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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія виявлення та реагування мережевих атак на основі XDR»

зі спеціальності *125 Кібербезпека та захист інформації*
(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

_____ Олександр ОЛЕЙНИКОВ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
ОЛЕЙНИКОВ Олександр
(прізвище, ім'я)

Керівник д.ф., МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 65 сторінок, 50 рисунків, 1 таблиця, 18 джерел.

Об'єкт дослідження – виявлення та реагування на мережеві атаки.

Предмет дослідження – технологія виявлення та реагування на мережеві атаки на основі CrowdStrike Falcon Insight XDR.

Мета роботи – розробити варіант технології виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR та рекомендації щодо її застосування.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, аналіз наслідків та загроз, тестування технології виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR.

В роботі проведено аналіз питання, щодо необхідності виявлення та реагування на мережеві атаки та проаналізовано потенційні наслідки відсутності систем виявлення та реагування на мережеві атаки.

Досліджено методи та засоби виявлення та реагування на мережеві атаки.

Запровоновано варіант технології виявлення та реагування на мережеві атаки на основі CrowdStrike Falcon Insight XDR та розроблено рекомендації щодо застосування даної технології. Визначено призначення, основні функції та склад компонентів даної технології.

На основі проведених досліджень, в роботі отримано варіант технології виявлення та реагування на мережеві атаки на основі CrowdStrike Falcon Insight XDR.

Галузь використання – кібербезпека організації.

XDR, МЕРЕЖЕВІ АТАКИ, ВИЯВЛЕННЯ ТА РЕАГУВАННЯ, МЕТОДИ ТА ЗАСОБИ, ТЕХНОЛОГІЯ, РЕКОМЕНДАЦІЇ, АРХІТЕКТУРА, МОДУЛІ, ФУНКЦІЇ

ABSTRACT

Text part of the master's qualification work: 65 pages, 50 figures, 1 table, 18 sources.

The purpose of the work is to develop a variant of the technology for detecting and responding to network attacks based on CrowdStrike Falcon Insight XDR and recommendations for its use.

Object of research - detection and response to network attacks.

Subject of research - technology for detecting and responding to network attacks based on CrowdStrike Falcon Insight XDR

Research methods - studying the literature on this topic, analyzing operational documentation, analyzing the consequences and threats, testing the technology for detecting and responding to network attacks based on CrowdStrike Falcon Insight XDR.

The paper analyzes the need to detect and respond to network attacks and analyzes the potential consequences of the lack of network attack detection and response systems.

The methods and means of detecting and responding to network attacks are investigated.

A variant of the technology for detecting and responding to network attacks based on CrowdStrike Falcon Insight XDR is proposed and recommendations for the use of this technology are developed. The purpose, main functions and composition of the components of this technology are determined.

Based on the research, a variant of the technology for detecting and responding to network attacks based on CrowdStrike Falcon Insight XDR is obtained.

The field of use is the cybersecurity of an organization.

XDR, NETWORK ATTACKS, DETECTION AND RESPONSE, METHODS AND MEANS, TECHNOLOGY, RECOMMENDATIONS, ARCHITECTURE, MODULES, FUNCTIONS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

NDR	—	Network Detection and Response
NTA	—	Network Traffic Analysis
DDoS	—	Distributed Denial of Service
XDR	—	Extended Detection and Response
EDR	—	Endpoint Detection and Response
SIEM	—	Security Information and Event Management
IoAs	—	Indicators of Attacks
IOCs	—	Indicators of Compromise
ШПЗ	—	шкідливе програмне забезпечення
ОС	—	операційна система
ML	—	Machine Learning
GDPR	—	General Data Protection Regulation
UEBA	—	User and Entity Behavior Analytics

ВСТУП

Актуальність дослідження.

Перехід організацій на гібридні та хмарні середовища створив новий рівень складності для забезпечення безпеки. Класичні інструменти кіберзахисту не пристосовані до розподілених інфраструктур, де кінцеві точки, сервери, та мережеві ресурси можуть бути розташовані в різних частинах світу. CrowdStrike Falcon Insight XDR вирішує ці виклики, забезпечуючи масштабований та централізований підхід до безпеки [1].

Falcon Insight XDR інтегрується з хмарними платформами, такими як AWS, Microsoft Azure та Google Cloud, що дозволяє безперервно моніторити активність у цих середовищах. Завдяки цьому можна швидко ідентифікувати підозрілі дії, наприклад, спроби несанкціонованого доступу або ексфільтрації даних із хмарних серверів.

Ще однією ключовою функцією є підтримка гібридних середовищ, які поєднують локальні та хмарні ресурси. Falcon Insight XDR об'єднує всі ці елементи в єдину систему моніторингу, що дозволяє командам безпеки отримувати повну картину активності та швидко реагувати на загрози. Наприклад, у випадку компрометації кінцевої точки в локальній мережі, система автоматично перевірить, чи не відбулося перенесення загрози на хмарну інфраструктуру [1].

Цей підхід особливо цінний для організацій із динамічними середовищами, такими як стартапи чи міжнародні корпорації, де гнучкість і масштабованість є ключовими. Falcon Insight XDR дозволяє зменшити ризики, пов’язані з кібератаками, та забезпечити відповідність стандартам безпеки навіть у найскладніших середовищах [1].

Тому тема кваліфікаційної роботи «Технологія виявлення та реагування мережевих атак на основі XDR» є актуальною.

Об'єкт дослідження – виявлення та реагування на мережеві атаки.

Предмет дослідження – технологія виявлення та реагування на мережеві атаки на основі CrowdStrike Falcon Insight XDR

Мета роботи – розробити варіант технології виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR та рекомендації щодо її застосування.

Наукові завдання:

- провести аналіз питання, щодо необхідності виявлення та реагування на мережеві атаки;
- проаналізувати потенційні наслідки відсутності систем виявлення та реагування на мережеві атаки;
- дослідити методи та засоби виявлення та реагування на мережеві атаки;
- розробити варіант технології виявлення та реагування на мережеві атаки на основі CrowdStrike Falcon Insight XDR та рекомендації щодо застосування даної технології. Визначити призначення, основні функції та склад компонентів даної технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, аналіз наслідків та загроз, тестування технології виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR.

Практичне значення одержаних результатів полягає в розробці технології виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR та рекомендації щодо застосування даної технології.

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

1 АНАЛІЗ НЕОБХІДНОСТІ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ МЕРЕЖЕВИХ АТАК

1.1. Аналіз необхідності виявлення та реагування на мережеві атаки

Технологія мережевого виявлення та реагування (NDR) з'явилася на початку 2010-х років для виявлення та зупинки мережевих загроз, які не можна легко заблокувати за допомогою відомих шаблонів атак або сигнатур. Технологія NDR, яку також називають аналізом мережевого трафіку (NTA), використовує машинне навчання і поведінкову аналітику для моніторингу мережевого трафіку і розробки базової лінії активності. Потім вони виявляють аномальну активність, пов'язану зі шкідливим програмним забезпеченням, цілеспрямованими атаками, інсайдерськими зловживаннями і ризикованою поведінкою. NDR дозволяють організаціям розпізнавати незвичайний трафік, який вказує на командування і контроль, латеральне переміщення, проникнення і активність шкідливого програмного забезпечення. Вони аналізують трафік між внутрішніми хостами та інтернетом, але також перевіряють трафік між внутрішніми хостами, включаючи внутрішні сервери, для точного виявлення атак [2].

Згідно з даними дослідження [3] розподіл атак – червень 2024 припадає:

1. Malware (21.3%)

Malware (шкідливе програмне забезпечення) — це будь-яке програмне забезпечення, створене для пошкодження, порушення роботи або отримання несанкціонованого доступу до комп'ютерних систем. До шкідливого ПЗ відносяться віруси, трояни, черв’яки, руткіти та шпигунські програми. Malware може викрасти конфіденційні дані, пошкодити файли або використовувати ресурси системи для атак.

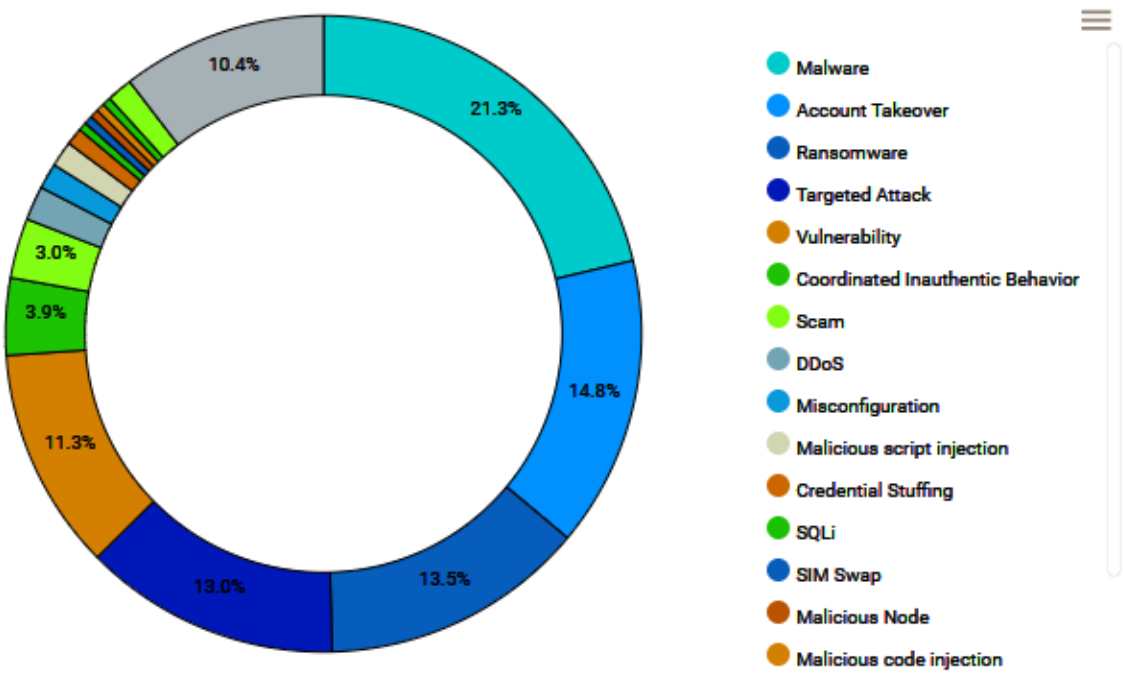

Рис. 1.1. Розподіл атак – червень 2024 згідно з [3]

2. Account Takeover (14.8%)

Account Takeover (перехоплення облікового запису) — це тип атаки, під час якого зловмисник отримує контроль над чужим обліковим записом, зазвичай через викрадені або вкрадені дані для входу. Після захоплення облікового запису зловмисник може використовувати його для доступу до особистих даних, здійснення фінансових транзакцій або розповсюдження шкідливого програмного забезпечення.

3. Ransomware (13.5%)

Ransomware — це тип шкідливого ПЗ, що блокує або шифрує файли користувача, вимагаючи викуп за їхнє розблокування. Ransomware-атаки часто націлені на організації, оскільки такі атаки можуть паралізувати операційну діяльність, змушуючи жертву заплатити викуп у криптовалюті, щоб уникнути втрати важливих даних [1-3].

4. Targeted Attack (13.0%)

Targeted Attack (цілеспрямована атака) — це складна та продумана атака, орієнтований на конкретну організацію, особу або систему. На відміну від

випадкових атак, цільові атаки проводяться з конкретними намірами, такими як викрадення конфіденційної інформації або порушення роботи певних систем.

5. Vulnerability (11.3%)

Vulnerability (уразливість) — це слабке місце в системі або програмному забезпеченні, яке використовують зловмисниками для отримання несанкціонованого доступу або виконання шкідливих дій. Уразливості можуть бути спричинені помилками в коді, неправильними налаштуваннями або навіть людськими помилками.

6. Coordinated Inauthentic Behavior (3.9%)

Coordinated Inauthentic Behavior — це організована діяльність, спрямована на маніпуляцію громадською думкою або створення неправдивих даних. Це часто пов’язане з поширенням фальшивих новин або масовим використанням ботів для дезінформації. Такі дії використовуються як частина соціальної інженерії для розповсюдження шкідливого контенту [1-3].

7. Scam (3.0%)

Scam (шахрайство) — це спроба обману, коли зловмисники обманом змушують жертву відправити їм гроші, надати конфіденційну інформацію або виконати певні дії. Це можуть бути фішингові атаки, шахрайство в електронній комерції або інші методи обману.

8. DDoS (10.4%)

DDoS (Distributed Denial of Service) — це тип атаки, при якій велика кількість запитів надіслана до сервера з багатьох пристроїв, що спричиняє його перевантаження і унеможливлює надання послуг користувачам. DDoS-атаки використовуються для порушення роботи веб-сайтів, мереж і систем [1-3].

9. Misconfiguration

Misconfiguration (неправильна конфігурація) — це налаштування системи або програмного забезпечення з порушеннями безпеки, що відкриває доступ до внутрішніх даних. Такі налаштування можуть включати відкриті порти, неправильні налаштування доступу або залишення даних у незахищеному вигляді.

10. Malicious Script Injection

Malicious Script Injection (ін'єкція шкідливого коду) — це метод атаки, коли зловмисники впроваджують шкідливий код у веб-сторінку або програму. Це може призвести до виконання коду від імені користувача, крадіжки інформації або поширення шкідливого ПЗ. Прикладами таких атак є XSS та SQL ін’єкції.

11. Credential Stuffing

Credential Stuffing — це метод атаки, коли зловмисник використовує масиви зламаних облікових даних для автоматизованого входу в системи. Оскільки багато людей використовують однакові паролі для різних сервісів, зловмисники можуть успішно отримати доступ до кількох акаунтів [1-3].

12. SQL Injection (SQLi)

SQL Injection (SQLi) — це тип атаки на бази даних, коли зловмисник вводить шкідливі SQL-запити в поля введення. Це дозволяє їм отримати доступ до конфіденційних даних, змінювати або видаляти інформацію в базі даних, що становить значну загрозу для безпеки веб-додатків.

13. SIM Swap

SIM Swap — це атака, в якій зловмисники перемикають номер телефону жертви на інші SIM-карти, що дозволяє їм отримати доступ до облікових записів жертви, особливо якщо вони захищені двофакторною автентифікацією через SMS.

14. Malicious Node

Malicious Node (шкідливий вузол) — це пристрій або система, яка включена в мережу з метою збору даних або розповсюдження шкідливого програмного забезпечення. Такі вузли можуть бути частиною ботнетів або використовуватися для шпигунства [1-3].

15. Malicious Code Injection

Malicious Code Injection (ін'єкція шкідливого коду) — це метод введення шкідливого коду в систему або додаток, який дозволяє зловмисникам отримати доступ або маніпулювати даними. Ін'єкція шкідливого коду може використовуватися для крадіжки даних, викрадення сеансів або знищення даних.

Тому, Дані свідчать, що поширеними типами атак у червні 2024 року були шкідливе ПЗ (21.3%), перехоплення облікових записів (14.8%), програми-вимагачі (13.5%) і цілеспрямовані атаки (13.0%). Ці загрози можуть порушити роботу систем, викрасти конфіденційні дані та завдати значних фінансових збитків.

Захист мережі від атак є критично важливим для забезпечення стабільної роботи організацій, захисту конфіденційної інформації та зменшення потенційних втрат.

1.2. Класифікація мережевих атак та їх вектори

З цифровою трансформацією загалом (і розширенням цифрового робочого місця зокрема) світ зіткнувся зі збільшенням кількості кібератак у різних формах і видах. Простіше кажучи, вони полягають у навмисному використанні комп'ютера для виведення з ладу або пошкодження системи, мережі, програми чи даних. Вони можуть відбуватися різними способами і можуть бути здійснені будь-ким, хто має доступ до Інтернету. Наслідки кібератаки можуть варіюватися від дрібних неприємностей до великих катастроф, залежно від того, що було атаковано і наскільки серйозно це було зроблено [4].

Модель мережевих комунікацій OSI складається з 7 рівнів. Кожен рівень відповідає за певний процес, що забезпечує надійний зв'язок між двома або більше пристроями. Коли створювався Інтернет, основна увага приділялася забезпеченню надійного зв'язку. Проблеми безпеки комунікацій з'явилися пізніше. Ці 7 рівнів діють як ланцюг з ланок. Якщо одна ланка розривається, розривається весь ланцюг комунікації. Таким чином, загроза безпеці може виникнути на будь-якому з 7 рівнів. Ці рівні називаються прикладним, презентаційним, сеансовим, транспортним, мережевим, канальним і фізичним. Прикладний рівень - це ваша поштова програма, фізичний рівень - це ваш кабель зв'язку, а все інше, що знаходиться між ними, допомагає вам спілкуватися [5].

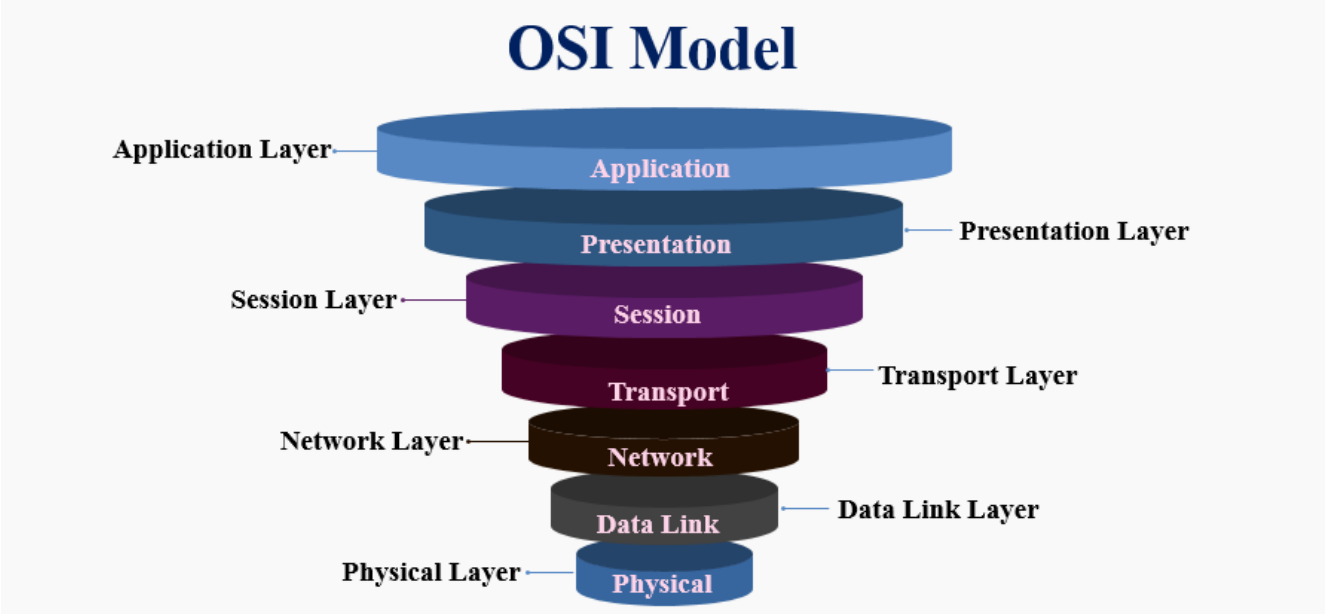

Рис. 1.2. Модель OSI [6]

Абстрактно кажучи, прикладний рівень забезпечує користувацький інтерфейс, тоді як рівень представлення відповідає за форматування, кодування та шифрування. Сеансовий рівень керує з'єднаннями. Транспортний рівень відповідає за сегментацію, послідовність і створення віртуальних каналів. Мережевий рівень забезпечує логічну мережеву адресацію та маршрутизацію, тоді як канальний рівень забезпечує кадрування та розміщення даних у мережевому середовищі. Нарешті, фізичний рівень кодує 1 і 0 в цифровий сигнал для передачі. Коли користувач вводить повідомлення на прикладному рівні, воно рухається назовні через презентацію, сеанс, транспорт, мережу, канал передачі даних до фізичного рівня, де перетворюється на пакет даних, що складається з одиниць та нулів. Потім він прямує до місця призначення по дроту. Нарешті, переходить з фізичного рівня на прикладний, щоб представити повідомлення одержувачу [5].

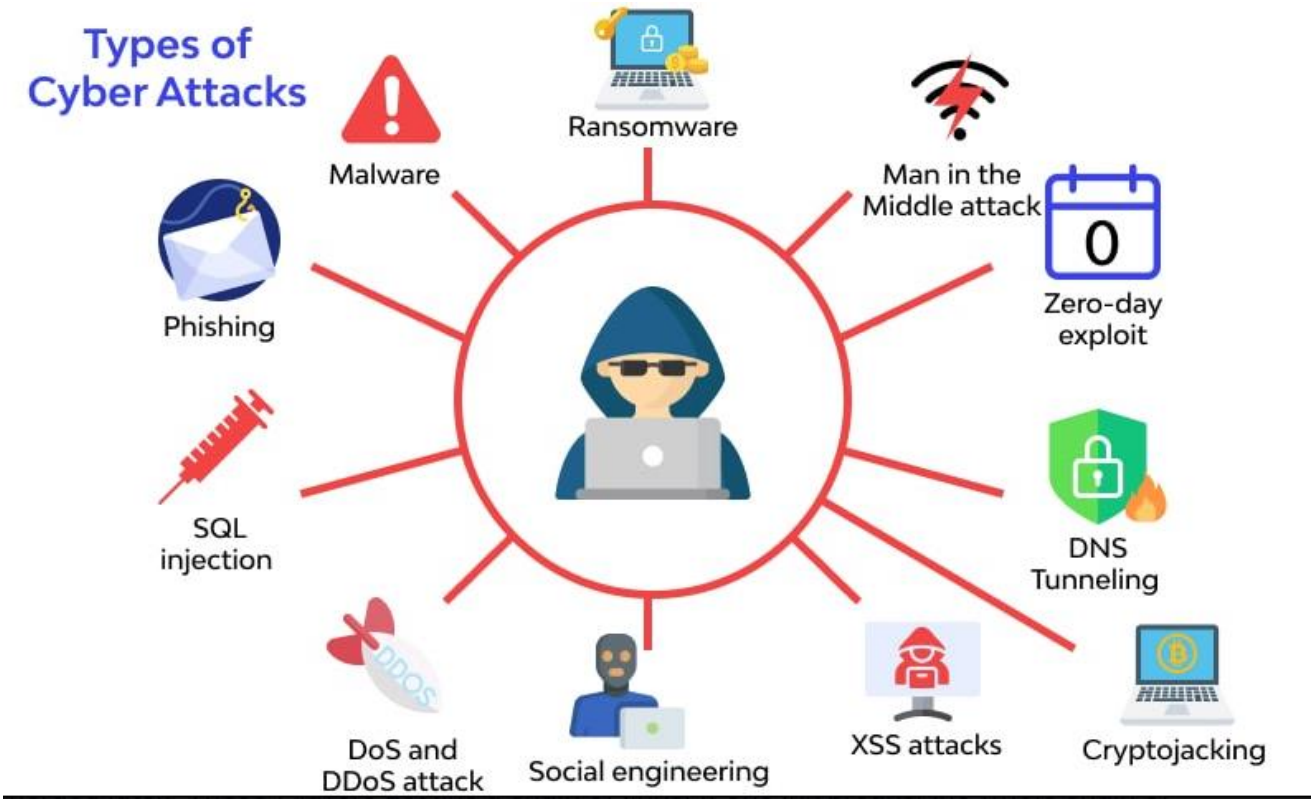

Рис. 1.3. Типи кібератак на мережу

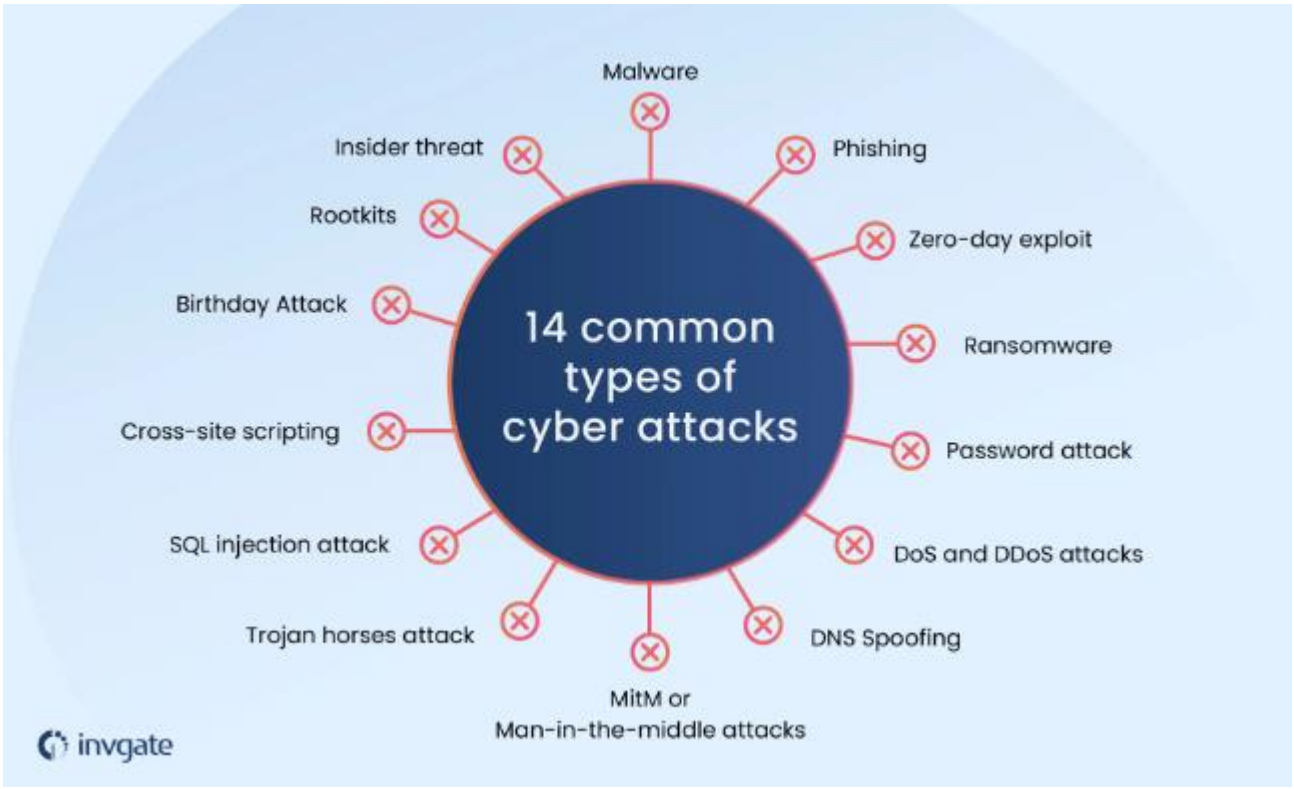

Рис. 1.4. 14 найпоширеніших видів кібератак [5]

Загрози на рівні додатків:

Загрози комунікації починаються на рівні додатків. Це найбільш вразливий рівень, оскільки користувачі взаємодіють з мережею за допомогою різних додатків. Люди можуть спричинити дорогі помилки через притаманні їм слабкості, якими можуть скористатися хакери за допомогою соціальної інженерії та шкідливих програм. Програми-вимагачі, віруси, трояни, черв'яки, руткіти, бекдори та різні види фішингових атак можуть статися через недбалість користувачів. Нещодавня атака на Uber була ініційована через WhatApp.Крім того, кіберзлочинці можуть здійснювати розподілені атаки на відмову в обслуговуванні (DDoS), HTTP-флуди, SQL-ін'єкції, міжсайтовий скриптинг, підміну параметрів, XSS-атаки, клавіатурні шпигуни, експлойти нульового дня, помилки в програмному забезпеченні на рівні додатків. Тому прикладний рівень є найскладнішим для захисту. Зловмисники знають, що користувачі - це найкращий шлях для проникнення в мережу. Безпечне програмне забезпечення, брандмауери веб-додатків (WAF) та безпечні послуги веб-шлюзів можуть допомогти пом'якшити деякі атаки. Однак, навчання користувачів є найбільш важливим фактором для захисту від атак, спрямованих на прикладний рівень. Тому моніторинг прикладного рівня є вкрай важливим для своєчасного виявлення атак та зменшення ризиків [5].

Загрози на рівні представлення:

Цей рівень виконує форматування, перетворення та шифрування даних. Зловмисники шукають недоліки шифрування на цьому рівні. Перехоплення SSL або прослуховування за допомогою атаки "зловмисника посередині" (MitM) є поширеним явищем на рівні представлення. Зловмисник спочатку встановлює шкідливе програмне забезпечення на комп'ютер жертви і використовує його в якості проксі-сервера, який виконує функції ненадійного центру сертифікації. Браузер жертви буде довіряти неправильному центру сертифікації, що дозволить зловмиснику читати передані повідомлення. Найкраще рішення - не допустити потрапляння шкідливого програмного забезпечення на ваш пристрій, переконавшись, що ваш антивірусний захист оновлений. Неправильно сформовані SSL-запити належать до найпоширеніших загроз на рівні представлення.

Загрози сеансового рівня:

Цей рівень встановлює сеанс з'єднання для забезпечення зв'язку між двома додатками. Перехоплення сеансу, крадіжка файлів cookie та інші атаки відбуваються на цьому рівні через міжсайтовий скриптинг. Використовуйте HTTPS-з'єднання для забезпечення наскрізного шифрування та запобігання доступу до файлів cookie з боку клієнтських скриптів, а також регенеруйте сеансовий ключ після встановлення автентифікації. Використовуйте SFTP замість FTP, щоб запобігти прослуховуванню FTP [5].

Загрози транспортного рівня:

Роль цього рівня полягає в управлінні передачею даних. Він використовує орієнтований на встановлення з'єднання протокол управління передачею (TCP) і протокол користувацьких дейтаграм (UDP) для передачі даних без встановлення з'єднання. Транспортний рівень розбиває дані, передані канальним рівнем, на пакети різного розміру перед передачею. Транспортний рівень схильний до атак на порти і протоколи. Він також страждає від розподілених атак на відмову в обслуговуванні (DDoS), таких як SYN-флуд і Smurf-атаки. Рішення - налаштувати брандмауер на закриття невикористовуваних портів. Використовуйте захист на транспортному рівні (TLS) для захисту всього обміну даними між веб-сервером і браузерами, включно з миттєвими повідомленнями, електронною поштою та голосовим зв'язком за допомогою IP-телефонії [5].

Загрози мережевого рівня:

Мережевий рівень взаємодіє з мережею за допомогою маршрутизаторів. Маршрутизатори забезпечують переміщення пакетів даних.Отримавши пакет з транспортного рівня, він додає до нього адресу інтернет-протоколу (IP-адресу) і вказує пакету, куди йти. Мережевий рівень відстежує пакети і керує всім трафіком за допомогою протоколів IPv4 і IPv6. Найпоширеніші атаки на мережевому рівні пов'язані з маршрутизаторами. Вони включають в себе розвідку, прослуховування, підміну та розподілену відмову в обслуговуванні (DDoS). Захист маршрутизаторів вимагає правильних налаштувань маршрутизатора та брандмауера. Використовуйте брандмауери між вашою мережею та іншими мережами.

Переконайтеся, що в операційній системі вашого маршрутизатора встановлені всі патчі безпеки. Вимкніть усі невикористовувані інтерфейси, заблокуйте невикористовувані порти та увімкніть фільтрацію пакетів, а також проводьте регулярний аудит з реєстрацією даних [5].

Загрози канального рівня:

На цьому рівні нулі та одиниці передаються між фізично з'єднаними вузлами через дроти або бездротове середовище. Канальний рівень стежить за помилками при передачі даних. Цей рівень складається з двох підрівнів, де підрівень керування доступом до середовища (MAC) є унікальним ідентифікатором пристрою, а підрівень керування логічним з'єднанням (LLC) є інтерфейсом між пристроєм і мережевим рівнем.Підрівень LLC відповідає за мультиплексування протоколів мережевого рівня. Підрівень MAC відповідає за фізичну адресацію.Канальний рівень відповідає за надійну передачу кадрів по фізичному каналу з повідомленням про помилки, впорядковану доставку кадрів і управління потоком.Кожен кадр має заголовок, тіло і трейлер.Зловмисники можуть переглядати або маніпулювати цими кадрами, щоб скомпрометувати ваші дані. Зловмисники здійснюють підміну MAC-адрес, переповнення MAC-адрес, широкомовні шторми, обхід віртуальних локальних мереж (LAN), а також ARP-отруєння та DHCP-атаки.

Загрози фізичного рівня:

Цей рівень складається з фізичних компонентів або електромагнітних хвиль, які проходять через дроти, кабелі, бездротові з'єднання, маршрутизатори, кінцеві точки, розетки тощо. Для них існують стандарти, які включають час передачі, відстань проходження, рівні напруги тощо. Найпоширенішими загрозами фізичного рівня є людський вандалізм, стихійні лиха, збої в електромережі тощо. Використання відмовостійких і резервних з'єднань, а також джерел безперебійного живлення є заходами пом'якшення наслідків. Концентратори і повторювачі, що працюють на фізичному рівні, бачать лише біти, але інші пристрої працюють на більш високих рівнях. Комутатори та мости - це пристрої канального рівня, які приймають рішення на основі адрес мережевого рівня. Маршрутизатори мають справу з адресами мережевого рівня. Робочі станції працюють на прикладному

рівні, обробляючи протоколи прикладного рівня. Будь-яке фізичне порушення роботи цих рівнів впливає на їхні функції. Кожна мережа, підключена до Інтернету, є потенційним об'єктом для атак на один або кілька рівнів OSI 7, які можуть порушити і вивести з ладу ваші операції. Хороша система управління ризиками інформаційної безпеки може допомогти вам зменшити ці ризики і захистити вашу мережу від вторгнень, а ваші дані - від витоку [5].

Вектор атаки - це шлях або засіб, за допомогою якого зловмисник або хакер може отримати доступ до комп'ютера або мережевого сервера, щоб доставити корисне навантаження або досягти зловмисного результату. Вектори атаки дозволяють хакерам використовувати вразливості системи, в тому числі людський фактор. До поширених векторів кібератак належать віруси і шкідливе програмне забезпечення, вкладення електронної пошти, веб-сторінки, спливаючі вікна, миттєві повідомлення (IM), чати і обман. За винятком обману, всі ці методи пов'язані з програмуванням або, в деяких випадках, з апаратним забезпеченням. Обман - це коли людину-оператора обманом змушують видалити або послабити захист системи. Певною мірою брандмауери та антивірусні програми можуть блокувати вектори атак. Але жоден метод захисту не є повністю захищеним від атак. Метод захисту може швидко застаріти, оскільки хакери постійно оновлюють вектори атак і шукають нові, щоб отримати несанкціонований доступ до комп'ютерів і серверів. Найпоширенішим шкідливим корисним навантаженням є віруси, які можуть функціонувати як власні вектори атак, троянські коні, хробаки та шпигунські програми. Сторонні виробники та постачальники послуг також можуть розглядатися як вектори атаки, оскільки вони становлять ризик для організації, якщо мають доступ до її конфіденційних даних.

Розглянемо різницю між вектором атаки та поверхнею атаки

Ці два терміни часто використовують як взаємозамінні, але це не одне й те саме. Вектор атаки відрізняється від поверхні атаки, оскільки вектор - це засіб, за допомогою якого зловмисник отримує доступ, а поверхня атаки - це те, що атакується. Одним з найбільш відомих хакерських атак була атака на ланцюжок поставок SolarWinds [7]. Було проведено розслідування для визначення векторів

атаки, але порушення могло бути результатом скомпрометованих облікових даних або можливого доступу через середовище розробки програмного забезпечення для управління інформаційними технологіями Orion компанії SolarWinds.

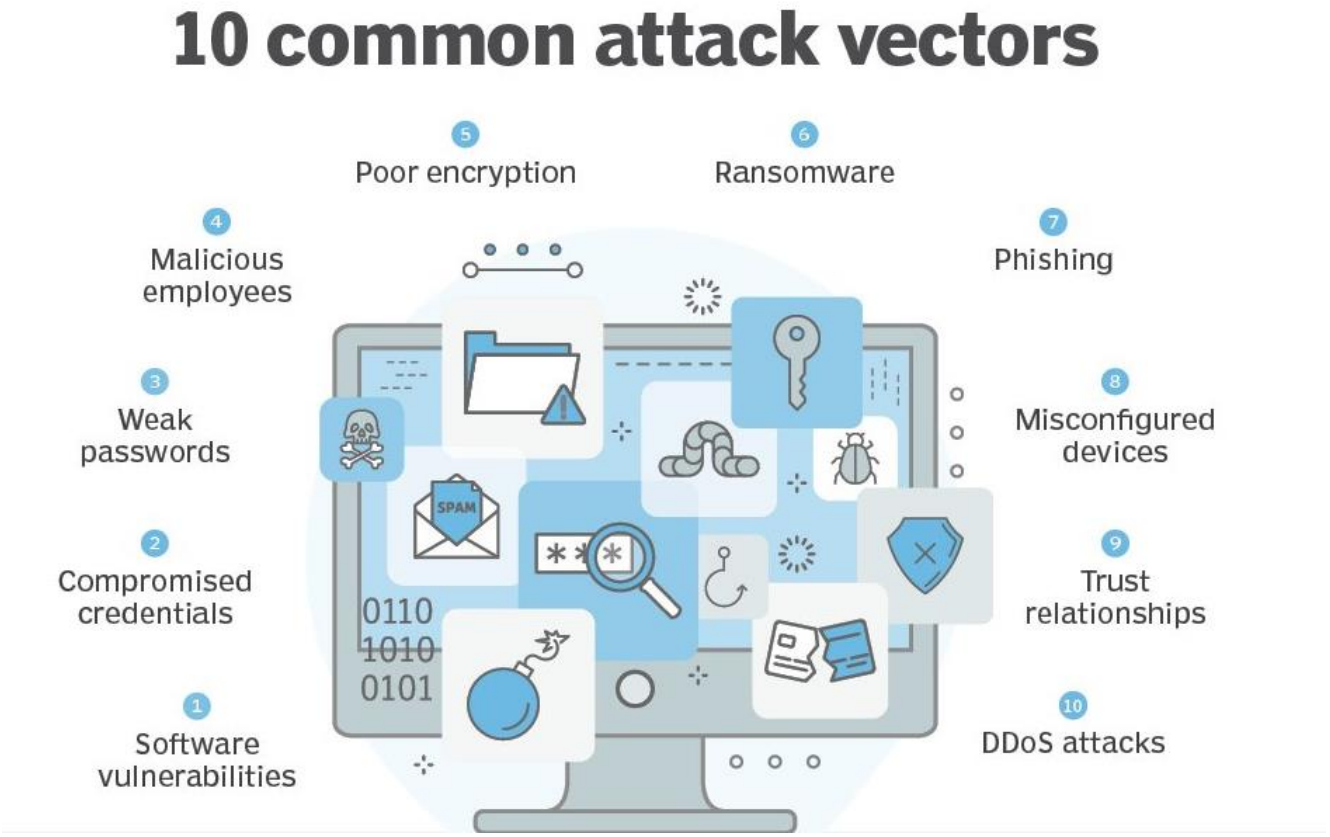

Рис. 1.5. 10 найпоширеніших векторів атак [7]

10 найпоширеніших векторів атак

Зловмисники постійно шукають нові вектори атак. До найпоширеніших векторів атак належать такі:

Вразливості в програмному забезпеченні. Якщо мережа, операційна система, комп'ютерна система або програма має незаплановану вразливість, зловмисник може використати вектор загрози, наприклад, шкідливе програмне забезпечення, щоб отримати несанкціонований доступ [7].

Скомпрометовані облікові дані користувачів. Користувачі можуть свідомо чи ненавмисно ділитися своїми ідентифікаторами та паролями. Це може бути зроблено усно, але кіберзловмисники також можуть отримати доступ до

облікових даних за допомогою атаки грубої сили, яка перебирає різні комбінації ідентифікаторів користувачів і паролів, доки не буде знайдено дозволений набір облікових даних. Потім хакер використовує ці облікові дані для злому мережі, системи або програми.

Слабкі паролі та облікові дані. При атаках грубої сили кіберзловмисники зосереджують свої зусилля на зламі ідентифікаторів користувачів і паролів, які є слабкими або можуть бути легко вгадані. Але хакери також викрадають облікові дані, використовуючи програми, які відстежують публічні мережі Wi-Fi на предмет того, коли користувачі вводять свої облікові дані доступу. Наприклад, хакер може встановити програмне забезпечення для клавіатурного шпигунства на робочу станцію користувача через заражений веб-сайт або електронну пошту. Програма записує дії користувача на клавіатурі, включаючи введення ідентифікатора та пароля. Хакери також можуть отримати доступ, змушуючи користувачів відкривати небажані вкладення електронної пошти, що містять шкідливі посилання на фальшиві веб-сайти, які переконують їх передати особисту інформацію (PII).

Зловмисні працівники. Зловмисні або незадоволені співробітники можуть зламувати мережі та системи, використовуючи свої допуски, щоб отримати конфіденційну інформацію, таку як списки клієнтів та інтелектуальну власність (IP), за яку вони або вимагають викуп, або продають іншим особам у негідних цілях [7].

Погане або відсутнє шифрування. У деяких випадках працівники – або IT-спеціалісти – можуть забути зашифрувати конфіденційну інформацію, що зберігається на ноутбуках і смартфонах у польових умовах. В інших випадках методи шифрування мають відомі недоліки або використовують лише обмежену кількість ключів для шифрування та захисту даних.

Програми-здирники. Вимагачі – це тип шкідливого програмного забезпечення, яке блокує дані на комп’ютері жертви, а зловмисник погрожує опублікувати дані жертви або заблокувати доступ до них, якщо не буде сплачено викуп. Програми-здирники можуть блокувати файли користувача, часто вимагаючи від нього грошову суму для розблокування файлів. Більшість програм-

здирників ненавмисно завантажуються користувачем на комп’ютер або в мережу. Це може бути файл, який користувач відкриває і який містить хробака – шкідливе програмне забезпечення, що поширюється мережею, або троянську програму, яка вбудовує в завантажений файл шкідливий програмний код, що блокує комп’ютер або дані користувача, а потім вимагає оплату [7].

Фішинг – оманлива практика зловмисників, які використовують електронні листи від авторитетних компаній. Фішинг – це оманлива практика надсилання електронних листів, в яких зловмисник видає себе за представника авторитетної компанії, щоб виманити у користувачів особисту інформацію, наприклад, паролі або номери кредитних карток. Списовий фішинг – це вузькоспрямована атака, яка націлена на одного одержувача з метою отримання несанкціонованого доступу до конфіденційної інформації компанії.

Неправильно сконфігуровані пристрої. Компанії можуть неправильно налаштувати захист свого програмного та апаратного забезпечення, що робить їх вразливими для хакерів. Попередні налаштування безпеки на обладнанні є недостатніми, і якщо IT-спеціалісти не переналаштовують це обладнання перед встановленням його в мережі, можуть статися зломи безпеки. В інших випадках компанії купують обладнання і забувають повністю налаштувати безпеку [7].

Довірчі відносини. У багатьох випадках компанії довіряють свою безпеку зовнішнім постачальникам систем і мереж, хмарним провайдерам і бізнес-партнерам. Коли системи цих третіх сторін зламані, інформація, яку отримують хакери, може також містити конфіденційну інформацію компаній, які обслуговуються цими постачальниками. Прикладом може бути злом мережі великого оператора кредитних карток або злом системи охорони здоров’я з викраденням конфіденційних даних пацієнтів.

Розподілені атаки на відмову в обслуговуванні (DdoS) – коли жертви отримують фальшиві електронні листи, що виводять систему з ладу. DdoS-атаки засипають жертв фальшивими електронними листами, роблячи їхню систему або мережу непридатною для використання, а послуги недоступними для їхніх адресатів. Ці атаки часто спрямовані на веб-сервери фінансових, комерційних та

урядових організацій і часто використовуються для відволікання уваги від інших мережевих атак.

1.3. Потенційні наслідки відсутності систем виявлення та реагування на атаки

Кібератаки мають суттєві наслідки для організацій, особливо якщо вони не використовують системи виявлення вторгнень (IDS). Розглянемо детально кожен із наслідків:

2. Втрата конфіденційних даних та інформації.

Компрометація клієнтських даних (наприклад, персональної, фінансової або медичної інформації) може призвести до крадіжки особистості або шахрайства. Втрата конфіденційної бізнес-інформації (інтелектуальної власності, стратегій, угод) може поставити організацію у невигідне становище на ринку. Можливість поширення інформації конкурентами або використання її хакерами для подальших атак [8].

Даний аспект дуже серйозний, оскільки наслідки можуть бути довготривалими і мати ефект доміно, включаючи втрату довіри клієнтів і партнерів.

2. Фінансові втрати.

Кібератаки призводять до значних фінансових втрат через викуп, прямі збитки від втрати даних або перебоїв у роботі бізнесу. Зниження доходів через втрату клієнтів, зупинку операцій або збільшення витрат на ліквідацію наслідків. Штрафи та компенсації клієнтам або партнерам, які постраждали від витоку даних. Інвестиції у відновлення систем та зміцнення кібербезпеки після атаки. Втрати від шахрайських операцій із використанням викрадених даних.

Фінансові втрати можуть бути катастрофічними, особливо для малого та середнього бізнесу, який не має значних резервів для відновлення [8].

2. Репутаційна шкода.

Порушення безпеки завдають шкоди репутації компанії, призводять до втрати довіри клієнтів та партнерів. За собою репутаційна шкода має наслідки:

- Зниження довіри клієнтів до здатності організації захищати їх дані.

- Втрата ділових партнерів, які уникають співпрацю з ненадійною компанією.

- Негативний медійний резонанс та поширення інформації про атаку, що впливає на імідж.

Репутаційна шкода може бути більш тривалою, ніж фінансова, оскільки відновлення довіри вимагає часу, зусиль і фінансових витрат [8].

4. Юридичні наслідки.

Компанії також несуть юридичну відповідальність за порушення безпеки та втрату даних наприклад: порушення вимог законодавства (наприклад, GDPR, HIPAA, PCI DSS) призводить до штрафів, судових позовів або позбавлення ліцензій. Витрати на юридичну допомогу, судові витрати та можливість фінансових компенсацій постраждалим.

Юридичні наслідки серйозно впливають на фінансову стабільність і функціонування компанії, особливо якщо штрафи великі [8].

Отже, відсутність систем виявлення вторгнень значно підвищує ризик серйозних наслідків, оскільки організація не здатна вчасно реагувати на загрози. Це створює ідеальні умови для розвитку атак і суттєво ускладнює процес відновлення. Інвестиції в XDR можуть суттєво знизити ймовірність критичних наслідків, забезпечуючи раннє попередження та відповідь на кіберзагрози.

Висновки до розділу 1

1. Проведено аналіз необхідності виявлення та реагування на мережеві атаки.

2. Приведено класифікацію мережевих атак та векторів атаки.

3. Проаналізовані потенційні наслідки відсутності систем виявлення та реагування на атаки для організації

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ МЕРЕЖЕВИХ АТАК

2.1. Методи та засоби виявлення та реагування на мережеві атаки

В попередньому розділі було наведено класифікацію атак та їх вектори, а для захисту від цих загроз використовуються методи та інструменти виявлення мережевих атак і реагування на них. Ефективна безпека мережі залежить не лише від запобігання атакам, а й від можливості швидко їх ідентифікувати, аналізувати та нейтралізувати. На рис. 2.1. наведені ключові стратегії виявлення та реагування до яких належать: Превентивний захист, Моніторинг і виявлення, Інцидентне реагування та Аналіз загроз.

Рис.2.1. Ключові стратегії виявлення та реагування

1. Превентивний захист це:

- Використання міжмережевих екранів (Firewall) для обмеження несанкціонованого доступу.

- Системи управління доступом (Access Control Systems) для мінімізації ризиків.

2. Моніторинг і виявлення це:

- Застосування систем виявлення вторгнень (IDS) і запобігання вторгненням (IPS), які аналізують мережевий трафік та визначають підозрілу активність або комбіновану модель XDR .

- Використання інструментів аналізу журналів (Log Analysis) для ретроспективного дослідження інцидентів.

3. Інцидентне реагування це:

-Розробка планів реагування на інциденти (Incident Response Plans).

- Автоматизація захисту за допомогою оркестрації (SOAR – Security Orchestration, Automation, and Response).

4. Аналіз загроз це:

- Застосування інструментів Threat Intelligence для збору та аналізу інформації про актуальні загрози.

- Використання моделей поведінки користувачів (UEBA – User and Entity Behavior Analytics) для виявлення відхилень.

Основні методи виявлення атак Рис.2.2.:

Сигнатурний аналіз: базується на порівнянні трафіку з відомими шаблонами (сигнатурами) атак.

Аналіз аномалій: використовує базові моделі нормальної поведінки для виявлення відхилень.

Поведінковий аналіз: ідентифікація атак на основі поведінкових змін в мережі.

Машинне навчання: застосування алгоритмів штучного інтелекту для аналізу великих обсягів даних і виявлення атак, що важко ідентифікувати за традиційними методами.

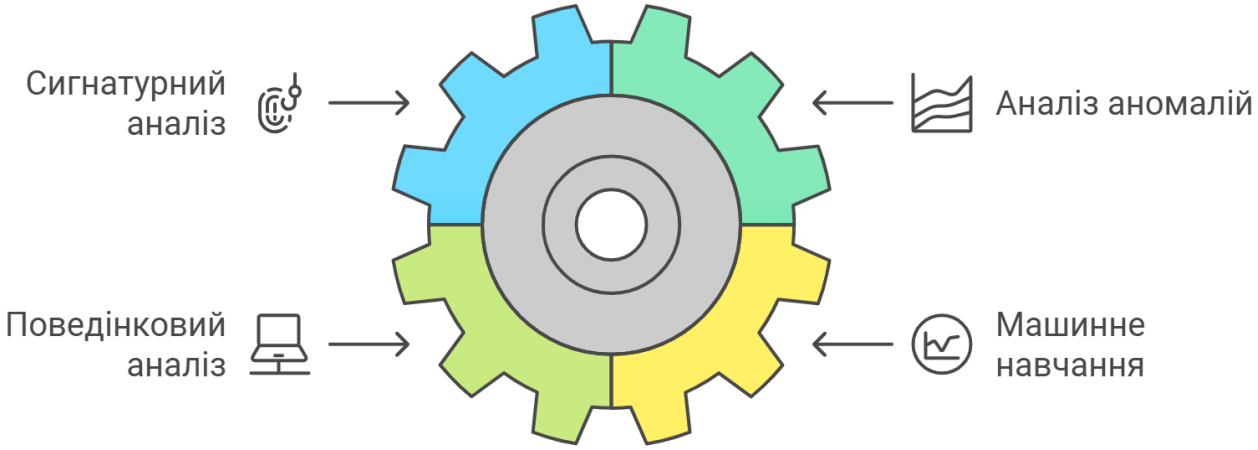

Рис.2.2. Основні методи виявлення атак

Проаналізуємо ключові технології XDR, SIEM та EDR, які використовуються для забезпечення кібербезпеки. Кожна з них має свої унікальні характеристики та призначена для вирішення певних завдань. Розглянемо їх відмінності та схожість [9].

SIEM (Security Information and Event Management)

Системи SIEM збирають та аналізують логи безпеки з різних джерел (мережевих пристроїв, серверів, додатків тощо). Вони дозволяють виявляти аномалії, корелювати події та створювати звіти про безпеку. Фокус SIEM системи орієнтований на збір та аналіз логів, забезпечуючи широку видимість подій у мережі. Системи SIEM можуть генерувати велику кількість помилкових спрацювань та вимагають значних зусиль для налаштування та тонкого налаштування [9].

EDR (Endpoint Detection and Response)

Рішення EDR фокусуються на захисті кінцевих точок (комп'ютерів, ноутбуків, мобільних пристроїв). Вони відстежують активність на пристроях, виявляють шкідливе ПЗ та аномалії, а також дозволяють реагувати на інциденти. Системи EDR забезпечують глибокий аналіз активності на кінцевих точках. Системи EDR зазвичай не надають повного контексту атаки, оскільки їхній фокус обмежений кінцевими точками.

XDR (Extended Detection and Response)

XDR є еволюцією EDR. Об'єднує дані з різних джерел (мережевих пристроїв, кінцевих точок, хмари тощо) для створення єдиної картини загроз. XDR використовує машинне навчання та штучний інтелект для виявлення складних атак та автоматизації реагування. XDR забезпечує розширену видимість та контекст атак, дозволяючи виявляти та реагувати на загрози на більш ранніх стадіях.

XDR пропонує більш високий рівень автоматизації, покращене виявлення загроз та більш швидке реагування на інциденти [9].

Таблиця 2.1

Порівняльна характеристика XDR, SIEM та EDR

Характеристика	**SIEM**	**EDR**	**XDR**
Джерела даних	Широкий спектр джерел	Кінцеві точки	Широкий спектр джерел, включаючи хмару
Функціональність	Збір, аналіз та кореляція логів	Виявлення загроз на кінцевих точках	Виявлення загроз, кореляція подій, автоматизація реагування
Фокус	Видимість мережі	Захист кінцевих точок	Розширена видимість та контекст атак
Складність	Висока	Середня	Середня-висока
Вартість	Середня-висока	Середня	Висока

SIEM: Ідеально підходить для організацій, яким необхідна загальна видимість подій у мережі та відповідність нормативним вимогам.

EDR: Оптимально для організацій, яким необхідно забезпечити захист кінцевих точок та виявити цільові атаки.

XDR: Є найбільш комплексним рішенням, яке підходить для організацій, яким необхідний високий рівень автоматизації, розширена видимість та швидке реагування на загрози.

Вибір оптимального рішення залежить від конкретних потреб організації:

XDR представляє собою наступний етап розвитку в галузі кібербезпеки. Він пропонує більш широкий спектр можливостей та більш високий рівень автоматизації порівняно з традиційними рішеннями SIEM та EDR.

Розглянемо Gartner® Magic Quadrant™ для EPP, XDR - це нова технологія, яка може запропонувати покращені можливості запобігання, виявлення та реагування на загрози для операційних команд безпеки. Створена на основі найширшої в галузі аналітики загроз, що базується на більш ніж 65 трильйонах щоденних сигналів і більш ніж 10 000 систем безпеки [10-11].

Рис. 2.3. Gartner® Magic Quadrant™ XDR 2024 [10-11]

CrowdStrike є лідером у цьому магічному квадранті. CrowdStrike Falcon є флагманським продуктом EPP. На додаток до основного EPP, CrowdStrike

пропонує зростаючий набір інтегрованих продуктів безпеки, включаючи захист особистості, хмарну безпеку, розширене виявлення та реагування, серед іншого.

Вендор запустив рішення Falcon for IT для керування кінцевими точками, дотримання вимог і моніторингу продуктивності. CrowdStrike також випустила Falcon NG-SIEM, який покращив представлення виявлень у своєму рідному портфоліо продуктів та сторонніх контролях безпеки. CrowdStrike також завершила придбання Bionic та Flow Security, зміцнивши свої позиції у сфері хмарної безпеки та безпеки додатків [10-11].

«19 липня 2024 року оновлення контенту CrowdStrike для клієнта Falcon спричинило збій, який вплинув на мільйони систем Windows у різних компаніях по всьому світу. CrowdStrike негайно відреагувала, відкликавши помилкове оновлення, підтримавши зусилля клієнтів щодо відновлення та оголосивши про покращення стійкості та тестування програмного забезпечення. Компанія Gartner врахувала цей інцидент в оцінці CrowdStrike. Gartner також надав подальший аналіз цього інциденту та його наслідків для клієнтів і потенційних клієнтів CrowdStrike у дослідженні, опублікованому за межами цієї порівняльної оцінки» [10-11].

2.2. Архітектура рішення CrowdStrike Falcon Insight XDR

XDR - це сучасний підхід до кібербезпеки, який об'єднує дані з різних джерел (мережі, кінцеві точки, хмара тощо) для виявлення загроз і реагування на них.

CrowdStrike дозволяє всім клієнтам EDR легко активувати можливості XDR у Falcon Insight XDR за допомогою простих у використанні пакетів з'єднувачів, які розблоковують міждоменні виявлення, розслідування та дії реагування на всі ключові домени безпеки з єдиної консолі. Як світовий лідер у сфері кібербезпеки, CrowdStrike використовує більш ніж десятирічний досвід створення провідного в галузі EDR, щоб забезпечити чудові можливості міждоменного виявлення, розслідування та реагування, щоб зупинити порушення та забезпечити неперевершений досвід для аналітиків безпеки [12].

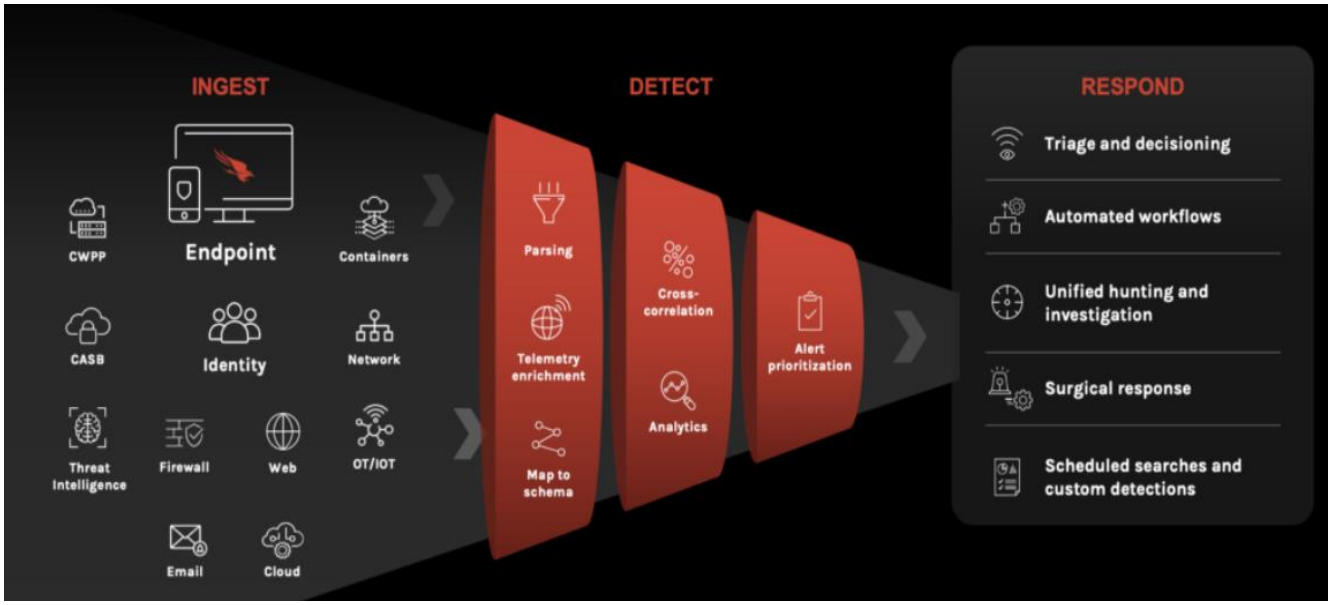

Рис. 2.4. Архітектура рішення Falcon Insight XDR [13]:

XDR об'єднує дані з розрізнених рішень безпеки, щоб вони могли працювати разом для покращення видимості загроз і скорочення часу, необхідного для виявлення атаки та реагування на неї. XDR забезпечує розширені можливості цифрового розслідування та пошуку загроз у кількох доменах з однієї консолі.

Робота XDR:

Крок 1. Прийом: приймайте та нормалізуйте обсяги даних із кінцевих точок, хмарних робочих навантажень, ідентифікаційних даних, електронної пошти, мережевого трафіку, віртуальних контейнерів тощо.

Крок 2. Виявлення: аналізуйте та співвідносьте дані, щоб автоматично виявляти приховані загрози за допомогою передового штучного інтелекту (AI) і машинного навчання (ML).

Крок 3 Відповідь: Пріоритезуйте дані про загрози за ступенем серйозності, щоб мисливці за загрозами могли швидко аналізувати та сортувати нові події, а також автоматизувати розслідування та дії реагування [13].

Ключові компоненти :

Централізована платформа: Збирає і аналізує дані з різних джерел.

Штучний інтелект та машинне навчання: Використовуються для виявлення аномалій і прогнозування загроз.

Автоматизація: Зменшує час реагування на інциденти.

Оркестрація: Координує дії різних інструментів безпеки.

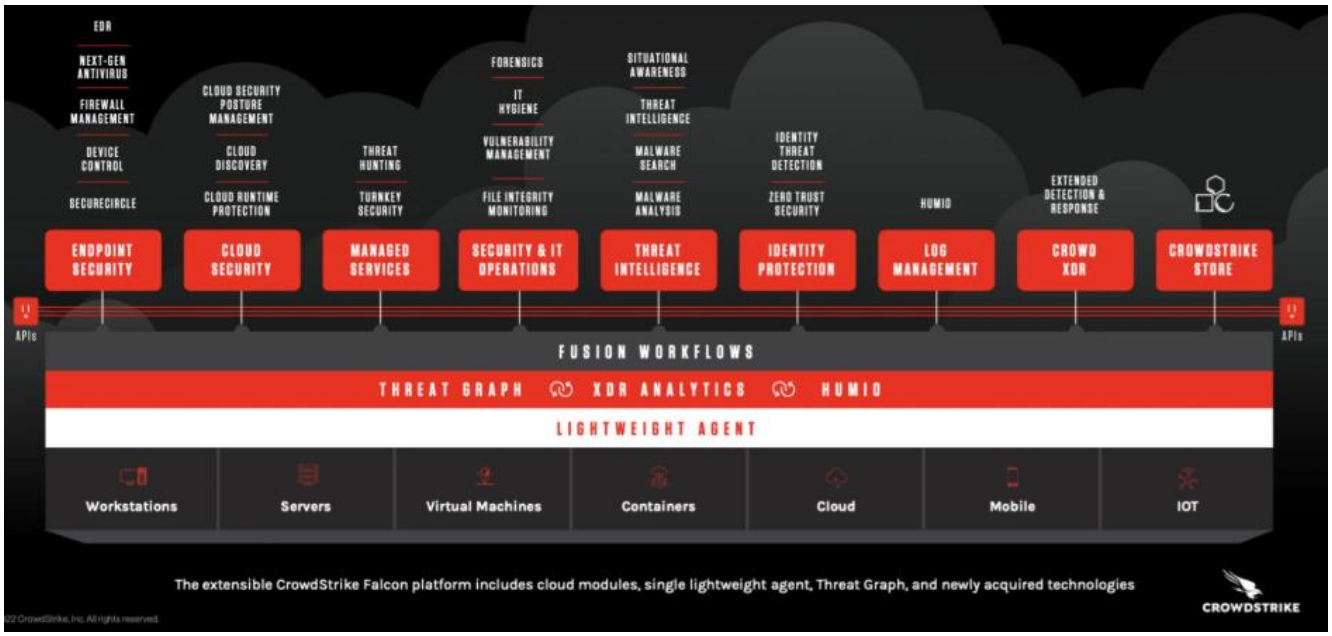

Рис. 2.5. Модулі платформи CrowdStrike [14]

Але існує кілька ключових аспектів архітектури CrowdStrike, про які варто згадати.

Агент/датчик

Легкий агент CrowdStrike має фундаментальне значення. Всі звикли думати, що безагенти – це добре, а агенти – погані, тому що ними потрібно керувати. Але в цьому випадку потужний, але невеликий, простий в установці і ненав'язливий агент є вигідним, оскільки він підтримує кілька модулів CrowdStrike і може підтримувати великі масштаби [14].

Усе в хмарі

Другим ключовим моментом є те, що CrowdStrike з самого початку догматично ставилася до передачі всіх даних телеметрії в хмару, щоб їх можна було проаналізувати. Чим більше агентів CrowdStrike встановлено по всьому світу, тим до більше даних вони мають доступ і тим краща розвідка.

Графік загроз

CrowdStrike розробила спеціально створену платформу графіка загроз та аналітики, яка дозволяє їй швидко отримувати майже в режимі реального часу

ключові телеметричні дані та виявляти не тільки відоме шкідливе програмне забезпечення, але й за допомогою машинного інтелекту, невідомого шкідливого програмного забезпечення та іншої потенційно шкідливої поведінки за допомогою індикаторів атаки (IoAs).

Масштабування нових продуктів і модулів за межі кінцевих точок

У минулому кварталі CrowdStrike повідомила, що ARR від нових продуктів склав $219 млн або близько 10% від загального ARR. Цей сегмент, що розвивається, стає значущою складовою бізнесу CrowdStrike і є ключем до консолідації встановленої бази точкових продуктів на ринку. Ці нові модулі включають Falcon Discover, який відстежує системи, використання додатків та облікові записи користувачів; Spotlight, який виділяє вразливі місця; і Identity Protection, призначений для моніторингу та захисту від ідентифікаційних атак. Модуль ідентифікації CrowdStrike з'явився в результаті придбання Preempt за 96 мільйонів доларів у 2020 році.

Тристоронній підхід CrowdStrike

CrowdStrike поєднує у своїй платформі три "суперсили":

AV – антивірус нового покоління – це означає, що це рішення на основі SaaS, яке може виконувати швидкий пошук телеметричних даних у хмарі, використовуючи власний графік загроз CrowdStrike;

EDR – Найкращий у своєму класі EDR (виявлення та реагування на кінцеві точки). CrowdStrike відправляє всю активність кінцевих точок у хмару і може обробляти дані майже в режимі реального часу. CrowdStrike EDR дозволяє шукати історію даних, і він співпрацює з платформами розвідки загроз, які передають дані в хмару CrowdStrike, що підвищує її інтелект. CrowdStrike EDR має можливості стримування для захисту від скомпрометованих систем.

Кероване полювання - Як і багато інших компаній, CrowdStrike має групу експертів, які стежать за загрозами. Перевагою CrowdStrike є обсяг даних та можливості її архітектури майже в режимі реального часу [14].

2.3. Призначення та функції Falcon XDR

Три модулі, які є частиною безпеки кінцевої точки — це Falcon Prevent, Falcon Insight і Falcon Device Control.

Рис. 2.6. Модулі CrowdStrike [15]

Перший модуль — Falcon Prevent, який є антивірусним модулем наступного покоління Falcon. Забезпечує комплексну та перевірену профілактику зловмисного програмного забезпечення та атак без зловмисного програмного забезпечення незалежно від того, чи є кінцеві точки онлайн чи офлайн.

Його широкі можливості антивірусу наступного покоління включають: здатність ідентифікувати відомі ШПЗ; машинне навчання зловмисного програмного забезпечення для невідомих експлойтів; блокування зловмисного програмного забезпечення; ексклюзивний індикатор поведінкових методів атаки [15].

Наступний модуль — це Falcon Insights, який є модулем EDR, що є виявленням кінцевої точки та реагуванням. Falcon Insight діє як відеореєстратор на кінцевій точці запису активності для виявлення інцидентів, які уникли запобігання,

забезпечує клієнтам повну видимість у режимі реального часу всього, що відбувається на їхніх кінцевих точках з точки зору безпеки, усуваючи ризик збою, що дозволяє зловмисникам залишатися у вашому середовищі непоміченим.

Falcon Insight виявляє ознаки атак, які могли уникнути інших засобів захисту, і забезпечує проактивне полювання на загрози, як у реальному часі, так і в усьому середовищі [15].

Наступним модулем є керування пристроєм Falcon, що забезпечує безпечне та відповідальне використання USB-пристрої в організації за допомогою одного легкого агента, він унікально поєднує видимість і детальний контроль і дозволяє йому та адміністраторам безпеки гарантувати, що використовуються схвалені USB-пристрої належним чином у своїх середовищах при використанні з Falcon Insight видимість розширена додаванням історії з можливістю пошуку та журналів використання USB-пристроїв, включаючи файли, записані на пристрої.

Наступне рішення — це безпека та його операції, що включає наступне:

Falcon Overwatch, Falcon Discover і Falcon Spotlight [15].

Першим модулем є Falcon Overwatch, який керується модулем полювання на загрози. Цей модуль відповідає за виявлення вторгнень, зловмисних дій і зловмисників, які можуть бути непомічені або в іншому випадку залишаються непоміченими, крім того, Falcon Overwatch активно шукає приховані та руйнівні кампанії зловмисного програмного забезпечення, сповіщаючи клієнтів і забезпечуючи відповідний захист.

Другий модуль — це Falcon Discover, цей модуль забезпечує обізнаність, щоб визначити, хто і що є у вашій мережі з ним ви можете знаходити потенційні сліпі зони у вашій архітектурі безпеки, щоб захиститися від атак, це досягається за допомогою трьох ключів Discover можливості, якими є інвентаризація додатків та керування інвентаризацією активів і моніторинг облікових записів [15].

Третій модуль — це Falcon Spotlight, який є модулем для керування вразливостями, він пропонує оцінку вразливості в реальному часі на кінцевих точках, яка завжди актуальна. Інтеграція Falcon Spotlight у платформу Falcon

CrowdStrike дає змогу клієнтам проводити оцінку вразливості в рамках повної системи захисту кінцевих точок.

Наступним рішенням є аналіз загроз який включає три модулі: Falcon X, пошукова система Falcon і пісочниця Falcon [15].

Перший модуль — Falcon X, який є модулем аналізу загроз. Falcon X виводить захист кінцевих точок на наступний рівень, поєднуючи пошук зловмисного програмного забезпечення в ізольованому програмному середовищі та розвідку про загрози в інтегроване рішення, яке виконує комплексну загрозу, аналіз за лічені секунди результатом цього аналізу є унікальна комбінація індивідуальних індикаторів компрометації.

Falcon X — єдине рішення, яке створює IOCS, як для загрози, яка фактично виникла у вашій організації, так і для всіх її відомих варіантів, одразу надсилаючи їх іншим інструментам безпеки, таким як брандмауери, шлюзи та інструменти оркестрації безпеки через api.

Другий модуль — пошукова система Falcon, яка є модулем для дослідження зловмисного програмного забезпечення. CrowdStrike створила найбільшу базу даних загроз із можливістю пошуку в індустрії безпеки, надаючи понад 100 мільярдів подій безпеки на день та індексуючи 400 мільйонів шкідливі файли, які можна шукати в режимі реального часу. Завдяки використанню унікального підходу до індексації пошукова система Falcon дозволяє клієнтам скористатися перевагами даних, щоб значно прискорити та покращити свої можливості дослідження зловмисного програмного забезпечення в центрі операцій безпеки [15].

Третій модуль — це Falcon Sandbox (пісочниця), яка створена для автоматизованого аналізу зловмисного програмного забезпечення, він поєднує дані про загрози з результатами рішення ізольованого програмного середовища, щоб аналітики могли краще розуміти складні атаки зловмисного програмного забезпечення та налаштовувати їхній захист. Falcon Sandbox виконує глибокий аналіз уникаючих і невідомих загроз, збагачує результати аналітикою загроз і надає дієві індикатори компрометації.

Останнє рішення — хмарна безпека, що включає три модулі:

Falcon Horizon, захист робочого навантаження в хмарі Falcon і безпека контейнера Falcon.

Перший модуль — це Falcon Horizon, який є модулем для керування станом, який оптимізує керування станом хмарної безпеки протягом життєвого циклу розробки програми для мультихмарних середовищ, що дозволяє безпечно розгортати програми в хмарі з більшою швидкістю та ефективністю [15].

Другий модуль — хмарний захист робочого навантаження Falcon, він забезпечує комплексний захист робочих навантажень і контейнерів від злому, що дозволяє створювати запущені та безпечні програми зі швидкістю та впевненістю.

Третій модуль це безпека контейнерів Falcon, він автоматизує безпечну розробку хмарних додатків, забезпечуючи повний захист і відповідність вимогам для контейнерів і хостів протягом життєвого циклу контейнера.

На основі цих функцій XDR-система будує граф атак, який покаже, як зловмисник проник у мережу і які дії він зробив. Потім система автоматично вживає заходів для стримування атаки, як-от блокування IP-адреси зловмисника, ізоляція зараженого пристрою або блокування підозрілих процесів.

Висновки до розділу 2

1. Досліджено методи та засоби виявлення та реагування на мережеві атаки.
2. Представлено архітектуру рішення CrowdStrike Falcon Insight XDR.
3. Розкрито призначення та функції модулів CrowdStrike.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ МЕРЕЖЕВИХ АТАК НА ОСНОВІ XDR

3.1. Розроблення варіанта розгортання технології виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR

Щоб отримати доступ до файлів датчиків CrowdStrike Falcon®, вам спочатку потрібно отримати доступ до вашого інстансу Falcon. Цей доступ буде надано електронною поштою від служби підтримки CrowdStrike і виглядатиме, як на рис. 3.2. Отримавши електронний лист, необхідно дотримуватись інструкцій щодо активації, наведених у електронному листі [16]. Це включатиме налаштування пароля та двофакторну автентифікацію.

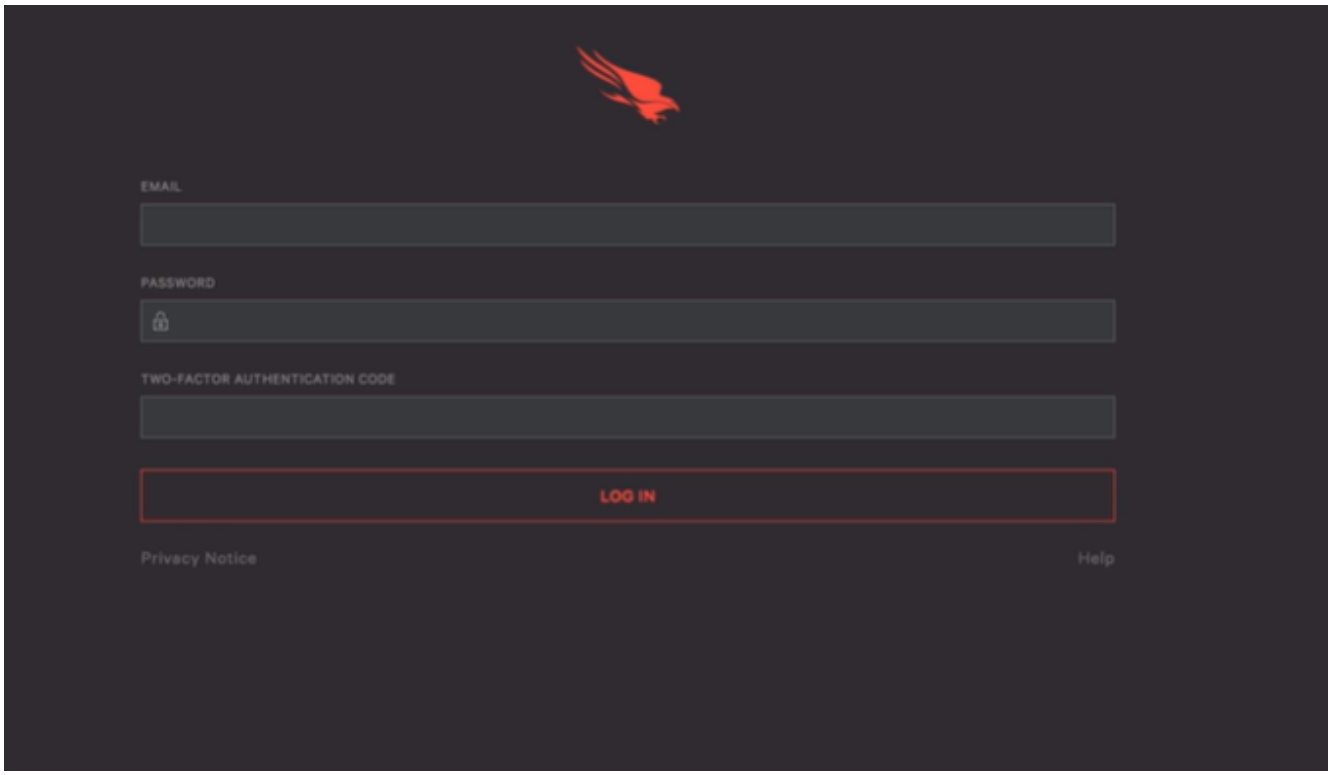

Рис. 3.1. Сторінка інстансу Falcon

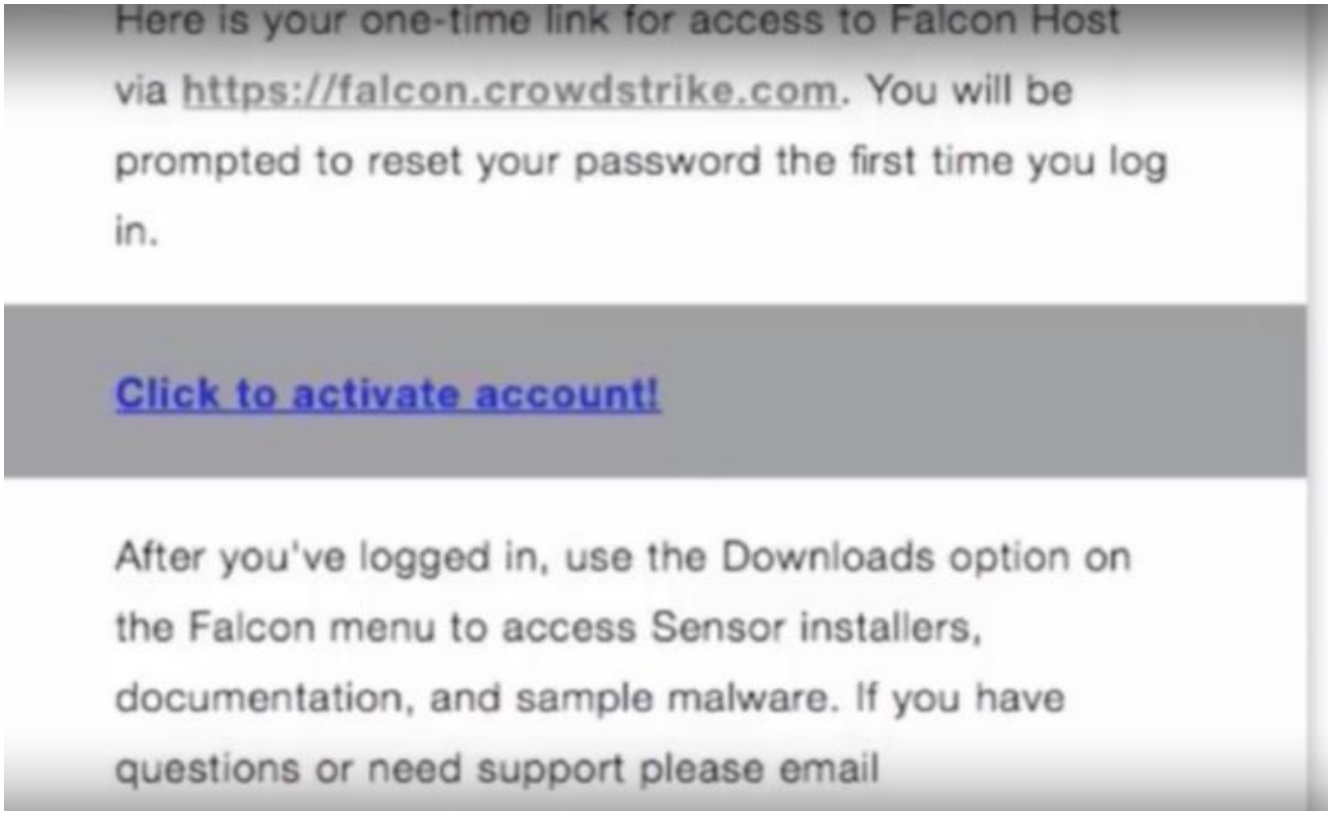

Рис. 3.2. Електронний лист з інструкціями встановлення та активації

Після активації, необхідно увійти у свій екземпляр Falcon [16]. На навігаційній панелі з лівого боку потрібно навести курсор миші на програму підтримки, яка знаходиться в нижній частині навігації, і вибрати опцію завантаження Рис. 3.3.

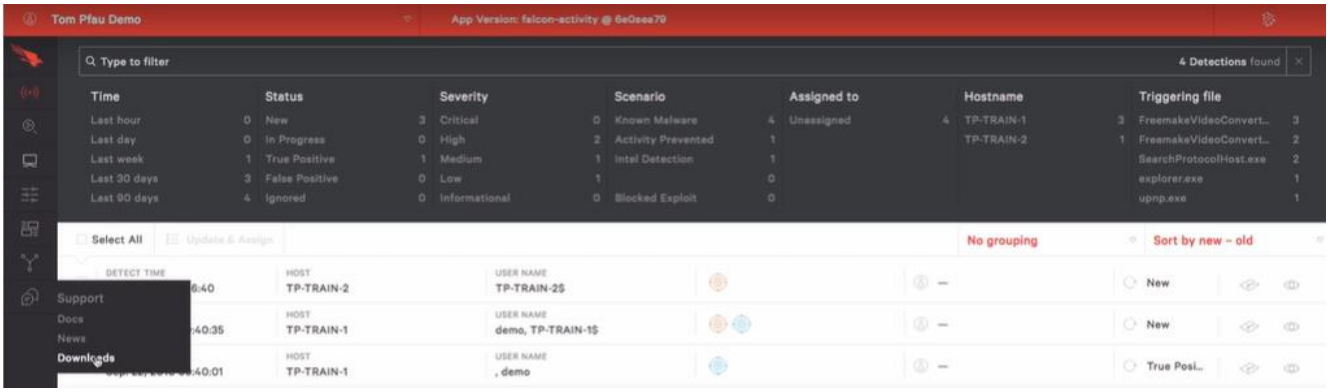

Рис. 3.3. Опція завантаження

Після цього будуть представлені всі завантаження, які стосуються екземпляра Falcon, включаючи документацію, роз'єми для SIM-карти, приклади API та зразки шкідливого програмного забезпечення Рис.3.4. Знаходимо відповідну

версію ОС, яку хочете розгорнути, і натискаємо на посилання для завантаження в правій частині сторінки [16].

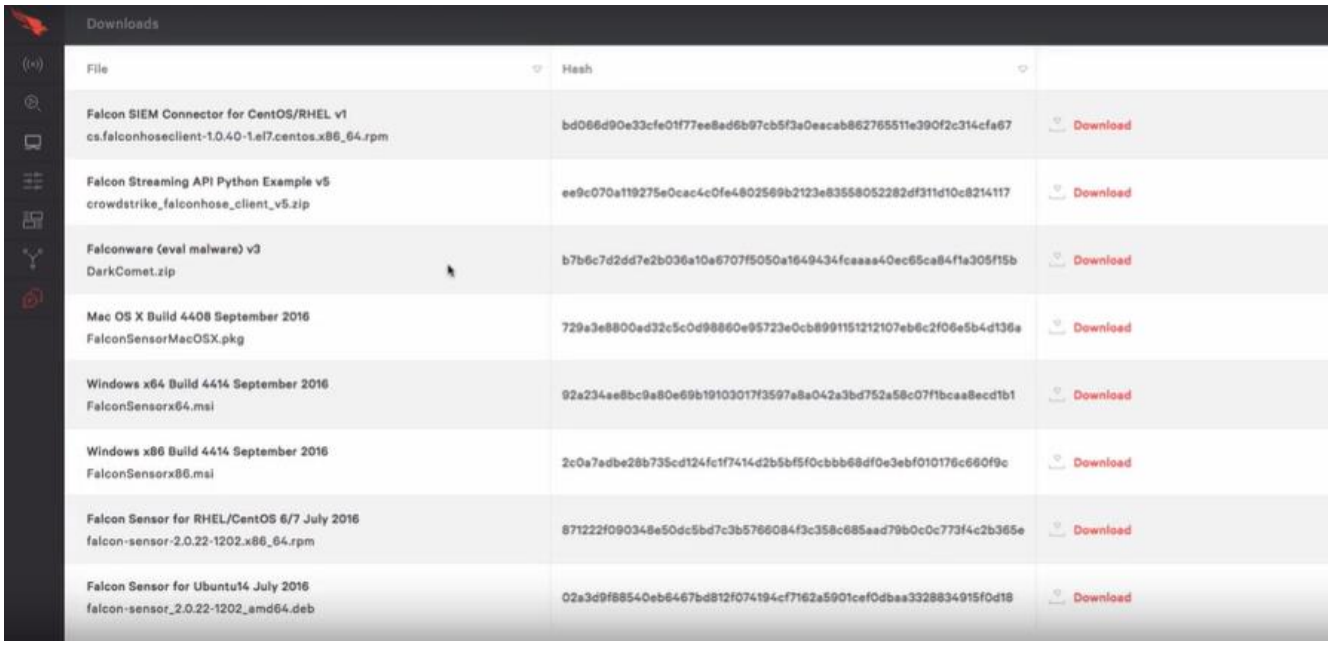

Рис. 3.4. Доступні завантаження, які стосуються екземпляра Falcon

Рис. 3.5. Процес встановлення та ліцензійні умови

Рис. 3.6. Завершення інсталяції

Повертаємося в інстанс Falcon, натискаємо на «Дослідження» Рис. 3.7. Уздовж верхньої панелі побачимо опцію з написом «Датчики» Рис.3.8. Натискаємо на це, а потім на "Нові встановлені датчики" Рис.3.8. Тут бачимо всі пристрої, на які нещодавно були встановлені нові датчики Falcon [16].

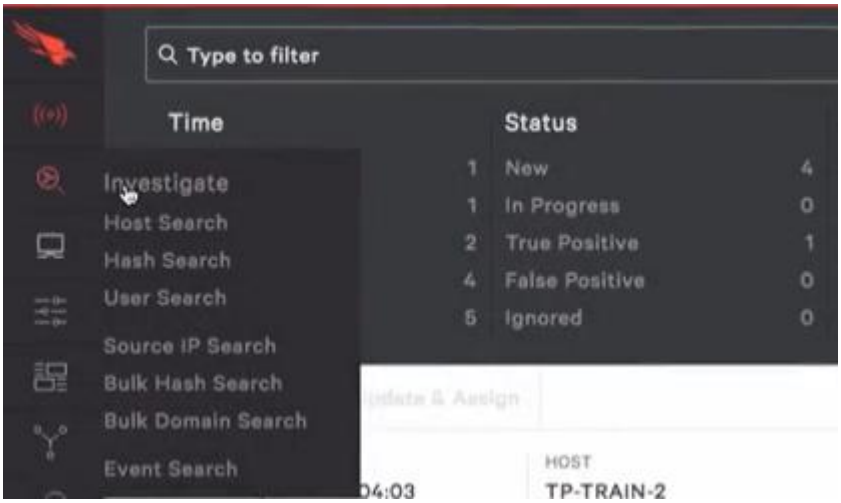

Рис. 3.7. Підменю «Дослідження»

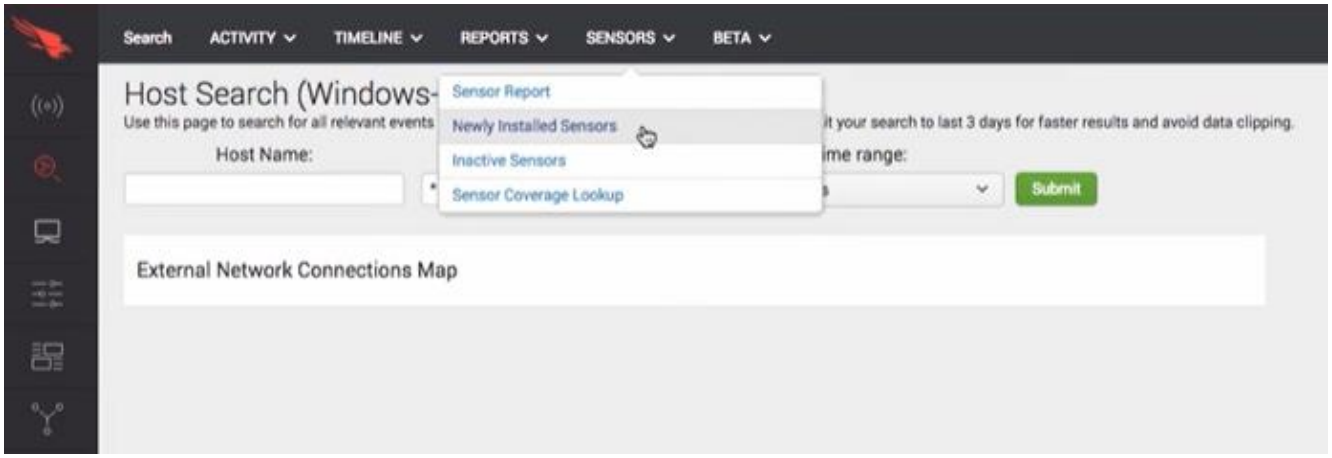

Рис. 3.8. Нові встановлені датчики

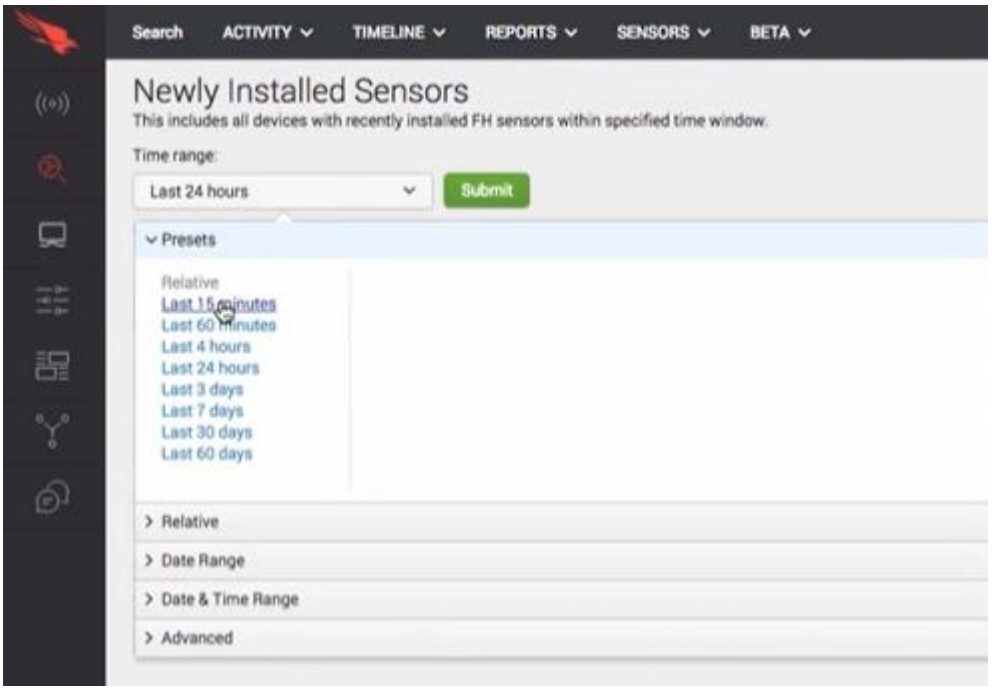

Рис. 3.9. Нові встановлені датчики за останні хвилини

Тепер перевіримо, чи працює датчик належним чином. Раніше було завантажено зразок файлу шкідливого програмного забезпечення з розділу завантажень у додатку "Активності" Рис. 3.10. Файл називається "DarkComic.zip". Отже, запускаємо цю програму. Тепер подивимося на додаток активності на екземплярі Falcon Рис. 3.11. Як видно, в системі спостерігається деяка активність, пов'язана з інструментом віддаленого доступу DarkComet. Інструменти були спіймані і кінцева точка була захищена Рис.3.12 - і все це протягом декількох хвилин без необхідності перезавантаження [16].

Рис. 3.10. Підменю активності

Рис. 3.11. Активність програми на екземплярі

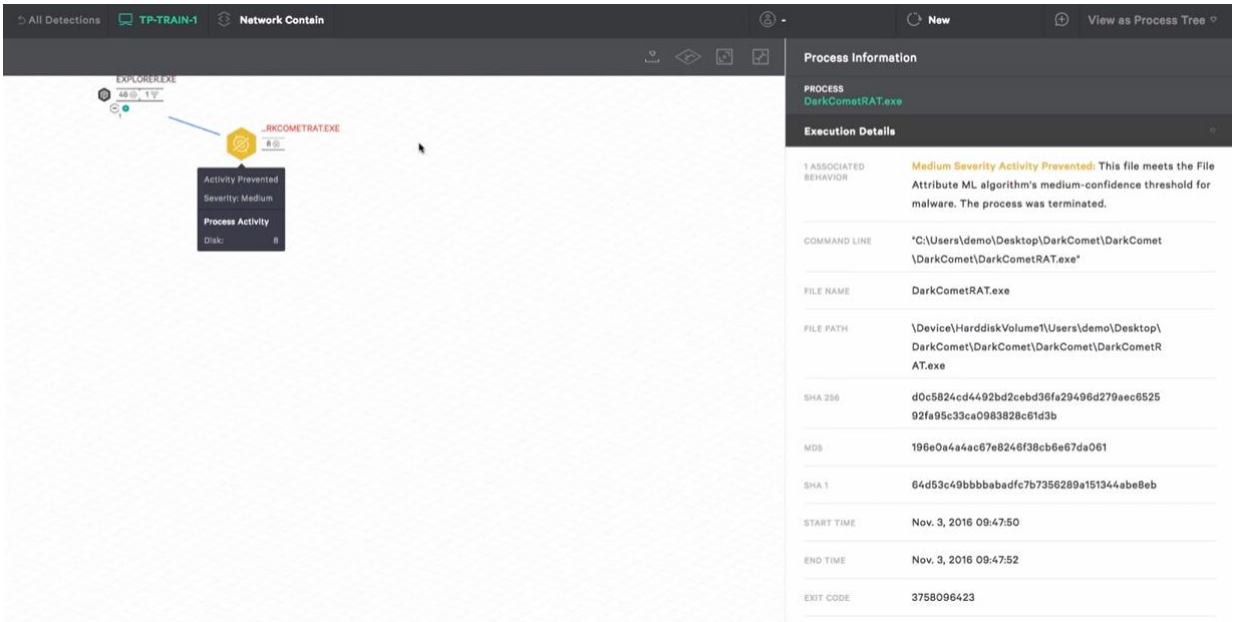

Рис. 3.12. Знайдена активність та захищена точка

3.2. Технологія виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR

Falcon Inside XDR — це комплексне рішення EDR, створене на основі неперевершеної видимості кінцевих точок, оскільки хмарна власна платформа CrowdStrike використовує агент кінцевої точки для збору детальних даних про події для аналізу за допомогою графіка загроз [17]. Поведінка, визнана шкідливою, призводить до виявлення подій, доступ до яких можна отримати на інформаційній панелі Рис. 3.13.

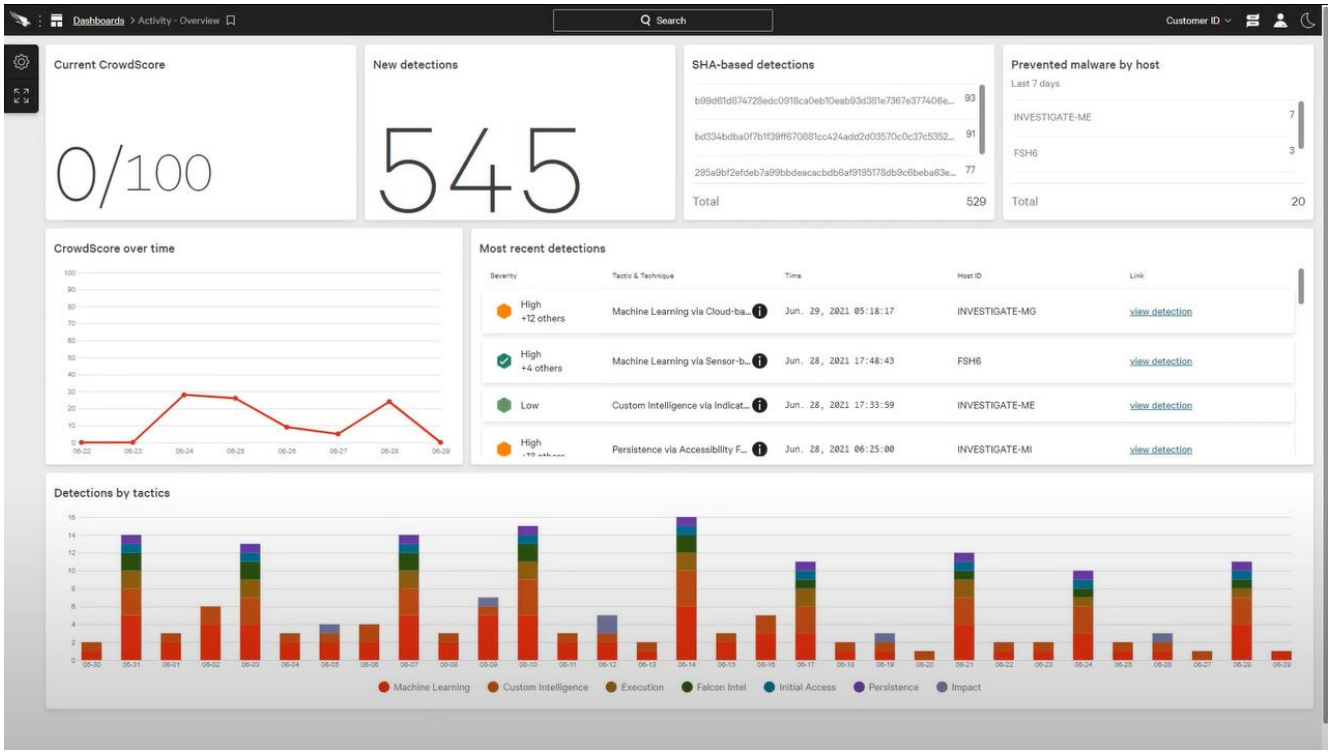

Рис. 3.13. Інформаційна панель (Dashboard)

Для кожного виявлення є підсумкова інформація про спостережувану тактику чи техніку Рис. 3.14, тоді як колір значка вказує на ступінь тяжкості Рис.3.15. додатка при виконанні.

Деталі, доступні в дереві процесів Рис. 3.16. Falcon Insight надає перегляд інциденту з додатковим контекстом і кореляцією [17].

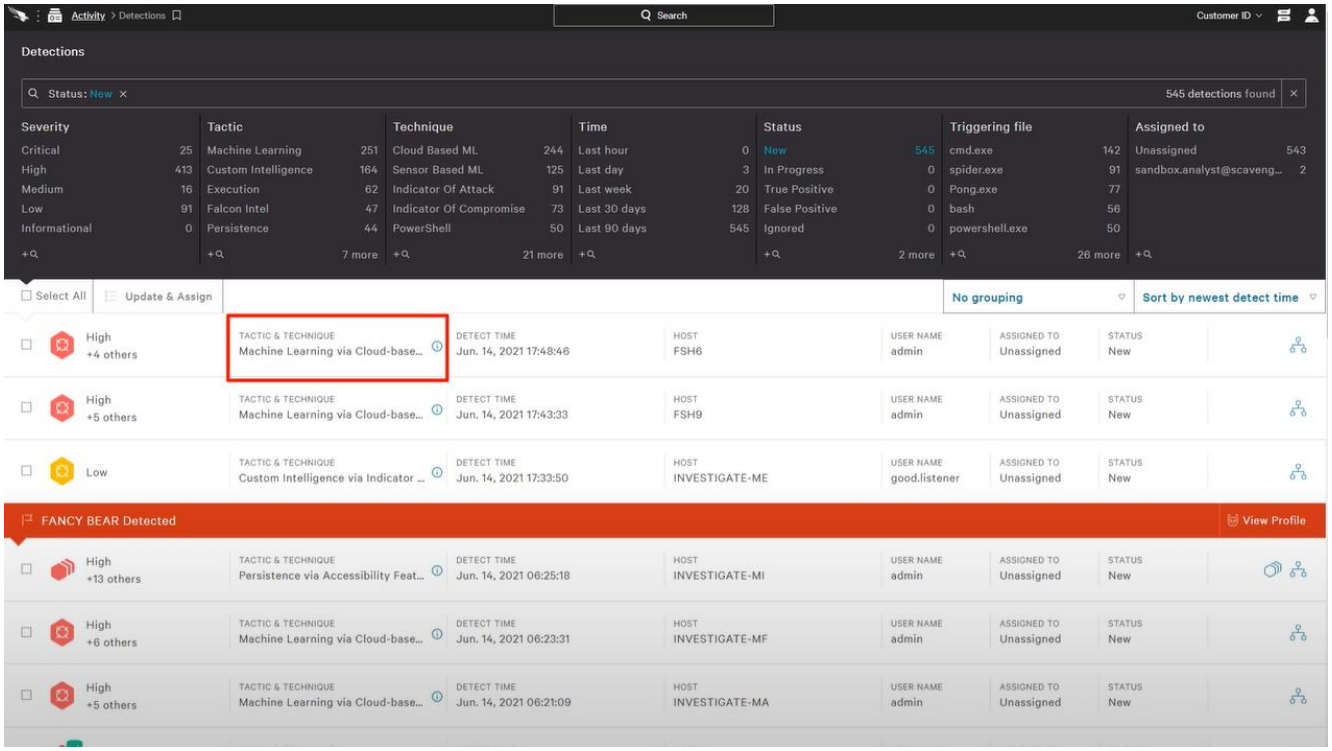

Рис. 3.14. Підсумкова інформація про спостережувану тактику та техніку

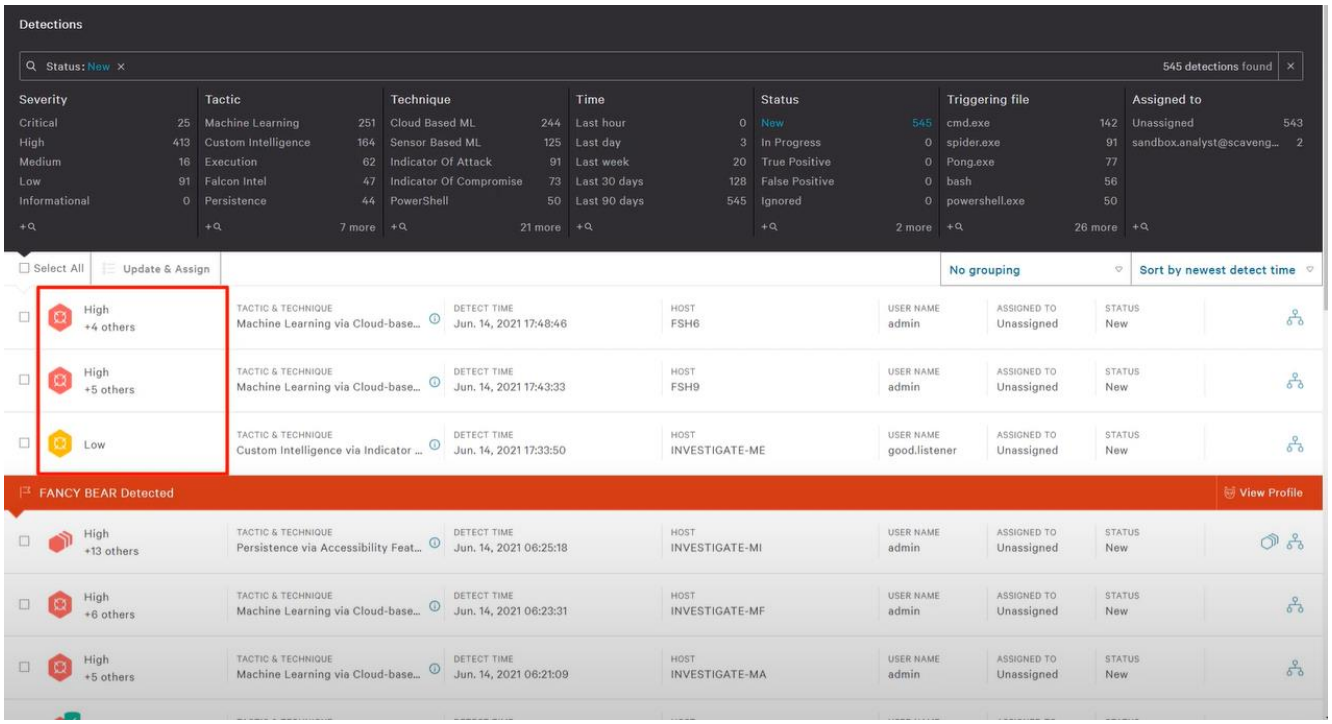

Рис. 3.15. Колір ступеня тяжкості

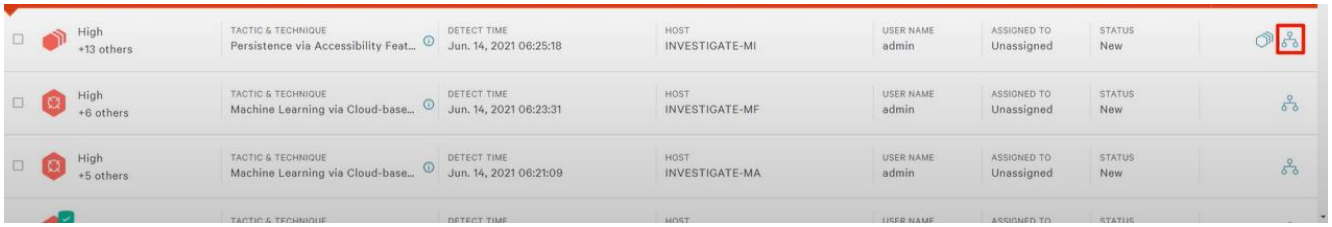

Рис. 3.16. Перехід в дерево процесів

Кожному інциденту присвоюється оцінка, щоб проілюструвати рівень критичності та допомогти визначити пріоритетність зусиль [17], використовуючи термінологію MITRE Рис. 3.17.

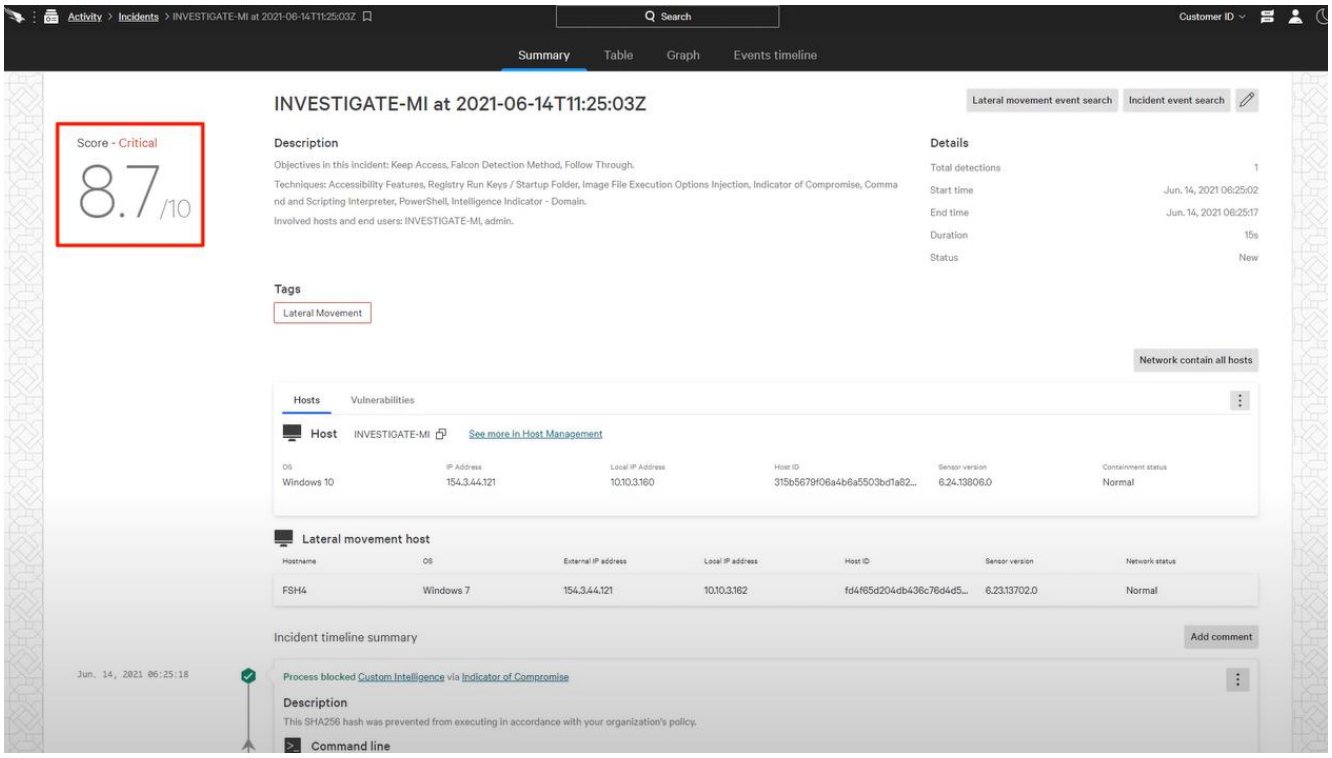

Рис. 3.17. Оцінка інциденту

У підсумковому описі представлені подробиці щодо дій, пов’язаних з інцидентом Рис. 3.18, а також інформацію про постраждалі хости Рис. 3.19 та часову шкалу подій Рис. 3.20, також є графічне представлення інциденту Рис.3.21, включаючи функцію повтору Рис.3.22, яка показує повний потік і порядок атаки. в якому доступні різні параметри накладання для виділення конкретних типів подій Рис. 3.23 і чітко ілюструють, що саме відбувалося під час атаки [17].

Рис. 3.18. Підсумковий опис

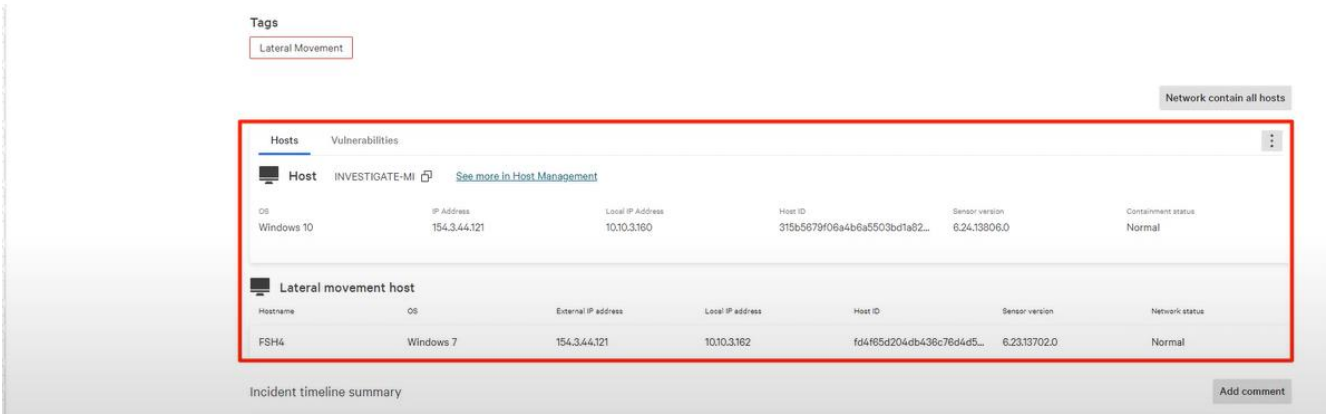

Рис. 3.19. Інформація про постраждалі хости

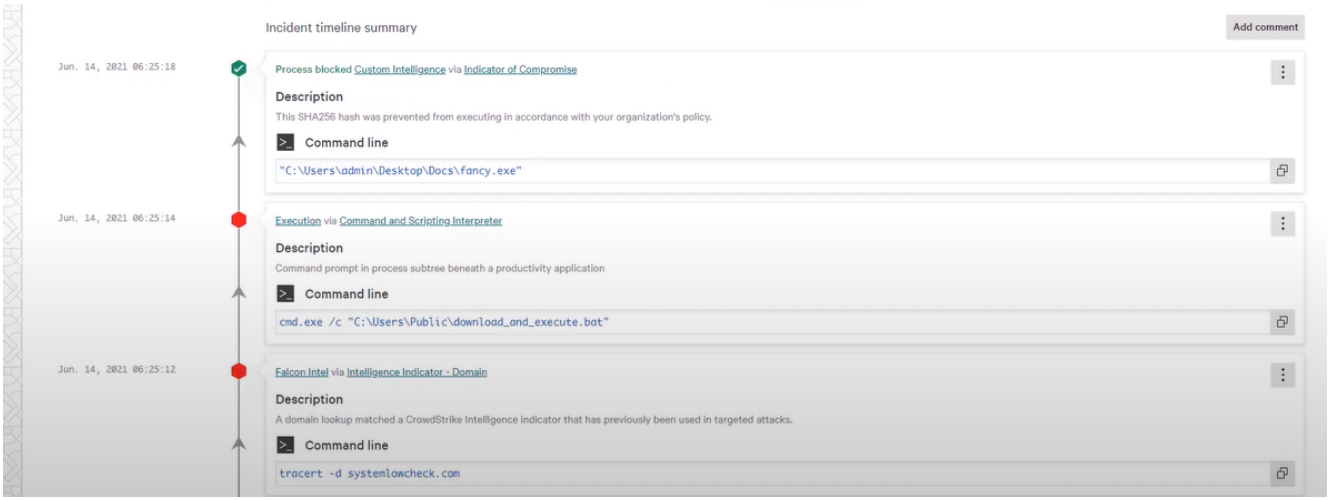

Рис. 3.20. Часова шкала подій

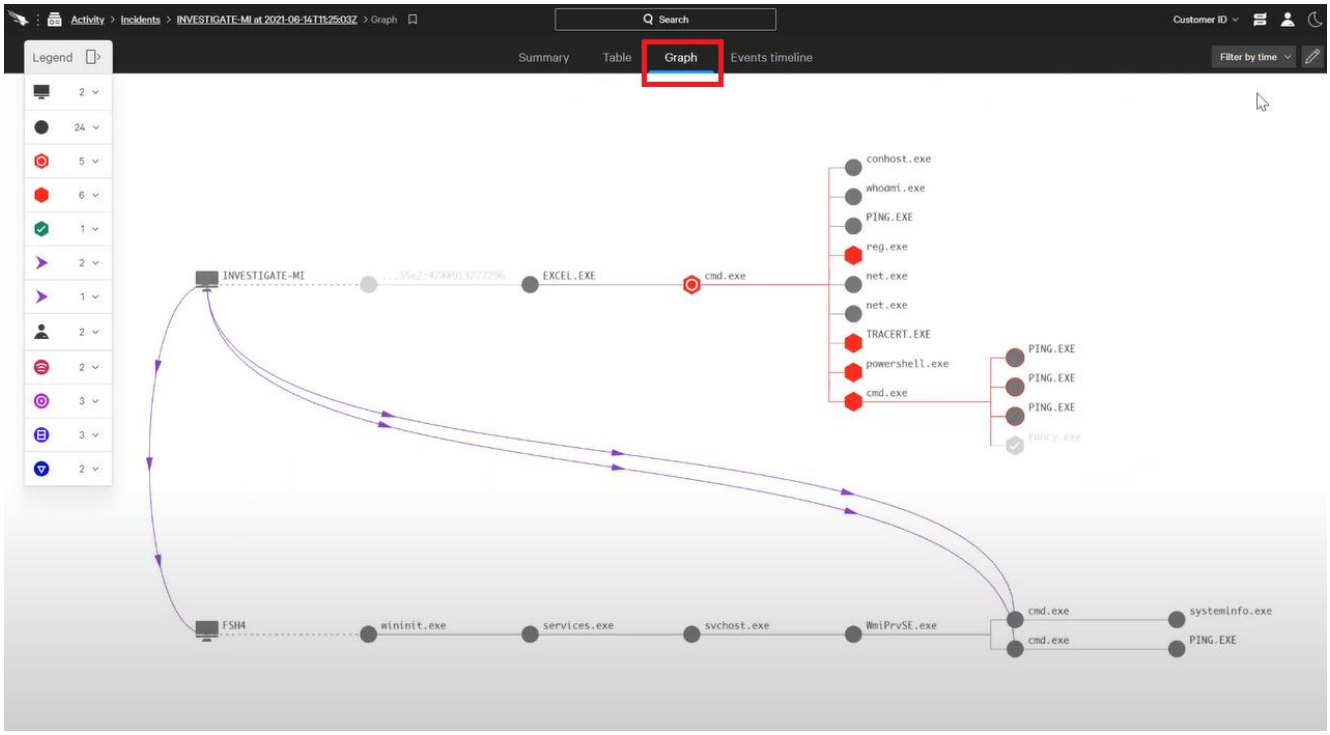

Рис. 3.21. Графічне представлення інциденту

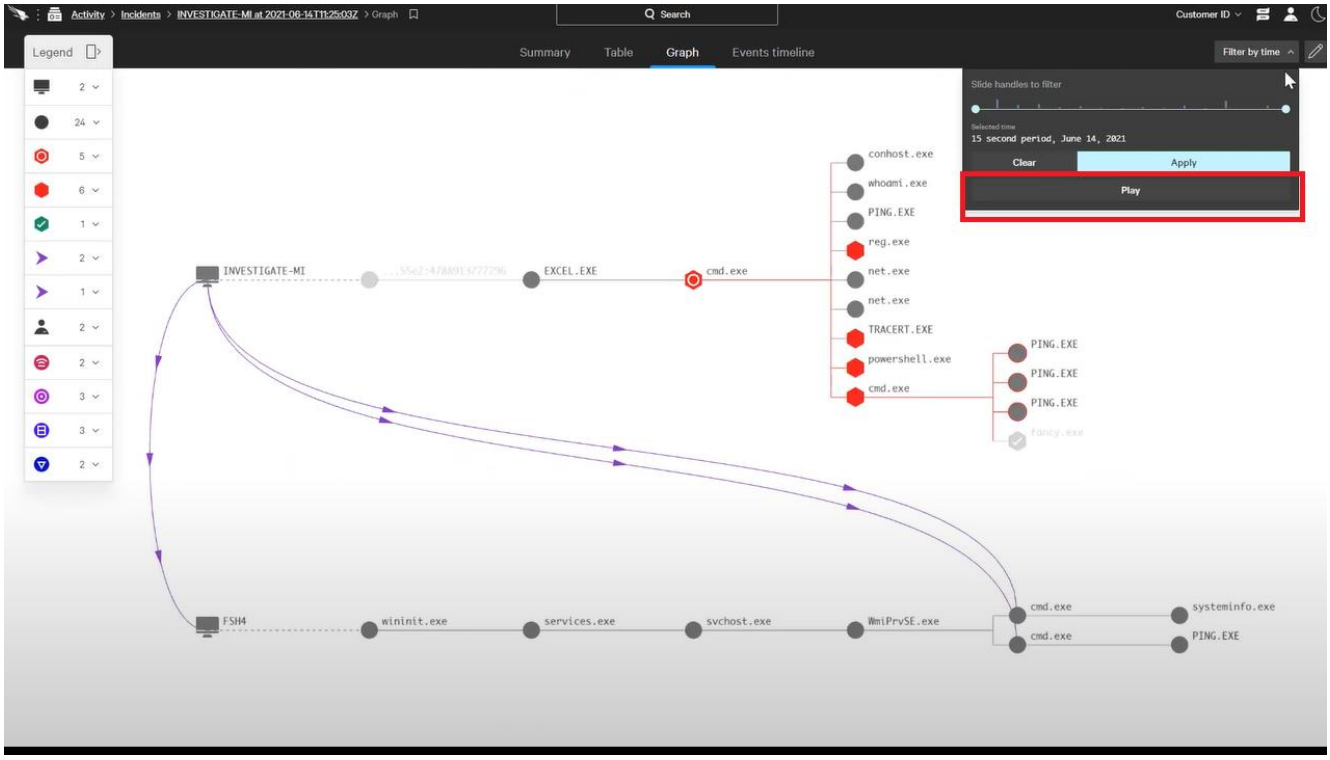

Рис. 3.22. Повний потік і порядок атаки

Рис. 3.23. параметри накладання для виділення конкретних типів подій

Тоді як вкладка «Користувачі» показує [17], який обліковий запис використовувався в різних точках атаки Рис. 3.24.

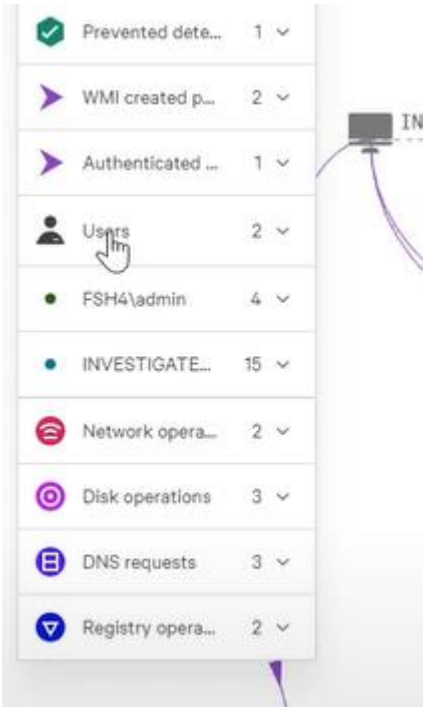

Рис. 3.24. Вкладка «Користувачі»

Вкладка «DNS» висвітлює зовнішні події, які вимагали запитів DNS Рис.3.25.

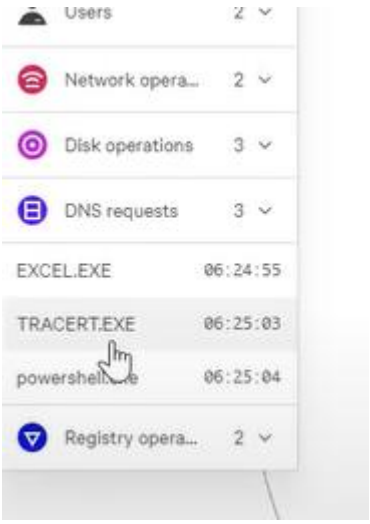

Рис. 3.25. зовнішні події, які вимагали запитів DNS

Зауважимо, що нічого в цьому виявленні не було визначено як зловмисне програмне забезпечення та попереджено [17], однак Falcon Insight розроблено, щоб дивитися за межі запобігання на інші дії, що відбуваються на кінцевих точках, натискання на певному вузлі розгорне подію, щоб отримати більше деталей, як приклад, краудстрайк виявив зміну реєстру, спрямовану на встановлення збереження за допомогою екранної клавіатури Рис. 3.26.

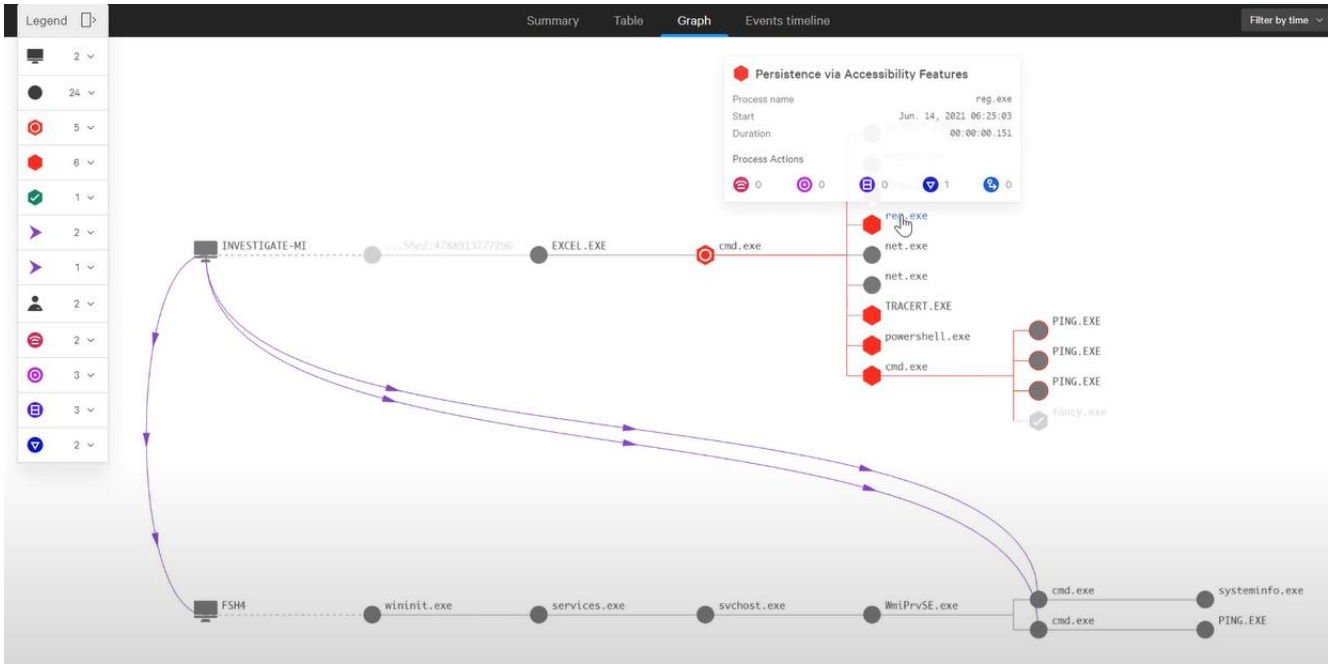

Рис. 3.26. Виявлення зміни реєстру

Представлені деталі виконання та техніка атаки Рис.3.27, Falcon Insight також документує точну команду реєстру, яка була використана Рис.3.28. Цей рівень деталізації особливо корисний для виправлення [17].

Рис. 3.27. Деталі виконання та техніка атаки

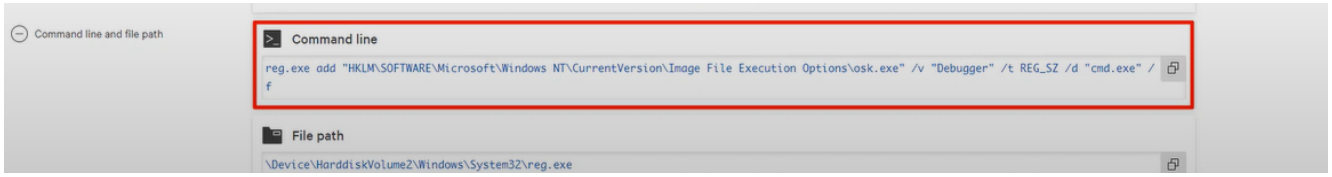

Рис. 3.28. Команда реєстру

Далі бачимо що є подія PowerShell Рис.3.29, хоча це не обов'язково шкідливий інструмент, яка має повну інформацію про командний рядок, корисна для визначення мети цієї події, тут ми бачимо, що метою було використання Mimicats Рис.3.30, широко використовуваного інструменту скидання облікових даних [17].

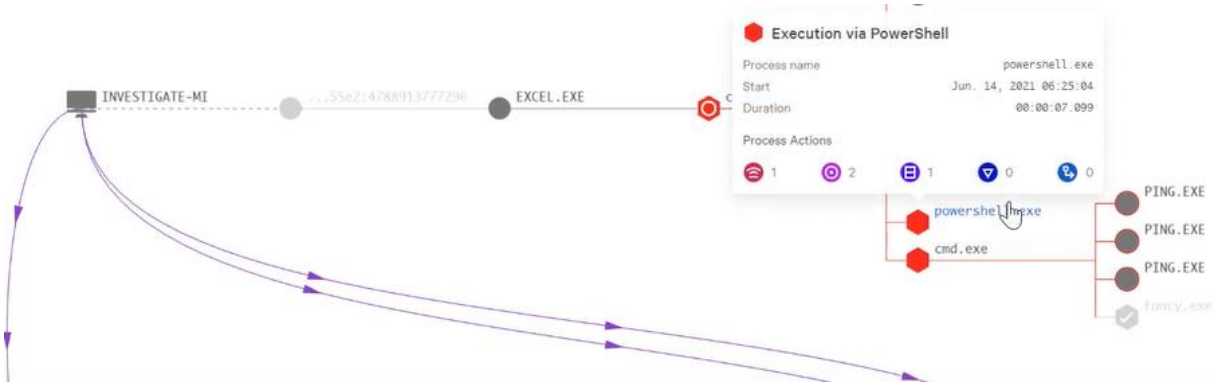

Рис. 3.29. Подія PowerShell

Рис. 3.30. Використання Mimicats

На Рис. 3.31. представлено можливість перегляду повної телеметрії для цієї події [17].

Рис. 3.31. Перегляд повної телеметрії для події

На вкладці хоста є варіант пошуку хосту або використання можливостей реагування Falcon Insight.

Мережеве стримування обмежує підключення хоста, щоб запобігти Інтернет-зв’язку та бічному переміщенню, щоб мінімізувати вплив під час розслідувань

Беспосереднє підключення до хоста у реальному часі, що надає можливість віддалено запускати команди, виконувані файли та сценарії Рис. 3.32.

Falcon Insight забезпечує виявлення видимості кінцевої точки і можливості реагування, щоб допомогти організаціям прискорити розслідування, виявити приховані атаки та зупинити порушення [17].

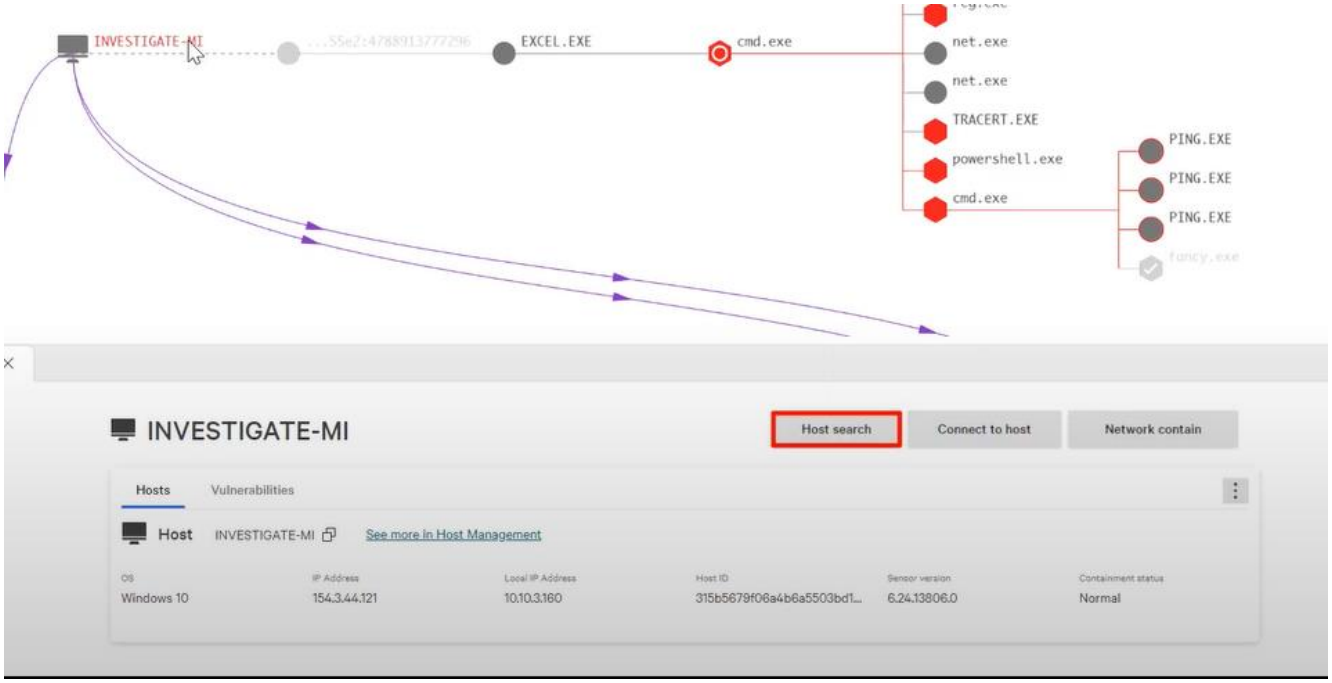

Рис. 3.32. Можливості вкладки хост

Розглянемо перше виявлення, ми бачимо використання metasploit і спробу входу грубою силою Рис.3.33.

Рис. 3.33. Використання metasploit і спроба входу грубою силою

Повна інформація включає список пов’язаних індикаторів окремо Рис.3.34, це можуть бути слабкі сигнали, але разом це малює більш чітку картину в цьому випадку бачимо докази з мережі кінцевої точки та ідентифікаційні дані об’єднуються, як частина єдиної кінцевої точки виявлення, яка виявила Masquerading, у той час як corelight позначив команду metasploit і керував трафіком

та ідентифікаційною інформацією, запущеною на невдалі спроби входу для кожного з цих індикаторів, перейдемо до пошуку Falcon XDR на основі humeo це дає змогу переглянути кожне окреме джерело даних, дізнатися більше про пов'язану телеметрію виявлення та навіть перейти до пошуку пов'язаних артифактів (artifacts) Рис.3.35-3.39.

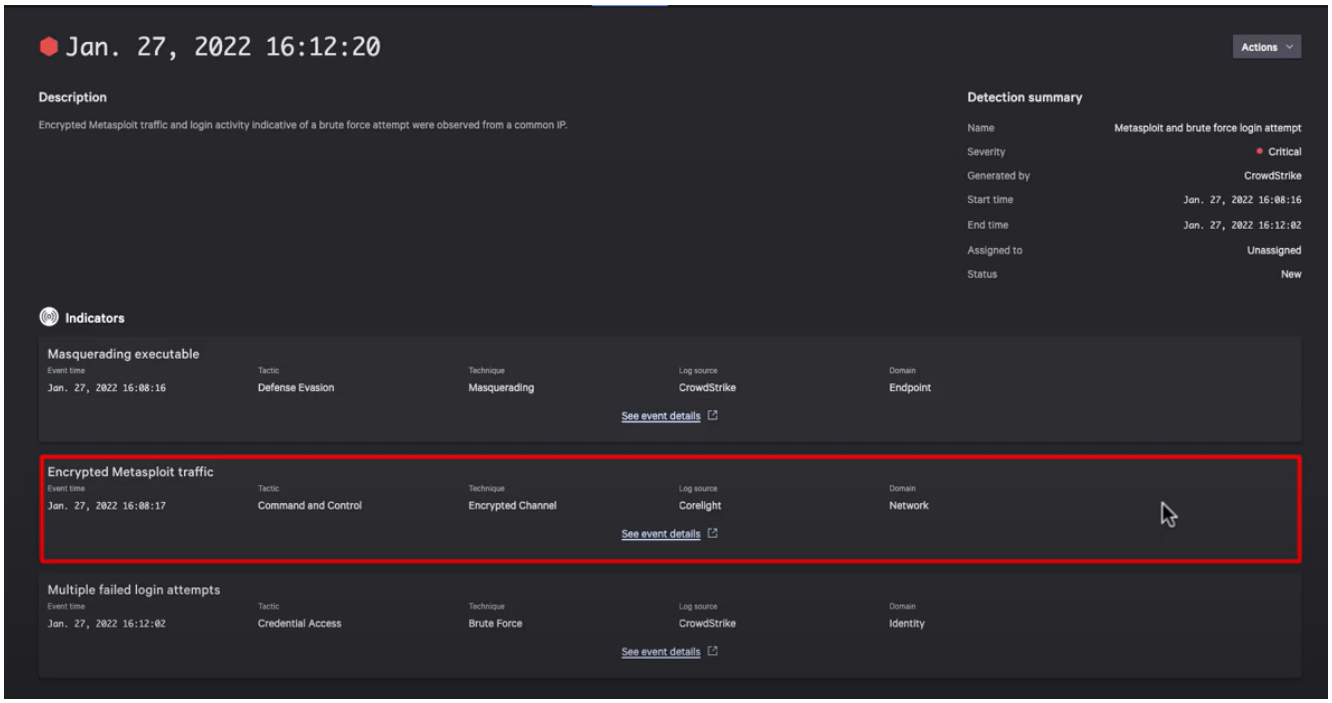

Рис. 3.34. Повна інформація спрацювання

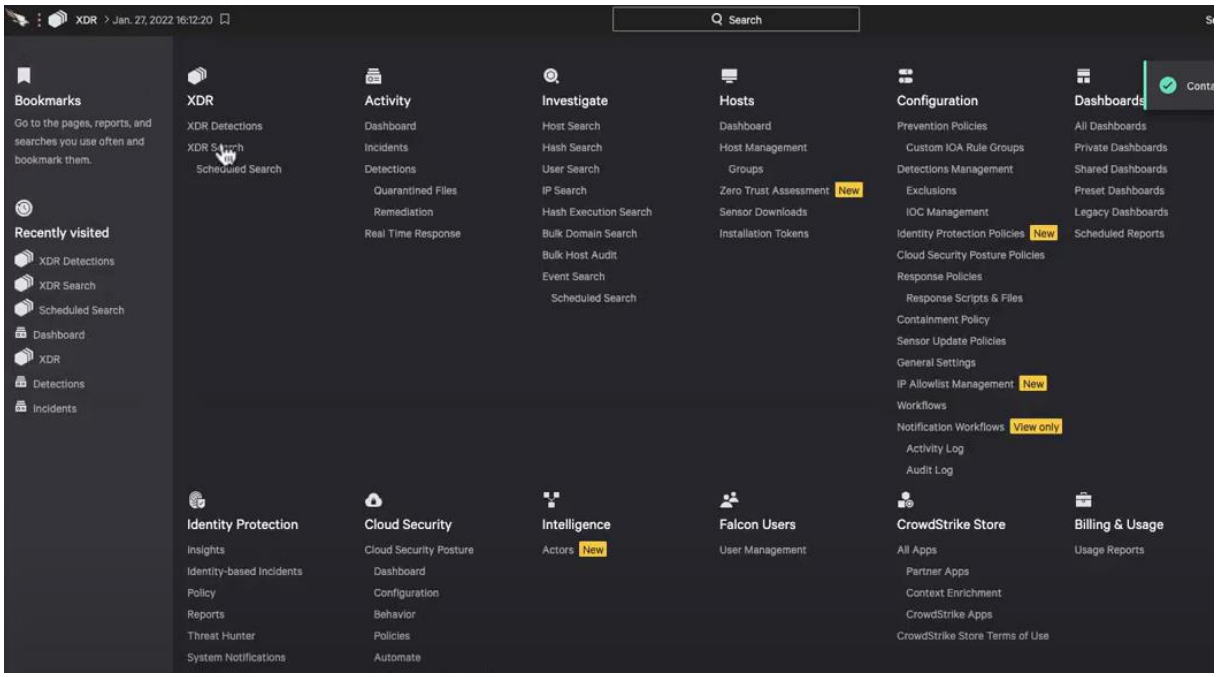

Рис. 3.35. Пошук Falcon XDR

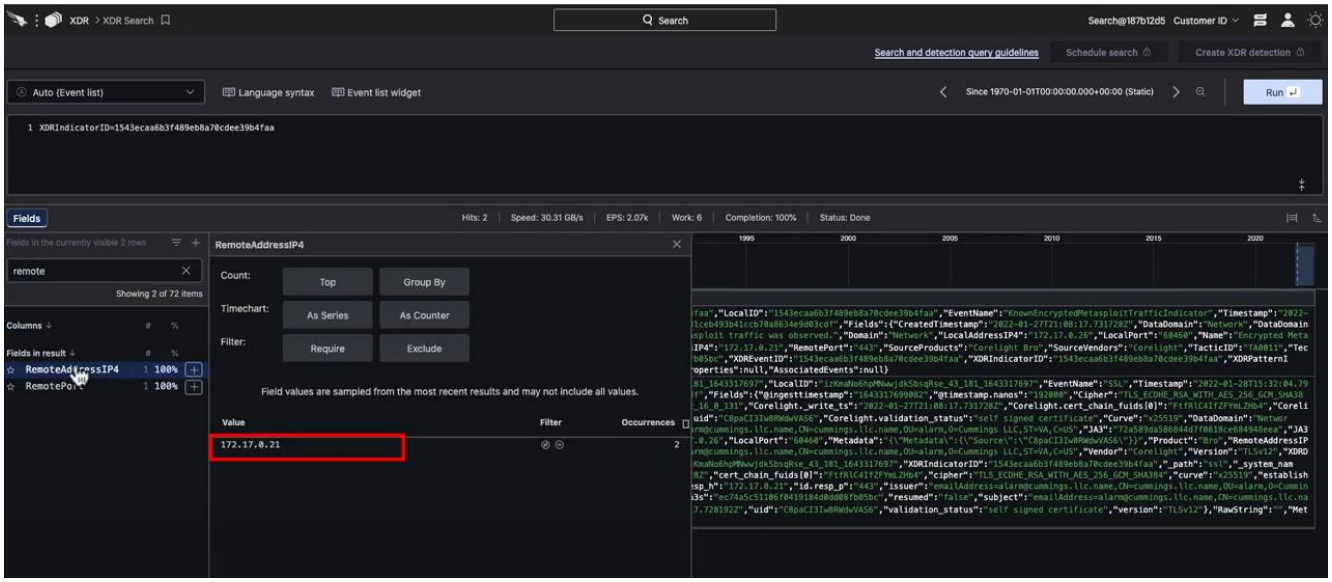

Рис. 3.36. Пошук пов’язаних artifacts

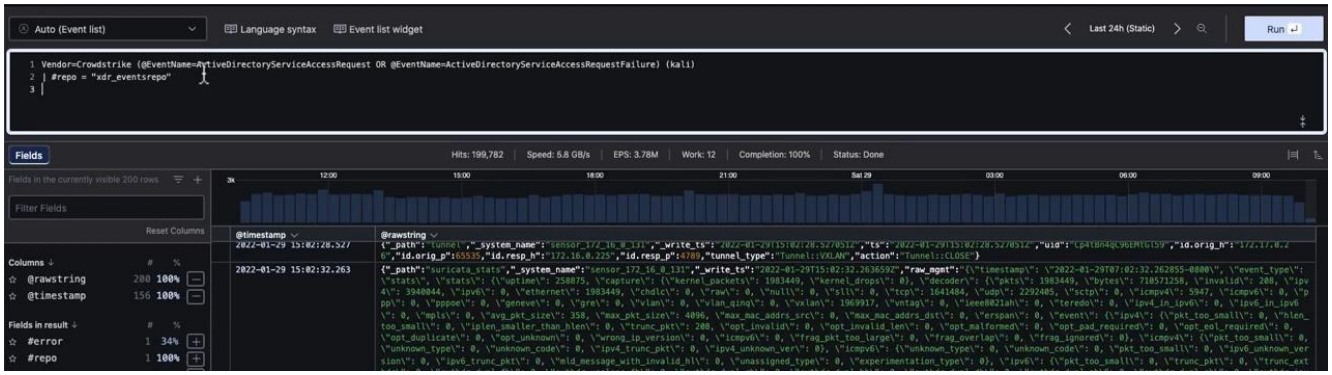

Рис. 3.37. Пошук пов’язаних artifacts

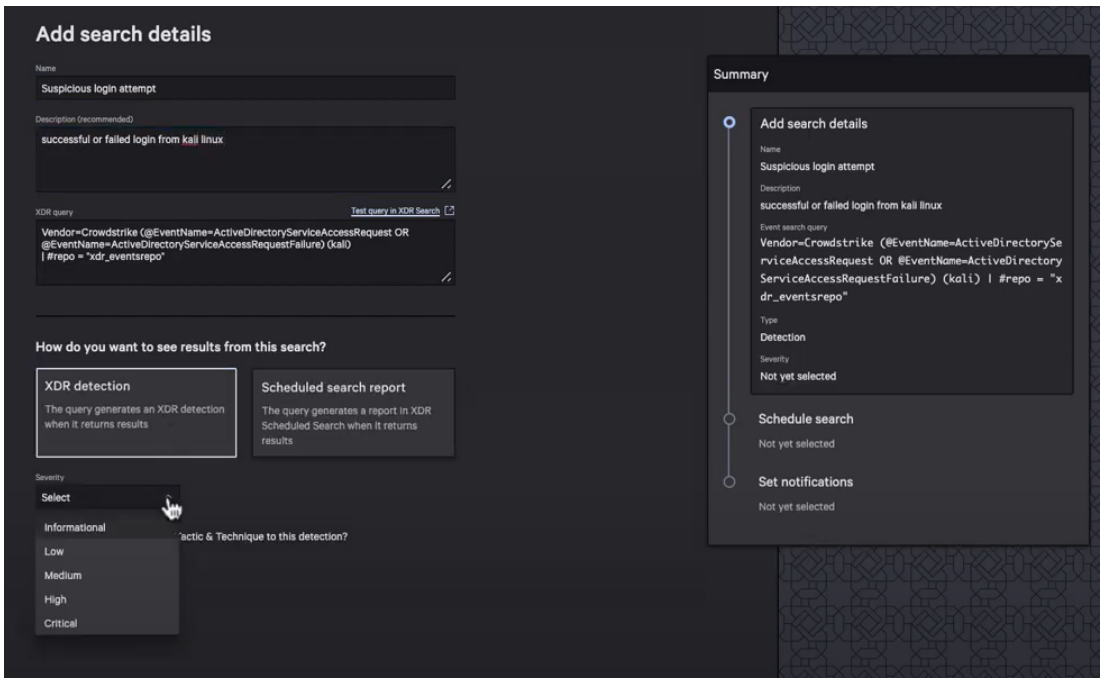

Рис. 3.38. Вибірковий пошук

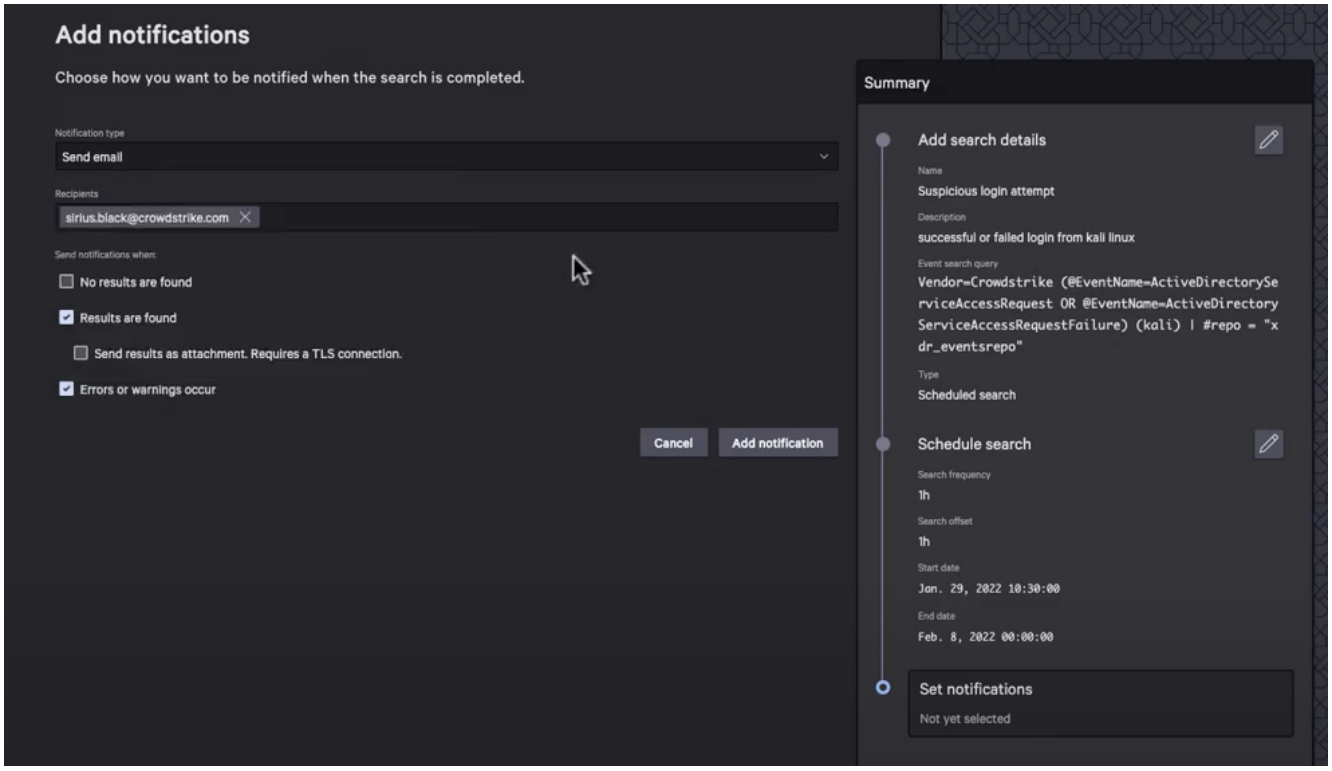

Рис. 3.39. Додавання сповіщень

3.3. Розроблення рекомендацій щодо застосування технології виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR

CrowdStrike Falcon Insight XDR – це потужний інструмент для виявлення та реагування на мережеві атаки. Нижче наведено рекомендації щодо застосування технології.

1. Детальна інвентаризація середовища

Перш ніж розпочати роботу з Falcon Insight XDR, необхідно провести детальну інвентаризацію IT-середовища.

2. Встановлення та конфігурація агента

Правильне встановлення та конфігурація агента Falcon Insight XDR на всіх кінцевих точках є ключовим для ефективної роботи системи.

3. Налаштування правил виявлення

Одним з ключових аспектів Falcon Insight XDR є можливість налаштування правил виявлення. Необхідне створення правил, які відповідають специфічним потребам організації.

4. Інтеграція з іншими системами безпеки

Для забезпечення комплексного захисту необхідно інтегрувати Falcon Insight XDR з іншими системами безпеки, такими як SIEM, Firewall. Це дозволить отримати більш повну картину загроз і ефективніше на них реагувати.

5. Налаштування сповіщень

Створення системи сповіщень, яка оперативно реагуватиме на виявлені інциденти. Налаштування сповіщення на електронну пошту, SMS або через інші канали комунікації.

6. Регулярне оновлення сигнатур

Для забезпечення актуальності захисту необхідне регулярне оновлення сигнатури загроз. Falcon Insight XDR автоматично завантажує нові сигнатури, але варто перевіряти цей процес вручну.

7. Аналіз журналів і звітів

Регулярний аналіз журналів і звітів, щоб виявити тенденції та потенційні загрози.

8. Проведення симуляцій атак

Регулярне проведення симуляцій атак для оцінки ефективності системи захисту та готовності персоналу до реагування на інциденти.

9. Навчання персоналу

10. Розслідування інцидентів

11. Розробка планів реагування на інциденти

Створення детальних планів реагування на різні типи інцидентів.

12. Моніторинг мережевого трафіку

Використання можливостей Falcon Insight XDR для моніторингу мережевого трафіку і виявлення підозрілої активності.

13. Аналіз поведінки користувачів

Аналіз поведінки користувачів для виявлення аномалій, які можуть свідчити про компрометацію облікового запису чи витік даних.

14. Резервне копіювання

Не менш важливе:

- Індивідуальний підхід: налаштування Falcon Insight XDR повинно бути індивідуальним для кожної організації з урахуванням її специфіки та потреб.

- Комплексний підхід: необхідно використовувати Falcon Insight XDR в комплексі з іншими інструментами безпеки для забезпечення максимального захисту.

- Регулярний моніторинг: постійний моніторинг системи і внесення необхідних змін.

- Співпраця з постачальником: при виникненні проблем звертатися за допомогою до фахівців CrowdStrike.

Дотримуючись цих рекомендацій, можна легко та ефективно використовувати CrowdStrike Falcon Insight XDR для захисту організації від мережевих атак і не тільки.

Висновки до розділу 3

1. Розроблено варіант розгортання технології виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR.

2. Продемонстровано роботу технології виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR.

3. Розроблено рекомендації щодо застосування технології виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи отримано наступні результати:

1. Проведено аналіз необхідності виявлення та реагування на мережеві атаки.

2. Приведено класифікацію мережевих атак та векторів атаки.

3. Проаналізовані потенційні наслідки відсутності систем виявлення та реагування на атаки для організації

4. Досліджено методи та засоби виявлення та реагування на мережеві атаки.

5. Представлено архітектуру рішення CrowdStrike Falcon Insight XDR.

6. Розкрито призначення та функції модулів CrowdStrike.

7. Розроблено варіант розгортання технології виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR.

8. Продемонстровано роботу технології виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR.

9. Розроблено рекомендації щодо застосування технології виявлення та реагування мережевих атак на основі CrowdStrike Falcon Insight XDR.

ПЕРЕЛІК ПОСИЛАНЬ

1. Олейников О.Д. Технологія виявлення та реагування мережевих атак на основі XDR. «Актуальні проблеми кібербезпеки» : Всеукр. науково-практ. конф., м. Київ, 25 жовт. 2024 р. Київ, 2024. С. 138–140.

2. What Is Network Detection and Response (NDR)?. Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-network-detection-and-response#five (дата звернення: 05.10.2024).

3. Passeri P. June 2024 Cyber Attacks Statistics. hackmageddon. URL: https://www.hackmageddon.com/2024/10/01/june-2024-cyber-attacks-statistics/ (дата звернення: 05. 10.2024).

4. Jaimovich D. 14 Most Common Types of Cyber Attacks (and How to Prevent Them). InvGate ITSM blog - ITAM, ESM, ITIL, and more. URL: https://blog.invgate.com/types-of-cyber-attacks (дата звернення: 05. 10.2024).

5. Meegammana N. The 7 Layers of Cyber Security : Attacks on OSI model. Journey to ISO 27001. URL: https://iso-27001-journey.blogspot.com/2022/10/the-7-layers-of-cyber-security-attacks.html (дата звернення: 10. 10.2024).

6. Gupta P. What is OSI Model | Comprehensive Guide to OSI Model. EDUCBA. URL: https://www.educba.com/what-is-osi-model/ (дата звернення: 10. 10.2024).

7. Shacklett M. E. What is attack vector?. Search Security. URL: https://www.techtarget.com/searchsecurity/definition/attack-vector (дата звернення: 10. 10.2024).

8. Кібератаки на Україну: огляд, деталі, наслідки - CoreWin. CoreWin. URL: https://corewin.ua/blog/malware-being-used-on-ukrainian-targets/ (дата звернення: 10. 10.2024).

9. Understanding the Difference Between EDR, SIEM, SOAR, and XDR. SentinelOne. URL: https://www.sentinelone.com/cybersecurity-101/xdr/understanding-the-difference-between-edr-siem-soar-and-xdr/ (дата звернення: 28. 10.2024).

10. Xdr Gartner Magic Quadrant 2024 - Addie Anstice. Addie Anstice - Explore ideas, tips guide and info Addie Anstice. URL: https://nanongweneth.pages.dev/cnropfs-xdr-gartner-magic-quadrant-2024-images-hfzavus/ (дата звернення: 28. 10.2024).

11. Magic Quadrant for Endpoint Protection Platforms / E. Mirolyubov та ін. Gartner. URL: https://www.gartner.com/doc/reprints?id=1-2IV5W7LE&ct=240920&st=sb (дата звернення: 28. 10.2024).

12. CrowdStrike Unlocks XDR for All EDR Customers and Expands Third-Party Integrations Across All Key Security Domains. CrowdStrike: We Stop Breaches with AI-native Cybersecurity. URL: https://www.crowdstrike.com/en-us/press-releases/crowdstrike-unlocks-xdr-for-all-edr-customers-and-expands-third-party-integrations/ (дата звернення: 28. 10.2024).

13. Aarness A. What is XDR? Extended Detection & Response | CrowdStrike. CrowdStrike: We Stop Breaches with AI-native Cybersecurity. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/extended-detection-and-response-xdr/ (дата звернення: 30. 10.2024).

14. Vellante D. Breaking Analysis: How CrowdStrike Plans to Become a Generational Platform - theCUBEResearch. theCUBEResearch. URL: https://thecuberesearch.com/breaking-analysis-how-crowdstrike-plans-to-become-a-generational-platform/ (дата звернення: 30. 10.2024).

15. WissenX Akademie. Crowdstrike - All Modules Explained | SOC EDR Vulnerability Management Threat Hunting & Intelligence, 2021. YouTube. URL: https://www.youtube.com/watch?v=_OFQy8w_Fms (дата звернення: 30. 10.2024).

16. How to Install a New CrowdStrike FalconÂ® Sensor [Video]. crowdstrike.com. URL: https://www.crowdstrike.com/resources/videos/installing-new-crowdstrike-falcon-sensor/ (дата звернення: 05.11.2024).

17. CrowdStrike. CrowdStrike Store - Falcon Insight, 2021. YouTube. URL: https://www.youtube.com/watch?v=j0Jl22Mo6B0 (дата звернення: 05.11.2024).

18. Corelight. [Demo Video] Corelight + CrowdStrike Falcon Insight XDR, 2022. YouTube. URL: https://www.youtube.com/watch?v=iU95zSYtiKE (дата звернення: 07.11.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)