МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

«SIEM-система для проведення аудиту подій кібербезпеки на підприємстві»

Завідувач випускаючої кафедри — **Довбиш А.С.**

Керівник роботи — **Кальченко В.В.**

Студентки групи КБ – 71 — **Козлової Д.О.**

СУМИ 2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерних наук

Затверджую_____

Зав. кафедрою Довбиш А.С.

"_____" _____ 2021 р.

ЗАВДАННЯ
до випускної роботи

Студентки четвертого курсу, групи КБ-71 спеціальності "Кібербезпека" денної форми навчання Козлової Дар'ї Олегівни.

Тема: "**SIEM-система для проведення аудиту подій кібербезпеки на підприємстві** "

Затверджена наказом по СумДУ

№_____ від _____ 2021р.

Зміст пояснювальної записки: 1)Аналіз предметної області;

2) Інформаційний огляд SIEM систем; 3) Постановка задачі;

4) Налаштування системи ;

Дата видачі завдання "_____"_____2021 р.

Керівник випускної роботи _____ Кальченко В.В.

Завдання приняв до виконання _____ Козлова Д.О.

РЕФЕРАТ

Записка: 41 сторінка, 28 рисунків, 1 таблиця, 12 джерел.

Об’єкт дослідження — SIEM система для проведення аудиту подій

Мета роботи — дослідити можливість використання SIEM системи для проведення аудиту кібербезпеки на підприємстві

Методи дослідження — реалізація вимог нормативних документів з кібербезпеки, стосовно аудиту подій в комп'ютерних системах.

Результати — проведено інформаційний огляд сучасних SIEM систем, обрано систему для реалізації вимог нормативних документів з кібербезпеки, виконано налаштування серверної та клієнтської частини системи.

SIEM СИСТЕМА, БЕЗПЕКА, АУДИТ, МОНІТОРИНГ, ЗАГРОЗА, ПІДПРИЄМСТВО, МЕРЕЖА, КОМП’ЮТЕР

ЗМІСТ

ВСТУП

Інформація сьогодні є одним із ключових активів будь-якого бізнесу. Сучасні інтернет-технології забезпечують можливості використання цього ресурсу для розвитку і підвищення прибутковості бізнесу. Однак вони ж дають широкий простір для діяльності зловмисників. Це обумовлює високий ступінь уразливості інформаційних систем і мереж.

Сьогоденні кіберзагрози набагато складніші і набагато серйозніші, ніж ми готові собі уявити. Тільки за останні п'ять років світові компанії пережили масштабні кібератаки такі як BlackEnergy, TeleBots, CryptoLocker, GreyEnergy, Industroyer, Petya і NotPetya, BadRabbit, Buhtrap, WannaCry, TeslaCrypt, Nyetya. Вони атакують підприємства критичної інфраструктури, енергетичного сектора, фінансові організації, транспортні та логістичні компанії, медичні та фармакологічні фірми, софтверні компанії. Із цього можна зробити висновок, що жодне підприємство не застраховане повністю від матеріальних чи фінансових втрат. Щоб убезпечити підприємства від таких атак, необхідно об'єктивно оцінити, чи надійно захищена інформаційна система. Для цього проводиться відповідна перевірка.

Аудит інформаційної безпеки - головний інструмент для контролю рівня захисту інформаційних активів. Він дає можливість керівництву та власникам оцінити реальний стан в сфері інформаційної безпеки, виявити вразливі місця та напрямки, отримати уявлення про необхідні заходи для підвищення захищеності. Його результати, за умови професійного виконання, забезпечують можливість побудови комплексної ефективної системи захисту, яка справляється зі своїми завданнями.

Побудова комплексної системи захисту інформації (КСЗІ) на основі результатів аудиту інформаційної безпеки дозволяє мати постійний контроль над системою, відстежувати всі події, модифікації даних та вчасно реагувати на них.

Проведення постійного аудиту безпеки неможливо якісно здійснити без наявності системних журналів. Однак, велика кількість даних для обробки з цих

журналів має і очевидний мінус: нас може просто «засипати» повідомленнями та попередженнями. Тоді перед фахівцями з кібербезпеки на підприємстві постає складне завдання – оптимізувати процес аналізу журналів та записів. Саме для цього були розроблені Security Information and Event Management (SIEM) системи, які стають дуже поширеними в останні роки.

SIEM забезпечує аналіз в реальному часі подій, що відбуваються в інформаційній системі. Подібний аналіз необхідний для виявлення і визначення небезпечних чи незвичних для системи подій безпеки та реагування на них.

На сьогоднішній день, існує велика кількість різноманітних SIEM-рішень від великої кількості розробників, що відрізняються функціоналом, можливими інтеграціями та методами аналізу даних.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Огляд загроз та ризиків комп’ютерних мереж малого підприємства

На теперішній час інформація є одним з найголовніших активів підприємств, який досліджують, як важливий ресурс розвитку суспільства. Глобальне розповсюдження комп’ютерів та пристроїв у багатьох сферах управління та виробництва співіснує з появою нових загроз інтересам підприємств, суспільства та навіть держави.

Водночас зі змінами та ускладненням методів та засобів автоматизації процесів для роботи з інформацією збільшується залежність підприємництва від ступеню безпеки використовуваних ними інформаційних технологій .

Можна виділити чималий перелік джерел, що становлять загрози інформаційній безпеці підприємства:

- незаконна діяльність економічних структур у сфері використання інформації, її поширення та формування;
- порушення встановлених правил обробки, збору та передачі інформації;
- навмисні та ненавмисні дії користувачів інформаційних систем;
- помилки на етапі проектуванні інформаційних систем;
- невідповідність технічних засобів або збої програмного забезпечення в інформаційних системах.

На сьогоднішній день фахівцями з кібербезпеки досліджується досить широкий асортимент загроз безпеці інформаційних систем, які можна класифікувати за рядом ознак (Рисунок 1.1).

Рисунок 1.1- Класифікація загроз безпеці інформаційної системи

Кожна з цих загроз може стати фатальною для підприємства. Витік важливої інформації, особистих даних співробітників чи клієнтів – все це може призвести до великих втрат, а , можливо, і до втрати бізнесу [1] .

1.2. Аналіз сучасного шкідливого програмного забезпечення

Програмне забезпечення - це сукупність програм, призначених для вирішення проблем на комп'ютері. Програма - це впорядкований набір команд. Програмне і апаратне забезпечення працюють в постійній взаємодії. Але не завжди програмне забезпечення працює на користь підприємства. Дуже часто це шкідливе програмне забезпечення.

Термін «шкідливе програмне забезпечення», «зловмисне програмне забезпечення», означає набір команд, який незаконно впроваджується у

комп’ютерну систему та може спричинити порушення безпеки, пошкодити інформаційні ресурси, та в деяких випадках ще й ресурси комп'ютерного обладнання [2].

Розглянемо основні типи загрозливих програм. Вони поділяються на класи за такими основними характеристиками (Рисунок 1.2) .

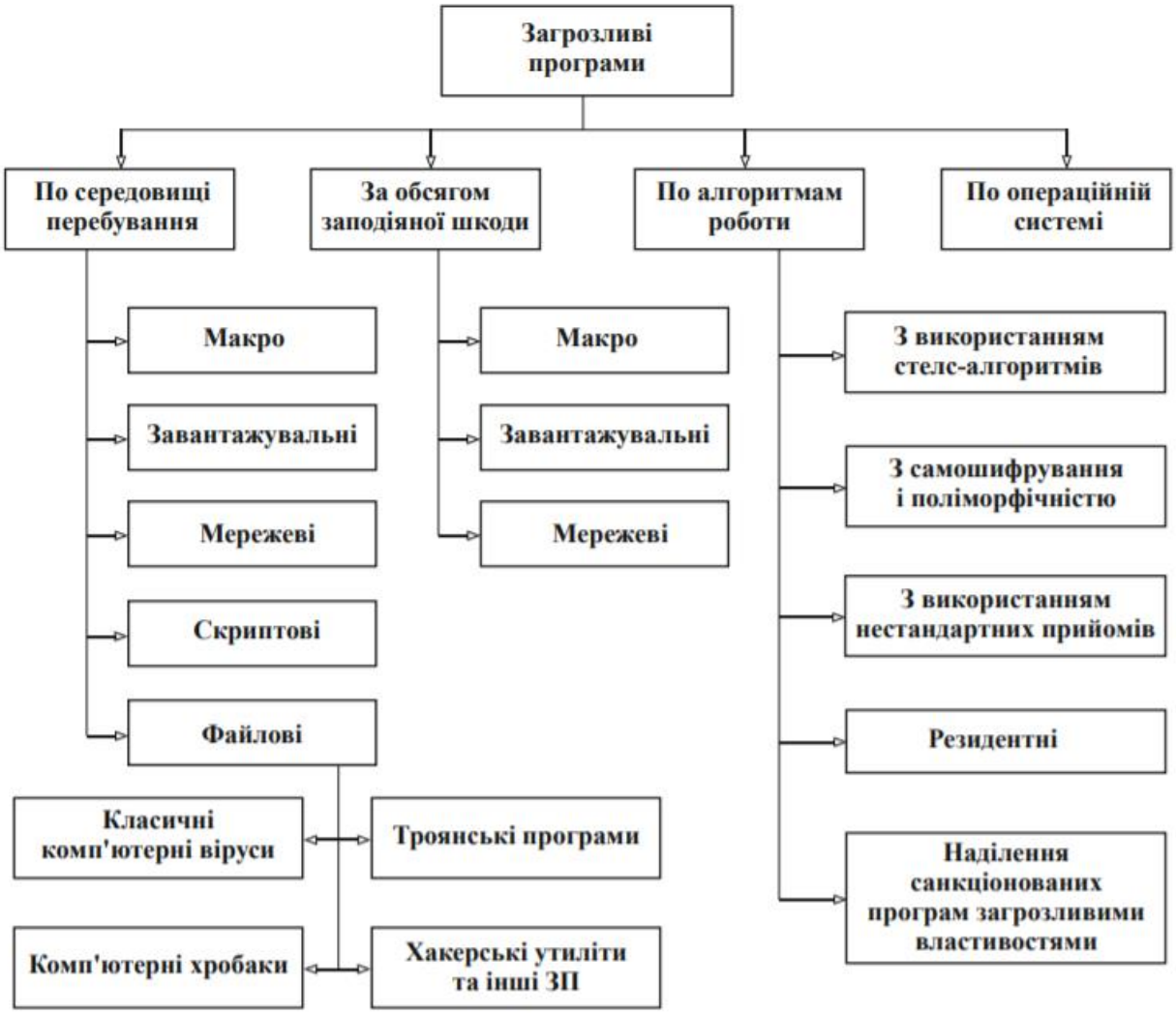

Рисунок 1.2 - Класифікація загрозливих програм

До шкідливого програмного забезпечення належать:

1) люки (точка входу до програми, яка дозволяє зловмиснику отримати доступ до програми за допомогою незвичайних процедур);

2) логічні бомби (код, що поміщається в звичайну програму; який що при певних умовах виконує незаконні дії; умовою для включення логічної бомби може бути модифікація або взагалі відсутність деяких файлів, певний день тижня або дата, а також запуск додатку особливим користувачем)

3) троянські коні (програма, в якій приховано код, здатний в разі спрацьовування виконати деяку небажану або шкідливу функцію.);

4) віруси (код. який може заражати інші програми, модифікуючи їх та роблячи здатними заражати інші програми самостійно);

5) черв'яки (програма, яка розповсюджується через мережу і не залишає своєї копії на магнітному носії, розповсюджується по мережі і чекає сприятливих умов для активізації);

6) зомбі (програма, яка приховано під'єднується до інших комп'ютерів мережі , а потім використовує їх для запуску атак, що ускладнює відстеження шляхів до розробника програми-зомбі);

7) програми-крадії паролів.

З цього можна зробити висновок, що шкідливе програмне забезпечення може бути присутнім на пристроях комп'ютерної мережі, а власники навіть не підозрювати про це.

1.3. Аналіз методів проникнення до комп'ютерних мереж

Зараз, коли майже кожен співробітник будь-якого підприємства потребує особистого комп'ютера та виходу в інтернет, дуже корисно відстежувати дії кожного користувача. Іноді трапляється так, що в системі виконуються дії, які не санкціоновані для якогось користувача, а він навіть не здогадується про них. Тоді ми можемо говорити про проникнення до мережі. Виділяють 3 групи проникнень до мережі підприємства за способом їх вчинення:

1) способи безпосереднього доступу. До таких відносяться злочини, при яких інформація модифікується, знищується або блокується. Також може бути виведено з ладу цілий пристрій. Такий доступ до інформації мають

співробітники та особи, що працюють з нею, або особи, що незаконно проникають у приміщення, де здійснюється опрацювання інформації. Такий спосіб у наш час стає менш поширеним через підсилення безпеки приміщень та можливості відстежувати дії кожного користувача;

2) способи віддаленого доступу. До таких можна віднести підключення до лінії зв'язку законного користувача системи та перехоплення інформації, перебирання паролів та електронний злом, який здійснюється через комп'ютерну мережу;

3) змішані способи. Це комбінація першого та другого типу. До них відносять підміну даних, таємне введення в чужу машину команд, що допомагають здійснювати незаплановані дії (троянський кінь), використання помилок у логіці побудови програм і виявлення таких уразливих місць та інше.

Зазвичай зловмисники використовують спеціальне обладнання. Наприклад, для безпосереднього доступу можуть буди використані лазерні диски, різноманітні накопичувачі, електронні ключі, особисті коди ідентифікації в системі; для віддаленого доступу – засоби супутникового або телефонного зв'язку, модеми.

Роблячи висновок, можна сказати, що небезпека може чекати підприємство як від власних співробітників, так і від сторонніх осіб [2] .

1.4. Постановка задачі

Для того, щоб інформація в системі перебувала у безпечному стані, запроваджуються комплексні системи захисту інформації для моніторингу подій.

В Україні комплексні системи захисту інформації будуються на основі Постанови Кабінету Міністрів України №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [3] .

Згідно з постановою, для кожного користувача в системі мають існувати правила доступу до службової, таємної та відкритої інформації; кожен користувач має бути ідентифікований в системі, у системі здійснюється обов’язкова реєстрація, кожна дія користувача в системі має бути визначена, має бути можливість перегляду спроб несанкціонованих дій з інформацією та інше. Тобто система, побудована на Постанові №373, повинна зберігати та обробляти велику кількість інформації про внутрішні події в системі для недопущення витоку чи модифікації інформації, що не є відкритою.

Для вирішення цього питання ми скористаємося Security Information and Event Management системою, зробимо необхідні налаштування та перевіримо її працездатність. Результатом має бути відповідь на питання: чи може Security Information and Event Management система бути використана для проведення аудити кібербезпеки на підприємстві?

2 ОГЛЯД SIEM СИСТЕМ

2.1. SIEM система та принцип її роботи

Security Information and Event Management (SIEM) – це система, яка збирає інформацію для подальшого аналізу і класифікації системним адміністратором або фахівцем з інформаційної безпеки.

Спочатку SIEM складалося з двох напрямків:

- Security Information Management (SIM) - перше покоління, побудоване на основі традиційних систем збору та управління журналами. SIM впровадила довгострокове зберігання, аналіз та звітування про дані журналів, а також поєднала журнали з інформацією про загрози.
- Security Event Management (SEM) - друге покоління, що стосується подій безпеки - агрегування, кореляція та повідомлення про події із систем безпеки, таких як антивірус, брандмауери та системи виявлення вторгнень (IDS), а також про події, про які повідомляється безпосередньо шляхом автентифікації, SNMP-пастки сервери, бази даних та інше.

У 2005 році відбулося об'єднання і з'явилося спільне поняття Security Information and Event Management [4] .

Дані для SIEM надходять з різних джерел. До них відносяться: журнали подій, які реєструються операційною системою або стороннім додатком; мережеве обладнання (маршрутизатори, проксі-сервери, шлюзи і т. д.), міжмережеві екрани (firewall), сканери вразливостей (спеціальне програмне забезпечення, яке знаходить уразливості всередині інфраструктури), CRM-системи (зберігають інформацію про клієнтів в одному місці, реєстрація проблем обслуговування та інше), робочі станції користувачів, антивірусне програмне забезпечення, інші ресурси, які реєструють події і здатні передавати їх через агентів або вбудованими засобами.

SIEM системи були введені десь близько 2000 року. Системи на цьому початковому етапі (з 2000 по 2005 рік) забезпечували базову агрегацію журналів

між різними типами систем, а також основні методи кореляції подій. Для виявлення нападу ці системи покладалися лише на відомі атаки загроз. Отже, вони були абсолютно не в змозі мати справу з атаками нульових днів на системи підприємств. Інші обмеження систем протягом цього періоду включали:

- Перші системи були розроблені на основі IP-адрес, а не користувачів. Завдяки динамічному розподілу IP-адрес та швидкому збільшенню кількості мобільних пристроїв, ідентифікація пристрою за його IP-адресою була фактично неможлива, оскільки одна IP-адреса фіксувала кілька пристроїв протягом дня.
- Традиційні системи використовують методи, що були засновані на правилах, для встановлення кореляції між різними подіями безпеки. Отже, оновлення сотень правил у режимі реального часу не лише забирає час, але й призводить до неоптимального використання ресурсів.

Принцип роботи SIEM системи можна пояснити наступними пунктами:

1. Збір даних. Більшість рішень SIEM збирають дані з інформаційної системи підприємства за допомогою агентів, встановлених на різних пристроях, включаючи кінцеві точки, сервери та мережеве обладнання, а також інших рішень безпеки, таких як брандмауери або інші пристрої захисту мережі. Рішення SIEM останнього покоління включають підтримку хмарних додатків та інфраструктури, корпоративних програм.

2. Розширення даних. Розширення даних додає контексту події. Рішення SIEM повинні збагачувати вхідні дані ідентифікацією, активами, геолокацією та інформацією про загрози, щоб допомогти у розслідуваннях. Розширення даних заповнює важливу інформацію, необхідну SIEM, щоб поєднати пов'язані події разом та допомогти у виявленні загроз.

3. Зберігання даних. Після розширення дані безпеки зберігаються в базі даних. Там їх можна шукати та посилатися на них під час розслідування. Частіше зберігаються лише дані з розширеною інформацією, але іноді зберігаються всі. Все залежить від того, що вимагає підприємство. Останнє покоління SIEM

використовує архітектуру великих даних з відкритим кодом, щоб скористатися їх необмеженою масштабованістю та можливістю зберігати історичні дані таким чином, щоб їх можна було легко шукати.

4. Застосування кореляції та аналітики. Рішення SIEM використовують різні методи, щоб зробити корисні висновки з даних та знайти аномалії. Ці методи аналітики різняться в залежності від виробника. Перші SIEM покладалися на просту кореляцію та попередження на основі підпису. Вони схильні до помилок, видають багато зайвого у вигляді помилкових спрацьовувань і можуть знаходити лише відомі загрози. Наступне покоління SIEM використовує передові аналітичні методи, крім підходів, заснованих на підписах, для виявлення відомих і невідомих загроз. Вони використовують складні алгоритми машинного навчання для точнішого виявлення загроз (поведінкова аналітика користувачів та сутності (UEBA) та інші).

5. Аналіз загроз. На базовому рівні SIEM повинна мати можливість інтегруватися зі стороннім рішенням організації, автоматизації та реагування на безпеку (SOAR - Security Orchestration, Automation and Response), щоб допомогти аналітикам у процесі розслідування та усунення потенційних загроз. Рішення SOAR надає аналітикам простір для збору інформації, відстеження кроків, здійснених під час розслідування, та запам'ятовування того, як загроза була усунена.

6. Надання статистики даних та звітування. SIEM дає можливість швидко здійснювати пошук у даних, дозволяючи заглиблюватися в попередження та шукати учасників. Візуалізовані дані можна зберегти як інформаційні панелі або експортувати у стандартному форматі даних. Є можливість використовувати готові звіти або створювати спеціальні звіти, якщо це потрібно [5] .

2.2. Основні виробники SIEM систем на ринку продуктів

Оскільки все більше керівників підприємств приходять до розуміння необхідності ретельного підходу до інформаційної безпеки, ринок SIEM-систем активно розвивається, а кількість представлених рішень стабільно розширюється. Далі стислий огляд найпоширеніших представників SIEM систем міжнародного ринку.

2.3. IBM QRadar Security Intelligence

Компанія IBM для захисту від загроз мережевої безпеки пропонує рішення IBM QRadar Security Intelligence Platform, яка надає спільну архітектуру для інтегрування інформації про безпеку та управління подіями і журналами, визначення аномальних ситуацій, аналізу інцидентів, реагування на них, управління конфігураціями та усунення вразливостей .

Єдина архітектура QRadar Security Intelligence Platform дозволяє аналізувати журнали, мережеві потоки, пакети, уразливості, а також дані про користувачів і ресурси. Використання Sense Analytics дає можливість проводити аналіз кореляції для виявлення найбільш серйозних загроз, атак і вразливостей в реальному часі. Це дає можливість IT-відділам розставити пріоритети і виділяти найважливіші інциденти з величезного потоку даних. Рішення автоматично реагує на інциденти і виконує нормативні вимоги за рахунок можливостей збору даних, визначення їх кореляції і складання звітності. Також передбачений аналіз наявних ризиків, викликаних некоректними конфігураціями пристроїв і відомими уразливими.

IBM QRadar Security Intelligence Platform включає в себе цілий ряд різних модулів. Одним з ключових компонентів рішення є інструмент IBM QRadar SIEM - система збору та аналізу подій. Він консолідує інформацію з журналів подій, що надходить від пристроїв, кінцевих точок і додатків в мережі. QRadar SIEM нормалізує і аналізує кореляцію для виявлення загроз безпеки, а також використовує передовий механізм Sense Analytics для виявлення нормальної

поведінки, виявлення аномалій, розкриття передових загроз. Цей програмний модуль дає можливість зібрати всі пов'язані події в один інцидент.

Можливість створювати докладні звіти щодо доступу до даних і дій користувачів забезпечує більш ефективне управління погрозами і відповідність стандартам. Варто також згадати, що QRadar SIEM можна використовувати в локальних і хмарних середовищах.

Крім того, варто відзначити, що в найближчим часом IBM планує використовувати платформу штучного інтелекту Watson в сфері безпеки, інтегрувавши її з програмним забезпеченням QRadar і базою даних X-Force. Це дозволить підвищити рівень аналітики для визначення характеру загроз, а також компенсувати брак IT-персоналу в сфері інформаційної безпеки.

З інструментом QRadar SIEM інтегрується перелік модулів, що підвищують його ефективність. Одним з найбільш важливих є QRadar Risk Manager, який зіставляє відомості про уразливість з даними про топологію мережі і з'єднаннях. Рішення знаходить уразливості в мережі підприємства і працюючих додатках, оцінивши ризики і мінімізувавши їх. Risk Manager відстежує конфігурацію маршрутизаторів, комутаторів, мережевих екранів і систем запобігання вторгнень, знаходячи умови, що представляють загрозу безпеці. Крім того, він дозволяє моделювати мережеві атаки та інші варіанти вторгнень, вносячи в конфігурацію мережі зміни, які дають можливість оцінити масштаб загрози.

Ще один цікавий інструмент - модуль QRadar Log Manager. Він збирає і обробляє дані про події в режимі реального часу, що надходять від маршрутизаторів, брандмауерів, комутаторів, мереж VPN, систем виявлення і запобігання вторгнень та інших джерел. Log Manager дає можливість спростити ведення необхідної звітності та контроль за дотриманням нормативно-правових вимог.

IBM QRadar SIEM є однією з найбільш ефективних аналітичних систем безпеки. Важливим є той факт, що рішення підтримує роботу з більш ніж 200

продуктами від провідних виробників і проводить збір, аналіз і кореляцію даних через широкий спектр систем, включаючи мережеві рішення, засоби безпеки, сервери, хости, операційні системи і додатки. Крім того, додатковою перевагою рішення є невисока вартість системи початкового рівня [7] .

2.4. Splunk Enterprise Security

Splunk Enterprise Security - система управління інформаційною безпекою та подіями, яка формує детальну картину машинних даних, що створюються різними технологіями безпеки (мережа, кінцеві точки, доступ, шкідливі програми, вразливість). Завдяки Splunk Enterprise Security фахівці з безпеки можуть швидко виявляти внутрішні і зовнішні атаки і приймати відповідні заходи. Це дозволяє спростити операції щодо захисту від загроз, мінімізувати ризик і забезпечити безпеку бізнесу. Splunk Enterprise Security оптимізує всі аспекти захисту та підходить для організацій будь-якого масштабу і професійного рівня.

Продукт складається з декількох модулів, які відповідають за проведення розслідувань та інтеграцію з безліччю зовнішніх сервісів. Такий підхід дає можливість проводити детальний аналіз за багатьма параметрами і встановлювати взаємозв'язок між подіями, які, на перший погляд, ніяк не співвідносяться один з одним. Splunk Enterprise Security дозволяє зіставляти дані по часу, розташуванню, створюваним запитам, підключенням до різноманітних систем та іншим параметрам.

Splunk User Behavior Analytics (Splunk UBA) допомагає підприємствам знаходити приховані загрози і аномальну поведінку користувачів, пристроїв і додатків за допомогою алгоритмів машинного самонавчання, аналітики базових ліній поведінки користувачів і тимчасових груп. Таким чином організації можуть виявляти постійні погрози підвищеної складності, зараження шкідливими програмами і внутрішні загрози. Splunk UBA забезпечує робочі процеси

аналітиків і розробників процедур безпеки, вимагає мінімум від адміністрування та інтегрується з існуючою інфраструктурою для виявлення прихованих загроз.

Інструмент також вміє працювати з великими масивами даних, які можуть оброблятися як в реальному часі, так і в режимі історичного пошуку, причому підтримується велика кількість джерел даних. Splunk Enterprise Security може індексувати сотні терабайт даних в день, тому його можна застосовувати в корпоративних мережах навіть дуже великих масштабів. Спеціальний інструмент MapReduce дозволяє швидко масштабувати систему і рівномірно розподіляти навантаження, завдяки чому продуктивність системи завжди залишається на прийнятному рівні. При цьому користувачам доступні конфігурації для кластеризації і аварійного відновлення [8] .

2.5. McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (ESM) – рішення в сімействі систем управління інформацією та подіями безпеки від компанії McAfee - відрізняється високою продуктивністю, надає інформацію для прийняття необхідних заходів і забезпечує інформацією про ситуацію в режимі реального часу. Швидкодія і масштаб цього рішення дозволяють фахівцям з безпеки виявляти, аналізувати і знешкоджувати приховані загрози, в той час як вбудована структура забезпечення нормативно-правової відповідності спрощує контроль за дотриманням вимог.

Рішення від компанії McAfee інтегрується як в якості фізичних і віртуальних пристроїв, а також програмного забезпечення. Воно складається з декількох модулів, які можуть застосовуватися як разом, так і окремо. Enterprise Security Manager забезпечує постійний моніторинг корпоративної IT-інфраструктури, збирає інформацію про загрози та ризики, дозволяє пріоритезувати загрози і швидко проводити розслідування. Для всієї інформації, що надходить, система розраховує базовий рівень активності і заздалегідь створює повідомлення, які надійдуть адміністратору, якщо рамки даної

активності будуть порушені. Також засіб вміє працювати з контекстом повідомлень, що значно розширює можливості аналізу і виявлення загроз, а також знижує кількість хибних сигналів.

McAfee ESM добре інтегрується з продуктами сторонніх виробників без використання API, що робить його сумісним з багатьма іншими популярними рішеннями в області безпеки. Також у нього є підтримка платформи McAfee Global Threat Intelligence, яка розширює традиційну функціональність SIEM. Завдяки їй, ESM отримує постійно оновлювану інформацію про загрози з усього світу. На практиці це дає, наприклад, можливість виявляти події пов'язані з підозрілими IP-адресами.

- Продукт складається з наступних компонентів, частина з яких обов'язкова. Рекомендовані до використання, щоб скористатися всім функціоналом McAfee SIEM:McAfee Enterprise Security Manager - основний компонент системи (обов'язковий);
- McAfee Event Receiver - збір і нормалізація сирих подій (обов'язковий);
- McAfee Enterprise Log Manager - зберігання сирих подій (рекомендований);
- McAfee Enterprise Log Search - пошук по сирим подій (опціональний);
- McAfee Advanced Correlation Engine (McAfee ACE) - додаткові можливості по кореляції подій (рекомендований);
- McAfee Application Data Monitor - моніторинг даних 7-го рівня OSI для виявлення загроз на рівні додатків (опціональний).

McAfee ESM надає інфраструктуру кореляції, яка дозволяє визначити значення кожної конкретної події, розмішуючи її в контекст, тобто показуючи хто, що, де, коли та чому зумовило появу даної події, це допомагає виявити вплив події на бізнес-ризик. Засоби кореляції забезпечують точну автоматичну

пріоритезацію загроз безпеки й порушень відповідності вимогам, показуючи події у відповідному бізнес-контексті.

При цьому для того, щоб така система забезпечувала ефективне виявлення інцидентів, швидке реагування та відсутність помилкових спрацьовувань, вона повинна бути налаштована відповідно до наявних в компанії бізнес-процесами та IT-інфраструктурою [9] .

2.6. Порівняльний аналіз сучасних SIEM систем

Порівняльний аналіз наведених вище систем представлено у Таблиця .

Таблиця 2.1 - Порівняльний аналіз SIEM систем

Критерій оцінки	**IBM Radar**	**Splunk**	**McAfee ESM**
Цільовий сегмент	Банківський, державний сектори, великий і середній бізнес	Всі сегменти у всіх галузях, від безкоштовних версій до найбільших інсталяцій	Державний сектор, великий і середній бізнес
Мови інтерфейсу	Російська, англійська	Російська, англійська	Англійська
Шляхи експлуатації інцидентів	Вручну	Автоматично настроюється ескалація на SOAR і інші засоби реагування через механізм модульних сповіщень Alerts. Ручна ескалація через Workflow Actions в картці інциденту	Ескалація вручну або при формуванні автоматичного оповіщення

Продовження таблиці 2.1

Прийняття рішень в рамках процесу обробки інцидентів	Ручне та автоматичне	Ручне	Ручне та автоматичне
Наявність встановлених графічних панелей (Dashboards)	7. Додатково з AppExchange може бути встановлено додаток візуалізації IBM QRadar Pulse	57	Понад 100 (поєднане зі звітами)
Наявність встановлених звітів	Більше 110, а також Content Extention Pack з IBM X-Force App Exchange	462	Більше 100
Операційна система в основі рішення	Red Hat Enterprise Linux	Linux з ядром 2.6+, Windows Server 2008 R2 і вище	Customized Mcafee linux

Продовження таблиці 2.1

Наявність сформованих образів для платформ віртуалізації	VMware, AWS	VMWare, AZURE, AWS, Docker Hub	VMware, KVM, AWS
Налаштування власної моделі визначення критичності уразливості	Ні	Так	Можна впливати на параметри критичності, використовуючи мітки Assets. Вплив на параметр ризику можливо з ризик-кореляції на базі правил
Можливість формування звітів у вигляді документів, формати експорту звітів	PDF, HTML, RTF, XML, XLS	Raw, PDF, CSV, XML, JSON	PDF, HTML, CSV

Отже, проглянувши порівняльний аналіз ми можемо зробити висновок, що система кожного виробника має свої особливості та переваги.

3 ПРАКТИЧНА ЧАСТИНА

3.1. Вибір методів розв’язання задачі

Сьогодні перед фахівцями інформаційної системи стає питання реалізації безпечного інформаційного середовища для підприємства. Щоб в будь-який момент часу мати змогу оцінити захищеність системи, треба обробляти велику кількість джерел, щоб зробити висновки.

Для того, щоб продемонструвати можливості SIEM системи мною було обрано AlienVault OSSIM, тому що система є безкоштовною та має досить широкий перелік можливостей для побудови надійної системи моніторингу.

AlienVault OSSIM (Open Source Security Information and Event Management) - це open-source версія AlienVault, однієї з лідируючих комерційних SIEM-систем. OSSIM - це фреймворк, що складається з декількох проектів з відкритим вихідним кодом, включаючи мережну систему виявлення вторгнень Snort, систему моніторингу мереж і вузлів Nagios, хостовую систему виявлення вторгнень OSSEC і сканер вразливостей OpenVAS.

Система побудована на стеку ElasticStack (Elasticsearch, Logstash, Kibana) і підтримує як збір даних на основі агентів, так і прийом системних журналів. Це робить її ефективною для моніторингу пристроїв, які генерують журнали, але не підтримують установку агента - мережеві пристрої, принтери і периферійних [6].

Також дуже зручним є EventLog Analyzer. За допомогою цього інструмента ви можете автоматизувати весь процес управління терабайтами генерованих пристроями журналів, збираючи, аналізуючи,, шукаючи, звітуючи та архівуючи з однієї централізованої консолі. Це програмне забезпечення допомагає контролювати цілісність файлів, проводити аналіз журналів, відстежувати привілейованих користувачів та відповідати різним регуляторним органам з питань відповідності. Це робиться за допомогою аналізу журналів, щоб миттєво генерувати низку звітів .

3.2. Розгортання AlienVault OSSIM

Встановленнясистеми здійснюється за допомогою готового інсталяційного образу, що містить в собі операційну систему Debian і всі необхідні встановлені компоненти і модулі.

3.2.1. Розгортання та налагодження серверної частини

Спочатку було завантажено останню версії дистрибутива OSSIM та встановлено VirtualBox на свій персональний комп'ютер. Віртуальна машина (ВМ), що буде створена під час роботи, буде виконувати роль віртуального сервера.

Створюємо віртуальну машину із представленими параметрами (Рисунок 3.1 та Рисунок 3.2)

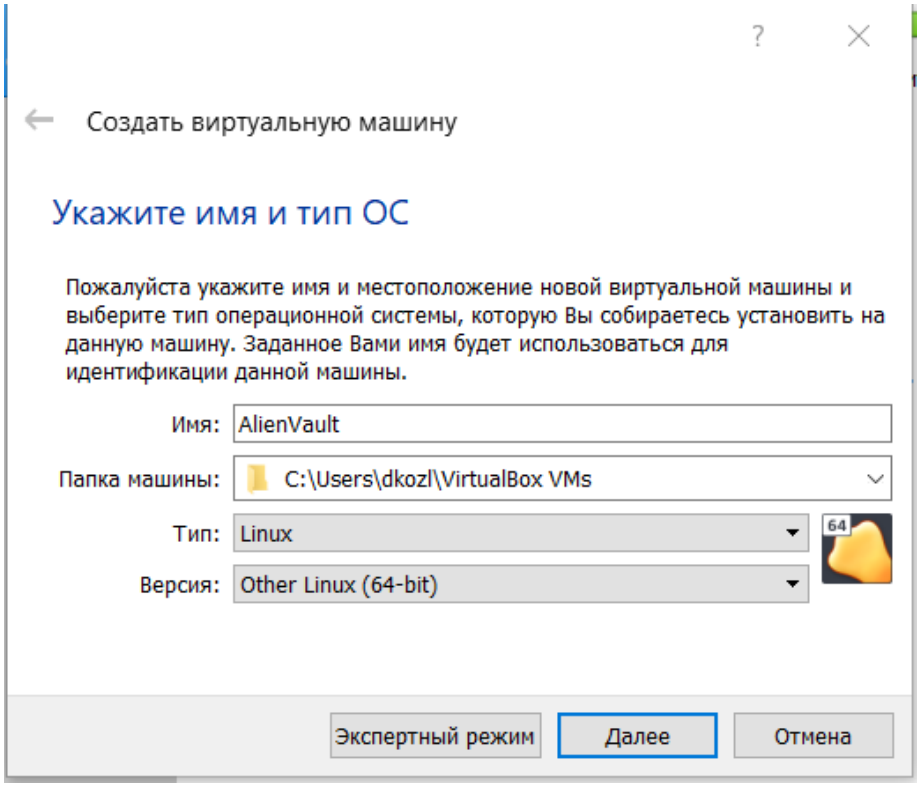

Рисунок 3.1 - Назва та тип операційної системи

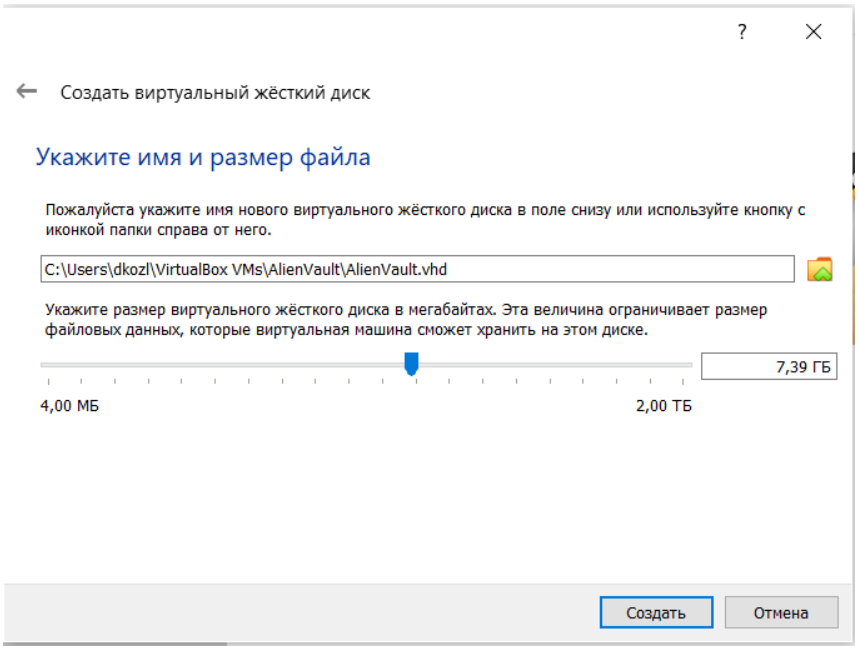

Рисунок 3.2 - Назва файлу майбутньої ВМ та розмір віртуального диску

Після успішного створення и запуску ВМ треба обрати завантажувальний диск (мені довелося вмонтувати образ диску за допомогою програми DAEMON Tools Lite, тому це диск E:) (Рисунок 3.3).

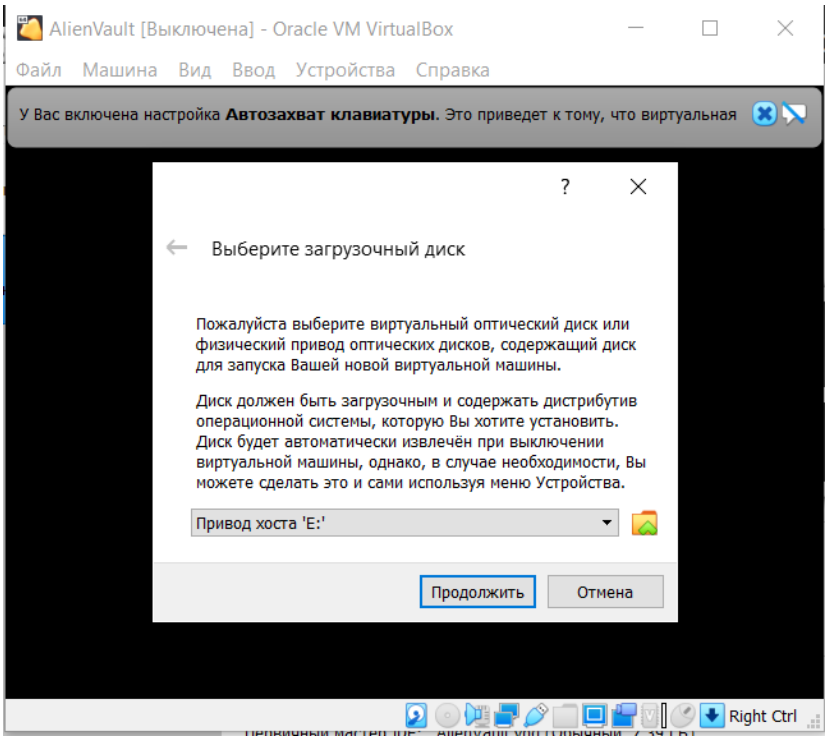

Рисунок 3.3 - Вибір навантажувального диску

Далі обираємо перший варіант встановлення, який не відрізняється від встановлення Debian (Рисунок 3.4).

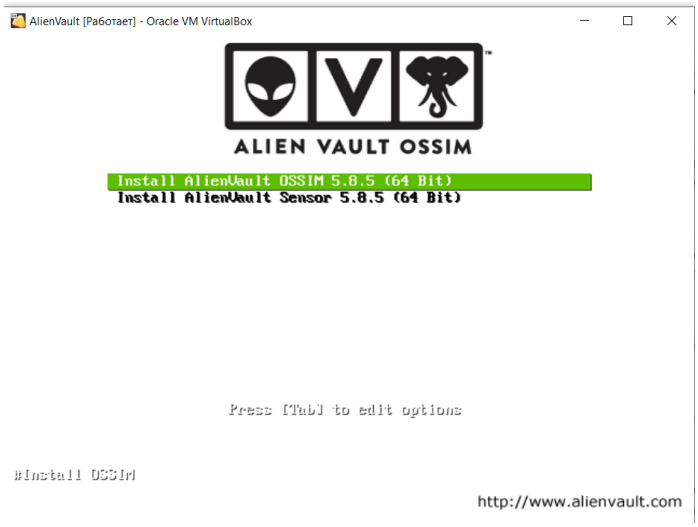

Рисунок 3.4 - Вибір варіанту встановлення

Обираємо мову та чекаємо повного завантаження.

Починаємо конфігурацію мережі. Вводимо IP, який буде використовуватися для входу через браузер. У моєму випадку це 192.168.1.150 (Рисунок 3.5)

Рисунок 3.5 - Визначення IP для SIEM системи

Після цього так само прописуємо маску підмережі – 255.255.255.0.

Після цих дій конфігурацію ВМ завершено.

Нам залишається лише авторизуватися та спробувати через браузер потрапити на наш віртуальний сервер (Рисунок 3.6 та Рисунок 3.7).

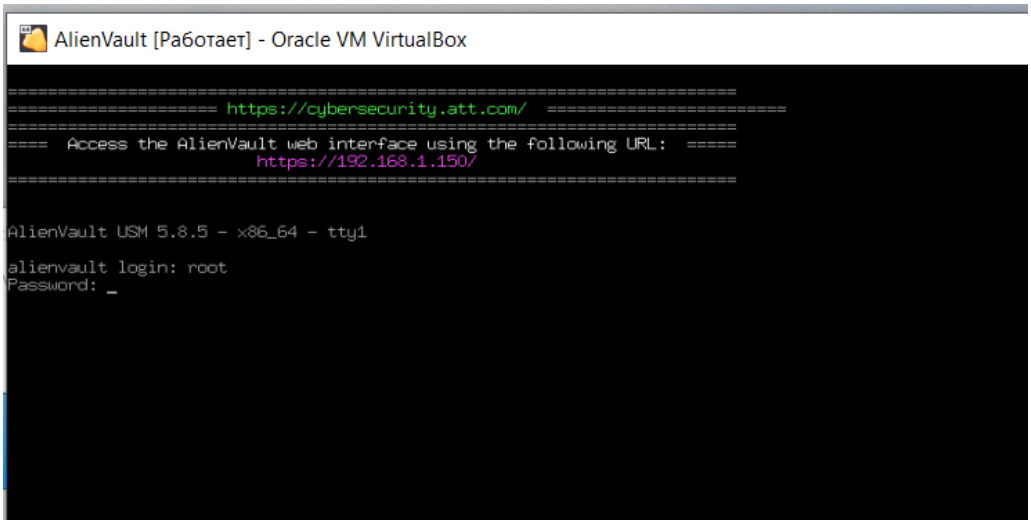

Рисунок 3.6 - Авторизація в системі через консоль

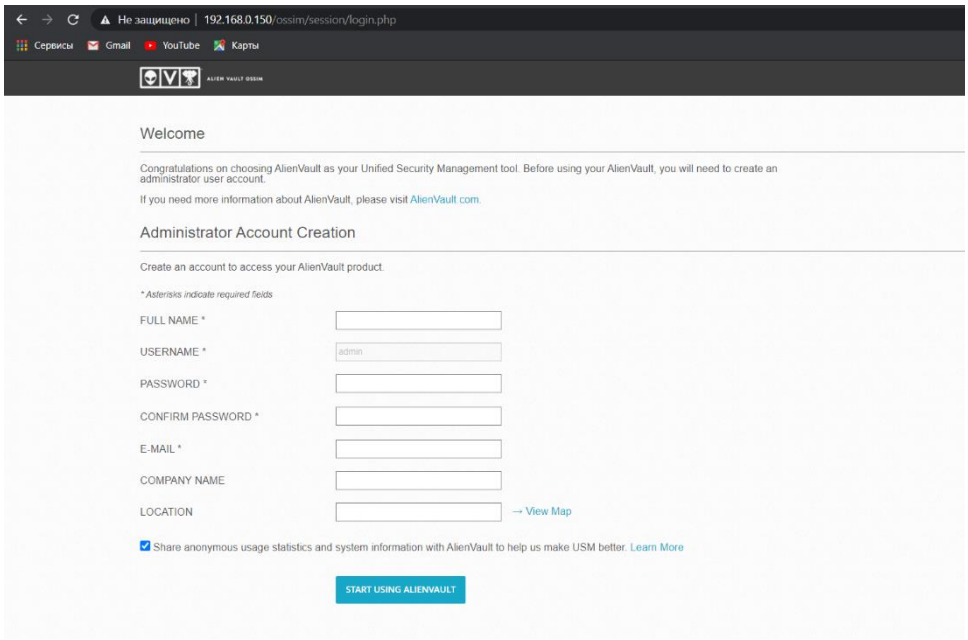

Рисунок 3.7 - Налаштування адмін-користувача через веб-сторінку

3.2.2. Розгортання клієнтської частини

Для того, щоб побачити як працює наша система, ми продовжуємо налаштування через веб-інтерфейс і додаємо мій локальний ноутбук до конфігурації. Для цього скануємо мережу 192.168.0.0/16, в якій знаходиться наша система та ноутбук (Рисунок 3.8).

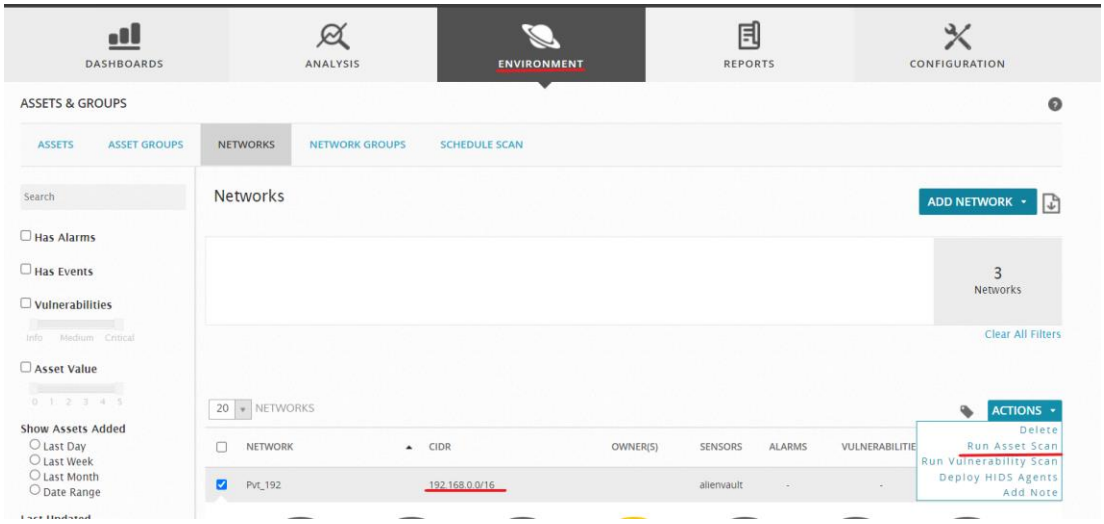

Рисунок 3.8 - Сканування локальної мережі

Отримуємо список пристроїв, що знаходяться в одній мережі (Рисунок 3.9).

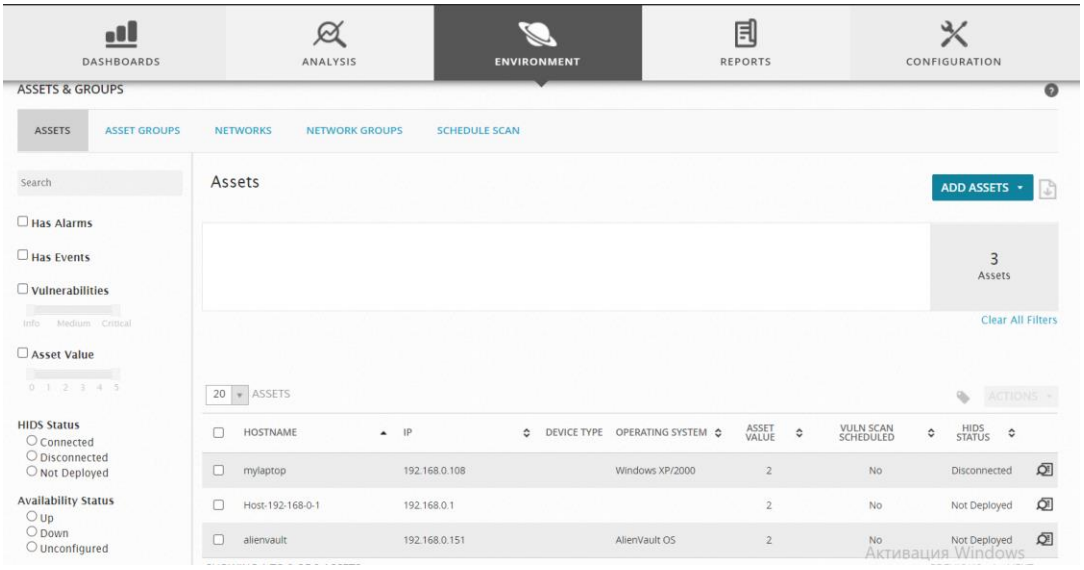

Рисунок 3.9 - Список локальних пристроїв

Як ми можемо побачити, наша система вже почала збирати інформацію щодо потрібного хосту (Рисунок 3.10).

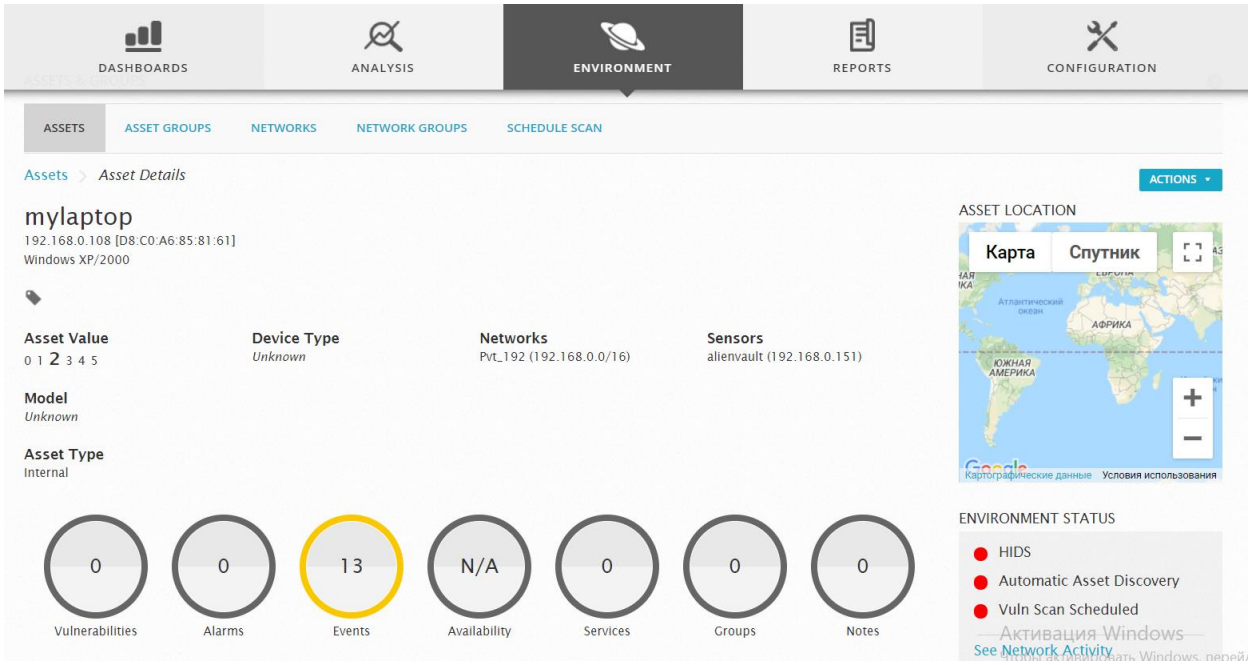

Рисунок 3.10 - Інформація, що була зібрана під час сканування мережі

Надалі ми можемо використовувати веб-інтерфейс для подальшого моніторингу та отримання необхідної інформації.

Dashboards - показує повне уявлення про всі компоненти сервера OSSIM, таких як серйозність загрози, вразливості в мережевому вузлі, стан розгортання, карти ризиків і статистика (Рисунок 3.11).

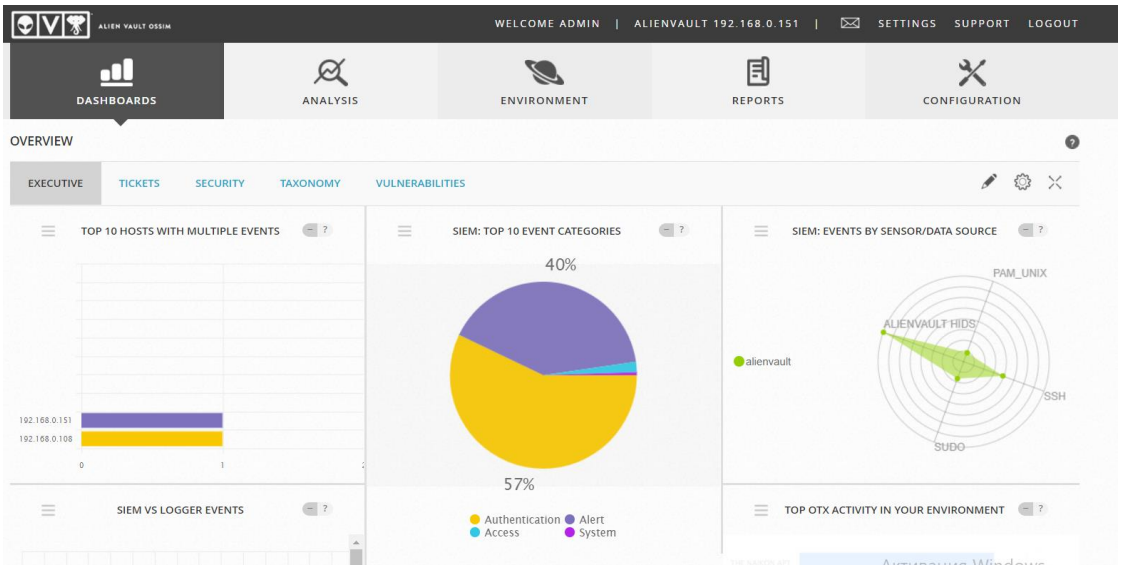

Рисунок 3.11 - Вкладка Dashboards

Analysis - є дуже важливою складовою будь-якого пристрою SIEM. Сервер OSSIM проаналізує хости на основі їх логів. Це меню показує сигнали тривоги, SIEM (події безпеки), тікети і необроблені логи (Рисунок 3.12).

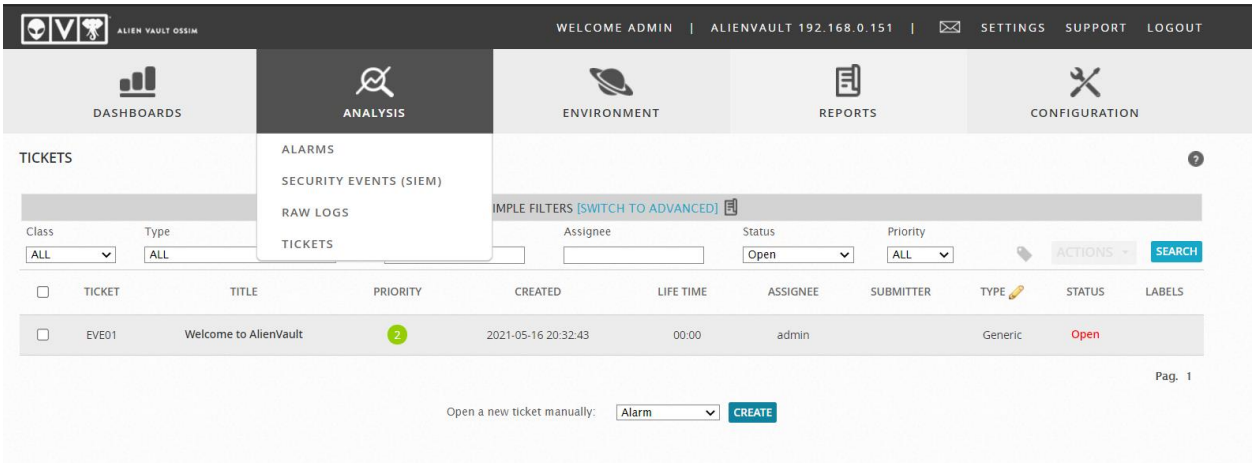

Рисунок 3.12 - Вкладка Analysis

Environment - у цьому меню сервера OSSIM настройки пов'язані з пристроями організації. Воно показує пристрої, групу і мережу, уразливості, мережевий потік і налаштування виявлення (Рисунок 3.13).

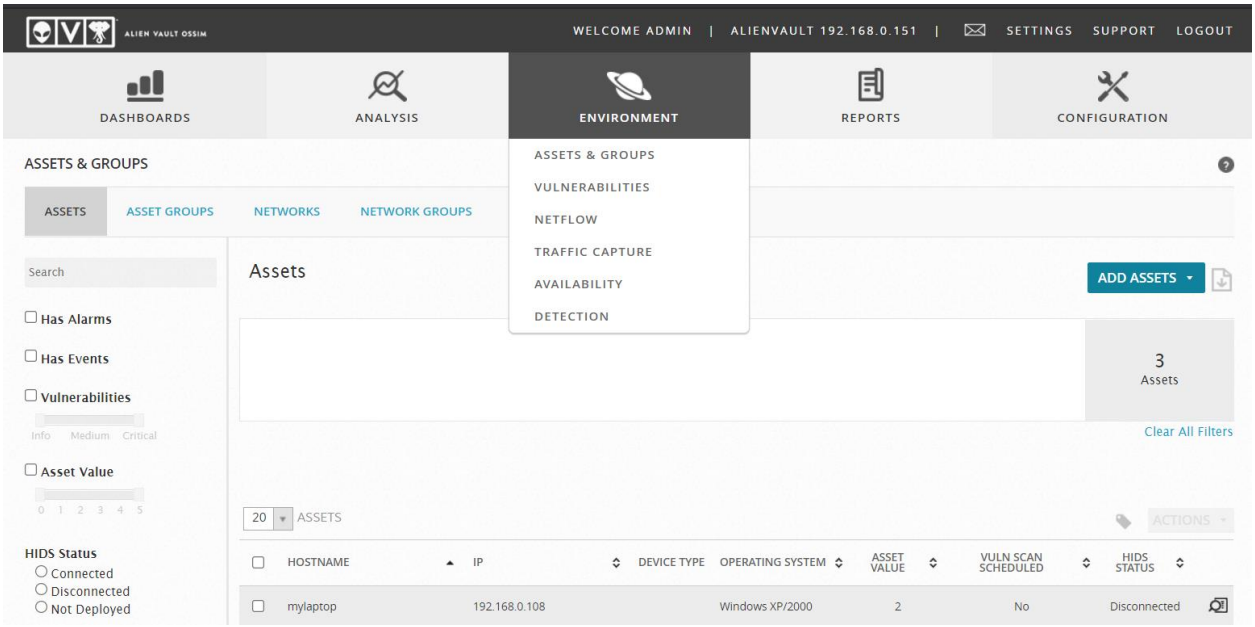

Рисунок 2 - Вкладка Environment

Reports - звітність є важливим компонентом будь-якого сервера реєстрації. Сервер OSSIM також генерує звіти, які дуже корисні для детального дослідження будь-якого конкретного хоста (Рисунок 3.14).

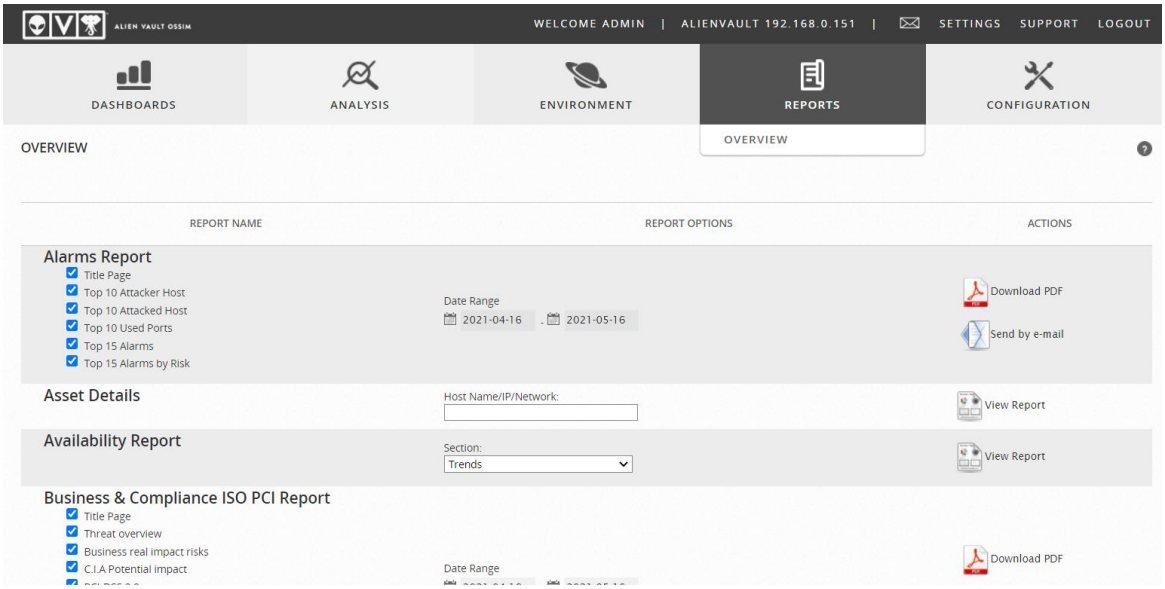

Рисунок 3.14 - Вкладка Reports

Configuration - для установки і настройки AlienVault SIEM (OSSIM) користувач може змінити налаштування сервера OSSIM, наприклад, змінити IP-адресу інтерфейсу управління, додати додатковий хост для моніторингу і логування, а також додати / видалити різні датчики або плагіни (Рисунок 3.15).

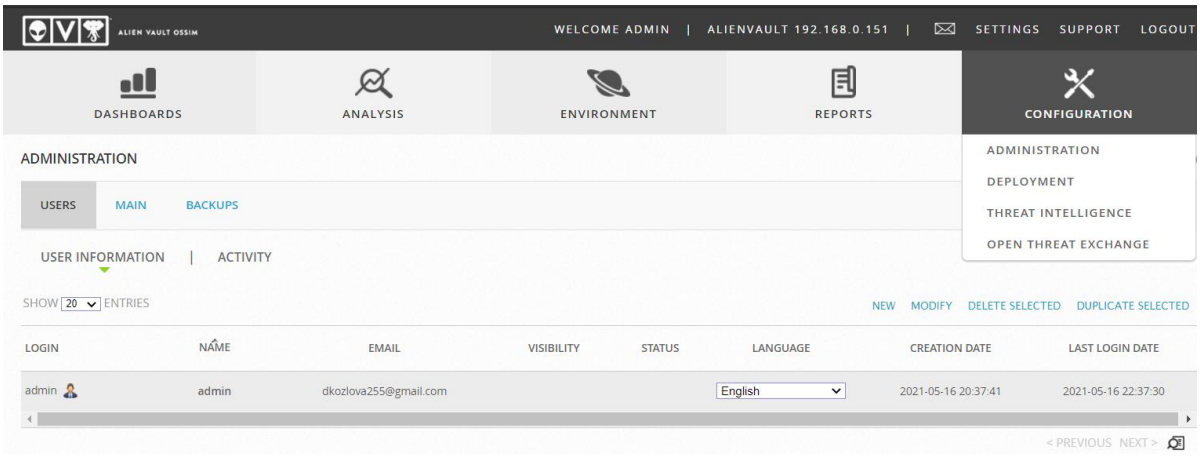

Рисунок 3.15 - Вкладка Configuration

3.3. Розгортання модулю EventLog Analyzer для AlienVault SIEM

EventLog Analyzer встановлюється як звичайна програма через завантажувач та не потребує попередніх налаштувань.

Оскільки EventLog Analyzer було запущено з робочої станції, вона автоматично починає моніторитися. Після авторизації ми бачимо вже зібрану

інформацію з хостової машини та вкладку Dashboard(містить декілька інформаційних панелей, які дають вам уявлення про важливі мережеві події) (Рисунок 3.16).

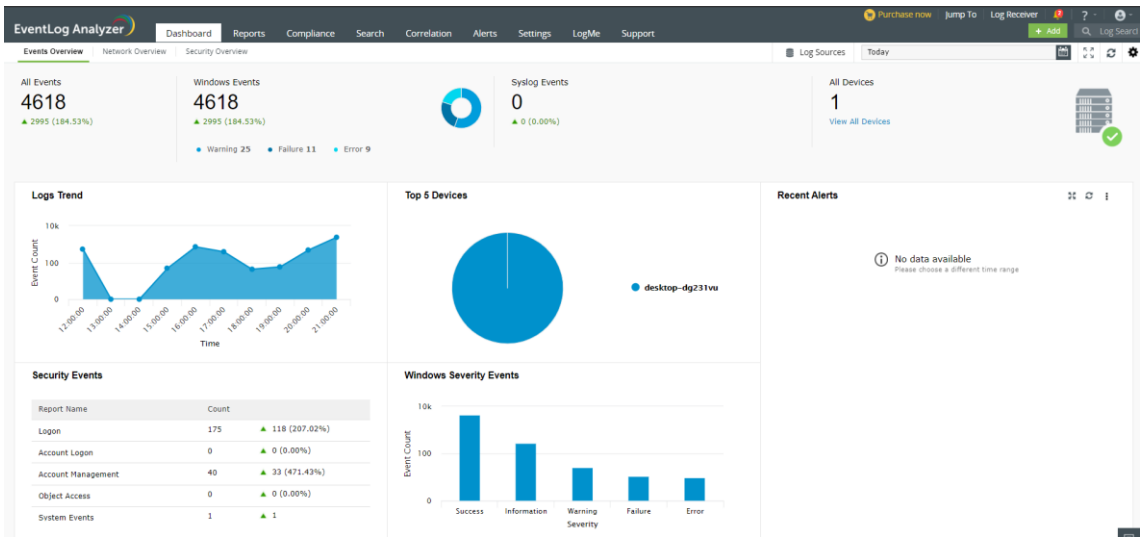

Рисунок 3.16 - Початкова сторінка EventLog Analyzer

Доступ до звітів можна отримати на вкладці "Reports" в інтерфейсі користувача. Кількість подій, показану у звітах, можна детально переглянути до необроблених журналів. Журнали можна додатково фільтрувати на основі різних полів журналу. EventLog Analyzer також дозволяє планувати автоматичне створення звітів та їх періодичне надсилання по електронній пошті. Спеціальні профілі звітів можна експортувати як файли XML, а згодом імпортувати, якщо це необхідно (Рисунок 3.17).

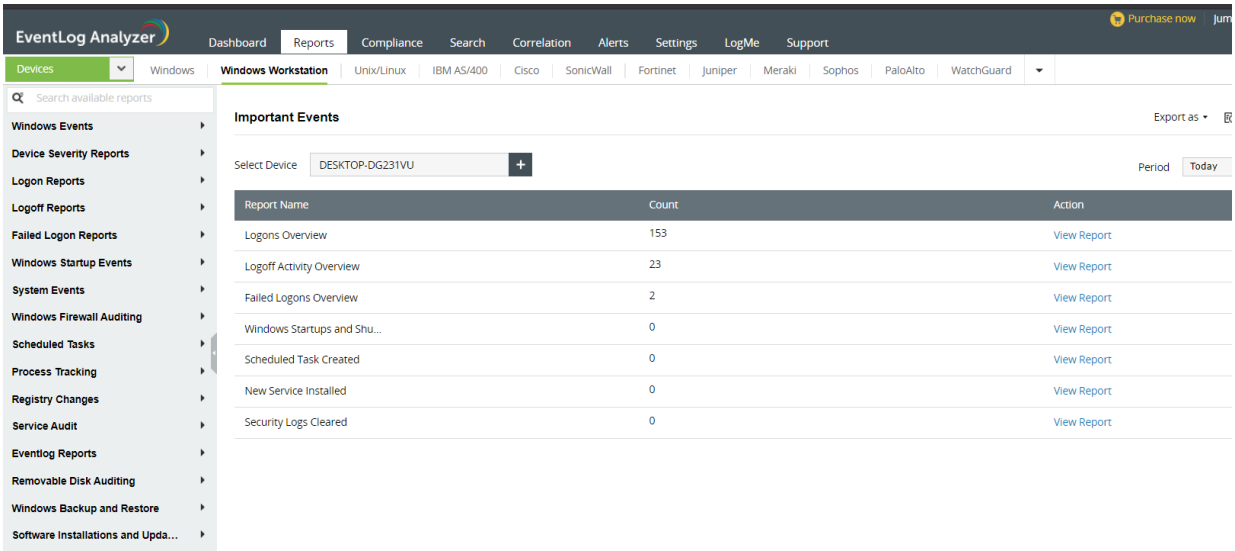

Рисунок 3.17 - Вкладка Reports

Також за допомогою цієї вкладки ми можемо продивлятися інформацію про входи і виходи з системи всіх користувачів, дивитися статистику за часом (у який час було найбільше входів чи виходів), за користувачами (частоту авторизацій кожного) та інше (Рисунок 3.18 та Рисунок 3.19).

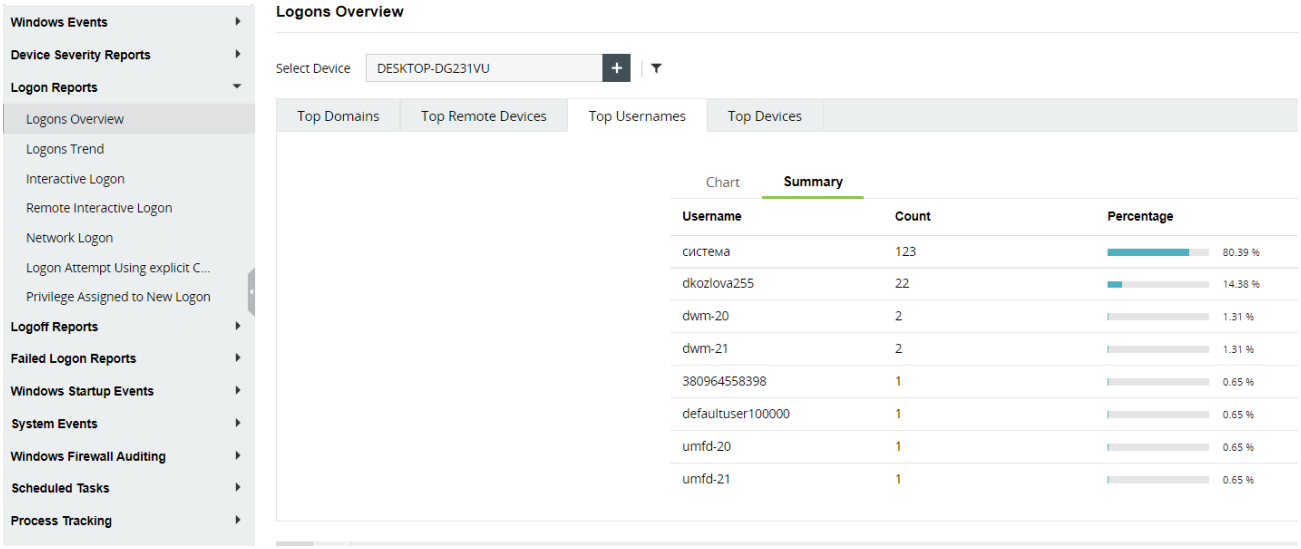

Рисунок 3.18 - Статистика авторизацій в системі по користувачам

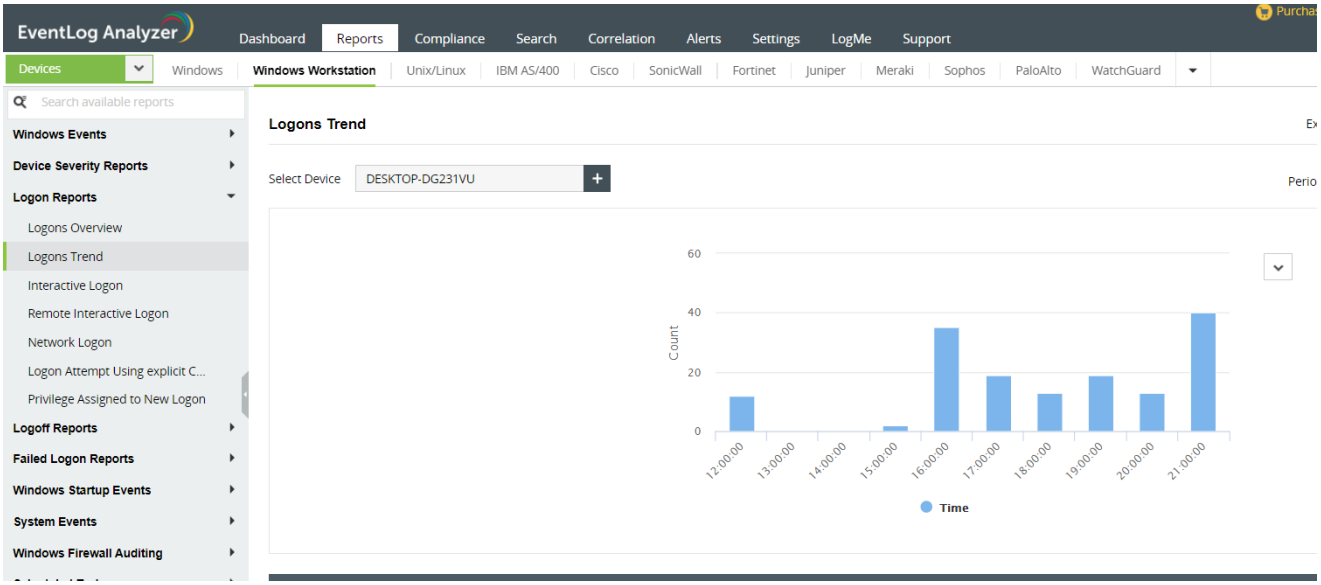

Рисунок 3.19 - Статистика авторизацій за часом

Також ми можемо продивлятися статистику невдалих авторизацій, бачити за якої причини користувача не було авторизовано (Рисунок 3.20).

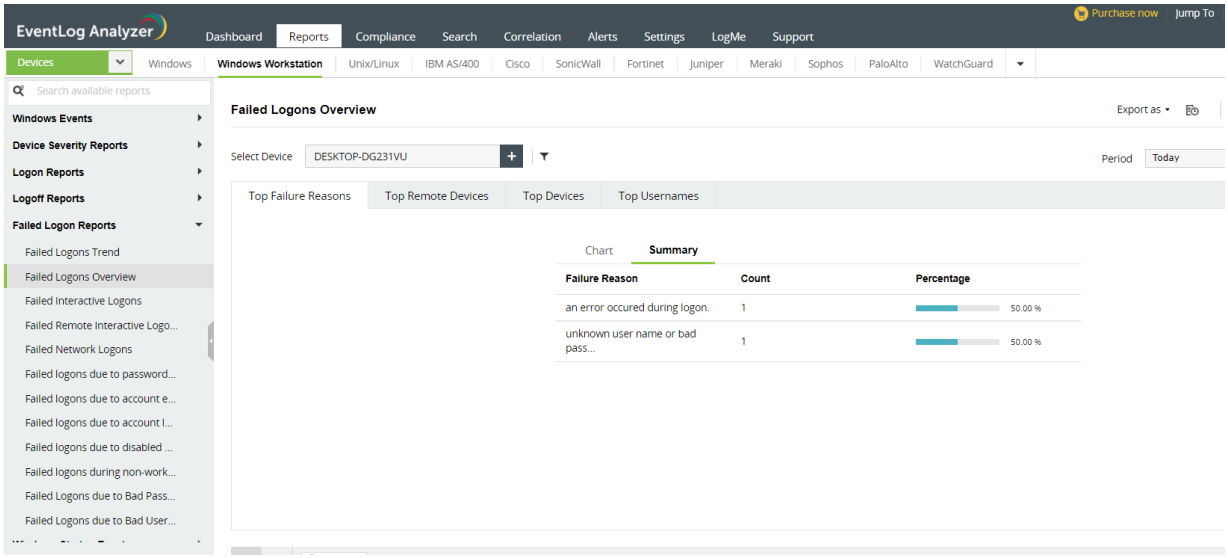

Рисунок 3.20 - Статистика невдалих авторизацій

Так само ми можемо продивлятися статистику з модифікації програмного забезпечення, продивлятися інформацію про початок і закінчення роботи будь-якого сервісу, який було ініційовано будь-яким користувачем, відстежувати зміни часу системи, модифікації правил міжмережевих екранів та багато іншого. Для Linux систем є можливість налаштувати моніторинг модифікації файлів, авторизацій користувачів через SSH чи FTP.

Є можливість налаштувати журнали, з яких система буде брати інформацію (Рисунок 3.21).

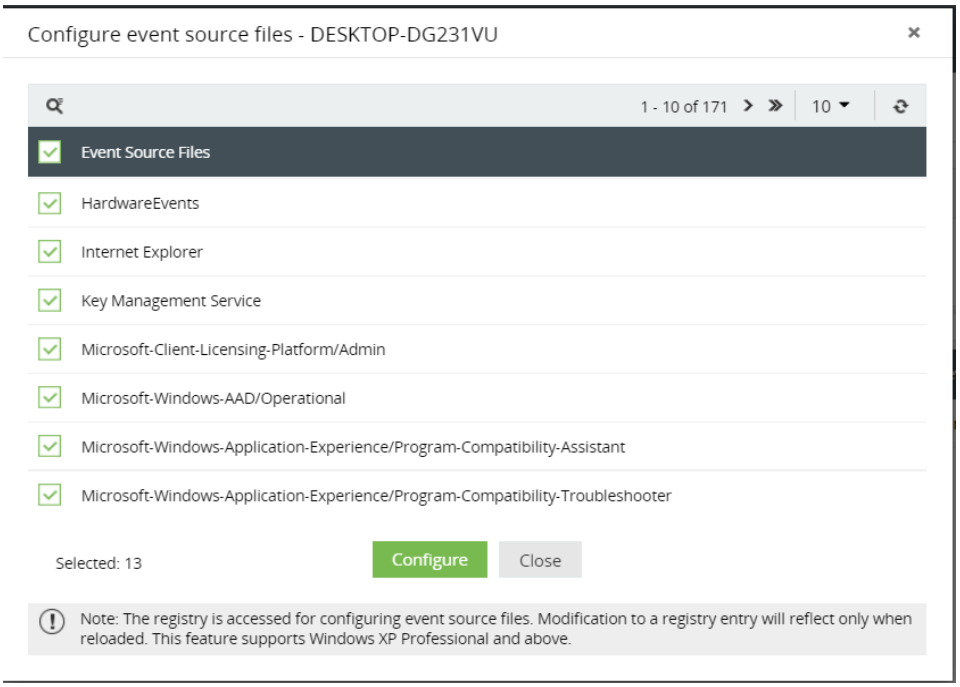

Рисунок 3.21 - Конфігурація файлів для інформації

За допомогою вкладки Alerts ми маємо можливість створити власні повідомлення про подію в системі (Рисунок 3.22). Текст повідомлення, тип події, пристрій є налаштованими, тому і повністю адаптованим під кожного адміністратора.

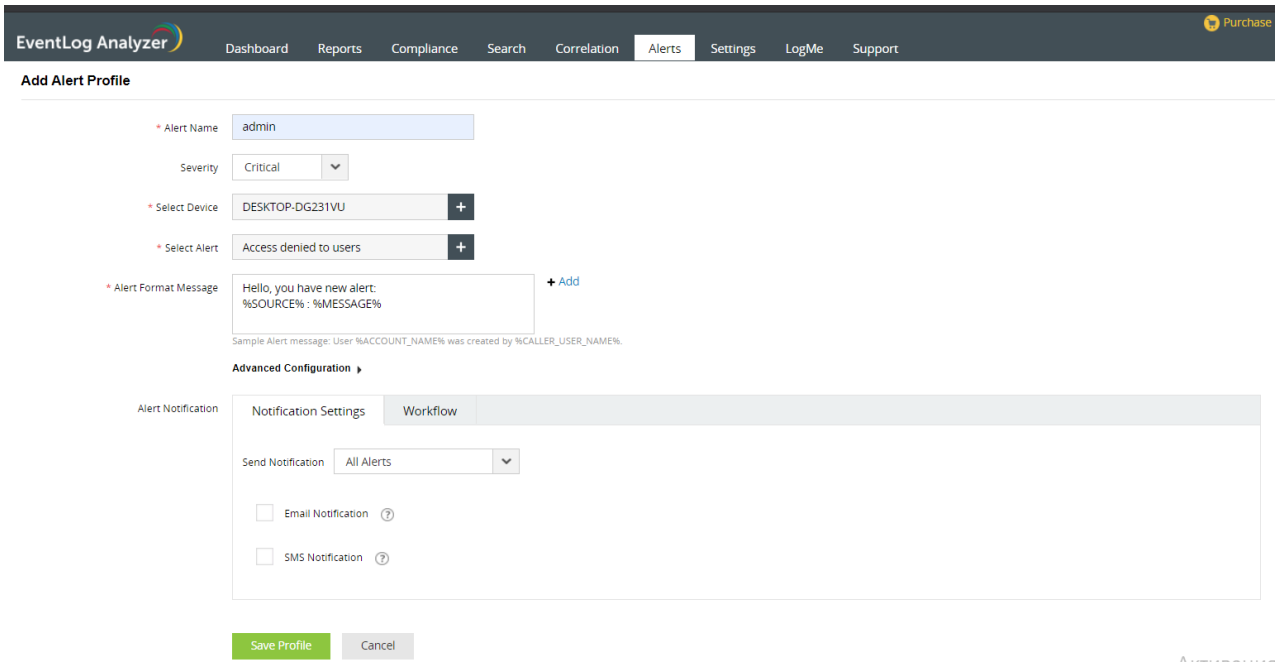

Рисунок 3.22 - Налаштування власних повідомлень

Також ми маємо можливість створити звіти за власними потребами. Мною було розроблено звіт про отримання доступу до файлів чи видалення їх на локальному комп’ютері (Рисунок 3.23, Рисунок 3.24, Рисунок 3.25 та Рисунок 3.26).

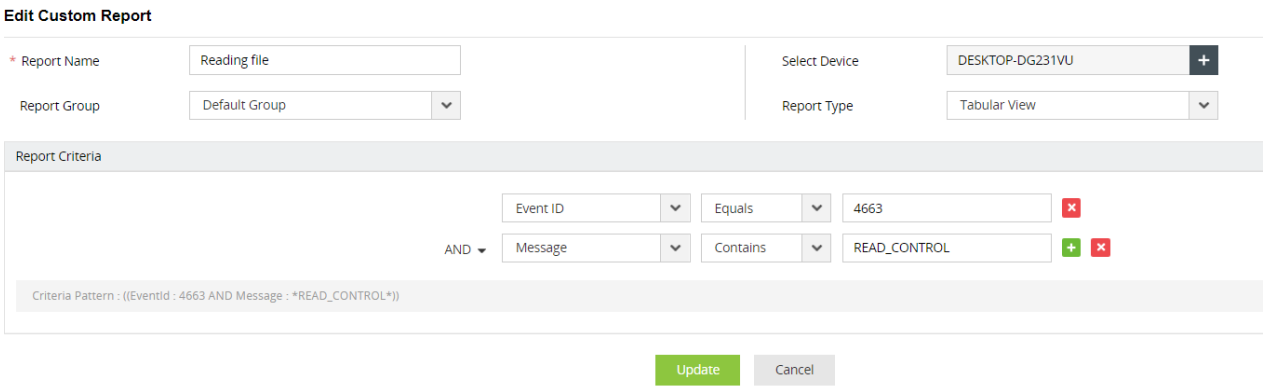

Рисунок 3.23 - Налаштування звіту “Reading files”

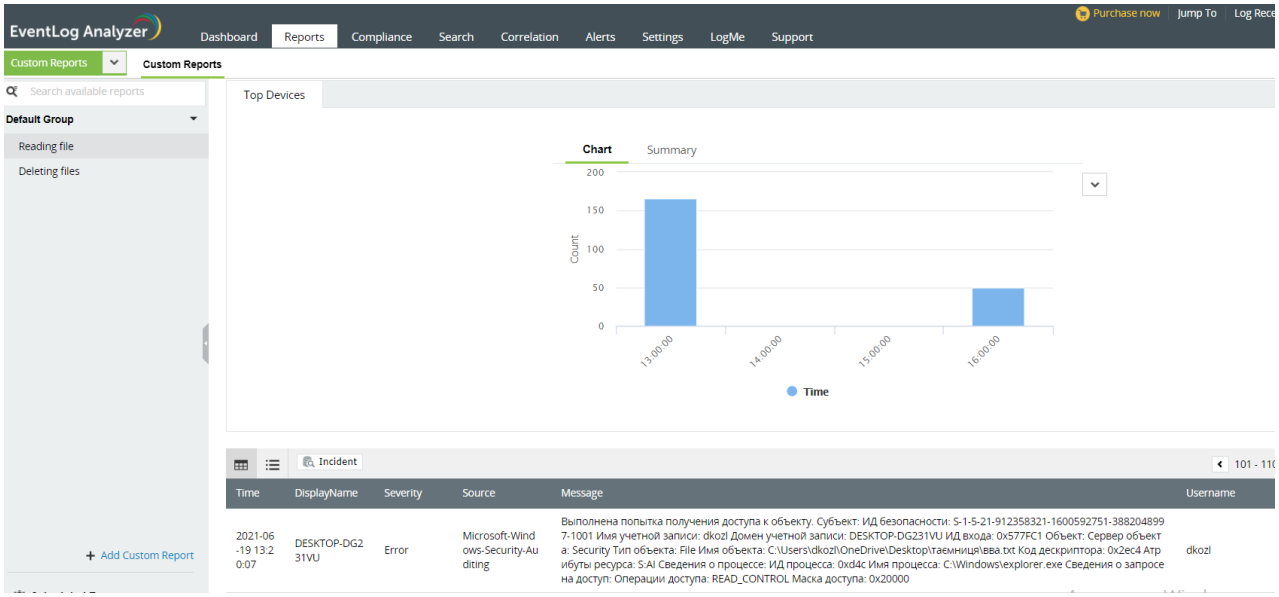

Рисунок 3.24 - Результат звіту “Reading files”

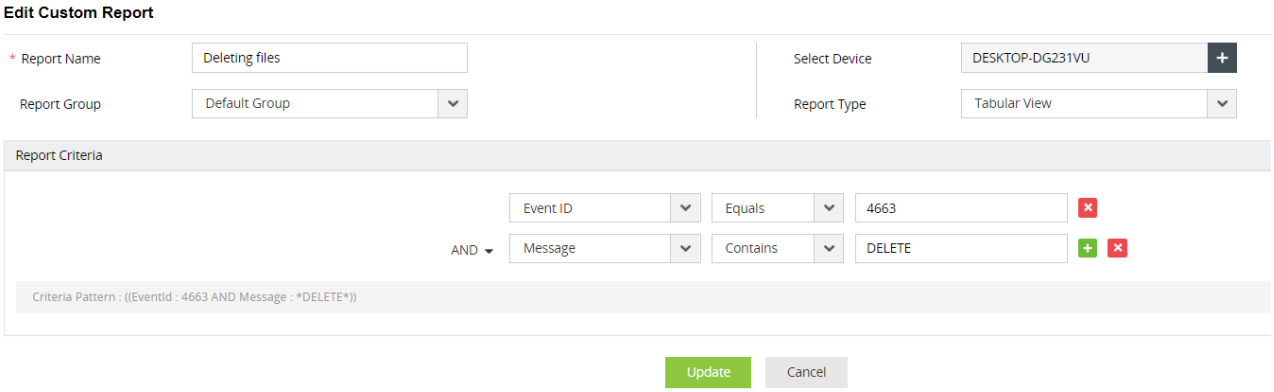

Рисунок 3.25 - Налаштування звіту "Deleting files"

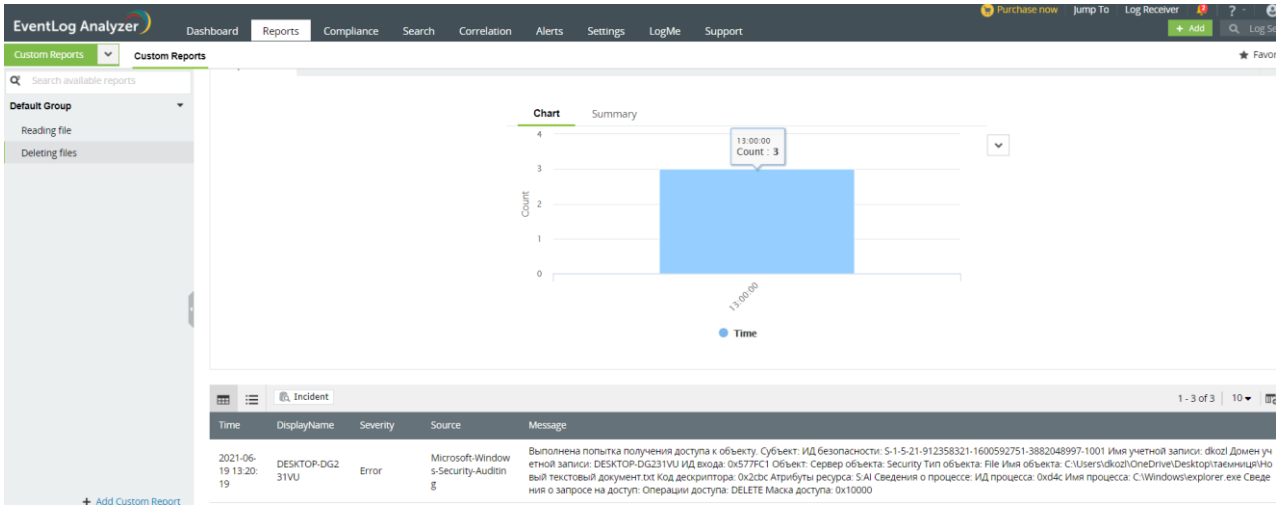

Рисунок 3.26 -Результат звіту "Deleting files"

3.4. Підсумки налаштування

Отже, розгорнувши і налаштувавши систему, я можу зробити висновок, що SIEM системи (на прикладі AlienVault OSSIM) можуть бути використані при побудові комплексних систем захисту інформації згідно з Постанови Кабінету Міністрів України №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [4] . Наша система виконує пункти 6 (забезпечення захисту від несанкціонованого та неконтрольованого ознайомлення зі службовою та таємною інформацією), 7 (надання доступу до інформації лише ідентифікованим та авторизованим користувачам), 11 (обов’язкова реєстрація користувачів, можливість перегляду результатів ідентифікації та автентифікації користувачів, виконання операцій з обробки інформації, спроб несанкціонованих спроб автентифікації чи дій з інформацією) та 15 (контроль за цілісністю програмного забезпечення, яке використовується на підприємстві).

ВИСНОВКИ

У цій роботі було проаналізовано сучасні загрози для інформаційних систем підприємств, види шкідливого програмного забезпечення та методи проникнення до комп’ютерних мереж. Також було зроблено огляд найвідоміших виробників SIEM систем, складання порівняльної характеристики.

Оскільки інформація є одним з найголовніших активів підприємства, тому потребує багато уваги з боку безпеки. Загрозу для інформації можуть нести як зовнішні зловмисники, так і внутрішні співробітники компанії. Підприємство, що має на меті захистити інформаційну систему, має планово проводити лекції для співробітників та нагадувати про покарання при порушенні регламентів роботи з таємною чи державною інформацією та впровадити моніторинг системи у реальному часі.

Щоб побудувати комплексну систему захисту інформації для проведення аудиту кібербезпеки на підприємстві було запропоновано SIEM систему. На практиці було продемонстровано її основний функціонал та способи моніторингу. Також було проаналізовано відповідність SIEM системи вимогам Постанови Кабінету Міністрів України №373.

СПИСОК ЛІТЕРАТУРИ

1. Зубок М.І. Інформаційна безпека в підприємницькій діяльності / М.І. Зубок. – К.: ГНОЗІС, 2015 – 216с.

2. Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats, 2020 – 242p.

3. Хорошко В.О., Чередниченко В.С., Шелест М.Є. Х 80 Основи інформаційної безпеки / За ред. проф. В.О. Хорошка. - К.: ДУІКТ, 2008.- 186 с.

4. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова від 29.03.2006 р. №373, зі змінами та доповненнями / Кабінет Міністрів України – 2006.

5. «Управление событиями информационной безопасности (SIEM)». [Електронний ресурс] – Режим доступу до ресурсу: http://www.in4sec.com.ua/upravlenie-soby-tiyami-informatsionnoj-bezopasnostisiem/

6. David R. Miller Security Information and Event Management (SIEM) Implementation (Network Pro Library) 1st Edition, 2010 – 464p.

7. Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architects, 2020 – 418p.

8. Ritvik Khanna. «How to use Elasticsearch, Logstash and Kibana to visualise logs in Python in realtime». [Електронний ресурс] – Режим доступу до ресурсу: https://www.freecodecamp.org/news/how-to-use-elasticsearch-logstashand-kibana-to-visualise-logs-in-python-in-realtime-acaab281c9de/

9. IBM QRadar Security Intelligence Platform (NDcPP21) Security Target, January, 15,2020 – 32 p.

10. «SPLUNK ДЛЯ БЕЗОПАСНОСТИ». [Електронний ресурс] – Режим доступу до ресурсу: https://www.splunk.com/pdfs/solution-guides/splunk-for-security-ru_ru.pdf

11. «McAfee Enterprise Security Manager 11.1.x Product Guide». [Електронний ресурс] – Режим доступу до ресурсу: https://docs.mcafee.com/ru-RU/bundle/enterprise-security-manager-11.1.x-product-guide/page/GUID-88473528-B9BD-4799-B3A7-BC7A8C22B55D.html

12. Tim Rains, Cybersecurity Threats, Malware Trends, and Strategies: Mitigate exploits, malware, phishing, and other social engineering attacks,2020 – 428p.