизована оцінка вразливості допомагає вам знайти слабкі місця у ваших критично важливих активах і вжити заходів для виправлення, перш ніж зловмисники використають їх для саботування вашого бізнесу або викрадення конфіденційних даних.

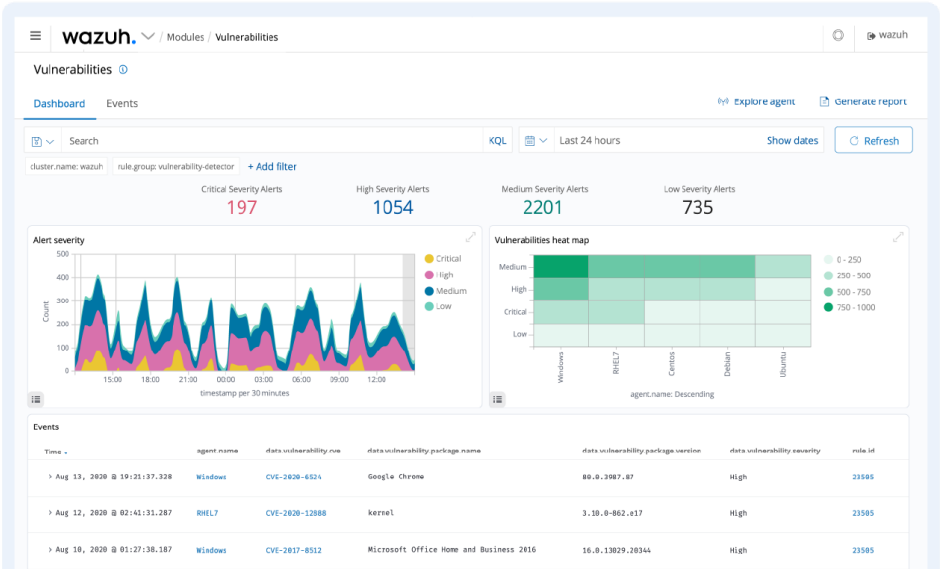

Рис. 2.5 Вікно виявлення уразливостей

- Оцінка конфігурації:

Wazuh відстежує налаштування конфігурації системи та програм, щоб переконатися, що вони відповідають вашим політикам безпеки, стандартам та/або посібникам із захисту. Агенти виконують періодичне сканування, щоб виявити програми, які, як відомо, є вразливими, невиправленими або ненадійно налаштованими.

Крім того, перевірки конфігурації можна налаштувати, адаптуючи їх відповідно до вашої організації. Сповіщення містять рекомендації щодо кращої конфігурації, посилання та зіставлення з нормативною відповідністю.

- Реагування на інцидент:

Wazuh надає готові активні відповіді для виконання різних заходів протидії активним загрозам, наприклад, блокування доступу до системи з джерела загрози, коли виконуються певні критерії. Крім того, Wazuh можна використовувати для віддаленого запуску команд або системних запитів, ідентифікації індикаторів компрометації (IOC) і допомоги у виконанні інших завдань криміналістики або реагування на інциденти.

- Відповідність нормативним вимогам:

Wazuh забезпечує деякі необхідні засоби контролю безпеки, щоб відповідати галузевим стандартам і правилам. Ці функції в поєднанні з масштабованістю та підтримкою кількох платформ допомагають організаціям відповідати вимогам технічної відповідності.

Wazuh широко використовується компаніями з обробки платежів і фінансовими установами для відповідності вимогам PCI DSS (Payment Card Industry Data Security Standard). Його веб-інтерфейс користувача надає звіти та інформаційні панелі, які можуть допомогти з цим та іншими правилами, такими як GDPR, NIST 800-53, GPG13, TSC SOC2 та HIPAA.

- Хмарна безпека:

Wazuh допомагає контролювати хмарну інфраструктуру на рівні API, використовуючи модулі інтеграції, які можуть отримувати дані безпеки від відомих хмарних провайдерів, таких як Amazon AWS, Azure або Google Cloud. Крім того,

Wazuh надає правила для оцінки конфігурації вашого хмарного середовища, легко виявляючи слабкі місця. Крім того, для моніторингу хмарних середовищ на рівні екземплярів зазвичай використовуються легкі та мультиплатформенні агенти Wazuh.

- Безпека контейнерів:

Wazuh забезпечує безпекову видимість ваших хостів і контейнерів Docker, відстежуючи їх поведінку та виявляючи загрози, вразливості та аномалії. Агент Wazuh має вбудовану інтеграцію з механізмом Docker, що дозволяє користувачам контролювати зображення, томи, параметри мережі та запущені контейнери.

Wazuh постійно збирає та аналізує детальну інформацію про час виконання. Наприклад, сповіщення про контейнери, що працюють у привілейованому режимі, уразливі програми, оболонку, що працює в контейнері, зміни постійних томів або зображень та інші можливі загрози.

2.2. Компоненти та архітектура Wazuh

Платформа Wazuh надає функції XDR і SIEM для захисту робочих навантажень хмари, контейнера та сервера. Вони включають аналіз даних журналу, виявлення вторгнень і зловмисного програмного забезпечення, моніторинг цілісності файлів, оцінку конфігурації, виявлення вразливостей і підтримку нормативної відповідності.

Рішення Wazuh базується на агенті Wazuh, який розгортається на контрольованих кінцевих точках, і на трьох центральних компонентах:

- Сервері Wazuh;
- Індексаторі Wazuh;
- Інформаційній панелі Wazuh.

1. Сервер Wazuh аналізує дані, отримані від агентів. Він обробляє його через декодери та правила, використовуючи аналіз загроз для пошуку добре відомих індикаторів компрометації. Один сервер може аналізувати дані від сотень або тисяч агентів і масштабувати горизонтально, якщо налаштувати його як кластер. Цей

центральний компонент також використовується для керування агентами, налаштування та оновлення їх віддалено, коли це необхідно.

Серверний компонент Wazuh аналізує дані, отримані від агентів , ініціюючи сповіщення при виявленні загроз або аномалій. Він також використовується для віддаленого керування конфігурацією агентів і моніторингу їх стану.

Сервер Wazuh використовує джерела аналізу загроз, щоб покращити свої можливості виявлення. Він також збагачує дані попереджень, використовуючи структуру MITER ATT&CK і нормативні вимоги, такі як PCI DSS, GDPR, HIPAA, і NIST 800-53, надаючи корисний контекст для аналітики безпеки.

Крім того, сервер Wazuh можна інтегрувати із зовнішнім програмним забезпеченням, таким як ServiceNow , Jira та PagerDuty , а також платформи обміну миттєвими повідомленнями, такі як Slack . Ці інтеграції зручні для оптимізації операцій безпеки.

- Архітектура сервера

Сервер Wazuh запускає механізм аналізу, Wazuh RESTful API, службу реєстрації агентів, службу підключення агентів, демон кластера Wazuh і Filebeat. Сервер інстальовано в операційній системі Linux і зазвичай працює на автономній фізичній машині, віртуальній машині, контейнері докерів або хмарному екземплярі.

На діаграмі нижче показано архітектуру та компоненти сервера:

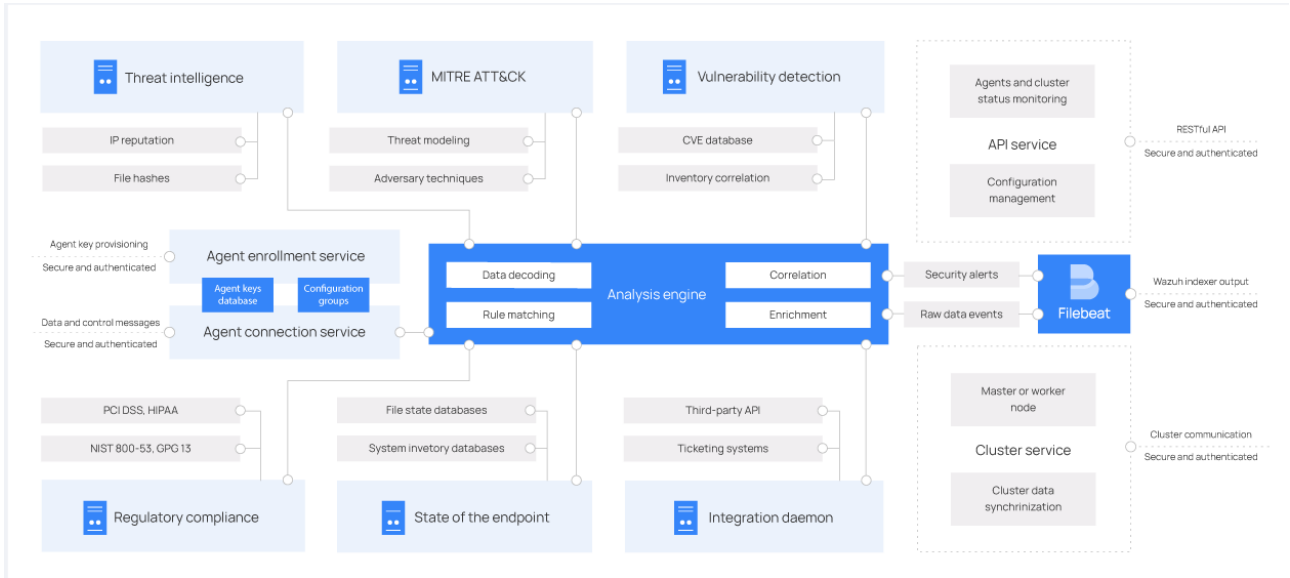

Рис. 2.6 Схема потоку даних

- Серверні компоненти

Сервер Wazuh складається з кількох перелічених нижче компонентів, які мають різні функції, наприклад реєстрацію нових агентів, перевірку ідентифікації кожного агента та шифрування зв’язку між агентом Wazuh і сервером Wazuh.

- Служба реєстрації агентів:

Використовується для реєстрації нових агентів. Ця служба надає та розповсюджує унікальні ключі автентифікації кожному агенту. Процес працює як мережева служба та підтримує автентифікацію за допомогою сертифікатів TLS/SSL або шляхом надання фіксованого пароля.

- Служба підключення агентів:

Ця служба отримує дані від агентів. Він використовує ключі, спільні для служби реєстрації, для перевірки ідентифікації кожного агента та шифрування зв’язку між агентом Wazuh і сервером Wazuh. Крім того, ця послуга забезпечує централізоване керування конфігурацією, що дозволяє віддалено надсилати нові параметри агента.

- Механізм аналізу:

Це серверний компонент, який виконує аналіз даних. Він використовує декодери для визначення типу інформації, що обробляється (події Windows, журнали SSH, журнали веб-сервера та інші). Ці декодери також витягують відповідні елементи даних із повідомлень журналу, такі як IP-адреса джерела, ідентифікатор події або ім’я користувача. Потім, використовуючи правила, механізм визначає конкретні шаблони в розшифрованих подіях, які можуть викликати сповіщення та, можливо, навіть викликати автоматичні контрзаходи (наприклад, заборона IP-адреси, зупинка запущеного процесу або видалення артефакту зловмисного програмного забезпечення).

- Wazuh RESTful API:

Ця служба надає інтерфейс для взаємодії з інфраструктурою Wazuh. Він використовується для керування параметрами конфігурації агентів і серверів, моніторингу стану інфраструктури та загального стану здоров'я, керування та редагування декодерів і правил Wazuh, а також запиту про стан контрольованих кінцевих точок. Інформаційна панель Wazuh також використовує його.

- Демон кластера Wazuh:

Ця служба використовується для горизонтального масштабування серверів Wazuh, розгортаючи їх як кластер. Така конфігурація в поєднанні з балансувальником мережевого навантаження забезпечує високу доступність і балансування навантаження. Демон кластера Wazuh — це те, що сервери Wazuh використовують для спілкування один з одним і підтримки синхронізації.

- Filebeat:

Використовується для надсилання подій і сповіщень до індексатора Wazuh. Він зчитує вихід аналітичної системи Wazuh і передає події в реальному часі. Він також забезпечує балансування навантаження при підключенні до багатовузлового кластера індексатора Wazuh.

2. Індексатор Wazuh — це високомасштабована система повнотекстового пошуку та аналітики. Цей центральний компонент Wazuh індексує та зберігає сповіщення, створені сервером Wazuh, і забезпечує пошук даних і аналітику майже в реальному часі. Індексатор Wazuh можна налаштувати як одновузловий або багатовузловий кластер, що забезпечує масштабованість і високу доступність.

Індексатор Wazuh зберігає дані як документи JSON. Кожен документ співвідносить набір ключів, імен полів або властивостей із відповідними значеннями, які можуть бути рядками, числами, логічними значеннями, датами, масивами значень, геолокаціями чи іншими типами даних.

Wazuh використовує чотири різні індекси для зберігання різних типів подій:

Таблиця 2.1

Види індексів

Індекс	Опис
wazuh-alerts	Зберігає сповіщення, створені сервером Wazuh. Вони створюються кожного разу, коли подія запускає правило з достатньо високим пріоритетом (цей поріг можна налаштувати).
wazuh-archives	Зберігає всі події (архівні дані), отримані сервером Wazuh, незалежно від того, чи спрацьовує правило.
wazuh-monitoring	Зберігає дані, пов’язані зі статусом агента Wazuh протягом певного часу. Він використовується веб-інтерфейсом, щоб показати, коли окремі агенти є або були Active, Disconnected, або .Never connected
wazuh-statistics	Зберігає дані, пов’язані з продуктивністю сервера Wazuh. Він використовується веб-інтерфейсом для представлення статистики продуктивності.

3. Інформаційна панель Wazuh – це веб інтерфейс користувача для візуалізації та аналізу даних. Він включає в себе готові інформаційні панелі для подій безпеки, нормативної відповідності, виявлені вразливі програми, дані моніторингу цілісності файлів, результати оцінки конфігурації, моніторинг хмарної інфраструктури. Він також використовується для керування конфігурацією Wazuh і моніторингу її стану.

4. Агенти Wazuh встановлюються на кінцевих точках, таких як ноутбуки, настільні комп’ютери, сервери, хмарні екземпляри або віртуальні машини. Вони забезпечують запобігання загрозам, їх виявлення та реагування. Вони працюють на таких операційних системах, як Linux, Windows, macOS, Solaris, AIX і HP-UX.

На додаток до можливостей моніторингу на основі агентів, платформа Wazuh може контролювати безагентні пристрої, такі як брандмауери, комутатори, маршрутизатори або мережі IDS, серед іншого. Наприклад, дані системного

журналу можна збирати через Syslog, а його конфігурацію можна відстежувати шляхом періодичного тестування даних, через SSH або через API.

2.3. Вимоги до системи та інсталяція Wazuh

Wazuh є безкоштовною платформою безпеки з відкритим кодом, його компоненти відповідають GNU General Public License, версія 2 і Apache License, версія 2.0.

Платформа надає два методи встановлення для кожного центрального компонента Wazuh. Обидва варіанти містять інструкції щодо встановлення центральних компонентів на одному або на окремих хостах. Для цього існує вся необхідна документація і це робить платформу Wazuh доволі дружелюбною до користувача.

Індексатор Wazuh і сервер Wazuh можуть бути встановлені на одному хості або розподілені в кластерних конфігураціях.

Робочий процес встановлення має відбуватися в такому порядку:

1. Індексатор Wazuh;

Індексатор Wazuh — це високомасштабована система повнотекстового пошуку та аналітики. Цей центральний компонент Wazuh індексує та зберігає сповіщення, створені сервером Wazuh, і забезпечує пошук даних і аналітику майже в реальному часі.

Встановити індексатор можна на одному хості або на кількох вузлах у конфігурації кластера. Це забезпечує масштабованість, високу доступність і покращену продуктивність.

Вимоги до встановлення індексатора:

Потрібно переконатися що операційна система підтримує та відповідає рекомендованих вимогам для встановлення індексатора Wazuh. Також необхідно переконатись в наявності прав root.

- Рекомендовані операційні системи

Індексатор Wazuh можна встановити на 64-бітну операційну системуLinux. Wazuh підтримує такі версії операційної системи:

Таблиця 2.2

Amazon Linux 2	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04

- Рекомендації щодо обладнання

Індексатор Wazuh можна встановити як одновузловий або багатовузловий кластер.

Рекомендації щодо обладнання для кожного вузла:

Таблиця 2.3

Мінімум			Рекомендовано	
Компонент	Оперативна пам’ять (ГБ)	ЦП (ядра)	Оперативна пам’ять (ГБ)	ЦП (ядра)
Індексатор Wazuh	4	2	16	8

- Вимоги до дискового простору

Обсяг даних залежить від кількості згенерованих сповіщень за секунду (APS). У цій таблиці вказано приблизний дисковий простір, необхідний агенту для зберігання сповіщень протягом 90 днів на сервері індексатора Wazuh, залежно від типу контрольованих кінцевих точок. Наприклад, для середовища з 80 робочими станціями, 10 серверами та 10 мережевими пристроями необхідний обсяг пам’яті на сервері індексатора Wazuh для 90 днів сповіщень становить 230 ГБ.

Таблиця 2.4

Контрольовані кінцеві точки	APS	Зберігання в індексаторі Wazuh (ГБ/90 днів)
Сервери	0,25	3,7

Робочі станції	0,1	1,5
Мережеві пристрої	0,5	7,4

2. Сервер Wazuh;

Сервер Wazuh аналізує дані, отримані від агентів Wazuh, ініціюючи сповіщення при виявленні загроз або аномалій. Він також використовується для віддаленого керування конфігурацією агентів і моніторингу їх стану.

Встановити сервер Wazuh можна на одному хості або на кількох вузлах у конфігурації кластера. Багатовузлові конфігурації забезпечують високу доступність і покращену продуктивність. А в поєднанні з балансувальником навантаження мережі можна досягти ефективного використання його потужності.

Вимоги до встановлення сервера:

Потрібно переконатися що операційна система підтримує та відповідає рекомендованих вимогам для встановлення сервера Wazuh. Також необхідно переконатись в наявності прав root.

- Рекомендовані операційні системи

Сервер Wazuh можна встановити на 64-бітну операційну систему Linux. Wazuh підтримує такі версії операційної системи:

Таблиця 2.5

Amazon Linux 2	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04

- Рекомендації щодо обладнання

Сервер Wazuh можна встановити як одновузловий або багатовузловий кластер.

Таблиця 2.6

Мінімум			Рекомендовано	
Компонент	Оперативна пам’ять (ГБ)	ЦП (ядра)	Оперативна пам’ять (ГБ)	ЦП (ядра)

Сервер Wazuh	2	2	4	8

- Вимоги до дискового простору

Обсяг даних залежить від кількості згенерованих сповіщень за секунду (APS). У таблиці 2.7 вказано приблизний дисковий простір, необхідний одному агенту для зберігання сповіщень протягом 90 днів на сервері Wazuh, залежно від типу контрольованих кінцевих точок Наприклад, для середовища з 80 робочими станціями, 10 серверами та 10 мережевими пристроями необхідний обсяг пам’яті на сервері Wazuh для 90 днів сповіщень становить 6 ГБ.

Таблиця 2.7

Контрольовані кінцеві точки	APS	Зберігання на сервері Wazuh (ГБ/90 днів)
Сервери	0,25	0,1
Робочі станції	0,1	0,04
Мережеві пристрої	0,5	0,2

- Масштабування

Щоб визначити, чи сервер Wazuh вимагає більше ресурсів, необхідно перевірити такі файли:

«/var/ossec/var/run/wazuh-analysisd.state»: змінна «events_dropped» вказує, чи події скидаються через брак ресурсів.

«/var/ossec/var/run/wazuh-remoted.state»: змінна «discarded_count» вказує, чи були відхилені повідомлення від агентів.

Ці дві змінні повинні дорівнювати нулю, якщо середовище працює належним чином. Якщо це не так, до кластера можна додати додаткові вузли.

3. Інформаційна панель Wazuh;

Цей центральний компонент – це гнучкий та інтуївно зрозумілий веб-інтерфейс для видобутку, аналізу та візуалізації даних безпеки. Він надає готові інформаційні панелі, що дозволяє легко переміщатися в інтерфейсі користувача.

За допомогою інформаційної панелі Wazuh користувачі можуть візуалізувати події безпеки, виявлені вразливості, дані моніторингу цілісності файлів, результати оцінки конфігурації, події моніторингу хмарної інфраструктури та стандарти відповідності нормативним вимогам.

Вимоги до встановлення інформаційної панелі:

Потрібно переконатися що операційна система підтримує та відповідає рекомендованих вимогам для встановлення інформаційної панелі Wazuh. Також необхідно переконатись в наявності прав root.

- Рекомендовані операційні системи

Інформаційну панель Wazuh можна встановити на 64-бітну операційну систему Linux. Wazuh підтримує такі версії операційної системи:

Таблиця 2.8

Amazon Linux 2	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04

- Рекомендації щодо обладнання

Інформаційну панель Wazuh можна встановити на виділеному вузлі або разом із індексатором Wazuh.

Вимоги до обладнання:

Таблиця 2.9

Мінімум			Рекомендовано	
Компонент	Оперативна пам’ять (ГБ)	ЦП (ядра)	Оперативна пам’ять (ГБ)	ЦП (ядра)
Інформаційна панель Wazuh	4	2	8	4

- Сумісність з браузером

Інформаційна панель Wazuh підтримує такі веб-браузери:

- Chrome 95 або новішої версії
- Firefox 93 або новішої версії
- Safari 13.7 або новішої версії

Інші браузери на основі Chromium також можуть працювати. Internet Explorer 11 не підтримується.

4. Агент Wazuh.

Агент Wazuh є мультиплатформенним і працює на кінцевих точках, які користувач хоче контролювати. Він спілкується з сервером Wazuh, надсилаючи дані майже в режимі реального часу через зашифрований та автентифікований канал.

Агент може бути встановлений на такі платформи:

- Linux
- Windows
- MacOS
- Кінцеві точки AIX
- Кінцеві точки HP-UX
- Кінцеві точки Solaris

Агент було розроблено з урахуванням необхідності моніторингу різноманітних кінцевих точок без впливу на їх продуктивність. Він підтримується найпопулярнішими операційними системами, і для цього потрібно в середньому 35 Мб оперативної пам'яті.

Агент Wazuh надає ключові функції для підвищення системи безпеки.

Таблиця 2.10

Зберігання логів у спеціальних лог-файлах	Виконання команд
Моніторинг цілісності файлів (FIM)	Оцінка конфігурації безпеки (SCA)

Інвентаризація системи	Виявлення шкідливих програм
Активне реагування	Безпека контейнера
Хмарна безпека	

Завдяки інтуїтивно зрозумілому інтерфейсу, процес розгортання агента Wazuh є доволі простим. Якщо Wazuh розгортається у великому середовищі з великою кількістю серверів або кінцевих точок, розгортання може бути легшим за допомогою засобів автоматизації, таких як: Puppet, Chef, Ansible тощо.

Щоб розгорнути нового агента, необхідно дотримуватись інструкцій на інформаційній панелі Wazuh. Потрібно перейти до Wazuh > Agents і натиснути на кнопку Deploy new agent.

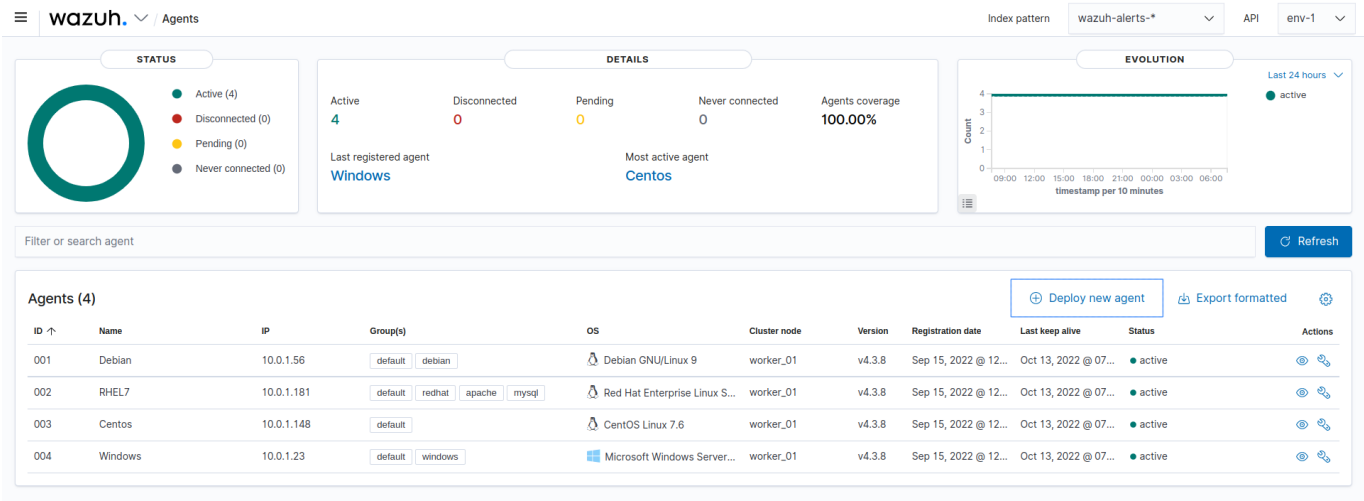

Рис. 2.7 Інформаційна панель Wazuh

Далі інформаційна панель Wazuh покаже наступні кроки для розгортання нового агента.

1. Обрати операційну систему яка встановлена на вибраному агенті.

2. Вибрати необхідно вказати адресу, яку агент використовує для зв’язку із серверов Wazuh. Це може бути IP-адреса або повне доменне ім’я. Wazuh може вказати її за замовчуванням.

3. Призначити агента до однієї або декількох груп.

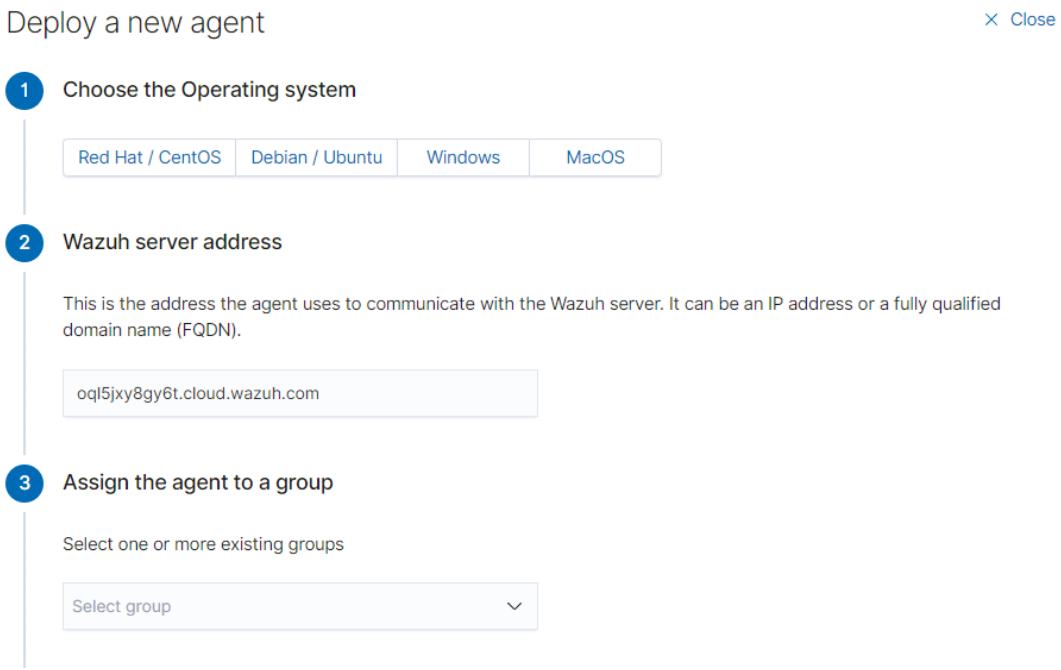

Рис. 2.8 Розгортання нового агента

4. Встановлення та реєстрація клієнта. Wazuh надасть необхідні команди, згідно з обраною операційною системою, які необхідно виконати в терміналі для автоматичної інсталяції агента. Якщо інсталятор знайде інший агент Wazuh у системі, він оновить його, зберігаючи конфігурацію.

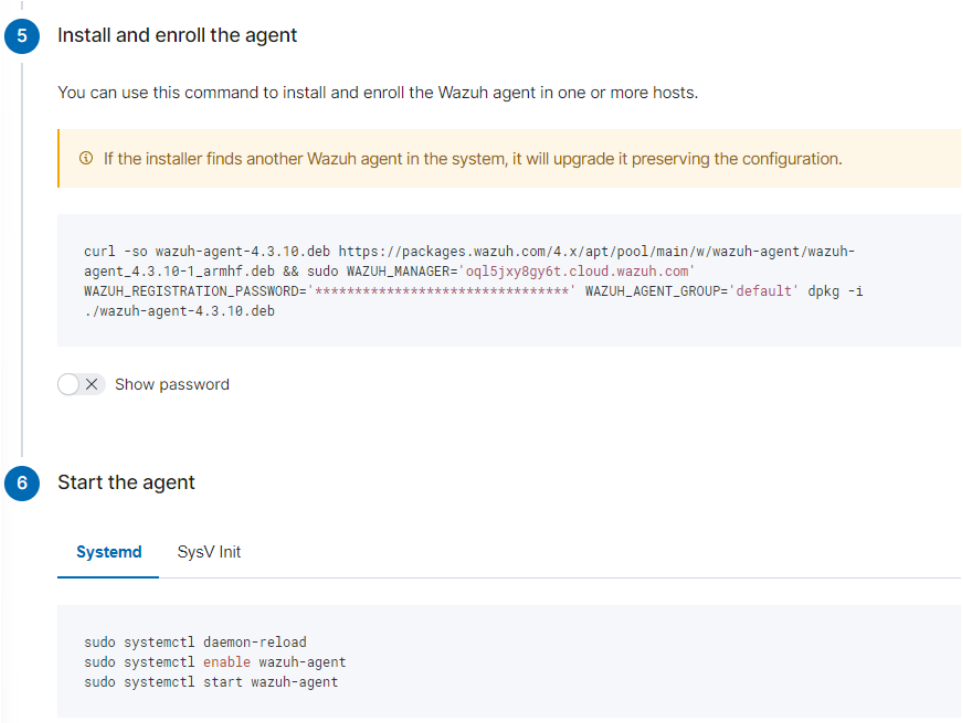

Рис. 2.9 Команди для розгортання нового агента

2.4. Можливості щодо управління Wazuh

Wazuh пропонує широкий спектр управління системою та окремими її можливостями. Серед них можна виділити ті, які є найбільш важливими при базовому використанні системи на невеликій кількості пристроїв.

- Збір даних журналу

Збір даних журналу – це процес у режимі реального часу, який дає сенс записам, створеним серверами або пристроями. Цей компонент може отримувати журнали через текстові файли або журнали подій Windows. Він також може безпосередньо отримувати журнали через віддалений системний журнал, що корисно для брандмауерів та інших подібних пристроїв.

Метою цього процесу є виявлення програмних або системних помилок, неправильних налаштувань, спроб вторгнення, порушень політики або проблем безпеки.

Вимоги до пам’яті та ЦП для агента Wazuh незначні, оскільки його основним обов’язком є пересилання подій менеджеру. Однак у менеджері Wazuh споживання процесора та пам’яті може швидко зрости залежно від кількості подій за секунду (EPS), які має проаналізувати менеджер.

- Контроль цілісності файлів

Система моніторингу цілісності файлів Wazuh (FIM) спостерігає за вибраними файлами та подає сповіщення, коли ці файли змінюються. Компонент, що відповідає за це завдання, називається syscheck. Цей компонент зберігає криптографічну контрольну суму та інші атрибути файлів або ключів реєстру Windows і регулярно порівнює їх із поточними файлами, які використовує система, спостерігаючи за змінами.

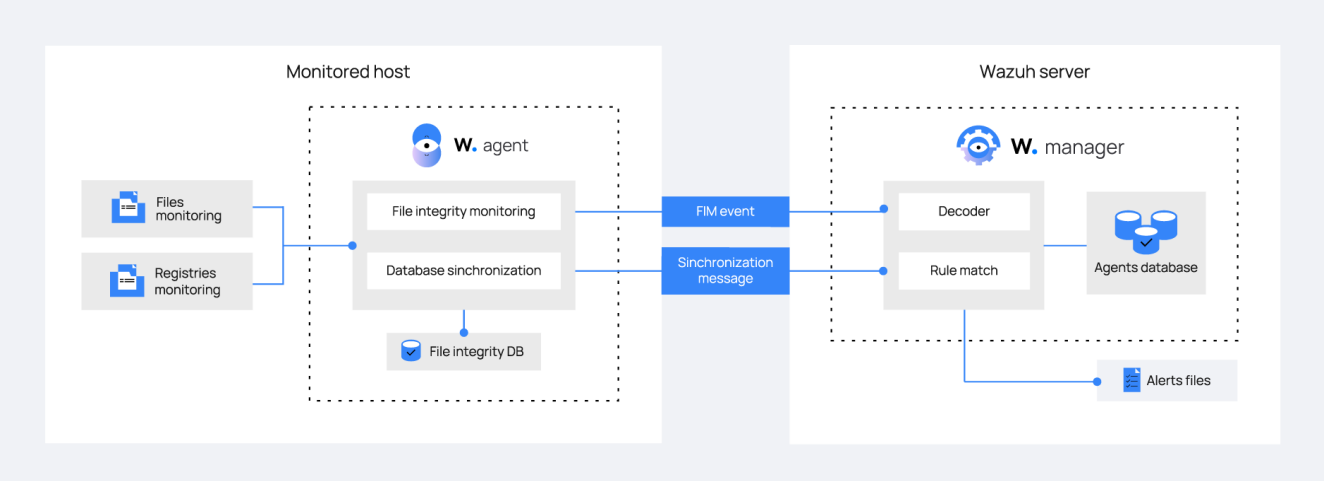

Рис. 2.10 Моніторинг цілісності файлів

Модуль FIM знаходиться в агенті Wazuh, де він запускає періодичне сканування системи та зберігає контрольні суми та атрибути файлів, що

відстежуються, і ключів реєстру Windows у локальній базі даних FIM. Модуль шукає зміни, порівнюючи контрольні суми нових файлів із контрольними сумами старих. Про всі виявлені зміни повідомляється менеджер Wazuh.

Механізм синхронізації FIM гарантує, що інвентаризація файлів у менеджері Wazuh завжди оновлюється щодо агента Wazuh, дозволяючи обслуговувати пов'язані з FIM запити API щодо агентів Wazuh. Синхронізація FIM базується на періодичних обчисленнях цілісності між агентом Wazuh і базами даних менеджера Wazuh, оновлюючи в менеджері Wazuh лише ті файли, які застаріли, оптимізуючи передачу даних FIM. Кожного разу, коли виявляються зміни у відстежуваних файлах та/або розділах реєстру, створюється сповіщення.

За замовчуванням для кожного агента Wazuh увімкнено та попередньо налаштовано системну перевірку, але рекомендується переглянути та змінити конфігурацію контрольованого хоста. За замовчуванням для кожного агента Wazuh увімкнено та попередньо налаштовано системну перевірку, але рекомендується переглянути та змінити конфігурацію контрольованого хоста.

- Виявлення аномалій і шкідливих програм

Виявлення аномалій стосується пошуку шаблонів у системі, які не відповідають очікуваній поведінці. Щойно зловмисне програмне забезпечення (наприклад, руткіт) встановлено в системі, воно модифікує систему, щоб приховати себе від користувача. Незважаючи на те, що зловмисне програмне забезпечення використовує для цього різноманітні методи, Wazuh використовує підхід широкого спектру для пошуку аномальних моделей, які вказують на можливих зловмисників.

Основним компонентом, що відповідає за це завдання, є rootcheck . Однак Syscheck також відіграє важливу роль.

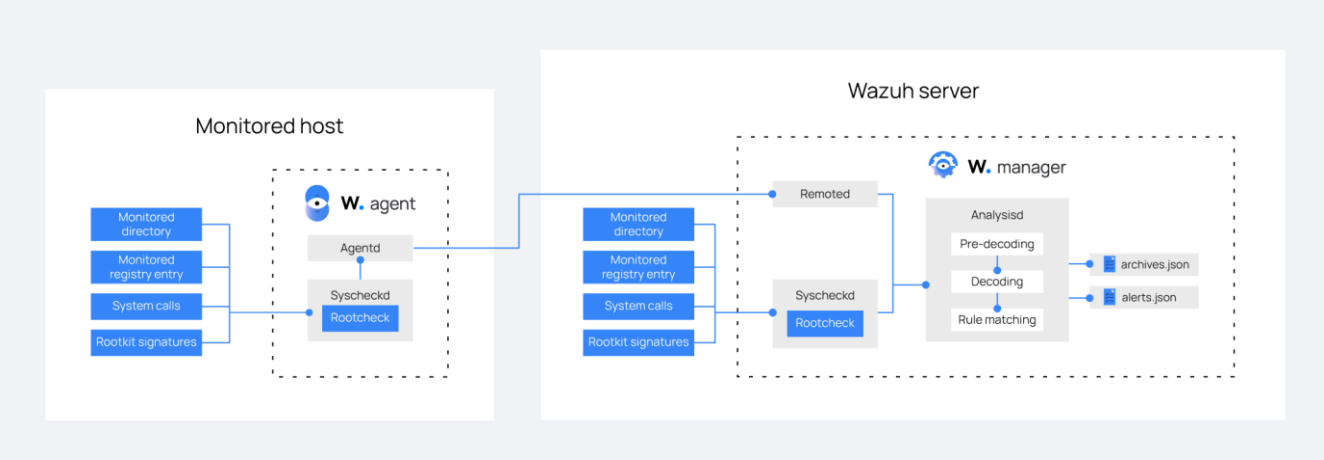

Рис. 2.11 Виявлення аномалій і шкідливих програм

Зловмисне програмне забезпечення може замінювати файли, каталоги та команди на хост-системі. Виконуючи моніторинг цілісності файлів, користувачі можуть перевіряти вибрані каталоги системи, щоб виявити ці дії.

- Оцінка конфігурації безпеки

Існує кілька інтеграцій Wazuh, які виконують сканування оцінки, включаючи CIS-CAT і нещодавно оцінку конфігурації безпеки (SCA). SCA була створена командою розробників Wazuh, щоб подолати обмеження, властиві іншим інтеграціям, зокрема:

- Інструмент CIS-CAT є запатентованим програмним забезпеченням, для використання якого потрібна зовнішня ліцензія.
- Модуль Rootcheck залежить від демона Syscheck , і канали його політик часто є застарілими.

Модуль оцінки конфігурації безпеки SCA спрямований на те, щоб надати користувачеві найкращий досвід під час виконання сканування політик захисту та конфігурації. Деякі з його ключових особливостей включають:

- Стан останнього сканування SCA. Результати перевірок для кожної ввімкненої політики зберігаються в менеджері Wazuh. З ними можна ознайомитися на вкладці SCA на інформаційній панелі Wazuh.
- Сповіщення про зміни стану SCA. Попередження надходять лише про зміни стану та нові перевірки, щоб уникнути накопичення повторних сповіщень під час кожного нового сканування. Зміни стану оновлюються в базі даних менеджера Wazuh.
- Формат YAML для файлів політики. Політика CIS базується на еталонних показниках CIS.

SCA виконує сканування, щоб виявити ризики або неправильні конфігурації на контрольованих хостах. Ці сканування оцінюють конфігурацію хостів за допомогою файлів політики, які містять правила, які потрібно перевірити на фактичну конфігурацію хоста. Наприклад, SCA може оцінити, чи потрібно змінити конфігурацію, пов’язану з паролем, видалити непотрібне програмне забезпечення, вимкнути непотрібні служби або перевірити конфігурацію стеку TCP/IP.

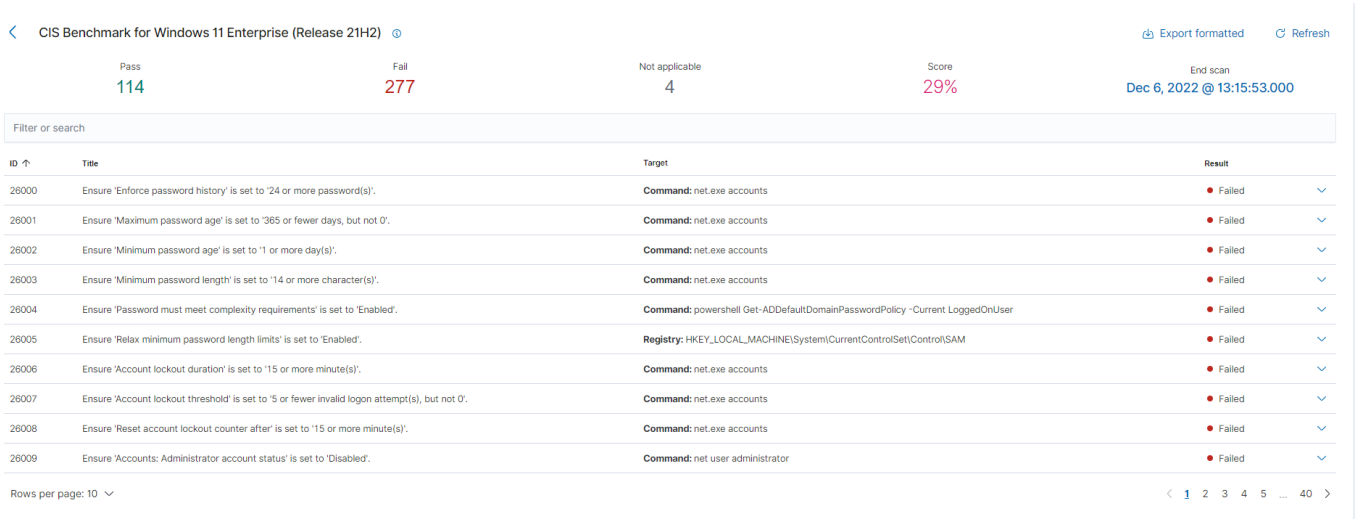

Рис. 2.12 Звіт сканування SCA

- Моніторинг політики безпеки

Моніторинг політики — це процес перевірки відповідності всіх систем набору попередньо визначених правил щодо параметрів конфігурації та схваленого використання програм.Для виконання цього завдання Wazuh використовує три компоненти: Rootcheck , OpenSCAP і CIS-CAT.

1. Rootcheck:

Починаючи з Wazuh v3.9.0, новий модуль SCA замінює Rootcheck під час моніторингу політики. Wazuh відстежує конфігураційні файли, щоб переконатися, що вони відповідають вашим політикам безпеки, стандартам або посібникам із захисту. Агенти виконують періодичне сканування, щоб виявити програми, які, як відомо, є вразливими, невиправленими або неправильно налаштованими.

Механізм rootcheck може виконувати такі перевірки:

- Перевірка чи запущений процес;
- Перевірка наявності файлу;
- Перевірка чи вміст файлу містить шаблон, наявність рядків у реєстрі.

2. OpenSCAP

OpenSCAP wodle — це інтеграція OpenSCAP із Wazuh HIDS , яка надає можливість виконувати конфігурацію та сканування вразливостей агента. Він в основному використовується для:

- Перевірка відповідності вимогам безпеки: політики OpenSCAP визначають вимоги, яким мають відповідати всі системи в організації, щоб відповідати застосовним політикам безпеки та/або тестам безпеки.

- Виконання оцінки вразливості: OpenSCAP визначає та класифікує вразливості в системі.
- Виконання спеціалізованих оцінок: OpenSCAP може виконувати спеціальні системні перевірки (тобто перевіряти підозрілі імена файлів і підозрілі розташування файлів).

Протокол автоматизації вмісту безпеки (SCAP) — це специфікація для вираження та маніпулювання даними безпеки стандартизованими способами. SCAP використовує кілька специфікацій для автоматизації безперервного моніторингу, керування вразливими місцями та звітування про результати сканування відповідності вимогам безпеки.

Компоненти процесу оцінки відповідності безпеки:

Сканер SCAP: це програма, яка читає політику SCAP і перевіряє, чи відповідає система їй. Існує багато інструментів для сканування систем на відповідність політикам SCAP. Сканер Wazuh є інтеграцією з NIST-сертифікованим сканером під назвою OpenSCAP .

Політики безпеки (вміст SCAP): вони визначають, як потрібно налаштувати систему та що перевіряти. Ці політики містять описи правил, яких ваша система має дотримуватися.

Профілі: кожна політика безпеки може містити кілька профілів, які надають набори правил і значень відповідно до конкретного базового рівня безпеки. Ви можете розглядати профіль як певну підмножину правил у політиці; профіль визначає, які правила, визначені в політиці, будуть фактично використані та які значення використовуватимуться під час оцінювання.

Оцінка (сканування): це процес, який сканер OpenSCAP виконує на агенті відповідно до певної політики безпеки та профілю. Зазвичай це займає лише кілька хвилин, залежно від кількості правил, вибраних у профілі.

3. Інтеграція CIS-CAT:

CIS-CAT було розроблено з метою інтеграції порівняльних оцінок CIS в агенті Wazuh.

CIS (Центр Інтернет-безпеки) – це організація, яка займається захистом приватних і державних організацій від кіберзагроз. Ця організація надає вказівки щодо порівняльних показників CIS, які є визнаним світовим стандартом і передовими методами захисту IT-систем і даних від кібератак.

Крім того, CIS-CAT Pro — це «міжплатформенна програма Java», розроблена для сканування цільових систем і створення звіту, що порівнює налаштування системи з контрольними тестами CIS. Існує понад 80 тестів CIS, які охоплюють майже всі ОС, забезпечуючи різні профілі залежно від конкретних потреб.

- Командний моніторинг

Бувають випадки, коли вам може знадобитися стежити за речами, яких немає в журналах. Щоб вирішити цю проблему, Wazuh містить можливість відстежувати вихідні дані певних команд і розглядати вихідні дані так, ніби це вміст файлу журналу.

Агенти мають можливість виконувати команди, що надходять від менеджера (через файли в поширеному каталозі). Після налаштування системи для моніторингу вихідних даних команди так, ніби це дані журналу, можна створити власні правила, як, наприклад, для аналізу журналу , щоб обробити вихідні дані та ініціювати сповіщення, коли критерії сповіщення відповідають.

- Активне реагування

Активні відповіді виконують різноманітні контрзаходи для усунення активних загроз, наприклад блокування доступу до агента з джерела загрози, коли виконуються певні критерії.

Активні відповіді виконують сценарій у відповідь на ініціювання певних сповіщень на основі рівня сповіщень або групи правил. Будь-яка кількість сценаріїв може бути ініційована у відповідь на тригер, однак ці відповіді слід ретельно розглядати. Погане виконання правил і відповідей може збільшити вразливість системи.

- Інвентаризація системи

Агенти Wazuh можуть збирати цікаву системну інформацію та зберігати її в базі даних SQLite для кожного агента на стороні менеджера. За це завдання відповідає модуль Syscollector.

Як зазначалося вище, основна мета цього модуля полягає в зборі найбільш релевантної інформації з контрольованої системи. Після запуску агента Syscollector періодично сканує визначені цілі (обладнання, ОС, пакети тощо), пересилаючи нещодавно зібрані дані менеджеру, який оновлює відповідні таблиці бази даних.

Інвентар агента збирається для різних цілей. Весь інвентар можна знайти на вкладці інвентаризації Wazuh APP для кожного агента, за допомогою запиту Wazuh API для отримання даних із БД. Також доступна вкладка Інструменти розробника . За допомогою цієї функції Wazuh API можна напряму запитувати про можливість фільтрації різних сканувань за будь-яким потрібним полем. Крім того, інвентар пакетів і виправлень використовується як канал для модуля виявлення вразливостей.

- Безагентний моніторинг

Моніторинг без агентів дозволяє контролювати пристрої або системи без агента через SSH, такі як маршрутизатори, брандмауери, комутатори та системи Linux/BSD. Це дозволяє користувачам із обмеженнями щодо встановлення програмного забезпечення відповідати вимогам безпеки та відповідності.

Сповіщення запускатимуться, коли змінюється контрольна сума на виведених даних, і відображатимуть або контрольну суму, або точний результат зміни.

3 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

3.1. Розгортання та конфігурація системи управління захистом кінцевих точок корпоративної інформаційної системи на базі Wazuh

Розгортання Wazuh версії 4.3 буде проводитись на віртуальній машині VMWare з операційною системою CentOS 7.

Порядок встановлення:

1. Індексатор Wazuh;
2. Сервер Wazuh;
3. Інформаційна панель Wazuh;
4. Розгортання клієнтів Wazuh.
   - Встановлення індексатора Wazuh.

Процес встановлення ділиться на три етапи.

1. Початкова конфігурація;

На цьому етапі необхідно вказати конфігурацію розгортання, створити сертифікати SSL для шифрування зв’язку між компонентами Wazuh і згенерувати випадкові паролі для захисту зв’язку.

Виконані команди для завантаження інсталятора Wazuh і файлу конфігурації.

curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh

curl -sO https://packages.wazuh.com/4.3/config.yml

Після чого редагуємо ./config.yml та заміняємо імена вузлів і IP-адреси на необхідні нам. Цю дію необхідно зробити для кожного вузла сервера, індексатора і інформаційної панелі Wazuh у випадку розгортання в режимі кластера.

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: WS-1
      ip: <172.17.142.202>
    #- name: node-2
    #  ip: <indexer-node-ip>
    #- name: node-3
    #  ip: <indexer-node-ip>
```

Так як ми проводимо розгортання в режимі одновузлового кластера, нам потрібно вказати лише одну IP-адресу поточного сервера, решту закоментовуємо.

Далі запускаємо помічника з опцією –generate-config-files для генерації ключа кластера Wazuh, сертифікатів і паролів, необхідних для встановлення індексатора. Ці файли розміщуються в каталозі ./wazuh-install-files.tar

```
# bash wazuh-install.sh --generate-config-files
```

При необхідності розгорнути багатовузловий кластер, ці файли необіхдно буде скопіювати на всі сервери розподіленого розгортання.

2. Встановлення вузлів індексатора Wazuh;

Встановлення вузлів індексатора проводимо за допомогою команди інсталятора.

```
# curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh
```

Далі запускаємо інсталятор з опцією --wazuh-indexer та назвою вузла, щоб установити та налаштувати індексатор Wazuh. Ім’я вузла має збігатися з ім’ям яке ми вказували у файлі config.yml на початку інсталяції – WS-1.

3. Ініціалізація кластера.

Останній етап інсталяції одновузлового кластера індексатора Wazuh складається із запуску сценарію адміністратора безпеки.

Запускаємо файл інсталятора з опцією --start-cluster на нашому вузлі індексатора, щоб завантажити інформацію про нові сертифікати і запустити кластер.

bash wazuh-install.sh --start-cluster

Ініціалізація кластера відбувається лише один раз, немає необхідності запускати цю команду на кожному вузлі.

- Встановлення сервера Wazuh

1. Завантажуємо файли інсталятора сервера Wazuh за допомогою команди:

curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh

Далі запускаємо інсталятор з опцією --wazuh-server, після якої вказуємо назву вузла. Ім’я вузла має збігатися з іменем вказаним раніше у файлі початкової конфігурації config.yml, в нашому випадку це WS-1.

bash wazuh-install.sh --wazuh-server wazuh-1

2. Для налаштування Filebeat необіхдно попередньо завантажити налаштований файл конфігурації.

curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.3/tpl/wazuh/filebeat/filebeat.yml

Наступним кроком редагуємо файл конфігурації який розташований за шляхом /etc/filebeat/filebeat.yml. Так як в нашому випадку сервер розташований на віртуальній машині, міняти адресу хоста яка за замовчуванням є localhost нам непотрібно.

Створюємо сховище ключів Filebeat для безпечного зберігання облікових даних автентифікації.

filebeat keystore create

Завантажуємо шаблон сповіщень для індексатора Wazuh.

curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/4.3/extensions/elasticsearch/7.x/wazuh-template.json

chmod go+r /etc/filebeat/wazuh-template.json

Встановлюємо модуль Wazuh для Filebeat.

curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.2.tar.gz | tar -xvz -C /usr/share/filebeat/module

3. Розгортання сертифікатів проводимо за допомогою заміни імені сертифіката вузла сервера Wazuh <server-node-name>, яке знаходиться у файлі конфігурації config.yml.

4. Запускаємо службу Filebeat.

systemctl daemon-reload

systemctl enable filebeat

systemctl start filebeat

Для перевірки виконуємо наступну команду, щоб переконатися, що Filebeat успішно установлено.

filebeat test output.

Рис. 3.1 Вивід команди filebeat test output

За результатами виводу, встановлюємо що серверний вузол Wazuh успішно встановлено. Якщо розгортання ведеться в режимі багатокластерного вузла, ці етапи необхідно повторити на кожному з вузлів. В нашому випадку використовується одновузловий кластер, тому можна переходити до наступного кроку.

- Встановлення інформаційної панелі

1. Встановлення залежностей пакетів

За допомогою команди, встановлюємо наступні пакети.

yum install libcap

2. Встановлення інформаційної панелі.

yum -y install wazuh-dashboard

3. Налаштування інформаційної панелі Wazuh починається з редагування файлу opensearch_dashboards.yml і заміни таких значень:

- server.host: цей параметр визначає хост сервера інформаційної панелі Wazuh. Щоб дозволити віддаленим користувачам підключатися,

необхідно встановити значення IP-адреси або DNS-ім’я сервера інформаційної панелі. Значення 0.0.0.0 прийматиме всі доступні IP-адреси хоста.

- opensearch.hosts: URL-адреси екземплярів індексатора Wazuh для використання всіх запитів. Інформаційну панель Wazuh можна налаштувати для підключення до кількох вузлів індексатора Wazuh в одному кластері. Адреси вузлів можна розділяти комами. Наприклад:

"https://10.0.0.2:9200", "https://10.0.0.3:9200",https://10.0.0.4:9200

4. Розгортання сертифікатів.

Для створення сертифікатів потрібно замінити ім’я вузла інформаційної панелі Wazuh <dashboard-node-name> на те, яке було задано раніше і використовується у файлі config.yml, після чого перемістити сертифікати у відповідне місце.

Рис. 3.2 Налаштований файл opensearch_dashboards.yml

NODE_NAME=<wazuh-wui>

Після чого послідовністю команд, переміщаємо сертифікати в директорію призначену для них.

mkdir /etc/wazuh-dashboard/certs

tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/ ./$NODE_NAME.pem ./$NODE_NAME-key.pem ./root-ca.pem

mv -n /etc/wazuh-dashboard/certs/$NODE_NAME.pem /etc/wazuh-dashboard/certs/dashboard.pem

mv -n /etc/wazuh-dashboard/certs/$NODE_NAME-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem

chmod 500 /etc/wazuh-dashboard/certs

chmod 400 /etc/wazuh-dashboard/certs/*

chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs

5. Запуск служби інформаційної панелі Wazuh.

Додамо параметри автозапуску за допомогою Systemd.

systemctl daemon-reload

systemctl enable wazuh-dashboard

systemctl start wazuh-dashboard

6. Отримання доступу до веб-інтерфейсу Wazuh за допомогою облікових даних.

Виконуємо команду # ip a для того щоб отримати IP-адресу веб-інтерфейсу сервера.

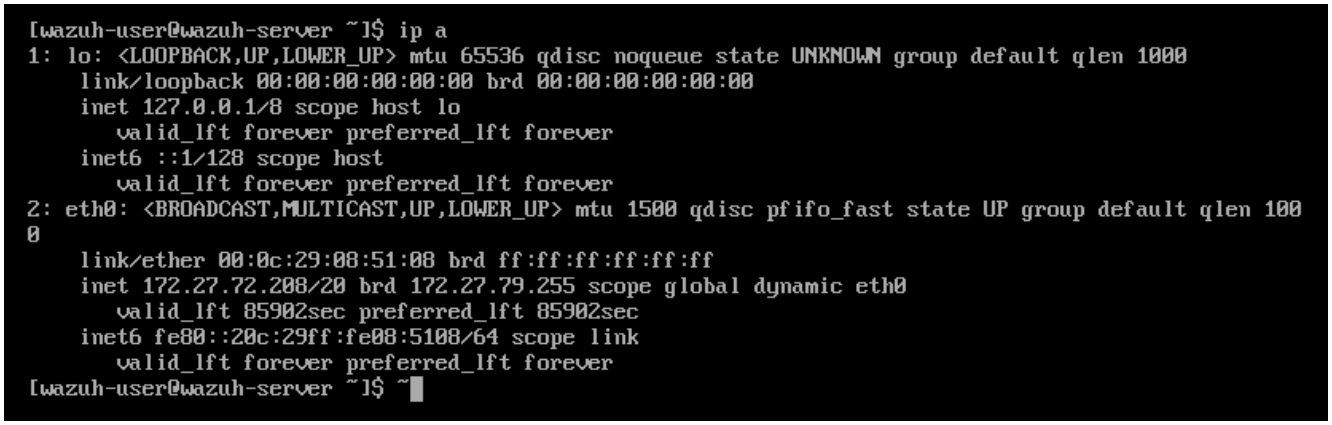

Рис. 3.3 Вивід команди ip a

Як можна бачити на скріншоті, веб-інтерфейс знаходиться за адресою “172.27.72.208”.

Для входу на веб-інтерфейс використовуємо наступні данні. Потрібно зазначити що облікові дані є встановленими системою за замовчуванням.

- URL: https://172.27.72.208
- Ім’я користувача: admin
- Пароль: admin

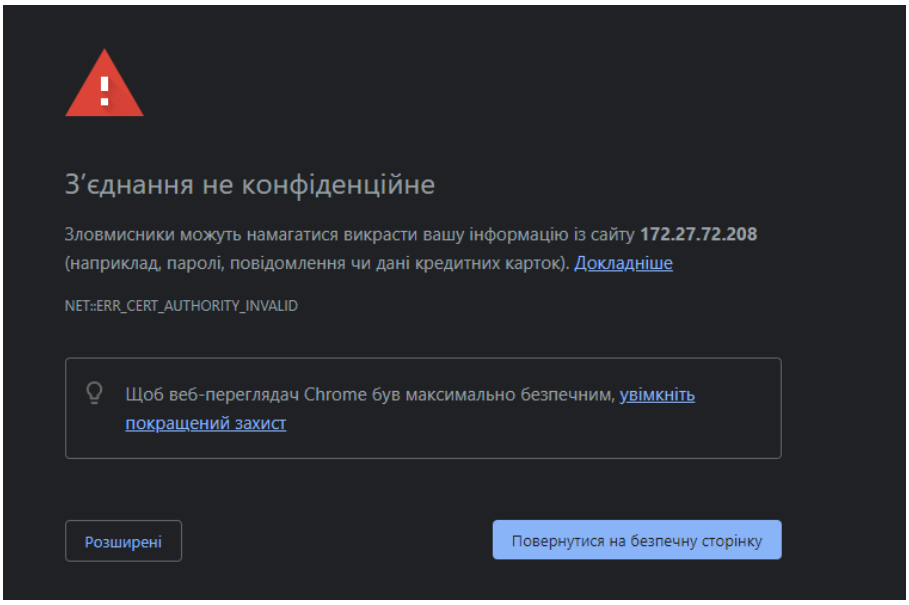

Рис. 3.4 Спроба доступу до інформаційної панелі

Коли ми вперше отримуємо доступ до інформаційної панелі Wazuh, браузер показує попередження про те, що сертифікат не був виданий довіреним центром. Виняток можна додати в розширених параметрах веб-браузер. Для підвищення безпеки, можна імпортувати в менеджер сертифікатів браузера попередньо згенерований файл root-ca.pem. Крім того можна налаштувати сертифікат від надійного центру.

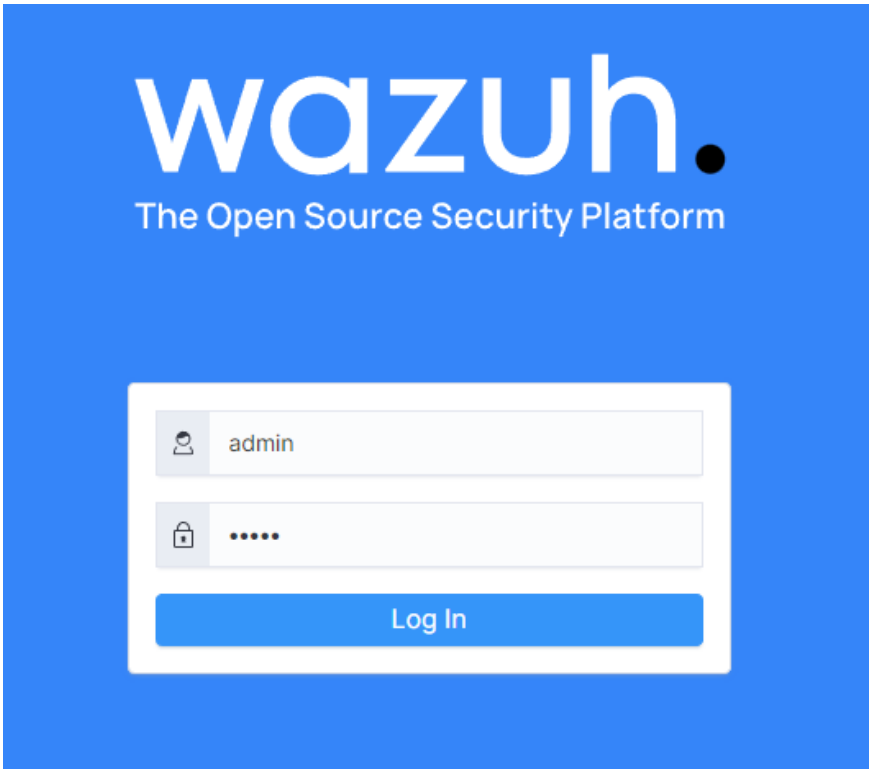

Рис. 3.5 Вікно авторизації інформаційної панелі

Після того як ми отримали доступ до сторінки, авторизуємся за допомогою даних вказаних вище.

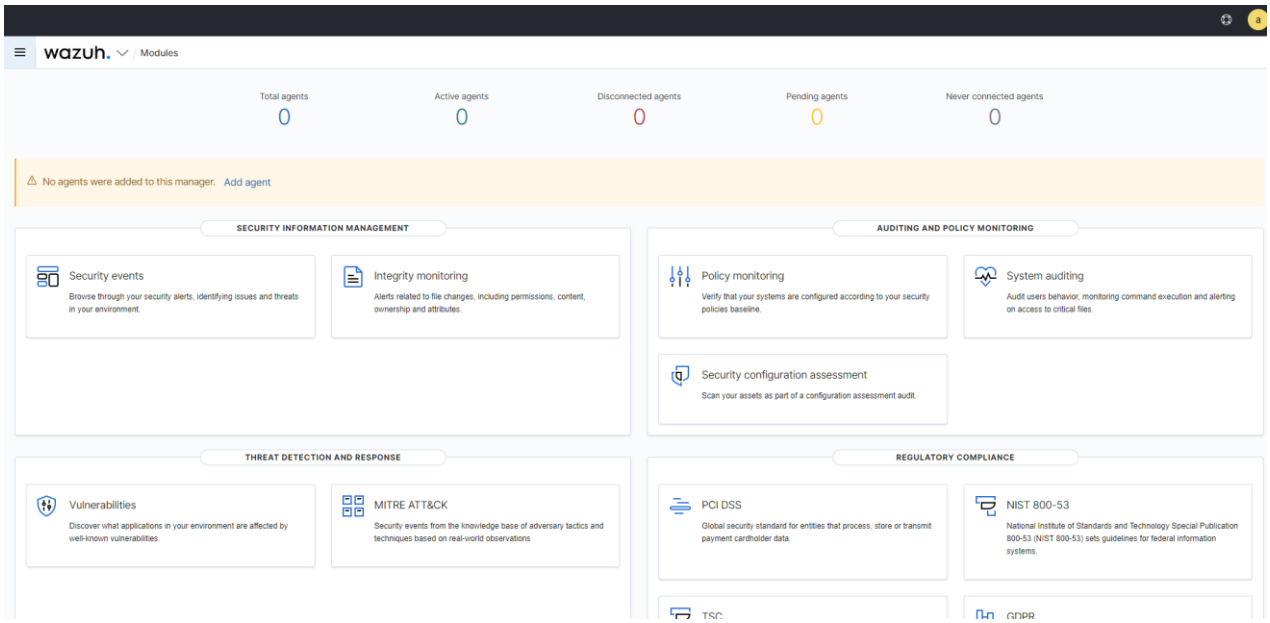

Рис. 3.6 Головна сторінка інформаційної панелі Wazuh

Для того щоб пересвідчитись що сервер працює і немає помилок, заходимо в меню Settings > Wazuh API Configuration, де можна перевірити підключення і статус сервера.

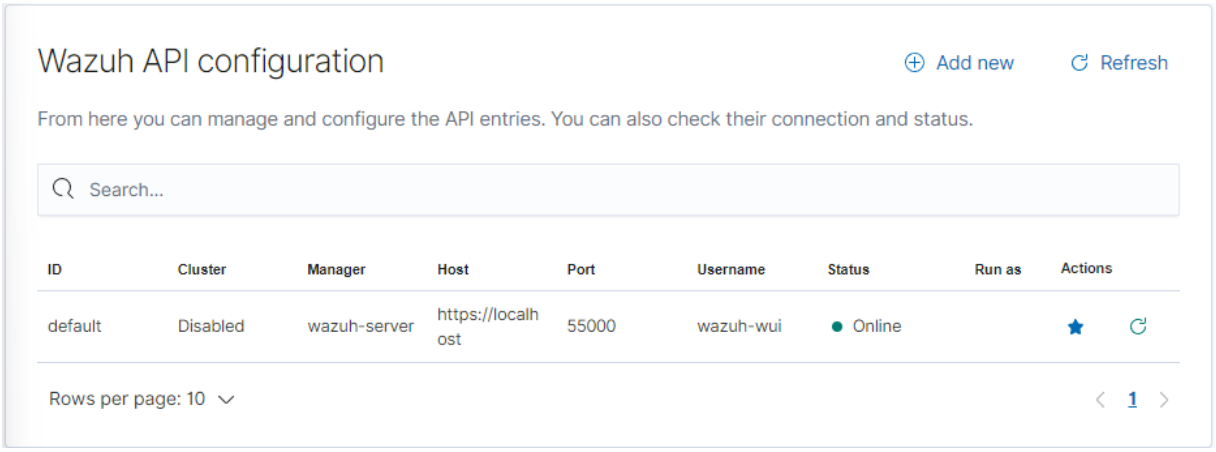

Рис. 3.7 Меню конфігурації API

Як можна побачити, сервер запущений і успішно функціонує.

Важливо підмітити, що після встановлення і налаштування всіх центральних компонентів Wazuh, рекомендується змінити облікові дані за замовчуванням, щоб захистити інфраструктуру від можливих атак. Виконуємо команду: # /usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh --change-all --admin-user wazuh --admin-password wazuh, після чого отримуємо нові згенеровані паролі.

Середовище Wazuh тепер готове, і можна продовжувати інсталяцію агента Wazuh, на кінцевих точках які потрібно контролювати.

- Розгортання агентів на кінцевих точках

Розгортання агентів буде проводитись на трьох кінцевих точках: Робоча станція під керуванням Windows 11, робоча станція під керуванням Ubuntu 22.04, та пристрій під керуванням Debian Linux.

1. Переходимо на інформаційну панель Wazuh, та обираємо меню Agents. Далі необхідно обрати бажаний тип операційної системи де буде проводитись розгортання агента.

Так як сервер знаходиться на віртуальній машині, в якості IP-адреси вказуємо “192.168.0.152”, назначаємо групу за замовчуванням “default” та створену нами групу “windows”.

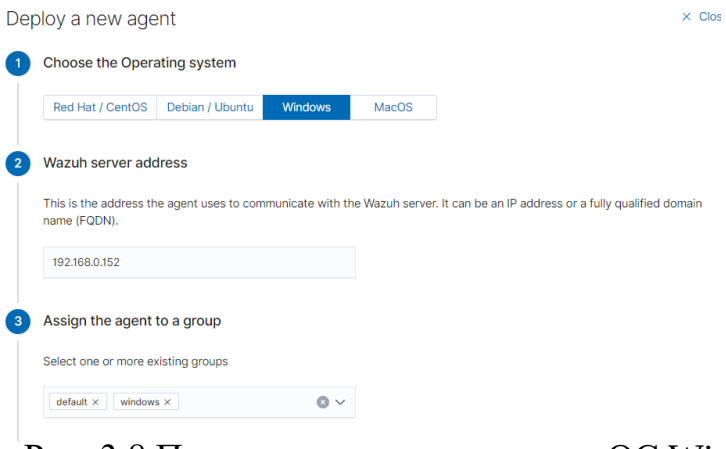

Рис. 3.8 Параметри розгортання для ОС Windows

Отримуємо команду, яку потрібно виконати через Windows PowerShell з використанням прав адміністратора.

Запускаємо PowerShell з правами адміністратора, де виконуємо команду. Після чого запускаємо агент командою “NET START WazuhSvc”.

```
PS C:\Windows\System32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/w
azuh-agent-4.3.10-1.msi -OutFile ${env:tmp}\wazuh-agent-4.3.10.msi; msiexec.exe /i ${en
v:tmp}\wazuh-agent-4.3.10.msi /q WAZUH_MANAGER='192.168.0.152' WAZUH_REGISTRATION_SERVE
R='192.168.0.152' WAZUH_AGENT_GROUP='default'
PS C:\Windows\System32> NET START WazuhSvc
The requested service has already been started.
```

Рис. 3.9 Команда PowerShell для розгортання агента

Для систем на Debian та Ubuntu виконуємо команди, які менеджер надав відповідно з вимогами.

Для Debian:

```
# curl -so wazuh-agent-4.3.10.deb
https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.3.10-
1_armhf.deb && sudo WAZUH_MANAGER='192.168.0.152'
WAZUH_AGENT_GROUP='default,debian' dpkg -i ./wazuh-agent-4.3.10.deb
```

Для Ubuntu:

```
# curl -so wazuh-agent-4.3.10.deb
https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.3.10-1_amd64.deb && sudo WAZUH_MANAGER='192.168.0.152' WAZUH_AGENT_GROUP='default,debian' dpkg -i ./wazuh-agent-4.3.10.deb
```

Тепер необхідно перевірити в інформаційні панелі, чи відображаються всі розгорнуті агенти в менеджері Wazuh, правильність встановлених груп.

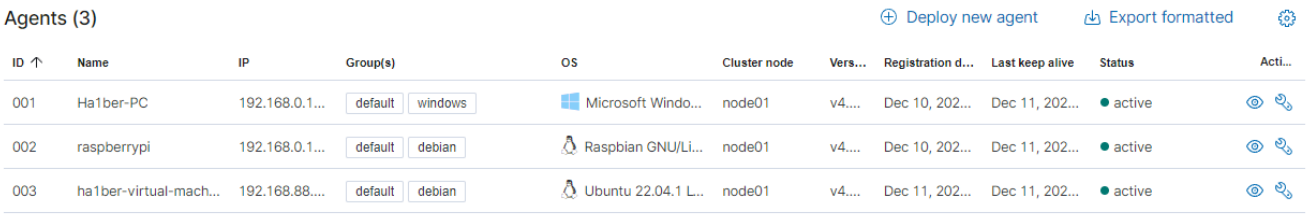

Рис. 3.10 Архітектура середовища Wazuh

Як можна побачити на скріншоті, всі агенти були успішно розгорнуті та підключені до менеджера, вказані групи встановлені правильно.

Потрібно підкреслити той факт, що навіть без детальної конфігурації, моніторинг в автоматичному режимі почав сканувати і перевіряти підключені агенти стандартними утилітами.

3.2. Технологія управління захистом кінцевих точок з Wazuh

Після розгортання агентів, переходимо до технології управління захистом кінцевих точок на яких вони розгорнуті. На головній панелі Wazuh, можна побачити перелічені в другому розділі модулі. Вони здатні забезпечити повноцінний захист кінцевої точки від можливих загроз.

- Контроль цілісності файлів
- Виявлення атаки грубою силою/активна протидія
- Виявлення вразливостей
- Виявлення та видалення шкідливих файлів та програм

Перевірка кожної із вищенаведених функцій захисту будемо проводити поетапно на кінцевих точках Windows та Ubuntu.

Побудова технології управління буде базуватися виключно на реальних сценаріях використання системи. На рисунку нижче зображено архітектуру середовища, в якому будуть проводитись дослідження функціоналу системи.

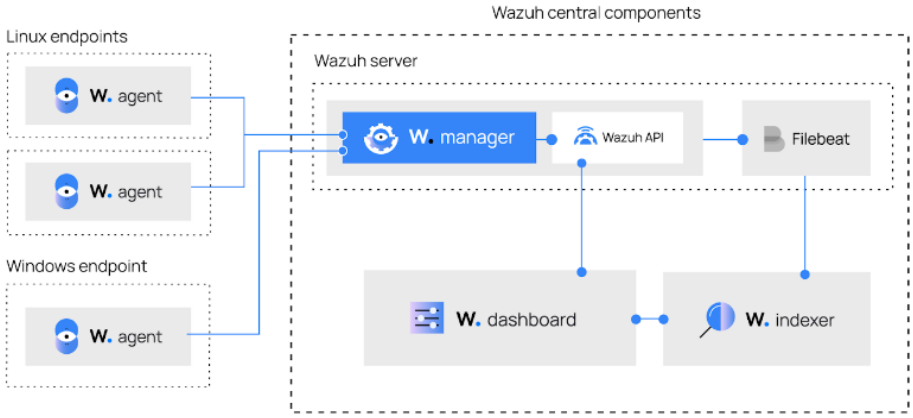

Рис. 3.11 Архітектура середовища Wazuh

Така архітектура використовується, тому що центральні компоненти Wazuh (сервер, індексатор і інформаційна панель) працюють в одній системі. Це пояснюється тим, що ми відстежуємо невелике середовище і немає потреби в розподіленій архітектурі.

1. Моніторинг цілісності файлів допомагає перевіряти конфіденційні файли та відповідати нормативним вимогам. Wazuh має вбудований модуль FIM, який відстежує зміни файлової системи, щоб виявити створення зміну та видалення файлів.

В нашому варіанті використання, Wazuh FIM буде виявляти зміни в контрольованих каталогах на кінцевих точках Ubuntu і Windows. Wazuh отримує інформацію про користувача і процес, які внесли зміни, за допомогою функціональності who-data-audit.

Для початку необхідно налаштувати агенти Wazuh для моніторингу змін файлової системи. У випадку Ubuntu це /root каталог. Для Windows – буде C:\Users\Administrator\Desktop. Для налаштування моніторингу, необхідно відредагувати файли конфігурацій агентів Wazuh на обох кінцевих точках.

У файлі конфігурації ossec.conf, активуємо розділ <Files integrity monitoring>, всередині блоку <syscheck> додаємо каталоги для моніторингу, після чого перезапускаємо агенти.

```
<!-- File integrity monitoring -->
<syscheck>
   <directories check_all="yes" report_changes="yes" realtime="yes">C:\Users\<mvdov>\Desktop</directories>
  <disabled>no</disabled>
```

Рис. 3.12 Приклад відредагованого файлу під каталог Windows

Після перезавантаження, перевіряємо роботу модуля. У вказаному для моніторингу каталозі створюємо файл під назвою “confidential.txt”, додаємо в нього вміст, після чого видаляємо. В результаті має з’явитися три сповіщення про три різних дії.

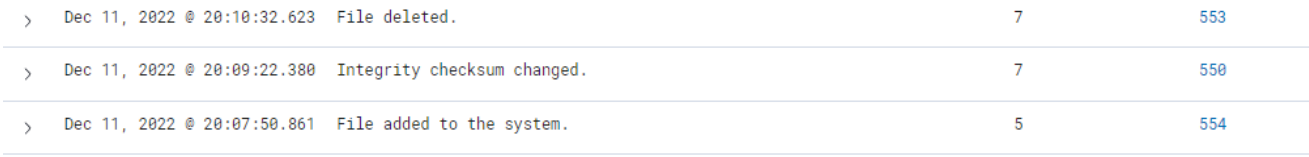

Рис. 3.13 Сповіщення про зміну, редагування та видалення файлу

При необхідності, ми можемо подивитися детальний звіт по кожній із подій.

Рис. 3.14 Детальний звіт про зміну файла

Файл звіту містить в собі всі необхідні для адміністратора дані. В тому числі точне місцерозташування файлу, користувача який виконав зміну, та символи які були змінені.

2. Активна протидія дозволяє Wazuh запускати команди для агента, у відповідь на певні тригери. У цьому випадку, ми моделюємо атаку методом грубої сили на SSH і налаштовуємо активну протидію для блокування IP-адреси зловмисника.

Перш за все, нам потрібно знати, коли виконувати відповідь. Ми можемо скористатися одним із наступних варіантів:

- Ідентифікатор правила: відповідь буде виконано на будь-яку подію з визначеним ідентифікатором.
- Група правил: відповідь буде виконано на будь-яку подію у визначеній групі.
- Залежність від рівня: відповідь буде виконано на будь-яку подію з вказаним або вищим рівнем.

Тепер, коли ми знаємо умови спрацювання активної протидії, ми маємо визначити, що саме вона має робити. Гнучкість конфігурації дозволяє користувачу використовувати як сценарії представлені за замовчуванням, так і створювати власні. Згідно документації, використаємо функцію “firewall-drop” і створимо на її базі сценарій. Перевага обраної функції в тому, що для роботи вона використовує локальний брандмауер і працює з усіма поширеними операційними системами Linux/Unix.

Для налаштування сценарію, необхідно відкрити в редакторі файл конфігурації менеджера “ossec.conf”, який розташований по шляху “/var/ossec/etc/ossec.conf/”. В розділі <active-response> активуємо блок функції “firewall-drop”.

В налаштуванні Wazuh для запуску активної відповіді використовуються такі поля:

- command: попередньо визначена команда (firewall-drop)
- location: Місце виконання команди. Ми хочемо виконати команду на агенті який повідомив про подію, отже визначаємо його як це місце виконання.
- rules_id: команда виконується, якщо спрацьовує передбачене менеджером правило 5712.
- timeout: час на який буде заблокована IP-адреса.

Додаємо в файлі конфігурації, в розділі <active-response> в підрозділі опцій наступний блок:

```
<!--
<active-response>
 <command>firewall-drop</command>
 <location>local</location>
 <rules_id>5712</rules_id>
 <timeout>1800</timeout>
</active-response>
-->
```

Рис. 3.15 Блок опцій активної протидії

Після налаштування, перезапускаємо сервер Wazuh.

Тепер все готово для імітації SSH-атаки, яка буде виконана з 192.168.0.111 на наш агент, який працює на 192.168.0.150. Для початку перевіряємо чи є з’єднання між зловмисником і агентом:

```
pi@raspberrypi:~ $ ping -c 5 192.168.0.150
PING 192.168.0.150 (192.168.0.150) 56(84) bytes of data.
64 bytes from 192.168.0.150: icmp_seq=1 ttl=64 time=13.9 ms
64 bytes from 192.168.0.150: icmp_seq=2 ttl=64 time=6.31 ms
64 bytes from 192.168.0.150: icmp_seq=3 ttl=64 time=4.33 ms
64 bytes from 192.168.0.150: icmp_seq=4 ttl=64 time=10.2 ms
64 bytes from 192.168.0.150: icmp_seq=5 ttl=64 time=11.6 ms

--- 192.168.0.150 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 4.333/9.267/13.895/3.484 ms
```

Рис. 3.16 Перевірка зв’язку командою ping

Тепер ми кілька разів намагаємося підключитися до агента через SSH, використовуючи недійсного користувача. Використовуємо для цього утиліту Hydra і текстовий документ з паролями для грубої атаки.

Як можна бачити в журналі подій, спрацювало правило 5712 про спробу атаки грубою силою, яке в свою чергу викликало правило 651 активної протидії “firewall drop”. IP-адресу зловмисника було заблоковано на визначений в файлі конфігурації час.

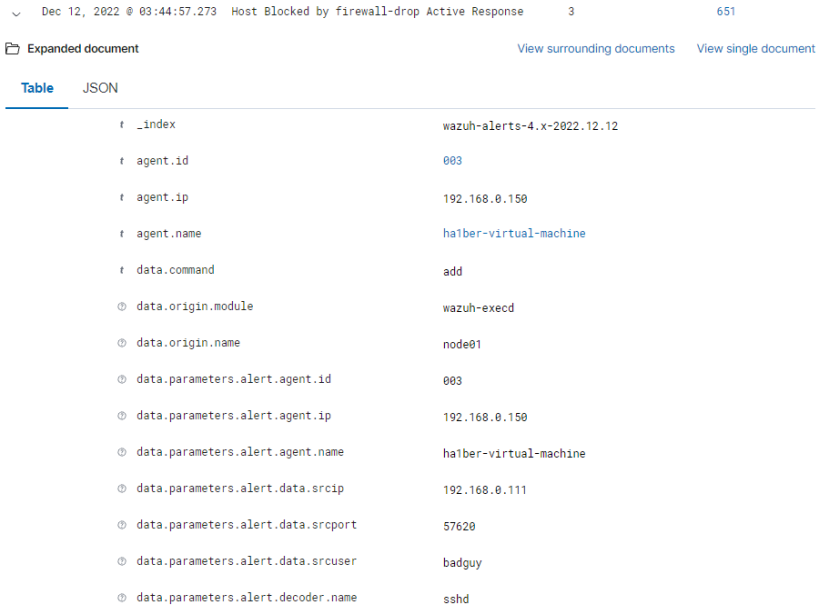

Рис. 3.17 Запис активної протидії в журналі подій

Далі спробуємо встановити зв’язок між пристроєм зловмисника і кінцевою точкою жертви за допомогою команди ping.

```
pi@raspberrypi:~ $ sudo hydra -l badguy -P passwords.txt 192.168.0.150 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-12 03:44:55
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:1/p:0), ~10 try per task
[DATA] attacking ssh://192.168.0.150:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-12 03:44:58
pi@raspberrypi:~ $ ping -c 5 192.168.0.150
PING 192.168.0.150 (192.168.0.150) 56(84) bytes of data.

--- 192.168.0.150 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4163ms
```

Рис. 3.18 Атака і спроба перевірки з’єднання після блокування

Як можна бачити на рисунку, перевірка агента від зловмисника неможлива, тому робимо висновок що активна протидія змогла заблокувати IP-адресу і вона працює належним чином.

3. Важливим елементом захисту кожної кінцевої точки є завчасне виявлення уразливостей. Wazuh використовує модуль Vulnerability Detector для виявлення враливостей у програмах і операційних системах, що працюють на кінцевих точках. Він періодично виконує сканування на виявлення вразливостей для програм і операційних систем на кожній контрольованій кінцевій точці.

Для початку, необхідно активувати модуль у файлі конфігурації, для тих операційних систем, на яких нам необхідно виявляти уразливості. Для цього на сервері Wazuh відкриваємо файл ossec.conf і вмикаємо модуль встановлюючи значення “yes” для тегу <enabled> для модуля Vulnerability Detector і кожної операційної системи яку ми збираємся сканувати.

```
<vulnerability-detector>
  <enabled>no</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>
```

Рис. 3.19 Ввімкнення модуля

Також дублюємо цю дію на блоки модуля для операційних систем.

Після цього, перевіряємо чи була автоматично створена база даних CVE, яка розташована за шляхом “/var/ossec/queue/vulnerabilities/cve.db”. Потрібно підкреслити, що залежно від мережі користувача, для завантаження бази даних уразливостей потрібен час. Також потрібно більше часу для сканування вразливих пакетів на контрольованій кінцевій точці.

Ми можемо візуалізувати дані сповіщень на інформаційній панелі Wazuh. Для цього, переходимо до модуля «Vulnerability Detector», обираємо агента та натискаємо на будь-яку вразливість.

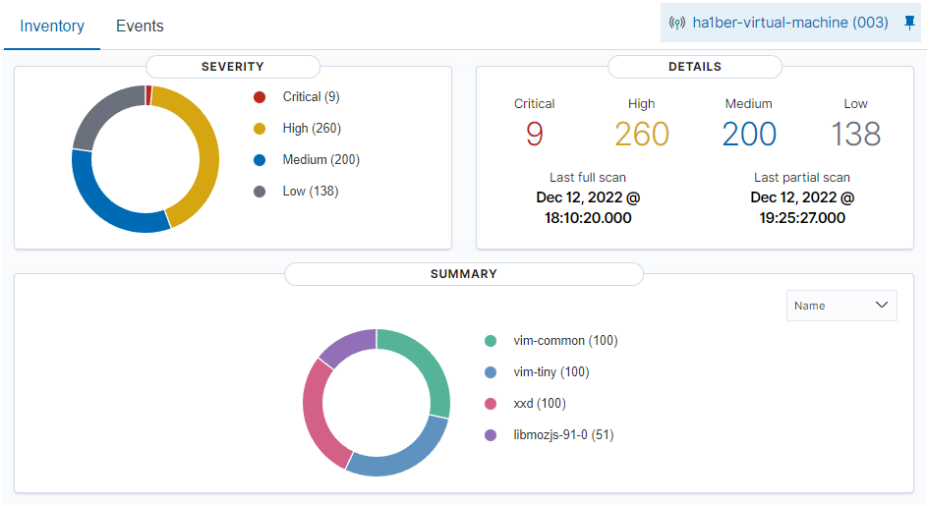

Рис. 3.20 Результати сканування вразливостей

Як можна бачити на рисунку, модуль виявлення вразливостей справився зі своєю задачею, та виявив уразливості. На інформаційній панелі результати подані у вигляді діаграми з розподіленням на тяжкість виявлених уразливостей. Далі ми

можемо подивитися деталі будь-якої з виявлених вразливостей. Дізнатися її класифікацію за CVE, та переглянути референсні посилання.

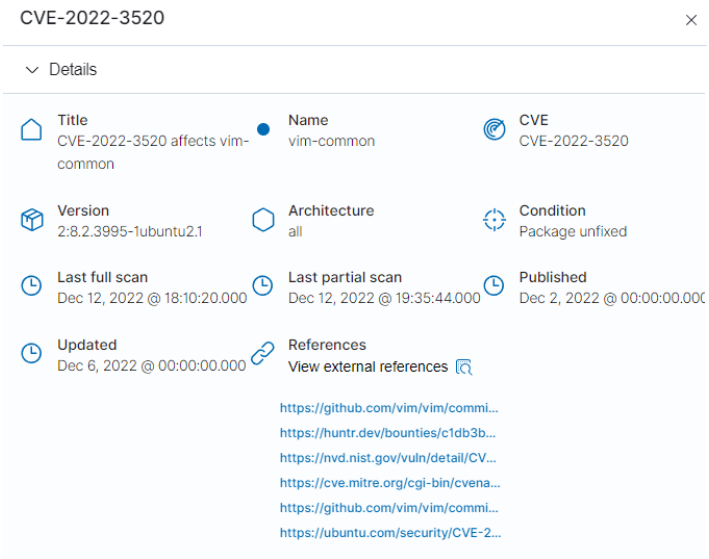

Рис. 3.21 Деталі виявленої вразливості

Як бачимо, згідно CVE, вразливість є відносно новою, тому це свідчить про актуальність бази даних вразливостей Wazuh.

4. Wazuh використовує модуль інтегратора для підключення до зовнішніх API та інструментів попередження, таких як VirusTotal.

У цьому випадку, ми використовуємо модуль Wazuh FIM для моніторингу каталогу на наявність змін і VirusTotal API для сканування файлів у каталозі. Потім налаштовуємо Wazuh на запуск сценарію активної відповіді та видалення файлів, які VirusTotal визначає як шкідливі. Тестувати цей варіант ми будемо на кінцевій точці Ubuntu. Хоча можливості конфігурації дозволяють налаштувати сканування для Windows та Unix систем.

Процес налаштування агента складається з того, що потрібно у файлі конфігурації ossec.conf налаштувати каталог для моніторингу в реальному часі. В нашому випадку ми будемо відстежувати /root каталог. Створюємо сценарій активної відповіді “remove_threat.sh”, який буде видаляти шкідливі файли з кінцевої точки. Після чого перезавантажуємо агент.

Сервер налаштовуємо наступним чином:

Додаємо правила до файлу конфігурації правил local_rules.xml на сервері Wazuh. Ці правила будуть попереджувати про зміни в каталозі /root, які були виявлені скануванням FIM.

```
<group name="syscheck,pci_dss_11.5,nist_800_53_SI.7,">
    <!-- Rules for Linux systems -->
    <rule id="100200" level="7">
      <if_sid>550</if_sid>
      <field name="file">/root</field>
      <description>File modified in /root directory.</description>
    </rule>
    <rule id="100201" level="7">
      <if_sid>554</if_sid>
      <field name="file">/root</field>
      <description>File added to /root directory.</description>
    </rule>
</group>

<group name="virustotal,">
  <rule id="100092" level="12">
    <if_sid>657</if_sid>
    <match>Successfully removed threat</match>
    <description>$(parameters.program) removed threat located at $(parameters.alert.data.virustotal$
  </rule>

  <rule id="100093" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
$ile)</description>
  </rule>
</group>
```

Рис. 3.22 Конфігурація local_rules.xml

Далі конфігуруємо файл ossec.conf, де створюємо блок <ossec_config> с модулем інтеграції virustotal. Використовуємо свій персональний ключ API VirusTotal. Це дозволяє запускати VirusTotal що разу, коли буде спрацьовувати будь-яке з правил 100201 або 100200.

Потім додаєм блоки, які стосуються активації активної відповіді, яка в свою чергу буде запускати раніше створений на контрольованому агенті сценарій “remove-threat.sh” коли VirusTotal позначатиме файл як шкідливий.

Для тестування працездатності, завантажимо тестовий файл EICAR до каталогу /root кінцевої точки Ubuntu. Після чого перевіряємо журнал подій по конкретній кінцевій точці.

	Time ▾	rule.description	rule.level	rule.id
›	Dec 13, 2022 @ 15:46:10.986	active-response/bin/remove-threat.sh removed threat located at /root/eicar.com	12	100092
›	Dec 13, 2022 @ 15:46:10.040	File deleted.	7	553
›	Dec 13, 2022 @ 15:46:09.908	VirusTotal: Alert - /root/eicar.com - 65 engines detected this file	12	87105
›	Dec 13, 2022 @ 15:46:07.523	File added to /root directory.	7	100201

Рис. 3.23 Реагування та видалення зараженого файлу

Як можна бачити, сповіщення було візуалізовано коректно. Час реакції з моменту додавання файлу до директорії /root та його видаленням склав 3,5 секунди, що є хорошим результатом для серверу який розгорнутий на віртуальній машині.

3.3. Розроблення рекомендацій щодо застосування технології управління захистом кінцевих точок корпоративної інформаційної системи

Згідно результатів аналізу та проведених досліджень технології. Можна розробити наступні рекомендації щодо застосування технології управління захистом на базі системи Wazuh.

1. Система Wazuh повністю відповідає нормативним вимогам PCI DSS, GDPR та HIPAA. Це робить систему повністю придатною для застосування в організаціях які застосовують процедури обробки інформації яка містить специфікації з необхідністю відповідати вище названим нормативним вимогам. Прикладом може слугувати NASA, де використовується Wazuh.
2. Так як Wazuh є системою з відкритим кодом, це дозволяє набагато точніше працювати з конфігурацією системи, що в свою чергу дозволяє адаптувати кожен індивідуальний сервер чітко під вимоги певної організації.
3. Підтримка кластерності дозволяє працювати з будь-якими обсягами клієнтів та обробляти необхідну кількість інформації.
4. Підтримка інтеграцій із зовнішніми API відкриває широкі можливості для постійного вдосконалення можливостей системи, також є можливість розробити інтеграцію із власним API організації якщо є така необхідність.
5. Підтримка агентом всіх поширених операційних систем що значно розширює охоплення можливих пристроїв організації.
6. Велике різноманіття способів розгортання серверної частини може відчутно скоротити витрати на серверне обладнання.
7. Підтримка інтеграції з хмарою Amazon AWS дозволяє встановлювати агент Wazuh на середовищах, а також моніторити служби AWS, для збору та аналізу даних інфраструктури.
8. Наявність хмарного середовища, що розміщує та керує всіма компонентами Wazuh на одній інтегрованій платформі. Гнучкість вибору середовищ

дозволяє обрати найбільш підходяще, середовище, опираючись на розміри та потреби організації.

9. Доволі детальна та зрозуміла документація, здатна значно знизити рівень помилок при налаштуванні і таким чином, знизити рівень можливих загроз від людського фактору.

ВИСНОВКИ

В ході роботи, було проаналізовано існуючі методи та засоби захисту кінцевих точок. Складена класифікація основних функціональних можливостей системи захисту кінцевих точок. У термінах запропонованої класифікації динамічні та гнучкі системи є найбільш актуальними та корисними в сучасних реаліях інформаційної безпеки.

Система управління захистом кінцевих точок це доволі гнучкий та мультифункціональний інструмент. Можливості які надає система, дозволяють доволі сильно покращити рівень безпеки та конфіденційності інформації в інформаційній системі організації. Варто підкреслити, що з плином часу еволюція можливих загроз, змушує так само стрімко розвиватися і всі можливі способи захисту від них. Вибір систем захисту кінцевих точок визначається топологією мережі, потрібними функціями захисту, а також особистими уподобаннями аналітика безпеки.

Попереджати порушення та їх наслідки, завжди було важким та комплексним завданням. Система управління захистом кінцевих точок, дозволяє спеціалісту значно розширити вже наявні можливості по захисту кінцевих точок. Звісно робити висновок, що система захисту кінцевих точок це єдине що необхідно для захисту інформаційної системи, не можна. Система захисту кінцевих точок, в решті решт, є одною з багатьох елементів в ланцюгу захисту інформаційної системи. Важливим елементом функціонування системи є фахівець з безпеки. Саме він керує всією безпекою. Тому навіть при найкращій системі захисту, варто розуміти, що без досвідченого спеціаліста, не можна гарантувати повний і беззаперечний захист. Система Wazuh це дуже гнучкий та потужний інструмент захисту інформації, завдяки своєму обсягу налаштувань та варіантів розгортання він може бути адаптований до роботи в будь-яких умовах, тому у випадку пошуку систем захисту кінцевих точок, однозначно система Wazuh варто того, щоб її розглянути.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про захист інформації в інформаційно телекомунікаційних системах».

2. Microsoft. Види шкідливого програмного забезпечення [Електронний ресурс] – Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-malware

3. Gonak I. PERSONAL CYBER DEFENSE OF THE CRYPTOCURRENCY BUSINESS ECONOMIC ENTITY. Scientific Notes of Ostroh Academy National University, "Economics" Series. 2021. T. 1, № 23(51). C. 23–28.

4. K. Scarfone, P. Mell, Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS), National Institute of Standards and Technology (NIST) (2007).

5. Захист кінцевих точок, EDR - iIT Distribution. iIT Distribution. [Електронний ресурс] – Режим доступу: https://iitd.com.ua/zashchita-konechnyh-tochek/ (дата звернення: 12.12.2022).

6. Snell M. M., Pruitt C. J., Curran K. L. F. Toxic Endpoint Analysis. Office of Scientific and Technical Information (OSTI), 2016.

https://www.bytemag.ru/articles/detail.php?ID=6850&sphrase_id=3833171.

7. What Is Endpoint Detection and Response? EDR Security Trellix [Електронний ресурс] – Режим доступу: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.

8. What is Endpoint Security? CrowdStrike. [Електронний ресурс] – Режим доступу: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/

9. CCNP Security: Intrusion Prevention and Intrusion Detection Systems [Електронний ресурс] – Режим доступу: https://www.ciscopress.com/articles/article.asp?p=1763920&seqNum=2.

10. Endpoint Protection Solutions: Cybersecurity & Threat Intelligence Services [Електронний ресурс] – Режим доступу:

https://www.webroot.com/us/en/resources/tips-articles/endpoint-protection-solutions-why-the-traditional-model-is-broken

11. Офіційний сайт проекту Wazuh [Електронний ресурс] – Режим доступу: https://wazuh.com/

12. Офіційний сайт документації Wazuh [Електронний ресурс] – Режим доступу: https://documentation.wazuh.com/current/index.html

13. Gillis A. S., Rosencrance L. What is SIEM? [Електронний ресурс] – Режим доступу: https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM

14. What is XDR?. Palo Alto Networks. [Електронний ресурс] – Режим доступу: https://www.paloaltonetworks.com/cyberpedia/what-is-xdr

15. Wazuh Reviews, Competitors and Pricing. Buying Intelligence and Reviews for Enterprise Technology. PeerSpot. [Електронний ресурс] – Режим доступу: https://www.peerspot.com/products/wazuh-reviews