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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Рекомендації щодо захисту кінцевих точок інформаційної системи організації на базі OpenEDR»

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

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

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

_____ Андрій БАЛАЦЬКИЙ
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
БАЛАЦЬКИЙ Андрій
(прізвище, ім'я)

Керівник д. т. н., професор, Гайдур Г.І.
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ВСТУП

Актуальність дослідження. Захист кінцевих точок відіграє ключову роль у кібербезпеці організації. Ці пристрої зберігають і обробляють важливу інформацію, тому їх компрометація може призвести до витоку конфіденційних даних. Вони також є однією з основних цілей для зловмисників, які можуть використовувати вразливості кінцевих точок для проникнення в корпоративну мережу. Крім того, безперебійна робота цих пристроїв необхідна для стабільного функціонування бізнес-процесів, адже атаки на них можуть спричинити фінансові збитки. В умовах віддаленої роботи забезпечення захисту кінцевих точок стає ще більш актуальним, оскільки пристрої все частіше працюють за межами захищеної корпоративної інфраструктури. Використання OpenEDR дозволяє ефективно виявляти та знешкоджувати загрози, забезпечуючи надійний захист кінцевих точок.

Рішення для виявлення та реагування на загрози на кінцевих точках (EDR) є важливим інструментом забезпечення кібербезпеки організації. Вони дозволяють відстежувати активність пристроїв у режимі реального часу, аналізувати поведінкові патерни та виявляти підозрілі дії, що можуть свідчити про загрози. Завдяки таким системам організації отримують детальну видимість подій на кінцевих точках, що дає змогу оперативно реагувати на потенційні атаки. Функціонал EDR передбачає виявлення аномалій, ізоляцію заражених пристроїв, глибокий аналіз інцидентів і впровадження ефективних заходів для усунення загроз.

Системи EDR здійснюють моніторинг активності процесів і додатків на кінцевих пристроях, аналізуючи їхню поведінку для виявлення аномалій. Будь-які відхилення від типових сценаріїв роботи можуть сигналізувати про можливу загрозу. У разі виникнення інциденту платформа надає детальний аналіз подій, що передували загрозі, допомагаючи швидко виявити причини та джерела атаки. Якщо виявлено шкідливу активність, EDR може автоматично ізолювати уражений пристрій від мережі, запобігаючи поширенню загрози та мінімізуючи потенційні наслідки.

Технології EDR допомагають організаціям впроваджувати політики безпеки на кінцевих пристроях, забезпечуючи їх відповідність встановленим стандартам та вимогам конфігурації. Інтеграція механізмів захисту кінцевих точок із такими рішеннями дозволяє створити ефективний бар'єр проти різноманітних кіберзагроз та значно підвищити загальний рівень безпеки.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження методів та засобів захисту кінцевих точок організації на базі OpenEDR.

Об'єкт дослідження – захист кінцевих точок організації.

Предмет дослідження – методи та засоби захисту кінцевих точок організації на базі OpenEDR.

Мета роботи розробити систему на базі рішення OpenEDR та надати рекомендації щодо застосування методів та засобів захисту кінцевих точок організації.

Наукові завдання:

дослідити сутність проблеми захисту кінцевих точок організації;

проаналізувати основні підходи до захисту кінцевих точок організації;

проаналізувати існуючі рішення із захисту кінцевих точок організації;

проаналізувати методи та засоби захисту кінцевих точок організації на базі OpenEDR;

запропонувати рішення для захисту кінцевих точок організації на базі OpenEDR;

розробити рекомендацій щодо застосування методів та засобів захисту кінцевих точок організації.

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

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів та засобів захисту кінцевих точок організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

1.1. Аналіз проблеми захисту кінцевих точок організації

Проблема захисту кінцевих точок є критично важливим аспектом забезпечення кібербезпеки організації. Кінцеві пристрої, такі як персональні комп'ютери, ноутбуки, мобільні пристрої, сервери та IoT-пристрої, безпосередньо взаємодіють із корпоративною мережею та можуть бути використані зловмисниками для компрометації інформаційних активів.

Згідно зі звітом IBM X-Force Threat Intelligence Index 2024, компрометація дійсних облікових записів стала найпоширенішим вектором початкового доступу, складаючи (30%) всіх кіберінцидентів. Це вперше, коли зловмисники настільки часто використовують викрадені або придбані облікові дані для отримання доступу до корпоративних мереж. Фішинг, що також становить (30%) атак, залишається критичною загрозою, хоча його загальний обсяг знизився на (44%) у порівнянні з 2022 роком (рисунок 1.1) [1].

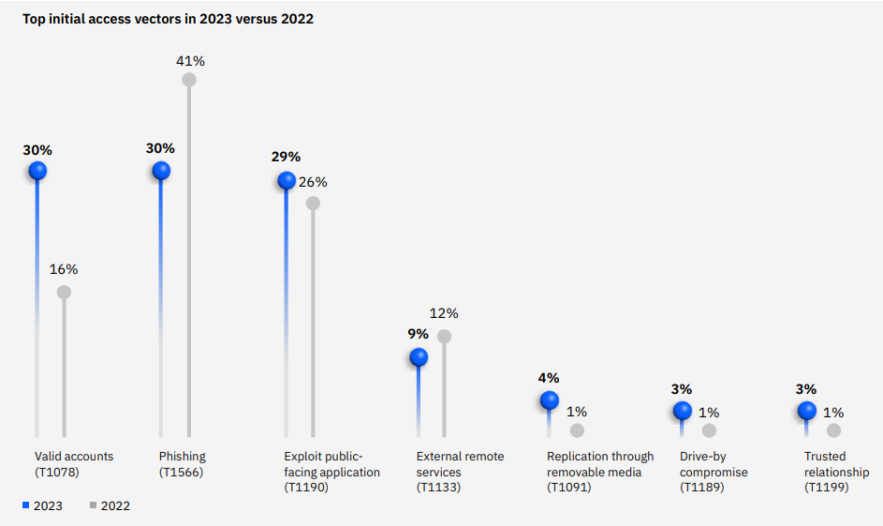

Рис. 1.1. Основні вектори початкового доступу у 2023 році порівняно з 2022 роком [1]

Крім того, інформаційно-крадійські шкідливі програми (infostealers) стали

серйозною проблемою, адже їх використання зросло на (266%) у порівнянні з попереднім роком це пок. Це свідчить про зміну тактики зловмисників, які дедалі більше покладаються на викрадення облікових даних замість традиційних методів злому (рисунок 1.2) [1].

Рис. 1.2. Найбільш впливові загрози кібербезпеці для організацій в порівняні між 2023 та 2022 роком [1]

Сучасні загрози для кінцевих точок включають зловмисне програмне забезпечення, фішинг, атаки на вразливості, витік даних та цільові атаки типу APT. Наприклад, зловмисне програмне забезпечення може впроваджуватися через заражені електронні листи або шкідливі веб-сайти, фішингові атаки спрямовані на отримання облікових даних користувачів, а експлойти можуть використовувати вразливості програмного забезпечення для отримання несанкціонованого доступу.

Дослідження Verizon Data Breach Investigations Report (DBIR) 2024 свідчить, що у (68%) випадків порушення безпеки пов’язані з людським фактором, включаючи фішингові атаки, використання слабких паролів та несанкціоноване встановлення програмного забезпечення. У 2024 році було зафіксовано збільшення атак програм-вимагачів втричі (зростання на 180%) порівняно з попереднім роком, що підкреслює критичну необхідність впровадження ефективних засобів захисту кінцевих точок (рисунок 1.3) [2].

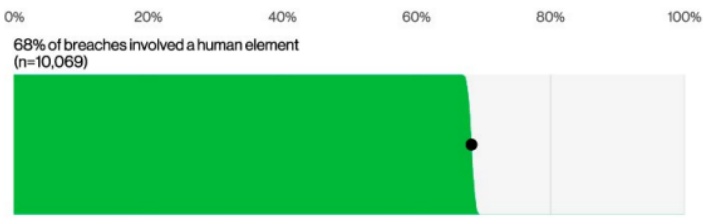

Рис. 1.3. Випадки порушення безпеки пов’язані з людським фактором [2]

Однією з ефективних методик аналізу загроз є порівняння типів атак та їх впливу на організацію. Основні типи атак та їх наслідки наведено в таблиці 1.1.

Таблиця 1.1.

Основні типи атак та їх наслідки

Тип атаки	Метод реалізації	Потенційні наслідки
Фішинг	Обман користувачів для розкриття даних	Викрадення облікових даних, злом аккаунтів
Програми-вимагачі (Ransomware)	Шифрування файлів із вимогою викупу	Втрата доступу до критичних даних
Використання вразливостей	Експлуатація невиправлених вразливостей	Несанкціонований доступ до систем
Інсайдерські загрози	Дії співробітників (навмисні або ненавмисні)	Витік конфіденційної інформації

Для ефективного захисту організації необхідний комплексний підхід, який передбачає застосування багаторівневої безпеки, впровадження передових технологій моніторингу та аналізу, а також активне управління ризиками. Одним з найефективніших рішень є впровадження EDR-систем, які забезпечують проактивний моніторинг та швидке реагування на загрози. Впровадження таких технологій дозволяє значно зменшити ризики компрометації кінцевих пристроїв і покращити загальний рівень кібербезпеки організації.

1.2. Аналіз підходів до захисту кінцевих точок організації

Захист кінцевих точок організації є ключовим елементом забезпечення інформаційної безпеки, оскільки саме ці пристрої часто стають мішенню для кібератак. Для їхнього захисту застосовуються різні підходи, які можна класифікувати на традиційні, сучасні та комплексні стратегії.

Традиційні підходи до захисту кінцевих точок базуються на використанні антивірусного програмного забезпечення та брандмауерів. Антивірусні програми здійснюють сканування файлів та процесів на наявність відомих шкідливих

сигнатур, тоді як брандмауери контролюють мережевий трафік, запобігаючи несанкціонованому доступу. Проте ці методи мають обмежену ефективність проти новітніх загроз, таких як атаки нульового дня або складні цільові атаки, оскільки вони покладаються на відомі сигнатури та правила. Традиційне керування кінцевими точками насамперед наголошує на ручному розгортанні програмного забезпечення, виправлень і оновлень безпеки. Ці методи, як правило, трудомісткі, схильні до помилок і неефективні, особливо для великих організацій з різними типами пристроїв. Крім того, вони стикаються з проблемами швидкого впровадження інновацій, щоб задовольнити вимоги сучасності, коли співробітники використовують поєднання особистих і корпоративних пристроїв [3].

Сучасні підходи включають використання систем виявлення та реагування на кінцевих точках (EDR). EDR-системи, такі як OpenEDR, забезпечують постійний моніторинг та аналіз активності на кінцевих точках, використовуючи поведінковий аналіз та машинне навчання для виявлення аномалій та потенційних загроз. Вони дозволяють швидко реагувати на інциденти та проводити детальний аналіз атак. Основні функції сучасного підходу [3]:

створює єдину контрольну точку для адміністраторів, щоб керувати всіма кінцевими точками, незалежно від їх типу чи розташування;

завдяки використанню автоматизованих процедур зменшується ручна праця;

включає проактивне виявлення загроз і реагування на них, автоматизоване керування виправленнями та шифрування для посилення безпеки;

підтримує портали самообслуговування, дистанційне усунення несправностей і сприяє ефективному розповсюдженню програмного забезпечення;

дозволяє компаніям плавно розширюватись, дозволяючи швидко включати нові кінцеві точки у свою діяльність.

Комплексні підходи до захисту кінцевих точок поєднують різні стратегії та технології для створення багаторівневої системи безпеки. Це може включати інтеграцію EDR з іншими засобами захисту, такими як системи виявлення вторгнень (IDS), засоби управління інформацією та подіями безпеки (SIEM), а також впровадження політик нульової довіри (ZT). Такий підхід передбачає

впровадження різноманітних заходів безпеки на різних рівнях мережі для створення більш стійкого механізму захисту. Штучний інтелект і машинне навчання необхідні для аналізу великих наборів даних для виявлення закономірностей, які можуть вказувати на потенційні загрози, що дозволяє організаціям завчасно випереджати дії кіберзлочинців. Чітко визначений план реагування на інциденти гарантує, що організації зможуть швидко й ефективно стримувати та усувати порушення безпеки, скорочуючи час простою та захищаючи конфіденційні дані [4].

Порівняння різних підходів до захисту кінцевих точок наведено в таблиці 1.2.

Таблиця 1.2

Підходи до захисту кінцевих точок

Підхід	Опис	Переваги	Недоліки
Традиційний	Використання антивірусів та брандмауерів для захисту від відомих загроз.	Простота впровадження, низька вартість.	Неефективність проти нових та складних атак, залежність від оновлення сигнатур.
Сучасний	Постійний моніторинг та аналіз поведінки на кінцевих точках з використанням машинного навчання.	Постійний моніторинг та аналіз поведінки на кінцевих точках з використанням машинного навчання.	Високі вимоги до ресурсів, необхідність кваліфікованого персоналу.
Комплексний	Інтеграція різних засобів захисту та впровадження політик нульової довіри.	Багаторівневий захист, адаптивність до нових загроз.	Складність впровадження, значні витрати на підтримку.

1.3. Аналіз існуючих рішень із захисту кінцевих точок організації

Сучасні рішення для захисту кінцевих точок еволюціонували від традиційних антивірусних програм до комплексних платформ, які поєднують різні технології для забезпечення багаторівневого захисту.

Традиційні антивірусні програми зосереджені на виявленні та блокуванні відомих шкідливих програм за допомогою сигнатурного аналізу. Хоча вони ефективні проти відомих загроз, їхня здатність протистояти новим, складним атакам обмежена. Тому виникла потреба в більш просунутих рішеннях.

Платформи захисту кінцевих точок (EPP) інтегрують антивірусні засоби з додатковими функціями, такими як брандмауери, контроль додатків та шифрування даних. Вони спрямовані на запобігання інфікуванню та забезпечують базовий рівень безпеки для кінцевих пристроїв. EPP часто можна описати як традиційне антивірусне рішення. Хоча розгортання антивірусного рішення покращить вашу безпеку на першій лінії, воно не захищає ваші кінцеві точки від більш складних загроз, які можуть знайти інший шлях до вашої мережі. Рішення безпеки кінцевої точки повинні мати можливості платформи захисту кінцевої точки, але вони також повинні мати можливості рішення для виявлення кінцевої точки та реагування (EDR) [5].

Системи виявлення та реагування на кінцевих точках (EDR) забезпечують постійний моніторинг активності на кінцевих точках, збір та аналіз даних для виявлення підозрілої поведінки та швидкого реагування на інциденти. EDR-рішення дозволяють не лише виявляти відомі загрози, але й ідентифікувати нові, раніше невідомі атаки. Прикладом такого рішення є OpenEDR, яке надає можливості для ефективного реагування на складні кіберзагрози, захищаючи дані та забезпечуючи безперервність бізнес-процесів. OpenEDR розроблена для негайного реагування, мінімізуючи час простою та зменшуючи навантаження на організації. У момент виявлення зловмисної активності OpenEDR автоматично ізолює уражену кінцеву точку від мережі. Це запобігає поширенню загрози та забезпечує безпеку інших систем під час вирішення проблеми. Використовуючи розширений аналіз загроз, OpenEDR блокує відомі та невідомі загрози, зокрема програми-вимагачі, зловмисне програмне забезпечення та експлойти нульового дня (Zero day), перш ніж вони можуть завдати шкоди. Автоматизовані відповіді забезпечують швидке стримування навіть у неробочий час або коли організації перевантажені [6].

Розширене виявлення та реагування (XDR) розширює концепцію EDR, об'єднуючи дані з різних джерел, включаючи мережевий трафік, сервери, хмарні середовища та електронну пошту. XDR надає централізовану видимість та контроль над усіма компонентами IT-інфраструктури, що дозволяє більш ефективно виявляти та реагувати на складні атаки. Наприклад, рішення від CrowdStrike забезпечує комплексний захист кінцевих точок, дозволяючи ефективно протидіяти витоку конфіденційної інформації та іншим кіберзагрозам. В основі XDR лежить інтеграція різних продуктів безпеки, які працюють синхронно для забезпечення глибокого аналізу та ефективного реагування на кіберзагрози в реальному часі. Ключові особливості та можливості [7]:

XDR використовує алгоритми машинного навчання для аналізу поведінки на кінцевих точках та в мережі, вміючи розпізнавати навіть найскладніші патерни атак, які можуть залишитися непоміченими традиційними системами виявлення;

платформа забезпечує швидке та автоматизоване реагування на виявлені загрози, здатна ізолювати інфіковані системи, виконувати скрипти рекомендації та навіть відновлювати операції без необхідності втручання людини;

збираючи дані з різних джерел, включно з електронною поштою, мережами та кінцевими точками, XDR надає комплексний огляд загроз, що дозволяє кібербезпековим командам бачити повну картину атаки та краще розуміти, як загрози проникають і поширюються у системах;

CrowdStrike XDR може масштабуватися відповідно до потреб бізнесу, забезпечуючи ефективний захист як для малого бізнесу, так і для великих корпорацій зі складними мережевими інфраструктурами;

інструменти звітності та аудиту, інтегровані в XDR, спрощують дотримання нормативних та галузевих вимог, забезпечуючи необхідну прозорість та контроль для відповідності стандартам безпеки.

Підхід «Нульова довіра» (ZT) базується на принципі, що жоден користувач або пристрій не повинні автоматично довірятися, навіть якщо вони знаходяться всередині корпоративної мережі. Кожен запит на доступ перевіряється, аутентифікується та авторизується, що особливо важливо для захисту кінцевих

точок, оскільки користувачі часто підключаються з різних пристроїв та локацій. Впровадження політик нульової довіри допомагає значно зменшити ризик несанкціонованого доступу до конфіденційних даних або систем [8].

Для кращого розуміння відмінностей між цими рішеннями та їх ефективності у захисті кінцевих точок організації наведено таблицю 1.3.

Таблиця 1.3.

Відмінності між рішеннями

Критерій	EPP	EDR	XDR	ZT
Основна функція	Виявлення та запобігання шкідливим програмам	Виявлення та реагування на загрози в режимі реального часу	Об'єднання даних з різних джерел для розширеного аналізу загроз	Доступ на основі принципу «не довіряй, перевіряй»
Метод виявлення загроз	Сигнатурний аналіз, евристика, брандмауери	Аналіз поведінки, телеметрія, машинне навчання	Кореляція даних з різних джерел (кінцеві точки, мережа, хмара)	Контроль доступу та багатофакторна автентифікація (MFA)
Реагування на загрози	Переважно запобігання (блокування загроз)	Виявлення загроз і їх нейтралізація вручну або автоматично	Автоматизоване реагування на інциденти, аналіз усієї екосистеми	Відмовлення у доступі до ресурсів без перевірки, мікросегментація мережі
Контроль доступу	Мінімальний	Частковий (залежить від інтеграції	Централізований моніторинг доступу та діяльності користувачів	Жорсткий контроль доступу, обмеження привілеїв користувачів
Покриття загроз	Відомі загрози (віруси, трояни, руткіти)	Невідомі загрози, атаки нульового дня	Комплексний аналіз загроз у різних середовищах	Внутрішні та зовнішні загрози, соціальна інженерія
Моніторинг у режимі реального часу	Ні	Так	Так (інтегрований у всю IT-інфраструктуру)	Так, постійний контроль користувачів і пристроїв

Продовження табл. 1.3

Відмінності між рішеннями

Критерій	EPP	EDR	XDR	ZT
Автоматизація	Обмежена (оновлення сигнатур)	Часткова (автоматичне виявлення загроз)	Висока (автоматизоване виявлення та реагування)	Політики автоматичного контролю доступу
Призначення	Базовий рівень кібербезпеки	Розширений рівень безпеки для аналізу загроз	Комплексний аналіз і управління загрозами	Контроль доступу та мінімізація ризиків компрометації
Приклад рішень	Symantec Endpoint Protection, McAfee, Kaspersky	CrowdStrike Falcon, OpenEDR, SentinelOne	Microsoft Defender XDR, Palo Alto Cortex XDR, CrowdStrike	Cisco Zero Trust, Microsoft Zero Trust, Okta Identity Cloud

Вибір відповідного рішення для захисту кінцевих точок залежить від специфіки організації, її розміру, галузі та рівня прийнятного ризику. Важливо враховувати такі фактори, як масштабованість, простота інтеграції з існуючою інфраструктурою, підтримка виявлення на основі поведінки, моніторинг у режимі реального часу та функції автоматизації. Поєднання різних підходів та технологій дозволяє створити багаторівневу систему захисту, здатну ефективно протидіяти сучасним кіберзагрозам.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА БАЗІ OPENEDR

2.1. Архітектура та компоненти рішення OpenEDR

Архітектура OpenEDR базується на модульному підході, що дозволяє гнучко адаптувати систему для різних сценаріїв кібербезпеки. Це рішення забезпечує глибокий аналіз подій на кінцевих точках, виявлення загроз та їх нейтралізацію. OpenEDR складається з кількох основних компонентів, кожен з яких виконує критично важливі функції у процесі моніторингу та захисту (рисунок 2.1) [9].

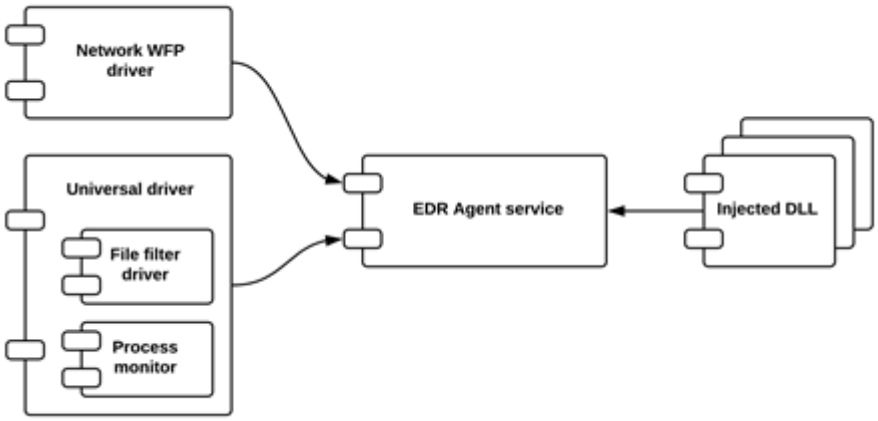

Рис. 2.1. Архітектурна схема взаємодії основних компонентів агента OpenEDR [9]

Системний монітор (System Monitor) є центральним компонентом рішення, який відповідає за збір телеметричних даних з кінцевої точки. Він безперервно відстежує активність процесів, файлові операції, мережевий трафік та зміни в реєстрі. Завдяки цьому OpenEDR здатний виявляти аномальні дії, які можуть свідчити про компрометацію системи. Наприклад, якщо система виявляє запуск процесу, що імітує легітимне ПЗ, але демонструє поведінку, характерну для загроз (наприклад, виконує приховане з'єднання з зовнішнім сервером), це може вказувати на атаку [10].

На рівні файлової системи працює міні-фільтр файлової системи (File-system

Mini-filter), який перехоплює запити на зміну файлів. Це дозволяє контролювати спроби шифрування, видалення або модифікації файлів з боку потенційно шкідливих програм. Особливо важливою ця функція є для захисту від програм-здирників (ransomware), які намагаються зашифрувати дані користувачів. У разі виявлення такої активності OpenEDR може заблокувати процес, який ініціює шифрування, та сповістити адміністратора про потенційну загрозу [10].

Для аналізу активності програмного забезпечення використовується компонент моніторингу процесів (Low-level Process Monitoring Component). Він контролює запуск, завершення та модифікацію процесів, дозволяючи виявляти загрози на основі поведінкового аналізу. Це означає, що навіть якщо шкідливе ПЗ використовує унікальні методи обходу традиційних сигнатурних засобів виявлення, OpenEDR може розпізнати його активність через аналіз дій, таких як спроба експлуатації вразливостей або виконання коду без дозволу [10].

Ще одним важливим елементом є моніторинг реєстру (Low-level Registry Monitoring Component), який відстежує критичні зміни у реєстрі Windows. Оскільки багато видів шкідливого ПЗ змінюють реєстр для отримання можливості автозапуску або внесення змін у параметри безпеки системи, цей компонент є необхідним для запобігання подібним атакам. Наприклад, якщо виявлено, що новий процес намагається додати себе до автозапуску Windows або змінити конфігурацію системних оновлень, OpenEDR може це миттєво заблокувати [10].

Аналіз мережевого трафіку здійснюється мережевим монітором (Network Monitor), який перевіряє як вхідні, так і вихідні з'єднання кінцевої точки. Він допомагає виявляти підозрілі запити, такі як спроби зв’язку з командно-контрольним сервером (C2), що часто використовується у кібератаках для керування зараженими пристроями. Якщо OpenEDR зафіксує спробу встановлення підозрілого з’єднання, система може автоматично заблокувати його та повідомити про загрозу [10].

Ключову роль у стабільності та безпеці рішення відіграє механізм самозахисту (Self-protection Provider). Він запобігає спробам зловмисного ПЗ або користувача вимкнути або змінити роботу OpenEDR. Це важлива функція, оскільки

сучасні загрози часто намагаються деактивувати засоби безпеки перед тим, як виконати шкідливі дії. Завдяки цьому OpenEDR продовжує функціонувати навіть у разі спроб його компрометації [10].

Архітектура OpenEDR забезпечує комплексний підхід до захисту кінцевих точок, об’єднуючи моніторинг системних подій, аналіз поведінки процесів, контроль мережевого трафіку та механізми самозахисту. Це дозволяє системі ефективно виявляти, аналізувати та блокувати загрози, що робить її цінним інструментом у забезпеченні кібербезпеки організацій.

2.2. Призначення та основні функції компонентів OpenEDR

OpenEDR є потужним інструментом для забезпечення безпеки кінцевих точок, що здійснює всебічний моніторинг різних аспектів системи, включаючи процеси, файлову систему, мережеву активність та системні зміни. Ці компоненти дозволяють зібрати всі необхідні дані для оперативного виявлення та реагування на потенційні загрози.

Моніторинг процесів є одним із основних аспектів функціонування OpenEDR. Він дозволяє стежити за всіма активними процесами на пристрої в реальному часі. Це включає запуск нових процесів, їх виконання та завершення, а також взаємодію процесів з іншими елементами системи. Процеси можуть бути інструментом для запуску шкідливого програмного забезпечення, тому важливо виявляти аномальні або небажані процеси, що можуть вказувати на зловмисну активність. Наприклад, програма, яка намагається змінити важливі системні файли або завантажити інші шкідливі програми, буде зафіксована за допомогою цього моніторингу. OpenEDR здатен не лише виявляти такі загрози, але й автоматично реагувати, блокуючи підозрілі процеси або обмежуючи їх діяльність.

Файлова система є ще одним важливим елементом, який моніторить OpenEDR. Це включає всі операції з файлами: створення, модифікацію, переміщення та видалення. Система контролює всі зміни в реальному часі, що дозволяє виявляти підозрілі активності, такі як зміну або видалення важливих

системних файлів, що може бути частиною атаки з використанням програм-вимагачів або інших видів шкідливого ПО. Наприклад, якщо зловмисник намагається змінити файли конфігурації або викрасти дані, OpenEDR зафіксує ці дії і негайно повідомить користувача або адміністратора. Крім того, система може запобігти доступу до цих файлів або заблокувати зловмисні програми, які намагаються їх модифікувати.

Моніторинг мережевої активності також є невід'ємною частиною роботи OpenEDR. Він аналізує весь трафік, що проходить через мережу, виявляючи потенційно небезпечні або підозрілі з'єднання. Наприклад, якщо комп'ютер починає передавати великі обсяги даних до невідомого зовнішнього ресурсу або здійснює підозрілі запити, це може вказувати на спроби викрадення даних або з'єднання з командно-керуючим сервером, що контролює шкідливе програмне забезпечення. OpenEDR також здатен виявляти атаки типу «розподілене відмовлення в обслуговуванні» (DDoS) або аномальний трафік, що виходить за межі нормальних шаблонів поведінки в мережі. Такі функції дозволяють вчасно виявляти та блокувати шкідливу активність, навіть до того, як вона може завдати шкоди системі.

Моніторинг системних змін включає відстеження змін у реєстрі Windows, конфігураціях системи та драйверах. Зловмисники часто намагаються змінювати ці налаштування, щоб забезпечити безперешкодне функціонування свого програмного забезпечення або отримати доступ до привілейованих прав користувача. Наприклад, зміни в реєстрі можуть використовуватись для запуску шкідливих програм при кожному завантаженні системи або для відключення засобів безпеки. OpenEDR постійно відстежує ці зміни та повідомляє про будь-які підозрілі дії. Це дає змогу зупинити загрози ще на етапі їх ініціації, запобігаючи серйозним наслідкам.

Таким чином, OpenEDR забезпечує всебічний контроль над системою, обробляючи дані з різних джерел та формуючи цілісну картину її стану в реальному часі. Це дозволяє не лише своєчасно виявляти загрози, а й оперативно реагувати на них, що забезпечує безпеку всієї інфраструктури. Для кращого розуміння взаємодії

функцій компонентів OpenEDR можна звернутися до візуалізації (рисунок 1.4) [11].

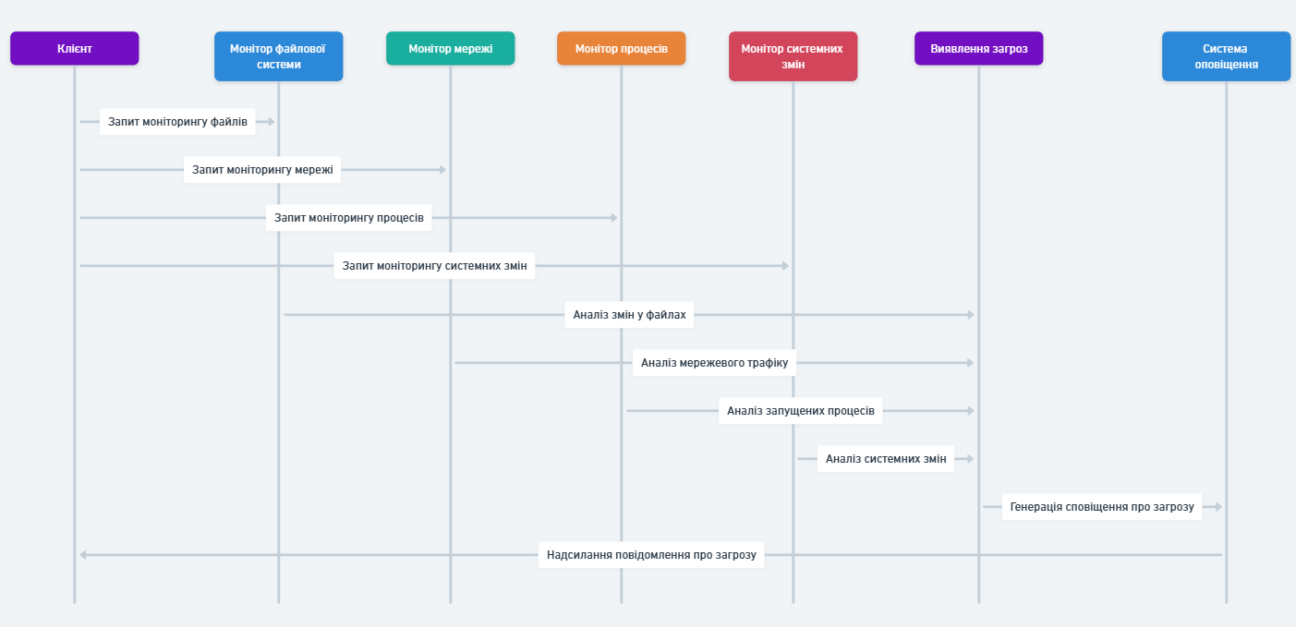

Рис. 2.2. Візуалізації взаємодії функцій компонентів OpenEDR [11]

2.3. Процеси функціонування рішення OpenEDR

На початковому етапі OpenEDR здійснює безперервний збір телеметричних даних з кінцевих пристроїв. Цей процес включає відстеження активності процесів, змін у файловій системі, доступу до реєстру та мережевої активності. Компонент Process Monitor відповідає за моніторинг процесів, використовуючи Injected DLL, яка впроваджується в кожен новий процес для перехоплення викликів API. Завантаження цієї бібліотеки здійснюється драйвером Loader for Injected DLL. Паралельно, System Monitor використовує File-system mini-filter для перехоплення запитів до файлової системи, а також компоненти для низькорівневого моніторингу процесів та реєстру, що дозволяє фіксувати створення або завершення процесів та зміни в реєстрі. Результати роботи цих компонентів формуються у вигляді лог-файлів, які містять детальну інформацію про активність системи. Логування підтримує ротацію файлів за різними критеріями, такими як розмір, час створення або запуски екземплярів процесу [10], як на рис. 2.3. Ці лог-файли надсилаються до центрального аналізатора, де відбувається подальша кореляція подій і виявлення потенційних загроз у режимі реального часу.

```
20181024-145504.254 0a24 [APPLICAT] [INF] Application started
20181024-145504.284 0a24 [APPLICAT] [INF] Config app.cfg is loaded
20181024-145505.254 0a24 [CONFIG..] [WRN] Section 'services' is not found
20181024-145504.284 0b48 [INJECTOR] [INF] New control thread is started
20181024-145614.254 0b48 [INJECTOR] [ERR] 0x0000A428 - Access denied
                                          Can't load driver inject.sys
                                          Call trace:
                                          -> driver.cpp:255 (WinAPI exception: 0x80040822 - Privileged
operation)
                                             inject.cpp:295
                                             main.cpp:28
20181024-145504.254 0a24 [APP.....] [INF] Application finished
```

Рис. 2.3. Приклад логування (лог-файлу) OpenEDR [10]

Важливим аспектом функціонування OpenEDR є забезпечення цілісності власних компонентів та конфігурації. Компонент Self-protection provider запобігає несанкціонованим змінам або видаленню критичних файлів та налаштувань системи. Це гарантує, що зловмисники не зможуть відключити або обійти механізми захисту, забезпечуючи стабільну роботу OpenEDR навіть під час активних атак [12].

Контроль за мережевими з'єднаннями здійснюється через компонент Network monitor, який аналізує вхідний та вихідний трафік на предмет підозрілої активності. Це включає виявлення незвичних з'єднань, спроб встановлення зв'язку з відомими зловмисними доменами або передачу великого обсягу даних, що може свідчити про витік інформації. Завдяки цьому компоненту, OpenEDR може оперативно реагувати на мережеві загрози, блокуючи або ізолюючи підозрілі з'єднання.

Зібрані телеметричні дані передаються до центрального сервісу Service, який ініціалізує та координує роботу інших компонентів для глибокого аналізу та реагування на виявлені загрози. Core Library надає базову функціональність та абстракцію операційної системи, спрощуючи взаємодію між компонентами та обробку даних. Ця бібліотека забезпечує незалежність від конкретної операційної системи, що дозволяє OpenEDR бути кросплатформеним рішенням [10], як на рис. 2.4. Крім того, Core Library використовує універсальне кодування UTF-8 для зберігання рядкових даних, що сприяє сумісності між різними платформами та оптимізує обробку текстової інформації.

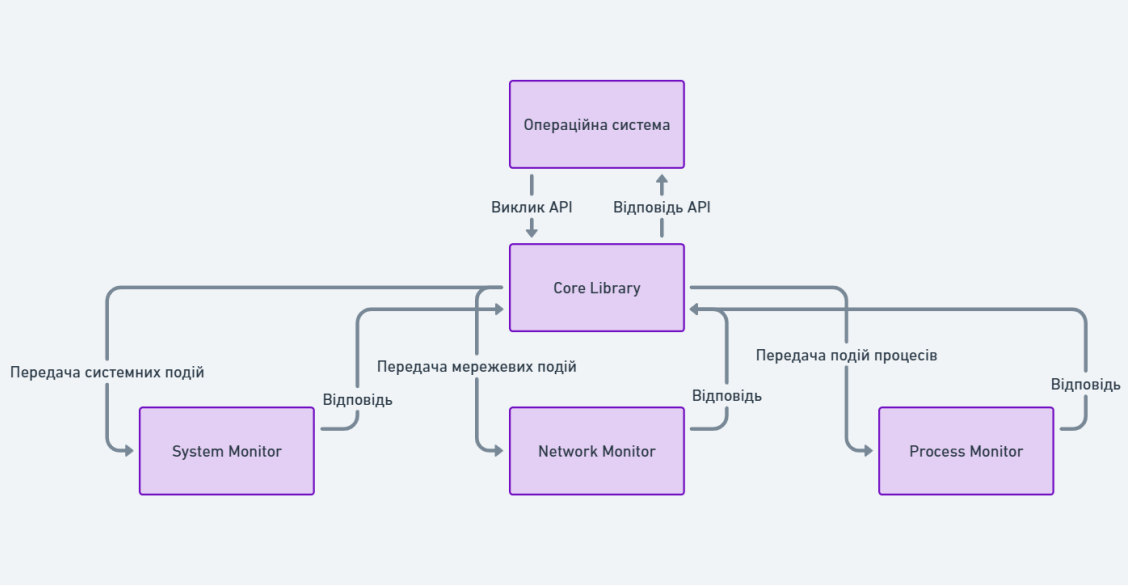

Рис. 2.4. Взаємодіє Core Library з іншими компонентами OpenEDR [11]

Після аналізу зібраних даних система визначає потенційні загрози та класифікує їх за рівнем ризику. У разі виявлення високоризикових загроз, OpenEDR може автоматично виконувати дії для їх нейтралізації, такі як ізоляція зараженого пристрою, завершення шкідливих процесів або блокування підозрілих мережевих з'єднань. Це забезпечує оперативне реагування на інциденти без необхідності втручання адміністратора, що особливо важливо для мінімізації потенційної шкоди від атак [13].

OpenEDR зберігає історичні дані про події та інциденти, що дозволяє проводити ретроспективний аналіз та виявляти довгострокові тенденції або повторювані патерни атак. Це сприяє покращенню стратегій захисту та адаптації до нових видів загроз. Крім того, збережені дані можуть бути використані для навчання персоналу та підвищення обізнаності про актуальні кіберзагрози.

Завдяки інтеграції цих процесів, OpenEDR забезпечує комплексний підхід до кібербезпеки, поєднуючи безперервний моніторинг, глибокий аналіз та автоматизоване реагування на загрози. Це дозволяє організаціям ефективно захищати свої інформаційні системи від сучасних кіберзагроз та мінімізувати потенційні збитки від атак. Доказом ефективності цього підходу є детальне відображення процесів та інцидентів у системі моніторингу OpenEDR, як показано на рис. 2.5.

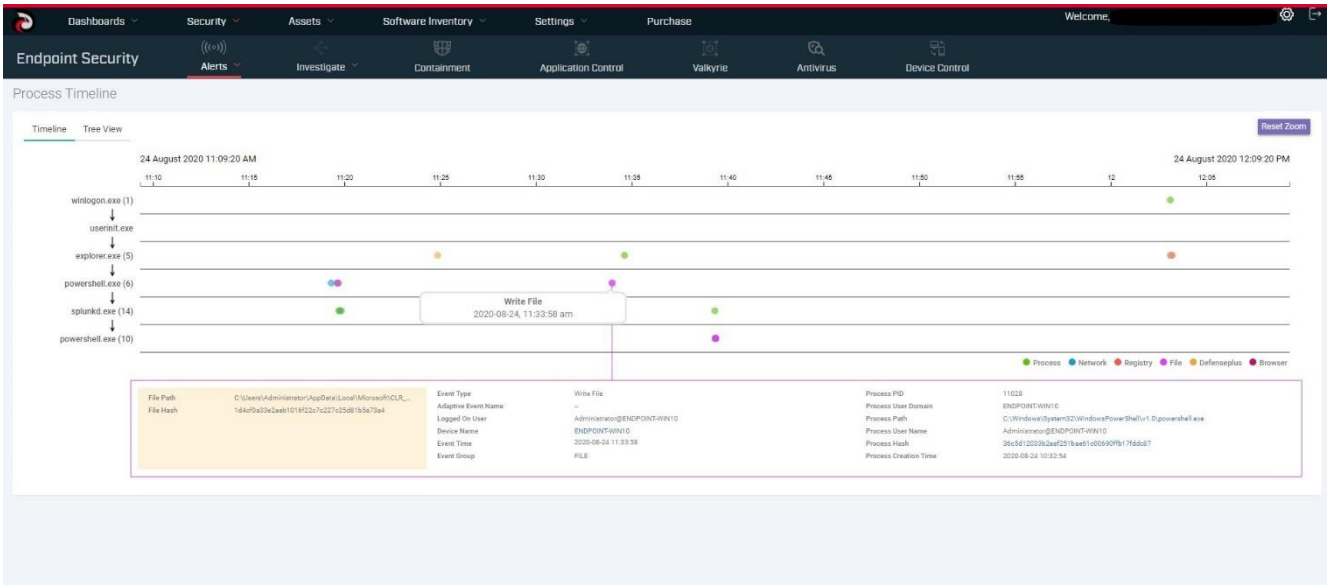

Рис. 2.5. Візуалізація таймлайну процесів [9]

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА БАЗІ OPENEDR

3.1. Реалізація системи захисту кінцевих точок організації з використанням OpenEDR

Для побудови системи захисту кінцевих точок використовується OpenEDR – відкрите рішення EDR (рисунок 3.1) [6].

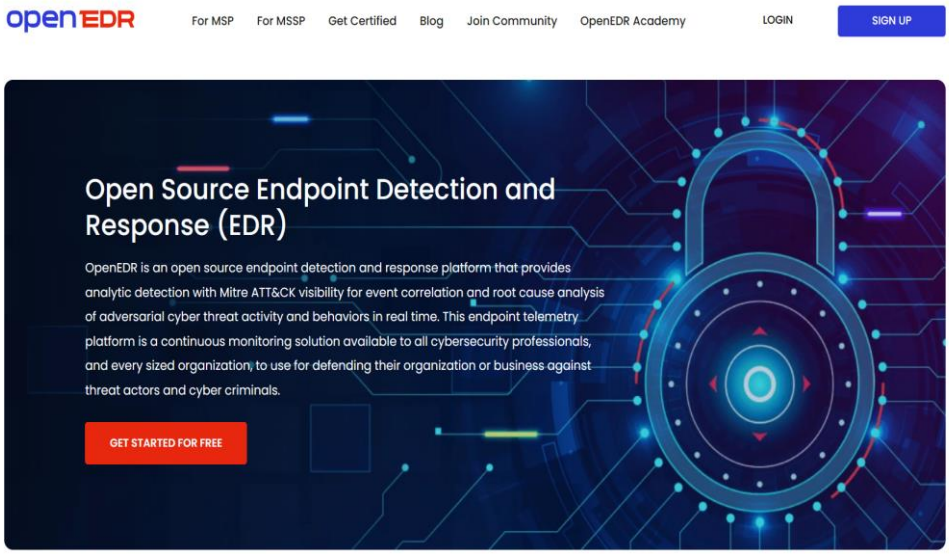

Рис. 3.1. Головна сторінка офіційного сайту платформи OpenEDR [6]

Адміністрування здійснюється через веб-інтерфейс OpenEDR. У хмарній версії платформи (Xcitium-hosted) необхідно зареєструвати обліковий запис, як на рис. 3.2. і додати кінцеві точки для моніторингу; при власному розгортанні доводиться самостійно розгортати серверну частину (наприклад, на базі ELK-stack) та налаштовувати агрегацію логів. Процес реєстрації є стандартним: потрібно вказати ім’я, адресу електронної пошти, пароль та підтвердити аккаунт через номер телефону. Вводимо потрібні дані та чекаємо перенаправлення.

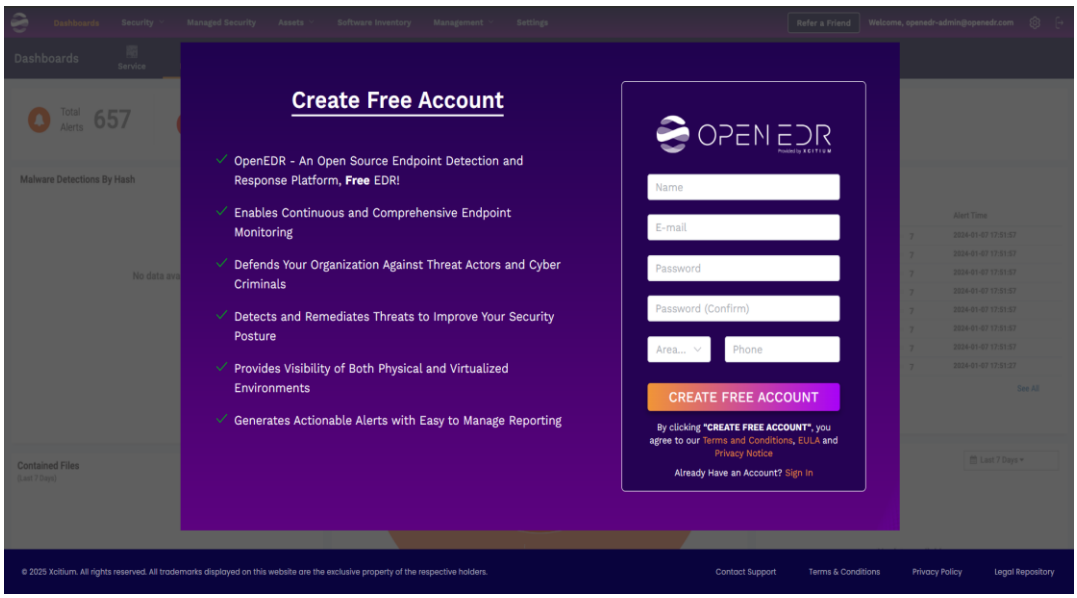

Рис. 3.2. Форма для створення безкоштовного аккаунту

Після завершення реєстрації користувача система автоматично перенаправляє на етап налаштування двофакторної автентифікації (Setup Your Two-Factor Authentication). Тут необхідно відсканувати QR-код за допомогою мобільного застосунку (наприклад, Google Authenticator або Authy) та ввести згенерований шестизначний код (рисунок 3.3). Після натискання кнопки Pair Authenticator двофакторна автентифікація активується — це важливий захід безпеки, що значно ускладнює несанкціонований доступ до адміністративної панелі, навіть якщо зловмисник отримає логін і пароль.

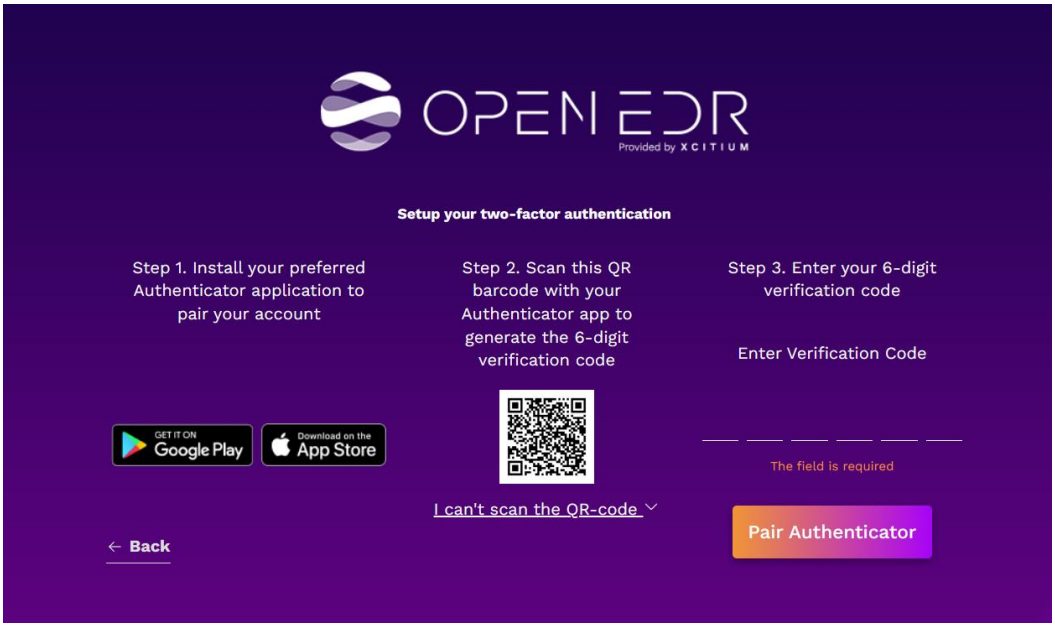

Рис. 3.3. Налаштування двофакторної автентифікації

Далі система повідомляє про успішне увімкнення 2FA (вікно 2FA Account Protection Enabled) і пропонує завантажити резервні коди відновлення (backup codes) у вигляді текстового файлу, як показано на рис. 3.4. Збереження цих кодів є рекомендованим кроком, оскільки вони дозволяють увійти до облікового запису в разі втрати доступу до мобільного пристрою з додатком 2FA.

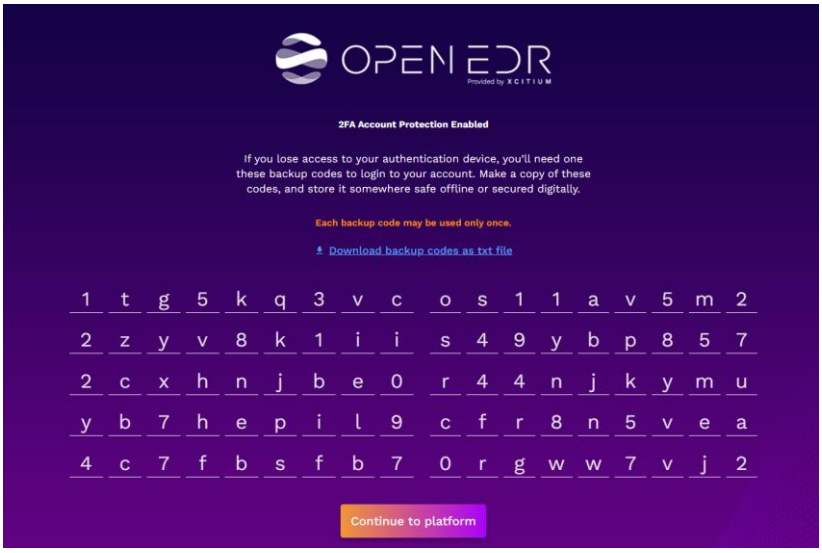

Рис. 3.4. Успішне увімкнення 2FA та пропозиція збереження резервних кодів

Наступним кроком є налаштування секретних запитань (Set Secret Questions): за замовчуванням пропонується ввести відповіді на три питання, але цей етап можна пропустити, як на рис. 3.5. Після цього користувача автоматично перенаправляється до головної сторінки веб-інтерфейсу платформи OpenEDR.

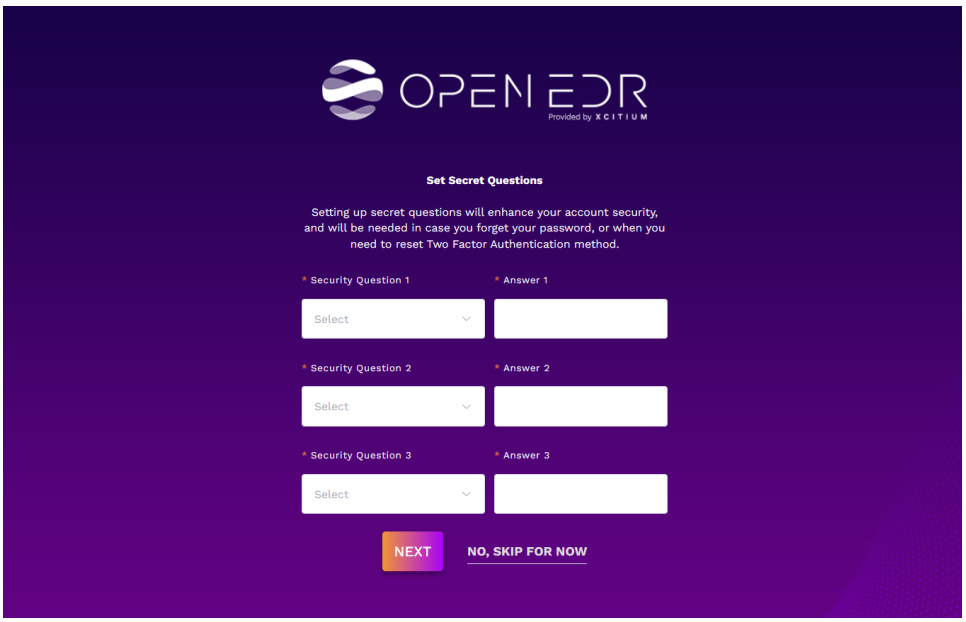

Рис. 3.5. Налаштування секретних запитань

Бачимо вікно майстра налаштування, яке з’являється при першому запуску платформи, і свідчить про початок провізії (тобто створення та налаштування) порталу OpenEDR. Повідомлення в центрі екрана інформує користувача, що триває підготовка середовища до подальшого використання, і цей процес може зайняти деякий час (рисунок 3.6).

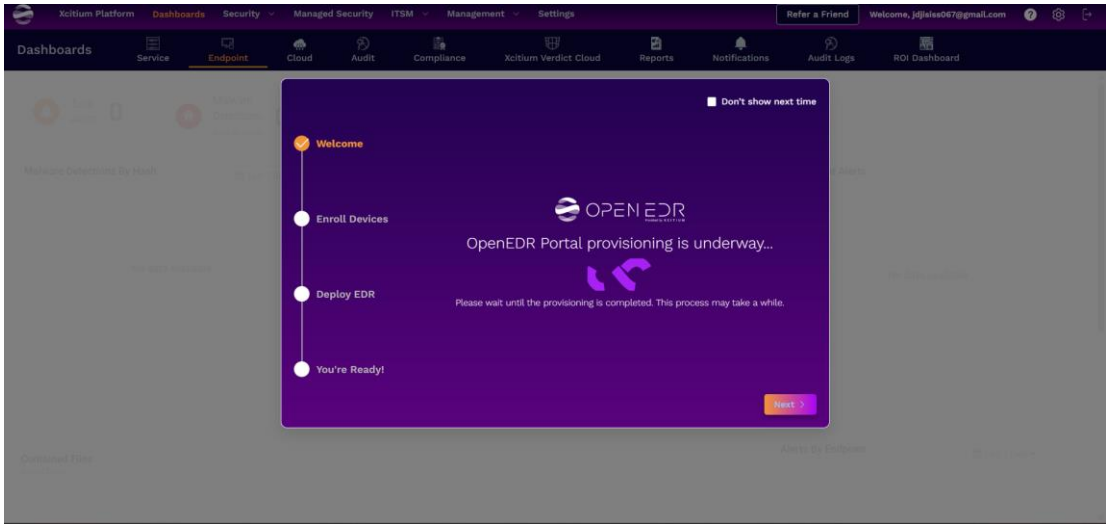

Рис. 3.6. Початок створення та налаштування порталу OpenEDR

Наступним етапом користувачеві пропонується завантажити OpenEDR Communication Agent за наданим унікальним посиланням, як на рис. 3.7. Установка агента на кожен пристрій є обов’язковою умовою, щоб пристрій був включений до списку захищених кінцевих точок.

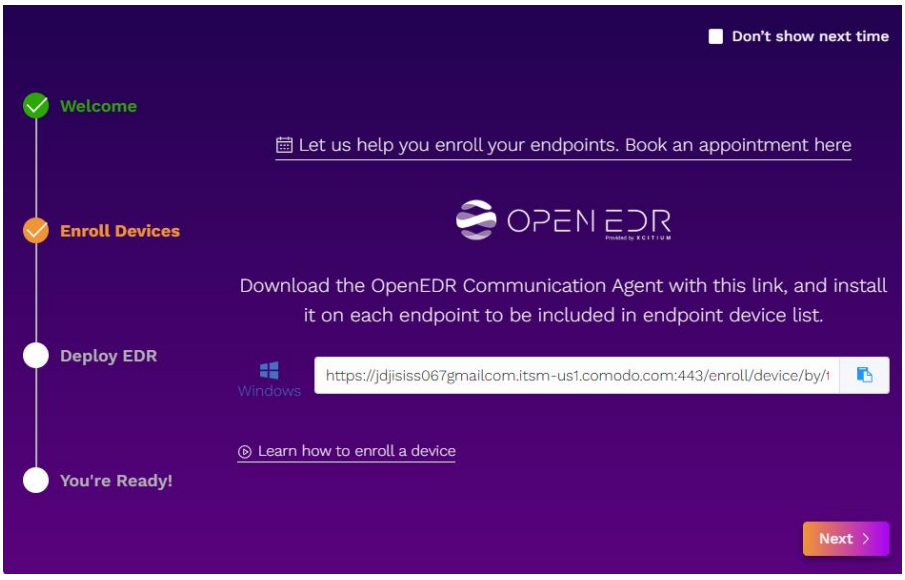

Рис. 3.7. Надання можливості завантаження агенту OpenEDR через посилання

На віртуальну машину з ОС Windows встановлюється агент OpenEDR через посилання (рисунок 3.8).

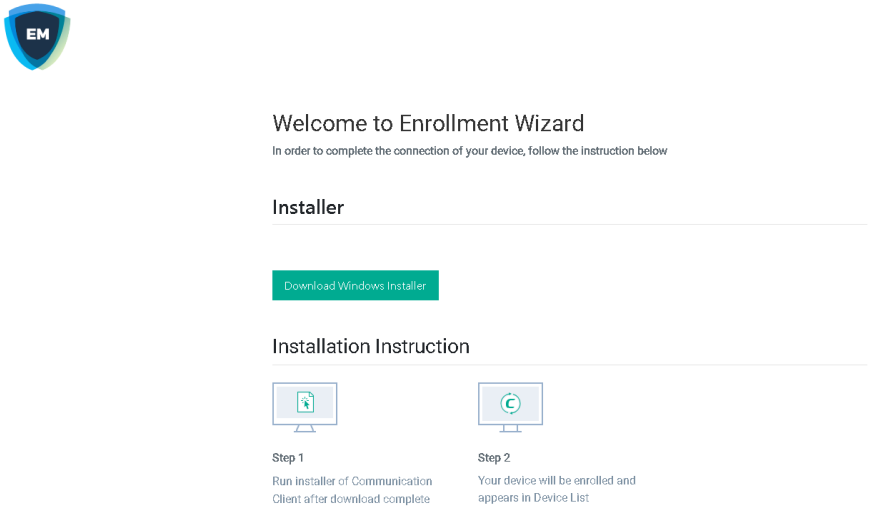

Рис. 3.8. Завантаження та запуск інсталятора Communication Agent на кінцевому пристрої.

Після цього, бачимо, що для реалізації системи захисту необхідно інсталювати спеціальний агент на кінцеві пристрої, який забезпечує зв'язок з EDR-порталом і дозволяє здійснювати моніторинг, контроль і захист мережевих вузлів.

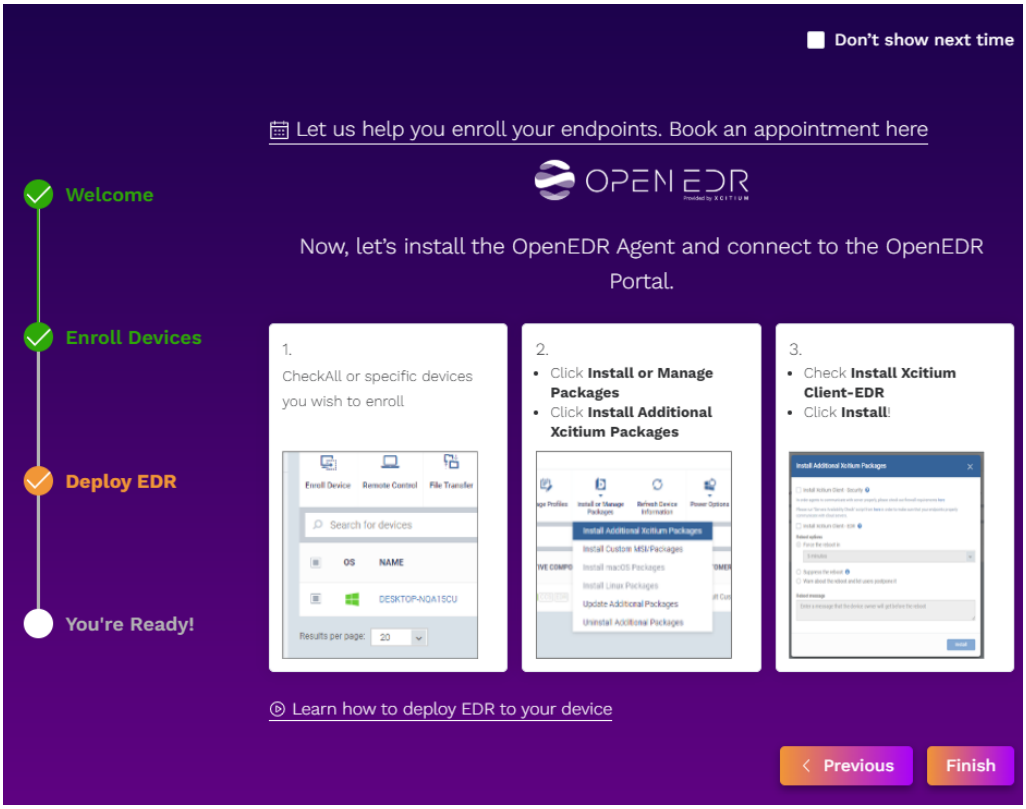

Рис. 3.9. Етап інсталяції OpenEDR агенту

З розділу Device Management платформи OpenEDR видно, що після виконання кроку Enroll Device, віртуальна машина з Windows (DESKTOP-22UJCEI) успішно з’явилася в списку пристроїв. Це свідчить про те, що агент встановлено і з’єднання з порталом налагоджено (рисунок 3.10). Наступним кроком є дозавантаження пакетів Xcitium Packages, щоб активувати повний функціонал EDR, включаючи виявлення загроз, моніторинг подій та автоматичне реагування.

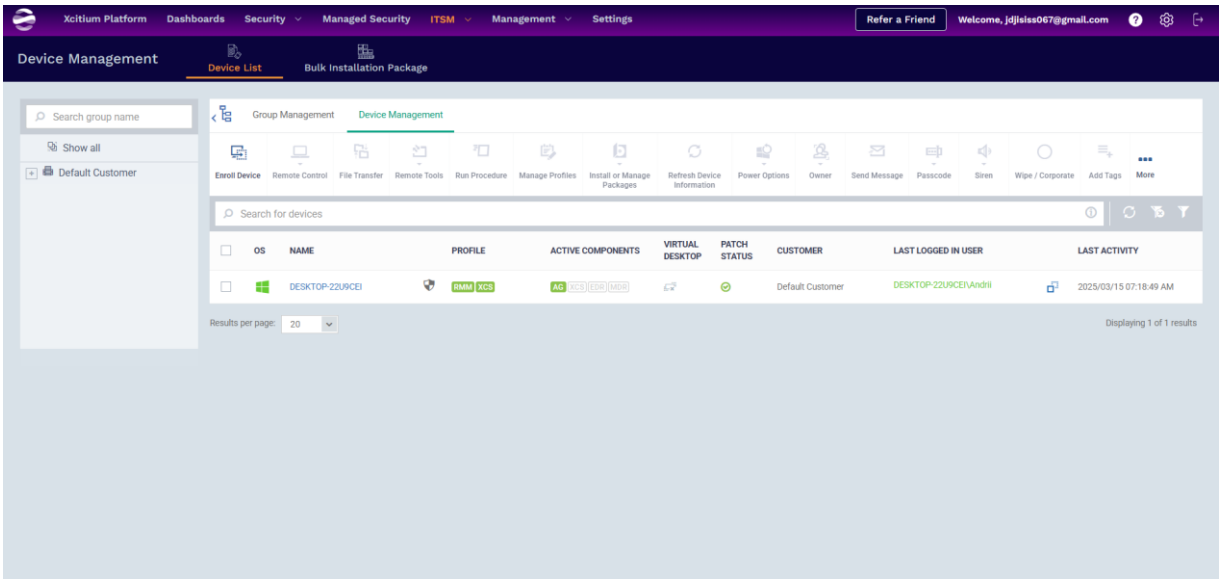

Рис. 3.10. Успішно встановлене з’єднання між порталом та ВМ

Під час оновлення компонентів пакета Xcitium, зокрема у процесі інсталяції або оновлення OpenEDR, користувач системи отримує повідомлення про необхідність перезавантаження пристрою. У рамках реалізації безпечної інсталяції адміністраторами був реалізований механізм автоматизованого відліку часу – таймер встановлюється на 5 хвилин (рисунок 3.11), після чого система автоматично перезавантажується. Це дає змогу застосувати зміни у системні компоненти захисту без втручання користувача та забезпечити цілісність і стабільність роботи системи. Такий підхід мінімізує ризики, пов’язані з людським фактором, і дозволяє гарантовано активувати всі нові засоби контролю та захисту на кінцевій точці, як і сприяє підвищенню загального рівня безпеки, зменшуючи вікно вразливості між завершенням оновлення та фактичним застосуванням змін. Крім того, це спрощує процес адміністрування великої кількості пристроїв у мережі, забезпечуючи одноманітність і контрольованість оновлень.

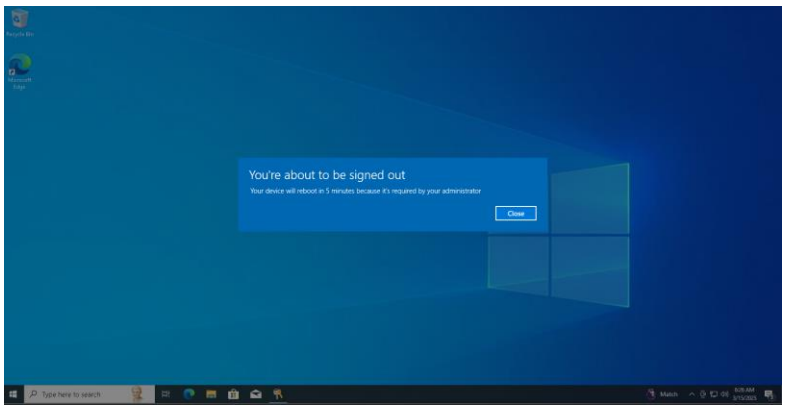

Рис. 3.11. Спрацювання механізму відліку часу

На панелі керування видно кінцеву точку з операційною системою Windows, яка належить до профілю захисту, що включає компоненти RMM, XCS, AG, EDR, та інші засоби безпеки. Це свідчить про те, що система коректно інтегрована у захищене середовище, де здійснюється моніторинг і контроль активностей, а також централізоване керування оновленнями й політиками безпеки, як на рис. 3.12.

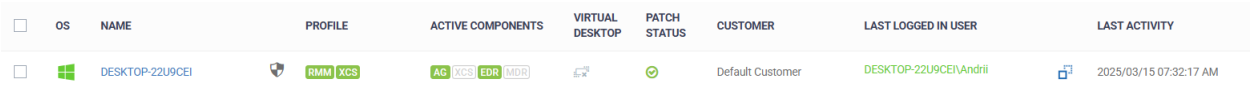

Рис. 3.12. Успішно під’єднання агенту OpenEDR

Агент доступний як підписаний MSI-пакет; за замовчуванням він інсталюється в каталог *C:\Program Files\COMODO\EdrAgentV2*.

Телеметричні події, зібрані агентом, зберігаються локально, за замовчуванням — у папці *C:\ProgramData\edrsvc\log*, як на рис. 3.13.

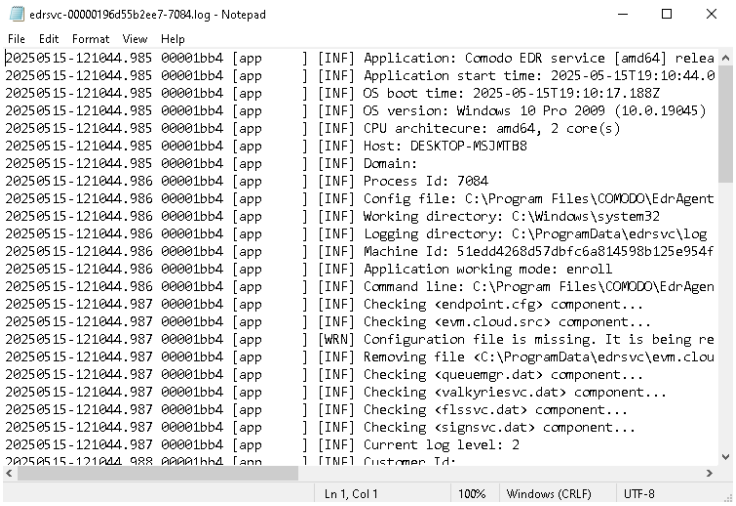

Рис. 3.13. Фрагмент лог-файлу роботи агента OpenEDR

3.2. Алгоритм розслідування кіберінцидентів у середовищі OpenEDR

Розслідування кіберінцидентів є ключовим елементом захисту інформаційних систем: воно дозволяє оперативно виявити зловмисні дії, локалізувати проблему та усувати наслідки атаки. EDR-системи суттєво полегшують цей процес, забезпечуючи цілодобовий моніторинг кінцевих пристроїв та детальну аналітику подій [14]. Зокрема, OpenEDR – відкрита платформа для виявлення і реагування на загрози – надає розширені можливості для фіксації подій, кореляції сигналів та глибокого аналізу інцидентів [15].

Алгоритм розслідування кіберінциденту зазвичай складається з послідовних етапів: збору даних, ідентифікації інциденту, аналізу, реагування та усунення наслідків. OpenEDR підтримує кожен із цих кроків.

Збір даних – агент OpenEDR на кожному кінцевому пристрої постійно фіксує події на рівні ядра ОС (файлові операції, запуск процесів, мережеві з’єднання тощо). Ця телеметрія централізується на сервері, що дає аналітикам повний хронологічний журнал активності всіх машин. Таким чином спеціаліст має вхідні дані для подальшого аналізу [6]. На рис. 3.14. зображено перелік процесів та подій, зібраних з кінцевої точки для подальшого аналізу. Ці дані включають відомості про запуск процесів, зміну файлів, мережеву активність тощо.

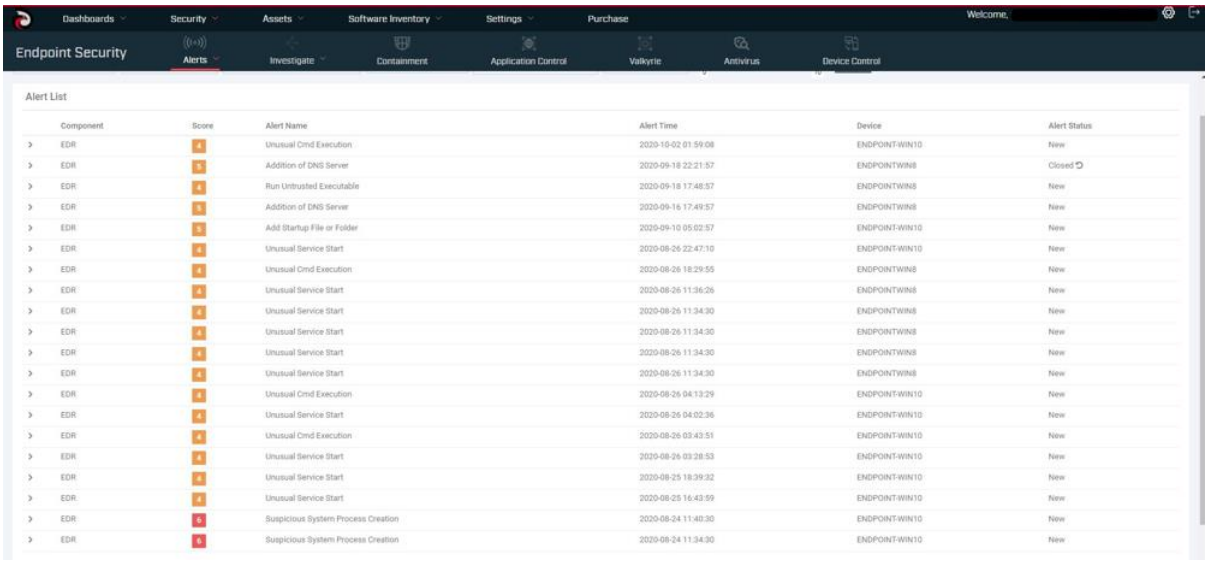

Рис. 3.14. Збір телеметрії агентом OpenEDR [9]

Ідентифікація інциденту – за допомогою політик виявлення та аналізу поведінки OpenEDR автоматично оцінює, чи є зафіксовані події ознаками інциденту. Наприклад, система виявляє підозрілі мережеві з'єднання, нерегламентовані запуски процесів або спроби модифікації системних файлів. Як зазначено в описі EDR, платформа «моніторить і збирає дані з кінцевих пристроїв для виявлення, аналізу, розслідування та реагування на загрози» [14]. Тож фахівець отримує сповіщення або аварійні сигнали, що вказують на можливу атаку. На рис. 3.15. відображено підозрілий процес (наприклад, powershell.exe з певними аргументами) та пов'язані з ним атрибути (шлях, хеш, ім'я користувача, час тощо). Інтерфейс показує подію «Suspicious System Process Creation» і допомагає оперативно помітити аномалії.

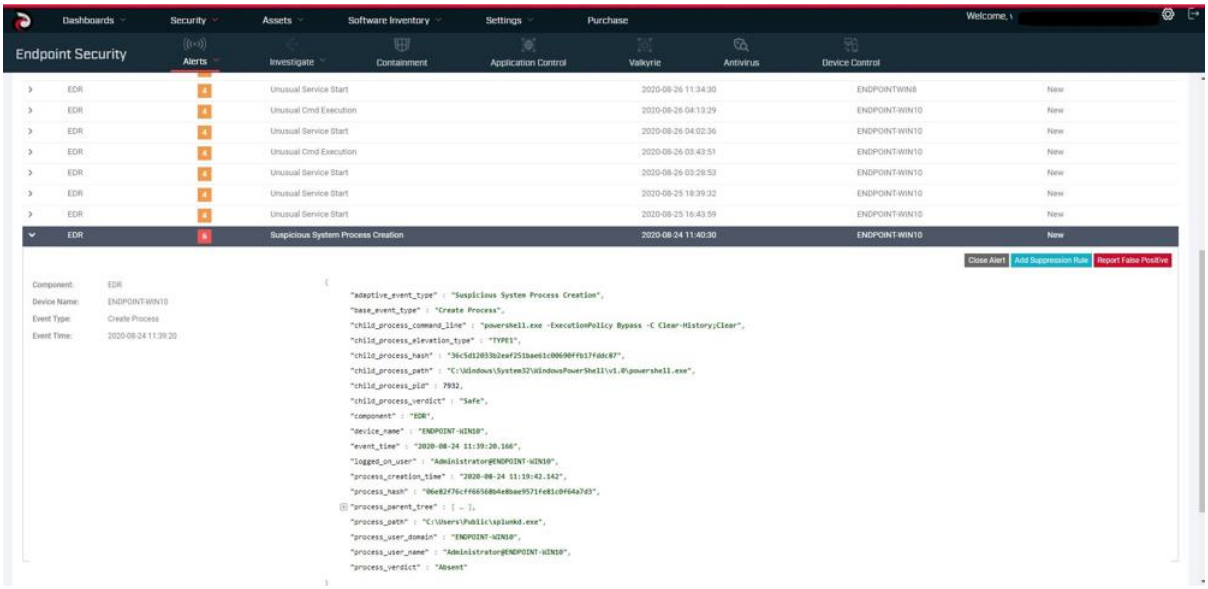

Рис. 3.15. Ідентифікування інциденту [9]

Аналіз інциденту – після ідентифікації інциденту аналітик використовує OpenEDR для детального дослідження. В інтерфейсі є можливість запускати SQL-подібні пошукові запити по зібраних журналах та використовувати фільтри з кореляцією за MITRE ATT&CK. Це дозволяє з'ясовувати, які саме дії виконувалися зловмисником (наприклад, запуск змінюваних файлів, віддалений доступ, скомпрометовані облікові записи тощо) [15]. OpenEDR також надає засоби форензики – наприклад, побудову дерев пошуку чи трекер подій, – завдяки чому спеціаліст може реконструювати хронологію атакуючих дій для встановлення

першопричини (root-cause). У режимі Process Timeline OpenEDR візуалізує послідовність процесів та подій навколо обраного інциденту. На рис. 3.16. показано, які процеси були породжені вибраним процесом і які події вони згенерували. Це дозволяє простежити розвиток атаки та зв'язки між процесами (зафарбовано відповідними типами подій).

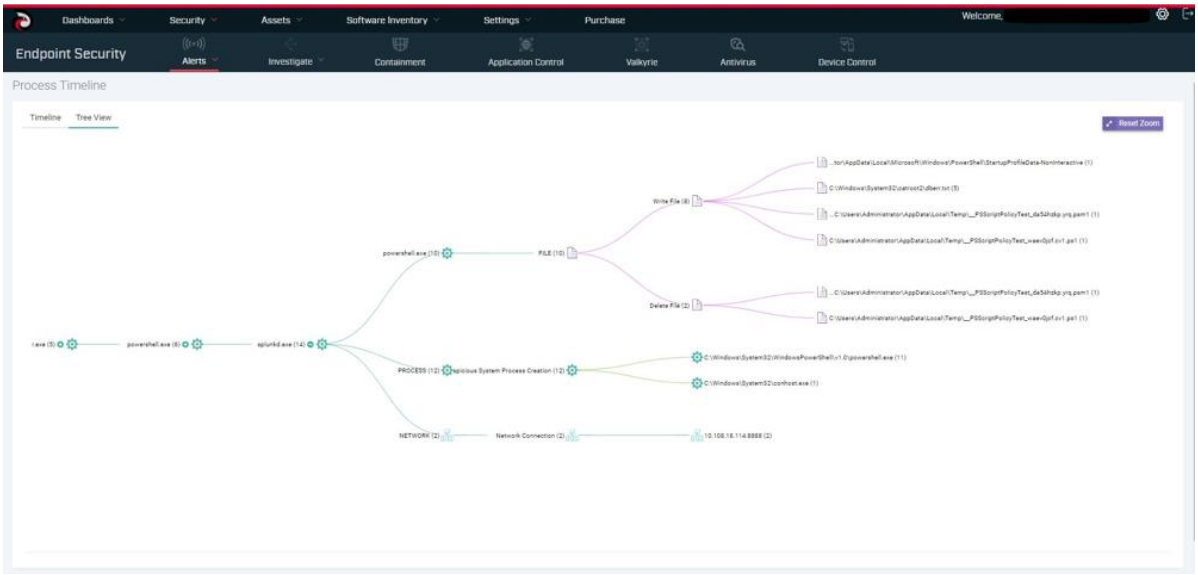

Рис. 3.16. Візуалізація послідовності процесів та подій навколо обраного інциденту [9]

Реагування – на цьому етапі приймаються оперативні заходи. OpenEDR дозволяє миттєво ізолювати уражений вузол від мережі, що запобігає подальшому розповсюдженню шкідливих програм. Окрім ізоляції, спеціаліст може вручну заблокувати небезпечні процеси або мережеві з'єднання через консоль OpenEDR, а також викликати інструменти (керовані політики) для усунення зараження. Таке оперативне втручання забезпечує локалізацію інциденту – усі інфіковані пристрої відключаються від роботи доти, доки загроза повністю не нейтралізована [6]. Модуль Event Search OpenEDR показує агреговані дані про типи подій, компоненти й файлові хеші. На верхній панелі задаються фільтри (компонент, тип подій, діапазон часу), а нижня частина відображає деталізовану інформацію про вибрану подію, як на рис. 3.17. Цей інструмент допомагає швидко переглянути суміжні події та підтвердити або спростувати підозри, сприяючи швидкій реакції.

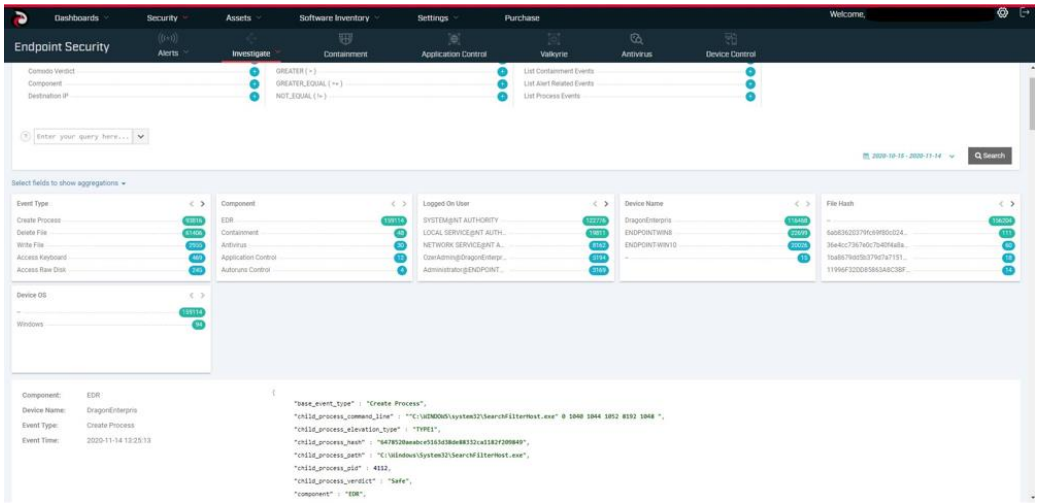

Рис. 3.17. Агреговані дані про типи подій, компоненти й файлові хеші [9]

Усунення наслідків – після локалізації загрози фахівець усуває саму причину інциденту. Наприклад, видаляються шкідливі файли, відновлюються модифіковані ресурси з резервних копій та встановлюються відсутні оновлення безпеки. OpenEDR допомагає відслідкувати, що було заражено, і повернути системи у робочий стан. Нарешті, впроваджуються профілактичні заходи (оновлення антивірусних баз, уточнення політик безпеки, навчання персоналу) для зменшення ризику повторного інциденту.

На рис. 3.14. узагальнено типові етапи реагування на кіберінциденти (за стандартами SANS/NIST): від попередньої підготовки та виявлення до локалізації загрози, її усунення і відновлення системи. OpenEDR підтримує всі ці етапи: від фіксації подій на рівні ОС до автоматичної ізоляції виявлених загроз. Завдяки зібраній телеметрії та можливості виконання поглибленого пошуку по логах спеціалісти отримують інструменти для детального аналізу інциденту на будь-якому з етапів [17].

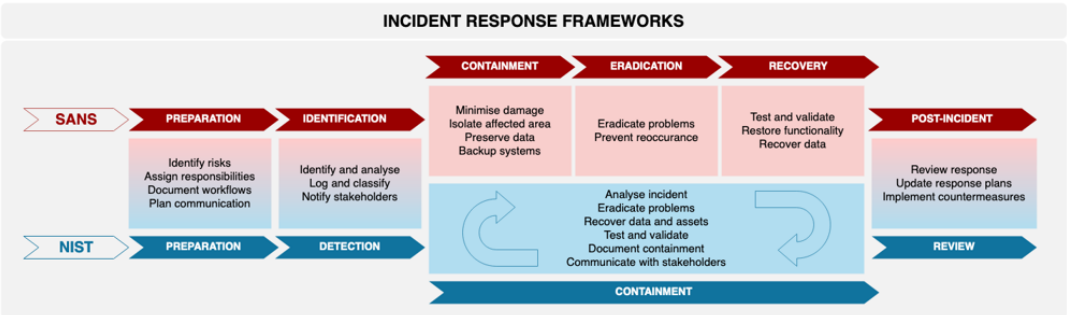

Рис. 3.18. Системи реагування на інциденти [17]

Один із прикладів практичного застосування OpenEDR описано в кейс-стаді фінансової компанії 2024 року. Після того як кілька комп'ютерів відобразили ненормально високе завантаження CPU та нескоординовані зміни файлів, платформа OpenEDR згенерувала сповіщення про підозрілу активність (виявлено несанкціоновані процеси та підозрілі мережеві з'єднання. Команда кібербезпеки провела поглиблений аналіз: завдяки функції threat hunting з'ясували, що початкове зараження сталося через фішингове посилання, після чого шкідливий код поширився по мережі. Форензик-аналіз у OpenEDR дозволив виявити, що вірус шифрував файли та намагався відправити дані на віддалений сервер. На етапі реагування за допомогою OpenEDR вразливі пристрої було негайно ізольовано від мережі, заблоковано шкідливі IP-адреси та терміновано підозрілі процеси. Після цього компанія відновила дані з резервних копій і посилила захисні політики. Цей кейс ілюструє, як OpenEDR забезпечує реальну прозорість і контроль над інцидентом – від початкового виявлення до повного усунення загрози [16].

Алгоритм розслідування кіберінцидентів із застосуванням OpenEDR базується на поетапній обробці даних: збір детальної телеметрії, виявлення аномалій, глибокий аналіз атаку, оперативне реагування та подальше відновлення. Впровадження OpenEDR у середовище організації дає змогу об'єднати ці етапи в єдиній системі: платформа забезпечує повний ланцюг дій від виявлення загрози до її нейтралізації, а також дозволяє постійно вдосконалювати політики безпеки на основі зібраних даних [6].

3.3. Практичні рекомендації щодо впровадження методів та інструментів захисту кінцевих точок організації на базі OpenEDR

Для ефективного використання OpenEDR в організації необхідно насамперед чітко розподілити відповідальність та оформити процеси. Рекомендується створити або залучити спеціалізовану команду кібербезпеки (SOC), яка відповідатиме за моніторинг і обробку інцидентів від OpenEDR. Слід провести інвентаризацію всіх кінцевих точок та забезпечити охоплення агента EDR на всіх

комп’ютерах і серверах, включно з портативними пристроями і робочими станціями адміністраторів. Адже, як зазначається в рекомендаціях, якщо на критичних кінцевих точках не встановлено агенту, «ви не зможете ні виявити, ні запобігти атакам, і не зберете необхідну інформацію у разі інциденту» [18].

Перед загальним розгортанням корисно провести пілотне тестування: вибрати кілька відповідальних користувачів (адміністраторів, керівників) і серверів для початкового впровадження. Це дозволить перевірити політики безпеки і оновлення, перш ніж застосовувати їх у масштабі всієї організації. Рекомендується спочатку запускати OpenEDR у режимі виявлення (Detect Only), щоб без негативного впливу на бізнес-процеси перевірити, як система працює з існуючими додатками [18].

Не менш важливо інтегрувати OpenEDR з існуючими інструментами безпеки, наприклад з SIEM або SOAR, для централізованого моніторингу подій та спрощення кореляції інцидентів. Всі зміни в конфігураціях і політиках слід документувати: визначити процедури оновлення налаштувань, описати процеси реагування та вести журнал операційних дій (своєрідний комплаєнс-процес). Заздалегідь потрібно також визначити рівні критичності пристроїв і подій (наприклад, дозвіл на призупинення процесів лише для інцидентів високої небезпеки), щоб відрегулювати автоматичне реагування OpenEDR відповідно до вимог організації [18].

При впровадженні OpenEDR часто трапляються наступні помилки:

реалізація EDR без аналізу потреб і ресурсів організації призводить до пропусків у безпеці й збоїв. Перед впровадженням варто провести аудит інформаційних активів, визначити критичні системи й узгодити графік оновлень. Без чіткого плану велика ймовірність неповного розгортання (наприклад, пропущені сервера або облікові записи), що знижує загальну ефективність захисту [19];

виключення з-під захисту навіть окремих ПК чи серверів створює «дірки» в безпеці. Пропуск агентів на робочих станціях із високим рівнем доступу (наприклад, адміністраторських терміналах) є особливо небезпечним. Як

підкреслюють експерти, якщо EDR-агент може бути встановлений на пристрій – його слід встановити: «ті багаті цілі саме й повинні бути включені» для забезпечення повного охоплення [18];

некоректно налаштовані правила виявлення і реагування призводять або до великої кількості хибних спрацювань, або пропуску реальних загроз. Наприклад, помилкові винятки чи занижені пороги спрацьовування дозволяють зловмиснику залишатися непоміченим. Щоб цього уникнути, необхідно налаштувати детектування під реальні сценарії організації та регулярно перевіряти ефективність правил. Краще утримуватись від виключення цілих директорій чи груп програм, крім суворо обґрунтованих випадків [18];

якщо OpenEDR працює «сам по собі» без передачі подій у загальну систему безпеки (SIEM, лог-менеджмент тощо), це ускладнює кореляцію і аналіз. Для комплексного захисту слід об’єднати дані EDR з даними з IDS/IPS, DLP або аналітичних платформ. Така інтеграція забезпечить ширшу видимість загроз і сприятиме швидшому реагуванню [19];

недостатня кваліфікація або тренування команди кібербезпеки призводить до невміння правильно інтерпретувати сповіщення. Якщо оператори не навчені аналізувати та реагувати на сигнали OpenEDR, ефективність системи падає. Тому потрібно проводити регулярні навчання: персонал має знати можливості платформи, розуміти значення різних індикаторів і вміти розслідувати інциденти [20];

навіть після впровадження EDR не можна «налаштувати та забути». Якщо не виділено ресурси для цілодобового моніторингу сповіщень, інциденти можуть залишатися необробленими. Організація повинна призначити відповідальних за моніторинг і реагування на інциденти, мати регламент оперативного реагування та чіткий план дій при виявленні загроз [19].

Політики реагування слід налаштовувати з урахуванням ролей пристроїв і критичності подій. Наприклад, можна заборонити запуск підозрілих процесів, відкриття незнайомих файлів чи підключення нових периферійних пристроїв (USB) до визначених машин. В OpenEDR можна детально налаштувати правилом

(Policy) і встановлювати різні рівні автоматичної реакції (від простого сповіщення до примусового завершення процесу або ізоляції). Як зазначено в описі OpenEDR, користувач має можливість «налаштовувати політики відповідно до конкретних вимог безпеки організації». Варто почати з базової політики безпеки для всіх кінцевих точок і лише пізніше, після отримання досвіду, додавати спеціальні винятки або більш жорсткі правила для окремих груп користувачів чи серверів [18].

Підтримка OpenEDR та кінцевих точок у актуальному стані — критично важлива. По-перше, слід регулярно оновлювати саму платформу OpenEDR (агентів і серверну частину) та ОС на кінцевих пристроях. Згідно з експертними рекомендаціями, усі компоненти EDR повинні своєчасно отримувати патчі «для усунення уразливостей та підтримки відповідності» сучасним вимогам. Крім того, оскільки OpenEDR — проєкт з відкритим кодом, платформа часто отримує «оперативні виправлення від спільноти» і має можливість швидкого релізу оновлень. Це слід використовувати на користь організації, своєчасно оновлюючи систему при появі нових версій або модулів [20].

По-друге, журналювання: збереження та архівація логів. OpenEDR веде детальні журнали активності, і ці записи мають зберігатися щонайменше стільки, скільки вимагають внутрішні політики безпеки або нормативні вимоги. Автоматизування збору логів з консолі керування (через SIEM чи інший сервер лог-менеджменту), щоб можна було довести факт моніторингу і провести ретельний аналіз інцидентів при необхідності. Регулярна перевірка на цілісність самих лог-файлів і переміщення їх у безпечне архівне сховище, щоб уникнути втрати важливої інформації [6].

По-третє, навчання персоналу. Навіть найкраща технічна система не спрацює без підготовлених людей. Як рекомендують експерти, безпека залежить від рівня навченості фахівців. Регулярні тренінги та навчальні вправи для аналітиків і операторів: як аналізувати тривоги OpenEDR, яким чином реагувати на різні типи інцидентів, як оцінювати ризик автоматичного втручання. Сама ж література підкреслює, що «підготовка команди до роботи з розгорнутим EDR-рішенням дозволяє більш ефективно використовувати систему». Навчання повинно

охоплювати інструктажі з політик, процедури ескалації інцидентів і відпрацювання сценаріїв від реагування до усунення загроз [19, 20].

Після запуску OpenEDR слід регулярно перевіряти налаштування і проводити аудит системи. Доцільно періодично моделювати інциденти (так звані «red team» або «pen-test» сценарії) та перевіряти, чи система їх виявляє та правильно реагує. Також, слід накладати зміни на тестовій підсистемі чи на пілотній групі перед поширенням на весь парк. Експерти радять «провести пілотне тестування на невеликій групі користувачів і серверів», щоб будь-які нові політики чи оновлення перевірити в контрольованому середовищі [18].

Крім того, регулярний аудит конфігурації OpenEDR є обов’язковим: щонайменше раз на рік (або після значних змін у інфраструктурі) необхідно перевіряти актуальність правил детектування, ефективність налаштувань та наявність нових критичних вразливостей. Як радять фахівці, періодичні перевірки («Conduct regular audits and assessments… and adjust as necessary») допомагають підтримувати відповідність внутрішнім політикам і нормативам. В ході аудиту слід аналізувати відсутність аномалій у логах (перевірка на накриття зловмисних дій), коректність привілеїв агентів, а також співвідношення кількості сповіщень та реальних інцидентів [20].

Загалом, впровадження OpenEDR слід бачити як безперервний процес: правильне пілотування, поступове нарощування політик, постійний моніторинг і періодичне тестування – усе це дозволить максимально використати потенціал платформи в захисті кінцевих точок.

ПЕРЕЛІК ПОСИЛАНЬ

1. X-Force Threat Intelligence Index 2024. URL: https://branden.biz/wp-content/uploads/2024/02/IBM-XForce-Threat-Intelligence-Index-2024.pdf (дата звернення: 16.03.2025).

2. 2024 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/Tdd9/reports/2024-dbir-data-breach-investigations-report.pdf (дата звернення: 16.03.2025).

3. Modern Endpoint Management vs. Traditional Approaches: A Comparison. URL: https://usawire.com/modern-endpoint-management-vs-traditional-approaches/ (дата звернення: 16.03.2025).

4. Beyond Antivirus Comprehensive Strategies For Holistic Endpoint Protection In 2024. URL: http://securetrust.io/blog/beyond-antivirus-comprehensive-strategies-for-holistic-endpoint-protection-in-2024/ (дата звернення: 16.03.2025).

5. What Is an Endpoint Protection Platform (EPP)?. URL: http://cisco.com/site/us/en/learn/topics/security/what-is-an-endpoint-protection-platform.html (дата звернення: 16.03.2025).

6. Open Source Endpoint Detection and Response (EDR). URL: https://www.openedr.com/ (дата звернення: 16.03.2025).

7. Які рішення CrowdStrike використовуються для захисту від кібератак?. URL: https://eska.global/blog/yaki-rishennya-crowdstrike-vikoristovuyutsya-dlya-zahistu-vid-kiberatak (дата звернення: 16.03.2025).

8. ТОП-7 стратегій для зміцнення захисту кінцевих точок у 2024 році. URL: https://www.kliksolutions.com.ua/great-info/7-strategij-dlya-zahystu-kinczevyh-tochok/ (дата звернення: 16.03.2025).

9. Open EDR public repository. URL: https://github.com/ComodoSecurity/openedr?tab=readme-ov-file (дата звернення:

16.03.2025).

10. Open EDR Components. URL: https://techtalk.comodo.com/2020/09/19/open-edr-components/ (дата звернення: 16.03.2025).

11. Інструмент для генерування діаграм. URL: https://whimsical.com/ (дата звернення: 16.03.2025).

12. Що таке протидія загрозам у кінцевих точках (EDR). URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-edr-endpoint-detection-response (дата звернення: 16.03.2025).

13. Xcitium openedr – виявлення та реагування на атаки кінцевих точок. URL: https://obozrevatel.org/xcitium-openedr-vyiavlennia-ta-reahuvannia-na-ataky-kintsevykh-tochok/ (дата звернення: 16.03.2025).

14. An Overview of Endpoint Detection and Response (EDR). URL: https://www.digitalguardian.com/blog/overview-endpoint-detection-and-response-edr (дата звернення: 16.03.2025).

15. Service, OpenEDR. URL: https://www.cisa.gov/resources-tools/services/openedr (дата звернення: 16.03.2025).

16. Malware Investigation Using OpenEDR: A Case Study of 2024 Attacks. URL: https://totalx.id/malware-investigation-using-openedr-a-case-study-of-2024-attacks (дата звернення: 16.03.2025).

17. Diagrams for a better incident response. URL: https://www.drawio.com/blog/diagrams-incident-response (дата звернення: 16.03.2025).

18. Endpoint Detection and Response Best Practices in 2024. URL: https://www.deepwatch.com/blog/endpoint-detection-and-response-best-practices-in-2024/ (дата звернення: 16.03.2025).

19. 7 Common EDR Deployment Mistakes and How to Resolve Them. URL:

https://solutionsreview.com/endpoint-security/common-edr-deployment-mistakes-and-how-to-resolve-them/ (дата звернення: 16.03.2025).

20. What Is Endpoint Detection and Response (EDR) Compliance. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-detection-and-response-edr-compliance (дата звернення: 16.03.2025)