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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

"Рекомендації щодо застосування Endpoint Protection в інформаційній системі організації"

за спеціальністю *125 Кібербезпека*
(код, назва спеціальності)
освітньо-професійна програма *Інформаційна та кібербезпека*
(назва програми)

Кваліфікаційна робота містить результати власного дослідження. Використання ідей, результатів та текстів інших авторів має бути з посиланням на відповідне джерело.

_____ Нікіта Головненко
(підпис)

Виконавець: студент вищої освіти групи БСД-44
Головненко Нікіта
(прізвище, ім'я)
Голова канд. наук з держ. упр., Скибун Олександр
(науковий ступінь, вчене звання, прізвище, ім'я)
Рецензент
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

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

Кафедра Системи та технології кібербезпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібербезпека

ЗАТВЕРДЖЕНО
Керівник відділу ІКБ
_____ Галина ГАЙДУР
«___»_____2025 рік

ЗАВДАННЯ
ДЛЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Головненко Нікіта Романович
(прізвище, ім'я)
1. Тема кваліфікаційної роботи:
Рекомендації щодо застосування Endpoint Protection в інформаційній системі організації
керівник кваліфікаційної роботи Олександр Скибун, канд. наук з держ. упр.
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджено наказом Державного університету інформації та зв'язку технології від "___» _____ 2025 № ____.

2. Кінцевий термін подання кваліфікаційної роботи здобувачем вищої освіти 06.06.2025

3. Вихідні дані для кваліфікаційної роботи
інформаційні ресурси організації;
Рішення EDR;
науково-технічна література, експлуатаційна документація, нормативні акти документи, міжнародні стандарти.

4. Зміст угоди та пояснювальної записки (перелік питань, що потребують розробки)
1. Дослідження проблеми захисту кінцевих точок організації.
2. Аналіз методів та засобів захисту кінцевих точок організації на основі FortiEDR.
3. Розробка рекомендацій щодо методів захисту кінцевих точок організації

5. Перелік графічних матеріалів
Презентація PowerPoint.

6. Дата видачі завдання 28.02.2025

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Сценічний псевдонім кваліфікаційна робота	Кінцевий термін завершення етапів робіт	Примітка
1.	Визначення актуальності проблеми захисту кінцевих точок організації.	03.03.2025	
2.	Аналіз науково-технічної літератури з теми кваліфікаційної роботи.	23.03.2025	
3.	Аналіз методів та засобів захисту кінцевих точок організації на основі EDR.	12.04.2025	
4.	Практична реалізація опції захисту кінцевих точок на основі FortiEDR для організації.	01.05.2025	
5.	Розробка рекомендацій щодо застосування методів та інструментів захисту кінцевих точок організації.	15.05.2025	
6.	Презентація результатів дослідження.	16.05.2025	
7.	Підготовка доповіді до захисту.	06.06.2025	

Студент вищої освіти _____ Нікіта Головненко
(підпис) *(ім'я, прізвище)*

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

ВІДГУК РЕЦЕНЗЕНТА

за кваліфікаційну роботу

заявник *Нікіта Головненко*

на тему: «Рекомендації щодо застосування Endpoint Protection в інформаційній системі організації»

Актуальність: Захист кінцевих точок організації, таких як сервери, ПК, ноутбуки та мобільні пристрої, є важливим для запобігання несанкціонованому доступу, витоку даних та втраті даних. Системи EDR забезпечують постійний моніторинг кінцевих точок, дозволяючи організаціям контролювати свій рівень безпеки та проактивно реагувати на нові загрози.

Кібератаки, які порушують роботу кінцевих точок організації або компрометують їх, можуть призвести до простоїв, впливаючи на продуктивність та безперервність бізнесу. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні аспекти:

1. На основі проведеного аналізу в роботі встановлено зміст проблеми захисту кінцевих точок організації та визначено мету та завдання цього виду безпеки, а також його складові .

2. Було досліджено методи та засоби захисту кінцевих точок організації на основі EDR.

3. Запропоновано варіант системи захисту кінцевих точок організації на основі FortiEDR та рекомендації щодо її застосування.

4. Текст викладено досить грамотно та послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал якісно оформлений. Список науково-технічної літератури свідчить про можливість використання матеріалів за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести аналіз змісту захисту кінцевих точок на прикладі конкретної організації.

2. У кваліфікаційній роботі було б бажано проілюструвати запропоновану процедуру застосування методів та інструментів захисту кінцевих точок на прикладі конкретної організації .

Зазначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: З урахуванням недоліків, кваліфікаційна робота заслуговує на оцінку **«добре»**, а заявнику **ГОЛОВНЕНКО Нікіті** присвоюється кваліфікація бакалавра з кібербезпеки за освітньою програмою «Інформаційна та кібербезпека».

Рецензент:

_____	_____	_____
(науковий ступінь, академічне звання)	*(підпис)*	*(ім'я, прізвище)*

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

ПРЕЗЕНТАЦІЯ
ГОЛОВИ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ПРО ЗАХИСТ КВАЛІФІКОВАНОЇ ПРАЦІ

для отримання ступеня бакалавра

Заявника надсилають Головненко Нікіта на захист кваліфікаційної роботи
(прізвище, ім'я)

Спеціальності 125 Кібербезпека
освітньо-професійна програма Інформаційна та кібербезпека
(код та назва спеціальності)

на тему: "Рекомендації щодо застосування Endpoint Protection в інформаційній системі організації"

Кваліфікаційна робота та огляд додаються.

Директор Інституту _____ Євгенія ІВАНЧЕНКО
(підпис) (ім'я, прізвище)

Висновок керівника
кваліфікаційної роботи

Заявник ***ГОЛОВНЕНКО Нікіта*** обрав тему роботи, метою якої було дослідження методів та засобів захист кінцевих точок організації та розробка рекомендацій щодо її впровадження. Перелік використаних джерел свідчить про здатність здобувача розуміти наукові питання та застосовувати їх у дослідженнях. Під час кваліфікаційної роботи ***ГОЛОВНЕНКО Нікіта*** продемонстрував добру теоретичну та практичну підготовку, здатність самостійно вирішувати проблеми та робити висновки. Роботу виконував сумлінно, точно та вчасно згідно з планом.

оцінити виконану кваліфікаційну роботу заявника ***НІКІТИ Головненка*** на **«добре»** та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Інформація та кібербезпека.

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

Висновок кафедри щодо

кваліфікаційної роботи

Розглядається кваліфікаційна робота. Кандидат ***ГОЛОВНЕНКО Нікіта*** дозволено захищатися
цієї кваліфікаційної роботи в екзаменаційній комісії.

Завідувач кафедри систем і технологій кібербезпеки
(ім'я)

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 62 сторінки, 13 рисунків, 5 таблиць, 33 джерела.

Мета роботи: розробка рекомендацій щодо застосування Endpoint Protection в інформаційній системі організації. Досягнення поставленої мети передбачає оцінку актуальності проблеми, аналіз існуючих підходів, порівняння популярних рішень для захисту кінцевих точок та обґрунтування вибору конкретного рішення для практичної реалізації.

Об'єкт дослідження: захист кінцевих точок організації. У роботі розглядаються основні загрози, що виникають при недостатньому захисті кінцевих пристроїв, таких як робочі станції, ноутбуки, сервери тощо. Особлива увага приділена сучасним типам атак, зокрема програмам-вимагачам, фішингу, використанню експлойтів нульового дня та шкідливому програмному забезпеченню.

Предмет дослідження: рекомендації щодо застосування Endpoint Protection в інформаційній системі організації. Робота спрямована на дослідження можливостей сучасних рішень класу EDR (Endpoint Detection and Response) з метою покращення загального рівня кіберзахисту організаційної інфраструктури.

Методи дослідження: опрацювання методом системного аналізу, огляд літератури з даної теми, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння. Здійснено критичний аналіз науково-технічних публікацій, нормативно-правових джерел, а також практичного досвіду впровадження систем EDR в різних організаціях.

Короткий зміст роботи: У кваліфікаційній роботі послідовно розв’язано низку завдань, що дозволили досягти поставленої мети – розробити рекомендації щодо застосування захисту кінцевих точок в інформаційній системі організації. Досліджено актуальність проблеми захисту кінцевих точок. Встановлено, що кінцеві пристрої є одним із головних векторів атак, а їх уразливість суттєво впливає

на безпеку інформаційних систем організації. Проведено аналіз науково-технічної літератури, експлуатаційної документації та міжнародних стандартів, що дозволило окреслити основні вимоги до систем захисту кінцевих точок та відокремити сучасні підходи до забезпечення безпеки. Визначено та проаналізовано існуючі методи і засоби захисту кінцевих точок на основі рішень класу EDR. Показано, що традиційні інструменти (антивірус, брандмауер) є недостатніми без активного моніторингу та реагування на загрози. Окреслено особливості архітектури, функцій і принципів роботи FortiEDR — платформи виявлення та реагування на інциденти. Встановлено, що FortiEDR забезпечує гнучку політику захисту, виявлення в реальному часі та автоматизовану відповідь на загрози. Реалізовано варіант захисту кінцевих точок організації на основі FortiEDR. Обґрунтовано доцільність його впровадження на прикладі типової організаційної структури. Надано опис архітектури, сценаріїв реагування, налаштування політик. Розроблено та запропоновано практичні рекомендації щодо впровадження засобів захисту кінцевих точок у інформаційній системі організації. Визначено, що ці рекомендації є доцільними до впровадження в умовах обмежених ресурсів та підвищеного рівня кіберризиків.

Системи виявлення та реагування на кінцеві точки (EDR) відіграють вирішальну роль у підвищенні безпеки кінцевих точок організації. Системи EDR призначені для постійного моніторингу дій та поведінки кінцевих точок, збирання телеметрії, виявлення аномалій та інцидентів. Вони забезпечують видимість активності кінцевих точок у режимі реального часу, дозволяючи організаціям швидко реагувати на загрози та ізолювати скомпрометовані пристрої.

У роботі досліджується проблема захисту кінцевих точок організацій, визначаються її мета та завдання. Аналізуються існуючі методи та інструменти захисту кінцевих точок організацій. Досліджуються методи та інструменти захисту кінцевих точок організацій на основі EDR. Визначається мета, основні функції та склад рішення EDR. Порівнюються можливості таких платформ, як Microsoft Defender for Endpoint, CrowdStrike, SentinelOne, FortiEDR.

На основі проведеного в роботі дослідження було запропоновано варіант

системи на базі FortiEDR. Розроблено практичні рекомендації для фахівц кібербезпеки щодо впровадження методів та засобів захисту кінцевих точок організації в умовах реального інформаційного середовища.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ІНФОРМАЦІЙНІ РЕСУРСИ, ОРГАНІЗАЦІЇ, КІНЦЕВІ ТОЧКИ, ЗАХИСТ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ, КІБЕРБЕЗПЕКА.

ЗМІСТ

ПЕРЕДЛІК УМОНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

APT – Advanced Persistent Threat

AV - Antivirus

BYOD – Bring-Yours Own-Device

DMZs – Demilitarized Zones

DNS – Domain Name System

EDR – Endpoint Detection and Response

EPP – Endpoint Protection Platform

ETDR – Endpoint Theat Detection and Response

IaaS – Infrastructure as a Service

NGFW – Next-Generation Firewall

PaaS – Platform as a Service

SIEM – Security Information and Event Monitoring

SSO – Single Sign-On

SSE – Cloud-Delivered Security Service Edge

VPN – Virtual Private Network

ZT – Zero Trust

ZTA – Zero Trust Architecture

ZTNA – Zero Trust Network Access

Endpoint Protection – захист кінцевих точок

ВСТУП

Актуальність дослідження. Захист кінцевих точок організації є критично важливим з кількох причин. По-перше, кінцеві точки, такі як комп'ютери, ноутбуки та мобільні пристрої, є носіями конфіденційних даних та мають до них доступ. Захист цих пристроїв є важливим для запобігання несанкціонованому доступу, витоку даних та втраті даних. По-друге, кінцеві точки часто є точками входу для кібератак. Скомпрометовані кінцеві точки можуть бути використані для атаки на всю корпоративну мережу. По-третє, кінцеві точки є засобами для повсякденних бізнес-операцій. Атака, яка порушує роботу або компрометує кінцеві точки, може призвести до простою, що впливає на продуктивність та безперервність бізнесу. Захист кінцевих точок є критично важливим для підтримки безпечного середовища віддаленої роботи.

Системи виявлення та реагування на кінцеві точки (EDR) відіграють вирішальну роль у покращенні безпеки кінцевих точок організації. Системи EDR призначені для постійного моніторингу дій та поведінки кінцевих точок. Вони можуть виявляти незвичайні закономірності або аномалії, які можуть свідчити про загрозу безпеці. Системи EDR також забезпечують видимість активності кінцевих точок у режимі реального часу, дозволяючи організаціям швидко реагувати на інциденти безпеки. Це включає ізоляцію скомпрометованих кінцевих точок, розслідування інцидентів та впровадження заходів щодо усунення наслідків.

Системи EDR аналізують поведінку процесів і програм на кінцевих точках. Відхилення від нормальних моделей поведінки можна позначити як потенційні загрози безпеці. У разі інциденту безпеки системи EDR сприяють аналізу, надаючи детальну інформацію про дії, що призвели до інциденту. Якщо на кінцевій точці виявлено загрозу, системи EDR можуть ізолювати уражену кінцеву точку від мережі, щоб запобігти поширенню шкідливого програмного забезпечення та обмежити потенційну шкоду.

Рішення EDR дозволяють організаціям застосовувати політики безпеки на кінцевих точках, гарантуючи відповідність пристроїв стандартам безпеки та

конфігураціям. Поєднуючи заходи безпеки кінцевих точок із системами EDR, організації можуть створити надійний захист від широкого спектру кіберзагроз та покращити загальну безпеку.

Вищезазначене визначає актуальність теми даної кваліфікаційної роботи, основним змістом якої є рекомендації щодо використання захисту кінцевих точок в інформаційній системі організації.

Об'єктом дослідження є захист кінцевих точок організації.

Предметом дослідження є рекомендації щодо використання захисту кінцевих точок в інформаційній системі організації.

Метою роботи є розробка версії системи на основі рішення EDR та рекомендацій щодо застосування методів і інструментів захисту кінцевих точок організації.

Наукові завдання:

дослідити суть проблеми захисту кінцевих точок організації;

проаналізувати основні підходи до захисту кінцевих точок організації;

проаналізувати існуючі рішення для захисту кінцевих точок організації;

проаналізувати методи та засоби захисту кінцевих точок організації на основі EDR;

запропонувати варіант системи захисту кінцевих точок організації на основі FortiEDR;

розробити рекомендації щодо застосування методів та інструментів для захисту кінцевих точок організації.

Методи дослідження – опрацювання методом системного аналізу, огляд літератури з даної теми, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння. Здійснено критичний аналіз науково-технічних публікацій, нормативно-правових джерел, а також практичного досвіду впровадження систем EDR в різних організаціях.

Практичне значення отриманих результатів: розроблено рекомендації щодо застосування методів та засобів захисту кінцевих точок організації, а також

рекомендації для фахівців з кібербезпеки щодо їх впровадження

1. ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

1.1. Аналіз проблеми захисту кінцевих точок організації

Кібербезпека - це сукупність заходів, процесів і технологій, що забезпечують захист комп'ютерних систем, мереж, програм і даних від кіберзагроз, які можуть порушити конфіденційність, цілісність або доступність інформації. Її основу становить реалізація CIA-тріади: Confidentiality, Integrity, Availability [19].

У контексті захисту кінцевих точок ці принципи мають особливе значення, оскільки саме кінцеві пристрої (робочі станції, ноутбуки, мобільні телефони, сервери) найчастіше виступають каналом атак, джерелом витоку даних або стартовою точкою внутрішніх загроз.

Згідно зі звітом Cybersecurity Insiders Report [1], зіткнувшись із викликами захисту від нових та дедалі складніших викликів організації повідомляють про зростання ризиків безпеки кінцевих точок, водночас відчуваючи неготовність до протидії новим загрозам за допомогою існуючих платформ безпеки кінцевих точок.

Фахівці з кібербезпеки вважають шкідливе програмне забезпечення (включаючи програми-вимагачі, трояни, експлойти тощо) найбільшою кіберзагрозою для своїх організацій (38%), далі йдуть людські помилки (23%) та експлойти нульового дня (18%). Це узгоджується з відповідними дослідженнями, які підкреслюють зростаючу загрозу від шкідливого програмного забезпечення, особливо програм-вимагачів (рис. 1.1) [1].

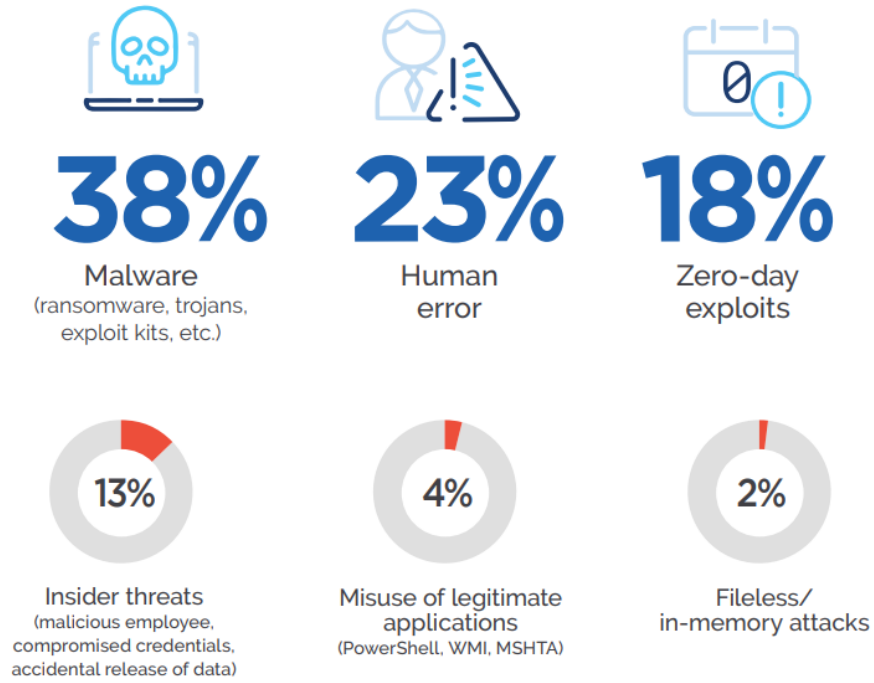

Рис. 1.1. Найбільші кіберзагрози для організацій [1]

Для ефективного виявлення, стримування, аналізу та усунення наслідків кібератак, рішення EDR повинно включати різні інструменти [2]:

агенти збору даних кінцевих точок , які відстежують та збирають дані про передачу файлів, процеси, активність та підключення до центрального сховища для аналізу;

автоматичні відповіді інтегровані в мережеві системи діють на основі попередньо налаштованих правил, наприклад, для виведення користувача з системи та повідомлення служби безпеки про відомий тип порушення;

аналіз та криміналістика з аналітикою в режимі реального часу для сортування потенційно шкідливих подій та інструментами криміналістики для виявлення загроз і аналізу після атаки.

Згідно з Gartner, ефективне рішення EDR також повинно мати такі розширені функції [2] як:

поєднання сучасних методів запобігання з можливостями виявлення та реагування;

єдиний легкий шлях;

хмарна інфраструктура;

об'єднання багатьох інструментів в одній консолі з додатковими можливостями інтеграції.

В результаті реалізації загроз в інформаційній системі може бути порушена конфіденційність (витік, перехоплення, видалення, копіювання, крадіжка, розголошення), цілісність (втрата, знищення, модифікація) та доступність (блокування) інформації. У цьому випадку порушення цілісності та (або) доступності інформації може призвести до порушення достовірності та своєчасності результатів функціонування інформаційної системи, аж до системного збою. Класифікацію загроз можна здійснити за великою кількістю характеристик. Найпоширеніші з них наведено в таблиці 1.1. [18]

Таблиця 1.1. Класифікація загроз [18]

Критерії загрози	Типи загроз
За типом власності інформації, що порушується	Загрози конфіденційності (витік, перехоплення, видалення, крадіжка, розголошення); Загрози цілісності
За характером порушення	Порушення конфіденційності даних; порушення працездатності серверів, мережевого обладнання, робочих станцій, незаконне втручання у функціонування серверів, мережевого обладнання, робочих станцій тощо;
За тяжкістю порушення	Незначні помилки; дрібне хуліганство; серйозні злочини, стихійні лиха та техногенні катастрофи;
Передбачаючи наслідки для правопорушника	Навмисне порушення; Ненавмисне порушення;
За мотивацією	Зловмисне порушення; Незловмисне порушення;
За повнотою	Закінчений; незакінчений;

За об'єктом дії	Загрози, спрямовані на всю інформаційну систему; загрози, спрямовані на окремі компоненти;
За причиною виникнення	Загрози, що виникають через відсутність технічного захисту; Загрози, що виникли через відсутність організаційних заходів;

Кінцеві пристрої (ноутбуки, мобільні телефони, сервери, пристрої Інтернету речей, тощо) представляють собою широку та постійно мінливу поверхню для атак. Компрометація кінцевих точок є основною причиною порушень: наприклад, галузеві звіти показують, що приблизно 70% усіх порушень безпеки відбувається на кінцевих точках, при цьому, 68% підприємств зазнали принаймні однієї атаки на кінцеві точки, яка вплинула на інфраструктуру або дані. Наведені вище дані підкреслюють, наскільки популярні кінцеві точки серед хакерів/кіберзлочинців. Поширені вектори атак зображені на супровідному графіку з опитування Інституту Ponemon [24], а саме: фішинг/соціальна інженерія (48%) та крадіжка облікових даних (56%), далі йдуть захоплення облікового запису, загальне шкідливе програмне забезпечення, відмова в обслуговуванні та інші тактики. Комплексний захист кінцевих точок організації є важливим, оскільки насправді атаки можуть скористатися будь-якою вразливістю, від зловмисних інсайдерів або невиправленого програмного забезпечення до вразливостей нульового дня та викрадених облікових даних.

Проблема посилюється низкою фундаментальних причин. Кінцеві точки в сучасному бізнесі стають дедалі різноманітнішими та численнішими. Наприклад, згідно з нещодавнім прогнозом, до 2025 року у світі буде близько 27 мільярдів підключених пристроїв «IoT» (iot-analytics.com), а корпоративні парки пристроїв часто працюють на численних операційних системах, включаючи Windows, macOS, Linux, Android, iOS та інші.

Безпека ускладнюється віддаленою роботою та впровадженням концепції «Принеси свій власний пристрій» (BYOD), що дозволяє співробітникам

використовувати некеровані та/або особисті пристрої, що не повністю контролюються організацією. Згідно з одним аналізом[16], компанії часто поєднують ПК, сервери, мобільні пристрої та кінцеві точки IoT, з обладнанням, керованим постачальниками, та BYOD, що призводить до серйозних прогалин у видимості та управлінні виправленнями.

Згідно з опитуваннями [24], багато фірм не мають повного контролю кінцевих точок. Наприклад, близько 51% підприємств не можуть бачити всі свої пристрої одночасно, а приблизно 63% підприємств не можуть контролювати кінцеві точки, які виходять за межі мережі. Зловмисники можуть використовувати вразливі кінцеві точки без перевірки, якщо вони не знають, чи є пристрої встановлені або чи вони виправлені.

Той факт, що на багатьох кінцевих точках присутні конфіденційні дані, посилює цю проблему видимості. Згідно з опитуванням [24], понад половина всіх вразливих кінцевих точок містили конфіденційні дані з absolute.com, що свідчить про те, що успішне порушення може призвести до прямого розголошення особистої інформації або інтелектуальної власності. Крім того, основні заходи безпеки кінцевих точок регулярно дають збій: наприклад, 42% кінцевих точок мають проблеми з антивірусом або шифруванням у будь-який момент часу, що робить дані вразливими.

Зловмисники (хакери/кіберзлочинці) мають можливість переміщатися по мережі оргнізації після порушення безпеки пристрою. Зламана кінцева точка «може служити точкою входу для кібератак, що потенційно може призвести до значних витоків даних (чутливої інформації, персональних даних, інформації для виробничих процесів тощо) та фінансових втрат», повідомляє Palo Alto Networks (paloaltonetworks.com).

Організаціям також доводиться мати справу з операційними та людськими проблемами. Згідно з опитуванням Absolute, типовий бізнес встановлює приблизно десять різних агентів безпеки на кожній кінцевій точці [25]. Хоча наявність кількох технологій безпеки може здаватися кращою, насправді таке «розповсюдження безпеки» призводить до суперечок, погіршення продуктивності та прогалин в

управлінні. За даними helpnetsecurity.com, «навіть найефективніші агенти кінцевих точок мають високу ймовірність збою» [25], оскільки агенти можуть конкурувати за системні ресурси або навіть виводити з ладу один одного.

Таблиця 1.1.2 – Основні типи загроз кінцевим точкам [26]

Тип загрози	**Опис**	**Приклад**
Шкідливе програмне забезпечення	Шкідливе програмне забезпечення, яке порушує роботу систем або пошкоджує їх	Трояни, віруси, черв'яки
Програми-вимагачі	Шифрує файли та вимагає викуп за розшифрування	WannaCry , REvil
Фішинг	Оманливі спроби отримати конфіденційні дані	Фальшиві електронні листи, підроблені вебсайти
Експлойт нульового дня	Атака, що використовує нерозкриті вразливості	EternalBlue (патч для попередніх версій Windows)

[Джерело: NIST SP 800-61r2] [26]

Сучасні організації дедалі більше покладаються на розподілені та мобільні обчислювальні середовища, в яких кінцеві точки, такі як робочі станції, ноутбуки, мобільні пристрої, віртуальні машини та пристрої Інтернету речей, безпосередньо підключені до важливих систем та конфіденційних даних. Хоча ця цифрова гнучкість є важливою для продуктивності, вона зробила кінцеві точки основним об'єктом кібератак.

Згідно з індексом розвідки загроз X-Force Threat Intelligence Index від IBM за 2023 рік, понад 80% початкових векторів доступу у зареєстрованих порушеннях походили з кінцевих точок [1]. Зловмисники використовують більшість кінцевих

точок як легкодоступні можливості через їхню доступність та різноманітні поверхні атаки. Від неоновленого програмного забезпечення та незахищених протоколів віддаленого робочого столу (RDP) до фішингу та соціальної інженерії, кінцеві точки є вразливими як на технічному, так і на людському рівнях.

Крім того, перехід до віддалених та гібридних моделей роботи вилучив багато кінцевих точок з-за традиційних периметральних захистів. Співробітники тепер отримують доступ до конфіденційних корпоративних систем з незахищених особистих пристроїв або загальнодоступних мереж, що експоненціально збільшує частоту поверхневих атак. Цей перехід вимагає переходу від моделей безпеки на основі периметра до стратегій, орієнтованих на кінцеві точки.

Значна проблема виникає через різноманітність середовищ кінцевих точок. Організації контролюють пристрої, що працюють на кількох системах (Windows, Linux, macOS), мають різні апаратні конфігурації та використовують широкий спектр архітектур додатків. Така різноманітність призводить до збільшення вразливостей у виявленні загроз і ускладнює ефективне забезпечення дотримання єдиних політик безпеки.

Фінансові наслідки атак на кінцеві точки є значними. Кампанії програм-вимагачів, спрямовані на кінцеві точки, коштували організаціям в середньому 4,54 мільйона доларів за інцидент у 2023 році [2]. Зловмисники використовують ці системи для встановлення стійкості, підвищення привілеїв, латерального переміщення та, зрештою, викрадання даних або виконання руйнівних корисних навантажень.

Окрім фінансових втрат, репутаційна шкода/втрата та регуляторні наслідки (наприклад, невідповідність GDPR, HIPAA, ISO 27001), які тягнуть за собою штрафи, підкреслюють важливість захисту кінцевих точок організації як основного компонента управління ризиками підприємства.

Щоб протидіяти цьому, організаціям потрібно більше рішень, які забезпечують постійну видимість, виявлення загроз у режимі реального часу та автоматизоване реагування на рівні кінцевих точок. Саме тут сучасні технології виявлення та реагування на кінцевих точках (EDR) стали важливими

інструментами для протидії.

1.2 Аналіз підходів до захисту кінцевих точок організації

Щоб вирішити ці проблеми, архітектури безпеки повинні використовувати численні багаторівневі засоби захисту (захист у глибину) в усьому середовищі кінцевих точок. Згідно з одною із рекомендацій щодо безпеки, захист у глибину «використовує комбінацію передових інструментів безпеки для захисту кінцевих точок, даних, програм та мереж організації», щоб «існували елементи для зупинки загроз, якщо одна лінія захисту скомпрометована» [27]. Фактично це передбачає поєднання передових інструментів виявлення та реагування зі звичайними обмеженнями кінцевих точок (брандмауери, шифрування та антивірусне програмне забезпечення).

Мінімальна безпека кінцевих точок все ще має своє місце. Щоб знайти відоме шкідливе програмне забезпечення, антивірусні програми використовують поведінкове, евристичне та сигнатурне виявлення. Вони поміщають загрози в карантин, щоб запобігти їхньому виконанню, одночасно виконуючи сканування файлів і процесів у режимі реального часу. Шифрування диска захищає дані, що зберігаються, у разі втрати або крадіжки пристрою, а брандмауери та безпечні шлюзи регулюють мережевий доступ до пристроїв і з них. Однак корпорації додають додаткові технології до антивірусних засобів, оскільки загрози вийшли за межі розпізнаваних сигнатур.

EDR – це значний прогрес. Активність кінцевих точок (запуски процесів, мережеві підключення, а також зміни реєстру та файлів) постійно відстежується та документується платформами EDR. Інструменти EDR можуть виявляти шкідливі або неочікувані дії (такі як горизонтальне переміщення або дивна активність процесів), які антивірусне програмне забезпечення на основі сигнатур пропустило б, збираючи цю обширну інформацію. Наприклад, Palo Alto Networks зазначає, що EDR може миттєво ізолювати та виправляти проблеми, виявляючи підозрілі зміни файлів або неочікувані спроби доступу [31]. Аналітика на основі штучного інтелекту та машинного навчання зазвичай інтегрована в сучасні системи EDR;

вони отримують дані інформації про загрози для виявлення нових атак та порівнюють поведінку кінцевих точок у реальному часі з навченими базовими показниками для виявлення відхилень.

Таким чином, EDR переходить від чистого запобігання до проактивної моделі виявлення/реагування. Він може автоматично поміщати заражені хости в карантин або скасовувати шкідливі зміни, що значно скорочує час перебування в карантині. Як пояснюється в одному галузевому блозі, EDR «забезпечує більш комплексний та динамічний підхід до захисту кінцевих точок від складного шкідливого програмного забезпечення, програм-вимагачів та цілеспрямованих атак» [17].

Архітектура нульової довіри – це модель безпеки, яка працює за принципом, що жодна особа чи пристрій не повинні автоматично вважатися надійними, навіть якщо вони знаходяться в межах периметра мережі. На відміну від традиційної моделі «замку та рову», яка працює виходячи з припущення про порушення безпеки та ніколи не пропонує невід'ємної довіри, засоби вибору доступу постійно оцінюють ідентичність користувача, стан пристрою та контекст для кожного запиту ресурсів. На практиці це передбачає використання надійних методів автентифікації (таких як багатофакторна автентифікація), обмеження горизонтального переміщення шляхом мікросегментації мереж та впровадження політики доступу з найменшими привілеями.

Провідні фахівці (наприклад на основі NIST SP800-207), визначають Zero Trust як комплексну стратегію, спрямовану на захист ресурсів та інформації підприємства, що включає ретельний процес перевірки кожного запиту на доступ. Стратегії, засновані на Zero Trust, часто підкреслюють критичну роль безпеки кінцевих точок; наприклад, перш ніж дозволити будь-якому пристрою підключитися до мережі, системи можуть вимагати, щоб пристрої були повністю оновлені останніми патчами та мали робочі агенти безпеки. Впровадження практики Zero Trust швидко зростає – опитування показало, що 61% організацій запровадили офіційну стратегію Zero Trust до 2023 року, порівняно з лише 24% у 2021 році – що підкреслює переконання, що постійна перевірка пристроїв зараз

вважається критично важливою.

Альтернативні методи включають сегментацію мережі та мікросегментацію, яка розділяє кінцеві точки на окремі зони безпеки, щоб обмежити вплив порушень. Аналітика поведінки користувачів та сутностей (UEBA) може розуміти типові закономірності користувачів/пристроїв та видавати сповіщення про відхилення. Хмарний захист кінцевих точок (SaaS-надання оновлень та аналітики) гарантує, що пристрої отримуватимуть своєчасну інформацію, навіть якщо вони не підключені до мережі. Платформи єдиного керування кінцевими точками (UEM) та керування мобільними пристроями (MDM), такі як Microsoft Intune та JAMF, забезпечують дотримання конфігурацій пристроїв, гарантують дотримання політик та пропонують функції для віддаленого видалення даних як з корпоративних, так і з особистих пристроїв. Регулярні оновлення патчів, оцінки вразливостей та перевірки відповідності допомагають зменшити відомі ризики безпеки.

З огляду на вищезазначене можна визначити що, сучасний захист кінцевих точок включає різні рівні: превентивні заходи (такі як антивірусні рішення, пісочниця та нагляд за пристроями), механізми виявлення (такі як EDR/XDR та поведінковий аналіз) та стратегії політик (включаючи обмеження доступу, сегментацію мережі та навчання користувачів) – усі вони сприяють комплексному підходу до безпеки.

Таблиця 1.2 Порівняльний аналіз провідних рішень для захисту кінцевих точок

Рішення	Тип	Основні можливості	Сильні сторони	Обмеження
Захисник Microsoft для кінцевих точок	EP/EDR	Вбудований захист Windows, аналітика загроз, автоматичне реагування	Рідна інтеграція, без додаткових витрат	Базові функції без преміум-ліцензії

Продовження таблиці 1.2

CrowdStrike Falcon	Хмарний EDR	Виявлення загроз на основі штучного інтелекту, розвідка загроз, легкий агент	Надійне виявлення, проактивне пошук загроз	Потрібне підключення до хмари
Singularity SentinelOne	EDR/XDR	Автономне виявлення та виправлення, функції відкату	Захист офлайн, автоматизація	Інтерфейс користувача менш інтуїтивно зрозумілий для деяких адміністраторів
FortiEDR	EDR	Захист до/після зараження, методи реагування, низький рівень хибнопозитивних результатів	Захист у режимі реального часу, безшовна інтеграція з Fortinet	Крива навчання, складне початкове налаштування
Symantec Endpoint Security	EP/EDR	Машинне навчання, моніторинг поведінки, DLP	Широка підтримка ОС, надійний контроль політик	Системно перевантажені, фрагментовані лінійки продуктів

1.3 Аналіз існуючих рішень для захисту кінцевих точок організації

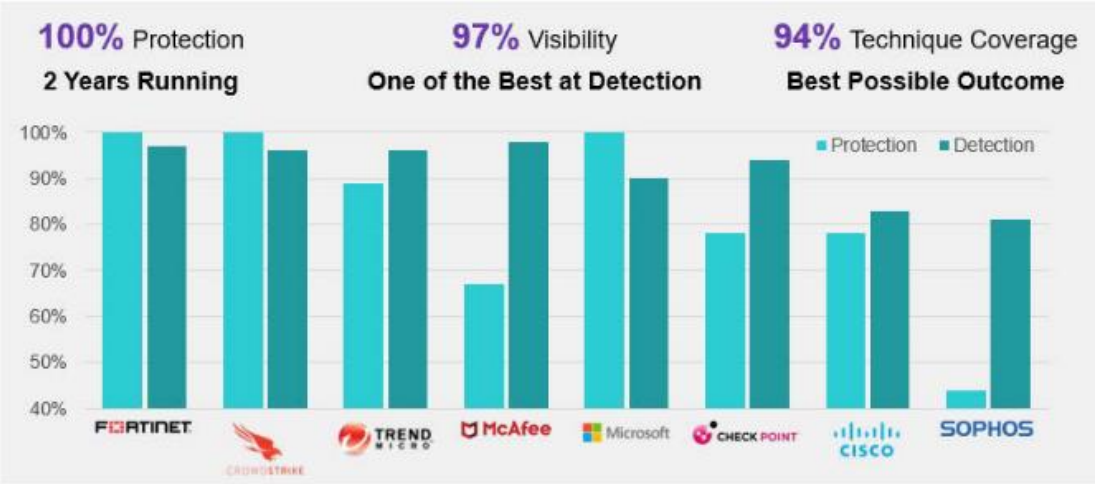

Рисунок 1.3: Стовпчаста діаграма, що порівнює таких постачальників, як Fortinet, Symantec, CrowdStrike, McAfee. [12]

Кілька комерційних продуктів ілюструють ці стратегії. Наприклад, Fortinet FortiEDR – це рішення EDR/EPP, яке пропонує автоматизований захист та реагування в режимі реального часу для кінцевих точок. Воно сумісне з пристроями Windows, Linux, macOS, Android та IoT , а також інтегрується з Fortinet Security Fabric для скоординованої захисної стратегії. FortiEDR забезпечує захист як до, так і після заражень, використовуючи машинне навчання та віртуальне виправлення для запобігання експлойтам, а також функції автоматизованого реагування для завершення або ізоляції шкідливих процесів.

CrowdStrike Falcon – ще одна відома платформа. Хмарна система EDR (Falcon Insight) від CrowdStrike забезпечує безперервну телеметрію та використовує штучний інтелект для аналізу загроз у своїй глобальній базі даних. Її агент у режимі ядра фіксує численні типи подій для судово-медичного аналізу, тоді як хмара безпеки «відображає торговельні технології у запатентованому графі загроз» для автоматичної протидії атакам у всьому світі. На практиці Falcon дозволяє командам безпеки ізолювати скомпрометовані системи та дистанційно виконувати дії реагування. CrowdStrike стверджує, що її користувачі отримують аналітику в режимі реального часу: наприклад, її метрика CrowdScore відображає загальний ризик атаки в режимі реального часу, допомагаючи організаціям визначити, чи

стикаються вони з активною загрозою [32].

Microsoft Defender for Endpoint – це всеохоплююча платформа, інтегрована в Windows і доступна також для інших операційних систем. Вона поєднує передові антивірусні технології з можливостями виявлення та реагування на кінцеві точки (EDR), керування вразливостями та розширеними можливостями виявлення та реагування (XDR) в одному хмарному пакеті. Defender for Endpoint забезпечує прозорість та покращений захист за допомогою штучного інтелекту на різних платформах, включаючи Windows, macOS, Linux, Android, iOS та деякі пристрої Інтернету речей . Як повідомляє Microsoft, щодня він аналізує понад 78 трильйонів сигналів загроз від своєї глобальної клієнтської бази. Основні функції включають рекомендації щодо зменшення поверхонь атаки, які виявляють загрози за допомогою поведінкового аналізу, функції автоматизованого розслідування та реагування, а також централізовану панель сповіщень [13]. У 2024 році Gartner визнав Microsoft лідером у захисті кінцевих точок, підкресливши широке покриття Defender та його безперешкодну інтеграцію в екосистему Microsoft 365 Defender [5].

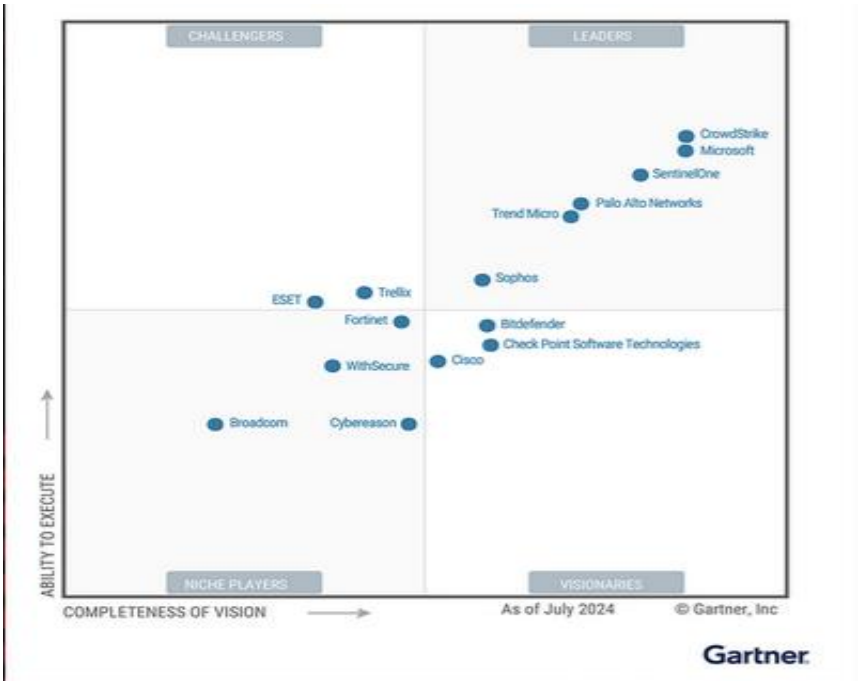

Рисунок 1.3: Магічний квадрант Gartner, що показує провідних постачальників засобів безпеки кінцевих точок у 2024 році [5]

Серед інших значних рішень – VMware Carbon Black, який зосереджений на виявленні загроз кінцевим точкам за допомогою методів поведінкової профілактики, та Palo Alto Cortex XDR, який інтегрує можливості EDR та XDR з аналітикою, отриманою з даних програм та мережі. Крім того, Sophos Intercept X добре відомий своїми антивірусними програмами нового покоління та можливостями глибокого навчання, спрямованими на ефективну протидію зловмисним тактикам, тоді як Trend Micro Apex One та Symantec (Broadcom) Endpoint Security також виділяються, поряд з новими конкурентами, такими як SentinelOne Singularity. Кілька з цих рішень надають пріоритет швидкому розгортанню, хмарним функціональним можливостям та сумісності з комплексними системами безпеки. Наприклад, Cortex XDR від Palo Alto може консолідувати журнали з різних джерел [18], а SentinelOne просуває свій автономний захист на основі штучного інтелекту [16].

Незважаючи на складні функції цих інструментів, організації часто стикаються з труднощами під час розгортання. Кілька агентів кінцевих точок можуть конфліктувати один з одним і споживати ресурси: дослідження в галузі показало, що в середньому на одному пристрої працює близько 10 агентів безпеки, що може погіршити продуктивність, а також створити нові вразливості, коли інструменти конфліктують. Об'єднання різноманітних продуктів для кінцевих точок у поточні операції безпеки може бути складним. Крім того, багатьом компаніям не вистачає спеціалізованого персоналу, необхідного для управління сучасними платформами EDR. Експерти зазначають, що захист широкого спектру кінцевих точок зазвичай вимагає більших, висококваліфікованих команд безпеки, а найм/навчання таких фахівців може бути дорогим. Фінансові обмеження впливають на цей сценарій, а також побоювання щодо взаємодії з користувачем; наприклад, суворі протоколи безпеки можуть перешкоджати продуктивності пристроїв або генерувати хибні спрацьовування, що може дратувати користувачів. Крім того, компанії повинні регулярно оцінювати нові ризики (такі як вразливості ланцюга поставок та проблеми, пов'язані з віддаленою роботою) та коригувати свої

рішення для кінцевих точок відповідно.

Таблиця 1.3 – Оцінка провідних постачальників засобів захисту кінцевих точок

Постачальник	Продукт	Магічний квадрант Gartner 2023	Рейтинг виявлення	Оцінка інновацій
Фортінет	FortiEDR	Лідер	97%	Високий
CrowdStrike	Falcon	Лідер	98%	Високий
SentinelOne	Singularity	Візіонер	95%	Дуже високий
Софос	Intercept X	Челленджер	90%	Помірний

[Джерело: Магічний квадрант Gartner для EPP, 2023][5]

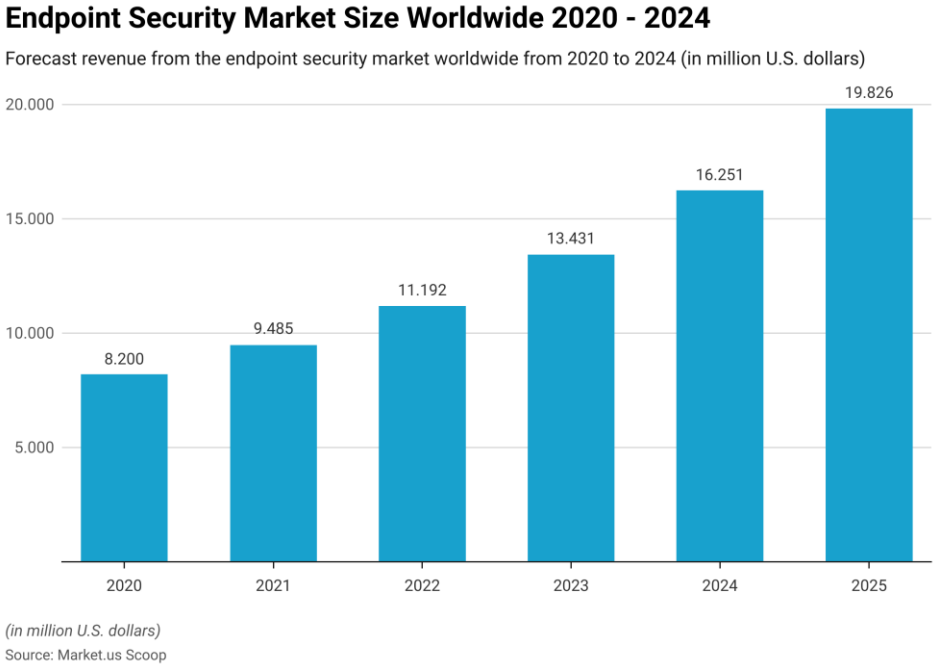

Рисунок 1.4. Гістограма або лінійна діаграма, що показує тенденції на ринку безпеки кінцевих точок з 2020 по 2025 рік [28]

Для ефективної оцінки рішень для захисту кінцевих точок необхідно враховувати кілька ключових критеріїв:

- Можливості запобігання: Ефективність у зупинці загроз до їх виконання;
- Точність виявлення: здатність виявляти відомі та невідомі загрози;
- Швидкість реагування: час для ізоляції, оповіщення та усунення наслідків;
- Споживання ресурсів: Продуктивність агента на кінцевих пристроях;
- Централізоване управління: інформаційні панелі, забезпечення дотримання політик, обробка сповіщень;
- Інтеграція: Сумісність із SIEM/SOAR, брандмауерами, сканерами вразливостей;
- Відповідність та звітність : підтримка журналів аудиту, нормативно-правових баз.

1.3.2 Провідні комерційні рішення

Таблиця 1.4 – Огляд деяких з найбільш визнаних рішень на ринку сьогодні:

Постачальник	Назва рішення	Профілактика	Виявлення	Відповідь	Сильні сторони
Fortinet	FortiEDR	Високий	Високий	Високий	Потужний поведінковий аналіз, блокування в режимі реального часу, інтеграція з Fortinet Fabric

Продовження таблиці 1.4

CrowdStrike	Платформа Falcon	Високий	Високий	Середній	Хмарний, чудова видимість, швидка телеметрія
SentinelOne	Singularity	Високий	Високий	Високий	Автономне виявлення, можливості відкату
Microsoft	Defender	Середній	Високий	Середній	Рідний для Windows, економічно вигідний
Sophos	Intercept X	Середній	Середній	Середній	Зручний інтерфейс із покращеним штучним інтелектом

Fortinet FortiEDR вирізняється своїм акцентом на запобіганні в реальному часі та легким використанням кінцевих точок. Його здатність працювати як на етапі до, так і після виконання – без необхідності драйверів рівня ядра – робить його придатним для середовищ, критично важливих для продуктивності.

2. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА ОСНОВІ FORTIEDR

2.1 Архітектура та компоненти рішення FortiEDR

FortiEDR, розроблений Fortinet, – це передове рішення для виявлення та реагування на кінцеві точки (EDR), яке забезпечує оперативне виявлення загроз та їх усунення для кінцевих точок, включаючи робочі станції, сервери та хмарні робочі навантаження. На відміну від традиційних платформ захисту кінцевих точок (EPP), FortiEDR робить акцент на проактивних стратегіях безпеки, поведінковому моніторингу та автоматизованому реагуванні на інциденти, зберігаючи при цьому мінімальний вплив на продуктивність кінцевих точок [10].

2.1.1 Огляд архітектури FortiEDR

FortiEDR складається з модульної, масштабованої та хмарної архітектури, яка включає такі основні компоненти:

1) Центральна консоль керування (CMC);
2) Сенсорні агенти;
3) Основний сервер;
4) Хмарні служби розвідки загроз;
5) Механізм пом'якшення наслідків [9];

Ці компоненти працюють разом, щоб забезпечити повну видимість, запобігання, виявлення та реагування на інциденти безпеки.

Таблиця 2.1 – Компоненти та ролі архітектури FortiEDR [9]

Компонент	Опис	Роль
Центральний менеджер	Веб-інтерфейс для налаштування	Управління політиками та оповіщення
Агрегатор	Агрегує дані кінцевих точок	Пересилає менеджеру та зберігає резервні копії

Колекціонер	Встановлено на кінцевій точці	Відстежує, запобігає та реєструє події
Хмарні сервіси	Хмарна платформа Fortinet	Оновлення, ліцензування, інформація про загрози

[Джерело: Посібник адміністратора Fortinet FortiEDR, 2023]

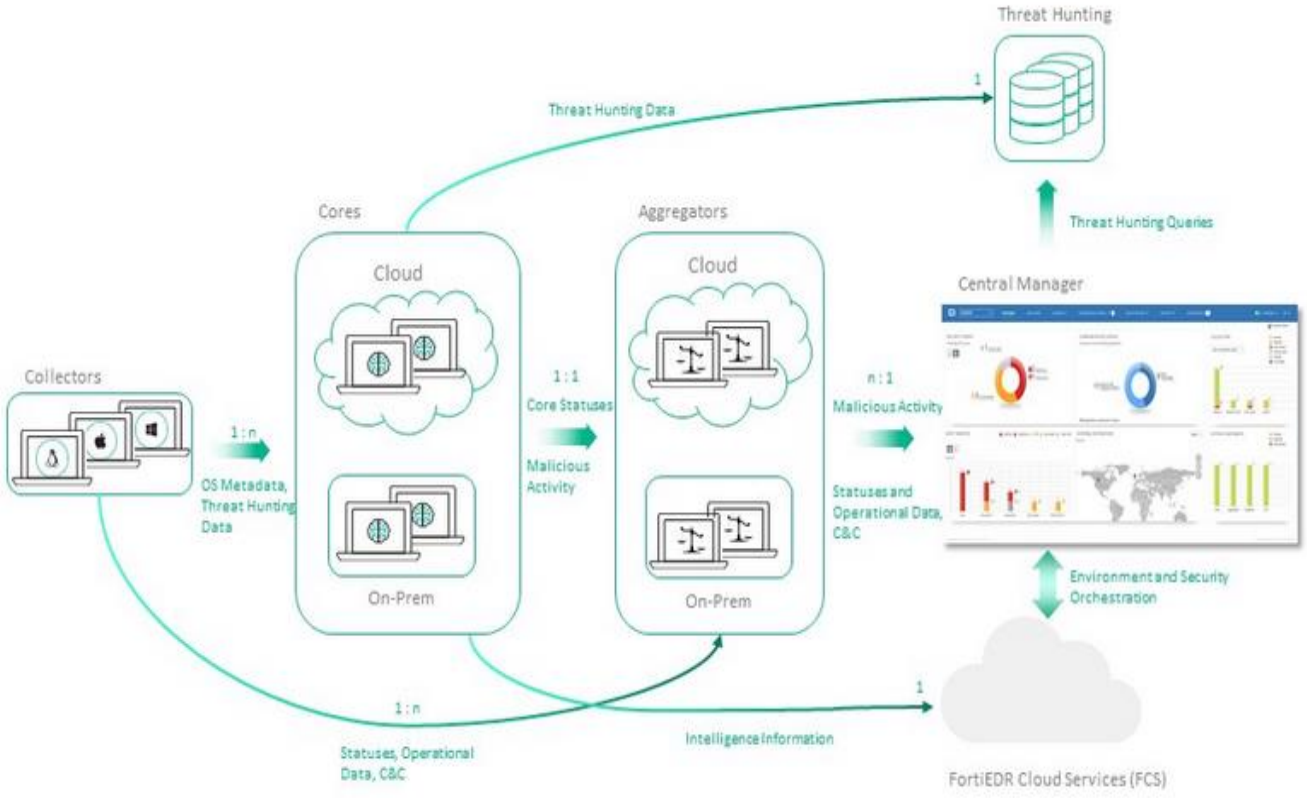

Рисунок 2.1: Компоненти FortiEDR [9]

2.1.2 Центральна консоль керування (CMC)

Центральна консоль керування функціонує як основний інтерфейс, який використовується аналітиками безпеки та адміністраторами. Її обов'язки включають встановлення політик, керування кінцевими точками, моніторинг сповіщень та ініціювання розслідувань. Як правило, CMC розміщується локально або в хмарі та взаємодіє з агентами через захищені з'єднання.

2.1.2 Сенсорний агент

Невеликий датчик FortiEDR встановлюється на кінцевих точках, таких як пристрої Windows, macOS або Linux. Він відстежує активність системи, зупиняє процеси та збирає дані телеметрії. Працюючи на рівні ядра, датчик виконує поведінковий аналіз запущених процесів, активності файлової системи та змін у реєстрі.

2.1.4 Основний сервер

Цей бекенд-компонент сприяє зв'язку між агентами та консоллю, керує зберіганням даних про події та обробляє канали інформації про загрози. Він також контролює розподіл робочого навантаження у великих корпоративних впровадженнях.Тобто у великих корпоративних мережах, де встановлено сотні або тисячі агентів FortiEDR, основний сервер:

- Оптимізує обробку подій: якщо від багатьох кінцевих точок надходить великий обсяг даних (телеметрії, подій безпеки), основний сервер розподіляє їх обробку між кількома сервісами чи вузлами (наприклад, Data Processor Nodes або Worker Nodes).
- Забезпечує масштабованість: система не перевантажується, тому що сервер розподіляє запити рівномірно між доступними обчислювальними ресурсами.
- Підтримує баланс навантаження (load balancing): автоматично керує тим, які частини інфраструктури обробляють дані від конкретних агентів це дозволяє підтримувати стабільну продуктивність навіть за умов високого трафіку.
- Забезпечує високу доступність (HA): у разі збоїв окремих компонентів система продовжує працювати, переадресовуючи навантаження на резервні вузли.

Уточнення з документації Fortinet: «The Core server manages workload distribution by coordinating traffic across Event Collector, Aggregator, and Communication Servers, especially in high-scale environments.» [9]

Тобто основний сервер – це «мозок», що розумно керує внутрішніми процесами, щоб усе працювало швидко, без втрат і затримок.

2.1.5 Хмарні аналітичні служби

FortiEDR включає служби розвідки загроз FortiGuard , які розширюють можливості локального виявлення за допомогою глобальних індикаторів компрометації (IOC), сигнатур шкідливих програм та профілів зловмисників. Ця інтеграція покращує здатність FortiEDR виявляти експлойти нульового дня та поліморфне шкідливе програмне забезпечення [9].

2.2. Призначення та основні функції компонентів FortiEDR

Кожен елемент FortiEDR має окрему роль, яка відіграє вирішальну роль в ефективному плані безпеки кінцевих точок. Нижче наведено короткий опис їхніх основних функцій.

2.2.1 Центральна консоль керування (CMC)

Консоль служить основним командним центром для всіх дій безпеки, що стосуються кінцевих точок. Її можливості включають:

- Автоматизоване зниження ризиків.
- Виявлення на основі поведінки.
- Полювання на загрози.
- Віртуальне лачення.
- Звітність та аналітика.
- Відповідь на основі ідентичності.

Крім того, ця консоль дозволяє інтеграцію з інструментами SIEM (керування інформацією та подіями безпеки), такими як Splunk та FortiSIEM [7].

2.2.2 Сенсорний агент

Датчик має три основні функції:

- Моніторинг поведінки в режимі реального часу: відстежує дії на кінцевій точці, включаючи виклики API, використання пам'яті та зміни у файлах.
- Запобігання зараженню: Зменшує ризики запуску розпізнаного шкідливого програмного забезпечення та спроби його використання.

- Виявлення після зараження: Виявляє малопомітні або нефайлові загрози шляхом аналізу поведінкових показників. [9]

Датчики можуть працювати в режимі «моніторингу» або «блокування» відповідно до політики безпеки, що дозволяє адаптивне розгортання та зменшує потенційні перебої.

2.2.3 Розвідка загроз та машинне навчання

FortiEDR поєднує традиційні методи на основі сигнатур із передовими методами машинного навчання (ML), які були навчені на великій колекції зразків шкідливих програм. Ці методи виявляють порушення в активності процесів та взаємодії систем, які не відповідають визнаним базовим рівням.

FortiGuard Labs від Fortinet постійно вдосконалюють ці моделі та надають їх через хмарні аналітичні служби. Виявлення на основі машинного навчання має вирішальне значення для виявлення безфайлового шкідливого програмного забезпечення, бінарних файлів, що живуть поза землею (LOLBins), та внутрішніх загроз. [9]

2.2.4 Механізм пом'якшення наслідків

Цей компонент виступає в ролі системи реагування в рамках FortiEDR . Він дозволяє:

1) Завершення процесів;
2) Ізоляція мереж;
3) Карантин файлів;
4) Автоматизовані методичні рекомендації для поширених типів атак (наприклад, програм-вимагачів, ескалація привілеїв);
5) Інтеграція з інструментами SOAR (оркестрація безпеки, автоматизація та реагування).

Механізм пом'якшення наслідків працює відповідно до встановлених або адаптивних правил, мінімізуючи середній час реагування (MTTR) [7].

2. 3. Процеси роботи з рішенням FortiEDR

Функціонування FortiEDR можна розділити на п'ять основних фаз: збір, запобігання, виявлення, реагування та усунення наслідків.

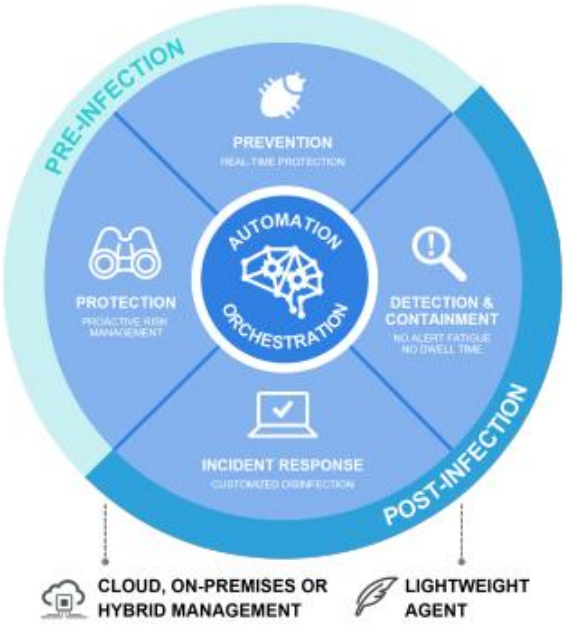

Рисунок 2.3: Фази роботи рішення FortiEDR. [7]

2.3.1 Збір та аналіз даних

FortiEDR починає реалізацію свого протоколу безпеки, збираючи обширні дані з кожної контрольованої кінцевої точки. Агент FortiEDR Collector постійно спостерігає за активністю на рівні ядра, документуючи виконання файлів, зміни пам'яті, активність процесів та мережеві підключення. Ця необроблена телеметрія безпечно передається до агрегатора, а потім аналізується центральним менеджером.

Процес збору даних базується на поведінковому аналізі та контекстній обізнаності, що дозволяє FortiEDR підтримувати пильність як до відомих, так і до невідомих загроз, не покладаючись виключно на сигнатури. Система використовує алгоритми машинного навчання для оцінки поведінки та класифікації подій у режимі реального часу. На відміну від традиційних антивірусних рішень,

аналітичний механізм FortiEDR оцінює намір дії, тим самим покращуючи свою здатність розрізняти доброякісну та шкідливу поведінку з більшою точністю [9].

2.3.2 Профілактика

FortiEDR розроблений для запобігання виконанню шкідливих дій до їх початку, використовуючи методи запобігання як до виконання, так і під час виконання. Колектор впроваджує політики запобігання на кінцевій точці, успішно блокуючи підозрілі процеси, перш ніж вони зможуть завдати шкоди [9].

2.3.3 Виявлення та кореляція

Якщо загроза безпеці обходить запобіжні заходи, спрацює компонент виявлення FortiEDR . Використовуючи телеметрію в режимі реального часу в поєднанні з історичним контекстом, FortiEDR розпізнає нетипову поведінку та моделі атак. Він використовує:

1) Виявлення поведінкових аномалій: позначає відхилення від базової поведінки.

2) Картування MITRE ATT&CK: співвідносить дії з відомими методами атаки.

3) Технологія відстеження коду: відображає походження та ланцюжок виконання підозрілих процесів.

4) Інтеграція розвідки загроз: включає зовнішні індикатори компрометації (IoC) від FortiGuard Labs.

Виявлення поєднується з кореляцією подій, коли кілька сповіщень групуються в один інцидент, якщо вони мають спільні індикатори або впливають на одну й ту саму систему. Це значно зменшує втому від сповіщень та прискорює час реагування аналітиків.

2.3.4 Механізми реагування

Коли виявляється загроза, FortiEDR може або автоматично запускати плани реагування, або сповіщати аналітиків про необхідність вжиття ручних заходів. Ці відповіді включають:

1) Ізоляція кінцевої точки від мережі.

2) Знищення шкідливих процесів у режимі реального часу.

3) Оповіщення адміністраторів через інтеграцію SIEM/SOAR.

4) Переміщення в карантин файлів, що підозрюються у шкідливості.

5) Запуск робочих процесів віддаленого розслідування або ескалації інцидентів.

Панель керування FortiEDR Central Manager надає аналітикам SOC часову шкалу подій, а також можливість ініціювати, налаштовувати або коригувати відповіді. Це дозволяє як автоматизоване управління, так і детальне ручне втручання, дотримуючись інструкцій організації.

2.3.5 Відновлення та усунення наслідків

Заключним етапом роботи FortiEDR є процес відновлення та усунення наслідків, який відбувається після інциденту. Після усунення загрози система надає допомогу для:

1) Відкат шкідливих змін (наприклад, модифікацій реєстру, втрачених файлів).

2) Відновлення безпечного стану системи за допомогою поведінкових знімків.

3) Підтримка судово-медичних розслідувань з дампом пам'яті та вилученням файлів.

4) Ведення журналу аудиту на предмет дотримання нормативних вимог (наприклад, ISO 27001, HIPAA).

FortiEDR зберігає вичерпну інформацію про судово-медичну експертизу, що дозволяє командам безпеки зрозуміти масштаби та походження атаки. Відновлення включає не лише технічні виправлення, але й перегляд стратегій запобігання та

оцінку процедур реагування на інциденти для підвищення стійкості в майбутньому.

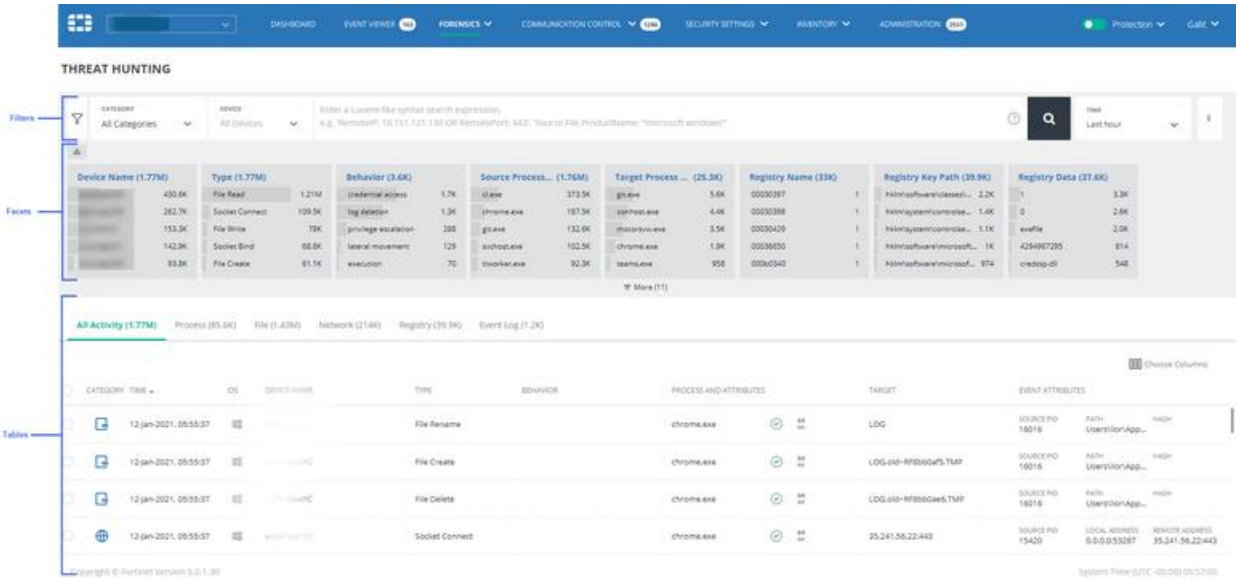

Рисунок 2.5: Робочий процес, що показує, як аналітики використовують FortiEDR для проактивного пошуку загроз. [7]

У цьому розділі було детально проаналізовано архітектуру, компоненти, принципи роботи та функціональні можливості рішення FortiEDR як сучасного інструменту захисту кінцевих точок. Встановлено, що FortiEDR поєднує можливості виявлення загроз у реальному часі, поведінкового аналізу, машинного навчання та автоматизованого реагування, що забезпечує високий рівень захисту від сучасних типів атак, включно з безфайловим шкідливим ПЗ, програмами-вимагачами та загрозами нульового дня.

Комплексна архітектура FortiEDR дозволяє масштабоване впровадження у середовищах з великою кількістю кінцевих точок, а також інтеграцію з іншими системами кіберзахисту, зокрема SIEM. Його здатність не лише виявляти, але й оперативно нейтралізовувати інциденти робить FortiEDR потужним інструментом для організацій, що прагнуть до підвищення рівня інформаційної безпеки.

Отже, використання FortiEDR є обґрунтованим вибором для організацій, які потребують надійного, гнучкого та автоматизованого рішення для захисту кінцевих точок в умовах зростаючих кіберризиків.

3. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗЦІЇ

У цьому розділі розглядається, як розробити та впровадити ефективний захист кінцевих точок за допомогою рішення FortiEDR від Fortinet . Він охоплює різні методи розгортання (локальні, хмарні та гібридні), процес розслідування інцидентів у FortiEDR, а також цільові технічні та політичні пропозиції щодо захисту кінцевих точок організації. Поради включають найкращі практики Fortinet та галузеві тематичні дослідження для демонстрації успішних стратегій.

Вибір правильної стратегії розгортання для FortiEDR залежить від різних організаційних факторів, включаючи розмір, галузь, потреби у відповідності та зрілість IT-інфраструктури. У цьому розділі представлено гнучкі варіанти розгортання, адаптовані до різних профілів підприємств.

Таблиця 3.1 – Рекомендовані сценарії розгортання FortiEDR [2]

Тип організації	Модель розгортання	Ключова перевага
Малий бізнес	Керований хмарою	Невисокі витрати на обслуговування, швидке налаштування
Середнє підприємство	Гібридний (локальний + хмарний)	Гнучкість + контроль
Велике підприємство	Локальна версія	Повний контроль, підтримка відповідності

[Джерело: Посібник з розгортання Fortinet]

3.1 Варіант розгортання системи захисту кінцевих точок організації на основі FortiEDR

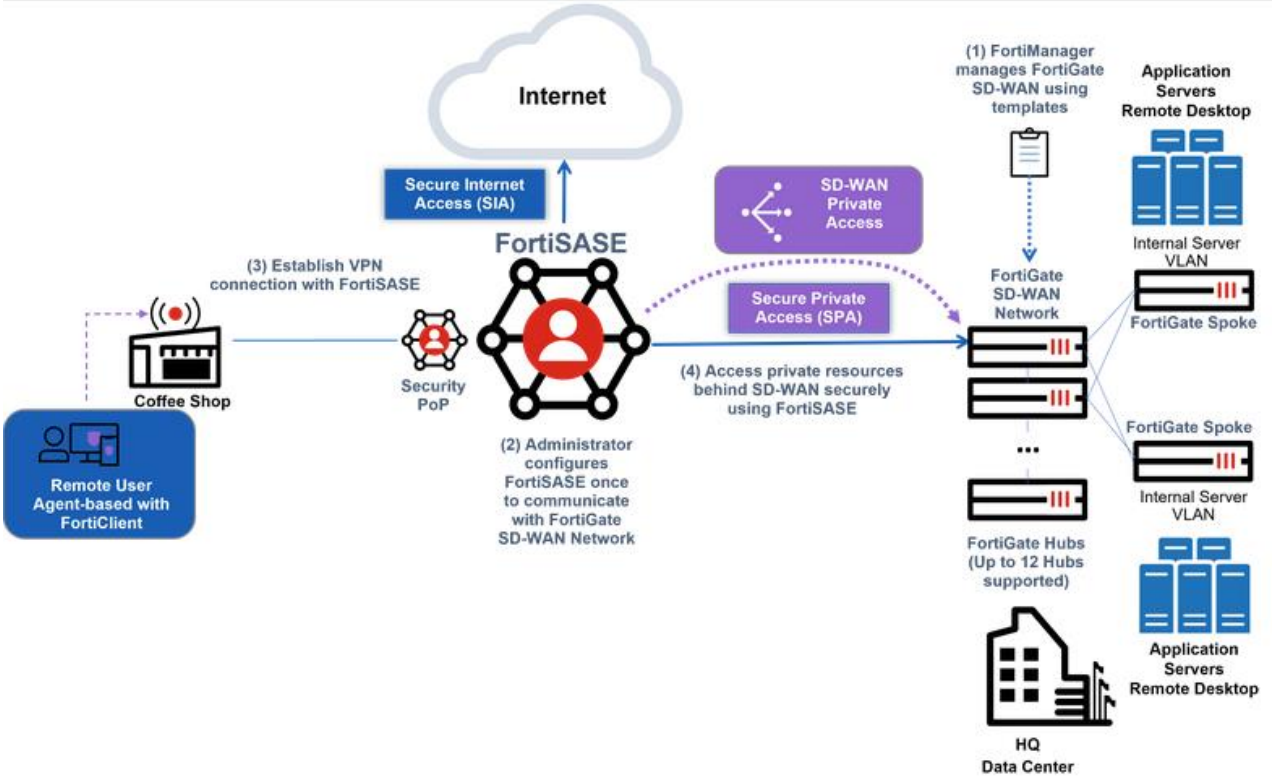

Рисунок 3.1: Діаграма, що показує, як FortiEDR вписується в існуючу інфраструктуру організації. [2]

FortiEDR підтримує гнучкі моделі розгортання, що відповідають різним потребам організації. Рішення використовує легкий колектор (агент) на кожній кінцевій точці та централізовану інфраструктуру управління (FortiEDR Core та Central Manager). Оскільки агент вимагає мінімальних ресурсів (зазвичай <1% процесорного часу, 120 МБ оперативної пам'яті, ~20 МБ диска), його можна встановлювати широко, не впливаючи на пристрої користувачів. FortiEDR можна розгортати локально (включаючи ізольовані середовища), у хмарі (через безпечні хмарні сервіси FortiEDR від Fortinet) або в гібридному режимі. Наприклад, у локальному режимі організація використовує власні сервери FortiEDR Core та агрегатор; у хмарному режимі кінцеві точки звітують перед багатокористувацькою хмарою управління Fortinet. Гібридне розгортання – поєднання локальних серверів

та хмарних сервісів – дозволяє критично важливим системам залишатися ізольованими, розширюючи охоплення для віддалених користувачів. У всіх випадках FortiEDR забезпечує автономний захист кінцевих точок (вбудований штучний інтелект захищає їх навіть у разі відключення) та інтегрується з інфраструктурою безпеки Fortinet (NGFW, NAC, SIEM тощо) для забезпечення виконання мережевих дій та обміну аналітичними даними.

3.1.1 Моделі розгортання

1. Локальне розгортання: рекомендується, коли існують вимоги до суворого контролю даних або дотримання обмежень. Локальне розгортання Ядро(я) FortiEDR можна встановити у внутрішньому центрі обробки даних або навіть в ізольованих мережах. Цей режим гарантує, що телеметрія не виходить за межі корпоративної мережі. У документації Fortinet зазначається, що FortiEDR «може бути розгорнутий локально в ізольованому середовищі» [10], захищаючи кінцеві точки як локально, так і офлайн. Найкращою практикою є використання виділеної підмережі керування та встановлення принаймні двох вузлів Core/Aggregator для високої доступності. Керування доступом на основі ролей (RBAC) слід увімкнути на консолі FortiEDR для розділення обов'язків (наприклад, аналітики та адміністратори), а безпечний сервер керування (JumpBox) може додатково ізолювати адміністративний доступ.

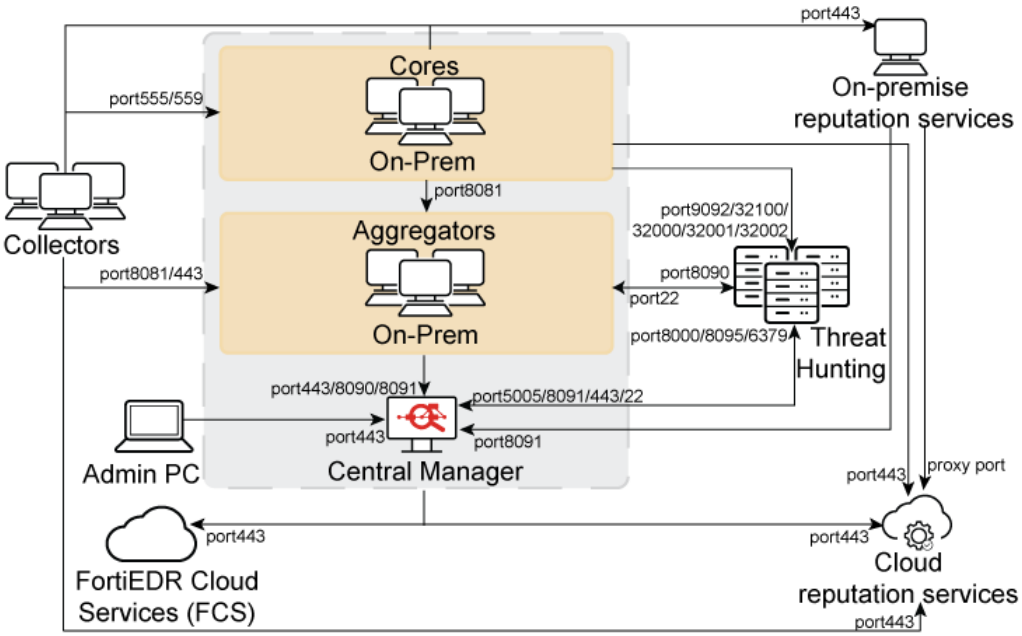

Рисунок 3.2: Схема локального (on-premise) розгортання компонентів FortiEDR та їх взаємодії [6]

Плюси:

1) Повний контроль над даними та інфраструктурою;
2) Відсутність залежності від зовнішніх хмарних сервісів;
3) Краща відповідність середовищам з повітряними зазорами.

Мінуси:

4) Вищі початкові витрати та навантаження на обслуговування;
5) Потрібен кваліфікований внутрішній персонал.

2. Розгортання у хмарі (FortiEDR Cloud): У цій моделі Fortinet розміщує площину управління. Кінцеві точки звітують перед хмарою Fortinet, що забезпечує спрощену масштабованість та обслуговування. У технічному описі Fortinet наголошується, що хмарно-керована платформа може бути «розгорнута на безпечному хмарному екземплярі» з багатокористувацьким управлінням. Використання хмари для розгортання дозволяє здійснювати оновлення та надає організаціям можливість швидко розширюватися до тисяч пристроїв. Однак цей метод вимагає надійного підключення до Інтернету для агентів. Ця стратегія особливо корисна для віддалених працівників або як рішення для швидкого розгортання (FortiEDR може захистити «сотні тисяч кінцевих точок» завдяки своїй інтегрованій хмарній інфраструктурі). Для конфіденційної інформації важливо гарантувати безпечний зв'язок з FortiCloud (наприклад, через VPN або проксі-сервер) для дотримання правил конфіденційності.

Плюси:

- Нижчі витрати на налаштування;
- Висока масштабованість та автоматичні оновлення;
- Швидке розгортання.

Мінуси:

- Менше налаштування інфраструктури;
- Вимагає сильної довіри до системи безпеки постачальника.

3. Гібридне розгортання: Цей підхід інтегрує як локальні, так і хмарні рішення. Наприклад, захищені системи або стаціонарні сервери можуть працювати з локальним ядром, тоді як мобільні пристрої та філії можуть використовувати FortiCloud. Fortinet пропонує потужну підтримку гібридних середовищ. Поширений метод включає налаштування FortiEDR Core як локального JumpBox, який безпечно підключається до FortiCloud, дозволяючи локальним кінцевим точкам повідомляти про інциденти навіть під час нестабільного підключення до Інтернету. Гібридні налаштування дозволяють організаціям поступово переходити до хмари або ізолювати критичні активи (такі як сервери DMZ), використовуючи хмарну аналітику для інших функцій.

Плюси:

1) Зберігає локальний контроль, водночас використовуючи переваги глобального інтелекту FortiGuard;
2) Добре підходить для регульованих галузей з віддаленими філіями.

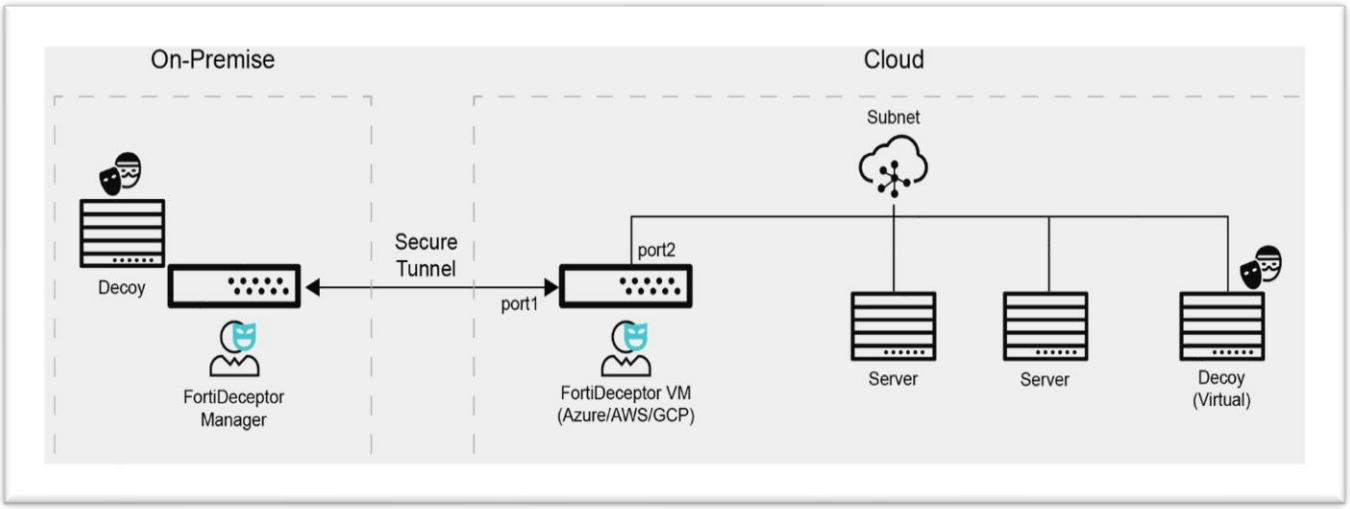

Рисунок 3.3: Схема гібридного розгортання компонентів FortiEDR та їх взаємодії [29]

3.1.2 Фази розгортання

Поетапний підхід забезпечує мінімальні збої:

1. Виявлення: інвентаризація існуючих кінцевих точок та інфраструктури.

2. Пілотне тестування: Розгорніть FortiEDR на невеликій тестовій групі (наприклад, у відділах IT та кадрів).

3. Режим моделювання політик: Запуск у режимі лише виявлення для тестування правил.

4. Поступове розгортання: Розширюйте розгортання по всіх відділах поетапно.

5. Налаштування та навчання: Коригування політик, удосконалення методичних посібників та навчання персоналу.

6. Перехід до режиму активного захисту з профілактикою: Перехід до режиму активного захисту в усій організації.

3.1.3 Технічні вимоги

- ОС кінцевої точки: Windows 10/11, Linux (RHEL, CentOS, Ubuntu), macOS.
- Вимоги до сервера (центральний менеджер):
  - 8-ядерний процесор, 32 ГБ оперативної пам'яті, понад 500 ГБ сховища;
  - захищена ОС (FortiOS , CentOS або власний образ);
- Мережеві порти:
  - TCP 8013 (Від колектора до агрегатора);
  - HTTPS для доступу до FortiGuard. [9]

3.1.4 Рекомендації щодо інтеграції

Для максимальної безпеки FortiEDR слід інтегрувати з:

1) Брандмауери FortiGate (для автоматичного блокування IP-адрес);
2) FortiSIEM або Splunk (для агрегації та аналізу журналів);
3) FortiNAC (для керування мережевим доступом на основі пристроїв);
4) Шлюзи безпеки електронної пошти (для виявлення фішингу). [9]

Такий взаємопов'язаний підхід розширює можливості реагування FortiEDR, запускаючи реакції на рівні мережі на загрози, що виникають на кінцевих точках.

FortiEDR тісно інтегрується з ширшою системою безпеки Security Fabric.

Його консоль може наказувати брандмауерам FortiGate блокувати шкідливі IP-адреси або ізолювати їх через FortiNAC . Це означає, що компрометація кінцевої точки може автоматично запускати стримування на рівні мережі. Підсумовуючи, гнучке розгортання FortiEDR (локально , хмарно, гібридно) та малий обсяг агентів дають організаціям можливість адаптувати рішення до своєї політики безпеки, ресурсів та нормативних обмежень.

3.2 Процедура проведення розслідувань інцидентів у рішенні FortiEDR

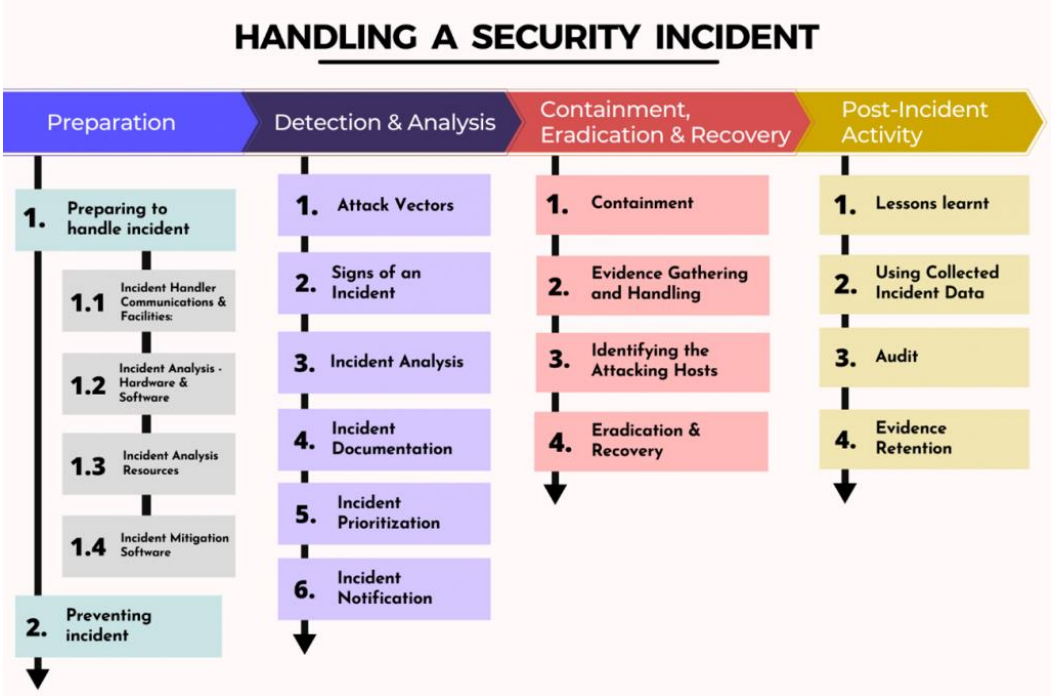

Рисунок 3.4: Фази реагування на інциденти згідно з NIST 800-61r2: підготовка, виявлення, стримування тощо [26]

FortiEDR реалізує комплексний робочий процес реагування на інциденти, який поєднує автоматичне стримування з глибоким судово-медичним аналізом. Коли кінцева точка демонструє підозрілу поведінку (наприклад, процес намагається виконати ризиковану дію), агент FortiEDR негайно блокує дію та надсилає «знімок» активності ОС та метаданих до ядра FortiEDR. Ядро використовує запатентовану технологію трасування коду для аналізу події в режимі реального часу. Законні запити дозволені, але зловмисні спроби блокуються, і генерується сповіщення про інцидент з повним контекстом (імена

процесів, інформація про реєстр/стан, користувач тощо). Найголовніше, що FortiEDR «автоматично збагачує дані» навколо кожного сповіщення, збираючи докази до та після зараження для сприяння судово-медичному аналізу.

Після отримання сповіщення аналітики використовують консоль FortiEDR Central Manager для перегляду часової шкали інциденту. Консоль відображає вертикальну хронологію всіх пов'язаних дій (створення файлів, мережевих підключень, запуску процесів), пов'язаних з інцидентом. Кожна подія на часовій шкалі відстежується за кодом до її батьківського елемента, створюючи чіткий ланцюжок причинно-наслідкових зв'язків («невід'ємний доказ»). Керований інтерфейс точно підкреслює, чому подію було позначено (зіставляючи її з методами MITRE ATT&CK) і навіть пропонує наступні кроки розслідування. Наприклад, якщо шкідливий скрипт PowerShell було заблоковано, часова шкала покаже створення цього скрипта певним процесом, команду, яку він виконав, і спроби потоків даних.

Таблиця 3.2 – Етапи плану реагування на інциденти на основі FortiEDR [26]

Сцена	Опис	Використані інструменти
Виявлення	Розпізнати загрозу	Колектор FortiEDR
Сортування	Пріоритетність серйозності інциденту	Центральний менеджер
Розслідувати	Проаналізуйте першопричину	Криміналістика часової шкали/пам'яті
Містити	Ізолювати кінцеву точку	Карантин
Відновлення	Відновіть безпечну роботу	Точка відновлення

[Джерело: NIST SP 800-61r2]

Для глибшого аналізу використовуються можливості FortiEDR для судово-медичної експертизи. Артефакти в пам'яті (наприклад, дампи процесів, що виконуються) зберігаються під час оповіщення, що дозволяє проводити офлайн-аналіз безфайлових атак. Надбудова Forensic Analysis дозволяє слідчим перевіряти

внутрішні дані стека, які призвели до інциденту. Використовуючи це, аналітики можуть досліджувати знімки пам'яті, витягувати файли або кущі реєстру з кінцевої точки та навіть детонувати підозрілий файл у FortiSandbox . Всі дані сповіщень (включаючи ці судово-медичні витяги) можна переглядати в консолі FortiEDR.

Тим часом FortiEDR підтримує кореляцію сповіщень шляхом інтеграції із зовнішніми системами. Всі сповіщення можна пересилати через syslog або REST API до SIEM (наприклад, FortiSIEM), де вони корелюються з даними брандмауера, мережі або журналу. Крім того, сама консоль FortiEDR кластеризує пов'язані сповіщення: кілька подій на одному хості (або на кількох хостах, що спільно використовують IOC зловмисника) групуються в один інцидент. Це єдине подання інцидентів гарантує, що аналітики бачать всю відповідну активність одночасно. Наприклад, якщо загроза перемістилася латерально на другу машину, FortiEDR відображатиме події обох машин в рамках одного інциденту.

Основна перевага FortiEDR полягає в його потужних можливостях криміналістики та розслідування, що дозволяє організаціям швидко та точно відстежувати, аналізувати та реагувати на кіберінциденти. FortiEDR надає структуровану систему реагування на інциденти, яку можна інтегрувати в ширший робочий процес центру операцій безпеки (SOC).

3.2.1 Виявлення та сповіщення про інциденти

FortiEDR виявляє підозрілу подію – незалежно від того, чи спричинена вона виявленням на основі поведінки, чи зіставленням розвідувальних даних – система створює об'єкт інциденту, який включає:

1) Хронологія активності з позначкою часу;
2) Пов'язані файли та процеси;
3) Задіяні активи та користувачі;
4) Відображені техніки ATT&CK. [33]

Інциденти одразу відображаються на панелі інструментів Central Manager і можуть ініціювати надсилання сповіщень електронною поштою/SIEM.

3.2.2 Реконструкція часової шкали

Однією з унікальних переваг FortiEDR є його здатність реконструювати повні ланцюжки подій, що призводять до інциденту безпеки та відбуваються після нього. Модуль часової шкали показує:

1) Початковий вектор компрометації (наприклад, шкідливий електронний лист, вставка USB);
2) Проміжна активність (наприклад, створення PowerShell, крадіжка облікових даних);
3) Кінцевий вплив (наприклад, витік даних, шифрування програм-вимагачів). [7]

Аналітики можуть використовувати фільтри для відстеження активності за ідентифікатором процесу, користувачем, часовим діапазоном або оцінкою ризику. Ця функціональність є важливою для розуміння масштабу атаки та перевірки її першопричини.

3.2.3 Збір даних для криміналістики

FortiEDR збирає та зберігає метадані й артефакти, які допомагають у глибокій криміналістиці, зокрема:

1) Хеші процесів;
2) Мережеві з'єднання (IP, порт, протокол);
3) Запис файлів та зміни в реєстрі;
4) Виконання зовнішніх команд;
5) Знімки пам'яті (необов'язково). [7]

Аналітики можуть експортувати ці дані або пересилати їх до SIEM/форензичних інструментів для дотримання вимог або судових розглядів.

3.2.4 Прийняття рішень щодо реагування

Щойно розслідування підтвердить шкідливу активність, FortiEDR забезпечить багаторівневе реагування залежно від серйозності та політики:

Низький ризик: лише сповіщати або автоматично вирішувати;

Середній ризик: Сповіщення та запит на підтвердження користувача;

Високий ризик: ізоляція кінцевої точки, завершення процесу, переміщення файлу в карантин.

Реагування може бути повністю автоматизованим (з використанням сценаріїв) або напівручним, залежно від рівня достовірності та операційної політики.

3.2.5 Аналіз після інциденту

Процедури після інциденту включають:

1) Створення звітів про інциденти для аудиту або використання у сфері дотримання вимог;
2) Оновлення політик запобігання для блокування подібних майбутніх загроз;
3) Ініціювання навчальних або інформаційних кампаній (якщо вектор атаки був керований користувачем);
4) Ключові показники ефективності реагування на інциденти (MTTD, MTTR) для реєстрації [21].

FortiEDR інтегрується з такими платформами, як FortiAnalyzer**,** для візуалізації тенденцій з плином часу та виявлення повторюваних моделей атак.

3.3 Рекомендації щодо застосування методів та засобів захисту кінцевих точок організації

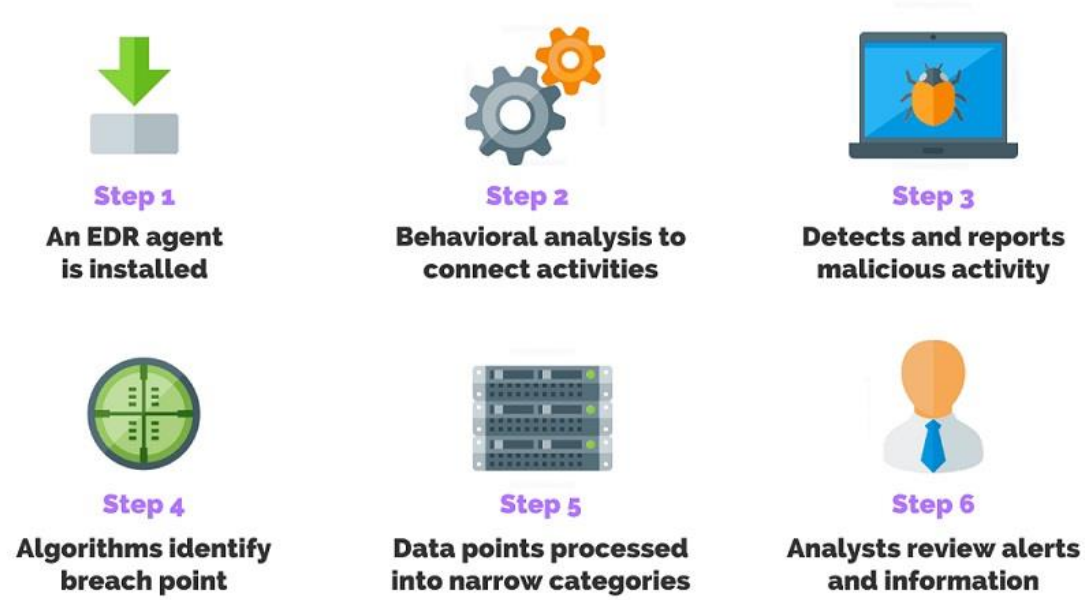

Рисунок 3.5: Життєвий цикл впровадження EDR-рішення [11]

Спираючись на передовий досвід та галузеві стандарти Fortinet, наступні рекомендації поєднують технічні засоби контролю та заходи політики для досягнення надійної безпеки кінцевих точок.

Застосовувати багаторівневу архітектуру безпеки. Жоден окремий інструмент не зупиняє всі атаки. Розгорніть FortiEDR як частину багаторівневого захисту, що включає брандмауери наступного покоління (NGFW), контроль доступу до мережі (NAC), фільтрацію електронної пошти/веб-сторінок та обізнаність користувачів. FortiEDR найефективніший при інтеграції з Fortinet Security Fabric: наприклад, сповіщення у FortiEDR можуть ініціювати блокування FortiGate шкідливих IP-адрес або карантин заражених хостів FortiNAC. Переконайтеся, що шлюзи електронної пошти та веб-проксі сканують вкладення та посилання, а засоби захисту периметра (NGFW, IDS/IPS) налаштовані відповідно до EDR. Наприклад, якщо FortiEDR виявляє шкідливе програмне забезпечення, IP-адресу кінцевої точки можна перенести на брандмауер для негайної ізоляції мережі.

Забезпечення посилення захисту кінцевих точок та керування виправленнями вілбувається таким чином: Обмежити поверхню атаки, вимкнувши невикористовувані служби та вимагаючи мінімальних привілеїв на пристроях

користувачів. Налаштуйвати політики FortiEDR для блокування або ізоляції виконуваних файлів та інструментів сценаріїв (PowerShell, макроси) за замовчуванням. Підтримувати актуальність виправлень ОС та програм на всіх кінцевих точках; «віртуальне виправлення» FortiEDR може зменшити ризик деяких випадків нульового дня, але своєчасне виправлення залишається критично важливим. Використовувати політики контролю пристроїв FortiEDR для обмеження знімних носіїв (блокування USB-накопичувачів) та впровадження повного шифрування диска на ноутбуках. Регулярно перевіряйте кінцеві точки на відповідність тестам безпеки (наприклад, CIS Benchmarks). В цілому використовувати FortiEDR можна не лише як інструмент виявлення, а також й для забезпечення контролю програм та зменшення вразливостей.

Централізація ведення журналу та моніторинг для дотримання вимог. Збирати та зберігати журнали кінцевих точок для відповідності нормативним вимогам або стандартам. Наприклад, підрядники оборонної сфери США (CMMC/NIST) повинні «моніторити, пом’якшувати та звітувати про всі типи кіберзагроз» [23]. Налаштовувати FortiEDR (та інші системи) для надсилання всіх сповіщень та ключової телеметрії до SIEM, такої як FortiSIEM. Тематичні дослідження Fortinet показують, що поєднання EDR з SIEM дозволяє організаціям/корпораціям вести журнали для аудитів протягом цілого року. Переконатися, що ваше SIEM або рішення для ведення журналу співвідносить сповіщення EDR з подіями мережі та сервера, щоб один інцидент (наприклад, шкідливе програмне забезпечення, спричинене фішингом) відображався в одному консолідованому вигляді. Регулярно переглядайте інформаційні панелі та автоматизовані звіти на наявність індикаторів компрометації.

Визначати та впровадити план реагування на інциденти. Розробити формальні процедури для розслідування та реагування на інциденти на кінцевих точках. Ролі та обов'язки (команда SOC, IT-адміністратори та керівництво) повинні бути чітко визначені в письмовому плані. Задокументувати, як використовувати інструменти розслідування FortiEDR та як передавати складні справи (наприклад, до FortiGuard MDR від Fortinet для експертного аналізу). Наприклад, Red Bull

розширив свій SOC, використовуючи FortiGuard MDR Forensics on Demand, зазначивши, що він забезпечує «відмінну видимість» та «дворівневу операційну команду» [14] для швидшого реагування.

Періодично проводити тренування (настільні тренування або тести на проникнення) з працівниками відповідальними за питання інформаційної та кібербезпеки в організації/корпорації, щоб перевірити, чи можуть команди реагувати, використовуючи дані про інциденти FortiEDR . Оновлювати сценарії у FortiEDR (або в системі SOAR), щоб автоматизувати поширені дії (ізоляція хоста, збір пам'яті). План реагування на інциденти також повинен прописувати кроки комунікації та відновлення (наприклад, повідомлення зацікавлених сторін, відновлення резервних копій).

Впроваджувати політики обізнаності користувачів та безпеки кінцевих точок. Технічні засоби контролю підкріплюються чіткими політиками. Забезпечте дотримання правил прийнятного використання, які забороняють ризиковану поведінку (наприклад, встановлення несанкціонованого програмного забезпечення, вимкнення інструментів безпеки). Вимагайте надійних паролів та багатофакторної автентифікації для входу в кінцеві точки та доступу до VPN. Забезпечте регулярне навчання, щоб користувачі розпізнавали фішинг та соціальну інженерію (основні вектори зараження кінцевих точок). Оскільки кінцеві точки часто використовуються у віддаленій або гібридній роботі, слід встановити політики для пристроїв типу «Принеси свій власний пристрій» (BYOD) та персональних пристроїв (наприклад, обов'язкове встановлення FortiEDR або FortiClient на будь-який пристрій, що отримує доступ до корпоративних даних). Заохочуйте оперативне повідомлення про втрачені або викрадені пристрої, щоб їх можна було ізолювати. Нарешті, підтримуйте актуальний перелік активів (у кого який пристрій) та забезпечте інтеграцію нових пристроїв з агентом FortiEDR та базовою конфігурацією.

За потреби використовувати керовані служби або розширені команди. Особливо для організацій без повноцінного SOC розгляньте кероване виявлення та реагування (MDR). Служба MDR від Fortinet може керувати FortiEDR як керованим

рішенням. Це ілюструє приклад із медичного обслуговування: провідний постачальник житлово-комунальних послуг розгорнув FortiEDR на 800 пристроях за допомогою FortiGuard MDR, звільнивши свій невеликий IT-персонал від цілодобового моніторингу. Команда MDR займалася моніторингом та початковим реагуванням, що дозволило клієнту отримати «видимість, аналіз, захист та виправлення в режимі реального часу» без найму великої команди безпеки. Меншим підприємствам слід зважити всі компроміси: керований EDR пришвидшує виявлення та реагування, тоді як більші підприємства можуть вести операції самостійно [7].

Здійснювати оновлення та вдосконалення системи на постійній основі. Безпека – це не одноразовий проект. Регулярно переглядайте журнали та панелі інструментів FortiEDR, щоб налаштовувати політики та усувати хибні спрацьовування. Підтримуйте програмне забезпечення FortiEDR в актуальному стані (та поновлюйте підписи/підписки), щоб отримувати користь від найновішої інформації про загрози. Оновлюйте стек безпеки кінцевих точок за потреби (наприклад, оновлюйте прошивку NGFW або NAC для роботи з останніми інтеграціями FortiEDR). Проводьте періодичне сканування вразливостей та тести на проникнення, щоб перевірити, чи кінцеві точки захищені належним чином. Відстежуйте галузеву інформацію про загрози та оновлення MITRE, а також відповідно коригуйте методичні рекомендації або політики FortiEDR.

Таблиця 3.3 – складена на основі рекомендацій Fortinet щодо забезпечення безпеки кінцевих точок, адаптовано за матеріалами [34]

Площа	Рекомендація	Інструмент/Метод
Виявлення загроз	Розгортання датчиків FortiEDR	FortiEDR
Управління	Використовуйте централізовану консоль	FortiEDR , SIEM
Латування	оновлень ОС та програмного забезпечення	Системи керування патчами
Контроль доступу	Забезпечити мінімальні привілеї та контроль програм	RBAC, білий список
Реагування на	Підготуйте схеми дій,	SOAR, ізоляція FortiEDR

інциденти	автоматизуйте стримування	
Віддалена робота	Захистіть віддалених користувачів за допомогою VPN + ZTNA	FortiClient , ZTNA
Навчання	Проводьте симуляції фішингу та інформаційні кампанії	Платформи для підвищення обізнаності
Інтеграція	Підключення EDR до мережевих систем та систем розвідки загроз	FortiGate , FortiAnalyzer , SIEM
Постійне вдосконалення	Аудит та перегляд політик і конфігурацій	Інструменти відповідності, повідомляє FortiEDR .

[Джерело What is Cybersecurity? | Types, Threats & Best Practices | Fortinet]

Щоб створити безпечне та стійке середовище кінцевих точок, організації повинні впровадити стратегічне поєднання технологій, політики, навчання та постійного моніторингу. Наведені нижче рекомендації взяті з передового досвіду, реального розгортання та інтеграційних рекомендацій Fortinet.

3.3.1 Технічні рекомендації

1. Увімкнути запобігання в реальному часі:

- Використовуйте модулі передвиконання та виконання FortiEDR для блокування відомих та невідомих загроз перед виконанням;
- Завжди тестуйте нові правила запобігання в режимі симуляції, перш ніж застосовувати їх глобально.

2. Забезпечити контроль застосунків:

- Ведіть затверджений список програмного забезпечення, яке дозволено запускати на кінцевих точках;
- Блокувати виконання невідомих або неавторизованих бінарних файлів.

3. Впроваджуйте мережеву ізоляцію:

- Налаштуйте FortiEDR для автоматичної ізоляції заражених кінцевих точок та блокування горизонтального переміщення;
- Інтеграція з FortiNAC або брандмауерами для розширеної автоматизації реагування.

4. Безпечний доступ до зовнішніх пристроїв:

- Вимкніть або обмежте використання USB за допомогою політики, якщо в цьому немає крайньої необхідності;
- Контролюйте журнали доступу до знімних носіїв на наявність аномалій.

5. Увімкнути функції захисту пам'яті:

- Активуйте методи зменшення експлойтів, такі як захист від розпилення купи даних та виявлення впровадження коду.

6. Плануйте часті оновлення EDR:

- Регулярно синхронізуйте дані з FortiGuard , щоб отримувати актуальну інформацію про загрози та отримувати вдосконалення механізму захисту. [9]

3.3.2 Рекомендації щодо організаційної політики

1. Визначення політики захисту кінцевих точок:

- Чітко окресліть політики прийнятного використання, контролю програмного забезпечення та встановлення виправлень;
- Обов’язково встановіть багатофакторну автентифікацію для віддаленого доступу.

2. Інтеграція навчання з питань безпеки:

- Регулярно навчайте співробітників фішингу, безпеці файлів та тактикам соціальної інженерії;
- Моделюйте реальні сценарії атаки, щоб перевірити готовність до реагування.

3. Встановлення контролю доступу на основі ролей (RBAC):

- Призначте ролі з найменшими привілеями в Центральному менеджері, зменшуючи внутрішні загрози.

4. Ведення журналів аудиту та відповідності:

- Використовуйте функції звітності FortiEDR для ведення журналів, необхідних для аудитів HIPAA, GDPR або ISO 27001. [9]

3.3.3 Рекомендації щодо моніторингу та покращення

1. Проводити періодичні оцінки ризику кінцевих точок:

- Оцініть вплив пристрою на основі використання, рівня доступу та місцезнаходження;
- Окремо позначайте та контролюйте кінцеві точки високого ризику.

2. Використання інтеграції SIEM/SOAR для кореляції:

- Пересилайте журнали FortiEDR на такі платформи, як FortiSIEM , Splunk або Microsoft Sentinel, для ширшої аналітики.

3. Регулярно проводите навчання з реагування на інциденти:

- Тестування робочих процесів реагування з використанням імітації програм-вимагачів або внутрішніх загроз;
- Відстежуйте показники ефективності, такі як середній час виявлення (MTTD) та середній час реагування (MTTR).

4. Впровадити архітектуру мережі Zero Trust:

- Забезпечте постійну перевірку всіх запитів на доступ за допомогою даних стану FortiEDR;
- Включіть оцінку ризиків пристроїв у політики контролю доступу. [9]

3.3.4 Довгострокові рекомендації

- Плануйте міграцію XDR для розширення видимості за межі кінцевих точок;
- Бюджет на цілодобовий моніторинг загроз через постачальника MDR, якщо внутрішній персонал обмежений;
- Моніторинг дорожніх карт постачальників EDR для забезпечення відповідності новим потребам у дотриманні вимог (наприклад, Директива NIS2, мандати CISA);
- Проводити щорічні оцінки червоної команди для перевірки ефективності виявлення кінцевих точок.

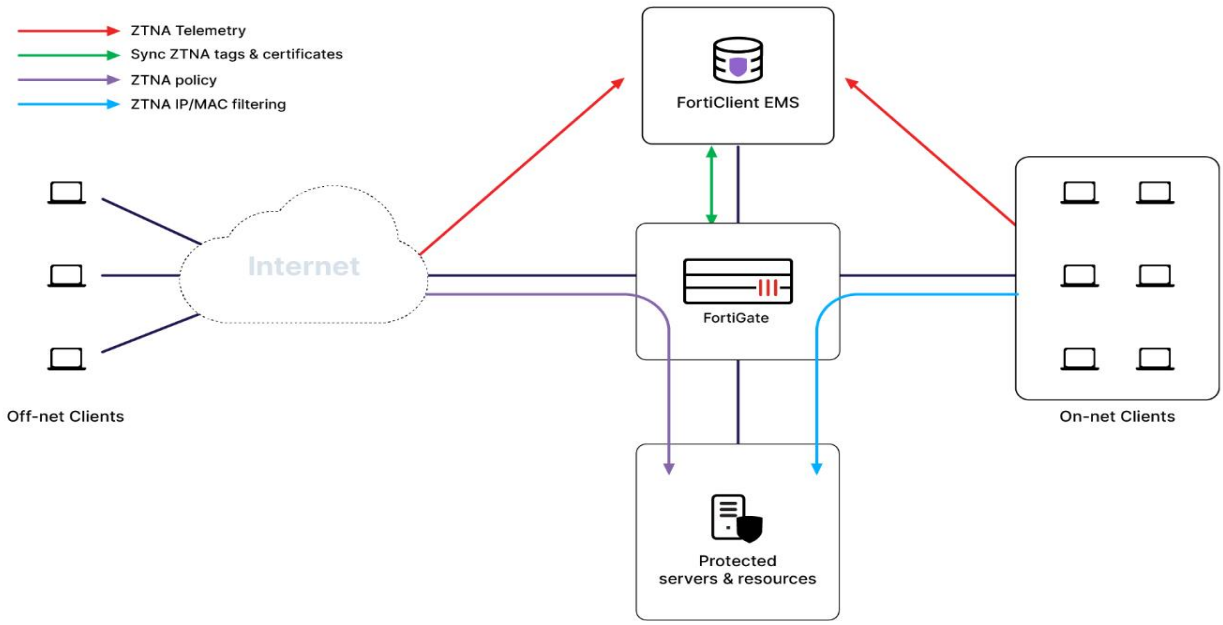

Рисунок 3.6: Ілюструє процеси телеметрії, тегування та застосування політик у контексті ZTNA. [15]

ВИСНОВКИ

У роботі розроблялись рекомендації щодо використання Endpoint Protection в інформаційній системі організації та визначається актуальність проблеми захисту кінцевих точок організації. Сьогодні існують серйозні проблеми у захисті кінцевих точок організацій від нових та дедалі складніших загроз. Спостерігається зростання ризиків для безпеки кінцевих точок організацій, які посилюються їхньою неготовністю до протидії новим загрозам за допомогою існуючих платформ безпеки кінцевих точок.

1. Проведено аналіз науково-технічної літератури з теми кваліфікаційної роботи. В результаті узагальнено сучасні підходи до безпеки, класифікацію загроз, вимоги міжнародних стандартів (зокрема NIST, ISO/IEC 27001) та практики використання рішень класу EDR у корпоративному середовищі організації.

2. Проаналізовано методи та засоби захисту кінцевих точок на основі технологій EDR. Оцінено функціональні можливості провідних платформ, таких як Microsoft Defender, CrowdStrike, SentinelOne та FortiEDR. Визначено ключові критерії вибору EDR-рішення для організації. Рішення EDR виконує функції безперервного моніторингу та збору даних з кінцевих точок для виявлення та усунення кіберзагроз у режимі реального часу. Таким чином, EDR відіграє вирішальну роль у загальній системі безпеки інформаційної системи організації.

3. Виявлення та реагування на кінцеві точки стало ключовим аспектом сучасної кібербезпеки, оскільки організації стикаються зі все більш складними кібератаками. FortiEDR — це комплексне рішення для захисту кінцевих точок, яке забезпечує виявлення загроз та реагування на них у режимі реального часу, автоматизоване реагування на інциденти та можливості цифрового розслідування.

4. Використання FortiEDR може допомогти організаціям скористатися перевагами останніх рекомендацій, забезпечуючи комплексну безпеку кінцевих точок, автоматизуючи процеси реагування на інциденти та спрощуючи впровадження найкращих практик безпеки кінцевих точок.

5. Запропоновано варіант розгортання системи FortiEDR в умовах типової

організації. Описано вимоги до IT-інфраструктури, алгоритм налаштування політик, інтеграцію з SIEM-системами та процес оперативного реагування на інциденти.

6. Розроблено практичні рекомендації щодо застосування методів і засобів захисту кінцевих точок в інформаційній системі організації. Сформульовано перелік кроків для IT-відділу та фахівців з кібербезпеки, що включає розгортання, моніторинг, підтримку та оновлення системи захисту.

7. Обґрунтовано наукову й прикладну значущість результатів дослідження. Запропоновані рекомендації можуть бути використані для підвищення рівня кіберзахисту в організаціях малого та середнього бізнесу, а також як методична основа для подальших досліджень у сфері захисту кінцевих точок.

Підсумовуючи зазначене вище можна відзначити, що правильне впровадження системи захисту кінцевих точок організації повинно сприяти ефективному захисту корпоративних інформаційних ресурсів в цілому.

ПЕРЕЛІК ПОСИЛАНЬ

1. Звіт про безпеку кінцевих точок за 2022 рік. Інсайдери кібербезпеки. URL-адреса: https://20645266.fs1.hubspotusercontent-na1.net/hubfs/20645266/CSI-2022-Endpoint-Security-Report-Adaptiva-Final-03282022%20(1).pdf. (дата звернення 02.05.2025).

2. Introducing FortiEDR | FortiEDR/XDR 7.0.0 | Fortinet Document Library. URL-адреса: https://docs.fortinet.com/document/fortiedr/7.0.0/administration-guide/354083/introducing-fortiedr. (дата звернення 02.05.2025).

3. Барретт, М. (2018), Структура покращення кібербезпеки критичної інфраструктури, версія 1.1. Структура кібербезпеки NIST, [онлайн]. URL-адреса: https://doi.org/10.6028/NIST.CSWP.04162018,https://www.nist.gov/cyberframework. (дата звернення 02.05.2025).

4. Виявлення та реагування на кінцеві точки (EDR). Огляди та рейтинги рішень. GARTNER. URL-адреса: https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions. (дата звернення 06.05.2025).

5. Серія «Захисник Microsoft для кінцевих точок» – Що таке Захисник для кінцевих точок? – Частина 1. URL-адреса: https://www.microsoft.com/en-us/security/blog/2023/03/02/microsoft-is-named-a-leader-in-the-2022-gartner-magic-quadrant-for-endpoint-protection-platforms/ . (дата звернення 06.05.2025).

6. Appendix C – ON PREMISE DEPLOYMENTS | FortiEDR/XDR 7.0.0 | Fortinet Document Library. URL-адреса: https://docs.fortinet.com/document/fortiedr/7.0.0/administration-guide/838338/appendix-c-on-premise-deployments . (дата звернення 07.05.2025)

7. FortiEDR Datasheet 04 April 2025 URL-адреса: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf (дата звернення 07.05.2025)

8. Архітектура робочого навантаження Carbon Black. VMware. URL-адреса:https://carbonblack.vmware.com/resource/carbon-black-workload-architecture#section1. (дата звернення 10.05.2025).

9. FortiEDR components | FortiEDR/XDR 6.0.0 | Fortinet Document Library. URL-адреса: https://docs.fortinet.com/document/fortiedr/6.0.0/administration-guide/970632/fortiedr-components (дата звернення 10.05.2025).

10. DATA SHEET FortiEDR™ Real-Time Endpoint Protection, Detection and Automated Response. [Онлайн]. URL-адреса: https://www.armacom.ch/fileadmin/data/files/Produkte/FortiEDR_Data-Sheet_ENG.pdf (дата звернення 10.05.2025).

11. EDR Report | Key Elements of an Effective EDR Solution [Онлайн]. URL-адреса: https://www.openedr.com/blog/edr-report/ (дата звернення 10.05.2025).

12. CrowdStrike vs Fortinet vs Microsoft vs Sophos vs Trend Micro 2025 | Gartner Peer Insights URL-адреса: https://www.gartner.com/reviews/market/endpoint-protection-platforms/compare/crowdstrike-vs-fortinet-vs-microsoft-vs-sophos-vs-trend-micro (дата звернення 10.05.2025).

13. Microsoft Defender XDR demonstrates 100% detection coverage across all cyberattack stages in the 2024 MITRE ATT&CK® Evaluations: Enterprise | Microsoft Security Blog. [Онлайн]. URL-адресаhttps://www.microsoft.com/en-us/security/blog/2024/12/11/microsoft-defender-xdr-demonstrates-100-detection-coverage-across-all-cyberattack-stages-in-the-2024-mitre-attck-evaluations-enterprise/ (дата звернення 11.05.2025).

14. Red Bull and Fortinet Join Forces to Improve Security with FortiEDR, CASE STUDY, 09.05.2024 . (дата звернення 11.05.2025).

15. ZTNA secure access | FortiGate / FortiOS 7.0.0 | Fortinet Document Library. [Онлайн]. URL-адреса: https://docs.fortinet.com/document/fortigate/7.0.0/ztna-architecture/14574/ztna-secure-access (дата звернення 12.05.2025).

16. AI-Powered Security Solutions | SentinelOne [Онлайн]. URL-адреса: https://www.sentinelone.com/platform/ai-cybersecurity/ (дата звернення 12.05.2025).

17. Що таке EDR? Протидія загрозам у кінцевих точках | Захисний комплекс Microsoft. [Онлайн]. URL-адреса: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-edr-endpoint-detection-response (дата звернення 12.05.2025).

18. Apply profiles to collection machine policies • Cortex XDR Documentation • Palo Alto Networks documentation portal URL-адреса: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Documentation/Apply-profiles-to-collection-machine-policies (дата звернення 14.05.2025).

19. Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. Pearson Education, 2019.

20. Symantec. Endpoint Protection Overview. Broadcom, 2023.

21. MITRE Corporation. EDR Evaluation Methodology. 2022. URL-адреса: https://attackevals.mitre.org/ (дата звернення 14.05.2025)

22. Palo Alto Networks. XDR vs EDR: What’s the Difference? 2023.

23. NIST SP 800-171r3. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. National Institute of Standards and Technology, 2024.

24. Ponemon institute 2022 report. Managing risks & costs at the edge.

25. Absolute is strengthening endpoint resilience for its customers URL-адреса: https://www.helpnetsecurity.com/2020/02/03/absolute-resilience-persistence/ (дата звернення 16.05.2025).

26. NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide URL-адреса: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (дата звернення 16.05.2025).

27. What is Defense in Depth? Defined and Explained | Fortinet URL-адреса: https://www.fortinet.com/resources/cyberglossary/defense-in-depth (дата звернення 16.05.2025).

28. Endpoint security market size 2024-2028| Statista URL-адреса: https://www.statista.com/statistics/497965/endpoint-security-market/ (дата звернення 16.05.2025).

29. FortiEDR Installation and Administration Guide V4.1 | PDF | Malware | Ransomware URL-адреса: https://www.scribd.com/document/633558257/FortiEDR-Installation-and-Administration-Guide-V4-

1#:~:text=%E2%80%A2%20DEPLOYMENT%20MODE%3A%20Specifies%20whether,Cloud (дата звернення 16.05.2025).

30. What is Cybersecurity? | Types, Threats & Best Practices | Fortinet URL-адреса: https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity (дата звернення 16.05.2025).

31. Optimize Endpoint Security with EDR - Palo Alto Networks URL-адреса: https://www.paloaltonetworks.com/cortex/endpoint-detection-and-response (дата звернення 25.05.2025).

32. Secure the Endpoint, Stop the Breach | CrowdStrike Endpoint Security URL-адреса: https://www.crowdstrike.com/en-us/platform/endpoint-security/ (дата звернення 26.05.2025).

33. MITRE ATT&CK® | ATT&CK Matrix for Enterprise URL-адреса: https://attack.mitre.org/ (дата звернення 26.05.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

Презентація