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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту кінцевих пристроїв на основі EDR системи»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

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

Виконав: здобувач вищої освіти групи БСДМ-63
БУТЕНКО Андрій
(ПРІЗВИЩЕ, Ім'я)

Керівник: МАРЧЕНКО Віталій
д.ф., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

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

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бутенку Андрію Сергійовичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія захисту кінцевих пристроїв на основі EDR системи»
керівник кваліфікаційної роботи: МАРЧЕНКО Віталій, д.ф., доцент,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
кінцеві пристрої
технологія захисту кінцевих пристроїв на основі CrowdStrike
програмні комплекси захисту кінцевих пристроїв
наукова та технічна література, експлуатаційна документація

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми захисту кінцевих пристроїв
2. Дослідження методів та засобів захисту кінцевих пристроїв
3. Розроблення варіанта технології захисту кінцевих пристроїв на основі EDR CrowdStrike

5. Перелік ілюстративного матеріалу:

Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми захисту кінцевих пристроїв	18.10.2023 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	21.10.2023 р.	
3.	Аналіз проблеми захисту кінцевих пристроїв	26.10. 2023р.	
4.	Дослідження методів та засобів захисту кінцевих пристроїв	02.11.2023 р.	
5.	Розроблення варіанта технології захисту кінцевих пристроїв на основі CrowdStrike EDR	14.11.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	25.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач вищої освіти _____ Андрій БУТЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

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

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Бутенко А.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія захисту кінцевих пристроїв на основі EDR системи».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач ***БУТЕНКО Андрій*** обрав тему роботи, метою якої було дослідити зміст технології захисту кінцевих пристроїв на основі CrowdStrike EDR. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***БУТЕНКО Андрій*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***БУТЕНКО Андрій*** на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Бутенко А.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Бутенка Андрія
на тему: «Технологія захисту кінцевих пристроїв на основі EDR системи».

Актуальність:

Проблеми захисту кінцевих пристроїв у сучасному світі визначається низкою ключових факторів, які вимагають високого рівня кібербезпеки для забезпечення цілісності, конфіденційності та доступності інформації. Зростання обсягів кіберзагроз та складність атак стає суттєвим викликом для організацій та індивідуальних користувачів. Атаки на кінцеві пристрої стають більш витонченими та масштабними, загрожуючи конфіденційності особистих даних та корпоративної інформації. Тому організації зосереджують свою увагу на впровадження технологій захисту кінцевих пристроїв. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми забезпечення захисту кінцевих пристроїв, досліджено методи та засоби захисту кінцевих пристроїв.
2. Запропоновано варіант технології захисту кінцевих пристроїв на основі EDR CrowdStrike.
3. 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 магістерської роботи.

Недоліки:

1. У кваліфікаційній роботі доцільно було б порівняти EDR CrowdStrike з іншими представниками EDR систем та надати звітність у вигляді порівняльної таблиці.
2. Запропонований варіант технології технології захисту кінцевих пристроїв на базі рішення CrowdStrike EDR доцільно було б показати на прикладі конкретного підприємств.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре»**, а здобувач **БУТЕНКО Андрій** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент: _____ _____
підпис *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 51 сторінка, 36 рисунків, 13 джерел.

Об'єкт дослідження – процес забезпечення захисту кінцевих пристроїв.

Предмет дослідження – технологія забезпечення захисту кінцевих пристроїв на базі рішення CrowdStike EDR.

Мета роботи – розробити варіанти технології захисту кінцевих пристроїв на базі рішення CrowdStike EDR для інформаційної системи підприємства та рекомендації щодо застосування технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, моделювання процесу захисту кінцевих пристроїв на базі рішення CrowdStike EDR.

В роботі проведено аналіз проблеми захисту кінцевих пристроїв на основі проаналізованих загроз кінцевих пристроїв. Проаналізовано існуючі технології захисту кінцевих пристроїв.

Досліджено методи та засоби захисту кінцевих пристроїв.

Запропоновано варіант технології захисту кінцевих пристроїв на базі рішення CrowdStike EDR. Визначено роль EDR систем у сучасних стратегіях кіберзахисту та компоненти і архітектуру EDR системи.

На основі проведених досліджень, в роботі розроблено варіант технології захисту кінцевих пристроїв на основі CrowdStike EDR та рекомендації щодо застосування технології захисту кінцевих пристроїв.

Галузь використання — кібербезпека інформаційної системи підприємства.

МЕТОДИ ТА ЗАСОБИ, АРХІТЕКТУРА, МОДУЛІ, ФУНКЦІЇ, EDR, ФІШИНГ, ПАТЧ, ЕКСПЛОЙТ, ФАЄРВОЛ, АНТИВІРУСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕНННЯ, КІНЦЕВІ ПРИСТРОЇ, ЗАГРОЗИ, СИСТЕМИ, ЗАХИСТ, КІБЕРБЕЗПЕКА

ABSTRACT

Text part of the master's qualification work: 51 pages, 36 figures, 13 sources.

Object of research - is the process of endpoint security.

Subject of research - is the technology of endpoint security based on the CrowdStike EDR solution.

The purpose of the work is to develop variants of endpoint security technology based on the CrowdStike EDR solution for the enterprise information system and recommendations for the use of technology.

Research methods - studying the literature on this topic, analyzing operational documentation, modeling the process of protecting endpoints based on the CrowdStike EDR solution.

The paper analyzes the problem of endpoint security based on the analyzed endpoint threats. Existing endpoint security technologies are analyzed.

Methods and means of protecting endpoints are investigated.

A variant of endpoint security technology based on the CrowdStike EDR solution is proposed. The role of EDR systems in modern cybersecurity strategies, as well as the components and architecture of the EDR system are determined.

Based on the research, the paper develops a variant of endpoint security technology based on CrowdStike EDR and recommendations for the use of endpoint security technology.

The field of use is cybersecurity of the enterprise information system.

METHODS AND MEANS, ARCHITECTURE, MODULES, FUNCTIONS, EDR, PHISHING, PATCH, EXPLOIT, FIREWALL, ANTIVIRUS SOFTWARE, END DEVICES, THREATS, SYSTEMS, PROTECTION, CYBERSECURITY

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

UEM	—	Unified Endpoint Management
ПК	—	персональний комп’ютер
IoT	—	інтернет речей
EDR	—	endpoint detection and response
IDS/IPS	—	intrusion detection and prevention systems
BYOD	—	bring your own device
EPP	—	endpoint protection platform
API	—	application programming interface
ПЗ	—	програмне забезпечення
ШІ	—	штучний інтелект
ШПЗ	—	шкідливе програмне забезпечення

ВСТУП

Актуальність дослідження. На сьогоднішній день багато працівників працюють віддалено або використовують кінцеві пристрої для доступу до корпоративних ресурсів. Кількість загроз і атак на кінцеві пристрої продовжує зростати, а їхня важлива роль у бізнес-процесах і зберіганні конфіденційної інформації робить ефективний захист невід'ємною частиною кібербезпеки [1].

Оскільки організації зберігають великі обсяги конфіденційної інформації на своїх кінцевих пристроях. Зловмисники прагнуть отримати несанкціонований доступ до цих даних для здійснення крадіжок або шантажу. Захист інформації, яка зберігається на кінцевих пристроях, стає стратегічно важливим завданням для організацій.

Звертаючи увагу на те що сучасна кіберзлочинність стає все більш виразною і складною. Зловмисники вдосконалюють свої методи та використовують нові технології для здійснення атак на користувачів та організації. Кінцеві пристрої, такі як комп'ютери, ноутбуки та смартфони, є основним об'єктом інтересу для зловмисників, оскільки вони містять велику кількість конфіденційної інформації.

Вищезазначені аргументи актуалізують тему даної кваліфікаційної роботи, зміст якої становлять дослідження щодо технології захисту кінцевих пристроїв на основі EDR системи та розробка рекомендацій щодо її впровадження.

Об'єкт дослідження – процес забезпечення захисту кінцевих пристроїв.

Предмет дослідження – технологія забезпечення захисту кінцевих пристроїв на базі рішення CrowdStike EDR.

Мета роботи – розробити варіант технології захисту кінцевих пристроїв на базі рішення CrowdStike EDR для інформаційної системи підприємства та рекомендації щодо застосування технології.

Наукові завдання:

- провести аналіз щодо проблеми забезпечення захисту кінцевих пристроїв;

- проаналізувати основні загрози кінцевих пристроїв;
- дослідити методи та засоби захисту кінцевих пристроїв;
- розробити варіант технології захисту кінцевих пристроїв на основі CrowdStike EDR та рекомендації щодо застосування даної технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, моделювання процесу захисту кінцевих пристроїв на базі рішення CrowdStike EDR.

Практичне значення одержаних результатів полягає в розробці варіанта технології захисту кінцевих пристроїв на базі рішення CrowdStike EDR для інформаційної системи підприємства та рекомендації щодо застосування технології для надійного захисту кінцевих пристроїв.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки» [1].

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ

1.1. Аналіз проблеми забезпечення захисту кінцевих пристроїв

Безпека кінцевих пристроїв — це практика захисту кінцевих пристроїв або пристроїв кінцевих користувачів, таких як настільні ПК, ноутбуки та мобільні пристрої, від використання зловмисниками та кампаніями. Системи безпеки кінцевих пристроїв захищають кінцеві пристрої в мережі або в хмарі від загроз кібербезпеці. Безпека кінцевих пристроїв еволюціонувала від традиційного антивірусного програмного забезпечення до комплексного захисту від складних зловмисних програм і нових загроз нульового дня [2].

Організації будь-якого розміру піддаються ризику з боку національних держав, хактивістів, організованої злочинності, а також зловмисних і випадкових внутрішніх загроз. Безпека кінцевих пристроїв часто розглядається як головна лінія кібербезпеки, і це одне з перших місць, де організації прагнуть захистити свої корпоративні мережі.

Оскільки обсяг і складність загроз кібербезпеці невпинно зростають, зростає й потреба в більш досконалих рішеннях безпеки кінцевих пристроїв. Сучасні системи захисту кінцевих пристроїв розроблені для швидкого виявлення, аналізу, блокування та стримування поточних атак. Для цього вони повинні співпрацювати один з одним та з іншими технологіями безпеки, щоб надати адміністраторам бачення передових загроз, щоб пришвидшити час виявлення та реагування на виправлення [3].

Кінцеві пристрої або точки – це фізичні пристрої, які підключаються до комп’ютерної мережі й обмінюються з нею інформацією. Приклади кінцевих точок: настільні комп’ютери, віртуальні машини, вбудовані й мобільні пристрої та сервери. Пристрої Інтернету речей, як-от камери, холодильники, системи освітлення й безпеки, розумні термостати, – це також кінцеві точки. Обмін інформацією між пристроями (наприклад, ноутбуком) і мережею, до якої вони підключені, схожий на спілкування двох людей по телефону.

Рис. 1.1. Приклади кінцевих пристроїв [4]

Співробітники більше не покладаються лише на настільні ПК в офісі. Найбільшу активність віддаленої роботи за останні кілька років, що спричинив COVID-19 збільшив використання ноутбуків, iPad, iPhone, розумних годинників тощо для доступу до важливої інформації компанії 24 години на добу, сім днів на тиждень з будь-якого місця та будь-коли. Вони також не обмежується пристроями користувача. Принтери, факсимільні апарати, системи торгових точок і постійно зростаючий список пристроїв Інтернету речей (IoT), які зараз отримують доступ до мережі, — усе це приклади кінцевих точок і можливих зон входу для зловмисників [5].

1.2. Аналіз загроз кінцевих пристроїв

Поширені ризики безпеки кінцевої точки

1. Фішинг (Phishing)

Фішинг — це хакерська техніка, за якої зловмисники надсилають оманливі електронні листи, які нібито походять із надійних джерел, як-от відомі особи чи організації, з метою змусити одержувачів завантажити віруси чи шкідливий вміст [5].

Ця техніка надзвичайно популярна завдяки високому відсотку успіху, що використовує притаманну цікавість користувачів. Якщо фішинговий лист потрапляє до папки "Вхідні" будь-якого одержувача, він має шанс досягти своїх зловмисних цілей.

Щоб протистояти фішинговим атакам, найкращі методи включають навчання безпеки, фільтрацію електронної пошти та антивірусне програмне забезпечення. Будь-яка організація, користувачі якої підключені до корпоративних мереж, повинна надати пріоритет реалізації цих заходів. Крім того, Уніфіковане керування кінцевими точками (UEM) пропонує додатковий рівень безпеки, надаючи інформацію про всі кінцеві точки мережі та контроль над ними .

2. Недосвідчене управління патчами (patch management)

Внесення виправлень саме по собі не є ризиком для безпеки кінцевих точок , але невміння керувати виправленнями та оновленнями може призвести до значних ризиків. Правильне керування виправленнями має вирішальне значення для запобігання зламаним пристроям, але в багатьох організаціях немає офіційного процесу виправлення [5].

Забезпечення оновлення кінцевих точок є важливим для усунення вразливостей, які можуть призвести до зараження пристроїв. У минулому надсилання щомісячних оновлень на комп’ютери в корпоративній мережі було відносно простим за допомогою групової політики. Однак із збільшенням кількості кінцевих точок, якими

потрібно керувати, і зростаючою кількістю пристроїв, які безпосередньо не підключені до мережі, процес став складнішим.

З появою моделей віддаленої та гібридної роботи відстежувати різні типи апаратного забезпечення, програмного забезпечення, операційних систем і мобільних пристроїв, що використовуються, стало складніше. Крім того, покладатися на регулярне підключення користувачів до корпоративної мережі для отримання необхідних оновлень більше не є надійним підходом, особливо за відсутності чітко визначеного процесу виправлення.

3. Втрата та крадіжки: пристроїв

Сумно, що мобільні пристрої зникають. Вони невеликі, потужні та цінні, тож чи скаржаться користувачі на втрату пристрою, чи злодії насолоджуються швидким прибутком, це велика справа.

Щороку повідомляють про викрадення або втрату мільйонів смартфонів, і лише невеликий відсоток із них повертають. Незалежно від того, чи належить пристрій компанії чи користувачу, якщо він коли-небудь містив будь-які дані компанії, існує значний ризик неправомірного використання. Окрім вартості самого пристрою, існує також занепокоєння щодо цінності будь-якої інформації, що зберігається на ньому, до якої можуть отримати доступ зловмисники, які можуть обійти PIN-код. Це включає незашифровані тексти та електронні листи [5].

4. Експлойти вразливостей програмного забезпечення та застарілі патчі

Використання вразливостей програмного забезпечення може бути не таким поширеним, як фішингові атаки, але їх потенційна шкода може бути настільки ж серйозною. Недоліки, що виникають через неправильну конфігурацію, застаріле програмне забезпечення та непослідовні виправлення, є головними цілями для хакерів, які прагнуть ними скористатися. Дивно, але організаціям зазвичай потрібно близько 97 днів, щоб повністю встановити оновлення, що робить використання вразливості програмного забезпечення одним із провідних методів атак програм-вимагачів.

Зловмисники зазвичай використовують дві стратегії, щоб використовувати невиправлені недоліки безпеки програмного забезпечення. У першому підході вони володіють попередніми знаннями про вразливість і використовують інструменти сканування для виявлення сприйнятливих до неї середовищ. У другому підході вони вибирають цільову організацію, сканують її мережу на наявність уразливостей безпеки, а потім використовують їх. Отримавши доступ, хакери прагнуть якомога ширше розповсюдити програми-вимагачі в середовищі [5].

1.3. Аналіз технологій захисту кінцевих пристроїв

Існує кілька ключових технологій захисту кінцевих пристроїв, які використовуються для забезпечення кібербезпеки та запобігання загрозам. До них входять:

Антивірусне програмне забезпечення (Antivirus Software):

Спеціалізовані програми, які виявляють, блокують та видаляють шкідливі програми, такі як віруси, троянські програми, черв'яки та інші види шкідливого коду.

Фаєрволи (Firewalls):

Захищають мережевий трафік, контролюючи доступ до та з кінцевого пристрою. Фаєрволи можуть блокувати небажані підключення та фільтрувати мережевий трафік.

Антишпигуни (Anti-spyware):

Програми, спрямовані на виявлення та видалення шпигунського програмного забезпечення, яке може намагатися неправомірно збирати інформацію про користувача.

Антімалварне програмне забезпечення (Anti-malware):

Широкий термін, що охоплює різні типи програм, призначених для виявлення та боротьби зі зловмисним програмним забезпеченням, таким як віруси, черв'яки, троянські програми, рекламне програмне забезпечення та інші загрози.

Endpoint Detection and Response (EDR):

Технологія, що надає розширені можливості виявлення, відгуку та реагування на загрози на рівні кінцевих пристроїв. EDR відстежує та реагує на незвичайну активність та загрози в реальному часі.

Системи виявлення та запобігання вторгненням (Intrusion Detection and Prevention Systems - IDS/IPS):

Моніторять мережевий трафік для виявлення та блокування аномальної активності, що вказує на вторгнення або атаку.

Патч-менеджмент:

Система управління патчами, яка відповідає за вчасне встановлення оновлень та патчів для програмного забезпечення та операційних систем з метою усунення вразливостей.

Шифрування даних:

Забезпечує захист конфіденційності інформації шляхом шифрування даних, щоб унеможливити несанкціонований доступ.

Ці технології часто використовуються разом у комплексних стратегіях для максимально ефективного захисту кінцевих пристроїв від різних кіберзагроз.

BYOD (bring your own device) [6]

Відноситься до корпоративної IT-політики, яка визначає, коли та як співробітники, підрядники та інші авторизовані кінцеві користувачі можуть використовувати власні ноутбуки, смартфони та інші персональні пристрої в мережі компанії для доступу до корпоративних даних і виконання свої посадові обов'язки.

Висновки до розділу 1

В розділі проаналізовано проблеми захисту кінцевих пристроїв, приведено та здійснено аналіз загроз кінцевих пристроїв, а також технологій захисту кінцевих пристроїв.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ

2.1. Дослідження сучасних методів та засобів захисту кінцевих пристроїв

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 [7].

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 [8].

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.

Для оцінки та вибору засобу захисту кінцевих точок проаналізуємо магічний квадрат Гартнер (Рис. 2.1.).

Для оцінки постачальників будь-якого сегменту ринку інформаційних технологій Gartner використовує дві лінійні прогресивні експертні шкали - "повнота бачення" (англ. completeness of vision) і "здатність реалізації" (ability to execute). Кожен постачальник, що потрапив у рамки розгляду досліджуваного сегмента ринку за певними правилами включення, оцінюється за цими двома критеріями: «повнота бачення» відкладається на осі абсцис , «здатність реалізації» — на осі ординат . Кожен постачальник, таким чином, виявляється в одному з чотирьох квадрантів площини , які називаються:

«лідери» (leaders) — постачальники з позитивними оцінками як з «повноті бачення», і з «здатності реалізації»,

«претенденти» (challengers) — постачальники з позитивними оцінками лише за «здатністю реалізації»,

«провидці» (visionaries) - постачальники з позитивними оцінками тільки по "повноті бачення",

«Нішеві гравці» (niche players) - постачальники з негативними оцінками за обома критеріями.

Рис. 2.1. Магічний квадрат Gartner EDR [9]

Gartner називає «магічним квадрантом» (за алюзією на магічний квадрат) звіт з аналізом будь-якого сегмента ринку, який включає зображення з розподілом постачальників за вказаними чвертями; щорічно компанія випускає кілька десятків магічних квадрантів на регулярній основі. Постачальники іноді відзначають навіть сам факт потрапляння в якийсь магічний квадрант окремим прес-релізом як визнання

ринкових досягнень, навіть якщо компанія згадана лише у квадранті «нішевих гравців»

2.2. Роль технології EDR у сучасних стратегіях кіберзахисту

Технологія EDR (Endpoint Detection and Response) в сучасних стратегіях кіберзахисту відіграє ключову роль у виявленні та реагуванні на загрози на рівні кінцевих пристроїв. Її значення зростає в умовах швидкого розвитку та вдосконалення кіберзлочинності [10].

Ролі EDR:

1. Виявлення Аномальної Активності:

Технологія EDR відіграє ключову роль у виявленні незвичайної або підозрілої активності на кінцевих пристроях. Вона моніторить системні та мережеві події, визначає аномалії та потенційні загрози, що вказують на вторгнення чи інші безпекові проблеми.

2. Реагування в Реальному Часі:

Однією з ключових функцій EDR є можливість реагувати на загрози в реальному часі. Вона автоматично виявляє та ізолює компрометовані пристрої, зменшуючи час реакції та мінімізуючи можливі збитки від атак.

3. Збирання та Аналіз Даних:

Технологія EDR забезпечує збір та аналіз розширених даних про поведінку систем та користувачів. Аналіз цих даних допомагає виявляти навіть складні загрози, що можуть бути упущені іншими заходами безпеки.

4. Виявлення та Блокування Шкідливих Програм:

EDR використовує сигнатури та алгоритми виявлення, щоб визначити та блокувати шкідливі програми, такі як віруси, троянські програми та інші загрози, забезпечуючи захист від різноманітних видів малвари.

5. Адаптація та Навчання:

EDR використовує методи штучного інтелекту та машинного навчання для постійного вдосконалення алгоритмів виявлення. Вона адаптується до нових видів загроз та навчається на основі актуальних даних.

6. Миттєве Виявлення та Реагування на Інциденти:

Завдяки технології EDR можливе миттєве виявлення та реагування на інциденти, забезпечуючи ефективний контроль над безпекою навіть у випадках складних та швидко змінюючих сценаріїв атак.

7. Моніторинг та Логування:

EDR забезпечує систематичний моніторинг та логування подій на кінцевих пристроях, що сприяє аналізу та розслідуванню інцидентів.

8. Стратегії Виявлення Інцидентів:

Технологія EDR надає можливості для розроблення та реалізації стратегій виявлення інцидентів, враховуючи особливості конкретного бізнесу та потенційні загрози.

9. Співпраця із Системами Інших Рівнів:

EDR може взаємодіяти з іншими рівнями захисту, такими як фаєрволи, антивіруси та системи виявлення вторгнень, для створення комплексного захисту.

10. Боротьба із Загрозами на Рівні Кінцевого Користувача:

EDR зосереджена на захисті конкретних кінцевих пристроїв, враховуючи ризики та виклики, які виникають на рівні користувача.

Таким чином, технологія EDR є необхідним компонентом сучасних стратегій кіберзахисту, забезпечуючи ефективний та прогресивний підхід до виявлення та реагування на загрози на рівні кінцевих пристроїв [10].

EPP проти EDR проти XDR

Рішення для захисту кінцевих точок зараз зазвичай називають EPP, які являють собою набори хмарних рішень безпеки кінцевих точок, які забезпечують більш надійний захист, ніж окремі продукти безпеки кінцевих точок, такі як антивірусне ПЗ.

Оскільки загрози кібербезпеці стають все більш складними, одних лише антивірусних рішень недостатньо, щоб зупинити передові методи зловмисного ПЗ та програм-вимагачів, які більше не базуються лише на сигнатурах, а тому їх важче виявити. EPP забезпечують запобігання та захист від загроз кібербезпеці, таких як: файлове або безфайлове зловмисне ПЗ, відомі та невідомі загрози, шкідливі сценарії та загрози на основі пам’яті. Захист від поведінкових загроз та аналіз на основі ШІ за допомогою машинного навчання допомагають завчасно ідентифікувати, виявляти та зупиняти нові загрози.

EPP також можуть надавати можливість виявляти та блокувати зловмисну діяльність, а також досліджувати та виправляти будь-які інциденти, які ухиляються від контролю захисту. Це відоме як EDR. EDR постійно відстежує пристрої кінцевих користувачів, щоб виявляти та реагувати на кіберзагрози, такі як: програми-вимагачі та зловмисне ПЗ. Телеметрія кінцевої точки, зібрана EDR, дозволяє сортувати та досліджувати виявлені загрози за допомогою процесів, які є високоавтоматизованими, що дозволяє командам SOC швидко виявляти загрози та реагувати на них.

Наступна еволюція захисту кінцевих точок відома як XDR. XDR — це новітній підхід до безпеки кінцевих точок, який пропонує покращений захист, виявлення та реагування завдяки інтеграції не лише даних кінцевих точок, а й даних із будь-якого джерела, наприклад мережі, хмарних даних або даних третіх сторін. Потім усі дані аналізуються з однієї консолі, а не з різних систем, щоб краще розслідувати інциденти та зняти навантаження з операцій SOC. Бажаним результатом для ефективного рішення XDR є не тільки забезпечення надійного захисту кінцевих точок, але й уможливлення більш спрощеного підходу до реагування на інциденти та створення цілеспрямованих, високоефективних виявлень. Консолідація цих рішень допомагає краще керувати ризиками та підвищити продуктивність операцій безпеки

2.3. Компоненти та архітектура CrowdStrike

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.

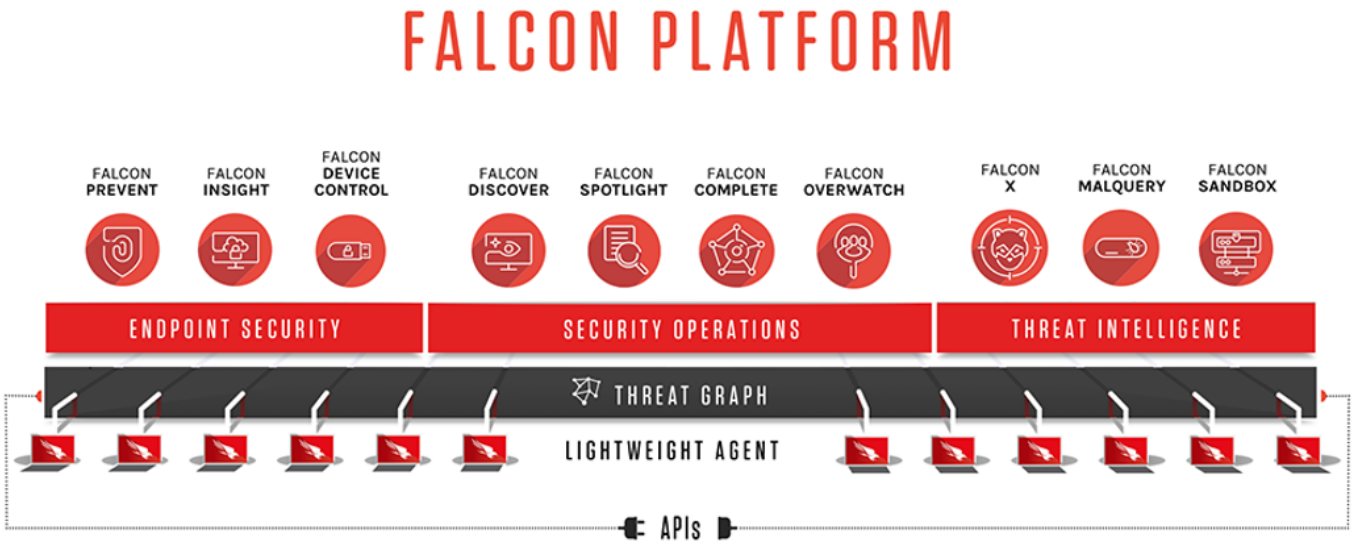

Рис. 2.2. Архітектура CrowdStrike Falcon

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 [12].

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

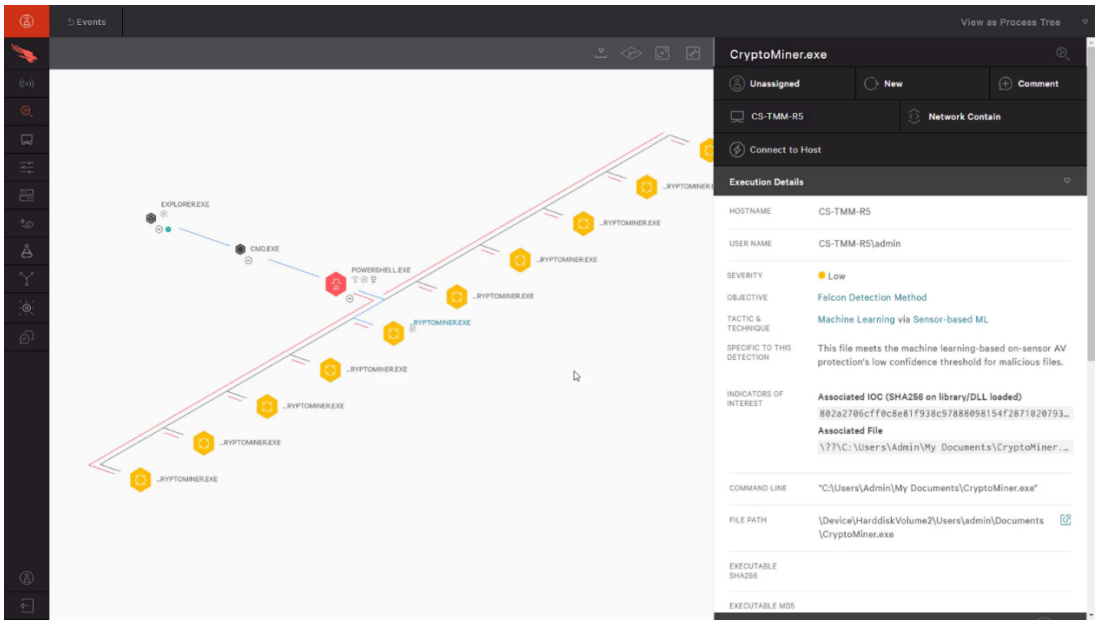

Рис. 2.3. Дослідження інциденту за допомогою CrowdStrike Falcon

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.

Можливості CrowdStrike

Виявляння

Єдиний легкий агент кінцевої точки CrowdStrike передає повну інформацію про подію на хмарну платформу в режимі реального часу. На основі цих даних про події інтерфейс користувача CrowdStrike надає інформаційну панель із миттєвим переглядом найновіших виявлень, інцидентів зловмисного програмного забезпечення за хостами та інцидентів зловмисного програмного забезпечення за користувачами. Поінформованість про найновіші події протягом 1 хвилини має вирішальне значення для вирішення завдання щодо часу [12].

Зрозуміння

Розглядаючи конкретну подію, CrowdStrike надає неперевершений контекст, включаючи повні деталі події, батьківські процеси, повні деталі командного файлу та поширеність – усе в контексті фреймворку MITRE. Цей рівень розуміння допомагає зрозуміти подію протягом 10 хвилин, щоб швидко вжити рішучих заходів щодо її усунення.

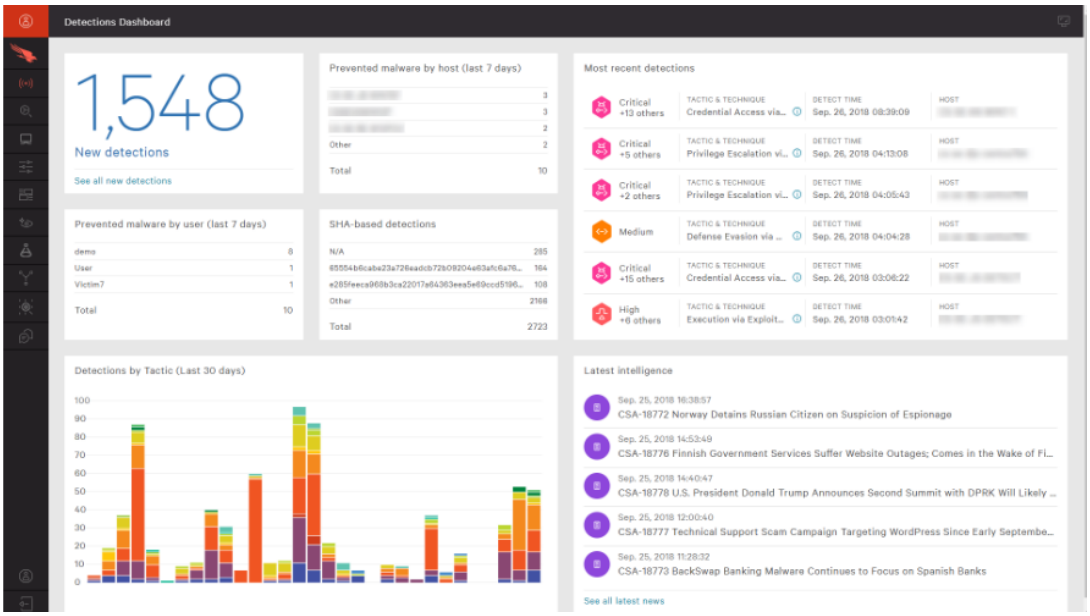

Рис. 2.4. Відображення виявлених інцидентів (Dashboard)

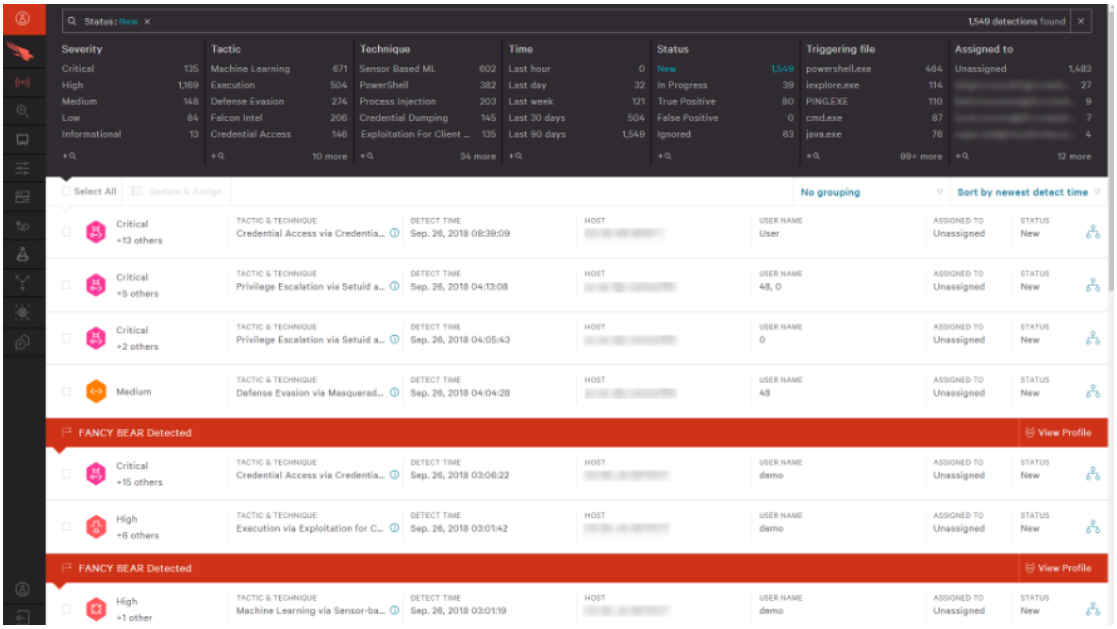

Рис. 2.5. Детальний опис кожного спрацювання

Відповідь

Falcon Insight пропонує всю інформацію та інструменти, необхідні для захисту середовища та відновлення постраждалих систем.

Мережеве обмеження допомагає гарантувати, що постраждалі системи не зможуть зв’язуватися із зовнішніми системами або ризикують переміститись в карантин.

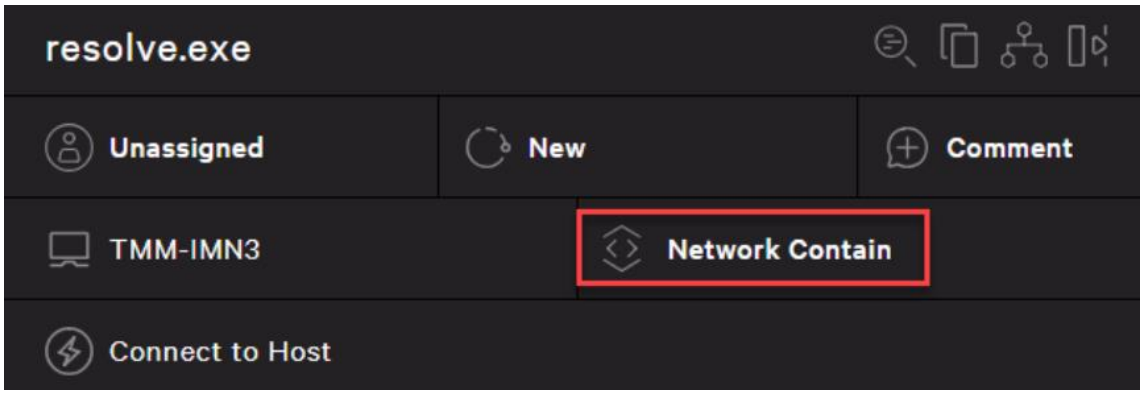

Рис. 2.6. Мережевий вміст

Реагування в реальному часі дає змогу віддалено виправляти системи за допомогою наведеної нижче команди, мінімізуючи витрати на простої і втрату продуктивності [12].

— навігація файловою системою, завантаження та видалення файлів і виконання багатьох операцій з файловою системою;

— список запущених процесів і завершення процесів;

— отримайте дампи пам'яті, журнали подій або будь-які інші файли;

— показати підключення до мережі;

— запитуйте, створюйте або змінюйте ключі реєстру.

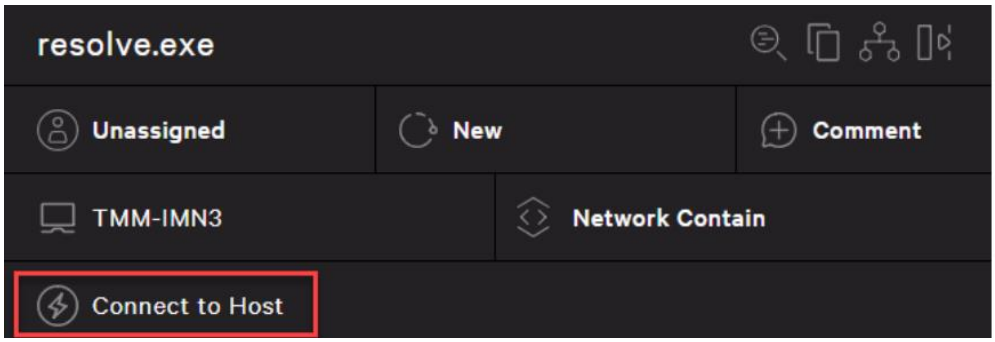

Рис. 2.7. Віддалене з’єднання

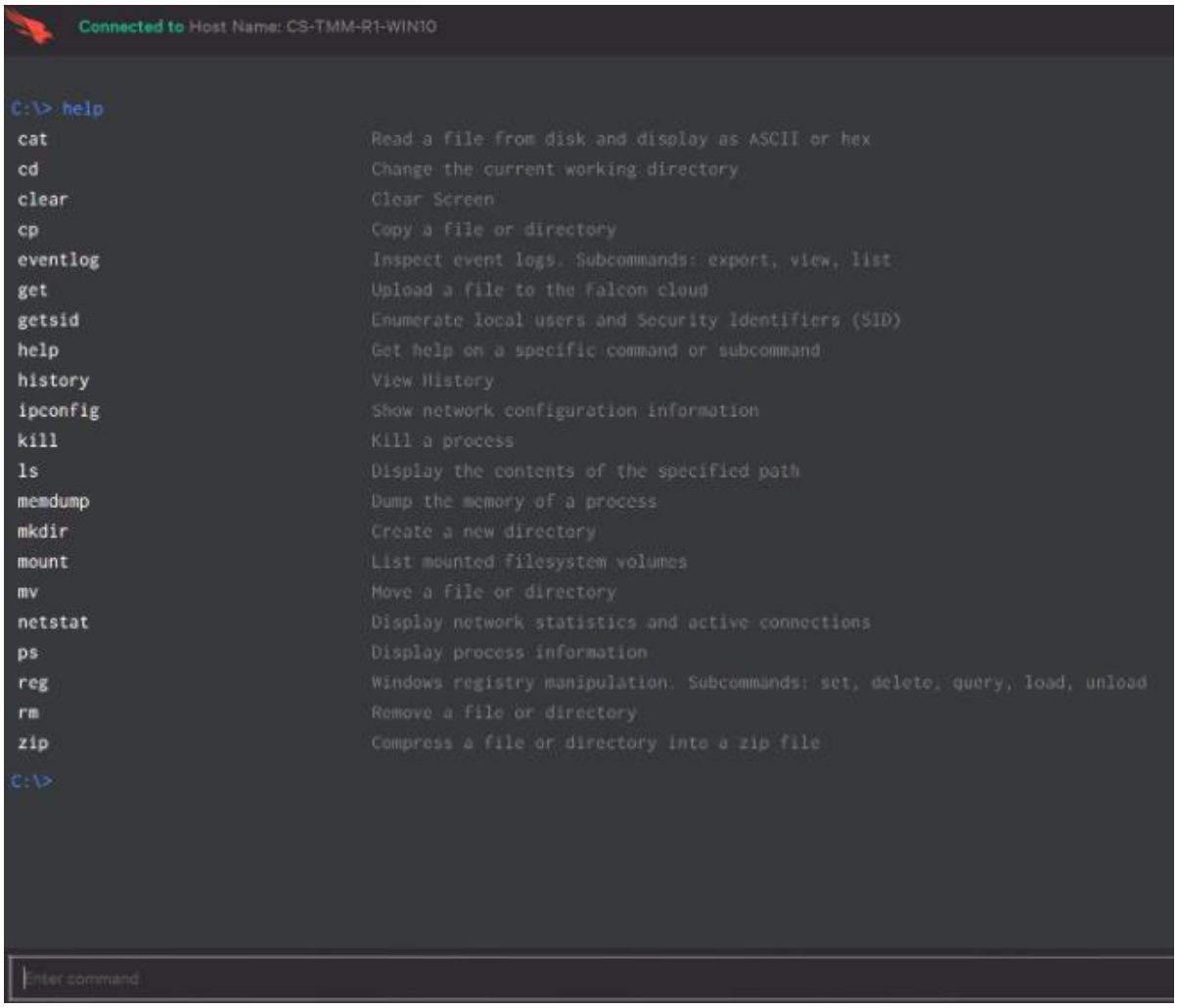

Рис. 2.8. Перелік допустимих команд віддаленого з’єднання

Falcon Insight від CrowdStrike надає фахівцям з реагування на інциденти комплексне рішення EDR, яке забезпечує їх повними і своєчасними даними. Завдяки швидкому виявленню, розумінню та усуненню інцидентів організація випереджає час прориву і запобігає перетворенню інциденту на витік інформації [12].

Висновки до розділу 2

В розділі було досліджено сучасні методи та засоби захисту кінцевих пристроїв, вибрано продукт CrowdStrike. Визначено основну роль EDR систем та приведені компоненти і архітектура CrowdStrike

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ НА ОСНОВІ EDR СИСТЕМИ

3.1. Розгортання та налаштування системи виявлення та реагування на загрози кінцевих пристроїв CrowdStrike EDR

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 отримуєте доступ до панелі керування.

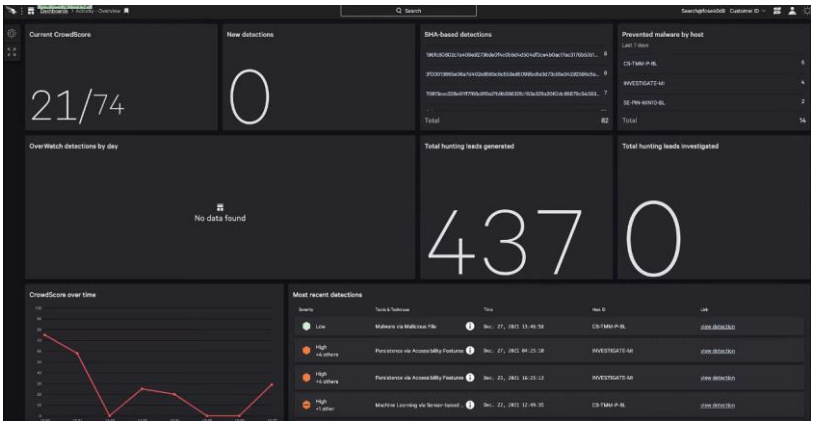

Рис. 3.1. Панель керування CrowdStrike Falcon

Для встановлення сенсору необхідно перейти до панелі керуваня пристроями.

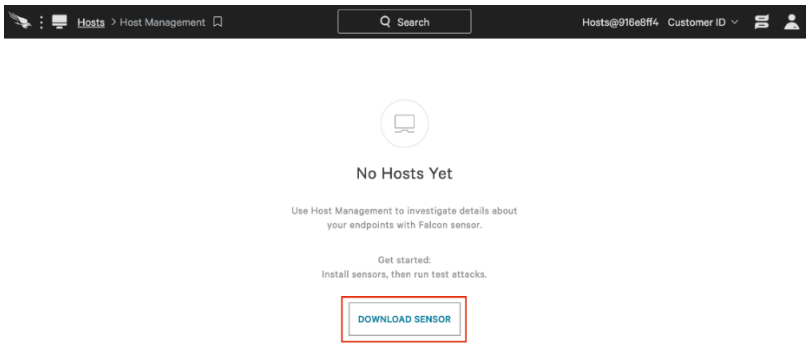

Рис. 3.2. Панель керування пристроями CrowdStrike Falcon

В даному меню обирається кінцевий пристрій на який потрібно встановити сенсор. Також необхідно скопіювати ID користувача, це знадобиться при інсталяції сенсору на кінцевий пристрій.

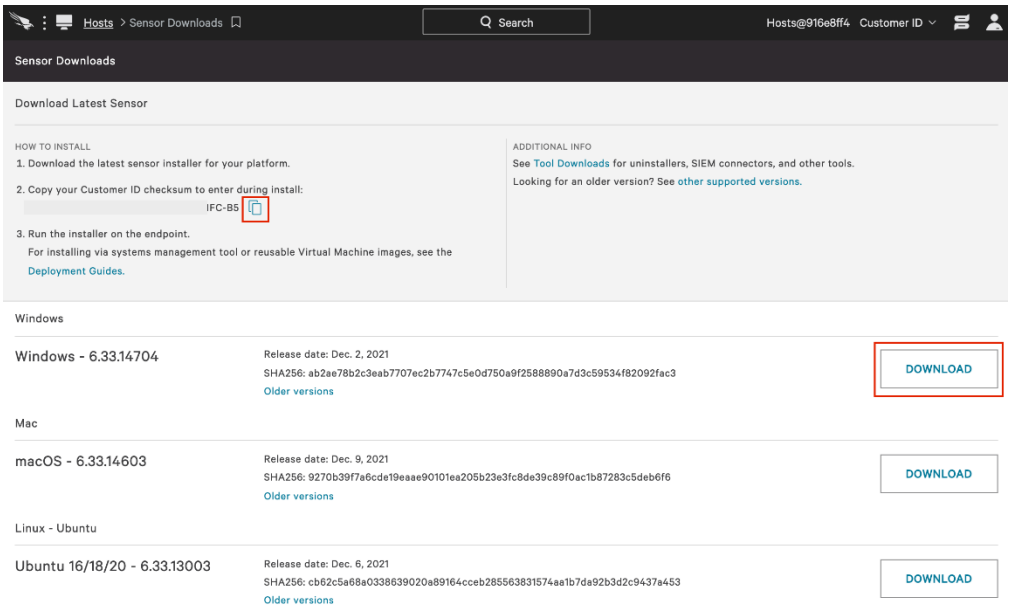

Рис. 3.3. Встановлення потрібного сенсору

Далі встановлюється 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.

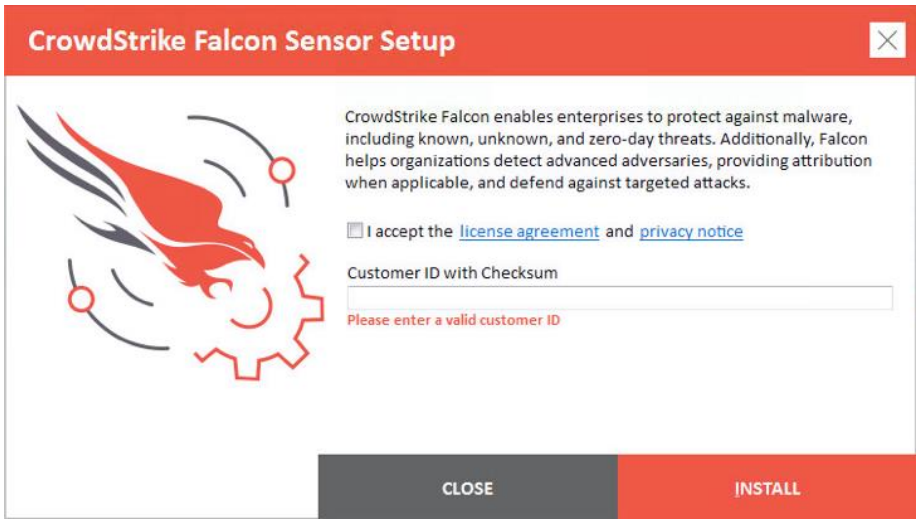

Рис. 3.4. Встановлення сенсору на кінцевий пристрій

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

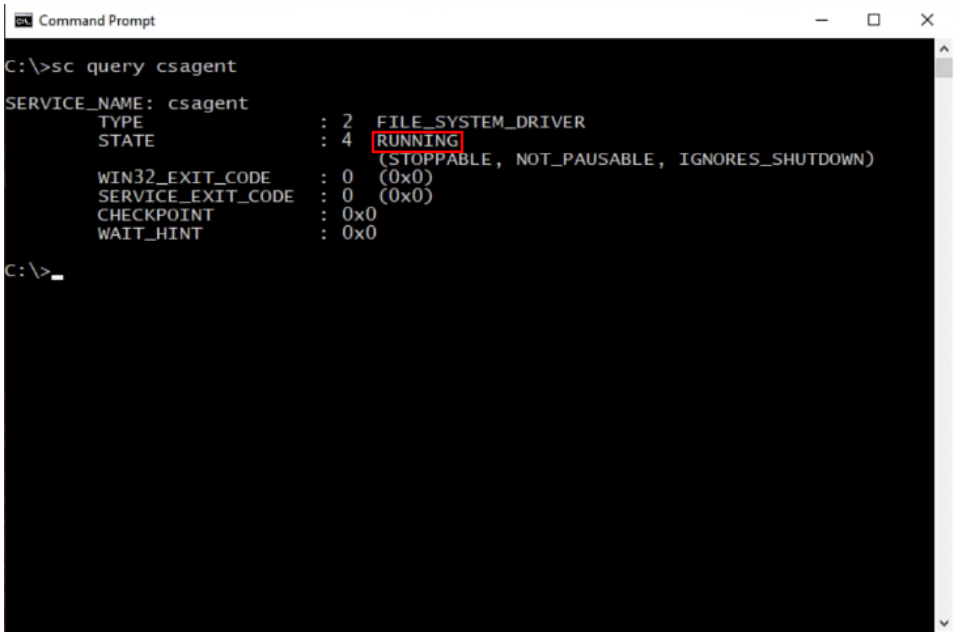

Рис. 3.5. Перевірка запущеного процесу

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

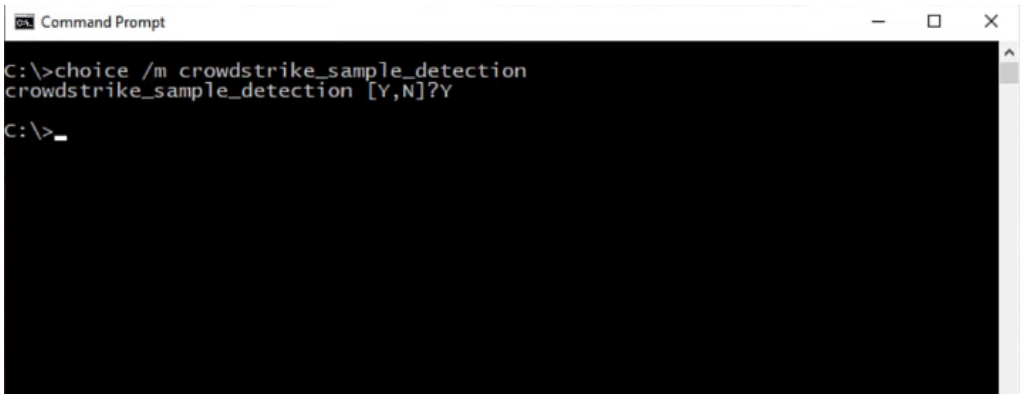

Рис. 3.6. Створення тестової загрози

На панелі керування з’являється нове сповіщення про загрозу.

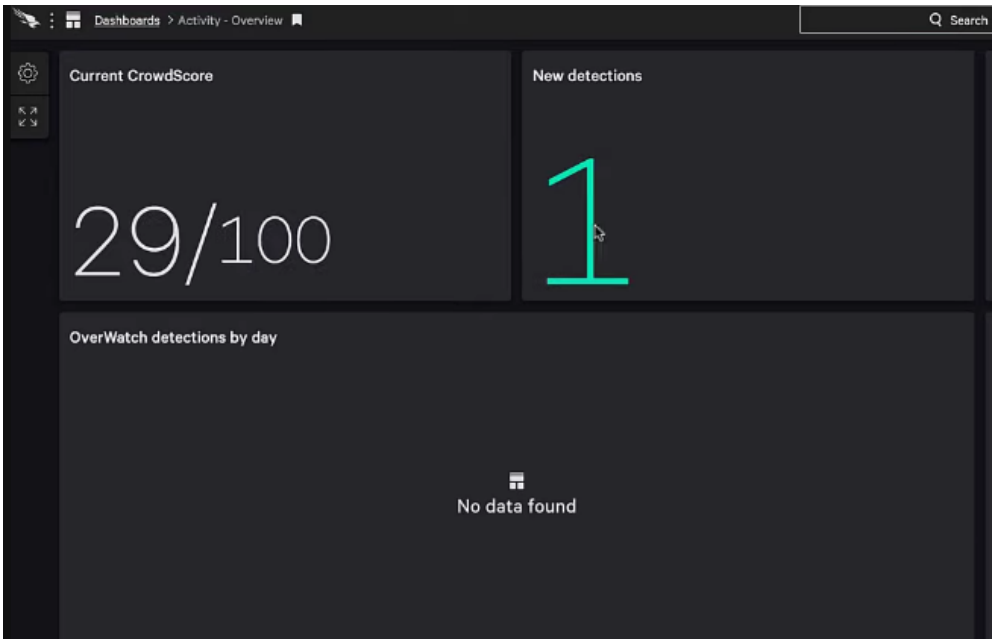

Рис. 3.7. Поява нової загрози на панелі керування

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

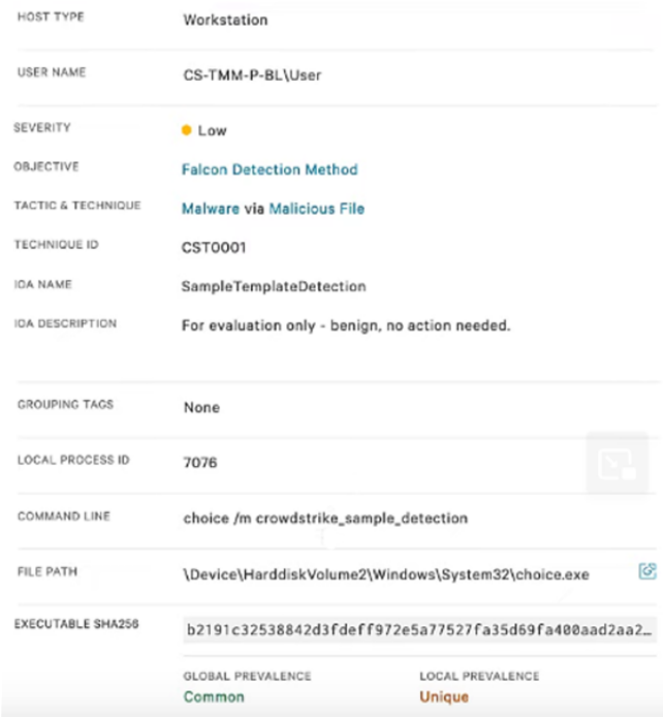

Рис. 3.8. Детальна інформація про тестову загрозу

3.2. Виявлення та реагування на загрози кінцевих пристроїв на базі рішення CrowdStrike EDR

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

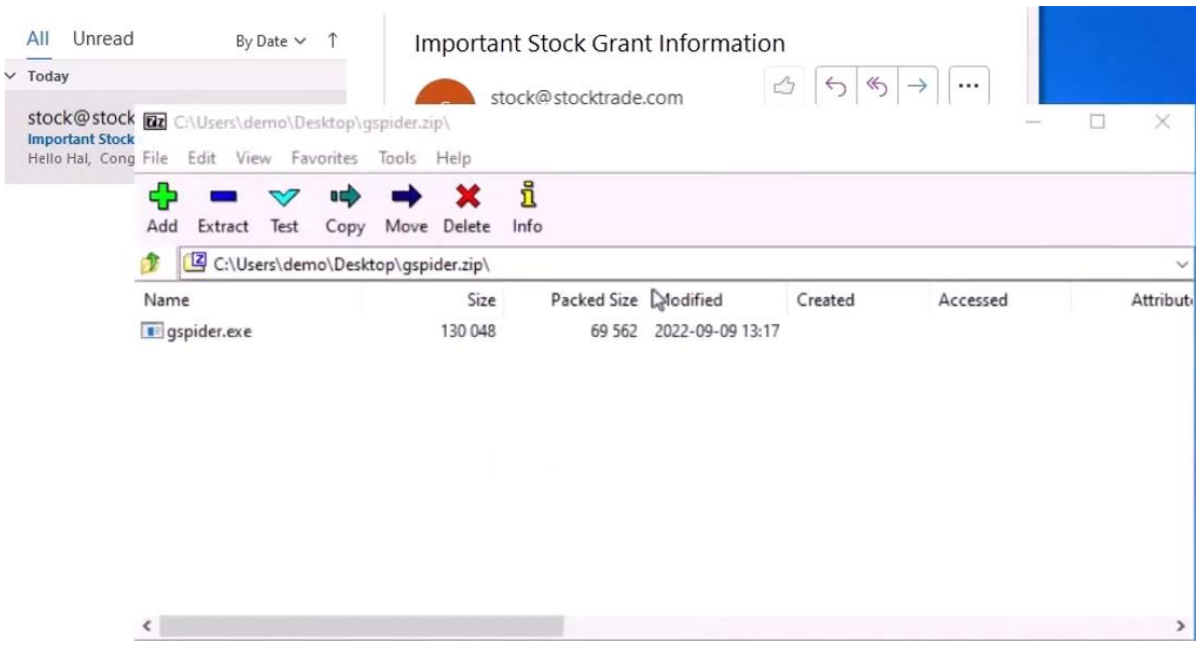

Рис. 3.9. Приклад отримання зловмисної програми в електронному листі

При спробі запустити програму виникає помилка, а також повідомлення від Falcon про те, що вайл було ізольовано.

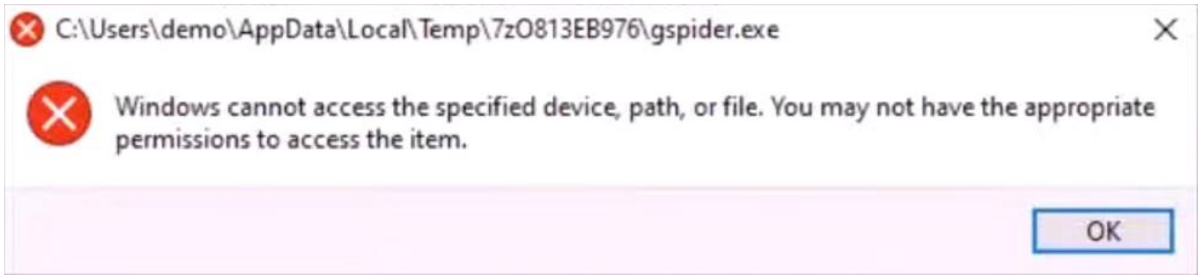

Рис. 3.10. Повідомлення про те, що шкідлива програма більше недоступна

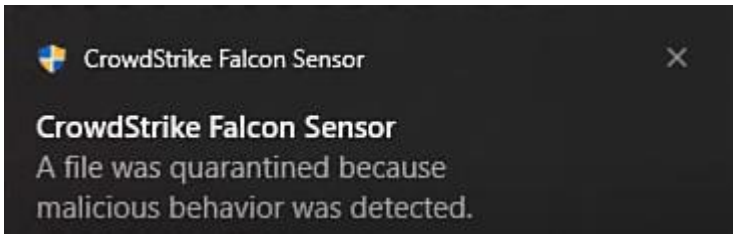

Рис. 3.11. Повідомлення від Falcon, про ізоляцію шкідливої програми

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

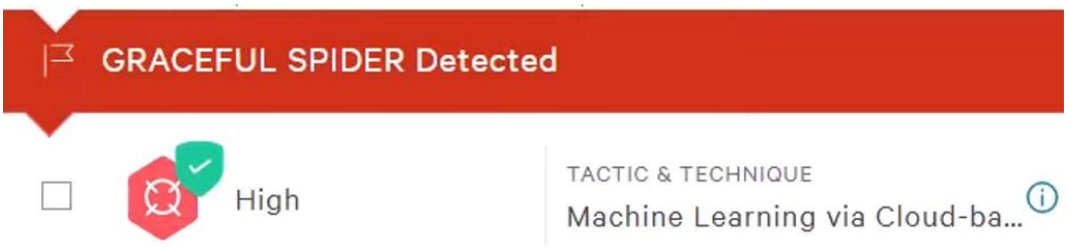

Рис. 3.12. Результати виявлення нової загрози

EDR дозволяє проаналізувати, як саме вірус чи ШПЗ потрапило на кінцевий пристрій, а саме Пошта → Архів → Вірус/ШПЗ.

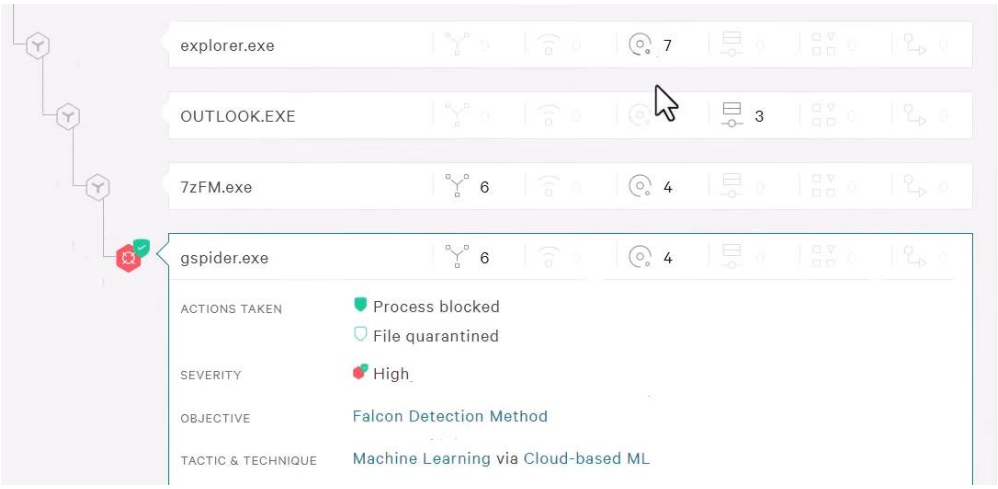

Рис. 3.13. Спосіб потрапляння вірусу на кінцевий пристрій

Також доступна більш детальна інформація про сам файл.

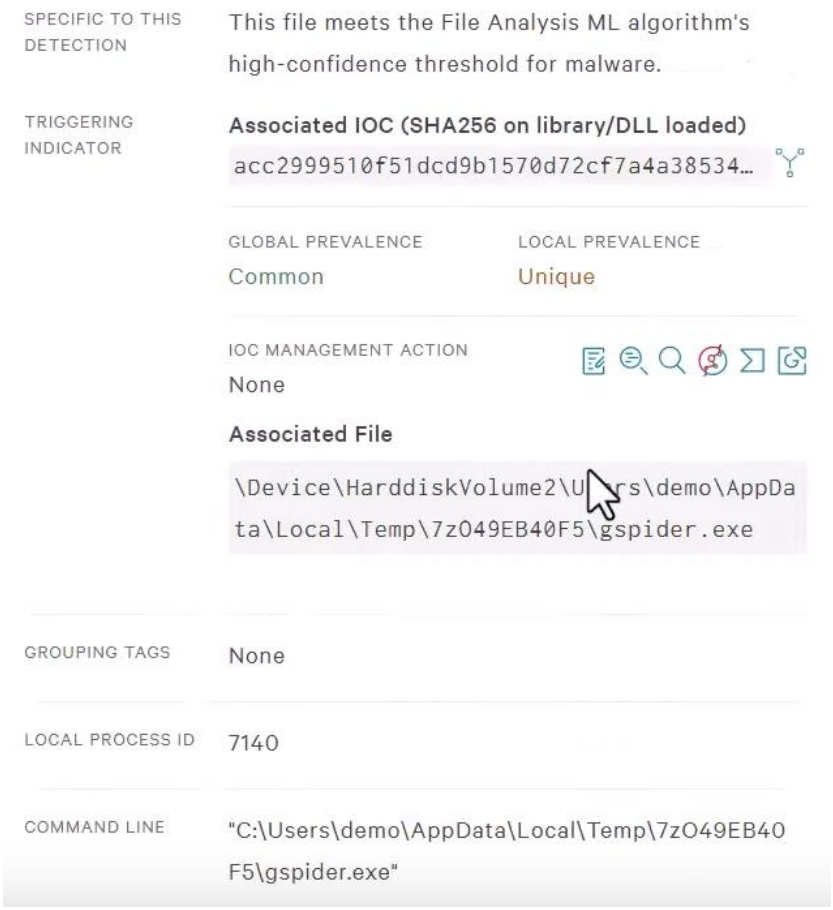

Рис. 3.14. Детальна інформація про файл

За допомогою звіту, який надає Falcon, фахівець даної галузі, що відповідає за реагування на інциденти відразу може детальніше ознайомитися з загрозою та джерелом даної загрози.

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

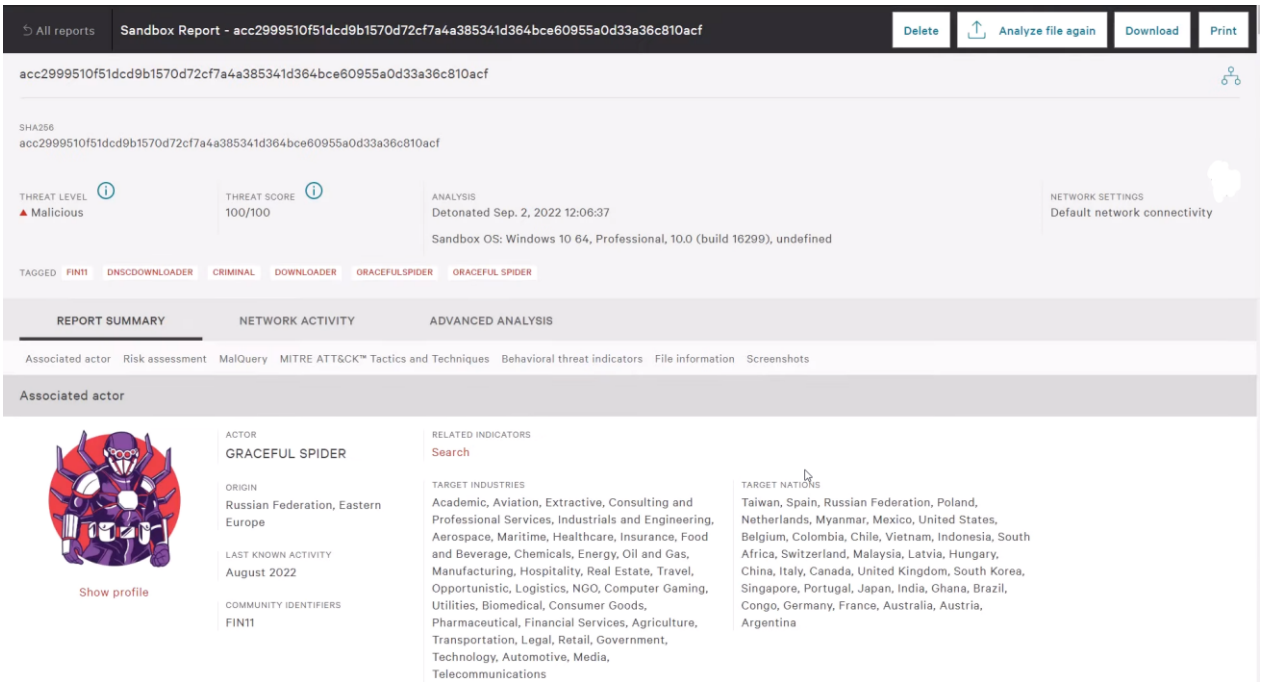

Рис. 3.15. Звіт про виявлену загрозу

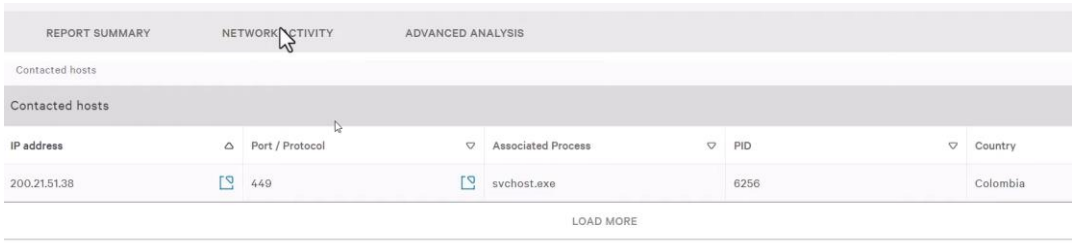

Рис. 3.16. Мережева активність загрози

Після цього налаштовується політика безпеки. Необхідно перейти в налаштування «Виявлення під час запису» та «Ізоляція під час запису» щоб аналізувати підозрілі файли під час їхнього запису на диск.

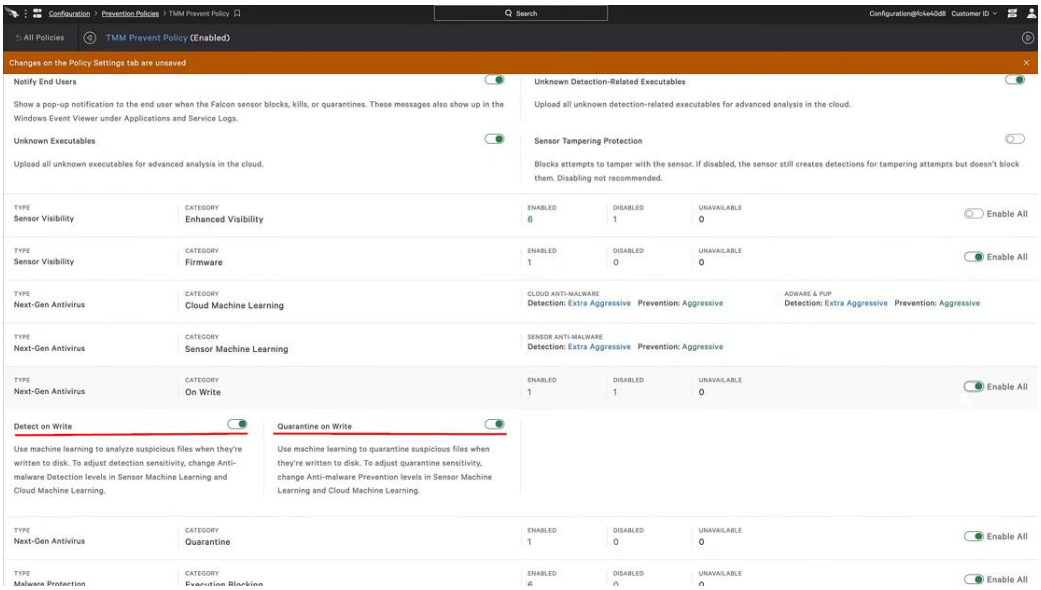

Рис. 3.17. Налаштування політики безпеки

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

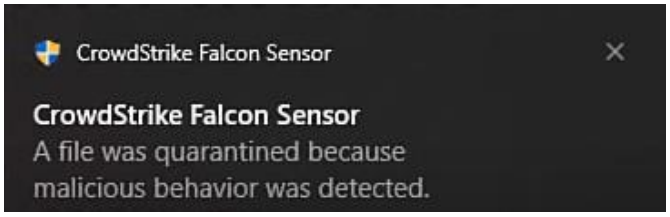

Рис. 3.18. Повідомлення від Falcon, про ізоляцію шкідливої програми

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

Рис. 3.19. Результати виявлення нової загрози

Falcon також надає корисну функцію для контролю USB пристроїв. Доступне надання різних рівнів доступу для таких пристроїв, як принтери та носії інформації.

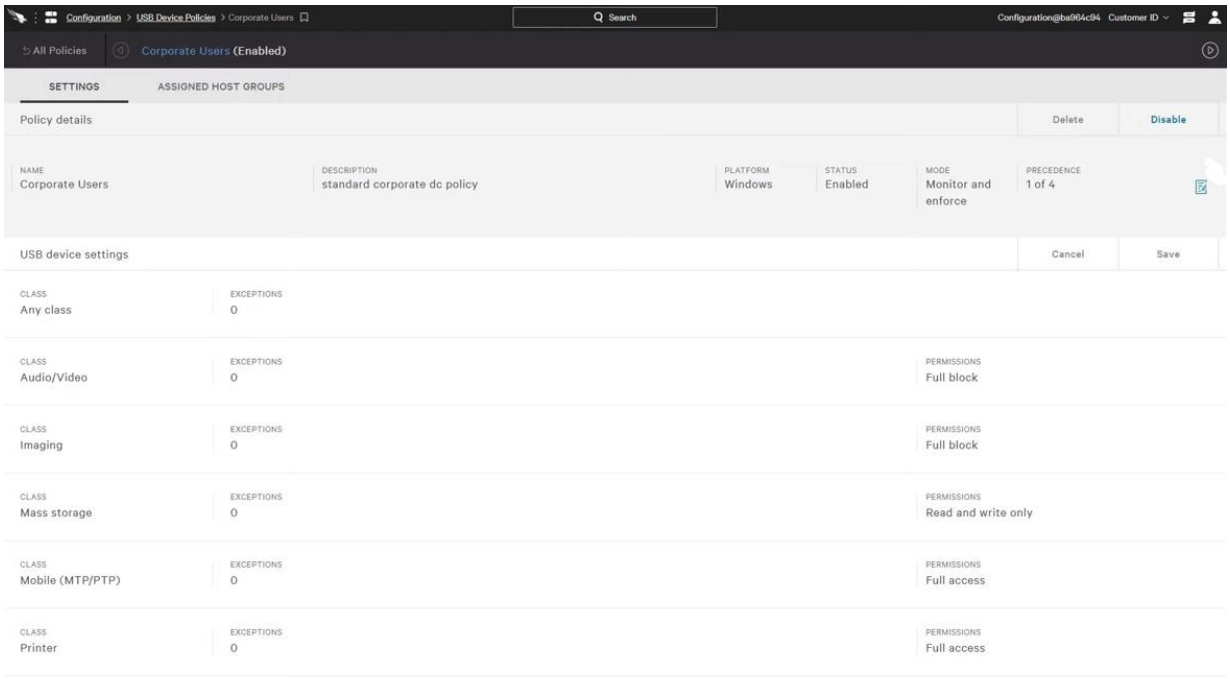

Рис. 3.20. Панель керування USB пристроями

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

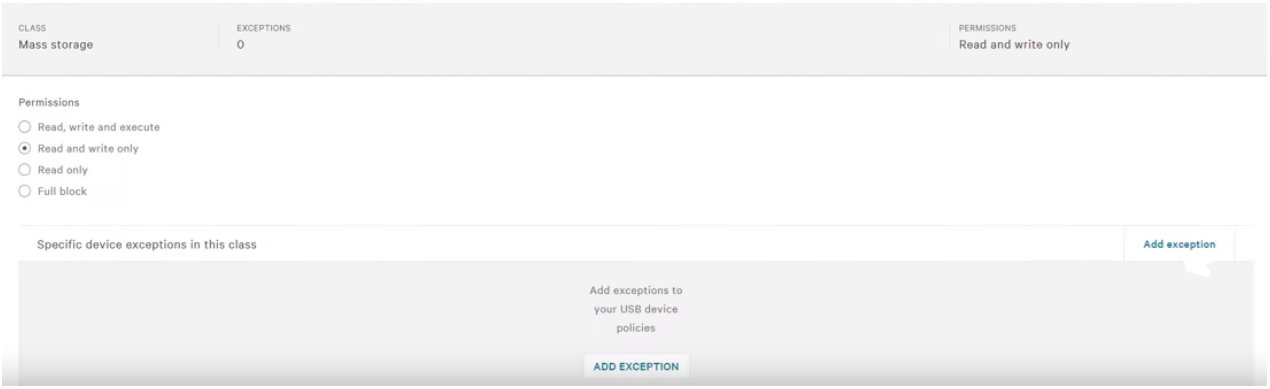

Рис. 3.21. Права доступу для користування носіями інформації

Для зручності та більш гнучкого керування додаються винятки до правил. Винятки можуть бути зроблені на основі ID пристрою або на основі виробника пристрою.

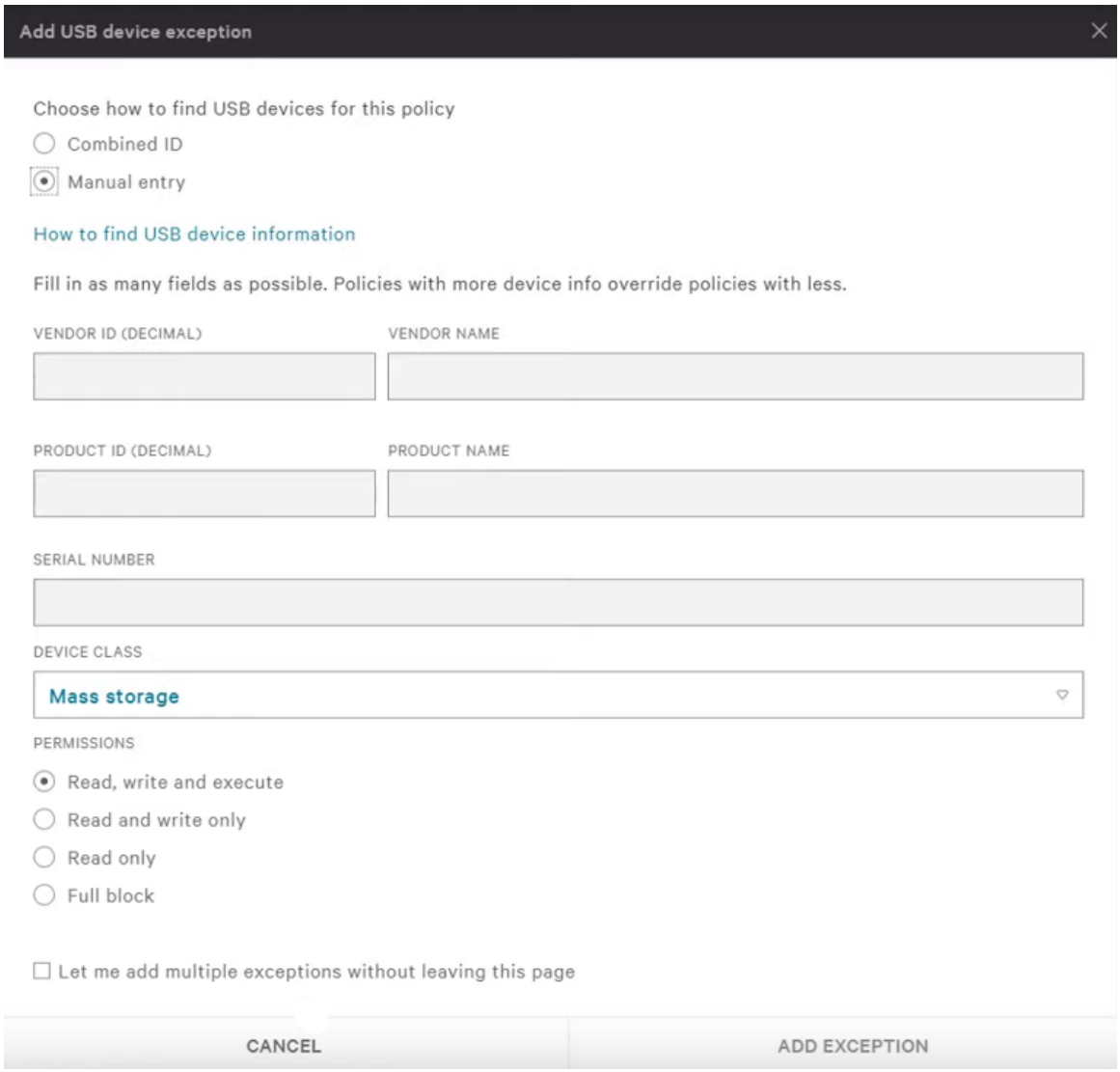

Рис. 3.22. Додавання винятку

Falcon дозволяє централізовано керувати налаштуванням фаєрвола, який встановлено на кінцевому пристрої. В панелі керування фаєрволом доступне редагування налаштування для групи пристроїв або створення нових груп пристрої. Це дуже корисно, 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.

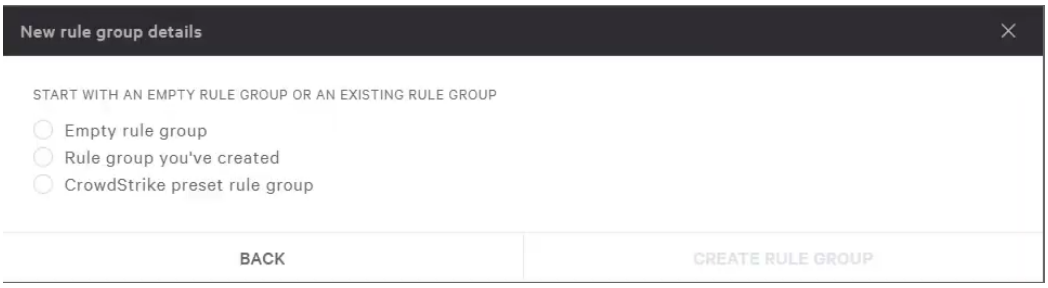

Рис. 3.23. Створення нової групи правил

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

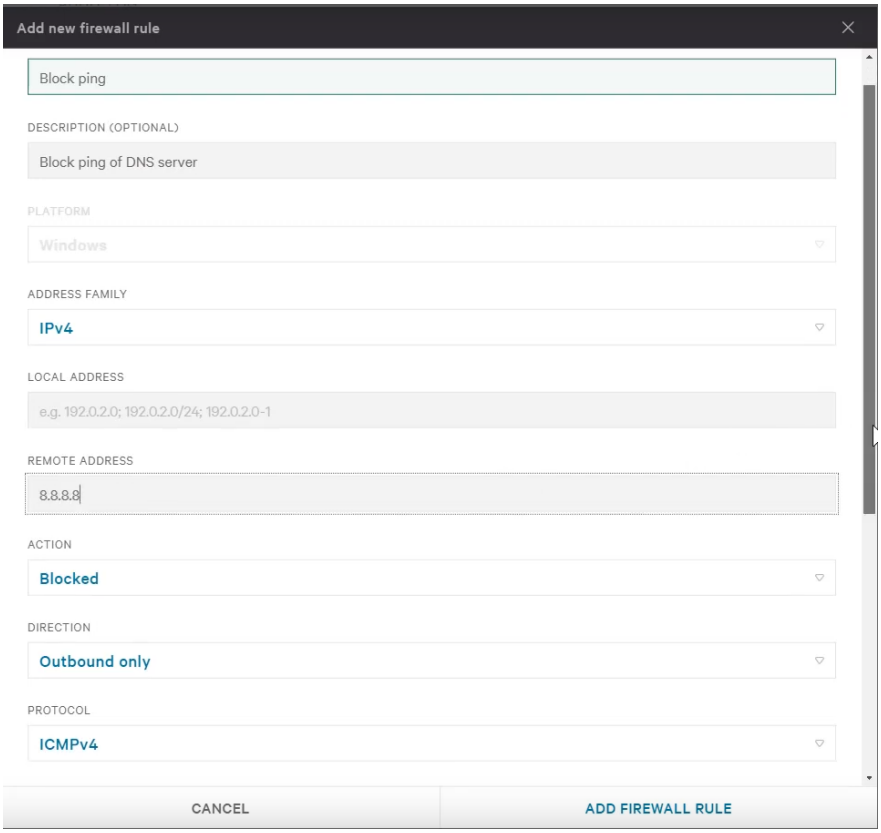

Рис. 3.24. Створення нового правила

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

Рис. 3.25. Налаштування профілю мережі

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

Рис. 3.26. Стан фаєрволу на кінцевому пристрої

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

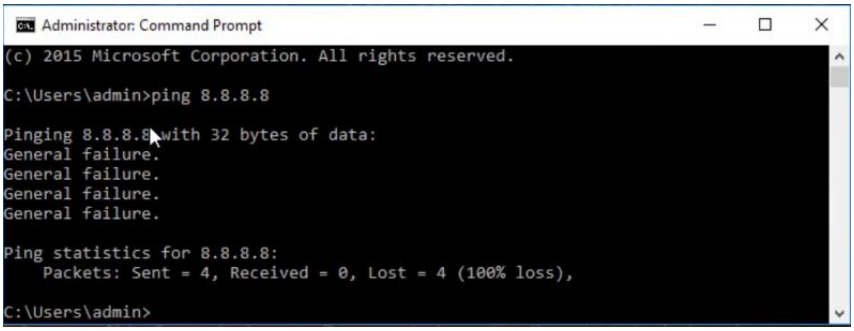

Рис. 3.27. Перевірка роботи фаєрволу

3.3. Розроблення рекомендацій щодо застосування технології виявлення та реагування на загрози кінцевих пристроїв на базі рішення CrowdStrike EDR

Впровадження технології виявлення та реагування на загрози (EDR) [13], зокрема на базі рішення CrowdStrike EDR, вимагає виваженого та систематичного підходу. Нижче подані рекомендації для ефективного використання цієї технології в організації:

1. Аналіз Інфраструктури та Оцінка Ризиків: Перед впровадженням CrowdStrike EDR провести аналіз існуючої інфраструктури та визначити основні ризики безпеки. Звертати увагу на критичні компоненти та додатки, щоб налаштувати EDR з урахуванням особливостей мережі.

2. Налаштування та Конфігурація: Відповідно до визначених ризиків та потреб безпеки, налаштуйте CrowdStrike EDR для виявлення конкретних загроз та адаптуйте його до ваших потреб.

3. Інтеграція із Іншими Засобами Захисту: Забезпечте інтеграцію CrowdStrike EDR з іншими засобами кіберзахисту, такими як антивірусне програмне забезпечення, файерволи та системи виявлення вторгнень, для створення комплексної системи захисту.

4. Оптимізація Виявлення та Відгуку: Використовуйте настроювання CrowdStrike EDR для оптимізації виявлення загроз та мінімізації хибно-позитивних спрацьовувань, щоб прискорити відгук на реальні загрози.

5. Автоматизація Реагування: Використовуйте можливості автоматизації CrowdStrike EDR для миттєвого реагування на інциденти та автоматичної ізоляції компрометованих пристроїв, щоб зменшити час реакції на атаки.

6. Моніторинг та Звітність: Активно використовуйте функції моніторингу та звітності CrowdStrike EDR для слідкування за подіями та вираження звітності про ефективність системи. Це допоможе у виявленні та усуненні можливих слабкостей.

7. Організація Навчань та Семінарів: Проводьте навчання та семінари для персоналу щодо ефективного використання CrowdStrike EDR. Навчіть персонал розпізнавати та відповідати на попереджувальні сигнали системи.

8. Створення Плану Реагування на Інциденти: Розробіть детальний план реагування на інциденти, включаючи ролі та відповідальності персоналу. Перевірте та практикуйте цей план регулярно.

9. Забезпечення Постійного Моніторингу та Оновлення: Проводьте постійний моніторинг ефективності CrowdStrike EDR та систем безпеки вцілому. Вчасно оновлюйте програмне забезпечення та вірусні бази даних.

10. Здійснення Резервного Копіювання та Відновлення: Розгляньте можливості для регулярного здійснення резервного копіювання та відновлення системи, щоб забезпечити можливість відновлення в разі успішного вторгнення чи іншого інциденту.

Висновки до розділу 3

В розділі було розгорнуто та налаштовано систему виявлення та реагування на загрози кінцевих пристрої. Проведено дослідження на виявлення та реагування на дані загрози, а також розроблено рекомендації щодо застосування технології виявлення та реагування на загрози кінцевих пристроїв на базі рішення CrowdStrike EDR. Впровадження CrowdStrike EDR в стратегію кіберзахисту має за мету не лише покращити виявлення та відгук на загрози, але і забезпечити комплексний та ефективний захист кінцевих пристроїв у вашій організації.

ВИСНОВКИ

CrowdStrike повністю автоматизує процес аналізу, інтегрує дані про загрози та надає розвідувальну інформацію, яка може бути використана для прийняття рішень. Вона забезпечує більш широкий контекст, що дозволяє аналітикам з безпеки працювати швидше і ефективніше, оскільки вони вчаться на прикладах атак і прагнуть захистити більшу організацію.

В розділі 1 проаналізовано проблеми захисту кінцевих пристроїв, приведено та здійснено аналіз загроз кінцевих пристроїв, а також технологій захисту кінцевих пристроїв.

В розділі 2 було досліджено сучасні методи та засоби захисту кінцевих пристроїв, вибрано продукт CrowdStrike. Визначено основну роль EDR систем та приведені компоненти і архітектура CrowdStrike

В розділі 3 було розгорнуто та налаштовано систему виявлення та реагування на загрози кінцевих пристрої. Проведено дослідження на виявлення та реагування на дані загрози, а також розроблено рекомендації щодо застосування технології виявлення та реагування на загрози кінцевих пристроїв на базі рішення CrowdStrike EDR.

Впровадження CrowdStrike EDR в стратегію кіберзахисту має за мету не лише покращити виявлення та відгук на загрози, але і забезпечити комплексний та ефективний захист кінцевих пристроїв у вашій організації

ПЕРЕЛІК ПОСИЛАНЬ

1. Бутенко А. С. Захист кінцевих пристроїв на основі EDR системи. Актуальні проблеми кібербезпеки : Всеукр. науково-практ. конф., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 49–51.

2. What Is Endpoint Security? How It Works & Its Importance | Trellix. Trellix | Revolutionary Threat Detection and Response. URL: https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-security/ (дата звернення: 10.10.2023).

3. Що таке кінцева точка?. microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-an-endpoint (дата звернення: 10.10.2023).

4. What is an Endpoint?. Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint#:~:text=An%20endpoint%20is%20a%20remote,Smartphones (дата звернення: 11.10.2023).

5. Galvin K. 7 best practices for endpoint security. The Quest Blog. URL: https://blog.quest.com/7-best-practices-for-endpoint-security/ (дата звернення: 13.10.2023).

6. What is Bring Your Own Device (BYOD)? | IBM. IBM in Deutschland, Österreich und der Schweiz | IBM. URL: https://www.ibm.com/topics/byod (дата звернення: 30.10.2023).

7. EDR vs EPP: Key Features, Differences, and How They Work Together. Perception Point. URL: https://perception-point.io/guides/endpoint-security/edr-vs-epp-key-features-differences-using-them-together/ (дата звернення: 01.11.2023).

8. Mellen A. Forrester Reprint. Forrester Reprint. URL: https://reprints2.forrester.com/#/assets/2/482/RES176332/report (дата звернення: 02.11.2023).

9. Fortinet was named a Visionary in the 2022 Gartner® Magic Quadrant™ for EPP. Fortinet. URL: https://www.fortinet.com/solutions/gartner-mq-endpoint-protection (дата звернення: 02.11.2023).

10. Welcome to CrowdStrike FalconÂ®. crowdstrike.com. URL: https://www.crowdstrike.com/blog/tech-center/welcome-to-crowdstrike-falcon/ (дата звернення: 15.11.2023).

11. How to Contain an Incident to Avoid a Breakout and Prevent a Breach. crowdstrike.com. URL: https://www.crowdstrike.com/blog/tech-center/contain_incident_breakout_time/ (дата звернення: 16.11.2023).

12. How to automate workflows with Falcon Fusion and Real Time Response. crowdstrike.com. URL: https://www.crowdstrike.com/blog/tech-center/falcon-fusion-and-real-time-response/ (дата звернення: 18.11.2023).

13. Falcon LogScale and Mimecast Integration: Mitigate Email Threats. crowdstrike.com. URL: https://www.crowdstrike.com/blog/tech-center/mitigate-cyber-risk-from-email-with-the-falcon-logscale-and-mimecast-integration/ (дата звернення: 20.11.2023).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)