

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми гібридного захисту від
шкідливого програмного забезпечення у Windows-мережі»

Виконав студент 4-го курсу групи КБ-19-1
спеціальності 125 «Кібербезпека»

 Андрій Анчис

Керівник доцент кафедри КІ та КБ, к.пед.н.,

 Олена Головня

Рецензент завідувач кафедри КІ та КБ, к.т.н., доцент

 Андрій Єфіменко

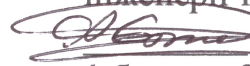
м. Житомир – 2023 рік

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
1 березня 2023 р.

ЗАВДАННЯ

на випускн кваліфікаційну роботу бакалавра

Студент: Анчис Андрій Олександрович

Тема роботи: «Проект підсистеми гібридного захисту від шкідливого програмного забезпечення у Windows-мережі»

затверджена Наказом університету від 1 березня 2023 р. № 99/с

Термін здачі студентом закінченої роботи 10 червня 2023 р.

Вихідні дані до проекту (роботи):

- Топологія мережі.
- Налаштований EDR.

Обладнання та програмне забезпечення:

1. GNS3 – програмне забезпечення для налаштування мережі.
2. Microsoft Defender for EDR – програмне забезпечення для захисту робочих станцій.

Консультанти розділів проекту (роботи)

Розділ	Консультант	Підпис, дата	
		завдання видав	завдання прийняв
1	Головня О. С.	01.03.2023 	26.03.2023 
2	Головня О. С.	27.03.2023 	05.05.2023 
3	Головня О. С.	05.05.2023 	10.06.2023 

Дата видачі завдання 1 березня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	16.03.2023	Виконано
2	Аналіз літературних джерел	17.03.2023	Виконано
3	Аналіз об'єкта дослідження	23.03.2023	Виконано
4	Постановка задачі дослідження	24.03.2023	Виконано
5	Розробка топології	25.03.2023	Виконано
6	Базові налаштування мережі	29.03.2023	Виконано
7	Вибір платформи захисту	17.04.2023	Виконано
8	Додавання робочих станцій	18.04.2023	Виконано
9	Керування доступом	18.04.2023	Виконано
10	Перевірка захищеності	21.05.2023	Виконано
11	Оформлення пояснювальної записки	25.05.2023	Виконано
12	Оформлення презентації	30.05.2023	Виконано
	Захист	23.06.2023	

Студент

Керівник




А. О. Анчис

О. С. Головня

АНОТАЦІЯ

Пояснювальна записка до кваліфікаційної роботи бакалавра на тему «Проект підсистеми гібридного захисту від шкідливого програмного забезпечення у Windows-мережі» складається з переліку умовних скорочень вступу, трьох розділів, висновків, списку використаної літератури та додатків.

Основний текст кваліфікаційної роботи викладено на 75 сторінках друкованого тексту.

Пояснювальна записка має 6 сторінок додатків. Список використаних джерел містить 21 найменувань і займає 3 сторінки. В роботі наведено 74 рисунки.

У першому розділі здійснено порівняння методів захисту робочих станцій, а також основних EDR-рішень для подальшої роботи.

У другому розділі розроблено топологію мережі, виконано її налаштування.

У третьому розділі проведено налаштування Microsoft Defender for EDR, що надало можливість встановлювати режими доступу для користувачів, що дозволяє обмежити права доступу до системи та забезпечити гнучкий контроль над безпекою. Також виконано симуляцію атаки на кінцевий пристрій та описано, як виявляється та знешкоджується загроза.

У додатку наведено налагодження використаних мережних пристроїв.

Ключові слова: МЕРЕЖА, БЕЗПЕКА, ПЗ, ПРАВА ДОСТУПУ, РОЗШИРЮВАНІСТЬ, МАСШТАБОВАНІСТЬ, СЕРВЕР, ДОСТУП, РОЗПОДІЛ, ЗАХИСТ, EDR, ДОЗВІЛ, ВИЯВЛЕННЯ, MICROSOFT DEFENDER, ПОЛІТИКИ.

КІК.КР.Б – 125 – 1 – ПЗ

Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми гібридного захисту від шкідливого програмного забезпечення у Windows-мережі	Лім.	Арк.	Аркуші
Розроб.		Анчис А. О.		20.06.23				
Керівник		Головня О. С.		20.06.23			4	82
Реценз.		Ефименко А. А.		20.06.23		ФІКТ, гр. КБ-19-1		
Н. Контр.								
Запверд.		Ефименко А. А.		20.06.23				

ANNOTATION

Explanatory note to the bachelor thesis on the topic "Project of the subsystem of hybrid protection against malicious software in the Windows network" consists of a list of notations and abbreviations, introduction, three sections, a conclusion, a list of used literature and appendices.

The text part is presented on 75 pages.

The explanatory note has 6 pages of annexes. The list of references contains 21 names and occupies 3 pages. The work contains 74 drawings.

In the first section, the methods of protecting workstations are compared, and the main EDR solutions for further work are compared.

In the second section, the basic settings of the network are performed, and its topology is developed.

In the third section, the configuration of Microsoft Defender for EDR was carried out. This provides the ability to set access modes for users, which allows you to limit access rights to the system and provide flexible control over security. It also simulates an attack on the end device and describes how the threat is detected and neutralized.

The appendix shows the configuration of the network devices used.

Keywords: NETWORK, SECURITY, SOFTWARE, ACCESS RIGHTS, EXPANSION, SCALE, SERVER, ACCESS, DISTRIBUTION, PROTECTION, EDR, PERMISSION, DISCOVERY, MICROSOFT DEFENDER, POLICIES.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	8
ВСТУП.....	9
РОЗДІЛ 1. Теоретичні відомості про методи захисту кінцевих вузлів.....	11
1.1 Огляд методів захисту кінцевих вузлів.....	11
1.2 Поняття про EDR-платформи.....	15
1.3 Порівняння EDR-платформ	20
РОЗДІЛ 2. Планування схеми мережі та схеми адресації.....	25
2.1 Аналіз вимог до мережі та її складових	25
2.2 Розробка схеми адресації	30
2.3 Базові налаштування мережі.....	32
Висновки до другого розділу.....	38
РОЗДІЛ 3. Налаштування EDR-захисту в мережі	39
3.1 Умови розгортання Microsoft Defender for EDR.....	39
3.2 Керування доступом користувачів у Microsoft Defender for Endpoint.....	45
3.3 Додавання пристроїв мережі до системи EDR	49
3.4 Керування загрозами та вразливостями засобами Microsoft Defender for Endpoint	57
3.5 Налаштування Microsoft Defender Application Guard	59
3.6 Правила зменшення поверхні атаки за допомогою Windows Defender Exploit Guard	63
3.7 Симуляція атаки на кінцевий пристрій	67
Висновки до третього розділу	71
ВИСНОВКИ	72
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	73

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ	76
Додаток А	77

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ – програмне забезпечення

EDR - Endpoint Detection and Response

SIEM - Security Information and Event Management

VLAN - Virtual Local Area Network

GPO - Group Policy Object

MDE - Microsoft Defender for Endpoint

MDAG - Microsoft Defender Application Guard

GUI - Graphical User Interface

ОС - операційна система

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

ВСТУП

Актуальність теми. Тема захисту пристроїв мережі є надзвичайно актуальною в сучасному кібербезпечному середовищі. Захист кінцевих точок відіграє важливу роль у запобіганні і виявленні атак, збереженні конфіденційності даних, захисті від втрати інтелектуальної власності та забезпеченні цілісності систем.

Кіберзлочинці постійно розвивають нові та складніші методи атак, спрямовані на кінцеві точки. Це включає шкідливі програми, вимагачів викупу, фішингові атаки та інші загрози. Захист кінцевих пристроїв стає ключовим фактором у виявленні та запобіганні цим загрозам.

Захист кінцевих точок стає все важливішим, оскільки люди та організації все більше залежать від технологій. Відомості, документи, комунікація та багато інших важливих аспектів життя та роботи зберігаються на пристроях, що робить їх привабливою мішенню для атак.

Багато секторів, таких як фінанси, охорона здоров'я та правоохоронні органи, мають суворі регуляторні вимоги щодо захисту конфіденційної інформації та персональних даних. Захист кінцевих точок є необхідною складовою для виконання цих вимог.

Отже, забезпечення ефективного та надійного захисту кінцевих точок стає вельми важливим для підтримки безпеки, захисту даних та забезпечення нормативної відповідності. Організації повинні активно використовувати інструменти та стратегії захисту кінцевих точок для забезпечення цих цілей.

Мета: розробка проєкту підсистеми гібридного захисту від шкідливого програмного забезпечення у Windows-мережі.

Завдання:

-Вивчення та розробка різних методів, технологій, інструментів та стратегій для ефективного захисту кінцевих вузлів.

-Налагодження топології мережі організації.

-Тестування мережі на проникнення та захист від шкідливого ПЗ.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

Об'єктом дослідження: кінцеві вузли(пристрої), що використовуються в комп'ютерних мережах.

Предмет дослідження: процес проектування та налаштування захисту кінцевих вузлів від шкідливих атак, загроз, вразливостей та несанкціонованого доступу.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

РОЗДІЛ 1. Теоретичні відомості про методи захисту кінцевих вузлів

1.1 Огляд методів захисту кінцевих вузлів

Методи захисту кінцевих вузлів можна розподілити за наступними напрямками.

1. Використання антивірусних програм для виявлення, блокування та видалення шкідливого програмного забезпечення, такого як віруси, троянці, черви та рекламне ПЗ.



Рис. 1.1. Приклади антивірусного ПЗ

Антивірусне програмне забезпечення є ключовим компонентом захисту комп'ютерних систем від шкідливих програм. Воно сканує файли, електронну пошту, веб-сторінки та інші об'єкти на наявність вірусів, троянців, червів, рекламного ПЗ та інших видів шкідливого коду. У разі виявлення загрози антивірус блокує або видаляє її, забезпечуючи безпеку користувача.

Антивірусні програми використовують різні методи для виявлення шкідливого коду, такі як сигнатурне сканування, евристичний аналіз та поведінковий моніторинг. Сигнатурне сканування порівнює файл з базою відомих шкідливих сигнатур, евристичний аналіз виявляє шкідливий код на основі його характеристик, а поведінковий моніторинг аналізує дії програми у реальному часі, щоб виявити аномальні або підозрілі дії.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

Регулярне оновлення антивірусного програмного забезпечення є важливим, оскільки це дозволяє йому залишатися ефективним проти нових загроз. Більшість антивірусних програм пропонують автоматичні оновлення бази даних сигнатур та алгоритмів виявлення [8].

2. Застосування заходів для запобігання інфікуванню системи шкідливим ПЗ, таких як файерволи, фільтри пошти та веб-контенту.

Файерволи допомагають контролювати вхідний та вихідний мережевий трафік, блокуючи потенційно шкідливі пакети даних та забезпечуючи додатковий рівень безпеки. Фільтри пошти та веб-контенту перевіряють вхідні повідомлення та веб-сторінки на наявність шкідливого коду, спаму або інших зловмисних посилань.

Навчання користувачів безпечному поведженню в Інтернеті може допомогти запобігти інфікуванню системи через небезпечні посилання, відкриття шкідливих вкладень або використання ненадійних програм.

3. Своєчасне встановлення оновлень та патчів безпеки для операційної системи та програмного забезпечення, що забезпечує закриття відомих уразливостей.

Оновлення та патчі безпеки випускаються розробниками програмного забезпечення з метою виправлення помилок, усунення уразливостей та покращення продуктивності. Зазвичай, вони рекомендуються для встановлення якомога швидше, адже кожен день, коли система залишається без оновлення, вона стає все більш вразливою перед зловмисниками.

Оновлення безпеки закривають ці уразливості та зменшують ризик зараження. Зловмисники використовують різні методи для отримання доступу до системи, включаючи відомі уразливості, тому забезпечується додатковий рівень захисту від несанкціонованого доступу, також в них часто містяться виправленні помилки для покращення продуктивності, що забезпечує стабільність роботи системи та підвищує її продуктивність. Після встановлення оновленого ПЗ забезпечується сумісність з новими технологіями та стандартами.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Обмеження доступу до кінцевого вузла та його ресурсів за допомогою аутентифікації, авторизації та аудиту.

Контроль доступу є ключовим елементом захисту кінцевих вузлів та їх ресурсів. Цей метод забезпечує обмеження доступу до важливих інформаційних ресурсів та даних, захищаючи їх від несанкціонованого доступу та зловживань.

Одним із способів контролю доступу є аутентифікація, яка дозволяє перевірити, чи має користувач право доступу до системи. Цей процес може здійснюватись за допомогою паролів, біометричних даних або інших методів.

Авторизація є іншим елементом контролю доступу. Вона визначає, які дії та ресурси користувач може виконувати та мати доступ до них. Цей процес забезпечує захист важливих ресурсів від несанкціонованого доступу.

Аудит також є важливим елементом контролю доступу. Він забезпечує запис дій користувачів та перевірку їх на відповідність політикам безпеки. Це дозволяє виявити можливі загрози та вжити заходи для їх запобігання.

Застосування контролю доступу може зменшити ризик витоку даних, ускладнити напади з зовнішньої та внутрішньої сторони, та забезпечити довіру до системи з боку користувачів.

5. Використання криптографічних методів для захисту конфіденційності та цілісності даних, які зберігаються на кінцевому вузлі або передаються через мережу.

Шифрування даних - це процес захисту конфіденційності та цілісності даних, що зберігаються на кінцевому вузлі або передаються через мережу, за допомогою криптографічних методів. Шифрування даних дозволяє зберігати та передавати інформацію у безпечний спосіб, таким чином запобігаючи несанкціонованому доступу до неї.

Шифрування може бути виконане на кінцевому вузлі, де дані зберігаються, або на мережевому рівні, де дані передаються через мережу. У випадку з кінцевим вузлом, дані можуть бути зашифровані на диску або у пам'яті, залежно від того, як вони

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

зберігаються. У випадку з мережевим рівнем, дані можуть бути зашифровані перед їх передачею через мережу за допомогою протоколів шифрування, таких як SSL (Secure Sockets Layer) або TLS (Transport Layer Security).

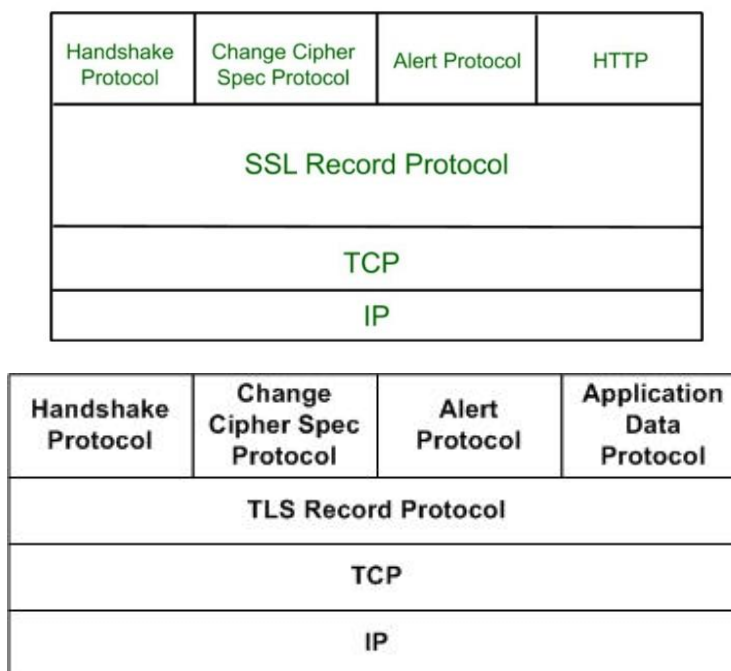


Рис. 1.2. Протоколи шифрування SSL та TLS

Шифрування даних може бути виконане за допомогою різних алгоритмів шифрування, таких як AES (Advanced Encryption Standard), DES (Data Encryption Standard) або RSA (Rivest–Shamir–Adleman). Кожен з цих алгоритмів має свої переваги та недоліки, тому вибір алгоритму залежить від потреб користувача та характеристик захищуваних даних [7].

6. Створення регулярних резервних копій важливих даних для запобігання втрати інформації в результаті атак або апаратних збоїв.

Резервне копіювання даних є важливим елементом безпеки даних для будь-якого бізнесу чи організації. Цей процес включає створення копій важливих даних та зберігання їх у безпечному місці, що дозволяє відновлювати доступ до даних в разі їх втрати чи пошкодження.

Існує кілька способів резервного копіювання даних, включаючи локальне зберігання на зовнішніх носіях, віддалене зберігання в хмарі або на інших серверах, а також копіювання на мережеві сховища. Окрім цього, необхідно регулярно тестувати

процес резервного копіювання, щоб переконатися, що він працює ефективно та надійно.

7. Освіта користувачів щодо загроз безпеки та найкращих практик для запобігання інфікуванню та компрометації кінцевих вузлів.

Користувачі є слабкою ланкою в системі безпеки, оскільки їхні дії можуть стати причиною інфікування та компрометації кінцевих вузлів. Однак, завдяки правильному навчанню користувачі можуть дізнатися про загрози безпеки та найкращі практики для запобігання інфікуванню та компрометації кінцевих вузлів.

Основна мета навчання користувачів полягає в тому, щоб допомогти їм розуміти ризики, які пов'язані з використанням комп'ютерів та мереж. Це включає ознайомлення з потенційними загрозами безпеки.

8. Відстеження активності на кінцевих вузлах та аналіз подій безпеки для виявлення та відповіді на можливі загрози.

Моніторинг та відстеження активності на кінцевих вузлах та аналіз подій безпеки є важливими складовими проактивного підходу до кібербезпеки. Це означає, що замість того, щоб реагувати на загрози після їх виникнення, команди забезпечення безпеки повинні виявляти і запобігати їм на ранніх етапах, перевіряючи активність на кінцевих вузлах та аналізуючи події безпеки.

Аналіз подій безпеки полягає у зборі та аналізі даних, що стосуються безпеки, щоб виявити загрози. Це може бути здійснене з використанням різноманітних інструментів аналізу даних, включаючи системи детекції вторгнень, системи управління журналами, системи моніторингу подій тощо.

1.2 Поняття про EDR-платформи

Endpoint Detection and Response Platforms (EDR) - це платформи, які використовуються для виявлення та реагування на загрози безпеки на різних кінцевих пристроях (endpoint) у корпоративних мережах. EDR-платформи працюють на кінцевих пристроях (наприклад, на комп'ютерах, мобільних телефонах, серверах) та забезпечують відстеження і аналіз активності цих пристроїв. Вони виявляють та

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

реагують на підозрілі активності, які можуть вказувати на наявність кібератак, такі як віруси, розширення шкідливого ПЗ та інші загрози. Основна функціональність EDR-платформ полягає в зборі інформації про кінцеві пристрої та їхню активність, виявленні аномальних змін у поведінці пристроїв, аналізі цих змін та реагуванні на підозрілу активність. Крім того, EDR-платформи можуть забезпечувати можливість блокування шкідливих програм та інших загроз на рівні кінцевих пристроїв, а також розгортання оновлень безпеки. В загальному, EDR-платформи є ефективним інструментом для забезпечення безпеки в корпоративних мережах, які мають велику кількість кінцевих пристроїв. Вони дозволяють виявляти та реагувати на загрози, що швидко змінюються та забезпечують більш високий рівень захисту пристроїв і даних користувачів [4].

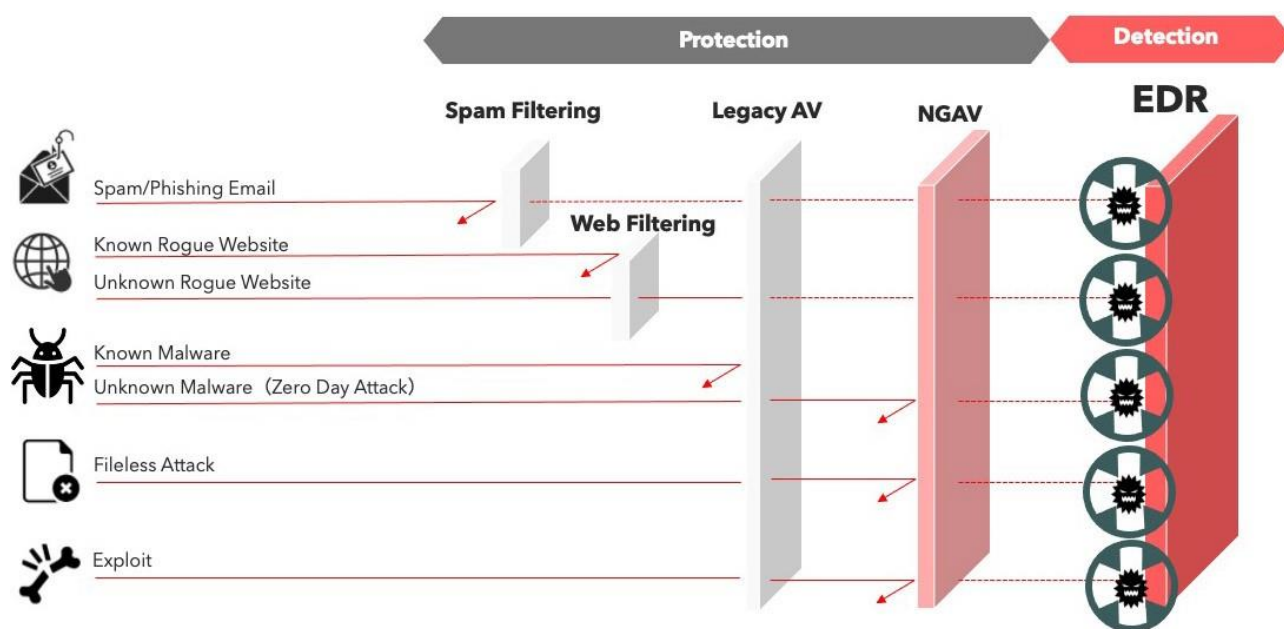


Рис. 1.3. Принцип роботи EDR

Системи EDR зазвичай включають наступні функції та можливості.

1. Надають можливість відстежувати дії та активності на кінцевих точках, щоб виявляти аномальні дії та потенційні загрози.

2. Використовують алгоритми машинного навчання та інші методи для виявлення потенційно шкідливої активності на кінцевих точках, такі як аномальна активність мережі, спроби вторгнення або зміни конфігурації пристрою.

3. Збирають інформацію про виявлені загрози та інші події на кінцевих точках, щоб допомогти аналізувати та вирішувати інциденти.

4. Надають можливість віддаленого управління кінцевими точками, таким чином забезпечуючи можливість дистанційного контролю та керування пристроями.

5. Дозволяють операторам безпеки швидко відреагувати на виявлені загрози та запобігти їх поширенню.

6. Можуть інтегруватися з іншими інструментами безпеки, такими як Security Information and Event Management (SIEM), щоб забезпечити більш ефективну захист мережі.

Відстеження та аналіз поведінки кінцевих точок є однією з ключових можливостей систем EDR. Ця функція дозволяє збирати дані про активність на кінцевих точках, в тому числі процеси, файлові операції та мережеві з'єднання, аналізувати їх та виявляти аномалії, що можуть свідчити про наявність загроз. Процес зазвичай здійснюється за допомогою алгоритмів машинного навчання, які навчаються розпізнавати типові патерни поведінки та виявляти аномалії. Наприклад, система може виявити незвичайний обсяг мережевого трафіку з певної кінцевої точки або спробу нетипового доступу до важливих файлів. Аналіз поведінки кінцевих точок може допомогти операторам безпеки швидко виявляти нові загрози та забезпечувати вчасну реакцію на них.

Виявлення загроз є ще однією ключовою можливістю систем EDR. Вони використовують алгоритми машинного навчання, статистичний аналіз та інші методи для виявлення потенційно шкідливої активності на кінцевих точках. Системи EDR можуть моніторити різноманітні типи активності на кінцевих точках, включаючи мережевий трафік, процеси, файлову активність та інші. Вони можуть виявляти спроби

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

вторгнення, включаючи використання відомих уразливостей або шкідливого програмного забезпечення, а також зміни конфігурації пристрою, які можуть свідчити про компрометацію безпеки. Виявлення потенційно шкідливої активності на кінцевих точках дозволяє операторам безпеки швидко реагувати на загрози та запобігати їхньому поширенню в мережі. Системи EDR можуть відправляти сповіщення про потенційно шкідливу активність до операторів безпеки, що дозволяє їм швидко реагувати на загрозу та приймати заходи щодо її ліквідації [6].

Системи EDR можуть збирати різноманітну інформацію про події на кінцевих точках, таку як час події, тип активності, використані ресурси та інші. Вони можуть також відстежувати залежності між подіями на кінцевих точках та визначати, чи є вони частиною більшого інциденту або кампанії атак. Зібрана інформація дозволяє операторам безпеки аналізувати та вирішувати інциденти, що відбуваються в мережі. Вони можуть використовувати цю інформацію для встановлення причин та пошуку відповідальних за інцидент, а також для прийняття заходів щодо його ліквідації. Крім того, системи EDR можуть збирати статистику про інциденти та загрози на кінцевих точках, що дозволяє операторам безпеки оцінити рівень загроз та виявити тенденції в їх поширенні [5].

З допомогою цих систем можна надавати можливість віддаленого управління кінцевими точками, що дає змогу дистанційно контролювати та керувати пристроями. Це дозволяє адміністраторам мережі та безпековим командам віддалено аналізувати стан пристроїв, виявляти та вирішувати проблеми, надавати допомогу користувачам, налаштовувати параметри системи та проводити інші дії, не потребуючи фізичного доступу до кожного пристрою. Це може бути особливо корисним для компаній з великою кількістю пристроїв, які знаходяться на різних місцях, а також для роботи з віддаленими працівниками. Однак, важливо враховувати можливі ризики безпеки, пов'язані з віддаленим управлінням пристроями, тому необхідно використовувати надійні засоби захисту та практикувати безпечні процедури роботи.

Системи EDR дозволяють операторам безпеки швидко реагувати на виявлені загрози та запобігти їх поширенню. Ці системи здатні виявляти потенційні загрози на кінцевих точках, таких як персональні комп'ютери, мобільні пристрої та сервери, та вчасно повідомляти про них операторів безпеки.

Одним з основних принципів систем EDR є реагування на події в режимі реального часу, що дозволяє операторам безпеки швидко відреагувати на потенційні загрози та запобігти їх поширенню. Зокрема, системи EDR можуть виявляти невідомі загрози, які не входять до списку відомих вірусів та зловмисного програмного забезпечення, та автоматично блокувати їх поширення. Це дозволяє зменшити час виявлення та реакції на загрозу, що зменшує можливість пошкодження кінцевих точок та важливих даних.

EDR може інтегруватися з іншими інструментами безпеки, такими як Security Information and Event Management (SIEM), щоб забезпечити більш ефективну захист мережі. Інтеграція з іншими інструментами безпеки дозволяє забезпечити повніший огляд захисних заходів та збільшити можливості виявлення та реагування на загрози.

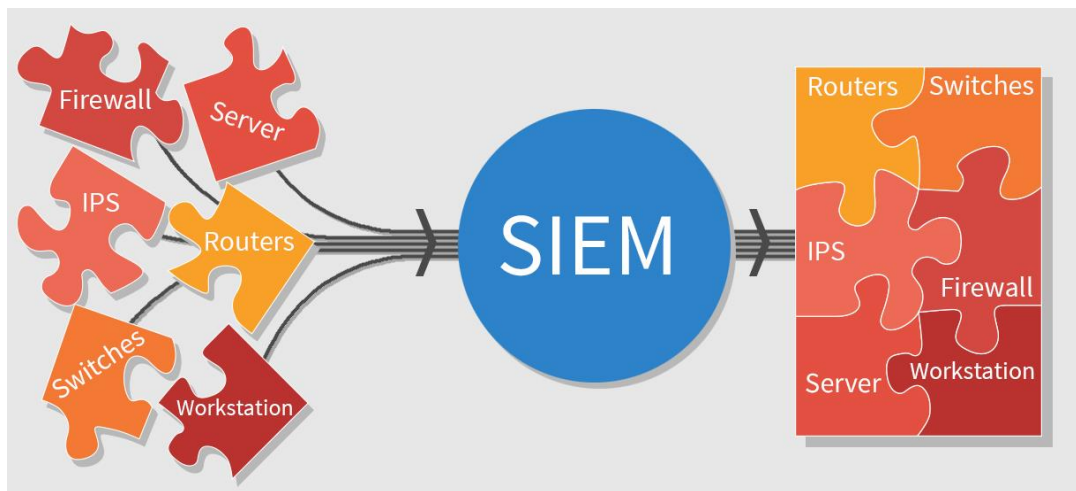


Рис. 1.4. Склад інструменту безпеки SIEM

SIEM-системи зазвичай збирають журнали подій з різних джерел у мережі, аналізують їх та виявляють потенційні загрози. Інтеграція з системами EDR дозволяє SIEM-системам отримувати дані про загрози, виявлені на кінцевих точках, що дозволяє

забезпечити більш повний огляд захисних заходів та збільшити ефективність виявлення та реагування на загрози [6].

Інтеграція з антивірусним програмним забезпеченням дозволяє забезпечити більш повний захист від відомих загроз, а інтеграція з фаєрволами дозволяє контролювати мережевий трафік та запобігати його передачі відомим або невідомим загрозам. Отже, інтеграція з іншими інструментами безпеки дозволяє забезпечити більш повний та ефективний захист мережі.

1.3 Порівняння EDR-платформ

Едр-платформи (EDR, Endpoint Detection and Response) є спеціалізованими рішеннями кібербезпеки, які призначені для виявлення, реагування та захисту від загроз на рівні кінцевих пристроїв (endpoints), таких як комп'ютери, сервери, мобільні пристрої тощо. Ці платформи спрямовані на забезпечення безпеки на рівні кінцевих точок і гарантують більш глибокий та точний контроль над захистом в порівнянні з традиційними антивірусними програмами.

Для вибору та використання з початку потрібно порівняти та обрати найбільш ефективне з представлених на ринку рішень [16].

McAfee - це широко відома компанія в сфері кібербезпеки, яка надає рішення для ефективного захисту від різноманітних загроз.



Рис. 1.5. - Логотип McAfee

Платформа McAfee пропонує комплексні інструменти для захисту, такі як антивірус, фаєрвол, захист від вторгнень та інші. Вона підтримує різні операційні системи та платформи, що дозволяє використовувати її в різних інфраструктурах [1].

SentinelOne - це EDR-платформа, яка використовує штучний інтелект та машинне навчання для виявлення та захисту від загроз.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		20



Рис. 1.6. – Логотип SentinelOne

Вона надає захист в реальному часі та автоматичну реакцію на інциденти, що допомагає забезпечити ефективний захист.

SentinelOne також має можливості для відновлення після атаки, що дозволяє організаціям швидко відновити нормальне функціонування після кібератак [1].

CrowdStrike - це платформа, яка спеціалізується на виявленні та захисті від атак з використанням штучного інтелекту та аналізу великих обсягів даних [2].



Рис. 1.7. – Логотип CrowdStrike

Вона відома своїм швидким виявленням загроз та високою точністю виявлення аномальної активності. CrowdStrike також має велику базу даних загроз, що допомагає прогнозувати нові атаки та забезпечує більш ефективний захист.

Microsoft Defender for Endpoints - це рішення, яке інтегровано з екосистемою Microsoft та забезпечує захист для систем, що працюють на операційній системі Windows [3].



Рис. 1.8. – Логотип Microsoft Defender for Endpoints

Воно має різні функції безпеки, включаючи антивірусний захист, виявлення загроз, контроль даних та інші. Microsoft Defender for Endpoints легко налаштовується та інтегрується з іншими продуктами Microsoft, що полегшує його впровадження у наявну інфраструктуру.

Таблиця 1.1.

Порівняння програмних продуктів

Платформа	+	-
McAfee	1. Великий досвід у сфері кібербезпеки. 2. Забезпечує комплексний захист від широкого спектру загроз. 3. Підтримує багато платформ та операційних систем.	Система може бути складною у налаштуванні та використанні.
SentinelOne	1. Використовує штучний інтелект та машинне навчання для виявлення загроз. 2. Забезпечує захист в реальному часі та реагує на загрози автоматично. 3. Має хорошу функціональність у виявленні та відновленні після атаки.	Вартість підписки може бути високою для деяких користувачів.

CrowdStrike	1. Швидке виявлення загроз та реагування на них. 2. Висока точність виявлення аномальної активності та вторгнень. 3. Велика база даних загроз, яка дозволяє прогнозувати нові атаки.	Можливі високі витрати на підписку для деяких користувачів.
Microsoft Defender for Endpoints	1. Інтегрований з інфраструктурою Microsoft та легко налаштовується. 2. Забезпечує добре покриття захисту для систем, що працюють на ОС Windows. 3. Має додаткові функції безпеки, такі як антивірус та захист від витоку даних.	Може бути недостатньо ефективний для систем, що працюють на інших операційних системах, крім Windows.

Загалом всі розглянуті платформи є достатньо ефективними в своїй сфері та можуть конкурувати між собою, проте так як мережа повністю працює на базі Windows, то Microsoft Defender for Endpoints буде найоптимальнішим рішенням.

Висновки до першого розділу

Методи захисту кінцевих вузлів можуть бути різними залежно від того, який тип захисту буде обрано для застосування. Деякі з методів захисту включають антивірусне програмне забезпечення, перевірку цілісності файлів, брандмауери, політики обмеження виконання програм та багато інших. Кожен з цих методів має свої переваги та недоліки і може використовуватись як окремо, так і в поєднанні з іншими методами.

Endpoint Detection and Response (EDR) - це технологія захисту кінцевих вузлів, що забезпечує збір даних про події та активність на кінцевих вузлах, аналіз цих даних для виявлення загроз та відповідних відповідей на них. EDR дозволяє забезпечити більш високий рівень безпеки та ефективної реакції на події на кінцевих вузлах.

Також виконано порівняння EDR-платформ, кожна має свої переваги та обмеження. McAfee відома своїм досвідом та комплексним захистом, SentinelOne використовує штучний інтелект для виявлення загроз та автоматичної реакції, CrowdStrike має високу точність виявлення аномальної активності, а Microsoft Defender for Endpoints інтегрований з екосистемою Microsoft та легко налаштовується.

Загалом, їх застосування є важливим елементом в розбудові комплексної системи кібербезпеки, що забезпечує захист кінцевих точок та реагування на потенційні загрози. Належне впровадження та налаштування може значно знизити ризик кібератак та захистити організацію від потенційних загроз.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

РОЗДІЛ 2. Планування схеми мережі та схеми адресації

2.1 Аналіз вимог до мережі та її складових

При проектуванні мережі використовувалась трирівнева ієрархічна модель мережі, яка включає в себе:

- рівень ядра;
- рівень розподілу;
- рівень доступу;

Розподіл об'єктів мережі за рівнями відбувається згідно з функціоналом, який виконує кожен об'єкт, це допомагає аналізувати кожен рівень незалежно від інших, тобто розподіл іде переважно не за фізичними поняттями, а за логічними.

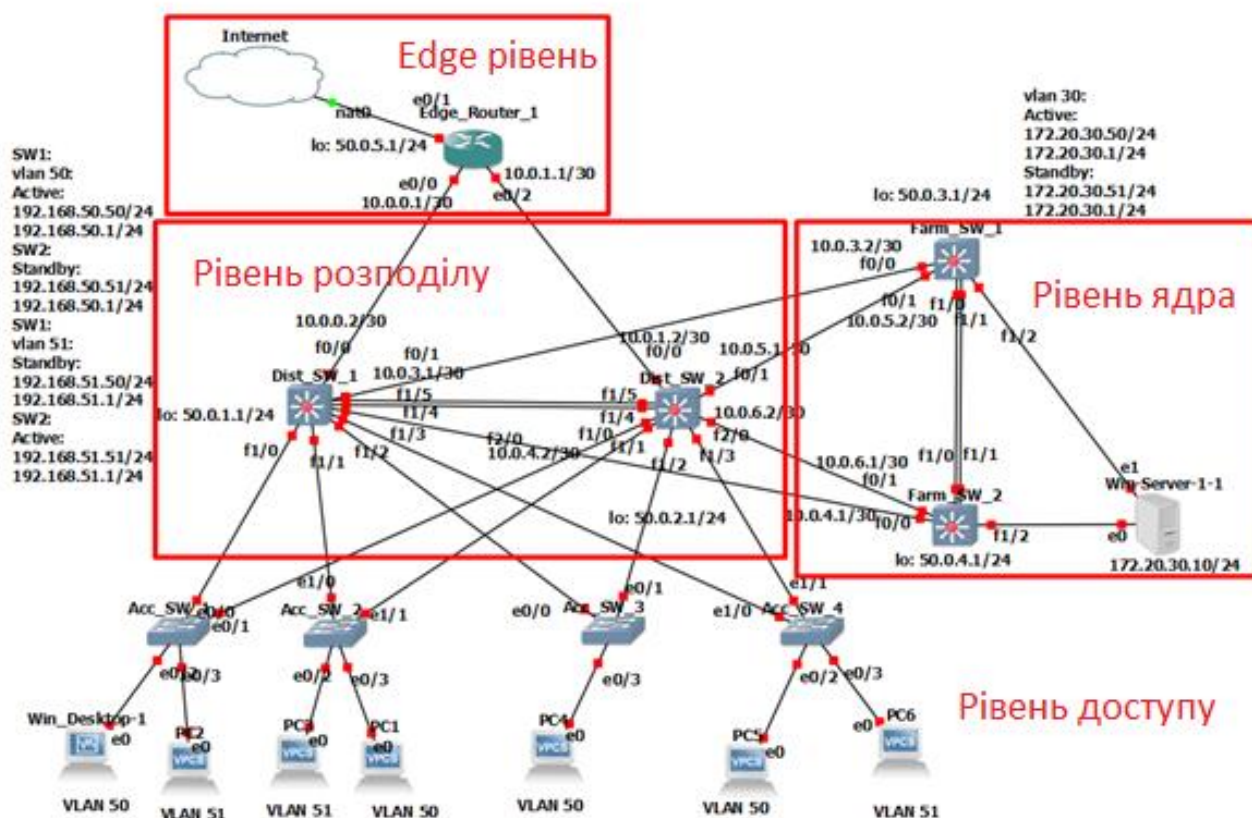


Рис. 2.1 – Загальна структура мережі

		Анчис А. О.		
		Головня О. С.		
Змн.	Арк.	№ докум.	Підпис	Дата

Базовий рівень формує ядро мережі. На верхівці ієрархії цей рівень відповідає за швидке та надійне пересилання великих обсягів трафіку. Рівень ядра включає в себе 1 сервер та 2 багаторівневі маршрутизатори.

Сервер з маршрутизаторами, які формують один окрему віртуальну мережу, закомутовані між собою. Призначенням даного рівня є швидка комутація трафіку. Трафік передається на рівні ядра для кількох користувачів. Однак на рівні розподілу обробляються дані користувача, що може призвести до додаткових запитів у базовий рівень. Оскільки будь-яка помилка тут впливає на подальшу роботу мережі, ядро має передбачати всі можливі затримки в роботі.

Рівень розподілу, також рівень робочих груп. Він розташований між базовим рівнем та рівнем доступу. Основні функції рівня поширення полягають у маршрутизації, фільтрації та доступі до локальних підмереж, а також у визначенні правил доступу пакетів до базового рівня. Рівень поширення повинен встановлювати найшвидший спосіб обробки запитів до служб та обміну даними з серверами. Пакети направлені на сервер проходять по найшвидшому на даний момент маршруту та потрапляють на рівень ядра. На рівні розподілу встановлюються додаткові політики безпеки та протоколи віддаленого доступу.

Рівень доступу включає комутатори рівня 2, що забезпечують підключення до робочих станцій. На висхідних лініях зв'язку пристрої рівня доступу підключаються до розподільних комутаторів. Ми можемо керувати контролем доступу та політикою та забезпечувати безпеку портів на рівні доступу. Комутатори рівня доступу забезпечують доставку пакетів до кінцевих пристроїв. Даний рівень включає в себе 2 підмережі. Рівень доступу є важливим лише для кінцевих користувачів, тому кількість трафіку на кожній підмережі менша ніж на розподільчій ланці.

Також рівень Enterprise edge – це рівень де знаходяться маршрутизатори, які з'єднується з Internet. Також на них працює NAT, Firewall, вони ж є VPN пристроями. До edge рівня також належать ASA, IDS та IPS.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Далі буде розглянуто детально кожний рівень та підмережі захищеної мережі організації.

Побудована ієрархічна модель дозволяє розвивати та масштабувати наявну обчислювальну мережу в міру зростання організації та відповідно мережі або проектувати нові великі мережі.

Такий підхід дозволяє реалізовувати принципи масштабованості мережі.

На рисунку 3.2 зображено ядро ієрархічної мережі.

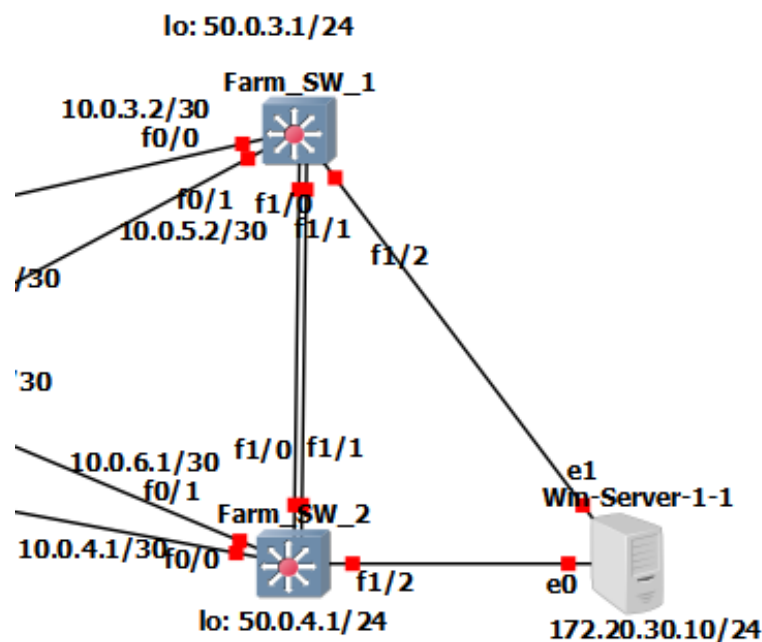


Рис. 2.2 – Структура VLAN 30

Тут ми бачимо, що кожен з мережевих інтерфейсів сервера прямо підключений до окремого комутатора, а комутатори з'єднані між собою агрегованим каналом. Ця конфігурація може забезпечити високу доступність мережі та більшу пропускну здатність для сервера, оскільки два мережевих інтерфейси можуть працювати паралельно.

Дана топологія не вимагає складної конфігурації та налаштування мережевих елементів тому вона є дуже простою.

Варто врахувати, що використання двох комутаторів може суттєво вплинути на ціну, а додавання нових серверів значно ускладнити налаштування даного сегменту мережі.

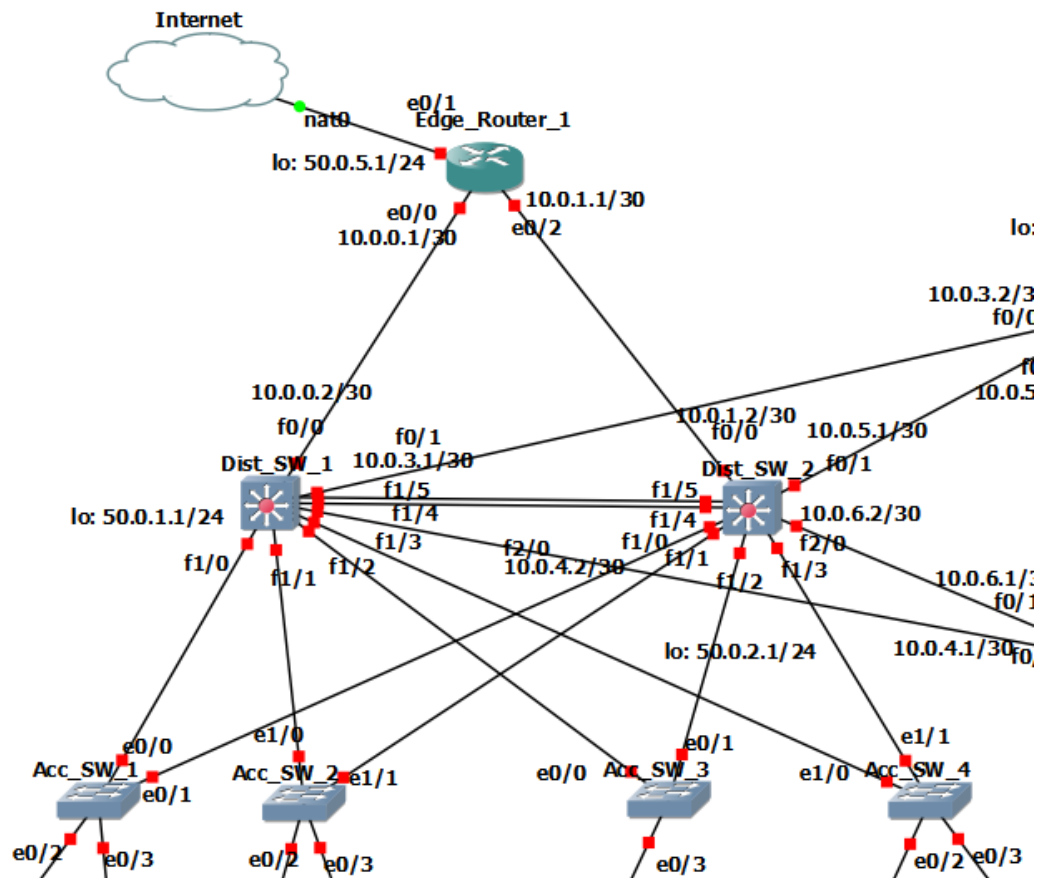


Рисунок 2.3 – Структура рівня ядра

Основні комутатори "Dist_SW_1" та "Dist_SW_2", які забезпечують з'єднання з рівнем ядра мережі, при цьому правильно розташовані каналні з'єднання. Комутаційні пристрої мають налаштування VLAN50 та VLAN51 для забезпечення IP-адресами кінцевих пристроїв мережі. Також до них під'єднуються другорядні комутатори, які забезпечують підключення до робочих станцій.

Edge-router є мережевим пристроєм, що використовується для підключення локальної мережі (LAN) до інтернет-мережі через технологію Network Address Translation (NAT), яка дозволяє забезпечити безпеку мережі та захист від зовнішніх атак.

Маршрутизатор може бути обладнаний різними інтерфейсами для підключення до різних типів мереж, таких як Ethernet, Wi-Fi, DSL, кабельна мережа тощо.

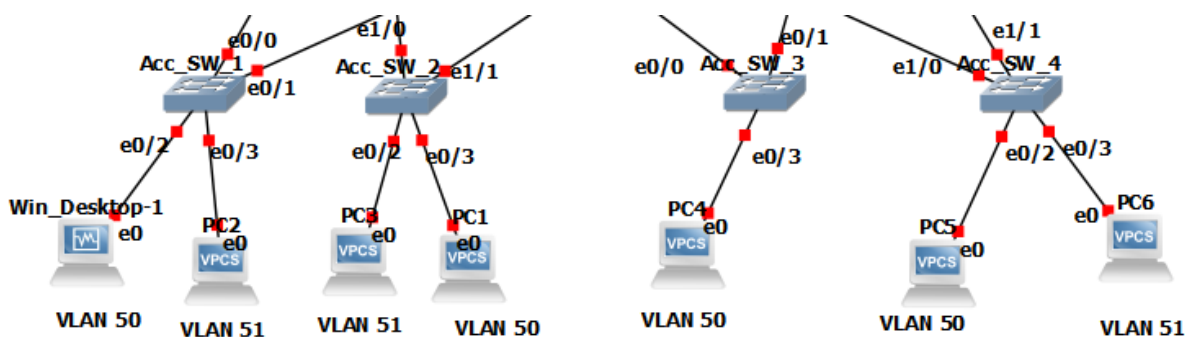


Рис. 2.4 – Структура VLAN 50-51

На рівні доступу маємо комутатори, які підключаються до робочих станцій і забезпечують доступ до мережі та Інтернету. У даному випадку, маємо 4 такі комутатори.

Кожен з цих комутаторів налаштований на підтримку VLAN50-51. Робочі станції, які підключені до цих комутаторів, отримають відповідні адреси зі своїх VLAN та зможуть зв'язуватися з іншими пристроями у мережі.

Крім того, на рівні доступу можуть бути встановлені різні механізми безпеки (що і є основною метою роботи), такі як безпека портів для обмеження доступу до мережі тільки певним пристроям, а також механізми автентифікації.

У загальному, на рівні доступу виконуються завдання забезпечення доступу робочих станцій до мережі та контролюється безпека мережі на цьому рівні.

Дана топологія мережі дозволяє ефективно управляти мережею та забезпечувати її масштабованість, а також підвищити безпеку та ефективність комунікації пристроїв в мережі.

2.2 Розробка схеми адресації

Структура адрес є важливою складовою ефективної організації мережі. Вона дозволяє використовувати доступний адресний простір більш ефективно та спрощує адміністрування мережі. Для досягнення цих цілей було ретельно сплановано ієрархію адресного простору і відповідно налаштовано мережеві пристрої. При цьому враховано потреби мережі в адресах, кількість підмереж і кількість пристроїв в кожній з них.

Схема адресації розроблена згідно з кількістю мереж та кількістю пристроїв в кожній мережі, з розрахунком на деяку кількість додаткових підключень.

Таблиця 2.1.

IP-адресація

Мережа/пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP - адреса	Префікс	Пристрій підключення	Порт
Комутатор Farm_SW_1	Інтерфейс Vlan30	172.20.30.50	/24	-	-
	stby	172.20.30.1	/24	-	-
	f0/1	10.0.5.2	/30	Dist_SW_2	f0/1
	f0/0	10.0.3.2	/30	Dist_SW_1	f0/1
Комутатор Farm_SW_2	Lo0	50.0.3.1	/24	-	-
	Інтерфейс Vlan30	172.20.30.51	/24	-	-
	stby	172.20.30.1	/24	-	-
	f0/0	10.0.4.1	/30	Dist_SW_1	f2/0
Комутатор Dist_SW_1	f0/1	10.0.6.1	/30	Dist_SW_2	f2/0
	Lo0	50.0.4.1	/24	-	-
	Інтерфейс Vlan50	192.168.50.50	/24	-	-
	stby	192.168.50.1	/24	-	-
Комутатор Dist_SW_1	Інтерфейс Vlan51	192.168.51.50	/24	-	-

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

	stby	192.168.51.1	/24		
--	------	--------------	-----	--	--

	f0/0	10.0.0.2	/30	Edge_Router_1	e0/0
	f0/1	10.0.3.2	/30	Farm_SW_1	f0/0
	f2/0	10.0.4.2	/30	Farm_SW_2	f0/0
	Lo0	50.0.1.1	/24	-	-
Комутатор Dist_SW_2	Інтерфейс Vlan50	192.168.50.51	/24	-	-
	stby	192.168.50.1	/24	-	-
	Інтерфейс Vlan51	192.168.51.51	/24	-	-
	stby	192.168.51.1	/24	-	-
	f0/0	10.0.1.2	/30	Edge_Router_1	e0/2
	f0/1	10.0.5.1	/30	Farm_SW_1	f0/1
	f2/0	10.0.6.2	/30	Farm_SW_2	f0/1
	Lo0	50.0.2.1	/24	-	-
Маршрутизатор Edge_Router_1	Мережний адаптер	194.191.1.2	/26	-	-
	Інтерфейс за замовчуванням	194.191.1.1	—	-	-
	Основний DNS-сервер	209.244.0.3	—	-	-
Сервер Win- Server-1-1	Мережний адаптер	172.20.30.10	/24	-	-
	Інтерфейс за замовчуванням	172.20.30.1	-	-	-
	Основний DNS-сервер	127.0.0.1	-	-	-
Робоча станція Win_Desktop-1	Мережний адаптер	192.168.50.3	/24	-	-
	Інтерфейс за замовчуванням	192.168.50.1	-	-	-
	Основний DNS-сервер	172.20.30.10	-	-	-

2.3 Базові налаштування мережі

1. Побудова мережі, як вказано в топології (рис. 2.1).

2. Налаштування базових параметрів пристроїв (табл. 2.1).

- Налаштування імен хостів;
- Налаштування IP-адрес інтерфейсів, згідно з таблицями IP-адресації;
- Вимкнення пошуку DNS, встановлення таймерів на консольне з'єднання, тощо;

3. Налагодження протоколу маршрутизації OSPF на пристроях мережі. Після їх встановлення необхідно переконатись, що маршрути OSPF встановлені правильно та що мережа використовує правильні маршрути. Також слід відслідковувати маршрути та забезпечувати їх безперебійність:

```
Dist_SW_1#show run | sec ospf
router ospf 1
router-id 2.2.2.2
log-adjacency-changes
network 10.0.0.0 0.0.0.3 area 0
network 10.0.3.0 0.0.0.3 area 0
network 10.0.4.0 0.0.0.3 area 0
network 50.0.1.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
network 192.168.51.0 0.0.0.255 area 0
```

Рис. 2.5. Налаштування OSPF на Dist_SW_1

4. Налаштування маршруту за замовчуванням на граничному маршрутизаторі мережі. Налаштування маршруту за замовчуванням на граничному маршрутизаторі (edge-router) мережі може бути корисним в разі, коли пакети приходять з підмережі, для якої в мережі немає жодного маршруту. В такому випадку граничний

маршрутизатор може використовувати маршрут за замовчуванням для надсилання пакетів до іншої мережі або до Інтернету.

```
Edge_Router_1#show run | sec ospf
router ospf 1
router-id 1.1.1.1
network 10.0.0.0 0.0.0.3 area 0
network 10.0.1.0 0.0.0.3 area 0
network 50.0.5.0 0.0.0.255 area 0
default-information originate
```

Рис. 2.6. Налаштування маршруту за замовчуванням

5. Конфігурування NAT на граничних маршрутизаторах.

Після налаштування на маршрутизаторі вхідні дані будуть перетворені відповідно до налаштувань правил NAT, що дозволить забезпечити доступ до мережі для пристроїв, які не мають публічного IP-адресу або перебувають за NAT.

Створення списку доступу для кінцевих користувачів для доступу в Інтернет:

```
Edge_Router_1#show run | sec acc
access-list 11 permit 192.168.0.0 0.0.255.255
```

Рис. 2.7. Список доступу

Позначення зовнішніх та внутрішніх інтерфейсів. Зовнішні потрібні для підключення до, наприклад, провайдера Інтернету, а внутрішні інтерфейси мають підключення, наприклад, до локальної мережі організації:

```
interface Ethernet0/0
ip address 10.0.0.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
interface Ethernet0/1
ip address dhcp
ip nat outside
ip virtual-reassembly in
interface Ethernet0/2
ip address 10.0.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
```

Рис. 2.8. Зовнішні та внутрішні інтерфейси NAT

Налаштування NAT Overload дозволяє багатьом комп'ютерам в локальній мережі спільно використовувати одну зовнішню IP-адресу для виходу в Інтернет (рис. 2.9).

```
ip nat inside source list 11 interface Ethernet0/1 overload
```

Рис. 2.9. NAT Overload

6. Налаштування HSRP. Це потрібно для роботи декількох комутаторів в одному сегменті як єдиний віртуальний комутатор, щоб забезпечити надійність та безпеку мережі.

```
interface Vlan50
 ip address 192.168.50.50 255.255.255.0
 ip helper-address 172.20.30.10
 shutdown
 standby 1 ip 192.168.50.1
 standby 1 priority 110
 standby 1 preempt
interface Vlan51
 ip address 192.168.51.50 255.255.255.0
 ip helper-address 172.20.30.10
 standby 2 ip 192.168.51.1
 standby 2 preempt
```

Рис. 2.10. Приклад налаштування HSRP

7. Налаштування балансування трафіку на Spanning Tree Protocol за кожен vlan. Дані дії виконуються для балансування трафіку. Для цього встановлюється більш високий пріоритет для портів, які потрібно використовувати більше, і більш низький пріоритет для тих, які потрібно використовувати менше. Це можна зробити на кожному комутаторі, встановивши пріоритет для кожного порту.

```
Dist_SW_1#show run | sec span
spanning-tree vlan 50 priority 24576
spanning-tree vlan 51 priority 28672
```

Рис. 2.11. Налаштування Spanning Tree Protocol

8. Налаштування DHCP з використанням відповідної ролі на Windows Server 2019. Враховуючи потреби мережі встановлюється пул використання адрес для VLAN50-51 та винятки (рис. 2.12).

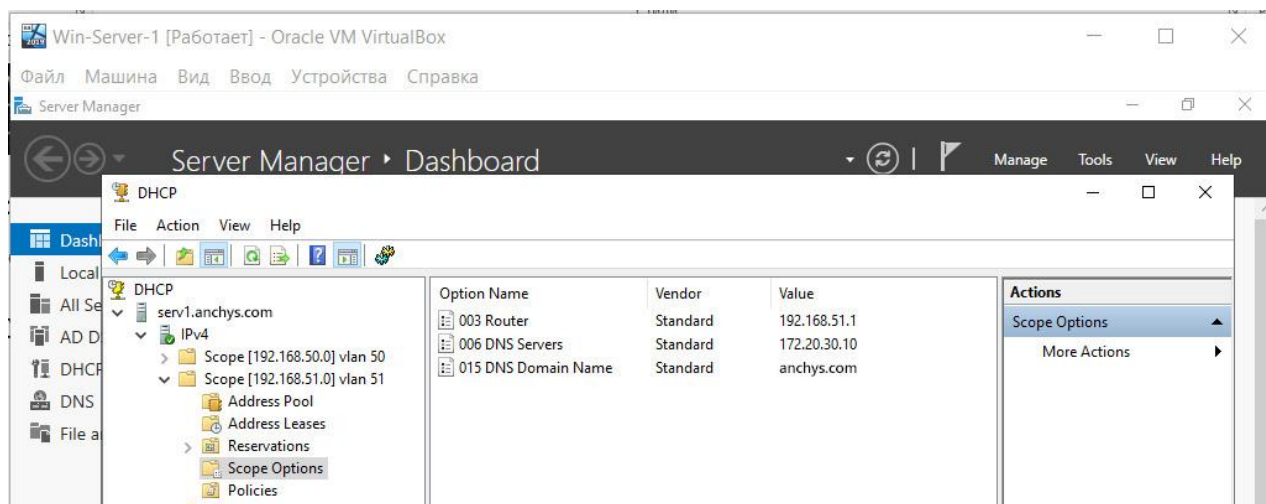


Рис. 2.12. Налаштування DHCP pools на сервері

Налаштування DHCP-Relay на комутаторах розподілу мережі. Ця функція дозволяє DHCP серверу обслуговувати підмережі (рис. 2.13).

```
interface Vlan50
ip address 192.168.50.51 255.255.255.0
ip helper-address 172.20.30.10
standby 1 ip 192.168.50.1
standby 1 preempt
interface Vlan51
ip address 192.168.51.51 255.255.255.0
ip helper-address 172.20.30.10
standby 2 ip 192.168.51.1
standby 2 priority 110
standby 2 preempt
```

Рис. 2.13. Налаштування DHCP-Relay

Налаштування агрегованого каналу, що дозволить об'єднати декілька фізичних з'єднань для підвищення пропускної здатності (рис. 2.14).

```

Dist_SW_1#show etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  S - suspended
        R - Layer3       S - Layer2
        U - in use
Group Port-channel  Ports
-----+-----+-----
1      Po1(SU)      Fa1/4(P)  Fa1/5(P)

```

Рис. 2.14. Налаштування агрегованого каналу

Встановлення 802.1q на агрегованому каналі для передачі даних різних VLAN через один фізичний канал (рис. 2.15).

```

Dist_SW_1#show int po1 tr
Port      Mode      Encapsulation  Status      Native vlan
Po1       on         802.1q         trunking    1

```

Рис. 2.15. 802.1q на агрегованому каналі

Створення домену Active Directory для централізованого управління користувачами, групами, політиками безпеки, ресурсами та іншими об'єктами, що зберігаються в домені (рис. 2.16).

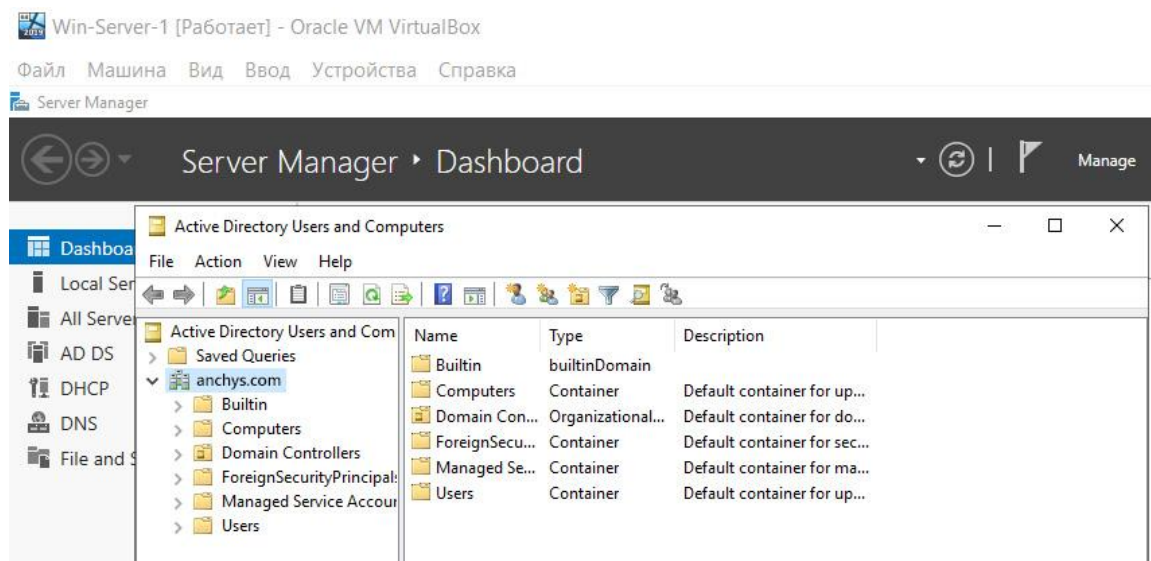


Рис. 2.16. домен Active Directory

Введення комп'ютера в домен для управління користувачами .введення політик безпеки та автоматизації процесів (рис. 2.17).

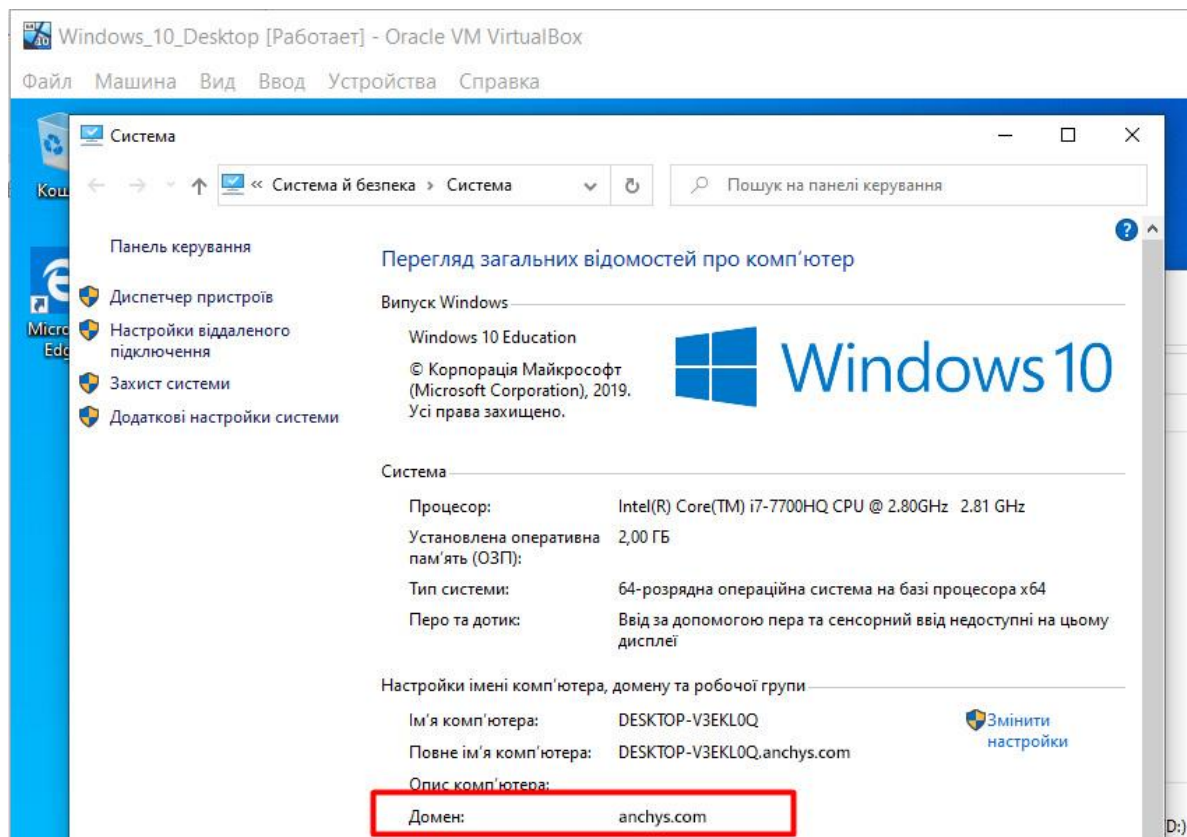


Рис. 2.17. Додавання робочої станції до домену

Висновки до другого розділу

Складено загальну структуру мережі. Виділено основні рівні мережі та описано їх функціонал.

Розробка схеми адресації є важливою складовою мережі, оскільки вона визначає адресаційний простір та розміщення пристроїв в мережі. При розробці схеми було враховано кількість пристроїв, їхню логічне групування.

Базові налаштування мережі дуже важливі для забезпечення її працездатності та ефективної роботи. Правильно налаштована мережа дозволяє забезпечити безперебійний доступ до інтернету, обмін даними між пристроями у мережі, а також зменшити ризик виникнення проблем з безпекою мережі.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

РОЗДІЛ 3. Налаштування EDR-захисту в мережі

3.1 Умови розгортання Microsoft Defender for EDR

Microsoft Defender for EDR забезпечує захист в реальному часі, виявляє й блокує загрози та має додаткові захисні можливості. Проте, щоб ефективно його використовувати, необхідно правильно спланувати його розгортання. У цьому контексті, важливо визначити, які пристрої та системи потребують захисту, яку конфігурацію використовувати, які правила поведінки й політики безпеки встановлювати та як забезпечувати постійну оновленість і моніторинг рішення.

Загалом планування розгортання можна представити як п'ятиетапний процес [10].

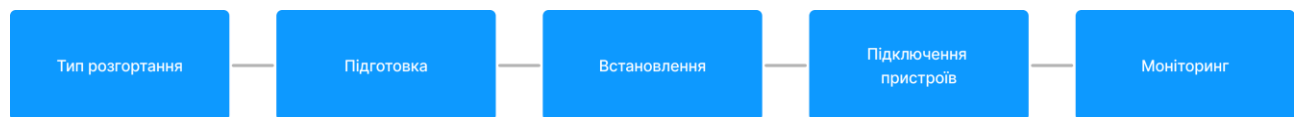


Рис. 3.1. – Етапи розгортання

Все починається з типу розгортання, потім потрібно підготувати середовище, правильно налаштувати, підключити пристрої, почати моніторинг і переконатися, що все захищено.

Тип розгортання дуже важливий для планування всієї стратегії розгортання.

Є три основні види розгортання, що залежать від величини мережі.

Evaluation

- Оцінюється здатність виробника
- Ефективність проекту з точки зору архітектури
- 5-50 пристроїв різних платформ

Рис. 3.2. – Оцінювання продукту РОС

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

Захист кінцевих точок може бути вузлом у всій системі безпеки підприємства, але все одно потрібно переконатися, що охоплено кожен аспект захисту кінцевих точок. Підприємства, незалежно від їх розміру, визначають певні значення або стандарти, щоб мати ефективний РОС(демонстрація практичної здійсненності технології з метою доказу того, що технологія робоча).

Саме перший вид розгортання є підходящим для поточної мережі, тому що наявність невеликої кількості пристроїв має невисоке навантаження та при цьому є досить гнучкою.

Pilot Deployment

- Ви в основному випробовуєте різні методи розгортання
- Ви знаєте, можливі проблеми, які можуть виникнути у вашому оточенні
- 200-300 пристроїв різних платформ

Рис. 3.3. – Пілотне розгортання

Пілотне розгортання під собою розуміє більш розгорнуту мережу з більшою кількістю кінцевих вузлів і має розуміння про можливі недоліки системи та їх уникнення в майбутньому.

Останнім етапом стане розгортання для всієї організації. Воно об'єднує в собі два попередні кроки, що використовуватимуться як проактивні заходи з точки зору забезпечення того, щоб усе було розгорнуто, як очікувалося.

Organization Wide Roll Out

- Ефективне планування
- Служба ІТ-обслуговування повинна бути готова вирішувати проблеми своєчасно, якщо вони з'являться
- Розгортання в масштабах організації — ви будете націлені на всі можливі кінцеві точки

Рис. 3.4. – Загальноорганізаційне впровадження.

Коли ми говоримо про розгортання в масштабах організації, кожна особа, є частиною системи, щоб зробити свій внесок у процес розгортання, знає про план і розуміє свої ролі та обов'язки.

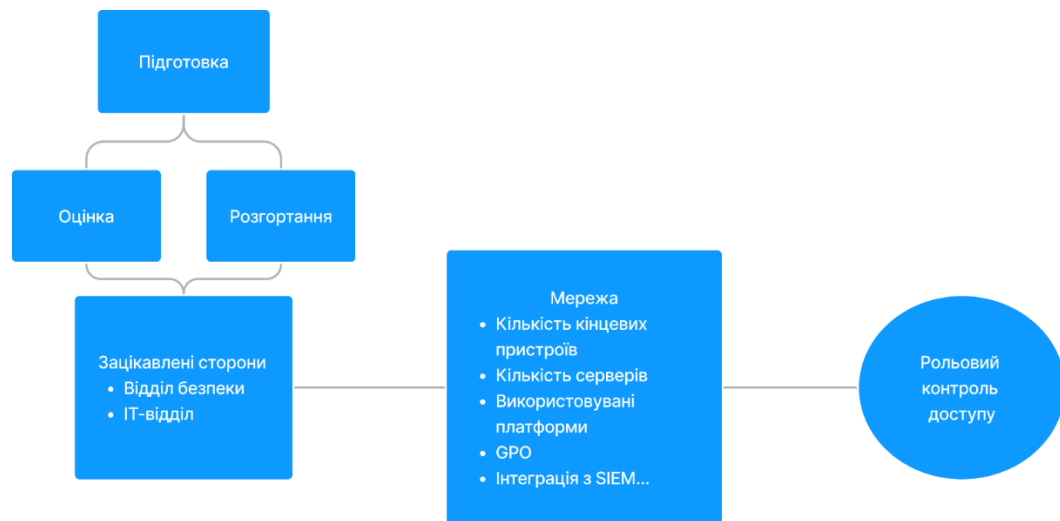


Рис. 3.5. – Умови забезпечення правильного розгортання

Перед розгортанням у всій організації всі працівники ІТ-команд і груп безпеки мають бути ознайомлені з певною консоллю, такою як securitycenter.windows.com або security.microsoft.com. Незалежно від типу розгортання, відповідні зацікавлені сторони повинні бути залучені, оскільки для успішного розгортання від кожної команди вимагається певний внесок.

Після визначення типу розгортання, відповідні зацікавлені сторони мають бути повідомлені і визначено кінцеву мету, також в Microsoft Defender for Endpoint повинно бути налаштовано правильний набір ролей, функцій або доступу.

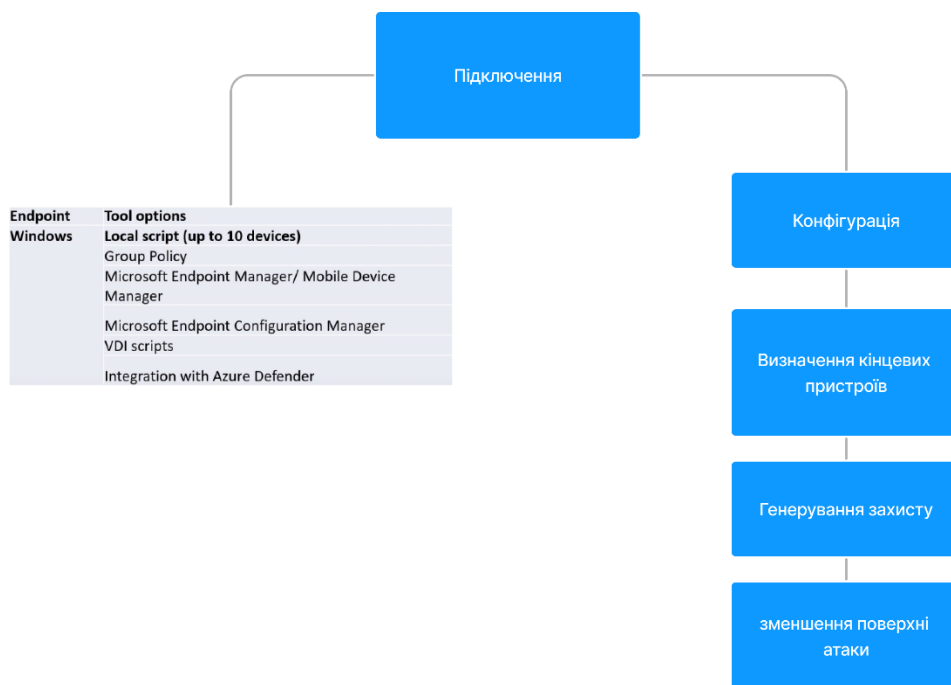


Рис. 3.6. – Порядок підключення та налаштування пристроїв

Якщо між пристроєм і службою кінцевої точки виникне будь-яке роз'єднання або неправильний зв'язок, результати будуть не такими, як очікується.

Для підключення пристроїв до Microsoft Defender for Endpoint існує декілька способів, що можна обрати відповідно до вимог.

Після додавання пристроїв потрібно налаштувати відповідні функції або послугу, які будуть виконувати захисні функції в мережі. Наприклад, виявлення кінцевої точки та реагування, захист наступного покоління або зменшення поверхні атаки.

Після ввімкнення всіх пристроїв і завершення необхідних налаштувань переходимо до основної мети розгортання EDR - перегляду сповіщень або аномалій. Це здійснюється у межах останнього етапу - етапу моніторингу.

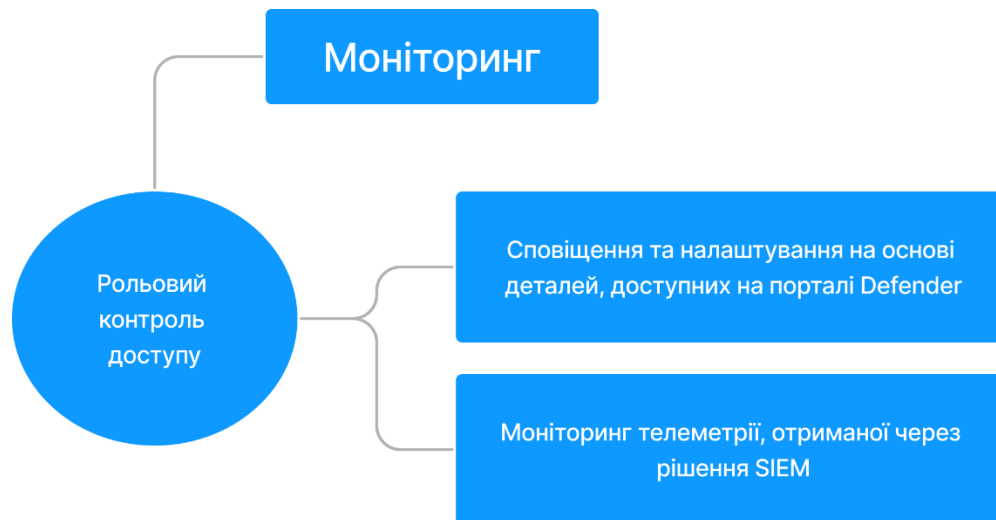


Рис. 3.7. – Принцип моніторингу загроз

При цьому, на основі налаштувань і конфігурації, сповіщення відображатимуться прямо на самому порталі Defender.

На основі правил, які ви спочатку визначили для команди безпеки, відповідна особа матиме повноважний доступ, щоб продовжувати та вносити зміни, так само адміністратор безпеки може вносити зміни в конфігурацію.

Все починається з надання правильного набору дозволів відповідним людям, щоб вони могли виконувати пов'язані з ними завдання. Таким чином можна організувати дуже ефективний моніторинг, що даватиме змогу відстежувати всі важливі події у даному середовищі та мати певність у тому, що застосовано правильний набір практик безпеки.

Якщо дотримуватися цих етапів планування розгортання, план розгортання буде значно кращим.

Є два портали, з яких можна отримати доступ до Microsoft Defender для кінцевих точок. Перший – це securitycenter.windows.com, який є спеціальним порталом для Microsoft Defender для кінцевих точок [12].

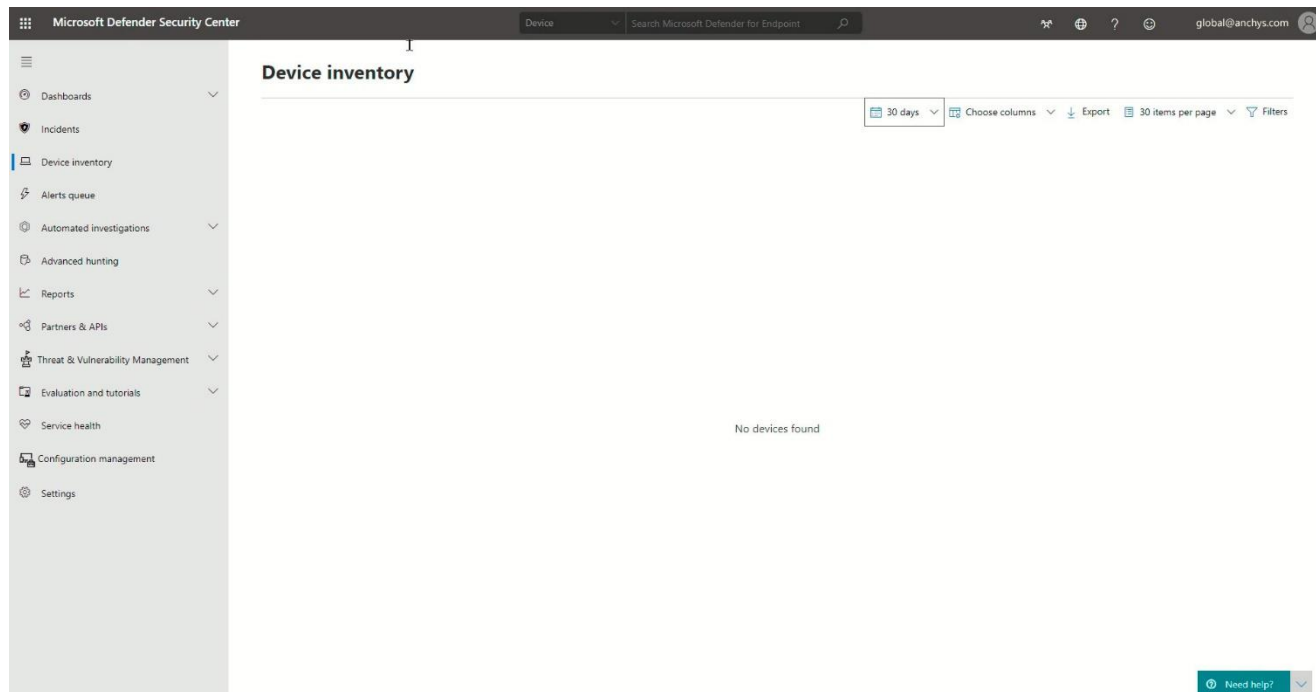


Рис. 3.8. – Портал Microsoft Defender

Другий – security.microsoft.com, який є новим порталом, який містить кілька служб безпеки.

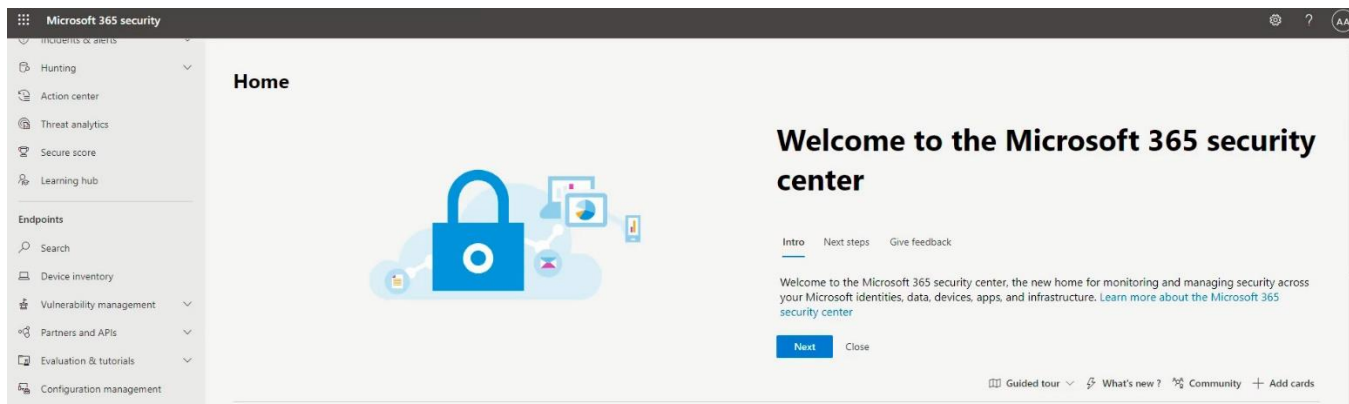


Рис. 3.9. – Портал Microsoft 365

Ще однією важливою функцією є переспрямування порталу. Після ввімкнення переспрямування порталу всі користувачі, які входять у систему на securitycenter.windows.com, будуть переспрямовані на цей конкретний портал.

Під час першого запуску майстра адаптації можна вибрати, де саме зберігати дані. Доступні такі місця для зберігання, як США, Великобританія та Європа, а верхня межа зберігання даних становить 180 днів.

У даному випадку варто обрати Європу, для швидшого оновлення даних.

З точки зору ввімкнення функцій попереднього перегляду все, що вам потрібно зробити, це натиснути розширені функції, прокрутити вниз і просто ввімкнути ту опцію, яку ви там побачите.

Щоб використовувати Microsoft Defender для кінцевих точок, потрібно мати відповідну ліцензію. Ці ліцензії включають Microsoft 365 E5, Microsoft 365 E5 Security, Microsoft 365 A5, Microsoft 365 E5 Compliance або Microsoft Defender for Endpoint Plan 1 або Plan 2.

В нашому випадку, ми маємо тимчасову ліцензію Plan 2, що дозволяє Microsoft Defender for Endpoints працювати з повноцінним функціоналом.

Щодо мережевих вимог, Microsoft Defender for Endpoints вимагає підключення до Інтернету та доступу до служб Microsoft Defender for Endpoint. Існує також залежність Microsoft Defender for Endpoints від Microsoft Defender for Anti-Malware або служби Microsoft Defender for Malware, яка працює на кінцевих точках.

3.2 Керування доступом користувачів у Microsoft Defender for Endpoint

Керування доступом на основі ролей в Microsoft Defender для кінцевих точок. Наприклад, група користувачів, до якої входять аналітики, повинні мати змогу лише переглядати інформацію про дії виконувани в мережі.

У Microsoft Defender існує три основні типи ролей: глобальний адміністратор, адміністратор безпеки та читач безпеки. Вони потрібні для надання користувачам відповідних прав [11].

Для великих компаній існує можливість поділу ролей за регіонами. Таким чином користувачі з встановленими ролями зможуть бачити лише пристрої, що входять саме до їх регіону.

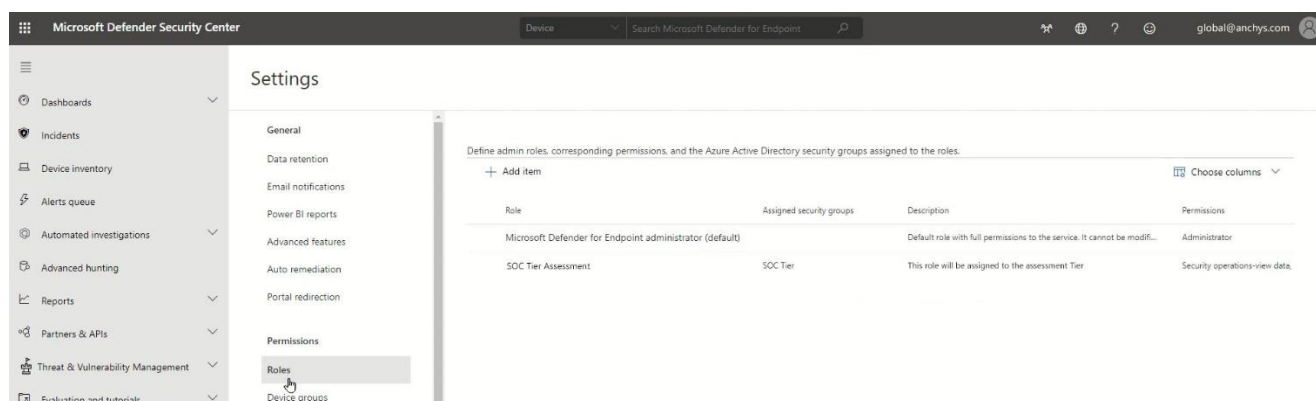


Рис. 3.10. – Створення ролі для аналітиків безпеки

В нашому випадку для даної мережі достатньо було створити додаткову роль для аналітиків безпеки, щоб вони мали відповідний доступ до порталу.

Оскільки мережа не надто розгалужена та знаходиться в межах одного підприємства, то не має сенсу створення ролей для різних підрозділів.

Використання ролі глобального адміністратора та однієї додаткової є цілком достатнім для використання, адміністрування та моніторингу системи.

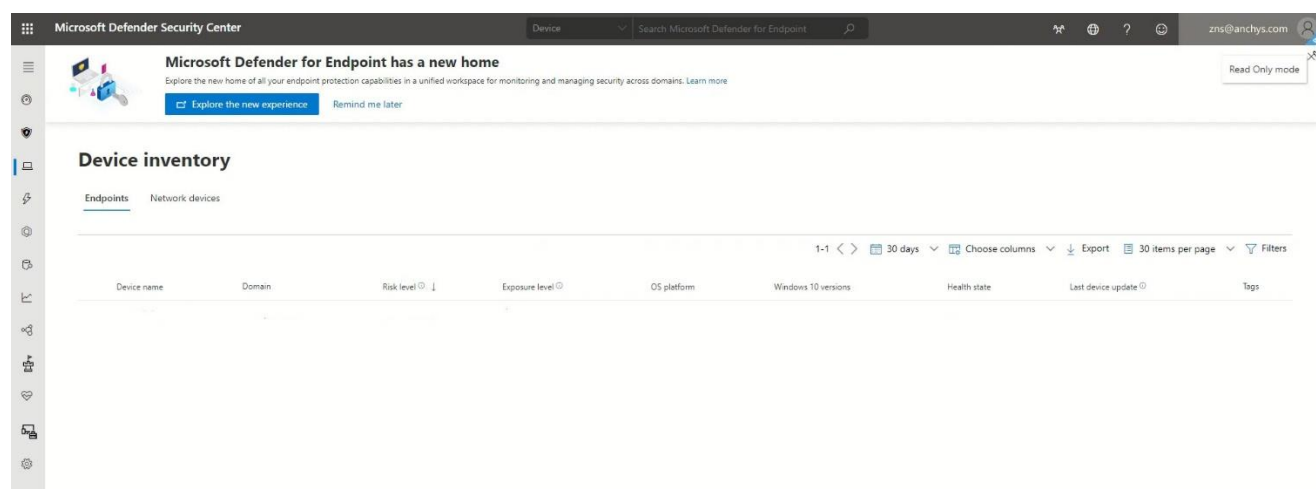


Рис. 3.11. – Read Only mode для аналітиків даних

Як ми можемо бачити, користувач знаходиться на рівні доступу, що дозволяє йому лише перегляд інформації (рис. 3.12).



Рис. 3.12. – Встановлені дозволи

Такі дозволи має група аналітиків.



Рис. 3.13. – Недоступність функцій

Тому при перегляді даних по одній з доступних машин, всі кнопки реагування будуть недоступні для користувача (рис. 3.14).

Request remediation for: Turn on Microsoft Defender Credential Guard

 You do not have the necessary permissions to submit a remediation request. Contact your administrator for details.

Рис. 3.14. – Заборона на виконання запиту

А при виконанні запиту можливо побачити оповіщення, що користувач не може виконати даних дій через недостатню кількість прав доступу (рис. 3.14).

Якщо ж увійти від імені адміністратора, то доступ до цих функцій буде дозволено (рис. 3.15).

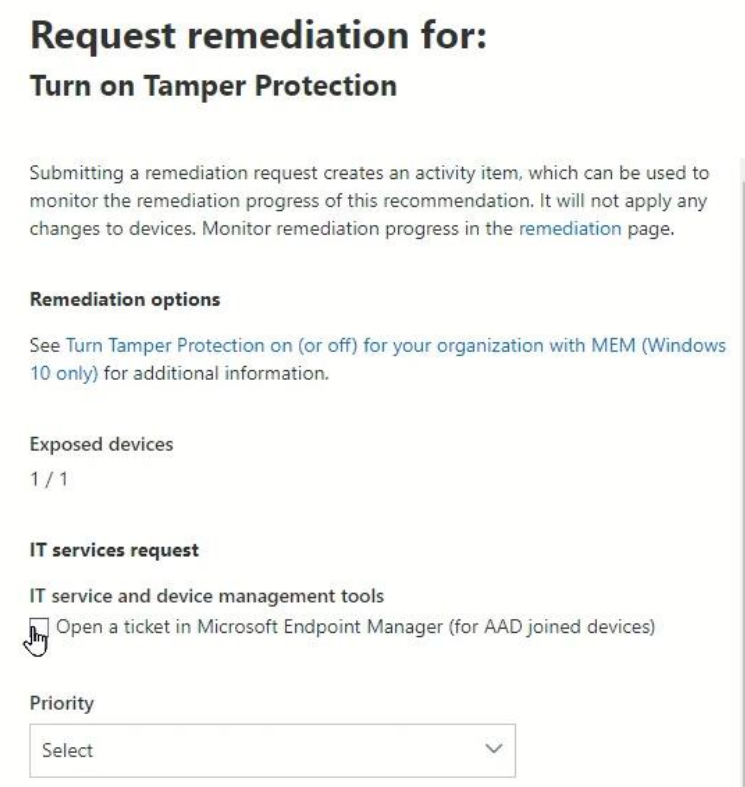


Рис. 3.15. – Запит від імені адміністратора

Загалом з технічного персоналу виділено 2 адміністратори та 3 особи аналітиків безпеки, що виконують аналіз потенційно небезпечних файлів.

Таблиця 3.1.

Технічний персонал

Адміністратор	global
	admin1
Аналітики безпеки	zns
	jho
	ags

3.3 Додавання пристроїв мережі до системи EDR

Опишемо процес адаптації пристроїв Windows 10 до Microsoft Defender for Endpoint.

Основним процесом адаптації є встановлення локального скрипта. Щоб розпочати цей процес, потрібно завантажити скрипт із порталу [20].

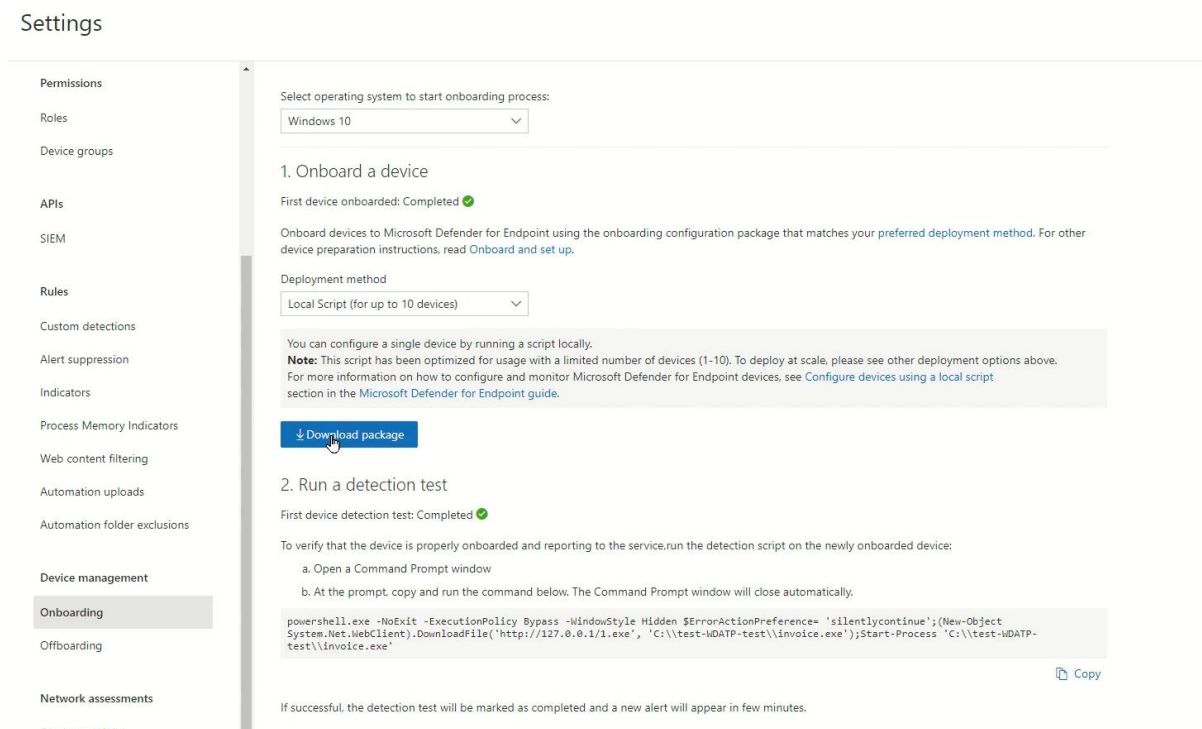


Рис. 3.16. – Завантаження відповідного скрипта

Після завантаження пакета потрібно запустити сценарій на пристрої, який буде підключено. Даний метод використовується для початкових пілотних пристроїв перед широким розгортанням рішення.

Але, перш ніж продовжити, потрібно переконатися, що всі конфігурації мережі та вимоги до ліцензування виконані.

Процес адаптації розглянуто на прикладі підключення «WS-1».

Сценарій запускається виключно з правами адміністратора. Після запуску сценарію необхідні записи реєстру повинні бути заповнені на пристрої.

```

Administrator: Command Prompt - WindowsDefenderATPLocalOnboardingScript.cmd
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\admin1\Desktop\WindowsDefenderATPLocalOnboardingPackage (5)

C:\Users\admin1\Desktop\WindowsDefenderATPLocalOnboardingPackage (5)>WindowsDefenderATPLocalOnboardingScript.cmd
This script is for onboarding machines to the Microsoft Defender for Endpoint services, including security and compliance products.
Once completed, the machine should light up in the portal within 5-30 minutes, depending on this machine's Internet connectivity availability and machine power state (plugged in vs. battery powered).
IMPORTANT: This script is optimized for onboarding a single machine and should not be used for large scale deployment.
For more information on large scale deployment, please consult the MDE documentation (links available in the MDE portal under the endpoint onboarding section).

Press (Y) to confirm and continue or (N) to cancel and exit: y

Starting Windows Defender Advanced Threat Protection onboarding process...

Testing administrator privileges
Script is running with sufficient privileges

Performing onboarding operations

Starting the service, if not already running

Windows Defender Advanced Threat Protection Service has not started yet
Waiting for the service to start

Successfully onboarded machine to Windows Defender Advanced Threat Protection

Press any key to continue . . .

```

Рис. 3.17. – Запуск сценарію

Щоб перевірити, чи пристрій успішно підключено, можна перейти до параметрів реєстру, які оновлюються після виконання процедури. Статус реєстрації можна знайти у розділі реєстру «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Advanced Threat Protection\Status». Успішна реєстрація відображатиме стан реєстрації 1, тоді як невдала – 0. Значення «org id» також можна порівняти зі значенням, отриманим із порталу.

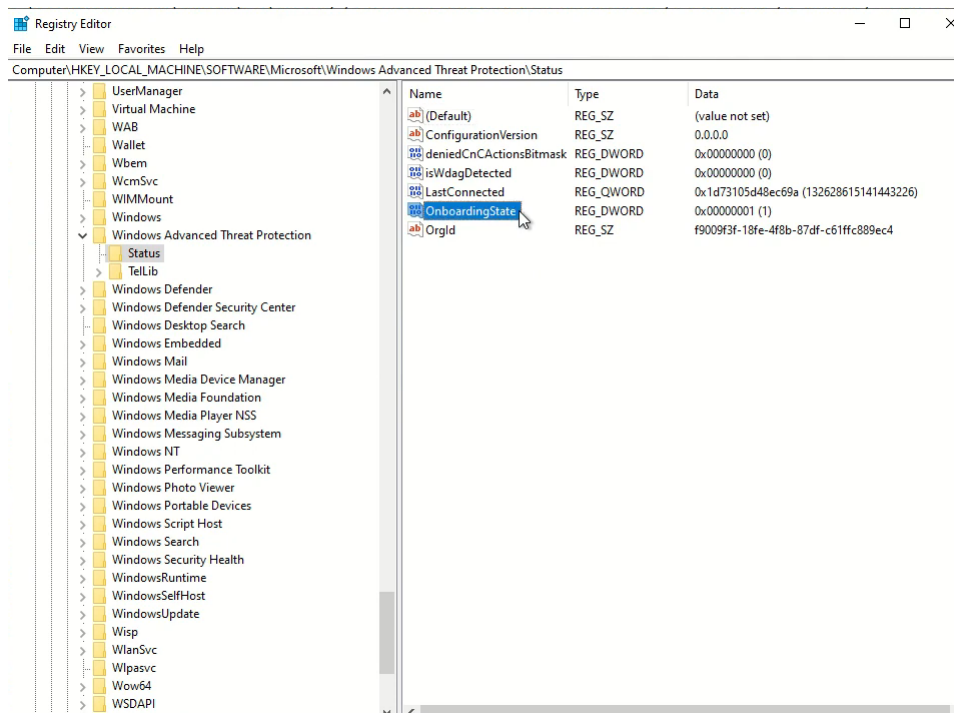


Рис. 3.18. – Перевірка реєстру

Щойно пристрій буде успішно зареєстровано, він має з'явитися на порталі Microsoft Defender for Endpoint протягом хвилини. Якщо цього не відбувається, може знадобитися усунення несправностей, щоб виявити будь-які проблеми з підключенням до мережі чи інші фактори.

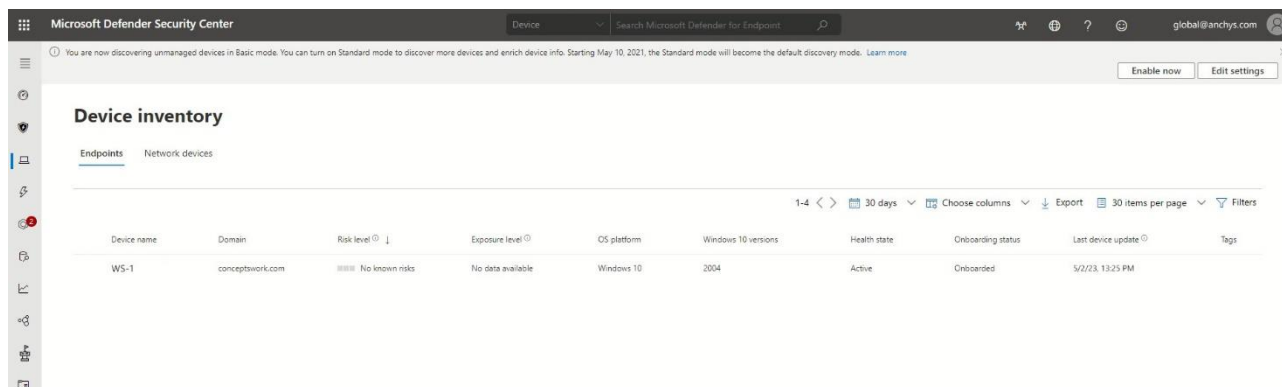


Рис. 3.19. – Результат додавання робочої станції

Інтегрування пристроїв Windows 10 за допомогою об'єктів групової політики [21].

Ми почнемо з розгортання та інсталяції пакета, а потім увімкнемо збір зразків для глибокого аналізу. Крім того, ми вивчимо необхідні журнали подій, щоб перевірити, чи успішно було зареєстровано пристрій. Нарешті, ми обговоримо інструмент аналізатора клієнта, сценарій, який допомагає у вирішенні проблем із підключенням. Отже, давайте зануримося в процес адаптації.

Для прикладу виконувалось підключення станції «WS-2».

Увійшовши в систему, потрібно обрати Windows 10 та «Групова політика», щоб завантажити пакет даних.

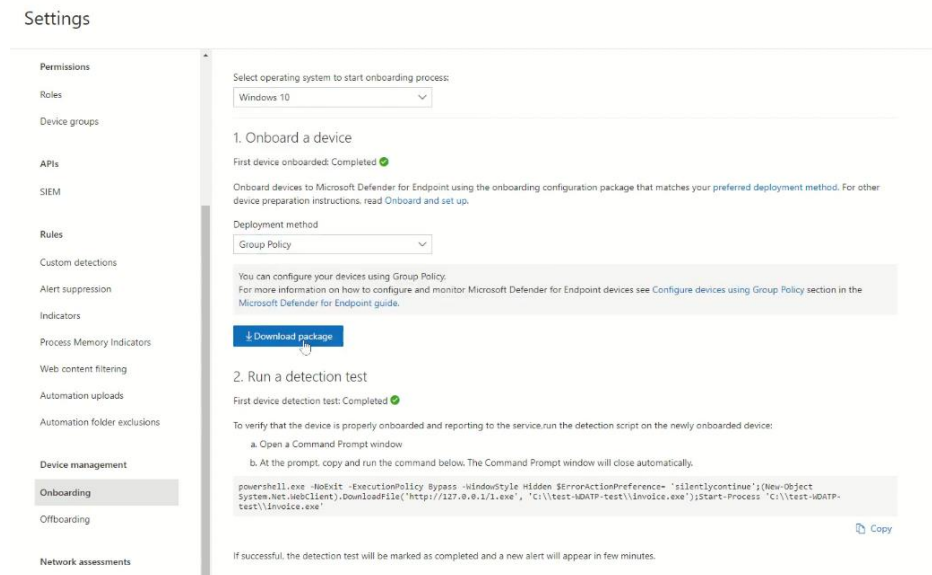


Рис. 3.20. – Завантаження пакету даних для групових політик

Створення об'єкта групової політики (GPO). Для цього потрібно відкрити консоль керування груповою політикою та створити нове GPO та нове завдання, яке розпочне процес реєстрації [9].

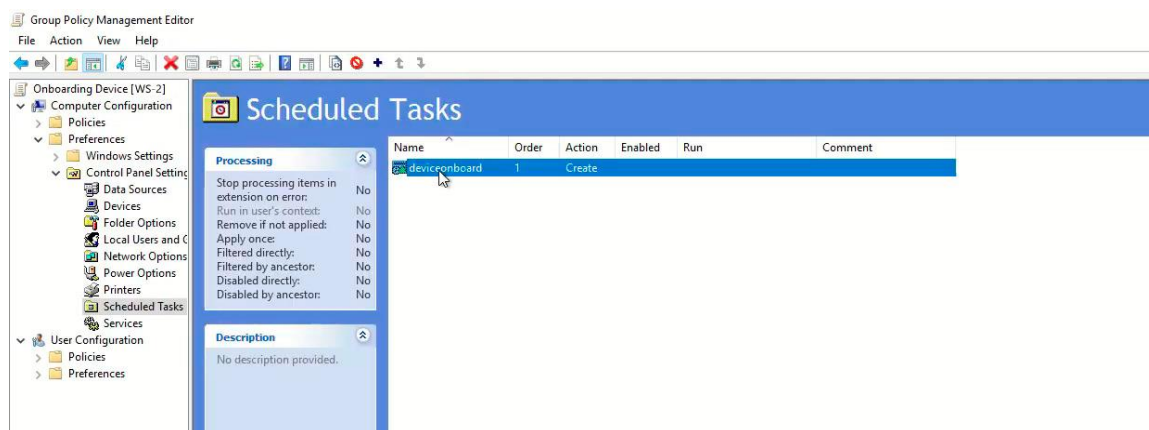


Рис. 3.21. – Створення завдання для групової політики

Увімкнення збору зразків для глибокого аналізу.

Оскільки папки «Windows Defender ATP» немає, перейти до попередньої конфігурації та до налаштувань панелі керування. Тут присутнє завдання адаптації пристрою.

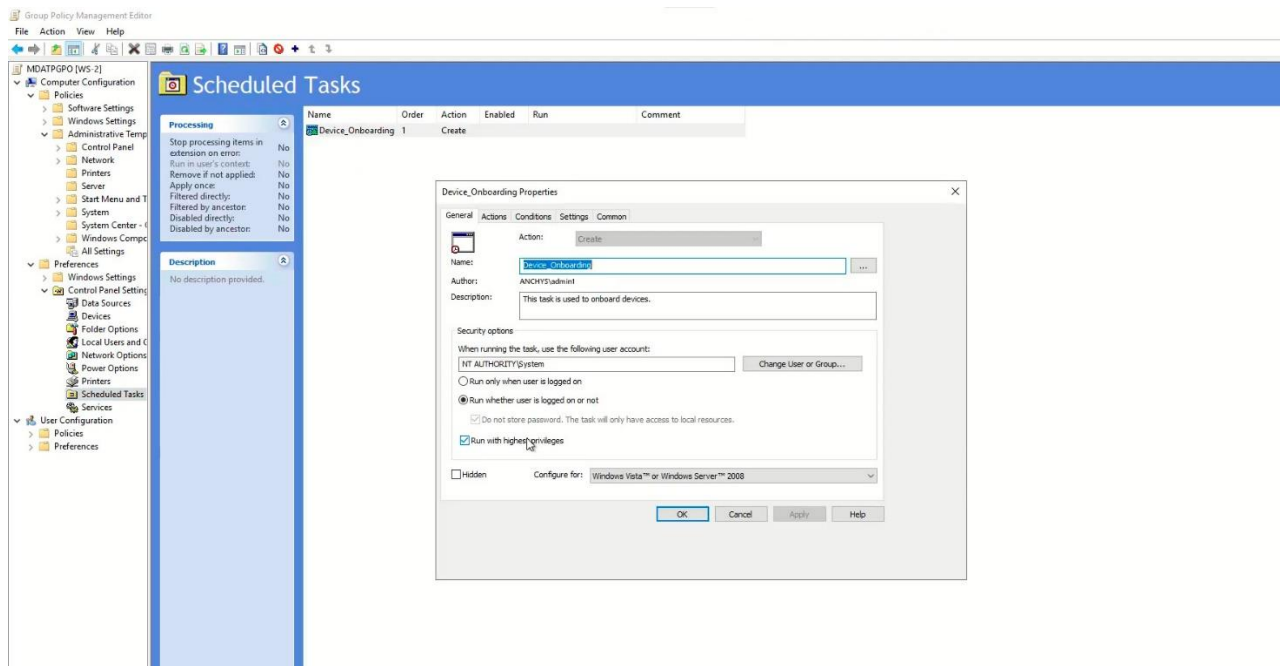


Рис. 3.22. – Адаптація пристрою

Потім помістити файли ADMX до Windows\PolicyDefinitions та ADML до Windows\PolicyDefinitions\en-US із завантаженого пакета до відповідної папки визначення політики.

Для того, щоб зміни швидше вступили в силу, в командному рядку виконується команда "gpupdate /force" на клієнтській машині, щоб оновити групову політику, а потім команда "gpresult /v", щоб перевірити, чи успішно застосовано GPO.

Після цього станція з'явиться на порталі.

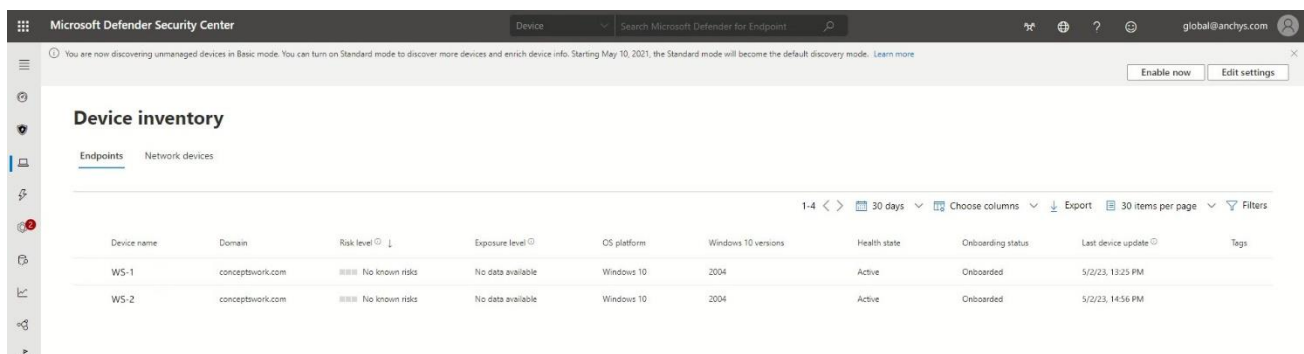


Рис. 3.23. – Результат додавання робочої станції

Далі розглянуто процес адаптації до Windows Server 2019 і передумови, про які потрібно пам'ятати, щоб забезпечити успішну адаптацію до MDE (Microsoft Defender for Endpoint).

Щоб Windows Server 2019 успішно підключився до MDE, переконайтеся, що AV-компонент Windows Defender інстальовано та служба Windows Defender запущена на машині та встановлені останні оновлення безпеки.

Перший крок — перевірити, чи AV-служба встановлена та запущена на машині. Команди "sc query windefend" та "sc qc windefend" використовуються саме для того, щоб перевірити стан служби.

```
SERVICE_NAME: windefend
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

C:\>sc qc windefend
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: windefend
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 2   AUTO_START
        ERROR_CONTROL       : 1   NORMAL
        BINARY_PATH_NAME    : "C:\Program Files\Windows Defender\MsMpEng.exe"
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : Windows Defender Antivirus Service
        DEPENDENCIES        : RpcSs
        SERVICE_START_NAME  : LocalSystem
```

Рис. 3.24. – Перевірка встановлення служби

Після перевірки реєстру на машині перед підключенням (аналогічно до підключення звичайної робочої станції) можна починати адаптацію.

На порталі обрано потрібну версію скрипта і завантажити його (рис. 3.25).

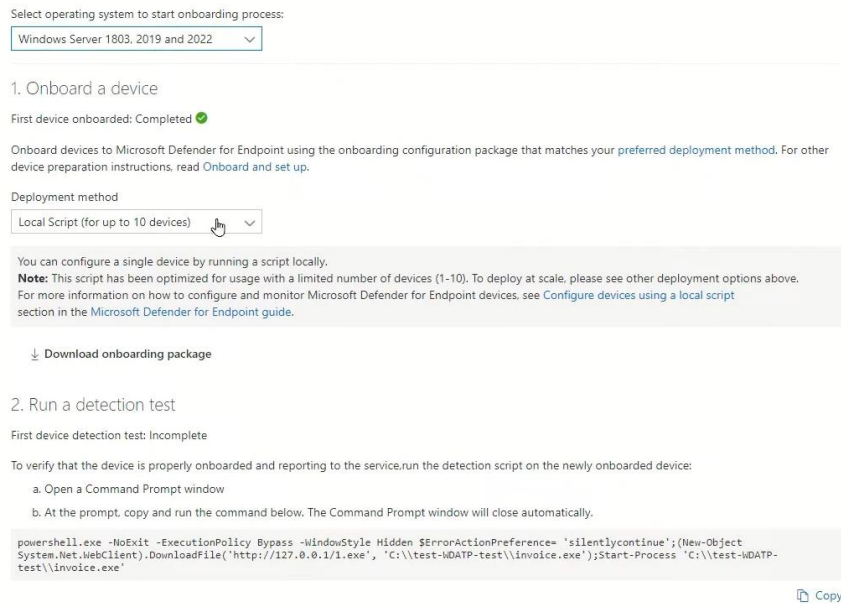


Рис. 3.25. – Завантаження скрипта для Windows-сервера

Для цього потрібно запустити завантажений скрипт, всі дії потрібно виконувати від імені адміністратора.

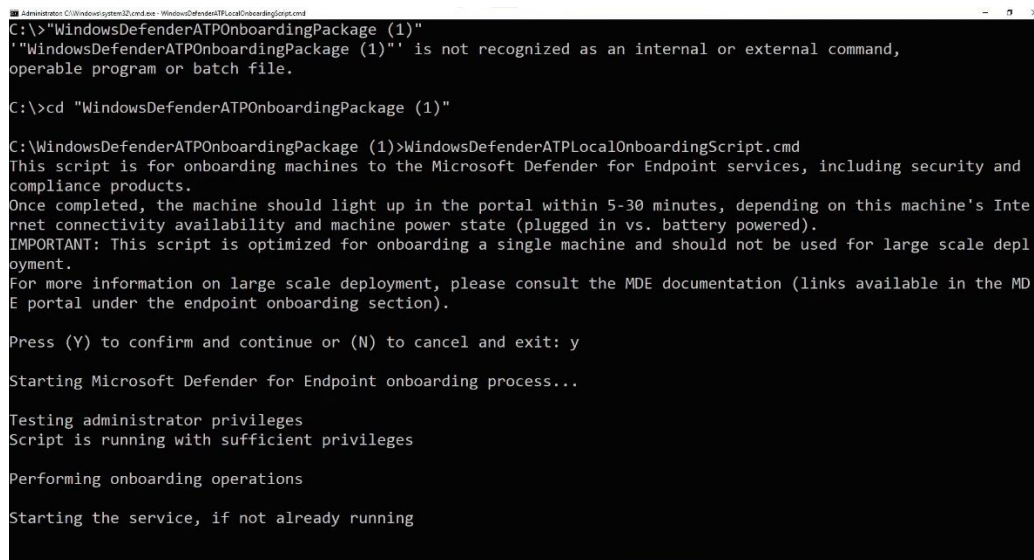


Рис. 3.26. – Запуск скрипта

Після встановлення, потрібно перевірити чи працює відповідна служба на даній машині. Для цього використовуємо команду «sc qc sense» (рис. 3.27).

```
C:\WindowsDefenderATPOnboardingPackage (1)>sc query sense

SERVICE_NAME: sense
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                                (NOT_STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
```

Рис. 3.27. – Перевірка роботи служби

Підключений до системи сервер можна побачити в списку всіх пристроїв на порталі (рис. 3.28).

Device name	Domain	Risk level	Exposure level	OS platform	Windows 10 versions	Health state	Onboarding status	Last device update	Tags
WS-1	conceptswork.com	No known risks	No data available	Windows 10	2004	Inactive	Onboarded	5/2/23, 13:23 PM	
WS-2	conceptswork.com	No known risks	No data available	Windows 10	2004	Inactive	Onboarded	5/2/23, 14:56 PM	
Win-Serv-1	conceptswork.com	No known risks	No data available	Windows Server 20...		Active	Onboarded	5/2/23, 19:31 PM	

Рис. 3.28. – Результат додавання сервера

Таким чином мають бути підключені всі робочі станції мережі. рис. 3.29 показано даний етап.

Device name	Domain	Risk level	Exposure level	OS platform	Windows 10 versions	Health state	Onboarding status	Last device update	Tags
WS-1	conceptswork.com	No known risks	No data available	Windows 10	2004	Inactive	Onboarded	5/2/23, 13:23 PM	
WS-2	conceptswork.com	No known risks	No data available	Windows 10	2004	Inactive	Onboarded	5/2/23, 14:56 PM	
Win-Serv-1	conceptswork.com	No known risks	No data available	Windows Server 20...		Active	Onboarded	5/2/23, 19:31 PM	
WS-3	conceptswork.com	No known risks	No data available	Windows 10	2004	Inactive	Onboarded	5/3/23, 10:17 AM	
WS-4	conceptswork.com	No known risks	No data available	Windows 10	2004	Inactive	Onboarded	5/3/23, 11:42 AM	
WS-5	conceptswork.com	No known risks	No data available	Windows 10	2004	Inactive	Onboarded	5/3/23, 13:15 PM	
WS-6	conceptswork.com	No known risks	No data available	Windows 10	2004	Active	Onboarded	5/3/23, 14:38 PM	
WS-7	conceptswork.com	No known risks	No data available	Windows 10	2004	Active	Onboarded	5/3/23, 17:58 PM	

Рис. 3.29. – Всі додані робочі станції

3.4 Керування загрозами та вразливостями засобами Microsoft Defender for Endpoint

Керування загрозами та вразливостями (Threat and Vulnerability Management, TVM) - це можливість, доступна в Microsoft Defender for Endpoint, яка може допомогти виявити та усунути вразливості, слабкі місця або неправильні конфігурації, які існують на кінцевих точках [17].

Загалом, керування загрозами та вразливістю є однією зі служб, які пропонує Microsoft Defender, і є основою всього захисту. Метою цієї служби є захист ваших кінцевих точок шляхом виявлення та усунення вразливостей, слабких місць і неправильних конфігурацій, які існують на певному пристрої.

Загальний спосіб роботи достатньо простий, основною умовою є підключення станції до системи, щоб була можливість надсилати дані до служби, на основі яких TVM зможе надавати рекомендації щодо безпеки.

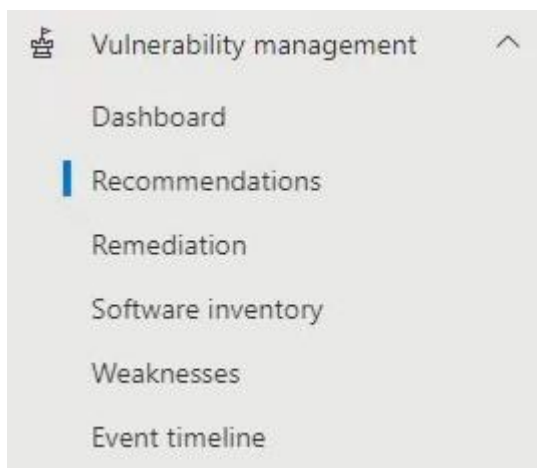


Рис. 3.30. – Функціонал TVM

На порталі знаходиться розділ, що включає в себе весь функціонал Threat and Vulnerability Management.

До розділу надається рольовий контроль доступу при створенні ролей для користувачів.

Інформаційна панель - це інструмент, що надає докладну інформацію про вразливості, ризики та рекомендації з питань безпеки. Ви зможете ознайомитися з останніми заходами з усунення проблем, переглянути уражені пристрої та знайти способи покращення загальної безпеки компанії. Кожен пункт на інформаційній панелі має посилання на більш детальну інформацію або на сторінку, де ви зможете виконати рекомендовані дії [13].

Рекомендації - тут можна ознайомитися з поточними рекомендаціями щодо безпеки та відповідною інформацією про потенційні загрози. Коли ви виберете елемент зі списку, відкриється панель з докладнішою інформацією про загрози та дії, які ви можете вжити.

Виправлення - тут перелічені всі дії, що були зроблені щодо усунення проблем, разом із їх статусом. Дії з виправлення можуть включати відправлення файлу в карантин, зупинку виконання процесу та блокування виявленої загрози. Заходи з усунення також можуть включати оновлення пристроїв, запуск антивірусного сканування та інші дії.

Інвентаризація - тут ви знайдете список програмного забезпечення та програм, що використовуються в вашій організації. Ви побачите веб-переглядачі, операційні системи та інше програмне забезпечення на пристроях, а також будуть вказані виявлені слабкі місця та загрози.

Слабкі сторони - цей розділ містить список вразливостей, разом з кількістю пристроїв в вашій організації, які їм піддаються. Якщо ви бачите "0" в розділі "Піддані ризику пристрої", то негайних дій не потрібно. Однак, ви можете отримати більше інформації про кожну вразливість, перераховану на цій сторінці. Обирайте елемент, щоб дізнатися більше про нього та про можливі заходи для зменшення потенційних загроз вашій компанії.

Хронологічна шкала подій - цей розділ відображає вразливості, які впливають на вашу організацію, у вигляді хронологічної шкали часу.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

3.5 Налаштування Microsoft Defender Application Guard

Microsoft Defender Application Guard (MDAG) — це безпекова функція, доступна, що є доступною для 10 та 11 версій Windows. MDAG забезпечує ізоляцію та захист від потенційно шкідливих файлів та веб-сайтів, зменшуючи ризик від атак та заражень комп'ютера [18].

Веб-ізоляція є основною функцією MDAG та дозволяє запускати небезпечні веб-сайти та файли в ізольованому середовищі, що відділяється від основної операційної системи. Це допомагає запобігти поширенню шкідливих програм, відокремлює процеси від основної системи та захищає її від можливих загроз.

Працює з невеликою кількістю веб-браузерів: Edge, Chrome, Mozilla, Internet Explorer, а також з усіма програмами MS Office.

Оскільки MDAG працює в окремому віртуальному середовищі, шкідливі програми або веб-сайти не зможуть проникнути або пошкодити систему, що забезпечить уникнення атак спричинених взаємодією зі шкідливими вмістом.

Адміністратори можуть встановлювати обмеження на доступ до файлів, друк, камери, мікрофону та інших ресурсів для підвищення безпеки.

Найпростішим для налаштування є автономний режим. Він дозволяє користувачам вручну запускати віртуалізований контейнер браузера Microsoft Edge. Цей режим в основному використовується для отримання досвіду та розуміння того, як працює функція.

Проте автономний режим має деякі обмеження. Він не керується жодною політикою чи контролем. Користувачам потрібно вручну відкрити вікно Application Guard, щоб отримати доступ до потенційно шкідливих сайтів.

Щоб увімкнути Microsoft Defender Application Guard існує два способи GUI або PowerShell. Метод GUI доступний, лише якщо ваша машина відповідає апаратним вимогам, які включають принаймні 4 ядра ЦП і 8 ГБ оперативної пам'яті. Однак PowerShell можна використовувати для встановлення, навіть якщо вимоги до

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

апаратного забезпечення не виконано, хоча у такому разі ця функція може не працювати належним чином.

Для запуску Application Guard на віртуальній машині з нижчою конфігурацією апаратного забезпечення, потрібно змінити деякі параметри реєстру (рис. 3.31), щоб примусово встановити цю функцію.

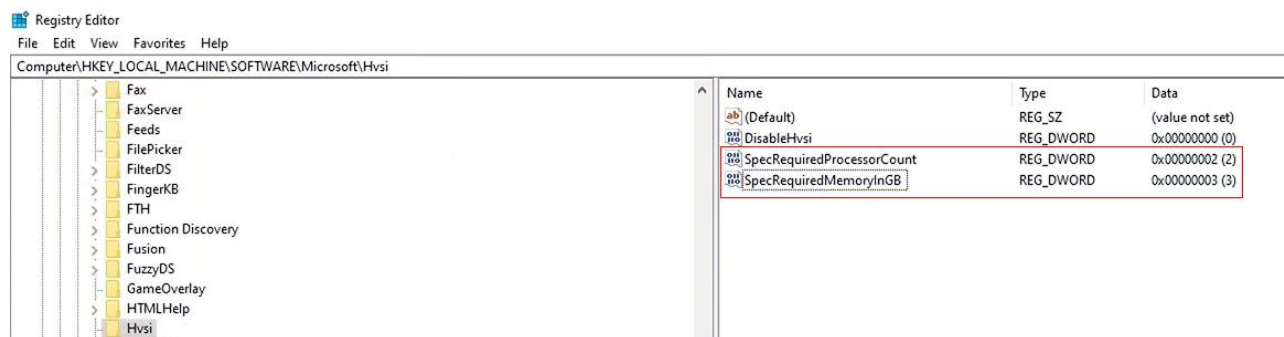


Рис. 3.31. – Додаткові записи реєстру для слабких робочих станцій

Після чого необхідно запустити дану функцію.



Рис. 3.32. – Запуск MDAG

В браузері з'явиться можливість увімкнути віртуалізований екземпляр Microsoft Edge, вибравши відповідний параметр у меню браузера. Диспетчер завдань

покаже новий запис для вікна Application Guard, вказуючи, що воно працює в контейнерному та ізольованому середовищі.

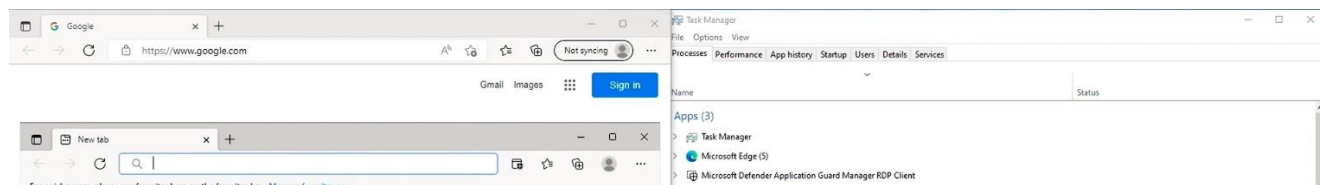


Рис. 3.33. – Безпечний режим браузера

Щоб перевірити журнали подій, пов'язані з Microsoft Defender Application Guard, можна скористатися засобом перегляду подій і перейти до папок, які починаються з «MDAG». Ці журнали містять інформацію про поведінку та події, пов'язані з Application Guard.

Корпоративний режим дозволяє визначити коло довіри, включаючи IP-адреси, хмарні ресурси, мережеві домени та проксі-сервери. Крім того, це дає змогу визначати політики обміну даними між віртуалізованими примірниками та різними браузерами та програмами. Цей режим можна ввімкнути за допомогою групової політики.

В даній мережі було обмежено доступ всім користувачам до мережних ресурсів та дозволено доступ лише до порталів Microsoft Defender, Azure, Google і docs.microsoft.com. Ці URL-адреси представляють коло довіри. Коли адміністратор отримує доступ до будь-якого ненадійного ресурсу, він буде відкритий у віртуалізованому екземплярі програм Microsoft Edge або Office.

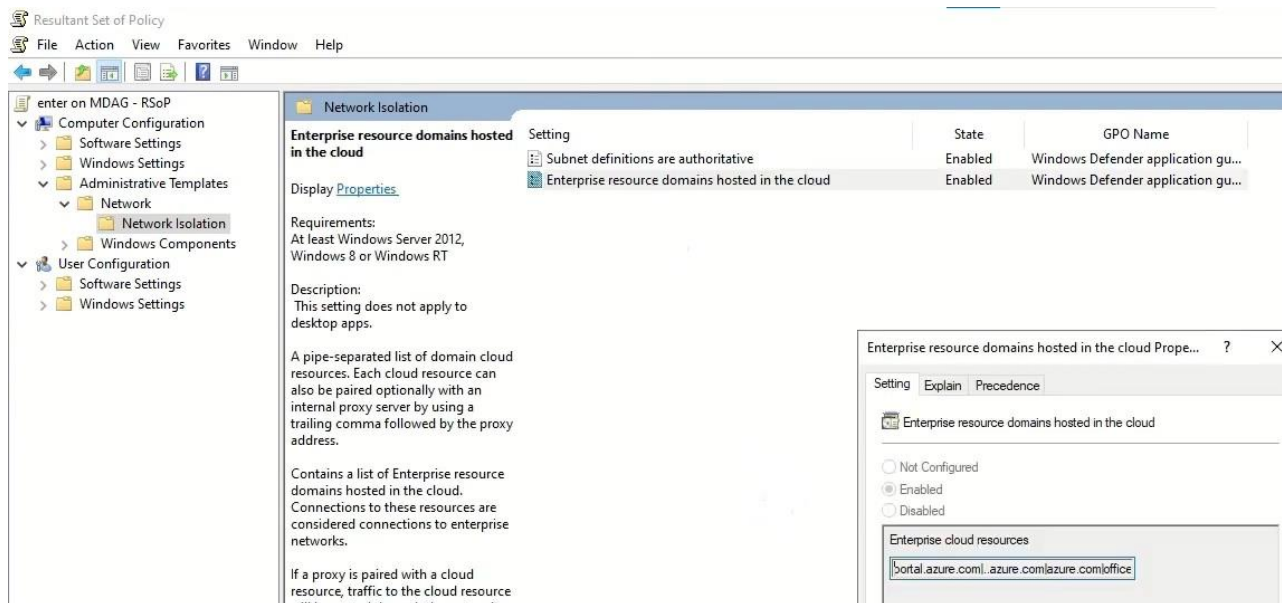


Рис. 3.34. – Дозволені сторінки для входу

Тепер, якщо я відкрию Microsoft Edge і спробую відвідати попередньо вказані сторінки, оскільки ці URL-адреси є частиною кола довіри, вони відкриються в браузері за замовчуванням без жодних додаткових дій.

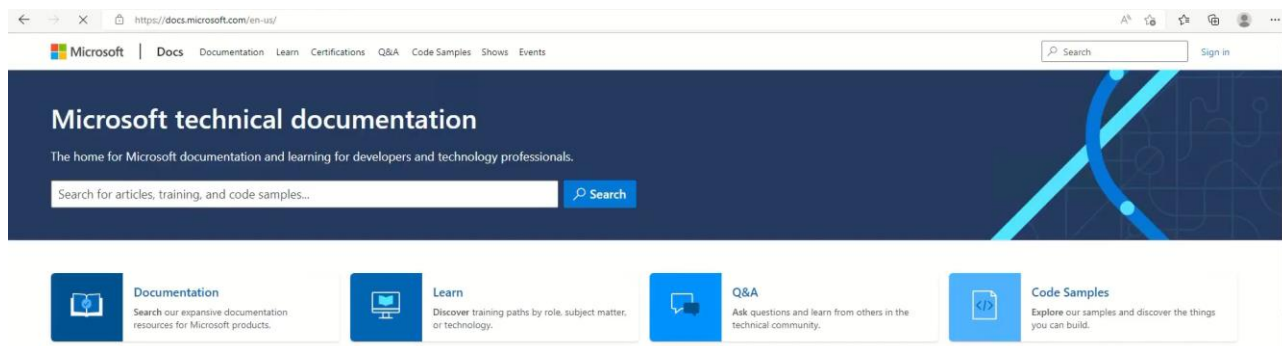


Рис. 3.35. – Відкрита веб-сторінка ресурсу docs/microsoft.com

Проте якщо перейти за будь-яким іншим посиланням, наприклад oracle.com, яке не входить до кола довіри, буде запущено віртуалізований екземпляр Edge.

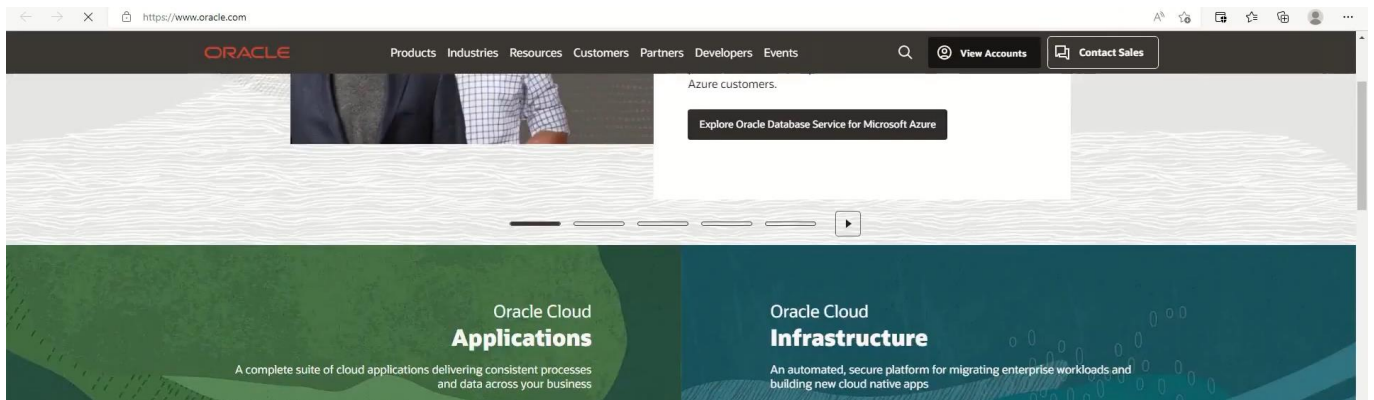


Рис. 3.36. – Запуск в безпечному режимі

Також можливо встановити обмеження на копіювання картинок, але копіювання тексту буде доступним.

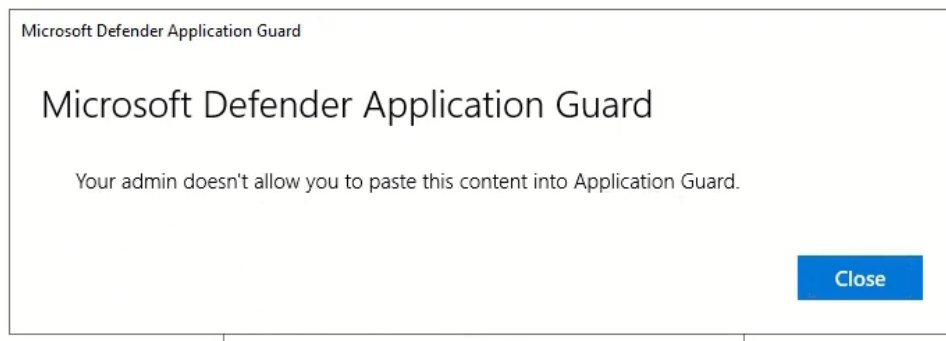


Рис. 3.37. – Заборона на виконання дій

Таким чином при спробі вставити скопійовану картинку до документу Word буде отримано вікно заборони MDAG на виконання даної дії.

3.6 Правила зменшення поверхні атаки за допомогою Windows Defender Exploit Guard

Дуже важливою частиною захисту кінцевих вузлів також є правила зменшення поверхні атаки(Attack Surface Reduction Rules). Призначено для зменшення атакованої площини (attack surface) і покращення безпеки комп'ютерів та пристроїв в організації.

Загалом надається 16 основних правил, що налаштовуються.

Таблиця 3.2.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

Правила зменшення поверхні атаки

Правила	ID	Статус
Блокувати зловживання експлуатованими вразливими підписаними драйверами	56a863a9-875e-4185-98a7-b882c64b5ce5	Audit
Заборона Adobe Reader для створення дочірніх процесів	7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c	Audit
Заборонити всім програмам Office створювати дочірні процеси	d4f940ab-401b-4efc-aadc-ad5f3c50688a	Block
Блокувати викрадення облікових даних із підсистеми локального центру безпеки Windows (lsass.exe)	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2	Block
Блокувати виконуваний вміст клієнта електронної пошти та веб-пошти	be9ba2d9-53ea-4cdc-84e5-9b1eeee46550	off
Блокувати запуск виконуваних файлів, якщо вони не відповідають критеріям поширеності, віку чи довіреного списку	01443614-cd74-433a-b99e-2ecdc07bfc25	Audit
Блокувати виконання потенційно обфускованих сценаріїв	5beb7efe-fd9a-4556-801d-275e5ffc04cc	Block
Заблокувати JavaScript або VBScript від запуску завантаженого виконуваного вмісту	d3e037e1-3eb8-44c8-a917-57927947596d	Block
Заборонити програмам Office створювати виконуваний вміст	3b576869-a4ec-4529-8536-b80a7769e899	Block
Заборонити програмам Office впроваджувати код в інші процеси	75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84	Block
Блокувати програму зв'язку Office від створення дочірніх процесів	26190899-1602-49e8-8b27-eb1d0a1ce869	Audit
Блокувати збереження через підписку на події WMI	e6db77e5-3df2-4cf1-b95a-636979351e5b	Audit
Блокувати створення процесів, що походять від команд PSEXEC і WMI	d1e49aac-8f56-4280-b9ba-993a6d77406c	Block
Блокувати ненадійні та непідписані процеси, які запускаються з USB	b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4	Block
Блокувати виклики API Win32 із макросів Office	92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b	Block

Використовуйте розширений захист від програм-вимагачів	c1db55ab-c21a-4637-bb3f-a12568109d35	Block
--	--------------------------------------	-------

Щоб увімкнути правила зменшення поверхні атаки, потрібно пам'ятати про кілька ключових моментів. Під час налаштування об'єкта групової політики потрібно перебувати в режимі аудиту. Також в налаштуваннях Windows Defender Exploit Guard в об'єкті групової політики потрібно переконатися, що інстальовано необхідні папки та оновлені файли адмх.

У конфігурації встановлюємо значення 2 для режиму аудиту та 1 для режиму блокування. Однак варто зауважити, що значення 6 також можна використовувати для одного режиму, як зазначено в офіційних статтях [14].

Щоб продемонструвати конфігурацію правил зменшення поверхні атаки, було налаштовано групову політику для VLAN50 під назвою ASR та налаштовано необхідні параметри для застосування до клієнтських машин.

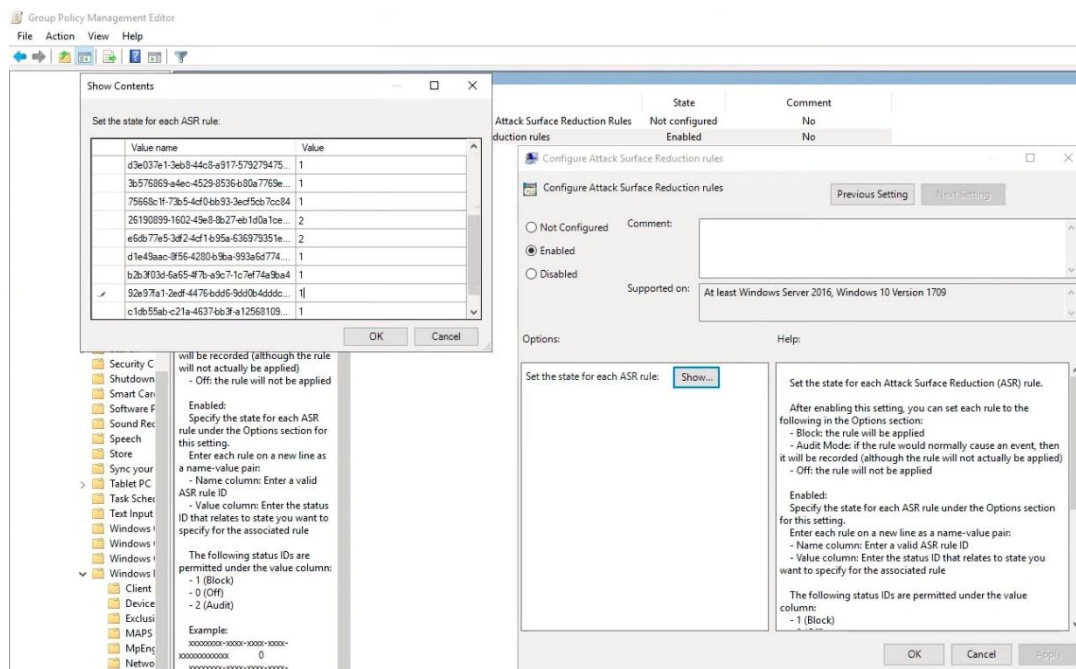


Рис. 3.38. – Встановлення правил зменшення поверхні атаки у відповідні положення

Після оновлення налаштувань групової політики та запуску оновлення GP клієнтська машина отримає налаштовані правила.

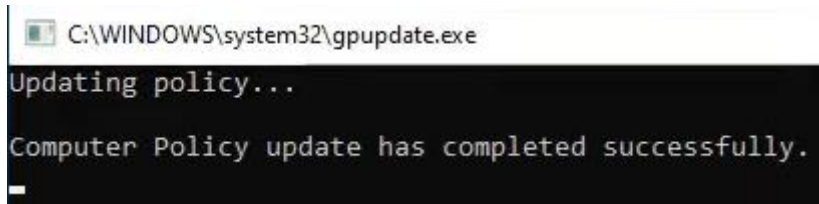


Рис. 3.39. – Оновлення політик

За допомогою команди Get-MpPreference перевіряється застосування політики.

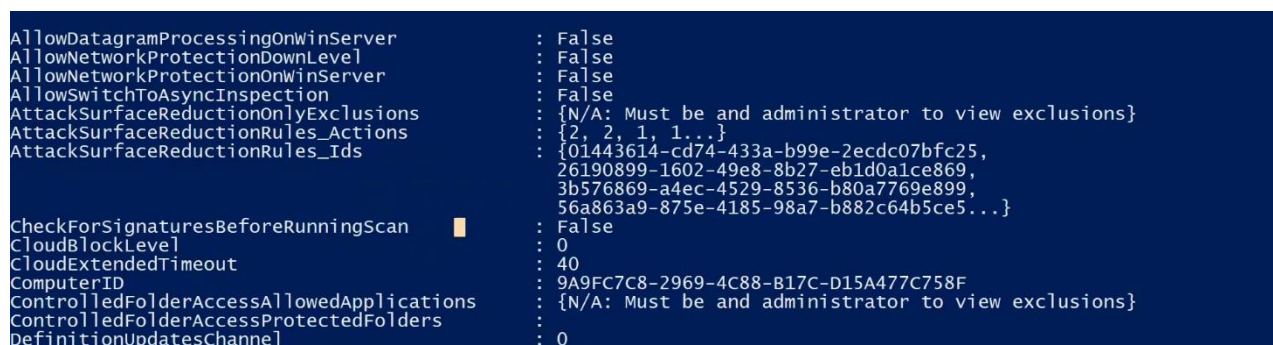


Рис. 3.40. – Перевірка застосування правил

Перевірити роботу правил можливо побачити при використанні команд PSEXEC (рис. 3.41).

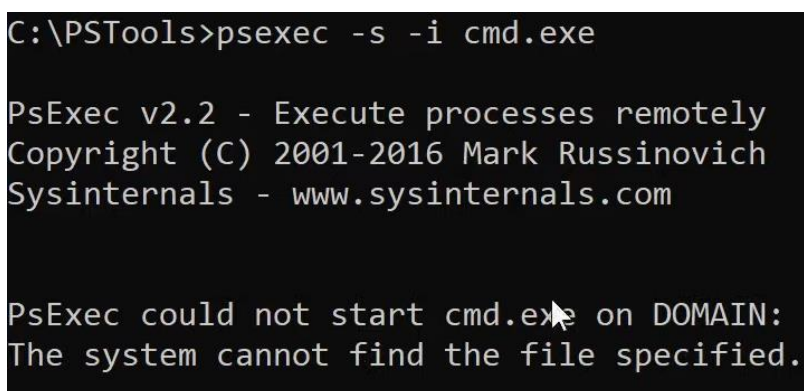


Рис. 3.41. – Спроба виконання команди PSEXEC

Після запуску отримаємо очікувану поведінку Windows Defender – процес PSEXESVC.exe заблоковано (рис. 3.42).

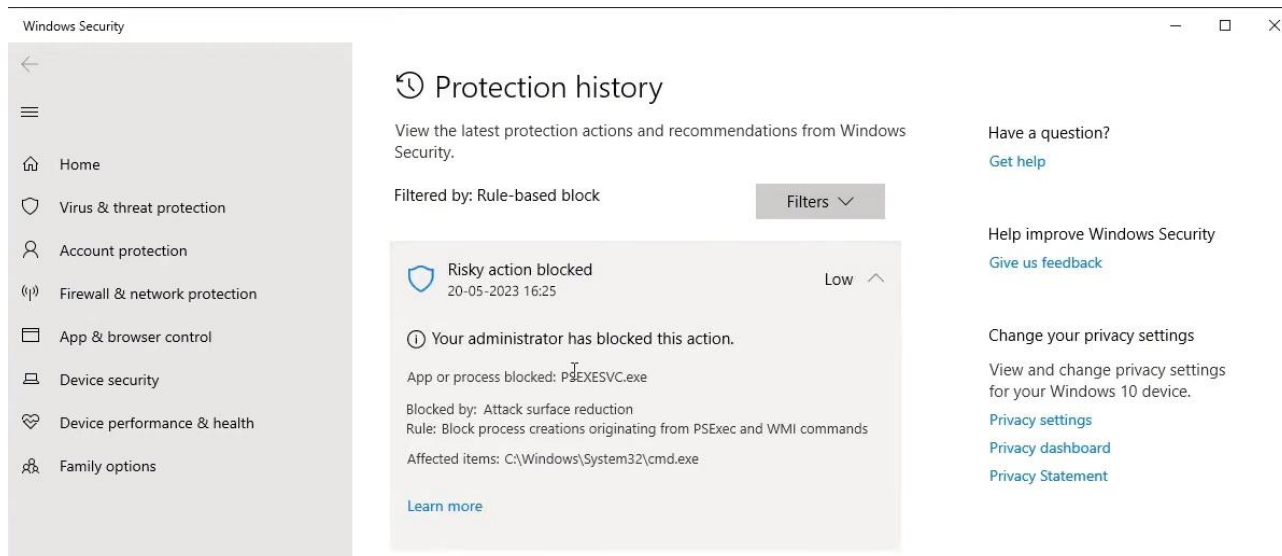


Рис. 3.42. – Блокування виконання команди

Налаштування правил зменшення поверхні атаки за допомогою групової політики є важливим кроком у підвищенні безпеки мережі.

3.7 Симуляція атаки на кінцевий пристрій

Для перевірки правильної роботи системи було застосоване автоматизоване дослідження та полювання за шкідливим ПЗ. В даному сценарії було симульовано атаку, яка запускає новий троян для Microsoft Defender для тестування можливостей автоматизованого розслідування кінцевих точок.

Ця можливість автоматизує перевірку та усунення відповіді на атаку. Під час реагування автоматизоване дослідження визначає та видаляє відомі артефакти атаки з уражених пристроїв. Microsoft Defender також може автоматично переходити до інших пристроїв, які можуть постраждати, і застосовувати ті самі відповідні дії.

Для запуску процесу було завантажено файл симуляції. З його допомогою моделюється атака. Даний файл може бути надіслано через фішинговий електронний лист. Документ містить код макросу, який скидає та завантажує виконуваний файл на пристрій.

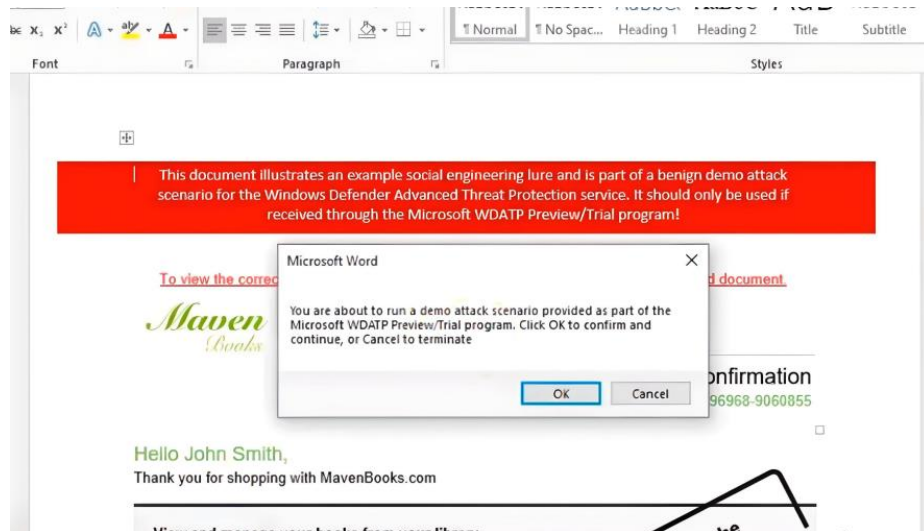


Рис. 3.43. – Запуск симуляції

Симуляція атаки на цьому закінчується, але справжній зломисник продовжить пошук інформації, збере дані та надішле їх до центру управління.

На порталі можна переглядати аспекти автоматизованого розслідування та реагування, пов'язані з імітацією атаки.

Можна побачити всі зломисні процеси, що відбувались під час атаки (рис. 3.44).

ⓘ The MDE SIEM API deprecation date has been set to December 31, 2023. Please see the [announcement](#) to plan your migration to a supported API. ✕

↓ Export 1 Week ▾ Customize columns Filter

Filters: Status: New +1 ✕

☐	Alert name	Tags	Severity	Investigation state	Status	Category	Detection source
☐	A suspicious file w...		■ ■ ■ Medium		● New	Malware	EDR
☐	Suspicious behavi...		■ ■ ■ Medium		● New	Execution	EDR
☐	Suspicious process...		■ ■ ■ Medium		● New	Execution	EDR
☐	Suspicious PowerS...		■ ■ ■ Medium		● New	Execution	EDR
☐	Suspicious behavi...		■ ■ ■ Medium		● New	Initial access	EDR
☐	Suspicious Task Sc...		■ ■ ■ Medium		● New	Persistence	EDR

Рис. 3.44. – Зломисні процеси

Також окремо є можливість перегляду сповіщень та графік розслідування, незавершені або схвалені дії з виправлення.

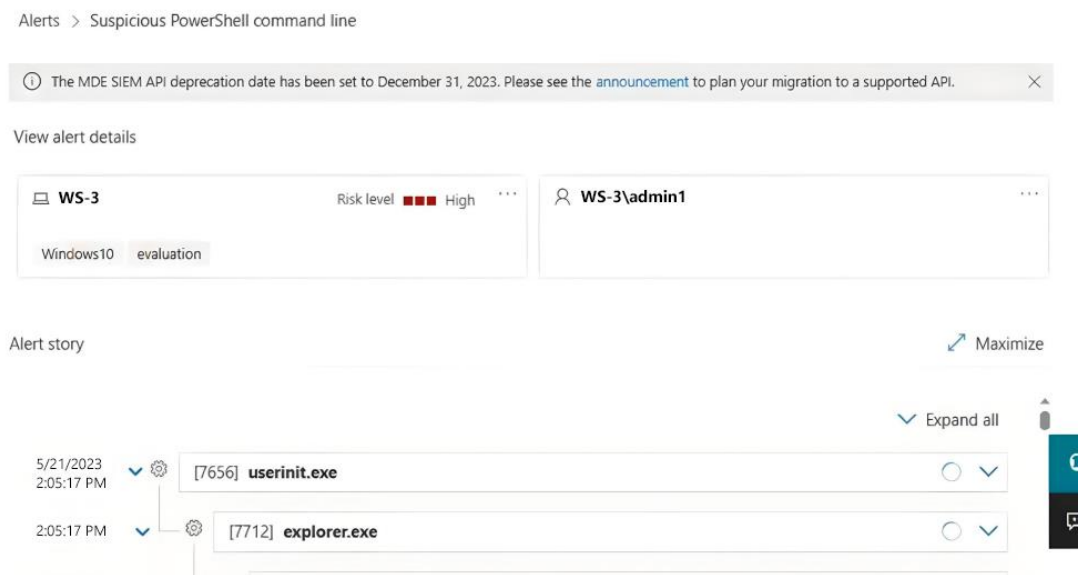


Рис. 3.45 – Деталі процесу

Під час розслідування інциденту в історії дій підозрілої програми можна дослідити кожен крок (рис. 3.46).

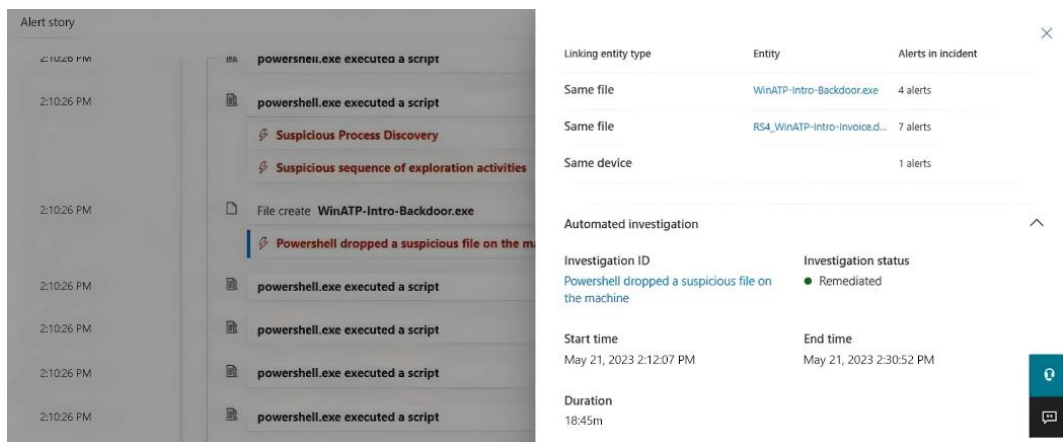


Рис. 3.46 – Деталі однієї дії процесу

Для кожної дії є можливість розгорнути її деталі, щоб мати розуміння на основі чого було зроблено висновок, що програма є шкідником та які кроки для цього виконувались.

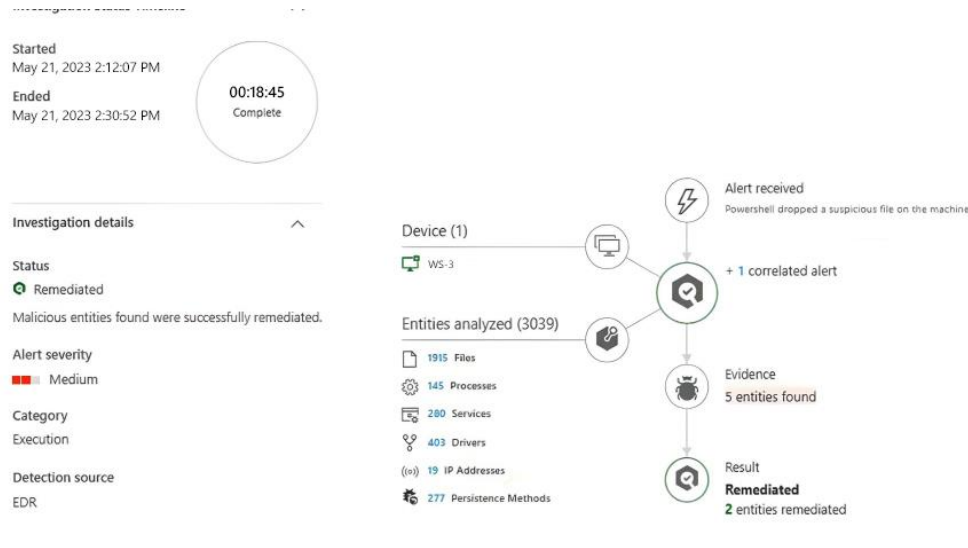


Рис. 3.47. – Діаграма зловмисного процесу

За потреби можна вирішити проблему вручну. Процесом можна керувати обравши його та позначивши як шкідливий об'єкт.

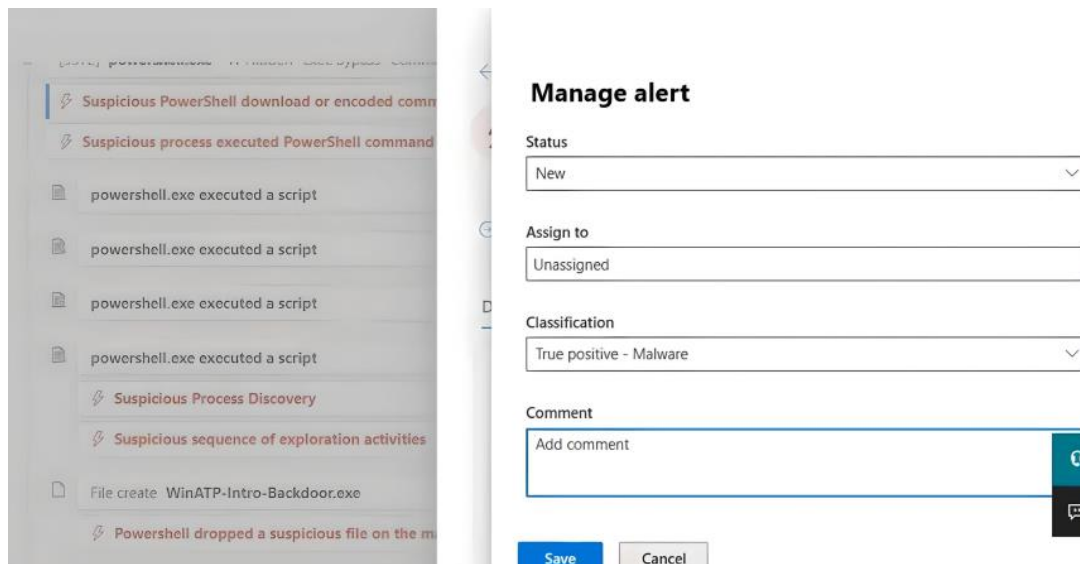


Рис. 3.48. – Керування дією процесу та її класифікація

Автоматизовані розслідування можуть масштабувати можливості запасів, виявляючи загрози атак на різних пристроях і захищаючи їх від небажаних змін.

Висновки до третього розділу

Загалом налаштування Microsoft Defender for Endpoints надають організаціям потужні інструменти для керування безпекою кінцевих точок. Це включає можливість встановлювати режими доступу для користувачів, що дозволяє обмежити права доступу до системи та забезпечити гнучкий контроль над безпекою. Крім того, можна легко додавати нові пристрої до системи та керувати їх безпекою з централізованої консолі.

Microsoft Defender for Endpoints також забезпечує високоефективне виявлення та реагування на загрози. Додатково, Microsoft Defender for Endpoints включає функцію Microsoft Defender Application Guard, яка дозволяє ізолювати небезпечні веб-сайти та файлові завантаження у віртуальних контейнерах, що забезпечує додатковий рівень захисту від потенційних загроз.

Нарешті, правила зменшення поверхні атаки дозволяють налаштовувати політики, які обмежують доступ до функцій та служб на кінцевих точках. Це допомагає зменшити вразливості та обмежити можливості атак для злоумисників.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

ВИСНОВКИ

У кваліфікаційній роботі було розроблено проєкт захищеної підсистеми гібридного захисту від шкідливого програмного забезпечення у Windows-мережі.

Протягом першого розділу розглядались методи захисту кінцевих вузлів. Досліджено технологію Endpoint Detection and Response (EDR). EDR дозволяє забезпечити більш високий рівень безпеки та ефективної реакції на події на кінцевих вузлах. Розглянуто основні конкурентні платформи EDR, проведено їх порівняльний аналіз для реалізації у практичній частині роботи.

В другому розділі сформовано загальний проєкт мережі. Описано будову мережі. Мережа являє собою трирівневу ієрархічну модель. Встановлено базові налаштування мережі для перевірки повної працездатності та обміну інформацією.

В третьому розділі були виконані основні кроки налаштування для забезпечення безпеки кінцевих точок. До них входило встановлення режиму доступу до користувачів, додавання пристроїв до системи, керування загрозами та вразливостями, використання Microsoft Defender Application Guard та правила зменшення поверхні атаки. Ці налаштування спрямовані на покращення безпеки пристроїв та захист від різних загроз, таких як шкідливі програми, вразливості та атаки. Також описано проведення симульованої атаки та успішне тестування автоматизованого розслідування кінцевих точок в Microsoft Defender for Endpoints підтверджують його високу ефективність у виявленні та реагуванні на нові загрози. Це підкреслює важливість платформи в створенні надійного та захищеного середовища для роботи з пристроями в організації.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке Endpoint Detection and Response [Електронний ресурс]. Режим доступу до ресурсу: <https://ua.softlist.com.ua/articles/chto-takoe-endpoint-detection/>
2. CrowdStrike [Електронний ресурс] – Режим доступу до ресурсу: <https://iitd.com.ua/crowdstrike/>
3. Відомості про Microsoft Defender For Endpoint [Електронний ресурс] – Режим доступу до ресурсу: <https://www.microsoft.com/uk-ua/security/business/endpoint-security/microsoft-defender-endpoint>
4. Ключові компоненти безпеки EDR [Електронний ресурс]. Режим доступу до ресурсу: <https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html>
5. Чому організації використовують EDR [Електронний ресурс]. Режим доступу до ресурсу: <https://www.ibm.com/topics/edr>
6. ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ [Електронний ресурс]. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/45723/1/NP_TZI_ITS.pdf
7. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ [Електронний ресурс]. Режим доступу до ресурсу: <https://uzhnu.edu.ua/en/infocentre/get/42935>
8. Про антивірусне ПЗ [Електронний ресурс]. Режим доступу до ресурсу: <https://ua.softlist.com.ua/articles/luchshie-antivirusy-dlya-windows-v-2022-godu/>
9. GPO: блокування програм і запобігання інсталяції програмного забезпечення [Електронний ресурс]. Режим доступу до ресурсу: <https://rdr-it.com/en/gpo-block-programs-and-prevent-software-installation-software-restriction/>
10. Налаштування та підготовка Microsoft Defender for endpoints [Електронний ресурс]. Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mde-p1-setup-configuration?view=o365-worldwide>
11. Deploy an endpoint detection and response (EDR) solution with Microsoft. - Microsoft Corporation, 2021. – 6с.

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

12. What is Microsoft Defender for Endpoint? [Електронний ресурс]. Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide>
13. Dashboard insights [Електронний ресурс]. Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/tvm-dashboard-insights?view=o365-worldwide>
14. Attack surface reduction (ASR) rules reference [Електронний ресурс]. Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide>
15. Документація по Microsoft Defender for Endpoint [Електронний ресурс]. Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/?view=o365-worldwide>
16. Найкращі рішення захисту кінцевих вузлів. [Електронний ресурс]. Режим доступу до ресурсу: <https://www.g2.com/categories/endpoint-detection-response-edr/free>
17. What is Microsoft Defender Vulnerability Management [Електронний ресурс] – Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide>
18. Microsoft Defender Application Guard overview [Електронний ресурс] – Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview>
19. Prepare to install Microsoft Defender Application Guard [Електронний ресурс] – Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/install-md-app-guard>
20. Onboard Windows devices using a local script [Електронний ресурс] – Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints-script?view=o365-worldwide>

21. Onboard Windows devices using Group Policy [Електронний ресурс] – Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints-gp?view=o365-worldwide>

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

ДОДАТКИ

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

Налагодження Dist_SW_1:

```

interface Loopback0
ip address 50.0.1.1 255.255.255.0
spanning-tree vlan 50 priority 24576
spanning-tree vlan 51 priority 28672
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname Dist_SW_1
boot-start-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 50 priority 24576
spanning-tree vlan 51 priority 28672
vlan internal allocation policy ascending
ip tcp synwait-time 5
ip address 50.0.1.1 255.255.255.0
interface Port-channel1
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
channel-group 1 mode active
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
channel-group 1 mode active
interface Ethernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto

interface Ethernet1/1

```

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

```

switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
interface Ethernet1/2
no switchport
ip address 10.0.0.2 255.255.255.252
interface Ethernet1/3
no switchport
ip address 10.0.3.1 255.255.255.252
interface Ethernet2/0
no switchport
ip address 10.0.4.2 255.255.255.252
interface Vlan50
ip address 192.168.50.50 255.255.255.0
standby 1 ip 192.168.50.1
standby 1 priority 110
standby 1 preempt
interface Vlan51
ip address 192.168.51.50 255.255.255.0
standby 2 ip 192.168.51.1
standby 2 preempt
router ospf 1
router-id 2.2.2.2
network 10.0.0.0 0.0.0.3 area 0
network 10.0.3.0 0.0.0.3 area 0
network 10.0.4.0 0.0.0.3 area 0
network 50.0.1.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
network 192.168.51.0 0.0.0.255 area 0

```

Налагодження Dist_SW_2:

```

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname Dist_SW_2
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 50 priority 28672
spanning-tree vlan 51 priority 24576
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Loopback0
ip address 50.0.2.1 255.255.255.0
interface Port-channel1
switchport
switchport trunk encapsulation dot1q
switchport mode trunk

```

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		78

```

interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
channel-group 1 mode active
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
channel-group 1 mode active
interface Ethernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
interface Ethernet1/1
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
interface Ethernet1/2
no switchport
ip address 10.0.1.2 255.255.255.252
interface Ethernet1/3
no switchport
ip address 10.0.5.1 255.255.255.252
interface Ethernet2/0
no switchport
ip address 10.0.6.2 255.255.255.252
interface Ethernet2/1
duplex auto
interface Ethernet2/2
duplex auto
interface Ethernet2/3
duplex auto
interface Ethernet3/0
duplex auto
interface Ethernet3/1
duplex auto
interface Ethernet3/2
duplex auto
interface Ethernet3/3
duplex auto
interface Vlan1
no ip address
shutdown
interface Vlan50
ip address 192.168.50.51 255.255.255.0
standby 1 ip 192.168.50.1
standby 1 preempt
interface Vlan51
ip address 192.168.51.51 255.255.255.0
standby 2 ip 192.168.51.1

```

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

```

standby 2 priority 110
standby 2 preempt
router ospf 1
router-id 3.3.3.3
network 10.0.1.0 0.0.0.3 area 0
network 10.0.5.0 0.0.0.3 area 0
network 10.0.6.0 0.0.0.3 area 0
network 50.0.2.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
network 192.168.51.0 0.0.0.255 area 0
no ip http server
control-plane
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login

```

Налагодження Farm_Dist _SW_1:

```

version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname Farm_Dist_SW1
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ip domain-lookup
ip cef
no ipv6 cef
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 30 priority 24576
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Loopback0
ip address 50.0.3.1 255.255.255.0
interface Port-channel1
switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode active
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode active
interface Ethernet0/2
no switchport

```

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip address 10.0.3.2 255.255.255.252
duplex auto
interface Ethernet0/3
interface Ethernet1/0
no switchport
ip address 10.0.5.2 255.255.255.252
duplex auto
interface Vlan30
ip address 172.20.30.50 255.255.255.0
standby 1 ip 172.20.30.1
standby 1 priority 110
standby 1 preempt
router ospf 1
router-id 4.4.4.4
network 10.0.3.0 0.0.0.3 area 0
network 10.0.5.0 0.0.0.3 area 0
network 50.0.3.0 0.0.0.255 area 0
network 172.20.30.0 0.0.0.255 area 0

```

Налагодження Farm_Dist_SW_2:

```

version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname Farm_Dist_SW2
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain-lookup
ip cef
no ipv6 cef
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 30 priority 28672
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Loopback0
ip address 50.0.4.1 255.255.255.0
interface Port-channel1
switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode active
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode active
interface Ethernet0/2
switchport access vlan 30
switchport mode access
interface Ethernet0/3

```

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no switchport
ip address 10.0.4.1 255.255.255.252
duplex auto
interface Ethernet1/0
no switchport
ip address 10.0.6.1 255.255.255.252
duplex auto
interface Vlan30
ip address 172.20.30.51 255.255.255.0
standby 1 ip 172.20.30.1
standby 1 preempt
router ospf 1
network 10.0.4.0 0.0.0.3 area 0
network 10.0.6.0 0.0.0.3 area 0
network 50.0.4.0 0.0.0.255 area 0
network 172.20.30.0 0.0.0.255 area 0

```

		Анчис А. О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		82