План лекції . Тема 7. Впровадження систем моніторингу та безпеки ІТ-інфраструктури.

- Огляд Wazuh як відкритої платформи для моніторингу безпеки.
- Огляд Snort як системи виявлення та запобігання вторгненням (IDS/IPS).
- Огляд Splunk Enterprise Security.
- Огляд IBM QRadar
- Огляд Elastic Security
- Огляд MS SCOM як інструменту системного моніторингу від Microsoft.

Вступ.

Сучасна ІТ-інфраструктура є складною, багатокомпонентною системою, що постійно піддається ризикам як з боку зовнішніх атак, так і внутрішніх збоїв. Ефективний моніторинг стану інфраструктури та безпеки є критично важливим для забезпечення стабільності бізнес-процесів, попередження інцидентів і своєчасного реагування на загрози.

Сьогодні ми розглянемо ключові інструменти, які дозволяють організувати та автоматизувати процес моніторингу та забезпечення безпеки ІТ-середовища. Зокрема, познайомимося з відкритою платформою **Wazuh**, потужним рішенням **Splunk Enterprise Security**, платформою для аналізу загроз **IBM QRadar**, гнучким стеком **Elastic Security**, а також рішенням від Microsoft — **System Center Operations Manager** (SCOM).

Ці системи є прикладами як комерційних, так і відкритих рішень, кожне з яких має свої особливості й переваги. Вивчення їхніх можливостей дозволить вам обрати найбільш ефективний підхід до впровадження моніторингу та захисту в реальних умовах..

Огляд Wazuh як відкритої платформи для моніторингу безпеки

Wazuh - це відкрита платформа для моніторингу безпеки, яка поєднує в собі можливості ELK Stack та розширення Wazuh до ELK Stack для виявлення загроз безпеки та реагування на них. Нагадаю, що ELK Stack це комплект відкритих програмних рішень Elasticsearch, Logstash та Kibana.

Wazuh починався як проект, заснованої у 2015 році однойменної компанії, що розширює функціональність ELK Stack, додавши можливості моніторингу безпеки. В основі Wazuh лежить інтеграція з ELK Stack, що дозволяє збирати, аналізувати та візуалізувати журнальні дані безпеки.
З часом, розвиток проекту Wazuh призвів до того, що він став самостійною платформою для моніторингу безпеки, яка включає в себе не тільки ELK Stack, але й інші компоненти та функціонал. Таким чином, Wazuh не просто розширює ELK Stack, але створює власну платформу, спеціалізовану на моніторингу безпеки. Вона використовується для виявлення та реагування на загрози безпеки в ІТ-інфраструктурі.

Основні версії Wazuh:

- ✓ Wazuh 2.x: Випущений близько 2017 року.
- ✓ Wazuh 3.x: Був випущений приблизно в 2018 році.
- ✓ Wazuh 4.x: Остання версія, яка була випущена приблизно у 2020 році.

Ці роки є лише наближеними і можуть відрізнятися залежно від конкретних випусків підверсій та точних дат. На момент написання цього документу актуальна версія Wazuh – 4.7.2.

Платформа Wazuh надає функції захисту робочих навантажень хмари, контейнера та серверу за допомогою двох важливих інструментів кібербезпеки:

XDR (Extended Detection and Response):

- ✓ **Розширене виявлення та реагування**: XDR – це комплексна стратегія кібербезпеки, яка використовує дані з різних джерел для виявлення та реагування на кіберзагрози.
- ✓ **Консолідація даних**: XDR об'єднує дані з телеметрії кінцевих точок, мережевого трафіку, журналів та інших джерел для отримання цілісного уявлення про кібербезпеку організації.
- ✓ **Автоматизація**: XDR використовує машинне навчання та інші методи автоматизації для пришвидшення виявлення та реагування на кіберзагрози.

SIEM (Security Information and Event Management):

- ✓ **Управління інформацією та подіями безпеки**: SIEM – це програмний продукт, який збирає та аналізує журнали безпеки та інші дані з різних джерел для виявлення кіберзагроз.
- ✓ **Кореляція подій**: SIEM корелює події з різних джерел, щоб ідентифікувати потенційні кіберзагрози, які інакше могли б залишитися непоміченими.
- ✓ **Моніторинг та оповіщення**: SIEM використовується для моніторингу мережі та систем на наявність ознак кібератак та для надсилання оповіщень про виявлені загрози.

XDR та SIEM доповнюють один одного, XDR фокусується на виявленні та реагуванні, а SIEM – на зборі та аналізі даних. Використання XDR та SIEM разом може значно покращити кібербезпеку організації.

Переваги Wazuh:

- ➢ **Відкритість:** Wazuh - це проект з відкритим кодом, що дає користувачам доступ до його коду та можливість його модифікації.
- ➢ **Безкоштовність:** Wazuh можна використовувати безкоштовно, що робить його доступним для організацій з обмеженим бюджетом.
- ➢ **Гнучкість:** Wazuh може використовуватися для моніторингу різних типів систем, включаючи сервери, робочі станції, мережеві пристрої та хмарні середовища.
- ➢ **Кросплатформенність**: Є кросплатформеним рішенням, що означає, що воно підтримується та може бути встановлене на різних операційних системах. Основні операційні системи, на яких можна встановити Wazuh, включають:
  - ✓ **Linux**: Wazuh підтримує багато дистрибутивів Linux, таких як Ubuntu, CentOS, Debian, Fedora, Red Hat Enterprise Linux (RHEL), openSUSE тощо.
  - ✓ **Windows**: Wazuh також може бути встановлено на операційних системах Windows, що дозволяє користувачам моніторити безпеку в їхніх середовищах Windows.

- ✓ **macOS**: Версії Wazuh також доступні для встановлення на комп'ютери з операційною системою macOS, що дозволяє користувачам забезпечити безпеку своїх систем Mac.

Кросплатформеність Wazuh робить його дуже гнучким і придатним для різних установок та інфраструктур. Це означає, що незалежно від того, яка операційна система використовується в вашій організації, ви можете встановити та використовувати Wazuh для моніторингу та забезпечення безпеки вашої інфраструктури.

- ➢ **Масштабованість:** Wazuh може масштабуватися для моніторингу великих IT-інфраструктур.
- ➢ **Простота використання:** Wazuh має інтуїтивно зрозумілий інтерфейс користувача, що робить його доступним для користувачів з різним досвідом.

Компоненти Wazuh

Рішення Wazuh базується на агентах Wazuh, які розгортається на контрольованих кінцевих точках, і на трьох центральних компонентах:

- ➢ Сервері – Wazuh Server
- ➢ Індексаторі – Wazuh indexer
- ➢ Інформаційній панелі – Wazuh dashboard

Wazuh Indexer

Індексатор Wazuh (Wazuh indexer) — це система повнотекстового пошуку та аналітики даних безпеки в реальному часі. Дані журналу, що надходять на сервер Wazuh, аналізуються та пересилаються до індексатора для індексування та зберігання. Ці події потім запитуються на інформаційній панелі Wazuh.

Індексатор Wazuh зберігає дані як документи JSON. Кожен документ пов'язує набір ключів, імен полів або атрибутів із відповідними значеннями, якими можуть бути символи, числа, логічні значення, дати, масиви значень, геолокації чи інші види даних.

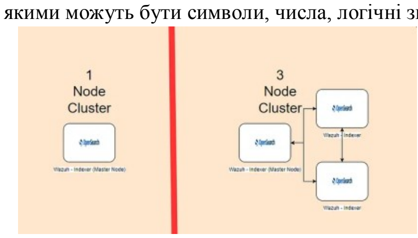


Рис. 07.01. Кластер з 1 вузлом і 3 вузлами

Індексатор Wazuh можна налаштувати як одновузловий або багатовузловий кластер, що забезпечує масштабованість і високу доступність. Він розподіляє документи між різними контейнерами, відомими як сегменти. У свою чергу, він розподіляє ці фрагменти між вузлами кластера. Розподіляючи документи між декількома шардами та розподіляючи ці сегменти між кількома вузлами, індексатор Wazuh забезпечує надлишковість. Надлишковість забезпечує доступність індексатора Wazuh у разі збою та збільшує пропускну здатність для запитів між вузлами кластера.

Індекси індексатора Wazuh. Покажчик — це сукупність документів, які пов'язані між собою. Індексатор Wazuh використовує індекси для зберігання та організації даних безпеки для швидкого пошуку. Wazuh використовує такі шаблони індексів для зберігання цих даних:

- ➢ wazuh-alerts-* : це шаблон індексу для сповіщень, створених сервером Wazuh.
- ➢ wazuh-archives-* : це шаблон індексу для всіх подій, надісланих на сервер Wazuh.
- ➢ wazuh-monitoring-* : це шаблон індексу для статусу агентів Wazuh.
- ➢ wazuh-statistics-* : це шаблон індексу для статистичної інформації сервера Wazuh.

Система підтримує створення спеціальних шаблонів індексу або зміну стандартного шаблону індексу.

Інформація про індекси Wazuhможе бути перевірена двома способами.

- ➢ З використанням веб-інтерфейсу користувача.
- ➢ Створенням запиту до API індексатора Wazuh.

Переіндексація. Коли в схему даних вносяться зміни, виникає необхідність повторно індексувати дані, щоб відобразити ці зміни. Існуючі дані можуть не відповідати оновленій схемі без повторного індексування, що призведе до невідповідності даних або помилок під час запитів. Повторне індексування дає змогу копіювати всі або частину ваших даних із вихідного індексу в індекс призначення.

Стандарти безпеки вимагають зберігати дані доступними для аудиту протягом мінімального періоду часу. Дані, які зберігаються довше цього терміну, можуть бути видалені, щоб заощадити місце для зберігання.

Також можливо визначити спеціальні політики для автоматичного видалення даних.

Wazuh Server

Сервер Wazuh аналізує дані, отримані від агентів. Він обробляє їх 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.

Сервер Wazuh складається з кількох перелічених нижче компонентів, які мають різний функціонал, 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. 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** отримує дані від агентів. Служба використовує ключі, спільні для служби реєстрації, для перевірки ідентифікації кожного агента та шифрування зв'язку між агентом Wazuh і сервером Wazuh. Крім того, служба підключення агентів забезпечує централізоване керування конфігурацією, що дозволяє віддалено надсилати нові параметри агентам.
- ➢ **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, блокування IP-адреси, зупинка запущеного процесу або видалення артефакту зловмисного програмного забезпечення).

- **Wazuh RESTful API**. Необхідно розпочати з значення абревіатури назви компоненту. RESTful API розшифровується як Representational State Transfer Application Programming Interface. REST - це архітектурний стиль для веб-сервісів, API - це інтерфейс програмування, який дозволяє двом програмам взаємодіяти одна з одною. Таким чином, RESTful API - це API, який використовує архітектурний стиль REST для надання доступу до ресурсів. RESTful API 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.
- **Wazuh cluster daemon** 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 а також забезпечує балансування навантаження при підключенні до багатовузлового кластера індексатора Wazuh.

Рис. 07.02. Wazuh Server та агенти у структур Wazuh

<u>Wazuh dashboard</u>

Інформаційна панель Wazuh — це веб-інтерфейс користувача для візуалізації та аналізу даних. Він включає в себе готові інформаційні панелі для

- ✓ подій безпеки
- ✓ нормативної відповідності
- ✓ виявлені вразливості програм
- ✓ 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 діаграмі нижче показано компоненти та потік даних Wazuh.

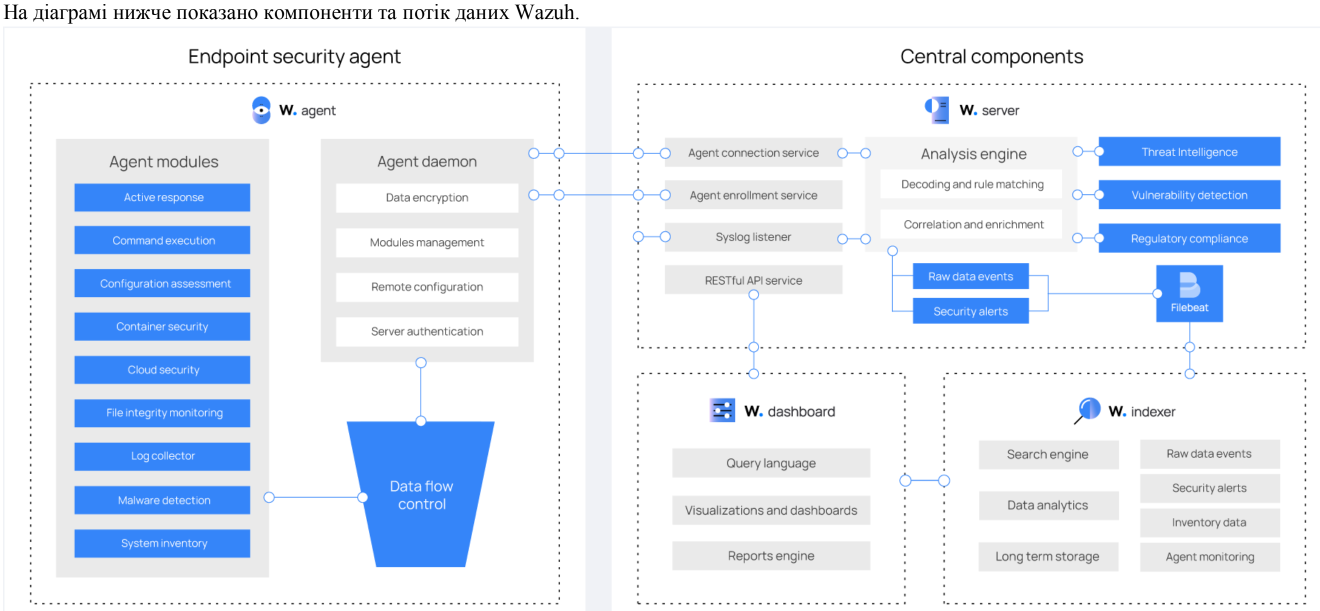


Рис. 07.03. Компоненти та потоки даних Wazuh

<u>Архітектура Wazuh</u>

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.

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. Багатовузлові кластери рекомендуються, якщо є багато контрольованих кінцевих точок, коли очікується великий обсяг даних або коли потрібна висока доступність.

Кластеризація серверів Wazuh це цікавий та сучасний приклад реалізації масштабування. Реалізація можлива починаючи з версії Wazuh 3.x (2018 рік). По суті, може бути кілька серверів, які працюють разом у режимі кластера та містять протокол, що дозволяє їм обмінюватися інформацією, необхідною для керування підключенням агентів. Іншими словами, агенти зможуть звітувати перед будь-яким нодом (сервером) у кластері, який розподілятиме навантаження між різними вузлами (нодами) та забезпечуватиме можливості високої доступності.

Як показано на рис 07.02, архітектура кластера базується на головному/клієнтському серверах. Головні вузли будуть відповідати за централізацію всієї конфігурації та керування Wazuh.

У рамках кластеризації можливе групування агентів, щоб налаштувати конкретну конфігурацію, політику кореневої перевірки та перевірку надійності для певної групи. Для кожної групи, сервер дистанційно надсилатиме агентам відповідні файли, автоматично застосовуючи зміни

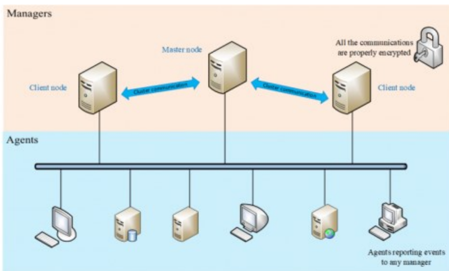


Рис. 07.04. Кластерізація менеджерів Wazuh

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.

На рис.07.03 показано архітектуру розгортання Wazuh. Він показує компоненти рішення та те, як сервер Wazuh і вузли індексатора Wazuh можуть бути налаштовані як кластери, забезпечуючи балансування навантаження та високу доступність.

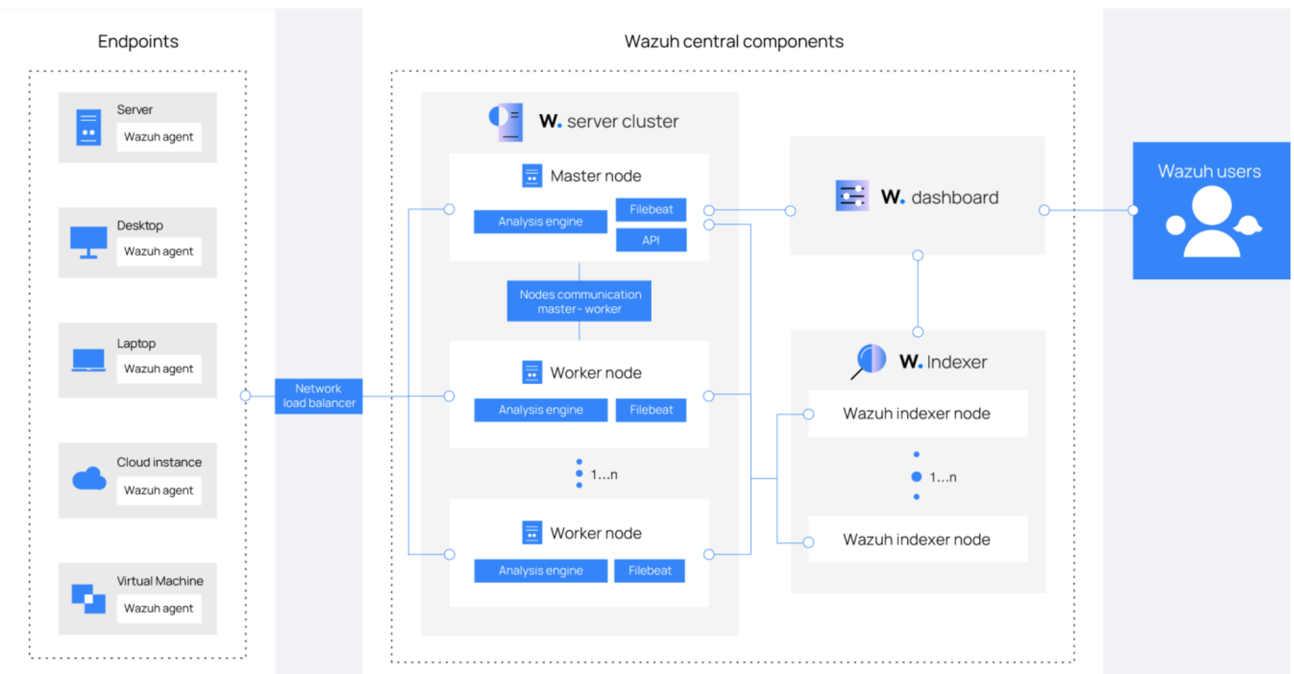


Рис. 07.05. Архітектура розгортання Wazuh

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 (номер порту можливо змінити налаштуванням). 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 два файли журналів, в залежності від того, чи спрацьовує правило:

- /var/ossec/logs/archives/archives.json містить усі події незалежно від того, чи спрацювало вони правило чи ні.
- /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 128 біт на блок і 256-бітними ключами. Шифрування Blowfish необов'язкове.

Сервер Wazuh використовує Filebeat для надсилання даних попереджень і подій до індексатора Wazuh за допомогою шифрування TLS. Filebeat зчитує вихідні дані сервера Wazuh і надсилає їх до індексатора Wazuh (за замовчуванням прослуховує порт 9200/TCP). Коли дані проіндексовано індексатором Wazuh, інформаційна панель Wazuh використовується для аналізу та візуалізації інформації.

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. Не будемо детально зупинятися на списку стандартних портів, які використовуються цими службами. При потребі їх можна розглянути у документації.

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). Файли щодня стискаються та підписуються за допомогою контрольних сум MD5, SHA1 і SHA256. Структура каталогу та імені файлу наступна:
root@wazuh-manager:/var/ossec/logs/archives/2024/Mar# ls -l

```
total 176
-rw-r----- 1 wazuh wazuh 234350 Mar  2 00:00 ossec-archive-01.json.gz
-rw-r----- 1 wazuh wazuh    350 Mar  2 00:00 ossec-archive-01.json.sum
-rw-r----- 1 wazuh wazuh 176221 Mar  2 00:00 ossec-archive-01.log.gz
-rw-r----- 1 wazuh wazuh    346 Mar  2 00:00 ossec-archive-01.log.sum
-rw-r----- 1 wazuh wazuh 224320 Mar  2 00:00 ossec-archive-02.json.gz
-rw-r----- 1 wazuh wazuh    350 Mar  2 00:00 ossec-archive-02.json.sum
-rw-r----- 1 wazuh wazuh 151642 Mar  2 00:00 ossec-archive-02.log.gz
-rw-r----- 1 wazuh wazuh    346 Mar  2 00:00 ossec-archive-02.log.sum
-rw-r----- 1 wazuh wazuh 315251 Mar  2 00:00 ossec-archive-03.json.gz
-rw-r----- 1 wazuh wazuh    350 Mar  2 00:00 ossec-archive-03.json.sum
-rw-r----- 1 wazuh wazuh 156296 Mar  2 00:00 ossec-archive-03.log.gz
-rw-r----- 1 wazuh wazuh    346 Mar  2 00:00 ossec-archive-03.log.sum
```

Рекомендується ротація та резервне копіювання архівних файлів відповідно до обсягу пам'яті сервера Wazuh . Використовуючи завдання cron, легко налаштовується зберігання лише певного часового проміжку архівних файлів локально на сервері, наприклад, минулого року чи останніх трьох місяців.
З іншого боку, можна відмовитися від зберігання архівних файлів і просто покластися на індексатор Wazuh для зберігання архіву. Ця альтернатива може бути кращою, якщо періодично виконується резервне копіювання моментальних знімків індексатора Wazuh або є багатовузловий кластер індексатора Wazuh з копіями фрагментів для високої доступності. Для цього також можна використовувати завдання cron, щоб перемістити знімки індексів на кінцевий сервер зберігання даних і підписати їх за допомогою алгоритмів хешування.

Можливості Wazuh

- **Моніторинг цілісності файлів:** Wazuh може відстежувати зміни файлів та повідомляти про підозрілу активність.
- **Моніторинг журналів:** Wazuh може збирати та аналізувати журнали з різних систем для виявлення загроз безпеки.
- **Моніторинг мережі:** Wazuh може відстежувати мережевий трафік та повідомляти про підозрілу активність.
- **Виявлення вторгнень:** Wazuh може використовувати правила Snort для виявлення вторгнень.
- **Моніторинг аномалій:** Wazuh може використовувати машинне навчання для виявлення аномальної поведінки.
- **Реагування на інциденти:** Wazuh може автоматизувати дії реагування на інциденти.

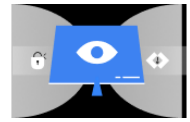
Wazuh – це система виявлення вторгнень (IDS) та система запобігання вторгненням (IPS), а не всебічний інструмент моніторингу та кібербезпеки. Треба розуміти, що Wazuh не має вбудованих функцій для моніторингу продуктивності та веб-додатків, не є антивірусом, не має вбудованих функцій для шифрування даних, не може моніторити хмарні інфраструктури без додаткових плагінів або інтеграцій, не може автоматично виправляти вразливості, не має вбудованих функцій для моніторингу IoT-пристроїв та не має вбудованих функцій для моніторингу контейнерів та баз даних.

Використання Wazuh для моніторингу цілісності файлів

Для цієї задачі Wazuh використовує модуль File Integrity Monitoring (FIM), що відстежує та сповіщає про зміни критичних файлів і каталогів та швидко виявляти зміни файлів, які вказують на компрометацію чи кібератаку. Використання FIM надає Wazuh наступні особливості:

- **Моніторинг в реальному часі - виявлення змін файлів і реакція на них у реальному часі.** Wazuh відстежує системні файли та каталоги в режимі реального часу, щоб виявляти зміни, коли вони відбуваються, і запускає сповіщення, які дозволяють негайно вжити заходів. Це допомагає організаціям пом'якшити вплив інцидентів безпеки
- **Виявлення порушень безпеки та втручання в систему за допомогою Wazuh FIM (File Integrity Monitoring)** - модуль вбудований в Wazuh, що використовується для моніторингу та оповіщення про зміни в критичних файлах та директоріях. Wazuh відстежує файли та каталоги, відстежуючи атрибути, дозволи, право власності та вміст. Він використовує хеш-значення для виявлення змін у файловій системі, виявлення зловмисних дій і зменшення внутрішніх загроз від окремих осіб або постачальників.

Рис. 07.06. DashBoard Wazuh



Як працює Wazuh FIM:

1. **Сканування**: Модуль FIM періодично сканує певні шляхи та моніторить певні директорії в режимі реального часу. Ви можете встановити, які шляхи моніторити в конфігурації агентів та менеджера Wazuh.
2. **Базова лінія**: FIM створює базову лінію, зберігаючи криптографічну контрольну суму та інші атрибути моніторингових файлів.
3. **Порівняння**: FIM порівнює інформацію базової лінії з інформацією про останню версію файлу. Це порівняння дає видимість змін та оновлень критичних файлів.
4. **Оповіщення**: Якщо FIM виявляє будь-які зміни в моніторингових файлах, він генерує сповіщення, яке може бути відправлене на різні канали, такі як електронна пошта, SNMP або syslog.

- **Відповідність нормативним вимогам щодо безпеки даних і конфіденційності.** Wazuh допомагає відстежувати модифікації важливих файлів і каталогів, щоб вони відповідали нормам, таким як PCI DSS, HIPAA, NIST 800-53, TSC і GDPR. Використовуючи модуль Wazuh FIM, ви можете продемонструвати аудиторам і регуляторам, що вжили заходів для підтримки безпеки та цілісності даних.

- **Централізоване управління -** відстеження змін файлів на кількох кінцевих точках із центрального розташування. Інформаційна панель Wazuh дозволяє налаштовувати політики FIM і керувати ними, аналізувати сповіщення та виконувати адміністративні завдання. Він пропонує вичерпні звіти про зміни файлів, надаючи докладну інформацію про повідомлені зміни

- **Масштабованість -** ефективне відстеження файлів та каталогів незалежно від обсягу даних. Розподілена архітектура Wazuh забезпечує масштабовану роботу модуля FIM шляхом розподілу робочого навантаження між кількома вузлами. Це забезпечує ефективне керування великою кількістю файлів і каталогів.

Кросплатформена підтримка – захист важливих та системних файлів в кількох операційних системах за допомогою модуля Wazuh FIM. Wazuh FIM підтримує різні операційні системи, включаючи Windows, Linux і macOS. Він забезпечує міжплатформну підтримку для моніторингу змін файлів у всій вашій ІТ-інфраструктурі, дозволяючи захистити вас від несанкціонованих змін і потенційних порушень безпеки.

Windows macOS Linux AIX HP-UX Solaris

Методи встановлення Wazuh

- **Вимоги до обладнання** значною мірою залежать від кількості захищених кінцевих точок і хмарних робочих навантажень. Це число може допомогти оцінити, скільки даних буде проаналізовано та скільки сповіщень безпеки буде збережено та проіндексовано.
  Комплекту центральних компонентів (Wazuh server, indexer, dashboard) на одному хості достатньо для моніторингу до 100 кінцевих точок і для 90 днів запитуваних/індексованих даних попереджень. У таблиці нижче показано рекомендована конфігурація для швидкого розгортання:

Агенти	**CPU**	**RAM**	**Зберігання (90 днів)**
1–25	4 vCPU	8 Гб	50 ГБ
25–50	8 vCPU	8 Гб	100 ГБ
50–100	8 vCPU	8 Гб	200 ГБ

  Для великих середовищ ми рекомендуємо розподілене розгортання. Конфігурація кластера з кількома вузлами доступна для сервера Wazuh і для індексатора Wazuh, що забезпечує високу доступність і балансування навантаження.

- **Операційна система.** Центральні компоненти Wazuh можна встановити на 64-бітну операційну систему Linux. Wazuh рекомендує будь-яку з наступних версій ОС: Amazon Linux 2, CentOS 7, 8, Red Hat Enterprise Linux 7, 8, 9, Ubuntu 16.04, 18.04, 20.04, 22.04

- **Стандартне встановлення Wazuh.** Завантажте та запустіть помічника встановлення Wazuh.
  curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh –a
  Коли помічник завершить інсталяцію, у вихідних даних відобразяться облікові дані доступу та повідомлення, яке підтверджує, що інсталяція пройшла успішно.

INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
User: admin
Password: <ADMIN_PASSWORD>
INFO: Installation finished.

Wazuh встановлено та налаштовано. Доступ до веб-інтерфейсу Wazuh за допомогою
https://<wazuh-dashboard-ip>
Облікові дані:
Ім'я користувача: admin
Пароль: <ADMIN_PASSWORD>

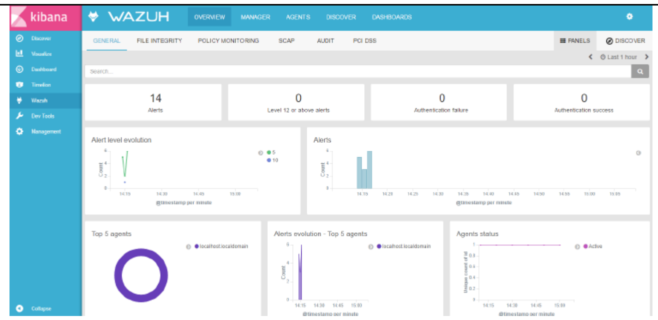
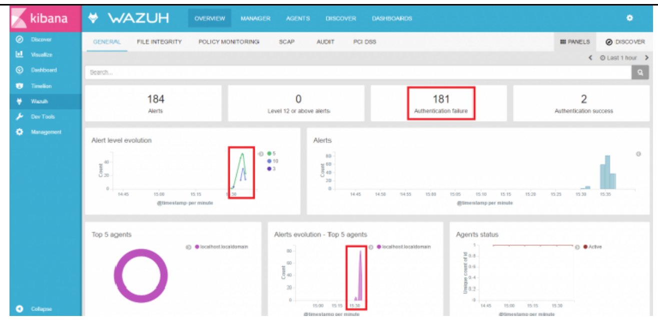
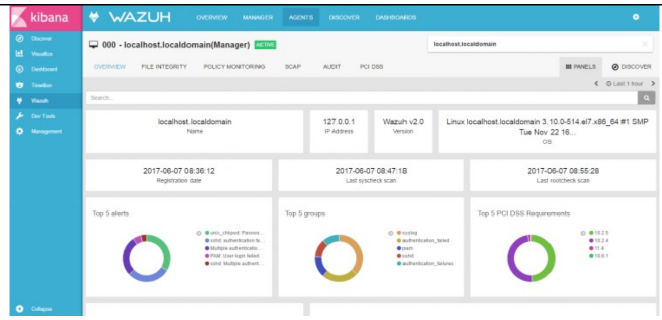
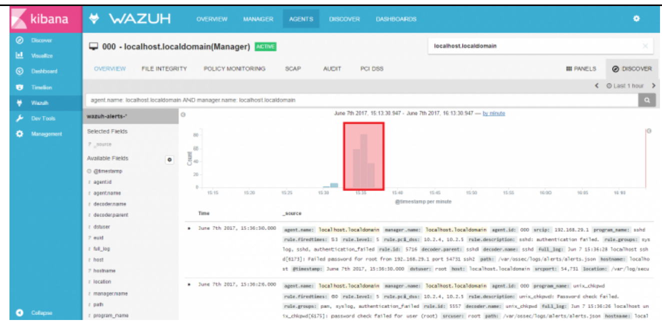
Коли доступ до інформаційної панелі Wazuh отримано вперше, браузер показує попередження про те, що сертифікат не був виданий довіреним центром. Це очікувано, і користувач має можливість прийняти сертифікат як виняток або, альтернативно, налаштувати систему на використання сертифікату від довіреного центру.
Можливо розпочати розгортання агентів Wazuh, що використовуються для захисту ноутбуків, настільних ПК, серверів, хмарних примірників, контейнерів або віртуальних машин. Агент легкий і багатоцільовий. Інструкції щодо розгортання агентів Wazuh можна знайти у веб-інтерфейсі користувача Wazuh або в документації .

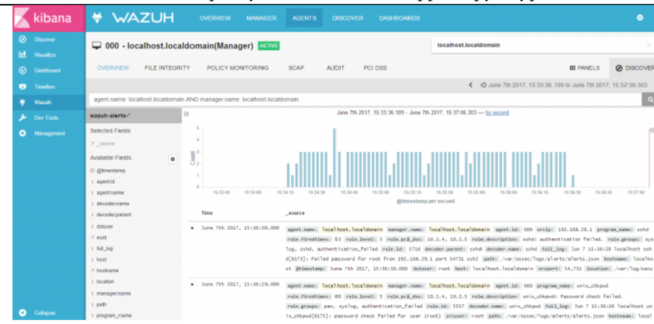
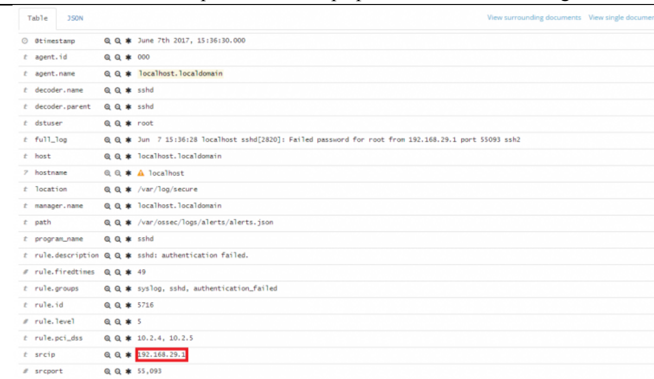
- **Встановлення Wazuh розгортанням готових до використання машини**
  - ✓ **Віртуальна машина (OVA).** Wazuh надає попередньо зібраний образ віртуальної машини (OVA), який можна імпортувати безпосередньо за допомогою VirtualBox або інших систем віртуалізації, сумісних з OVA.
  - ✓ **Образи машини Amazon (AMI).** Попередньо створений образ машини Amazon (AMI), який можна запускати безпосередньо в хмарному екземплярі AWS.

- **Встановлення контейнерів.**
  - ✓ **Розгортання на Docker**. Docker — це набір продуктів платформи як послуги (PaaS), які доставляють програмне забезпечення в пакетах, які називаються контейнерами. За допомогою Docker ви можете встановити та налаштувати розгортання Wazuh як архітектуру з одним хостом.
  - ✓ **Розгортання на Kubernetes**. Kubernetes — це система з відкритим кодом для автоматизації розгортання, масштабування та керування контейнерними програмами. Цей тип розгортання використовує зображення Wazuh із Docker і дозволяє створювати середовище Wazuh.

<u>Огляд Wazuh на прикладі атаки грубою силою</u>

Коротко пройдемося по стандартному прикладу роботи з Wazuh.

Головний вигляд програми Wazuh, перше, що ви побачите, натиснувши Wazuh у меню ліворуч. Додаток має різні розділи для навігації, як видно у верхньому меню. Прямо під верхнім є друге меню, пов'язане з виділеним розділом у верхній частині. Почнемо із загального огляду. Як бачите, у нас ще дуже мало даних, однак ми можемо отримати уявлення про різну інформацію, яку надає програма. У першому розділі наведено стислий перелік попереджень, надано інформацію про загальну кількість попереджень, ті, які можна вважати критичними, і ви, можливо, захочете перевірити в першу чергу, і, нарешті, ті, що стосуються успішної та невдалої автентифікації. Крім того, є кілька графіків, що показують еволюцію сповіщень за одиницю часу.	 Рис. 07.07. Wazuh General Overview
Другий розділ стосується різних агентів у середовищі. У нашому прикладі лише один агент. Існує третій розділ, який не показаний на знімку екрана, який дає нам підсумок сповіщень, маючи можливість перевірити найбільш генеровані сповіщення та впорядкувати їх за кількістю або рівнем. Варто зазначити, що все в додатку можна натискати, тобто ми можемо легко фільтрувати дані, і все буде змінено, включно з інформаційними панелями, просто щоб показати відфільтровану інформацію. На рис.7.08 показане відображення згенерованої атаки грубої сили. Ця атака запускає сповіщення кожного разу, при невдалій автентифікації. Цікаво побачити різні піки, показані на графіках. Такий вигляд матиме головний екран програми після нападу.	 Рис. 07.08. Wazuh General Overview After Brute Force
Перейдемо до розділу агентів, натиснувши «Agents» у верхньому меню. Тут ми побачимо різних агентів, які ми маємо в нашому середовищі, і деяку цікаву інформацію, таку як ім'я агента, ідентифікатор, IP-адреса та статус агента (підключено, відключено або ніколи не підключався). Якщо ми звернемося до нашого конкретного агента, ми знайдемо додаткові відомості про те, що відбувається в цьому агенті. Іншими словами, ми застосували фільтр, щоб показати лише дані, пов'язані з цим агентом. Нижче наведено вигляд агента атакованого сервера. Цей перегляд пропонує кілька корисних графіків про конкретного агента. Одним із них є графік «5 найпопулярніших сповіщень», який включає «Кілька помилок автентифікації». Той, що праворуч, повідомляє нам вимоги PCI DSS (стандарт Payment Card Industry Data Security Standard), на які впливають згенеровані сповіщення.	 Рис. 07.09. Вкладка Panels Wazuh Agents
Тепер, коли ми знаємо, що хтось намагався увійти, наступним кроком є детальна перевірка сповіщення. У правому верхньому кутку екрана ми бачимо дві закладки. Активна – Panels та неактивна, що праворуч від активної – Discover. Переходимо до неактивної панелі і відкривається деталізація події. Тобто, якщо ви хочете отримати додаткові відомості про певне сповіщення, необхідно перейти на вкладку Discover (виявлення).	 Рис. 07.10. Вкладка Discover Wazuh Agents

Зверніть увагу, що графік можна збільшити у червоній рамці, для отримання більш конкретних даних. Просто обираємо потрібну область графіка, що нас зацікавила. Після цього відобразяться всі сповіщення, які були запущені між вибраним часом.	 Рис. 07.11. Обрана область графіка Discover Wazuh Agents
Тепер ми можемо відкрити нашу подію помилки автентифікації, і ми отримаємо наступну інформацію. У списку тривог знаходимо authentication failure event. Отримуємо доступ до деталей: ім'я агента та ідентифікатор, кількість разів, коли це сповіщення було запущено, рівень, вплив PCI-контролю тощо, вихідна IP-адреса (червоним). Це приклад, щоб трохи розповісти про один з підходів в експлуатації Wazuh. Підходів дуже багато, вони описані в основному в відеороликах. Існує навіть кілька каналів на Youtube. Ось один з таких каналів: https://www.youtube.com/channel/UC3Kr7V99AXOOOuPy4bLhS8w	 Рис. 07.12. Деталізація події з списка тривог.

Огляд Snort як системи виявлення та запобігання вторгненням (IDS/IPS).

Snort — це одна з найпопулярніших у світі систем виявлення та запобігання вторгненням (IDS/IPS) з відкритим вихідним кодом. Вона забезпечує ефективний аналіз мережевого трафіку в режимі реального часу та здатна як виявляти, так і блокувати підозрілу або небезпечну мережеву активність.

Основою роботи Snort є система правил. Ці правила описують сигнатури зловмисної активності, наприклад, характерні ознаки DoS-атак, спроб сканування портів, експлойтів, аномальних протоколів тощо. Snort порівнює вхідні мережеві пакети з цими правилами, і у разі збігу може або згенерувати сповіщення, або відразу заблокувати небезпечний трафік, залежно від обраного режиму роботи.

Snort підтримує три основні режими використання:

- **Сніффер трафіку** — подібно до утиліти tcpdump, Snort дозволяє переглядати мережеві пакети у режимі реального часу.
- ***Логер (реєстратор)*** — фіксує трафік у лог-файли для подальшого аналізу чи налагодження.
- **Повноцінна система запобігання вторгненням (IPS)** — здійснює аналіз трафіку та може блокувати зловмисні пакети відповідно до налаштованих правил.

Snort є доступним для завантаження та використання як у навчальних, так і в корпоративних середовищах. Однією з його переваг є підтримка різних наборів правил:

- Набір правил спільноти (**Community Ruleset**) — створений та підтримуваний активною спільнотою користувачів Snort. Цей набір є безкоштовним і відкритим для всіх охочих.
- Набір правил для передплатників (**Snort Subscriber Ruleset**) — розробляється та перевіряється командою безпеки Cisco Talos. Цей набір призначений для комерційних користувачів, які мають підписку, і отримують оновлення правил у режимі реального часу одразу після їх виходу для клієнтів Cisco.
- **Registered User Ruleset** (безкоштовно, але з затримкою) До цього типу правил ще повернемося, коли торкнемось ліцензування.

Оновлення правил та налаштування Snort здійснюється через офіційний портал Snort.org.
Серед ключових переваг Snort можна відзначити:

- **Гнучкість налаштування**. Можливість створювати власні правила для специфічних потреб мережі.
- **Підтримка інтеграції з іншими системами моніторингу**. Як приклад, журнали Snort можуть бути імпортовані до SIEM-рішень таких як Wazuh, Splunk або QRadar для поглибленого аналізу.
- **Широке застосування у корпоративних середовища**х завдяки високій продуктивності, великій спільноті та надійності.

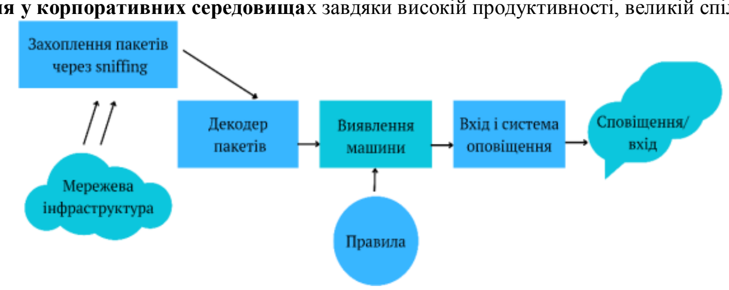


Рис. 07.13. Архітектура Snort

Архітектура Snort має чітко структуровану модульну будову, що зображена рис. 7.13.
Розглянемо основні компоненти:

- **Захоплення пакетів через sniffing.** Snort починає свою роботу з прослуховування мережевого трафіку. За допомогою механізму сніффінгу система отримує всі вхідні пакети, що проходять через мережу.
- **Декодер пакетів.** Захоплені пакети надходять на декодер, який розбирає кожен пакет, ізолюючи заголовки протоколів, що відповідають різним рівням моделі OSI. Це дозволяє Snort отримати інформацію про структуру пакета для подальшого аналізу.
- **Виявлення машини (детекція).** Основна функціональність Snort зосереджена саме в цьому блоці. Механізм виявлення аналізує вміст кожного пакета, порівнюючи його з набором правил. Правила можуть визначати характерні ознаки атак, спроб проникнення або аномальної активності в мережі.
- **Система правил.** Серце Snort — це база правил, яка може бути як стандартною (наприклад, набір Community Ruleset), так і кастомізованою під специфіку конкретного середовища. Кожне правило описує умови, за яких трафік вважається підозрілим або зловмисним.
- **Вхід і система оповіщення.** Якщо пакет відповідає умовам певного правила, система спрацьовує: формується запис про подію та надсилається відповідне сповіщення адміністратору або іншим захищеним системам.

Таким чином, Snort функціонує як потужний фільтр мережевого трафіку, здатний оперативно реагувати на загрози.

Архітектура Snort демонструє його здатність ефективно інтегруватися в корпоративну мережеву інфраструктуру як система первинного аналізу та виявлення загроз. Однак максимальну ефективність Snort досягає, коли виступає не як окремий інструмент, а як джерело подій для більш комплексних рішень.

Варто зазначити, що Snort виконує роль одного з основних джерел подій про мережеву активність. Його доцільно використовувати у поєднанні з іншими системами, які ми розглядаємо у цій темі, для побудови комплексної системи моніторингу та безпеки IT-інфраструктури. Наприклад, Snort можна використовувати для детекції атак на мережевому рівні, а зібрані події корелювати у SIEM-системах для отримання повної картини безпекових інцидентів.

Таким чином, Snort є важливим елементом в арсеналі засобів забезпечення безпеки корпоративних мереж, що доповнює можливості інших рішень, підсилюючи загальний рівень захисту мережевої інфраструктури.

Встановлення Snort. Підтримувані операційні системи. Snort є кросплатформеним рішенням і може бути встановлений на:

- Linux (найпопулярніші дистрибутиви: Ubuntu, Debian, CentOS, Fedora, Red Hat)
- FreeBSD
- macOS
- Windows (є спеціальний інсталятор для Windows, але використовується рідше через складнішу інтеграцію)

Основні залежності. Перед встановленням Snort необхідно підготувати систему, встановивши такі компоненти:

- Libpcap (для Linux) / WinPcap / npcap (для Windows). Бібліотека для захоплення мережевого трафіку.
- DAQ (Data Acquisition Library). Бібліотека, яка надає Snort доступ до мережевого інтерфейсу для роботи з пакетами.
- PCRE (Perl Compatible Regular Expressions). Використовується для роботи з регулярними виразами у правилах Snort.
- Libdnet (на Linux). Потрібна для низькорівневої роботи з мережею.
- Barnyard2 (необов'язково). Додатковий компонент для обробки та експорту логів Snort у базу даних або SIEM.
- PulledPork (опціонально). Інструмент для автоматичного завантаження та оновлення правил Snort.

Snort має двоїсте ліцензування, що дозволяє гнучко використовувати його як у комерційних, так і некомерційних цілях:

- **GPLv2 (GNU General Public License, версія 2)**. Це базова ліцензія Snort, яка дозволяє безкоштовне використання, модифікацію та розповсюдження програмного забезпечення. Вона підходить для освітніх цілей, лабораторій, дослідницьких проектів і навіть використання у продуктивному середовищі, якщо дотримано вимоги GPL.

- **Комерційна ліцензія від Cisco.** Оскільки Snort належить компанії Cisco, існує можливість укладання комерційної угоди для інтеграції Snort у пропрієтарні рішення або для отримання додаткової підтримки та розширених можливостей.

Правила Snort з урахуванням ліцензування:

- **Community Rules** (безкоштовні) — доступні всім користувачам Snort.
- **Subscriber Ruleset** (платна підписка) — більш розширений набір правил з оновленнями для комерційних клієнтів та організацій, які бажають отримувати нові правила якомога швидше.
- **Registered User Ruleset** (безкоштовно, але з затримкою) — доступні після реєстрації, але з деякою затримкою порівняно з платною підпискою.

Таким чином, для навчальних цілей та базового використання достатньо Community Rules та GPLv2 ліцензії. Для серйозних корпоративних впроваджень варто розглядати підписку на оновлення правил або укладення комерційного контракту.

<u>Огляд Splunk Enterprise Security</u>

Splunk Inc. — це американська компанія -розробник програмного забезпечення , розташована в Сан-Франциско, Каліфорнія, яка виробляє програмне забезпечення для пошуку, моніторингу та аналізу машинно-генерованих даних через веб-інтерфейс. Його програмне забезпечення допомагає отримувати, індексувати та співвідносити дані в реальному часі в репозиторії з можливістю пошуку , з якого можна створювати графіки, звіти, сповіщення, інформаційні панелі та візуалізації.
Фірма використовує машинні дані для ідентифікації шаблонів даних, надання показників, діагностики проблем і надання інформації для бізнес-операцій. Це горизонтальна технологія, яка використовується для керування програмами , безпеки та відповідності , а також для бізнес- та веб-аналітики.

У вересні 2023 року було оголошено, що Splunk буде придбана компанією Cisco за 28 мільярдів доларів США за угоду за готівку. Трансакцію було завершено 18 березня 2024 року.
Це була найбільша угода в історії Cisco. На той час у Splunk було 1100 патентів із такими клієнтами, як Singapore Airlines, Papa Johns, Heineken і McLaren. Splunk продовжував працювати під тим самим керівництвом, а ціни залишалися незмінними.

Splunk Enterprise Security (ES) – система управління інформаційною безпекою та подіями (англ. Security and information event management, SIEM), яка формує детальну картину машинних даних, що створили додаткові технології безпеки (мережа, кінцеві точки, доступ, шкідливі програми, вразливість і перевірка). Завдяки Splunk Enterprise Security фахівці з безпеки швидко ідентифікують внутрішні та зовнішні атаки та приймають відповідні запити. Splunk Enterprise Security дозволяє спростити операції із захисту від загроз, мінімізувати ризик і забезпечити безпеку вашого бізнесу. Рішення оптимізує всі аспекти захисту та підходить для організації будь-якого масштабу та професійного рівня, дозволяє здійснювати пошук кореляцій, оповіщення, звітності та панелі моніторингу з урахуванням ваших потреб.
Splunk ES використовується для постійного моніторингу в реальному часі, швидкого реагування на інциденти, в якості операційного захисту центру або для керівників, які необхідні відомості про ділові ризики.

Ключові можливості застосування продукту:
- **Моніторинг в реальному часі** – отримання чіткого і наочного виявлення про стан безпеки організації, крім налаштувань виявлення і деталізації даних аж до базових подій.
- **Призначення пріоритетів і вжиття відповідних заходів** – представлення даних у контексті безпеки для розширення можливості виявлення загроз та оптимізації реагування на інциденти.
- **Швидке розслідування** – використання ситуативного пошуку, а також статичних, динамічних та візуальних кореляцій для виявлення шкідливих дій.
- **Багатоетапні розслідування** – аналіз пошкоджений і наслідковий аналіз для виявлення динамічних дій, пов'язаних із загрозами.

Splunk Enterprise Security запускається в середовищі Splunk Enterprise або Splunk Cloud. Рішення Splunk ES може бути розгорнуто у вигляді програми або хмарної служби, у загальнодоступному або приватному, а також у гібридному програмно-хмарному середовищі.
Ось основні результати впровадження у якості SIEM саме Splunk Enterprise Security:
- **Поліпшення операцій по забезпеченню безпеки.** Прискорене реагування на інциденти та демонстрація відповідності вимогам за допомогою великого обладнання вбудованих панелей моніторингу, видимих таблиць, звітів і процесів реагування на інциденти, включаючи оцінки ризиків, швидкий пошук, аналітику, кореляції та індикатори безпеки.
- **Підвищення рівня безпеки.** Оптимізація процесів моніторингу безпеки, розстановки пріоритетів, реагування, стримування та відновлення аналізу всіх машинних даних для оцінки впливу сповіщень або інцидентів.

- **Призначення пріоритетів подій безпеки та розслідувань**. Поліпшення процесу прийняття рішень і розробка стратегії усунення ризиків з урахуванням вимог бізнесу шляхом застосування оцінок ризиків до будь-якої події, активу, виклику чи користувача у зв'язку з їх відносною важливістю або цінністю для бізнесу.
- **Виявлення внутрішніх і складних загроз.** Перевірка привілейованого доступу та незвичайної діяльності шляхом використання даних про відхилення, виявлених додатком UBA, а також застосування користувальницького контексту та контексту активів до всіх машинних даних для моніторингу користувачів та активів.
- **Ухвалення більш обґрунтованих рішень.** Більш ефективне розслідування інцидентів і активний захист, оцінка їх масштабу на основі даних про загрози з різних джерел, включаючи безкоштовні канали аналізу загроз, підписки на послуги сторонніх постачальників, правоохоронні органи, FS-ISAC, STIX / TAXII, Facebook ThreatExchange, а також інші внутрішні та загальнодоступні джерела.
- **Використання аналізу загроз.** Аналітичні дані по загрозам з небагатьох джерел можна об'єднувати, дедуплицировать і позначати ними ваги. Це дозволяє використовувати широкий спектр індикаторів компрометації для всіх аспектів моніторингу, оповіщення, звітності, розслідувань і криміналістичного аналізу.
- **Моніторинг в реальному часі.** Виявлення незвичайних дій, які можуть бути ознаками складних загроз, за допомогою статистичного аналізу, відхилень, виявлених додатком UBA, пошуку кореляцій, динамічних граничних умов і засобів виявлення відхилень від норми.
- **Оптимізація реагування на інциденти.** Оптимізація розслідувань динамічних, багатоетапних атак завдяки можливості візуалізувати інформацію про атаки і, отже, краще розуміти через час, а також будувати наступний ланцюжок різних подій для швидкого визначення подальших дій.
- **Підвищення операційної ефективності.** Автоматичне і напівавтоматичне прийняття рішень допомагає клієнтам прискорити розслідування та вжиття заходів з повним контекстом у програмі Adaptive Response.
- **Розуміння значення показників безпеки.** Спрощення аналізу за допомогою логічних або фізичних проявів візуальної таблиці, що дозволяє краще дізнатися про основні показники безпеки, включаючи доступ, DNS, ідентифікацію, електронну пошту, IDS, ліцензування, шкідливі ПЗ, події, продуктивність, ризики, SSL, шкідливі дії, трафік, UBA, оновлення, вразливість і мережеву активність.

Короткий огляд Enterprise Security (ES)

Панель моніторингу безпеки забезпечує постійний моніторинг і швидку оцінку ситуації, відстежуючи основні індикатори та метрики безпеки за даними з різних джерел (посвідчення, доступ, шкідливі програми, кінцеві точки та аналіз загроз). Усі аспекти джерел даних, основні індикатори та видимі виявлення на основі аналізуються та адаптуються з урахуванням робочих процедур організації. За допомогою інтерфейсу дисплея типу «вкажи и клацни» можна використовувати вбудовані процеси і дії прямо з графічного.	Аналіз інцидентів дозволяє швидко класифікувати події, розставляти пріоритети незвичайних подій і реагувати на них, визначаючи пріоритетний інцидент і порушені вузли. Отримуються дані про контекстний інцидент та використовується будь-який атрибут інциденту для пошуку додаткових індикаторів і відповідних подій. Фахівці з безпеки можуть співпрацювати і використовувати єдине виявлення про всі дії, пов'язані з інцидентом, а також аналізувати вихідні дані і переглядати журнал дій, пов'язаних з інцидентом.

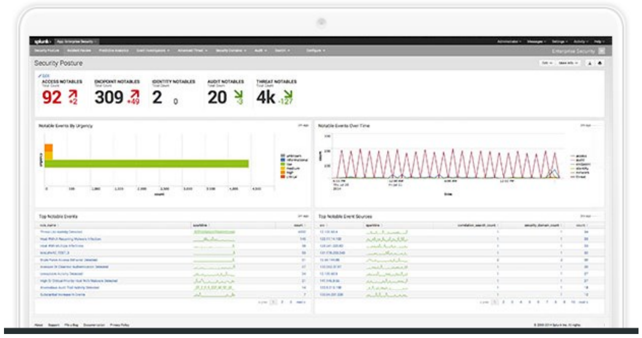


Рис. 07.13. Панель моніторингу безпеки

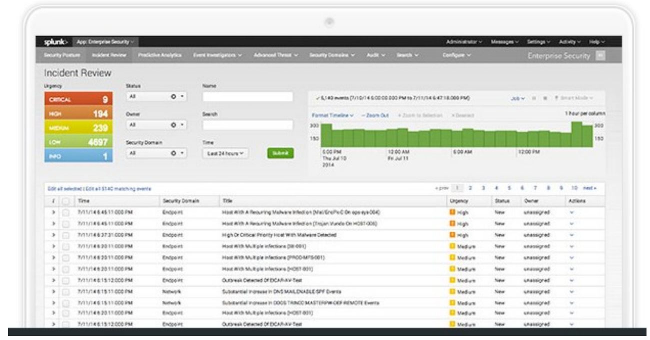


Рис. 07.14. Аналіз інцидентів

Аналізатор активів дає можливість перевірити кореляцію дій на пристроях, що виконують різні технології. Можна додати тимчасові рамки та скласти сценарій на основі подій, а потім створити пошукові запити для виявлення цих подій або поділитися сценарієм з іншою групою членів.

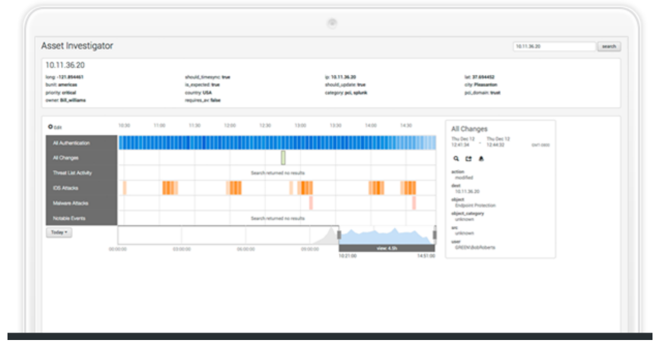


Рис. 07.15. Аналізатор активів

Панель моніторингу дій загроз забезпечує прямий доступ до подій, які корелюються з усіма джерелами аналітичних даних по загрозам: підписки на послуги сторонніх постачальників, правоохоронні органи, внутрішні та загальнодоступні джерела. Ця панель показує тенденції, дії користувачів і події для вузлів, пов’язані з аналітичними даними за загрозами. Використовуйте аналіз загроз у якості надісланої точки робочого процесу або для різних аспектів моніторингу, звітності та розслідування.

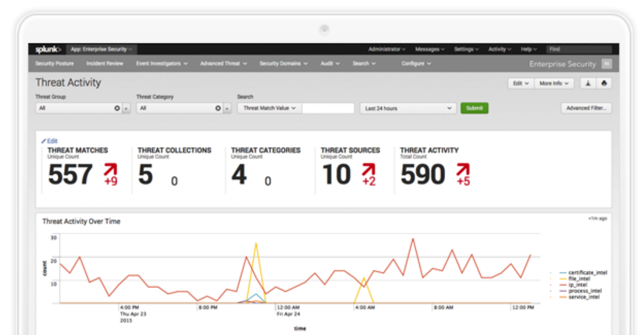


Рис. 07.15. Дії загрози

Журнал аналізатора запускає багатоетапні процеси аналізу та розслідування, дозволяючи зосередитися на відстеженні атак, у той час як система реєструє ваші пошукові запити, дії та нотатки, зроблені в ході розслідування. Усі важливі події, дії та помітки можна додати на тимчасову шкалу атак і розслідувань. Це дозволяє візуалізувати інформацію про атаки і краще зрозуміти, а також будувати наступний ланцюжок різних подій для швидкого визначення.

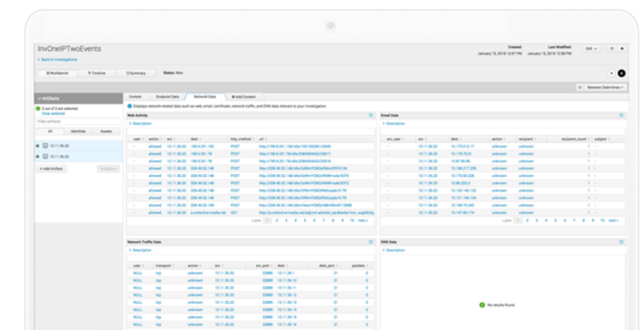


Рис. 07.16. Засоби для розслідування

Protocol Intelligence забезпечує швидкий доступ до мережевих даних і включає панелі з основними полями з найбільш розширеними протоколами. Дані надаються додатком Splunk App for Stream або мережевого розслідування. Побудовані звіти з ключовими полями з мережевими даними спрощують створення профілів для виявлення ознак незвичайної активності. Аналіз загроз використання електронної пошти, DNS-запитів і відповідей, а також сертифікатів SSL для прискореного виявлення інцидентів і реагування.

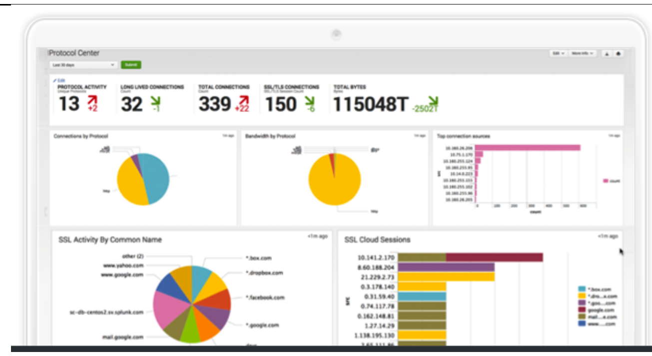


Рис. 07.17. Аналіз даних протоколів

Візуальні таблиці призначені для візуалізації даних користувачами, які відображають топологію, робочі процеси, комплексне виявлення, розслідування та реагування. Панелі моніторингу використовуються для зведення та виявлення у відповідному контексті з урахуванням конкретних вимог. Для створення візуальної таблиці доступний вибір із понад 100 показників безпеки, включаючи події.

Adaptive Response забезпечує ефективність використання, а також оптимізує виявлення загроз та вживання заходів, що використовуються з використанням контексту робочого процесу для прийняття рішень – автоматичного та напівавтоматичного. Аналітики можуть як обробляти дії реагування автоматично, так і аналізувати їх індивідуально, щоб

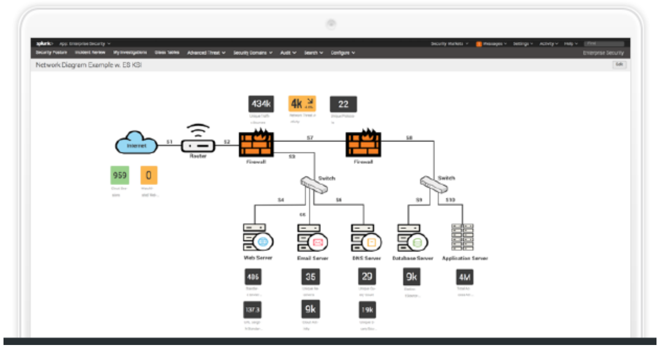


Рис. 07.18. Візуальні таблиці

можна було отримати додатковий контекст або ввести деякі заходи в системі безпеки, де наявні продукти різних постачальників.

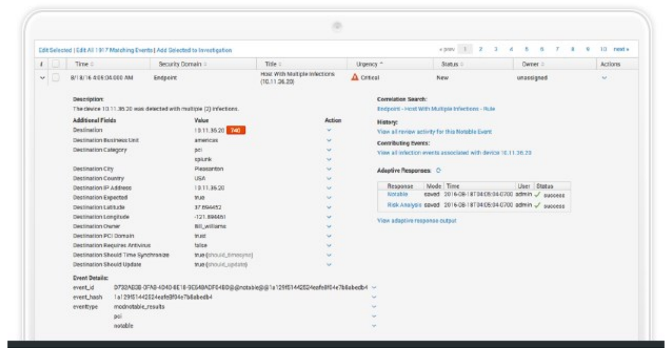


Рис. 07.19. Адаптивна відповідь

Grafana Dashboard Solution для Splunk використовується для візуалізації даних зі Splunk у Grafana. Чотири причини такого поєднання:
1. Альтернативний інструмент візуалізації
Splunk має власний UI для візуалізації даних, але Grafana пропонує ширші можливості кастомізації, більш зручний та гнучкий підхід до створення дашбордів.
2. Об'єднання даних з різних джерел
Grafana підтримує мультиджерельний підхід, що дозволяє:
Поєднувати дані зі Splunk з іншими джерелами (Prometheus, Zabbix, InfluxDB, OpenSearch тощо). Будувати єдину панель моніторингу для всіх систем.
3. Оптимізація продуктивності
Splunk добре підходить для збереження та пошуку логів, але важкі аналітичні запити можуть бути ресурсомісткими. Grafana, кешуючи або агрегуючи дані, може зменшувати навантаження на Splunk.
4. Покращені можливості інтеграції
Grafana має гнучкі опції алертів, інтеграцію з месенджерами (Slack, Telegram) і системами DevOps (Jenkins, Kubernetes).

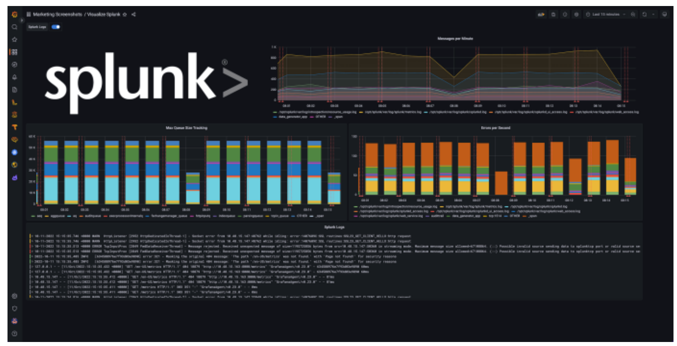


Рис. 07.20. Grafana Dashboard Solution для Splunk

Огляд IBM QRadar: архітектура та можливості

IBM QRadar — це комплексне рішення у сфері управління інформаційною безпекою та подіями (SIEM - Security Information and Event Management), яке використовується для моніторингу, аналізу та реагування на кіберзагрози в корпоративних мережах. QRadar поєднує в собі різні технології аналізу мережевого трафіку, журналів подій, управління вразливостями та автоматизації процесів реагування, що робить його одним із найбільш потужних продуктів у сфері кібербезпеки.
Перш ніж розглянути QRadar у інфраструктурі, необхідно зрозуміти кілька основних компонентів, які забезпечують його належну роботу.

Модульність

IBM QRadar SIEM (система управління інформацією та подіями безпеки) має модульну архітектуру, що дозволяє масштабувати розгортання шляхом додавання нових пристроїв, кінцевих точок і серверів до вашої інфраструктури для покращення аналізу та збору логів. Також можна інтегрувати додаткові модулі для аналізу, які легко завантажуються з IBM App Exchange. До них, зокрема, належать:

- ✓ QRadar Vulnerability Manager (менеджер вразливостей QRadar)
- ✓ QRadar Risk Manager (менеджер ризиків QRadar)
- ✓ QRadar Watson Integration (інтеграція з Watson)
- ✓ QRadar Incident Forensics (цифрова криміналістика або розслідування інцидентів інформаційної безпеки QRadar)

Цей список не є вичерпним, оскільки доступні й інші модулі для розширення функціональності.

Три рівні: що це таке?
Архітектура QRadar також використовує концепцію рівневості та складається з трьох основних рівнів, через які інформація передається від кінцевих точок до агента. Зверніть увагу, що ця архітектура застосовується у всіх типах розгортань, незалежно від розміру організації, складності мережі чи кількості використовуваних компонентів.
Але спершу… Як працює трирівневість та що це таке?
IBM QRadar у реальному часі збирає, обробляє, агрегує, корелює, зберігає та візуалізує дані з усіх підключених кінцевих точок. Опрацьовані та очищені дані надають вам аналітичну інформацію для моніторингу ІТ-інфраструктури. Це зазвичай реалізується у вигляді сповіщень, інцидентів та відповідей на загрози, які QRadar виявляє в режимі реального часу.
До розгортання можна також додати додаткові модулі, які ми згадували раніше. Наприклад, модуль Incident Forensics допомагає проаналізувати дії зловмисника, виявити його сліди та швидше зробити висновки на основі залишених артефактів. Це значно скорочує час, необхідний команді реагування на інциденти (IR), для розслідування загроз, зафіксованих QRadar. Він також сприяє швидкому усуненню порушень, запобіганню втрат даних і новим атакам.

Повертаємося до рівнів

Далі розглянемо, які три рівні містить архітектура QRadar і детальніше заглибимося в кожен із них:

- ❖ **Збір даних (Data collection)**
- ❖ **Обробка даних (Data processing)**
- ❖ **Пошук даних (Data searches)**
  - ➢ **Збір даних (Data Collection)** є нижнім або першим рівнем архітектури QRadar, і його місія проста: «збирати все з вашої мережі». Це включає такі типи даних, як:
    - ✓ Журнали подій (events, log files)
    - ✓ Мережеві потоки (flows)
    - ✓ Інші типи інформації, такі як результати сканування, конфігураційні файли, знімки трафіку (packet captures) тощо…

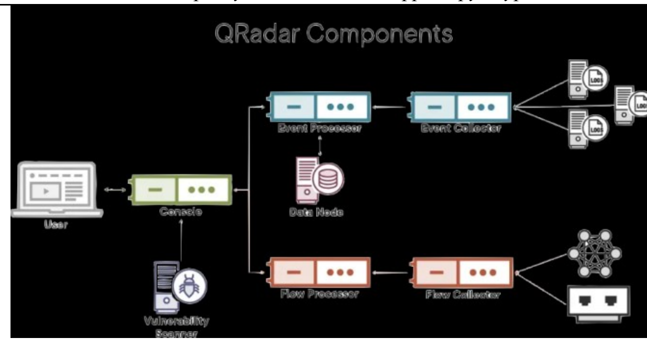


Рис. 07.21. Типова архітектура IBM QRadar

Для збору подій і потокових даних QRadar використовує QRadar Event Collectors та QRadar QFlow Collectors (про «потоки» ми поговоримо далі). QRadar може отримувати події з різних джерел у мережі, таких як фаєрволи, системи запобігання вторгнень (IPS) та інші пристрої безпеки. Для збору даних використовуються різні протоколи, найпоширенішим з яких є syslog. Інші варіанти:

- ✓ syslog-tcp
- ✓ SNMP
- ✓ SCP, SFTP, FTP (для отримання подій)
- ✓ JDBC
- ✓ Check Point OPSEC
- ✓ SMB/CIFS

Два основних типи даних. QRadar працює з двома основними типами даних:

- ✓ **Дані подій (Event Data).** Події відображають активність, яка відбулася на кінцевій точці у певний момент часу. Наприклад:
  - Зміна конфігурації фаєрвола
  - Збій у мережі
  - Невдалі спроби входу
  - Вхідні/вихідні підключення
  - Логування електронної пошти тощо
- ✓ **Дані потоків (Flow Data).** Мережеві потоки містять інформацію про сесії зв’язку між пристроями в мережі. Потоки конвертуються у так звані «записи потоку» (flow records), які містять:
  - IP-адреси
  - Порти
  - Обсяг переданих байтів
  - Кількість пакетів
  - Протокол зв’язку

Хоча цей етап носить назву Data Collection, дані все одно проходять на ньому первісну обробку:

1. **Парсинг (Parsing).** Сирі події перетворюються у зручний для читання формат. Це виконується за допомогою DSM Editor (Device Support Model Editor), що дозволяє швидко адаптувати дані під необхідний формат. Перед налаштуванням парсера необхідно забезпечити отримання журналів через syslog або інші протоколи.
2. **Нормалізація (Normalization).** На цьому етапі дані перетворюються у формат, що містить корисні поля (наприклад, IP-адреси), які QRadar може використовувати для подальшого аналізу.
3. **Визначення джерела подій.** Після нормалізації QRadar ідентифікує джерело подій на основі заголовків IP. Події агрегуються у записи, проте якщо QRadar не може визначити джерело журналів (log source), вони направляються до модуля аналізу трафіку для автоматичного виявлення. Якщо QRadar знаходить нове джерело логів, він надсилає запит на додавання цього джерела у консоль керування QRadar.

Крім цього, за допомогою модуля Incident Forensics можна виконувати повний перехоплення трафіку (packet capture) для глибшого аналізу загроз.

Таким чином, на рівні збору подій QRadar виконує основні завдання:

- ✅ Збирає дані за допомогою відомих протоколів
- ✅ Моніторить події та керує чергами для оптимального навантаження
- ✅ Парсить сирі події у формат, придатний для аналізу
- ✅ Аналізує джерела логів за допомогою DSM, підтримує автоматичне виявлення
- ✅ Агрегує події на основі спільних атрибутів
- ✅ Передає події до інших SIEM-систем, якщо це необхідно

Далі переходимо до наступного рівня — обробки даних (Data Processing).

- ➢ **Обробка даних (Data Processing).** Після того як дані пройшли всі необхідні етапи на першому рівні (збору даних), вони передаються на другий рівень — рівень обробки. Тут працюють два основних компоненти:
  - ✅ Обробники подій (Event Processors)
  - ✅ Обробники потоків (Flow Processors)

  Їх завдання — обробити отримані дані та передати їх на фінальний рівень. Пройшовши етап збору, дані трансформуються, перш ніж їх можна буде використовувати для пошуку та аналізу. Як відбувається обробка?

  1. Перше, через що проходять дані, — це механізм Custom Rules Engine (CRE). Це механізм спеціальних правил, який аналізує вхідні події. Саме тут створюються сповіщення та інциденти (offenses & alerts) на основі отриманих даних. Усі події зберігаються для довготривалого зберігання (storage persistence).
  2. Як працюють правила в CRE? Адміністратори налаштовують користувацькі правила (custom rules) через консоль QRadar. Якщо отримані події відповідають умовам правил, спрацьовують певні дії або реакції. Таким чином, QRadar може автоматично виявляти загрози та реагувати на них у реальному часі.

3. Передача подій у консоль в реальному часі Обробники подій (Event Processors) передають дані безпосередньо в консоль QRadar. Вся інформація миттєво відображається у вкладці "Log Activity" (Журнал активності). Дані обробляються в реальному часі, а не відтворюються з бази.
4. Збереження даних. Події не тільки аналізуються в потоці, але й зберігаються для подальшого аналізу та розслідувань. Отже, другий рівень відповідає за аналіз подій, застосування правил безпеки та збереження даних для подальшого використання.

Крім того, у Data Processing є ще один рівень абстракції, який ми раніше не згадували, – це Magistrate. Custom Rules Engine (CRE) не передає співставлені події безпосередньо на консоль. Замість цього вони спочатку надходять до Magistrate на консолі QRadar. Його завдання – створювати та керувати інцидентами (offenses) на консолі. Magistrate виконує три основні функції:

- ✓ Правила для інцидентів (Offense Rules) – визначає, що робити у разі створення інциденту.
- ✓ Керування інцидентами (Offense Management) – оновлення статусу інцидентів, додавання додаткової інформації тощо.
- ✓ Зберігання інцидентів (Offense Storage) – всі події зберігаються у базі даних PostgreSQL.

Окрім цього, Magistrate Processing Core (MPC) відповідає за кореляцію інцидентів з повідомленнями про події, що надходять від різних Event Processor компонентів.

Далі розглянемо останній рівень — пошук і аналіз даних (Data Searches).

- ➢ **Пошук даних (Data Searches)**

На завершальному етапі нормалізовані та оброблені дані передаються до останнього рівня в QRadar, де вони стають доступними для пошуку користувачами. Це дозволяє аналізувати, створювати звіти та розслідувати сповіщення, правила та інциденти через консоль QRadar. Консоль також надає можливість аналітикам виконувати дії та адміністративні завдання.

У розподілених середовищах консоль QRadar не виконує обробку подій і потоків, а також не зберігає дані. Натомість вона використовується як інтерфейс користувача, де можна здійснювати пошуки, переглядати звіти, отримувати сповіщення та проводити розслідування.

- ➢ **Приклади архітектури**
  - ✓ **Розподілена архітектура.** Приклад 1: Кілька колекторів і процесорів, підключених до консолі, допомагають розподілити навантаження між декількома компонентами та забезпечують розділення середовищ.
  - ✓ **Розподілена архітектура.** Приклад 2: Тут ми маємо 2 Data Collection з 1 процесором подій

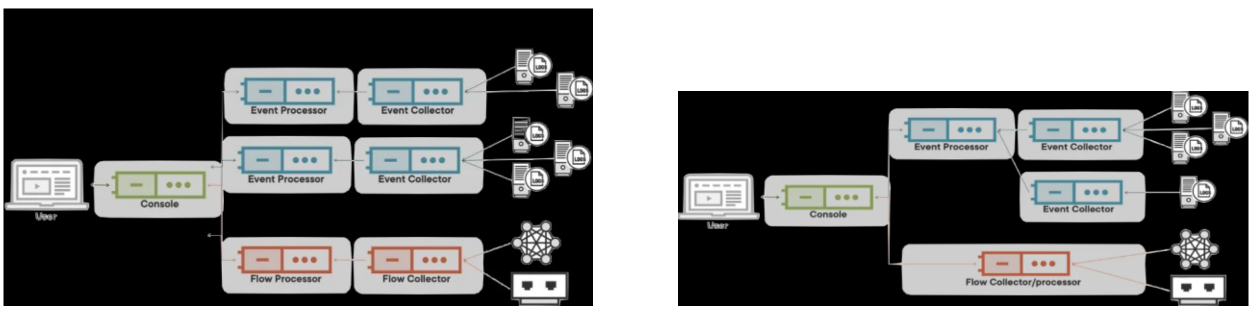


Рис. 07.21. Приклади розподіленої архітектури QRadar

- ✓ **Концепція централізованої архітектури QRadar** передбачає, що всі його компоненти працюють в межах єдиного серверного рішення. Такий підхід найчастіше використовується в малих та середніх компаніях, де обсяг подій і мережевого трафіку невеликий. QRadar має спеціальний компонент "все в одному" (All-in-One), який об'єднує всі ключові функції системи: збір даних, обробку подій та потоків, а також забезпечує інтерфейс користувача. Це дозволяє розгорнути SIEM-рішення без необхідності окремих серверів для різних функцій.
- ✓ **Мультитенантність (мультиорендність) у QRadar** означає можливість обслуговування кількох клієнтів в одному спільному середовищі. Замість того щоб розгортати окреме середовище для кожного клієнта, можна використовувати єдину консоль, яка керує декількома процесорами подій і потоків, а також колекторами. При цьому дані кожного клієнта залишаються ізольованими, що гарантує безпеку та конфіденційність інформації.
- ✓ **Хмарне розгортання** - QRadar може працювати як локальне рішення (on-premises) або як хмарне рішення (QRadar on Cloud, QROC), що дозволяє організаціям обирати зручний варіант.

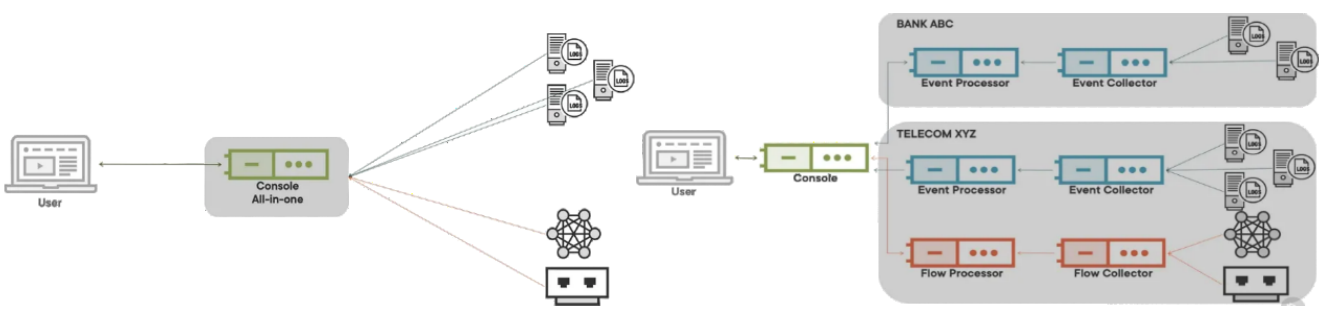


Рис. 07.22. Приклади централізованої та мультитенантної архітектури QRadar

Ліцензування IBM QRadar

QRadar має гнучку систему ліцензування, яка залежить від конкретного модуля та обсягу оброблюваних подій. Основні підходи:

- ✓ Ліцензія на обсяг подій (EPS - Events Per Second). Використовується для SIEM і визначає кількість подій, які система може обробити за секунду. Наприклад, організація може придбати ліцензію на 5000 EPS або більше.

- ✓ Ліцензія на мережевий трафік (FPM - Flows Per Minute). Використовується для аналізу мережевого трафіку (QNI, Network Insights). Дозволяє обробляти певну кількість мережевих потоків на хвилину.
- ✓ Ліцензія для QRadar on Cloud (QROC). Передбачає підписку на SaaS-рішення з оплатою за використання ресурсів.
- ✓ Модульні ліцензії

Цікаві факти про IBM QRadar

✓ IBM QRadar входить до списку лідерів ринку SIEM-рішень за оцінками Gartner та Forrester.
✓ Включає вбудований механізм машинного навчання для виявлення складних атак.
✓ Поєднує SIEM та SOAR в єдиній платформі, що спрощує реагування на інциденти.
✓ Має власний маркетплейс (IBM Security App Exchange) для розширення функціоналу.

Огляд Elastic Security.

Elastic Security - окремий продукт, створений на базі ELK Stack, який спеціалізується на кібербезпеці. У цій темі доречніше розглянути саме його, а не більш відомий та розпіарений ELK Stack - універсальний набір інструментів для роботи з логами та даними. Elastic Security – це спеціалізоване рішення для кібербезпеки, яке базується на ELK Stack. Тобто Elastic Security є частиною екосистеми ELK, але з додатковими можливостями для безпеки.

- ➢ **ELK Stack (Elastic Stack)** - набір інструментів для збору, зберігання, аналізу та візуалізації логів і даних. Він складається з:
  - ✓ **Elasticsearch** – пошуковий та аналітичний рушій для зберігання та обробки даних.
  - ✓ **Logstash** – інструмент збору, обробки та перенаправлення логів.
  - ✓ **Kibana** – інтерфейс для візуалізації даних та аналітики.
  - ✓ **Beats** – легкі агенти для збору даних із різних джерел.

  Elastic Stack використовується для моніторингу логів, бізнес-аналітики, аналізу продуктивності та багатьох інших задач.
- ➢ **Elastic Security**, створений на базі ELK Stack, який спеціалізується на кібербезпеці. Він включає:
  - ✓ Захист кінцевих точок (**Endpoint Security**) – запобігання та виявлення загроз на пристроях.
  - ✓ **SIEM (Security Information and Event Management**) – збір та аналіз подій безпеки в реальному часі.
  - ✓ **Threat Hunting** – активний пошук загроз у даних.
  - ✓ Аналітику загроз (**Threat Intelligence**) – інтеграцію зі сторонніми джерелами загроз.

Elastic Security поєднує функції виявлення загроз у SIEM із засобами запобігання та реагування на інциденти на кінцевих точках в єдиному рішенні. Ці аналітичні та захисні можливості, посилені швидкістю та розширюваністю Elasticsearch, дозволяють аналітикам захищати організацію від загроз ще до того, як вони спричинять шкоду чи втрати.

Ключові можливості та переваги Elastic Security:

- ✓ **Централізоване управління безпекою**: єдиний інтерфейс для моніторингу, виявлення та реагування на загрози в масштабі всієї інфраструктури.
- ✓ **Detection Engine**: ефективне виявлення атак, помилкових конфігурацій та підозрілої активності на основі правил і попередньо налаштованих задач машинного навчання, включно з безсигнатурними атаками.
- ✓ **Інтерактивні візуалізації**: потужні засоби для дослідження подій, аналізу зв'язків між процесами та розслідування інцидентів.
- ✓ Вбудоване управління інцидентами (**Case Management**): можливість створювати, відслідковувати інциденти та автоматизувати дії у відповідь.
- ✓ **Інтеграція з популярними платформами**: гнучка взаємодія з зовнішніми сервісами для спрощення обробки інцидентів та розширення функціональності.
- ✓ **Потужна автоматизація та гнучке адміністрування**: можливість налаштовувати, масштабувати та інтегрувати рішення під потреби організації.

Компоненти та робочий процес Elastic Security

Наступна діаграма наочно ілюструє робочий процес Elastic Security.

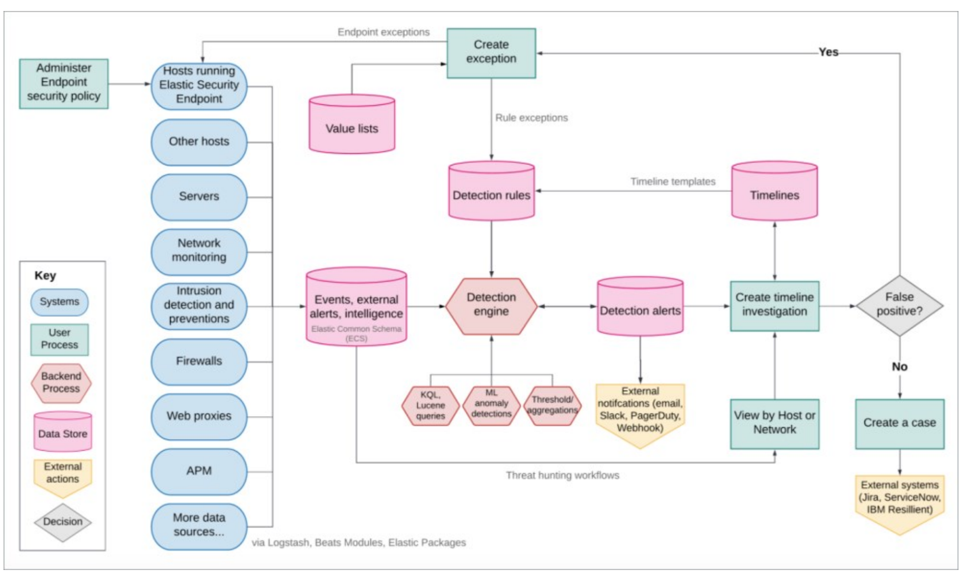


Рис. 07.23. Компоненти та робочий процес Elastic Security

Короткий огляд процесу та його основних компонентів:

Дані надходять з різних джерел, в тому числі з хостів, до **Elasticsearch** у такий спосіб:

- **Elastic Endpoint Security** – інтеграція Elastic Agent, яка захищає хости від шкідливого програмного забезпечення та передає наступні набори даних:
  - ✓ Windows: процеси, мережеві з'єднання, файли, DNS, реєстр, завантаження DLL та драйверів, виявлення шкідливого ПЗ
  - ✓ Linux/macOS: процеси, мережеві з'єднання, файли
- Інтеграції (**Integrations**) – зручний спосіб надсилання даних у Elastic Stack. Доступні інтеграції для популярних сервісів та платформ, таких як Nginx, AWS, MongoDB, а також для універсальних джерел, як-от лог-файли.
- Модулі Beat (**Beat modules**) – легковагові агенти збору даних. Вони дозволяють отримувати та обробляти специфічні набори даних із поширених джерел, таких як події хмарних сервісів, журнали ОС та метрики. До основних модулів, пов'язаних із безпекою, належать:

Отримані дані уніфікуються відповідно до **Elastic Common Schema (ECS)** і зберігаються у **Elasticsearch** для подальшого аналізу.

Додаток **Elastic Security** у **Kibana** використовується для керування Detection engine, Cases та Timeline, а також для адміністрування хостів із запущеним Endpoint Security.

- **Detection engine** – автоматичний пошук підозрілої активності хостів і мережі за допомогою:
  - ✓ Правил виявлення (**Detection rules**) – періодично аналізують дані (індекси Elasticsearch), отримані з ваших хостів, на предмет підозрілих подій. Якщо така подія виявлена, створюється сповіщення. Сповіщення можуть надсилатися у Slack, електронну пошту чи інші зовнішні системи. Ви можете створювати власні правила або використовувати попередньо налаштовані.
  - ✓ Винятків (**Exceptions**) – дозволяють зменшити шум і кількість хибнопозитивних спрацьовувань. Винятки прив'язані до правил і блокують створення сповіщень, якщо виконуються певні умови. Списки значень (Value lists) містять дані про події, які можуть бути використані як критерії винятків. Якщо Elastic Endpoint Security встановлено на ваших хостах, можна додавати винятки для шкідливого ПЗ безпосередньо у додатку Security.
  - ✓ Задач машинного навчання (**Machine learning jobs**) – автоматичне виявлення аномалій у подіях хостів і мережі. Для кожного хоста визначаються бали аномальності (Anomaly scores), які можна використовувати в правилах виявлення загроз.
  - ✓ **KQL/Lucene queries, Thresholds/Aggregations** – для кастомного пошуку та агрегацій.

Після спрацьовування правил

- **Detection Alerts** – тригери можуть бути надіслані в Slack, Email, Jira, ServiceNow, Webhooks тощо.
- **Timeline** – робочий простір для розслідування подій та сповіщень. Використовує запити (queries) та фільтри (filters) для деталізації подій, пов'язаних із конкретним інцидентом. Шаблони Timeline (Timeline templates) можуть бути прикріплені до правил та використовуватися при розслідуванні сповіщень.Збереження та обмін Timeline – дозволяє ділитися розслідуваннями з іншими користувачами та додавати їх до Cases
- **Cases** – внутрішня система управління інцидентами безпеки. Дозволяє створювати, відстежувати та обмінюватися інформацією про інциденти безпосередньо у Security. Інтегрується із зовнішніми системами управління заявками
- **Адміністрування.** Перегляд та керування хостами, на яких працює Elastic Endpoint Security. Надсилання даних у Elastic Security. Процес збору даних для Elastic Security та встановлення інтеграції Endpoint Security описано у відповідних розділах документації.

Візуалізація та адміністрування:

Elasticsearch – розподілена система зберігання, пошуку та аналітики в реальному часі. Вона чудово підходить для індексації потоків напівструктурованих даних, таких як журнали чи метрики.

Kibana – платформа для аналітики та візуалізації даних, розроблена для роботи з Elasticsearch. За допомогою Kibana можна здійснювати пошук, переглядати та аналізувати дані, а також створювати різноманітні графіки, таблиці та карти.

Таким чином робочий процес Elastic Security виглядає наступним чином:

Дані з різних систем потрапляють у Elastic Stack. Detection Engine аналізує ці дані.У разі виявлення підозрілої активності створюється Alert. За необхідності запускається Timeline Investigation. Якщо підтверджено загрозу – створюється Case. Інциденти можуть надсилатися до зовнішніх систем.

Ліцензування. Elastic Security доступний як у безкоштовній, так і у платних версіях.

1. Безкоштовна версія (**Basic License**) Elastic Security включена у безкоштовну версію Elastic Stack. Базові функції:
   - ✓ Збір, пошук та аналіз логів
   - ✓ Візуалізація даних у Kibana
   - ✓ Фільтрація, обробка та збагачення подій безпеки
   - ✓ Ручне дослідження загроз та аналіз інцидентів

   доступні без додаткових витрат.
2. Платні плани (**Gold, Platinum, Enterprise License**). Щоб отримати розширені можливості, потрібна комерційна ліцензія (Elastic Security for Elasticsearch Service). У платних версіях додається:
   - ✓ Автоматизоване виявлення загроз (Detection Engine) – правила кореляції та аналітика загроз.
   - ✓ Автоматизація реагування (SOAR-функції) – інтеграція з SIEM/SOAR рішеннями, керування інцидентами.
   - ✓ Endpoint Security – розширений захист кінцевих точок із можливістю блокування атак.
   - ✓ Машинне навчання для поведінкового аналізу – виявлення аномалій.
   - ✓ Доступ до підтримки Elastic – технічна допомога та консультації.

Безкоштовна версія достатня для базового моніторингу та аналізу загроз, але для повноцінного SIEM-рішення з автоматизацією, інтеграціями та захистом кінцевих точок рекомендується платна ліцензія.

Детальніше про актуальні умови ліцензування можна подивитися на офіційному сайті Elastic.

Огляд MS SCOM як інструменту системного моніторингу від Microsoft.

Що ж таке Microsoft SCOM (System Center Operations Manager)?

У попередніх лекціях ми вже ознайомилися з основним призначенням Microsoft SCOM. Зараз зосередимо увагу на архітектурі та практичних аспектах впровадження цього інструменту.

Важливі компоненти Microsoft SCOM

System Center Operations Manager відстежує різні комп'ютери, пристрої, програми та служби в корпоративному ІТ-середовищі та повідомляє адміністраторам, які з цих об'єктів моніторингу справні, а які – ні. Він також надсилає сповіщення, коли виявляє проблеми, надає корисну інформацію про виявлену проблему, знаходить її причину та впроваджує можливе рішення.

Для виконання всіх вищезазначених завдань різні компоненти працюють разом у SCOM. Ці компоненти є частиною групи керування, яка створюється під час інсталяції SCOM і є основною функціональною одиницею. Компоненти можуть існувати на одному сервері або можуть бути розподілені між кількома серверами. Компоненти SCOM включають наступне:

- **Оперативна база даних**. База даних SQL Server , яка містить усі конфігураційні дані та зберігає дані моніторингу на короткий термін.
- **База даних сховища даних.** Також база даних SQL Server, хоч і така, яка зберігає дані моніторингу та сповіщень для історичних цілей, тобто довгострокового зберігання.
- **Сервер керування.** Адмініструє групу керування та спілкується з базою даних.
- **Сервер звітності.** Створює та представляє звіти, створені з даних у базі даних сховища даних .
- **Агент.** Служба, встановлена на комп'ютері для збору даних моніторингу, створення сповіщень і запуску відповідей; він повідомляє серверу керування в групі керування.
- **Послуга Агент моніторингу.** Збирає дані про продуктивність, виконує завдання та надсилає зібрані дані на сервер керування.

SCOM, як вказує його назва, не є вузькоспеціалізованим інструментом моніторингу MS. Це скоріше набір програмного забезпечення для розгортання, налаштування, керування та моніторингу всіх серверів, компонентів і служб ІТ-інфраструктури Windows.

Operations Manager призначений для моніторингу всієї інфраструктури, тому часто це складний звір із багатьма рухомими частинами, попередніми умовами та залежностями, ролями сервера, агентами тощо. Корпорація Майкрософт детально описує їх у своєму посібнику щодо системних вимог для SCOM, але ми трошки пізніше коротко пробіжимося по цим вимогам. Архітектура SCOM виглядає приблизно так, як показано на рис. 07.07.

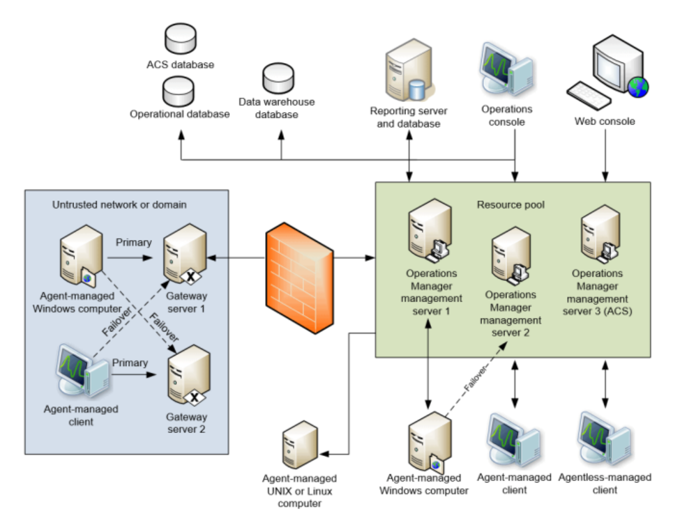


Рис. 07.07 Архітектура SCOM

Агенти Microsoft SCOM

У System Center Operations Manager агент — це служба, встановлена на комп'ютері, яка шукає дані конфігурації і заздалегідь збирає відомості для аналізу та створення звітів, вимірює стан працездатності об'єктів, що відстежуються, таких як база даних SQL або логічний диск, і виконує завдання на вимогу оператора або у відповідь умову. Вона дозволяє Operations Manager відстежувати операційні системи Windows, Linux та UNIX, а також компоненти ІТ-служби, встановлені на них, наприклад веб-сайт або контролер домену Active Directory.

- **Агент Windows**

  На відстежуваному комп'ютері Windows агент Operations Manager вказаний як служба Microsoft Monitoring Agent (MMA). Служба Microsoft Monitoring Agent збирає дані про події та продуктивність, виконує завдання та інші робочі процеси, визначені в пакеті керування. Навіть якщо ця служба не може підключитися до сервера керування, якому вона підпорядковується, вона продовжує працювати і поміщає зібрані дані та події в чергу на диску комп'ютера, що спостерігається. Під час відновлення підключення служба Microsoft Monitoring Agent надсилає зібрані дані та події на сервер керування.

  Іноді Microsoft Monitoring Agent називають службою працездатності.

  Служба Microsoft Monitoring Agent також працює на серверах керування. На сервері керування ця служба виконує робочі процеси моніторингу та керує обліковими даними. Для запуску робочих процесів служба викликає процеси MonitoringHost.exe за допомогою вказаних облікових даних. Ці процеси виконують спостереження та збирають дані журналів подій, дані інструментарію керування Windows (WMI), а також виконують такі дії, як запуск скриптів. Агент Operations Manager надсилає попередження та дані виявлення на призначений основний сервер управління, який записує ці дані до робочої бази даних. Крім того, агент відправляє дані про події, продуктивність та стан на основний сервер управління, який одночасно записує ці дані в робочу базу даних і в базу даних сховища даних.

Агент надсилає дані відповідно до параметрів розкладу для кожного правила та монітора. У разі оптимізованих правил збору даних дані передаються тільки в тому випадку, якщо вибірка лічильника відрізняється від попередньої вибірки на вказану величину допуску, наприклад, на 10%. Це допомагає скоротити мережевий трафік та обсяг даних, що зберігаються у робочій базі даних.

Крім того, всі агенти регулярно відправляють пакет даних, званий пульсом , на сервер управління: за умовчанням це відбувається кожні 60 секунд. Мета пульсу полягає у перевірці доступності агенту та зв'язку між агентом та сервером управління. Детальний опис реалізації механізму пульс див. у статті [How Heartbeats Work in Operations Manager] (Принципи роботи пульсу в Operations Manager) .

Якщо коротко, то SCOM використовує тактові сигнали для моніторингу каналів зв'язку між агентом і основним сервером керування агентом. Пакет даних регулярно, за замовчуванням кожні 60 секунд, надсилається від агента на сервер керування через порт 5723 (TCP).

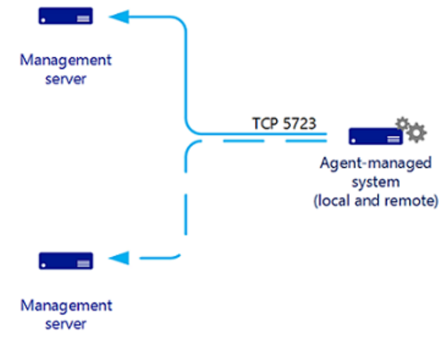


Рис. 07.08 Management server - Agent-managed host

Якщо агент чотири рази не може надіслати Heartbeats сигнал, створюється сповіщення про збій серцевого ритму служби працездатності, і сервер керування намагається зв'язатися з комп'ютером за допомогою ping. Якщо комп'ютер не відповідає на запит ping, створюється сповіщення, що не вдалося підключитися до комп'ютера.

Для кожного агенту, Operations Manager запускає спостерігач служби працездатності, який спостерігає стан віддаленої служби працездатності з точки зору сервера управління. Агент взаємодіє із сервером управління через TCP-порт 5723.

- **Агент Linux/UNIX**

Архітектура агенту UNIX та Linux істотно відрізняється від архітектури агенту Windows. Агент Windows має службу працездатності, відповідальну за оцінку працездатності комп'ютера, що відстежується. Агент UNIX та Linux не запускає службу працездатності. Натомість він передає відомості до служби працездатності на сервері управління для оцінки. На сервері керування запускаються всі робочі процеси для моніторингу стану операційної системи, визначені у реалізації пакетів керування UNIX та Linux:

✓ Диск	✓ Операційна система
✓ Процесор	✓ Процеси
✓ Пам'ять	✓ Файли журналу
✓ Мережеві адаптери	

Агенти UNIX та Linux для Operations Manager складаються з диспетчера об'єктів CIM (тобто сервера CIM) та набору постачальників CIM.

CIM - Common Information Model. Це модель даних, яка використовується для представлення та обміну інформацією про керовані об'єкти в середовищі SCOM. Диспетчер об'єктів CIM - це серверний компонент, що реалізує WS-Management зв'язку, автентифікації, авторизації та відправки запитів постачальникам.

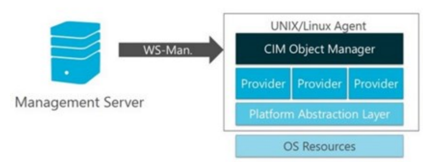
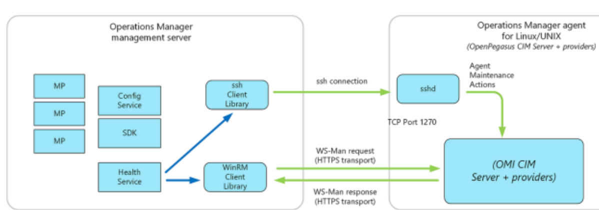


Рис. 07.09 Management server – Unix/Linux host

WS-Management (Web Services Management) - це відкритий стандарт, який описує протокол на основі SOAP для управління серверами, пристроями, програмами та різними веб-сервісами. Постачальники є ключовим елементом реалізації CIM в агенті, визначаючи класи та властивості CIM, взаємодіючи з API ядра для отримання необроблених даних, форматуючи дані (наприклад, обчислюючи різниці та середні значення) та обслуговуючи запити, надіслані диспетчером об'єктів CIM. В операційних системах з System Center Operations Manager 2007 R2 по System Center 2012 SP1 диспетчер об'єктів CIM, що використовується в агентах UNIX та Linux Operations Manager, є сервером OpenPegasus. Постачальники, які використовуються для збору даних моніторингу та складання відповідних звітів, розробляються Майкрософт та надаються на сайті CodePlex.com з відкритим кодом.



У System Center 2012 R2 Operations Manager цей підхід було змінено, а в основі агентів UNIX і Linux як диспетчер об'єктів CIM тепер лежить повністю узгоджена реалізація інфраструктури ***Open Management Infrastructure (OMI).*** У випадку агентів UNIX/Linux Operations Manager OMI замінює OpenPegasus. Як і OpenPegasus, OMI - це спрощена і переносима реалізація диспетчера об'єктів CIM з відкритим кодом, хоча вона легша за вагою і портативніша, ніж OpenPegasus. Ця реалізація, як і раніше, використовується в System Center 2016 — Operations Manager та пізніших версій.

Обмін даними між сервером управління та агентом UNIX та Linux ділиться на дві категорії: обслуговування агента та моніторинг працездатності. На сервері керування для взаємодії з комп'ютером UNIX або Linux використовуються два протоколи:

- ✓ Secure Shell (SSH) та протокол SFTP. Використовується для завдань з обслуговування агента, включаючи встановлення, оновлення та видалення агентів.
- ✓ Веб-служби для керування (WS-Management). Використовується для всіх операцій моніторингу та виявлення вже встановлених агентів.

Взаємодія між сервером керування Operations Manager та агентом UNIX та Linux здійснюється за допомогою WS-Man за протоколом HTTPS та інтерфейсом WinRM. Усі завдання з обслуговування агента виконуються за протоколом SSH через порт 22. Спостереження за працездатністю виконується за допомогою WS-MAN через порт 1270. Сервер управління запитує дані конфігурації та продуктивності через WS-MAN, перш ніж оцінити дані та повідомити стан працездатності. Усі дії, такі як обслуговування агентів, моніторів, правил, завдань та відновлень, налаштовуються для використання попередньо заданих профілів відповідно до вимог застосування непривілейованого або привілейованого облікового запису.

На зміну синхронним інтерфейсам API WSMAN, які використовувалися за умовчанням, прийшли нові асинхронні API інфраструктури керування (MI) Windows. Вони дозволяють виконувати масштабування та моніторинг кількох систем UNIX та Linux на одному сервері управління в System Center Operations Manager 2016 та пізніших версій.

Не будемо зупинятись на деталях того, як усе це працює, оскільки це велика тема, і ці деталі добре описано в документації, яку Ви будете вивчати, якщо доведеться налаштовувати такого звіра☺ . Проте, коротко кажучи, Operations Manager виявляє сервери для моніторингу та встановлює на кожному з них агента, який «збиратиме дані, порівнюватиме вибіркові дані з попередньо визначеними значеннями, створюватиме сповіщення та запускатимемо відповіді». Сервер керування надсилає деталі конфігурації та логіку моніторингу кожному агенту, використовуючи пакети керування (про це трохи пізніше), які визначають логіку моніторингу для кожного компонента. Монітори збирають дані про стан «здоров'я» об'єкта, що контролюється, а правила визначають, які події та дані продуктивності збирати та що з ними робити.

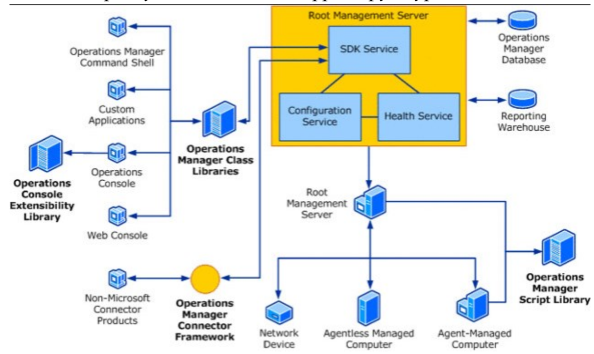


Рис. 07.10 Архітектура SCOM

Стандартна інсталяція SCOM — це, по суті, лише базова структура, на якій можна розмістити пакети керування. Кожен пакет визначає як структуру програми або служби, яку слід відстежувати, так і всі її компоненти та їхні взаємозв'язки (модель служби), а також дані, які слід збирати для оцінки працездатності цієї програми (модель працездатності).

Агент автоматично виявляє всі попередньо визначені «об'єкти» в моделі обслуговування для пакета керування. Наприклад, для SQL Server це включатиме бази даних, файли баз даних, завдання тощо. Для кожного об'єкта (логічно згрупованого в класи) він збирає дані моніторингу, визначені моделлю працездатності, і надсилає їх назад на сервер керування, який зберігає дані моніторингу та сповіщень в операційній базі даних (тут зберігається поточна звітність) і в сховищі даних (для історичних даних).

SCOM — це гарний інструмент моніторингу на системному рівні для звітування про загальний стан і продуктивність різноманітної серверної інфраструктури та служб, які на ній працюють. Він збирає дані про широкий спектр системних показників, служб, станів процесів і лічильників продуктивності Windows для кожного сервера. Він відстежуватиме журнали подій сервера. Він повідомлятиме про будь-які невдалі входи на сервер та інші помилки та попередження сервера. Він попередить вас про проблеми з процесором, пам'яттю чи вводом/виводом або помилки мережі. Він сповістить вас, коли на фізичному диску чи логічному томі буде мало місця для зберігання.

Проблеми справді виникають, лише якщо ви намагаєтеся розширити функціональність SCOM для моніторингу складних програм або служб, таких як SQL Server. SCOM не розроблявся для того, щоб заглиблюватися в «нутрощі» складної служби, щоб допомогти зрозуміти, що саме там відбувається, коли щось йде не так. Продукт створений та задуманий як спосіб надання загальної картини моніторингу.

Налаштування правил, моніторів і сповіщень SCOM для пакетів керування певними конкретними ролями є складною справою, що ускладнюється відносно поганою документацією. Для цього потрібні спеціальні знання як SCOM, так структури та алгоритмів ролі чи служби, моніторинг якої налаштовується. Зазвичай, налаштування такого моніторингу за допомогою SCOM передбачає написання користувацьких правил і моніторів, або, в крайньому випадку, навіть написання власного пакету керування. Навіть після того, як усе налаштовано та запрацює, багато команд все одно виявляють, що отримані дані моніторингу важко зрозуміти. Знову ж таки, для інтерпретації даних і дій на основі них потрібна спеціальна експертиза. Складність для організації такого моніторингу полягає в розумінні межі між тим, що SCOM може і повинен контролювати, і тим, що можна зробити краще та більш масштабованим способом за допомогою інструменту, розробленого спеціально для моніторингу спеціалізованих служб.

Таким чином, SCOM є чудовим інструментом системного рівня, але в ньому будуть відсутні важливі діагностичні дані та дані для усунення несправностей, необхідні для дослідження деталей проблеми продуктивності нижчого рівня, таких як статистика виконання, плани запитів, стани очікування, ланцюг блокування тощо.

Щоб зовсім Вас не розчарувати у можливостях SCOM розглянемо його інформаційну панель

Користувач сам налаштовуєте інформаційну панель із інформацією, яку хоче бачити. Якщо необхідно побачити базову лінію для метрики, щоб порівняти поточну поведінку з «нормою», потрібно буде створити базову лінію. Як зазначалося раніше, команди часто створюють необхідну інформаційну панель фрагментарно, оскільки вони дізнаються, які дані їм дійсно потрібні для діагностики кожного типу проблеми. Це - класичний, нормальний підхід до побудови гарної системи моніторингу.

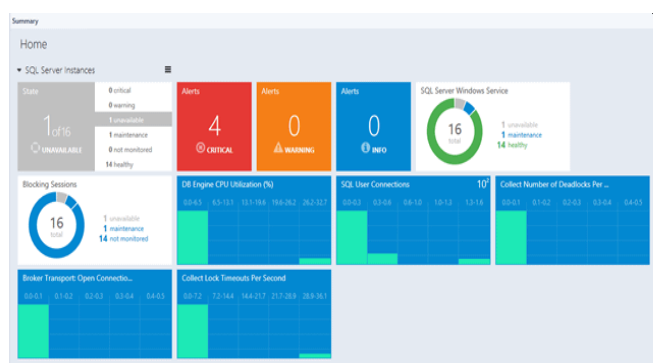


Рис. 07.11 Інформаційна панель SCOM

Загальним результатом є те, що, хоча SCOM пропонує єдиний координаційний центр для всього моніторингу всіх систем, він недоступний для тих у IT-команді, яким може знадобитися реагувати на попередження, але яким бракує повних, детальних знань про домен всі елементи та складові інфраструктури, що моніториться. Але, погодьтеся, такі знання необхідні для побудови будь якої моніторингової системи.

Функціонал SCOM, що базується на RBAC

В передостанній та останній версіях 2022-2025 року SCOM підтримує вдосконалений контроль доступу на основі ролей і нові вбудовані ролі для покращення взаємодії з користувачем. Наприклад, він підтримує роль адміністратора лише для читання, яка надає дозволи на читання в SCOM, включаючи звітування. Роль уповноваженого адміністратора подібна до ролі адміністратора лише для читання, за винятком дозволів на звітування. Адміністратори також можуть створювати спеціальні ролі користувачів із певними дозволами в SCOM.

Трошки докладніше про контроль доступу на основі ролей (RBAC). Це метод обмеження доступу до мережі на основі ролей окремих користувачів на підприємстві. Організації використовують RBAC, також званий ролевою безпекою , для аналізу рівнів доступу на основі ролей і обов'язків співробітника.

Обмеження доступу до мережі є важливим для організацій, які мають багато співробітників, підрядників або дозволяють третім сторонам , таким як клієнти та постачальники, мати доступ до мережі, оскільки ефективний моніторинг доступу до мережі може бути складним. Компанії, які залежать від RBAC, краще можуть захистити свої конфіденційні дані та критично важливі програми. RBAC гарантує, що користувачі отримують доступ лише до інформації, необхідної для виконання своєї роботи, запобігаючи доступу до інформації, яка їх не стосується.

Роль працівника в організації визначає дозволи, які надаються особі, гарантуючи, що працівники нижчого рівня не зможуть отримати доступ до конфіденційної інформації або виконувати завдання високого рівня.
RBAC базується на концепції ролей і привілеїв. Доступ залежить від таких факторів, як повноваження, компетентність і відповідальність. Доступ до мережі та інших ресурсів, як-от доступ до певних файлів або програм, може обмежувати працівник. Наприклад, певні файли можуть бути доступними лише для читання, але до певних файлів або програм можна надати тимчасовий доступ для виконання завдання. Організації можуть визначити, чи є користувач кінцевим користувачем, адміністратором чи спеціалістом. Ці ролі також можуть збігатися або давати різні рівні дозволів для окремих ролей.

Використання RBAC має багато переваг, зокрема такі:
- **Покращена ефективність роботи.** За допомогою RBAC компанії можуть зменшити потребу в паперовій роботі та зміні паролів , коли вони наймають нових співробітників або змінюють ролі існуючих співробітників. RBAC дозволяє організаціям швидко додавати та змінювати ролі, а також застосовувати їх на різних платформах, операційних системах і програмах. Це також зменшує можливість помилок під час призначення дозволів користувача. Крім того, за допомогою RBAC компанії можуть легше інтегрувати сторонніх користувачів у свої мережі, надавши їм попередньо визначені ролі.
- **Покращена відповідність.** Кожна організація повинна дотримуватися місцевих, державних і федеральних норм. Компанії зазвичай вважають за краще впроваджувати системи RBAC, щоб відповідати нормативним і законодавчим вимогам щодо конфіденційності та конфіденційності, оскільки керівники та IT-відділи можуть ефективніше керувати доступом до даних і їх використанням. Це особливо важливо для фінансових установ і організацій охорони здоров'я, які керують конфіденційними даними.

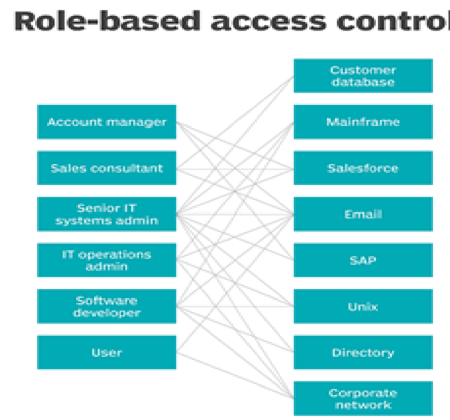


Рис. 07.12 Ілюстрація RBAC моделі

- **Підвищена видимість.** RBAC надає мережевим адміністраторам і менеджерам більше видимості та нагляду за бізнесом, а також гарантує, що авторизованим користувачам або гостям надається доступ лише до того, що їм потрібно для виконання своєї роботи.
- **Зменшені витрати.** Заборонивши користувачам доступ до певних процесів і додатків, компанії можуть зберегти або більш економно використовувати такі ресурси, як пропускна здатність мережі, пам'ять і сховище.
- **Зменшення ризику зламу та витоку даних.** Впровадження RBAC означає обмеження доступу до конфіденційної інформації, таким чином зменшуючи ймовірність порушення даних або витоку даних.

Ще одна нова функція в SCOM полягає в тому, що організації з вимкненими протоколами безпеки Windows LAN Manager New Technology можуть вибрати тип автентифікації Reporting Manager як Windows Negotiate під час встановлення. Крім того, адміністратори можуть закрити сповіщення про несправний монітор здоров'я. Вони також можуть оновити бази даних SCOM за допомогою наявної установки SQL Always-On без необхідності вносити зміни після налаштування.
У SCOM сертифікат Secure Hash Algorithm-1 зашифровано за допомогою SHA-256. Крім того, groupId підтримується в API даних Get Alert, а джерело — повне доменне ім'я — можна переглянути під час налаштування пакета керування. Серед інших корисних функцій SCOM 2022/25:
- Підтримка опції сортування за стовпцем у Підсумку замін (Overrides Summary)
- Значення налаштованих реєстрів зберігаються під час оновлення до SCOM 2019.
- Деталі реєстру сховища даних зберігаються під час оновлення неосновних серверів керування.
- Веб-консоль використовує Hypertext Markup Language 5 (HTML5) замість Silverlight.
- Підтримка .NET 48, Ubuntu 20, Oracle Linux 8, Debian 10 і Debian 11.
- Джерело сповіщення (монітор/правило), яке можна переглянути в розділі Консоль > Моніторинг > Активні сповіщення.
- Вилучено залежність від облікового запису LocalSystem.
- Усі звіти про відстеження змін доступні в одній папці (Change Tracking).

Системні вимоги для SCOM
Щоб отримати максимальну користь від SCOM, важливо спочатку перевірити системні вимоги та переконатися, що ці вимоги виконуються. Тим не менш, SCOM розроблений як гнучкий і масштабований, тому вимоги до апаратного та програмного забезпечення для певних сценаріїв можуть відрізнятися від наведених нижче рекомендацій.
- Необхідно дотримуватися рекомендованих обмежень для всіх контрольованих елементів, включаючи комп'ютери, які контролює агент, консолі одночасних операцій, комп'ютери, керовані агентом і Unix або Linux на групу керування, а також мережеві пристрої, якими керує пул ресурсів із трьома або більше серверами керування.
- Кількість додатків для моніторингу продуктивності додатків має бути менше 400.
- Кількість URL-адрес, які відстежуються на агента, має бути менше 50.
- Мінімум 8 гігабайт пам'яті та 10 ГБ дискового простору потрібні для конфігурації таких ролей, як сервер керування, сервер шлюзу, який керує до 2000 агентів, сервер веб-консолі та сервер SQL Server Reporting Services.
- Для будь-якої ролі сервера SCOM мінімальною вимогою до процесора x64 є чотириядерний центральний процесор 2,66 ГГц.
- Для налаштування сервера керування Operations Manager потрібна мінімальна версія Windows Server 2019 Standard або Datacenter.
- Для компонента сервера звітів Operations Manager потрібна версія Windows Server 2019 або Windows Server 2022 Standard або Datacenter.

Крім того, під час оновлення інсталяцій System Center 2019 – Operations Manager, інтегрованого з одним або кількома компонентами System Center, адміністратори повинні переконатися, що спочатку оновлено Orchestrator, а потім Service Manager, Data Protection Manager, Operations Manager і Virtual Machine Manager.
Серед інших мінімальних системних вимог для налаштування Microsoft SCOM:
- Internet Explorer (IE) 11 і Silverlight 5 для забезпечення зворотної сумісності клієнтських браузерів із інформаційними панелями з підтримкою Silverlight.
- Windows PowerShell версії 2.0 або 3.0 для консолі Operations Manager. Налаштування Command Shell Operations Manager виконується у консолі SCOM розділ "Administration" (Адміністрування), вкладці "Settings" (Налаштування) - "Security" (Безпека) активацією відповідної опції.
- .NET Framework 4.7.2 або 4.8 для сервера керування та сервера шлюзу.

- Microsoft Edge версії 88, IE версії 11, Google Chrome версії 88 для клієнтського веб-браузера для веб-консолі HTML5.
- Налаштований протокол передачі гіпертексту або безпечне прив'язування HTTP .
- Клієнтська операційна система Windows 10 і Windows 11 .
- Служби доменів Active Directory (AD DS) справні та підтримуються на певних мінімальних рівнях конфігурації. AD DS використовується для керування автентифікацією та авторизацією користувачів, а також для розподілу та організації об'єктів, таких як сервери, комп'ютери, служби та ролі, у доменній мережі. Мінімальні рівні конфігурації AD DS зазвичай відповідають певним версіям операційної системи Windows Server, які підтримуються SCOM. Наприклад, у хмарній реалізації, використовується Azure Active Directory (Azure AD) від Microsoft, можливе також використання гібридної служби доменів. Основні аспекти, пов'язані з використанням дерева каталогів у роботі SCOM, включають:
  - ✓ **Автентифікація і авторизація**. SCOM використовує службу доменів AD DS для автентифікації користувачів та надання їм відповідних дозволів на доступ до ресурсів системи моніторингу.
  - ✓ **Розподіл об'єктів**. Об'єкти, що моніторяться SCOM, такі як сервери, комп'ютери, програмне забезпечення та служби, організовуються відповідно до структури дерева каталогів AD DS. Це дозволяє керувати об'єктами моніторингу та надавати доступ до них з різних компонентів SCOM.
  - ✓ **Ролі та дозволи**. AD DS дозволяє налаштовувати ролі та дозволи користувачів SCOM з використанням Role-Based Access Control (RBAC). Це дозволяє диференціювати доступ користувачів до функціональності SCOM відповідно до їхніх обов'язків та повноважень.
  - ✓ **Розгортання і реплікація**. AD DS може бути використане для керування процесом розгортання та реплікації SCOM, дозволяючи ефективно розподіляти об'єкти моніторингу та забезпечувати доступність служби моніторингу у різних географічних регіонах.
- Система доменних імен встановлена та справна для належної підтримки AD DS і SCOM.

Інтеграція з іншими продуктами управління підприємством

Багато організацій використовують одну або декілька платформ для моніторингу своєї ІТ-інфраструктури. Ці платформи збирають дані про роботу серверів, мереж, програмного забезпечення та інших компонентів ІТ-системи. Одна з цих платформ використовується як центральна. Вона збирає дані з інших платформ та надає загальну картину роботи ІТ-інфраструктури. Ця платформа також використовується для:

- Запису та ескалації інцидентів: Коли виникають проблеми, платформа може записати їх та повідомити про них відповідним людям.
- Аналізу та візуалізації даних: Платформа може аналізувати дані, щоб виявити проблеми та тенденції. Вона також може візуалізувати дані за допомогою інформаційних панелей, щоб їх було легше зрозуміти.

SCOM може бути частиною цієї структури. Взаємодія між Operations Manager та іншими продуктами досягається багатьма різними методами залежно від технічних і бізнес-вимог. Нижче наведено загальні методи взаємодії з Operations Manager:

- System Center – Orchestrator із пакетами інтеграції, доступними від Microsoft, сторонніх розробників і спільноти, щомістять додаткові дії, які розширюють функціональні можливості Orchestrator для зв'язку та обміну даними з іншими сторонніми системами.
- Конектори, створені на основі Operations Manager Connector Framework (OMCF), розроблені з Operations Manager SDK , надають методи та типи, які можна використовувати для ініціалізації та керування конектором, а також для отримання чи надсилання операційних даних. Деякі приклади конекторів, які використовуються для інтеграції з Operations Manager, — це інші продукти System Center, як-от Service Manager і Virtual Machine Manager (VMM), а також сторонні продукти, такі як Nagios або IBM Netcool. Підключення до зовнішніх систем зазвичай виконується за допомогою веб-служби.
- Надсилання запитів до операційних баз даних SQL або баз даних сховищ для отримання певних наборів даних для спеціальних звітів або інформаційних панелей.

Інші користувацькі конектори розроблено та впроваджено для підтримки розширених сценаріїв, таких як збагачення сповіщень, включаючи додаткову інформацію перед тим, як сповіщення пересилається в систему керування інцидентами, виконує кореляцію попереджень або забезпечує розширені функції сповіщень за допомогою Operations Manager.

Operations Manager також інтегрується з Azure Monitor для пересилання зібраних подій, сповіщень і даних продуктивності для подальшого аналізу та забезпечує кращу видимість для організації.

Інтеграція між Operations Manager та іншими продуктами моніторингу та керування зазвичай налаштовується між одним сервером керування та іншим продуктом керування. Або в інших випадках між декількома серверами керування або вказуючи назву групи керування Operations Manager. Підтримка кількох підключених груп керування не підтримується, і кожній групі керування потрібно буде інсталювати окремий екземпляр конектора для кожної групи керування. Це включає інтеграцію між System Center Orchestrator, VMM і Service Manager.

Плануючи безперервність обслуговування, важливо оцінити та визначити ризики, вплив і варіанти відновлення для розгортання Operations Manager, щоб підтримувати цільовий рівень обслуговування.

Якщо сервер керування підтримує інтеграцію (через з'єднувач, розміщений безпосередньо на сервері керування або з іншого продукту System Center, наприклад VMM, Orchestrator або Service Manager), потрібно спланувати це за допомогою ручних або автоматичних кроків відновлення залежно від інтеграції. налаштування та послідовність кроків, необхідних для повернення до нормальної функціональності.

Управління подіями та моніторинг інфраструктури – це ключові компоненти кібербезпеки.

Ми розглянули SIEM-рішення (Elastic Security, Wazuh, Splunk ES, QRadar) зосереджені на зборі, аналізі та кореляції безпекових подій. У дану тему також додано моніторинг ІТ-інфраструктури (MS SCOM), що фокусується на контролі стану серверів, додатків та мереж, але його події також можуть бути важливими для безпеки.

Ось кілька зв'язків, які виправдовують розгляд SCOM у цьому ряді:

- ✓ **Логи та події як джерело даних для SIEM.** MS SCOM генерує події про збої серверів, продуктивність додатків, зміни в конфігурації. Ці події можуть містити індикатори компрометації або аномалії, які важливі для SIEM-рішень. Наприклад, якщо сервер Active Directory починає повільно відповідати, це може бути ознакою DDoS-атаки або зловмисного впливу.
- ✓ **Кореляція безпеки та продуктивності.** SIEM працює з логами, щоб аналізувати аномальну поведінку (логіни в незвичайний час, підозрілі запити). SCOM допомагає діагностувати, чи проблема спричинена атакою, чи звичайним збоєм в інфраструктурі.
- ✓ **MS SCOM + SIEM = комплексне бачення безпеки та стабільності.** Наприклад, QRadar або Splunk можна інтегрувати з SCOM для отримання подій про стан серверів і служб, щоб детальніше розуміти причини проблем.

Організації, які вже використовують Microsoft Active Directory, Exchange, SQL Server, SharePoint, часто мають MS SCOM як стандартне рішення моніторингу. Якщо в організації впроваджують SIEM-рішення, воно має отримувати логіки не лише від кінцевих точок, а й з серверів, додатків та баз даних. Отже, MS SCOM виконує роль "постачальника" важливих подій у SIEM-систему. Таким чином SCOM не замінює SIEM, але доповнює його

SIEM-рішення аналізують події безпеки, виявляють загрози, автоматизують реакцію.

MS SCOM стежить за стабільністю IT-інфраструктури, але його події можна використовувати для аналізу атак.
У комплексній системі кіберзахисту ці дві категорії мають працювати разом.

Порівняння платформ моніторингу безпеки

Порівняємо розглянуті популярні платформи моніторингу безпеки:

Платформа	Особливості платформи	Ліцензійна політика	Агентна структура
Wazuh	Відкритий код: Wazuh - це відкрита платформа з відкритим вихідним кодом, що дозволяє користувачам переглядати, змінювати та розповсюджувати його за власним бажанням. Інтеграція з ELK Stack: Wazuh інтегрується з ELK Stack (Elasticsearch, Logstash, Kibana), що надає потужні можливості для збору, аналізу та візуалізації даних безпеки. Правила виявлення загроз: Wazuh надає готові правила виявлення загроз, а також можливість створювати власні правила для виявлення конкретних видів загроз. Масштабованість: Wazuh може бути масштабований для використання великими організаціями та корпораціями.	Відкрита ліцензія: Wazuh використовує ліцензію GNU General Public License (GPL), що означає, що він є відкритим програмним забезпеченням і доступний для використання, модифікації та розповсюдження безкоштовно. Проте, при комерційному використанні можуть виникати вимоги до додаткових платних підтримки або послуг.	Агентно-серверна архітектура. Агенти Wazuh встановлюються на кожному хості, який потрібно моніторити і збирають дані безпеки та події з хостів, надсилаючи їх на Wazuh manager для аналізу та обробки. **«Важкість агентів»** Агенти Wazuh вважаються легкими та ефективними. Вони не використовують значні ресурси системи і можуть ефективно працювати на різних операційних системах. **Протоколи спілкування** Агенти Wazuh використовують протоколи TLS (Transport Layer Security) та syslog для комунікації з Wazuh manager. TLS забезпечує захищену та шифровану комунікацію, а syslog використовується для надсилання журналів подій.
Snort	**Система виявлення вторгнень (IDS) та система запобігання вторгнень (IPS):** Snort може працювати як IDS, аналізуючи мережевий трафік у режимі моніторингу, так і як IPS, активно блокуючи небажаний трафік. **Підтримка різних ОС:** Доступний для Linux, FreeBSD, macOS, Windows. **Підтримка правил:** Використовує власні набори правил для аналізу трафіку та виявлення атак, дозволяє створювати власні правила. **Висока продуктивність:** Підтримує масштабування для обробки високошвидкісного трафіку.	- **Відкрите ПЗ з обмеженнями**: Базова версія Snort розповсюджується під відкритою ліцензією GPLv2, безкоштовна для використання, модифікації та розповсюдження. - **Комерційна підписка**: Доступ до актуальних сигнатур та технічної підтримки через **Snort Subscriber Ruleset** (Cisco Talos). - Безкоштовні правила з затримкою у 30 днів доступні всім користувачам.	- **Агентно-серверна модель відсутня**: Snort зазвичай розгортається окремо на хості або мережевому вузлі як автономний сенсор. Можлива інтеграція з системами управління (наприклад, Snorby, BASE, або Splunk/ELK через syslog). – **«Важкість агентів»**: Залежить від обсягу трафіку і правил. На потужних системах Snort працює ефективно, проте при великому обсязі мережевого трафіку потребує відповідних ресурсів (CPU, RAM). - **Протоколи спілкування**: Snort самостійно не використовує мережеві протоколи для обміну з сервером, але може надсилати лог-файли або події через **syslog**, **Unified2**, або **JSON** до SIEM/аналізаторів подій.
Splunk Enterprise Security	Можливості аналізу даних: Splunk Enterprise Security володіє потужними можливостями аналізу даних, включаючи машинне навчання та аналітику в реальному часі. Широкий вибір інтеграцій: Splunk має велику кількість готових інтеграцій з іншими системами безпеки та інструментами моніторингу. Комерційна підтримка: Splunk пропонує комерційну підтримку для своїх продуктів та послуг, що може бути корисним для підтримки великих підприємств.	Пропрієтарна ліцензія: Splunk Enterprise Security використовує пропрієтарну ліцензію, що означає, що доступ до продукту надається за плату, і користувачам може знадобитися купувати ліцензії для використання та отримання підтримки.	Агентно-серверна архітектура. Агенти Splunk Forwarder встановлюються на кожному хості для збору та передачі даних до Splunk Indexer або Splunk Heavy Forwarder. **«Важкість агентів»** Splunk Forwarder вважається важким, особливо при великому обсязі даних або при роботі на ресурсозмінних системах. **Протоколи спілкування** Splunk Forwarder використовує протоколи Splunk Data Stream Protocol (SDSP) або HTTP Event Collector (HEC) для надсилання даних на Splunk Indexer або Splunk Heavy Forwarder.
IBM QRadar	Події в реальному часі: IBM QRadar пропонує можливості моніторингу та аналізу подій в реальному часі для виявлення загроз безпеки. Кореляція подій: QRadar використовує алгоритми кореляції подій для виявлення складних загроз та інцидентів безпеки. Широкі можливості налаштування: QRadar надає широкі можливості	Пропрієтарна ліцензія: IBM QRadar також використовує пропрієтарну ліцензію, тому доступ до продукту надається за плату, і користувачам може знадобитися купувати ліцензії для використання та отримання підтримки.	Агентно-серверна архітектура. Агенти QRadar Event Collector (QEC) встановлюються на кожному хості для збору та передачі подій до QRadar Console або QRadar Event Processor. **«Важкість агентів»** Агенти QRadar Event Collector вважаються важкими у великих розподілених мережах або при великому обсязі даних.

	налаштування для відповідності потребам конкретних організацій.		**Протоколи спілкування** QRadar Event Collector використовує протоколи Syslog або IBM QRadar Protocol (QRPT) для надсилання подій на QRadar Console або QRadar Event Processor.
Elastic Security	Вбудована аналітика безпеки: Elastic Security має вбудовану систему аналізу безпеки, яка використовує машинне навчання та аналітику в реальному часі. Масштабованість: Elastic Security може бути легко масштабований для використання в різних масштабах організацій. Еластичність: Використання Elastic Stack дозволяє легко розширювати функціональність та інтегрувати різноманітні джерела даних.	Elastic має змішану модель ліцензування, яка включає в себе як безкоштовний відкритий код, так і комерційні рішення. Elastic Security, як частина Elastic Stack, може бути доступним для використання на безкоштовній основі за умови відповідності умовам ліцензування Elastic. Проте, для використання деяких просунутих функцій або для підтримки може знадобитися купівля комерційної ліцензії.	Агентно-серверна архітектура. Beats агенти (наприклад, Filebeat або Winlogbeat) встановлюються на кожному хості для збору та передачі даних до Elasticsearch. **«Важкість агентів»** Beats агенти вважаються легкими та ефективними. Вони не потребують значних ресурсів системи і можуть працювати на різних операційних системах. **Протоколи спілкування** Beats агенти використовують протоколи HTTP або HTTPS для відправлення даних до Elasticsearch. Вони також можуть використовувати Logstash для обробки даних перед їхнім зберіганням у Elasticsearch.
MS SCOM	Централізований моніторинг: SCOM забезпечує централізоване моніторинг середовища, включаючи сервери, додатки, мережеве обладнання та хмарні сервіси (Azure). Глибока інтеграція з Microsoft продуктами: Особливо добре інтегрується з Windows Server, Active Directory, SQL Server та іншими продуктами Microsoft. Можливість моніторингу як Windows, так і Linux систем. Підтримка кастомізації: Можна створювати власні пакети управління (Management Packs) для розширення функціональності. Вбудована система оповіщень та дашбордів.	Пропрієтарна ліцензія: SCOM постачається в рамках Microsoft System Center suite, ліцензування здійснюється на основі моделей серверних ліцензій (Server ML) та клієнтських ліцензій (Client ML). Ліцензії розподіляються відповідно до кількості керованих операційних систем, підрозділів або пристроїв. Потребує окремої ліцензії для кожного моніторингового вузла.	Агентно-серверна архітектура. Агенти SCOM (Microsoft Monitoring Agent - MMA) встановлюються на кожному хості, який потребує моніторингу, та збирають дані про стан системи, додатків та подій, передаючи їх на SCOM Management Server для обробки. «Важкість агентів»: Агенти MMA вважаються помірно легкими, добре оптимізованими для роботи в середовищах Windows, проте на Linux можуть потребувати додаткових налаштувань. Протоколи спілкування: Використовують протоколи TCP/IP з шифруванням SSL/TLS для захищеної передачі даних. Можлива інтеграція з Azure Monitor через Azure Log Analytics Gateway.

Кожна з цих платформ має свої унікальні переваги та можливості, і вибір між ними залежить від конкретних потреб вашої організації, бюджету та інших факторів. Відмітимо, що всі порівняні платформи мають агентно-серверну архітектуру, у якій лише агенти Wazuh та Elastic Security відрізняються своєю «легкістю» в незалежності від розмірів мережі, обсягу даних та ресурсозмінності.

Висновки:
Ефективна побудова систем моніторингу та кібербезпеки потребує комплексного, стратегічно виваженого підходу. Жоден окремий інструмент, навіть настільки потужний, як Elastic Security, не здатен повністю задовольнити всі вимоги сучасного підприємства або організації. Справжня ефективність досягається шляхом інтеграції та грамотного поєднання різноманітних рішень: як уже розглянутих нами Elastic Stack компонентів, так і інших популярних систем моніторингу, таких як Nagios, Zabbix, Grafana, Prometheus, а також засобів SIEM, IDS/IPS та спеціалізованих аналітичних платформ.

Кожен з продуктів має свої сильні сторони, можливості та обмеження. Наприклад, одні інструменти краще підходять для збору й візуалізації метрик, інші — для обробки логів, кореляції подій, або виявлення аномалій у мережевому трафіку. Важливо враховувати специфіку інфраструктури, завдання організації, рівень критичності окремих систем та доступні ресурси для обслуговування обраних рішень.

Таким чином, комплексна система моніторингу та безпеки повинна бути побудована як єдиний цілісний механізм, у якому різні компоненти доповнюють один одного, забезпечуючи багаторівневу видимість, раннє виявлення загроз та своєчасне реагування. Лише поєднання різноманітних технологій та їх правильна інтеграція дозволяють досягти високого рівня надійності та стійкості інформаційної системи в умовах сучасних кіберзагроз.

Корисні посилання

Ресурси для вивчення Wazuh:
Офіційний сайт Wazuh: https://wazuh.com/
Документація Wazuh: https://documentation.wazuh.com/
Блог Wazuh: https://blog.wazuh.com/
GitHub Wazuh: https://github.com/wazuh/wazuh

Ресурси для вивчення Snort
Snort main page: https://www.snort.org/
Snort Documents: https://www.snort.org/documents#OfficialDocumentation

Ресурси для вивчення IBM QRadar
IBM QRadar Security Intelligence Platform. Documentation: https://www.ibm.com/docs/en/qsip/7.5?topic=started-qradar-overview
IBM Security QRadar Functions and Capabilities: https://medium.com/@4ghora/ibm-security-qradar-functions-and-capabilities-2eff8212a3e7

Ресурси для вивчення Elastic Security
Elastic main page security: https://www.elastic.co/security

Ресурси для вивчення MS SCOM
Microsoft SCOM: https://www.techtarget.com/searchwindowsserver/definition/Microsoft-System-Center-Operations-Manager-Microsoft-SCOM
Heartbeats in SCOM: https://learn.microsoft.com/en-us/system-center/scom/manage-agent-heartbeat-overview?view=sc-om-2022