ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ НА БАЗІ EDR СИСТЕМИ»

Виконав студент 4 курсу, групи БСД-43
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Качний І.С.
(прізвище та ініціали)
Керівник Марченко В.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітня програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Качному Іллі Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема бакалаврської роботи: «Дослідження шляхів та розробка рекомендацій Щодо захисту кінцевих пристроїв на базі EDR системи»

керівник бакалаврської роботи Марченко Віталій Вікторович, асистент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «24 » лютого 2023 року № 26.

2. Строк подання студентом бакалаврської роботи 29.05.2023 р.

3. Вихідні дані до бакалаврської роботи
корпоративна інформаційна система;
програмний комплекс захисту кінцевих пристроїв;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми захисту кінцевих пристроїв.
2. Методи та засоби захисту інформації за допомогою систем виявлення та реагування на загрози.
3. Процес реагування на загрози кінцевим пристроям.
4. Рекомендації щодо застосування CrowdStrike Falcon EDR для захисту кінцевих пристроїв.

5. Перелік графічного матеріалу
1. Тема бакалаврської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3. Результати аналізу загроз інформаційної безпеки, пов’язаних з використанням кінцевих пристроїв.
4. Призначення та можливості систем виявлення та реагування на загрози на кінцевих пристроях.
5. Призначення та можливості CrowdStrike Falcon EDR
6. Рекомендації щодо використання EDR систем
7. Висновки за результатами роботи.

6. Дата видачі завдання 24.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Визначення актуальності проблеми захисту кінцевих пристроїв.	25.02.2023 р.	
2.	Аналіз наукової та технічної літератури з питань теми бакалаврської роботи.	03.05.2023 р.	
3.	Аналіз методів та засобів безпеки кінцевих пристроїв.	10.05.2023 р.	
4.	Дослідження можливостей захисту кінцевих пристроїв на базі CrowdStrike Falcon	14.05.2023 р.	
5.	Розроблення рекомендацій щодо застосування систем виявлення та реагування на загрози на кінцевих пристроях.	21.05.2023 р.	
6.	Оформлення результатів дослідження.	24.05.2023 р.	
7.	Підготовка доповіді до захисту.	28.05.2023 р.	

Студент _____ Качний І.С.
(підпис) прізвище та ініціали

Керівник бакалаврської роботи _____ Мерченко В.В.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на бакалаврську роботу

студента Качного Іллі Сергійовича
на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту кінцевих пристроїв на базі EDR системи»

Актуальність: Перехід на дистанційну форму роботи привів до збільшення загроз, пов'язаних з використанням кінцевих пристроїв. Компрометація кінцевого пристрою може привести до витоку конфіденційної інформації особи та компанії, а також надати зловмиснику доступ до внутрішньої мережі компанії. Тому тема бакалаврської роботи є актуальною та своєчасною.

Позитивні сторони:
1. На основі проведеного аналізу в роботі було встановлено загрози безпеці кінцевих пристроїв.
2. Було досліджено спосіб роботи та загальні можливості EDR систем.
3. Практичний розгляд роботи EDR системи на прикладі CrowdStrike Falcon.
4. Розроблення рекомендацій щодо застосування EDR систем для захисту кінцевих пристроїв.
5. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою бакалаврської роботи.

Недоліки:
1. У бакалаврській роботі бажано було б порівняти на практиці обрану EDR систему та антивірусне програмне забезпечення.
2. Експеримент із застосуванням EDR системи також бажано було б провести для мобільного пристрою.

Висновок: Враховуючи недоліки, бакалаврська робота заслуговує оцінку **відмінно**, а студент **Качний І.С.** – присвоєння кваліфікації: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	
Має практичну цінність	
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Качний І.С. до захисту бакалаврської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту кінцевих пристроїв на базі EDR системи».
Бакалаврська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Качний І.С. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Берестяна Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студент ***Качний І.С.*.** обрав тему роботи, метою якої було дослідження шляхів та розробка рекомендацій щодо захисту кінцевих пристроїв на базі EDR системи. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Качний І.С. показав добру теоретичну та практичну підготовку. Роботу виконував сумлінно, акуратно та вчасно за планом.
Все це дозволяє оцінити виконану бакалаврську роботу студента Качного Іллі Сергійовича на оцінку **«відмінно»** та присвоїти йому кваліфікацію: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студент Качний І.С.
(прізвище та ініціали)
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

“____” _____ 2023 року

РЕФЕРАТ

Текстова частина бакалаврської роботи: 40 сторінок, 33 рисунків, 12 джерел.

Об'єкт дослідження – процес захисту кінцевих пристроїв в корпоративній інформаційній системи.

Предмет дослідження – методи та засоби захисту кінцевих пристроїв.

Мета роботи – розробити рекомендації щодо застосування систем виявлення та реагування на загрози для захисту кінцевих пристроїв.

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

В роботі приведено основні відомості про загрози інформаційної безпеки в корпоративній інформацій системі.

Проаналізовано різні види загроз, які пов'язані з використанням кінцевих пристроїв.

Досліджено методи та засоби захисту кінцевих пристроїв.

Досліджено можливості CrowdStrike Falcon EDR.

На основі досліджень проведених в роботі розроблено рекомендації щодо застосування систем виявлення та реагування на загрози на кінцевих пристроях.

Галузь використання – кібербезпека корпоративних інформаційних систем.

ЗАХИСТ КІНЦЕВИХ ПРИСТРОЇВ, КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ, СИСТЕМИ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ НА КІНЦЕВИХ ПРИСТРОЯХ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

EDR – Endpoint detection and response

EPP – Endpoint protection platform

XDR – Extended Detection and Response

NGAV – Next-Generation Antivirus

DDoS – Distributed denial-of-service

IoT – Internet of things

SECaaS – Security as a service

ВСТУП

Актуальність дослідження. З початком епідемії коронавірусу, світ стикнувся зі значними змінами в робочому середовищі та способах комунікації. Дистанційна робота стала новою реальністю для багатьох людей і організацій. Цей перехід до віддаленого режиму праці має значний вплив на актуальність захисту кінцевих пристроїв.

Компрометація кінцевого пристрою може привести до витоку конфіденційної інформації особи та компанії, а також надати зловмиснику доступ до внутрішньої мережі компанії. Тому організації повинні бути готові до виявлення та запобігання кіберзагрозам, які спрямовані на кінцеві пристрої.

Об'єкт дослідження – процес захисту кінцевих пристроїв в корпоративній інформаційній системи.

Предмет дослідження – методи та засоби захисту кінцевих пристроїв.

Мета роботи – розробити рекомендації щодо застосування систем виявлення та реагування на загрози для захисту кінцевих пристроїв.

Завдання бакалаврської роботи:

проаналізувати загрози інформаційної безпеки в корпоративній інформацій системі;

проаналізовати різні види загроз, які пов'язані з використанням кінцевих пристроїв;

дослідити методи та засоби захисту кінцевих пристроїв;

дослідити можливості CrowdStrike Falcon EDR;

розробити рекомендації щодо застосування систем виявлення та реагування на загрози на кінцевих пристроях.

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

Практичне значення одержаних результатів: рекомендації щодо використання EDR систем для забезпечення кібербезпеки у корпоративних інформаційних системах.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

1.1. Огляд основних загроз та ризиків, пов'язаних з безпекою інформації в корпоративній інформаційній системі

Сучасна корпоративна система - це складна розподілена комп'ютерна мережа, яка автоматизує обробку інформації, пов'язаної з бізнес-процесами компанії. Для досягнення цієї мети використовуються найновіші технології в галузі інформаційних, комп'ютерних, мережевих, програмних, мультимедійних та комунікаційних технологій.

Ці системи розгортаються на різних рівнях, включаючи апаратні та програмні засоби, що використовуються в процесі обробки даних. Крім того, корпоративні системи повинні бути забезпечені необхідними механізмами захисту даних, щоб запобігти несанкціонованому доступу до конфіденційної інформації.

Для підтримки цих систем необхідні кваліфіковані спеціалісти, які забезпечують безперебійну роботу комп'ютерних мереж, програмних засобів та інших складових системи. Вони також відповідають за розробку, впровадження та підтримку нових функцій та можливостей системи.

Інформаційна безпека - стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій.

Основними загрозами безпеці при використанні корпоративних систем є як зовнішні, так і внутрішні атаки, направлені на порушення доступності, цілісності і конфіденційності інформаційних ресурсів.

Загроза порушення конфіденційності є однією з найбільш серйозних проблем у сфері інформаційної безпеки. Ця загроза полягає у можливості несанкціонованого доступу до конфіденційної інформації, такої як особисті дані клієнтів, фінансова інформація компанії, інтелектуальна власність та інші конфіденційні документи. Порушення конфіденційності може призвести до серйозних наслідків, включаючи фінансові втрати, втрату довіри клієнтів та інші негативні наслідки для репутації компанії.

Оскільки інформаційні системи корпорацій містять значну кількість конфіденційної інформації, захист цієї інформації є критично важливим завданням для забезпечення стійкості та успішності діяльності компанії.

Загроза порушення цілісності інформації полягає в можливості несанкціонованого втручання в інформаційні системи компанії, що може призвести до порушення цілісності даних та інформаційних ресурсів компанії. Навмисна або випадкова зміна, видалення або вставлення нової інформацію в систему компанії, може призвести до неправильних рішень та негативних наслідків для бізнесу. Також, ця загроза може бути використана зловмисниками для шантажу, вимагання викупу та інших злочинних цілей.

Порушення доступності інформації полягає в можливості заблокування або знищення інформаційних ресурсів компанії, що може призвести до відсутності доступу до необхідної інформації та серйозних збитків для бізнесу. Наприклад, така загроза може бути реалізована шляхом відправки великої кількості запитів на сервер компанії, що може призвести до перевантаження мережі та відмови в обслуговуванні.

У 2022 році на промисловість припала найбільша частка кібератак серед провідних галузей у всьому світі. Протягом досліджуваного року кібератаки на промислові компанії становили майже 25 відсотків від загальної кількості кібератак. За ними йдуть фінанси та страхування - близько 19%. Бізнес та сфера обслуговування посіли третє місце з часткою 14,6 відсотка [1].

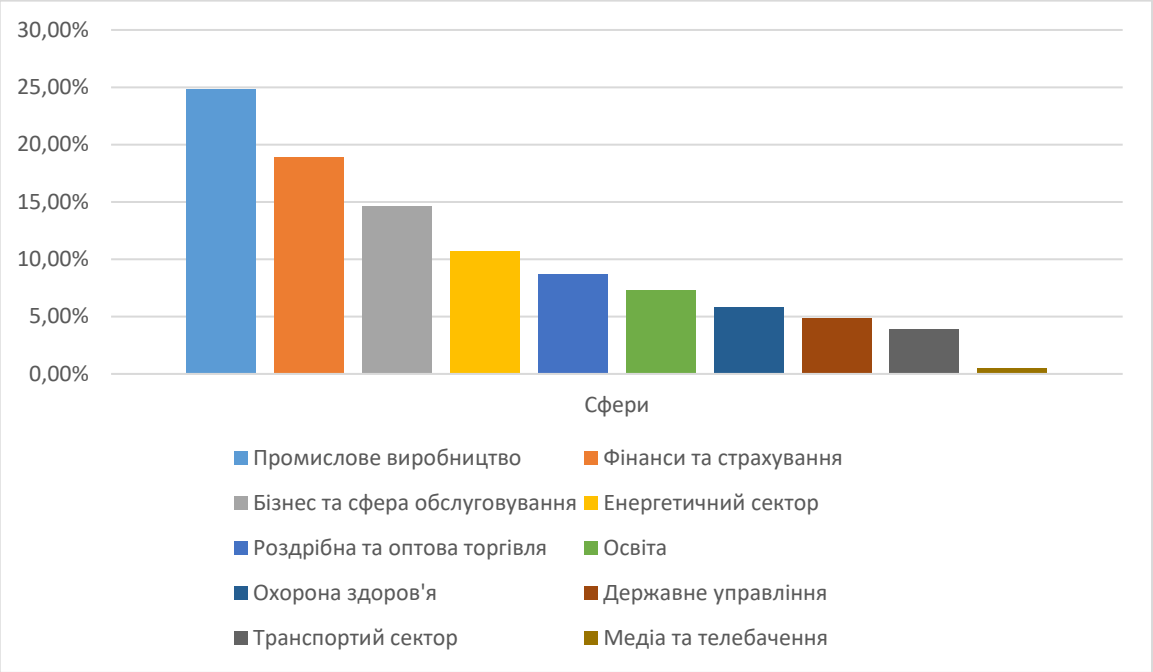


Рис. 1.1. Розподіл кібератак по галузях у світі за 2022 рік

Також протягом 2022 року головними загрозами інформаційної безпеки стали [2]:

- Програми-вимагачі;
- Шкідливе програмне забезпечення;
- Відмова в обслуговуванні (DDoS);
- Загрози соціальної інженерії;
- Атаки на ланцюги постачання.

Програми-вимагачі - тип атаки, під час якої зловмисники шифрують дані організації та вимагають оплату за відновлення доступу. У деяких випадках зловмисники можуть також викрасти інформацію організації та вимагати додаткову оплату за нерозголошення інформації органам влади, конкурентам або громадськості.

Шкідливе програмне забезпечення - це загальний термін, що використовується для опису будь-якого програмного забезпечення або мікропрограми, призначеної для виконання несанкціонованого процесу, який матиме негативний вплив на конфіденційність, цілісність і доступність системи. Прикладами шкідливого коду є віруси, хробаки, троянські програми та інші об'єкти

на основі коду, які заражають комп'ютер. Шпигунські програми та деякі форми рекламного ПЗ також є прикладами шкідливого коду.

Розподілена відмова в обслуговуванні (DDoS) націлена на доступність систем і даних. Атаки відбуваються, коли користувачі системи або сервісу не мають доступу до відповідних даних, послуг або інших ресурсів. Це може бути досягнуто шляхом виснаження ресурсів сервісу або перевантаження компонентів мережевої інфраструктури.

Соціальна інженерія охоплює широкий спектр діяльності, яка намагається використати людську помилку або поведінку людини з метою отримання доступу до інформації або послуг. Соціальна інженерія використовує різні форми маніпуляцій, щоб змусити жертву припуститися помилки або передати конфіденційну чи секретну інформацію. Прикладом є заохочення користувачів відкривати документи, файли чи електронні листи, відвідувати веб-сайти або надавати неавторизованим особам доступ до систем чи послуг. І хоча ці трюки можуть зловживати технологіями, вони завжди покладаються на людський фактор, щоб бути успішними.

Атаки на ланцюги поставок націлені на відносини між організаціями та їхніми постачальниками. Дана атака складається з комбінації щонайменше двох атак. Зокрема, перша атака на постачальника, яка потім використовується для атаки на ціль для отримання доступу до її активів. Цією ціллю може бути кінцевий споживач або інший постачальник. Таким чином, для того, щоб атаку можна було класифікувати як атаку на ланцюг поставок, і постачальник, і клієнт повинні бути цілями.

1.2. Аналіз загроз, що виникають для кінцевих пристроїв в процесі роботи з інформаційною системою

В останні роки кількість кінцевих пристроїв на підприємствах зросла. Особливо це стало помітно після пандемії Covid-19, яка призвела до популяризації віддаленої роботи по всьому світу. Оскільки все більше співробітників працюють з дому або підключаються до громадського Wi-Fi в дорозі, корпоративні мережі

тепер мають більше кінцевих пристроїв, ніж будь-коли. І кожен кінцевий пристрій може бути потенційною ціллю для атак.

Безпека кінцевих користувачів, або захист кінцевих точок, стосується захисту пристроїв - таких як настільні комп'ютери, ноутбуки та мобільні пристрої - від загроз кібербезпеки. Кінцеві пристрої можуть створювати місця для проникнення в мережу організації, якими можуть скористатися кіберзлочинці [3].

Кінцевий пристрій - це будь-який пристрій, який підключається до мережі організації за межами брандмауера. Приклади кінцевих пристроїв включають:

- ПК;
- Ноутбуки;
- Планшети;
- Мобільні телефони;
- Пристрої для інтернету речей (IoT);
- Розумні годинники;
- Цифрові принтери;
- Системи торгових точок (POS);
- Медичне обладнання.

Компаніям необхідно захищати свої дані та бути в курсі найсучасніших кіберзагроз. Але багатьом малим і середнім компаніям не вистачає ресурсів для постійного моніторингу мережевої безпеки та інформації про клієнтів, і вони часто замислюються про захист своєї мережі лише тоді, коли кібератака вже сталася. Навіть тоді компанії можуть зосередитися на своїй мережі та інфраструктурі, залишаючи деякі з найбільш вразливих елементів - тобто кінцеві пристрої - незахищеними.

Ризики, пов'язані з кінцевими пристроями та їхніми конфіденційними даними, є постійною проблемою кібербезпеки. Більше того, ландшафт кінцевих точок розвивається, а підприємства - малі, середні та великі - стають мішенями для кібератак.

Види загроз, пов’язаних з безпекою кінцевих пристроїв:

- Фішингові атаки

- Втрата пристроїв
- Застарілі оновлення
- Втрата та крадіжка даних
- Програми-вимагачі
- DDoS
- Атаки ботнет-мереж

Фішинг

Найпопулярніша і найменш складна форма атаки - фішинг - полягає у використанні фальшивих повідомлень для отримання інформації. Повідомлення нібито надходить від надійного суб'єкта (наприклад, банку або відомої компанії), щоб обманом змусити користувачів надати особисту інформацію або завантажити шкідливе програмне забезпечення. Потім ця інформація або шкідливе програмне забезпечення використовується для отримання доступу до системи користувача, а звідти - для проникнення в більшу мережу, в якій працює користувач.

Втрата пристроїв

За даними TrendMicro, понад 40% інцидентів з витоком даних у період з 2005 по 2015 рік були спричинені втратою або викраденням кінцевих пристроїв, таких як ноутбуки, планшети та смартфони [4].

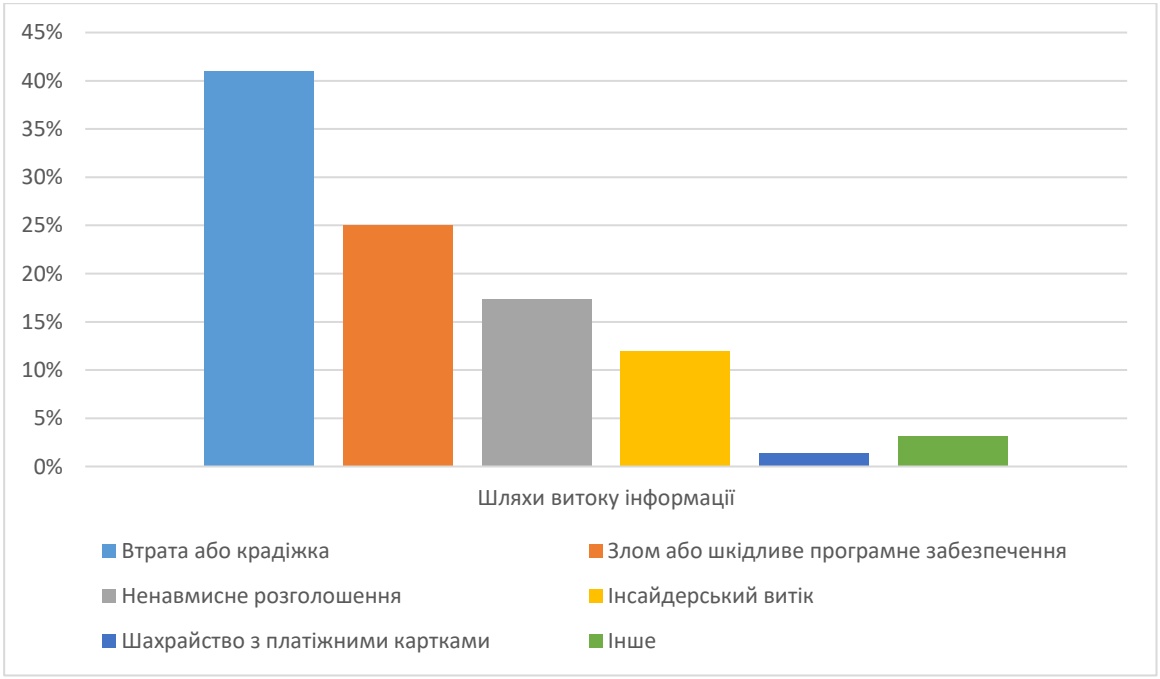


Рис. 1.2. Інциденти пов’язані з витоком даних

Застарілі оновлення

Постійні оновлення – необхідність для коректної та безпечної роботи пристроїв та програм. І все ж багато компаній все ще нехтують своєчасним оновленням ПЗ. Найвідоміший приклад - витік даних Equifax у 2017 році. Агентство кредитної звітності не змогло виправити критичну вразливість на одному зі своїх серверів, що дозволило хакерам викрасти персональні дані 148 мільйонів американських споживачів.

Втрата та крадіжка даних

Втрата даних - це безповоротне видалення даних. Для окремого користувача кінцевого пристрою це означає втрату особистих фотографій, портфоліо чи листування, які зберігалися роками. Для організації це може нести ще серйозніші наслідки: згідно з дослідженням Техаського університету, 94% компаній, які зазнали значної втрати даних, збанкрутували - 43% і закрилися негайно, а 51% закрилися протягом двох років.

Програми-вимагачі

Цей тип шкідливого програмного забезпечення шифрує всі файли користувачів, роблячи їх недоступними, доки не буде сплачено викуп. У більшості випадків програма маскується під легальну програму, яка обманом змушує користувачів запустити її - однак з'явилися новіші версії, які не потребують втручання користувача і можуть автоматично переміщатися між комп'ютерами в мережі. Найгірше у програмах-вимагачах - це їхня невибіркова дія. На відміну від більшості атак, які цілеспрямовано націлені на великі підприємства в надії отримати грошову вигоду, програми-вимагачі поширюються як вірус і можуть вразити практично будь-кого.

DDoS

Розподілена атака на відмову в обслуговуванні використовує потік вхідного трафіку, щоб перевантажити веб-сайт, сервер або мережу. Вона використовує скомпрометовані пристрої, в тому числі кінцеві пристрої, для багаторазового доступу до цільового сайту і врешті-решт порушує його пропускну здатність, що призводить до відмови в обслуговуванні звичайного трафіку.

Атака ботнет-мереж

Ботнет-мережа - це набір пристроїв, які були скомпрометовані і можуть контролюватися сторонніми особами. Вони можуть використовуватися для розсилки спаму, зараження інших пристроїв або здійснення DDoS-атак в рамках ботнет-кампанії. По суті, пристрій стає частиною "зомбі-армії" без відома власника. У минулому ботнети обмежувалися комп'ютерами. Сьогодні, завдяки поширенню IoT ширший спектр бездротових пристроїв є вразливим до зараження ботнетом. Це смартфони та планшети, смарт-телевізори, камери відеоспостереження і навіть "розумні" побутові прилади. Цей ризик для безпеки кінцевих пристроїв є додатковою проблемою, оскільки після зараження частина обчислювальної потужності, енергії та пропускної здатності пристрою спрямовується на атаки ботнету щоразу, коли він активується для участі в ботнет-кампанії.

Наразі більшість працівників організацій у всьому світі працюють дистанційно. Дистанційна робота забезпечує гнучкість співробітників, але вона також створює низку проблем з безпекою. Найбільше занепокоєння стосовно ризиків інформаційної безпеки стосуються наступних проблем:

- Відсутність фізичної безпеки на робочому місці;
- Ризик зараження шкідливим програмним забезпеченням;
- Захист зовнішніх комунікацій;
- Захист мережі;
- Злочинці використовують пристрої для отримання доступу до мережі;
- Фішингові атаки та соціальна інженерія;
- Втрата або крадіжка пристроїв;
- Забезпечення зовнішнього доступу до внутрішніх ресурсів.

Як можна побачити більшість з цих проблем пов’язана з використанням кінцевих пристроїв.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ СИСТЕМ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ

2.1. Огляд сучасних EDR систем та їхніх функціональних можливостей

Терміни "захист кінцевих пристроїв", "безпека кінцевих пристроїв" і "платформи захисту кінцевих пристроїв" часто використовуються як взаємозамінні для позначення централізовано керованих рішень безпеки, які організації використовують для захисту кінцевих пристроїв. Захист кінцевих пристроїв працює шляхом перевірки файлів, процесів і систем на наявність підозрілої або зловмисної активності.

Організації можуть встановити платформу захисту кінцевих точок (EPP) на пристроях, щоб запобігти використанню зловмисниками шкідливого програмного забезпечення або інших інструментів для проникнення в їхні системи. EPP можна використовувати разом з іншими інструментами виявлення та моніторингу для виявлення підозрілої поведінки та запобігання порушенням до того, як вони відбудуться [5].

Основні особливості EPP:

- Сигнатури загроз - антивірусна функція, яка виявляє загрози, порівнюючи їх з відомими сигнатурами шкідливого програмного забезпечення;
- Статичний аналіз - аналіз підозрілих бінарних файлів, як правило, з використанням методів машинного навчання, для виявлення шкідливих компонентів;
- Поведінковий аналіз - за відсутності відомих сигнатур загроз, EPP може аналізувати поведінку кінцевих пристроїв і виявляти аномальні шаблони, які потребують розслідування;
- Білі та чорні списки - блокують або дозволяють доступ до певних IP-адрес, URL-адрес і додатків;

• Пісочниця - тестування на предмет зловмисної активності шляхом запуску файлів у віртуальному середовищі перед звичайним виконанням на кінцевому пристрої;

EDR (endpoint detection and response) означає "виявлення та реагування на кінцевих пристроях". Системи EDR зазвичай розгортаються як агенти на кінцевих точках, хоча деякі рішення є безагентними. Вони відстежують і збирають дані про активність кінцевих пристроїв, виявляють шаблони загроз і надають як ручні, так і автоматизовані можливості для виявлення підозрілої активності на кінцевих точках.

Основні особливості EDR:

• Виявлення загроз і сповіщення - виявляє зловмисну активність і незвичні процеси на кінцевій точці та сповіщає команди безпеки;

• Розслідування інцидентів - можливість збору інформації про інцидент інформаційної безпеки та даних про трафік з декількох кінцевих точок;

• Ізоляція - автоматично ізолює заражені кінцеві пристрої та запобігає поширенню загроз мережею;

• Реагування на інциденти - дозволяє командам безпеки виконувати стирання та повторне створення образу скомпрометованого кінцевого пристрою або скидання паролів.

Загалом, платформа захисту кінцевих пристроїв або EPP вважається пасивним захистом від загроз, тоді як EDR є більш активним, оскільки допомагає розслідувати і локалізувати порушення, які вже відбулися. EPP захищає кожен кінцевий пристрій шляхом ізоляції, тоді як EDR надає контекст і дані для атак, які охоплюють кілька кінцевих пристроїв. Сучасні платформи для захисту кінцевих пристроїв, як правило, поєднують в собі як EPP, так і EDR [6].

Для управління захистом кінцевих пристроїв є централізована консоль управління, до якої організації можуть підключити свою мережу. Консоль дозволяє адміністраторам відстежувати, розслідувати та реагувати на потенційні кіберзагрози. Це може бути досягнуто за допомогою локального, хмарного або гібридного підходу:

- Локальний підхід передбачає локальний центр обробки даних, який виступає в ролі центру для консолі управління. Для забезпечення безпеки він зв'язується з кінцевими точками через агента. Цей підхід вважається застарілою моделлю і має недоліки, оскільки адміністратори, як правило, можуть керувати кінцевими точками лише в межах свого периметру;
- Хмарний. Цей підхід дозволяє адміністраторам контролювати та керувати кінцевими пристроями через централізовану консоль управління в хмарі, до якої пристрої підключаються віддалено. Хмарні рішення дозволяє розширити можливості адміністраторів.;
- Гібридний підхід поєднує локальні та хмарні рішення. Цей підхід став більш поширеним після того, як пандемія призвела до збільшення кількості віддаленої роботи. Організації адаптували свою застарілу архітектуру та пристосували її елементи до, щоб отримати деякі хмарні можливості.

Розглянемо деякі з популярних EDR.

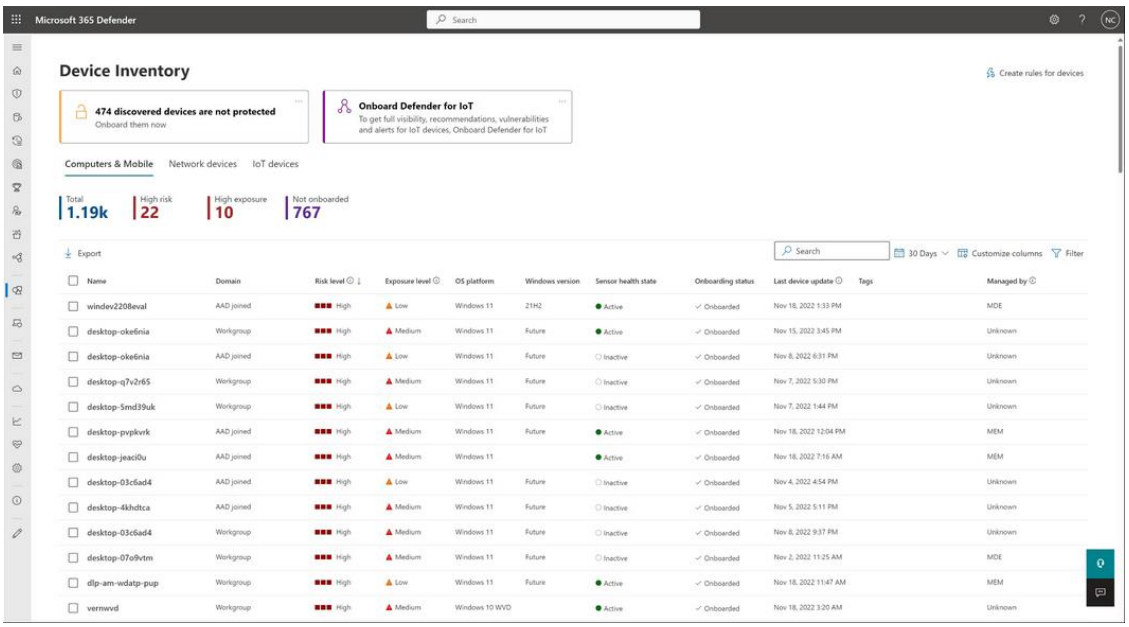


Рис. 2.1. Microsoft Defender for Endpoint

Microsoft Defender для кінцевих пристроїв (MDE) - це центральний компонент пакета Microsoft 365 Defender, до якого входять Microsoft Defender для Office 365, Microsoft Defender для кінцевих пристроїв, Microsoft Cloud Application Security. Їхнє рішення не використовує агентів або сканування, а натомість

використовує вбудовані в операційну систему сенсори, які виявляють вразливості та неправильні конфігурації, а потім визначають пріоритетність вразливостей на основі багатьох факторів [7].

Microsoft Defender для кінцевих пристроїв - це комплексне рішення для захисту кінцевих точок, яке забезпечує превентивний захист, виявлення порушень, автоматизоване розслідування та реагування. Він допомагає захиститися від програм-вимагачів, безфайлових шкідливих програм та інших складних атак на Windows, macOS, Linux, Android та iOS.

Переваги Microsoft Defender:

- Без агентів – не потребує додаткової інфраструктури та агентів для розгортання на кінцевих пристроях на базі операційної системи Windows;
- Масштабованість - Створений на основі хмарних технологій, Microsoft Defender може масштабуватися понад мільйон кінцевих пристроїв;
- Аналіз загроз - звіти з аналітики загроз дозволяють організаціям швидко зрозуміти нові глобальні загрози, побачити, чи впливають вони на даний момент, оцінити їх уразливість і вжити заходів для пом'якшення наслідків, щоб підвищити свою стійкість до цих загроз;
- Управління загрозами та вразливостями - відстежує вразливості програмного забезпечення Microsoft і сторонніх розробників та проблеми з конфігурацією безпеки. Потім він автоматично вживає заходів для зменшення ризиків і зниження рівня ризику;
- Вбудована автоматизація - автоматизація на основі штучного інтелекту для дослідження чи є загроза реальною, і вживання автоматичні дії з усунення загрози для швидкого відновлення ураженого пристрою;

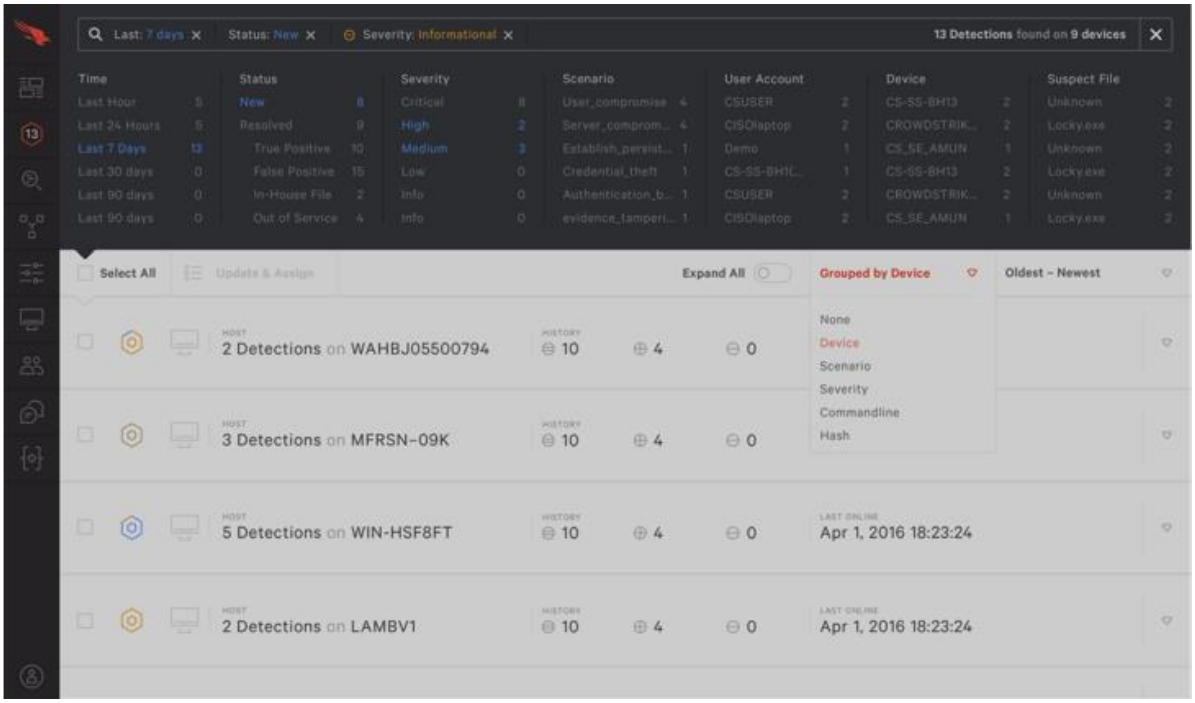


Рис. 2.2. CrowdStrike (Falcon)

CrowdStrike Falcon - це провідне в галузі рішення EDR, призначене для підвищення ефективності роботи аналітиків і слідчих груп організації. Воно має функцію "швидкого пошуку", яка повертає результати з журналів, телеметрії, даних щодо виявлення загроз та відкритих розслідувань. Розподіл оповіщень за пріоритетами та категоріями інцидентів не дає кінцевим користувачам перевантажуватись оповіщеннями, які потребують їхньої уваги. Їх продукт Insights також дозволяє зіставляти сповіщення з системою MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) [8].

Дане рішення розроблено таким чином, щоб забезпечити все, що може знадобитися організації для виявлення і зупинки будь-якої загрози на кінцевих точках або в мережі. Також впроваджуються додаткові рішення, що виходять за рамки захисту кінцевих точок, включаючи рішення для захисту ідентичності та рішення для оркестрування, автоматизації та реагування на загрози (SOAR), які тісно інтегруються з Falcon.

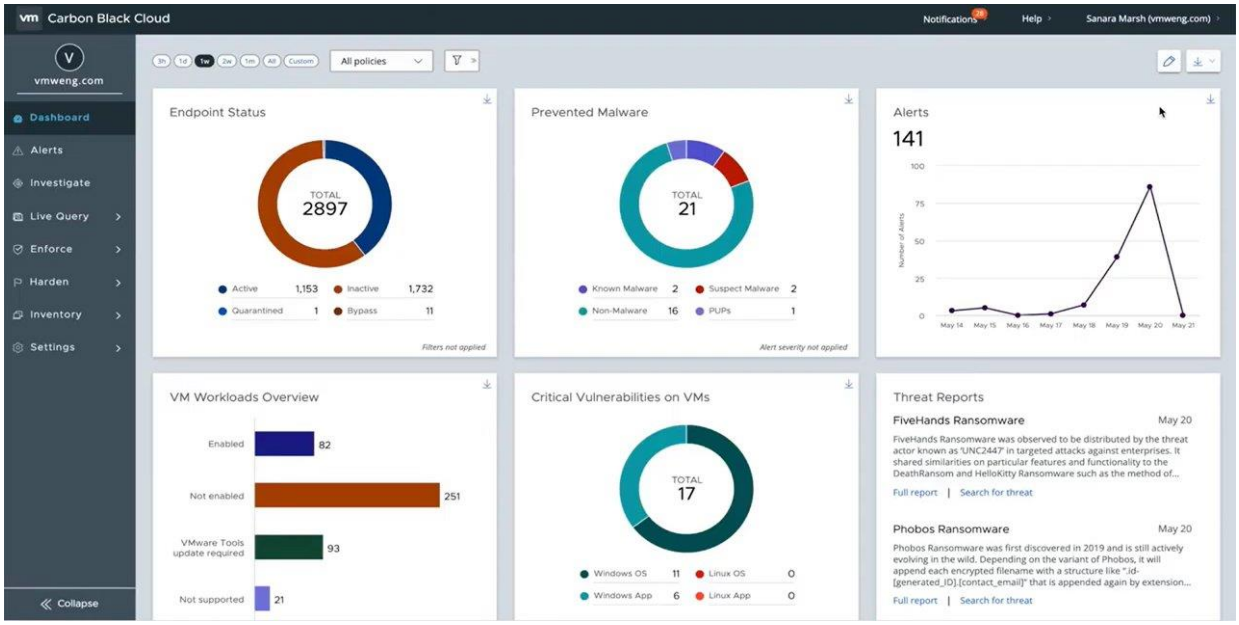


Рис. 2.3. VMware Carbon Black Endpoint

VMware Carbon Black орієнтоване на організації, яким потрібне повністю локальне і самокероване рішення для захисту кінцевих точок без втрати функціональності. Воно включає такі функції, як пошук загроз і реагування на інциденти, призначені для онлайн і офлайн SOC [9]. Фахівці з реагування на інциденти можуть швидко отримати доступ до даних кінцевих точок з центрального розташування, а також витягувати або переміщувати файли, зупиняти процеси і виконувати дампи пам'яті віддалено за допомогою інтуїтивно зрозумілого інтерфейсу користувача. Існує також хмарне рішення Carbon Black Cloud, яке дозволяє організаціям будь-якого розміру модернізувати захист своїх кінцевих точок за допомогою хмарних засобів виявлення, аналізу загроз, автоматизації та безлічі інтеграцій з більшістю систем захисту.

Основні можливості VMware Carbon Black:

- Видимість подій, орієнтована на користувача - відстеження подій, орієнтованих на користувача, з мережевою телеметрією, яка вказує на зловмисну активність, наприклад, різні форми зловживання обліковими записами, аномальну поведінку при автентифікації та внутрішні загрози;
- Відкрита масштабована екосистема - забезпечує готову інтеграцію з провідними постачальниками в різних галузях;

• Видимість мережевих з'єднань за допомогою спостережень системи виявлення вторгнень (IDS) – дозволяє візуалізувати та аналізувати мережеві дані за допомогою безперервного збору та аналіз мережевих параметрів, даних трафіку, даних TLS і даних прикладних протоколів.

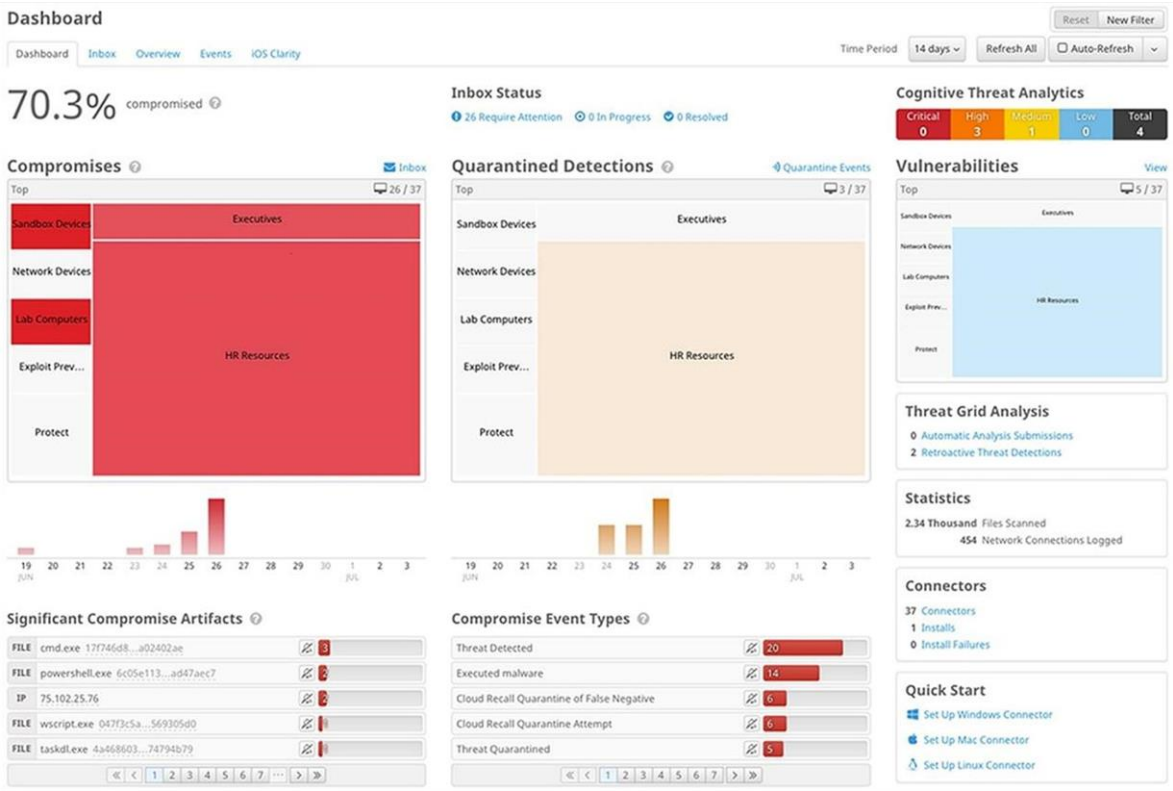


Рис. 2.4. Cisco (Secure Endpoint)

Cisco Secure Endpoint об'єднує функції запобігання, виявлення, пошуку загроз і реагування на них в єдиному рішенні, що використовує можливості хмарної аналітики. Secure Endpoint захищає пристрої під управлінням Windows, Mac, Linux, Android та iOS за допомогою розгортання в публічній або приватній хмарі [10].

Cisco Secure Endpoint - це рішення з одним агентом, яке забезпечує комплексний захист, виявлення, реагування та управління доступом користувачів для захисту від загроз на кінцевих пристроях. Платформа SecureX та система розширеного виявлення і реагування (XDR) вбудована в Secure Endpoint.

Особливості Cisco (Secure Endpoint):

• Керування пристроєм - Secure Endpoint дозволяє контролювати використання USB-накопичувачів і запобігати атакам з цих пристроїв;

• Низький рівень розповсюдженості - Secure Endpoint автоматично виявляє виконувані файли, які існують ваших кінцевих точках, і аналізує їх у нашій хмарній пісочниці, щоб виявити нові загрози;

• Захист від зловмисних дій - Secure Endpoint постійно відстежує всю активність кінцевих точок і забезпечує виявлення та блокування ненормальної поведінки запущених програм на кінцевих точках під час виконання;

• Поведінковий захист - Secure Endpoint постійно відстежує всю активність користувачів і кінцевих пристроїв для захисту від зловмисної поведінки в режимі реального часу, порівнюючи потік записів активності з набором шаблонів активності атак, які динамічно оновлюються в міру розвитку загроз.

2.2. Аналіз можливостей програмного комплексу CrowdStrike Falcon Endpoint Protection

CrowdStrike Falcon Platform - це хмарне рішення для захисту кінцевих пристроїв, яке допомагає малому та великому бізнесу забезпечити антивірусний захист і контроль над пристроями. CrowdStrike Falcon забезпечує IT-безпеку для підприємств будь-якого розміру. Він може масштабуватися для підтримки тисяч кінцевих пристроїв [11].

Платформа забезпечує захист комп'ютерів під управлінням Windows, Mac і Linux, включаючи сервери Windows і мобільні пристрої. Falcon також відповідає нормативним вимогам. Серед клієнтів компанії - банки, уряди та організації охорони здоров'я.

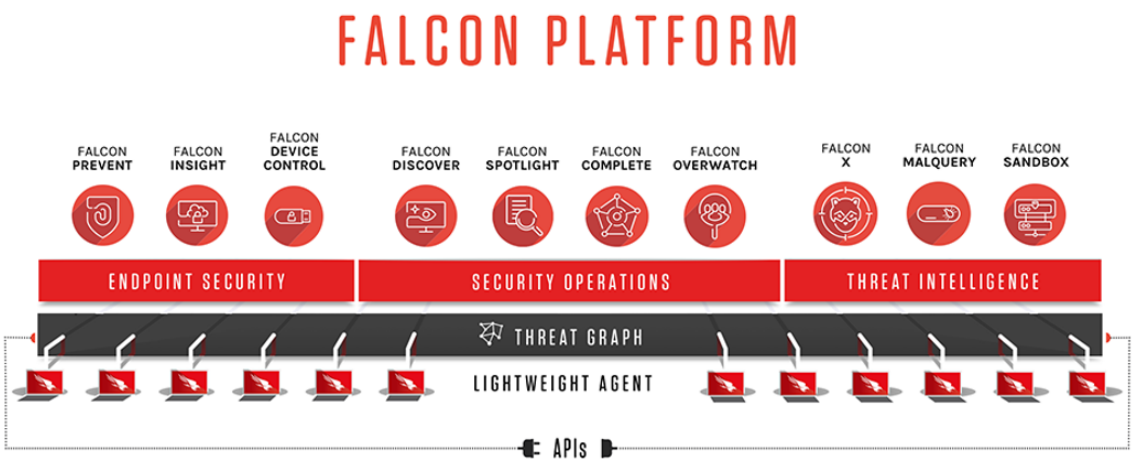


Рис. 2.5. Архітектура CrowdStrike Falcon

Threat Graph - хмарний штучний інтелект прогнозує та запобігає сучасним загрозам у режимі реального часу [12].

Особливості Threat Graph:

- База даних - Threat Graph безперервно збирає, контекстуалізує та збагачує високоточні телеметричні дані про події безпеки кінцевих пристроїв, робочих навантажень та ідентифікаційних даних. База даних фіксує і виявляє взаємозв'язки між елементами даних;
- Аналіз загроз - доповнює телеметрію контекстом про реальні загрози, що допомагає виявляти нові атаки, пов'язані з відомими джерелами загроз;
- Глибокий аналіз – штучний інтелект та поведінковий аналіз виявляють нові та незвичні загрози в режимі реального часу, а потім попереджає або блокує їх на основі політик;
- Пошуковий механізм - надає можливості для фахівців з реагування на інциденти, забезпечуючи безперешкодний доступ до даних, необхідних для швидкого отримання інформації;
- API (інтерфейс прикладного програмування) - Забезпечує тісну інтеграцію зі сторонніми та власними рішеннями безпеки;
- Зберігання даних - Регулярно зберігає інформацію про безпеку для підтримки відповідності вимогам, довгострокового архівування або інтеграції зі сторонніми аналітичними механізмами.

CrowdStrike використовує модульний підхід до своїх рішень у сфері безпеки. Це дає можливість обирати продукти, необхідні для конкретних задач. В залежності від обраного продукту, можуть бути доступними наступні функції:

- Falcon Prevent - антивірус нового покоління (NGAV). Антивірус нового покоління використовує технології штучного інтелекту, поведінковий аналіз та сканування пам'яті для виявлення складних і невідомих загроз, включаючи безфайлові атаки;
- Falcon Intelligence - автоматизований аналіз загроз. Falcon Intelligence дозволяє компаніям будь-якого розміру краще розуміти загрози, з якими вони стикаються, і надає дієві і персоналізовані дані для захисту від майбутніх атак;
- Falcon Device Control - забезпечує необхідну видимість і детальний контроль для обмеження ризиків, пов'язаних з USB-пристроями. Falcon Device Control автоматично повідомляє тип пристрою із зазначенням виробника, назви продукту та серійного номеру. Ви маєте доступ до всіх пристроїв, що працюють через шину USB;
- Falcon Firewall Management Software - дозволяє створювати та впроваджувати політики фаєрволу пристрою. Falcon Firewall Management миттєво посилює захист від мережевих загроз з мінімальним впливом на хост - від початкового ввімкнення до постійного щоденного використання;
- Falcon Insight XDR - безперервно відстежує всю активність кінцевих точок і аналізує дані в режимі реального часу для автоматичного виявлення активності загроз, що дозволяє виявляти і запобігати сучасним загрозам в міру їх виникнення. Команди безпеки можуть швидко розслідувати інциденти, реагувати на оповіщення та проактивно шукати нові загрози;
- Falcon OverWatch - проактивне виявлення загроз. Falcon OverWatch - це служба керованого виявлення загроз, яке забезпечує глибокий і безперервний аналіз співробітниками CrowdStrike, для постійного пошуку аномальних або нових технік, які розроблені, щоб обійти стандартні технології безпеки;
- Falcon Discover - забезпечує видимість інфраструктури без необхідності розгортання або управління апаратним забезпеченням. Критично важливою

частиною безпеки IT-середовища є встановлення та підтримка засобів контролю безпеки для всіх елементів вашої організації в середовищі. Falcon Discover пропонує більшу зручність і прозорість для відстеження та інвентаризації всіх основних об'єктів, додатків, активів і облікових записів в режимі реального часу.

Falcon використовує комбінацію засобів захисту, включаючи штучний інтелект для аналізу даних кінцевих точок, індикатори атак для виявлення та кореляції дій, що вказують на потенційні загрози, та усунення експлойтів для зупинки атак, спрямованих на вразливості програмного забезпечення. Його основним компонентом є модуль Falcon Prevent, антивірусна технологія CrowdStrike. Він входить до складу всіх пакетів продуктів CrowdStrike.

Falcon Prevent - це антивірус нового покоління (NGAV). Традиційне антивірусне програмне забезпечення виявляло загрози на основі сигнатур шкідливого програмного забезпечення. Кіберзлочинці знають про це, і тепер використовують тактику обходу цих методів виявлення.

Технологія NGAV спрямована на боротьбу з сучасними більш складними типами шкідливого програмного забезпечення. Антивірус від Falcon поєднує в собі машинне навчання, аналіз поведінкових характеристик шкідливого програмного забезпечення та аналіз загроз для точного розпізнавання загроз і вжиття заходів.

З точки зору щоденного управління безпекою, платформа Falcon надає інструменти, які допоможуть діагностувати підозрілу активність та ідентифікувати реальні загрози. Це здійснюється за допомогою веб-консолі управління. Консоль дозволяє легко налаштовувати різні політики безпеки для ваших кінцевих пристроїв. Ви можете вказати різні політики для серверів, корпоративних робочих станцій і віддалених працівників.

При дослідженні підозрілої активності дерево процесів CrowdStrike є особливо корисною функцією. Воно розбиває ланцюжок атаки у візуальному форматі, щоб надати чітку картину атаки.

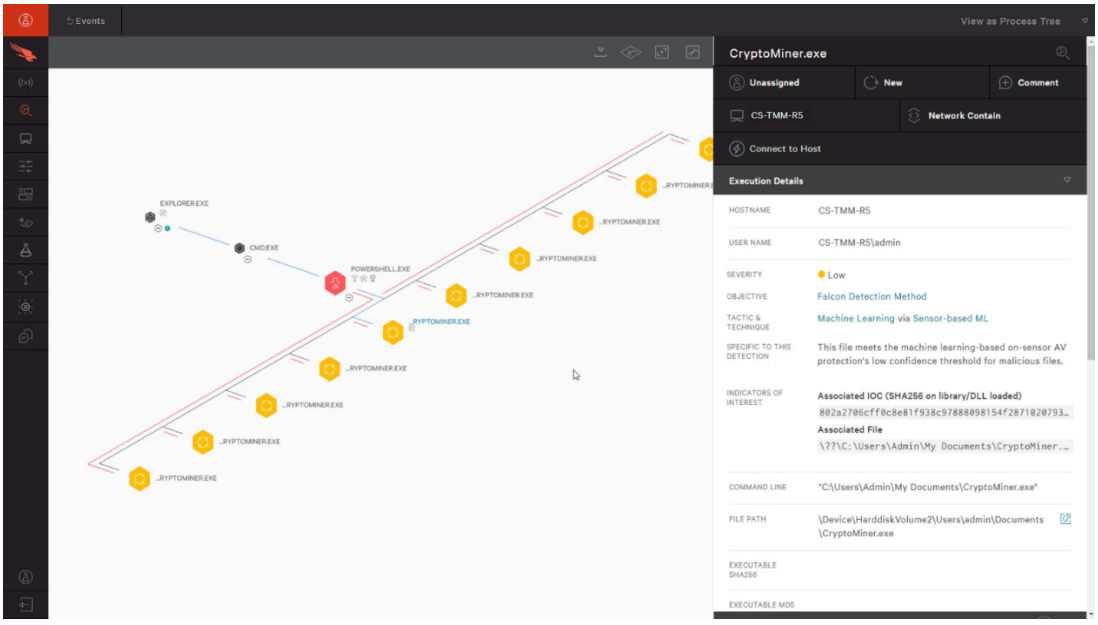


Рис. 2.6. Дослідження інциденту за допомогою CrowdStrike Falcon

Дерево процесів надає інформацію про серйозність загрози та дії, вжиті для її усунення. На цьому ж екрані ви можете швидко оновити профіль безпеки, щоб у майбутньому заблокувати запуск позначеного файлу у вашій IT-мережі, або, якщо це хибне спрацьовування, додати його до білого списку допустимих об'єктів.

Коли Falcon Prevent виявляє шкідливе програмне забезпечення, він надає посилання на додаткові відомості про атаку, включаючи відому інформацію про кіберзлочинців. Це надає додатковий контекст, наприклад, використання вразливостей у програмному забезпеченні, щоб допомогти вашій IT-команді забезпечити належне виправлення та оновлення ваших систем.

2.3. Переваги та недоліки EDR

Переваги EDR:

- Підвищена видимість корпоративної мережі. EDR підвищує прозорість мережі компанії, забезпечуючи безперервний моніторинг кінцевих точок, що дозволяє виявляти загрози і реагувати на них в режимі реального часу. Вони надають детальну інформацію про кінцеву точку, включаючи запущені процеси та програми, а також файли та налаштування реєстру. Це дозволяє компаніям швидко виявляти та усувати загрози, а також запобігати їх виникненню в першу чергу. Крім

того, EDR забезпечує видимість активності користувачів, дозволяючи компаніям відстежувати поведінку користувачів і виявляти підозрілу активність.;

• Відповідність вимогам. У багатьох галузях існують спеціальні правила щодо того, як зберігати дані та отримувати до них доступ, щоб відповідати галузевим стандартам, таким як HIPAA або GDPR. За допомогою EDR компанії можуть відстежувати будь-яку підозрілу активність і розслідувати джерела будь-яких потенційних загроз. EDR також надає детальні звіти, які можна використовувати для демонстрації відповідності аудиторам, гарантуючи, що компанія відповідає необхідним вимогам;

• Зменшення ризиків. EDR забезпечують компанії зниження ризиків завдяки безперервному моніторингу кінцевих точок. Це дозволяє компаніям швидко виявляти і реагувати на загрози в режимі реального часу, знижуючи ризик атаки. Оскільки служби EDR надають детальну інформацію про кінцеву точку, компанії можуть швидко виявити потенційні вразливості та усунути їх до того, як вони будуть використані, знижуючи ризик порушення інформаційної безпеки.

Недоліки EDR:

• Вартість EDR. В середньому, вартість захисту кінцевих пристроїв починається від $45 на рік за користувача, а більшість співробітників мають більше одного пристрою. Співвідношення між обмеженістю ресурсів, кількістю кінцевих пристроїв і бюджетом може призвести до виникнення прогалин, які роблять організації вразливими до атак;

• Вимоги до людських ресурсів. Продукти EDR необхідні для виявлення та реагування на нові загрози, тоді як антивірусні функції захищають пристрої від відомих загроз. Припустимо, що EDR не інтегрований з антивірусною програмою. У цьому випадку кінцевий користувач встановлює ці два рішення окремо, а це означає, що на його пристрої буде два агенти і дві консолі управління, за якими повинні стежити служби безпеки;

• Обмежений аналіз загроз. Окремо взяті рішення EDR не мають механізмів для виявлення та реагування на невідомі загрози, що змушує користувачів поєднувати їх з платформами захисту кінцевих пристроїв (EPP) для запобігання

атакам та надання ефективних можливостей для усунення наслідків. Типовий продукт EDR вимагає підключення до хмари, що може призвести до затримок у захисті кінцевих пристроїв. Відсутність належної хмарної інфраструткури та з’єднання дасть зловмиснику певний час затримки, який він може використати для компрометації пристрою, шифрування файлів, витоку конфіденційної інформації та видалення слідів атаки;

- EDR представляє невеликий огляд мережевої безпеки. EDR дає вузьке уявлення про безпеку системи в організації. Його видимість обмежена конкретною кінцевою точкою і залишається сліпою до зовнішнього мережевого трафіку;

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ CROWDSTRIKE FALCON ENDPOINT PROTECTION PLATFORM, ЯК ІНСТРУМЕНТУ ДЛЯ ЗАХИСТУ КІНЦЕВИХ КОРИСТУВАЧІВ

3.1. Встановлення та налаштування CrowdStrike

CrowdStrike Falcon – це повністю хмарне рішення, що пропонує безпеку як послугу (SECaaS). Воно не вимагає встановлення серверів або контролерів, звільняючи від зайвих витрат пов'язаних з управлінням, обслуговуванням і оновленням локального програмного забезпечення або обладнання.

Після реєстрації отримуємо доступ до панелі керування.

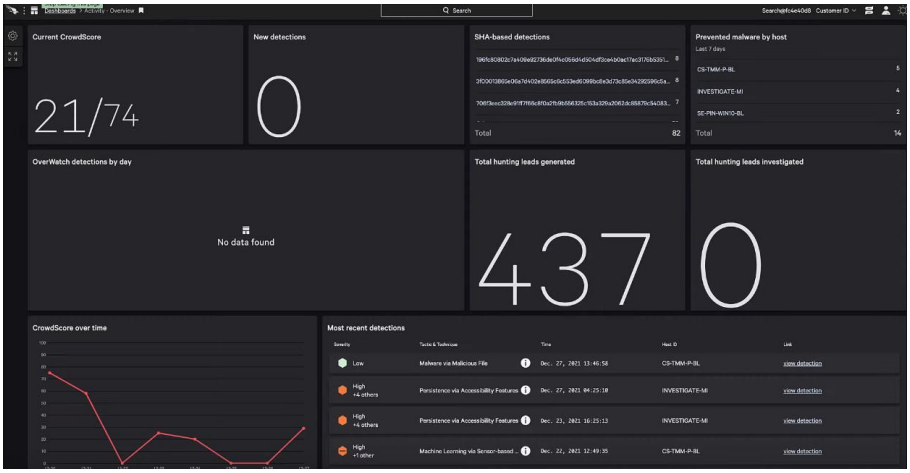


Рис. 3.1. Панель керування CrowdStrike Falcon

Для встановлення сенсору переходимо до панелі керуваня пристроями.

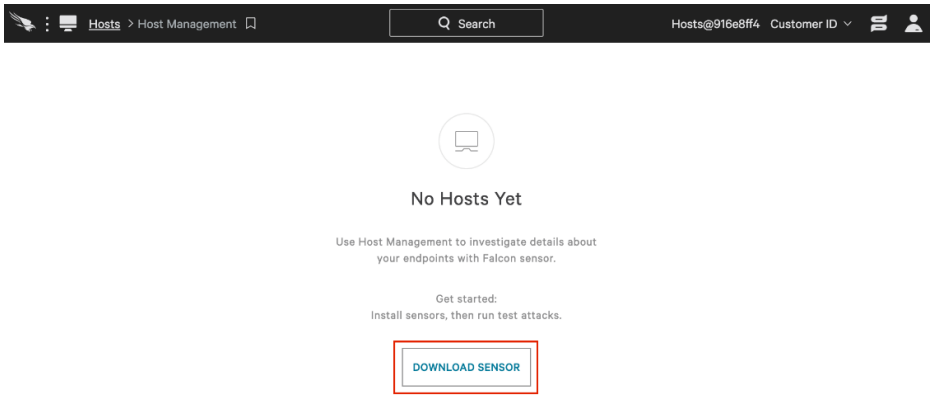


Рис. 3.2. Панель керування пристроями CrowdStrike Falcon

Тут обираємо кінцевий пристрій на який потрібно встановити сенсор. Також варто скопіювати ID користувача, це знадобиться при інсталяції сенсору на кінцевий пристрій.

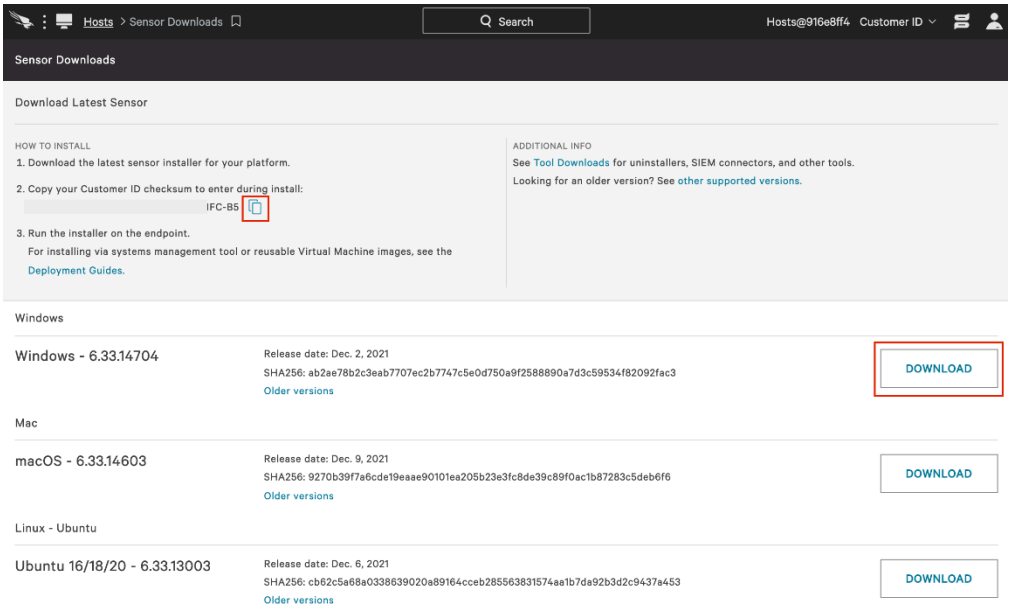


Рис. 3.3. Встановлення потрібного сенсору

Після цього встановлюємо сенсор на кінцевий пристрій. Конструкція датчика Falcon робить його надзвичайно легким (споживає 1% або менше центрального процесора) і ненав'язливим: без інтерфейсу, без спливаючих вікон, без перезавантажень, а всі оновлення виконуються безшумно і автоматично.

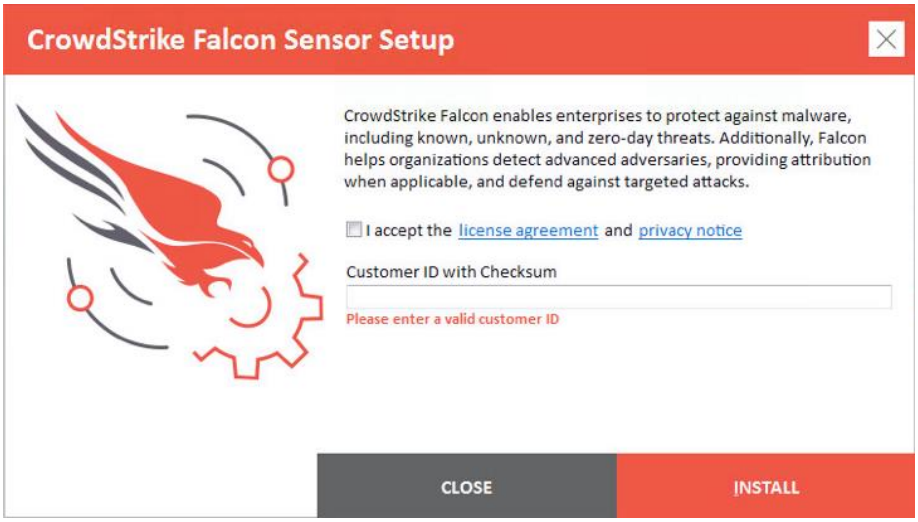


Рис. 3.3. Встановлення сенсору на кінцевий пристрій

Для того, щоб переконатися, що сенсор встановлено в терміналі на кінцевому пристрої вводимо наступну команду: *sc query csagent*. В результаті бачимо, що сервіс запущено, а отже сенсор успішно встановлено.

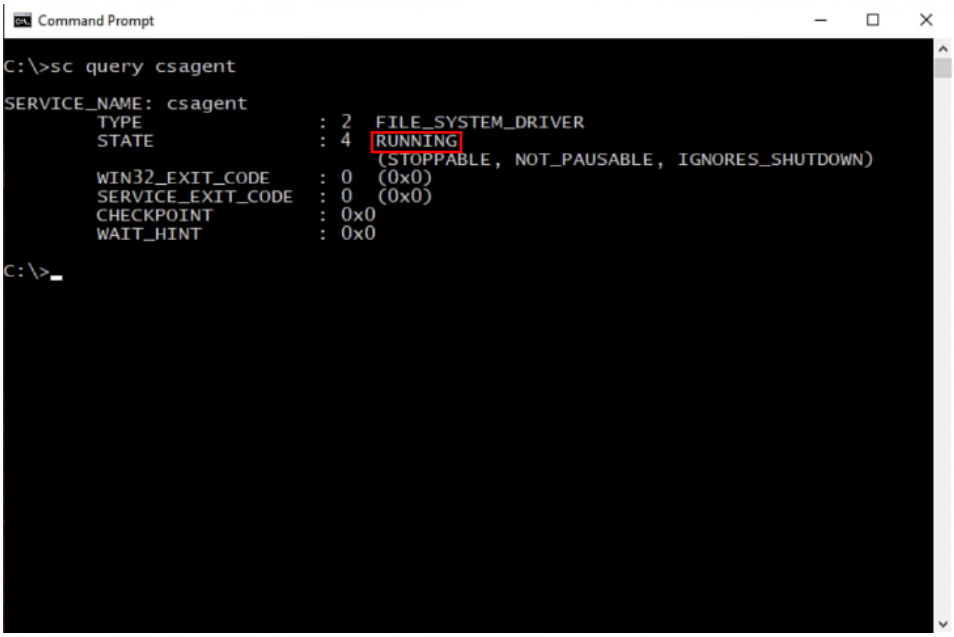


Рис. 3.4. Перевірка запущеного процесу

Також для того щоб переконатися в тому, що сенсор працює, можна згенерувати тестову загрозу. Для цього в консолі кінцевого пристрою вводимо команду *choice /m crowdstrike_sample_detection* та натискаємо *Y* для підтвердження.

Рис. 3.5. Створення тестової загрози

Тим часом, на панелі керування з’являється нове сповіщення про загрозу.

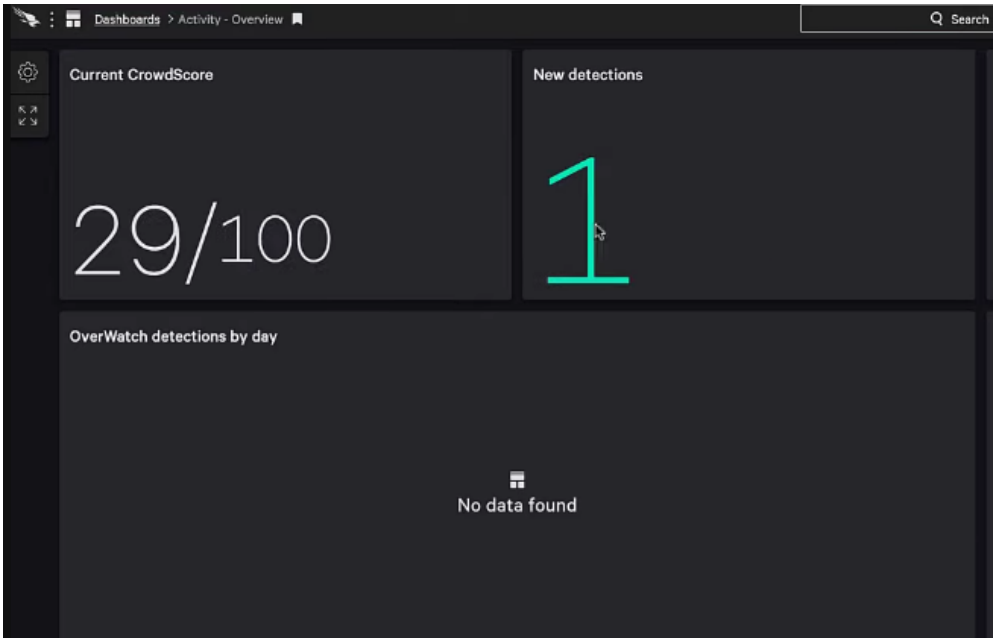


Рис. 3.6. Поява нової загрози на панелі керування

Переглядаючи деталі виявленої загрози можна переглянути інформацію, стосовно пристрою який згенерував сповіщення та що саме стало причиною сповіщення.

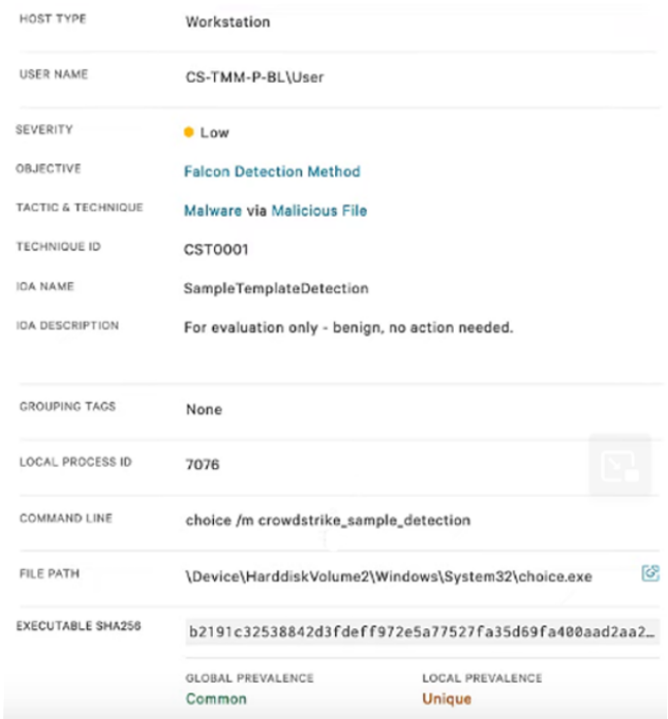


Рис. 3.7. Детальна інформація про тестову загрозу

3.2. Дослідження ефективності захисту кінцевих користувачів

Розглянемо приклад коли користувач отримав електронний лист з вкладенням яке містить шкідливе програмне забезпечення.

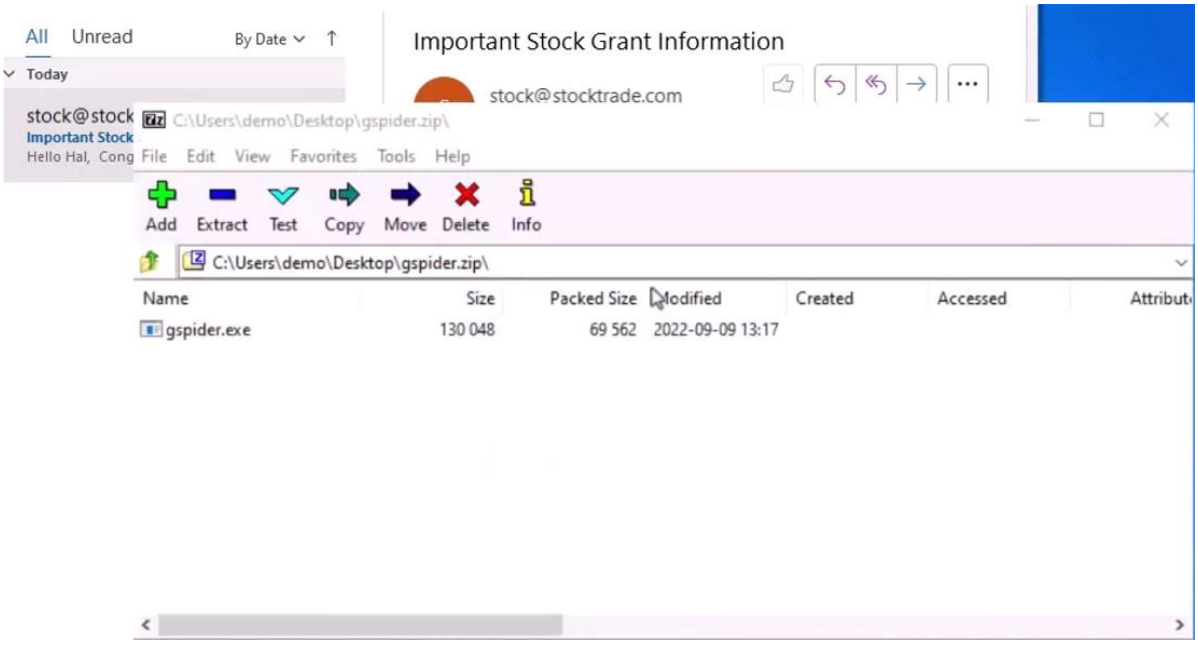


Рис. 3.8. Приклад отримання зловмисної програми в електронному листі

При спробі запустить цю програму ми побачимо помилку, а також повідомлення від Falcon про те, що вайл було ізольовано.

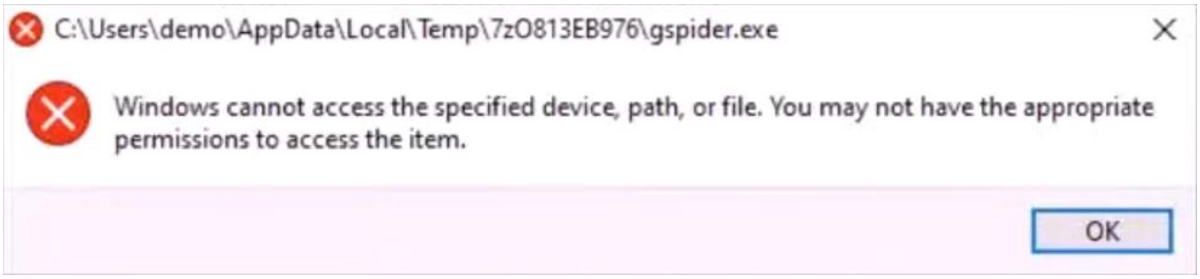


Рис. 3.9. Повідомлення про те, що шкідлива програма більше недоступна

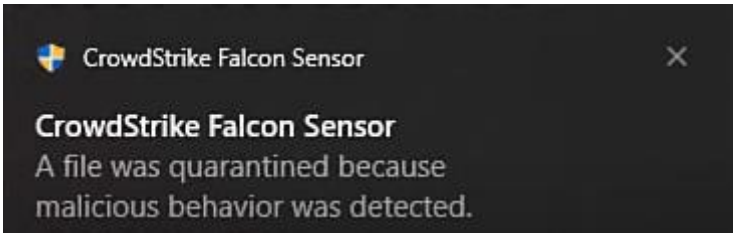


Рис. 3.10. Повідомлення від Falcon, про ізоляцію шкідливої програми

CrowdStrike Falcon також дозволяє переглянути та проаналізувати додаткову інформацію стосовно події в панелі керування. В панелі керування з’явився новий запис, стосовно події інформаційної безпеки.

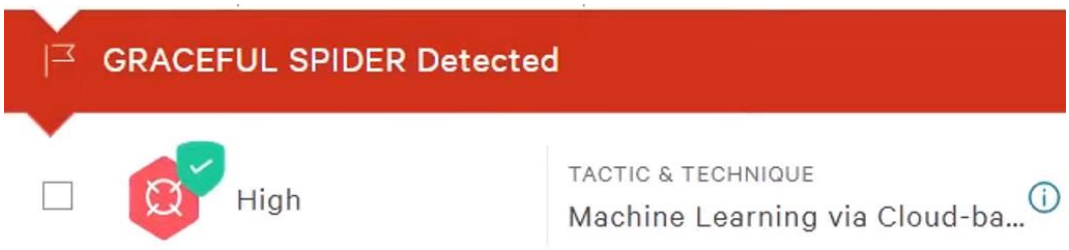


Рис. 3.11. Результати виявлення нової загрози

Ми можемо проаналізувати, як саме вірус потрапив на кінцевий пристрій, а саме Пошта → Архів → Вірус.

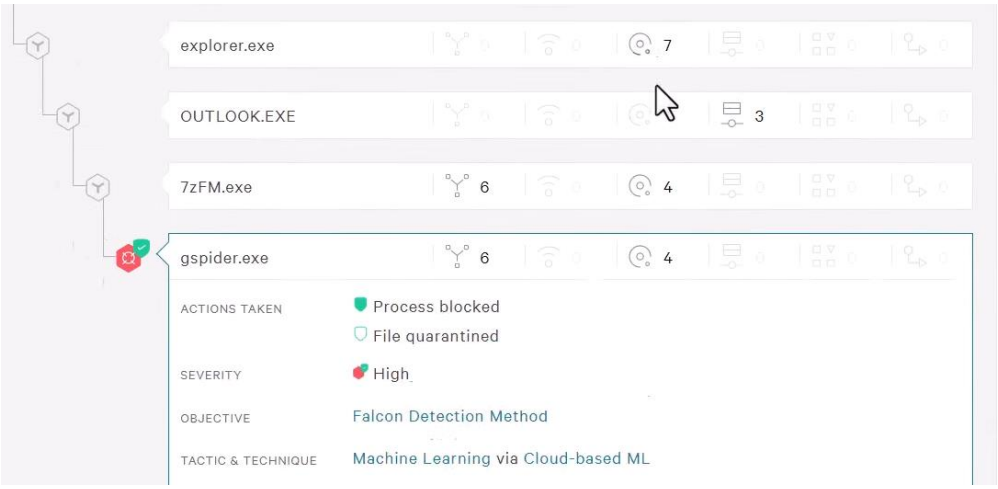


Рис. 3.12. Спосіб потрапляння вірусу на кінцевий пристрій

Також доступна більш детальна інформація про сам файл.

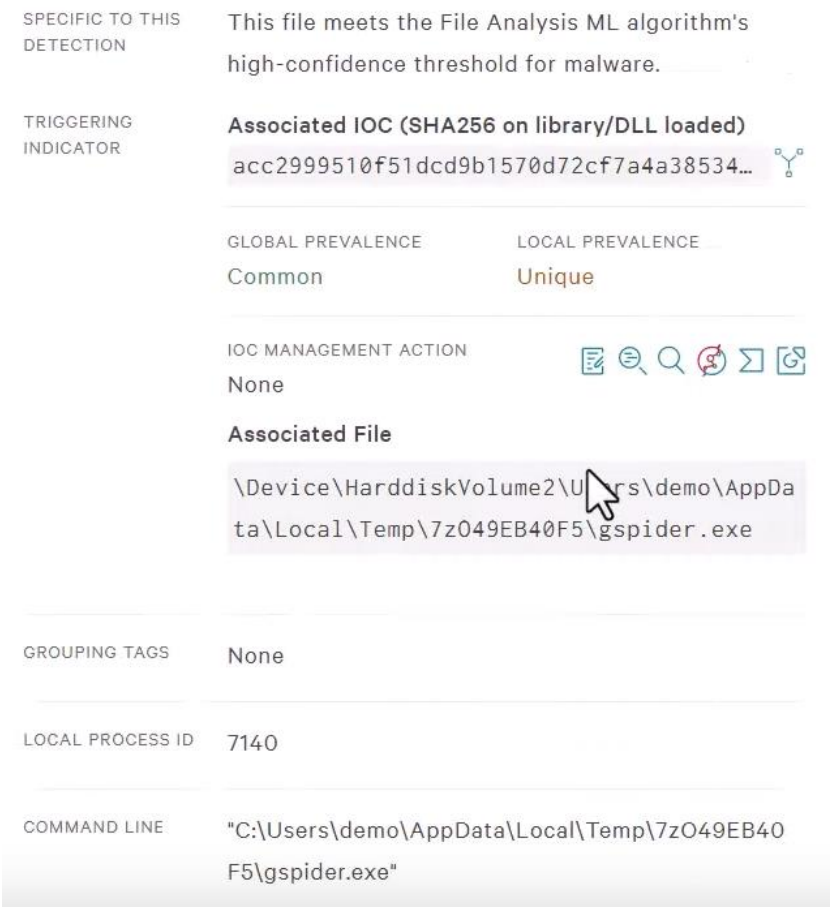


Рис. 3.13. Детальна інформація про файл

За допомогою звіту, який надає Falcon, можна детальніше ознайомитися з загрозою та джерелом даної загрози.

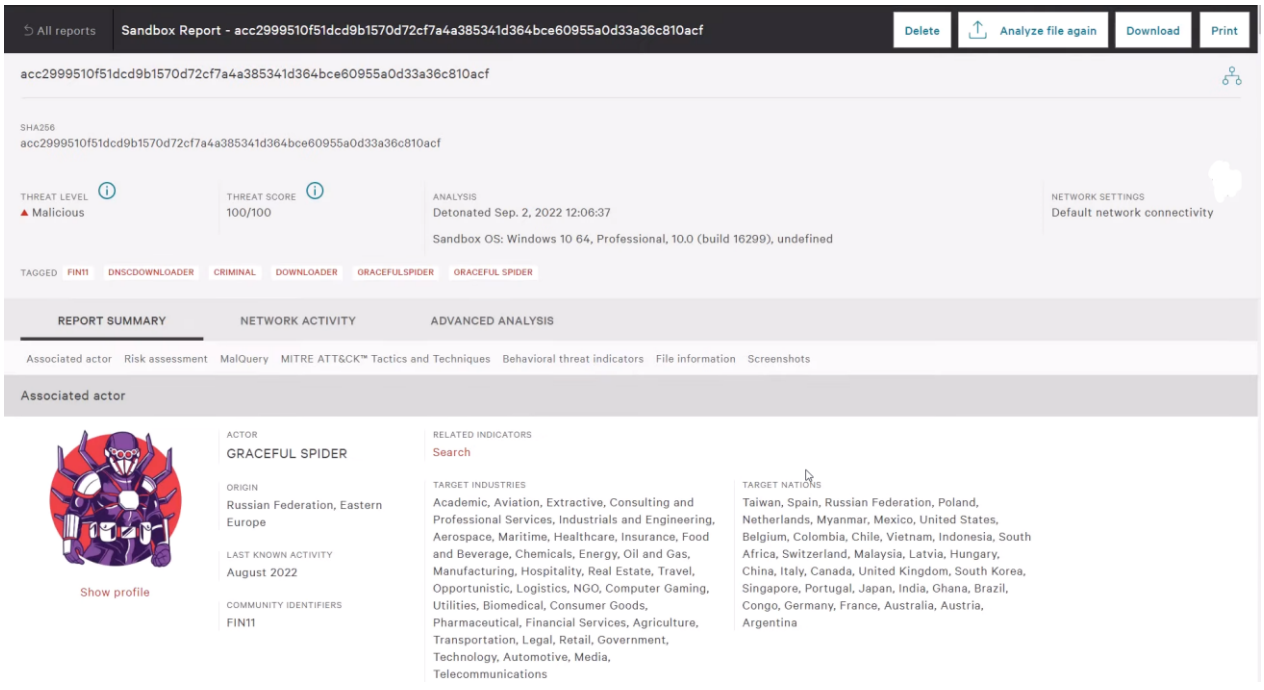


Рис. 3.14. Звіт про виявлену загрозу

Тут же доступна інформація, щодо мережевої активності та мережевих з’єднань які зловмисник намагався встановити за допомогою даного вірусу. Вся ця інформація допомагає ознайомитися з існуючими загрозами та допомагає виявити їх на інших пристроях.

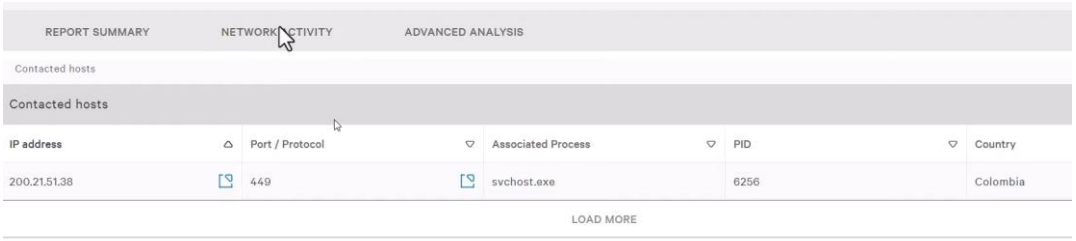


Рис. 3.15. Мережева активність загрози

Після цього спробуємо налаштувати політику безпеки. Вмикаємо налаштування «Виявлення під час запису» та «Ізоляція під час запису» щоб аналізувати підозрілі файли під час їхнього запису на диск.

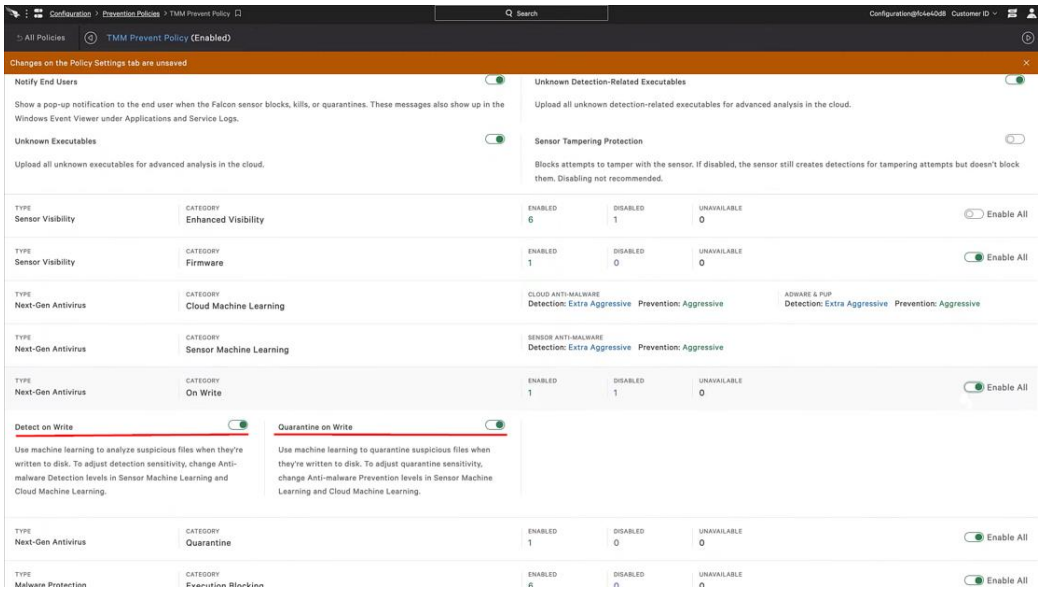


Рис. 3.16. Налаштування політики безпеки

Тепер при спробі розпакувати арів з вірусом його одразу ж буде ізольовано.

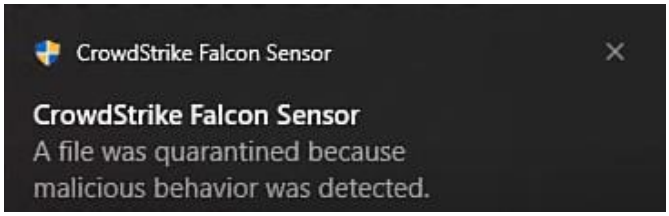


Рис. 3.17. Повідомлення від Falcon, про ізоляцію шкідливої програми

Біла позначка в кутку даної загрози означає, що процес або операцію було примусово зупинено.

Рис. 3.18. Результати виявлення нової загрози

Falcon також надає корисну функцію для контролю USB пристроїв. Ви можете надати різні рівні доступу для таких пристроїв, як принтери та носії інформації.

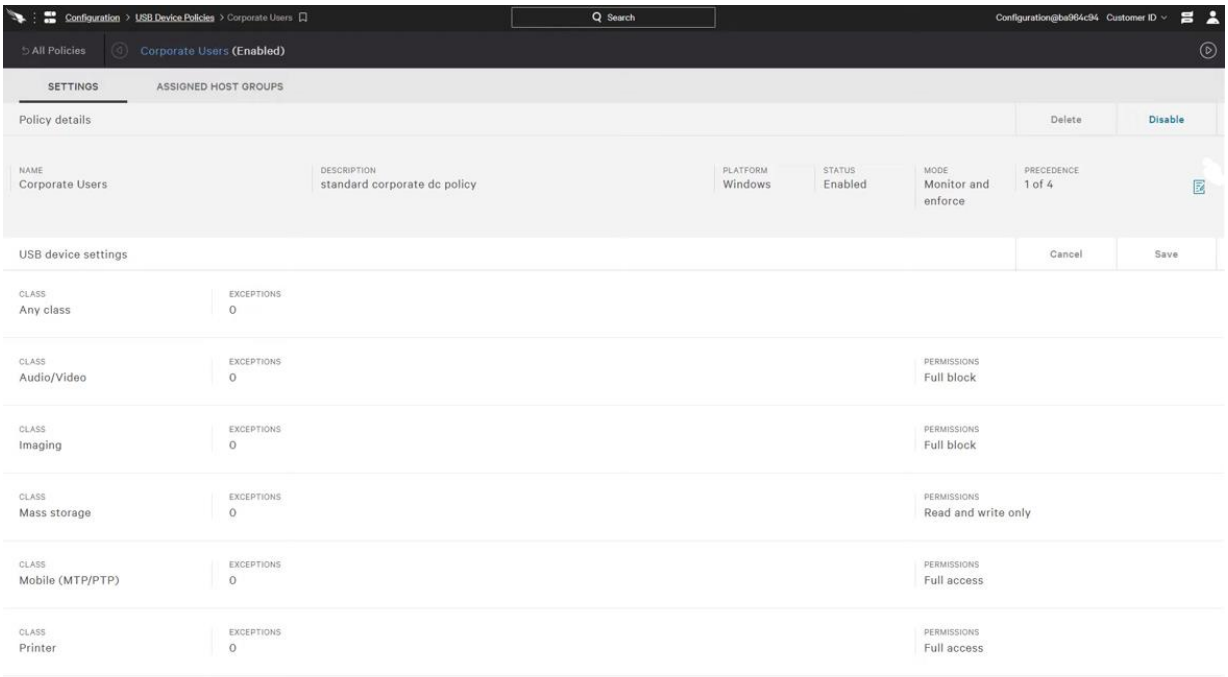


Рис. 3.19. Панель керування USB пристроями

Для кожної категорії девайсу можна обрати відповідні права доступу. Якщо користувач під’єднає заборонений девайс, він отримає повідомлення з поясненням що підключення того чи іншого пристрою заборонено політикою компанії.

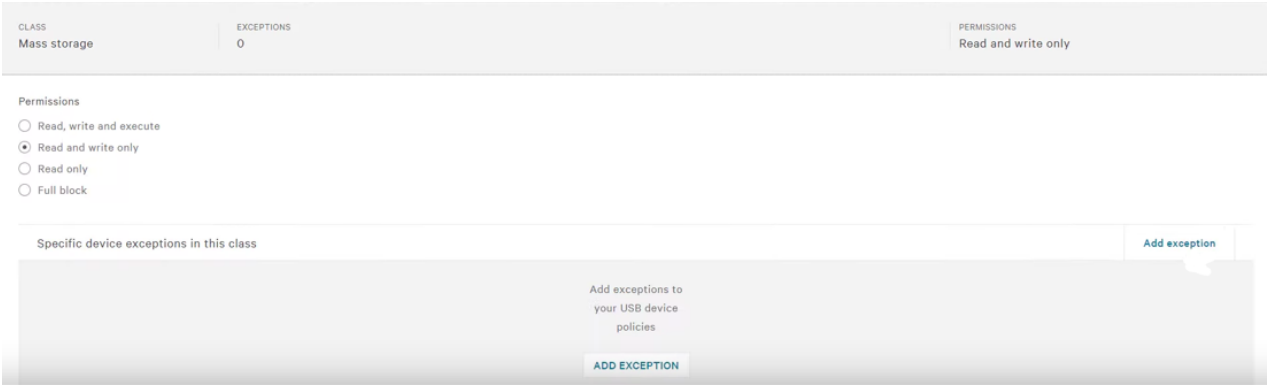


Рис. 3.20. Права доступу для користування носіями інформації

Для зручності та більш гнучкого керування можна додавати вийнятки до правил. Винятки можуть бути зроблені на основі ID пристрою або на основі виробника пристрою.

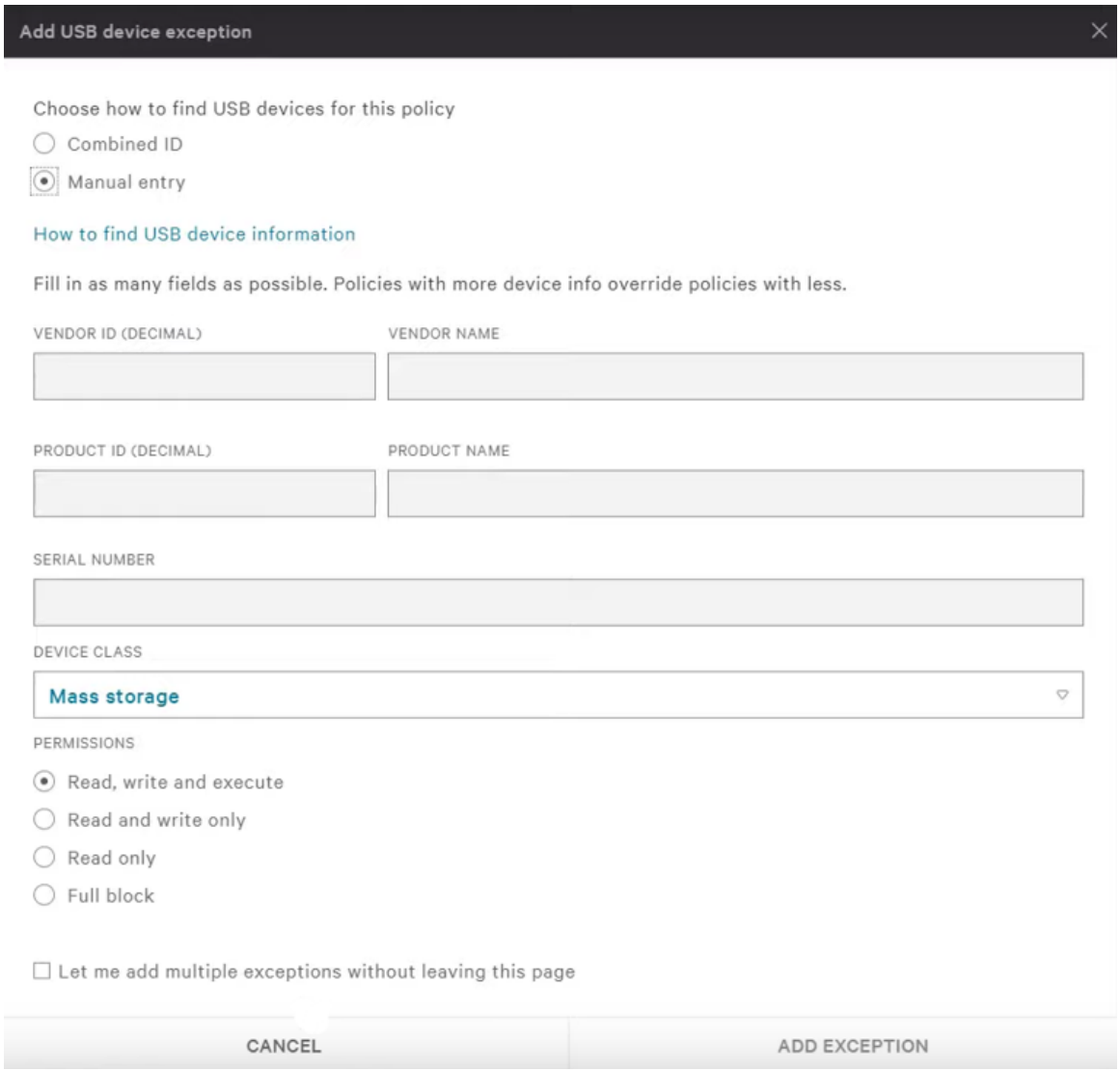


Рис. 3.21. Додавання винятку

Falcon дозволяє централізовано керувати налаштуванням фаєрвола, який встановлено на кінцевому пристрої. В панелі керування фаєрволом можна редагувати налаштування для групи пристроїв або створити нову групу пристрої. Це може бути корисним, якщо в компанії існують різні правила для різних типів пристроїв. При створенні нової групи правил можна одразу додати існуючі, або заздалегідь приготовлені правила. Також є можливість додати правила пізніше.

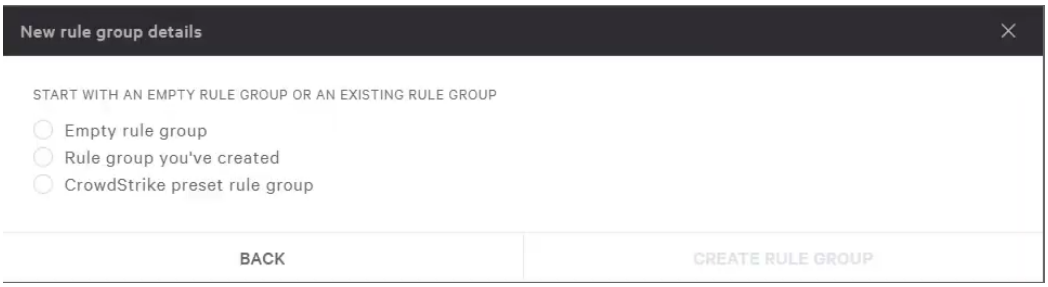


Рис. 3.22. Створення нової групи правил

Для кожного нового правила треба додати назву та опис, а також прописати які саме дії будуть дозволені чи заблоковані. Наприклад можна додати правило для блокування запитів до певний DNS серверів.

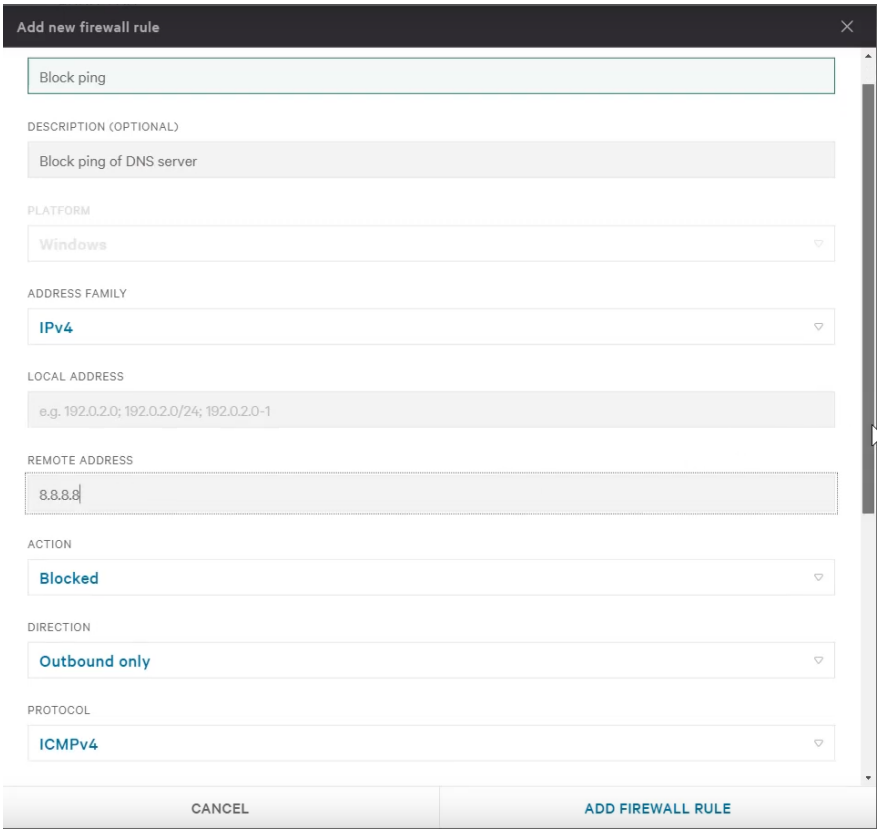


Рис. 3.23. Створення нового правила

Тут же для кожного правила можна вказати профіль мережі. Ця функція допомагає гарантувати, що правила застосовуються в правильних обставинах, наприклад, коли користувач перебуває у внутрішній або публічній мережі.

Рис. 3.24. Налаштування профілю мережі

Після створення та введення в дію нового правила, можна побачити таке повідомлення про стан фаєрволу на кінцевому пристрої.

Рис. 3.25. Стан фаєрволу на кінцевому пристрої

Для того, щоб переконатися, що правило працює, спробуємо відправити запит на заблокований нами DNS сервер.

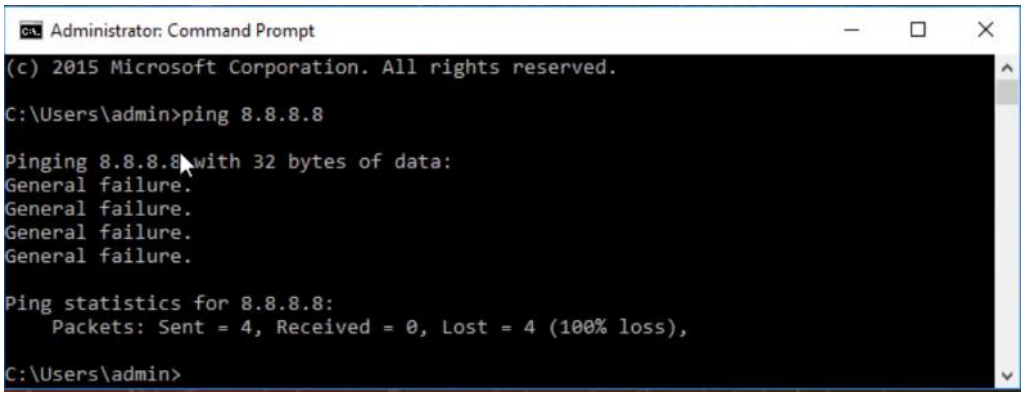


Рис. 3.25. Перевірка роботи фаєрволу

3.3. Розробка рекомендацій щодо захисту кінцевих користувачів на основі EDR

При розгортанні EDR підприємствам слід дотримуватися кількох рекомендацій, щоб забезпечити успішне впровадження та ефективний захист від кібератак. Ось кілька ключових аспектів, на які варто звернути увагу:

• Сформувати чітке розуміння середовища організації: Перш ніж розгортати рішення EDR, організації повинні мати чітке уявлення про своє середовище, включаючи кількість і типи кінцевих точок, додатків і даних. Таке розуміння допоможе організаціям визначити, які дані їм потрібно захистити, а також сформувати стратегію розгортання EDR;

• Впровадити комплексну стратегію захисту кінцевих точок: Рішення EDR - це лише частина комплексної стратегії безпеки кінцевих точок. Підприємства також повинні впроваджувати інші заходи безпеки, такі як антивірусне програмне забезпечення, брандмауери та системи запобігання вторгненням, щоб забезпечити багаторівневий захист від загроз;

• Забезпечити належне розгортання та конфігурацію: Щоб забезпечити ефективність EDR, його необхідно розгорнути та налаштувати належним чином. Це включає в себе забезпечення охоплення всіх кінцевих точок, інтеграцію рішення з іншими інструментами безпеки, а також належне налаштування та моніторинг сповіщень;

• Моніторинг та аналіз сповіщень: Рішення EDR генерують велику кількість сповіщень, тому важливо відстежувати та аналізувати їх, щоб визначити, які з них є справжніми загрозами, а які - хибними спрацьовуваннями. Підприємства повинні мати спеціальну команду, відповідальну за моніторинг та аналіз сповіщень, щоб забезпечити швидке реагування на реальні загрози;

• Регулярне оновлення: Рішення EDR можуть виявляти загрози та реагувати на них, лише якщо кінцеві точки правильно оновлені та мають відповідні патчі. Підприємства повинні мати процес управління оновленнями, щоб гарантувати, що на всіх кінцевих точках встановлені найновіші патчі та оновлення безпеки;

- Проводьте регулярне тестування та експертизу: Регулярне тестування та експертиза EDR системи і загальної стратегії безпеки кінцевих точок мають вирішальне значення для забезпечення належного захисту організації від кіберзагроз. Це включає в себе проведення тестування на проникнення та оцінку вразливостей для виявлення слабких місць і поліпшення загального стану безпеки.

ВИСНОВКИ

Захист кінцевих пристроїв є надзвичайно важливою складовою кібербезпеки в сучасному цифровому світі. З поширенням дистанційної роботи під час епідемії коронавірусу зростає залежність від цих пристроїв, що робить їх більш вразливими перед кіберзагрозами. У світі, де кількість кібератак постійно зростає, ефективний захист кінцевих пристроїв стає критично важливим для збереження конфіденційності, цілісності та доступності даних.

Проаналізовано теоретичні матеріали щодо загроз інформаційної безпеки. Виявлено види загроз, які є актуальними для кінцевих пристроїв.

Проведено аналіз існуючих методів та засобів виявлення та реагування на загрози на кінцевих пристроях.

Досліджено роботу програмного комплексу CrowdStrike Falcon. Показано можливості, щодо реагування на кіберінциденти.

Для більш ефективного використання EDR систем було розроблено відповідні рекомендації.

Варто зазначити, що запропоновані рекомендації не дають сто відсоткової гарантії забезпечення необхідного рівня безпеки кінцевих пристроїв. Проте користуючись рекомендаціями працівник відділу інформаційної безпеки матиме можливість поліпшити рівень захищеності від загроз, спрямованих на кінцеві пристрої.

Рекомендації у своїй роботі можуть використовувати керівники відділів інформаційної безпеки та працівники відділу інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Distribution of cyber attacks across worldwide industries in 2022. URL: https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/ (дата звернення: 04.05.2023)

2. ENISA Threat Landscape 2022. URL: https://www.deepl.com/ru/translator#en/uk/ENISA%20Threat%20Landscape%202022 (дата звернення: 05.05.2023)

3. What Is Endpoint Security. URL: https://www.deepl.com/ru/translator#en/uk/What%20Is%20Endpoint%20Security%3F (дата звернення: 06.05.2023)

4. Follow the Data: Dissecting Data Breaches and Debunking Myths. URL: https://documents.trendmicro.com/assets/wp/wp-follow-the-data.pdf (дата звернення: 06.05.2023)

5. EDR vs EPP: Key Features, Differences, and How They Work Together. URL: https://perception-point.io/guides/endpoint-security/edr-vs-epp-key-features-differences-using-them-together/ (дата звернення: 07.05.2023)

6. The Forrester Wave: Endpoint Detection And Response Providers, Q2 2022. URL: https://reprints2.forrester.com/#/assets/2/482/RES176332/report (дата звернення: 08.05.2023)

7. Microsoft Defender for Endpoint. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWOklP?culture=en-us&country=US (дата звернення: 08.05.2023)

8. Best Endpoint Detection & Response (EDR) Software. URL: https://www.g2.com/categories/endpoint-detection-response-edr (дата звернення: 08.05.2023)

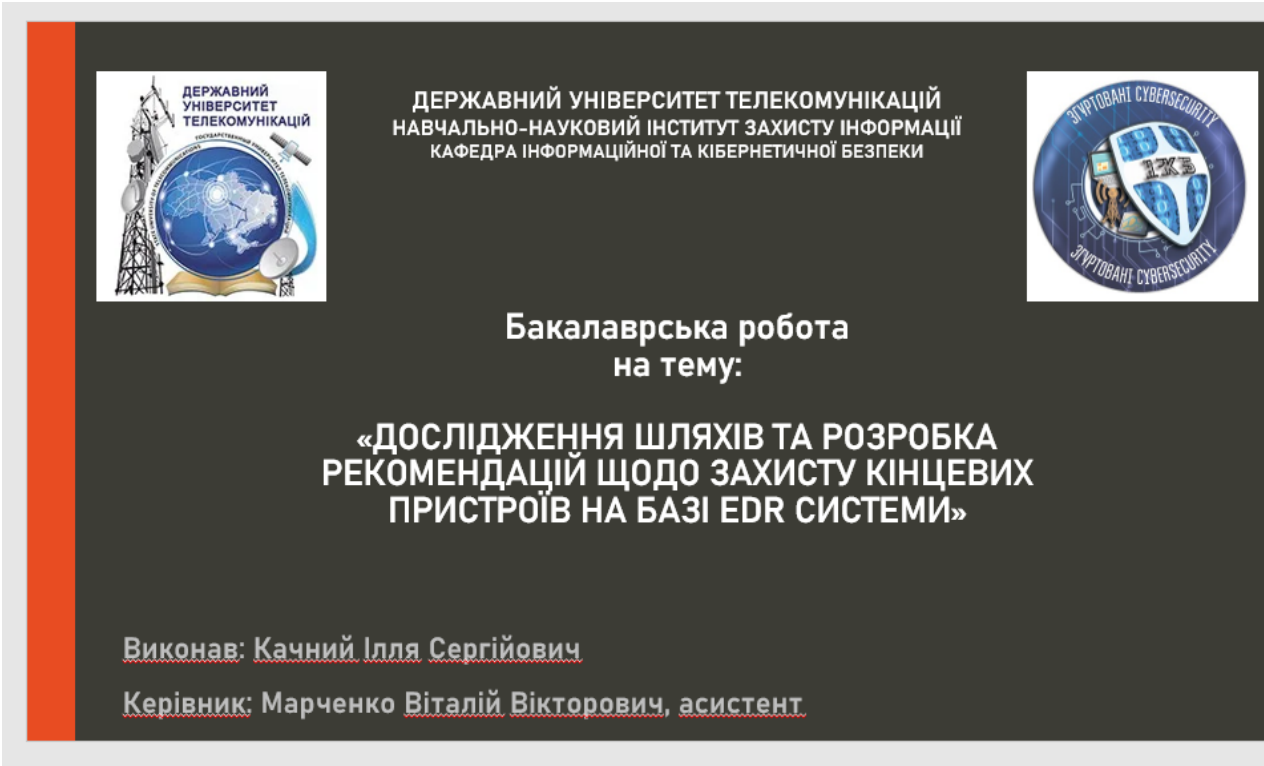
9. VMware Carbon Black Endpoint. URL: https://www.vmware.com/products/carbon-black-endpoint.html (дата звернення: 08.05.2023)

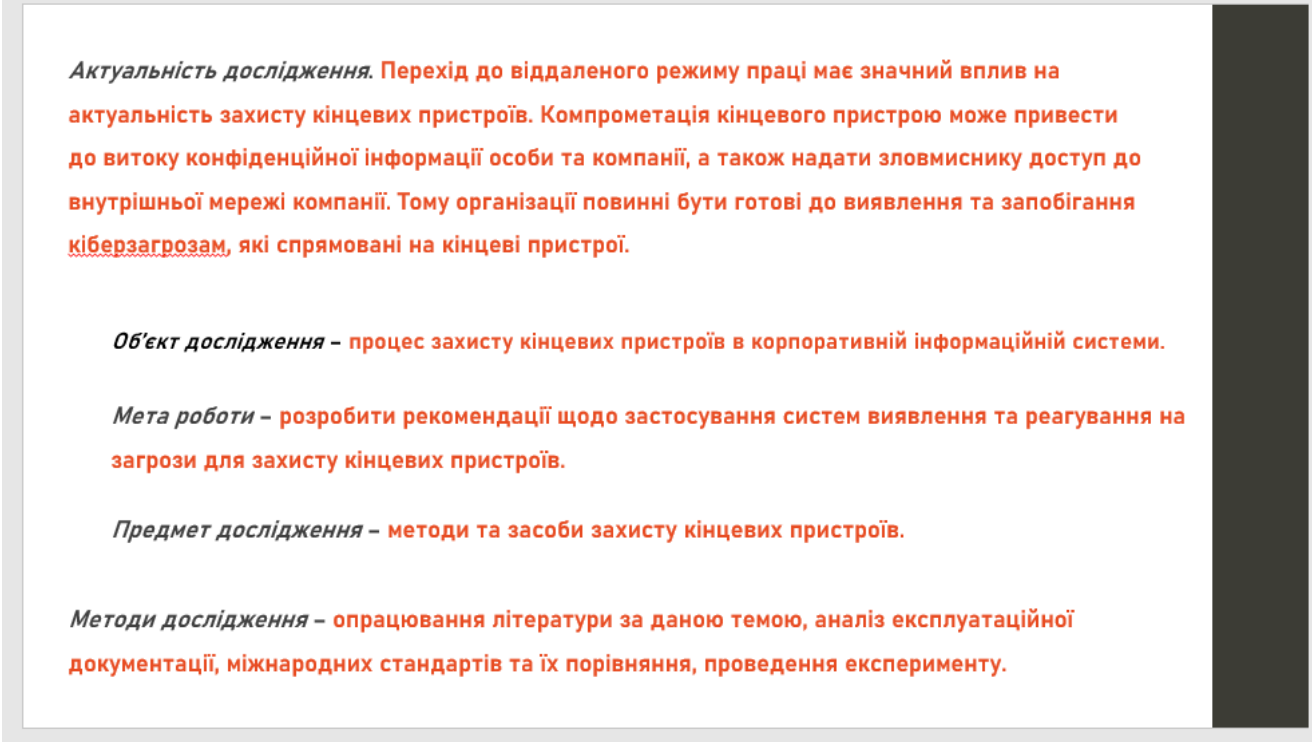
10. Cisco Secure Endpoint Data Sheet. URL: https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html (дата звернення: 08.05.2023)

11. CrowdStrike. One Platform. Complete Protection. URL: https://www.crowdstrike.com/falcon-platform/ (дата звернення: 13.05.2023)

12. CrowdStrike Threat Graph. URL: https://www.crowdstrike.com/falcon-platform/threat-graph/ (дата звернення: 13.05.2023)

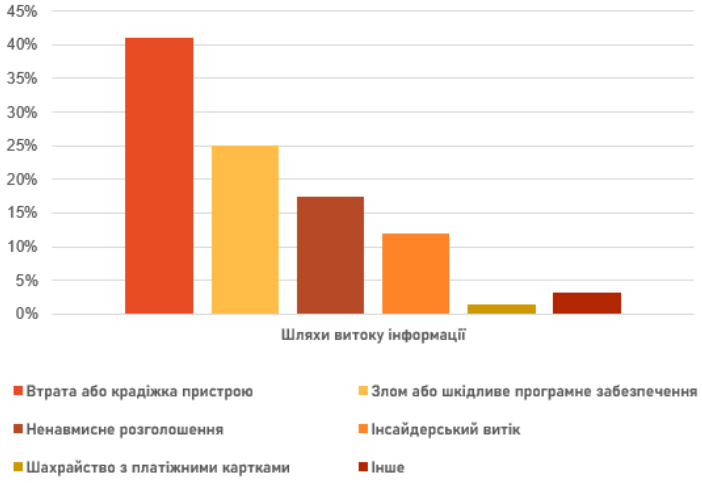
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)





Загрози для кінцевих пристроїв

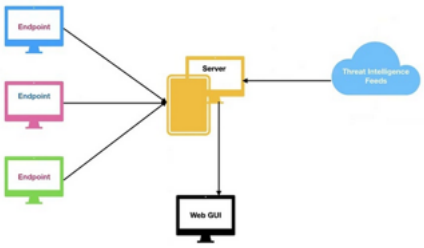
- Фішингові атаки
- Шкідливе програмне забезпечення
- Втрата пристроїв
- Застарілі оновлення
- Втрата та крадіжка даних
- Програми-вимагачі
- DDoS
- Атаки ботнет-мереж



EPP vs EDR

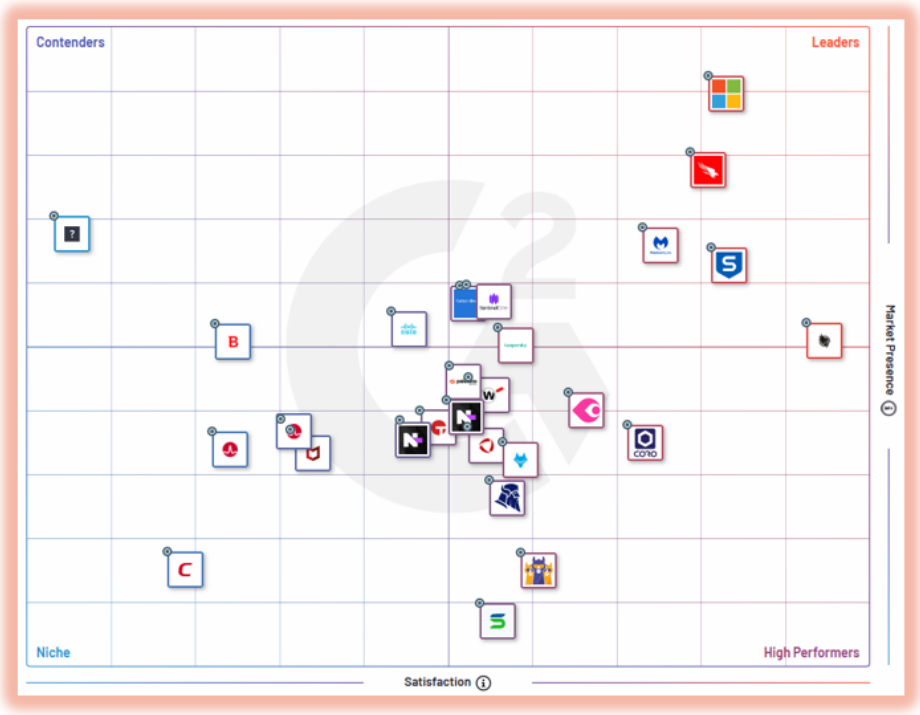
Особливості EDR

- Виявлення загроз і сповіщення - виявляє зловмисну активність і незвичні процеси на кінцевій точці та сповіщає команди безпеки;
- Розслідування інцидентів - можливість збору інформації про інцидент інформаційної безпеки та даних про трафік з декількох кінцевих точок;
- Ізоляція - автоматично ізолює заражені кінцеві пристрої та запобігає поширенню загроз мережею;
- Реагування на інциденти - дозволяє командам безпеки виконувати стирання та повторне створення образу скомпрометованого кінцевого пристрою або скидання паролів



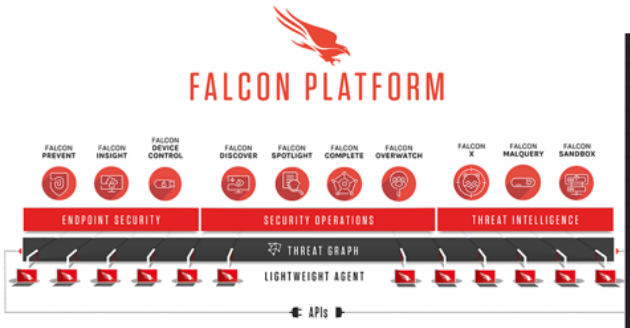
Особливості EPP

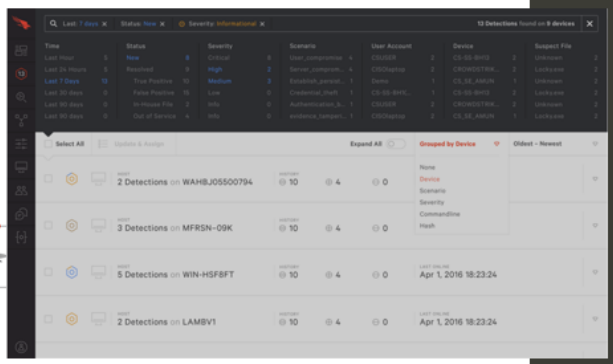
- Сигнатури загроз - антивірусна функція, яка виявляє загрози, порівнюючи їх з відомими сигнатурами шкідливого програмного забезпечення;
- Статичний аналіз - аналіз підозрілих бінарних файлів, як правило, з використанням методів машинного навчання, для виявлення шкідливих компонентів;
- Поведінковий аналіз - за відсутності відомих сигнатур загроз, EPP може аналізувати поведінку кінцевих пристроїв і виявляти аномальні шаблони, які потребують розслідування;
- Пісочниця - тестування на предмет зловмисної активності шляхом запуску файлів у віртуальному середовищі перед звичайним виконанням на кінцевому пристрої

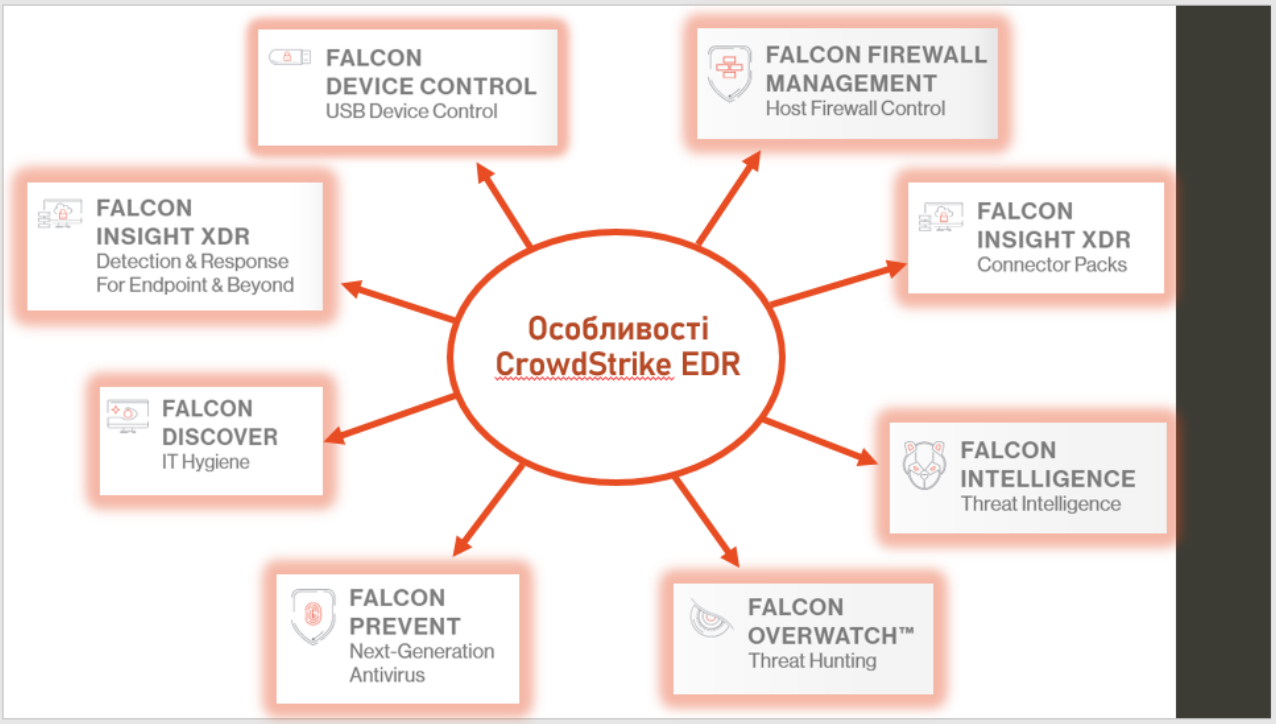


CrowdStrike Falcon

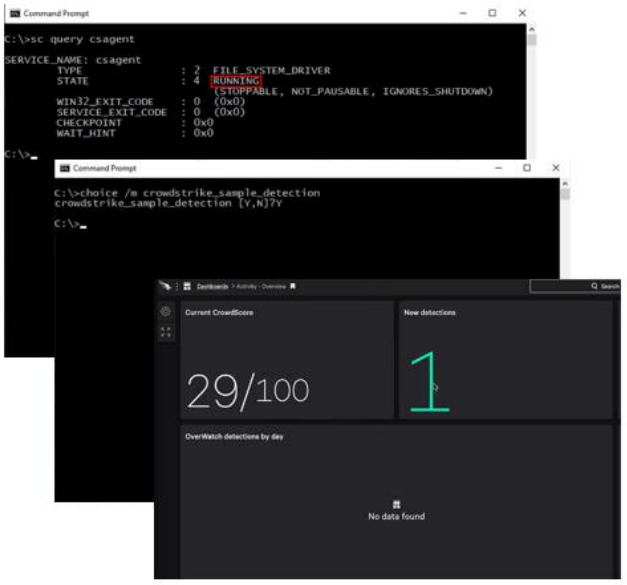
CrowdStrike Falcon Platform - це хмарне рішення для захисту кінцевих пристроїв, яке допомагає малому та великому бізнесу забезпечити антивірусний захист і контроль над пристроями. Платформа забезпечує захист комп'ютерів під управлінням Windows, Mac і Linux, включаючи сервери Windows і мобільні пристрої. Falcon також відповідає нормативним вимогам. Серед клієнтів компанії - банки, уряди та організації охорони здоров'я.

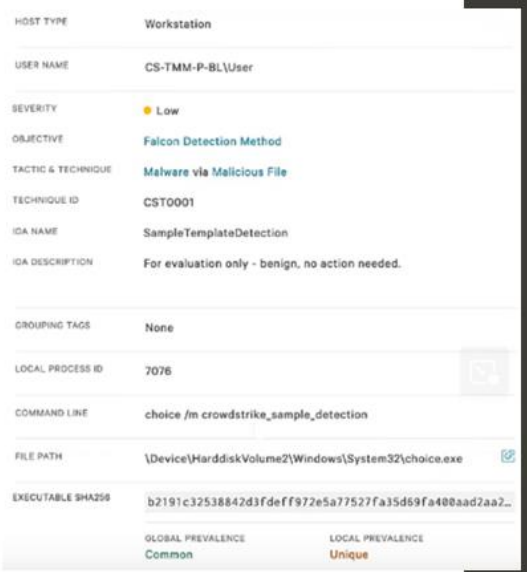




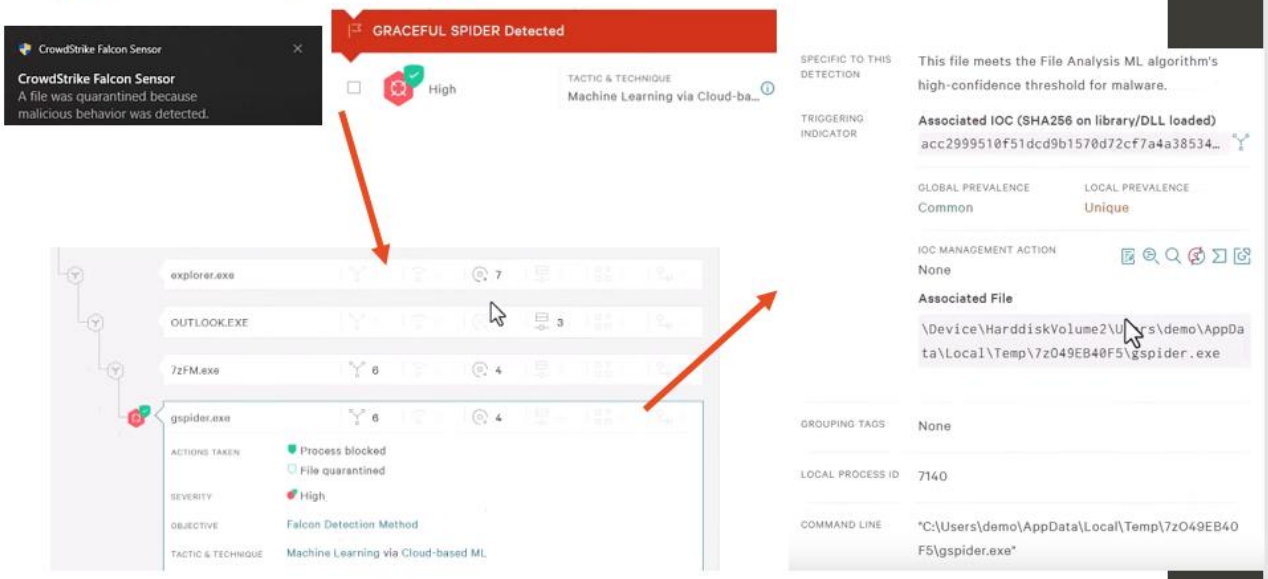


Перевірка роботи агенту

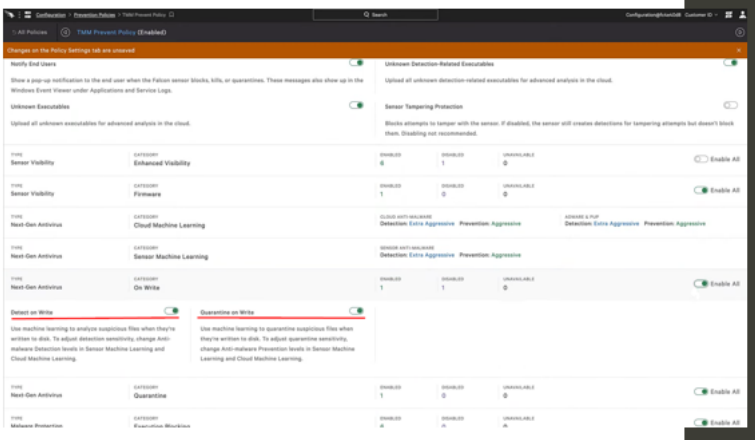




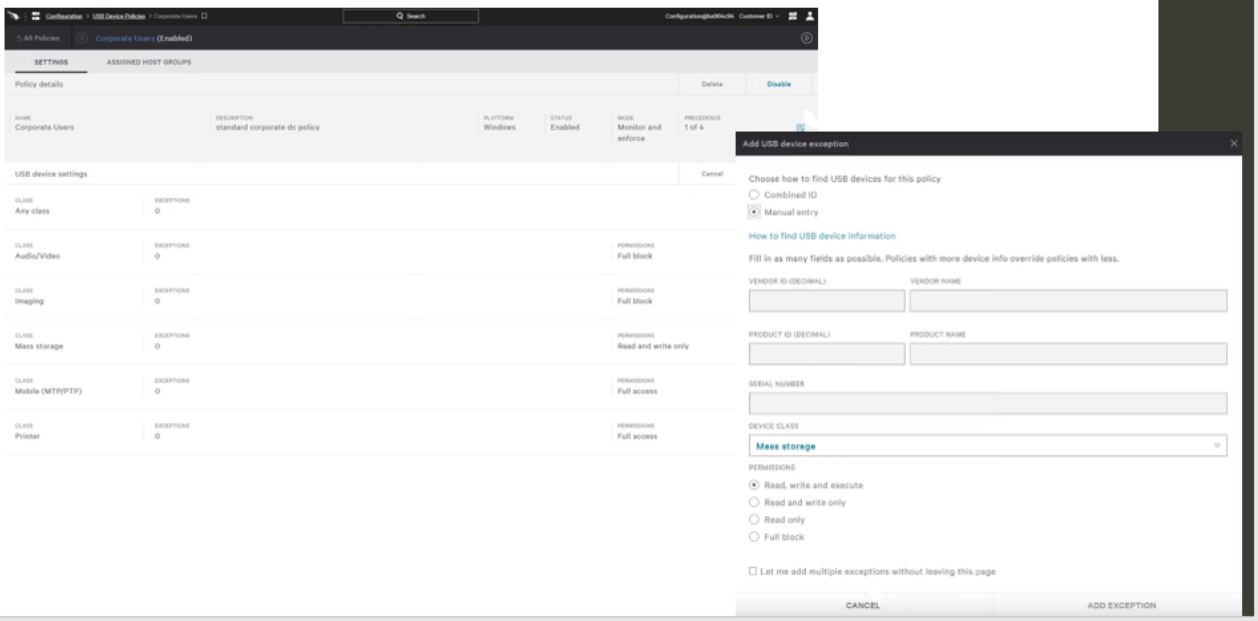
Демонстрація роботи EDR



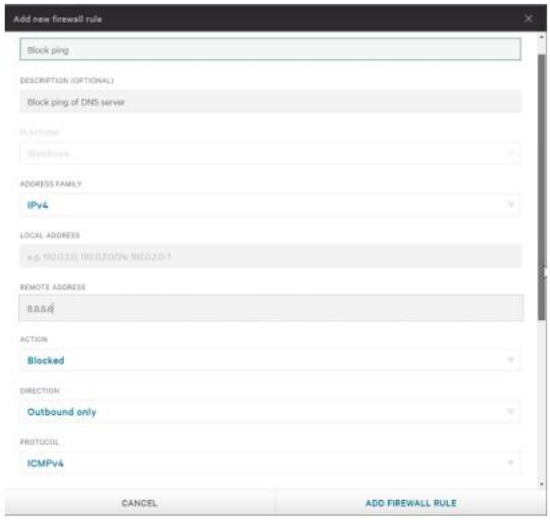
Вмикаємо налаштування «Виявлення під час запису» та «Ізоляція під час запису» щоб аналізувати підозрілі файли під час їхнього запису на диск.

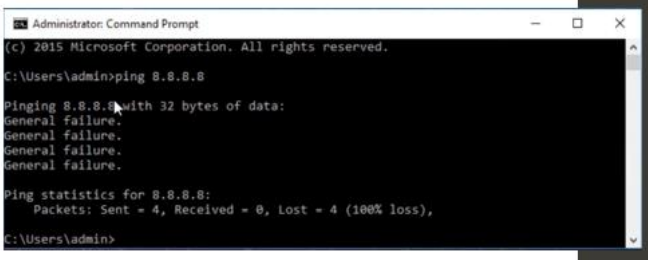


Контроль USB-пристроїв



Управління фаєрволом





Загальні рекомендації щодо використання EDR систем

- Сформувати чітке розуміння середовища організації: Перш ніж розгортати рішення EDR, організації повинні мати чітке уявлення про своє середовище, включаючи кількість і типи кінцевих точок, додатків і даних.
- Впровадити комплексну стратегію захисту кінцевих точок: Рішення EDR - це лише частина комплексної стратегії безпеки кінцевих точок. Підприємства також повинні впроваджувати інші заходи безпеки, такі як антивірусне програмне забезпечення, брандмауери та системи запобігання вторгненням, щоб забезпечити багаторівневий захист від загроз.
- Моніторинг та аналіз сповіщень: Рішення EDR генерують велику кількість сповіщень, тому важливо відстежувати та аналізувати їх, щоб визначити, які з них є справжніми загрозами, а які - хибними спрацьовуваннями.
- Проводьте регулярне тестування та експертизу: Регулярне тестування та експертиза EDR системи і загальної стратегії безпеки кінцевих точок мають вирішальне значення для забезпечення належного захисту організації від кіберзагроз.

Дякую за увагу

Виконав: Качний Ілля Сергійович

Керівник: Марченко Віталій Вікторович, асистент