ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо виявлення шкідливого програмного забезпечення на прикладі платформа Wazuh SIEM і XDR»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Соломія АНДРЕЇШИН
(підпис)

Виконала: здобувачка вищої освіти групи БСД-42
АНДРЕЇШИН Соломія
(прізвище, ім'я)

Керівник д.техн.н., професор КУЗНЕЦОВ Олександр
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 55 сторінок, 20 рисунків, 17 джерел.

Об'єкт дослідження – процеси ідентифікації та аналізу шкідливого програмного забезпечення.

Предмет дослідження – методи та технології виявлення, аналізу та нейтралізації шкідливого програмного забезпечення з використанням платформ Wazuh SIEM і XDR.

Методи дослідження – аналіз сучасних наукових робіт, статей та технічної документації для вивчення особливостей та можливостей платформ Wazuh SIEM та XDR. Експериментальне тестування для оцінки ефективності виявлення шкідливого програмного забезпечення. Використання кейс-стаді для аналізу реальних сценаріїв використання. Порівняльний аналіз з іншими системами кібербезпеки для виявлення унікальних переваг та можливостей розглядуваних платформ.

У цій роботі зосереджено увагу на аналізі сучасних підходів до виявлення шкідливого програмного забезпечення з використанням інструментів Wazuh SIEM та XDR. Розглянуто ключові аспекти та функціональні можливості цих систем, включаючи моніторинг, логування подій і аналіз даних для ефективного виявлення потенційних загроз. Аналізуються основні компоненти платформи Wazuh, їх роль у захисті інформаційних систем, а також взаємодія з іншими інструментами кібербезпеки для забезпечення більш комплексного покриття безпеки. Особлива увага приділена рекомендаціям щодо оптимізації використання цих систем у корпоративних середовищах, з акцентом на необхідності навчання персоналу і розробці ефективних процедур реагування на інциденти.

Галузь використання – кібербезпека інформаційних ресурсів організації.

КІБЕРБЕЗПЕКА, WAZUH SIEM, XDR, ВИЯВЛЕННЯ ШКІДЛИВОГО ПЗ, АНАЛІЗ ПОДІЙ БЕЗПЕКИ, РЕАГУВАННЯ НА ІНЦИДЕНТИ, АВТОМАТИЗАЦІЯ МОНІТОРИНГУ БЕЗПЕКИ, КОРПОРАТИВНА БЕЗПЕКА, РОЗРОБКА РЕКОМЕНДАЦІЙ З КІБЕРБЕЗПЕКИ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

EDR — endpoint detection and response;

SIEM — security information and event management;

XDR — extended detection and response;

ПЗ — програмне забезпечення;

ПК — персональний комп’ютер;

ПНП — потенційно небажана програма;

ШПЗ — шкідливе програмне забезпечення.

ВСТУП

Актуальність дослідження. У сучасному світі, де обсяг цифрових даних зростає експоненціально, а взаємодія між різноманітними цифровими сервісами стає все більш складною та інтегрованою, питання кібербезпеки виходить на перший план. Шкідливе програмне забезпечення, здатне не тільки завдати шкоди окремим користувачам, але й паралізувати роботу цілих корпорацій або навіть держав, стає все більш витонченим і складним для виявлення. У цьому контексті, системи виявлення та реагування на інциденти, такі як Wazuh SIEM і XDR, відіграють ключову роль у захисті інформаційних систем від кіберзагроз.

Платформи Wazuh SIEM і XDR, що інтегрують можливості збору, аналізу, моніторингу та реагування на кіберзагрози в реальному часі, стають незамінними інструментами в арсеналі фахівців з кібербезпеки. Використання таких систем дозволяє не тільки виявляти вже відомі види шкідливого ПЗ, але й ефективно ідентифікувати нові, раніше невідомі загрози, завдяки постійному аналізу поведінкових патернів та аномалій в системах.

Проте, незважаючи на значний потенціал та широке поширення цих технологій, існує ряд викликів, пов'язаних з їх ефективним впровадженням та налаштуванням. Питання конфігурації, інтеграції з існуючою IT-інфраструктурою, а також розробка оптимальних стратегій моніторингу та реагування на інциденти потребують детального вивчення та адаптації під конкретні умови використання.

Робота над цією бакалаврською роботою має на меті не лише аналіз сучасних підходів до виявлення шкідливого програмного забезпечення з використанням Wazuh SIEM і XDR, але й розробку рекомендацій щодо оптимізації їх використання для підвищення ефективності кіберзахисту організацій. Такий підхід не тільки сприятиме зміцненню кібербезпеки на рівні окремих компаній, але й забезпечить важливий внесок у загальну стабільність і безпеку інформаційного простору на національному та міжнародному рівнях. Розвиток і вдосконалення інструментів для ідентифікації та нейтралізації шкідливого програмного забезпечення є критично важливим для протистояння постійно еволюціонуючим кіберзагрозам. В

контексті України, країни, що стикається з численними кібератаками у світлі сучасних геополітичних викликів, ця проблематика набуває особливої актуальності.

Об'єкт дослідження процеси ідентифікації та аналізу шкідливого програмного забезпечення.

Предмет дослідження – методи та технології виявлення, аналізу та нейтралізації шкідливого програмного забезпечення з використанням платформ Wazuh SIEM і XDR.

Мета роботи – розробити комплексні рекомендації щодо виявлення та нейтралізації шкідливого програмного забезпечення в інформаційних системах за допомогою платформ Wazuh SIEM і XDR, з акцентом на оптимізацію їх конфігурації та використання в різноманітних організаційних контекстах для підвищення ефективності кіберзахисту.

Наукові завдання:

дослідити актуальність та специфіку виявлення шкідливого програмного забезпечення в сучасних інформаційних системах;

проаналізувати можливості та функціональні особливості платформ Wazuh SIEM і XDR для виявлення та нейтралізації шкідливого програмного забезпечення;

вивчити сучасні методи та технології кіберзахисту, з акцентом на роль та місце систем SIEM і XDR у стратегіях забезпечення інформаційної безпеки;

провести порівняльний аналіз Wazuh SIEM і XDR з альтернативними рішеннями у галузі кібербезпеки для виявлення переваг та обмежень;

розробити рекомендації щодо оптимізації використання Wazuh SIEM і XDR для підвищення ефективності виявлення шкідливого програмного забезпечення в різних типах організацій;

сформулювати методичні вказівки щодо налаштування Wazuh SIEM і XDR з метою забезпечення комплексного захисту від сучасних кіберзагроз.

Методи дослідження – опрацювання тематичної літератури, інтернет-джерел, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: розроблено рекомендації

щодо застосування методів та засобів виявлення та нейтралізації шкідливого програмного забезпечення за допомогою платформ Wazuh SIEM і XDR, а також надано керівництво для вдосконалення процедур кіберзахисту та адаптації сучасних технологічних рішень в контексті забезпечення безпеки інформаційних систем.

1 ОГЛЯД АКТУАЛЬНОСТІ ПРОБЛЕМИ ВИЯВЛЕННЯ ШКІДЛИВОГО ПЗ

1.1 Значення та потреби в ідентифікації шкідливого ПЗ у сучасних IT-інфраструктурах

У сучасному світі, де цифровізація проникла в усі сфери нашого життя, від повсякденної діяльності до глобальних бізнес-процесів, безпека інформаційних технологій стала однією з ключових пріоритетів. Інформаційні системи та IT-інфраструктури, які є основою для зберігання, обробки та передачі даних, стикаються з безперервним потоком кіберзагроз, серед яких шкідливе програмне забезпечення (ПЗ) виступає однією з найпоширеніших та найнебезпечніших. Виявлення та нейтралізація шкідливого ПЗ є критично важливим для забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів.

Шкідливе ПЗ може мати різноманітні форми та цілі, від простих вірусів, що спричиняють незначні незручності, до складних програм, що цілеспрямовано викрадають конфіденційні дані, здійснюють шпигунство або проводять деструктивні атаки на критичну інфраструктуру. У цьому контексті, ідентифікація шкідливого ПЗ є першим та одним з найважливіших кроків у кіберзахисті, що вимагає комплексного підходу та використання передових технологій і методик.

Ефективність ідентифікації шкідливого ПЗ безпосередньо впливає на здатність організацій своєчасно реагувати на загрози, мінімізувати збитки та запобігти потенційним інцидентам безпеки. У зв'язку з цим, розробка та вдосконалення методів виявлення та аналізу шкідливого ПЗ стає ключовою задачею для спеціалістів у галузі кібербезпеки.

Аналізуючи статистику щодо загального обсягу шкідливого програмного забезпечення, варто пам'ятати, що багато окремих зразків шкідливого програмного забезпечення мають обмежений термін придатності: тобто вони активно використовуються зловмисниками лише протягом короткого періоду часу, перш ніж вони переходять до створення нових варіантів.

Тим не менш, зростання обсягів шкідливого програмного забезпечення та збереження високого рівня атак свідчать про те, що атаки, пов'язані зі шкідливим програмним забезпеченням, залишаються надзвичайно серйозною кіберзагрозою [1].

Згідно [1], нині у кіберпросторі існує близько 1,2 мільярда шкідливих програм та потенційно небажаних програм (ПНП). Як можна бачити на рис. 1.1., кількість такого типу програмного забезпечення постійно зростає.

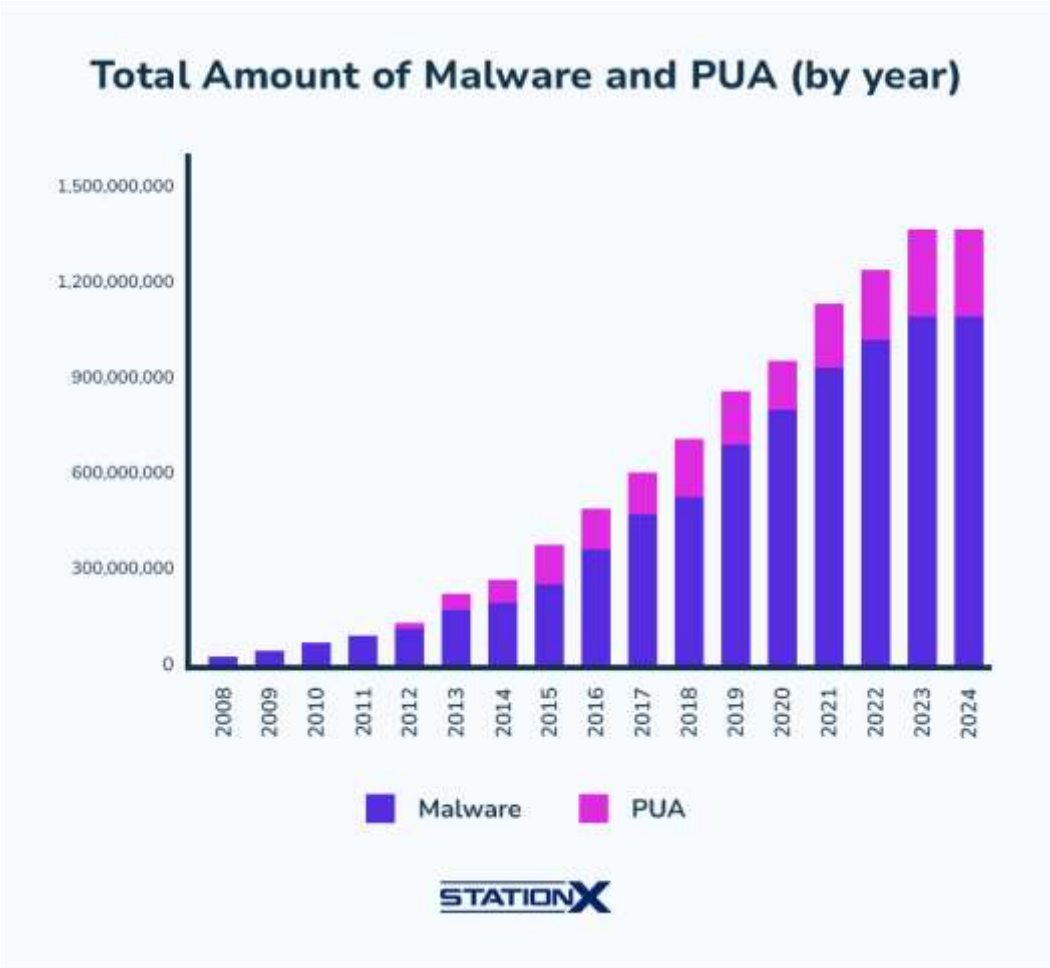

Рис. 1.1. Загальна кількість ШПЗ та ПНП за роками

За даними [1], минулого року зловмисники розгортали в середньому 200 454 унікальних скриптів шкідливого програмного забезпечення на день - або приблизно 1,5 нових зразків за хвилину.

Поява нових зразків шкідливого програмного забезпечення свідчить також про зменшення загального рівня резистентності систем до негативних впливів. Так, у звіті про кібербезпеку [2] прогнозується, що збитки від кіберзлочинності сягнуть

9,5 трильйонів доларів у 2024 році і перевищать 10,5 трильйонів доларів у 2025 році. До прикладу, у 2022 році до Центру скарг на інтернет-злочинність ФБР надійшло понад 800 000 скарг, і хоча це на 5% менше, ніж у 2021 році, фактична сума втрат у доларовому еквіваленті зросла на 49%. У дослідженні [3] також було прогнозовано стрімкий ріст кіберзлочинності у найближчі роки (рис. 1.2)

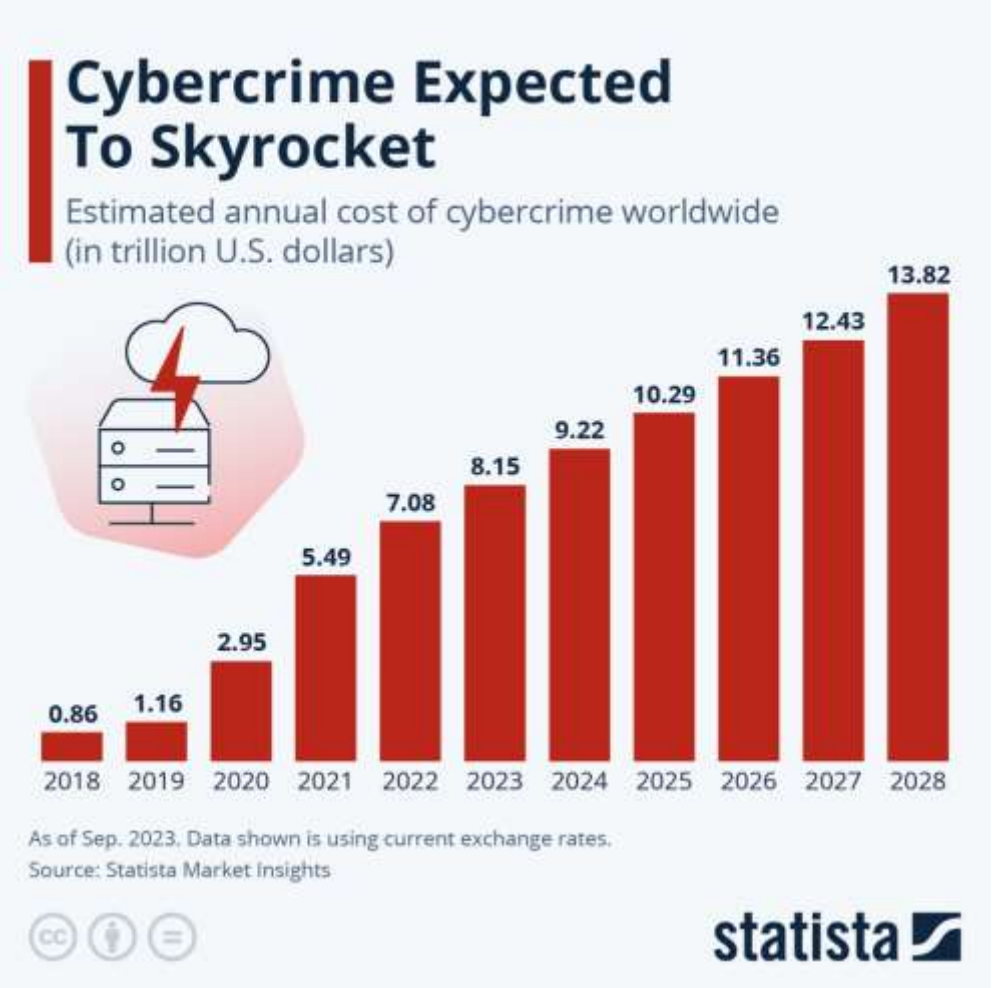

Рис. 1.2. Прогнозований ріст негативних наслідків реалізації загроз інформаційним системам через кіберзлочинність [3]

Ці цифри вказують на постійно зростаючу потребу в розробці та впровадженні ефективних механізмів ідентифікації та протидії шкідливому ПЗ. Враховуючи велику кількість нових зразків шкідливого програмного забезпечення, що з'являються щодня, одноразові заходи безпеки або застарілі методи виявлення стають недостатньо ефективними. Організаціям необхідно постійно оновлювати свої системи безпеки та методи ідентифікації шкідливого ПЗ, використовуючи

найсучасніші технології та дані розвідки про загрози.

З огляду на вищезазначену статистику, стає очевидною критична роль комплексних систем ідентифікації та реагування на інциденти, таких як Wazuh SIEM і XDR. Ці системи дозволяють не просто виявляти вже відоме шкідливе ПЗ, а й аналізувати поведінку системи та мережевий трафік для ідентифікації потенційно шкідливих аномалій, що можуть вказувати на нові, раніше невідомі типи атак. Ефективне використання цих систем вимагає глибокого розуміння сучасних кіберзагроз та постійного оновлення знань та інструментів, здатних протистояти їм.

1.2. Аналіз типів шкідливого програмного забезпечення та їх вплив на інформаційну систему організації

Існує багато різних типів шкідливих програм, і зловмисники постійно розробляють більш складні версії, які важко виявити. Тому дуже важливо організовувати проактивні заходи для захисту інформаційної системи організації.
З огляду на те, що незалежний інститут IT-безпеки AV-Test щодня реєструє понад 450 000 нових шкідливих програм, шкідливе програмне забезпечення може бути найбільшою загрозою для організації [4].

Успішна атака шкідливого програмного забезпечення може призвести до втрати доходів, неочікуваних простоїв, викрадення даних та інших дорогих наслідків.

Під шкідливим програмним забезпечення мається на увазі будь-який шкідливий код, програмне забезпечення або скрипт, розгорнутий суб'єктом загрози, щоб завдати шкоди організації або окремій особі. Шкідливе програмне забезпечення зазвичай прикріплюється до електронних листів, вбудовується в шахрайські посилання, ховається в рекламі або підстерігає на різних сайтах, які потенційна жертва можете відвідати. Кінцева мета шкідливого програмного забезпечення - завдати шкоди або використати комп'ютери та мережі, часто для крадіжки даних або грошей.

Достатньо одного необережного кліку працівника, щоб шкідливе програмне забезпечення встановилося і почало виконувати свою програму. Кількість атак шкідливих програм продовжує зростати, пов'язані з ними витрати продовжують зростати, а вектори загроз і типи атак продовжують урізноманітнюватися і ускладнюватися. Наприклад, програма-вимагач як послуга (RaaS) відкрила нові шляхи атак для кіберзлочинців, яким не вистачає технічного досвіду професіоналів. Не кажучи вже про те, що все більше організацій використовують пристрої Інтернету речей і збільшують рівень оцифрування, а це означає, що кількість атак на ланцюги поставок неминуче зростатиме.

Хоча існує багато різних варіацій шкідливого програмного забезпечення, у інформаційній системі організаці найчастіше можна зіткнутися з наступними типами шкідливих програм (табл. 1.1) [5]:

Таблиця 1.1 [5]

Типи шкідливого ПЗ

Тип ШПЗ	Функція	Приклад атаки
Програми-здирники	Відключає доступ жертви до даних до моменту сплати викупу	RYUK
Безфайлове ШПЗ	Вносить зміни до файлів, які є рідними для ОС	Astaroth
Шпигунське ПЗ	Збирає дані про активність користувачів без їхнього відома	DarkHotel
Рекламне ПЗ	Показує небажану рекламу	Fireball
Трояни	Маскується під легітимний код	Emotet
Черв’яки	Поширюється мережею шляхом реплікації	Stuxnet
Руткіти	Дає хакерам віддалений контроль над пристроєм жертви	Zacinlo
Кейлоґери	Відстежує натискання клавіш користувачами	Olympic Vision

Продовження табл. 1.1

Типи шкідливого ПЗ

Тип ШПЗ	Функція	Приклад атаки
Віруси	Самовідтворюється, вбудовуючись у інші програми або файли з метою зміни функціонування комп'ютера без відома або дозволу користувача.	ILOVEYOU

Розглянемо кожен із видів шкідливого програмного забезпечення детальніше.

Програми-здирники - це програмне забезпечення, яке використовує шифрування, щоб позбавити жертву доступу до її даних до моменту сплати викупу. Організація-жертва частково або повністю втрачає можливість працювати, поки не заплатить, але немає жодних гарантій, що після оплати буде отримано необхідний ключ шифрування або що наданий ключ шифрування буде працювати належним чином. Приклад повідомлення, що з'являється у випадку успішної реалізації атаки програмни-здирника зображено на рис. 1.3.

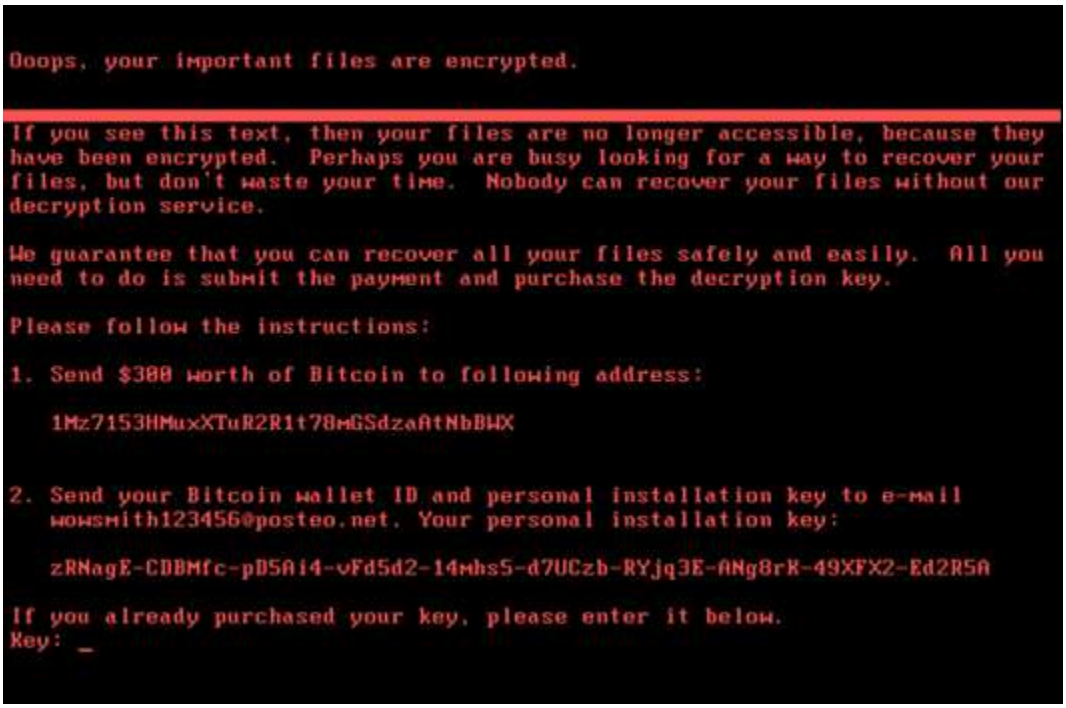

Рис. 1.3. Повідомлення програми-здирника Petya [5]

Безфайлове шкідливе програмне забезпечення спочатку нічого не встановлює,

натомість воно вносить зміни у файли, які є рідними для операційної системи, такі як PowerShell або WMI. Оскільки операційна система розпізнає змінені файли як легітимні, безфайлові атаки не відстежуються антивірусним програмним забезпеченням, а оскільки ці атаки є прихованими, вони вдесятеро успішніші за традиційні атаки шкідливих програм.

Прикладом безфайлового шкідливого програмного забезпечення є Astaroth - програма, яка розсилала користувачам спам із посиланнями на файл ярлика .LNK. Коли користувачі завантажували цей файл, запускався інструмент WMIC, а також низка інших легальних інструментів Windows. Ці інструменти завантажували додатковий код, який виконувався лише в пам'яті, не залишаючи жодних слідів, які можна було б виявити за допомогою сканерів вразливостей. Потім зловмисник завантажив і запустив троянську програму, яка викрала облікові дані і завантажила їх на віддалений сервер.

Шпигунські програми збирають інформацію про дії користувачів без їхнього відома чи згоди. Це можуть бути паролі, пін-коди, платіжна інформація та неструктуровані повідомлення.

Шпигунські програми не обмежуються браузером комп'ютера: вони також можуть діяти в критично важливих додатках або на мобільному телефоні.

Навіть якщо викрадені дані не є критично важливими, вплив шпигунських програм часто поширюється на всю організацію, оскільки погіршується продуктивність і знижується ефективність роботи.

Прикладом шпигунського програмного забезпечення є DarkHotel, який націлився на лідерів бізнесу та уряду, що використовували готельний WIFI, використовував кілька типів шкідливого програмного забезпечення, щоб отримати доступ до систем, що належать певним впливовим людям. Отримавши доступ, зловмисники встановлювали кейлоґери, щоб перехоплювати паролі та іншу конфіденційну інформацію своїх жертв.

Рекламне ПЗ відстежує активність користувача в Інтернеті, щоб визначити, яку рекламу йому показувати. Хоча рекламне ПЗ схоже на шпигунське, воно не встановлює жодного програмного забезпечення на комп'ютер користувача і не

перехоплює натискання клавіш.

Небезпека рекламного ПЗ полягає в порушенні приватності користувача - дані, зібрані рекламним ПЗ, зіставляються з даними, зібраними відкрито чи приховано, про активність користувача в інших місцях в Інтернеті, і використовуються для створення профілю цієї особи, який включає в себе інформацію про те, хто її друзі, що вона купила, куди вона подорожувала тощо. Ця інформація може бути передана або продана рекламодавцям без згоди користувача.

Приклад рекламного ПЗ: у 2017 році рекламне ПЗ під назвою Fireball заразило 250 мільйонів комп'ютерів і пристроїв, викрадаючи браузери, щоб змінити пошукові системи за замовчуванням і відстежувати веб-активність. Однак це шкідливе програмне забезпечення мало потенціал стати чимось більшим, ніж просто неприємністю. Три чверті з них могли віддалено запускати код і завантажувати шкідливі файли.

Троян маскується під легітимний код або програмне забезпечення. Після завантаження нічого не підозрюючими користувачами троян може отримати контроль над системою жертви для зловмисних цілей. Троянські програми можуть ховатися в іграх, додатках або навіть патчах для програмного забезпечення, а також можуть бути вбудовані у вкладення, що містяться у фішингових листах.

Приклад трояна – Emotet. Це складний банківський троян, який існує з 2014 року. З Emotet складно боротися, оскільки він уникає виявлення на основі сигнатур, є стійким і містить модулі-розповсюджувачі, які допомагають йому поширюватися. Троян настільки поширений, що є предметом попередження Міністерства внутрішньої безпеки США, в якому зазначається, що боротьба з Emotet коштувала державним, місцевим, племінним і територіальним урядам до 1 мільйона доларів за один інцидент.

Хробаки використовують вразливості в операційних системах, щоб проникнути в мережу. Вони можуть отримати доступ кількома способами: через вбудовані в програмне забезпечення бекдори, через ненавмисні вразливості в програмному забезпеченні або через флеш-накопичувачі. Після проникнення у систему, черв'яки можуть використовуватися зловмисниками для проведення

DDoS-атак, викрадення конфіденційних даних або атак з вимогою викупу.

Приклад хробака – Stuxnet. Він, ймовірно, був розроблений американськими та ізраїльськими спецслужбами з метою перешкодити ядерній програмі Ірану. Хробак був впроваджений в іранське середовище через флеш-накопичувач. Оскільки середовище було захищене повітряним зазором, його творці ніколи не думали, що Stuxnet зможе покинути мережу своєї цілі - але це сталося. Опинившись на волі, Stuxnet агресивно поширювався, але не завдав великої шкоди, оскільки його єдиною функцією було втручання в роботу промислових контролерів, які керували процесом збагачення урану.

Вірус - це фрагмент коду, який вбудовується в програму і виконується під час її запуску. Потрапивши в мережу, вірус може бути використаний для крадіжки конфіденційних даних, DDoS-атак або атак з вимогою викупу.

Віруси дуже часто плутають із троянами. Однак вірус не може виконуватися або розмножуватися, якщо програма, яку він заразив, не запущена. Ця залежність від програми-хоста відрізняє віруси від троянів, які вимагають, щоб користувачі завантажили їх, і хробаків, які не використовують програми для виконання. Багато видів шкідливого програмного забезпечення підпадають під декілька категорій: наприклад, Stuxnet - це і хробак, і вірус, і руткіт.

Руткіт - це програмне забезпечення, яке надає зловмисникам віддалений контроль над комп'ютером жертви з повними адміністративними привілеями. Руткіти можуть впроваджуватися в додатки, ядра, гіпервізори або мікропрограми. Вони поширюються через фішинг, шкідливі вкладення, шкідливі завантаження та скомпрометовані спільні диски. Руткіти також можуть використовуватися для приховування інших шкідливих програм, наприклад, кейлоґерів.

Прикладом руткіта є Zacinlo, який заражає системи, коли користувачі завантажують підроблену програму VPN. Після встановлення Zacinlo проводить перевірку системи на наявність конкуруючого шкідливого програмного забезпечення і намагається його видалити. Потім він відкриває невидимі браузери і взаємодіє з контентом так, як це робить людина - прокручуючи, виділяючи і клікаючи. Ця активність має на меті обдурити програмне забезпечення для

поведінкового аналізу. Корисне навантаження Zacinlo виникає, коли шкідливе програмне забезпечення натискає на рекламу в невидимих браузерах. Це шахрайство з рекламними кліками забезпечує зловмисникам частину доходу.

Кейлоґер - це тип шпигунського програмного забезпечення, яке відстежує активність користувача. Кейлоґери мають законне застосування: компанії можуть використовувати їх для моніторингу діяльності співробітників, а сім'ї - для відстеження поведінки дітей в Інтернеті.

Однак, якщо їх встановити зі зловмисною метою, клавіатурні шпигуни можуть бути використані для крадіжки паролів, банківських даних та іншої конфіденційної інформації. Кейлоґери можуть потрапити в систему через фішинг, соціальну інженерію або шкідливі завантаження.

До прикладу, кейлоґер під назвою Olympic Vision використовувався для атак на бізнесменів США, Близького Сходу та Азії з метою компрометації ділової електронної пошти. Olympic Vision використовує методи фішингу та соціальної інженерії для зараження систем своїх жертв з метою викрадення конфіденційних даних і шпигунства за бізнес-транзакціями. Кейлоґер не є складним, але його можна придбати на чорному ринку за $25, тому він легко доступний для зловмисників.

Шкідливе програмне забезпечення є серйозною загрозою для бізнесу будь-якого розміру. Важливо знати про різні типи шкідливих програм, а також про різні способи їх передачі.

Отож, імплементація заходів для захисту бізнесу від шкідливого програмного забезпечення може допомогти мінімізувати потенційну шкоду, яку воно може завдати. Саме тому важливо використовувати надійні заходи безпеки, щоб захистити організацію від шкідливих впливів зловмисників та їхніх розробок.

1.3. Аналіз існуючих рішень виявлення шкідливого програмного забезпечення у інформаційній системі організації

У контексті стрімкого розвитку цифрових технологій та збільшення кіберзагроз, існує вагома потреба в ефективних методах виявлення шкідливого програмного забезпечення в інформаційних системах організацій. Різноманіття і складність сучасних кібератак вимагають від фахівців кібербезпеки використання комплексного підходу та передових технологій для забезпечення захисту інформаційних активів. В цьому розділі буде проведено детальний аналіз існуючих рішень для виявлення шкідливого програмного забезпечення, які застосовуються в інформаційних системах організацій.

Метою аналізу є ідентифікація ключових характеристик, переваг, обмежень та ефективності різних інструментів та методологій виявлення шкідливого ПЗ. Це дозволить не лише зрозуміти поточний стан сфери кібербезпеки, але й виявити потенційні шляхи покращення захисту інформаційних систем. Враховуючи швидкі зміни у сфері кіберзагроз, постійне оновлення та адаптація захисних рішень є необхідністю для підтримки високого рівня безпеки.

Одним із провідних рішень у напрямку виявлення вразливостей є ESET Protect [6].

ESET Protect - це комплексне рішення для управління безпекою, призначене для бізнесу, яке зосереджене на виявленні та усуненні різних форм шкідливого програмного забезпечення, зокрема вірусів, програм-вимагачів і шпигунських програм. Зазвичай воно пропонує хмарні або локальні варіанти керування, що дає змогу гнучко розгортати його відповідно до потреб організації [7].

Ключові функції часто включають:

Багаторівневий захист: Використання передових технологій, таких як машинне навчання, аналіз поведінки та хмарні системи репутації для виявлення та блокування загроз.

Захист кінцевих точок: Захист усіх кінцевих точок (комп'ютерів, смартфонів, планшетів і серверів) за допомогою антивірусів, антишпигунських програм,

брандмауерів і фільтрації спаму для захисту від фішингу та шкідливого програмного забезпечення.

Захист даних: Надання інструментів і функцій для захисту конфіденційних даних, запобігання їх витоку та забезпечення відповідності нормативним вимогам щодо захисту даних.

Віддалене керування: Пропонує централізовану консоль управління, яка дозволяє IT-адміністраторам контролювати всю мережеву безпеку з одного місця, полегшуючи застосування політик, оновлення та моніторинг в масштабах всієї організації.

Налаштовуваність і масштабованість: Дозволяє компаніям адаптувати налаштування безпеки до своїх конкретних потреб і масштабувати рішення в міру зростання організації.

ESET Protect має на меті спростити управління IT-безпекою з акцентом на автоматизацію та простоту використання, забезпечуючи при цьому надійний захист від нових загроз. Для отримання найточнішої та найактуальнішої інформації про ESET Protect і про те, як він може задовольнити потреби вашої організації у сфері безпеки, зверніться до офіційних ресурсів ESET або до відділу продажів.

ESET Protect - це комплексне рішення для забезпечення безпеки бізнесу, яке охоплює різні форми захисту від кіберзагроз, зокрема шкідливого програмного забезпечення, програм-вимагачів, фішингу та сучасних постійних загроз (APT). Він легко інтегрується в IT-інфраструктуру бізнесу, пропонуючи як локальні, так і хмарні варіанти розгортання відповідно до різних організаційних потреб та уподобань.

Серед переваг рішення:

Простота та ефективність: Завдяки централізованій консолі керування ESET Protect спрощує розгортання, керування та моніторинг рішень для захисту, зменшуючи складність і ресурси, необхідні для управління IT-безпекою.

Удосконалений захист від загроз: Використовуючи передові технології ESET, зокрема машинне навчання та хмарний аналіз, ESET Protect забезпечує

проактивний захист від нових та еволюціонуючих загроз, гарантуючи, що IT-інфраструктура бізнесу захищена від новітніх кіберзагроз.

Масштабованість: Зі зростанням бізнесу змінюються і його потреби в безпеці. Масштабована архітектура ESET Protect означає, що він може легко рости разом з бізнесом, забезпечуючи безперервний захист без необхідності повної перебудови системи безпеки.

ESET Protect - це комплексне, гнучке й ефективне рішення для кібербезпеки, призначене для підприємств будь-якого розміру. Акцент на розширеному виявленні загроз у поєднанні з простотою управління та масштабованістю робить його надійним вибором для організацій, які прагнуть посилити свій кіберзахист.

Іншим лідером у галузі, щоправда, у класі рішень SIEM, є FortiSIEM [8]. FortiSIEM (Security Information and Event Management) - це рішення, розроблене компанією Fortinet. FortiSIEM надає організаціям комплексну та інтегровану платформу, призначену для покращення їхнього стану безпеки та управління відповідністю нормативним вимогам, пропонуючи видимість у реальному часі в їхньому IT-середовищі [9]. Ось огляд того, що пропонує FortiSIEM:

Основні компоненти FortiSIEM призначені для надання організаціям інтегрованої, комплексної платформи, яка посилює їхню безпеку, керує дотриманням нормативних вимог і забезпечує операційну ефективність у всіх IT-середовищах. В основі FortiSIEM лежить функція Unified Security Analytics, яка агрегує і співвідносить дані з різних джерел, включаючи пристрої безпеки, мережеву інфраструктуру, сервери і додатки. Цей уніфікований підхід забезпечує повне уявлення про ландшафт безпеки організації в режимі реального часу, що дозволяє більш ефективно виявляти і знижувати рівень загроз.

Ключовою особливістю FortiSIEM є функція виявлення та реагування на інциденти, яка використовує розширені аналітичні можливості для виявлення складних загроз безпеці та аномалій в міру їх виникнення. Цей компонент автоматизує процес виявлення, аналізу та реагування на інциденти, значно скорочуючи час від виявлення до усунення. Він призначений для оптимізації роботи та підвищення ефективності команд безпеки в боротьбі з кіберзагрозами.

Крім того, FortiSIEM спрощує управління комплаєнсом, пропонуючи широкі функції звітності, які допомагають організаціям дотримуватися різних регуляторних стандартів, таких як PCI DSS, HIPAA, GDPR та інших. Він автоматизує генерацію та архівування необхідних звітів, гарантуючи, що організації можуть продемонструвати відповідність з легкістю та ефективністю.

На додаток до безпеки та відповідності, FortiSIEM також фокусується на моніторингу продуктивності та доступності критично важливої IT-інфраструктури та додатків. Це гарантує, що будь-які проблеми, які потенційно можуть вплинути на бізнес-операції, будуть швидко виявлені та вирішені, підтримуючи безперервність роботи та мінімізуючи час простою.

Масштабованість і гнучкість рішення також мають фундаментальне значення, дозволяючи йому задовольняти потреби різних організацій, незалежно від їх розміру. FortiSIEM можна розгортати в різних середовищах, включаючи локальну, хмарну або гібридну модель, пропонуючи організаціям гнучкість у виборі конфігурації, яка найкраще відповідає їхній конкретній IT-архітектурі та бізнес-вимогам.

В цілому, основні компоненти FortiSIEM працюють в тандемі, забезпечуючи цілісний підхід до управління інформацією та подіями безпеки, об'єднуючи аналітику безпеки, реагування на інциденти, дотримання нормативних вимог і операційний моніторинг в єдину ефективну платформу, яка підтримує організації в їх постійній боротьбі з кіберзагрозами, забезпечуючи при цьому дотримання нормативних вимог та операційну стійкість.

Ще одне програмне забезпечення, Wazuh, становить собою унікальне рішення, яке ефективно поєднує в собі функціонал і можливості класів систем, згаданих раніше, а саме - Security Information and Event Management (SIEM) та Extended Detection and Response (XDR). Ця інтеграція робить Wazuh одночасно потужним інструментом для збору, аналізу безпекових подій з різних джерел і розширеного виявлення загроз та реагування на них. Популярність Wazuh серед організацій різного масштабу пояснюється його гнучкістю, масштабованістю та

високим рівнем адаптації під специфічні потреби безпеки, забезпечуючи комплексний захист інформаційних систем.

Wazuh - це потужне рішення для моніторингу безпеки з відкритим вихідним кодом, яке поєднує в собі можливості управління інформацією та подіями безпеки (SIEM) і виявлення та реагування на кінцеві точки (EDR) для забезпечення комплексного захисту від кіберзагроз. Саме такий синтез різних класів рішень і робить його унікальним гравцем на ринку. Wazuh покликаний допомогти організаціям захистити своє цифрове середовище, пропонуючи розширені можливості виявлення загроз, реагування на інциденти та управління відповідністю нормативним вимогам [10].

Невід'ємною частиною її дизайну є ефективний механізм реагування на інциденти. Wazuh швидко сповіщає команди безпеки про виявлення загрози, надаючи їм детальну інформацію про характер загрози. Це дає змогу оперативно та обґрунтовано реагувати, що важливо для зменшення ризиків та мінімізації потенційних збитків. Крім того, Wazuh виступає надійним союзником в управлінні комплаєнсом, сприяючи дотриманню суворих регуляторних стандартів, таких як PCI DSS, HIPAA та GDPR. Це досягається завдяки ретельній реєстрації, моніторингу та звітності, які є ключовими для всебічного аналізу даних і дотримання вимог.

Платформа також поширює свій захист на кінцеві точки, пропонуючи надійний захист кінцевих точок. Завдяки таким функціям, як моніторинг цілісності файлів, аналіз даних журналів і виявлення шкідливого програмного забезпечення, Wazuh посилює систему безпеки кінцевих точок, слугуючи критично важливою лінією захисту від кібервторгнень.

Масштабованість і гнучкість є одними з визначальних рис Wazuh, що дозволяє задовольнити динамічні вимоги безпеки будь-якої організації. Модульна архітектура та відкрите програмне забезпечення Wazuh, яке можна розгортати в різних середовищах - фізичному, віртуальному або хмарному, - дозволяють широко кастомізувати рішення. Це гарантує, що організації можуть адаптувати Wazuh до

своїх конкретних потреб безпеки, що робить його універсальним інструментом в арсеналі кібербезпеки.

Інтегруючи ці основні компоненти в єдину платформу з відкритим вихідним кодом, Wazuh забезпечує потужне і комплексне рішення для сучасних викликів кібербезпеки. Здатність забезпечувати розширене виявлення загроз, оптимізоване реагування на інциденти, суворе управління відповідністю та інтегрований захист кінцевих точок робить Wazuh безцінним активом для організацій, які прагнуть посилити свою систему кібербезпеки.

У цьому розділі ми провели детальний аналіз трьох передових рішень у сфері кібербезпеки: FortiSIEM від Fortinet, ESET Protect та Wazuh. Кожне з цих рішень пропонує унікальний набір функцій, спрямованих на захист інформаційних систем від широкого спектру кіберзагроз.

FortiSIEM вирізняється своєю здатністю до швидкого виявлення і реагування на інциденти, а також ефективним управлінням інцидентами. ESET Protect, зі свого боку, надає комплексний захист кінцевих точок та даних, з акцентом на простоту управління та ефективність виявлення загроз.

Проте, серед аналізованих рішень, Wazuh виділяється як найперспективніший кандидат для подальшого дослідження. Його відкритий код та гнучкість роблять Wazuh особливо привабливим для організацій, що прагнуть налаштувати систему безпеки під свої унікальні потреби. Wazuh об'єднує в собі функціональність SIEM і EDR, пропонуючи комплексний захист від кіберзагроз, з можливістю масштабування під різні вимоги безпеки. Окрім того, його здатність до інтеграції з різноманітними інструментами та платформами робить Wazuh вкрай ефективним у будівлі цілісної системи кіберзахисту.

2. АНАЛІЗ МОЖЛИВОСТЕЙ ТА ФУНКЦІОНАЛУ WAZUH SIEM І XDR В КОНТЕКСТІ ВИЯВЛЕННЯ ШКІДЛИВОГО ПЗ

2.1. Аналіз класів рішень SIEM і XDR

У сучасному світі кібербезпеки, де кіберзагрози еволюціонують із кожним днем, ефективне управління безпекою та відповідь на інциденти є ключовими для захисту інформаційних систем організацій. У цьому контексті, рішення Security Information and Event Management (SIEM) та Extended Detection and Response (XDR) відіграють вирішальну роль. Вони не лише допомагають ідентифікувати та реагувати на кіберзагрози в реальному часі, але й забезпечують комплексний огляд безпекового стану інфраструктури. Цей розділ присвячено детальному аналізу класів рішень SIEM і XDR, їхньої ролі в стратегії кібербезпеки сучасних організацій та порівняльному аналізу їхніх можливостей та використання.

SIEM рішення зосереджені на агрегації, аналізі та зберіганні журналів подій з різних джерел в межах IT-інфраструктури, надаючи IT-фахівцям інструменти для моніторингу, виявлення та реагування на безпекові інциденти. З іншого боку, XDR пропонує розширений підхід, об'єднуючи дані та аналітику з різних точок захисту для більш глибокого аналізу і швидшого виявлення складних загроз.

Обидва класи рішень мають свої унікальні переваги та обмеження, і вибір між ними або вирішення їхнього спільного використання залежить від специфічних потреб та вимог організації до кібербезпеки. Вивчення та аналіз цих рішень дозволить краще зрозуміти, як вони можуть бути інтегровані в загальну структуру кібербезпеки організації для забезпечення більш ефективного захисту від широкого спектру кіберзагроз.

Щодо рішень класу SIEM, то на найпростішому рівні вони виконують певні функції агрегації, консолідації та сортування даних для виявлення загроз і дотримання вимог щодо відповідності даних. Хоча деякі рішення відрізняються за можливостями, більшість з них пропонують однаковий базовий набір функцій [11]:

Керування журналом. SIEM збирає дані про події з широкого спектру джерел по всій IT-інфраструктурі організації, включаючи локальні та хмарні середовища.

Дані журналів подій від користувачів, кінцевих точок, додатків, джерел даних, хмарних робочих навантажень і мереж, а також дані з апаратного і програмного забезпечення для забезпечення безпеки, наприклад, міжмережевих екранів або антивірусного програмного забезпечення, збираються, зіставляються і аналізуються в режимі реального часу.

Деякі рішення SIEM також інтегруються зі сторонніми каналами розвідки загроз, щоб співвідносити свої внутрішні дані про безпеку з раніше розпізнаними сигнатурами і профілями загроз. Інтеграція з каналами загроз у режимі реального часу дозволяє командам блокувати або виявляти нові типи сигнатур атак.

Кореляція та аналітика подій. Кореляція подій є невід'ємною частиною будь-якого рішення SIEM. Використовуючи розширену аналітику для виявлення і розуміння складних шаблонів даних, кореляція подій дає можливість швидко знаходити і зменшувати потенційні загрози для безпеки бізнесу.

Рішення SIEM значно покращують середній час виявлення (MTTD) і середній час реагування (MTTR) для команд IT-безпеки, розвантажуючи ручні робочі процеси, пов'язані з поглибленим аналізом подій безпеки.

Моніторинг інцидентів та оповіщення про безпеку. SIEM консолідує аналіз на єдиній центральній інформаційній панелі, де команди безпеки відстежують активність, сортують сповіщення, ідентифікують загрози та ініціюють реагування або усунення.

Більшість інформаційних панелей SIEM також включають візуалізацію даних у режимі реального часу, що допомагає аналітикам безпеки виявляти сплески або тенденції підозрілої активності. Використовуючи настроювані, заздалегідь визначені правила кореляції, адміністратори можуть негайно отримувати сповіщення і вживати відповідних заходів для зменшення загроз до того, як вони матеріалізуються в більш серйозні проблеми безпеки.

Комплаєнс-менеджмент та звітність. Рішення SIEM є популярним вибором для організацій, які підлягають різним формам нормативно-правового

регулювання. Завдяки автоматизованому збору та аналізу даних SIEM є цінним інструментом для збору та перевірки даних про дотримання нормативних вимог у всій бізнес-інфраструктурі.

Рішення SIEM можуть генерувати звіти про відповідність вимогам PCI-DSS, GDPR, HIPPA, SOX та інших стандартів у режимі реального часу, зменшуючи навантаження на управління безпекою та виявляючи потенційні порушення на ранніх стадіях, щоб їх можна було усунути. Багато рішень SIEM постачаються з попередньо встановленими, готовими до використання надбудовами, які можуть генерувати автоматизовані звіти, призначені для дотримання вимог нормативно-правових актів.

Незалежно від того, наскільки великою чи малою є організація, дуже важливо вживати проактивних заходів для моніторингу та зменшення ризиків IT-безпеки. Рішення SIEM приносять користь підприємствам різними способами і стали важливим компонентом в оптимізації робочих процесів безпеки.

Рішення SIEM забезпечують централізований аудит відповідності та звітність по всій бізнес-інфраструктурі. Розширена автоматизація спрощує збір та аналіз системних журналів і подій безпеки, що дозволяє зменшити використання внутрішніх ресурсів, одночасно дотримуючись суворих стандартів звітності про відповідність.

Завдяки покращеній видимості IT-середовищ, SIEM може стати важливим фактором підвищення ефективності роботи між відділами.

Центральна інформаційна панель забезпечує уніфікований перегляд системних даних, оповіщень і сповіщень, що дозволяє командам ефективно спілкуватися і співпрацювати при реагуванні на загрози та інциденти безпеки.

З огляду на те, як швидко змінюється ландшафт кібербезпеки, організаціям необхідно мати можливість покладатися на рішення, здатні виявляти і реагувати як на відомі, так і на невідомі загрози безпеці.

Використовуючи інтегровані канали розвідки загроз і технології штучного інтелекту, рішення SIEM можуть допомогти командам безпеки ефективніше реагувати на широкий спектр кібератак, включаючи:

Внутрішні загрози: Уразливості в системі безпеки або атаки, що походять від осіб, які мають санкціонований доступ до мереж і цифрових активів компанії.

Фішинг: повідомлення, які виглядають як надіслані надійним відправником, часто використовуються для крадіжки даних користувачів, облікових даних для входу в систему, фінансової інформації або іншої конфіденційної бізнес-інформації.

Програми-вимагачі: Шкідливе програмне забезпечення, яке блокує дані або пристрій жертви і погрожує зберегти їх заблокованими або ще гірше, якщо жертва не заплатить викуп зловмиснику.

Розподілені атаки на відмову в обслуговуванні (DDoS): Атаки, які бомбардують мережі та системи некерованим трафіком з розподіленої мережі викрадених пристроїв (ботнету), знижуючи продуктивність веб-сайтів і серверів до неможливості їх використання.

Витік даних: Крадіжка даних з комп'ютера або іншого пристрою, що здійснюється вручну або автоматично за допомогою шкідливого програмного забезпечення.

Зі зростанням популярності віддаленої роботи, додатків SaaS і політик BYOD організаціям потрібен рівень видимості, необхідний для зменшення мережевих ризиків за межами традиційного периметра мережі.

Рішення SIEM відстежують всю мережеву активність всіх користувачів, пристроїв і додатків, значно підвищуючи прозорість всієї інфраструктури і виявляючи загрози незалежно від того, звідки здійснюється доступ до цифрових активів і сервісів.

Що ж стосується рішень класу XDR, то рішення Extended Detection and Response забезпечують уніфіковану платформу для моніторингу та реагування на різноманітні мережеві загрози [12]. Інструменти можуть запобігати, виявляти, аналізувати та реагувати на загрози, які впливають на вашу мережу. Цей набір функцій об'єднано в одному інструменті, що дозволяє оптимізувати роботу та покращити управління операціями. Це також призводить до покращення

реагування на атаки. Інформація може безперешкодно надсилатися інструментам реагування, що призводить до швидкого та ефективного усунення загрози.

Рішення XDR є невід'ємними компонентами комплексної системи кібербезпеки. Вони не тільки дають командам безпеки більше інформації про мережу та події, але й координують реагування. Завдяки широкому спектру та комплексності інструментів, інформація та реагування краще пов'язані між собою по всій вашій організації, що призводить до скорочення часу вирішення проблем та підвищення ефективності. Вони дозволяють організаціям захищатися від широкого спектру загроз, включаючи:

- сучасні постійні загрози (APT);
- безфайлове шкідливе програмне забезпечення;
- фішинг;
- вразливості нульового дня;
- внутрішні загрози;
- DDoS-атаки.

Після того, як дані потрапляють на платформу XDR, можна запустити складний аналіз для виявлення тенденцій і потенційних загроз. XDR використовує штучний інтелект, щоб знайти винятки в крихтах даних, які він збирає. З часом штучний інтелект стане більш точним, оскільки він створить більш чітку картину вашої поведінки і вашої системи. Це дозволяє йому виявляти моделі поведінки, які в іншому випадку залишилися б непоміченими людським аналізом.

Рішення XDR надають чітку інформаційну панель, яка дозволяє адміністраторам розуміти зібрані дані. Це гарантує, що адміністратор може прийняти обґрунтоване рішення щодо характеру загрози та забезпечити ефективність своїх політик безпеки.

Саме за допомогою цієї аналітичної панелі ви можете зрозуміти поточні або усунуті атаки. Графіки вузлів і часові шкали чітко пояснюють, як атака проникла у вашу систему, і відстежують її шлях у вашій мережі. У разі поточних атак це дозволяє захистити області, які ще не були уражені, тим самим підтримуючи

безпеку мережі. Якщо шаблон атаки було відтворено, XDR позначить його і надасть інформацію про те, як найкраще протистояти цій атаці.

Після виявлення загрози XDR може вжити точних заходів для її усунення. Це може включати блокування IP-адреси, блокування домену або карантин підозрілого ресурсу. XDR може реагувати автоматично, забезпечуючи тим самим якнайшвидше припинення атак. Автоматичне реагування відбувається за заздалегідь визначеним планом, щоб гарантувати, що критично важлива для бізнесу інфраструктура не буде виведена з ладу без нагляду з боку людини. Цей план може бути адаптований адміністратором, але також діятиме динамічно - рішення XDR реагуватиме на проблему, з якою стикається, і реагуватиме на поведінку конкретної загрози.

Наприклад, якщо кінцева точка заражена, її можна негайно заблокувати в мережі, а не чекати схвалення цього простого кроку від зайнятого IT-спеціаліста. Це запобігає поширенню шкідливого програмного забезпечення, дозволяючи персоналу зосередитися на найбільш складних і нагальних проблемах.

Для більш складних атак IT-спеціалістам може знадобитися більше контролю над реагуванням XDR. Вимагаючи втручання людини лише в разі крайньої необхідності, можна зменшити втому від інформаційних панелей, водночас гарантуючи, що IT-персонал зможе зосередитися на важливих питаннях. "Втома від тривог" - це проблема, з якою наразі стикаються 83% [13] співробітників служби безпеки - це коли особа, відповідальна за управління реагуванням, перевантажена, а згодом втрачає чутливість до кількості тривог. Якщо більшість тривог є хибними, адміністратор навряд чи зможе оцінити всю важливість загрози.

Рішення XDR є важливим елементом системи кібербезпеки організації завдяки надійному та ефективному захисту, який вони можуть забезпечити. Завдяки широкому спектру можливостей і функцій вони дозволяють підвищити рівень виявлення загроз і можуть забезпечити більш цілеспрямоване усунення наслідків інцидентів. Це, в кінцевому підсумку, призводить до покращення безпеки та підвищення відмовостійкості операцій. Ось деякі інші переваги рішення XDR:

• XDR може виявляти більш складні, сучасні загрози.

• Захищає ширший діапазон мережевих областей, ніж інші рішення.

• Ефективний аналіз даних.

• Автоматизація зменшує навантаження на IT-команду, дозволяючи їй перенаправити свої зусилля.

• Постійно розвивається і вдосконалюється завдяки можливостям машинного навчання.

• Уніфікованим рішенням легше керувати, ніж декількома незалежними технологіями.

Рішення XDR використовується для посилення та вдосконалення існуючих засобів захисту кібербезпеки, тим самим зміцнюючи обороноздатність організації. Це досягається шляхом виявлення вразливостей і загроз на ранніх стадіях їхнього життєвого циклу, а потім розгортання ефективних засобів усунення для зведення загрози нанівець. Вирішуючи проблему на ранній стадії її життєвого циклу, їй дається менше можливостей завдати шкоди, а це означає, що для її усунення потрібно менше фактичної роботи.

Таким чином, у цьому розділі ми здійснили детальний аналіз і порівняння рішень класів SIEM і XDR, розглянувши їх ключові характеристики, сфери застосування та внесок у загальну стратегію кібербезпеки організацій. Рішення SIEM зосереджені на агрегації, аналізі та зберіганні журналів подій, надаючи IT-фахівцям інструменти для моніторингу, виявлення та реагування на безпекові інциденти. З іншого боку, XDR пропонує більш розширений підхід, об'єднуючи дані та аналітику з різних точок захисту для глибокого аналізу і швидкого виявлення складних загроз.

Обидва підходи мають свої унікальні переваги та можуть внести значний вклад у забезпечення кібербезпеки. Однак, наш аналіз виявив, що Wazuh, що поєднує в собі функціональність і можливості обох класів рішень, стоїть окремо як найбільш обіцяючий кандидат для подальшого вивчення та впровадження.

Wazuh виділяється завдяки своїй відкритій архітектурі, масштабованості та гнучкості, що дозволяє організаціям не лише адаптувати рішення під свої унікальні потреби, але й забезпечити комплексний захист від широкого спектру кіберзагроз.

Використання Wazuh може значно підвищити ефективність виявлення загроз, спростити управління інцидентами та оптимізувати процеси відповідності нормативним вимогам.

Таким чином, Wazuh представляє собою вагомий інструмент в арсеналі кібербезпеки організації, здатний забезпечити не лише високий рівень захисту, але й гнучкість та адаптивність у відповіді на постійно змінювані кіберзагрози. Ось чому, з урахуванням проведеного аналізу, Wazuh рекомендується як найбільш перспективне рішення для подальшого дослідження та інтеграції в стратегію кібербезпеки сучасних організацій.

2.2. Архітектура платформи Wazuh

Архітектура платформи Wazuh представляє собою комплексне рішення в області кібербезпеки, розроблене для забезпечення глибокого моніторингу безпеки, виявлення загроз, відповіді на інциденти та здійснення вимог до відповідності в IT-інфраструктурах різноманітних масштабів і складності. Цей розділ призначений для детального розгляду структури та ключових компонентів архітектури Wazuh, які разом формують її потужну основу для забезпечення безпеки інформаційних систем.

Архітектура Wazuh складається з декількох взаємопов'язаних елементів, що працюють синхронно для збору, аналізу та кореляції даних з різних джерел, включаючи кінцеві точки, мережі та сервери. Це дозволяє організаціям отримувати реальне уявлення про свій безпековий статус і ефективно реагувати на шкідливі дії або вразливості в їхніх IT-системах.

Архітектура Wazuh базується на агентах, які працюють на кінцевих точках, що контролюються, і пересилають дані про безпеку на центральний сервер. Підтримуються пристрої без агентів, такі як фаєрволи, комутатори, маршрутизатори та точки доступу, які можуть активно надсилати дані журналів через Syslog, SSH або за допомогою свого API. Центральний сервер декодує та

аналізує вхідну інформацію і передає результати на індексатор Wazuh для індексації та зберігання.

Кластер індексатора Wazuh - це сукупність одного або декількох вузлів, які взаємодіють між собою для виконання операцій читання та запису індексів. Невеликі розгортання Wazuh, які не потребують обробки великих обсягів даних, можна легко впоратися за допомогою одновузлового кластера. Кластери з декількома вузлами рекомендуються, коли є багато кінцевих точок, за якими ведеться спостереження, коли очікується великий обсяг даних або коли потрібна висока доступність.

У виробничих середовищах рекомендується розгортати сервер Wazuh та індексатор Wazuh на різних хостах. У цьому сценарії Filebeat використовується для безпечного пересилання сповіщень Wazuh і заархівованих подій на кластер індексатора Wazuh (одновузловий або багатовузловий) за допомогою шифрування TLS.

На рис. 2.1. представлена архітектура розгортання Wazuh. Вона показує компоненти рішення і те, як сервер Wazuh і вузли індексатора Wazuh можуть бути сконфігуровані як кластери, забезпечуючи балансування навантаження і високу доступність [14].

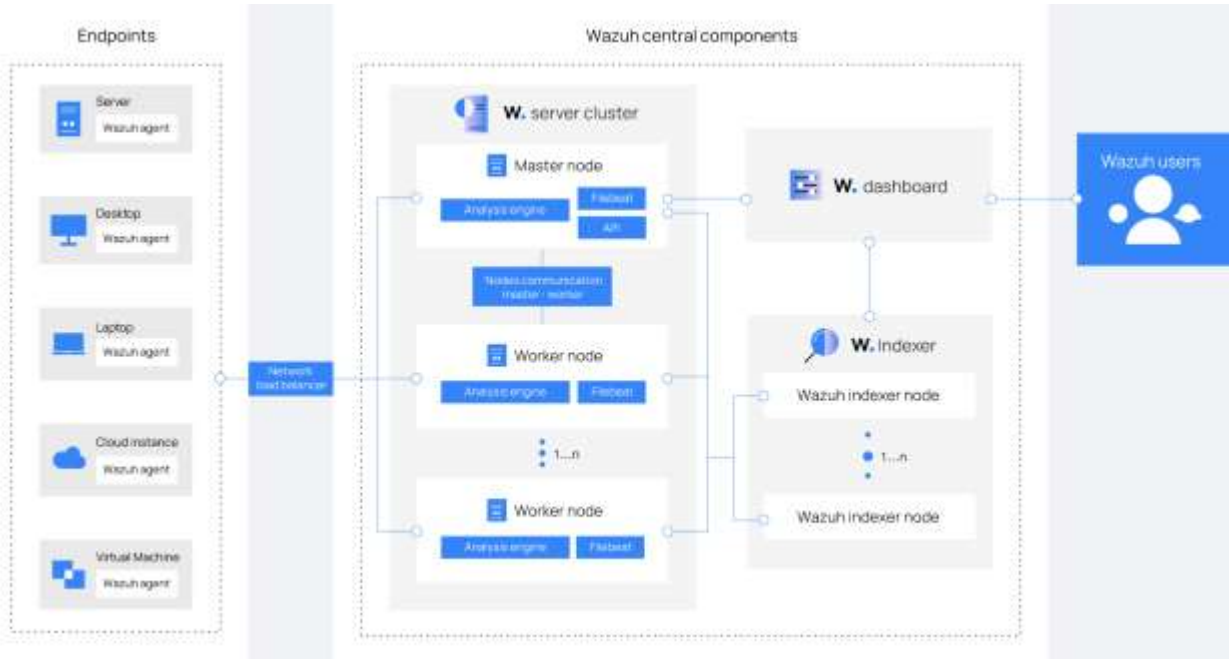

Рис. 2.1. Центральні компоненти рішення Wazuh [14]

Агент Wazuh постійно надсилає події на сервер Wazuh для аналізу та виявлення загроз. Щоб почати надсилати ці дані, агент встановлює з'єднання з серверною службою для підключення агентів, яка за замовчуванням слухає порт 1514 (це можна налаштувати). Потім сервер Wazuh розшифровує і перевіряє отримані події на відповідність правилам, використовуючи механізм аналізу. Події, які викликають спрацьовування правила, доповнюються даними попередження, такими як ідентифікатор правила та назва правила. Події можуть бути записані в один або обидва з наведених нижче файлів, залежно від того, чи спрацювало правило, чи ні:

• Файл /var/ossec/logs/archives/archives.json містить усі події, незалежно від того, чи спрацювало правило, чи ні.

• Файл /var/ossec/logs/alerts/alerts.json містить лише події, які викликали спрацювання правила з достатньо високим пріоритетом (поріг налаштовується).

Протокол повідомлень Wazuh за замовчуванням використовує шифрування AES з 128 бітами на блок і 256-бітними ключами. Шифрування Blowfish не є обов'язковим.

Сервер Wazuh використовує Filebeat для надсилання оповіщень та даних про події до індексатора Wazuh, використовуючи шифрування TLS. Filebeat зчитує вихідні дані сервера Wazuh і надсилає їх до індексатора Wazuh (за замовчуванням прослуховує порт 9200/TCP). Після того, як дані проіндексовані індексатором Wazuh, інформаційна панель Wazuh використовується для видобутку та візуалізації інформації.

Інформаційна панель Wazuh запитує RESTful API Wazuh (за замовчуванням прослуховує порт 55000/TCP на сервері Wazuh) для відображення інформації про конфігурацію та стан сервера і агентів Wazuh. Він також може змінювати налаштування конфігурації агентів або сервера за допомогою викликів API. Цей зв'язок шифрується за допомогою TLS та автентифікується за допомогою імені користувача та пароля.

Як тривожні, так і нетривожні події зберігаються у файлах на сервері Wazuh, а також надсилаються до індексатора Wazuh. Ці файли можуть бути записані у

форматі JSON (.json) або звичайному текстовому форматі (.log). Ці файли щодня стискаються і підписуються з використанням контрольних сум MD5, SHA1 і SHA256. Структура каталогів та імен файлів виглядає, як на рис. 2.2.

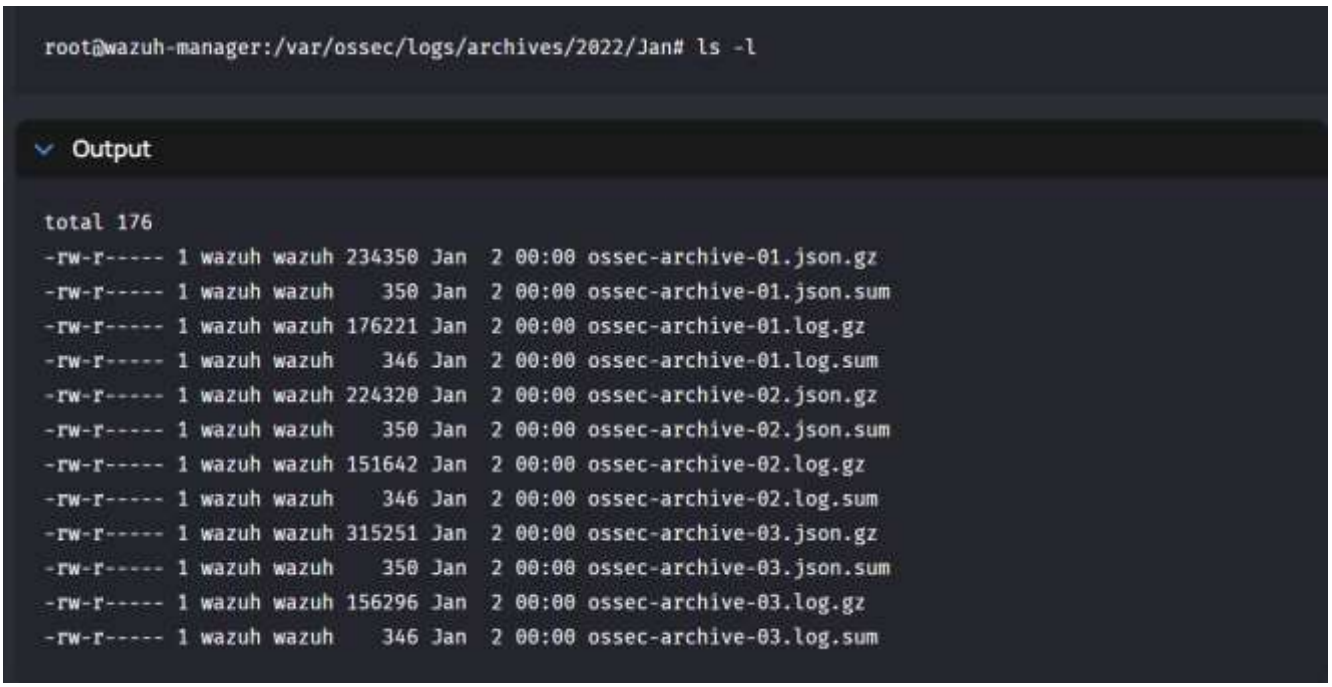

Рис. 2.2. Файли логів Wazuh

Ротацію та резервне копіювання архівних файлів рекомендується здійснювати відповідно до обсягу пам'яті сервера Wazuh. Використовуючи завдання cron, можна легко зберігати на сервері лише певний часовий проміжок архівних файлів, наприклад, за минулий рік або за останні три місяці.

Отже, Wazuh відіграє ключову роль в організації кібербезпеки для організацій. Детальний огляд структури та компонентів Wazuh виявив її здатність ефективно збирати, аналізувати та корелювати дані з різноманітних джерел для ідентифікації та реагування на потенційні загрози. Модульна природа Wazuh, що підтримується агентами на кінцевих точках і здатність до інтеграції з різноманітними джерелами даних та інструментами безпеки, забезпечує гнучкість, необхідну для адаптації до унікальних вимог безпеки кожної організації.

Розгортання Wazuh у виробничих середовищах, зокрема розділення сервера Wazuh та індексатора на різні хости для забезпечення оптимальної продуктивності та високої доступності, є важливим кроком для підтримки масштабування та

надійності системи. Це дозволяє ефективно обробляти великі обсяги даних і забезпечувати безперервний моніторинг безпеки.

Використання шифрування для захисту даних, які передаються між компонентами системи, забезпечує високий рівень конфіденційності та цілісності інформації. Крім того, можливість візуалізації та детального аналізу за допомогою інформаційної панелі Wazuh значно спрощує процес ідентифікації загроз та вжиття відповідних заходів реагування.

Загалом, архітектура Wazuh надає потужну основу для розробки і впровадження ефективної стратегії кібербезпеки, яка може адаптуватися до змінних умов кіберпростору та вимог до безпеки. Вона виступає як центральна точка управління кібербезпекою, здатна інтегрувати різноманітні інструменти та сервіси для забезпечення всебічного захисту інформаційних активів організації.

2.3. Функціональні можливості та модулі рішення Wazuh

У рамках комплексного підходу до кібербезпеки, рішення Wazuh виокремлюється своїм широким спектром функціональних можливостей, які відповідають вимогам сучасних IT-інфраструктур. Цей розділ зосереджено на детальному аналізі ключових функціональних можливостей Wazuh, що забезпечують ефективний захист від широкого спектру кіберзагроз, управління інцидентами безпеки, а також відповідність нормативно-правовим та галузевим стандартам.

Функціональні можливості Wazuh охоплюють не лише базові аспекти безпеки, такі як виявлення шкідливого програмного забезпечення та моніторинг змін у системі, але й передові технології аналізу даних та відповіді на інциденти. Це включає глибоку інтеграцію з обладнанням і програмами, що дозволяє забезпечити ретельний моніторинг активів та швидке реагування на потенційні загрози.

Особлива увага приділяється також системам управління конфігураціями, контролю цілісності файлів, аналітиці поведінки користувачів і мережевому

моніторингу, що разом формують багатошаровий захист. Вивчення цих функціональних можливостей дозволить користувачам глибше зрозуміти, як Wazuh може бути інтегрований у загальну систему кібербезпеки організації, а також як це рішення може бути налаштоване для задоволення специфічних потреб безпеки.

Розглянемо детальніше основні функціональні можливості SIEM і XDR рішення Wazuh [15]. Першою і доволі важливою функціональною можливістю є моніторинг цілісності файлів (FIM) - це процес безпеки, який використовується для моніторингу цілісності системних файлів і файлів додатків. FIM є важливим рівнем захисту для будь-якої організації, яка контролює конфіденційні активи. Він забезпечує захист конфіденційних даних, програм і файлів пристроїв шляхом моніторингу, регулярного сканування та перевірки їхньої цілісності. Це допомагає організаціям виявляти зміни в критично важливих файлах у своїх системах, що знижує ризик викрадення або компрометації даних. Цей процес може заощадити час і гроші на втраченій продуктивності, недоотриманих доходах, репутаційних збитках і штрафах за порушення законодавчих і регуляторних норм.

Wazuh має вбудовану функцію моніторингу цілісності файлів. Модуль Wazuh FIM відстежує файли і каталоги та запускає сповіщення, коли користувач або процес створює, змінює або видаляє відстежувані файли. Він виконує базове сканування, зберігаючи криптографічну контрольну суму та інші атрибути відстежуваних файлів. Коли користувач або процес змінює файл, модуль порівнює його контрольну суму та атрибути з базовою лінією. Якщо він виявляє невідповідність, то видає сповіщення. Модуль FIM виконує сканування в режимі реального часу і за розкладом, залежно від конфігурації FIM для агентів і менеджера.

Серед переваг модуля FIM Wazuh - управління змінами, виявлення загроз і реагування на них, а також дотримання нормативних вимог, як показано нижче.

Одна з найважливіших функцій - виявлення шкідливого програмного забезпечення. Це процес аналізу комп'ютерної системи або мережі на наявність шкідливого програмного забезпечення та файлів. Засоби захисту можуть виявляти

шкідливе програмне забезпечення, перевіряючи його на наявність сигнатур відомих шкідливих програм. Інструменти безпеки також можуть виявляти зловмисну активність, виявляючи підозрілу поведінку програмного забезпечення. Коли шкідливе програмне забезпечення заражає систему, воно може модифікувати її за допомогою різних методів, щоб уникнути виявлення. Wazuh використовує широкий спектр підходів для протидії цим методам, щоб виявити шкідливі файли та аномальні шаблони, які вказують на присутність шкідливого програмного забезпечення.

Модуль моніторингу цілісності файлів (FIM) Wazuh допомагає виявляти шкідливі файли на відстежуваних кінцевих точках. Сам по собі модуль FIM не може виявити шкідливі файли. Однак можна виявити шкідливе програмне забезпечення, поєднавши модуль FIM з правилами виявлення загроз і джерелами розвідки загроз. Також можна налаштувати Wazuh на використання подій FIM з такими джерелами інформації про загрози, як VirusTotal і списки CDB, що містять хеші файлів, а також сканування YARA для виявлення шкідливого програмного забезпечення.

Wazuh виявляє поведінку руткітів на відстежуваних кінцевих точках за допомогою модуля Rootcheck. Rootcheck безперервно контролює кінцеві точки і генерує сповіщення, коли виявляє будь-яку аномалію. Моніторинг аномалій гарантує, що Wazuh виявить шкідливе програмне забезпечення, яке методи, засновані на сигнатурах, могли пропустити. Rootcheck також використовує відомі сигнатури руткітів і троянів, щоб виявити їхню присутність на відстежуваних кінцевих точках. Гнучкість Wazuh гарантує, що користувачі можуть самостійно оновлювати ці сигнатури руткітів.

Функція збору журналів Wazuh дозволяє збирати журнали сторонніх програм для виявлення шкідливого програмного забезпечення. Використовуючи цю можливість, Wazuh збирає та аналізує журнали різних програм для виявлення шкідливого програмного забезпечення, таких як Windows Defender та ClamAV.

Оцінка конфігурації безпеки (Security Configuration Assessment, SCA) - це процес перевірки відповідності всіх систем набору заздалегідь визначених правил

щодо налаштувань конфігурації та дозволеного використання додатків. Один з найбільш надійних способів захистити кінцеві точки - зменшити їхню вразливість. Цей процес широко відомий як загартовування. Оцінка конфігурації - це ефективний спосіб виявити слабкі місця у кінцевих точках і виправити їх, щоб зменшити поверхню атаки.

Модуль Wazuh SCA виконує сканування для виявлення неправильних конфігурацій і вразливостей на контрольованих кінцевих точках і рекомендує дії для їх усунення. Ці сканування оцінюють конфігурацію кінцевих точок за допомогою файлів політик, які містять правила, що перевіряються на відповідність фактичній конфігурації кінцевих точок. Політики SCA можуть перевіряти наявність файлів, каталогів, ключів і значень реєстру, запущених процесів, а також рекурсивно перевіряти наявність файлів всередині каталогів.

Наприклад, модуль SCA може оцінити, чи потрібно змінити конфігурацію, пов'язану з паролями, видалити непотрібне програмне забезпечення, відключити непотрібні служби або перевірити конфігурацію стека TCP/IP.

Політики для модуля SCA написані у форматі YAML. Цей формат було обрано тому, що він є зручним для читання і зрозумілим. Тому, можна легко написати власні політики SCA або розширити існуючі відповідно до потреб організації. Крім того, Wazuh розповсюджується з набором готових політик, які в основному базуються на бенчмарках CIS, що є усталеним стандартом для захисту кінцевих точок.

Команди безпеки часто стикаються з проблемами при реагуванні на інциденти, такими як своєчасне реагування на події з високим ступенем тяжкості або забезпечення повних заходів з пом'якшення наслідків. Їм може бути складно збирати відповідну інформацію в режимі реального часу, що ускладнює розуміння повного масштабу інциденту. Ці проблеми ускладнюють стримування та пом'якшення наслідків кібератаки.

Платформа Wazuh SIEM та XDR покращує реагування на інциденти:

- Забезпечення видимості подій безпеки в режимі реального часу;
- зменшення втоми від оповіщень;

- автоматизації дій у відповідь на загрози;
- надання готових сценаріїв реагування.

Wazuh має модуль активного реагування, який допомагає командам безпеки автоматизувати дії реагування на основі певних тригерів, що дозволяє їм ефективно управляти інцидентами безпеки.

Автоматизація дій реагування гарантує, що високопріоритетні інциденти розглядаються та усуваються вчасно та послідовно. Це особливо цінно в умовах, коли команди безпеки обмежені в ресурсах і повинні визначати пріоритети у своїх зусиллях з реагування.

Модуль активного реагування Wazuh виконує ці сценарії на відстежуваних кінцевих точках, коли спрацьовує оповіщення певного ідентифікатора правила, рівня або групи правил. Ви можете встановити будь-яку кількість сценаріїв для запуску у відповідь на тригер; однак ви повинні ретельно продумати ці реакції. Погана реалізація правил і реакцій може збільшити вразливість кінцевого пристрою.

На рис. 2.3 показано робочий процес активного реагування.

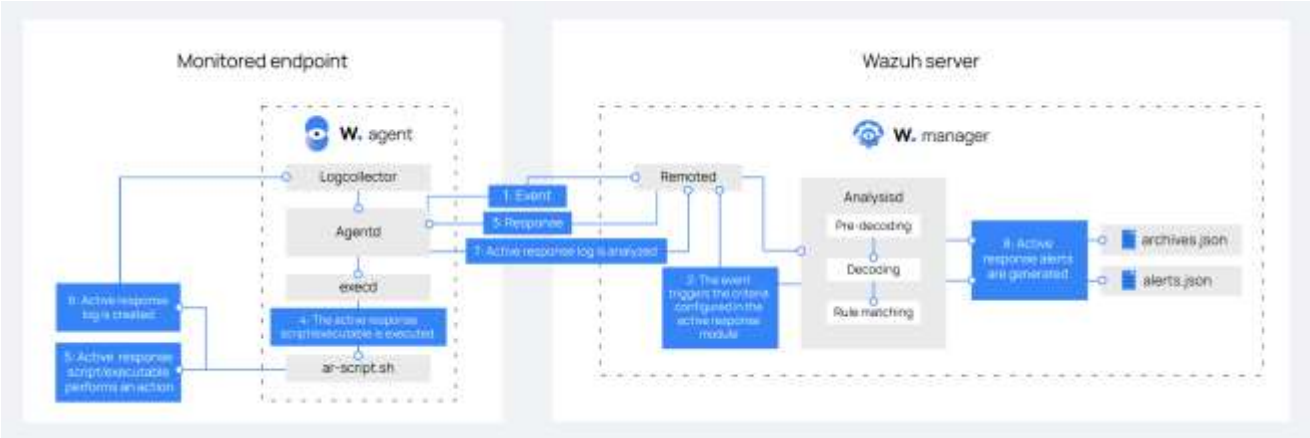

Рис. 2.3. Активне реагування

Функція «Збір даних журналів» передбачає збір і консолідацію журналів з різних джерел журналів у мережі. Збір даних журналів допомагає командам безпеки відповідати нормативним вимогам, виявляти та усувати загрози, а також виявляти помилки додатків та інші проблеми з безпекою.

Wazuh збирає, аналізує і зберігає журнали з кінцевих точок, мережевих пристроїв і додатків. Агент Wazuh, запущений на контрольованій кінцевій точці, збирає і пересилає системні журнали і журнали додатків на сервер Wazuh для аналізу. Крім того, ви можете надсилати повідомлення журналів на сервер Wazuh за допомогою syslog або сторонніх API-інтеграцій.

Модуль Wazuh Vulnerability Detector допомагає користувачам виявляти вразливості в операційній системі та додатках, встановлених на кінцевих точках, за якими здійснюється моніторинг. Модуль працює за допомогою вбудованої інтеграції Wazuh із зовнішніми каналами вразливостей, індексованими Canonical, Debian, Red Hat, Arch Linux, Amazon Linux Advisories Security (ALAS), Microsoft та Національною базою даних вразливостей (NVD).

Можливості моніторингу команд Wazuh дозволяють відстежувати вивід певних команд і обробляти вивід як вміст журналу. Моніторинг команд можна використовувати для моніторингу різних речей, таких як використання дискового простору, середнє навантаження, зміна мережевих слухачів і запущених процесів, щоб переконатися, що всі важливі процеси запущені.

Моніторинг команд можна використовувати для виявлення різноманітних аномалій і загроз. Наприклад, можна відстежувати зміни у результатах виконання команди netstat, які вказують на те, що було додано або видалено нового мережевого слухача. Також можна відстежувати наявність певних рядків у виводі команди ps, що може свідчити про запуск шкідливого процесу.

Моніторинг політик - це процес перевірки відповідності всіх систем набору заздалегідь визначених правил щодо налаштувань конфігурації та дозволеного використання додатків.

Wazuh використовує три компоненти для виконання цього завдання: Rootcheck, OpenSCAP та CIS-CAT.

Також важливо зазначити, що Wazuh допомагає впроваджувати вимоги щодо відповідності нормативним вимогам для підтримки та прозорості. Це досягається за рахунок автоматизації, покращеного контролю безпеки, аналізу журналів та реагування на інциденти.

Набір правил Wazuh за замовчуванням забезпечує підтримку фреймворків і стандартів PCI DSS, HIPAA, NIST 800-53, TSC і GDPR. Правила та декодери Wazuh використовуються для виявлення атак, системних помилок, неправильних конфігурацій безпеки та порушень політик [16].

Завдяки своїм комплексним функціям, Wazuh забезпечує не тільки виявлення та реагування на загрози в реальному часі, але й виконує глибокий аналіз даних для прогнозування потенційних вразливостей і запобігання майбутнім інцидентам безпеки. Через моніторинг цілісності файлів, збір журналів, виявлення шкідливого програмного забезпечення та аналітику поведінки, Wazuh сприяє створенню міцного захисту для IT-інфраструктур організацій різного масштабу.

Особливе значення має здатність Wazuh адаптуватися до конкретних потреб організації, дозволяючи не лише виявляти вже відомі типи загроз, але й ефективно реагувати на нові, невідомі виклики. Ця адаптивність, у поєднанні з високою масштабованістю та гнучкістю в налаштуванні, робить Wazuh незамінним інструментом в арсеналі кібербезпеки сучасних організацій.

3. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ ТА ОПТИМІЗАЦІЇ WAZUH SIEM І XDR ДЛЯ ЗАХИСТУ ВІД ШКІДЛИВОГО ПЗ

3.1. Стратегії інтеграції Wazuh SIEM і XDR в інформаційні системи організацій

Wazuh - це платформа безпеки, яка забезпечує уніфікований захист XDR та SIEM для кінцевих точок та хмарних робочих навантажень. Рішення складається з єдиного універсального агента і трьох центральних компонентів: сервера Wazuh, індексатора Wazuh і інформаційної панелі Wazuh. Для отримання додаткової інформації ознайомтеся з документацією "Початок роботи".

Wazuh є безкоштовною програмою з відкритим кодом. Його компоненти поширюються на умовах Стандартної публічної ліцензії GNU, версія 2, та Ліцензії Apache, версія 2.0 (ALv2) [17].

Індексатор Wazuh і сервер Wazuh можуть бути встановлені на одному хості або розподілені в кластерних конфігураціях. Можна вибрати один з двох способів встановлення кожного центрального компонента Wazuh. Обидва варіанти містять інструкції щодо встановлення центральних компонентів на одному хості або на окремих хостах.

Користувач може ознайомитися з документацією по швидкому запуску, щоб виконати установку "все-в-одному". Це найшвидший спосіб підготувати центральні компоненти Wazuh до роботи.

Для більшої гнучкості розгортання та налаштування, необхідно встановити центральні компоненти Wazuh, почавши з розгортання індексатора Wazuh. Цей метод розгортання дозволяє встановити все-в-одному, а також встановити компоненти на окремих серверах.

На рис. 3.1. зображено робочий процес встановлення, якого користувач повинен буде дотримуватися.

Рис. 3.1. Процес встановлення компонентів [18]

Для корпоративних рішень важливе також встановлення Wazuh агента на кінцеві точки співробітників. Агент Wazuh - це єдине і легке програмне забезпечення для моніторингу. Це кросплатформенний компонент, який можна розгорнути на ноутбуках, настільних комп'ютерах, серверах, хмарних екземплярах, контейнерах або віртуальних машинах. Він забезпечує видимість безпеки кінцевої точки шляхом збору критично важливих системних і прикладних записів, даних інвентаризації та виявлення аномалій.

Якщо центральні компоненти Wazuh вже встановлені у корпоративному середовищі, то необхідно вибрати операційну систему для встановлення агенту і дотримуватися інструкцій по встановленню, щоб розгорнути агент на кінцевих точках.

Розглянемо детальніше процес встановлення необхідних компонентів. Центральні компоненти Wazuh можна встановити на 64-розрядну операційну систему Linux. Wazuh рекомендує будь-яку з наступних версій операційної системи: CentOS 7, 8; Ubuntu 16.04, 18.04, 20.04, 22.04; Red Hat Enterprise Linux 7, 8, 9; Amazon Linux 2. У випадку цієї роботи було обрано Ubuntu 22.04.

Для того, аби ініціювати процес установки, користувач або адміністратор системи може скористуватися системною утилітою curl

$$curl\ -sO\ https://packages.wazuh.com/4.7/wazuh-install.sh\ \&\&\ sudo\ bash\ ./wazuh-install.sh\ -a$$

Після цього ініціюється процес встановлення усіх необхідних пакетів для роботи рішення (рис. 3.2.)

Рис. 3.2. Процес встановлення усіх пакетів для функціювання рішення

Слідом необхідно відвідати вебсторінку та здійснити авторизацію, як адміністратор системи.

Рис. 3.3. Процес ідентифікації (введення імені адміністратора) та автентифікації (введення паролю)

Як тільки користувач здійснить успішний вхід до системи, йому буде надано доступ до дешбордів та подальших налаштувань рішення. Загальний вигляд стартової сторінки зображений на рис. 3.4.

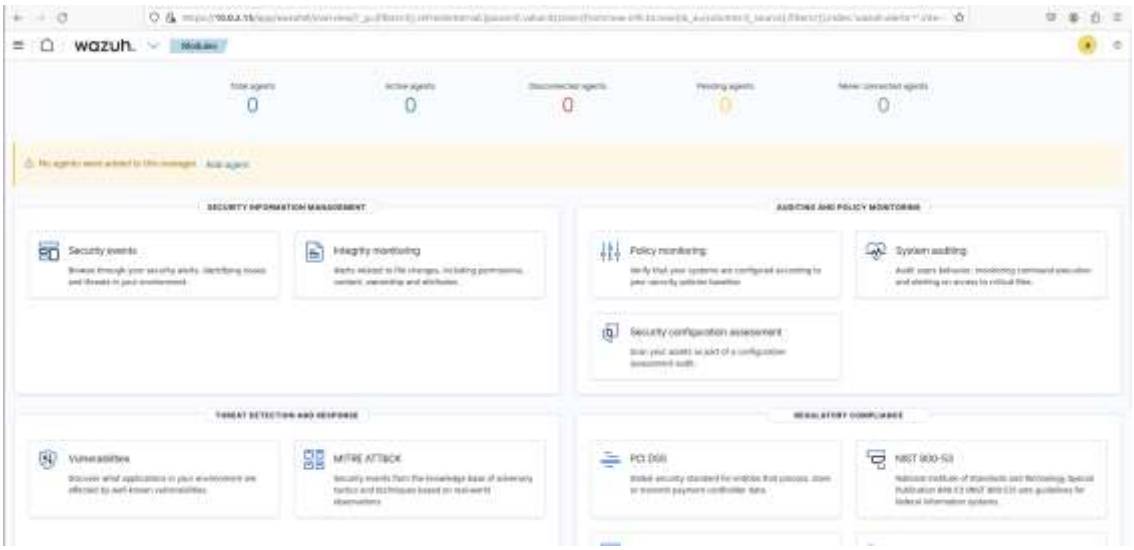

Рис. 3.4. Дешборд рішення Wazuh SIEM і XDR

Для початку роботи з рішенням необхідно підключити агенти. Агенти можуть бути кінцевими точками з операційними системами Windows, Linux і macOS. Для розгортання агенту необхідно здійснити налаштування на веб частині рішення: вказати IP адресу сервісу та додаткові налаштування (рис. 3.5).

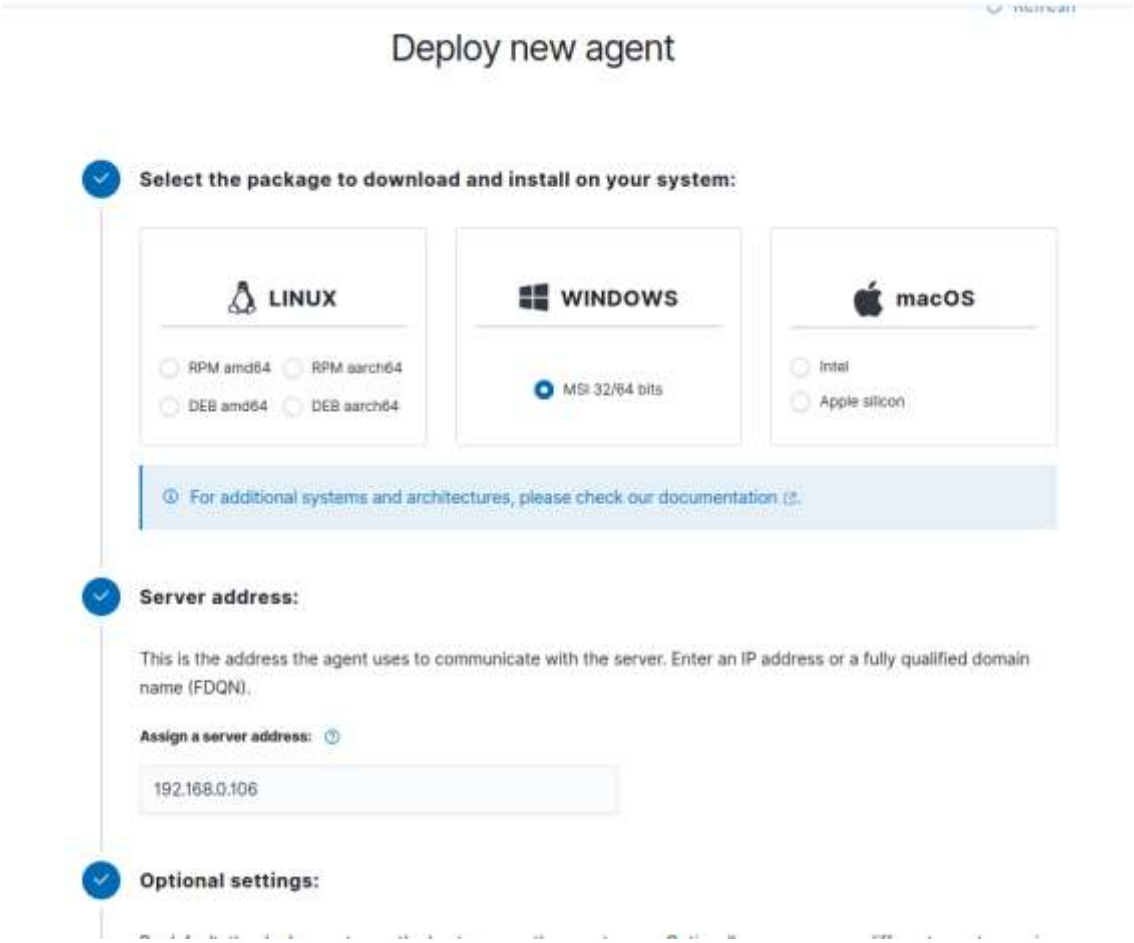

Рис. 3.5. Початок розгортання агенту

Слідом слід виконати налаштування на агентський частині, де розгорнутий сам Wazuh. Для цього слід використовувати наступну команду у середовищі PowerShell: Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.3-1.msi -OutFile ${env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='192.168.0.106' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='halychyna' WAZUH_REGISTRATION_SERVER='192.168.0.106'. Розглянемо складові цієї команди детальніше.

Invoke-WebRequest: Ця команда в PowerShell використовується для відправлення HTTP або HTTPS запитів до веб-сервера та отримання відповіді. Вона може використовуватися для завантаження файлів з інтернету.

-Uri: Параметр, що вказує URL, з якого потрібно завантажити файл. У цьому випадку, це URL до файлу інсталятора агента Wazuh версії 4.7.3 для Windows.

-OutFile: Вказує шлях і назву файлу, куди буде збережено завантажений файл. **${env.tmp}\wazuh-agent** вказує на те, що файл буде збережено у тимчасовій папці системи під назвою **wazuh-agent**.

msiexec.exe: Це виконувана програма, що використовується для встановлення, модифікації та видалення програм в форматі Windows Installer (.msi).

/i: Параметр команди **msiexec.exe**, що ініціює встановлення пакета.

${env.tmp}\wazuh-agent: Шлях до файлу інсталятора, який був завантажений.

/q: Параметр для **msiexec.exe**, що вказує на те, що інсталяція повинна виконуватися у тихому режимі без відображення інтерфейсу користувача.

WAZUH_MANAGER='192.168.0.106': Вказує IP-адресу або ім'я сервера Wazuh, до якого буде підключатися агент.

WAZUH_AGENT_GROUP='default': Встановлює групу, до якої належатиме агент. У цьому випадку, це стандартна група 'default'.

WAZUH_AGENT_NAME='halychyna': Встановлює ім'я для агента Wazuh.

WAZUH_REGISTRATION_SERVER='192.168.0.106': Вказує сервер реєстрації для агента.

Після виконаних дій, можна запустити агентську програму Wazuh, яка забезпечує моніторинг та звітування стану безпеки системи. Запускаючи цю команду, активується служба Wazuh, що дозволяє агенту почати свою роботу на машині, збираючи дані безпеки та відправляючи їх на сервер Wazuh для аналізу.

NET START WazuhSvc

У разі успішно проведених налаштувань, повинен з’явитися запис, що сповіщатиме про вдалий старт служби.

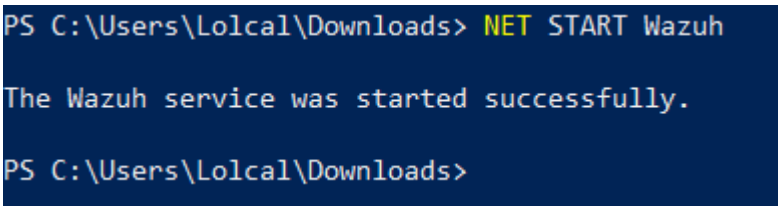

Рис. 3.6. Вдалий старт Wazuh

Тепер необхідно ініціювати старт збору інформації про агент за допомогою інтерфейсу користувача. Для цього необхідно і достатньо ввести IP менеджера та, за наявності, автентифікаційний ключ.

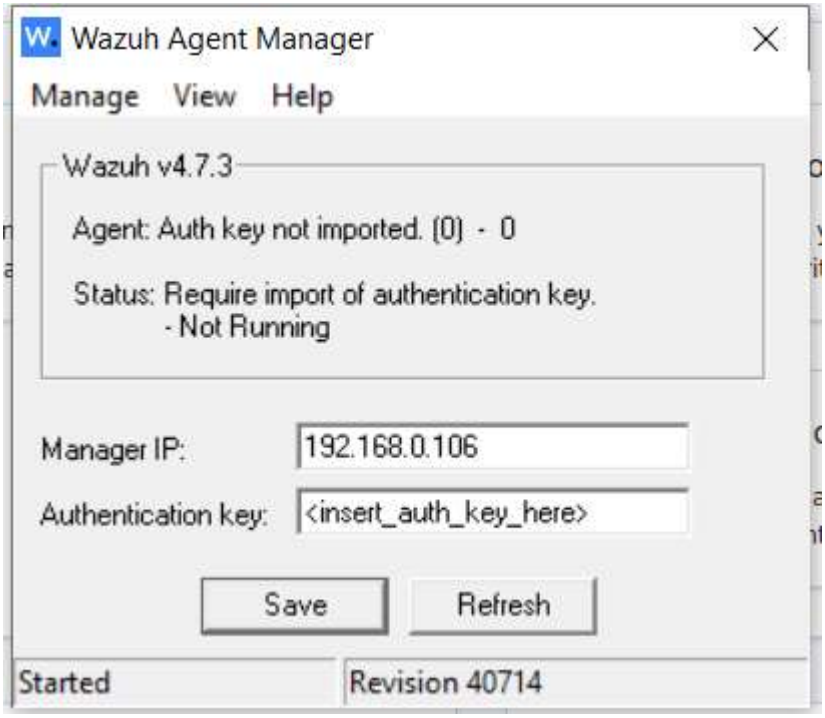

Рис. 3.7. Прикінцеві налаштування підключення агенту Wazuh

У разі вдалого підключення, агент повинен відображатись на дешборді менеджера, як показано на рис. 3.8.

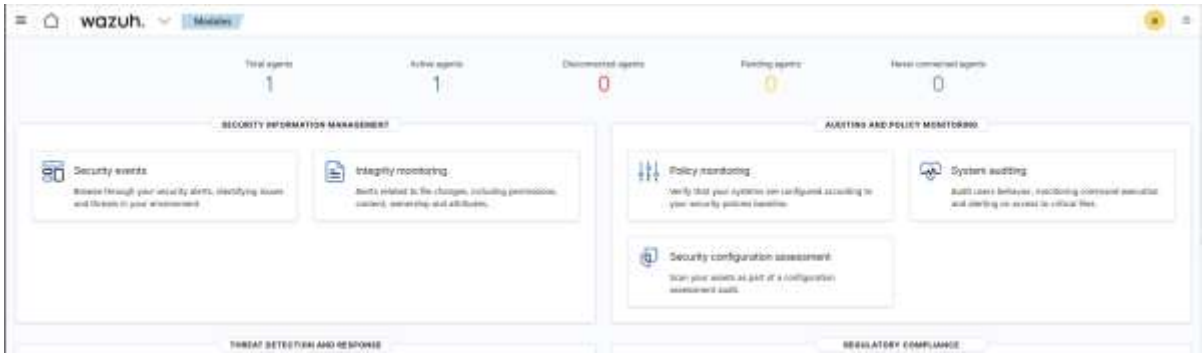

Рис. 3.8. Агент на дешборді менеджера

Після вдалого налаштування можна також переглянути детальнішу інформацію про агента.

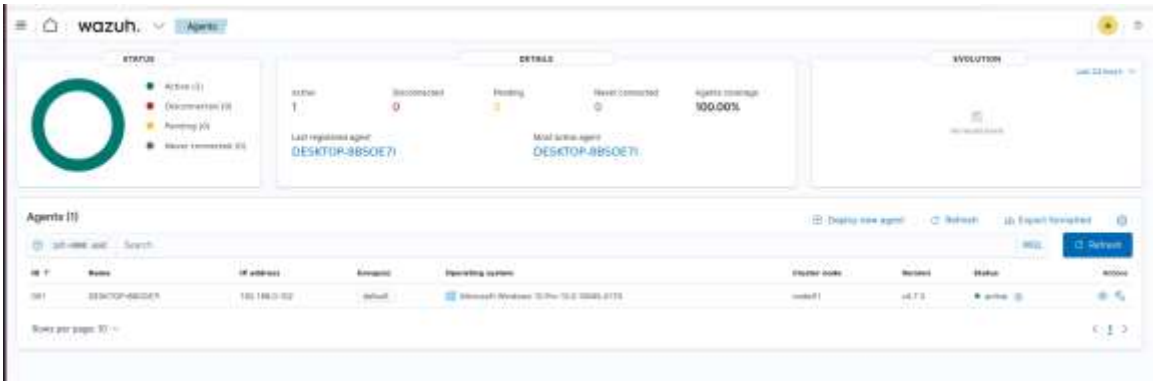

Рис. 3.9. Перегляд інформації про підключений агент

Основні категорії даних, які доступні для перегляду:

Статус агента: перевірка, чи активний агент, чи він в офлайні, а також час останнього зв'язку з сервером.

Конфігурація агента: деталі конфігурації, включаючи налаштування, пов'язані з безпекою, моніторингом цілісності, логами та іншими параметрами.

Інформація про ОС: версія та інші характеристики операційної системи, на якій працює агент.

Мережева інформація: IP-адреси, маска мережі, інформація про шлюзи та інші мережеві параметри.

Зареєстровані події: події, зареєстровані агентом, які могли б включати спроби входу, помилки, підозрілі дії та інше.

Сповіщення безпеки: сповіщення, генеровані на основі аналізу подій, що можуть вказувати на потенційні загрози або вразливості.

Виявлені вразливості: інформація про будь-які виявлені вразливості в системах або програмах, встановлених на агенті.

Інтегральність файлів: результати моніторингу цілісності файлів, включаючи зміни в критичних файлах або каталогах.

Історія змін конфігурації: записи про будь-які зміни в конфігурації агента або системи, які можуть вплинути на безпеку.

Процеси та сервіси: інформація про активні процеси та сервіси на агенті.

Ця інформація доступна через інтерфейс користувача Wazuh або може бути отримана через API для детального аналізу та інтеграції з іншими системами моніторингу та управління безпекою. Вона допомагає адміністраторам та командам з кібербезпеки ефективно відстежувати стан і поведінку агентів, швидко реагувати на інциденти та вдосконалювати загальну безпеку організації.

Завдяки модульності та гнучкості Wazuh, організації можуть ефективно розгортати центральні компоненти та агенти, оптимізуючи їх для різних операційних середовищ та вимог безпеки. Окрема увага до різних варіантів встановлення та налаштування дозволяє адаптувати систему для конкретних потреб кожної організації, забезпечуючи при цьому високий рівень захисту та ефективність реагування на загрози.

Інтеграція Wazuh вже встановлених корпоративних інфраструктур, а також налаштування агентів на кінцевих точках, забезпечують комплексний захист даних і ресурсів організації. Це включає моніторинг цілісності системи, збір логів, аналіз поведінки та навіть виявлення аномалій, що сприяє ранньому виявленню потенційних загроз і зменшенню ризику їх впливу на діяльність організації.

Загалом, впровадження Wazuh SIEM і XDR дає можливість не тільки реагувати на інциденти, але й активно передбачати потенційні загрози, використовуючи дані та аналітику для постійного покращення систем безпеки. Це,

у свою чергу, сприяє зміцненню загальної обороноздатності інформаційних систем і підвищенню рівня довіри стейкхолдерів до організації.

3.2. Моніторинг, логування та аналіз даних для виявлення шкідливого ПЗ

Системи логування і моніторингу є одними з ключових аспектів кіберзахисту організацій, оскільки вони дозволяють не тільки фіксувати дії в системі, але й аналізувати ці дані для виявлення аномалій, які можуть вказувати на наявність або спробу інфікування шкідливим ПЗ чи реалізацію будь-яких зловмисних подій. Це включає в себе все: від простого моніторингу доступу до файлів і використання мережевих ресурсів до складних аналітичних процедур на основі машинного навчання, які можуть розпізнавати складні шаблони поведінки, характерні для шкідливих атак.

Методи логування даних часто включають збір інформації з різних джерел, таких як серверні журнали, журнали подій, системні журнали операційних систем, мережеві журнали та багато інших. Ефективне ведення журналів допомагає організаціям зберігати важливі докази діяльності системи, які можуть бути використані для пост-інцидентного аналізу та розслідувань у разі кібератак.

Аналіз зібраних даних здійснюється за допомогою різноманітних аналітичних інструментів, у випадку Wazuh це модуль SIEM-системи. Цей інструмент обробляє великі обсяги даних в реальному часі, що дозволяє виявляти незвичайні або підозрілі відхилення, які можуть свідчити про спроби злому або проникнення шкідливого ПЗ.

В Wazuh перегляд інцидентів та подій, що відбулися у системі, зазвичай здійснюється через інформаційну панель (dashboard) у Wazuh Kibana plugin. Цей інструмент інтегрований з Elastic Stack, зокрема з Kibana, що дозволяє користувачам візуалізувати і аналізувати дані в режимі реального часу (рис. 3.10.).

Рис. 3.10. Перегляд інцидентів та подій, що відбулися у системі

Інформаційна панель Wazuh надає зручний і інтуїтивно зрозумілий інтерфейс для візуалізації подій та інцидентів, що відбуваються в мережі організації. Це включає графіки, табличні представлення та інші візуальні елементи, які допомагають швидко оцінювати стан системи. Так, наприклад, на рис. 3.11. зображено часову шкалу подій, де за часом можна проглянути інтенсивність усіх подій, що відбувалися у системі протягом деякого періоду часу.

Рис. 3.11. Часова шкала подій

Як згадувалося раніше, логування подій у Wazuh дозволяє організаціям збирати, зберігати і аналізувати дані про події в їхніх системах, що є ключем до ідентифікації та усунення потенційних загроз. Основні компоненти логування включають Wazuh Manager і Wazuh Agents.

Wazuh Manager є центральним вузлом системи, що виконує аналіз подій, отриманих від агентів. Він обладнаний спеціалізованими декодерами, які

розшифровують вхідні логи, визначаючи формати і протоколи для детального аналізу вмісту. Аналізатор подій фільтрує ці дані через різноманітні правила, щоб виявити відхилення або підозрілу поведінку, генеруючи сповіщення для подальших дій.

Wazuh Agents, розгорнуті на кінцевих точках, виконують локальний моніторинг активності, збираючи логи з операційних систем, застосунків та інших джерел. Ці дані пересилаються до Wazuh Manager, де вони аналізуються та обробляються. Агенти можуть також виконувати моніторинг цілісності файлів та використовувати різноманітні модулі для виявлення змін у системі або несанкціонованих змін у файлах.

Для ефективного логування та моніторингу, Wazuh використовує різноманітні методи збору логів, включаючи активний збір (агенти активно збирають та пересилають логи) та пасивний збір (агенти чи системи пересилають логи за допомогою syslog або інших механізмів на сервер). Комбінація цих методів забезпечує комплексний огляд стану системи, дозволяючи адміністраторам швидко реагувати на інциденти і адаптувати захисні стратегії відповідно до поточного безпекового ландшафту.

Детальний огляд лог-файлу деякої події можна побачити на рис. 3.12. У цьому розділі можна проглянути найважливіші елементи, що стосуються події, такі як, наприклад, ідентифікаційні дані, процеси, час і дату, де відбулась подія, який характер виконуваних дій та ін. Важливо звернути увагу на кожен з цих аспектів, оскільки вони можуть допомогти виявити причини і наслідки події, а також оцінити її вплив на систему в цілому. Крім того, лог-файли можуть містити додаткову інформацію, таку як рівень привілеїв, під якими були виконані дії, та статус завершення процесів. Аналізуючи ці дані, можна більш точно визначити джерело і природу події, а також розробити стратегії для запобігання подібним випадкам у майбутньому.

Рис. 3.12. Детальна інформація про подію у журналі подій

Додатково Wazuh допомагає впроваджувати вимоги щодо відповідності нормативним вимогам для підтримки та наочності дотримання нормативних вимог. Це досягається за рахунок автоматизації, покращеного контролю безпеки, аналізу журналів та реагування на інциденти. Так, до прикладу, рішення містить функціонал автоматичного сканування кінцевих точок за бенчмарком CIS, що є однією із найпоширеніших методик оцінювання вразливостей у системі. Така оцінка допоможе сформувати звіт, у якому буде детально проаналізовано компоненти захисту системи та надано практичні рекомендації щодо підвищення рівня захищеності системи (рис. 3.13).

Рис. 3.13. Оцінка CIS Benchmark у середовищі Wazuh SIEM і XDR

Набір правил Wazuh за замовчуванням включає підтримку широкого спектру міжнародно визнаних фреймворків і стандартів забезпечення безпеки, таких як PCI DSS, HIPAA, NIST 800-53, TSC і GDPR. Це забезпечує організаціям засоби для дотримання вимог регулювання безпеки даних і зменшує ризики пов’язані з втратою даних та іншими безпековими інцидентами. Ці правила допомагають в автоматизації процесів моніторингу та реагування на загрози, виявленні порушень політик безпеки, та забезпеченні відповідності до актуальних законодавчих та галузевих вимог. Використання цих правил у Wazuh дозволяє компаніям значно підвищити рівень внутрішньої та зовнішньої безпеки, мінімізувати вразливості та оптимізувати процеси відповідності (рис. 3.14). Правила та декодери Wazuh використовуються для виявлення атак, системних помилок, неправильних конфігурацій безпеки та порушень політик.

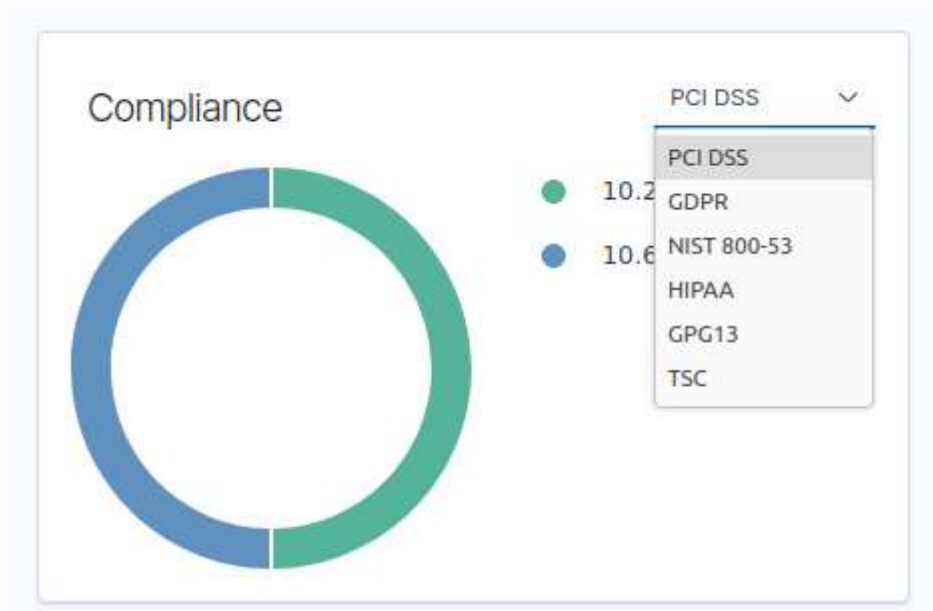

Рис. 3.14. Перевірка на відповідність одного із функціонуючих агентів вимогам міжнародних стандартів

Системи логування та моніторингу відіграють фундаментальну роль у забезпеченні кібербезпеки організацій, дозволяючи не лише фіксувати дії в системі, але й аналізувати ці дані для виявлення потенційних аномалій та зловмисних дій. Завдяки збору інформації з різноманітних джерел та використанню складних аналітичних інструментів, таких як Wazuh SIEM, організації можуть ефективно

реагувати на інциденти та виявляти шкідливі втручання до того, як вони спричинять значну шкоду. Wazuh забезпечує не тільки комплексний моніторинг стану систем, але й допомагає забезпечувати відповідність регулятивним вимогам, підтримуючи безпеку інформаційних активів на високому рівні.

3.3. Рекомендації щодо застосування методів та засобів виявлення шкідливого програмного забезпечення

Ефективне виявлення та протидія шкідливому програмному забезпеченню вимагає від організацій не тільки вибору адекватних технологій, але й розуміння стратегічних і тактичних аспектів їх впровадження в існуючі IT-інфраструктури.

Важливо визнати, що немає універсального рішення для всіх типів організацій або всіх видів загроз. Вибір інструментів та методик повинен базуватися на специфічних потребах безпеки, ресурсах, якими диспонує організація, та особливостях її інформаційних систем. Розглянемо стратегічний підхід до вибору і оптимізації інструментів виявлення шкідливого програмного забезпечення, що дозволить максимально збільшити ефективність захисних механізмів та мінімізувати ризики для інформаційних активів організації.

Для забезпечення комплексного захисту інформаційної системи, необхідно впровадити глибокий та всебічний моніторинг мережі. Цей підхід передбачає збір даних з різних точок доступу та вузлів мережі, що дозволяє отримати повне уявлення про мережеву активність. Використання систем SIEM, на кшталт Wazuh, забезпечує ефективний аналіз зібраних даних, виявлення аномалій та вчасне реагування на потенційні загрози. Аналітичні здібності таких систем дозволяють виявляти та класифікувати загрози на основі поведінкових шаблонів, забезпечуючи високий рівень безпеки. Реальний час обробки інформації критично важливий для оперативного виявлення та нейтралізації кібератак, що робить системи SIEM незамінним інструментом у стратегії кібербезпеки організації.

Для зміцнення кібербезпеки та підвищення ефективності виявлення та реагування на шкідливе програмне забезпечення, критично важливим є інтеграція

Wazuh з ширшим спектром інструментів безпеки. Зокрема, інтеграція з міжмережевими екранами та системами запобігання вторгненням (IPS) забезпечує додатковий рівень моніторингу та захисту, дозволяючи виявляти та блокувати потенційно зловмисні спроби до того, як вони досягнуть критичних активів. Антивірусне програмне забезпечення, що працює разом з Wazuh, може допомогти в ідентифікації та нейтралізації відомих видів шкідливих програм на ранніх етапах їхнього проникнення. Така інтеграція не тільки підвищує загальну здатність до виявлення загроз, але й забезпечує більш широкий огляд захищеності інформаційних систем, дозволяючи розробити більш ефективні стратегії реагування на інциденти. Отже, застосування цього комплексного підходу є ключем до підвищення рівня захисту організації від сучасних кіберзагроз.

Оновлення та адаптація бази правил Wazuh до поточного ландшафту кіберзагроз є вирішальними діями для забезпечення надійного виявлення та протидії сучасним загрозам. Регулярне оновлення сигнатур вірусів та інших відомих індикаторів компрометації є фундаментальним для підтримки ефективності Wazuh у боротьбі з найновішими шкідливими програмами та вірусами. Важливим є також аналіз поведінкових патернів користувачів та систем, який дозволяє ідентифікувати аномалії, що можуть свідчити про несанкціоновані дії або спроби вторгнення. Адаптація правил та моніторингових процедур до еволюції тактик кіберзлочинців дозволяє не тільки реагувати на поточні загрози, але й проактивно протидіяти потенційним майбутнім атакам. Така багаторівнева стратегія оновлення та адаптації забезпечує, що система безпеки залишається респонсивною та ефективною у швидкозмінному цифровому світі.

Навчання персоналу користуванню системами SIEM та XDR є критично важливим для забезпечення ефективного моніторингу та реагування на інциденти безпеки в організації. Освітні програми мають зосереджуватися на роз'ясненні функціональності цих інструментів, методиках виявлення аномалій та оптимальних стратегіях для швидкого реагування. Розробка чітких і деталізованих процедур реагування на інциденти дозволить скоротити час відклику та ефективно управляти наслідками кібератак. Такі процедури повинні включати кроки для

ідентифікації, оцінки та ліквідації вразливостей, а також забезпечувати збереження доказів для подальшого аналізу та відповідності законодавчим вимогам. Належне навчання та чіткі процедури реагування не тільки підвищують безпеку інформаційних активів, але й підсилюють довіру до інформаційної безпеки в організації.

У цьому розділі ми розглянули стратегії та рекомендації щодо використання систем SIEM та XDR для ефективного моніторингу та виявлення шкідливого програмного забезпечення у корпоративних інформаційних системах. Було підкреслено важливість глибокого моніторингу мережі з використанням Wazuh, який забезпечує аналіз поведінкових шаблонів та виявлення загроз в реальному часі. Також наголошується на інтеграції Wazuh з іншими захисними інструментами, такими як міжмережеві екрани та антивірусні програми, для створення комплексного бар'єру проти кіберзагроз. Важливим аспектом є оновлення та налаштування правил Wazuh для відповідності новітнім кіберзагрозам через періодичне оновлення сигнатур та адаптацію до нових кіберзлочинних стратегій. Навчання персоналу та розробка чітких процедур реагування на інциденти безпеки мають вирішальне значення для зниження часу відклику та мінімізації збитків від можливих інцидентів. Збір та аналіз даних через логування подій дозволяє зберігати важливі докази діяльності системи, що є ключем до ефективного реагування на інциденти та пост-інцидентний аналіз. Впровадження цих рекомендацій дозволить організаціям підвищити рівень безпеки, ефективно ідентифікувати та відповідати на кіберзагрози, забезпечуючи захист критично важливих інформаційних ресурсів.

ВИСНОВКИ

У роботі було проведено всебічне дослідження шляхів виявлення шкідливого програмного забезпечення та розроблено рекомендації щодо його нейтралізації на прикладі платформ Wazuh SIEM і XDR. Дослідження охоплювало кілька ключових аспектів, що сприяли розумінню ефективності та функціональності сучасних систем моніторингу та реагування на інциденти.

Спочатку було виконано аналіз актуальності проблеми виявлення шкідливого програмного забезпечення. Було показано, що в сучасному світі цифрових технологій обсяг кіберзагроз постійно зростає, що робить необхідним впровадження надійних і ефективних засобів захисту. Шкідливе програмне забезпечення може завдати значної шкоди як окремим користувачам, так і організаціям в цілому, спричиняючи фінансові втрати, викрадення конфіденційних даних та порушення нормального функціонування інформаційних систем.

У рамках роботи було здійснено детальний огляд існуючих рішень для виявлення шкідливого програмного забезпечення. Особливу увагу було приділено аналізу платформ Wazuh SIEM і XDR, які забезпечують комплексний моніторинг та аналіз безпекових подій. Було розглянуто архітектуру, функціональні можливості та модулі цих платформ, що дозволило виявити їх ключові переваги та обмеження.

На основі проведеного аналізу було розроблено комплекс рекомендацій щодо оптимального використання платформ Wazuh SIEM і XDR для ефективного виявлення та реагування на шкідливе програмне забезпечення. Зокрема, було розроблено стратегії інтеграції цих рішень у інформаційні системи організацій, а також рекомендації щодо моніторингу логування та аналізу даних. Було акцентовано увагу на необхідності навчання персоналу та розробці ефективних процедур реагування на інциденти.

Практичне значення одержаних результатів полягає в тому, що розроблені рекомендації можуть бути використані організаціями для покращення своєї кібербезпеки. Впровадження платформ Wazuh SIEM і XDR дозволяє не лише

ефективно виявляти відомі види шкідливого ПЗ, але й ідентифікувати нові, раніше невідомі загрози завдяки постійному аналізу поведінкових патернів та аномалій в системах.

Таким чином, проведене дослідження та розроблені рекомендації роблять важливий внесок у забезпечення захисту інформаційних систем від сучасних кіберзагроз. Вони сприяють зміцненню кібербезпеки на рівні окремих організацій, а також забезпечують важливий внесок у загальну стабільність і безпеку інформаційного простору на національному та міжнародному рівнях. Реалізація запропонованих заходів дозволить мінімізувати ризики, пов'язані з шкідливим програмним забезпеченням, та підвищити загальний рівень кіберзахисту.

ПЕРЕЛІК ПОСИЛАНЬ

1. +65 Malware Statistics for 2024. StationX. URL: https://www.stationx.net/malware-statistics/#:~:text=Malware%20Attack%20Rates&text=In%202022,%20there%20were%205.5,(10.5%20billion%20attacks%20globally). (date of access: 10.03.2024).

2. Punjwani M., Campbell S. Cybersecurity statistics in 2024. https://www.usatoday.com/money/blueprint/business/vpn/cybersecurity-statistics/. URL: https://www.usatoday.com/money/blueprint/business/vpn/cybersecurity-statistics/ (date of access: 12.03.2024).

3. Fleck A. Cybercrime Expected To Skyrocket in Coming Years. URL: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/ (date of access: 13.03.2024).

4. Most Common Malware Attacks. Arctic Wolf. URL: https://arcticwolf.com/resources/blog/8-types-of-malware/ (date of access: 13.03.2024).

5. 12 Types of Malware + Examples That You Should Know. URL: https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/ (date of access: 13.03.2024).

6. ESET Leader in G2 summer report for ESET PROTECT Advanced. URL: https://www.eset.com/us/about/newsroom/press-releases/eset-leader-in-g2-summer-report-for-eset-protect-advanced-3/ (date of access: 14.03.2024).

7. ESET Protect Entry - багаторівневий захист для бізнесу | ESET. ESET. URL: https://www.eset.com/ua/business/entry-protection/ (дата звернення: 08.05.2024).

8. FortiSIEM Ratings Overview. URL: https://www.gartner.com/reviews/market/security-information-event-management/vendor/fortinet/product/fortisiem (date of access: 20.03.2024).

9. SIEM Solutions & Tools | Get Best Enterprise SIEM Software | FortiSIEM. Fortinet. URL: https://www.fortinet.com/products/siem/fortisiem (date of access: 20.03.2024).

10. Wazuh information. URL: https://wazuh.com/ (date of access: 26.03.2024).

11. What is SIEM?. URL: https://www.ibm.com/topics/siem#:~:text=SIEM%20solutions%20allow%20organizations%20to,implement%20more%20effective%20security%20processes. (date of access: 26.03.2024).

12. Zawalnyski A. The Top XDR Solutions | Expert Insights. Expert Insights. URL: https://expertinsights.com/insights/the-top-xdr-solutions/ (date of access: 27.03.2024).

13. 2020 State of SecOps and Automation. URL: https://assets-www.sumologic.com/resources/brief/2020_State_of_SecOps_and_Automation.pdf (date of access: 03.04.2024).

14. Architecture. Wazuh. URL: https://documentation.wazuh.com/current/getting-started/architecture.html (date of access: 08.04.2024).

15. Capabilities - User manual | Wazuh documentation. Wazuh. URL: https://documentation.wazuh.com/current/user-manual/capabilities/index.html (date of access: 08.04.2024).

16. Regulatory compliance | Wazuh documentation. Wazuh. URL: https://documentation.wazuh.com/current/compliance/index.html (date of access: 15.04.2024).

17. Installation guide | Wazuh documentation. Wazuh. URL: https://documentation.wazuh.com/current/installation-guide/index.html (date of access: 22.04.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)