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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо захисту робочих станцій від загроз нульового дня на базі eset endpoint security.»

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

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

Виконав: здобувач вищої освіти групи БСД-43
Таранов Владислав
(прізвище, ім'я)

Керівник к.військ.н., доцент ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 53 сторінки, 14 рисунків, 11 джерел.

Об'єкт дослідження – захист кінцевих точок організації від загроз нульового дня.

Предмет дослідження – методи та засоби захисту кінцевих точок організації на базі ESET Endpoint Security.

Мета роботи – розробити рекомендації щодо виявлення вразливостей нульового дня на кінцевих точках підприємства за допомогою ESET Endpoint Security.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

У роботі досліджено проблему захисту кінцевих точок організації, визначено його мету та завдання. Проведено аналіз існуючих методів та засобів захисту кінцевих точок організації, а також досліджено методи та засоби захисту кінцевих точок організації на базі ESET Endpoint Security. На основі проведених досліджень запропоновано варіант системи на базі ESET Endpoint Security та розроблено рекомендації щодо реалізації методів та засобів захисту кінцевих точок організації.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ, КІНЦЕВІ ТОЧКИ, ЗАХИСТ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ, ЗАГРОЗИ НУЛЬОВОГО ДНЯ.

ЗМІСТ

Стор.

ВСТУП.....9
1 ДОСЛІДЖЕННЯ ПОТОЧНИХ ПРОБЛЕМ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ ТА ЗАГРОЗ НУЛЬОВОГО ДНЯ НА КІНЦЕВИХ ТОЧКАХ ПІДПРИЄМСТВА..... 11
1.1 Аналіз проблеми забезпечення захисту кінцевих точок організації..... 11
1.2 Аналіз вимог міжнародних стандартів забезпечення виявлення кіберзагроз на корпоративних кінцевих точках.....16
1.3 Мета та завдання виявлення загроз нульового дня на кінцевих точках підприємства.....20
1.4 Аналіз існуючих засобів виявлення загроз нульового дня на кінцевих точках підприємства.....23
2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ЗАГРОЗ НУЛЬОВОГО ДНЯ НА КІНЦЕВИХ ТОЧКАХ ПІДПРИЄМСТВА НА БАЗІ ESET ENDPOINT SECURITY..... 26
2.1 Рішення компанії ESET щодо виявлення кіберзагроз і загроз нульового дня на кінцевих точках підприємства.....26
2.2 Призначення, основні функції та склад комплексу виявлення загроз нульового дня на кінцевих точках підприємства на базі ESET Endpoint Security.....31
2.3 Реалізація технології виявлення загроз нульового дня на кінцевих точках підприємства в рішенні ESET Endpoint Security.....35
3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ НУЛЬОВОГО ДНЯ НА КІНЦЕВИХ ТОЧКАХ ПІДПРИЄМСТВА ЗА ДОПОМОГОЮ ESET ENDPOINT SECURITY..... 38
3.1 Порядок розгортання рішення ESET Endpoint Security і додавання кінцевих точок до мережі ESET PROTECT.....38
3.2 Алгоритм реалізації виявлення загроз нульового дня на кінцевих точках підприємства на базі ESET Endpoint Security.....45
3.3 Розроблення рекомендацій щодо виявлення загроз нульового дня на кінцевих точках підприємства на базі ESET Endpoint Security.....46
ВИСНОВКИ..... 49
ПЕРЕЛІК ПОСИЛАНЬ.....51
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ.....53

ВСТУП

Актуальність дослідження: Сучасне бізнес-середовище невтомно конфронтується з загрозами кібербезпеки, особливо в контексті зростаючої кількості атак на кінцеві точки підприємств. Захист кінцевих точок, таких як робочі станції, ноутбуки та сервери, є критичним компонентом загальної стратегії кібербезпеки будь-якої організації. Особливе значення має захист від загроз нульового дня, які використовують невідомі уразливості в програмному забезпеченні і можуть призвести до значних втрат даних та збоїв у роботі систем.

ESET Endpoint Security є комплексним рішенням для захисту кінцевих точок в корпоративних мережах, що забезпечує високий рівень безпеки та надійності. Використовуючи продуктивні алгоритми машинного навчання та штучного інтелекту, ESET Endpoint Security забезпечує постійний моніторинг системи на предмет потенційно небезпечних активностей, що дозволяє оперативно реагувати на загрози та мінімізувати ризики для бізнесу.

Вищесказане визначає актуальність теми цієї кваліфікаційної роботи полягає у дослідженні методів і засобів захисту кінцевих точок організації від загроз нульового дня на базі ESET Endpoint Security. Дослідження спрямоване на аналіз і розробку рекомендацій щодо ефективного використання ESET Endpoint Security як рішення для забезпечення кібербезпеки кінцевих точок підприємства.

Це дослідження спрямоване на аналіз та розробку рекомендацій щодо ефективного використання ESET Endpoint Security як рішення для забезпечення кібербезпеки кінцевих точок підприємства.

Об’єкт дослідження: процеси захисту кінцевих точок підприємства від загроз нульового дня.

Предмет дослідження: методи та засоби захисту кінцевих точок підприємства від загроз нульового дня на основі ESET Endpoint Security.

Мета роботи: розробити рекомендації щодо виявлення загроз нульового дня на кінцевих точках підприємства за допомогою ESET Endpoint Security.

Наукові завдання:

дослідити поточні проблеми виявлення загроз нульового дня на кінцевих точках підприємства;

проаналізувати наукову та технічну літературу з питань теми кваліфікаційної роботи;

проаналізувати проблематику виявлення загроз нульового дня на кінцевих точках підприємства;

проаналізувати методи та засоби виявлення загроз нульового дня на кінцевих точках підприємства на базі ESET Endpoint Security;

розробити рекомендації щодо виявлення загроз нульового дня на кінцевих точках підприємства за допомогою ESET Endpoint Security.

Методи дослідження - опрацювання літератури заданою темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано рекомендації фахівцям з кібербезпеки щодо забезпечення безпечного доступу гібридних працівників до корпоративних додатків.

1 ДОСЛІДЖЕННЯ ПОТОЧНИХ ПРОБЛЕМ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ ТА ЗАГРОЗ НУЛЬОВОГО ДНЯ НА КІНЦЕВИХ ТОЧКАХ ПІДПРИЄМСТВА

1.1 Аналіз проблеми забезпечення захисту кінцевих точок організації

Захист кінцевих точок, таких як робочі станції, ноутбуки, мобільні пристрої та сервери, є критичним компонентом загальної стратегії кібербезпеки будь-якої організації. Кінцеві точки часто є основними цілями для кібератак, оскільки вони можуть служити вхідними точками для зловмисників, які прагнуть отримати доступ до мережі організації та її даних. Атаки на кінцеві точки можуть охоплювати такі загрози, як шкідливе ПЗ, фішингові атаки, експлойти вразливостей, програми-вимагачі та складніші цільові атаки (APT).

Основні проблеми і тенденції в цій галузі включають:

зростання кількості та складності загроз - зловмисники використовують дедалі витонченіші методи атак, як-от фішинг, шкідливе ПЗ і цільові атаки. Найпоширенішими темами фішингових листів стали "Замовлення", "Оплата", "Купівля" і "Рахунок". Шкідливі програми можуть проникати в системи через уразливості та дозволяти зловмисникам отримувати віддалений доступ;

різноманітність пристроїв і платформ - сучасні організації використовують широкий спектр пристроїв, що працюють на різних операційних системах і платформах. Це розмаїття ускладнює управління безпекою, тому що кожен пристрій може мати свої вразливості і вимагає спеціальних засобів захисту;

збільшення кількості кінцевих точок - зростання кількості мобільних пристроїв, ноутбуків і віддалених робочих місць розширює поверхню атаки. Кожне робоче місце і підключене обладнання є потенційною точкою входу для зловмисників. Дистанційна робота, що практикується багатьма компаніями, також підвищує ризики;

брак кваліфікованих кадрів - організаціям складно знайти й утримати фахівців із кібербезпеки, здатних протистояти сучасним загрозам. Це призводить до недостатнього захисту кінцевих точок;

необхідність нових інструментів захисту - традиційні засоби захисту, такі як файрволи й антивіруси, не справляються з новими видами атак. Потрібні рішення класу Endpoint Detection and Response (EDR), здатні виявляти і запобігати складним загрозам;

оновлення та патч-менеджмент - оновлення програмного забезпечення та своєчасне застосування патчів є основними методами запобігання використанню відомих вразливостей. Однак, управління оновленнями на великій кількості пристроїв може бути складним завданням, особливо у великих організаціях.

Захист кінцевих точок є найважливішим аспектом загальної стратегії кібербезпеки організації. З урахуванням поточних і нових загроз, використання комплексних рішень, як-от ESET Endpoint Security, у поєднанні з методами моніторингу, навчання користувачів і управління оновленнями, дає змогу створити надійний захисний периметр і знизити ризики кібератак.

Статистична інформація про загрози наведена в таблиці 1.1 і рисунку 1.1.

Таблиця 1.1 [1]

Кваліфікація та розподіл загроз для кінцевих точок організації за роками (2022-2024)

Критерії загроз	Види загроз	2022 (%)	2023 (%)	2024 (%)
Шкідливе ПЗ	Віруси	10	9	8
	Хробаки	8	7	6
	Трояни	11	10	7
	Шпигунське ПЗ	5	4	4
	Програми-вимагачі	13	15	18
Загрози на основі мережі	DDoS атаки	9	9	8
	Міжмережеві атаки	7	6	6
	Експлойти	8	10	12
Соціальна інженерія	Фішинг	12	11	10

Критерії загроз	Види загроз	2022 (%)	2023 (%)	2024 (%)
	Вішинг	3	4	5
	Смішинг	2	3	4
Внутрішні загрози	Недозволені дії співробітників	3	2	1
	Витік даних	9	10	11

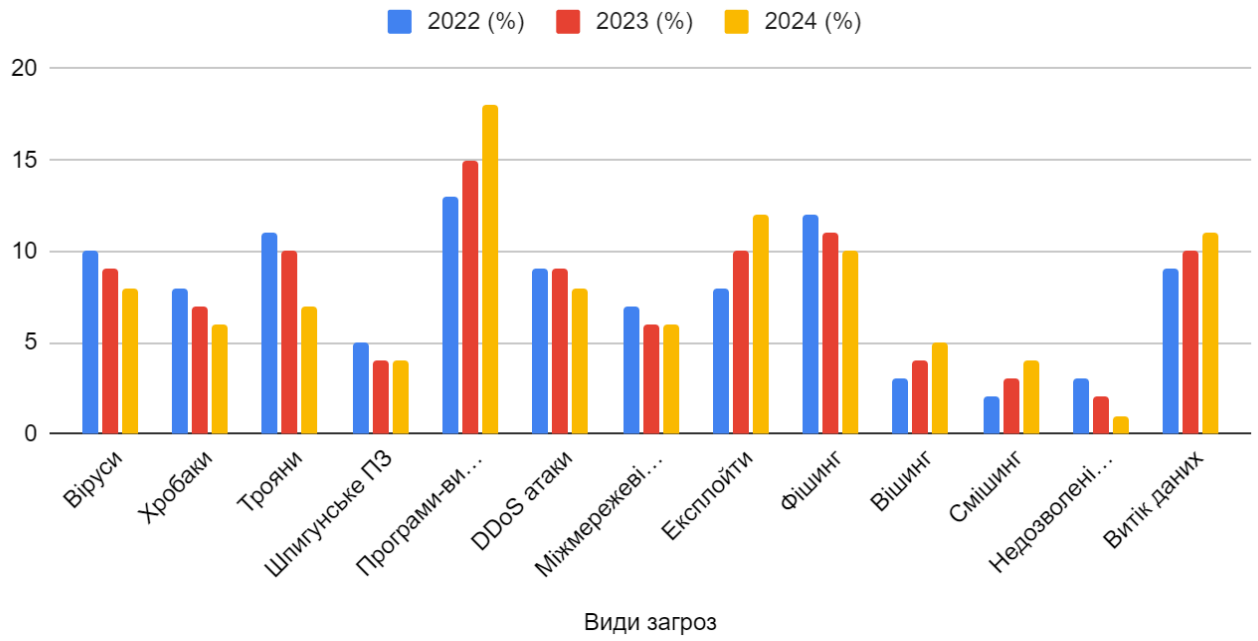

Рис. 1.1 - Класифікація та розподіл загроз для кінцевих точок організації за роками (2022-2024)

Основні тенденції:

програми-вимагачі (Ransomware) продовжують зростати, оскільки вони стають дедалі популярнішими серед кіберзлочинців;

фішинг залишається найпоширенішою формою соціальної інженерії, проте його частка трохи знижується в міру збільшення обізнаності користувачів;

експлойти збільшують свою частку в загальній кількості загроз, що пов'язано зі зростанням складності та частоти цільових атак;

шкідливе ПЗ, таке як віруси і хробаки, поступово знижують свою актуальність порівняно з більш сучасними загрозами, такими як програми-вимагачі та експлойти.

Нижче наведена таблиця 1.2 з конкретними прикладами загроз, з якими стикалися організації та опис наслідків інцидентів.

Таблиця 1.2

Приклади кіберзагроз

Кіберзагроза	Приклад інциденту	Наслідки інциденту
Віруси	Вірус ILOVEYOU, який поширився через електронну пошту в 2000 році	Втрати даних, паралізація роботи організацій, фінансові втрати (понад $10 млрд)
Хробаки	Хробак WannaCry, що використовував вразливість в Windows у 2017 році	Зашифровані дані, вимагання викупу, значні фінансові втрати, призупинення роботи систем
Трояни	Троянський кінь Zeus, який викрадав банківські дані	Викрадення конфіденційних даних, фінансові втрати, компрометація рахунків
Програми-вимагачі	Програма-вимагач Petya, що атакувала глобальні компанії у 2017 році	Зашифровані дані, зупинка операційної діяльності, великі фінансові збитки
Фішинг	Фішингова атака на організацію Target у 2013 році	Викрадення даних кредитних карток мільйонів клієнтів, втрати репутації, фінансові збитки
DDoS атаки	DDoS атака на сервіс Dyn у 2016 році	Недоступність багатьох популярних веб-сайтів, фінансові втрати, порушення роботи сервісів
Експлойти	Експлойт EternalBlue, використаний у атаках WannaCry і NotPetya	Широкомасштабні зараження систем, вимагання викупу, зупинка критично важливих сервісів
Недозволені дії співробітників	Витік даних з Facebook через компанію Cambridge Analytica у 2018 році	Викрадення персональних даних, втрати репутації, великі штрафи

Пояснення до таблиці 1.2:

віруси: вірус ILOVEYOU поширювався через електронні листи, спричиняючи значні фінансові збитки та паралізуючи роботу багатьох організацій по всьому світу;

хробаки: WannaCry використовував вразливість у Windows для шифрування даних та вимагання викупу, призупиняючи роботу численних систем;

трояни: Троян Zeus був спрямований на викрадення банківських даних, що призводило до фінансових втрат та компрометації рахунків;

програми-вимагачі: Petya зашифрувала дані на комп’ютерах жертв, зупиняючи операційну діяльність та завдаючи значних фінансових збитків;

фішинг: Атака на Target призвела до викрадення даних кредитних карток, що спричинило втрати репутації та фінансові збитки;

DDoS атаки: Атака на сервіс Dyn зробила багато популярних веб-сайтів недоступними, порушуючи роботу сервісів та завдаючи фінансових втрат;

експлойти: EternalBlue був використаний у атаках WannaCry і NotPetya, що призвело до широкомасштабного зараження систем та вимагання викупу;

недозволені дії співробітників: Витік даних з Facebook через Cambridge Analytica викликав втрати репутації та великі штрафи через викрадення персональних даних.

Приклади Zero-day атак за 2024 рік [2,3,4]:

Microsoft Windows Zero-Days: У квітні 2024 року Microsoft виправила дві активно експлуатовані вразливості. Перша, CVE-2024-26234, була пов'язана з підробкою проксі-драйвера, виявленого в шкідливому драйвері, підписаному дійсним сертифікатом Microsoft Hardware Publisher; друга, CVE-2024-29988, дозволяла обходити функцію захисту SmartScreen і була використана для розповсюдження шкідливого ПЗ, включаючи кампанії Water Hydra, спрямовані на фінансовий сектор [2,3,4];

QakBot Malware: У травні 2024 року Microsoft виправила вразливість, яка використовувалася для поширення шкідливого ПЗ QakBot на вразливих системах Windows; атака була спрямована на доставку різних шкідливих завантажень на інфіковані комп'ютери [5];

Safari WebKit Zero-Day: У березні 2024 року під час хакерського змагання Pwn2Own була виявлена та виправлена уразливість нульового дня в Safari, яка використовувалася для експлуатації веб-переглядача [6];

Google Chrome Zero-Day: У травні 2024 року Google випустила оновлення для Chrome, щоб виправити шосту за рік вразливість нульового дня, яка активно використовувалася у атаках [6];

Cisco ASA and FTD Zero-Days: У квітні 2024 року компанія Cisco повідомила про експлуатацію двох уразливостей нульового дня у їхніх системах Adaptive Security Appliance (ASA) і Firepower Threat Defense (FTD), які використовувалися для зламування державних мереж по всьому світу з листопада 2023 року [6].

Ці інциденти підкреслюють важливість регулярного оновлення систем безпеки та впровадження заходів для захисту від нових загроз.

Отже захист кінцевих точок є ключовим аспектом кібербезпеки організації, оскільки ці точки часто стають головними цілями для кібератак. Аналіз показав, що зростаюча кількість та складність загроз, різноманітність пристроїв і платформ, збільшення кількості кінцевих точок, брак кваліфікованих кадрів і необхідність нових інструментів захисту ускладнюють завдання забезпечення безпеки. Використання комплексних рішень, таких як ESET Endpoint Security, є критично важливим для створення надійного захисного периметру.

1.2 Аналіз вимог міжнародних стандартів забезпечення виявлення кіберзагроз на корпоративних кінцевих точках

У цій галузі забезпечення безпеки кінцевих точок у корпоративному середовищі важливу роль відіграють міжнародні стандарти, що надають рекомендації та вимоги для виявлення та запобігання кіберзагрозам. Найважливіші стандарти, які стосуються цієї теми:

ISO/IEC 27001:2013 [7]:

опис: міжнародний стандарт для систем управління інформаційною безпекою (СУІБ). Він містить вимоги до створення, впровадження, підтримання та поліпшення системи управління інформаційною безпекою;

ключові аспекти: оцінка ризиків безпеки, впровадження контролів для управління ідентифікованими ризиками, безперервне поліпшення процесів безпеки.

NIST SP 800-53 Revision 5 [8]:

опис: посібник з безпеки комп'ютерних систем, розроблений Національним інститутом стандартів і технологій (NIST) США. Воно пропонує каталог заходів безпеки та конфіденційності для федеральних інформаційних систем і організацій.

ключові аспекти: управління ідентифікацією та доступом, захист від шкідливого коду, виявлення та реагування на інциденти, безперервний моніторинг безпеки.

CIS Controls Version 8 [9]:

опис: список передових методів з кібербезпеки, розроблений Центром інтернет-безпеки (CIS). Контроли діляться на основні, базові та організаційні заходи.

ключові аспекти: інвентаризація та управління активами, контроль використання адміністративних привілеїв, захист даних, виявлення та реагування на інциденти.

MITRE ATT&CK Framework [10]:

опис: модель і база знань для опису дій супротивника, які можна використовувати для поліпшення безпеки, управління загрозами та захисту кінцевих точок.

ключові аспекти: тактики, техніки і процедури (TTPs) противника, методи виявлення атак, управління загрозами на основі даних реальних атак.

GDPR (General Data Protection Regulation) [11]:

опис: регламент Європейського союзу про захист даних, який містить вимоги до обробки та захисту персональних даних.

ключові аспекти: оцінювання та управління ризиками для даних, заходи захисту даних за замовчуванням і за проектом, виявлення та повідомлення про порушення даних.

Міжнародні стандарти забезпечення виявлення кіберзагроз на корпоративних кінцевих точках надають великий набір рекомендацій і вимог, спрямованих на підвищення рівня безпеки. Вони охоплюють такі ключові області:

оцінювання та управління ризиками: регулярне оцінювання ризиків і впровадження контролів для їхнього пом'якшення є основоположними елементами всіх розглянутих стандартів;

виявлення та реагування на інциденти: безперервний моніторинг, виявлення інцидентів і адекватне реагування на них відіграють критичну роль у захисті кінцевих точок;

контроль доступу та привілеїв: управління доступом до інформації та систем, а також мінімізація використання адміністративних привілеїв допомагають знизити ризики;

захист даних: захист даних, зокрема особистих даних, є важливою частиною всіх стандартів, особливо в контексті відповідності вимогам GDPR.

безперервне поліпшення: усі стандарти наголошують на необхідності постійного поліпшення процесів безпеки для адаптації до нових загроз і змін у технології;

Таблиця 1.3

Порівняльна таблиця стандартів

Стандарт	Ключові вимоги	Сфера застосування
ISO/IEC 27001	Оцінка ризиків, впровадження контролів, неперервне покращення системи управління інформаційною безпекою (СУІБ)	Загальна інформаційна безпека в організаціях
NIST SP 800-53	Управління ідентифікацією та доступом, захист від шкідливого ПЗ, виявлення та реагування на інциденти, неперервний моніторинг	Федеральні інформаційні системи та організації США
CIS Controls	Інвентаризація та управління активами, контроль використання адміністративних привілеїв, захист даних, виявлення та реагування на інциденти	Передові методи кібербезпеки для всіх типів організацій
MITRE ATT&CK	Тактики, техніки та процедури (TTPs) противника, методи виявлення атак, управління загрозами на основі даних реальних атак	Опис дій противника, поліпшення управління загрозами
GDPR	Оцінка та управління ризиками для даних, заходи захисту даних за замовчуванням і за проектом, виявлення та повідомлення про порушення даних	Захист персональних даних у Європейському Союзі

Пояснення до таблиці 1.3:

ISO/IEC 27001:

ключові вимоги: стандарт вимагає оцінки ризиків, впровадження відповідних контролів та постійного покращення процесів безпеки; метою є створення системи управління інформаційною безпекою (СУІБ), яка захищає конфіденційність, цілісність та доступність інформації;

сфера застосування: використовується для забезпечення загальної інформаційної безпеки в організаціях будь-якого типу та розміру;

NIST SP 800-53:

ключові вимоги: цей стандарт містить рекомендації щодо управління ідентифікацією та доступом, захисту від шкідливого ПЗ, виявлення та реагування на інциденти, а також неперервного моніторингу безпеки;

сфера застосування: призначений для федеральних інформаційних систем і організацій США, але також використовується як орієнтир у приватному секторі;

CIS Controls:

ключові вимоги: включає інвентаризацію та управління активами, контроль використання адміністративних привілеїв, захист даних та виявлення і реагування на інциденти;

сфера застосування: використовується як набір передових методів кібербезпеки для всіх типів організацій, від малих до великих;

MITRE ATT&CK:

ключові вимоги: описує тактики, техніки та процедури (TTPs) противника, методи виявлення атак та управління загрозами на основі реальних даних про атаки;

сфера застосування: використовується для опису дій противника, поліпшення управління загрозами та захисту кінцевих точок;

GDPR:

ключові вимоги: вимагає оцінки та управління ризиками для персональних даних, впровадження заходів захисту даних за замовчуванням і за проектом, а також виявлення та повідомлення про порушення даних;

сфера застосування: регламентує захист персональних даних у Європейському Союзі та впливає на всі організації, які обробляють дані громадян ЄС.

Отже міжнародні стандарти, такі як ISO/IEC 27001, NIST SP 800-53, CIS Controls, MITRE ATT&CK та GDPR, надають широкий спектр рекомендацій і вимог для підвищення рівня безпеки кінцевих точок. Вони включають оцінку ризиків, безперервний моніторинг, управління доступом, захист даних і постійне поліпшення процесів безпеки. Використання цих стандартів дозволяє організаціям створити надійну систему захисту і мінімізувати ризики кібератак.

1.3 Мета та завдання виявлення загроз нульового дня на кінцевих точках підприємства

Метою виявлення загроз нульового дня на кінцевих точках підприємства є забезпечення високого рівня кібербезпеки шляхом своєчасного виявлення, аналізу та нейтралізації невідомих або нових загроз, які використовують невиправлені уразливості в програмному забезпеченні.

Таблиця 1.4

Мета та завдання виявлення загроз нульового дня на кінцевих точках підприємства

Завдання	Опис	Приклади технологій та методик
Моніторинг та аналіз активностей		
Неперервний моніторинг	Впровадження систем постійного моніторингу активностей на кінцевих точках для швидкого виявлення підозрілих дій або аномалій	Системи виявлення та реагування на кінцевих точках (EDR) такі, як ESET Enterprise Inspector, SIEM-платформи (Splunk, IBM QRadar)

Завдання	Опис	Приклади технологій та методик
Аналіз поведінки	Використання технологій поведінкового аналізу для ідентифікації потенційно шкідливих дій, які можуть свідчити про загрозу нульового дня	Поведінкові аналітичні інструменти (Cylance, Darktrace), машинне навчання та AI
Ідентифікація та класифікація загроз		
Евристичний аналіз	Використання евристичних методів для виявлення нових загроз на основі аналізу поведінки програмного забезпечення	Антивірусні програми з евристичним аналізом (ESET Endpoint Security, Kaspersky)
Аналіз аномалій	Виявлення відхилень від нормальної поведінки системи або мережі, що може вказувати на наявність нульових загроз	Системи аналізу аномалій (Splunk User Behavior Analytics, Vectra AI)
Впровадження технологій проактивного захисту		
Пісочниця (Sandboxing)	Використання ізольованого середовища для безпечного виконання та аналізу підозрілих файлів та програм	Технології пісочниці (Cuckoo Sandbox, FireEye)
Штучний інтелект (AI) та машинне навчання (ML)	Впровадження AI та ML для аналізу великих обсягів даних і прогнозування нових загроз на основі поведінкових моделей	AI та ML рішення (ESET Augur, IBM Watson for Cyber Security)
Реагування на інциденти		
Автоматичне реагування	Розробка автоматизованих процедур для швидкого реагування на виявлені загрози, включаючи ізоляцію уражених кінцевих точок та видалення шкідливого ПЗ	Інструменти автоматичного реагування (Cortex XSOAR, Demisto, ServiceNow Security Operations)
Розробка планів дій	Створення детальних планів реагування на інциденти, включаючи кроки для мінімізації впливу загроз та відновлення нормальної роботи систем	Інцидент-менеджмент системи (NIST Cybersecurity Framework, ISO/IEC 27035)
Оновлення та управління патчами		

Завдання	Опис	Приклади технологій та методик
Регулярне оновлення ПЗ	Забезпечення своєчасного оновлення операційних систем та програмного забезпечення на кінцевих точках для закриття відомих уразливостей	Системи управління патчами (Microsoft WSUS, Red Hat Satellite)
Управління патчами	Використання автоматизованих інструментів для управління патчами та забезпечення оперативного виправлення уразливостей	Платформи для управління патчами (Ivanti Patch Management, SolarWinds Patch Manager)
Освіта та підвищення обізнаності користувачів		
Навчання співробітників	Проведення регулярних тренінгів для підвищення обізнаності співробітників щодо загроз нульового дня та методів їх виявлення і запобігання	Платформи для навчання (KnowBe4, Infosec IQ)
Розробка політик безпеки	Створення та впровадження політик безпечного використання корпоративних пристроїв та ресурсів	Документація політик (NIST SP 800-53, ISO/IEC 27002)
Інтеграція з іншими системами безпеки		
Централізоване управління	Інтеграція засобів виявлення загроз нульового дня з іншими системами кібербезпеки для координації заходів захисту та обміну інформацією про загрози	Централізовані консолі управління (ESET Security Management Center, Splunk)
Взаємодія з SIEM	Використання платформ SIEM для кореляції даних і забезпечення всебічного аналізу інцидентів безпеки	SIEM платформи (Splunk, IBM QRadar, ArcSight)

Отже метою виявлення загроз нульового дня є забезпечення високого рівня кібербезпеки через своєчасне виявлення, аналіз і нейтралізацію нових загроз. Завдання включають моніторинг та аналіз активностей, ідентифікацію та класифікацію загроз, впровадження проактивних технологій захисту, автоматичне реагування на інциденти, регулярне оновлення ПЗ і підвищення обізнаності користувачів. Виконання цих завдань дозволяє ефективно виявляти та нейтралізувати загрози нульового дня.

1.4 Аналіз існуючих засобів виявлення загроз нульового дня на кінцевих точках підприємства

Виявлення таких загроз нульового дня (Zero-day threats) є критичним завданням для забезпечення захисту кінцевих точок підприємства. Існує кілька основних засобів виявлення цих загроз (таблиця 1.5), кожен з яких має свої переваги, обмеження та виклики (таблиця 1.6).

Таблиця 1.5

Основні засоби виявлення загроз нульового дня

Засіб виявлення	Опис	Приклади технологій
Антивірусні програми з проактивним захистом	Використовують сигнатурний та евристичний аналіз для виявлення відомих і потенційно небезпечних програм	ESET Endpoint Security, Kaspersky, Symantec
Системи виявлення та запобігання вторгненням (IDS/IPS)	Використовують сигнатурний аналіз для виявлення відомих загроз та аналіз аномалій для виявлення нових загроз	Snort, Suricata, Palo Alto Networks
Системи виявлення та реагування на кінцевих точках (EDR)	Постійно відстежують і аналізують активність на кінцевих точках для виявлення підозрілої або аномальної поведінки	ESET Enterprise Inspector, CrowdStrike Falcon, Carbon Black
Технології штучного інтелекту (AI) та машинного навчання (ML)	Використовують алгоритми машинного навчання для аналізу великих обсягів даних і виявлення патернів, які можуть свідчити про наявність загроз	IBM Watson for Cyber Security, Darktrace, Cylance
Платформи загального управління безпекою (SIEM)	Збирають і аналізують дані з різних джерел для виявлення кореляцій, які можуть вказувати на наявність загроз	Splunk, IBM QRadar, ArcSight
Технології ізоляції браузера	Виконують веб-контент у віддаленому ізольованому середовищі для запобігання потраплянню шкідливого коду на кінцеві точки	Bromium, Menlo Security

Таблиця 1.6

Обмеження та виклики існуючих засобів виявлення загроз нульового дня

Обмеження та виклики	Опис	Можливі шляхи подолання
Обмеженість сигнатурного аналізу	Сигнатурний аналіз виявляє лише відомі загрози і неефективний проти нових, невідомих загроз нульового дня	Впровадження евристичного аналізу та поведінкових методів
Великий обсяг даних для аналізу	Аналіз великих обсягів даних може бути складним і вимагати значних обчислювальних ресурсів	Використання технологій AI та ML для автоматизації аналізу
Висока складність налаштування та управління	Налаштування та управління системами IDS/IPS і SIEM можуть бути складними і вимагати високої кваліфікації фахівців	Проведення регулярних тренінгів та навчання персоналу
Фальшиві спрацьовування	Системи можуть генерувати велику кількість фальшивих позитивних спрацьовувань, що ускладнює роботу фахівців	Вдосконалення алгоритмів аналізу аномалій та поведінкових методів
Недостатня видимість у мережі	Деякі технології можуть не забезпечувати повну видимість активностей у мережі, що ускладнює виявлення загроз	Використання багаторівневого підходу до безпеки, включаючи EDR та SIEM
Повільне оновлення сигнатур	Затримка в оновленні сигнатур може призвести до пропущення нових загроз	Впровадження хмарних репутаційних систем та автоматичних оновлень
Різноманітність пристроїв та платформ	Підприємства використовують широкий спектр пристроїв і платформ, що ускладнює забезпечення безпеки	Впровадження уніфікованих рішень для управління безпекою різних платформ

Можливі шляхи подолання викликів:

інтеграція декількох технологій: Використання комбінації різних засобів виявлення, таких як EDR, SIEM, AI та ML, для забезпечення багаторівневого захисту;

автоматизація процесів: Використання автоматизованих інструментів для управління патчами, реагування на інциденти та аналізу даних;

постійне навчання персоналу: Регулярні тренінги та навчання співробітників для підвищення їх обізнаності про нові загрози та методи їх виявлення;

використання хмарних рішень: Впровадження хмарних репутаційних систем для швидкого оновлення сигнатур та покращення ефективності виявлення загроз;

розробка та впровадження політик безпеки: Створення чітких політик безпеки для управління доступом, використанням пристроїв та реагуванням на інциденти.

Отже існуючі засоби виявлення загроз нульового дня на кінцевих точках підприємства представляють собою багаторівневий підхід, що включає комбінацію різних технологій і методів. Для ефективного виявлення та запобігання таким загрозам підприємства повинні використовувати:

антивірусні програми з проактивним захистом і пісочницями для аналізу і випробування підозрілих файлів;

системи EDR для детального моніторингу та аналізу поведінки кінцевих точок;

AI і ML технології для прогнозування і виявлення нових загроз на основі аналізу великих обсягів даних;

SIEM платформи для кореляції подій і моніторингу в реальному часі;

технології ізоляції браузера для запобігання потраплянню шкідливого ПЗ через веб-контент.

Комбінація цих засобів дозволяє підприємствам створити надійний захист від нульових загроз і мінімізувати ризик компрометації їх кінцевих точок.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ЗАГРОЗ НУЛЬОВОГО ДНЯ НА КІНЦЕВИХ ТОЧКАХ ПІДПРИЄМСТВА НА БАЗІ ESET ENDPOINT SECURITY

2.1 Рішення компанії ESET щодо виявлення кіберзагроз і загроз нульового дня на кінцевих точках підприємства

Компанія ESET пропонує комплексні рішення для виявлення та нейтралізації кіберзагроз, включаючи загрози нульового дня, на кінцевих точках підприємства. Продукти ESET надають багаторівневий захист, використовуючи передові технології для забезпечення безпеки організацій від сучасних кіберзагроз.

Таблиця 2.1

Основні компоненти та технології ESET для виявлення загроз

Технологія	Опис
Антивірус та антишпигунське ПЗ	Використовують сигнатурний та евристичний аналіз для виявлення відомих і потенційно небезпечних програм.
Хмарні репутаційні системи	Забезпечують швидке реагування на нові загрози, використовуючи інформацію з глобальної хмарної мережі ESET LiveGrid.
Виявлення та реагування на кінцевих точках (EDR)	ESET Enterprise Inspector забезпечує безперервний моніторинг, детальний аналіз і реагування на загрози.
Аналіз аномалій та поведінковий аналіз	Системи ESET аналізують поведінкові патерни для виявлення відхилень від норми, що може вказувати на нові або нульові загрози.
Пісочниця (Sandboxing)	Виконання підозрілих файлів в ізольованому середовищі для детального аналізу їхньої поведінки.
Машинне навчання та штучний інтелект (AI)	ESET Augur поєднує кілька нейронних мереж для забезпечення високої точності виявлення нових і невідомих загроз.
Інтеграція з іншими рішеннями безпеки	Централізовані консолі управління ESET Security Management Center і ESET PROTECT дозволяють централізовано керувати всіма аспектами безпеки кінцевих точок.

Опис технологій:

антивірус та антишпигунське ПЗ:

принцип роботи: використовують поєднання сигнатурного та евристичного аналізу для виявлення відомих загроз і підозрілої поведінки. Сигнатурний аналіз порівнює файли з базою даних відомих загроз, тоді як евристичний аналіз оцінює поведінку програм для виявлення потенційно небезпечних дій.

приклад використання: ESET Endpoint Security забезпечує захист від шкідливих програм, включаючи віруси, хробаки, трояни та шпигунське ПЗ.

хмарні репутаційні системи:

принцип роботи: ESET LiveGrid (графік 2.1) - глобальна хмарна мережа, що збирає інформацію про загрози від мільйонів користувачів по всьому світу. Це дозволяє швидко ідентифікувати нові загрози та забезпечувати оперативний захист. Хмарні репутаційні системи аналізують файли та URL-адреси в режимі реального часу, оцінюючи їхню безпеку на основі глобальної бази даних.

приклад використання: Швидке виявлення та блокування нових загроз, які ще не внесені до локальних баз даних сигнатур.

Виявлення та реагування на кінцевих точках (EDR):

принцип роботи: ESET Enterprise Inspector забезпечує безперервний моніторинг активностей на кінцевих точках, детальний аналіз подій та оперативне реагування на загрози. Використовуючи поведінковий аналіз і машинне навчання, EDR системи можуть виявляти складні атаки, включаючи загрози нульового дня.

приклад використання: Постійний моніторинг активності файлів, мережевих з'єднань та системних подій для виявлення підозрілої поведінки.

Аналіз аномалій та поведінковий аналіз:

принцип роботи: Системи ESET аналізують поведінкові патерни, виявляючи аномалії, що можуть свідчити про наявність нових загроз. Поведінковий аналіз дозволяє ідентифікувати загрози, які не можуть бути виявлені традиційними методами, зокрема сигнатурним аналізом.

приклад використання: Виявлення відхилень від норми у поведінці програмного забезпечення, що може вказувати на наявність загроз нульового дня.

пісочниця (Sandboxing):

принцип роботи: Пісочниця створює ізольоване середовище, в якому підозрілі файли можуть виконуватися без ризику для основної системи. Це дозволяє детально аналізувати поведінку файлів та визначати, чи є вони шкідливими.

приклад використання: Аналіз підозрілих файлів в ізольованому середовищі для визначення їхньої шкідливості.

Машинне навчання та штучний інтелект (AI):

принцип роботи: ESET Augur (графік 2.2) використовує кілька нейронних мереж для аналізу великих обсягів даних та виявлення нових і невідомих загроз. Машинне навчання дозволяє системі самонавчатися та покращувати свою ефективність з часом.

приклад використання: Аналіз поведінкових моделей та історичних даних для виявлення нових загроз

Інтеграція з іншими рішеннями безпеки:

принцип роботи: Централізовані консолі управління, такі як ESET Security Management Center і ESET PROTECT, дозволяють централізовано керувати всіма аспектами безпеки кінцевих точок. Це забезпечує координацію заходів захисту та обмін інформацією про загрози.

приклад використання: Централізоване управління різними рішеннями безпеки та їхня інтеграція для покращення загального рівня безпеки.

Отже ESET пропонує комплексні рішення для виявлення та нейтралізації кіберзагроз, включаючи загрози нульового дня. Основні технології ESET включають антивірус та антишпигунське ПЗ, хмарні репутаційні системи, EDR, аналіз аномалій, пісочницю та AI. Використання цих технологій дозволяє забезпечити багаторівневий захист кінцевих точок, що значно підвищує рівень безпеки організації.

Додаткова інформація:

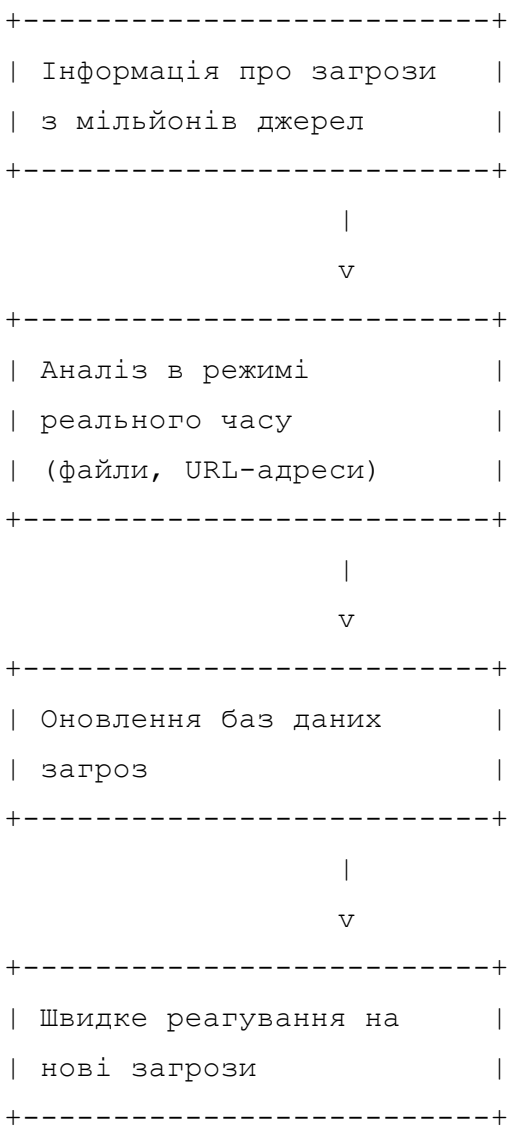

Рис. 2.1 - Принцип роботи хмарних репутаційних систем ESET LiveGrid

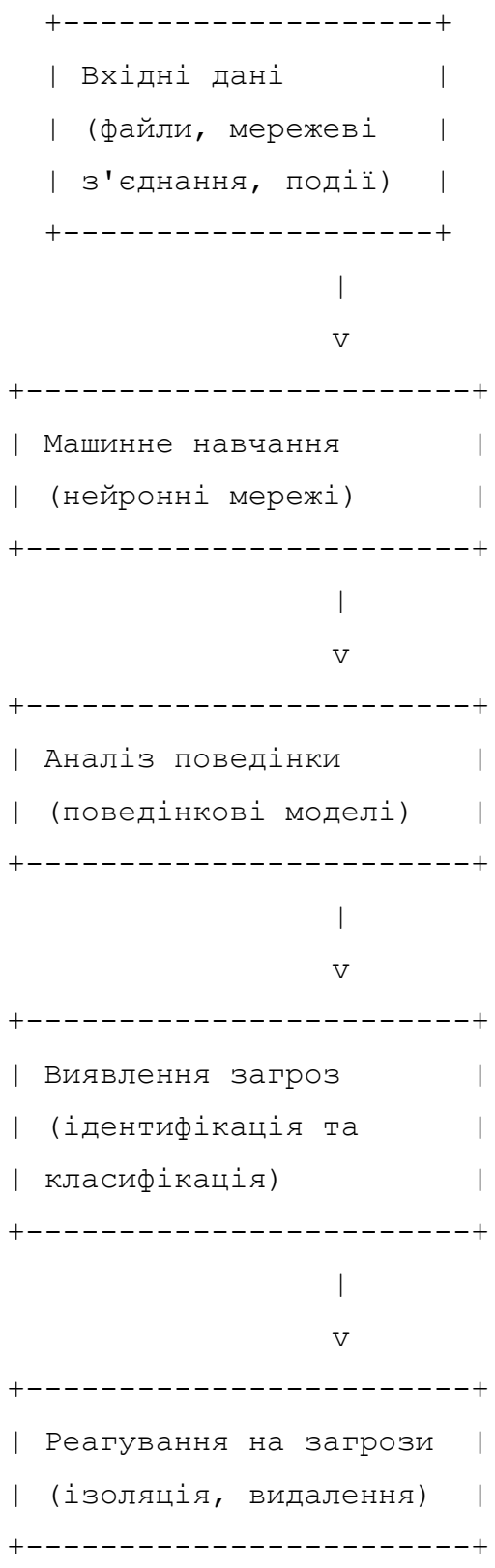

Рис. 2.2 Принцип роботи ESET Augur

2.2 Призначення, основні функції та склад комплексу виявлення загроз нульового дня на кінцевих точках підприємства на базі ESET Endpoint Security

Розглянемо призначення, основні функції та склад комплексу виявлення загроз нульового дня на кінцевих точках підприємства на базі ESET Endpoint Security на прикладі кейс-стаді.

Кейс-стаді: Впровадження ESET Endpoint Security в організації "TechSolutions Inc."

Опис організації: "TechSolutions Inc." – середня технологічна компанія з 500 співробітниками, що спеціалізується на розробці програмного забезпечення та наданні IT-консультаційних послуг. Головний офіс компанії розташований у Києві, з додатковими офісами в Одесі та Львові. Організація використовує велику кількість кінцевих точок, включаючи робочі станції, ноутбуки та сервери.

Проблема: Компанія "TechSolutions Inc." зіткнулася з підвищеним ризиком загроз нульового дня, які залишаються непоміченими традиційними антивірусними рішеннями. Зокрема, було кілька інцидентів, коли нові шкідливі програми використовували невиправлені уразливості в програмному забезпеченні, що призвело до втрати даних та збоїв у роботі систем.

Мета впровадження: Забезпечити високий рівень кібербезпеки, зокрема, захист від загроз нульового дня, шляхом впровадження ESET Endpoint Security для моніторингу, виявлення та нейтралізації нових загроз.

Рішення: Впровадження ESET Endpoint Security та ESET Enterprise Inspector (EDR) для всіх кінцевих точок організації.

Основні функції ESET Endpoint Security зазначені в таблиці 2.1.

Впровадження ESET Endpoint Security в "TechSolutions Inc.":

підготовка: аналіз поточного стану безпеки та ідентифікація ключових уразливостей; планування розгортання ESET Endpoint Security на всіх кінцевих точках;

розгортання: інсталяція ESET Endpoint Security та ESET Enterprise Inspector на робочі станції, ноутбуки та сервери; налаштування політик безпеки та правил для виявлення загроз нульового дня.

моніторинг та налаштування: пезперервний моніторинг активностей за допомогою ESET Enterprise Inspector. Адаптація налаштувань на основі виявлених загроз та їхньої класифікації.

Отримані результати:

виявлення загроз нульового дня: протягом першого місяця після впровадження, ESET Endpoint Security ідентифікував кілька загроз нульового дня, які залишалися непоміченими попередніми антивірусними рішеннями. Наприклад, було виявлено шкідливе ПЗ, яке використовувало нову уразливість у поштовому клієнті компанії.

зменшення інцидентів безпеки: кількість інцидентів безпеки значно зменшилася, завдяки проактивному виявленню та нейтралізації загроз. Це дозволило уникнути втрат даних та збоїв у роботі систем.

підвищення рівня обізнаності співробітників: завдяки регулярним тренінгам та навчанням з використанням ESET Endpoint Security, обізнаність співробітників про загрози нульового дня та методи їх виявлення значно зросла.

поліпшення загального рівня безпеки: Інтеграція ESET Endpoint Security з існуючими рішеннями безпеки дозволила створити єдину систему захисту, що значно покращило загальний рівень безпеки в організації.

Таблиця 2.2

Результати впровадження ESET Endpoint Security в "TechSolutions Inc." (до встановлення)

Місяць	Виявлені загрози нульового дня	Інциденти безпеки	Втрати даних	Збої в роботі систем	Час на реагування на інциденти	Рівень обізнаності співробітників
Липень	0	10	2	2	5 годин	Низький
Серпень	0	9	1	1	5 годин	Низький
Вересень	0	11	1	1	5 годин	Низький
Жовтень	0	8	1	1	5 годин	Низький

Місяць	Виявлені загрози нульового дня	Інциденти безпеки	Втрати даних	Збої в роботі систем	Час на реагування на інциденти	Рівень обізнаності співробітників
Листопад	1	10	0	2	5 годин	Низький
Грудень	1	12	0	1	5 годин	Низький

Таблиця 2.3

Результати впровадження ESET Endpoint Security в "TechSolutions Inc." (пів року після встановлення)

Місяць	Виявлені загрози нульового дня	Інциденти безпеки	Втрати даних	Збої в роботі систем	Час на реагування на інциденти	Рівень обізнаності співробітників
Січень	1	2	0	0	1 година	Високий
Лютий	1	2	0	0	1 година	Високий
Березень	0	2	0	0	1 година	Високий
Квітень	1	1	0	0	1 година	Високий
Травень	0	1	0	0	1 година	Високий
Червень	1	1	0	0	1 година	Високий

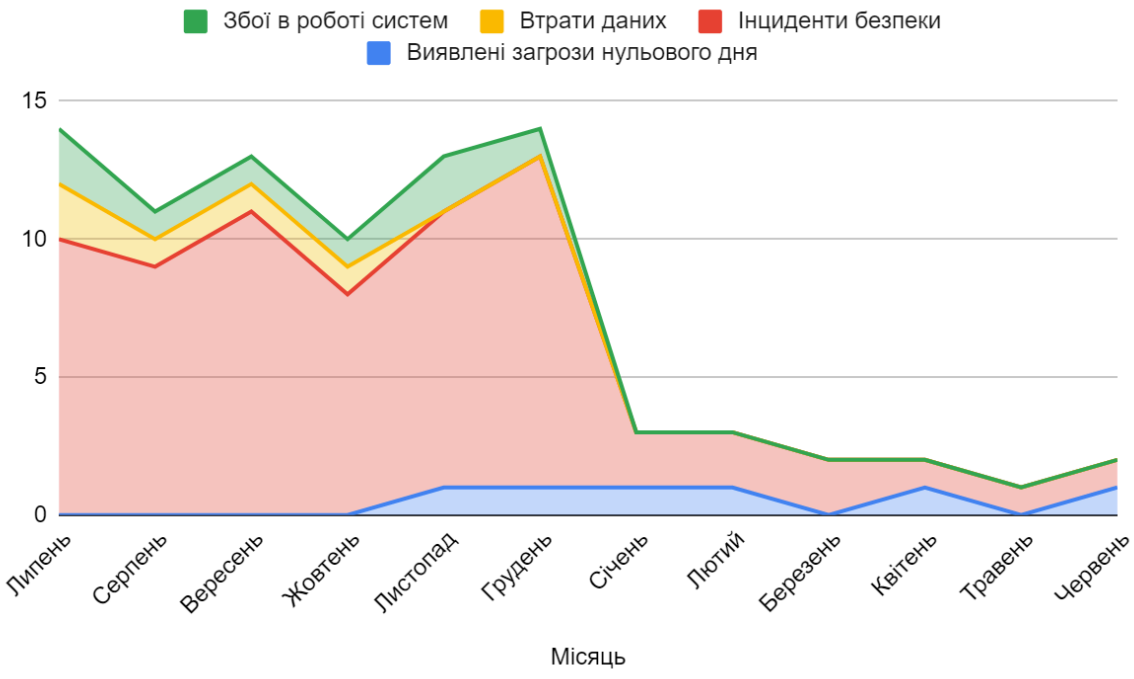

Рис. 2.3 - Порівняльний графік таблиць 2.2 і 2.3

Таблиця 2.4

Порівняльна таблиця до таблиць 2.2 і 2.3

Показник	До встановлення	Після встановлення
Виявлені загрози нульового дня	2 за пів року	4 за пів року
Інциденти безпеки	В середньому 10 на місяць	В середньому 1-2 на місяць
Втрати даних	4 випадки за пів року	0 випадків за пів року
Збої в роботі систем	7 випадків за пів року	0 випадків за пів року
Час на реагування на інциденти	5 годин	1 година
Рівень обізнаності співробітників	Низький	Високий

Виявлення загроз нульового дня: до встановлення: лише 2 випадки за пів року; після встановлення: 4 випадки за пів року.

Інциденти безпеки: до встановлення: в середньому 10 інцидентів на місяць; після встановлення: в середньому 1-2 інциденти на місяць.

*Втрати даних: д*о встановлення: 4 випадки за пів року; після встановлення: 0 випадків за пів року.

Збої в роботі систем: до встановлення: 7 випадків за пів року; після встановлення: 0 випадків за пів року.

Час на реагування на інциденти: до встановлення: 5 годин; після встановлення: 1 година.

Рівень обізнаності співробітників: до встановлення: низький; після встановлення: високий.

Впровадження ESET Endpoint Security в "TechSolutions Inc." продемонструвало ефективність рішення у боротьбі з загрозами нульового дня. Виявлення загроз нульового дня покращилось, оскільки ESET Endpoint Security дозволило ідентифікувати більше нових загроз. Кількість інцидентів значно зменшилася завдяки проактивному виявленню та нейтралізації загроз. ESET Endpoint Security допомогло уникнути втрат даних. Час на реагування значно скоротився. Підвищення рівня обізнаності завдяки тренінгам та навчанням.

Використання передових технологій, таких як хмарні репутаційні системи та машинне навчання, дозволило виявити та нейтралізувати нові загрози, підвищуючи рівень безпеки кінцевих точок підприємства.

2.3 Реалізація технології виявлення загроз нульового дня на кінцевих точках підприємства в рішенні ESET Endpoint Security

Загрози нульового дня представляють серйозну небезпеку для корпоративних кінцевих точок через їхню здатність використовувати невідомі уразливості. ESET Endpoint Security надає ефективні методи для виявлення і нейтралізації таких загроз.

Процес впровадження:

аналіз поточного стану безпеки: перед впровадженням ESET Endpoint Security, необхідно виконати оцінку поточного стану захисту кінцевих точок. Це включає виявлення наявних уразливостей та аналіз можливих векторів атак;

планування розгортання: на основі результатів аналізу розробляється детальний план розгортання. Він включає визначення обсягу робіт, розподіл ресурсів, встановлення термінів та визначення відповідальних осіб;

інсталяція: ESET Endpoint Security встановлюється на всі кінцеві точки підприємства, включаючи робочі станції, ноутбуки та сервери;

налаштування: після інсталяції проводиться налаштування політик безпеки, таких як фільтрування веб-трафіку, контроль доступу до USB-пристроїв та налаштування антивірусного захисту;

моніторинг та налаштування: система моніторингу ESET Enterprise Inspector (EDR) налаштовується для постійного відстеження активностей на кінцевих точках. Включаються механізми поведінкового аналізу та аналізу аномалій для виявлення загроз нульового дня;

поведінковий аналіз: використання поведінкових моделей для виявлення аномалій у роботі програмного забезпечення. Це дозволяє визначити підозрілі активності, які можуть свідчити про нові або невідомі загрози;

пісочниця (Sandboxing): підозрілі файли ізолюються у віртуальному середовищі, де їхня поведінка аналізується без ризику для основної системи. Це дозволяє виявляти шкідливі програми, які використовують уразливості нульового дня;

машинне навчання та штучний інтелект: технології AI та ML використовуються для аналізу великих обсягів даних і виявлення нових загроз на основі поведінкових патернів. ESET Augur, який поєднує кілька нейронних мереж, забезпечує високий рівень точності у виявленні загроз;

автоматизовані дії: після виявлення загрози система автоматично ізолює уражені кінцеві точки, видаляє шкідливе ПЗ та проводить необхідні заходи для нейтралізації загрози;

план реагування: розробка та впровадження детальних планів реагування на інциденти, що включають конкретні кроки для мінімізації впливу загроз і відновлення нормальної роботи систем;

оновлення та управління патчами: для забезпечення захисту від загроз нульового дня важливо своєчасно оновлювати операційні системи та програмне забезпечення. Використання систем управління патчами дозволяє автоматизувати процес оновлення та забезпечити оперативне виправлення уразливостей;

навчання співробітників: регулярні тренінги для підвищення обізнаності співробітників щодо загроз нульового дня та методів їх виявлення і запобігання;

інтеграція з іншими системами безпеки: ESET Endpoint Security інтегрується з існуючими рішеннями безпеки для координації заходів захисту та обміну інформацією про загрози. Централізоване управління через консолі ESET Security Management Center і ESET PROTECT дозволяє ефективно керувати всіма аспектами безпеки кінцевих точок.

Показники ефективності після впровадження ESET Endpoint Security можна продивитись у кейс-стаді розділу 2.2, таблицях 2.2, 2.3, 2.4.

Отже реалізація технології виявлення загроз нульового дня за допомогою ESET Endpoint Security включає аналіз поточного стану безпеки, планування розгортання, інсталяцію та налаштування системи, моніторинг і аналіз загроз.

Використання поведінкового аналізу та пісочниці дозволяє ефективно виявляти нові загрози. Впровадження ESET Endpoint Security забезпечує надійний захист кінцевих точок від загроз нульового дня і мінімізує ризики для бізнесу.

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ НУЛЬОВОГО ДНЯ НА КІНЦЕВИХ ТОЧКАХ ПІДПРИЄМСТВА ЗА ДОПОМОГОЮ ESET ENDPOINT SECURITY

3.1 Порядок розгортання рішення ESET Endpoint Security і додавання кінцевих точок до мережі ESET PROTECT

Для успішного розгортання ендпоінт продуктів потрібно вже мати встановленний веб інтерфес ESET PROTECT [5].

Потрібно відкрити ESET PROTECT у веб-браузері та увійти. Далі натиснути Завдання → Операційна система → Інсталяція програмного забезпечення → Створити → Завдання клієнта (рисунок 3.1).

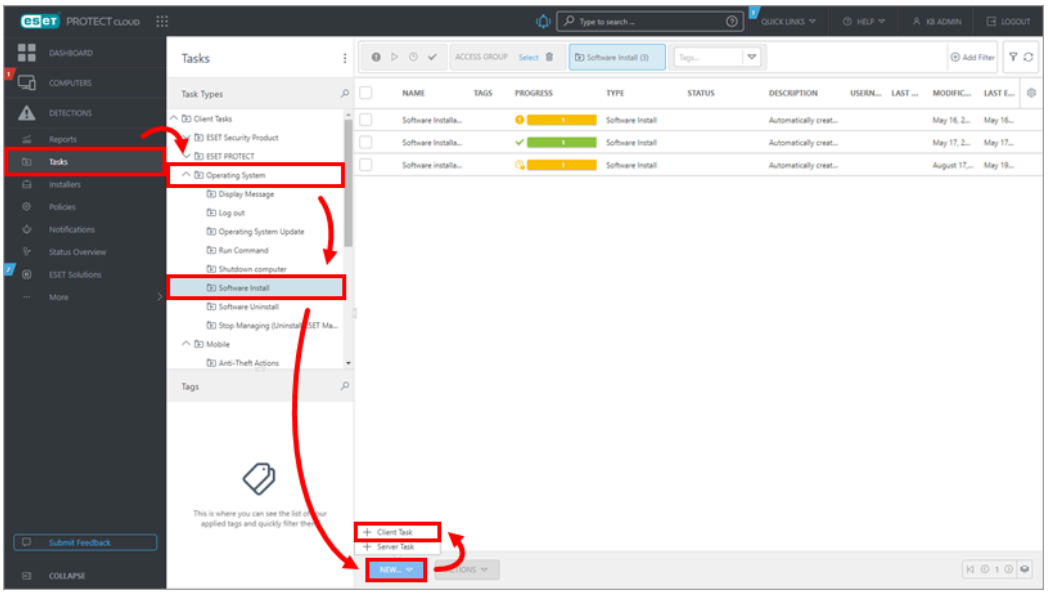

Рис. 3.1 - Інсталяція програмного забезпечення

У розділі «Основні» ввести назву в поле «Ім’я» . Поле Опис необов’язкове . У розкривних меню «Категорія завдань» і «Завдання» буде автоматично встановлено значення « Усі завдання » та « Встановлення програмного забезпечення» відповідно. Потрібно натиснути Продовжити (рисунок 3.2).

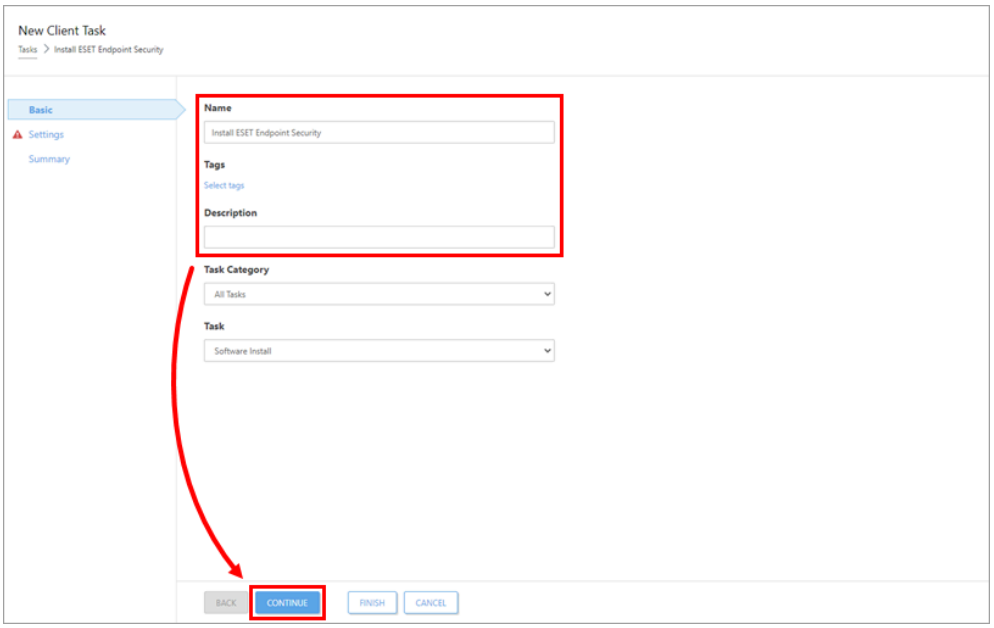

Рис 3.2 Встановлення програмного забезпечення

У розділі «Параметри» в розділі «Пакет для встановлення» є два варіанти вибору пакета, який буде встановлено на цільових клієнтах: «Встановити пакет зі сховища» або « Встановити за прямою URL-адресою пакета» .

Щоб встановити пакет зі сховища:

потрібно переконатись, що вибрано « Установити пакет зі сховища» . Потрібно вибрати операційну систему (у цьому прикладі вибрано Windows) і натиснути «Вибрати» нижче «Вибрати пакет зі сховища» . У вікні «Вибір продукту» вибрати продукт і мову зі спадного меню «Мова» . За бажанням можна розгорнути Налаштувати додаткові параметри , де можна вибрати конкретну версію продукту. Потрібно перевірити наявність найновішої версії бізнес-продуктів ESET . Натиснути OK . (рисунок 3.3);

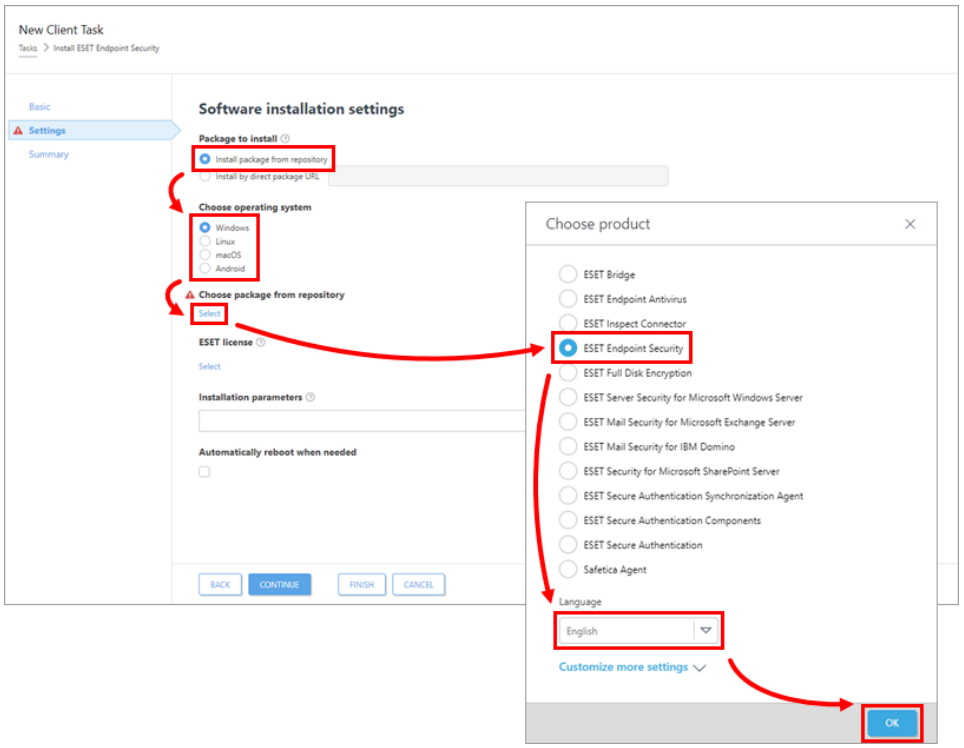

Рис.3.3 - Пакет для встановлення зі сховища

попередньо встановлено прапорець поруч із пунктом « Дозволити інсталювати останню версію продукту, для якої прийнято ліцензійну угоду» . Потрібно зняти цей прапорець, якщо ви не хочете інсталювати останню версію вибраного продукту. Натиснути ліцензію під ліцензією ESET, щоб змінити її. За бажанням установити прапорець біля пункту « Активувати ESET LiveGuard», щоб увімкнути цю функцію (перегляньте примітку та ліцензію нижче). Установити прапорці поруч із пунктами Увімкнути систему зворотного зв'язку ESET LiveGrid® (рекомендовано) і поруч із пунктом Увімкнути виявлення потенційно небажаних програм . Установити прапорець нижче Автоматично перезавантажувати за потреби та налаштуйте параметри Відкласти та Дозволити користувачеві скасовувати дію, якщо це необхідно. (рисунок 3.4).

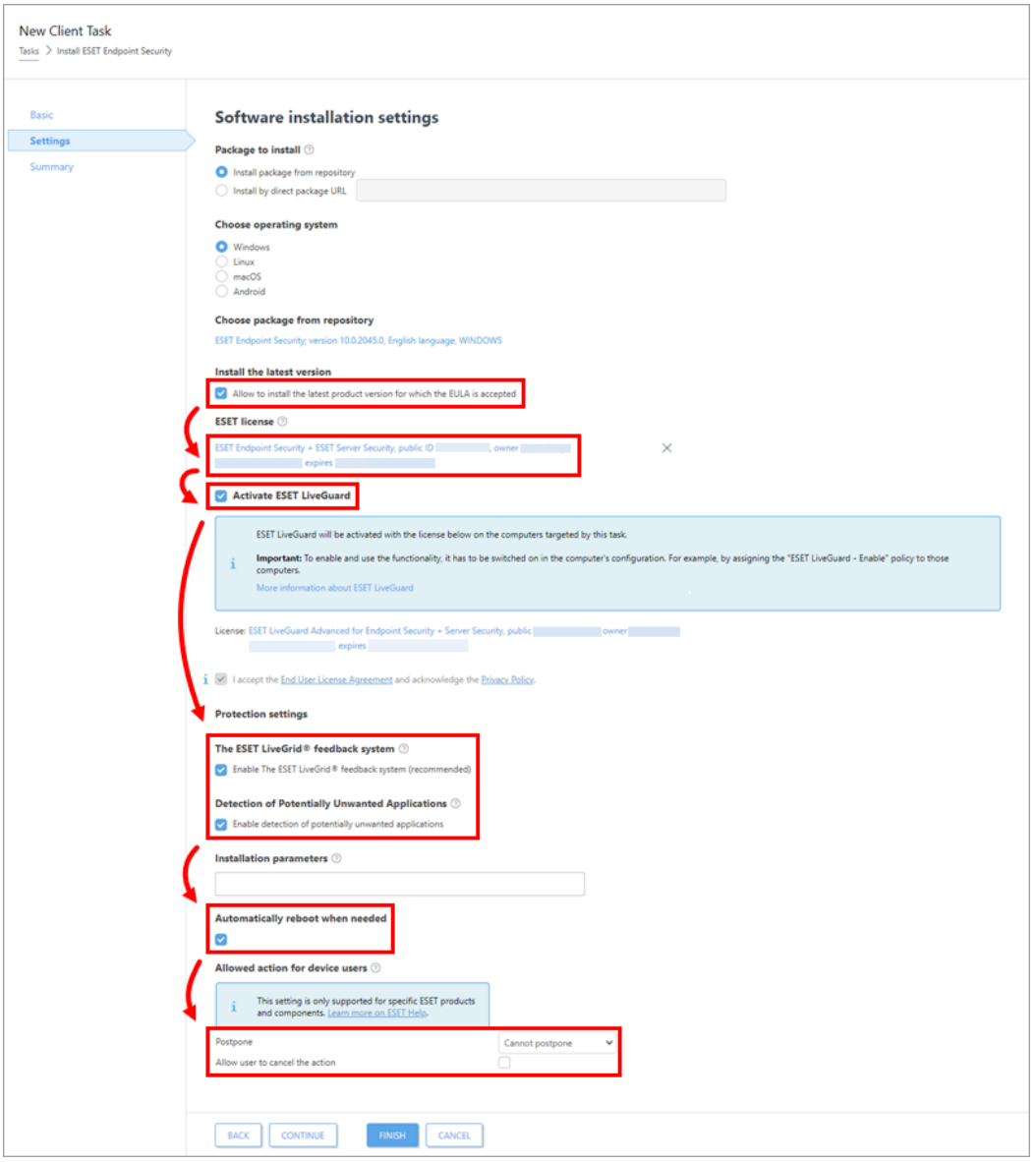

Рис. 3.4 - Процес встановлення зі сховища (1)

Щоб установити пакет, ввівши цільову URL-адресу:

перевірте наявність найновішої версії бізнес-продуктів ESET;

обрати «Установити за прямою URL-адресою пакета» , ввести або URL-адресу пакета у відповідне поле. Натисніть «Вибрати» під «Ліцензія ESET» лише під час інсталяції нового продукту чи оновлення продуктів, які не активовано, або якщо ви хочете змінити ліцензію, яка зараз використовується, на іншу зі списку доступних ліцензій. Установіть прапорець Я приймаю Ліцензійну угоду кінцевого користувача. Установіть прапорець нижче Автоматично

перезавантажувати за потреби та налаштуйте параметри Відкласти та Дозволити користувачеві скасовувати дію, якщо це необхідно (рисунок 3.5);

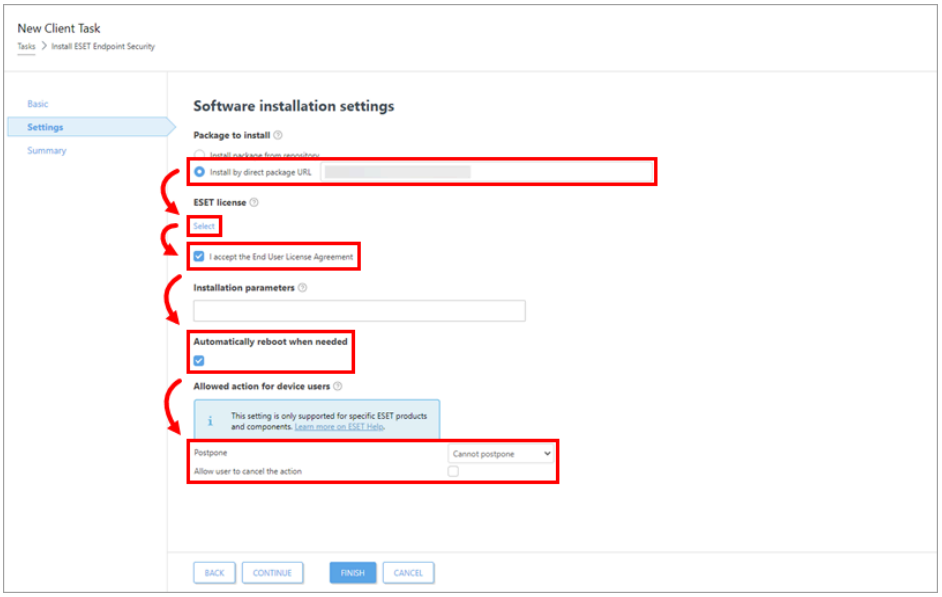

Рис. 3.5 - Процес встановлення зі сховища (2)

Натиснути Підсумок → Готово (рисунок 3.6).

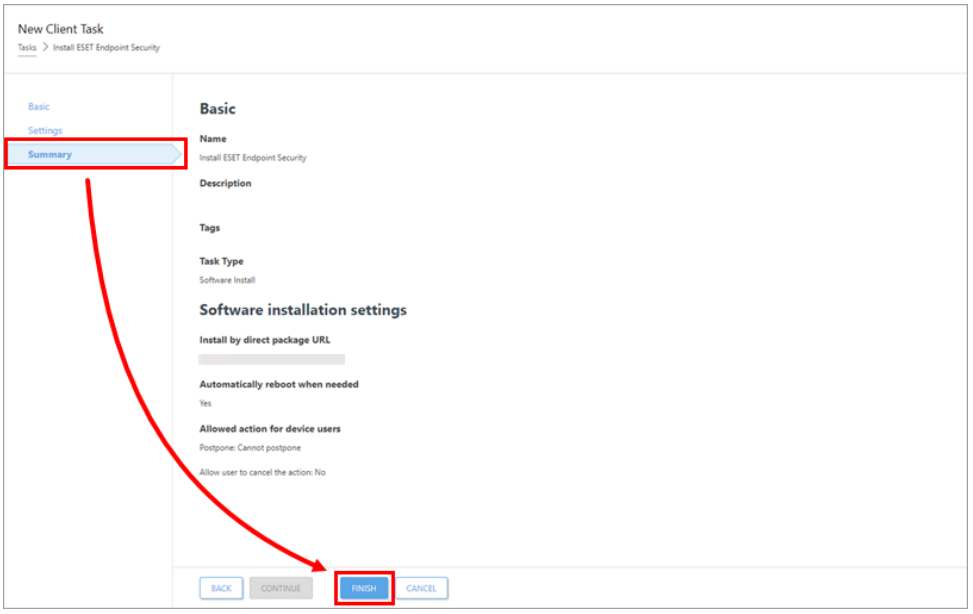

Рис. 3.6 - Процес встановлення зі сховища (3)

Коли з’явиться запит, натисніть « Створити тригер». (рисунок 3.7).

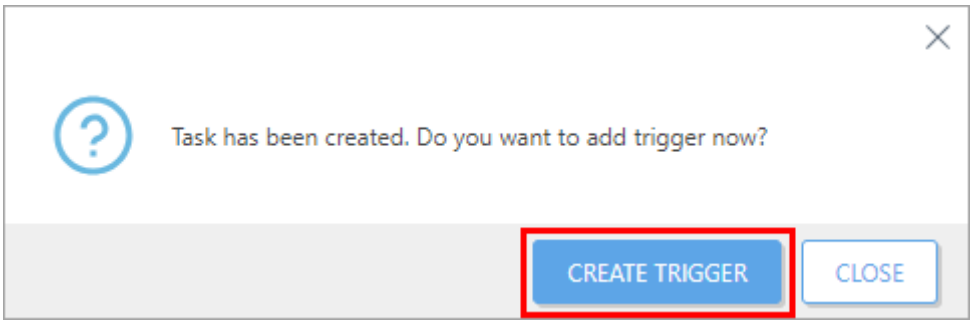

Рис. 3.7 - Створення тригеру (1)

Ввести назву тригера в поле «Опис тригера» та натисніть « Продовжити». (рисунок 3.8)

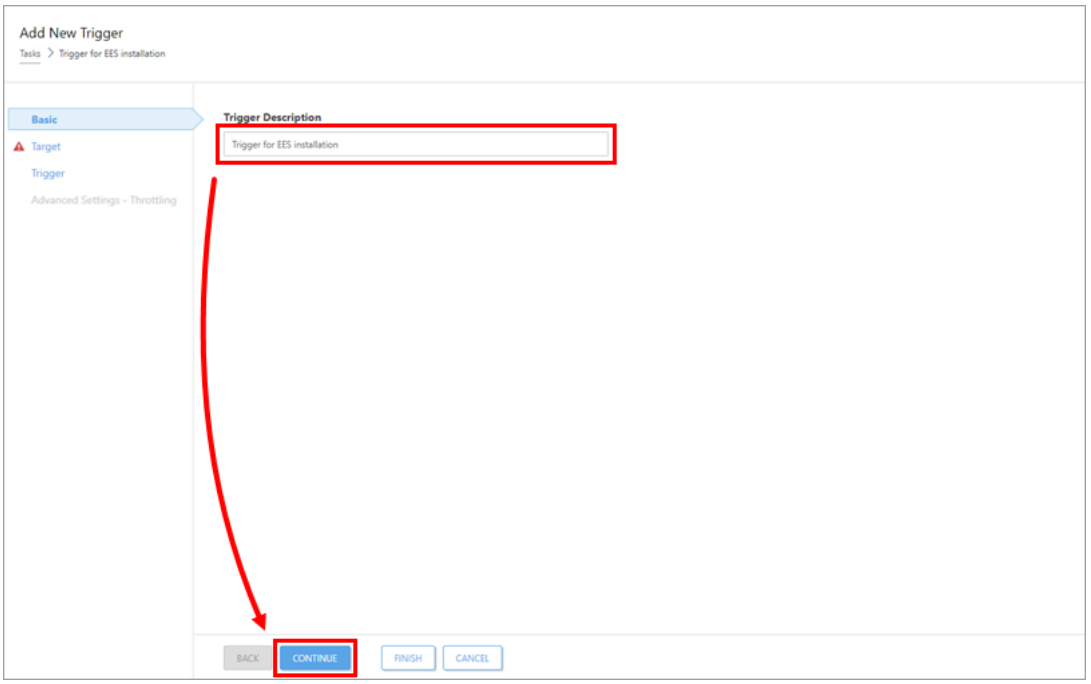

Рис.3.8 - Створення тригеру (2)

Натиснути Додати цілі . Установити прапорці біля комп'ютерів або груп, яким потрібно надіслати це завдання, і натисніть OK . (рисунок 3.9)

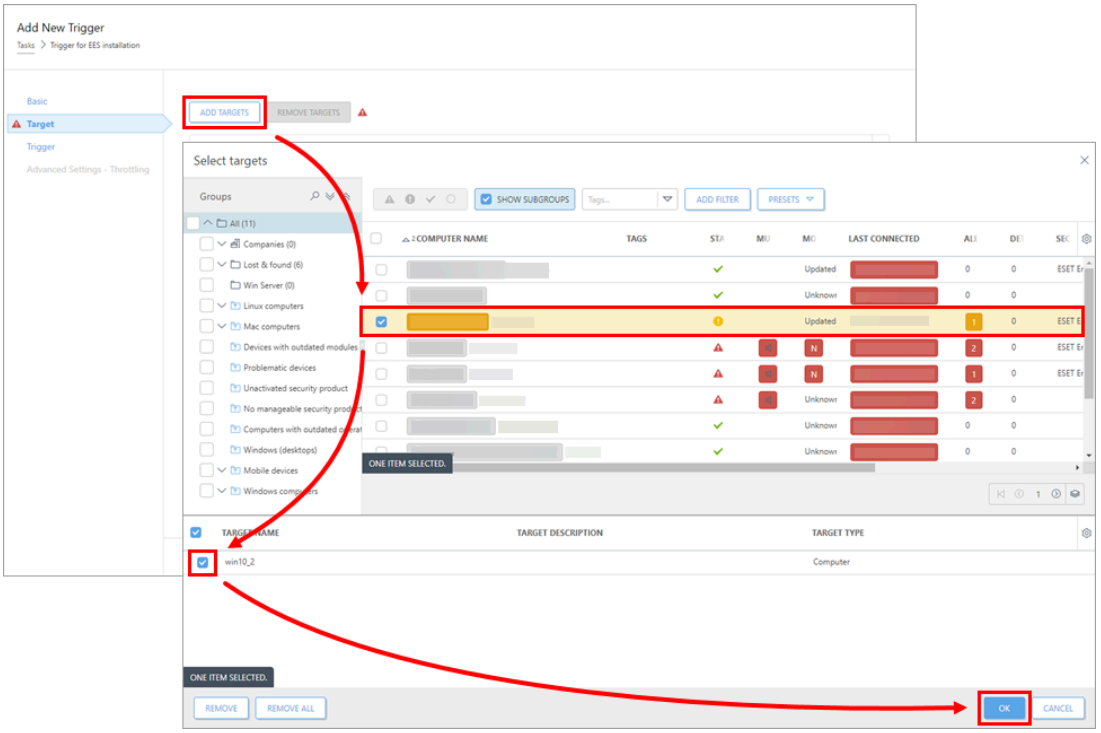

Рис. 3.9 - Вибір груп

Натиснути Тригер , вибрати тип тригера зі спадного меню та натисніть Готово . (рисунок 3.10)

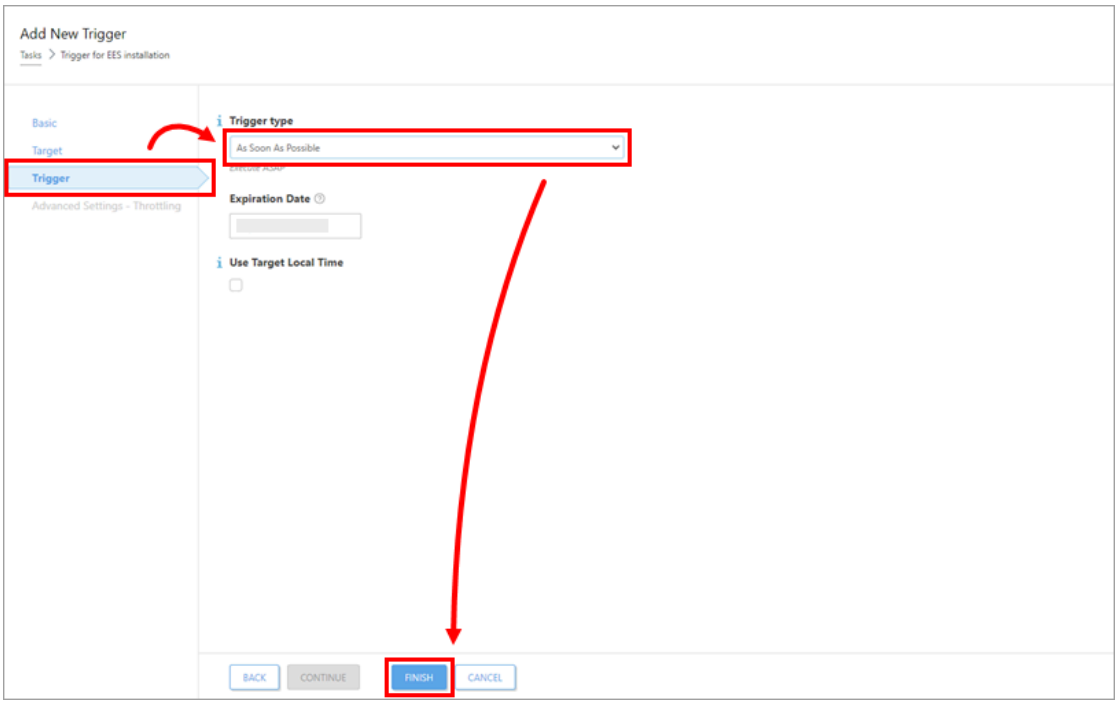

Рис. 3.10 - Налаштування тригеру

Надіслати завдання активації на комп’ютери, на яких інстальовано ESET Endpoint або продукти ESET Server/Mail Security, щоб вони могли регулярно отримувати оновлення.

3.2 Алгоритм реалізації виявлення загроз нульового дня на кінцевих точках підприємства на базі ESET Endpoint Security

Для забезпечення ефективного виявлення загроз нульового дня на кінцевих точках підприємства, необхідно розробити та впровадити детальний алгоритм, який враховує всі аспекти захисту:

Підготовка: збір та аналіз даних про поточні вразливості кінцевих точок; встановлення ESET Endpoint Security на всі кінцеві точки підприємства; налаштування політик безпеки, включаючи фільтрування веб-трафіку та контроль доступу до USB-пристроїв.

Аналіз активностей: використання ESET Enterprise Inspector для безперервного моніторингу активностей; налаштування системи поведінкового аналізу для виявлення аномалій.

Виявлення загроз: використання алгоритмів машинного навчання для аналізу великих обсягів даних; ізоляція підозрілих файлів у пісочниці для безпечного виконання та аналізу їхньої поведінки.

Реагування: автоматизація дій на виявлені загрози, включаючи ізоляцію уражених кінцевих точок та видалення шкідливого ПЗ, розробка та впровадження детальних планів реагування на інциденти.

Оновлення та патч-менеджмент: використання систем управління патчами для своєчасного оновлення операційних систем та програмного забезпечення, регулярний моніторинг і аналіз ефективності оновлень.

Розглянемо конкретний випадок впровадження алгоритму в компанії "TechSolutions Inc." з кейс-стаді з розділу 2.2:

підготовка: аналіз поточного стану безпеки, встановлення ESET Endpoint Security;

аналіз активностей: використання ESET Enterprise Inspector для моніторингу активностей;

виявлення загроз: ізоляція підозрілих файлів у пісочниці;

реагування: автоматичне ізолювання та видалення шкідливого ПЗ;

оновлення: регулярні оновлення систем управління патчами.

3.3 Розроблення рекомендацій щодо виявлення загроз нульового дня на кінцевих точках підприємства на базі ESET Endpoint Security

В даному розділі представлені рекомендації щодо ефективного виявлення загроз нульового дня на кінцевих точках підприємства з використанням продукту ESET Endpoint Security. На основі передових технологій та практичного досвіду будуть надані поради з підвищення рівня безпеки та зменшення ризику інцидентів, що виникають внаслідок нових та невідомих загроз. Рекомендації щодо виявлення загроз нульового дня на кінцевих точках підприємства на базі ESET Endpoint Security:

Встановлення та налаштування ESET Endpoint Security: Завантажте та встановіть останню версію ESET Endpoint Security на всі кінцеві точки підприємства. Використовуйте централізовану консоль управління (ESET Security Management Center) для моніторингу та управління всіма пристроями.

Налаштування політик безпеки: Створіть та налаштуйте політики безпеки, що відповідають вимогам підприємства. Забезпечте включення всіх функцій ESET Endpoint Security, таких як антивірусний захист, антишпигунське ПЗ, контроль веб-доступу та захист USB-пристроїв. Встановіть жорсткі правила для управління доступом до зовнішніх пристроїв (наприклад, заборона або обмеження використання USB-пристроїв).

Використання проактивних методів:

поведінковий аналіз: Включіть поведінковий аналіз у налаштуваннях ESET Endpoint Security для виявлення аномалій у роботі програмного забезпечення.

Використовуйте функцію HIPS (Host-based Intrusion Prevention System) для відстеження та аналізу поведінки програм на кінцевих точках.

пісочниця (Sandboxing): Налаштуйте ESET Endpoint Security для використання пісочниці. Це дозволить ізолювати підозрілі файли в віртуальному середовищі для їхнього безпечного аналізу. Регулярно перевіряйте звіти про аналіз файлів у пісочниці для виявлення нових загроз.

Машинне навчання та штучний інтелект: Активуйте функції машинного навчання та штучного інтелекту в ESET Endpoint Security для автоматичного виявлення нових загроз на основі аналізу великих обсягів даних. Регулярно оновлюйте моделі машинного навчання, щоб забезпечити їхню актуальність і ефективність.

Безперервний моніторинг: Використовуйте ESET Enterprise Inspector (EDR) для постійного моніторингу активностей на кінцевих точках. Налаштуйте систему для автоматичного сповіщення про підозрілі активності та потенційні загрози.

Автоматизація реагування: Впровадьте автоматизовані процедури реагування на інциденти, включаючи ізоляцію уражених кінцевих точок та видалення шкідливого ПЗ. Використовуйте скрипти та політики для автоматичного блокування підозрілих дій.

Своєчасне оновлення: Забезпечте регулярне оновлення операційних систем і програмного забезпечення на всіх кінцевих точках. Використовуйте системи управління патчами для автоматизації процесу оновлення.

*Моніторинг оновлень: в*ідстежуйте статус оновлень і патчів через консоль управління ESET Endpoint Security. Проведіть регулярний аудит для забезпечення своєчасного застосування всіх критичних оновлень.

Регулярні тренінги: Проводьте регулярні тренінги для співробітників з метою підвищення їхньої обізнаності щодо загроз нульового дня та методів їхнього виявлення і запобігання. Використовуйте навчальні платформи, такі як KnowBe4, для проведення тренінгів і симуляцій фішингових атак.

Розробка політик безпеки: Створіть та впровадьте чіткі політики безпечного використання корпоративних пристроїв та ресурсів. Регулярно оновлюйте

політики відповідно до нових загроз і технологічних змін.

Централізоване управління: Інтегруйте ESET Endpoint Security з іншими системами безпеки для забезпечення координації заходів захисту та обміну інформацією про загрози. Використовуйте централізовані консолі управління, такі як ESET Security Management Center, для моніторингу та управління всіма аспектами безпеки кінцевих точок.

Взаємодія з SIEM: Використовуйте платформи SIEM (Security Information and Event Management) для кореляції даних і забезпечення всебічного аналізу інцидентів безпеки. Налаштуйте автоматичне передавання даних про загрози з ESET Endpoint Security до SIEM для оперативного виявлення та реагування.

ВИСНОВКИ

Аналіз поточних проблем виявлення загроз нульового дня показує, що основними викликами є складність виявлення нових і невідомих вразливостей, висока швидкість поширення шкідливого ПЗ та його адаптація до заходів захисту. Також значним викликом є те, що методи атак стають все більш складними, включаючи використання соціальної інженерії та складних обхідних методів, як у випадку з CVE-2024-29988 та CVE-2024-21412.

Огляд наукової та технічної літератури виявив, що більшість досліджень зосереджені на розробці нових алгоритмів та систем для виявлення загроз нульового дня, таких як використання машинного навчання, поведінкових аналізів та евристичних методів. Багато робіт також акцентують увагу на важливості інтеграції різних підходів для покращення ефективності систем виявлення загроз (IDS/IPS).

Основними проблемами виявлення загроз нульового дня є недосконаліть традиційних методів сигнатурного аналізу, затримка у розробці і впровадженні патчів та оновлень, а також недостатня підготовка персоналу до реагування на нові загрози. Крім того, збільшення використання складних методів обфускації та маскування шкідливого ПЗ ускладнює його виявлення.

Методи і засоби виявлення загроз нульового дня на базі Endpoint Detection and Response (EDR) включають аналіз поведінки, використання машинного навчання для виявлення аномалій, а також інтеграцію з інформаційними системами безпеки (SIEM). Проте, кожен з цих методів має свої обмеження і потребує регулярного оновлення і адаптації до нових загроз).

Розробка рекомендацій щодо виявлення загроз нульового дня на кінцевих точках підприємства за допомогою ESET Endpoint Security

Для покращення виявлення загроз нульового дня рекомендується:

Інтеграція кількох рівнів захисту: Поєднання різних технологій, таких як поведінковий аналіз, сигнатурні методи та машинне навчання, для покращення загальної ефективності.

Регулярні оновлення: Забезпечення своєчасного оновлення систем захисту та баз даних загроз.

Навчання персоналу: Підвищення обізнаності та навчання співробітників щодо нових методів атак і способів захисту від них.

Моніторинг та аналітика: Постійний моніторинг кінцевих точок і аналіз подій для швидкого виявлення і реагування на підозрілі активності [3,4].

Проблеми виявлення загроз нульового дня на кінцевих точках підприємства залишаються актуальними і вимагають комплексного підходу, який включає в себе використання передових технологій, регулярне оновлення систем безпеки, навчання персоналу та постійний моніторинг. Інтеграція різних методів виявлення та швидке реагування на нові загрози можуть значно підвищити рівень захисту підприємства від атак нульового дня.