ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ ІНЦИДЕНТАМИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ПІДПРИЄМСТВА НА БАЗІ РІШЕННЯ WAZUH»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Гізун І.І.
(прізвище та ініціали)

Керівник Гайдур Г.І.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КІС – Корпоративна інформаційна система

СУІБ – Система управління інформаційною безпекою

CVE – Common Vulnerabilities and Exposures

ELK – ELK Stack: Elasticsearch, Logstash, Kibana

IDS – Intrusion Detection System

IP – Internet Protocol

DoS – denial of service

DDoS – distributed denial of service

DLP – Data Leak Prevention

SCA – Security Configuration Assessment

SIEM – Security information and event management

ВСТУП

Кіберінциденти – це не просто технічні проблеми, це проблеми бізнесу. Чим швидше їх можна пом’якшити, тим менше шкоди вони можуть завдати.

Можна згадати недавні порушення, які тижнями залишалися в заголовках. Компанія була повідомлена завчасно, але не вирішила проблему? Чи їхні публічні повідомлення применшували серйозність інциденту, щоб заперечити подальше розслідування? Чи було погано організоване спілкування з постраждалими особами, що призвело до більшої плутанини? Чи звинувачували керівників у неправильному поводженні з інцидентом — чи то, що вони не сприймали його серйозно, чи вживали дій, таких як розпродаж акцій, які погіршили інцидент? Це ознаки того, що організація не мала плану.

Оскільки план реагування на інциденти — це не лише технічне питання, план IR повинен бути розроблений таким чином, щоб він відповідав пріоритетам організації та її рівню прийнятного ризику.

Керівники реагування на інциденти повинні розуміти короткострокові оперативні вимоги своїх організацій і довгострокові стратегічні цілі, щоб мінімізувати збої та обмежити втрату даних під час і після інциденту.

Інформація, отримана в процесі реагування на інциденти, також може бути використана в процесі оцінки ризиків, а також у сам процес реагування на інциденти, щоб забезпечити кращу обробку майбутніх інцидентів і посилити безпеку в цілому. Коли інвестори, акціонери, клієнти, засоби масової інформації, судді та аудитори запитують про інцидент, компанія з планом реагування на інциденти може вказати на свої записи та довести, що вона ретельно підійшла до атаки.

Об’єктом дослідження є процес забезпечення управління інцидентами інформаційної системи.

Предметом дослідження є технологія управління інцидентами інформаційної системи.

Метою роботи є розробка системи для забезпечення управління інцидентами інформаційної системи.

Для досягнення цієї мети були поставлені такі наукові завдання:

- дослідити зміст управління інцидентами на сучасному підприємстві;
- проаналізувати існуючі методи та засоби управління інцидентами;
- дослідити можливості застосування програмного комплексу Wazuh з метою забезпечення управління інцидентами інформаційної системи.

Практичне значення одержаних результатів полягає у якісному використанні комплекса Wazuh для управління інцидентами, а також у розробці рекомендацій щодо управління інцидентами в сучасній інформаційній системі.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1. Призначення, структура, функції та умови функціонування корпоративної інформаційної системи

Підприємства використовують корпоративні інформаційні системи для автоматизації виробничих процесів, обробки текстів, електронних таблиць і графічних програм. Більшість компаній використовують їх для обробки замовлень клієнтів і обробки рахунків і платежів постачальників. Банки використовують різноманітні інформаційні системи для обробки таких транзакцій, як депозити, зняття в банкоматах та платежі за кредитами. Більшість споживчих операцій також включають інформаційні системи [1].

Компанії зазвичай мають кілька типів інформаційних систем. Системи підтримки управління – це динамічні системи, які дозволяють користувачам аналізувати дані для прогнозування, визначення бізнес-тенденцій та моделювання бізнес-стратегій. Системи автоматизації офісу покращують потік комунікацій у всій організації. Кожен тип інформаційної системи обслуговує певний рівень прийняття рішень: оперативний, тактичний і стратегічний.

Корпоративні інформаційні системи призначені для автоматизації всіх функцій управління фірмою або корпорацією, що має територіальну роз’єднаність між підрозділами, філіями, відділеннями або офісами.

Корпоративна інформаційна система (далі – КІС) – це інформаційна система, що підтримує оперативний і управлінський облік на підприємстві та представляє інформацію для оперативного прийняття управлінських рішень.

КІС охоплює всі управлінські процеси. В умовах великих підприємств і вона може бути більш ефективна, оскільки забезпечує взаємодію масових і добре

організованих процесів швидкодіючими засобами сучасних інформаційних і телекомунікаційних технологій високого науково-технічного рівня.

Основними особливостями КІС є [2]:

комплексність охоплення функцій управління;

підвищена впорядкованість ділових процесів;

масовість операцій;

ефективність використання комп'ютерно-телекомунікаційного устаткування та програмного забезпечення;

можливість локальної установки та впровадження окремих частин системи;

адаптивність функціональної та інструментальної структури системи до особливостей керованого об'єкта;

можливість розвитку системи після її впровадження.

КІС використовуються для:

зберігання та аналізу інформації: складні та повні бази даних, які містять конфіденційну інформацію, наприклад, дані транзакцій, а також діяльності співробітників і клієнтів. Результати цього аналізу дають розуміння, яке може допомогти особам, які приймають рішення, вирішити поточні та майбутні проблеми;

допомоги у прийнятті рішень: КІС проводять внутрішній аналіз із зовнішніми джерелами, щоб, наприклад, порівнювати внутрішнє розуміння з інформацією про загальний стан економіки;

допомога в управлінні бізнес-процесами: КІС використовуються для розробки систем для бізнес-функцій. Бізнес-процеси можна спростити, а непотрібну діяльність можна впорядкувати за допомогою використання інформаційних систем, адаптованих до загальних бізнес-завдань, таких як виробництво, ланцюг поставок і процеси співробітників.

В умовах підприємства виділяють основні можливості КІС, такі як:

доступ до інформації. Легкий і швидкий доступ до інформації, включаючи конфіденційну інформацію, дослідження ринку, фінансові записи, щоб приймати зважені рішення;

збір даних. Корпоративні інформаційні системи збирають дані як ззовні, так і всередині організації. Ці дані об’єднуються разом і розміщуються в сховищах даних, які потім об’єднуються в мережу для аналітики;

співпраця. Однією з найкорисніших функцій корпоративних інформаційних систем є легкість, завдяки якій різні відділи та розподілені команди можуть співпрацювати над прийняттям рішень, беручи до уваги величезні обсяги даних із низки різних джерел або відділів.

1.2. Аналіз проблеми управління інцидентами в інформаційній системі підприємства

На сьогоднішній день процеси виявлення загроз та реагування залишаються складними. Проблема полягає лише в тому, що кібератаки продовжують зростати в обсязі та витонченості. Тобто, вони продовжують вдосконалюватися для збільшення своєї ефективності та ускладнення виявлення. Це передбачає потребу у пошуку шляхів виявлення вразливостей та забезпечення захисту корпоративних інформаційних систем.

Понад три чверті (76%) спеціалістів вважають, що виявлення загрози та реагування на інцидент сьогодні складніші, ніж це було лише два роки тому. Це вражаючий результат, особливо зважаючи на величезну кількість уваги, ресурсів та інвестицій, витрачених протягом останніх кількох років на стратегії та продукти захисту для забезпечення кібербезпеки – і це потенційно може підтвердити, що ситуація може тільки погіршитися в майбутньому [3].

Поняття інформаційної безпеки:

Стандарт ISO 27001 визначає інформаційну безпеку як: «збереження конфіденційності, цілісності і доступності інформації; крім того, можуть бути включені і інші властивості, такі як достовірність, неможливість відмови від авторства, достовірність».

Конфіденційність – забезпечення доступності інформації тільки для тих, хто має відповідні повноваження (авторизовані користувачі).

Цілісність – забезпечення точності і повноти інформації, а також методів її обробки.

Доступність – забезпечення доступу до інформації авторизованим користувачам, коли це необхідно.

Загрози інформаційної безпеки – це різні дії, які можуть привести до порушень стану захисту інформації. Іншими словами – це потенційно можливі події, процеси або дії, які можуть завдати шкоди інформаційним та комп'ютерним системам [4].

Загрози інформаційній системі підприємства можна розділити на два типи: природні і штучні. До природних відносяться природні явища, що не залежать від людини, наприклад урагани, повені, пожежі, тощо. Штучні загрози залежать безпосередньо від людини і можуть бути навмисними та ненавмисними. Ненавмисні загрози виникають через необережність, неуважність та незнання. Прикладом таких загроз може бути установка програм, що не входять в число необхідних для роботи і в подальшому порушують роботу системи, що і призводить до втрати інформації. Навмисні загрози, на відміну від попередніх, створюються спеціально. До них можна віднести атаки зловмисників як ззовні, так і зсередини компанії. Результат реалізації цього виду загроз – втрати коштів та інтелектуальної власності компанії. Основні загрози інформаційній системі підприємства наведено на рис 1.1.

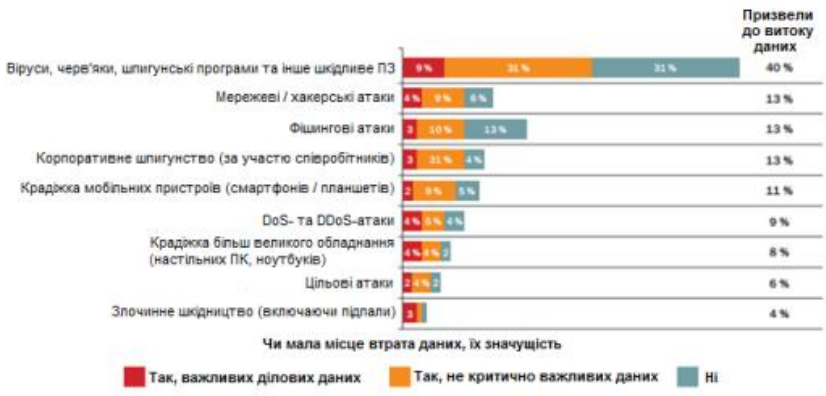

Рис. 1.1. Основні загрози інформаційній системі підприємства [5]

Все частіше зловмисники переходять від атак «в лоб» до більш складних і розподілених сценаріїв (Advanced Persistent Threat, APT). Загальні принципи, на яких будується APT, давно відомі. Наприклад, застосування соціальної інженерії, щоб спровокувати користувача перейти за посиланнями та відкрити прикріплений файл. Також зловмисники можуть використовувати вразливості для отримання доступу до системи. Проблема ж у тому, що в разі подібної атаки всі засоби захисту можуть мовчати, так як вирвані з контексту інциденти не будуть сприйматися як серйозна загроза. Але в той же самий час, аналіз сукупності інцидентів може явно вказати на атаку.

Управління інцидентами інформаційної безпеки – це процес або набір процесів, на вхід яких подаються дані, отримані в результаті збору і протоколювання даних про події, що стосуються інформаційних систем, а на виході цих процесів отримують інформацію про причини інциденту, що відбувся, про збиток, нанесений організації, і заходи, які необхідно вжити для того, щоб інцидент не повторився у майбутньому. Таким чином, УІІБ спрямовано на вдосконалення системи забезпечення безпеки підприємства. Крім того, одержувані на виході дані є, по суті, єдиною об’єктивною інформацією для визначення ймовірності загроз при аналізі ризиків.

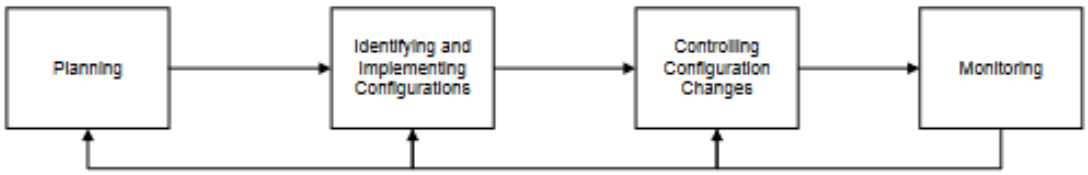

Рис. 1.2 Фази управління інцидентами інформаційної безпеки

Управління подіями і інцидентами, що забезпечується рішеннями класу SIEM (Security Information and Event Management) – один з ключових процесів забезпечення інформаційної безпеки на підприємстві.

Рішення допомагає:

зібрати і обробити дані про події та стани компонентів інформаційної безпеки підприємства;

контролювати активності пристроїв;

виявляти і розслідувати інциденти;

зберігати журнали подій в мережі з зазначенням аномалій, атак і несанкціонованих спроб доступу;

підвищити ефективність процесу управління інцидентами.

Саме ці властивості приписують сучасним SIEM-системам – здатність виявляти атаки по частинкам, аномаліям, пост-аналізу подій, тощо. SIEM-система неспроможна самостійно запобігати інцидентам, як і не має вбудованих захисних функцій. Призначення даної системи полягає в аналізі даних, що надходять від різних інших систем,, таких як Intrusion Detection System (IDS), Data Leak Prevention (DLP), міжмережевих екранів, антивірусів, активного мережевого обладнання, системи контролю доступу і аутентифікації, сканерів вразливостей, і тощо, а також реєстрації і повідомлення про інцидент при виявленні відхилення від норм за заздалегідь заданими критеріями.

В цілому система класу SIEM здатна виявляти факти мережевих атак у внутрішньому і зовнішньому периметрах, вірусні епідемії або окремі зараження шкідливим програмним забезпеченням, спроби несанкціонованого доступу до конфіденційної інформації, шахрайство, а також визначати помилки і збої в роботі інформаційних систем, уразливості, помилки конфігурацій в засобах захисту та інформаційних системах.

В якості засобу для підвищення ефективності виявлення загроз було розглянуто SIEM-систему та визначено її основні переваги та недоліки. Системи даного класу дозволяють домогтися практично повної автоматизації процесу виявлення загроз.

Універсальність SIEM-системи обумовлюється гнучкістю її логіки. Однак для її ефективного функціонування необхідні корисні джерела і ретельно написані правила кореляції.

Саме вони, в сукупності з розміром накопиченої статистики в базі, в подальшому визначать кількість хибно-позитивних спрацювань системи, які, на жаль, неминучі на момент початку її експлуатації. Як джерело вхідної інформації для SIEM-системи може бути використана практично будь-яка подія.

Збір даних від джерел в SIEM-системі здійснюється встановленими на них агентами. У разі відсутності колектора відповідного джерела, події можуть бути відправлені в форматі стандарту Syslog.

Основним завданням SIEM-системи є своєчасне виявлення, оперативне реагування та запобігання загрозам. Для цього необхідно складання правил кореляції з урахуванням актуальних для компанії ризиків, а також постійна актуалізація самих правил фахівцями.

В цілому загрози кібербезпеки можуть завдавати шкоди та збитків корпоративним інформаційним системам. Основні джерела загроз – хакери, намагаються отримати доступ до систем організацій з метою крадіжки даних, коштів або виведення з ладу обладнання.

SIEM-системи дозволяють домогтися практично повної автоматизації процесу виявлення загроз, але при не правильному налаштуванні призводять до нераціональної витрати коштів.

1.3. Мета та завдання технології управління інцидентами в інформаційній системі підприємства

Протягом двох років складність управління інцидентами лише збільшувалась, зловмисники стали більш витонченими та небезпечними і своєчасне виявлення стало справжньою проблемою. Шкідливе ПЗ, додатки-вимагачі, інциденти, пов’язані з компрометацією робочої пошти та ін. Рішення з кібербезпеки в інформаційних системах підприємства повинні забезпечувати виявлення поведінкових аномалій у режимі реального часу, забезпечувати швидке

реагування на інциденти та інтелектуальну візуалізацію мережі та всіх її взаємопов’язаних вузлів

Основним завданням технології управління інцидентами є збір, агрегація, індексування та аналізу даних безпеки, допомагаючи організаціям виявляти вторгнення, загрози та поведінкові аномалії.

SIEM-система повинна сканувати відстежуванні системи, шукаючи шкідливе програмне забезпечення, руткіти та підозрілі аномалії. Також невід’ємною частиною збору даних є аналіз журналів операційної системи та програм та їх аналіз і зберігання відповідно до спрацьованих правил на ту чи іншу подію.

В SIEM-системі повинна бути присутня можливість зберігання дані інвентаризації програмного забезпечення та порівнює з базами даних CVE (Common Vulnerabilities and Exposure), щоб ідентифікувати добре відоме вразливе програмне забезпечення.

Система управління інформаційної безпеки (СУІБ) – та частина загальної системи управління, яка заснована на підході бізнес-ризиків при створенні, впровадженні, функціонуванні, моніторингу, аналізі, підтримці і поліпшенні інформаційної безпеки.

Система управління інформаційною безпекою повинна забезпечувати безпечність та надійність функціонування інформаційних систем підприємства. Впровадження та функціонування СУІБ стосується всіх підрозділів і насамперед керівників. Тому посадові особи повинні брати безпосередню участь у вирішенні питань, які належать до сфери їх відповідальності, під час впровадження та функціонування СУІБ.

Для впровадження СУІБ необхідно сформулювати план скорочення ризику, який визначає відповідні дії, що управляють, ресурси, зобов'язання і пріоритети для управління ризиками інформаційної безпеки та виконати план зменшення ризиків для того, щоб досягти встановлених цілей, які включають аналіз фінансування і розподілу ролей і обов'язків. Також необхідно впровадити методику і інші засоби управління, здатні своєчасно виявити події безпеки і реакцію у відповідь на інциденти безпеки

Цілі СУІБ та заходи безпеки, які вже запроваджені і ті, що будуть додатково впроваджені в разі необхідності, а також відповідна документація, що описує функціонування СУІБ, повинні бути зрозумілими для всіх, кого це стосується. Тому обов'язковою умовою успішного функціонування СУІБ є також проведення відповідних навчань працівників з питань інформаційної безпеки (ІБ).

Основними цілями управління інцидентами є:

відновлення нормальної роботи служб в найкоротші терміни;

зведення до мінімуму впливу інцидентів на роботу організації;

забезпечення злагодженої обробки всіх інцидентів і запитів обслуговування;

зосередження ресурсів підтримки на найбільш важливіших напрямах;

надання відомостей, що дозволяють оптимізувати процеси підтримки, зменшити кількість інцидентів і запланувати управління.

Також важливу роль для розробки технології управління інцидентами в інформаційній системі підприємства відіграють міжнародних стандартів та чинне законодавство України.

Такими стандартами є:

Вимоги 10 і 11.5 PCI DSS

ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements.

HIPAA Section 164.308(a)(1)(ii)(D), Section 164.308(a)(5)(ii)(C), Section 164.312(b), Section 164.316(b)(2)(i) [6].

НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

Стандарт BSI-100-2У.

Для реалізації системи управління інцидентами інформаційної безпеки необхідно:

виділити ресурси для розробки та впровадження системи управління інцидентами;

визначити область функціонування системи управління інцидентами;

розробити комплекс процесів системи управління;

навчити персонал;

впровадити процеси управління інцидентами та інтегрувати їх зі вже функціонуючими процесами управління інформаційної безпекою, такими як, інвентаризація активів, аналіз ризиків та оцінка ефективності;

розробити архітектуру і комплекс технічних засобів з автоматизації процесів управління інцидентами і моніторингу подій інформаційної безпеки;

впровадити комплекс програмно-технічних засобів автоматизації управління інцидентами.

Також при експлуатації різного роду систем інформаційної безпеки управління інцидентами є одним з найважливіших постачальників даних для аналізу функціонування подібних систем, оцінки ефективності використовуваних заходів зниження ризиків і планування поліпшень в роботі системи.

Для подолання реальної або потенційної шкоди працездатності системи, яку завдають інциденти, необхідно організувати процес управління ними. Він включає в себе рис. 1.2:

визначення переліку подій, які є інцидентами;

визначення факту вчинення інциденту інформаційної безпеки;

оповіщення відповідальної особи про виникнення інциденту;

порядок усунення наслідків і причин інциденту;

порядок розслідування інциденту;

винесення дисциплінарних стягнень;

реалізація необхідних коригувальних і превентивних заходів

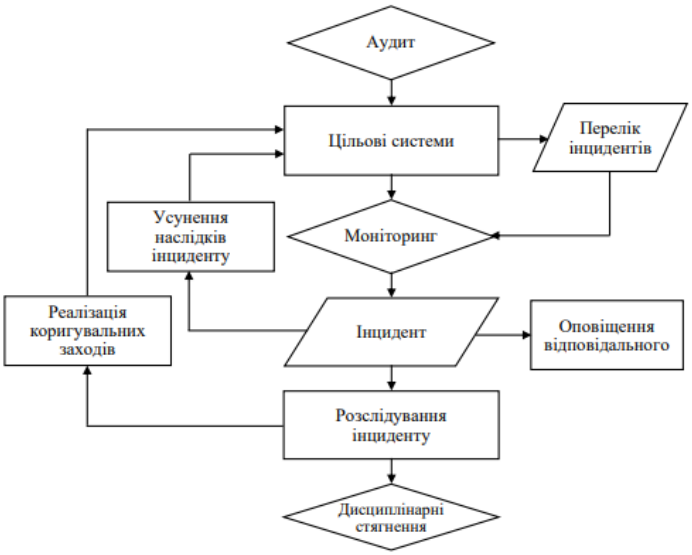

Рис.1.3 Процес управління інцидентами [7]

1.4. Аналіз існуючих технологій управління інцидентами в інформаційній системі підприємства

Для управління інцидентами ІБ підприємству необхідно реалізувати можливість своєчасного виявлення інцидентів та адекватного реагування на них відповідними контрзаходами. У цьому відношенні з метою моніторингу захищеності інфраструктури, управління інцидентами ІБ, контролю відповідності вимогам в структурі сучасних підприємств представлені центри управління ІБ, що здійснюють пошук та усунення вразливостей, аналіз зовнішніх та внутрішніх джерел щодо актуальних кіберзагроз та розробку заходів щодо захисту, збору, аналізу та аудиту журналів подій в системі, а також виявлення, аналіз, реагування на інциденти та розробку заходів щодо покращення діючих процесів та заходів ІБ на основі отриманого досвіду.

Обробка інцидентів передбачає визначення їх пріоритетів, що дозволяє оцінювати ймовірність реалізації ризиків і тяжкості наслідків від них, і відповідно своєчасно реагувати і розслідувати інциденти з найвищим ризиками. Пріоритет визначається впливом (комерційним збитком або потенційним пошкодженням, зокрема, бази користувачів, безпеки, репутації, бренду), терміновістю (швидкодією

щодо усунення ознак інциденту, зокрема витік даних або активне поширення шкідливого програмного забезпечення). Зазвичай інциденти обробляються відповідно до присвоєного їм пріоритету.

Для організації управління інцидентами в інформаційній системі підприємства СУІБ необхідно виконати наступне:

Впровадити правила моніторингу і перевірки і інші засоби управління для того, щоб:

своєчасно виявляти помилки в результатах процесу;

своєчасно розпізнавати невдалі порушення безпеки і інциденти, що вдалися;

керувати менеджментом, щоб визначити, чи належно виконується робота по безпеці, доручена людям або здійснювана інформаційними технологіями;

сприяти виявленню подій безпеки і таким чином, використовуючи певні показники, попереджати інциденти безпеки, і визначити ефективність дій, зроблених для запобігання порушенню безпеки.

Проводити регулярні перевірки ефективності СУІБ (включаючи обговорення політики СУІБ і її завдань, перевірку засобів управління безпекою), зважаючи на результати аудитів, інцидентів, результати вимірів ефективності, пропозиції і рекомендації усіх зацікавлених сторін.

Проводити оцінку ефективності засобів управління, щоб виявити, чи задоволені вимоги безпеки.

Проводити перевірку оцінки ризиків по запланованих періодах, приймаючи в уваги зміни в:

підприємстві;

технології;

бізнес-цілях і процесах;

ідентифікованих погрозах;

ефективності впроваджених засобів управління;

зовнішніх подіях, наприклад, зміни в юридичному середовищі.

Проводити внутрішні аудити СУІБ в заплановані періоди

Записи повинні створюватися і зберігатися для того, щоб забезпечити підтвердження відповідності вимогам і ефективне функціонування СУІБ. Записи необхідно захищати і перевіряти. СУІБ повинна враховувати будь-які юридичні і регулятивні вимоги і договірні зобов'язання. Записи мають бути зрозумілі, легко ідентифіковані і відновлені. Засоби управління, необхідні для ідентифікації, зберігання, захисту, відновлення, тривалості зберігання і знищення записів, мають бути документально затверджені і введені в дію.

Відповідно до стандарту BSI-100-2У [8] записі необхідно включати інформацію про події для безпеки та інциденти, що відносяться до СУІБ.

Прикладами записів є гостьова книга, протоколи аудиту і заповнені форми авторизації доступу.

В якості засобу для підвищення ефективності виявлення загроз було розглянуто SIEM-системи та визначено її основні переваги та недоліки. Системи даного класу дозволяють домогтися практично повної автоматизації процесу виявлення загроз.

Враховуючи переваги та можливості, які надають SIEM-системи, була встановлена мета дослідити дані засоби та класифікувати їх методом експертних оцінок

Базове порівняння проводилося за наступними основними показниками (чинниками):

рекомендована оперативна пам’ять;

рекомендований CPU;

тип ліцензії;

типи джерел даних;

максимальний EPS;

максимальний FPM;

робота в хмарі;

архітектура;

тип інтерфейсу управління;

система Asset Management;

вбудований сканер вразливостей;

колектор PCAP;

автоматична інтеграція з фідами

можливість створення своїх графічних панелей;

вартість.

Табл.1.1 Порівняння SIEM-систем

Характеристика	IBM Qradar	Splunk Enterprise	Micro Focus ArcSight	Wazuh
Рекомендована оперативна пам’ять	24 GB	12 GB	16 GB	4 GB
Рекомендований CPU	2 x Xeon Gold 6132 14C 2.6 GHz 19 MB Cache 3.70 GHz)	Intel x86 64-bit chip architecture. 12 CPU cores at 2Ghz or greater speed per core.	8 ядер Xeon 3.0GHz	2 ядра Xeon 3.0GHz
Тип ліцензії	Коммерційна	Коммерційна	Комерційна	Open Source
Типи джерел даних	Веб-сервери, система антивірусного захисту, сервер віртуальних машин, зовнішній та внутрішній міжмережеві екрани, сервери баз даних, стандартні лог-файли аудиту в ОС Windows Server	Абсолютно всі джерела даних які представляють системні логи, алерти та тикети або сповіщення. Бази даних, міжмережеві екрани, лог файли ОС, логи мережевих пристроїв	Антивірусні програми, захист даних,брандмауери, журнал безпеки, фільтрація пошти, мейнфрейм сервера, моніторинг мережі, ОС, аналіз навантаження, політика безпеки, VPN на сервері, веб-фільтрація, безпроводова безпека, веб-кеш	Будь-які джерела даних, що можуть бути представлені у формі логів – журнали подій з кінцевих точок, журнали безпеки, логи захисних систем, логи TAP`ів тощо, а також Netflow.
Максимальний EPS	25000 подій в секунду	22000 eps	ArcSight Connector — 2000-4000 EPS, Event Broker — більш ніж 500000	Не обмежується. Залежить від

			EPS, ArcSight ESM — 50000 EPS	можливостей сервера.
Максимальний FPM	300000 в хвилину	150000 в хвилину	100000 в хвилину	Не обмежується. Залежить від можливостей сервера.
Робота в хмарі	Присутня	Присутня	Присутня	Присутня
Архітектура	Red Hat Enterprise Linux, PostgreSQL, Ariel DB, VMware, AWS	Linux, all 3.x and 4.x kernel versions, Linux, all 2.6 kernel versions, macOS 10.15, PowerLinux, Little Endian kernel version 2.6 and higher, FreeBSD 11, Windows Server 2016 and Server 2019, Windows 10	Red Hat Enterprise Linux\CentOS\SuSE Enterprise Linux, CORR-Engine, VmWare	CentOS/RHEL, Oracle Linux, Ubuntu Linux, Debian Linux, Windows Server 2012-2019
Тип інтерфейсу управління	Веб-консоль	Веб-консоль	Веб-консоль (ArcSight Command Center) і товстий клієнт (ArcSight Console)	Веб-консоль, можливий доступ через CLI.
Система Asset Management	Залежить від сканерів безпеки, CSV-файлів, API	Asset and Identity Framework by Splunk	ArcSight Asset Import Connector (можливіть автоматичного створення активів), кореляційними правилами, вручну. Можлива інтеграція з будь-якими системами класу CMDB, що відповідають за облік активів	Відсутня система автоматичного Asset Management, нові активи додаються в ручному режимі.

Вбудований сканер вразливостей	Відсутній. Присутня можливість інтеграції зі сканерами	Відсутній. Присутня можливість інтеграції зі сканерами	Відсутній. Присутня можливість інтеграції з усіма сканерами великих вендорів, можливість інтеграції по API і звіти різних форматів	Відсутній. Присутня можливість обробки логів із зовнішніх систем виявлення вразливостей.
Колектор PCAP	Присутній	Присутній	Присутній	Присутній, обробляє формат JSON.
Автоматична інтеграція з фідами	Присутня	Присутня	Присутня	Частково, інтеграція відбувається в режимі обробки логів.
Можливість створення своїх графічних панелей	Присутня. Також присутня можливість візуалізації за допомогою додаткових додатків	Присутня	Так, додатково присутня інтеграція з пакетами панелей візуалізації в ArcSight Content Brain	Присутня.
Вартість	63 000 $	21 600 $	24 000$	Безкоштовна. Можливе замовлення платної підтримки та доступу до розширеного функціоналу від 22$ на місяць.

Висновки до розділу 1

Проаналізовано функції корпоративної системи, її переваги та недоліки.

Досліджено статистику щодо використання технології управління інцидентами в інформаційній системі підприємства.

Визначено основні типи та види вразливостей корпоративної інформаційної системи.

Підкреслено особливості захисту системи, такі як знання вразливостей системи, вчасне реагування на інциденти, знання нормативно-правової бази правильне налаштування SIEM-систем. Досліджено різні рівні категорій безпеки системи.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ІНЦИДЕНТАМИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ПІДПРИЄМСТВА НА БАЗІ WAZUH SIEM

2.1. Призначення, можливості та функції рішення Wazuh SIEM

Платформа Wazuh [9] надає функції для захисту хмарних, контейнерних та серверних робочих навантажень. До них відносяться аналіз даних журналу, виявлення вразливостей і шкідливих програм, моніторинг цілісності файлів, оцінка конфігурації, виявлення вразливостей і підтримка відповідності нормативним вимогам. Рішення Wazuh засноване на наступних трьох компонентах:

агент Wazuh: встановлюється на кінцевих точках, таких як ноутбуки, стаціонарні комп'ютери, сервери, хмарні екземпляри або віртуальні машини. Він забезпечує можливості запобігання, виявлення і реагування. Він підтримує платформи Windows, Linux, macOS, HP-UX, Solaris і AIX.

сервер Wazuh: аналізує дані, отримані від агентів, обробляє їх за допомогою декодерів і правил, а також використовує аналіз загроз для пошуку добре відомих індикаторів компрометації. Один сервер може аналізувати дані від сотень або тисяч агентів і масштабуватися по горизонталі при налаштуванні у вигляді кластера. Сервер також використовується для управління агентами, їх налаштування та віддаленого оновлення при необхідності.

Elastic Stack: індексує і зберігає сповіщення, створені сервером Wazuh. Крім того, інтеграція між Wazuh і Kibana забезпечує потужний користувальницький інтерфейс для візуалізації та аналізу даних. Цей інтерфейс також можна використовувати для управління конфігурацією Wazuh і відстеження її статусу.

Можливості Wazuh:

аналіз даних журналу – процес осмислення в реальному часі записів, створених серверами чи пристроями. Цей компонент може отримувати журнали

через текстові файли або журнали подій Windows. Він також може безпосередньо отримувати журнали через віддалений системний журнал, що корисно для брандмауерів та інших подібних пристроїв. Метою цього процесу є виявлення помилок програми або системи, помилкових конфігурацій, спроб вторгнення, порушень політики або проблем із безпекою. Вимоги до пам’яті та центрального процесора агента Wazuh незначні, оскільки його основним обов’язком є пересилання подій менеджеру. Однак у менеджера Wazuh споживання процессора та пам’яті може швидко зростати залежно від подій у секунду (EPS), які менеджер повинен аналізувати ;

моніторинг цілісності файлів – відстежує вибрані файли та сповіщає про зміну цих файлів. Компонент, відповідальний за це завдання, називається syscheck . Цей компонент зберігає криптографічну контрольну суму та інші атрибути відомого хорошого файлу або ключа реєстру Windows і регулярно порівнює його з поточним файлом, що використовується системою, спостерігаючи за змінами;

Auditing who-data: Починаючи з версії 3.4.0, до Wazuh входить функція, яка отримує хто-інформацію з моніторингових файлів. Ця інформація містить користувача, який вніс зміни у відстежувані файли, а також назву програми або процес, що використовувався для їх виконання;

Anomaly and malware detection: Виявлення аномалії стосується дії пошуку шаблонів у системі, які не відповідають очікуваній поведінці. Як тільки шкідливе програмне забезпечення (наприклад, руткіт) встановлено в системі, воно змінює систему, щоб приховатись від користувача. Хоча шкідливе програмне забезпечення використовує різні методи для досягнення цього, Wazuh використовує широкий спектр підходів до пошуку аномальних моделей, які вказують на можливих зловмисників. Основним компонентом, що відповідає за це завдання, є rootcheck , однак Syscheck також відіграє важливу роль;

Monitoring security policies (моніторинг політики безпеки): це процес перевірки відповідності всіх систем набору заздалегідь визначених правил щодо налаштувань конфігурації та затвердженого використання програми. Wazuh

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

Monitoring system calls (моніторинг системних викликів): Система аудиту Linux забезпечує спосіб відстеження інформації, що стосується безпеки на комп'ютері. Спираючись на заздалегідь налаштовані правила, Аудит розвідує детальний журнал у реальному часі про події, що відбуваються у вашій системі. Ця інформація є важливою для критично важливих середовищ для встановлення порушника політики безпеки та дій, які вони вчинили;

Command monitoring (контроль команди): коли виникає потреба стежити за речами, яких немає в журналах, Wazuh надає можливість відстежувати результати певних команд та обробляти результати, ніби це вміст файлу журналу;

Active response (активна відповідь): виконує різні контрзаходи для вирішення активних загроз, наприклад, блокування доступу до агента з джерела загроз при дотриманні певних критеріїв. Активні відповіді виконують сценарій у відповідь на спрацьовування певних попереджень на основі рівня попередження або групи правил. Будь-яка кількість сценаріїв може бути ініційована у відповідь на тригер, однак ці відповіді слід ретельно розглянути. Погана реалізація правил та відповідей може збільшити вразливість системи;

Agentless monitoring (безагентний моніторинг): дозволяє відстежувати пристрої чи системи без агента через SSH, таких як маршрутизатори, брандмауери, комутатори та системи linux / bsd. Це дозволяє користувачам з обмеженнями на встановлення програмного забезпечення відповідати вимогам безпеки та відповідності. Попередження будуть спрацьовувати, коли контрольна сума на виході змінюється, і відображатиме або контрольну суму, або точну різницю зміни на виході;

Anti-flooding mechanism (механізм проти затоплення) : Цей механізм призначений для запобігання негативному впливу на мережу або менеджера великих сплесків подій на агента. Він використовує чергу за методом «дірявого відра», яка збирає всі згенеровані події та надсилає їх менеджеру зі швидкістю

нижче зазначених подій на секунду. Це допомагає уникнути втрати подій або несподіваної поведінки компонентів Wazuh;

Agent labels (етикетки агентів): Ця функція дозволяє користувачеві налаштувати інформацію про сповіщення від агентів, включаючи конкретну інформацію, пов’язану з агентом, що генерує попередження. Це може виявитися корисним при зверненні або перегляді попереджень. Крім того, у великих середовищах цю можливість можна використовувати для ідентифікації груп агентів за будь-якою загальною характеристикою, наприклад, за їх часовим поясом;

System inventory (інвентаризація системи): Агенти Wazuh можуть збирати цікаву системну інформацію та зберігати її в базі даних SQLite для кожного агента на стороні менеджера. За це завдання відповідає модуль Syscollector;

Vulnerability detection (виявлення вразливості) : Wazuh здатний виявляти вразливості в додатках, встановлених в агентах, використовуючи модуль виявлення вразливостей. Цей аудит програмного забезпечення проводиться шляхом інтеграції каналів вразливості, індексованих Canonical, Debian, Red Hat та Національною базою даних про вразливості;

VirusTotal integration: Wazuh може сканувати відстежувані файли на наявність шкідливого вмісту у відстежуваних файлах. Це рішення можливе завдяки інтеграції з VirusTotal, яка є потужною платформою, яка об’єднує кілька антивірусних продуктів разом із механізмом онлайн-сканування. Поєднання цього інструменту з нашим механізмом FIM забезпечує прості засоби сканування файлів, які контролюються, щоб перевірити їх на наявність шкідливого вмісту;

Osquery: Модуль Wazuh, що дозволяє керувати інструментом Osquery від агентів Wazuh, маючи можливість встановлювати конфігурацію Osquery та збирати інформацію, що генерується Osquery, щоб відправити її менеджеру, генеруючи відповідні попередження, якщо це необхідно. Osquery можна використовувати для відображення операційної системи як високоефективної реляційної бази даних. Це дозволяє писати запити на основі SQL для вивчення даних операційної системи;

Agent key polling (опитування ключа агента) : Модуль Wazuh, що дозволяє отримувати ключі, що зберігаються у зовнішній базі даних. Модуль дозволяє

отримувати інформацію про агента із зовнішньої бази даних, наприклад MySQL або будь-якого механізму баз даних;

Fluentd forwarder(вільний транспортер): Цей модуль дозволяє Wazuh пересилати повідомлення на сервер Fluentd. Fluentd – це реєстратор збору даних з відкритим кодом, який постачається разом із чудовими плагінами для створення власного рівня реєстрації. Цей модуль дозволяє переадресовувати отримані повідомлення із виділеного UDP-сокета на сервер Fluentd. Сервер Fluentd може знаходитись на тій самій локальній машині або віддаленій машині;

Для попередження несанкціонованого доступу та отримання прав доступу до конфіденційної інформації непривілейованими користувачами, здійснюється моніторинг за допомогою спеціального програмного забезпечення, в функціональні можливості якого входить:

збір лог файлів з віддалених підконтрольних машин;

структування та аналіз отриманих данних;

надсилання алертів при виявленні спроби отримання root прав;

зараження руткітами та інших важливих подій, сповіщення про які можна налаштувати власноруч;

забезпечення безперебійного збору логів, без втрат у разі виходу з ладу одного з менеджерів, що власне здійснюють контроль за подіями безпеки.

На ці всі функції а можливості діє система логування. Події управління інцидентами в інформаційній системі підприємства журналюються та індексуються відповідним рівнем за рахунок порівняння ідентифікаторів у форматі JSON. Відповідній події або інциденту надається рівень, за замовчуванням в системі налаштовано 15 рівнів сповіщень.

Табл.2.1 Рівні сповіщень в SIEM-системі Wazuh

Рівень	Назва	Опис
0	Ігнорується	Жодних заходів не вжито. Використовується, щоб уникнути помилкових спрацьовувань. Ці правила

		перевіряються перед усіма іншими. Вони включають події, які не стосуються безпеки.
2	Системне сповіщення про низький пріоритет	Системні сповіщення або повідомлення про статус. Вони не мають жодного значення для безпеки.
3	Успішні/санкціоновані події	Вони включають успішні спроби входу, події дозволу брандмауера тощо.
4	Помилка низького пріоритету системи	Помилки, пов’язані з поганою конфігурацією або невикористаними пристроями/програмами. Вони не мають жодного значення для безпеки і зазвичай викликані встановленням за замовчуванням або тестуванням програмного забезпечення.
5	Помилка, створена користувачем	Вони включають пропущені паролі, заборонені дії тощо. Самі по собі вони не мають жодного значення для безпеки.
6	Атака низької релевантності	Вони вказують на хробак або вірус, які не впливають на систему (наприклад, червоний код для серверів apache тощо). Вони також включають часті події IDS і часті помилки
7	Відповідність «погане слово».	Вони містять такі слова, як «погано», «помилка» тощо. Ці події в більшості випадків є несекретними і можуть мати певне значення для безпеки.
8	Вперше бачив	Включіть події, які ви бачили вперше. Під час першого запуску події IDS або першого входу користувача.

		Він також включає дії, що стосуються безпеки (наприклад, запуск сніфера або щось подібне).
9	Помилка з недійсного джерела	Включати спроби входу в систему як невідомий користувач або з недійсного джерела. Може мати значення для безпеки (особливо якщо повторюється). Вони також містять помилки щодо облікового запису «admin» (root).
10	Кілька помилок, створених користувачами	Вони включають кілька неправильних паролів, кілька невдалих входу тощо. Вони можуть свідчити про атаку або просто про те, що користувач просто забув свої облікові дані.
11	Попередження про перевірку цілісності	Вони містять повідомлення про модифікацію бінарних файлів або наявність руткітів (від Rootcheck). Вони можуть свідчити про успішну атаку. Також включені події IDS, які будуть ігноровані (велика кількість повторів).
12	Подія високої важливості	Вони включають повідомлення про помилки або попередження від системи, ядра тощо. Вони можуть свідчити про атаку на конкретну програму.
13	Незвичайна помилка (велика важливість)	У більшості випадків це відповідає загальному шаблону атаки.
14	Подія високої важливості безпеки	Більшість випадків виконується з кореляцією, і це вказує на атаку.

15	Сильний напад	Немає шансів помилкових спрацьовувань. Необхідна негайна увага.

2.2. Компоненти та архітектура рішення Wazuh

Програмний комплекс Wazuh, що складається таких основних компонентів:

Wazuh Server базується на наборі програм, де кожна програма або компонент призначені для виконання певного завдання. Ці компоненти працюють разом, щоб:

аналізувати дані, отримані з різних журналів,

активувати попередження, коли подія журналу відповідає правилу,

зареєструвати нових клієнтів / агентів та надсилати дані на сервер Elastic Stack.

Elastic Stack використовується для індексації, перегляду та візуалізації даних попереджень Wazuh. Крім того, додаток Wazuh для Kibana можна використовувати для візуалізації налаштувань конфігурації, правил, декодерів та інформації про статус агента. Інформаційні панелі, що використовуються для візуалізації, включають, але не обмежується політикою, дотриманням вимог та моніторингом цілісності файлів.

Filebeat – це легковажний доставник лог-повідомлень. Принцип його роботи полягає в моніторингу та збиранні лог-повідомлень з лог-файлів і пересиланні їх в Elasticsearch або Logstash для індексування.

Wazuh agent працює на відстежуваних системах і відповідає за збір даних журналів та подій, виконуючи сканування моніторингу політики, виявляючи шкідливе програмне забезпечення та руткіти та запускаючи сповіщення про зміну відстежуваних файлів. Він взаємодіє із сервером Wazuh через зашифрований та автентифікований канал. Присутня можливість встановлення Wazuh agent на такі ОС:

Linux;

Windows;

macOS;

AIX;

HP-UX;

Solaris;

Присутні два різні варіанти розгортання Wazuh:

Все-в-одному: сервер Wazuh і Elastic Stack встановлюються на одному хості безпосередньо у системі. Крім того, присутня можливість завантажити готовий до використання OVA або запустити екземпляр EC2 за допомогою AMI.

Розподілений: кожен компонент встановлюється на окремому хості як одновузловий або багатовузловий кластер. Цей тип розгортання забезпечує високу доступність і масштабованість продукту, а також зручний для великих робочих середовищ.

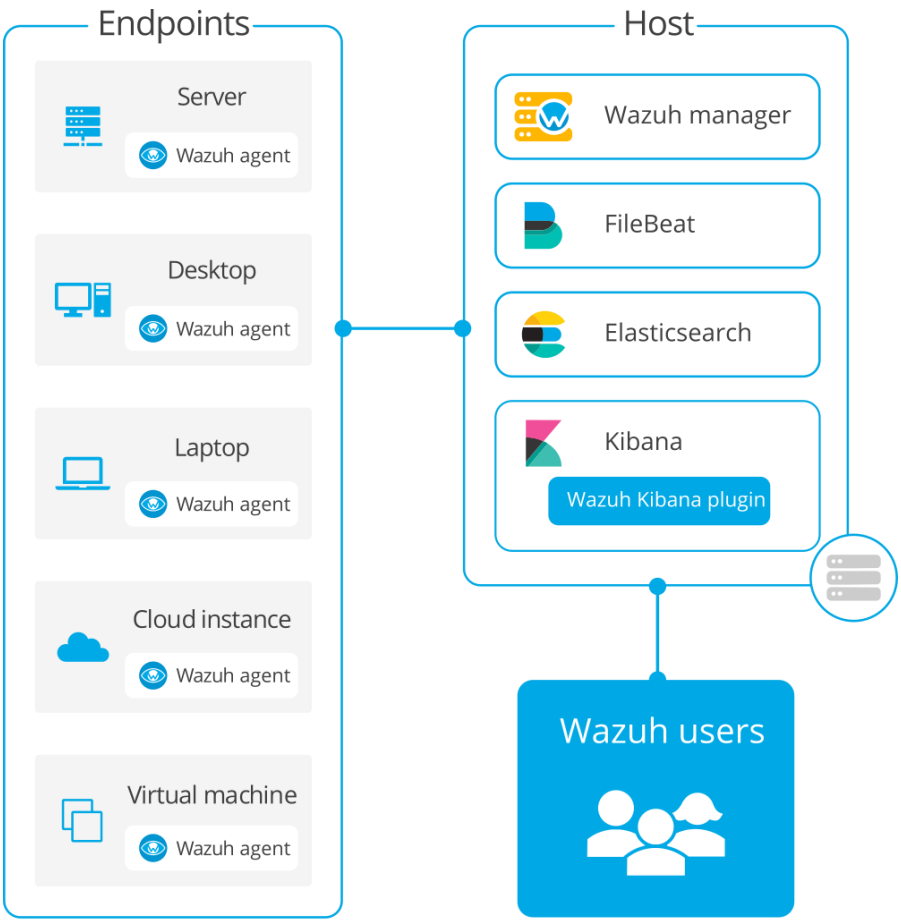

Рис.2.1 Архітектура програмного комплексу Wazuh типу розгортання «все в одному» [10]

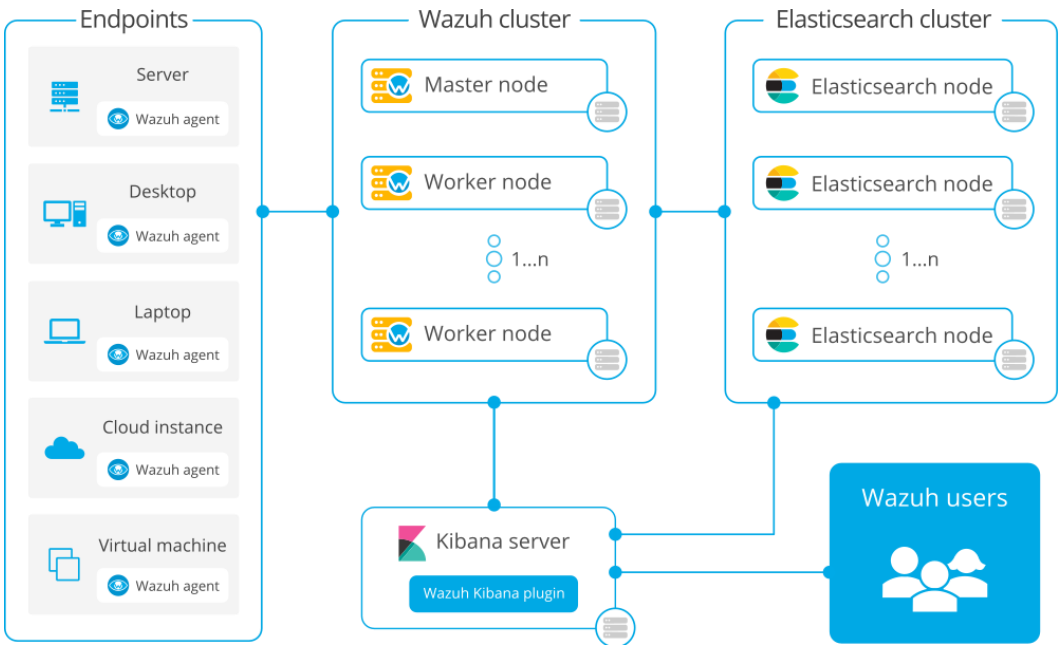

Рис.2.2 Архітектура програмного комплексу Wazuh «розроділеного» типу розгортання

2.3 Призначення та архітектура рішення Elastic Stack

Elastic Stack – це скорочення від трьох проектів з відкритим вихідним кодом: Elasticsearch, Logstash і Kibana. Elasticsearch – це ядро всієї системи, яке поєднує функції бази даних, пошукової та аналітичної системи. Logstash – це конвеєр обробки даних на стороні сервера, який отримує дані з декількох джерел одночасно, парсить лог, а потім відправляє до бази даних Elasticsearch. Kibana надає функцію візуалізації даних за допомогою діаграм та графіків у Elasticsearch. Також через Kibana можна адмініструвати базу даних. [11]

Табл. 2.2 Призначення компонентів Elastic Stack

Компонент	Мета
Elasticsearch	Сховище даних і пошукова система
Kibana	Пошуковий інтерфейс і візуалізації

Security	Аутентифікація та контроль доступу для кластера
Alerting	Отримання сповіщень, коли дані відповідають певним умовам
SQL	Присутня можливість використання SQL або мови обробки каналів для запиту даних
Index State Management	Автоматизація індексних операцій
Performance Analyzer	Відстеження та оптимізація кластера
Anomaly Detection	Визначення нетипових даних та отримання автоматичних сповіщень
Asynchronous Search	Виконання пошукових запитів у фоновому режимі

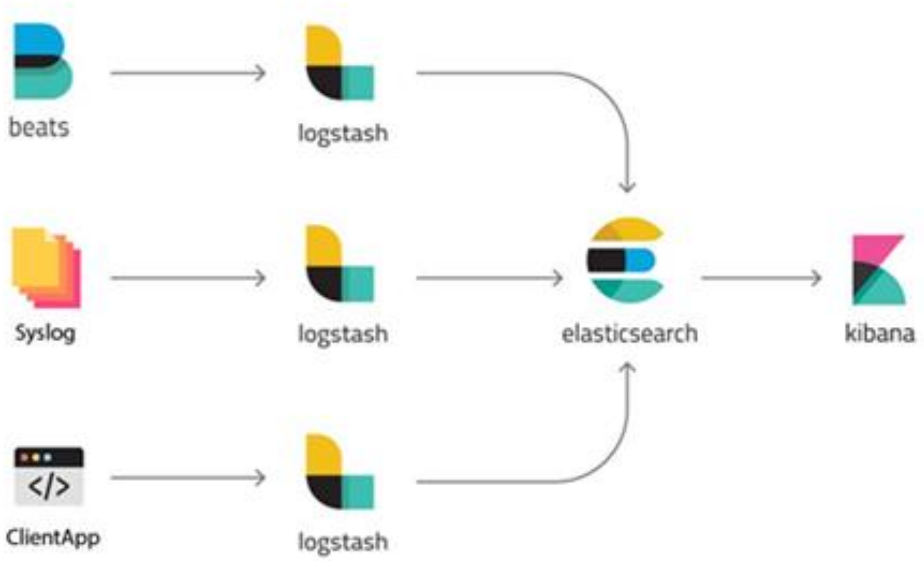

Рис. 2.3 архітектура рішення Elastic Stack

Logstash – це утиліта для обробки лог подій з різних джерел, за допомогою якої можна виділити поля та їх значення у повідомленні, також можна налаштувати фільтрацію та редагування даних. Після всіх маніпуляцій Logstash перенаправляє

події до кінцевого сховища даних. Утиліта налаштовується лише через файли конфігурації.

Типова конфігурація Logstash являє собою файл(и), що складається з декількох вхідних потоків інформації (input), кілька фільтрів для цієї інформації (filter) і кілька вихідних потоків (output). Виглядає це як один або кілька конфігураційних файлів, які в найпростішому варіанті (який не робить взагалі нічого) виглядає так:

```
input {
  tcp {
    type =>
    port => "11111"
  }
}
filter {
  mutate {
    type => ==
    add_field => [ =>                    ]
  }
}
output {
  stdout {
    type => >
    message => "%{habra_field}: %{@message}"
  }
}
```

Рис. 2.4 файл налаштування Logstash

В INPUT необхідно налаштувати на який порт будуть приходити логи і за яким протоколом, або з якої папки читати нові файли, що постійно дозаписуються. У FILTER необхідно налаштувати парсер логів: розбір полів, редагування значень, додавання нових параметрів чи видалення. FILTER це поле для керування повідомленням, яке приходить на Logstash з масою варіантів редагування. У OUTPUT необхідно налаштувати відправлення вже розібраного логу, у разі якщо це Elasticsearch відправляється JSON запит, у якому відправляються поля зі значеннями, або ж у рамках дебага можна виводити в stdout чи записувати файл.

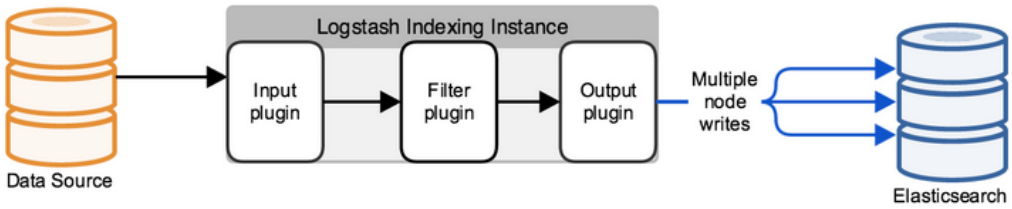

Рис. 2.5 схема роботи Logstash [12]

Elasticsearch – це рішення для повнотекстового пошуку, але з додатковими зручностями, наприклад, легкого масштабування, реплікації та іншого, що зробило продукт дуже зручним та гарним рішенням для високонавантажених проектів з великими обсягами даних. Elasticsearch є нереляційним сховищем (NoSQL) документів у форматі JSON, та пошуковою системою на базі повнотекстового пошуку Lucene. Апаратна платформа – Java Virtual Machine, тому системі потрібна велика кількість ресурсів процесора та оперативної пам’яті для роботи.

Кожне повідомлення, як з Logstash або за допомогою API запиту, індексується як “документ” – аналог таблиці в реляційних SQL. Усі документи зберігаються в індексі – аналог бази даних SQL.

Вся робота з базою даних будується на JSON запитах за допомогою REST API, які або видають документи за індексом, або статистику у форматі: питання – відповідь. Для того щоб всі відповіді на запити візуалізувати була написана Kibana, яка представляє собою веб-сервіс.

Kibana дозволяє шукати\брати дані і статистику з бази даних Elasticsearch, але на основі відповідей будуються безліч красивих графіків і дашбордів. Також система має функціонал адміністрування бази даних Elasticsearch.

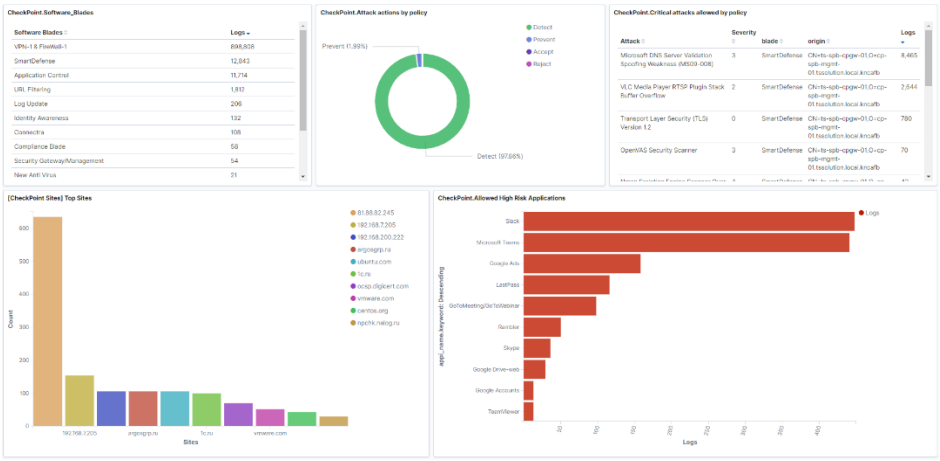

Рис. 2.6 приклад звіту в Kibana

Спочатку налаштовується метрика, це значення, яким будуть агрегуватися всі поля. Метрики обчислюються з урахуванням значень, витягнутих тим чи іншим способом із документів. Значення зазвичай витягуються з полів документа, але можуть бути згенеровані з використанням скриптів. У BUCKETS можна додати кілька поділок до створення кількох стовпців чи таблиць, обмеження тут скоріш стоять логічні. В AGGREGATION можна вибрати яким способом відбуватиметься поділ на сегменти: ipv4 range, date range, Terms тощо. Найбільш цікавим вибором є саме Terms і Significant Terms, розподіл на сегменти проводиться за значеннями певного поля індексу, різниця між ними полягає в кількості значень, що повертаються, і їх відображення.

Замість рядків в Elasticsearch використовуються два типи даних – текст і ключове слово. В результаті Elasticsearch рахує кількість логів за певний час з агрегуванням за значенням у полі продукції. У Custom Label необхідно задати назву колони, яке відображатиметься в таблиці, задати час за який необхідно зібрати логи. Kibana починає процес візуалізації, шляхом відправлення запитів до Elasticsearch.

2.4 Призначення та архітектура рішення Filebeat

Filebeat — це легкий вантажовідправник для пересилання та централізації даних журналу, написаний мовою програмування Java. Встановлений як агент на серверах, Filebeat відстежує файли журналів або розташування, які вказані, збирає події журналу та пересилає їх до Elasticsearch або Logstash для індексації.[13]

Filebeat запускає один або кілька процесів, які шукають у місцях, що були вказані для даних журналу. Для кожного журналу, який Filebeat знаходить, Filebeat запускає комбайн. Кожен комбайн зчитує окремий журнал для нового вмісту та надсилає нові дані журналу до libbeat, який об'єднує події та надсилає агреговані дані на вихід, що був налаштуваний для Filebeat. Комбайн відповідає за читання вмісту окремого файлу. Комбайн зчитує кожен файл, рядок за рядком, і відправляє вміст на вихід. Для кожного файлу запускається один комбайн. Комбайн відповідає за відкриття та закриття файлу, а це означає, що дескриптор файлу залишається відкритим під час роботи комбайна. Якщо файл видалено або перейменовано під час його збирання, Filebeat продовжує читати файл. Це має побічний ефект, що місце на диску зарезервовано, поки комбайн не закриється. За замовчуванням Filebeat зберігає файл відкритим, поки не буде досягнуто close_inactive.

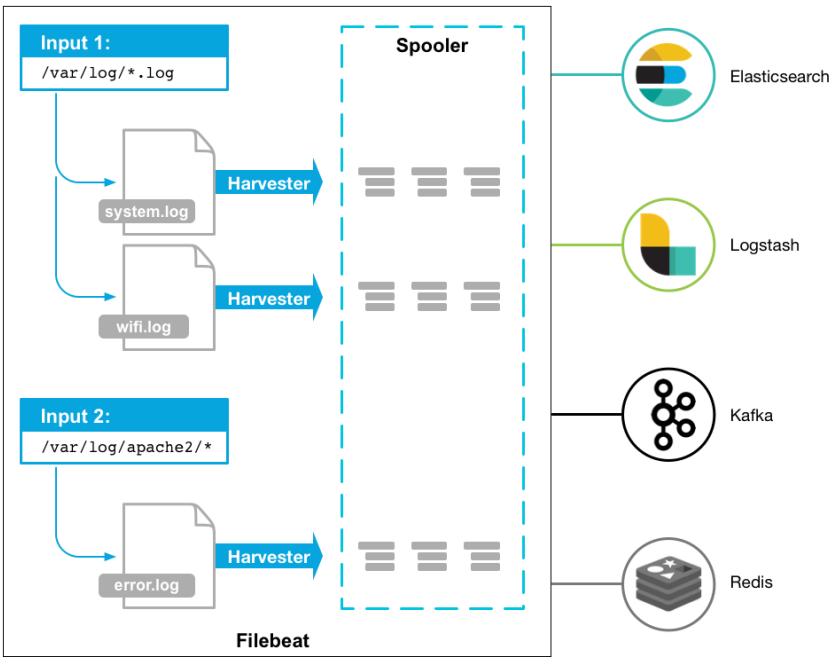

Рис. 2.7 схема процесу роботи Filebeat

Filebeat має безліч вхідних інтерфейсів для різних джерел лог-повідомлень.

Filebeat зберігає стан кожного файлу і часто скидає стан на диск у файлі реєстру. Цей стан використовується для запам'ятовування останнього зсуву, з якого зчитував комбайн, і для забезпечення надсилання всіх рядків журналу. Якщо вихідні дані,

2.5 Вимоги до системи для інсталяції Wazuh SIEM

Підтримувані операційні системи

Сервер Wazuh і компоненти Elastic Stack можна встановити в таких операційних системах Linux:

Amazon Linux 2

CentOS 7 і новіших версій

Debian 8 ELTS і новіших версій

Fedora Linux 31 і новіших версій

openSUSE Tumbleweed, Leap 15.2 і новіші

Oracle Linux 6 Extended та новішої версії

Red Hat Enterprise Linux 6 ELS і новіших версій

Ubuntu 14.04 ESM і новіших версій

Розгортання типу «все в одному».

При розгортанні «все в одному» сервер Wazuh і Elastic Stack встановлюються на одному хості. Типовий варіант використання такого середовища підтримує близько 100 агентів.

Мінімальні вимоги для такого типу розгортання – 4 ГБ оперативної пам’яті та 2 ядра ЦП, а рекомендовані – 16 ГБ ОЗП та 8 ядер ЦП. Потрібна 64-розрядна операційна система.

Вимоги до дискового простору залежать від генерованих сповіщень за секунду (APS). Очікуваний APS суттєво різниться залежно від кількості та типу контрольованих кінцевих точок. Приблизний обсяг пам’яті на одного агента,

необхідний для сповіщень протягом 90 днів залежно від типу контрольованої кінцевої точки (табл.1).

Табл. 2.3 розрахунок використаного обсягу пам’яті для розгортання типу «все в одному»

Відстежуванні кінцеві точки	APS	Зберігання (90 днів/ ГБ)
Сервери	0,25	3.8
Робочі станції	0.1	1.5
Мережні пристрої	0,5	7.6

Розподілене розгортання

У розподіленому розгортанні і сервер Wazuh, і Elastic Stack встановлюються на окремих хостах. Ця конфігурація рекомендована для середовищ, які вимагають високої доступності та масштабованості служб.

Сервер Wazuh і Elastic Stack можуть бути встановлені як одновузловий кластер, так і як багатовузловий кластер. Kibana можна встановити на тому самому вузлі, що й Elasticsearch, або на виділеному хості. Рекомендації щодо обладнання для кожного вузла (табл 2.2):

Табл. 2.4 вимоги для розгортання типу «розподілене розгортання»

Мінімум			Рекомендовано	
Компонент	RAM (ГБ)	ЦП (ядра)	RAM (ГБ)	ЦП (ядра)
Сервер Wazuh	2	2	8	4
Elastic Stack	4	2	16	8

Необхідна 64-розрядна операційна система.

Що стосується вимог до дискового простору, кількість даних залежить від генерованих сповіщень за секунду (APS). Приблизний дисковий простір на одного

агента, необхідний для зберігання сповіщень протягом 90 днів на сервері Wazuh і на сервері Elasticsearch, залежно від типу контрольованих кінцевих точок (табл 2.3):

Табл. 2.5 – розрахунок використаного обсягу пам’яті для розгортання типу «розподілене розгортання»

Відстежувані кінцеві точки	APS	Зберігання (90 днів/ ГБ) на сервері Wazuh	Зберігання (90 днів/ ГБ) на Elasticsearch
Сервери	0.25	0.1	3.7
Робочі станції	0.1	0.04	1.5
Мережні пристрої	0.5	0.2	7.4

Щоб визначити, чи потребує сервер Wazuh більше ресурсів, можна відстежувати такі файли:

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

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

Ці дві змінні мають дорівнювати нулю, якщо середовище працює належним чином. Якщо це не так, до кластера можна додати додаткові вузли. Щоб контролювати, чи працює середовище Elastic Stack належним чином, доступні такі інструменти, як аналізатор продуктивності. У разі потреби масштабування рекомендується розподілене розгортання Wazuh з Elastic Stack.

Elasticsearch або Logstash, недоступні, Filebeat відстежує останні надіслані рядки і продовжить читати файли, як тільки вихідні дані знову стануть доступними. Під час роботи Filebeat інформація про стан також зберігається в пам’яті для кожного входу. Коли Filebeat перезапускається, дані з файлу реєстру використовуються для відновлення стану, і Filebeat продовжує роботу кожного комбайна в останній відомої позиції.

Для кожного входу Filebeat зберігає стан кожного знайденого файлу. Оскільки файли можна перейменувати або перемістити, імені файлу та шляху недостатньо для ідентифікації файлу. Для кожного файлу Filebeat зберігає унікальні ідентифікатори, щоб визначити, чи був файл зібраний раніше.

2.6 Можливості щодо адміністрування Wazuh SIEM

У цьому розділі описані основні можливості адміністрування та забезпечення управління інцидентами в інформаційній системі підприємства.

Автоматизоване управління журналами і аналіз прискорюють виявлення загроз. У багатьох випадках докази атаки можна знайти в повідомленнях журналу пристроїв, систем і додатків. Wazuh можна використовувати для автоматичного агрегування та аналізу даних журналу.

Агент Wazuh, що працює на кінцевій точці, відповідає за читання операційної системи та журналів додатків повідомлень, пересилання тих, на сервер Wazuh, де відбувається аналіз. Коли агент не розгорнутий, сервер також може отримувати дані через системний журнал від мережевих пристроїв або додатків.

Після створення сервером Wazuh сповіщення відправляються в компонент Elastic Stack, де вони збагачуються інформацією про геолокації, зберігаються та індексуються. Потім Kibana можна використовувати для пошуку, аналізу та візуалізації даних.

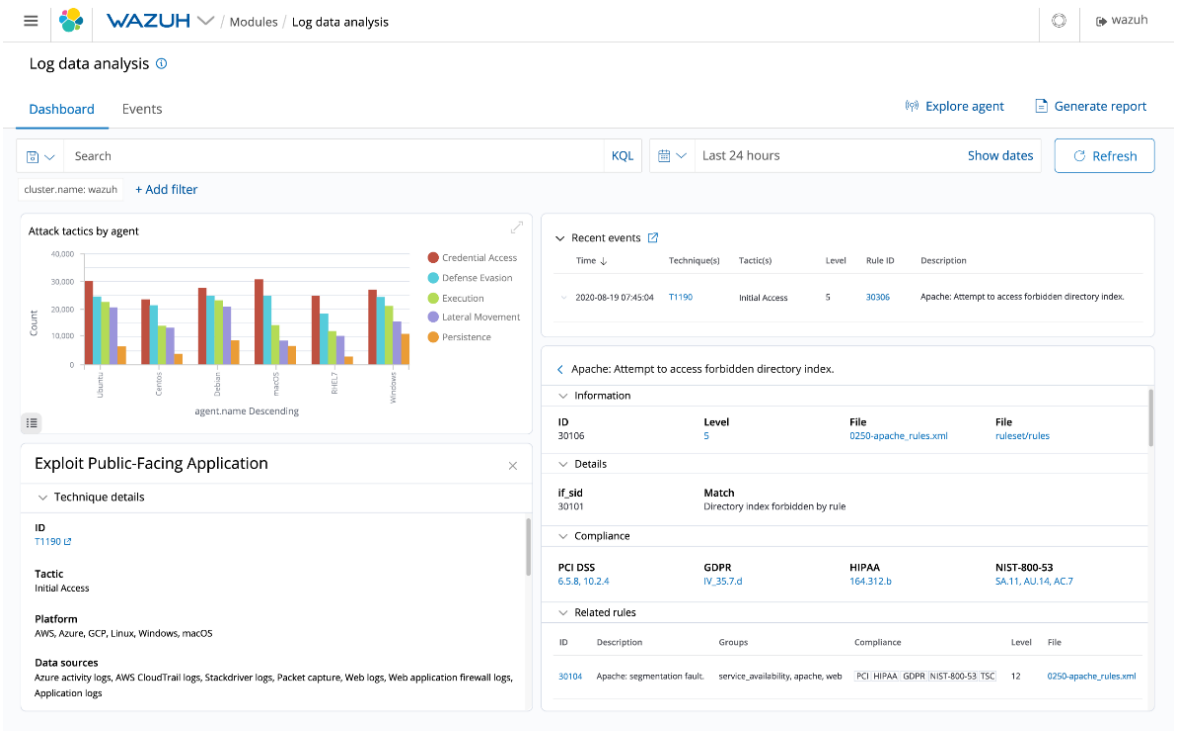

Рис.2.8 Відображення аналізу даних журналу

Компонент моніторингу цілісності файлів (FIM) виявляє та попереджає про зміну файлів операційної системи або додатків. Ця можливість часто використовується для виявлення доступу або змін до конфіденційних даних.

Повноцінний звіт змін файлів можна знайти на панелі управління FIM, яка надає можливості деталізації для перегляду всіх деталей ініційованих попереджень.

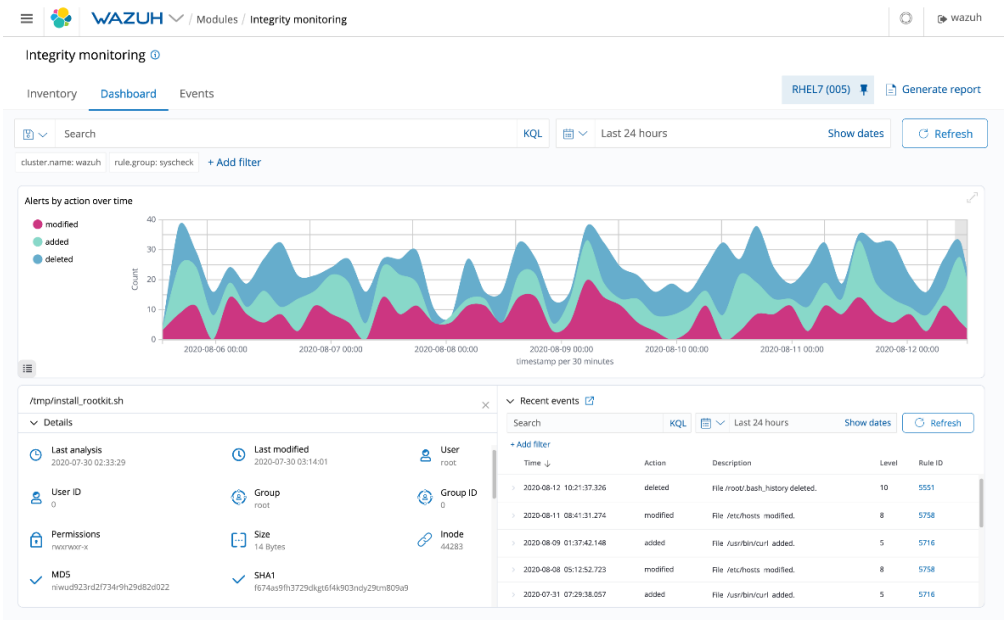

Рис.2.9 Відображення процесу моніторингу цілісності файлів [14]

Агент Wazuh періодично сканує систему, що відстежується, для виявлення руткітів як на рівні ядра, так і на рівні користувацького простору. Цей тип шкідливого програмного забезпечення зазвичай замінює або змінює існуючі компоненти операційної системи, щоб змінити поведінку системи. Руткіти можуть приховувати інші процеси, файли та мережеві підключення.

Wazuh використовує різні механізми виявлення для пошуку системних аномалій або відомих вторгнень. Це періодично робить компонент Rootcheck.

Також агент Wazuh автоматизує реакцію на загрози при їх виявленні. Крім іншого, агент може заблокувати мережеве з'єднання, зупинити запущений процес або видалити шкідливий файл. Він також може запускати призначені для користувача сценарії, розроблені користувачем (наприклад, Python, Bash або PowerShell).

Щоб скористатися цією функцією, користувачі визначають умови, які будуть запускати дії сценарію. Ці умови зазвичай включають виявлення і оцінку загроз. Наприклад, користувач може використовувати правила аналізу журналу для виявлення спроби вторгнення і базу даних IP-репутації для оцінки загрози шляхом пошуку IP-адреси джерела спроби підключення.

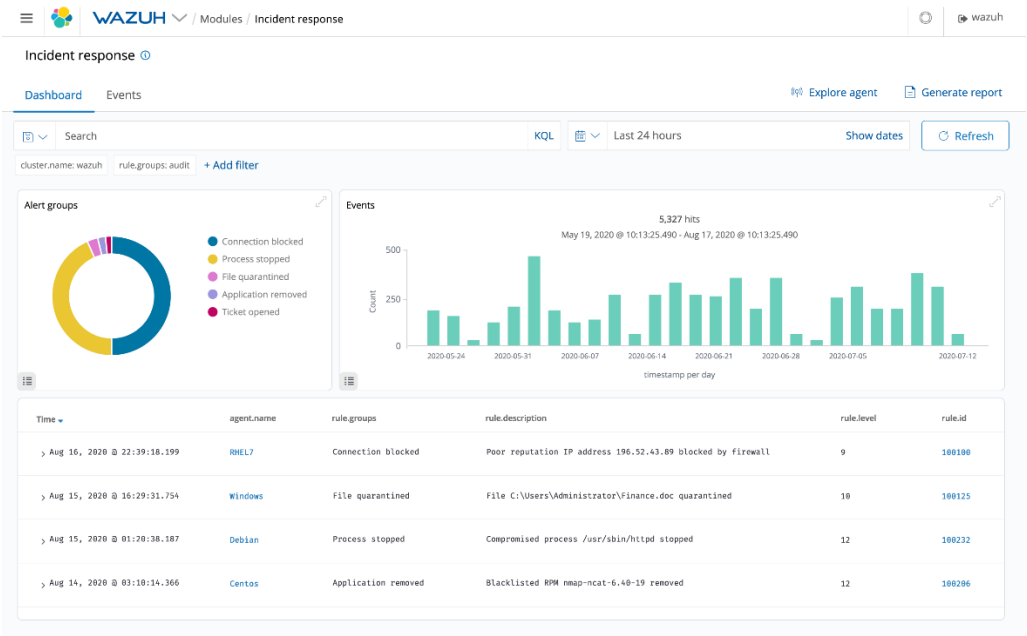

Рис. 2.10 Відображення процесу спрацювання активної відповіді

Модуль Wazuh SCA допомагає підтримувати стандартну конфігурацію через контрольовані кінцеві точки.

Коли модуль SCA включений, агент Wazuh періодично виконує сканування, повідомляючи про неправильну конфігурацію в системі. Ці сканування оцінюють конфігурацію системи за допомогою файлів політик, які містять набір перевірок, що необхідно запустити. Наприклад, SCA може перевіряти конфігурацію файлової системи, перевіряти наявність оновлень програмного забезпечення або виправлень безпеки, бачити, чи включений локальний брандмауер, визначати непотрібні запущені служби або перевіряти політику паролів користувачів.

Політики сканування SCA написані в форматі YAML.

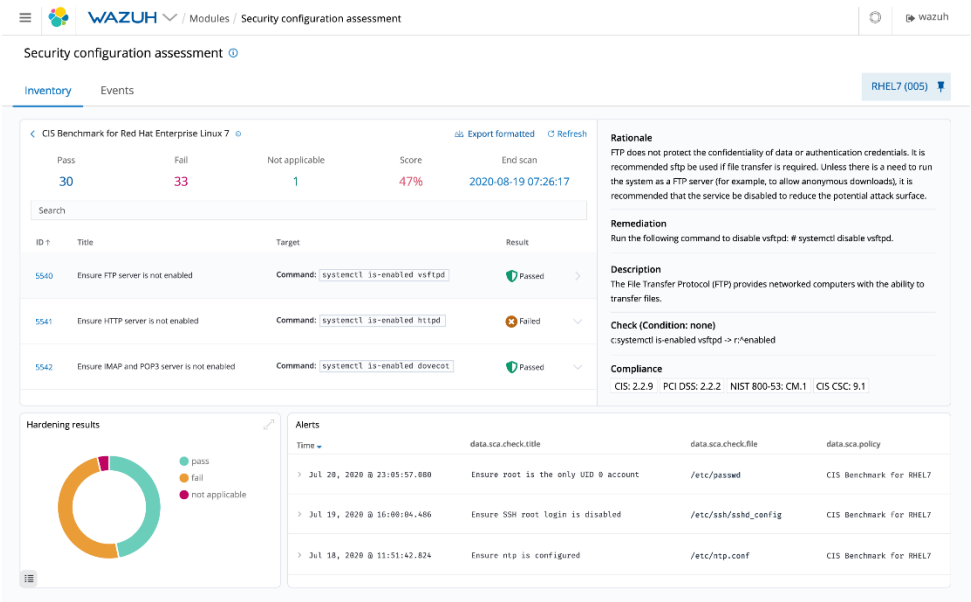

Рис.2.11 Відображення процесу сканування конфігурації системи

Модуль інвентаризації системи агента Wazuh збирає інформацію про апаратне та програмне забезпечення з системи. Ця можливість допомагає ідентифікувати активи та оцінити ефективність управління виправленнями.

Зібрані дані інвентаризації для кожної кінцевої точки, за якою ведеться спостереження, можна запросити через Wazuh RESTful API з призначеного для користувача веб-інтерфейсу. Це включає використання пам’яті, дисковий простір,

характеристики ЦП, мережеві інтерфейси, відкриті порти, запущені процеси і список встановлених додатків.

Для збору даних агент Wazuh періодично виконує сканування (часовий інтервал налаштовується). Після завершення сканування агент порівнює нові дані інвентаризації зі старими з попереднього сканування. Таким чином агент ідентифікує системні події, наприклад, коли був відкритий новий порт, процес був зупинений або було встановлено новий додаток.

Wazuh може виявляти вразливі додатки і складати звіти про ризики.

Для виявлення уразливого програмного забезпечення Wazuh використовує базу даних Common Vulnerabilities and Exposures (далі – CVE), створену автоматично з використанням даних, взятих з наступних джерел:

https://canonical.com: CVE для дистрибутивів Ubuntu Linux.

https://access.redhat.com: CVE для дистрибутивів Red Hat і CentOS Linux.

https://www.debian.org: CVE для дистрибутивів Debian Linux.

https://nvd.nist.gov/: CVE з Національної бази даних вразливостей.

https://www.microsoft.com/msrc: Центр підтримки безпеки Майкрософт.

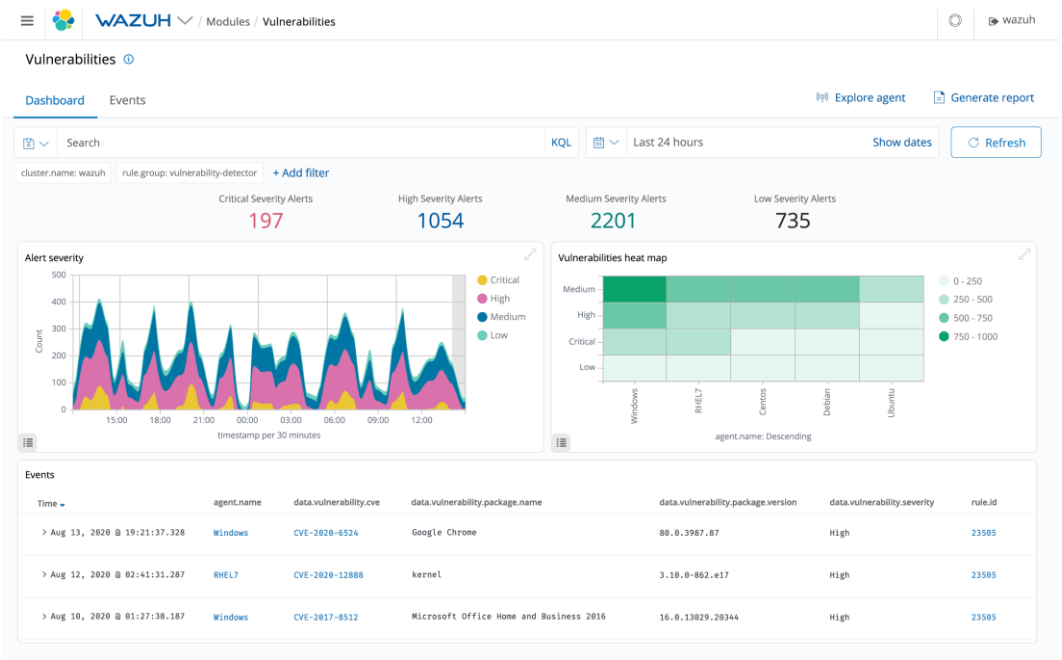

Рис.2.12 Відображення процесу виявлення вразливостей

Платформа безпеки Wazuh забезпечує виявлення загроз, відповідність конфігурації і безперервний моніторинг для мультихмарних та гібридних середовищ.

Він здатний захищати хмарні робочі навантаження шляхом моніторингу інфраструктури на двох різних рівнях:

Рівень кінцевої точки: моніторинг хмарних примірників або віртуальних машин за допомогою легкого агента безпеки Wazuh.

Рівень хмарної інфраструктури: моніторинг хмарних сервісів і активності шляхом збору та аналізу даних з API провайдера. Підтримуються Amazon AWS, Microsoft Azure і Google Cloud Platform.

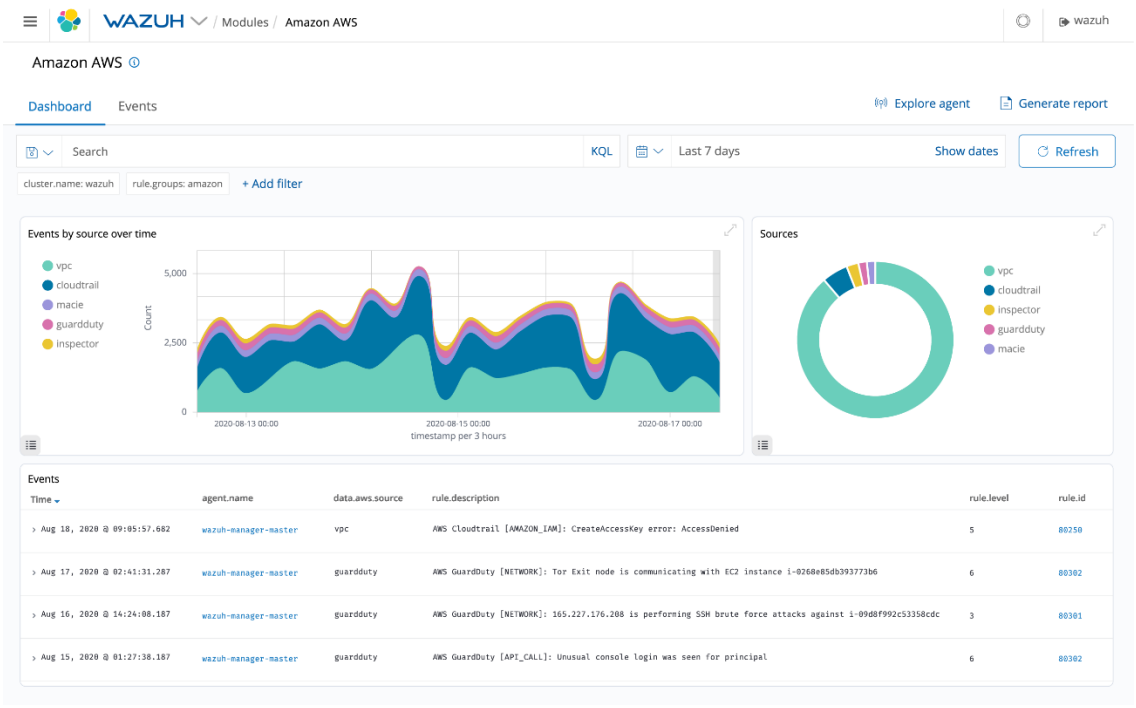

Рис.2.13 Відображення процесу моніторингу хмарної безпеки

Wazuh використовується для відстеження ознак інцидентів безпеки в контейнерах з попередженням в режимі реального часу. Wazuh може захищати робочі навантаження контейнерів на двох різних рівнях:

Рівень інфраструктури. Wazuh надає наступні механізми для моніторингу хостів Docker або вузлів Kubernetes:

Інтеграція з механізмом Docker та API Kubernetes: в цьому сценарії модуль Wazuh для Docker діє як передплатник. Він прослуховує події Docker або Kubernetes, маючи можливість попереджати про виявлення аномалії або інциденту безпеки;

Розгортання агента Wazuh на хостах Docker і вузлах Kubernetes: для самокерованої інфраструктури розгортання агента Wazuh забезпечує повний набір функцій безпеки, таких як виявлення шкідливих програм, моніторинг цілісності файлів, оцінка конфігурації, аналіз даних журналу, виявлення вразливостей та активні відгуки;

Інтеграція з постачальниками розміщеної інфраструктури (наприклад, Google GKE, Amazon EKS і т. Д.). В цьому випадку модулі Wazuh для моніторингу безпеки хмари завантажують журнали аудиту керованих послуг для аналізу безпеки.

Рівень контейнера. Щоб отримати видимість на рівні контейнера, можна розгорнути агент Wazuh в контейнері Kuberentes DaemonSet. Такий тип розгортання гарантує, що агент Wazuh буде працювати на всіх вузлах кластера Kuberentes. Крім того, інші модулі Kuberentes зможуть відправляти дані (наприклад, повідомлення журналу додатків) в контейнер DaemonSet, щоб агент міг їх обробити і переслати на сервер Wazuh для аналізу безпеки.

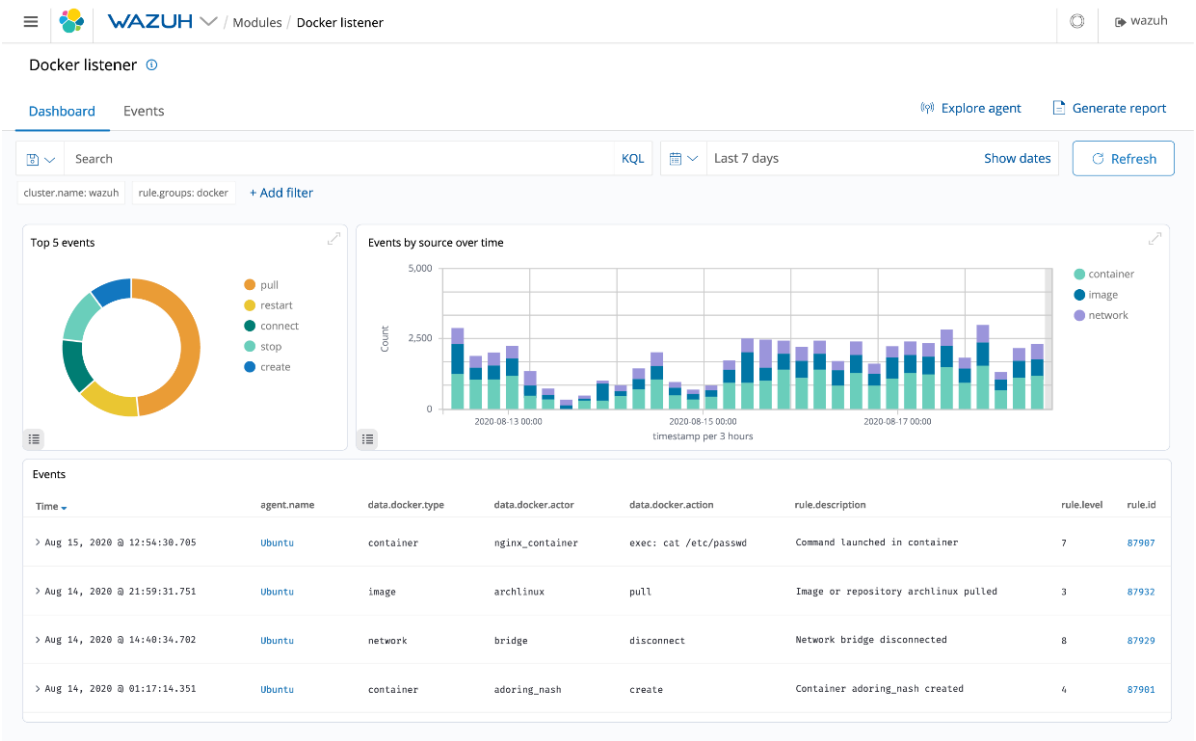

Рис.2.14 Відображення процесу моніторингу контейнерів

Платформа Wazuh часто використовується для задоволення технічних аспектів нормативних вимог. Wazuh не тільки забезпечує необхідні засоби управління безпекою (наприклад, виявлення вторгнень, оцінку конфігурації, аналіз журналів, виявлення вразливостей та інше) для відповідності вимогам, але також використовує свої можливості SIEM для централізації, аналізу та збагачення даних безпеки.

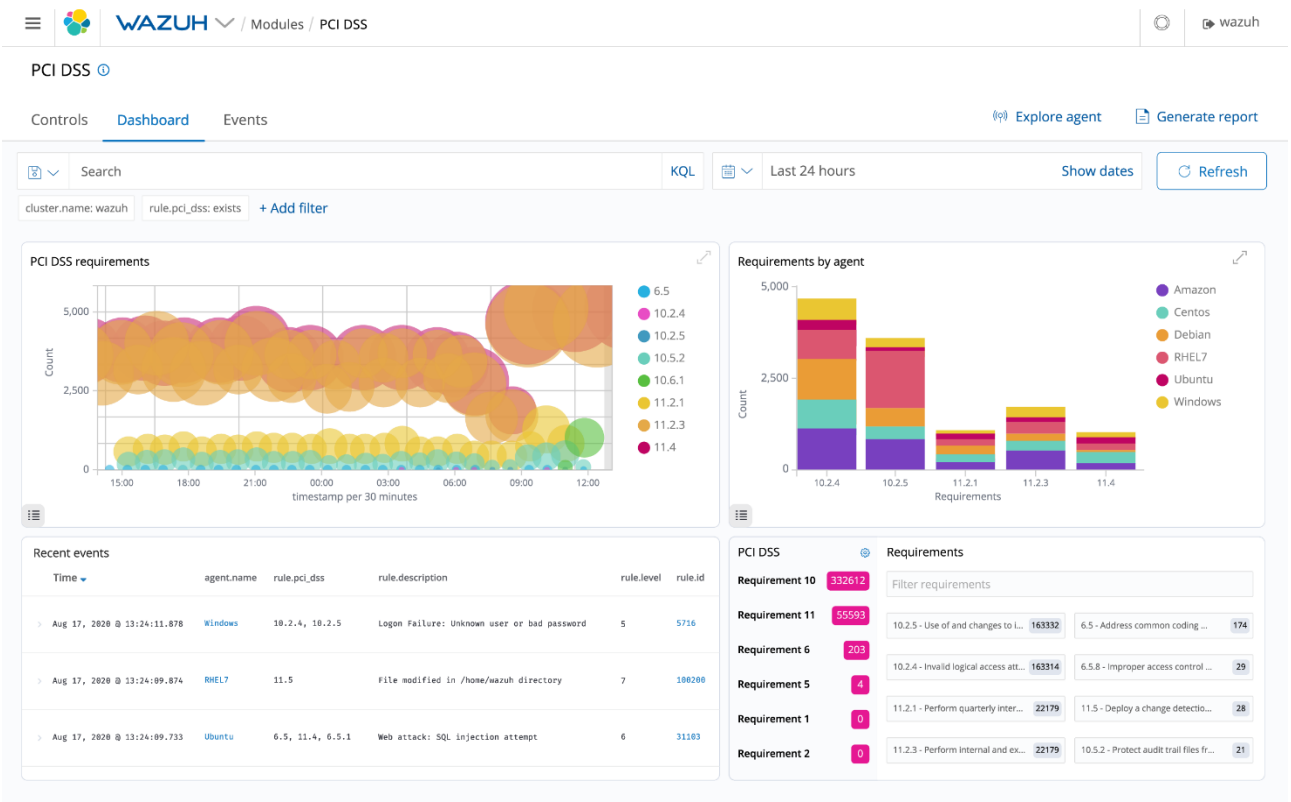

Рис. 2.15 Відображення процесу збору інформації з агентів

Висновки до розділу 2

Досліджено основні компоненти SIEM-системи Wazuh, їх функції та можливості.

Проаналізовано системні вимоги для встановлення SIEM-системи Wazuh, для типу «все в одному» та розподіленого типу встановлення.

Проаналізовано та досліджено функції збору інформації з хостів агентами Wazuh, процес моніторингу контейнерів та хмарних середовищ.

Досліджено процес налаштування та роботи активної відповіді.

3 РОЗРОБЛЕННЯ ВАРІАНТА УПРАВЛІННЯ ІНЦИДЕНТАМИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ПІДПРИЄМСТВА НА БАЗІ WAZUH SIEM

3.1 Розроблення варіанта конфігурації системи управління інцидентами в інформаційній системі підприємства на базі Wazuh

На основі документації розробника щодо управління інцидентами в інформаційній системі підприємства, присутній варіант базової конфігурації SIEM-системи Wazuh.

За замовчуванням при встановленні та фінальній конфігурації SIEM-системи встановлюється обліковий запис адміністратора безпеки.

Адміністратор безпеки – фахівець з питань інформаційної безпеки, призначений внутрішнім документом організації для забезпечення впровадження та підтримки роботи засобів захисту інформації[15].

Обов’язками адміністратора безпеки є:

визначити порядок організації моніторингу та управління подіями безпеки відповідно до прийнятої політики безпеки.

контроль наявності підключення всіх машин до сервера сервісу моніторингу, аналізу та управління подіями безпеки.

слідкування за проблемами в мережі, виявлення аномалій, шкідливої активності та попередження атак хакерів.

розслідування причини та походження подій, що порушують правила безпеки та створюють загрозу або вже порушують конфіденційність, доступність та цілісність інформації.

Це перший обліковий запис, який буде створено під час процесу встановлення. Далі необхідно виконати створення інших облікових записів, надати їм лише потрібні права та використовувати обліковий запис адміністратора безпеки за крайньої необхідності.

3.1.1 Налаштування сповіщень електронною поштою

Wazuh можна налаштувати для відправлення попереджень по електронній пошті на один або декілька адрес електронної пошти при розробленні певних правил або для щоденних повідомлень про події.

Табл 3.1 Доступні параметри конфігурації електронної пошти:

Назва	Значення за замовченням	Допустимі значення
alerts_log – перемикає написання попереджень на /var/ossec/logs/alerts/alerts.log		Відсутні
повідомлення по електронній пошті – перемикає використання сповіщень електронною поштою		Відсутні
email_to – вказує одержувача електронної пошти для попереджень	Відсутнє	Будь-яка діюча адреса електронної пошти
email_reply_to – вказується адреса «для відповіді», що міститься в оповіщеннях по електронній пошті	Відсутнє	Будь-яка діюча адреса електронної пошти
smtp_server – параметр визначає, який SMTP-сервер використовувати для доставки попереджень	Відсутнє	дійсне ім'я хоста або IP-адресу. повний шлях до виконуваного файлу, схожий на sendmail.

hello_server – визначає, як сервер ossec буде ідентифікувати себе при відправці пошти	notify.ossec.net	Будь-яке допустиме ім’я хоста
email_maxperhour – встановлює максимальну кількість повідомлень по електронній пошті, які можуть бути відправлені за годину. Всі електронні листи понад цей погодинний поріг поміщаються в чергу для відправки разом в одному електронному листі в кінці години	12	Будь-яке число від 1 до 1000000
email_idsname – ім'я буде додано в заголовки електронного листа з вказаним значення	Відсутнє	Будь-яке ім’я
email_log_source – вибирає файл попереджень для читання	alerts.json	alerts.log або alerts.json
статистика – встановлює рівень серйозності подій, які генеруються статистичним аналізом	8	Будь-який рівень від 0 до 16
logall – задає, чи слід зберігати події, навіть якщо вони не активують правило з результатами, записаними в /var/ossec/logs/archives/archives.log	Відсутнє	так/ні

logall_json – задає, чи слід зберігати події, навіть якщо вони не активують правило з результатами, записаними в /var/ossec/logs/archives/archives.json	Відсутнє	так/ні
розмір пам’яті – встановлює розмір пам'яті для механізму кореляції подій	8192	Будь-яке ціле число, але значення менше 2048 будуть замінені на 2048
white_list – вказує IP-адресу, для якого не будуть активуватися активні відповіді. Для кожного <while_list> тега може бути зазначений тільки один IP-адрес, але можна використовувати кілька IP-адрес, включаючи кілька <white_list> тегів	Відсутнє	Будь-яка IP-адреса або мережевий блок
host_information – встановлює рівень серйозності подій, що генеруються монітором змін хоста	8	Можна використовувати будь-який рівень від 0 до 16
jsonout_output – перемикає запис попереджень в форматі JSON в /var/ossec/logs/alerts/alerts.json, які будуть включати ті ж події, що будуть відправлятися в alerts.log, тільки в форматі JSON	так	так/ні
prelude_output – перемикає вивід Prelude	ні	так/ні

Щоб налаштувати Wazuh для відправки попереджень електронною поштою, необхідно налаштувати параметри електронної пошти в <global> розділі ossec.conf файлу.

```
<ossec_config>
    <global>
        <email_notification>yes</email_notification>
        <email_to>me@test.com</email_to>
        <smtp_server>mail.test.com</smtp_server>
        <email_from>wazuh@test.com</email_from>
    </global>
    ...
</ossec_config>
```

Рис. 3.1. Налаштування Wazuh для відправки попереджень електронною поштою

Після налаштування вищезазначеного email_alert_level потрібно встановити мінімальний рівень попередження, який спричинить електронний лист. За замовчуванням для цього рівня встановлено 12.

```
<ossec_config>
  <alerts>
      <email_alert_level>10</email_alert_level>
  </alerts>
  ...
</ossec_config>
```

Рис. 3.2. Налаштування рівня попередження Wazuh

Після alert_level налаштування, Wazuh потрібно перезапустити, щоб зміна набрала чинності.

Для Systemd:

 # systemctl restart wazuh-manager

Для SysV Init:

 # service wazuh-manager restart

3.1.2 Налаштування виводу syslog

Параметри конфігурації для відправки попереджень на сервер системного журналу:

server;

port;

level;

group;

rule_id;

location;

use_fqdn;

format.

Табл 3.2 Доступні параметри конфігурації виводу syslog:

Назва	Значення за замовченням	Допустимі значення
Server IP-адрес або ім’я хосту сервера системного журналу		Будь-який діючий IP-адрес
Port Порт для пересилки попереджень	514	Будь-який діючий порт
Level Мінімальний рівень пересилки попереджень		Будь-який рівень від 1 до 16
Group Група правил пересили попереджень		Будь-яка діюча група. Необхідно розділіти декілька

		груп вертикальною рисскою («|»).
Rule_id Ідентифікатор правил перенаправлення попереджень		Будь-який доступний rule_id
Location Поле «Місце розташування» відноситься до джерела попередження, яке може бути: syscheck; rootcheck; file path(путь файла); Command or its alias(Команда або її псевдонім); command_tag (wodle); aws-cloudtrail; cis-cat; vulnerability-detector(детектор вразливостей); syscollector(системний колектор);		Будь-яке доступне місце розташування
Use_fqdn Переключити для повного або скороченого імені хосту, налаштованого на сервері. За замовчуванням ossec скорочує ім'я хосту до першої точки (".") Під час	ні	так /ні

створення повідомлень системного журналу		
Format Формат виводу попереджень. Коли jsonout_output в глобальному розділі включений, попередження зчитаються з alerts.json, а не з alerts.log для формату JSON.		Cef – виведе дані в форматі загальних подій ArcSight. Splunk – буде виводити дані в форматі, зручному для Splunk. Json – буде виводити дані в форматі JSON, які можуть використовуватися різними інструментами

Налаштування:

Вказана конфігурація надсилатиме попередження, 192.168.1.240, а якщо рівень попередження вище 9 - також 192.168.1.241.

```
<ossec_config>
  <syslog_output>
    <level>9</level>
    <server>192.168.1.241</server>
  </syslog_output>

  <syslog_output>
    <server>192.168.1.240</server>
  </syslog_output>
</ossec_config>
```

Рис. 3.3. Налаштування виводу syslog

Для застосування змін, перезапустити Wazuh:

Для Systemd:

 # systemctl restart wazuh-manager

Для SysV Init:

 # service wazuh-manager restart

3.1.3 Створення автоматичних звітів

Щоденні звіти - це зведення попереджень, що спрацьовують щодня. Налаштування індивідуального звіту здійснюється, використовуючи report опцію в ossec.conf файлі.

Правила також можна фільтрувати за рівнем, джерелом, іменем користувача, ідентифікатором правил та інше.

Попередній перегляд звіту може бути створений шляхом передачі вмісту файлу alerts.log демона ossec-reportd.

Параметри, за якими можна налаштувати звіти:

group(група);

category(категорія);

rule(правило);

level(рівень);

location(місце розташування);

srcip(джерело);

user(користувач);

title(заголовок);

email_to;

showlogs.

Налаштування:

Конфігурація буде посилати щоденний звіт про всіх syscheck сповіщень example@test.com.

```
<ossec_config>
  <reports>
      <category>syscheck</category>
      <title>Daily report: File changes</title>
      <email_to>example@test.com</email_to>
  </reports>
</ossec_config>
```

<

Рис. 3.4. Налаштування щоденного звіту Wazuh

Правила також можуть бути відфільтровані за рівнем, джерелом, іменем користувача, ідентифікатором правила тощо.

Наприклад:

На основі конфігурації система надсилатиме звіт із усіма правилами, які запускаються з рівнем вище 10.

```
<ossec_config>
  <reports>
      <level>10</level>
      <title>Daily report: Alerts with level higher than 10</title>
      <email_to>example@test.com</email_to>
  </reports>
</ossec_config>
```

Рис. 3.5. Налаштування рівнів щоденного звіту Wazuh

Попередній перегляд звіту може бути створений шляхом передачі вмісту файлу alerts.log до демона ossec-reportd :

cat /var/ossec/logs/alerts/alerts.log | /var/ossec/bin/ossec-reportd -n "Daily report: Alerts with level higher than 10" -s -f level 10 2> report-test.txt

3.1.4 Додання політики SCA в конфігурації агента для виявлення вразливостей

Модуль оцінки конфігурації безпеки: це набір попередньо визначених політик, які Wazuh використовував для запуску перевірки конфігурації щодо

інфраструктури з встановленими агентами. Це використовується для посилення безпеки і написано на yaml. Якщо політика не дотримана, менеджеру буде надіслано сповіщення.

```
<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <time>04:00</time>
  <skip_nfs>yes</skip_nfs>

  <policies>
    <policy>etc/shared/cis_debian10.yml</policy>
    <policy enabled="no">ruleset/sca/cis_debian9.yml/policy>
    <policy>/my/custom/policy/path/my_policy.yaml</policy>
  </policies>
</sca>
```

Рис. 3.6. Налаштування політики SCA

Присутня можливість налаштувати Wazuh на перевірку шкідливих команд, наприклад [eval(base64_decode], тому ми наведемо список процесів для перевірки.

Щоб створити команду, ми використовуємо команду wodle в Wazuh. Це потрібно додати до файлу /var/ossec/etc/shared/default/agent.conf.

```
<wodle name="command">
  <disabled>no</disabled>
  <tag>ps-list</tag>
  <command>ps -eo user,pid,cmd</command>
  <interval>10s</interval>
  <ignore_output>no</ignore_output>
  <run_on_start>yes</run_on_start>
  <timeout>5</timeout>
</wodle>
```

Рис. 3.7. Налаштування політики SCA для перевірки шкідливих команд

Далі необхідно створити правило для виявлення процесів, які оцінюють код base64

```
nano /var/ossec/etc/rules/local_rules.xml<group name=”wazuh,”>
  <rule id=”100001" level=”0">
    <location>command_ps-list</location>
    <description>List of running process.</description>
    <group>process_monitor,</group>
  </rule>
    <rule id=”100002" level=”10">
    <if_sid>100001</if_sid>
    <match>eval(base64_decode</match>
    <description>Reverse shell detected.</description>
    <group>process_monitor,attacks</group>
  </rule>
</group>
```

Рис. 3.8. Налаштування правил розпізнавання для перевірки шкідливих команд політики SCA

3.2 Технологія застосування програмного комплексу Wazuh

У цьому розділі показано технологію управління Wazuh на прикладі найпоширеніших проблем в більшості підприємств.

3.2.1 Додання хостів до системи управління інцидентами та виявлення їх вразливостей

Для початка процесу управління інцидентами необхідно встановити агенти, які будуть надсилати інформацію до системи. Виявлення вразливостей у Wazuh здійснюється:

Агенти збирають інформацію про локальні програми та періодично надсилають її менеджеру; db sqlite для кожного агента зберігається в менеджері з цією інформацією. Менеджер використовує глобальну базу даних уразливостей, яка створюється з загальнодоступних репозиторіїв CVE, яка використовується для перевірки інформації з даними інвентаризації програм агента.

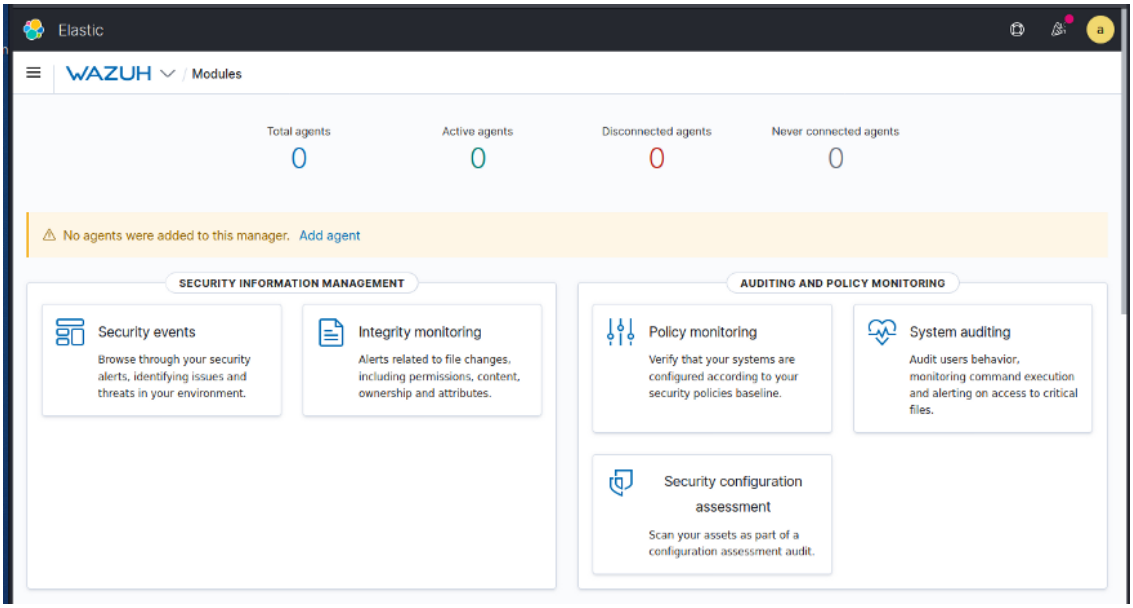

Рис. 3.8 Інтерфейс Wazuh

Для додання агенту необхідно виконати «Add agent» та заповнити форму додання агента, де потрібно вказату його ОС та архітектуру, тощо. На що Wazuh надасть команди для встановлення та запуску агента, запропонує додати його до групи .

Команда для встановлення агента:

curl -so wazuh-agent-4.2.2.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.2.2-1_amd64.deb && sudo WAZUH_MANAGER='localhost' dpkg -i ./wazuh-agent-4.2.2.deb

Команда для запуску агента:

sudo systemctl daemon-reload

sudo systemctl enable wazuh-agent

sudo systemctl start wazuh-agent

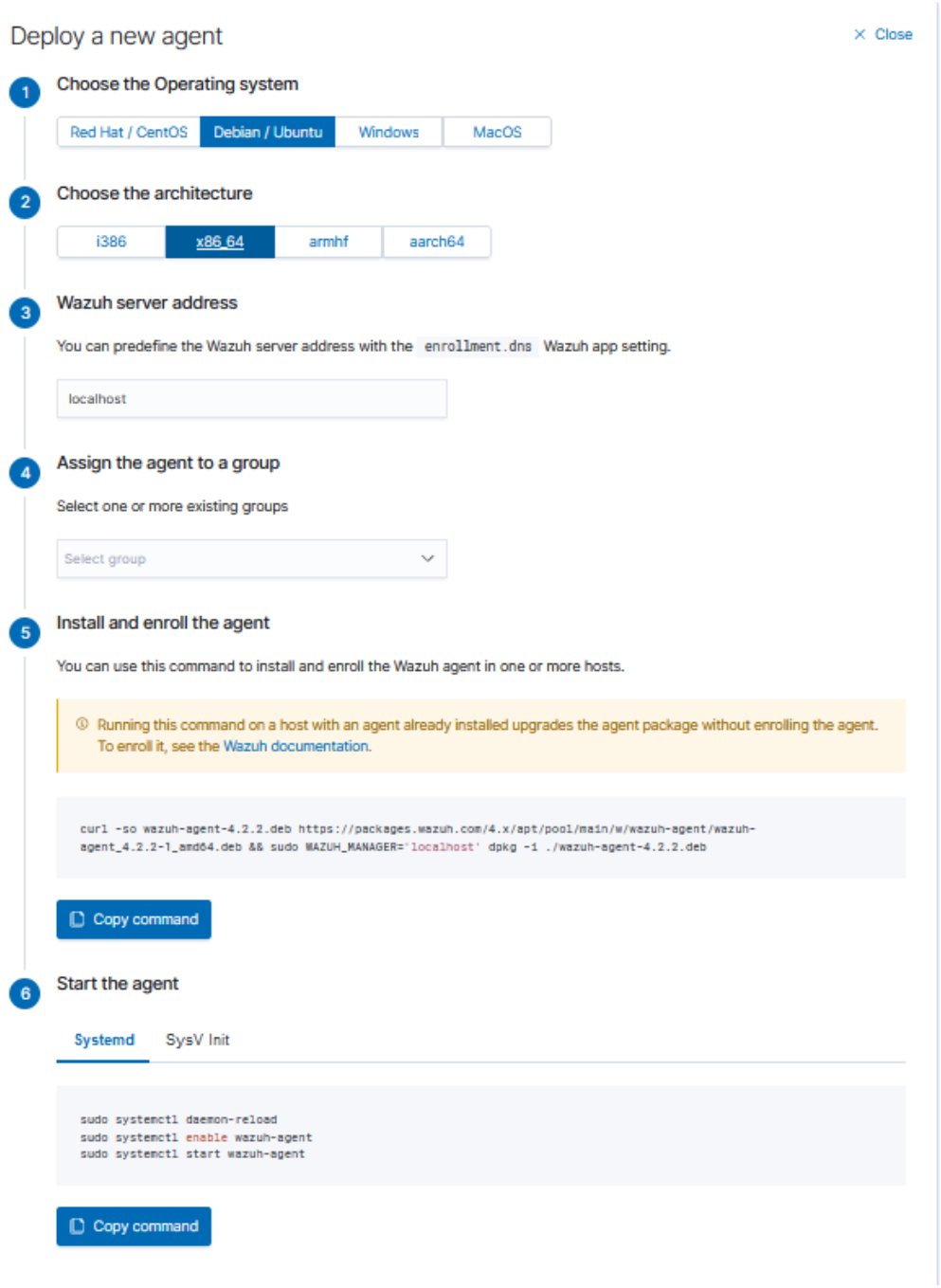

Рис. 3.9 Додання та встановлення агента на машину

Після успішного встановлення потрібно оновити сторінку та на головному екрані буде відображатися кількість агентів.

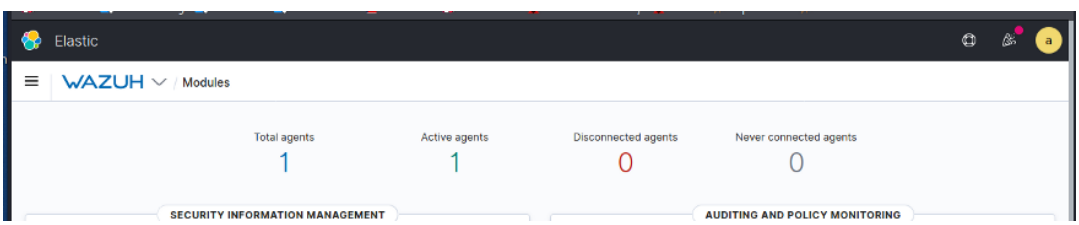

Рис. 3.10 Інтерфейс Wazuh зі встановленим агентом

Для перевірки доданої машини необхідно натиснути на «Active agent»

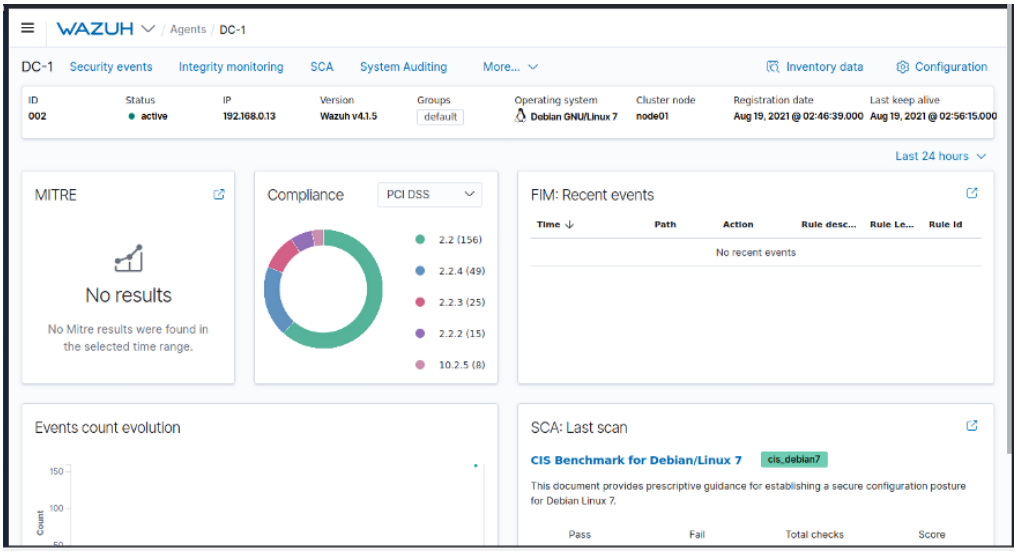

Рис. 3.11 Огляд доданої машини

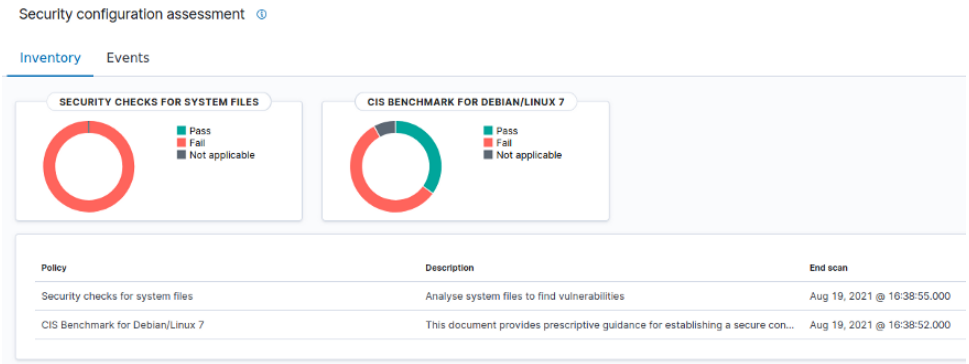

Рис. 3.12 огляд панелі SCA в доданій машині

Відповідно до заданих політик SCA Wazuh виявив проблеми з безпекою.

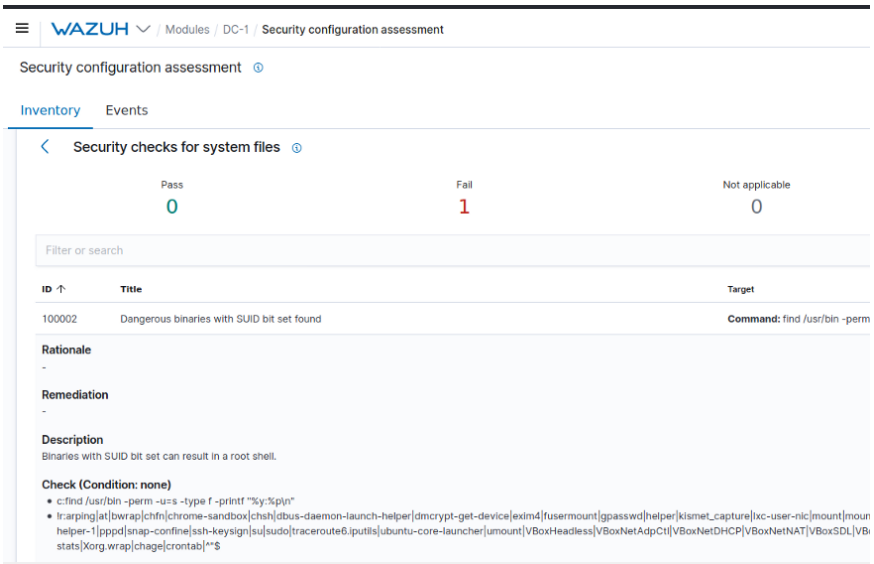

Рис. 3.13 Проблеми з безпекою доданої машини

3.2.2 Проведення кібератаки на машину

Перед початком було перевірено вкладку «Security events», де показуються всі події безпеки.

Рис. 3.14 Вкладка «Security events»

Для перевірки технології управління інцидентами було завантажено та встановлено Kali Linux — це похідний від Debian дистрибутив Linux, розроблений для цифрової криміналістичної експертизи та тестування на проникнення. Він підтримується та фінансується Offensive Security.

Далі було запущено metasploit на машині Kali Linux і використано експлойт.

Експлойт— це частина програмного забезпечення, фрагмент даних або послідовність команд, які використовують помилку чи вразливість, щоб викликати ненавмисне або непередбачене поведінка, яка може відбуватися на комп’ютерному програмному забезпеченні, апаратному забезпеченні чи чомусь електронному (зазвичай комп’ютеризованому). Така поведінка часто включає такі речі, як отримання контролю над комп’ютерною системою, надання дозволу на підвищення привілеїв або атаку відмови в обслуговуванні (DoS або пов’язана з ними DDoS). exploit/unix/webapp/drupal_drupalgeddon2, щоб створити користувача на скомпрометованій машині та отримати сповіщення про атаку.

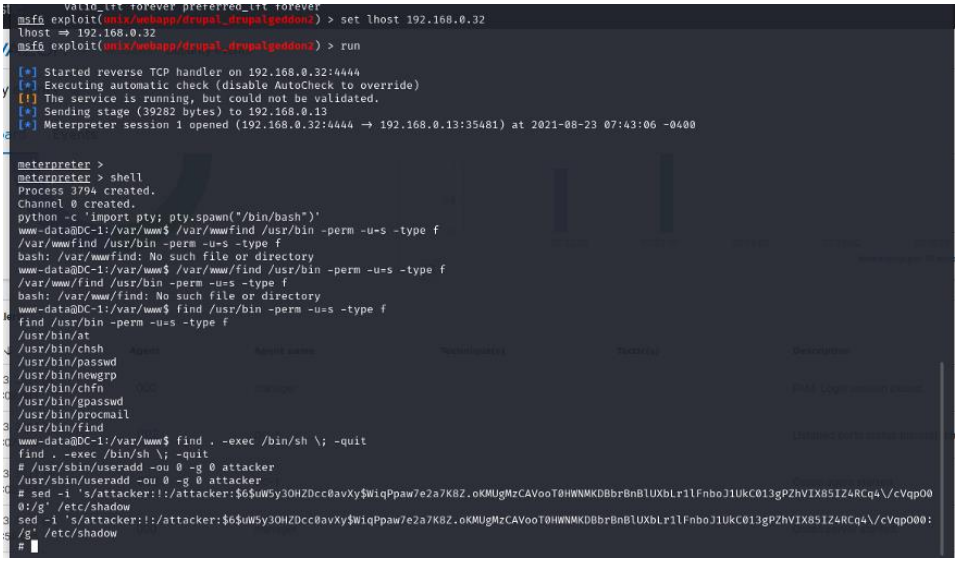

Рис. 3.15 Початок кібератаки

Після проведення кібератаки в SIEM-системі відображається:

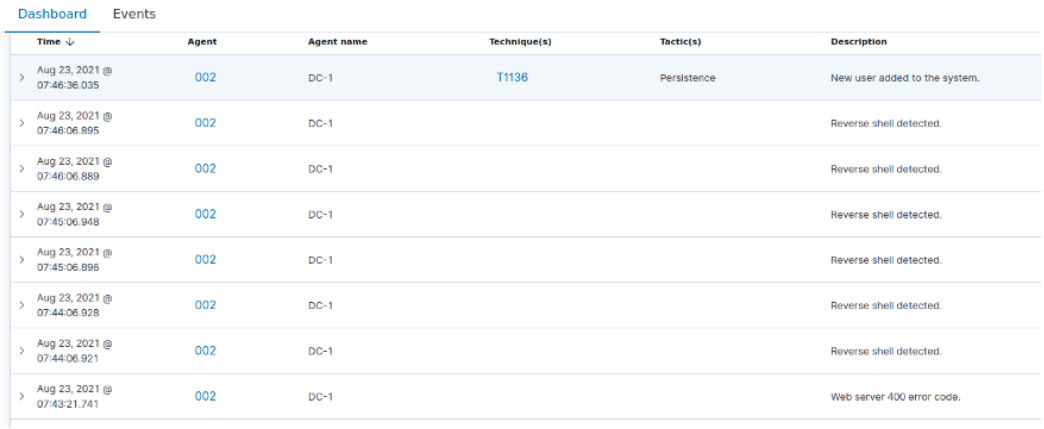

Рис. 3.16 Відображення сповіщень про проведення кібератаки

В сповіщеннях вказано початок атаки, зазначений у «Код помилки веб-сервера 400», потім також було помічено зворотну оболонку та створення користувача.

Для того, зоб SIEM-система надалі змогла перешкоджати зловмисним діям необхідно провести налаштування механізму активної відповіді. В SIEM-системі Wazuh присутня можливість налаштувати активну відповідь для блокування на довільний період часу на основі правил, які спрацювали та їх кількості:

```
<!-- Put active response here -->
<!-- 5712 - ssh bruteforce -->
<!-- 31168 - shellshock -->
<!-- 100704,100705 - blacklist's -->
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>5712,100705</rules_id>
  <timeout>300</timeout>
</active-response>
```

Рис. 3.17 Приклад налаштування активної відповіді

Для перевірки було виконано кібератаку типу «Shellshock». Shellshock — це сімейство помилок безпеки в оболонці Unix Bash, перша з яких була розкрита 24 вересня 2014 року. Shellshock може дозволити зловмиснику змусити Bash виконувати довільні команди та отримати несанкціонований доступ до багатьох Інтернет-сервіси, такі як веб-сервери, які використовують Bash для обробки запитів:

ShellshockTarget="localhost"

curl --insecure $ShellshockTarget -H "User-Agent: () { :; }; /bin/cat /etc/passwd"

До SIEM-системи Wazuh надійшло повідомлення про можливу атаку типу «Shellshock» та відповідне правило, реакція на яке і надійшла до системи:

_id	3euVN28Bxf-j-G8xjir1
_index	wazuh-alerts-3.x-2019.12.24
_score	-
_type	_doc
agent.id	002
agent.ip	172.30.0.30
agent.name	linux-agent
data.protocol	GET
data.srcip	::1
data.url	/
decoder.name	web-accesslog
full_log	::1 - - [24/Dec/2019:11:05:43 +0000] "GET / HTTP/1.1" 200 4833 "-" "() { :; }; /bin/cat /etc/passwd" "-"
id	1577185543.1084649
input.type	log
location	/var/log/nginx/access.log
manager.name	wazuh-manager
rule.description	Shellshock attack attempt
rule.firedtimes	3
rule.gdpr	IV_35.7.d
rule.groups	web, accesslog, attack
rule.id	31166
rule.info	CVE-2014-6271https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
rule.level	15
rule.mail	true
rule.nist_800_53	SI.4
rule.pci_dss	11.4
timestamp	Dec 24, 2019 @ 12:05:43.068

Рис. 3.18 Детальний опис повідомлення

```
<rule id="31166" level="15">
    <if_sid>31101,31108</if_sid>
    <regex>"\(\)\s*{\s*:;\s*}\s*;|"\(\)\s*{\s*foo:;\s*}\s*;|"\(\)\s*{\s*ignored;\s*}\s*|"\(\)\s*{\s*gry;\s*}\s*;</regex>
    <description>Shellshock attack attempt</description>
    <info type="cve">CVE-2014-6271</info>
    <info type="link">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271</info>
    <group>attack,pci_dss_11.4,gdpr_IV_35.7.d,nist_800_53_SI.4,</group>
  </rule>
```

Рис. 3.19 Детальний опис правила

Після спрацювання двох сповіщень про атаку типу «Shellshock» система виконує активну відповідь, про що і повідомляє:

Rule ID	Description	Level	Count
602	Host Unblocked by firewall-drop.sh Active Response	3	12
601	Host Blocked by firewall-drop.sh Active Response	3	7
605	Host Blocked by route-null.cmd Active Response	3	6
606	Host Unblocked by route-null.cmd Active Response	3	1

Рис. 3.20 Сповіщення про блокування та розблокування хоста у зв’зку з таймаутом

3.3 Розроблення рекомендацій щодо технології управління інцидентами в корпоративній інформаційній системі.

За умови створення нових політик безпеки, нових інцидентів кібербезпеки необхідно вчасно реагувати та управляти інцидентами.

Присутня можливість сформувати наступні рекомендації щодо впровадження та використання технології управління інцидентами в інформаційній системі організації:

1. Необхідно налаштувати моніторинг і оповіщення в режимі реального часу

Загалом ця функція є критичним пріоритетом для всіх організацій. Можливість відстежувати та співвідносити загрози в режимі реального часу може бути різницею між незначною помилкою та дорогим пошкодженням і збоєм у роботі ваших систем. Зловмисники та код рухаються швидко, тому вашій команді безпеки потрібно працювати так само швидко.

2. Присутня можливість налаштувати моніторинг активності користувачів

Легко забути, що найчастіше найбільша небезпека для вашої системи криється у ваших власних організаціях. Незалежно від того, чи то через зловмисність, чи через помилку, інсайдерські загрози можуть спричинити ще більший зрив, ніж зовнішній учасник, особливо якщо вони є привілейованим користувачем із розширеним доступом. Відстеження всієї активності користувачів може попередити вас про порушення та виявити неправильне використання та помилки. Крім того, привілейований моніторинг користувачів є вимогою багатьох режимів відповідності.

3. Необхідно використовувати можливість дослідження випадків використання

В SIEM-системах присутня відкрита екосистема, яка дозволяє конфігураціям користувачів підтримувати їх унікальні випадки використання. Використання криміналістичного аналізу даних може знизити ризик, дозволяючи зосередитися на поширених випадках використання у вашому конкретному середовищі. Ці варіанти

використання можуть бути зосереджені як на проектах безпеки, так і на проектах, які не стосуються безпеки, як-от IT-операції.

4. Необхідно використовувати можливість виявлення загроз у навколишньому середовищі

Організації потребують безлічі різних технологій для роботи. SIEM-система повинна мати можливість нормалізувати та співвідносити всі ці різні потоки даних у загальний формат і надати йому значення. Необхідно переконатися, що SIEM-система може обробляти Linux, Windows, бази даних, веб-сервіси, програми або обладнання. Це повинно обмежуватися не лише стандартними джерелами даних, а всіма джерелами в середовищі вашої організації. Для максимальної ефективності SIEM-система повинна мати можливість легко інтегрувати будь-які налаштовані канали, від застарілих програм до доморощених баз даних.

5. Рекомендується налаштувати довгострокове зберігання подій

Немає ніякого шляху: дані займають багато місця. Оскільки журнали постійно передають дані, знадобиться SIEM-система з достатнім простором для зберігання всього цього. Для належного аналізу може знадобитися зберігати більше даних на тривалий термін. Дотримання вимог також може вимагати тривалого зберігання даних. Хоча зберігання важливе, ефективне рішення повинно дозволити точно налаштувати типи даних, які необхідні для зберігання, за винятком даних, які не є шкідливими.

6. Необхідно враховувати процес масштабованості

SIEM-система повинна не тільки функціонувати для організації в їхньому поточному стані, але також повинні мати можливість масштабування з організацією в усіх відношеннях. Наприклад, хоча організації можуть планувати розширення інфраструктури, майже неможливо передбачити, скільки більше даних вони вироблятимуть у міру зростання. Багато рішень SIEM-систем ліцензуються за обсягом оброблених даних, який не тільки важко оцінити, але може різко та швидко збільшити витрати. Необхідно знайти рішення SIEM, яке ліцензує на більш передбачувані вимірювання, як-от пристрій або джерело даних, які можна запланувати заздалегідь, запобігаючи неприємним сюрпризам у розмірі

ліцензійних зборів. Невеликі організації можуть навіть отримати необхідне покриття за допомогою безкоштовного SIEM-системи, наприклад Event Manager, який забезпечує повну функціональність для обмеженої кількості пристроїв і може легко розширюватися до корпоративної версії в міру зростання організації.

7. Необхідно використовувати можливість різного роду інтеграцій

Оскільки пакет безпеки організації розширюється, може бути легко випадково збільшити робоче навантаження вашої IT-команди, вимагаючи від неї маніпулювати надлишком продуктів, які не можуть спілкуватися один з одним. Деякі рішення SIEM-системи можуть отримувати дані з інших корпоративних програм, наприклад, антивірусного програмного забезпечення, дані входу, програмне забезпечення для аудиту безпеки тощо. Це не тільки заощаджує додатковий час, але й забезпечує цілісну картину вашого оточення.

8. Необхідно налаштувати звітність

IT-операції та групи безпеки зобов’язані регулярно надавати звіти як аудиторам, так і керівникам. Більшість організацій також повинні дотримуватися кількох правил, що додає складності та зусиль щодо звітності. SIEM-система має бути здатна надавати будь-які з цих контекстно релевантних звітів вам і вашій команді керівництва.

9. Необхідно налаштувати підтримку журналювання

Значення SIEM-системи зменшується, якщо він не може отримувати й розуміти дані журналу з усіх джерел, що генерують журнали в організації. Найочевиднішим є засоби управління безпекою підприємства, такі як брандмауери, віртуальні приватні мережі, системи запобігання вторгненням, шлюзи електронної пошти та веб-безпеки, а також продукти для захисту від шкідливих програм. Цілком розумно очікувати, що SIEM-система буде розуміти файли журналів, створені будь-яким основним продуктом або хмарною службою в цих категоріях. Якщо цього інструмента немає, він не повинен мати жодної ролі у ваших операціях безпеки.

10. Необхідно налаштувати підтримку можливості реєстрації

Конкретні програми та програмне забезпечення організації можуть не мати надійних можливостей ведення журналу. Деякі системи та служби SIEM можуть доповнювати їх, виконуючи власний моніторинг на додаток до звичайної роботи з керування журналами. Загалом, це розширює SIEM-систему від суворо централізованого інструменту збору, аналізу та звітності до створення необроблених даних журналів від імені інших хостів.

11. Рекомендується налаштувати розвідку загроз

Більшість SIEM-систем здатні приймати канали розвідки загроз. Ці канали, які часто отримують з окремих підписок, містять актуальну інформацію про активність загроз, що спостерігаються в усьому світі, включно з тим, які хости використовуються для проведення або запуску атак і які характеристики цих атак. Найбільша цінність використання цих каналів полягає в тому, що SIEM-система дозволяє точніше ідентифікувати атаки та приймати більш обґрунтовані рішення, часто автоматично, про те, які атаки необхідно зупинити та який найкращий спосіб їх зупинити. Звичайно, якість розвідки про загрози різниться між постачальниками. Фактори, які слід враховувати під час оцінки розвідки загроз, повинні включати, як часто оновлюється інформація про загрози та як постачальник розвідки загроз показує свою впевненість у зловмисній природі кожної загрози.

12. Рекомендується налаштувати криміналістичні можливості SIEM-системи

Криміналістичні можливості є критеріями оцінки SIEM-систем, що розвиваються. Традиційно SIEM-системи збирають лише дані, надані з інших джерел журналів. Однак нещодавно деякі системи SIEM-системи додали різні криміналістичні можливості, які можуть збирати власні дані щодо підозрілої діяльності. Поширеним прикладом є можливість захоплення повних пакетів для мережевого з’єднання, пов’язаного зі зловмисною діяльністю. Якщо припустити, що ці пакети не зашифровані, аналітик SIEM-системи може уважніше переглянути їх вміст, щоб краще зрозуміти природу пакетів. Іншим аспектом криміналістичної експертизи є протоколювання активності хоста; продукт SIEM може виконувати таке ведення журналу в будь-який час, або журнал може бути запущений, коли

інструмент SIEM-системи відображає підозрілу активність, пов’язану з певним хостом.

13. Необхідно враховувати функції під час аналізу даних

SIEM-системи, які використовуються для виявлення і обробки інцидентів, повинні забезпечувати функції, які допомагають користувачам самостійно переглядати та аналізувати дані журналу, а також власні сповіщення та інші дані, надані SIEM-системою. Однією з причин цього є те, що навіть високоточна SIEM-система іноді неправильно інтерпретує події та генерує помилкові результати, тому людям потрібно мати спосіб підтвердити результати SIEM-системи. Інша причина цього полягає в тому, що користувачам, які займаються аналітикою безпеки, потрібні корисні інтерфейси для полегшення їх розслідування. Приклади таких інтерфейсів включають складні можливості пошуку та можливості візуалізації даних.

14. Необхідно вірно налаштувати автоматизованого реагування SIEM-системи

Іншим критерієм оцінки SIEM-системи є можливості автоматичного реагування продукту. Це часто є завданням окремої організації, оскільки воно сильно залежить від архітектури мережі організації, засобів керування мережевою безпекою та інших аспектів управління безпекою. Наприклад, SIEM-система може не мати можливості направляти брандмауер організації або інші засоби керування мережевою безпекою для припинення зловмисного з’єднання. Крім того, що SIEM-система може повідомляти свої потреби іншим основним елементам контролю безпеки організації, важливо також враховувати наступні характеристики:

Скільки часу потрібно SIEM-системі, щоб виявити атаку та направити відповідні засоби контролю безпеки, щоб її зупинити?

Як захищено зв’язок між SIEM-системою та іншими засобами безпеки, щоб запобігти прослуховуванню та зміні?

Наскільки ефективна SIEM-система у припиненні атак до того, як виникне пошкодження?

15. Необхідно враховувати відповідності вимогам безпеки

Більшість SIEM-систем пропонують можливості звітності, що налаштовуються. Багато з цих продуктів також пропонують вбудовану підтримку для створення звітів, які відповідають вимогам різних ініціатив щодо відповідності вимогам безпеки. Кожна організація повинна визначити, які ініціативи є застосовними, а потім переконатися, що SIEM-система підтримує якомога більше цих ініціатив. Для будь-яких ініціатив, які SIEM-система не підтримує, необхідно переконатися, що SIEM-система підтримує належні параметри звітності, що налаштовуються відповідно до ваших вимог.

Висновки до розділу 3

Розроблено варіант конфігурації системи управління інцидентами в інформаційній системі на базі Wazuh. Наведені приклади налаштування основних функцій, необхідних для управління інцидентами.

Розроблені загальні рекомендації щодо управління інцидентами в інформаційній системі.

ВИСНОВКИ

Метою даної роботи була розробка системи управління інцидентами в сучасній інформаційній системі на базі рішення Wazuh.

В роботі досліджено особливості та завдання управління інцидентами та проаналізовані науково-технічні дані. В результаті було визначено головні проблеми управління інцидентами у сучасних інформаційних системах. Була встановлена необхідність управління інцидентами для забезпечення кібербезпеки інформаційних систем.

Проаналізувавши наявні методи та засоби управління інцидентами були встановлені критерії оцінки програмних комплексів щодо його реалізації.

Були визначені можливості програмного комплексу Wazuh та його основні архітектурні особливості щодо реалізації управління інцидентами. Надані інструкції по базовій конфігурації для інформаційної системи.

Проаналізовано можливості програмного комплексу Wazuh щодо виконання процесу управління інцидентами веб-додатків у сучасному підприємстві.

Розроблено варіант конфігурації програмного комплексу для управління інцидентами, а також показано технологію управління Wazuh на прикладі найпоширеніших проблем щодо реагування на інциденти на сучасних підприємствах.

Розроблено загальні рекомендації щодо забезпечення якісного управління інцидентами в інформаційній системі.

Запропоновано порядок розгортання та налаштування програмного комплексу Wazuh.

ПЕРЕЛІК ПОСИЛАНЬ

1.Корпоративні інформаційні системи [Електронний ресурс] – https://stud.com.ua/33775/informatika/korporativni_informatsiyni_sistemi

2. КОРПОРАТИВНІ ІНФОРМАЦІЙНІ СИСТЕМИ Інформаційні технології автоматизації управління в масштабах корпорації [Електронний ресурс] – https://pidru4niki.com/74260/informatika/korporativni_informatsiyni_sistemi

3.«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ» [Електронний ресурс] – http://www.dut.edu.ua/uploads/p_1739_27992763.pdf

4. ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА:СОЦІОТЕХНІЧНИЙ АСПЕКТ Підручник [Електронний ресурс] – http://www.dut.edu.ua/uploads/p_303_79299367.pdf

5. The Growing Challenges of Threat Detectionand Response[Електронний ресурс] – Режим

доступу: https://symantec-enterprise-blogs.security.com/blogs/feature-stories/growing-challenges-threat-detection-and-response.

6. HIPPA Audit Protocol [Електронний ресурс] – https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

7. Процес управління інцидентами [Електронний ресурс] – https://uk.myservername.com/getting-started-with-incident-tracking

8. Стандарт BSI-100-2У [Електронний ресурс] – https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile.

9. Wazuh SIEM [Електронний ресурс] – https://wazuh.com/

10. Wazuh installation guide [Електронний ресурс] – https://documentation.wazuh.com/current/installation-guide/

11. What is the ELK Stack? [Електронний ресурс] – https://www.elastic.co/what-is/elk-stack

12. What is the Logstash? [Електронний ресурс] – https://dotsandbrackets.com/processing-logs-logstash

13. Lightweight shipper for logs [Електронний ресурс] – https://www.elastic.co/beats/filebeat

14. Wazuh FIM [Електронний ресурс] – https://documentation.wazuh.com/current/index.html

15. ПОСТАНОВА 26.11.2015 № 829 Про затвердження нормативно-правових актів з питань інформаційної безпеки [Електронний ресурс] – https://zakon.rada.gov.ua/laws/show/v0829500-15#Text