ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Розробка системи моніторингу вразливостей та перевірки відповідності стандартам безпеки з використанням Wazuh для малого та середнього бізнесу»

на здобуття освітнього ступеня магістра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ _____
(підпис) Ім'я, ПРІЗВИЩЕ здобувача

Виконав: Ігор СИНІЙ
здобувач вищої освіти
група ІСДМ-64

Керівник: Сергій СОЛОМАХА
науковий ступінь, вчене звання к.е.н., доцент

Рецензент:
науковий ступінь, вчене звання _____
Ім'я, ПРІЗВИЩЕ

Київ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Інформаційних систем та технологій
Ступінь вищої освіти Магістр
Спеціальність Інформаційні системи та технології
Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІСТ
Каміла СТОРЧАК
«____» _____20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Синьому Ігорю Ананійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Розробка системи моніторингу вразливостей та перевірки відповідності стандартам безпеки з використанням Wazuh для малого та середнього бізнесу»

керівник кваліфікаційної роботи Сергій СОЛОМАХА, к. е. н., доцент
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15» жовтня 2024 року №320.

2. Строк подання кваліфікаційної роботи 27 грудня 2024 року.

3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, офіційна документація WAZUH, стандарти безпеки.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження галузевих стандартів кібербезпеки
2. Аналіз можливості використання продукту WAZUH для аудиту стану кібербезпеки підприємства

3. Розробка процесу встановлення та запуску продукту WAZUH

5. Перелік графічного матеріалу: *презентація*
1. Використання SIEM-продуктів для аудиту кібербезпеки
2. Технічні особливості розгортання продукту WAZUH в гетерогенному середовищі операційних систем
3. Автоматизована система передачі оповіщень продукту Wazuh

6. Дата видачі завдання15 жовтня 2024 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз галузевих стандартів кібезрбезпеки	19.10-05.11.24	Виконано
2	Порівняльний аналіз засобів автоматизованого аудиту кібербезпеки робочих станцій	05.11-12.11.24	Виконано
3	Перевірка можливостей розгортання продукту Wazuh для вибраного бізнес-замовника	13.11-19.11.24	Виконано
4	Вибір схеми встановлення продукту Wazuh	20.11-25.11.24	Виконано
5	Тестове розгортання продукту Wazuh	27.11-03.12.24	Виконано
6	Практичне розгортання продукту Wazuh на стороні бізнес-замовника	04.12-10.12.24	Виконано
7	Оформлення наукової роботи: вступ, висновки, реферат	11.12-20.12.24	Виконано
8	Розробка презентаційних матеріалів	21.12-26.12.24	Виконано

Здобувач вищої освіти _____ Ігор СИНІЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Сергій СОЛОМАХА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 70 стор., 30 рис., 10 табл., 32 джерел.

Об'єкт дослідження – процес аудиту інформаційної безпеки на відповідність галузевим стандартам за допомогою програмних продуктів Wazuh безкоштовної версії.

Предмет дослідження – методи та функціональні можливості програмного продукту Wazuh у його безкоштовній версії для забезпечення відповідності вимогам кібербезпеки, визначеним сертифікаціями організації Trusted Partner Network.

Мета роботи – розробка аналітичного опису доцільності використання безкоштовної версії програмного продукту сканування системних вразливостей Wazuh для самостійного аудиту інформаційної безпеки на підприємствах на відповідність галузевим стандартам.

Методи дослідження: методи аналізу технічної документації, порівняльного аналізу можливостей програмного забезпечення, практичних тестів та аналізу отриманих результатів. В результаті проведено порівняння Wazuh з іншим інструментом сканування вразливостей – AlienVault OSSIM.

Короткий зміст роботи: Досліджено функціональні можливості програмного продукту Wazuh, включаючи встановлення, конфігурування, запуск та аналіз отриманих звітів. Описано галузеві стандарти кібербезпеки, їх значення для сертифікації та вплив на операційні можливості бізнесу. Розглянуто процес розгортання Wazuh та проведено тестування його можливостей у реальному середовищі. Проведено порівняльний аналіз Wazuh з AlienVault OSSIM, визначено сильні та слабкі сторони Wazuh як додаткового інструменту сканування вразливостей. Продемонстровано, як використання Wazuh може позитивно вплинути на спроможність підприємств відповідати сертифікаційним вимогам.

КЛЮЧОВІ СЛОВА: КІБЕРБЕЗПЕКА, СКАНЕР ВРАЗЛИВОСТЕЙ, SIEM, СТАНДАРТИ БЕЗПЕКИ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 76 pages, 30 figures, 10 tables, 32 sources.

Object of the research – the process of information security auditing for compliance with industry standards using the free version of the Wazuh software product.
Subject of the research – methods and functional capabilities of the Wazuh software product in its free version to ensure compliance with cybersecurity requirements defined by the Trusted Partner Network certifications.
Purpose of the research – to develop an analytical description of the feasibility of using the free version of the Wazuh vulnerability scanning software product for self-audit of information security at enterprises to ensure compliance with industry standards.
Research methods: methods of technical documentation analysis, comparative analysis of software capabilities, practical testing, and result analysis. As a result, a comparison of Wazuh with another vulnerability scanning tool, AlienVault OSSIM, was conducted.
Brief content of the work: The functional capabilities of the Wazuh software product were studied, including installation, configuration, operation, and analysis of the generated reports. Industry cybersecurity standards were described, highlighting their importance for certification and their impact on business operational capabilities. The deployment process of Wazuh was examined, and its capabilities were tested in a real-world environment. A comparative analysis of Wazuh with AlienVault OSSIM was carried out, identifying the strengths and weaknesses of Wazuh as an additional vulnerability scanning tool. It was demonstrated how the use of Wazuh can positively impact the ability of enterprises to meet certification requirements.

KEYWORDS: CYBERSECURITY, VULNERABILITY SCANNER, SIEM, SECURITY STANDARDS.

ЗМІСТ

ВСТУП

Безпека є однією з ключових умов стабільної діяльності сучасних організацій, що впливає на всі аспекти їх функціонування, від фінансових показників до репутації. Забезпечення безпеки потребує значних ресурсів, часу та зусиль на її впровадження, підтримку та регулярну перевірку. Хоча впровадження систем безпеки може створювати певні незручності та вимагати додаткових витрат, ігнорування цього аспекту загрожує серйозними наслідками. Втрата даних або витік конфіденційної інформації можуть завдати організації значних фінансових збитків, підірвати довіру клієнтів, призвести до зупинки бізнес-процесів і навіть зруйнувати компанію. Особливого значення у цьому контексті набуває кібербезпека, яка займає провідне місце у системі захисту інформаційних активів сучасних організацій.

Актуальність теми дослідження зумовлена зростанням значення кібербезпеки в умовах стрімкого розвитку інформаційних технологій, цифровізації бізнесу та збільшення масштабів використання інформаційних систем. Інформація стала стратегічним активом для організацій, а її захист є ключовою умовою забезпечення стабільної роботи. В умовах сучасного інформаційного простору зростає кількість загроз, пов’язаних із кібератаками, які можуть спричинити зупинку бізнес-процесів, втрату репутації та значні фінансові збитки. Для українського бізнесу це питання є особливо актуальним через постійні кібератаки з боку країни-агресора, а також необхідність відповідності міжнародним стандартам кібербезпеки для інтеграції до світової економіки. Відповідність цим стандартам є обов’язковою умовою для отримання інвестицій, міжнародної співпраці та доступу до ринків країн «глобального Заходу».

Метою дослідження є аналіз доцільності використання безкоштовного програмного продукту Wazuh для проведення самостійного аудиту інформаційної безпеки підприємств малого та середнього бізнесу з подальшою підготовкою до сертифікації відповідно до міжнародних стандартів кібербезпеки. Для досягнення

поставленої мети необхідно вирішити такі завдання: провести огляд сучасних інструментів для аудиту кібербезпеки та визначити їхні переваги та недоліки; вивчити функціональні можливості продукту Wazuh, включаючи процес розгортання, налаштування та використання; провести порівняльний аналіз Wazuh із комерційними рішеннями, такими як AlienVault OSSIM; розробити рекомендації щодо впровадження Wazuh у практику малого та середнього бізнесу; оцінити ефективність використання Wazuh для підготовки до сертифікації відповідно до міжнародних стандартів кібербезпеки.

Об’єктом дослідження є процес аудиту інформаційної безпеки для відповідності галузевим стандартам. Предметом дослідження є функціональні можливості безкоштовного програмного продукту Wazuh для проведення самостійного аудиту інформаційної безпеки.

У роботі використано комплекс методів дослідження, зокрема: аналіз літературних джерел для вивчення сучасних підходів до забезпечення кібербезпеки та огляду наявних програмних продуктів; порівняльний аналіз для визначення переваг і недоліків Wazuh у порівнянні з іншими інструментами; експериментальний метод для практичного тестування можливостей Wazuh у реальному середовищі; аналіз отриманих результатів для формулювання практичних рекомендацій.

Практична значущість дослідження полягає у створенні рекомендацій для підприємств малого та середнього бізнесу щодо використання Wazuh як інструменту для самостійного аудиту інформаційної безпеки. Це дозволить знизити витрати на впровадження комерційних рішень, підвищити рівень кіберзахисту та забезпечити відповідність міжнародним стандартам, що сприятиме зростанню конкурентоспроможності та стабільності бізнесу. Результати роботи можуть бути використані для підготовки підприємств до сертифікації кібербезпеки, що є важливим кроком для інтеграції у міжнародні ринки та забезпечення довгострокового розвитку.

У рамках роботи також проведено детальний аналіз практичних аспектів використання Wazuh, його переваг та недоліків порівняно з іншими інструментами. Окрему увагу приділено аналізу його можливостей у контексті сучасних вимог кібербезпеки, що дозволяє підприємствам ефективно підготуватися до викликів сучасного цифрового середовища.

Апробація результатів та публікації:

1. ІНТЕГРОВАНА СИСТЕМА МОНІТОРИНГУ ВРАЗЛИВОСТЕЙ ТА ПЕРЕВІРКИ ВІДПОВІДНОСТІ ГАЛУЗЕВИМ СТАНДАРТАМ БЕЗПЕКИ ІЗ ВИКОРИСТАННЯМ WAZUH ДЛЯ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ. Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу: матеріали ІІ Всеукраїнської науково-технічної конференції (м. Київ, 18 листопада 2024 року). Навчально-науковий інститут інформаційних технологій ДУІКТ, Київ, 2024. 393 с.

2. Дорожня карта інформаційно-комунікаційної галузі України: матеріали V Всеукраїнської науково-практичної конференції (м. Київ, 28 листопада 2024 року). Навчально-науковий інститут менеджменту та підприємництва ДУІКТ. Київ, 2024. 228 с.

1 КІБЕРБЕЗПЕКА ЯК КРИТИЧНИЙ ФАКТОР ВЕДЕННЯ БІЗНЕСУ

1.1 Огляд галузевих стандартів кібербезпеки та їх значення для бізнесу

В залежності від сфери операційної діяльності підприємства, існують різні рівні цінності інформації, яка використовується в його роботі. Комерційно важлива інформація є вкрай цінною, а тому необхідно запобігати її витокам. В процесі переходу оперування даними в паперовій формі до здебільшого використання цифрових форматів, збільшилася вагомість захисту носіїв та цифрових каналів передачі даних. Самостійна розробка систем кіберзахисту, особливо для малого та навіть середнього бізнесу буде тривалим і дуже бюджетно затратним процесом. Тому, були створені галузеві стандарти, які, відповідно до галузі, описують вимоги, яким має відповідати підприємство у своїй роботі. Вагома частина вимог стосується саме захисту інформації через механізм кібербезпеки. Надалі, будемо називати ці вимоги як «шаблони кібербезпеки». Далі, за текстом, розглянемо найбільш поширені стандарти безпеки для бізнесу.

HIPAA (Health Insurance Portability and Accountability Act) [1] — це американський стандарт захисту персональної інформації у медичній сфері, який передбачає суворі вимоги до захисту даних, що стосуються здоров'я пацієнтів. Його мета — забезпечити конфіденційність, цілісність та доступність медичної інформації, а також уникнути витоків даних і кібератак. Оскільки HIPAA — це американський стандарт, юридично його застосування не є обов'язковим для українських компаній, за винятком випадків, коли вони працюють з американськими медичними установами або мають міжнародні проекти в сфері охорони здоров'я, що вимагають дотримання цього стандарту. Однак з огляду на зростання кібератак та значення захисту персональної інформації, деякі підприємства в Україні, які працюють в медицині або в обслуговуванні медичних закладів, можуть орієнтуватися на вимоги HIPAA з таких причин (рис. 1.1):

Рис. 1.1 Переваги використання стандарту HIIPA

Серед основних переваг використання стандарту HIIPA відзначається:

- **Забезпечення міжнародної довіри та конкурентоспроможності**. Дотримання стандартів HIPAA може слугувати знаком якості для потенційних клієнтів чи інвесторів із США або Європи, демонструючи високий рівень захисту даних і сприяючи співпраці.
- **Отримання локальних законів про захист персональних даних**. Українські закони, такі як Закон України «Про захист персональних даних», накладають певні вимоги щодо захисту інформації, але не мають таких суворих норм, як HIPAA. Проте підприємства, що орієнтуються на HIPAA, можуть покращити свої локальні практики захисту даних і уникати ризиків, пов'язаних з можливими витоками.
- **Оптимізація внутрішніх процесів**. Використання найкращих практик, закріплених у HIPAA, сприяє організації ефективного процесу обробки і зберігання медичних даних, знижуючи ймовірність технічних помилок і збоїв.
- **Адаптація до майбутнього вступу України до ЄС**. Очікується, що в разі вступу до ЄС вимоги до захисту персональних даних будуть більш жорсткими,

зокрема завдяки вже існуючому Регламенту ЄС щодо захисту даних (GDPR). HIPAA може слугувати певною "базою" для розуміння і дотримання європейських стандартів захисту.

Деякі українські компанії з IT-індустрії, особливо ті, що надають аутсорсинг медичних IT-послуг для клієнтів у США, використовують вимоги HIPAA як частину свого стандарту захисту даних. Це, зокрема, стосується медичних стартапів, які працюють на американському ринку, і деяких приватних клінік, які впроваджують системи зберігання медичних записів із орієнтацією на міжнародні вимоги. Загалом, HIPAA може бути корисним керівництвом для українських медичних підприємств та IT-компаній, що працюють в галузі охорони здоров'я.

Наступним розглянутим галузевим стандартом є GDPR (General Data Protection Regulation) [2] — це Регламент Європейського Союзу щодо захисту персональних даних, який набрав чинності у 2018 році. Його вимоги стосуються не тільки компаній, розташованих в ЄС, але і будь-яких організацій, що обробляють персональні дані громадян ЄС, незалежно від їхнього географічного розташування. У випадку українських підприємств це може бути особливо актуально для компаній, що ведуть бізнес із клієнтами чи партнерами в Європі.

Для українських компаній, перевагами (рис. 1.2) застосування GDPR, будуть:

- **Співпраця з клієнтами та партнерами з ЄС**. Українські підприємства, які надають послуги або продукти для європейських клієнтів, змушені дотримуватись GDPR, оскільки обробляють їхні персональні дані. Це стосується, зокрема, компаній з IT-індустрії, які пропонують послуги обробки даних, аутсорсингових IT-послуг, електронної комерції тощо.
- **Конкурентоспроможність і довіра**. Дотримання вимог GDPR свідчить про високий рівень захисту даних, що допомагає українським компаніям завоювати довіру європейських партнерів та клієнтів. Це стає важливою перевагою в умовах глобальної конкуренції, коли клієнти дедалі більше звертають увагу на захист своїх персональних даних.

- **Підготовка до майбутнього вступу України до ЄС**. Україна поступово інтегрується до європейського простору, і дотримання GDPR може полегшити перехід на європейські стандарти в майбутньому. Це також дозволяє уникнути ризику санкцій у разі недотримання правил при роботі з європейськими громадянами.
- **Мінімізація ризиків витоку даних**. GDPR передбачає жорсткі вимоги до безпеки зберігання та обробки даних, що дозволяє захистити інформацію від витоків, хакерських атак і випадкових інцидентів. Дотримання цих вимог допомагає уникати фінансових втрат та репутаційних ризиків, пов'язаних із витоками даних, адже штрафи за порушення правил захисту даних можуть досягати до 20 мільйонів євро або 4% від світового обороту компанії, залежно від того, що більше.

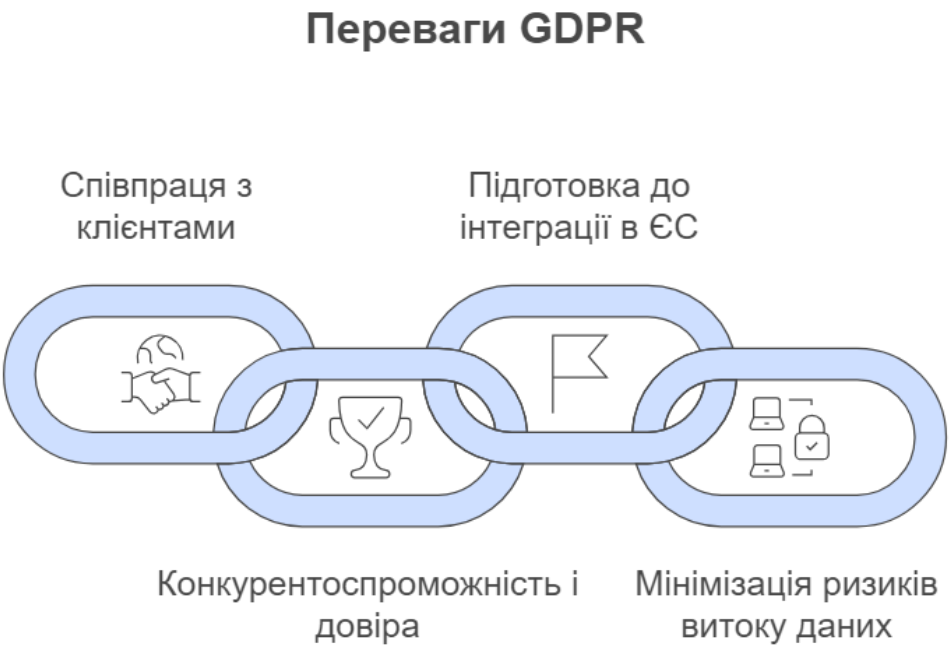


Рис. 1.2 Переваги використання стандарту GDPR

Використання стандартів GDPR передбачає забезпечення наступних компонентів (рис. 1.3):

1. **Політика конфіденційності та обробки даних**. Компанії створюють та публікують політику конфіденційності, яка пояснює, які дані збираються, з якою метою та як вони захищені. Зазвичай, це стосується як вебсайтів, так і мобільних додатків або будь-яких інших онлайн-сервісів.
2. **Згода на обробку даних**. GDPR вимагає, щоб користувачі давали згоду на обробку своїх даних добровільно та усвідомлено. Тому українські компанії часто додають окремі форми та повідомлення для отримання згоди на обробку даних, коли це необхідно.
3. **Підвищення рівня безпеки**. Компанії впроваджують заходи безпеки, що відповідають вимогам GDPR, такі як шифрування, аутентифікація користувачів, регулярний моніторинг систем на предмет витоків, а також аудит доступів до персональних даних.
4. **Доступ до персональних даних і право на видалення**. GDPR надає користувачам право на доступ до їхніх даних та їх видалення. Тому багато українських компаній розробляють внутрішні процедури для реалізації цих прав — від надання звіту про збережені дані до можливості їхнього видалення на вимогу користувача.
5. **Реєстрація інцидентів**. GDPR вимагає від компаній повідомляти про будь-які витоки персональних даних протягом 72 годин. Українські компанії, які працюють з європейськими даними, впроваджують системи та процедури для швидкого реагування на подібні інциденти.

Саме тому, багато українських компаній, особливо з IT-індустрії, електронної комерції та сфери обслуговування, уже орієнтуються на GDPR. Вони використовують цей стандарт для покращення захисту даних, підвищення рівня довіри клієнтів і підготовки до майбутньої інтеграції України в ЄС. Це також сприяє підвищенню культури захисту даних в Україні та допомагає уникнути

репутаційних ризиків і санкцій за недотримання вимог при роботі з європейськими клієнтами.

Рис. 1.3 Компоненти відповідності стандарту GDPR

PCI DSS [3] – стандарти безпеки для роботи з банківськими картковими сервісами. Стандарт PCI DSS (Payment Card Industry Data Security Standard).

PCI DSS — це глобальний стандарт, який регулює вимоги до забезпечення безпеки даних платіжних карток. Він розроблений Радою стандартів безпеки платіжних карток (PCI SSC, Payment Card Industry Security Standards Council), заснованою такими організаціями, як Visa, MasterCard, American Express, Discover і JCB.

Стандарт застосовується до будь-якої організації, яка обробляє, зберігає або передає дані платіжних карток, включаючи (рис. 1.4):

- Ритейлерів.
- Провайдерів платіжних послуг.
- Банки.
- Електронні магазини.

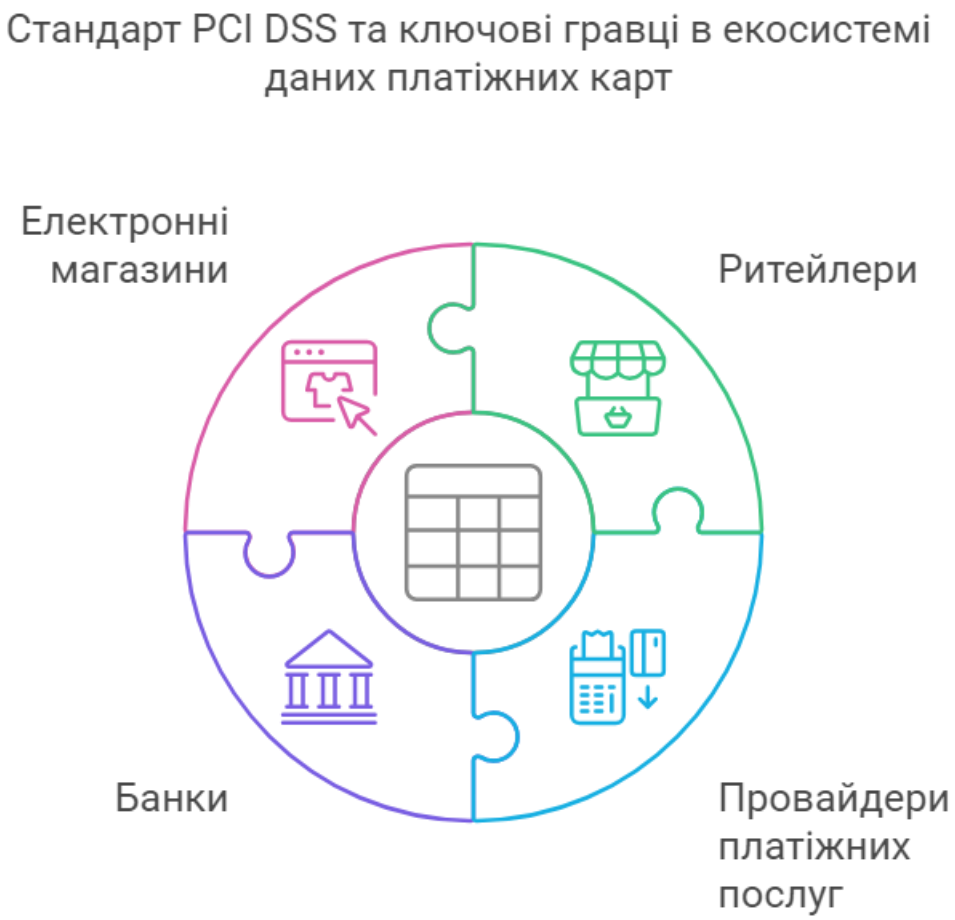


Рис. 1.4 Основні бізнес-сфери використання стандартів PCI DSS

PCI DSS складається з 12 основних вимог, розподілених за шістьма категоріями, котрі передбачають наступні критерії (рис. 1.5):

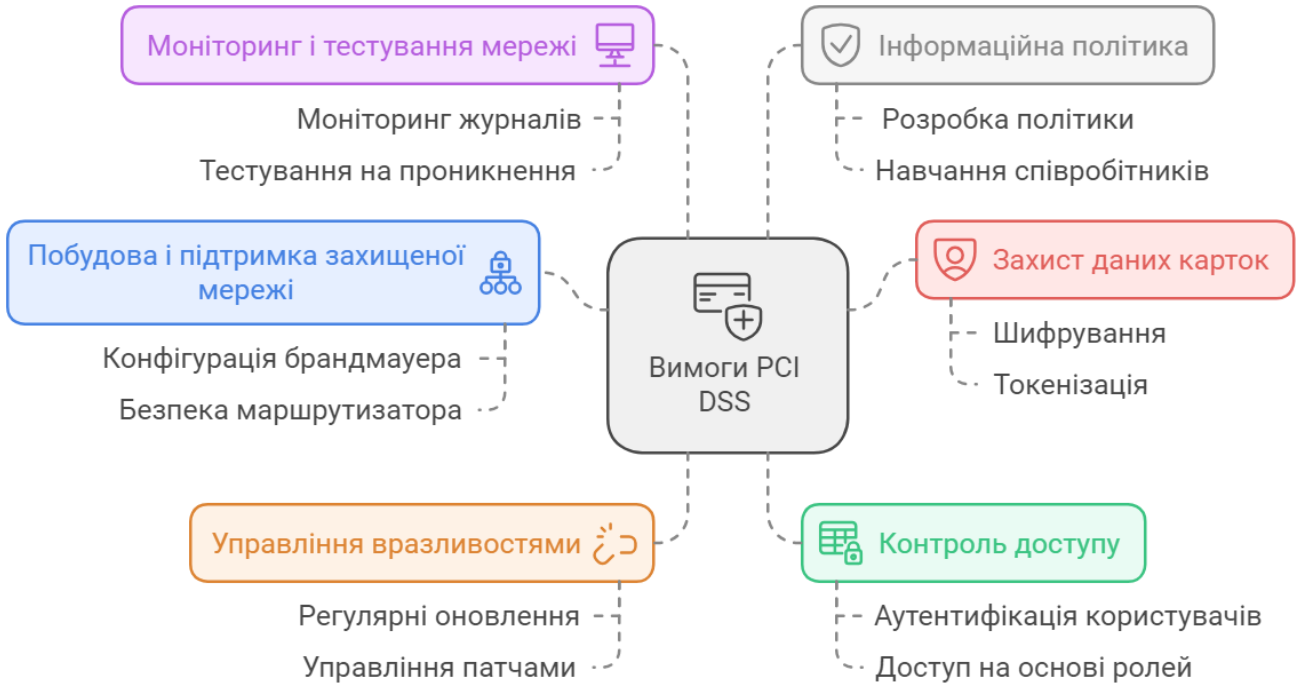


Рис. 1.5 Основні категорії стандарту PCI DSS

Категорія 1: Побудова та підтримка безпечної мережі

- Встановлення та підтримка конфігурації брандмауера (firewall):
  - Забезпечує захист мережі від несанкціонованого доступу.
  - Вимагає чіткої політики управління трафіком.
- Використання унікальних паролів і заборона стандартних паролів виробника:
  - Стандартні облікові записи та паролі, які постачаються з обладнанням чи програмним забезпеченням, повинні бути змінені.

Категорія 2: Захист даних платіжних карток

- Захист збережених даних платіжних карток:
  - Обмеження зберігання даних власника картки (Cardholder Data, CHD).
  - Використання шифрування для захисту даних.
- Шифрування переданих даних власника картки через відкриті мережі:
  - Забезпечення захисту даних під час передавання через Інтернет чи інші незахищені мережі.
  - Використання протоколів, таких як TLS, SSH або IPsec.

Категорія 3: Управління вразливостями

- Розробка та підтримка програмного забезпечення з антивірусним захистом:
  - Антивірусне програмне забезпечення повинно бути встановлене на всіх пристроях, де це необхідно, і регулярно оновлюватися.
- Розробка та підтримка безпечних систем і програм:
  - Регулярне оновлення операційних систем і програмного забезпечення для усунення відомих вразливостей.
  - Використання систем управління виправленнями (patch management).

Категорія 4: Реалізація сильних заходів контролю доступу

- Обмеження доступу до даних власника картки за принципом найменших привілеїв:
  - Надання доступу тільки тим співробітникам, які мають на це бізнес-необхідність.
- Унікальна ідентифікація кожного користувача, який має доступ до системи:
  - Використання унікальних облікових записів для кожного користувача.
  - Застосування багатофакторної автентифікації (MFA).
- **Обмеження фізичного доступу до даних власника картки:**
  - Захист серверних приміщень, центрів обробки даних і інших фізичних місць, де зберігаються або обробляються дані.

Категорія 5: Моніторинг і тестування мережі

- Відстеження і моніторинг усіх доступів до мережевих ресурсів і даних власника картки:
  - Журналізація/логування усіх дій, пов’язаних із доступом до даних.
  - Зберігання журналів подій щонайменше 1 рік.
- Регулярне тестування систем безпеки та процесів:
  - Виконання сканування на вразливості та тестування на проникнення.
  - Перевірка безпеки всіх точок доступу до мережі.

Категорія 6: Забезпечення політики безпеки інформації

- Розробка, впровадження і підтримка політики інформаційної безпеки:
  - Визначення політик, які регулюють управління даними платіжних карток.
  - Навчання співробітників принципам кібербезпеки.

В Україні стандарт PCI DSS обов'язковий для всіх компаній, які обробляють дані платіжних карток, зокрема:

- Банки та фінансові установи: зобов’язані дотримуватись PCI DSS для забезпечення безпеки транзакцій.
- Платіжні системи та електронні магазини: якщо ці організації обробляють або зберігають дані платіжних карток клієнтів, дотримання стандарту є обов'язковим.
- POS-термінали та платіжні шлюзи: постачальники таких рішень зобов’язані впроваджувати механізми захисту, згідно PCI DSS.

Хоча стандарт PCI DSS прямо не закріплений у законах України, він є обов’язковим у рамках контрактів з міжнародними платіжними системами, такими як Visa та MasterCard. Невиконання вимог PCI DSS може призвести до:

- Штрафів від платіжних систем.
- Відключення від обробки карткових платежів.
- Юридичної відповідальності за витік даних клієнтів.

1.2. Сертифікація TPN як необхідна умова виходу на ринок медіаіндустрії

Втрата унікальності контенту до початку його комерційного використання завдає серйозних збитків правовласнику. Чим вищим є очікуваний прибуток від розповсюдження контенту, тим вищими будуть збитки від несанкціонованого доступу та, відповідно, висуваються серйозніші вимоги до захисту інформації.

У роботі розглянуто досвід найуспішнішого та найдорожчого ринку кіновиробництва, де суворі стандарти безпеки на кожному етапі, забезпечують захист унікального цифрового продукту.

Існує американська асоціація MPA (Motion Picture Association), яка займається захистом інтересів великих кінокомпаній, таких як Disney, Warner Bros., Universal, Sony Pictures, Paramount, Netflix та інші. Вона також визначає стандарти безпеки для захисту інтелектуальної власності.

За умови партнерської співпраці з будь-якою компанією, власник медіаконтенту проводив регулярні перевірки бізнесу можливого партнера, приділяючи велику увагу безпеці інформаційних технологій, оскільки контент розповсюджується зараз, саме цифровими каналами передачі даних.

В певний момент, учасники асоціації MPA, вирішили делегувати функції аудиту єдиній уповноваженій структурі, яку самі й заснували - Trusted Partner Network (TPN). По суті, це програма розроблена MPA у партнерстві з Content Delivery & Security Association (CDSA), яка забезпечує перевірку та сертифікацію компаній, що працюють з медіаконтентом.

TPN об'єднує інструменти, рекомендації та аудит для створення надійної мережі компаній-партнерів, яким можуть довіряти великі гравці медіаіндустрії. Основна мета TPN — захист медіаконтенту від витоків, піратства та несанкціонованого доступу (рис. 1.6).

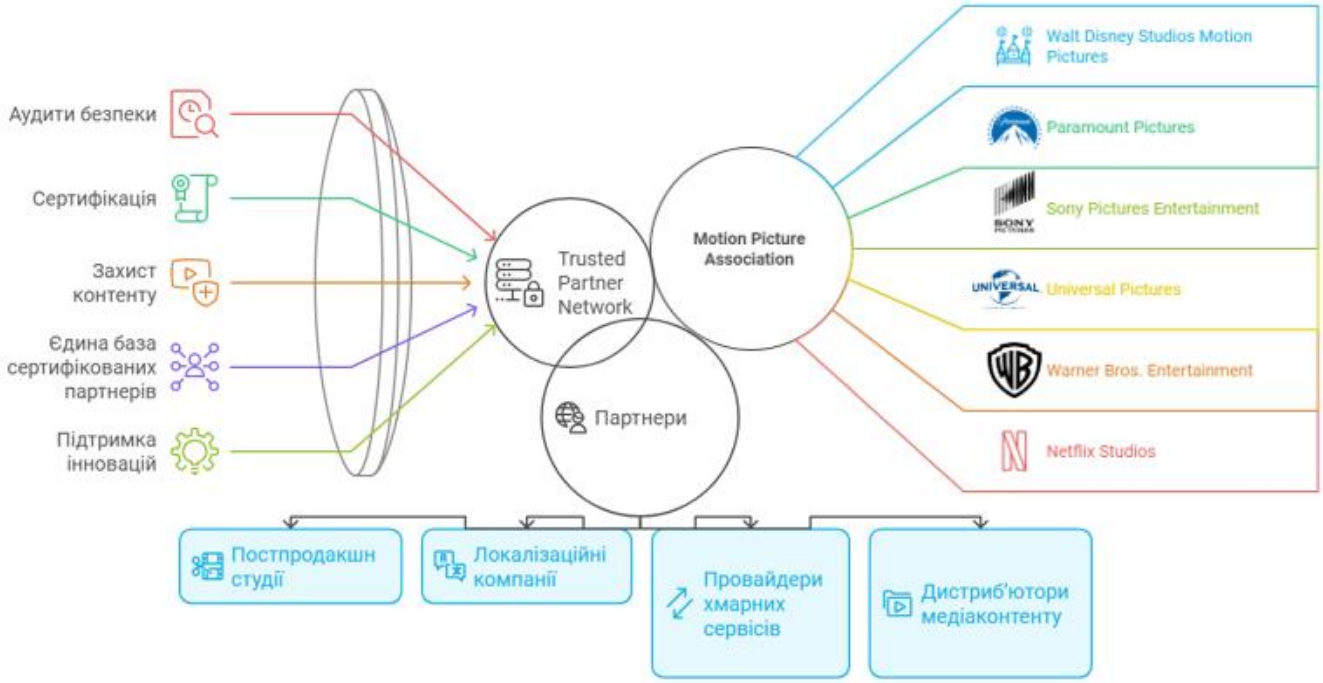


Рис. 1.6 Взаємодія структури MPA, TPN та партнерів

Сертифікація TPN є обов’язковою умовою для роботи з ліцензованим медіаконтентом, такими як фільми, серіали та інші відеоматеріали. Вона гарантує, що компанія:

- Відповідає міжнародним стандартам інформаційної та фізичної безпеки.
- Має належні процеси для захисту інтелектуальної власності.
- Може працювати з великими студіями, дистриб'юторами та платформами, такими як Netflix, Disney+ чи HBO.

TPN необхідна для компаній, які:

- Займаються постпродакшеном (монтаж, візуальні ефекти, колористика тощо).
- Працюють з дублюванням, субтитруванням або локалізацією контенту.
- Розробляють технології, пов’язані з дистрибуцією контенту.
- Здійснюють хостинг, стрімінг чи доставку медіаконтенту.

TPN охоплює декілька ключових аспектів безпеки:

- **Фізична безпека: з**ахист прилеглої території, офісних приміщень, серверних кімнат і серверів та робочих станцій (контроль доступу, відеоспостереження).
- **Інформаційна безпека:** шифрування даних під час передавання і зберігання та захист мережі та систем від кібератак.
- **Процеси управління ризиками:** регулярне оновлення програмного забезпечення, а також політики доступу до контенту (принцип найменших привілеїв).
- **Навчання персоналу:** проведення тренінгів з інформаційної безпеки.
- Українські компанії, які прагнуть працювати з великими гравцями світової медіаіндустрії, такими як Netflix, Disney чи Amazon, повинні довести свою відповідність високим стандартам безпеки.

TPN-сертифікація є своєрідним "пропуском" до співпраці з великими студіями, а її відсутність, навпаки, може стати «закритим шлагбаумом».

До переваг сертифікації TPN для українських компаній відносять:

- **Доступ до глобального ринку:** Можливість співпраці з міжнародними медіакомпаніями.
- **Підвищення конкурентоспроможності:** Сертифікат TPN є визнаним маркером надійності.
- **Захист власної репутації:** Відповідність міжнародним стандартам безпеки мінімізує ризики витоків.

TPN фактично є незалежною структурою, яка відіграє роль «воротаря» на ринку медіаконтенту, допускаючи до співпраці з правовласниками лише ті компанії, що відповідають строгим вимогам сертифікації. Важливо розуміти, що специфіка кінотеатрального контенту робить його вразливим до передчасних витоків: навіть найменше розголошення деталей сюжету, діалогів або відеоряду в одній країні може завдати глобальних збитків. У сучасну епоху миттєвого

поширення інформації через глобальну мережу Інтернет, піратські копії можуть блискавично охопити весь світ, завдаючи шкоди індустрії в усіх куточках планети. З відомих українських компаній, котрі пройшли сертифікацію TPN зазначено групу FILM.UA та її студію дубляжу Postmodern [4], студію LeDoyen [5], компанію StarLight Creative Studio [6], анімаційну групу «Karandash animation studio» [7] зі спеціалізацію у сфері обробки відеоконтенту.

Це неповний перелік компаній з цією успішною, галузевою, сертифікацією, але йде мова лише про одиниці, можливо більше десятка найменувань, що свідчить про складність успішного проходження сертифікації TPN.

Особливої ваги сертифікація TPN в Україні набула в момент жорсткого локдауну через загрозу COVID-19 та водночас, виходу на ринок України онлайн-медіаплатформи Netflix.

Малі гравці на ринку послуг обробки медіаконтенту залишилися без замовлень, через тотальне закриття кінотеатрів та відсутності робіт з кінотеатральними версіями фільмів. Натомість Netflix, як онлайн-платформа стала дуже популярною, але співпраця з нею передбачала наявну сертифікацію TPN.

Також, великі хмарні провайдери IT-послуг не оминули явну сертифікацію своїх послуг за стандартами CDSA та MPA, якими, власне й опікується TPN. Це стосується Microsoft Azure [8,9], Amazon Web Services [10], Google Cloud [11], Alibaba Cloud [12].

Маючи відповідну сертифікацію, Amazon та Microsoft, залучили до себе таких великих гравців ринку як SONY, Disney, Paramount як платформу, для розповсюдження контенту через свої мережі CDN.

Підсумовуючи, можна виділити успішні кейси використання TPN у медіаіндустрії.

Netflix активно впроваджує TPN (Trusted Partner Network) для забезпечення кібербезпеки у своїй діяльності, особливо під час роботи з постачальниками.

Компанія використовує TPN для оцінки ризиків та управління безпекою в рамках співпраці з численними аутсорсинговими партнерами.

Результати:

- Середній час перевірки нових партнерів скоротився на 30%, що, як наслідок, пришвидшило запуск проектів.
- Рівень відповідності вимогам MPAA (Американської асоціації кінокомпаній) зріс до 98%.

Warner Bros. Entertainment впровадила TPN як частину свого комплексного підходу до захисту преміальних відеоматеріалів у пост-продакшн процесах. Завдяки TPN було запроваджено стандартизовані протоколи роботи для партнерів у різних країнах.

Результати:

- Зменшення ризиків несанкціонованого доступу до контенту на 40%.
- Прискорення перевірок постачальників на відповідність кібербезпеці на 25%.
- Підвищення надійності захисту файлів у хмарних середовищах до 99.5%.

Disney+ використовує TPN для координації глобальних постачальників, що працюють над створенням і трансляцією оригінального контенту. Завдяки інтеграції TPN, платформа значно вдосконалила механізми оцінки безпеки даних у партнерських студіях.

Результати:

- Скорочення витрат на управління ризиками на 20%.
- Поліпшення ефективності захисту від «фішингових» атак і кібератак завдяки індивідуальним рекомендаціям TPN.
- Стандартизація протоколів роботи з постачальниками у понад 30 країнах.

Sony Pictures інтегрувала TPN для захисту інтелектуальної власності під час пост-продакшн робіт і обміну файлами з партнерами. TPN допоміг запровадити жорсткі вимоги до безпеки та дотримання конфіденційності.

Результати:

- Зниження кількості скарг на витоки конфіденційної інформації на 50%.
- Покращення аудиторських показників відповідності вимогам ISO 27001 на 35%.
- Скорочення часу на оцінку ризиків постачальників на 15%.

Paramount Pictures застосовує TPN як частину своєї політики захисту преміального контенту в пост-продакшн процесах і розподілі файлів між студіями та аутсорсинговими партнерами.

Результати:

- Витрати на забезпечення безпеки скоротилися на 18%, завдяки стандартизації процесів через TPN.
- Підвищення довіри з боку клієнтів і партнерів: частка сертифікованих постачальників зросла до 92%.
- Загальний рівень захищеності контенту зріс на 38%.

Ці кейси демонструють, що TPN не лише забезпечує відповідність кібербезпеці, а й сприяє підвищенню ефективності бізнес-процесів, зменшенню витрат та покращенню управління ризиками.

Усі великі компанії, відзначають позитивну роль з заощадженням ресурсів як фінансових так і часових, отримують вищий прибуток, зберігають вищий рівень захисту даних. Це сприяє більш комфортній роботі компаній, де творча діяльність над створенням чи обробкою контенту повинна мати пріоритет. Зупинки виробничого ланцюжка через злам кібербезпеки суміжного виробничого партнера на будь-якому етапі сповільнюють усіх абсолютно.

Саме тому, так символічно називається мережа сертифікованих партнерів – Trusted Partner Network – Довірена Партнерська Мережа.

1.3. Методика проведення самостійного аудиту кібербезпеки підприємства

Частка запитань, котрі стосуються кібербезпеки, що виникає у відповідальних співробітників підприємств при сертифікації TPN складає біля 60%, отож, самостійна підготовка та наступний постійний аудит стану кіберзахисту є важливим та необхідним.

Першим етапом підготовки, має бути ознайомлення з публічно доступними рекомендаціями MPA [13], обговорення вимог в межах компанії, визначення команди та розподіл зон відповідальності, яка буде опікуватися змінами, планування бюджетів, встановлення термінів, налагодження комунікації з зовнішніми постачальниками

Проведення самостійного аудиту кібербезпеки для малого чи середнього підприємства (МСП) є важливим кроком для забезпечення захисту даних, мінімізації ризиків та дотримання нормативних вимог. Нижче (рис. 1.7.) запропоновано методику, яка адаптована для МСП і передбачає покроковий підхід.

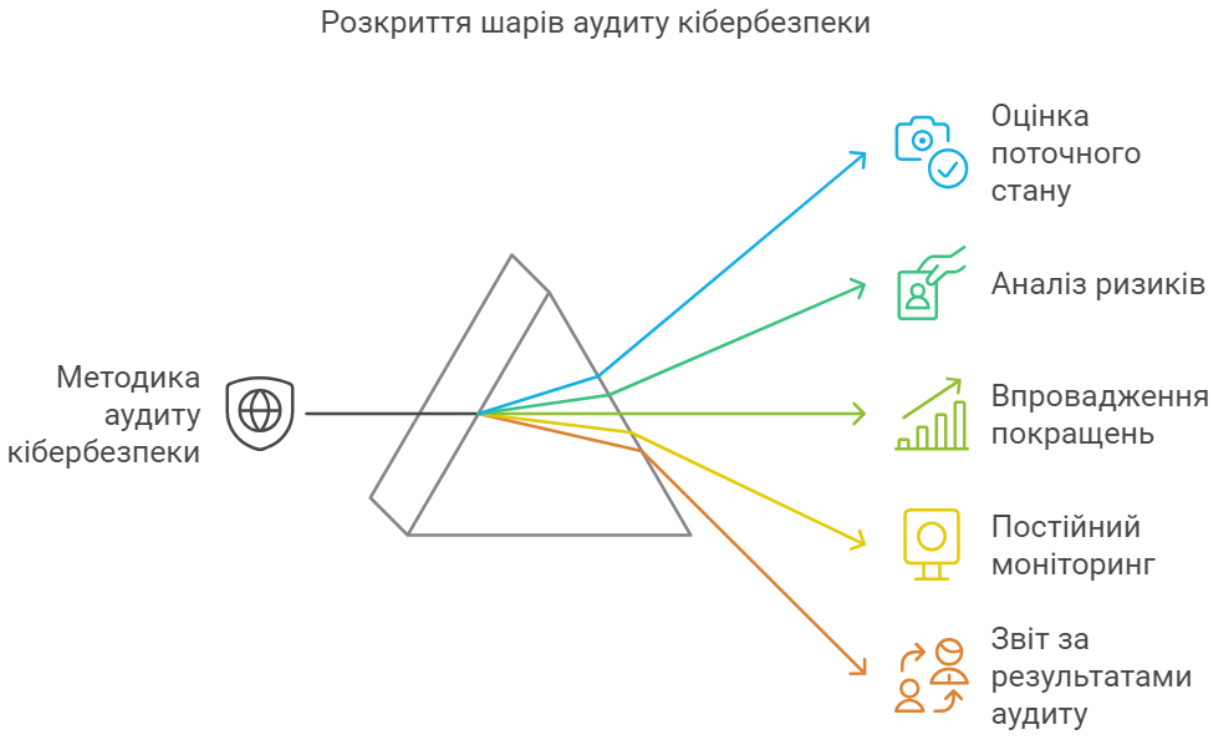


Рис. 1.7. Етапи проведення самостійного аудиту кібербезпеки

Запропонований план проведення самостійного аудиту кібербезпеки для МСП складається з ряду важливих етапів. Які ми нижче опишемо:

1. Підготовчий етап

Визначення мети аудиту:

- Оцінити поточний стан кібербезпеки.
- Виявити слабкі місця та загрози.
- Розробити план дій для усунення виявлених ризиків.

Формування команди:

- Залучити IT-фахівців компанії, якщо вони є чи замовити зовнішнього спеціаліста.
- Визначити відповідального за кібербезпеку (наприклад, системного адміністратора або IT-менеджера).

Визначення активів:

- Скласти список активів, які потребують захисту:
  - Сервери, робочі станції, мережеве обладнання.
  - Дані (персональні, фінансові, комерційні).
  - Програмне забезпечення, включаючи CRM, ERP та інше.

2. Оцінка поточного стану

Інвентаризація IT-активів:

- Зробити список пристроїв, операційних систем і версій програмного забезпечення.
- Перевірити наявність ліцензій програмного забезпечення (ПЗ)
- Перевірити облікову та фактичну кількість обладнання та ПЗ
- Вписати місцезнаходження IT-активу та відповідальних осіб

Проаналізувати політики і процедури:

- Чи існують політики інформаційної безпеки (паролі, доступ до даних)?

- Чи проводяться регулярні резервні копії? Як вони зберігаються?
- Чи навчаються співробітники основам кібербезпеки?

Оцінити доступи і права:

- Перевірити, чи є привілейовані облікові записи.
- Переконатися, що користувачі мають доступ лише до необхідних їм ресурсів.

Перевірка оновлень:

- Чи оновлені операційні системи, ПЗ та мережеве обладнання?
- Чи використовуються автоматичні оновлення?

Оцінка мережевої безпеки:

- Перевірити налаштування брандмауера (Firewall).
- Перевірити VPN, якщо використовується для віддаленого доступу.
- Виконати тест на відкриті порти.

Перевірка резервного копіювання:

- Переконатися, що резервні копії є актуальними.
- Випробувати процес відновлення з резервної копії.

3. Аналіз ризиків

Ідентифікація загроз:

- Небезпечні email-файли, фішингові атаки.
- Зловмисне ПЗ, віруси, програми-вимагачі.
- Ненадійні паролі або вразливості в програмному забезпеченні.

Оцінка ймовірності та впливу:

- Оцінити, наскільки ймовірним є виникнення кожної загрози.
- Визначити, який вплив матиме реалізація загрози (втрата даних, простої, фінансові втрати).
- Чи є в наявності актуальний “План безперервності бізнесу” (BCP – Business Continuity Plan)?

- Чи є в наявності актуальний “План аварійного відновлення” (DRP – Disaster Recovery Plan)?

Визначення пріоритетів, ризиків:

- Скласти список ризиків за пріоритетом: критичні, високі, середні, низькі.
- Класифікувати наявні дані за наступними критеріями:
    - Високий рівень важливості (Конфіденційні дані)
    - Середній рівень важливості (Внутрішні дані)
    - Низький рівень важливості (Публічні дані)

4. Впровадження покращень

Покращення базових практик:

- Встановити багатофакторну автентифікацію (MFA).
- Забезпечити регулярне оновлення ОС і ПЗ.
- Ввести політику складних паролів.
- Впровадити регулярну автоматизовану перевірку кібербезпеки

Захист мережі:

- Використати брандмауери та системи виявлення вторгнень (IDS/IPS).
- Встановити антивірусні програми на всі пристрої.

Резервне копіювання:

- Організувати резервні копії критично важливих даних
- Забезпечити утримання додаткових копій резервних даних на зовнішньому носії або в хмарі, але найкраще – в обох місцях одночасно.
- Впровадити регулярні перевірки процесу відновлення.

Навчання співробітників:

- Провести тренінги щодо фішингу, зловмисних програм та безпечного використання Інтернету.
- Ввести процедури повідомлення про підозрілі дії.

5. Постійний моніторинг і перевірки

Впровадження моніторингових інструментів:

- Використати безкоштовні інструменти, як-от OSSEC, nmap, Snort, Zabbix, GrayLog AlienVault OSSIM, Wazuh чи аналогічні .
- Запровадити регулярний аналіз журналу системних подій.

Періодичний аудит:

- Запланувати регулярні перевірки систем безпеки кожні 6–12 місяців.
- Актуалізуйте список ризиків та покращень.
- Для документації та процедур забезпечуйте версійність внесених змін з їх описом.

Тестування захищеності:

- Використати інструменти для перевірки на вразливості, наприклад, AlienVault OSSIM, Nessus**,** nmap OpenVAS**,** Qualys, Wazuh**.**

6. Звіт за результатами аудиту

Після завершення аудиту створити звіт, який включатиме:

- Виявлені слабкі місця.
- Пропоновані дії з їх усунення.
- Список ризиків із пріоритетами.
- План впровадження покращень.

Такий підхід дозволить забезпечити базовий рівень кібербезпеки для малого чи середнього підприємства, мінімізуючи ризики та підвищуючи стійкість до кібератак.

З набутого, практичного досвіду, саме етап самостійної підготовки заощадить значні фінансові бюджети та затрати часу. Лише маючи практично 100-відосткову відповідність вимогам MPA, є сенс вперше оформляти заявку до TPN для розгляду компанію як претендента на сертифікацію.

Після оплати обов’язкового першого внеску, заявку компанії розглянуть, зареєструють в системі TPN як кандидата та згодом буде надано доступ до ресурсів платформи Trusted Partner Network.

Після заповнення анкети з відомостями про компанію, також запропонують заповнити онлайн-опитувальник та завантажити на ресурс TPN наявні документації, схеми, плани, журнали, опис процедур, налаштування фаєрволів тощо.

Система опитувальника не дозволить надіслати документ, доки він не буде заповнений на 100%. Лише після повного, самостійного заповнення, відповіді та документи будуть ретельно перевірені. Згодом, можливі уточнюючі запитання та потреба в нових документах чи документаціях за вимогою представників TPN. Лише після цього, компанія отримає дату проведення фізичної сертифікації, сертифікованим з боку TPN спеціалістом з відвідинами компанії та фактичною перевіркою та порівнянням усіх зазначених в опитувальнику даних з реальним станом справ.

Не слід очікувати, що прогалини чи недосконалості компанії-кандидата на сертифікацію TPN будуть якимось чином непомічені чи проігнорованими – перевірятися будуть усі заповнені вами відповіді опитувальника.

Досвід важливості та ефективності затрачених ресурсів задля підготовки до сертифікації та її постійна підтримка та удосконалення не є чимось унікальним, а навпаки, є правильним підходом в глобальному сенсі. Дуже гарно це ілюструє дослідження однієї з найбільших аудиторський компаній світу Deloiite. Так, згідно їхнього звіту [14] глобального впливу рівня кібербезпеки на прибуток бізнесу, зафіксовано наступні цифри (рис. 1.8):

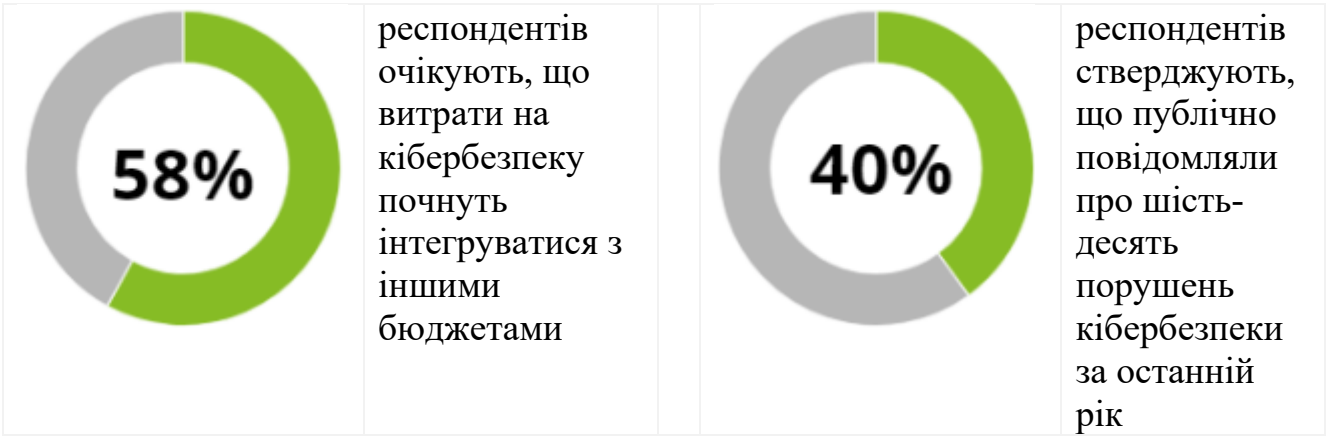


Рис. 1.8. Дослідження Deloiite у звіті «Глобальне майбутнє кіберпростору»

Наступні відповіді на запитання «*Якою мірою ви очікуєте досягти наступних бізнес-результатів за допомогою ваших ініціатив з кібербезпеки?*» в категорії «*Технології, медіа та телеком*» фіксують рівень понад 80% позитивних очікувань від реалізації заходів щодо підсилення кібербезпеки.

Таблиця 1.1

Очікування переваг глобального бізнесу від покращення кібербезпеки

Показник	- помірною мірою	- значною мірою
Підвищення ефективності та гнучкості	44%	45%
Покращення виявлення загроз та реагування на них	41%	47%
Збільшення доходів	44%	44%
Підвищення довіри до бренду та репутації	40%	46%
Захист інтелектуальної власності	44%	41%
Зміцнення довіри до цілісності технологій/даних	35%	51%
Підвищення рівень задоволеності та утримання клієнтів	44%	42%
Реалізація місії/цілі бізнесу	47%	38%

Наведені в табл. 1.1 цифри, свідчать про розуміння комерційними структурами, які виконують операційну діяльність у сфері медіа та телекомунікацій важливості інвестицій в рішення для підвищення рівня кібербезпеки. Кіберстійкість стає значущим елементом корпоративної культури. Бізнес, що активно розбудовує культуру кібербезпеки і регулярно проводить навчання своїх співробітників, значно зменшує ризики виникнення інцидентів, пов’язаних з людським фактором, які є однією з головних причин кібератак. З огляду на високу частоту кібератак і складність сучасних загроз, стає очевидним, що інвестування у кібербезпеку є не просто витратою, а критично важливою стратегією для забезпечення стійкості бізнесу.

2 АНАЛІЗ СИСТЕМИ МОНІТОРИНГУ ВРАЗЛИВОСТЕЙ WAZUH

2.1. Функціональні можливості та особливості Wazuh

Одним з продуктів для безперервного аналізу стану кібербезпеки підприємства було обрано рішення Wazuh.

Даний продукт – це багатофункціональна та ефективна платформа для моніторингу вразливостей і забезпечення безпеки. Її можливості з аналізу подій, управління політиками безпеки та інтеграції з іншими системами роблять її ідеальним вибором для підприємств, які прагнуть забезпечити високу кіберстійкість. Завдяки відкритому коду та підтримці масштабування, Wazuh може задовольнити потреби як малих компаній, так і великих корпорацій. через наступні його можливості (рис. 2.1):

- Моніторинг цілісності файлів (File Integrity Monitoring, FIM) – виявлення змін в налаштуваннях та підтримка процесу “керування змінами / Change management”
- Виявлення вразливостей – обробка бази вразливостей Common Vulnerabilities and Exposures (CVEs)
- Моніторинг подій і аналітика журналів – можливість виявити аномалії чи атаки на підключені мережеві станції в реальному часі
- Відповідність стандартам безпеки – для перевірки наявних системних налаштувань щодо відповідності стандартам безпеки
- Сповіщення та інтеграція з іншими системами – продукт має модуль сповіщень, що дозволяє налаштувати повідомлення для різних сценаріїв: від критичних інцидентів до рутинних подій. Це забезпечує своєчасне інформування команди безпеки та допомагає швидко реагувати на загрози.
- Підтримка операційних систем MacOS, Linux, Windows – цільова компанія використовує різні версії усіх цих операційних систем

- Створення звітів аудиту – необхідність наявності, принаймні щомісячних, повних звітів аудиту кібербезпеки, як робочих станцій внутрішньої мережі так і результати сканування опублікованих зовнішніх сервісів

Рис. 2.1 Функціональні можливості Wazuh

До особливостей продукту Wazuh відносять (рис. 2.2):

1. **Масштабованість.** Платформа розроблена для роботи у великих інфраструктурах. Завдяки розподіленій архітектурі Wazuh може обробляти велику кількість агентів і даних.
2. **Відкрите програмне забезпечення.** Wazuh є open-source проектом, що дозволяє організаціям адаптувати платформу під свої потреби без необхідності купувати дорогі ліцензії.

3. **Реальний час.** Система працює в реальному часі, забезпечуючи оперативне виявлення та реагування на загрози.

4. **Кросплатформеність.** Wazuh підтримує різні операційні системи, включаючи Windows, Linux, macOS, що робить її універсальним рішенням для гетерогенних середовищ.

5. **Активне співтовариство.** Завдяки активному співтовариству розробників і користувачів, Wazuh регулярно оновлюється, включаючи нові функції та поліпшення.

Рис. 2.2 Ключові особливості Wazuh

Що важливо, платформа Wazuh надає функції захисту робочих навантажень для хмари, контейнеру чи серверів за рахунок використання таких підходів

кібербезпеки, як **XDR** (e**X**tended **D**etection and **R**esponse) - активний XDR захист від сучасних загроз, з наступними можливостями (рис. 2.3):

- **Threat hunting** (*полювання на загрози*) - зниження середнього часу реагування на інциденти. Цей модуль Wazuh автоматично реагує на загрози, аби зменшити потенційний вплив на вашу інфраструктуру. Можливо використовувати як вбудовані дії реагування так і створювати власні дії відповідно до плану реагування на інциденти в організації.
- **Behavioral analysis** (*поведінковий аналіз*) – можливість виявляти та реагувати на загрози на основі аналізу незвичайної поведінки. Цей аналіз передбачає використання розширеної аналітики для виявлення відхилень від нормальної, очікуваної поведінки, що може свідчити на потенційні загрози безпеці. В цей функціонал включають моніторинг цілісності файлів, мережевого трафіку, поведінки користувачів та аномалій у показниках продуктивності системи.
- **Automated response** (*автоматизоване реагування*) - реагування на інциденти за допомогою Wazuh. Система може автоматично реагувати на загрози, та зменшувати потенційний вплив на інформаційну інфраструктуру. Можливо використовувати і вбудовані дії реагування і створювати власні, відповідно до плану реагування на інциденти.
- **Cloud workload protection** (*захист хмарних робочих навантажень*) – дозволяє захистити компоненти у хмарному середовищі і контейнерів, в тому числі. Wazuh вміє працювати з хмарними сервісами для збору та аналізу телеметрії. Що дуже важливо, продукт спроможний захистити в тому числі гібридні хмарні середовища, включаючи контейнерну інфраструктуру, виявляючи та реагуючи на поточні та нові загрози.
- **Threat intelligence** (*розвідка загроз*) - Wazuh використовує канали розвідки загроз для виявлення відомих загроз і реагування на них. Він інтегрується з джерелами даних з описом загроз, включаючи аналітику даних з відкритих джерел (OSINT), комерційні канали та дані, надані користувачами, щоб надавати актуальну інформацію про потенційні загрози.

- **Compliance and reporting** (*відповідність та звітність*) – перевірка відповідності нормативним вимогам, створення звітів за-для демонстрації ефективності програми безпеки організації. Wazuh має можливість автоматично виконувати перевірки на відповідність нормативним вимогам і стандартам безпеки, таким як PCI-DSS, HIPAA, GDPR тощо.
-

Рис. 2.3 Можливості модуля Wazuh XDR

SIEM (**S**ecurity **I**nformation and **E**vent **M**anagement) - централізована платформа для агрегування та аналізу телеметрії в режимі реального часу з метою виявлення загроз і дотримання нормативних вимог. Wazuh може збирати дані про події з різних джерел, таких як кінцеві точки, мережеві пристрої, хмарні робочі навантаження та додатки, щоб розширити охоплення безпеки.

Для рішення Wazuh характерними можливостями SIEM є (Рис. 2.4):

- **Security log analysis** (*аналіз журналів безпеки*) - Wazuh збирає, зберігає та аналізує дані про події безпеки, щоб виявити аномалії або ознаки компрометації.

Платформа SIEM додає контекстну інформацію до сповіщень, щоб прискорити розслідування та скоротити середній час реагування.

- **Vulnerability detection** (*виявлення вразливостей*) - Виявлення вразливостей на компонентах мережі, де розгорнуто агент Wazuh. Wazuh визначає пріоритетність виявлених вразливостей, щоб пришвидшити процес прийняття рішень та усунення. Ця функція гарантує відповідність нормативним вимогам, зменшуючи при цьому поверхню для атак.
- **Security Configuration Assessment** (*оцінка конфігурації безпеки*) - можливості виявлення неправильних конфігурацій і недоліків безпеки у вашій інфраструктурі. Wazuh сканує ваші системи на відповідність критеріям Центру інтернет-безпеки (CIS), щоб виявити та усунути вразливості, неправильні конфігурації або відхилення від найкращих практик і стандартів безпеки.
- **Regulatory compliance** (*відповідність нормативним вимогам*) - відстеження та можливість продемонструвати відповідність різним нормативним документам, таким як PCI DSS, NIST 800-53, GDPR, TSC SOC2 та HIPAA.
-

Рис. 2.4 Можливості модуля Wazuh SIEM

2.2. Порівняння Wazuh з альтернативними системами моніторингу вразливостей

На обраному для впровадження продукту Wazuh представнику малого бізнесу, було виявлено вже розгорнуте, подібне за функціоналом, рішення на основі продукту AllienVault OSSIM. Для визначення доцільності встановлення ще одного продукту, було проведено аналіз обох програм та подано аргументи, щодо користі встановлення продукту Wazuh.

Порівняльний опис оформлено в табл. 2.1. Особливу увагу слід звернути на таку властивість як «простота використання». Замовнику потрібно було аргументувати пропозицію встановити нове рішення, яке складніше від вже наявного, з аналогічним функціоналом.

Таблиця 2.1

Порівняння програмних продуктів Wazuh та AlienVault OSSIM

Властивість	**Wazuh**	**AlienVault OSSIM**
Основна спрямованість	Основна увага зосереджена на моніторингу вразливостей, управлінні конфігураціями, аналізі журналів та моніторингу відповідності політикам безпеки. Wazuh пропонує широкий набір інтеграцій із SIEM-рішеннями, такими як Elastic Stack.	Головний фокус — це комплексна система SIEM, що забезпечує кореляцію подій, аналіз трафіку, моніторинг вразливостей та управління вторгненнями. AlienVault OSSIM більше орієнтований на централізацію безпеки.
Архітектура	Побудований на розподіленій архітектурі, що дозволяє масштабуватися для обробки великої кількості даних. Завдяки агентам Wazuh забезпечує тісну інтеграцію з кінцевими точками.	Платформа OSSIM є централізованою системою, яка поєднує кілька модулів для збору даних, кореляції подій та моніторингу трафіку. Вона більше підходить для середовищ із помірною складністю.

Продовження таблиці 2.1

Властивість	Wazuh	AlienVault OSSIM
Моніторинг вразливостей	Використовує бази CVE та інтеграцію з NVD для виявлення вразливостей у програмному забезпеченні. Пропонує деталізовані звіти про вразливості з рекомендаціями щодо їх усунення.	Також підтримує моніторинг вразливостей через інтеграцію з OpenVAS. Однак цей функціонал є менш гнучким і більш обмеженим у порівнянні з Wazuh.
Аналіз журналів	Високоефективний аналіз журналів із підтримкою великої кількості джерел (операційні системи, мережеве обладнання, додатки). Підтримка Elastic Stack дозволяє створювати гнучкі візуалізації та звіти.	Аналіз журналів є складовою частиною SIEM-рішення, але можливості кастомізації візуалізацій і звітів дещо обмежені у порівнянні з інтеграцією Wazuh та Elastic Stack.
Кореляція подій	Підтримує базову кореляцію подій через аналіз логів та інші механізми моніторингу. Для більш складних сценаріїв кореляції потрібна інтеграція з Elastic Stack або іншими SIEM-рішеннями.	Одна з основних переваг — вбудована система кореляції подій з використанням попередньо налаштованих правил. Вона підходить для організацій, які потребують простого та швидкого впровадження SIEM.
Інтеграція	Легко інтегрується з Elastic Stack для візуалізації даних та створення кастомних панелей. Також підтримує інтеграцію з іншими SIEM-системами та зовнішніми базами даних.	Пропонує інтеграцію з OpenVAS, Suricata та іншими інструментами безпеки, але можливості розширення обмежені в порівнянні з Wazuh.
Масштабованість	Розподілена архітектура дозволяє легко масштабувати систему для великих організацій із великою кількістю кінцевих точок.	Менш масштабований через централізовану архітектуру, що може стати обмеженням для великих підприємств.

Продовження таблиці 2.1

Властивість	Wazuh	AlienVault OSSIM
Простота використання	Має більш складну конфігурацію на етапі впровадження, але після налаштування забезпечує гнучкість та багатий функціонал.	Простий у впровадженні завдяки попередньо налаштованим модулям, але менш адаптивний до специфічних потреб організацій.
Вартість	Повністю безкоштовний open-source проєкт із активною підтримкою спільноти.	Також є open-source рішенням, але для отримання розширеного функціоналу необхідно використовувати платний AlienVault USM (Unified Security Management).

Коли обирати Wazuh? Якщо організації потрібна гнучка та масштабована платформа для моніторингу вразливостей, аналізу журналів та відповідності стандартам безпеки, Wazuh стане ідеальним рішенням.

Коли обирати AlienVault OSSIM? Якщо очікується проста у використанні SIEM-система з базовим функціоналом моніторингу вразливостей і кореляції подій, AlienVault OSSIM буде оптимальним вибором.

Обидві системи мають свої сильні сторони, тому остаточний вибір залежить від вимог до функціоналу, масштабу інфраструктури та бюджету.

В нашому випадку, вибраній організації було запропоновано паралельне використання обох продуктів. До вже робочого рішення AlienVault OSSIM запропоновано додати новий продукт Wazuh. Оскільки в деяких налаштуваннях ці рішення можуть конфліктувати, задача вимагатиме детального опису внесених змін.

Можливою альтернативою до продуктів AlienVault OSSIM та Wazuh можна частково розглядати рішення Lynis [16], яке має open-source варіант та серед своїх можливостей зазначає підтримку перевірки відповідності налаштувань до

рекомендацій CIS Benchmarks. Нажаль, великим обмеженням в нашому випадку, мусимо рахувати відсутність підтримки операційних систем Windows у списку підтримуваних. На противагу, сильною стороною є підтримка Linux/Unix орієнтованих систем, в тому числі й MacOS. Ми ж маємо не забувати, що в нашій роботі ми розглядаємо організації, що працюють з медіа-контентом, де професійні продукти обробки звуку та відео часто працюють на базі операційних систем MacOS, як стандарту де-факто.

Згадаємо продукт Security Onion [16] який вільним для завантаження та використання та у своєму функціоналі має можливості здійснення перевірки мережі через програми Snort або Suricata. Складність продукту в тому, що це лише набір інструментів, а усі налаштування необхідно буде виконувати самостійно. Також, відсутня вбудована можливість перевірки на відповідності CIS Benchmarks та формування відповідних звітів. Вважаємо, що цей продукт складно рекомендувати у якості «швидкого старту» при проведенні самостійного аудиту безпеки організації.

Продукт CIS-CAT Lite [17] від безпосереднього розробника CIS Benchmarks дозволяє безкоштовно виконати деякі тести на відповідність цим стандартам. Програма надає базові можливості сканування відповідно до CIS Benchmarks, але значно обмежена у функціональності порівняно з Pro версією і підходить для організацій, які потребують базового аналізу відповідності, але не можуть виправдати вартість повного членства в CIS SecureSuite. Великий мінус – відсутність централізованої консолі керування. Тут, навпаки, потрібно запускати цю програму безпосередньо на кожній клієнтській станції, для отримання звітів.
Коротко згадаємо безкоштовний продукт Trivy [18] який більше розрахований для самодіагностики помилок конфігурації для програмних пакетів та налаштувань певних збірок Linux. Нам цей продукт не підійде через відсутність підтримки систем Windows та Mac OS.

2.3. Переваги використання Wazuh для малого та середнього бізнесу

Попри наявність департаментів IT у великому чи відділів IT у середньому бізнесі, та відповідні бюджети, малий бізнес часто неспроможний навіть утримувати IT-спеціаліста на постійній основі. Це, також, особливо стосується проектів-стартапів, які маючи бізнес-ідею, мають встигнути безперешкодно розвинутися у перший рік операційної діяльності. Будь-яка заминка, зупинка, втрата часу, може збанкрутувати юний бізнес-проект через його постійні витрати, які переважають операційні доходи.

Використання open-source продуктів аналізу кібербезпеки поєднує бюджетність їх використання та ефект від підвищення стану захищеності інформаційних систем. Взявши за основу рекомендації Держспецзв'язку [7], котрі базовані на світових стандартах [8], [9] перевіримо продукт Wazuh у якості можливого інструменту реалізації наших цілей табл. 2.2.

Таблиця 2.2

Технічні можливості аудиту стану кібербезпеки засобами WAZUH щодо відповідності стандартам NIST SP 800-53 [9]*

Розділ - код, англійською	**Нотатки до розділу**	**Загальна кількість секцій розділу**	**Кількість секцій розділу, під перевіркою Wazuh**
Access Control - **AC**	Контроль доступу	131	46
Awareness and training - **AT**	Поінформованість та навчання	15	5
Audit and accountability - **AU**	Аудит та підзвітність	56	38
Assessment, authorization and monitoring - **CA**	Оцінка, дозволи та моніторинг	25	9
Configuration management - **CM**	Управління конфігураціями	54	35

Продовження таблиці 2.2

Розділ - код, англійською	**Нотатки до розділу**	**Загальна кількість секцій розділу**	**Кількість секцій розділу, під перевіркою Wazuh**
Contingency planning - **CP**	Планування на випадок надзвичайних ситуацій	49	0
Identification and authentication - **IA**	Ідентифікація та автентифікація	55	19
Incident response - **IR**	Реагування на інциденти	40	27
Maintenance - **MA**	Обслуговування	28	9
Media protection - **MP**	Захист носіїв інформації	19	5
Physical and environmental protection - **PE**	Фізичний захист та навколишнього середовища	51	0
Planning - **PL**	Планування	11	3
Program management - **PM**	Управління програмами	37	7
Personnel security - **PS**	Безпека персоналу	18	0
Personally identifiable information processing and transparency - **PT**	Обробка персональних даних та прозорість	21	4
Risk assessment - **RA**	Оцінка ризиків	22	13
System and services acquisition - **SA**	Придбання систем та послуг	105	20
System and communications protection - **SC**	Захист систем та комунікацій	140	40

Продовження таблиці 2.2

Розділ - код, англійською	**Нотатки до розділу**	**Загальна кількість секцій розділу**	**Кількість секцій розділу, під перевіркою Wazuh**
System and information integrity - **SI**	Цілісність системи та інформації	101	50
Supply chain risk management - **SR**	Управління ризиками ланцюга постачання	27	0

* - статус Withdrawn (Відкликано) – не враховувався у підрахунку

Згідно аналізу щодо відповідності стандарту NIST SP 800-53 [9] до результатів аудиту можливостей розгорнутої системи аналізу кібербезпеки на базі продукту Wazuh, можемо констатувати, що це рішення забезпечує неповне, часткове задоволення наших задач. Звісно ж, секції вимог [9], які стосуються створення логіки організаційних процесів, наявності документації, забезпечення фізичної безпеки, роботи з персоналом, контролю логістичних ланцюжків, захисту навколишнього середовища не можуть бути автоматично перевірені продуктом Wazuh.

Ще раз визначаючи переваги Wazuh — це відкрите рішення для моніторингу безпеки, яке пропонує комплексні можливості для захисту IT-інфраструктури. Використання Wazuh приносить ряд значущих переваг, які роблять його популярним вибором серед багатьох організацій, зайнятих питаннями кібербезпеки. Ось деякі з ключових переваг використання Wazuh:

Всебічне виявлення загроз - дозволяє організаціям ефективно виявляти потенційні загрози та зловживання в реальному часі. Завдяки інтеграції з іншими інструментами безпеки, Wazuh надає широкі можливості для аналізу та кореляції подій, що допомагає виявляти складні атаки, які можуть залишитися непоміченими іншими системами.

Моніторинг цілісності файлів - функція моніторингу цілісності файлів в Wazuh дозволяє слідкувати за будь-якими змінами у системних файлах та конфігураціях. Це критично важливо для забезпечення того, що вразливі або важливі файли не були змінені в результаті несанкціонованих дій.

Логування та аналіз подій - Wazuh ефективно збирає, аналізує та зберігає логи з різних джерел, забезпечуючи глибокий аналіз даних. Це дозволяє адміністраторам систем і фахівцям з безпеки швидко виявляти та реагувати на підозрілу поведінку або потенційні загрози.

Перевірка на відповідність стандартам - продукт допомагає організаціям дотримуватися вимог, таких як PCI DSS, HIPAA, GDPR та інші. Завдяки гнучким налаштуванням і обширним можливостям звітності, Wazuh може бути налаштований для відповідності специфічним вимогам комплаєнсу.

Відкрите програмне забезпечення - як відкритий продукт, Wazuh пропонує високий рівень прозорості, гнучкості та можливість налаштування. Спільнота розробників постійно працює над удосконаленнями і оновленнями, що забезпечує актуальність інструменту відповідно до останніх тенденцій і загроз у сфері кібербезпеки.

Легкість інтеграції - легко інтегрується з широким спектром інших інструментів і технологій, включаючи Elasticsearch для збору та аналізу даних, а також різні платформи моніторингу і управління безпекою. Це дозволяє організаціям створювати комплексні системи безпеки, які відповідають їхнім унікальним потребам.

Використання Wazuh є ефективним рішенням для організацій, які прагнуть забезпечити комплексний захист своїх IT-інфраструктур в умовах зростаючих кіберзагроз. Його широкі можливості і гнучкість роблять його ідеальним вибором для компаній будь-якого розміру. Продукт може рости, розвиватися, масштабуватися паралельно з ростом організації.

3 ВПРОВАДЖЕННЯ РІШЕННЯ ДЛЯ МОНІТОРИНГУ СИСТЕМНИХ ВРАЗЛИВОСТЕЙ НА БАЗІ WAZUH

3.1. Концептуальна модель розгортання Wazuh у реальному бізнес-середовищі

Архітектура Wazuh складається з трьох основних компонентів (рис. 3.1): агента, сервера та індексатора.

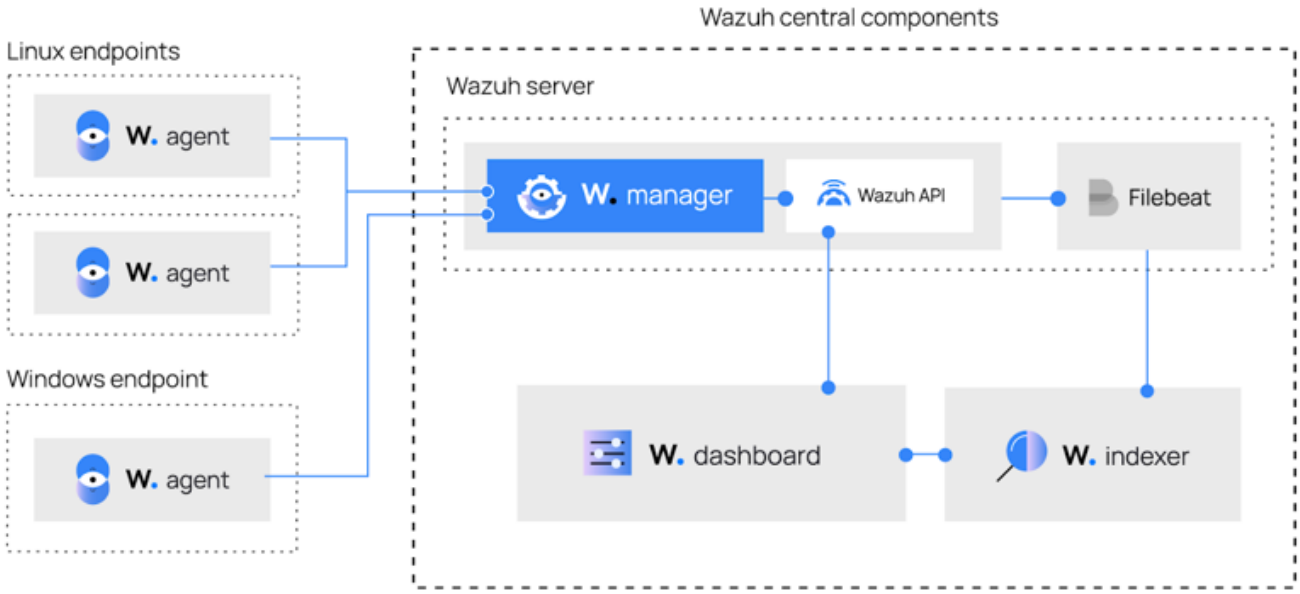


Рис. 3.1 Концептуальна схема розгортання рішення Wazuh [10]

На вибір можлива гнучкість в технічній реалізації рішення, а саме – вибір операційної системи, на якій буде оперувати серверна частина продукту - Amazon Linux 2, Amazon Linux 2023; Centos 7, 8; Red Hat Enterprise Linux 7, 8, 9; Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04.

Усі компоненти можливо встановити на одному сервері, але для розгортання системи, яка архітектурно може легко розширюватися з часом, рекомендується серверні ролі розділяти, та, більше того – встановлювати по кілька екземплярів ролі будуючи кластерні рішення, що передбачено та підтримується системами Wazuh.

Зважаючи на реалії сьогодення, де вплив військових дій додає вищого рівня ризику функціонуванню IT-інфраструктури в Україні, пропонуємо розглядати гібридний варіант встановлення, де частина інфраструктури розміщена у фізичній IT-інфраструктурі організації, частина учасників кластеру – в українських дата-центрах, а ще частина – у хмарному середовищі великих провайдерів на зразок Google Cloud, Amazon AWS чи Microsoft Azure.

Тут буде спостерігатися розподіл по вартості володіння та доступності сервісів. Найдорожчим варіантом, більш за-все, буде оренда ресурсів великих хмарних провайдерів, натомість, при терміновій, часто позаплановій евакуації бізнесу, це дозволить не втрати дані, навіть втративши фізичну локацію та її IT-інфраструктуру.

Рішення Wazuh включає в себе ряд компонентів, які ми описуємо нижче:

1. Wazuh Agent

Цей компонент в архітектурі Wazuh, встановлюється на кінцевих точках, таких як сервери та робочі станції, для моніторингу безпеки, збору даних та виявлення загроз.

Першим кроком є встановлення Wazuh Agent на кінцевих точках, що потребують моніторингу. Після встановлення, агент потрібно зареєструвати на Wazuh Manager — центральному компоненті системи, який обробляє дані від агентів. Реєстрація зазвичай включає налаштування унікального ідентифікатора агента та ключа аутентифікації, що забезпечує безпечне з'єднання між агентом і менеджером. Після встановлення та запуску сервісу, Wazuh Agent починає виконувати низку функцій моніторингу на кінцевій точці, включаючи:

- **Моніторинг цілісності файлів** - агент відстежує зміни у файловій системі, порівнюючи поточний стан файлів з їх попередніми станами.
- **Виявлення зловмисного ПЗ** - агент може використовувати різні сигнатури та евристичні правила для виявлення потенційно шкідливих програм.

- **Збір системних логів** - агент збирає логи з різних системних джерел, включаючи системні журнали, застосунки та служби.

Зібрані дані, включаючи повідомлення про інциденти, логи та результати аналізу, передаються до Wazuh Manager через зашифроване з'єднання. Дані надсилаються у форматі, який оптимізований для аналізу та кореляції на стороні менеджера.

Використання Wazuh Agent дозволяє організаціям забезпечувати глибокий моніторинг безпеки та оперативно реагувати на загрози, підтримуючи високий рівень захисту IT-інфраструктури.

2. Wazuh Server

Це центральний компонентом архітектури Wazuh який також відомий як Wazuh Manager. Він відповідає за аналіз, обробку та управління даними, які збираються Wazuh Agents з різних кінцевих точок.

Основні функції ролі Wazuh Server:

- **Збір інформації** - отримує дані зібрані агентами, які включають логи системи, звіти про цілісність файлів, інформацію про конфігурації системи, дані про виявлені загрози та інші важливі метрики безпеки.
- **Обробка і аналіз даних** - після отримання даних, сервер використовує різні аналітичні інструменти для обробки і аналізу цієї інформації. Він використовує кореляційні правила, алгоритми виявлення загроз, і гнучкі шаблони пошуку для виявлення ненормальних поведінок або можливих безпекових інцидентів.
- **Кореляція подій -** Wazuh Server використовує механізми кореляції подій для з'єднання різних логів та сповіщень в єдині інциденти. Це дозволяє системі точно ідентифікувати складні атаки, які можуть бути розподілені у часі та виконуватися через різні системи.

- **Управління сповіщеннями** - Wazuh Server керує налаштуваннями сповіщень, які відправляються адміністраторам або іншим системам керування за допомогою інтеграції з зовнішніми інструментами та платформами.
- **Звітність і моніторинг** - сервер генерує звіти про стан безпеки, виявлені загрози, і відповідність стандартам безпеки. Крім того, Wazuh Manager надає інтерфейс для моніторингу поточного стану IT-інфраструктури.
- **Управління агентами** - керує налаштуваннями та оновленнями для агентів, включаючи розгортання оновлень правил виявлення, оновлень сигнатур антивірусів та інших компонентів безпеки.

На основі рекомендацій (табл. 3.1) щодо апаратної частини нами було обрано конфігурацію за мінімальними вимогами щодо обсягів оперативної пам’яті та кількості процесорних ядер. Оскільки саме рішення розгорнуте у віртуалізованій інфраструктурі, виділення додаткових ресурсів оперативної пам’яті чи процесорних потужностей не потребуватиме тривалого часу.

Таблиця 3.1

Рекомендації апаратної частини для Wazuh Server

Компонент	Мінімально		Рекомендовано	
	Оперативна пам’ять (Gb)	Центральний процесор (ядра)	Оперативна пам’ять (Gb)	Центральний процесор (ядра)
Wazuh Server	2	2	4	8

Щодо дискового простору, то ґрунтуючись рекомендаціями (табл. 3.2), можливе заповнення даними для 18-ти серверів та 28-ми робочих станцій замовника, за 365 днів складе 11,68Gb (табл. 3.3).

Фактично виділений дисковий простір було надано в 32Gb, чого має бути достатньо в річному вимірі утримання даних.

Таблиця 3.2

Рекомендації щодо об’єму дискового простору для Wazuh Server

Кількість агентів моніторингу	Кількість повідомлень в секунду	Дисковий простір, в Gb за 90 днів
Сервери	0,25	0,1
Робочі станції	0,1	0,04
Мережеві пристрої	0,5	0,2

Таблиця 3.3

Рекомендації замовнику щодо об’єму дискового простору для Wazuh Server

Кількість агентів могніторингу	Дисковий простір, в Gb за 360 днів	Необхідний простір в Gb для утримання даних за 360 днів
Сервери == 18	0,4	18 × 0,4 = 7,2
Робочі станції == 28	0,16	28 × 0,16 = 4,48

3. Wazuh Indexer

Цей компонент заснований на технології Elasticsearch, яка широко використовується розподіленою системою пошуку та аналітики і призначений для зберігання, індексації та пошуку даних, зібраних Wazuh Manager:

- **Індексація та Зберігання** - відповідає за прийом логів та інших типів даних від Wazuh Manager, які включають системні логи, звіти про виявлення загроз, інформацію про стан системи, деталі про мережевий трафік, і т.д. Ці дані індексуються для забезпечення швидкого пошуку і аналітики.
- **Пошук та Аналітика** - завдяки потужним можливостям Elasticsearch, дозволяє виконувати складні запити на пошук та аналітичні операції з даними, що допомагає аналізувати тенденції, виявляти аномалії та відстежувати загрози в реальному часі.

- **Масштабованість** - може масштабуватися горизонтально для підтримки збільшення обсягів даних та запитів. Це дозволяє адаптувати систему під зростаючі потреби організацій без втрати продуктивності.

Керуючись рекомендаціями виробника (табл. 3.4) щодо обсягів оперативної пам’яті та кількості процесорних ядер, нами було обрано конфігурацію за мінімальними вимогами, адже рішення розгорнуте у віртуалізованій інфраструктурі, виділення додаткових ресурсів оперативної пам’яті чи процесорних потужностей не потребуватиме тривалого часу.

Таблиця 3.4

Рекомендації апаратної частини для Wazuh Indexer

Компонент	Мінімально		Рекомендовано	
	Оперативна пам’ять (Gb)	Центральний процесор (ядра)	Оперативна пам’ять (Gb)	Центральний процесор (ядра)
Wazuh Server	4	2	16	8

Щодо дискового простору, то керуючись рекомендаціями виробника (Табл. 3.5), можливе заповнення даними для 18-ти серверів та 28-ми робочих станцій замовника, за 90 днів складе 108,6 Gb:

Для 18-ти серверів, за 90 днів: $3{,}7 \times 18 = 66{,}6$ Gb

Для 28-ми станцій, за 90 днів: $1{,}5 \times 28 = 42{,}0$ Gb

Таблиця 3.5

Рекомендації щодо об'єму дискового простору для Wazuh Indexer

Кількість агентів могніторингу	Кількість повідомлень в секунду	Дисковий простір, в Gb за 90 днів
Сервери	0,25	3,7
Робочі станції	0,1	1,5
Мережеві пристрої	0,5	7,4

Зважаючи на регламентований час утримання записів журналів безпеки в 1 рік, ми збільшили наші обрахункові дані в 4 рази, до 360 діб. В результаті фіксуємо (Табл. 3.6) 434,4 Gb - як рекомендований мінімальний дисковий простір для серверу Wazuh Indexer.

Для 18-ти серверів, за 360 днів: 66,6 × 4 = 266,4 Gb

Для 28-ми станцій, за 360 днів: 42,0 × 4 = 168,0 Gb

Таблиця 3.6

Рекомендації замовнику щодо об'єму дискового простору для Wazuh Indexer

Кількість агентів могніторингу	Дисковий простір, в Gb за 360 днів	Необхідний простір в Gb для утримання даних за 360 днів
Сервери == 18	14,8	18 × 14,8 = 266,4
Робочі станції == 28	6,0	28 × 6,0 = 168,0

4. Wazuh Dashboard

Цей компонент дозволяє користувачам візуалізувати та аналізувати зібрані дані про безпеку, та надає інтерфейс для швидкого доступу до звітів, моніторингу стану безпеки та управління інцидентами, з такими можливостями:

- **Інтерактивна візуалізація -** можливість створювати різноманітні візуалізації, такі як графіки, таблиці, та карти, які допомагають зрозуміти складні набори даних та виявляти тенденції та аномалії в поведінці системи.
- **Реалізація звітів -** дозволяє генерувати звіти на основі зібраних даних, включаючи інформацію про виявлені загрози, зміни в системі, інциденти безпеки та стан відповідності нормативним вимогам.
- **Моніторинг стану системи** - надає огляд поточного стану системи та безпеки, включаючи стан агентів, оновлення правил виявлення, стан моніторингу цілісності файлів та багато іншого.
- **Керування конфігураціями -** можливо використовувати Wazuh Dashboard для перегляду та зміни налаштувань Wazuh агентів, управління політиками безпеки, та налаштування правил виявлення загроз.

Керуючись рекомендаціями виробника (табл. 3.7) щодо обсягів оперативної пам’яті та кількості процесорних ядер, Нами було обрано конфігурацію за мінімальними вимогами щодо обсягів оперативної пам’яті та кількості процесорних ядер. Окремо зазначимо, що обсяг дискового простору було встановлено на рівні 16Gb.

Таблиця 3.7

Рекомендації щодо об'єму дискового простору для Wazuh dashboard

Компонент	Мінімально		Рекомендовано	
	Оперативна пам’ять (Gb)	Центральний процесор (ядра)	Оперативна пам’ять (Gb)	Центральний процесор (ядра)
Wazuh dashboard	4	2	8	4

Провівши аналіз поточної схеми мережевих підключень вибраної для впровадження Wazuh комерційної організації, було виявлене резервування фізичних та логічних сервісів на всіх її сегментах. Зважаючи на діючу підписку про нерозголошення комерційної інформації, подається виключно спрощена схема (рис. 3.2) мережі, до якої можна додатково зазначити, що:

- Інтернет-підключення захищене фаєрволом;
- Сервіси компанії, опубліковані для доступу з терен Інтернету – захищені окремим фаєрволом та не мають прямого доступу до ресурсів локальної мережі як і немає доступу з локальних мереж до цих, опублікованих в Інтернеті сервісів;
- Набори мережевих ресурсів виокремлені в свої окремі мережі фізично чи/та з використанням технології VLAN;
- Комунікації між внутрішніми мережами відбувається виключено через внутрішній фаєрвол;
- Правила фаєрволу діють за принципом «заборонено усе, що явно не дозволено» з обмеженнями по протоколах, портах та маршрутах трафіку;

- Компанія використовує технології віртуалізації.
- За рахунок використання певної кількості серверів віртуалізації, є можливість створення кластерних рішень з розосередженням компонентів по різним фізичним серверам організації.

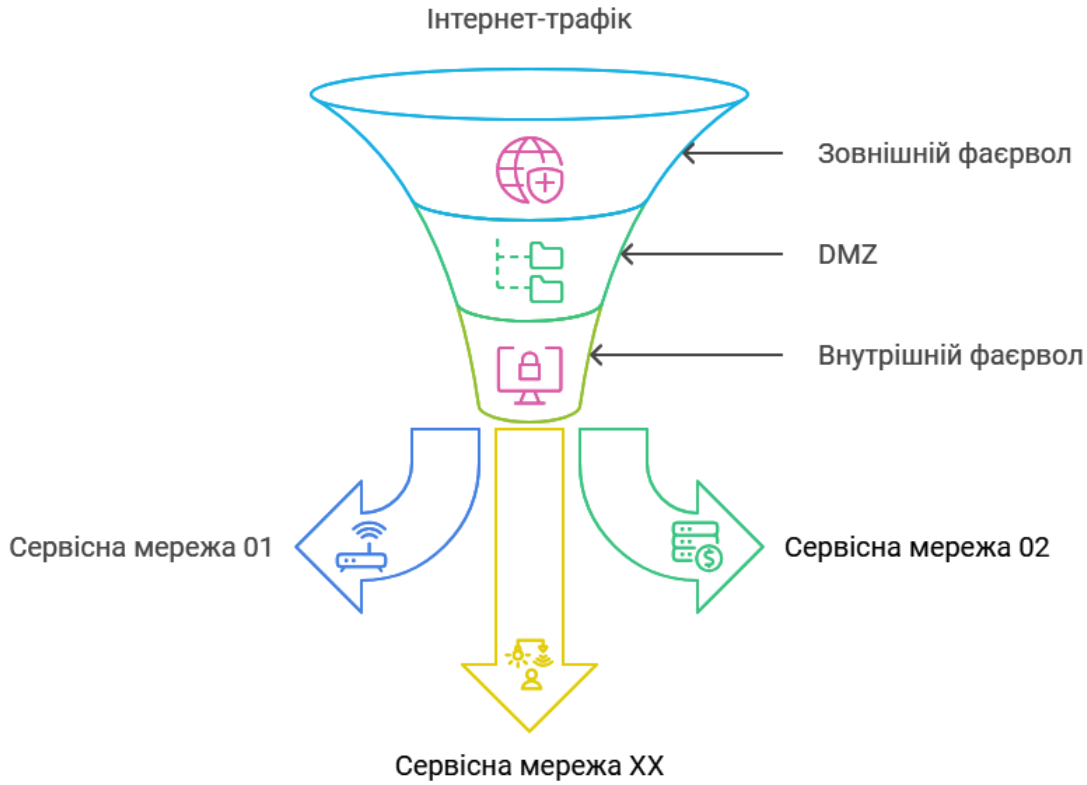


Рис 3.2 Спрощена схема мережі організації до початку впровадження Wazuh

Після консультацій, з організацією було узгоджено рішення, згідно якого:

- створюється нова, окрема мережа, виокремлена в новий VLAN;
- створюється набір віртуальних станцій, згідно типових рекомендацій розробника Wazuh;
- усі мережеві адреси налаштовуються виключно в ручному режимі, без використання сервісів DHCP;
- на початковому етапі тестування, створені віртуальні станції будуть працювати з обмеженими системними ресурсами, мінімально рекомендованими виробником Wazuh;

- заздалегідь документуються мережеві маршрути включно з напрямом «від-до», протоколом, цифрою мережевого порта, функціональною роллю;
- організація-замовник надає перелік мережевих ресурсів, на яких заплановано встановлення компонентів Wazuh Agent;
- на кінцевих робочих станціях з Wazuh Agent буде створено виключення в налаштуваннях локального фаєрволу, антивірусу та в політиках запуску програм для коректного функціонування агента сервісу;
- узгоджено встановлення останньої стабільної версії компонентів Wazuh

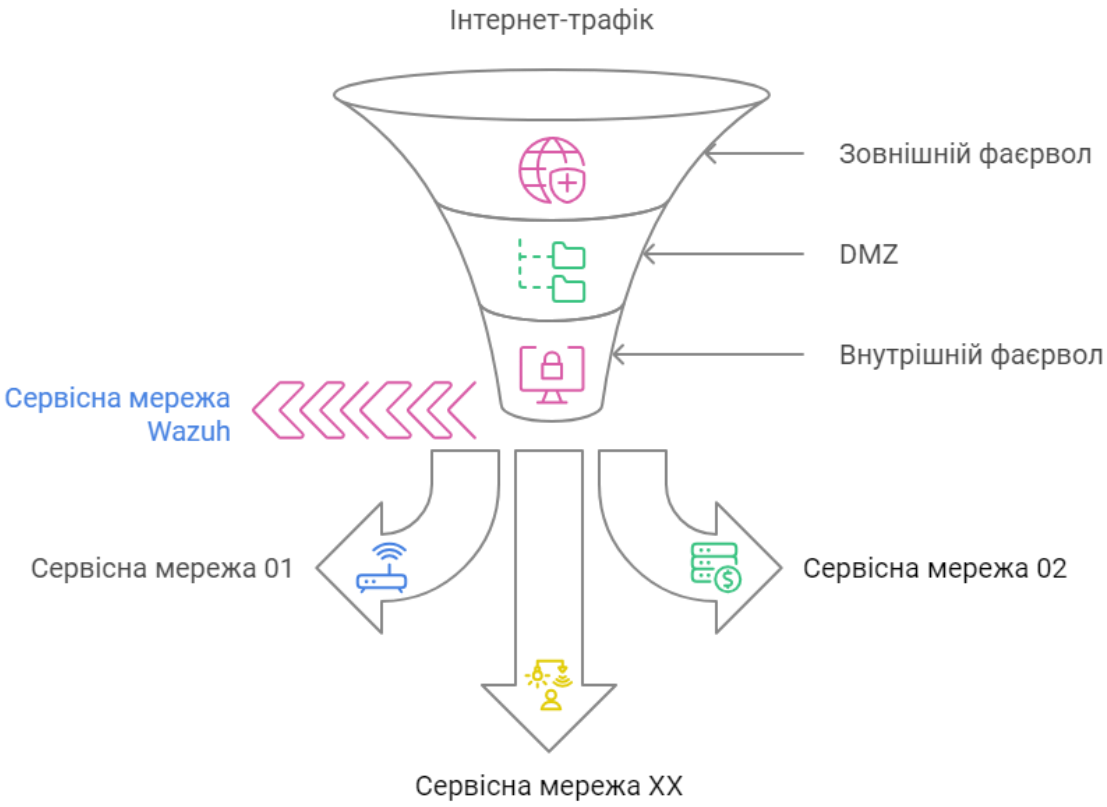


Рис 3.3 Спрощена схема мережі організації з включенням сервісної мережі Wazuh

Особливістю реалізації рішення, яке пропонується в рамках кваліфікаційної роботи, виявилося бажання замовника у використанні операційної системи Debian 12 у якості платформи для запуску компонентів системи. Така специфіка додала потреби в лабораторному дослідженні нюансів встановлення, адже

операційна система Debian не вказана, як така, що гарантовано підтримуються виробником ПЗ [25].

Натомість, зважаючи на згадку лінійки операційних систем Ubuntu, як таких, що підтримуються в сценаріях розгортання Wazuh, та заважаючи на те, що Ubuntu базована саме на системі Debian, було проведено підготовчі роботи для визначення потенціалу сумісності поєднання Debian12/Wazuh. Далі, буде описано досвід цього тестування.

Першим сценарієм розгортання були обрані інструкції категорії **Assisted installation** (*Допомога в установці*). Нажаль, після покрокового виконання усіх описаних процедур, було зафіксовані помилки підключення ролі Dashboard до ресурсів ролі Wazuh-Server. Час на спроби вирішення помилок виявився тривалим та зайняв біля одного робочого дня для дослідження, що на нашу думку, є надто надмірною та неефективною тратою часу. Зважаючи на обмежений час для роботи в IT-системі замовника, ми відмовились від цього сценарію розгортання.

В наступній ітерації, встановлення виконувалося за описом документації в категорії **Step-by-step installation** (*Покрокове встановлення*). У даному випадку, встановлення усіх компонентів рішення Wazuh було вдалим і у фіналі було отримано робочу систему. Таким чином вдалося поза основною тематикою нашої роботи, визначити можливість розгортання рішення Wazuh на офіційно не зазначеній операційний системі Debian 12.

Нижче виокремлено додаткові особливості розгортання. Отож, в основі платформи, використовувалася операційна система Debian 12.8 зі встановленням з базовими компонентами та додатково – SSH Server. Додатково, було встановлено лише компоненти **debhelper** та **curl.**

Також, для наступної демонстрації замовнику, паралельно були розгорнуті віртуалізовані операційні системи без додаткових налаштувань але з ініціацією отримання останніх доступних для операційної системи оновлень. Тут, основною метою було створити тестове середовище для визначення ризику можливого

включення у виробничу мережу неналежно підготовлених щодо кібербезпеки операційних систем.

Виявилося, що помилково названі робочі станції зі вже встановленими компонентами Wazuh Agent залишалися зі старими назвами в консолі Wazuh навіть після зміни назви робочої станції. Отож, компонент агенту не може динамічно оновлювати своє ім’я на стороні серверу.

Корекцію можливо здійснити лише в консолі серверної частини, наприклад, наступними кроками:

Для отримання списку зареєстрованих Wazuh-агентів, в консолі Wazuh-Server виконується команда

```
/var/ossec/bin/manage_agents -l
```

Визначивши номер станції за значенням ID, видаляється запис командою

```
/var/ossec/bin/manage_agents -r <agent-id>
```

Wazuh Agent на переназваній операційній системі перереєструється з цією новою назвою на сервері Wazuh Server та отримає новий ID, наступний після цифри найбільшого ID.

Варто зазначити важливі зміни, виконані в конфігурації Wazuh-Server, де були перейменовані файли cis_###.yml.disabled на cis_###.yml у каталозі правил /var/ossec/ruleset/sca

Також, внесено зміни в файл конфігурації **ossec.config:**

Увімкнено розширену журналізація подій:

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>yes</logall>
    <logall_json>yes</logall_json>
```

Інтервал перевірок знижено з 12 до 2 годин:

```
<sca>
    <enabled>yes</enabled>
    <scan_on_start>yes</scan_on_start>
    <interval>2h</interval>
    <skip_nfs>yes</skip_nfs>
</sca>
```

Таким чином, було свідомо зменшено паузу між виконання автоматизованих тестів безпеки станцій з боку серверу Wazuh.

3.2. Автоматизація встановлення та налаштування Wazuh, перевірка його працездатності

Автоматизація встановлення та налаштування Wazuh значно спрощує процес розгортання системи моніторингу безпеки, особливо в масштабних інфраструктурах. Після успішного налаштування важливо перевірити працездатність системи, щоб переконатися в її коректному функціонуванні.

Одним з варіантів автоматизації, буде попереднє розгортання та налаштування компонентів Wazuh та їх збереження у якості шаблонних. Такий варіант відмінно підійде при використанні систем віртуалізації, де збережені образи операційних систем будуть потребувати лише запуску процедур оновлення та очікуватимуть підключення агентів моніторингу.

Академічно, більш правильним, будуть рішення скриптового, автоматичного встановлення з використанням заданих параметрів на рівні змінних. Такі практики часто притаманні спеціалістам DevOps і мають сенс за умови частого, регулярного розгортання типових рішень. Тут, мова йде про інструменти Puppet, Chef, Ansible, Terraform.

Наш шлях до автоматизації, слідував через покрокове виконання описаних в офіційній документації дій для встановлення на платформі операційній системі з

DEB-пакетами. Усі кроки записувалися та перевірялися можливі помилки. Використовуючи засоби віртуалізації, віртуальну машину записували на проміжних етапах, аби залишалася можливість повернутися до попереднього стану операційної системи за умови внесення помилкових даних в процесі розгортання.

Для автоматизації процесу встановлення Wazuh можна скористатися офіційним скриптом установки, який спрощує розгортання всіх необхідних компонентів.

Процес спрощеного розгортання ролі **Wazuh Indexer**:

Завантаження скрипта установки:

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

Завантаження шаблону конфігурації:

```
curl -sO https://packages.wazuh.com/4.9/config.yml
```

Редагування файлу конфігурації:

```
nano ./config.yml
```

Де, у файлі вносяться дані (*ip-адреси тут, для прикладу*):

```
nodes:
  indexer:
    - name: node-1
      ip: "10.100.0.235"
  server:
    - name: wazuh-1
      ip: "10.100.0.236"
  dashboard:
    - name: dashboard
      ip: "10.100.0.237"
```

Виконується скрипт встановлення з ініціацією генерування налаштувань:

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

Встановлення ролі Wazuh Indexer:

```
bash wazuh-install.sh --wazuh-indexer node-1
```

Ініціалізація кластер ролі Wazuh Indexer:

```
bash wazuh-install.sh --start-cluster
```

Отримання паролю адміністратора:

```
tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O
| grep -P "\'admin\'" -A 1
```

Перевірка підключення, де <ADMIN_PASSWORD> - пароль адміністратора з попередньої команди:

```
curl -k -u admin:<ADMIN_PASSWORD> https://10.100.0.235:9200
```

Перевірка учасників кластеру Wazuh Indexer:

```
curl -k -u admin:<ADMIN_PASSWORD> https://10.100.0.235:9200/_cat/nodes?v
```

З серверу ролі Wazuh Indexer копіюються попередньо згенеровані конфігураційні файли до сервері ролі Wazuh Server та Wazuh Dashboard, за шаблоном команди, змінивши користувача, та ip-адресу цільового серверу.

```
scp wazuh-install-files.tar admin@10.100.0.236:
```

Процес спрощеного розгортання ролі **Wazuh Server**:

Підключеннядо станції з запланованою роллю Wazuh Server.

Завантаження скрипта установки:

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

Встановлення ролі Wazuh Server:

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

Процес спрощеного розгортання ролі **Wazuh Dashboard**:

Підключення до станції з запланованою роллю Wazuh Dashboard.

Завантаження скрипта установки:

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

Встановлення ролі Wazuh Dashboard:

```
bash wazuh-install.sh --wazuh-dashboard dashboard
```

За результатами виконання, має бути отримана стрічка з адресою серверу, логіном ролі Administrator та його паролем підключення.

Варіанти автоматизації розгортання Wazuh Agent залежить від середовища, в якому функціонують системні компоненти. Наприклад, для робочих станцій, учасників домену Microsoft Active Directory можна розгорнути групову політику з ініціацією встановлення інсталяційного пакету Wazuh Agent яку приєднуємо до організаційного юніту домену з об’єктами класу комп’ютер.

Використовуючи компоненти Puppet Agent на клієнтських станціях та Puppet Master у якості керуючого ресурсу, можливо ініціювати встановлення Wazuh модулів як під системами класу Linux, MacOS так і Windows.

Використання інструменту Ansible буде швидким та простим рішенням, але лише за умови тривалої підготовки та тестування Ansible playbook описів, що зафіксує втрату часу на вивчення цього додаткового інструменту і матиме сенс лише при регулярному застосуванні написаних шаблонів, що більше характерне для сервісного бізнесу, де існує часта потреба розгортання типових конфігурацій Wazuh. Для малого та середнього бізнесу, який має на меті заощадження коштів та намагається використовувати суто власні IT-ресурси, не радимо ускладнювати цей доволі простий процес розгортання, описаний вище як **Step-by-step installation**.

Швидка альтернатива – розгортання підготовленого типового образу Wazuh в якості віртуальної станції формату OVA. Даний формат можна без зайвої

конвертації імпортувати (рис. 3.4) в середовище віртуалізації VMware ESXi або скористатися безкоштовною програмою VirtualBox, встановлену на виділену робочу станцію.

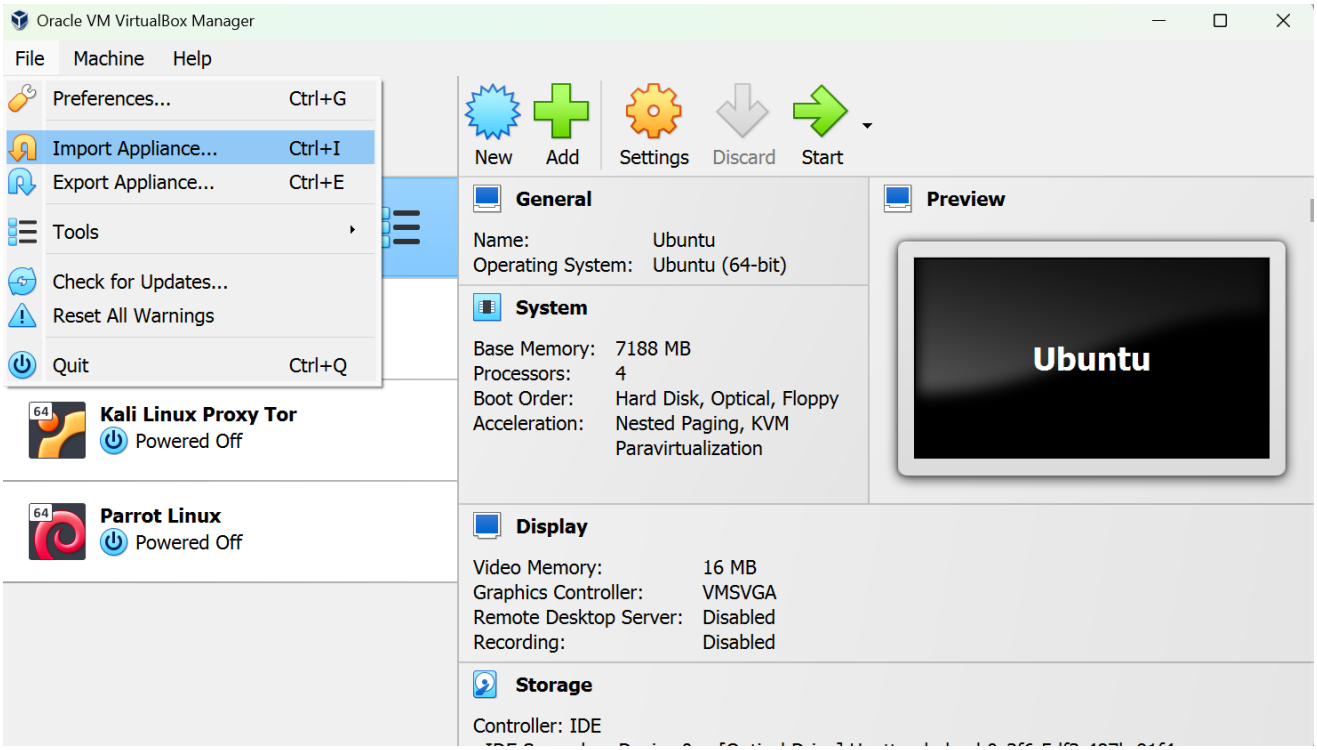


Рис. 3.4 Імпорт образу Wazuh в програмі VirtualBox

3.3. Аналіз звітів про вразливості та їх відповідність галузевим стандартам кібербезпеки

Після успішного розгортання та налаштування серверної частини нашого рішення Wazuh, були розгорнуті операційні системи, аналогічні по версіям до наявних у виробничій мережі, та встановлено агенти моніторингу Wazuh Agent.

Наша наступна мета – провести тестування базових систем без додаткових маніпуляцій щодо підсилення параметрів кіберзбезпеки.

Для чистоти експерименту, усі системи було оновлено останніми бюлетенями безпеки. За умови наявної відсутності сервісів оновлення – свідомо були розгорнуті останні наявні версії покоління операційних систем.

Слід добре розуміти причини розмаїтості наданих надалі операційних систем. Справа в тому, що кіноіндустрія часто оперує унікальними програмами та рішеннями які відмінно виконують свої задачі, але не мають розвитку, тому стають заручниками операційних систем та програмних компонентів, з якими були випущені. Отож, нижче перелік оновлених операційних систем, встановлених з мінімальним пакетом програмного забезпечення в їх базовій конфігурації та рівень їх відповідності до останніх версій рекомендованих параметрів, згідно CIS Benchmark:

CentOS 6.9 – система не оновлюється виробником, але використовується у виробничих процесах в організації. Мінусом використання даної системи є положення про необхідність використання операційних систем за схемою «остання, мінус один», яка передбачає, що остання та її попередня версії дозволені для використання з точки зору безпеки.

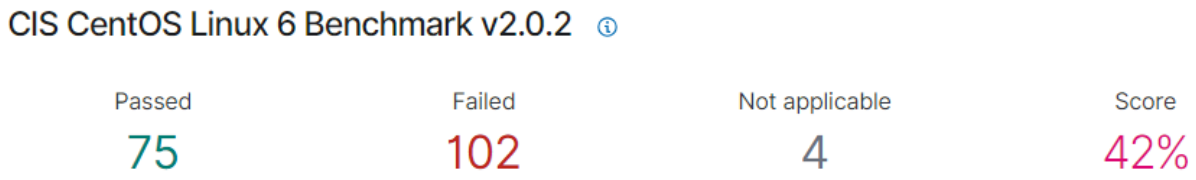


Рис. 3.5 Результат сканування тестової системи Linux CentOS 6.9

CentOS 7.9 – система не оновлюється виробником, але використовується у виробничих процесах в організації. Аналогічно до системи Centos 7.9 – використання цієї версії не рекомендоване до використання у виробничій мережі.

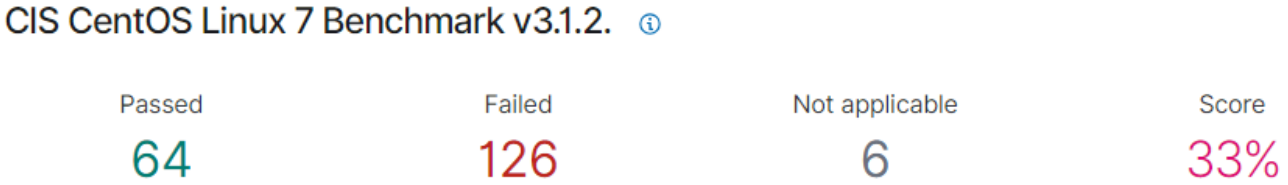


Рис. 3.6 Результат сканування тестової системи Linux CentOS 7.9

Ubuntu 20.04 – система підтримується. Можливе оновлення до більш актуальних версій. Використовується в організації. Рекомендуємо виконати тестування сумісності в роботі програм з новішою версією Ubuntu 22.04. за умови позитивного тестування – оновитися до версії Ubuntu 22.04.

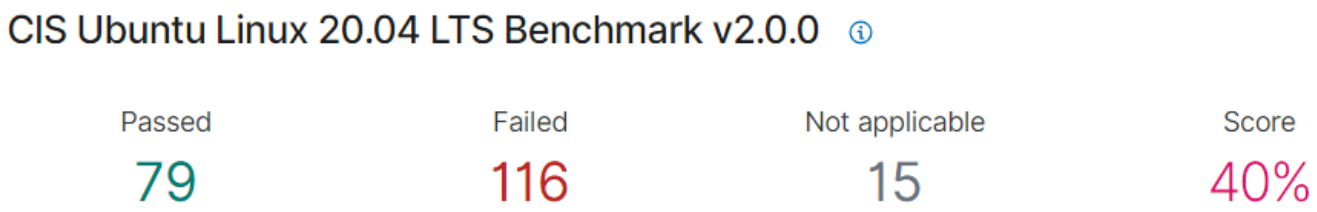


Рис. 3.7 Результат сканування тестової системи Linux Ubuntu 20.04

Ubuntu 24.04 – система підтримується, остання актуальна версія лінійки. Нажаль, на момент проведення тестування, рішення Wazuh не підтримувало моніторинг налаштувань CIS Benchmark для цієї системи. Згідно з повідомленнями на тематичних форумах, розробники пояснили, що ведуть роботи по інтеграції даного тесту, а готовність Wazuh до аналізу CIS Benchmark для цієї системи анонсоване на 1 квартал 2025-го року. Але ми, зі свого боку, надали рекомендацію компанії не поспішати з оновленням старіших систем цієї лінійки, аби не отримати слушне зауваження з боку аудиторів щодо відсутності документальних доказів фактичної відповідності налаштувань згідно CIS Benchmark.

Вважаємо, що негативний результат, це теж результат, адже ми змогли запобігти потенційним зауваженням, тобто, рішення Wazuh превентивно вказала нам на потенційні ризики.

Debian 12.8 – найновіша систем, стабільна гілка, регулярні оновлення. Розглядається для довготривалого використання з перенесенням частини сервісів на цю платформу.

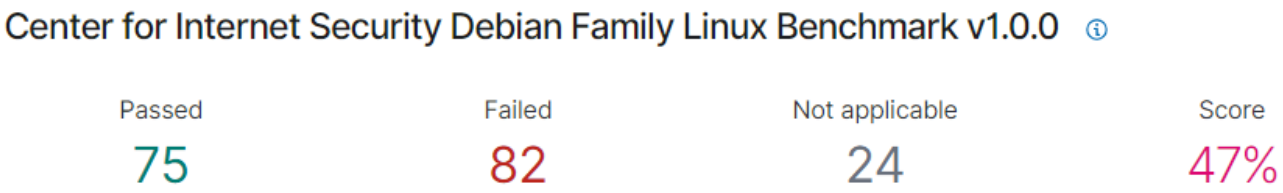


Рис. 3.8 Результат сканування тестової системи Linux Debian 12.8

Windows 10 Pro 22H2 – виробник оголосив про завершення підтримки даної системи в 2025-му році. Використовується в організації. Можливо оновити до наступної версії системи.

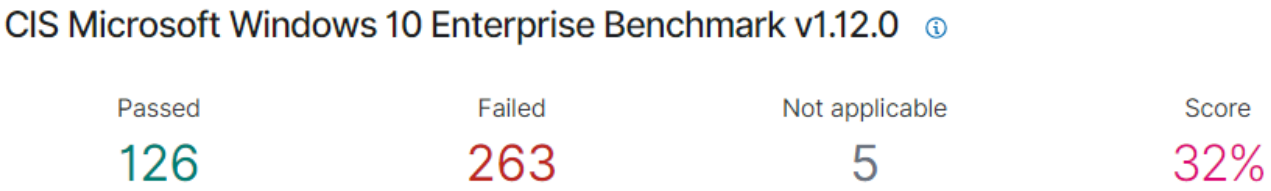


Рис. 3.9 Результат сканування тестової системи Microsoft Windows 10 Pro 22H2

Windows 11 Pro 24H2 – остання актуальна версія системи. Використовується в організації. Рекомендована у якості оновлення з існуючих систем під керуванням Windows 10. За нашим досвідом, більшість ліцензійних ключів Windows 10 дозволяють прозоре оновлення до версії Windows 11, а актуальна підтримка виробника системи пакетами оновлень є однією з вимог TPN, що лише підсилює нашу позицію щодо рекомендації використання цієї версії системи як базової в організації.

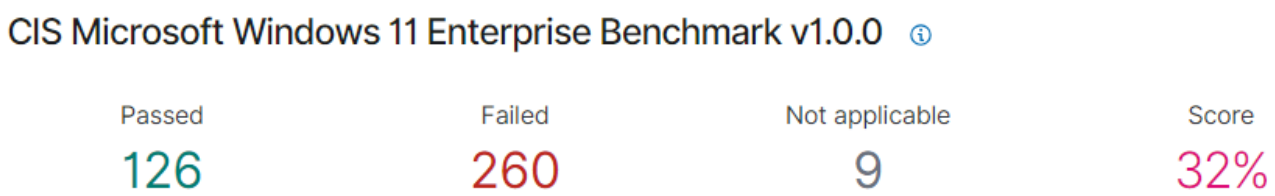


Рис. 3.10 Результат сканування тестової системи Microsoft Windows 11 Pro 24H2

Windows Server 2019 – система підтримується. Використовується в організації.

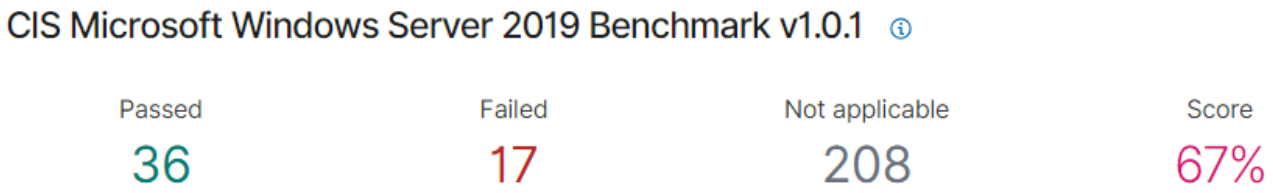


Рис. 3.11 Результат сканування тестової системи Windows Server 2019

Windows Server 2022 – більш актуальна система. Тестується в організації. Рекомендуємо у якості оновлення з версії Windows Server 2019.

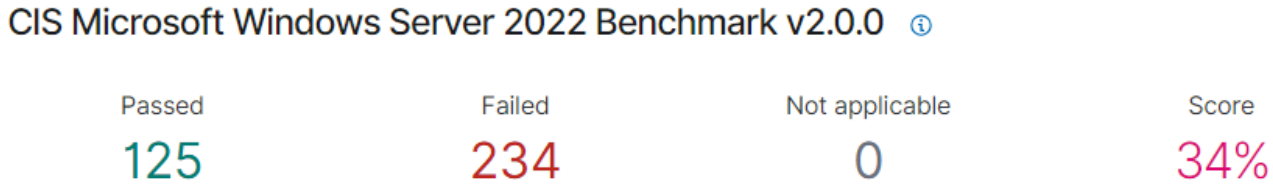


Рис. 3.12 Результат сканування тестової системи Windows Server 2022

Windows Server 2025 – остання актуальна система. Тестується в організації. Станом на грудень 2024, немає розроблених офіційних CIS Benchmark для даної системи. Нами подана рекомендація зачекати з розгортанням даної операційної системи в IT-інфраструктурі замовника до часу, коли рішення Wazuh інтегрує шаблон перевірки цієї системи в свої системи аналізу.

Перевірка спроможності рішення Wazuh щодо вимог сертифікації TPN.

Беручи за основу стандарт NIST 800-53, можна забезпечити вимоги **CA-7 Continuous monitoring** компонентом Wazuh dashboard виконуючи наступні дії:

В консолі Wazuh dashboard – в лівому меню Explore і під ним Discover (рис. 3.12). Вибираємо в полі **Field** значення **rule.groups** а в значення **Value** додаємо фільтр для подій **authentication_success**.

Вимога **AU-6 Audit record review, analysis, and reporting** забезпечується заходами перегляду журналу шляхом вибору модуля NIST 800-53 Wazuh Dashboard, далі **Events** (рис. 3.13). В тому ж вікні в закладці **Controls** можливо переглянути події вимог NIST 800-53.

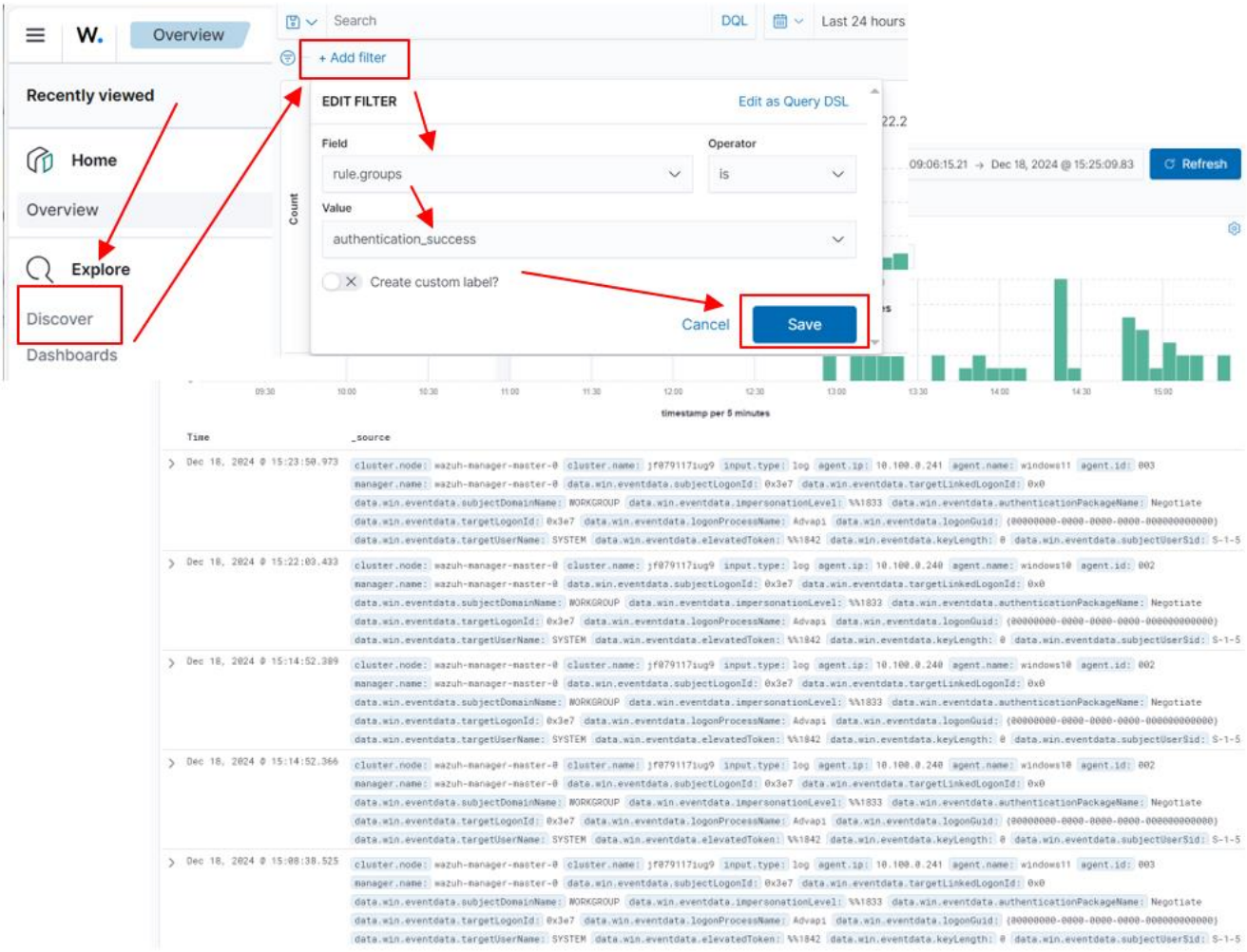


Рис. 3.12 Фільтрування подій категорії “authentication_success”

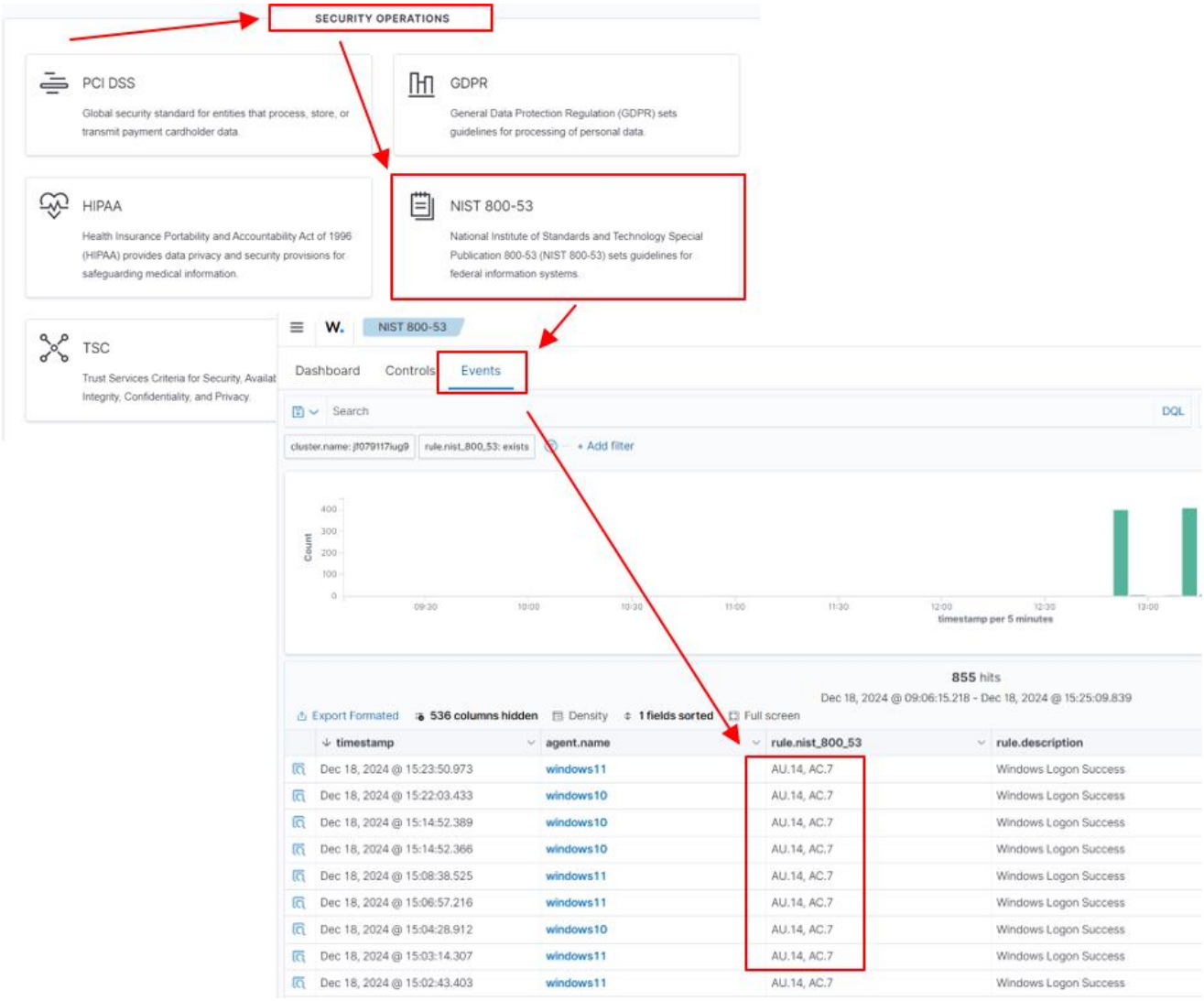


Рис. 3.13 Огляд системних подій в консолі Wazuh dashboard

Вимоги **IA-4 Identifier management**, **SI-4 System monitoring, SI-3 Malicious code protection** та **SI-7 Software, firmware, and information integrity** забезпечує модуль **Threat Hunting** з визначенням невдалих спроб реєстрації в системі. В цьому ж вікні вибравши закладку **Events**, перейдемо безпосередньо до подій, які, в свою чергу, теж можна розкрити при натисканні для отримання ще більш деталізованої зібраної інформації.

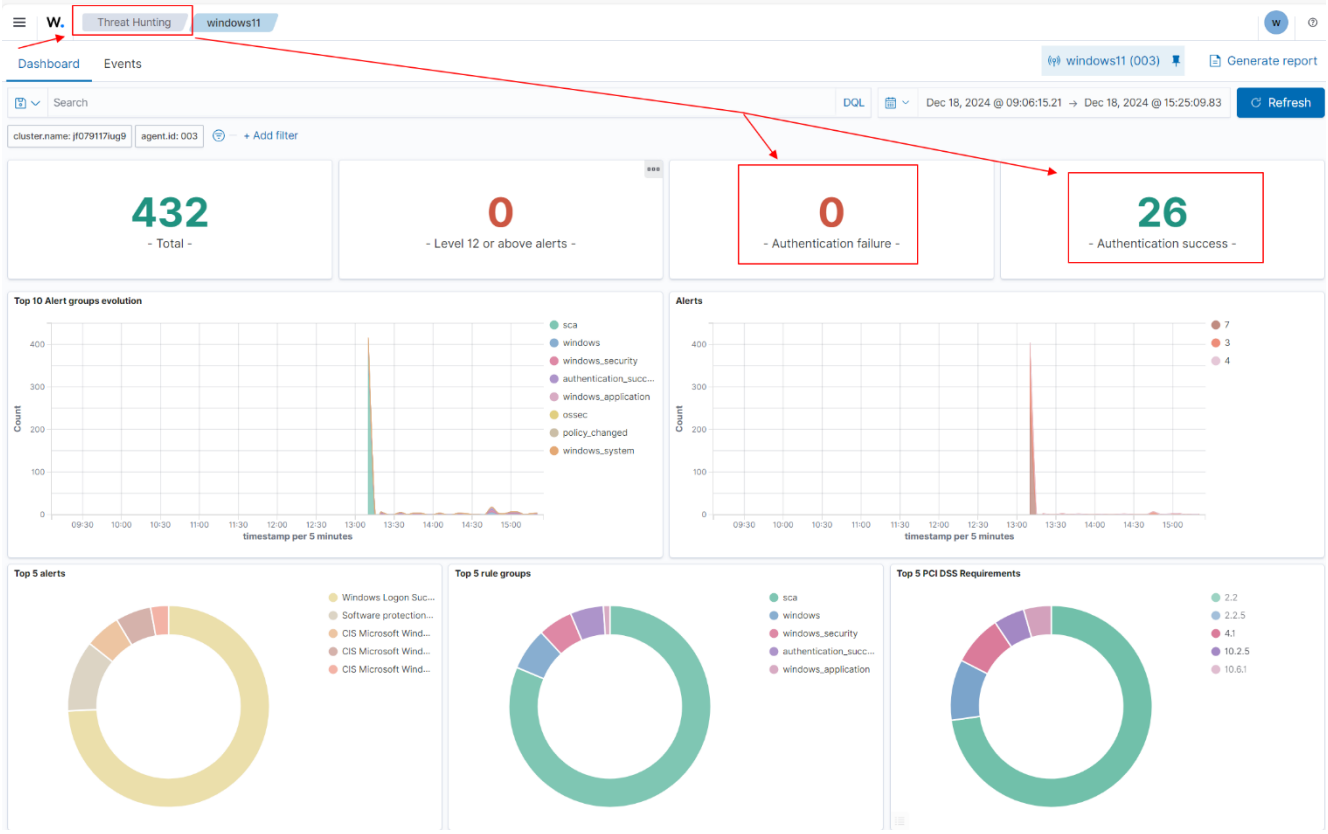


Рис. 3.14 Модуль Threat Hunting в консолі Wazuh dashboard

Секції **SC-7 Boundary protection**, **IA-5 Authenticator management**, **CM-6 Configuration settings** забезпечує модуль Configuration Assesment (Рис. 3.15), а огляд тестування на відповідність CIS Benchmark було описано вище по тексту, в даному пункті розділу 3.

Вимоги **SC-28 Protection of information at rest** та **CM-3 Configuration changes control** забезпечить модуль **File integrity monitoring** в секції **Endpoint Security** (рис. 3.16).

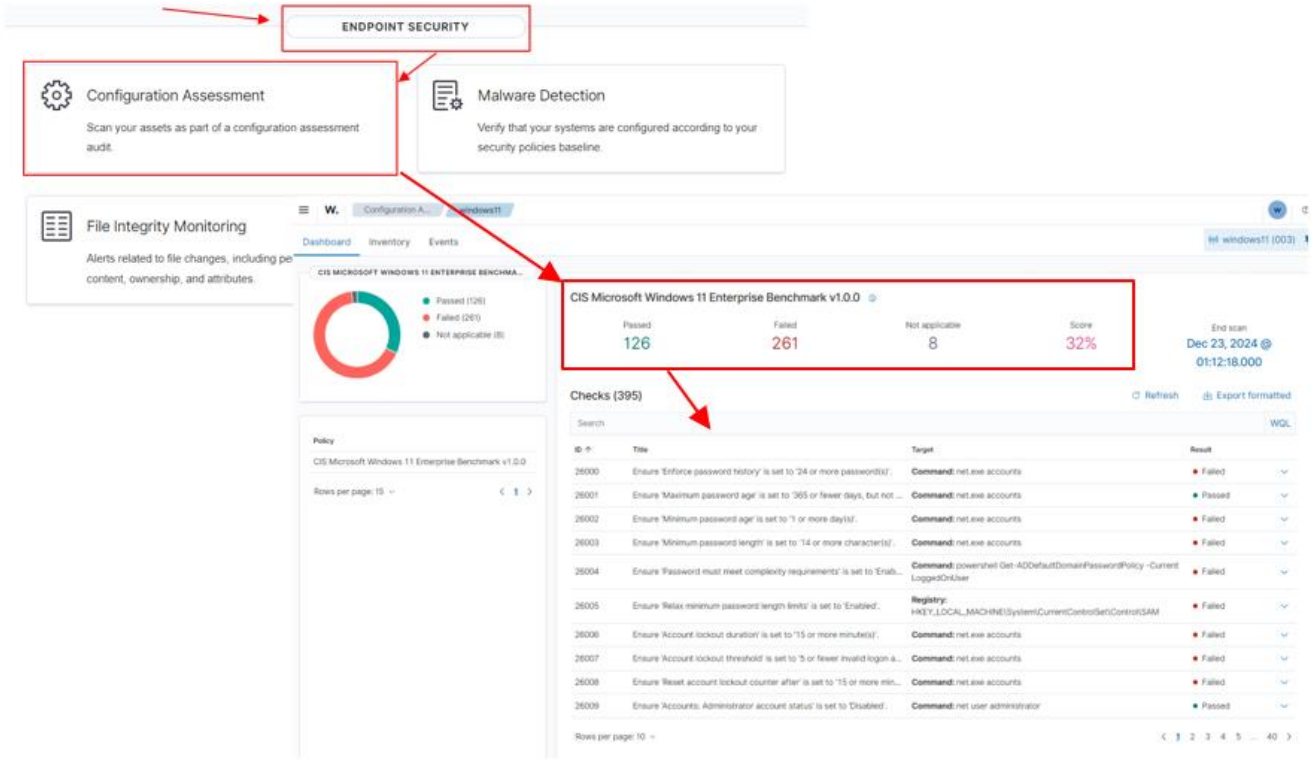


Рис. 3.15 Модуль Configuration Assessment в консолі Wazuh dashboard

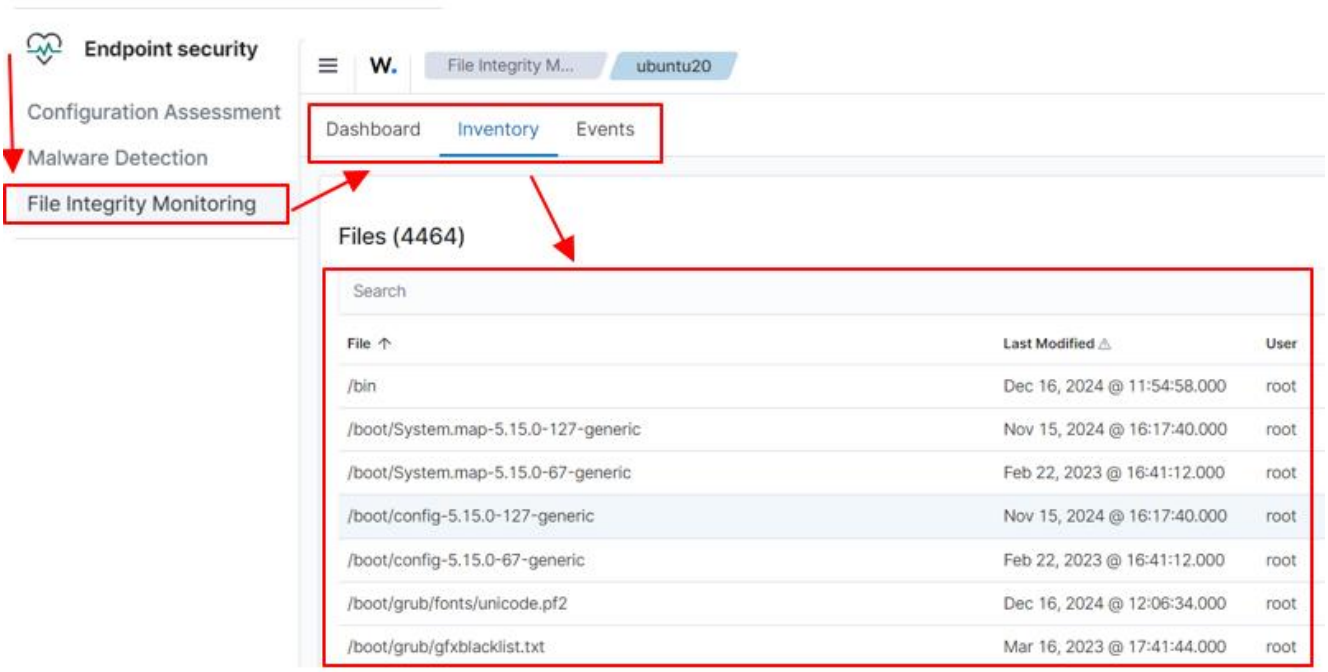


Рис. 3.16 Модуль File Integrity Monitoring в консолі Wazuh dashboard

Первинна інвентаризація апаратних засобів та програмних ресурсів при проведенні самостійного аудиту і, надалі, поточної перевірки змін забезпечує модуль **Inventory Data**. Його запуск здійснюється шляхом вибору агенту моніторингу (робочої станції), наприклад через почерговість вибору **пунктів Server management** – **Endpoint Summary** – вибір робочої станції – пункт меню **Inventory data**. Отримані звіти забезпечують виконання вимог **CM-7 Least functionality** та **CM-8 System component inventory**.

Вимоги **RA-5 Vulnerability monitoring and scanning** та **SC-38 Operations security** забезпечує секція **Threat Intelligence**, модуль **Vulnerability detection** (рис. 3.17) зі застереженнями щодо необхідності зміни конфігурації на стороні Wazuh Server та Wazuh Agent.

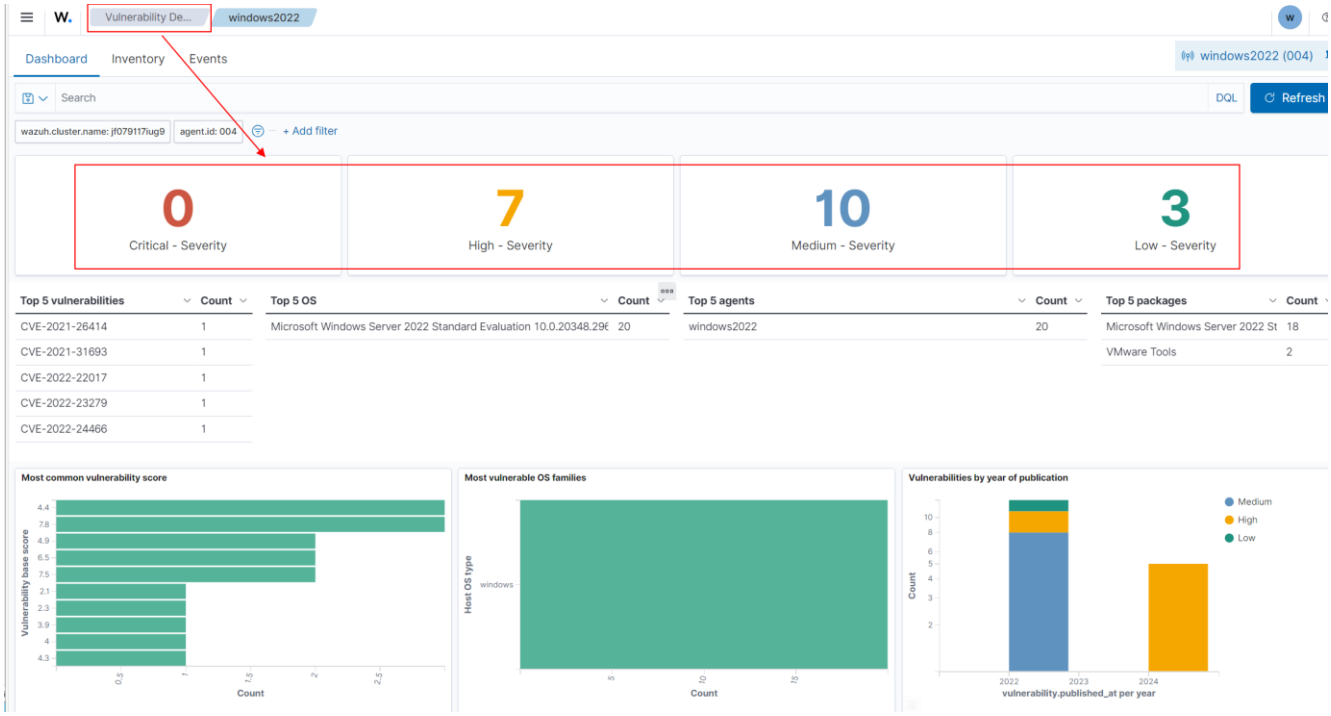


Рис. 3.17 Модуль Vulnerability detection в консолі Wazuh dashboard

Використовуючи функціональність **Active Response**, рішення Wazuh забезпечує виконання вимог **AC-7 Unsuccessful logon attempts** та **SC-5 Denial-of-service protection.** Зауважимо, щодо необхідності зміни конфігурації на стороні

Wazuh Server де необхідно чітко прописати реакцію на події невдалих спроб реєстрації в системі.

Модуль **MITTRE ATT&CK** з секції **Threat Intelligence** (рис. 3.18) стосується забезпечення вимог **RA-10 Threat hunting** та **PM-16 Threat awareness program**. Додаткові налаштування модуля через створення власних сигнатур атак, реакції на події чи моніторингу цілісності критичних файлів дозволяє адаптувати Wazuh під специфіку окремо взятої організації.

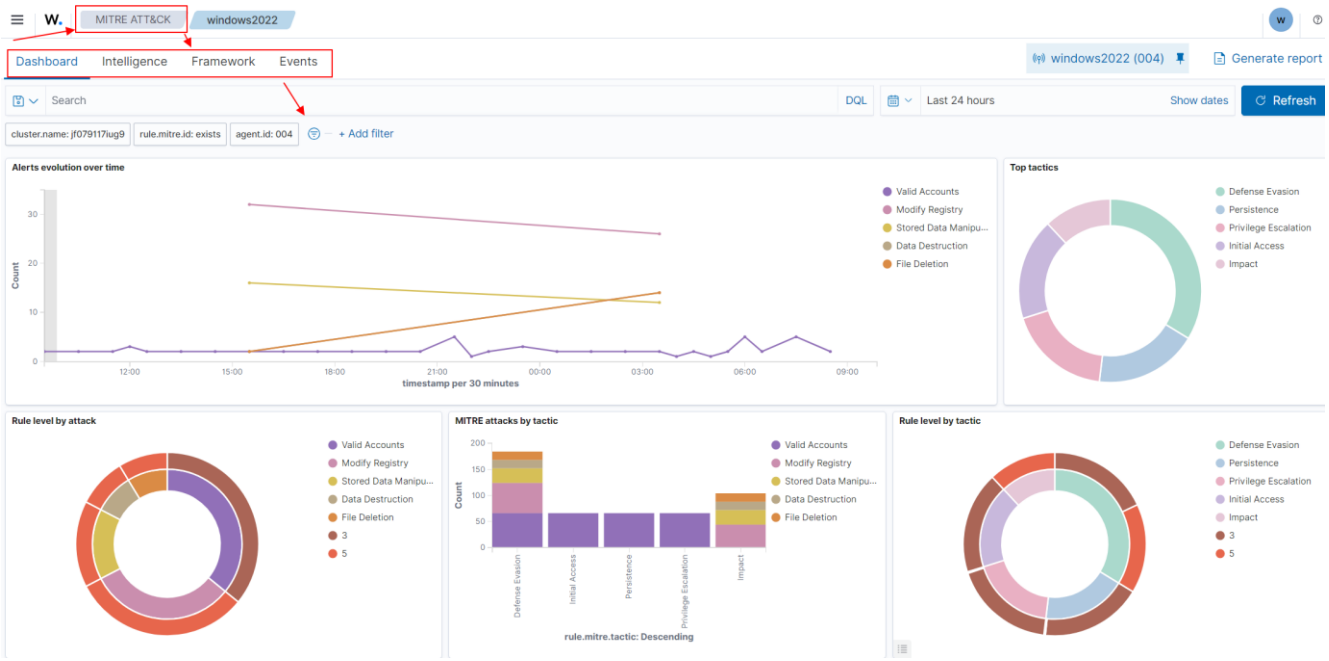


Рис. 3.18 Модуль MITRE ATT&CK в консолі Wazuh dashboard

Підсумовуючи отримані результати рішенням Wazuh після проведення тестування розгорнутої для замовника інфраструктури, ми отримали позитивну реакцію організації з намірами використання продукту в паралельному режимі разом з AlienVault OSSIM до наступної сертифікації TPN. Такому рішенню спряв сам продукт Wazuh з ефектними та ефективними інструментами візуалізації, звітності, дослідження, можливості специфічних налаштувань.

ВИСНОВКИ

У результаті проведеної роботи було проаналізовано можливості використання безкоштовної версії програмного продукту Wazuh для самостійного аудиту інформаційної безпеки підприємств. Розроблено аналітичний підхід до оцінки ефективності Wazuh, визначено його сильні та слабкі сторони у порівнянні з альтернативним рішенням AlienVault OSSIM. Проведено порівняльний аналіз, який дозволив виявити найбільш доцільні сценарії застосування Wazuh залежно від масштабу організації.

Проведений аналіз показав, що Wazuh є ефективним інструментом для малих та середніх підприємств завдяки його доступності та архітектурній гнучкості. Він дозволяє здійснювати базовий аудит кібербезпеки, адаптувати конфігурацію під потреби організації, створювати власні правила моніторингу, а також відновлювати конфігурацію системи після несанкціонованих змін за допомогою скриптів автоматизації.

Дослідження виявило, що впровадження сертифікацій за міжнародними стандартами, такими як PCI DSS, GDPR, HIPAA, а також участь у програмі TPN (Trusted Partner Network), значно підвищує конкурентоспроможність підприємств на міжнародних ринках. Сертифікація TPN відкриває можливості для співпраці з провідними світовими компаніями у сфері медіапослуг.

Практична значущість роботи полягає у створенні рекомендацій щодо використання Wazuh для самостійного аудиту кібербезпеки. Запропоновано оптимальні сценарії розгортання Wazuh, зокрема хмарну версію Wazuh Cloud для тестування та формат OVA для віртуалізації. Також розглянуто можливості сумісності Wazuh з різними операційними системами та надано рекомендації щодо оновлення застарілих систем до актуальних версій.

Подальші дослідження можуть зосередитись на детальному аналізі ефективності використання Wazuh у великих організаціях, а також на розробці нових конфігураційних рішень для підвищення продуктивності. Перспективним

напрямом є дослідження можливостей інтеграції Wazuh із сучасними хмарними платформами та впровадження більш складних сценаріїв автоматизації процесів кібербезпеки.

Проведене дослідження підтверджує, що безкоштовна версія Wazuh є ефективним інструментом для підвищення рівня кібербезпеки малих і середніх підприємств, сприяє оптимізації процесу самостійного аудиту інформаційної безпеки та підвищенню стійкості IT-інфраструктури до сучасних кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Jeffrey A. Marron. Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. *NIST*, February 2024 – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf

2. General Data Protection Regulation (GDPR) – URL: https://gdpr.eu/tag/gdpr/

3. PCI DSS: v4.0.1. *PCI Security Standards Cuncils*, June 2024 – URL: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

4. Офіційний сайт компанії Film.ua. – URL: https://film.ua/en/news/2526

5. Офіційний сайт компанії LeDoyen. – URL: https://ledoyen.com.ua/ua/pro-kompaniyu#9058-gal7

6. Офіційний сайт компанії StarLight Creative Studio. – URL: https://starlightcreative.studio/

7. Офіційний сайт компанії Karandash. – URL: https://krndsh.com/about_us/

8. Azure Compliance / Azure Compliance Offering / Media and entertainment / Motion Picture Association (MPA). *Microsoft*. – URL: https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-mpa

9. Azure Compliance / Azure Compliance Offering / CDSA. *Microsoft*. – URL: https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-cdsa

10. MPA & Studio Security. *Amazon Web Services*. – URL: https://aws.amazon.com/compliance/mpa/

11. Compliance / MPA. *Google Cloud*. – URL: https://cloud.google.com/security/compliance/mpa

12. Attestations & Certifications MPA. *Alibaba Cloud*. – URL: https://www.alibabacloud.com/en/trust-center/mpaa?_p_lc=1&spm=a3c0i.17650567.2445100110.33.739e2ae3e3E3Rg

13. The MPA Content Security Best Practices, maintained by the TPN. *Trusted Partner Network*. – URL: https://www.ttpn.org/wp-content/uploads/2023/08/MPA-Content-Security-Best-Practices-v5.2_Aug30_2023-Release.xlsx

14. Global Future of Cyber Survey, 4th Edition. *Deloitte* – URL: https://www.deloitte.com/global/en/services/risk-advisory/research/global-future-of-cyber.html?id=gx:2ps:3gl:4cyber:5:6con:20241021::2024focs-paidsearch-emea&gad_source=1&gclid=CjwKCAiAmfq6BhAsEiwAX1jsZ7K8Z-rvNQvEngfLuyY1DTo1eYveR9lPrNvCa2LFdZbnJ98oN2qKMhoCFQgQAvD_BwE

15. Lynis. *Cisofy*. – URL: https://cisofy.com/lynis/#introduction

16. Security Onion. *Security Onion Solutions, LLC* – URL: https://securityonionsolutions.com/

17. CIS-CAT Lite. *Center for Internet Security, Inc®* – URL: https://learn.cisecurity.org/cis-cat-lite

18. The all-in-one open source security scanner. *Trivy*. – URL: https://trivy.dev/latest/

19. Cybersecurity Breach Bankruptcy: It Does Happen. *The Fractional CISO*. – URL: https://fractionalciso.com/cybersecurity-breach-bankruptcy/

20. Which Cybercrimes Generated the Largest Financial Losses in 2023? *VERISK ANALYTICS®*. – URL: https://core.verisk.com/Insights/Emerging-Issues/Articles/2024/June/Week-2/2023-Cybercrime-Losses

21. Державна служба спеціального зв'язку та захисту інформації України. *Наказ Адміністрації Держспецзв'язку від 10.07.2024 №354 «Про затвердження Рекомендацій з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації»*. — URL: https://cip.gov.ua/services/cm/api/attachment/download?id=65339

22. ISO: Global standards for trusted goods and services. *Information technology — Security techniques — Code of practice for information security controls*. — URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

23. National Institute of Standards and Technology. *NIST SP 800-53 Release 5.1.1*. —URL: https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home

24. Proof of Concept Guide. *Wazuh, Inc.*. — URL: https://documentation.wazuh.com/current/proof-of-concept-guide/index.html

25. Quickstart. *Wazuh, Inc.* — URL: https://documentation.wazuh.com/current/quickstart.html

26. Installation guide. *Wazuh, Inc.* — URL: https://documentation.wazuh.com/current/installation-guide/index.html

27. ISO 27001 Checklist: 9-step Implementation Guide. *IT Governance Ltd.* — URL: https://www.itgovernance.co.uk/blog/iso-27001-checklist-a-step-by-step-guide-to-implementation

28. Cybersecurity self-assessment for SMEs. *European Cybersecurity Competence COmmunity (ECCO).* — URL: https://cyberwatching.eu/cybersecurity-best-practices-smes-assessment

29. TryHackMe Room — Custom Alert Rules in Wazuh. *@haircutfish.* — URL: https://medium.com/@haircutfish/tryhackme-room-custom-alert-rules-in-wazuh-5bce71e3bd01

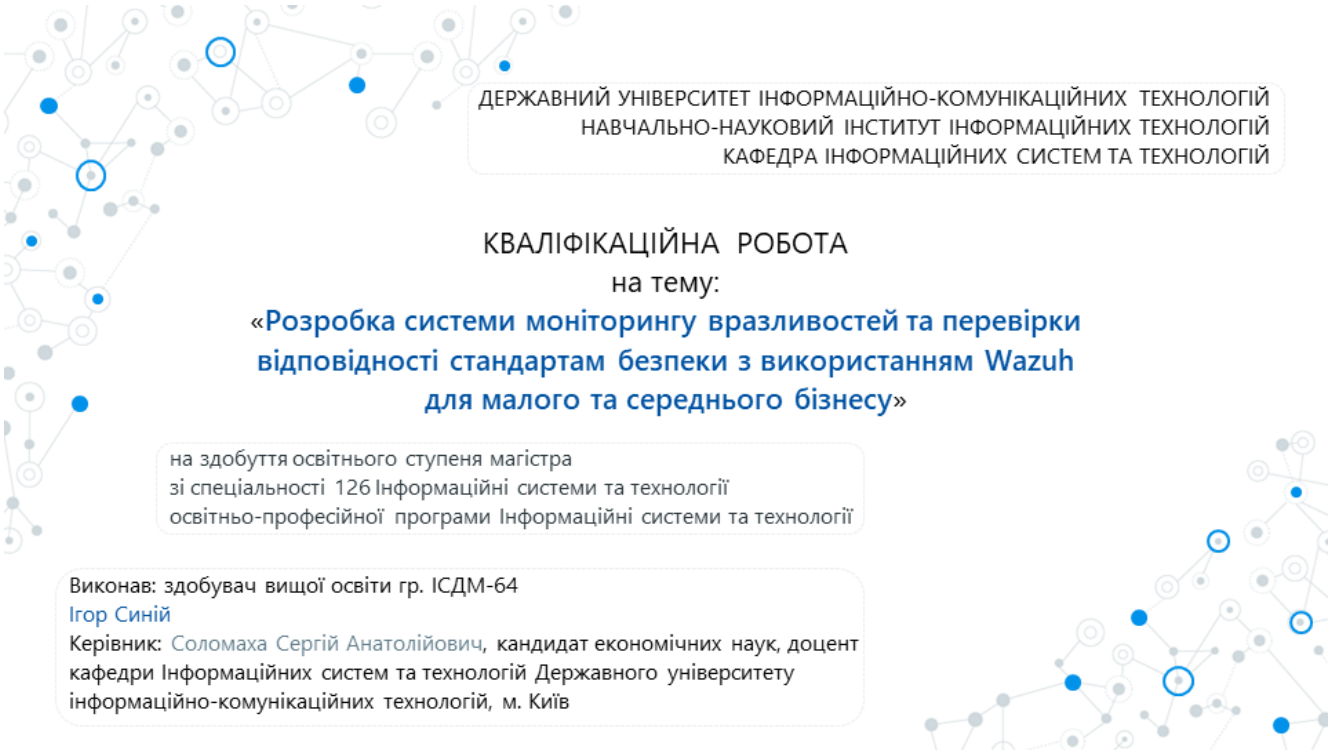
30. AlienVault OSSIM vs Wazuh comparison. *PeerSpot.* — URL: https://www.peerspot.com/products/comparisons/alienvault-ossim_vs_wazuh

31. AlienVault OSSIM vs Wazuh vs Security Onion. *Rabah RAHLI, Cyber Security Analyst* — URL: https://www.linkedin.com/pulse/alienvault-ossim-vs-wazuh-security-onion-rabah-rahli-oytce/

32. Hit the Road and Implement Your Cybersecurity Roadmap. *Center for Internet Security, Inc®* — URL: https://www.cisecurity.org/insights/blog/hit-the-road-and-implement-your-cybersecurity-roadmap

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)



Галузеві стандарти захисту інформації

Захист персональних даних

GDPR

Система управління інформаційною безпекою

Information Security Management System ISO 27001 Certified

HIPAA Compliance

Захист персональної інформації у медичній сфері

PCI DSS COMPLIANT

Безпека банківських карткових сервісів

NIST 800-53 Revision 5 Security Controls

Стандарт інформаційної безпеки

Trusted Partner Network

MARVEL STUDIOS NETFLIX UNIVERSAL Paramount Walt Disney MGM SONY PICTURES

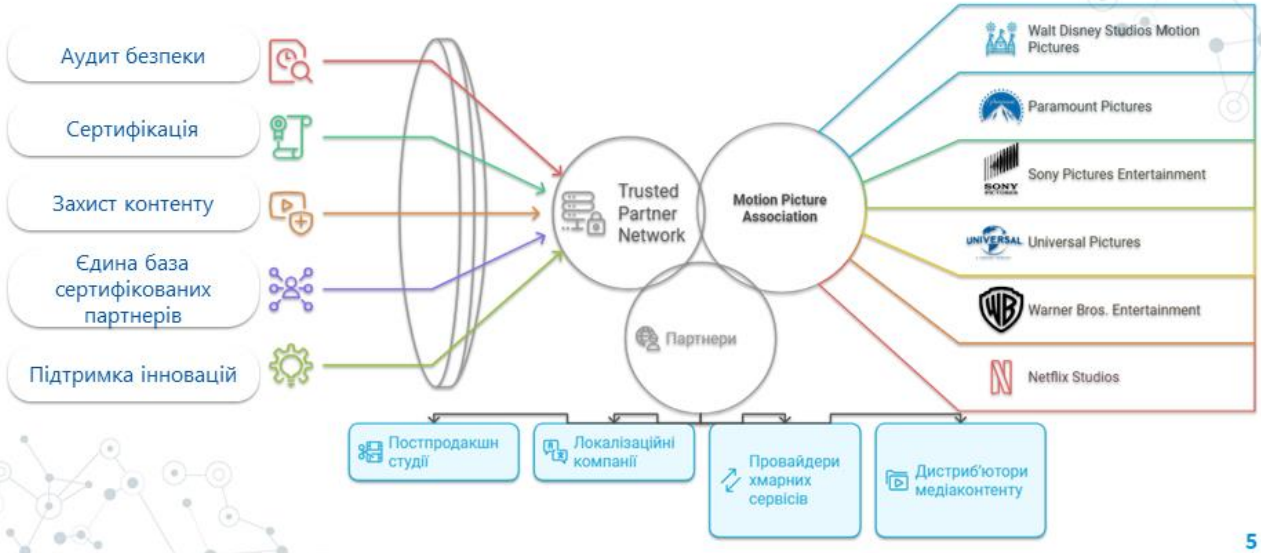
MPA TPN TRUSTED PARTNER NETWORK

CDSA

Сертифікація TPN

обов'язкова умова для роботи з ліцензованим медіаконтентом

Взаємодія структури MPA, TPN та партнерів



Методика самостійного аудиту кібербезпеки

Інструменти перевірки кібербезпеки

- моніторинг
- аудит
- тестування

Nessus vulnerability scanner

Qualys.

SNORT

ALIEN VAULT

wazuh.

WIRESHARK

NMAP PROJECT

OSSEC

AUTOPSY DIGITAL FORENSICS

graylog

Greenbone OpenVAS
Open Vulnerability Assessment Scanner

wazuh.

особливості продукту

Масштабованість
Здатність зростати та адаптуватися до зростаючих вимог

Активне співтовариство
Підтримується зацікавленою та активною базою користувачів

Відкрите програмне забезпечення
Програмне забезпечення є вільно доступним та модифікованим

Кросплатформеність
Працює на різних операційних системах

Моніторинг в реальному часі
Надає миттєві сповіщення та інсайти

wazuh.

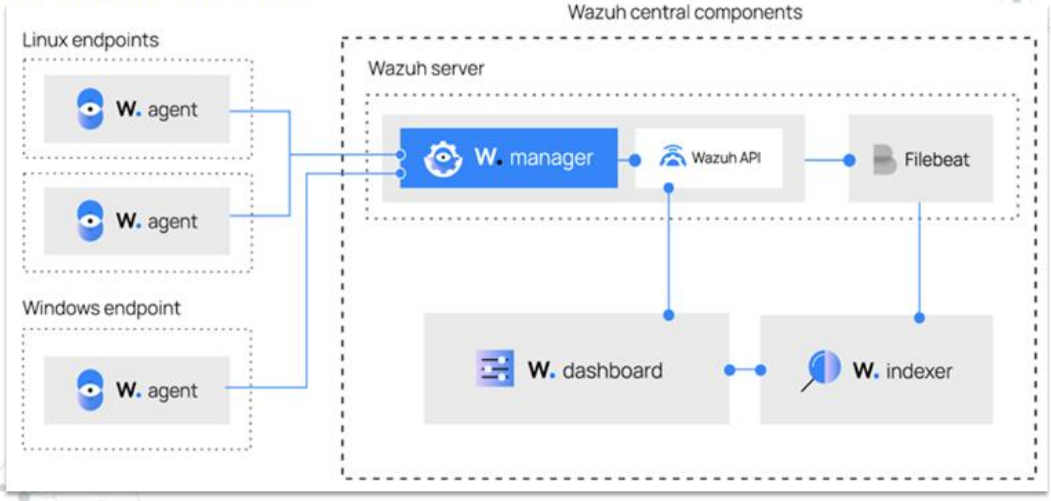
функціональні модулі

SIEM

XDR

wazuh.

концептуальна схема



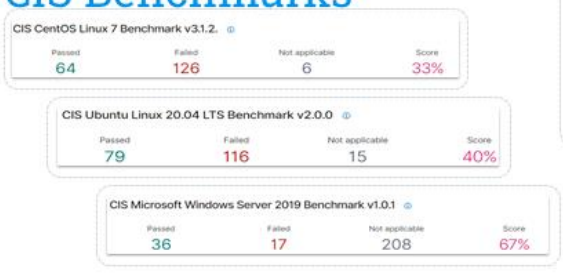
wazuh.

схема розгортання

wazuh.

тести та звіти

CIS Benchmarks

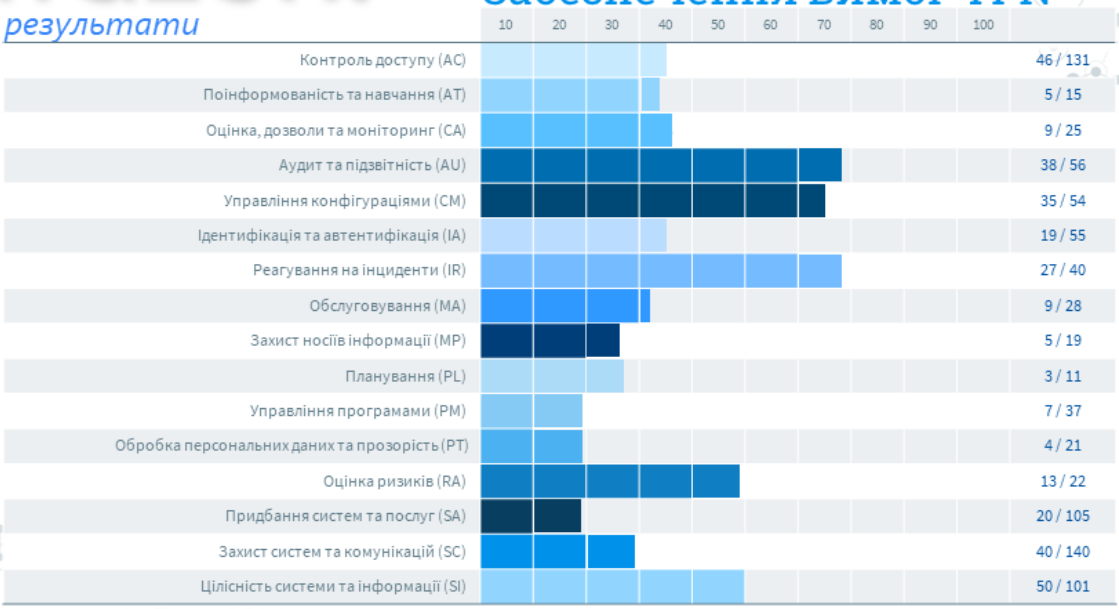


WAZUH Dashboard

wazuh.

результати

Забезпечення вимог TPN



Висновки

- Сертифікація TPN – забезпечує стійкість кібербезпеки і сприяє розвитку компанії
- Використання Wazuh забезпечить понад 30% вимог TPN
- Перша тестова перевірка – з використанням Wazuh Cloud
- Рекомендоване розгортання Wazuh – *Step-by-Step Installation*
- Перевага Wazuh – архітектурна гнучкість та можливість адаптації під свої потреби
- Не рекомендується використання операційних систем без наявних CIS Benchmark

Апробація результатів дослідження

Синій І.А. "Інтегрована система моніторингу вразливостей та перевірки відповідності галузевим стандартам безпеки із використанням Wazuh для малого та середнього бізнесу". Тези доповіді. II всеукраїнська науково-технічна конференця «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу». Київ, 18.11.2024р.

Синій І.А. "Оцінка доцільності пропагації системи моніторингу вразливостей Wazuh як інструменту забезпечення аудиту кібербезпеки підприємства з боку державних органів України". Тези доповіді. V науково-практична конференція студентів і молодих учених «Дорожня карта інформаційно-комунікаційної галузі України». Київ - 25.11.2024р.

Дякую за увагу!