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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Засоби захисту кінцевих точок організації від атак типу ransomware»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Володимир ДІДКОВСЬКИЙ
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
ДІДКОВСЬКИЙ Володимир
(прізвище, ім'я)

Керівник Ст. Викладач Сич М.В.
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

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

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___” _____ 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дідковському Володимиру Максимовичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи:
Засоби захисту кінцевих точок організації від атак типу ransomware

керівник кваліфікаційної роботи Сич М.В. ст. викладач
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 06.06.2024 р.

3. Вихідні дані до кваліфікаційної роботи
аналіз науково-технічної літератури і нормативних документів;
порівняльний аналіз засобів захисту;
наукова та технічна література, експлуатаційна документація, нормативні
експертна оцінка, імітаційне моделювання кібератаки та практичне сценарне тестування засобів захисту (на прикладі CrowdStrike).

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Вивчення природи атак типу ransomware, їх вплив на інформаційну безпеку організацій та основні вектори проникнення.
2. Аналіз існуючих підходів та засобів захисту кінцевих точок від програм-вимагачів, виявлення їх недоліків і переваг.
3. Дослідження архітектури, функції та механізмів захисту платформи

CrowdStrike Falcon як сучасного рішення для захисту кінцевих точок.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Проведеня імітаційного сценарію атаки та реагування за допомогою CrowdStrike або розглядання реальних кейсі впровадження.

7. Розробка рекомендацій для фахівців з кібербезпеки щодо впровадження та використання засобів захисту кінцевих точок (на прикладі CrowdStrike) для протидії ransomware.

6. Дата видачі завдання 28.02.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Збір інформації, аналіз літературних джерел та нормативних рекомендацій (NIST, CISA, Gartner) з тематики ransomware та захисту кінцевих точок.	18.05.2025 р.	
2.	Дослідження платформи CrowdStrike Falcon, вивчення технічної документації та звітів про ефективність..	20.05.2025 р	
3.	Підготовка імітаційного сценарію атаки та опрацювання практичних аспектів застосування CrowdStrike; формування рекомендацій.	25.05.2025 р	
4.	Оформлення роботи, підготовка реферату, презентації, рецензування та доопрацювання.	04.06.2025 р	
5.	Розроблення рекомендацій щодо застосування методів та засобів захисту кінцевих точок організації.	05.05.2025 р	
6.	Оформлення результатів дослідження.	05.05.2025 р	
7.	Остаточне редагування, подання роботи до захисту.	06.06.2025 р.	

Здобувач вищої освіти _____ Володимир ДІДКОВСЬКИЙ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Микола СИЧ
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Бакалаврська кваліфікаційна робота: 45 стор., 3 розд., 12 джерел.

Ключові слова: кібербезпека, програма-вимагач, ransomware, кінцева точка, EDR, CrowdStrike, Falcon, захист інформації, поведінковий аналіз, антивірус.

Об'єкт дослідження – процеси та засоби забезпечення кібербезпеки кінцевих точок підприємства.

Предмет дослідження – технології виявлення та запобігання атакам типу ransomware на кінцевих пристроях організації, зокрема можливості платформи CrowdStrike Falcon.

Мета роботи проаналізувати сучасні методи захисту кінцевих точок від атак програм-вимагачів та дослідити можливості платформи CrowdStrike як прикладового рішення для протидії ransomware-атакам.

Методи дослідження – аналіз науково-технічної літератури і нормативних документів, порівняльний аналіз засобів захисту, експертна оцінка, імітаційне моделювання кібератаки та практичне сценарне тестування засобів захисту (на прикладі CrowdStrike).

Роботу присвячено дослідженню засобів захисту кінцевих точок організації від атак типу ransomware (програм-вимагачів) з акцентом на сучасному хмарному рішенні CrowdStrike Falcon. У роботі проаналізовано актуальність проблеми — зростання кількості атак ransomware, значні фінансові та репутаційні втрати від них для організацій усіх галузей. Розглянуто типову тактику дій зловмисників (ланцюг атаки), основні вектори проникнення (фішингові розсилки, уразливі RDP-сервіси, експлойти тощо) та труднощі захисту кінцевих пристроїв у сучасному корпоративному середовищі.

В рамках дослідження проведено огляд традиційних та новітніх підходів до захисту кінцевих точок: від класичних антивірусів до засобів EDR (Endpoint Detection and Response). Особливу увагу приділено платформі CrowdStrike Falcon як одному з провідних представників EDR-рішень на ринку. Детально описано її архітектуру (легкий агент на пристрої + потужна аналітика в хмарі CrowdStrike), основні функції (машинне навчання для детектування загроз, Indicators of Attack для поведінкового аналізу, база загроз Threat Graph, модуль проактивного полювання OverWatch тощо) та механізми захисту від програм-вимагачів. Наведено результати незалежних тестувань, що підтверджують 100% ефективність CrowdStrike Falcon у виявленні та зупинці ransomware.

Практична частина роботи демонструє застосування CrowdStrike Falcon на прикладі імітованої атаки програмою-вимагачем: проілюстровано, як рішення в реальному часі виявляє підозрілі дії, блокує шкідливий скрипт, ізолює заражену кінцеву точку та повідомляє фахівців, запобігаючи розвитку інциденту. На основі проведеного аналізу сформовано рекомендації для підприємств щодо посилення

захисту від ransomware: впровадження сучасних EDR-рішень, регулярне резервне копіювання даних, навчання персоналу кібергігієні, проведення тренувань (tabletop-ігор) та постійний моніторинг активності.

Результати роботи впроваджено у вигляді методичних рекомендацій для IT-відділу умовного підприємства щодо реагування на атаки програм-вимагачів (додаток: презентація з основними висновками). Отримані результати можуть бути використані фахівцями з кібербезпеки при виборі та розгортанні засобів захисту кінцевих точок, а також при розробці політик інформаційної безпеки, спрямованих на протидію ransomware.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ, КІНЦЕВІ ТОЧКИ, ЗАХИСТ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

ЗМІСТ

ВСТУП

Актуальність дослідження. Атаки типу *ransomware* (програми-вимагачі) набули масштабів епідемії у сфері кібербезпеки останніх років. Зловмисники застосовують ransomware для шифрування даних організацій з наступним вимаганням викупу, часто поєднуючи шифрування з крадіжкою даних і загрозою їх оприлюднення (тактика «подвійного вимагання» або *double extortion*). Частота та масштаб таких атак стрімко зростають: лише у 2023 році на програми-вимагачі припадало близько 24% всіх кіберінцидентів, а загальна сума виплат зловмисникам перевищила 1 млрд доларів США, встановивши новий трагічний рекорд. Від атак не застрахований жоден сектор – постраждали як малі фірми, так і корпорації, державні установи, лікарні та заклади освіти. Більше того, такі інциденти завдають організаціям колосальних збитків: шифрування критичних даних паралізує бізнес-процеси, призводить до простою сервісів, втрати довіри клієнтів. Економічні та репутаційні втрати від ransomware-атак обчислюються мільйонами, а відновлення після них є складним і тривалим процесом. Це робить проблему захисту від програм-вимагачів надзвичайно актуальною і пріоритетною для служб кібербезпеки.

Кінцеві точки (робочі станції, ноутбуки, сервери) – одні з основних цілей атак ransomware, адже саме на них зберігаються важливі дані та виконуються бізнес-задачі. Сучасне робоче середовище (тренди віддаленої роботи, розширення мережі за рахунок мобільних та IoT-пристроїв) призводить до збільшення кількості кінцевих пристроїв і, відповідно, розширення поверхні атаки для зловмисників. Більшість інцидентів ransomware починаються з компрометації саме кінцевої точки – наприклад, відкриття співробітником фішингового електронного листа з шкідливим вкладенням або використання викрадених облікових даних для доступу до віддаленого робочого столу (RDP). Серед типових векторів початкового проникнення програм-вимагачів фахівці відзначають: фішингові розсилки (доставка шкідливих документів чи посилань), атаки через відкриті вразливі служби (RDP, VPN) при недостатньому захисті паролем або відсутності MFA,

експлуатацію вразливостей у програмному забезпеченні, використання вже наявного “малваре-присутності” (так званого «precursor malware») в мережі. За даними рекомендацій CISA, зловмисники часто отримують початковий доступ через незахищені зовнішні служби (наприклад, RDP), після чого розвивають атаку всередині мережі, використовуючи вбудовані засоби Windows та інші методи “living off the land”. Не менш поширеним є і шлях через компрометацію облікових даних (викрадені або підібрані паролі), а також через фішинг – відкриття шкідливого вкладення нічого не підозрюючим користувачем. Потрапивши на кінцевий пристрій, сучасні зразки ransomware діють блискавично: протягом лічених хвилин вони можуть поширитися мережею, знайти та зашифрувати цінні файли, видалити резервні копії та затерти сліди. Середній час від початкового проникнення до повного шифрування значної частини мережі часто вимірюється годинами, а інколи й менше. Тому швидкість виявлення та реагування на атаки програм-вимагачів є критичною – запізнення навіть на кілька хвилин може означати, що шкоду завдано.

Традиційні підходи до захисту кінцевих точок – такі як класичні антивірусні програми, що покладаються на бази відомих сигнатур – на жаль, часто виявляються недостатніми перед обличчям сучасних *“zero-day”* загроз та майстерності кіберзлочинців. Програми-вимагачі постійно мутують, шифрувальники швидко змінюють сигнатури, використовують поліморфізм, впроваджують функції обходу захисту (відключення антивірусу, видалення тіньових копій тощо). Якщо антивірус не впізнає новий зразок за сигнатурою – кінцева точка буде скомпрометована. Окрім того, усе більшого поширення набувають безфайлові атаки (*fileless malware*), коли зловмисний код виконується в пам’яті або через скрипти (наприклад, PowerShell) без збереження файлів на диску – такі дії ще складніше виявити сигнатурними методами. За цих умов індустрія кібербезпеки перейшла до концепції *“Endpoint Detection and Response” (EDR)* – комплексних рішень для моніторингу кінцевих точок у реальному часі, виявлення підозрілої поведінки та швидкого реагування на інциденти. Важливість впровадження EDR та інших проактивних засобів відзначається в офіційних рекомендаціях. Зокрема,

керівництво #StopRansomware від CISA радить використовувати централізовані антивірусні рішення з автоматичним оновленням та функціями виявлення як відомих шкідливих програм, так і ознак атаки, а також застосовувати білі списки додатків та/або EDR на всіх пристроях для блокування неавторизованого ПЗ. NIST у своєму проекті профілю кібербезпеки для захисту від ransomware (NIST IR 8374) підкреслює, що жодна організація не застрахована від атак і потрібно заздалегідь оцінити свою готовність, впровадити засоби моніторингу, виявлення, реагування та відновлення. Таким чином, науково-технічне завдання забезпечення надійного захисту кінцевих точок від програм-вимагачів є надзвичайно актуальним та практично значущим в галузі кібербезпеки.

Об'єкт дослідження – захист кінцевих точок від атак типу ransomware.

Мета роботи Метою даної роботи є дослідження сучасних засобів захисту кінцевих точок організації від атак типу ransomware та розробка рекомендацій щодо їх ефективного використання на прикладі платформи CrowdStrike Falcon. Для досягнення поставленої мети необхідно вирішити такі завдання: провести аналіз природи атак програм-вимагачів та проблем захисту кінцевих точок; дослідити існуючі технології та інструменти захисту (традиційні та новітні); здійснити огляд архітектури та функціональних можливостей рішення CrowdStrike Falcon як одного з лідерів ринку; проаналізувати механізми протидії ransomware в рамках цього рішення; змоделювати сценарій атаки і показати роботу засобу захисту на практиці; сформулювати практичні рекомендації для фахівців з кібербезпеки.

розробити рекомендацій щодо застосування методів та засобів захисту кінцевих точок організації.

Методи дослідження – При виконанні роботи використовувалися такі методи: аналіз та узагальнення інформації з наукових статей, стандартів і керівництв (в частині загальної характеристики загроз ransomware та підходів до захисту); порівняльний аналіз функцій і можливостей різних засобів захисту кінцевих точок на основі огляду літератури та аналітичних звітів (зокрема звітів Gartner Magic Quadrant, незалежних тестувань тощо); інструментальний аналіз технічної документації CrowdStrike Falcon (офіційні білі книги, звіти SE Labs, тощо) для вивчення її архітектури та механізмів; метод сценарного моделювання – для опису дій системи захисту при реалізації атаки; а також елементи експертного

підходу при формулюванні рекомендацій (враховано найкращі практики CISA, NIST, досвід фахівців).

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ ВІД АТАК ТИПУ RANSOMWARE

1.1. Розвиток загрози програм-вимагачів та її вплив на організації

Програми-вимагачі (ransomware) – це вид шкідливого програмного забезпечення, що призначений для несанкціонованого шифрування даних на комп'ютері жертви з наступним вимаганням викупу за відновлення доступу. Типова атака ransomware розгортається таким чином: спершу шкідливий код потрапляє в систему (через виконання зараженого файлу або експлуатацію уразливості), потім він намагається поширитися на інші пристрої мережі, паралельно шифруючи файли на локальних і мережевих носіях, після чого жертві відображається повідомлення з вимогою сплатити викуп (зазвичай у криптовалюті) для отримання ключа розшифрування. Сучасні програми-вимагачі еволюціонували далеко за межі простого шифрування: як зазначалось у вступі, зловмисники часто використовують подвійне вимагання, коли окрім шифрування, ще й викрадають конфіденційні дані жертви, погрожуючи їх оприлюдненням або продажем, якщо викуп не буде сплачено. Такий підхід створює додатковий важіль тиску на організацію, адже навіть за наявності резервних копій даних питання витоку інформації та порушення конфіденційності залишається серйозною проблемою. Більш того, фіксуються випадки *"потрійного"* вимагання, коли атакувальники, окрім шифрування і витоку, застосовують додатковий шантаж – наприклад, здійснюють DDoS-атаки на сервіси жертви або особисто звертаються до клієнтів/партнерів жертви з повідомленням про злам, аби ті тиснули на керівництво сплатити викуп.

Збитки від атак ransomware для бізнесу є надзвичайно суттєвими. Втрата доступу до даних призводить до зупинки критичних бізнес-процесів – компанія фактично не може здійснювати операційну діяльність, поки системи не будуть відновлені. Це особливо небезпечно для сфер охорони здоров'я (де збій у доступі

до медичної інформації ризикує життями пацієнтів), енергетики, фінансів та державних послуг. Навіть якщо вдається відновити дані з резервних копій, простої і відновлення можуть тривати від кількох днів до кількох тижнів, що спричиняє значні фінансові втрати. Додатково, компрометація даних підриває довіру клієнтів та партнерів, шкодить репутації організації, що може мати довгострокові негативні наслідки. Факт виплати викупу теж не гарантує повного вирішення проблеми: по-перше, немає гарантії, що зловмисники виконають обіцянки і нададуть діючий ключ розшифрування; по-друге, оплата стимулює злочинців до нових атак і може зробити організацію ціллю повторного нападу. З огляду на це, органи влади та експерти майже одностайно не рекомендують сплачувати викуп (якщо це можливо уникнути). Значно більш ефективною стратегією є запобігання атаці або принаймні оперативне виявлення і припинення її до того, як вона завдала непоправної шкоди.

На жаль, статистика свідчить, що загроза ransomware лише зростає. За останні роки зафіксовано значне збільшення кількості атак. Наприклад, за даними IBM, у 2023 році 24% усіх кіберінцидентів, розслідуваних компанією, були пов’язані з програмами-вимагачами. У грошовому вимірі 2023 рік став рекордним: загальний обсяг виплачених викупів за даними аналітиків перевищив 1,0 – 1,1 млрд доларів США (для порівняння, у 2022 році ця цифра була майже вдвічі меншою через тимчасовий спад активності, пов’язаний з геополітичними подіями). Серед резонансних випадків останнього часу – атаки на найбільший трубопровідний оператор США Colonial Pipeline (2021), ірландську систему охорони здоров’я HSE (2021), мережу медичних закладів Universal Health Services, а також масові атаки через злами програмних постачальників (наприклад, через уразливість у популярному інструменті передачі файлів MOVEit у 2023 р. постраждали сотні організацій по всьому світу). Ці інциденти показують, що програми-вимагачі загрожують усім секторам: від енергетики і транспорту до освіти, від малого бізнесу до транснаціональних корпорацій. Зважаючи на це, питання захисту від ransomware на рівні організації є надзвичайно актуальним, і міжнародні організації з кібербезпеки (CISA, ENISA, NIST) розробляють спеціальні рекомендації та керівництва з протидії цій загрозі.

.

1.2. Типові вектори реалізації атак ransomware на кінцевих пристроях

Щоб ефективно захиститися від програм-вимагачів, потрібно розуміти, як саме відбувається зараження кінцевої точки – тобто які шляхи проникнення й розповсюдження використовують зловмисники. Нижче розглянемо основні етапи типового ланцюга атаки ransomware та вектори, задіяні на кожному з них:

- Первинне проникнення (Initial Access): На цій фазі атакувальник отримує початковий доступ до хоча б одного вузла мережі (найчастіше – до робочої станції користувача). Найпоширеніший вектор – це фішинг: жертві надсилається електронний лист із соціальною інженерією, що спонукає відкрити вкладений файл (наприклад, документ Office з макросом) або перейти за посиланням на заражений вебсайт. В результаті користувач несвідомо завантажує та запускає шкідливий код. Інший популярний шлях – атаки на відкриті сервіси: зловмисники сканують Інтернет на наявність незахищених або уразливих служб (RDP, SSH, VPN) і, виявивши такі, проводять брутфорс або експлуатацію відомих вразливостей. За даними спільного звіту CISA та ФБР, велика частка інцидентів ransomware розпочиналась саме зі зламу відкритого RDP-сервера шляхом підбору або викрадення паролю адміністратором. Також трапляються випадки, коли зловмисники купують на чорному ринку вже готовий доступ до мережі компанії (облікові дані компрометованих користувачів або доступ через бекдор, встановлений іншим шкідливим ПЗ). Додамо, що часто початкове проникнення відбувається не самим ransomware, а так званим «попередником» – іншою шкідливою програмою (*precursor malware*). Наприклад, тривалий час популярною схемою була інфекція трояном-крадієм даних (QakBot, Emotet тощо), який потім завантажував модуль-вимагач (Ryuk, Conti) у вже скомпрометовану мережу. Це ускладнює захист, адже перша стадія може залишитися непоміченою, якщо засобам безпеки не вдалося вчасно зупинити початковий malware.
- Розгортання шкідливого ПЗ (Execution & Installation): Після потрапляння у систему, шкідливий код (чи то безпосередньо ransomware, чи його «провісник») прагне закріпитися. Наприклад, файл-вимагач може скопіювати себе в системні

директорії, додати ключ у автозавантаження реєстру Windows або використати планувальник завдань, аби зберегти стійкість до перезавантаження системи. Деякі сучасні ransomware діють швидко, не турбуючись про довготривалу присутність – вони можуть почати шифрування одразу, щойно запущені, особливо у випадку «ручних» атак, коли оператор безпосередньо керує процесом. Але часто перед шифруванням виконується підготовка: відключення системних засобів захисту (антивірусів, брандмауерів), видалення резервних Shadow Copies (командами vssadmin delete shadows), щоб унеможливити відновлення даних, а також можлива ескалація привілеїв – спроба отримати права адміністратора на системі, що дасть більший контроль (наприклад, через експлойти локальних привілеїв або викрадення паролів у пам’яті).

- Вертикальне та горизонтальне просування (Privilege Escalation & Lateral Movement): Якщо атака спрямована на всю мережу, зловмисники після компрометації однієї машини починають ширити вплив. Вертикальна ескалація – здобуття вищих привілеїв – може бути необхідна для вимкнення захисного ПО чи шифрування мережевих дисків. Горизонтальне переміщення по мережі (lateral movement) дозволяє вийти за межі початкової точки входу й охопити більше пристроїв. Для цього атакувальники застосовують ряд методів: використання інструментів адміністрування (WMIC, Powershell, PsExec) для віддаленого виконання, пошук відкритих SMB-ресурсів і копіювання свого ПЗ туди, сканування мережі на інші вразливі машини, підбір паролів до сусідніх систем тощо. Багато сучасних груп ransomware діють як “advanced persistent threat” (APT): вони можуть кілька днів або тижнів потай досліджувати мережу жертви, розгортаючи бекдори і крадучи дані, і лише потім запускають масове шифрування одночасно по всій інфраструктурі, щоб максимізувати шкоду. Тактика «живучості» в мережі і використання легітимних інструментів (наприклад, вбудованих утиліт Windows) робить їх виявлення стандартними засобами складним, адже дії зловмисників маскуються під законну активність адміністрування.
- Шифрування та вимагання (Encryption & Exfiltration): Це фінальна фаза атаки програм-вимагача. На цьому етапі шкідливе ПЗ запускає масове шифрування

файлів на локальних дисках і мережевих ресурсах, використовуючи сильні криптоалгоритми (AES, RSA тощо). Зазвичай кожен файл (або група файлів) шифрується унікальним ключем, який, у свою чергу, зашифрований публічним ключем зловмисників – таким чином розшифрування можливе лише при отриманні приватного ключа, який тримають нападники. Жертві відображається повідомлення-вимога (ransom note) – як текстовий файл на робочому столі або заміна шпалер – зі звісткою про шифрування і інструкціями щодо оплати викупу (адреса криптогаманця, контактні дані для зв'язку тощо). Одночасно часто відбувається екфільтрація – якщо дані ще не були викрадені раніше, програма-вимагач може перед шифруванням відправити копії файлів на сервер, контрольований нападниками, з метою подальшого шантажу. Після завершення шифрування більшість зловмисних програм видаляє себе або "лягає на дно", залишаючи на екрані лише інструкції для потерпілих. На цьому цикл атаки завершено – далі все залежить від дій жертви (оплата викупу чи відмова і відновлення самотужки).

Такий сценарій описує типову поведінку ransomware, хоча в реальних випадках можуть бути варіації. Наприклад, деякі «масові» поширені родини (на кшталт WannaCry чи REvil) автоматизовано сканували Інтернет і вражали системи без прямого керування оператором, тоді як сучасні цільові атаки майже завжди здійснюються в режимі ручного управління (human-operated ransomware), де живі хакери в реальному часі керують інструментами у мережі жертви. Це ускладнює захист, адже людина-оператор може адаптувати свої дії під обставини, шукати шляхи обходу працюючих засобів захисту, реагувати на часткові виявлення.

Чому кінцеві точки – уразлива ланка? Робочі станції користувачів традиційно є одним з найменш захищених елементів, оскільки на них виконується різноманітне програмне забезпечення, користувачі можуть взаємодіяти з зовнішніми ресурсами (веб, пошта), вставляти зовнішні носії. Людський фактор – користувач може випадково запустити шкідливий файл, піддавшись на соціальну інженерію. Крім того, багато організацій мають десятки або сотні кінцевих пристроїв, що ускладнює централізований контроль: оновлення ОС можуть встановлюватися із запізненням,

конфігурація систем безпеки не завжди є уніфікованою. Зловмисники ж постійно шукають найслабші ланки – достатньо зламати одну незахищену машину, щоб отримати плацдарм для атаки. До того ж, часто кінцеві точки фізично знаходяться поза периметром корпоративної мережі (ноутбуки співробітників поза офісом), минаючи традиційні мережеві засоби захисту (брандмауери, шлюзи безпеки), що робить їх більш вразливими.

Отже, ефективний захист кінцевих точок від ransomware має охоплювати весь цикл атаки: від запобігання первинному проникненню (через фільтрацію фішингових листів, захист RDP, багатофакторну автентифікацію, регулярні патчі), до механізмів виявлення підозрілої активності вже після компрометації (моніторинг поведінки процесів, виявлення спроб ескалації та поширення), і, звісно, швидкого реагування – ізоляції ураженого хоста, блокування виконання шкідливого коду, повідомлення персоналу для вжиття заходів. Саме тому дедалі більше організацій впроваджують комплексні засоби захисту кінцевих точок (Endpoint Protection Platform, EPP), ключовим компонентом яких є EDR – системи виявлення та реагування на кінцевих точках. Сучасні EDR-рішення поєднують традиційний антивірус (для відомих загроз) із проактивним поведінковим аналізом, машинним навчанням для визначення нових шкідливих зразків, а також забезпечують збір телеметрії з хостів для подальшого розслідування інцидентів. Такі рішення працюють у режимі 24/7 та покликані зменшити «час до виявлення» та «час до реагування» з днів чи годин до хвилин і навіть секунд. Впровадження засобів EDR є нині галузевим стандартом: аналітики Gartner відзначають, що все більше підприємств переходять від окремих антивірусів до платформ захисту кінцевих точок (EPP), які включають функції запобігання, виявлення та реагування на загрози. Прикладом такої платформи є CrowdStrike Falcon, яка набула значного поширення у світі і визнана лідером ринку згідно ряду незалежних оцінок. Цьому рішенню і присвячено наступні розділи роботи.

1.3. Існуючі засоби захисту кінцевих точок: недоліки та потреба в EDR

Перш ніж перейти до огляду рішення CrowdStrike, доцільно коротко розглянути основні категорії засобів захисту кінцевих точок, що використовуються на практиці, оцінити їх сильні та слабкі сторони у контексті протидії ransomware.

- Антивірусні програми (Traditional Antivirus, AV). Це найстаріший і найдосі поширений клас засобів безпеки кінцевих точок. Класичний антивірус працює на основі сигнатурного аналізу – має базу відомих «відбитків» шкідливих програм (хеші файлів, фрагменти коду) і порівнює з ними файли, що виконуються в системі. Якщо знайдено відповідність – файл блокується або видаляється. Також антивіруси часто мають базові евристичні аналізатори, що намагаються виявити нові загрози за схожістю з відомими зразками. Перевага антивірусів – вони ефективні проти відомих загроз і можуть запобігти масовим епідеміям, якщо сигнатури оновлені. Недоліки – відставання від нових загроз: зловмисники легко модифікують код ransomware, щоб уникнути виявлення, використовуючи упаковщики, шифруючи свій код, тощо. AV-продукти часто не здатні вчасно розпізнати *zero-day* або поліморфні зразки програм-вимагачів. До того ж, вони зазвичай реагують постфактум (коли файл вже потрапив у систему і почав виконання). У випадку швидкісних шифрувальників навіть кілька хвилин роботи до блокування можуть означати шифрування великої кількості файлів. Таким чином, традиційні AV є необхідним компонентом, але їх явно недостатньо для повноцінного захисту від сучасних ransomware-кампаній.
- Міжмережеві екрани та мережеві засоби (Firewall, IPS). Брендмауери і системи запобігання вторгненням на мережевому рівні можуть відфільтровувати частину злочинного трафіку – наприклад, блокувати відомі шкідливі домени, сервери керування, по яким ransomware намагається отримати ключі шифрування чи зливати дані. Проте, все більше атак здійснюється всередині мережі або через шифровані канали, тому мережеві інструменти мають обмежений огляд. До того ж, коли багато пристроїв працює поза периметром (віддалено), мережевий захист їх може не охоплювати.

- Засоби резервного копіювання та відновлення (Backup/Restore). Строго кажучи, це не запобіжний засіб, а засіб мінімізації збитків. Наявність актуальних offline-резервних копій даних дозволяє відновитися після атаки, не сплачуючи викуп. Це суттєво послаблює позицію зловмисників. Однак резервне копіювання не перешкоджає самому факту атаки і шифрування – воно лише забезпечує "страхову" опцію. Багато організацій, на жаль, не приділяють належної уваги резервуванню, або ж копії теж виявляються уразливими (підключені постійно до мережі і також зашифровані нападником). Тому лише на бекапи покладатися небезпечно.
- Системи контролю доступу та привілеїв (IAM, PAM). Обмеження прав користувачів (принцип найменших привілеїв) та використання багатофакторної автентифікації значно ускладнюють дії зловмисників. Наприклад, якщо користувач працює не під адміністратором, ransomware не зможе легко вимкнути системні служби чи шифрувати мережеві диски. Захист облікових записів (MFA, унікальні паролі) зменшує ризик зламу через RDP. Однак цими заходами має опікуватися загальна політика безпеки – вони є фоновими, і жодна політика повністю не виключає людської помилки чи технічної уразливості.
- Endpoint Detection and Response (EDR) – сучасні платформи захисту кінцевих точок. Це відносно новий клас рішень, що поєднує кілька технологій: проактивне моніторинг поведінки процесів на хості, виявлення аномалій за допомогою правил (Indicators of Attack) та алгоритмів машинного навчання, збір детальної телеметрії (журнали подій, дії програм, зміни файлів реєстру, мережеві з'єднання) та інструменти реагування (можливість ізолювати хост від мережі, зупинити процес, видалити файл, провести аналіз). EDR зазвичай функціонує як агент на кожній кінцевій точці, що постійно відправляє дані в централізовану систему (найчастіше – хмарну) для аналізу. На відміну від традиційного антивірусу, який відповідає переважно на відомі загрози, EDR намагається виявити і нові, ще невідомі атаки на основі поведінкових ознак. Наприклад, різка масова модифікація великої кількості файлів користувача процесом, який раніше не проявляв такої активності, може бути розцінена як потенційно шкідлива (ознака

шифрувальника). Або ж запуск vssadmin.exe з параметрами видалення копій тіньового копіювання – це нетипова дія, яка може трактуватися як індикатор атаки (Indicator of Attack, IOA), характерний для ransomware. EDR-продукт здатен заблокувати такі дії *на льоту*, навіть якщо сам файл-зловмисник невідомий сигнатурно. Крім того, EDR надає аналітикам інформацію для розслідування інциденту: які дії виконав шкідливий процес, що він запустив, які файли змінив, яким сервером намагався з'єднатися тощо. Це дає змогу встановити джерело проникнення і виконати повне усунення наслідків (eradication) – видалити всі компоненти, виправити вразливості, через які стала можлива атака.

На практиці, на сьогодні кращим підходом вважається комплексне поєднання вищеназваних засобів. Жоден з них окремо не гарантує 100% захисту, але разом вони суттєво знижують ризики. Проте ядром саме оперативного виявлення та зупинки ransomware зараз виступають рішення класу EDR/EPP. Вони постійно розвиваються, інтегруючи все нові функції (наприклад, елементи автоматизації реагування – *SOAR*, чи розширене виявлення на рівні всієї інфраструктури – *XDR*).

CrowdStrike Falcon – одна з провідних сучасних EDR-платформ – була обрана нами для детального дослідження у зв'язку з її високою репутацією та широким використанням у світі. Ця платформа неодноразово демонструвала високу ефективність проти атак програм-вимагачів. Так, відповідно до результатів незалежного тестування SE Labs (Enterprise Advanced Security) за 2024 рік, рішення CrowdStrike забезпечило 100% виявлення та запобігання ransomware-атакам (найвищий результат серед усіх учасників). Компанія CrowdStrike вже п'ятий рік поспіль відзначена як лідер у Magic Quadrant від Gartner у категорії платформ захисту кінцевих точок, що підтверджує її спроможність задавати галузеві стандарти. За даними самої компанії, її клієнтами є сотні найбільших корпорацій світу (в тому числі 254 з 500 найбільших компаній США за списком Fortune) – такий рівень довіри з боку бізнесу свідчить про ефективність і надійність технології.

У наступному розділі ми розглянемо архітектуру та складові платформи CrowdStrike Falcon, а також проаналізуємо, яким чином вона реалізує захист

кінцевих точок від атак типу ransomware.

2 ОГЛЯД РІШЕННЯ CROWDSTRIKE FALCON ДЛЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК

2.1. Архітектура платформи CrowdStrike: хмарна інфраструктура та агент

CrowdStrike Falcon – це хмарна платформа кібербезпеки, спеціалізована на захисті кінцевих точок і хмарних робочих навантажень. Її архітектура реалізована за моделлю *“endpoint agent + cloud”*, що означає наявність легкого клієнтського агента на кожній кінцевій точці, тісно інтегрованого з потужною аналітичною інфраструктурою у хмарі. Такий підхід дозволяє поєднати мінімальне навантаження на сам кінцевий пристрій із високою швидкістю обробки та масштабованістю за рахунок хмарних обчислень.

Основні компоненти архітектури CrowdStrike Falcon:

- Falcon Sensor (Агент) – маленький програмний модуль (~30 МБ), що встановлюється на кінцевій точці (Windows, Mac, Linux, мобільні ОС). Агент працює на рівні ядра ОС та користувацького простору, відстежуючи ключові події: запуск процесів, звернення до файлів, зміни реєстру, мережеві з’єднання тощо. Falcon Sensor спроектовано бути невимогливим до ресурсів: за даними CrowdStrike, він споживає мінімум пам’яті та ЦП і практично не впливає на продуктивність системи, що було одним з пріоритетів дизайну. Агент може самостійно, локально, блокувати відомі загрози – в нього вбудовані моделі машинного навчання (наприклад, для офлайн-виявлення шкідливих файлів за їх характеристиками) та правила блокування (фільтри I/O). Але основна його задача – збір та передача телеметрії у хмару. Усі зафіксовані події (а їх генерується величезна кількість щодня в масштабі компанії) відправляються у хмарне сховище CrowdStrike для глибинного аналізу системою Threat Graph. Важливо відзначити, що дизайн Falcon Sensor враховує вимоги безперервного захисту: навіть якщо кінцева точка тимчасово офлайн (без Інтернету), агент все одно може автономно запобігти

атакам, покладаючись на локальні моделі AI та кеш правил, а щойно відновиться зв’язок – передасть усі дані й отримає оновлення.

- CrowdStrike Cloud (хмарна платформа CrowdStrike Security Cloud) – центр обробки даних і керування Falcon. Це високонавантажена хмарна інфраструктура, яка щодня приймає і аналізує телеметрію від мільйонів агентів по всьому світу. За повідомленнями компанії, Threat Graph (аналітичне ядро в хмарі) щотижня корелює понад трильйон подій з кінцевих точок у реальному часі. Використовуючи розвинені алгоритми big data та AI, платформа виявляє підозрілі взаємозв’язки та шаблони, які можуть вказувати на злочинну активність. Наприклад, якщо на кількох незалежних системах по світу агент зафіксує схожу послідовність дій, що відповідає невідомому раніше шкідливому сценарію, Threat Graph може “скласти пазл” і створити нове правило або модель для виявлення такої загрози надалі. В хмарі також зберігаються Indicators of Compromise (IOC) – відомі сигнатури, хеші, домени, IP, пов’язані зі зловмисниками – та Indicators of Attack (IOA) – узагальнені моделі поведінки атак. Коли від агента надходять дані, вони порівнюються з базами IOC/IOA і проганяються через ML-алгоритми. Якщо виявлено небезпечну активність, в хмарі генерується оповіщення (alert), яке відображається на консолі аналітика.
- Консоль керування Falcon (Web UI) – хмарний інтерфейс, де фахівці можуть переглядати всі виявлення, деталі інцидентів, історичну телеметрію, а також керувати налаштуваннями та відповідами. Через цю консоль безпеки можна, наприклад, в один клік відправити команду на агент ізолювати конкретну кінцеву точку (тобто від’єднати її від мережі, залишивши тільки канал зв’язку з хмарою CrowdStrike). Також консоль надає засоби пошуку по всій зібраній базі даних подій (для *threat hunting*, проактивного полювання за загрозами). Оскільки рішення є хмарним SaaS, оновлення (нові функції, аналітика) доставляються автоматично через хмару, немає потреби розгортати чи оновлювати сервери на території замовника. Це знижує витрати на підтримку і забезпечує масштабованість: клієнт може легко розширити захист на тисячі нових хостів, просто встановивши агент, без турбот про інфраструктуру моніторингу.

Архітектурні переваги CrowdStrike Falcon:

- *Єдиний легковагий агент:* CrowdStrike одним з перших на ринку запропонував об’єднати різні функції (антивірус, EDR, моніторинг стану хоста) в одному агенті, щоб уникнути «засмічення» системи кількома клієнтами безпеки. Це спрощує адміністрування і зменшує сумарне навантаження на кінцеву точку. Як зазначено в документації, Falcon-агент поєднує в собі NGAV (Next-Gen AV), EDR та модуль керованого полювання OverWatch – традиційно для цього потрібні були б окремі рішення.
- *Хмарно-орієнтована обробка:* Перенесення “мозкового центру” в хмару дає можливість задіяти для аналізу значні обчислювальні потужності, недоступні на звичайному ПК. Таким чином, навіть дуже складні алгоритми AI можуть працювати швидко, обробляючи потік подій у реальному часі. Крім того, хмара агрегує дані від усіх клієнтів CrowdStrike, створюючи ефект «колективного розвідника» – як тільки нова загроза виявлена у когось одного, інформація про неї стає відома для захисту інших. Така архітектура особливо ефективна проти масових кампаній ransomware: наприклад, якщо одна компанія зазнала атаки новим видом шифрувальника, Falcon може розпізнати його поведінку і оперативно почати блокувати аналогічні атаки по всій своїй клієнтській базі.
- *Масштабованість та доступність:* Хмарна реалізація означає, що рішення легко масштабується під будь-який розмір організації. Не потрібно ставити додаткові сервери при рості з 100 до 10000 хостів – цим опікується провайдер. Також забезпечується висока доступність сервісу (хмарні кластери з резервуванням) – події завжди будуть доставлені і проаналізовані з мінімальними затримками.
- *Оновлення та інновації:* CrowdStrike регулярно додає нові можливості у Falcon без участі замовника – наприклад, впровадження штучного інтелекту нового покоління (у 2023 було анонсовано “AI-powered IOAs” – використання ШІ для генерації нових поведінкових правил). Завдяки SaaS-моделі клієнти миттєво отримують вигоду від цих інновацій без складних оновлень.

Важливо відзначити, що архітектура Falcon побудована з урахуванням вимог

безпеки самих переданих даних: телеметрія з агентів шифрується при передачі, в хмарі застосовуються механізми багаторівневого контролю доступу та ізоляції даних клієнтів. Це критично, оскільки кінцеві точки можуть передавати чутливу інформацію (наприклад, імена файлів, хеші документів). CrowdStrike проходить зовнішні аудити та сертифікації, щоб підтвердити надійність своєї хмарної архітектури в плані захисту інформації клієнтів.

Отже, архітектурно CrowdStrike Falcon забезпечує постійний, централізований контроль за безпекою кінцевих точок із використанням переваг хмарних технологій. Це створює фундамент для ефективної реалізації різноманітних функцій захисту, про які йтиметься далі**.**

2.2. Функції та можливості Falcon: NGAV, EDR, Threat Intelligence, OverWatch

Платформа CrowdStrike Falcon включає кілька модулів та функціональних компонентів, які разом утворюють багаторівневу систему захисту кінцевих точок. Розглянемо основні з них та їх роль у протидії загрозам:

- NGAV (Next-Generation AntiVirus) – “Антивірус нового покоління”. Цей модуль відповідає за превентивне блокування відомих та невідомих шкідливих програм. На відміну від традиційного AV, Falcon NGAV покладається не на сигнатури, а на машинне навчання та поведінковий аналіз. Falcon аналізує файли до їх виконання (статичний AI-аналіз) – за більш ніж 1000 параметрами файлу модель визначає, чи схожий він на шкідливий. Наприклад, аналізується структура коду, послідовності байтів, присутність характерних фрагментів, які притаманні малварі. Такий підхід дозволяє зупиняти нові зразки, для яких ще немає сигнатур. При цьому платформа враховує і контекст виконання: якщо навіть файл формально не відомий як вірус, але намагається зробити щось підозріле (наприклад, Word-процес запускає сценарії PowerShell з завантаженням коду з Інтернету), то спрацює відповідне правило IOA на блокування. NGAV також має класичні антивірусні можливості – сканування хосту на відомі загрози, карантин шкідливих файлів. У

контексті ransomware NGAV служить першою лінією оборони: він може попередити запуск відомого сімейства програми-вимагача (якщо хеш чи модель збігається з базою) ще до того, як той почне шифрування. Випереджаючий поведінковий аналіз здатний виявити і “0-денні” зразки, зокрема за такими ознаками, як спроби масового відкриття файлів для запису (початок шифрування), швидке створення/видалення файлів з певними розширеннями (наприклад, створення записок-вимог). Тобто NGAV CrowdStrike – це не просто антивірус, а інтелектуальний модуль запобігання, інтегрований з рештою системи.

- EDR (Endpoint Detection & Response) – Виявлення та реагування на хості. Цей модуль відповідає за безперервний моніторинг та детекцію підозрілої активності і надає інструменти для реагування. Falcon EDR збирає телеметрію про усі значущі події на кінцевій точці: які процеси запускалися, які модулі завантажувалися, які файли створювалися/видалялися, які ключі реєстру змінювалися, які з’єднання встановлювалися. У випадку виявлення потенційної загрози, EDR створює детальну хронологію атаки (attack timeline) – у консолі CrowdStrike це представлено у вигляді “дерева процесів” і списку дій злоумисника. Наприклад, для інциденту ransomware можна побачити: “Proc01 (excel.exe) -> запускає Proc02 (cmd.exe з параметром /c запуска PowerShell) -> Proc03 (powershell.exe) виконує команду, що завантажує payload -> створено файл X.exe -> запущено X.exe -> X.exe шифрує файл Y.docx…”. Така прозорість надзвичайно важлива для розслідування та усунення загрози, адже дозволяє зрозуміти, звідки взявся шифрувальник (через Excel з макросом) і які дії він встиг виконати. Крім пасивного збору, EDR дає змогу активно реагувати: через консоль аналітик може надіслати на агент команду завершити певний процес, видалити файл, або навіть відкрити сеанс “Remote Shell” – інтерактивно підключитися до зараженої машини в режимі командного рядка для глибшого аналізу (переглянути запущені процеси, вивантажити підозрілі файли для аналізу, запустити скрипти очищення). Однією з ключових можливостей Falcon є миттєва ізоляція хоста – якщо виявлено, що станція заражена, її можна перевести в режим ізоляції (мережеві з’єднання блокуються окрім зв’язку з Falcon Cloud) в один клік. Це запобігає поширенню

ransomware по мережі навіть якщо загроза ще повністю не нейтралізована на самому хості. Ізольовану машину потім можна обстежити і відновити без ризику для інших. EDR функціонал CrowdStrike особливо цінний у боротьбі з цілеспрямованими атаками: навіть якщо певна частина атаки пройшла повз превентивний захист, EDR покликаний вчасно виявити аномальну поведінку та дати можливість швидко відреагувати, мінімізувавши збитки.

- Threat Intelligence (TI) – база загроз та аналітичні дані. CrowdStrike Falcon тісно інтегрований з розвідувальними даними про кіберзагрози. Це означає, що система “знає” про актуальні тактики, техніки і процедури (TTPs) різних хакерських груп, включно з тими, що застосовуються операторами ransomware. CrowdStrike як компанія має власний підрозділ Threat Intelligence, який відстежує діяльність кіберзлочинних спільнот, аналізує зразки malware, випускає звіти. Ця інформація вбудована у Falcon: кожне виявлення зіставляється з відомими акторами загроз. Наприклад, якщо була зафіксована специфічна послідовність команд, характерна для групи FIN12 (відомої використанням Ryuk ransomware), в консолі може відобразитися, що “ймовірний противник: Wizard Spider” (умовна назва групи, що за цим стоїть). Це допомагає краще розуміти контекст атаки. Практично важливо, що база IOC (Indicator of Compromise) постійно оновлюється – відомі хеші файлів-вимагачів, IP-адреси серверів керування, домени для витоку даних – все це автоматично враховується при аналізі телеметрії. Крім того, модуль CrowdStrike Threat Intelligence дозволяє аналітику робити запити і отримувати досьє на виявлені артефакти: наприклад, якщо знайдено файл з певним хешем, можна одразу в консолі глянути, чи відомий він і до якого сімейства malware належить. TI також надає прогнозні дані: наприклад, попередження про нові кампанії ransomware, що були помічені в певній галузі. Загалом, інтеграція розвідки загроз робить реагування більш обґрунтованим і швидким – фахівці мають більше інформації під рукою, щоб прийняти рішення.

- CrowdStrike OverWatch – кероване проактивне полювання (Managed Threat Hunting). Це унікальна функція Falcon, яка полягає у тому, що команда експертів CrowdStrike 24/7 відстежує аномалії в телеметрії клієнтів і допомагає

виявляти складні загрози, які могли пройти непоміченими автоматичними засобами. Фактично OverWatch – це *додатковий рівень* над автоматичною EDR: це люди-аналітики, озброєні спеціальними інструментами, які шукають ледь помітні ознаки вторгнень. Якщо вони знаходять щось підозріле, вони повідомляють команду безпеки організації і допомагають у розслідуванні. Ця послуга особливо корисна проти дуже витончених атак, де нападники можуть використовувати невідомі методи. У контексті ransomware OverWatch може, наприклад, виявити на ранній стадії проникнення трояна-інфостілера або незвичні рухи в мережі (що може свідчити про підготовку до майбутнього розгортання шифрувальника) і попередити до того, як відбудеться шифрування. CrowdStrike наводить приклади, коли OverWatch зупиняв атаки рансомваре в зародку – при появі лише кількох команд атакувальників у системі, до запуску самого шифрувальника. Таким чином, клієнти Falcon отримують комбінований підхід: ШІ + експерти для найвищої ефективності.

- Додаткові модулі Falcon: Окрім вищезгаданих, платформа має ще низку компонентів, які доповнюють безпеку. Наприклад, Falcon Firewall Management – модуль для централізованого керування брандмауером Windows з консолі Falcon (дозволяє швидко застосувати політики блокування портів, адрес під час інциденту). Falcon Device Control – контроль використання зовнішніх пристроїв (USB-накопичувачів), що може запобігти занесенню malware з флешок. Falcon Discover/Spotlight – модулі для оцінки стану хоста (вразливості, інвентаризація програм) – корисно для усунення слабких місць, якими можуть скористатися зловмисники. Також є Falcon XDR, що розширює видимість за межі кінцевих точок (на мережеві пристрої, хмарні сервіси), проте в контексті даної роботи ключовим залишається EDR на кінцевих системах.

Загалом, CrowdStrike Falcon надає багатоешелонний захист кінцевої точки: спочатку спрацьовує превентивний рівень (NGAV), якщо він не зупинив – поведінкові алгоритми і перевірки в хмарі (IOA) сигналізують EDR, далі при необхідності втручається людина-аналітик (чи то з боку замовника, чи OverWatch). Така глибока оборона створює значні труднощі для програм-вимагачів. Навіть

якщо новий зразок зуміє оминути один бар’єр, він імовірно буде спійманий на іншому.

Ефективність CrowdStrike Falcon проти ransomware підтверджена численними тестами і випадками з практики. Окрім згаданого 100% результату в SE Labs 2024, варто згадати, що Falcon здобув найвищі оцінки і в інших незалежних оцінюваннях. Наприклад, у 2024 році платформа отримала відзнаку AAA і була визнана кращою за точністю детектування складних багатоступеневих атак (включно з тими, що імітували дії північнокорейських ransomware-груп). У огляді радару GigaOm 2024 Falcon також названо лідером та «outperformer» за можливостями запобігання ransomware. Такі результати означають, що функціонал Falcon не лише декларується, а й реально спрацьовує у випробуваннях, наближених до бойових умов.

Отже, CrowdStrike Falcon – це комплексне рішення, яке реалізує концепцію “вбити атаку в зародку”: завдяки поєднанню інтелектуальних алгоритмів та експертного контролю, платформа здатна виявити дії програм-вимагачів на найранніших стадіях (наприклад, коли ще тільки відбувається спроба вимкнути резервні копії або ескалація привілеїв) і миттєво зупинити їх, не допускаючи масового шифрування. Наступний підрозділ розгляне конкретні механізми Falcon, спрямовані саме на боротьбу з ransomware, більш прикладно.

1.3. Механізми протидії ransomware в CrowdStrike Falcon

З огляду на наведені вище функціональні можливості Falcon, детальніше сфокусуємося на тому, як саме ця платформа виявляє та зупиняє атаки програм-вимагачів. Адже, хоча принципи роботи вже описані, важливо зрозуміти специфічні механізми та сценарії, які реалізовані в CrowdStrike для протидії саме ransomware.

1. Поведенкові індикатори атаки (IOA) для виявлення шифрування. В арсеналі Falcon є набір правил, що описують характерні поведінкові шаблони ransomware. Наприклад, одна з ключових ознак – це неприродна кількість операцій

шифрування/перезапису файлів за короткий час. Якщо процес, особливо раніше невідомий, починає відкривати файли один за одним і змінювати їх вміст (а розширення файлів при цьому змінюються на підозрілі .locked, .crypt або випадкові суфікси) – це явна червона прапор. Falcon моніторить швидкість і характер файлових операцій: коли вони виходять за межі типових для легітимних програм (наприклад, архіватор або програма резервного копіювання теж можуть масово обробляти файли, але їх профіль відомий), спрацьовує тривога. Такі правила враховують і еволюцію ransomware – наприклад, сучасні програми-вимагачі можуть спочатку шифрувати лише частину кожного файлу (щоб прискорити процес). Алгоритми Falcon навчені помічати і такі аномалії (нетипове часткове перезаписування багатьох файлів). Інший приклад IOA – спроба видалення тіньових копій та резервних копій системи: якщо процес виконує команду vssadmin.exe Delete Shadows /All /Quiet або аналог через WMI, Falcon кваліфікує це як потенційно зловмисну дію, властиву ransomware (адже легітимним програмам рідко потрібно масово видаляти точки відновлення). Ще один індикатор – звернення до служб шифрування системи (CryptoAPI) великою кількістю викликів, або завантаження бібліотек шифрування. Усі ці поведінкові шаблони не прив'язані до конкретного шкідливого ПЗ, а саме відстежують *"що робить процес"* (IOA), завдяки чому Falcon може зупиняти нові, ще небачені зразки рансомваре.

2. AI-моделі для статичного аналізу файлів-вимагачів. CrowdStrike розробила статичні моделі машинного навчання, які працюють на рівні агента та в хмарі. Ці моделі були натреновані на мільйонах зразків шкідливих і легітимних файлів. У випадку ransomware, вони можуть розпізнавати характерні ознаки навіть у нових виконавчих файлах. Дослідження показали, що багато родин ransomware мають спільні риси в коді (наприклад, використання певних бібліотек шифрування, схожі секції даних тощо). Модель Falcon враховує сотні таких характеристик. Тому, коли на кінцеву точку потрапляє потенційний шифрувальник, є велика імовірність, що його вловить ML-детектор ще до виконання. Скажімо, користувач завантажив з Інтернету файл Invoice_PDF.exe (маскується під документ). Щойно цей файл зберігся на диску і користувач намагається його запустити, Falcon Sensor перевіряє

файл своєю AI-моделлю. Якщо файл дійсно є ransomware, модель з високою вірогідністю класифікує його як malicious – тоді запуск блокується, а файл поміщається в карантин. У протоколі Falcon буде записано запобігання загрозі. Таким чином, багато атак спиняються на самому початку, ще до шкідливих дій. У випадку невпевненості (низький рівень "злостивості" за оцінкою) файл може бути дозволений до запуску, але тоді вступають в дію поведінкові механізми, описані вище.

3. Автоматичне реагування: ізоляція і знищення процесу. Коли Falcon детектує, що процес поводиться як ransomware, він може виконати автоматичне реагування в режимі реального часу. Політики CrowdStrike конфігуруються за бажанням замовника – наприклад, можна виставити, щоб при спрацьовуванні критичного правила IOA агент автоматично завершував процес. У випадку ransomware більшість організацій саме так і налаштовують: щойно виявлено поведінку шифрування – процес знищується негайно. Це зупиняє подальше шифрування. Одночасно (або одразу після цього) можна ввімкнути авто-ізоляцію хоста від мережі. Деякі компанії обирають робити ізоляцію вручну, але якщо пріоритет – убезпечити мережу, то автоматична ізоляція – ефективний шлях. Іноді застосовується комбінація: процес блокується автоматично, а ізоляція вимагає підтвердження аналітиком. В будь-якому разі, Falcon здатен дуже швидко вжити протидіючих заходів. Наприклад, у демонстраційному відео CrowdStrike показано, як при спробі запустити відомий зразок HydraCrypt, Falcon за мілісекунди його завершує, і система встигає зашифрувати лише декілька файлів, а решта – вцілілі. Потім адміністратор бачить алерт з переліком тих кількох файлів, що постраждали, може їх відновити з копій, та усунути сам зловмисний файл. Порівняно, без захисту, той самий зразок за хвилини зашифрував би тисячі файлів.

4. Розширене виявлення lateral movement та дій, що передують шифруванню. Багато рансомваре-атак не починаються раптово з шифрування, а мають підготовчі фази. Falcon уважно відстежує ознаки проникнення і "повзучої" атаки: підозрілі інструменти (Mimikatz – інструмент для крадіжки паролів,

використовується операторами ransomware; запуск сканерів мережі; використання легальних утиліт для виконання команд WMI, PowerShell). Якщо у мережі організації стоїть Falcon, то навіть якщо зловмисники проникли і діють обережно, є велика ймовірність, що якась їх дія підніме “шум”. Наприклад, виконання нетипової команди PowerShell з вбудованим малварним скриптом – Falcon її виявить (бо агент бачить усі команди PowerShell), навіть якщо та команда ще не шифрує файли, але завантажує інструмент. Таким чином, Falcon часто може “зловити” атаку до стадії шифрування. В одному кейсі (умовному, для демонстрації) наводиться ситуація: співробітник відкрив документ, що призвело до виклику PowerShell. Falcon одразу це зловив і заблокував скрипт, ізолював хост, ще до того, як рансомваре встигло завантажитися. Організація відбулася малим переляком – було розслідувано інцидент, змінено поштову політику, користувача проконсультовано. Такі ранні детекції особливо стають можливими, якщо компанія користується послугою OverWatch: досвідчені аналітики можуть помітити навіть одиничне *несанкціоноване використання інструменту адмінування* у нетиповий час і одразу попередити службу безпеки.

5. Запобігання повторному запуску та “самолікування”. Припустимо, Falcon заблокував виконання якогось ransomware-процесу. Але файл-зловмисник лишився на диску. Якщо користувач або система знов його запустить – сценарій повториться. Щоб уникнути повторень, Falcon має функцію Quarantine – виявлені шкідливі файли можуть автоматично переміщуватися в карантин (або видалятися, залежно від налаштувань). Карантин – це ізольоване сховище, звідки файл вже не запуститься. Адміністратор потім може переглянути ці файли, відновити, якщо помилково, або остаточно знищити. Також Falcon контролює автозапуск: якщо ransomware встиг додати запис в автозапуск (щоб після перезавантаження активуватися), то при розслідуванні інциденту через консоль видно ці зміни, і можна їх відкотити одразу (Falcon має скрипти для відновлення системного стану).

6. Оповіщення та координація з Response Team. Хоча це стосується людського фактору, але теж важливий механізм: CrowdStrike Falcon генерує чіткі,

пріоритетизовані оповіщення. При інциденті ransomware, як правило, буде High/Critical Alert з позначкою, що виявлено підозрілу активність, схожу на програму-вимагач. В оповіщенні буде детально вказано, що саме виявлено: наприклад, “Suspicious file encryption activity detected by Falcon (possible ransomware) on host X” з деталями. Це дозволяє команді безпеки миттєво включитись у ситуацію. Через інтеграції (Falcon API) можна налаштувати, щоб таке критичне сповіщення приходило на електронну пошту, месенджер або в SOAR-систему. Таким чином, час реакції команди SOC мінімізується. Більше того, якщо компанія придбала послугу Falcon Complete (повністю керований захист), то фахівці CrowdStrike самі виконають усі дії для стримування і ліквідації загрози за клієнта, практично в режимі аутсорсингового SOC. Це може бути критично для малих організацій, де немає великої внутрішньої команди кібербезпеки – вони отримують підтримку експертів 24/7. У випадку ransomware така модель зазвичай забезпечує реагування протягом кількох хвилин: згідно зі звітом CrowdStrike, середній час до повного усунення загрози (Mean Time to Remediate) для їхніх клієнтів Falcon Complete складає 35 хвилин, тоді як у середньому по галузі цей показник – 162 години. Це драматична різниця, що може означати запобігання катастрофі.

Підсумовуючи, механізми Falcon проти ransomware зводяться до швидкої багатоетапної фільтрації потенційно шкідливих дій: на етапі запуску файлу, на етапі виконання перших команд, на етапі масових дій, і навіть після – на етапі розслідування та прибирання. Усе це реалізовано під єдиним “дахом” платформи, що дозволяє автоматизувати і пришвидшити процес. Практичний досвід численних компаній, які мали Falcon під час реальних атак, демонструє його ефективність. Як приклад, є відгуки IT-директорів: *“CrowdStrike був єдиним інструментом, що зупинив моделювання атаки з програмою-вимагачем найшвидше”*, – зазначає представник банку. Інша компанія після впровадження Falcon повідомила, що тільки завдяки йому виявили спробу зараження і зупинили поширення рансомваре, тоді як інші засоби не спрацювали. Ці свідчення узгоджуються з тестовими даними і підтверджують, що механізми Falcon реально дієві у бойових умовах.

Таким чином, розглянувши архітектуру (2.1), функціонал (2.2) та конкретні механізми захисту (2.3) CrowdStrike Falcon, можемо зробити висновок, що дане рішення представляє собою передовий комплексний засіб захисту кінцевих точок. У наступному розділі роботи ми звернемося до практичної сторони – опишемо приклад застосування Falcon при імітованій атаці та надамо рекомендації щодо впровадження подібних рішень у організаціях.

3 ПРАКТИЧНЕ ЗАСТОСУВАННЯ CROWDSTRIKE: КЕЙС АТАКИ ТА РЕКОМЕНДАЦІЇ

3.1. Сценарій реагуванянвання на атаку програми-вимагача з використанням Falcon

Для закріплення розглянутих теоретичних положень розробимо умовний сценарій кібератаки типу ransomware на підприємство та проілюструємо, як рішення CrowdStrike Falcon допомагає її виявити та нейтралізувати. Цей сценарій базується на реальних тактиках злочинців і демонструє роботу засобу захисту в динаміці.

Умовна вихідна ситуація: Підприємство «AlphaCorp» має ~500 кінцевих пристроїв (робочі станції під керуванням Windows 10/11). На всіх встановлено Falcon Sensor, який підключений до хмарної платформи CrowdStrike. У компанії діє політика безпеки, але на практиці є вразливі місця: зокрема, не всі користувачі уважно ставляться до підозрілих листів, а один зовнішній сервер з RDP було залишено відкритим для віддаленого доступу технічного спеціаліста. Атакуюча сторона – відома хакерська група, що займається подвійним вимаганням (припустимо, група під кодовою назвою *"BlackWolf"*, асоційована зі штамом ransomware "DarkLock"). Мета атакуючих – проникнути в мережу AlphaCorp, зашифрувати сервери та робочі станції, викрасти конфіденційні дані і вимагати викуп.

Хід атаки та дії Falcon:

- *Етап 1: Початкове проникнення.* Зловмисники з групи BlackWolf сканують мережевий периметр AlphaCorp і виявляють відкритий RDP-порт на одному з серверів. Вони здійснюють брутфорс-атаку і підбирають слабкий пароль адміністратора (наше припущення – на жаль, пароль був простим "Password123"). Отримавши доступ через RDP, вони встановлюють на сервері свій *бекдор (reverse shell)* для зручнішого контролю. Поки що Falcon Sensor на цьому сервері (якщо він встановлений) може не одразу заблокувати дії, адже зловмисник діє обережно,

використовуючи штатний RDP-сесійний процес. Проте Falcon вже записує телеметрію: нове підключення RDP з незвичної IP-адреси, запуск командного рядка від імені системи. Ці дії поки що не однозначно зловмисні, але в базі Falcon вони збережені. Якщо компанія використовує OverWatch, то мисливці можуть звернути увагу на нетипову активність у позаробочий час і помітити виконання підозрілого інструменту (бекдора). При припущенні стандартного сценарію без OverWatch, поки що атака лишається непоміченою.

- *Етап 2: Розвідка та поширення в мережі.* Отримавши початковий плацдарм, хакери починають розвідку: з компрометованого сервера вони сканують внутрішню мережу, шукають інші машини, відкриті шари SMB, намагаються переслати свій бекдор на інші системи. Вони знаходять файловий сервер та кілька робочих станцій у тій самій доменній мережі. Їм вдається скористатися тим, що багато користувачів у домені мають адміністративні сесії на своїх ПК і пароль адміністратора домену збережений (можливо, вони витягують хеші паролів за допомогою MimiKatz). Зрештою, зловмисники захоплюють контроль ще над 5 машинами, серед яких – один контролер домену (дуже поганий розвиток подій для компанії). Дії Falcon на цьому етапі: Шкідлива активність стає більш інтенсивною, і Falcon починає видавати перші тривожні дзвіночки. Наприклад, при запуску утиліти Mimikatz для вилучення паролів Falcon Sensor на контролері домену розпізнає її як відому malicious-tool і блокує виконання (Mimikatz має відомий підпис, а поведінка – доступ до пам’яті LSASS – явно підозріла). Оператор BlackWolf помічає, що Mimikatz впав, але йому вдалося витягти частину даних до блокування. Falcon генерує сповіщення “Credential Dumping attempt blocked” на контролері. У консолі SecOps AlphaCorp в цей момент з’являється попередження високого рівня. Якщо їх SOC моніторить 24/7, вони вже можуть почати реагувати – перевіряти, що сталось на тому контролері. Припустимо, вночі нікого не було, і це сповіщення залишилось до ранку. (У реальності, такі критичні алерти зазвичай налаштовують дублювати на пошту, тому ймовірно, хтось би побачив навіть вночі. Але для демонстрації припустимо невеличку затримку.) Далі, зловмисники розгортають на декількох машинах інструмент Cobalt Strike (популярний легально-

протиправний пентестинг інструмент, часто використовуваний злочинцями). Falcon добре вміє детектувати *beacon-активність* Cobalt Strike: він фіксує, що невідомий процес генерує зашифрований трафік на нетиповий зовнішній сервер. Спрацьовує правило IOA/IOC і Falcon видає ще один алерт – "Possible C2 Beacon detected" на двох станціях. Таким чином, до ранку в консолі Falcon вже є кілька серйозних попереджень, хоча основна шифрувальна атака ще не почалась.

- *Етап 3: Активна фаза – запуск ransomware.* Після підготовки (викрадення даних, встановлення бекдорів на багатьох вузлах) група BlackWolf вирішує одночасно запустити свій основний інструмент – програму-вимагач DarkLock – по всіх можливих системах. Вони завантажують на кожну скомпрометовану машину виконуваний файл darklock.exe (власне шифрувальник) і запускають його приблизно синхронно, щоб максимізувати ефект (і ускладнити реагування). І тут повною мірою вступає в дію CrowdStrike Falcon: По-перше, файл darklock.exe на момент запуску жодного разу не зустрічався у цій мережі, але Falcon's ML-аналізатор перевіряє його. Модель визначає з вірогідністю ~95%, що це шкідлива програма (оскільки DarkLock має схожість з іншими відомими ransomware, наприклад, присутні рядки з фразами викупу, використовує функції шифрування з бібліотеки CryptoAPI, характерна секція ресурсів тощо). На двох машинах з п'яти Falcon автоматично блокує виконання darklock.exe ще на старті – тобто там жоден файл не встигає зашифруватись. На інших трьох машинах припустимо, що зловмисники використали модифіковану версію, яку модель пропустила (низька ймовірність, але припустимо найгірше). Там darklock.exe починає свою роботу: він відразу намагається видалити тіньові копії (vssadmin), запустити шифрування документів користувача. Falcon Sensor миттєво виявляє ці дії: правило IOA "Mass file modifications" спрацьовує протягом секунд – агент бачить, що процес відкрив 10 файлів .docx і .xlsx підряд за кілька секунд. Також зафіксовано запуск vssadmin.exe з параметром Delete Shadows. Цих двох ознак досить, щоб Falcon класифікував поведінку як ransomware. Автоматична реакція: На всіх трьох машинах агент виконує команду *"kill process"* стосовно darklock.exe. Процеси шифрувальників завершуються. За цей короткий інтервал (скажімо, 5-10

секунд) вони встигли частково зашифрувати файли в папках “Мої документи” користувачів. Але як тільки їх зупинено, подальша шкода припиняється. Одночасно Falcon ініціює ізоляцію цих систем від мережі (згідно політики, яка була настроєна компанією після отримання попередніх тривожних сигналів). Отже, ті 5 машин (2 заблокували запуск + 3 зупинили під час шифрування) тепер від’єднані від решти мережі. Зловмисники на своєму боці бачать, що вони втратили зв’язок зі своїми бекдорами на більшості хостів. Вони намагаються повторно запустити ransomware через інші машини, але Falcon вже додав хеш darklock.exe до бази блокування – будь-яка спроба запустити той же файл на іншому вузлі негайно блокується. В цей момент команда SOC AlphaCorp вже повністю залучена: їм надійшла серія критичних сповіщень Falcon: “Ransomware behavior detected and prevented on host X, Y, Z”. Вони також отримали (можливо, від OverWatch або власного аналізу) інформацію про попередні кроки атаки, які були виявлені. Тож вони розуміють, що мережа під масштабним нападом, але найгірше (масштабне шифрування) вдалося зупинити.

- *Етап 4: Усунення наслідків та відновлення.* Після стримання атаки, настає фаза відновлення контролю та розслідування. Завдяки Falcon, у AlphaCorp є детальна інформація про кожну дію зловмисників. Аналітики відкривають в консолі CrowdStrike інцидент і бачать повний “дерево” атаки: починаючи з того RDP-підключення (тепер все стало ясно, звідки все почалось), далі дії на сервері, поширення, запуск malicious tools, аж до спроб шифрування. Falcon зібрав і зберіг копії підозрілих файлів (бекдори, сам darklock.exe). Команда безпеки за підтримки IT відділу починає відновлювати системи: перевіряють, які файли були зашифровані на тих трьох машинах – в основному користувацькі документи, які на щастя, можна відновити з резервних копій (в AlphaCorp практикувалось щоденне бекапування на центральний сервер, який нападники не встигли зачепити). Пошкоджені машини перевстановлюються або очищаються: Falcon’s remediation scripts допомагають видалити усі сліди – агенти OverWatch можуть проконсультувати, щоб точно викорінити кожен бекдор. Компанія повідомляє про інцидент та, за необхідності, залучає правоохоронців, передаючи їм артефакти

(Falcon дозволяє експортувати записи журналу). Важливо, що викуп платити не довелося – хоча частина даних була зашифрована, вони були відновлені з копій, а самі зловмисники втратили важелі тиску (їх програма не завдала критичної шкоди, а викрадені дані мінімальні – вони не встигли багато ексфільтрувати, поки їх не виявили). В результаті, інцидент, який міг (продовження) Атака, яка могла спричинити катастрофічні наслідки, була успішно відбита завдяки поєднанню превентивних та детективних можливостей CrowdStrike Falcon. У підсумку втрата даних мінімальна (усі зашифровані файли відновлено з резервних копій), жодні критичні сервіси не постраждали, а зловмисники були витіснені з мережі. Важливим результатом цього кейсу стало підвищення обізнаності керівництва AlphaCorp щодо загрози ransomware і ефективності сучасних засобів захисту: після інциденту компанія вирішила розширити використання EDR на всі сервери, посилити політики паролів та впровадити обов'язкову багатофакторну автентифікацію для віддаленого доступу.

Наведений сценарій, хоча і є гіпотетичним, відображає типову динаміку реальних атак та демонструє, що своєчасне впровадження платформи захисту кінцевих точок на кшталт CrowdStrike дає змогу значно знизити ризики від програм-вимагачів. У наступному підрозділі на основі цього та інших прикладів сформулюємо узагальнені рекомендації для захисту від ransomware.

3.2. Рекомендації щодо впровадження засобів захисту кінцевих точок

На основі проведеного дослідження та аналізу сценарію реагування можна розробити ряд рекомендацій для фахівців з кібербезпеки та IT-підрозділів щодо підвищення рівня захисту кінцевих точок від атак типу ransomware. Нижче подано ключові поради та кращі практики:

- Впровадити сучасне EDR-рішення на всіх критичних кінцевих точках. Традиційний антивірус слід доповнити або замінити на платформу EDR (таку як CrowdStrike Falcon або аналогічні). Вона забезпечить поведінковий моніторинг та швидке реагування на нетипову активність. Обов'язково налаштувати автоматичне

блокування виявлених програм-вимагачів і ізоляцію уражених хостів – це стримає поширення атаки на ранніх стадія.

- Регулярно оновлювати програмне забезпечення та усувати вразливості. Більшість ransomware проникає, експлуатуючи відомі дірки в системах або слабкі паролі. Тому необхідно налагодити процес встановлення патчів для ОС та основних програм на кінцевих пристроях. Особливу увагу – сервісам віддаленого доступу (RDP, VPN): їх потрібно або надійно захистити (VPN, MFA, брандмауери), або відключити, якщо вони не потрібн.
- Використовувати принцип найменших привілеїв і контроль доступу. Користувачі повинні працювати під обліковими записами з обмеженими правами. Адміністративні облікoвки – тільки для спеціальних задач і окремо. Рекомендується впровадити Multi-Factor Authentication (MFA) для доступу до критичних систем і віддалених сервісів. Це значно ускладнить дії зловмисників, навіть якщо вони здобудуть пароль. Також слід забезпечити унікальні надійні паролі для всіх облікових записів (жодних повторних чи простих паролів).
- Налаштувати централізований журналювання та моніторинг (SIEM/SOC). Дані від EDR та інших систем безпеки мають централізовано збиратися і аналізуватися. Якщо ресурсів на власний SOC немає, варто розглянути послуги керованого моніторингу (MDR) або хоча б отримувати критичні сповіщення на відповідальних осіб цілодобово. У разі інциденту реакція повинна бути максимально швидкою – бажано, щоб SOC міг втрутитися протягом хвилин.
- Регулярно робити резервні копії та ізолювати їх від основної мережі. Backup – остання лінія захисту. Необхідно створити політику резервування важливих даних (на файлових серверах, робочих станціях керівництва, тощо) з періодичністю, що відповідає критичності даних (щоденно, щотижнево). Копії слід зберігати офлайн або в середовищі, недоступному з локальної мережі (наприклад, у хмарному сховищі з обмеженим доступом). Це гарантує, що навіть у разі успішної атаки організація зможе відновити інформацію без викупу. Важливо періодично перевіряти цілісність та відновлюваність резервних копій.
- Проводити навчання користувачів з кібергігієни. Людський фактор –

один з основних ризиків. Тому варто регулярно навчати співробітників розпізнавати фішингові листи, небезпечні вкладення, підозрілі посилання. Роз'яснити, що відкривати файли з невідомих джерел або запускати макроси – небезпечно. Тренування повинні бути постійними (щоквартальні короткі курси, розсилки з порадами. Поведінка користувачів – перша лінія оборони, і її зміцнення знижує ймовірність компрометації кінцевої точки.

- Впроваджувати практики "Zero Trust" на рівні мережі та доступу. Зайві зв'язки між сегментами мережі варто обмежити (мікросегментація). Якщо навіть атака трапиться, шкідливий софт не повинен легко пересуватися по всій мережі. Використовувати мережеві екрануючі засоби (брандмауери, мережеві ізолятори) та системи виявлення вторгнень (IDS/IPS) для моніторингу трафіку на предмет команд керування та контролю (C2), які використовують програми-вимагач. Принцип Zero Trust: не довіряти жодному пристрою за замовчуванням, поки він не аутентифікований і не відповідає політикам безпеки. На практиці це означає перевірку кожного доступу, постійний моніторинг аномалій.
- Відпрацьовувати плани реагування на інциденти (IRP) та регулярно проводити навчання. Організація повинна мати чіткий план дій на випадок атаки ransomware. У ньому визначені ролі – хто відключає мережу, хто сповіщає керівництво, хто зв'язується з правоохоронцями, хто відповідає за комунікацію з громадськістю, тощо. Цей план слід тестувати: проводити навчальні *tabletop-exercises* та імітаційні атаки (red team/blue team. Такі вправи допомагають виявити слабкі місця у підготовці та підвищують готовність команди діяти швидко і злагоджено.
- Використовувати розвіддані про загрози та оновлювати захист відповідно до них. Постійно стежити за рекомендаціями авторитетних організацій (CISA, НБУ, CERT-UA тощо) щодо актуальних загроз програм-вимагачів. Використовувати Threat Intelligence в засобах захисту (як у CrowdStrike Falcon) для отримання свіжих IOC/IOA. Це допоможе бути на крок попереду нападників, знаючи їхні нові технік.
- Оцінити економічні аспекти: кіберстрахування та ROI від засобів

захисту. Варто зазначити, що наявність ефективного захисту (EDR, налаштовані процеси) може навіть знизити витрати на кіберстрахування компанії, оскільки страховики враховують зрілість кібербезпеки. Є приклади, коли компанії після впровадження передових засобів знижували свої страхові премії на ~34. Тобто інвестиції у захист кінцевих точок не лише запобігають інцидентам, а й фінансово виправдані.

Зібрані рекомендації узгоджуються з порадами експертів та офіційними гідами (наприклад, “10 Tips to Prevent Ransomware” від CrowdStrik та спільними матеріалами CISA/MS-ISA). Їх впровадження комплексно підвищить стійкість організації до атак програм-вимагачів. Важливо усвідомити, що не існує одного чарівного засобу: потрібен системний підхід, який поєднує передові технології (такі як CrowdStrike Falcon), добре налагоджені процеси та підготовлений персонал. Лише так можна мінімізувати ризики і втрати від постійно еволюціонуючих кіберзагроз.

ВИСНОВКИ

У дипломній кваліфікаційній роботі проаналізовано проблему захисту кінцевих точок організації від атак типу *ransomware* (програм-вимагачів) та досліджено можливості її вирішення на прикладі сучасної платформи CrowdStrike Falcon. На основі проведеного дослідження можна зробити такі основні висновки:

1. Атаки програм-вимагачів становлять одну з найсерйозніших кіберзагроз сучасності. Вони надзвичайно поширені (до 1/4 всіх інцидентів кібербезпеки у 2023 році були пов'язані з ransomwar) та завдають величезних збитків організаціям по всьому світу (сума виплат викупів у 2023 побила рекорди, перевищивши $1 млрд). Ransomware-атаки еволюціонували: зловмисники застосовують подвійне вимагання (шифрування + викрадення дани), складні багатостадійні тактики проникнення і ухилення від захисту. Це обумовлює актуальність розвитку нових підходів до захисту, особливо на рівні кінцевих пристроїв, де ці атаки безпосередньо реалізуються.

2. Традиційні засоби захисту кінцевих точок (антивіруси) мають обмежену ефективність проти сучасних програм-вимагачів. Вони не встигають за кількістю нових зразків malware та не відслідковують поведінкові аномалії. Для протидії *"невідомим"* атакам потрібно застосовувати поведінковий аналіз, машинне навчання та проактивний моніторинг. Саме тому концепція Endpoint Detection and Response (EDR) стала новим стандартом: EDR-рішення працюють у режимі реального часу, відстежуючи підозрілі дії (IOA) і швидко реагуючи на них. Офіційні рекомендації (CISA, NIST) наголошують на впровадженні EDR та білого списку додатків як одних з ключових засобів захисту від ransomwar.

3. CrowdStrike Falcon – одна з провідних EDR-платформ – пропонує комплексний багаторівневий захист кінцевих точок. Її архітектура (легкий агент + хмарна аналітика Threat Graph) дозволяє масштабовано та швидко обробляти телеметрію, виявляти атаки на ранніх етапах і ділитися розвідданими про загрози між усіма клієнтами. Falcon об'єднує в собі функції наступного покоління

антивірусу (NGAV), поведінкового виявлення (IOA), інтегрованої Threat Intelligence, а також надає можливості миттєвого реагування (блокування процесів, ізоляція хостів) і навіть залучає команду експертів 24/7 (OverWatch) для пошуку прихованих загро. Всі ці компоненти працюють узгоджено, що продемонструвало високу ефективність: за незалежними тестами, CrowdStrike Falcon досягає 100% результативності у виявленні та зупинці атак програм-вимагачі.

4. Механізми Falcon проти ransomware охоплюють весь цикл атаки. Система може попередити виконання шкідливого коду за допомогою ML-моделей (блокуючи нові зразки до запуску), а якщо той запустився – впізнати характерні дії (шифрування файлів, вимкнення резервних копій) і автоматично припинити проце. Завдяки цьому зводяться до мінімуму збитки – шифрування зупиняється після кількох файлів замість тисяч. До того ж, Falcon надає деталізовану інформацію для розслідування (ланцюжок дій атакувальника), що допомагає усунути вразливості та не допустити повторення інциденту. Практичний кейс, розглянутий у роботі, підтвердив: впровадження Falcon дозволило нейтралізувати складну багатостадійну атаку, уникнути виплати викупу і швидко відновити роботу компанії. Без такого засобу атака могла б мати катастрофічні наслідки.

5. Для ефективного захисту від ransomware важливий комплексний підхід. Використання передового рішення такого як CrowdStrike Falcon значно підсилює оборону, але його треба доповнювати організаційними заходами. Необхідно впроваджувати політику *“глибоко ешелонованого захисту”*: регулярні резервні копії (offline), суворий контроль доступу (MFA, найменші привілеї), навчання персоналу, сегментація мережі, плани реагування на інциденти. Тільки поєднання технологій, процесів і людської підготовки створює надійний щит.

6. Практичні рекомендації, розроблені в роботі, можуть бути впроваджені в організаціях для посилення захисту кінцевих точок. До них належать: вибір та розгортання EDR-платформи, налаштування автоматизованого реагування на інциденти, удосконалення кібергігієни користувачів, моніторинг та аналіз логів, регулярне тестування планів реагування тощо. Виконання цих рекомендацій здатне суттєво знизити ймовірність успішної атаки програм-вимагачів або щонайменше

обмежити її вплив на діяльність організації до прийнятного мінімуму.

Загальний висновок: захист кінцевих точок від атак типу ransomware можливий лише за умови проактивного, багаторівневого підходу із залученням сучасних технологічних рішень. CrowdStrike Falcon є яскравим прикладом такого рішення, що продемонструвало високу результативність проти програм-вимагачів на практиці. Однак, незалежно від вибору конкретного інструменту, організаціям слід дотримуватися принципу постійної кіберготовності: *“попередити, виявити, реагувати та відновитися”*. Лише тоді вони зможуть впевнено протистояти викликам, які несуть програми-вимагачі та інші сучасні кіберзагрози.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cybersecurity and Infrastructure Security Agency (CISA), **“#StopRansomware Guide”**, May 2023. (Оновлене керівництво з запобігання та реагування на атаки програм-вимагачів https://www.cisa.gov/stopransomware/ransomware-guide#:~:text=Ransomware%20is%20a%20form%20of,of%20extortion%20without%20employing%20ransomware

2. Tahir B., “A Ransomware Playbook Aligned with NIST SP 800–61”, *Medium*, Oct. 2023. (Стаття з оглядом інцидентів ransomware у 2023 році та рекомендаціями https://medium.com/@tahirbalarabe2/a-ransomware-playbook-aligned-with-nist-sp-800-61-123750c2453d

3. Chainalysis Team, “Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline”, Feb. 2024. (Аналітичний звіт про рекордні обсяги викупів у криптовалюті в 2023 р https://www.chainalysis.com/blog/ransomware-2024/#:~:text=Ransomware%20payments%20in%202023%20surpassed,the%20business%20over%20%24100%20million

4. NIST Interagency Report (IR) 8374 Rev.1 (Draft), “Ransomware Risk Management: A Cybersecurity Framework Profile”, Jan. 2025. (Проект профілю кібербезпеки для протидії ransomware; автори: M. Souppaya et al., NIST https://doi.org/10.6028/NIST.IR.8374r1.ipd

5. CrowdStrike, “Comprehensive Ransomware Protection – CrowdStrike Falcon”, *CrowdStrike Solutions*, 2024. (Офіційний опис можливостей Falcon щодо захисту від програм-вимагачів: https://www.crowdstrike.com/en-us/platform/endpoint-security/ransomware-protection/#:~:text=Proven%20protection

6. CrowdStrike, “CrowdStrike named a Leader by Gartner in 2024 Magic Quadrant for Endpoint Protection Platforms”, *Press Release*, Dec. 2024. (Повідомлення про визнання Falcon лідером квадранту Gartner; 5-й рік поспіль https://www.crowdstrike.com/en-us/resources/reports/gartner-mq/#:~:text=A%20Five

7. CrowdStrike, “Falcon Endpoint Detection & Response (EDR) – Service Description”, *G-Cloud 14 Documents*, May 2024. (Технічний опис архітектури та можливостей Falcon; хмарна платформа, агент, Threat Graph https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-14/documents/718117/259554352326676-service-definition-document-2024-05-07-1101.pdf#:~:text=intelligent%20agent,real%20time%20across%20the%20globe

8. WebAsha Technologies, “Cracking the Code: How CrowdStrike Falcon Uses Cloud-Native AI and Real-Time Threat Intelligence to Prevent Ransomware Attacks”, Blog, Apr. 2025. (Огляд технічних переваг Falcon проти ransomware, приклад з охороною здоров’я https://www.webasha.com/blog/cracking-the-code-how-crowdstrike-falcon-uses-cloud-native-ai-and-real-time-threat-intelligence-to-prevent-ransomware-attacks#:~:text=2,Learning

9. CrowdStrike, “CrowdStrike Falcon Platform Achieves Perfect Score in SE Labs’ Most Comprehensive Ransomware Evaluation”, *CrowdStrike Blog*, Oct. 2024. (Блог про результати тестування SE Labs: Falcon досяг 100% захисту від програм-вимагачів

https://www.crowdstrike.com/en-us/platform/endpoint-security/ransomware-protection/#:~:text=Proven%20protection

10. CISA & MS-ISAC, “Joint Ransomware Guide (2020, updated 2023)”, *StopRansomware Initiative*, 2023. (Спільний посібник Федеральних агентств США щодо захисту від ransomware; найкращі практики та чеклісти) https://www.cisa.gov/stopransomware/ransomware-guide#:~:text=as%20business%20email%20compromise%20%28BEC%29,tune

11. CrowdStrike, “CrowdStrike Named a Leader and Outperformer in 2024 GigaOm Radar for Ransomware Prevention”, *CrowdStrike Blog*, Jul. 2024. (Звіт про визнання Falcon лідером серед засобів захисту від ransomware за версією GigaOm

https://www.crowdstrike.com/en-us/platform/endpoint-security/ransomware-protection/#:~:text=Named%20a%20Leader%20and%20Outperformer

12 Carl Baron (CISO, Euro Construction Corp.), Testimonial in CrowdStrike Ransomware Case Study, 2023. (“...Two CrowdStrike-protected devices detected the

attack and alerted us... prevented the ransomware from spreading...” – досвід реального клієнта https://www.crowdstrike.com/en-us/platform/endpoint-security/ransomware-protection/#:~:text=%3E%20%20%E2%80%9CThe%20two%20CrowdStrike,Carl%20Baron%2C%20CISO%20Image

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)