ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління захистом кінцевих точок організації на базі рішення Wazuh»

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

_____ Денис ГАРКУША
(підпис)

Виконав: здобувач(ка) вищої освіти групи БСДМ-62
ГАРКУША Денис
(прізвище, ім'я)

Керівник д.т.н., проф. КОЖУХІВСЬКИЙ Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

API – Application Programming Interface

APT – Advanced Persistent Threat

CDN – Content Delivery Network

DDoS – Distributed Denial of Service

DNS – Domain Name System

EDR – Endpoint Detection and Response

IaaS – Infrastructure as a Service

IAM – Identity and Access Management

HIDS – Host-based Intrusion Detection System

MSSP – Managed Security Service Provider

WAAP – Web Application and API protection

SOC – Security Operations Center

OWASP – Open Web Application Security Project

XDR – Extended Detection and Response

ВСТУП

Актуальність дослідження. Кожен пристрій, який співробітники використовують для підключення до корпоративних мереж, представляє потенційний ризик, який зловмисники можуть використовувати для викрадення корпоративних даних. Ці пристрої або кінцеві точки поширюються, що ускладнює завдання їх захисту. Тому для організацій життєво важливо розгортати інструменти та рішення, які захищають передову лінію кібербезпеки. Технологія безпеки кінцевих точок відіграє життєво важливу роль у захисті організацій від загроз, що стають все більш небезпечними.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження технології захисту кінцевих точок організації на базі Wazuh.

Об'єкт дослідження – захист кінцевих точок організації.

Предмет дослідження – технологія захисту кінцевих точок організації на базі Wazuh.

Мета роботи – розробити порядок застосування технології захисту кінцевих точок організації на базі Wazuh та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми захисту кінцевих точок організації;

проаналізувати підходи до захисту кінцевих точок організації;

проаналізувати існуючі рішення для захисту кінцевих точок організації;

проаналізувати методи та засоби захисту кінцевих точок організації на базі Wazuh;

розкрити порядок реалізації технології захисту кінцевих точок організації на базі Wazuh.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології захисту кінцевих точок організації на базі Wazuh, а також

розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

1.1. Дослідження проблеми захисту кінцевих точок організації

Cisco у Звіті 2024 року [1] відмічає, що сьогоднішній ландшафт загроз складніший, ніж будь-коли, і організаціям важко втриматися. Мільярди користувачів, пристроїв і пристроїв Інтернету речей підключаються до корпоративних мереж, хмарних додатків і даних у такому масштабі, якого ми не бачили в минулому.

У той же час компанії стикаються зі складним і різноманітним ландшафтом загроз, які виходять за рамки програм-вимагачів і фішингу. Лише за минулий рік багато хто також зіткнувся з підкиданням облікових даних, атаками на ланцюжки поставок, соціальною інженерією та криптоджекінгом. Суб’єкти кіберзагроз часто використовували старі вразливості програмного забезпечення в звичайних програмах [1].

У всьому світі ландшафт загроз кібербезпеці продовжує швидко розвиватися та залишається складним: більше половини організацій (54%) стикалися з інцидентом кібербезпеки минулого року, а три чверті (73%) усіх організацій вважають, що вони, ймовірно, бути порушені інцидентом кібербезпеки протягом наступних 12-24 місяців [1].

Ключова тенденція, яку підкреслив Звіт Cisco [1], полягає в тому, що сьогодні компанії бачать зовнішніх гравців як більшу загрозу, ніж внутрішніх. Серед опитаних 62% підкреслили, що зовнішні актори є для них найбільшою загрозою, тоді як лише 31% сказали те саме щодо внутрішніх акторів. Це помітний зсув у порівнянні з 2023 роком, коли обидві вважалися майже однаковими загрозами. Одним із ключових факторів такого повороту може бути той факт, що загрози кібербезпеці з боку зовнішніх гравців стають дедалі витонченішими.

Незважаючи на те, що шкідливе програмне забезпечення (76%) і фішинг (54%) залишаються найпопулярнішими типами атак, 37% компаній постраждали від підміни облікових даних, 32% мали атаки на ланцюг поставок і соціальну інженерію, а 27% сказали, що зазнали інцидентів криптозлому в минулому році (рисунок 1.1) [1].

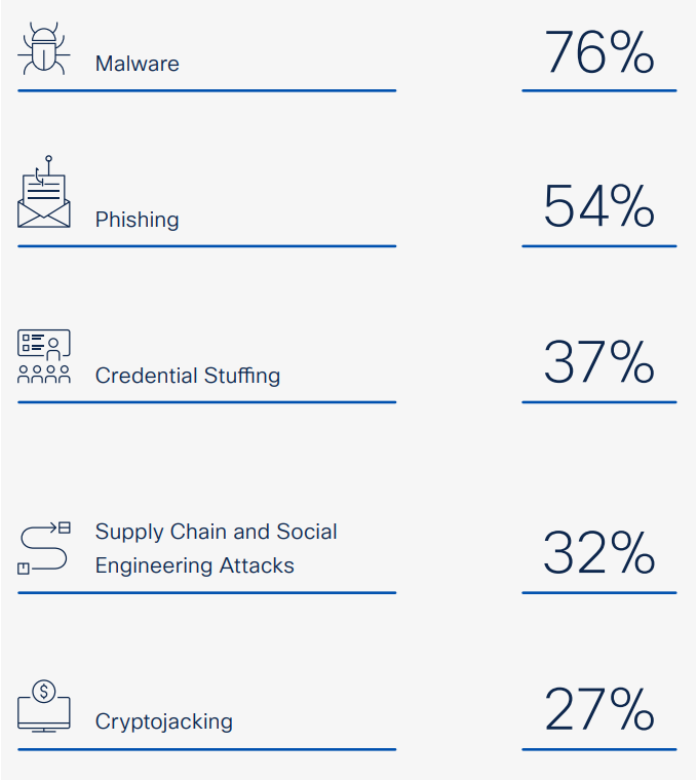


Рис.1.1. Співвідношення типів атак, які зазнають компанії [1]

Проблеми для організацій стають ще більшими, оскільки світ гібридної роботи продовжує додавати ще один рівень складності до ландшафту загроз. Індекс показує, що 91% співробітників в організаціях використовують кілька мереж для підключення до роботи. Фактично, майже кожен третій (29%) співробітник щотижня переходить принаймні між шістьма мережами. 85% організацій стверджують, що їхні співробітники отримують доступ до платформ компанії з некерованих пристроїв, а 43% цих співробітників повідомляють, що вони витрачають 20% свого часу на мережу компанії з таких пристроїв [1].

Фінансовий вплив цих інцидентів є значним. Серед тих, хто постраждав від інциденту минулого року, більше половини (52%) сказали, що це коштувало їхній організації щонайменше 300 000 доларів США, тоді як 12% сказали, що наслідки

становили 1 мільйон доларів США або більше. Цікавою тенденцією, яка виділялася, був той факт, що більшість компаній, які мали вплив на 1 мільйон доларів США або більше, були тими, які мають річний дохід понад 100 мільйонів доларів США. З іншого боку, більшість тих, хто сказав, що вплив склав менше 200 000 доларів США, були компаніями з річним доходом менше 2 мільйонів доларів США. Виходячи з цих відповідей, загальний фінансовий вплив компаній, які минулого року постраждали від інциденту кібербезпеки, склав близько 3,38 мільярда доларів США [1].

Cisco у Звіті 2024 року [1] відмічає, що кожен підключений пристрій є потенційною точкою входу для зловмисників, які можуть проникнути в мережу організації. Продовжують відбуватися значні витоки даних через доступ через незахищені пристрої.

Отже, незалежно від того, який тип пристрою підключається до мережі, його потрібно захистити. Щоб зробити це ефективно, організації повинні підтвердити цілісність пристрою, який збирається підключити, і мати вбудовані засоби захисту кінцевої точки. Це дозволить їм віддалено керувати пристроєм і виявляти будь-які аномалії в тому, як цей пристрій поводиться в реальному часі.

З цього приводу у Звіті Cisco за 2024 року [1] зазначається, що майже дві третини (63%) респондентів обрали використання вбудованих рішень, таких як брандмауери на основі хоста та IPS, як ключові рішення для захисту машин. Організації визнають привілейоване становище базової системи введення/виведення (BIOS) при ініціалізації операційних систем і пов’язаних з ними вразливостей, причому 57% розгортають рішення в цій області. Інструменти поведінки машини та захисту від аномалій також виявилися цінними в арсеналі компанії для захисту від машинних загроз 47% розгорнули це рішення.

Існує ймовірність того, що в деяких галузях промисловості може навіть існувати припущення, що атака на пристрій не є найприбутковішою справою для зловмисників – це лише засіб переслідувати особу та мережу.

Отже, проблеми захисту кінцевих точок організацій є надзвичайно актуальними в сучасному цифровому світі, де кіберзагрози стають все більш

витонченими та поширеними. Кінцеві точки (наприклад, комп'ютери, смартфони, планшети) є вразливими місцями в мережі будь-якої організації, оскільки через них зловмисники можуть отримати доступ до конфіденційних даних, порушити роботу систем та завдати значних фінансових збитків.

Основними проблемами захисту кінцевих точок організацій є:

різноманітність пристроїв. Сучасні організації використовують широкий спектр пристроїв, що ускладнює управління їхньою безпекою;

мобільні пристрої та пристрої Інтернету речей. Поширення мобільних пристроїв створює додаткові ризики, оскільки вони часто підключаються до різних мереж і можуть бути легко втрачені або вкрадені;

віддалена робота співробітників. Зростання популярності віддаленої роботи збільшує площу атаки, оскільки пристрої співробітників підключаються до корпоративної мережі з різних місць;

складні атаки на інформаційні ресурси організацій. Зловмисники використовують все більш складні методи атак, такі як фішинг, соціальна інженерія та безфайлові атаки, які важко виявити традиційними засобами захисту;

людський фактор. Помилки співробітників, такі як клікання на підозрілі посилання або використання слабких паролів, залишаються однією з основних причин кібератак;

швидке поширення загроз. Нові загрози з’являються щодня, і традиційні антивіруси часто не встигають за ними;

недостатні ресурси. Не всі організації мають достатні ресурси для впровадження ефективних систем захисту кінцевих точок.

Необхідно відмітити, що кібератаки можуть призвести до значних фінансових збитків через втрату даних, викуп, репутаційні ризики та простої у роботі. Також витік конфіденційних даних може серйозно підірвати довіру клієнтів та партнерів. Тому, передові країни приймають все більш суворі закони щодо захисту даних, що покладають на організації додаткову відповідальність. Також, зростання геополітичної напруженості призводить до збільшення кількості цілеспрямованих кібератак.

Для ефективного захисту кінцевих точок організації необхідно застосовувати комплексний підхід, який включає:

впровадження систем виявлення та реагування на інциденти (Endpoint Detection and Response, EDR). EDR дозволяє виявляти і досліджувати підозрілу активність на кінцевих точках;

регулярне оновлення програмного забезпечення. Своєчасне встановлення патчів усуває вразливості, які можуть бути використані зловмисниками;

навчання співробітників. Співробітники повинні бути поінформовані про основні загрози кібербезпеки та правила безпечної роботи в Інтернеті;

багатофакторна автентифікація. Багатофакторна автентифікація значно ускладнює несанкціонований доступ до облікових записів;

резервне копіювання даних. Регулярне резервне копіювання даних дозволяє відновити їх у разі втрати або пошкодження;

політика безпеки. Розробка та дотримання чіткої політики безпеки є важливим елементом захисту кінцевих точок.

Отже, захист кінцевих точок є однією з найважливіших задач для будь-якої організації. Зростання кіберзагроз вимагає від компаній постійно вдосконалювати свої системи безпеки та адаптуватися до нових викликів.

1.2. Аналіз підходів до виявлення загроз кінцевим точкам організації та реагування на них

Microsoft зазначає [2], що підприємства дедалі частіше працюють у багатохмарних і гібридних середовищах, де вони стикаються з мінливою системою кіберзагроз і складними проблемами безпеки. На відміну від цільових систем, таких як виявлення та реагування кінцевих точок, платформи розширеного виявлення та реагування (Extended Detection and Response, XDR) розширюють охоплення для захисту від більш складних типів кібератак. Вони об’єднують можливості виявлення, дослідження та реагування в широкому діапазоні доменів, включаючи кінцеві точки організації, гібридні ідентифікатори,

хмарні програми та робочі навантаження, електронну пошту та сховища даних. Вони також підвищують ефективність операцій безпеки (SecOps) завдяки розширеній видимості ланцюга кібератак, автоматизації та аналітиці на основі штучного інтелекту та широкому аналізу загроз.

Розглянемо ключові можливості платформ XDR.

Платформи XDR координують виявлення кіберзагроз і реагування на всю цифрову власність організації. Вони допомагають швидко зупиняти кібератаки, об'єднуючи різноманітні інструменти безпеки на одній платформі, руйнуючи традиційні підходи та рішення безпеки для покращення захисту від кіберзагроз.

XDR збирає сповіщення низького рівня та зв'язує їх з інцидентами, швидше надаючи аналітикам безпеки повну картину кожної потенційної кібератаки. Аналітикам більше не потрібно переглядати випадкові фрагменти інформації, щоб виявити та зрозуміти кіберзагрозу, підвищуючи продуктивність і сприяючи швидшому реагуванню.

Оскільки XDR отримує сповіщення з ширшого набору джерел, аналітики можуть переглядати повний ланцюжок кібератак складної атаки, яка інакше могла б залишитися непоміченою рішеннями для точкової безпеки. Краща видимість скорочує час розслідування та підвищує ймовірність успішного усунення повної кібератаки.

Використовуючи високоточні сигнали безпеки та вбудовану автоматизацію, XDR виявляє поточні кібератаки. Потім він ініціює ефективні дії реагування на інциденти, включаючи ізоляцію скомпрометованих пристроїв і облікових записів користувачів, щоб завадити зловмисникам. Використовуючи ці можливості, організації можуть значно знизити ризики, обмежити наслідки, а також скоротити та спростити аналітикам розслідування та очищення після інцидентів.

Застосування штучного інтелекту (ШІ) та машинного навчання в XDR робить ШІ для кібербезпеки масштабованим і ефективним. Від моніторингу загрозливої поведінки та надсилання сповіщень до розслідування та виправлення, XDR використовує штучний інтелект для автоматичного виявлення, реагування та пом'якшення можливих кібератак. За допомогою машинного навчання XDR може

створювати профілі підозрілої поведінки, позначаючи їх для перевірки аналітиками.

Використовуючи вбудовані можливості автоматизації, XDR повертає в безпечний стан активи, скомпрометовані програмами-вимагачами, фішингом і бізнес-поштовими кампаніями. Рішення виконує такі дії відновлення, як припинення зловмисних процесів, видалення зловмисних правил пересилання та зберігання уражених пристроїв і облікових записів користувачів. Звільнені від повторюваних ручних завдань, групи безпеки можуть зосередитися на боротьбі зі складнішими кіберзагрозами з високим ризиком.

XDR об’єднує кілька продуктів безпеки на одній хмарній платформі, яка проактивно захищає від кіберзагроз. Платформа XDR зазвичай включає такі ключові компоненти [2]:

інструменти виявлення та реагування на кінцеві точки (EDR) відстежують різні кінцеві точки, включаючи мобільні телефони, ноутбуки та пристрої Інтернету речей (IoT). EDR допомагає підприємствам виявляти, аналізувати, досліджувати та реагувати на підозрілі дії, які вислизають від антивірусного програмного забезпечення;

платформи XDR використовують найновіші можливості штучного інтелекту та машинного навчання для автоматичного виявлення аномалій, визначення пріоритетів активних загроз і надсилання сповіщень. Вони також пропонують аналітику поведінки користувачів і об’єктів для фільтрації помилкових тривог;

безпека електронної пошти та можливості захисту особистих даних захищають облікові записи користувачів і комунікації від несанкціонованого доступу, втрати або компрометації. Хмарна безпека та інструменти захисту даних допомагають захистити хмарні системи та дані від внутрішніх і зовнішніх уразливостей, таких як випадки порушення даних. Виявлення мобільних загроз забезпечує видимість і захист усіх пристроїв, у тому числі персональних, підключених до корпоративної мережі;

механізм аналітики безпеки використовує штучний інтелект і

автоматизацію, щоб відсіювати безліч окремих сповіщень і співвідносити їх з інцидентами. Механізм збагачує виявлення інформаційними даними про кіберзагрози, а саме детальними контекстними відомостями про поточні та інші загрозливі атаки. Інтелектуальні дані про загрози як вбудовані в платформи XDR, так і отримані із зовнішніх глобальних каналів;

захищена та масштабована інфраструктура даних дозволяє підприємствам збирати, зберігати та обробляти великі обсяги необроблених даних. Рішення має підключатися до кількох джерел даних, включаючи сторонні програми та інструменти в хмарних, локальних і гібридних середовищах, і підтримувати різні типи та формати даних;

плейбуки автоматичних відповідей – це набір дій з усунення проблем, які групи безпеки можуть використовувати для автоматизації та оркестрування своїх реакцій на загрози. Плейбуки можна запускати вручну у відповідь на певні типи інцидентів або сповіщень або запускати автоматично, коли їх запускає правило автоматизації.

Palo Alto Networks [3] зазначає, що розширене виявлення та реагування (XDR) представляє еволюцію традиційних рішень кібербезпеки, пропонуючи більш інтегрований та автоматизований підхід до виявлення загроз і реагування на них. Оскільки кіберзагрози стають все більш складними, XDR забезпечує комплексний механізм захисту, який об’єднує кілька рівнів безпеки.

XDR розроблено для подолання складності сучасних загроз і обмежень традиційних заходів безпеки, пропонуючи уніфікований підхід до виявлення загроз, дослідження та реагування. Воно інтегрує дані з багатьох джерел, включаючи кінцеві точки, мережі, хмарні середовища, ідентифікацію та керування доступом, а також додатки [3].

Ця цілісна видимість дає змогу командам безпеки ефективно виявляти та нейтралізувати складні багатоетапні атаки. Ключові переваги XDR [3]:

можливості автоматичного виявлення загроз;

спрощені операції безпеки;

скорочений час відповіді;

покращений стан безпеки.

XDR збирає дані з різних рівнів безпеки, включаючи кінцеві точки, мережі та хмарні середовища. Він використовує машинне навчання та штучний інтелект для аналізу цих даних у режимі реального часу, виявлення закономірностей і аномалій, які вказують на потенційні загрози.

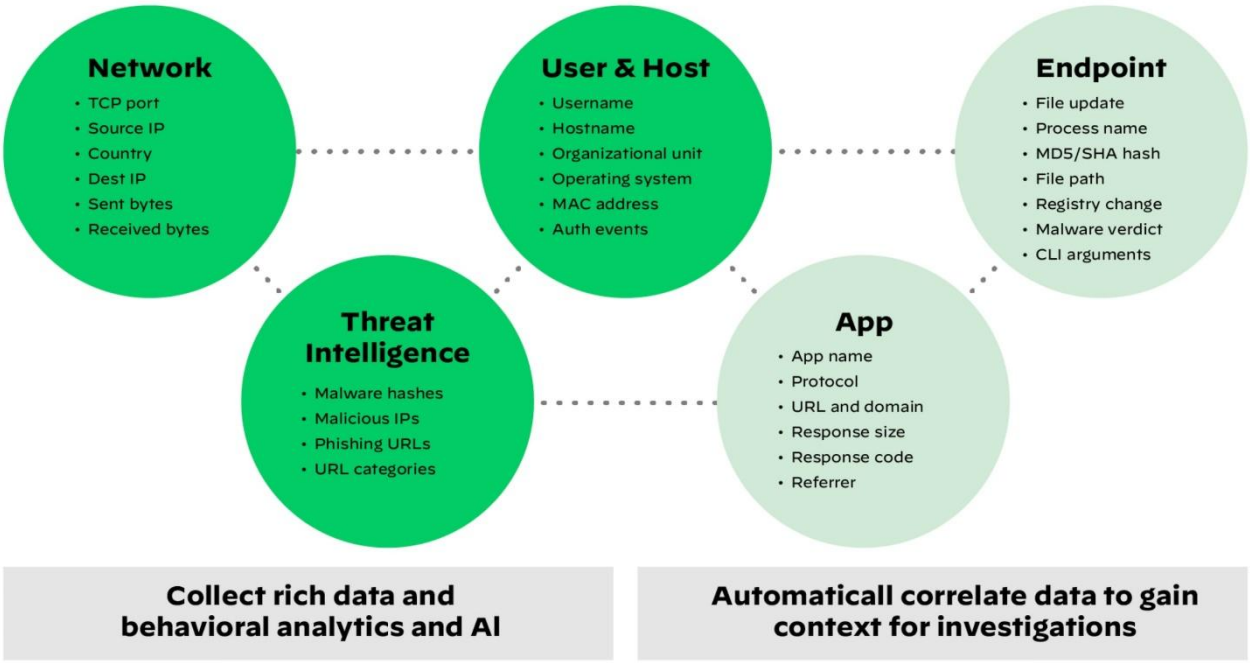


Рис. 1.2. Основні функції XDR [3]

Наприклад, якщо кінцева точка виявляє незвичайну активність під час входу, тоді як мережевий рівень реєструє спроби викрадання даних, XDR корелює ці події, щоб викликати автоматичну відповідь.

Розглянемо процес розслідування та реагування на базі XDR.

Розуміння детального робочого процесу XDR має вирішальне значення для повного використання його потенціалу. Платформи XDR безперервно відстежують і збирають сповіщення та журнали з різних інструментів безпеки в IT-інфраструктурі організації, включаючи кінцеві точки, мережі, керування ідентифікацією та доступом, а також хмарні середовища.

Початкова фаза виявлення зосереджена на виявленні потенційних інцидентів безпеки за допомогою [3]:

уніфікованого збору даних. XDR збирає дані з багатьох джерел, забезпечуючи централізований перегляд усіх подій безпеки та сповіщень;

інтеграції аналізу загроз. Постійні оновлення з глобальних каналів аналізу загроз покращують здатність платформи виявляти відомі та нові загрози;

збагачення даних. Оскільки дані надходять у XDR із кількох джерел, пов'язані події в потоці даних об'єднуються в об'єднані події, розширюючи початковий контекст. З'єднані дані можуть включати IP-адреси, домени, хеші файлів і дані аналізу загроз;

розширеної аналітики. Алгоритми машинного навчання аналізують збагачені дані, щоб виявити закономірності та аномалії, які можуть вказувати на інцидент безпеки.

Після виявлення потенційного інциденту наступним кроком є групування пов'язаних сповіщень в один інцидент, розповідь про історію атаки, як вона розгорталася, і надання повного контексту. Потім кожен інцидент оцінюється та розставляється за ступенем тяжкості.

Групування сповіщень – після того як XDR проаналізує об'єднані дані з кількох джерел, щоб знайти нові аномалії, він групує їх з іншими сповіщеннями від кінцевої точки, хмари, мережі та інших датчиків, щоб створити єдиний інцидент.

Оцінка інциденту – комбінований інцидент, що представляє повну історію атаки, потім оцінюється за серйозністю того, що виявив XDR. Потім аналітики безпеки можуть використовувати цю оцінку, щоб визначити пріоритетність свого дослідження.

На основі встановленого висновку ініціюються відповідні дії реагування, щоб пом'якшити загрозу та виправити уражені системи [3]:

індикатори блокування. Платформа блокує виявлені шкідливі індикатори, такі як IP-адреси, домени та хеші файлів;

ізоляція кінцевої точки. Уражені кінцеві точки ізольовано від мережі, щоб запобігти подальшому поширенню загрози;

керування сеансами. Сеанси користувачів очищаються та відкликаються, а

для захисту облікових записів застосовується багатофакторна автентифікація (MFA);

скидання пароля. Паролі користувачів скидаються, щоб запобігти несанкціонованому доступу, якщо це необхідно;

закриття інциденту. Інцидент закривається автоматично без подальших дій, що мінімізує збої в нормальній роботі.

Постійний моніторинг і регулярне сканування гарантують, що безпека організації залишається надійною, а будь-які нові загрози миттєво виявляються та усуваються [3]:

моніторинг у режимі реального часу. Інформаційні панелі забезпечують видимість у режимі реального часу стану кінцевих точок і статусу інцидентів, уможливлюючи проактивне керування загрозами;

сканування неактивних загроз. Періодичні сканування виявляють неактивні шкідливі програми, які можуть активуватися за певних умов;

гігієна та відповідність. Платформа відстежує гігієну кінцевих точок, забезпечуючи відповідність політикам безпеки та мінімізуючи ризики від зовнішніх пристроїв, таких як USB.

Розглянемо основні компоненти архітектури XDR.

Архітектура XDR (рисунок 1.3) поєднує різні елементи кібербезпеки, щоб представити загальне уявлення про виявлення загроз, аналіз і реагування. Його основні елементи забезпечують інтегровану платформу для безперебійного виявлення, аналізу та реагування в кількох областях [4]. Функції основних компонентів XDR [4]:

збір і агрегація даних. Це формує фундаментальний рівень XDR, де необроблені дані збираються з різних джерел. Він інтегрує телеметрію з багатьох середовищ для забезпечення повної видимості. Основні джерела даних включають:

дані кінцевих точок: журнали або поведінкові дані, згенеровані кінцевими точками, будь то сервери, ноутбуки, мобільні пристрої чи будь-які пристрої IoT. Це допомагає відстежувати такі аномалії, як зловмисне програмне забезпечення у

корпоративних системах або незвичну поведінку;

мережеві дані: інформація про мережевий трафік, зокрема потоки пакетів, аномалії мережі, журнали брандмауера та історію з'єднань;

хмарні дані фіксують діяльність у корпоративному хмарному середовищі, IaaS, PaaS або SaaS. Рішення аналізує шаблони доступу, використання додатків та діяльність API у хмарі, що може виявити неправильні конфігурації або порушення;

дані додатків: це включає дані рівня додатків, такі як журнали корпоративних додатків, баз даних і веб-служб. Ця інформація є дуже корисною для виявлення атак, таких як впровадження SQL, XSS або незаконний доступ до додатка.

аналіз та кореляція даних. Архітектура XDR включає збір великої кількості даних безпеки з різних джерел. Розширена аналітика та алгоритми машинного навчання корелюють події з корпоративних систем, щоб ідентифікувати шаблони, які насправді вказують на кіберзагрозу.

інтеграція аналізу загроз. Системи XDR включають канали з платформ аналізу загроз, які надають інформацію в реальному часі про нові загрози, вразливості та тактику атак. Таким чином, за допомогою такого інтелекту механізм виявлення в XDR буде покращено, і команди безпеки навіть будуть заздалегідь повідомлені про ризики.

Завдяки такій інтеграції організація не відстає від світових тенденцій загроз. Це також означає, що організація завжди може захиститися від відомих атак і щойно знайдених експлойтів.

автоматизований механізм реагування. Системи XDR мають автоматизовані механізми реагування, які роблять реагування на інциденти більш ефективним. Після виявлення та підтвердження загрози платформа може виконувати заздалегідь визначені дії, наприклад ізолювати уражені пристрої, блокувати шкідливі IP-адреси або ініціювати сканування системи.

Таким чином, автоматизація зберігає поширення атак локалізованим, скорочує час відповіді та зменшує швидкість зменшення шкоди. Це також

запобігає перевантаженню груп безпеки та дозволяє їм більше зосередитися на складних або стратегічних питаннях.

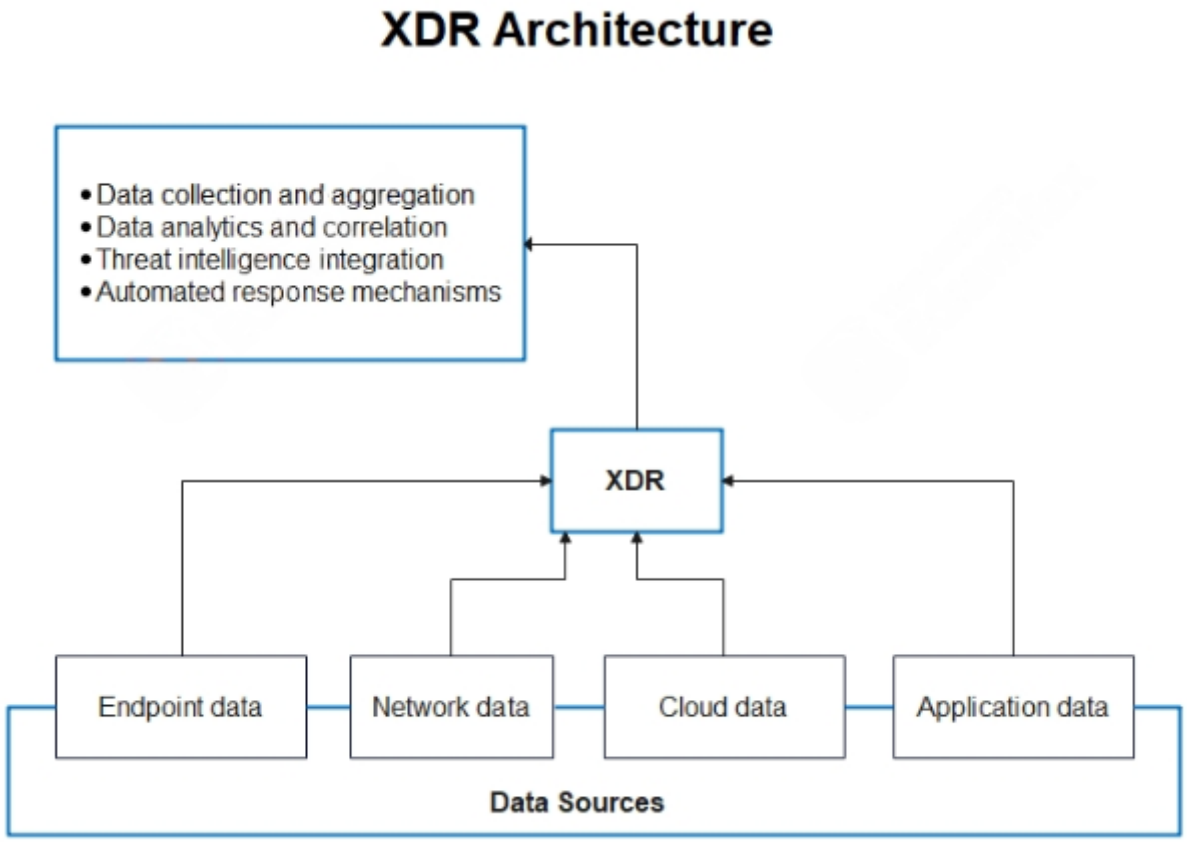


Рис. 1.3. Основні компоненти архітектури XDR [4]

Завдяки інтеграції виявлення, збагачення, аналізу та автоматизованого реагування в уніфікований робочий процес XDR значно покращує здатність організації виявляти і реагувати на інциденти безпеки до того, як станеться порушення. Використання цих можливостей забезпечує проактивний і комплексний підхід до кібербезпеки, захищаючи організацію від нових загроз.

Оскільки організації стикаються з постійно зростаючим ландшафтом загроз і дедалі складнішими IT-екосистемами, XDR пропонує спрощений підхід до управління безпекою шляхом консолідації та автоматизації різноманітних завдань.

Одним із ключових способів XDR спрощення операцій безпеки є централізована видимість. Традиційні рішення безпеки часто генерують сповіщення з різних джерел, наповнюючи команди безпеки великою кількістю

даних для аналізу.

XDR вирішує цю проблему, об’єднуючи дані з кінцевих точок, мереж, програм і хмарних середовищ в єдину платформу. Це однопанельне подання надає командам безпеки всебічне уявлення про стан безпеки організації, усуваючи потребу в навігації різними інструментами та інтерфейсами.

Ця спрощена видимість прискорює виявлення загроз і сприяє швидшому прийняттю рішень, оскільки спеціалісти з безпеки можуть зрозуміти ширший контекст інциденту та оцінити його серйозність у режимі реального часу.

Крім того, можливості автоматизації XDR значно підвищують ефективність операцій безпеки. Замість сортування кожного сповіщення рішення XDR групують пов’язані сповіщення в один інцидент, що представляє всю атаку, і оцінює ці інциденти на основі серйозності. Аналітики можуть налаштовувати автоматичні відповіді, досліджувати ці інциденти та самостійно виконувати відповідні дії.

Ця автоматизація прискорює процес реагування та мінімізує ризик людської помилки, звільняючи персонал служби безпеки, щоб зосередитися на більш стратегічних ініціативах. Рутинні та повторювані завдання, такі як сортування сповіщень, ізоляція скомпрометованих кінцевих точок та ініціювання робочих процесів реагування на інциденти, безперебійно виконуються платформою XDR, що дозволяє командам безпеки розподіляти свій досвід там, де це найбільш важливо.

1.3. Аналіз існуючих рішень для захисту кінцевих точок організації

Розглянемо рішення для виявлення загроз та управління інформацією та подіями безпеки.

Комерційні рішення

Splunk є одним з найпопулярніших SIEM рішень на ринку. Відрізняється гнучкою платформою для аналізу даних, але може бути досить дорогим.

IBM QRadar – ще одне відоме SIEM рішення з широкими можливостями для

виявлення та реагування на загрози. Пропонує розширену аналітику та інтеграцію з іншими продуктами IBM.

AlienVault USM – комплексне рішення для управління безпекою, яке включає SIEM, а також інші функції, такі як сканування вразливостей та управління патчами.

RSA NetWitness – потужне SIEM-рішення з фокусом на розширену аналітику та виявлення загроз.

Рішення з відкритим кодом

Graylog є популярним рішенням SIEM з відкритим кодом, яке відоме своєю простотою використання та масштабованістю.

Elastic Stack представляє собою сукупність інструментів з відкритим кодом (Elasticsearch, Kibana, Beats, Logstash) для пошуку, аналізу та візуалізації даних, що часто використовується для створення власних SIEM-рішень.

OSSEC – ще одне рішення SIEM з відкритим кодом, яке фокусується на безпеці хостів і може бути гарною альтернативою Wazuh.

При виборі рішення, подібного до Wazuh, варто врахувати наступні фактори:

вартість: треба брати до уваги як ліцензійні витрати, так і витрати на інфраструктуру та обслуговування;

функціональність: необхідно оцінити, які функції вам необхідні (збір даних, аналіз, візуалізація, автоматизація);

масштабованість: необхідно переконатися, що рішення зможе обробляти необхідний обсяг даних і масштабуватися разом з корпоративною інфраструктурою;

інтеграція: необхідно перевірити, чи інтегрується рішення з іншими наявними системами і інструментами;

спільнота: активна спільнота користувачів і розробників може значно полегшити використання і підтримку рішення.

Треба зауважити, що вибір SIEM-системи – це стратегічне рішення, яке впливає на безпеку організації. Тому рекомендується залучити до цього процесу

фахівців з інформаційної безпеки.

Wazuh – це потужне SIEM-рішення з відкритим кодом, яке набуло значної популярності завдяки своїм можливостям та гнучкості. Однак, на ринку існують й інші достойні конкуренти. Давайте порівняємо деякі з них:

Wazuh vs. Graylog

Схожість: обидва рішення є популярними SIEM-системами з відкритим кодом, які пропонують гнучку платформу для збору, аналізу та візуалізації даних.

Відмінності:

Фокус: Wazuh більше зосереджений на безпеці та виявленні загроз, тоді як Graylog пропонує більш широкий спектр функцій для лог-менеджменту.

Агенти: Wazuh використовує легких агентів для збору даних з кінцевих точок, тоді як Graylog часто інтегрується з іншими системами за допомогою протоколів syslog, Elasticsearch та ін.

Правила: Wazuh має більш розвинену систему правил для виявлення загроз, тоді як Graylog більше покладається на Elasticsearch для пошуку та аналізу даних.

Wazuh vs. Elastic Stack

Схожість: Обидва рішення базуються на Elasticsearch для зберігання та пошуку даних, що забезпечує високу швидкість та масштабованість.

Відмінності:

Комплексність: Elastic Stack – це сукупність інструментів, тоді як Wazuh – це спеціалізоване SIEM-рішення. Для побудови SIEM на базі Elastic Stack потрібна додаткова конфігурація та розробка.

Функціональність: Wazuh пропонує готові рішення для виявлення загроз та відповіді на інциденти, тоді як Elastic Stack вимагає більшої налаштування для досягнення подібних результатів.

Wazuh vs. OSSEC

Схожість: Обидва рішення є SIEM-системами з відкритим кодом, які фокусуються на безпеці хостів.

Відмінності:

Модульність: Wazuh має більш модульну архітектуру, що дозволяє легко

розширювати його функціональність.

Спільнота: Wazuh має більшу та активнішу спільноту розробників та користувачів.

Таблиця 1.1

Зведена таблиця порівняння рішень з відкритим кодом

Характеристика	Wazuh	Graylog	Elastic Stack	OSSEC
Фокус	Безпека, SIEM	Лог-менеджмент	Пошук та аналіз даних	Безпека хостів
Агенти	Легкі агенти	Системні журнали, Elasticsearch	Beats	Легкі агенти
Правила	Розширена система правил	Elasticsearch-запити	Elasticsearch-запити	Власна мова правил
Спільнота	Велика, активна	Велика, активна	Дуже велика	Середня

Вибір оптимального рішення з відкритим кодом для моніторингу та захисту кінцевих точок залежить від багатьох факторів, включаючи розмір корпоративної інфраструктури, рівень досвіду команди фахівців, необхідні функціональні можливості та бюджет.

Давайте розглянемо детальніше, як різні рішення підходять для цих завдань:

Рішення Wazuh надає уніфікований захист XDR і SIEM для кінцевих точок і хмарних робочих навантажень [5].

Переваги рішення Wazuh:

комплексний підхід: Wazuh пропонує широкий спектр функцій, включаючи моніторинг цілісності файлів, виявлення вторгнень, управління вразливостями та ін.;

агенти: легкі агенти Wazuh забезпечують ефективний збір даних з кінцевих точок;

правила: гнучка система правил дозволяє налаштувати систему відповідно до ваших потреб.

Якщо потрібне повне рішення для захисту кінцевих точок з широким набором функцій і гнучкою конфігурацією, рішення Wazuh є відмінним вибором.

Рішення OSSEC – це масштабована система виявлення вторгнень на основі хоста (Host-based Intrusion Detection System, HIDS) з відкритим кодом.

OSSEC має потужний механізм кореляції та аналізу, який включає аналіз журналів, моніторинг цілісності файлів, моніторинг реєстру Windows, централізоване застосування політики, виявлення руткітів, сповіщення в режимі реального часу та активне реагування. Воно працює на більшості операційних систем, включаючи Linux, OpenBSD, FreeBSD, MacOS, Solaris і Windows (рисунок 1.4) [6].

Переваги:

фокус на безпеці хостів: OSSEC спеціалізується на моніторингу цілісності файлів, виявленні вторгнень та аналізі журналів;

легкість у використанні: OSSEC має досить простий інтерфейс і відносно нескладну конфігурацію.

Якщо потрібне просте та ефективне рішення для моніторингу безпеки хостів, OSSEC може бути хорошим варіантом.

Рис. 1.4. Компоненти рішення OSSEC [6]

Elasticsearch – це система розподіленого пошуку та аналітики, масштабоване сховище даних і векторна база даних, побудована на Apache Lucene. Вона оптимізована для швидкості та відповідності робочим

навантаженням у виробничому масштабі. Elasticsearch використовується для пошуку, індексування, зберігання та аналізу даних будь-якої форми та розміру практично в реальному часі [7].

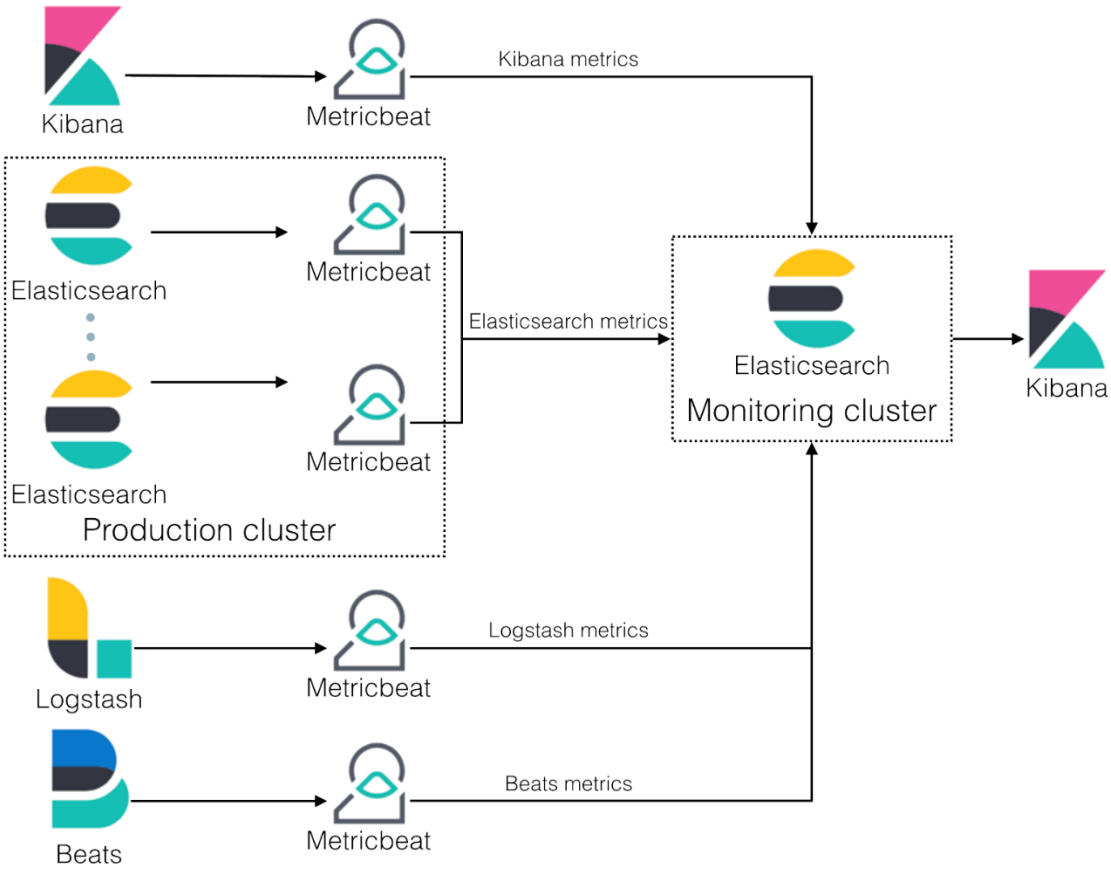


Рис. 1.5. Архітектура для моніторингу кластера на базі Elasticsearch [7]

Переваги:

гнучкість: Elastic Stack дозволяє створювати власні рішення для збору, аналізу та візуалізації даних;

масштабованість: легко масштабується для обробки великих обсягів даних.

Якщо потрібна максимальна гнучкість і ви готові інвестувати час у розробку власного рішення, Elastic Stack – відмінний вибір.

Рішення Graylog є потужним рішенням для керування інформацією та подіями безпеки (SIEM), яке пропонує надійну платформу аналітики журналів, яка спрощує збір, пошук, аналіз і попередження всіх типів даних, створених машиною. Воно спеціально розроблений для збору даних із різноманітних джерел, що дозволяє централізувати, захистити та ефективно контролювати дані

журналу. Graylog може виконувати широкий спектр функцій кібербезпеки, таких як [8]:

агрегація даних;

аналітика даних безпеки (звіти та інформаційні панелі);

кореляція та моніторинг подій безпеки;

криміналістичний аналіз;

виявлення інцидентів і реагування;

реагування на події в реальному часі або консоль оповіщення;

інтелект загроз;

аналітика поведінки користувачів і організацій (UEBA);

управління відповідністю IT.

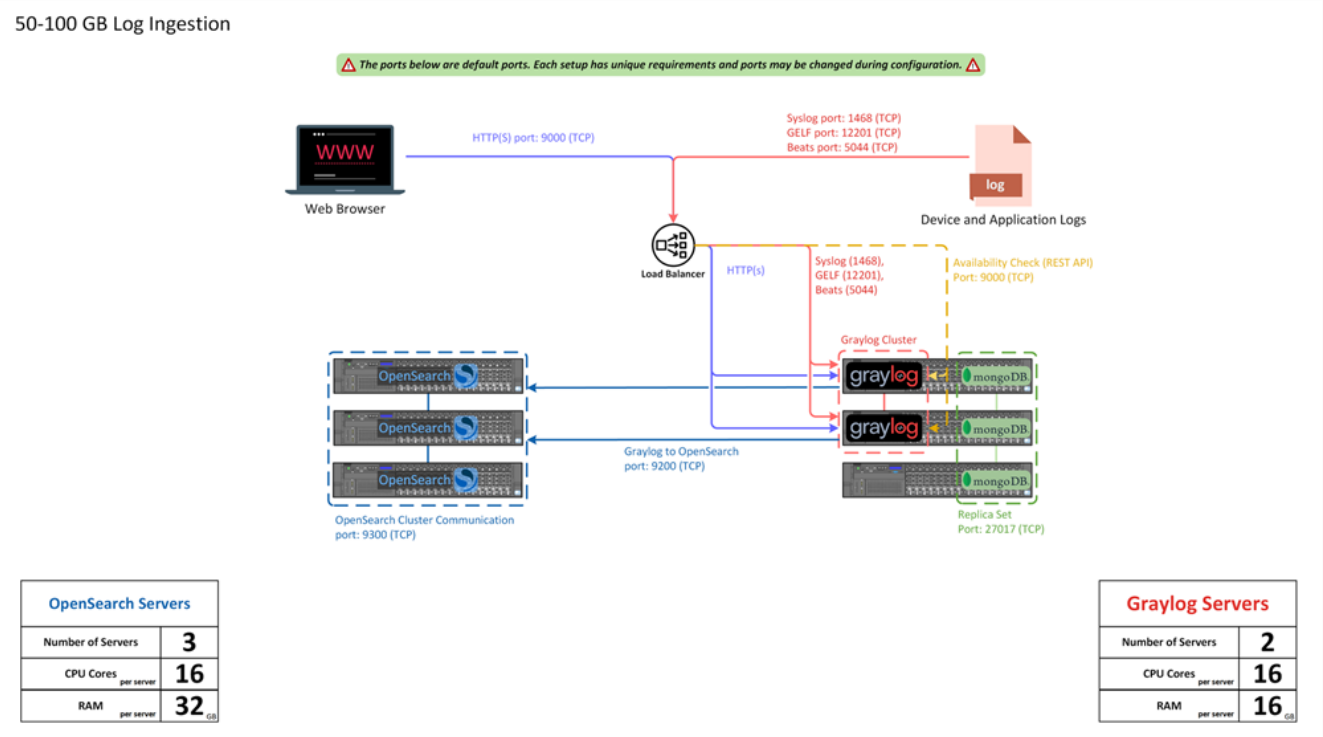


Рис. 1.6. Багатохостова кластерна архітектура Graylog [8]

Багатохостова кластерна архітектура Graylog (рисунок 1.6) забезпечує високу доступність і масштабованість для великих виробничих середовищ. Кластеризація стає можливою за допомогою механізму лідер-послідовник, який визначається користувачем. Це дозволяє розподіляти вузли Graylog, які називаються лідерами, на кількох фізичних або віртуальних машинах. Ці головні

вузли є основними точками контакту між адміністраторами та користувачами, чиї запити направляються через них до їхніх підписників. Потім підписники обробляють вхідні повідомлення за допомогою відповідного процесора.

Примірники Graylog, MongoDB і OpenSearch можна додавати до кластерів; в результаті ми можемо збільшити розмір кластера Graylog, щоб задовольнити більші потреби в прийомі даних.

Отже, всі розглянуті нами рішення з відкритим кодом є безкоштовними для завантаження та використання. Це одна з головних переваг рішень з відкритим кодом. Ми можемо вільно встановлювати, модифікувати та розповсюджувати їх відповідно до ліцензії.

Однак, варто зазначити кілька важливих нюансів:

підтримка. Хоча програмне забезпечення безкоштовне, професійна підтримка та консультації зазвичай надаються за додаткову плату. Багато компаній пропонують комерційні сервіси з підтримки та розробки для рішень з відкритим кодом;

інфраструктура. Для роботи будь-якого програмного забезпечення потрібна відповідна інфраструктура (сервери, сховища тощо). Вартість обслуговування інфраструктури може бути значною, особливо для великих розгортань;

час та ресурси. Впровадження та підтримка будь-якого рішення з відкритим кодом вимагає певних знань та навичок. Якщо немає власної команди фахівців, то може знадобитися залучити сторонніх експертів.

Рішення з відкритим кодом пропонують відмінну альтернативу комерційним продуктам, але перед прийняттям рішення варто ретельно оцінити всі пов'язані з цим витрати та ресурси.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА БАЗІ WAZUH

2.1. Призначення та основні функції рішення Wazuh

Платформа Wazuh Extended Detection and Response (XDR) надає комплексне рішення безпеки, яке виявляє, аналізує та реагує на загрози на кількох рівнях IT-інфраструктури. Wazuh збирає телеметрію з кінцевих точок, мережевих пристроїв, хмарних робочих навантажень, сторонніх API та інших джерел для уніфікованого моніторингу та захисту безпеки [12].

Wazuh – це безкоштовна платформа безпеки з відкритим кодом, яка об’єднує можливості XDR і SIEM. Вона захищає робочі навантаження в локальних, віртуалізованих, контейнерних і хмарних середовищах. Wazuh допомагає організаціям і окремим особам захистити свої дані від загроз безпеки. Це рішення широко використовується тисячами організацій по всьому світу, від малих до великих підприємств [9].

Wazuh – це ефективне рішення безпеки, яке забезпечує організації необхідними інструментами та можливостями для виявлення та запобігання постійним атакам. Завдяки розширеним можливостям полювання на загрози групи безпеки можуть залишатися проактивними у виявленні та усуненні нових загроз і ефективно захищати свої бізнес-процеси.

Розглянемо основні функції платформи Wazuh.

1. Полювання на загрозу.

Рішення Wazuh забезпечує повну видимість, реєструючи різні компоненти корпоративної IT-інфраструктури, включаючи ОС, додатки, бази даних тощо. Рішення Wazuh допомагає мисливцям за загрозами робити точні висновки, надаючи цілісне уявлення про бізнес-інфраструктуру як у хмарі, так і в локальній мережі [12].

Рішення Wazuh надає можливості розкрити потужність корпоративних

даних безпеки за допомогою достатніх можливостей зберігання журналів, індексування та запитів. Рішення Wazuh зберігає журнали протягом тривалого періоду часу, забезпечуючи всеосяжний аудит подій безпеки. Його можливості індексування та запитів полегшують швидкий пошук і виявлення потенційних проблем і першопричини інцидентів безпеки.

Рішення Wazuh відображає події у корпоративному середовищі за допомогою тактики, техніки та процедур (TTP) у рамках MITER ATT&CK. Рішення Wazuh дозволяє командам безпеки формулювати гіпотези, узгоджуючи їх із відомими TTP, які використовують групи загроз. Це спрощує розслідування полювання на загрози, полегшуючи ідентифікацію та проактивне реагування на потенційні загрози.

Перехресна телеметрія з інтегрованими каналами аналізу загроз. Рішення Wazuh легко інтегрується з такими платформами аналізу загроз, як VirusTotal, AlienVault OTX, URLhaus, MISP і AbuseIPDB. Цей підхід, заснований на розвідці, використовує найновіші дані розвідки про загрози, дозволяючи команді фахівців виявляти потенційні загрози та проводити ретельне розслідування.

Рішення Wazuh надає можливості покращити пошук загроз за допомогою спеціальних наборів правил і декодерів для ефективного виявлення та розслідування. Рішення Wazuh надає командам безпеки можливість досліджувати та пом’якшувати загрози, дозволяючи створювати власні набори правил. Ці набори правил спрямовані на конкретні IoC для ефективної оптимізації операцій безпеки. Завдяки точному налаштуванню можливостей виявлення Wazuh задовольняє унікальні вимоги та мінімізує ризик непомічення потенційних загроз.

Рішення Wazuh надає можливості бути попереду загроз безпеці за допомогою проактивного виявлення. Функція моніторингу команд Wazuh дозволяє командам безпеки віддалено виконувати команди на контрольованих кінцевих точках і аналізувати вихідні дані. Це дозволяє командам безпеки виявляти підозрілі дії шляхом активного пошуку індикаторів компрометації.

Рішення Wazuh дозволяє візуалізувати події безпеки за допомогою настроюваних інформаційних панелей і створювати звіти на інформаційній панелі

Wazuh, щоб отримати цінну інформацію про інциденти, тенденції та аномалії. Інформаційна панель Wazuh дає змогу мисливцям за загрозами ефективно оцінювати дані безпеки, спрощуючи процес виявлення можливих загроз. Рішення Wazuh також містить інтегрований механізм звітності для створення індивідуальних звітів.

2. Поведінковий аналіз.

Рішення Wazuh надає можливості виявлення загроз та реагування на них на основі незвичних моделей поведінки. Можливості аналізу поведінки Wazuh передбачають використання розширеної аналітики для виявлення відхилень від нормальної поведінки, які можуть вказувати на потенційні загрози безпеці. Ці можливості включають моніторинг цілісності файлів, мережевого трафіку, поведінки користувачів і аномалій у показниках продуктивності системи.

3. Автоматична відповідь.

Рішення Wazuh зменшує середній час реагування на інциденти за допомогою модуля активного реагування Wazuh. Рішення Wazuh автоматично реагує на загрози, щоб зменшити потенційний вплив на корпоративну інфраструктуру. Ми можемо використовувати вбудовані дії реагування або створювати спеціальні дії відповідно до вашого плану реагування на інциденти.

4. Хмарний захист робочого навантаження.

Рішення Wazuh забезпечує безпеку корпоративних хмарних робочих навантажень і контейнерів. Рішення Wazuh має вбудовану інтеграцію з хмарними службами для збору та аналізу телеметрії.

Рішення Wazuh захищає власні та гібридні хмарні середовища, включаючи контейнерну інфраструктуру, виявляючи поточні та нові загрози та реагуючи на них.

5. Розвідка загроз.

Рішення Wazuh включає канали аналізу загроз для виявлення відомих загроз і реагування на них. Воно інтегрується з джерелами аналізу загроз, включаючи розвідку з відкритим кодом (OSINT), комерційні канали та дані, надані користувачами, щоб надавати актуальну інформацію про потенційні загрози.

6. Відповідність і звітність.

Рішення Wazuh надає можливості дотримуватися нормативних вимог, створення звітів та демонстрації ефективності корпоративної програми безпеки. Рішення Wazuh виконує перевірки на відповідність нормам і стандартам безпеки, таким як PCI-DSS, HIPAA, GDPR тощо.

2.2. Архітектура рішення Wazuh

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

Рішення Wazuh складається з трьох центральних компонентів платформи та одного універсального агента.

Рішення Wazuh базується на агенті Wazuh, який розгортається на контрольованих кінцевих точках, і на трьох центральних компонентах: сервері Wazuh, індексаторі Wazuh і інформаційній панелі Wazuh.

Індексатор Wazuh – це високомасштабована система повнотекстового пошуку та аналітики. Цей центральний компонент індексує та зберігає сповіщення, створені сервером Wazuh.

Сервер Wazuh аналізує дані, отримані від агентів. Він обробляє його через декодери та правила, використовуючи аналіз загроз для пошуку добре відомих індикаторів компрометації (IoC). Один сервер може аналізувати дані від сотень або тисяч агентів і масштабувати горизонтально, якщо налаштувати його як кластер. Цей центральний компонент також використовується для керування агентами, налаштування та оновлення їх віддалено, коли це необхідно.

Інформаційна панель Wazuh – це веб-інтерфейс користувача для візуалізації та аналізу даних. Вона включає в себе готові інформаційні панелі для пошуку загроз, відповідності нормативним вимогам (наприклад, PCI DSS, GDPR, CIS,

HIPAA, NIST 800-53), виявлені вразливі програми, дані моніторингу цілісності файлів, результати оцінки конфігурації, моніторинг хмарної інфраструктури події та ін. Інформаційна панель Wazuh також використовується для керування конфігурацією Wazuh і моніторингу її стану.

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

На додаток до можливостей моніторингу на основі агентів, платформа Wazuh може контролювати безагентні пристрої, такі як брандмауери, комутатори, маршрутизатори або мережі IDS, серед іншого. Наприклад, дані системного журналу можна збирати через Syslog, а його конфігурацію можна відстежувати шляхом періодичного тестування даних, через SSH або через API.

На рисунку 2.1 показано компоненти та потік даних Wazuh.

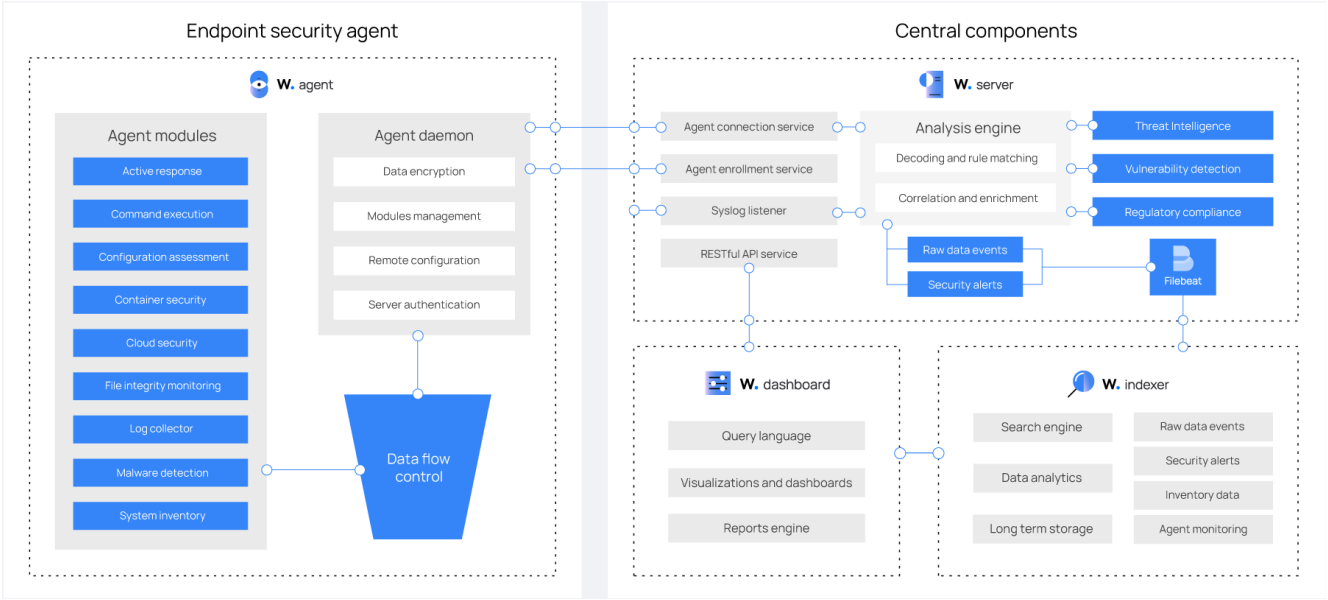


Рис. 2.1. Архітектура платформи Wazuh [9]

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

майже в реальному часі. Індексатор Wazuh можна налаштувати як однохостовий або багатохостовий кластер, що забезпечує масштабованість і високу доступність.

Індексатор Wazuh зберігає дані як документи JSON. Кожен документ співвідносить набір ключів, імен полів або властивостей із відповідними значеннями, які можуть бути рядками, числами, логічними значеннями, датами, масивами значень, геолокаціями чи іншими типами даних [9].

Індекс – це сукупність пов'язаних між собою документів. Документи, що зберігаються в індексаторі Wazuh, розподіляються між різними контейнерами, відомими як сегменти. Розподіляючи документи між декількома шарами та розподіляючи ці сегменти між кількома хостами, індексатор Wazuh може забезпечити надлишковість. Це захищає корпоративну систему від апаратних збоїв і збільшує пропускну здатність запитів, коли вузли додаються до кластера.

Wazuh використовує чотири різні індекси для зберігання різних типів подій, які наведені в таблиці 2.1.

Таблиця 2.1

Індекси для зберігання різних типів подій в Wazuh

Індекс	опис
wazuh – **сповіщення**	Зберігає сповіщення, створені сервером Wazuh . Вони створюються кожного разу, коли подія запускає правило з достатньо високим пріоритетом (цей поріг можна налаштувати).
wazuh - **архіви**	Зберігає всі події (архівні дані), отримані сервером Wazuh , незалежно від того, чи спрацьовує правило.
wazuh - **моніторинг**	Зберігає дані, пов'язані зі статусом агента Wazuh протягом певного часу. Він використовується веб-інтерфейсом для відображення того, коли окремі агенти є або були `Active` , `Disconnected` , або . `Never connected`
wazuh - **статистика**	Зберігає дані, пов'язані з продуктивністю сервера Wazuh . Він використовується веб-інтерфейсом для представлення статистики продуктивності.

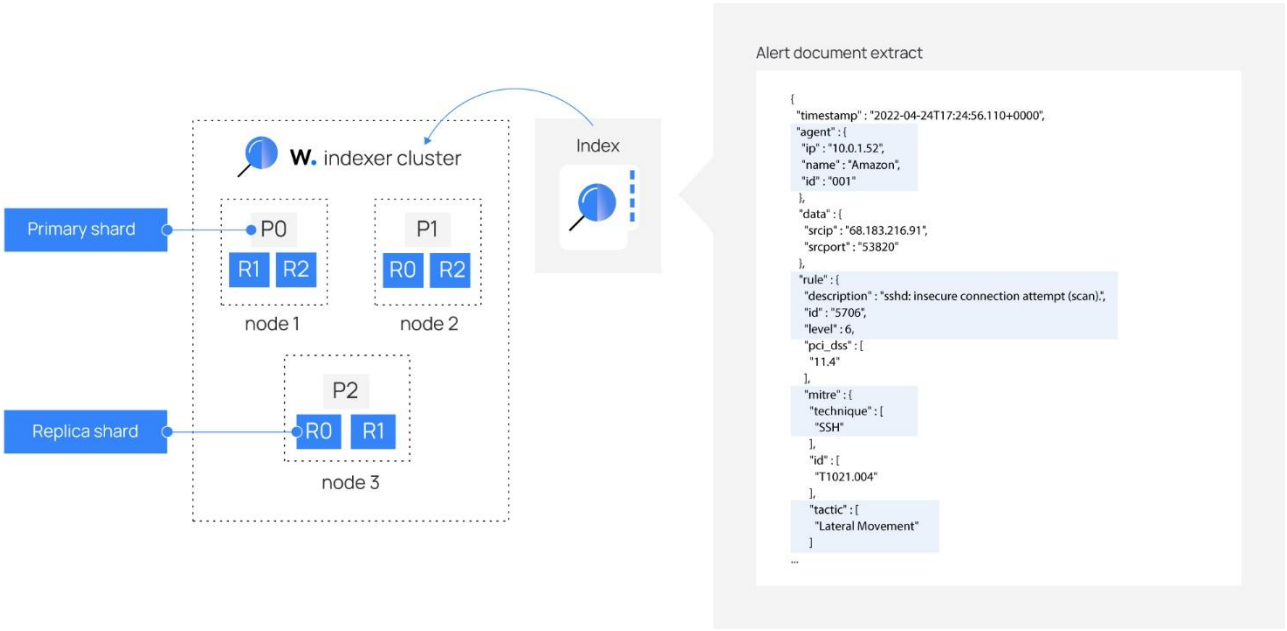


Рис. 2.2. Схема індексування в Wazuh [9]

Ми можемо взаємодіяти з кластером індексатора Wazuh за допомогою REST API індексатора Wazuh, який пропонує велику гнучкість. Ми можемо виконувати пошук, додавати або видаляти документи, змінювати індекси тощо.

Ось приклад запиту до індексатора Wazuh, який повертає сповіщення про останнє бокове переміщення за допомогою техніки SSH [9]:

```
GET /wazuh-alerts-4.x-*/_search
{
  "query": {
    "bool": {
      "must": [
        {"term": { "rule.mitre.tactic": "Lateral Movement" } },
        {"term": { "rule.mitre.technique": "SSH" } }
      ]
    }
  },
  "sort": [
    { "timestamp": { "order": "desc" } }
  ],
  "size": 1
}
```

Нижче наведено фрагмент результату запиту, який є частиною індексованого документа сповіщення:

```
{
  "timestamp" : "2022-04-24T17:24:56.110+0000",
  "agent" : {
   "ip" : "10.0.1.52",
   "name" : "Amazon",
   "id" : "001"
  },
  "data" : {
    "srcip" : "68.183.216.91",
    "srcport" : "53820"
  },
  "rule" : {
    "description" : "sshd: insecure connection attempt (scan).",
    "id" : "5706",
    "level" : 6,
    "pci_dss" : ["11.4"],
    "mitre" : {
      "technique" : [
        "SSH"
      ],
      "id" : ["T1021.004"],
      "tactic" : [
        "Lateral Movement"
     ]
    }
  },
  "full_log" : "Apr 24 17:24:55 ip-10-0-1-52 sshd[32179]: Did not receive identification string from 68.183.216.91
  "location" : "/var/log/secure",
  "predecoder" : {
    "hostname" : "ip-10-0-1-52",
    "program_name" : "sshd",
    "timestamp" : "Apr 24 17:24:55"
  },
  "decoder" : {
    "parent" : "sshd",
    "name" : "sshd"
  },
  "GeoLocation" : {
    "city_name" : "Frankfurt am Main",
    "country_name" : "Germany",
    "region_name" : "Hesse"
  }
```


Індексатор Wazuh добре підходить для чутливих до часу випадків використання, таких як аналітика безпеки та моніторинг інфраструктури, оскільки це пошукова платформа майже в реальному часі. Затримка від часу індексації документа до моменту, коли він стає доступним для пошуку, дуже мала, зазвичай одна секунда.

Окрім швидкості, масштабованості та стійкості, індексатор Wazuh має кілька вбудованих функцій, які роблять зберігання та пошук даних ще ефективнішим, наприклад зведення даних, сповіщення, виявлення аномалій та керування життєвим циклом індексу.

Серверний компонент Wazuh аналізує дані, отримані від агентів , ініціюючи сповіщення при виявленні загроз або аномалій. Він також використовується для

віддаленого керування конфігурацією агентів і моніторингу їх стану [9].

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

Крім того, сервер Wazuh можна інтегрувати із зовнішнім програмним забезпеченням, включаючи системи продажу квитків, такі як ServiceNow, Jira та PagerDuty, а також платформи обміну миттєвими повідомленнями, такі як Slack. Ці інтеграції зручні для оптимізації операцій безпеки [9].

Розглянемо архітектуру сервера Wazuh.

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

На рисунку 2.3 показано архітектуру та компоненти сервера Wazuh.

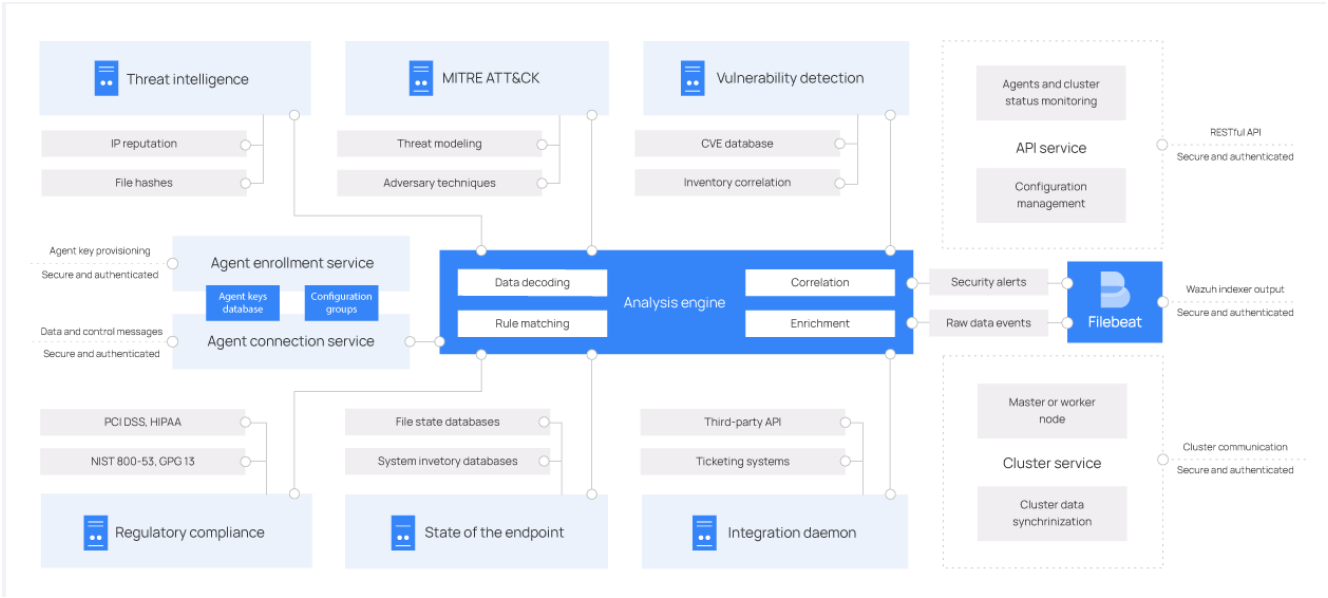


Рис. 2.3. Архітектура та компоненти сервера Wazuh [9]

Сервер Wazuh складається з кількох перелічених нижче компонентів, які

мають різні функції, наприклад реєстрацію нових агентів, перевірку ідентифікації кожного агента та шифрування зв’язку між агентом Wazuh і сервером Wazuh.

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

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

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

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

Демон кластера Wazuh: ця служба використовується для горизонтального масштабування серверів Wazuh, розгортаючи їх як кластер. Така конфігурація в поєднанні з балансувальником мережевого навантаження забезпечує високу доступність і балансування навантаження. Демон кластера Wazuh це те, що

сервери Wazuh використовують для спілкування один з одним і підтримки синхронізації.

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

Інформаційна панель Wazuh – це гнучкий та інтуїтивно зрозумілий веб-інтерфейс користувача для видобутку, аналізу та візуалізації подій безпеки та даних сповіщень. Він також використовується для управління та моніторингу платформи Wazuh. Крім того, він надає функції для керування доступом на основі ролей (RBAC) і єдиного входу (SSO).

Візуалізація та аналіз даних. Веб-інтерфейс допомагає користувачам переміщатися між різними типами даних, зібраних агентом Wazuh, а також сповіщеннями безпеки, створеними сервером Wazuh. Користувачі також можуть створювати звіти та створювати власні візуалізації та інформаційні панелі [9].

Як приклад, Wazuh надає готові інформаційні панелі для відповідності нормативним вимогам, таким як PCI DSS, GDPR, HIPAA та NIST 800-53. Він також надає інтерфейс для навігації між структурою MITRE ATT&CK і пов’язаними сповіщеннями.

Моніторинг та налаштування агентів. Інформаційна панель Wazuh дозволяє користувачам керувати конфігурацією агентів і відстежувати їхній статус. Наприклад, для кожної контрольованої кінцевої точки користувачі можуть визначати, які модулі агентів будуть увімкнені, які файли журналів читатимуться, які файли відстежуватимуться на предмет змін цілісності або які перевірки конфігурації виконуватимуться [9].

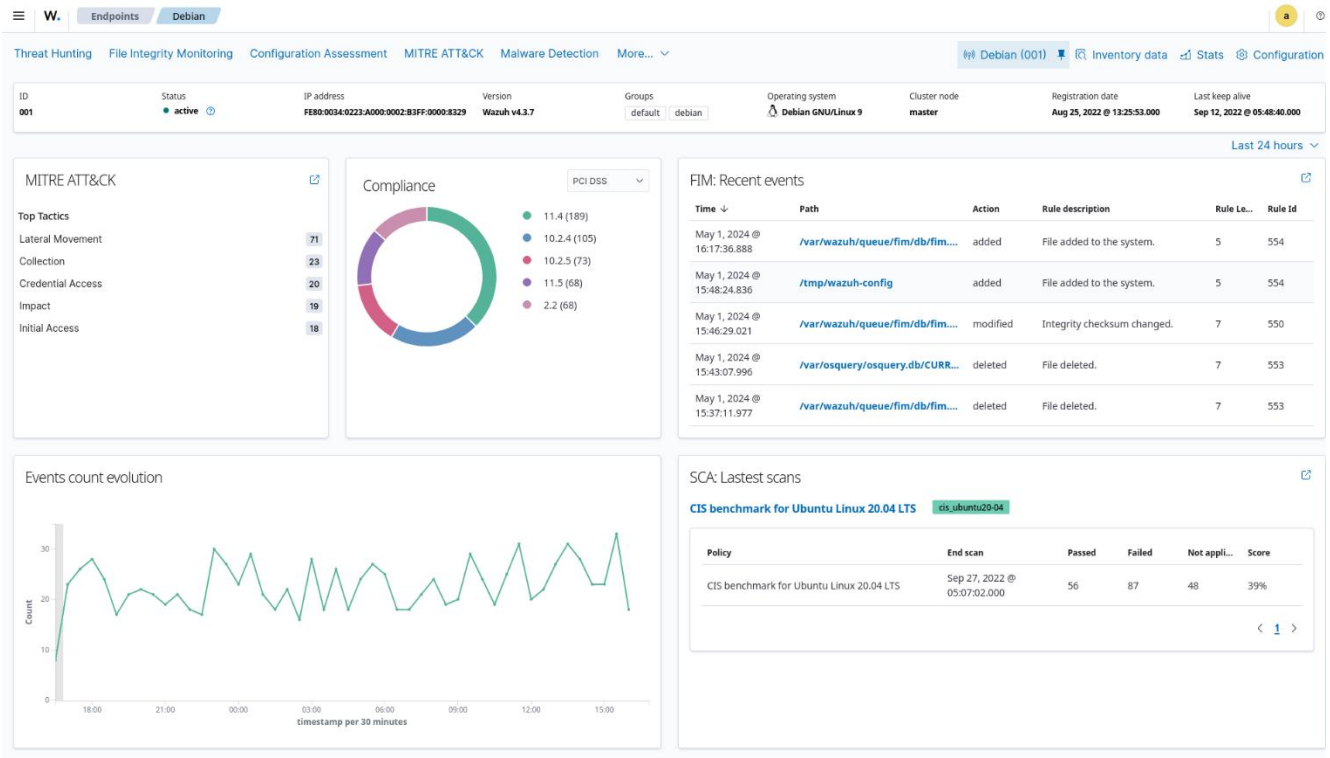


Рис. 2.3. Інформаційна панель Wazuh

Інформаційна панель Wazuh надає інтерфейс користувача, призначений для керування розгортанням Wazuh. Це включає моніторинг стану, журналів і статистики різних компонентів Wazuh. Він також включає налаштування сервера Wazuh і створення спеціальних правил і декодерів для аналізу журналів і виявлення загроз.

Інформаційна панель Wazuh містить інструмент перевірки набору правил, який може обробляти повідомлення журналу, щоб перевірити, як вони декодуються та чи відповідають вони правилу виявлення загроз чи ні. Ця функція особливо корисна, коли створено спеціальні декодери та правила, і користувач хоче їх протестувати.

Інформаційна панель Wazuh також містить консоль API для взаємодії користувачів з API Wazuh. Це можна використовувати для керування розгортанням Wazuh (наприклад, керування конфігураціями сервера чи агента, моніторинг стану та повідомлень журналу, додавання чи видалення агентів тощо).

Агент Wazuh працює в Linux, Windows, macOS, Solaris, AIX та інших операційних системах. Його можна розгорнути на ноутбуках, настільних

комп’ютерах, серверах, хмарних примірниках, контейнерах або віртуальних машинах. Агент допомагає захистити вашу систему, надаючи можливості запобігання загрозам, їх виявлення та реагування. Він також використовується для збору різних типів даних системи та програм, які він пересилає на сервер Wazuh через зашифрований та автентифікований канал.

Агент Wazuh має модульну архітектуру. Кожен компонент відповідає за свої власні завдання, включаючи моніторинг файлової системи, читання повідомлень журналу, збір даних інвентаризації, сканування конфігурації системи та пошук шкідливих програм. Користувачі можуть керувати модулями агентів за допомогою налаштувань конфігурації, адаптуючи рішення до своїх конкретних випадків використання.

На рисунку 2.4 показано архітектуру та компоненти агента.

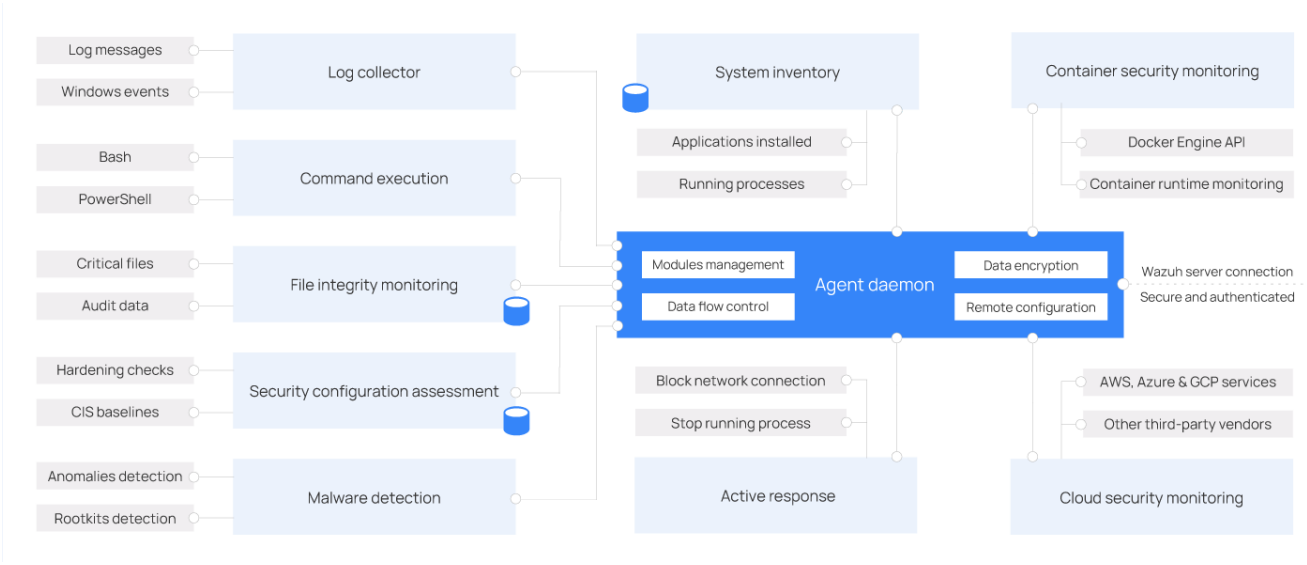


Рис. 2.4. Архітектура та компоненти агента Wazuh [9]

Усі модулі агентів можна налаштувати та виконувати різні завдання безпеки. Ця модульна архітектура дозволяє вмикати або вимикати кожен компонент відповідно до потреб безпеки. Нижче ви можете дізнатися про різні цілі всіх модулів агента.

Колектор логів: цей компонент агента може читати плоскі файли журналів і події Windows, збираючи повідомлення журналу операційної системи та програм.

Він підтримує фільтри XPath для подій Windows і розпізнає багаторядкові формати, такі як журнали аудиту Linux. Він також може збагачувати події JSON додатковими метаданими.

Виконання команд: агенти періодично запускають авторизовані команди, збирають їхні результати та повідомляють про них на сервер Wazuh для подальшого аналізу. Ми можемо використовувати цей модуль для різних цілей, наприклад для моніторингу вільного місця на жорсткому диску або отримання списку останніх користувачів, які входили в систему.

Моніторинг цілісності файлів (FIM): цей модуль відстежує файлову систему, повідомляючи про створення, видалення або зміну файлів. Він відстежує зміни в атрибутах файлів, дозволах, власності та вмісті. Коли відбувається подія, він фіксує подробиці про те, хто, що та коли в реальному часі. Крім того, модуль FIM створює та підтримує базу даних із станом відстежуваних файлів, що дозволяє виконувати запити віддалено.

Оцінка конфігурації безпеки (SCA): цей компонент забезпечує безперервну оцінку конфігурації, використовуючи стандартні перевірки на основі тестів Центру безпеки в Інтернеті (CIS). Користувачі також можуть створювати власні перевірки SCA, щоб контролювати та застосовувати свої політики безпеки.

Інвентаризація системи: цей модуль агента періодично виконує сканування, збираючи дані інвентаризації, такі як версія операційної системи, мережеві інтерфейси, запущені процеси, встановлені програми та список відкритих портів. Результати сканування зберігаються в локальних базах даних SQLite, які можна запитувати віддалено.

Виявлення зловмисного програмного забезпечення: використовуючи підхід без сигнатур, цей компонент здатний виявляти аномалії та можливу присутність руткітів. Крім того, він шукає приховані процеси, приховані файли та приховані порти під час моніторингу системних викликів.

Активна відповідь: цей модуль запускає автоматичні дії при виявленні загроз, ініціюючи відповіді на блокування мережевого з’єднання, зупинку запущеного процесу або видалення шкідливого файлу. Користувачі також можуть

створювати власні відповіді, коли це необхідно, і налаштовувати, наприклад, відповіді для запуску двійкового файлу в пісочниці, захоплення мережевого трафіку та сканування файлу антивірусом.

Моніторинг безпеки контейнера: цей модуль агента інтегровано з API Docker Engine для моніторингу змін у контейнерному середовищі. Наприклад, він виявляє зміни в зображеннях контейнерів, конфігурації мережі або обсягах даних. Крім того, він сповіщає про контейнери, що працюють у привілейованому режимі, і про користувачів, які виконують команди у запущеному контейнері.

Моніторинг хмарної безпеки: цей компонент відстежує хмарні постачальники, такі як Amazon Web Services, Microsoft Azure або Google GCP. Він нативно спілкується з їхніми API. Він здатний виявляти зміни в хмарній інфраструктурі (наприклад, створюється новий користувач, змінюється група безпеки, зупиняється хмарний екземпляр тощо) і збирати дані журналу хмарних служб (наприклад, AWS Cloudtrail, AWS Macie, AWS GuardDuty, Azure Active Directory тощо)

Агент Wazuh зв’язується з сервером Wazuh для передачі зібраних даних і подій, пов’язаних із безпекою. Крім того, агент надсилає оперативні дані, повідомляючи про свою конфігурацію та статус. Після підключення агент можна оновлювати, контролювати та налаштовувати віддалено з сервера Wazuh.

Зв'язок агента з сервером відбувається через захищений канал (TCP або UDP), що забезпечує шифрування та стиснення даних у реальному часі. Крім того, він містить механізми керування потоком, щоб уникнути затоплення, постановки подій у чергу, коли це необхідно, і захист пропускної здатності мережі.

Нам потрібно зареєструвати агента перед першим підключенням до сервера. Цей процес надає агенту унікальний ключ, який використовується для автентифікації та шифрування даних.

2.3. Порядок функціонування рішення Wazuh

Архітектура Wazuh базується на агентах, які працюють на контрольованих кінцевих точках і передають дані безпеки на центральний сервер. Безагентні пристрої, такі як брандмауери, комутатори, маршрутизатори та точки доступу, підтримуються та можуть активно надсилати дані журналу через Syslog, SSH або за допомогою свого API. Центральний сервер декодує та аналізує вхідну інформацію та передає результати в індексатор Wazuh для індексування та зберігання [9].

Кластер індексатора Wazuh – це набір з одного або кількох вузлів, які спілкуються один з одним для виконання операцій читання та запису в індексах. Невеликі розгортання Wazuh, які не вимагають обробки великих обсягів даних, можуть бути легко оброблені кластером з одним вузлом. Багатохостові кластери рекомендуються, якщо є багато контрольованих кінцевих точок, коли очікується великий обсяг даних або коли потрібна висока доступність.

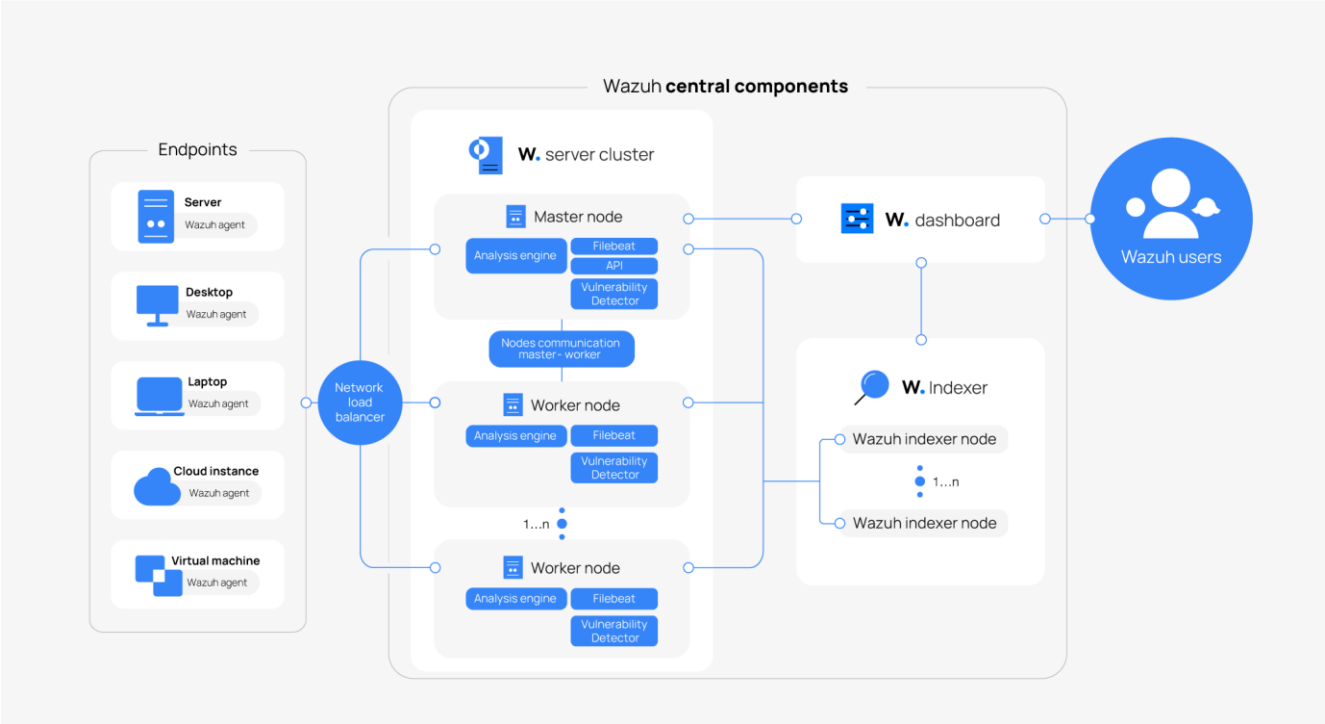


Рис. 2.5. Архітектура рішення Wazuh [9]

Для робочих середовищ рекомендується розгортати сервер Wazuh та індексатор Wazuh на різних хостах. У цьому сценарії Filebeat використовується для безпечного пересилання сповіщень Wazuh і заархівованих подій до кластера індексатора Wazuh (з одним або кількома вузлами) за допомогою шифрування TLS [9].

На рисунку 2.5 показано архітектуру розгортання Wazuh. Ми бачимо компоненти рішення та те, як сервер Wazuh і вузли індексатора Wazuh можуть бути налаштовані як кластери, забезпечуючи балансування навантаження та високу доступність.

Агент Wazuh постійно надсилає події на сервер Wazuh для аналізу та виявлення загроз. Щоб розпочати надсилання цих даних, агент встановлює з’єднання зі службою сервера для підключення агента, який прослуховує порт 1514 за замовчуванням (це можна налаштувати). Потім сервер Wazuh декодує та перевіряє за правилами отримані події, використовуючи механізм аналізу. Події, які запускають правило, доповнюються даними попередження, такими як ідентифікатор правила та назва правила. Події можуть бути передані в один або обидва файли, залежно від того, чи спрацьовує правило [9]:

файл */var/ossec/logs/archives/archives.json* містить усі події незалежно від того, чи спрацювало вони правило чи ні;

файл */var/ossec/logs/alerts/alerts.json* містить лише події, які спрацювали за правилом із достатньо високим пріоритетом (поріг можна налаштувати).

Протокол повідомлень Wazuh за замовчуванням використовує шифрування AES із 128 бітами на блок і 256-бітними ключами. Шифрування Blowfish необов’язкове.

Розглянемо взаємодію сервера та індексатора Wazuh.

Сервер Wazuh використовує Filebeat для безпечної передачі даних попереджень і подій до індексатора Wazuh за допомогою шифрування TLS. Filebeat відстежує вихідні дані з сервера Wazuh і пересилає їх до індексатора Wazuh, який за замовчуванням слухає порт 9200/TCP. Після індексації ми можемо проаналізувати та візуалізувати дані на інформаційній панелі Wazuh.

Модуль виявлення вразливостей оновлює список вразливостей. Він також генерує сповіщення, надаючи інформацію про вразливі місця системи.

Інформаційна панель Wazuh запитує Wazuh RESTful API (за замовчуванням прослуховує порт 55000/TCP на сервері Wazuh), щоб відобразити конфігурацію та інформацію про стан сервера та агентів Wazuh. Він також може змінювати параметри конфігурації агентів або сервера через виклики API. Цей зв'язок шифрується за допомогою TLS і автентифікується за допомогою імені користувача та пароля.

Кілька служб використовуються для зв'язку компонентів Wazuh. В таблиці 2.2 наведено список стандартних портів, які використовуються цими службами. За потреби користувачі можуть змінювати ці номери портів.

Таблиця 2.2

Список стандартних портів, які використовуються службами Wazuh

Component	Port	Protocol	Purpose
Wazuh server	1514	TCP (default)	Agent connection service
	1514	UDP (optional)	Agent connection service (disabled by default)
	1515	TCP	Agent enrollment service
	1516	TCP	Wazuh cluster daemon
	514	UDP (default)	Wazuh Syslog collector (disabled by default)
	514	TCP (optional)	Wazuh Syslog collector (disabled by default)
	55000	TCP	Wazuh server RESTful API
Wazuh indexer	9200	TCP	Wazuh indexer RESTful API
	9300-9400	TCP	Wazuh indexer cluster communication
Wazuh dashboard	443	TCP	Wazuh web user interface

Архівне зберігання даних. Як сповіщення, так і події, що не стосуються сповіщень, 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 та підписуються за допомогою контрольних сум MD5, SHA1 і SHA256. Структура каталогу та імені файлу така [9]:

root@wazuh-manager:/var/ossec/logs/archives/2022/Jan# ls -l

Рекомендується ротація та резервне копіювання архівних файлів відповідно до обсягу пам’яті сервера Wazuh. Використовуючи завдання cron, ми можемо легко зберігати лише певний часовий проміжок архівних файлів локально на сервері, наприклад, минулого року чи останніх трьох місяців.

З іншого боку, ми можемо відмовитися від зберігання архівних файлів і просто покладатися на індексатор Wazuh для зберігання архіву. Ця альтернатива може бути кращою, якщо ви періодично виконуєте резервне копіювання моментальних знімків індексатора Wazuh і/або маєте багатовузловий кластер індексатора Wazuh із копіями фрагментів для високої доступності. Ми навіть можемо використовувати завдання cron, щоб перемістити зроблені знімки індексів на кінцевий сервер зберігання даних і підписати їх за допомогою алгоритмів хешування MD5, SHA1 і SHA256.

3 ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА БАЗІ WAZUH

3.1. Технологія виявлення шкідливих програм із застосуванням рішення Wazuh

За допомогою рішення Wazuh ми можемо виявити функціонування шкідливих програм.

Шкідливе програмне забезпечення відноситься до будь-якого програмного забезпечення, спеціально розробленого для шкоди або використання комп’ютерних систем, мереж або користувачів. Воно створюється з наміром отримати несанкціонований доступ, завдати шкоди, викрасти конфіденційну інформацію або виконати інші шкідливі дії в цільовій системі. Існують різні типи шкідливих програм, кожна з яких має певні функції та методи зараження. Деякі поширені типи шкідливого програмного забезпечення включають віруси, хробаки, програми-вимагачі, ботнети, шпигунські програми, трояни та руткіти.

Виявлення шкідливого програмного забезпечення має вирішальне значення для захисту комп’ютерних систем і мереж від кіберзагроз. Це допомагає виявляти та запобігати шкідливому програмному забезпеченню, яке може спричинити втечу даних, компрометацію системи та фінансові втрати.

Традиційні методи, які покладаються виключно на виявлення на основі сигнатур, мають обмеження та не можуть виявити нові загрози. Підходи на основі сигнатур борються з виявленням атак нульового дня, поліморфних шкідливих програм та інших методів ухилення, які використовують суб’єкти загроз. У результаті організації ризикують отримати невиявлені зломи та викрадання даних. Wazuh дає змогу організаціям виявляти та ефективно реагувати на складні та обхідні загрози. Wazuh охоплює різні модулі, які ідентифікують властивості шкідливого програмного забезпечення, дії, мережеві підключення тощо.

Розглянемо порядок виявлення шкідливих дій за допомогою правил

виявлення загроз рішення Wazuh.

У Wazuh є правила виявлення загроз, які дозволяють виявляти шкідливе програмне забезпечення на основі поведінки. Замість того, щоб покладатися виключно на попередньо визначені сигнатури, Wazuh зосереджується на моніторингу та аналізі ненормальної поведінки шкідливих програм. Це дозволяє Wazuh виявляти відомі та раніше невідомі загрози. Таким чином Wazuh забезпечує проактивний і адаптований захист від кіберзагроз. У Wazuh є готові набори правил, спеціально розроблені для ініціювання сповіщень про розпізнані шаблони зловмисного програмного забезпечення, забезпечуючи швидку реакцію на потенційні інциденти безпеки. Наприклад, на зображенні нижче показано сповіщення з ідентифікатором правила 92213, яке спрацьовує, коли виконуваний файл опускається в папку, яка зазвичай використовується зловмисним програмним забезпеченням. Це сповіщення спонукає команди безпеки розпочати розслідування та процес усунення.

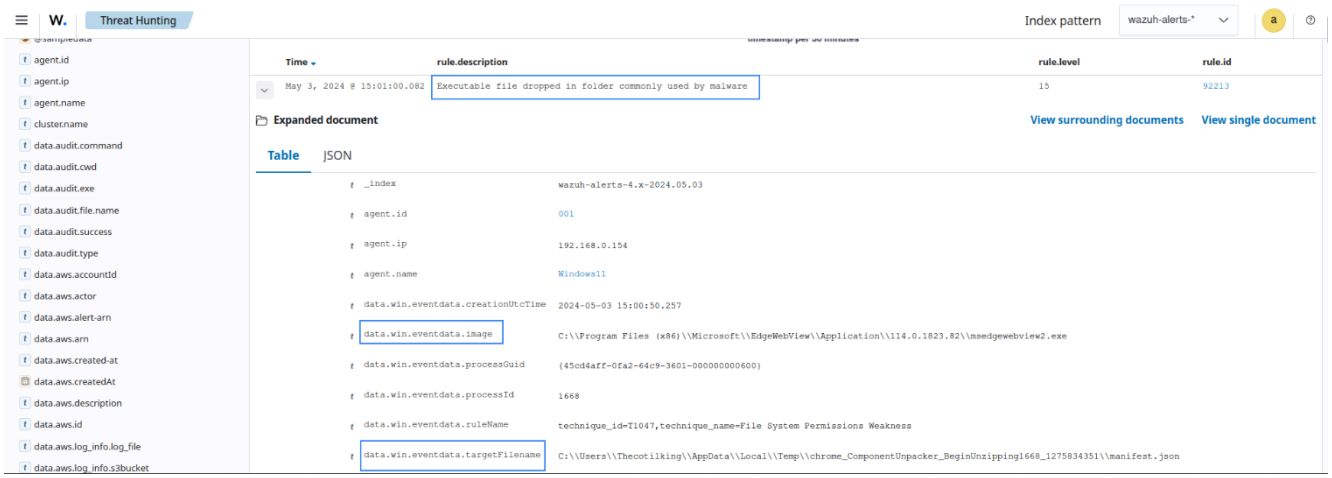


Рис. 3.1. Панель Threat Hunting

Рішення Wazuh дозволяє користувачам створювати власні правила для більшої гнучкості у виявленні, дозволяючи їм зосередитися на відповідних діях і оптимізуючи виявлення шкідливих програм. Wazuh декодує та організовує журнали від контрольованих кінцевих точок у поля, які потім можна використовувати для створення спеціальних правил для сповіщень у разі

виявлення зловмисної активності.

Правила Wazuh використовують кілька полів, які позначають індикатори компрометації (IoC), щоб зменшити помилкові спрацьовування та виявити відоме шкідливе програмне забезпечення на основі певної поведінки. Ці правила можуть пов'язувати пов'язані дії шкідливого програмного забезпечення, такі як вторгнення, ескалація привілеїв, бічний рух, обфускація та ексфільтрація для комплексного виявлення.

Нижче наведено приклад деяких спеціальних правил Wazuh, створених для попередження про зловмисну діяльність шкідливого програмного забезпечення LimeRAT [9]:

```
<group name="lime_rat,sysmon,">

  <!-- Rogue create netflix.exe creation -->
  <rule id="100024" level="12">
    <if_sid>61613</if_sid>
    <field name="win.eventdata.image" type="pcre2">\.exe</field>
    <field name="win.eventdata.targetFilename" type="pcre2">(?i)[c-z]:\\\\Users\\\\.+\\\\AppData\\\\Roaming\\\\check
    <description>Potential LimeRAT activity detected: checker netflix.exe created at $(win.eventdata.targetFilename)
    <mitre>
      <id>T1036</id>
    </mitre>
  </rule>

  <!-- Registry key creation for persistence -->
  <rule id="100025" level="12">
    <if_group>sysmon</if_group>
    <field name="win.eventdata.details" type="pcre2">(?i)[c-z]:\\\\Users\\\\.+\\\\AppData\\\\Roaming\\\\checker netf
    <field name="win.eventdata.targetObject" type="pcre2" >HKU\\\\.+\\\\Software\\\\Microsoft\\\\Windows\\\\CurrentV
    <field name="win.eventdata.eventType" type="pcre2" >^SetValue$</field>
    <description>Potential LimeRAT activity detected:  $(win.eventdata.details) added itself to the Registry as a st
    <mitre>
      <id>T1547.001</id>
    </mitre>
  </rule>

  <!-- Network activity detection -->
  <rule id="100026" level="12">
    <if_sid>61605</if_sid>
    <field name="win.eventdata.image" type="pcre2">(?i)[c-z]:\\\\Users\\\\.+\\\\AppData\\\\Roaming\\\\checker netfli
    <description>Potential LimeRAT activity detected: Suspicious DNS query made by $(win.eventdata.image).</descript
    <mitre>
      <id>T1572</id>
    </mitre>
  </rule>
```

```
<!-- Rogue create netflix.exe creation -->
<rule id="100024" level="12">
  <if_sid>61613</if_sid>
  <field name="win.eventdata.image" type="pcre2">\.exe</field>
  <field name="win.eventdata.targetFilename" type="pcre2">(?i)[c-z]:\\\\Users\\\\.+\\\\AppData\\\\Roaming\\\\check
  <description>Potential LimeRAT activity detected: checker netflix.exe created at $(win.eventdata.targetFilename)
  <mitre>
    <id>T1036</id>
  </mitre>
</rule>

<!-- Registry key creation for persistence -->
<rule id="100025" level="12">
  <if_group>sysmon</if_group>
  <field name="win.eventdata.details" type="pcre2">(?i)[c-z]:\\\\Users\\\\.+\\\\AppData\\\\Roaming\\\\checker netf
  <field name="win.eventdata.targetObject" type="pcre2" >HKU\\\\.+\\\\Software\\\\Microsoft\\\\Windows\\\\CurrentV
  <field name="win.eventdata.eventType" type="pcre2" >^SetValue$</field>
  <description>Potential LimeRAT activity detected:  $(win.eventdata.details) added itself to the Registry as a st
  <mitre>
    <id>T1547.001</id>
  </mitre>
</rule>

<!-- Network activity detection -->
<rule id="100026" level="12">
  <if_sid>61605</if_sid>
  <field name="win.eventdata.image" type="pcre2">(?i)[c-z]:\\\\Users\\\\.+\\\\AppData\\\\Roaming\\\\checker netfli
  <description>Potential LimeRAT activity detected: Suspicious DNS query made by $(win.eventdata.image).</descript
  <mitre>
    <id>T1572</id>
  </mitre>
</rule>


<!-- LimeRAT service creation -->
<rule id="100028" level="12">
  <if_sid>61614</if_sid>
  <field name="win.eventdata.targetObject" type="pcre2" >HKLM\\\\System\\\\CurrentControlSet\\\\Services\\\\disk</
  <field name="win.eventdata.eventType" type="pcre2" >^CreateKey$</field>
  <description>Potential LimeRAT activity detected: LimeRAT service $(win.eventdata.targetObject) has been created
    <mitre>
  <id>T1543.003</id>
    </mitre>
</rule>

/group>
```

Ці правила створюють сповіщення, які відображаються в модулі пошуку загроз на інформаційній панелі Wazuh.

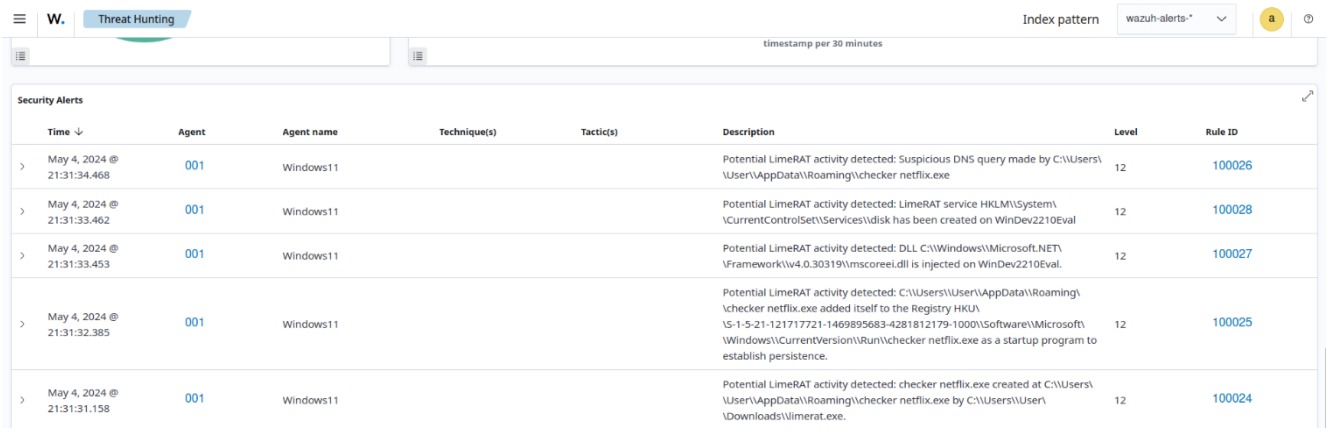


Рис. 3.2. Сповіщення, які відображаються в модулі пошуку загроз на інформаційній панелі Wazuh

Wazuh визначає поведінку, що вказує на шкідливе програмне забезпечення, генерує попередження та сповіщення в реальному часі, що дозволяє командам безпеки швидко реагувати та зменшувати потенційні ризики до їх ескалації.

Використання моніторингу цілісності файлів для виявлення шкідливих програм.

Моніторинг цілісності файлів (FIM) є цінним компонентом у виявленні шкідливих програм. Wazuh надає можливості FIM для моніторингу та виявлення змін у файлах і каталогах на контрольованих кінцевих точках. Ці зміни включають створення, модифікацію або видалення. Хоча FIM надає важливу інформацію, поєднання його з іншими можливостями та інтеграціями ще більше підвищує його ефективність у виявленні зловмисного програмного забезпечення. Wazuh дозволяє групам безпеки створювати власні правила на основі подій FIM, що дозволяє цільове виявлення шкідливих програм. Ці настроювані правила співвідносять події FIM із певними індикаторами компрометації, такими як підозрілі розширення файлів, фрагменти коду чи відомі сигнатури шкідливих програм.

На рисунку 3.3 показано сповіщення, коли веб-оболонка створює або змінює файл на веб-сервері.

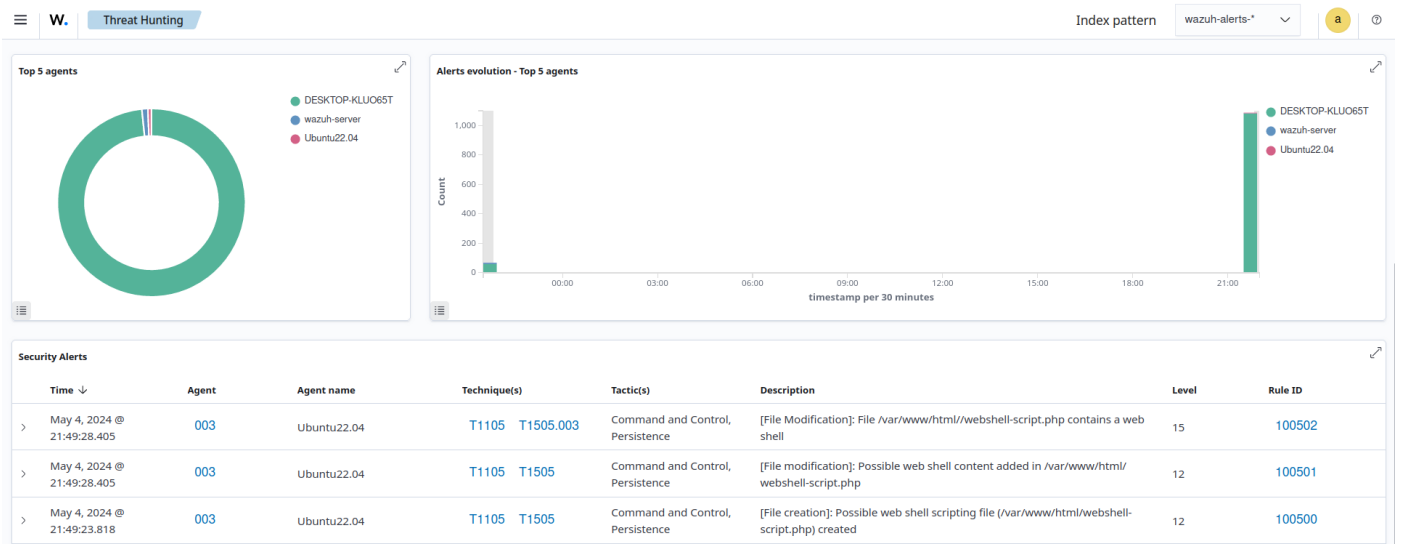
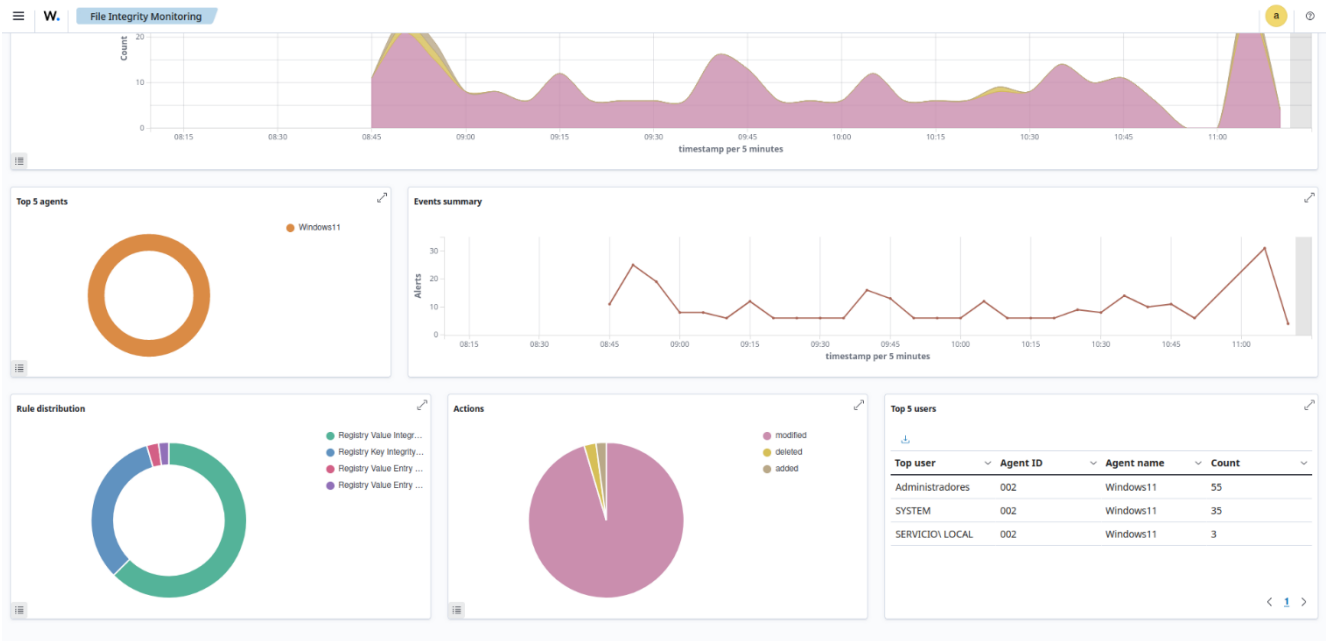


Рис. 3.3. Сповіщення, коли веб-оболонка створює або змінює файл на веб-сервері

Шкідливе програмне забезпечення часто націлюється на реєстр Windows, щоб досягти зловмисних цілей, таких як встановлення стійкості та виконання інших шкідливих дій. Модуль моніторингу цілісності файлів (FIM) Wazuh включає моніторинг реєстру Windows , який відстежує типові шляхи до реєстру для виявлення змін. Коли відбуваються зміни, модуль FIM ініціює сповіщення в режимі реального часу, дозволяючи командам безпеки швидко виявляти підозрілі маніпуляції з ключами реєстру та реагувати на них.

На рисунку 3.4 показано інформаційну панель модуля Wazuh FIM і події змін реєстру Windows.



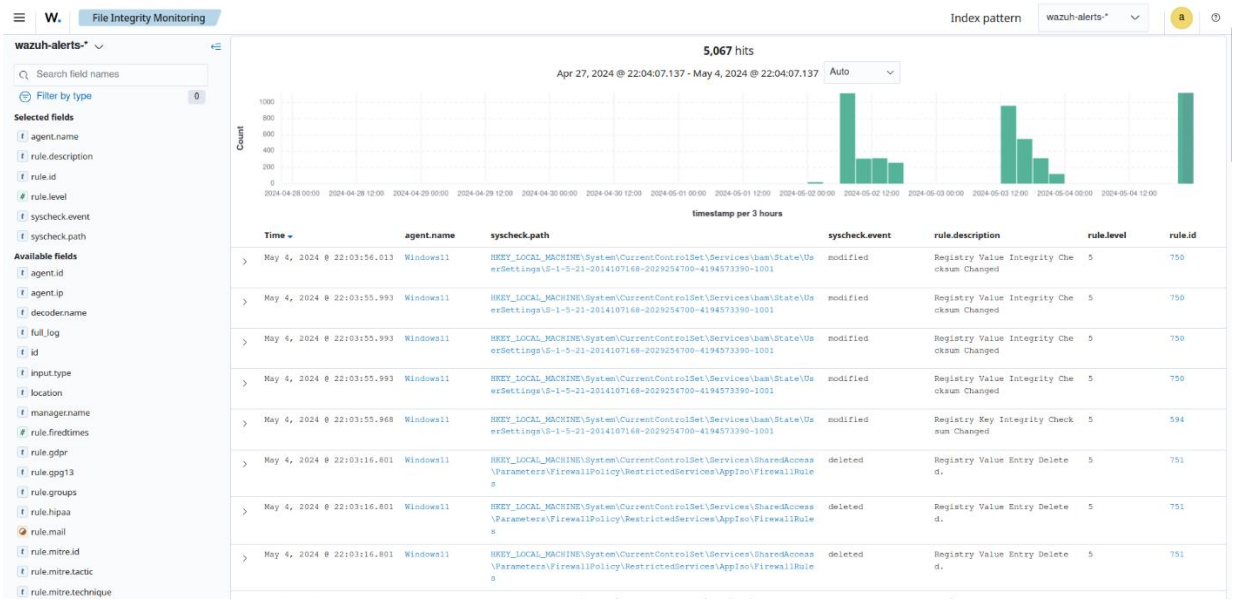


Рис. 3.4. Інформаційна панель модуля Wazuh FIM і події змін реєстру Windows

Покращення виявлення шкідливого програмного забезпечення за допомогою інтеграції аналізу загроз.

Користувачі можуть розширити свої можливості виявлення шкідливого програмного забезпечення за допомогою інтеграції з джерелами аналізу загроз. Ці розвідувальні канали збагачують базу знань Wazuh додатковою актуальною інформацією про відомі шкідливі IP-адреси, домени, URL-адреси та інші показники компрометації. Приклади джерел аналізу загроз, з якими Wazuh може інтегруватися, включають VirusTotal, MISP тощо.

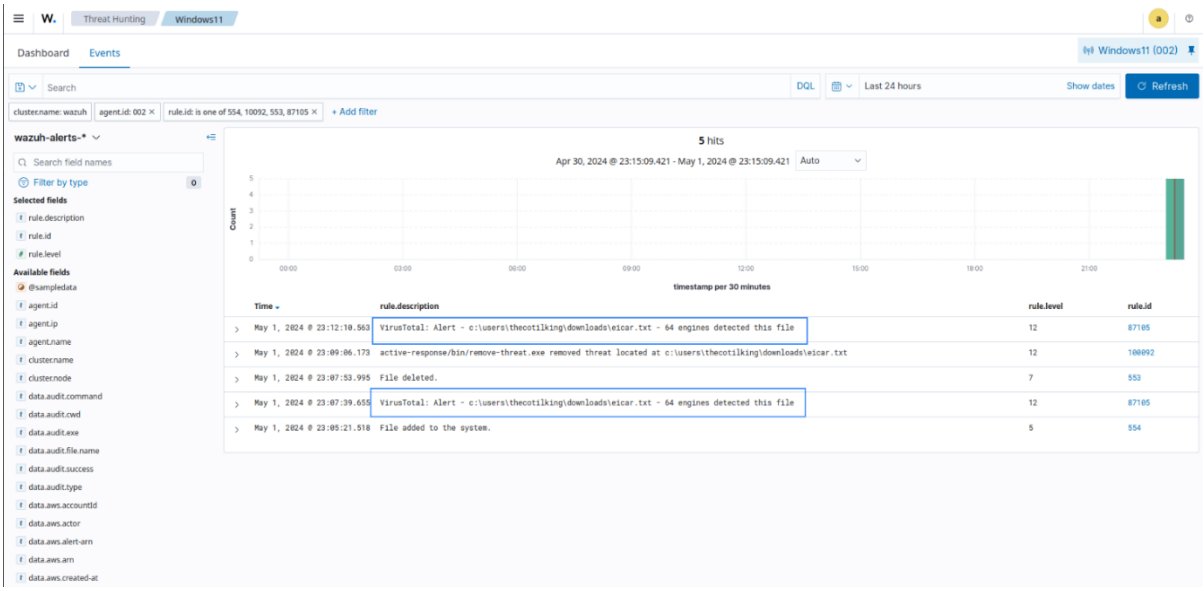


Рис. 3.5. Приклад інтеграції з джерелами аналізу загроз

Wazuh активно ідентифікує шкідливі файли, порівнюючи ідентифіковані IoC з інформацією, що зберігається в списках CDB (постійних базах даних). Ці списки можуть зберігати відомі індикатори шкідливого програмного забезпечення (IoC), включаючи хеші файлів, IP-адреси та доменні імена.

Ми можете налаштувати записи у форматі *key:value* або *key:* для індивідуального виявлення, приклад такого показаний нижче. Для виявлення використовується список CBD, що містить відомі хеші шкідливих програм MD5 для шкідливих програм Mirai та Xbash:

```
e0ec2cd43f71c80d42cd7b0f17802c73:mirai
55142f1d393c5ba7405239f232a6c059:Xbash
```

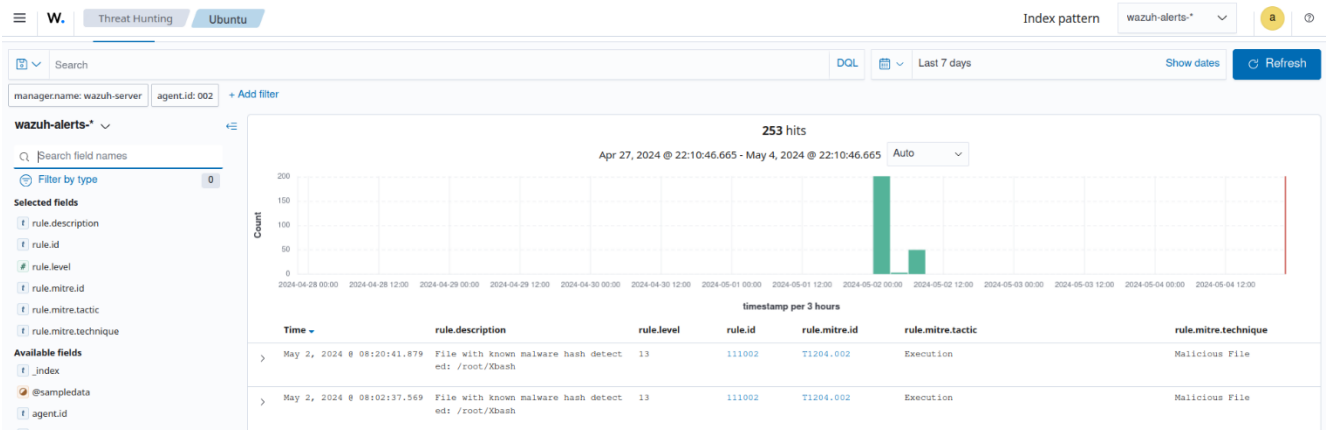


Рис. 3.6. Панель ідентифікації шкідливих файлів

Виявлення прихованих загроз за допомогою виявлення руткітів.

Руткіти – це зловмисне програмне забезпечення, призначене для приховування присутності шкідливого програмного забезпечення на кінцевій точці шляхом маніпулювання функціями операційної системи, такими як зміна системних викликів або модифікація структур даних ядра. Wazuh має модуль Rootcheck , який періодично сканує контрольовану кінцеву точку для виявлення руткітів як на рівні ядра, так і на рівні простору користувача. Rootcheck визначає й попереджає про потенційну активність руткітів. Аналізуючи поведінку системи та порівнюючи її з відомими шаблонами руткітів, Wazuh миттєво виявляє шаблони, пов’язані з руткітами, і створює сповіщення для подальшого

дослідження.

Нижче ми показуємо приклад сповіщення, яке створює модуль Wazuh Rootcheck, коли він виявляє аномалію у файловій системі:

```
** Alert 1668497750.1838326: - ossec,rootcheck,pci_dss_10.6.1,gdpr_IV_35.7.d,
2022 Nov 15 09:35:50 (Ubuntu) any->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
Rootkit 't0rn' detected by the presence of file '/usr/bin/.t0rn'.
title: Rootkit 't0rn' detected by the presence of file '/usr/bin/.t0rn'.
```

Незважаючи на те, що Wazuh продовжує покращувати свої можливості виявлення поведінки руткітів , модуль моніторингу команд також можна налаштувати для моніторингу дій командного рядка в кінцевих точках, дозволяючи виявляти зловмисні команди та дії зловмисного програмного забезпечення. Цей модуль надає організаціям комплексний підхід до виявлення прихованих загроз і ефективного захисту своїх систем.

Система моніторингу вимагає виявлення шкідливих програм і аномалій.

Wazuh відстежує системні виклики на кінцевих точках Linux, щоб покращити виявлення шкідливих програм і допомогти у виявленні аномалій. Wazuh використовує систему аудиту Linux для моніторингу системних викликів.

Моніторинг системних викликів у поєднанні з моніторингом цілісності файлів Wazuh (FIM) та інтеграцією аналізу загроз покращує виявлення шкідливих програм. Він фіксує важливі для безпеки події, такі як доступ до файлів, виконання команд і підвищення привілеїв, надаючи інформацію про потенційні інциденти безпеки в реальному часі. Цей комплексний підхід посилює стійкість організацій до кібербезпеки. На рисунку 3.7 показано візуалізація сповіщення про зловживання привілеями на інформаційній панелі Wazuh для Ubuntu Linux 22.04.

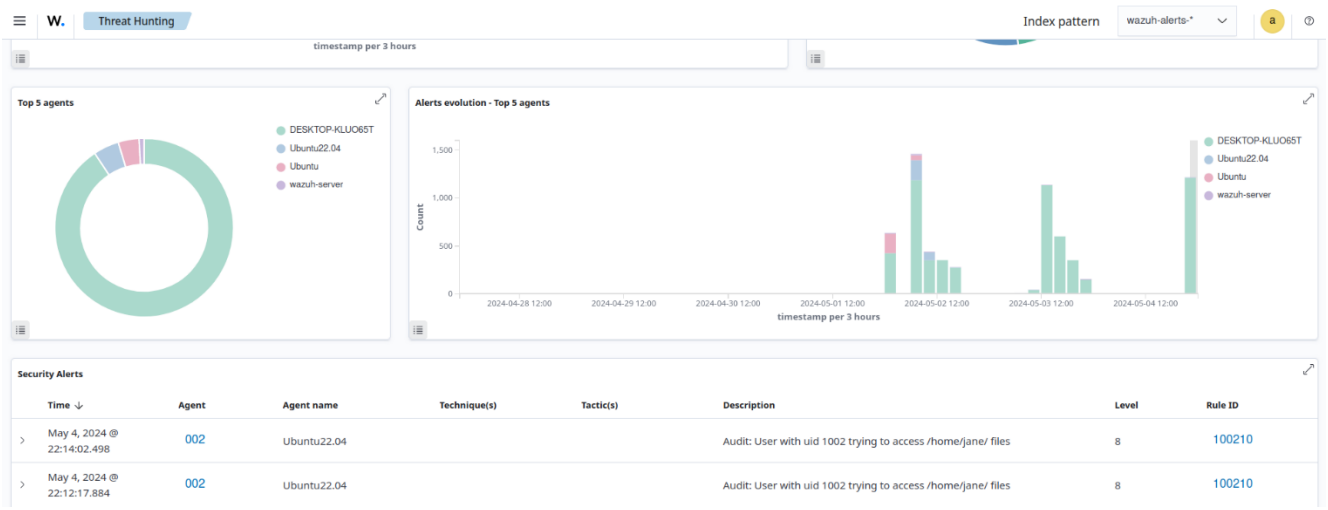


Рис. 3.7. Сповіщення про зловживання привілеями

Отже, рішення Wazuh надає командам безпеки можливість використовувати правила аудиту, надані Auditd. Створення власних правил на основі подій системних викликів покращує виявлення шкідливого програмного забезпечення та підвищує загальну стійкість кібербезпеки.

3.2. Технологія реагування на інциденти із застосуванням рішення Wazuh

Інцидент безпеки стосується будь-якої несприятливої події чи діяльності, яка ставить під загрозу конфіденційність, цілісність або доступність цифрових активів, мереж, даних або ресурсів. Такі інциденти включають несанкціонований доступ, витік даних, зараження шкідливим програмним забезпеченням, атаки на відмову в обслуговуванні та будь-які інші дії, які ставлять під загрозу безпеку інформаційно-технологічного середовища організації [9].

Мета реагування на інциденти полягає в тому, щоб ефективно впоратися з інцидентом безпеки та якомога швидше відновити нормальну роботу бізнесу. Оскільки цифрові активи організацій постійно зростають, управління інцидентами вручну стає дедалі складнішим, отже, потреба в автоматизації [9].

Автоматизоване реагування на інциденти передбачає автоматичні дії, які виконуються під час реагування на інциденти безпеки. Ці дії можуть включати ізоляцію скомпрометованих кінцевих точок, блокування шкідливих IP-адрес, розміщення заражених пристроїв на карантині або вимкнення скомпрометованих облікових записів користувачів. Автоматизуючи реагування на інциденти, групи кібербезпеки скорочують час реагування на виявлені загрози, запобігають або мінімізують вплив інцидентів і ефективно обробляють велику кількість подій безпеки [9].

Модуль Wazuh Active Response дозволяє користувачам запускати автоматизовані дії при виявленні інцидентів на кінцевих точках. Це покращує процеси реагування на інциденти в організації, дозволяючи командам безпеки вживати негайних автоматизованих дій для протидії виявленим загрозам.

Ми також можемо налаштувати дії як зі збереженням стану, так і без збереження стану. Активні відповіді без збереження стану є одноразовими діями, тоді як відповіді зі збереженням стану повертають свої дії через деякий час.

Активні дії реагування за замовчуванням.

Готові сценарії доступні в кожній операційній системі, яка запускає агенти Wazuh. Деякі зі стандартних сценаріїв активної відповіді показано в таблиці 3.1.

Таблиця 3.1

Деякі зі стандартних сценаріїв активної відповіді

Назва сценарію	Опис
disable-account	Відключає обліковий запис користувача
firewall-drop	Додає IP-адресу до списку заборонених iptables.
firewall-drop	Додає IP-адресу до спадного списку брандмауера.
restart.sh	Перезапускає агент або сервер Wazuh.
netsh.exe	Блокує IP-адресу за допомогою netsh.

Настроювані дії активної відповіді.

Однією з переваг модуля Wazuh Active Response є його адаптивність. Wazuh дозволяє командам безпеки створювати власні активні дії відповіді на будь-якій

мові програмування, пристосовуючи їх до своїх конкретних потреб. Це гарантує, що при виявленні загрози відповідь може бути налаштована відповідно до вимог організації.

Автоматизація реагування на інциденти за допомогою Wazuh.

Щоб використовувати модуль Wazuh Active Response, нам потрібно налаштувати дію, яка буде виконуватися, коли на контрольованій кінцевій точці відбувається певна подія. Наприклад, ми можемо налаштувати модуль Wazuh Active Response на видалення зловмисного виконуваного файлу із зараженої кінцевої точки. У наведених нижче прикладах ми показуємо, як модуль Wazuh Active Response обробляє різні інциденти.

Видалення шкідливих програм.

Ми можемо використовувати модуль Wazuh Active Response у поєднанні з модулем моніторингу цілісності файлів та інтеграцією VirusTotal для виявлення та видалення шкідливих файлів із кінцевої точки.

На рисунку 3.8 показані такі дії:

1. Ідентифікатор правила 554 запускається, коли файл додається до Downloadskаталогу, який відстежується за допомогою модуля моніторингу цілісності файлів Wazuh.

2. Ідентифікатор правила 87105 спрацьовує, коли Wazuh витягує хеш файлу, запитує дані про хеш файлу з бази даних VirusTotal через свій API та отримує відповідь на зловмисний файл.

3. Ідентифікатор правила 553 запускається, коли файл видаляється з Downloadskаталогу, який відстежується за допомогою модуля моніторингу цілісності файлів Wazuh.

4. Ідентифікатор правила 11000 запускається, коли модуль Wazuh Active Response видаляє шкідливий файл із кінцевої точки.

У цьому сценарії модуль Wazuh Active Response автоматично видаляє шкідливий файл, скорочуючи час між виявленням загрози та пом’якшенням.

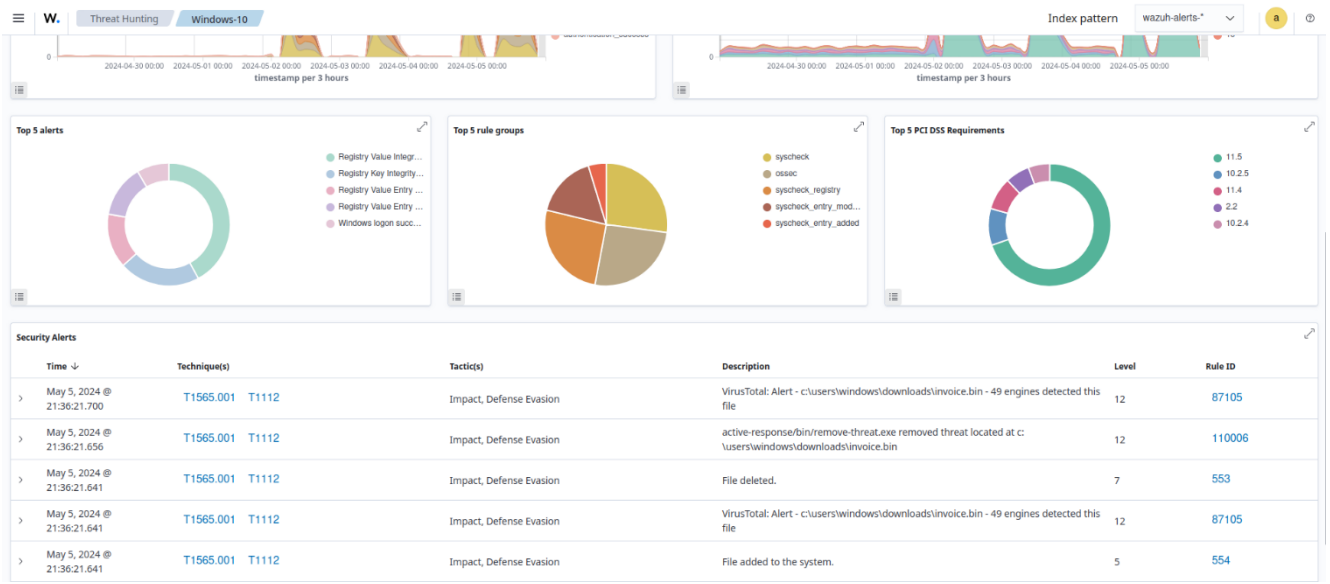


Рис. 3.8. Дії відповіді

Відповідь на DoS-атаки.

Основна мета DoS-атаки полягає в тому, щоб зробити ціль недоступною для законних користувачів, викликаючи відмову в обслуговуванні. На рисунку 3.9 показується, як модуль Wazuh Active Response блокує шкідливі IP-адреси, які виконують DoS проти веб-сервера на кінцевій точці Ubuntu.

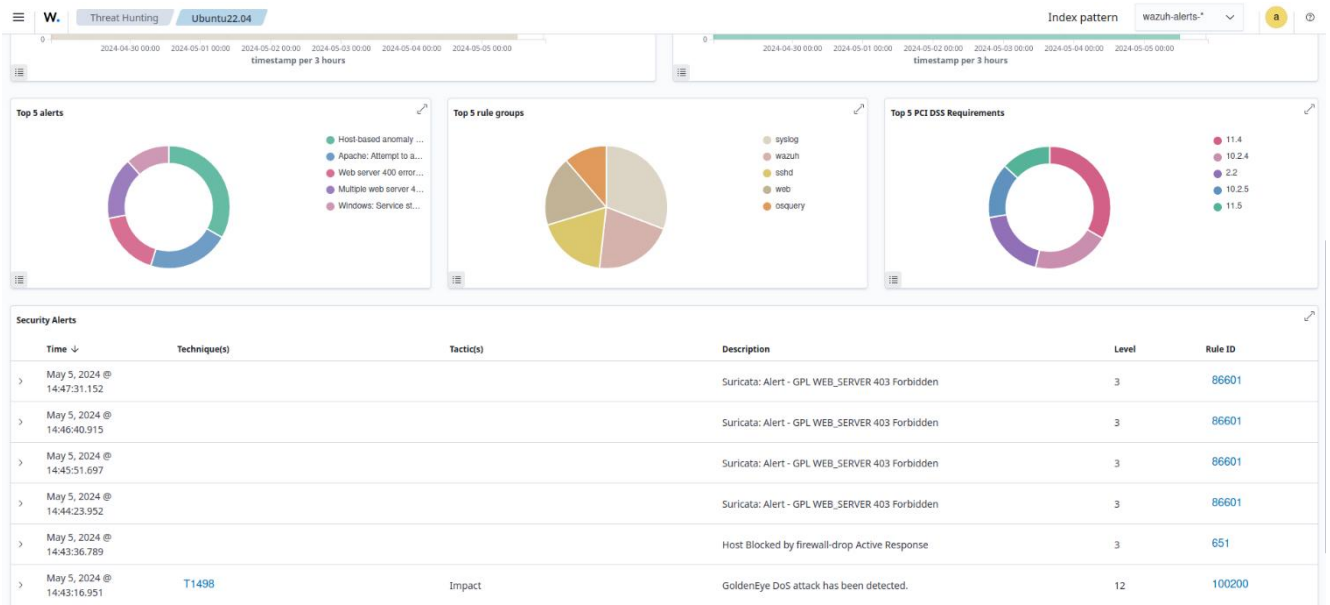


Рис. 3.9. Відповідь на DoS-атаку

У цьому випадку модуль Wazuh Active Response автоматично блокує

шкідливі хости від виклику DoS-атаки на веб-сервері. Таким чином забезпечується доступність веб-сервера для авторизованих користувачів.

Вимкнення облікового запису користувача після атаки грубої сили.

Блокування облікового запису – це захід безпеки, який використовується для захисту від атак грубої сили шляхом обмеження кількості спроб входу, які користувач може зробити протягом визначеного часу. Ми використовуємо модуль Wazuh Active Response, щоб вимкнути обліковий запис користувача, пароль якого вгадується зловмисником.

На рисунку 3.10 показано, як модуль Wazuh Active Response вимикає обліковий запис на кінцевій точці Linux і знову вмикає його через 5 хвилин.

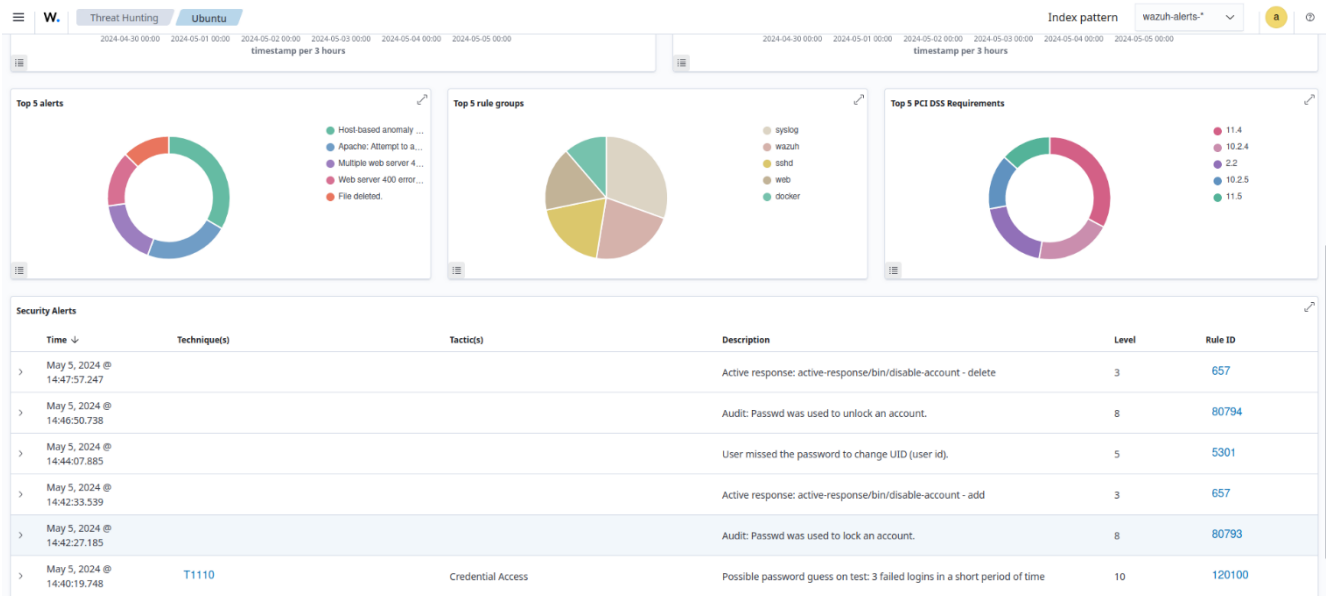


Рис. 3.10. Відповідь на атаку грубої сили

У цьому сценарії, коли зловмисник неодноразово намагається вгадати пароль користувача та не вдається, обліковий запис стає тимчасово недоступним. Це заважає зловмисникам, які покладаються на методи грубої сили, щоб вгадати паролі облікових записів користувачів.

Отже, використовуючи модуль Wazuh Active Response, фахівці можуть автоматизувати реагування на різні інциденти. Таким чином забезпечується ефективне реагування на інциденти.

3.3. Рекомендації щодо захисту кінцевих точок організації

Захист кінцевих точок є одним з найважливіших аспектів кібербезпеки організації. Адже саме через них злочинці найчастіше проникають в інформаційні системи. Треба мати на увазі, що будь-яка кінцева точка може стати потенційним входом для зловмисників.

Моніторинг та реагування на загрози є складовими частинами загального процесу забезпечення кібербезпеки з таких міркувань:

проактивний захист: завдяки постійному моніторингу можна виявити загрози на ранніх стадіях, ще до того, як вони завдадуть шкоди;

швидке реагування: чим швидше ми виявимо та усунемо загрозу, тим менше будуть збитки;

зменшення ризиків: регулярний моніторинг дозволяє виявити вразливості в системі та усунути їх, знижуючи загальний рівень ризику.

Для захисту кінцевих точок організацій необхідно застосовувати такі технології:

EDR: це комплексний підхід, який включає в себе:

виявлення: використання різноманітних методів для виявлення шкідливої активності на кінцевих точках;

аналіз: глибокий аналіз інцидентів для розуміння їхньої природи та масштабів;

реагування: автоматизація процесів реагування на інциденти.

UEBA (User and Entity Behavior Analytics): аналіз поведінки користувачів та систем для виявлення аномалій, які можуть вказувати на атаку.

Патч-менеджмент: регулярне оновлення програмного забезпечення для усунення відомих вразливостей.

Менеджмент привілеїв: контроль доступу до систем та даних на основі принципу найменших привілеїв.

Підвищення свідомості користувачів: навчання співробітників основним принципам кібербезпеки.

Для реалізації ефективного захисту кінцевих точок необхідно проводити такі заходи:

виберіть надійні рішення: при виборі EDR-систем, UEBA-розв'язків та інших інструментів звертайте увагу на їх функціональність, інтеграцію з іншими системами та відгуки користувачів;

створіть план реагування на інциденти: розробіть детальний план дій на випадок виявлення кібератаки;

регулярне проведення навчання співробітників: навчайте співробітників основним принципам кібербезпеки та правилам поведінки в мережі;

проводення регулярних аудитів: оцінюйте ефективність системи захисту та вносьте необхідні зміни.

Важливо розуміти, що жодна система не є абсолютно захищеною. Тому важливо поєднувати різні засоби захисту та регулярно оновлювати свою стратегію кібербезпеки.

Рішення з відкритим кодом, такі як Wazuh, мають ряд переваг: гнучкість, прозорість, активну спільноту та, часто, безкоштовність. Що слід враховувати при виборі рішення з відкритим кодом, такі як Wazuh:

функціональність: які саме функції вам потрібні (моніторинг файлів, системних викликів, мережевого трафіку тощо)?

масштабованість: чи зможе рішення масштабуватися разом з вашою інфраструктурою?

інтеграція: Чи легко інтегрується з іншими системами, які ви використовуєте?

підтримка: Який рівень підтримки ви можете очікувати від спільноти або комерційних провайдерів?

Для втілення рішення з відкритим кодом, такі як Wazuh, необхідно провести наступні заходи:

почніть з оцінки ваших потреб: визначте, які саме загрози ви хочете виявляти і які дані потрібно збирати;

оцініть ресурси: виберіть рішення, яке відповідає вашим технічним

можливостям і бюджету;

зверніться до спільноти: задайте питання на форумах та в чатах, щоб отримати рекомендації та допомогу;

розгляньте гібридний підхід: комбінуйте відкриті рішення з комерційними продуктами для отримання більш комплексного захисту.

Захист кінцевих точок є критично важливим для забезпечення кібербезпеки будь-якої організації. Ключовими рекомендаціями щодо моніторингу та реагування на загрози є:

1. Впровадження розширеного виявлення та реагування (EDR):

оберіть EDR-систему, яка відповідає вашим потребам та масштабам організації. Вона має забезпечувати детальний аналіз поведінки, виявлення аномалій та автоматизацію реагування;

об’єднайте EDR з іншими інструментами безпеки (SIEM, XDR, Firewall) для отримання більш повного уявлення про стан безпеки;

слідкуйте за оновленнями EDR-системи та баз даних загроз, щоб забезпечити захист від нових атак.

2. Аналіз поведінки користувачів та сутностей (UEBA):

створіть детальний профіль нормальної поведінки користувачів та систем;

використовуйте UEBA для виявлення відхилень від встановленої норми, які можуть вказувати на атаку;

ретельно розслідуйте всі виявлені аномалії, щоб підтвердити або спростувати наявність загрози.

3. Менеджмент патчів та вразливостей:

впровадьте автоматизовану систему управління патчами, щоб своєчасно усувати відомі вразливості;

пріоритезуйте встановлення патчів, які усувають критичні вразливості;

необхідно проводити регулярні аудити вразливостей для виявлення нових ризиків.

4. Керування привілеями:

надавайте користувачам тільки ті привілеї, які необхідні для виконання

їхніх обов’язків;

розділіть мережу на сегменти з різними рівнями доступу для обмеження поширення шкідливого програмного забезпечення;

періодично переглядайте та оновлюйте матрицю привілеїв.

5. Свідомість користувачів:

проводьте регулярні тренінги для співробітників з питань кібербезпеки;

використовуйте симуляції фішингових атак для оцінки рівня обізнаності співробітників;

розробіть чіткі політики безпеки та доводьте їх до відома всіх співробітників.

6. Резервне копіювання та відновлення:

регулярно створюйте резервні копії критичних даних;

регулярно тестуйте процедури відновлення для перевірки їхньої ефективності;

зберігайте резервні копії в безпечному місці, недоступному для зловмисників.

7. Реагування на інциденти:

розробіть детальний план реагування на інциденти, який включає в себе кроки, які необхідно виконати у разі виявлення загрози;

сформуйте команду реагування на інциденти, яка буде відповідати за розслідування та усунення наслідків кібератак;

регулярно переглядайте та вдосконалюйте план реагування на основі отриманого досвіду.

8. Відкриті джерела інформації:

слідкуйте за останніми новинами в галузі кібербезпеки та оперативно реагуйте на нові загрози;

беріть участь у обміні інформацією з іншими фахівцями з кібербезпеки.

Кібербезпека – це постійний процес, який вимагає постійної уваги та інвестицій. Необхідно регулярно оцінювати ефективність вжитих заходів безпеки та вносити необхідні зміни.

ВИСНОВКИ

В роботі досліджено проблему захисту кінцевих точок організації. Встановлено, що проблеми захисту кінцевих точок організацій є надзвичайно актуальними в сучасному цифровому світі, де кіберзагрози стають все більш витонченими та поширеними. Кінцеві точки (наприклад, комп'ютери, смартфони, планшети) є вразливими місцями в мережі будь-якої організації, оскільки через них зловмисники можуть отримати доступ до конфіденційних даних, порушити роботу систем та завдати значних фінансових збитків.

Визначено існуючі підходи до захисту кінцевих точок організації. Завдяки інтеграції виявлення, збагачення, аналізу та автоматизованого реагування в уніфікований робочий процес XDR значно покращує здатність організації виявляти і реагувати на інциденти безпеки до того, як станеться порушення. Використання цих можливостей забезпечує проактивний і комплексний підхід до кібербезпеки, захищаючи вашу організацію від нових загроз.

Проаналізовано існуючі рішення захисту кінцевих точок організації. Вибір оптимального рішення з відкритим кодом для моніторингу та захисту кінцевих точок залежить від багатьох факторів, включаючи розмір корпоративної інфраструктури, рівень досвіду команди фахівців, необхідні функціональні можливості та бюджет.

Рішення Wazuh надає функції XDR і SIEM для захисту робочих навантажень хмари, контейнера та сервера. Вони включають аналіз даних журналу, виявлення вторгнень і шкідливого програмного забезпечення, моніторинг цілісності файлів, оцінку конфігурації, виявлення вразливостей і підтримку нормативної відповідності. Рішення Wazuh складається з трьох центральних компонентів платформи та одного універсального агента.

В роботі розглянуто технологію виявлення шкідливих програм із застосуванням рішення Wazuh. Виявлення шкідливого програмного забезпечення має вирішальне значення для захисту комп’ютерних систем і мереж від

кіберзагроз. Це допомагає виявляти та запобігати шкідливому програмному забезпеченню, яке може спричинити втечу даних, компрометацію системи та фінансові втрати.

В роботі розглянуто технологію реагування на інциденти із застосуванням рішення Wazuh. Автоматизоване реагування на інциденти передбачає автоматичні дії, які виконуються під час реагування на інциденти безпеки. Ці дії можуть включати ізоляцію скомпрометованих кінцевих точок, блокування шкідливих IP-адрес, розміщення заражених пристроїв на карантині або вимкнення скомпрометованих облікових записів користувачів. Автоматизуючи реагування на інциденти, групи кібербезпеки скорочують час реагування на виявлені загрози, запобігають або мінімізують вплив інцидентів і ефективно обробляють велику кількість подій безпеки.

Розроблено рекомендації фахівцям з кібербезпеки щодо захисту кінцевих точок організації.

Таким чином, правильна реалізація технології захисту кінцевих точок організації має забезпечити ефективний захист корпоративних даних та кібербезпеку інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. 2024 Cisco Cybersecurity Readiness Index. URL: https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf

2. What is extended detection and response (XDR)? Microsoft. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-xdr

3. What Is Extended Detection and Response (XDR)? Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-extended-detection-response-XDR

4. XDR Architecture: What Is It and How to Implement. SentinelOne. November 5, 2024. URL: https://www.sentinelone.com/cybersecurity-101/endpoint-security/xdr-architecture/

5. Wazuh. The Open Source Security Platform. URL: https://wazuh.com/

6. OSSEC Documentation. 3.6.0. URL: https://www.ossec.net/docs/

7. Elasticsearch Guide. 8.17. URL: https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html

8. Graylog Docs. 6.0. URL: https://go2docs.graylog.org/6-0/what_is_graylog/what_is_graylog.htm

9. Wazuh. Getting started with Wazuh. Version 4.9. URL: https://documentation.wazuh.com/current/getting-started/index.html

10. Wazuh. User manual. Version 4.9. URL: https://documentation.wazuh.com/current/user-manual/index.html

11. Wazuh. Installation guide. Version 4.9. URL: https://documentation.wazuh.com/current/installation-guide/index.html

12. Active XDR protection from modern threats. Wazuh. URL: https://wazuh.com/platform/xdr/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)