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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія виявлення та реагування на загрози на основі Trend Vision One»

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

_____ Ярослав Терно
(підпис)

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

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

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

Київ 2024

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

Терно Ярославу Анатолійовичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: «Технологія виявлення та реагування на загрози на основі Trend Vision One»

керівник кваліфікаційної роботи МАРЧЕНКО Віталій Вікторович, д.ф.
(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
інформаційні ресурси;
рішення Trend Vision One;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1.Дослідження проблеми виявлення та реагування на загрози

2.Аналіз методів та засобів виявлення та реагування на загрози на основі Trend Vision One

3. Технологія виявлення та реагування на загрози

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми	01.10.2024 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	12.10.2024 р.	
3.	Аналіз методів та засобів виявлення та реагування на загрози на основі Trend Vision One	27.10.2024 р.	
4.	Технологія виявлення та реагування на загрози	03.11.2024 р.	
5.	Розроблення рекомендацій щодо застосування технології виявлення та реагування на загрози на основі Trend Vision One	15.11.2024 р.	
6.	Оформлення результатів дослідження.	26.11.2024 р.	
7.	Підготовка доповіді до захисту.	15.12.2024 р.	

Здобувач вищої освіти _____ Ярослав Терно
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Терно Ярослав
на тему: «Технологія виявлення та реагування на загрози на основі Trend Vision One»

Актуальність: У сучасних умовах стрімкого зростання кількості та складності кіберзагроз, забезпечення ефективного виявлення та своєчасного реагування є ключовим завданням для організацій. Системи кіберзахисту, такі як Trend Vision One, дозволяють не лише автоматизувати процеси моніторингу безпеки, але й підвищити точність виявлення загроз за допомогою сучасних технологій штучного інтелекту та машинного навчання. Їх використання є актуальним для захисту критичної інфраструктури, запобігання витокам даних та зменшення часу реакції на інциденти.

Необхідно зауважити, що впровадження та застосування платформ кібербезпеки, таких як Trend Vision One, дозволяє ефективно виявляти загрози та оперативно на них реагувати, забезпечуючи надійний захист інформації.. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу в роботі було визначено основні сучасні виклики та типи загроз.
2. Досліджено методи та засоби забезпечення кібербезпеки на базі Trend Vision One, що дозволяє ефективно реагувати на виклики сучасних загроз.
3. Розглянуто зміст технології та рекомендації щодо її застосування. технологію виявлення та реагування на загрози за допомогою платформи Trend Vision One, а також наведено рекомендації щодо її застосування.
4. Текст роботи викладено чітко та послідовно, висновки є змістовними, графічний матеріал оформлено якісно. Список використаної літератури демонструє вміння працювати з актуальними джерелами за тематикою дослідження.

Недоліки:

1. У роботі варто було б провести аналіз можливих умов функціонування засобу багатовимірного візуального аналізу Trend Vision One у взаємодії з різними інформаційними системами.
2. Експеримент із застосуванням рішення Trend Vision One бажано провести на вихідних даних, які відображають конкретну кіберзагрозу.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**відмінно»**, а здобувач **Терно Ярослав** - присвоєння кваліфікації магістр з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Рецензент:

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

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИРис

Направляється здобувач Терно Ярослав 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: на тему: «Технологія виявлення та реагування на загрози на основі Trend Vision One».
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач ***Терно Ярослав*** обрав тему роботи, метою якої було дослідити технологію виявлення та реагування на загрози за допомогою платформи Trend Vision One. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***Терно Ярослав*** 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 ***Терно Ярослав*** на оцінку **"відмінно"** та присвоїти йому кваліфікацію магістр з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач ***Терно Ярослав*** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 76 сторінок, 29 рисунків, 4 таблиці, 20 джерел.

Об'єкт дослідження – системи виявлення та реагування на загрози в інформаційній безпеці.

Предмет дослідження – методи та технології виявлення загроз і реагування на них, що реалізовані в платформі Trend Vision One.

Мета роботи – аналіз сучасних підходів до виявлення та реагування на кіберзагрози з використанням платформи Trend Vision One, вивчення її архітектури, механізмів роботи, а також розробка рекомендацій щодо ефективного застосування цієї технології для захисту інформаційних систем.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, вивчення сучасних викликів та типів загроз у сфері кібербезпеки.

Технологія Trend Vision One забезпечує інтегроване виявлення, аналіз та реагування на загрози в єдиній хмарній платформі. Вона поєднує сучасні механізми кіберзахисту, такі як розширене виявлення та реагування (XDR), аналіз поведінки користувачів і пристроїв (UEBA), а також автоматизоване управління інцидентами безпеки. Платформа використовує штучний інтелект і машинне навчання для аналізу даних, виявлення складних загроз і швидкого реагування на інциденти. Trend Vision One надає централізоване управління через єдину консоль, що забезпечує ефективність роботи фахівців із кібербезпеки.

У роботі проаналізовано проблему забезпечення захисту інформаційних ресурсів організацій від сучасних кіберзагроз, визначено її мету та завдання. Проведено аналіз існуючих технологій виявлення та реагування на загрози в інформаційній безпеці. Досліджено методи та засоби, реалізовані на базі платформи Trend Vision One, її архітектуру, основні функції та механізми роботи.

На основі проведених досліджень розроблено порядок використання технології виявлення та реагування на загрози з використанням платформи Trend Vision One. Запропоновано рекомендації для фахівців із кібербезпеки, які спрямовані на підвищення рівня захисту інформаційних систем та забезпечення безпеки даних в онлайн-середовищі.

Галузь використання – інформаційна безпека підприємств, організацій та установ, що потребують захисту від сучасних кіберзагроз та забезпечення безпеки критичних даних.

TREND VISION ONE, ПРОТИДІЯ ЗАГРОЗАМ, КІБЕРБЕЗПЕКА, ЗАХИСТ АНТИВИРУСОМ, ЕФЕКТИВНИЙ ЗАХИСТ КОМП'ЮТЕРА, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КОМП'ЮТЕРА, ЗАХИСТ КІНЦЕВИХ ТОЧОК.

ABSTRACT

Text part of the master's qualification work: 76 pages, 29 figures, 4 tables, 20 sources.

Object of research – threat detection and response systems in information security.

Subject of research – methods and technologies for threat detection and response implemented in the Trend Vision One platform.

The aim of research – analysis of modern approaches to threat detection and response using the Trend Vision One platform, study of its architecture, mechanisms, and development of recommendations for the effective application of this technology to protect information systems.

Research methods – literature review on the topic, analysis of operational documentation, and examination of modern challenges and types of threats in cybersecurity.

The Trend Vision One technology provides integrated detection, analysis, response to threats within a single cloud platform. It combines advanced cybersecurity mechanisms such as Extended Detection and Response (XDR), User and Entity Behavior Analytics (UEBA), and automated incident management. The platform leverages artificial intelligence and machine learning to analyze data, detect complex threats, and rapidly respond to incidents. Trend Vision One offers centralized management through a unified console, enhancing the efficiency of cybersecurity professionals.

The study analyzes the problem of protecting organizational information resources from modern cyber threats, defining its purpose and objectives. Existing technologies for threat detection and response in information security were analyzed. The methods and tools implemented on the Trend Vision One platform, including its architecture, core functions, and operating mechanisms, were explored.

Based on the research, a framework for utilizing the Trend Vision One platform for threat detection and response has been developed. Recommendations were proposed for cybersecurity specialists aimed at enhancing the security of information systems and safeguarding data in online environments.

Field of application – information security of enterprises, organizations, and institutions that require protection from modern cyber threats and the safeguarding of critical data.

TREND VISION ONE, THREAT RESPONSE, CYBERSECURITY, ANTIVIRUS PROTECTION, EFFECTIVE COMPUTER SECURITY, METHODS AND TOOLS FOR COMPUTER SECURITY, ENDPOINT PROTECTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SIEM – Security Information and Event Monitoring

URL – Uniform Resource Locator

XSS – Cross-Site Scripting

IDR – Incident Detection and Response

EDR – Endpoint Detection and Response

XDR – Extended Detection and Response

IOA – Indicators of Attack

TTP – Tactics, Techniques, and Procedures

ASP – Application Service Provider

RAR – Roshal Archive

ZIP – Zone Improvement Plan

IP – Internet Protocol

AI – Artificial Intelligence

ШІ – Штучний інтелект

ІТ – Інформаційні технології

API – Application Programming Interface

MFA – Multi-Factor Authentication

ICS – Industrial Control Systems

OT – Operational Technology

5G – Fifth Generation

LLM – Large Language Model

DevOps – Development and Operations

SOAR – Security Orchestration, Automation, and Response

ВСТУП

Актуальність дослідження. Традиційний підхід до кіберзахисту, орієнтований на захист периметру корпоративної мережі, втрачає свою ефективність у сучасних умовах. Зростання популярності віддаленої роботи, міграція корпоративних даних у хмару та активна цифрова трансформація вимагають від IT-спеціалістів і фахівців з кібербезпеки впровадження нових моделей забезпечення безпеки.

Розширення меж корпоративних систем та зростання кількості загроз створюють необхідність у рішеннях, здатних забезпечити захист незалежно від фізичного місця знаходження користувачів чи ресурсів. Традиційні інструменти, такі як брандмауери, засоби запобігання втраті даних (DLP), захищені веб-шлюзи та брокери безпеки доступу до хмари (CASB), часто працюють як окремі рішення, що не можуть забезпечити повноцінний захист у розподіленому середовищі.

На цьому фоні платформи інтегрованого виявлення та реагування, такі як Trend Vision One, набувають критичної важливості. Trend Vision One пропонує єдину хмарну платформу, яка забезпечує багаторівневий захист інформаційних систем. Завдяки поєднанню таких технологій, як розширене виявлення і реагування (XDR), аналіз поведінки користувачів і пристроїв (UEBA), а також автоматизоване управління інцидентами, платформа дає змогу організаціям ефективно протистояти сучасним кіберзагрозам.

Основною перевагою платформи є її централізований підхід до захисту, що дозволяє спростити управління, знизити залежність від застарілих апаратних засобів та інтегрувати політики безпеки для всіх користувачів і ресурсів незалежно від їхнього місцезнаходження.

Об’єкт дослідження – системи виявлення та реагування на загрози в інформаційній безпеці.

Предмет дослідження – методи та технології виявлення загроз і реагування на них, що реалізовані в платформі Trend Vision One.

Мета роботи – аналіз сучасних підходів до виявлення та реагування на кіберзагрози з використанням платформи Trend Vision One, вивчення її архітектури, механізмів роботи, а також розробка рекомендацій щодо ефективного застосування цієї технології для захисту інформаційних систем.

Наукові завдання:

провести аналіз сучасних загроз у сфері кібербезпеки;

дослідити існуючі методи виявлення та реагування на кіберзагрози;

вивчити функціональні можливості та архітектуру платформи Trend Vision One;

розробити рекомендації щодо ефективного застосування платформи Trend Vision One;

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, вивчення сучасних викликів та типів загроз у сфері кібербезпеки.

Практичне значення одержаних результатів: запропоновано порядок використання технології виявлення та реагування на загрози за допомогою платформи Trend Vision One, а також розроблено рекомендації для фахівців із кібербезпеки щодо її впровадження та ефективного застосування для забезпечення безпеки інформаційних систем.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ

1.1. Сучасні виклики та типи загроз

Кіберзагрози – це широкий спектр загроз, пов’язаних з використанням інформаційних технологій для здійснення несанкціонованого доступу, модифікації, знищення або розголошення інформації, а також для порушення доступності інформаційних систем. З розвитком цифрових технологій та їх все більшою інтеграцією в усі сфери життя, кіберзагрози стають все більш складними та витонченими.

Загрози кібербезпеці актуалізуються через дію таких чинників, зокрема, як:

- невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;
- недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;
- безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;
- недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;
- недостатня ефективність суб’єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;
- недостатній рівень координації, взаємодії та інформаційного обміну між суб’єктами забезпечення кібербезпеки [2].

Кіберзагрози також можна поділити на наступні види:

Таргетовані атаки (advanced persistent threat). В залежності від цілей, можна виділити дві протилежні тактики атак на комп'ютерні системи. Перший

варіант – застосувати для атаки програмне забезпечення (вірус, троянський кінь), маючи на меті компрометацію якомога більшої кількості систем. Другий варіант – провести атаку прицільно (звідки й назва «таргетовані», тобто націлені), для компрометації комп'ютерів конкретної установи або навіть конкретних користувачів (як правило, посадових осіб високого рангу або їхніх помічників, науковців, взагалі людей, які мають справу з особливо цінною інформацією);

Кібертероризм (вплив на системи керування). Те, що власне і називають кібертерроризмом – можливість впливу через комп'ютерну мережу (зокрема, Інтернет) на системи керування транспортом, промисловими об'єктами, будинками та будь-якими технологічними процесами. ІКТ надають терористам кілька інструментів: застосування комп'ютерних мереж для керування, координації дій і підготовки терактів; можливість терористам напряму звертатись до широкого кола людей, використовуючи сервіси сучасного Інтернету; потенційно будь-який технологічний процес, яким керує цифрова система керування (або SCADA), може стати об'єктом атаки кібертерористів;

Кібервійни – це застосування інформаційних технологій для досягнення військових або політичних цілей шляхом атак на комп'ютерні системи, мережі та дані. Це форма сучасного конфлікту, яка може мати далекосяжні наслідки для економіки, політики та суспільства в цілому.

Основні характеристики кібервійни:

- Невидимість**:** На відміну від традиційних воєн, кібервійни часто відбуваються непомітно, без фізичних руйнувань.
- Глобальний масштаб**:** Кіберпростір не має географічних кордонів, тому кібератаки можуть здійснюватися з будь-якої точки світу.
- Низька вартість: Для проведення кібератаки не потрібні великі ресурси, що робить її доступною для держав, злочинних груп та окремих хакерів.
- Багатогранність: Кібератаки можуть мати різні цілі: від крадіжки інформації до дестабілізації критичної інфраструктури.

Хактивізм. Зловживання інформацією у соціальних мережах (вплив на суспільство). Деякі хакерські угруповання ставлять за мету видобування

конфіденційної (іноді таємної) інформації і розкриття її шляхом розміщення в Інтернеті у вільному доступі. Як правило, йдеться про викриття таємних операцій, змов, корупції та інших дій на рівні урядів чи окремих політичних сил, які суперечать закону, принципам демократії й іншим загальнолюдським цінностям;

Атаки на банківські системи (викрадення грошей). Чим ширше у банківській сфері застосовуються інформаційно-комунікативні технології, тим більше можливостей для махінацій у цій сфері. Дуже поширеними є фішинг, викрадення і використання атрибутів платіжних карток, а також застосування дуже складного і досконалого шкідливого програмного забезпечення для втручання в роботу систем клієнт-банк;

Атаки на електронний уряд. «Електронний уряд» – інформаційно-комунікаційна система, або об'єднання інформаційно-комунікаційних систем, що автоматизує інформаційну взаємодію органів державної влади та органів місцевого самоврядування з громадянами та суб'єктами господарювання з метою підвищення ефективності надання державних послуг. Атаки на електронний уряд можуть зашкодити функціонуванню такої системи, а у країнах з низьким рівнем впровадження інформаційно-комунікаційних технологій – підірвати довіру до демократичних перетворень і технічного прогресу;

Апаратні закладки у мікросхемах та прошивках комп'ютерного і мережного обладнання [1].

Мережеві загрози також діляться на три види.

Програмно технічні загрози стали першим видом загроз, що викликала панічні настрої як приватних користувачів, так і представників великих бізнес структур, а також державних органів.

Економічні загрози – наступна проблема. Після того як в мережу прийшов бізнес, стали популярні системи інтернет-платежів, пожвавилася електронна торгівля, з'явилися системи інтернет банкінгу.

Актуальними стали зломи платіжних акаунтів, фішинг атаки, продаж номерів кредитних карт. Всі учасники ринку займалися розробкою систем захисту від економічних кіберзагроз, а також розробкою правил поводження з грошима в

інтернеті.

Після того як публікація контенту, як текстового, так і фото, відео стала доступна кожному, з’явилися так звані *контентні кіберзагрози* і відповідно появу нового підвиду кібербезпеки — контентної безпеки.

До контентних загроз відноситься поширення матеріалів, що порушують законодавство. До них відносяться:

- терористична і екстремістська інформація;
- сектантська інформація;
- злочини проти персональних даних, честі та гідності особи;
- нарко пропаганда;
- насильство в інтернеті, пропаганда злочинів та навчання щодо їх скоєння.

Сьогодні більшу актуальність становлять загрози, пов’язані з розповсюдженням матеріалів екстремістського змісту, ксенофобські матеріали, а також пропаганда злочинів, пов’язаних з наркотиками і тероризмом [3].

Рівні небезпечності шкідливих програм:

Хоча чіткої класифікації за рівнями небезпечності не існує, можна виділити кілька основних категорій:

Низький рівень: Шкідливі програми, які викликають незначні проблеми, наприклад, уповільнення роботи комп'ютера або відображення реклами.

Середній рівень: Шкідливі програми, які можуть завдати серйозної шкоди системі, наприклад, викрасти дані або зробити систему непридатною для використання.

Високий рівень: Шкідливі програми, які можуть спричинити катастрофічні наслідки, наприклад, повне руйнування системи або виведення з ладу критично важливих інфраструктур.

Комп'ютерний вірус - це тип шкідливого програмного забезпечення, або малверу, який поширюється між комп'ютерами та завдає шкоди даним і програмному забезпеченню. Комп'ютерні віруси спрямовані на порушення роботи систем, викликання серйозних операційних проблем та призведення до втрати та

витоку даних. Важливо знати про комп'ютерні віруси, що вони розроблені для поширення між програмами та системами. Комп'ютерні віруси зазвичай прикріплюються до виконуваного файлу-носія, що призводить до виконання їх вірусного коду під час відкриття файлу. Потім код поширюється з документа або програмного забезпечення, до якого він прикріплений, через мережі, диски, програми обміну файлами або заражені вкладення електронної пошти.

Класифікація за принципом розповсюдження:

Дискові (завантажувальні) віруси — це тип атаки інфікує завантажувальний сектор диска або таблицю розділів. При запуску комп'ютера вони отримують контроль над системою ще до завантаження операційної системи.

Файлові віруси — це тип атаки інфікує виконувані файли (EXE, COM, DLL тощо), додаючи свій код до коду цих файлів.

Макровіруси — це тип атаки який розповсюджуються у документах, які підтримують макроси (наприклад, Microsoft Word, Excel). Вони виконуються при відкритті документа.

Поліморфні віруси — це тип атаки який змінює свій код при кожному копіюванні, ускладнюючи виявлення антивірусними програмами.

Стелс-віруси — це тип атаки який маскують свою присутність, приховуючи зміни, внесені в інфіковані файли.

Троянський кінь — це тип програми, яка прикидається чимось іншим, щоб проникнути на пристрій і заразити його шкідливим програмним забезпеченням. Тому вірус-троянський кінь — це вірус, замаскований під щось інше. Наприклад, віруси можуть ховатися в неофіційних іграх, додатках, на сайтах обміну файлами та в піратських фільмах.

Комп'ютерний черв'як — це не вірус. Черв'яки не потребують хостової системи і можуть поширюватися між системами та мережами без участі користувача, тоді як вірус вимагає виконання його коду користувачем.

Руткіт — це не вірус. Руткіти — це програмні пакети, які надають зловмисникам доступ до систем. Вони не можуть самостійно розмножуватися або поширюватися між системами.

«Баг» — це поширене слово, яке використовується для опису проблем з комп'ютерами, але програмний баг не є вірусом. Баг — це помилка або недолік у програмному коді, яку хакери можуть використовувати для запуску кібератаки або поширення шкідливого програмного забезпечення. [4]

Кетфіш (Catfishing) — це людина, яка створює фальшивий особистий профіль на соціальній мережі або сайті знайомств з метою обману або шахрайства. Зазвичай метою кетфішингу є фінансова чи матеріальна вигода, однак ці техніки можуть також використовуватися для отримання привілейованого доступу або інформації від бізнесу.

Фішинг (Phishing) — це вид кібератаки, в якій зловмисники видають себе за надійне або легітимне джерело, зазвичай з метою отримання конфіденційної та особистої інформації, такої як паролі та/або деталі акаунтів жертви. Фішингові шахрайства часто націлені на жертв через електронну пошту, намагаючись змусити їх відвідати вебсторінку, заповнити фальшиву форму або завантажити вкладення. Дізнайтеся більше про різні типи фішингу, як захистити свою електронну пошту та запобігти фішинговим атакам.

Вимагачі (Ransomware) — це тип шкідливого програмного забезпечення, яке може заблокувати пристрій або зашифрувати його вміст, що перешкоджає користувачу отримати доступ до своїх особистих файлів з метою вимагання грошей. В обмін оператори шкідливого коду обіцяють — звісно, без жодних гарантій — відновити доступ до ураженого пристрою чи даних. Вимагачі можуть з’являтися в різних формах, найчастіше — у вигляді спливаючих вікон на комп’ютері, але користувачі повинні бути обережні з небажаними електронними листами, які можуть обманом змусити їх перейти на небезпечні сайти або завантажити шкідливі файли. Читайте далі, щоб дізнатися більше та як захиститися від вимагачів.

Шкідливе програмне забезпечення (malware) — це поєднання двох слів: "malicious" (зловмисний) і "software" (програмне забезпечення) і описує будь-який вид шкідливого коду, який спеціально створений для проникнення в комп'ютер або пристрій без дозволеного доступу. Цей термін використовується для

охоплення всіх різновидів шкідливих програм, від комп'ютерних вірусів до троянських коней, незалежно від того, як вони впливають на жертв, як поводяться або який збиток завдають. Хоча шкідливе ПЗ не пошкоджує апаратне забезпечення, воно може красти, видаляти або захоплювати дані, а також шпигувати за вашою діяльністю, не повідомляючи про це.

Спам — це цифровий аналог небажаної пошти. Він описується як будь-яка форма небажаної масової комунікації (Unsolicited Bulk Email, або UBE). Поширеним видом спаму є комерційний електронний лист (Unsolicited Commercial Email, або UCE). Ці небажані листи надсилаються з анонімного джерела на велику кількість адрес, і навіть якщо лише декілька людей відреагують, відправник все одно отримує прибуток. Однак "спам" іноді надсилається через миттєві повідомлення, такі як текстові повідомлення або прямі повідомлення в соціальних мережах. Дізнайтеся більше про те, як розпізнати спам-листи та захистити свій сервер електронної пошти [5].

Denial-of-service (DoS/DDoS) — це переповнення ресурсів системи до такої міри, що вона не здатна відповідати на законні запити на обслуговування. **Розподілена атака типу denial-of-service (DDoS)** є подібною, оскільки також має на меті виснажити ресурси системи. Атака DDoS ініціюється величезною кількістю заражених шкідливим програмним забезпеченням комп'ютерів, що контролюються зловмисником. Ці атаки називаються "атаками на відмову в обслуговуванні", оскільки жертва не може надати послугу тим, хто хоче отримати доступ до неї.

Людина посередині (MITM) — це порушення в кібербезпеці, які дозволяють зловмиснику підслуховувати дані, що передаються між двома особами, мережами або комп'ютерами. Цю атаку називають "людина посередині", оскільки зловмисник займає позицію "посередині" між двома сторонами, які намагаються спілкуватися. Таким чином, зловмисник шпигує за взаємодією між цими сторонами.

Викрадення сесії (session hijacking) — це один з кількох типів атак "людина посередині" (MITM). У цьому випадку зловмисник захоплює сесію між

клієнтом і сервером. Комп'ютер, що використовується для атаки, замінює свою IP-адресу на IP-адресу комп'ютера клієнта, і сервер продовжує сесію, не підозрюючи, що він спілкується зі зловмисником, а не з клієнтом. Така атака є ефективною, оскільки сервер використовує IP-адресу клієнта для перевірки його особи. Якщо IP-адреса зловмисника вставлена в процесі сесії, сервер може не підозрювати про порушення, оскільки вже веде зв'язок у рамках довіреної сесії.

Спеціалізований фішинг (spear phishing) - відноситься до конкретного типу цілеспрямованої фішингової атаки. Атакуючий витрачає час на дослідження своїх цілей і пише повідомлення, які, ймовірно, будуть особисто актуальні для жертви. Ці типи атак називають "спеціалізованим" фішингом, оскільки атакуючий точно націлюється на одну конкретну жертву. Повідомлення буде здаватися легітимним, через що може бути важко виявити атаку спеціалізованого фішингу.

Впровадження (injection) Structured Query Language (SQL) — це поширений метод, що використовує вразливості веб-сайтів, які залежать від баз даних для обслуговування своїх користувачів. Клієнти — це комп'ютери, які отримують інформацію від серверів, а SQL-атака використовує SQL-запит, надісланий від клієнта до бази даних на сервері. Команда вставляється або «впроваджується» у поле даних замість чогось іншого, що зазвичай там є, наприклад, пароля або логіну. Сервер, що містить базу даних, потім виконує цю команду, і система стає вразливою для атакуючого.

Отруєний URL (URL poisoning) — це інтерпретація URL-адрес атакуючі змінюють і підробляють певні адреси URL, щоб отримати доступ до особистих і професійних даних жертви. Цей вид атаки також називається отруєнням URL (URL poisoning). Назва «інтерпретація URL» походить від того, що атакуючий знає порядок, у якому інформація URL веб-сторінки має бути введена. Потім атакуючий «інтерпретує» цю синтаксис, використовуючи її для того, щоб зрозуміти, як отримати доступ до областей, до яких у нього немає прав доступу.

Груба сила (brute-force attack) — це тип атаки отримала свою назву від "грубого" або простого методу, що використовується в атаці. Зловмисник просто намагається вгадати облікові дані для входу особи, яка має доступ до цільової

системи. Як тільки йому вдається вгадати правильно, він отримує доступ.

Drive-by - це тип атаки хакер вбудовує шкідливий код в незахищений веб-сайт. Коли користувач відвідує сайт, скрипт автоматично виконується на його комп'ютері, інфікуючи його. Назва "drive-by" походить від того, що жертві потрібно лише "проїхати" повз сайт, відвідавши його, щоб заразитися. Не потрібно нічого натискати на сайті чи вводити будь-яку інформацію.

Міжсайтовим скриптуванням або (XSS) — це тпи атаки коли зловмисник передає шкідливі скрипти, використовуючи клікабельний контент, який надсилається до браузера жертви. Коли потерпілий клацає на контент, скрипт виконується. Оскільки користувач вже увійшов у сесію веб-застосунку, те, що він вводить, сприймається як легітимне веб-застосунком. Однак скрипт, що виконується, був змінений зловмисником, що призводить до виконання непередбаченої дії від імені "користувача".

Прослуховування — це тип атаки який передбачає перехоплення трафіку зловмисником, коли дані передаються через мережу. Таким чином, зловмисник може збирати імена користувачів, паролі та іншу конфіденційну інформацію, таку як номери кредитних карток. Прослуховування може бути активним або пасивним.

День народження — це тип атаки коли зловмисник зловживає функцією безпеки: хеш-алгоритмами, які використовуються для перевірки достовірності повідомлень. Хеш-алгоритм є цифровим підписом, і отримувач повідомлення перевіряє його, перш ніж визнати повідомлення автентичним. Якщо хакер може створити хеш, який ідентичний тому, що відправник додав до свого повідомлення, зловмисник може просто замінити повідомлення відправника на своє. Отримуючий пристрій прийме його, оскільки у нього правильний хеш. [6]

Антивірусні програми можна класифікувати за їхнім призначенням:

Детектори – виявляють файли, які містять віруси.

Лікарі (фаги) – "лікують" заражені програми або документи, видаляючи віруси з пошкоджених файлів.

Ревізори – фіксують стан програм і дисків, порівнюючи їх із попередніми версіями, та повідомляють про будь-які виявлені невідповідності.

Фільтри – перехоплюють системні запити, які можуть бути використані вірусами для розмноження та завдання шкоди.

Блокувальники – перехоплюють небезпечні дії вірусів, такі як відкриття файлів для запису чи запис у завантажувальний сектор диска, та сповіщають користувача про це.

Сканери – перевіряють файли на жорсткому диску та в оперативній пам'яті на наявність шкідливого програмного забезпечення.

Імунізатори – попереджають користувача та/або заважають зараженню вірусами.

Для профілактики зараження комп’ютера вірусами слід дотримуватись певних правил:

1. **Встановіть антивірусне програмне забезпечення**: Використовуйте надійні антивірусні програми, які регулярно оновлюються, щоб забезпечити максимальний захист.
2. **Оновлюйте операційну систему та програми**: Регулярно встановлюйте оновлення для вашої ОС та програм, оскільки вони можуть містити патчі безпеки, які усувають вразливості.
3. **Будьте обережні з електронною поштою**: Не відкривайте вкладення або посилання в електронних листах від невідомих відправників, оскільки це може бути спроба фішингу чи розповсюдження шкідливого ПЗ.
4. **Не завантажуйте програмне забезпечення з неперевірених джерел**: Використовуйте лише офіційні веб-сайти або перевірені платформи для завантаження програм.
5. **Увімкніть брандмауер**: Використовуйте брандмауер для захисту вашої мережі та комп'ютера від несанкціонованого доступу.
6. **Регулярно створювати резервні копії даних**: Зберігайте копії важливих файлів на зовнішніх накопичувачах або у хмарних сервісах, щоб зменшити ризик втрати даних у разі зараження.
7. **Будьте уважні до налаштувань безпеки браузера**: Вимкнути автоматичне завантаження файлів та увімкніть блокувальники реклами, щоб уникнути

шкідливих сайтів.

8. **Захищайте свої паролі**: Використовуйте складні паролі та змінюйте їх регулярно. Не зберігайте паролі на комп'ютері у текстових файлах.
9. **Навчайтеся і підвищувати обізнаність**: Ознайомтеся з типами загроз і методами їх запобігання, щоб бути більш обізнаними щодо кібербезпеки.
10. **Обмежити доступ до адміністративних прав**: Не надавайте стороннім користувачам доступ до облікових записів з адміністративними правами, щоб зменшити ризик злому.

Сучасні кіберзагрози є складними та багатогранними, вимагаючи від держав, організацій та окремих користувачів постійного удосконалення засобів захисту і адаптації до нових викликів у сфері кібербезпеки.

1.2. Аналіз підходів виявлення та реагування на загрози

У сфері кібербезпеки існує кілька термінів, які використовуються для опису різних типів систем виявлення та реагування на загрози. Серед них IDR, EDR та XDR — чотири часто вживані терміни. Хоча на перший погляд вони можуть здаватися схожими, існують суттєві відмінності між ними, які важливо розуміти. Тепер давайте обговоримо різницю між IDR, EDR, XDR та SIEM.

Виявлення та реагування на інциденти (IDR) - це процеси та дії, пов’язані з ідентифікацією, аналізом і реагуванням на потенційні інциденти безпеки в IT-інфраструктурі організації. Виявлення інцидентів стосується безперервного моніторингу інфраструктури організації для виявлення будь-яких ознак шкідливої активності [7].

Порушення безпеки - також відоме як витік даних, виникає, коли конфіденційні, захищені або приватні дані копіюються, передаються, переглядаються або використовуються особою, яка не має на це дозволу. Ці дані можуть бути викрадені, утримувані для викупу або навіть знищені, зазвичай з метою фінансової вигоди.

Інцидент безпеки – це дія, яка суперечить політиці безпеки організації. Що ж робить інцидент безпеки відмінним від порушення даних? Інцидент безпеки є

порушенням політики, яке, якщо скоєно з зловмисним наміром, є порушенням.

Інцидент безпеки може включати в себе різноманітні дії. Деякі з більш навмисних, зловмисних прикладів включають скомпрометований обліковий запис користувача або жертву фішингової атаки. Інші можуть бути випадковими, наприклад, втрата флеш-накопичувача з конфіденційною інформацією або ненавмисне розкриття інформації, яка не повинна бути публічною. Незалежно від того, було це зроблено навмисно чи ні, важливо повідомити про це команду реагування на інциденти кібербезпеки, щоб вони були в курсі можливих атак і забезпечували захист інформації.

Респондент на інциденти – це особа, яка швидко і точно розслідує та стримує атаки. Вони можуть бути не першими, хто виявляє атаку, але їхнім завданням є оцінка серйозності інциденту кібербезпеки, визначення уражених користувачів і активів, а також усунення – очищення від атаки, щоб зловмисники більше не могли отримати доступ до внутрішньої мережі. Респондент на інциденти не обов’язково має бути співробітником вашої компанії, оскільки існують компанії, які надають зовнішніх респондентів для інших бізнесів. Зовнішні респонденти можуть запропонувати широкий спектр послуг, від розширення вашої команди безпеки до допомоги у прискоренні розслідування та стримування, а також допомоги у розробці вашої власної команди безпеки.

Як зловмисники проникають в компанію?

Способи проникнення зловмисників у компанію можуть відрізнятися, але у будь-якому випадку зловмисник повинен виконати хоча б один із кроків ланцюга атаки, який є графічним представленням кроків, необхідних для проникнення в компанію. Ланцюг атаки розділений на п'ять різних етапів: інфільтрація та збереження, розвідка, бічний рух, цільова місія та підтримка присутності. Важливо зазначити, що для успішного проникнення зловмисники не зобов’язані виконувати всі ці кроки або в такому порядку, хоча перший крок завжди виконується.

1. Інфільтрація та збереження: На цьому етапі зловмисники намагаються отримати початковий доступ до вашої мережі, щоб закріпитися в ній. Сюди

входять фішинг, викрадені облікові дані та шкідливе ПЗ.

2. Розвідка: На цьому етапі зловмисники оцінюють ситуацію та планують наступну мішень.
3. Бічний рух: Коли зловмисник переміщується з одного пристрою на інший, це називається бічним рухом. На цьому етапі зловмисник використовує скомпрометовані облікові дані, щоб отримати доступ до інших пристроїв.
4. Цільова місія: Цільові місії – це критично важливі активи або системи з великою цінністю, такі як захищена медична інформація або дані кредитних карток.
5. Підтримка присутності: Останнім кроком є створення бекдорів для підтримки присутності [8].

Виявлення та реагування на інциденти (IDR) є ключовим процесом для захисту інформаційних систем від зловмисників, що включає виявлення, відстеження та усунення загроз. Інциденти безпеки можуть виникати як внаслідок навмисних дій, так і випадкових помилок, тому важливо мати команду реагування, здатну швидко оцінити та нейтралізувати загрози, щоб запобігти крадіжці цінних даних.

EDR (Endpoint Detection and Response) — це програмне забезпечення для виявлення та реагування на загрози на кінцевих точках, використовується командами операцій безпеки для виявлення, стримування, розслідування та усунення наслідків кібератак, таких як програми-вимагачі та інше шкідливе програмне забезпечення. Інструменти EDR застосовуються для виявлення підозрілої активності на хостах і кінцевих точках, підключених до мережі, таких як мобільні телефони, настільні комп’ютери, ноутбуки та віртуальні машини [9]. Коли загроза виявлена, система EDR може негайно вжити заходів для ізоляції або усунення загрози.

Як працює EDR?

Рішення EDR записують активності та події, що відбуваються на кінцевих точках і всіх робочих навантаженнях, надаючи командам безпеки видимість, необхідну для виявлення інцидентів, які інакше залишилися б непоміченими.

Рішення EDR повинно забезпечувати безперервну та всебічну видимість того, що відбувається на кінцевих точках у режимі реального часу.

Інструмент EDR має пропонувати розширені можливості для виявлення загроз, розслідування та реагування, зокрема: пошук та розслідування даних про інциденти, обробку попереджень, перевірку підозрілої активності, полювання на загрози та виявлення й стримування зловмисної діяльності.

Ключові функції EDR

Автоматичне виявлення прихованих атакувальників

Технологія EDR поєднує всебічну видимість усіх кінцевих точок з індикаторами атак (IOA) і застосовує поведінкову аналітику, що аналізує мільярди подій в режимі реального часу, щоб автоматично виявляти сліди підозрілої поведінки.

Розуміння окремих подій як частини ширшої послідовності дозволяє інструменту EDR CrowdStrike застосовувати логіку безпеки, розроблену на основі CrowdStrike Intelligence. Якщо послідовність подій збігається з відомим IOA, інструмент EDR ідентифікує активність як зловмисну й автоматично надсилає попередження про виявлення. Користувачі також можуть створювати власні запити, використовуючи хмарну архітектуру Falcon Insight для отримання результатів за п'ять секунд або менше.

Інтеграція з розвідкою про загрози

Інтеграція з CrowdStrike Adversary Intelligence забезпечує швидше виявлення дій, тактик, технік та процедур (TTP), які ідентифіковані як зловмисні. Це надає контекстну інформацію, включно з атрибуцією, надаючи відомості про супротивника й інші деталі атаки.

Кероване полювання на загрози для проактивного захисту

Використовуючи EDR, мисливці за загрозами проактивно шукають, розслідують і консультують щодо активності загроз у вашому середовищі. Коли вони знаходять загрозу, вони працюють разом з вашою командою, щоб здійснити тріаж, розслідувати й усунути інцидент, перш ніж він стане повномасштабним порушенням.

Забезпечення видимості в режимі реального часу та історичних даних

EDR працює як цифровий відеореєстратор на кінцевих точках, записуючи важливу активність для відстеження інцидентів, що уникли запобігання. Клієнти мають доступ до всебічної видимості того, що відбувається на їхніх кінцевих точках з точки зору безпеки, оскільки CrowdStrike відстежує сотні різних подій, таких як створення процесів, завантаження драйверів, зміни в реєстрі, доступ до дисків, пам'яті або мережі.

Це надає командам безпеки корисну інформацію, зокрема:

- Локальні й зовнішні адреси, з якими з'єднується хост
- Усі облікові записи користувачів, які входили в систему, як безпосередньо, так і віддалено
- Зведення змін у ASP-ключах, виконуваних файлах і використанні адміністративних інструментів
- Виконання процесів
- Зведена та детальна мережева активність на рівні процесів, включаючи DNS-запити, з'єднання й відкриті порти
- Створення архівних файлів, включаючи RAR та ZIP
- Використання знімних носіїв

Цей повний огляд активності кінцевих точок, пов'язаної з безпекою, дозволяє командам "спостерігати" за діями супротивника в реальному часі, спостерігаючи, які команди вони використовують і які техніки застосовують під час спроби проникнути або переміститися в межах середовища.

Прискорення розслідувань

EDR від CrowdStrike здатен прискорити розслідування і, зрештою, усунення загрози, оскільки інформація, зібрана з кінцевих точок, зберігається у хмарі CrowdStrike через платформу Falcon з архітектурою на основі ситуаційної моделі.

Ця швидкість і рівень видимості, в поєднанні з інтегрованою, контекстуалізованою розвідкою, забезпечують інформацію, необхідну для ретельного розуміння даних. Це дозволяє командам безпеки ефективно

відстежувати навіть найбільш складні атаки, швидко виявляти інциденти, проводити тріаж, верифікацію та пріоритезацію, що призводить до швидшого та більш точного усунення загроз.

Можливість швидкого і рішучого усунення загроз

CrowdStrike EDR може ізолювати кінцеву точку, що називається “мережевим блокуванням". Це дозволяє організаціям швидко ізолювати потенційно скомпрометовані хости від усієї мережевої активності.

У режимі ізоляції кінцева точка все ще може передавати й отримувати інформацію з хмари CrowdStrike, і цей стан ізоляції зберігається навіть під час перезавантаження, забезпечуючи захист на весь час інциденту [10].

XDR (Extended Detection and Response) — це відносно новий термін, який з'явився в індустрії кібербезпеки. XDR є комплексним підходом до виявлення та реагування на загрози, що виходить за межі традиційних систем [11]. EDR, які фокусуються переважно на захисті кінцевих пристроїв, XDR пропонує комплексне рішення, що об'єднує дані з багатьох джерел для створення єдиного консолідованого огляду безпеки.

Основні характеристики XDR:

1. Інтеграція даних: XDR збирає та корелює дані з різних джерел, таких як:

- **Кінцеві пристрої:** комп'ютери, ноутбуки, мобільні пристрої.
- **Мережевий трафік:** аналіз активності в локальних та глобальних мережах.
- **Хмарні сервіси:** платформи та додатки, що працюють у хмарі.
- **Додатки:** веб-додатки та програмне забезпечення, що використовується в організації.

2. Контекстуалізація загроз: Збір та аналіз даних з різних джерел дозволяє XDR надавати контекстуалізовану інформацію про загрози, що допомагає виявити складні атаки, які можуть не бути виявлені ізольованими системами безпеки.

3. Автоматизація реагування: XDR включає автоматизовані механізми реагування, що дозволяє командами безпеки швидше вживати заходів для усунення загроз. Це може включати блокування шкідливих IP-адрес, ізоляцію скомпрометованих систем, або автоматичне застосування патчів до вразливостей.

4. Поглиблений аналіз загроз: Використовуючи аналітику та машинне навчання, XDR може виявляти аномалії в поведінці користувачів і пристроїв, що може свідчити про наявність загроз. Це дозволяє своєчасно виявляти потенційні вторгнення.

5. Спрощене управління**:** Оскільки XDR об'єднує дані з кількох джерел, це знижує складність управління безпекою. Команди можуть отримати єдиний огляд безпеки через одну платформу, що спрощує процеси реагування та моніторингу.

6. Покращена видимість: XDR надає організаціям покращену видимість загроз у всіх аспектах їхньої IT-інфраструктури. Це дозволяє швидше виявляти та реагувати на потенційні загрози, а також покращує загальний стан безпеки.

XDR стає важливим елементом сучасної стратегії кібербезпеки, оскільки дозволяє організаціям більш ефективно боротися з постійно зростаючими загрозами. Завдяки інтеграції даних з кількох джерел, автоматизації процесів реагування та поглибленому аналізу загроз, XDR забезпечує більш надійний захист і знижує ризики для організацій.

Системи управління інформацією та подіями безпеки (SIEM) — система, яка збирає, аналізує та накопичує дані про події безпеки. Ці програмні продукти розуміють багато форматів журналів додатків, можуть швидко шукати необхідні дані в цих журналах і зберігати їх тривалий час [12].

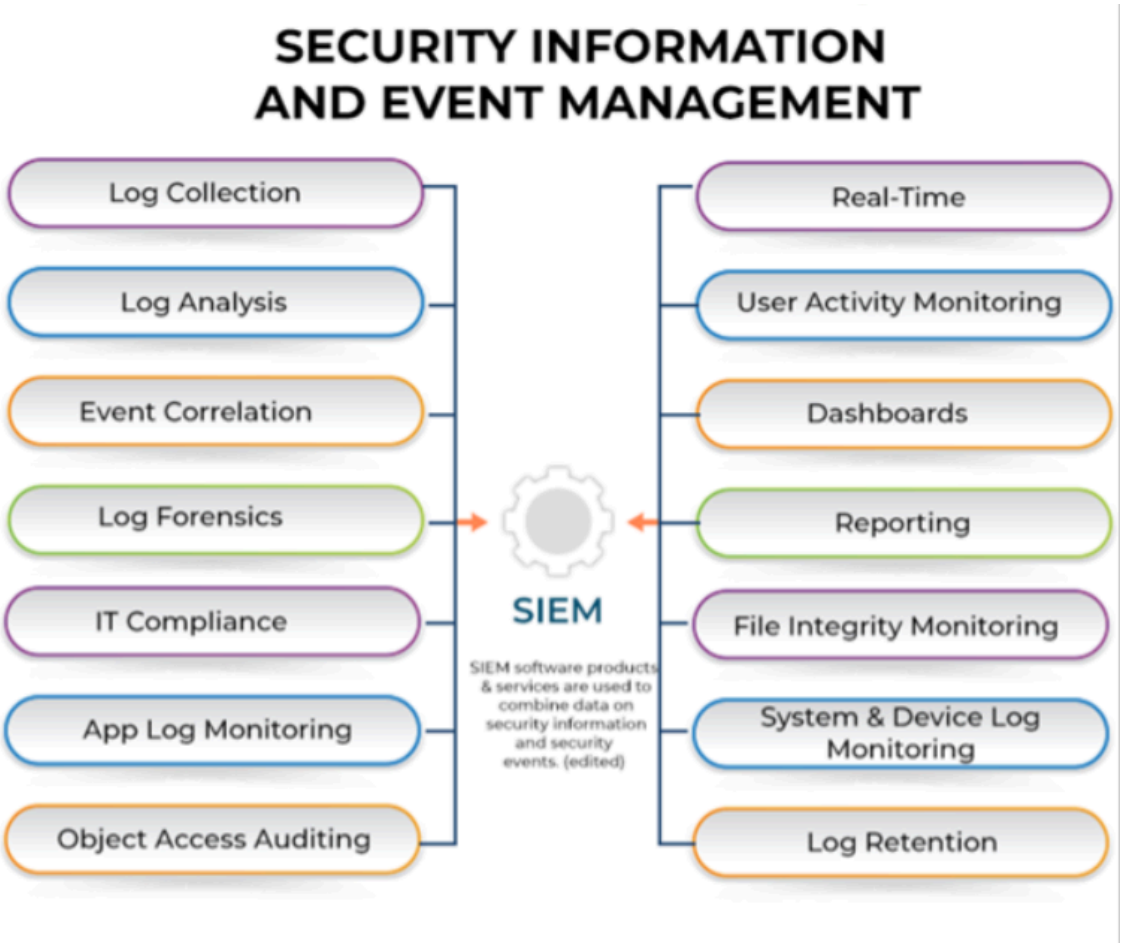

Рис. 1.1. Інформація про безпеку та керування подіями (SIEM)

SIEM — це поєднання управління інформаційною безпекою (SIM) і управління подіями безпеки (SEM). Вона повідомляє організації про можливі атаки, інциденти інформаційної безпеки чи навіть проблеми з дотриманням нормативних вимог. Рішення SIEM пропонують моніторинг і аналіз подій у реальному часі, посилюючи виявлення загроз і управління інцидентами безпеки за допомогою збору живих даних і історичних даних про події безпеки.

Основні функції SIEM охоплюють відстеження, логування, збирання та управління даними з безпеки для забезпечення відповідності чи проведення аудиту. Це також включає операційні можливості, такі як складання звітів, агрегування даних, моніторинг безпеки та моніторинг активності користувачів.

Як працює SIEM?

Організації можуть використовувати програмне забезпечення SIEM для

моніторингу, аудиту та повторної перевірки всіх журналів, які генерують їхні системи, включаючи програми, пристрої або домашні комп’ютери. Це дозволяє їм отримувати попередження про можливі проблеми з безпекою до їх виникнення, замість того щоб покладатися на реактивні дії.

Програмне забезпечення SIEM допомагає збирати дані, що генеруються різними програмами, мережевими пристроями та системами безпеки, такими як хости, мережі, міжмережеві екрани (фаєрволи) та події антивірусів, серед інших. Потім воно об'єднує всю інформацію в одному центральному місці.

Наприклад, коли SIEM ідентифікує загрозу, він створює попередження та повідомляє про атаку відповідних зацікавлених сторін. Користувацькі панелі інструментів SIEM також допомагають зменшити час, витрачений на перевірку помилкових спрацьовувань.

Розуміння архітектури системи управління інформацією та подіями безпеки (SIEM)

SIEM в основному стосується виявлення, запобігання та управління загрозами. Метою платформи SIEM є забезпечення ситуаційної обізнаності в реальному часі. Вона дозволяє організації своєчасно виявляти та реагувати на атаки.

Архітектура відіграє ключову роль у забезпеченні стабільної роботи SIEM. По суті, перед впровадженням SIEM потрібно приділити достатньо уваги її налаштуванню та технологічним аспектам.

Давайте розглянемо основні компоненти архітектури SIEM і отримаємо цінні уявлення про функціональні можливості цієї системи.

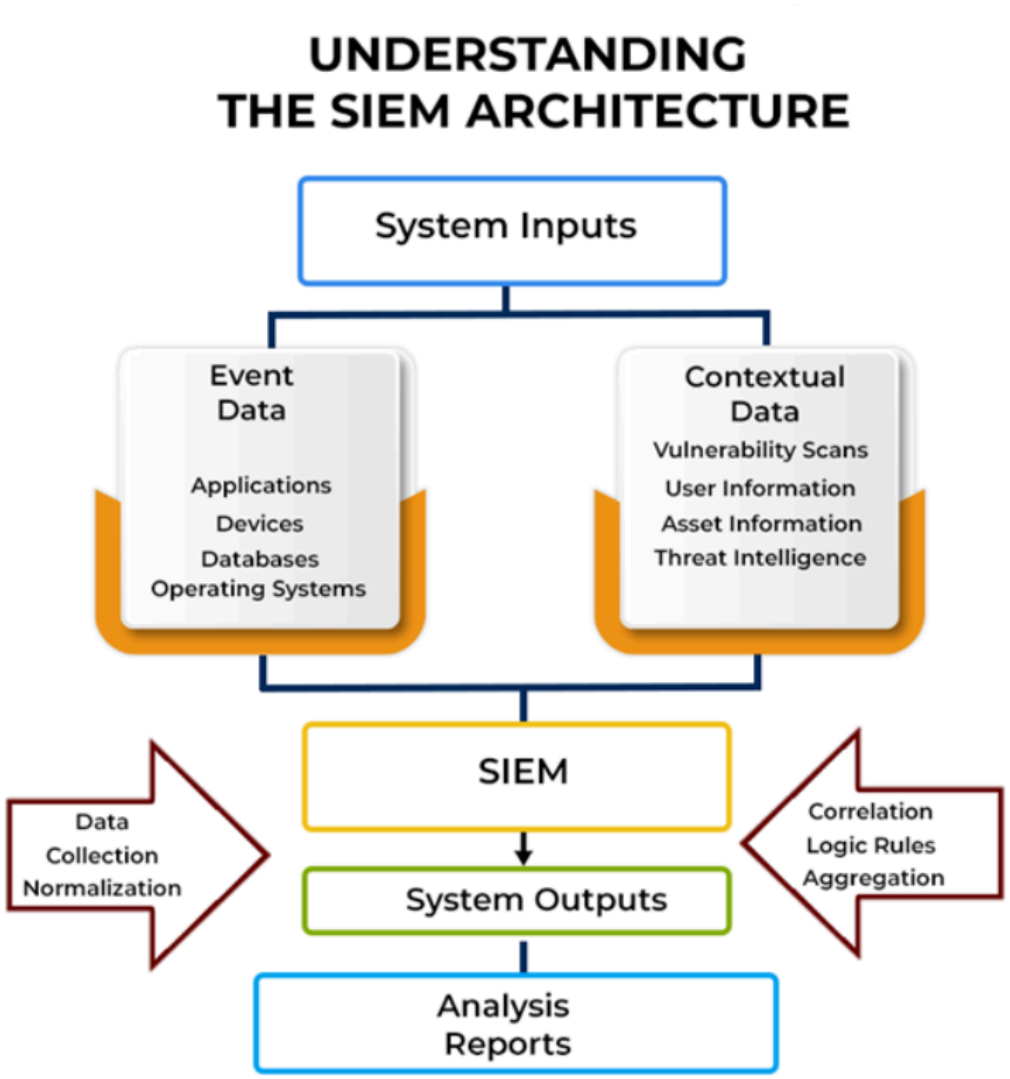

Рис. 1.2. Архітектура SIEM

1. Управління журналами

SIEM розумно збирає дані для надання широкого спектру зручної інформації, як-от продуктивність співробітників, фінансовий стан компанії, поведінка клієнтів тощо. Цей компонент відповідає за збір даних, їх управління та збереження минулих даних. Як показано на рисунку вище, SIEM збирає як дані подій, так і контекстні дані, включаючи дані від встановлених сервісів, пристроїв, мережевих протоколів, протоколів зберігання даних та потокових протоколів.

2. Нормалізація журналів

Як видно з рисунка, SIEM отримує події та контекстні дані, для яких нормалізація є важливою. Ключовий момент тут полягає в тому, що процес

перетворення подій у потрібну інформацію про безпеку можна здійснити шляхом фільтрації та видалення неактуальних або небажаних даних. Головна мета — позбутися непотрібних і дубльованих даних, залишивши тільки ті, що є корисними для подальшого аналізу.

3. Джерела журналів

Для чіткого розуміння процесу включення журналів у систему SIEM потрібно звернути увагу на збір, об’єднання та аналіз внутрішніх журналів. Ці журнали можна отримати з різних систем, як-от мережевих додатків, систем безпеки чи хмарних систем. Основна мета цього компонента — визначити джерела даних та напрямки їх транспортування.

4. Хостинг і звітність SIEM

Для хостингу SIEM доступні різні моделі, зокрема власний хостинг, хмарний хостинг і гібридний хостинг. SIEM виявляє та звітує про підозрілі або шкідливі дії на основі наявних журналів.

5. Моніторинг у реальному часі

Витоки даних є однією з найбільших загроз для бізнесу сьогодні. SIEM забезпечує рішення для моніторингу в реальному часі, що не тільки допомагає виявляти шкідливі атаки, але й визначає їх джерела, прогнозує загрози та вживає необхідних заходів для запобігання можливим витокам даних.

Операційний процес управління інформацією про безпеку та подіями (SIEM).

Одним із ключових елементів архітектури SIEM є операційний процес, який формує ефективну стратегію зниження кіберзагроз. Проте вся ця інформація може бути надто складною для розуміння, тому важливо знайти спосіб її оптимізації.

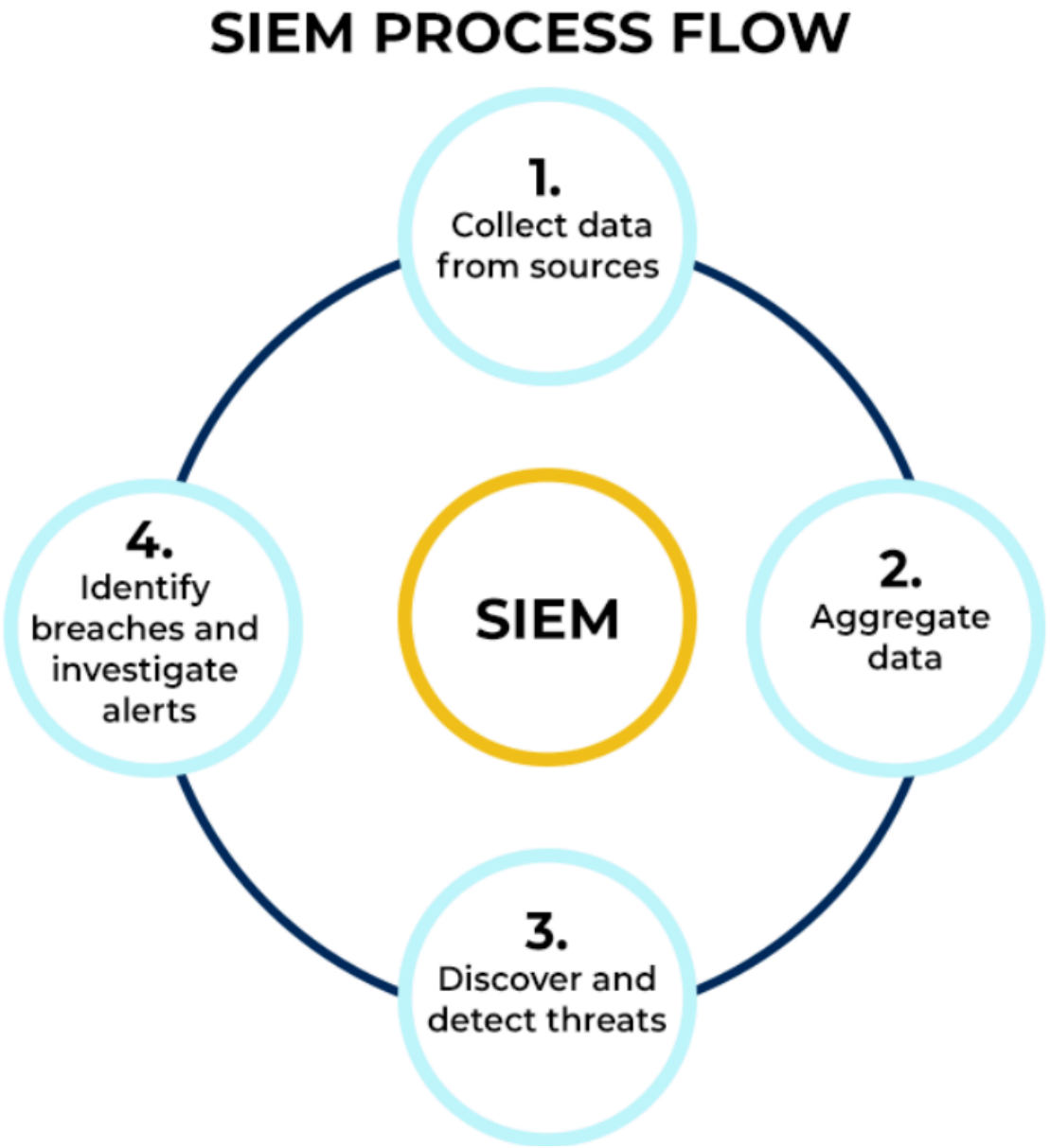

Рис. 1.3. Операційний процес SIEM

Правильні оперативні рекомендації можуть дозволити SIEM стати проактивною частиною повної архітектури управління інформаційною безпекою підприємства. Інструменти SIEM обробляють величезні обсяги даних, зібраних з різних джерел, і перетворюють їх на дієву інформацію, яка допомагає захистити бізнес. Плавна інтеграція між архітектурою SIEM і оперативними процесами є ключовою для покращення продуктивності системи.

Давайте розглянемо етапи, які входять до оперативного процесу SIEM:

1. Збір даних

Інструменти SIEM збирають журнали, різні типи даних і події з джерел всередині IT-системи організації. Після збору даних з цих пристроїв SIEM відповідає за їх стандартизацію та збереження у форматі, що дозволяє легкий аналіз і перегляд.

SIEM може збирати дані двома способами:

- **Автоматизований збір даних**: Це передбачає установку агента на пристрої та прямі з'єднання для отримання файлів журналів зі сховища (формат syslog) або протоколу потокового передавання подій, і зберігання всього в одному легко доступному місці, щоб організація могла отримати повну видимість загроз, з якими вона стикається.
- **Характеризація активів**: При категоризації інформаційно-технологічної інфраструктури організації важливо сегментувати або розділяти мережу на менші групи активів, які мають певну спільну рису чи функцію. Деякі приклади категорій IT-активів: пристрої, мережі та програми. Це допомагає у моніторингу мережевої активності та виявленні активів із високим рівнем ризику.

Таблиця 1.1.

Типові джерела даних SIEM

Додатки	Події безпеки	Журнали мережі	Пристрої
Веб-додатки	Трафік брандмауера	Безпровідні точки доступу	Мобільні пристрої
SaaS-додатки	Безпека кінцевих точок (антивірусні та антималварні засоби)	Віртуальні мережі	Особисті ноутбуки чи настільні комп'ютери
Інтране-додатки	Фільтри веб-додатків	Маршрутизатори, комутатори	Спільні робочі станції між людьми

2.Управління даними

Після збору даних починається процес управління даними. Дані, збережені у

належному вигляді, можуть значно покращити функціонування управління інформацією та подіями безпеки.

Зберігання: Інструменти SIEM мають здатність збирати величезну кількість даних. Ці дані можуть зберігатися на місці, у хмарі або в обох варіантах. Найважливіше, щоб місця зберігання мали високий рівень безпеки, щоб уникнути будь-якої втрати даних.

Ярусність: Розміщення даних має базуватися на їхній релевантності та важливості. Наприклад, "гарячі" дані, що використовуються для живого моніторингу безпеки, слід розміщувати в середовищах з високою продуктивністю. У той же час "холодні" дані, які можуть не використовуватися негайно, повинні зберігатися у дешевших середовищах зберігання.

Категоризація: Категоризація допомагає покращити продуктивність і ефективність інструментів SIEM. Це можна зробити, оптимізуючи та індексувавши дані для забезпечення аналізу, переглядів і досліджень, використовуючи розуміння загроз для категоризації ризиків загрози, працюючи з алгоритмами виявлення для зменшення ймовірності хибнопозитивних результатів і встановлюючи політики для стандартизованих робочих процесів з даними.

3. Зберігання даних

Інструменти управління інформацією та подіями безпеки містять велику кількість даних, які потребують певного ступеня сортування та фільтрації, щоб зменшити надмірні дані, що займають місце для зберігання в організації. Це, у свою чергу, також допомагає зберігати критично важливі дані.

Крім того, вимоги з дотримання стандартів PCI, DSS, HIPAA і SOX зобов'язують зберігати критичні журнали від 1 до 7 років. Розуміння зберігання даних також може допомогти аналізувати тенденції поведінки користувачів і нетипові патерни безпеки в майбутньому.

SIEM використовує такі методи для мінімізації обсягу журналів:

Сервери Syslog: Syslog є гнучким стандартом журналів, що дозволяє організації зберігати велику кількість даних у стандартизованому форматі. Syslog стискає великі обсяги даних і дозволяє легко шукати ці журнали, використовуючи

складні інструменти запитів.

Графік видалення журналів: SIEM автоматично видаляє дані журналів, які зберігалися довше, ніж цього вимагає політика зберігання. Зазвичай файли журналів можна безпосередньо отримати зі сховища в форматі Syslog.

Фільтрація журналів: Програмне забезпечення SIEM організації може фільтрувати журнали, які не завжди потрібні для виконання вимог дотримання або для цілей судової експертизи. Адміністратори SIEM можуть фільтрувати журнали за джерелом, типом, часом або іншими визначеними правилами. Крім того, використання фільтрації журналів може значно зменшити обсяги даних, що обробляються.

Сумаризація: Журнали можуть бути узагальнені, щоб зменшити кількість даних, що зберігаються на подію, але при цьому зберігати важливі частини, такі як кількість подій, унікальні IP-адреси тощо.

4. Інтеграції SIEM

При інтеграції процесів управління інформацією та подіями безпеки з іншими інструментами кібербезпеки синергія надає всій компанії вищий рівень захисту. Це відбувається тому, що використання платформи з управління SIEM, яка інтегрується з різноманітними програмними засобами, дозволяє виявляти, запобігати та локалізувати загрози безпеці в міру їх виникнення.

Одне із багатьох рішення тому що воно не вибирає, яке програмне забезпечення використовує команда, якщо тільки його дані можуть бути безпечно інтегровані в платформу SIEM. Приклади кількох варіантів інтеграції SIEM включають програмне забезпечення для управління ідентифікацією та доступом, інструменти управління оновленнями, інструменти безпеки хмари та інструменти управління ризиками третіх сторін [13].

1.3. Роль штучного інтелекту та машинного навчання у виявленні загроз

Штучний інтелект – це “технічна та наукова сфера, присвячена створеним системам, які генерують результати, такі як контент, прогнози, рекомендації або рішення для певного набору визначених людиною цілей”.

Насправді, ШІ — це просто практичний інструмент, а не панацея. Він настільки ефективний, наскільки хорошими є алгоритми та методи машинного навчання, які визначають його дії. ШІ може стати дуже вправним у виконанні певного завдання, але для цього потрібні величезні обсяги даних і повторень. Він просто навчається аналізувати великі обсяги даних, розпізнавати шаблони та робити прогнози або приймати рішення на основі цих даних, постійно покращуючи свою продуктивність з часом.

Сьогодні значення ШІ вийшло за межі простого оброблення даних і включає в себе розробку машин, здатних до навчання, міркування та розв'язання проблем. Машинне навчання стало настільки "компетентним", що здатне створювати все — від програмного коду до зображень, статей, відео та музики. Це наступний рівень ШІ, так званий генеративний ШІ, який відрізняється від традиційного ШІ своїми можливостями та застосуванням. Якщо традиційні системи ШІ переважно використовуються для аналізу даних та створення прогнозів, то генеративний ШІ йде далі, створюючи нові дані, схожі на ті, які були використані під час навчання .

Приклади технологій штучного інтелекту

Отже, що може робити ШІ? Більшість людей знайомі з ним через розумні колонки та голосові помічники на смартфонах, такі як Siri та Alexa, але нові технології штучного інтелекту постійно роблять наше життя легшим та ефективнішим у багатьох інших сферах [14].

Ось деякі приклади технологій та застосування штучного інтелекту:

Охорона здоров’я: Штучний інтелект використовується для аналізу даних пацієнтів, що допомагає лікарям швидше ставити діагнози та обирати оптимальні варіанти лікування. Наприклад, нещодавно було розроблено AI-систему під назвою AsymMirai, яка може прогнозувати рак грудей за п’ять років до його

появи. Завдяки цій технології лікарі можуть зберегти життя пацієнток, запобігти непотрібним тестам і заощадити кошти.

Фінанси: ШІ стає незамінним помічником у боротьбі з шахрайством та оптимізації інвестицій. Сучасні інструменти на базі AI здатні за лічені секунди обробляти величезні обсяги даних. Це дозволяє компаніям приймати обґрунтовані рішення в реальному часі, що критично важливо в умовах швидко змінюваного ринку.

Освіта: ШІ робить навчання доступнішим і персоналізованим. Інтерактивні платформи адаптують курси під потреби кожного студента, забезпечуючи індивідуальний підхід до навчання. А чат-боти завжди готові відповісти на ваші запитання, допомагаючи з матеріалом у будь-який час.

Транспорт: ШІ робить транспорт більш безпечним та комфортним. Алгоритми, що аналізують трафік, прогнозують затори та знаходять найзручніші маршрути, щоб ви швидше дісталися до місця призначення, змінюють наше уявлення про пересування .

Розваги: Платформи, такі як Netflix або YouTube, використовують ШІ для персоналізації контенту. Вони аналізують ваші вподобання, щоб запропонувати ті фільми чи відео, які вас зацікавлять. Це значно спрощує пошук контенту та створює для вас унікальні рекомендації. [15].

Унікальні можливості, які забезпечують системи на основі штучного інтелекту для зміцнення кібербезпекових захистів:

Адаптивне навчання: використання моделей машинного навчання в системах ШІ для постійного вдосконалення можливостей виявлення загроз у відповідь на еволюціонуючі загрози.

Поглиблене розпізнавання патернів: виявлення патернів атакувальників і аномалій серед величезних обсягів даних, включаючи тонкі ознаки злочинної діяльності, які не можуть бути виявлені людськими аналітиками.

Обробка даних в масштабах: алгоритми ШІ обробляють та аналізують величезні обсяги даних для виявлення загроз на швидкостях і обсягах, недоступних для людських аналітиків.

Автоматизовані відповіді: можливість миттєвого пом'якшення загроз.

Прогностична аналітика: проактивне виявлення майбутніх загроз і вдосконалення процесів полювання на загрози шляхом аналізу тенденцій і патернів у даних.

Зменшення кількості хибних спрацьовувань: усунення трудомістких оцінок загроз для команд безпеки шляхом розуміння різниці між безпечними та злочинними активностями.

Важливо розуміти, як ШІ допомагає краще виявляти загрози та змінює спосіб виявлення та обробки потенційних небезпек. Ось ключові методи та інструменти ШІ, які модернізують традиційне виявлення загроз до більш сучасних, швидших та перспективних підходів до забезпечення безпеки.

Висновки до розділу 1:

У першому розділі було здійснено комплексний аналіз проблеми виявлення та реагування на загрози, що охоплює сучасні виклики кібербезпеки, типи загроз, а також підходи до їх ідентифікації та усунення. Визначено ключові аспекти використання технологій IDR, EDR, XDR та SIEM, які забезпечують різні рівні моніторингу, аналізу та захисту інформаційних систем.

Особливу увагу приділено ролі штучного інтелекту та машинного навчання, які сприяють вдосконаленню механізмів виявлення загроз за рахунок поведінкового аналізу, автоматизації процесів і зниження кількості помилкових спрацювань. Розглянуто переваги інтеграції цих технологій із сучасними платформами для створення проактивного та багаторівневого захисту.

Таким чином, дослідження цього розділу закладає основу для розуміння сучасних тенденцій у кібербезпеці, демонструючи важливість комплексного підходу до виявлення загроз та інтеграції інноваційних технологій для ефективного реагування на них.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ НА ОСНОВІ TREND VISION ONE

2.1 Призначення та основні функції платформи Trend Vision One

Trend Vision One — це комплексна платформа кібербезпеки, яка об'єднує можливості запобігання, виявлення та реагування в єдине інтегроване рішення. Завдяки штучному інтелекту та розширеній розвідці загроз, вона забезпечує надійний захист від кіберзагроз, спрощуючи операції безпеки [16].

Ось основні призначення та функції цієї платформи:

Призначення платформи Trend Vision One

Централізоване управління кібербезпекою — надає єдиний центр управління для всіх аспектів безпеки, що дозволяє IT-спеціалістам контролювати та керувати безпекою з одного інтерфейсу.

Захист від кіберзагроз — платформа розроблена для виявлення, аналізу та реагування на складні кіберзагрози, включаючи атаки зловмисного програмного забезпечення, фішинг, спроби вторгнення та інші форми кіберзлочинності.

Зменшення ризиків для бізнесу — допомагає організаціям зменшити ризики витоків даних та інших інцидентів безпеки, забезпечуючи захист критично важливих систем та даних.

Основні функції Trend Vision One

1. Виявлення та реагування на загрози (XDR)

Платформа використовує розширене виявлення та реагування (XDR) для збору та кореляції даних із різних точок — від кінцевих пристроїв до серверів і хмарних середовищ. Це дозволяє виявляти загрози на ранніх стадіях та швидко на них реагувати.

2. Аналіз загроз у реальному часі

Trend Vision One використовує машинне навчання та штучний інтелект для аналізу даних у реальному часі, що допомагає виявляти підозрілі дії та аномалії, які можуть вказувати на можливу загрозу.

3. Автоматизація безпекових процесів

Платформа підтримує автоматизацію процедур кібербезпеки, що включає автоматичне виявлення та усунення загроз. Це значно скорочує час реакції на інциденти та знижує навантаження на IT-відділи.

4. Захист хмарних середовищ

Trend Vision One інтегрується з хмарними платформами (AWS, Azure, Google Cloud), забезпечуючи захист хмарної інфраструктури та додатків від кібератак та вразливостей.

5. Моніторинг поведінки користувачів

Функціонал аналізу поведінки користувачів дозволяє виявляти аномальні дії, наприклад, підозрілу активність користувача, що може свідчити про компрометацію облікового запису або інсайдерську загрозу.

6. Звітування та аналітика

Платформа надає детальні звіти про інциденти безпеки, активність загроз і стан захисту, що дозволяє організаціям приймати обґрунтовані рішення щодо своєї кібербезпеки.

Trend Vision One призначена для організацій, які потребують надійного захисту від сучасних кіберзагроз, ефективного управління інцидентами безпеки та мінімізації ризиків для своїх IT-систем.

2.2 Механізми виявлення загроз у Trend Vision One

Trend Vision One - це не просто XDR-система, це комплексний інструмент всебічного моніторингу загроз на декількох рівнях безпеки. Фактично, система збирає і автоматично зіставляє дані на кількох рівнях, використовує механізми кореляції подій і постійно оновлювану базу моделей і правил виявлення атак, а також підтримує глобальний аналіз загроз.від кіберзагроз [17].

Рис. 2.4. Архітектура захисту на основі XDR (Extended Detection and Response)

Attack Surface Risk Management (Керування ризиками поверхні атаки) — це стратегія, спрямована на захист організації від кіберзагроз шляхом управління "поверхнею атаки", тобто всіма можливими точками, через які система може зазнати атаки. Основна мета — знизити ризики, пов’язані з цими точками, забезпечуючи всебічний захист і підвищення загальної кіберстійкості.

Основні етапи керування ризиками поверхні атаки:

Discover Attack Surface (Відкрийте поверхню атаки) це процес ідентифікації всіх можливих точок доступу, через які система може зазнати кібератаки. Цей етап включає:

Інвентаризацію активів: збір повної інформації про всі ресурси, які мають підключення до мережі, включаючи сервери, бази даних, пристрої, користувацькі облікові записи, додатки тощо.

Аналіз підключень: виявлення всіх мережевих підключень і комунікацій між різними компонентами системи, що можуть становити ризик.

Виявлення вразливостей: визначення слабких місць у системі, які можуть стати мішенню для атак, наприклад, застаріле ПЗ або недостатньо захищені API.

Assess Risk (Оцінка ризику) включає аналіз виявлених точок атаки з метою

визначення ймовірності та потенційного впливу загроз:

Класифікація загроз: виявлення можливих загроз і їх класифікація на основі рівня ризику для організації.

Оцінка ймовірності атаки: оцінка того, наскільки ймовірно, що певна загроза буде реалізована через конкретну точку доступу.

Аналіз впливу: оцінка того, який збиток може спричинити успішна атака на конкретний актив, включаючи фінансові збитки, втрату даних або репутаційні ризики.

Mitigate Risk (Пом'якшення ризику) передбачає впровадження заходів, які знижують ризики для виявлених точок доступу. Це можуть бути як технічні, так і організаційні заходи:

Зміцнення захисту: впровадження додаткових механізмів захисту, таких як багатофакторна аутентифікація, шифрування даних, та обмеження прав доступу.

Патчинг і оновлення: своєчасне оновлення ПЗ для усунення вразливостей.

Оркестрація реагування: автоматизація реагування на інциденти, що дозволяє швидко блокувати підозрілу активність, відключати вразливі системи або проводити аудит доступу.

Навчання персоналу: проведення тренінгів для співробітників для підвищення обізнаності про кіберзагрози та правильну поведінку під час роботи з чутливими даними.

Zero Trust Architecture (Архітектура нульової довіри) — це модель кібербезпеки, яка базується на принципі "нікому не довіряй, завжди перевіряй". Вона передбачає, що жоден користувач, пристрій або додаток не повинні автоматично вважатися надійними, незалежно від їхнього місця в мережі (всередині або поза межами корпоративної мережі).

Основні принципи архітектури нульової довіри:

Постійна аутентифікація та авторизація:

Користувачі та пристрої повинні проходити аутентифікацію кожного разу, коли намагаються отримати доступ до ресурсів, незалежно від їхнього попереднього статусу.

Авторизація базується на контексті, який враховує роль, поведінкові дані, місцезнаходження та інші фактори.

Мінімальні привілеї (Least Privilege Access):

Доступ надається на основі принципу найменших привілеїв, що означає, що кожен користувач або пристрій отримує лише ті права доступу, які потрібні для виконання конкретних завдань.

Це значно знижує ймовірність компрометації критичних активів у випадку порушення безпеки.

Моніторинг і реєстрація активності:

Весь мережевий трафік та активність у системі реєструються та моніторяться в реальному часі. Це допомагає швидко виявляти аномальні дії та реагувати на потенційні загрози.

Використовується аналітика та машинне навчання для виявлення підозрілої активності.

Сегментація мережі:

Система розділяється на ізольовані сегменти, щоб обмежити вплив потенційних загроз. Якщо одна частина мережі зазнає атаки, інші сегменти залишаються захищеними.

Це дозволяє зупинити поширення загроз всередині організації.

Використання багатофакторної аутентифікації (MFA):

Багатофакторна аутентифікація є ключовим елементом Zero Trust, забезпечуючи додатковий рівень захисту шляхом вимоги підтвердження особи через кілька незалежних факторів.

Extended Detection and Response (XDR) (Розширене виявлення та реагування) — це інтегрована платформа безпеки, що об'єднує та корелює дані з різних джерел для ефективного виявлення, розслідування та реагування на кіберзагрози. XDR забезпечує узгоджену захисну стратегію, яка охоплює весь ланцюг атак, мінімізує час на виявлення загроз і спрощує реагування.

Основні функції XDR:

Об'єднання даних з різних джерел:

XDR збирає, обробляє та корелює дані з різних захисних систем, таких як захист кінцевих точок, мережевий трафік, хмарні сервіси, електронна пошта, користувацькі ідентифікації тощо.

Це забезпечує єдине уявлення про загрози, що дозволяє аналітикам кібербезпеки краще зрозуміти ланцюг атак і вплив загроз на організацію.

Інтегрований моніторинг та виявлення загроз:

XDR використовує машинне навчання та аналітику поведінки для виявлення аномалій та загроз на основі комплексної оцінки поведінки користувачів, пристроїв та застосунків.

Виявляються навіть складні атаки, які не завжди можна виявити за допомогою традиційних систем захисту, таких як антивірус або фаєрвол.

Швидке та автоматизоване реагування на інциденти:

XDR автоматизує процес реагування на загрози, що дозволяє швидко ізолювати заражені системи, усувати вразливості або обмежувати доступ до критично важливих ресурсів.

Це зменшує вплив атак і забезпечує більш швидке повернення до нормального функціонування організації.

Єдина консоль для управління безпекою:

XDR забезпечує централізовану консоль для моніторингу, аналізу та управління інцидентами, що знижує складність роботи з численними розрізненими інструментами.

Це дозволяє командам безпеки бачити всю картину подій і зосереджуватися на пріоритетних загрозах.

Зниження навантаження на команди безпеки:

Завдяки автоматизації й кореляції подій XDR значно зменшує кількість помилкових сповіщень і знижує навантаження на команди безпеки, дозволяючи їм зосередитися на більш критичних завданнях.

Аналітика загроз та інші інструменти XDR сприяють підвищенню ефективності роботи й швидкому реагуванню на складні загрози.

Категорії послуг керування (Managed Services):

Endpoint Security (Безпека кінцевих точок): захист комп'ютерів, серверів та інших пристроїв, що підключаються до мережі.

Email Security (Безпека електронної пошти): захист від загроз, пов'язаних з електронною поштою, таких як фішинг та шкідливі вкладення.

Network Security (Мережева безпека): моніторинг мережевого трафіку для виявлення загроз, таких як DDoS-атаки або спроби проникнення.

Cloud Security (Безпека хмари): захист хмарних інфраструктур, що забезпечує безпеку даних і додатків у хмарі.

Identity Security (Безпека ідентичності): захист облікових записів користувачів і управління доступом.

Різні аспекти захисту:

1. User and Identity (Користувач і ідентичність) — захист облікових записів користувачів та їхньої ідентифікації, що включає управління доступом та багатофакторну аутентифікацію.
2. Email (Електронна пошта) — захист електронної пошти від фішингу, шкідливих вкладень і посилань, що є одними з основних каналів для атак.
3. Endpoints and Servers (Кінцеві точки та сервери) — захист кінцевих пристроїв, таких як комп'ютери та сервери, від вірусів, троянів та інших загроз.
4. Cloud Infrastructure (Хмарна інфраструктура) — безпека хмарних середовищ і платформ, що забезпечує захист даних і додатків, які працюють у хмарі.
5. Applications (Застосунки) — захист застосунків від загроз, зокрема вразливостей у програмному забезпеченні, які можуть бути використані для атак.
6. Code Repository (Репозиторій коду) — захист репозиторіїв коду для запобігання витоку або пошкодженню вихідного коду, який є важливим активом для компаній.
7. Data (Дані) — безпека даних, що включає захист від несанкціонованого доступу, шифрування та забезпечення конфіденційності.
8. Network (Мережа) — захист мережі від проникнень, зокрема від DDoS-атак

та інших мережевих загроз, що забезпечує безпечний обмін даними.

9. 5G — захист інфраструктури 5G, яка надає швидший і більш комплексний зв’язок, але також створює нові потенційні точки атаки.
10. ICS/OT (Системи керування і операційні технології) — безпека для промислових систем керування та операційних технологій, які використовуються на виробництвах, в енергетиці та інших галузях для забезпечення роботи критично важливої інфраструктури.

Orchestration and Automation (Оркестрація та автоматизація) — це компонент безпеки, що відповідає за координацію і автоматизацію дій у кібербезпеці, зменшуючи час на реагування на загрози та підвищуючи ефективність захисту.

Екстракція та автоматизація включає такі елементи:

Risk Mitigation IT Automation (Пом'якшення ризиків автоматизація IT):

Забезпечує зниження кібер ризиків завдяки автоматизованому виконанню безпекових завдань, таких як оновлення, патчинг, ізоляція систем та управління доступом.

Автоматизовані процеси також знижують навантаження на IT-команди та забезпечують своєчасне реагування на загрози.

Custom Playbooks, Case Management (Індивідуальні сценарії, Керування випадками):

Створення індивідуальних сценаріїв (playbooks) для реагування на різні типи атак і загроз, що забезпечує швидку та точну реакцію.

Управління випадками (case management) дозволяє організувати розслідування інцидентів, відстежувати їх статус та координувати дії команди безпеки для покращення реагування на інциденти.

Global Threat Intelligence (Глобальна аналітика загроз) — забезпечує моніторинг і аналіз глобальних загроз для захисту організації від новітніх атак. Це включає:

Attack Surface Intelligence, Zero Day Initiative (Інтелект про поверхню атаки, ініціатива нульового дня):

Збір даних про вразливі поверхні, що можуть бути використані

зловмисниками, і виявлення загроз на різних рівнях інфраструктури.

Ініціатива нульового дня спрямована на виявлення та усунення нових вразливостей, які ще не мають відомих методів захисту.

Threat Research, Big Data Analytics (Дослідження загроз, аналітика великих даних):

Постійне дослідження нових загроз для створення ефективних стратегій захисту.

Аналітика великих даних дозволяє аналізувати величезні обсяги інформації для виявлення шаблонів і аномалій, що можуть свідчити про загрози.

AI Native Foundation (Штучний інтелект як основа) — це використання ШІ та машинного навчання для підтримки та розвитку функцій безпеки. Включає такі елементи:

AI Privacy and Ethics, AI Companion (Конфіденційність та етика ШІ, ШІ-компаньйон):

Забезпечення конфіденційності та етичного використання ШІ для зниження ризиків, пов'язаних із обробкою персональних даних.

ШІ-компаньйон, що підтримує команди безпеки, забезпечуючи додаткові можливості для аналізу та розв'язання проблем безпеки.

Generative AI, custom LLM, Machine Learning (Генеративний ШІ • індивідуальна мовна модель, машинне навчання):

Використання генеративного ШІ для розробки адаптивних методів аналізу і прогнозування загроз.

Індивідуальні великі мовні моделі (LLM) дозволяють використовувати мовні інструменти для автоматизації, розслідування та реагування на інциденти.

Машинне навчання сприяє створенню самонавчальних систем для виявлення загроз, аналізу даних та адаптації до нових атак.

Ecosystem Integration (Інтеграція екосистеми) — це підхід, що забезпечує інтеграцію різних інструментів, платформ та технологій для створення єдиної екосистеми кібербезпеки. Інтеграція екосистеми дозволяє ефективніше виявляти, аналізувати та реагувати на загрози завдяки об'єднанню можливостей різних

рішень безпеки та забезпечує їх узгоджену роботу [18].

Основні переваги Ecosystem Integration:

Цілісність і координація: Завдяки інтеграції різних рішень безпеки компанії отримують єдину, узгоджену систему, що дозволяє більш ефективно реагувати на загрози. Це забезпечує узгодженість у процесах захисту даних і зменшує час, необхідний на реагування на інциденти.

Швидший обмін інформацією: Інтеграція забезпечує миттєвий обмін інформацією між компонентами системи безпеки, що дозволяє краще бачити загальну картину загроз і виявляти потенційні вразливості в режимі реального часу.

Розширена функціональність: Інтеграція екосистеми дозволяє використовувати передові можливості, такі як автоматизація, машинне навчання, штучний інтелект та аналітику великих даних. Це значно підвищує здатність організації до виявлення та нейтралізації складних загроз.

Скорочення кількості помилкових сповіщень: Об'єднана система, що корелює дані з різних джерел, дозволяє зменшити кількість помилкових сповіщень і сфокусуватися на дійсно важливих загрозах.

Trend Vision One — це потужна XDR-система, яка забезпечує багаторівневий моніторинг загроз та керування кібербезпекою. Її ключові елементи включають керування ризиками поверхні атаки, архітектуру нульової довіри, автоматизовану реакцію на інциденти та інтеграцію різних інструментів кібербезпеки. Завдяки поєднанню AI, аналізу великих даних та автоматизації, платформа дозволяє швидко виявляти й нейтралізувати загрози, зменшуючи навантаження на команди безпеки та забезпечуючи всебічний захист організації.

2.3 Порівняння функціональності Trend Vision One з іншими технологіями

Trend Micro було засновано Стівом Чангом, Дженні Чанг і Євою Чен у 1988 році для розробки антивірусного програмного забезпечення, але на цьому вони не

зупинилися. За останні 30 років ми стали лідерами ринку в галузі гібридної хмари, мережевої та кінцевої безпеки.

ІТ-інфраструктура продовжує змінюватися, поведінка користувачів стає більш ризикованою, а загрози еволюціонують. Ми постійно впроваджуємо інновації, щоб залишатися на крок попереду зловмисників. Наші засновники задали тон, культуру та шлях до інновацій, створивши сильну команду пристрасних людей, які працюють разом, щоб зробити світ безпечним для обміну цифровою інформацією сьогодні та в майбутньому [19].

Таблиця 3.2.

Порівняльний аналіз функціональності Trend Vision One із іншими схожими технологіями

Функціонал	Trend Vision One	CrowdStrike Falcon	Microsoft Defender for Endpoint	Palo Alto Cortex XDR	SentinelOne
Тип платформи	XDR із багатошаровим підходом	EDR із підтримкою XDR	EDR із інтеграцією в екосистему Microsoft	XDR для мереж, кінцевих точок і хмари	EDR із автоматизацією
Виявлення загроз	Використовує AI та машинне навчання	AI для аналізу поведінки кінцевих точок	Аналіз даних із використанням Microsoft AI	Глибока кореляція подій і AI	Автономне реагування на загрози
Захист кінцевих точок	Глибокий аналіз, захист від Zero-Day загроз	Надійний, швидке виявлення	Тісна інтеграція із Windows	Універсальний для різних середовищ	Висока швидкість реакції
Інтеграція даних	Дані з мереж, пошти, кінцевих точок, хмар	Дані з кінцевих точок	Глибока інтеграція в Microsoft 365 та Azure	Об'єднання мережевих, кінцевих і хмарних даних	Дані з кінцевих точок

Таблиця 3.3.

Порівняльний аналіз функціональності Trend Vision One із іншими схожими технологіями

Функціонал	Trend Vision One	CrowdStrike Falcon	Microsoft Defender for Endpoint	Palo Alto Cortex XDR	SentinelOne
Автоматизація реагування	Сценарії реагування, інтеграція з SOAR	Інтеграція із зовнішніми платформами	Автоматизація на базі Microsoft Sentinel	Інтеграція з SOAR	Підтримка автономного реагування
Хмарна безпека	Підтримка AWS, Azure, Google Cloud	Підтримка мультихмарних середовищ	Найкраще підходить для Azure	Підтримка хмарних платформ	Масштабованість для хмар
Кореляція подій	Сильна, завдяки XDR-аналітиці	Обмежена до кінцевих точок	Висока, у межах Microsoft середовища	Потужна, із фокусом на мережі	Помірна
Інтерфейс	Інтуїтивний, з єдиною панеллю управління	Простий для кінцевих точок	Інтеграція з Microsoft Security Center	Централізований	Інтуїтивний
Звітування	Детальні звіти про загрози	Стандартні звіти	Вбудовані звіти із інтеграцією Power BI	Потужні звіти	Налаштовувані звіти
Орієнтація	Для середніх і великих компаній	Підходить для будь-яких масштабів	Найкраще для корпоративних Windows середовищ	Для великих корпоративних середовищ	Для організацій будь-якого розміру

Таблиця 3.4.

Порівняльний аналіз функціональності Trend Vision One із іншими схожими технологіями

Функціонал	Trend Vision One	CrowdStrike Falcon	Microsoft Defender for Endpoint	Palo Alto Cortex XDR	SentinelOne
Переваги	Універсальність, інтеграція, XDR-аналітика	Надійність у захисті кінцевих точок	Інтеграція з Microsoft екосистемою	Глибока кореляція, аналітика	Підтримка автономного реагування
Недоліки	Висока вартість для невеликих компаній	Обмеження в мережевих даних	Залежність від екосистеми Microsoft	Дорожнеча, складність налаштувань	Менший обсяг XDR-аналітики

Trend Vision One виділяється серед інших платформ своєю універсальністю та інноваційним підходом до XDR (Extended Detection and Response). Завдяки багатошаровій аналітиці, інтеграції даних із різних джерел (кінцеві точки, мережі, пошта, хмари) та потужним інструментам автоматизації, ця платформа ідеально підходить для середніх і великих компаній, які потребують комплексного захисту від сучасних кіберзагроз.

У порівнянні:

1. **CrowdStrike Falcon** є ефективним у захисті кінцевих точок, але обмежений у кореляції подій та аналізі мережевих загроз.
2. **Microsoft Defender for Endpoint** пропонує відмінну інтеграцію в екосистему Microsoft, але залежність від цієї екосистеми може бути недоліком для компаній із гібридною або мультихмарною інфраструктурою.
3. **Palo Alto Cortex XDR** має сильну кореляцію подій і потужну аналітику, але його висока вартість та складність налаштування можуть бути стримуючими факторами.

4. **SentinelOne** вирізняється швидким автономним реагуванням і зручністю використання, але його аналітичні можливості XDR залишаються обмеженими.

Таким чином, Trend Vision One чудово підходить для компаній, які шукають платформу, здатну забезпечити глобальний огляд загроз, автоматизацію процесів редагування та масштабованість у мульти хмарних середовищах. Висока вартість може стати недоліком для невеликих організацій, проте її функціональні можливості виправдовують інвестиції для підприємств, що прагнуть максимального рівня кібербезпеки.

Висновки до розділу 2:

У другому розділі було проведено детальний аналіз методів і засобів виявлення та реагування на загрози з використанням платформи Trend Vision One. Основна увага була приділена її призначенню, функціональності та механізмам виявлення загроз. Розглянуто ключові компоненти платформи, що забезпечують багатошаровий підхід до захисту, включаючи інтеграцію даних з різних джерел, автоматизацію процесів реагування та використання штучного інтелекту для глибокого аналізу.

Також здійснено порівняння функціональності Trend Vision One з іншими схожими технологіями, такими як CrowdStrike Falcon, Microsoft Defender for Endpoint, Palo Alto Cortex XDR та SentinelOne. Особливу увагу приділено аспектам виявлення загроз, захисту кінцевих точок, інтеграції даних, хмарній безпеці та автоматизації реагування.

Результати аналізу демонструють переваги Trend Vision One у багатошаровому підході до безпеки, її універсальності та здатності інтегруватися в різні середовища. Разом з тим було зазначено потенційні обмеження, що дозволяє сформувати цілісний підхід до оцінки й вибору платформ для кіберзахисту відповідно до потреб організації.

3 ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ

3.1 Реєстрація та отримання онлайн Trend Vision One

Все починається з офіційного сайту trendmicro.com [20], де потрібно перейти до вкладки **Business** та натиснути кнопку **“Claim your 30 day free trial now”**. Після цього відкриється спливаюче вікно для реєстрації. Вносимо всі дані, які просить сайт.

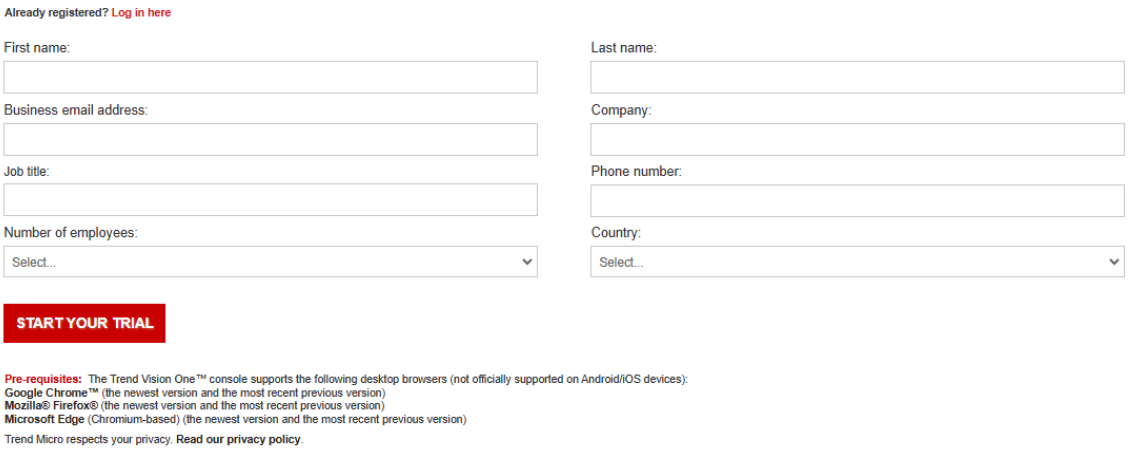

Рис. 3.5. Форма реєстрації

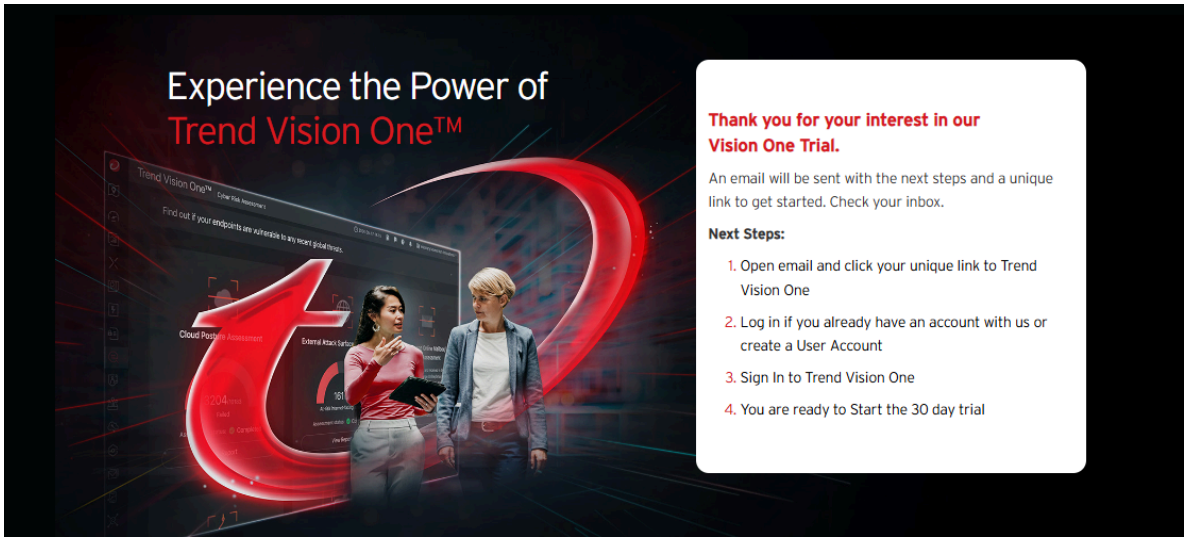

Рис. 3.6. Підтвердження через електронну пошту

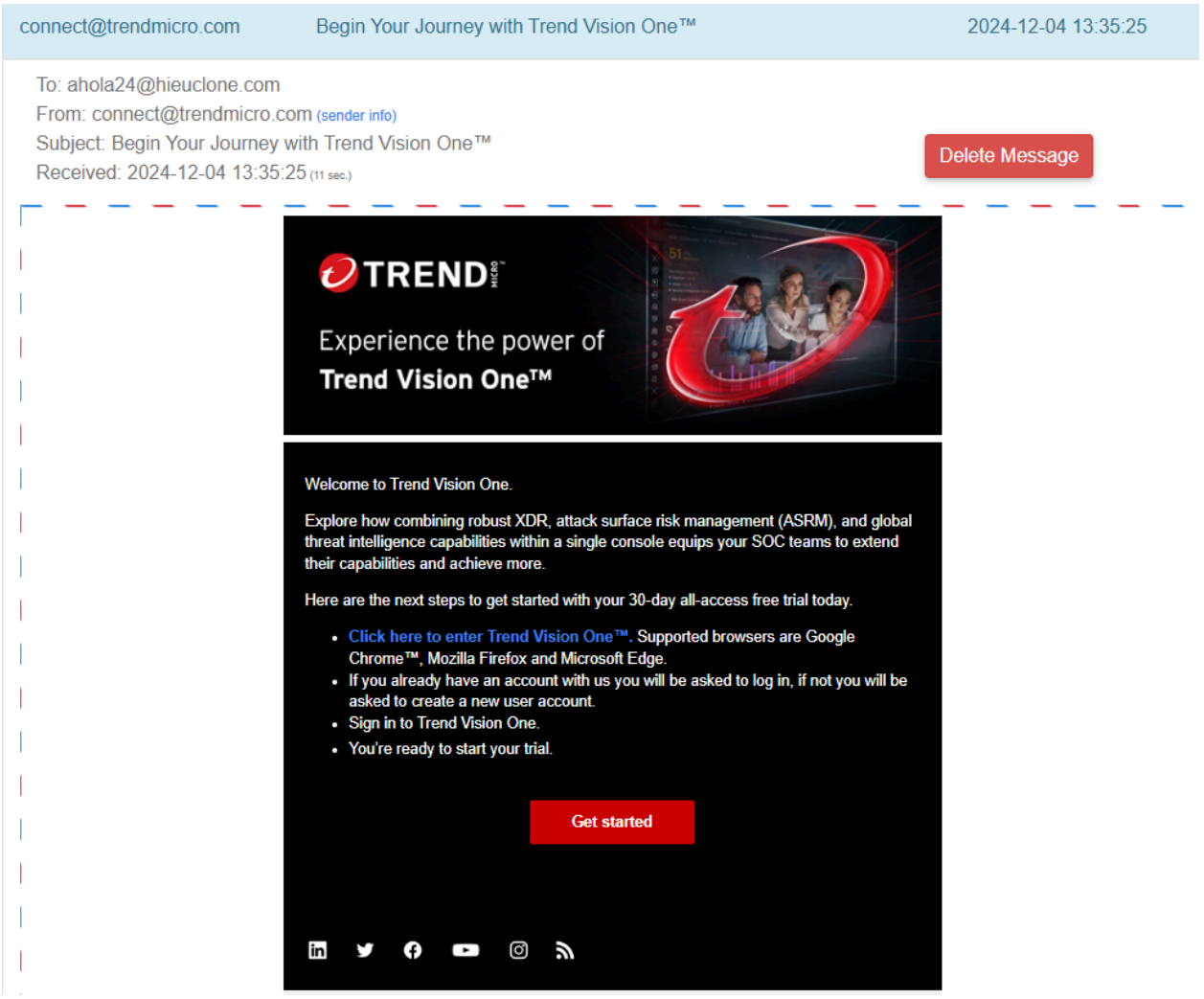

Рис. 3.7. Лист, який прийшов для підтвердження

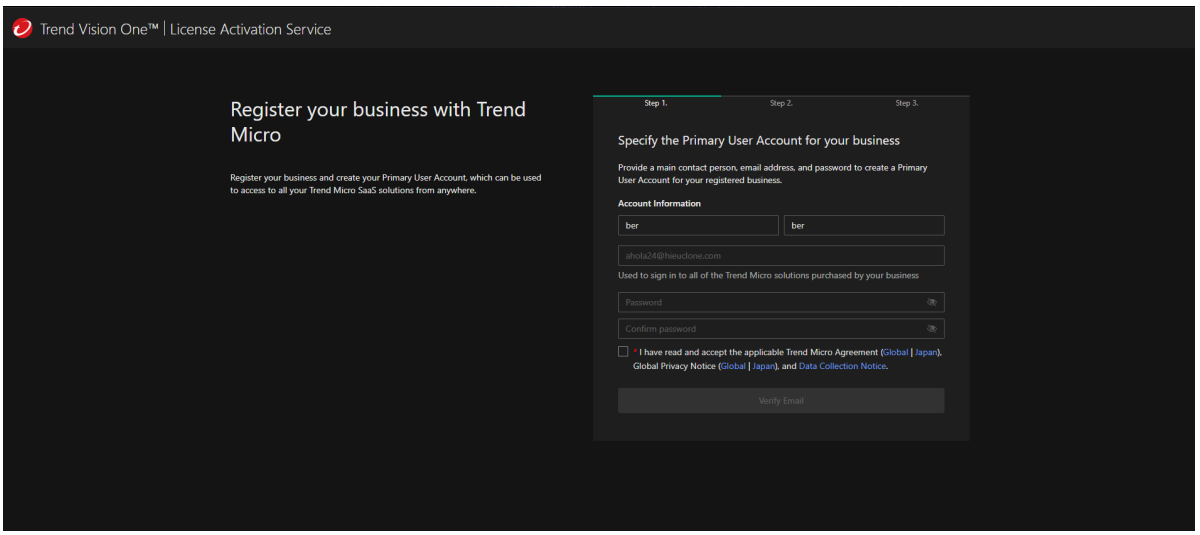

Рис. 3.8. Продовження реєстрації: "Крок 1" — Створення паролю для входу в систему

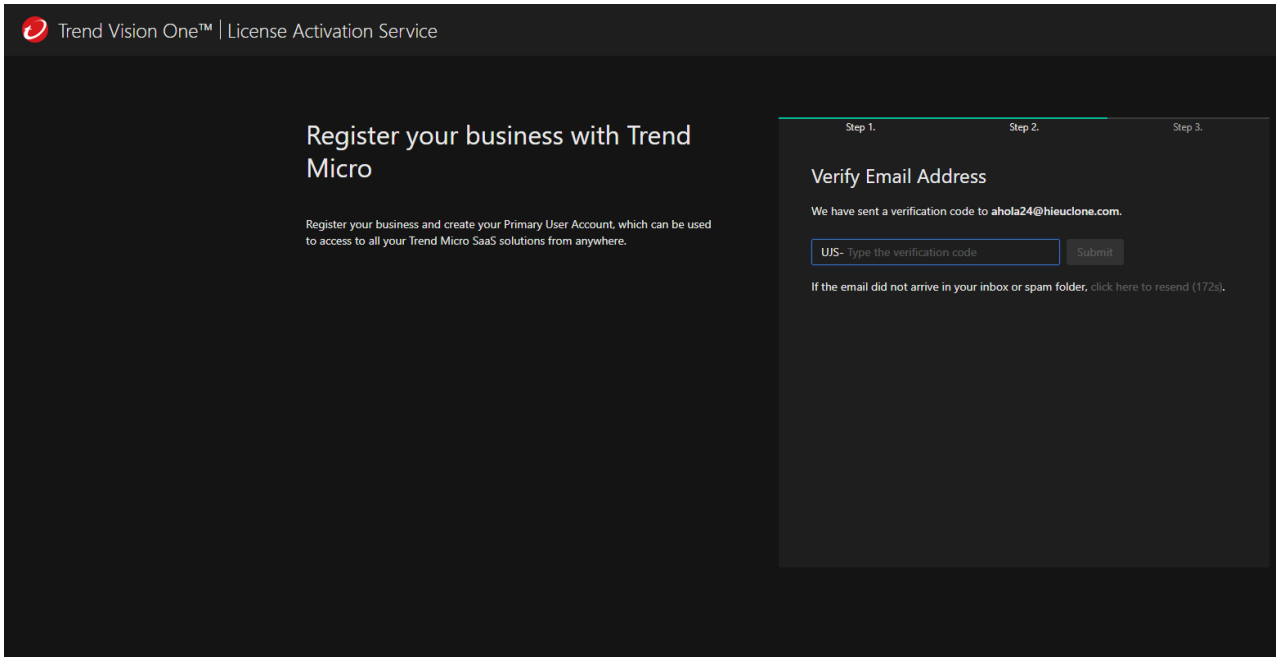

Рис. 3.9. Продовження реєстрації: "Крок 2" — Сайт відправив код для верифікації

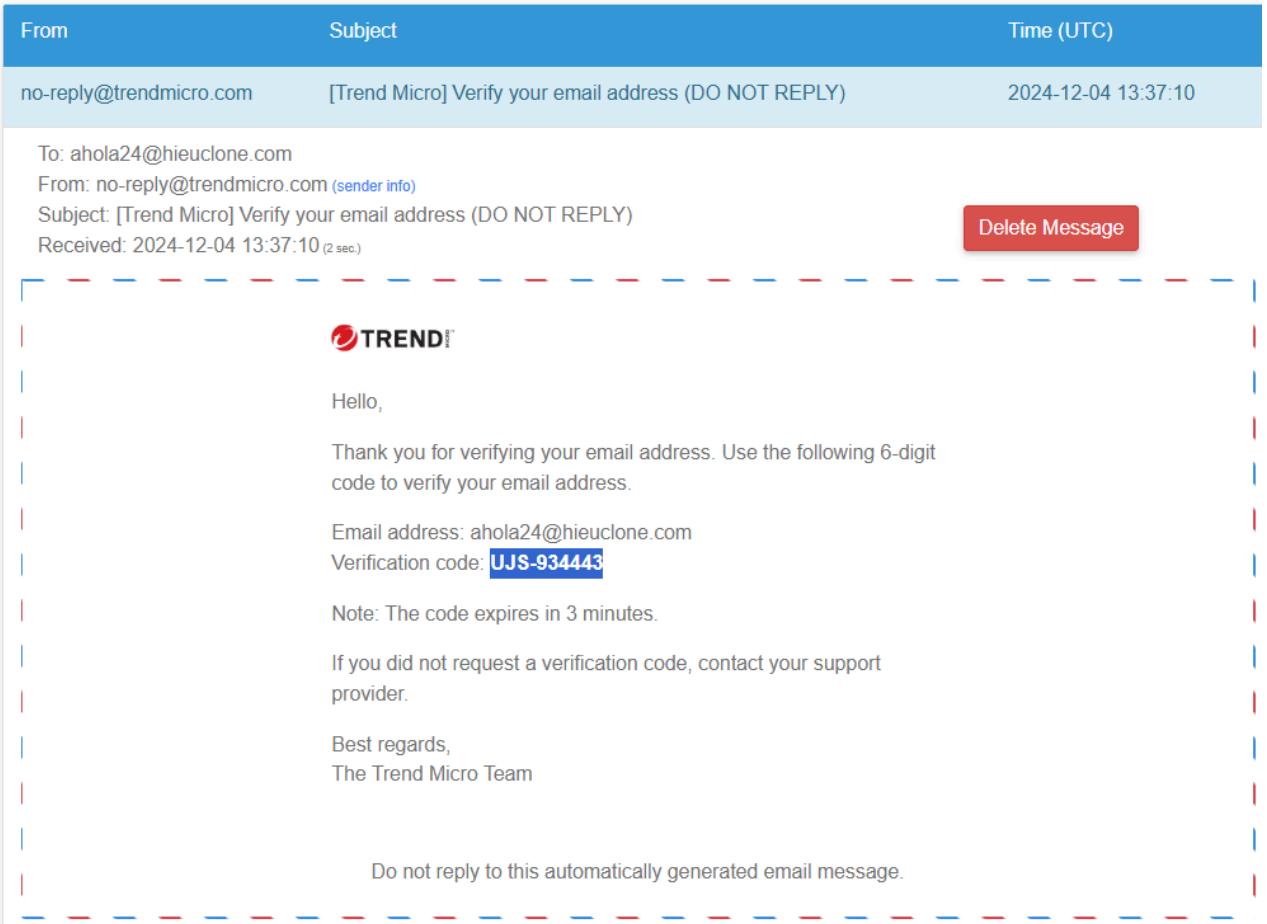

Рис. 3.10. Лист із кодом для верифікації

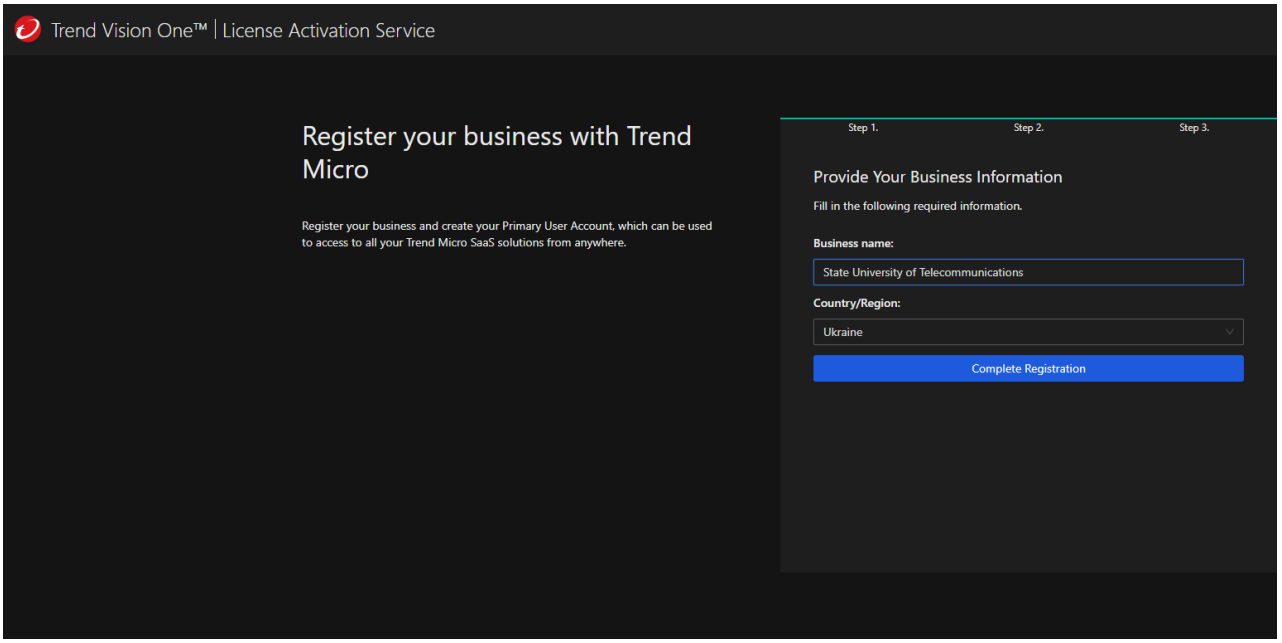

Рис. 3.11. Продовження реєстрації: "Крок 3" — Вибираємо назву компанії та країну

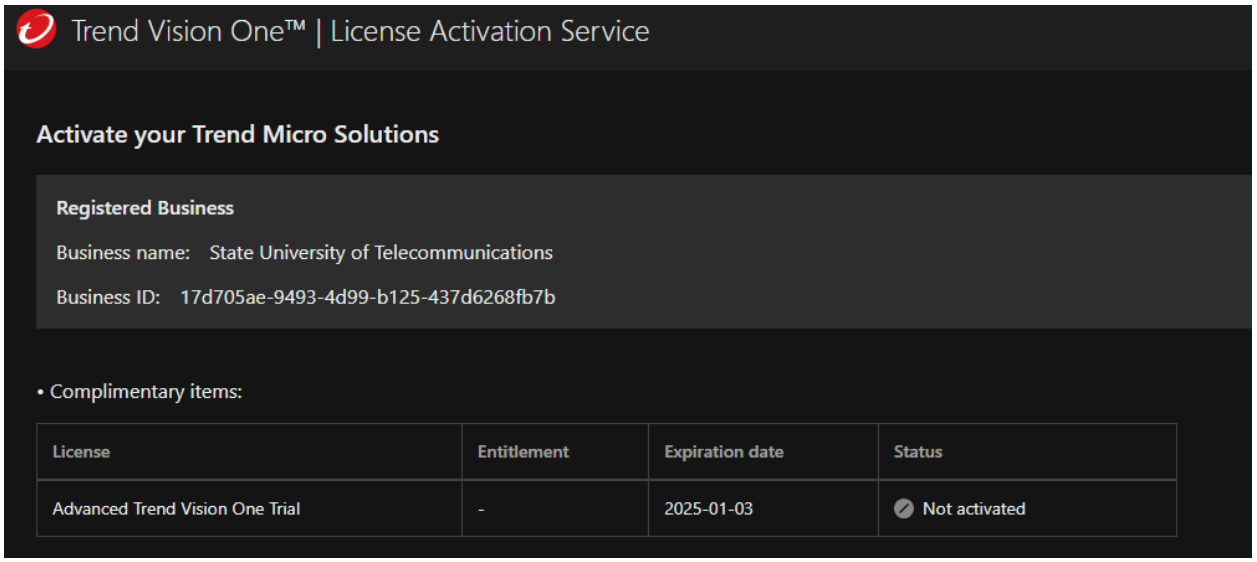

Рис. 3.12. Активація Trend Micro Solutions

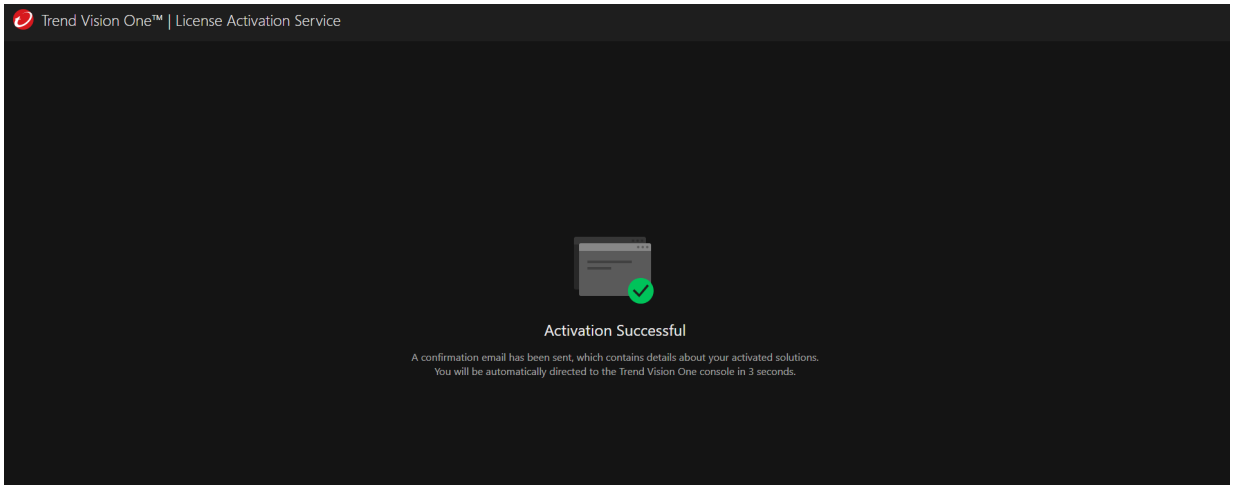

Рис. 3.13. Інформаційне вікно із “Activation Successful” (Активація успішна),

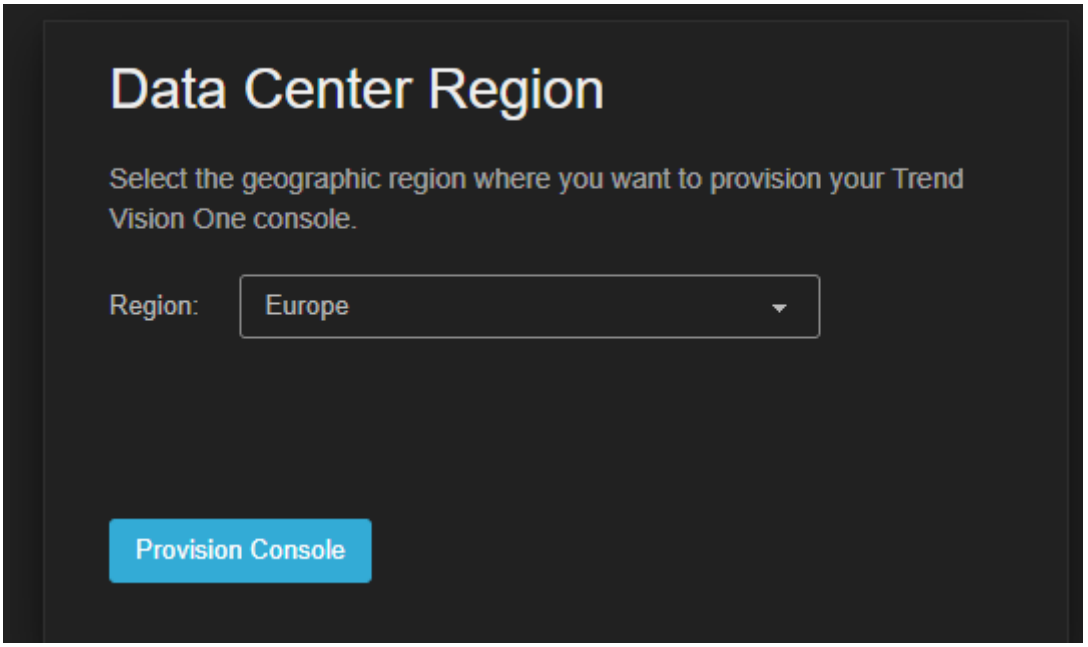

Рис. 3.14. Інформаційне вікно з вибором регіону розташування

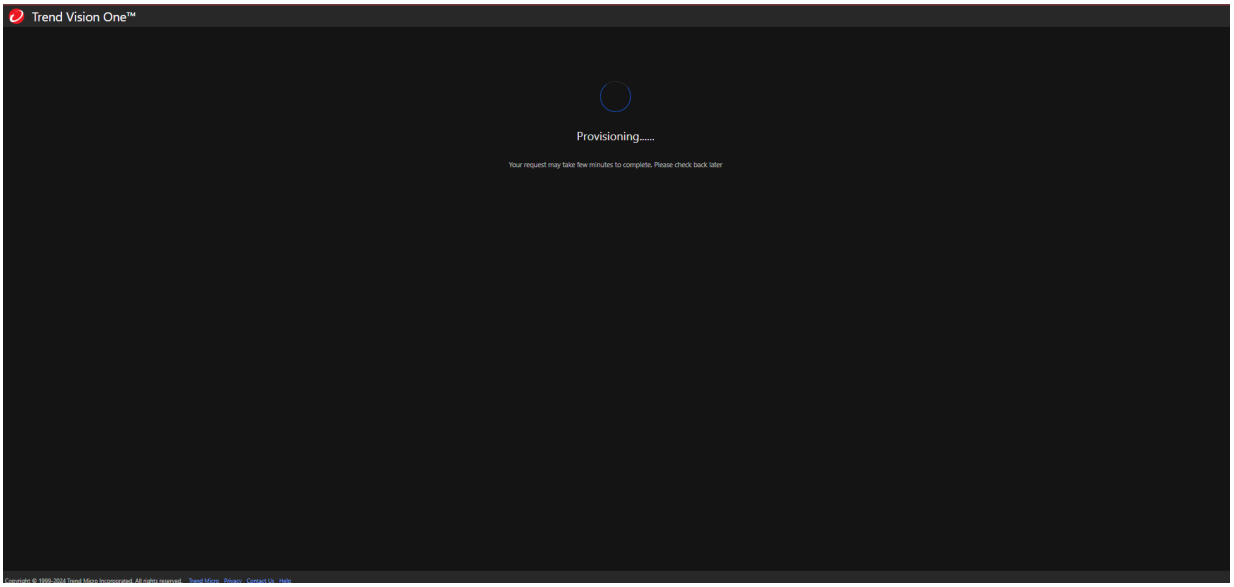

Рис. 3.15. Інформаційне вікно завантаження інтерфейсу платформи Trend Micro One

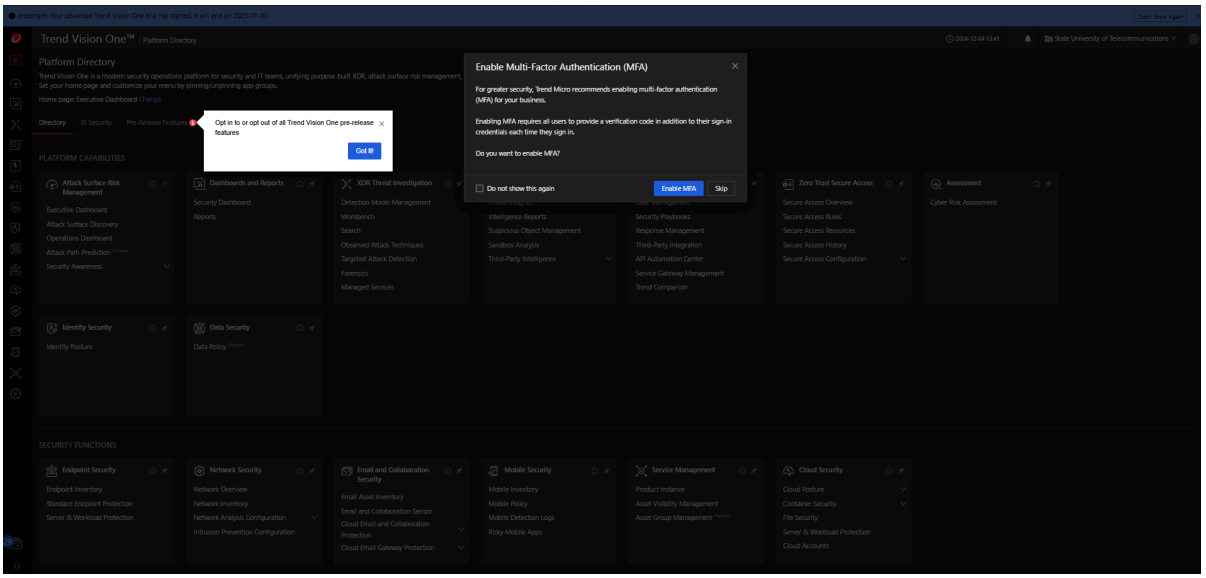

Рис. 3.16. Перший запуск та головна сторінка Trend Vision One

Розроблено рекомендації щодо пошагового пошуку та реєтація Trend Vision One на офіційному сайті, а також . Платформа успішно завантажена.

Під час дослідження функціональних можливостей Trend Vision One було виявлено, що цей продукт має багато корисних функцій для забезпечення кібербезпеки. Загалом, Trend Vision One може бути відмінним вибором для тих, хто шукає надійне і зручне рішення для захисту від різноманітних кіберзагроз.

Платформа забезпечує високий рівень захисту від шкідливих програм, включаючи віруси, шпигунський та рекламний софт, руткіти, а також загрози в режимі реального часу.

Однією з переваг Trend Vision One є те, що вона не суттєво впливає на продуктивність комп'ютера, на відміну від багатьох інших антивірусів, які можуть використовувати значну частину оперативної пам'яті. Платформа підтримує різні операційні системи, включаючи Windows, Mac та Android, що робить її універсальним рішенням для забезпечення безпеки на різних пристроях.

3.2 Технологія застосування рішення Trend Vision One

На етапі виконання робити зробимо невелике дослідження, встановлення та налаштування агента.

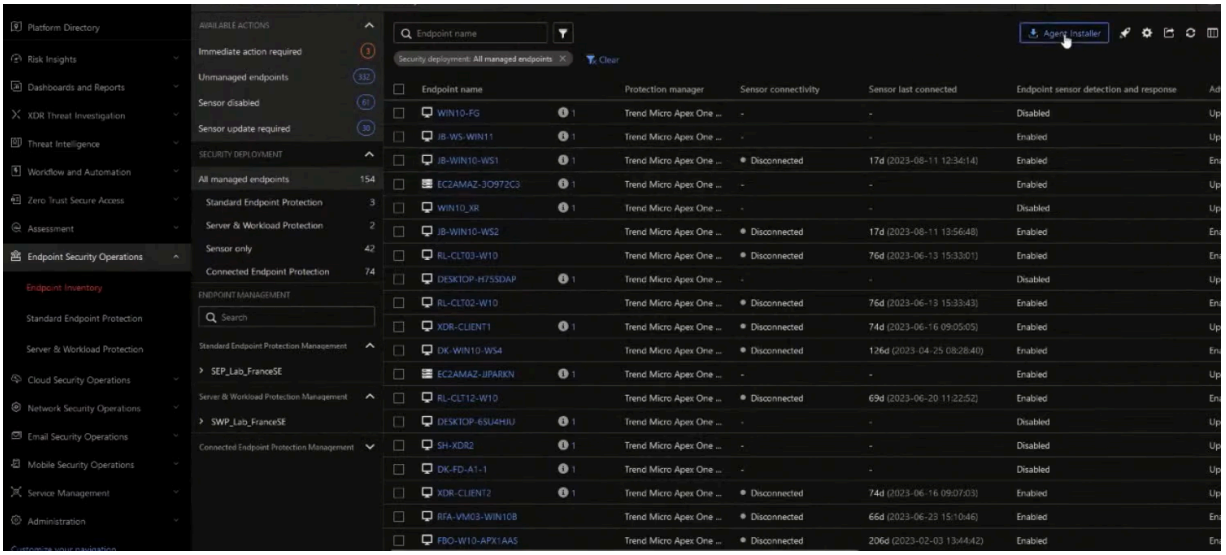

Рис. 3.17. Встановлюємо агент із новою інфраструктурою, вибираємо опцію “Agent Installer”.

Доступні три варіанти: стандартний захист кінцевих точок, захист серверів та робочих навантажень, а також сенсор кінцевих точок.

Стандартний захист кінцевих точок призначений для Windows і MacOS, зокрема для Windows 10/11.

Захист серверів та робочих навантажень використовується для серверів на базі Windows та Linux.

Сенсор кінцевих точок забезпечує базову функціональність без реального часу захисту. (Рис. 3.70).

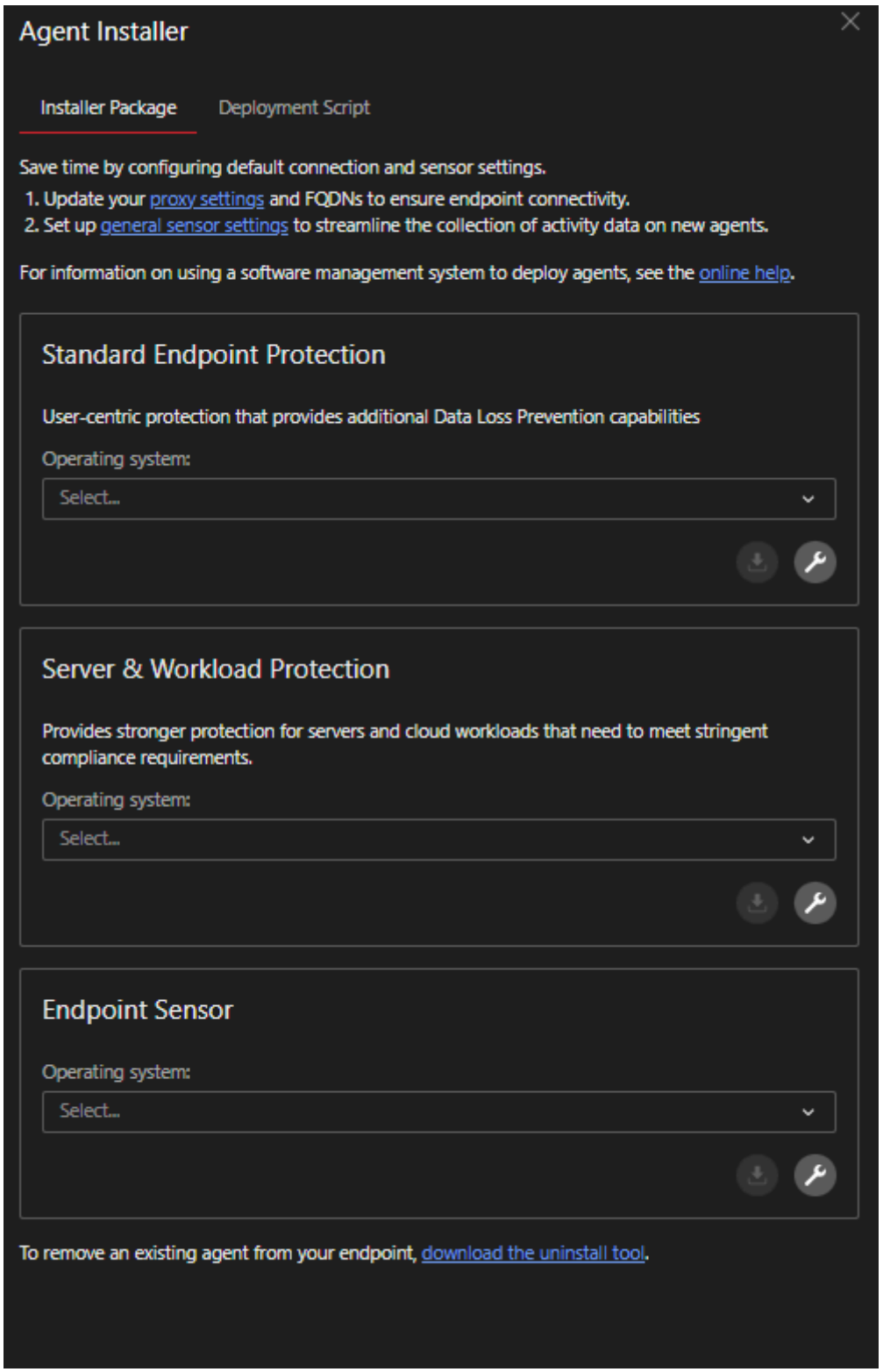

Рис. 3.18. Інформаційному вікні є три види агентів для встановлення.

Я створю чотири віртуальні машини на перших двох. Встановлю стандартний захист кінцевої точки, а третій — датчик і дані.

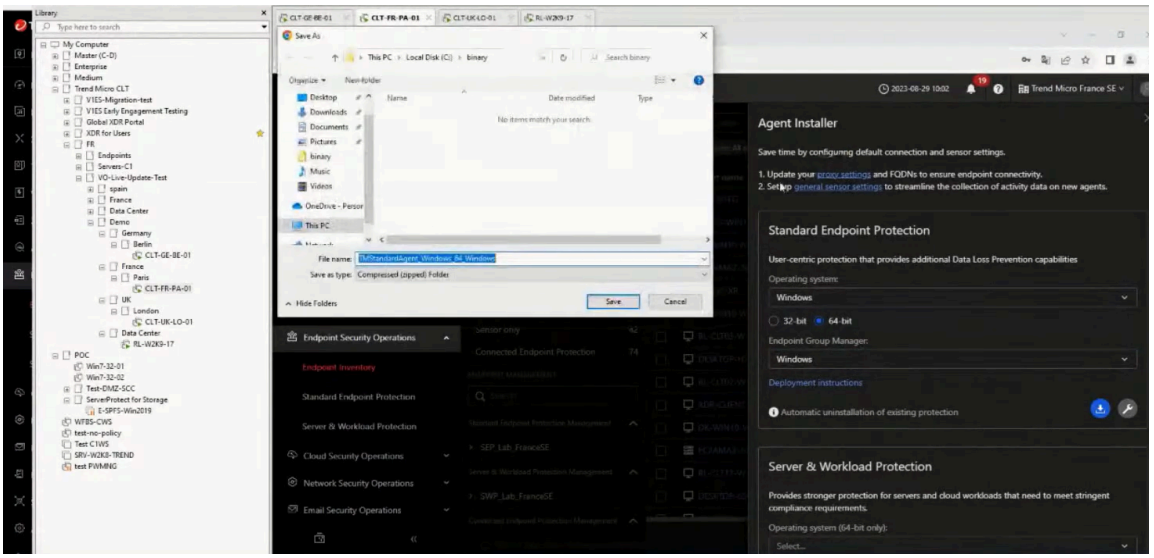

Рис. 3.19. Завантаження стандартного захисту кінцевих точок для Берлінського офісу

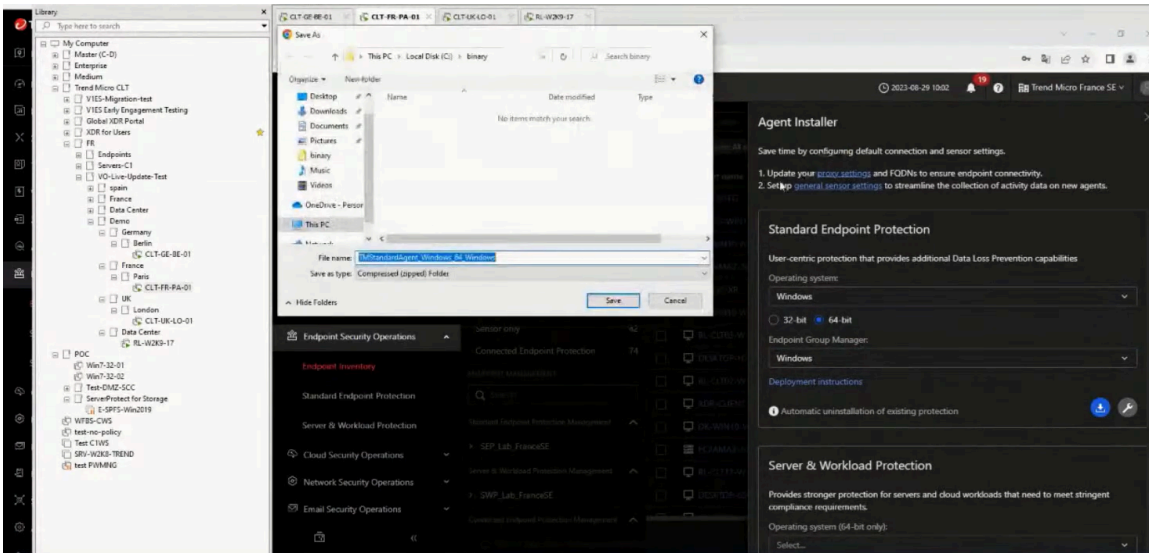

Рис. 3.20. Завантаження стандартного захисту кінцевих точок для Паризького офісу

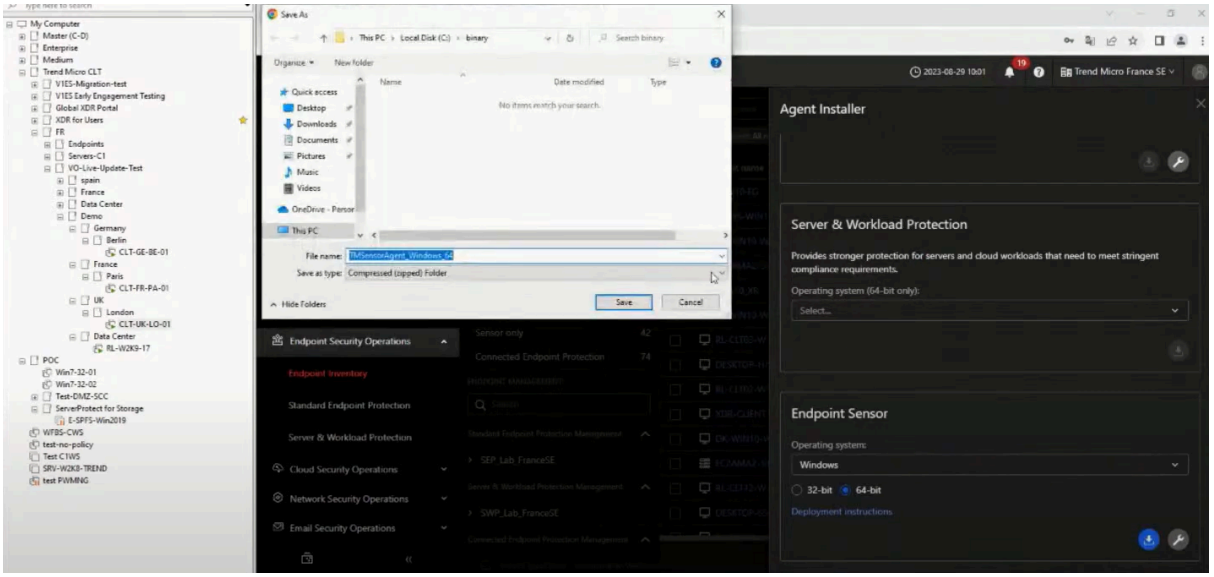

Рис. 3.21. Завантаження сенсора кінцевих точок для Лондонського офісу

Потім я запускаю сервер і захист робочого навантаження, тому першим кроком буде вибір операційної системи.

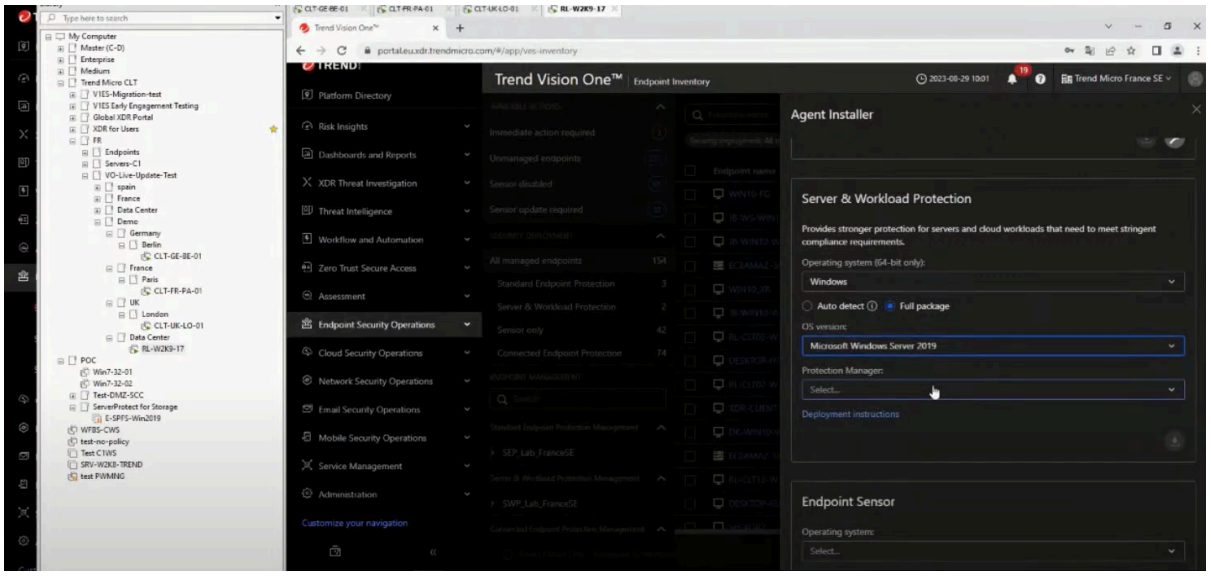

Рис. 3.22. Завантаження сервера “Microsoft Windows Server 2019”

Проводимо розпакування для всі чотирьох файлів.

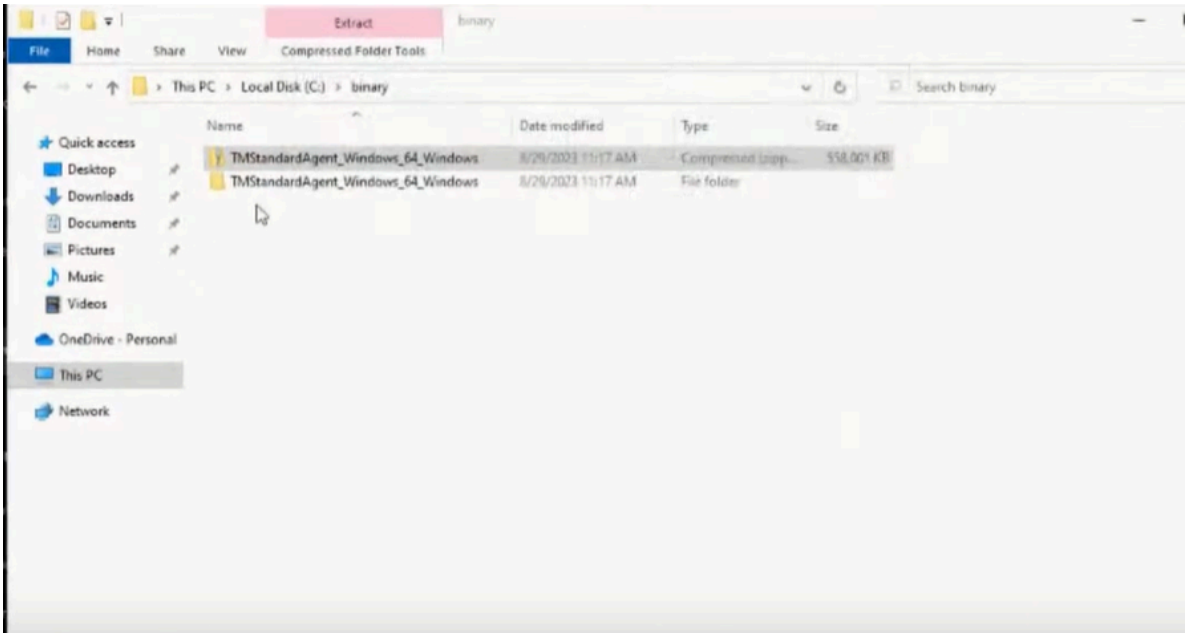

Рис. 3.23. Розпаковуємо zip-файл завантажений

Заходимо в розпакований фай так відкриваємо консоль “cmd”з правами адміністратора. Потім у водимо таку команду C:\binary\TMSstandardAgent_Windows_64_Windows > EndpointBasecamp.exe для з’єднання між моєю кінцевою точкою та інфраструктурою Trend Micro.

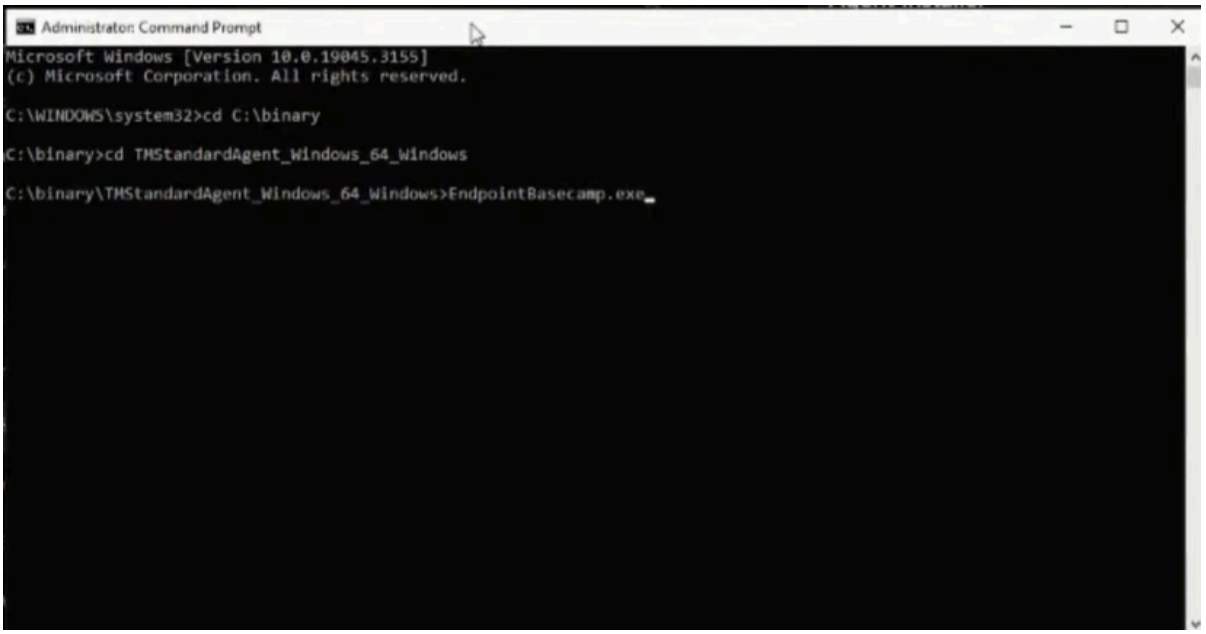

Рис. 3.24. Запуск файла “EndpointBasecamp.exe.”

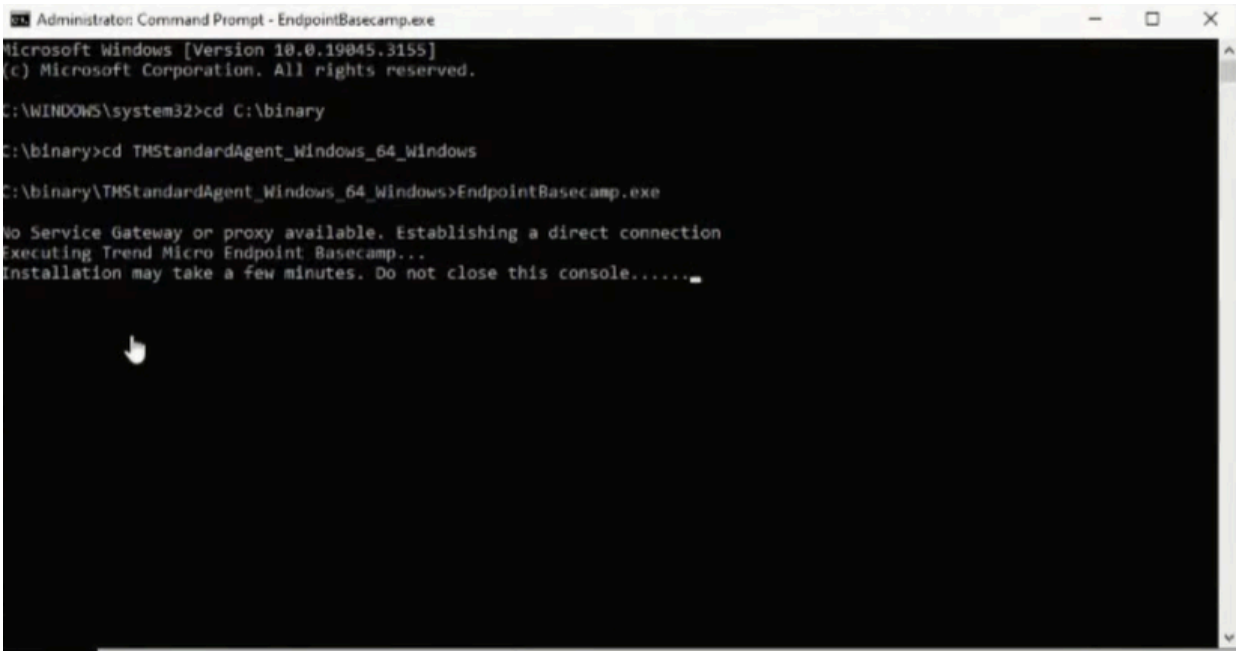

Рис. 3.25. Проводиться підключення до Trend Micro One.

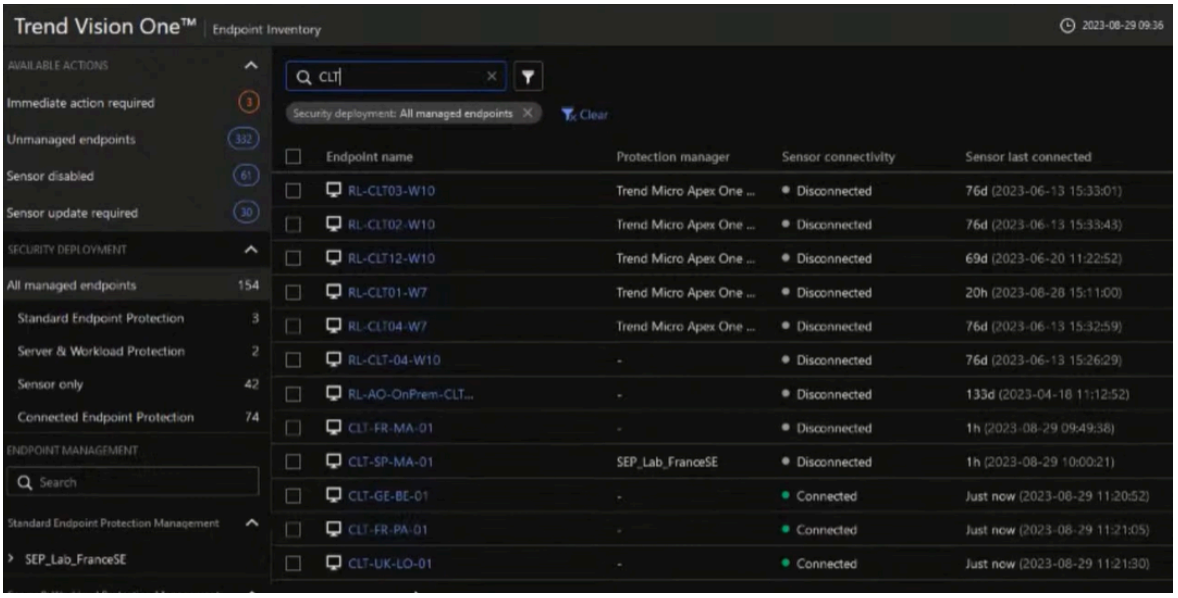

Рис. 3.26. Заходим Endpoint Inventory проводим фільтрацію “CLT” останні 3 бачимо що були з'єднані.

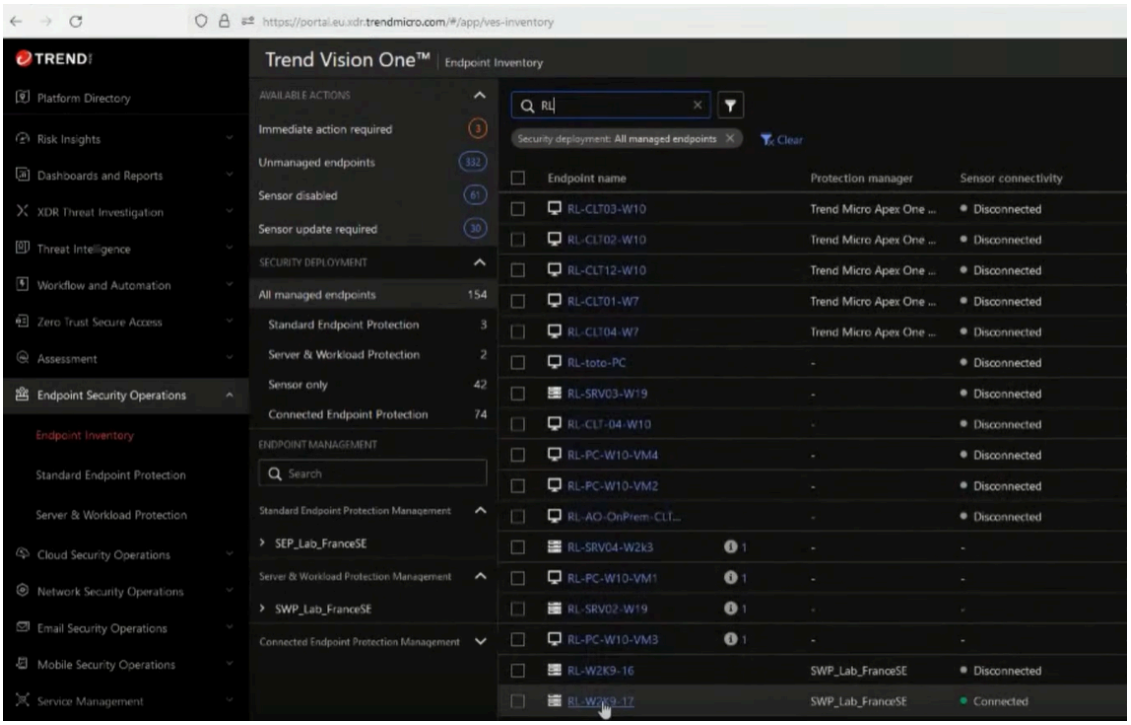

Рис. 3.27. Заходим Endpoint Inventory проводим фільтрацію “RL” останній бачимо що був з'єднаний

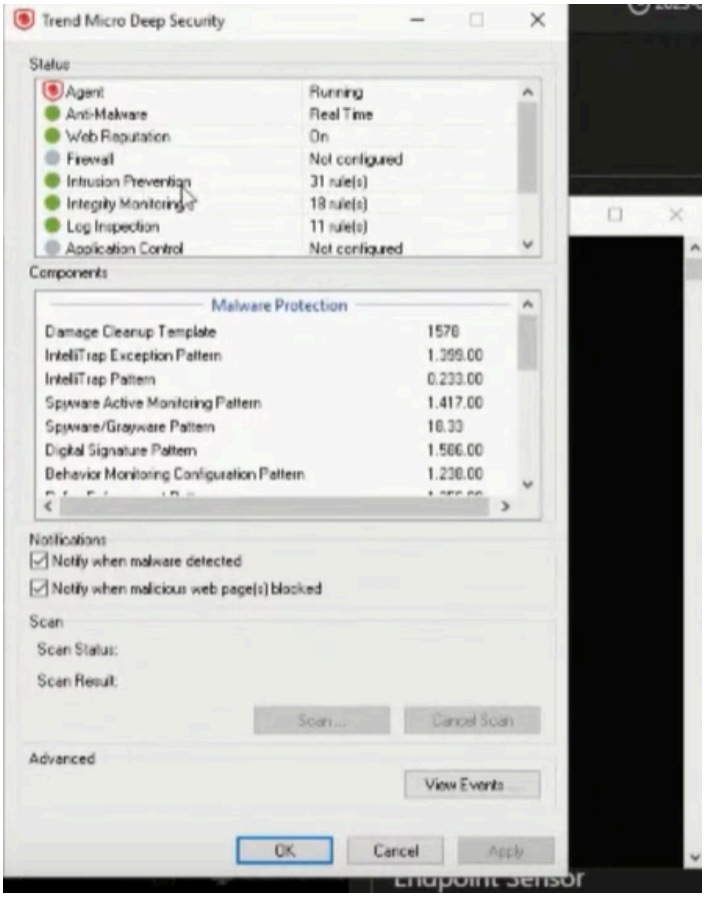

Рис. 3.28. Піктограма Apex

Переходимо на Trend Vision One та заходимо Server and workload protection > Computers, потім знаходимо свій комп'ютер. Бачимо ті ж самі дані щой в піктограмі Apex

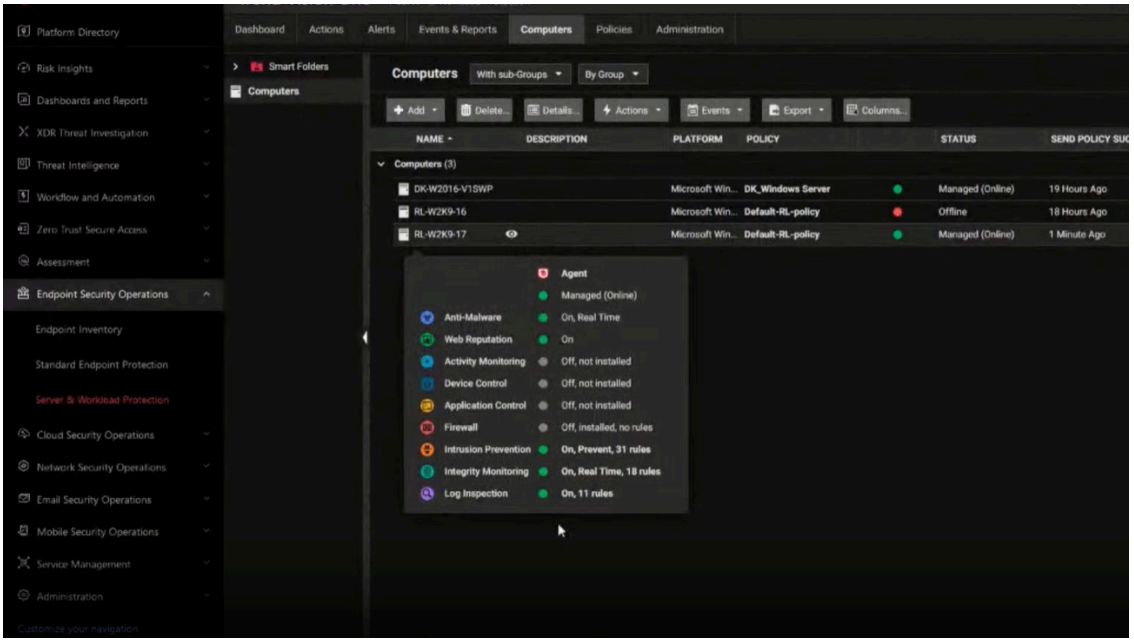

Рис. 3.29. Піктограма Apex вже Trend Vision One

Під час виконання завдання з встановлення та налаштування агентів у Trend Vision One було здійснено всебічне дослідження функціональних можливостей платформи. Встановлення різних агентів — стандартного захисту кінцевих точок, сенсора кінцевих точок, а також захисту серверів та робочих навантажень — дозволило оцінити гнучкість і багатофункціональність інфраструктури Trend Micro.

У ході роботи було встановлено стандартний захист кінцевих точок для Берлінського та Паризького офісів, сенсор кінцевих точок для Лондонського офісу. Налаштовано сервер і захист робочих навантажень для операційної системи Microsoft Windows Server 2019. Проведено інтеграцію кінцевих точок із інфраструктурою Trend Micro через виконання команди у консольному інтерфейсі, що забезпечило успішне підключення агентів.

Trend Vision One підтвердила високу якість її функціоналу. Інтуїтивно зрозумілий процес налаштування. Можливість гнучкого вибору агентів відповідно

до потреб організації. Легкий доступ до інформації через Trend Vision One, що відображає дані, зібрані агентами та сервером.

Платформа Trend Vision One підтвердила свою ефективність для забезпечення комплексного захисту кінцевих точок, серверів і робочих навантажень, що робить її чудовим вибором для впровадження в сучасній IT-інфраструктурі.

3.3 Рекомендації щодо застосування технології виявлення та реагування на загрози на основі Trend Vision One

Trend Vision One є платформою, яка спеціалізована для захисту від загроз, забезпечує додаткову цінність і нові переваги понад рішення XDR, дозволяючи бачити більше та реагувати швидше. Завдяки розширеним можливостям XDR (розширеного виявлення та реагування), які збирають і автоматично співвідносять дані з різних рівнів безпеки — електронної пошти, кінцевих точок, серверів, хмарних робочих навантажень і мереж — Trend Micro Vision One запобігає більшості атак завдяки автоматизованому захисту [19]. Нижче наведено ключові рекомендації щодо ефективного застосування Trend Vision One.

1. Інтеграція з існуючими системами безпеки

XDR для централізованого контролю: Використання Extended Detection and Response (XDR) дозволяє об'єднати різні системи та джерела даних (мережі, кінцеві точки, сервери, хмари) в єдину платформу, що значно покращує координацію та ефективність реагування.

API-інтеграція: Trend Vision One забезпечує API для інтеграції з іншими інструментами безпеки, такими як SIEM або SOAR, що допомагає автоматизувати та оптимізувати процеси реагування.

2. Постійне оновлення та адаптація під нові загрози

Оновлення на основі загрозового інтелекту: Постійні оновлення дозволяють платформі інтегрувати останні дані про загрози з глобальних мережевих джерел та адаптуватися до нових типів атак. Це дозволяє уникати вразливостей від нових шкідливих програм та сценаріїв атак.

Автоматичне самонавчання системи: Використання штучного інтелекту та машинного навчання дозволяє платформі самонавчатися на основі нових загроз, що були виявлені, та автоматично оптимізувати алгоритми виявлення.

3. Проактивний моніторинг і аналіз поведінки

Поведінковий аналіз користувачів і пристроїв: Trend Vision One дозволяє вести моніторинг поведінки як користувачів, так і пристроїв, щоб виявляти потенційні відхилення, які можуть свідчити про загрозу. Це допомагає виявляти навіть складні атаки, які можуть проходити непомітними для традиційних систем.

Аналітика поведінкових аномалій: Рекомендовано регулярно проводити аналіз на основі поведінкових даних, щоб швидко виявляти нові загрози та уникати шкідливих впливів на систему.

4. Проактивне прогнозування загроз

Використання ШІ для прогнозування загроз: Вбудовані алгоритми штучного інтелекту здатні аналізувати значні обсяги даних, щоб передбачити можливі атаки. Рекомендовано налаштувати проактивне повідомлення про потенційні загрози, що дозволяє команді з безпеки завчасно діяти.

Аналіз тенденцій та адаптація: Рекомендовано регулярно оновлювати налаштування системи відповідно до нових тенденцій загроз, що дає змогу підвищити рівень захищеності в умовах постійного розвитку кіберзагроз.

5. Оптимізація процесу реагування та відновлення

Автоматизація інцидентів безпеки: Використання можливостей автоматизованого реагування дозволяє швидше нейтралізувати загрози. Trend Vision One може самостійно виконувати необхідні дії для мінімізації впливу атак.

Оперативний контроль і звітність: Рекомендовано використовувати функціонал звітності для надання командам із безпеки актуальних даних про стан системи та виявлені інциденти, що спрощує управління ризиками та прийняття стратегічних рішень.

6. Залучення багаторівневих механізмів захисту

Модульний підхід до безпеки: Trend Vision One підтримує можливість додавання нових модулів для покращення функціональності безпеки, що дозволяє

легко адаптувати рішення до потреб конкретної організації.

Багатофакторна аутентифікація та сегментація: Використання багатофакторної аутентифікації та сегментація мережі забезпечують додатковий рівень захисту та знижують ризик потенційних атак.

Trend Vision One забезпечує не лише високий рівень захисту завдяки розширеному виявленню та реагуванню на загрози, але й дозволяє організаціям проактивно прогнозувати загрози. Для оптимального застосування цієї платформи рекомендовано використовувати її модульність для адаптації під потреби компанії, постійно оновлювати систему та застосовувати AI для аналізу поведінки і прогнозування, що допоможе забезпечити високу ефективність кіберзахисту.

Висновки до розділу 3:

У третьому розділі було детально розглянуто технології виявлення та реагування на загрози за допомогою Trend Vision One. Зокрема, було описано процес реєстрації та отримання доступу до онлайн-системи Trend Vision One, а також ключові етапи встановлення та налаштування агента для ефективної роботи платформи.

Також були надані рекомендації щодо застосування технологій Trend Vision One для ефективного виявлення та реагування на загрози в різних організаційних середовищах. Визначено ключові фактори, які необхідно враховувати при впровадженні платформи, а також рекомендації щодо налаштувань, щоб забезпечити найвищу ефективність захисту інформаційних систем.

Таким чином, третій розділ надає цінну інформацію для впровадження технології Trend Vision One в рамках комплексної стратегії кіберзахисту, а також підкреслює важливість її правильного налаштування та інтеграції для досягнення максимальної ефективності.

ВИСНОВКИ

В роботі проведено дослідження актуальності проблеми, визначено його мету та завдання.

Проаналізовано основні типи загроз у сучасному кіберпросторі, включаючи кіберзлочинність, шкідливе програмне забезпечення та атаки із застосуванням соціальної інженерії, а також труднощі їх виявлення через швидкий розвиток технологій.

Розглянуто різні типи систем і ключові підходи до виявлення та реагування на загрози, кожен з яких має свої переваги. IDR та EDR фокусуються на виявленні загроз на кінцевих пристроях, XDR забезпечує інтеграцію даних з різних джерел для кращого огляду, а SIEM збирає та аналізує журнали подій для виявлення інцидентів по всій інфраструктурі.

Проаналізовано, як сучасні технології штучного інтелекту та машинного навчання підвищують ефективність виявлення складних загроз, автоматизують процеси та прискорюють реагування.

Досліджено методи та засоби забезпечення виявлення та реагування на загрози в інформаційній безпеці на базі платформи Trend Vision One. Визначено основне призначення, ключові функції та архітектурні особливості рішення Trend Vision One.

Платформа Trend Vision One забезпечує інтегроване виявлення та реагування на загрози завдяки використанню розширеного виявлення і реагування (XDR), аналізу поведінки користувачів і пристроїв (UEBA) та автоматизованого управління інцидентами безпеки. Платформа застосовує штучний інтелект та алгоритми машинного навчання для аналізу великих обсягів даних, визначення складних загроз та їхньої швидкої нейтралізації.

На основі досліджень, проведених у роботі, запропоновано порядок використання платформи Trend Vision One для забезпечення кіберзахисту організацій.

Функції безпеки Trend Vision One можна гнучко налаштовувати відповідно до потреб організації. Особливості платформи, такі як централізоване управління та створення агента, були детально розглянуті в цій роботі.

Trend Vision One надає організаціям комплексний захист від кіберзагроз, інтегруючи дані з різних джерел, застосовуючи аналітику штучного інтелекту та підтримуючи автоматизацію процесів. Платформа дозволяє ефективно виявляти, реагувати на загрози та запобігати їм, забезпечуючи захист активів як у локальних, так і в хмарних середовищах.

Розроблено рекомендації щодо використання технології виявлення та реагування на загрози за допомогою Trend Vision One. Надаються рекомендації щодо оптимізації роботи платформи, підвищення її ефективності та адаптації до специфічних потреб організації.

Таким чином, зроблено висновки про ефективність платформи Trend Vision One у виявленні та реагуванні на загрози, а також надано рекомендації щодо її впровадження в організаціях для підвищення рівня кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Апробація: М. В. Грайворонський «Теоретичні і прикладні проблеми фізики, математики та інформатики» Київ: НТУУ «КПІ». 2015. 21-23 травня 2015 ст. 10-17.

2. Стратегія кібербезпеки України URL: http://zakon3.rada.gov.ua/laws/show/96/2016 (дата звернення: 15.03.2016).

3. Класифікація кіберзагроз та їх легітимація у нормативно-правових актах україни.URL: https://goal-int.org/klasifikatsiya-kiberzagroz-ta-yih-legitimatsiya-u-normativno-pravovih-aktah-ukrayini/ (дата звернення: 13.04.2017).

4. What are Computer Viruses? URL: https://www.fortinet.com/resources/cyberglossary/computer-virus (дата звернення: 01.11.2024).

5. Types of Cyber Security Threats. URL: https://www.eset.com/uk/types-of-cyber-threats/ (дата звернення: 13.08.2024).

6. What is a Cyber Attack? URL: https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks (дата звернення: 02.11.2024).

7. Incident Detection and Response URL: https://docs.tenable.com/cyber-exposure-studies/nis-2-directive/Content/IncidentDetectionAndResponse.htm (дата звернення: 03.10.2023).

8. What is Incident Detection and Response? URL: https://www.rapid7.com/blog/post/2016/03/29/what-is-incident-detection-and-response/ (дата звернення: 07.09.2024).

9. Learn how Endpoint Detection and Response (EDR) security can improve protection for your organization. URL: https://www.fortinet.com/resources/cyberglossary/what-is-edr (дата звернення: 26.10.2023).

10. What is Endpoint Detection and Response (EDR)? URL: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detec

tion-and-response-edr/ (дата звернення: 26.10.2023).

11. Threat Detection and Response Systems (IDR, EDR, and XDR). URL: https://headsec.tech/posts/idredrxdr/ (дата звернення: 16.03.2023).

12. Що таке управління інформаційною безпекою та подіями (SIEM) і чому це важливо? URL: https://eska.global/blog/sho-take-upravlinnya-informacijnoyu-bezpekoyu-ta-podiyami-siem-i-chomu-ce-vazhlivo (дата звернення: 05.08.2022).

13. What Is Security Information and Event Management (SIEM)? Definition, Architecture, Operational Process, and Best Practices URL: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-siem/ (дата звернення: 24.02.2022).

14. What is artificial intelligence (AI)? URL: https://www.iso.org/artificial-intelligence/what-is-ai (дата звернення: 22.05.2024).

15. Застосування штучного інтелекту: сфери, приклади, переваги та труднощі URL: https://university.sigma.software/where-is-artificial-intelligence-used/ (дата звернення: 22.10.2024).

16. Trend Vision One: A Platform Attracting 10k Enterprise Users URL: https://cybermagazine.com/articles/trend-vision-one-the-platform-winning-10k-enterprise-users (дата звернення: 04.08.2024).

17. Trend Micro & Elcore & Crayon URL: https://www.crayon.com/ua/resources/events/trendmicro_10november/ (дата звернення: 10.11.2024).

18. Solution Brochure Trend Vision One™ URL: www.trendmicro.com/en_us/business/products/one-platform.html?modal=s8a-btn-readsoln-brief-38e459 (дата звернення: 26.09.2023).

19. History, Vision, and Values URL: https://www.trendmicro.com/en_us/about/history-vision-values.html (дата звернення: 10.11.2024).

20. What is Trend Vision One? URL: https://www.softwarereviews.com/products/trend-vision-one?c_id=391

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)