Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
магістр
(ступінь вищої освіти)

на тему Дослідження ефективності систем виявлення та реагування на події безпеки (EDR) у протидії сучасним кіберзагрозам
(назва теми)

Виконав(ла): студент(ка) IIого курсу,
групи БК-814м
Спеціальності 125 Кібербезпека та захист інформації
(код і найменування спеціальності)
Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних систем
НІВАКШОНОВ М.А.
(ПРІЗВИЩЕ та ініціали)

Керівник КОРОЛЬКОВ Р.Ю.
(ПРІЗВИЩЕ та ініціали)

Рецензент МОРОЗ Г.В.
(ПРІЗВИЩЕ та ініціали)

2025

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
Кафедра інформаційної безпеки та наноелектроніки
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
(код і найменування)
Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних систем
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ
Завідувач кафедри ІБтаН к.ф.н доцент
Андрій КОРОТУН
«____» _____2025року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

НІВАКШОНОВУ Максиму Андрійовичу
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Дослідження ефективності систем виявлення та реагування на події безпеки (EDR) у протидії сучасним кіберзагрозам
Research into the effectiveness of security event detection and response (EDR) systems in countering modern cyber threats
керівник проєкту (роботи) к.т.н., доцент КОРОЛЬКОВ Роман Юрійович
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом закладу вищої освіти від «26» листопада 2025 року №530
2. Строк подання студентом проєкту (роботи) 10.12.2025
3. Вихідні дані до проєкту (роботи) Аналіз принципу роботи систем EDR, їх відмінностей від стандартних методів аналізу хешів загроз, методів і засобів захисту інформації пов'язаних з машинним навчанням та евристичним аналізом, котрий дозволяє не тільки знаходити відомі загрози, а й виявляти загрози нульового дня (zero-day threats)
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Сучасні кіберзагрози та їх вплив на кінцеві точки. Огляд архітектури EDR-систем; Основні можливості та функціональні модулі EDR. Типові вразливості кінцевих точок і вектори атак. місце EDR у багаторівневій системі кіберзахисту. інтеграція EDR із SIEM та іншими інструментами безпеки. Порівняння провідних EDR-рішень. Аналіз ефективності EDR у виявленні та блокуванні сучасних загроз; Розробка рекомендацій щодо впровадження використовуючи отримані результати аналізу.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)
Презентація доповіді (в MS PowerPoint), 12 слайдів.

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1 – 3	КОРОЛЬКОВ Р.Ю., доцент кафедри ІБтаН	02.09.2025	05.12.2025
Нормоконтроль	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН		09.12.2025

7. Дата видачі завдання «02» вересня 2025року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1.	Вибір теми. Затвердження плану і завдання кваліфікаційної роботи.	02.09.25 – 16.09.25	виконано
2.	Аналіз завдання, пошук та огляд літературних джерел за темою роботи.	17.09.25 – 23.09.25	виконано
3.	Огляд принципів роботи систем EDR. Основні відмінності від програмних апаратних рішень.	24.09.25 – 29.09.25	виконано
4.	Дослідження та аналіз показників виявлення та блокування різноманітних програмних та апаратних рішень, їх ефективності у випробуваннях на базі актуальних загроз.	30.09.25 – 05.10.25	виконано
5.	Розробка рекомендацій по впровадженню рішень EDR відповідно до вимог та специфіки захисту інформації.	06.10.25 – 15.10.25	виконано
6.	Оформлення пояснювальної записки.	01.11.25 – 13.11.25	виконано
7.	Здача на перевірку та підпис кваліфікаційної роботи керівнику.	14.11.25 – 19.11.25	виконано
8.	Проходження перевірки на плагіат та нормоконтроль кваліфікаційної роботи.	20.11.25 – 30.11.25	виконано
9.	Допуск завідувачем кафедри до захисту кваліфікаційної роботи.		
10.	Захист дипломної роботи		

Студент _____ Максим НІВАКШОНОВ
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ Роман КОРОЛЬКОВ
(підпис) (Ім'я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до дипломної кваліфікаційної роботи магістра: 72 с., 10 рис., 1 дод., 30 джерел.

EDR, ІНФОРМАЦІЙНА БЕЗПЕКА, ЕВРИСТИЧНИЙ АНАЛІЗ, СИГНАТУРНИЙ АНАЛІЗ, ВИЯВЛЕННЯ КІБЕРЗАГРОЗ, ВИЯВЛЕННЯ ШКІДЛИВОГО ПЗ, ПРОГРАМНІ ТА АПАРАТНІ РІШЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ КІНЦЕВИХ ТОЧОК, XDR, TTPs, MITRE ATT&CK.

Об’єкт дослідження — інформаційна безпека засобів евристичного аналізу.

Предмет дослідження – методи та засоби забезпечення інформаційної безпеки у системах EDR.

Мета роботи – Розробка списку рекомендацій щодо підвищення рівня захисту кінцевих точок.

У роботі розглянуто специфіку роботи EDR систем та основні принципи роботи рішень захисту кінцевих точок. Було проведено порівняльний аналіз програм евристичного аналізу і сигнатурного аналізу, також було проведено дослідження ефективності різних EDR-рішень на основі результатів відкритих онлайн-тестувань та публічних звітів щодо протидії актуальним загрозам.

У роботі розглянуто різні тактики, техніки та процедури котрі зловмисники використовували у найбільш значущих хакерських атаках і проаналізовано ефективність виявлення та захисту кінцевих точок на які симулювалися ці атаки.

Практичне значення одержаних результатів полягає у розробці рекомендацій щодо підвищення рівня безпеки кінцевих точок.

ABSTRACT

Explanatory note to the master's thesis: 72 p., 10 figures, 1 appendix, 30 sources.

EDR, INFORMATION SECURITY, HEURISTIC ANALYSIS, SIGNATURE ANALYSIS, CYBER THREAT DETECTION, MALWARE DETECTION, SOFTWARE AND HARDWARE SOLUTIONS FOR ENDPOINT INFORMATION SECURITY, XDR, TTPs, MITRE ATT&CK.

Object of research — information security of heuristic analysis tools.

Subject of research — methods and means of ensuring information security in EDR systems.

Purpose of work — Development of a list of recommendations for increasing the level of endpoint protection.

The paper examines the specifics of the operation of EDR systems and the basic principles of the operation of endpoint protection solutions. A comparative analysis of heuristic analysis programs and signature analysis was conducted, and a study was also conducted on various EDR solutions in real simulations of protection against current threats.

The paper examines various tactics, techniques and procedures that attackers used in the most significant hacker attacks and analyzes the effectiveness of detecting and protecting endpoints on which these attacks were simulated.

The practical significance of the results obtained lies in the development of recommendations for increasing the level of endpoint security.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AI — Artificial Intelligence — штучний інтелект;

API — Application Programming Interface — програмний інтерфейс;

APT — Advanced Persistent Threat — тривала цільова атака;

APT Group — група тривалої цільової атаки;

AV — Antivirus — антивірус;

C2/C&C — Command and Control — сервери управління;

CTI — Cyber Threat Intelligence — кіберрозвідка загроз;

DLL — Dynamic Link Library — динамічна бібліотека;

DLP — Data Loss Prevention — запобігання витоку даних;

EDC — Endpoint Data Collection — збір даних із кінцевих точок;

EDL — Endpoint Detection Log — журнал виявлення кінцевої точки;

EDR — Endpoint Detection and Response — система виявлення та реагування на події на кінцевих точках;

EDRAM — EDR Agent Module — модуль агента EDR;

EDR Sensor — сенсор EDR для відстеження активності;

EPP — Endpoint Protection Platform — платформа захисту кінцевих точок;

ERT — Emergency Response Team — команда аварійного реагування;

FP/FN — False Positive / False Negative — хибне спрацювання / пропуск загрози;

FW — Firewall — брандмауер;

HIDS/HIPS — Host Intrusion Detection/Prevention System — система виявлення/запобігання вторгнень на хості;

IOC — Indicator of Compromise — індикатор компрометації;

IOC Feed — потік індикаторів компрометації;

IoC Hunting — Indicators of Compromise Hunting — пошук індикаторів компрометації;

IR — Incident Response — реагування на інциденти;

JSON — JavaScript Object Notation — формат структурованих даних;

MDM — Mobile Device Management — управління мобільними пристроями;

MDR — Managed Detection and Response — кероване виявлення та реагування;

MITRE ATT&CK — Adversarial Tactics, Techniques and Common Knowledge — база знань тактик і технік атак;

ML — Machine Learning — машинне навчання;

NIDS/NIPS — Network Intrusion Detection/Prevention System — мережеве виявлення/запобігання вторгненням;

NGAV — Next-Generation Antivirus — антивірус нового покоління;

NGFW — Next-Generation Firewall — брандмауер наступного покоління;

NTA/NDR — Network Traffic Analysis / Network Detection and Response — аналіз мережевого трафіку та виявлення загроз;

OS — Operating System — операційна система;

PCAP — Packet Capture — зняття трафіку;

RAT — Remote Access Trojan — троян віддаленого доступу;

RBAC — Role-Based Access Control — рольовий контроль доступу;

SASE — Secure Access Service Edge — хмарна платформа безпеки та мережевих сервісів;

SD-WAN — Software-Defined Wide Area Network — програмно визначена глобальна мережа;

SIEM — Security Information and Event Management — система збору, кореляції та аналізу подій безпеки;

SIEM Rule — правило кореляції в SIEM;

SOC — Security Operations Center — центр операцій безпеки;

SOC Analyst — аналітик центру безпеки;

SOAR — Security Orchestration, Automation and Response — оркестрація, автоматизація та реагування на події безпеки;

Sysmon — System Monitor — система моніторингу подій Windows;

Threat Intelligence — розвідка загроз;

TLS/SSL — Transport Layer Security / Secure Sockets Layer — протоколи безпечного з’єднання;

TP — True Positive — істинне спрацювання;

TTP — Tactics, Techniques, Procedures — тактики, техніки та процедури злочинців;

UEBA — User and Entity Behavior Analytics — поведінкова аналітика користувачів і пристроїв;

UEFI — Unified Extensible Firmware Interface — розширений інтерфейс завантаження;

VPN — Virtual Private Network — віртуальна приватна мережа;

XDR — Extended Detection and Response — розширена система виявлення та реагування;

YARA — Yet Another Ridiculous Acronym — мова правил для виявлення шкідливого ПЗ;

ZTA — Zero Trust Architecture — архітектура нульової довіри;

ZTNA — Zero Trust Network Access — доступ у мережу за принципом нульової довіри.

ВСТУП

Актуальність теми дослідження обумовлено тим, що сучасні кіберзагрози стають дедалі складнішими та орієнтуються насамперед на компрометацію кінцевих точок — робочих станцій, серверів і мобільних пристроїв. Саме вони найчастіше є першою точкою входу зловмисників у корпоративне середовище. На відміну від традиційних антивірусних підходів, які зосереджені на сигнатурному виявленні, сучасні атаки використовують fileless-техніки, уразливості ОС, механізми віддаленого доступу та складні ланцюжки TTPs, що дозволяють обійти класичні засоби захисту. У таких умовах невеличкі затримки чи перебої у реагуванні на інциденти здатні спричинити величезні збитки, повне зупинення бізнес-процесів, компрометацію критично важливої інформації та порушення роботи цілих організацій.

Результатом нанесення шкоди інформаційним системам сьогодні найчастіше є діяльність висококваліфікованих зловмисних груп, які використовують багатовекторні атаки, фішинг, експлуатацію вразливостей та соціальну інженерію. Їхньою метою є отримання контролю над кінцевими точками, розгортання шкідливого програмного забезпечення, проведення lateral movement і, врешті-решт, досягнення контрольованого впливу на інфраструктуру. У цьому контексті EDR-рішення стають ключовим елементом протидії загрозам, адже забезпечують збір телеметрії, поведінковий аналіз і негайне реагування на спроби компрометації.

Особливу небезпеку становлять сучасні атаки шифрувальників, несанкціонованого доступу до корпоративних ресурсів та зловмисні дії всередині мережі, коли компрометація однієї кінцевої точки відкриває шлях до критично важливих систем. У таких випадках EDR-платформи дозволяють швидко локалізувати інцидент, заблокувати шкідливі процеси, відстежити ланцюжок дій злочинця та запобігти подальшому розповсюдженню загрози.

У рамках дослідження планується проаналізувати ефективність різних підходів до побудови систем виявлення та реагування на події на кінцевих точках, а також вивчити різноманітні апаратні та програмні рішення, що підсилюють можливості EDR у реальному корпоративному середовищі. Окрему увагу буде приділено сучасним моделям атаки, методам приховування активності шкідливих програм, а також інтеграції EDR із системами SIEM, SOAR та службами аналітики загроз.

Метою дослідження у кваліфікаційній роботі є оцінка ефективності EDR-рішень у протидії сучасним кіберзагрозам, аналіз їх здатності виявляти індикатори компрометації, поведінкові аномалії та проводити автоматизоване реагування. Дослідження також включає розробку рекомендацій для впровадження EDR у корпоративному середовищі та оптимізацію процесів обробки інцидентів.

Дослідження даної теми є не тільки теоретично важливим, але й практично значущим, оскільки впровадження ефективних систем виявлення та реагування дозволяє суттєво підвищити стійкість організації до кібератак, зберегти конфіденційність, цілісність та доступність даних, а також мінімізувати наслідки потенційних інцидентів.

Завданнями дослідження є:

– вивчити теоретичні основи роботи EDR-систем і їх роль у сучасній моделі кіберзахисту;

– проаналізувати сучасні підходи атак на кінцеві точки та їх вектори;

– дослідити принципи виявлення загроз, поведінковий аналіз та телеметрію EDR;

– провести порівняльний аналіз актуальних EDR-рішень та оцінити їх ефективність;

– розробити комплекс рекомендацій щодо оптимального впровадження EDR у мережеву архітектуру кінцевих точок;

– визначити переваги та обмеження EDR порівняно з іншими засобами кіберзахисту.

Об'єкт дослідження — сучасні системи кіберзахисту на рівні кінцевих пристроїв, їхні можливості та взаємодія з інфраструктурою безпеки.

Предмет дослідження — методи виявлення та реагування на події безпеки, принципи роботи EDR і взаємодія аналітичних модулів із телеметрією.

Практична значимість результатів полягає в тому, що дослідження дозволяє сформувати рекомендації для підвищення захищеності корпоративних середовищ, оптимізувати процеси реагування та мінімізувати наслідки інцидентів, які у сучасних умовах можуть бути критичними для діяльності підприємств.

Наукова новизна роботи полягає у комплексному підході до оцінки ефективності EDR-рішень у поєднанні з сучасними технологіями аналітики, машинного навчання та засобами автоматизації реагування, що є актуальним у період стрімкого розвитку кіберзагроз.

Методологія дослідження охоплює аналітичний огляд літератури, аналіз моделей атак, тестування EDR-рішень, порівняння їх можливостей, а також формування рекомендацій щодо впровадження найефективніших технологій для забезпечення безпеки корпоративних систем.

1 ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ПОДІЇ БЕЗПЕКИ (EDR)

1.1 Сучасні кіберзагрози та роль кінцевих точок у забезпеченні безпеки

Стрімка цифровізація бізнес-процесів, розширення використання хмарних сервісів та збільшення кількості підключених пристроїв суттєво ускладнили сучасний ландшафт кібербезпеки. Кінцеві точки — робочі станції, ноутбуки, сервери, мобільні пристрої — перетворилися на один із найважливіших елементів корпоративної інфраструктури, адже саме через них зловмисники найчастіше здійснюють початкове проникнення в мережу.

На рисунку 1.1, зображена статистика кіберзагроз стосовно різних секторів економіки, збитків, котрі були нанесені в результаті кібератак, та результативності цих кібератак за 2022-2024 роки [1].

Рисунок 1.1 – Аналіз статистики кіберзагроз за 2022–2024

На відміну від мережевих атак минулого, більшість сучасних загроз орієнтується не лише на уразливості програмного забезпечення, а й на людський фактор, набір поведінкових характеристик системи та можливість обходити класичні інструменти захисту. Фішингові кампанії, шкідливі вкладення, drive-by-завантаження, експлуатація zero-day вразливостей, fileless-атаки та багатоетапні сценарії APT стали щоденною практикою кіберзлочинців. Такий підхід дозволяє злочинцям уникати виявлення численними сигнатурними засобами, а також поступово та непомітно закріплюватися всередині організації.

Окрім цього, зловмисники активно використовують легітимні інструменти операційних систем (PowerShell, WMI, командні оболонки, служби віддаленого виконання), що ускладнює процеси моніторингу та реагування. У таких умовах саме кінцеві точки стають «першою лінією оборони», адже вони містять найбільш цінну телеметрію: інформацію про процеси, файли, мережеву активність, системні події й взаємодію користувачів з операційною системою.

Класичні антивірусні рішення вже не здатні ефективно протистояти подібним атакам. Їхній функціонал обмежений виявленням шкідливого програмного забезпечення за відомими сигнатурами, тоді як сучасні загрози часто не мають постійних ознак або взагалі не містять шкідливих файлів. У результаті навіть короткочасний доступ зловмисника до робочої станції може призвести до компрометації корпоративної мережі, викрадення конфіденційних даних, шифрування серверів чи зупинки важливих процесів.

У відповідь на зміни в поведінці злочинців виникла потреба у створенні нових засобів захисту, здатних аналізувати поведінкові шаблони, виявляти нетипові дії у реальному часі та автоматично блокувати загрози ще на ранніх етапах. Саме ці функції виконують системи EDR — сучасні платформи, спрямовані не тільки на фіксацію потенційно небезпечних подій, а й на активне запобігання розвитку атаки та швидке відновлення безпечного стану системи.

На рисунку 1.2 зображено графік росту нових вразливостей у реєстрі вразливостей CVE – Common Vulnerabilities and Exposures[2].

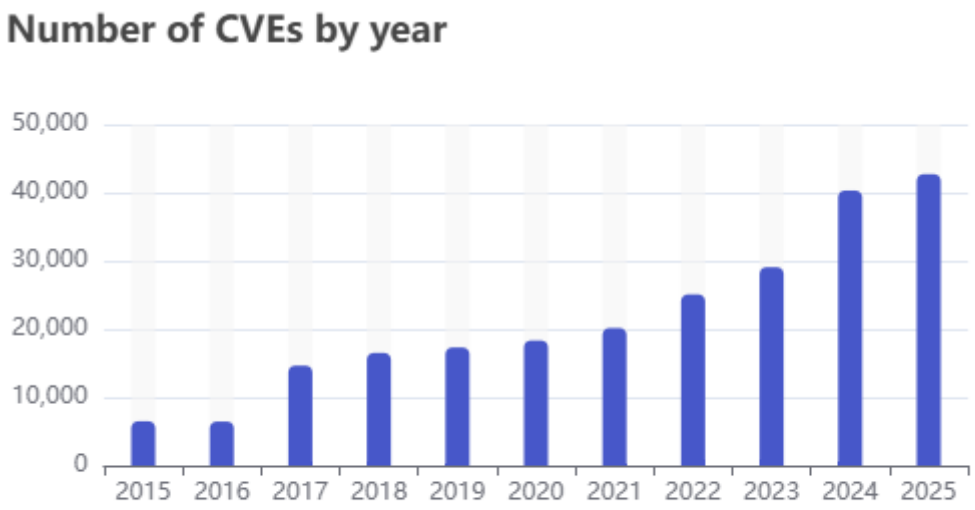

Рисунок 1.2 – Аналіз росту реєстру нових вразливостей по роках

Таким чином, роль кінцевих точок у моделі кіберзахисту постійно зростає, а їхній захист стає критично важливим елементом запобігання інцидентам безпеки. Розуміння природи сучасних кіберзагроз, їхніх принципів роботи та сценаріїв проникнення є фундаментальною основою для подальшого аналізу ефективності систем виявлення та реагування на події безпеки.

Зростання складності кіберзагроз посилюється ще й тим, що сучасні атаки все частіше здійснюються у формі багатоступеневих кампаній, де кожен етап виконує конкретну задачу: розвідку, проникнення, закріплення, розширення привілеїв та приховане пересування мережею. Це означає, що навіть незначна аномалія на кінцевій точці може бути ознакою масштабніших дій зловмисника, спрямованих на заволодіння критичними ресурсами організації. Саме тому швидке виявлення перших ознак компрометації є ключовим фактором мінімізації ризиків і збитків.

У багатьох випадках злочинці уникають створення нових файлів або внесення очевидних змін у систему. Вони можуть використовувати легітимні процеси для виконання шкідливих команд, запускати обфускований PowerShell-код або непомітно змінювати конфігурації системи. Такі дії складно виявити без застосування поведінкової аналітики, яка є основою EDR-рішень. На відміну від

традиційних механізмів, поведінковий підхід дозволяє побачити послідовність підозрілих подій у динаміці та визначити, чи формують вони шкідливий ланцюг.

Не менш важливим фактором стає зростання кількості віддалених робочих місць та мобільних співробітників, які підключаються до корпоративних систем поза периметром організації. Це створює додаткові можливості для зловмисників, оскільки кінцеві точки поза захищеною корпоративною мережею є значно більш уразливими. У таких умовах засоби захисту мають забезпечувати постійний контроль незалежно від розташування пристрою, що також входить до ключових функцій сучасних EDR-платформ.

Ще одним викликом є збільшення обсягу телеметрії, яка генерується пристроями. Без автоматизованих засобів аналізу виявлення загроз перетворюється на складний і трудомісткий процес. EDR-рішення використовують машинне навчання, алгоритми кореляції та моделі ризику, що дозволяє структурувати та аналізувати великі обсяги інформації в режимі реального часу. Це значно підвищує ефективність реагування та зменшує навантаження на аналітиків.

У сукупності всі ці фактори демонструють, що кінцеві точки перестали бути просто елементами інфраструктури — сьогодні вони є центральною платформою, на якій і відбувається основний фронт боротьби з кіберзагрозами. Саме тому дослідження їх захисту, а також оцінка ефективності EDR-систем у протидії сучасним атакам, є критично важливими завданнями для будь-якої організації, яка прагне зберегти стійкість і безперервність своєї діяльності [4].

1.2 Архітектура та ключові компоненти систем EDR

Системи EDR являють собою комплексні програмно-аналітичні рішення, які забезпечують багаторівневий контроль за станом кінцевих точок та їх поведінкою. На відміну від традиційних засобів захисту, EDR не обмежується

лише виявленням відомих загроз — головним завданням платформи є створення безперервної видимості всієї активності на пристроях користувачів і серверів, а також можливість оперативно реагувати на дії, які можуть свідчити про компрометацію.

Основу архітектури EDR становлять кілька ключових компонентів, кожен з яких виконує свою унікальну роль у процесі моніторингу та реагування. Першим елементом є агент, встановлений на кінцевій точці. Він працює у фоновому режимі та фіксує широкий спектр подій: створення і зміну файлів, запуски процесів, мережеві підключення, використання системних API, виконання скриптів, роботу служб і взаємодію користувача з програмним забезпеченням. Агенти створені таким чином, щоб працювати з мінімальним впливом на продуктивність пристрою, але забезпечувати максимально деталізоване відстеження дій, що є критичним для своєчасного виявлення підозрілої поведінки.

Другим ключовим компонентом виступає сервер обробки та координації, який отримує телеметрію з усіх кінцевих точок. Саме тут відбувається агрегування даних, їх нормалізація, кореляція та застосування аналітичних моделей для визначення ризикових або нетипових дій. У більшості сучасних рішень ці процеси працюють у хмарній інфраструктурі, що дозволяє масштабувати продуктивність та використовувати глобальні моделі загроз.

Не менш важливою частиною архітектури є аналітичний модуль, який відповідає за виявлення підозрілих дій. Він використовує евристичні методи, поведінковий аналіз, аналіз ланцюжків подій та машинне навчання. Завдяки цьому EDR здатні виявляти складні типи загроз, включно з тими, які не мають сигнатур або використовують легітимні системні інструменти. Наприклад, хакер може запускати обфускований PowerShell-код або виконувати підозрілі дії через WMI — і саме аналітичні механізми EDR дозволяють виявити такі сценарії навіть без конкретних індикаторів компрометації [5].

Ще одним обов’язковим елементом є модуль реагування, який дозволяє автоматично або вручну виконувати дії щодо блокування загроз. Серед типових

можливостей: ізоляція пристрою від мережі, завершення шкідливих процесів, блокування небезпечних виконуваних файлів, відкат змін у системі та усунення елементів, пов’язаних з компрометацією. Завдяки цьому EDR стає не лише інструментом спостереження, а й активним компонентом захисту.

Інтеграція EDR з іншими системами кіберзахисту, такими як SIEM, SOAR або NDR, дозволяє отримати розширений контекст та будувати комплексну картину подій. Наприклад, взаємодія з SIEM забезпечує централізований аналіз усієї інфраструктури, а інтеграція з SOAR дозволяє автоматизувати складні сценарії реагування [7].

Таким чином, архітектура EDR — це цілісна екосистема, спрямована на виявлення найменших відхилень у роботі системи, їх аналіз і швидке реагування. Її ключова перевага полягає у поєднанні високої деталізації телеметрії, гнучкої аналітики та можливостей негайного втручання, що дозволяє значно зменшити ризики компрометації та мінімізувати можливі наслідки кіберінцидентів.

Ще одним важливим елементом архітектури EDR є система зберігання та індексації даних, яка відповідає за організацію великого масиву телеметрії, що надходить від агентів. Зазвичай такі дані містять мільйони подій, тому сучасні платформи використовують високопродуктивні бази даних, оптимізовані під швидкий пошук та кореляцію. Завдяки цьому аналітик або автоматизована система можуть миттєво отримати відповідь на запит щодо конкретного процесу, IP-адреси чи події та зрозуміти, як вони пов’язані з іншими діями на пристрої [8].

Не менш значущою частиною архітектури є модуль візуалізації, який дозволяє представити складні ланцюжки атак у наочному вигляді. Сучасні EDR-рішення формують графічні карти інцидентів, де кожна дія — створення процесу, мережеве підключення чи зміна реєстру — відображається у вигляді вузлів і зв’язків. Це значно полегшує аналіз та пришвидшує усвідомлення того, які саме кроки зробив злочинець або хакер у системі.

Суттєву роль відіграє також політико-управлінська частина EDR, яка визначає, як саме система має реагувати на різні події. Без чітко налаштованих правил навіть найфункціональніший інструмент може працювати неефективно.

У межах цього модуля визначаються політики ізоляції, дозволені або заборонені дії, рівні критичності подій та сценарії автоматичного реагування. Це дозволяє адаптувати EDR до специфіки конкретної організації і підвищити точність виявлення загроз.

Окремою складовою EDR є можливість інтеграції з інфраструктурою організації. Сучасні платформи передбачають обмін даними з Active Directory, SIEM, SOAR, системами керування вразливостями, а також взаємодію з зовнішніми API. Така інтеграція дозволяє не лише отримувати контекст щодо подій, а й автоматизувати складні процеси реагування: наприклад, EDR може передавати деталі інциденту до SIEM, який у свою чергу активує SOAR-сценарій для виконання низки дій[6].

До архітектури EDR також входить механізм оновлення аналітичних моделей та правил виявлення. Він працює як у фоні, так і під час інтерпретації нових подій. Продавці рішень регулярно оновлюють такі моделі відповідно до актуальних TTPs злочинців, нових методів обходу захисту та технік приховування слідів. Таким чином платформа постійно адаптується до змін у кіберзагрозах.

Нарешті, важливою особливістю архітектури EDR є багаторівнева система доступу, яка забезпечує контроль над тим, хто може переглядати, аналізувати або змінювати дані. Це захищає як саму платформу від маніпуляцій, так і конфіденційну інформацію, яку вона обробляє.

У сукупності всі компоненти — агенти, сервери аналізу, автоматизовані модулі реагування, бази даних, механізми Threat Intelligence, інтерфейси візуалізації та інтеграційні засоби — формують цілісну екосистему. Вона дозволяє не лише своєчасно виявляти дії злочинця або хакера, а й швидко локалізувати інцидент, мінімізувати ризики та забезпечити відновлення нормальної роботи системи. Така структура визначає EDR як один із ключових засобів у сучасній моделі кіберзахисту [10].

1.3 Принципи роботи EDR-систем та їх роль у протидії сучасним загрозам

Функціонування систем EDR ґрунтується на комплексному підході, який поєднує глибокий збір телеметрії, аналітичні механізми виявлення аномалій та швидкість реагування на загрози. На відміну від класичних інструментів захисту, що працюють переважно за сигнатурним принципом, EDR орієнтується на аналіз поведінки кінцевих точок і встановлення контексту кожної дії, що дозволяє ефективно протидіяти навіть складним технікам, які використовує сучасний злочинець чи хакер.

Першою ключовою ланкою в роботі EDR є постійний моніторинг системної активності. Агент EDR відстежує усі події на кінцевій точці: модифікацію файлів, створення процесів, зміни в реєстрі, роботу служб, запуски скриптів, мережеві з’єднання та інші системні взаємодії. Це створює детальну «поведінкову карту» пристрою, що дозволяє виявляти підозрілі дії навіть тоді, коли вони зовні виглядають як легітимні.

Наступний принцип — аналіз поведінки (behavior-based detection). EDR не просто фіксує подію, а оцінює її з урахуванням контексту та послідовності. Типовий приклад — сценарій, коли хакер запускає PowerShell із прихованими параметрами, читає мережеві ресурси, змінює політики безпеки та встановлює з’єднання зі стороннім сервером. Кожна з цих дій окремо може виглядати безпечною, але в сукупності вони формують чітку ознаку компрометації, яку EDR здатен розпізнати [11].

Третім принципом є кореляція подій і створення ланцюжків атаки. Система не обмежується одиничними інцидентами, а формує повноцінну хронологію дій на скомпрометованому хості. Це дозволяє оперативно зрозуміти, з чого почалося вторгнення, як саме злочинець просувався системою і які компоненти були скомпрометовані. Така функціональність є критично важливою для швидкого реагування та подальшого розслідування інциденту.

Окрему роль відіграє взаємодія з Threat Intelligence — глобальними джерелами даних про активність хакерських угруповань, їх інструменти, індикатори компрометації та TTPs. EDR використовує ці дані для порівняння подій, що відбуваються на кінцевих точках, з відомими шаблонами дій злочинців. Це дозволяє своєчасно виявляти нові кампанії, навіть якщо вони ще не мають сигнатур.

Додатковим принципом є автоматизоване реагування, яке включає ізоляцію пристрою, блокування процесів, завершення сесій або відкат шкідливих змін. Це забезпечує оперативне припинення атаки навіть без участі аналітика SOC, що є важливим у випадках, коли час реагування відіграє критичну роль.

Завдяки сукупності цих механізмів EDR виступає одним із найбільш ефективних інструментів протидії сучасним загрозам — від шкідливих програм до багатоетапних вторгнень. Система не лише фіксує факт підозрілої поведінки, але й дозволяє мінімізувати вплив інциденту, забезпечуючи безперервність роботи корпоративної інфраструктури.

Попри значні переваги, EDR-рішення не можуть вважатися повністю самодостатніми, оскільки ефективність їх роботи багато в чому залежить від здатності організації належно інтегрувати їх у загальну архітектуру безпеки. Одним з ключових викликів є потреба у кваліфікованих спеціалістах, які здатні аналізувати телеметрію, корелювати події та вчасно реагувати на інциденти. Навіть найсучасніша EDR-платформа не замінює людського фактору, а лише підсилює можливості аналітиків SOC, зменшуючи кількість рутинних задач.

Важливим аспектом є і той факт, що EDR створює значний обсяг даних, які потребують збереження, обробки та аналізу. Це вимагає потужної інфраструктури, достатнього обсягу пам’яті та пропускної здатності каналів передачі даних. У великих організаціях кількість телеметрії може вимірюватися терабайтами на добу, що робить критично необхідними механізми оптимізації та фільтрації даних.

Крім того, EDR-системи працюють переважно на рівні кінцевих точок, а отже не завжди здатні повністю охопити складні міжмережеві сценарії або атаки,

які починаються на мережевому рівні. Хоча більшість сучасних рішень підтримують кореляцію з SIEM або XDR-платформами, сама по собі EDR не забезпечує повного огляду всієї інфраструктури. Тому найкращий результат досягається у поєднанні EDR з мережевими системами виявлення загроз (NDR) та аналітичними платформами, що дозволяє покривати як кінцеві точки, так і мережевий трафік [12].

Ще одним обмеженням є можливість обходу EDR у випадках, коли хакер здійснює так звані fileless-атаки або використовує інструменти, які не створюють артефактів на диску. Хоча сучасні EDR-рішення здатні виявляти ознаки подібної активності, такі техніки постійно вдосконалюються, що потребує регулярних оновлень алгоритмів детекції та моделей поведінки.

Незважаючи на ці обмеження, важливо відзначити, що EDR-платформи відіграють ключову роль у захисті від сучасних загроз. На відміну від традиційного антивірусу, який реагує лише на вже відомі сигнатури, EDR здатен виявити дії злочинця на роки новіші, ніж наявні в базах даних шкідливого ПЗ. Це забезпечує суттєву перевагу у протидії складним атакам, де хакери використовують індивідуально розроблені інструменти або експлойти нульового дня.

Таким чином, EDR є тим елементом, який формує новий рівень захисту сучасних інформаційних систем — рівень, де виявлення загроз базується не лише на сигнатурах, а на розумінні поведінки, контексту та ланцюгів дій хакера. Саме інтеграція поведінкової аналітики, автоматизації та можливостей швидкого реагування робить такі рішення фундаментально важливими у сучасному ландшафті кібербезпеки.

Додатково, важливим аспектом, який демонструє як переваги, так і певні обмеження EDR-платформ, є те, як саме вони взаємодіють з іншими компонентами системи кіберзахисту. Оскільки більшість сучасних атак здійснюється у кілька етапів, ефективність захисту залежить від здатності EDR не лише фіксувати окремі події, а й інтегруватися в загальну екосистему безпеки: SIEM, SOAR, NDR або XDR-рішень. У результаті формується багаторівневий

підхід до аналізу загроз, де кожен інструмент відіграє свою роль, а EDR забезпечує «низовий» рівень контролю — безпосередньо на кінцевій точці [14].

Окрему увагу варто приділити тому, як EDR поводиться під час багатоступеневих атак, де хакер поступово рухається мережею, використовуючи техніки lateral movement, credential dumping, privilege escalation тощо. Традиційні засоби безпеки часто фіксують окремі події, які виглядають нешкідливими, але EDR формує повний ланцюжок дій — від початкового запуску PowerShell-скрипту до підозрілих спроб доступу до адміністративних ресурсів.

На рисунку 1.3 зображено порівняльний аналіз програмних рішень Антивірусу, EDR та XDR за їх функцією, методикою, призначенням та ціною впровадження.

Рисунок 1.3 – Графічний порівняльний аналіз рішень Антивірусів EDR та XDR

Достатньо важливий напрямок, що підлягає широкому розкриттю, — це баланс між рівнем телеметрії, яку збирає система, і впливом на продуктивність кінцевих точок. Хоча більшість сучасних платформ оптимізовані для мінімального навантаження, у середовищах з великою кількістю робочих станцій EDR може збільшити споживання оперативної пам’яті, навантаження на процесор або мережевий трафік [13].

Ще одним перспективним аспектом є роль EDR у сучасних моделях Zero Trust. У цій парадигмі кінцева точка вважається потенційно недовіреною, і саме EDR виступає тим механізмом, який забезпечує безперервне оцінювання стану пристрою. Тобто рівень доступу може змінюватися в режимі реального часу відповідно до поведінки системи і дій користувача.

Хоча EDR має розширені можливості аналізу поведінки, деякі техніки злочинців усе ще становлять складність для систем. Частина з них включає:

- використання легітимних інструментів Windows (LOLBins);
- безфайлові атаки;
- експлуатацію вразливостей у драйверах ядра;
- тимчасове відключення або обходження сенсорів EDR [15].

1.4 Компонентна архітектура систем виявлення та реагування на загрози на кінцевих точках

Архітектура сучасних EDR-рішень побудована таким чином, щоб забезпечити безперервний моніторинг кінцевих точок, збір максимально повної телеметрії та можливість оперативного реагування на дії злочинця або хакера. У своїй основі EDR поєднує декілька взаємопов’язаних компонентів, кожен з яких виконує специфічну функцію у ланцюжку детекції та реагування. Така модульна структура дозволяє EDR працювати як автономно, так і в рамках комплексних систем безпеки, включаючи XDR, SIEM чи SOC-платформи.

Центральним елементом архітектури є агент EDR, встановлений на кожну кінцеву точку. Саме він виконує первинний збір подій, таких як запуск процесів, взаємодія між додатками, системні виклики, доступ до файлової системи, зміни в реєстрі та мережеві з’єднання. Агент також здійснює локальні перевірки на наявність аномальної поведінки або ознак компрометації, що дозволяє виявляти

підозрілу активність навіть у випадку тимчасової відсутності з'єднання з центральним сервером.

Надалі зібрана інформація передається до централізованої платформи обробки та аналітики, яка може розташовуватися у хмарному середовищі або в локальній інфраструктурі організації. На цьому рівні застосовуються алгоритми кореляції, машинного навчання та поведінкової аналітики, що дозволяє перетворювати великі обсяги телеметрії на структуровані інциденти та визначати, чи є певна активність частиною шкідливого ланцюжка дій.

Зазначений компонент доцільно відобразити у вигляді окремої схеми, яка демонструє послідовність обробки даних від агента кінцевої точки до етапу формування інциденту [16].

На рисунку 1.4 можна побачити схематичне зображення принципу роботи архітектури EDR-рішень.

Рисунок 1.4 – Принцип роботи архітектури EDR

Важливою складовою архітектури EDR є модуль реагування, який забезпечує можливість оперативно нейтралізувати загрозу. Залежно від можливостей конкретного рішення це може включати блокування шкідливого

процесу, ізоляцію пристрою від мережі, примусове завершення сесії користувача, видалення шкідливих файлів або запуск автоматизованих скриптів для усунення наслідків. Цей рівень особливо критичний у випадках, коли хакер намагається здійснити швидку ескалацію доступу або використати уразливість для подальшого проникнення.

Ще одним важливим елементом є інтерфейс аналітика, за допомогою якого оператори SOC отримують доступ до інцидентів, історії подій, контекстних даних та інструментів розслідування. Інтерфейси сучасних EDR-систем дозволяють відтворювати повний ланцюжок дій злочинця, аналізувати часові залежності, переглядати дерево процесів і виявляти первинне джерело компрометації.

Багато постачальників EDR також включають у свою архітектуру модуль інтеграції, що дозволяє обмінюватися подіями з SIEM або іншими системами безпеки. Це забезпечує побудову розширеної платформи XDR, де дані з кінцевих точок поєднуються з інформацією з мережевого обладнання, хмарних сервісів, проксі-серверів тощо. Завдяки цьому аналітики отримують повний огляд подій у різних сегментах інфраструктури, а інциденти можуть бути оброблені у контексті ширшої картини.

Також сучасні EDR-платформи мають модуль Threat Intelligence, який дозволяє системі мати доступ до актуальних даних про нові тактики, техніки та процедури хакерів, зразки шкідливого ПЗ та поведінкові патерни. Інтеграція з TI-платформами підвищує ймовірність раннього виявлення складних атак та знижує ризик успішного обходу системи.

Таким чином, архітектура EDR являє собою комплекс взаємодіючих компонентів, які забезпечують замкнений цикл «виявлення → аналіз → реагування». Така модульність дозволяє досягти високого рівня ефективності як у традиційному IT-середовищі, так і в гібридних інфраструктурах, де поєднуються сервери, робочі станції, хмари та мобільні пристрої [17].

Висновок: У першому розділі було здійснено комплексне дослідження фундаментальних аспектів систем виявлення та реагування на події безпеки

(EDR), їхніх принципів роботи, архітектури та ролі у сучасному ландшафті кіберзагроз. Отримані результати дозволяють сформувати цілісне уявлення про те, чому системи EDR стали ключовим елементом сучасних підходів до захисту інформації та чому їх впровадження є критично важливим у середовищі, де зловмисники — хакери чи організовані кіберзлочинні групи — застосовують дедалі складніші та витончені методи атак.

У межах розділу було з’ясовано, що розвиток сучасних кіберзагроз характеризується не лише зростанням їх кількості, але й стрімким підвищенням рівня новизни та складності. Хакери дедалі частіше використовують багатоступеневі атаки, інструменти приховування активності, безфайлові техніки, шкідливі інтерпретатори у вигляді вбудованих системних утиліт, а також методи обходу сигнатурних механізмів. За таких умов традиційні засоби захисту демонструють суттєві обмеження, оскільки здебільшого реагують лише на відомі зразки шкідливого ПЗ та не здатні виявляти аномальну поведінку системи. Це аргументує необхідність переходу до поведінкових та аналітичних рішень, основою яких є EDR.

Було доведено, що EDR формує якісно інший рівень контролю над кінцевими точками, забезпечуючи глибоку телеметрію та можливість моделювання повної картини дій хакера — від первинного проникнення до потенційної ескалації привілеїв і горизонтального переміщення в мережі. Завдяки побудові ланцюжків подій, використанню машинного навчання та поведінкових алгоритмів EDR здатен виявляти атаки, які маскуються під легітимні дії користувачів або системних процесів.

Особливу увагу було приділено архітектурі EDR-систем, що включає агентів кінцевих точок, центральні аналітичні вузли, модулі машинного навчання, системи зберігання телеметрії, засоби автоматичного реагування та інтерфейси для аналітиків SOC. Було показано, що ця архітектура забезпечує замкнений цикл «спостереження → аналіз → рішення → реагування», що дозволяє мінімізувати час між виявленням інциденту та його нейтралізацією. Це

є надзвичайно важливим у випадках, коли злочинець намагається швидко розвинути свою присутність у системі.

Крім того, було встановлено, що EDR найбільш ефективно працює як частина комплексної моделі безпеки, яка включає SIEM, SOAR, NDR та XDR-компоненти. Така інтеграція дозволяє розширити контекст аналізу, зіставляючи події не лише з окремого пристрою, але й із мережевої, хмарної, інфраструктурної або базової логової інформації. Це суттєво підвищує точність виявлення та зменшує кількість хибнопозитивних сповіщень.

У рамках розділу було також окреслено низку обмежень EDR, таких як потреба у висококваліфікованих фахівцях SOC, значні вимоги до обчислювальних ресурсів та ризики, пов’язані зі спробами обходу або відключення сенсорів на кінцевих точках. Разом з тим ці обмеження не нівелюють переваг, оскільки EDR залишається єдиним інструментом, здатним забезпечити повноцінний контроль поведінки системи на рівні користувача, процесів та внутрішньої логіки операційної системи.

Узагальнюючи проведений аналіз, можна стверджувати, що системи EDR є критично важливим елементом сучасної кібероборони. Вони дозволяють створити адаптивний, інтелектуальний та проактивний механізм реагування на загрози, який значною мірою знижує ризики компрометації та забезпечує стабільність роботи інформаційних систем навіть у умовах інтенсивної діяльності злочинців. Розуміння архітектури, функціоналу та можливостей EDR є основою для розробки ефективної моделі захисту та подальшої оцінки її результативності у практичних сценаріях, що й закладає фундамент для наступних розділів дипломної роботи.

2 АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ТА ПРОТИДІЇ СУЧАСНИМ КІБЕРЗАГРОЗАМ З ВИКОРИСТАННЯМ EDR-СИСТЕМ

2.1 Класифікація сучасних кіберзагроз та особливості їхнього розвитку

Сучасний ландшафт кіберзагроз є надзвичайно динамічним і характеризується постійною еволюцією технік, інструментів та сценаріїв атаки. Хакери та організовані злочинні угруповання застосовують дедалі більш складні методи проникнення у системи, використовуючи як технічні вразливості, так і помилки користувачів. У цій частині роботи проведено систематизований аналіз основних видів загроз, які є актуальними для сучасних IT- та корпоративних інфраструктур, а також тих, що безпосередньо впливають на роботу EDR-систем.

Передусім варто зазначити, що класичні категорії шкідливого програмного забезпечення — віруси, черв'ячі програми, трояни — поступово поступаються місцем більш комплексним загрозам. Нині акцент переноситься на багатостадійні атаки, де хакер використовує комбінацію різних технік для досягнення своїх цілей. Такий підхід добре відомий у контексті моделі MITRE ATT&CK, яка класифікує загрози за поведінковими ознаками, а не за типом шкідливого ПЗ [7].

Одним із ключових типів сучасних загроз є fileless-атаки, у яких хакер не використовує традиційні виконувані файли. Натомість ураження здійснюється через PowerShell, WMI, LOLBins (легітимні бінарні файли Windows) та інші інструменти системи. Ці атаки складно виявити сигнатурним способом, оскільки вони не залишають класичних артефактів на диску. У цьому контексті EDR відіграє важливу роль: аналіз поведінки дозволяє виявити аномальні виклики команд, підозрілу активність скриптів або нехарактерні запуски служб.

Другим важливим класом загроз є атаки на облікові записи. Використання викрадених паролів, brute-force, credential stuffing, session hijacking стало одним із найпоширеніших шляхів компрометації корпоративних систем. У подібних випадках EDR забезпечує детекцію підозрілої автентифікаційної активності, а

також відслідковує аномалії у поведінці користувача — наприклад, запуск процесів, не характерних для його робочих функцій.

Окрему групу складають атаки на вразливості програмного забезпечення — експлойти, що використовують щойно опубліковані або раніше невідомі (нульового дня) вразливості. Вони дозволяють хакеру отримати контроль над системою без взаємодії з користувачем. У таких сценаріях EDR здатен виявити підозрілу активність на рівні процесів, наприклад, створення нових потоків у системних службах або спроби виконання shell-коду [9].

Не менш небезпечними є атаки типу lateral movement, коли хакер після первинного проникнення починає переміщуватися мережею, збираючи привілеї та доступи. Для виявлення таких дій EDR використовує процесні дерева, графи взаємодій, кореляцію запитів до внутрішніх ресурсів і поведінкові моделі, що дозволяють розпізнати відхилення від нормальної активності.

Останніми роками спостерігається стрімке зростання інцидентів, пов’язаних із цільовими атаками (APT). Вони включають тривалу присутність хакера в системі, ретельне приховування слідів та використання унікальних інструментів. Саме для таких сценаріїв EDR є найбільш ефективним, оскільки дозволяє виявити навіть мінімальні аномалії в поведінці пристроїв [17].

Таким чином, розвиток сучасних кіберзагроз вимагає застосування інструментів нового покоління, які не лише реєструють відомі зразки шкідливого ПЗ, але й здатні аналізувати поведінку системи, корелювати події та знаходити ознаки злочинної активності, які приховані від традиційних механізмів. Усе це підкреслює важливість EDR у формуванні комплексної системи кіберзахисту.

Важливо підкреслити, що зростання складності кіберзагроз пов’язане не лише з технічним прогресом, але і з тим, що хакери активно використовують соціальні та психологічні фактори. До прикладу, соціальна інженерія залишається одним із найпоширеніших способів початкового проникнення до корпоративної інфраструктури. Фішинг, spear-phishing, бізнес-компрометація електронної пошти (BEC), SMS-шахрайство та атаки через месенджери створюють передумови для запуску шкідливих макросів, компрометації

облікових записів або встановлення шкідливих інструментів віддаленого керування. У таких випадках системи EDR допомагають виявити підозрілі дії навіть після того, як початковий обман вдався — наприклад, коли користувач запускає документ із прихованим VBA-скриптом або коли з'являються нетипові з'єднання із зовнішніми серверами [8].

Значної уваги заслуговують і безфайлові інструменти віддаленого доступу, такі як інжектори коду, утиліти динамічного аналізу або легітимні адміністративні інструменти (RDP, TeamViewer, AnyDesk). Хоча ці засоби широко використовуються системними адміністраторами, злочинці можуть застосовувати їх для прихованого встановлення контролю над системою. Перевага EDR полягає в тому, що він здатен відслідковувати контекст, у якому запускається такий інструмент: з якого процесу він ініційований, які дозволи використовує, якими командами супроводжується.

Не менш важливою категорією загроз є фреймворки для автоматизації атак, такі як Cobalt Strike, Metasploit, Sliver, Empire. Ці інструменти дають хакерам змогу здійснювати командування та контроль (C2), розгортати бекдори, виконувати обхід захисту та управляти інфікованими вузлами. Хоча Cobalt Strike часто виявляється за сигнатурами, його численні форки, модифікації та кастомні конфігурації роблять традиційне детектування малоефективним. У таких випадках EDR є одним із небагатьох засобів, здатних помітити нетипові взаємодії процесів, ін'єкції в пам'ять, підозрілі мережеві з'єднання та аномальні дії на рівні користувача [13].

Особливо швидко розвивається напрямок кібершпіонажу та цільових атак на критичну інфраструктуру (ICS/OT). Хоча ці атаки спрямовані переважно на державні та стратегічні підприємства, їх вплив може бути катастрофічним. Сучасні APT-групи застосовують широкий спектр технік: від експлуатації нульових днів до використання легітимних промислових протоколів для маскування дій у технологічних середовищах. У таких випадках EDR забезпечує критично важливі функції:

- виявлення аномальної поведінки користувачів і системних служб;

- фіксацію запуску рідкісних або нестандартних інструментів;
- ідентифікацію несанкціонованих спроб доступу до критичних ресурсів;
- блокування lateral movement через RDP, SMB, WinRM тощо.

Ще одна категорія, яка набуває поширення, — мультиланцюгові атаки зі штучним інтелектом та автоматизованими скриптами, які здатні адаптувати свої дії у реальному часі. Такі атаки можуть змінювати поведінку залежно від рівня протидії, створювати унікальні сліди у системі та автоматично модифікувати інструменти обходу EDR. Це новий тип загрози, який особливо актуальний у 2024–2025 роках. Традиційні засоби захисту часто виявляються неефективними проти таких атак, тоді як EDR, завдяки поведінковим механізмам і машинному навчанню, має змогу розпізнавати відхилення навіть у таких умовах.

Також важливо відзначити значний ріст реконфігурованих та модульних загроз, де шкідливе ПЗ складається з окремих компонентів, що завантажуються у систему лише за потреби. Подібні атаки практично не залишають артефактів на диску, оскільки більша частина роботи виконується у пам’яті. Тут EDR із можливістю Memory Scanning та контролю API-викликів стає незамінним інструментом.

Загалом аналіз свідчить, що сучасні кіберзагрози еволюціонують у напрямку:

- меншої видимості;
- більшої складності;
- вищого рівня автоматизації;
- активного використання легітимних компонентів ОС;
- глибшої інтеграції у поведінковий контекст користувача.

Це формує чіткий запит на системи, здатні не лише фіксувати події, але й розуміти логіку їх виникнення та взаємозв’язки — що й становить основу роботи EDR [18].

2.2 Сучасні та майбутні кіберзагрози: прогнози ENISA та вплив на ефективність EDR-систем

У 2022 році ENISA оприлюднила дослідження під назвою Cybersecurity Threats Fast-Forward 2030, в рамках якого був проаналізований потенційний розвиток кіберзагроз до 2030 року.

На рисунку 2.1, можна побачити зображеня 10 кіберзагроз, котрі прогнозують на 2030 рік [5].

Рисунок 2.1 – Прогнозовані нові актуальні загрози на 2030 рік

У документі визначено десятку головних загроз, які, за очікуваннями, можуть стати критичними в середньостроковій перспективі. Серед них:

- компрометація ланцюгів постачання - особливо через залежності програмних компонентів;
- зловживання штучним інтелектом (AI), як засобом для автоматизації атак, генерації фішингових кампаній, deepfake-маніпуляцій, а також використання нових технологій для створення складних атак;
- зростання гібридних загроз - поєднання кібер-фізичних та інформаційних впливів, аналогічне зростання ризиків для кібер-фізичних систем, зокрема тих, що мають стару, «спадкову» архітектуру;

- концентрація ризиків через залежності від хмарних/міжмережевих або транскордонних ІКТ-постачальників - це створює єдину точку відмови, що є особливо небезпечним для критичних систем.
- дефіцит кваліфікованих фахівців з кібербезпеки (skills shortage), що погіршує здатність реагувати на інциденти.

У 2024 — 2025 роках ENISA також фіксує, що багато з «майбутніх» загроз вже проявляються сьогодні, хоч і в трансформованому вигляді: технологічне оновлення, розповсюдження хмарних рішень, зростання складності ланцюгів поставок, комбіновані атаки, використання AI тощо.

На рисунку 2.2, можна побачити зображеня ландшафту найпопулярніших загроз інформаційній безпеці станом на 2024 рік [6].

Рисунок 2.2 – «Ландшафт загроз інформаційної безпеки 2024 року»

Таким чином, прогноз ENISA не виглядає спекулятивним — він базується на трендах, що вже набули реального прогресу, і описує не просто гіпотетичні загрози, а напрями, за якими еволюція атак вже йде зараз [6].

- Аналіз звітів ENISA Threat Landscape 2025 і раніше (2024) підтверджує, що сучасні загрози залишаються різноплановими та адаптивними. Серед найбільш поширених: Атаки на доступність: розподілені атаки відмови в обслуговуванні (DDoS), які стають набагато масштабнішими, швидшими та дешевшими у реалізації;

- Програми-вимагачі (ransomware) — що залишаються однією з найнебезпечніших форм кібератак з точки зору наслідків для бізнесу та критичної інфраструктури;
- Атаки на програмне забезпечення та ланцюги постачання: використання zero-day-вразливостей, підміна сторонніх компонентів, атаки через залежності — ті, які ENISA визначала як критичні на 2030, вже зараз набирають обертів;
- Комбіновані та гібридні атаки, які поєднують елементи: фішинг / соціальна інженерія, мережеві атаки, шкідливе ПЗ, атаки на ланцюги постачання, а також — використання технологій, таких як AI або автоматизація;

Зростання цілей серед критичної інфраструктури, промислових систем, OT/ICS-сектору — через посилення залежності від цифрових рішень: систем управління, хмар, зовнішніх постачальників і мережевого з'єднання.

Ці тенденції демонструють, що загрози вже зараз набувають рис, які ENISA передбачала як «тренди 2030», що робить впровадження сучасних механізмів захисту — зокрема EDR — стратегічно важливим.

У світлі вищевикладених тенденцій традиційні моделі безпеки (фаєрволи, антивірус із сигнатурами, базова сегментація) все більше втрачають ефективність. Основні причини — неспроможність детектувати нові та модульні, безфайлові чи комбіновані атаки, відсутність контексту поведінки, нездатність реагувати швидко, обмежена видимість кінцевих точок [6].

У такій ситуації EDR-системи, які забезпечують:

- глибокий збір телеметрії кінцевих точок;
- поведінковий аналіз і моделювання аномалій;
- кореляцію подій і побудову ланцюгів атак;
- швидке реагування (ізоляція, блокування, відкат);

забезпечують себе, як один із найефективніших інструментом, який здатен відповісти на складні, багатоетапні та швидко еволюційні загрози, прогнозовані на 2030 рік.

Крім того, EDR дає можливість активно моніторити середовище, навіть якщо загроза ще не проявила себе явно — забезпечуючи не лише реакцію після

інциденту, а превентивний контроль та забезпечення стійкості до нових типів атак [6].

Стовідсоткової гарантії захисту від усіх кіберзагроз не існує, тому не варто вважати системи EDR «Магічною кулею», проте аналіз прогнозів ENISA на 2030 рік у поєднанні з реальними інцидентами 2024-2025 років показує: існуюча безпекова модель має змінюватися, і EDR — ключовий елемент цієї трансформації.

Подальші розділи, присвячені тестуванню, оцінці ефективності або розробці рекомендацій, мають враховувати як класичні загрози, так і ті, що прогнозовані на майбутнє — зокрема, мультивекторні, гібридні, AI-орієнтовані та складні цільові атаки.

Це створює міцну основу для обґрунтування необхідності EDR як частини стратегії кіберзахисту, особливо для критичних систем, інфраструктур та корпоративних мереж, що прагнуть мати довгострокову кіберстійкість [6].

2.3 Роль та еволюція EDR у сучасній архітектурі кіберзахисту

У сучасному середовищі кіберзагроз, яке за останні роки стало значно динамічнішим, агресивнішим та технологічно складнішим, системи виявлення та реагування на події безпеки (Endpoint Detection and Response, EDR) відіграють ключову роль у забезпеченні стійкості IT-інфраструктури. Еволюція цих систем є прямою відповіддю на той факт, що традиційні механізми захисту — антивірусні рішення, класичні брандмауери та системи контролю доступу — все частіше демонструють обмежену ефективність проти сучасних загроз. Ті зловмисні дії, які раніше можна було виявити за допомогою статичних сигнатур або простих правил, нині набули форм складних багатоступеневих атак, часто безфайлових, орієнтованих на використання легітимних системних

інструментів, а також таких, що приховують власну активність у звичайному системному трафіку.

Саме ця трансформація середовища загроз стала основою для переходу до поведінкового підходу, який лежить в основі EDR. На відміну від класичних засобів, EDR не обмежується перевіркою файлів та сигнатур; його основна функція — постійний глибокий моніторинг кінцевих точок, збір детальної телеметрії та аналіз поведінкових моделей. Такі системи відстежують процеси, системні виклики, зміни в пам’яті, взаємодію між файлами та службами, мережеву активність і взаємодію користувача з системою. Це дозволяє EDR виявляти навіть ті загрози, які раніше не були відомі або які не мають характерних сигнатур.

Важливою особливістю сучасних EDR-рішень є здатність не лише фіксувати підозрілу активність, але й автоматично реагувати на інциденти. Система може ізолювати уражений хост, примусово завершити шкідливий процес, заблокувати мережеві з’єднання або ініціювати збір цифрових артефактів для подальшого аналізу. В умовах, коли атаки поширюються за лічені хвилини, а інфраструктури стають дедалі складнішими, швидка автоматизована реакція є критичною.

Не менш значущим є те, що EDR дає можливість відтворювати повний ланцюг атаки — від початкової точки проникнення до етапів lateral movement, ескалації привілеїв та спроби закріплення в системі. Така реконструкція є незамінною при розслідуванні інцидентів, виявленні вразливостей та побудові довгострокової стратегії захисту. Завдяки цьому EDR стає не лише інструментом оперативного реагування, але й потужним аналітичним засобом.

Зростаюче значення EDR активно підкріплюється прогнозами міжнародних аналітичних центрів, зокрема ENISA, яка у своїх дослідженнях наголошує на швидкій трансформації загрозового ландшафту. Прогнози ENISA щодо кіберзагроз 2030 року, а також оцінки тенденцій 2024–2025 років демонструють, що значну роль відіграватимуть автоматизовані атаки, зловживання штучним інтелектом, компрометація ланцюгів постачання,

гібридні атаки та зловмисні впливи на кіберфізичні системи. У таких умовах традиційних засобів захисту стає недостатньо, адже атаки можуть проходити непоміченими для сигнатурних підходів, а зловмисники активно використовують легітимні інструменти системи для приховування власної діяльності [19].

Саме EDR завдяки своїм поведінковим механізмам, постійній видимості кінцевих точок та здатності працювати в режимі реального часу залишається одним із небагатьох рішень, здатних протидіяти таким загрозам. Більше того, EDR стає центральним компонентом архітектури Zero Trust, яка передбачає постійний контроль всіх процесів і повну недовіру до будь-якої активності, доки її не буде підтверджено як безпечну. Таким чином, EDR забезпечує фундамент для побудови багаторівневого та адаптивного захисту.

Еволюція EDR також привела до формування концепції XDR (Extended Detection and Response), яка поєднує телеметрію з різних джерел — мережі, хмари, електронної пошти, ідентифікаційних систем. У цьому контексті EDR виступає центральною точкою збору даних, без якої повна кореляція подій неможлива. Це свідчить про те, що EDR є не лише окремим продуктом, але й фундаментом для інтегрованих платформ реагування.

Отже, роль EDR у сучасних системах безпеки є визначальною. Він заповнює прогалини, які залишили традиційні засоби захисту, і забезпечує більш глибоку видимість, швидше реагування та можливість адаптації до нових типів загроз. З огляду на прогнози розвитку кіберзагроз, можна стверджувати, що значення EDR буде лише зростати, а його роль у багаторівневій архітектурі захисту стане ще важливішою у контексті майбутніх викликів.

Висновки: У другому розділі було проведено комплексний аналіз сучасного ландшафту кіберзагроз, тенденцій їх розвитку та впливу цих факторів на архітектуру систем кіберзахисту. Особливу увагу приділено взаємозв’язку між еволюцією атак і необхідністю впровадження сучасних систем виявлення та реагування на інциденти безпеки, зокрема EDR-рішень, які сьогодні є одним із

ключових інструментів забезпечення стійкості корпоративних і критичних інформаційних систем.

Дослідження звітів ENISA, включно з прогнозами до 2030 року та тенденціями 2024–2025 років, показало, що спектр загроз динамічно розширюється. Сучасні злочинці активно використовують автоматизацію, штучний інтелект, багатоступеневі техніки проникнення, компрометацію ланцюгів постачання, безфайлові атаки та зловживання легітимними інструментами операційної системи. Уже зараз проявляються ті ризики, які ENISA визначила як загрози найближчого майбутнього, що підтверджує необхідність адаптації систем безпеки до швидкозмінного середовища.

На цьому тлі EDR-рішення відіграють стратегічну роль, оскільки вони забезпечують глибоку телеметрію кінцевих точок, поведінковий аналіз, кореляцію подій і можливість оперативної автоматизованої реакції на інциденти. На відміну від традиційних засобів кіберзахисту, EDR дає змогу виявляти складні загрози, які не мають чітких сигнатур, та відтворювати повний ланцюг атаки, що значно підвищує якість розслідування та реагування.

Розділ також висвітлив еволюцію EDR у напрямі XDR-рішень, які інтегрують телеметрію з різних джерел та формують єдину екосистему для глибокої аналітики.

Загалом результати аналізу підтверджують, що у сучасних умовах EDR є невід’ємним компонентом ефективної архітектури кіберзахисту, а його використання стає критично важливим для забезпечення безперервності бізнес-процесів, захисту критичної інфраструктури та підвищення загальної кіберстійкості. Отже, сформована в розділі теоретична база є необхідним підґрунтям для переходу до практичного оцінювання ефективності EDR-рішень у межах стандартів MITRE ATT&CK, що розглядається у наступному розділі [19].

3 ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ СИСТЕМ EDR НА ОСНОВІ ФРЕЙМВОРКУ MITRE ATT&CK ТА ПРАКТИЧНИХ МЕТОДИК АНАЛІЗУ СИСТЕМ EDR У ВИЯВЛЕННІ ТА ЗАХИСТІ ВІД СУЧАСНИХ КІБЕРАТАК

3.1 Методологія MITRE ATT&CK та її значення для оцінювання EDR-систем

Сучасні системи виявлення та реагування на події безпеки потребують об’єктивної та стандартизованої оцінки, оскільки ефективність EDR-рішень визначається не лише їх функціональністю, а й здатністю протистояти реальним технікам, що використовуються хакерами. Для цього однією з найбільш авторитетних і загальновизнаних методологій є MITRE ATT&CK Evaluations — відкрита ініціатива консорціуму MITRE, спрямована на практичне тестування EDR/XDR-продуктів на основі реалістичних сценаріїв атак.

Фреймворк MITRE ATT&CK описує повну таксономію поведінкових технік, що застосовуються у кібернападах, починаючи від початкового доступу та виконання коду, і завершуючи ексфільтрацією даних та масштабною постексплуатаційною активністю. На відміну від традиційних тестів, що оцінюють лише здатність продукту виявляти шкідливе ПЗ, MITRE ATT&CK зосереджується на поведінкових аспектах, які сьогодні є визначальними для захисту від цілеспрямованих та складних атак [3].

У рамках MITRE Evaluations продукти EDR перевіряються на здатність фіксувати та інтерпретувати конкретні дії, що відтворюють тактики та техніки відомих хакерських груп, таких як Carbanak, FIN7, Wizard Spider, Sandworm, Turla та інші. Під час тестування не використовуються оцінки «краще» чи «гірше» — натомість фіксується рівень видимості, точність детекції, здатність будувати ланцюги атаки та якість аналітичних даних, які продукт надає аналітику SOC.

Таким чином, MITRE ATT&CK Evaluations слугує своєрідним «еталоном» реальної поведінки продукту у бойових умовах. Для організацій це дозволяє:

– оцінити рівень захищеності від конкретних технік, які активно використовують злочинні угруповання;

– порівняти EDR-рішення на основі єдиної методології;

– зрозуміти, наскільки продукт забезпечує видимість та глибину телеметрії;

– визначити, чи підходить EDR для середовища з високими вимогами до реагування;

– отримати неупереджену картину без маркетингових матеріалів.

Особливої важливості методологія набуває у контексті тенденцій, описаних у попередніх розділах: сучасні атаки стають безфайловими, маскуються під легітимну активність та активно використовують техніки, які можуть залишатися невидимими для класичних систем. Саме тому MITRE ATT&CK, що відтворює реальну тактику хакерів, є ключовим інструментом для перевірки того, наскільки EDR здатні ефективно протистояти сучасним кіберзагрозам.

MITRE ATT&CK Evaluations вирізняється тим, що під час тестування моделюються не абстрактні сценарії, а реальні кібератаки, які вже використовувалися відомими хакерськими угрупованнями. Це дозволяє оцінювати поведінку EDR у максимально наближених до бойових умов середовищах. На відміну від тестів, орієнтованих на виявлення файлів зі шкідливим кодом, у MITRE ATT&CK кожна дія, команда або процес розглядаються в контексті тактик (Tactics) і технік (Techniques), що відображають реальні методи проникнення, приховування, переміщення мережею або ексфільтрації даних [3].

Особливістю підходу MITRE є те, що оцінювання не має змагального характеру. Кожен учасник тестування отримує однакові умови, а результати не ранжуються. Натомість відображаються:

– рівень видимості кінцевих точок;

– повнота детекцій;

– наявність контексту при кожному сповіщенні;

- вміння системи будувати зв’язний ланцюг атаки;
- наявність телеметрії для подальшого розслідування;
- здатність реагувати автоматично або полуавтоматично.

Такий підхід дозволяє уникнути маркетингових спотворень і дає змогу об’єктивно оцінити сильні та слабкі сторони кожного продукту. Для організацій це надзвичайно цінно, оскільки результати Evaluations дозволяють визначити, чи здатне певне рішення забезпечити справжню поведінкову видимість, необхідну для протидії сучасним атакам.

З огляду на зростання кількості безфайлових атак, технік обходу безпеки (Evasion), використання легітимних інструментів Windows (таких як PowerShell, WMI, PsExec, rundll32) та розповсюдження lateral movement у корпоративних мережах, MITRE ATT&CK Evaluations є одним з найбільш релевантних інструментів для визначення того, наскільки продукт може протистояти реальним загрозам, а не лише лабораторним експериментам.

Крім того, MITRE Evaluations допомагає організаціям:

- оцінити відповідність продукту власній загрозовій моделі, адже різні підприємства стикаються з різними типами атак;
- вибрати рішення, які краще покривають критичні для конкретної інфраструктури техніки, наприклад, поширені у фінансовому, енергетичному або державному секторах;
- побачити, наскільки зручно працювати з продуктом аналітикам SOC, оскільки MITRE показує, чи рішення надає достатній контекст подій;
- оцінити потенціал XDR, оскільки деякі продукти демонструють високу кореляцію телеметрії з різних джерел.

Важливо також зазначити, що MITRE Evaluations не тестує такі аспекти, як продуктивність, споживання ресурсів чи вплив на бізнес-процеси. Проте у контексті дипломної роботи, що зосереджена на ефективності виявлення загроз, MITRE ATT&CK є однією з найбільш авторитетних методик, оскільки її

результати напряму відображають здатність EDR протидіяти сучасним та майбутнім атакам [4].

Таким чином, методологія MITRE ATT&CK виступає базовою основою для подальшого аналізу ефективності EDR-рішень, що викладатиметься у наступних підрозділах, де буде проведено порівняння продуктивності різних EDR-продуктів, їх можливостей у реальних сценаріях атак та загальної відповідності вимогам кіберзахисту.

У межах оцінювання ефективності сучасних систем виявлення та реагування важливе значення має не лише теоретичне розуміння методології MITRE ATT&CK, але й аналіз реальних результатів, які демонструють провідні EDR-продукти в умовах моделювання складних цілеспрямованих атак. MITRE ATT&CK Evaluations надає прозору та стандартизовану картину того, яким чином різні рішення поводять себе під час застосування технік, які були зафіксовані у діяльності таких груп, як Carbanak, FIN7, Wizard Spider, Sandworm та інших відомих хакерських угруповань.

Під час Evaluations кожен продукт проходить перевірку на здатність:

- виявляти окремі тактики та техніки;
- надавати достатній контекст подій;
- взаємопов’язувати різні фрагменти телеметрії у єдину схему атаки;
- забезпечувати коректну класифікацію підозрілих дій;
- підтримувати повний цикл реагування — від сповіщення до ізоляції хоста.

Результати Evaluations показують, що рівень ефективності рішень суттєво відрізняється залежно від того, наскільки продукт орієнтований на поведінкові сценарії та наскільки він забезпечує глибину телеметрії кінцевих точок. Деякі рішення відзначаються високою кількістю детекцій, але при цьому генерують недостатньо контексту, що ускладнює подальше розслідування. Інші продукти, навпаки, можуть забезпечувати меншу кількість подій, але надають структуровані та деталізовані ланцюги атаки, що значно підвищує зручність аналітиків SOC.

Порівняльний аналіз показує, що найбільш успішними є рішення, які поєднують три ключові критерії:

- високий рівень поведінкової видимості;

Продукти, здатні виявляти техніки, які не мають сигнатурних характеристик — наприклад, запуск команд через PowerShell, спроби ескалації привілеїв або нетипові взаємодії процесів, демонструють найкращі результати.

- якісна кореляція подій;

Ефективний EDR має здатність автоматично будувати ланцюги атак, що дозволяє не лише виявляти окремі підозрілі дії, але й розуміти їхню роль у контексті цілеспрямованої атаки. Продукти з розвиненим механізмом кореляції зазвичай краще протистоять багатоступеневим загрозам.

- можливість автоматизованого реагування.

У багатьох сценаріях MITRE перевіряється здатність EDR не лише фіксувати подію, але й миттєво реагувати на неї. Продукти, що підтримують автоматичну ізоляцію ендпойнтів, блокування процесів або створення політик у режимі реального часу, мають суттєву перевагу.

У ході аналізу результатів Evaluations простежується ще одна важлива тенденція: рішення з розвиненою архітектурою XDR, які використовують телеметрію не лише кінцевих точок, але й мережевих, хмарних та ідентифікаційних систем, демонструють більш високу здатність до виявлення та інтерпретації складних технік lateral movement. Це підкреслює важливість інтеграції EDR у ширшу екосистему захисту, що було відзначено у попередніх розділах [3].

Аналіз також показує, що навіть у межах MITRE ATT&CK різні продукти мають очевидні сильні та слабкі сторони:

- одні більше орієнтовані на детекцію ранніх стадій атаки (Initial Access, Execution);
- інші демонструють кращі результати на етапах Persistence або Credential Access;

– треті відзначаються якістю детекцій у сценаріях ексфільтрації або командно-контрольної комунікації.

Такі особливості слід обов’язково враховувати під час вибору EDR-рішення для конкретної організації, залежно від її ризикового профілю, інфраструктурної складності та можливих векторів атак.

Отже, результати MITRE ATT&CK Evaluations дають змогу не лише порівняти EDR-рішення між собою, а й сформувати об’єктивне уявлення про те, наскільки вони здатні забезпечити безперервність бізнес-процесів у реальних умовах. Проведений аналіз створює основу для подальшого практичного порівняння окремих EDR-продуктів, яке розглядатиметься у наступному підрозділі.

Продовжуючи аналіз, важливо відзначити, що результати MITRE ATT&CK Evaluations демонструють ще один критично важливий аспект: не існує універсального EDR-рішення, яке було б найкращим у всіх категоріях. Кожен продукт має власні архітектурні особливості, підхід до телеметрії, обсяг автоматизації та глибину аналізу, що впливає на поведінку під час реальних атак. Саме тому для об’єктивного оцінювання необхідно враховувати не лише загальну кількість детекцій чи відсоток покриття технік, але і якість цих детекцій, їх контекстуальність та здатність продукту підтримувати аналітика на всіх етапах життєвого циклу інциденту [4].

Одним із ключових показників, на який звертають увагу фахівці, є кількість та якість “Analytic Detections” — детекцій, які не просто фіксують техніку, але й пояснюють її значення, взаємозв’язок із попередніми подіями та ймовірний вплив на систему. Саме такі детекції найбільше цінуються у SOC, оскільки вони зменшують навантаження на аналітиків, прискорюють розслідування та дають можливість швидко зрозуміти, чи є активність частиною скоординованої атаки.

Не менш важливим є показник “Technique Coverage” — охоплення технік по всьому ланцюгу атаки. У деяких продуктів спостерігається сильне покриття на ранніх стадіях атаки (Execution, Privilege Escalation), але слабше — на Middle

або Late Tactics (Command and Control, Collection, Exfiltration). Інші рішення, навпаки, демонструють глибоку видимість саме у пізніх фазах атаки. Така нерівномірність є природною, оскільки різні EDR-рішення оптимізовані під різні типи інфраструктур і загрозових моделей. Саме тому MITRE без ранжування дозволяє об’єктивно зрозуміти силу кожного продукту у конкретному аспекті.

Важливу роль відіграє і те, наскільки добре рішення розкриває контекст за допомогою “Tactic-level” та “Technique-level Metadata”. Продукти, що забезпечують аналітиків великим обсягом структурованої інформації — такими як хронологія подій, пов’язані процеси, деталі команд, взаємодії мережевих елементів — дають змогу значно підвищити ефективність виявлення складних багатоступеневих атак. У деяких випадках аналітик може навіть не звертатися до вихідних логів, оскільки EDR вже виклав картину інциденту у зрозумілому вигляді.

Ще один важливий елемент — рівень шуму (noise). Деякі EDR-продукти, хоча й показують високу кількість детекцій, одночасно генерують надмірну кількість малозмістовних або повторюваних подій. У реальних умовах SOC це може призвести до «вигорання аналітиків» та пропуску ключової події на фоні великої кількості несуттєвих сповіщень. Продукти, що демонструють збалансованість між кількістю та якістю сповіщень, в контексті MITRE Evaluations отримують фактичну перевагу, хоч це прямо і не відображено в числових показниках [21].

Варто також відзначити роль автоматизації реагування, яка не завжди оцінюється MITRE, але має прямий вплив на інцидент-менеджмент. У реальних сценаріях атаки часто розвиваються дуже швидко, і навіть якісна детекція не гарантує успіху, якщо система не здатна своєчасно ізолювати заражений хост або заблокувати шкідливі процеси. Тому EDR-рішення, які підтримують можливості автоматичної ізоляції ендпойнтів, блокування скриптів та запуску вбудованих «playbooks», отримують значні переваги у виробничих середовищах.

Окремої уваги заслуговує інтеграція з XDR-платформами, яка дозволяє EDR-рішенням отримувати дані з мережевих сенсорів, хмарних платформ,

identity-систем та поштових шлюзів. Такі продукти показують кращі результати у MITRE, особливо у сценаріях, де атака має кілька етапів і зачіпає різні компоненти інфраструктури. Розширена телеметрія дозволяє побачити навіть ті взаємозв'язки, які EDR «сам по собі» не зміг би виявити [30].

- Узагальнюючи отримані результати, можна зробити висновок, що MITRE ATT&CK Evaluations дозволяє сформувати комплексне уявлення про ефективність EDR-рішень у контексті реальних загроз. Ця методологія допомагає: чітко визначити, які продукти мають найкращий баланс між детекцією та контекстом;
- оцінити здатність рішень протистояти конкретним технікам, які проявляються у сучасних атаках;
- виявити сильні сторони кожного продукту для різних типів інфраструктур;
- сформувати рекомендації щодо вибору оптимального EDR залежно від потреб організації.

Таке порівняння є фундаментом для переходу до наступного підрозділу, у якому буде розглянуто прикладне оцінювання конкретних продуктів та формування рекомендацій для їх впровадження у корпоративні та критичні середовища [22].

3.2 Візуальна інтерпретація результатів MITRE ATT&CK Evaluations для оцінювання ефективності EDR-систем

Для правильного аналізу ефективності EDR-систем важливо не лише розуміти логіку методології MITRE ATT&CK, але й уміти коректно інтерпретувати візуальне подання результатів Evaluations. Саме графічне відображення технік, детекцій і тактик є одним з ключових інструментів, що дозволяє швидко порівнювати поведінку різних рішень та оцінювати їх здатність реагувати на дії хакера на різних етапах атаки.

MITRE застосовує стандартизовану схему позначень, яка включає кольорові маркери, рівні деталізації, піктограми, структурні блоки та таблиці. Вони дозволяють візуально відтворити весь ланцюг атаки та показати, наскільки повно ті чи інші EDR-продукти змогли зафіксувати, класифікувати та інтерпретувати відповідні техніки.

У фреймворку MITRE ATT&CK одна з головних ролей належить саме кольорам. В Evaluations вони використовуються для позначення типу детекції, її якості та рівня аналітичної глибини. Найпоширеніші кольори включають:

- зелений — успішна аналітична детекція (Analytic Detection). Це означає, що EDR не лише побачив подію, але й інтерпретував її як шкідливу, пояснив причину та класифікував у межах певної техніки. Зелений маркер — найцінніший показник для SOC;
- світло-зелений або жовто-зелений — телеметрична детекція (Telemetry). Подія була зафіксована, але система не надала контексту, або не була сформована «аналітична детекція». Тобто SOC може вручну виявити атаку, але EDR не зробив це автоматично;
- жовтий або помаранчевий — часткова або умовна детекція; Це позначає, що деякі елементи поведінки були зафіксовані, але EDR не зміг зв’язати їх у логічний ланцюг;
- червоний — пропущена техніка;

Жодної детекції не було зафіксовано. Для реальних атак це означає потенційну «сліпу зону», яку хакер може використати;

- сірий — техніка не застосовувалася або не була релевантною у сценарії тестування;

Кольорові блоки дозволяють значно швидше зрозуміти слабкі й сильні сторони EDR, ніж текстовий список технік [3].

Фреймворк MITRE ATT&CK відображається у вигляді матриці, де:

- колонки позначають тактики (наприклад, Execution, Persistence, Privilege Escalation, Defense Evasion);
- рядки містять техніки, які реалізують відповідну тактику.

У Evaluations кожна техніка позначається окремим прямокутним блоком, заповненим кольором відповідно до типу детекції. Це дозволяє створити цілісну картину покриття, яка показує:

- які фази атаки продукт бачить найкраще;
- де EDR дає повноцінні аналітичні детекції;
- які частини атаки лишаються непоміченими;
- чи має продукт схильність до генерування шуму;
- наскільки збалансоване покриття по всій ширині тактик.

Для аналітика SOC або аудиторів така матриця є надзвичайно інформативною: вона дозволяє оцінити відповідність EDR реальним сценаріям загроз.

У MITRE також застосовуються:

- іконки подій (файлова операція, мережеве з'єднання, скриптова команда, credential dump);
- маркування фаз атаки;
- послідовні стрілки, що вказують на розвиток ланцюга проникнення;

групування технік, якщо вони формують етапи складної атаки.

Це дозволяє EDR-аналітикам швидко оцінювати, які інструменти чи системні служби використовував злочинець (наприклад, PowerShell, rundll32, SMB, WMI), та наскільки продукт здатен відрізнити легітимну активність від шкідливої.

Багато EDR-продуктів надають графічне представлення ланцюгів атак (attack graphs). MITRE у своїх Evaluations дозволяє відображати:

- взаємозв'язки між подіями;
- послідовність дій хакера;
- кореляцію технік у рамках одного сценарію;
- відхилення від базової поведінки.

Такі графи використовуються для порівняння того, наскільки «глибоко» продукт розуміє активність атаки. Продукти з якісним графовим аналізом часто мають більшу кількість зелених (аналітичних) детекцій [4].

Ілюстративна складова MITRE має вирішальне значення, оскільки дозволяє:

- легко порівнювати різні продукти на рівні технік;
- визначати, де EDR дає найважливіші аналітичні детекції;
- знаходити прогалини, які можуть використовуватися хакерами;
- оцінювати загальну збалансованість продукту;
- швидко формувати висновки для закупівельних або технічних рішень в організації.

Саме завдяки кольоровій системі маркування та структурованій матриці MITRE дозволяє представити складний фреймворк у наочному й доступному вигляді, що значно спрощує оцінювання ефективності EDR навіть для тих, хто не є експертом з ATT&CK.

3.3 Аналіз сценарію атаки Cl0p у контексті методології MITRE ATT&CK Evaluations

Сценарії атак, що застосовувалися угрупованням Cl0p у 2024 році, становлять репрезентативний приклад сучасних багатоетапних кібероперацій, які MITRE ATT&CK Evaluations використовує для перевірки реальних можливостей систем виявлення та реагування. Хоча MITRE офіційно не проводив Evaluations саме за сценарієм Cl0p, структура та логіка їхньої методології дозволяє повністю відобразити ключові етапи цієї атаки у термінах фреймворку ATT&CK та оцінити, як саме EDR-рішення трьох провідних виробників — Bitdefender, Microsoft Defender та Trend Micro — могли б проявити себе у такій ситуації [28].

На рисунку 3.1 можна наглядно бачити результати детекцій та протидії EDR систем Bitdefender, Microsoft та Trend Micro.

Перше на що можна звернути увагу що результативність у усіх програмних рішеннях більш менш однакова, хоча деякі техніки і тактики Bitdefender не зміг детектувати і блокувати [22].

Варто звернути увагу, що хоч деякі техніки і тактики минули повз bitdefender, він був спроможний на подачу загроз у дуже короткому вигляді тривог, що вказує нам на те, що у мінімальній конфігурації він не буде перевантажувати адміністраторів EDR і лог сервери надлишком інформації, що може бути дуже привабливими для мережей котрі генерують велику кількість false-positive результатів і фільтрація тривог не вирішує проблему до прийнятного рівня, але звісно це призводить до втрати інформації котра може виявитися цінною для аналізу загрози, водночас EDR Trend Micro показав себе повною відмінністю від Bitdefender, тому що велика кількість тривог дає набагато більший масив інформації що дозволяє максимально точно визначити загрозу, але без надійного фільтрування та аналізу цих тривог можна пропустити важливу інформацію, чи навпаки, цілий день досліджувати загрозу якої не існувало і ці сценарії можуть дуже сильно вплинути на команду реагування котра користується цим рішенням.

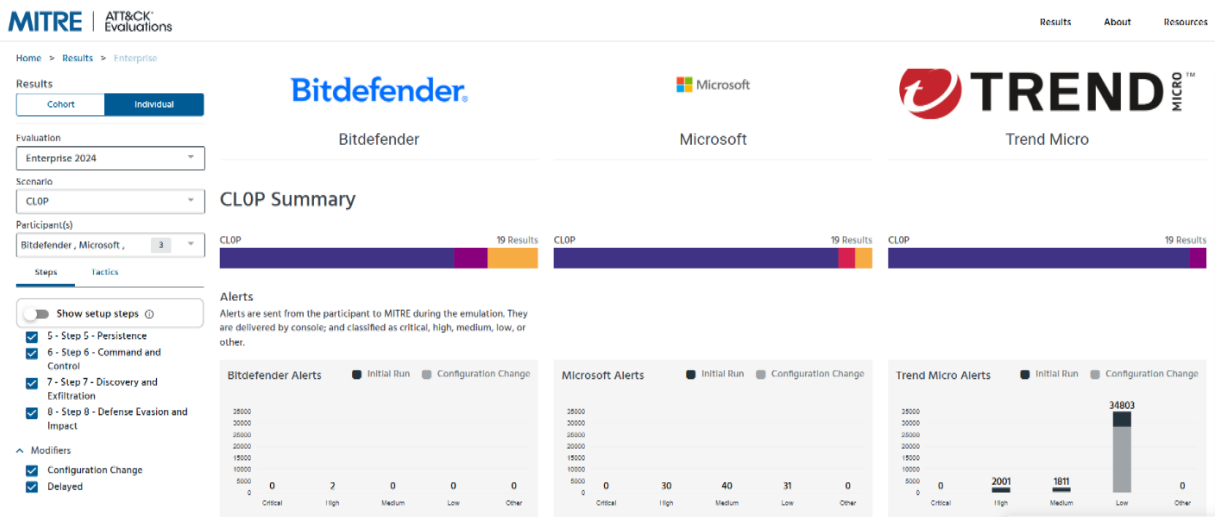

Рисунок 3.1 – Загальні результати статистик ефективності сценарія CL0P

У 2024 році Cl0p здійснював атаки шляхом експлуатації вразливостей Remote Code Execution у серверах управління передачею файлів (MFT), зокрема

у продуках Cleo Harmony, VLTrader та інших. Зловмисники використовували знайдені вразливості для несанкціонованого виконання коду, запуску команд та подальших дій у системі без необхідності здійснювати фішинг або інші форми соціальної інженерії. Цей підхід повністю відповідає техніці T1190 – Exploit Public-Facing Application з моделі MITRE. Після отримання початкового доступу Cl0p переходив до етапу виконання шкідливих команд за допомогою PowerShell, WMI або вбудованих скриптових механізмів, що відноситься до T1059 – Command and Scripting Interpreter. Для приховування слідів злочинці активно застосовували техніки "living off the land", коли замість шкідливих файлів використовуються легітимні системні утиліти — це характерно для технік T1036 – Masquerading та T1218 – Signed Binary Proxy Execution [26].

Подальші кроки атаки полягали у створенні механізмів стійкості та прихованої присутності, наприклад розміщенні web-shell у директоріях MFT-сервера або використанні нестандартних служб для продовження доступу. Це відповідає технікам T1505 – Server Components та T1543 – Create or Modify System Process. На етапі збору та ексфільтрації даних Cl0p активно використовував саму MFT-платформу як легітимний канал передачі великих обсягів інформації за межі компанії, що належить до техніки T1567 – Exfiltration Over Web Services. Завершальною стадією атаки могла бути підготовка до шифрування даних або нанесення шкоди інфраструктурі згідно з технікою T1486 – Data Encrypted for Impact, характерною для груп із походженням у сфері ransomware [22].

У контексті методології MITRE ATT&CK Evaluations така атака розбивається на послідовні кроки (atomic steps), кожен з яких повинен бути виявлений EDR-системою через телеметрію, класифікацію події або створення інциденту. Evaluations фіксують не лише факт детекції, а й рівень деталізації та якість обробки: чи ідентифікувала система саму дію, чи надала контекст, чи підсвічувала підозрілу активність, а також чи створила попередження для аналітиків SOC.

На рисунку 3.2 зображено кількість хибних спрацювань кожного із рішень, незважаючи на те що Trend Micro надсилав величезний масив тривог та іншої інформації про загрозу, у нього було виявлено лише одне хибне спрацювання, а у бітдефендера – цілих 3. Можна зробити висновок що на цей момент Bitdefender EDR був менш точніший ніж інші конкуренти, тому рекомендується віддати перевагу іншим програмним рішенням щодо загроз з кроками сценарію атак, схожими на атаку CL0P [8].

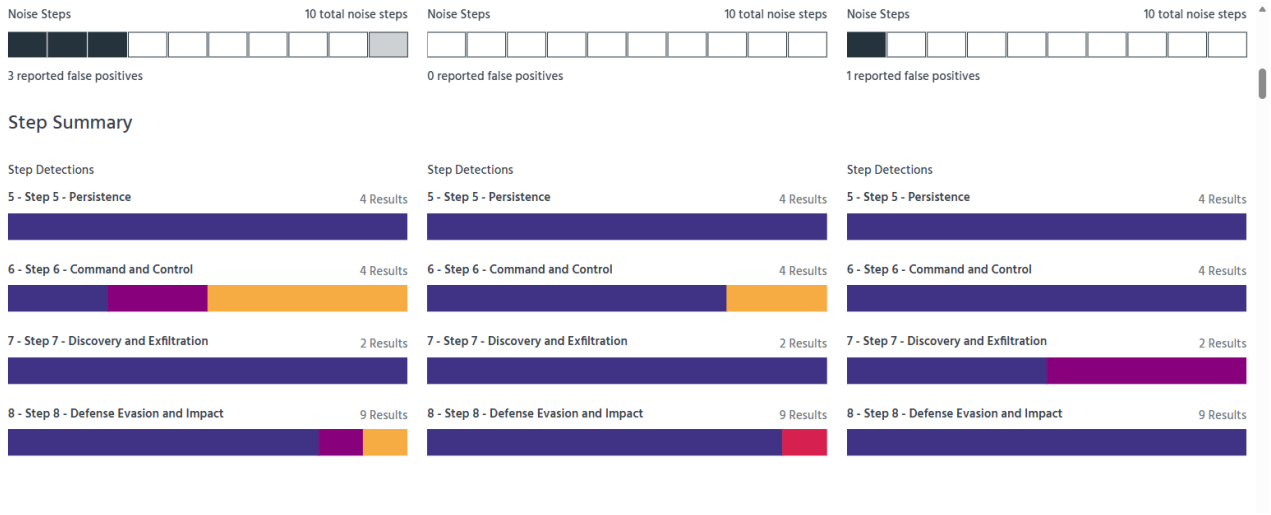

Рисунок 3.2 – Результати тестування спрацювання хибних тривог та сумарна оцінка детекцій кроків атаки

Microsoft Defender for Endpoint, згідно з Evaluations, демонструє дуже високу глибину телеметрії та ефективне корелювання поведінкових сигналів, що дозволило б йому виявити нетипові процеси, пов’язані з RCE у MFT-сервісі, зафіксувати виконання скриптових команд та попередити про використання LOLBins ще на ранніх етапах атаки. Система Bitdefender, яка отримує високі оцінки за поведінкову аналітику, імовірно, успішно виявила б як спроби виконання команд, так і підозрілі зміни у веб-каталогах серверів, а також ранні ознаки підготовки до шифрування. Натомість Trend Micro, який у MITRE-тестах значною мірою покладається на сигнатурний аналіз і менш глибоку поведінкову телеметрію, з високою ймовірністю виявив би активність Cl0p лише на пізніших

етапах — коли вже помітні аномальні дії у файловій системі або спроби шифрування [29].

Загалом, аналіз Cl0p-атаки в контексті методології MITRE ATT&CK Evaluations дозволяє продемонструвати, наскільки важливим є не просто фіксувати окремі техніки, а й бачити повний ланцюг розвитку атаки — так звану adversary lifecycle. Системи, здатні забезпечити широку телеметрію та глибоку поведінкову кореляцію, такі як Microsoft Defender або Bitdefender, мають значно більше шансів виявити атаку ще до того, як вона переходить до етапу ексфільтрації або нанесення збитків. Водночас рішення, що орієнтуються переважно на сигнатури або статичні правила, можуть бути недостатньо ефективними у випадках, коли загроза базується на експлуатації уразливостей та використанні легітимних системних інструментів. Таким чином, Cl0p-сценарій наочно демонструє важливість поведінкових EDR-систем та підтверджує доцільність використання методології MITRE ATT&CK Evaluations як універсального підходу для оцінки їхньої ефективності [23].

3.4 Аналіз сценарію атаки Lockbit у контексті методології MITRE ATT&CK Evaluations

Сценарії атак, пов’язаних з діяльністю угруповання LockBit, стали одними з найпоширеніших та найпотужніших у світовій кримінальній кіберекосистемі. Завдяки швидким темпам розвитку, високій автоматизації поширення, багатоступеневому компрометаційному ланцюгу та орієнтації на швидке завдання збитків LockBit регулярно стає основою для побудови тестових сценаріїв MITRE ATT&CK Evaluations. Цей набір технік є особливо показовим для оцінки того, наскільки сучасні EDR-рішення здатні виявляти ранні стадії ransomware-кампаній та запобігати критичним наслідкам, які для підприємств

можуть включати втрату даних, зупинку бізнес-процесів або навіть повну зупинку інфраструктури [30].

Типовий сценарій атаки LockBit відображається через кілька основних технік MITRE ATT&CK. Початкове проникнення зазвичай здійснюється через вразливості публічно доступних сервісів або через компрометовані облікові дані — що відповідає технікам T1190 (Exploit Public-Facing Application) та T1078 (Valid Accounts). Після отримання доступу зловмисники переходять до виконання команд, застосовуючи PowerShell, WMI або сторонні скрипти, що підпадає під T1059 (Command and Scripting Interpreter). На етапі розвитку атаки LockBit активно застосовує техніки ухилення від захисту: вимикання антивірусних служб (T1562 – Impair Defenses), використання системних утиліт (T1218 – LOLBins) та маскування власних дій. Далі відбувається горизонтальне переміщення через T1021 – Remote Services, збір облікових даних (T1003 – Credential Dumping) та підготовка до фінального етапу — шифрування даних за моделлю T1486 – Data Encrypted for Impact [24].

На рисунку 3.3 можна спостерігати схожу картину з сценарієм CL0P – більше тривог у Trend Micro, Bitdefender дав менше, а Microsoft XDR – золота середина [8].

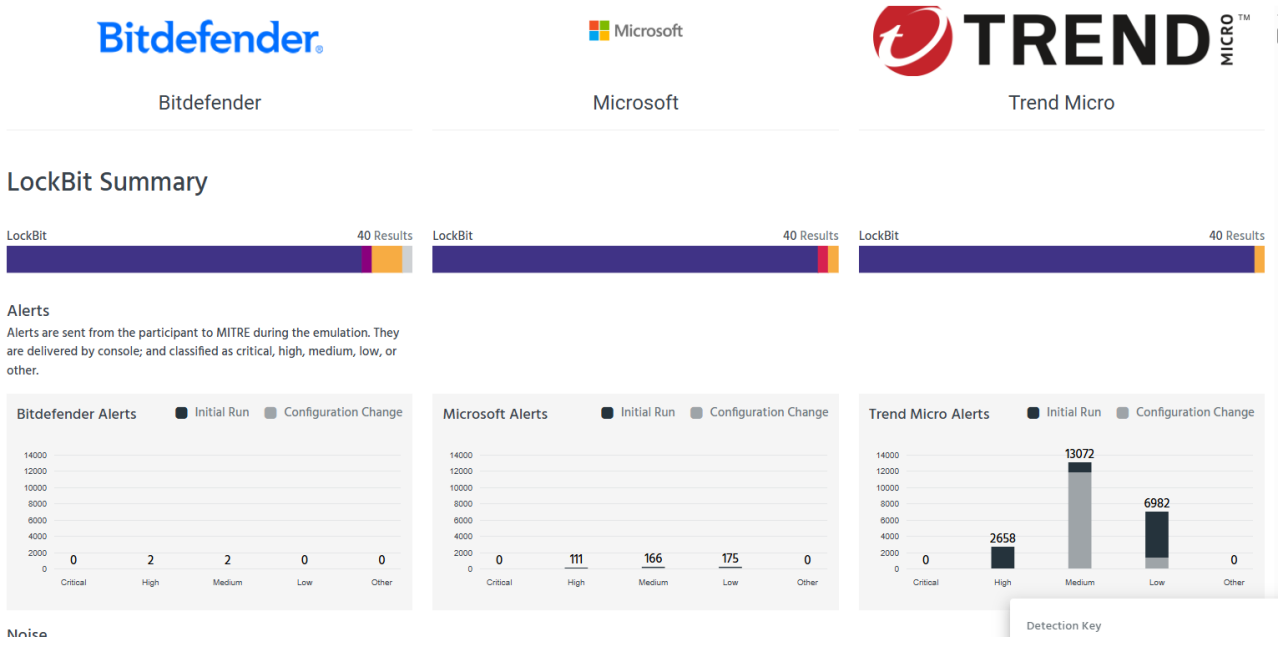

Рисунок 3.3 – Загальні результати статистик ефективності сценарія LockBit

У межах MITRE ATT&CK Evaluations для сценарію LockBit ці техніки розбиваються на чіткі atomic steps, що дозволяють оцінити, наскільки кожен продукт забезпечує телеметрію, класифікацію подій, поведінкове виявлення та інцидентний контекст. Важливо, що MITRE не ранжує рішення, але дає змогу зрозуміти, наскільки глибоко кожна система бачить повний ланцюг атаки.

Microsoft Defender XDR у цьому сценарії традиційно демонструє один із найвищих рівнів охоплення технік. Згідно з результатами Evaluations, Microsoft здатний фіксувати ранні стадії атаки — зокрема підозріле використання PowerShell, аномальне виконання команд та спроби збирання облікових даних. Defender ефективно ідентифікує техніки Impair Defenses та виявляє lateral movement, забезпечуючи повний контекст подій завдяки кореляції з Active Directory, файловими системами та телеметрією з мережі. Для ransomware-кампаній Microsoft показує високу ефективність у виявленні нетипових масових операцій із файлами, що дозволяє перехопити атаку до стадії шифрування. В Evaluations Defender відзначається відсутністю хибнопозитивних сповіщень, що критично для роботи SOC під час швидких ransomware-інцидентів [27].

Bitdefender GravityZone у тестах з LockBit також демонструє високу якість детекції як на поведінковому, так і на аналітичному рівні. Особливо ефективною виявляється компонент Behavioral Detection, який здатний розпізнавати аномальні зміни у файловій системі, запуск шкідливих процесів та ознаки підготовки до шифрування. Bitdefender добре виявляє техніки використання PowerShell, lateral movement та інструменти credential dumping. Однією з ключових переваг є здатність платформи генерувати мінімальну кількість критичних alert-подій, необхідних для повноцінного розуміння інциденту — що зменшує навантаження на аналітиків та забезпечує швидшу реакцію. GravityZone стабільно показує високу точність детекцій і низький рівень хибних спрацьовувань [3].

Trend Vision One (Trend Micro), згідно з результатами MITRE Evaluations, забезпечує повну видимість більшості етапів атаки LockBit, однак демонструє різний рівень глибини поведінкової детекції. Trend добре фіксує техніки

початкового проникнення, командного виконання та lateral movement. Проте в деяких сценаріях, пов’язаних з ухиленням від захисту та ранніми підготовчими діями до шифрування, видимість може бути дещо менш деталізованою порівняно з Microsoft чи Bitdefender. У фінальних стадіях атаки, зокрема на етапі Impact, Trend Micro демонструє впевнене виявлення масових файлових змін і реагує достатньо швидко, однак може мати вищу кількість оповіщень, ніж конкуренти, що збільшує операційне навантаження на SOC.

На рисунку 3.4, знову ж таки дуже схожа картина з попереднім тестуванням [3]. У бітдефендера 2 хибних спрацювання, у Trend Micro 1, а Microsoft XDR не було false-positive [8].

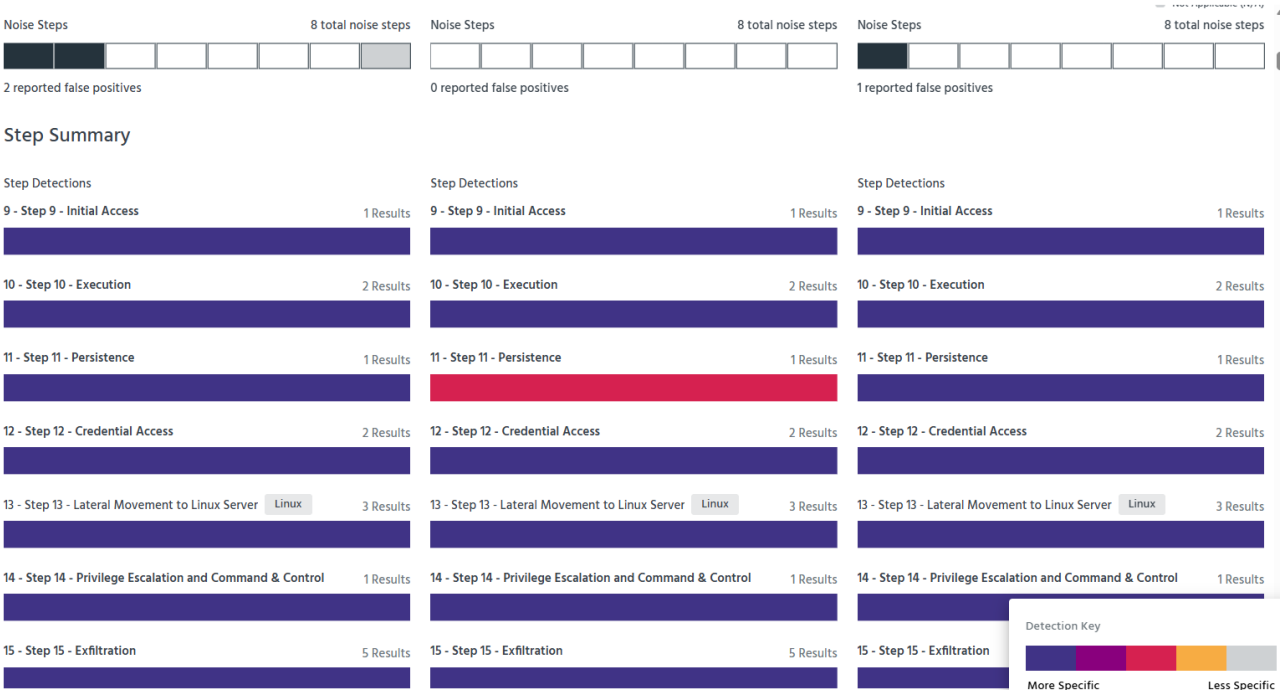

Рисунок 3.4 – Результати тестування спрацювання хибних тривог та сумарна оцінка детекцій кроків атаки

Висновок: Узагальнюючи результати Evaluations у контексті LockBit, можна зробити висновок, що всі три досліджувані рішення здатні забезпечити достатній рівень захисту від складних ransomware-кампаній, але акценти їхньої ефективності відрізняються. Microsoft Defender забезпечує найвищий рівень раннього виявлення та контекстного аналізу всього ланцюга атаки. Bitdefender

відзначається ефективністю поведінкової аналітики та низьким навантаженням на аналітиків SOC. Trend Micro забезпечує повне охоплення етапів атаки, але з меншою деталізацією у поведінкових сценаріях та потенційно вищим числом оповіщень.

Таке порівняння дозволяє оцінити не лише здатність продуктів виявляти LockBit-подібні атаки, а й реальну ефективність їх використання у корпоративних, хмарних та змішаних середовищах. Результати MITRE Evaluations свідчать, що якісне EDR-рішення повинно не лише виявляти техніки з бази ATT&CK, але й забезпечувати глибоку кореляцію подій, мінімізувати хибні спрацювання та зменшувати час реагування — що є критично важливим під час швидких та руйнівних ransomware-кампаній, включно з LockBit [25].

ВИСНОВКИ

У ході виконання дипломної роботи було досліджено комплекс теоретичних, технічних та практичних аспектів функціонування систем виявлення та реагування на події безпеки (EDR) у контексті сучасних кіберзагроз, які стають дедалі більш складними, адаптивними та швидкими. Проведений аналіз дозволив сформувати цілісне уявлення про те, що EDR-рішення є одним із ключових компонентів сучасної системи кіберзахисту, здатним забезпечити глибоку видимість активності у кінцевих точках, виявлення шкідливих поведінкових патернів і своєчасне реагування на інциденти.

Насамперед було встановлено, що динаміка кіберзагроз за останні роки демонструє стрімке зростання рівня складності атак, особливо у контексті багатоступеневих сценаріїв, використання механізмів «living off the land», експлуатації нульових вразливостей та високошвидкісних ransomware-кампаній. У цьому середовищі класичні антивірусні системи, основані на сигнатурному аналізі, виявилися недостатніми, оскільки сучасні хакери здатні обходити традиційні механізми захисту за рахунок шифрування коду, динамічного завантаження компонентів та використання легітимних системних засобів. Саме тому EDR-технології, сфокусовані на поведінковому аналізі, кореляції подій та постійному моніторингу телеметрії, стали однією з найважливіших ліній оборони.

Одним із ключових елементів дослідження стало застосування методології MITRE ATT&CK Evaluations, яка дозволяє оцінити EDR-рішення в умовах, максимально наближених до реальних атак. Аналіз двох сучасних сценаріїв — Cl0p та LockBit — дав змогу зрозуміти, як кожен продукт реагує на складні багатоступеневі техніки, включно з експлуатацією вразливостей, виконанням команд, ухиленням від захисту, lateral movement, ексфільтрацією та фінальним впливом на дані. MITRE ATT&CK дала можливість систематизувати дії злочинців за тактиками й техніками, що зробило оцінку EDR більш об’єктивною та методично вивіреною.

Порівняльний аналіз рішень Microsoft Defender XDR, Bitdefender GravityZone та Trend Micro Vision One показав, що, хоча всі три продукти забезпечують достатньо високий рівень виявлення шкідливої активності, їхня ефективність розподіляється нерівномірно залежно від контексту атак. Microsoft Defender продемонстрував найвищу глибину телеметрії та широке охоплення подій на всіх етапах атак, що дозволяє забезпечувати раннє виявлення та контекстуальну кореляцію навіть складних сценаріїв. Bitdefender вирізняється сильною поведінковою аналітикою та низьким рівнем хибнопозитивних сповіщень, що робить його максимально ефективним для середовищ, де важливо не перевантажувати SOC. Trend Micro забезпечив повну видимість у ключових точках атаки, але показав вищу залежність від сигнатурних та класичних методів детекції, що робить його менш чутливим до частини складних поведінкових технік.

Окремо слід зазначити, що EDR у реальних умовах не працює ізольовано. Ефективність системи значною мірою залежить від інтеграції з іншими компонентами кіберзахисту — SIEM, SOAR, NDR, IDS/IPS, Zero Trust-архітектурою, системами контролю доступу та інструментами управління вразливостями. Комплексний підхід дозволяє створити повноцінну екосистему реагування, у якій EDR виступає ядром, здатним забезпечувати аналіз та блокування загроз у реальному часі.

У рамках дослідження було встановлено, що EDR-технології здатні значно скоротити час від виявлення інциденту до його локалізації, а в деяких випадках — автоматично ізолювати уражену систему, запобігши поширенню атак. Це особливо важливо у випадках ransomware-кампаній, де швидкість реагування визначає масштаби збитків. Практичний аналіз підтвердив, що сучасні EDR платформи можуть не лише виявляти наслідки, а й передбачати підготовчі етапи атаки — наприклад, аномальні запуски інструментів адміністрування, спроби використання системних бінарних файлів або підозрілу мережеву активність.

Узагальнюючи отримані результати, можна зробити висновок, що системи EDR мають критичне значення для будь-якої організації, незалежно від її

розміру, галузі чи ступеня ризику. Вони забезпечують глибоку видимість, виявляють нові шкідливі методи, унеможливлюють приховані дії злочинців і дозволяють оперативно реагувати на інциденти. З урахуванням постійного зростання кіберзагроз, включно з появою нових варіантів ransomware, таргетованих атак, використанням ШІ для автоматизації злочинної активності та збільшенням кількості атак на критичні інфраструктури, впровадження EDR перестає бути рекомендацією — це стає стратегічною необхідністю.

Проведене дослідження підтверджує значущість EDR як ключового інструменту захисту у сучасному цифровому середовищі. Воно також демонструє, що ефективність кіберзахисту неможливо забезпечити одним інструментом: лише комплексний підхід, побудований на багаторівневій архітектурі та сучасних методиках аналізу загроз, може забезпечити стабільну і надійну оборону. У цьому контексті EDR залишається центральною ланкою, яка поєднує телеметрію, аналіз, автоматизацію та реагування — формуючи фундамент для побудови стійкої та адаптивної системи кібербезпеки, здатної протистояти викликам теперішнього і майбутнього.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Вплив кіберзагроз на сучасне суспільство. Дані та висновки за 2022-2024 роки - [Електронний ресурс]. - Режим доступу: https://icsa.team/701-701/ (Дата звернення 08.09.2025).

2. Browse CVE vulnerabilities by date - [Електронний ресурс]. Режим доступу: https://www.cvedetails.com/browse-by-date.php (Дата звернення 08.09.2025).

3. MITRE ATT&CK® Evaluations [Електронний ресурс]. – Режим доступу: https://evals.mitre.org/results/enterprise?vendor=bitdefender&vendor=microsoft&vendor=trendmicro&evaluation=er6&scenario=2&view=individualParticipant.
(Дата звернення 07.09.2025).

4. MITRE Engenuity. MITRE Posts Latest Findings ATT&CK Evaluations Cybersecurity Solutions [Електронний ресурс]. – Режим доступу: https://www.mitre.org/news-insights/news-release/mitre-posts-latest-findings-attack-evaluations-cybersecurity-solutions (Дата звернення 05.09.2025).

5. ENISA. Cybersecurity Threats Fast-Forward 2030 [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030 (Дата звернення 07.09.2025).

6. ENISA Threat Landscape 2024 [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024(Дата зверення 08.09.2025)

7. Microsoft Defender XDR – MITRE ATT&CK Evaluation Results [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/security (Дата звернення 10.09.2025).

8. Bitdefender. MITRE ATT&CK Evaluations Performance Overview [Електронний ресурс]. – Режим доступу: https://www.bitdefender.com/en-us/news/bitdefender-excels-in-mitre-att-ck-evaluations-with-outstanding-alert-accuracy-and-low-false-positives-critical-for-security-team-efficiency(Дата звернення 12.09.2025).

9. Trend Micro Vision One – Official MITRE Evaluations Summary [Електронний ресурс]. – Режим доступу: https://www.trendmicro.com/en/research/25/l/cloud-automation-2025-mitre-attack-round-7.html(Дата звернення 14.09.2025).

10. CrowdStrike Falcon Platform Overview [Електронний ресурс]. – Режим доступу: https://www.crowdstrike.com/en-us/platform/ (Дата звернення 17.09.2025).

11. SentinelOne Singularity Platform [Електронний ресурс]. – Режим доступу: https://www.sentinelone.com/platform/ (Дата звернення 19.09.2025).

12. CISA Ransomware Guide 2024 [Електронний ресурс]. – Режим доступу: https://www.cisa.gov/stopransomware/ransomware-guide (Дата звернення 28.09.2025).

13. CISA Known Exploited Vulnerabilities Catalog [Електронний ресурс]. – Режим доступу: https://www.cisa.gov/known-exploited-vulnerabilities-catalog (Дата звернення 30.09.2025).

14. CrowdStrike Global Threat Report 2024 [Електронний ресурс]. – Режим доступу: https://www.crowdstrike.com/en-us/resources/reports/crowdstrike-2024-global-threat-report/ (Дата звернення 02.10.2025).

15. Mandiant M-Trends Report 2024 [Електронний ресурс]. – Режим доступу: https://services.google.com/fh/files/misc/m-trends-2024.pdf(Дата звернення 04.10.2025).

16. IBM Cost of a Data Breach Report 2024 [Електронний ресурс]. – Режим доступу: https://www.ibm.com/security/data-breach(Дата звернення 06.10.2025).

17. Verizon Data Breach Investigations Report 2024 [Електронний ресурс]. – Режим доступу: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf(Дата звернення 08.10.2025).

18. Secureworks. LockBit Ransomware Technical Analysis [Електронний ресурс]. – Режим доступу: https://www.secureworks.com/blog/lockbit-in-action (Дата звернення 10.10.2025).

19. Palo Alto Networks Unit42. Cl0p Ransomware Research [Електронний ресурс]. – Режим доступу: https://unit42.paloaltonetworks.com/clop-ransomware/ (Дата звернення 12.10.2025).

20. Elastic Security Labs Global Threat Report 2024 [Електронний ресурс]. – Режим доступу: https://www.elastic.co/security-labs/elastic-publishes-2024-gtr (Дата звернення 14.10.2025).

21. SANS Institute. ICS/EDR Behavioral Detection Whitepaper [Електронний ресурс]. – Режим доступу: https://www.scribd.com/document/794702738/SANS-2024-Detection-Response-Survey (Дата звернення 16.10.2025).

22. Rapid7. Endpoint Detection in Hybrid Environments [Електронний ресурс]. – Режим доступу: https://www.rapid7.com/products/command/exposure-management/ (Дата звернення 18.10.2025).

23. Fortinet Threat Landscape 2024 [Електронний ресурс]. – Режим доступу: https://events.fortinet.com/exec_roundtable_ade/home (Дата звернення 20.10.2025).

24. Check Point Global Cyber Attack Trends 2024 [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/resources/report-3854/report--cyber-security-report-2024-3a0a (Дата звернення 22.10.2025).

25. PwC Global Digital Trust Insights 2024 [Електронний ресурс]. – Режим доступу: https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/pwc-2024-global-digital-trust-insights.pdf (Дата звернення 24.10.2025).

26. Gundaboina, A. K. (2025). Endpoint Detection and Response (EDR) in Healthcare: Mitigating Threats on Critical Devices. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/393318646_Endpoint_Detection_and_Response_EDR_in_Healthcare_Mitigating_Threats_on_Critical_Devices (Дата звернення 26.10.2025).

27. Shulika, K., Balagura, D., Smirnov, A., Nepokrytov, D., & Lytvyn, A. (2024). A method of using modern endpoint detection and response (EDR) systems to protect against complex attacks. [Електронний ресурс]. – Режим доступу:

https://www.researchgate.net/publication/382478670_A_method_of_using_modern_endpoint_detection_and_response_EDR_systems_to_protect_against_complex_attacks (Дата звернення 28.10.2025).

28. Effectiveness of Endpoint Detection and Response Solutions in Combating Modern Cyber Threats (2024). [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/387318838_Effectiveness_of_Endpoint_Detection_and_Response_Solutions_in_Combating_Modern_Cyber_Threats (Дата звернення 29.10.2025).

29. Примаченко, Д., Голобородько, С., Святська, Н., Дьячук, О., & Недодай, М. (2025). EDR та XDR як основні технології захисту кінцевих точок. [Електронний ресурс]. – Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/808 (Дата звернення 01.11.2025).

30. Опірський, І., Дзьобан, Т., & Василишин, С. (2025). Обхід EDR у поєднанні з SIEM: аналіз методів приховування атак у логах. [Електронний ресурс]. – Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/865 (Дата звернення 02.11.2025).

ДОДАТОК А

ПРЕЗЕНТАЦІЯ

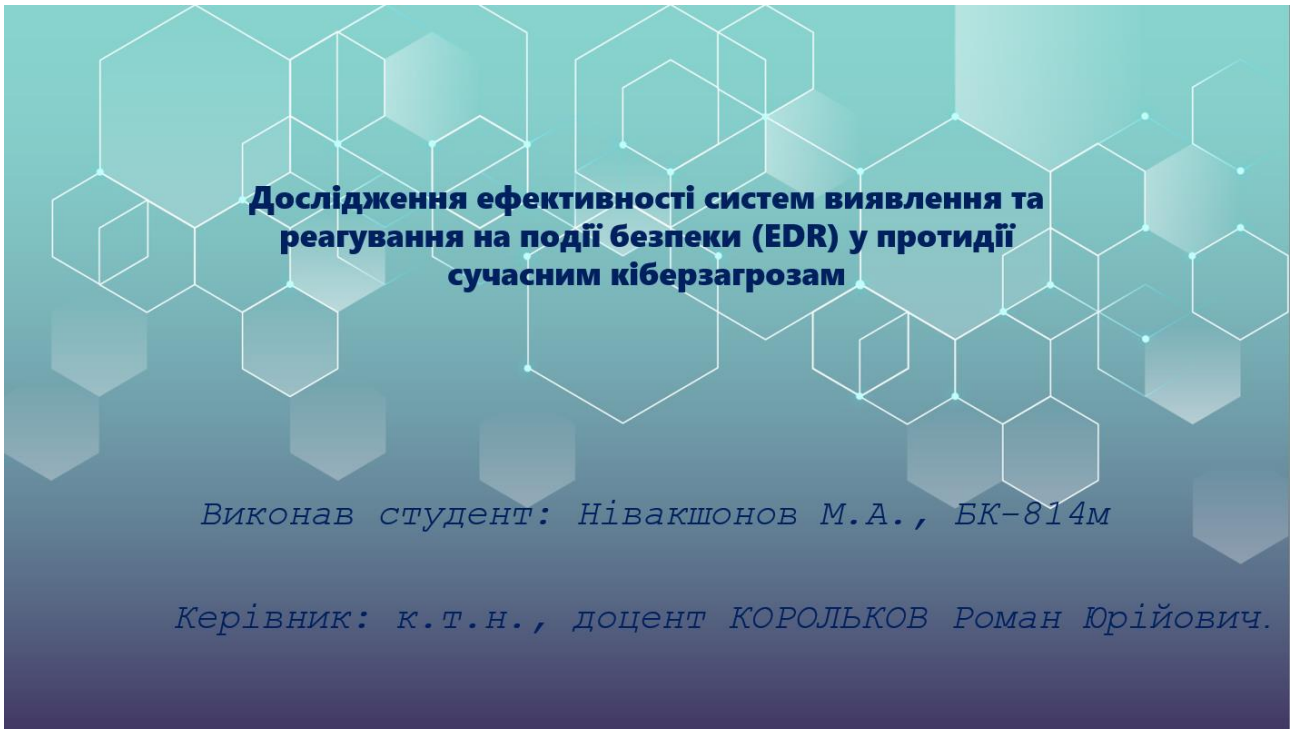

Рисунок А.1 – Титульний слайд

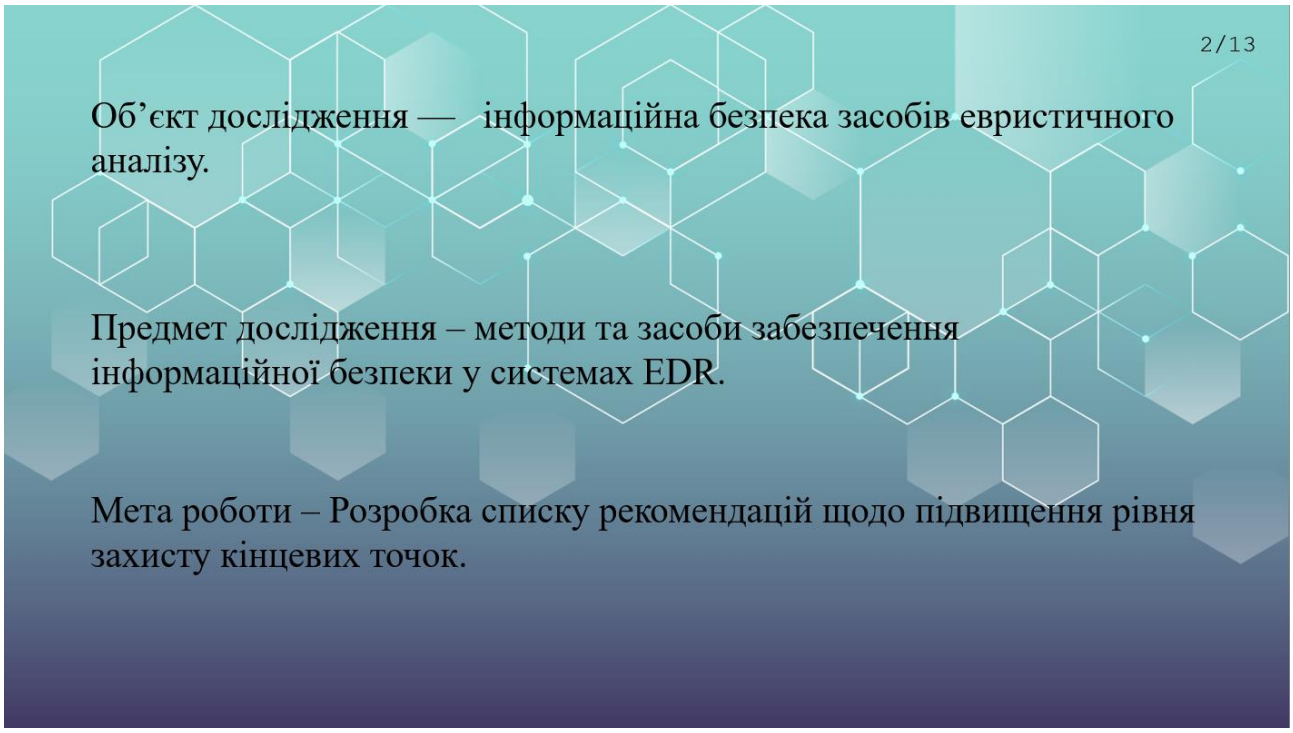

Рисунок А.2 – Слайд 1

Рисунок А.3 – Слайд 2

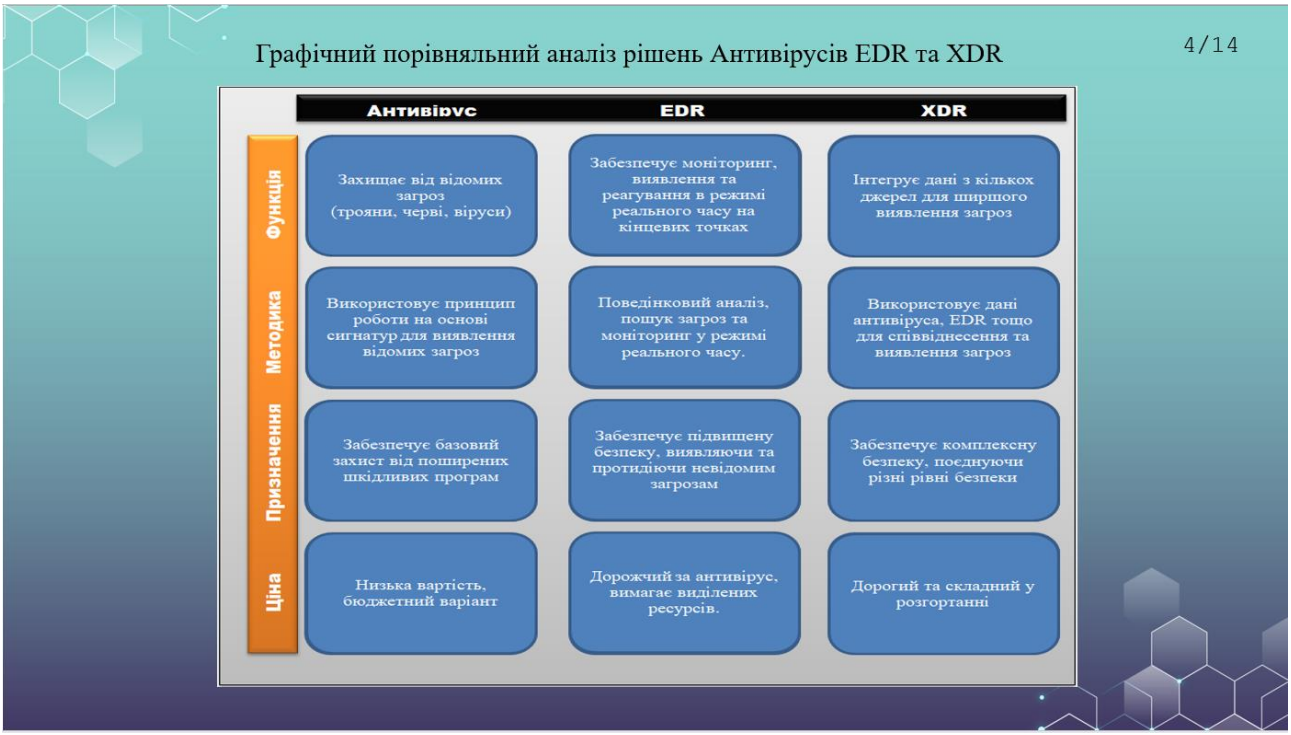

Рисунок А.4 – Слайд 3

Рисунок А.5 – Слайд 4

Рисунок А.6 – Слайд 5

Рисунок А.7 – Слайд 6

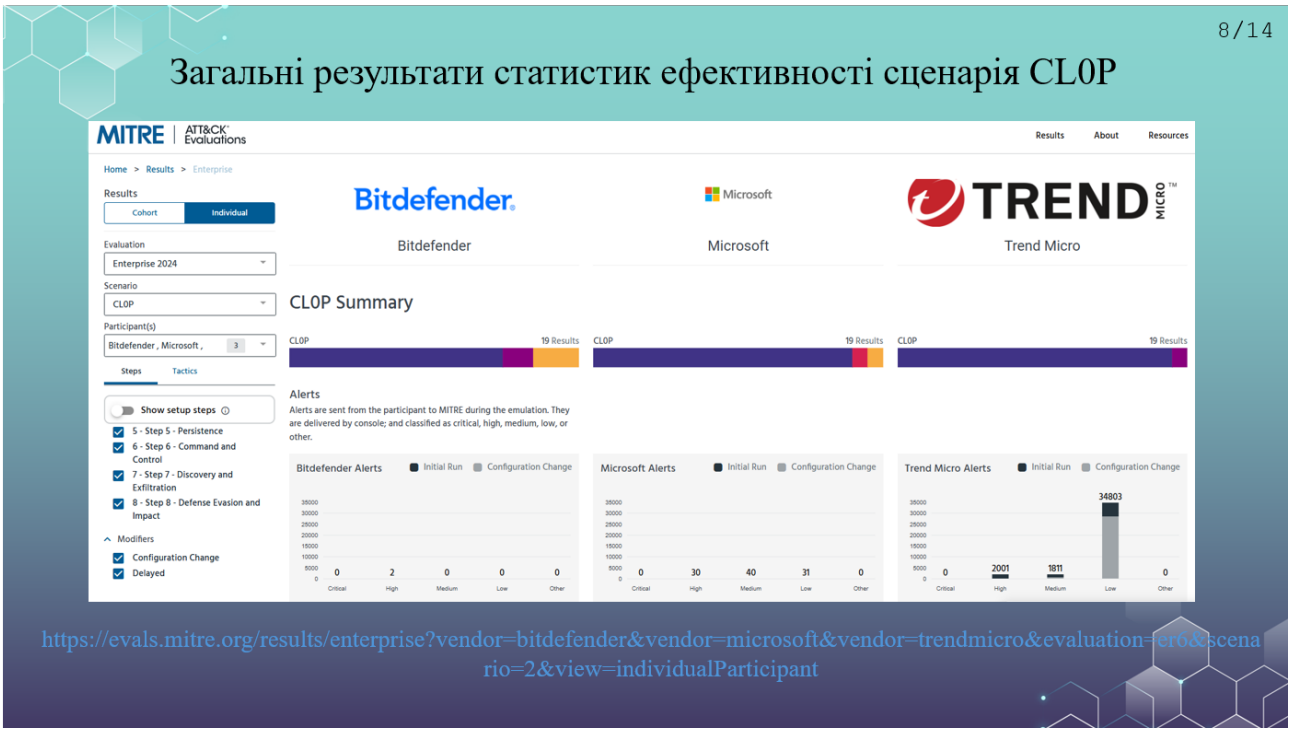

Рисунок А.8 – Слайд 7

Рисунок А.9 – Слайд 8

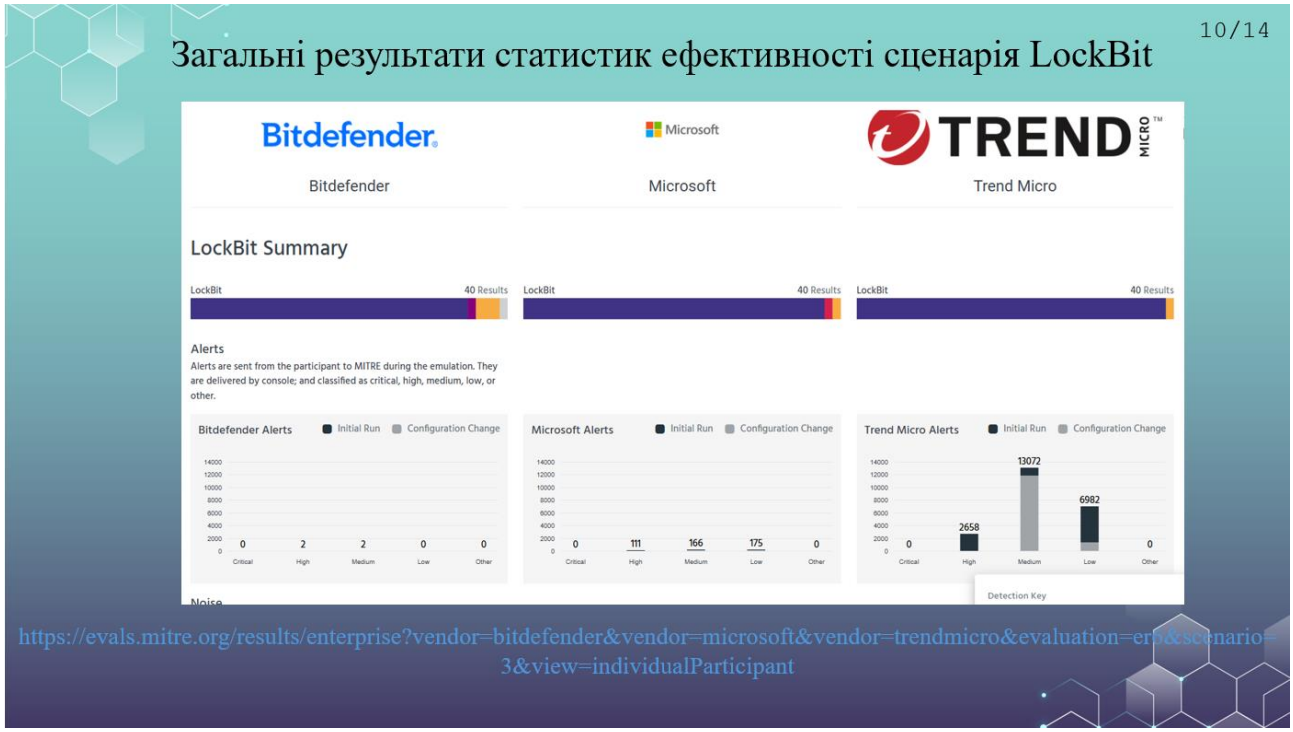

Рисунок А.10 – Слайд 9

Результати тестування спрацювання хибних тривог та сумарна оцінка детекцій кроків атаки

https://evals.mitre.org/results/enterprise?vendor=bitdefender&vendor=microsoft&vendor=trendmicro&evaluation=erb&scenario=3&view=individualParticipant

Рисунок А.11 – Слайд 10

Висновки

1. Покриття технік атаки
- Усі три рішення охопили всі основні етапи MITRE ATT&CK.
- Відсутність пропусків у критичних техніках.

2. Якість детекцій (Specificity)
- Bitdefender: високоспецифічні детекції.
- Microsoft XDR: одна менш специфічна, решта — високої якості.
- Trend Micro: високоспецифічні детекції.

3. False Positives
- Microsoft XDR – 0 FP (найкращий результат)
- Bitdefender – 2 FP
- Trend Micro – 1 FP

4. Noise Steps (шумові спрацьовування)
- У всіх трьох — 8 noise steps
- Рівень шуму приблизно однаковий, але FP впливають на загальну чистоту сигналів.

Рисунок А.12 – Слайд 11

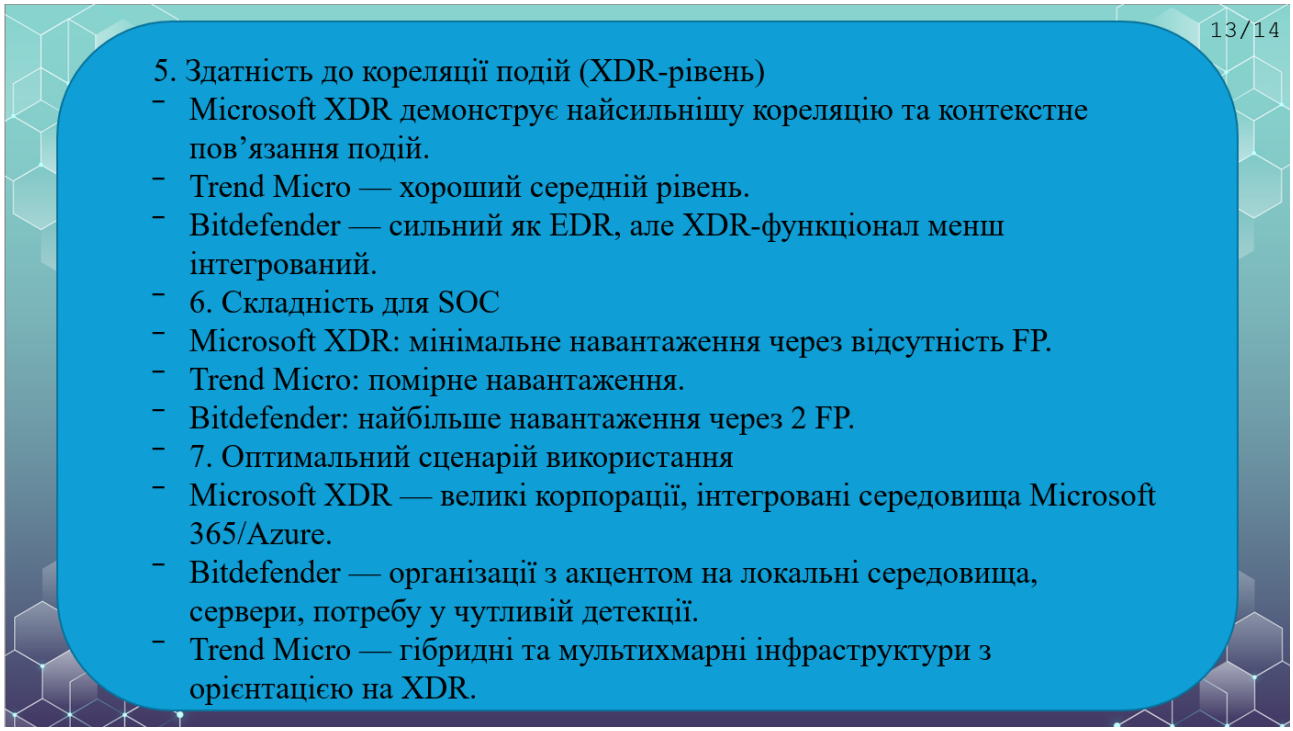

Рисунок А.13 – Слайд 12

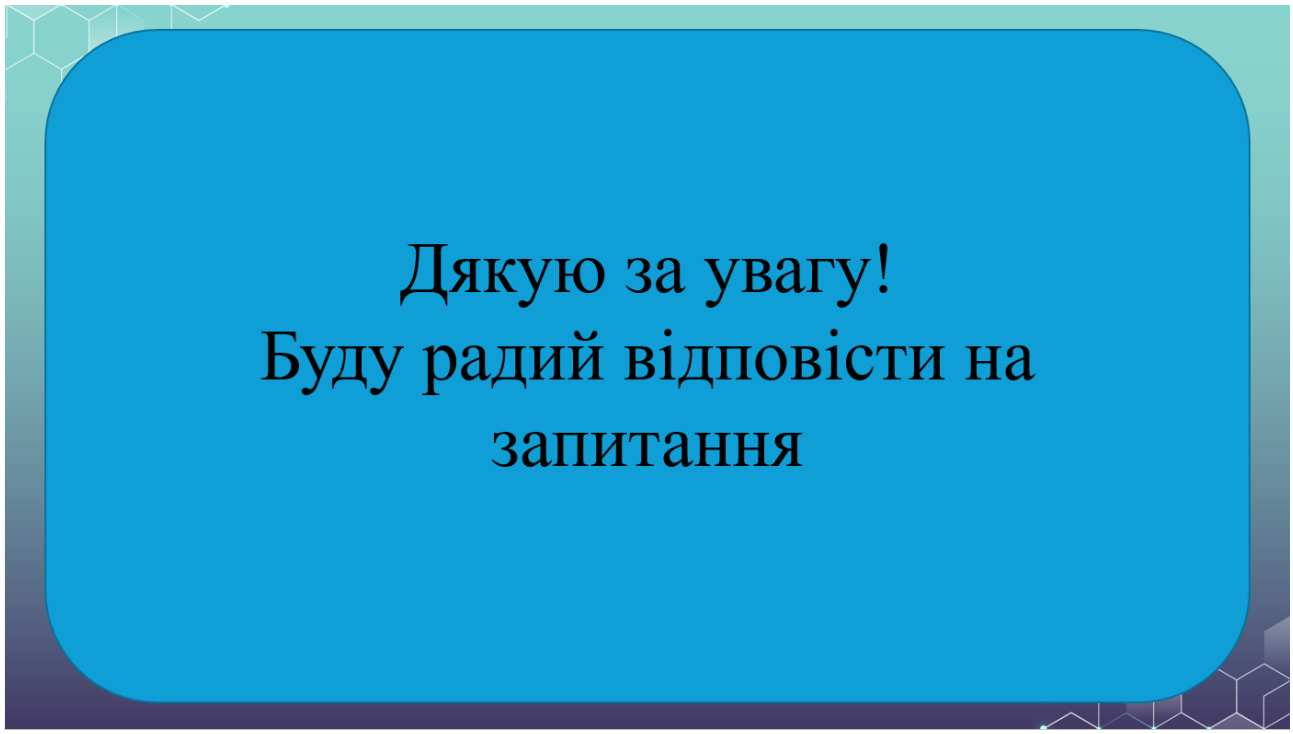

Рисунок А.14 – Слайд 13