УДК 004.056.53:004.492.3
DOI: 10.31673/2409-7292.2025.027390

Опірський І.Р., Олійник А.В., Василишин С.І.

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ XDR РІШЕНЬ ДЛЯ ВИЯВЛЕННЯ ТА УСУВАННЯ ЗАГРОЗ

У контексті цифрової трансформації, коли залежність організацій від IT-інфраструктури стрімко зростає, збільшується і рівень кіберзагроз. Згідно з актуальними даними, кількість кібератак на організації у 2024 році зросла на 75% у порівнянні з попереднім роком, досягнувши 1876 інцидентів на тиждень. У відповідь на ці виклики відбувається еволюція засобів захисту — на зміну традиційним рішенням приходять комплексні системи XDR (Extended Detection and Response). Дослідження фокусується на порівняльному аналізі XDR та EDR (Endpoint Detection and Response) рішень, розкриваючи їх фундаментальні відмінності та практичну ефективність. XDR-платформи забезпечують розширене збирання та аналіз даних з різноманітних джерел (мережеві події, хмарні сервіси, електронна пошта) замість обмеження лише кінцевими пристроями, що дозволяє формувати цілісну картину безпеки організації. Особливу увагу приділено механізмам автоматизації memory forensics в XDR-системах: досліджено, що сучасні платформи здатні автоматизувати збір даних з оперативної пам'яті та розгортати спеціалізовані DFIR-утиліти через механізм "remediation". Проведено практичне порівняння виявлення однакових загроз EDR та XDR на прикладі багатофазної фішингової атаки з використанням LOLBINs, що продемонструвало суттєві переваги XDR у швидкості та точності реагування. Встановлено, що XDR-рішення демонструють вищу ефективність завдяки кореляції подій з різних джерел, застосуванню машинного навчання та поведінкової аналітики. Проаналізовано основні XDR-рішення на ринку (CrowdStrike Falcon, SentinelOne Singularity, Microsoft Defender, Elastic Security) та їх особливості в реалізації механізмів захисту. Результати дослідження підтверджують, що інтеграція XDR з додатковими системами (мережевими пристроями, хмарними сервісами, системами аутентифікації) створює комплексну систему захисту, значно підвищуючи спроможність організацій протидіяти сучасним складним кіберзагрозам. Додатково, дослідження виявило, що XDR-системи ефективно виявляють приховані fileless-атаки та руткіти, які традиційно становлять найбільшу проблему для звичайних засобів захисту. Важливим аспектом є також здатність XDR-рішень зменшувати кількість хибних спрацювань завдяки контекстуальному аналізу подій, що знижує навантаження на команди безпеки та підвищує загальну ефективність операцій SOC. Незважаючи на значні переваги XDR, дослідження підкреслює, що для повноцінного захисту критично важливої інфраструктури необхідне поєднання автоматизованих XDR-рішень з глибокою експертизою DFIR-фахівців, особливо при аналізі нових та невідомих загроз.

Ключові слова: XDR, EDR, CrowdStrike Falcon, Microsoft Defender, шкідливе програмне забезпечення, memory forensics, LOLBINs, безфайлові атаки, кібербезпека, інтеграція систем захисту.

Вступ

В умовах, коли цифрова трансформація охоплює дедалі більше сфер діяльності, зростає і залежність організацій від IT-інфраструктури. Разом з цим зростає і рівень загроз — як зовнішніх, так і внутрішніх. У відповідь на ці виклики відбувається еволюція засобів захисту: на зміну вузькоспеціалізованим рішенням приходять комплексні підходи, які здатні охопити ширший контекст атаки. Саме в цьому контексті дедалі більшої актуальності набувають XDR-системи (Extended Detection and Response), які вважаються наступним етапом розвитку традиційних засобів кібербезпеки.

XDR-рішення пропонують не просто розширення можливостей EDR, а створюють єдину платформу для агрегації, аналізу та кореляції даних із різних джерел. Це дозволяє виявляти складні багатоступеневі атаки, що могли би залишитися непоміченими при ізольованому аналізі. Завдяки інтеграції з мережею, хмарними середовищами, електронною поштою, ідентифікаційними сервісами й іншими джерелами, XDR здатен формувати більш повну картину активності в організації. У підсумку фахівці з безпеки отримують не просто сигнали про інциденти, а цілісні ланцюги подій із контекстом, що значно спрощує реагування.

Використання XDR також відкриває нові горизонти для автоматизації аналітики, зокрема в таких складних процесах, як аналіз пам'яті. Сучасні рішення здатні виявляти нетипову активність навіть на рівні оперативної пам'яті, що є критично важливим у боротьбі з безфайловими атаками та продвинутими шкідливими програмами. Особливо цінною є здатність систем виводити підозрілі шаблони поведінки та формувати рекомендації з урахуванням контексту всієї інфраструктури.

На ринку вже сформувався пул провідних постачальників XDR, які активно розвивають свої продукти, додаючи функціональність штучного інтелекту, машинного навчання та поведінкової аналітики. Водночас вибір рішення залежить від багатьох чинників — від технічної архітектури організації до наявних систем захисту, з якими потрібно забезпечити інтеграцію. У зв'язку з цим виникає потреба у глибокому порівняльному аналізі — не лише функціоналу систем, а й їхньої ефективності в реальних умовах.

XDR стає не просто модним словом, а відповіддю на нові типи загроз, які не вкладаються в класичні сигнатурні або поведінкові рамки. Саме тому дослідження цієї технології є актуальним кроком у напрямку побудови проактивної та адаптивної системи кіберзахисту.

Постановка проблеми

Використання застарілого антивірусного ПЗ, що не здатне усунути нові загрози, створює критичні вразливості в сучасних IT-інфраструктурах. За даними досліджень, кіберзагрози у 2024 році демонструють рекордне зростання. Зокрема, за другий квартал 2024 року зафіксовано 30% збільшення середньої кількості кібератак на організацію порівняно з 2023 роком, а за третій квартал — 75% приріст (до 1876 атак на організацію на тиждень (рис.1) [1]. Цей стрімкий приріст підкреслює, що віртуальні атаки стають дедалі частішими та витонченішими.

Рис. 1. Кількість атак на організацію всередньому за тиждень (2021-2024)

Сучасні загрози відрізняються високою технічною складністю. Наприклад, fileless-атаки виконуються без встановлення звичайного файлу на диску і майже не залишають слідів для традиційного антивірусу. Схожим чином rootkit-и модифікують ядро операційної системи та приховують зловмисні процеси від стандартних засобів виявлення.

Водночас існуючі традиційні рішення мережевої та прикладної безпеки мають суттєві обмеження: сигнатурні антивіруси не встигають за стрімким нарощуванням нових варіантів шкідливих програм (наприклад, у 2018 році щоденно виявлялося близько 350 тисяч унікальних загроз) (рис. 2) [2]. Класичні фаєрволи також дедалі частіше виявляються неефективними проти новітніх тактик зловмисників (експлойти нульового дня, шифрований трафік, поліморфні віруси тощо). Це створює значні «сліпі плями» у захисті, через які кіберзлочинці можуть уникати детекції.

Отже, для протидії таким викликам використовують рішення Extended Detection and Response (XDR). XDR об'єднує та корелює дані з різних джерел — від кінцевих пристроїв та серверів до мережі, хмарних сервісів і поштових систем — забезпечуючи консолідований огляд усіх подій у середовищі. За рахунок кореляції розрізнених сигналів XDR може виявляти

багатоступеневі ланцюжки атак, що залишаються непоміченими при ізольованому аналізі окремих логів. Вбудовані в XDR механізми машинного навчання дозволяють автоматично виявляти приховані загрози й аномалії поведінки, зменшуючи кількість хибних спрацювань і прискорюючи реакцію на інциденти.

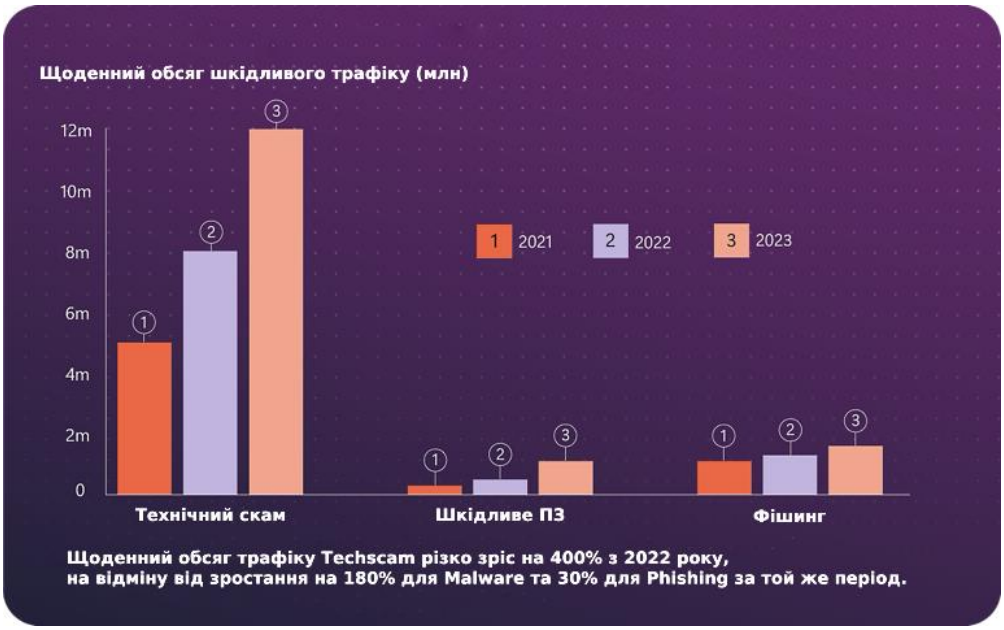

Рис.2. Щоденний обсяг шкідливого трафіку в інтернеті

Проте навіть найсучасніші XDR-системи потребують доповнення експертним аналізом пам'яті, адже «аналіз пам'яті може надати інформацію, недоступну при аналізі диску». Поєднання XDR із ручною меморі-форензикою створює синергію: автоматизовані системи швидко фільтрують та пріоритизують сигнали, а фахівці досліджують in-memory-артефакти атак, забезпечуючи повноцінний захист.

Аналіз останніх досліджень та публікацій

Проблематика XDR-систем та пов'язаних із ними технологій виявлення та реагування на кіберзагрози активно досліджується багатьма науковцями та експертами галузі. У роботі «XDR: The Evolution of Endpoint Security Solutions — Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future» [3] автори розглядають концепцію XDR-платформи, яка, за їхніми словами, «інтегрує кінцеві, мережеві та хмарні дані» для зупинки складних атак. Стверджується, що такий підхід дозволяє об'єднати запобігання, виявлення та реагування у єдину систему з повною наскрізною видимістю та аналітикою. Також автори роблять висновок, що XDR-платформа суттєво підвищує оперативну ефективність захисту та зменшує час реагування завдяки централізації даних. Дослідження «Performance Evaluation of Open-Source Endpoint Detection and Response Combining Google Rapid Response and Osquery for Threat Detection» [4] представляє відкриту EDR-систему на основі Google GRR і Osquery. Тестування цієї системи показало, що за стандартних налаштувань вона виявляє лише близько 28.5% тактик APT-атак. Автори відмічають, що спеціалізація та налаштування правил Osquery може суттєво збільшити покриття виявлення; загалом інтегрована система GRR+osquery демонструє потенціал стати ефективним рішенням з високим охопленням виявлення загроз.

У статті «Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive Review» [5] автори провели всебічний огляд розвитку EDR-технологій. Вони підкреслюють, що EDR-системи відіграють ключову роль в ідентифікації, розслідуванні та реагуванні на загрози в сучасних IT-інфраструктурах. У статті детально описано історію розвитку EDR та вплив на них машинного навчання, поведінкової аналітики і розвідувальної

© Опірський І.Р., Олійник А.В., Василишин С.І. (2025). Дослідження ефективності XDR рішень для виявлення та усування загроз. Сучасний захист інформації, 2(62), 141–157.
https://doi.org/10.31673/2409-7292.2025.027390

інформації про загрози; також обговорюються виклики впровадження (масштабованість, продуктивність, ухиляння від детектування). Аналіз кейсів та індустріальних трендів у роботі свідчить про високу ефективність EDR у боротьбі з сучасними загрозами, а також розглядається перспективна інтеграція EDR з XDR, ШІ та автоматизацією для подальшого підвищення продуктивності систем захисту. У дослідженні «Demystifying Behavior-Based Malware Detection at Endpoints» [6] було досліджено продуктивність ML-методів поведінкового виявлення шкідливого ПЗ безпосередньо на кінцевих пристроях. Виявлено, що моделі, навчені на даних з пісочниць, демонструють високу точність (>90%) у лабораторному середовищі, але їхня ефективність суттєво падає до ~20–50% при застосуванні на реальних кінцевих системах. Автори зазначають, що причини такого розриву — шум міток і різноманітність поведінки у відкритому середовищі — і показують, що тренування на даних реальних пристроїв дозволяє підвищити точність на 5–30% у порівнянні з базовими підходами.

У роботі «XDR: The Evolution of Endpoint Security Solutions» [7] автори розглядають XDR як новий платформний підхід, що об'єднує дані з кінцевих пристроїв, мережі та хмари для забезпечення цілого комплексу функцій — попередження, виявлення, розслідування та реагування на атаки в режимі реального часу. У статті обґрунтовано, що XDR «об'єднує та розширює можливості виявлення й реагування за декількома рівнями захисту», забезпечуючи централізовану видимість організації, глибокий аналіз і автоматичний захист по всьому стеку технологій. Отже, автори роблять висновок, що XDR надає інтегровану, проактивну систему захисту, що спрощує завдання аналітиків безпеки та підвищує оперативність захисту (наприклад, зупинку атак на ранніх стадіях). Аналіз існуючих публікацій свідчить про актуальність і перспективність досліджень у сфері XDR-рішень. Проте залишаються недостатньо висвітленими питання практичної ефективності XDR у порівнянні з EDR при виявленні сучасних складних атак, а також механізми інтеграції XDR з іншими системами безпеки та їхній вплив на загальну ефективність захисту. Ці аспекти і стали предметом дослідження у даній роботі.

Метою даного дослідження є визначення ефективності XDR-рішень для виявлення та усунення сучасних кіберзагроз у порівнянні з традиційними EDR-системами, а також аналіз механізмів інтеграції XDR з іншими компонентами безпекової інфраструктури.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Дослідити ключові відмінності між XDR та EDR з точки зору архітектури, функціоналу та підходів до виявлення загроз.
2. Виявити, яку телеметрію збирають XDR-системи для ідентифікації потенційних загроз та яким чином відбувається кореляція подій з різних джерел.
3. Проаналізувати найпопулярніші додаткові інтеграції, що розширюють можливості XDR-платформ та підвищують їхню ефективність.
4. Дослідити, які етапи memory forensics були автоматизовані за допомогою XDR та які обмеження залишаються при використанні автоматизованих підходів.
5. Провести порівняльний аналіз ефективності виявлення однакових загроз між EDR та XDR на практичних прикладах.
6. Визначити найбільш ефективні XDR-рішення, представлені на ринку, та виявити їхні специфічні особливості в реалізації механізмів захисту.

Виконання поставлених завдань дозволить сформувати комплексне уявлення про актуальний стан розвитку XDR-технологій, їхні переваги та обмеження, а також надати практичні рекомендації щодо впровадження та використання XDR-рішень для підвищення рівня кібербезпеки організацій.

Результати дослідження

Дослідження відмінності між EDR та XDR

EDR та XDR це невід'ємна частина захисту від загроз для ендпоінтів у світі. Але між ними є ключові відмінності і зараз я розкажу чому варто використовувати XDR задля більшої

© Опірський І.Р., Олійник А.В., Василишин С.І. (2025). Дослідження ефективності XDR рішень для виявлення та усування загроз. Сучасний захист інформації, 2(62), 141–157.
https://doi.org/10.31673/2409-7292.2025.027390

безпеки вашої інфраструктури. EDR (Endpoint Detection and Response) – це система виявлення та реагування на загрози, орієнтована на кінцеві пристрої. У епоху, коли традиційні антивірусні рішення стали недостатніми для боротьби з витонченими загрозами, EDR-системи забезпечують моніторинг і захист окремих кінцевих пристроїв у реальному часі. Вони збирають і аналізують дані про активність процесів, зміни файлів та мережеві з'єднання на кожному пристрої, що дає змогу виявляти аномалії й негайно реагувати на атаки.

XDR (Extended Detection and Response) – це розширений підхід до виявлення та реагування на загрози, який використовує дані з декількох компонентів IT-інфраструктури. На відміну від EDR, XDR надає комплексний і цілісний огляд безпеки всієї організації. Він агрегує і корелює телеметрію з різних джерел – кінцевих пристроїв, мережевого трафіку, хмарних сервісів, поштових систем тощо. Таким чином, XDR об'єднує дані з систем типу SIEM, NDR, UEBA і самих EDR, що дозволяє виявляти складні багатокомпонентні атаки, які могли б бути непоміченими традиційним EDR.XDR-аналітика застосовує розширені алгоритми та машинне навчання для кореляції подій між різними доменами, надаючи більш повне розуміння загроз і прискорюючи реагування на них.

Також кожен підхід має як свої плюси так і свої мінуси.

EDR: головний недолік – обмеженість охоплення. Системи EDR мають видимість тільки на рівні окремих пристроїв і не бачать загроз, що поширюються всередині мережі або хмарного середовища. Це створює ризик пропуску багатокрокових атак, які розповсюджуються далі від стартової точки. Також поведінковий аналіз EDR-систем може генерувати значну кількість хибних сповіщень, що збільшує навантаження на команду безпеки.

XDR: недоліками XDR є складність і вартість впровадження. Для роботи XDR необхідно інтегрувати кілька систем та джерел даних, що вимагає ресурсів та кваліфікованих фахівців. Підтримка такої комплексної платформи може бути дорогою, а її налаштування складнішим, ніж у окремих EDR-продуктів.

Таблиця 1

Наведено основні відмінності між EDR та XDR [8]

Можливості	**EDR**	**XDR**
Виявлення загроз	+	+
Постійний моніторинг	+	+
Полювання на загрози	+	+
Реагування на інциденти	+	+
Захист хмарних середовищ	-	+
Захист систем ідентифікації та доступу	-	+
Аналіз мережевого трафіку	-	+
Журналювання для відповідності вимогам	-	+
Керовані послуги	+	+

Таким чином, EDR є спеціалізованим рішенням для виявлення та реагування на загрози на окремих кінцевих пристроях, забезпечуючи швидку локалізацію атак на рівні комп'ютера. Натомість XDR пропонує більш широку перспективу – воно об'єднує дані з кількох доменів

© Опірський І.Р., Олійник А.В., Василишин С.І. (2025). Дослідження ефективності XDR рішень для виявлення та усування загроз. Сучасний захист інформації, 2(62), 141–157.
https://doi.org/10.31673/2409-7292.2025.027390

(мережі, хмари, електронної пошти тощо) і тим самим дозволяє виявляти просунуті багатокомпонентні загрози.

Виявити як XDR виявляють шкідливе програмне забезпечення. XDR спираються на широкий спектр телеметрії та методів (подекуди є інтеграції з e-mail сервером, IAM та MDM сервісами, та інші), щоб виявляти навіть найскладніші загрози. ключові компоненти XDR (рис. 3) [9].

Рис. 3. Архітектура XDR (CrowdStrike Falcon)

Поведінкова аналітика. ml-моделі відстежують відхилення від «норми» для процесів, користувачів і хостів — скажімо, запуск powershell під system із нетиповими аргументами.

Rule-based і yara/ioc-matching. готові правила з хешами, urls, ip-адресами та yara-сигнатурами ловлять відомі зразки шкідника. дані беруться з ti-платформ на кшталт virustotal, otx alienvault, abuse.ch, hybrid analysis, misp, cert-feeds тощо.

Перевірка у пісочницях. підозрілий файл запускають у «пісочниці» та фіксують створені процеси, мережеві з'єднання, зміни реєстру й файлові операції; на основі цього ml-движок вирішує, чи шкідливий зразок.

Аналіз мережевого трафіку (nta/ndr). аналіз мережевих потоків виявляє звернення до сумнівних адрес або трафік на типові c2-порти (4444, 6666).

Шкідливий powershell & wmi детектори. ловлять обфусковані скрипти та wmi-команди, які часто застосовують у windows ad для розвідки (net share, gpo, перелік активних користувачів тощо).

Інтегрована розвідка загроз. автоматично збагачують події даними про фішингові домени, підроблені dkim/dmarc/spf, шкідливі вкладення й аномальні email-заголовки.

Завдяки цим механізмам xdr значно скорочує mean-time-to-detect/response у SOC. Однак найскладніші загрози — fileless malware та руткіти — нерідко «маскуються» під легітимні процеси й вимагають глибокого memory analysis руками dfir-аналітика, щоб остаточно підтвердити компрометацію та згенерувати нові yara/ioc для подальшого підсилення XDR.

Найпопулярніші додаткові інтеграції на xdr

У XDR-системах збирають журнали подій з різноманітних джерел — мережевих пристроїв, хмарних сервісів, систем електронної пошти та провайдерів ідентичності. Типові джерела включають журнали мережевих пристроїв (брандмауери, маршрутизатори) у форматі Syslog/CEF, хмарні журнали активності (наприклад, AWS CloudTrail, Azure Activity Logs чи потоки мережевих безпекових груп), журнали електронної пошти Office 365 (через Microsoft 365 Defender) та журнали входів у Azure Active Directory. Такі дані, як відзначають експерти,

© Опірський І.Р., Олійник А.В., Василишин С.І. (2025). Дослідження ефективності XDR рішень для виявлення та усування загроз. Сучасний захист інформації, 2(62), 141–157.
https://doi.org/10.31673/2409-7292.2025.027390

є «безцінними» для ідентифікації загроз до того, як вони завдадуть шкоди. Наприклад, журнали брандмауерів часто дозволяють виявляти аномалії мережевого трафіку (великі передавання файлів, сканування портів тощо). Хмарні журнали фіксують усі дії в облікових записах і ресурсах (адміністративні, дані та мережеві події), що допомагає знаходити несанкціоновані зміни та аналізувати хід кібератак. Журнали поштових сервісів і дані ідентифікації дозволяють виявляти фішингові атаки та підозрілі спроби входу до облікових записів. Microsoft Defender XDR (Рис.4) інтегрується з низкою продуктів Microsoft для розширеного моніторингу. За допомогою Microsoft Graph Security API ця платформа отримує об'єднані сповіщення від Defender for Endpoint, Defender for Office 365, Defender for Identity, Defender for Cloud Apps та інших компонентів платформи Defender. Azure Active Directory постачає журнали всіх типів аутентифікаційних подій (включаючи інтерактивні та сервісні входи). Також XDR-система може приймати мережеві логи з брандмауерів (наприклад, Azure Firewall) і аналітичних систем. Кожен із цих логів виконує свою роль: журнали Azure AD дозволяють відстежувати компрометацію облікових записів, журнали поштових сервісів — фішингові кампанії і шкідливі вкладення, а мережеві журнали — нетипову активність у мережі.

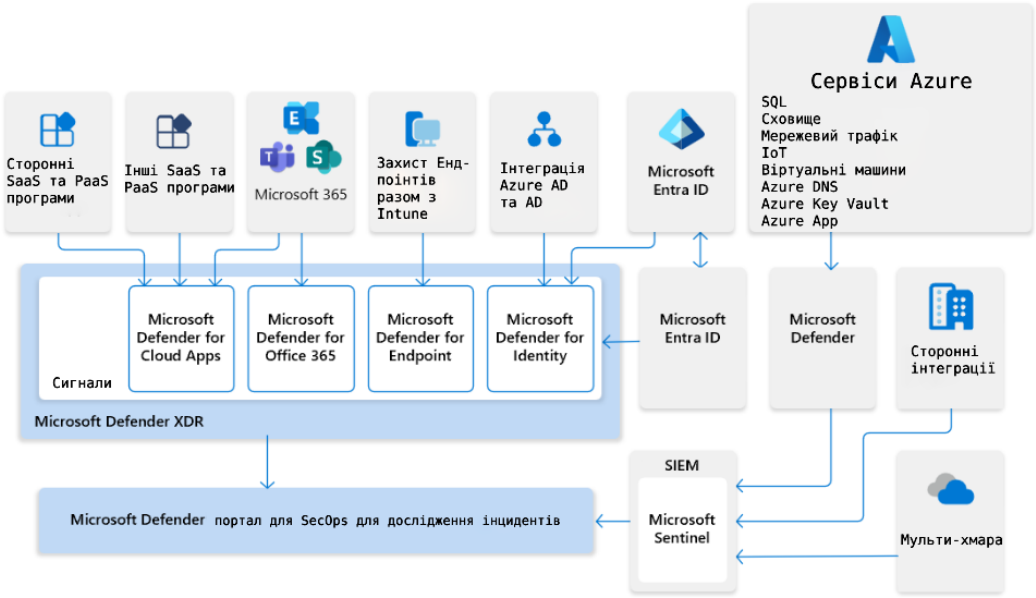

Рис.4. Архітектура XDR (Microsoft Defender) [10]

CrowdStrike Falcon XDR також використовує розмаїття джерел. Система Threat Graph збирає високочастотну телеметрію з усіх кінцевих точок (Windows, macOS, Linux) і хмарних навантажень у масштабах мережі. Модуль Device Control надає повну видимість USB-пристроїв, фіксуючи дані та файли, що передаються через них – це дозволяє виявляти несанкціоновану ексфільтрацію даних або запуск шкідливого ПЗ через USB-носії. Компонент Cloud Workload Protection індексує журнали хмарних сервісів (наприклад AWS CloudTrail та VPC Flow Logs), які допомагають виявляти підозрілі зміни у хмарних середовищах. Поєднання цих джерел дозволяє аналізувати складні сценарії атак: Threat Graph виявляє кореляції між подіями на кінцевих точках, USB-логи сигналізують про передачу чи викрадення даних, а журнали хмарних навантажень — про нетиповий доступ до ресурсів (рис.5.)

Виявлення Reverse-shell by Microsoft Defender

Опис загрози: Reverse-shell яке було створене за допомогою легітимних інструментів Windows (PowerShell).

Короткий опис дій:

- запуск в PowerShell;

© Опірський І.Р., Олійник А.В., Василишин С.І. (2025). Дослідження ефективності XDR рішень для виявлення та усування загроз. Сучасний захист інформації, 2(62), 141–157.
https://doi.org/10.31673/2409-7292.2025.027390

1. {Invoke-WebRequest -URI https://commandcontrol.smartscreentestratings.com};
2. Виявлення та блокування загрози by Microsoft Defender;
3. Приклад інциденту що з'явився в консолі управління Microsoft Defender.

Дослідження: У даному кейсі було проведене тестування чи виявить Microsoft Defender reverse-shell запущений через PowerShell. Користувач відкривши powershell спробував виконати команду Invoke-WebRequest -URI.

https://commandcontrol.smartscreentestratings.com (powershell запит) – що надсилає http/https запит на домен що ми надали в команді. В даному випадку цей домен був нашим прихованим доменом що буде в подальшому надсилати c2 команди. Далі цю активність помітив Microsoft Defender оскільки: 1. Ця активність є підозрілою оскільки зазвичай користувачі відкривають веб сторінку з браузера, а не з powershell. 2. відпрацювала UEBA (Аналіз поведінки користувачів) на підтвердження виконання підозрілих дій.

Всі ці деталі і спричинили те що Microsoft Defender заборонив виконання даного процесу (заблокований процес) (рис. 6), а також створив інцидент в admin консолі (рис. 7.).

Отже сучасні xdr-рішення вміють виявляти загрози які маскуються під звичайну поведінку користувачів використовуючи легітимні програми windows.

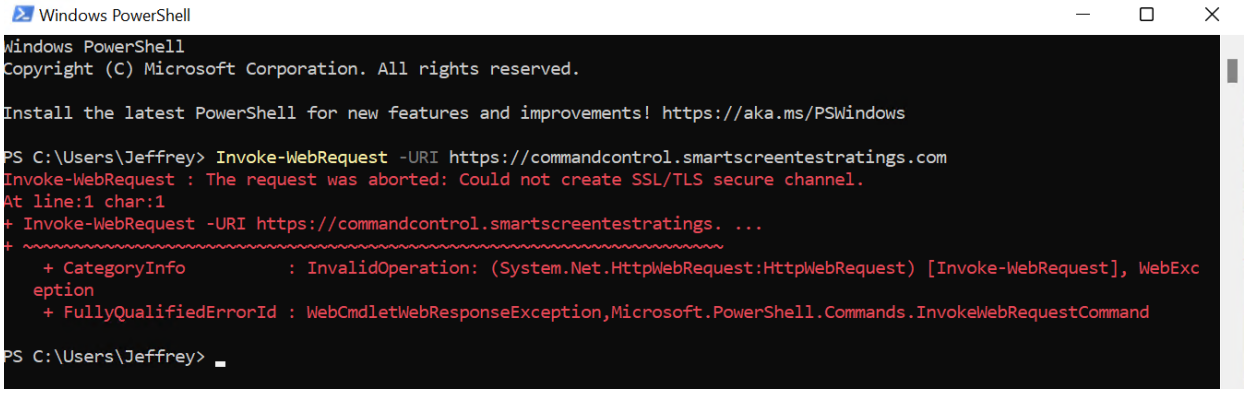

Рис. 5. Powershell запит про нетиповий доступ до ресурсу

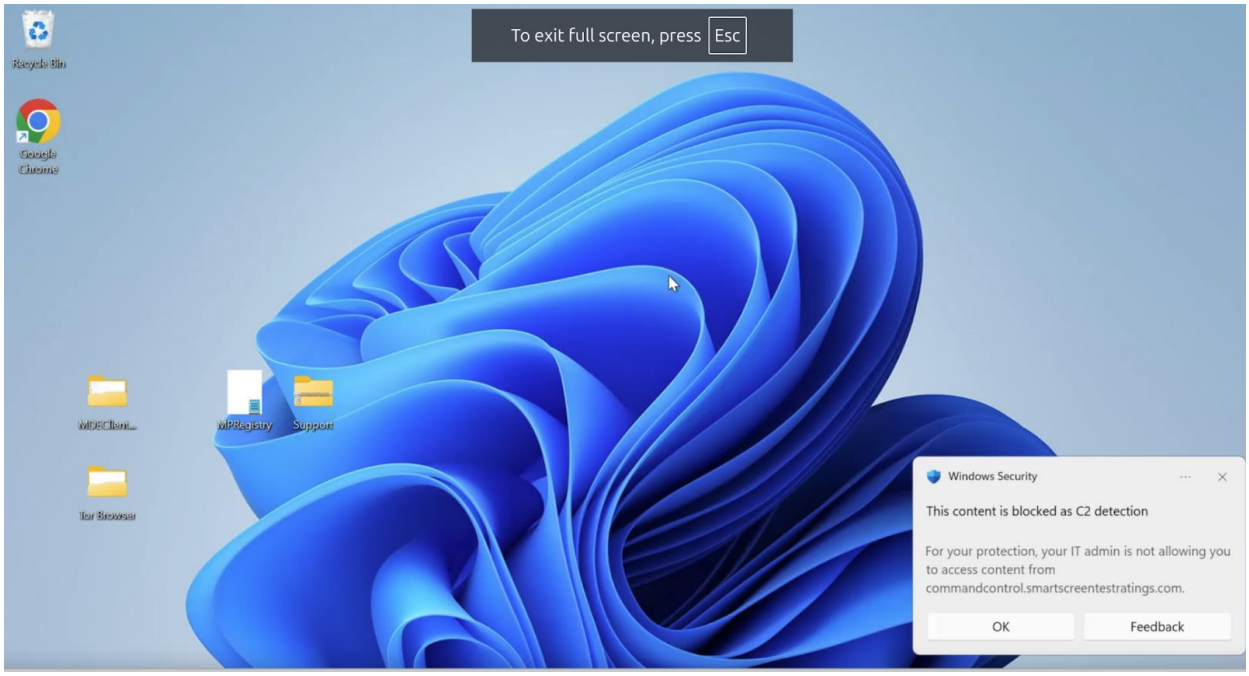

Рис. 6. Заблокований процес Microsoft Defender

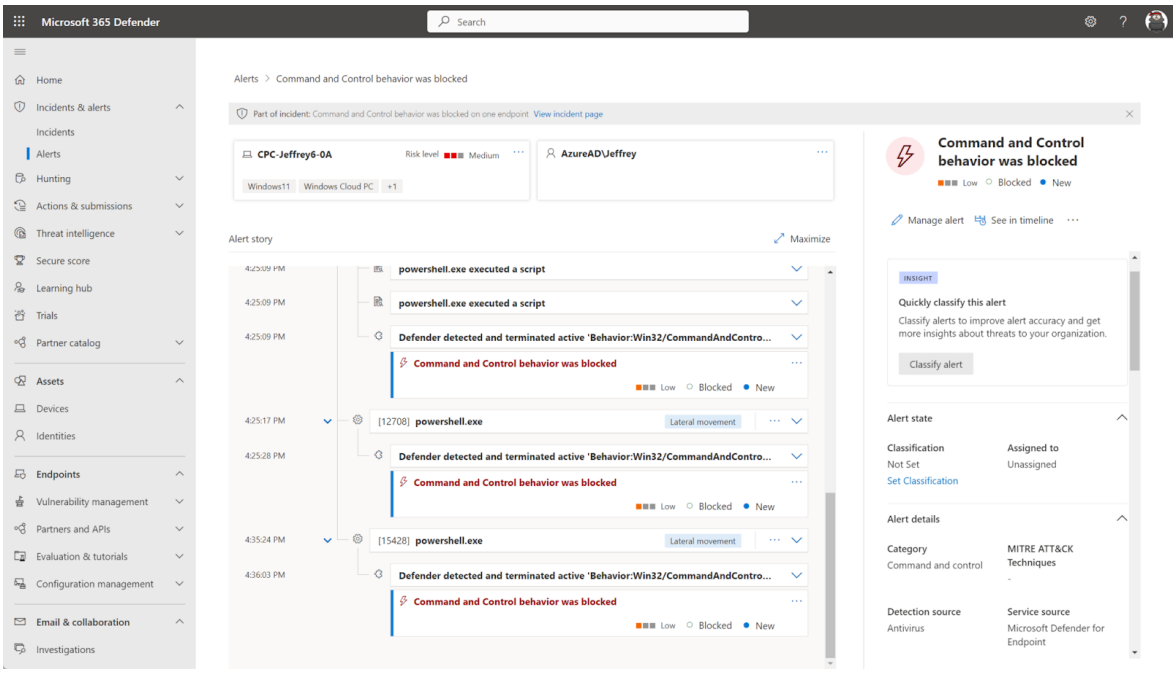

Рис. 7. Інцидент в admin консолі

Приклад інтеграції Microsoft Defender з email-сервером для виявлення підробленого електронного листа

Опис загрози: підроблені електронні листи можуть нести в собі великі ризики безпеки для компанії. Оскільки найслабша ланка захисту це людина, то зазвичай всі атаки в першу чергу спрямовані на них. Спрямовуючи атаку на не технічно підкованих користувачів (бугалтерів, service desk, тощо) хакери можуть легко зламати їх акаунти які потім будуть використовуватися для подальших дій у мережі компанії.

Дослідження:

1. Виявлення скомпроментованого email;
2. Дослідження хедерів емейлу, dkim, dmarc, spf;
3. Перевірка чи користувач був скомпрометований через фішинг.

Опис дослідження: до користувача xxxx@xxxx.com було надіслано лист від ніби то користувача hr@xxxx.com. Перевіривши хедери даного email використовуючи Microsoft Header Analyzer було виявлено що лист було надіслано не з домену xxxx.com а з домену knownbe4.com що є популярною програмою на тест по фішингу у світі. Даний емейл не пройшов перевірку DMARC (Рис.8). (DMARC — технологія, що дозволяє отримувачу електронної пошти перевірити справжність її відправника).Також було помічено підозрілу деталь, яка вказувала на те що лист по часу не співпадав на кілька хвилин в залежності від двох полів для аналізу що також було підмічено. Всі ці фактори і вплинули на те що Microsoft Defender класифікував цей лист як фішинговий та закарантинував його. На даний момент інтеграції xdr з емаіл серверами допомагають зменшити кількість фішингових листів що були успішно проексплуатовані, а також допомагають легше досліджувати їх на предмет APT, інших таргетованих атак, тощо.

Переваги використання XDR та ручної memory forensics

XDR — комплексна, переважно автоматизована система, що поєднує швидкий аналіз пам’яті, ml-евристику, yara/sigma-правила й ioc з threat-intel-фідів. цей інструментарій забезпечує оперативне блокування відомих атак і безперервний моніторинг інфраструктури. Коли ж атакувальники використовують нові техніки (fileless malware, приховані руткіти), необхідна ручна memory forensics. фахівець dfir аналізує дамп пам’яті, відстежує атипові ланцюжки виконання та відновлює повний kill chain. результати розслідування формують

© Опірський І.Р., Олійник А.В., Василишин С.І. (2025). Дослідження ефективності XDR рішень для виявлення та усування загроз. Сучасний захист інформації, 2(62), 141–157.
https://doi.org/10.31673/2409-7292.2025.027390

актуальні yara-сигнатури й ioc, що збагачують xdr і підвищують його точність. Поєднання xdr та memory forensics забезпечує оптимальний баланс між швидкістю реагування і глибиною розслідування, що є ключовою перевагою сучасної кібероборони (табл. 2).

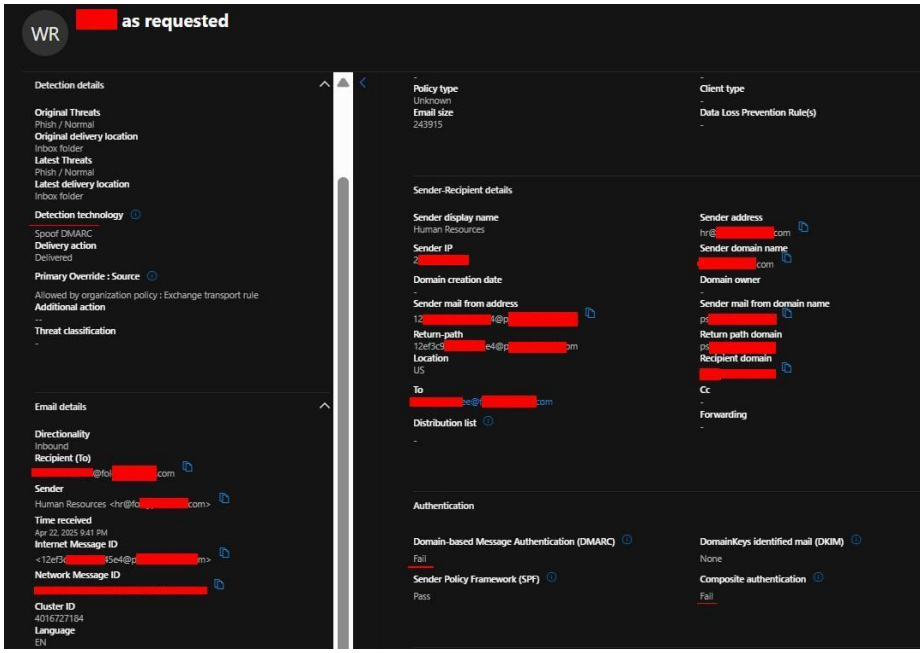

Рис. 8. Скріншот інциденту підробленого листа

Таблиця 2

Основні аспекти форензики пам'яті за допомогою
XDR та ручної перевірки DFIR-спеціалістом

Аспект	**XDR**	**Ручна форензіка (Volatility, тощо)**
Швидкість реакції	Миттєва	Залежить від аналізу оператора
Автоматизація	Повністю автоматизована	Ручна
Глибина аналізу	Середня	Висока
Вимоги до кваліфікації	нижчі (SOC-аналітик може реагувати)	Високі (DFIR-аналітик, threat hunter)
Можливості кастомізації	Обмежена	Повна
Залежність від вендора	Висока	Незалежна

Найкращі XDR рішення

Сьогодні на ринку доступний цілий спектр xdr-рішень, кожне з яких робить акцент на власні сильні сторони. нижче узагальнено чотири найбільш помітні продукти та ті технології, які виділяють їх з-поміж конкурентів. Crowdstrike Falcon спеціалізується на протидії прихованому впорскуванню коду. рушій виявляє dll injection, code injection і process hollowing — прийоми, що дозволяють шкіднику працювати всередині легітимного процеса. окремий детектор ловить shellcode у пам’яті, а поведінкова аналітика підкріплена керованою службою falcon overwatch, яка підтверджує спірні інциденти у режимі

«людина-в-циклі». Sentinelone Singularity робить ставку на безперервний контроль оперативної пам’яті. real-time memory inspection дає змогу виявляти reflective dll-loading і api-hooking до того, як шкідливий код зафіксується на диску. запатентований двигун storyline ai автоматично пов’язує події в єдину хронологію, спрощуючи розслідування. Microsoft Defender глибоко інтегрований у ядро windows та cloud-екосистему azure. продукт відстежує in-memory indicators, виявляє зловживання lolbins (утилітами на кшталт rundll32 чи mshta), а також сканує скрипти через amsi ще до їхнього виконання. Elastic security xdr вирізняється відкритою архітектурою: elastic agent у зв’язці з osquery збирає докладну телеметрію, яку можна миттєво опитувати sql-запитами. платформа підтримує кастомні правила detections-engine та повністю сумісна з yara/sigma, що спрощує обмін знаннями всередині спільноти. Попри різні підходи, усі розглянуті рішення мають спільну мету — швидко виявити безфайлові атаки й загрози, що ховаються лише у пам’яті. crowdstrike концентрується на ін’єкціях, sentinelone — на безперервному моніторингу ram, microsoft — на тісній інтеграції з windows, а elastic — на гнучкості та відкритому коді. вибір платформи залежить від потреб організації: глибини контролю, вимог до open-source, наявності хмарної інфраструктури чи потреби у керованій експертизі. у будь-якому випадку саме комбінація цих технологій формує найбільш повний щит проти сучасних загроз (табл. 3).

Таблиця 3

Основні відмінності, що відрізняють різні XDR-рішення між собою

Рішення	**Memory forensics функції**	**Особливості**
CrowdStrike Falcon	Виявлення dll injection, code injection, process hollowing, shellcode in memory	Потужний behavioral engine, Falcon Overwatch
SentinelOne Singularity XDR	Real-time memory inspection, in-memory attack detection	Patented Storyline AI для відслідковування дій
Microsoft Defender XDR	In-memory indicators, detection of LOLBins, AMSI integration	Глибока інтеграція з Windows
Elastic Security XDR	аналітика пам’яті через Elastic Agent + Osquery + rules	open-source, YARA/Sigma підтримка

Порівняння виявлення виду фішингу (EDR and XDR) що використовує lolbins (підвид fileless malware) для встановлення з'єднання з c2 сервером

Розглянемо ще один тип загроз з розсилки фішингу для встановлення зєднання з c2 сервером (рис. 9).

Рис. 9. Граф подій під час атаки

Зловмисник розсилає фішингові листи та приватні повідомлення, які ведуть на щойно зареєстрований, але «безпечний»-з-вигляду домен із tls-сертифікатом. На сторінці жертву зустрічає підроблена re-captcha (рис. 10): після кліку «i'm not a robot» з'являється зелена позначка успіху, хоча насправді в той момент javascript виконує приховану операцію — він копіює в буфер обміну команду {mshta https://cdn-stealth[.]xyz/drop.hta} (рис. 11). Далі на екрані спливає інструкція-настанова: аби завершити перевірку, натисніть win + r і просто вставте те, що вже скопійовано (Підроблена Captcha 3 (рис. 12)). Користувач виконує підказку, запускаючи таким чином системний інтерпретатор mshta.exe. програма завантажує файл drop.hta з домену зловмисника; усередині hta-скрипт тягне прихований powershell-payload і запускає його без видимих вікон. payload установлює в пам'яті info-stealer, який збирає з браузерів паролі, cookies і дані криптогаманців, після чого надсилає здобич на команд-і-контроль-сервер через https. Усе відбувається під виглядом дій, ініційованих самим користувачем та з використанням підписаних microsoft-бінарників, тому стандартні захисні системи майже не реагують.

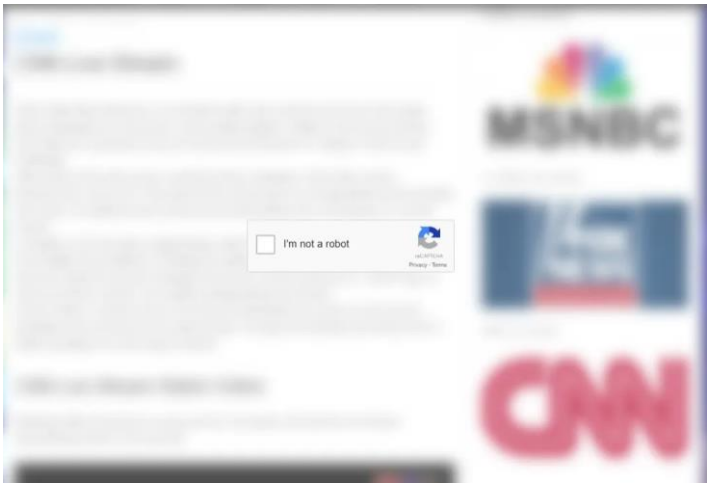

Рис.10. Підроблена Captcha 1

XDR: ми бачимо сам інцидент (може включати в собі кілька алертів) який був згенеровано в Microsoft Defender (Підроблена Captcha XDR інцидент). У ньому видно на що саме стригерився інцидент який включає в себе кілька алертів: 1. Виконання через mshta.exe підозрілої команди що ймовірніше за все використовуючи обфускований powershell скрипт встановлювала з'єднання з C2 сервером. Перед цим алертом ми також бачимо зміну в реєстрі, де для ключа *a* було встановлене значення "mshta …." це вказує на те яка команда та де було виконана, оскільки всі команди які запускаються за допомогою програми "виконати" відображаються в регістрі HKU. Також тут ми маємо змогу перевірити звідки було завантажено цей файл, оскільки нам дає таку можливість Microsoft Defender, коли показує всі процеси що були запущені на ПК від часу його останнього запуску. Також ми бачимо що цей файл було завантажено з Microsoft Outlook (аналог Gmail від Microsoft). Інтеграція Microsoft Defender та Microsoft Exchange дає нам змогу перевірити хто надіслав цей лист, якщо це внутрішній користувач перевірити його на ознаки скомпроментованого акаунту, або на ознаки шпіонажу. Це все ми можемо дізнатися з Microsoft Defender оскільки такі можливості дає нам великий його список інтеграцій.Оцінка за якість відпрацювання 10/10 оскільки все було виявлено та знешкоджено, також була змога дослідити те як ця загроза з'явилася на хості.

EDR: SentinelOne також помітив загрозу, але виявив і знешкодив він її на іншому етапі. Як можна побачити [Підроблена Captcha EDR інцидент] виявив він її на стадії завантаження файлу через powershell. Тобто він не зміг проаналізувати память, і зрозуміти що перша команда в powershell яка була сильно обфускована і мала вигляд "w h -nop -ep un -E.

JABFAGsAWgBKAGgAVQBaACAAPQAgACcANgA5ADYANQA3ADgANQAzADcAN
AA2ADEANwAyADcANAAyAEQANQAwADcAMgA2AEYANgAzADYANQA3ADMANwAz
ADIAMAAyADI…" що вона є шкідливою для системи. Він це не зробив, що показує також рівень та швидкість детекції складних загроз EDR системами. Також ми не можемо проаналізувати як з'явилася ця загроза на системі, оскільки ми не бачимо повної картини дерева процесів, а тільки те що сталося і було запущено після mshta.exe.

Відсутність інтеграції не дає нам змогу спростити версію корпоративного фішингу, що також є важливим упущенням тут. Оцінка за відпрацювання 6/10 все також було виявлено і знешкоджено але на дві стадії атаки пізніше, також обмежений скоуп інтеграції не дає змогу дослідити як загроза з'явилася на хості.

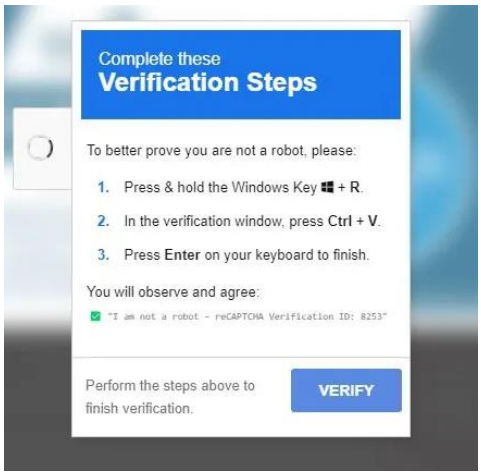

Рис. 11. Підроблена Captcha 2

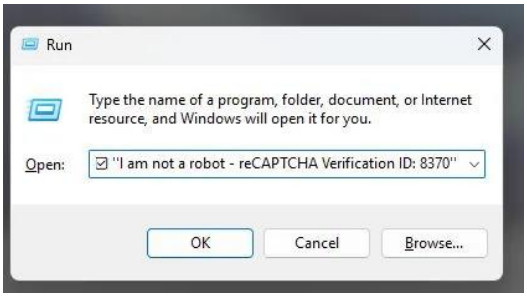

Рис.12. Підроблена Captcha 3

Сучасні xdr-платформи навчились «ловити» саме такі ланцюжки — від clipboard-хайджеку до виклику mshta та in-memory payload-ів (рис. 12-13).

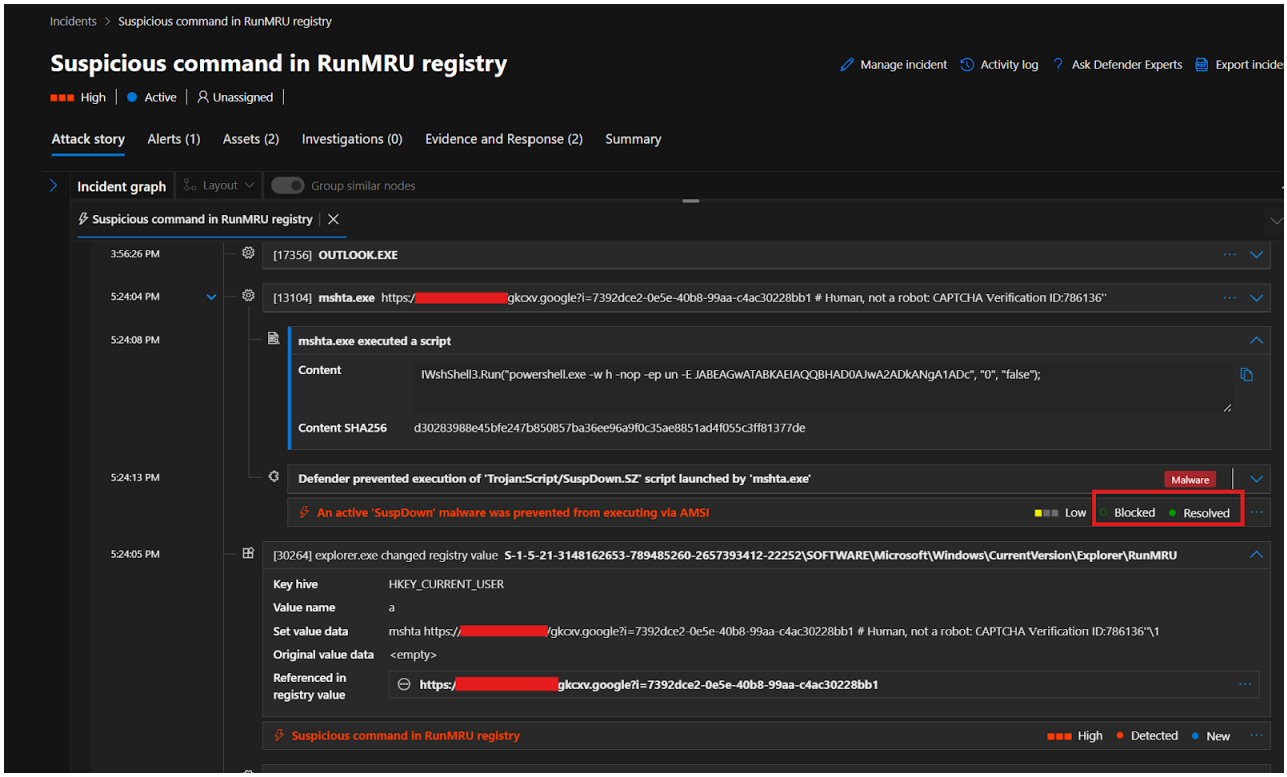

Рис. 12. Підроблена Captcha XDR інцидент

© Опірський І.Р., Олійник А.В., Василишин С.І. (2025). Дослідження ефективності XDR рішень для виявлення та усування загроз. Сучасний захист інформації, 2(62), 141–157.
https://doi.org/10.31673/2409-7292.2025.027390

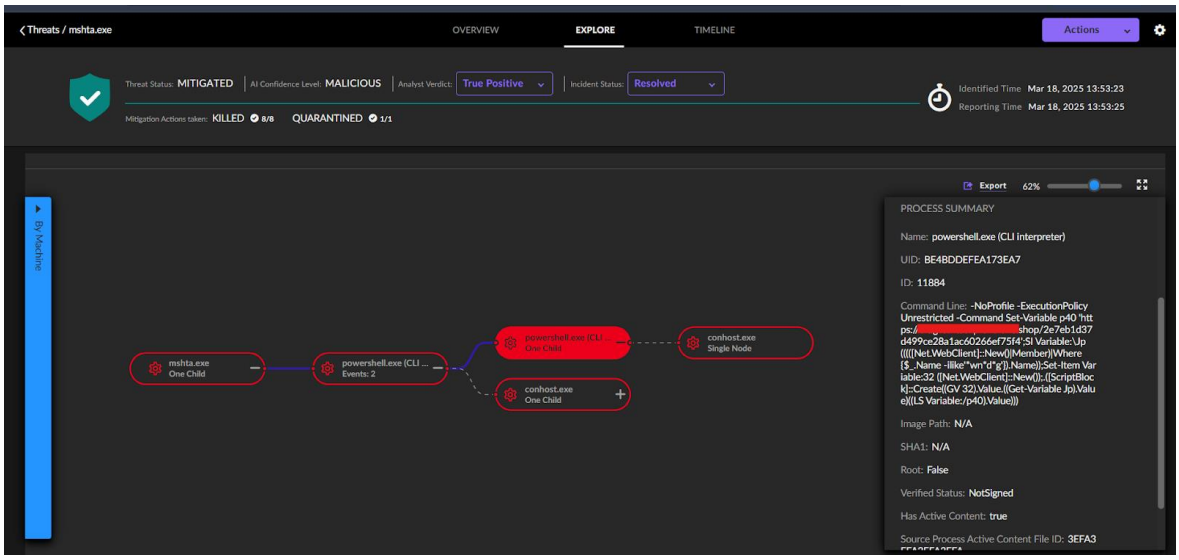

Рис. 13. Підроблена Captcha EDR інцидент

Узагальнення результатів порівняльного аналізу XDR-рішень

Проведене дослідження ефективності XDR-рішень у порівнянні з традиційними EDR-системами дозволило виявити ключові переваги та обмеження кожного підходу до забезпечення кібербезпеки. Встановлено, що основною перевагою XDR-платформ є здатність до формування єдиної картини загрози на основі даних з різних джерел, що особливо важливо при виявленні складних багатоступеневих атак.

Розглянуті практичні приклади протидії фішинговим атакам та виявлення шкідливої активності переконливо демонструють, що XDR-рішення забезпечують більш раннє виявлення потенційних загроз та створюють ширший контекст для їх аналізу. Водночас, ефективність XDR суттєво залежить від якості інтеграції з різними компонентами IT-інфраструктури та налаштування кореляційних правил.

Найбільш перспективними виявилися XDR-рішення, які поєднують потужні можливості аналізу поведінки (як у CrowdStrike Falcon), безперервний моніторинг пам'яті (як у SentinelOne Singularity), глибоку інтеграцію з операційною системою (як у Microsoft Defender) та гнучкість налаштування (як у Elastic Security). При цьому жодне з досліджених рішень не забезпечує повної автоматизації процесів розслідування інцидентів, особливо при роботі з новими типами загроз.

Результати порівняльного тестування XDR та EDR на прикладі виявлення багатофазної фішингової атаки підтверджують, що XDR-системи забезпечують суттєво вищу повноту бачення атаки та можливість її раннього виявлення. XDR здатні відстежувати весь ланцюжок атаки, починаючи від маніпуляцій з буфером обміну і закінчуючи встановленням зв'язку з командним центром зловмисника, тоді як EDR-системи часто виявляють лише окремі фрагменти цього ланцюжка, не поєднуючи їх в єдину картину.

Отримані результати мають важливе практичне значення для організацій, які прагнуть підвищити рівень захисту своєї IT-інфраструктури та перейти від реактивної до проактивної парадигми кібербезпеки. Впровадження XDR-рішень дозволяє не лише підвищити ефективність виявлення та реагування на загрози, але й оптимізувати роботу команд безпеки за рахунок зменшення кількості хибних спрацювань та автоматизації рутинних операцій.

Висновки

У результаті дослідження було встановлено, що XDR (Extended Detection and Response) суттєво відрізняється від традиційних EDR (Endpoint Detection and Response) рішень. Платформи XDR поширюють збирання та аналіз даних на різні лог сорси (мережеві події, хмарні сервіси, електронну пошту, тощо) замість обмеження тільки ендпоінтами. Це дозволяє

© Опірський І.Р., Олійник А.В., Василишин С.І. (2025). Дослідження ефективності XDR рішень для виявлення та усування загроз. Сучасний захист інформації, 2(62), 141–157.
https://doi.org/10.31673/2409-7292.2025.027390

отримати цілісне уявлення про безпеку організації: XDR корелює події з кількох джерел (наприклад, SIEM, UEBA, NDR разом з EDR) і будує єдину картину кіберінциденту. Така інтеграція дає змогу виявляти складні багатофазні атаки, які традиційне EDR не помічає. Зокрема, якщо атака починається з компрометації ендпоінта, EDR виявить її на цьому початковому етапі, але може не помітити подальше латеральне пересування зловмисника. Натомість XDR, збираючи дані з мережевих потоків, хмарних сервісів, ідентичностей тощо, може відразу ідентифікувати нетипову поведінку (наприклад, адмінську активність звичайного користувача) і виявити всю послідовність дій «за лаштунками» атаки. Отже, у порівнянні з EDR, XDR демонструє кращу здатність до виявлення складних загроз завдяки глибшому аналізу корельованих даних і використанню машинного навчання.

XDR-платформи характеризуються широким спектром збирання телеметрії для виявлення загроз. До стандартних даних відносяться події мережевого трафіку (шаблони потоку, періметричні та латеральні з'єднання, підозріла активність, TLS-фінгерпрінт), журнали хмарних робочих навантажень (конфігураційні зміни, активації нових інстансів, дії користувачів, виконані команди, файлові операції, зміни реєстру), телеметрія електронної пошти (метадані повідомлень, прикріплення, зовнішні посилання, активність користувача) та дані з кінцевих пристроїв (запущені процеси, виконані команди, мережеві з'єднання, операції з файлами та реєстром).

Таким чином, XDR-консолідують різнорідну телеметрію, що дозволяє реконструювати ланцюжки атаки від початку і до кінця. Завдяки цьому платформа отримує контекст за подіями: наприклад, поєднання реєстраційних записів про виконання процесів на ендпоінтах і патернів мережевого руху може вказати на приховане інфікування, яке окремо жоден з джерел не виявив би. Така комплексна телеметрія є критичною для кореляції подій та раннього виявлення складних загроз.

Встановлено, що XDR-системи пропонують численні додаткові інтеграції з іншими рішеннями безпеки. Зокрема, вони орієнтовані на об'єднання даних із мережевими пристроями (фаєрволи, IDS/IPS), хмарними сервісами і сервісами аутентифікації. Наприклад, XDR «підтягуватиме» події з системи управління ідентичностями чи фаєрволів. Перевага глибоких інтеграцій – у повноті картини ситуації: коли всі контрольно-пропускні точки й джерела сигнатур зламу пов'язані, XDR може більш точно визначати походження загрози.

У контексті memory forensics досліджено, що XDR-платформи значною мірою автоматизують етапи збору даних з оперативної пам'яті. Крім того, XDR може розгортати спеціалізовані DFIR-утиліти (наприклад, KAPE) через механізм «remediation», автоматизуючи збір артефактів (файлів, реєстру, образів пам'яті) під час інцидентів. Таким чином, у процесі memory forensics XDR бере на себе операції з вилучення пам'яті та первинного збору артефактів, що суттєво скорочує час на підготовчі кроки розслідування. Хоча детальний аналіз отриманого образу пам'яті, як правило, виконується зовнішніми інструментами, «телеметрійний» підхід XDR забезпечує накопичення інформації (про процеси, мережеві з'єднання тощо) і без прямого зняття образу, що часто замінює частину ручної роботи. Загалом, XDR робить етапи memory forensics більш оперативними та менш трудомісткими.

При безпосередньому порівнянні детекції однакової загрози EDR та XDR виявилося, що XDR дає змогу помітно швидше і точніше реагувати на багатофазні атаки. Завдяки широкому охопленню даних XDR відстежує приховані зв'язки між подіями: наприклад, послідовні сигнали компрометації (запуск шкідливого коду на ендпоінті, подальші аномалії в мережі, підозрілі дії користувача тощо) розпізнаються як єдиний ланцюжок загрози. У ситуації тестування однакової хмарної чи фішингової атаки EDR може спочатку видати сповіщення про інфікований пристрій, а подальші кроки зловмисника (латеральний рух, ексфільтрація) виявити пізніше або з великим запізненням. Натомість XDR автоматично фіксує такі ланцюгові переходи і видає більш цілеспрямовані сигнали: він не тільки вказує на сам пристрій, а й намагається інтегрувати аналогічні події з різних сенсорів у єдину атаку. Це

дозволяє аналітикам більш проактивно реагувати і знижувати кількість хибних спрацювань. В цілому, порівняльний аналіз підтверджує переваги XDR у підвищенні якості виявлення складних загроз за рахунок розширеної кореляції даних та автоматизації, тоді як EDR залишається ефективним для ізольованих інцидентів на кінцевих пристроях, але не забезпечує такого ж наскрізного покриття.

Перелік посилань

1. Check Point Research Reports Highest Increase of Global Cyber Attacks Seen in Last Two Years – a 30% Increase in Q2 2024 Global Cyber Attacks. URL: https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks (дата звернення: 10.05.2025).

2. Microsoft Digital Defense Report: 600 million cyberattacks per day around the globe. URL: https://news.microsoft.com/en-cee/2024/11/29/microsoft-digital-defense-report-600-million-cyberattacks-per-day-around-the-globe/ (дата звернення: 10.05.2025).

3. «XDR: The Evolution of Endpoint Security Solutions – Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future» [Електронний ресурс]. Режим доступу: https://www.researchgate.net/ publication/ 354190628 _ XDR _ The_ Evolution_ of_ Endpoint_ Security_ Solutions_ Superior_ Extensibility_ and_ Analytics_to_ Satisfy_the_Organizational_Needs_of_the_Future.

4. «Performance Evaluation of Open-Source Endpoint Detection and Response Combining Google Rapid Response and Osquery for Threat Detection» [Електронний ресурс]. Режим доступу: https://www.researchgate.net/ publication / 358697816 _ Performance _Evaluation_of_Open-Source_Endpoint_Detection_and_Response_Combining_ Google_Rapid_Response_and_Osquery_for_Threat_Detection.

5. «Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive Review» [Електронний ресурс]. Режим доступу: https: // www.e3s-conferences.org / articles / e3sconf / pdf / 2024/86/e3sconf_ rawmu2024_01006.pdf.

6. Demystifying Behavior-Based Malware Detection at Endpoints» [Електронний ресурс]. Режим доступу: https://arxiv.org/html/2405.06124v1.

7. XDR: The Evolution of Endpoint Security Solutions -Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/ 354190628 _ XDR _ The _ Evolution_of_Endpoint _ Security _ Solutions _ Superior _ Extensibility_and_Analytics_to_ Satisfy_the_Organizational_Needs_of_the_Future#:~:text=XDR%3A%20The%20Evolution%20of%20Endpoint,Organizational.

8. Antivirus vs EDR vs XDR: Key Differences and Benefits. URL: https://www.threatintelligence.com/blog/ antivirus-vs-edr-vs-xdr (дата звернення: 10.05.2025).

9. Extended Detection and Response (XDR). CrowdStrike. URL: https: // www.crowdstrike.com/en-us/cyber-security-101/endpoint-security/extended-detection-and-response-xdr/ (дата звернення: 10.05.2025).

10. Microsoft 365 Defender integration with Microsoft Sentinel. Microsoft Learn. URL: https://learn.microsoft. com / en-us / azure / sentinel / microsoft-365-defender-sentinel-integration?tabs=defender-portal (дата звернення: 10.05.2025).

11. Block C2 communication with Defender for Endpoint. URL: https://jeffreyappel.nl/block-c2-communication-with-defender-for-endpoint/ (дата звернення: 10.05.2025).

12. Fake CAPTCHA websites hijack your clipboard to install information stealers. Malwarebytes. URL: https://www.malwarebytes.com/blog/news/2025/03/fake-captcha-websites-hijack-your-clipboard-to-install-information-stealers (дата звернення: 10.05.2025).

13. Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges: [Електронний ресурс]. Режим доступу: https: // www.researchgate.net/publication/364769363_Fileless_ malware_threats_Recent_advances_analysis_approach_through_memory_forensics_and_research_challenges.

14. A Malware Detection Approach Based on Deep Learning and Memory Forensics: [Електронний ресурс]. Режим доступу: https://www.mdpi.com/2073-8994/15/3/758.

15. Microsoft Detection Tools Sniff Out Fileless Malware: [Електронний ресурс]. Режим доступу: https:// www.trendmicro.com / vinfo / us /security/news/cybercrime-and-digital-threats/microsoft-detection-tools-sniff-out-file-less-malware.

16. The Role of Anomaly Detection in XDR: Enhancing Threat Visibility and Response: [Електронний ресурс]. Режим доступу: https://fidelissecurity.com/cybersecurity-101/xdr-security/anomaly-detection-in-xdr-solutions/.

17. Cortex XDR IOC rule details: [Електронний ресурс]. Режим доступу: https://docs-cortex.paloaltonetworks. com/r/Cortex-XDR/Cortex-XDR-Cloud-Documentation/IOC-rule-details.

18. XDR Threat Investigation: [Електронний ресурс]. Режим доступу: https: // docs.trendmicro.com/en-us/ documentation/article/trend-vision-one-xdr-threat-investigation-whatsnew.

19. Perks of Sigma and YARA rules in an EDR: [Електронний ресурс]. Режим доступу: https://harfanglab.io /blog/product/perks-sigma-yara-edr/.

© Опірський І.Р., Олійник А.В., Василишин С.І. (2025). Дослідження ефективності XDR рішень для виявлення та усування загроз. Сучасний захист інформації, 2(62), 141–157.
https://doi.org/10.31673/2409-7292.2025.027390

20. What Are SIGMA Rules: [Електронний ресурс]. Режим доступу: https://socprime.com/blog/sigma-rules-the-beginners-guide/.

21. What is a C2 server? [Електронний ресурс]. Режим доступу: https://www.portnox.com/cybersecurity-101/what-is-a-c2-server/.

22. Offensive WMI – Active Directory Enumeration [Електронний ресурс]. Режим доступу: https://0xinfection.github.io/posts/wmi-ad-enum/.

23. DKIM, SPF and DMARC Guid [Електронний ресурс]. Режим доступу: https: // www.mimecast.com/content/dkim-spf-dmarc-explained/.

24. Block C2 communication with Defender for Endpoint: [Електронний ресурс]. Режим доступу: https://jeffreyappel.nl/block-c2-communication-with-defender-for-endpoint/.

25. How Cortex XDR Global Analytics Protects Against Supply Chain Attacks: [Електронний ресурс]. Режим доступу: https://www.paloaltonetworks.com/blog/security-operations/how-cortex-xdr-global-analytics-protects-against-supply-chain-attacks/.

26. Antimalware Scan Interface (AMSI): [Електронний ресурс]. Режим доступу: https://learn.microsoft.com/windows/win32/amsi/antimalware-scan-interface-portal.

Надійшла 20.05.2025