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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розроблення рекомендацій щодо захисту кінцевих точок від програм-вимагачів на базі Microsoft Defender»

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

_____ Ірина ПЕРЕКЛІТА
(підпис)

Виконала: здобувач вищої освіти групи БСД-42
ПЕРЕКЛІТА Ірина
(прізвище, ім'я)

Керівник к.військ.н., доцент ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

APT – Advanced Persistent Threat

DNS – Domain Name System

EDR – Endpoint Detection and Response

EPP – Endpoint Protection Platform

EPS – Endpoint Protection Software

GDPR – General Data Protection Regulation

IOA – Indicators of Attacks

MDE – Microsoft Defender for Endpoint

NGAV – Next-Generation Antivirus

PaaS – Platform as a Service

SIEM – Security Information and Event Monitoring

VPN – Virtual Private Network

ВСТУП

Актуальність дослідження. Дослідження шляхів та розроблення рекомендацій щодо захисту кінцевих точок від програм-вимагачів на базі Microsoft Defender залишається актуальним завдяки постійній загрозі кібербезпеці, яка швидко еволюціонує. Хоча Microsoft Defender є одним з передових інструментів для захисту кінцевих точок, програми-вимагачі постійно змінюють свої тактики та атакують уразливості в програмному забезпеченні.

Останні події та відомі вразливості підкреслюють необхідність постійного аналізу та покращення заходів безпеки, зокрема використання інструментів, які пропонує Microsoft Defender. Дослідження може допомогти виявити нові методи атак, розробити ефективні рекомендації щодо вдосконалення конфігурацій та стратегій захисту кінцевих точок, а також сприяти усуненню виявлених вразливостей.

Microsoft Defender, як інтегрована частина екосистеми продуктів Microsoft, постійно отримує оновлення та покращення, спрямовані на боротьбу з новими загрозами. Завдяки постійному аналізу великих обсягів даних та використанню штучного інтелекту, Microsoft Defender може швидко виявляти й блокувати навіть найбільш витончені атаки. Інтеграція з іншими сервісами та продуктами Microsoft, такими як Microsoft 365 або Azure, дозволяє створити комплексну систему захисту, що дозволяє ефективно моніторити та реагувати на загрози на всіх рівнях IT інфраструктури організації.

Підвищення уваги до кібербезпеки в бізнес-середовищі також підкреслює важливість таких досліджень. Забезпечення надійного захисту кінцевих точок стає невід'ємною складовою стратегії інформаційної безпеки будь-якої компанії чи організації. Таким чином, дослідження шляхів та рекомендацій, спрямованих на поліпшення захисту кінцевих точок за допомогою Microsoft Defender, залишається важливим завданням у сфері кібербезпеки.

Попри стійкий розвиток кіберзагроз та появу нових вразливостей, Microsoft Defender продовжує залишатися ключовим інструментом у сфері кібербезпеки. Його постійне вдосконалення та оновлення дозволяють ефективно протистояти різноманітним загрозам. Дослідження шляхів захисту кінцевих точок на базі Microsoft Defender є актуальним завдяки його потенціалу у виявленні, блокуванні та аналізі шкідливих програм та атак. Враховуючи зростаючу складність кіберзагроз та постійну необхідність адаптації заходів безпеки, такі дослідження стають ключовими для забезпечення ефективного захисту користувачів та організацій від потенційних загроз.

Об'єкт дослідження – захист кінцевих точок від програм-вимагачів.

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

Мета роботи – розробити рекомендації щодо застосування методів та засобів захисту кінцевих точок від програм-вимагачів на базі Microsoft Defender.

Наукові завдання:

дослідити сутність проблеми захисту кінцевих точок;

проаналізувати основні підходи до захисту кінцевих точок;

проаналізувати існуючі рішення із захисту кінцевих точок від програм-вимагачів;

проаналізувати методи та засоби захисту кінцевих точок від програм-вимагачів на базі Microsoft Defender;

розробити рекомендацій щодо застосування методів та засобів захисту кінцевих точок від програм-вимагачів.

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

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

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ВІД ПРОГРАМ-ВИМАГАЧІВ

1.1 Аналіз проблеми захисту кінцевих точок від програм-вимагачів

Відповідно до звіту Cybersecurity Insiders [1], організації стикаються з серйозними проблемами у захисті від нових та все більш витончених кіберзагроз. Це призводить до зростання ризиків для безпеки кінцевих точок. Водночас, багато організацій відчувають себе непідготовленими до протидії цим загрозам за допомогою існуючих платформ безпеки кінцевих точок.

Серед головних кіберзагроз, з якими стикаються організації, фахівці з кібербезпеки виділяють шкідливе програмне забезпечення (38%), таке як програми-вимагачі, трояни та набори експлойтів. На другому місці - людські помилки (23%), а на третьому - експлойти нульового дня (18%). Ці дані підтверджуються результатами інших досліджень, які показують зростання загрози з боку шкідливого програмного забезпечення, особливо програм-вимагачів (рисунок 1.1).

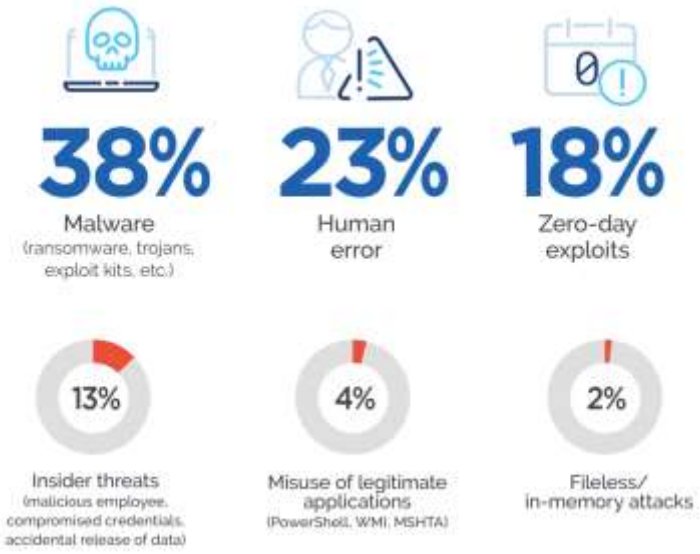

Рис. 1.1. Найбільші загрози кібербезпеці для організацій

Згідно до звіту Cybersecurity Insiders, більшість організацій відчули зростання кіберзагроз для своїх кінцевих точок (66%). Двадцять відсотків фахівців з кібербезпеки повідомляють, що за останні 12 місяців їхня організація зазнала «успішної» атаки на кінцеві точки, яка скомпрометувала активи даних та/або IT-інфраструктуру(рисунок 1.2). Кількість невиявлених атак, ймовірно, значно вища.

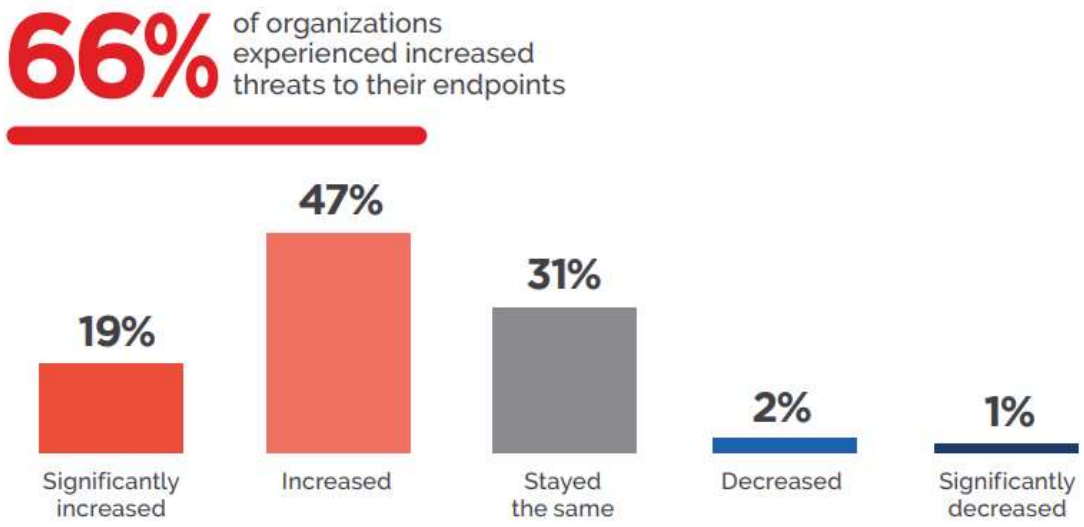

Рис. 1.2. Організації, що зіткнулися з підвищеними загрозами для своїх кінцевих точок

Програми-вимагачі становлять дедалі більшу загрозу для організацій усіх розмірів. Ці шкідливі програми можуть зашифрувати дані на заражених пристроях, роблячи їх недоступними для користувачів, і вимагати викуп за їх розшифровку. Атаки програм-вимагачів можуть призвести до значних фінансових втрат, порушення роботи та шкоди для репутації.

Зловмисники постійно розробляють нові та більш витончені методи атак програм-вимагачів. Деякі з останніх тенденцій включають [2-5]:

використання вразливостей нульового дня: зловмисники все частіше використовують вразливості нульового дня, які ще не відомі постачальникам

програмного забезпечення, для атак програм-вимагачів;

націлювання на ланцюги постачання: зловмисники нападають на постачальників, щоб отримати доступ до мереж своїх клієнтів;

використання криптовалют: зловмисники використовують криптовалюти, такі як Bitcoin, щоб отримувати викупи, що ускладнює відстеження платежів;

атаки типу "подвійне вимагання": зловмисники крадуть дані, перш ніж шифрувати їх, і вимагають викуп за розшифровку даних, а також загрожують оприлюднити дані, якщо викуп не буде сплачено;

Захист кінцевих точок від програм-вимагачів (ransomware) є критично важливим завданням для забезпечення безпеки інформаційних систем. Програми-вимагачі є одним з найпоширеніших і найнебезпечніших типів шкідливого програмного забезпечення, що атакують кінцеві точки, такі як комп'ютери, ноутбуки, смартфони та інші пристрої.

Програми-вимагачі - це тип шкідливого програмного забезпечення, яке шифрує дані на зараженому пристрої та вимагає викупу за їх розшифровку. Ці атаки можуть мати руйнівні наслідки для особистих користувачів та організацій, такі, як:

фінансові втрати: викуп за розшифровку даних може сягати тисяч або навіть мільйонів доларів, що призводить до значних фінансових втрат для організацій. Атаки програм-вимагачів також можуть призвести до непрямих витрат, таких як простої, втрата продуктивності, витрати на відновлення даних, юридичні витрати та шкода репутації;

втрата даних: особисті користувачі можуть втратити цінні фотографії, документи, музику, відео та інші файли, що може мати значний емоційний та фінансовий вплив. Організації можуть втратити конфіденційну інформацію, таку як дані клієнтів, медичні записи або фінансові дані, що може призвести до порушення нормативних вимог, штрафів та судових розглядів; [6]

пошкодження репутації: атаки програм-вимагачів можуть завдати шкоди

репутації організації, підірвати довіру клієнтів та партнерів і призвести до втрати бізнесу. Негативний вплив на репутацію може тривати роками, навіть після успішного відновлення даних;

операційні збої: шифрування даних може призвести до простоїв комп'ютерів, серверів та мереж, що негативно впливає на роботу організацій. [7] Навіть без повного простою, атаки програм-вимагачів можуть призвести до значного зниження продуктивності, оскільки співробітники не зможуть отримати доступ до важливих даних та програм.

Захист кінцевих точок від програм-вимагачів є надзвичайно важливою та багатогранною проблемою, що вимагає комплексного підходу. Програми-вимагачі, які зловмисники використовують для шифрування або блокування даних з метою отримання викупу, є однією з найбільш поширених та руйнівних загроз у сучасному кіберпросторі. Їх атаки можуть призвести до значних фінансових втрат, порушення роботи організацій та втрати конфіденційних даних.

1.2 Аналіз підходів до захисту кінцевих точок від програм-вимагачів

Атаки програм-вимагачів можуть мати руйнівні наслідки для організацій та окремих людей, призводячи до втрати даних, фінансових збитків, простоїв у роботі та пошкодження репутації.

Існує багато різних підходів до захисту кінцевих точок від програм-вимагачів.

Аналіз підходів до захисту кінцевих точок від програм-вимагачів демонструє складність і багатогранність цього завдання. Зважаючи на постійне вдосконалення методів атак, організації повинні застосовувати комплексні заходи для захисту своїх систем.

Вибір правильного підходу до захисту кінцевих точок вимагає розуміння специфіки загроз і наявних рішень. Сучасні рішення включають використання

платформ захисту кінцевих точок (EPP) та інструментів для виявлення та реагування на атаки (EDR), які поєднують в собі антивірусні програми, файрволи, системи виявлення вторгнень та інші технології. Важливо обрати такі платформи, що забезпечують ефективний захист у реальному часі, включаючи функції автоматичного відновлення після атак та ізоляцію уражених пристроїв.

Захист кінцевих точок від програм-вимагачів є важливим елементом кібербезпеки, оскільки атаки такого типу можуть призвести до значних фінансових втрат та втрати даних. Для забезпечення ефективного захисту використовуються різноманітні підходи, які можна умовно розділити на технічні, організаційні та освітні заходи. Кожен з них має свої переваги і недоліки, і їх поєднання дозволяє забезпечити надійний рівень захисту.

Варто розглянути технічні заходи безпеки. *Антивірусне та антивимагачеве програмне забезпечення* є основним інструментом для виявлення і блокування шкідливих програм. Сучасні рішення використовують багаторівневий підхід, який включає сигнатурний аналіз для виявлення відомих загроз, евристичний аналіз для визначення нових загроз за допомогою аналізу поведінки програм, і поведінковий аналіз, що дозволяє виявляти підозрілі дії у режимі реального часу. Регулярні оновлення антивірусних баз даних є критично важливими для забезпечення захисту від нових загроз. [8]

Брандмауери та мережеві фільтри контролюють мережевий трафік, забезпечуючи бар'єр між внутрішньою мережею та зовнішнім світом. Вони блокують підозрілі з'єднання та запобігають проникненню шкідливого програмного забезпечення через мережеві вразливості. Фільтрація контенту дозволяє блокувати доступ до відомих зловмисних сайтів та фільтрувати шкідливий контент.

Системи виявлення та запобігання вторгнень (IDS/IPS) моніторять мережевий трафік і аналізують його на наявність аномальної або підозрілої активності. IDS системи виявляють атаки в режимі реального часу, тоді як IPS

системи можуть автоматично блокувати такі атаки, забезпечуючи проактивний захист.

Регулярні оновлення та патчинг програмного забезпечення допомагають усунути відомі вразливості, що можуть бути використані програмами-вимагачами. Оновлення операційних систем, додатків та іншого програмного забезпечення є ключовими для запобігання експлуатації цих вразливостей. Важливо автоматизувати процес оновлення для зменшення ризику людських помилок та прискорення реагування на нові загрози. Регулярне оновлення програмного забезпечення є критичним елементом захисту. Застарілі системи є вразливими до нових атак, тому важливо забезпечити своєчасне встановлення всіх патчів та оновлень. Це включає як операційні системи, так і всі програми, що використовуються на кінцевих точках.

Використання резервного копіювання даних є ще одним важливим аспектом захисту. Навіть у випадку успішної атаки, наявність актуальних резервних копій дозволяє швидко відновити роботу без виплати викупу. Цей процес повинен бути автоматизованим і регулярним, щоб забезпечити актуальність збережених даних

Перейдемо до організаційних заходів, що є не менш важливими.

Політики безпеки є важливою складовою захисту кінцевих точок. Впровадження політик, що регулюють доступ користувачів до ресурсів системи на основі принципу найменших привілеїв, дозволяє знизити ризик несанкціонованого доступу. Створення регулярних резервних копій критично важливих даних забезпечує можливість відновлення після атаки, і резервні копії повинні зберігатися в захищених місцях, бажано поза межами основної мережі.

План реагування на інциденти включає розробку та тестування планів реагування на кіберінциденти, що дозволяє швидко та ефективно реагувати на атаки. Ці плани повинні включати кроки для ізоляції заражених систем, повідомлення відповідних осіб та відновлення даних з резервних копій.

Проведення форензичних розслідувань після інцидентів допомагає визначити, як відбулася атака, які вразливості були використані та які дії необхідно вжити для уникнення подібних атак у майбутньому.

Освітні заходи варті серйозної уваги, адже завдяки обізнаності персоналу можна запобігти певному відсотку атак.

Навчання персоналу є критичним аспектом захисту від програм-вимагачів. Регулярне навчання співробітників щодо виявлення фішингових атак та інших методів соціальної інженерії допомагає запобігти проникненню шкідливого програмного забезпечення. Співробітники повинні знати, як виглядають підозрілі електронні листи, посилання та вкладення, а також як правильно реагувати у разі підозри на атаку. Людський фактор часто є найслабшою ланкою у безпеці, тому проведення регулярних тренінгів з кібербезпеки допомагає зменшити ризик успішних фішингових атак та інших методів соціальної інженерії.

Симуляції та тестування фішингових атак дозволяють перевірити готовність персоналу та виявити слабкі місця у знаннях співробітників. Проведення регулярних симуляцій допомагає оцінити, наскільки ефективно співробітники можуть розпізнавати та реагувати на фішингові загрози, а аналіз результатів дозволяє вносити відповідні зміни до освітніх програм та політик безпеки.

1.3 Аналіз існуючих рішень із захисту кінцевих точок від програм-вимагачів

Захист кінцевих точок від програм-вимагачів (ransomware) є критично важливим завданням для сучасних організацій, оскільки атаки такого типу можуть призвести до значних фінансових втрат, втрати даних та порушення

операційної діяльності. Існує широкий спектр рішень, що спрямовані на захист кінцевих точок від цих загроз. Вони включають як традиційні антивірусні програми, так і більш сучасні технології, такі як системи виявлення та реагування на інциденти (EDR), багатошаровий захист, регулярні оновлення програмного забезпечення та навчання користувачів.

Антивірусне програмне забезпечення залишається однією з основних ліній захисту від програм-вимагачів. Воно використовує сигнатурний аналіз для виявлення відомих загроз та евристичний аналіз для визначення нових загроз на основі поведінкових моделей.

Приклад: традиційні антивірусні програми, використовують комбінацію сигнатурного та поведінкового аналізу для виявлення і блокування відомих загроз. Системи EDR, такі як CrowdStrike Falcon, додають можливості для виявлення аномальної поведінки і швидкого реагування на інциденти у режимі реального часу. Багатошаровий захист, що реалізується в таких продуктах, як Sophos Intercept X з технологією CryptoGuard, забезпечує додаткові рівні безпеки шляхом виявлення та блокування зловмисного шифрування файлів.

Регулярне оновлення програмного забезпечення посідає неабияке місце для захисту даних. Вразливості у програмному забезпеченні часто використовуються для проникнення програм-вимагачів. Регулярні оновлення та патчі зменшують ризик успішної експлуатації цих вразливостей.

Приклад: Microsoft Defender: Ця антивірусна програма автоматично отримує оновлення через Windows Update, що допомагає забезпечити захист від нових загроз. Регулярні оновлення та автоматичні патчі є ключовими для забезпечення безпеки кінцевих точок від програм-вимагачів. *Microsoft Defender for Endpoint:* комплексне рішення, яке пропонує широкий спектр функцій захисту кінцевих точок, включаючи антивірусний захист, захист від шкідливого програмного забезпечення, захист від програм-вимагачів, захист від поведінки, захист від експлойтів та централізоване управління. Defender for Endpoint добре

інтегрується з іншими продуктами Microsoft, такими як Microsoft 365, що може полегшити його розгортання та керування.[9]

Рис. 1.3. Квадрат Gartner ® Magic Quadrant ™ для платформ захисту кінцевих точок (грудень 2023 р.).

Навчання персоналу є важливим аспектом захисту, оскільки багато атак починаються з фішингових листів або інших методів соціальної інженерії. Навчання допомагає користувачам розпізнавати підозрілі дії та правильно реагувати на них.

Приклад: KnowBe4 Security Awareness Training: ця платформа надає інтерактивні тренінги з кібербезпеки, включаючи симуляції фішингових атак. Метою є підвищення обізнаності користувачів і зменшення ризику успішних атак програм-вимагачів через соціальну інженерію

Платформи, такі як KnowBe4, пропонують інтерактивні тренінги з кібербезпеки, що допомагають співробітникам розпізнавати і правильно реагувати на потенційні загрози.

Технології EDR-системи дозволяють виявляти і реагувати на підозрілі дії на кінцевих точках у режимі реального часу. Вони аналізують поведінку програм і користувачів для виявлення аномалій, що можуть вказувати на атаку.

Приклад: CrowdStrike Falcon: ця платформа EDR забезпечує виявлення загроз у реальному часі, аналізуючи поведінку кінцевих точок і використовуючи штучний інтелект для виявлення аномалій. Вона також надає можливості для миттєвого реагування, такі як ізоляція уражених систем від мережі

Багатошаровий підхід до захисту кінцевих точок передбачає використання кількох різних технологій і методів для забезпечення надійної безпеки.

Приклад: Sophos Intercept X: це рішення включає технологію CryptoGuard, яка виявляє і блокує зловмисне шифрування файлів. CryptoGuard аналізує вміст файлів, використовуючи математичні алгоритми, щоб виявити ознаки шифрування, незалежно від того, де виконуються зловмисні процеси. Також воно автоматично відновлює зашифровані файли, зменшуючи вплив на бізнес

Створення регулярних *резервних копій* є ключовим для відновлення після атак програм-вимагачів. Важливо, щоб резервні копії зберігалися у захищених місцях і були доступні для швидкого відновлення.

Приклад: Acronis Cyber Backup: це рішення забезпечує резервне копіювання та відновлення даних з використанням хмарних сервісів та локальних сховищ. Acronis використовує технологію активного захисту, що включає функції захисту від програм-вимагачів, виявляючи і блокуючи зловмисне шифрування файлів у режимі реального часу.

Таким чином, сучасний підхід до захисту кінцевих точок від програм-вимагачів включає використання комплексних рішень, які поєднують технологічні інновації з організаційними заходами та навчанням користувачів, що дозволяє ефективно протистояти цим загрозам і мінімізувати їх вплив на бізнес.

Захист кінцевих точок від програм-вимагачів є складним і багатогранним

завданням, яке вимагає поєднання технічних, організаційних та освітніх заходів. Використання сучасних технологій, таких як антивірусні програми, брандмауери, IDS/IPS системи та регулярне оновлення програмного забезпечення, є ключовими компонентами технічного захисту. Організаційні заходи, такі як політики безпеки, управління доступом та резервне копіювання, допомагають зменшити ризики та забезпечити швидке відновлення після атак. Освітні заходи, включаючи регулярне навчання та симуляції, підвищують обізнаність співробітників про кіберзагрози та готують їх до ефективного реагування на інциденти.

Комплексний підхід до захисту кінцевих точок дозволяє ефективно протистояти загрозам програм-вимагачів та забезпечити надійний рівень кібербезпеки в організації.

Програми-вимагачі становлять значну загрозу для будь-якої організації, адже вони можуть призвести до втрати даних, простою в роботі та фінансових втрат. Тому захист кінцевих точок від цих кіберзагроз є критичним завданням.

У цьому розділі проаналізовано проблему захисту кінцевих точок від програм-вимагачів, підходи до її вирішення та існуючі на ринку рішення.

Аналіз проблеми:

програми-вимагачі стають дедалі більш витонченими та небезпечними;

вони можуть заразити будь-який пристрій, підключений до Інтернету;

зараження може призвести до втрати даних, простою в роботі та фінансових втрат.

Аналіз підходів:

Профілактика (запобігання зараженню пристроїв);

виявлення (виявлення заражених пристроїв);

реагування (нейтралізація загрози та відновлення даних).

Найефективніший підхід до захисту кінцевих точок ґрунтується на багатошаровому захисті, який поєднує в собі різні методи.

Аналіз рішень:

на ринку доступно багато рішень з захисту кінцевих точок від програм-вимагачів;

кожне рішення має свої власні сильні та слабкі сторони;

при виборі рішення важливо врахувати такі фактори, як розмір організації, тип даних, які зберігаються, та бюджет.

На основі проведеного аналізу можна зробити такі висновки:

захист кінцевих точок від програм-вимагачів є критичним завданням для будь-якої організації;

не існує універсального рішення, яке б підходило всім;

найефективніший підхід до захисту ґрунтується на багатошаровому захисті, який поєднує в собі різні методи;

при виборі рішення з захисту кінцевих точок важливо ретельно вивчити всі доступні варіанти та вибрати те, яке найкраще відповідає вашим потребам.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК НА БАЗІ MICROSOFT DEFENDER

2.1. Архітектура та компоненти рішення Microsoft Defender

Архітектура Microsoft Defender for Endpoint, послуги, яка дає змогу користувачам запобігати, виявляти, розслідувати та реагувати на складні загрози, що спрямовані на їхні пристрої (кінцеві точки). Як ключовий компонент Microsoft 365 Defender, вона поєднує можливості Defender for Endpoint, Defender for Office 365, Defender for Identity та Defender for Cloud Apps, пропонуючи інтегрований підхід до кібербезпеки. [10]

Розгялнемо основні компоненти архітектури.

Портал Microsoft 365 Defender: команди з безпеки використовують портал для доступу до даних Defender for Endpoint та взаємодії з кінцевими точками. Вони можуть досліджувати потенційні загрози, реагувати на порушення або покращувати свою безпекову позицію. Це місце, де відбувається аналіз безпеки. Портал надає інформаційні панелі, різноманітні звіти та різні види огляду окремих об'єктів. Аналітики безпеки можуть швидко перемикатися між різними даними.

Крім візуалізації даних, портал надає командам з безпеки багатий набір інструментів для розслідування інцидентів, таких як просунуте полювання, живий відгук та багато інших дій у відповідь. Портал пропонує численні функції, які полегшують роботу зайнятих аналітиків безпеки. Далі ми розглянемо сенсори кінцевих точок.

Рис.2.1. Функції Microsoft Defender for Endpoint

Датчики кінцевих точок (The Defender for Endpoint sensors): збирають події, пов'язані з безпекою, з підключених кінцевих точок і надсилають ці події до клієнтських орендарів. Для цього потрібне лише підключення до інтернету, тому сервіс підтримує майже будь-який можливий сценарій для пристроїв, що належать компанії. Команди з безпеки також можуть ініціювати дії на кінцевих точках, такі як збирання підозрілих файлів, ізоляція від мережі або запуск повного антивірусного сканування.

Відомі кінцеві точки в мережі, звісно, не є єдиною проблемою безпеки. Саме тому Defender for Endpoint надає можливість виявляти некеровані пристрої, які можуть бути присутніми в мережі і часто є джерелом шкідливої активності. Всі засоби безпеки Microsoft Defender for Endpoint на кінцевій точці генерують цінні події безпеки. Сюди входять управління загрозами та вразливостями, захист нового покоління, зменшення поверхні атаки, сенсори EDR та багато інших, а також сервіс оновлення.

Рис.2.2. Цінні події безпеки кінцевих точок

Однак команди з безпеки повинні ввімкнути та налаштувати деякі з цих засобів перед тим, як вони почнуть генерувати події. Клієнти можуть використовувати ці дані, які майже в режимі реального часу, для моніторингу, звітності, розслідувань та полювання на загрози. Крім того, сервіс використовує ці дані сенсорів для кореляції, виявлення порушень, видимості, аналітики безпеки та обміну сигналами з іншими службами Microsoft 365 Defender.

Рис.2.3. Цілі використання дані датчиків

Відповідно до *Microsoft Azure cloud*, кожен клієнт отримує спеціальний орендар Defender for Endpoint, повністю ізольований від інших орендарів. Звісно, це означає, що дані клієнтів ізольовані та захищені в межах їхніх орендарів. Доступ до цих даних можуть отримати лише клієнти через автентифікацію Azure Active Directory, а сам доступ відповідно реєструється.

В межах кожного орендаря є великий словник індикаторів атак (Indicators of Attack, IOA). Він включає евристику, поведінкові правила, машинне навчання та алгоритми виявлення аномалій, які виявляють підозрілі події, пов'язані з атаками, в даних датчиків.

Крім того, Defender for Endpoint використовує великі дані, машинне навчання, унікальний погляд на екосистему Windows та інтелектуальний графік безпеки для перетворення поведінкових сигналів на корисні виявлення та рекомендовані дії. Система автоматизації автоматично розпочинає розслідування та виправлення загроз тоді, коли служба генерує попередження.

Частина орендарів клієнтів є детонаційна камера для детального аналізу файлів. Це пісочниця, де команди безпеки можуть завантажувати підозрілі файли та отримувати зрозумілий звіт. Завдяки цьому методу можна досліджувати потенційні загрози з максимальною ефективністю та безпекою.

Defender for Endpoint безперебійно інтегрується з іншими службами безпеки Microsoft, такими як Defender for Office 365, Defender for Identity та Defender for Cloud Apps, пропонуючи єдиний підхід до кібербезпеки. Крім того, інтеграція з Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft Information Protection та Microsoft Endpoint Manager відкриває нові можливості для користувачів. Багатий набір API дозволяє інтегруватися з існуючою інфраструктурою безпеки, системами SIEM або системами тикетів, а також створювати власні робочі процеси безпеки. Крім того, клієнти мають можливість додавати власні дані про загрози, використовуючи API або інтерфейс консолі.

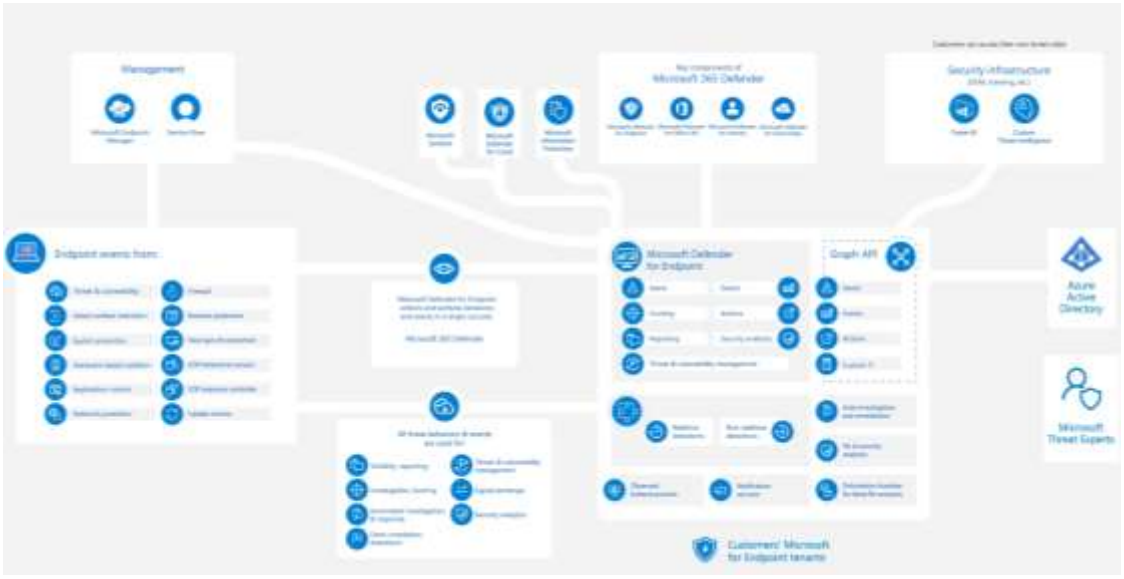

Рис.2.4. Загальна архітектура Microsoft Defender for Endpoint

Microsoft Defender for Endpoint - це корпоративна платформа безпеки кінцевих точок, розроблена для того, щоб допомогти корпоративним мережам запобігати, виявляти, досліджувати та реагувати на розширені загрози.

На наведеній нижче діаграмі наведено архітектуру та інтеграцію Microsoft Defender for Endpoint.

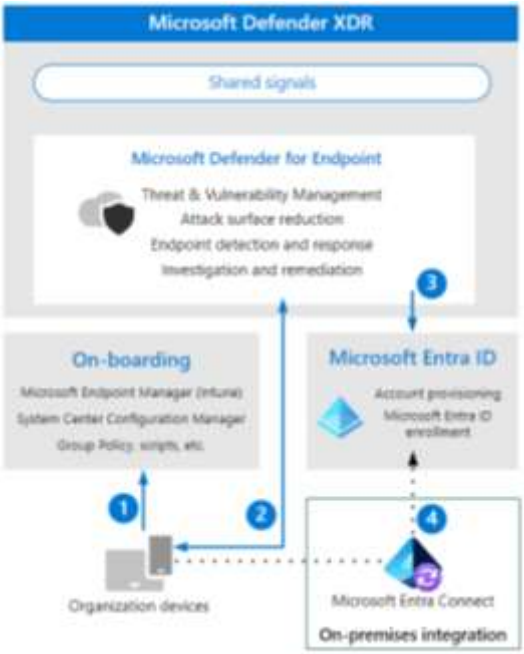

Рис.2.5. Архітектура та інтеграція Microsoft Defender

У наступній таблиці наведено опис ілюстрації.

Таблиця 2.1.

№	Опис
1	Пристрої підключаються за допомогою одного з підтримуваних інструментів керування.
2	Вбудовані пристрої надають дані сигналу Microsoft Defender for Endpoint і відповідають на них.
3	Керовані пристрої приєднуються та/або реєструються в Microsoft Entra ID.
4	Пристрої Windows, приєднані до домену, синхронізуються з Microsoft Entra ID за допомогою Microsoft Entra Connect.
5	Оповіщення, розслідування та реагування Microsoft Defender for Endpoint (MDE) тепер управляються в Microsoft Defender XDR.

2.2. Призначення та основні функції компонентів Microsoft Defender for Endpoint

Microsoft Defender for Endpoint є комплексним рішенням для захисту кінцевих точок, яке об’єднує різні компоненти для забезпечення всебічного захисту від сучасних загроз.

Microsoft Defender for Endpoint включає кілька компонентів, кожен з яких має свої конкретні призначення та функції. Розглянемо кожен з них детальніше з прикладами.

Threat and Vulnerability Management (TVM) спрямоване на виявлення та управління вразливостями в програмному забезпеченні та системних налаштуваннях організації. Це дозволяє командам безпеки оцінювати ризики та пріоритизувати заходи для усунення вразливостей, зменшуючи потенційні

загрози.[11]

Основні функції:

оцінка вразливостей: TVM сканує кінцеві точки на наявність вразливостей у встановленому програмному забезпеченні та системних налаштуваннях;

пріоритизація: Вразливості пріоритизуються на основі потенційного ризику, що дозволяє командам безпеки зосередитися на найбільш критичних загрозах;

рекомендації: TVM надає детальні рекомендації щодо усунення вразливостей, включаючи інформацію про необхідні патчі та налаштування систем.

Приклад: після виявлення вразливості в популярному програмному забезпеченні, TVM надає детальні інструкції для впровадження відповідного патчу, допомагаючи адміністраторам швидко закрити цю вразливість і зменшити ризик експлуатації.

Attack Surface Reduction (ASR) призначений для зменшення поверхні атаки шляхом застосування набору політик і правил, які обмежують можливість здійснення шкідливих дій на кінцевих точках.

Основні функції:

блокування підозрілих дій: ASR запобігає виконанню небезпечних дій, таких як запуск макросів в Office документах або створення підпроцесів, що можуть бути використані для атак;

фільтрація веб-контенту: блокує доступ до небезпечних веб-сайтів або типів контенту відповідно до політики організації;

Приклад: якщо хакер спробує використовувати макрос в Excel для запуску шкідливого коду, ASR блокує виконання цього макросу, запобігаючи потенційній атаці.

*Next-Generation Protection з*абезпечує захист від сучасних загроз, використовуючи підписи шкідливого ПЗ, евристичний аналіз і машинне

навчання для виявлення та блокування шкідливих програм у реальному часі.[12]

Основні функції:

реальний час: виявлення і блокування відомих і нових загроз у режимі реального часу.

евристика та машинне навчання: використання передових алгоритмів для аналізу поведінки файлів і процесів.

Приклад: під час відкриття зараженого файлу, Next-Generation Protection визначає його шкідливу природу на основі поведінкових ознак і блокує файл до того, як він зможе завдати шкоди.

Endpoint Detection and Response (EDR) постійно моніторить кінцеві точки для виявлення підозрілої активності та складних атак. Цей компонент дозволяє командам безпеки оперативно реагувати на інциденти.

Основні функції:

моніторинг активності: збирає і аналізує телеметрію з кінцевих точок;

автоматична відповідь: виявляє і реагує на підозрілу активність, автоматично вживаючи заходів для ізоляції та усунення загроз;

Приклад: якщо на комп'ютері користувача виявляється підозріла активність, наприклад, створення несанкціонованого завдання планувальника, EDR може автоматично ізолювати цей комп'ютер від мережі для запобігання поширенню загрози.

Automated Investigation and Remediation (AIR) автоматизує процеси розслідування інцидентів і застосування коригувальних заходів, зменшуючи час реакції на загрози.

Основні функції:

автоматизоване розслідування: використовує попередньо визначені сценарії для аналізу інцидентів;

автоматизоване виправлення: автоматично виконує дії для усунення загроз, такі як ізоляція пристрою або видалення шкідливого ПЗ.

Приклад: якщо система виявляє шкідливе ПЗ на одному з комп'ютерів, AIR може автоматично виконати повне сканування та видалити шкідливе ПЗ, відновлюючи нормальну роботу комп'ютера.

Microsoft Threat Experts надає розширену підтримку з боку експертів з кібербезпеки, які допомагають виявляти та реагувати на складні загрози.

Основні функції:

експертна допомога: доступ до фахівців Microsoft, які можуть допомогти з аналізом та розслідуванням інцидентів;

проактивне виявлення загроз: фахівці допомагають виявляти та реагувати на складні загрози, які можуть бути пропущені автоматизованими системами.

Приклад: у випадку складної атаки, яка потребує глибокого аналізу, команди безпеки можуть звернутися до Microsoft Threat Experts для отримання рекомендацій та допомоги у розслідуванні інциденту.

Ці компоненти працюють разом, забезпечуючи всебічний захист кінцевих точок, допомагаючи організаціям ефективно виявляти, аналізувати та реагувати на загрози.

Рис.2.7. Компоненти Microsoft Defender

2.3. Процеси функціонування рішення Microsoft Defender for Endpoint

Microsoft Defender for Endpoint починає свою роботу з безперервного моніторингу всіх кінцевих точок (комп'ютерів, серверів, мобільних пристроїв), які підключені до системи. Цей процес включає збір телеметрії, яка містить дані про активність файлів, мережеві підключення, системні події, поведінкові патерни та інші дії. Дані надсилаються до хмарного середовища Microsoft для подальшого аналізу. Цей процес забезпечує збір інформації для виявлення потенційних загроз у реальному часі.

Після збору дані аналізуються за допомогою машинного навчання, евристичних методів і спеціалізованих алгоритмів. Defender for Endpoint використовує великий обсяг даних, отриманих з глобальної мережі телеметрії, для побудови моделей виявлення загроз. Система також інтегрується з Microsoft Intelligent Security Graph, що дозволяє використовувати інформацію про загрози з різних джерел і покращувати точність виявлення.

У разі виявлення загрози, Defender for Endpoint генерує сповіщення та автоматично вживає заходів для нейтралізації загрози. Ці заходи можуть включати ізоляцію зараженого пристрою від мережі, запуск повного сканування на наявність шкідливих програм або видалення шкідливих файлів. Всі ці дії виконуються автоматично або під керівництвом аналітиків безпеки, які можуть переглядати і коригувати процеси в разі потреби.

Аналітики безпеки можуть використовувати інструменти для детального аналізу та полювання на загрози. Advanced Hunting дозволяє створювати власні запити на основі Kusto Query Language (KQL) для глибокого аналізу телеметрії і виявлення потенційних загроз. Цей інструмент дозволяє проводити комплексні розслідування, включаючи аналіз поведінкових патернів і виявлення аномалій.

Компонент Automated Investigation and Remediation (AIR) використовує AI і машинне навчання для автоматичного розслідування інцидентів та застосування

виправних заходів. Це дозволяє значно скоротити час реагування на загрози і підвищити ефективність захисту. Наприклад, у разі виявлення підозрілого файлу AIR може автоматично запустити його аналіз у пісочниці (sandbox), видалити його або ізолювати заражений пристрій.

Для складних випадків, які потребують глибшого аналізу, організації можуть звертатися до Microsoft Threat Experts. Ця послуга надає доступ до експертів з кібербезпеки, які допомагають виявляти, аналізувати та реагувати на складні загрози. Експерти можуть надавати рекомендації, допомагати у розслідуваннях і забезпечувати проактивне виявлення загроз, що дозволяє організаціям краще захищати свої ресурси.

Ці компоненти працюють разом, забезпечуючи всебічний захист кінцевих точок, допомагаючи організаціям ефективно виявляти, аналізувати та реагувати на загрози.

Детальніше розглянемо одну із найновіших функцій Microsoft Defender for Endpoint. Захисні програми потребують усіх можливих переваг у боротьбі з програмами-вимагачами. Клієнти Microsoft Defender for Endpoint тепер можуть автоматично припиняти атаки, керовані людиною, такі як програми-вимагачі, на ранніх етапах без необхідності впровадження додаткових засобів. Організаціям достатньо лише підключити свої пристрої до Defender for Endpoint, щоб скористатися перевагами цієї технології з розширеним виявленням та реагуванням (XDR), яка використовує штучний інтелект і тепер доступна ще більшій кількості клієнтів.

Автоматичне припинення атак (Automatic attack disruption) використовує сигнали з усіх робочих навантажень Microsoft Defender (ідентифікація, кінцеві точки, електронна пошта та SaaS-додатки), щоб зупиняти складні атаки з високою точністю. Якщо початок атаки, керованої людиною, виявлено на одному пристрої, система одночасно зупинить кампанію на цьому пристрої та захистить всі інші пристрої в організації. У нападника не залишиться жодних можливостей

для продовження атаки.[13]

Атака припинення досягає цього результату, ізолюючи скомпрометованих користувачів на всіх пристроях, щоб випередити нападників, перш ніж вони зможуть діяти шкоду, наприклад, використовуючи облікові записи для бічного руху, крадіжки облікових даних, викрадення даних і віддаленого шифрування. Ця функція, що ввімкнена за замовчуванням, виявляє, чи має скомпрометований користувач пов'язану активність з будь-яким іншим кінцевим пристроєм, і негайно припиняє всю вхідну та вихідну комунікацію, фактично ізолюючи його. Навіть якщо користувач має найвищий рівень дозволів і зазвичай не підпадає під сферу дії засобів безпеки, нападник все одно буде обмежений у доступі до будь-якого пристрою в організації. Завдяки такому децентралізованому захисту, переривання атаки врятувало 91 відсоток цільових пристроїв від спроб шифрування.

До цього часу раннє виявлення таких кампаній становило значні виклики для команд з безпеки, оскільки нападники зазвичай маскують свої дії під звичайну поведінку користувачів. І хоча інші постачальники можуть виявляти ці техніки атак, лише Microsoft Defender може автоматично їх зупиняти цілодобово, навіть коли ваша команда з безпеки може бути офлайн. Завдяки широкому спектру сигналів і глибокому аналізу поведінки користувачів від Microsoft, команди з безпеки тепер мають потужний новий інструмент для ефективного зупинення складних атак програм-вимагачів у великих масштабах.

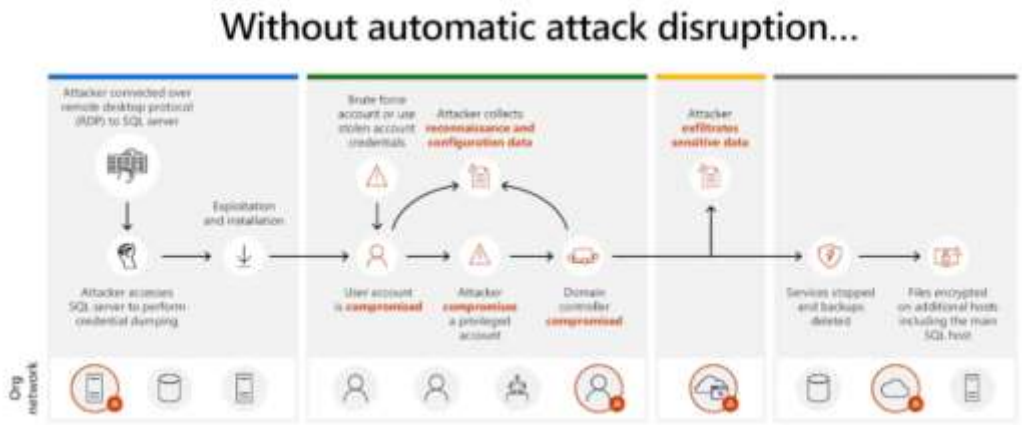

Рис.2.8. Атака програмою-вимагачем без автоматичного припинення атак

Рис.2.9. Атака програмою-вимагачем з автоматичним припиненням атак

Ця функція приховано порушувала атаки на реальні організації з 2022 року. Наприклад, у серпні 2023 року хакери зламали пристрої в медичній дослідницькій лабораторії. На кону були життя людей та мільйони доларів, витрачених на дослідження, тому потенційний викуп за зашифровані дані був дуже високим. Під час атаки хакери вручну виконували команди та використовували протокол віддаленого робочого столу для підключення до одного з SQL-серверів лабораторії. Потім вони здійснили дамп облікових даних

— перший крок до отримання доступу до 55 інших пристроїв у мережі. Проте, хакери не знали, що підключення до SQL-сервера стане останнім кроком у їхній кампанії з програмою-вимагачем. Їх негайно відключили від усіх пристроїв лабораторії, і аналітикам з безпеки навіть не довелося втручатися.

Ця дослідницька лабораторія була однією з небагатьох клієнтів Microsoft, які брали участь у тестуванні цієї новітньої технології. З серпня 2023 року понад 6500 пристроїв були захищені від шифрування під час атак програм-вимагачів, здійснених такими групами хакерів, як BlackByte та Akira, а також найманими червоними командами.

Поговоримо про важливе нововведення таке, як *автоматичне переривання атак,* яке зрівнює шанси на захист.

Програми-вимагачі — один з найпоширеніших типів атак, з якими стикаються організації. У 2022 році в усьому світі було зафіксовано майже 236,7 мільйона атак програм-вимагачів, а прогнозовані витрати до 2031 року можуть зрости до 265 мільярдів доларів США щорічно. З огляду на збільшення обсягу та впливу таких атак, як програми-вимагачі, аналітикам з безпеки потрібна автоматизація, яку пропонує переривання атак, щоб ефективно масштабувати свій захист.

Щоб допомогти захисникам у цій нерівній битві, у листопаді 2022 року Microsoft Defender запровадив автоматичне переривання атак: новітню технологію, яка зупиняє атаки з швидкістю машини, використовуючи кореляцію сигналів з різних доменів в один інцидент високої точності. У поєднанні з автоматизованими можливостями реагування на інциденти, Microsoft Defender є єдиною платформою XDR, яка захищає від атак програм-вимагачів як на рівні організації, так і на рівні пристроїв.

Окрім програм-вимагачів, переривання атак охоплює найпоширеніші й найскладніші атаки, такі як компрометація бізнес-електронної пошти та атаки посередника. Ці сценарії включають поєднання різних векторів атак, таких як

кінцеві точки, електронна пошта, ідентифікаційні дані та додатки, що створює значні труднощі для команд з безпеки у виявленні джерела атаки. Більшість постачальників засобів безпеки не мають достатньо точних сигналів, щоб навіть визначити факт атаки, не кажучи вже про можливість її переривання. Автоматичне переривання атак вирішує цю проблему, надійно виявляючи та зупиняючи атаки у джерелі, надаючи захисникам час для реагування до того, як зловмисник зможе завдати шкоди.

Як кажуть у сфері безпеки, питання не в тому, чи буде порушено вашу систему, а коли це станеться. Захист кінцевих точок вимагає багаторівневого підходу, включаючи виправлення вразливостей, використання антивірусів нового покоління для нейтралізації загроз на периметрі, автоматичне дослідження та реагування для усунення загроз на рівні окремих пристроїв і автоматичне переривання атак на рівні організації для обмеження поширення атаки.

Ефективність та охоплення переривання атак збільшуються з кожним продуктом, інтегрованим у Microsoft Defender. Хоча більшість атак програм-вимагачів відбувається на кінцевих точках, важливо розгорнути весь комплекс заходів безпеки для захисту додатків, ідентифікаційних даних, електронної пошти та співпраці від поширених сценаріїв, таких як компрометація бізнес-електронної пошти, атаки посередника та майбутні загрози. Це дозволяє організаціям отримувати користь не лише від можливостей переривання атак, але й від усіх багатих функцій для найважливіших завдань безпеки.

Нові можливості ізоляції користувачів допоможуть клієнтам будь-якого розміру автоматично захищатися від атак програм-вимагачів. Для малого та середнього бізнесу, який часто не має доступу до складних рішень або експертів з безпеки, ця функція, увімкнена за замовчуванням, забезпечує захист від новітніх загроз, дозволяючи їм зосередитися на веденні свого бізнесу.

Звідомлення про архітектуру, компоненти та процеси функціонування

Microsoft Defender for Endpoint дають розуміння про те, як це рішення працює та яким чином воно захищає комп'ютерні системи. Ці аспекти допомагають підвищити ефективність захисту та реагування на загрози в сучасному інформаційному середовищі.

Архітектура та компоненти рішення Microsoft Defender:

Microsoft Defender for Endpoint складається з різних компонентів, включаючи агенти, хмарні служби та аналітичні інструменти;

агенти розгортаються на кінцевих пристроях і забезпечують моніторинг та захист в реальному часі;

хмарні служби надають централізоване керування, аналізують дані та надають інтелектуальні рекомендації щодо виявлення та реагування на загрози.

Призначення та основні функції компонентів Microsoft Defender for Endpoint:

основне призначення рішення полягає в захисті кінцевих пристроїв від різноманітних кіберзагроз, включаючи віруси, шкідливі програми та атаки з використанням вразливостей;

компоненти виявляють та блокують загрози в реальному часі, забезпечуючи безпеку як на рівні мережі, так і на рівні кінцевих пристроїв;

додаткові функції включають аналіз поведінки, виявлення аномалій та автоматизовану реакцію на інциденти.

Процеси функціонування рішення Microsoft Defender for Endpoint:

рішення надає неперервний моніторинг стану безпеки кінцевих пристроїв, здатність реагувати на загрози в реальному часі та відновлювати пошкоджені системи;

процес аналізує дані з кінцевих пристроїв та хмарних служб, використовуючи розумові технології для виявлення та аналізу потенційних загроз;

реакція на загрози може включати автоматичне блокування підозрілих дій,

ізоляцію кінцевих пристроїв та надання рекомендацій щодо подальших заходів.

Загалом, Microsoft Defender for Endpoint є комплексним рішенням для захисту кінцевих пристроїв, яке поєднує в собі агентів, хмарні служби та аналітичні інструменти для забезпечення безпеки в сучасному цифровому середовищі.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ВІД ПРОГРАМ-ВИМАГАЧІВ

3.1. Варіант розгортання системи захисту кінцевих точок на базі Microsoft Defender

Microsoft Defender для серверів у Microsoft Defender для хмарної інфраструктури надає виявлення загроз та передові захисні засоби для Windows та Linux-машин, що працюють в Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP) та в локальних середовищах. Цей план включає інтегровану ліцензію для Microsoft Defender для кінцевих точок, базові налаштування безпеки та оцінки рівня операційної системи, сканування вразливостей, адаптивний контроль застосунків (AAC), моніторинг цілісності файлів (FIM) та багато іншого. [14]

Microsoft Defender для серверів має автоматичну, вбудовану інтеграцію з Microsoft Defender для кінцевих точок. Захистити кінцеві точки варто за допомогою інтегрованого рішення EDR від Defender для хмарної інфраструктури: Microsoft Defender для кінцевих точок. З цією активованою інтеграцією надається доступ до виявлених вразливостей через менеджмент вразливостей Microsoft Defender.

Microsoft Defender для серверів пропонує два варіанти планів з різним рівнем захисту та власною вартістю. Дізнайтись більше про ціни Microsoft Defender для хмарної інфраструктури можна на сторінці тарифікації.

Існує декілька варіантів розгортання системи захисту кінцевих точок на базі Microsoft Defender (MDE):

1. Локальне розгортання.

2. Хмарне розгортання.

3. Гібридне розгортання.

Щоб обрати план, яий правильно підійде тій чи іншій організації/особистій мережі тощо, вато розглянути переваги та недоліки кожного варіанту розгортання системи захисту кінцевих точок на базі Microsoft Defender (MDE).

Наступна таблиця наочно покаже для якого типу організацій підходить той чи інший варіант.

Таблиця 3.1.

Переваги, недоліки і призначення варіантів розгортання системи захисту

Варіант	Переваги	Недоліки	Призначення
Локальне розгортання	1. **Більший контроль:** Клієнт має повний контроль над розгортанням та адмініструванням MDE. 2. **Від'єднаність від Інтернету:** MDE можна розгорнути в автономному режимі, що може бути важливо для організацій з жорсткими вимогами до безпеки. 3. **Гнучкість:** Клієнт може налаштувати	1. **Складність:** Локальне розгортання MDE може бути складнішим, ніж розгортання в хмарі. 2. **Витрати:** Потрібно буде придбати та підтримувати локальний сервер. 3. **Обмежена масштабованість:** Локальне розгортання може бути важко	1. Великі та складні організації. 2. Організації з жорсткими вимогами до безпеки. 3. Організації, які не хочуть залежати від хмарних служб.

	MDE відповідно до своїх потреб.	масштабувати для великих організацій.	
Хмарне розгортання	1. **Простота:** Розгортання MDE в хмарі дуже просте. 2. **Масштабованість:** MDE можна легко масштабувати для великих організацій. 3. **Низькі витрати:** Не потрібно купувати та підтримувати локальний сервер. 4. **Автоматичні оновлення:** MDE автоматично оновлюється Microsoft.	1. **Менший контроль:** Клієнт має менший контроль над розгортанням та адмініструванням MDE, ніж при локальному розгортанні. 2. **Залежність від Інтернету:** MDE потребує підключення до Інтернету для роботи. 3. **Безпека:** Деякі організації можуть мати сумніви щодо безпеки хмарного розгортання.	1. Малі та середні організації. 2. Організації, які не мають можливості керувати локальним сервером. 3. Організації, які хочуть швидко та легко розгорнути MDE.
Гібридне розгортання	1. **Гнучкість:** Гібридне розгортання дає гнучкість розгортання	1. **Складність:** Гібридне розгортання може	1. Великі та складні організації з

	MDE як локально, так і в хмарі. 2. **Контроль:** Клієнт має більший контроль над локальною частиною розгортання MDE. 3. **Масштабованість:** Клієнт може масштабувати хмарну частину розгортання MDE для великих організацій.	бути складнішим, ніж локальне або хмарне розгортання. 2. **Витрати:** Потрібно буде придбати та підтримувати локальний сервер, а також платити за хмарні послуги.	локальними та хмарними ресурсами. 2. Організації, які хочуть мати більший контроль над локальною частиною розгортання MDE.

Щоб увімкнути план Defender для серверів для захисту всіх машин у підписці Azure, обліковому запису AWS або проекті GCP, слід виконати такі кроки:

1. Увійти в портал Azure.
2. Знайти та вибрати Microsoft Defender для хмарної інфраструктури.
3. У меню Defender для хмарної інфраструктури вибрати Налаштування середовища.
4. Вибрати відповідну підписку Azure, обліковий запис AWS або проект GCP.
5. На сторінці планів Defender перемістити перемикач Servers в положення Увімкнено.

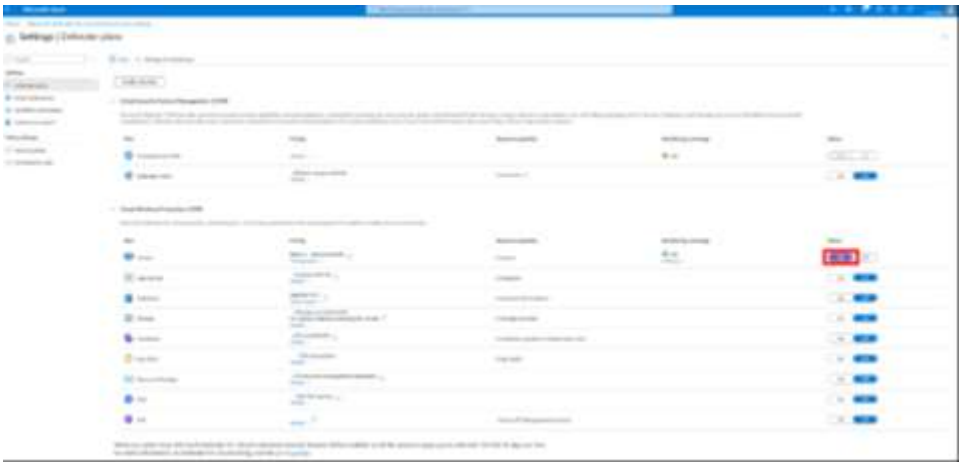

Рис.3.1. Увімкнення перемикача Servers

Після увімкнення плану у з'являється можливість налаштувати функції плану відповідно до потреби організації. При увімкненні Defender для серверів у підписці, покриття не розширюється на підключену робочу область. Клієнту потрібно увімкнути Defender для серверів на рівні робочої області Log Analytics.

Після увімкнення плану Defender для серверів буде запропоновано вибрати, який план - План 1 або План 2 - увімкнути. Існують два плани, які можна обрати, вони надають різні рівні захисту для ресурсів.

Варто порівняти доступні функції, що надаються кожним планом.

Рис.3.2. Порівняння двох планів з різним функціоналом

Щоб обрати план Defender для серверів потрібно:

увійти в портал Azure;

знайти та вибрати Microsoft Defender для хмарної інфраструктури;

у меню Defender для хмарної інфраструктури вибрати Налаштування середовища;

вибрати відповідну підписку Azure, обліковий запис AWS або проект GCP;

вибрати Змінити план.

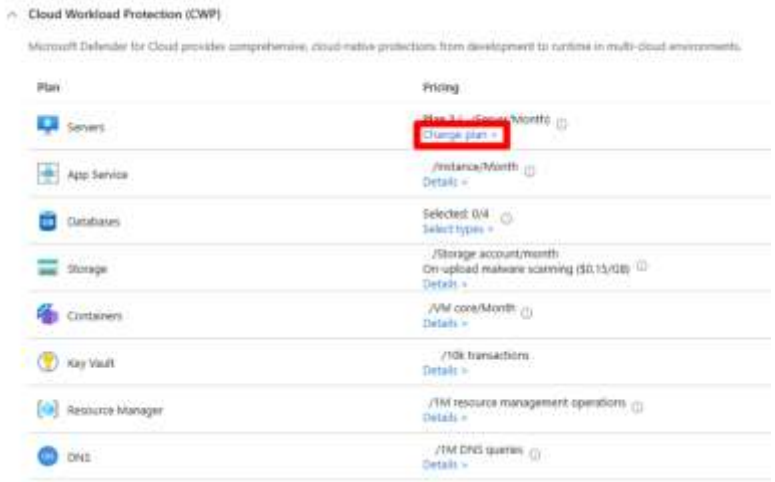

Рис.3.3. Зміна плану

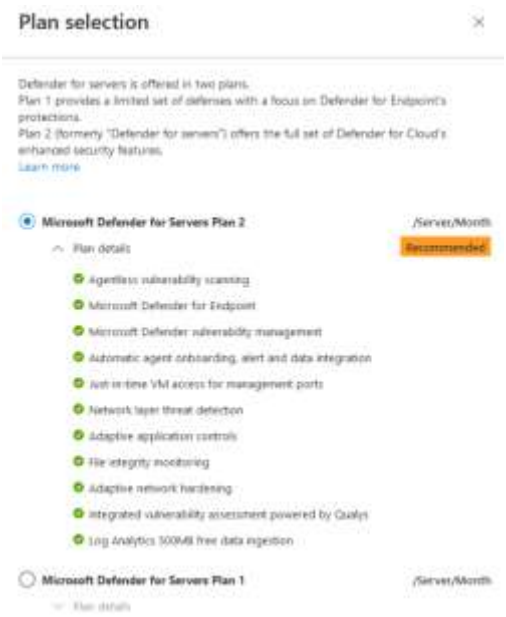

Рис.3.4. Вибір плану

Після увімкнення плану можна налаштувати його функції відповідно до потреб.

Коли увімкнено Defender для серверів у підписці, охоплення, яке надається Defender для серверів, автоматично не поширюється на робочі області Log Analytics. Для цього потрібно увімкнути Defender для серверів для кожної робочої області окремо. Defender для серверів у робочих областях підтримує лише План 2.

Щоб увімкнути Defender для серверів у робочій області Log Analytics потрібно:

увійти в портал Azure;

знайти та вибрати Microsoft Defender для хмарної інфраструктури;

у меню Defender для хмарної інфраструктури обрати Налаштування середовища;

вибрати відповідну робочу область;

перемістити перемикач для плану серверів в положення Увімкнено.

Рис.3.5. Увімнення Defender для серверів

Увімкнення Defender для серверів у робочій області Log Analytics не забезпечує всіх доступних засобів захисту. Також можливо захистити робочі області Log Analytics за допомогою Foundational CSPM та SQL серверів на машинах.

Щоб захистити всі існуючі та майбутні ресурси, рекомендовано увімкнути Defender for Servers для всієї підписки на Azure.

Можна виключити певні ресурси або керувати конфігураціями безпеки на нижчому рівні ієрархії, увімкнувши план Defender for Servers на рівні ресурсу. Ввімкнути план можна на рівні ресурсу за допомогою REST API або в масштабі.

Серед підтримуваних типів ресурсів:

віртуальні машини Azure;

локальна з Azure Arc;

масштаб віртуальної машини Azure встановлює Flex.

Можливість увімкнути або вимкнути Defender for Servers на рівні ресурсу доступна виключно через REST API.

Увімкнувши план, можна налаштувати функції плану відповідно до потреб.

3.2. Порядок проведення розслідування інцидентів в рішенні Microsoft Defender

Для проведення розслідування інцидентів у Microsoft Defender, необхідно дотримуватись наступного процесу:

Спершу виявляють інциденти за допомогою автоматичних інструментів в Microsoft Defender. Ці інструменти включають аналітику загроз, автоматичні розслідування та оповіщення, що допомагають визначити ймовірні загрози і визначити їх пріоритет. [15]

Сповіщення є основою всіх інцидентів і вказують на появу зловмисних або підозрілих подій у вашому оточенні. Сповіщення зазвичай є частиною ширшої атаки та надають підказки про інцидент.

Інцидент на порталі Microsoft Defender — це набір пов’язаних сповіщень і пов’язаних даних, які складають історію атаки. Це також файл справи, який ваш SOC може використовувати для розслідування цієї атаки та управління, впровадження та документування відповіді на неї.

Служби Microsoft Sentinel і Microsoft Defender створюють сповіщення, коли виявляють підозрілу чи зловмисну подію чи дію. Окремі сповіщення надають цінні докази завершеної або поточної атаки. Проте все більш поширені та складні атаки зазвичай використовують різноманітні методи та вектори проти різних типів активів, таких як пристрої, користувачі та поштові скриньки. Результатом є численні сповіщення з різних джерел для кількох активів у вашій цифровій власності.

У Microsoft Defender XDR пов'язані сповіщення об'єднуються, щоб створити інциденти. Інциденти завжди надають ширший контекст атаки, однак аналіз сповіщень може бути цінним, коли потрібен глибший аналіз.

У *черзі сповіщень* відображається поточний набір сповіщень. Ви потрапляєте до черги сповіщень у розділі *Інциденти та сповіщення* > *Сповіщення* під час швидкого запуску порталу Microsoft Defender.

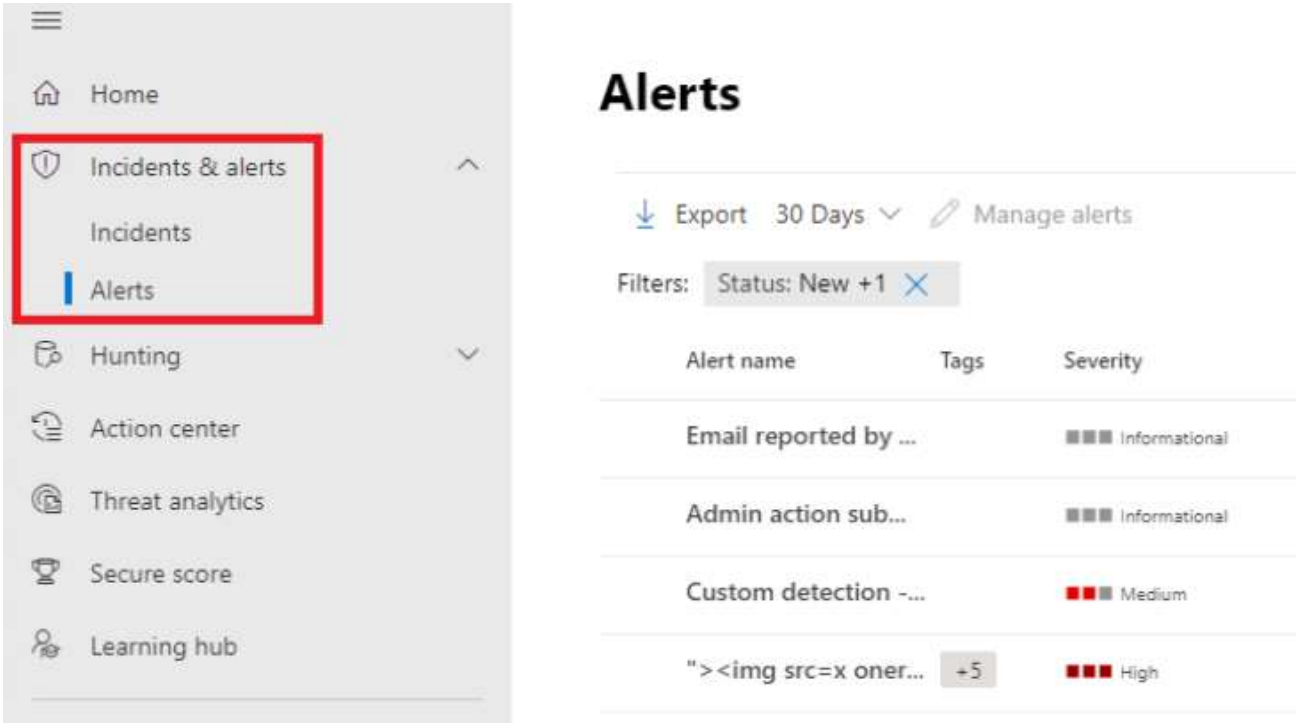

Рис.3.6. Розділ Сповіщення

Тут з'являються сповіщення від різних рішень безпеки Microsoft, як-от

Microsoft Defender для кінцевої точки, Microsoft Defender для Office 365 і Microsoft Defender XDR.

За замовчуванням у черзі сповіщень на порталі Microsoft Defender відображаються нові та поточні сповіщення за останні 30 днів. Останнє сповіщення знаходиться у верхній частині списку, тому ви можете побачити його першим.

У черзі сповіщень за замовчуванням ви можете вибрати *«Фільтр»*, щоб побачити панель *фільтрів*, у якій можна вказати підмножину сповіщень. Ось приклад.

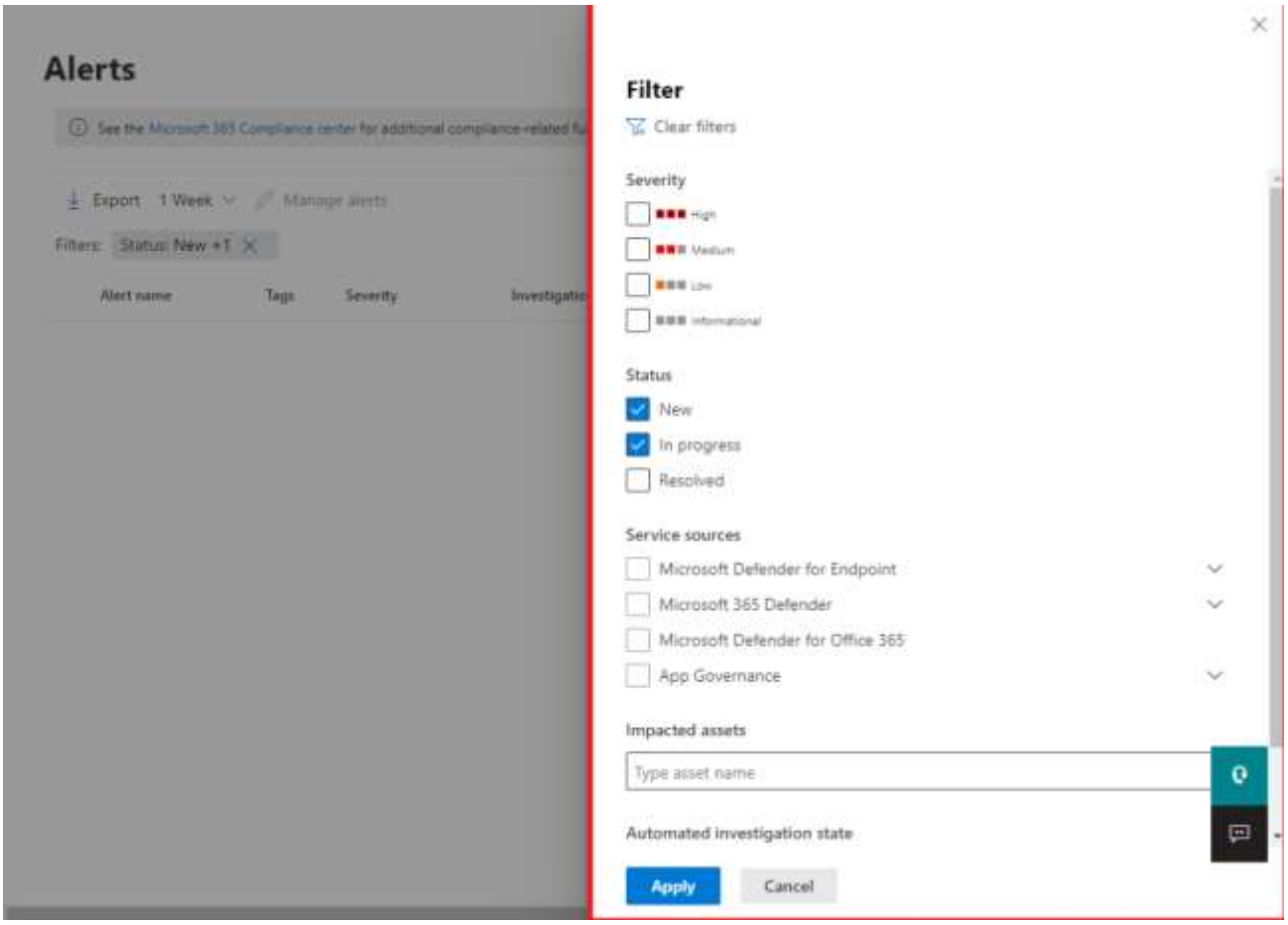

Рис.3.7. Панель фільтрів

В Microsoft Defender ви можете фільтрувати оповіщення за кількома критеріями для більш ефективного управління інцидентами та розслідуваннями.

Ці критерії включають:

важливість (severity): дозволяє фільтрувати оповіщення за рівнем серйозності загрози, наприклад, висока, середня або низька важливість. Це допомагає пріоритезувати розслідування найважливіших загроз;

статус (status): можливість фільтрувати оповіщення за їх поточним статусом, таким як активні, закриті або в очікуванні дії. Це полегшує відстеження ходу розслідування і виконання необхідних дій;

джерела сервісів (service sources): фільтрація за джерелами сервісів дозволяє вам бачити оповіщення, що надходять з різних частин системи, таких як Microsoft Defender for Endpoint, Microsoft Defender for Office 365 тощо;

об’єкти (entities): допомагає фільтрувати оповіщення за затронутими об’єктами, такими як пристрої, користувачі або поштові скриньки. Це корисно для розуміння, які ресурси були піддані впливу загрози;

стан автоматичного розслідування (automated investigation state): можливість фільтрувати оповіщення за станом автоматичного розслідування, щоб побачити, які оповіщення вже оброблені автоматично, а які ще потребують втручання.

Ці фільтри дозволяють швидко звузити область пошуку та сфокусуватися на найважливіших аспектах інциденту, що значно спрощує процес розслідування та реагування на загрози.

Оскільки кожне з окремих сповіщень розповідає лише частину історії, а групування окремих сповіщень вручну, щоб отримати інформацію про атаку, може бути складним і трудомістким, уніфікована операційна платформа безпеки автоматично визначає пов’язані сповіщення як від Microsoft Sentinel, так і від Microsoft Defender XDR — і об’єднує їх та пов’язану з ними інформацію в інцидент.[16]

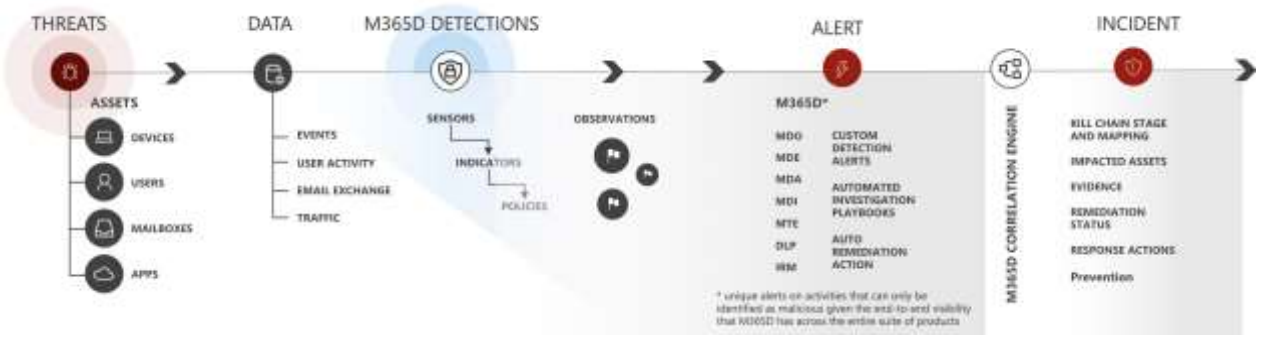

Рис.3.8. Об’єднання компонентів у інцидент

Після ідентифікації інциденту проводиться аналіз його компонентів, таких як атакуючі дії, затронуті ресурси (пристрої, користувачі, поштові скриньки) та інші пов'язані оповіщення. Цей аналіз включає перегляд "історії атаки", що відображає хронологію подій та взаємозв'язок між різними елементами атаки.

Групування пов’язаних сповіщень за інцидентом дає повне уявлення про атаку. Наприклад, можна побачити:

звідки почався напад;

яка тактика була використана;

як далеко зайшла атака на вашу цифрову нерухомість;

масштаб атаки, наприклад, скільки пристроїв, користувачів і поштових скриньок було вражено;

усі дані, пов’язані з атакою.

Уніфікована платформа операцій безпеки на порталі Microsoft Defender містить методи автоматизації сортування, розслідування та вирішення інцидентів і надання допомоги в них.

Microsoft Copilot у Defender використовує штучний інтелект для підтримки аналітиків у складних і трудомістких щоденних робочих процесах, включаючи наскрізне розслідування інцидентів і реагування з чітко описаними історіями атак, покроковими дієвими вказівками щодо виправлення та зведеними звітами про інциденти, природною мовою Пошук KQL і експертний аналіз коду —

оптимізація ефективності SOC у даних Microsoft Sentinel і Defender XDR.

Ця можливість є доповненням до інших функцій на основі штучного інтелекту, які Microsoft Sentinel привносить в уніфіковану платформу, у сферах аналітики поведінки користувачів і об’єктів, виявлення аномалій, багатоетапного виявлення загроз тощо.

Автоматизоване припинення атак використовує сигнали високої достовірності, зібрані з Microsoft Defender XDR і Microsoft Sentinel, щоб автоматично припиняти активні атаки на швидкості машини, стримуючи загрозу та обмежуючи вплив.

Якщо ввімкнено, Microsoft Defender XDR може автоматично досліджувати та вирішувати сповіщення з джерел Microsoft 365 і Entra ID за допомогою автоматизації та штучного інтелекту. Ви також можете виконати додаткові кроки для усунення атаки.

Правила автоматизації Microsoft Sentinel можуть автоматизувати сортування, призначення та керування інцидентами, незалежно від їх джерела. Вони можуть застосовувати теги до інцидентів на основі їх вмісту, придушувати шумні (хибнопозитивні) інциденти та закривати вирішені інциденти, які відповідають відповідним критеріям, вказуючи причину та додаючи коментарі.

У Microsoft Defender керування інцидентами здійснюється через розділ "Investigation & response" у меню швидкого доступу порталу. Для доступу до інцидентів та оповіщень необхідно перейти до розділу "Incidents & alerts" і обрати "Incidents".

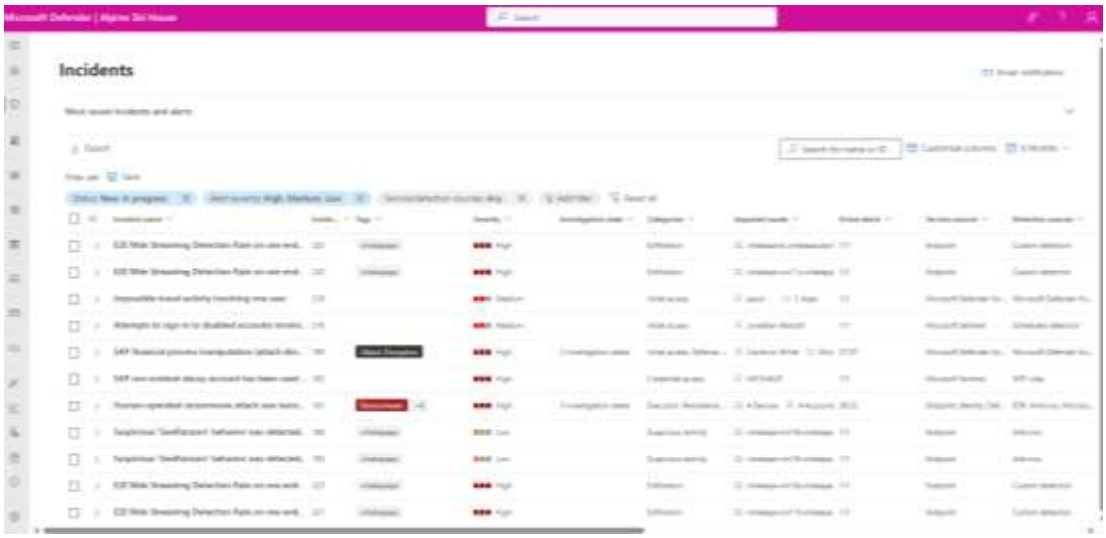

Рис.3.9. Розділ Incidents

Вибір назви інциденту відображає сторінку інциденту, починаючи з повної *історії атаки* інциденту, включаючи:

сторінка сповіщень у межах інциденту: обсяг сповіщень, пов'язаних із інцидентом, і інформація про них на одній вкладці;

графік: візуальне представлення атаки, яке з'єднує різні підозрілі об'єкти, які є частиною атаки, з об'єктами активів, які складають цілі атаки, наприклад користувачів, пристроїв, програм і поштових скриньок.

Користувач може переглядати активи та інші деталі сутності безпосередньо з графіка та діяти на них за допомогою варіантів відповіді, як-от вимикання облікового запису, видалення файлу чи ізоляції пристрою.

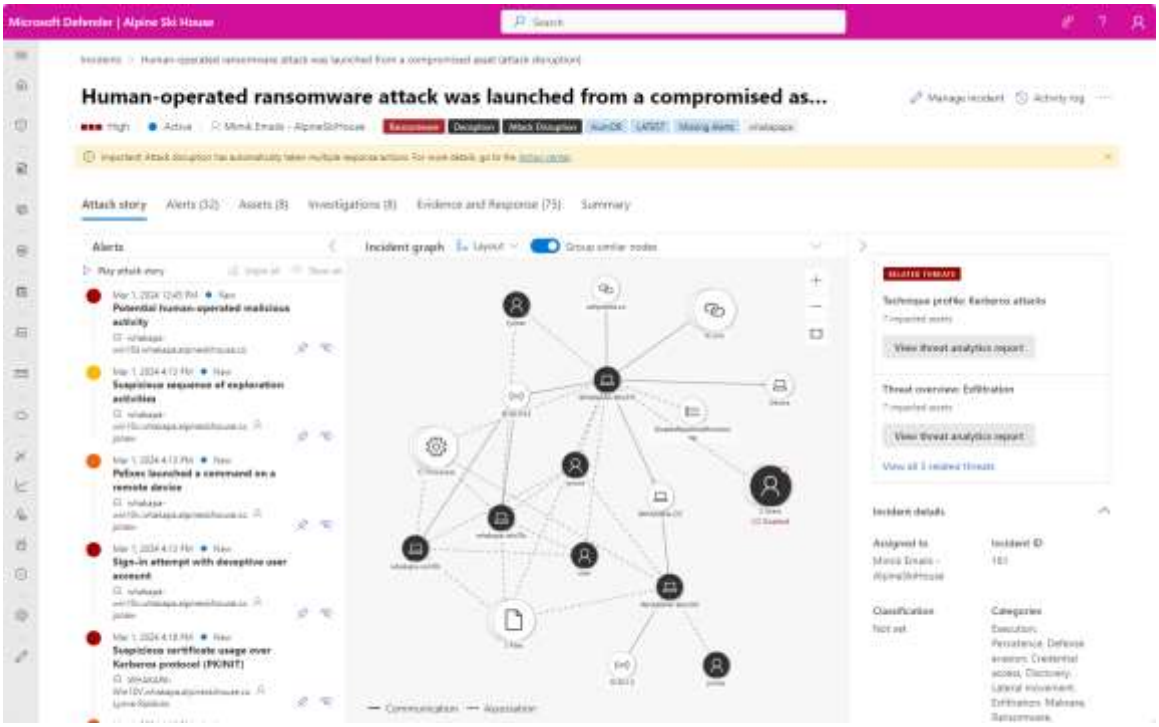

Рис.3.10. Сторінка інциденту

Сторінка інциденту складається з таких вкладок:

Історія нападу: як згадувалося вище, ця вкладка містить хронологію атаки, включаючи всі сповіщення, об’єкти активів і вжиті дії з усунення;

Оповіщення: усі сповіщення щодо інциденту, їх джерела та інформація;

Активи: усі активи (захищені об’єкти, такі як пристрої, користувачі, поштові скриньки, програми та хмарні ресурси), які були визначені як частина інциденту або пов’язані з ним;

Розслідування: усі автоматизовані розслідування, ініційовані сповіщеннями про інцидент, включаючи статус розслідувань та їх результати;

Докази та відповідь: усі підозрілі об’єкти в сповіщеннях про інцидент, які є доказами, що підтверджують історію нападу. Ці сутності можуть включати IP-адреси, файли, процеси, URL-адреси, ключі та значення реєстру тощо.

*Резюме: к*оротний огляд активів, пов’язаних зі сповіщеннями.

Ось приклад робочого процесу для реагування на інциденти в Microsoft 365

за допомогою порталу Microsoft Defender.

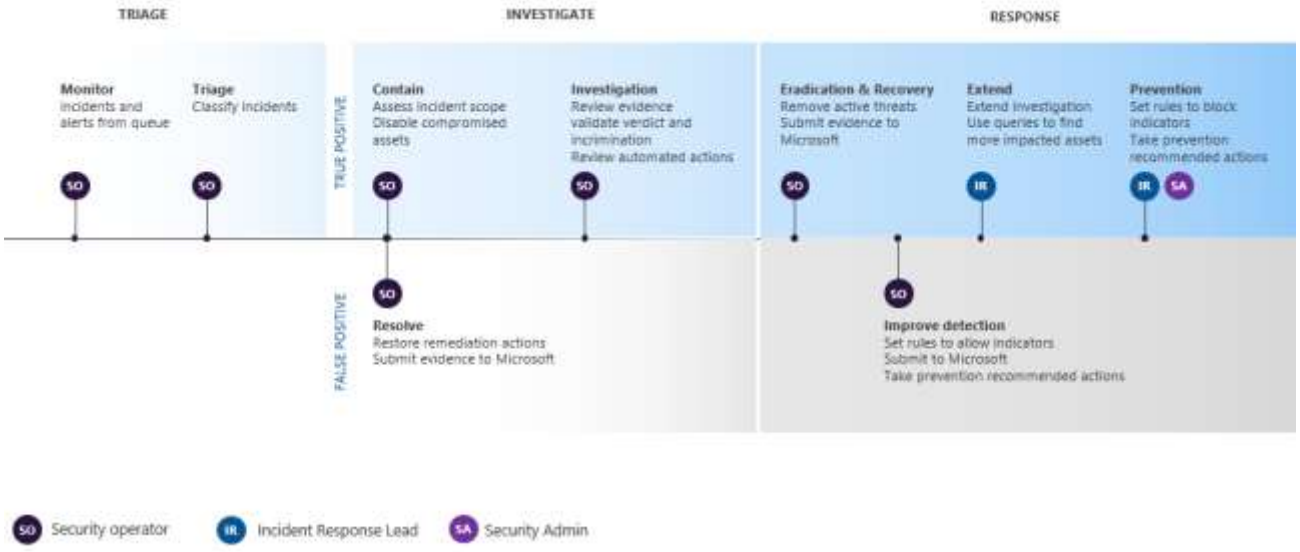

Рис.3.11. Приклад робочого процесу для реагування на інциденти

На постійній основі визначайте інциденти з найвищим пріоритетом для аналізу та вирішення в черзі інцидентів і готуйте їх до реагування. Це поєднання:

сортування для визначення інцидентів з найвищим пріоритетом за допомогою фільтрації та сортування черги інцидентів;

управління інцидентами, змінюючи їх назву, призначаючи їх аналітику та додаючи теги та коментарі.

Користувач може використовувати правила автоматизації Microsoft Sentinel, щоб автоматично сортувати та керувати (і навіть реагувати) на деякі інциденти під час їх створення, усуваючи найпростіші для обробки інциденти, які займають місце у черзі.

Після ідентифікації інциденту проводиться аналіз його компонентів, таких як атакуючі дії, затронуті ресурси (пристрої, користувачі, поштові скриньки) та інші пов'язані оповіщення. Цей аналіз включає перегляд "історії атаки", що відображає хронологію подій та взаємозв'язок між різними елементами атаки.

Наступним кроком є виконання розслідувань, які можуть бути автоматичними або ручними. Автоматичні розслідування зазвичай виявляють та

нейтралізують загрози, проте в деяких випадках вимагається ручне втручання для додаткового аналізу та затвердження дій. Це включає перевірку логів, взаємодію з затронутими об'єктами та оцінку доказів.

Після завершення розслідування переходять до етапу стримування загрози. Це може включати ізоляцію заражених пристроїв, блокування шкідливих IP-адрес або відключення скомпрометованих облікових записів. Важливо мінімізувати подальший вплив інциденту.

Останнім етапом є відновлення системи та ресурсів до стану, в якому вони перебували до інциденту. Це також включає документування результатів розслідування, проведення пост-інцидентного аналізу для вивчення типу атаки та її впливу, а також оновлення внутрішніх політик і процедур безпеки на основі отриманого досвіду.

3.3. Рекомендації щодо застосування методів та засобів захисту кінцевих точок

Розглянемо рекомендації щодо застосування методів та засобів захисту кінцевих точок на базі Microsoft Defender for Endpoint.

Запровадити багаторівневий захист: *антивірусна та антімалуерна програма*: Microsoft Defender Antivirus входить до складу Microsoft Defender for Endpoint і забезпечує захист від відомих загроз, таких як віруси, шпигунські програми та трояни. Користувач також може використовувати сторонні антивірусні програми разом із Microsoft Defender Antivirus.

Правила зменшення кібератак: правила зменшення кібератак у Microsoft Defender for Endpoint дозволяють блокувати шкідливі дії, такі як запуск небажаних програм та використання небезпечних веб-сайтів. Користувач може створити власні правила або використовувати попередньо визначені правила,

надані Microsoft.

EDR (Endpoint Detection and Response): EDR в Microsoft Defender for Endpoint використовує машинне навчання для виявлення та реагування на невідомі загрози. EDR може виявляти підозрілу поведінку на ваших пристроях і автоматично вживати заходів, таких як ізоляція заражених пристроїв або блокування шкідливих процесів.

Використовувати централізоване керування: портал Microsoft Defender – це централізована консоль, яка дозволяє керувати безпекою ваших кінцевих точок. За допомогою порталу ви можете створювати та розгорніть політики безпеки, відстежувати стан безпеки ваших пристроїв та отримувати сповіщення про загрози.

Політики безпеки: дозволяють вам налаштувати захист своїх кінцевих точок. Користувач може створити політики для таких речей, як антивірусна програма, правила зменшення кібератак та EDR.

Відстеження стану безпеки: портал Microsoft Defender надає огляд стану безпеки ваших кінцевих точок. Користувач може побачити, які пристрої оновлені, які пристрої мають загрози та які політики безпеки застосовуються.

Сповіщення про загрози: Microsoft Defender for Endpoint може надсилати вам сповіщення про загрози, виявлені на ваших кінцевих пристроях. Можна налаштувати сповіщення, щоб отримувати їх електронною поштою, SMS або у програмі Microsoft Teams.

Забезпечити постійне оновлення Microsoft Defender for Endpoint: важливо регулярно оновлювати Microsoft Defender for Endpoint, щоб отримувати останні визначення вірусів та функції безпеки. Можливо автоматично оновлювати Microsoft Defender for Endpoint або оновлювати його вручну.

Оновлення операційних систем та програмного забезпечення: також важливо оновлювати операційні системи та програмне забезпечення на своїх

кінцевих пристроях. Оновлення часто містять виправлення помилок безпеки, які можуть допомогти захистити пристрої від кібератак.

Налаштування автоматичного оновлення: можна налаштувати автоматичне оновлення операційних систем та програмного забезпечення на кінцевих пристроях. Це допоможе гарантувати, що пристрої завжди оновлені до останніх виправлень безпеки.

Навчити своїх користувачів основам кібербезпеки. Це включає те, як розпізнавати та уникати фішингових атак та інших соціальних інженерних атак, як використовувати надійні паролі та як захищати особисті дані.

Фішингові атаки та соціальна інженерія - це поширені методи, які кіберзлочинці використовують для крадіжки особистих даних або зараження комп'ютерів шкідливим програмним забезпеченням. Навчіть своїх користувачів, як розпізнавати ці атаки та уникати їх.

Надійні паролі - це перша лінія захисту від кібератак. Навчіть своїх користувачів використовувати надійні паролі, які важко відгадати. Вони повинні використовувати різні паролі для різних облікових записів і нікому не розголошувати свої паролі.

Захист особистих даних: навчіть своїх користувачів захищати свої особисті дані. Це включає те, як бути обережними з тим, яку інформацію вони публікують в Інтернеті, як використовувати надійні методи автентифікації та як захищати свої фізичні пристрої.

Регулярне тестування на проникнення: варто проводити тестування на проникнення, щоб виявити потенційні вразливості у вашій мережі безпеки. Тестування на проникнення може допомогти вам визначити, як кіберзлочинці можуть отримати доступ до ваших систем і даних.

Використання результатів тестування на проникнення: використовуйте результати тестування на проникнення для покращення вашої позиції безпеки. Це може включати виправлення вразливостей, оновлення програмного

забезпечення або впровадження нових засобів безпеки.

Microsoft Threat Experts: Microsoft Threat Experts - це команда експертів з кібербезпеки, які можуть допомогти розслідувати та реагувати на складні кібератаки.

Microsoft Threat Intelligence – це служба, яка надає інформацію про нові кіберзагрози. Цю інформацію можна використовувати для покращення вашої позиції безпеки та захисту від кібератак.

Незважаючи на всі заходи безпеки, завжди важливо мати резервне копіювання важливих даних. Таким чином, ви зможете відновити інформацію у разі успішної атаки.

Використовуйте службу резервного копіювання в хмарі: служби резервного копіювання в хмарі, такі як Microsoft Azure Backup, пропонують зручний і масштабований спосіб резервного копіювання ваших даних. Ці служби автоматично резервують ваші дані в безпечний центр обробки даних, що полегшує їх відновлення у разі потреби.

Використовуйте локальне резервне копіювання: на додаток до резервного копіювання в хмарі, ви також повинні створювати локальні резервні копії ваших даних. Це може бути корисно, якщо вам потрібно швидко відновити дані або якщо у вас немає підключення до Інтернету.

Регулярно резервуйте копії: важливо регулярно резервувати копії ваших даних. Це допоможе гарантувати, що у вас є найновіша версія ваших даних у разі потреби.

Перевірте резервні копії: важливо регулярно перевіряти резервні копії, щоб переконатися, що їх можна відновити. Це можна зробити, відновивши невелику кількість даних або створивши тестову резервну копію

Застосовуючи ці рекомендації, користувач може підвищити рівень захисту своїх кінцевих точок та зменшити ризик кібератак.

На прикладі компанії Cielo розглянемо, як дотримання та використання

продуктів Microsoft (зокрема Microsoft Defender for Endpoint) приводить до безпеки даних та розквіту організації.[17]

Кожна компанія, яка обробляє фінансові дані своїх клієнтів, зобов'язана захищати цю інформацію. Cielo, одна з найбільших компаній платіжних систем у Латинській Америці як за прибутком, так і за ринковою вартістю, дуже серйозно ставиться до цієї відповідальності. Компанія не тільки підтримує чіткі канали зв'язку з клієнтами та високий ступінь прозорості щодо контролю даних, але й постійно працює над покращенням своєї безпеки. «Безпека даних — це надзвичайно динамічний простір, — говорить Глауко Сампайо, керівник інформаційної безпеки Cielo. «Як професіонал у цій сфері я завжди вивчаю тенденції та залишаюся в курсі того, що, зрештою, є постійно змінюваним ландшафтом загроз».

Як і більшість великих компаній, протягом багатьох років Cielo вдосконалювала свою інфраструктуру безпеки даних, впроваджуючи рішення, які відповідають її безпосереднім потребам. Це призвело до створення IT-ландшафту, який забезпечував хорошу видимість критичних активів компанії, але був дорогим і трудомістким для підтримки. Потрібні були постійні трудомісткі зусилля, щоб підтримувати правильну роботу рішення. Ці витрати ускладнювалися необхідністю залучати та підтримувати спеціалістів, які пройшли навчання на різноманітних платформах від багатьох постачальників рішень. Однак більш обтяжливим, ніж усі ці проблеми, була відсутність сумісності між рівнями безпеки рішення.

Нещодавно Cielo визначила інтегровану платформу, здатну замінити комплексне рішення безпеки. Важливо те, що ця платформа не лише підвищила ефективність роботи, але й підвищила швидкість реагування на загрози та зміцнила загальну безпеку компанії, надаючи контроль над конфіденційними даними, які потрібні Cielo. Нове рішення, повністю створене на основі технології Microsoft, базується на Microsoft Defender XDR, Microsoft

Sentinel і Intune , а також містить Microsoft Purview , Defender для Office 365 , Defender for Endpoint , Defender for Identity , Defender for Cloud Apps і Microsoft Entra ID.

Заміна застарілого рішення для керування кінцевими точками стала великою перемогою для Cielo. Внутрішні системи та локалізовані налаштування понад 5000 пристроїв зробили перехід складним. Компанія переконалася, що необхідні зміни вносяться поступово, щоб мінімізувати будь-який потенційний негативний вплив на користувачів. Це рішення виправдалося як фінансово, так і з точки зору досвіду користувачів. Компанія Cielo змогла припинити свій дорогий контракт із постачальником застарілих рішень, і користувачі швидко здобули впевненість у своїх навичках із новими рішеннями Microsoft. «На початку процесу усиновлення у нас була велика кількість запитань і деякі дебати, — згадує Сампайо. «Коли наші спеціалісти з безпеки завоювали впевненість у цій технології, вони швидко стали одними з наших найрішучіших прихильників рішень Microsoft Security».

Cielo також вважає Defender і Intune фундаментальними для своєї нової архітектури безпеки. Defender XDR забезпечує видимість на рівні інцидентів у численних і різноманітних кінцевих точках компанії, а Intune допомагає ідентифікувати активи компанії, а також потенціал виконання дій проти них. Інші рішення Microsoft також відіграють важливу роль. «Мені подобається Purview за його можливості класифікації документів і запобігання витокам інформації», — зазначає Сампайо. «Ми також високо цінуємо Defender for Endpoint та Identity як основні рівні захисту нашого середовища».

Під час впровадження кожного з цих рішень компанія Cielo переконалася, що освіта співробітників є центром процесу впровадження. Це поглибило розуміння співробітниками не лише технологій, які вони мали під рукою, але й їхніх обов’язків як розпорядників даних. «Для кожної компанії важливо мати безпеку даних у своїй ДНК», — каже Сампайо. «Так ми працюємо в Cielo».

З моменту переходу на рішення безпеки Microsoft Cielo покращив свою безпеку кількома способами. «Застосувавши численні сумісні рішення безпеки Microsoft, ми покращили наші профілактичні можливості, час реагування на інциденти та можливості моніторингу нашого середовища», — каже Сампайо. «І ми зробили все це набагато швидше, ніж могли б».

Ці переваги також продовжували зростати після процесу усиновлення. Наприклад, підвищена автоматизація зіграла важливу роль у тому, що Сампайо описує як різке скорочення часу виявлення загроз і стримування. Команда безпеки Cielo також була приємно здивована передовими технічними можливостями рішення та частотою, з якою Microsoft розширює його функціональність, у тому числі шляхом додавання нових можливостей. «У якийсь момент сторонні технології створили потенційні прогалини в нашій системі безпеки», — згадує Сампайо. «На щастя, рішення Microsoft заповнили ці прогалини без додаткових витрат для нас».

Консолідуючи систему безпеки, Cielo зменшила свої операційні витрати, збільшила видимість і підвищила загальний рівень зрілості безпеки. Але Сампайо бачить ще одну важливу перевагу. «Консолідація може дати реальну можливість зламати застійні парадигми, впорядкувати процес і відкрити можливості для вдосконалення, які лідери бізнесу інакше могли б не помітити», — каже він. «З огляду на так багато можливостей, я не бачу причин не скористатися цією можливістю».

ВИСНОВОК

У цій роботі досліджено проблему захисту кінцевих точок в організаціях, визначено мету та завдання дослідження. Сьогодні існують серйозні виклики у захисті кінцевих точок від нових і дедалі витонченіших загроз. Спостерігається зростання ризиків для безпеки кінцевих точок, посилене недостатньою підготовленістю до протидії новим загрозам за допомогою існуючих платформ безпеки кінцевих точок.

Проведено аналіз сучасних технологій захисту кінцевих точок в організаціях. Рішення Microsoft Defender for Endpoint виконує функції постійного моніторингу і збору даних з кінцевих точок для виявлення та усунення кіберзагроз у режимі реального часу. Таким чином, Microsoft Defender for Endpoint відіграє ключову роль у загальній системі забезпечення безпеки інформаційних систем організації.

У роботі досліджено проблему захисту кінцевих точок, визначено його мету та завдання. Проведено аналіз існуючих методів та засобів захисту кінцевих точок, включаючи методи та засоби на базі Microsoft Defender for Endpoint.

Проаналізовано основні підходи до захисту кінцевих точок, що дозволило виділити найефективніші методи та засоби для забезпечення безпеки інформаційних систем організацій. Виявлено, що використання сучасних рішень, таких як Microsoft Defender for Endpoint, є критично важливим для забезпечення надійного захисту від нових і складних кіберзагроз. Завдяки функціям постійного моніторингу, збору даних та виявлення загроз у режимі реального часу, Microsoft Defender for Endpoint значно підвищує рівень безпеки кінцевих точок. Застосування цих підходів і технологій дозволяє організаціям ефективно протистояти кіберзагрозам і підтримувати цілісність своїх інформаційних систем.

Проаналізовано існуючі рішення із захисту кінцевих точок від програм-вимагачів, що дозволило виділити найбільш ефективні методи та інструменти для забезпечення кібербезпеки організацій. Виявлено, що використання сучасних рішень є критично важливим для забезпечення надійного захисту від нових і складних кіберзагроз, зокрема програм-вимагачів. Завдяки функціям постійного моніторингу, збору даних та виявлення загроз у режимі реального часу, Microsoft Defender for Endpoint значно підвищує рівень безпеки кінцевих точок. Застосування цих підходів і технологій дозволяє організаціям ефективно протистояти програмам-вимагачам і підтримувати цілісність своїх інформаційних систем. Таким чином, впровадження та правильне налаштування цих рішень є важливим кроком у зміцненні кібербезпеки та зниженні ризиків, пов'язаних із програмами-вимагачами.

У результаті досліджень було визначено призначення, основні функції та склад рішення Microsoft Defender for Endpoint.

На основі проведених досліджень був запропонований варіант системи на базі Microsoft Defender for Endpoint. Також розроблено рекомендації щодо застосування методів та засобів захисту кінцевих точок від програм-вимагачів.

Зокрема, рекомендується впровадження багаторівневого захисту, що включає використання антивірусного програмного забезпечення, регулярні оновлення систем, навчання персоналу з питань кібербезпеки та здійснення резервного копіювання важливих даних. Застосування цих рекомендацій дозволить організаціям ефективно протистояти програмам-вимагачам і підтримувати цілісність своїх інформаційних систем.

Практичне застосування результатів роботи може знайти використання у сферах, де критично важливим є забезпечення надійності і безпеки програмного забезпечення.