ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТАЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту кінцевих точок інформаційної системи організації від сучасних загроз на прикладі Cortex-XDR»

зі спеціальності *125 Кібербезпека та захист інформації*
(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

_____ Семен МОСКОВКА
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62
МОСКОВКА Семен
(прізвище, ім'я)

Керівник д.т.н., професор ГАЙДУР Галина
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

EPM – Endpoint Protection Modules

IoCs – Indicators of Compromise

ITDR – Threat Detection and Response

MTTD – Mean Time to Detect

MTTR – Mean Time to Respond

NTA – Network Traffic Analysis

TTPs – tactics, techniques, and procedures

UEBA – user and entity behavior analytics

XDR – Extended Detection and Response

ВСТУП

Актуальність захисту кінцевих точок сьогодні є надзвичайно важливою. Кінцеві точки — це наші ноутбуки, смартфони, сервери та всі інші пристрої, з якими працюють користувачі інформаційної системи організації. Саме ці пристрої стали головною мішенню для кіберзлочинців, для проведення атак, які здатні порушити виконання бізнес процесів організацій. Сучасні атаки за остання роки значно ускладнилися і стали більш витонченими. Як приклад, зловмисники використовують штучний інтелект для створення більш переконливих фішингових повідомлень і маскування шкідливого програмного забезпечення. Такі атаки можуть бути на виявлені користувачем.

Традиційні антивіруси вже не можуть ефективно протистояти цим новим загрозам, таким як програми-вимагачі (ransomware) та цілеспрямовані атаки. Кінцеві точки є дверима до найцінніших корпоративних даних та інтелектуальної власності організацій. Якщо ці пристрої будуть скомпрометовані, це призведе до витоку даних, значних фінансових втрат та шкоди репутації компанії. Тому захист кінцевих точок вимагає комплексних рішень з функціями виявлення та реагування (EDR), які постійно моніторяться і захищають пристрої в режимі реального часу.

Таким чином, дослідження питань захисту кінцевих точок має важливе значення для забезпечення стабільності та безпеки організацій у сучасному інформаційному середовищі.

Об’єкт дослідження – захист кінцевих точок інформаційної системи організації.

Предмет дослідження – технологія захисту кінцевих точок інформаційної системи на прикладі Cortex-XDR.

Метою роботи – є дослідження технології захисту кінцевих точок інформаційної системи на прикладі Cortex-XDR та розробка рекомендації щодо її застосування.

Наукові завдання:

дослідити сутність проблеми захисту кінцевих точок інформаційної системи організації;

проаналізувати підходи до вирішення проблеми захисту кінцевих точок інформаційної системи організації;

проаналізувати існуючі технології захисту кінцевих точок інформаційної системи організації;

проаналізувати методи та засоби захисту кінцевих точок інформаційної системи організації; на прикладі Cortex-XDR;

розробити рекомендації щодо застосування технології захисту кінцевих точок інформаційної системи організації на прикладі Cortex-XDR.

Методи дослідження: опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, практичне використання засобів захисту віддалених користувачів.

Практичне значення одержаних результатів: запропоновано рекомендації щодо захисту кінцевих точок інформаційної системи організації.

Апробація результатів.

Гайдур Г.І., Московка С.М. Захист кінцевих точок інформаційної системи організації від сучасних загроз. *Актуальні проблеми кібербезпеки*: матеріали всеукраїнської наук.-практ. конф., м. Київ: ДУІКТ, 29 жовт. 2025р. Київ. С 202-203.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Проблема безпеки кінцевих точок в інформаційній системи організації

Безпека кінцевих точок – це підхід до кібербезпеки, який захищає пристрої кінцевих користувачів, такі як ноутбуки, настільні комп'ютери, мобільні телефони та сервери, від кіберзагроз. Він гарантує безпеку цих точок доступу до мережі організації, запобігаючи несанкціонованому доступу зловмисників або компрометації даних [1, 19].

Безпека кінцевих точок розширює периметр безпеки організації на кожен окремий пристрій, який підключається до її мережі (рис.1.1). Ці пристрої, або «кінцеві точки», є потенційними точками входу для кібератак , що робить їх комплексний захист першочерговим завданням [1, 19].

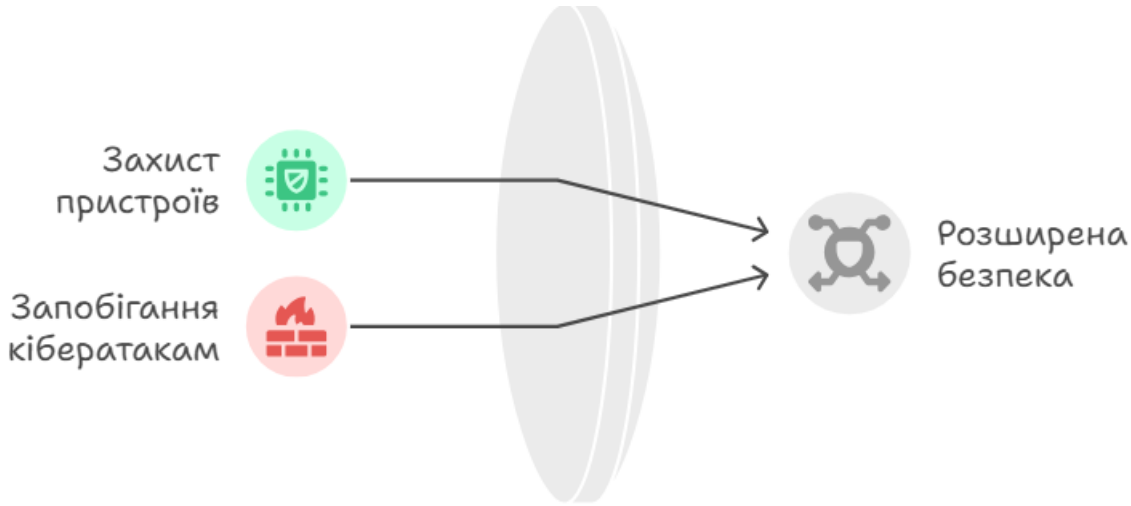

Рис.1.1. Безпека кінцевих пристроїв

Ефективна безпека кінцевих точок — це не просто встановлення антивірусного програмного забезпечення; вона охоплює складний набір технологій та стратегій, розроблених для виявлення, запобігання та реагування на загрози, спрямовані на ці критичні точки доступу (рис.1.2).

Рис.1.2. Компоненти захисту кінцевої точки [11]

Оскільки сучасна робоча сила стає дедалі мобільнішою та розподіленою, традиційний мережевий периметр розчиняється, висуваючи кінцеві точки на передній план кіберзахисту. Захист цих пристроїв безпосередньо сприяє захисту конфіденційних даних, підтримці безперервності роботи та збереженню репутації організації.

Безпека кінцевих точок є надзвичайно важливим питанням, оскільки кінцеві точки є основними цілями для кібератак, часто слугуючи початковою точкою компрометації для ширших мережевих вторгнень. Величезний обсяг та різноманітність кінцевих пристроїв — від ноутбуків та мобільних телефонів до пристроїв та серверів Інтернету речей — створюють розширену поверхню для атак, що потребує спеціального захисту. Без стійкого захисту кінцевих точок навіть складні засоби захисту периметра можуть бути обійдені загрозами, які безпосередньо спрямовані на пристрої користувачів.

Розширення поверхні атаки

Поширення віддаленої роботи, мобільних пристроїв та хмарних додатків значно розширило традиційний периметр мережі. Кожна кінцева точка, що має

доступ до корпоративних ресурсів, є потенційною вразливістю. Кіберзлочинці використовують ці окремі точки входу за допомогою різних векторів атак, включаючи фішинг , шкідливе програмне забезпечення та непатчеве програмне забезпечення, що робить безпеку кінцевих точок критично важливою лінією захисту.

«Захист кінцевих точок» зазвичай стосується повного спектру інструментів, процесів і послуг, що використовуються для захисту всього масиву кінцевих точок організації, незалежно від їх розташування чи формату. Його можна вважати стратегічним підходом до безпеки кінцевих точок, що охоплює низку різних інструментів і послуг. Одним із таких наборів інструментів є виявлення та реагування на кінцеві точки (EDR), що є важливою частиною загальної системи захисту кінцевих точок [15].

Рішення EDR використовує такі можливості, як безперервний моніторинг, інтегрована аналітика загроз, брандмауери, контроль доступу тощо, для проактивного сканування даних кінцевих точок на наявність активності, яка може свідчити про потенційну атаку або компрометацію, що може призвести до інциденту безпеки, такого як зараження шкідливим програмним забезпеченням або витік даних. Інструменти EDR є неоціненною частиною ширшої стратегії захисту кінцевих точок, як це показано на рис 1.3.

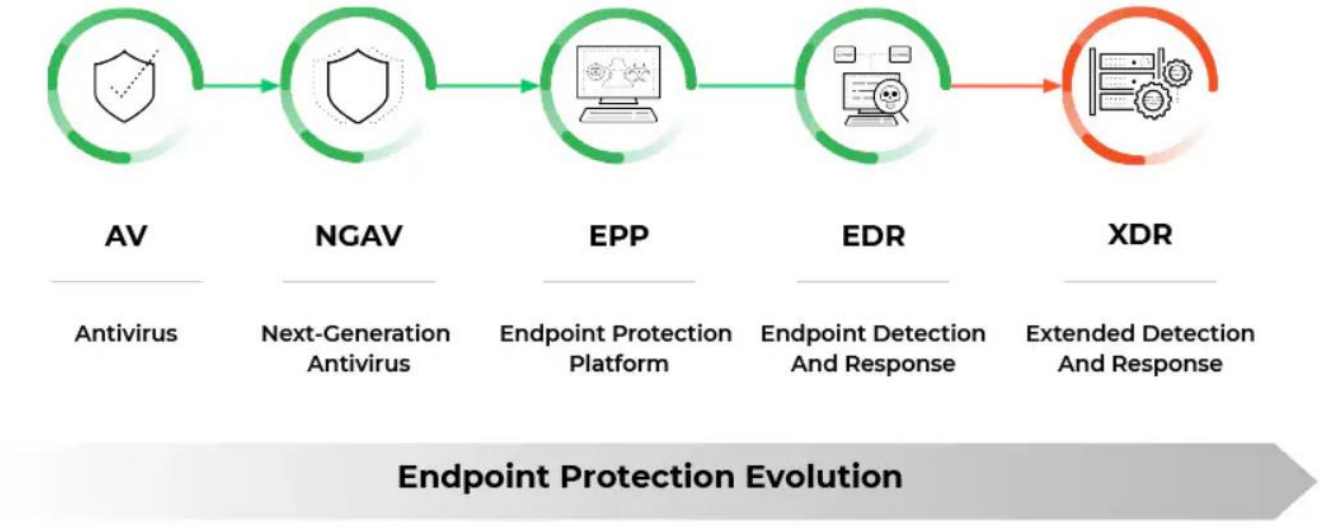

Рис. 1.3. Еволюція захисту кінцевих точок

Захист кінцевих точок зміцнює захист організації від великої та зростаючої кількості загроз, вразливостей та векторів атак. Серед найпоширеніших та найчастіших загроз для кінцевих точок є шкідливе програмне забезпечення , складні постійні загрози , фішинг та соціальна інженерія .

Інші типи атак на кінцеві точки, які стратегія захисту кінцевих точок повинна виявляти та відбивати, включають:

Крадіжка облікових даних;

Несанкціонований доступ до мережі;

Безфайлове шкідливе програмне забезпечення;

Програми-вимагачі;

Витік даних.

Зрештою, ще одним важливим ризиком для надійної безпеки кінцевих точок є внутрішні загрози , які можуть бути недбалими або зловмисними. Ненавмисні, випадкові атаки на кінцеві точки виникають через неправильні конфігурації засобів контролю безпеки або прості помилки користувача, що може призвести до «відкриття дверей» для хакерів.

Однак зловмисники-інсайдери є надзвичайно небезпечними, оскільки вони мають доступ, засоби та можливості отримати доступ до даних, які вони можуть вирішити викрасти або надіслати третім сторонам. Організації повинні мати план реагування на інциденти та відповідні можливості реагування, щоб запобігти поширенню будь-якої виявленої загрози по мережі та пов'язаних з нею системах.

Захист кінцевих точок широко застосовується в організаціях будь-якого розміру, у всіх галузях промисловості, з різним ступенем технічної складності та в усіх географічних регіонах. Існує безліч варіантів використання рішень для захисту кінцевих точок, оскільки поширеність і важливість систем кінцевих точок зростають безперервно.

Фактично, зі зростанням впровадження технології Інтернету речей, очевидно, що сама кількість кінцевих точок стрімко зросте в найближчі роки. Існує багато важливих випадків використання, коли організаціям слід впроваджувати рішення для захисту кінцевих точок. До них належать:

Запобігання зараженню шкідливим програмним забезпеченням. Рішення для захисту кінцевих точок використовують виявлення на основі сигнатур, евристичний аналіз та моніторинг поведінки для запобігання зараженню кінцевих точок шкідливим програмним забезпеченням [15].

Керування пристроями/ Функції керування пристроями для керування та обмеження використання периферійних пристроїв, таких як USB-накопичувачі та зовнішні пристрої зберігання даних.

Контроль програм. Організації повинні визначати та забезпечувати дотримання політик, що регулюють роботу програм, що працюють на кінцевих точках.

Виявлення та реагування на кінцеві точки (EDR). Можливості моніторингу та реагування в режимі реального часу життєво важливі для виявлення та реагування на складні загрози кінцевим точкам.

Шифрування файлів і дисків. Рішення для захисту кінцевих точок можуть пропонувати функції шифрування для шифрування файлів і дисків на кінцевих точках.

Запобігання втраті даних (DLP). функції DLP відстежують і контролюють передачу конфіденційних даних з кінцевих точок і запобігають спробам вилучення, крадіжки або передачі даних неавторизованим третім сторонам.

Аналіз поведінки користувачів (UEBA). Функції UEBA аналізують поведінку користувачів на кінцевих точках для виявлення аномалій та потенційних ознак компрометації.

Захист від фішингу та соціальної інженерії. Організаціям потрібні рішення для виявлення та блокування фішингових електронних листів, шкідливих веб-сайтів та інших атак соціальної інженерії, спрямованих на обман користувачів.

Керування виправленнями. ці можливості забезпечують оперативне оновлення кінцевих точок останніми виправленнями безпеки та оновленнями програмного забезпечення.

Віддалене керування та моніторинг. Рішення для захисту кінцевих точок зазвичай включають централізовані консолі керування, які дозволяють

адміністраторам віддалено розгортати, налаштовувати, контролювати та керувати політиками безпеки та оновленнями на всіх кінцевих точках в організації.

1.2. Аналіз загроз кінцевих точок інформаційної системи організації

Характер кіберзагроз постійно розвивається, а зловмисники використовують дедалі складніші методи, щоб уникнути виявлення.

Зловмисники все частіше здійснюють багатосторонні атаки, причому 86% інцидентів стосуються атак на різних фронтах, таких як кінцеві точки та хмарні ресурси, згідно зі звітом про реагування на інциденти Unit 42 за 2025 рік . Кінцеві точки були найчастішою ціллю цих атак, як видно з таблиці нижче [13].

Таблиця 1.1.

Вектор атак на кінцеві точки

Поверхні атаки	**Відсоток випадків**
Кінцеві точки	72%
Людина	65%
Ідентифікація	63%
Мережа	58%
Електронна пошта	28%
Хмара	27%
Застосунки	21%
SecOps	14%
База даних	1%

Традиційні антивірусні рішення на основі сигнатур часто не справляються з поліморфним шкідливим програмним забезпеченням, безфайловими атаками та

експлойтами нульового дня. З іншого боку, передові рішення для захисту кінцевих точок використовують штучний інтелект (ШІ) та машинне навчання (МН) для проактивного виявлення та пом'якшення цих нових загроз, тим самим забезпечуючи більш динамічний захист.

Багато кібератак спрямовані на викрадення або компрометацію конфіденційних даних, що знаходяться на кінцевих точках або доступні через них. Надійні заходи безпеки кінцевих точок є життєво важливими для запобігання витокам даних, які можуть призвести до значних фінансових втрат, шкоди репутації та юридичних наслідків. Крім того, такі нормативно-правові бази, як GDPR , HIPAA та CCPA, вимагають добре продуманого захисту даних, що робить комплексну безпеку кінцевих точок важливою для дотримання вимог.

Атаки програм-вимагачів у 2024 році призвели до середньої виплати викупу в розмірі 2,73 мільйона доларів, що майже вдвічі більше, ніж сума, сплачена попереднього року. Ці атаки є значною причиною фінансових втрат та операційних збоїв для підприємств, часто зупиняючи діяльність до сплати викупу або відновлення систем [13].

Інциденти безпеки, що впливають на кінцеві точки, можуть порушити бізнес-операції, що робить ефективний захист кінцевих точок важливим для підтримки безперервності та мінімізації простоїв. Згідно з дослідженням Інституту Понемона, 68% організацій зазнали однієї або кількох атак на кінцеві точки, які успішно скомпрометували дані та/або їхню IT-інфраструктуру. Крім того, 68% IT-фахівців повідомили, що частота атак на кінцеві точки зросла порівняно з попереднім роком.

1.3. Підходи до вирішення проблеми захисту кінцевих точок інформаційної системи організацій

Безпека кінцевих точок працює за допомогою багаторівневого підходу, який інтегрує різні технології та методології для захисту пристроїв від початкового компрометування шляхом постійного моніторингу та реагування. Ця комплексна стратегія виходить за рамки традиційного антивірусу, забезпечуючи проактивний

захист, виявлення загроз у режимі реального часу та можливості автоматизованого реагування [13, 14].

Профілактика – це перша лінія захисту в безпеці кінцевих точок, метою якої є блокування загроз до того, як вони зможуть виконатися або завдати шкоди.

Виявлення на основі сигнатур

Традиційний метод виявлення на основі сигнатур ідентифікує відоме шкідливе програмне забезпечення, порівнюючи сигнатури файлів з базою даних раніше виявлених загроз. Хоча він ефективний проти встановлених загроз, він менш ефективний проти нового або поліморфного шкідливого програмного забезпечення.

Евристичний аналіз

Евристичний аналіз досліджує поведінку та характеристики файлів або процесів на наявність підозрілої активності, яка може свідчити про невідоме шкідливе програмне забезпечення. Цей метод може виявляти нові або модифіковані загрози, яким бракує відомої сигнатури.

Машинне навчання та штучний інтелект

Передові рішення для захисту кінцевих точок використовують штучний інтелект та машинне навчання для аналізу величезних обсягів даних та виявлення закономірностей, що вказують на шкідливу активність. Це дозволяє виявляти загрози нульового дня та складні атаки, розуміючи нормальну та аномальну поведінку (рис.1.4).

Рис.1.3. Штучний інтелект та машинне навчання в безпеці кінцевих точок

Контроль додатків

Контроль програм обмежує, які програми можуть запускатися на кінцевій точці, запобігаючи запуску несанкціонованого або потенційно шкідливого програмного забезпечення. Це значно зменшує поверхню атаки.

Керування пристроями

Контроль пристроїв керує та обмежує використання зовнішніх пристроїв, таких як USB-накопичувачі, щоб запобігти витоку даних або зараженню шкідливим програмним забезпеченням.

Виявлення

Виявлення зосереджено на виявленні загроз, які могли обійти початкові запобіжні заходи, забезпечуючи видимість активності кінцевих точок у режимі реального часу.

Поведінковий аналіз

Метод поведінкового аналізу постійно відстежує процеси кінцевих точок та поведінку користувачів на наявність аномалій, позначаючи незвичайні дії, такі як спроби доступу до конфіденційних файлів або зміни системних налаштувань, що може свідчити про компрометацію.

Індикатори компрометації (IoCs -Indicators of Compromise)

IoCs (інтерфейс клієнта) – це цифрові артефакти, знайдені в мережі або операційній системі, які вказують на вторгнення в комп’ютер. Рішення для захисту кінцевих точок сканують ці індикатори, такі як хеші певних файлів, IP-адреси або зміни розділів реєстру, щоб виявити активні загрози.

Інтеграція розвідки загроз

Платформи захисту кінцевих точок (EPP) інтегруються з глобальними потоками інформації про загрози, що дозволяє їм розпізнавати та блокувати нові та нові загрози, щойно їх виявляє ширша спільнота кібербезпеки .

Реагування та усунення наслідків

Після виявлення загрози рішення для безпеки кінцевих точок надають інструменти та можливості для швидкого реагування та усунення наслідків, мінімізації збитків та відновлення безпечного стану кінцевої точки.

Автоматизована відповідь

Багато сучасних рішень можуть автоматично ізолювати скомпрометовані кінцеві точки, поміщати шкідливі файли в карантин або завершувати підозрілі процеси без втручання людини. Це значно скорочує час, необхідний для реагування на загрозу.

Виявлення та реагування на кінцеві точки (EDR)

Рішення EDR надають розширені можливості для безперервного моніторингу, виявлення загроз, розслідування та реагування на них на рівні кінцевих точок. Вони збирають та аналізують дані кінцевих точок, щоб дозволити командам безпеки зрозуміти повний масштаб атаки, проводити судово-медичний аналіз та організовувати заходи з усунення наслідків.

Надаймо типи рішень для безпеки кінцевих точок .

Безпека кінцевих точок охоплює різні рішення, розроблені для захисту кінцевих точок мережі. Кожен тип безпеки кінцевих точок відіграє життєво важливу роль у захисті від шкідливого програмного забезпечення, несанкціонованого доступу та інших кіберзагроз, зокрема:

Антивірус наступного покоління (NGAV). Використовує штучний інтелект та машинне навчання для виявлення, запобігання та видалення як відомих, так і невідомих шкідливих програм із пристроїв.

Виявлення та реагування на кінцеві точки (EDR). Моніторить та збирає дані для виявлення та реагування на складні загрози в режимі реального часу.

Розширене виявлення та реагування (XDR). Інтегрує дані кінцевих точок із мережевою, електронною та хмарною безпекою для комплексної видимості загроз та автоматизованого реагування.

Керування мобільними пристроями (MDM) та захист від мобільних загроз (MTD) : керує, контролює та захищає мобільні пристрої співробітників, одночасно захищаючи їх від загроз, пов'язаних з мобільними пристроями.

Zero Trust Network Access (ZTNA). Перевіряє стан безпеки пристрою перед наданням доступу до мережі, замінюючи традиційні підходи VPN.

Керування станом безпеки хмари (CSPM). Захищає хмарні кінцеві точки та робочі навантаження за допомогою постійного моніторингу відповідності.

Безпека електронної пошти та захист від фішингу. Контролює загрози електронної пошти за допомогою аналізу на основі штучного інтелекту для виявлення складного фішингу та компрометації ділової електронної пошти.

Запобігання втраті даних (DLP) та безпека даних. Запобігає витоку конфіденційних даних з організації, забезпечуючи шифрування та керування правами доступу.

Проблеми безпеки кінцевих точок

Захист кінцевих точок створює унікальні проблеми в сучасному динамічному ландшафті загроз. Поширення пристроїв, складність атак і управління різноманітними середовищами сприяють цим труднощам (Рис.1.5).

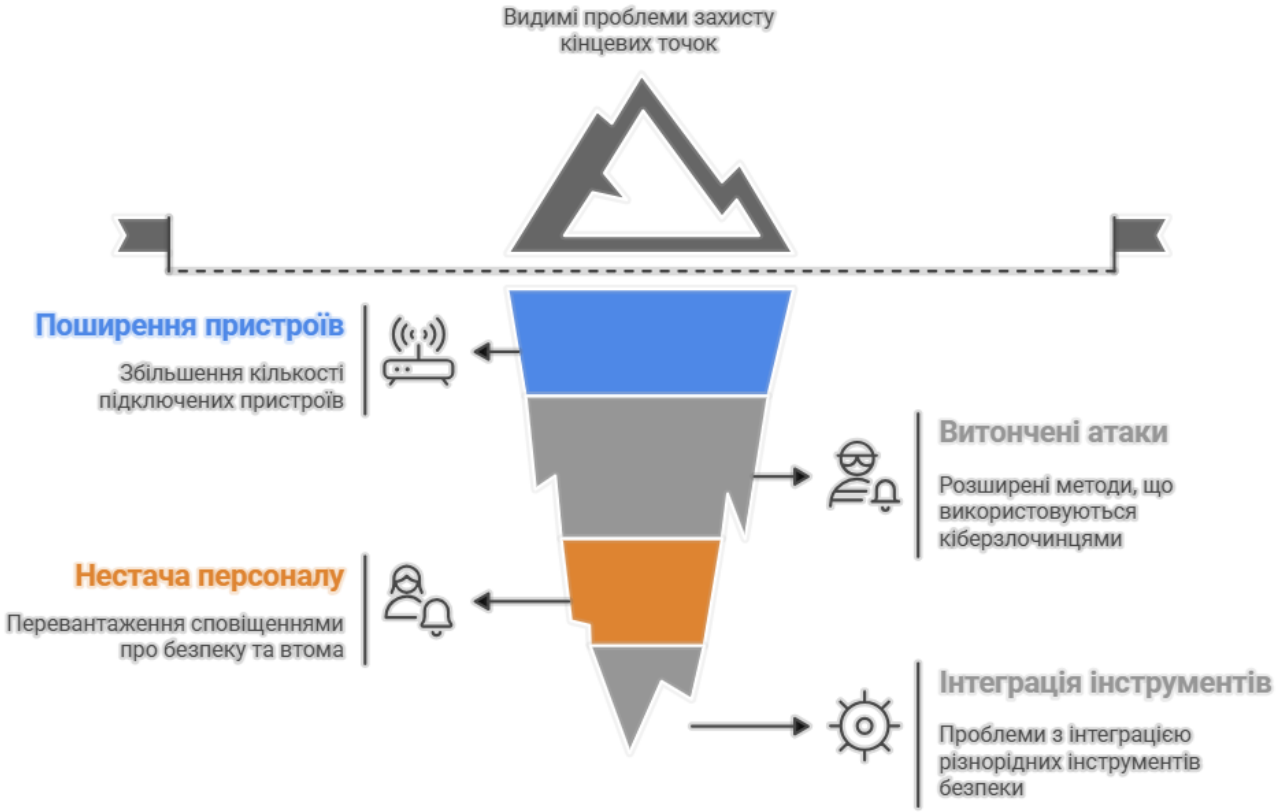

Рис.1.5. Проблеми безпеки кінцевої точки

1. Поширення пристроїв

Широке впровадження персональних пристроїв, віддаленої роботи та політики «принеси свій власний пристрій» (BYOD) призвело до вибухового зростання кількості та різноманітності кінцевих точок, що підключаються до корпоративних мереж. Кожен пристрій — ноутбук, смартфон, планшет, датчик

Інтернету речей — є потенційною точкою входу для зловмисників, значно розширюючи поверхню атаки. Керування безпекою в такій різноманітній та розсіяній екосистемі є складним за своєю суттю.

2. Витончені методи атаки

Кіберзлочинці постійно вдосконалюють свої методи, використовуючи передові методи, такі як безфайлове шкідливе програмне забезпечення, поліморфні віруси, атаки «живе поза землею» та складні фішингові кампанії. Ці методи розроблені для уникнення традиційного виявлення на основі сигнатур та використання вразливостей у поведінці людини або конфігураціях системи. Рішення для безпеки кінцевих точок повинні використовувати поведінкову аналітику, машинне навчання та штучний інтелект для протидії цим передовим загрозам .

3. Нестача персоналу

Команди безпеки часто стикаються з величезною кількістю сповіщень про безпеку від різних інструментів, що призводить до «втоми від сповіщень». Через це справжні загрози можуть залишатися непоміченими серед цього шуму. Водночас існує значна глобальна нестача кваліфікованих фахівців з кібербезпеки, що ускладнює для організацій належне укомплектування персоналом центрів операцій безпеки (SOC) та ефективне управління складними рішеннями для захисту кінцевих точок.

4. Інтеграція різнорідних інструментів

Багато організацій використовують набір різнорідних інструментів безпеки, кожен з яких розроблений для певної функції. Інтеграція цих інструментів у цілісну та ефективну систему безпеки є значним викликом. Відсутність сумісності може створювати сліпі зони, призводити до неефективних робочих процесів та перешкоджати комплексному виявленню загроз і скоординованому реагуванню. Єдиний підхід, який інтегрує різні функції безпеки, має вирішальне значення.

1.4. Аналіз технологій виявлення та реагування на загрози кінцевої точки

XDR (Extended Detection and Response) (це вдосконалена версія виявлення та реагування на кінцеві точки (EDR), яка залучає інші інструменти безпеки та координує все з хмари.

XDR — це платформа, яка складається з низки модулів, що працюють разом. До платформи входять такі компоненти:

Збір даних , який можна адаптувати з EDR.

Пошук загроз , який може бути SIEM, менеджером вразливостей або і тим, і іншим.

Аналіз поведінки користувачів та об'єктів (UEBA) для виключення хибнопозитивних звітів.

Оркестрація, автоматизація та реагування на загрози (SOAR) для зменшення загроз.

Деякі постачальники пропонують ці модулі як окремі продукти, так і в пакеті послуг.

XDR розшифровується як Extended Detection and Response (розширене виявлення та реагування) . Це вдосконалена версія виявлення та реагування на кінцеві точки (EDR), яка залучає інші інструменти безпеки та координує все з хмари.

Згідно з [17] можна виділити лідерів рішень XDR (рис.1.6).

Рис.1.6. Лідери ринку XDR

Palo Alto Cortex XDR — найкраща система XDR від компанії, яка й придумала цей термін.

CrowdStrike Falcon поєднує локальні модулі та SaaS-системи в єдину платформу безпеки.

TrendMicro XDR — хмарна SIEM-система, яка координує роботу з локальними службами безпеки того ж постачальника, включаючи безпеку електронної пошти.

Платформа Cynet XDR. Ця платформа використовує процедури штучного інтелекту та забезпечує високий ступінь автоматизації вирішення загроз у своїх хмарних сервісах.

У таблиці 1.2 надамо результати порівняння архітектури, функціонального фокусу та ринкового позиціонування чотирьох лідерів XDR рішень.

Таблиця 1.2.

Порівняння лідерів XDR рішень

Критерій	**Palo Alto Cortex XDR**	**CrowdStrike Falcon (XDR/Insight)**	**Trend Micro Vision One (XDR)**	**Cynet XDR (360 AutoXDR)**
Архітектурний Фокус	Хмарний, Глибока Інтеграція. Платформа, побудована навколо великих даних.	Хмарно-орієнтований, EDR. Акцент на легкому агентові та швидкості.	Платформа Управління Ризиками Vision One. Орієнтація на гібридні та хмарні робочі навантаження.	Автономний Захист "Все-в-одному". Інтеграція NGAV/EDR/SOAR/MDR.
Ключові Джерела Телеметрії	Endpoint, Network, Cloud, Identity. Додаткові модулі захисту кінцевих точок.	Endpoint, Cloud Workload, Identity. Централізовано через Threat Graph™.	Endpoint, Cloud Workload, Email/Messaging, Network. Широке охоплення гібридного середовища.	Endpoint, Network, User, Deception. Вбудовані модулі захисту.
SOAR та Автоматизація	Cortex XSOAR (Окремий, але тісно інтегрований продукт).	Власні можливості орк. + Широка інтеграція через Marketplace.	Власні автоматизовані робочі процеси та AI Companion.	Вбудовані SOAR-подібні функції (AutoXDR) для повністю автоматизованої інв. та рем..
Managed Detection & Response (MDR)	Доступно як окрема послуга (Cortex XDR Managed Threat Hunting).	Falcon Complete (окремий високопреміальний пакет).	Managed XDR Services (Різні пакети для різних векторів).	Вбудовано та включено 24/7 CyOps (без додаткової вартості).
Цільовий ринок	Великі Корпорації (Enterprise), Користувачі екосистеми PAN.	Великі Корпорації (Enterprise), Організації, що цінують швидкість EDR.	Середні та Великі Корпорації (Mid/Large Enterprise) з гібридними потребами.	Малий та Середній Бізнес (SMB/Mid-Market) з обмеженими ресурсами SOC.

Отже, ринок XDR демонструє значний потенціал, щоб замінити або значно доповнити традиційний ринок SIEM (Security Information and Events Management), особливо у сфері виявлення загроз. XDR, завдяки своїй нативній телеметрії та інтегрованій кореляції, може виявляти складні сучасні загрози, які оминають традиційні системи збору логів.

Незважаючи на це, повне заміщення SIEM не передбачається, оскільки SIEM продовжує підтримувати важливі функції управління логами, забезпечення відповідності (Compliance) та аналізу даних, що не стосуються безпеки.

Ключовий стратегічний тренд полягає у консолідації та нативності. Успіх XDR прямо залежить від його здатності об'єднувати дані та інструменти. Рішення, які пропонують максимально нативний, неінтегрований досвід, мають перевагу в операційній ефективності. Так Cortex XDR, демонструє, що автоматизація швидко стає обов'язковою, а не додатковою функцією XDR. Стратегічні інвестиції повинні бути спрямовані на платформи з глибокою, нативною інтеграцією можливостей SOAR та MDR, оскільки це єдиний шлях до моделі "агентського SOC" та ефективного використання AI у кібербезпеці, що мінімізує операційну складність.

Для дослідження, в наступному розділі розглянемо технологію Cortex XDR.

Висновки до розділу 1

1. В результаті аналізу, визначено основні проблеми захисту кінцевих точок організації.

2. Визначено вектор атак на кінцеві точки, що впливає на кінцеві точки та можуть порушити бізнес-операції організацій.

3. Запропоновано підходи для забезпечення безпека кінцевих точок, що працює за допомогою багаторівневого підходу, що інтегрує різні технології та методології для захисту пристроїв від початкового компрометування шляхом постійного моніторингу та реагування.

4. Визначено, шляхом порівняльного аналізу рішення Cortex-XDR, яке найбільше відповідає запропонованому багатошарового підходу.

2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ ВІД СУЧАСНИХ ЗАГРОЗ

2.1. Архітектура Cortex-XDR

Cortex XDR представляє собою новий стандарт у рішеннях розширеного виявлення та реагування (XDR), яке пропонує комплексні можливості захисту, виявлення та реагування. Аналізуючи дані з кінцевої точки Cortex та різних сторонніх джерел, він ефективно протидіє загрозам та сучасним атакам, які розвиваються, у сфері кібербезпеки. Cortex XDR виходить за рамки традиційної безпеки кінцевих точок та забезпечує повну видимість мережі, кінцевих точок, хмари, сторонніх джерел та джерел ідентифікації.

В свої основі Cortex XDR спирається на розширені основи виявлення та реагування та пропонує передове рішення, орієнтоване на хмарні середовища, яке включає:

– професійне рішення;

– мережеву криміналістику ідентифікації кінцевих точок XDR.

На рис.2.1. представлено високорівневу архітектуру ключових компонентів та інтеграцій Cortex XDR.

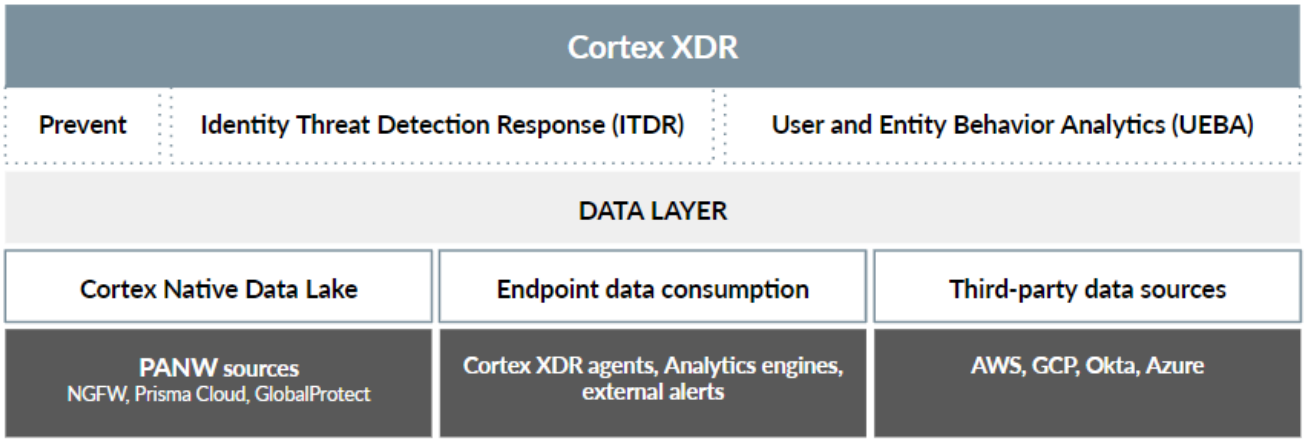

Рис. 2.1. Високорівнева архітектура Cortex XDR

Архітектура включає такі стандартні компоненти:

Cortex XDR надає єдиний інтерфейс, за допомогою якого ви можете досліджувати та сортувати сповіщення, вживати заходів щодо усунення недоліків та визначати політики для виявлення шкідливої активності в майбутньому.

Рівень даних XDR у вашому клієнті Cortex XDR зберігає журнали всіх типів даних.

Аналітика Cortex XDR також може використовувати дані кінцевих точок для автоматичного виявлення загроз після вторгнення та повідомлення про них. Аналітичний механізм може використовувати дані кінцевих точок для генерації сповіщень про аномальну поведінку мережі, таку як активність сканування портів.

Cortex Native Data Lake — це хмарна інфраструктура логування, яка дозволяє централізувати збір і зберігання журналів, згенерованих вашими агентами Cortex XDR, незалежно від місцезнаходження. Агенти Cortex XDR і Cortex XDR пересилають усі журнали до Cortex Native Data Lake. Ви можете переглядати журнали своїх агентів у Cortex XDR . За допомогою програми Log Forwarding ви також можете пересилати журнали до зовнішнього приймача системних журналів.

2.2. Компоненти та функції архітектури Cortex XDR безпеки кінцевої точки

Агент Cortex XDR

Розширені атаки на основі шкідливого програмного забезпечення можуть легко обійти традиційні антивіруси та потенційно завдати шкоди інформаційній системі організації. Захист кінцевої точки інформаційної системи організації полягає у використанні Cortex XDR агентів.

Агент Cortex XDR є основним компонентом рішення для захисту кінцевих точок. Аналізуючи файли до та після їх виконання, він виявляє явні ознаки атак, включаючи шкідливе програмне забезпечення нульового дня, атаки без файлів та атаки на основі скриптів. Адміністратори безпеки можуть швидко розгорнути уніфікований хмарний агент на своїх кінцевих точках, щоб миттєво почати

блокувати розширені атаки та збирати дані для виявлення та реагування на виявлені загрози [3].

Агент Cortex XDR забезпечує повний захист від загроз кінцевих точок, запобігаючи кожному можливому вектору атаки за допомогою використання одного агента шляхом об'єднання кількох взаємодоповнюючих механізмів:

локальний аналіз на основі штучного інтелекту блокує шкідливе програмне забезпечення до його запуску, використовуючи локальну модель машинного навчання, що базується на комплексному наборі даних з глобальних джерел. Модель побудована на унікальному гнучкому фреймворку, що дозволяє постійно оновлюватися, щоб гарантувати постійну доступність найновіших локальних засобів виявлення загроз.

– інтеграція з хмарною службою запобігання шкідливим програмам WildFire забезпечує глибоку перевірку невідомих файлів, а аналітичні дані автоматично передаються між агентами кінцевих точок Palo Alto Networks, брандмауерами наступного покоління та хмарною інфраструктурою.

– захист від поведінкових загроз блокує невідомі загрози, розпізнаючи послідовність подій, пов'язаних зі шкідливим програмним забезпеченням та атаками без файлів. Цей механізм аналізує поведінку кількох пов'язаних процесів, щоб виявити атаки, навіть якщо окремі дії не сигналізують про шкідливу активність.

– захист від програм-вимагачів на основі поведінки захищає ваші кінцеві точки від програм-вимагачів, виявляючи процеси, які намагаються змінити або зашифрувати файли, забезпечуючи ще один рівень захисту від прихованих програм-вимагачів.

– захист збору облікових даних запобігає доступу таких інструментів, як Mimikatz, до системних паролів, гарантуючи, що зловмисники та зловмисні інсайдери не зможуть зловживати обліковими даними або розширювати привілеї.

Використання агента Cortex XDR дозволяє блокування експлойтів за допомогою техніки для раннього припинення атак. Зловмисники часто використовують вразливості систем і програм, щоб отримати контроль над

кінцевими точками та встановити шкідливе програмне забезпечення. Щоб випереджати постійно розвиваються експлойти, агент Cortex XDR ідентифікує техніки та методи експлойтів, а не просто виявляє експлойти за допомогою сигнатур. Ідентифікація на коженому кроці експлойта, порушує життєвий цикл атаки та робить загрози неефективними.

Агенти Cortex XDR запобігають експлойтам кількома методами:

– захист перед експлойтами блокує методи розвідки та профілювання вразливостей до того, як зловмисники запустять експлойти, ефективно запобігаючи атакам.

– запобігання експлойтам на основі технік запобігає відомим експлойтам та експлойтам нульового дня без будь-яких попередніх знань про загрози, блокуючи такі методи експлойтів, як переповнення буфера або захоплення DLL.

– запобігання експлойтам ядра блокує експлойти, які використовують вразливості в ядрі операційної системи для створення процесів з підвищеними привілеями системного рівня. Агент Cortex XDR також перешкоджає методам ін'єкцій, що використовуються для завантаження та запуску шкідливого коду з ядра.

– захист від експлойтів десеріалізації Java блокує експлойти, такі як Log4Shell та SpringShell, виявляючи атаки, такі як модифікація атрибутів сервера зі шкідливого джерела.

Використання агента Cortex XDR дозволяє максимізувати точність поведінкового захисту від загроз за допомогою створення правил.

Поведінковий захист від загроз забезпечує точний та своєчасний захист, тісно поєднуючи дослідження загроз, видимість активних загроз у мережах клієнтів та телеметрію тихих правил для забезпечення ефективної безпеки — і все це зі швидкими глобальними оновленнями для всіх агентів. Кожне нове правило запускається в тихому режимі, що дозволяє фахівцям Cortex XDR швидко впроваджувати нові правила з надзвичайно низьким рівнем хибних спрацьовувань (рис. 2.2).

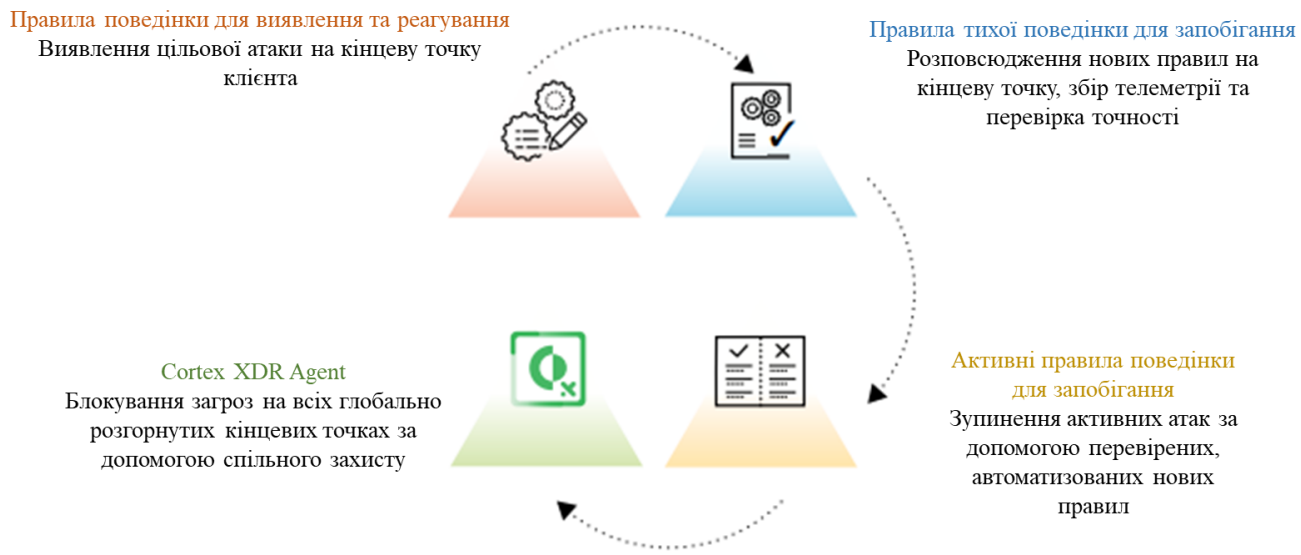

Рис.2.2. Впровадження правила захисту від поведінкових загроз без попередження перетворюються на активні правила

Виявлення та реагування на загрози ідентифікації (ITDR)

Хоча багато організацій покладаються на традиційні підходи до безпеки для захисту від цих загроз, для виявлення загроз ідентичності та зловмисних інсайдерів. Ці атаки часто відбуваються в мережі організації, що ускладнює їх виявлення за допомогою інструментів безпеки на основі контроля периметра.

Більше того, виявлення загроз, пов'язаних з ідентичністю, по суті, полягає у розрізненні підозрілої, але нешкідливої активності та справді зловмисної активності, що в більшості випадків вимагає експертно розроблених алгоритмів навчання для точного виявлення потенційних загроз та реагування на них.

Нарешті, загрози ідентичності та зловмисні інсайдерські атаки часто здійснюються протягом тривалого періоду, що ускладнює їх виявлення за допомогою традиційних механізмів виявлення.

Регулярні оцінки ризиків є важливим компонентом належного ведення кіберзахисту. Регулярні оцінки можуть допомогти забезпечити відповідність рівня ризиків організації її бізнес-цілям. У міру розвитку організації її профіль ризику може змінюватися, оскільки додаються нові бізнес-підрозділи, програми та

системи. Регулярні оцінки можуть допомогти виявити зміни у вразливості до ризиків та дозволити організаціям відповідно скоригувати свій рівень безпеки.

Крім того, оцінка ризиків з часом може допомогти організаціям встигати за змінами в ландшафті загроз. Тактики, методи та процедури, що використовуються зловмисниками, постійно розвиваються, і організації повинні мати можливість адаптувати свою безпеку, щоб випереджати нові загрози. Регулярна оцінка ризиків може допомогти виявити нові та перспективні загрози та дозволити організаціям впроваджувати нові заходи безпеки для захисту від них [4].

Щоб ефективно керувати ризиками, пов'язаними із загрозами для особистих даних та зловмисними інсайдерами, організації повинні мати чітке уявлення про потенційні ризики та приймати обґрунтовані рішення щодо їх пом'якшення.

Це вимагає повного розуміння ризикової ситуації в організації та здатності моніторити та аналізувати поведінку користувачів для виявлення потенційних загроз.

Застосовуючи комплексний підхід до безпеки, організації можуть значно зменшити свою вразливість до загроз для особистих даних та зловмисних інсайдерів, а також краще захистити свої активи та репутацію [4].

Компонент виявлення та реагування на загрози Cortex Identity (ITDR) – це сучасний модуль, призначений для забезпечення проактивного захисту від векторів загроз, пов’язаних з ідентифікацією, таких як скомпрометовані облікові записи та зловмисні інсайдери. Використовуючи можливості штучного інтелекту та автоматизації, модуль надає розширені можливості виявлення, які дозволяють організаціям швидко виявляти, розслідувати та зрештою реагувати на загрози ідентифікації (Рис.2.3).

Новий модуль такі функції:

– швидке приймання рішення завдяки розширеному уявленню про ризики організації.

– отримування аналітичної інформацію про актив, щоб легко виявляти приховані загрози.

– автоматизація та налаштовування безперервного аналізу діяльності користувачів та хостів.

– швидке сортування та дослідження сповіщенн за допомогою точної інформації профілю.

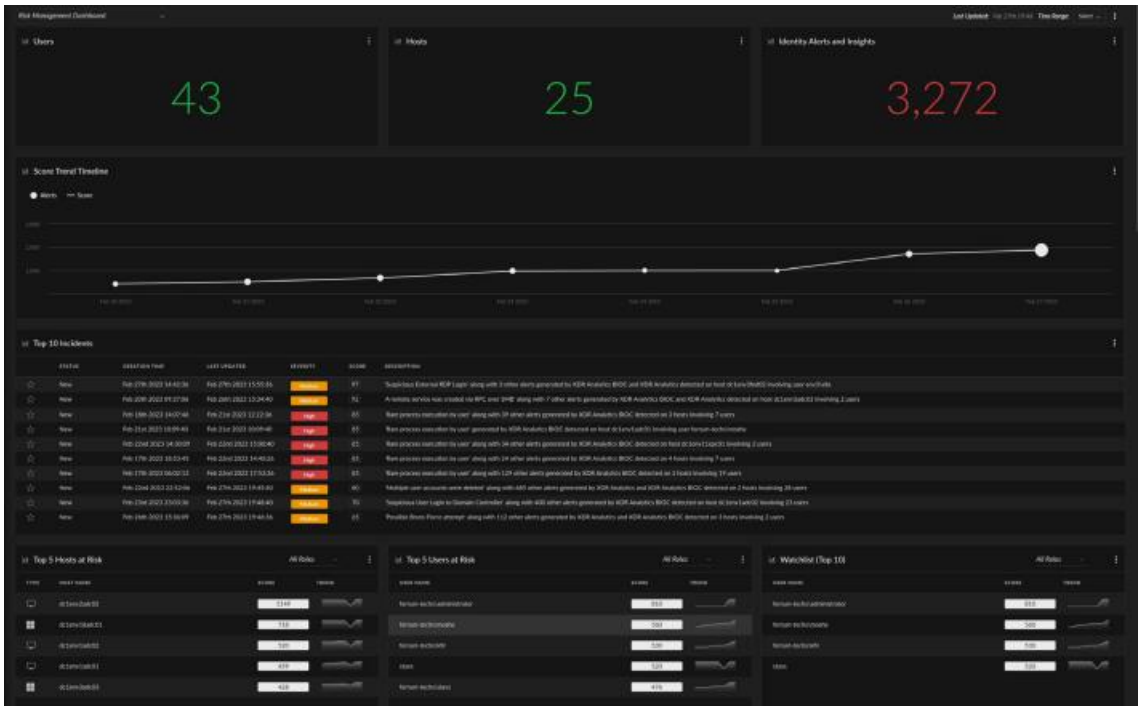

Рис.2.3. Інформаційна панель ITDR, що надає статистику ризиків та тенденції [5]

Атаки на основі ідентифікації

Атаки на основі ідентифікаційних даних створюють унікальні проблеми, які вимагають спеціалізованих підходів та виділення ресурсів. Організації повинні подолати технічні, операційні та організаційні перешкоди для впровадження ефективного захисту від загроз ідентифікаційним даним [6].

Поширені загрози, пов'язані з ідентифікацією

Атаки з використанням перевантаження облікових даних. Використання повторно використаних паролів у кількох сервісах шляхом тестування великих обсягів комбінацій імені користувача та пароля на цільових системах. Зловмисники використовують бази даних облікових даних з попередніх порушень, щоб отримати несанкціонований доступ до ресурсів організації [6].

Фішингові атаки. Спрямовані на користувачів за допомогою складних методів соціальної інженерії, призначених для крадіжки облікових даних або обману користувачів для встановлення шкідливого програмного забезпечення. Сучасні фішингові атаки часто видають себе за довірені служби, використовують домени, що виглядають легітимними, та включають персоналізований контент для підвищення рівня успішності [6].

Ескалація привілеїв. Зловмисники, які отримали початковий доступ, намагаються отримати дозволи вищого рівня в цільових системах. Успішна ескалація привілеїв дозволяє зловмисникам отримати доступ до конфіденційних даних, змінювати конфігурації системи та встановлювати механізми постійного доступу [6].

Захоплення облікового запису. Відбувається, коли зловмисники отримують повний контроль над законними обліковими записами користувачів за допомогою різних засобів, включаючи крадіжку облікових даних, перехоплення сеансу або використання вразливостей автентифікації. Скомпрометовані облікові записи надають зловмисникам легітимні шляхи доступу, які обходять багато традиційних засобів контролю безпеки [6].

Зловмисна діяльність інсайдерів. Охоплює низку загроз з боку нинішніх або колишніх співробітників, які зловживають своїми дозволеними правами доступу. Внутрішні загрози можуть включати крадіжку даних, саботаж, шахрайство або несанкціоноване розголошення конфіденційної інформації [6].

Поєднуючи розширені можливості виявлення загроз, як частину аналітики ідентифікації з модулем ITDR, який захищає загрози ідентифікації на пізніших етапах життєвого циклу атаки, рішення Cortex забезпечує захист від загроз, пов'язаних з ідентифікацією, які були згадані вище, протягом усього життєвого циклу атаки. Такий інтегрований підхід гарантує, що потенційні загрози виявляються та пом'якшуються якомога раніше, зменшуючи ризик витоків даних та інших інцидентів безпеки [6].

Модуль надає такі можливості:

Поєднання можливостей виявлення та реагування на загрози ідентифікації (ITDR) з аналітичними та ризик-орієнтованими виявленнями, а також аналітикою поведінки користувачів і об'єктів (UEBA).

Зменшити різнорідний технологічний стек та знизите витрати.

Замінити існуючі можливості UEBA.

Замінити деякі можливості постачальників ITDR.

Ключові компоненти ITDR

Рішення ITDR побудовані на кількох основних компонентах, які разом забезпечують їхню здатність моніторити, виявляти та реагувати на загрози, пов'язані з ідентифікацією. Ці компоненти працюють разом, щоб забезпечити комплексний захист інфраструктури ідентифікації організації.

Безперервна видимість та моніторинг ідентифікації

Ефективне ITDR починається з повсюдного контролю в режимі реального часу всіх дій, пов'язаних з ідентифікацією, в усьому IT-ландшафті — локально, у хмарі та в гібридних середовищах. Це включає моніторинг спроб автентифікації, запитів на доступ, змін привілеїв, модифікацій каталогів (наприклад, Active Directory, Azure AD) та поведінки користувачів у різних програмах та системах. Це охоплює як людські, так і нелюдські ідентичності, такі як облікові записи служб та токени OAuth, гарантуючи, що жодна ідентичність не залишиться непоміченою.

Поведінкова аналітика та виявлення аномалій

Поведінкова аналітика, наріжний камінь ITDR, встановлює базову лінію нормальної поведінки ідентифікації. Вона використовує машинне навчання (ML) та штучний інтелект (AI) для аналізу закономірностей у активності користувачів, таких як час входу в систему, місцезнаходження, використання пристроїв та доступ до ресурсів.

Будь-яке суттєве відхилення від цього встановленого базового рівня, як-от незвичайний вхід з нової країни, спроба доступу до висококонфіденційних даних поза робочим часом або швидке підвищення привілеїв, запускає сповіщення як потенційну аномалію. Ця можливість має вирішальне значення для виявлення складних атак, які в іншому випадку могли б здаватися легітимними.

Інтеграція розвідки загроз

Рішення ITDR інтегруються із зовнішніми та внутрішніми потоками інформації про загрози. Це включає інформацію про відомі методи атак, індикатори компрометації (IOC), пов'язані з крадіжкою особистих даних, та нові загрози, пов'язані з ідентифікацією. Зіставляючи спостережувану активність, пов'язану з ідентифікацією, з даними про загрози, ITDR може виявляти відомі шкідливі моделі та визначати пріоритети загроз, що дозволяє швидше та більш обґрунтовано реагувати.

Управління станом безпеки ідентифікаційних даних

Окрім простого виявлення загроз, рішення ITDR часто включають можливості для оцінки та управління станом безпеки самої інфраструктури ідентифікації. Це включає постійне виявлення неправильних конфігурацій, надмірних дозволів, тіньових IT-ідентифікаторів та інших вразливостей, які можуть використовувати зловмисники. ISPM допомагає проактивно посилювати системи ідентифікації, зменшуючи загальну поверхню атаки та мінімізуючи ймовірність успішних атак на основі ідентифікації.

Можливості автоматизованого та ручного реагування

Виявивши загрозу, ITDR забезпечує швидке реагування. Це може включати автоматизовані дії, такі як:

– застосування посиленої автентифікації (наприклад, вимога багатофакторної автентифікації) для підозрілих входів.

– тимчасове блокування або деактивація скомпрометованих облікових записів.

– скасування підозрілих сесій або токенів доступу.

– ізоляція уражених систем або користувачів.

– автоматичне скидання паролів.

Окрім автоматизації, ITDR надає командам безпеки необхідний контекст та інструменти для ручного розслідування та усунення недоліків, такі як детальні журнали, дані експертизи та керовані робочі процеси для стримування та усунення складних загроз.

Інтеграція з існуючими екосистемами безпеки

Для максимальної ефективності рішення ITDR безперешкодно інтегруються з ширшим стеком безпеки організації. Це включає передачу високоточних сповіщень про ідентифікацію до SIEM для співвіднесення з іншими даними безпеки, обмін контекстом з платформами XDR для комплексного розслідування загроз, а також роботу з системами IAM та PAM для забезпечення дотримання та оновлення політик доступу на основі інформації про загрози в режимі реального часу. Така сумісність гарантує, що безпека ідентифікації є цілісною частиною загальної стратегії кібербезпеки.

User Entity Behavior Analytics (UEBA)

Аналіз поведінки користувачів та сутностей (UEBA) – це рішення з кібербезпеки, що постійно розвивається та використовує розширену аналітику для виявлення аномалій поведінки користувачів та сутностей у мережі організації. На відміну від традиційних заходів безпеки, UEBA зосереджується на закономірностях та нюансах діяльності користувачів, використовуючи цю інформацію для виявлення потенційних загроз безпеці[7].

UEBA виникла у відповідь на зростаючу складність кіберзагроз, особливо тих, що стосуються інсайдерських атак та передових постійних загроз (APT). UEBA еволюціонувала від простого виявлення аномалій до машинного навчання, штучного інтелекту та аналітики великих даних, пропонуючи більш динамічний та прогнозний підхід до кібербезпеки.

Системи UEBA збирають комплексні дані, включаючи активність користувачів, мережевий трафік та журнали доступу. Ці дані складають основу аналізу UEBA, враховуючи складні алгоритми, які ретельно вивчають кожен аспект поведінки користувачів у мережі.

Суть функціональності UEBA полягає в його здатності встановлювати базовий рівень «нормальної» поведінки для кожного користувача та об’єкта. Потім модуль постійно порівнює поточну активність з цим базовим рівнем, позначаючи аномалії, які можуть свідчити про потенційні загрози безпеці, такі як витік даних, внутрішні загрози або скомпрометовані облікові записи.

UEBA значно покращує виявлення складних і малопомітних кіберзагроз, особливо тих, які обходять традиційні заходи безпеки. Його підхід до поведінкового аналізу особливо практичний проти внутрішніх загроз і аварійних атак (APT), що робить його дедалі важливішим для бізнесу та пропонує кілька ключових функцій і переваг:

Виявлення внутрішніх загроз. UEBA особливо ефективний у виявленні зловмисних або недбалих дій інсайдерів. Оскільки ці користувачі мають законний доступ до систем, їхні шкідливі дії може бути складніше виявити за допомогою звичайних інструментів безпеки.

Поведінкове профілювання та оцінка ризиків. Інструменти UEBA часто включають механізми поведінкового профілювання та оцінки ризиків. Ці функції допомагають пріоритезувати сповіщення безпеки, дозволяючи командам безпеки зосередитися на найважливіших проблемах.

Вимоги до відповідності та нормативні вимоги. Багато галузей мають суворі вимоги до захисту даних та конфіденційності. UEBA допомагає виконати ці вимоги, надаючи детальну аналітику поведінки користувачів та забезпечуючи швидке виявлення та усунення аномальної діяльності.

Розширене виявлення загроз. Системи UEBA використовують розширену аналітику для виявлення аномальної поведінки або аномалій у діяльності користувачів. Це має вирішальне значення для виявлення складних кіберзагроз, які традиційні заходи безпеки можуть пропустити, таких як внутрішні загрози, скомпрометовані облікові записи або розширені постійні загрози (APT).

Покращений рівень безпеки. Інтегруючи UEBA у свою стратегію безпеки, компанії можуть покращити свій рівень безпеки. UEBA забезпечує глибше та детальніше уявлення про діяльність користувачів, що допомагає ефективніше виявляти та зменшувати ризики.

Запобігання втраті даних. UEBA може допомогти запобігти витокам та втратам даних, відстежуючи поведінку користувачів. Він може виявляти незвичайні моделі доступу або передачі даних, які можуть свідчити про витік даних або спробу крадіжки.

Ефективне реагування на інциденти. У разі інциденту безпеки інструменти UEBA можуть надати детальний контекст та записи про активність користувачів. Ця інформація є критично важливою для швидкого та ефективного реагування на інциденти, допомагаючи мінімізувати вплив порушень безпеки.

Автоматизоване реагування та виправлення. Розширені рішення UEBA можуть інтегруватися з іншими інструментами безпеки для автоматизації реагування на виявлені загрози. Це скорочує час і зусилля, необхідні для виправлення, і підвищує загальну ефективність SOC.

Довгостроковий аналіз тенденцій та криміналістика. Інструменти UEBA можуть зберігати та аналізувати довгострокові дані, що є цінним для аналізу тенденцій та криміналістичних розслідувань після інциденту безпеки.

Адаптація до мінливого ландшафту загроз. Системи UEBA можуть адаптуватися до розвитку кіберзагроз, постійно навчаючись на нових моделях даних. Це допомагає компаніям випереджати нові загрози.

Розглянемо приклади застосування UEBA, таких як виявлення внутрішніх загро, ідентифікація скомпрометованого облікового запису, виявлення аномалій, шахрайство тощо.

Рішення UEBA можуть виявляти потенційно зловмисні дії інсайдерів, такі як доступ співробітників до конфіденційних даних або їх завантаження в незвичний час або в незвично великих обсягах, що може свідчити про крадіжку даних [7, 8].

Якщо поведінка користувача раптово змінюється — наприклад, він отримує доступ до різних систем або даних, які зазвичай не використовує, особливо в незвичний час — це може свідчити про те, що його обліковий запис було скомпрометовано [7, 8].

Інструменти UEBA можуть виявляти аномалії в IT-системах та мережах, такі як незвичайні місця або час входу в систему, неочікувані потоки даних або сплески в доступі до даних чи їх використанні [7, 8].

У фінансовій сфері або сфері електронної комерції UEBA може бути використана для виявлення шахрайської діяльності, такої як незвичайні моделі транзакцій, що вказує на потенційне шахрайство або фінансові злочини [7, 8].

У сфері охорони здоров’я UEBA може допомогти забезпечити дотримання законів про конфіденційність, контролюючи доступ до медичних записів пацієнтів та виявляючи, чи отримує персонал доступ до записів без законної потреби [7, 8].

UEBA може бути важливим інструментом для виявлення APT, коли зловмисники проникають у системи та залишаються непоміченими протягом тривалого часу, оскільки він може виявляти ледь помітні, довгострокові зміни в поведінці [7, 8].

Запобігання витоку даних: моніторинг доступу до даних та їх переміщення дозволяє UEBA виявляти потенційні спроби витоку даних, такі як копіювання великих обсягів даних на зовнішні накопичувачі або завантаження їх у хмарні сервіси [7, 8].

UEBA часто працює з системами безпеки, такими як SIEM (системи управління інформацією та подіями безпеки) , покращуючи загальні можливості виявлення загроз та реагування на них [7, 8].

Системи UEBA можуть автоматизувати оповіщення служб безпеки про підозрілу активність, а іноді інтегруватися із системами реагування для вжиття негайних заходів, таких як блокування користувача або зміна контролю доступу [7, 8].

Інтеграція з XDR. Можливості UEBA тепер інтегруються з XDR (Extended Detection and Response) – вдосконаленим інструментом виявлення загроз, що розвинувся на основі EDR (Endpoint Detection and Response). XDR являє собою значний прогрес, пропонуючи глибше розуміння та ширший охоплення, ніж традиційні продукти SIEM. Він покращує видимість загроз у різних джерелах даних, таких як мережі, кінцеві точки та хмари [7].

XDR об'єднує функціональність EDR, UEBA, NTA та антивіруса наступного покоління в єдине рішення, забезпечуючи комплексну видимість та складну поведінкову аналітику. Ця інтеграція не лише прискорює процеси розслідування, але й значно підвищує ефективність команд безпеки завдяки автоматизації, забезпечуючи надійніший захист від загроз безпеці в усій інфраструктурі [7].

Проведемо порівняння UEBA та NTA, для розуміння доцільності включення цього рішення для виявлення загроз кінцевої точки організації (табл.2.1) [7, 8].

Таблиця 2.1.

Порівняння UEBA та NTA

UEBA	NTA
Переваги	
1. Дозволяє застосовувати аналітику та науку про дані для реєстрації даних, щоб виявляти загрози безпеці, які в іншому випадку могли б залишатися прихованими у величезних репозиторіях. 2. Дозволяє відстежувати та контролювати всіх користувачів та інші організації, що користуються мережею. 3. Зменшує кількість подій безпеки та значно підвищує операційну ефективність.	1. Дозволяє компаніям бачити всі події, а не лише зареєстровані, по всій своїй мережі, включаючи кожен аспект діяльності та методів зловмисника, від ранніх до пізніх стадій атаки. 2. Дозволяє компаніям створювати профілі мережевих пристроїв та облікових записів користувачів. 3. Розгортається з відносною легкістю.
Недоліки	
1. Пропонує вузьке уявлення про поведінку та події мережі, оскільки журнали UEBA увімкнено лише в невеликій частині мережі компанії. 2. Не може точно визначити конкретні атаки на безпеку. 3. Покладається на журнали третіх сторін для моніторингу, виявлення та аналізу потенційних загроз і призначення оцінок ризику –	1. Окуповується за короткий час, але все одно вимагає досвіду команди безпеки, щоб знати, на які типи проблем безпеки звертати увагу та як їх виявляти. 2. Пропонує покриття, яке хоч і широке, але неглибоке. 3. Не може відстежувати місцеві події.

UEBA	NTA
якщо/коли реєстратор третьої сторони виходить з ладу, UEBA не зможе виконувати свою роботу. 4. Повільне розгортання – багато постачальників стверджують, що UEBA можна розгорнути за кілька днів, але клієнти Gartner повідомляють, що це часто займає 3–6 місяців у простих випадках використання та до 18 місяців у складних. 5. Вимагає багато міжфункціональних погоджень та налаштування системи.	

Рішення UEBA та NTA використовують машинне навчання та аналітику для виявлення підозрілої або шкідливої активності майже в режимі реального часу. У той час як системи UEBA аналізують поведінку користувачів, системи NTA відстежують весь мережевий трафік та записи потоків, щоб виявити потенційні атаки. Обидва рішення надають аналітичну інформацію для зменшення загроз, перш ніж вони завдадуть шкоди.

2.3. Ключові характеристики захисту кінцевої точки

Ключові характеристики захисту кінцевої точки на базі Cortex XDR забезпечують:

Повну видимість. На відміну від традиційних рішень, Cortex XDR забезпечує повну видимість, не обмежуючись кінцевою точкою. Вона охоплює мережу, хмару, сторонні джерела та джерела ідентифікації, пропонуючи цілісний підхід до виявлення загроз.

Скороченний часу виявлення та реагування. Cortex XDR значно скорочує середній час виявлення (MTTD) та середній час реагування (MTTR), покращуючи загальні можливості реагування на інциденти.

Виявлення загроз, орієнтоване на ідентифікацію. Готове виявлення загроз, орієнтоване на ідентифікацію, охоплює тактики, методи та процедури початкового доступу (TTP). Доступні додаткові доповнення для розширеної аналітики виявлення загроз на основі ідентифікації, наприклад, внутрішніх загроз.

Автоматизація для підвищення ефективності. Cortex XDR реалізує спрощені дії автоматизації, оптимізуючи процеси розслідування для аналітиків безпеки та роблячи їх ефективнішими у реагуванні на загрози.

Доведена ефективність за оцінками MITRE. Cortex XDR може похвалитися вражаючими результатами оцінювання MITRE ATT&CK Round 4, досягнувши 97% рівня виявлення.

Виявлення на основі науки про дані. Використовуючи алгоритми машинного навчання, Cortex XDR забезпечує справжні виявлення на основі науки про дані, мінімізуючи шум та підвищуючи ефективність, особливо загроз, які важко виявляються.

Масштабованість на основі хмарних технологій. Cortex XDR розроблено для масштабування відповідно до потреб підприємства, використовуючи можливості хмари без вимог до локальних рішень.

Уніфікований агент кінцевої точки. Уніфікований агент кінцевої точки включає методи та засоби, що забезпечує антивірус наступного покоління (NGAV), виявлення та реагування на кінцеві точки (EDR), брандмауер хоста, керування пристроями, шифрування диска та додаткові доповнення для збору даних та аналізу даних хоста.

Використання згаданих характеристик, надає рішенню Cortex XDR ефективно вирішувати проблем безпеки, з якими стикаються організації сьогодні:

Всебічне застосування. Cortex XDR руйнує ізоляцію рішень безпеки, надаючи інтегроване рішення, що охоплює агента кінцевої точки, аналітику виявлення

загроз, автоматизацію, виявлення загроз ідентифікації та можливості цифрової криміналістики.

Безперервна інтеграція даних про загрози. Cortex XDR вирішує проблему застарілої та фрагментованої інформації про загрози, постійно інтегруючи дослідження загроз Unit 42 та Cortex, надаючи клієнтам актуальну аналітику.

Балансування виявлення загроз. Cortex XDR зменшує ризик пропуску виявлення як відомих, так і невідомих загроз, що підтверджується стороннім тестуванням. Він підтримує низьке співвідношення сигнал/шум, зменшуючи кількість хибнопозитивних результатів та позбавляючи аналітиків з безпеки необхідності полювати за хибними прапорцями.

Збільшення рентабельності інвестицій. Cortex XDR пропонує підвищену рентабельність інвестицій порівняно з вузькоспеціалізованими рішеннями для виявлення та реагування на загрози кінцеві точки (EDR) та рішеннями для управління інформацією та подіями безпеки (SIEM). Воно забезпечує підвищену ефективність виявлення, мінімізуючи при цьому навантаження на клієнтів.

Виявлення загроз на основі ідентифікації. Cortex XDR виділяється тим, що вирішує зростаючу проблему загроз на основі ідентифікації, охоплюючи внутрішні загрози, горизонтальне переміщення та аномальну поведінку користувачів і об'єктів за допомогою модуля виявлення та реагування на загрози ідентифікації (ITDR).

Отримані переваги виявлення загроз, є результатом можливостей збору та обробки даних з різних джерел до рішення Cortex XDR, які є основою для застосування описаних технологій, що в свою чергу підкреслює ефективність обраного рішення для виявлення сучасних загроз.

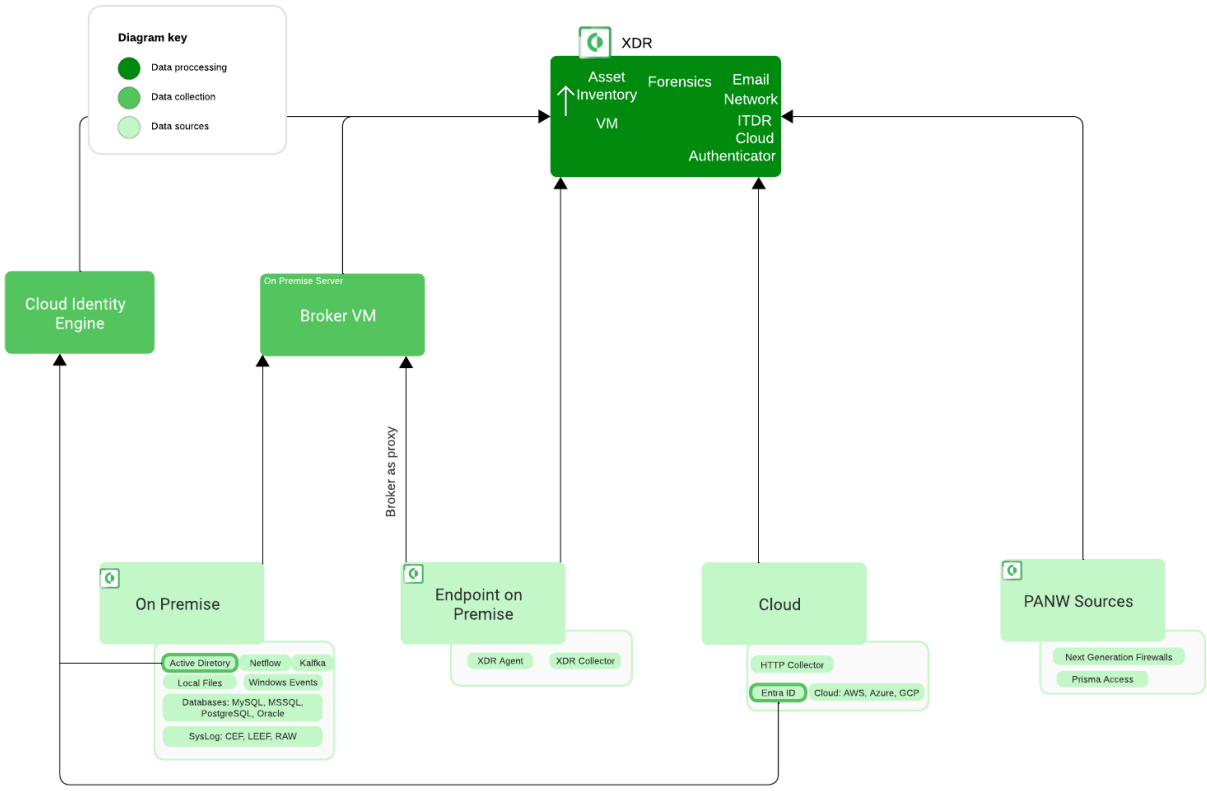

Рис. 2.4. Збір та обробка даних з різних джерел до Cortex XDR

Джерела даних збираються внизу ланцюжка та обробляються локальними серверами та механізмами. Дані спочатку обробляються та аналізуються за допомогою XQL, що дозволяє виконувати запити та аналіз. Оброблені дані інтегруються з віртуальними машинами, аналітикою на основі криміналістики та штучного інтелекту, моделями машинного навчання. Це дозволяє Cortex XDR автоматизувати сповіщення та безпеку.

Висновки 2 розділу

1. Визначено архітектуру Cortex XDR, яка дозволяє впровадити методи та захисту кінцеих точок від сучасних загроз.

2. Визначено основні компоненти технології Cortex XDR та їх функції, в основі якої є агент Cortex XDR, що забезпечує повний захист від загроз кінцевих точок, технологія ITDR яка призначена для виявлення загроз, пов'язаних з ідентичністю та призначений для забезпечення проактивного захисту від векторів

загроз, пов’язаних з ідентифікацією, технологія UEBA, як рішення з кібербезпеки, що постійно розвивається та використовує розширену аналітику для виявлення аномалій поведінки користувачів та сутностей у мережі організації.

3. Визначено ключові характеристики Cortex XDR, які забезпечують повну видимість, швидке виявлення та реагування на сучасні загрози кінцевої точки інформаційної системи організації.

3 ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВОЇ ТОЧКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

3.1. Технологія захисту кінцевої точки на прикладі Cortex-XDR

Технологія Cortex XDR вирішу багато питань з кібербезпеки для захисту кінцевої точки організації. Основні можливості технології представлено на рисунку 3.1 [10].

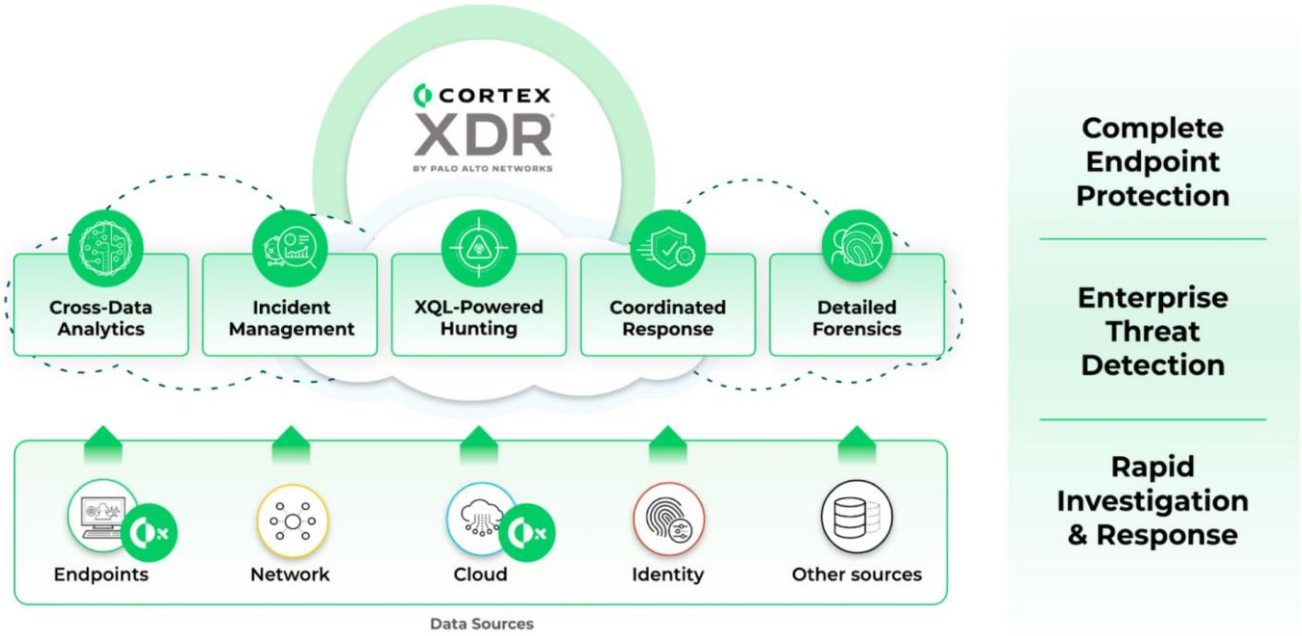

Рис.3.1. Можливості технології Cortex XDR

Cortex XDR руйнує ізольовані рішення безпеки, пропонуючи агента кінцевих точок, механізм аналітики виявлення загроз, автоматизацію для кінцевих точок та сповіщень, виявлення загроз ідентифікації, можливості криміналістики та підтримку отримання даних третіх сторін.

Відсутність актуальної та інтегрованої аналітики загроз у технологіях безпеки є значною проблемою, з якою стикається більшість організацій. Cortex XDR постійно інтегрує кураторські дослідження загроз Unit 42® та Cortex, позбавляючи клієнтів надзвичайного навантаження, пов'язаного з аналітикою загроз та їх виявленням.

Cortex XDR вирішує проблему ігнорування як відомих, так і невідомих загроз, що доведено сторонніми тестами, зберігаючи при цьому низьке співвідношення сигнал/шум, щоб зменшити кількість хибнопозитивних результатів та позбавити аналітиків безпеки необхідності полювати за хибними прапорцями.

Загальновизнано, що розрізнені та погано інтегровані рішення є дорогими та не знижують ризики до прийнятного рівня. Cortex XDR забезпечує вищу рентабельність інвестицій (ROI) порівняно з вузькоспеціалізованими рішеннями EDR та роздутими рішеннями SIEM, які створюють більше навантаження на клієнта з управління ними та забезпечують меншу ефективність виявлення.

Рішення, орієнтовані на EDR та не орієнтовані на XDR, не мають виявлення загроз на основі ідентифікації, що все більше турбує організації. Cortex XDR вирішує внутрішні загрози, горизонтальне переміщення, аномальну поведінку користувачів та об'єктів за допомогою модуля виявлення та реагування на загрози ідентифікації (ITDR).

Основні складові технології Cortex XDR, які входять до захисту кінцевої точки організації, представлено у таблиці 3.1.

Таблиця 3.1.

Складові технології Cortex XDR

	XDR Запобігання	**XDR Pro для кінцевої точки**
Антивірус наступного покоління. Блокує шкідливе програмне забезпечення, програми-вимагачі, експлойти та безфайлові атаки.	+	+
Захист кінцевих точок Захист кінцевих точок за допомогою контролю пристроїв, брандмауера та шифрування диска	+	+
Виявлення та реагування Точне визначення атак за допомогою аналітики на основі		+

штучного інтелекту та координація реагування		
Кероване виявлення та реагування. Дозволяє експертам Unit 42 працювати для вас цілодобово, щоб виявляти загрози та реагувати на них.		+
Кероване полювання на загрози. Дозволяє експертам Unit 42 працювати цілодобово, щоб виявляти складні загрози.		+
Аналітика хостів. Знаходить вразливості та охоплюйте кінцеві точки, щоб усунути загрози		+
Швидке розслідування інцидентів за допомогою вичерпних цифрових доказів		+
Події безпеки третіх сторін Надсилання подій безпеки з інших джерел даних		+
Інтеграції Рішення для аналізу загроз, Slack, надсилання системного журналу	+	+
Аналітика безпеки. Застосування машинного навчання та виявлення UEBA до даних безпеки.		+
Виявлення загроз ідентифікації та реагування на них (модуль ITDR) Виявлення важковиявлюваних загроз, таких як інсайдери, переміщення даних, компрометація облікових даних		+
Розширені дані пошуку загроз (модуль XTHD) Збирають розширені дані на кінцевій точці для підтримки операцій глибокого пошуку загроз у середовищі.		+

Відомо, що кібератаки спрямовані на кінцеві точки, щоб завдати шкоди, викрасти інформацію або досягти інших цілей, пов'язаних з отриманням контролю над комп'ютерними системами. Зловмисники здійснюють кібератаки, або змушуючи користувача ненавмисно запускати шкідливий виконуваний файл, відомий як шкідливе програмне забезпечення, або використовуючи слабкість у легітимному виконуваному файлі для запуску шкідливого коду за лаштунками без відома користувача.

Один із способів запобігання цим атакам — ідентифікувати файли, динамічно підключані бібліотеки (DLL) та інші фрагменти коду, щоб визначити, чи є вони шкідливими, і, якщо так, запобігти виконанню цих компонентів, спочатку зіставивши кожен потенційно небезпечний модуль коду зі списком конкретних відомих сигнатур загроз. Слабкістю цього є те, що антивірусні рішення на основі сигнатур витрачають багато часу на виявлення новостворених загроз, відомих лише зловмиснику (також відомих як атаки нульового дня або експлойти), та додавання їх до списків відомих загроз, що залишає кінцеві точки вразливими до оновлення сигнатур.

Cortex XDR використовує ефективніший та результативніший підхід до запобігання атакам, який усуває необхідність у традиційних антивірусних засобах. Замість того, щоб намагатися встигати за постійно зростаючим списком відомих загроз, Cortex XDR встановлює низку перешкод, які запобігають атакам у їхніх початкових точках входу, де легітимні виконувані файли збираються несвідомо дозволити зловмисникам доступ до системи.

Cortex Cloud пропонує багатометодне рішення для захисту з модулями захисту від експлойтів, які виявляють вразливості програмного забезпечення в процесах, що відкривають невиконувані файли, та модулями захисту від шкідливого програмного забезпечення, які перевіряють виконувані файли, DLL-файли та макроси на наявність шкідливих сигнатур та поведінки. Використання цього багатометодного підходу разом з аналізом штучного інтелекту Cortex Cloud може запобігти всім типам атак, незалежно від того, чи є це відомими чи невідомими загрозами.

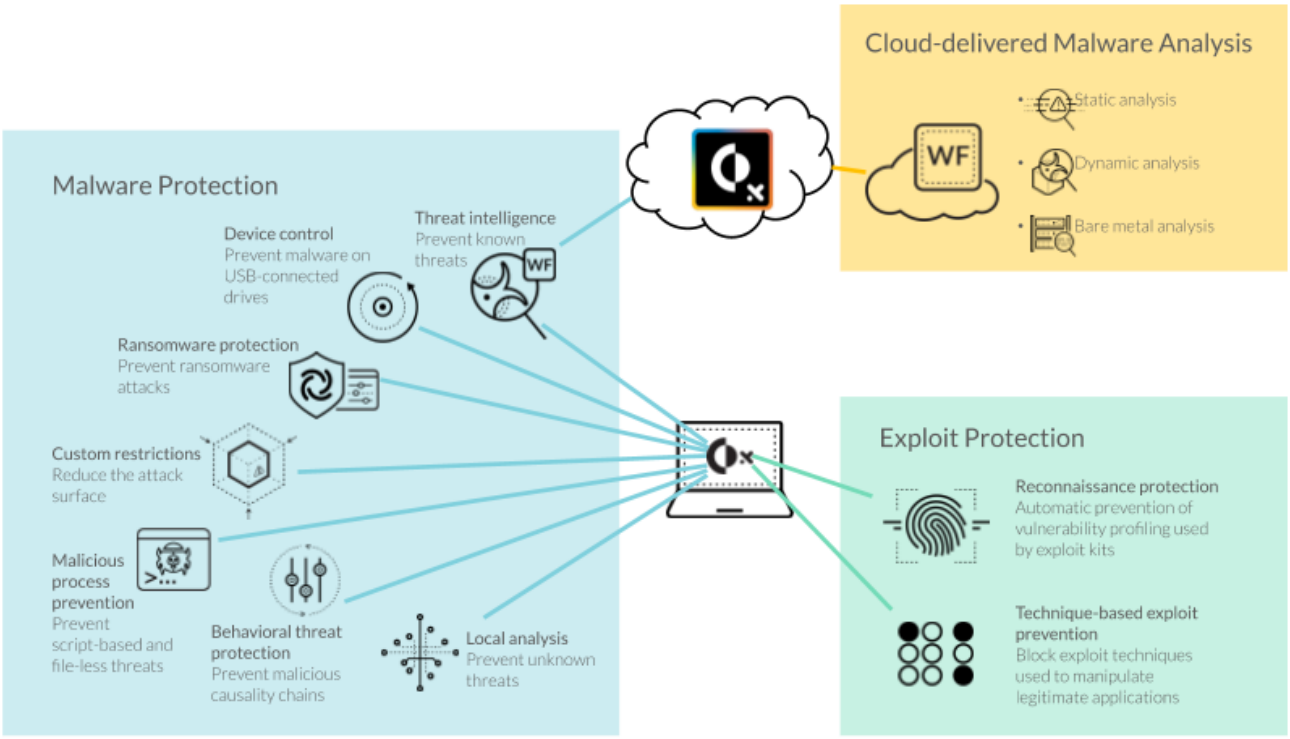

Рис.3.2. Технологія захисту від шкідливого програмного забезпечення

Складемо таблицю для розуміння, який тип захисту від шкідливого програмного забезпечення можна з використанням технології Cortex XDR. Технологія запобігання шкідливим програмам використовує методи пом'якшення, які реалізують захист від шкідливих програм на кінцевих точках на основі різних операційних систем.

Таблиця 3.2.

Типи захисту від шкідливого програмного забезпечення

Тип	Опис
Захист від несанкціонованого втручання	Дозволяє захищати від спроб втручання.
Захист від веб-оболонки	Дозволяє захищати процеси кінцевих точок від запуску шкідливих веб-оболок.
Захист файлів ASP та ASPX	Дозволяє захищати кінцеві точки від запису шкідливих файлів ASP та ASPX у файлову систему.
Захист збору облікових даних	Дозволяє захищати кінцеві точки від процесів, які намагаються отримати доступ до паролів та інших облікових даних або викрасти їх.

Тип	Опис
Захист криптомайнерів	Дозволяє захищати від спроб знайти або викрасти криптовалюти.
Динамічний захист ядра	Дозволяє захищати кінцеві точки від загроз рівня ядра, таких як буткіти, руткіти та вразливі драйвери.
Сканування кінцевих точок	Дозволяє сканувати кінцеві точки та підключені знімні диски на наявність сплячих, неактивних шкідливих програм.
Захист від загроз фінансового шкідливого програмного забезпечення	Дозволяє захищати від методів, характерних для фінансового та банківського шкідливого програмного забезпечення.
Глобальні правила захисту від поведінкових загроз	Дозволяє використовувати правила для захисту кінцевих точок від шкідливих ланцюгів причинно-наслідкових зв'язків.
Захист IIS	Дозволяє захищатися від атак Internet Information Server (IIS).
Захист шелл-коду в процесі	Дозволяє захищати від загроз атаки шеллкоду всередині процесу.
Зловмисна реакція на ланцюг причинно-наслідкових зв'язків	Дозволяє автоматично реагувати на виявлення шкідливих ланцюжків причинно-наслідкових зв'язків.
Захист від шкідливих дочірніх процесів	Дозволяє запобігати атакам на основі скриптів. Такі атаки можуть бути використані для поширення шкідливого програмного забезпечення шляхом блокування цільових процесів, які зазвичай використовуються для обходу традиційних методів безпеки.
Захист від шкідливих пристроїв	Дозволяє захищати від підключення потенційно шкідливих пристроїв до кінцевих точок.
Перевірка мережевих пакетів	Дозволяє аналізувати мережеві пакетні дані на наявність шкідливої поведінки.
Файли Office з аналізом макросів	Дозволяє аналізувати та запобігати запуску шкідливих макросів, вбудованих у файли Microsoft Office (Word, Excel), на кінцевих точках Windows.
Перевірка файлів на вимогу	Дозволяє сканувати кінцеві точки та підключені знімні диски на наявність сплячих, неактивних шкідливих програм.
Перевірка файлу під час запису	Дозволяє відстежувати шкідливі файли та вживати заходів щодо них під час процесу запису.

Тип	Опис
Захист від крадіжки пароля	Дозволяє запобігати атакам, які витягують паролі з пам'яті за допомогою інструменту Mimikatz.
Портативний виконуваний файл та DLL	Дозволяє аналізувати та запобігати запуску шкідливих виконуваних файлів і DLL-файлів на кінцевих точках Windows.
Перевірка файлу скрипта PowerShell	Дозволяє аналізувати та запобігати запуску шкідливих файлів сценаріїв PowerShell на кінцевих точках Windows.
Захист від програм-вимагачів	Дозволяє захищати від шифрувальних дій, пов'язаних з атаками програм-вимагачів.
Захист від обходу заходів безпеки	Дозволяє захищати кінцеві точки від зловмисників, які намагаються обійти вбудовані засоби безпеки Windows.
Запобігання обходу UAC	Дозволяє захищатися від механізму обходу контролю доступу користувачів (UAC), пов'язаного зі спробами підвищення прав.
Захист UEFI	Дозволяє захищати кінцеві точки від спроб маніпуляцій з Unified Extensible Firmware Interface (UEFI).
Захист файлів скриптів VB	Дозволяє захищати кінцеві точки від шкідливих файлів VB-скриптів.

Для боротьби з атакою, в якій зловмисник використовує програмний експлойт або вразливість, Cortex XDR використовує модулі захисту кінцевих точок (EPM). Кожен EPM спрямований на певний тип експлойту в ланцюжку атак. Деякі можливості, які надають Cortex Cloud EPM, включають запобігання розвідці, запобігання пошкодженню пам'яті, запобігання виконанню коду та захист ядра.

Запобігання розвідці запобігає зловмисникам зондувати мережу на наявність вразливостей, зберігаючи при цьому можливість проводити внутрішнє розвідувальне тестування.

Запобігання пошкодженню пам'яті запобігає використанню зловмисниками вразливостей, пов'язаних з пошкодженням пам'яті.

Запобігання виконанню коду запобігає появі шкідливого коду, який може дозволити зловмисникам розгортати додаткове шкідливе програмне забезпечення для крадіжки конфіденційних даних.

Захист ядра захищає ядро від загроз та експлойтів ядра.

3.2. Рекомендації використання технологій захисту кінцевої точки від сучасних атак на прикладі Cortex-XDR

Агент Cortex XDR використовує передові багаторівневі методи захисту та запобігання для захисту ваших кінцевих точок від відомих та невідомих шкідливих програм та програмних експлойтів.

Розробимо рекомендації щодо захисту від експлойтів для захищених процесів на кінцевій точці.

У типовому сценарії атаки зловмисник намагається отримати контроль над системою, спочатку пошкоджуючи або обходячи розподіл пам'яті чи обробники. Використовуючи методи пошкодження пам'яті, такі як переповнення буфера та пошкодження динамічно виділеної пам'яті (купи), хакер може викликати помилку в програмному забезпеченні або використати вразливість у процесі. Потім зловмисник повинен маніпулювати програмою для запуску коду, наданого або вказаного зловмисником, уникаючи виявлення. Якщо зловмисник отримує доступ до операційної системи, він може завантажити шкідливе програмне забезпечення, таке як троянські коні (програми, що містять шкідливі виконувані файли), або іншим чином використовувати систему на свою користь. Агент Cortex XDR запобігає таким спробам експлуатації, використовуючи пастки на кожному етапі спроби експлуатації (рис.3.3).

Коли користувач відкриває невиконуваний файл, такий як PDF-документ або документ Word, і процес, який відкрив файл, захищений, агент Cortex XDR безперешкодно вводить код у програмне забезпечення. Це відбувається на якомога раннішому етапі, до того, як будь-які файли, що належать процесу, будуть завантажені в пам'ять. Потім агент Cortex XDR активує один або кілька модулів захисту всередині захищеного процесу. Кожен модуль захисту спрямований на певну техніку експлуатації та призначений для запобігання атакам на вразливості програми, засновані на пошкодженні пам'яті або логічних недоліках.

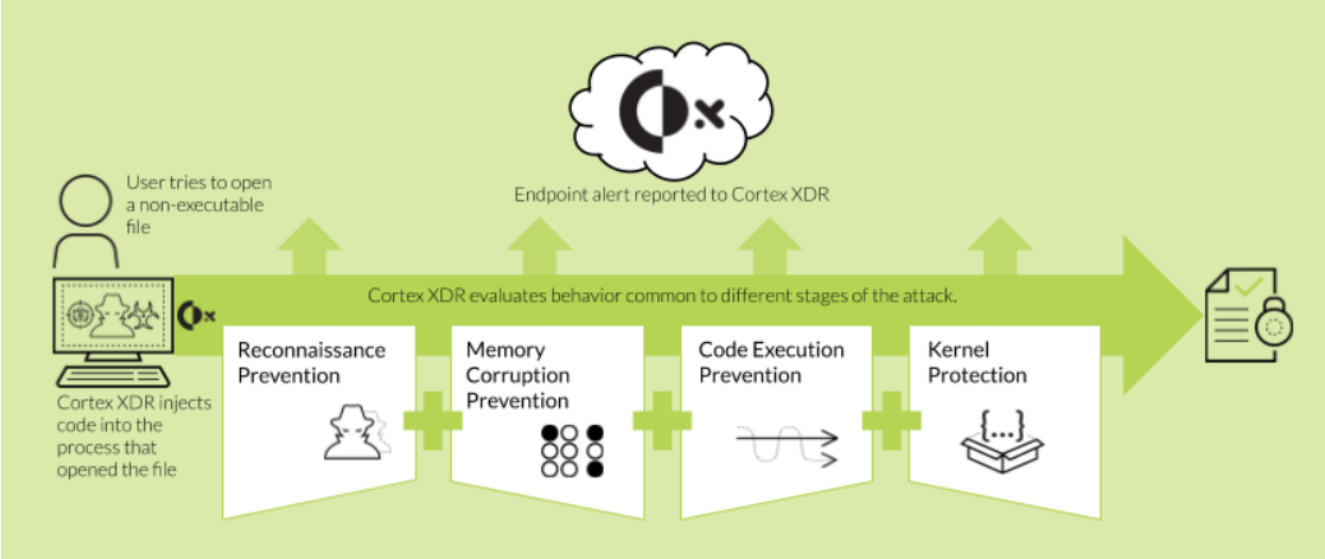

Рис.3.3. Процес виявлення експлойтів на кінцевій точці на основі агентів Cortex XDR

Окрім автоматичного захисту процесів від таких атак, агент Cortex XDR повідомляє про будь-які події безпеки до Cortex XDR та виконує додаткові дії, визначені в політиці безпеки кінцевої точки. Звичайні дії, що виконуються агентом Cortex XDR, включають збір даних експертизи та повідомлення користувача про подію.

Політика безпеки кінцевих точок за замовчуванням захищає найвразливіші та найчастіше використовувані програми, але адміністратори також можуть додати інші сторонні та власні програми до списку захищених процесів.

Розглянемо процес та надаймо рекомендації щодо роботи технології захисту від шкідливого програмного забезпечення.

Агент Cortex XDR забезпечує захист від шкідливого програмного забезпечення в серії з чотирьох фаз оцінювання, як це показано на рис.3.4.

Фаза 1: Оцінка політики захисту процесуальних питань дочірних процесів.

Фаза 2: Оцінка політики обмежень.

Фаза 3: Визначення вердикту хешу.

Фази 4: Оцінка політики захисту від шкідливого програмного забезпечення.

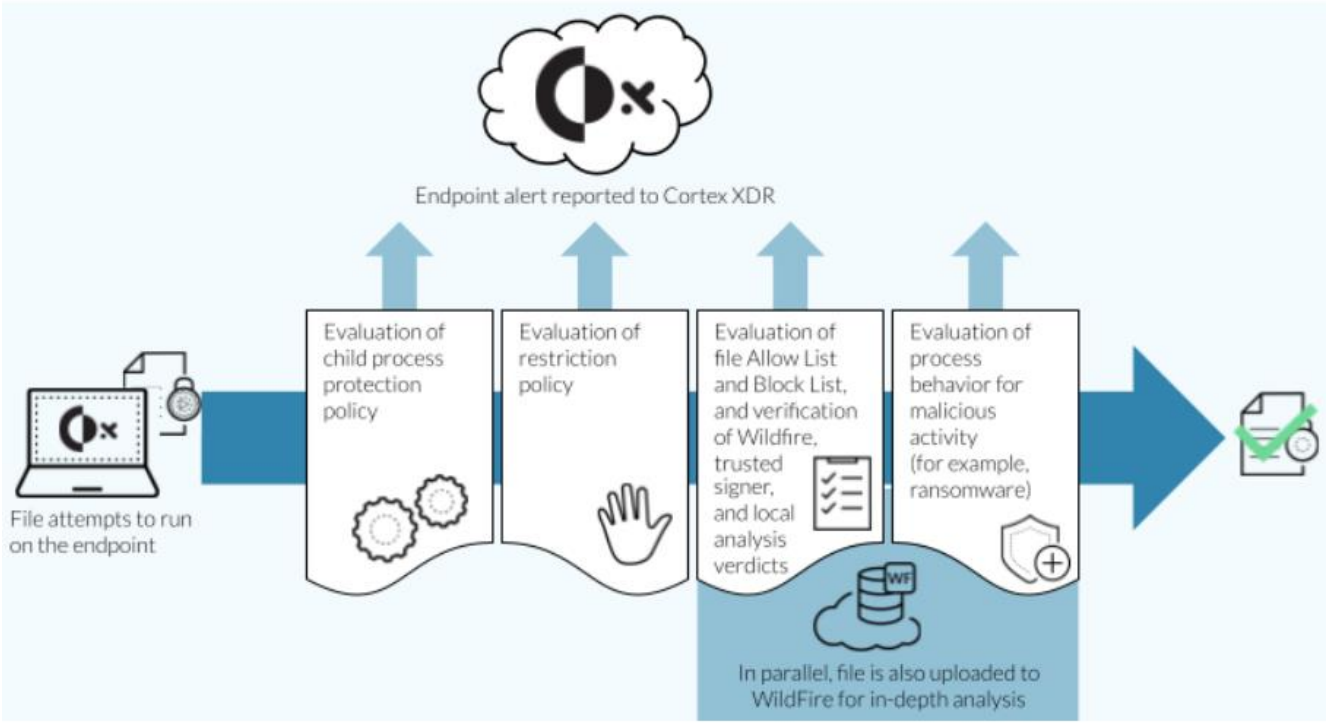

Рис.3.4. Фази оцінювання захисту від шкідливого програмного забезпечення

Фаза 1: Оцінка політики захисту процесуальних питань дочірних процесів

Коли користувач намагається запустити виконуваний файл, операційна система намагається запустити виконуваний файл як процес. Якщо процес намагається запустити будь-які дочірні процеси, агент Cortex XDR спочатку оцінює політику захисту дочірніх процесів. Якщо батьківський процес є відомим цільовим процесом, який намагається запустити обмежений дочірній процес, агент Cortex XDR блокує запуск дочірніх процесів і повідомляє про подію безпеки Cortex XDR . Наприклад, якщо користувач намагається відкрити документ Microsoft Word (за допомогою процесу winword.exe), а документ містить макрос, який намагається запустити заблокований дочірній процес (наприклад, WScript), агент Cortex XDR блокує дочірній процес і повідомляє про подію Cortex XDR . Якщо батьківський процес не намагається запустити жодних дочірніх процесів або намагається запустити дочірній процес, який не обмежений, агент Cortex XDR переходить до Фази 2: Оцінка політики обмежень .

Фаза 2: Оцінка політики обмежень

Агент Cortex XDR перевіряє, чи виконуваний файл не порушує жодних правил обмеження. Наприклад, у вас може бути правило обмеження, яке блокує виконувані файли, запущені з мережевих розташувань. Якщо правило обмеження застосовується до виконуваного файлу, агент Cortex XDR блокує виконання файлу та повідомляє про подію безпеки Cortex XDR , і, залежно від конфігурації кожного правила обмеження, агент Cortex XDR також може повідомити користувача про подію запобігання.

Якщо до виконуваного файлу не застосовуються правила обмеження, агент Cortex XDR переходить до Фази 3: Визначення вердикту хешування .

Фаза 3: Визначення вердикту хешу

Агент Cortex XDR обчислює унікальний хеш за допомогою алгоритму SHA-256 для кожного файлу, який намагається запуститися на кінцевій точці. Залежно від увімкнених функцій, агент Cortex XDR виконує додатковий аналіз, щоб визначити, чи є невідомий файл шкідливим чи безпечним. Агент Cortex XDR також може надсилати невідомі файли до Cortex XDR для поглибленого аналізу WildFire.

Щоб визначити вердикт для файлу, агент Cortex XDR оцінює файл у такому порядку:

1. Виняток хешування. Виняток хешування дозволяє вам змінити вердикт для певного файлу, не впливаючи на налаштування у вашому профілі захисту від шкідливих програм. Політика винятків хешування оцінюється першою та має пріоритет над усіма іншими методами визначення вердикту хешування.

Наприклад, ви можете налаштувати виняток хешування для будь-якої з наступних ситуацій:

– Ви хочете заблокувати файл, який має сприятливий вердикт.

– Ви хочете дозволити запуск файлу, який має вердикт про шкідливе програмне забезпечення. Загалом, рекомендовано скасовувати вердикт про шкідливе програмне забезпечення лише після того, як ви скористаєтеся доступними ресурсами аналізу загроз, такими як WildFire та AutoFocus, щоб визначити, що файл не є шкідливим.

– Ви хочете вказати вердикт для файлу, який ще не отримав офіційного вердикту WildFire.

Після налаштування хеш-винятку, Cortex XDR розповсюджує його під час наступного зв'язку heartbeat з будь-якими кінцевими точками, які раніше відкривали файл.

Коли файл запускається на кінцевій точці, агент Cortex XDR спочатку оцінює будь-які відповідні хеш-винятки для файлу. Хеш-виняток визначає, чи слід розглядати файл як шкідливе програмне забезпечення. Якщо файлу присвоюється вердикт «нешкідливий», агент Cortex XDR дозволяє його відкриття.

Якщо для файлу не налаштовано виняток хешування, агент Cortex XDR далі оцінює вердикт, щоб визначити ймовірність наявності шкідливого програмного забезпечення.

2. Підписувачі з високим рівнем довіри (Windows та Mac). Агент Cortex XDR відрізняє підписувачів з високим рівнем довіри, таких як Microsoft, від інших відомих підписувачів. Щоб підтримувати паритет із підписувачами, визначеними у WildFire, Palo Alto Networks регулярно переглядає список підписувачів з високим рівнем довіри та відомих підписувачів і вносить будь-які зміни до оновлень вмісту. Список підписувачів з високим рівнем довіри також включає підписувачів, включених до списку дозволів Cortex XDR . Коли невідомий файл намагається запуститися, агент Cortex XDR застосовує такі критерії оцінки: Файли, підписані підписувачами з високим рівнем довіри, дозволені для запуску, а файли, підписані заблокованими підписувачами, блокуються, незалежно від вердикту WildFire . В іншому випадку, коли файл не підписано підписувачем з високим рівнем довіри або підписувачем, включеним до списку блокування, агент Cortex XDR далі оцінює вердикт WildFire . Для кінцевих точок Windows оцінка інших відомих підписувачів відбувається, якщо оцінка WildFire повертає невідомий вердикт для файлу.

3. Вердикт WildFire. Якщо файл не підписано високонадійним підписувачем на кінцевих точках Windows та Mac, агент Cortex XDR виконує пошук хеш-вердикту, щоб визначити, чи вже існує вердикт у його локальному кеші.

Якщо виконуваний файл має вердикт про шкідливе програмне забезпечення, агент Cortex XDR повідомляє про подію безпеки Cortex XDR, і, залежно від налаштованої поведінки для шкідливих файлів, агент Cortex XDR виконує одну з наступних дій.

Блокує файл.

Блокує та поміщає файл у карантин.

Повідомляє користувача про файл, але все одно дозволяє його виконання.

Записує проблему в журнал без повідомлення користувача та дозволяє виконання файлу.

Якщо вердикт позитивний, агент Cortex XDR переходить до наступного етапу оцінки — Фази 4: Оцінка політики захисту від шкідливого програмного забезпечення .

Якщо хеш не існує в локальному кеші або має невідомий вердикт, агент Cortex XDR далі оцінює, чи підписано файл відомим підписувачем.

4.Локальний аналіз. Коли невідомий виконуваний файл, DLL або макрос намагається запуститися на кінцевій точці Windows або Mac, агент Cortex XDR використовує локальний аналіз, щоб визначити, чи є він ймовірно шкідливим програмним забезпеченням. На кінцевих точках Windows, якщо файл підписано відомим підписувачем, агент Cortex XDR дозволяє запуск файлу та не виконує додаткового аналізу. Для файлів на кінцевих точках Mac та файлів, які не підписані відомим підписувачем на кінцевих точках Windows, агент Cortex XDR виконує локальний аналіз, щоб визначити, чи є файл шкідливим програмним забезпеченням. Локальний аналіз використовує статичний набір правил зіставлення зі зразками, які перевіряють кілька функцій та атрибутів файлу, а також статистичну модель, розроблену за допомогою машинного навчання на основі даних про загрози WildFire. Модель дозволяє агенту Cortex XDR досліджувати сотні характеристик файлу та видавати локальний вердикт (доброякісний чи шкідливий), коли кінцева точка перебуває в автономному режимі або Cortex XDR недоступний. Агент Cortex XDR може покладатися на вердикт локального аналізу, доки не отримає офіційний вердикт WildFire або виняток хешування.

Локальний аналіз увімкнено за замовчуванням у профілі захисту від шкідливих програм. Оскільки локальний аналіз завжди повертає вердикт для невідомого файлу, якщо ввімкнути агенту Cortex XDR параметр Блокувати файли з невідомим вердиктом , агент блокуватиме невідомі файли лише у випадку помилки локального аналізу або вимкнення локального аналізу

Фаза 4: Оцінка політики захисту від шкідливих програм

Якщо попередні фази оцінки не ідентифікують файл як шкідливе програмне забезпечення, агент Cortex XDR спостерігає за поведінкою файлу та застосовує додаткові правила захисту від шкідливого програмного забезпечення. Якщо файл демонструє шкідливу поведінку, таку як активність на основі шифрування, поширена у програм-вимагачів, агент Cortex XDR блокує файл і повідомляє про подію безпеки Cortex XDR .

Якщо шкідливої поведінки не виявлено, агент Cortex XDR дозволяє файлу (процесу) продовжувати роботу, але продовжує моніторити поведінку протягом усього життєвого циклу процесу.

Всі данні щодо безпеки кінцевої точки можна побачати на інформаційній панелі Cortex XD. Панелі інструментів пропонують графічні огляди діяльності вашого клієнта. Це дозволяє ефективно контролювати загальну активність середовища інформаційної системи. Кожна панель інструментів містить віджети, які підсумовують інформацію про кінцеву точку в графічному або табличному форматі (рис.3.4) [18].

Рис.3.5. Інформаційна панель Cortex XD

Дашборди в Cortex XDR 4.x призначені для моніторингу системної активності у інформаційній системі організації.

: Дашборди допомагають відстежувати загальну активність системи, що дозволяє помічати аномалії, пов'язані зі шкідливим ПЗ за рахунок моніторингу активності.

Дашборд забезпечують миттєву видимість стану безпеки через Command Center dashboards, дозволяючи швидко перейти до детального розслідування інцидентів.

Дашборди є точкою входу для аналітиків SOC, які можуть використовувати попередньо визначені або кастомні дашборди для виявлення, розслідування та реагування на загрози, включно зі шкідливим програмним забезпеченням.

На дашбордах може бути відображена інформація про події, пов'язані з файлами, процесами та мережевими з'єднаннями, які є ключовими для виявлення та запобігання поширенню шкідливого програмного забезпечення.

Висновки до розділу 3

1. Запропоновано основні шляхи щодо використання технології Cortex XDR, які входять до захисту кінцевої точки організаці. Cortex XDR використовує ефективніший та результативніший підхід до запобігання атакам, який усуває необхідність у традиційних антивірусних засобах.

2. Запропоновано технологію захисту від шкідливого програмного забезпечення на основі методу пом'якшення, яке реалізує захист від шкідливих програм на кінцевих точках на основі різних операційних систем.

3. Розроблено рекомендації використання технологій захисту кінцевої точки від сучасних атак на прикладі Cortex-XDR для виявлення експлойтів та шкідливого програмного забезпечення на основі серії з чотирьох фаз оцінювання.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні результати:

1. В результаті аналізу, визначено основні проблеми захисту кінцевих точок організації.

2. Визначено вектор атак на кінцеві точки, що впливає на кінцеві точки та можуть порушити бізнес-операції організацій.

3. Запропоновано підходи для забезпечення безпека кінцевих точок, що працює за допомогою багаторівневого підходу, що інтегрує різні технології та методології для захисту пристроїв від початкового компрометування шляхом постійного моніторингу та реагування.

4. Визначено, шляхом порівняльного аналізу рішення Cortex-XDR, яке найбільше відповідає запропонованому багатошарового підходу.

5. Визначено архітектуру Cortex XDR, яка дозволяє впровадити методи та захисту кінцеих точок від сучасних загроз.

6. Визначено основні компоненти технології Cortex XDR та їх функції, в основі якої є агент Cortex XDR, що забезпечує повний захист від загроз кінцевих точок, технологія ITDR яка призначена для виявлення загроз, пов'язаних з ідентичністю та призначений для забезпечення проактивного захисту від векторів загроз, пов’язаних з ідентифікацією, технологія UEBA, як рішення з кібербезпеки, що постійно розвивається та використовує розширену аналітику для виявлення аномалій поведінки користувачів та сутностей у мережі організації.

7. Визначено ключові характеристики Cortex XDR, які забезпечують повну видимість, швидке виявлення та реагування на сучасні загрози кінцевої точки інформаційної системи організації.

8. Запропоновано основні шляхи щодо використання технології Cortex XDR, які входять до захисту кінцевої точки організаці. Cortex XDR використовує ефективніший та результативніший підхід до запобігання атакам, який усуває необхідність у традиційних антивірусних засобах.

9. Запропоновано технологію захисту від шкідливого програмного забезпечення на основі методу пом'якшення, яке реалізує захист від шкідливих програм на кінцевих точках на основі різних операційних систем.

10. Розроблено рекомендації використання технологій захисту кінцевої точки від сучасних атак на прикладі Cortex-XDR для виявлення експлойтів та шкідливого програмного забезпечення на основі серії з чотирьох фаз оцінювання.

ПЕРЕЛІК ПОСИЛАНЬ

1. Вступ до Cortex-XDR. URL: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-4.x-Documentation/Learn-about-Cortex-XDR .

2. Захист кінцевих точок. URL: https://docs-cortex.paloaltonetworks.com/r/Cortex-CLOUD/Cortex-Cloud-Runtime-Security-Documentation/Endpoint-protection .

3. Cortex XDR Endpoint Protection Solution Guide. URL: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/guides/cortex-xdr-endpoint-protection-solution-guide

4. Identity Threat Detection and Response (ITDR). URL: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-Documentation/Identity-Threat-Detection-and-Response-ITDR .

5. Cortex Identity Threat Detection and Response Module. URL: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/identity-threat-detection-and-response-module .

6. What Is Identity Threat Detection and Response (ITDR)? URL: https://www.paloaltonetworks.com/cyberpedia/identity-threat-detection-and-response-itdr .

7. What is UEBA (User and Entity Behavior Analytics)? URL: https://www.paloaltonetworks.com/cyberpedia/what-is-user-entity-behavior-analytics-ueba .

8. Playbook of the Week: Suspicious SSO? Check It Out with XSOAR. URL: https://www.paloaltonetworks.com/blog/security-operations/playbook-of-the-week-suspicious-sso-check-it-out-with-xsoar/ .

9. Кращі практики XDR. URL: https://www.comparitech.com/net-admin/best-xdr-tools/ .

10. Опис ліцензії. URL: https://www.paloaltonetworks.com/resources/whitepapers/cortex-xdr-at-a-glance .

11. Що таке кінцева точка. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-security .

12. Агент Cortex-XDR. URL:https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/8.1/Cortex-XDR-Agent-Administrator-Guide/Install-the-Cortex-XDR-Agent-with-Installer-and-Content-Update-Package .

13. Звіт щодо інцедентів. URL: https://www.paloaltonetworks.in/resources/research/unit-42-incident-response-report

14. Ризики використання кінцевих точок. URL: https://engage.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf .

15. Безпека кінцевих точок. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-protection#why .

16. Що таке XDR URL:. https://www.paloaltonetworks.com/cyberpedia/what-is-extended-detection-response-XDR .

17. Квадрант лідерів SDR. URL: https://www.softwarereviews.com/awards/data-quadrant-awards-2024-extended-detection-response .

18. Дашборд Cortex-XDR. URL: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-4.x-Documentation/About-dashboards .

19. Гайдур Г.І., Московка С.М. Захист кінцевих точок інформаційної системи організації від сучасних загроз. *Актуальні проблеми кібербезпеки*: матеріали всеукраїнської наук.-практ. конф., м. Київ: ДУІКТ, 29 жовт. 2025р. Київ. С 202-203.