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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту кінцевих точок організацій від шкідливого програмного забезпечення на основі машинного навчання та штучного інтелекту»

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

_____ Вадим МИРОНОВ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62
МИРОНОВ Вадим
(прізвище, ім'я)

Керівник к.т.н., доцент ВЛАСЕНКО В.О.
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
кібербезпеки
_____ Галина ГАЙДУР
___ жовтня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

МИРОНОВ Вадима Ігоровичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія захисту кінцевих точок організації від шкідливого програмного забезпечення на основі машинного навчання та штучного інтелекту»
керівник кваліфікаційної роботи Власенко В.О., к.т.н., доцент
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» жовтня 2024 року № ___.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
технічні документи виробників.
рішення XDR.
технічна література, наукові статті, документація вендора, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Технологія впливу машинного навчання та штучного інтелекту на захист кінцевих точок в сучасних EDR та XDR.
2. Аналіз впливу штучного інтелекту на ефективність популярних системах захисту кінцевих точок

3. Практичне дослідження функцій штучного інтелекту в одній із популярних EDR або XDR систем для оцінки їх ефективності

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 19.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення потреби додавання штучного інтелекту в системі захисту кінцевих точок аналізуючи сучасні загрози.	01.10.2024 р.	
2.	Дослідження наукових публікацій та технічної документації вендорів для ознайомлення із продуктами.	12.10.2024 р.	
3.	Аналіз впливу штучного інтелекту на ефективність популярних системах захисту кінцевих точок.	27.10.2024 р.	
4.	Практичне дослідження функцій машинного навчання в одній із популярних EDR або XDR систем для оцінки їх ефективності.	03.11.2024 р.	
5.	Висновок та рекомендації щодо ефективності та переваг штучного інтелекту, з підтвердженням або спростуванням цих тверджень.	15.11.2024 р.	
6.	Оформлення результатів дослідження.	26.11.2024 р.	
7.	Підготовка доповіді до захисту.	15.12.2024 р.	

Здобувач вищої освіти _____ Олександр МИРОНОВ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ В. ВЛАСЕНКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача МИРОНОВ Вадим

на тему: «Технологія захисту кінцевих точок організацій від шкідливого програмного забезпечення на основі машинного навчання та штучного інтелекту»

Актуальність: Кінцеві точки стали невід'ємною частиною життя. Важко уявити людину, яка б не користувалась телефоном або комп'ютером, для роботи або розваг. Якщо звичайна людина сама вирішує що робити зі своїми даними, то великі компанії мають штат співробітників, які працюють із чутливою інформацією на своїх комп'ютерах та ноутбуках, відправляють листи використовуючи свої телефони, зберігають дані на своїх серверах, друкують важливі документи на своїх принтерах. Це все може порушити безпеку інформаційних активів компанії. Для уникнення витоку даних, потрібні надійні системи захисту, такі як: EDR або XDR та штат кваліфікованих співробітників. Але постає питання, що робити, коли сервісів стає більше, кількість пристрої росте, а кіберзагрози оновлюються настільки швидко, що важко відслідкувати.

На допомогу приходить штучний інтелект, що буде доповнювати традиційні функції системи захисту кінцевих точок. Алгоритми машинного навчання допоможуть попереджувати, реагувати та створювати звіти на основі виконаної роботи, а штучний асистент буде підказувати оптимальні кроки для усунення загрози, надавати рекомендацій щодо покращення безпеки, а також допомагати приймати рішення посилаючись на аналіз поточних даних.

Позитивні сторони:

1. При проведенні аналізу, було досліджено вплив штучного інтелекту на ефективність сучасних систем захисту кінцевих точок;
2. Зроблено дослідження існуючих систем захисту кінцевих точок, функції яких використовують алгоритми машинного навчання для покращення роботи;
3. Перевірено на практиці одного із вендорів сучасних EDR, XDR систем для підтвердження або спростування ефективності інтелектуального захисту;
4. В тексті присутні відомості актуальної інформації від виробників систем захисту на момент написання диплому. Робота має чіткі та опрацьовані висновки, які дають відповідь на питання про потребу цифрового інтелекту в сучасних EDR, XDR.

Недоліки:

1. Описане в дипломі має в більшості теоретичні доводи описані в офіційній документації власників продуктів, які не могли бути перевірені через не достаток ресурсів;
2. Не було протестовано в умовах реального використання в компанії;
3. Розробник рішень, який буде перевірятись на практиці був обраний через доступність його перевірки, а не виключно на основі високих рейтингів.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **добре**, а здобувач(ка) **МИРОНОВ Вадим** – присвоєння кваліфікації магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім'я, прізвище)*

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач МИРОНОВ Вадим до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія захисту кінцевих точок організацій від шкідливого програмного забезпечення на основі машинного навчання та штучного інтелекту».
Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***МИРОНОВ Вадим*** обрав тему роботи, метою якої було дослідити зміст технології забезпечення безпечної роботи гібридних працівників організації та розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***МИРОНОВ Вадим*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***МИРОНОВА Вадима*** на оцінку ***добре*** та присвоїти кваліфікацію магістра з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ В. ВЛАСЕНКО
(підпис) *(ім'я, прізвище)*
____ _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **МИРОНОВ Вадим** допускається до захисту даної кваліфікаційної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 109 *сторінок, 24 рисунки, 1 таблиця, 101 джерело.*

Об'єкт дослідження – сучасні засоби захисту кінцевих точок з використанням технологій машинного навчання та штучного інтелекту.

Предмет дослідження – технології, що використовуються для забезпечення безпеки кінцевих точок.

Мета роботи – зробити висновок щодо ефективності та переваг штучного інтелекту, з підтвердженням або спростуванням тверджень виробників продукту.

Методи дослідження – ознайомлення із технічною літературою, публічними науковими статтями, а також офіційною документацією виробника продукту.

Особливу увагу приділено аналізу можливостей штучного інтелекту в системах EDR, XDR, щоб отримати розуміння про ефективність виявлення загроз та способів реагування на них. В роботі показано, як інтеграція засобів комп'ютерного навчання облегшує роботу спеціалістів, для того, щоб вони мали більше часу на дослідження більш складних загроз. Простежено за продуктам різних виробників, для розуміння про сучасні засоби детектування зловмисного впливу на систему. Розглянуто те, як інтелектуальні алгоритми покращують точність виявлення зловмисної активності в системі та у разі отримання інформації про загрозу – знешкоджують її ізолюючи пристрій, щоб уникнути подальшого розповсюдження в системі. Зробити аналіз, чи обґрунтовано впроваджувати цифрових помічників, які будуть аналізувати запити від спеціаліста для створення зрозумілої картини подій, що сталися. Автоматизація створення звітів, які пояснюють простою мовою спеціалістам проблему, яку було вирішено, для подальшого аналізу кібератаки. Також, приділити частину роботи о роздумах, наскільки доцільно впроваджувати нові технології, підрахувати кількість переваг та недоліків.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ШТУЧНИЙ ІНТЕЛЕКТ, МАШИННЕ НАВЧАННЯ, ЗАХИСТ КІНЦЕВИХ ТОЧОК, АВТОМАТИЗАЦІЯ РЕАГУВАННЯ.

ABSTRACT

Text part of the qualification work: 109 pages, 24 figures, 1 table, 10 sources.

Object of research – modern endpoint security tools using machine learning and artificial intelligence technologies..

Subject of research – technologies used to ensure endpoint security.

The aim of research – draw a conclusion about the effectiveness and benefits of artificial intelligence, confirming or refuting the claims of product manufacturers.

Research methods – familiarization with technical literature, public scientific articles, and official documentation of the product manufacturer.

Particular attention is paid to analyzing the capabilities of artificial intelligence in EDR and XDR systems to gain an understanding of the effectiveness of threat detection and response. The paper shows how the integration of computer learning tools facilitates the work of specialists so that they have more time to research more complex threats. Products from different manufacturers are analyzed to understand the state-of-the-art tools for detecting malicious impact on the system.

Consider how intelligent algorithms improve the accuracy of detecting malicious activity in the system and, if information about the threat is received, neutralize it by isolating the device to avoid further spread in the system. Analyze whether it is reasonable to introduce digital assistants that will analyze requests from a specialist to create a clear picture of the events that have occurred. Automate the creation of reports that explain in simple language to specialists the problem that has been solved for further analysis of the cyberattack.

Also, devote part of your work to thinking about how expedient it is to introduce new technologies, calculating the number of advantages and disadvantages.

Field of application – cybersecurity of information resources of the organization.

ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, ENDPOINT PROTECTION, RESPONSE AUTOMATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

EDR - Endpoint Detection and Response

XDR (Extended Detection and Response)

IoT (Internet-of-Things)

BYOD (Bring Your Own Device)

CNAPP (Cloud-Native Application Protection Platform)

DevSecOps (Development, Security, and Operations)

CSPM (Cloud Security Posture Management)

CWPP (Cloud Workload Protection Platform)

XQL (eXtended Query Language)

APT (Advanced Persistent Threats)

NGAV (Next-Gen Antivirus)

AI (Artificial intelligence)

ML (Machine Learning)

SIEM (System Information Event Manager)

MSSP (Managed Security Service Provider)

IAM (Identity and Access Management)

MFA (Multi-factor authentication)

DPI (Deep Packet Inspection)

NIDS (Network Intrusion Detection System)

IoC (Indicators of Compromise)

CASB (Cloud Access Security Broker)

SaaS (Software as a Service)

SSPM (SaaS Security Posture Management)

CNN (Convolutional Neural Networks)

MLP (Multilayer Perceptrons)

DBSCAN (Density-Based Spatial Clustering of Applications with Noise)

GNN (Graph Neural Networks)

LSTM (Long Short-Term Memory)

HMMs (Hidden Markov models)

DQN (Deep Q-Network)

PPO (Proximal Policy Optimization)

KNN (K-Nearest Neighbors)

RNN (Recurrent Neural Networks)

ВСТУП

Актуальність дослідження. З кожним роком, кількість пристроїв, які підключаються до мережі зростає. Сучасні компанії дедалі більше залежать від комп'ютерів, ноутбуків, телефонів, принтерів та інших периферійних пристроїв, які можуть оптимізувати затрати часу при роботі. Із підвищенням кількості таких кінцевих точок в компанії – піднімається ризик стати жертвою кіберзлочинців, які прагнуть отримати конфіденційні дані для подальшого використання у свої зловмисних цілях. Сучасні засоби обробки інформації та комунікації, несуть загрозу не тільки людині, як окремому користувачу через втрату особистих даних, але й компаніям, які можуть втратити свій бізнес через недостатню безпеку пристроїв із якими вони взаємодіють. Щоб захистити робочі пристрої від кібератак – були створені системи для захисту кінцевих точок.

EDR рішення справлялись із своєю задачею, а саме виявляли загрози на рівні кінцевих точок, щоб забезпечувати захист та реагувати на інциденти, але із часом традиційні системи стали недостатньо ефективними для протидіянням загрозам сучасного світу та були змінені на XDR рішення, які покращити свої функції реагування та протидії загрозам завдяки відстежуванню змін в мережевому трафіку та хмарних ресурсах, що дозволило створити комплексний захист не тільки самого обладнання, а й ресурсів до яких це обладнання має доступ. Це було значне покращення, яке й досі використовується багатьма виробниками систем захисту, але все повинно вдосконалюватись, щоб встигати за трендами, тому з часом навіть XDR рішення вже не могли покрити вимоги, які ставали перед системою. Потрібно було створювати системи, які б могли адаптуватись під сучасну інформаційну картину світу. Системи, які б могли самовдосконалюватись.

Штучний інтелект зміг забезпечити справжній проактивний захист, який виявляє та реагує на загрозу до її активації, допомагає автоматизувати рутинні процеси та що найголовніше – навчатися на існуючих загрозах, щоб зупиняти майбутні.

Об'єкт дослідження – дослідження впливу штучного інтелекту на ефективність сучасних систем захисту кінцевих точок.

Предмет дослідження – EPP, EDR та XDR рішення, що використовують штучний інтелект для захисту кінцевих точок.

Мета роботи – дослідити вплив використанням штучного інтелекту в системах захисту кінцевих точок для протидії кіберзагрозам, надати висновки та рекомендації щодо впровадження цих систем.

Наукові завдання:

проаналізувати сучасні дослідження та наукову літературу на предмет доцільності застосування штучного інтелекту в системах захисту кінцевих точок;

порівняти ефективність традиційних систем та сучасних в яких використовується штучний інтелект;

отримати практичні результати протидії загрозам за допомогою функцій комп'ютерного інтелекту впроваджених в системи захисту кінцевих точок;

проаналізувати алгоритми машинного навчання, які можуть використовуватись в сучасних технологіях захисту кінцевих точок;

надати рекомендації по впровадженню, вдосконаленню та адаптації організацій із використанням сучасних рішень захисту кінцевих точок.

Методи дослідження – дослідження та обробка інформації із наукової та технічної літератури, із документації розробника програмного забезпечення та практичні перевірка реагування системи на сучасні загрози.

Практичне значення одержаних результатів: допомога у прийнятті рішення щодо доцільності впровадження системи захисту кінцевих точок із штучним інтелектом, рекомендації по впровадженню систем захисту кінцевих точок зі штучним інтелектом.

1 ДОСЛІДЖЕННЯ ТЕОРЕТИЧНИХ АСПЕКТІВ РОБОТИ ШТУЧНОГО ІНТЕЛЕКТУ ТА СИСТЕМ ЗАХИСТУ КІНЦЕВИХ ТОЧОК

1.1. Ознайомлення із основою базовими поняттями штучного інтелекту та систем захисту кінцевих точок

Кінцева точка - це фізичний пристрій, що підключений до мережі, в якій може обмінюватись інформацією [1].

Кінцеві пристрої надають користувачу доступ до внутрішньої комп'ютерної мережі та виходу в глобальну мережу інтернет для взаємодії із інформаційними ресурсами.

Також є специфічні кінцеві пристрої, які виконують роль датчиків для моніторингу певних подій пов'язаних із критичною інфраструктурою, наприклад: заміри рівня радіації на АЕС.

Пристрої, які виконують роль кінцевих точок можна поділити на 2 типи: обчислювальні та периферійні.

До обчислювального типу пристроїв входить все, що має обчислювальні потужності та допомагає виконувати операції обробки даних. Допомагає взаємодіяти із додатками для виконання роботи. Сюди можна віднести: телефони, ноутбук, комп'ютери, планшети, сервери, віртуальні машини та навіть части інтернет речей, які можуть обробляти та здійснювати обчислення певного типу інформації. Беручи до уваги більш детально функціонал цих пристроїв, можна виділити:

1. *Комп'ютери та ноутбуки* - стандартні офісні пристрої, які покривають базовий функціонал: використання додатків, взаємодія із внутрішньої мережею, взаємодія із інтернетом за допомогою веб-браузера.

2. *Телефони та планшети* - мобільні пристрої, які в нас час можуть виконувати майже весь функціонал, як і комп'ютери з ноутбуками: підключатись до мережі, працювати із додатками, працювати із інтернетом(робити пошуки в інтернеті, працювати із поштою і т.д.). Варто зауважити, що більшість телефонів та планшетів в організації працюють за принципом BYOD, що не дозволяє

додавати його до переліку офісного обладнання, так як це персональний пристрій власника.

3. *Сервери***,** віртуальні *машини***,** функціональні *IoT* та інші подібні пристрої - технологічні пристрої, які в наш час вважаються необхідною складовою кожної компанії. Вони забезпечують обробку та зберігання даних, проводять моніторинг різних систем та загалом допомагають в керування бізнес-процесами в сучасних організаціях.

Периферійні пристрої - виконують роль допоміжних пристроїв, які забезпечують додаткову функціональність: ввід/вивід інформації та виконання нескладних функціональних обов'язків.

В даному випадку, в якості кінцевої точки виступають - багатофункціональні пристрої(БФП), принтери та сканери. Вони організовують друк, сканування та копії документів в середині мережі, займається обміном інформації із іншими пристроями.

Всі ці пристрої можуть бути вразливими перед кібератаками. Якщо вчасно не виявити та не попередити загрозу - наслідки можуть бути критичними для компанії. Від витоку даних компанії до збоїв у роботі бізнес-процесів. У найгіршому сценарії кібератака може призвести до штрафів або навіть репутаційних збитків перед партнерами та клієнтами.

Загрози описані нижче, зможуть показати, важливість уваги на захист кінцевих девайсів в організації [1,2], щоб уникнути проблем описаних вище:

1. *Фішинг* - популярний метод кібератаки, де зловмисники користуються прийомами соціальної інженерії, для отримання інформації конфіденційної інформації методом обману користувача. Конфіденційна інформація може включати в себе: паролі, дані банківських карток або документи із чутливою інформацією. Найчастіше фішинг маскують під електроні листи, які надходять користувачу або групі користувачів. Відправником листа може виступати довірена особа у вигляді партнера, підрядника або навіть внутрішнього користувача компанії, якого було скомпрометовано раніше. Небезпека цього листа полягає в інформації, яка там описана та вкладенні, яке там знаходиться. Це може бути небезпечне посилання при переході на який буде завантажено

шкідливе ПО або перехід на небезпечний сайт, який буде просити ввести облікові дані користувача або ще якусь секретну інформацію. В деяких листах можуть бути небезпечні документи, в яких буде прописаний шкідливий код для крадіжки даних. Всі дії направлені на отримання несанкціонованого доступу до інформації. Достатньо тільки одному із користувачів взаємодіяти із листом - це може призвести до ланцюгу подій, які стануть кібератакою.

Загроза полягає в тому, що антивірусне ПЗ не може побачити шкідливий сайт або файл до того, як він буде відкритий. Людина також не зможе визначити небезпеку без спеціальний знань в області кібербезпеки, бо велика кількість фішингових атак була створена спеціалістами в сфері психології, які знають як підвищити ефективність своїх листів, а тим самим - підвищити рівень ймовірного успіху підловити свою жертву в кіберпросторі;

2. *Програми-вимагачі* є однією з небезпечних форм кіберзлочинності, яка здатна зруйнувати весь бізнес. Зараження кінцевої точки цією програмою шифрує всі файли жертви. Зазвичай даний тип атаки розповсюджується на всю компанію. Є навіть вірогідність шифрування серверів із резервною копією, що унеможливлює відновлення даних. У разі вдалого шифрування даних - зловмисники просят викуп своїх даних. Плату за відновлення доступу до даних. Зазвичай сума викупу становить настільки великі суми, що компанія може бути не готова оплатити її, тому краще вкласти ці гроші в захищеність систем, ніж віддати їх кіберзлочинцям. Але існує ймовірність, що навіть після оплати - дані не будуть розшифровані. Найкраща практика попередження даного типу атаки - стратегія по бєкапуванню даних та захист кінцевих точок, через які загроза може розповсюджуватись на всі інші робочі станції;

3. *Атаки нульового дня* - один з найбільш складних типів загроз. Вони націлені на вразливості ПЗ, про яке не знає розробник, тому відсутні будь-які виправлення або патчі. Кіберзлочинці намагаються використати ці вразливі програми до того, як розробник дізнається про дану загрозу і створить відповідне оновлення. Описане вище означає, що всі системи, які мають дане програмне забезпечення залишаються беззахисними перед таким типом атак. Традиційні засоби безпеки, такі як: антивіруси - не можуть виявити їх сигнатури. Тому для

захисту від цих атак потрібні більш просунуті засоби захисту кінцевих точок, які можуть користуватись даним додатком для роботи;

4. *Відсутність оновлень програмного забезпечення* - ризик для пристрою в подальшому бути скомпрометованим. Деякі оновлення, окрім покращення функціоналу - покращують безпеку. Застаріле програмне забезпечення або вчасно не оновлена система можуть призвести до здійсненню атаки по вразливостям, які не були виправлені в старих версіях. Це може спричинити віддалений доступ до мережі, блокування роботи або доступ до конфіденційних даних. Тому важливо стежити, щоб система та програми, які використовуються не мали застарілих версій;

5. *Слабкі паролі або слабкі політики безпеки* - загроза для системи, яка дає зловмисникам можливість отримати доступ до облікових даних, а в подальшому до файлів. Прості паролі, які не відповідають рекомендаціям, створюють значний ризик як для пристрою так і для мережі в цілому, бо отримавши доступ до однієї машини - можна отримати доступ до всіх, якщо вчасно не ізолювати робочу станцію. Несвоєчасна зміна паролю або використання одного і того ж паролю для декількох облікових засобів спричиняє значну загрозу для безпеки інформаційних ресурсів. Може легко призвести до несанкціонованого доступу до облікових записів. досвідчені хакери часто використовують вкрадені облікові дані для проникнення в різні системи. Такі дані можуть бути отримані через фішингові атаки або витоки інформації, коли велика кількість облікових записів опиняється під загрозою;

6. *Підключення небезпечних USB* та інших переферійних пристроїв – несе значний ризик безпеки кінцевих точок, адже це може призвести до автоматичного завантаження шкідливого ПЗ, яке може вивести з ладу працездатність робочої станції або цілої мережі. Потрібен контроль за тим, що підключається до робочої станції;

7. *Крадіжка або втрата пристрою* – загроза, яка може принести великої шкоди організації у випадку слабкої захищеності пристрою. Відсутність важкого паролю та відсутність шифрування відкриє доступ зловмиснику до важливої інформації;

8. *Ненадійне програмне забезпечення* – завантажування програмного забезпечення з неперевірених джерел, може містити шкідливий код, який в подальшому може бути розгорнутий на робочу станцію або розповсюдитись на всю мережу. Саме використання піратського програмного забезпечення, які не мають регулярних оновлень безпеки або модифіковано іншою людиною, стає загрозою. Важливо контролювати звідки був скачаний додаток та використовувати додатки тільки від перевіреного розробники;

9. *Інсайдерська загроза* – тип компрометації конфіденційних даних від навмисних чи ненавмисних дій внутрішнього співробітника компанії. До цього необережність та незнання правил безпеки людиною або якщо людина мала зловмисні наміри по передачі інформації іншій компанії. Регулярне навчання співробітників із кібербезпеки та моніторинг їхньої активності допомагає знизити ці ризики.

Безпека кінцевих пристроїв є критично важливою складовою загальної кібербезпеки організації, оскільки саме через кінцеві точки найчастіше здійснюються атаки. Всі загрози описані вище можуть легко скомпрометувати кінцеві пристрої, призвести до втрати конфіденційних даних та значних фінансових збитків. Підірвати довіру партнерів та підрядників, що може призвести до зниження репутації компанії.

Недостатня увага до безпеки кінцевих точок може призвести до кібератак, що здатні принести проблему компанії. Щоб цього уникнути потрібно приділяти увагу до захисту кінцевих точок, впроваджуючи системи захисту по типу: EDR, XDR – рішень

Сучасні системи захисту інформації все частіше інтегруються із штучним інтелектом для підвищення ефективності виявлення загроз, а також реагування на них. Використанням алгоритмів машинного навчання дозволяє аналізувати велику кількість даних, щоб потім, на основі проаналізованих даних – виявляти аномалії в роботі. Важливо розуміти базові поняття про штучний інтелект, щоб можна було проаналізувати його роботу.

Штучний інтелект - це технічна та наукова галузь, присвячена спроектованій системі, яка генерує вихідні дані, такі як зміст, прогнози,

рекомендації або рішення для певного набору цілей, визначених людиною [5]. Генеративний штучний інтелект відрізняється від традиційного сферами застосування та задачами, де його можна застосовувати. Традиційний штучний інтелект в основному знаходить своє використання в аналізі даних та прогнозуванні. Сучасна система штучного інтелекту, яка побудована на генеративному ШІ - створює нові дані.

Data Science – це наука, яка розповідає про методи аналізу та вилучення цінної інформації із даних. Дана наука має взаємозв'язок із іншими галузями, такими як: наука про мислення, машинне навчання та робота із великими масивами даних. Дані проходять етапи обробки та підготовки для того, що в подальшому на них можна було навчити алгоритм виконувати певні задачі [4,6].

Machine Learning - можна виділити як підмножину штучного інтелекту, але це також є наука о розробці алгоритмів, які здатні навчатись на основі великих обсягів даних без потреби налаштовувати та програмувати кожне рішення. Алгоритм знаходить закономірності та патерни в інформації, які надаються для навчання. Основна суть полягає в тому, що замість програмування кожного сценарію під окремі задачи, можна зробити щоб модель сама навчалась на тих даних, які їй були надані [5].

Один з найсучасніших та найефективніших напрямків машинного навчання є *глибоке машинне навчання* [4,6]. Цей напрям використовує *нейронні мережі*, які моделюють роботу людського мозку, навчається на основі свого досвіду та із урахуванням своїх помилок, кожного разу роблячи краще свої результати.

Ключові параметри для ефективного навчання моделі [4]:

Дані – це базова інформація, дані, на яких потрібно навчати систему. Дані не повинні містити помилки, так як це може погано вплинути на модель, яка навчається. Тому варто добре структурувати та обробляти дані, для отримання більш релевантних відповідей та точних прогнозів.

Ознаки – це конкретна характеристика даних, яку використовують для навчання моделі. Від правильних ознак залежить точність моделі. Чи більше інформативними є ознаки, тим краще модель зможе розпізнавати закономірності

та робити прогнози.

Алгоритм – це інструкція або послідовність дій для вирішення задачі. Від алгоритму залежить, які математичні операції будуть виконуватись для досягнення результату. Алгоритм впливає на ефективність навчання моделі, обробку даних та прогнозування.

Види машинного навчання:

Навчання із вчителем – підхід навчання моделі із використанням мічених даних, де мітка може позначати правильну відповідь. Обраний об’єкт буде помічений правильно для того, щоб вона навчилась розпізнавати об’єкт в майбньому;

Навчання без вчителя – підхід навчання моделі де відсутні мітки. Модель вивчає подібності в даних. Вона самостійно знаходить структуру без необхідності їх помічати. Метод використовується при кластеризації даних або виявлення аномалій;

Навчання з підкріпленням – підхід до навчання побудований на основі винагород та покарань за свої дії. Цей підхід має популярність у динамічних середовищах: ігри або автономне керування транспортом.

Є моделі машинного навчання, які можуть використовувати свої алгоритми для протидії загрозам:

Автоенкодер (універсальний метод) - це нейронна мережа, що складається з енкодера для стискання даних і декодера для їх відновлення, з мінімізацією похибки реконструкції. Його навчають на нормальних даних, щоб точно відтворювати їх, але при обробці аномалій похибка реконструкції суттєво зростає, що дозволяє їх виявляти. Основні застосування автоенкодерів включають виявлення аномалій, зменшення розмірності даних, видалення шуму та генерацію нових зразків. Їх універсальність робить автоенкодери цінним інструментом для аналізу даних у різних доменах [82].

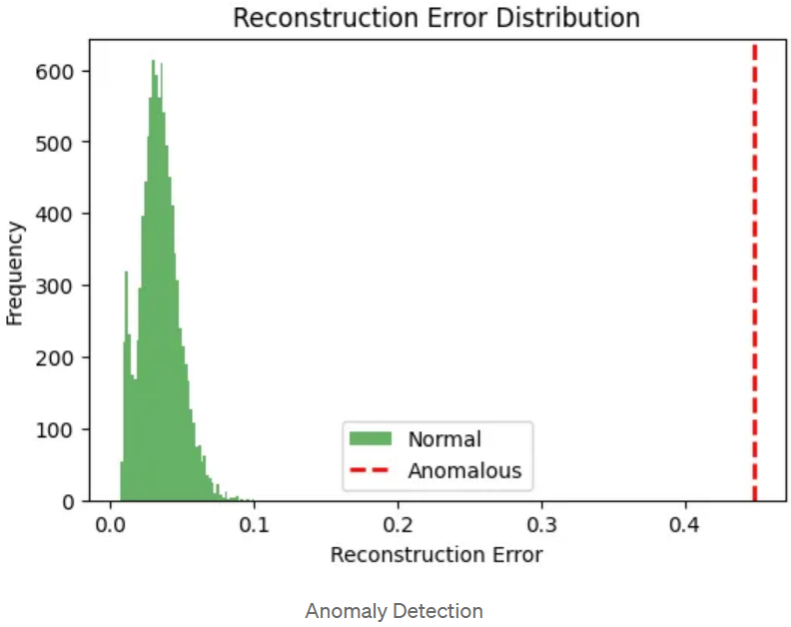


Рис 1.1. Розподіл похибки реконструкції для виявлення аномалій [82]

Isolation Forest - це алгоритм для виявлення аномалій, який працює шляхом випадкового поділу даних і швидко ізолює відхилення (рисунок 1.2). Аномальні точки ізолюються швидше, оскільки вони суттєво відрізняються від решти даних. Цей метод ефективний для аналізу великих наборів даних і не потребує попереднього навчання. У кібербезпеці він використовується для виявлення незвичної активності, такої як кібератаки чи несанкціонований доступ. Завдяки простоті та ефективності, Isolation Forest допомагає вчасно реагувати на загрози [83].

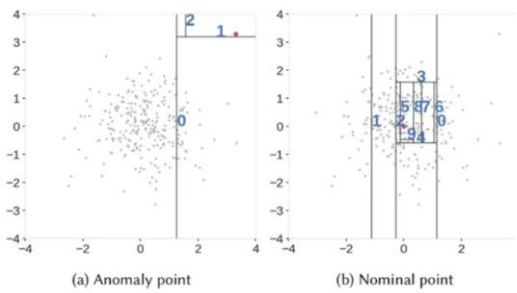


Рис 1.2. Процес ізоляції аномальних і нормальних точок в Isolation Forest [83]

One-Class SVM - це алгоритм машинного навчання, призначений для виявлення аномалій, коли доступні лише нормальні дані для навчання. Він створює гіперплощину, що охоплює більшість нормальних точок у просторі ознак; нові точки, що знаходяться поза цією областю, класифікуються як аномалії (рисунок 1.3). У сфері кібербезпеки One-Class SVM використовується для виявлення незвичайної активності, такої як несанкціонований доступ або аномалії в мережевому трафіку, шляхом ідентифікації відхилень від нормальної поведінки. Це дозволяє ефективно виявляти потенційні загрози, навіть без наявності даних про попередні атаки [84].

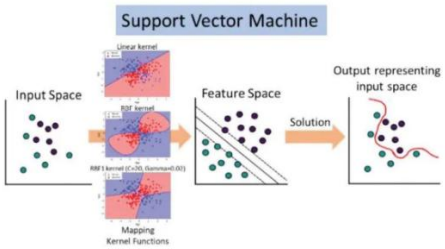


Рис 1.3. Розділ класів за допомогою гіперплоскості в Support Vector Machine (SVM) [85]

Random Forest (універсальний метод) - це алгоритм машинного навчання, який створює ансамбль дерев рішень для покращення точності та надійності прогнозів. Кожне дерево може прийняти своє рішення, після цього відповіді аналізуються і утворюється загальна оцінка. У сфері кібербезпеки, зокрема для захисту від фішингових атак, Random Forest аналізує різноманітні характеристики, такі як компоненти URL, вміст електронних листів, інформацію про відправника та сертифікати SSL/TLS, щоб визначити, чи є ресурс легітимним або потенційною фішинговою загрозою [86].

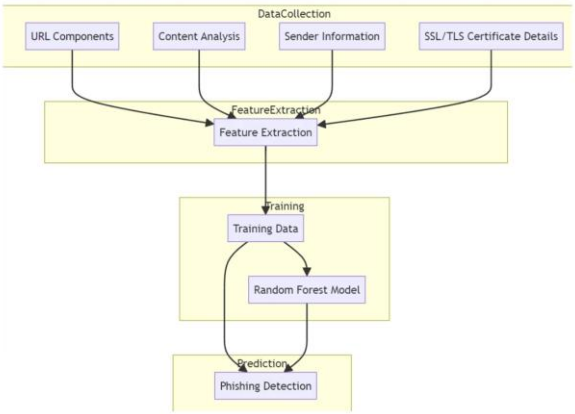


Рис 1.4. Процес виявлення фішингу за допомогою Random Forest [86]

SVM - це алгоритм машинного навчання, призначений для виявлення аномалій, коли доступні лише нормальні дані для навчання. One-Class SVM створює одну межу для визначення, чи належить точка до нормального класу, тоді як звичайний SVM розділяє дані між двома або більше класами за допомогою кількох меж [84].

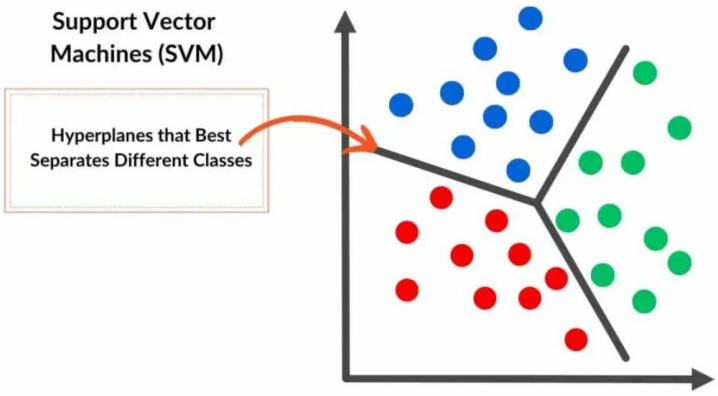


Рис 1.5. Гіперплощини для розділення класів у Support Vector Machine (SVM) [84]

Логістична регресія - це статистичний метод для бінарної класифікації, який оцінює ймовірність належності об'єкта до одного з двох класів. У кібербезпеці її застосовують для ідентифікації фішингових загроз, класифікуючи електронні листи або веб-сторінки як легітимні чи фішингові на основі аналізу

різних характеристик. Завдяки своїй здатності ефективно розрізняти між двома можливими станами, логістична регресія є корисним інструментом для підвищення захисту від фішингових атак [87].

Convolutional Neural Networks (CNN) - це тип глибоких нейронних мереж, які спеціалізуються на аналізі зображень і структурованих даних. Вони використовують конволюційні шари для виділення ключових особливостей, таких як контури чи текстури, що дозволяє ефективно працювати з візуальною інформацією [98]. У кібербезпеці CNN застосовуються для виявлення шкідливого ПЗ за аналізом пам’яті чи динамічних графічних підписів, а також для ідентифікації фішингових веб-сайтів.

Multilayer Perceptrons (MLP) - це базова архітектура нейронних мереж, яка складається з вхідного шару, одного або кількох прихованих шарів і вихідного шару. MLP працює із структурованими даними та використовується для загальних задач класифікації й регресії [99]. У кібербезпеці MLP може виконувати класифікацію електронних листів як спам або аналізувати лог-файли для виявлення аномалій.

K-means - це популярний алгоритм кластеризації, який розділяє дані на k груп, на кластери (рисунок 1.6) на основі схожості між ними. У сфері кібербезпеки K-means застосовується для виявлення аномалій, класифікації шкідливого ПЗ та фільтрації спаму [88].

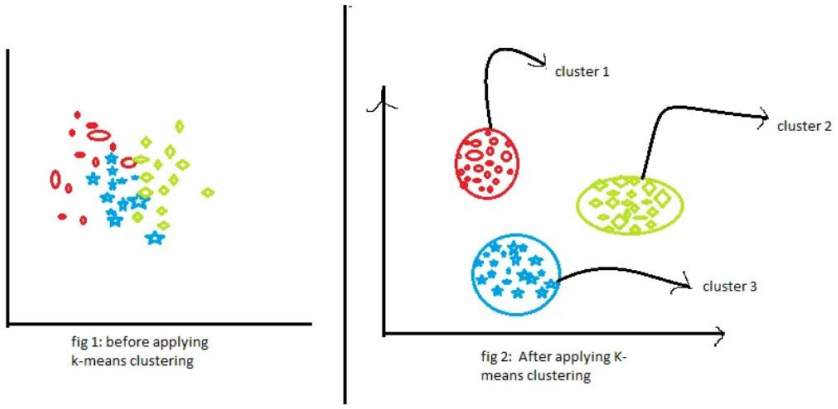


Рис 1.6. K-means кластеризація [88]

DBSCAN (Density-Based Spatial Clustering of Applications with Noise) - це алгоритм кластеризації, який групує точки даних на основі їхньої щільності, дозволяючи виявляти кластери довільної форми та ідентифікувати аномалії або шум [89]. На відміну від K-means, DBSCAN не вимагає заздалегідь визначати кількість кластерів і ефективно працює з даними, що містять шуми та викиди. У сфері кібербезпеки DBSCAN застосовується для виявлення аномальної активності в мережевому трафіку, ідентифікації підозрілих патернів та кластеризації подій без необхідності попереднього знання кількості загроз, що робить його цінним інструментом для аналізу складних і нерегулярних даних.

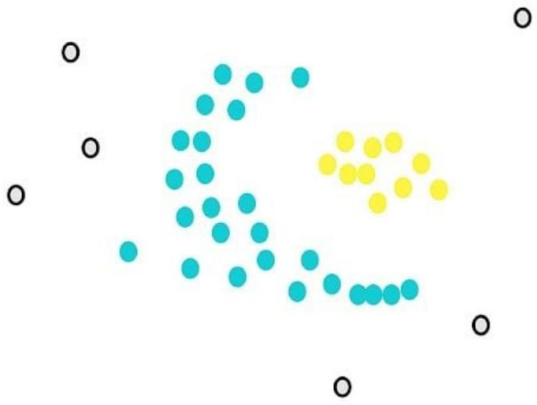


Рис 1.7. Ілюстрація кластеризації DBSCAN: щільні кластери та ідентифікація шуму [89]

Graph Neural Networks (GNN) - це тип глибоких нейронних мереж, які працюють з графовими даними, де об'єкти представляються вузлами, а їхні взаємозв’язки - ребрами. GNN дозволяють вузлам обмінюватися інформацією з сусідами, що дозволяє враховувати як локальний контекст, так і глобальну структуру графа [100]. У кібербезпеці GNN використовуються для аналізу мережевого трафіку, виявлення аномалій у поведінці користувачів, ідентифікації зловмисних IP-адрес і прогнозування потенційних загроз на основі взаємозв’язків у даних. Завдяки своїй здатності аналізувати складні графові

структури, GNN є потужним інструментом для роботи з даними в системах захисту інформації.

Також варто згадати метод ієрархічної кластеризації, який використовує підхід поступового об’єднання або розділення кластерів для створення ієрархії груп даних. Цей метод включає велику кількість алгоритмів, таких як метод одиночної зв’язності, повної зв’язності та Уорда, які дозволяють адаптувати кластеризацію до різних типів даних. Проте через велику кількість таких алгоритмів їх детальний опис виходить за межі цього тексту.

LSTM (Long Short-Term Memory) (універсальний метод) - це тип рекурентної нейронної мережі, яка здатна зберігати та використовувати інформацію з довгих послідовностей даних завдяки механізмам забування, збереження та передачі важливої інформації (рисунок 1.7). Основна особливість LSTM - здатність виявляти довготривалі залежності в даних, що дозволяє ефективно аналізувати складні часові ряди та патерни [90]. У кібербезпеці LSTM використовується для виявлення аномалій і прогнозування атак, аналізуючи історичні дані та реальний час, що допомагає ідентифікувати багатоступеневі загрози або нетипову активність.

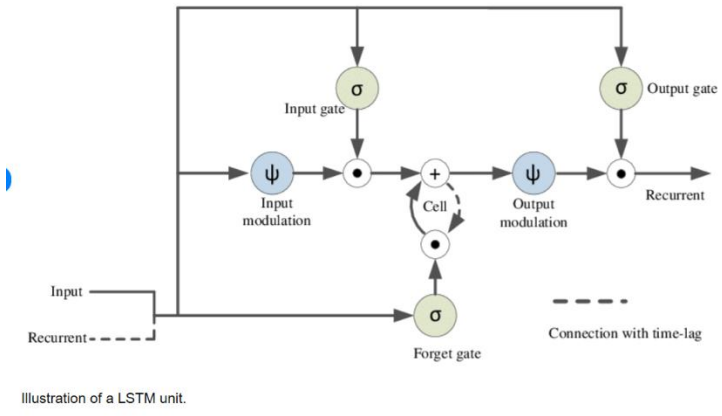


Рис 1.8. Ілюстрація роботи LSTM [90]

Прихована марковська модель (HMM) - це статистична модель, яка описує систему через послідовність прихованих станів, що впливають на спостережувані події, причому ймовірність переходу до наступного стану

залежить лише від поточного стану. HMM використовується для аналізу часових рядів та моделювання ймовірностей переходу між подіями [91]. У кібербезпеці HMM допомагає аналізувати послідовності дій, прогнозувати можливі загрози та виявляти нетипову поведінку, наприклад, підозрілі послідовності дій користувачів або багатоступеневі атаки.

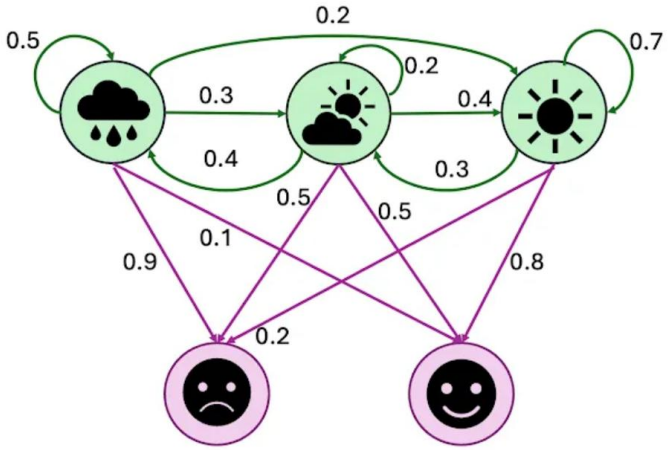


Рис 1.9. Приклад роботи HMM [91]

Q-Learning - це алгоритм навчання з підкріпленням, який дозволяє агенту навчатися оптимальним діям у середовищі на основі винагороди, не потребуючи попередньої моделі середовища. Він зберігає значення дій у Q-таблиці, щоб вибирати найкращі рішення для досягнення максимальної винагороди [92]. У кібербезпеці Q-Learning використовується для автоматизації реагування на загрози, визначення оптимальної послідовності дій (наприклад, ізоляція вузлів чи блокування атак), а також адаптації до нових загроз у реальному часі, що підвищує ефективність захисту.

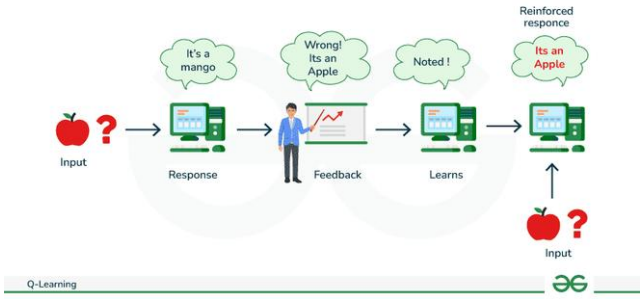


Рис 1.10. Приклад роботи Q-Learning [93]

Deep Q-Network (DQN) - це алгоритм навчання з підкріпленням, який поєднує Q-Learning із глибокими нейронними мережами для вирішення задач у складних середовищах із великою кількістю станів. Нейронна мережа в DQN замінює Q-таблицю, прогнозуючи Q-значення для кожної можливої дії в заданому стані, що дозволяє навчатися оптимальним стратегіям навіть у динамічних і багатовимірних умовах [94]. У кібербезпеці DQN використовується для автоматизації реагування на складні атаки, аналізу мережевого трафіку та адаптації до нових загроз у реальному часі, забезпечуючи більш ефективне управління ризиками та протидію атакам.

Proximal Policy Optimization (PPO) - це алгоритм навчання з підкріпленням, який дозволяє агенту оптимізувати свої дії для досягнення максимальної винагороди, зберігаючи стабільність і ефективність. PPO обмежує великі зміни у стратегії через механізм кліпінгу, що робить навчання більш надійним і адаптивним для складних середовищ [95]. У кібербезпеці PPO використовується для автоматизації реагування на загрози, вибору оптимальних дій у реальному часі та адаптації до нових атак, забезпечуючи ефективне та динамічне управління захистом.

K-Nearest Neighbors (KNN) (універсальний) - це простий алгоритм машинного навчання, який використовується для класифікації та регресії, ґрунтуючись на схожості нових даних із відомими зразками. Алгоритм порівнює новий об'єкт із K найближчими сусідами в багатовимірному просторі характеристик, використовуючи метрики відстані (наприклад, евклідову відстань), і визначає клас об'єкта на основі більшості сусідів [96, 97]. У

кібербезпеці KNN застосовується для виявлення шкідливого ПЗ, аналізу мережевого трафіку та класифікації загроз. Наприклад, він може ідентифікувати шкідливі програми на основі їхніх характеристик, як-от API-виклики чи патерни поведінки, допомагаючи швидко та точно розрізняти безпечні й небезпечні об'єкти [96].

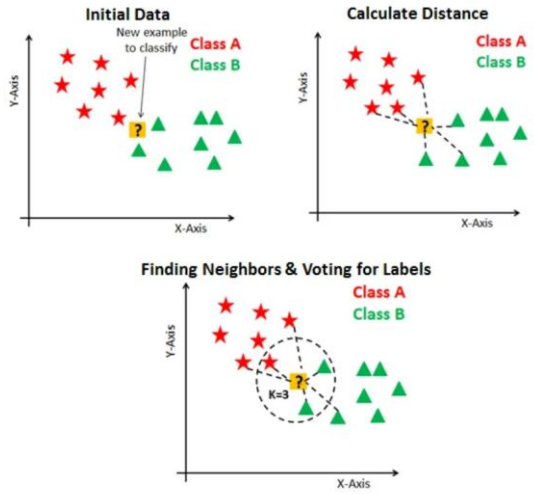


Рис 1.11. Приклад роботи K-Nearest Neighbors [96]

Recurrent Neural Networks (RNN) - це тип глибоких нейронних мереж, які працюють із послідовними даними, такими як текст, часова серія чи логи. Вони використовують зворотні зв’язки для запам’ятовування інформації з попередніх кроків, що дозволяє враховувати контекст у часі [101]. У кібербезпеці RNN застосовуються для аналізу мережевих логів, виявлення патернів у послідовностях атак і прогнозування майбутніх загроз на основі історичних даних. Завдяки здатності моделювати поведінкові послідовності, RNN допомагають ідентифікувати складні багатоступеневі атаки та відхилення від нормальної поведінки.

1.2 Еволюція технологій захисту кінцевих точок

Еволюція систем захисту кінцевих точок: детальний аналіз методів та

технологій [7].

*Період із 2005-2010 рік***.**

*1***.** *Виявлення за сигнатурами*

Цей метод базується на порівнянні файлів і програм із базою даних відомих сигнатур шкідливого програмного забезпечення. Сигнатура - це унікальний цифровий відбиток вірусу або іншої шкідливої програми, отриманий шляхом аналізу її коду [8].

*2***.** *Евристичне виявлення*

Евристичні методи аналізують код програм на наявність підозрілої поведінки в системі та структурі коду, що може бути характерним для шкідливого ПЗ. Це дозволяє виявляти невідомі або модифіковані віруси, які ще не мають сигнатур. Алгоритми евристичного аналізу ставали більш складними, враховуючи нові техніки маскування шкідливого ПЗ. Це допомогло зменшити кількість хибнопозитивних спрацювань та підвищити ефективність виявлення [9].

*3***.** *Аналіз журналів*

Моніторинг системних журналів (логів) для виявлення аномальних або підозрілих дій. Журнали містять інформацію про роботу системи, запуск програм, зміни в налаштуваннях тощо. З часом з'явилися інструменти для автоматизації аналізу логів, що дозволило швидше реагувати на інциденти. Інтеграція з системами оповіщення підвищила ефективність реагування.

*4***.** *Системи виявлення вторгнень на основі хостів* **(***HIDS***)**

HIDS моніторять активність на окремих пристроях (хостах) для виявлення ознак вторгнення або несанкціонованого доступу. Вони аналізують зміни в файлах, налаштуваннях системи та інші параметри [10]. Розширення можливостей HIDS включало інтеграцію з іншими системами безпеки та покращення алгоритмів виявлення шляхом впровадження більш складних правил та профілів поведінки.

*5***.** *Брандмауери*

Брандмауери контролюють вхідний та вихідний мережевий трафік на основі встановлених правил безпеки. Вони блокують небажані з'єднання та

захищають систему від мережевих атак [11]. Від простих пакетних фільтрів до станційних брандмауерів, які враховують стан з'єднань та застосунків. З'явилися також персональні брандмауери для індивідуальних користувачів.

6. Антивірусне програмне забезпечення

Поєднує різні методи, такі як виявлення за сигнатурами та евристичний аналіз, для виявлення та видалення шкідливого ПЗ. Антивіруси сканують різні файли для виявлення зловмисної активності [12].

7. Ручне реагування на інциденти

Команди безпеки аналізують та реагують на інциденти вручну, використовуючи свій досвід та інструменти для виявлення та усунення загроз. Розробка стандартної політики безпеки при роботі із кінцевими пристроями та забезпечення реагування на атаки.

8. Візуалізація дисків і криміналістика

Створення точних копій (образів) дисків для аналізу та збереження доказів. Криміналістичний аналіз допомагає виявити джерело загрози та спосіб проникнення [13]. Розробка більш досконалих інструментів для швидкого візуалізації та аналізу великих обсягів даних.

9. Шифрування кінцевих точок

Захист даних на пристрої шляхом їхнього шифрування, що унеможливлює доступ до них без відповідних ключів або паролів. Від шифрування окремих файлів до повного шифрування диска [14].

10. Контроль на основі політик

Встановлення правил та політик, що визначають, які дії дозволені на кінцевих точках. Наприклад, обмеження встановлення програм або доступу до певних ресурсів. Розробка централізованих систем управління політиками, що дозволяють застосовувати їх на всіх пристроях організації.

Цей період характеризується на статичних підходах, таких як виявлення за сигнатурами та прості евристичні аналізи. Обмеження цих методів, зокрема їхня мала ефективність проти нових та невідомих загроз, підкреслили потребу в більш адаптивних та інтелектуальних рішеннях. Хоча штучний інтелект ще не був широко застосований в даний період часу, саме в цей час стало зрозуміло, що

традиційні методи недостатні для ефективного захисту.

Вплив на розвиток ШІ:

- потреба в більш ефективних рішеннях спонукала дослідників, аналітиків та інженерів звернути увагу на потенціал ШІ та алгоритмів машинного навчання;
- інтеграція простих евристичних методів створила основу для подальшого впровадження машинного навчання;
- зростання кількості та складності кіберзагроз вимагало нових підходів, що підштовхнуло розвиток ШІ в сфері безпеки.

*Період із 2011-2015 рік***.**

*1***.** *Поведінковий аналіз*

Моніторинг та аналіз поведінки програм та користувачів для виявлення підозрілих або аномальних дій [15]. Наприклад, раптове видалення великої кількості файлів або нетипова мережна активність. Впровадження більш складних алгоритмів, які враховують контекст та історію поведінки для зменшення хибнопозитивних результатів.

*2***.** *Експертиза пам'яті*

Аналіз оперативної пам'яті системи, може бути корисним для аналізу дампів пам'яті, щоб виявляти складні загрози, такі як руткіти та безфайлові шкідливі програм, які не залишають слідів на диску. Розробка інструментів для збереження та аналізу дампів пам'яті.

*3***.** *Аналіз мережевого трафіку*

Моніторинг та аналіз мережевого трафіку для виявлення аномалій або підозрілих з'єднань за допомогою технології NIDS [16]. Глубокий аналіз трафіку починаючи із другого рівня моделі OSI за допомогою технології DPI [17].

*4***.** *Виявлення індикаторів компрометації* **(***IoC***)**

Використання відомих індикаторів компрометації, таких як хеші файлів, записи системних журналів IP-адреси, домени, які можуть вказувати, що в систему проникла загроза [18]. Автоматизація процесу збору та обміну IoC між організаціями та системами безпеки.

*5***.** *Евристичні виявлення*

Додаткове застосування евристичних методів для виявлення нових та модифікованих загроз шляхом аналізу поведінки та структур коду. Відбулося покращення алгоритмів та зменшення хибнопозитивних спрацювань шляхом врахування контексту та історії подій. Використання машинного навчання для підвищення точності евристичних методів.

6. Пісочниця

Запускає підозрілі файли в ізольованому середовищі (пісочниці), що може імітувати систему користувача, для спостереження за їхньою поведінкою без ризику для основної системи [19]. Створення більш реалістичних пісочниць, які важко відрізнити від реальної системи, щоб обманути складні шкідливі програми.

7. Виявлення аномалій

Використовує статистичні моделі та алгоритми машинного навчання для виявлення відхилень від нормальної поведінки системи або користувачів. Впровадження адаптивних моделей, які враховують зміну поведінки з часом.

Зі збільшенням складності кібератак традиційні методи виявилися ще менш ефективними. У цей період почали активно застосовувати поведінковий аналіз, виявлення аномалій та пісочниці. Почали більше досліджувати питання про використання індикаторів компрометації. З’явилися перші алгоритми машинного навчання, які використовувалися для покращення точності виявлення загрози та зменшення кількості хибнопозитивних результатів, що покращувало аналітику.

Вплив на розвиток ШІ:

- початок використання алгоритмів машинного навчання показало їхню ефективність та потенціал у сфері безпеки, що посприяло його розповсюдженню;
- збір та аналіз даних про поведінку систем та користувачів створили базу для тренування моделей штучного інтелекту;
- необхідність в обробці та інтерпретації складних даних стимулювала розвиток алгоритмів та методів машинного навчання.

Період із 2016-2020 рік

1. Машинне навчання та аналіз поведінки

Алгоритми машинного навчання почали аналізувати великі обсяги даних про поведінку програм та користувачів для виявлення складних загроз. Впровадження глибокого навчання та нейронних мереж для аналізу більш складних патернів.

2. Ізоляція кінцевих точок

Автоматичне або ручне ізолювання зараженого пристрою від мережі для запобігання поширенню загрози під час розслідування інциденту [20]. Інтеграція з системами управління та автоматизація процесу ізоляції.

3. Хмарні рішення EDR

Endpoint Detection and Response (EDR) рішення, які окрім роботи локально, мають змогу працюють у хмарі, дозволяють централізовано збирати та аналізувати дані з кінцевих точок [20]. Підвищення масштабованості та доступності, інтеграція з іншими хмарними сервісами.

4. Виявлення шкідливих програм без файлів

Виявляє шкідливі програми, які не залишають файлів на диску, працюючи лише в оперативній пам'яті або використовуючи легітимні системні процеси. Розробка інструментів для моніторингу пам'яті та аналізу динамічної поведінки системи.

5. Технології обману **(***deception technologies***)**

Створюють фальшиві ресурси(пристрої, користувачі), пастки та приманки, щоб виявити та відволікти атакуючих [21]. Покращення реалістичності обманних середовищ та інтеграція з іншими системами безпеки.

6. Безпека кінцевих точок IoT та OT

Захист пристроїв Інтернету речей (IoT) та операційних технологій (OT), які часто мають обмежені можливості безпеки. Розробка спеціалізованих рішень для моніторингу та захисту цих пристроїв, враховуючи їхні специфічні потреби та обмеження.

7. Аналіз поведінки користувачів та організацій **(***UEBA***)**

Моніторинг та аналіз поведінки користувачів для виявлення аномальної поведінки або відхилення в його діях [22]. Інтеграція з іншими системами

безпеки та використання більш складних моделей поведінки.

8. Інтеграція API **(***інтерфейсу додатків та програмування***)**

Використання API для інтеграції різних систем та інструментів безпеки, що дозволяє автоматизувати процеси та покращити обмін даними. Відкриті API та стандартизація протоколів спростили інтеграцію та взаємодію між системами.

9. Обмін потоковою аналітикою

Обробка та аналіз даних про безпеку в реальному часі з різних джерел(Приклад: різні системи захисту або різні типи кінцевих точок) для швидкого виявлення та реагування на загрози.

Цей період характеризується значним стрибком у застосуванні ШІ в системах захисту. Машинне навчання стало ключовим інструментом для аналізу великих обсягів даних та виявлення складних і невідомих загроз. Використання глибокого навчання та нейронних мереж дозволило значно підвищити ефективність виявлення та зменшити кількість хибних спрацювань.

*Вплив на розвиток ШІ***:**

- існуючі сучасні загрози в кіберпросторі стимулювали покращення існуючих та розробку нових алгоритмів ШІ;
- необхідність в обробці великих обсягів даних призвела до розвитку апаратного забезпечення та хмарних технологій, що, в свою чергу, сприяло розвитку систем штучного інтелекту;
- успіх у застосуванні ШІ в безпеці сприяло його впровадженню в інші сфери та підвищило довіру до технології. І навпаки, впровадження в різні процеси сприяло продовження розвитку даної сфери в кібербезпеці.

В період із 2021-2024 рік

1. Розширене виявлення та реагування **(***XDR***)**

Об'єднує дані з різних джерел: кінцевих точок, мереж, хмарних сервісів для цілісного виявлення та реагування на загрози [23]. Інтеграція з SIEM (Security Information and Event Management) та SOAR (Security Orchestration, Automation, and Response) системами для автоматизації процесів.

2. Архітектура нульової довіри **(***Zero Trust Architecture***)**

Принцип ніколи не довіряй, завжди перевіряй передбачає постійну

верифікацію всіх користувачів та пристроїв незалежно від їхнього місцезнаходження. Впровадження мікросегментації мережі, багатофакторної автентифікації та динамічного контролю доступу [24].

3. Виявлення загроз на основі штучного інтелекту

Використовує передові методи ШІ, такі як глибоке навчання та нейронні мережі, для прогнозування та виявлення нових загроз. Постійне навчання моделей на актуальних даних про загрози, включаючи інформацію з відкритих джерел та темного вебу.

4. Захист на основі аналізу загроз

Використовує інформацію про актуальні загрози для адаптації систем безпеки та налаштування захисту. Інтеграція з автоматизованими системами реагування та оновлення захисту в реальному часі.

5. Поведінкова біометрія

Аналізує унікальні поведінкові характеристики користувачів, такі як ритм набору тексту, рухи миші, для автентифікації та виявлення аномалій. Покращена технологія поведінкового аналізу користувача на персональних, специфічних шаблонах його дій. Покращення точності та надійності за рахунок більш складних моделей та алгоритмів.

6. Хмарні рішення EDR

Розширення функціональності EDR для хмарних середовищ та віддалених робочих місць, враховуючи зміни в робочих моделях (віддалена робота). Підвищення масштабованості та доступності, інтеграція з хмарними сервісами та платформами.

7. Автоматизоване реагування на інциденти

Система автоматично, швидко та точно реагує на загрозу до того, як вона стане порушенням, зменшуючи час реагування та мінімізуючи людський фактор [25]. Впровадження SOAR платформ зможе покращити ефективність для комплексної автоматизації та оркестрації процесів безпеки.

8. Інтеграція екосистем

Об'єднання різних систем безпеки та інструментів в єдину екосистему для покращення видимості та ефективності. Відкриті стандарти, API та спільні

платформи дозволили різним продуктам взаємодіяти та обмінюватися даними.

У цей період ШІ став центральним елементом у розробці передових систем захисту, таких як XDR та архітектура нульової довіри. Складність та швидкість сучасних кібератак вимагали від систем безпеки можливості прогнозувати загрози та реагувати на них в реальному часі. ШІ та машинне навчання стали критичними для аналізу великих обсягів даних, автоматизації реагування та прийняття рішень.

*Вплив на розвиток ШІ***:**

- виклики сучасних загроз стимулювали розвиток більш точних та швидких моделей ШІ;
- автоматизація в системах реагування посприяло розвитку ШІ, здатного приймати рішення без втручання людини.
- розвиток хмарних технологій та розподілених обчислень дозволив масштабувати напрями застосування ШІ та підвищити його ефективність.
- зростання залежності від ШІ в безпеці привернуло увагу до питань етики, прозорості алгоритмів та захисту від маніпуляцій.

1.3 Архітектура системи захисту кінцевих точок: компоненти, методи та роль штучного інтелекту

Архітектура системи захисту кінцевих точок (EDR) складається з двох основних компонентів: серверної частини та агентів, встановлених на кінцеві точки. Кінцевими точками виступають пристрої, які описані в розділі 1.1, які підключені до корпоративної мережі. Всі ці пристрої потребують захист від кіберзагроз. В архітектурі відмічені 2 основні частини: серверна частина та агент, що відправляє дані [26].

Серверна частина EDR

Серверна частина EDR є центральним елементом, який керує всією системою. Вона може бути розгорнута як у хмарному середовищі, так і локально, в залежності від вимог підприємства. Вибір між варіантами розгортання може залежати від організації. Приклад: критична інфраструктура та державні

установи потребують локального розгортання для забезпечення конфіденційності своїх даних ніж будь-яка інша приватна організація. Вибір залежить від інфраструктури та роду діяльності компанії. Хмарне рішення зазвичай дешевше та легше масштабувати, але може мати ризики, пов'язані з передачею даних за межі підприємства.

Серверна частина забезпечує доступ до управління всіма агентами через вебконсоль, яка дозволяє командам кібербезпеки відстежувати стан кінцевих точок, керувати налаштуваннями політик безпеки та аналізувати події. Консоль дозволяє аналітикам переглядати інциденти, для оцінки рівня загроз та реагування на підозрілі дії. Сервер також може інтегруватися з іншими системами безпеки, такими як SIEM, що дозволяє об'єднати та аналізувати дані з різних джерел для більш ефективного реагування на інциденти.

Серверна частина відповідає за отримання телеметричних даних від агентів для їх подальшого аналізу та обробки, щоб оцінити стан кінцевого пристрою. Використовуючи алгоритми машинного навчання та аналізу поведінки, сервер може виявляти підозрілі патерни в даних, що дозволяє виявляти актуальні та нові загрози. При виявленні потенційних ризиків – аналітикам буде надано сповіщення для подальшої обробки можливого інциденту. Це дає змогу оперативно вживати заходи з реагування на інциденти безпеки та забезпечує можливість централізованого управління безпекою всієї інфраструктури.

Сучасні засоби кінцевих точок, де загальна обробка даних виконується серверною частино, можуть мати функії описані нижче:

1. Відображати графіки, що візуалізують хронологію та деталі інциденту, для перегляду та аналізу подій, що сталися;

2. Створювати детальні звіти, які будуть забезпечувати повний опис інциденту, виявлені загрози, взаємодії між компонентами системи та рекомендації для усунення проблеми.

3) отримати більше інформації за допомогою штучного помічника, який буде надавати рекомендацію в реальному часі та допомагати із вирішенням певного типу рутинних задач.

Агенти EDR

Агенти EDR є програмним забезпеченням, яке встановлюється на кінцеві точки. Вони відповідають за моніторинг активності на кожному пристрої та передачу даних про можливі загрози до серверної частини. Агенти працюють на рівні операційної системи, де вони контролюють різні аспекти роботи пристрою, включаючи процеси, файли, мережеві з'єднання та системні виклики. Це дозволяє їм виявляти підозрілу активність, яка може свідчити про спробу атаки або зараження шкідливим програмним забезпеченням. Інформацію, яку отримує агент називається *телеметрією*, яка надходить від *сенсорів*, які займаються стеженням за подіями в системі. Сенсори можуть бути вбудованими в ОС або розробленими спеціалістами, які створюю антивірусні рішення.

Основні функції агентів EDR включають:

1. Моніторинг процесів та поведінки системи: агенти можуть відстежувати створення нових процесів, зміни у файлах або з'єднання з зовнішніми мережами, що допомагає виявляти підозрілу активність;

2. Аналіз телеметрії: агенти можуть збирати дані та відправляти їх до серверної частини для отримання результатів подальших вказівок.

3. Ізоляція заражених пристроїв: у разі виявлення інциденту безпеки агенти можуть ізолювати кінцеву точку від мережі, щоб запобігти подальшому розповсюдженню загрози.

Існує три типи агентів: *базовий, проміжний та розширений*.

Базовий агент надає обмежений набір функцій для моніторингу активності, такий як статичний аналіз файлів і перехоплення API-викликів. Пояснення роботи компонентів на схемі (рисунок 1.1) описані нижче:

1. Static scanner (статичний сканер) – компонент, який виконує статичний аналіз файлів або довільні діапазони віртуальної пам’яті. Основа антивірусного сервісу;

2. Hook DLL (DLL-функція перехоплення) – відповідає за перехоплення викликів певних функцій API. Це допомагає опізнати нестандартну або потенційно шкідливу поведінку програм, яка може свідчити про наявність загрози, такої як троян, вірус або інше шкідливе програмне забезпечення.

3. Kernel-mode driver(драйвер ядра) – драйвер, який працює в ядрі та відповідає за впровадження перехоплюючої DLL у процеси певних програм для того, щоб збирати телеметрію.

4. Agent service (агент) – відповідає за збір телеметрії та передачу інформації до серверної частини. Деякі агенти мають властивість локально обробляти зібрані дані та генерувати сповіщення.

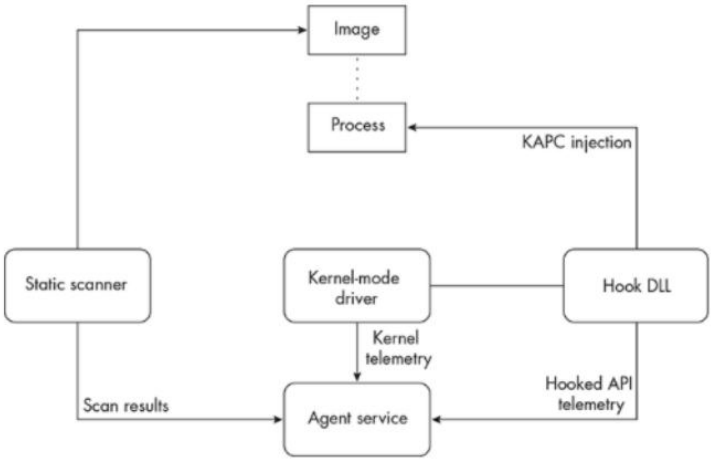


Рисунок 1.12. Базова архітектура агента [25]

Проміжний агент окрім функцій базового агента, має додаткові функції, включаючи мережевий аналіз трафіку та моніторинг файлових операцій. Він додає можливість моніторингу мережевого трафіку та роботу із файлами, що дозволяє краще виявляти зловмисну активність. Більшість агентів належать до середнього рівня складності. Ці агенти можуть впроваджувати не тільки свої сенсори, а й задіяти сенсори операційної системи для розширення можливості збору телеметрії.

Пояснення роботи компонентів на схемі (рисунок 1.2) описані нижче:

1. Network filter (драйвери мережевих фільтрів) – драйвери, які аналізують трафік для виявлення ознак зловмисної активності;

2. Filesystem minifilter (драйвери фільтрів файлової системи) – драйвери, що відстежують операції у файловій системі комп’ютера;

3. ETW (Event Tracing for Windows) – компонент, який слідкує за подіями,

які були створені операційною системою(в даному випадку це Windows) або сторонніми програмами;

4. ELAM service (компоненти раннього запуску антивірусного ПЗ) – компонент, що завантажується найпершим, ще до інших системних компонентів. Це дозволяє контролювати запуск інших програм або драйверів, щоб вчасно запобігти завантаженню шкідливого коду.

Описаний схема (рисунок 1.2) агент може не реалізовувати всі перелічені компоненти. Зазвичай може використовуватись драйвер ELAM, який розгортається разом з драйвером ядра.

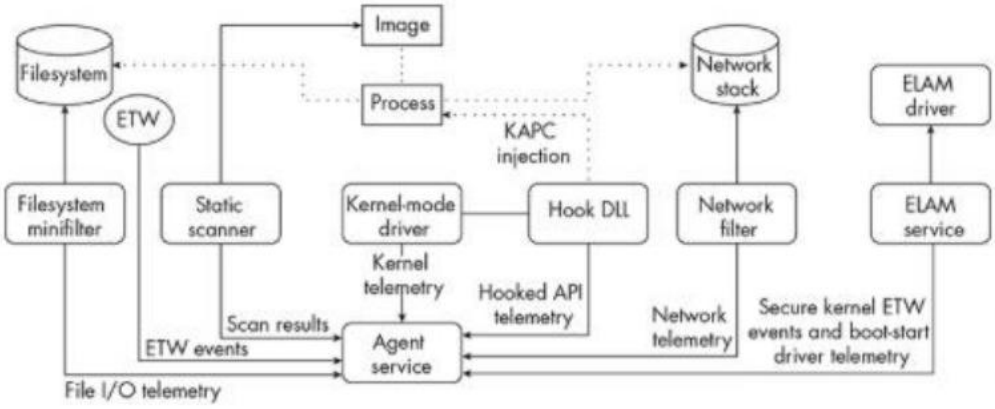


Рисунок 1.13. Архітектура проміжного агента [25]

Розширений агент має додаткові або специфічні функції, які залежать від постачальника продукту. Це може бути пісочниця, де будуть перевірятись файли на наявність шкідливого коду або підозрілої поведінки та deception-функція, що буде створювати пастки для зловмисника в системі та виявити його активність на ранніх етапах.

2. ОГЛЯД ТА ВИБІР СУЧАСНИХ ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ІЗ ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ДОСЛІДЖЕННЯ

2.1 Огляд сучасних систем захисту кінцевих точок із ШІ

Огляд сучасних систем буде проводить на основі висновків авторитетних видань, які проводять дослідження ефективності систем, а також визнання систем користувачами. Аналіз буде проводитись на основі 3 відомих аналітичних джерела, таких як: Gartner, Forrester та IDC та незалежних лабораторій по тестуванню продуктів, таких як: AV-COMPARATIVES та MITRE ATT&CK Evaluations.

Gartner - це провідна дослідницька компаній, яка спеціалізується на наданні стратегічних досліджень, консультацій і об'єктивних оглядів на основі глибокого аналізу ринку [27]. Одним із найвідоміших інструментів даної компанії є *Magic* Quadrant, який показує лідерів, новаторів та претендентів разом із нішевими гравцями на ринку технологій [28]. Він використовує чіткі критерії, щоб оцінити кожного вендора за такими параметрами, як повнота бачення та здатність до реалізації.

Для вендорів, які створюють системи захисту, важливо бути представленими в Magic Quadrant, адже це не тільки підтверджує їхнє лідерство або інноваційний підхід, а й підвищує довіру серед клієнтів. Діаграма Magic Quadrant for Endpoint Protection Platforms (рисунок 2.1) показав рейтинг виробників, які мають найкращі рішення в категорії Enpoint Protection Platform в 2024 році.

Рисунок 2.1. Magic Quadrant for Endpoint Protection Platforms July 2024 [29]

Forrester - є однією з провідних дослідницьких фірм, яка зосереджена на наданні стратегічних рекомендацій для бізнесів у галузі цифрових технологій [30]. Один з найвідоміших продуктів Forrester - *Forrester Wave*. Даний інструмент допомагає покупцям ознайомитись із аналізом компанії стосовно обраного типу продукту та зробити свій вибір [31].

Цей звіт деталізує функціональні можливості, інтеграції, а також стратегії розвитку продуктів різних вендорів, показуючи їхню здатність відповідати поточним і майбутнім потребам ринку. Участь вендорів у Forrester Wave може підвищити репутацію на ринку, оскільки звіт зосереджений на деталях, що показують глибину функціональності продуктів і інновацій. Діаграма Forrester Wave for Extended Detection and Response Platforms (рисунок 2.2) показує рейтинг найкращих постачальників розширених систем захисту в 2024 році.

Рисунок 2.2. Forrester Wave for Extended Detection and Response Platforms Q2 2024 [32]

IDC одна з провідних світових компаній, що спеціалізується на проведенні досліджень, аналізі ринків та наданні консультацій у сфері інформаційних технологій [33]. Аналітичний інструмент компанії, такий як *IDC MarketScape* надає якісну оцінку постачальника продуктів. Використовує збалансований підхід, щоб проаналізувати стратегію та можливості постачальника, а в подальшому надати свою думку, яка допоможе при виборі [34]. Участь у IDC MarketScape допомагає вендорам збудувати репутацію на ринку та продемонструвати, як їхні продукти відповідають очікуванням у сфері інновацій і технологічної ефективності. Діаграма IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2024 (рисунок 2.3) показує рейтинг найкращих постачальників сучасних засобів кінцевих точок в 2024 році.

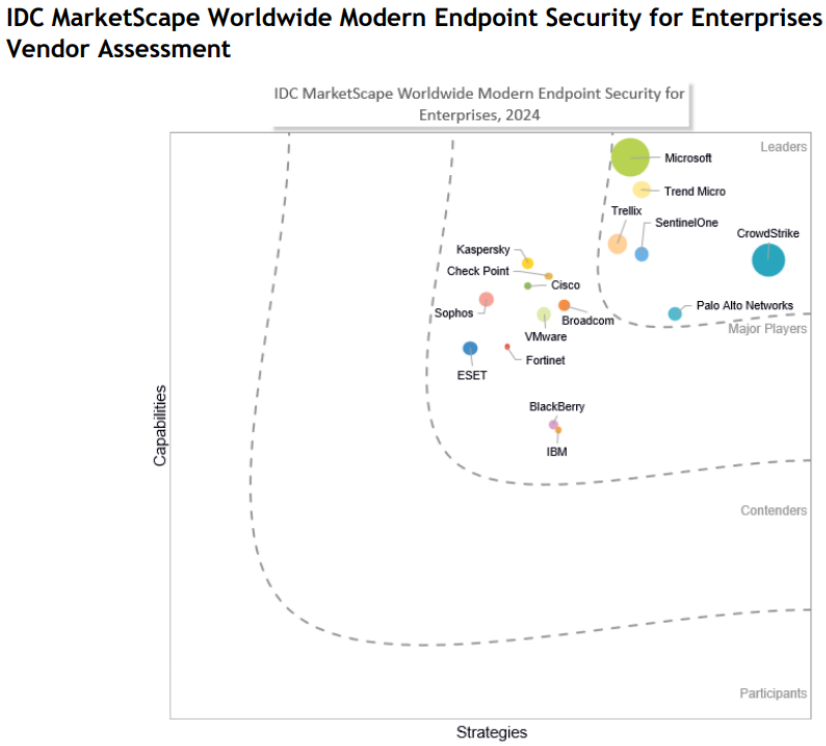


Рисунок 2.3. IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2024 [35]

AV-Comparatives - це незалежна організація, яка спеціалізується на тестуванні рішень для кібербезпеки, зокрема антивірусних продуктів. Компанія створює середовище для тестування, де продукти проходять перевірку. Успішне завершення тестування надасть компанії сертифікацію, яка визнана у всьому світі [36]. Одним із інструментів для аналізу є *CyberRisk Quadrant*. Ключовими параметрами є: здатність запобігати та реагувати на загрози та загальна вартість володіння продуктом вендора за 5 років. Діграма також має поділку на 4 категорії: стратегічних лідерів, візіонерів кібербезпеки, сильних претендетів та тих, хто не був сертифікований [37].

Отримання сертифікації в Enterprise EPR CyberRisk Quadrant (рисунок 2.4) показує, які вендори є лідерами, з точки зору ефективності та продуктивності.

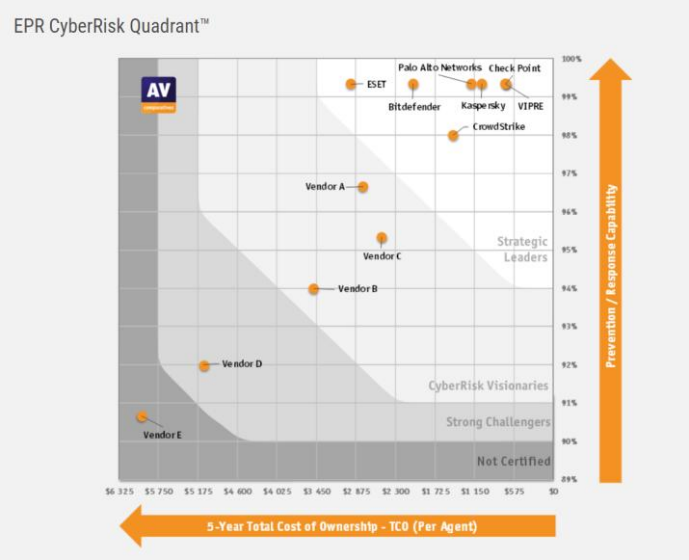


Рисунок 2.4. Enterprise EPR 2024 CyberRisk Quadrant [37]

MITRE ATT&CK Evaluations - це тестування кібербезпекових продуктів на основі фреймворку *MITRE ATT&CK*, який моделює методи, що використовують хакери на різних етапах атаки. Під час тестів оцінюється здатність продуктів виявляти, блокувати та реагувати на реалістичні загрози [38].

Вендорам важливо представити свої продукти в MITRE ATT&CK Evaluations, як і в Enterprise так і в MDR рішеннях, оскільки це підвищує довіру до їхніх рішень. Результати демонструють реальну ефективність продуктів у відтворених сценаріях, що підсилює репутацію вендорів і допомагає користувачам вибирати оптимальні рішення для захисту. В даному випадку MITRE ENGENUITY ATT&CK® Evaluations Managed Services 2024, являється найкращим показником, для наглядного показу ефективності взаємодії людини(спеціалістів із інформаційної безпеки) та комплексної системи захисту кінцевих точок.

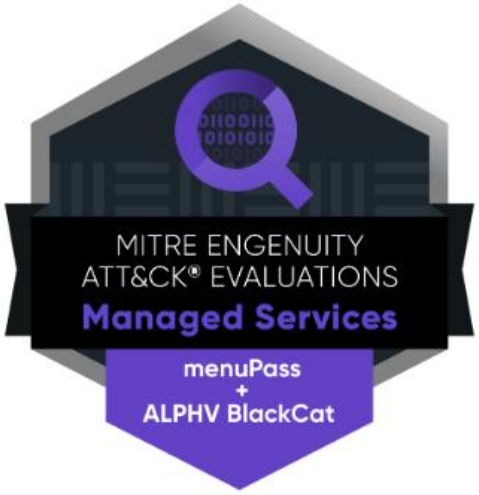


Рисунок 2.5. MITRE ENGENUITY ATT&CK® Evaluations Managed Services 2024 [38]

Згідно з аналізом авторитетних інформаційних джерел, описаних вище, було визначено трьох ключових вендорів, продукти яких потребують детального дослідженн. Microsoft, Palo Alto Networks та CrowdStrike є провідними компаніями в області захисту кінцевих точок завдяки своїм технологіям штучного інтелекту, здатності адаптуватися до сучасних загроз та сильній присутності на ринку кібербезпеки.

Номінації та оцінки Microsoft

1. Gartner

Згідно Gartner Magic Quadrant for EPP 2024 компанія Microsoft отримала статус Leader, що є найвищою відзнакою для компанії. Microsoft об’єднала Defender XDR із Microsoft Sentinel, створивши єдине середовище для управління безпекою, покращило агенти для Linux та працює над уніфікацією агентів для кінцевих точок для спрощення розгортання та експлуатації. Аналітичне джерело Gartner, відмітило [39], що сильні сторони компанії, куди входять: швидка реакції на потреби ринку та досвід роботи, продуктова стратегія та дорожня карта безпеки Microsoft узгоджуються з новими вимогами клієнтів щодо консолідації операцій з безпеки та ефективну стратегію продажів та велику, усталену клієнтську базу. Але в той час були і застереження у вигляді: змінного

досвіду клієнтів із технічною підтримкою та підтримкою облікових записів, яку вони отримували від Microsoft; складної та важкої для розуміння моделі ліцензування, про що також повідомляли користувачі; та обмеженої кількості галузевих продуктів, варіантів ціноутворення і відсутності підтримки для локального розгортання EPP.

2. Forrester

За оцінкою Forrester [40] за 2 квартал 2024 року, Microsoft була визнана лідером у сфері платформ розширеного виявлення та реагування (XDR). Microsoft Defender XDR отримав найвищі бали в трьох основних категоріях: «стратегія», «поточна пропозиція» та «присутність на ринку». Компанія досягла найвищих результатів у 15 із 22 критеріїв, включаючи такі показники, як «Виявлення на рівні кінцевих точок», «Поверхневе дослідження», «Полювання на загрози», «Досвід аналітиків», «Бачення» та «Інновації». Ця висока оцінка підкреслює сильну позицію Microsoft у розробці ефективних інноваційних рішень для забезпечення кібербезпеки.

3. IDC

Microsoft була визнана лідером у трьох сегментах IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2024 для сучасної безпеки кінцевих точок завдяки своєму продукту Defender for Endpoint [41]. Аналітичний центр визнає у продуктів компанії високий рівень автоматизації загроз, впровадження генеративного ШІ для прискорення аналізу інцидентів і забезпечення комплексного захисту для Windows, Linux, macOS, iOS, Android і IoT. Ці досягнення роблять Microsoft популярним вибором для організацій різного масштабу, які прагнуть до гнучких і масштабованих рішень кібербезпеки.

4. MITRE ENGENUITY ATT&CK® Evaluations Managed Services 2024

Згідно звіту «MITRE ENGENUITY ATT&CK® Evaluations Managed Services 2024 for Microsoft» [42] система продемонструвала високий рівень ефективності. Microsoft Defender продемонструвала високу ефективність у тестуванні на основі сценаріїв атак menuPass та ALPHV (BlackCat) в оцінюванні MITRE Engenuity ATT&CK®. Вона успішно виявила широкий спектр атак, який

охоплював 43 техніки, і забезпечила своєчасне реагування, зокрема з середнім часом до виявлення (MTTD) у 24 хвилини. З 37 детекцій 27 були визначені як такі, що потребують дій, підкреслюючи високу операційну готовність до нейтралізації загроз.

Номінації та оцінки CrowdStrike

1. Gartner

Згідно Gartner Magic Quadrant for EPP 2024 [39] компанія CrowdStrike отримала статус Leader, що є найвищою відзнакою для компанії. Вона є лідером у своєму секторі, пропонуючи широкий набір продуктів безпеки, включаючи CrowdStrike Falcon - флагманський продукт EPP. CrowdStrike представила захист даних кінцевих точок, а також рішення Falcon for IT для управління кінцевими точками та виконанням нормативних вимог. Аналіз авторитетних видань демонструє результати, в яких можна відмітити:

CrowdStrike вирізняється швидкою реакцією на ринкові потреби, високою часткою на ринку EPP і надійними послугами для клієнтів, а її стратегія узгоджується з новими вимогами ринку, які постають перед компанією. Водночас компанія стикається з викликами такими як інцидент Channel File 291, що показав недоліки в контролі якості. Варто відмітити, що ціни продуктів є вищими за середні. Крім того, обмежена географічна присутність і мовна підтримка CrowdStrike можуть обмежувати її доступність у різних регіонах.

2. Forrester

Зі інформацією Forrester Wave for Extended Detection and Response Platforms Q2 2024 [43], CrowdStrike була визнана єдиним постачальником у звіті Forrester Wave 2024, який отримав найвищі оцінки за бачення, інновації та дорожню карту. Її платформа XDR встановлює нові стандарти, забезпечуючи комплексний підхід до кібербезпеки. CrowdStrike пропонує XDR-функції безкоштовно для клієнтів EDR, що підвищує швидкість розслідувань та надає розширену видимість і виявлення загроз у реальному часі. Самец ця стратегія дозволяє клієнтам ефективно захищати критичні активи від сучасних загроз.

3. IDC

CrowdStrike була визнана одним із лідерів, у звіті IDC MarketScape:

Worldwide Modern Endpoint Security for Enterprises 2024 [44], очоливши ринок сучасної безпеки кінцевих точок третій рік поспіль. Аналітична компанія високо оцінила зростання частки ринку CrowdStrike та її прибутки, завдяки платформі Falcon, що об'єднує безпеку кінцевих точок, хмари та ідентифікацію загроз. Має інструменти на базі штучного інтелекту та використовує машинне навчання. Falcon вирізняється швидким впровадженням, інтегрованою загрозою аналітикою та легким агентом для зниження складності управління.

4. AC-COMPARETIVES

CrowdStrike отримала високу оцінку від AV-Comparatives у тесті Endpoint Prevention and Response (EPR) 2024 завдяки 100% показникам активного й пасивного реагування на загрози у всіх фазах атак [45]. Falcon Elite один із основних компонентів якого, EDR виділяється потужним поєднанням автоматизованого запобігання загрозам, гнучким для налаштування та інтегрованого інструментарію для розслідувань. Платформа забезпечує детальне відображення атак та мінімізує кількість хибних спрацьовувань, що робить систему ефективним рішенням для захисту корпоративних середовищ.

5. MITRE ENGENUITY ATT&CK® Evaluations Managed Services 2024

CrowdStrike продемонстрував вражаючу ефективність у тестуванні з імітацією атак menuPass і ALPHV (BlackCat), успішно виявивши 43 техніки і змогла забезпечити 40 із 42 можливих детекцій, які потребували дій. Час до виявлення становив усього 4 хвилини, що свідчить про швидку реакцію. Високий рівень критичних та важливих сповіщень підтверджує здатність CrowdStrike забезпечувати пріоритетний моніторинг і оперативне реагування на серйозні загрози [46].

Номінації та оцінки Palo Alto Network

1. Gartner

Згідно Gartner Magic Quadrant for EPP 2024 компанія Palo Alto Networks отримала статус Leader, що є найвищою відзнакою для компанії. Palo Alto Networks, як лідер у Magic Quadrant, пропонує флагманський продукт для захисту кінцевих точок (EPP), а також широкий асортимент інтегрованих рішень для забезпечення мережевої, хмарної безпеки та операцій безпеки. Останні

оновлення включають уніфікований агент, який об'єднує можливості захисту хмарних робочих навантажень і EDR, а також покращені функції XDR для криміналістики та захисту систем. Компанія вдосконалила модулі безпеки та додала їх для розширення можливості безпеки для захисту UEFI та додала захист для Windows від загроз при записі [39].

2. Forrester

Palo Alto Networks визнана одним із лідерів у звіті Forrester Wave 2024 для платформ XDR за свою платформу Cortex XDR. Висока оцінка була здобута компанією за інновації, стратегію продукту, зокрема за використання AI та машинного навчання для поглибленого аналізу загроз, інтеграцію телеметрії з різних джерел і підтримку централізованого управління кібербезпекою. Платформа дозволяє операційним центрам безпеки ефективно виявляти та реагувати на загрози в реальному часі [48].

3. IDC

Аналіз IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2024, показанав що вендор знаходиться в категорії лідери [35]. Із цього можна зробити висновок, що компанія має добре розвинену стратегію та конкурентну позицію на ринку із іншими лідерами сфери.

4. AC-COMPARETIVES

Palo Alto Networks у 2024 році отримала сертифікацію «Strategic Leader» за результатами тестування категорії Endpoint Prevention and Response (EPR) від AV-Comparatives для продукту Cortex XDR Pro [48]. Платформа змогла продемонструвати 100%-ий показник як активного (запобігання), так і пасивного (виявлення) реагування на всі тести, що були надані незалежним аналітиком. Ці тести охоплювали фази компрометації, внутрішнього розповсюдження та порушення активів.

5. MITRE ENGENUITY ATT&CK® Evaluations Managed Services 2024 У 2024 році платформа Palo Alto Networks Cortex XDR показала одні із найкращих результатів в оцінюванні MITRE ENGENUITY ATT&CK® Evaluations Managed Services 2024. Palo Alto Networks продемонструвала високу ефективність у тестуванні menuPass та ALPHV (BlackCat), успішно змогла виявити 43 техніки

та забезпечивши 34 з 38 можливих детекцій, які потребували дій. Середній час до виявлення становив 24 хвилини, що свідчить про здатність системи швидко реагувати на загрози. Згідно графіку акцент на високих і низьких сповіщеннях, що вказує на належний моніторинг загроз та пріоритизацію безпеки. Загалом, рішення Palo Alto Networks забезпечує сильний рівень захисту з помірною оперативністю в реагуванні на кіберзагрози [49].

2.2 Ознайомлення з функціональними можливостями систем захисту кінцевих точок із застосуванням технологій штучного інтелекту

Microsoft

Microsoft має XDR систему, яка може об'єднувати дані про загрози з різних джерел для виявлення загроз із різних джерел та реагування на атаки. До розширеного захисту також входить Microsoft Defender для кінцевих точок, який в свою чергу, виконує функцію управління та моніторингу кінцевих точок, забезпечуючи їхню безпеку та відповідність політикам компанії. Поєднуючи ці рішення, вони створюють комплексне рішення для захисту інфраструктури, дозволяючи запобігати загрозам, швидко реагувати на інциденти та зберігати контроль над усіма кінцевими точками в організації.

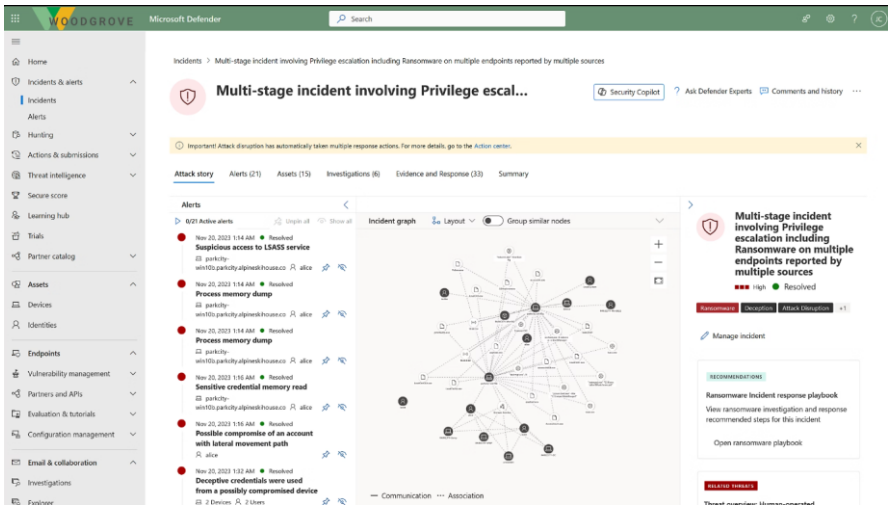


Рисунок 2.6. Інтерфейс Microsoft Defender для кінцевих точок[50]

Microsoft Defender для кінцевих точок

В якості систем захисту вендора Microsoft, можна виділити: Microsoft Defender для захисту кінцевої точки та Microsoft XDR із додатковими рішеннями для розширеного захисту.

Microsoft Defender для кінцевих точок має набір функцій (рисунок 2.7), які забезпечують повноцінний захист кінцевих пристроїв.

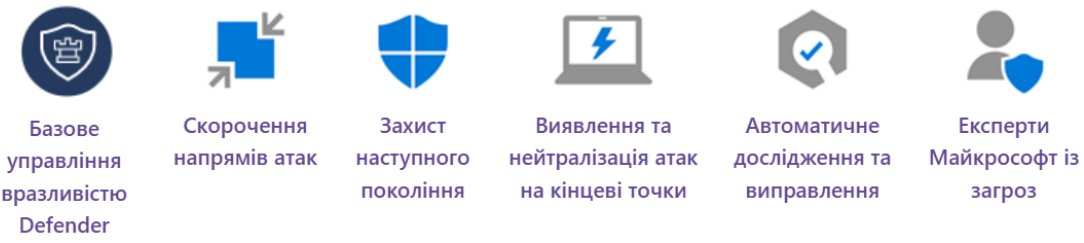


Рисунок 2.7. Набір захисних функцій Microsoft Defender для кінцевих точок [51]

Кожне із цих напрямів захисту має в своєму арсеналі технології, які працюють завдяки комп'ютерному інтелекту.

1. «*Базове управління вразливістю Defender*»

Функція відповідає за постійний моніторинг активів, оцінку ризиків та пріоритизацію критичних вразливостей [52]. Вона автоматично генерує рекомендації для їх усунення, враховуючи контекстні фактори та потенційний вплив на систему, із цього можна зробити висновок про використання штучного інтелекту в даній функції.

2. «*Скорочення напрямів атак*»

Забезпечує зменшення площі атаки через захист від експлойтів, мережевий і веб-контроль, управління доступом до даних та пристроїв [53]. Використовуючи штучний інтелект для аналізу поведінкових сигналів, щоб надати рекомендації по зниженню ризиків.

3. «*Захист наступного покоління*»

Забезпечує захист нового покоління, використовуючи машинне навчання та штучний інтелект для аналізу поведінкових сигналів і блокування сучасних загроз [54].

4. «*Виявлення та нейтралізація атак на кінцеві точки*»

Використовується для виявлення, дослідження та реагування на складні загрози у режимі близькому до реального часу, з можливістю вжити відповідні заходи для знешкодження загрози [55]. Генерація сповіщень для аналітиків про виявлення загрози, а також рекомендації по знешкодженню загрози може бути обумовлена використанням систем штучного інтелекту.

5. «*Автоматичне дослідження та виправлення*»

Автоматичне розслідування в Microsoft Defender for Endpoint дозволяє системі виконувати аналіз інцидентів без прямого втручання аналітика. Це забезпечує швидке виявлення та реагування на потенційні загрози. Ця функція автоматично ідентифікує підозрілу активність, збирає пов’язану інформацію про подію, проводить аналіз і, за необхідності, ініціює заходи для нейтралізації загрози [56]. Автоматизація аналізу потенційних загроз та автоматична ініціація заходів по знешкодженню загрози, може бути пов’язана із алгоритмами машинного навчання, які були навчені реагувати на події.

6. «*Експерти* «*Майкрософт*» *із загроз*»

Функція відповідає за проактивне полювання, моніторинг та аналіз загроз, що скорочує час очікування реакції на подію. Механізм штучного інтелекту відповідає за виявлення та пріоритетність відомих та невідомих атак [57].

Microsoft Defender для кінцевих точок включає ряд новітніх функцій, які підсилюють загальний захист та управління безпекою в організації. *Захисний комплекс Copilot* допомагає командам безпеки швидше приймати рішення, надаючи рекомендації на основі штучного інтелекту, *технологія омани* створює пастки для зловмисників, запобігаючи доступу до реальних ресурсів. Це можуть бути нереальні аккаунти або пристрої для дослідження подальших дій зловмисника, а *глобальний аналіз кіберзагроз* забезпечує актуальну інформацію про загрози у світі, що допомагає оперативно реагувати на нові типи атак збираючи сигнали із безлічі джерел та оброблюючи спеціалістами [58].

Microsoft XDR

Комплексне рішення для виявлення, аналізу та реагування на загрози, таке як Microsoft XDR (рисунок 2.8), яке об'єднує сигнали з різних джерел безпеки, таких як: кінцеві точки, пошта, ідентифікації, хмара, для забезпечення повного огляду та автоматизованого реагування на атаки.

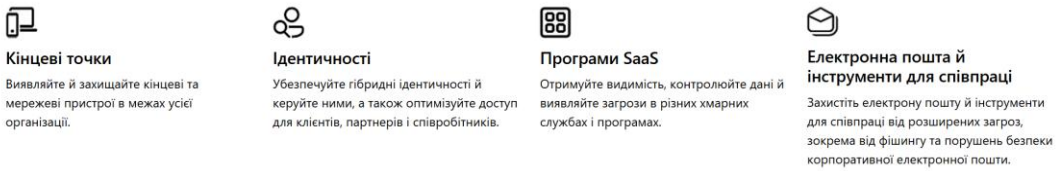


Рисунок 2.8 – Набір захисних функцій Microsoft XDR [59]

Microsoft Defender для захисту кінцевих точок – рішення Microsoft Defender for Endpoint, яке захищає пристрої користувачів від кіберзагроз. Більш детальна інформація про можливості системи, була описана вище;

Microsoft Defender для захисту ідентичності - це хмарне рішення Microsoft Defender for Identity, яке захищає гібридні середовища, виявляючи підозрілу активність користувачів та аномалії [60]. Можна зробити висновок, що ШІ використовується для аналізу поведінкових патернів, виявлення аномалій і загроз у реальному часі.

Microsoft Defender для хмари - це платформа захисту хмарних додатків Microsoft Defender for Cloud Apps, забезпечує всебічний захист SaaS-додатків, контролюючи їх використання, виявляючи потенційно небезпечні дії та захищаючи критичні дані. Система об’єднує функції безпеки CASB для виявлення тіньових IT-ресурсів і видимості додатків, а також SSPM для покращення стану безпеки та адаптації до нових загроз [61].

Microsoft Defender для захисту пошти – це рішення Microsoft Defender for Office 365, яке захищає організації від загроз, забезпечуючи захист електронної пошти та інших сервісів Microsoft 365 від складних загроз, таких як фішинг, шкідливі вкладення та посилання. Сервіс може аналізувати вміст у реальному часі, виявляти та блокувати потенційно небезпечні файли й URL-адреси, а також

забезпечує розширене відстеження загроз [62]. Штучний інтелект може використовуватись для аналізу поведінкових патернів, прогнозування нових загроз і автоматизованого реагування на інциденти, що значно підвищує швидкість і точність захисту.

CrowdStrike

CrowdStrike Falcon Insight EDR та XDR – є сучасними рішеннями захисту кінцевих точоко від CrowdStrike.

Falcon EDR - це сучасне рішення, розроблене CrowdStrike для виявлення, дослідження і реагування на загрози безпеки кінцевих точок. Він входить до складу комплексного захисту CrowdStrike Platform (рисунок 2.9). Основні можливості платформи можна описати так:

1. *Автоматизоване виявлення загроз***:** Система використовує можливості штучного інтелекту для того, щоб автоматично виявляти аномальну активність на кінцевих точках [63].

2. *Повноцінне дослідження інцидентів***:** Платформа робить глубокий аналіз кожного інциденту, який трапився, щоб спеціалісти мали змогу переглядати контекст атак та отримувати детальну інформацію про всі етапи загрози [63]. Штучний інтелект може використовуватись для автоматичного аналізу інцидентів, кореляції подій, побудови причинно-наслідкових зв'язків.

3. *Реагування в режимі реального часу***:** Falcon EDR має змогу негайного реагування на загрози, використовуючи інтегровані компоненти управління кінцевими точками [63].

4. *Хмарна платформа***:** Дана платформа працює на основі хмарної архітектури, щоб забезпечувати високу масштабованість і можливість обробки великого обсягу даних у режимі реального часу [63].

5. *Аналіз поведінки користувачів***:** Використовуючи штучний інтелект, система захисту має змогу постійно моніторити поведінку користувачів і процесів, що допомагає виявляти навіть ті загрози, які не можна ідентифікувати за допомогою традиційних сигнатурних методів [63].

6. *Інтеграція з Falcon Platform***:** Система інтегрується з іншими продуктами, що забезпечує комплексний підхід до кібербезпеки [63].

Рисунок 2.9. Інтерфейсне вікно CrowdStrike Falcon [64]

CrowdStrike Falcon Platform поєднує в собі компоненти для захисту системи на різних рівнях. Він має в своєму складі: Endpoint Security & XDR, Cloud Security, Threat Intelligence, Identity Protection, Security & IT Ops, Observability. Endpoint Security & XDR має в собі систему Falcon XDR, яка дозволяє використовувати інформацію з кількох джерел для кращої координації та розуміння атак, а також їх нейтралізації. Завдяки інтеграції з іншими модулями платформи, цей підхід допомагає швидше реагувати на інциденти та мінімізувати потенційні наслідки атак [65].

Опис основних компонентів Endpoint Security & XDR [65]:

1. *Falcon Prevent* - антивірус нового покоління, захищає від всіх типів зловмисного ПЗ, від звичайних програм до складних атак. Має швидке розгортання та миттєвий захист кінцевих точок [65].

Завдяки штучному інтелекту, агент може зупиняти загрози в оффлайн режимі, використовуючи такі методи як: аналітика загроз, поведінковий аналіз та усунення експлойтів [66].

2. *Falcon Insight XDR* – це розширене рішення для виявлення та реагування на загрози, яке може об’єднувати телеметрію з різних джерел, включаючи

кінцеві точки, ідентифікацію, хмарні робочі навантаження та аналіз загроз, для аналізу даних із різних джерел і покращення ефективності безпеки [67].

3. *Falcon Device Control* – безпечне використання USB-пристроїв за рахунок повної видимості та детального контролю над їх використанням. Надає спеціалістам повну інформацію про файли, які були записані на носій інформації.

Завдяки технології машинного навчання, може ідентифікувати понад 40 мов програмування, що запобігає несанкціонованому витоку вихідного коду [68].

4. *Falcon Firewall Management* - дозволяє централізовано керувати налаштуваннями міжмережевих екранів на кінцевих точках, забезпечуючи посилений контроль трафіку та відповідність політикам безпеки [65].

Опис всіх інших компонентів, які можуть бути інтегровані із Falcon XDR, для покращення захисту кінцевих точок [66]:

Cloud Security забезпечує захист хмарних ресурсів. Має модулі, такі як Falcon Horizon, які забезпечують захист активів у хмарі та відповідність вимогам безпеки.

Threat Intelligence модулі надають інформацію про актуальні загрози та допомагають прогнозувати потенційні атаки, забезпечуючи проактивний захист.

Identity Protection рішення дозволяють захищати облікові записи та ідентифікаційні дані користувачів, запобігаючи компрометації та використанню скомпрометованих облікових записів.

Модулі для *Security* **&** *IT Ops*, такі як Falcon Discover, забезпечують управління активами та автоматизацію операцій безпеки, допомагаючи ідентифікувати вразливості та покращувати загальну видимість.

Компоненти *Observability* забезпечують моніторинг інфраструктури та допомагають краще розуміти активність мережі й кінцевих точок, що сприяє швидшому виявленню аномалій та загроз.

Palo Alto Network

Cortex XDR - це сучасна платформа для розширеного виявлення та реагування на загрози (Extended Detection and Response, XDR), яка інтегрує дані з різних джерел для забезпечення захисту системи, з метою попередження атак та мінімізації збитків.

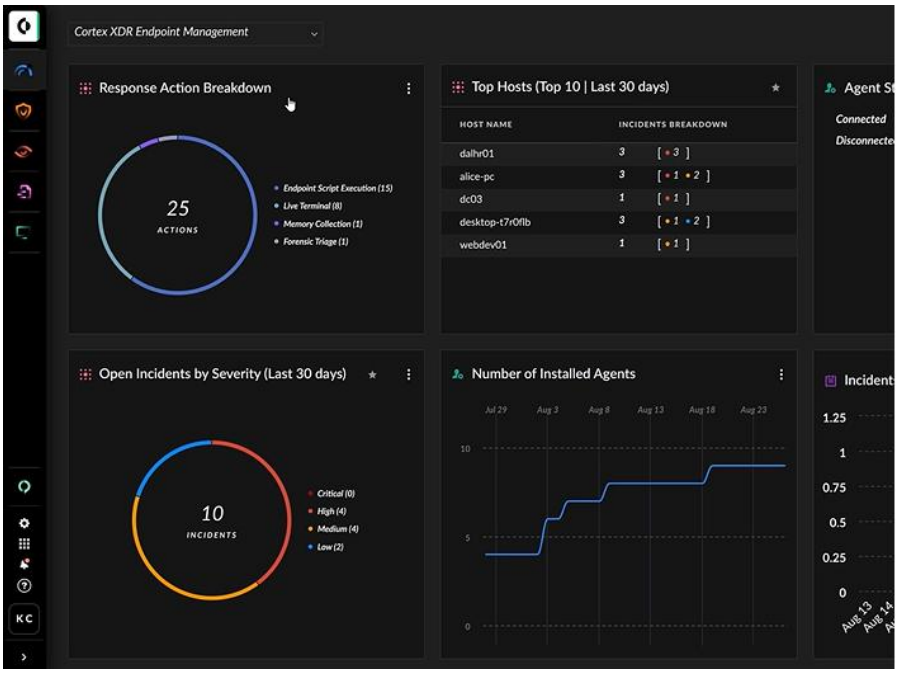


Рисунок 2.10. Інтерфейсне вікно Palo Alto Cotrex XDR [73]

Cortex XDR поєднує сучасні можливості захисту кінцевих точок, моніторинг облікових записів і активний пошук загроз. Використовуючи штучний інтелект і машинне навчання, система автоматично виявляє, ізолює та усуває загрози, аналізуючи поведінку для визначення аномалій, що можуть свідчити про небезпеку. Для запобігання, виявлення та реагування система має такі можливості [69, 70]:

1. *Повна видимість середовища*: Cortex XDR інтегрує дані з кінцевих точок, мереж і хмар для швидкого виявлення загроз.

2. *Виявлення загроз за допомогою машинного навчання*: Використовує поведінковий аналіз для виявлення аномальної активності, забезпечуючи оцінку ризиків для користувачів, а модель машинного навчання, яке орієнтована на

виявлення загроз, використовує алгоритми для виявлення складних та нових типів атак, які не можуть бути помічені традиційними методами, що дозволяє захистити систему на проактивному рівні.

3. *Глобальна аналітика*: Використовує дані про клієнтів для виявлення загроз, яка може бути інтегрована з Threat Intelligence, щоб протидіяти новим та сучасним загрозам, включаючи атаки «нульового дня», що дозволяє аналітикам краще розуміти природу атаки, швидше приймати рішення та вчасно реагувати на нові загрози [69, 70].

На основі отриманих даних, проходить навчання алгоритмів, щоб виявити нові патерни атак. Це допомагає покращати ефективність пошуку нових загроз.

4. *Швидке дослідження*: Надає повну картинку інциденту роблячи детальну розвідку загрози. Функція SmartScore XDR використовує алгоритми машинного навчання для пріоритезації ризиків, що дозволяє команді швидко оцінити ризики атаки. Фукнція централізованого керування інцидентами допомагає швидко та ефективно реагувати спеціалістам кібербезпеки.

5. *Автоматизація через Cortex XSOAR*: Автоматизація допомагає проводити процес розслідування та реагування, інтегруючись з іншими продуктами, що дозволяє покращити реагування на інциденти.

Окремо можна виділити можливості агента Cortex XDR, який пропонує новий рівень захисту від шкідливого програмного забезпечення різної складності на кінцевому пристрої. Система штучного інтелекту допомагає точно виявляти загрози на основі аналітики та швидко виправляти ситуацію.

Основні можливості агента, які можна відмітити [69, 70]:

1. *Блокування атак на кінцевих точках*: Cortex XDR забезпечує надійний захист від зловмисного ПЗ. Локально перевіряє кожен файл використовуючи штучний інтелект, який постійно вдосконалюється для протидії новим методам атак. Вивчає поведінку декількох процесів для виявлення атаки. Інтеграція із Palo Alto Networks WildFire може підвищити точність аналізу шкідливого ПЗ.

2. *Керування USB та Bluetooth-пристроями*: Проводить моніторинг та керування доступом до USB-пристроїв використовуючи політики контролю доступу. Bluetooth Device Control допомагає контролювати Bluetooth-пристрої, а

саме отримати інформацію про підключення пристроїв до кінцевих точок та налаштовувати політики доступу різних Bluetooth-пристроїв до кінцевих точок.

3. *Брандмауер хоста та шифрування дисків***:** Система включає засоби для контролю трафіку на хостах і можливість шифрування дисків, що допомагає знизити ризики компрометації системи. Брандмауер забезпечує захист для різних операційних систем, як для Windows, так і для macOS, а функція шифрування дозволяє створювати політики для підвищення безпеки даних.

4. *Гнучкі варіанти реагування***:** Платформа надає засоби для швидкого реагування, такі як ізоляція кінцевих точок та обмеження мережевої активності. Автоматичний аналіз основних причин допомагає автоматично знаходити причини інцидентів та створювати рекомендації для їх усунення, що підвищує ефективність роботи аналітиків. Функція Live Teminal дозволяє використовувати системні команди або скрипти на кінцевих пристроях не порушуючи їх роботу [69, 70].

В даному випадку штучний інтелект може надавати рекомендації для ізоляції точки, щоб уникнути подальшого розповсюдження атаки. Playbooks можуть використовуватись для автоматичного знешкодження загрози. В якості додаткових функцій, можна виділити *глибоку форензику*, яка дозволяє проводити детальні розслідування інцидентів, навіть коли пристрій не підключений до мережі. Це надає можливість відстежувати весь ланцюг атаки та збирати докази для глибокого аналізу [69, 70]. Штучний інтелект оброблює інформацію, яка потрапила до системи, щоб на її основі зробити ланцюг подій та детальну інформацію про кожний етап.

Розширений пошук загроз, який проводить більш детальний та розширений пошук загроз, а також надає можливість активного дослідження середовища для виявлення прихованих загроз за допомогою спеціалізованих інструментів та аналітичних методів. Проводить більш детальний та розширений пошук загроз [69, 70].

Charlotte AI спеціалізований генеративний AI-асистент від CrowdStrike. Він дозволяє користувачам задавати питання природною мовою та отримувати швидкі, точні й дієві відповіді, спрощуючи робочі процеси.

2.3 Практичне дослідження функціональних можливостей систем захисту кінцевих точок із застосуванням технологій штучного інтелекту

Microsoft

Тест Microsoft Defender Experts for XDR був проведений для оцінки здатності системи виявляти, запобігати та реагувати на складні кіберзагрози, використовуючи модель MITRE ATT&CK. Згідно звіту [71] цей тест дозволив відтворити весь цикл кіберзагрози, починаючи від початкового доступу й до розгортання шкідливого програмного забезпечення. Тестування було проведене з 12 по 16 лютого 2024 року в середовищі MITRE Engenuity, де атакуючий актор, Purple Typhoon (також відомий як POTASSIUM/APT10/MenuPass), виконував цільові атаки, а захисники вживали відповідних заходів для їх стримування. Аналіз включає опис дій обох сторін, з використанням тактик і технік, які відображені в MITRE ATT&CK.

MITRE ATT&CK є відкритою моделлю, яка описує тактики, техніки і процедури (TTP), які використовують атакуючі під час компрометації мережі. Ця модель використовується для тестування захисту організацій, визначення найбільш вразливих етапів атаки та оцінки ефективності відповідних засобів захисту. Microsoft Defender for XDR, система розширеного виявлення і відповіді, використовує потужні інструменти для аналітики, телеметрії та автоматизованого розслідування інцидентів для запобігання багаторівневим атакам.

У цьому звіті детально розглядається весь цикл атак, включаючи техніки, якими користувалось угрупування від початкового доступу, виконання шкідливих програм, латеральний рух, ексфільтрацію даних і розгортання шифрувальника, а також дії захисників для стримування загрози.

Етапи атаки

Етап 1. Початковий доступ та встановлення бекдору

Дата атаки: 12 лютого 2024 року.

Тактики атакуючих: На першому етапі атакуючі використовували легітимні канали віддаленого доступу для проникнення в середовище жертви.

Використовувався RDP для входу на систему GABUMON з акаунту DIGIRUNAWAY\KIZUMI з джерела IP-адреси 116.83.1.29. Атака була ретельно спланована з використанням компрометованих облікових даних. Після входу атакуючий використовував утиліту certutil.exe для завантаження шкідливих файлів, які потім були інтегровані до легітимного процесу Notepad++. Це було зроблено з використанням техніки DLL Search Order Hijacking, коли версія DLL-файлу із шкідливим кодом була розміщена у каталозі, який система перевіряє першим. Таким чином, Quasar RAT (удосконалена версія RAT, відома як віддалене адміністрування шкідливого ПЗ) була завантажена і запущена, що дало атакуючому змогу керувати системою дистанційно.

Додатково, зловмисник активував кейлогер, який виявив облікові дані адміністратора домену - DIGIRUNAWAY\KIZUMI.DA, що дало змогу отримати вищий рівень доступу.

Техніки, що використовувались:

1. Initial Access (T1078.002): Зловмисник використав валідні облікові дані для RDP доступу до системи GABUMON через користувача DIGIRUNAWAY\KIZUMI використовуючи IP 116.83.1.29.

2. Execution (T1059.003, T1218, T1574.001): Використання cmd.exe, certutil.exe та DLL Search Order Hijacking також згадується у звіті. Зловмисник використовував ці інструменти для завантаження й виконання зловмисних файлів на GABUMON і PARROTMON.

3. Credential Access (T1056.001): Встановлення кейлогера підтверджується для крадіжки облікових даних користувача DIGIRUNAWAY\KIZUMI.DA.

4. Command and Control (T1071.001): Використання HTTP для зв'язку з командним сервером також задокументовано, наприклад, домени ten-cent.us і notepad-plusplus-updates.com

Захисні дії:

Інцидент 363 розпочався з неавторизованого доступу через RDP до системи GABUMON. Зловмисник завантажив шкідливий файл VERSION.dll та використав Quasar RAT, троян для віддаленого доступу, для контролю над системою. Після цього було здійснено мережеву розвідку з метою збору

інформації про мережу. Зловмисник також здійснив повторний вхід та запустив cmd.exe, що призвело до компрометації адміністративних облікових даних за допомогою кейлоггера. Інцидент охопив одну систему (GABUMON) та два компрометованих користувача. Штучний інтелект було використано для поведінкового аналізу користувачів та пристроїв, що дозволило виявити аномалії, такі як нетипові RDP-підключення та завантаження шкідливих файлів. Аналіз мережевого трафіку допоміг виявити патерни командно-контрольного трафіку Quasar RAT та нетипову мережеву активність. Моніторинг системних викликів та процесів дав змогу виявити запуск cmd.exe та використання кейлоггера. Для виявлення аномалій у RDP-підключеннях використовувалися алгоритми Isolation Forest та One-Class SVM. Isolation Forest - це метод, який будує ансамбль випадкових ізолюючих дерев для виявлення аномалій, визначаючи, наскільки легко об'єкти відокремлюються від решти даних. One-Class SVM використовує метод опорних векторів для визначення меж, що відокремлюють нормальну активність від аномальної, з використанням нелінійних ядер, таких як RBF, що дозволяє виявити складні аномальні патерни. Глибокі нейронні мережі (CNN) застосовувалися для аналізу мережевого трафіку та виявлення шкідливих патернів. Convolutional Neural Networks (CNN) були використані для виявлення характерних шаблонів у трафіку, що дозволило розпізнавати аномальні послідовності та сигнатури, які характерні для шкідливого програмного забезпечення. Рекурентні нейронні мережі (RNN) та приховані марковські моделі (HMM) використовувалися для моніторингу системних викликів та виявлення нетипової поведінки. RNN, зокрема LSTM (довготривала короткочасна пам'ять), здатні запам'ятовувати послідовність дій, що дозволяє їм ефективно аналізувати системні виклики та розпізнавати відхилення від нормальної поведінки. Приховані марковські моделі (HMM) використовувалися для створення моделей типової поведінки процесів та дозволяли виявляти відхилення на основі ймовірнісних переходів між станами.

Інцидент 364 показав, що на пристрої GHOSTMON був запущений файл ghosts.exe, який Microsoft Defender позначив як загрозу Trojan/Bearfoos.A!ml. Файл виконувався з каталогу C:\ghosts_client\Release\ і належав до платформи

GHOSTS, що використовується для симуляції користувацьких дій. Користувач yishida запустив ghosts.exe через explorer.exe, було завантажено складання .NET у пам'ять, а також виконано команду reset-ghosts.bat, ймовірно, віддалено з пристрою HOMELANDER. Згодом був запущений taskkill.exe для завершення кількох процесів, включаючи ghosts.exe, firefox.exe та chrome.exe. Штучний інтелект використовувався для класифікації активності як легітимної або шкідливої, враховуючи контекст виконання файлу та завантаження складання .NET. Також штучний інтелект допоміг зменшити кількість хибнопозитивних спрацьовувань шляхом аналізу контексту та поведінки файлу. Для первинної класифікації загроз використовувалися алгоритми Random Forest або SVM, які аналізували характеристики файлу. Random Forest - це ансамблевий метод, що використовує множину дерев рішень для оцінки ймовірності загрози, об'єднуючи результати кількох дерев для отримання більш точного результату. Support Vector Machine (SVM) використовувався для класифікації на основі характеристик файлу, таких як цифровий підпис та динамічна поведінка, та дозволяв створювати оптимальні гіперплощини для розділення легітимної та шкідливої активності. Глибокі нейронні мережі (CNN, MLP) застосовувалися для поглибленого аналізу та зменшення хибнопозитивів. Multi-Layer Perceptron (MLP) є класичною повнозв'язною нейронною мережею, яка використовувалася для обробки вхідних характеристик та аналізу їх складної взаємодії, що допомогло краще розрізняти легітимну та шкідливу активність. Автоенкодери використовувалися для аналізу поведінки процесів та виявлення відхилень. Автоенкодери - це нейронні мережі, які навчаються кодувати вхідні дані в компактне представлення та відновлювати їх. Виявлення відхилень здійснювалося на основі неможливості точного відновлення аномальної активності, що сигналізує про відхилення від нормальної поведінки.

Під час інциденту 372 відбулося RDP-підключення з зовнішньої IP-адреси 116.83.1.29 до пристрою CECILMON під обліковим записом DIGIRUNAWAY\kizumi. З пристрою BUTCHERMON було здійснено HTTP-запит до URL http://116.83.1.29:52388. З тієї ж IP-адреси було здійснено підключення під різними обліковими записами до кількох пристроїв, зокрема

marakawa на BUTCHERMON, ykaida на KIMERAMON. Штучний інтелект був використаний для виявлення підозрілих мережевих з'єднань та аномальної активності облікових записів. Аналіз мережевого трафіку допоміг ідентифікувати аномальні патерни та можливі командно-контрольні з'єднання. Поведінковий аналіз дозволив виявити відхилення від типової активності користувачів та пристроїв. Для виявлення нетипових IP-адрес та портів у мережевих з'єднаннях використовувалися алгоритми Isolation Forest та One-Class SVM. Isolation Forest був ефективним для виявлення аномалій у великій кількості підключень, швидко визначаючи ізольовані випадки, що не відповідали нормальним патернам. One-Class SVM допомагав моделювати нормальні з'єднання, а потім виявляти ті, що виходять за межі цих норм. Кластеризація (DBSCAN) використовувалася для кореляції автентифікаційних даних. DBSCAN (Density-Based Spatial Clustering of Applications with Noise) дозволяла групувати активність за IP-адресами та обліковими записами, виявляючи щільні кластери нормальної активності та визначаючи відокремлені випадки як аномальні. Graph Neural Networks (GNN) застосовувалися для моделювання взаємодії між пристроями та обліковими записами. GNN дозволяли представляти мережеві взаємодії у вигляді графів, де вузли - це пристрої або облікові записи, а ребра - це взаємодії між ними. Це дозволяло моделювати складні мережеві патерни та виявляти аномальні зв'язки, які можуть свідчити про компрометацію. LSTM та RNN використовувалися для поведінкового аналізу користувачів. Рекурентні нейронні мережі (RNN), особливо LSTM, здатні запам'ятовувати довготривалі залежності у послідовностях дій користувачів, що дозволяло виявляти відхилення у поведінці, такі як вхід з незвичної IP-адреси або нетипова послідовність дій.

Етап 2. Латеральний рух та збір облікових даних

Дата атаки: 13 лютого 2024 року.

Тактики атакуючих: Зловмисники створили заплановане завдання (schtasks) на системі PARROTMON, яке регулярно запускало легітимний Notepad++, що був підмінений шкідливим кодом через DLL Search Order Hijacking. Це дозволило їм отримати постійний доступ до контролера домену.

Після цього вони виконали сканування мережі, охоплюючи TCP порти 80, 445, 22, 3389 та UDP порт 53, щоб знайти інші вразливі системи та цінні ресурси для подальших атак. Також зловмисники за допомогою утиліти ntdsutil.exe зробили копію файлу ntds.dit, який містить облікові дані всіх користувачів домену, що дозволило їм отримати доступ до паролів користувачів через збережені облікові дані та реєстрові файли SYSTEM та SECURITY.

Техніки, що використовувались:

1. Persistence (T1053.005): Зловмисники створили заплановане завдання (schtasks) для регулярного запуску шкідливого коду.

2. Credential Access (T1003.003): Зловмисники зробили копію файлу ntds.dit, що містить облікові дані користувачів домену.

3. Credential Access (T1005): Зловмисники зібрали дані з локальної системи, включаючи реєстрові файли SYSTEM та SECURITY.

Захисні дії:

Інцидент 374 включав латеральне переміщення зловмисників з системи GABUMON на систему PARROTMON, встановлення шкідливого програмного забезпечення на PARROTMON, копіювання шкідливих файлів через SMB-протокол, створення запланованого завдання Notepad++ Script, а також підключення до підозрілих доменів, таких як ten-cent[.]us та notepad-plusplus-updates[.]eu. Штучний інтелект (ШІ) відіграв ключову роль у виявленні та аналізі інциденту. Зокрема, моделі машинного навчання (МН) аналізували мережевий трафік у реальному часі, виявляючи нетипові патерни у використанні SMB-протоколу та підозрілі домени, з якими встановлювалися з'єднання. Поведінковий аналіз, виконаний ШІ, порівнював дії на PARROTMON з типовими патернами поведінки, виявляючи аномалії у створенні запланованих завдань та встановленні програм. Система XDR автоматично генерувала оповіщення, надаючи команді захисників детальну інформацію для оперативного реагування. Для детекції аномалій у мережевому трафіку могли використовуватися алгоритми Isolation Forest та One-Class SVM. Ці моделі аналізували трафік, виявляючи відхилення від нормальних патернів використання SMB та DNS-запитів. У разі виявлення аномалій здійснювалося

автоматичне блокування підозрілих мережевих з'єднань та сповіщення команди безпеки. Для аналізу створення запланованих завдань використовувалися автоенкодери, які навчалися на нормальних послідовностях і виявляли аномальні завдання, блокуючи їх виконання та генеруючи оповіщення. Для класифікації шкідливих доменів застосовувалися Random Forest та SVM, які аналізували характеристики доменів та блокували доступ до виявлених шкідливих ресурсів. Алгоритми машинного навчання грали важливу роль у моніторингу мережевого трафіку, аналізі системних подій та процесів, а також автоматизації захисних реакцій, таких як блокування та генерація оповіщень.

Інцидент 377 полягав у завантаженні TeamViewer на систему, що було позначено системою XDR як підозрілу активність. Подальший аналіз показав, що завантаження було легітимним. ШІ допоміг фільтрувати хибнопозитивні спрацьовування, аналізуючи контекст завантаження, враховуючи час, користувача та історію використання. Поведінковий аналіз підтвердив, що завантаження відповідало нормальній поведінці користувача. Алгоритми, такі як Random Forest та SVM, могли використовуватися для початкової оцінки файлу, аналізу метаданих та цифрових підписів. Глибокі нейронні мережі (MLP) забезпечували контекстуальний аналіз, враховуючи поведінку користувача та корпоративні політики, що дозволяло знизити кількість хибнопозитивних спрацьовувань та запобігти зайвим втручанням у роботу користувача. Алгоритми сприяли аналізу контексту та поведінки для точнішої оцінки загроз, зменшенню хибнопозитивних спрацьовувань та підтримці прийняття рішень командою безпеки через надання релевантної інформації.

Інцидент 379 включав використання ntdsutil.exe для доступу до облікових даних, створення прихованої папки для зберігання викрадених даних, використання whoami.exe для збору інформації про систему, а також сканування мережі для пошуку додаткових цілей. ШІ забезпечив швидку обробку лог-файлів, аналіз системних викликів та кореляцію подій для створення повної картини атаки. Для аналізу системних команд та процесів використовувалися LSTM та RNN, які моделювали типову послідовність команд в системі та виявляли відхилення, такі як використання адміністративних інструментів з

незвичайними параметрами. Автоенкодери аналізували файлові операції та рух даних, виявляючи нетипові дії, такі як створення прихованих папок та копіювання великих обсягів даних. Graph Neural Networks (GNN) використовувалися для створення графічної моделі взаємодій між процесами, файлами та мережевими з'єднаннями, що дозволяло виявляти аномальні шляхи та взаємозв'язки, які вказували на атаку. Алгоритми допомагали моніторити системні дії, корелювати різнорідні дані для повного розуміння атаки та автоматизувати реагування на виявлені загрози. Аналіз також вказував на можливу компрометацію файлів ntds.dit та реєстру, з наявністю бекдорів та командно-контрольних з'єднань. Хоча прямих доказів викрадення не було знайдено, ШІ забезпечив аналіз мережевого трафіку для виявлення бекдорів, прогнозування потенційних загроз та оцінку ризиків. Для виявлення бекдорів та C2-з'єднань використовувалися алгоритми Random Forest, SVM та глибокі нейронні мережі, які аналізували характеристики мережевого трафіку та класифікували з'єднання як легітимні або шкідливі. Graph Neural Networks (GNN) моделювали можливі шляхи атаки та виявляли вузли з високим ризиком у мережі, що дозволяло здійснювати превентивні заходи для захисту критичних ресурсів.

*Етап 3***.** *Проникнення в новий домен і розширення бекдору*

Дата атаки: 14 лютого 2024 року.

*Тактики атакуючих***:** Зловмисники зібрали інформацію про об'єкти Active Directory в домені DIGIREVENGE за допомогою утиліти dsquery.exe. Під час латерального переміщення вони створили три шкідливі файли на системі KIMERAMON, використавши метод DLL Search Order Hijacking. На KIMERAMON було створено службу Notepad, яка запускала легітимний Notepad++ з шкідливою бібліотекою VERSION.dll, встановивши бекдор і з'єднавшись з командним сервером зловмисників. Вони також ін'єктували шкідливий код у процес svchost.exe для збору інформації про систему. Для викрадення облікових даних зловмисники використали утиліту secretsdump, щоб отримати хеші паролів та іншу конфіденційну інформацію, зберігаючи результати у файл C:\Windows\Temp\tmp4541.

Техніки, що використовувались:

1. Discovery (T1087.002): Використання dsquery.exe для збору інформації про облікові записи в домені DIGIREVENGE.

2. Credential Access (T1003.002): Утиліта secretsdump використовувалася для отримання хешів паролів з SAM (Security Account Manager).

Захисні дії:

Інцидент 383 характеризувався використанням кількох типів шкідливого програмного забезпечення (ПЗ) на одному пристрої, що дозволило зловмисникам значно підвищити ефективність атаки та уникнути виявлення. Однією з основних загроз була активність Quasar RAT (Remote Access Trojan), яка використовувалася для віддаленого доступу та контролю над системою. Для аналізу шкідливих файлів було застосовано статичний та динамічний аналіз, що включали перевірку метаданих, хешів, розмірів файлів, а також запуск файлів у пісочниці для спостереження за їхньою поведінкою. На основі отриманих даних будувалися моделі поведінки для виявлення шкідливих патернів. Також проводилася кластеризація загроз для групування схожих шкідливих програм та ідентифікації нових сімейств ПЗ. Штучний інтелект (ШІ) відіграв ключову роль у процесі аналізу. Зокрема, алгоритми ШІ використовувалися як для статичного, так і для динамічного аналізу файлів, з метою побудови моделей поведінки та виявлення нетипових дій програм. Також ШІ допомагав у кластеризації загроз, використовуючи алгоритми для групування схожих шкідливих файлів та ідентифікації нових сімейств. Для аналізу активності Quasar RAT були задіяні поведінкові сигнатури та мережевий моніторинг для виявлення командно-контрольного трафіку. Для виконання статичного аналізу файлів використовувалися глибокі нейронні мережі, такі як CNN та MLP, що дозволяли класифікувати файли на шкідливі та легітимні на основі метаданих та вмісту, а також виявляти патерни, характерні для шкідливого ПЗ. При динамічному аналізі в пісочниці застосовувалися рекурентні нейронні мережі (RNN), які аналізували послідовності дій файлів під час виконання та виявляли аномальну поведінку. Кластеризація загроз здійснювалася за допомогою алгоритмів K-Means та DBSCAN, які групували схожі файли для виявлення нових загроз та

ідентифікації аномалій. Для аналізу мережевої активності Quasar RAT використовувалися Graph Neural Networks (GNN), які моделювали мережеві взаємодії як графи та виявляли командно-контрольні сервери.

Під час інциденту 385 зловмисники забезпечували стійкість шкідливого ПЗ у системі, створюючи нові служби для автозапуску при завантаженні системи та додаючи відповідні записи у реєстр. Крім того, було виявлено латеральне переміщення зловмисників між системами в мережі, що сприяло поширенню шкідливого ПЗ. Штучний інтелект був задіяний для перевірки нових служб, використовуючи білі та чорні списки для ідентифікації легітимних та шкідливих служб. Алгоритми ШІ також аналізували характеристики нових служб для виявлення відхилень. Для поведінкового аналізу користувачів та пристроїв використовувалися графові моделі для аналізу мережевих з'єднань та виявлення патернів переміщення зловмисників у мережі. Для аналізу нових служб та автозапусків використовувався алгоритм Isolation Forest, що дозволяв виявляти аномальні служби на основі відхилення від нормальних параметрів. Поведінковий аналіз здійснювався за допомогою прихованих марковських моделей (HMM), які моделювали типові дії користувачів та пристроїв та виявляли відхилення, що могли вказувати на компрометацію. Аналіз мережевих з'єднань проводився за допомогою Graph Neural Networks (GNN), що дозволяло візуалізувати та аналізувати мережеві взаємодії, а також виявляти незвичні шляхи переміщення зловмисників.

Під час інциденту 387 було виявлено підозріле вихідне з'єднання до невідомої IP-адреси 121.93.44.121. Система автоматично створила інцидент для подальшого розслідування. Аналіз мережевого трафіку здійснювався з використанням алгоритмів ШІ для виявлення аномалій та ідентифікації відхилень від типового трафіку. Для детекції аномалій у мережевому трафіку використовувався алгоритм One-Class SVM, який навчався на нормальному трафіку для виявлення підозрілих з'єднань. Threat Intelligence був задіяний для оцінки репутації IP-адреси за допомогою зовнішніх баз даних, що дозволило автоматично оновлювати бази загроз. Пріоритезація інцидентів здійснювалася за допомогою алгоритму Random Forest, що класифікував інциденти за рівнем

ризику з урахуванням багатьох факторів.

Інцидент 388 характеризувався багатоступінчастим виконанням коду з ухиленням від засобів захисту, а також ін'єкцією шкідливого коду в системні процеси, зокрема svchost.exe. Система виявила аномалію через поведінковий аналіз та надала рекомендації для захисту, такі як автоматичне блокування підозрілих процесів, відновлення налаштувань безпеки та моніторинг змін конфігурацій.Для поведінкового аналізу використовувалися LSTM (Long Short-Term Memory Networks), що моделювали послідовність дій системних процесів та виявляли відхилення від нормальної поведінки. Моніторинг пам'яті здійснювався за допомогою автоенкодерів, які навчалися на нормальних зразках пам'яті процесів та виявляли аномалії. Для моніторингу конфігурацій використовувалися Random Forest або SVM, що дозволяло виявляти зміни в налаштуваннях безпеки та класифікувати їх як легітимні або шкідливі.

Етап 4. Експлуатація та ексфільтрація даних

Дата: 15 лютого 2024 року.

Тактики атакуючих: 15 лютого 2024 року зловмисники здійснили атаку на систему KIMERAMON та DATAMON, використовуючи обліковий запис DIGIREVENGE\ZORIMOTO для доступу через RDP. Вони запустили скрипт ADRecon.ps1 для збору даних про Active Directory та виконали шкідливий файл netbnmp.exe для крадіжки інформації. Захисні функції Windows Defender були вимкнені, а налаштування WDigest змінені, щоб красти облікові дані у відкритому вигляді. Вони також зробили дамп пам'яті процесу LSASS і викрали його на віддалений домен через Rclone. Після цього зловмисники перемістилися на систему ALPHAMON, використовуючи інший обліковий запис. На ALPHAMON вони завантажили Wmiexec для віддаленого виконання команд та архіватор WinRAR для збору даних. Вони створили архів з важливими даними та викрали його через віддалений мережевий ресурс. Після цього зловмисники очистили журнали подій та видалили сліди використання Wmiexec, завершивши активність на той день.

Техніки, що використовувались:

1. Credential Access (T1003.001): Дамп пам'яті процесу LSASS для

отримання облікових даних.

2. Defense Evasion (T1070.001): Очищення журналів подій.

3. Collection (T1560.001): Використання WinRAR для створення архіву важливих даних.

Захисні дії:

Інцидент 388 стосувався підозрілої активності процесу notepad++.exe, який встановив з'єднання з зовнішньою IP-адресою 121.93.44.121, створив файл 04DFAA.log та здійснив ін'єкцію коду в процес svchost.exe. У подальшому процес svchost.exe виконував команди для збору системної інформації, що свідчило про розвідувальну діяльність. Використання утиліти secretsdump.exe вказувало на спробу крадіжки облікових даних. Для виявлення аномальної поведінки були застосовані алгоритми Isolation Forest та One-Class SVM, які виділили нестандартні дії процесу notepad++.exe, такі як встановлення зовнішніх мережевих з'єднань та ін'єкція коду. Аналіз мережевого трафіку здійснювався за допомогою алгоритму K-Nearest Neighbors (KNN), що дозволило виявити підозріле з'єднання з невідомою IP-адресою. Графові нейронні мережі (GNN) використовувались для моделювання взаємодій між процесами та мережевими ресурсами, що також допомогло ідентифікувати нетипову поведінку.

Інцидент 398 виявив шкідливе ПЗ SuspShadowCreate, яке використовувало команду vssadmin.exe для створення тіньових копій файлів, що може вказувати на підготовку до ексфільтрації даних або шифрування (ransomware). Штучний інтелект ідентифікував аномалії в використанні vssadmin.exe поза типовими сценаріями резервного копіювання. Приховані марковські моделі (HMM) та алгоритми One-Class SVM або Isolation Forest були використані для аналізу типових сценаріїв використання системних утиліт. Аномальна поведінка, пов'язана зі створенням тіньових копій від імені SYSTEM, була визначена як потенційна загроза. Автоенкодери допомогли виявити високий рівень помилки реконструкції, що свідчило про нетипову активність.

Інцидент 399 показав, що користувач zorimoto увійшов на пристрій через RDP, завантажив шкідливий скрипт, увімкнув WDigest для крадіжки облікових даних, створив дамп lsass.exe та передав його через rclone на сервер. Також було

проведено мережеве сканування. Для аналізу поведінки користувачів використовувались моделі LSTM (Long Short-Term Memory Networks), які виявили послідовність дій користувача як нетипову. Алгоритм One-Class SVM визначив зміну налаштувань безпеки (увімкнення WDigest) як аномалію. Аналіз мережевого трафіку з використанням Isolation Forest дозволив виявити передачу великого обсягу даних та мережеве сканування як аномальні дії.

Під час інциденту 406 користувач zorimoto здійснив RDP-вхід, завантажив netbnmp.exe через BITSAdmin та створив файл InfoStealer.dll, який згодом був поширений на інший пристрій. Використання BITSAdmin для завантаження файлів було ідентифіковане як аномальне завдяки аналізу прихованими марковськими моделями (HMM). Автоенкодери виявили створення та розповсюдження InfoStealer.dll як відхилення від норми.

Інцидент 403, обліковий запис kizumi.da створював нових користувачів та додавав їх до привілейованих груп в Active Directory, що свідчило про потенційну компрометацію. ШІ моделі, зокрема One-Class SVM, ідентифікували ці дії як аномальні, оскільки вони не відповідали типовій поведінці адміністративного облікового запису. LSTM дозволив визначити послідовність дій kizumi.da як нетипову, а графові нейронні мережі (GNN) виявили незвичні зміни у взаємозв'язках об'єктів Active Directory.

Інцидент 408 показав, що користувач kmimi використав Openconsole.exe для завантаження шкідливого скрипта w.vbs з підозрілого домену та ініціював мережеве сканування SMB-ресурсів. Алгоритми Random Forest або SVM класифікували домен завантаження w.vbs як підозрілий. LSTM ідентифікував дії користувача як нетипові, а Isolation Forest виявив мережеве сканування як аномалію.

Інцидент 411 під час якого зловмисник завантажив файл giagl.crl на пристрій alphamon через WMI, зберіг його як conhost.exe та використав для стиснення файлів та викрадення архіву. Приховані марковські моделі (HMM) ідентифікували нетипове використання WMI для передачі файлів, а алгоритми Random Forest виявили невідповідності файлу conhost.exe з відомими легітимними файлами. Автоенкодери також виявили очищення журналів подій

як аномалію через відсутність очікуваних записів.

Етап 5. Виконання шифрувальника

Дата: 16 лютого 2024 року.

Тактики атакуючих: Зловмисник отримав доступ до системи RAREMON через RDP, використовуючи локальний обліковий запис, і розпочав низку атак на інші системи домену. Спочатку було використано завдання для запуску шкідливого коду на PARROTMON, а потім ініційовано RDP-сесію до KIMERAMON, використовуючи облікові дані DIGIREVENGE\ZORIMOTO, для завантаження інструменту collector1.exe. За допомогою PSEXEC та облікових даних DIGIREVENGE\YKAIDA.DA, шкідливий файл був розгорнутий на семи системах домену DIGIREVENGE.NET. Інструмент зібрав дані, які були відправлені через SFTP. Пізніше зловмисник завантажив файл digirevenge на KIMERAMON, а потім передав його на систему LEOMON, виконавши команди для знищення резервних копій віртуальних машин. Врешті, ransomware digirevenge.exe було завантажено на систему KIMERAMON, що поширився на інші системи, шифруючи файли та залишаючи записки з вимогою викупу. Для відключення відновлення Windows було використано команду bcdedit. Усі дії свідчать про цілеспрямовану атаку з метою викрадення даних, знищення резервних копій та розгортання шкідливого ПЗ, здійснену добре підготовленим зловмисником.

Техніки, що використовувались:

1. Exfiltration (T1048.001): Відправка зібраних даних через SFTP.

2. Impact (T1485, T1486, T1490): Знищення резервних копій віртуальних машин на системі LEOMON. Шифрування файлів за допомогою ransomware digirevenge.exe та використання команди bcdedit для відключення відновлення Windows.

3. Execution (T1127): Використання PSEXEC для розгортання collector1.exe на семи системах.

4. Collection: (T1119): Збір даних за допомогою інструменту collector1.exe.для запуску шкідливого програмного забезпечення на віддалених системах.

Захисні дії:

Інцидент 416 пов'язаний із багатоетапною атакою на системи KIMERAMON, DATAMON, BUTCHERMON та інші. Зловмисники використовували обліковий запис DIGIREVENGE\YKAIDA.DA для розгортання інструменту ExMatter за допомогою утиліти PSEXEC. ExMatter, як відомо, є інструментом для збору даних із систем, і зібрана інформація була передана на віддалений домен. Також було зафіксовано видалення тіньових копій, що вказує на підготовку до атаки програм-вимагачів. Штучний інтелект зіграв важливу роль у виявленні цієї атаки. Було зафіксовано одночасне розгортання виконуваних файлів на кількох системах, що не відповідало типовій активності облікового запису YKAIDA.DA. Це виявили алгоритми, які аналізують поведінкові патерни, а саме Long Short-Term Memory Networks (LSTM) та приховані марковські моделі (Hidden Markov Models, HMM). LSTM змоделювали послідовності дій облікового запису, використовуючи довготривалі залежності, та виявили масове розгортання ExMatter як аномалію. HMM, своєю чергою, змоделювали ймовірнісні переходи між станами, вказавши на низьку ймовірність спостережуваної послідовності дій. Інцидент також включав використання PSEXEC для поширення шкідливого коду, яке було виявлено алгоритмами Isolation Forest та One-Class Support Vector Machine (SVM). Isolation Forest ізолював аномальні точки даних, ідентифікуючи нетипове використання PSEXEC, тоді як One-Class SVM, навчаючись на нормальних даних, моделював межу нормальної поведінки та позначив використання PSEXEC як підозріле. Аналіз мережевого трафіку виявив ексфільтрацію даних, завдяки використанню графових нейронних мереж (Graph Neural Networks, GNN) та автоенкодерів. GNN моделювали мережеві взаємодії як графи та виявили нетипові патерни передачі великих обсягів даних на віддалений домен. Автоенкодери, натомість, навчаючись відтворювати нормальний трафік, виявили аномалії через високу помилку реконструкції. Що стосується видалення тіньових копій, то алгоритм HMM змоделював послідовності системних команд, ідентифікувавши видалення тіньових копій як нетипову дію, яка вказує на підготовку до атаки програм-вимагачів.

Інцидент 426 включав розгортання програми-вимагача RAPIDSTOP на кількох пристроях. Зловмисник використовував обліковий запис YKAIDA.DA для виконання PSEXECSVC.EXE із шкідливим навантаженням DIGIREVENGE.EXE, що блокувало відновлення операційної системи та модифікувало системні файли. Окрім цього, через обліковий запис MARAKAWA був здійснений доступ через SSH із правами root, після чого завершено роботу віртуальних машин та видалено їх знімки. Штучний інтелект був застосований для виявлення аномалій у використанні облікового запису YKAIDA.DA. Моделі машинного навчання, такі як LSTM та One-Class SVM, ідентифікували нетипову активність, пов'язану з розгортанням шкідливого програмного забезпечення. LSTM змоделювали послідовність дій облікового запису та виявили відхилення від норми, а One-Class SVM, навчившись на нормальній поведінці, позначив підозрілі дії. Розпізнавання дій, характерних для програм-вимагачів, було здійснено за допомогою алгоритмів Random Forest та глибоких нейронних мереж (Convolutional Neural Networks, CNN, та Multi-Layer Perceptron, MLP). Random Forest класифікував блокування відновлення ОС та модифікацію файлів як шкідливі дії на основі характеристик, тоді як CNN та MLP розпізнали складні патерни, характерні для програм-вимагачів, з високою точністю. Доступ через SSH з підвищеними привілеями був виявлений як аномальний завдяки HMM, які моделювали типові сценарії доступу. Крім того, автоенкодери ідентифікували нетипове завершення роботи віртуальних машин як аномалію. Графові нейронні мережі (GNN) забезпечили кореляцію подій, поєднавши інформацію про дії облікових записів, мережеві з'єднання та системні події, що дозволило створити повну картину атаки та виявити масштаб загрози. Таке корелювання є важливим для розуміння складності атак та координації дій для їх нейтралізації. Застосування алгоритмів штучного інтелекту, таких як LSTM, HMM, Random Forest, GNN та автоенкодери, забезпечило ефективне виявлення аномальної поведінки, аналіз мережевих загроз та кореляцію подій. Це підтверджує високу ефективність використання штучного інтелекту для виявлення та нейтралізації сучасних кіберзагроз.

3 РЕКОМЕНАДЦІЇ ТА ПРОПОЗИЦІЇ ЩОДО ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ

3.1 Технологія впровадження сучасних систем захисту кінцевих точок із штучним інтелектом

Основні рекомендації щодо впровадження сучасних систем захисту кінцевих точок, які наділені функціями штучного інтелекту та алгоритмами машинного навчання, включаючи вибір відповідних інструментів, інтеграцію з існуючою інфраструктурою та підготовку персоналу, що допоможе забезпечити комплексний та адаптивний захист кінцевих точок в організації. Рекомендації нижче можуть допомогти організаціям впровадити даний тип систем.

Рисунок 3.1. Кроки впровадження EDR в організації [72]

1. Вимоги та планування

1.1 Збір вимог та планування

Перед впровадженням EDR чи XDR важливо визначити вимоги організації до безпеки та оцінити наявні ресурси.

1. Типи кінцевих точок: Ідентифікувати, які кінцеві точки (сервери, робочі станції, мобільні пристрої) потребують захисту.

2. Інтеграція з іншими системами: Перевірити, чи підтримує система інтеграцію з уже наявними засобами безпеки та управління.

3. Потреба в автоматизації: Визначити, які завдання можна автоматизувати за допомогою AI.

Також необхідно оцінити поточний рівень готовності організації до впровадження нових технологій. Важливо провести аудит кібербезпеки для виявлення слабких місць та потенційних вразливостей, що можуть бути використані кіберзловмисниками. Це дозволить краще спланувати процес впровадження та уникнути проблем у майбутньому [74].

1.2. Пілотне розгортання

Пілотне розгортання є важливим етапом, що дозволяє оцінити ефективність системи в реальних умовах. Компаніям рекомендується починати з невеликої кількості кінцевих точок для тестування всіх функцій, таких як виявлення, реагування та автоматизація процесів. Це дозволить виявити можливі проблеми, налаштувати параметри системи та перевірити інтеграцію з іншими компонентами кібербезпеки із якими потрібно буде взаємодіяти.

На цьому етапі важливо також залучити до процесу ключових стейкхолдерів, включаючи IT-відділ та команду з кібербезпеки. Спільна робота дозволить краще адаптувати систему до вимог організації та врахувати специфіку роботи різних підрозділів. Важливо також підготувати чіткий план реагування на можливі інциденти, що можуть виникнути під час пілотного розгортання [74, 75].

1.3. Масштабування та налаштування політик

Після успішного пілотного розгортання слід перейти до повномасштабного впровадження системи з одночасним налаштуванням політик безпеки, які були обрані для впровадження, таких як автоматичне блокування підозрілих дій та повідомлення про інциденти. На цьому етапі важливо налаштувати політики реагування на загрози відповідно до специфіки роботи організації.

Налаштування політик може включати визначення правил виявлення та реагування на підозрілі дії, а також встановлення порогових значень для активації певних дій системи. Наприклад, автоматичне блокування певної активності може бути налаштоване на основі аналізу поведінкових шаблонів

користувачів. Необхідно враховувати фактор мінімізації хибнопозитивних спрацьовувань. Це допоможе уникнути блокування легітимних процесів та непотрібного навантаження на команду з кібербезпеки [74].

2. Вибір вендора для EDR/XDR систем

Вибір постачальника рішення EDR чи XDR є критично важливим для ефективності впровадження. Різні вендори пропонують різний функціонал, і важливо вибрати систему, яка найкраще відповідає потребам вашої організації. Для того, щоб обрати вендора, потрібно звертати увагу на такі критерії при виборі вендора:

1. Інтеграція з наявними рішеннями: Наскільки легко рішення інтегрується з іншими системами безпеки та управління?

2. Здатність до масштабування: Чи може рішення ефективно працювати при збільшенні кількості кінцевих точок або обсягів даних?

Також важливо звернути увагу на підтримку та обслуговування з боку вендора. Забезпечення своєчасних оновлень та надання технічної підтримки є критичними для підтримання високого рівня безпеки. Варто оцінити, наскільки активно вендор займається розвитком своєї системи та впровадженням нових функцій, що дозволяють адаптуватися до змін у кіберзагрозах і завжди мати актуальний захист від сучасних загроз.

Ще одним фактором є можливість отримання пробного періоду або демо-версії платформи, для оцінки її функціональності перед повним впровадженням. Це допомагає знизити ризики неправильного вибору та дає змогу протестувати систему в реальних умовах [74].

3. Виклики при впровадженні EDR та XDR

Попри всі переваги, впровадження систем EDR та XDR має свої виклики, серед яких:

1. Інтеграція з наявними інструментами: Відсутність належної інтеграції може призвести до розрізненості систем безпеки та зниження ефективності.

2. Фальшиві тривоги: Використання AI, у деяких випадках все ще можуть виникати фальшиві спрацювання, що потребують ручної перевірки.

3. Кваліфікація персоналу: Для роботи з системами EDR/XDR потрібні

кваліфіковані фахівці, здатні ефективно використовувати аналітичні дані, надані системою.

Для подолання цих викликів, важливо розробити чітку стратегію інтеграції нових рішень у поточну архітектуру безпеки. Це може включати попередню оцінку всіх наявних засобів безпеки, визначення можливостей інтеграції та взаємодії, а також тестування всіх інтеграційних компонентів на етапі пілотного впровадження.

Щоб зменшити кількість фальшивих тривог слід налаштувати систему таким чином, щоб вона могла враховувати специфіку роботи організації та поведінкові шаблони її користувачів. Використання алгоритмів машинного навчання та алгоритмів AI дозволяє адаптувати систему до змін у поведінці користувачів і знижувати кількість помилкових спрацьовувань [74].

4. Рекомендації щодо успішного впровадження

4.1. Навчання персоналу

Впровадження системи захисту кінцевих точок вимагає кваліфікованого персоналу. Спеціалісти повинні пройти навчання, щоб використовувати можливості платформи максимально ефективно. Важливо навчати фахівців не лише технічним аспектам, але й особливостям роботи з інцидентами безпеки, які можуть бути.

Крім навчання спеціалістів з кібербезпеки, важливо також проводити навчання для загального персоналу організації. Це включає підвищення обізнаності щодо поточних загроз та правил безпеки, які допомагають уникнути інцидентів [74, 75]. Навчання повинно охоплювати такі основні аспекти:

1. Виявлення фішингових атак, для уникнення зламу;

2. Правильне поводження з підозрілими файлами та електронними листами;

3. Вимоги до створення та зберігання надійних паролів.

4.2. Постійний моніторинг та оцінка ефективності

Навіть після впровадження важливо проводити постійний моніторинг роботи системи, для оцінки її ефективності та своєчасно вносити корективи. Використання аналітики та звітності дозволяє краще розуміти, як система

захищає кінцеві точки, та виявляти можливі покращення.

Моніторинг системи включає аналіз журналів подій, виявлення аномальної активності та відстеження продуктивності системи. Саме регулярні аудити дозволяють визначити, наскільки ефективно система може виявляти та блокувати загрози, а також наскільки швидко реагувати на інциденти. Це дозволяє своєчасно виявляти слабкі місця та впроваджувати необхідні зміни [75].

4.3. Автоматизація рутинних завдань

AI у системах EDR та XDR дозволяє автоматизувати рутинні процеси, такі як аналіз журналів подій та реагування на хибні тривоги. Це значно знижує навантаження на фахівців з безпеки та дозволяє зосередитися на більш складних інцидентах.

Така автоматизація в системі, також включає автоматичне реагування на певні типи загроз. Наприклад, у разі виявлення підозрілої активності система може автоматично ізолювати кінцеву точку від мережі, якщо в цьому є необхідність, щоб запобігти поширенню загрози. Це дозволяє мінімізувати час реагування на інциденти та зменшити можливий вплив на організацію.

Для успішного впровадження необхідно ретельно планувати процес, вибирати надійних вендорів, навчати персонал та забезпечувати постійний моніторинг і вдосконалення системи. Дотримання наведених рекомендацій допоможе організаціям ефективно захищати свої кінцеві точки від сучасних загроз.

Важливо враховувати, що кіберзагрози постійно еволюціонують, і системи захисту мають та повинні адаптуватися до цих змін. Регулярне оновлення системи, використання сучасних алгоритмів AI та машинного навчання, а також проведення навчання персоналу дозволяють забезпечити належний рівень безпеки та захистити організацію від потенційних атак. Постійна співпраця між різними підрозділами організації, включаючи IT, кібербезпеку та керівництво, є ключовою для успішного впровадження та підтримання системи захисту кінцевих точок на високому рівні.

3.2 Пропозиція щодо покращення традиційних рішень шляхом впровадження сучасних технологій

Зі зростанням складності кіберзагроз, організації можуть стикатись із новими загрозами, що вимагають вдосконалених рішень для захисту кінцевих точок. Традиційні антивірусні рішення у вигляді антивірусу, які використовують сигнатурний аналіз, стають менш ефективними проти сучасних складних атак. Такі загрози як Zero-Day, APT та дії пов'язані із зловмисною діяльність, яка впливає на електронну пошту, наприклад: фішинг, потребують підходу, який не обмежується лише виявленням вже відомих загроз, а також може включати моніторинг і аналіз поведінки систем та користувачів. Системи захисту кінцевих точок, такі як EDR та NGAV, пропонують проактивний підхід до безпеки завдяки поведінковому аналізу, автоматизованому реагуванню та інтеграції AI. В якості пропозиції, розглядається можливість вдосконалення традиційних рішень захисту шляхом інтеграції сучасних технологій, надаючи рекомендації на основі порівняльного аналізу переваг, обмежень традиційних і сучасних підходів. Застосування нових методів забезпечить більш високий рівень захисту від нових загроз та зможе знизити ймовірність успішних атак, тим самим зменшуючи ризики для організацій та забезпечуючи надійну кібербезпеку [76-81].

Відмінності традиційних рішень в порівнянні із сучасними, можна наглядно побачити в таблиці 3.1.

Таблиця 3.1

Порівнянна традиційних та сучасних рішень захисту кінцевих точок [76-81]

Параметр	*Традиційні рішення*	*Сучасні рішення*
Метод виявлення загроз	Сигнатурний аналіз	Поведінковий аналіз, AI, машинне навчання
Тип загроз	Тільки відомі загрози	Відомі, невідомі, Zero-Day загрози
Моніторинг системи	Переважно періодичне сканування	Постійний моніторинг у реальному часі

Здатність до кореляції подій	Відсутня	Є можливість кореляції подій між різними кінцевими точками
Реагування на інциденти	Переважно вручну	Автоматизоване реагування, ізоляція загроз, сценарії усунення (playbooks)
Орієнтація захисту	Охоплення тільки окремих кінцевих точок	Глобальний захист з інтеграцією даних між всіма кінцевими точками
Захист від атак Zero-Day	Обмежений	Розширений захист за допомогою поведінкового аналізу та машинного навчання
Автоматизація процесів	Відсутня	Високий рівень автоматизації: від виявлення загроз до їх усунення
Обмін даними між компонентами	Локальний, обмежений	Централізований обмін даними між всіма компонентами системи
Інтеграція з іншими засобами безпеки	Обмежена	Розширена інтеграція з фаєрволами, мережевими аналізаторами, SIEM тощо
Робота в гібридних середовищах	Обмежена	Підтримка як локальних, так і хмарних середовищ
Швидкість реагування на загрозу	Може бути уповільненою через ручну взаємодію	Миттєва завдяки автоматизованим механізмам реагування
Аналітика та звітність	Основні звіти, мало інформації для аналізу	Детальна аналітика подій, глибокий аналіз причин загрози
Підхід до захисту	Реактивний (реагування після виявлення загрози)	Проактивний (виявлення та запобігання на основі аналізу поведінки та прогностичних моделей)

*Рекомендації***:**

1. Інтеграція поведінкового аналізу: Традиційні антивірусні рішення

потребують інтеграції поведінкового аналізу для покращення виявлення загроз. Поведінковий аналіз дозволяє виявляти аномалії в роботі програм і систем, що є важливим для запобігання Zero-Day атакам та складним атакам. Згідно з [78], EDR використовує моделі аналізу поведінки, що дозволяє ефективно виявляти підозрілу активність, яку традиційні рішення не можуть визначити.

2. Автоматизація реагування: Впровадження автоматизованого реагування на загрози може допомогти організаціям швидше реагувати на загрози та мінімізувати людський фактор. Сучасні EDR мають змогу автоматично ізолювати інфіковані кінцеві точки та ініціювати процеси відновлення, що значно скорочує час реагування на інциденти. Інформація [81] підкреслює, що відповідь у реальному часі є критично важливим фактором для ефективної боротьби з загрозами.

3. Централізоване управління та кореляція подій: Традиційні рішення мають вдосконалюватись інструментами централізованого збору даних та їх кореляції. Це може дозволити виявляти складні атаки на основі аналізу взаємозв'язків між подіями. За даними [79], сучасні EDR дозволяють збирати дані з різних кінцевих пристроїв, що покращує видимість і контроль над безпекою.

4. Підтримка хмарних середовищ: Сучасні загрози часто спрямовані на гібридні та хмарні середовища, традиційні рішення мають адаптуватися до таких самих умов. Інтеграція хмарних технологій захисту дозволяє забезпечити видимість і контроль над кінцевими точками незалежно від їх місцезнаходження. Згідно [76] наголошує на зручності використання хмарної платформи для керування кінцевими точками.

5. Постійний моніторинг та аналітика: Традиційні антивірусні рішення мають забезпечувати постійний моніторинг кінцевих точок для виявлення підозрілої активності у реальному часі. Використання систем штучного інтелекту та алгоритмів машинного навчання дозволяють швидко реагувати на загрози та виявляти приховані загрози. Даний ресурс [80] підкреслює, що постійний моніторинг дозволяє ефективніше захищати систему, ніж періодичні сканування.

6. Навчання користувачів: Користувачі, які працюють за робочими пристроями залишаються найбільш вразливою частиною системи безпеки. Необхідність підвищувати обізнаність користувачів щодо можливих загроз та навчати їх відповідним заходам безпек, зможе посилити політики безпеки, які використовує компанія. Це зменшить ризики, пов'язані з соціальною інженерією.

7. Використання інструментів штучного інтелекту: Інтеграція сучасних засобів у традиційні антивірусні рішення дозволяє підвищитиефективність у виявленні нових загроз та запобіганні їм. Засоби ШІ можуть аналізувати великі обсяги даних, виявляти аномалії та приймати рішення щодо нейтралізації загроз. Інформація [80] наголошує на важливості використання AI для захисту від складних загроз.

8. Інтеграція з іншими продуктами безпеки: Традиційні антивірусні рішення мають бути інтегровані з іншими засобами кібербезпеки, такими як фаєрволи, засоби для аналізу мережевого трафіку та системи інформаційної безпеки, такими як: SIEM. Це дозволяє створити багаторівневий захист і забезпечити максимально ефективну взаємодію між різними компонентами системи безпеки.

9. Розширення можливостей реагування на інциденти: Впровадження EDR дозволяє значно розширити можливості реагування на інциденти, надаючи інструменти як для глибокого аналізу причин інциденту так і для запобігання їх повторенню. Це критично важливо для забезпечення постійного вдосконалення безпеки організації.

3.3 Рекомендації щодо адаптації технологій під потреби організацій

Захист кінцевих точок є ключовою складовою кібербезпеки сучасних організацій. Він включає використання програмних та апаратних засобів для забезпечення безпеки всіх пристроїв, що підключаються до корпоративної мережі, від комп'ютерів до смартфонів і IoT-пристроїв. Але різні організації мають різні ресурси та потреби. Для правильної адаптації технології захисту відповідно до розміру організації, потрібно враховувати їхні можливості та

особливості. Нижче приведено приведені рекомендації по адаптації технології до малої, середньої та великої компанії.

1. Адаптація технологій до малої організації

1.1 Особливості малих організацій

Організації меншого розміру зазвичай мають обмежені фінансові та людські ресурси, що має вплив на їхню здатність ефективно реагувати на сучасні кіберзагрози. Кількість кінцевих точок у таких організаціях також невелика, а технічна підтримка може обмежуватись одним або кількома фахівцями, які відповідають за всі аспекти роботи інфраструктури.

1.2 Вибір технології захисту

Для малих організацій найбільш доцільним є використання рішень, які не вимагають великих інвестицій і прості у впровадженні та підтримці. Основні рекомендації:

1. *Хмарні рішення*: Використання хмарних рішень для захисту кінцевих точок дозволяє зменшити витрати на апаратне забезпечення та мінімізувати потребу в спеціалізованих IT-кадрах. Такі рішення можуть бути із інтегрованим антивірусом та системою управління дозволять забезпечити базовий захист без великих вкладень.

2. *Автоматизація функцій захисту*: Малі організації часто не мають ресурсу на оперативне реагування на інциденти. Використовувати автоматизаційні сценарії для виявлення і запобігання загрозам (так звані playbooks) може значно полегшити життя IT-спеціалістам.

3. *Антивірусні рішення з додатковими функціями*: Підприємства малого розміру можуть вибрати антивірусні рішення, які пропонують розширені функції, такі як брандмауер, антифішинг та захист від рансомвару в одному пакеті. Це дозволяє зменшити витрати та мінімізувати кількість інструментів, які потрібно налаштовувати і обслуговувати.

1.3 Практичні рекомендації

1. Використання єдиного провайдера безпеки для зменшення складності управління. Використання одного вендора допоможе краще зрозуміти можливості його продуктів та як вони працюють між собою;

2. Автоматизоване оновлення систем та антивірусного захисту для зменшення ризику пропуску важливих оновлень.

3. Використання базових політик доступу для обмеження несанкціонованого використання корпоративних ресурсів.

2. Адаптація захисту для середніх організацій

2.1 Особливості середніх організацій

Середні організації мають більшу кількість кінцевих точок, що збільшує потенційні вектори атаки. Крім того, вони можуть мати розподілену IT-інфраструктуру, яка включає кілька офісів, і більш складну організаційну структуру. Дані організації можуть мати окремий підрозділ інформаційної безпеки або кілька спеціалізованих IT-фахівців.

2.2 Вибір технології захисту

Для середніх організацій підходять рішення, які забезпечують трохи більший рівень контролю та можливості для розширення своїх систем безпеки. Основні рекомендації:

1. *EDR системи*: Даний рівень організацій може розглядати рішення захисту кінцевих точок, які містять додаткові функції моніторингу активності на кінцевих точках, виявлення підозрілої поведінки і реагування на інциденти.

2. *Інтеграція із додатковими системами*: Організації середнього розміру, можуть отримати додаткову користь від інтеграції різних систем захисту кінцевих пристроїв. Це дозволяє отримувати централізоване управління та уявлення про інциденти безпеки і швидше реагувати на загрози.

3. *Управління мобільними пристроями*: Оскільки мобільні пристрої є важливим елементом інфраструктури середніх організацій, важливо впроваджувати політики керування ними для забезпечення додаткового контролю над доступом до корпоративних даних.

2.3 Практичні рекомендації

1. Використання централізованої панелі для моніторингу всіх кінцевих точок в організації за допомогою продуктів, які були впроваджені та інтегровані.

2. Навчання для спеціалістів кібербезпеки з метою підвищення обізнаності про нові кіберзагрози, техніки захисту та роботу із системами захисту

3. Нові тактики та системи, допоможуть із впровадженням політик сегментації мережі для зменшення можливостей переміщення атакуючого всередині корпоративної мережі.

3. Адаптація захисту для великих організацій

3.1 Особливості великих організацій

Великі організації мають складну інфраструктуру, що включає велику кількість кінцевих точок, кілька центрів обробки даних, розподілені офіси та, часто, велику кількість співробітників, які можуть працювати віддалено. Вони стикаються з високими вимогами до інформаційної безпеки через підвищений інтерес кіберзлочинців до їх організації та через необхідність дотримання різних нормативних вимог.

3.2 Вибір технології захисту

Для великих організацій потрібні комплексні та масштабовані рішення, які можуть інтегруватися з існуючими системами і забезпечити високий рівень автоматизації та координації дій між підрозділами. Основні рекомендації:

1. *Комплексне рішення для виявлення і реагування на загрози*: Використання XDR-рішень, дозволяє об'єднати дані з різних джерел для кращого виявлення загроз і координації дій між різними системами захисту (кінцеві точки, мережа, електронна пошта тощо).

2. *Безпека як послуга*: Додатковою опцією для організації може бути впровадення керованих послуг з безпеки (MSSP) для моніторингу та реагування на інциденти. Це може допомогти зменшити навантаження на внутрішній відділ інформаційної безпеки та підвищити рівень захисту за рахунок кваліфікованих співробітників.

3. *Розширене управління доступом*: Впровадження багатофакторної автентифікації, управління ролями і політиками доступу, що забезпечить кращий контроль над користувачами та їх правами доступу до різних ресурсів.

4. *Сегментація та зонування*: Великі організації можуть використовувати принципи зонування для поділу мережі на ізольовані сегменти, що мінімізує можливість розповсюдження загроз у разі компрометації.

3.3 Практичні рекомендації

1. Створення спеціалізованих команд безпеки (SOC), які відповідатимуть за моніторинг та реагування на інциденти в реальному часі.

2. Використання поведінкового аналізу для виявлення аномальної активності та проактивного запобігання атакам.

3. Регулярне проведення навчань для співробітників з кібербезпеки, а також тестування захищеності систем за допомогою внутрішніх чи зовнішніх пентестів.

ВИСНОВКИ

Висновок дипломної роботи узагальнює основні результати дослідження впливу штучного інтелекту на системи захисту кінцевих точок та їх ефективність у протидії сучасним кіберзагрозам. Дослідження показало, що зі зростанням складності загроз, новими підходами та тактиками атаки, традиційні засоби захисту, такі як антивірусні програми, більше не можуть забезпечити необхідний рівень безпеки. Постало питання про необхідне використання нових підходів, зокрема впровадження систем на основі штучного інтелекту.

Штучний інтелект забезпечує проактивний захист, який дозволяє не лише виявляти та реагувати на загрози, а й запобігати їх виникненню завдяки прогнозуванню на основі аналізу поведінкових патернів. В якості переваги сучасних систем захисту, таких як XDR (розширене виявлення та реагування), можна зазначити здатність збирати й аналізувати дані з різних джерел, включаючи кінцеві точки, мережевий трафік та хмарні ресурси. Завдяки використанню алгоритмів машинного навчання та глибокого навчання ці системи здатні самонавчатись, аналізуючи попередній досвід для покращення реакції на загрозу, що значно підвищує їхню ефективність у виявленні нових типів атак, таких як атаки нульового дня або безфайлові загрози.

Протягом еволюції технологій захисту кінцевих точок від статичних антивірусних систем до сучасних рішень на основі ШІ, було відмічено кілька ключових етапів. Спершу використовувались підходи на основі сигнатур, що були ефективними лише для вже відомих загроз. Наступним етапом стало впровадження евристичного аналізу, який дозволив виявляти загрози на основі аналізу підозрілих інструкцій та структур коду. З розвитком кіберзлочинності виникла необхідність застосовувати більш вдосконалені методи, такі як поведінковий аналіз, виявлення аномалій та ізоляція кінцевих точок. У цьому контексті особливу роль відіграли системи EDR (виявлення та реагування на кінцевих точках), які почали активно використовувати алгоритми машинного навчання для підвищення точності виявлення загроз.

Сучасні рішення, такі як Microsoft Defender, Palo Alto Cortex XDR та CrowdStrike Falcon, які були проаналізовані в роботі, є прикладами ефективного впровадження штучного інтелекту в системи захисту. Вони не лише забезпечують базовий захист від загроз, а й використовують інтелектуальні алгоритми для автоматизації реагування на інциденти, що значно зменшує час реагування на загрози та мінімізує вплив людського фактора.

Також важливо відзначити розвиток хмарних рішень для захисту кінцевих точок, які дозволяють централізовано керувати безпекою великої кількості пристроїв, що особливо актуально у зв'язку зі зростанням популярності віддаленої роботи. Хмарні технології захисту забезпечують масштабованість, гнучкість і доступність, що робить їх популярним вибором для сучасних організацій. Крім того, можна зазначити, що впровадження архітектури нульової довіри (Zero Trust Architecture) посилило підхід до безпеки, де кожна взаємодія має бути підтверджена незалежно від її походження.

Проведений аналіз підтвердив, що впровадження систем захисту кінцевих точок із застосуванням штучного інтелекту є доцільним і необхідним кроком для забезпечення ефективної кібербезпеки сучасних організацій. Такого роду системи мають високу адаптивність до змінних загроз, що особливо важливо в умовах постійного зростання складності та кількості атак. Використання систем ШІ дозволяє створити комплексну систему безпеки, яка може не тільки виявляти та усувати загрози, а й навчатися на попередньому досвіді для запобігання майбутнім інцидентам.

На основі результатів дослідження можна надати рекомендації щодо впровадження сучасних систем захисту кінцевих точок із застосуванням технологій штучного інтелекту. Компаніям варто оцінити наявні загрози та обрати систему, яка найбільше відповідає їхнім потребам. Наступним кроком важливо забезпечити інтеграцію таких систем із іншими засобами кібербезпеки, такими як SIEM або IAM, для підвищення ефективності реагування на інциденти. На останок варто зауважити про необхідність забезпечити постійне навчання моделей ШІ на актуальних даних, що дозволить підвищити точність виявлення загроз та зменшити кількість хибних спрацьовувань.

Таким чином, впровадження штучного інтелекту в системи захисту кінцевих точок є важливим кроком для забезпечення надійної та ефективної кібербезпеки. Використання сучасних рішень на основі ШІ дозволяє створити проактивний підхід до захисту, який відповідає викликам сучасного кіберпростору та забезпечує високий рівень безпеки для організацій різного масштабу. Подальший розвиток технологій захисту кінцевих точок та впровадження інноваційних рішень на основі ШІ допоможуть знизити ризики кібератак і забезпечити стабільну роботу бізнесу в умовах зростаючих кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Tanium. What are Endpoint Devices? URL: https://www.tanium.com/blog/what-are-endpoint-devices/ (дата звернення: 13.10.2024).

2. Klik Solutions. ТОП-5 загроз для кінцевих точок та як партнерство з провайдером керованих послуг кібербезпеки допомагає їх нейтралізувати. URL: https://www.kliksolutions.com.ua/great-info/zagrozy-dlya-kinczevyh-tochok/ (дата звернення: 14.10.2024).

3. NinjaOne. Endpoint Devices Explained with Examples. URL: https://www.ninjaone.com/blog/endpoint-devices-explained-with-examples/ (дата звернення: 14.10.2024).

4. Evergreens. Огляд машинного навчання. URL: https://evergreens.com.ua/ua/articles/machine-learning-overview.html (дата звернення: 16.10.2024).

5. Zfort. Штучний інтелект чи машинне навчання? В чому різниця. URL: https://www.zfort.com.ua/blog/shtuchnii-intelekt-chi-mashinne-navchannya-v-chomu-riznicya (дата звернення: 16.10.2024).

6. Сучасна освіта. Штучний інтелект. Інженерія знань. Машинне навчання – в чому різниця? URL: https://osvita.in.net/articles/133 (дата звернення: 16.10.2024).

7. Kaur H., Sanjai SL, Paul T., Thakur RK, Reddy KV, Mahato J, Naveen K. Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive Review. E3S Web of Conferences 556, 01006 (2024). Lovely Professional University. С. 3. URL: https://doi.org/10.1051/e3sconf/202455601006 (дата звернення: 14.10.2024).

8. VPN Unlimited. Сигнатура атаки. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/attack-signature (дата звернення: 24.10.2024).

9. VPN Unlimited. Евристичний вірус. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/heuristic-

virus?srsltid=AfmBOooJHvn66mP8Srtro9dA1ePh4ExLubt2pNWhH9ldVzLIYJbvxCif (дата звернення: 24.10.2024).

10. Sysdig. What is HIDS? URL: https://sysdig.com/learn-cloud-native/what-is-hids/#:~:text=A%20Host%2DBased%20Intrusion%20Detection,security%20breach%20or%20attempted%20attack (дата звернення: 24.10.2024).

11. ESET. Брандмауер. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/brandmauer/?srsltid=AfmBOoqFLbekiDQRiXSjitaCP9RZJHceMkMFPcnSU8DdzAWdkdqOv0Tq (дата звернення: 24.10.2024).

12. VPN Unlimited. Антивірус. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/antivirus?srsltid=AfmBOopyYyAQyy1qn--jP7OGJd9xUPtddvicb07dF27jx773HTzoF7VX (дата звернення: 24.10.2024).

13. Arizona Western College. Cyber Criminology. URL: https://www.azwestern.edu/degrees-and-certificates/transfer-degree/cyber-criminology#:~:text=Cyber%20criminology%20explores%20Internet%20Crimes,in%20the%20investigation%20and%20prosecution (дата звернення: 14.10.2024).

14. Kingston. What is Encryption. URL: https://www.kingston.com/ua/blog/data-security/what-is-encryption (дата звернення: 14.10.2024).

15. Mediacom. Як працює антивірус? Технологія за лаштунками. URL: https://mediacom.com.ua/yak-pratsyue-antivirus-texnologiya-za-lashtunkami/ (дата звернення: 22.10.2024).

16. Sapphire. NIDS. URL: https://www.sapphire.net/blogs-press-releases/nids/ (дата звернення: 22.10.2024).

17. SNT. Управління і аналіз трафіка DPI. URL: https://www.snt.ua/portfolio/it-resheniya/operatorskie-resheniya/upravlenie-i-analiz-trafika-dpi (дата звернення: 22.10.2024).

18. Fortinet. Indicators of Compromise (IOCs). URL: https://www.fortinet.com/resources/cyberglossary/indicators-of-

compromise#:~:text=Indicators%20of%20compromise%20(IOCs)%20refer,or%20another%20breach%20in%20security (дата звернення: 22.10.2024).

19. Check Point. What is Sandboxing? URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-sandboxing/#:~:text=Sandboxing%20is%20a%20cybersecurity%20practice,inspect%20untested%20or%20untrusted%20code (дата звернення: 22.10.2024).

20. Microsoft. What is EDR (Endpoint Detection and Response). URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-edr-endpoint-detection-response (дата звернення: 22.10.2024).

21. Microsoft. Manage the deception capability in Microsoft Defender XDR. URL: https://learn.microsoft.com/en-us/defender-xdr/deception-overview (дата звернення: 22.10.2024).

22. Cyber Business. Аналітика поведінки користувачів та суб'єктів господарювання (UEBA). URL: https://cyber.business.gov.ua/cybercatalogue/user-and-entity-behavior-analytics-ueba (дата звернення: 22.10.2024).

23. Microsoft. Що таке XDR? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-xdr (дата звернення: 24.10.2024).

24. Palo Alto Networks. What is a Zero Trust Architecture. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture (дата звернення: 24.10.2024).

25. CrowdStrike. Endpoint Detection and Response (EDR). URL: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/?srsltid=AfmBOoq2u_AGM-8eWcNRI1qD0FBTP_f4GtOYibMcWzl1ZKYCWKPTry3I (дата звернення: 24.10.2024).

26. Шуліка К., Балагура Д., Смірнов А., Непокритов Д., Литвин А. Метод використання сучасних систем захисту кінцевих точок (EDR) для убезпечення від комплексних атак. Innovative technologies and scientific solutions for industries. 2024. No. 2 (28). DOI: https://doi.org/10.30837/2522-9818.2024.2.182.

(дата звернення: 24.10.2024).

27. Wikipedia. Gartner. URL: https://en.wikipedia.org/wiki/Gartner (дата звернення: 27.10.2024).

28. Gartner. Magic Quadrant Research. URL: https://www.gartner.com/en/information-technology/research/magic-quadrant (дата звернення: 27.10.2024).

29. SentinelOne. Storyline Active Response - Gartner MQ 24. URL: https://assets.sentinelone.com/storyline-active-response/gartner-mq-24?xs=817098 (дата звернення: 27.10.2024).

30. Forrester. About Us - Fact Sheet. URL: https://www.forrester.com/about-us/fact-sheet/ (27.10.2024).

31. Forrester. Forrester Wave Methodology. URL: https://www.forrester.com/policies/forrester-wave-methodology/ (дата звернення: 27.10.2024).

32. Microsoft. Microsoft is Named a Leader in the Forrester Wave for XDR. URL: https://www.microsoft.com/en-us/security/blog/2024/06/03/microsoft-is-named-a-leader-in-the-forrester-wave-for-xdr/ (дата звернення: 27.10.2024).

33. IDC. Analysts. URL: https://www.idc.com/analysts (дата звернення: 27.10.2024).

34. IDC. IDC MarketScape. URL: https://www.idc.com/promo/idcmarketscape (дата звернення: 27.10.2024).

35. Softprom. IDC MarketScape Worldwide Modern Endpoint Security for Enterprises 2024 Vendor Assessment. URL: https://softprom.com/sites/default/files/materials/idc-marketscape-worldwide-modern-endpoint-security-for-enterprises-2024-vendor-assessment.pdf (дата звернення: 27.10.2024).

36. AV-Comparatives. About Us. URL: https://www.av-

comparatives.org/about-us/ (дата звернення: 27.10.2024).

37. AV-Comparatives. Endpoint Prevention & Response (EPR) Test 2024. URL: https://www.av-comparatives.org/tests/endpoint-prevention-response-epr-test-2024 (дата звернення: 27.10.2024).

38. MITRE Engenuity. Managed Services - MenuPass and BlackCat. URL: https://attackevals.mitre-engenuity.org/managed-services/menupass-blackcat/ (дата звернення: 27.10.2024).

39. SentinelOne. Storyline Active Response - Gartner MQ 24. URL: https://assets.sentinelone.com/storyline-active-response/gartner-mq-24?xs=817098 (дата звернення: 27.10.2024).

40. Microsoft. Microsoft is Named a Leader in the Forrester Wave for XDR. URL: https://www.microsoft.com/en-us/security/blog/2024/06/03/microsoft-is-named-a-leader-in-the-forrester-wave-for-xdr/ (дата звернення: 27.10.2024).

41. Microsoft. Microsoft Named as a Leader in Three IDC MarketScapes for Modern Endpoint Security. URL: https://techcommunity.microsoft.com/t5/security-compliance-and-identity/microsoft-named-as-a-leader-in-three-idc-marketscapes-for-modern/ba-p/4083116 (дата звернення: 27.10.2024).

42. MITRE Engenuity. Microsoft Evaluation - MenuPass & BlackCat Scenario. URL: https://attackevals.mitre-engenuity.org/results/managed-services?vendor=microsoft&evaluation=menupass-blackcat&scenario=1 (дата звернення: 27.10.2024).

43. CrowdStrike. CrowdStrike Named a Leader in XDR Q2 2024. URL: https://www.crowdstrike.com/en-us/press-releases/crowdstrike-named-a-leader-in-xdr-q2-2024/ (дата звернення: 27.10.2024).

44. CrowdStrike. Ranked First in Worldwide Modern Endpoint Security Market Share for Third Time. URL: https://www.crowdstrike.com/en-us/press-releases/crowdstrike-ranked-first-in-worldwide-modern-endpoint-security-market-share-for-third-time/ (дата звернення: 27.10.2024).

45. AV-Comparatives. Endpoint Prevention & Response (EPR) Test - CrowdStrike 2024. URL: https://www.av-comparatives.org/wp-content/uploads/2024/09/EPR_CrowdStrike_2024.pdf (дата звернення: 27.10.2024).

46. MITRE Engenuity. CrowdStrike Evaluation - MenuPass & BlackCat Scenario. URL: https://attackevals.mitre-engenuity.org/results/managed-services?vendor=crowdstrike&evaluation=menupass-blackcat&scenario=1 (дата звернення: 27.10.2024).

47. Palo Alto Networks. Forrester Names Palo Alto Networks a Leader in XDR. URL: https://www.paloaltonetworks.com/blog/2024/06/forrester-names-palo-alto-networks-a-leader-in-xdr/ (дата звернення: 27.10.2024).

48. AV-Comparatives. Endpoint Prevention & Response (EPR) Test - Palo Alto Networks 2024. URL: https://www.av-comparatives.org/wp-content/uploads/2024/09/EPR_PaloAlto_2024.pdf (дата звернення: 27.10.2024).

49. MITRE Engenuity. Palo Alto Networks Evaluation - MenuPass & BlackCat Scenario. URL: https://attackevals.mitre-engenuity.org/results/managed-services?vendor=paloaltonetworks&evaluation=menupass-blackcat&scenario=1 (дата звернення: 27.10.2024).

50. Microsoft. Microsoft Defender for Endpoint. URL: https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-endpoint (дата звернення: 01.11.2024).

51. Microsoft. Microsoft Defender for Endpoint - MTE Overview. URL: https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint#mte (дата звернення: 01.11.2024).

52. Microsoft. Defender Vulnerability Management. URL: https://learn.microsoft.com/en-us/defender-vulnerability-management/defender-vulnerability-management (дата звернення: 01.11.2024).

53. Microsoft. Overview of Attack Surface Reduction Capabilities. URL: https://learn.microsoft.com/en-us/defender-endpoint/overview-attack-surface-

reduction (дата звернення: 01.11.2024).

54. Microsoft. Next-Generation Protection in Microsoft Defender for Endpoint. URL: https://learn.microsoft.com/en-us/defender-endpoint/next-generation-protection (дата звернення: 01.11.2024).

55. Microsoft. Overview of Endpoint Detection and Response Capabilities. URL: https://learn.microsoft.com/en-us/defender-endpoint/overview-endpoint-detection-response (дата звернення: 02.11.2024).

56. Microsoft. Automated Investigations in Microsoft Defender for Endpoint. URL: https://learn.microsoft.com/en-us/defender-endpoint/automated-investigations (дата звернення: 02.11.2024).

57. Microsoft. Endpoint Attack Notifications in Defender for Endpoint. URL: https://learn.microsoft.com/en-us/defender-endpoint/endpoint-attack-notifications (дата звернення: 02.11.2024).

58. Microsoft. Microsoft Defender for Endpoint. URL: https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-endpoint (дата звернення: 02.11.2024).

59. Microsoft. Microsoft Defender XDR. URL: https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-xdr (дата звернення: 02.11.2024).

60. Microsoft. What is Microsoft Defender for Identity. URL: https://learn.microsoft.com/en-us/defender-for-identity/what-is (дата звернення: 02.11.2024).

61. Microsoft. What is Microsoft Defender for Cloud Apps. URL: https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps (дата звернення: 02.11.2024).

62. Microsoft. Office 365 Advanced Threat Protection Service Description. URL: https://learn.microsoft.com/en-us/office365/servicedescriptions/office-365-

advanced-threat-protection-service-description (дата звернення: 02.11.2024).

63. CrowdStrike. Falcon Insight Data Sheet. URL: https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf (дата звернення: 04.11.2024).

64. CrowdStrike. Endpoint Security Platform. URL: https://www.crowdstrike.com/platform/endpoint-security/?srsltid=AfmBOopq0xEalit3XCXJltxSZuizvfDOgy_NU5PvThivTMdiA8eYgFGC (дата звернення: 04.11.2024).

65. IITD. CrowdStrike Falcon Platform - Всі модулі. URL: https://iitd.com.ua/ru/solutions/crowdstrike-falcon-platform-vsi-moduli/ (дата звернення: 04.11.2024).

66. CrowdStrike. Falcon Prevent NGAV. URL: https://www.crowdstrike.com/platform/endpoint-security/falcon-prevent-ngav/?srsltid=AfmBOoroAF3GPH-5xysdudaP5A1MjliTkoJIEKvcPCiucOSVUD-dUBM0 (дата звернення: 04.11.2024).

67. CrowdStrike. Falcon XDR Data Sheet. URL: https://crowdstrike-iitd.io/wp-content/uploads/2023/06/falcon-xdr-data-sheet-ru.pdf (дата звернення: 04.11.2024).

68. CrowdStrike. Falcon Device Control. URL: https://www.crowdstrike.com/platform/endpoint-security/falcon-device-control/?srsltid=AfmBOorfs197sYcUIaQFQdGgwRvkcn86EPHWvcFfqzaraUJRxvo4RCZ8 (дата звернення: 04.11.2024).

69. Palo Alto Networks. Cortex XDR Datasheet. URL: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/cortex-xdr (дата звернення: 04.11.2024).

70. Palo Alto Networks. Cortex XDR Overview. URL: https://www.paloaltonetworks.com/cortex/cortex-xdr (дата звернення: 04.11.2024).

71. Microsoft Defender Experts for XDR. Summary Incident Report: Purple Typhoon Activity Affecting MITRE Engenuity. (дата звернення: 14.10.2024)

72. Trio. Endpoint Detection and Response. URL: https://www.trio.so/blog/endpoint-detection-and-response/ (дата звернення: 07.11.2024).

73. Palo Alto Networks. Cortex XDR. URL: https://www.paloaltonetworks.com/cortex/cortex-xdr (дата звернення: 07.11.2024).

74. Palo Alto Networks. What is EDR Deployment. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-edr-deployment (дата звернення: 07.11.2024).

75. Trio. Endpoint Detection and Response. URL: https://www.trio.so/blog/endpoint-detection-and-response/ (дата звернення: 07.11.2024).

76. WatchGuard. What is the Difference Between Traditional Antivirus and EDR? URL: https://www.watchguard.com/wgrd-news/blog/what-difference-between-traditional-antivirus-and-edr (дата звернення: 07.11.2024).

77. Cybriant. Antivirus vs. EDR. URL: https://cybriant.com/2019/07/16/antivirus-vs-edr/ (дата звернення: 07.11.2024).

78. ThiefDroppers. EDR vs. Traditional Antivirus for Endpoint Security. URL: https://www.thiefdroppers.com/blogs/edr-vs-traditional-antivirus-for-endpoint-security (дата звернення: 07.11.2024).

79. Amiseq. How Do Traditional Antivirus Solutions Differ from EDR? URL: https://amiseq.com/how-do-traditional-antivirus-solutions-differ-from-edr/ (дата звернення: 07.11.2024).

80. Office1. Traditional Antivirus vs. EDR vs. Next-Gen Antivirus. URL: https://www.office1.com/blog/traditional-antivirus-vs-edr-vs-next-gen-antivirus (дата звернення: 07.11.2024).

81. Turrito. Traditional Antivirus vs. EDR - Endpoint Detection and Response. URL: https://www.turrito.com/traditional-antivirus-vs-edr-endpoint-detection-and-response/ (дата звернення: 07.11.2024).

82. Weida Gang. Demystifying Anomaly Detection with Autoencoder Neural Networks. URL: https://medium.com/@weidagang/demystifying-anomaly-detection-with-autoencoder-neural-networks-1e235840d879 (дата звернення: 01.12.2024).

83. Ju Rabikumarsingh. Anomaly Detection: Isolation Forest in 5 Min. URL: https://medium.com/@ju.rabikumarsingh/anomaly-detection-isolation-forest-in-5-min-1902a16dd1fc (дата звернення: 01.12.2024).

84. Spot Intelligence. Anomaly Detection with One-Class SVM. URL: https://spotintelligence.com/2024/05/27/anomaly-detection-one-class-svm/ (дата звернення: 01.12.2024).

85. Roshmita Dey. Anomaly Detection Using Support Vectors. URL: https://medium.com/@roshmitadey/anomaly-detection-using-support-vectors-2c1b842213ed#:~:text=One%2DClass%20Support%20Vector%20Machine,data%20is%20available%20for%20training (дата звернення: 01.12.2024).

86. Insights2TechInfo. Random Forest's Impact on Real-Time Phishing Defence. URL: https://insights2techinfo.com/random-forests-impact-on-real-time-phishing-defence/ (дата звернення: 01.12.2024).

87. Insights2TechInfo. Leveraging Logistic Regression for Phishing Threat Identification. URL: https://insights2techinfo.com/leveraging-logistic-regression-for-phishing-threat-identification-3/ (дата звернення: 01.12.2024).

88. Arnab Saha. K-Means Cluster and Its Use Case in Cyber Security. URL: https://arnabsaha1.medium.com/k-means-cluster-and-its-use-case-in-cyber-security-3abfaab2ec09 (дата звернення: 01.12.2024).

89. BuiltIn. DBScan Algorithm Overview. URL: https://builtin.com/articles/dbscan (дата звернення: 01.12.2024).

90. Maizi. Long Short-Term Memory (LSTM) Algorithm. URL: https://medium.com/@maizi5469/long-short-term-memory-lstm-algorithm-in-651a2942ae46 (дата звернення: 01.12.2024).

91. Palak V. Hidden Markov Model in Machine Learning. URL: https://medium.com/@palakvb02/hidden-markov-model-in-machine-learning-a744ada52166 (дата звернення: 01.12.2024).

92. DataScientest. Q-Learning: Machine Learning with Reinforcement Learning. URL: https://datascientest.com/en/q-learning-machine-learning-with-reinforcement-learning (дата звернення: 01.12.2024).

93. GeeksForGeeks. Q-Learning in Python. URL: https://www.geeksforgeeks.org/q-learning-in-python/ (дата звернення: 01.12.2024).

94. Shruti Dhumne. Deep Q-Network (DQN). URL: https://medium.com/@shruti.dhumne/deep-q-network-dqn-90e1a8799871 (дата звернення: 01.12.2024).

95. Danushi DK. PPO Algorithm. URL: https://medium.com/@danushidk507/ppo-algorithm-3b33195de14a (дата звернення: 01.12.2024).

96. Amul Dhungel. K-Nearest Neighbors Algorithm in Cybersecurity: Detecting Malware. URL: https://medium.com/@amuldhungel01/ml-4-k-nearest-neighbors-algorithm-in-cybersecurity-detecting-malware-d559a7ed3822 (дата звернення: 01.12.2024).

97. GeeksForGeeks. K-Nearest Neighbours Algorithm Overview. URL: https://www.geeksforgeeks.org/k-nearest-neighbours/ (дата звернення: 01.12.2024).

98. GeeksForGeeks. Introduction to Convolutional Neural Network (CNN). URL: https://www.geeksforgeeks.org/introduction-convolution-neural-network/ (дата звернення: 01.12.2024).

99. DataCamp. Multilayer Perceptrons in Machine Learning. URL:

https://www.datacamp.com/tutorial/multilayer-perceptrons-in-machine-learning (дата звернення: 01.12.2024).

100. GeeksForGeeks. What are Graph Neural Networks (GNN). URL: https://www.geeksforgeeks.org/what-are-graph-neural-networks/ (дата звернення: 01.12.2024).

101. AWS. What is a Recurrent Neural Network (RNN)? URL: https://aws.amazon.com/ru/what-is/recurrent-neural-network/ (дата звернення: 01.12.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

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

Кваліфікаційна робота на тему:

«Технологія захисту кінцевих точок організацій від шкідливого програмного забезпечення на основі машинного навчання та штучного інтелекту»

Виконав: студент групи БСДМ-62 МИРОНОВ Вадим
Керівник: к.т.н., доцент ВЛАСЕНКО В.О.

1

Мета роботи – дослідити вплив використанням штучного інтелекту в системах захисту кінцевих точок для протидії кіберзагрозам, надати висновки та рекомендації щодо впровадження цих систем.

Предмет дослідження – EPP, EDR та XDR рішення, що використовують штучний інтелект для захисту кінцевих точок.

Об'єкт дослідження – дослідження впливу штучного інтелекту на ефективність сучасних систем захисту кінцевих точок.

Наукові завдання:

проаналізувати сучасні дослідження та наукову літературу на предмет доцільності застосування штучного інтелекту в системах захисту кінцевих точок;

порівняти ефективність традиційних систем та сучасних в яких використовується штучний інтелект;

отримати практичні результати протидії загрозам за допомогою функцій комп'ютерного інтелекту впроваджених в системи захисту кінцевих точок;

проаналізувати алгоритми машинного навчання, які можуть використовуватись в сучасних технологіях захисту кінцевих точок;

надати рекомендації по впровадженню, вдосконаленню та адаптації організацій із використанням сучасних рішень захисту кінцевих точок.

2

Кінцеві точки, типи та загрози.

Кінцева точка - це фізичний пристрій, що підключений до мережі, в якій може обмінюватись інформацією.

Кінцеві пристрої надають користувачу доступ до внутрішньої комп'ютерної мережі та виходу в глобальну мережу інтернет для взаємодії із інформаційними ресурсами.

Типи кінцевих точок:

1. *Обчислювальні пристрої* - має обчислювальні потужності та допомагає виконувати операції обробки даних. Допомагає взаємодіяти із додатками для виконання роботи. Кінцеві пристрої надають користувачу доступ до внутрішньої комп'ютерної мережі та виходу в глобальну мережу інтернет для взаємодії із інформаційними ресурсами.
2. *Периферійні пристрої* - виконують роль допоміжних пристроїв, які забезпечують додаткову функціональність: ввід/вивід інформації та виконання нескладних функціональних обов'язків.

1. Фішинг
2. Програми-вимагачі
3. Атаки нульового дня
4. Відсутність оновлень програмного забезпечення
5. Слабкі паролі або слабкі політики безпеки
6. Підключення небезпечних USB
7. Крадіжка або втрата пристрою
8. Ненадійне програмне забезпечення
9. Інсайдерська загроза

3

Базові поняття штучного інтелекту

Штучний інтелект - це технічна та наукова галузь, присвячена спроектованій системі, яка генерує вихідні дані, такі як зміст, прогнози, рекомендації або рішення для певного набору цілей, визначених людиною. Генеративний штучний інтелект відрізняється від традиційного сферами застосування та задачами, де його можна застосовувати. Традиційний штучний інтелект в основному знаходить своє використання в аналізі даних та прогнозуванні. Сучасна система штучного інтелекту, яка побудована на генеративному ШІ - створює нові дані.

Data Science – це наука, яка розповідає про методи аналізу та вилучення цінної інформації із даних. Дана наука має взаємозв'язок із іншими галузями, такими як: наука про мислення, машинне навчання та робота із великими масивами даних. Дані проходять етапи обробки та підготовки для того, що в подальшому на них можна було навчити алгоритм виконувати певні задачі.

Machine Learning - можна виділити як підмножину штучного інтелекту, але це також є наука о розробці алгоритмів, які здатні навчатись на основі великих обсягів даних без потреби налаштовувати та програмувати кожне рішення. Алгоритм знаходить закономірності та патерни в інформації, які надаються для навчання. Основна суть полягає в тому, що замість програмування кожного сценарію під окремі задачі, можна зробити щоб модель сама навчалась на тих даних, які їй були надані.

Ключові параметри для ефективного навчання моделі [4]:

Дані – це базова інформація, дані, на яких потрібно навчати систему. Дані не повинні містити помилки, так як це може погано вплинути на модель, яка навчається. Тому варто добре структурувати та обробляти дані, для отримання більш релевантних відповідей та точних прогнозів.

Ознаки – це конкретна характеристика даних, яку використовують для навчання моделі. Від правильних ознак залежить точність моделі. Чи більше інформативними є ознаки, тим краще модель зможе розпізнавати закономірності та робити прогнози.

Алгоритм – це інструкція або послідовність дій для вирішення задачі. Від алгоритму залежить, які математичні операції будуть виконуватись для досягнення результату. Алгоритм впливає на ефективність навчання моделі, обробку даних та прогнозування.

Види машинного навчання:

Навчання із вчителем – підхід навчання моделі із використанням мічених даних, де мітка може позначати правильну відповідь. Обраний об'єкт буде поміченний правильно для того, щоб вона навчилась розпізнавати об'єкт в майбньому;

Навчання без вчителя – підхід навчання моделі де відсутні мітки. Модель вивчає подібності в даних. Вона самостійно знаходить структуру без необхідності їх помічати. Метод використовується при кластеризації даних або виявлення аномалій;

Навчання з підкріпленням – підхід до навчання побудований на основі винагород та покарань за свої дії. Цей підхід має популярність у динамічних середовищах: ігри або автономне керування транспортом.

Алгоритми машинного навчання

Дана аблиця є узагальненням ключових алгоритмів машинного навчання, що застосовуються в кібербезпеці. Вона демонструє типи алгоритмів, їхні основні функції та особливості використання для виявлення, аналізу та реагування на загрози. Представлені алгоритми охоплюють широкий спектр методів: від виявлення аномалій та класифікації загроз до прогнозування атак і автоматизації реагування. Таблиця дозволяє зрозуміти, як кожен з алгоритмів працює та які завдання він вирішує у контексті забезпечення інформаційної безпеки.

Алгоритм	Тип	Застосування в кібербезпеці	Опис
Автоенкодер	Нейронна мережа (без учителя)	Виявлення аномалій, зменшення розмірності, видалення шуму	Стискає та відновлює дані, виявляючи аномалії за великою похибкою реконструкції.
Isolation Forest	Алгоритм машинного навчання (без учителя)	Виявлення аномалій	Ізолює аномалії шляхом випадкового поділу даних.
One-Class SVM	Алгоритм машинного навчання (без учителя)	Виявлення аномалій	Створює гіперплощину, що охоплює нормальні дані, аномалії знаходяться поза нею.
Random Forest	Алгоритм машинного навчання (з учителем)	Захист від фішингу, класифікація загроз	Ансамбль дерев рішень для підвищення точності прогнозів.
SVM	Алгоритм машинного навчання (з учителем)	Виявлення аномалій, класифікація	Розділяє дані на класи за допомогою гіперплощини.
Логістична регресія	Статистичний метод	Ідентифікація фішингових загроз	Оцінює ймовірність належності об'єкта до одного з двох класів.
CNN	Нейронна мережа	Виявлення шкідливого ПЗ, ідентифікація фішингових веб-сайтів	Аналізує зображення та структуровані дані.
MLP	Нейронна мережа	Класифікація електронних листів, аналіз лог-файлів	Базова архітектура нейронних мереж для класифікації та регресії.
K-means	Алгоритм кластеризації (без учителя)	Виявлення аномалій, класифікація шкідливого ПЗ	Розділяє дані на кластери на основі схожості.
DBSCAN	Алгоритм кластеризації (без учителя)	Виявлення аномалій в мережевому трафіку	Групує точки даних на основі їхньої щільності.
GNN	Нейронна мережа	Аналіз мережевого трафіку, виявлення аномалій	Працює з графовими даними, враховуючи взаємозв'язки між об'єктами.
LSTM	Нейронна мережа	Виявлення аномалій, прогнозування атак	Аналізує послідовності даних, виявляючи довготривалі залежності.
HMM	Статистична модель	Аналіз послідовностей дій, прогнозування загроз	Моделює систему через послідовність прихованих станів.
Q-Learning	Алгоритм навчання з підкріпленням	Автоматизація реагування на загрози	Навчає агента оптимальним діям на основі винагороди.
DQN	Алгоритм навчання з підкріпленням	Автоматизація реагування на загрози	Поєднує Q-Learning з нейронними мережами.
PPO	Алгоритм навчання з підкріпленням	Автоматизація реагування на загрози	Оптимізує дії агента, зберігаючи стабільність.
KNN	Алгоритм машинного навчання (з учителем)	Виявлення шкідливого ПЗ, аналіз мережевого трафіку	Класифікує об'єкти на основі схожості з найближчими сусідами.
RNN	Нейронна мережа	Аналіз мережевих логів, виявлення патернів атак	Працює з послідовними даними, враховуючи контекст у часі.

Еволюція систем захисту кінцевих точок

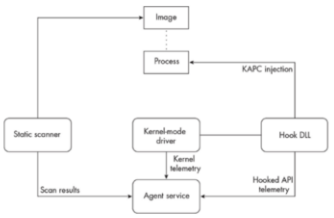
Роки	Методи, що використовуються в EDR
2005-2010	Виявлення за сигнатурами, евристичне виявлення, аналіз журналів, системи виявлення вторгнень на основі хостів (HIDS), брандмауери та антивірусне програмне забезпечення, ручне реагування на інциденти, візуалізація дисків і криміналістика, шифрування кінцевих точок, контроль на основі політик.
2011-2015	Поведінковий аналіз, експертиза пам'яті, аналіз мережевого трафіку, виявлення індикаторів компрометації (IoC), евристичні виявлення, пісочниця, виявлення аномалій.
2016-2020	Машинне навчання та аналіз поведінки, ізоляція кінцевих точок, хмарні рішення EDR, виявлення шкідливих програм без файлів, технології обману, безпека кінцевих точок IoT та OT, аналіз поведінки користувачів та організацій (UEBA), інтеграція API (інтерфейсу додатків та програмування) та обмін потоковою аналітикою.
2021-2023	Розширене виявлення та реагування (XDR), архітектура нульової довіри, виявлення потоків на основі штучного інтелекту (ШІ)[7][8], захист на основі аналізу загроз, поведінкова біометрія, хмарні рішення EDR, автоматизоване реагування на інциденти, інтеграція екосистем.

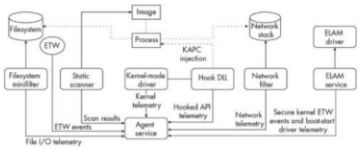
Архітектура системи захисту кінцевих точок

Система захисту кінцевих точок (EDR): серверна частина та агенти

Серверна частина EDR
Сервер є центральним елементом системи EDR, який може бути розгорнутий локально або в хмарі залежно від потреб організації. Він отримує телеметричні дані від агентів для аналізу, виявлення загроз та централізованого управління кінцевими точками. Сервер забезпечує:

Агенти EDR
Агенти встановлюються на кінцеві точки для моніторингу їхньої активності, збору телеметрії та передачі її на сервер. Вони працюють на рівні операційної системи.
Типи агентів:
1.Базовий агент - базовий моніторинг з обмеженим функціоналом.
2.Проміжний агент - більш широкий аналіз для середніх організацій.
3.Розширений агент - повний функціонал для великих організацій.





7

Вибір виробника системи захисту

Forrester - є однією з провідних дослідницьких фірм, яка зосереджена на наданні стратегічних рекомендацій для бізнесів у галузі цифрових технологій

Gartner - це провідна дослідницька компанія, яка спеціалізується на наданні стратегічних досліджень, консультацій і об'єктивних оглядів на основі глибокого аналізу ринку

MITRE ATT&CK Evaluations - це тестування кібербезпекових продуктів на основі фреймворку *MITRE ATT&CK*, який моделює методи, що використовують хакери на різних етапах атаки.

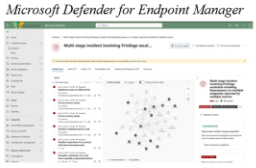
AV-Comparatives - це незалежна організація, яка спеціалізується на тестуванні рішень для кібербезпеки, зокрема антивірусних продуктів.

IDC одна з провідних світових компаній, що спеціалізується на проведенні досліджень, аналізі ринків та наданні консультацій у сфері інформаційних технологій

8

Ознайомлення з функціональними можливостями систем захисту кінцевих точок із застосуванням технологій штучного інтелекту

Microsoft Defender for Endpoint Manager

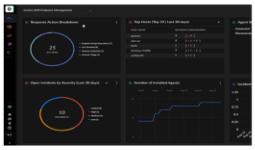


1. *Базове управління вразливістю Defender*
2. *Скорочення напрямів атак*
3. *Захист наступного покоління*
4. *Виявлення та нейтралізація атак на кінцеві точки*
5. *Автоматичне дослідження та виправлення*
6. *Експерти «Майкрософт» із загроз*

CrowdStrike Falcon EDR

1. *Автоматизоване виявлення загроз*
2. *Повноцінне дослідження інцидентів*
3. *Реагування в режимі реального часу*
4. *Хмарна платформа*
5. *Аналіз поведінки користувачів*
6. *Інтеграція з Falcon Platform*

Palo Alto Cortex XDR



1. *Повна видимість середовища*
2. *Виявлення загроз за допомогою машинного навчання*
3. *Глобальна аналітика*
4. *Швидке дослідження*
5. *Автоматизація через Cortex XSOAR*

Microsoft Defender for Endpoint Manager
Ця платформа використовує засоби штучного інтелекту для виявлення багатоступеневих атак і автоматизації реагування. Завдяки інтеграції з Microsoft 365 і Azure, Defender застосовує поведінковий аналіз та машинне навчання для ідентифікації загроз, нейтралізації атак на кінцеві точки та оптимізації вразливостей. Інструменти автоматичного дослідження та рекомендації від експертів Microsoft забезпечують швидку й ефективну обробку інцидентів.

CrowdStrike Falcon EDR
Falcon EDR використовує штучний інтелект для автоматизованого виявлення загроз і прогнозування ризиків. Завдяки поведінковому аналізу, платформа може аналізувати дії користувачів і пристроїв у реальному часі, що дозволяє зупиняти складні атаки до їхнього розгортання. Інтеграція з Falcon Platform дозволяє об'єднувати дані з різних джерел, що підсилює аналіз і робить реагування швидким і точним.

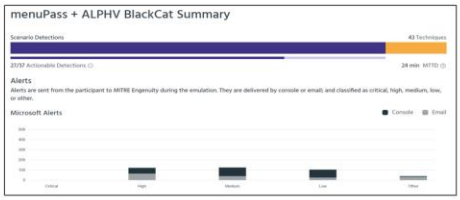
Palo Alto Cortex XDR
Cortex XDR використовує алгоритми машинного навчання для аналізу великих обсягів телеметрії, що допомагає ідентифікувати навіть складні атаки. Завдяки глобальній аналітиці, платформа забезпечує повну видимість середовища та швидке дослідження інцидентів. Інтеграція з Cortex XSOAR дозволяє автоматизувати реагування та координацію між командами безпеки, забезпечуючи адаптивність до нових загроз у реальному часі.

9

Практичне дослідження функціональних можливостей систем захисту кінцевих точок із застосуванням технологій штучного інтелекту (Часть 1)

Фіолетова смуга: показує загальну кількість виявлених сценаріїв атак.
Жовта смуга: відображає кількість технік атак, використаних у цих сценаріях.
Світло-фіолетова смуга: вказує на кількість сценаріїв, де система змогла зреагувати/
Actionable Detections: 27 з 37 виявлених сценаріїв були "actionable", тобто система не тільки їх виявила, але й змогла на них відреагувати (наприклад, заблокувати або сповістити адміністратора).
MTTD: 24 хвилини - це середній час виявлення загрози (Mean Time To Detect).
Alerts: Гістограма показує кількість сповіщень (alert), згенерованих системою Microsoft Alerts під час тестування.
Сповіщення класифікуються за рівнем критичності: Critical, High, Medium, Low, Other. Темно-сірий колір показує кількість сповіщень, надісланих через консоль, а світло-сірий - через email.

Висновок про аналіз Microsoft XDR у межах MITRE ATT&CK Evaluation (MDR):
1.Ефективність виявлення: Microsoft XDR виявила 27 із 37 actionable detections (сценаріїв, на які можна реагувати).Було застосовано 43 техніки з ATT&CK, що підтверджує покриття різних методів атак.
2.Час виявлення: Середній час виявлення загрози (MTTD) становив 24 хвилини, що свідчить про високу швидкість реагування.
3.Класифікація сповіщень: Сповіщення були поділені за рівнями критичності, з акцентом на "High" та "Medium", що дозволяє операторам правильно розставляти пріоритети в реагуванні.
Загальна оцінка: Microsoft XDR показала сильні сторони у виявленні загроз, використовуючи машинне навчання та автоматизацію. Цей результат демонструє її здатність відповідати сучасним викликам кіберзагроз і надає аналітикам ефективні інструменти для реагування.



10

Практичне дослідження функціональних можливостей систем захисту кінцевих точок із застосуванням технологій штучного інтелекту (Часть 2)

День	Дії атакуючих	TTPs	Дії захисників	Опис роботи алгоритмів
12.02.2024	Зловмисники: Використовують скомпрометовані облікові дані для RDP-підключення. Встановлюють бекдор (з використанням PowerShell скрипту). Маскують свою активність під легітимний трафік.	T1078.002, T1059.003, T1218, T1574.001, T1056.001, T1071.001	Захисники: Виявляють аномалії у RDP-підключеннях (нетипова IP-адреса, час підключення). Аналізують мережевий трафік на наявність підозрілих патернів. Моніторять системні виклики для виявлення запуску шкідливих процесів.	За допомогою Isolation Forest та One-Class SVM виявлено аномалії у RDP-підключеннях. CNN та RNN використані для аналізу мережевого трафіку, а HMM - для моніторингу системних викликів.
13.02.2024	Зловмисники: Використовують Mimikatz для збору облікових даних. Переміщуються по мережі, використовуючи PsExec та WMI. Сканують мережу та збирають інформацію про систему.	T1053.005, T1003.003, T1005	Захисники: Блокують підозрілі мережеві з'єднання. Аналізують поведінку процесів на предмет аномалій. Виявляють та класифікують шкідливі домени.	Isolation Forest та One-Class SVM застосовані для виявлення аномалій у мережевому трафіку. Автоенкодери використані для аналізу поведінки, а Random Forest та SVM - для класифікації шкідливих доменів та блокування з'єднань.
14.02.2024	Зловмисники: Використовують Golden Ticket, Pass-the-Hash та Kerberoasting атаки для проникнення в новий домен. Встановлюють нові бекдори для збереження доступу. Приховують свою активність.	T1087.002, T1003.002	Захисники: Аналізують файли на наявність шкідливого коду. Кластеризують загрози для виявлення спільних патернів. Моніторять мережеву активність для виявлення аномалій.	CNN, MLP та RNN використані для статичного та динамічного аналізу файлів. K-Means та DBSCAN застосовані для кластеризації загроз, а GNN - для аналізу мережевої активності.
15.02.2024	Зловмисники: Використовують SQL ін'єкції для доступу до бази даних. Ексфільтрують дані з бази даних та файлового сервера. Використовують BITSAdmin для завантаження шкідливого ПЗ. Очищують журнали подій.	T1003.001, T1070.001, T1560.001	Захисники: Аналізують мережевий трафік на наявність підозрілих потоків даних. Виявляють аномалії у поведінці користувачів та системних утиліт. Моніторять налаштування безпеки на предмет змін.	HMM використаний для аналізу типових сценаріїв використання системних утиліт. One-Class SVM та Isolation Forest застосовані для виявлення аномалій у поведінці користувачів та налаштованих безпеки. Автоенкодери та LSTM використані для аналізу мережевого трафіку.
16.02.2024	Зловмисники: Запускають шифрувальник на комп'ютерах жертв. Вимагають викуп за розшифровку даних. Знищують резервні копії. Використовують SSH для доступу до критичних систем.	T1048.001, T1485, T1486, T1490, T1127, T1119	Захисники: Виявляють та блокують поширення шифрувальника. Аналізують мережеві з'єднання на наявність підозрілої активності. Відновлюють дані з резервних копій. Корелюють події для повного розуміння атаки.	LSTM та HMM використані для аналізу поведінки облікових записів. One-Class SVM та Random Forest застосовані для виявлення аномалій у мережевому трафіку. CNN та MLP використані для розпізнавання дій програм-вимагачів. Автоенкодери та GNN застосовані для кореляції подій та аналізу доступу SSH.

11

Технологія впровадження сучасних систем захисту кінцевих точок із штучним інтелектом

1. Вимоги та планування
На етапі вимог та планування важливо визначити, які саме потреби організації повинна задовольняти система. Серед основних аспектів — типи кінцевих точок, що потребують захисту, інтеграція нової системи з уже наявними засобами безпеки та управління, а також можливість автоматизації певних завдань за допомогою штучного інтелекту. Перед початком впровадження варто провести аудит кібербезпеки, щоб оцінити слабкі місця, рівень готовності організації до впровадження нових технологій та виявити потенційні вразливості, які можуть бути використані зловмисниками.

2. Пілотне розгортання
Пілотне розгортання є ключовим етапом, що дозволяє протестувати ефективність системи в реальних умовах. На цьому етапі рекомендується починати з обмеженої кількості кінцевих точок, щоб оцінити функції системи, такі як виявлення загроз, реагування та автоматизація процесів. Важливо залучити до процесу ключових стейкхолдерів, включаючи IT-відділ та команду кібербезпеки, для налаштування параметрів системи й забезпечення її сумісності з іншими компонентами. Паралельно потрібно підготувати план реагування на інциденти, що можуть виникати в процесі тестування.

3. Масштабування та налаштування політик
Після успішного завершення пілотного впровадження можна переходити до масштабування системи на всі кінцеві точки організації. На цьому етапі відбувається налаштування політик безпеки, які включають автоматичне блокування підозрілих дій і повідомлення про інциденти. Також налаштовуються правила виявлення та реагування на загрози з урахуванням специфіки роботи організації. Особливу увагу слід приділяти мінімізації хибнопозитивних спрацьовувань.

4. Вибір вендора для EDR/XDR систем
Вибір постачальника рішень EDR чи XDR є критично важливим для ефективного впровадження. Вендор повинен пропонувати систему, яка легко інтегрується з іншими інструментами безпеки, підтримує масштабування та забезпечує регулярне оновлення для адаптації до сучасних загроз. Важливим є технічне обслуговування, своєчасні оновлення та можливість протестувати систему в реальних умовах через пробний період або демо-версію. Це допоможе знизити ризики неправильного вибору та забезпечити відповідність рішення потребам організації.

5. Виклики при впровадженні EDR та XDR
Під час впровадження систем EDR та XDR організації можуть зіткнутися з низкою викликів. Зокрема, недостатня інтеграція з існуючими інструментами може знизити ефективність загальної системи безпеки. Використання AI може спричиняти фальшиві тривоги, які потребують ручної перевірки. Також впровадження таких систем вимагає наявності кваліфікованого персоналу, здатного ефективно працювати з новими технологіями. Подолання цих викликів можливе завдяки належному налаштуванню системи, адаптації під потреби організації та навчання фахівців.

6. Рекомендації для успішного впровадження
Важливо забезпечити підготовку персоналу до використання нових систем. Навчання має охоплювати як технічні аспекти для фахівців із кібербезпеки, так і підвищення обізнаності загального персоналу про актуальні загрози та правила безпеки. Навіть після впровадження системи необхідно постійно моніторити її ефективність, аналізувати журнали подій і проводити регулярні аудити для виявлення слабких місць і внесення коректив. Автоматизація рутинних завдань, таких як аналіз журналів подій і реагування на загрози, значно знижує навантаження на команди з кібербезпеки та скорочує час реагування. Це допомагає зосередитися на складніших інцидентах і мінімізувати потенційні наслідки загроз.

12

Пропозиція щодо покращення традиційних рішень шляхом впровадження сучасних технологій

Ключові напрями вдосконалення антивірусних рішень

1.Інтеграція поведінкового аналізу: Поведінковий аналіз допомагає виявляти аномалії в роботі систем, запобігаючи Zero-Day атакам та складним загрозам, які традиційні рішення не можуть визначити.

2.Автоматизація реагування: Сучасні системи EDR автоматично ізолюють інфіковані кінцеві точки, що прискорює реагування та знижує ризики помилок через людський фактор.

3.Централізоване управління та кореляція подій: Збір і аналіз даних із кінцевих пристроїв дозволяють ідентифікувати складні атаки та забезпечувати більшу видимість загроз.

4.Підтримка хмарних середовищ: Інтеграція з хмарними платформами забезпечує контроль над кінцевими точками незалежно від їхнього місцезнаходження.

5.Постійний моніторинг та аналітика: Постійний моніторинг із використанням ШІ та алгоритмів машинного навчання дозволяє виявляти приховані загрози та швидко реагувати на інциденти.

6.Навчання користувачів: Підвищення обізнаності користувачів про загрози та правила безпеки допомагає зменшити ризики, пов'язані з соціальною інженерією.

7.Інструменти штучного інтелекту: ШІ аналізує великі обсяги даних, виявляє аномалії та приймає рішення щодо нейтралізації загроз, підвищуючи ефективність захисту.

8.Інтеграція з іншими продуктами безпеки: Зв'язок із фаєрволами, SIEM та засобами аналізу мережевого трафіку створює багаторівневий захист і покращує взаємодію систем.

9.Розширення можливостей реагування на інциденти: Інструменти EDR дозволяють глибше аналізувати причини інцидентів і розробляти заходи для їх запобігання в майбутньому.

Параметр	Традиційні рішення	Сучасні рішення
Метод виявлення загроз	Сигнатурний аналіз	Поведінковий аналіз, AI, машинне навчання
Тип загроз	Тільки відомі загрози	Відомі, невідомі, Zero-Day загрози
Моніторинг системи	Переважно періодичне сканування	Постійний моніторинг у реальному часі
Здатність до кореляції подій	Відсутня	Є можливість кореляції подій між різними кінцевими точками
Реагування на інциденти	Переважно вручну	Автоматизоване реагування, ізоляція загроз, сценарії усунення (playbooks)
Орієнтація захисту	Охоплення тільки окремих кінцевих точок	Глобальний захист з інтеграцією даних між всіма кінцевими точками
Захист від атак Zero-Day	Обмежений	Розширений захист за допомогою поведінкового аналізу та машинного навчання
Автоматизація процесів	Відсутня	Високий рівень автоматизації: від виявлення загроз до їх усунення
Обмін даними між компонентами	Локальний, обмежений	Централізований обмін даними між всіма компонентами системи
Інтеграція з іншими засобами безпеки	Обмежена	Розширена інтеграція з фаєрволами, мережевими аналізаторами, SIEM тощо
Робота в гібридних середовищах	Обмежена	Підтримка як локальних, так і хмарних середовищ
Швидкість реагування на загрозу	Може бути уповільненою через ручну взаємодію	Миттєва завдяки автоматизованим механізмам реагування
Аналітика та звітність	Основні звіти, мало інформації для аналізу	Детальна аналітика подій, глибокий аналіз причин загрози
Підхід до захисту	Реактивний (реагування після виявлення загрози)	Проактивний (виявлення та запобігання на основі аналізу поведінки та прогностичних моделей)

Рекомендації щодо адаптації технологій під потреби організацій

1. Малі організації
Особливості: Обмежені ресурси, невелика кількість кінцевих точок.
Рішення:
1. Хмарні рішення з антивірусом;
2. Автоматизація (playbooks);
3. Комплексні антивірусні рішення.

Рекомендації: Єдиний провайдер безпеки, автоматичні оновлення, базові політики доступу.

2. Середні організації
Особливості: Більша кількість кінцевих точок, розподілена інфраструктура.
Рішення:
1. EDR для моніторингу;
2. Інтеграція систем захисту;
3. Управління мобільними пристроями.

Рекомендації: Централізоване управління, навчання фахівців, сегментація мережі.

3. Великі організації
Особливості: Складна інфраструктура, високі вимоги до безпеки.
Рішення:
1. XDR для координації захисту;
2. MSSP (зовнішні сервіси моніторингу);
3. Багатофакторна автентифікація, сегментація мережі.

Рекомендації: Створення SOC, поведінковий аналіз, навчання та пентести.

Висновки

Висновок дипломної роботи узагальнює основні результати дослідження впливу штучного інтелекту на системи захисту кінцевих точок та їх ефективність у протидії сучасним кіберзагрозам. Дослідження показало, що зі зростанням складності загроз, новими підходами та тактиками атаки, традиційні засоби захисту, такі як антивірусні програми, більше не можуть забезпечити необхідний рівень безпеки. Постало питання про необхідне використання нових підходів, зокрема впровадження систем на основі штучного інтелекту.

Штучний інтелект забезпечує проактивний захист, який дозволяє не лише виявляти та реагувати на загрози, а й запобігати їх виникненню завдяки прогнозуванню на основі аналізу поведінкових патернів. В якості переваги сучасних систем захисту, таких як XDR (розширене виявлення та реагування), можна зазначити здатність збирати й аналізувати дані з різних джерел, включаючи кінцеві точки, мережевий трафік та хмарні ресурси. Завдяки використанню алгоритмів машинного навчання та глибокого навчання ці системи здатні самонавчатись, аналізуючи попередній досвід для покращення реакції на загрозу, що значно підвищує їхню ефективність у виявленні нових типів атак, таких як атаки нульового дня або безфайлові загрози.

Протягом еволюції технологій захисту кінцевих точок від статичних антивірусних систем до сучасних рішень на основі ШІ, було відмічено кілька ключових етапів. Спершу використовувались підходи на основі сигнатур, що були ефективними лише для вже відомих загроз. Наступним етапом стало впровадження евристичного аналізу, який дозволив виявляти загрози на основі аналізу підозрілих інструкцій та структур коду. З розвитком кіберзлочинності виникла необхідність застосовувати більш вдосконалені методи, такі як поведінковий аналіз, виявлення аномалій та ізоляція кінцевих точок. У цьому контексті особливу роль відіграли системи EDR (виявлення та реагування на кінцевих точках), які почали активно використовувати алгоритми машинного навчання для підвищення точності виявлення загроз.

Сучасні рішення, такі як Microsoft Defender, Palo Alto Cortex XDR та CrowdStrike Falcon, які були проаналізовані в роботі, є прикладами ефективного впровадження штучного інтелекту в системи захисту. Вони не лише забезпечують базовий захист від загроз, а й використовують інтелектуальні алгоритми для автоматизації реагування на інциденти, що значно зменшує час реагування на загрози та мінімізує вплив людського фактора.

Також важливо відзначити розвиток хмарних рішень для захисту кінцевих точок, які дозволяють централізовано керувати безпекою великої кількості пристроїв, що особливо актуально у зв'язку зі зростанням популярності віддаленої роботи. Хмарні технології захисту забезпечують масштабованість, гнучкість і доступність, що робить їх популярним вибором для сучасних організацій. Крім того, можна зазначити, що впровадження архітектури нульової довіри (Zero Trust Architecture) посилило підхід до безпеки, де кожна взаємодія має бути підтверджена незалежно від її походження.

Проведений аналіз підтвердив, що впровадження систем захисту кінцевих точок із застосуванням штучного інтелекту є доцільним і необхідним кроком для забезпечення ефективної кібербезпеки сучасних організацій. Такого роду системи мають високу адаптивність до змінних загроз, що особливо важливо в умовах постійного зростання складності та кількості атак. Використання систем ШІ дозволяє створити комплексну систему безпеки, яка може не тільки виявляти та усувати загрози, а й навчатися на попередньому досвіді для запобігання майбутнім інцидентам.

На основі результатів дослідження можна надати рекомендації щодо впровадження сучасних систем захисту кінцевих точок із застосуванням технологій штучного інтелекту. Компаніям варто оцінити наявні загрози та обрати систему, яка найбільше відповідає їхнім потребам. Наступним кроком важливо забезпечити інтеграцію таких систем із іншими засобами кібербезпеки, такими як SIEM або IAM, для підвищення ефективності реагування на інциденти. На останок варто зауважити про необхідність забезпечити постійне навчання моделей ШІ на актуальних даних, що дозволить підвищити точність виявлення загроз та зменшити кількість хибних спрацьовувань.

Таким чином, впровадження штучного інтелекту в системи захисту кінцевих точок є важливим кроком для забезпечення надійної та ефективної кібербезпеки. Використання сучасних рішень на основі ШІ дозволяє створити проактивний підхід до захисту, який відповідає викликам сучасного кіберпростору та забезпечує високий рівень безпеки для організацій різного масштабу. Подальший розвиток технологій захисту кінцевих точок та впровадження інноваційних рішень на основі ШІ допоможуть знизити ризики кібератак і забезпечити стабільну роботу бізнесу в умовах зростаючих кіберзагроз.