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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Рекомендації щодо виявлення складних загроз та цільових атак засобами XDR»

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

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

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

_____ Олександр ШЕВЧЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСД-44
ШЕВЧЕНКО Олександр
(прізвище, ім'я)

Керівник асистент кафедри, МУРЗІН Ігор
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ВСТУП

Актуальність дослідження. Складні загрози та цільові атаки, зокрема атаки з використанням нових тактик, технік і процедур, вимагають від засобів кіберзахисту здатності до виявлення неочевидних аномалій, аналізу взаємозв'язків між подіями та забезпечення глибокого контексту для реагування. Традиційні інструменти, які функціонують ізольовано, зазвичай не здатні своєчасно виявляти багатокомпонентні атаки, особливо ті, що здійснюються у кілька етапів із тривалим перебуванням у системі. У відповідь на це виникла потреба в рішеннях, які забезпечують єдину платформу для кореляції даних з різних джерел і автоматизації процесів виявлення та реагування.

Концепція XDR надає змогу інтегрувати дані з кінцевих точок, мереж, хмарних сервісів і систем безпеки, забезпечуючи наскрізну аналітику загроз. Вона дозволяє фахівцям з безпеки своєчасно виявляти відхилення в поведінці користувачів, пристроїв і програмного забезпечення, знижуючи ймовірність пропуску атаки або помилкової інтерпретації інциденту. Одним із провідних комерційних рішень у цьому класі є Cortex XDR — платформа, яка поєднує можливості аналізу телеметрії, поведінкової аналітики, машинного навчання та автоматизованого реагування.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження підходів до виявлення складних загроз та цільових атак із застосуванням засобів класу XDR, зокрема механізмів поведінкового аналізу, кореляції подій та аналітики загроз на прикладі платформи Cortex XDR.

Об'єкт дослідження — процес виявлення складних загроз та цільових атак із застосуванням засобів XDR.

Предмет дослідження — методи та засоби виявлення складних загроз і цільових атак за допомогою XDR-рішень.

Мета роботи розробити рекомендації щодо застосування методів та засобів виявлення складних загроз і цільових атак за допомогою XDR-рішень.

Наукові завдання:

проаналізувати особливості складних загроз і цільових атак, зокрема їх ознаки, етапи та методи маскування;

дослідити принципи функціонування XDR-рішень та їх відмінності від традиційних засобів виявлення загроз;

проаналізувати функціональні можливості платформи Cortex XDR у контексті виявлення складних загроз;

оцінити ефективність методів поведінкової аналітики, використання IOC/BIOC, XQL-запитів та механізмів кореляції подій;

сформувати практичні рекомендації щодо виявлення складних загроз і цільових атак із використанням засобів XDR.

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

Практичне значення одержаних результатів полягає у розробленні узагальнених рекомендацій для фахівців з кібербезпеки щодо застосування методів і засобів виявлення складних загроз на базі XDR. Отримані результати можуть бути використані при проєктуванні та вдосконаленні систем захисту організацій, а також у навчальному процесі підготовки спеціалістів з інформаційної безпеки.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науково-практичній конференції «Цифрова трансформація кібербезпеки», яка відбулася 24 квітня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ВИЯВЛЕННЯ СКЛАДНИХ ЗАГРОЗ ТА ЦІЛЬОВИХ АТАК

1.1. Аналіз проблеми виявлення складних загроз та цільових атак

Цільові атаки, які в академічній і технічній літературі зазвичай визначаються як передові стійкі загрози (Advanced Persistent Threats), являють собою спеціально спроєктовані операції, спрямовані на конкретні організації, галузі або осіб. Їх відмінною рисою є індивідуальний характер і висока адаптивність, що вирізняє їх серед масових чи випадкових атак. Основною метою таких кампаній виступає не лише отримання конфіденційної інформації або компрометація IT-інфраструктури, а й досягнення довгострокових стратегічних цілей, включаючи вплив на прийняття рішень, порушення бізнес-процесів або шпигунство в інтересах зовнішніх суб'єктів. Реалізація таких атак вимагає залучення висококваліфікованих фахівців, які нерідко мають підтримку державних структур або діють від імені організованих злочинних угруповань [1].

APT-кампанії характеризуються цілеспрямованістю, наявністю чітко визначеної місії та здатністю підтримувати стійку присутність у мережі жертви протягом тривалого часу. Зловмисники можуть залишатися непоміченими в інформаційній інфраструктурі організації протягом місяців або навіть років, поступово збираючи розвіддані, підвищуючи привілеї доступу, розширюючи зону компрометації та забезпечуючи механізми повторного входу. Подібна поведінка вимагає від захисних систем здатності до тривалої аналітики, кореляції подій та реагування на поведінкові аномалії.

Останні роки засвідчують суттєве ускладнення тактик, технік і процедур (TTPs), що використовуються APT-групами. Підходи, які раніше були характерними лише для кібервійськових підрозділів держав, активно застосовуються комерційно мотивованими злочинцями. Це вказує на зміну вектору загроз від інструменталізованих, масових атак до точкових, технічно складних та

багаторівневих операцій. Зловмисники дедалі частіше вдаються до довгострокових, економічно вигідних схем, що значно ускладнює їх виявлення, ідентифікацію джерела загрози та ефективне реагування [2].

Серед характерних технічних рис APT-операцій варто виокремити кілька ключових механізмів. Частим є використання цільових фішингових повідомлень (spear phishing), які ретельно маскуються під легітимну комунікацію й орієнтовані на конкретних осіб, що володіють доступом до критичних ресурсів. Широко застосовуються уразливості нульового дня, що надає атакуючим значну перевагу в умовах відсутності оновлень або механізмів протидії. У рамках кампаній також фіксується активне використання прихованого шкідливого програмного забезпечення — зокрема, безфайлових компонентів, складних троянів або програм-вимагачів, які, окрім завдання шкоди, можуть слугувати відволікаючим елементом або інструментом фінансування подальших дій.

Особливу складність для систем безпеки становить імітація інфраструктури та поведінкових шаблонів відомих APT-груп, що дозволяє зловмисникам ухилятися від детектування на основі сигнатур. При цьому активно використовуються сервери управління, зашифрований командно-контрольний трафік та антифорензичні техніки, включаючи стирання слідів, зміни атрибутів файлів, впровадження в легітимні процеси тощо. Прикладами таких загроз є шкідливі кампанії з використанням Ryuk Ransomware або DarkTequila Banking Trojan, які демонструють високу технічну складність реалізації та стійкість до виявлення. APT-групи, як-от APT41, широко застосовують складні механізми завантаження шкідливих компонентів, зокрема DLL sideloading, DLL hollowing та маніпуляції зі стеком викликів. Інші, зокрема Lazarus Group, орієнтовані на фінансові злочини, включаючи злам банківських систем, криптовалютних платформ і запуск програм-вимагачів із великою сумою викупу.

Структурна модель типового APT-нападу включає кілька етапів, що логічно і технічно взаємопов’язані. На етапі розвідки атакуючі здійснюють збір інформації щодо мережевої архітектури цілі, посадових обов’язків співробітників, відкритих сервісів та наявних механізмів захисту, що дозволяє обрати вектор проникнення.

Далі відбувається первинна компрометація, яка часто реалізується за допомогою фішингових листів або експлуатації вразливостей у зовнішніх компонентах. Після первинного проникнення розгортається латеральний рух, у межах якого атакуючі пересуваються мережею, здобуваючи контроль над новими системами, підвищуючи рівень доступу та закріплюючи присутність у середовищі. Завершальним етапом є ексфільтрація даних — їх приховане виведення за межі організації, що може супроводжуватись відволікаючими діями, такими як атаки типу DDoS або запуск шкідливого ПЗ з гучним ефектом.

Ураховуючи багаторівневий характер APT-операцій, ефективне виявлення потребує не лише фіксації окремих подій, а й побудови повної картини атаки шляхом кореляції сигналів із різних джерел. Це вимагає від засобів кіберзахисту високого рівня аналітичної здатності, контекстної обізнаності та гнучких механізмів реагування на кожному етапі атаки. Створення таких умов можливе лише за наявності інтегрованих платформ класу XDR, що поєднують телеметрію з багатьох джерел, поведінковий аналіз та автоматизацію процесів реагування [3].

1.2. Методи та підходи до виявлення складних загроз у корпоративному середовищі

Незважаючи на зростання обізнаності про передові стійкі загрози та постійне вдосконалення захисних механізмів, традиційні засоби кібербезпеки демонструють істотні обмеження у виявленні таких складних атак. Їх архітектура базується переважно на сигнатурному аналізі, що ґрунтується на виявленні відомих шаблонів шкідливого програмного забезпечення. Цей підхід виявляється малоефективним у випадках з експлуатацією вразливостей нульового дня, застосуванням безфайлових шкідливих програм або використанням адаптивного зловмисного коду, який змінюється з кожною ітерацією. Системи, що покладаються на сигнатури, не здатні виявляти нові, раніше невідомі загрози, а підтримання актуальності бази сигнатур потребує значних обчислювальних ресурсів та постійного людського втручання.

Додаткову складність становлять обфускація коду та поліморфізм, які дозволяють шкідливому програмному забезпеченню залишатися поза межами виявлення.

Альтернативою є евристичний підхід, який аналізує поведінку об'єктів у системі з метою виявлення відхилень. Проте, попри свою проактивність, такий аналіз також має низку обмежень, серед яких висока частота хибнопозитивних спрацювань, що можуть порушити стабільність IT-інфраструктури. Динамічне тестування у пісочницях, як одна зі складових евристичного аналізу, вимагає значних ресурсів і часто не спрацьовує проти складного зловмисного ПЗ, яке здатне ідентифікувати середовище виконання та уникати активації до потрапляння в реальну систему. Застарілі мережеві засоби, включаючи фаєрволи, що працюють на рівні транспортного протоколу, забезпечують лише базову фільтрацію трафіку, не аналізуючи його зміст. Це уможливлює проходження атак на рівні прикладного програмного забезпечення, зокрема SQL-ін’єкцій чи XSS, непоміченими.

Такі обмеження створюють сліпі зони у захисті, дозволяючи зловмисникам зберігати присутність у мережах протягом тривалого часу. Це особливо актуально для APT-кампаній, які характеризуються багатоступеневістю, стійкістю та тривалим перебуванням у середовищі жертви. Нездатність традиційних засобів виявити загрози, що не мають відповідної сигнатури, зумовлює необхідність переходу до інтелектуальних систем, здатних аналізувати поведінкові патерни та виявляти складні, приховані атаки.

Окремої уваги потребують загрози, пов’язані з безфайловими атаками, атаками на ланцюги постачання та хмарною інфраструктурою. Безфайлові атаки здійснюються з використанням легітимних системних інструментів, таких як PowerShell або WMI, та працюють винятково у пам’яті, що робить їх невидимими для сканерів, орієнтованих на файли. Атаки на ланцюги постачання дозволяють компрометувати організації через довірені сторонні продукти або сервіси, обходячи традиційні периметрові засоби захисту. У свою чергу, хмарно-орієнтовані загрози спрямовані на інфраструктуру, що функціонує поза межами локального середовища, й потребують нових методів моніторингу, адаптованих до динамічних гібридних архітектур. Усі ці категорії атак ускладнюються

використанням зловмисниками інструментів штучного інтелекту та машинного навчання, що підвищує рівень автоматизації, адаптивності та ускладнює виявлення.

Зміна структури корпоративного середовища лише посилює ці виклики. Зі збільшенням розподіленості систем, інтеграції хмарних сервісів та взаємодії з численними підрядниками, концепція периметра безпеки втрачає актуальність. Умовний "периметр" більше не обмежується фізичною чи логічною межею, а розмивається у складному поєднанні кінцевих точок, внутрішніх мереж, хмарних ресурсів та ідентичностей користувачів. Це вимагає від засобів захисту не лише здатності аналізувати трафік, а й враховувати контекст, поведінкові аномалії та взаємозв’язки між компонентами у різних доменах.

У межах такої трансформації традиційні системи виявлення вторгнень також демонструють обмеження. Вони мають знижену ефективність щодо зашифрованого трафіку, створюючи додаткові сліпі зони у безпеці. Схильність до хибнопозитивних спрацювань, навантаження на IT-фахівців, ресурсоємність та зниження загальної продуктивності мережі — всі ці аспекти обмежують ефективність IDS у виявленні складних загроз. У результаті зростає потреба у переході до масштабованих, гнучких, інтелектуально керованих систем виявлення та реагування, які здатні протистояти новому поколінню атак, адаптованих до складного й швидко змінного технологічного середовища.

Для ефективного виявлення складних загроз у корпоративному середовищі сучасні підходи до кібербезпеки активно інтегрують передові технології. Центральну роль у цьому процесі відіграють машинне навчання (ML) і штучний інтелект (AI), які забезпечують здатність обробляти великі обсяги даних у реальному часі, виявляти аномалії та адаптуватися до нових сценаріїв атак. Ці технології дозволяють системам безпеки переходити від традиційного сигнатурного підходу до проактивного аналізу поведінки [4].

ML-алгоритми забезпечують автоматичне оновлення сигнатур загроз без втручання людини. Поведінковий аналіз, натомість, фокусується не на визначених шаблонах атак, а на виявленні відхилень від нормальної діяльності. Це дає змогу

виявляти zero-day-атаки, внутрішні загрози та складні APT, які зазвичай маскуються під звичайну активність.

User and Entity Behavior Analytics

Аналітика поведінки користувачів і сутностей є важливим інструментом для виявлення потенційних загроз. Вона поєднує алгоритми ML та AI для аналізу журналів входу, шаблонів доступу, геолокації, а також логів з мережевих пристроїв, серверів, кінцевих точок та додатків. На основі цих даних система формує профілі поведінки для кожного користувача або об’єкта.

UEBA дозволяє виявляти відхилення від норми — наприклад, аномально великі передачі даних або нетипову активність під обліковим записом. Такий підхід забезпечує раннє виявлення внутрішніх загроз, скомпрометованих облікових записів, DDoS-атак та інших потенційних інцидентів безпеки.

Threat Intelligence

Інструменти розвідки загроз надають організаціям можливість ідентифікувати вразливості до того, як вони будуть використані зловмисниками. Завдяки цим рішенням забезпечується:

- аналіз тактик і технік атак;
- кореляція індикаторів компрометації (IoC);
- створення контекстних сповіщень про активність APT;
- навчання та підвищення обізнаності команд безпеки.

Розвідка загроз є невіддільною частиною проактивного захисту: вона не тільки дозволяє реагувати на інциденти, а й передбачати атаки, що формує базу для превентивних заходів. Важливим елементом цього підходу є обмін інформацією між організаціями та постачальниками засобів захисту.

Еволюція інструментів: EDR, NDR, SIEM, SOAR, XDR

Для комплексного виявлення загроз у корпоративному середовищі застосовується ціла низка рішень, які пройшли значну еволюцію — від ізольованих модулів до інтегрованих платформ.

- EDR — орієнтований на захист кінцевих точок (ПК, серверів, мобільних пристроїв). Забезпечує виявлення шкідливого ПЗ, ізоляцію заражених пристроїв, полювання на загрози, розслідування інцидентів та криміналістику.
- NDR — аналізує мережевий трафік для виявлення латерального руху, ексфільтрації даних та іншої підозрілої активності в мережі. Забезпечує глибоку видимість міжсистемних взаємодій.
- SIEM — агрегує журнали подій з усієї мережі, проводить аналіз на основі правил і поведінкових моделей. Забезпечує відповідність стандартам, виявлення IoC, але потребує налаштування та генерує велику кількість сповіщень, часто вимагаючи ручного втручання.
- SOAR — автоматизує обробку інцидентів, об'єднуючи різні джерела даних і виконуючи попередньо налаштовані сценарії (плейбуки). Орієнтований на зрілі SOC-команди; фокусується на швидкому реагуванні.
- XDR — є логічним продовженням EDR. Поєднує дані з кінцевих точок, мереж, хмарних середовищ, SIEM та інших систем, надаючи уніфіковану картину безпеки. Завдяки централізованому збору, кореляції та аналізу інцидентів XDR забезпечує швидше виявлення, пріоритизацію та усунення загроз [5].

XDR є кульмінацією еволюції засобів виявлення загроз, що долає проблему фрагментованості між окремими рішеннями. Порівняльний аналіз чітко демонструє, що такі інструменти, як EDR, NDR, SIEM і SOAR, хоча й ефективні у своїх нішах, зазвичай працюють як ізольовані системи, кожна з власними обмеженнями. Натомість XDR позиціонується як наступний етап розвитку — "еволюція EDR", яка не просто додає нові функціональні можливості, а змінює саму парадигму: від точкових рішень до інтегрованої платформи.

XDR об'єднує дані з кінцевих точок, мережевої інфраструктури, хмарних сервісів, SIEM і SOAR-систем у єдине аналітичне середовище. Така централізація дозволяє досягти цілісного огляду подій безпеки та ефективно виявляти складні, багатовекторні атаки, що перетинають кілька шарів захисту — ситуації, які залишалися б поза увагою у випадку розрізнених інструментів.

Крім того, XDR суттєво знижує навантаження на аналітиків безпеки, мінімізуючи «втому від сповіщень» завдяки автоматичній кореляції та пріоритизації інцидентів. Це значно скорочує ключові показники реагування: середній час виявлення, розслідування та реагування, що є критично важливим для оперативного нейтралізування загроз типу APT [6].

1.3. Аналіз існуючих рішень для виявлення складних загроз та цільових атак

Багато організацій стикаються з проблемою фрагментарного розуміння питань кібербезпеки. Рішення класу XDR забезпечують ширший функціонал порівняно з традиційними EDR-системами, виходячи за межі захисту лише робочих станцій і серверів, охоплюючи інші мережеві компоненти. Хоча EDR орієнтований на кінцеві точки, XDR забезпечує розширене охоплення завдяки обробці телеметрії з таких джерел, як Active Directory, NGFW, системи автентифікації, поштові шлюзи, мережеві сенсори та інші. У процесі роботи з XDR аналітики, фахівці з розслідування інцидентів та інші експерти мають змогу поєднувати внутрішні дані з додатковими джерелами для підвищення ефективності реагування на інциденти.

Сучасні EDR-рішення дедалі частіше інтегруються у екосистеми XDR-постачальників і надаються за окремими ліцензійними моделями. У випадках, коли в організації відсутні інші засоби безпеки або власний експертний персонал, доцільним є впровадження XDR як комплексної послуги, яка виходить за межі традиційного захисту кінцевих точок. Таким чином, постачальники XDR поєднують функції EDR і MDR із додатковими можливостями аналізу, кореляції, реагування та розслідування інцидентів.

XDR-постачальники надають спеціалізовані рішення для захисту інфраструктури підприємств — від кінцевих точок до ідентифікаційних систем. Вони інтегрують дані з різних джерел телеметрії, здійснюють аналітику, формують контекст подій і забезпечують кореляцію сповіщень. Такі рішення можуть бути

реалізовані як у хмарі, так і локально, що робить їх привабливими для організацій із обмеженими ресурсами.

Функціональність XDR включає реагування на інциденти, захист мережі, електронної пошти та хмарних середовищ. Основна мета полягає в протидії складним загрозам, таким як програмне забезпечення-вимагач, фішинг, шкідливе ПЗ і цілеспрямовані атаки.

XDR-рішення можуть бути реалізовані як повністю керовані служби або як платформи, якими керує самостійно організація. Такі сервіси дозволяють створити цілісну систему кіберзахисту шляхом консолідації інформації з різних джерел та підвищення ефективності процесів виявлення і реагування на загрози.

Необхідність застосування XDR зумовлена потребою в централізованому підході до виявлення загроз, який дозволяє проводити глибокий аналіз подій без обмеження на окремі сегменти, як-от мережі або кінцеві точки. Завдяки об'єднанню даних з електронної пошти, хмар, додатків, мереж і пристроїв у єдину панель моніторингу, XDR забезпечує повну видимість подій у IT-інфраструктурі.

Додатковою перевагою є здатність XDR виявляти складні та приховані загрози, що залишаються поза межами уваги ізольованих інструментів. Системи XDR дозволяють оперативно блокувати шкідливу активність, ізолювати скомпрометовані вузли та автоматизувати реакцію, що суттєво скорочує час реагування.

Автоматизація обробки інцидентів та аналітики сприяє підвищенню ефективності роботи команд безпеки. XDR-рішення також дозволяють адаптуватися до нових загроз завдяки постійному оновленню моделей машинного навчання та баз знань про загрози.

На ринку 2025 року представлено низку провідних XDR-рішень:

SentinelOne Singularity™ XDR

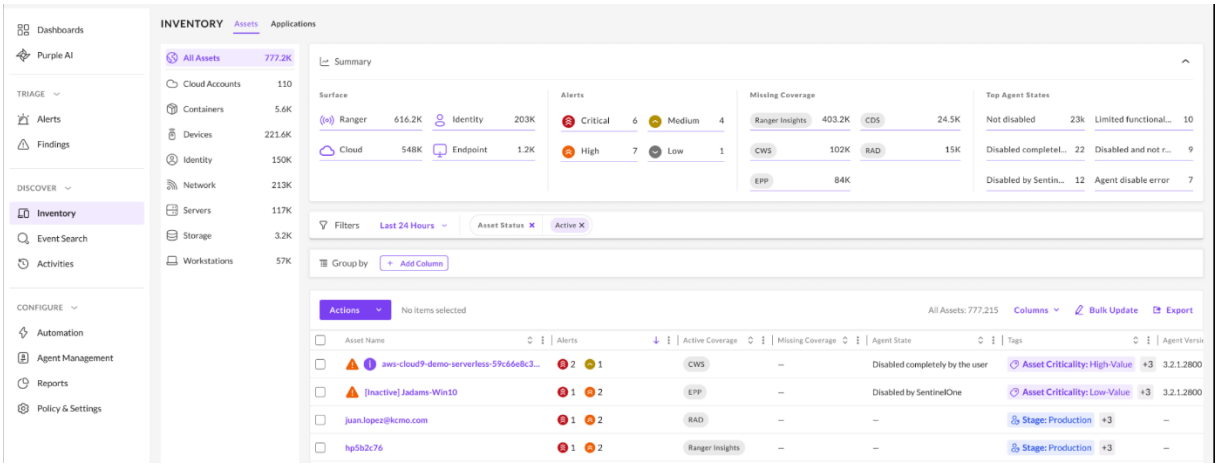

Рис.1.1. Інтерфейс SentinelOne Singularity™ XDR

Ця платформа поєднує поведінкову аналітику, машинне навчання та автономні агенти, які діють безперервно навіть у режимі офлайн. Рішення здатне агрегувати телеметрію з кінцевих точок, хмарних ресурсів, мережевих джерел і сторонніх SIEM/SOAR-систем. Система автоматизує виявлення, обмеження, ліквідацію та відновлення після інцидентів, пропонуючи візуалізацію векторів атак за MITRE ATT&CK. Модуль ActiveEDR дозволяє аналітикам швидко аналізувати причинно-наслідкові зв’язки, а функція Storyline зберігає повну хронологію подій. Інтеграція з WatchTower Services забезпечує доступ до розвідданих про загрози та професійного супроводу розслідувань.

Cortex XDR від Palo Alto Networks

Одна з найбільш технологічно розвинених XDR-платформ, яка забезпечує інтеграцію з брандмауерами, проксі, хмарними службами, поштовими шлюзами та сторонніми EDR. Cortex XDR використовує аналітику поведінки користувачів і пристроїв (UEBA), автоматизоване виявлення та реагування, а також XQL Search — мову запитів для ручного аналізу. Платформа тісно інтегрована з Cortex Data Lake, що дозволяє швидко масштабуватися і забезпечує високу швидкість обробки подій. Автоматизація Playbooks у поєднанні з SOAR-платформою дозволяє здійснювати реакцію без втручання людини.

Trend Micro Vision One

Рис.1.2. Архітектура Trend Micro Vision One

Мультивекторна XDR-платформа, яка охоплює захист електронної пошти, хмарних обчислень (AWS, Azure, GCP), IoT/OT-середовищ, мереж і кінцевих точок. Платформа використовує AI-движки для аналізу телеметрії, має єдину консоль керування, інтеграцію з Zero Trust Framework і підтримує виявлення lateral movement. Trend Micro Vision One дозволяє автоматизувати блокування на основі корельованих сповіщень, проводити глибоку форензику та використовує патерни загроз, отримані з Trend Micro Smart Protection Network.

CrowdStrike Falcon XDR

Платформа відзначається високою швидкістю розгортання та низьким споживанням ресурсів. Заснована на cloud-native архітектурі, вона поєднує поведінкову аналітику, загрозову розвідку (Threat Graph) і API-інтеграції з іншими продуктами. Falcon XDR забезпечує видимість не тільки кінцевих точок, а й поштових сервісів, мереж, ідентифікаційних систем та інфраструктурних служб. Рішення також підтримує Threat Hunting і керовані сервіси Falcon Complete.

Symantec XDR (Broadcom)

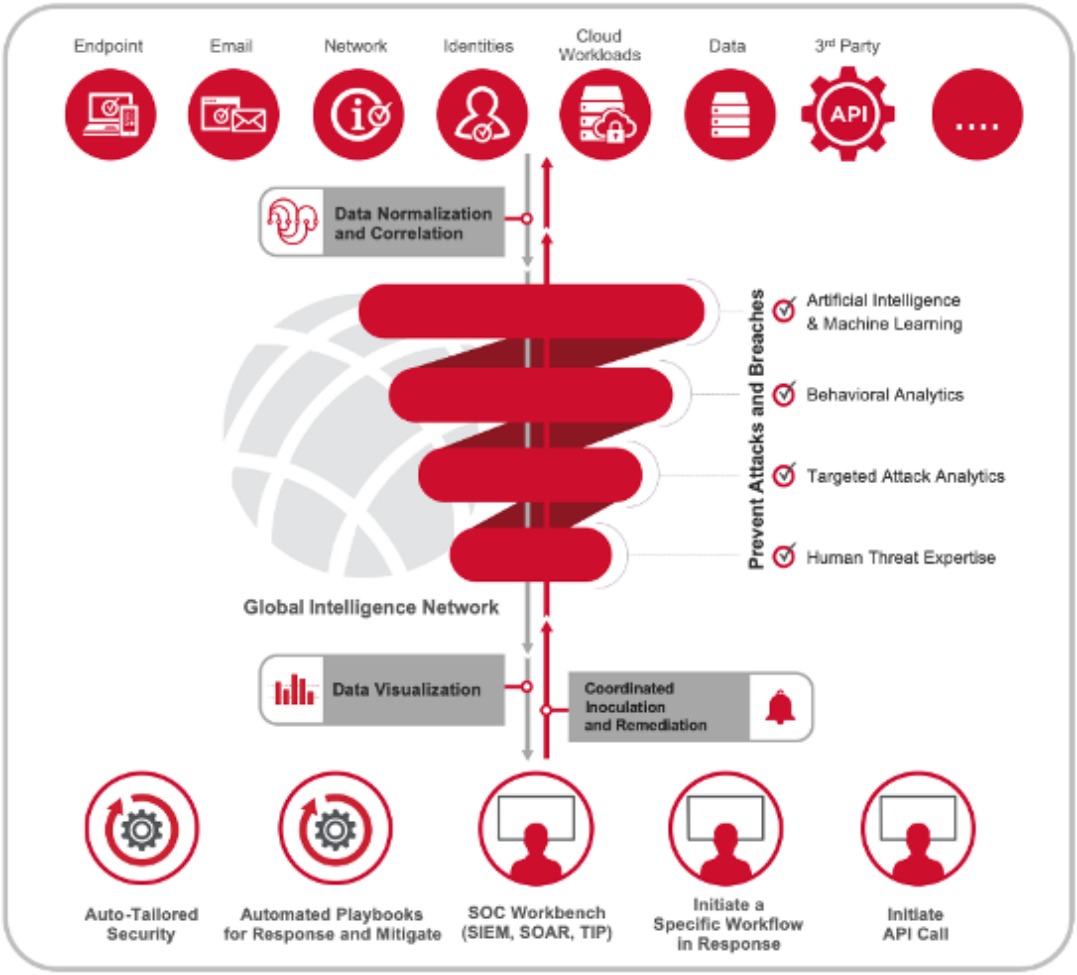

Рис.1.3. Переваги Symantec XDR (Broadcom)

Це платформа з розвиненими функціями Data Loss Prevention (DLP), виявлення загроз на основі машинного навчання, аналітики поведінки (UEBA) та контролю доступу. Symantec інтегрує телеметрію з мережевих пристроїв, хмарних ресурсів і мобільних систем, забезпечуючи єдину зведену панель для SOC-аналітиків. Особливістю є гнучке моделювання політик безпеки з урахуванням контексту (risk-based policies) і можливість розгортання як локально, так і в хмарі.

McAfee MVISION XDR

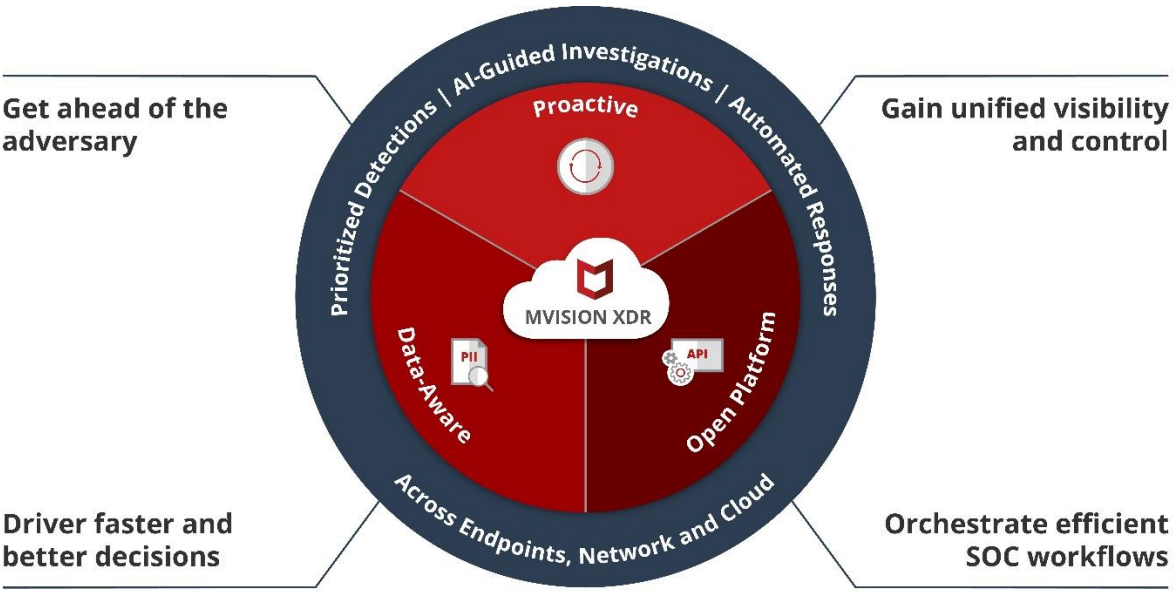

Рис.1.4. Переваги платформи McAfee MVISION XDR

Фокус платформи — на забезпеченні безперервного моніторингу та виявленні аномалій у багатохмарних і гібридних середовищах. Рішення поєднує аналіз поведінки, загрозову розвідку, а також автоматизоване реагування на основі передналаштованих сценаріїв. McAfee MVISION забезпечує інтеграцію з CASB, SIEM, DLP та керуванням ідентичностями, а також підтримує модульну архітектуру розширення функціоналу за потреби.

Під час вибору відповідного XDR-постачальника слід проаналізувати прогалини в захисті та ідентифікувати ключові потреби організації — чи йдеться про кінцеві точки, хмарні середовища чи розподілені мережі. Важливо оцінити здатність платформи до масштабування, глибину аналітики, рівень автоматизації, відповідність нормативним вимогам і загальну вартість володіння, включаючи ліцензування, підтримку та інтеграцію. Інтуїтивні інтерфейси, відкриті API й адаптивні алгоритми — важливі критерії ефективної інтеграції у діючу інфраструктуру.

Таким чином, обґрунтований вибір XDR-рішення має ґрунтуватися на поєднанні функціональних характеристик, потреб організації та стратегічних цілей у сфері безпеки.

Аналіз різних рішень свідчить про те, що Cortex XDR від Palo Alto Networks є доцільним вибором для глибокого дослідження у сфері виявлення складних загроз і цільових атак. Архітектура платформи, побудована на основі Cortex Data Lake, дозволяє ефективно агрегувати та нормалізувати дані з різних джерел, що критично важливо для виявлення багатовекторних атак. Аналітичний механізм, поведінкова аналітика й алгоритми ML забезпечують виявлення як відомих, так і раніше невідомих загроз. Крім того, можливості XQL Search та автоматизації реагування підвищують швидкість аналізу інцидентів і зменшують їхній вплив. Завдяки комплексному підходу Cortex XDR є яскравим прикладом ефективності інтегрованих XDR-рішень [7].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ СКЛАДНИХ ЗАГРОЗ ТА ЦІЛЬОВИХ АТАК ЗАСОБАМИ XDR

2.1. Архітектура та компоненти рішення Cortex XDR

Концепція Extended Detection and Response спрямована на подолання обмежень традиційних інструментів кіберзахисту, які функціонують ізольовано та не забезпечують узгодженої картини загроз у межах інформаційної інфраструктури. Платформа XDR забезпечує централізовану агрегацію та обробку телеметрії з різних джерел, зокрема кінцевих точок, хмарних робочих навантажень, мережі, електронної пошти, ідентифікаційних систем і контейнеризованих середовищ. Об'єднання таких даних у межах єдиної системи дозволяє забезпечити цілісне уявлення про інциденти безпеки, підвищити точність виявлення загроз та скоротити час на розслідування.

Ключовим принципом побудови XDR-рішень є нормалізація та уніфікація зібраної інформації. Обробка великомасштабних обсягів подій із різнорідних джерел відбувається за допомогою спеціалізованих конвеєрів, які перетворюють сировинну телеметрію у стандартизовані записи. Це уможливлює застосування уніфікованих запитів, алгоритмів виявлення та засобів кореляції по всьому спектру джерел. Відсутність нормалізації унеможливлювала б ефективне виявлення складних багатовекторних атак через фрагментацію контексту і зростання кількості хибнопозитивних спрацювань [8].

Однією з основних переваг XDR є створення єдиного контексту безпеки. Завдяки глибокій інтеграції на всіх рівнях інфраструктури, XDR забезпечує повний огляд подій безпеки, дозволяючи оперативно ідентифікувати складні атаки з використанням міжсередовищевої кореляції. Платформа трансформує розрізнені сигнали в пріоритезовані інциденти з насиченим контекстом, що дає змогу аналітикам зосереджувати увагу на найбільш критичних загрозах. Такий підхід істотно знижує навантаження на персонал центрів операцій безпеки (SOC),

мінімізуючи вплив явища «втоми від сповіщень» і знижуючи ризик вигорання. Автоматизація сортування подій, їх фільтрація та контекстуалізація сприяють підвищенню ефективності реагування на загрози.

Прикладом практичної реалізації концепції XDR є платформа Cortex XDR від Palo Alto Networks. Архітектура цього рішення базується на використанні масштабованого хмарного сховища Cortex Data Lake, яке виконує функції централізованої платформи зберігання, обробки та нормалізації структурованих і неструктурованих даних. Cortex Data Lake забезпечує горизонтальну масштабованість, допускає гнучке розширення обсягів у залежності від потреб організації та підтримує низку сценаріїв використання, включно з машинним навчанням, кореляцією подій, виявленням аномалій і спеціалізованими дослідженнями. Завдяки високій щільності телеметричних даних з різноманітних джерел створюється насичений контекст, що підвищує точність алгоритмів виявлення на основі AI/ML і забезпечує стійкість до складних атак.

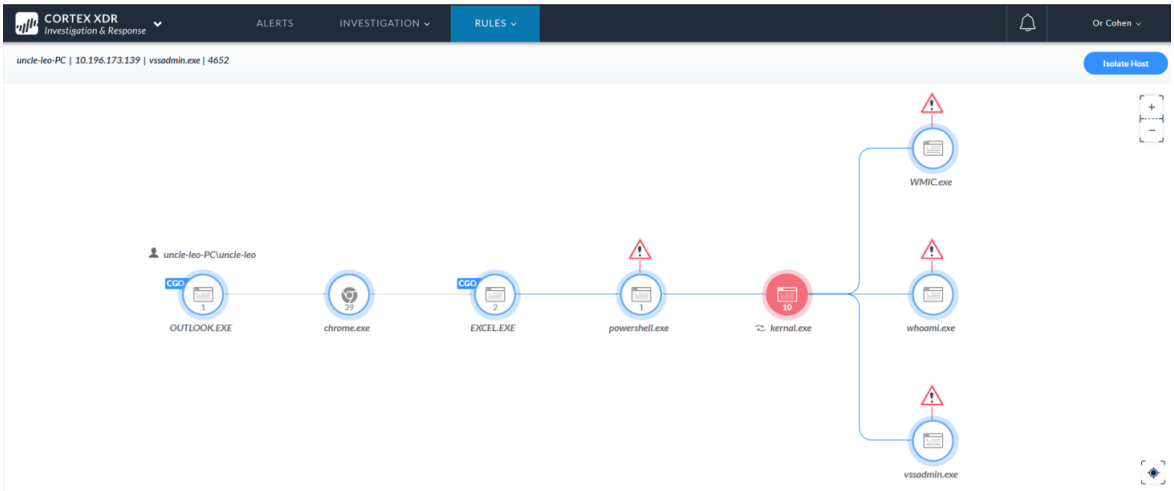

Рис.2.1. Дослідження Cortex XDR

Компоненти Cortex XDR функціонують у тісній взаємодії для забезпечення цілісного захисного контуру. Агенти, які розгортаються на кінцевих точках під управлінням Windows, macOS і Linux, забезпечують як захист у реальному часі, так і збір даних для подальшого аналізу. Телеметрія надходить як від нативних продуктів Palo Alto Networks, включно з міжмережевими екранами нового

покоління та рішенням Traps, так і від сторонніх систем, що генерують журнали та сповіщення. Такий підхід дозволяє знизити вартість впровадження для поточних користувачів екосистеми Palo Alto Networks, тоді як для нових клієнтів достатньо розгорнути мінімальний набір сенсорів для отримання повноцінного функціоналу.

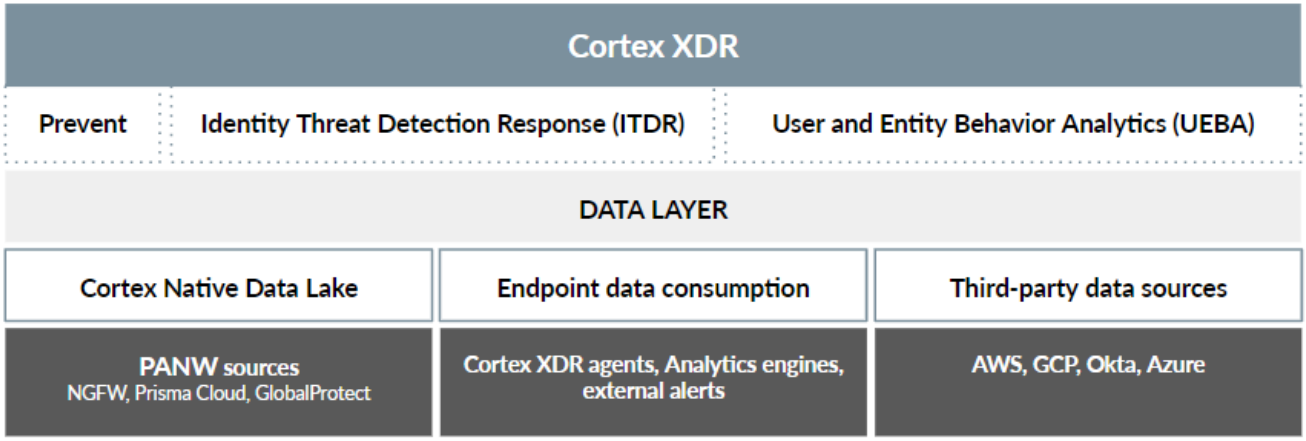

Рис. 2.2. Архітектура ключових компонентів Cortex XDR

Аналітичний модуль Cortex XDR застосовує поведінкові моделі, алгоритми машинного навчання та методи штучного інтелекту для виявлення аномальної та прихованої активності. Однією з ключових функцій є реалізація механізмів аналітики поведінки користувачів, які дозволяють будувати багатовимірні профілі активності, включно з розрахунком ризик-оцінок. Модуль кореляції здійснює автоматичне поєднання подій з різних джерел — мережевих сегментів, кінцевих точок і хмарної інфраструктури — в єдині інциденти, що суттєво підвищує точність виявлення атак і скорочує загальну кількість сповіщень. За даними виробника, це дозволяє зменшити обсяг сигналів, що потребують перевірки, до 98%.

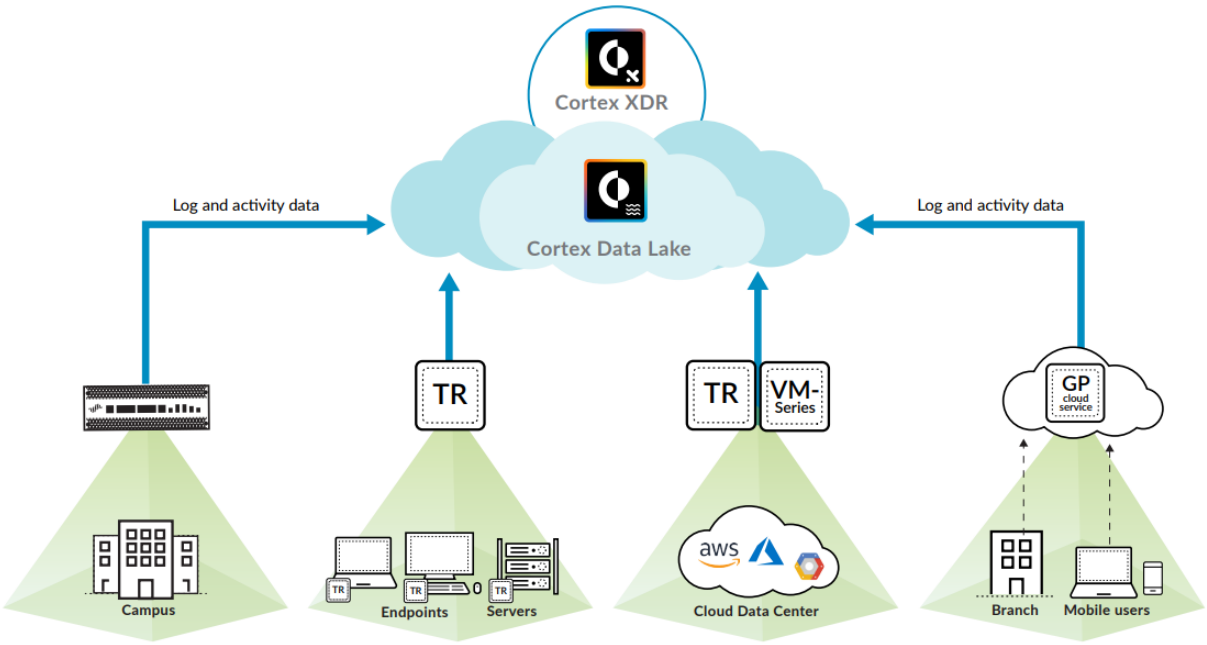

Рис. 2.3. Аналіз даних з будь-якого джерела для виявлення та реагування

Управління всіма функціями платформи здійснюється з централізованої консолі, яка забезпечує доступ до конфігурування політик захисту, моніторингу подій, засобів розслідування та реагування. Інтерфейс консолі оптимізовано для спрощення навігації й ефективної роботи аналітиків, що сприяє скороченню часу на обробку інцидентів та підвищує загальну продуктивність операцій з кіберзахисту [9].

2.2. Призначення та основні функції компонентів Cortex XDR

Рішення Cortex XDR реалізує багаторівневу архітектуру, кожен компонент якої виконує чітко визначені функції у межах єдиної системи виявлення, попередження, розслідування та реагування на загрози. Центральним елементом виступає агент Cortex XDR, розгорнутий на кінцевих точках. Його основною функцією є запобігання загрозам та збір телеметрії. Агент забезпечує захист від широкого спектра атак, зокрема експлойтів, шкідливих програм, програм-вимагачів, а також безфайлових атак, використовуючи механізми штучного інтелекту для аналізу файлів. Він також реалізує поведінковий захист, що дозволяє

виявляти аномальні взаємодії процесів, і включає додаткові засоби контролю: хостовий фаєрвол, шифрування диска та моніторинг USB-пристроїв, що істотно знижує ризики несанкціонованого втручання або витоку даних [10].

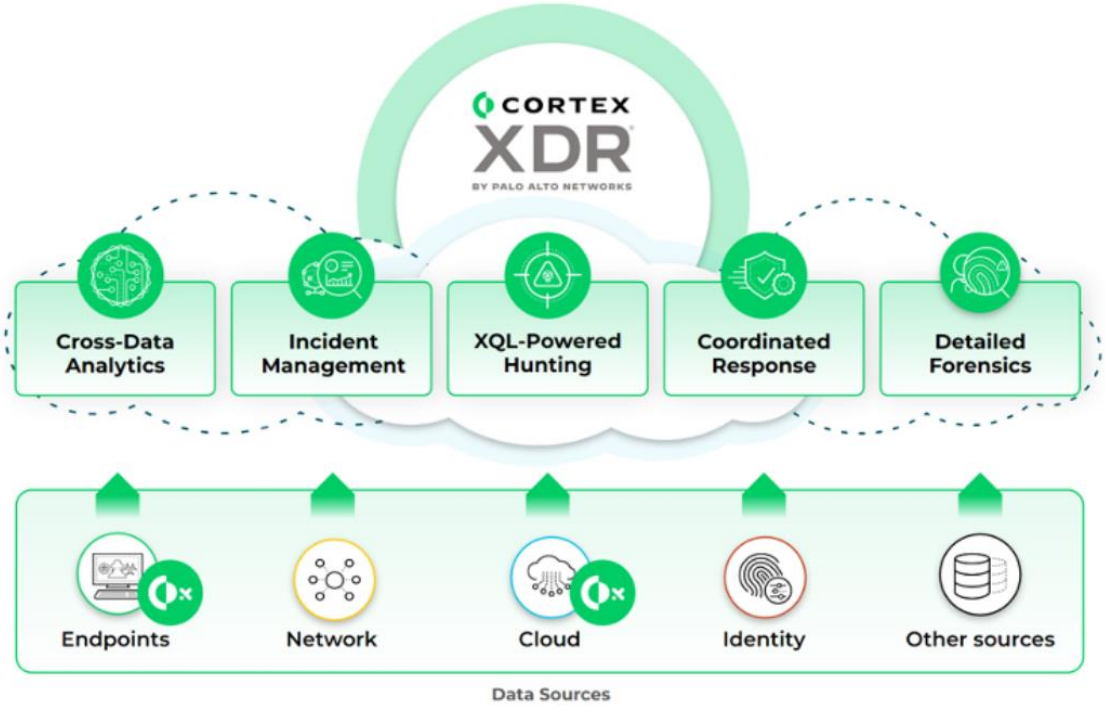

Рис. 2.4. Cortex XDR виконує аналіз даних з будь-якого джерела для виявлення та реагування

Усі дані, зібрані агентами, передаються до централізованого сховища Cortex Data Lake, що виконує функцію агрегації та нормалізації інформації з усіх джерел. Цей компонент підтримує обробку як структурованих, так і неструктурованих даних, забезпечуючи гнучкість у роботі з великими обсягами телеметрії. Cortex Data Lake масштабований до рівня петабайтів інформації, що робить його придатним для обробки даних корпоративного рівня. Окрім того, сховище інтегрується з аналітичними механізмами штучного інтелекту й машинного навчання, забезпечуючи уніфікований контекст для подальшого аналізу.

Ключовим аналітичним інструментом платформи є аналітичний двигун на основі AI/ML, призначений для виявлення аномалій та прихованих загроз шляхом аналізу поведінки користувачів і систем. Його робота базується на безперервному

профілюванні активності як користувачів, так і мережевих об'єктів. Реалізовано підтримку аналітики поведінки користувачів, що дає змогу оцінювати ризики на основі поведінкових шаблонів. Крім того, використовується глобальна міжклієнтська аналітика для виявлення атак нульового дня та загроз, що виникають у ланцюгах постачання. Завдяки побудові причинно-наслідкових зв’язків система автоматично встановлює джерело загрози, оцінює репутацію залучених об’єктів і формує хронологічну послідовність подій.

Наступним важливим елементом є модуль кореляції інцидентів, що дозволяє об’єднувати розрізнені сигнали безпеки в єдині логічно пов’язані інциденти. Це значно спрощує процес розслідування й знижує навантаження на аналітиків безпеки. Застосування цього модуля дозволяє зменшити кількість сповіщень на понад 98%, усуваючи зайві або повторювані сигнали. Також реалізовано автоматичне виявлення першопричини інциденту, оцінку репутації пов’язаних об’єктів і відтворення повної картини подій.

Для забезпечення проактивного захисту у платформі передбачено компонент XQL Search, що дозволяє здійснювати розширене "полювання" на загрози. Цей інструмент використовує власну мову запитів — XQL (XDR Query Language), спеціально розроблену для ефективного аналізу великих обсягів подій з кінцевих точок, хмарних середовищ і мережевої інфраструктури. Завдяки високій виразності мови користувачі можуть створювати складні запити, проводити глибоку кореляцію даних і візуалізувати результати, що підвищує точність і швидкість розслідування інцидентів.

Усі функціональні можливості платформи доступні через централізовану консоль управління Cortex XDR, яка об’єднує налаштування політик, управління активами, моніторинг сповіщень, керування правилами виявлення (IOC, BIOC, правила кореляції), аналітичні панелі та інструменти візуалізації. Консоль також підтримує інтеграцію з зовнішніми рішеннями через API, що відкриває додаткові можливості для автоматизації процесів безпеки.

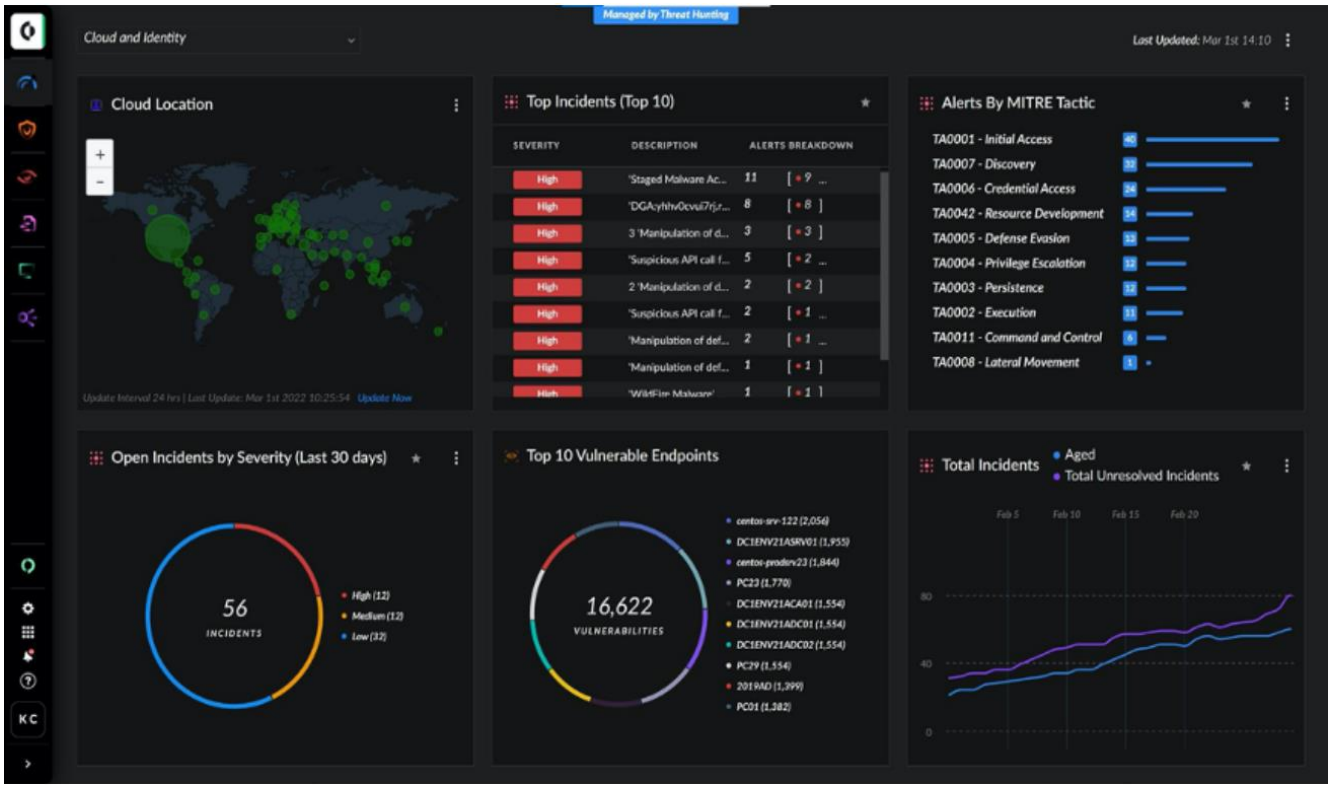

Рис. 2.5. Настроювана інформаційна панель Cortex XDR

Крім того, Cortex XDR включає інструменти автоматизації реагування, які дозволяють ізолювати кінцеві точки, зупиняти зловмисні процеси, ініціювати сканування або збирати артефакти в автоматичному або ручному режимі. Можна створювати правила, які запускають відповідні дії за заданих умов, таких як тип сповіщення, рівень ризику чи ознаки загрози. Окремо передбачено механізм Live Terminal, що забезпечує інтерактивний доступ до системи з можливістю виконання команд у середовищах CLI, PowerShell або Python, що значно розширює можливості ручного аналізу та втручання [11].

2.3. Інтеграція Cortex XDR з іншими засобами інформаційної безпеки та SIEM-системами

Ефективність платформи Cortex XDR значною мірою зумовлюється її здатністю до глибокої інтеграції з іншими засобами інформаційної безпеки, що дозволяє формувати єдину взаємопов’язану екосистему захисту в межах

корпоративної інфраструктури. Одним із ключових напрямів такої інтеграції є взаємодія з міжмережевими екранами нового покоління виробництва Palo Alto Networks. Ці пристрої виконують функції як сенсорів, так і точок примусу, забезпечуючи передачу мережевої телеметрії до Cortex Data Lake, що уможливлює негайне реагування на інциденти безпеки. Зокрема, XDR може обмежувати мережеву активність до або від кінцевих пристроїв, оперативно реалізуючи політики захисту [12].

Ще одним важливим елементом інтеграції є використання сервісу WildFire — хмарної платформи запобігання шкідливому програмному забезпеченню від Palo Alto Networks. Цей сервіс надає детальну інформацію про поведінку підозрілих об'єктів і зразків шкідливого ПЗ, виявлених у середовищі організації, що підвищує точність виявлення загроз. Таким чином, Cortex XDR отримує змогу використовувати раніше впроваджені компоненти інфраструктури як частину єдиного захисного середовища, що дозволяє ефективно переорієнтувати наявні інвестиції та зменшити складність розгортання нових рішень.

Особливе місце займає інтеграція з системами управління інформацією та подіями інформаційної безпеки (SIEM), такими як Stellar Cyber, IBM Security QRadar та іншими. На відміну від SIEM-систем, які переважно зосереджені на зборі та аналізі журналів подій, Cortex XDR охоплює ширший спектр телеметрії — від даних кінцевих точок до мережевого трафіку та хмарних сервісів. Це дозволяє системам SIEM отримувати збагачені, контекстуалізовані дані для покращеної кореляції інцидентів, що забезпечує більш точне виявлення складних і багатостадійних атак. У цьому сценарії Cortex XDR виконує функції первинного виявлення та реагування в реальному часі, тоді як SIEM-системи можуть зосередитися на завданнях довготривалого зберігання, відповідності нормативним вимогам і побудові звітності. Такий розподіл ролей дозволяє уникнути дублювання функціональності та підвищує загальну ефективність засобів інформаційної безпеки.

Рис. 2.6. Модель взаємодії компонентів Cortex Platform для розширення можливостей XDR

Розширення функціональності Cortex XDR також досягається через інтеграцію зі сторонніми інструментами безпеки поза межами екосистеми Palo Alto Networks. Платформа підтримує обробку журналів і сповіщень від рішень інших виробників, що дає змогу розширити охоплення мережі та забезпечити повноцінне виявлення загроз незалежно від джерела. Дані від сторонніх сенсорів автоматично поєднуються з телеметрією з кінцевих точок, що дозволяє значно скоротити час на встановлення першопричини інциденту й оптимізує навантаження на аналітиків.

Крім того, Cortex XDR інтегрується з платформою оркестрації, автоматизації та реагування на інциденти Cortex XSOAR. Це дозволяє здійснювати автоматизоване реагування відповідно до попередньо визначених сценаріїв, що охоплюють понад 370 сторонніх інструментів. Така взаємодія забезпечується через публічні API, які також надають стороннім програмам можливість отримувати оновлення про інциденти, запитувати додаткові дані, змінювати статус подій або змінювати їх критичність. Також реалізовано можливість інтеграції зі зовнішніми службами розвідки загроз, такими як VirusTotal, з метою перевірки окремих артефактів, виявлених у ході розслідування [13].

Завдяки широким інтеграційним можливостям, Cortex XDR не лише не витісняє вже існуючі інструменти, а навпаки — підвищує ефективність їх використання, об’єднуючи розрізнені компоненти системи безпеки в уніфіковане аналітичне середовище. У цій ролі XDR виконує функцію координуючої ланки, який забезпечує узгодженість дій усіх елементів системи кіберзахисту та сприяє досягненню вищого рівня адаптивності, автоматизації та оперативності реагування на загрози.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ СКЛАДНИХ ЗАГРОЗ ТА ЦІЛЬОВИХ АТАК ЗАСОБАМИ XDR НА ПРИКЛАДІ CORTEX

3.1. Варіант розгортання Cortex XDR в корпоративному середовищі

Розгортання Cortex XDR у корпоративному середовищі вимагає ретельного планування та виконання, оскільки платформа пропонує гнучкі моделі, що відповідають різним інфраструктурним потребам. Організації можуть обирати між локальним (on-premises), хмарним або гібридним розгортанням, що дозволяє адаптувати рішення до існуючої інфраструктури та вимог безпеки. Хоча локальне розгортання передбачає використання виділеного обладнання та його обслуговування, хмарні та гібридні варіанти забезпечують масштабованість та зменшують навантаження на внутрішні ресурси. Наприклад, ліцензія Cortex XDR Pro per GB підтримує хмарне розгортання, усуваючи потребу в локальних рішеннях для збору журналів та даних. Ця гнучкість є вирішальною для адаптації до різноманітних корпоративних середовищ та забезпечення безперервного захисту, дозволяючи організаціям обирати модель, яка найкраще відповідає їхній інфраструктурі, вимогам до безпеки та бюджетним обмеженням.

Для успішного розгортання Cortex XDR необхідно врахувати кілька ключових інфраструктурних компонентів, кожен з яких відіграє свою роль у забезпеченні всебічного захисту та збору даних. Центральним елементом системи є Агенти Cortex XDR, легке програмне забезпечення, що встановлюється на кінцевих точках, таких як пристрої під керуванням Windows, macOS, Linux та Android. Ці агенти функціонують як основні сенсори, безперервно відстежуючи активність кінцевих точок, ідентифікуючи загрози та зупиняючи шкідливу поведінку або файли. Вони збирають широкий спектр телеметрії, включаючи метадані про кінцеві точки (ідентифікатори процесів, користувачів, час створення), інформацію про завантажені DLL-файли (повний шлях, розмір, хеші, підпис), деталі процесів (PID батьківського та дочірнього процесів, аргументи командного

рядка, рівень цілісності, хеші, підпис), мережеві події (IP-адреси, порти, протоколи, статус з'єднання, DNS-запити, HTTP-з'єднання) та зміни реєстру (створення, видалення, перейменування ключів та значень). Для оптимальної продуктивності агенти вимагають двоядерного процесора (для версії 7.0 і вище), мінімум 2 ГБ оперативної пам'яті та 5 ГБ вільного місця на жорсткому диску. Важливо, щоб вони підтримували зв'язок із сервером Cortex XDR через TCP-порт 443.

Вся зібрана телеметрія та журнали централізуються в Cortex Data Lake, масштабованому хмарному сховищі. Це централізоване сховище даних є фундаментальним, оскільки воно дозволяє механізму XDR корелювати розрізнені події та генерувати високоточні сповіщення. Cortex Data Lake не лише зберігає величезні обсяги сирих даних у їхньому нативному форматі, але й забезпечує їх нормалізацію, збагачення та аналітичну обробку через конвеєр прийому даних.

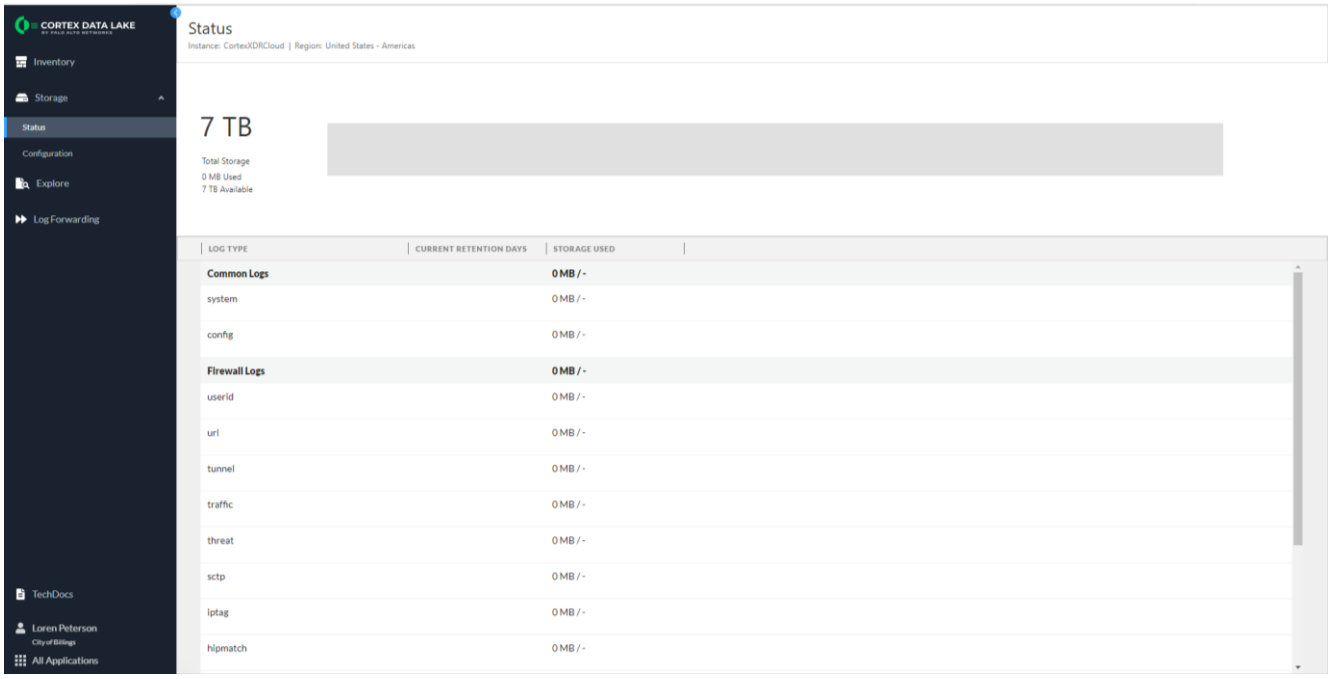

Рис. 3.1. Cortex Data Lake

Це сховище підтримує гнучкі моделі зберігання, включаючи гаряче \ та холодне зберігання, з можливістю розширення періодів утримання даних за допомогою додаткових ліцензійних надбудов. Наприклад, стандартна ліцензія Cortex XDR зазвичай надає місяць гарячого зберігання, але це може бути

розширено до кількох місяців або навіть років за допомогою додаткових ліцензій, таких як Period-Based Retention - Hot Storage або Additional Hot Storage. Холодне зберігання, що вимагає мінімум шести місяців додаткової ліцензії, стає доступним після закінчення періоду гарячого зберігання, забезпечуючи економічно ефективне довгострокове зберігання для цілей відповідності та глибокого полювання на загрози. Переваги використання Data Lake включають виняткову масштабованість (здатність зберігати петабайти даних), гнучкість щодо типів даних (структуровані, напівструктуровані, неструктуровані), економічну ефективність завдяки використанню об'єктного зберігання, покращену аналітику та швидший час до отримання інсайтів, а також підтримку реального часу та надійні можливості відновлення після збоїв.

Для середовищ, що вимагають збору даних з різноманітних зовнішніх систем, незамінною є Брокерська віртуальна машина (Broker VM).

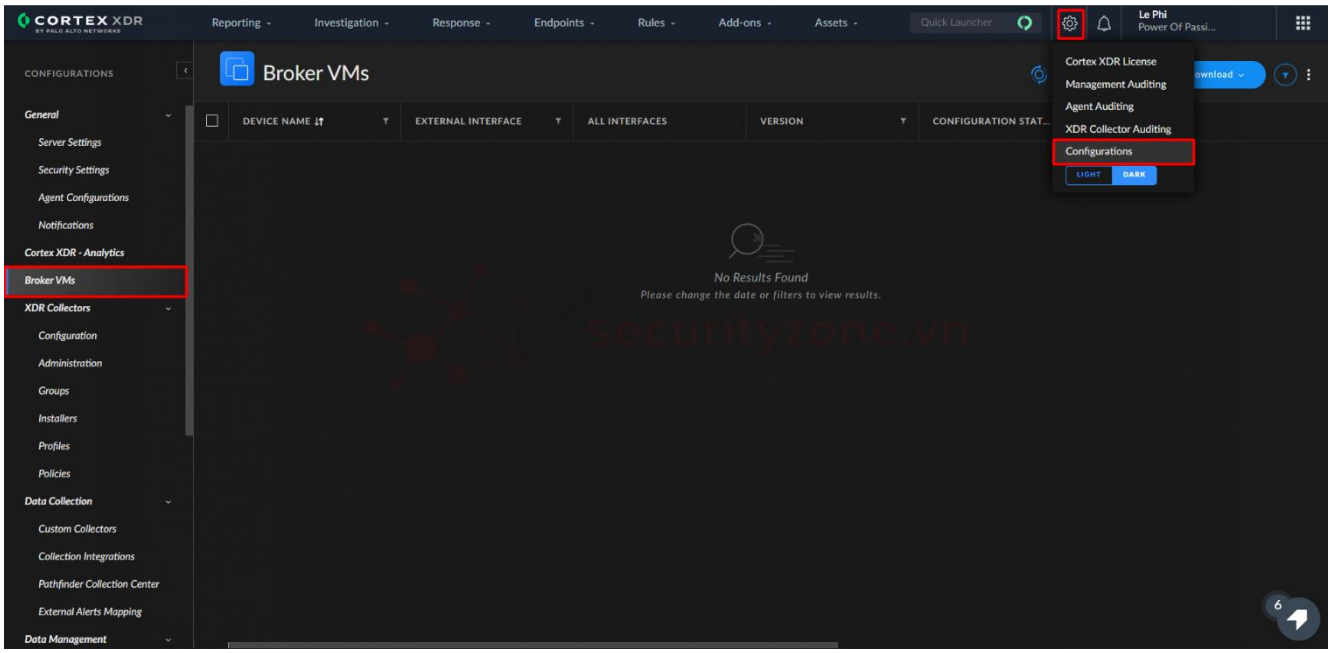

Рис. 3.2. Broker VM

Ця модульна віртуальна машина підтримує різні аплети, призначені для безпечного отримання даних та їх завантаження до Cortex Data Lake. Ці аплети включають:

- Syslog Collector: Для отримання syslog-повідомлень із зовнішніх систем, підтримує Active/Active конфігурацію для високої доступності.
- NetFlow Collector: Для збору та аналізу даних мережевого трафіку, також підтримує Active/Active.
- Windows Event Collector (WEC): Для збору журналів подій Windows, підтримує Active/Active.
- Kafka Collector, CSV Collector, FTP Collector, Files and Folders Collector, DB Collector: Для збору даних з Apache Kafka, CSV-файлів, FTP-трансферів, вказаних каталогів та баз даних відповідно. Ці аплети підтримують Active/Passive конфігурацію.
- Local Agent Settings: Функціонує як проксі-сервер для агентів, кешуючи пакети встановлення та оновлення контенту, що особливо корисно для мереж з обмеженим доступом до Інтернету.
- Network Mapper: Виконує виявлення пристроїв у мережі за допомогою активного сканування, не підтримує високу доступність.

Broker VM також дозволяє налаштовувати правила парсингу (parsing rules) для попередньої обробки, фільтрації, збагачення та маршрутизації журналів перед їх прийомом у набір даних, що допомагає зменшити вихідний мережевий трафік та оптимізувати використання ліцензії "Pro Per GB". Для підтримки великого обсягу даних, наприклад, 10 000 подій на секунду на ядро, Broker VM вимагає мінімум 8-ядерного процесора, 8 ГБ оперативної пам'яті та 512 ГБ дискового простору [14].

Нарешті, надійна мережа є першочерговою. Це передбачає забезпечення безперешкодного доступу до комунікаційних серверів Cortex XDR, сховищ та інших важливих ресурсів. Крім того, мережеві конфігурації повинні дозволяти однорангові оновлення контенту між агентами для оптимізації використання пропускної здатності. Загальна рекомендація полягає у виділенні 120 Мбіт/с пропускної здатності на кожні 100 000 агентів, з лінійним масштабуванням для більших розгортань. Важливо також врахувати можливість налаштування проксі-серверів для агентів Cortex XDR, що дозволяє їм комунікувати з платформою через

визначений проксі, а не безпосередньо з Інтернетом, що є типовим для середовищ з суворими мережевими політиками.

Розгортання XDR-рішення повинно слідувати ретельно структурованому, поетапному підходу, щоб мінімізувати операційні збої та забезпечити стабільність системи. Цей процес зазвичай починається з попередньої підготовки, що включає налаштування служб доступу Cortex XDR, конфігурацію брандмауера для дозволу необхідного зв'язку з серверами та сховищами Cortex XDR, а також встановлення необхідних сертифікатів та увімкнення перевірок CRL Windows. Одночасно виконується точний розрахунок пропускної здатності для оцінки необхідної мережевої потужності для запланованої кількості агентів, дотримуючись моделі лінійного масштабування (120 Мбіт/с на 100 000 агентів).

Після підготовки ініціюється пілотне розгортання, під час якого агент Cortex XDR встановлюється на невеликій, контрольованій групі з 3-10 кінцевих точок. Цей етап, що зазвичай триває близько одного тижня, є критично важливим для тестування очікуваної поведінки агента, включаючи ін'єкцію та застосування політик, а також для підтвердження відсутності негативних змін у досвіді користувача. Після успішного завершення пілотного розгортання, розгортання поступово розширюється на більші групи зі схожими атрибутами (наприклад, апаратне забезпечення, програмне забезпечення, профілі користувачів), з метою охоплення до 100 кінцевих точок протягом приблизно двох тижнів.

Наступний етап передбачає повномасштабне розгортання, під час якого агент Cortex XDR широко розповсюджується по всій організації, доки всі кінцеві точки не будуть захищені; цей процес може зайняти два або більше тижнів, залежно від розміру підприємства. Одночасно з розгортанням агентів, важливо визначити та налаштувати корпоративні політики, додаючи правила захисту для сторонніх або внутрішніх програм та ретельно тестуючи їх. Це включає створення індивідуальних профілів запобігання для різних платформ (Windows, macOS, Linux), налаштування дій при виявленні шкідливих скриптів, невідомих файлів або спроб крадіжки облікових даних, а також визначення режимів дії, таких як блокування, звітність або вимкнення, разом із параметрами карантину. Політики

потім уточнюються шляхом їх розгортання на невеликій кількості часто використовуваних кінцевих точок для тонкого налаштування, зазвичай протягом одного тижня. Завершальним кроком є глобальна фіналізація політик, розгортання уточнених правил захисту по всій мережі, процес, який займає лише кілька хвилин.

Постійні оновлення є життєво важливими для підтримки ефективної позиції безпеки. Агенти Cortex XDR можуть отримувати оновлення контенту негайно або з налаштованою затримкою до 30 днів. Поетапний план розгортання оновлень, починаючи з контрольної групи та поступово розширюючись (наприклад, 10%, 40%, 80% та повне розгортання), настійно рекомендується для забезпечення стабільності та мінімізації збоїв. Управління пропускною здатністю для цих оновлень також є ключовим для оптимізованої продуктивності.

Cortex XDR розроблений для безперешкодної інтеграції з існуючим стеком безпеки організації, тим самим максимізуючи цінність попередніх інвестицій та підвищуючи загальну позицію безпеки. Інтеграція з NGFW від Palo Alto Networks та пристроями Panorama дозволяє Cortex XDR збирати журнали мережевого трафіку та дані, забезпечуючи розширену видимість мережевої активності. Для цього потрібні дозволи Super User як на облікових записах Cortex XDR, так і на NGFW/Panorama, а також увімкнення профілів пересилання журналів у правилах брандмауера.

Cortex XDR може інтегруватися з системами управління інформацією та подіями безпеки, такими як Microsoft Sentinel або Splunk, для централізованої агрегації журналів та покращеного аналізу. Наприклад, оновлений конектор Codeless Connector Platform для Microsoft Sentinel пропонує гранульований контроль над збором даних та ефективно обробляє великі обсяги даних, включаючи журнали кінцевих точок, сповіщення, журнали аудиту управління та журнали аудиту агентів. Для інтеграції зі Splunk необхідно отримати API Key та Key ID з порталу Cortex XDR та налаштувати відповідний додаток Splunk Add-on for Palo Alto Networks. Ця інтеграція дозволяє XDR збагачувати дані SIEM та автоматизувати подальші розслідування.

Інтеграція з SOAR, такими як Cortex XSOAR, дозволяє автоматизувати реакції на інциденти та виконувати плейбуки в різних інструментах безпеки. Це включає можливість синхронізації та оновлення інцидентів Cortex XDR, їх класифікації, відображення полів, вилучення та збагачення індикаторів, а також виконання автоматизованих дій, таких як ізоляція кінцевих точок, блокування файлів або завершення процесів.

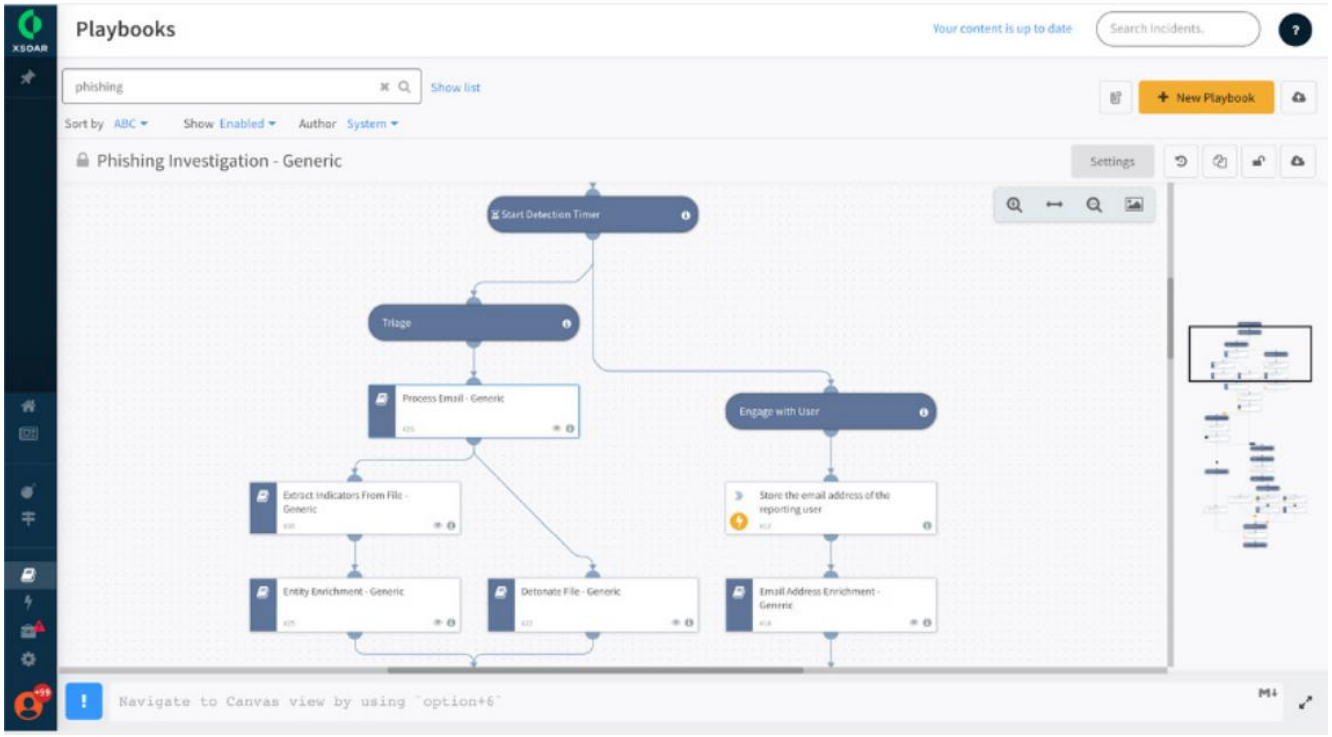

Рис. 3.3. Cortex XSOAR phishing playbook

Cortex XDR також отримує переваги від надійної інтеграції розвідданих про загрози, зокрема з Palo Alto Networks Threat Intelligence Cloud та WildFire. WildFire аналізує невідомі файли, надаючи детальні дані про їхню поведінку та вердикти (шкідливі, безпечні, сірі), що підвищує точність виявлення. Cortex XDR також може інтегруватися із зовнішніми службами розвідданих про загрози, такими як VirusTotal, відображаючи відповідні оцінки в деталях інцидентів.

Щодо хмарних середовищ та управління ідентифікацією, Cortex XDR моніторить та керує подіями та даними в хмарі, мережі та на кінцевих точках. Він інтегрується з рішеннями управління ідентифікацією, такими як Okta, для

розширеної видимості даних автентифікації та виявлення незвичайної активності користувачів, що є критично важливим для ідентифікації скомпрометованих облікових записів та внутрішніх загроз. Хмарні політики робочих навантажень у Cortex XDR допомагають запобігати порушенням безпеки в хмарних середовищах виконання, визначаючи правила та дії на основі етапів SDLC (CI, розгортання, виконання). Крім того, Cortex XDR може збирати журнали та дані з Microsoft 365 за допомогою Microsoft Graph API, збираючи електронні листи, інформацію про користувачів, групи та дані каталогу [15].

3.2. Розробка рекомедацій щодо виявлення складних загроз та цільових атак на базі рішення Cortex XDR

Cortex XDR є високофункціональним інструментом забезпечення кібербезпеки, що реалізує комплексний підхід до виявлення, аналізу та нейтралізації складних загроз, зокрема цільових атак, використовуючи сучасні технології штучного інтелекту, машинного навчання та глибоку інтеграцію з різними джерелами телеметрії. Платформа функціонує на основі багаторівневої архітектури виявлення загроз, яка дозволяє ефективно ідентифікувати як відомі шкідливі об'єкти, так і невідомі атаки, що не мають сигнатурної ознаки. Одним із ключових компонентів такої архітектури є модулі поведінкової аналітики, які забезпечують безперервне профілювання дій користувачів, кінцевих точок і застосунків.

Завдяки вбудованим алгоритмам машинного навчання та штучного інтелекту, система здатна динамічно формувати базові моделі "нормальної" поведінки для окремих суб'єктів в інформаційному середовищі, включаючи індивідуальні профілі користувачів, процесів, пристроїв та їхніх взаємодій. Виявлення аномалій ґрунтується на виявленні відхилень від цих моделей, що дозволяє своєчасно фіксувати загрози, які можуть залишитися поза межами традиційних методів захисту. Зокрема, таким чином ідентифікуються атаки, що супроводжуються крадіжкою облікових даних, зловживанням автентифікаційними

токенами або використанням тунельованих DNS-запитів, які зазвичай не детектуються на рівні стандартних систем виявлення.

Для підвищення ефективності детекції Cortex XDR поєднує сигнатурні та поведінкові підходи, використовуючи індикатори компрометації та поведінкові індикатори компрометації. BIOC-правила створюються з використанням мови запитів XQL, яка забезпечує високий ступінь гнучкості при формуванні умов виявлення на основі різних типів подій. Завдяки підтримці фільтрації подій, логічних умов і часових рамок, XQL дає змогу створювати детальні правила, які знижують кількість хибнопозитивних спрацьовувань. Крім того, аналітики мають змогу верифікувати створені правила на історичних даних, що дозволяє оцінити потенційну ефективність ще до розгортання в продуктивному середовищі.

Важливою складовою екосистеми Cortex XDR є інтеграція з сервісом WildFire — хмарною системою автоматичного аналізу файлів на наявність шкідливого коду. Цей сервіс дозволяє класифікувати невідомі файли на основі аналізу їхньої поведінки в ізольованому середовищі, що доповнює поведінкову аналітику XDR додатковим джерелом високоточних вердиктів щодо шкідливості, нейтральності або підозрілої активності файлів.

Платформа забезпечує виявлення цілого спектра загроз, серед яких — програми-вимагачі, атаки типу Advanced Persistent Threat (APT), внутрішні загрози, а також атаки на ланцюги постачання. У випадку ransomware-атак Cortex XDR здатний виявляти характерні дії, що передують масовому шифруванню даних, зокрема аномальні модифікації реєстру, нетипову зміну розширень файлів або запуск процесів шифрування з високою інтенсивністю. Водночас система може автоматично ініціювати заходи реагування, наприклад ізолювати скомпрометовані вузли, щоб обмежити подальше розповсюдження загрози. Для протидії APT-атакам платформа забезпечує всебічну видимість кінцевих точок, мережевого трафіку, програмної взаємодії та поведінкових моделей користувачів, з можливістю детального кореляційного аналізу на рівні всієї інфраструктури [16].

Детектування ознак APT відбувається через ідентифікацію патернів, характерних для тривалих прихованих атак — зокрема спроб несанкціонованого

доступу, використання вразливостей з ескалацією привілеїв, встановлення бекдорів, тривалого прихованого збору даних тощо. Крім того, поведінковий аналіз дозволяє ідентифікувати внутрішні загрози, що проявляються у вигляді нетипових дій співробітників: доступ до конфіденційних файлів поза межами службових обов'язків, несанкціоноване завантаження великих обсягів даних або підозріла активність у неробочі години. Cortex XDR також забезпечує моніторинг зовнішніх взаємодій, що дає змогу виявляти атаки на ланцюги постачання шляхом виявлення аномальної активності сторонніх користувачів, а також інтегрувати внутрішні сигнали з зовнішніми джерелами розвідданих для ідентифікації компрометованих компонентів у програмному забезпеченні або інфраструктурі постачальників.

Проактивне полювання на загрози у межах платформи реалізується за допомогою побудови гіпотез, що ґрунтуються на відомих TTP, розвідданих про поточні загрози або специфічних факторах ризику для конкретного середовища. Аналітики можуть ініціювати глибоке дослідження телеметрії за допомогою XQL-запитів, які дозволяють здійснювати пошук як в окремих наборах даних, так і по всій множині xdr_data, забезпечуючи високий рівень деталізації запитів. Такий підхід дає змогу виявляти складні загрози, зокрема бічне переміщення (наприклад, копіювання SSH-ключів, доступ до привілейованих систем), а також спроби прихованого розгортання інструментів керування. Інтеграція з фреймворком MITRE ATT&CK надає аналітикам можливість співвідносити виявлену активність з класифікованими техніками атак, що сприяє більш точному формуванню гіпотез і побудові сценаріїв реагування.

Для забезпечення ефективності роботи команди безпеки важливим аспектом є зниження кількості хибнопозитивних сповіщень. У цьому контексті важливу роль відіграють правила кореляції, які є основою логічного зіставлення окремих подій у межах складних сценаріїв атак. Оптимізація таких правил передбачає багатоетапний процес: аналіз історичних даних для виявлення повторюваних індикаторів загроз, формування часових вікон, що дозволяють охопити як швидкі, так і повільні атаки, а також впровадження контекстної фільтрації на основі критичності активів або типу взаємодії. Крім того, об'єднання різних типів подій

сприяє формуванню більш повної картини атаки, а порогові значення дозволяють кількісно оцінити ризик і формувати сповіщення лише за наявності сукупності критеріїв.

Усі новостворені правила підлягають перевірці в тестовому середовищі за допомогою режиму симуляції, що забезпечує високу достовірність моделі перед її впровадженням у продуктивне середовище. Cortex XDR також підтримує імпорт даних із зовнішніх джерел розвідки, таких як MITRE ATT&CK, AlienVault OTX або власні джерела організації, що забезпечує оперативне оновлення бази індикаторів компрометації. Крім виявлення, платформа забезпечує запобігання шкідливій активності шляхом конфігурації профілів запобігання для різних операційних систем — Windows, macOS, Linux — з можливістю адаптації дій (блокування, повідомлення, карантин) залежно від типу виявленої загрози [17].

3.3. Розробка рекомендацій щодо виявлення складних загроз та цільових атак засобами XDR

Для ефективного виявлення складних загроз та цільових атак необхідно застосовувати комплексний підхід, що враховує постійну еволюцію методів зловмисників та складність IT-середовищ. Традиційні заходи безпеки, що базуються на сигнатурах, часто є недостатніми, що вимагає переходу до проактивних, адаптивних стратегій виявлення та реагування.

Складні загрози, такі як APT, є високоорганізованими та витонченими кібератаками, що здійснюються кваліфікованими зловмисниками, часто спонсорованими державами. Ці атаки є довгостроковими кампаніями, що включають кілька етапів та різноманітні методи, спрямовані на отримання та підтримання доступу протягом значного періоду. Вони характеризуються місійно-орієнтованими зловмисниками, стратегічними цілями (кібершпигунство, фінансова вигода, хактивізм, руйнування), наполегливістю, інтенсивністю ресурсів та скритністю. Життєвий цикл APT включає початковий доступ, розгортання шкідливого програмного забезпечення, розширення доступу та латеральне

переміщення, підготовку атаки, ексфільтрацію або завдання шкоди, а також подальші атаки для забезпечення персистентності. Цільові атаки, хоча й відрізняються за масштабом, також є навмисними та продуманими, що включають збір розвідувальної інформації, проникнення, командно-контрольну комунікацію, латеральне переміщення, виявлення активів та ексфільтрацію даних. Ефективне виявлення таких загроз вимагає ідентифікації ланцюжків, здавалося б, нешкідливих подій та тонких поведінкових аномалій з часом, а не покладання виключно на ізольовані індикатори компрометації [18].

Для розуміння та протидії цим загрозам використовується фреймворк MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge). Він надає детальний огляд методів, які використовують зловмисники, допомагаючи зрозуміти "чому" (тактики) та "як" (техніки та процедури) працюють атаки. Фреймворк класифікує 14 тактик, таких як початковий доступ, виконання, персистентність, підвищення привілеїв, ухилення від захисту, доступ до облікових даних, виявлення, латеральне переміщення, збір, ексфільтрація та командно-контрольні канали. Зіставлення TTP APT з MITRE ATT&CK надає структурований спосіб розуміння поведінки зловмисників, що дозволяє застосовувати проактивний підхід до безпеки. Впровадження MITRE ATT&CK включає ідентифікацію відповідних тактик та технік, моделювання загроз, аналіз прогалин, посилення заходів безпеки, навчання персоналу, включення знань до планів реагування на інциденти, а також безперервний моніторинг та вдосконалення.

XDR є рішенням з кібербезпеки, яке об'єднує дані про загрози з різних інструментів безпеки, що дозволяє більш ефективно та швидко розслідувати, виявляти загрози та реагувати на них. Це еволюція EDR, що розширює його сферу застосування за межі лише кінцевих точок, включаючи мережі, сервери, хмарні робочі навантаження, електронну пошту та інші рівні безпеки. XDR збирає необроблені дані з різних джерел, застосовує розширену аналітику та алгоритми машинного навчання для кореляції подій, інтегрує розвідку загроз та має автоматизовані механізми реагування. На відміну від SIEM, який є переважно пасивним аналітичним інструментом, XDR прагне вирішити проблеми

ефективного виявлення та реагування на цільові атаки, включаючи аналіз поведінки та профілювання. XDR також пропонує спрощену автоматизацію порівняно зі SOAR, забезпечуючи можливість дій від платформи XDR до підключених інструментів безпеки.

Palo Alto Networks Cortex XDR є платформою розширеного виявлення та реагування, яка моніторить та керує подіями та даними хмари, мережі та кінцевих точок, поєднуючи функції запобігання інцидентам, виявлення, аналізу та реагування в централізованій платформі. Архітектура Cortex XDR включає додаток Cortex XDR, Cortex Data Lake, аналітичний двигун, брандмауери наступного покоління, Prisma Access, GlobalProtect та агенти Cortex XDR.

Cortex XDR використовує багатогранний підхід для виявлення складних загроз. Застосовується поведінкова аналітика та машинне навчання для безперервного профілювання поведінки користувачів та кінцевих точок, виявлення аномальної активності та запобігання загрозам нульового дня. Система досліджує завантажені файли за допомогою ШІ, блокує поведінку, схожу на експлойти, та ідентифікує шкідливі передачі даних або процеси, пропонуючи захист від програм-вимагачів, безфайлового шкідливого програмного забезпечення та інструментів збору облікових даних. Cortex XDR автоматично об'єднує дані кінцевих точок, мережі, хмари та ідентифікації з різних джерел у Cortex Data Lake, руйнуючи силоси безпеки та забезпечуючи повну картину кожної загрози. Використовується мова запитів Cortex (XQL) для виявлення шаблонів, аномалій або послідовностей дій, які можуть вказувати на шкідливу поведінку. Cortex XDR пропонує готові правила з покриттям MITRE ATT&CK, автоматично виявляючи активні атаки та зіставляючи сповіщення з конкретними тактиками та техніками. Система забезпечує 360-градусний огляд користувачів, включаючи показники ризику, для виявлення скомпрометованих облікових записів та зловживання обліковими даними.

Для ефективного використання Cortex XDR у виявленні складних загроз та цільових атак рекомендується комплексний підхід. Необхідно забезпечити інтеграцію всіх відповідних джерел даних (кінцеві точки, мережі, хмара,

ідентифікація, сторонні брандмауери) у Cortex Data Lake для максимальної видимості та кореляції. Слід активно застосовувати можливості ШІ та машинного навчання Cortex XDR для безперервного профілювання поведінки користувачів та кінцевих точок, виявлення аномалій та запобігання загрозам нульового дня. Важливо розробляти та впроваджувати спеціальні правила кореляції за допомогою XQL для виявлення конкретних шаблонів або послідовностей дій, унікальних для ландшафту загроз організації або відомих TTP APT, налаштовувати та оптимізувати політики для захисту від шкідливого програмного забезпечення, контролю пристроїв, брандмауера хоста та шифрування диска, регулярно переглядаючи та коригуючи їх на основі виявлених ризиків. Агенти Cortex XDR та вміст повинні підтримуватися оновленими для забезпечення найновіших функцій безпеки та сумісності, використовуючи поетапний план розгортання для мінімізації збоїв . Інтеграція з постачальниками ідентифікації, такими як Okta або Azure AD, розширює видимість даних автентифікації, дозволяючи виявляти зловживання обліковими даними та забезпечувати запобігання атакам на основі ідентифікації .

У сфері проактивного виявлення загроз слід активно шукати приховане шкідливе програмне забезпечення, цільові атаки та внутрішні загрози, використовуючи інструменти пошуку Cortex XDR. Для цілодобового моніторингу та експертного аналізу можуть бути використані керовані послуги полювання на загрози. Необхідно постійно зіставляти можливості виявлення з фреймворком MITRE ATT&CK для виявлення та усунення прогалин у безпеці, пріоритизації захисту та розуміння поведінки зловмисників . Особливу увагу слід приділяти виявленню незвичайної активності облікових записів користувачів, нехарактерного доступу/передачі даних, раптового збільшення спроб фішингу, файлів у незвичайних місцях та аномалій у вихідних даних, оскільки ці тонкі ознаки часто є першими індикаторами складних атак. Виявлені загрози слід автоматично збагачувати даними зовнішніх джерел розвідки загроз для отримання глибшого контексту та прийняття більш обґрунтованих рішень щодо безпеки .

У контексті реагування на інциденти та відновлення, слід використовувати автоматизовані механізми реагування Cortex XDR та заздалегідь визначені

"плейбуки" для швидкого стримування та усунення загроз . Це включає такі дії, як ізоляція кінцевих точок, блокування шкідливого трафіку, припинення ланцюжків причинності та запуск сканування на шкідливе програмне забезпечення. Автоматизований аналіз першопричин Cortex XDR та криміналістичні часові шкали допомагають швидко виявити походження, обсяг та вплив атак, а також відтворити дії зловмисників . Інтелектуальне групування та дедуплікація сповіщень зменшують втому від сповіщень та спрощують розслідування, забезпечуючи повну картину кожного інциденту . Інтеграція Cortex XDR з існуючими платформами SOAR може забезпечити розширену оркестрацію та автоматизовані "плейбуки" у ширшій екосистемі безпеки . Функція Live Terminal дозволяє швидко перевіряти та стримувати загрози без порушення роботи кінцевих користувачів, надаючи прямий доступ до кінцевих точок для виконання команд та сценаріїв .

Cortex XDR демонструє високу ефективність у виявленні та реагуванні на складні загрози та цільові атаки, про що свідчить його комплексна інтеграція даних, розширена аналітика та високі показники в оцінках MITRE ATT&CK, включаючи нульовий рівень помилкових спрацьовувань та 100% виявлення на рівні техніки . Його здатність уніфікувати дані з кінцевих точок, мереж, хмари та джерел ідентифікації забезпечує неперевершену видимість, дозволяючи виявляти приховані, багатоетапні атаки, які традиційні розрізнені інструменти часто пропускають . Автоматизований аналіз першопричин платформи, інтелектуальне групування сповіщень та можливості швидкого реагування значно скорочують час розслідування та втому від сповіщень, підвищуючи ефективність центрів операцій безпеки .

Майбутні тенденції вказують на подальше розширення можливостей XDR, особливо завдяки досягненням у галузі штучного інтелекту (ШІ) та генеративного ШІ (GenAI) . Провідні постачальники XDR впроваджують помічників безпеки на основі GenAI для обробки величезних обсягів даних у реальному часі, виявлення шаблонів, автоматичного створення зведень інцидентів та надання рекомендацій для розслідувань. Це ще більше мінімізує помилкові спрацьовування та

пріоритезує критичні сповіщення. Фокус XDR зміщується від реактивного до проактивного, причому запобігання стає четвертою основною обіцянкою, що обумовлено глибшою інтеграцією з даними ідентифікації та використанням розвідки загроз . ШІ в XDR продовжуватиме спрощувати складні завдання, знижуючи бар'єри для входу нових фахівців з безпеки та розширюючи можливості існуючих команд . Рішення XDR продовжуватимуть розвиватися, з регулярними оновленнями агентів та вмісту, новими функціями та покращеною інфраструктурою бекенду для підтримки мільярдів подій на секунду.

ВИСНОВКИ

У ході проведеного дослідження розглянуто підходи до виявлення складних загроз і цільових атак із використанням технологій класу XDR на прикладі рішення Cortex XDR. Було проаналізовано архітектуру та функціональні можливості платформи, її здатність інтегрувати розрізнені джерела телеметрії з кінцевих точок, мережевої інфраструктури, хмарних сервісів та сторонніх систем, а також ефективно застосовувати методи поведінкового аналізу для виявлення загроз, які залишаються поза межами виявлення традиційних сигнатурних підходів. Cortex XDR використовує багаторівневу модель аналізу, поєднуючи індикатори компрометації, поведінкові індикатори компрометації, машинне навчання, аналіз невідомих об’єктів через WildFire та кореляцію подій у межах масштабного аналітичного середовища. Цей підхід дозволяє не лише фіксувати факти компрометації, але й виявляти ранні ознаки потенційної атаки на етапах розвідки, ініціалізації або прихованої активності.

Дослідження продемонструвало, що Cortex XDR є ефективним засобом виявлення таких складних загроз, як кампанії APT, атаки програм-вимагачів, внутрішні загрози з боку компрометованих або зловмисних користувачів, а також атаки на ланцюг постачання, які часто маскуються під легітимну активність або використовують компрометовані інструменти розробки. Завдяки створенню поведінкових профілів для користувачів, систем і додатків, платформа виявляє навіть незначні аномалії, які можуть свідчити про підготовку атаки або відхилення від нормального функціонування. Інтеграція з MITRE ATT&CK дозволяє узгоджувати виявлення з відомими тактиками, техніками та процедурами атакувальників, що підвищує якість розслідування інцидентів і покращує оперативну відповідь на інциденти.

Особлива увага у дослідженні приділена механізмам формування правил кореляції, поведінкових індикаторів, а також можливостям платформи у підтримці процесу полювання на загрози.

Засоби формування XQL-запитів надають аналітикам інструменти для побудови складних гіпотез, верифікації нових TTP та виявлення ланцюгів дій зловмисника задовго до фактичного нанесення шкоди. У процесі дослідження розглянуто також аспекти оптимізації виявлення з метою мінімізації хибнопозитивних спрацювань, зокрема застосування історичних даних, часових вікон, відображення сутностей та об’єднання типів подій задля досягнення кращого контексту та зменшення рівня шуму в системі.

Результати аналізу дали змогу сформулювати рекомендації щодо ефективного використання функціоналу Cortex XDR для забезпечення комплексного захисту організацій від загроз підвищеної складності. Платформа довела свою ефективність як інструмент раннього виявлення, детального аналізу, проактивного реагування та полювання на загрози. Її застосування забезпечує не лише оперативне виявлення атак, а й створює основу для побудови стратегії превентивного захисту, орієнтованої на динамічний розвиток загроз і адаптивність атакувальних технік. Таким чином, використання Cortex XDR дозволяє організаціям перейти від реактивної моделі безпеки до проактивної, підвищуючи стійкість інфраструктури до складних і цільових атак.

ПЕРЕЛІК ПОСИЛАНЬ

1. What Are Advanced Persistent Threats (APT) & 5 Defensive Measures. *All-in-One Cybersecurity Platform - Cynet*. URL: https://www.cynet.com/advanced-persistent-threat-apt-attacks/ (дата звернення: 03.04.2025).
2. The Evolution of Cybercrime: Adapting to APT Techniques. *Critical Start*. URL: https://www.criticalstart.com/the-evolution-of-cybercrime-adapting-to-apt-techniques/ (дата звернення: 03.04.2025).
3. What Is an Advanced Persistent Threat (APT)? | Splunk. *Splunk*. URL: https://www.splunk.com/en_us/blog/learn/apts-advanced-persistent-threats.html (дата звернення: 04.04.2025).
4. What is Heuristic Analysis? Definition and Examples - ThreatDown by Malwarebytes. *ThreatDown by Malwarebytes*. URL: https://www.threatdown.com/glossary/what-is-heuristic-analysis/ (дата звернення: 04.04.2025).
5. Understanding the Difference Between EDR, SIEM, SOAR, and XDR. *SentinelOne*. URL: https://www.sentinelone.com/cybersecurity-101/xdr/understanding-the-difference-between-edr-siem-soar-and-xdr/ (дата звернення: 08.04.2025).
6. EDR vs. NDR vs. XDR: How to Pick a Detection Response Solution. *SentinelOne*. URL: https://www.sentinelone.com/cybersecurity-101/endpoint-security/edr-vs-ndr-vs-xdr/ (дата звернення: 08.04.2025).
7. Explore 6 XDR Vendors For 2025. *SentinelOne*. URL: https://www.sentinelone.com/cybersecurity-101/xdr/xdr-vendors/ (дата звернення: 10.04.2025).
8. Enhancing Incident Response Readiness with XDR Integration. *Threat Intelligence*. URL: https://www.threatintelligence.com/blog/incident-response-readiness (дата звернення: 10.04.2025

9. *We are Exclusive Networks*. URL: https://www.exclusive-networks.com/ma/wp-content/uploads/sites/2/2020/12/cortex-xdr.pdf (дата звернення: 18.04.2025).

10. *Cortex Help Center*. URL: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Documentation/Get-started-with-Cortex-XDR (дата звернення: 18.04.2025).

11. Cortex XDR. URL: https://webobjects2.cdw.com/is/content/CDW/cdw/on-domain-cdw/brands/palo-alto-networks/cortex-xdr.datasheet.pdf?=gcl (дата звернення: 26.04.2025).

12. Palo Alto Networks documentation portal. *Palo Alto Networks documentation portal*. URL: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Documentation/Ingest-data-from-Next-Generation-Firewall (дата звернення: 26.04.2025).

13. Cortex XDR. *Exclusive Networks*. URL: https://www.exclusive-networks.com/se/wp-content/uploads/sites/25/2021/11/palo-alto-networks-datasheet-cortex-xdr.pdf (дата звернення: 02.05.2025).

14. Research and Markets. Extended Detection and Response (XDR) Global Markets 2024-2027: Leveraging New Capabilities to Expand Across Regions and Maturity Levels, Developing New Technology, Detections, and Intelligence. *GlobeNewswire News Room*. URL: https://www.globenewswire.com/news-release/2025/02/26/3033119/28124/en/Extended-Detection-and-Response-XDR-Global-Markets-2024-2027-Leveraging-New-Capabilities-to-Expand-Across-Regions-and-Maturity-Levels-Developing-New-Technology-Detections-and-Intel.html (дата звернення: 02.05.2025).

15. Compare Cortex XDR vs. CrowdStrike now. *Palo Alto Networks*. URL: https://www.paloaltonetworks.com.au/cortex/xdrvscrowdstrike (дата звернення: 06.05.2025)

16. The Gold Standard: Cortex XDR's Unmatched Results in MITRE's Latest Evaluation. *Welcome to the WEI Tech Exchange Blog*. URL: https://blog.wei.com/the-gold-standard-cortex-xdrs-unmatched-results-in-mitres-latest-evaluation (дата звернення: 06.05.2025).

17. How to Reduce False Positives & Ensure Data Accuracy for Enterprises | Fidelis Security. *Fidelis Security*. URL: https://fidelissecurity.com/threatgeek/xdr-security/reduce-false-positives-and-ensure-data-accuracy-with-xdr/ (дата звернення: 15.05.2025).

18. Labs P. What Is Advanced Persistent Threat (APT)?. *Automated Security Validation Platform | Picus*. URL: https://www.picussecurity.com/resource/glossary/what-is-advanced-persistent-threat-apt (дата звернення: 20.05.2025).