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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Захист кінцевих точок організації від атак програм-вимагачів на базі Carbon Black Cloud Endpoint Security Standard»

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

_____ Лев ЧЕГЛАКОВ
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
ЧЕГЛАКОВ Лев
(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 2025

ВСТУП

Актуальність дослідження. Кінцеві точки, такі як робочі станції, сервери, ноутбуки та мобільні пристрої, є основними точками взаємодії користувачів з корпоративними даними та мережевими ресурсами. Вони часто стають першою ланкою в ланцюгу кібератак, оскільки є зручними мішенями для початкового проникнення зловмисників. В умовах зростаючої кількості та складності кібератак, зокрема атак програм-вимагачів, захист кінцевих точок організації набуває критичного значення.

Згідно з даними Coveware середньо-квартальний показник суми виплати викупу становив 554 тис доларів у 4-ому кварталі 2024 року, що на 16% більше, ніж у 3-ому кварталі 2024 року. Однак, медіанні суми викупу є більш надійними показниками того, куди рухається ринок. Медіанний розмір платежу викупу знизився на 45% у 4 кварталі 2024 року до 110 тис доларів. Виплати продовжують залишатися крайнім варіантом переважно для тих, хто не має іншої альтернативи для відновлення критично важливих даних. Несправні інструменти дешифрування як нових, так і старих програм-вимагачів, а також зростаюча недовіра до здатності зловмисників виконувати свої обіцянки відштовхують жертв від сплати викупу.

Системи виявлення та реагування на кінцевих точках відіграють ключову роль у створенні багаторівневої системи захисту від атак програм-вимагачів. Вони забезпечують безперервний моніторинг активності на кінцевих точках, збір телеметрії, аналіз поведінки процесів, файлів та мережевих з'єднань. Це дозволяє виявляти аномалії та потенційні загрози, які традиційні антивіруси можуть пропустити. Крім того, EDR-рішення надають інструменти для швидкого розслідування інцидентів, ізоляції скомпрометованих пристроїв та автоматизованого реагування, що мінімізує час простою та потенційний збиток від кібератак.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження методів та засобів захисту кінцевих

точок організації від атак програм-вимагачів на базі Carbon Black Cloud Endpoint Security Standard.

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

Предмет дослідження – методи та засоби захисту кінцевих точок організації від програм-вимагачів на базі Carbon Black Cloud Endpoint Standard.

Мета роботи – розробити рекомендації щодо застосування методів та засобів захисту кінцевих точок організації від атак програм-вимагачів на базі рішення Carbon Black Cloud Endpoint Security Standard.

Наукові завдання:

дослідити сутність проблеми атак програм-вимагачів та їх вплив на кінцеві точки організації;

проаналізувати основні принципи та підходи до захисту кінцевих точок організації від програм-вимагачів;

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

проаналізувати методи та засоби захисту кінцевих точок організації від атак програм-вимагачів на базі Carbon Black Cloud Endpoint Security Standard;

запропонувати варіант системи захисту кінцевих точок організації від програм-вимагачів на базі Carbon Black Cloud Endpoint Security Standard;

розробити рекомендації щодо захисту кінцевих точок організації від програм-вимагачів.

Методи дослідження – опрацювання технічної літератури, офіційної документації 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 організації від атак програм-вимагачів, які можуть бути використані фахівцями з кібербезпеки для підвищення рівня захищеності інформаційних систем від програм вимагачів.

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

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ ВІД ПРОГРАМ-ВИМАГАЧІЧВ

1.1 Аналіз проблеми захисту кінцевих точок організації від атак програм-вимагачів

Програми-вимагачі – це тип шкідливого програмного забезпечення, яке шифрує дані жертви, а зловмисник вимагає "викуп", або оплату, щоб відновити доступ до файлів і мережі. Зазвичай жертва отримує ключ розшифровки після оплати, щоб відновити доступ до своїх файлів. Якщо викуп не сплачено, зловмисник публікує дані на сайтах витоку даних (DLS) або блокує доступ до файлів назавжди [1].

Загальні витрати за викуп програми-вимагачів мають щорічну тенденцію до зростання, хоча менше компаній вирішують платити викупи. Згідно з даними Coveware [2] середньо-квартальний показник суми виплати викупу становив 554 тис доларів у 4-ому кварталі 2024 року, що на 16% більше, ніж у 3-ому кварталі 2024 року. Однак, медіанні суми викупу є більш надійними показниками того, куди рухається ринок. Медіанний розмір платежу викупу знизився на 45% у 4 кварталі 2024 року до 110 тис доларів. Тенденції зміни середнього значення викупу зображено на рисунку 1.1.

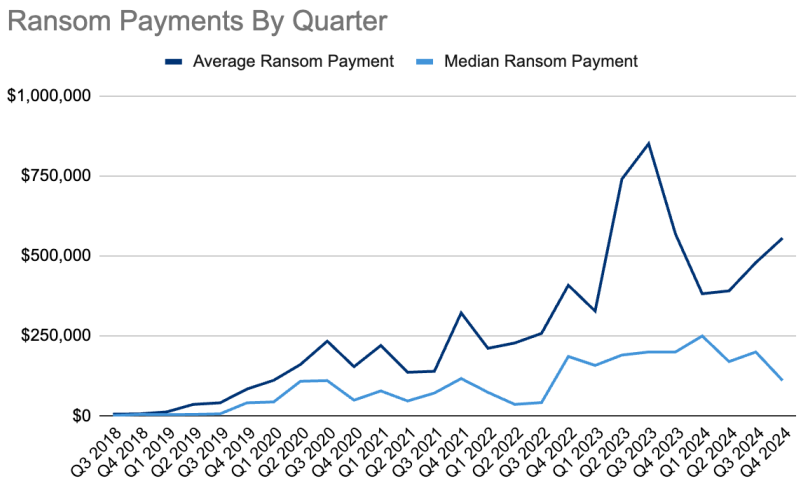


Рис. 1.1. Тенденції зміни середнього значення викупу [2]

Виплата викупу продовжують залишатися крайнім варіантом переважно для тих, хто не має іншої альтернативи для відновлення критично важливих даних. Несправні інструменти дешифрування як нових, так і старих програм-вимагачів, а також зростаюча недовіра до здатності зловмисників виконувати свої обіцянки відштовхують жертв від сплати викупу. Найбільший відомий платіж за викуп становив близько 75 мільйонів доларів. Цей платіж не був розголошений жертвою, і про нього відомо лише тому, що його виявили та підтвердили дослідники з ThreatLabz [3]. Відсутність розкриття інформації від компанії є одним із прикладів того, чому важко отримати повну картину витрат та інших збитків від глобальної кіберзлочинності. Хоча ми не маємо повної картини ландшафту загроз та їхнього впливу, у нас є деякі інші цікаві дані.

Програми-вимагачі, можна поділити на п’ять основних типів, перелік яких наведено нижче [5]:

криптографічні програми-вимагачі (шифрувальники) – один з найвідоміших і найшкідливіших варіантів. Цей тип шифрує файли та дані в системі, роблячи вміст недоступним без ключа розшифровки;

блокувальники – повністю блокують доступ до системи, через що файли та програми стають недоступними. На екрані блокування відображається вимога викупу, можливо, з годинником зворотного відліку, щоб підвищити терміновість і змусити жертву діяти шляхом психологічного тиску на людину;

програми для залякування – це фальшиве програмне забезпечення, яке стверджує, що виявило вірус або іншу проблему у системі, і вимагає заплатити, щоб вирішити «знайдену проблему». Деякі типи таких програм блокують комп'ютер, тоді як інші просто заповнюють екран спливаючими повідомленнями, не пошкоджуючи при цьому файли;

програми-витоку – загрожують розповсюдженням конфіденційної особистої або корпоративної інформації в Інтернеті, через що багато жертв подібної атаки панікують і платять викуп, щоб запобігти потраплянню приватних даних до чужих рук або в публічний простір. Одним з прикладів даного типу програм-вимагачів є програми на поліцейську тематику, які видають себе за правоохоронців і

попереджають, що виявлено незаконну діяльність в Інтернеті, але тюремного ув'язнення можна уникнути, сплативши штраф;

RaaS (Ransomware as a Service) – це шкідливе програмне забезпечення, анонімно розміщене "професійним" хакером, який займається всіма аспектами атаки, від розповсюдження програм-вимагачів до збору платежів і відновлення доступу в обмін на частку від сплаченого викупу.

Процес атаки програм вимагачів зазвичай виглядає наступним чином [1]:

крок 1: зараження. Зловмисники, що керують програмами-вимагачами, часто використовують фішингові електронні листи та методи соціальної інженерії для зараження комп'ютера жертви зловмисним програмним забезпеченням. У більшості випадків жертва натискає на шкідливе посилання в електронному листі, яке завантажує та запускає на пристрої жертви програму-вимагач;

крок 2: шифрування. Після зараження пристрою або системи програми-вимагачі шукають і шифрують цінні файли або всі існуючі файли. Залежно від варіанту, шкідливе програмне забезпечення може знайти можливість поширитися на інші пристрої та системи в організації для збільшення обсягу завданої шкоди;

крок 3: вимога викупу. Після того, як дані зашифровані, для розблокування файлів потрібен ключ розшифровки. Щоб отримати ключ розшифрування, жертва повинна слідувати інструкціям, залишеним зловмисником у вимогах про викуп, де вказано, як заплатити зловмиснику – зазвичай у крипто-валюті. Приклад вікна із вимогами програми-вимагача NotPetya [5], зображено на рисунку 1.2 .

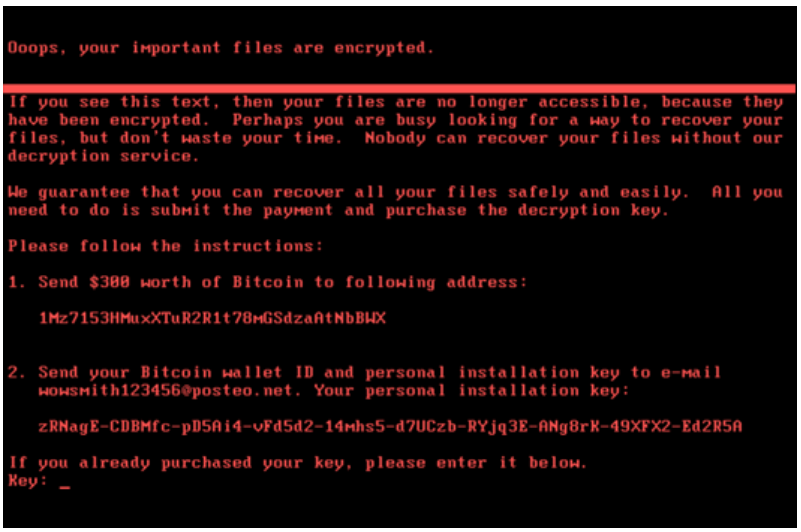


Рис. 1.2. Вимоги зловмисника для отримання ключа дешифрування [1]

Також, прикладом може бути NetWalker – програми-вимагач, написана на мові C++, вона була розміщена на скритих форумах як Ransomware-as-a-Service (RaaS) користувачем, який, як відомо, входить до групи під назвою CIRCUS SPIDER.

NetWalker шифрує файли в локальній системі, відображає мережеві ресурси та шукає в мережі додаткові ресурси, намагаючись отримати до них доступ за допомогою токенів безпеки всіх зареєстрованих користувачів системи жертви. Процес атаки NetWalker [6] зображено на рисунку 1.3.

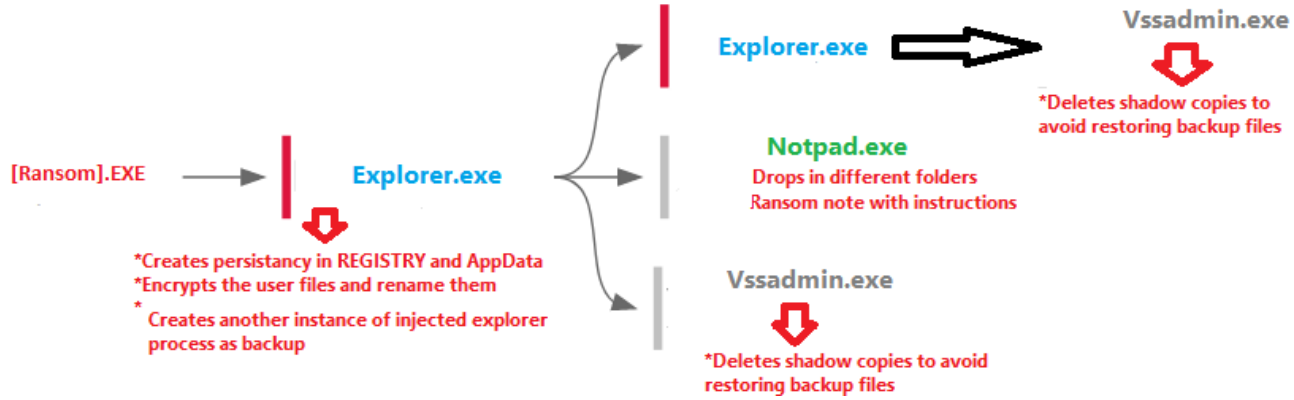


Рис. 1.3. Процес атаки програми-вимагача NetWalker [6]

Отже, програми-вимагачі становлять одну з найбільших кіберзагроз для сучасних організацій. Їхня здатність шифрувати критичні дані та порушувати безперервність бізнес-процесів робить захист кінцевих точок ключовим завданням інформаційної безпеки.

1.2 Аналіз підходів до захисту кінцевих точок організації від атак програм-вимагачів

Захист кінцевих точок від програм вимагачів, має розглядатися як комплексна проблема, яку неможна вирішити впровадженням лише одного типу рішень безпеки, як наприклад антивірусне програмне забезпечення. Спеціалізовані

інструменти безпеки можуть забезпечити комплексний захист від програм-вимагачів як на рівні мережі, файлової системи, так і на рівні додатків.

Засоби захисту від атак програм-вимагачів, можуть застосовувати наступні методи протидії для виявлення та блокування програм-вимагачів [7]:

блокування попереднього завантаження – застосування механізмів проти експлойтів і безфайлових шкідливих програм, які зазвичай слугують способом доставки корисного навантаження для програм-вимагачів, запобігаючи їхньому потраплянню на кінцеві точки в першу чергу;

запобігання виконання – застосовування статичного аналізу на основі машинного навчання для виявлення шаблонів програм-вимагачів у бінарних файлах до їх виконання;

блокування під час виконання – використовується поведінковий аналіз для виявлення поведінки, схожої на поведінку програм-вимагачів, і зупинка процесу, якщо він демонструє подібну поведінку;

розвідка загроз – отримання інформації з різних каналів про відомі програми-вимагачі, для їх виявлення на кінцевих точках;

нечітке виявлення – використовує механізм нечіткого хешування для виявлення автоматизованих варіантів відомих програм-вимагачів, у яких було незначною мірою змінено код, для уникнення виявлення за хешем;

пісочниця – дозволяє запускати програму-вимагач у ізольованому середовищі, що симулює реальну систему, аналізує виконання програми та блокує виконання на реальній системі у разі виявлення зловмисної поведінки, схожої на поведінку програми-вимагача;

файли-приманки – встановлення фальшивих файлів на хости і застосування механізму, який гарантує, що вони будуть зашифровані першими у випадку використання програми-вимагача. Як тільки у системі виявлено поведінку, що шифрує дані файли, процес який виконує шифрування зупиняється;

блокування розповсюдження – ідентифікація сигнатур мережевої активності, що генеруються хостами під час автоматичного розповсюдження програми-

вимагача, та ізолює заражені хости від мережі, для унеможливлення розповсюдження зловмисної програми.

Отже, ефективний захист кінцевих точок від програм-вимагачів потребує багаторівневого підходу, що поєднує різноманітні технології та методи виявлення, запобігання і реагування. Лише комплексне використання спеціалізованих інструментів безпеки – від статичного аналізу й поведінкового моніторингу до ізольованих середовищ і файлів-приманок – дозволяє вчасно виявляти та зупиняти загрози, знижуючи ризик шифрування критичних даних та подальшого поширення зловмисного ПЗ в інфраструктурі. Такий підхід забезпечує не лише проактивну, а й адаптивну оборону в умовах постійної еволюції кіберзагроз.

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

Програмне забезпечення для захисту від програм-вимагачів – це спеціалізований інструмент, призначений для виявлення, блокування та нейтралізації програм-вимагачів до того, як вони встигнуть завдати шкоди [8]. Воно використовує комбінацію передових технологій, включаючи аналіз поведінки, машинне навчання і штучний інтелект (ШІ), для моніторингу та виявлення підозрілих дій у вашій мережі.

На відміну від традиційних антивірусних програм, програмне забезпечення для захисту від програм-вимагачів орієнтоване на унікальні характеристики таких програм, такі як здатність шифрувати файли і вимагати викуп. Така спеціалізована спрямованість робить його важливим компонентом будь-якої стратегії кібербезпеки, особливо для підприємств, які обробляють конфіденційні або цінні дані.

Програмне забезпечення для захисту від програм-вимагачів має низку переваг, які виходять за рамки базових антивірусних рішень. Ці інструменти призначені для забезпечення комплексних механізмів захисту, які захищають ваші дані та забезпечують безперервність роботи.

Нижче наведено перелік ключових переваг програмного забезбечення для захисту від програм-вимагачів [8]:

посилений захист: Завдяки багаторівневому захисту ці рішення можуть ефективно виявляти, запобігати та реагувати на атаки зловмисників. На відміну від традиційних антивірусних програм, які розпізнають лише відомі загрози, програмне забезпечення для захисту від програм-вимагачів може виявляти та блокувати нові загрози в режимі реального часу, захищаючи ваші дані навіть від найновіших кіберзагроз;

економічна ефективність: Інвестиції в програмне забезпечення для захисту від програм-вимагачів допомагають уникнути високих витрат, пов'язаних з атаками, таких як виплати викупу, витрати на відновлення даних і потенційні судові витрати. Надійний захист часто обходиться набагато дешевше, ніж ліквідація наслідків атаки, яка може вплинути на ваші гроші та ресурси;

безперервність роботи: Ефективний захист від програм-вимагачів підтримує бізнес-операції, швидко ізолюючи та усуваючи загрози до того, як вони поширяться та нанесуть шкоду великій кількості пристроїв. Це мінімізує час простою та забезпечує доступність критично важливих систем і даних. Безперебійна робота допомагає зберегти довіру клієнтів і ділову репутацію;

забезпечення відповідності вимогам: Захист від програм-вимагачів підтримує відповідність вимогам до даних, захищаючи конфіденційну інформацію від несанкціонованого доступу. Наприклад, медична галузь повинна дотримуватися суворих стандартів безпеки даних відповідно до Закону про переносимість і відповідальність за медичне страхування (HIPAA). Ефективне програмне забезпечення для захисту забезпечує конфіденційність даних пацієнтів і підвищує довіру до організації.

Для порівняння рішень безпеки захисту кінцевих точок від програм вимагачів, було обрано наступні системи: Microsoft Defender, Bitdefender GravityZone, Sentinel One. Порівняння проведено за основними функціональними можливостями:

загальний підхід до захисту кінцевих точок;

здатність виявляти та реагувати на програми-вимагачі;

механізми ізоляції заражених пристроїв;

інтеграція з іншими системами безпеки;

особливості аналітики інцидентів та звітності.

Загальний підхід до захисту кінцевих точок:

Bitdefender GravityZone (далі GravityZone) – це система, що забезпечує багаторівневий захист кінцевих точок, поєднуючи антивірус, EDR (Endpoint Detection and Response), XDR (Extended Detection and Response), поведінковий аналіз, машинне навчання та хмарну аналітику. Це дозволяє виявляти та блокувати загрози на ранніх етапах, включаючи невідомі варіанти програм-вимагачів [10];

Microsoft Defender for Endpoint – це компонент єдиної платформи Microsoft Defender XDR. Він поєднує вбудований у Windows Антивірус нового покоління (NGAV) та розширені механізми EDR/XDR. Defender застосовує сигнатурний аналіз, хмарні розвідувальні дані, моніторинг поведінки та правила зменшення поверхні атаки (ASR) для перехоплення загроз.. Важливо, що Defender легко інтегрується з іншими сервісами Microsoft [11] (Azure, Defender for Cloud, Office 365 та іншими);

SentinelOne Singularity – це автономна XDR-платформа, що використовує штучний інтелект і глибоке машинне навчання для запобігання й аналізу атак. SentinelOne поєднує можливості NGAV та EDR у одному агенті і може діяти автономно, без постійного зв’язку агенту з хмарою. Система спеціалізується на поведінковому аналізі за допомогою ШІ, з можливістю миттєвого реагування на аномалії в реальному часі [12].

Здатність виявляти та реагувати на програми-вимагачі:

GravityZone: використовує технологію Ransomware Mitigation [13], яка виявляє аномальні спроби шифрування файлів, створює тимчасові резервні копії в пам'яті та автоматично відновлює файли після блокування шкідливого процесу. Цей підхід ефективний навіть проти нових та невідомих варіантів програм-вимагачі;

Microsoft Defender for Endpoint: включає в себе технології NGAV і правила «Attack Surface Reduction» (ASR), що блокують відомі шкідливі сценарії,

завантаження шифрувальника з мережі, запуск непідписаних скриптів та інші [14]. Також, захист від програм-вимагачів у Windows реалізується за допомогою функції «Контрольованого доступу до папок». Система швидко генерує сповіщення у разі виявлення шкідливої поведінки і надає покрокові рекомендації для реагування (наприклад, інструкції щодо ізоляції зараженої машини або відновлення з резервної копії);

SentinelOne: агент системи аналізує поведінку процесів у реальному часі й може зупинити виконання програми-вимагача до початку шифрування файлів системи. Унікальність платформи – це вбудована функція rollback, вона дозволяє робити копії файлів і в разі реалізації атаки автоматично повертає їх до стану перед шифруванням [15]. SentinelOne забезпечує багатовекторне захоплення даних, що дозволяє точно корелювати події, пов’язані з ransomware.

Механізми ізоляції заражених пристроїв:

GravityZone: дозволяє адміністраторам ізолювати заражені кінцеві точки від мережі, блокувати шкідливі файли та встановлювати віддалене з'єднання для подальшого аналізу. Ці дії допомагають запобігти поширенню загроз в мережі організації;

Microsoft Defender for Endpoint: має вбудовані механізми ізоляції кінцевої точки від мережі. Через Defender-портал адміністратор може виконати дію «contain device» – повністю відключити пристрій від внутрішньої мережі та Інтернету [16]. Ця дія припиняє будь-яку зовнішню комунікацію з зараженого хоста, залишаючи лише зв’язок із сервером безпеки. Така ізоляція стримує розповсюдження програми-вимагача, запобігає викраденню даних та бічному руху всередині мережі організації;

SentinelOne: одна з ключових функцій – швидка ізоляція інфікованих кінцевих точок. Через консоль можна миттєво ізолювати машину: система блокує будь-який мережевий трафік (вхідний і вихідний), крім зв’язку із сервером керування. SentinelOne підтримує як ручне, так і автоматичне виконання дій ізоляції на базі налаштованих правил у системі.

Інтеграція з іншими системами безпеки:

GravityZone: підтримує інтеграцію з SIEM/SOAR системами, такими як Splunk, QRadar та Netsurion Open XDR, що дозволяє централізовано моніторити події безпеки та автоматизувати реагування на інциденти [17];

Microsoft Defender for Endpoint: служить ядром широкої платформи безпеки Microsoft. Його події та інциденти можуть бути відправлені в Microsoft Sentinel (SIEM) – для цього є готові конектори [18]. Також, Defender взаємодіє з Defender for Cloud Apps, Defender for Identity, Office 365, корелюючи і збагачуючи дані про події. Таким чином, аналітики отримують єдине середовище для розслідування інцидентів всього набору рішень Microsoft;

SentinelOne: має «Singularity Marketplace» з численними конекторами і вбудованими інтеграціями. Зокрема, SentinelOne пропонує інтеграцію з SIEM-системами: наприклад, офіційний додаток для IBM QRadar дозволяє передавати детальні логи та алерти прямо в QRadar і запускати дії реагування безпосередньо з SIEM-консолі. Також підтримуються Splunk, Elastic, ArcSight тощо. Крім SIEM, SentinelOne може надсилати і приймати IOC/CTI (cyber threat intelligence), а також інтегруватися з SSO, MDM і хмарними платформами (AWS, Azure). Все це дозволяє поєднувати інформацію з Endpoint із загальною аналітичною платформою.

Особливості аналітики інцидентів та звітності:

GravityZone: надає розширену аналітику інцидентів, включаючи візуалізацію ланцюга атаки, аналіз першопричин та кореляцію подій [4*]. Функція Incident Advisor допомагає швидко оцінити ситуацію та прийняти відповідні заходи. Також доступні детальні звіти про активність програм-вимагачів та статус відновлення файлів;

Microsoft Defender for Endpoint: надає аналітику через єдиний портал Microsoft Defender. Система групує схожі сповіщення в інциденти, показує пов’язані пристрої, вектори атаки та контекст загроз. Також можна експортувати інциденти в Azure Sentinel для створення звітів і дашбордів.;

SentinelOne: крім стандартних звітів, SentinelOne пропонує унікальний модуль Deep Visibility, що дозволяє аналітикам проводити розвідку загроз, глибоко

досліджуючи зібрані деталі роботи системи: від мережевих з’єднань до викликів API. Система відображає повну історію процесів і дозволяє фільтрувати події за різними критеріями. Крім того, у платформі є вбудований механізм автоматичних звітів і панелей із метриками безпеки.

Підсумок порівняння зображено у таблиці 1.1.

Таблиця 1.1.

Порівняння рішень захисту від програм-вимагачів

Критерій	**Bitdefender GravityZone**	**Microsoft Defender for Endpoint**	**SentinelOne**
Тип рішення	NGAV + EDR + XDR	NGAV + EDR + XDR	NGAV + автономний XDR
Захист від ransomware	Поведінковий аналіз, стрімінгове запобігання (HyperDetect, Sandbox Analyzer)	ASR, сигнатури, хмарна аналітика	AI-моделі, виявлення поведінки, повний rollback
Ізоляція заражених пристроїв	Є (ізоляція через консоль)	Є (ізоляція через портал)	Є (автоматична та ручна ізоляція)
Інтеграція з SIEM/SOAR	Splunk, API, інші SIEM-платформи	Microsoft Sentinel, XDR, Defender for Cloud, O365	Splunk, QRadar, ArcSight, Singularity Marketplace
Аналітика та розслідування інцидентів	Повна візуалізація, графи подій	Єдиний XDR-огляд, деталізація інцидентів	Глибокий аналіз, ізольована телеметрія, миттєві дії реагування

Таким чином, програмне забезпечення для захисту від програм-вимагачів є важливим елементом сучасної кібербезпеки, надаючи організаціям високоякісні інструменти для виявлення, запобігання та нейтралізації загроз до того, як вони можуть спричинити серйозні наслідки. Завдяки інноваційним підходам, таким як машинне навчання, штучний інтелект та глибокий аналіз поведінки, ці рішення забезпечують не лише високий рівень захисту, а й допомагають підтримувати

безперервність роботи та відповідність вимогам безпеки. Порівняння популярних систем, таких як Bitdefender GravityZone, Microsoft Defender for Endpoint і SentinelOne, показує їх різноманітні підходи до захисту кінцевих точок, виявлення атак і інтеграції з іншими інструментами безпеки. Кожна з цих платформ має свої переваги, що дозволяє організаціям обирати рішення, яке найкраще відповідає їхнім потребам в залежності від специфіки і масштабів бізнесу.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА БАЗІ CARBON BLACK CLOUD ENDPOINT SECURITY STANDARD

2.1 Призначення та основні функції рішення Carbon Black Cloud Endpoint Security Standard

Carbon Black Cloud Endpoint Standard – це хмарна NGAV-платформа, що базується на поведінковому аналізі [9]. Основна мета Carbon Black Cloud Endpoint Security Standard – забезпечити проактивний захист кінцевих точок від широкого спектру загроз, включаючи як відомі, так і нові атаки, шляхом поєднання передових технологій виявлення та реагування. Агенти на кінцевих точках безперервно збирають телеметрію, події і виявляють підозрілі дії (наприклад, спроби масового шифрування файлів) за допомогою евристики і штучного інтелекту. Система пропонує центральну консоль управління в хмарі. Інтерфейс є інтуїтивно зрозумілим і легким у навігації.

Основні функції системи Carbon Black Cloud Endpoint Standard:

захист від шкідливого та безпечного програмного забезпечення. Carbon Black Cloud Endpoint Standard допомагає забезпечити комплексний захист даних організації та інформації про клієнтів від шкідливих і легітимних програм, а також від атак, що відбуваються поза мережею (LoL). За допомогою готових політик, система спросщує розгортання та експлуатацію щоб адаптувати захист до потреб організації. Система дозволяє бути в курсі останніх атак, отримуючи оновлення від експертів VMware Threat Analysis Unit. Carbon Black Cloud Endpoint Standard зупиняє атаки нешкідливого ПЗ, аналізуючи всю послідовність подій, щоб виявити загрозу;

прискорення розслідування та час реагування. Carbon Black Cloud Endpoint Standard надає централізований хмарний адміністративний інтерфейс, який поєднує в собі антивірус нового покоління (NGAV) і засоби виявлення та

реагування на загрози для кінцевих точок (EDR) у легкому рішенні, яке швидко розгортається і яким легко керувати. Endpoint Standard розроблений для забезпечення найкращого захисту кінцевих точок з найменшими адміністративними зусиллями, об'єднуючи всі дані та інструменти, необхідні для аналізу першопричин, розслідувань в режимі реального часу, віддаленого реагування та управління політиками в єдиній консолі. Рішення дозволяє зменшити вартість і час, необхідні на проведення розслідування та реагування на інциденти. Завдяки видимості всього ланцюжка атак та аналізу активності кінцевих точок, аналітикам не потрібно витрачати час на відстеження того, які системи було уражено і коли;

багаторівневий захист. Рішення Carbon Black Cloud Endpoint Standard використовує декілька рівнів захисту, включаючи репутацію файлів та евристики, машинне навчання та поведінкові моделі, для аналізу активності кінцевих точокдля аналізу активності кінцевих точок і блокування зловмисної поведінки, щоб зупинити всі типи атак до того, як вони досягнуть критично важливих систем та завдадуть шкоди. Завдяки гнучким поведінковим політикамполітики запобігання, захист можна легко адаптувати до конкретних потреб організації;

інтеграція з іншими системами. Carbon Black Cloud Endpoint Standard має можливість інтеграції з SIEM/SOAR-платформами (наприклад, Splunk, IBM QRadar, ServiceNow) через API для покращення координації та автоматизації процесів безпеки.

Отже, система . Carbon Black Cloud Endpoint Standard, призначена для забезпечення захисту кінцевих точок організації від атак, у режимі реального часу. Основні функції – виявлення шкідливої поведінки, реагування на інциденти, ізоляція заражених пристроїв, блокування підозрілих дій, збір телеметрії.

2.2 Архітектура та компоненти рішення Carbon Black Cloud Endpoint Security Standard

Рішення Carbon Black Cloud Endpoint Security Standard – це хмарна платформа захисту кінцевих точок (EPP) [9], яка не потребує розгортання великої кількості компонентів у інфраструктурі організації, що дозволяє забезпечити більшу відмовостійкість, знижуючи витрати на обслуговування системи. архітектуру рішення зображено на рисунку 2.1.

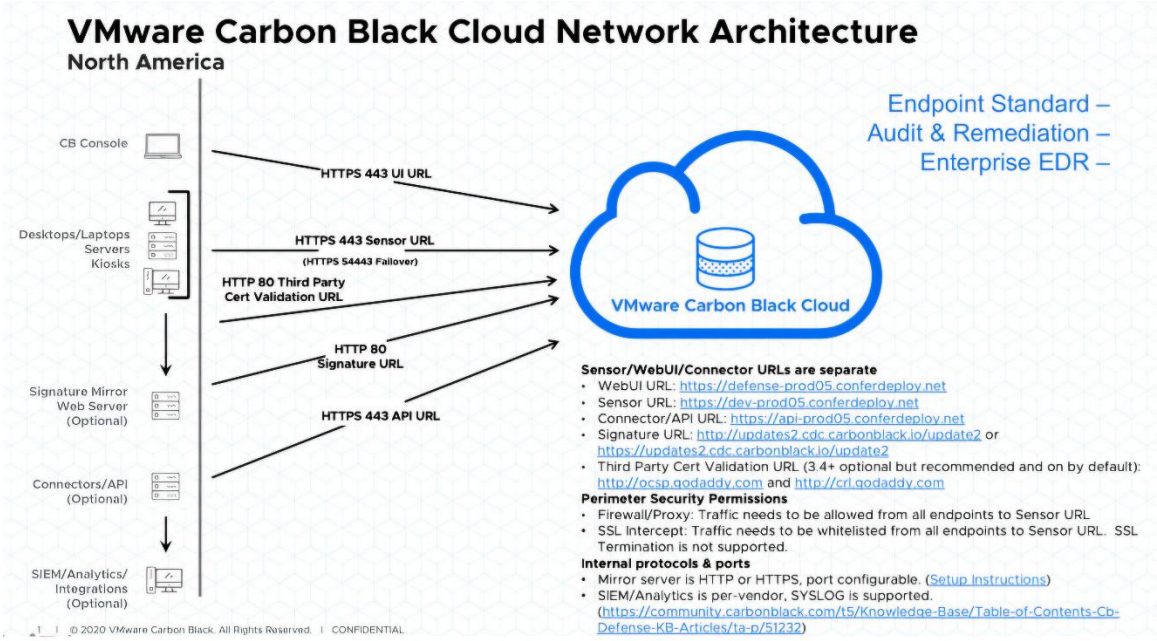


Рис. 2.1. Архітектура рішення Carbon Black Cloud Endpoint Security Standard [20]

Рішення Carbon Black Cloud Endpoint Security Standard, включає в себе такі основні компоненти:

агенти(сенсори) Carbon Black Cloud;

хмарна платформа Carbon Black Cloud;

консоль керування Carbon Black Cloud (Cloud Console);

Оскільки аналітика та обробка даних з кінцевих точок відбуваються в хмарі, це забезпечує високий рівень масштабованості та відмово-стійкості, на відміну від рішень, що повністю розгортаються та функціонують всередині інфраструктури організації. Агент підтримується на всіх основних типах операційних систем – Windows, Linux, MacOS, а також може бути розгорнутий на VDI машинах, що

забезпечує високий рівень покриття. Сервісна шина платформи обробляє більше трильйону подій щодня, забезпечуючи централізоване управління і видимість.

Основні функції та призначення компонентів рішення Carbon Black Cloud Endpoint Security Standard:

агент Carbon Black Cloud – встановлюється на кінцеві точки у організації. Агент безперервно моніторить систему та збирає події (запуск процесів, зміни файлів і реєстру, мережеві з'єднання, метадані бінарних файлів тощо). Також, агент виконує блокування підозрілих процесів згідно з політиками безпеки;

консоль керування Carbon Black Cloud (Cloud Console) – веб-інтерфейс для адміністраторів і аналітиків. Через консоль здійснюється керування системою: створення та політик захисту, перегляд сповіщень та подій, запуск пошукових запитів по журналам подій, розслідування інцидентів і виконання заходів реагування (наприклад, ізоляція пристрою);

хмарна платформа Carbon Black Cloud – серверна інфраструктура для отримання, зберігання і аналізу даних, отриманих з встановлених агентів. У хмарі події від агентів обробляються та індексуються, застосовуються аналітичні моделі машинного навчання та поведінкового аналізу. На основі результатів аналізу формуються сповіщення про підозрілі події та інциденти;

Хмарна платформа складається з пов'язаних між собою сервісів, що безпосередньо виконують аналіз, аналітику даних, графічне відображення . Перелік сервісів платформи та їх функції описано нижче:

служби Dashboard (UI/Console) – надають можливості входу до системи та забезпечують графічне відображення елементів консолі для хмари VMware CarbonBlack Cloud;

служби пристроїв – забезпечують зв'язок для комунікації між встановленими агентами та хмарою, включаючи:

реєстрацію/встановлення датчиків;

завантаження телеметрії подій;

пошук репутації нових виконуваних файлів на кінцевих пристроях;

отримання оновлень політик;

ізоляція пристроїв;

віддалене підключення у режимі реального часу;

видалення сенсорів.

служби обробки подій – отримують, обробляють та індексують події, отримані з кінцевих пристроїв за допомогою встановлених сенсорів на кінцевих точках організації;

служби сповіщень – дозволяють надсилати повідомлення електронною поштою та SIEM безпосередньо з VMware Carbon Black Cloud;

служби API – Endpoint Standard і VMware Carbon Black Cloud пропонують різні служби API, такі як:

CBAPI та Rest API;

з'єднувачі SIEM;

двофакторна автентифікація;

SAML-логіни.

CDC Reputation Services – надають інформацію про репутацію файлів, виявлених кінцевими точками під управлінням Endpoint Standard, в режимі реального часу;

служба хмарного аналізу – додатковий компонент, що може бути налаштований в консолі веб-інтерфейсу за допомогою параметра політики «Надсилати невідомі двійкові файли для аналізу», служба хмарного аналізу завантажує копії унікальних виконуваних файлів до Служби репутації CDC для перевірки файлу перед його виконанням;

кероване виявлення (додатковий компонент): VMware Carbon Black Managed Detection – це спеціалізована команда зі спеціальними службами для моніторингу та сортування сповіщень з кінцевих точок.

Таким чином, рішення включає агент на кінцевій точці, хмарну платформу з аналітичним ядром та вебінтерфейс для управління. Така архітектура забезпечує масштабованість, централізований контроль та гнучке розгортання.

2.3 Процеси функціонування рішення Carbon Black Cloud Endpoint Security Standard

Робота рішення Carbon Black Cloud Endpoint Standard побудована на основі безперервного моніторингу та хмарної аналітики подій кінцевих точок організації. Агент встановлюється на кожен пристрій і постійно відслідковує події на рівні ОС: запуск та припинення процесів, операції з файлами і реєстром, мережеві з'єднання, підключення зовнішніх носіїв та інші події. Ці події передаються через безпечне https з'єднання на сервери Carbon Black Cloud для подальшої обробки та аналізу отриманої інформації.

У хмарі отримані події надходять у систему обробки (Event Processing Services), де індексуються та аналізуються. Сенсор приймає рішення застосування дій щодо виконуваних файлів(додатків) на основі їх репутації [21]. Опис типів репутації наведено у таблиці 2.1.

Таблиця 2.1.

Типи репутації у Carbon Black Cloud Endpoint Standard

Тип репутації	**Опис**
Effective Reputation	Присвоюється сенсором, на основі аналітики Carbon Black, хмарних даних та будь-яких інших даних, визначених в момент, коли відбулася подія виконання.
Cloud Reputation (Initial)	Репутація хешу файлу на основі даних Carbon Black Cloud, що присвоюється етапі обробки події хмарними сервісами рішення.
Cloud Reputation (Current)	Перевірка хешу файлу в режимі на основі даних Carbon Black Cloud, що присвоюється у режимі реального часу.

Проаналізований додаток може мати більше однієї репутації. Кількість присвоєних рівнів репутації залежить від кількості різних джерел, які агент використовує для кешування репутацій одного і того ж файлу SHA256. Наприклад, додаток можете мати одну репутацію з хмари, одну – з локального сканера і одну – завдяки попередньому існуванню.

Порядок, в якому Carbon Black Cloud використовує репутації, якщо виконуваний файл має більше однієї репутації наведено у таблиці 2.2. Пріоритет репутації вказано в порядку спадання, де 1 – найвищий пріоритет, а 11 – найнижчий.

Таблиця 2.2.

Можливі значення присвоєної репутації

№	Назва	Опис
1	Ignore	Це самоперевірка, яку Carbon Black Cloud призначає для файлів своїх продуктів, надаючи їм повні дозволи для виконання. Тільки файли, підписані Carbon Black, отримують цей статус. Файли, не підписані Carbon Black, слід додатково перевіряти.
2	Company Approved List	Включає конкретні хеші, які переважають репутації з нижчим пріоритетом. Адміністратор може вручну додавати додаток до списку затверджених компанією за SHA-256 хешем.
3	Company Banned List	Вказує на шкідливу або непотрібну поведінку. Хеші, додані до списку заблокованих компанією, переважають репутації з нижчим пріоритетом.
4	Trusted Approved List	Призначено за допомогою аналітики Carbon Black та джерел розвідки загроз. Вказує на хеш як відомий файл, який не несе загрози. Файл підписаний видавцем та сертифікатом, що знаходиться в списку, керованому Carbon Black.
5	Known Malware	Призначено за допомогою аналітики Carbon Black та джерел розвідки загроз. Вказує на додаток як на відоме шкідливе ПЗ.
6	Suspect Malware (Heuristic)	Призначено за допомогою аналітики Carbon Black та джерел розвідки загроз. Вказує на додаток як на підозріле шкідливе ПЗ, але аналіз не може підтвердити, чи є файл шкідливим. Потрібен подальший аналіз.

№	Назва	Опис
7	Adware/PUP Malware	Призначено за допомогою аналітики Carbon Black та джерел розвідки загроз. Вказує на додаток, який позначений як PUP (потенційно небажана програма) або рекламне ПЗ.
8	Local White	Призначається для файлів, підписаних через сертифікати, файлів, що існують до встановлення сенсора, або файлів, створених додатками, визначеними в IT Tools. Може бути призначено за шляхом файлу або підписом сертифіката.
9	Common Approved List	Призначено, коли файл підписано та він не знаходиться в списках відомих дозволених або шкідливих файлів, або якщо хеш був проаналізований, але не потрапив до цих списків.
10	Not Listed/Adaptive Approved List	Призначається, коли сенсор не може знайти запис про хеш у базі даних репутацій, зазвичай для нових хешів або оновлених додатків. Адаптивний затверджений список потребує додаткового аналізу для повної довіри серед усіх організацій.
11	Unknown	Призначається, коли немає відповіді від жодного з джерел репутацій, що використовуються сенсором. Невідома репутація призначається новим файлам, додаткам, що з'являються на пристрої без активованої локальної скануючої функції, або без мережевого з'єднання з хмарою.

Після визначення репутації із найвищим пріоритетом, система перевіряє дії відповідно до налаштованих політик безпеки. Політика визначає превентивні дії та встановлює налаштування сенсора [22]. Політики – це набір превентивних правил і поведінкових налаштувань, які визначають, як агент взаємодіє з об'єктом і блокує або дозволяє певну поведінку. В рамках політик, можуть бути створені власні правила блокування, дозволів додатків та може бути змінено спосіб взаємодії агенту з хмарою Carbon Black Cloud. Система має попередньо визначені політики, що розроблені вендором як шаблони для поширених випадків використання. Ці політики можуть бути застосовані до сенсорів у першочерговому вигляді або до параметрів політики можуть бути внесені зміни. Попередньо визначені політики не можуть бути видалені.

Попередньо визначені політики встановлюють базовий рівень захисту для ресурсів у середовищі організації. Опис даних політик наведено у таблиці 2.3:

Таблиця 2.3

Опис базових політик Carbon Black Cloud Endpoint Standard

Назва політики	**Опис**
Standard	Блокує відоме та підозріле шкідливе програмне забезпечення, а також запобігає ризикованим операціям, таким як очищення пам'яті та ін'єкції коду. За замовчуванням ця політика призначається усім новим агентам, які розгортаються.
Monitored	Відстежує активність додатків кінцевих пристроїв та реєструє події на Панелі керування. За винятком блокування відомого шкідливого програмного забезпечення, ця політика не виконує жодних превентивних дій.
Advanced	Більш агресивно реагує на дії у системі, політика може блокувати операції від системних утиліт і запобігає ризикованій поведінці, яка з більшою ймовірністю може призвести до хибних спрацьовувань.

Якщо подія відповідає заданим правилам політики (наприклад, запуск небезпечної програми або підозрілої послідовності дій), застосовується налаштована дія реагування на процес, наприклад – блокування. Далі події корелюються між собою та з контекстом інших кінцевих точок – використовується поведінкова аналітика. Загальне правило формування інциденту полягає в тому, що коли система виявляє аномальний патерн у певній послідовності дій, що може свідчити про атаку (наприклад, великий обсяг змін у файлах або підозрілу мережеву активність), створюється інцидент.

Агент може виявляти події, які пов’язані із поведінкою програми-вимагача, фіксуючи типовий ланцюг дій зловмисника, наприклад – процес, який масово шифрує файли. Хмара порівнює цю послідовність дій із шаблоном «ransomware-like behavior» – якщо є співпадіння, система може автоматично припинити процес або виконати іншу дію згідно з застосованою до сенсора політикою захисту. Таким чином Carbon Black Cloud може ідентифікувати підвищену активність програми-вимагача і згенерувати сповіщення з високим пріоритетом, для подальшого розслідування аналітиками безпеки.

Адміністратори/аналітики безпеки можуть взаємодіяти з подіями через веб-консоль Carbon Black Cloud. У консолі можна переглядати список сповіщень безпеки (alerts) та деталі подій (Observations) з усіх кінцевих пристроїв, виконувати пошукові запити по ключовим полям і фільтрувати інциденти за різними ознаками. Аналітик може переглядати пов’язані події, що стали частиною одного інциденту за допомогою їх автоматичного групування та зручного графічного відображення у вигляді дерева подій. На основі зібраної інформації з кінцевих точок, можна відстежити етапи вторгнення, виконання зловмисних дій та прийняти рішення про подальші дії реагування. За необхідності адміністратор безпеки може ініціювати ізоляцію мережевого підключення конкретного пристрою та віддалено підключитися до нього для проведення розслідування та реагування.

Отже, агент системи постійно фіксує активність на пристрої, відправляє дані на аналітичну платформу, де виявляються загрози та генеруються попередження. Реакція може бути автоматизована або ініційована вручну через консоль управління.

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

3.1 Варіант розгортання системи захисту кінцевих точок організації від програм-вимагачів на базі Carbon Black Cloud Endpoint Security Standard

Перед початком впровадження рішення Carbon Black Cloud Endpoint Security Standard необхідно здійснити попередню підготовку інфраструктури. Основні кроки включають:

інвентаризація кінцевих точок. Визначення кількості пристроїв, які підлягають захисту: робочі станції, ноутбуки, сервери. Рекомендовано створити класифікацію за рівнем критичності. Це допоможе зрозуміти необхідний розмір ліцензії;

визначення політик безпеки. До розгортання варто розробити базові політики реагування на інциденти, обмеження доступу, категорії дозволеної активності, політики блокування;

налаштування мережевих з’єднань. Carbon Black працює у хмарному середовищі, тож необхідно підготувати безпечний канал взаємодії між кінцевими точками та хмарною консоллю. Варто забезпечити безперешкодний доступ до *.conferdeploy.net, *.carbonblack.io та інших хмарних ресурсів;

реєстрація в сервісі VMware Carbon Black Cloud.

Після проведення підготовки та реєстрації акаунту, може бути отриманий доступ до хмарної платформи. При вході до консолі, буде відображено аналітична панель з базовою інформацією про систему та підказками, як почати користуватися системою. Приклад вигляду аналітичної панелі зображено на рисунку 3.1.

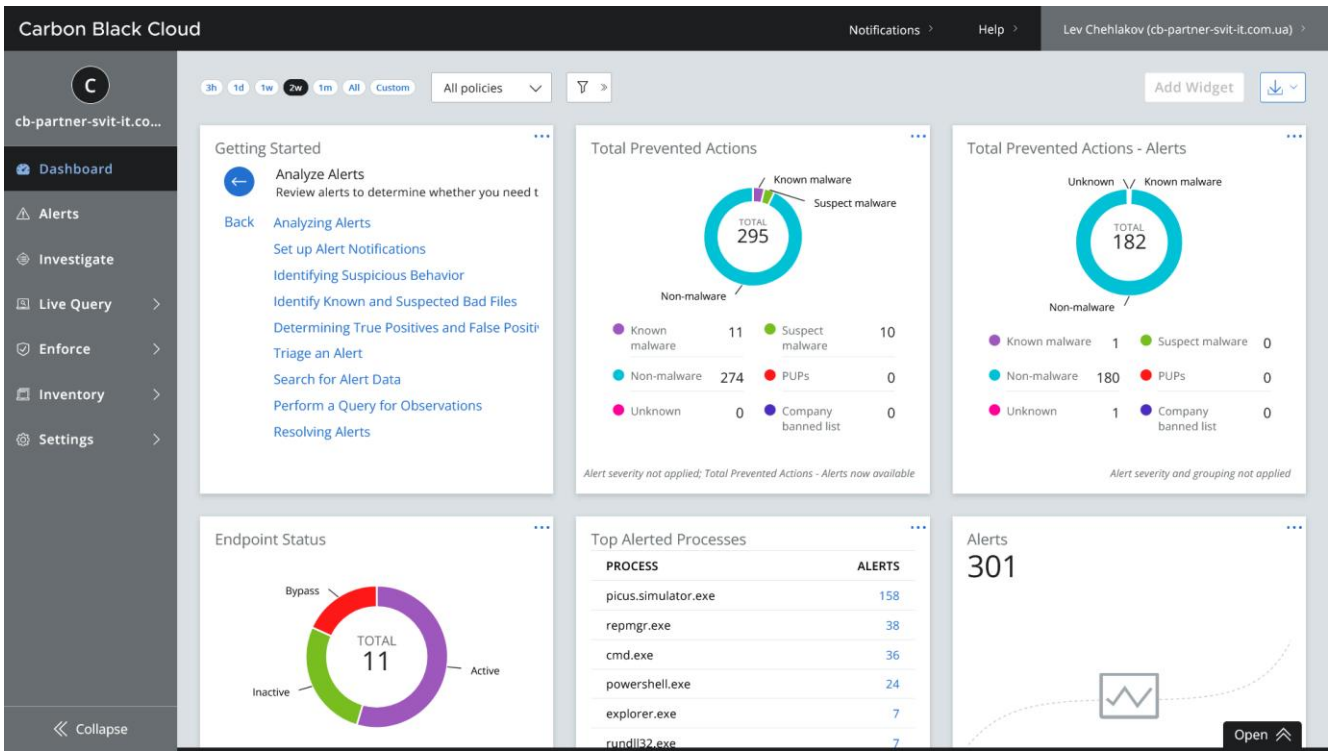


Рис. 3.1. Аналітична панель системи

До консолі можна додати нових користувачів, які будуть займатися аналітикою та/або реагуванням на події, що надходять до системи із кінцевих точок. Права доступу користувача надаються на основі присвоєної користувачу ролі, яка містить в собі певний рівень доступу до різного функціоналу системи. Carbon Black Cloud Endpoint Standard надає деякі попередньо налаштовані ролі, також система дозволяє створювати користувацькі ролі. Приклад створення користувача, що буде мати роль аналітика, зображено на рисунку 3.2.

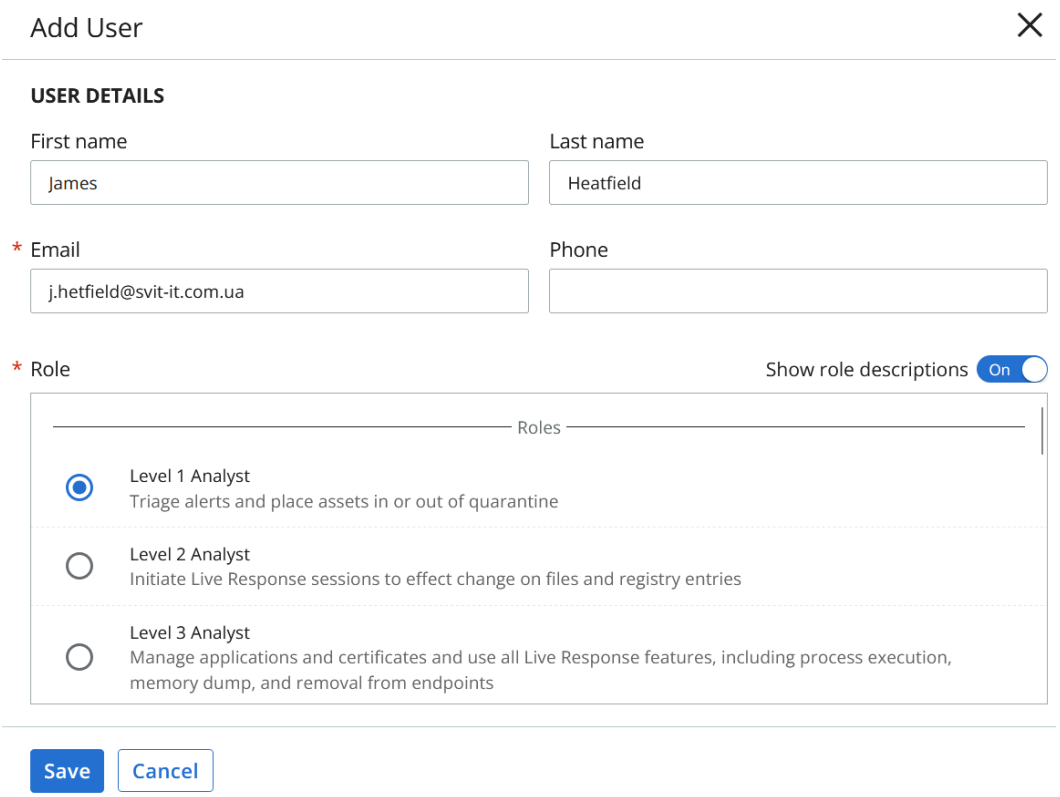


Рис. 3.2. Створення користувача системи

Після додавання користувачів, слід обрати початкову політику, яку буде застосовано до хостів. Для виконання не лише моніторингу, а і блокувань рекомендується почати із політики Standard, яка за замовчуванням наявна у системі. Приклад списку налаштованих політик у системі, зображено на рисунку 3.3.

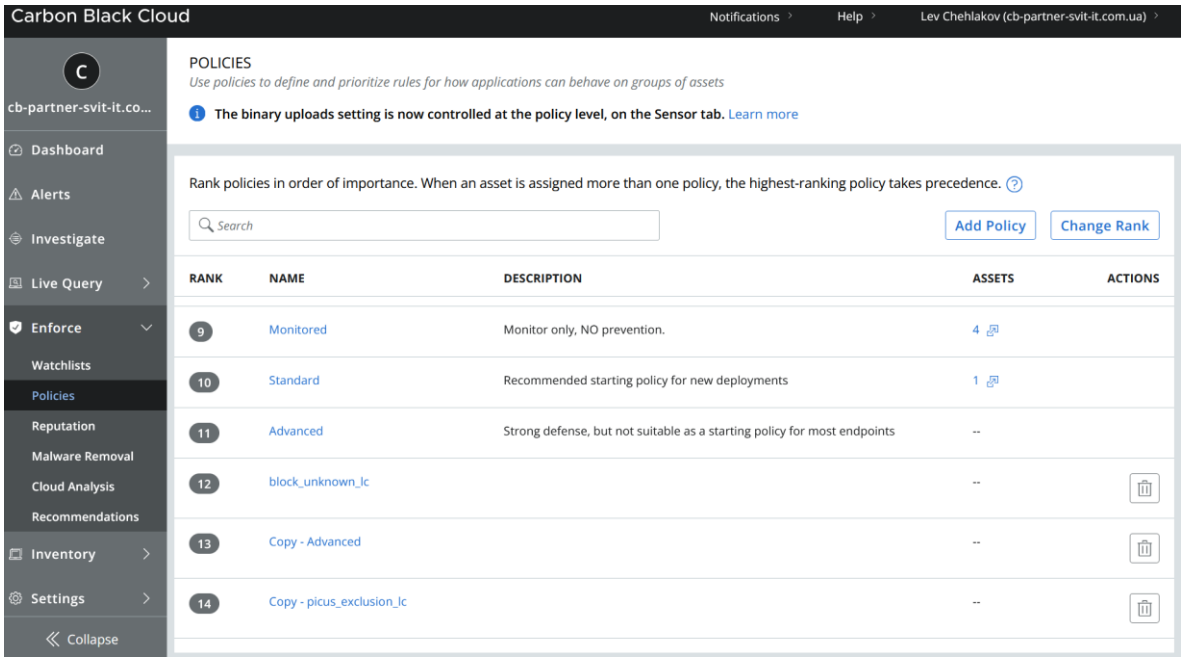


Рис. 3.3. Налаштовані політики захисту системи

Приклад загальних налаштувань політики Standard, зображено на рисунку 3.4.

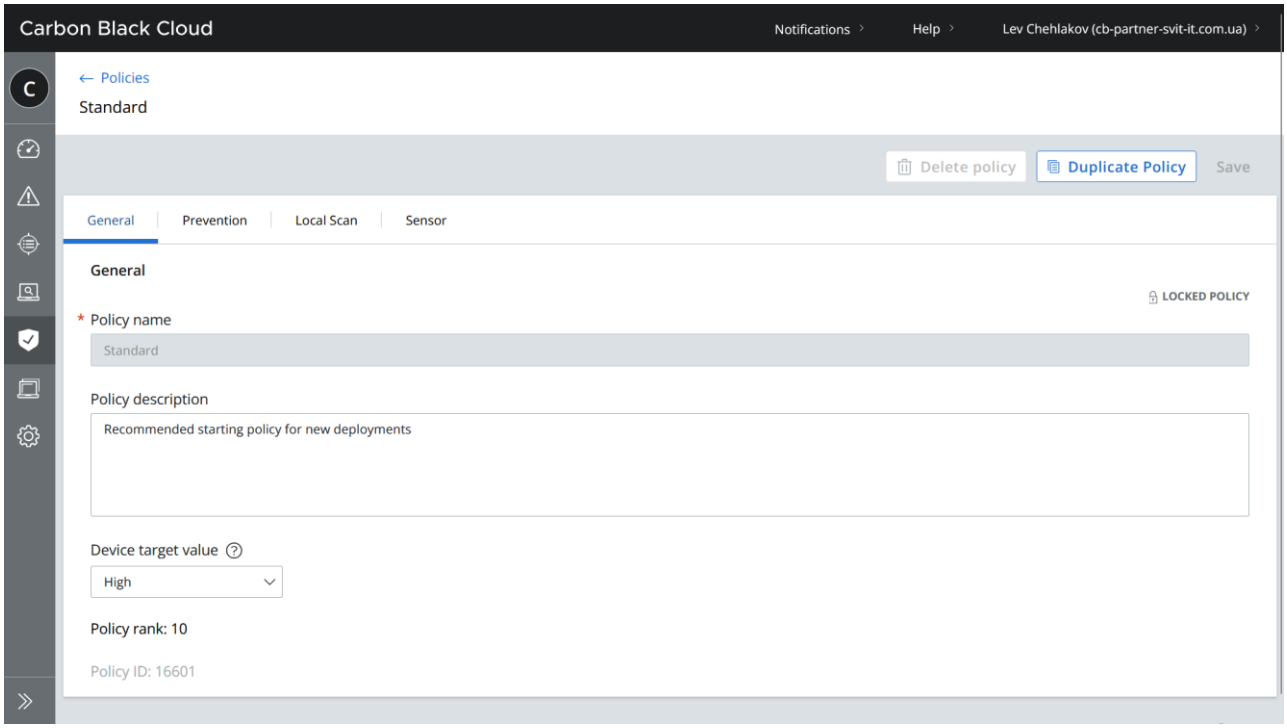


Рис. 3.4. Загальні налаштування політики

Налаштування правил захисту у політиці розподіляються на кілька розділів, які описують:

базовий захист;

дозволи (виключення);

правила блокування та ізоляції;

правила контролю USB девайсів;

правила завантаження файлів до хмари.

Приклад налаштувань правил базового захисту, наведено на рисунку 3.5.

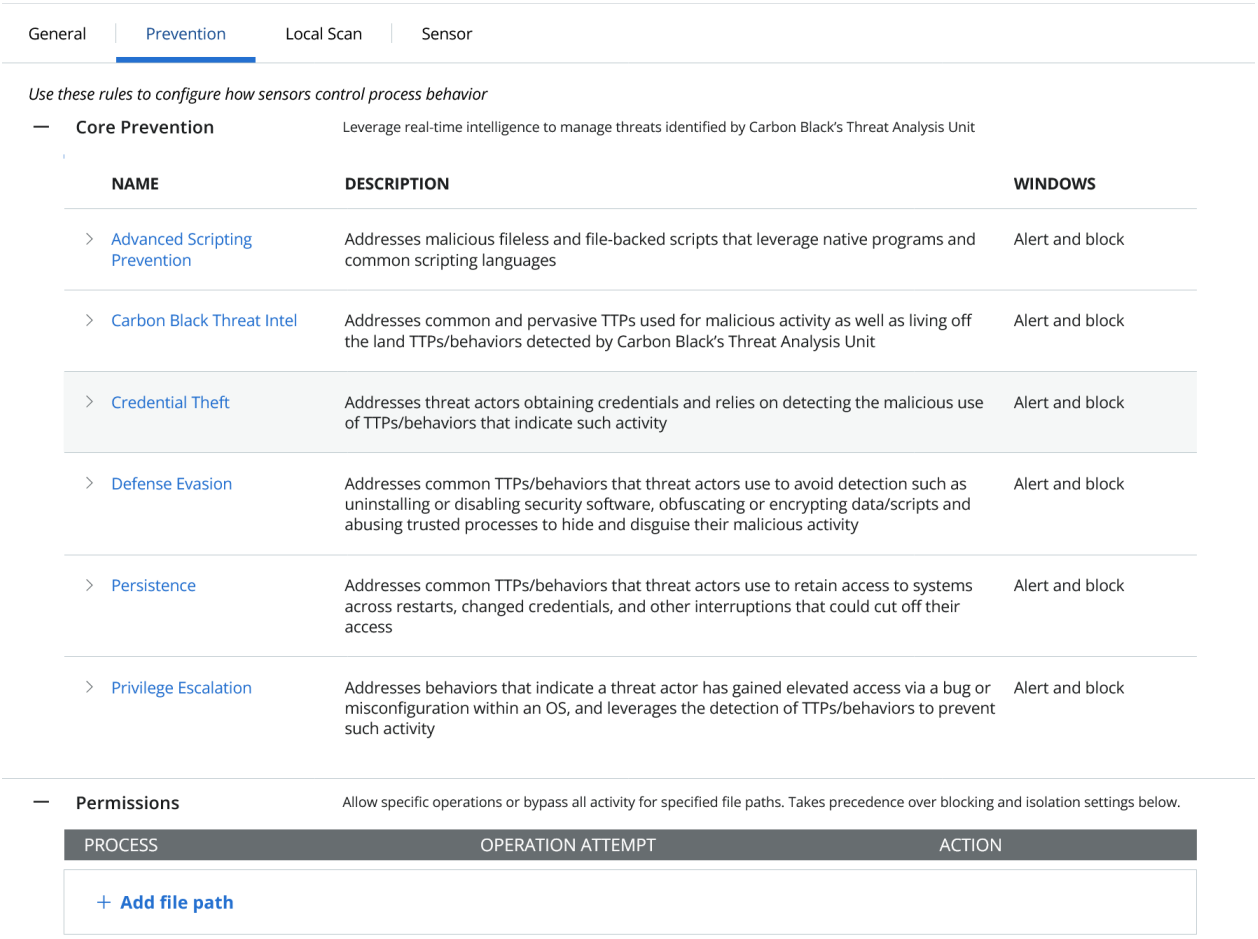


Рис. 3.5. Налаштування базового захисту у політиці

Приклад налаштувань правил блокування та ізоляції, наведено на рисунку 3.6.

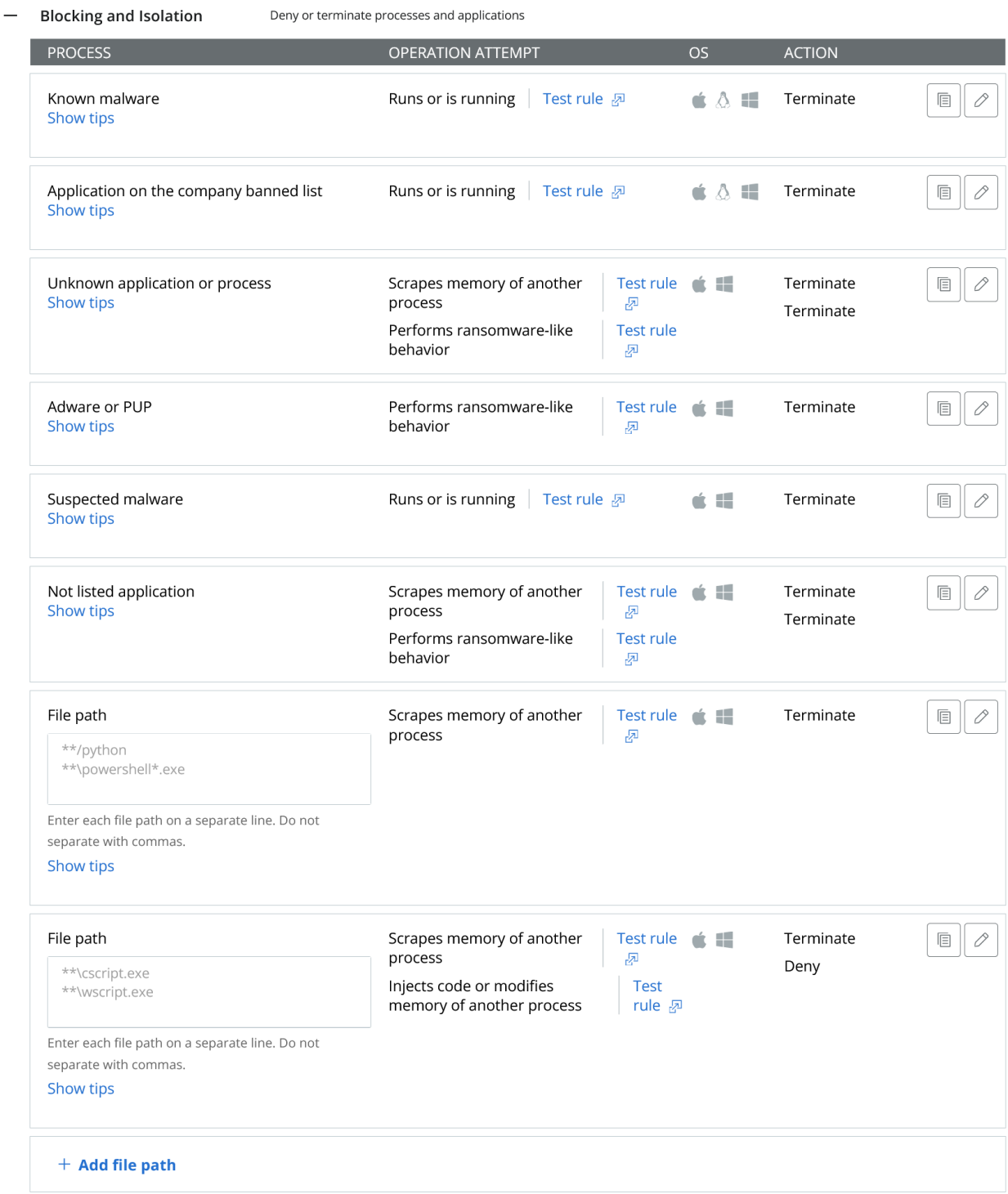


Рис. 3.6. Налаштування правил захисту та блокування

Приклад налаштувань контролю USB девайсів та завантаження файлів до хмари, наведено на рисунку 3.7.

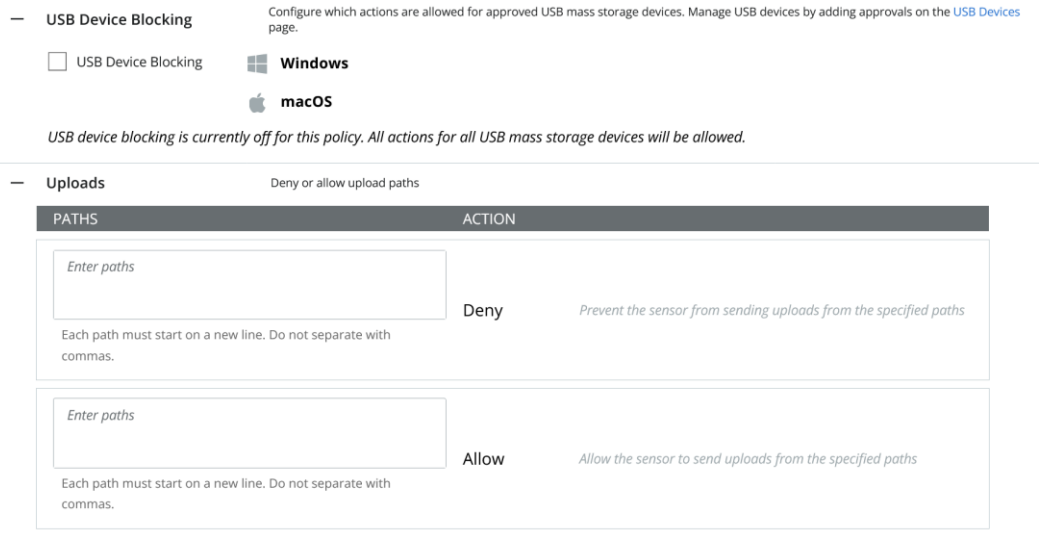


Рис. 3.7. налаштування контролю USB девайсів та завантаження файлів до хмари

Налаштування параметрів локального сканування визначає агресивність сканування виконуваних файлів та параметри оновлень сигнатур. Приклад налаштувань локального сканування зображено на рисунку 3.8.

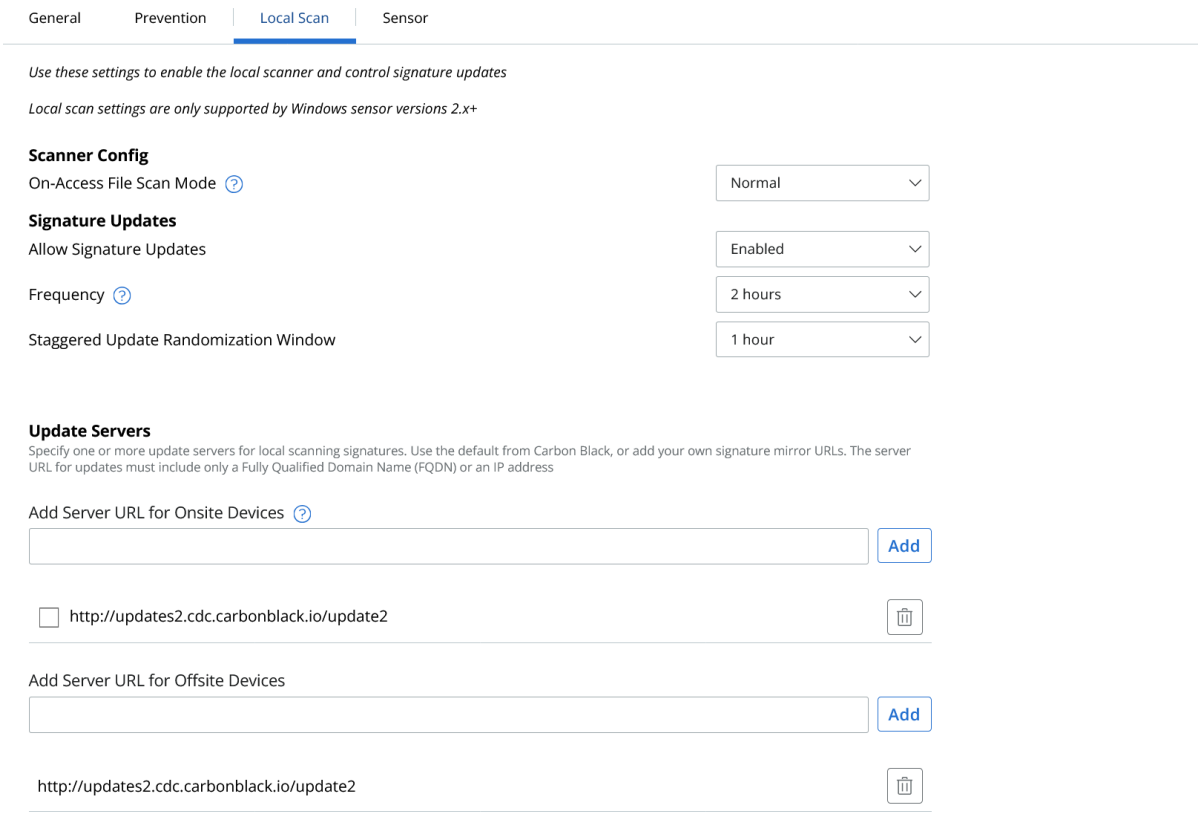


Рис. 3.8. Приклад налаштувань локального сканування

Розділ «Sensor» у політиці – дозволяє налаштувати загальну поведінку сенсора: відображення іконки на кінцевому пристрої, дозвіл на підключення до пристрою з консолі та інші. Приклад налаштування опцій розділу «Sensor», зображено на рисунку 3.9.

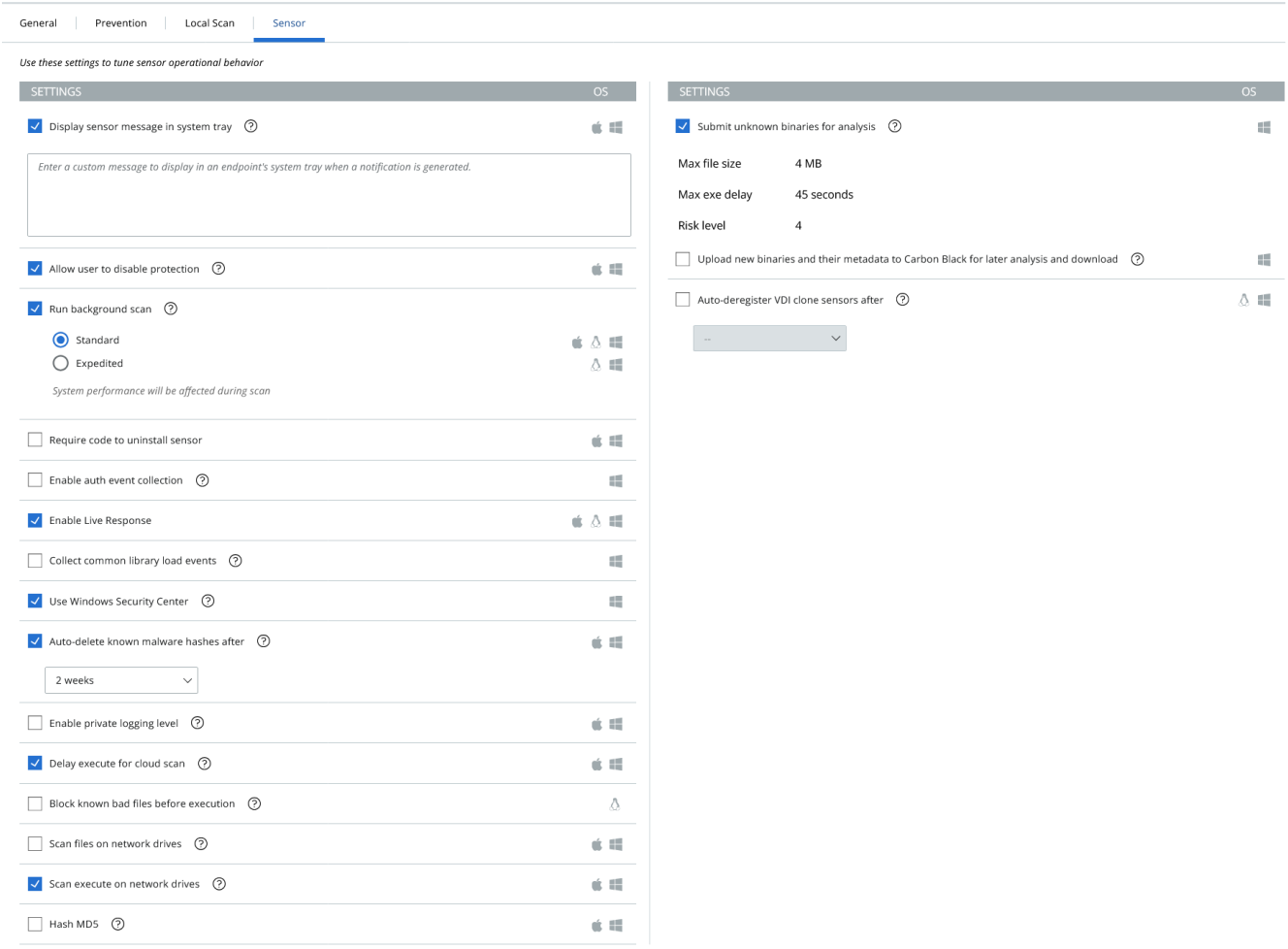


Рис. 3.9. Налаштування загальної поведінки сенсора

Після налаштування політик, необхідно перейти до встановлення сенсорів на пристроях. Одним із методів для встановлення – є відправка запиту на встановлення сенсора до кінцевого користувача по пошті. Приклад відправки з консолі запиту на встановлення сенсора, зображено на рисунку 3.10.

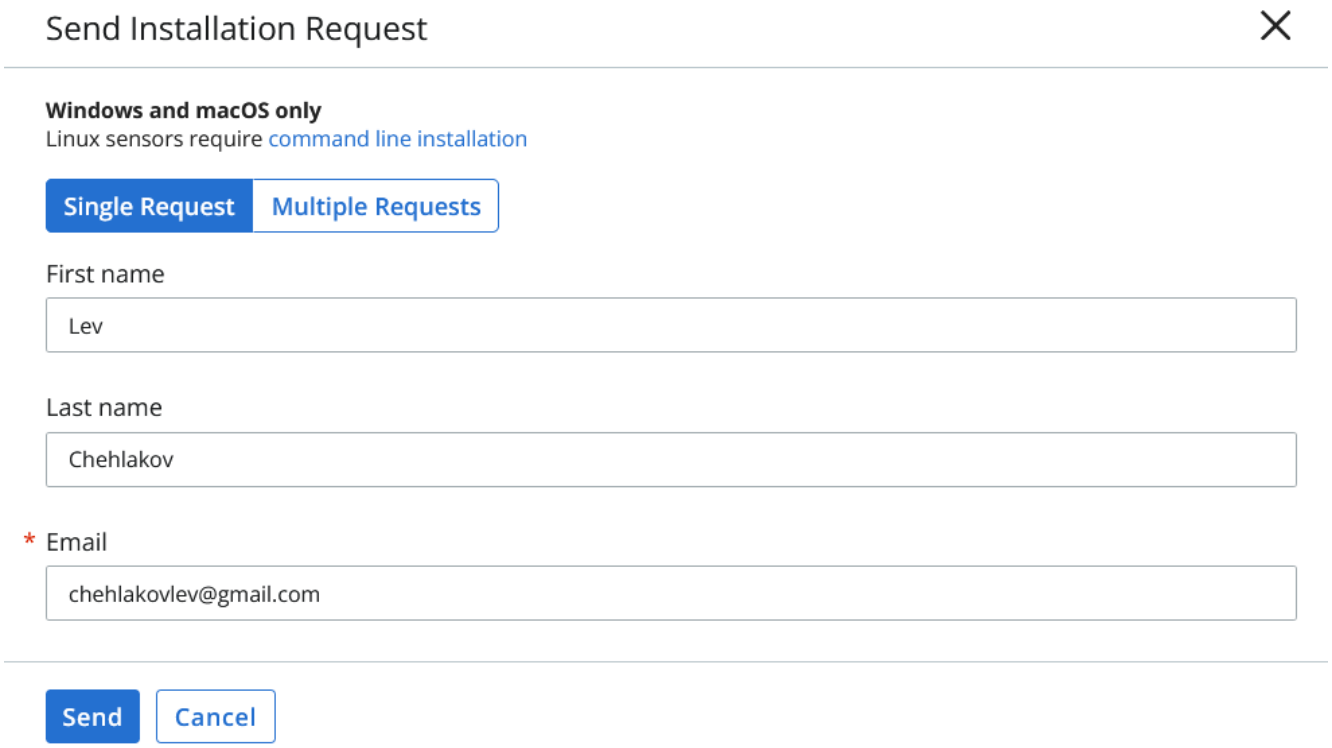


Рис. 3.10. Відправка запиту на встановлення агенту

Запит на встановлення має посилання на завантаження інсталятора сенсора та унікальний код активації для використання під час встановлення. Приклад отриманого на пошту запиту, зображено на рисунку 3.11.

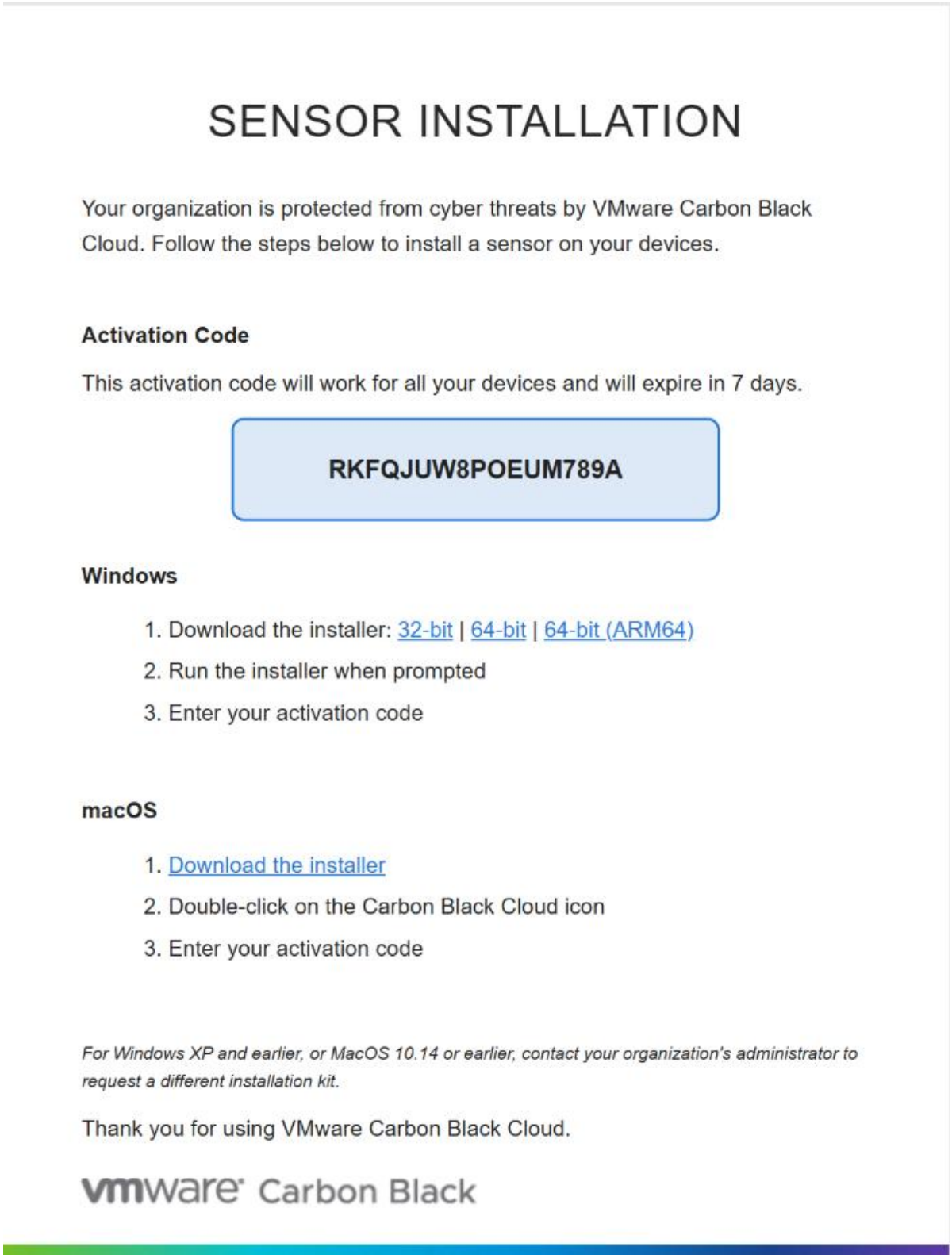


Рис. 3.11. Запит на встановлення сенсора

Приклад використання коду активації продукту під час інсталяції, наведено на рисунку 3.12.

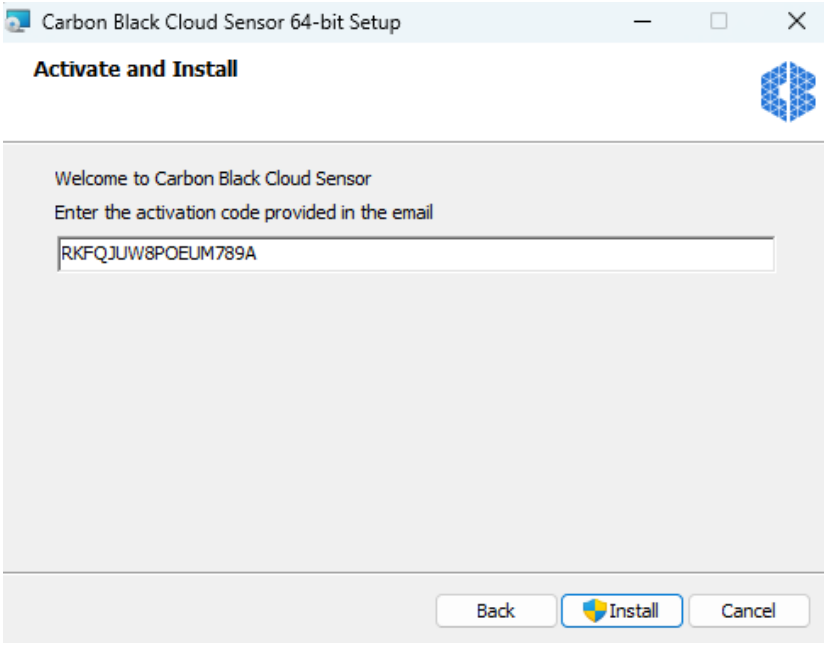


Рис. 3.12. Використання коду активації

Після успішного завершення інсталяції сенсора, він буде відображатися у консолі. З консолі можна здійснювати керування сенсорами, виконуючи наступні дії: видаляти сенсор, присвоювати політику захисту, оновлювати сенсор та інші. Приклад відображення кінцевих точок з встановленим сенсором, зображено на рисунку 3.13.

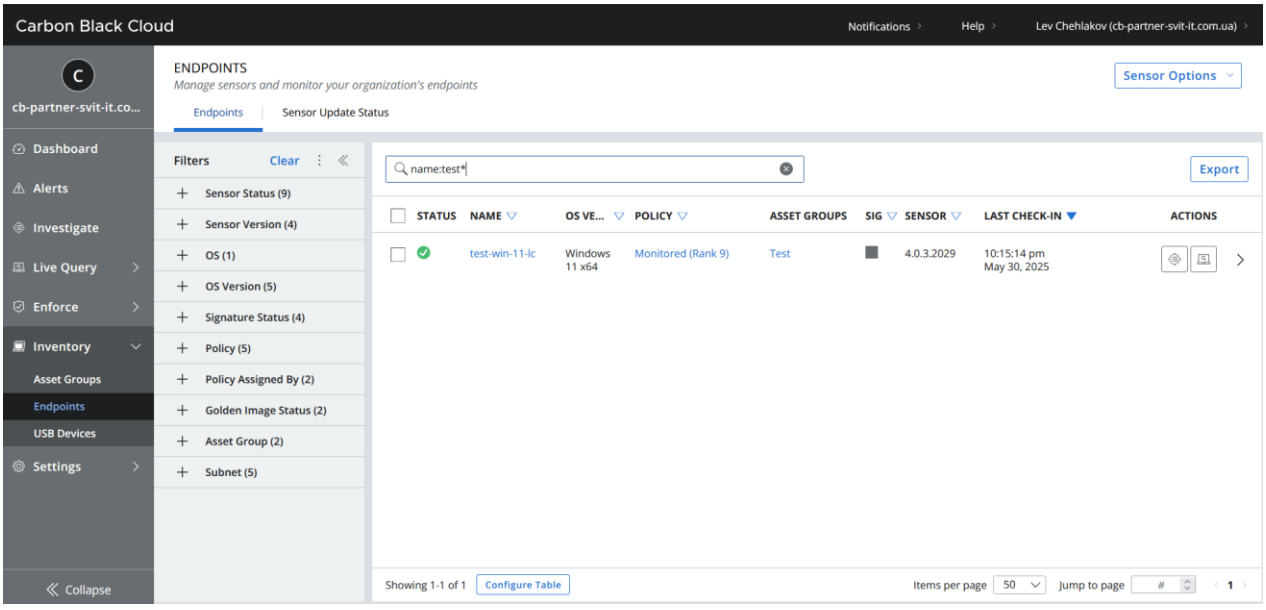


Рис. 3.13. Пристрої, що мають встановлені сенсори

Оскільки за замовчуванням до сенсорів призначається політика «Monitored», необхідно присвоїти політику «Standard» за допомогою дії присвоєння політики для вибраного сенсора. Приклад присвоєння політики «Standard» зображено на рисунку 3.14.

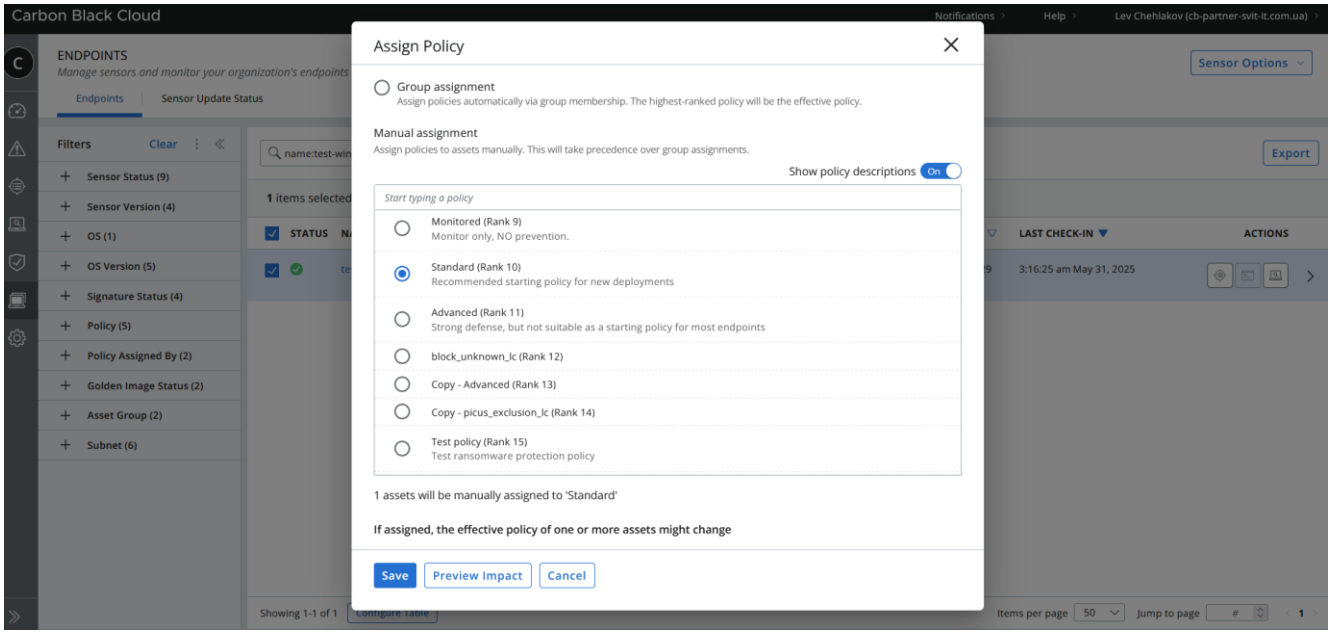


Рис. 3.14. Присвоєння сенсору іншої політики вручну

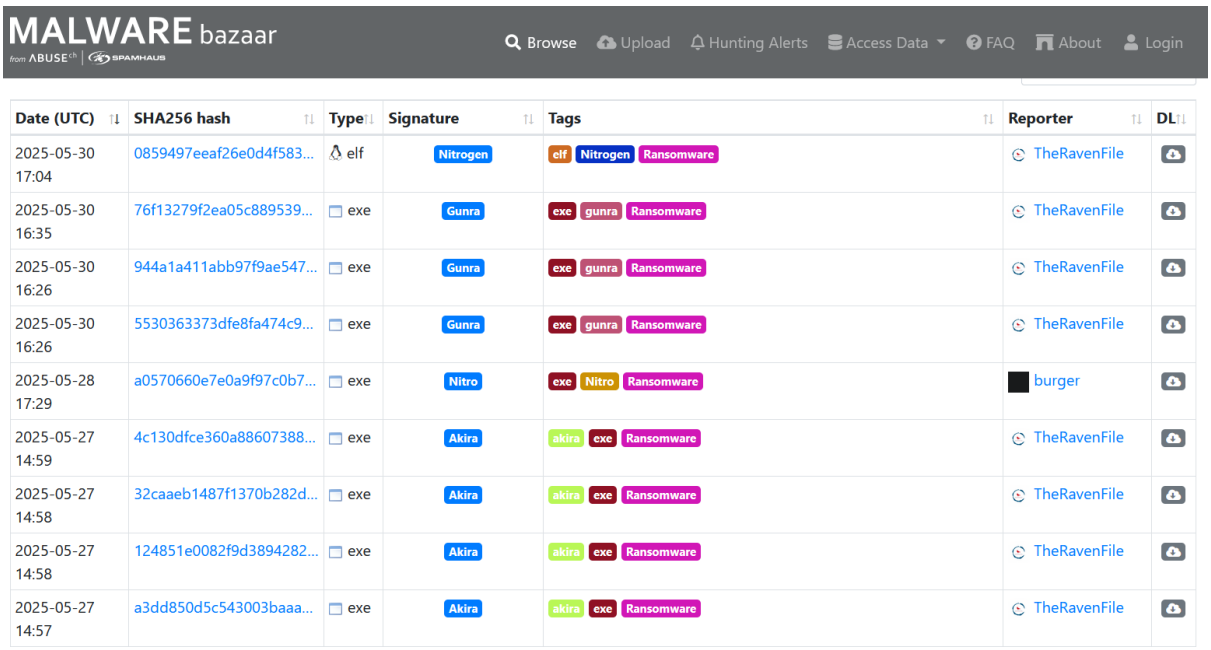
Після зміни політики, сенсору знадобиться декілька хвилин для її отримання з хмари та застосування.

Таким чином, було наведено приклад розгортання системи Carbon Black Cloud Endpoint Security Standard та проведено її початкове налаштування.

3.2 Порядок проведення розслідування інцидентів в рішенні Carbon Black Cloud Endpoint Security Standard

Для перевірки ефективності блокування програм-вимагачів за допомогою рішення Carbon Black Cloud Endpoint Standard, було використано відомі зразки зловмисного програмного забезпечення та симуляцію атак програм-вимагачів.

Відомі зразки програм-вимагачів було завантажено з електронного ресурсу «malware bazaar». Приклад зразків програм-вимагачів, доступних для завантаження зображено на рисунку 3.15.



Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2025-05-30 17:04	0859497eeaf26e0d4f583...	elf	Nitrogen	elf Nitrogen Ransomware	TheRavenFile	
2025-05-30 16:35	76f13279f2ea05c889539...	exe	Gunra	exe gunra Ransomware	TheRavenFile	
2025-05-30 16:26	944a1a411abb97f9ae547...	exe	Gunra	exe gunra Ransomware	TheRavenFile	
2025-05-30 16:26	5530363373dfe8fa474c9...	exe	Gunra	exe gunra Ransomware	TheRavenFile	
2025-05-28 17:29	a0570660e7e0a9f97c0b7...	exe	Nitro	exe Nitro Ransomware	burger	
2025-05-27 14:59	4c130dfce360a88607388...	exe	Akira	akira exe Ransomware	TheRavenFile	
2025-05-27 14:58	32caaeb1487f1370b282d...	exe	Akira	akira exe Ransomware	TheRavenFile	
2025-05-27 14:58	124851e0082f9d3894282...	exe	Akira	akira exe Ransomware	TheRavenFile	
2025-05-27 14:57	a3dd850d5c543003baaa...	exe	Akira	akira exe Ransomware	TheRavenFile	

Рис. 3.15. Відомі зразки програм вимагачів

Рішення Carbon Black Cloud Endpoint Standard блокувало завантажені зразки ШПЗ на етапі запису на диск, що відбувався при розкритті архіву зі зразком. Приклад повідомлення блокування програми зображено на рисунку 3.16.

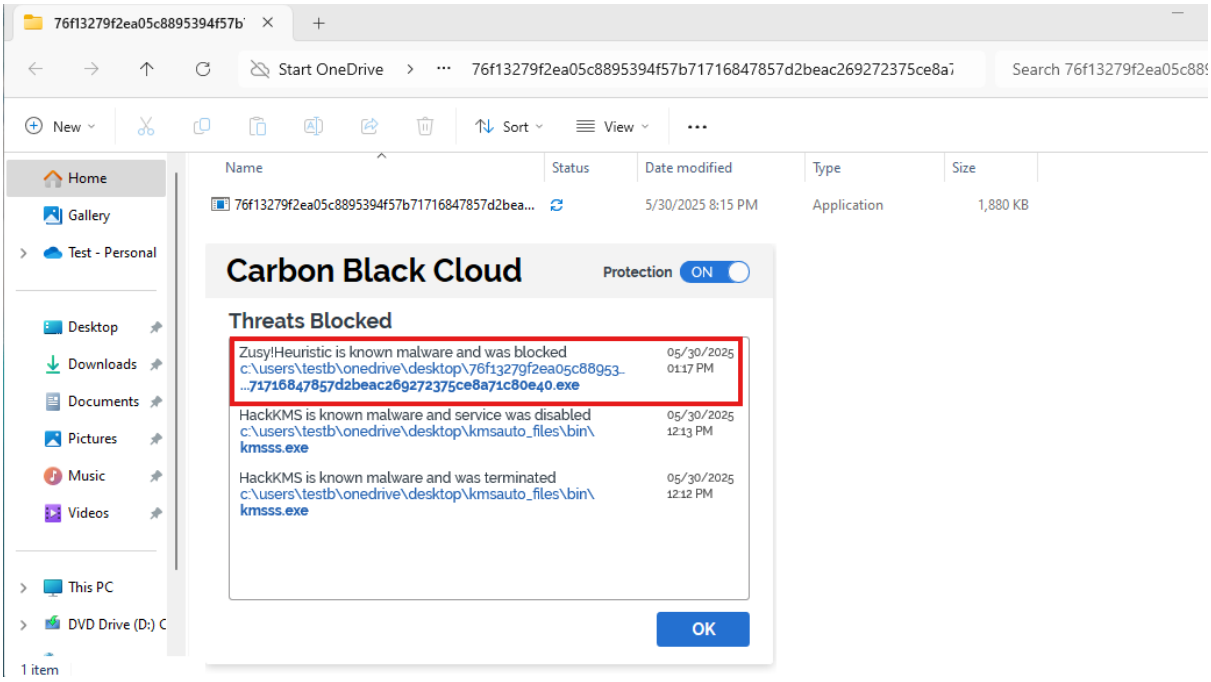


Рис. 3.16. Блокування відомого шкідливого файлу

Для проведення симуляції поведінки програм вимагачів на реальних прикладах послідовності дій, що зловмисники виконують під час атаки, було використано BAS платформу Picus. Оскільки Picus використовує агент для симуляції атак, було створено та застосовано нову політику захисту до сенсора, для уникнення небажаного блокування агенту Picus. З платформи Picus було запущено симуляції декількох реальних прикладів атак програм вимагачів на кінцеві пристрої, перелік яких зображено на рисуннку 3.17. За результатами проведення симуляції, усі акти були успішно заблоковані, хоча деякі етапи цих атак пройшли успішно.

Threat Name	Severity	Attack Module	Actions	Attacker's Objectives	Prevention
Picus Labs CVE 2025-29824 Post-Exploitation Campaign		Windows Endpoint	11 Actions	2 3	
Medusa Ransomware Campaign		Windows Endpoint	18 Actions	4 3	
Black Basta Ransomware Chat Log Campaign		Windows Endpoint	11 Actions	2 5	
Helldown Ransomware Campaign		Windows Endpoint	13 Actions	3 3	
Ryuk Ransomware Campaign		Windows Endpoint	11 Actions	1 4	
Ragnar Locker Ransomware Campaign		Windows Endpoint	11 Actions	3 3	
TA505 Ransomware Campaign		Windows Endpoint	10 Actions	1 6	
Netwalker Ransomware Malware Campaign		Windows Endpoint	6 Actions	2 1	
Valak Ransomware Malware Campaign		Windows Endpoint	7 Actions	3 1	

Рис. 3.17. Симуляція атак програм вимагачів

У системі Carbon Black, було створено відповідні сповіщення про зловмисну активність на кінцевому пристрої, сповіщення зображені на рисунку 3.18.

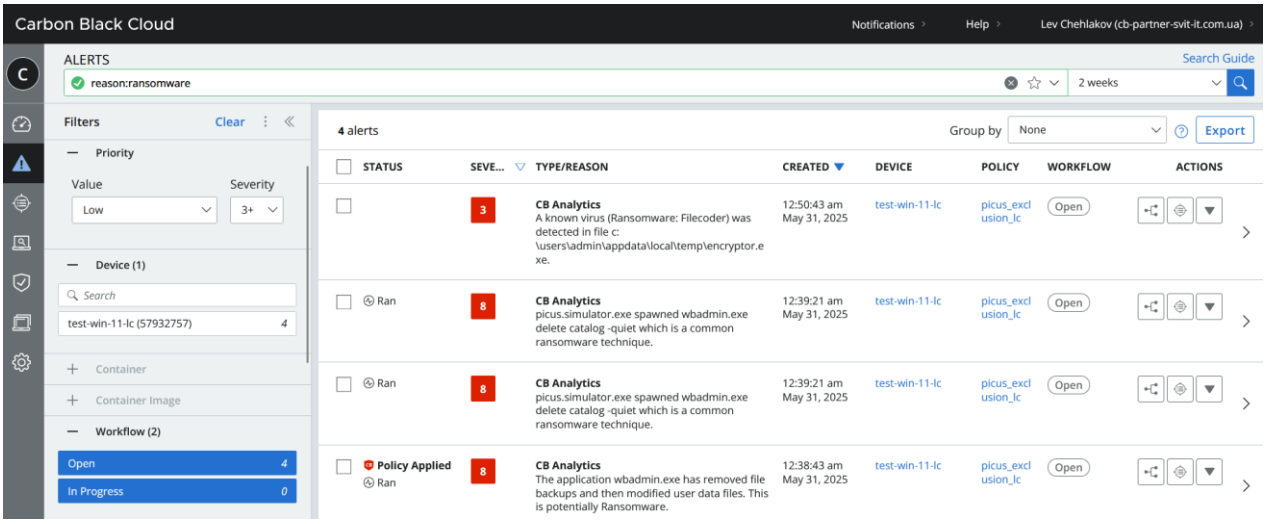


Рис. 3.18. Сповіщення про зловмисну поведінку

Після відкриття деталей спрацювання сенсора, можна переглянути детальну інформацію про сукупність дій на кінцевому пристрої, що спричинили дане спрацювання. Також можна переглянути візуалізацію дерева процесів, що призвели до створення спрацювання, як зображено на рисунку 3.19.

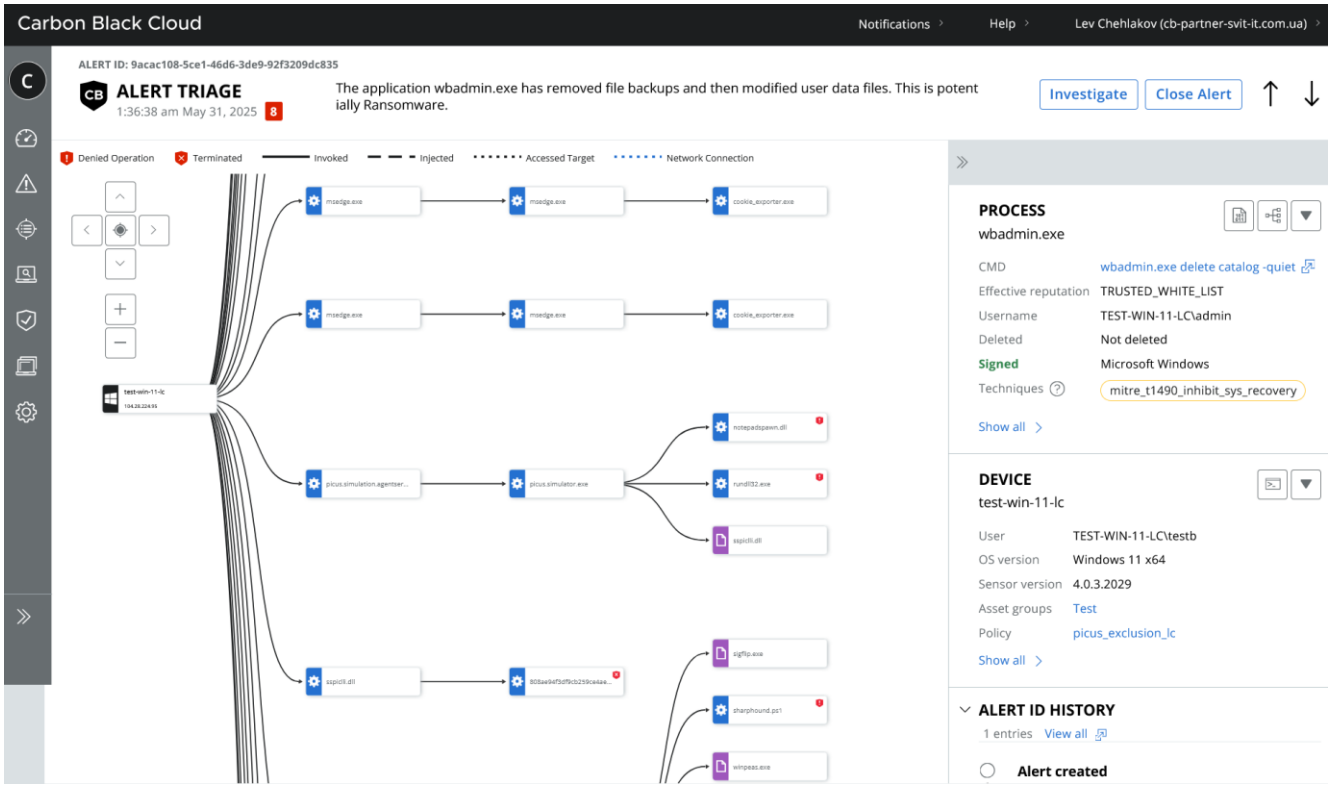


Рис. 3.19. Деталі спрацювання

Натиснувши кнопку «Investigate», можна перейти до розслідування конкретного процесу, що виконував зловмисні дії, як зображено на рисунку 3.20.

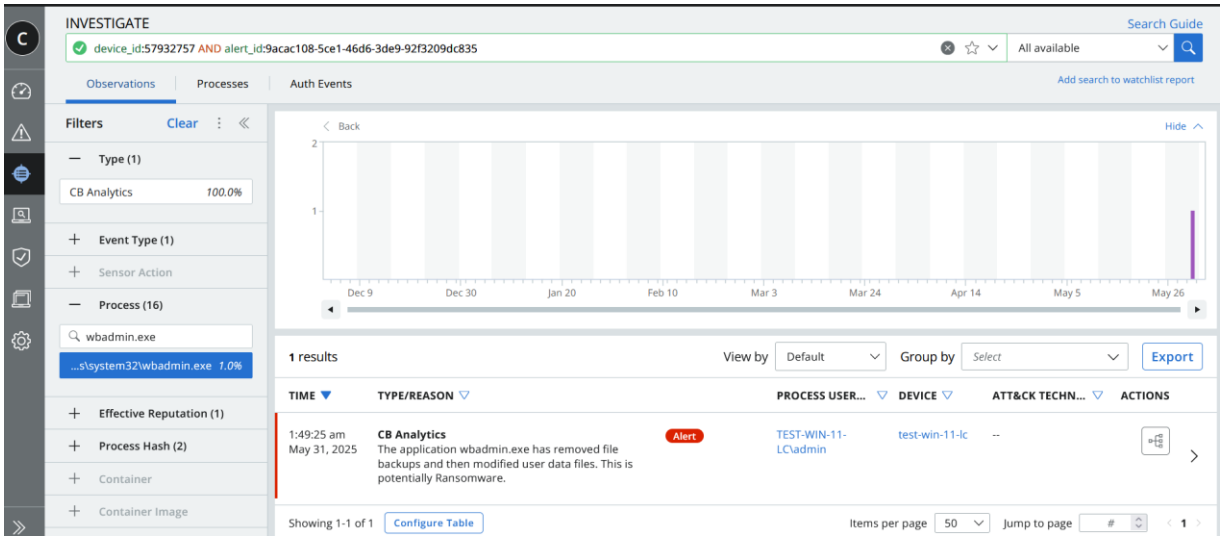


Рис. 3.20. Розслідування процесу

Відкривши деталі процесу, можна побачити інформацію про його шлях, значення хешу SHA-256, ідентифікаційний номер на момент виявлення та пов’язані процеси, як показано на рисунку 3.21.

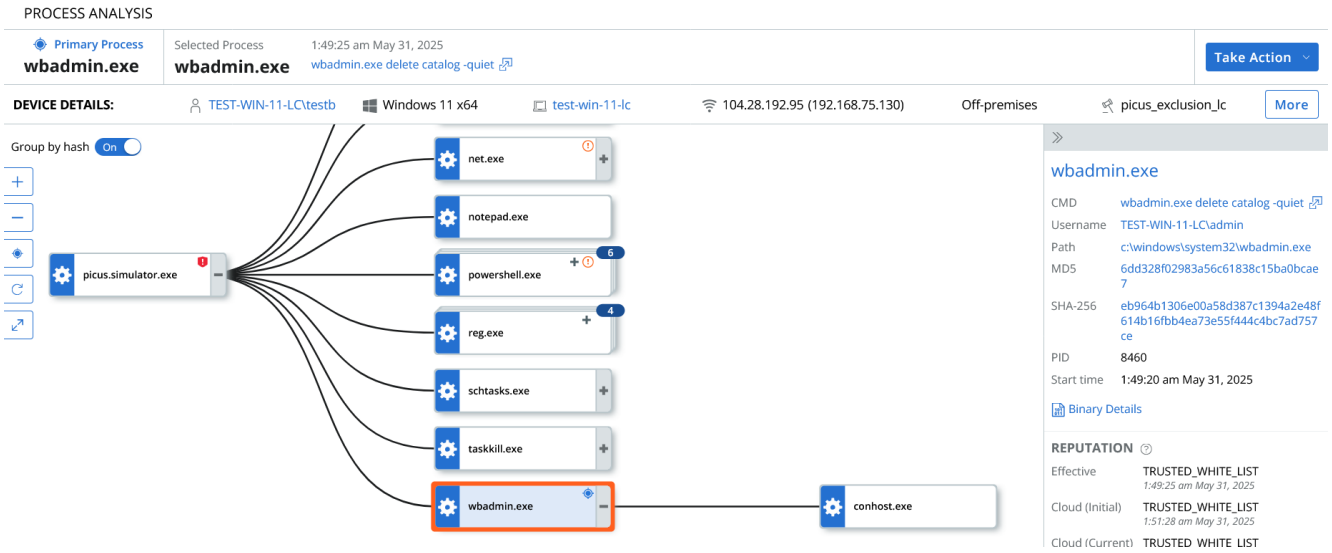


Рис. 3.21. Інформація про процес, що здійснював зловмисну поведінку

Із панелі інформації про процес можна виконати певні дії реагування на зловмисну поведінку, перелік дій зображено на рисунку 3.22.

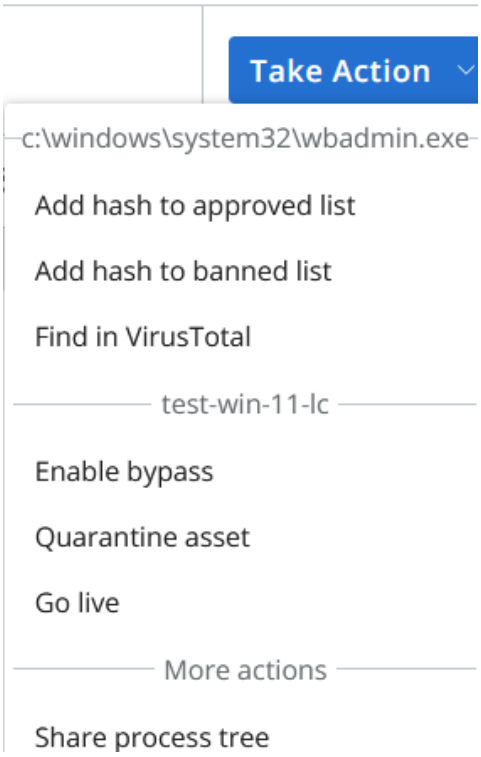


Рис. 3.22 . Доступні дії для виконання

Зокрема, можна виконати ізоляцію хоста за допомогою дії Quarantine asset, для обмеження мережевої активності, щоб попередити розповсюдження атаки у мережі. Також можна виконати підключення у режимі реального часу до хоста, де було помічено зловмисний процес, для виконання глибшого розслідування та реагування. Приклад підключення до хоста та перелік доступних для виконання команд зображено на рисунку 3.23.

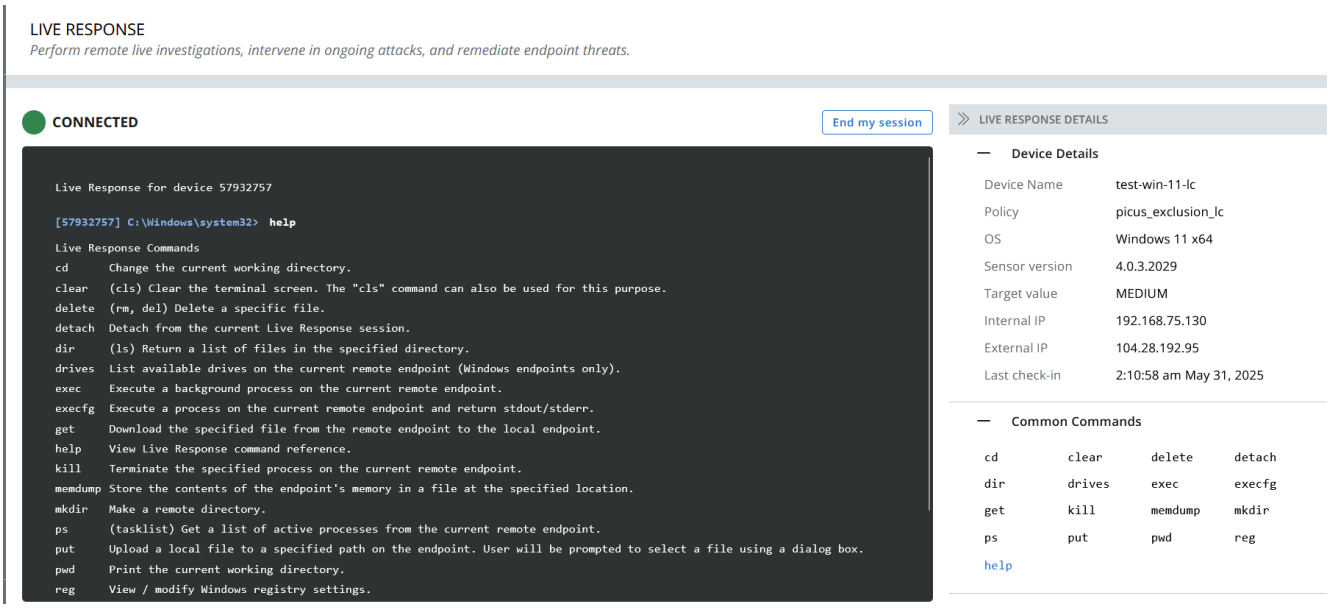


Рис. 3.23. Підключення у режимі реального часу до кінцевого пристрою

Після проведення розслідування, сповіщення може бути закрите, як показано на рисунку 3.24

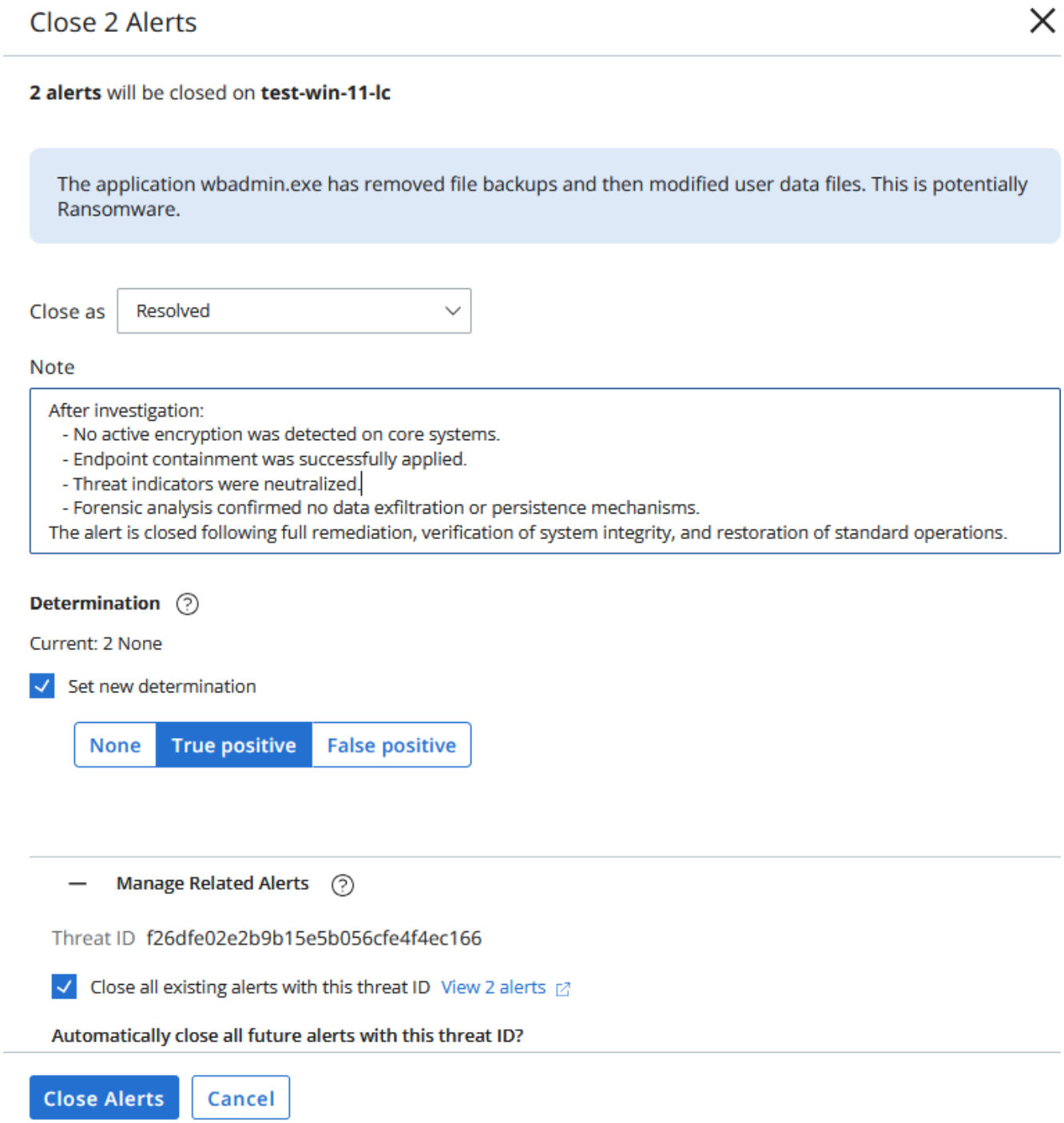


Рис. 3.24. Закриття сповіщення

За результатами тестування рішення Carbon Black Cloud Endpoint Standard, рекомендується виконувати наступні дії, для покрашення ефективності роботи системи :

під час впровадження поступово підвищувати агресивність політик захисту, попередньо протестувавши нові політики у тестовому середовищі, для відслідковування та виправлення потенційної некоректної роботи сенсорів, наприклад – виявлення false-positive та додавання їх у виключення;

розподілення прав доступу до системи серед адміністраторів, аналітиків SOC і інших співробітників відповідно до принципу мінімальних привілеїв, використовуючи вбудовану систему ролей Carbon Black. Регулярно переглядати та редагувати список доданих до консолі користувачів відповідно до кадрових змін у організації або при зміні функціональних обов'язків;

налаштувати передачу подій у SIEM-систему для проведення кореляційного аналізу;

регулярно перевіряти наявність оновлень для агентів та сигнатур Carbon Black на кінцевих точках, а також ревізувати й коригувати політики безпеки з урахуванням нових типів загроз;

регулярно переглядати створені для інтеграції з іншими рішеннями API ключі, безпечно зберігати API ключі;

регулярно переглядати додані до виключень програми.

Рекомендації з покращення захисту від програм вимагачів:

у налаштованих політиках додати опцію блокування процесу, якщо помічено поведінку схожу на типову поведінку програм вимагачів. Застосувати дану опцію до вказаних категорій процесів:

Not listed application;

Unknown application or process;

Suspected malware;

Adware or PUP.

у налаштованих політиках додати опцію блокування процесу, якщо помічено поведінку схожу на типову поведінку програм вимагачів для наступних поширених розширень, які можуть бути використані під час атаки:

***.a3x	***.ppam	***.vbe
***.bat	***.pps	***.vbs
***.bin	***.ppsm	***.vbscript
***.btm	***.ppsx	***.wcm
***.cmd	***.ppt	***.wpm
***.com	***.pptm	***.ws
***.doc	***.pptx	***.wsf
***.docb	***.ps1	***.wsh
***.docm	***.ps1xml	***.xlam
***.docx	***.psc1	***.xlm
***.dotm	***.psd1	***.xls
***.exe	***.psm1	***.xlsb
***.js	***.py	***.xlsb
***.jse	***.pyc	***.xlsm
***.jsx	***.pyo	***.xlsx
***.pot	***.scr	***.xlt
***.potm	***.sys	***.xltm
***.potx	***.tmp	***.xltx
***.ppam	***.vb	

Отже, було наведено приклад проведення розслідування інциденту у системі Carbon Black Cloud Endpoint Security Standard на прикладі симуляції атаки програми-вимагача. Надано рекомендації для налаштування Carbon Black Cloud Endpoint Security Standard, що підвищать ефективність виявлення та блокування програм вимагачів.

3.3 Рекомендації щодо застосування методів та засобів захисту кінцевих точок організації від атак програм-вимагачів

Рекомендується дотримуватися найкращих практик поглибленого захисту для захисту від програм вимагачів. Зокрема, відповідно до звіту NIST по управлінню ризиками програм-вимагачів [23], рекомендується виконувати наступні базові дії для захисту від програм-вимагачів:

1. Проводити навчання співробітників, як уникнути зараження прогамами-вимагачами:

не відкривати файли або переходити за посиланнями з невідомих джерел без попередньої перевірки антивірусом або уважної перевірки посилань;

не використовувати особисті вебсайти та застосунки (електронна пошта, чати, соцмережі) з робочих комп'ютерів;

не підключати особисті пристрої до робочих мереж без дозволу;

проводити навчання працівників щодо кібергігієни та загроз програм-вимагачів.

2. Визначати та виправляти вразливості, що можуть бути використані програмами-вимагачами:

вчасно встановлювати патчі та оновлення безпеки на кінцевих точках;

використовувати принцип нульової довіри (zero trust) у мережі організації, для уникнення розповсюдження програм-вимагачів в середині організації;

налаштувати кінцеві пристрої так, щоб для виконання дозволялися лише авторизовані додатки, які було додано до білого списку;

3. Проводити навчання з виявлення атак

використовувати програмне забезпечення для виявлення шкідливого ПЗ (NGAV, EDR та інші), зокрема налаштувати автоматичну перевірку електронної пошти та USB-носіїв на наявність зловмисних програм;

постійно відстежувати служби каталогів, журнали подій та інші дані функціонування на предмет компрометації або активної атаки;

блокувати доступ до серверів, IP-адрес, портів або протоколів, що відомі як зловмисні, а також використовувати продукти з перевіркою доменів на цілісність.

4. Ускладнювати поширення ransomware:

не використовувати облікові записи з адміністративними привілеями без потреби – використовувати стандартні облікові записи з багатофакторною автентифікацією;

не залишати систему автентифікації без захисту – впровадити затримки автентифікації або автоматичне блокування облікових записів при спробах підбору паролів;

керувати доступом до облікових записів та регулярно перевіряти, що кожен користувач має лише необхідні повноваження для виконання функціональних обов'язків;

не зберігати критичні дані у змінному вигляді – використовувати незмінні формати зберігання даних для уникнення їхнього автоматичного перезапису;

не дозволяти необмежений зовнішній доступ до внутрішньої мережі – забезпечити доступ лише через безпечні VPN-з'єднання.

5. Проводити навчання та підготовку до реагування на атаки програм-вимагачів:

розробити, реалізувати і регулярно тестувати план реагування на інциденти з атак програм-вимагачів, включаючи розподіл ролей та стратегій прийняття рішень;

створювати резервні копії, забезпечити їх безпеку та ізоляцію, і регулярно тестувати процес відновлення;

підтримувати актуальний список контактів для реагування на атаки (внутрішні й зовнішні), включаючи правоохоронні органи, юристів і фахівців з інцидентів.

Також, загальні рекомендації щодо захисту від атак типу ransomware на кінцеві точки, описано у міжнародному стандарті ISO/IEC 27002:2022 [24]. Вони охоплюють ключові технічні та організаційні заходи, які слід впроваджувати для зниження ризиків, пов'язаних із шкідливим програмним забезпеченням:

сканування електронної пошти – сканування вмісту та фільтрація електронної пошти повинні використовуватися для виявлення шкідливих програм до того, як

вони потраплять до кінцевих користувачів та зможуть бути завантажені і виконані на кінцевій системі;

спам-фільтрація – виконує запобігання потрапляння фішингових електронних листів до кінцевих користувачів. Крім того, спам-фільтри фільтри перевіряють автентичність вхідних електронних листів за допомогою таких технологій, як Sender Policy Framework і DomainKeys Identified Mail;

блокування реклами – блокування банерів та інших видів реклами, що можуть вести на фальшиві сайти, через які може відбуватися завантаження програм-вимагачів;

використання мережевих фільтрів – застосування програмних або апаратних пристроїв, що контролюють мережевий трафік за допомогою політик чи правил доступу або блокування, що можуть бути налаштовані для IP-адрес, MAC-адрес та портів. Існують також мережеві фільтри для конкретних додатків, наприклад, фільтри для веб-додатків (WAF) і безпечні поштові шлюзи, які зосереджені на виявленні зловмисної активності, спрямованої на певний додаток;

використання систем виявлення та запобігання вторгнень (IDS/IPS) – IDS надсилає сповіщення, коли виявлення зловмисного мережевого трафіку, в той час як IPS намагається запобігти та попередити про виявлену зловмисну активність у мережі або на робочій станції користувача. Ці рішення базуються на розпізнаванні атак на сигнатурах відомої зловмисної мережевої активності;

сегментація мережі – поділ мережі на кілька підмереж, створених відповідно до бізнес-потреб і технологічних вимог, для зменшення ризику розповсюдження програм-вимагачів у мережі організації. Це може включати різні підмережі для керівників, фінансів, операцій та людських ресурсів. Залежно від необхідного рівня безпеки, ці мережі можуть не можуть не мати змоги спілкуватися безпосередньо. Сегментація часто здійснюється за допомогою використання мережевих комутаторів або правил брандмауера;

перевірка внутрішнього трафіку – виявляє трафік командування і управління (C2) на основі даних про відомі загрози, включаючи виявлення підключень до

зловмисних IP-адрес, доменів чи використання підозрілих сертифікатів під час комунікації;

сканування мережевих артефактів – динамічний аналіз поведінки файлів на наявність загроз за допомогою штучного інтелекту для виявлення шкідливого коду.

захист автономних резервних копій – окреме збереження та захист копій гарантує, що резервні копії не будуть постійно підключені до комп'ютерів та мереж, до яких вони до комп'ютерів і мереж, для яких створюються резервні копії, відповідно вони не будуть зашифровані у разі успішної реалізації атаки програм-вимагачів.

ВИСНОВКИ

У роботі проведено дослідження проблеми захисту кінцевих точок організації від атак програм-вимагачів, визначено її мету та завдання. Сучасні організації стикаються зі значним зростанням кількості та складності атак програм-вимагачів, що створює серйозні ризики для цілісності та доступності даних на кінцевих точках. Існуючі засоби захисту часто виявляються недостатніми для ефективної протидії цим загрозам.

Проаналізовано основні методи та засоби захисту кінцевих точок організації від програм-вимагачів. Традиційні антивірусні рішення часто не забезпечують достатнього рівня протидії сучасним багатовекторним атакам. Ефективний захист кінцевих точок від програм-вимагачів потребує проактивних методів виявлення, таких як поведінковий аналіз, машинне навчання та аналіз репутації файлів, здатних ідентифікувати підозрілу активність ще до того, як вона завдасть шкоди.

Проаналізовано існуючі рішення захисту кінцевих точок організації від програм-вимагачів. Розглянуто провідні платформи, що пропонують захист від програм-вимагачів. Системи EDR, завдяки своїм можливостям безперервного моніторингу, збору детальної телеметрії та аналізу подій на кінцевих точках, є найбільш ефективними у боротьбі зі складними та прихованими атаками програм-вимагачів. Дані системи мають функціональні можливості виявлення аномалій та оперативного реагування на загрози.

Проаналізовано методи та засоби захисту кінцевих точок організації від атак програм-вимагачів на базі Carbon Black Cloud Endpoint Security Standard. Розглянуто архітектуру платформи Carbon Black Cloud, її ключові компоненти та їх функції. Описано, як Carbon Black Cloud використовує хмарні технології для аналізу загроз у реальному часі, поведінкового аналізу та аналізу репутації для виявлення та блокування програм-вимагачів. Показано механізми автоматизованого реагування, ізоляції скомпрометованих пристроїв та відновлення після атаки.

Запропоновано варіант системи захисту кінцевих точок організації від програм-вимагачів на базі Carbon Black Cloud Endpoint Security Standard. Описано послідовність етапів впровадження, необхідні налаштування політик безпеки та використання централізованої консолі управління для моніторингу та реагування. Представлено принципи конфігурування захисних механізмів для максимальної ефективності протидії атакам програм-вимагачів.

За результатами проведеної роботи розроблено рекомендації щодо захисту кінцевих точок організації від програм-вимагачів. Ці рекомендації враховують технічні аспекти розгортання та налаштування Carbon Black Cloud Endpoint Security Standard, організаційні аспекти управління інцидентами, а також найкращі практики щодо моніторингу, реагування та підтримки системи. Вони спрямовані на підвищення загального рівня кіберстійкості організації до атак програм-вимагачів.

Отже, захист кінцевих точок від атак програм-вимагачів займає ключове місце серед процесів, що підтримують безперервну діяльність організації. Carbon Black Cloud Endpoint Security Standard – це комплексне рішення, що дозволяє не лише ефективно виявляти та блокувати програми-вимагачі, а й надавати глибинний контекст для розслідування інцидентів та оперативного реагування. Рішення допомагає організаціям дотримуватись кращих практик у сфері кібербезпеки, оскільки може бути гнучко налаштоване для конкретних потреб та сценаріїв загроз.

Таким чином, продумані та налагоджені процеси захисту кінцевих точок, посилені сучасними EDR-рішеннями, мають сприяти ефективному захисту кінцевих точок організації від атак програм-вимагачів та забезпечувати стабільності функціонування інформаційних систем.

ПЕРЕЛІК ПОСИЛАНЬ

1. What is a ransomware attack? | crowdstrike. CrowdStrike: We Stop Breaches with AI-native Cybersecurity. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ (дата звернення: 31.05.2025).

2. Will Law Enforcement success against ransomware continue in 2025?. Coveware: Ransomware Recovery First Responders. URL: https://www.coveware.com/blog/2025/1/31/q4-report (дата звернення: 04.06.2025)

3. Abrams L. Dark Angels ransomware receives record-breaking $75 million ransom. BleepingComputer. URL: https://www.bleepingcomputer.com/news/security/dark-angels-ransomware-receives-record-breaking-75-million-ransom/ (дата звернення: 31.05.2025).

4. 5 Most Common Types of Ransomware | CrowdStrike. CrowdStrike: We Stop Breaches with AI-native Cybersecurity. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/types-of-ransomware/ (дата звернення: 31.05.2025).

5. 16 Ransomware Examples From Recent Attacks | CrowdStrike. CrowdStrike: We Stop Breaches with AI-native Cybersecurity. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-examples/ (дата звернення: 31.05.2025).

6. NetWalker Ransomware Report. All-in-One Cybersecurity Platform – Cynet. URL: https://www.cynet.com/attack-techniques-hands-on/netwalker-ransomware-report/ (дата звернення: 31.05.2025).

7. 6 ransomware protection strategies you must know. All-in-One Cybersecurity Platform – Cynet. URL: https://www.cynet.com/ransomware/6-ransomware-protection-strategies-you-must-know/ (дата звернення: 31.05.2025).

8. 10 Best Ransomware Protection Companies and Software. Sangfor Technologies. URL: https://www.sangfor.com/blog/cybersecurity/10-best-ransomware-protection-companies-and-software (дата звернення: 31.05.2025).

9. VMware by Broadcom – Cloud Computing for the Enterprise. URL:

https://www.vmware.com/docs/vmwcb-datasheet-endpoint-standard (дата звернення: 31.05.2025).

10. Anti Ransomware Security - Bitdefender GravityZone. Bitdefender. URL: https://www.bitdefender.com/en-gb/business/gravityzone-platform/anti-ransomware (дата звернення: 04.06.2025).

11. Microsoft Defender XDR integration with Microsoft Sentinel. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/azure/sentinel/microsoft-365-defender-sentinel-integration?tabs=defender-portal (дата звернення: 31.05.2025).

12. SentinelOne | KI-gestützte Cybersecurity-Plattform für Unternehmen. URL: https://go.sentinelone.com/rs/327-MNM-087/images/SEN0202_DataSheet_EPP_WEB.pdf (дата звернення: 31.05.2025).

13. Ransomware Mitigation. Bitdefender - Weltspitze in Cybersicherheit. URL: https://www.bitdefender.com/business/support/en/77209-533523-ransomware-prevention-and-mitigation.html (дата звернення: 04.06.2025).

14. Built-in protection helps guard against ransomware – Microsoft Defender for Endpoint. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/defender-endpoint/built-in-protection (дата звернення: 31.05.2025).

15. What is Ransomware Rollback?. SentinelOne. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-ransomware-rollback/ (дата звернення: 31.05.2025).

16. Take response actions on a device in Microsoft Defender for Endpoint – Microsoft Defender for Endpoint. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/defender-endpoint/respond-machine-alerts (дата звернення: 31.05.2025).

17. Netsurion. Bitdefender GravityZone (on-Premises) Integration | Netsurion. Netsurion. URL: https://www.netsurion.com/data-source-integrations/bitdefender-gravityzone-on-premises (дата звернення: 04.06.2025).

18. Microsoft Defender XDR integration with Microsoft Sentinel. Microsoft Learn:

Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/azure/sentinel/microsoft-365-defender-sentinel-integration?tabs=defender-portal (дата звернення: 31.05.2025).

19. Ransomware Protection - Bitdefender TechZone. GravityZone Platform Bitdefender TechZone. URL: https://techzone.bitdefender.com/en/security-layers/protection/ransomware-protection.html (дата звернення: 04.06.2025).

20. Support Documents and Downloads. URL: https://docs.broadcom.com/doc/vmware-carbon-black-cloud-reference-architecture (дата звернення: 31.05.2025).

21. Inc C. Reputation Assignment. TechDocs. URL: https://techdocs.broadcom.com/us/en/carbon-black/cloud/carbon-black-cloud/index/cbc-user-guide-tile/GUID-9EC9EBA9-2BAF-49FB-96D5-D28917679998-en/GUID-84BBD4DA-CA1C-437D-A42D-95FDE82B6E81-en/GUID-41FE63FF-9D6E-4CEC-9EE3-2BC8153B09D3-en.html (дата звернення: 31.05.2025).

22. Inc C. Managing Policies. TechDocs. URL: https://techdocs.broadcom.com/us/en/carbon-black/cloud/carbon-black-cloud/index/cbc-user-guide-tile/GUID-9EC9EBA9-2BAF-49FB-96D5-D28917679998-en/GUID-814C8950-5560-49D6-8E74-466ECE460D4F-en.html (дата звернення: 31.05.2025).

23. Murugiah, S. Ransomware Risk Management : NIST Technical Series Publications. [Електронний ресурс]. Gaithersburg, MD : National Institute of Standards and Technology, 2025. Режим доступу: https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8374r1.ipd.pdf (дата звернення: 09.06.2025).

24. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. На заміну ISO/IEC 27002:2013 ; чинний від 2022-10-15. Вид. офіц. International Organization for Standardization, 2022. 152 с.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)