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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система виявлення вразливостей в інформаційній системі організації»

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

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

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

_____ Кирило КОМАЩЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
КОМАЩЕНКО Кирило
(прізвище, ім'я)

Керівник: к. держ.упр. СКИБУН Олександр
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент: д.е.н., проф. ЛЕГОМІНОВА Світлана
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

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

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри СТКБ
_____ Галина ГАЙДУР
“___” _____ 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

КОМАЩЕНКО Кирила Андрійовича
(прізвище, ім’я)

1. Тема кваліфікаційної роботи:
«Система виявлення вразливостей в інформаційній системі організації»

керівник кваліфікаційної роботи СКИБУН Олександр, к. держ.упр.
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2025 року № 56.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 06.06.2025 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.
3. Вихідні дані до кваліфікаційної роботи
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Теоретичні основи виявлення вразливостей в інформаційній системі організації
2.Дослідження автоматизованих систем виявлення вразливостей в інформаційній системі організації.
2. Аналіз методів та засобів інтеграції автоматичних систем виявлення вразливостей в інформаційній системі організації
3. Розроблення рекомендацій щодо мінімізації витрат малим корпораціям під час

вибору за запровадження автоматизованих виявлення вразливостей в інформаційній системі організації

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 28.02.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми щодо автоматизованих систем.	03.03.2025 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	24.03.2025 р.	
3.	Аналіз методів та засобів інтеграції автоматичних систем виявлення вразливостей в інформаційній системі організації.	05.04.2025 р.	
4.	Практична реалізація варіанту використання автоматичних систем з пошуку вразливостей	28.04.2025 р.	
5.	Розроблення рекомендацій щодо мінімізації витрат малим компаніям під час вибору за запровадження автоматизованих виявлення вразливостей в інформаційній системі організації	10.05.2025 р.	
6.	Оформлення результатів дослідження.	26.05.2025 р.	
7.	Підготовка доповіді до захисту.	06.06.2025 р.	

Здобувач вищої освіти _____ Кирило КОМАЩЕНКО
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Олександр СКИБУН
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача КОМАЩЕНКО Кирила
на тему: «Система виявлення вразливостей в інформаційній системі організації».

Актуальність:

Позитивні сторони:

Недоліки:

Висновок:

Рецензент:	д.е.н., професор		ЛЕГОМІНОВА Світлана
	(науковий ступінь, вчене звання)	*(підпис)*	*(ім'я, прізвище)*

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач КОМАЩЕНКО Кирило до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньої програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Система виявлення вразливостей в інформаційній системі організації»

Кваліфікаційна робота і рецензія додаються.
Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач КОМАЩЕНКО Кирило обрав тему роботи,

Керівник кваліфікаційної роботи _____ Олександр СКИБУН
(підпис) *(ім'я, прізвище)*
"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач КОМАЩЕНКО Кирило допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи:

Об'єкт дослідження – процес управління кібербезпекою в корпоративних мережах.

Предмет – автоматизація виявлення та усунення вразливостей з використанням сучасних інструментів.

Мета роботи: Розробити план щодо інтегрування автоматичних систем розпізнавання вразливостей для малих корпорацій, мінімізуючи витрати, не втрачаючи релевантної цих дій.

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

Ця тема була спрямована на автоматизацію виявлення та усунення вразливостей з використанням сучасних інструментів автоматизації, а також усунення «людського фактору» у подібних процесах, адже частіш за все, саме через нього корпорації страждають більш за все. Приклад: у липні 2023 року компанія «Нова пошта» стала жертвою масованої кібератаки, яка паралізувала її онлайн-сервіси на 3 доби. Основна причина – відсутність автоматизованого моніторингу та реагування на загрози. Як наслідок, більше 300 відділень були неактивними, та логістична зв'язка між користувачами була призупинена.

В роботі досліджено проблему відсутності автоматизаційних алгоритмів реагування на можливі вразливості, а також способи економії ресурсів, для встановлення подібних алгоритмів малим корпораціям, з важливим змістом баз даних про клієнтів. На основі досліджень будуть запропоновані варіанти рішень, завдяки яким можна буде уникнути «людського фактору», а також зекономити на витратах, без втрати релевантності систем реагування на загрози, та самих фахівців кібербезпеки.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 8

РОЗДІЛ 1 ОЗНАЙОМЛЕННЯ ТА ВИВЧЕННЯ ПРОБЛЕМИ АВТОМАТИЗАЦІЇ У КОРПОРАЦІЯХ, НАЙЧАСТІШІ ПРОБЛЕМИ ТА ПРИЧИНИ УНИКНЕННЯ ПОДІБНОГО ФУНКЦІОНАЛУ. 12

1.1. Ознайомлення з автоматичними процесами, їх переваги та недоліки. 10

1.2. Перші кроки автоматизаційних процесів, хронологія подій та розвиток систем. 17

1.3. Вплив автоматизації на сферу кібербезпеки 19

1.4. Аналіз методів та засобів інтеграції автоматичних систем 21

РОЗДІЛ 2 Практична реалізація варіанту використання автоматичних систем з пошуку вразливостей 28

2.1. Вибір інструменту та аналіз функціоналу для виконання завдання. 31

2.2. Інсталяція інструменту, налаштування та нові проблеми. 33

2.3. Результати та підсумок практичної частини. 47

РОЗДІЛ 3 Розроблення рекомендацій щодо мінімізації витрат малим корпораціям 48

ВИСНОВКИ 56

ПЕРЕЛІК ПОСИЛАНЬ 57

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 60

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

IDS – Системи виявлення вторгнень

VRA – Vulnerability Response Automation

AVSS – Automated Vulnerability Scanning Systems

CVE – Common Vulnerabilities and Exposures

ШІ – Штучний Інтелект

API – Application Programming Interface.

IDS/IPS – Intrusion Detection/Prevention Systems

SMTP – Simple Mail Transfer Protocol

WL – White List

PII – Personally identifiable information

SIEM – Security Information and Event Management

ВСТУП

Актуальність дослідження: Автоматизація відповіді на вразливості в інформаційних системах набуває критичного значення в умовах сучасного кіберпростору. По-перше, зростання кількості та складності кіберзагроз вимагає швидкого реагування – за даними досліджень, у 2024 році щодня з'являлося понад 100 нових вразливостей. По-друге, ручні методи виявлення та усунення вразливостей стають неефективними через масштаби сучасних інфраструктур. По-третє, автоматизовані системи дозволяють скоротити час реагування з тижнів до годин, що критично важливо для запобігання серйозним інцидентам.

Основні аспекти дослідження: Сучасні системи автоматизації відповіді на вразливості (Vulnerability Response Automation) поєднують:

1. Інтелектуальні механізми;
2. Сканування алгоритми оцінки ризиків;
3. Автоматизовані сценарії усунення загроз;
4. Інтеграцію з існуючими системами безпеки;

Мета та завдання дослідження: Метою роботи є розробка комплексного підходу до автоматизації процесів виявлення, класифікації та усунення вразливостей в корпоративних інформаційних системах. Для досягнення цієї мети вирішуються такі завдання:

1. аналіз сучасних методів виявлення вразливостей;
2. дослідження архітектур автоматизованого реагування;
3. розробка алгоритму пріоритезації вразливостей;
4. створення моделі інтеграції з SIEM-системами.

Об'єкт і предмет дослідження: Об'єктом дослідження є процеси керування вразливостями в корпоративних інформаційних системах. Предметом – методи та засоби автоматизації відповіді на вразливості.

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

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів захисту від вразливостей, щоб уникнути людського

фактору для більш швидкого реагування, а також зекономити ресурс на витрати фахівцям кібербезпеки, без втрати відсоткової користі.

РОЗДІЛ 1 ОЗНАЙОМЛЕННЯ ТА ВИВЧЕННЯ ПРОБЛЕМИ АВТОМАТИЗАЦІЇ У КОРПОРАЦІЯХ, НАЙЧАСТІШІ ПРОБЛЕМИ ТА ПРИЧИНИ УНИКНЕННЯ ПОДІБНОГО ФУНКЦІОНАЛУ

1.1 Ознайомлення з автоматичними процесами, їх переваги та недоліки

Автоматизація зараз є не розкішшю, а необхідністю у сфері кібербезпеки. Працювати без неї просто неможливо. Автоматизовані сервіси – від сканування вразливостей до реагування на атаки – є основою захисту даних. Їхня важливість також значно зросла завдяки швидкому росту кібер-атак та їхній складності. Наприклад, дослідження IBM також показує, що виявлення атак під керівництвом людини займає в середньому понад 200 днів, тоді як автоматизована система може скоротити цей проміжок до годин або навіть хвилин.

Проте автоматизація - це більше, ніж просто інструмент - вона охоплює машинне навчання, аналіз великих даних та навіть штучний інтелект. Це не тільки спосіб виявлення проблем, але й потужний інструмент для їх передбачення, що все більше стає необхідністю як для великих корпорацій та уряду, так і для малих підприємств. Але, як і будь-яка технологія, вона має свої обмеження, які слід враховувати під час використання.

Це процес використання спеціалізованого програмного забезпечення та алгоритмів для автоматичного сканування інформаційних систем з метою ідентифікації слабких місць у їхній конфігурації, програмному коді або інфраструктурі. Вона передбачає застосування інструментів, які без безпосередньої участі людини аналізують систему на відповідність відомим шаблонам вразливостей (CVE, OWASP Top 10, тощо). До ключових переваг належать скорочення часу оцінки ризиків, усунення людського фактору та масштабованість для великих мереж. Сучасні рішення часто інтегрують машинне навчання для виявлення аномалій, що дозволяє прогнозувати нові типи

загроз.

Таблиця 1.1.

Основні компоненти автоматизованих процесів безпеки.[персональна таблиця]

Компонент	**Опис**	**Типи / Підкатегорії**	**Приклади інструментів**
Системи виявлення вторгнень (IDS)	Моніторять мережевий трафік та активність систем на наявність аномалій або підозрілих дій. Використовують сигнатурний та аномалійний аналіз.	– Мережеві (NIDS) – Хостові (HIDS) – Гібридні	Snort, Suricata, OSSEC, Bro/Zeek
Системи управління інформацією та подіями безпеки (SIEM)	Агрегують дані з різних джерел (журнали, трафік, системи безпеки) для кореляції подій, виявлення загроз та генерування звітів.	– Локальні рішення – Хмарні платформи	Splunk, IBM QRadar, ArcSight, Wazuh
Автоматизовані системи управління доступом	Контролюють права доступу до ресурсів на основі політик (RBAC, ABAC). Інтегруються з IAM (Identity and Access Management).	– Ролі-базований контроль (RBAC) – Атрибут-базований (ABAC) – Політики нульової довіри (Zero Trust	Okta, Microsoft Azure AD, Keycloak, Ping Identity

Продовження Таблиці 1.1

Рішення для реагування на інциденти (SOAR) SIEM	Автоматизують усунення загроз: блокування IP, ізоляція пристроїв, сповіщення адміністраторів. Часто інтегруються.	– Платформи з вбудованими playbooks – Сценарії оркестрації	Palo Alto Cortex XSOAR, TheHive, FortiSOAR, Demisto

Таблиця 1.2.

Функціонал інструменту з прикладів:(Системи виявлення вторгнень (IDS).[персональна таблиця]

Інструмент	**Функціонал**	**Використання**
Snort	Аналізує мережевий трафік у реальному часі, виявляє атаки на основі сигнатур (наприклад, SQL-ін’єкції) та аномалій. Підтримує власні правила.	— Мережі корпоративного рівня — Захист периметру (наприклад, біля фаєрволів)
Suricata	Покращена версія Snort з підтримкою багатопоточності, інтеграцією з SIEM та автоматичним оновленням правил. Може блокувати трафік (як IPS).	– Великі інфраструктури (телеком, фінанси) – Хмарні середовища
OSSEC	Хостовий IDS: моніторить файлові зміни, логіни, підозрілі процеси. Працює на Linux/Windows, інтегрується з SIEM.	– Сервери з критичними даними – Захист від внутрішніх загроз

Таблиця 1.3.

SIEM-системи [персональна таблиця]

Інструмент	*Функціонал*	*Використання*
Splunk	Збирає дані з будь-яких джерел (логи, трафік, API), аналізує їх через ML, генерує звіти та сповіщення. Має власну мову SPL для запитів.	— Кібербезпека банків — Розслідування інцидентів
IBM QRadar	Автоматично класифікує події, будує графі зв’язків між атаками (наприклад, ланцюги MITRE ATT&CK). Підтримує регуляторні стандарти (GDPR).	— Великі корпорації — Урядові установи
Wazuh	Open-source рішення з функціями SIEM, IDS та моніторингу вразливостей. Працює на агентах, які збирають дані з хостов.	— Стартапи, малий бізнес — Захист хмарних серверів (AWS, Azure)

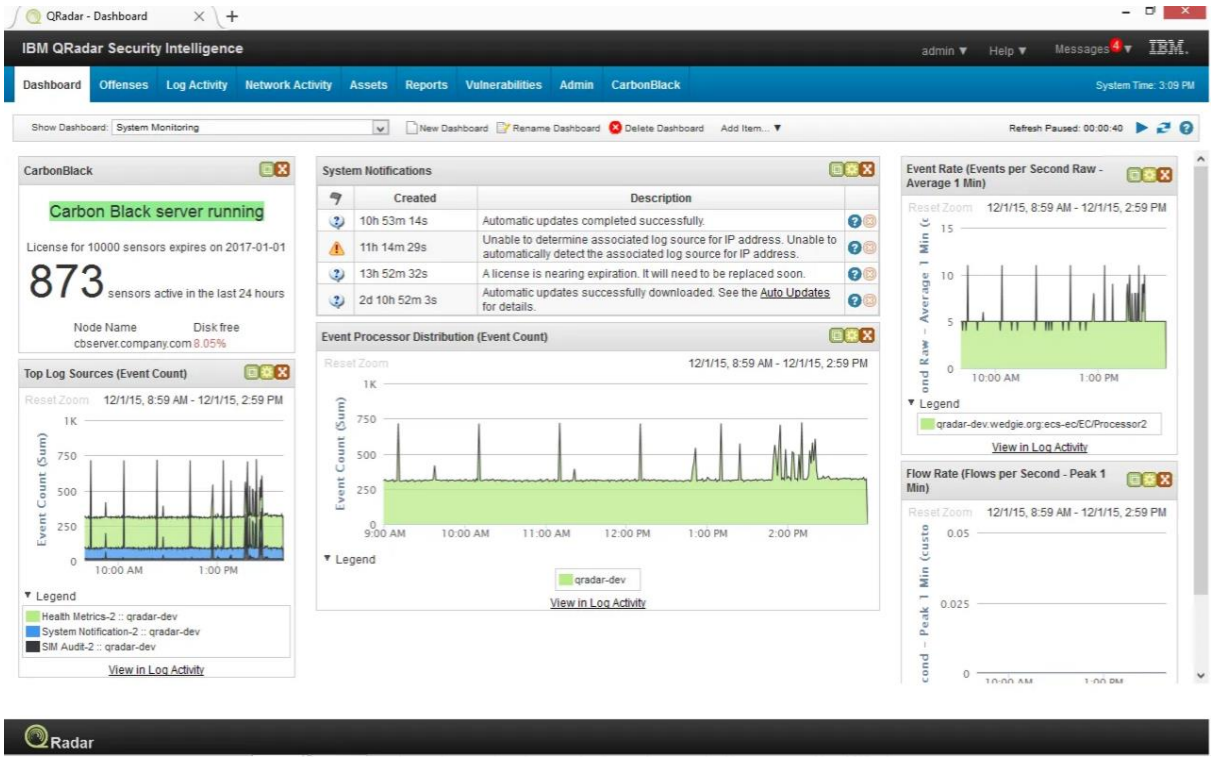

Рис1.1. Інтерфейс програми Qradar. [29]

Таблиця 1.4.

Системи управління доступом

Інструмент	**Функціонал**	**Використання**
Okta	Централізована аутентифікація (SSO), MFA, управління ролями (RBAC). Інтегрується з 7,000+ додатками (наприклад, Slack, Zoom).	— Хмарні сервіси — Компанії з розподіленими командами
Microsoft Azure AD	Ідентифікація користувачів у середовищі Microsoft (Office 365, Azure). Підтримує політики умовного доступу (наприклад, «блокируй вхід з VPN»).	— Організації на стекі Microsoft — Державні установи

Таблиця 1.5.

SOAR-рішення

Інструмент	**Функціонал**	**Використання**
Palo Alto Cortex XSOAR	Автоматизує реагування: блокує IP, видаляє шкідливі файли, створює тикети в ServiceNow. Має бібліотеку готових "playbooks".	— SOC (Security Operations Center) — Інтеграція з Palo Alto фаєрволами
TheHive	Open-source платформа для спільної роботи над інцидентами. Дозволяє зв’язувати події, вести журнали розслідувань.	— CERT-команди — Аналітики з кібербезпеки

Концепція автоматизації виявлення вразливостей, основні переваги. Сукупність технологічних та методологічних підходів, спрямованих на заміну ручних процесів сканування інструментами, які автономно ідентифікують слабкі місця в IT-інфраструктурі на основі актуальних баз CVE, правил OWASP та машинного навчання. Вона ґрунтується на трьох рівнях:

1. Автоматизоване сканування мереж, ПО та конфігурацій.
2. Інтеграція з SIEM/SOAR для швидкого реагування.
3. Адаптивні алгоритми для виявлення аномалій.

Ключові переваги включають зниження часу виявлення з тижнів до годин, усунення людських помилок та можливість масштабування для складних середовищ. Сучасні реалізації, такі як Tenable.io або Qualys VMDR, демонструють ефективність цього підходу, зокрема у проактивному запобіганні інцидентам, що підтверджено кейсами впровадження у банківському секторі (наприклад, зниження ризиків на 40% за рік).

1.2 Перші кроки процесів автоматизації, хронологія подій та розвиток систем

Автоматизація безпеки бере свій початок з появи комп'ютерних систем у 1960-х роках. У той час безпека більше стосувалася методології захисту комп'ютерів у фізичному сенсі, що означало забезпечення фізичного доступу до систем і захисту апаратного забезпечення від несанкціонованого доступу. Однак, з розвитком технологій та зростанням популярності комп'ютерних мереж, в кінці 80-х років на ринку з'явилися нові потреби. Зокрема, зростаючий попит з боку компаній на автоматизовані засоби захисту для нових типів даних, які стали доступними через мережі, змусив фахівців у галузі безпеки переосмислити свої підходи до захисту інформації.

1970-ті роки: У цей період почали з'являтися системи контролю доступу, які стали першою формою захисту даних та систем безпеки. Ці системи дозволяли обмежувати доступ до інформації у тій чи іншій мірі, що надавало можливість контролювати, хто може отримати доступ до чутливих даних. Системи контролю доступу не були складними і в основному призначалися для захисту невеликих спільнот від комп'ютерних мереж, забезпечуючи базові механізми безпеки, проте їхня роль у формуванні основ безпеки була незаперечною.

1980-ті роки: Цей період став знаковим з точки зору появи мереж, які кардинально змінили підходи до безпеки. Разом з цим, з'явилися перші системи виявлення вторгнень (IDS), які дозволяли виявляти несанкціонований доступ до систем. Вони стали важливими інструментами для організацій, дозволяючи своєчасно реагувати на загрози та зменшувати ризики. У цей же період почали розробляти перші антивірусні програми, які автоматично сканували файли на наявність шкідливого програмного забезпечення, що стало важливим кроком у боротьбі з комп'ютерними вірусами.

1990-ті роки: Це десятиліття відзначилося значним зростанням систем управління інформацією та подіями безпеки (SIEM). Ці системи почали збирати та аналізувати дані з багатьох джерел для виявлення загроз, що дозволяло

організаціям мати більш комплексну картину стану безпеки. Завдяки цим технологіям, фахівці з інформаційної безпеки отримали можливість об’єднувати дані з різних систем безпеки, що сприяло більш ефективному реагуванню на інциденти та поліпшенню загального огляду ситуації з безпекою.

2000-ні роки: Цей період став свідком зростання «консолідованих систем», таких як SOAR (Оркестрація, автоматизація та реагування на безпеку). Ці системи об’єднували кілька технологій безпеки під одним дахом, що дозволяло не лише автоматизувати виявлення загроз, але й значно покращити реакцію на них. Завдяки SOAR, організації змогли оптимізувати свої процеси реагування на інциденти, скоротити час на виявлення та реагування на загрози, а також підвищити ефективність роботи своїх команд з безпеки.

Ідея автоматизованого сканування вразливостей виникла разом із розвитком мережевих технологій. Одним із перших інструментів був «The Network Security Scanner», розроблений у 1985 році групою дослідників на чолі з Робертом Моррісом (Robert T. Morris) – пізніше відомим через створення першого інтернет-черв’яка Morris Worm (1988). Цей сканер аналізував UNIX-системи на наявність слабких паролів і відомих конфігураційних помилок. На початку 1990-х компанія ISS (Internet Security Systems) заснувала перший комерційний продукт – Internet Scanner (1992 рік), який став стандартом для аудиту безпеки в корпораціях (зокрема, у банках та урядових установах). Він дозволяв:

1. Автоматично виявляти відомі вразливості (наприклад, у серверах SunOS).
2. Генерувати звіти для відповідності регуляторним вимогам.
3. Зменшити витрати на ручні перевірки на 60–70% (за даними ISS, 1994).

1.3 Вплив автоматизації на сферу кібербезпеки

Автоматизація відіграє ключову роль у трансформації сфери кібербезпеки, забезпечуючи нові можливості для захисту інформаційних систем від

зростаючих кіберзагроз. Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням кількості кіберзагроз, що потребує вдосконалених механізмів протидії. Однією з ключових складових ефективної кібербезпеки є виявлення вразливостей у програмному забезпеченні, інфраструктурі та мережах. Автоматизаційні системи пошуку вразливостей (Automated Vulnerability Scanning Systems, AVSS) стали невід'ємним інструментом для забезпечення проактивного захисту. Наразі автоматизація виконує декілька ролей у сучасному світі, а саме: автоматизація у виявленні вразливостей, вплив на стратегії кібербезпеки, економічні та етичні аспекти. Ми розглянемо їх більш детальніше.

Вплив автоматизації на стратегії кібербезпеки.

Інтеграція AVSS у практику організацій призвела до змін у стратегіях кібербезпеки. По-перше, з'явився акцент на безперервному моніторингу замість періодичних перевірок. По-друге, автоматизація дозволила масштабувати захист для великих інфраструктур, таких як хмарні сервіси або IoT-мережі.

Важливим аспектом є стандартизація. AVSS сприяли розповсюдженню таких фреймворків, як OWASP Top 10 або NIST Cybersecurity Framework, які визначають критерії оцінки вразливостей. Це полегшило взаємодію між різними організаціями та державними установами у боротьбі з кіберзлочинністю.

Роль автоматизації у виявленні вразливостей корпорацій та машинне навчання.

Традиційні методи пошуку вразливостей ґрунтувалися на ручному аналізі коду або пентестінгу, що вимагало значного часу та кваліфікованих фахівців. AVSS змінили цей підхід, запровадивши алгоритми сканування, які можуть автоматично аналізувати великі обсяги даних, порівнювати їх із базами відомих вразливостей (наприклад, CVE) та генерувати звіти у реальному часі. Це дозволило скоротити час реагування на загрози з місяців до годин, а іноді й хвилин.

Однак автоматизація не є панацеєю. Системи можуть давати хибно-позитивні результати або пропускати нові, невідомі вразливості (zero-day). Тому їх часто поєднують із методами штучного інтелекту для покращення точності. Наприклад, машинне навчання допомагає виявляти аномалії в мережевому трафіку або підозрілу поведінку програм, також завдяки базі з минулих інцидентів, як тільки програма знайде знайомий патерн – одразу почне приймати рішення щодо усунення загрози, в той час як людині знадобилося б кілька годин, щоб знайти той самий патерн. Наразі більша частина корпорацій займається саме машинним навчанням систем, інвестування йде саме на персонал обслуговування та корегування штучного інтелекту, найбільш затребувана професія з сфери машинного навчання є саме ML-Engineer, в Україні заробітна плата на цій посаді починається з 1000$, нажаль мала заробітна плата викликана ситуацією в країні та проблемною економікою з великими податками, але в країнах Європи на тій ж самій посаді заробітна плата досягає 70 000€ на рік, що рахується як 5 800€ на місяць. Серед вибору професії на майбутнє, посада ML-Engineer є самою привабливою, враховуючи потенційні загрози, щодо відсутності потенційного рекрутингу на такі посади як Junior Dev, тощо. Адже саме завдяки ШІ сфера програмування та кібербезпеки просовується далі, потреба у вигляді кадрів, що будуть займатися обслуговуванням та навчанням ШІ надзвичайно зростає.

1.4 Аналіз методів та засобів інтеграції автоматичних систем виявлення вразливостей

У межах опрацювання зазначеної тематики було здійснено всебічний аналіз існуючих підходів до інтеграції автоматичних систем виявлення вразливостей. Узагальнення результатів дозволило окреслити методологічні засади інтеграційних процесів та визначити ефективні засоби реалізації таких систем у сучасному інформаційному середовищі.

Методології інтеграції :

Інтеграція автоматичних систем виявлення вразливостей може бути реалізована декількома варіантами, найкорисніші з них є:

1. Вбудовування в існуючу інфраструктуру;
2. Використання API;
3. Модульна архітектура.

Нижче розглянемо більш детально кожну з них.

Перший варіант – Вбудовування в існуючу інфраструктуру:

Вбудовування в існуючу інфраструктуру передбачає собою інтеграцію системи виявлення вразливостей безпосередньо в існуючу систему управління безпекою, (такі варінати як SIEM) або ж наприклад, системи моніторингу. Такий метод дозволяє нам збирати та отримувати інформацію про недоліки та вразливості в режимі реального часу, та змогу реагувати на них миттєво.

Другий варіант – використання API, цей метод підійде якщо є основна частина коду, котра відповідає за перевірку на вразливості, але відсутні вхідні данні для навчання машини знаходити вразливості. Завдяки цьому методу, в вашу систему можна буде інтегрувати API будь якої другої системи виявлення вразливостей, адже більша частина має саме відкрите API, що також дозволяє нам зекономити кошти на інсталюванні системі. Такий варіант дозволяє забезпечити можливість автоматизації процесів, зокрема, автоматичного реагування на вразливості або планування регулярних сканувань.

Третій варіант – Модульна архітектура.

Ознайомившись з матеріалами спеціалістів, було зрозуміло, що менша частина компаній звертається до модульної структури систем, видаляючи певні модулі, заміняючи їх на інші. Саме через це, модульна архітектура дозволить організаціям додавати або видаляти модулі, доповнювати їх а також редагувати, дивлячись на потреби. Такий метод дозволить адаптувати систему до змін у вже готовій інфраструктурі, котра працює не перший тиждень, не пошкодити вже накопичений роками алгоритм, а лише скорегувати один або декілька його

модулів. Таким чином, організації котра працює з певною системою довгий період часу не знадобиться нова система у разі потреб, а необхідно лише провести редактування самих модулів, що значно економить кошти на витрати.

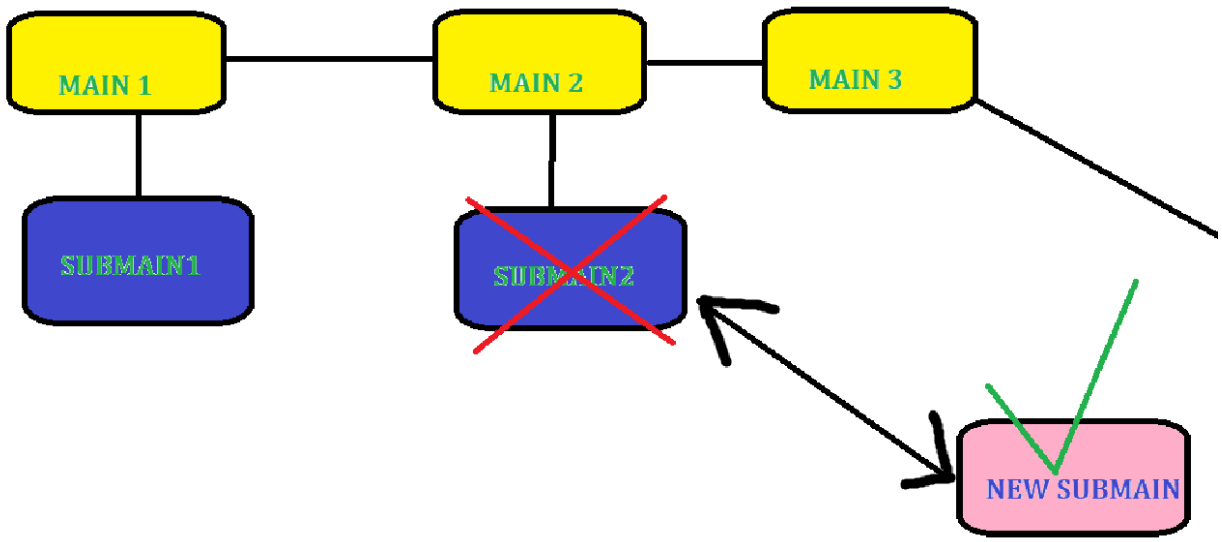

Рис. 1.2 Наглядний приклад заміни субмодулю на новий, без втрати важливих даних [28]

Після вивчення методів інтеграції, перейдемо до самих засобів інтеграції, а також необхідних вимог щодо самої інтеграції.

Для успішної інтеграції систем виявлення вразливостей в інформаційні системи організацій потрібно використовувати різні способи, деякі з них це:

1. Системи управління інформаційною безпекою;
2. Платформи для автоматизації;
3. Системи моніторингу мережі;

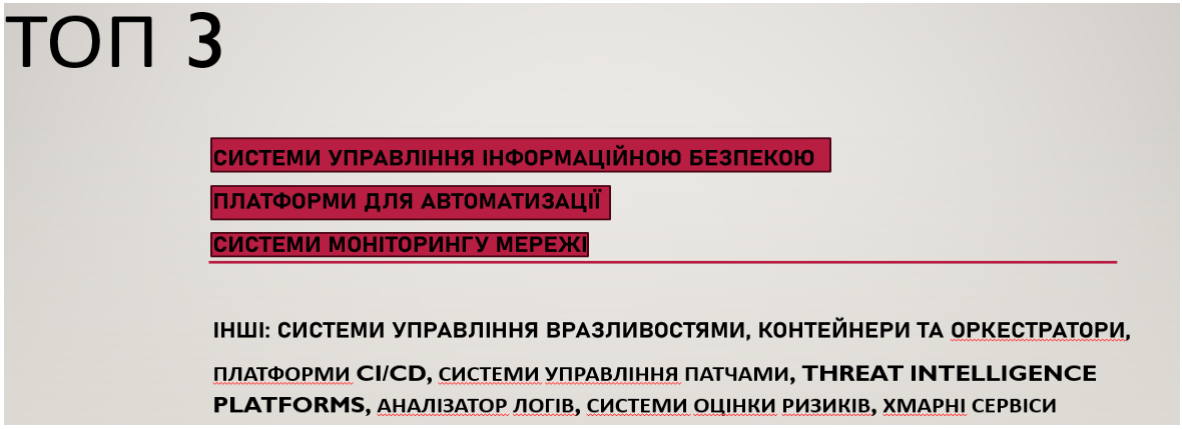

Рис 1.3 Перелік засобів інтеграції систем виявлення вразливостей [27]

Розглядаючи більш детально кожний з топу цих засобів, ми отримуємо такий результат:

Перший варіант – Системи управління інформаційною безпекою:

Системи управління інформаційною безпекою – це системи, які керують подіями безпеки, можуть бути інтегровані для автоматичного збору даних про вразливості та шкідливе ПЗ, а також їх аналізу. Системи, як Splunk або ArcSight, можуть обробляти велику кількість даних і надавати аналітику в режимі реального часу.

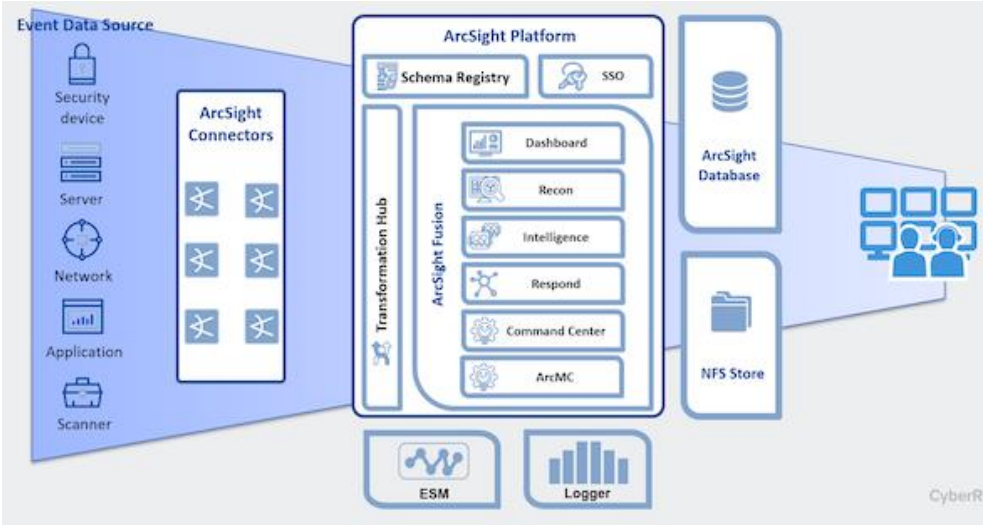

Рис 1.4 Архітектура платформи ArcSight [26]

Другий варіант – Платформи для автоматизації:

Платформи для автоматизації. Використання платформ, таких як Ansible або Puppet, для автоматизації процесів управління безпекою може значно спростити інтеграцію систем виявлення вразливостей. Це дозволяє автоматично

налаштовувати, оновлювати та керувати системами безпеки на всіх етапах життєвого циклу самої програми. Завдяки своїй здатності автоматично виконувати рутинні завдання, що зазвичай вимагають значних зусиль з боку адміністратора. Вони дозволяють організаціям створювати шаблони для конфігурацій, які можна легко адаптувати під різні середовища, забезпечуючи однорідність та стандартизацію налаштувань безпеки. За допомогою цих платформ можна не лише автоматично розгортати системи виявлення вразливостей, але й регулярно оновлювати їх, що є критично важливим для захисту від нових загроз. Додатково, інтеграція з системами виявлення вразливостей дозволяє швидко реагувати на виявлені вразливості, автоматизуючи процеси, такі як впровадження патчів або зміна конфігурацій, що в свою чергу знижує ризик людських помилок і підвищує загальний рівень безпеки інформаційної системи. Автоматизація не лише зменшує навантаження на IT-команду, але й дозволяє їй зосередитися на більш стратегічних завданнях, таких як аналіз ризиків та розвиток нових ініціатив у сфері кібербезпеки.

Рис 1.5 Інтерфейс застосунку Puppet в панелі керування [25]

Третій варіант– Системи моніторингу мережі.

Цей варіант передбачає собою інтеграцію з вже встановленними

системами моніторингу, такими як Nagios або Zabbix. Дозволяє не тільки виявляти вразливості, а також мати повний контроль над станом мережі в режимі реального часу. Такий варіант надає можливість швидко виявляти аномалії та можливі загрози, наприклад, виявлення підвищеного трафіку або незвичайних запитів може сигналізувати про спробу атаки або зловмисну активність. Завдяки цій інтеграції, адміністратори отримують можливість миттєво реагувати на аномалії, що в свою чергу знижує ризики кібератак і допомагає зберегти цілісність та конфіденційність даних. Крім того, системи моніторингу можуть автоматично генерувати повідомлення про виявлені проблеми, що дозволяє IT-командам швидше вживати відповідних заходів, покращуючи загальну стратегію управління безпекою в організації. Таким чином, інтеграція таких систем не лише підвищує ефективність виявлення вразливостей, але й сприяє створенню проактивної безпекової культури в організації.

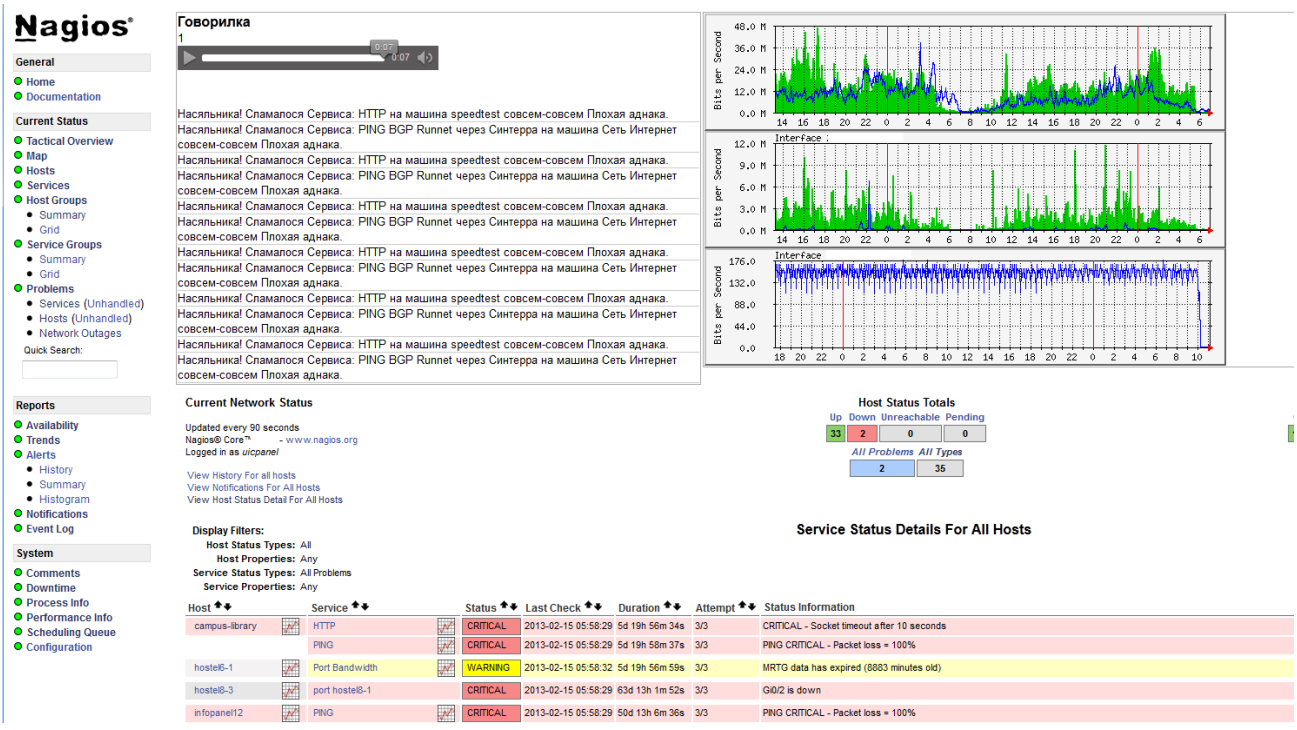

Рис 1.5 Приклад голосового повідомлення завдяки застосунку Nagios [24]

При інтеграції цих автоматизованих систем ми повинні усвідомлювати, що не тільки технічна експертиза зробить їх функціональними в нашому середовищі, але ми повинні відповідати певним вимогам. Організація потребує відповідних ресурсів, людських або фінансових, доброго знання своїх власних

діяльностей і визначення структури інформаційної системи. Без цього інтеграція може бути заплутаною або навіть гіршою.

Проте, незважаючи на численні переваги, прийняття автоматизованих систем виявлення вразливостей стикається з кількома викликами, які потрібно врахувати, і таким чином слід розробити стратегію.

1. Сумісність системи:

Головним викликом в автоматизації систем виявлення вразливостей є те, як зробити нову систему сумісною з різними апаратними і програмними забезпеченнями. Нові системи часто не можуть правильно взаємодіяти зі старими програмами, що може спричинити помилки системи або втрату даних. Це потрібно вирішити на ранньому етапі інтеграції (аналіз/планування), оскільки ми повинні перевірити технічне середовище, щоб бути впевненими, що нове рішення підходить до попередніх (або мати мінімально можливу необхідну ситуацію задокументованою). Нестача відповідної сумісності може потенційно загальмувати підвищення безпеки інформаційної системи.

2. Витрати на впровадження:

Додавання автоматизованих систем виявлення вразливостей породжує потенціал, що дорогі витрати на початку можуть виявитися непередбаченими для інтеграції, і ця можливість повинна бути зважена проти переваг систем виявлення вразливостей на кожному етапі процесу. Ці витрати можуть бути не тільки фактичним придбанням системи, але й будь-якими іншими асоційованими витратами, такими як навчання, конфігурація та підтримка персоналу. З швидко розвиваються технологіями, я припускаю, це може вимагати регулярного включення в бюджет на оновлення та додавання функцій. Тому необхідно заздалегідь врахувати бюджет для інтеграції і забезпечити джерела для довгострокового обслуговування системи.

3. Культурні аспекти в організації, що змінюється:

Коли організація приймає нову технологію, це зазвичай вимагає великої адаптації в культурі організації, можливо, найбільшої перешкоди для інтеграції. Співробітники повинні бути навчені належним чином використовувати нові

інструменти та усвідомлювати небезпеки їх використання. Це передбачає набагато більше, ніж навчання технологіям чи технічному кодексу практики – це про розвиток безпечного «ставлення на всіх рівнях організації». Якщо культурні фактори справді будуть змінені, це може зайняти багато часу і потребуватиме зусиль з боку керівництва для сприяння і мотивації співробітників у адаптації до нових способів роботи.

Отже, можна відзначити, що автоматизація та інтеграція систем виявлення вразливостей є складним завданням, яке вимагає комбінованого підходу до викликів, які можуть виникнути. Глибоке планування, оцінка витрат і зміни в організаційній культурі є ключовими елементами, які можуть значно вплинути на успіх впровадження таких систем.

РОЗДІЛ 2 ПРАКТИЧНА РЕАЛІЗАЦІЯ ВАРІАНТУ ВИКОРИСТАННЯ АВТОМАТИЧНИХ СИСТЕМ З ПОШУКУ ВРАЗЛИВОСТЕЙ

Після дослідження теоретичного матеріалу, було прийнято рішення запропонувати компанії ТОВ «ДК-3», що займається вивченням та дослідженням шкідливого ПЗ систему, котра зможе детектити ймовірні загрози на тестовому сайті, а також обмежувати користувачів видаленого робочого столу, що належить компанії у використанні неправомірних по посаді процесів. Було розроблено план, що обув затвердженим керівником практики задля «парі» між кодерами що займаються шкідливим ПЗ, та юним новачком, котрий має бажання довести знавцям що має собі ціну.

Після обговорення плану, була створена певна таблиця, до якої було включено наступні колонки:

1– Посада;

2 – Можливі процеси;

3 – -Дозволені посилання;

4 – Реагування;

5 – Заборонені процеси.

Записавши усі данні, ми отримуємо таку таблицю:

Таблиця 2.1.

Посада	Можливі процеси	Дозволені посилання	Заборонені процеси	Реагування
Head Of Team	Відкривання CRM, Admin-панелі. Використання софту для аналізу шкідливого ПЗ, процеси Windows котрі вмикаються з вмиканням Windows	Google.com, усі сайти з протоколом https://	–	У разі виявлення загрози порушення прав, система надсилає повідомлення на Admin-панель, де Head підтверджує правильність дій або використовує функцію карантин
Assistant Of Head	Відкривання CRM, Використання софту для аналізу шкідливого ПЗ, процеси Windows котрі вмикаються з вмиканням Windows	Google.com, усі сайти з протоколом https://	Спроба відкриття Admin-панелі	У разі виявлення загрози порушення прав, система автоматично блокує користувача, відібравши повністю всі права, та перезапускає робочий стіл у форматі безпечного запуску, до момента підтвердження керівником відділу правильність дій.
HR Recruiter	Відкривання CRM, процеси Windows котрі вмикаються з вмиканням Windows	Google.com, усі сайти з протоколом https://	Спроба відкриття Admin-панелі, Використання софту для аналізу шкідливого ПЗ	У разі виявлення загрози порушення прав, система автоматично блокує користувача, відібравши повністю всі права, та перезапускає робочий стіл у форматі безпечного запуску, до момента підтвердження керівником відділу правильність дій.
Middle Developer / Malware Analyst	Використання софту для аналізу шкідливого ПЗ, процеси Windows котрі вмикаються з вмиканням Windows	Google.com, усі сайти з протоколом https://	Спроба відкриття CRM або Admin-панелі, перехід на посилання youtube.com, jut.su, anilibria.com.	У разі виявлення загрози порушення прав, система автоматично блокує користувача, відібравши повністю всі права, та перезапускає робочий стіл у форматі безпечного запуску, до

				моменту підтвердження керівником відділу правильність дій.

Аналізуючи дані із таблиці 2.1. можна побачити заборону для категорії Middle Developer, Malware Analyst відкривати Youtube, та дивитися аніме на роботі, чим майже усі працівники полюбляли займатися, та це є проблемою, через яку втарчався потенційно зароблений прибуток. Щодо інших заборон, це всім і так відомо, але у разі загрози одного облікового запису можна буде отримати повністю всі дані, саме тому такий план був розроблений.

Після отримання усієї інформації та узгодження простору для роботи, була надана сума у розмірі 1000$, що є не великими витратами для малої корпорації, кейси котрої починають свою суму від 2500$. Звичайно, усі витрати повинні були відправитися на бухгалтерію, та я отримав прохання максимально зекономити, адже проект був тестовим, можна сказати як жарт, та навряд чи буде використовуватися, саме тому зараз ми наближаємося до вибору інструменту та практичної частини.

2.1 Вибір інструменту та аналіз функціоналу для виконання завдання.

Ознайомившись з декількома інструментами, та дослідивши їх функціонал, моїм вибором став інструмент «OSSEC», адже з переваг він є безкоштовним та працює на вже захищеній системі, аналізуючи її поведінку, конфігурацію та журнали подій, а це саме те що нам потрібно.

Почнемо з теоретичної частини, що саме таке OSSEC, де його використовують та що він робить. Що таке OSSEC? [30]. OSSEC (Open Source Security Events Correlation) – це система виявлення вторгнень на основі хосту з відкритим вихідним кодом (HIDS). OSSEC – це повноцінна платформа для моніторингу та контролю ваших систем. Як відкрите програмне забезпечення, OSSEC дозволяє компаніям досягати своїх цілей у сфері безпеки, миттєво виявляючи загрози. У цій статті ми розглянемо деякі ключові аспекти OSSEC –

від моніторингу файлів до аналізу журналів та виявлення атак.

OSSEC є гнучким інструментом безпеки, який можна розгорнути на різних платформах, таких як локальні мережі або хмарні технології. Основна функція OSSEC полягає в аналізі даних і дії на підставі виявлення шкідливої активності в журналах повідомлень. Він складається з кількох частин:

1. Агент: Встановлюється на кожному сервері (або комп'ютері), який слід моніторити. Агент отримує інформацію про системні події та відправляє її на сервер.
2. Сервер: Головна система, що отримує інформацію від агентів, обробляє та звітує.
3. Веб-інтерфейс: Дозволяє адміністраторам бачити результати аналізу, конфігурувати систему та отримувати сповіщення про виявлені загрози.

З основних функцій цього інструменту можна створити певний перелік:

1. Моніторинг файлів: OSSEC має можливість відстежувати зміни у файловій системі. Це особливо корисно для моніторингу невизначених змін, внесених до конфігураційних файлів, системних файлів та важливих даних.

- Функціональність:
  - Визначення відмінностей між файлами (додавання, видалення, модифікація).
  - Моніторинг доступу до файлів та їх дозволів.
  - Отримання попереджень на основі підозрілих змін.

2. Аналіз журналів: OSSEC обробляє журнали подій з різних систем, включаючи операційні системи, додатки та мережеві пристрої.

- *Функціональність:*
  - Збирання журналів з багатьох систем в одне місце.
  - Перегляд журналів для виявлення аномалій та команд (наприклад, невдачі паролів, зміни в системі).
  - Ідентифікація повторюваних шаблонів або аномальних дій.

3. Виявлення атак: OSSEC включає в себе більше, ніж просто інструмент для пошуку атак проти системи. Це поширюється на активне спостереження за

поведінкою користувачів та системи.

- *Функціональність:*
  - Ідентифікація спроб вторгнення (груба сила).
  - Реагування на виявлені загрози шляхом автоматичного блокування IP-адрес або повідомлення адміністраторів.
- Створення звітів у відповідь на виявлені атаки та їхню природу.

Далі переходимо до самого парктичного підходу рішення.

2.2 Інсталяція інструменту, налаштування та нові проблеми.

Отже після вибору інструменту, ми переходимо до його установки на сам сервер, де й будемо усе це робити.

Першим етапом нам потрібно знайти сам інструмент на просторах інтернету, адже за рахунок того, що він є безкоштовним, деякі елементи коду мали бекдори, саме тому довелося перевіряти наявність на загрози через VT(Virus Total).

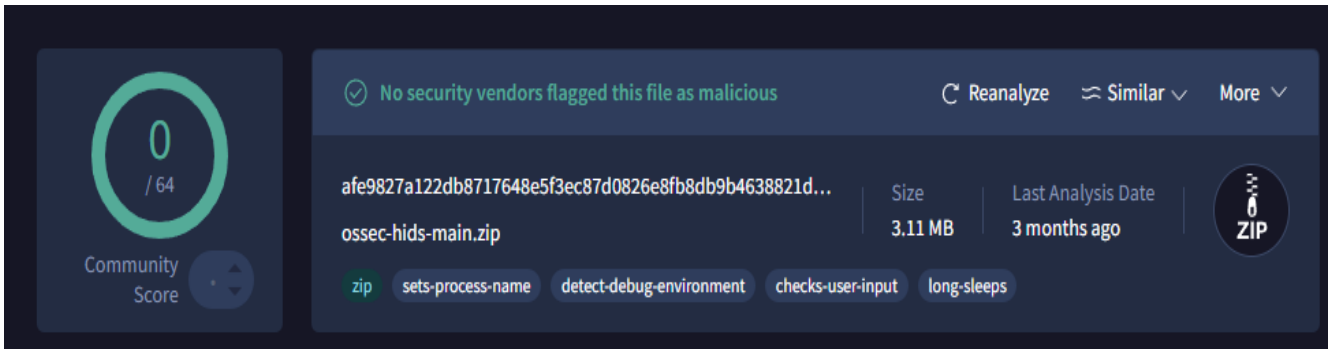

Рис 2.1 Перевірка інстурменту OSSEC на наявність загроз через VT

Після перевірки на ймовірні бекдори та експлойти, ми починаємо готувати систему для інсталювання пакету інструментів OSSEC та усіх помічників до нього.

Першим кроком встановлюємо WINSCP для отримання доступу до самого серверу, та щоб мати змогу керувати самими файл

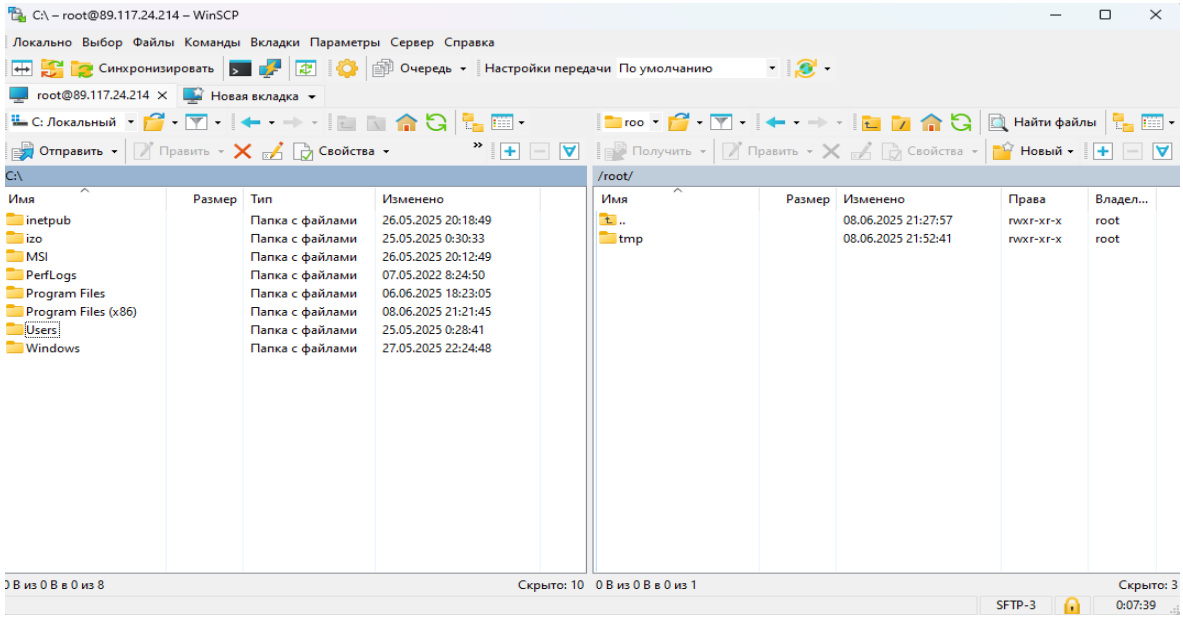

Рис 2.2 Інтерфейс програми WinSCP до вже підключеного серверу

Другим кроком є встановлення додаткового інтерфейсу консолі Putty, за декілька років користування я звик саме до нього, саме тому використовувати його буду й подалі. З переваг я можу віднести синергію з інструментом WinSCP, та простоту в користуванні, зручна панель без недоліків, можливо наразі маються інтерфейси зручніші аніж цей, але золоте правило програміста є: «Працює – не чіпай».

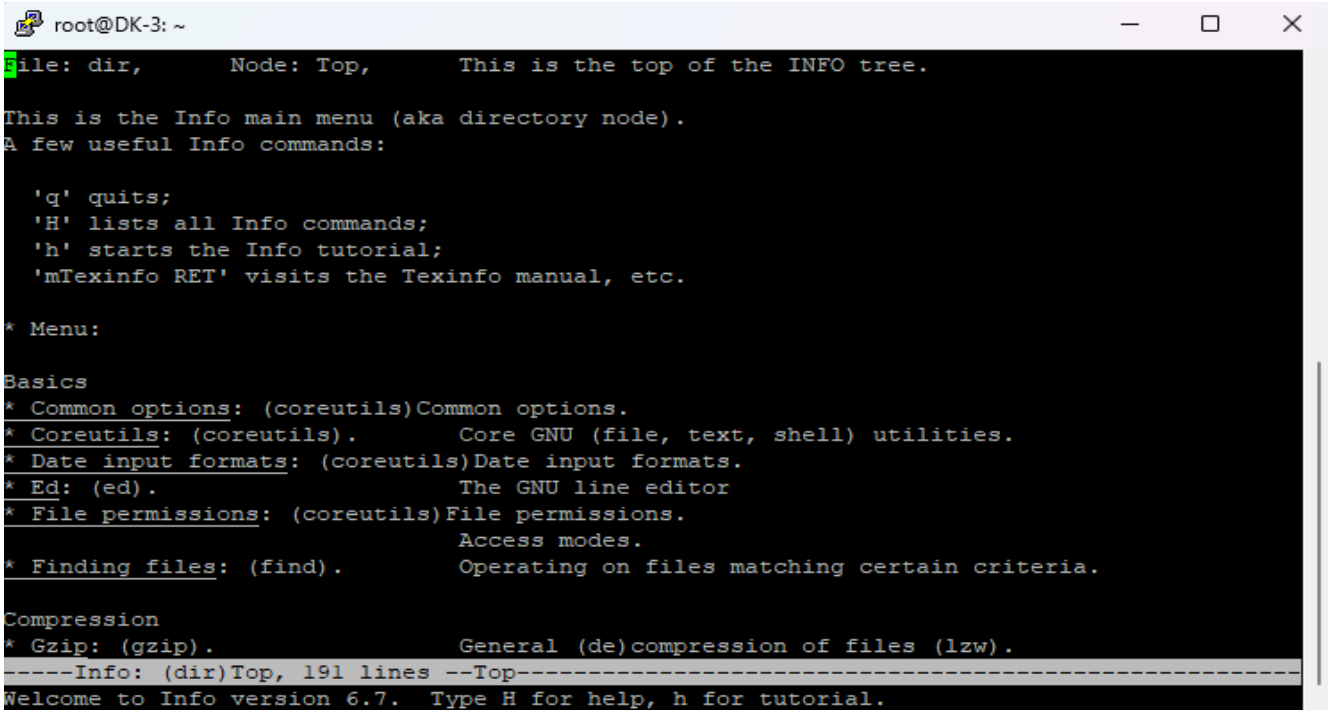

Рис 2.3 Консоль Putty до вже підключеного серверу ТОВ DK-3

Після підготовки усіх інструментів, ми переходимо до консолі налаштування VDS серверу, та інсталюємо пакет файлів для OSSEC.

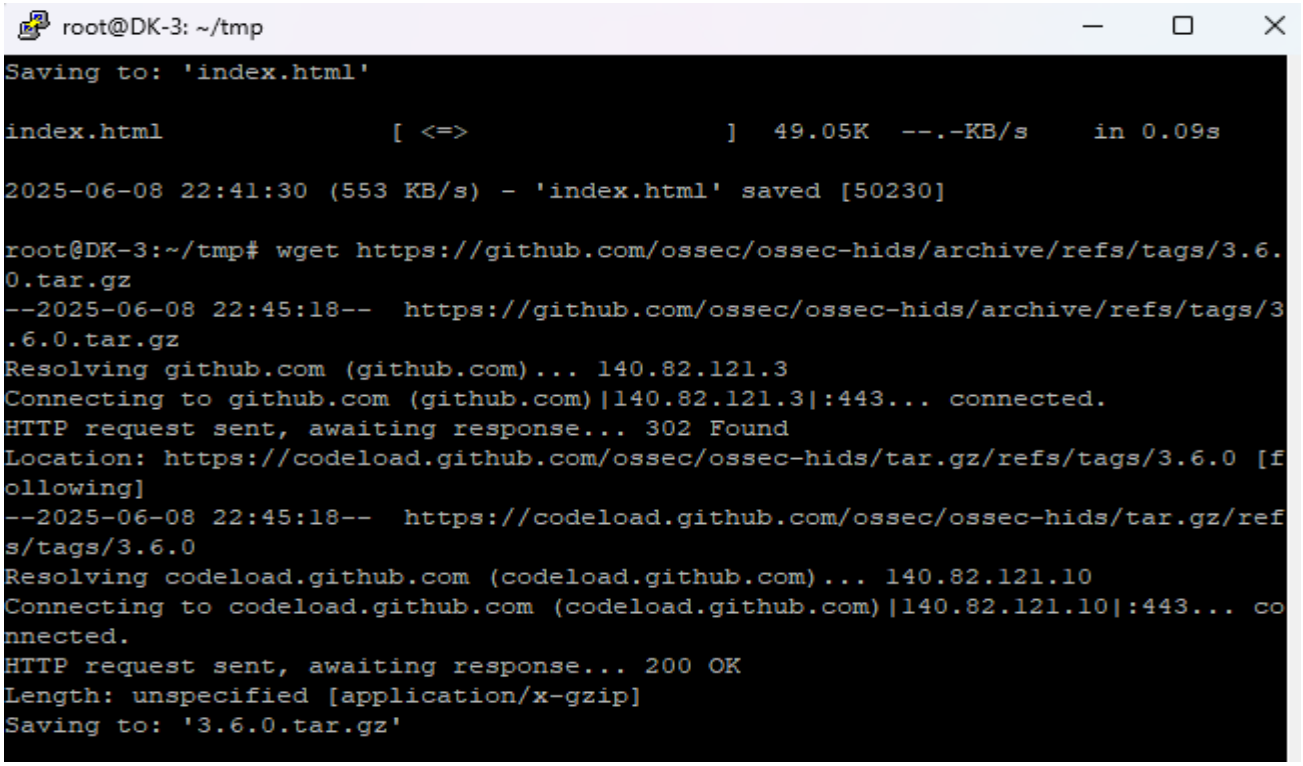

Рис 2.4 Процес встановлення інструменту OSSEC

Одразу як завантажили сам пакет файлів, ми розархівовуємо його.

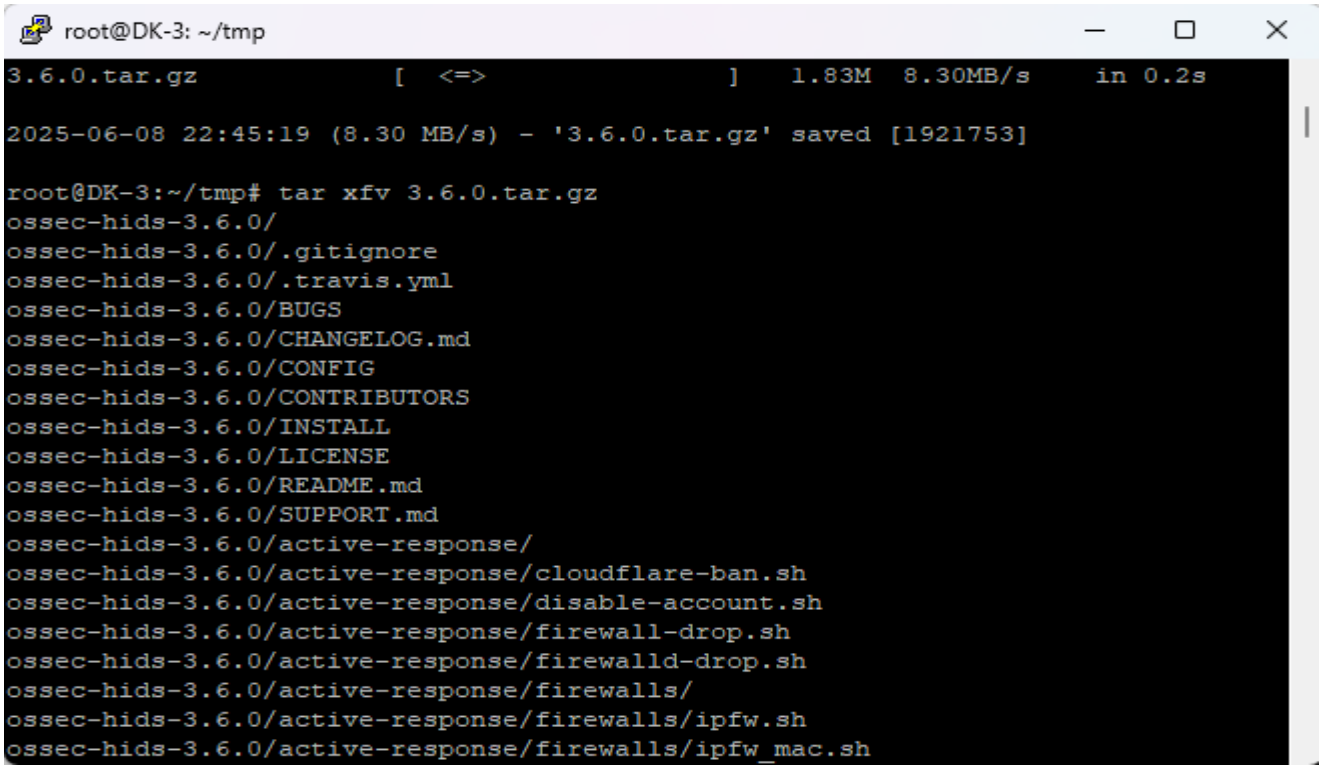

Рис 2.5 Розархівування архіву файлів для інструменту OSSEC

Тепер нам потрібно перейти у директорію ossec-hids-3.6.0, та дістати необхідні бібліотеки, щоб їх інсталювати. Вони безкоштовні, що є великим плюсом для корпорації, адже на даний момент з усіх витрат є лише 16$ на сам сервер, але в подальшому ми звернемося до платних бібліотек, з допомогою яких ми зможемо використовувати більший функціонал.

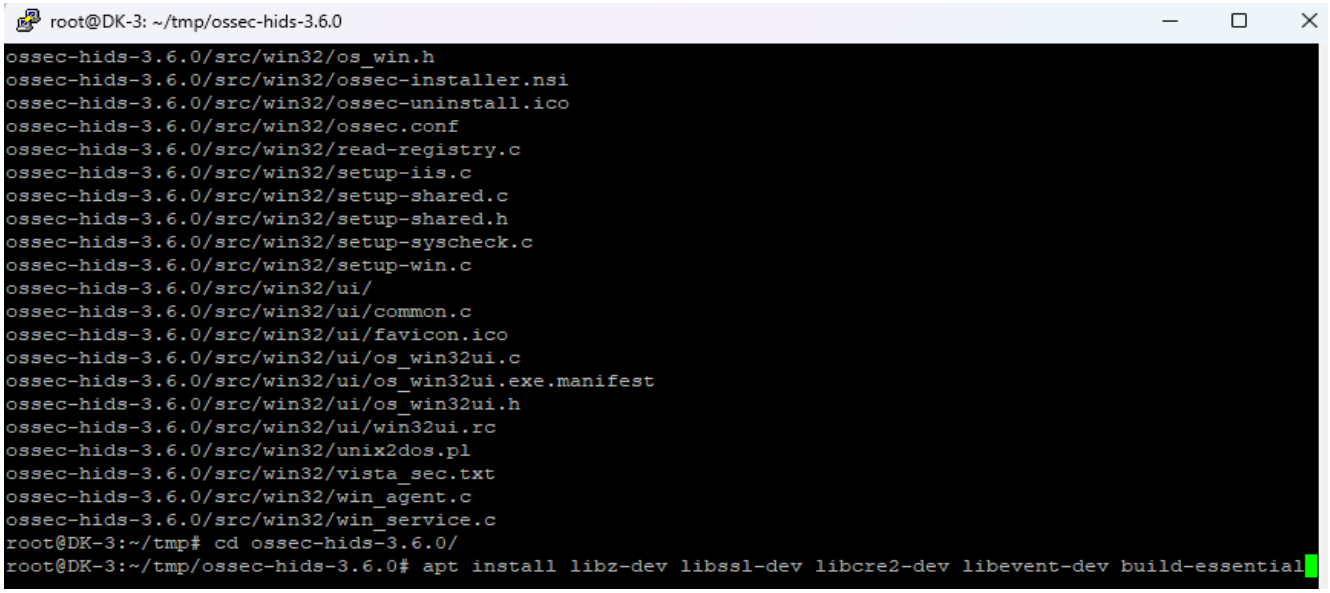

Рис 2.6 (Подання запиту на сервер для інсталяції необхідних бібліотек)

Також до бібліотек була додана можливість надсилання листа на електронну пошту, з якої ми і будемо керувати усіма процесами, як адмін панель.

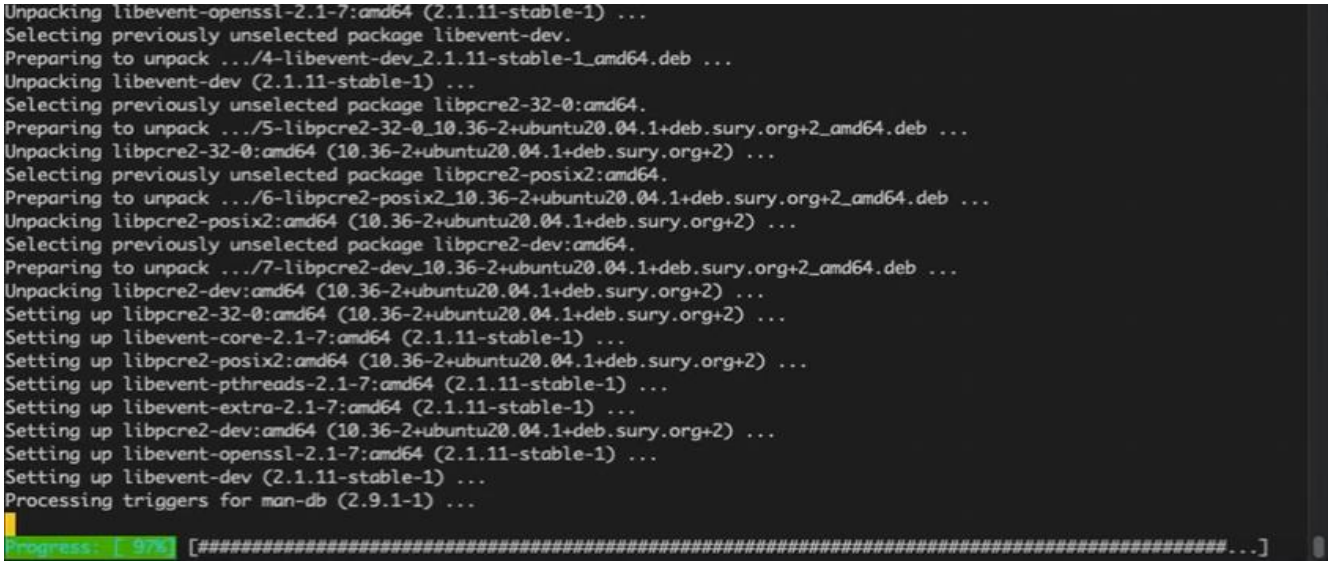

Рис 2.7 Встановлення на сервер самих бібліотек, з додаванням змоги відправки електронної пошти

Після того, як наш сервер надав позитивну відповідь щодо встановлення усіх бібліотек, ми перевіряємо чи все правильно стоїть, командою терміналу: *ls*

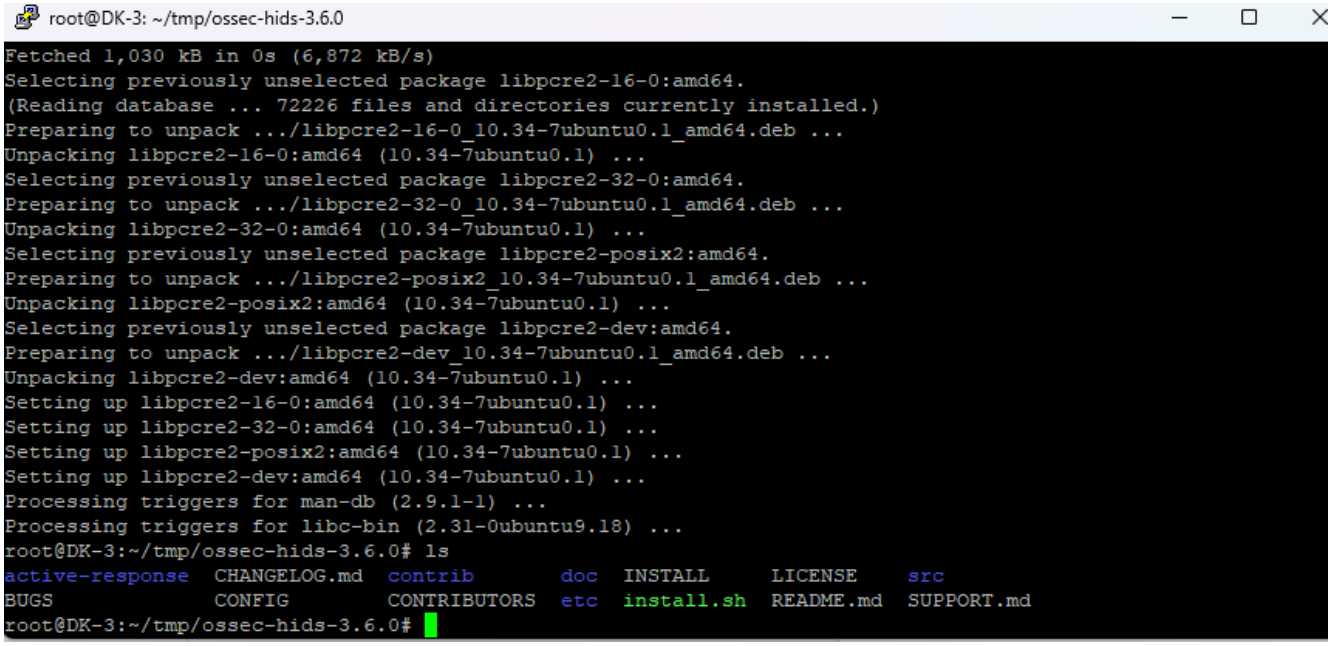

Рис 2.8 Перелік встановлених файлів у папці tmp

Перша частина практичного завдання майже виконана, все що необхідно зробити, це запустити процес встановлення самого інструменту, це ми зробимо командою:

bash install.sh

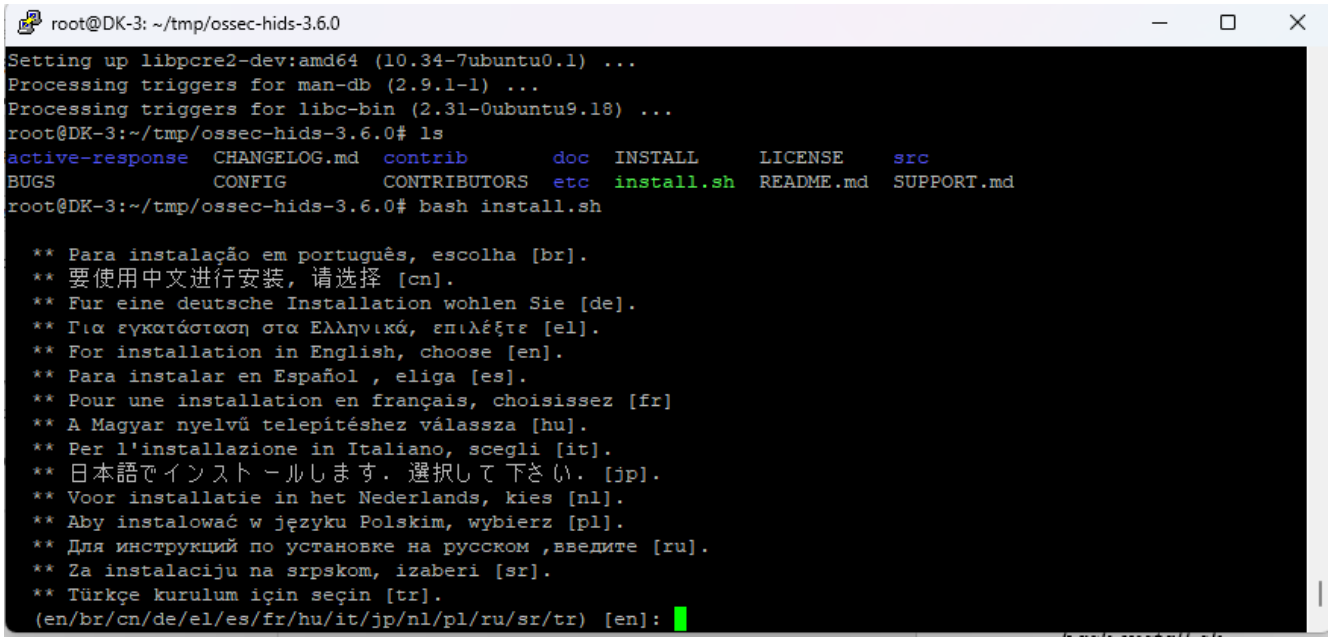

Рис 2.9 Меню інсталятора директорії ossec-hids

Після запуску команди, інструмент пропонує нам обрати мову для коду, ми залишаємо англійську, та тиснемо ENTER, після чого обираємо тип встановлення директорії як server, написавши відповідь на запитання:

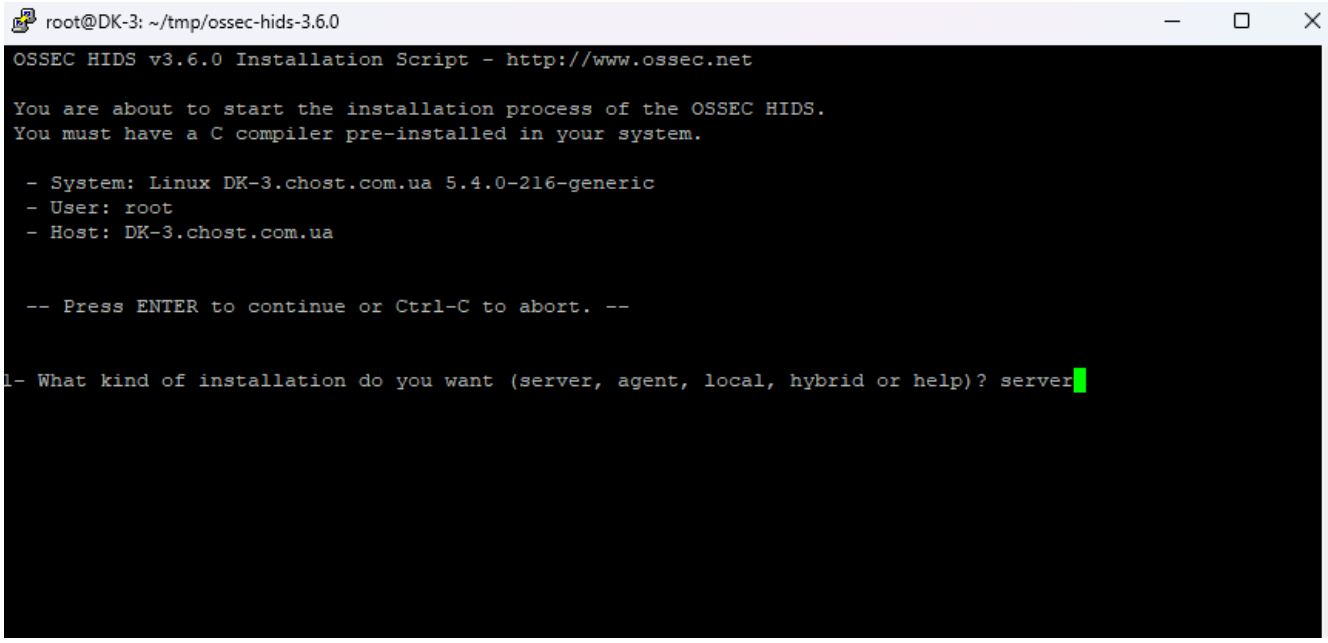

Рис. 2.10 Вибір типу інсталяції для інструменту

Далі йде сам процес встановлення, а саме налаштування: Директорія інсталяції, повідомлення на електрону адресу, вказання самої електронної адреси, вибір свого SMTP серверу, перевірка цілісності файлів, процес виявлення та аналізу руткитів (rootkit), використання активних відповідей, заборону або блокування мережевого трафіку, додання інших IP адрес у WL, та керування передачою файлів.

Тепер щодо самого налаштування, ми отримуємо таку конфігурацію:

1. Kind of server (server, agent, local, hybrid or help): server
2. Installation environment: /var/ossec
3. E-mail notification: yes
4. Your e-mail address: hbggff9@gmail.com
5. Do you want to use SMTP server as google.com: no
6. Whats your SMTP server?: localhost
7. Do you want to run the integrity check demon?: yes

8. Do you want to run the rootkit detection?: yes
9. Do you want to enable active response?: yes
10. Do you want to enable firewall-drop?: yes
11. Do you want to add more IPs to WL: 192.168.1.15
12. Do you want to enable remote syslog?: yes

Після вдалого задання конфігурації, інструмент переходить до компіляції.

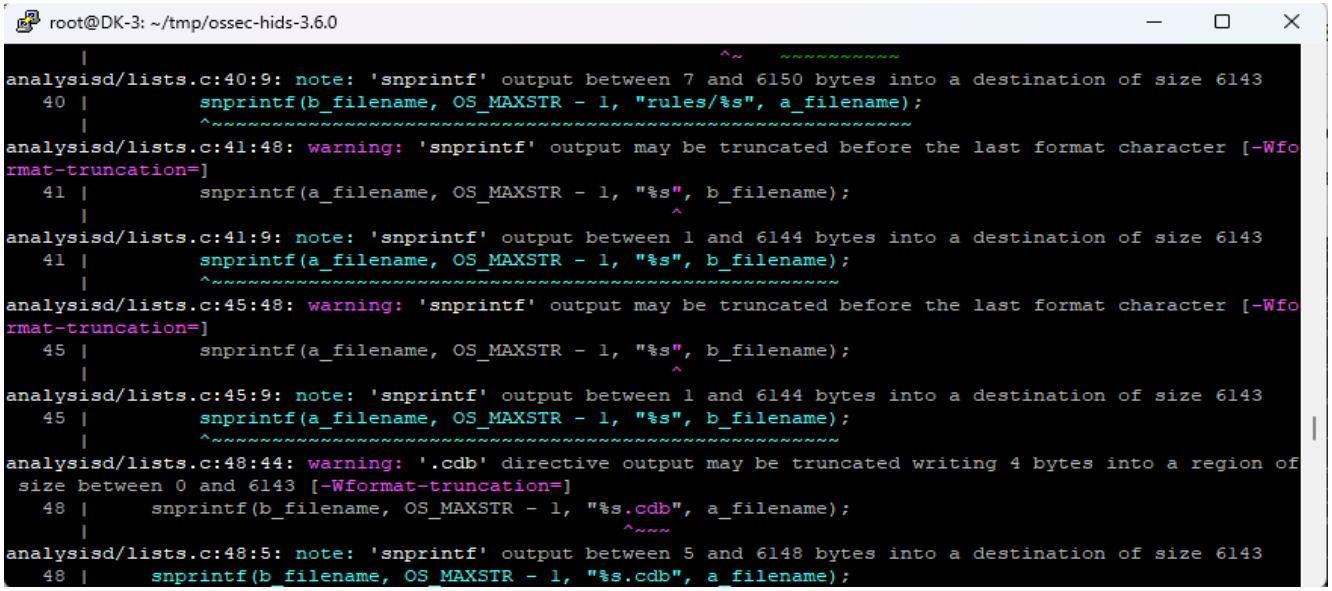

Рис 2.11 Процес компіляції інструменту

Одразу після вдалої компіляції, інструмент повідомляє нам, що все зроблено правильно, та пропонує нам перейти до завершення процесу інсталяції (рис 2.12).

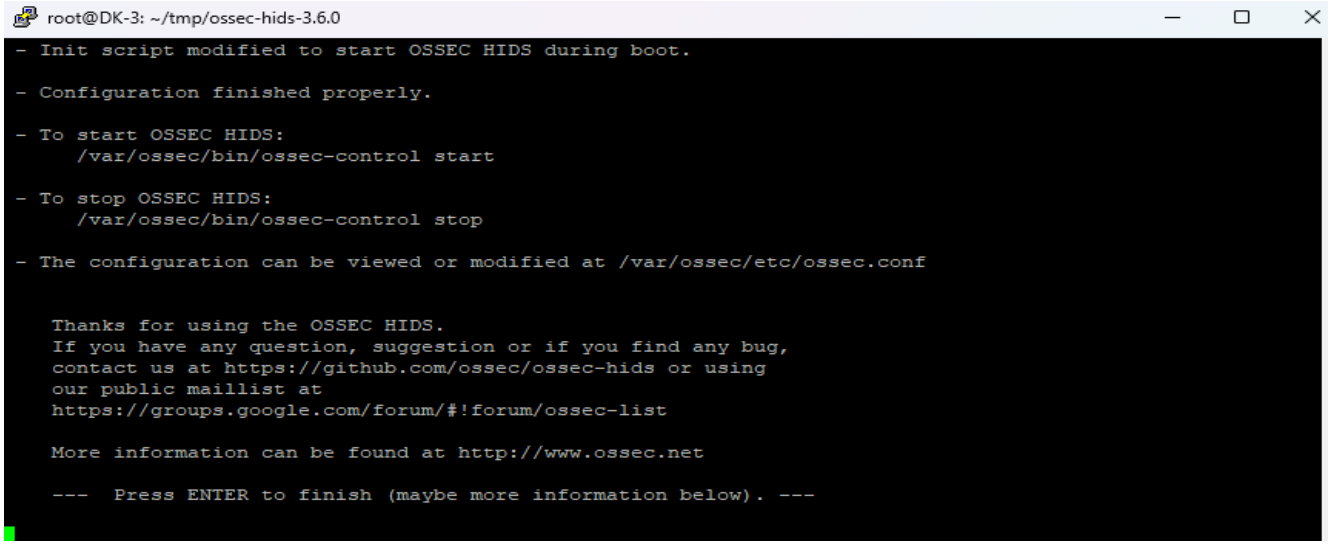

Рис 2.12 Вітання інструменту щодо завершення процесу інсталювання

Як тільки процес інсталяції буде завершено, ми переходимо до бібліотеки /vaar/osec, та видаляємо функцію send e-mail, тому що функціонуюча система не надасть нам змоги відсилати необхідні листи на електрону пошту. Замість цієї бібліотеки ми будемо використовувати SMTP сервер Postfix, на базі WAZUH.

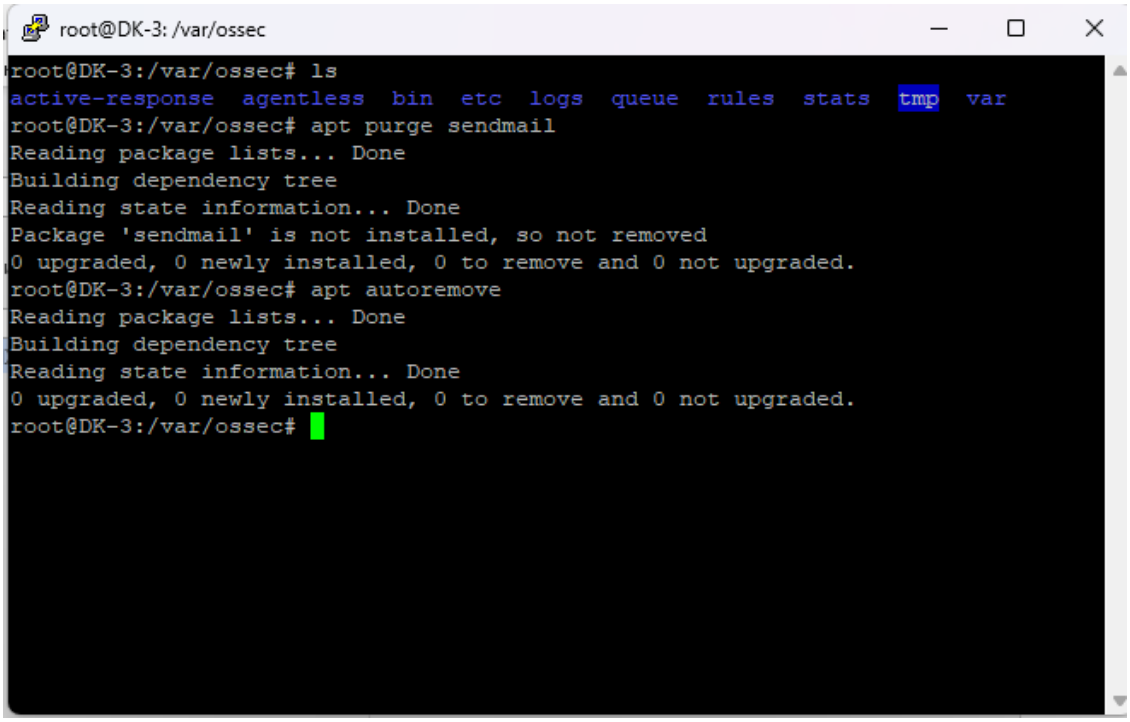

Рис 2.13 Видалення бібліотеки sendmail

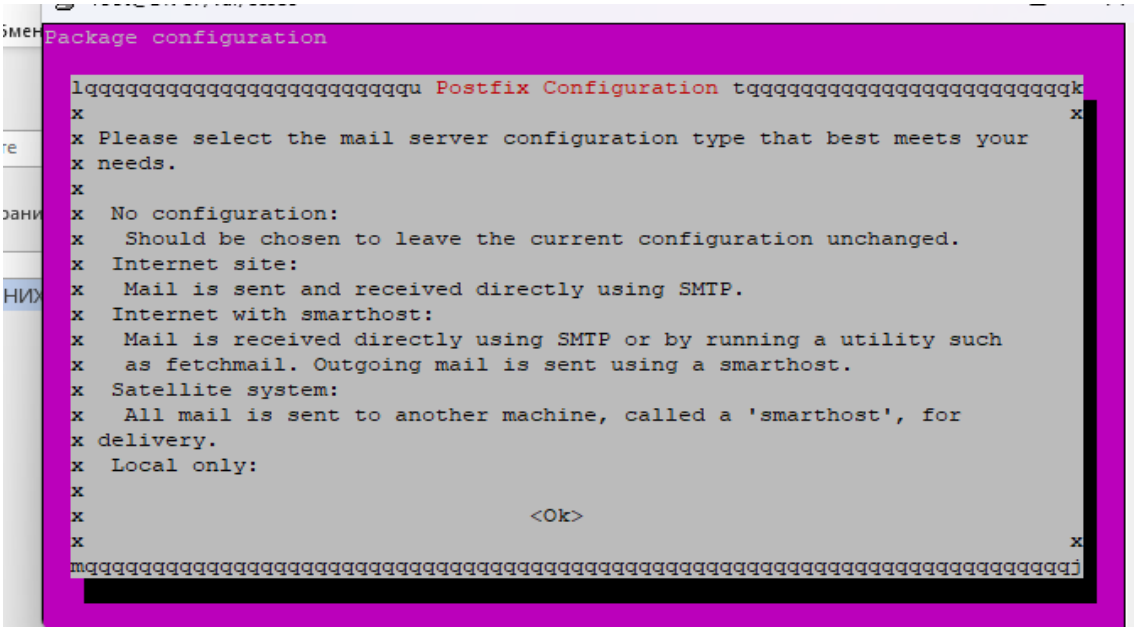

Рис 2.14 Привітання SMTP серверу POSTFIX

На рис 2.14 ми бачимо що інструмент повідомляє нас про можливості функціоналу, та просить нас обрати необхідний тип конфігурації, ми обираємо

Local only, що буде надавати нам змогу в подальшому відкрити свій сертифікат, через який ми зможемо отримувати CMC.

Після вибору необхідної мережі та введеня хосту, нам необхідно відкріті файл конфігурації Postfix командою: vim /etc/postfix/main.cf , скролимо до самогу низу доки не знаходимо параметр: «smtp_tls_session_cache_database», та видаляємо усе що нижче, заміняючи на код з документації сайту WAZUH. (рис. 2.15).

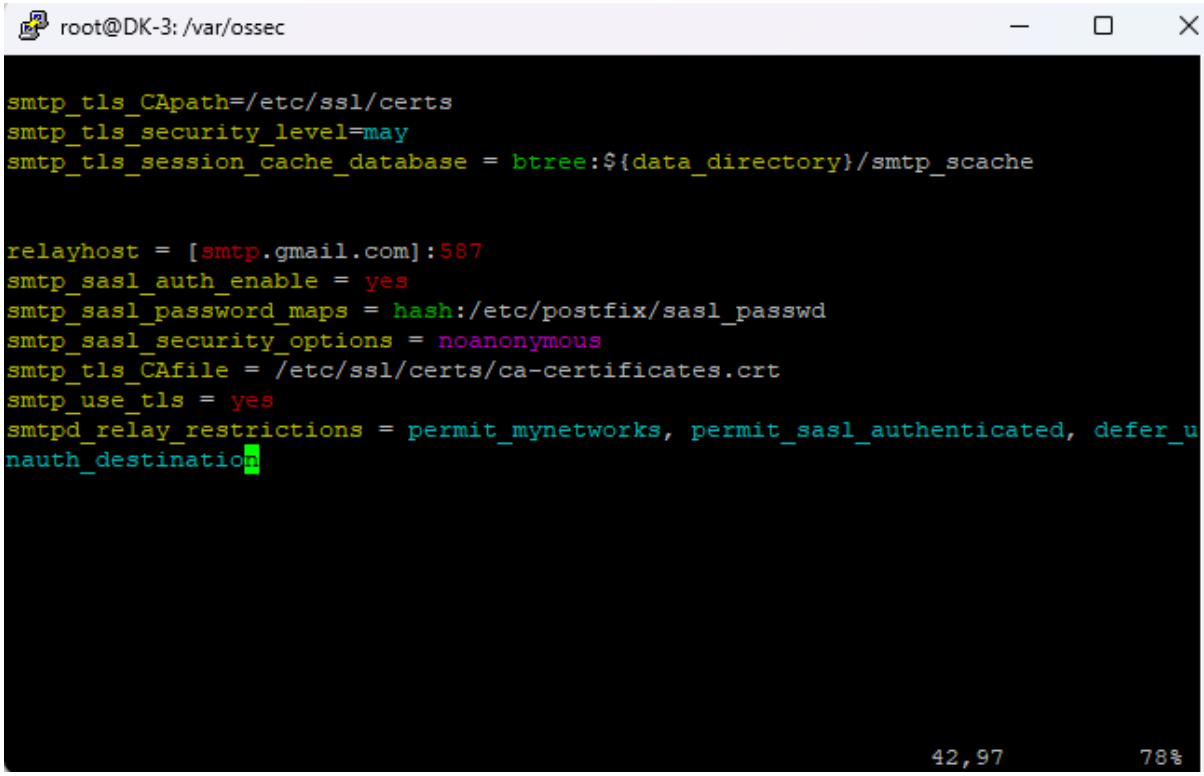

Рис 2.15 Приклад правильного налаштування файлу конфігурації

По завершенню цих дій, ми отримуємо такий результат, але рядок з параметром: «smtp_tls_CAfile» необхідно виправити, залишивши лише /etc/postfix/server.pem.

Як тільки но налаштування конфігу буде завершено виходимо з режиму редактору кнопкою Esc, та вводимо команду: «:wq», одразу перезаходимо в цю папку командою cd, та перевіряємо наявність сертифікату: «/etc/ssl/certs/ssl-cert-snakeoil.pem», переконуємось що він є, та вводимо команду по генерації сертифікату: «openssl req -new -newkey rsa:2048 -nodes -out certreq.txt -keyout private.key». Для першого тесту додаткову інформацію можемо не вводити,

залишаємо усі налаштування стандартними. (рис. 2.16).

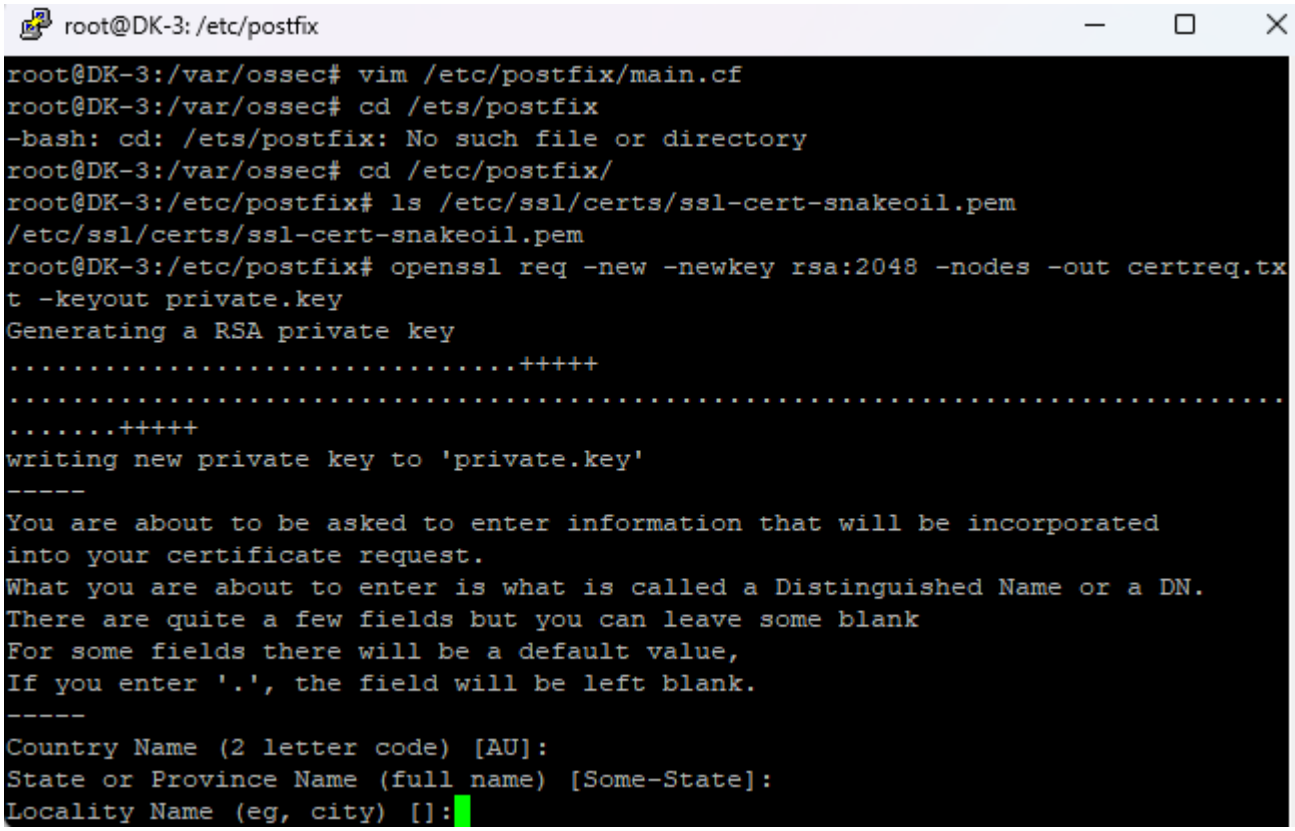

Рис. 2.16 Панель генерації сертифікату для відправки електроної пошти

Важливе зауваження щодо паролю, створити котрий нам запропонує процес створення сертифікату – ні в якому разі його не створюємо! Усі налаштування залишаються незмінними, та генеруємо сертифікат, після чого командою: vim certreq.txt перевіряємо його наявність, та виходимо з нього нічого не змінюючи також. (рис 2.17).

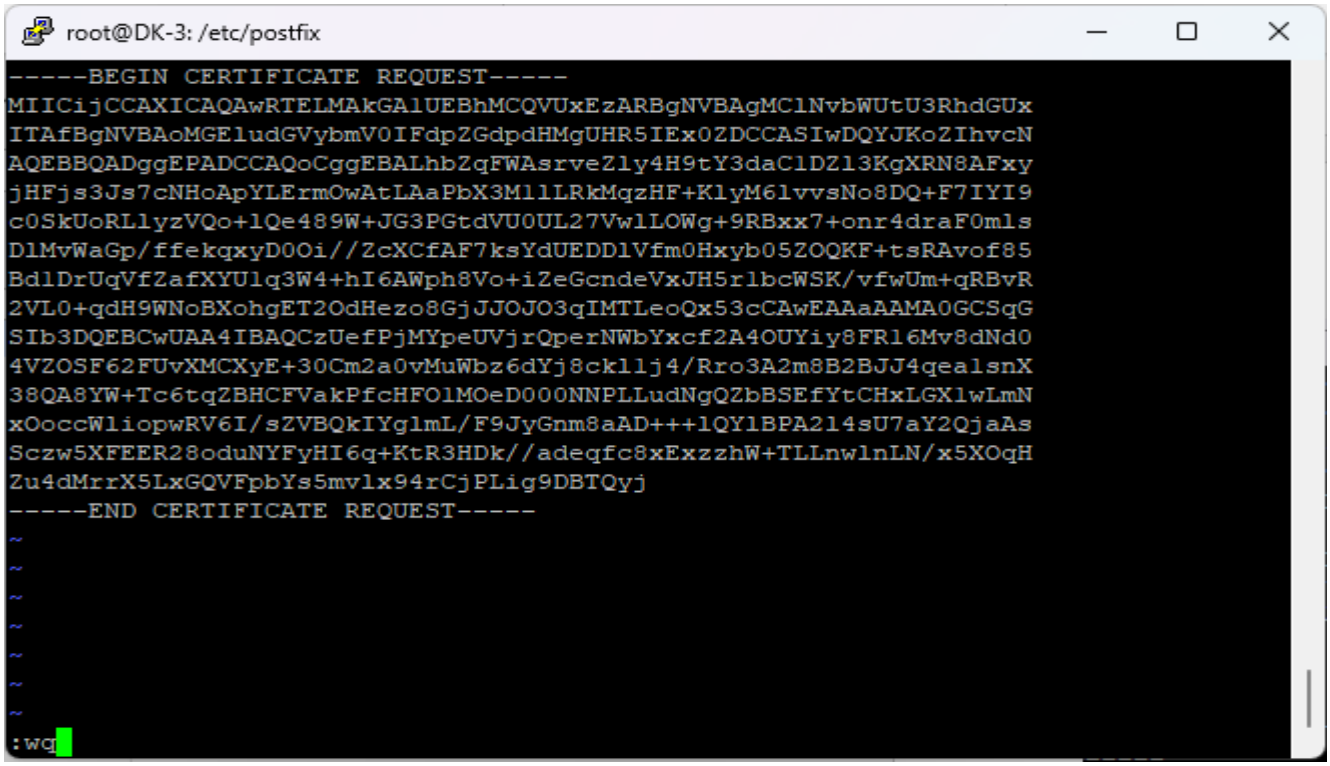

Рис 2.17 Унікальний сертифікат для віпдправлення повідомлень

Далі змінюємо назву документу на “cacert.pem” для подальшого користування, та надсилаємо нову команду: «cat /etc/ssl/certs/ssl-cert-snakeoil.pem cacert.pem > server.pem».

Цією командою ми робимо злияння двух сертифікатів в один, за допомогою котрого ми зможемо отримувати посилання на пошту, а також повідомлення у саму панель, щодо входу небажаних користувачів, а також у разі виникнення підозрілого трафіку (Наприклад: хтось захотів подивитись аніме під час робочого часу).

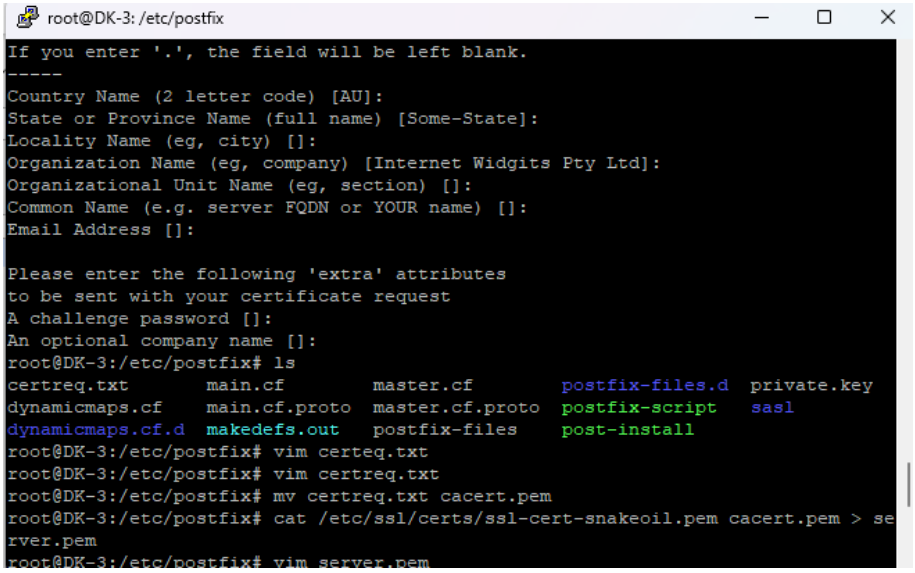

Рис 2.18 Злиття двох сертифікатів в один, котрий буде використовуватися

Тепер, ми налаштовуємо інструмент для входу в саму пошту, на моєму прикладі я це зроблю зі своєю, тому деяка інформація на рисунках біде відсутня.

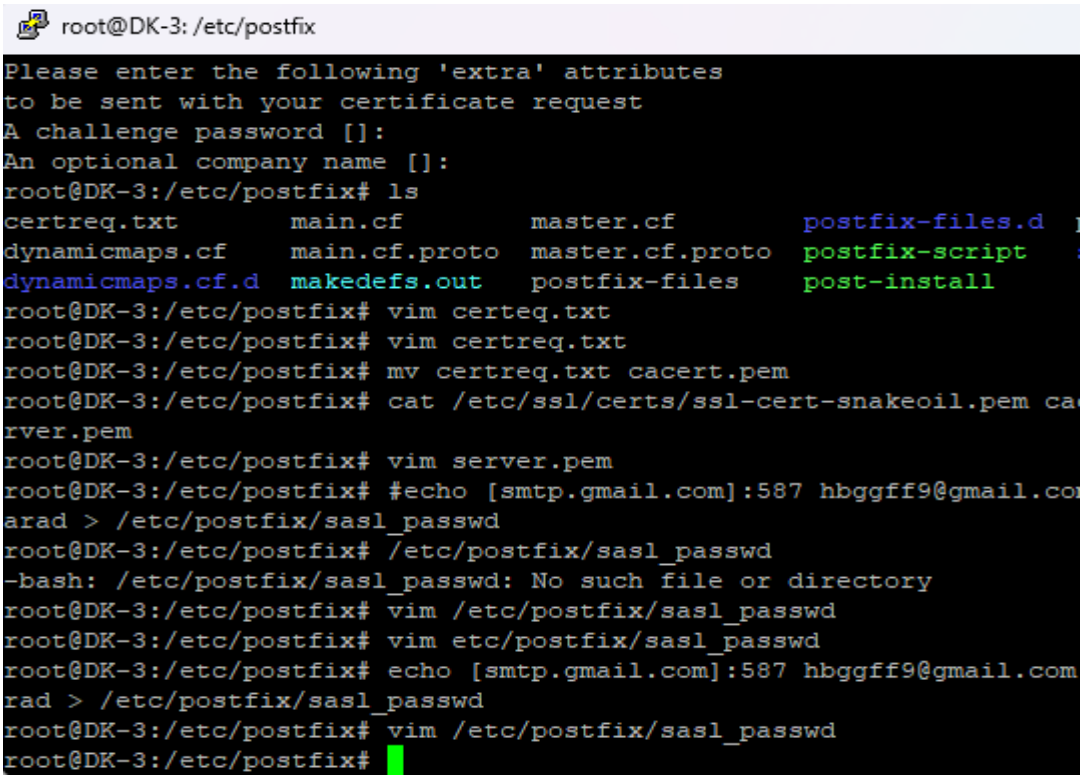

Рис 2.19 Команда налаштування даних для входу в пошту

Після введеної команди перевіряємо, чи всі данні були вставленні правильно, адже деякі можуть бути некоректними через спец-символи, та

виходимо з редактору файлу.

Тепер, по завершенню налаштування надсилаємо тестовий запит на вхід до серверу під ім’ям HR-1 з неправильним паролем, та перевіряємо тестову пошту на працездатність повідомлень та прийняття рішень:

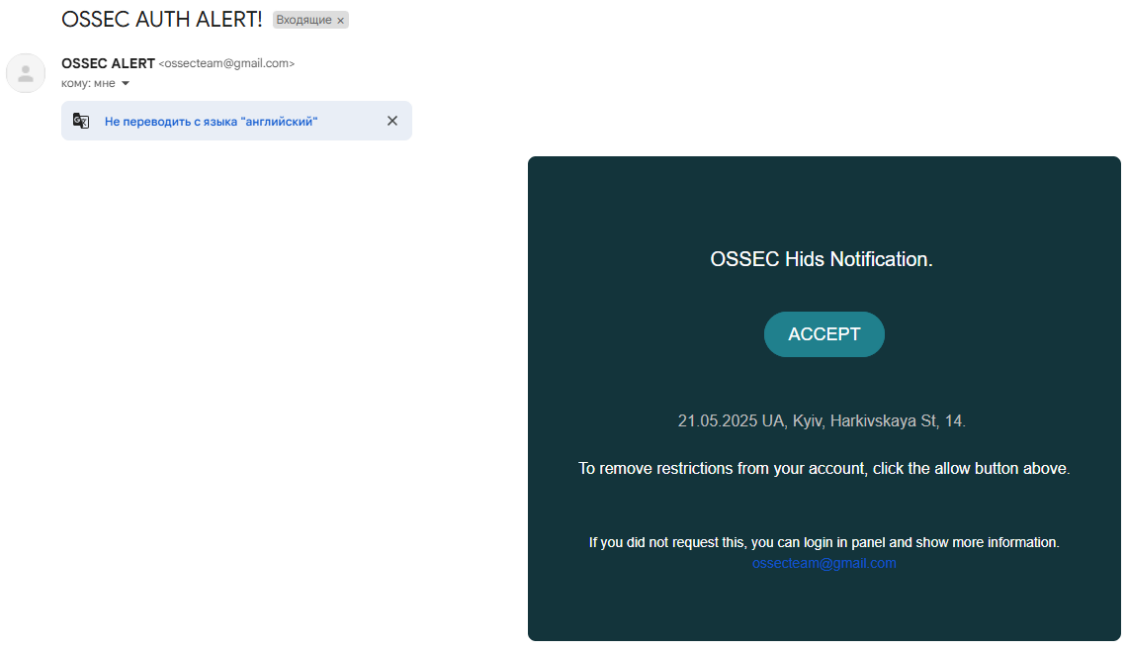

Рис 2.20 Панель повідомлення на електронну пошту після підозрілої авторизації

Таким чином ми інтегрували автоматизовану систему на сервер, який тепер буде якісно захищенний від брутфорсу та невідомих айпі адрес. Невідомі вони будуть завдяки WL, котрий нам пропонував налаштувати сам інструмент OSSEC під час інсталяції.

Тепер ми переходимо до іншої проблеми, а саме небажаного трафіку в гуглі, нажаль заблокувати сам трафік ми не можемо через інструмент, але серверна частина та брендмаузер дозволить нам це зробити через налаштування, а вже сам інструмент буде надсилати нам повідомлення, як тільки побачить на обліковому записі працівників цей трафік, також туди ж ми підв’яжемо необхідні процеси, а саме:

Відкриття CRM Mid Malware Analyst, відкриття адмін-панелі звичайними працівниками, та спроба відкрити сайт з аніме на робочому обліковому запису.

Першим етапом нам необхідно заборонити кожній категорії відкривати певні сайти, це ми робимо таким чином:

– Відкриваємо файл від ім’я адміністратора який розташований C:\Windows\System32\drivers\etc\hosts, та додаємо рядки з текстом: «127.0.0.1 anilibria.com», та інші котрі мають відношення до аніме.

Таким чином усі сайти можна буде переписати, я обрав цей метод, тому що його можна з’єднати з інструментом, насправді було б легше заборонити усі сайти окрім робочих через інструмент, але тоді усім буде відомо щодо заборони, а так на першу спробу відкрити сайт з переглядом свого улюбленого аніме кимось з працівників – одразу викличе увагу керівника, та жарт буде вдалий.

Другим етапом ми налаштовуємо повідомлення щодо заходу на небажаний сайт, це пов’язано з CRM для одних користувачів, та сайтів з аніме для інших. Для початку налаштування повідомлень, ми відкриваємо файл конфігурації інструменту OSSEC для додавання параметру та призначення моніторингу веб-ресурсів командою:

```
<DK-3WARE >/var/log/apache2/access.log</location>
```

Далі створюємо правило у файлі rules/local_rules.xml таким чином:

```
<group name="web-access">
  <rule id="100001" level="5">
    <decoded_as>apache</decoded_as>
    <match>anilibria.tv</match>
    <description>Access to anime site detected</description>
  </rule>
</group>
```

Налаштування самої пошти ми не чіпаємо, адже все було налаштовано вище, тепер перезавантажуємо систему та перевіряємо на сервері під правами Malware Analyst сайт Anilibria.tv:

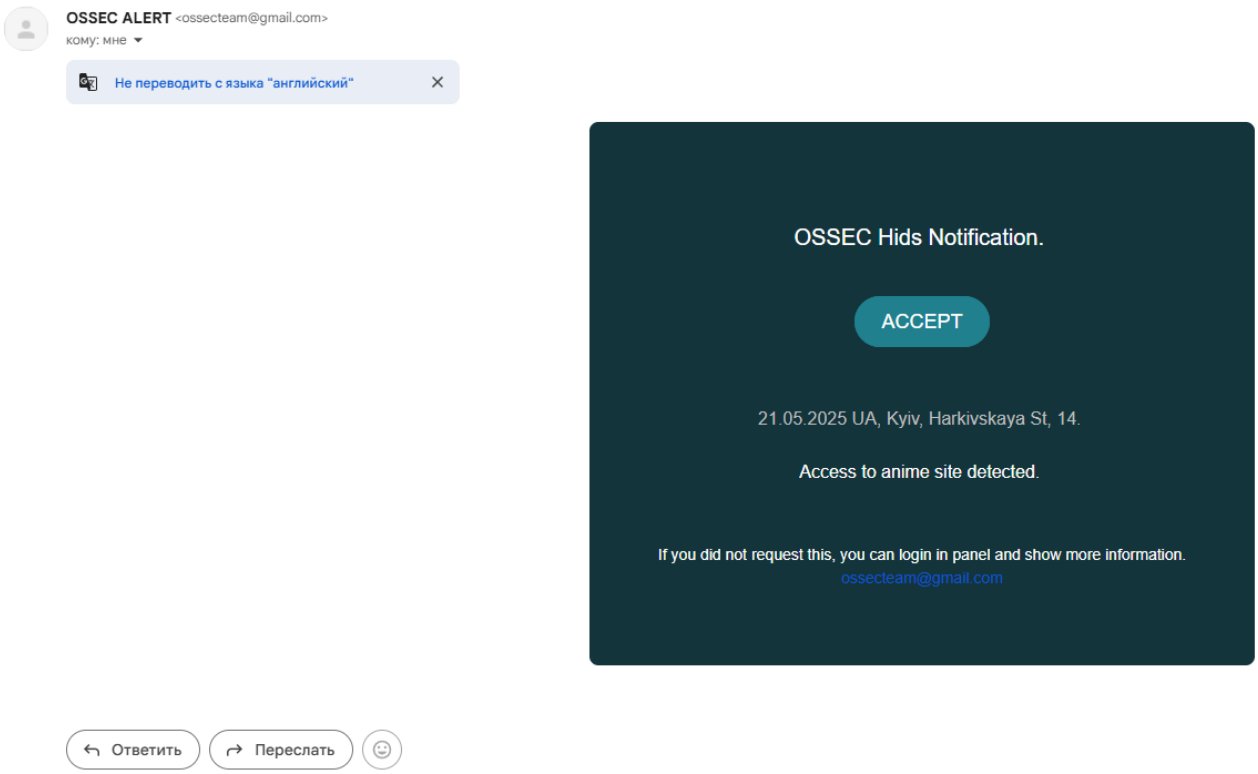

Рис 2.21 Повідомлення від OSSEC на спробу зайти до сайту anilibria.tv

Після виконання процедури з сайтом CRM та адмін-панелі, повторюємо дію, та отримуємо позитивний результат.

2.3. Результати та підсумок практичної частини

По завершенню практичної частини ми отримали доволі таки змішаний результат. З однієї сторони нам вдалося мінімізувати витрати для корпорації та використати малу частину самого бюджету, створивши інструмент для компанії котрий зможе моментально реагувати на спроби атаки за допомогою брутфорсу, реагувати та повідомляти керівництво у разі спроби відкриття файлів або веб-серверів людиною, котра не повинна мати прав на подібні дії. Звичайно, це лише доля від функціоналу самого інструменту, але ціль була максимально зекономити кошти з використанням максимально великої ефективності, і для малих компаній наявність подібного інструменту я вважаю великим плюсом аніж мінусом, тому що при можливій атакі на бази даних OSSEC також зможе

виявити неправомірний доступ та моментально зреагувати на це, запобігаючи втрати компаній як не на мільйони, так на десятки або сотні тисяч гривень в реаліях України. Звісно, є платні версії інструменту з можливостями машинного навчання та варіаціями реагування на подібні обставини, але використавши навіть базову версію інструменту ми отримуємо у результаті надійну систему котра зможе захистити невелику компанію від різних подій, які можуть бути прописані та з легкістю встановленні в конфігуратор інструменту. Нажаль моїх навичок в програмуванні не буде достатньо щоб створити окрему адмін панель компанії, котра буде зв’язана з самим інструментом, враховуючи усі бази даних та інструмент корпорації, але використавши свої знання та матеріал у публічному доступу я зміг створити систему, котра реагує на загрози, і ці загрози можна програмувати, починаючи від невдалих спроб входу, так і переходу на небажанні посилання.

РОЗДІЛ 3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО МІНІМІЗАЦІЇ ВИТРАТ МАЛИМ КОРПОРАЦІЯМ

Після проведеної роботи на тему щодо автоматизаційних ресурсів в корпорації та проаналізувавши їх плюси з недоліками, можна запропонувати рекомендації для малих фірм та корпорацій щодо мінімізації витрат, щоб мати змогу захистити важливі дані та інформацію від зловмисників, котрі наважаються посягнути на їх конфіденційність.

Першим кроком для корпорації буде аналізом можливих ризиків, вони бувають різних типів, та для кожного з них є своє рішення. Також нашу увагу потрібно звернути й на можливі наслідки, до яких може привести все ж таки вдача атака від порушників.

Рис 3.1 Типи ризиків кібербезпеки

Після визначення ризиків, в моїй роботі у другій частині була розглянута крадіжка конфіденційної інформації та спроба компрометації облікових даних ми переходимо до іншого запитання – яка система нам необхідна, для того щоб захиститися від цих самих ризиків?

Таким чином користувачі опиняються серед широкого вибору інструментів, програм, протоколів а також систем, що можуть допомогти захиститися від тієї або іншої кіберзагрози. Нижче нами представлено інструменти з функціоналом, типом коду, а також цінами.

Таблиця 3.1.

Перелік інструментів з функціоналом, типом коду та цінами [13,14,15,16,17,18,19,20,21,22]

Назва системи	**Тип**	**Ціна**	**Основні функції:**
OpenVAS	Відкритий	Безкоштовно	Сканування вразливостей, аналіз конфігурацій
Nessus	Комерційний	~$2,390/рік	Глибоке сканування, управління вразливостями, звіти
Qualys	Комерційний	Від $4,000/рік	Моніторинг безпеки, управління вразливостями, звіти
Burp Suite	Комерційний	Від $399/рік	Тестування веб-додатків, виявлення вразливостей
Acunetix	Комерційний	Від $4,500/рік	Автоматичне сканування веб-сайтів, управління вразливостями
CylancePROTECT	Комерційний	Від $30/пристрій/місяць	Захист від шкідливого ПЗ, моніторинг активності
LastPass	Комерційний	Від $36/рік	Менеджер паролів, захист облікових записів
Dashlane	Комерційний	Від $59.99/рік	Менеджер паролів, моніторинг безпеки
Zscaler	Комерційний	На запит	Захист веб-трафіку, управління доступом
Bitdefender GravityZone	Комерційний	Від $39.99/пристрій/рік	Захист від шкідливого ПЗ, управління вразливостями

Таким чином ми отримуємо результати щодо різних потреб та цін, в якомусь випадку, при наявності лише декількох пристроїв ми можемо використовувати LastPass для захисту облікових записів від потенційних атак, це можуть бути сервіси аутсорсу, де вся інформація зберігається на поштових скриньках, в іншому випадку, коли нам потрібно зберегти безпеку нашої клієнтської бази даних ми можемо використовувати Acunetix, якщо вся

інформація зберігається на сайті.

Саме на подібні випадки нам необхідно звертати увагу до систем або інструментів, що ми плануємо використовувати в подальшому.

Після вибору потреб та інструменту, ми можемо перейти до ще одного способу зекономити кошти, якщо вже володіємо деяким ресурсом, а саме – використання пробних версій, які можуть бути безкоштовні та з відкритим кодом, і гарним варіантом для малого бізнесу аби збалансувати власні витрати на IT-інфраструктуру з їх безпекою даних. У нинішній економічній ситуації, з обмеженими ресурсами, такі пропозиції дозволяють малим організаціям/компаніям/фірмам користуватися потужними додатками без значних економічних витрат.

Безкоштовне програмне забезпечення іноді вважається достатнім для маленьких компаній. Це особливо цінно для стартапів, які починають роботу над проектами і не можуть собі дозволити купівлю дорогих ліцензій комерційних продуктів. Наприклад, ви можете отримати необхідний захист і організацію роботи в безкоштовних « зразках» антивірусного програмного забезпечення або інструментах управління проектами. Це дозволяє малим фірмам зосередитися на розвитку бізнесу, не застрягаючи на витратах на програмне забезпечення.

Альтернативи з відкритим кодом пропонують ще більше можливостей для економії коштів і налаштування. Вони не тільки дозволяють користувачам запускати програмне забезпечення безкоштовно, але також модифікувати його вихідний код, щоб відповідати конкретним вимогам бізнесу. Це корисно, коли компанії мають внутрішніх програмістів, які можуть внести ці зміни. Наприклад, малі підприємства можуть покладатися на системи управління контентом з відкритим кодом для створення та управління своїми вебсайтами, зменшуючи таким чином витрати на розробку та обслуговування.

Звісно, фактор безпеки також є дуже важливим. З вільно доступними версіями з відкритим кодом маленькі компанії можуть залишатися хранителями своїх даних. Наявність вихідного коду робить можливим використання перевірок на уразливості та детекторів шкідливого ПО для визначення

загального рівня безпеки. Більше того, проекти з відкритим кодом часто мають активну базу користувачів і спільноту розробників за ними, і тому вони часто оновлюються і патчуються, що знову ж таки є кроком до безпеки програмного забезпечення.

Отже, для малих компаній безкоштовні та відкриті випуски є одним з найпростіших способів зберегти контроль над даними і підтримувати необхідний рівень безпеки. Ці рішення дозволяють легко налаштовувати інструменти, які можуть використовуватися бізнесом, і вони можуть очікувати, що вони будуть одночасно високо функціональними та безпечними.

Після обрання певної системи, встановлення її в інформаційну систему компанію для подальшого використання. У цьому контексті пропонуємо такі варіанти економії витрат, а саме:

Перший варіант – аутсорсиннг.

Аутсорсинг все частіше використовується як стратегія малими корпораціями для зменшення інвестиційних та операційних витрат на інформаційні системи. Залучення зовнішніх фахівців або компаній для виконання певних завдань дозволяє підприємствам зосередитися на своїх основних бізнес-процесах, одночасно зменшуючи витрати на персонал, технології та інфраструктуру.

Однією з переваг аутсорсингу є можливість доступу до компетентних професіоналів без необхідності постійного їх найму. Це особливо важливо для малих організацій, які можуть бути обмежені в трудових ресурсах і нездатні підтримувати велику IT-команду. За словами The Patriot Ledger через AP, залучаючи зовнішніх експертів, компанії можуть використовувати їхні знання та таланти для значного покращення процесів [23]. Наприклад, малий і середній бізнес може передати за кордон розробку програмного забезпечення або управління системами безпеки, що дозволяє зекономити на витратах на навчання та утримання персоналу.

Крім того, аутсорсинг дозволяє знизити витрати на технологічну інфраструктуру. Постачальники послуг часто мають у своєму розпорядженні

сучасні технології або можуть отримати їх за доступними цінами, що не завжди можливе для малих компаній. Як результат, підприємства можуть користуватися новітніми рішеннями без необхідності інвестувати в дороге обладнання або програмне забезпечення. Це особливо актуально у сфері технологій, де постійні оновлення і модернізації є необхідними, щоб залишатися конкурентоспроможними.

Гнучкість в управлінні ресурсами також доступна при аутсорсингу. Малі підприємства можуть структурувати свої витрати відповідно до коливань ринку, залучаючи зовнішніх експертів за потребою. Це запобігає витратам на утримання надлишкового персоналу під час періодів низького попиту чи спадів. З іншого боку, у часи зростання бізнесу, компанії можуть швидко збільшити обсяги аутсорсингу, щоб впоратися з новими викликами.

Отже, аутсорсинг є ефективним методом для малих компаній скоротити витрати на впровадження системи. Він надає доступ до ресурсів та технологій за запитом, знижує витрати на персонал та інфраструктуру, а також забезпечує гнучкість у управлінні бізнес-процесами.

Другим варіантом, при наявності спеціалістів в сфері IT, які вже знаходяться в компанії, є використання внутрішнього ресурсу.

Використання власних співробітників – особливо IT-відділу – для впровадження та розгортання нових систем є одним із способів для малих підприємств як скоротити витрати, так і зберегти контроль над своїми системами. Самостійне залучення власних експертів дає компаніям змогу обійтися без витрат на зовнішніх консультантів, які можуть бути високими, особливо для тих, хто працює з обмеженим бюджетом. Зовнішні агентства, найімовірніше, не матимуть знань і розуміння специфіки, потреб та викликів конкретної організації — вони могли б без цього обійтися, натомість внутрішній персонал вже знайомий і є ідеальним для налагодження систем, які повною мірою відповідають потребам компанії.

Пов’язана проблема із залученням власних фахівців, а не зверненням до зовнішніх навичок, полягає в тому, що IT-спеціалісти можуть швидше реагувати

на зміни та проблеми, які виникають під час інтеграції проєкту. Вони добре знають поточну інфраструктуру, тому можуть безперешкодно впроваджувати нові технології в існуючу систему. Завдяки цьому ризики помилок усуваються, а бізнес-процеси проходять гладко. Аналогічно, внутрішні експерти компанії можуть швидше навчати інших співробітників, як користуватися новими системами, підвищуючи загальну ефективність.

Використання наявних співробітників для рекрутингу також зберігає дані в компанії. Залучення зовнішніх консультантів може містити ризики, пов’язані з безпекою інформації, оскільки сторонні особи отримують доступ до конфіденційних даних компанії. Крім того, завдання містить менше консультативних елементів, адже експерти вже є в команді, з більшим бажанням зберігати інформацію внутрішньо і дотримуватись політик безпеки.

Використання внутрішніх ресурсів для налаштування системи є доброю альтернативою для малих компаній. Це не лише знижує витрати, але також гарантує ефективність, швидку реакцію та безпеку даних. Внутрішні фахівці можуть визначити потреби організації та перетворити їх у вимоги, що забезпечують не лише успішне впровадження нових практик, але й закладають основу для зростання компанії в майбутньому, а це є великим плюсом як для компанії, так і самих фахівців.

Третім та фінальним етапом щодо економії ресурсу в компанії є максимальна оптимізація витрат на підтримку обладнання та систем, у разі використання рекомендацій з першого та другого варіантів разом із використанням третього – коли усі компанії без систем захисту зможуть отримати таку нагоду найближчим часом, маючи лише бажання та трохи вільного часу на пошуки необхідних варіантів.

Перш за все повинен відмітити, що одним з найкращих варінатів є підтримання українських постачальників програмного продукту, та використання їх обладнання або систем може значно зекономити нам витрати, завдяки прямому контакту з продавцем, який можливо не буде враховувати в ціну продукту подібні параметри як маркетинг та подібні.

Завдяки комунікації з нашими розробниками ми даємо їм змогу просувати свій продукт, надавати відгуки щодо працездатності а також поради щодо подальшого покращення продукції, задля виходу її на європейський ринок товарів у сфері кібербезпеки.

У разі вже встановленої системи та подальшому бажанні підтримувати жорсткий план економії коштів, ми повинні прислуховуватися до аналітики системи, а також її оновлення. Саме завдяки аналітиці ми зможемо отримати певний результат щодо експлуатації інструменту, а завдяки оновленню присунемо ризики щодо використання старих експлойтів, які зможуть задати небезпеку для нашої компанії.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи на тему «Система виявлення вразливостей в інформаційній системі організації» було здійснено комплексне дослідження теоретичних засад, сучасних підходів, програмних рішень, а також практичну реалізацію з урахуванням актуальних вимог до безпеки корпоративного середовища. В рамках цієї роботи розроблялись рекомендації щодо мінімізації витрат малим корпораціям під час вибору за запровадження автоматизованих виявлення вразливостей в інформаційній системі організації. В цілому було отримано наступні результати.

1. Проведено аналіз проблеми, в результаті якого було визначено поняття автоматизованих систем пошуку загроз та шкідливого забезпечення, їх структуру та типи, а також принцип роботи автоматизованих систем у зв’язці з штучним інтелектом, який покращує інструмент, але також може призвести до хибних дій, у разі яких можуть виникнути складнощі.

2. За результатами проведеного аналізу проблеми, створено прототип автоматичного інструменту з реагування на загрози таких як: Спроба авторизації неуповноваженим користувачем у систему, небажаний доступ до веб-ресурсу, спроба авторизації до адмін панелі користувачем без наданих прав доступу.

Таким чином, розробивши невелику систему на базі інструменту OSSEC з відкритим типом файлу вдалося мінімізувати витрати на систему безпеки до вищого мінімуму, отримавши відносно ефективну систему для невеликої компанії, що значно покращує положення в сфері захисту інформації.

3. В роботі надано рекомендації для малих компаній/фірм/організацій, щодо ефективних способів економії витрат у разі вирішення встановлення автоматичної системи з пошуку вразливостей або шкідливого програмного забезпечення. Було проведено дослідження а також вивчення матеріалу щодо систем різних типів, а також цілей щоб забезпечити конфіденційність будь якого з видів айті ресурсу.

4. Представлені рекомендації розроблено у вигляді варіантів та етапів,

починаючи з самої думки над встановленням, вирішенням який саме інструмент потрібен, закінчуючи етапом обслуговування. Варіанти складалися відносно положення в країні, а також певного досвіду у сфері кібербезпеки, що сподіваюся може допомогти деяким компаніям, які не мають змоги витрачати великі кошти на реалізації захисту, але мають великий потенціал у будь якій сфері, що зможе допомогти розвивати економіку нашої країни.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ринок праці та статистика URL: https://secrets.tbank.ru/blogi-kompanij/rynok-truda-v-2024-godu/?utm_referrer=https%3A%2F%2Fwww.google.com%2F ()
2. Інформація щодо штучного інтелекту URL: https://eztuir.ztu.edu.ua/bitstream/handle/123456789/8762/121.pdf?sequence=1&isAllowed=y
3. Інструменти сканування вразливостей URL: https://www.guru99.com/uk/vulnerability-scanning-tools.html
4. Типи вразливостей URL: https://iitd.ua/najkrashhi-praktiki-efektivnogo-upravlinnya-vrazlivostyami/
5. Архітектура платформи ArcSight URL: https://www.anti-malware.ru/reviews/Micro-Focus-ArcSight
6. Використання системи сповіщення Nagios URL: https://arsen-borovinskiy.blogspot.com/2013/02/nagios-voice-notification.html
7. Оцінка IT ризиків URL: https://www.bdo.ua/uk-ua/services-2/audit/it-audit/it-risk-assessment
8. Інструмент OSSEC з практичної частини URL: https://github.com/ossec/ossec-hids/releases
9. Документація Postfix URL: https://documentation.wazuh.com/current/user-manual/manager/alert-management.html#smtp-server-with-authentication
10. Научна бібліотека з автоматизації URL: https://digtvbg.com/files/books-for-hacking/The%20Web%20Application%20Hacker%27s%20Handbook%20-%20Finding%20and%20Exploiting%20Security%20Flaws%2C%202nd%20Edition%20by%20Dafydd%20Stuttard%2C%20Marcus%20Pinto.pdf
11. База знань щодо метрикам та реагуванням URL: https://attack.mitre.org/
12. Оцінка вразливостей систем URL: https://cve.mitre.org/
13. Інструмент OPENVAS URL: https://www.greenbone.net/en/testnow/

14. Інстурмент Nessus URL: https://www.tenable.com/buy

15. Інструмент Qualys URL: https://aws.amazon.com/marketplace/pp/prodview-5g6ecotizcru6

16. Інструмент BurpSuite URL: https://allsoft.ua/p1640183455-burp-suite-professional.html?utm_source=google&utm_medium=cpc&utm_campaign=%7B%7BcampaignName%7D%7D&gad_source=1&gad_campaignid=22363999122&gbraid=0AAAAApZmhIxg7yYVxMQGkq2Gpq4dp0qz5&gclid=Cj0KCQjwmK_CBhCEARIsAMKwcD4vx_QW-hQYge9QAwxZ6SIgXNLI-BPZhUrdb03Vd8rjB8xG58zTFS8aAl1uEALw_wcB

17. Інструмент Acunetix URL: https://soft.rozetka.com.ua/ua/72107751/p72107751/

18. Інструмент CylanceProtect URL: https://store.manageengine.com/mobile-device-manager/

19. Інструмент Lastpass URL: https://www.keepersecurity.com/ru_RU/pricing/business-and-enterprise.html?_gl=1*uv0zn*_up*MQ..*_gs*MQ..&gclid=Cj0KCQjwmK_CBhCEARIsAMKwcD5JSCpTBbfv5UWzVL3Yu3lK7xn-UNM54loa1L6QfHE3x8gBaoTUcQkaAqr4EALw_wcB&gbraid=0AAAAAD8Fm55imZMTkO7MWXUOD5y2QlNox

20. Інструмент DashLine URL: https://www.dashlane.com/getpremium

21. Інструмент Zscaler URL: https://softlist.com.ua/ua/catalog/zscaler-internet-access-

22. Інструмент Bitdefender GravityZone URL: https://www.bitdefender.com/en-us/business/smb-products/business-security

23. Газета The Patriot Ledger URL: https://www.patriotledger.com/story/business/columns/2022/02/16/advantages-outsourcing-your-accounting-and-finance-function-cliftonlarsonallen-llp/6811517001/

24. Інструмент з голосовим повідомленням Nagios URL: https://arsen-borovinskiy.blogspot.com/2013/02/nagios-voice-notification.html

25. Perforce Puppet Blog URL: https://www.puppet.com/blog/estate-reporting
26. Обзор Micro Focus ArcSight URL: https://www.anti-malware.ru/reviews/Micro-Focus-ArcSight
27. Топ вразливостей ІКС URL: https://7eminar.ua/news/7053-top-5-vrazlivostei-iks-yak-zaxistiti-svoyi-sistemi-vid-kiberzagroz
28. Модульна та субмодульна архітектура URL: https://dou.ua/forums/topic/36547/
29. IBM QRadar: The Architecture URL: https://syedhasan010.medium.com/ibm-qradar-the-architecture-e09721ba3205
30. OSSEC WIKI URL: https://ru.wikipedia.org/wiki/OSSEC

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)