ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка
до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ТА АВТОМАТИЗАЦІЇ РЕАГУВАННЯ НА ІНЦИДЕНТИ НА БАЗІ КОМПЛЕКСУ РІШЕНЬ ВІД ESET»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Смирнов Д.С.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ВСТУП

Актуальність дослідження. В наш стрімкий час все більше людей в світі надають перевагу сучасним цифровим технологіям. Використання смартфонів, ноутбуків є повсякденням. Посилює процес діджиталізації перехід з офісу до віддаленої роботи. Зв'язку з цим виріс ризик загроз кібератак.

Різноманітність атак збільшилась. Основними цілями є критичні активи та системи, які підтримують життєдіяльність інформаційних процесів. З'являється можливість пошкодити чи викрасти інформацію, зруйнувати технічні засоби, вивести з ладу програмне забезпечення чи системи зв'язку.

Завжди вважалось, що ризик кібератак на критичну інфраструктуру є низьким через необхідність спеціальних знань про конфігурацію системи управління та адміністративні операції.

Кібератаки постійно розвиваються як у складності, так і в масштабах, вони досягли такого масштабу, що Всесвітній економічний форум вважає це другим найбільш загрозливим ризиком для глобальної торгівлі протягом наступного десятиліття [1]. У більшості кібератак зловмисник намагається використати один експлойт або механізм, щоб скомпрометувати якомога більше хостів і намагатися негайно використати зловживання збереженою інформацією та ресурсами якомога швидше.

На відміну від більшості кібератак, які мають за основу методику «вдарити та втікти» складні атаки відомі через їх високий ризик. Часто зловмисники використовують складні техніки та методи за допомогою різних векторік атак, що дозволяє їм залишатися прихованими та подовжити контроль над скомпрометованими хостами. Справді, цей контроль може тривати кілька років, як показали численні подібні випадки.

Крім цього, останні тенденції загроз вказують на схильність зловмисників використання безфайлових атак, неодноразово показуючи неспроможність звичайних методів захисту протистояти їм.

Ступінь наукової розробки. Удосконалено підходи в захисті кінцевих точок та автоматизації реакції на інциденти. Практичному значенні використання систем на основі ESET.

Практичне значення одержаних результатів становлять собою рекомендації для удосконалення системи реагування на інциденти та зміну стереотипного погляду на програмні комплекси компанії ESET.

Апробація результатів дипломної роботи. Основні наукові та технічні аспекти теми магістерської роботи були представлені та обговорені на :

1. Всеукраїнська наукова конференція на тему «Актуальні проблеми кібербезпеки»

1. АНАЛІЗ ПРОБЛЕМИ РЕАГУВАННЯ ІНЦИДЕНТИ БЕЗПЕКИ

1.1. Призначення, структура, функції та умови функціонування корпоративної інформаційної системи

Інформаційно-телекомунікаційна система [2] (ІТС) — це сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле

Інформаційна система була визначена з двох точок зору: одна що стосується його функції; інший, що стосується його структури.

З функціонального точки інформаційна система - це технологічно реалізований носій з метою запису, зберігання та поширення даних.

Зі структурної точки ; інформаційна система складається з сукупності людей, процеси, дані, моделі, технології та частково формалізована мова, формуючи цілісну структура, яка виконує певну організаційну мету або функцію. Функціональне визначення має свої переваги в тому, що фокусується на тому, що фактичні користувачі - з концептуальної точки зору- робити з інформаційною системою під час використання. Вони спілкуються з експертами для вирішення певної проблеми. Структурне визначення пояснює, що ІС є соціально-технічними системами, тобто системи, що складаються з людей, правил поведінки, а також концептуальних і технічних артефакти.

Інформаційну систему можна технічно визначити як набір взаємопов'язаних компонентів, які збирають (або отримують), обробляють, зберігають і поширюють інформацію для підтримки прийняття рішень і контролю в організації. На додаток до інформаційні системи підтримки прийняття рішень, координації та контролю може також допомогти менеджерам і працівникам аналізувати проблеми, візуалізувати складні предметів і створювати нові продукти.

Три види діяльності в інформаційній системі виробляють інформацію, яка організаціям необхідно приймати рішення, контролювати операції, аналізувати проблеми, і створювати нові продукти чи послуги. Це введення, обробка, вихід.

Вхідні дані фіксують або збирають вихідні дані всередині організації або із зовнішнього середовища. Обробка перетворює ці вихідні дані в а більш змістовна форма. Вихід передає оброблену інформацію в людей, які будуть використовувати його, або до діяльності, для якої вона буде використовуватися. Інформація системи також вимагають зворотного зв'язку, який виводиться на відповідне значення членів організації, щоб допомогти їм оцінити або виправити вводу.

Комп'ютери забезпечують ефективні способи обробки даних, і вони є необхідною частиною інформаційної системи. Однак ІС включає набагато більше, ніж просто комп’ютери. Успішне застосування ІС вимагає розуміння бізнесу та його середовища, яке підтримується. Вивчаючи інформаційні системи, недостатньо просто дізнатися про комп’ютери. Комп’ютери – це лише частина складної системи повинні бути спроектовані, експлуатовані та обслуговуватися.

Інформаційні технології широко визначають як сукупність комп'ютерів, систем, які використовує організація.

Інформаційні технології, у своєму визначенні, відноситься до технологічної сторони інформаційної системи. Це включає обладнання, програмне забезпечення, бази даних, мережі та інші електронні пристрої. Це можна розглядати як підсистему інформаційної системи. Іноді, однак, термін інформаційні технології також використовується як синонім інформаційна система.

Термін ІТ у найширшому значенні використовується для опису організації збір інформаційних систем, їх користувачів та управління тим наглядає за ними. Основна роль ІТ – бути вирішальним компонентом організаційної діяльності та процесів. З часом ця роль стане все більш важливою. Тому це необхідно, щоб кожен керівник і професійний співробітник дізнався про ІТ не лише у своїй спеціалізованій галузі, а й у всій організації та також у між організаційних умовах. Очевидно, буде ефективнішими в обраній кар’єрі, якщо так зрозуміти, як створюються, використовуються та керуються успішні інформаційні системи. Крім того, багато в чому, маючи рівень комфорту з інформаційними технологіями дозволить вам, поза роботою та у вашому особистому житті, щоб скористатися перевагами нових ІТ-продуктів та систем у міру їх розробки.

1.2. Аналіз необхідності забезпечення захисту від несанкціонованого доступу

Тактика кіберзагроз постійно розвивається, щоб уникнути виявлення інструментами безпеки кінцевих точок. Компанії зазнають матеріальних втрат.

Кінцева точка як найцінніший ресурс компанії, на якій зберігається на оброблюється інформація. Можливості реагування на інциденти на кінцевій точці дають змогу активно підходити до пошуку вразливостей всередині підприємства та дозволяє покращити безпеку.

Звичайні кіберзлочинці мають на меті вкрасти дані та отримати прибуток, тоді як розширені постійні загрози можуть красти власні дані або впливати на політику в іншій країні на додаток до фінансової мотивації. З 2015 по 2018 роки кіберзлочинці постійно змінювались тактики, використовуючи програми-вимагачів, шкідливі програм для майнингу і безфайлові шкідливі програми. Атаки, що включають використання вразливостей на ланцюжок поставок і безфайлові атаки залишаються величезною проблемою для організацій. В результаті цього важливо мати можливості виявлення інцидентів на кінцевій точці та реакції на інциденти, що можуть навіть обходити механізми безпеки.

Інцидент - випадок, який фактично або неминуче ставить під загрозу, без законних повноважень, цілісність, конфіденційність або доступність інформації або інформаційної системи, або є порушенням або безпосередньою загрозою порушення закону, політик безпеки, процедур безпеки або прийнятного використання політик.

Порушення даних з іншого боку, це вплив, що призводить до втрати різноманітних даних або несанкціонований доступ або модифікація даних з подальшим погіршенням або втратою конфіденційність, цілісності та доступі до конфіденційних даних. Не всі інциденти призводять до неминучого впливу, але загрози та порушення призводять до однакового навантаження на загальні ресурси реагування на інциденти. Незважаючи на вдосконалені технології, все більше застосовується автоматичні аналітики великих даних, штучний інтелект, хмарні обчислення та кращі

інтеграція різних рівнів інструментів кібербезпеки та платформи для додаткової ефективності.

Потенційна шкода підприємству в результаті успішного злому даних може включати всі або деякі компоненти з наступного:

- Втрата репутації
- Втрата критичних даних
- Дорогі юридичні зобов'язання
- Фактична втрата коштів та інтелектуальної власності
- Зрив бізнес-процесу

Будь-який з цих факторів ризику може спричинити значну кількість невдач для організації та її благополуччя, а в деяких випадках призводять до фактичного банкрутства.

Загрози будуть продовжувати зростати, а також націлені об’єкти схильні до можливих порушень, що ще більше розкриває невідповідність поточної методології та стратегії пом'якшення загроз.

Ландшафт загроз став більш складним і витонченим, технології розвідки та аналітики загроз вдосконалилися. Цільові атаки APT протягом багатьох років були серйозною загрозою для компаній і урядів. Більше і більше цілеспрямовані та складні технічні атаки створюються для проникнення в корпоративні мережі, для вилучення даних або, у випадку з програмним забезпеченням-вимагачем, зашифрувати його та вимагати шалених платежів за його розшифрування. Останній тренд нападів

озброєний програмним забезпеченням-вимагачем, вимагати додаткового викупу за не опублікування вилучених корпоративних даних.

Раніше зловмисники або група зловмисників нападали з цілю зруйнувати організацію з метою фінансової вигоди або навіть проявити себе, завдавши шкоди репутації компанії. У всіх цих нападах зловмисники не намагалися приховати свої дії. Однак такі типи атак все ще існують, але це інший рівень, захиститись від якого на сьогодні можливо стандартними методами.

Новий клас нападів характеризується ретельною підготовкою групи зловмисників для досягнення своєї мети. Зазвичай метою є непомітна крадіжка даних. Термін, наведений для цього клас атак — Advanced Persistent Threats (APT). APT зловмисники можуть використовувати [3] відомі методи, щоб проникнути до цільової інфраструктури, але інструменти, які вони використовують для проникнення – нові, раніше невідомі. Як вказує термін, інструменти, що використовуються, є передовими, і вони повинні бути такими, щоб зловмисник залишався в інфраструктурі на триваліший період. Зазвичай APT низькорівневі загрози, які повільно розширяються в інфраструктурі, переміщаючись з системи на іншу, отримуючи необхідну інформацію та експортують її до свого центру управління. APT зазвичай виконуються добре фінансовані. Атака припиняється лише тоді, коли її виявляють або при отриманні усіх необхідних даних. Так чи інакше, чимало шкоди завдає тій організації, яка стала жертвою APT атаки, іноді непоправної шкоди, що найчастіше зустрічається в випадку, коли був напад не виявляється, доки не потраплять усі необхідні дані. Мета атаки APT полягає не тільки в тому, щоб зібрати ціль даних суб'єкта, але також залишатися непоміченими. Для цього зловмисники працюють над створенням складних інструментів, таких як нові типи шкідливих програм, які зазвичай не виявляється антивірусним програмним забезпеченням на основі сигнатур або системи виявлення та запобігання вторгненням. Вони збираю детальну інформацію про організацію, наприклад інструменти та методи захисту, які використовує організація. Крім того, вони проводять час у визначення вразливих місць у всіх цих інструментах та створення шкідливі програми, які використовуватимуть цю вразливості. Тоді вони розсилати ці створені шкідливі програми, часто за допомогою фішингу, щоб отримати доступ до мережі організації робота.

APT часто виконується групою досвідчених зловмисників, які добре підготовлені. APT - це військовий термін, адаптований до інформаційної безпеки контекст, який відноситься до нападів. APT визначається комбінацією трьох слів [4]:

- Розширена: Зловмисники APT зазвичай добре фінансуються доступ до передових інструментів і методів, необхідних для виконання APT атака. Ці передові методи включають використання кілька векторів атаки для запуску, а також для збереження атаки збирається .
- Стійка: зловмисники APT дуже рішучі та наполегливі і вони не здаються. Як тільки вони потрапляють у систему, вони намагаються залишатися в системі якомога довше. Вони планують за використання кількох ухильних методів, щоб уникнути виявлення шляхом системи виявлення вторгнення їхньої цілі. Вони слідують "низько і повільний "підхід до збільшення швидкості їх успіху.
- Загроза: Загроза в APT -атаках зазвичай становить конфіденційні дані втрата або перешкоджання критичним компонентам або місії. Ці зростають загрози для багатьох національних організацій та організацій які мають передові системи захисту, які охороняють свої місії та/або дані.

Щоб досягти поставленої мети [5], нападники повинні йти через кілька стадій атак у різних формах, поки залишаючись непоміченим. Кілька етапів передбачають встановлення опори, сканування внутрішньої мережі та бічне переміщення від однієї системи до іншої в мережі для досягнення мети системи та виконувати свою шкідливу діяльність. Слідуючи за руйнівної діяльності, зловмисники можуть вирішити залишитися продовжувати свою шкідливу діяльність на інших системах у мережу або залишити систему після очищення слідів, в залежності від вимоги. Часто ці кілька етапів передбачають потрапляння в одну з систем всередині мережі та підвищення привілеїв, якщо це необхідно для досягнення цільової системи з наступним доступом до чутливих систем і надсилання статусу/інформації через підключення до Інтернету до центру управління.

Передові постійні загрози часто неправильно розуміються і цей термін все частіше використовується в промисловості як виправдання нездатність організацій захистити себе від чогось іншого - це цілеспрямована атака. З іншого боку, останнім часом, як пояснили у були зафіксовані атаки з цілями, які є насправді не зазна-

чено NIST під APT, але використовувані методи і характеристики цих атак, що вказує на необхідність перегляду визначення розширених постійних загроз для включення інших доменів нові цілі атаки

Завдяки своїй природі та впливу, ці атаки приділяли багато уваги дослідженням, оскільки неоднорідність векторів атак створює багато проблем для традиційних механізмів безпеки. Наприклад, через прихований характер APT обходять антивіруси[6]; тому потрібні більш досконалі методи для їх своєчасного виявлення. Системи виявлення та реагування кінцевих точок (EDR) забезпечують більш цілісний підхід до безпеки організації, оскільки, крім підписів, EDR корелюють інформацію та події на кількох хостах організації. Тому окремі події з кінцевих точок [7], які можуть опинитися за межами радара, збираються, обробляються та співвідносяться, надаючи синім командам глибоке уявлення про загрози, яким піддається периметр організації

Ще одним видом складних атак є Cyber Kill Chain. Cyber Kill Chain - це модель, яка дозволяє аналітикам безпеки розкласти кібератаку, незважаючи на її складність, на взаємно невиключні фази. Той факт, що кожна фаза ізольована від інших, дозволяє аналізувати кожну частину [8] атаки окремо та створювати методи пом’якшення та правила виявлення, які можуть полегшити механізми захисту для атаки, про яку йдеться, або подібних. Більше того, офіцери з безпеки повинні вирішувати менші проблеми, одну за одною, що набагато ефективніше, ніж стикатися з великою проблемою в цілому. У моделі Cyber Kill Chain актор загрози намагається проникнути в комп’ютерну мережу за допомогою набору послідовних, поетапних і прогресуючих кроків. Таким чином, якщо будь-який етап атаки запобігти, то атака не буде успішною

Успішна стратегія кіберзахисту залежить від швидкої, ефективної та швидкої реакції на інцидент. На жаль, аспект «люди» у стратегії реагування на інцидент виявився слабкою ланкою і фактично несе відповідальність за загальну повільну та неефективну реакцію на стримування або порушення кібератаки в усьому світі.

1.3. Аналіз проблеми реагування на інциденти безпеки

Поле реагування на інциденти в ІТ-безпеці — це загальний процес під час інциденту, який стався в комп’ютерній мережі або системі. Воно включає виявлення, аналіз, усунення та стримування атаки. Ця здатність- можливості необхідні для того, щоб адекватно реагувати на атаки на системи і мати можливість обмежити пов'язаний ризик, пов'язаний із таким випадком. В останні роки кількість атак на Інтернет зросла, і більше організацій нарощування оборонних можливостей. Однак ІТ-інфраструктура швидко змінюється, і команди безпеки працюють постали перед новими викликами. Тому вони повинні розвиватися. Реагування на інциденти є основою інформаційної безпеки, тому потрібно покращувати підходи, щоб залишатися на високому рівні. Тим не менш, перш ніж вдосконалюватись, потрібно знати, які проблеми реагування на інциденти. Традиційно багато організацій дотримуються процесів та інструментів, які було введено багато років тому. Передовий досвід базується на методах, запроваджених майже 30 років тому. Це не означає, що ці процедури ще не діють, але в минулому було багато прикладів, які доводять, що хороші підходи повинні адаптуватися до змін, що відбуваються в поточному ландшафт у цифровому середовищі.

Для того, щоб успішно виправити систему, яка була інфікована, необхідно впровадити дії, що усунуть проблему, а також потрібно впевнитись, що система не має нічого зловмисного. Тому зусилля щодо впровадження оновлення важливі, і в багатьох випадках їх можливо автоматизувати.

Це важливо, для того, щоб виконати необхідні дії якомога швидше.

Іншою проблемою – це комунікаційної здатності інформувати власників системи про їхні уражені системи. Це пов’язано з відсутністю стандарту, що описує безпеку команди та за які мережі вони відповідають. Ця проблема ще більше актуально в хмарних середовищах, де нелегко визначити власників а системи.

Інтернет змінюється і що аналітикам безпеки досі не вистачає здатності реагувати на нові загрози. Інтернет збільшується в розмірах і використовується в країнах, які не в змозі будувати розширити можливості для піклування про ІТ-безпеку.

Коли створювався Інтернет, головною ідеєю було те, що кожна організація буде запускати свої служби в своїх системах і буде частиною Інтернету. Проте в останні роки функціонують послуги в Інтернеті різко змінився. Організації користуються стандартними послугами інших компаній, що називаються хмарними провайдерами. Крім того, такі провайдери не тільки надають послуги, а й цілі системи для своїх клієнтів.

Сьогодні все більше організацій більше не керують власною мережею, і тому команда безпеки стикається з проблемою проблема в тому, що системи можуть бути скрізь в Інтернеті та в мережі датчики більше не можна використовувати виключно. Це має величезний вплив на можливості такої команди, і тому необхідно змінити їх стратегію виявлення і реагувати на атаки. Остання зміна в Інтернеті, яка впливає на служби безпеки, - це зростання вбудовані системи та системи керування в Інтернет. Деякі з вбудованих системи створені для меншого бюджету, тому безпека не була частиною їх дизайн, а також процес створення патчів безпеки не на місці. Це призводить до ситуації, коли зараз маємо багато систем, підключених безпосередньо до Інтернет, які мають слабку безпеку, і зловмисники можуть використовувати їх для нарощування ботнет-мереж.

Також проблема полягає в тому, як експерти з безпеки мають зв'язатися з власниками таких пристроїв, тому що часто вони не знають про кінцевих споживачів не мають технічної підготовки. Інша категорія пристроїв – це пристрої, які керуються безпосередньо через Інтернет. Такі пристрої керують критично важливими інфраструктурами, такими як генерування електроенергії. системи або фабрики, що виробляють фармацевтику. Вони пов’язані, тому що це полегшує віддалений моніторинг та обслуговування. Тому атака на такий об’єкт з критичною інфраструктурою стає все більшою легко.

Оскільки компанії поспішили адаптуватися до змін у роботі та бізнес-моделях, викликаних пандемією, багато з них, залишили безпеку на задній план. Половина чи більше опитуваних компанією PWC стверджують, що вони не повністю зменшили ризики, пов’язані з віддаленою роботою (50%), цифровизацією (53%) або використанням хмари (54%).

Забезпечення дистанційної роботи триває до сьогодні. Станом на березень 2020 року сімдесят відсотків організацій покладалися на підхід аутентифікації, орієнтований на паролі, навіть з досягненням біометричних даних, багатофакторної аутентифікації (MFA). Тим часом працівники — особливо представники покоління тисячоліть (51%) і покоління Z (45%) визнають використання додатків і програм на своїх робочих пристроях, які їх роботодавець прямо заборонив . Віддалена робота відсунула переваги організації до звичайних домашніх пристроїв, які не настільки загартовані, як корпоративні мережі.

Важливо, що компанії не завжди враховують унікальні ризики безпеки, пов'язані з впровадженням хмари та віддаленої роботи, або вони не враховують ці ризики достатньо рано, щоб скористатися всіма перевагами хмари та уникнути додаткових витрат.

Хакери, не втрачаючи часу, використовували справжній всплесе векторів атак, які супроводжувалися збільшенням кількості можливих з'єднань, пристроїв, програм і даних. Щонайменше половина організацій повідомили про те, що їх вразило зловмисне програмне забезпечення через оновлення програмного забезпечення (54%), атаки на ланцюжок постачання програмного забезпечення (51%) та компрометація ділової електронної пошти (50%).

За статистикою лише 55% або менше жертв сказали, що вони «добре підготовлені» до усунення порушень, тобто 45% не були.

Безпека ланцюга поставок програмного забезпечення тепер привертає увагу генерального директора та правління. Компанії працюють на коді, розробленому власноруч, взятому з відкритого коду та/або придбаному у постачальників технологій — в екосистемі, яка працює на довірі.

Наприкінці 2020 року підприємствам стало відомо про шпигунську кампанію, яка успішно внесла шкідливе програмне забезпечення в оновлення програмного забезпечення за кілька місяців до його активації. У другій половині 2021 року 64% респондентів опитування очікують збільшення атак на ланцюжок поставок

програмного забезпечення, про які повідомляється, тоді як 66% прогнозують збільшення інцидентів зловмисного програмного забезпечення, про які повідомляється, через оновлення програмного забезпечення.

Попити на програми-вимагачі — і платежі — зростають. Зараз зловмисники зазвичай стягують одну суму за надання цифрового ключа для розблокування файлів і серверів, які вони зашифрували, і окрему викуп, щоб не розкривати вкрадені дані. У США, Канаді та Європі найвищий платіж викупу подвоївся до 10 мільйонів доларів у 2020 році, рекорд швидко був повалений у березні 2021 року з новиною про виплату в 40 мільйонів доларів.

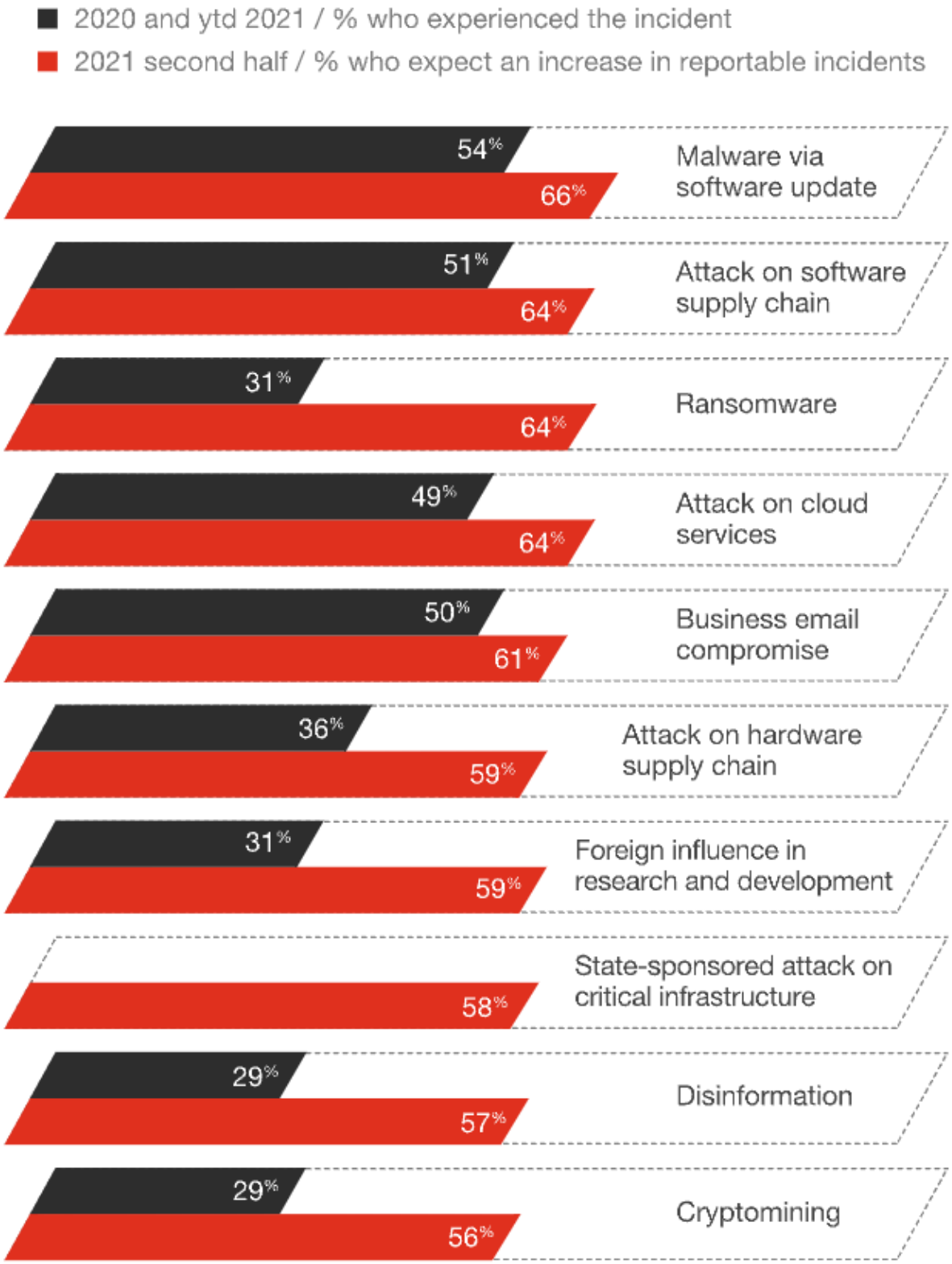

Рис 1.1 Інциденти безпеки в порівнянні 2020 та 2021 рр.

Співробітники за клавіатурою можуть бути мимовільними учасниками порушень даних: 85% порушень у 2020 році були пов’язані з людським фактором, згідно

зі звітом Verizon про розслідування порушень даних за 2021 рік . Переважна більшість порушень через соціальну інженерію спричиняє фішинг, причому об’єктом вибору є хмарні сервери електронної пошти.

Сьогодні більшість випадків обробки інцидентів базується на процесах, розроблених багато років тому. Однак ці процеси були створені в той час, коли можна було обробляти інциденти керувати вручну і тоді, коли зараження систем не відбулося щодня у великій кількості. У більшому організацій кількість уразливих систем може легко перевищити розмір де більше не можливо обробляти їх вручну.

Крім цього, потрібно відстежувати правильний порядок виправлення. Таке відстеження для більшої кількості систем неможливо вручну.

Інша проблема в автоматизації з метою інформування інших груп безпеки, що системи під їх контролем якщо не використовується для здійснення цієї атаки, вам потрібно створити систему, яка дозволить щоб повідомити їх автоматично. Сьогодні більшість команд безпеки створюють власні інструменти під час такої атак і більшість систем не можуть взаємодіяти один з одним.

2. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ТА РЕАГУВАННЯ НА БАЗІ РІШЕНЬ ESET

У минулому концепція кінцевої точки поширювалася лише на робочі станції та сервери. Сьогодні захист розширився, включивши мобільні пристрої, віртуальні середовища, хмарні рішення та багато іншого. IT -інфраструктури стали більш складними і взяли на себе набагато більш важливу роль у підтримці функціонування безперервних процесів. Аналіз великих даних, розподілене зберігання даних, автоматизація процесів – все з них вимагають сучасних підходів до забезпечення безпеки. В той самий час, конфіденційні дані та фінансові активи привертають все більшу увагу кіберзлочинців. Більшість сьогоднішніх загроз - це інструмент завдання шкоди своїм жертвам значних фінансових та репутаційних збитків. Складні атаки становлять новий виклик для розробників рішень для IT -безпеки, а забезпечення ефективного захисту від них вимагає нових підходів. Нижче наведено перелік атрибутів, якими повинен володіти сучасний захист кінцевих точок:

- мінімальний вплив на цільову систему в результаті збалансованої роботи задіяних технологій;
- оперативне виявлення: передові методи виявлення аномальної діяльності, у тому числі використання експертних хмарних сервісів;
- автоматизоване розслідування виявлених інцидентів;
- автоматичний відкат шкідливих дій у системі;
- передача інформації про інциденти в систему кореляції подій SIEM та інші рішення;
- просте управління: інтуїтивно зрозумілий інтерфейс з попередньо налаштованими функціональними можливостями;
- централізоване управління;
- контроль цілісності технологій внутрішнього захисту;
- ефективні послуги: підтримка продукту, дослідження, навчання тощо.

Для кіберзлочинців важливо не лише обходити початкову фільтрацію, але й обійти технології виявлення, відповідальні за раннє виявлення шкідливого програмного забезпечення. Інфекцію можна вважати успішною лише тоді, коли шкідливий код дозволено працювати в середовищі. Для цього кіберзлочинці постійно вдосконалюють свої методи для обходу технологій виявлення. Основні прийоми перераховані нижче:

- пакувальники - містять зловмисне тіло в упакованому вигляді, ускладнюючи його виявлення;
- обфускація коду – використовується спеціальними компіляторами для ускладнення коду рівень алгоритму;
- поліморфізм - коли код шкідливої програми змінюється, поки він є виконується;
- поліморфізм сервера – коли є новий зразок шкідливої програми генерується зловмисним сервером при кожному зверненні до сервера;
- шифрування- багаторівневе шифрування використовується для приховування частини коду механізми виявлення. Часто використовується разом із затемненням;
- уразливості, включаючи 0-day -використання вразливостей програмного забезпечення є ефективним способом зараження;
- обхід пісочниць – пісочниці перевіряють виконуваний файл запустивши його в ізольованому середовищі та проаналізувавши його логіку роботи.

Шкідливий код можна виявити за допомогою сигнатур або евристично. Хакери використовують різні методи модифікації алгоритму коду для запобігання емулятору від визначення його логіки. Використання двох або більше з перерахованих вище методів у поєднанні є потужним кіберзлочином. в практичній практиці, часто використовується для проникнення в середовище захищеного вузла. Єдиний спосіб протистояти цьому - використовувати комплексний технологічний захист поставляється з найновішими методами управління та аналізу виконуваних об'єктів.

З вищенаведеного списку видно, що сучасний захист - це вже не просто механізм виявлення на основі сигнатур. Це цілий ряд складних технологій, що робить управління інфраструктурою ще важливішим. Вибираючи засоби безпеки, слід враховувати також важливі функціональні вимоги. Зрозуміло, які технології застосовуються в середині рішення, і як вони пов'язані між собою. Це точно так важливо оцінити рівень компетенції та досвіду виробника та оцінити здатність продовжувати розвивати технології в майбутньому. Саме тому, сьогоднішній захист – це складних багаторівневий комплекс, який включає в себе управління, моніторинг за складними рішеннями та посилення безпеки шляхом використання додаткових рішень над базовими.

2.1. Технології комплексного захисту кінцевих точок

Еволюція загроз, спрямованих на бізнес, стала причиною появи нового покоління технологій безпеки кінцевих точок.

ESET Endpoint security [9] – це комплексний підхід до комп’ютерної безпеки. Нове ядро сканування ThreatSense, що працює в додатковими модулями брандмауера та антиспаму дозволяє швидко та точнго захищати кінцеву точку. Результатом такого поєднання є інтелектуальна система, яка безперервно захищати від атак та шкідливого програмного забезпечення. Використання ESET Endpoint Security з ESET PROTECT у корпоративному середовищі дозволяє легко керувати будь -якою кількістю робочих станцій клієнта, застосовувати політики та правила, контролювати виявлення та віддалено налаштовувати клієнтів з будь -якого мережевого комп’ютера.

Кожен модуль представлений групою автономних технологій захисту. Це означає, що кожна з технологій здатна автоматично виявляти та блокувати загрози, що належить до його компетенції.

Нині загрози поширюються усіма можливими інформаційними каналами, і це так надзвичайно важливо, щоб периметр захищеного вузла був надійно захищений.

Технології запобіжного блокування використовуються для моніторингу основної діяльності захищеного вузла, що дозволяє раннє виявлення та блокування відомих загроз на усіх можливих способах потрапляння інформації до системи (Інтернет, змінні носії та інші).

Безпека мережевих з'єднань контролюється системою виявлення вторгнень (IDS), яка є мережевим датчиком на основі підписів. Під час роботи IDS застосовує технологію глибокої перевірки пакетів (DPI), що дозволяє мережі датчик для контролю всього прохідного трафіку. Це означає, що він може швидко виявити декілька підозрілих та небезпечних подій в мережі. Деякі приклади мережевих подій:

- активне сканування портів;
- спроби підключення до різних портів операційної системи;
- виявлення ненормального мережевого зв'язку, наприклад, використання дистанційного керування інструменти управління, команди, надіслані з C&C (у випадках, що стосуються бот-мереж). При виявленні небезпечної події в мережі датчик блокує з’єднання використання функцій брандмауера.

Брандмауер - технологія блокування, яка фільтрує мережеву активність захищеного вузол згідно з попередньо встановленими правилами щодо:

- фільтрація мережевих пакетів та потоків даних;
- програмна активність при взаємодії з мережею.

Інтернет -ресурси *є* одним із джерел загроз. Довірений веб-вузол може бути скомпрометований і шкідливий сценарій або 0-day CVE можуть в кінцевому підсумку розміщуватися на ньому, що робить повсякденні операції небезпечні. Для забезпечення зручної та безпечної роботи з Інтернет-ресурсами в ESET Endpoint Security застосовується технологія веб-фільтрації, яка складається з двох рівнів захисту. Перший рівень пов’язаний з хмарною і відповідає за пасивну фільтрацію, тобто забезпечує розвідку в режимі реального часу щодо того, до якої категорії належить веб -ресурс або яка репутація у нього. База даних репутації класифікує URL адреси за такими категоріями:

- шкідлива URL -адреса - становить небезпеку зараження;

- фішингова URL-адреса – використовується для крадіжки особистої інформації;
- невідома URL - інформація про репутацію недоступна;
- захищена URL -адреса - безпечний ресурс. Веб -фільтрація істотно сприяє безпеці, блокує більшість відомих веб-сайтів бути небезпечним і зберігати ресурси захищеного вузла.

Другий рівень заснований на технології динамічного аналізу і аналізу вмісту, що завантажується з усіх невідомих веб -ресурсів.

Портативні пристрої також становлять потенційну загрозу для захищеного вузла. Контроль пристроїв визначає тип підключеного пристрою та пропонує користувачеві просканувати його. Цей контроль допомагає виявити випадки підробки, наприклад, коли змінний носій маскується під клавіатуру, щоб уникнути сканування. Кіберзлочинці використовують цей метод для обману технологій безпеки та проникнення через захищений периметр.

Електронна пошта є однією з точок зараження, яку найбільше використовують кіберзлочинці. Існує ціла тенденція в соціальній інженерії під назвою spear phishing - це підхід розроблений, щоб мати ретельно цілеспрямований вплив. Наприклад, спеціально виготовлений електронна пошта може бути надіслана цільовому користувачеві, що містить експлойт разом із заархівованим вкладення; паролі до архівів можуть бути надані в тілі повідомлення або в графічному вигляді. Це накладає певні вимоги до захисту інструменти, а саме можливість автоматичного відкриття та аналізу заархівованих файлів.

Невід’ємною частиною захисту від шкідливого програмного забезпечення є аналіз файлів на основі підписів. Технологія аналізу на основі підписів застосовується для різних засобів захисту сценарії, коли об’єкт потрібно швидко перевірити на наявність а загроза. У сценарії електронної пошти він потрібен для перевірки вкладених файлів.

Метод на основі підписів має певні переваги; ось чому він застосовується спочатку для аналізу файлів. Його основними перевагами є:

- Швидке виявлення;

- мінімальний рівень помилкових спрацьовувань;
- малий попит на ресурси захищеного вузла.

Цей метод, природно, обмежений кількістю підписів, наявних у бази даних (яка постійно оновлюється). З цієї причини на основі підписів аналіз працює в поєднанні з евристичним аналізом.

У сценарії захисту електронної пошти машинне навчання надає унікальні можливості розпакування захищених паролем архівних вкладень. Для цього він витягує пароль від тіла повідомлення (який є графічним або текстовий формат). Це один із прийомів, які використовують кіберзлочинці для обходу технології виявлення: захищений архів діє як «сейф», вміст з яких недоступні для аналізу. Щоб розпізнати наданий пароль у графічному форматі використовується алгоритм машинного навчання. Після цього, пароль використовується для вилучення вмісту архіву, захищеного паролем.

Додатковим захистом до усіх цих модулів є репутаційний сервіс - це частина ESET Endpoint Secuerity забезпечує виявлення загроз оперативно. Робиться це за допомогою онлайн-баз даних репутації, що містять детальну інформацію про об’єкти. Бази даних постійно поповнюються з експертною інформацією. Інформація, що передається містить зразок або копію файлу, у якому з’явилася загрозу, шлях до цього файлу, ім’я файлу, дату та час, процес, через який загроза з’явилася на комп’ютері та інформацію про операційну систему. Надаючи підзорілі зразки та метадані з усього світу, система захисту на основі хмари дозволяє негайно реагувати на невідомі загрози.

Кожен невідомий файл становить потенційну загрозу для захищеного вузла і вимагає особлива увага з боку технологій захисту.

Для таких випадків багаторівневий захист має просунутий сценарій, в якому глибокий проводиться аналіз із застосуванням методів машинного навчання. Існує кілька технологій аналізу файлів.

- Аналіз файлів на основі підписів. За цим сценарієм технологія на основі підписів відіграє роль базового фільтра - це надає вироки для всіх відомих файлів і

залишає лише невідомі файли аналізується за допомогою методів машинного навчання.

- Аналіз файлів за допомогою методів машинного навчання Це найсучасніша технологія багаторівневого захисту. Він проходить глибоко аналіз файлів, тому загрози можна виявити завчасно. Ця технологія заснована на виконання двох паралельних процесів, які виконують аналіз файлів на статичних і динамічні дані.

Ці два процеси поділяються на три етапи, кожна з яких складається з певних групи технологій. Статичний і динамічний підходи добре працюють поєднувати та компенсувати потенційні недоліки один одного, такі як:

- Коли модель навчається статичним атрибутам шкідливих програм, деякі можуть з'явитися файли, які незначно відрізняються від чистих файлів;
- коли модель навчається за динамічними атрибутами, деякі програми можуть не працювати демонструють шкідливу поведінку – для них може знадобитися конкретне середовище або виділений командний рядок для запуску.

2.2. Призначення та архітектура централізованого керування комплексним захистом на базі рішень ESET Protect

Для того, щоб рішення надійно працювало, у нього є інструменти для управління ним безпеки. Це забезпечує цілісність захисту, включаючи захист від користувача намагається вимкнути його. Ці засоби самозахисту перехоплюють і блокують небезпечні операції з ресурсами у довіреному середовищі, незалежно від прав і привілеїв користувача. Це вирішує проблему вразливостей, які можуть дозволити зловмисній програмі отримати доступ права адміністратора.

Компонент ESET Protect був розроблений для гнучкої безпеки управління. Він надає детальну інформацію про стан кінцевої точки безпеки та про централізовану політику безпеки. Завдяки цьому підвищується безпека корпоративної мережі до наступних особливостей:

- Оцінка вразливості та управління виправленнями;
- інвентаризація обладнання та програмного забезпечення;

- гнучка операційна система та забезпечення додатків;
- розповсюдження програмного забезпечення;
- контроль доступу до складних корпоративних мереж

ESET Protect – консоль адміністрування, що дозволяє віддалено керувати продуктами ESET на робочих станціях, серверах та мобільних пристроях у мережевому середовищі з центрального місця.

ESET Protect використовує клієнт-серверну архітектуру, тобто архітектура в якій клієнти (віддалені кінцеві точки) запитують та отримують послуги від централізованого серверу. Сервери чекають надходження запитів від клієнтів, а потім відповідають на них. В ідеалі сервер забезпечує стандартизований прозорий інтерфейс для клієнтів, щоб клієнтам не було потрібно знати про особливості системи (тобто апаратного та програмного забезпечення), що надає послугу. Клієнти часто перебувають на робочих станціях або на персональних комп'ютерах, тоді як сервери розташовані в інших місцях мережі, як правило, на більш потужних машинах. Ця обчислювальна модель особливо ефективна, коли клієнти та сервер мають окремі завдання, які вони регулярно виконують. При обробці лікарняних даних, наприклад, на клієнтському комп'ютері може бути запущена прикладна програма для введення інформації про пацієнта, тоді як на серверному комп'ютері запущена інша програма, яка керує базою даних, в якій постійно зберігається інформація. Багато клієнтів можуть отримати доступ до інформації сервера одночасно, і в той же час клієнтський комп'ютер може виконувати інші завдання, наприклад надсилати електронну пошту. Оскільки комп'ютери клієнта і сервера вважаються незалежними пристроями, модель клієнт-сервер повністю відрізняється від старої моделі, в якій централізований мейнфрейм виконував усі завдання пов'язаних з ним.

Визначаючи клієнт-серверні системи як системи, що масштабуються, деякі аналітики вважають, що одноранговий зв'язок є більш спритним та універсальним для забезпечення належного управління непередбачуваними робочими навантаженнями. Експерти говорять про такі речі, як зони надмірності та доступності та відновлення після відмови, як засіб для забезпечення безперебійної роботи бізнес-систем онлайн, незважаючи на зміни попиту чи інші проблеми.

Однією з найважливіших проблем є ефективність атаки розподіленої відмови в обслуговуванні (DDoS), оскільки середня модель клієнт/сервер не була налаштована на порогові значення вище певного обсягу трафіку. Пірингові системи можуть вирішити багато з цих проблем та захистити системи від DDoS-атак та подібних кібератак. Періодичний зв'язок також допомагає у вирішенні деяких інших збоїв на основі однієї точки відмови. З появою децентралізованих та розподілених систем, наприклад, незмінних технологій бухгалтерського обліку в блокчейні, однорангові системи стають все більш популярними і починають замінювати архітектури клієнт/сервер.

ESET Protect складається з таких компонентів [10]:

- Сервер ESET Protect – компонент, що обробляє зв’язок з агентами, збирає та зберігає дані в базі даних.
- ESET Management Agent – компонент, що відповідає за зв’язок між ESET Protect та клієнтськими комп’ютерами.
- Датчик виявлення несанкціонованого доступу – датчик ESET PROTECT Rogue Detection (RD) виявляє некеровані комп’ютери, присутні у вашій мережі, і надсилає їх інформацію на сервер ESET PROTECT. Це дозволяє легко додавати нові клієнтські комп’ютери до захищеної мережі. Датчик RD запам'ятовує комп'ютери, які були виявлені, і не надсилатиме одну і ту ж інформацію двічі.
- Apache HTTP Proxy - це служба, яку можна використовувати в поєднанні з ESET PROTECT для розповсюдження оновлень на клієнтські комп’ютери та інсталяційні пакети до агента управління ESET. Додатково можливо налаштувати переадресацію зв'язку від ESET Management Agents до сервера ESET PROTECT.
- Mobile device connector (MDC) - це компонент, який дозволяє керувати мобільними пристроями за допомогою ESET PROTECT, дозволяючи керувати мобільними пристроями (Android та iOS) та адмініструвати ESET Endpoint Security для Android.

- Віртуальний пристрій ESET PROTECT – ESET PROTECT VA призначений для користувачів, які хочуть запустити ESET PROTECT у віртуалізованому середовищі.
- Веб-консоль – основний інтерфейс, який дозволяє керувати клієнтськими комп'ютерами. Він відображає стан клієнтів у мережі та дозволяє віддалено розгортати рішення ESET.

В веб-консолі можливо отримати детальну інформацію про всю інфраструктури та керувати всіма рішеннями безпеки ESET. Це веб-інтерфейс, доступ до якого можна отримати за допомогою браузеру з будь-якого місця та пристрою.

За допомогою веб-консолі можливо отримати доступ до будь-яких компонентів адміністрування, які доступні за допомогою веб-консолі. Серед ключових компонентів та функцій можливо виділити:

1) Панель інструментів (рис. 2.1) – початкова сторінка [11], яка включає в себе інформацію про кількість пристроїв та їх класифікацію згідно з їх станом. Крім цього, можливо створювати користувацькі графічні звіти.

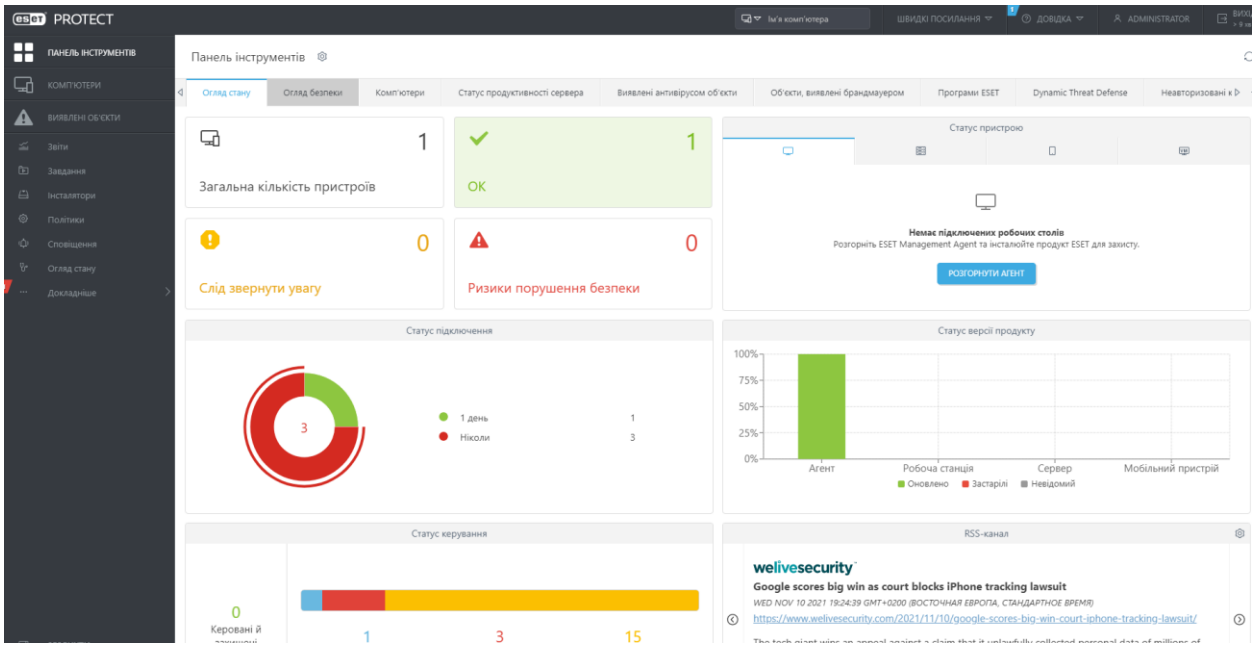

Рис. 2.1 Панель інструментів ESET Protect

З основних графічних звітів можливо виділити:

- «Огляд стану» — це екран за замовчуванням, що відображає загальну інформацію про вашу мережу.
- «Загальна кількість пристроїв» – відображає кількість керованих пристроїв на основі останнього звітного статусу.
- Стан пристрою – відображає кількість керованих пристроїв на основі типу продукту безпеки, встановленого у відповідних вкладках. Якщо жоден продукт безпеки цієї групи не розгорнутий, на вкладці відобразиться варіант розгортання відповідного пакета інсталятора.
- Статус з'єднання - відображає список останніх підключень керованих пристроїв.
- Статус версії продукту – відображає співвідношення актуальних і застарілих версій продуктів безпеки на основі платформи.
- Статус керування – відображає кількість керованих і захищених (клієнтські пристрої з інстальованим агентом ESET і продуктом безпеки), керовані (клієнтські пристрої лише з агентом), некеровані (клієнтські пристрої у вашій мережі, які відомі ESET PROTECT, але без агента) та Rogue (клієнтські пристрої, невідомі ESET PROTECT, але виявлені датчиком Rogue Detection Sensor).
- RSS-канал. Відображає RSS-канал із WeLiveSecurity та порталу бази знань ESET.

2) Комп’ютери (рис. 2.2) – це веб-сторінка, яка включає в себе інформацію за групами за групами відображаються всі клієнтські пристрої, додані до цього ESET PROTECT. Кожен пристрій відноситься до окремої статичної групи. Натисніть групу зі списку (зліва), щоб переглянути учасників (клієнтів) цієї групи на панелі справа.

Некеровані комп’ютери (клієнти в мережі, на яких не встановлено ESET Management agent чи продукт ESET для захисту), які зазвичай відображаються в групі Утрачені та знайдені. Статус клієнта, що відображається у веб-консолі ESET PROTECT не залежить від налаштувань продуктів ESET для захисту на клієнтському комп’ютері. Ось чому навіть якщо певний статус не відображається в клієнті,

відомості про нього все одно передаються на веб-консоль ESET PROTECT. Щоб переміщувати клієнтів між групами можливо перетягти його.

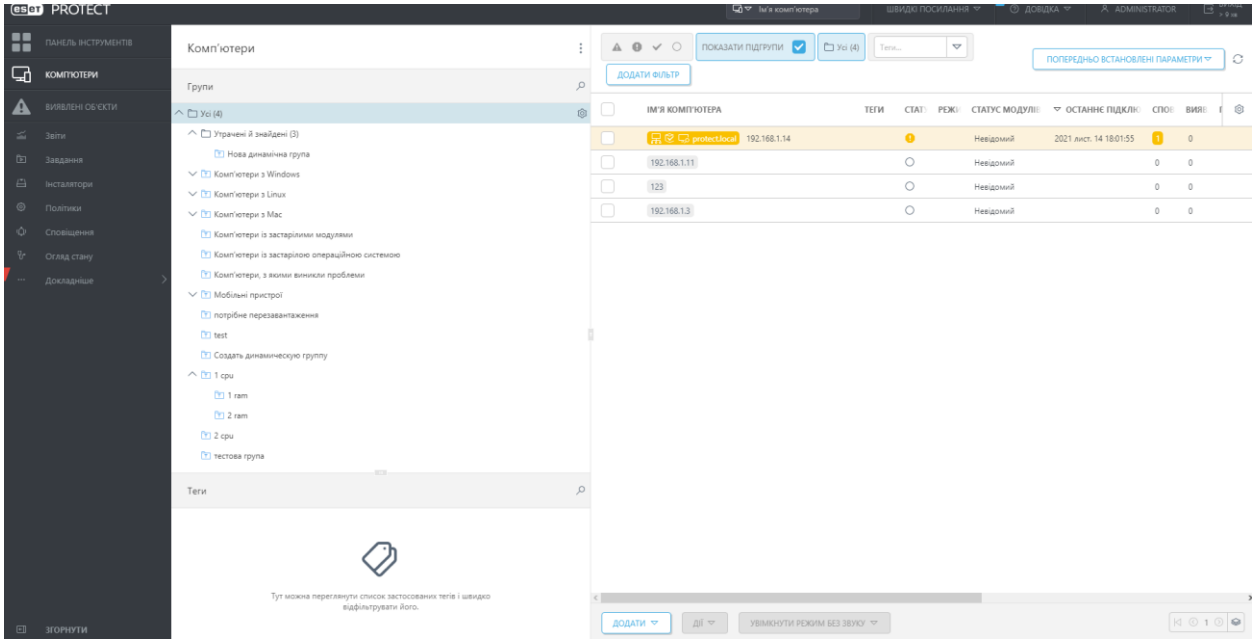

Рис.2.2 Розділ «Комп’ютери» веб-консолі ESET Protect

Групи можна розуміти як папки, де комп’ютери та інші об’єкти класифікуються за категоріями. Для комп’ютерів і пристроїв можна використовувати попередньо визначені групи та шаблони груп або створювати нові. Клієнтські комп’ютери можна додавати до груп. Це дозволяє структурувати комп’ютери та впорядковувати їх. Можливо додавати комп’ютери до статичних груп. Статичні групи керуються вручну, тоді як динамічні групи впорядковуються автоматично на основі певних критеріїв у шаблоні. Коли комп’ютери об’єднані в групи можливо призначити цим групам політики, завдання або налаштування. Потім політика, завдання або налаштування застосовуються до всіх членів групи. Існує два типи груп клієнтів статичні групи та динамічні групи.

Статичні групи – це групи вибраних клієнтських комп’ютерів та інших об’єктів. Члени групи статичні і можуть бути додані/вилучені лише вручну, а не на основі динамічних критеріїв. Об’єкт може бути присутнім лише в одній статичній групі. Статичну групу можна видалити, лише якщо в ній немає об’єктів.

Динамічні групи – це групи пристроїв (а не інші об’єкти, як-от завдання чи політики), які стали членами групи, відповідаючи певним критеріям. Якщо клієнтський пристрій не відповідає цим критеріям, його буде видалено з групи. Комп’ютери, які задовольняють критеріям, будуть додані до групи автоматично.

3) У розділі «Виявлення» (рис. 2.3) наведено огляд виявлення шкідливого програмного забезпечення або шкідливої поведінки на керованих пристроях.

У цьому розділі надається детальна інформація про тип виявлення, дію яку було виконано по відношенню до виявлення. Також, надається інформація на якому комп’ютері було виявлення та час і дату події.

За допомогою контекстного меню можливо виконувати певні ручні дії – сканування комп’ютера, створення виключення.

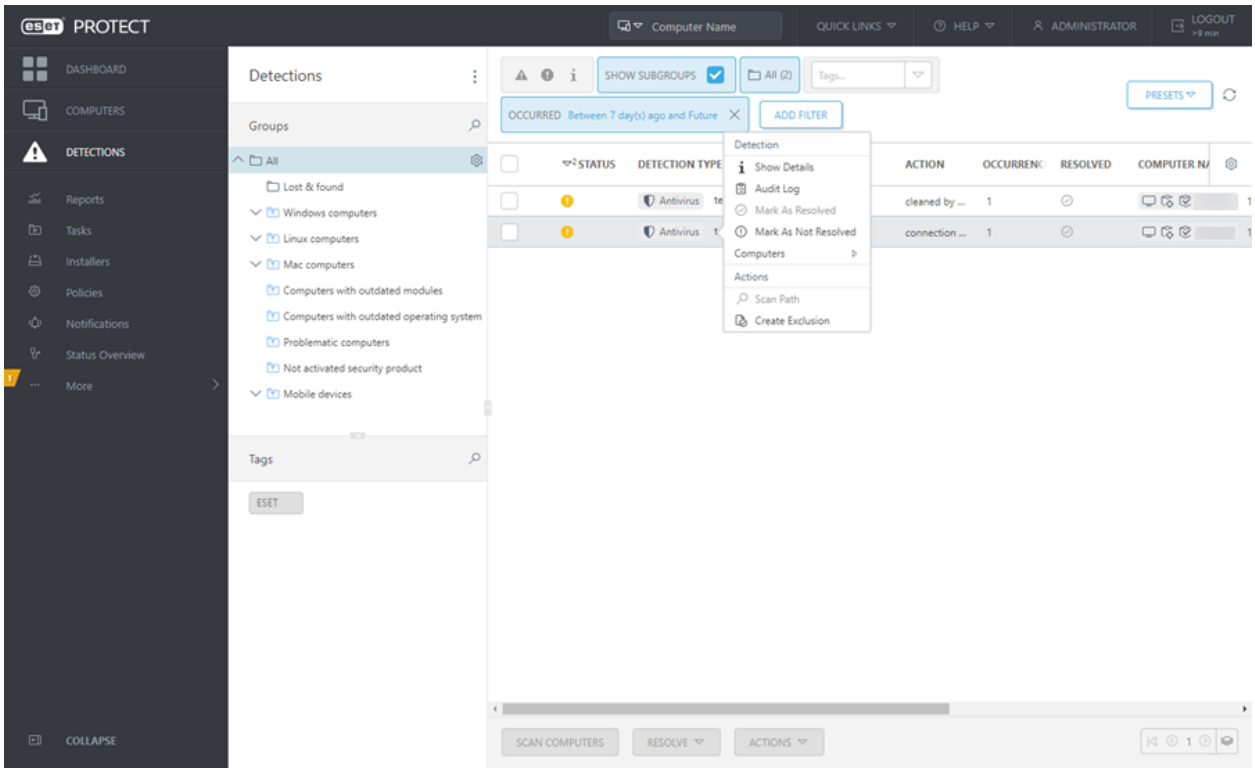

Рис.2.3 Розділ «Комп’ютери» веб-консолі ESET Protect

4) Звіти (рис. 2.4) за допомогою яких можливо отримати доступ до бази даних і можливість відфільтрувати її дані в зручний спосіб. Вікно звітів містить дві таблиці:

- Категорії та шаблони – вкладка за замовчуванням. Вона містить огляд категорій і шаблонів звітів. Можливо створювати нові звіти та категорії або виконувати інші пов’язані зі звітами дії.
- Заплановані звіти – ця вкладка містить огляд запланованих звітів. На ній також можна запланувати новий звіт.

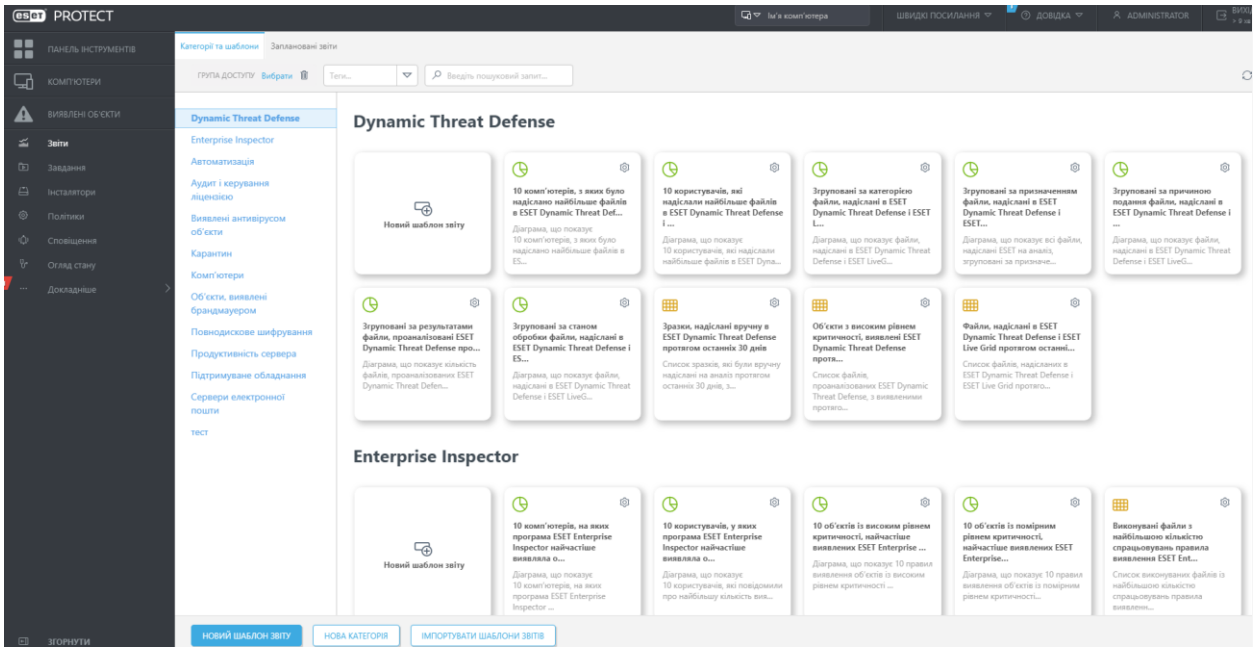

Рис.2.4 Розділ «Комп’ютери» веб-консолі ESET PROTECT

5) Завдання (рис. 2.5) можна використовувати для керування сервером ESET PROTECT, клієнтськими комп’ютерами та інстальованими на них продуктами ESET. Завдання допомагають автоматизувати виконання поширених процесів. Можливо скористатися набором попередньо налаштованих завдань, які охоплюють найпоширеніші сценарії, або створити власне завдання з певними налаштуваннями. Використовуйте завдання для виконання дій на клієнтських комп’ютерах. Для успішного виконання завдання потрібно мати необхідні права доступу до завдання та об’єктів (пристроїв), які використовуються під час його виконання. Щоб дізнатися більше про права доступу, перегляньте список дозволів.

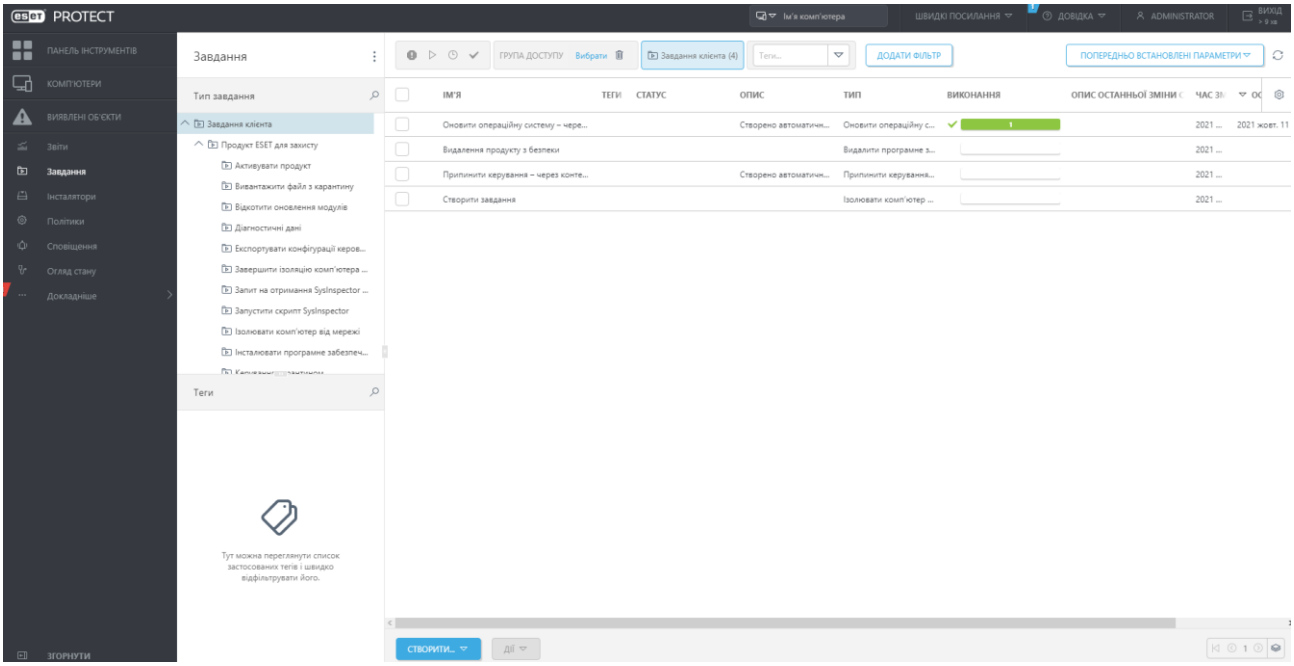

Рис.2.5 Розділ «Завдання» веб-консолі ESET PROTECT

Існує дві основні категорії завдань: завдання клієнта та завдання сервера.

Можливо призначити клієнтські завдання групам або окремим комп’ютерам. Створене завдання виконується за допомогою тригера. Для клієнтського завдання можна налаштувати кілька тригерів. Клієнтські завдання розподіляються на клієнти, коли агент ESET Management на клієнті підключається до сервера ESET PROTECT. Тому може пройти певний час, поки результати виконання завдання передаються на сервер ESET PROTECT. Можливо керувати інтервалом підключення агента ESET Management, щоб пришвидшити виконання завдання.

•Серверні завдання виконує сервер ESET PROTECT самостійно або на інших пристроях. Серверні завдання не можна призначити конкретному клієнту або клієнтській групі. Для кожного серверного завдання можна налаштувати лише один тригер. Якщо завдання потрібно виконати з різними подіями, для кожного тригера має бути окреме серверне завдання.

6) Політики (рис. 2.6) використовуються для застосування певних конфігурацій до продуктів ESET, які виконуються на клієнтських комп’ютерах.

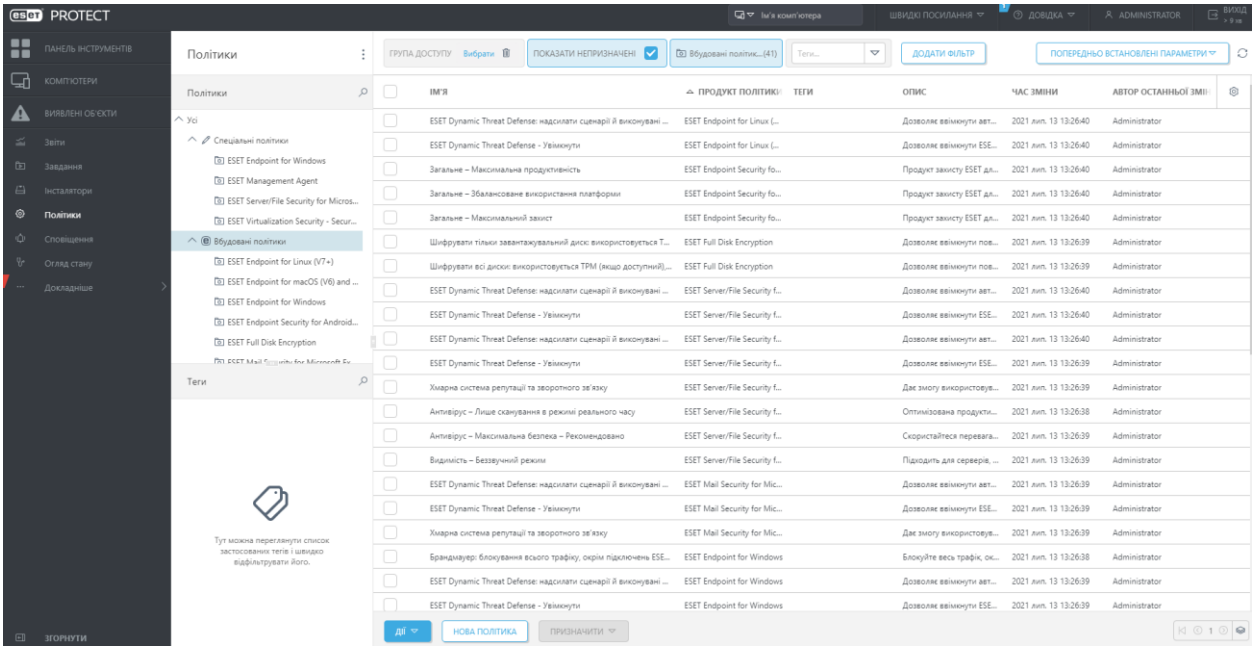

Рис.2.6 Розділ «Політики» веб-консолі ESET Protect

Це дозволяє не налаштовувати продукт ESET на кожному клієнтському комп'ютері окремо. Політики можуть бути спрямовані на окремі комп'ютери або на декілька груп (статичних і динамічних). Комп'ютеру або групі можна призначити кілька політик.

2.3. Призначення та архітектура додаткових рішень ESET для протистояння сучасним кібератакам

2.3.1. Виявлення низькорівневих загроз

Жодне рішення захисту кінцевої точки не може забезпечити стовідсотковий рівень виявлення невідомого шкідливого програмного забезпечення. Щоб допомогти фахівцям із безпеки захищати свої конфіденційні дані, виявляти й досліджувати інциденти безпеки, розширені загрози та цілеспрямовані атаки чи злому на кінцеві пристрої, потрібен інструмент безпеки.

Термін виявлення та реагування кінцевої точки (EDR), також відомий як виявлення і реагування кінцевої точки (EDR), ввів А. Чувакін [12] ще в 2013 році. Як видно з назви, це механізм безпеки кінцевої точки, який не охоплює мережу.

У сфері інформаційної безпеки технологія EDR — це не просто передовий засіб для захисту робочих станцій і серверів від складних загроз. Рік за роком кінцеві точки залишається основною метою зловмисників і найпоширенішою точкою входу в інфраструктуру організації, що вимагає належної уваги та захисту. Телеметрія є цінною інформацією, необхідною для якісного розслідування інцидентів. З появою нового протоколу шифрування TLS 1.3 та його активним поширенням важливість доступу ще більше зросла.

По-перше, технологія EDR може забезпечити видимість команді SOC, і сьогодні більшість організацій в основному зосереджені на моніторингу діяльності мережі.

У рамках роботи центрів моніторингу та реагування на інциденти такі компанії рідко або лише частково підключають кінцеві точки як джерела подій у системах SIEM. Це пов’язано з високою вартістю збору та обробки журналів з усіх кінцевих точок, а також генерацією великої кількості подій для розбору при досить високому рівні помилкових спрацьовувань, що зазвичай призводить до перевантаження та неефективного використання дорогих ресурсів.

Виявлення кінцевих точок і відповідь знаходить ці невловимі атаки. EDR передбачає постійний моніторинг ваших IT-систем у поєднанні з автоматизованим аналізом даних для виявлення підозрілої активності на ваших кінцевих точках (комп’ютерних пристроях, які використовуються у вашій IT-мережі, включаючи ноутбуки, мобільні телефони та сервери).

3 важливих елемента ефективного виявлення кінцевої точки та безпеки реагування (EDR).

Ці компоненти необхідні для успішної безпеки EDR. Ці елементи створюють видимість, необхідну для виявлення порушення безпеки та реагування на нього.

Складні загрози та цілеспрямовані атаки з використанням невідомого шкідливого коду, скомпрометованих облікових записів, безфайлових методів, легітимних додатків та дій, які не несуть під собою нічого підозрілого, потребують багаторівневого підходу до виявлення з використанням передових технологій. Залежно від того чи іншого вендора, EDR зазвичай може включати різні технології виявлення, що працюють в автоматичному, напівавтоматичному режимі, а також вбудовані інструменти, що вимагають постановки завдань вручну, із залученням висококваліфікованих кадрів. Наприклад, це може бути: антивірус, двигун поведінкового аналізу, пісочниця, пошук індикаторів компрометації (IOC), робота з індикаторами атак IOC, зіставлення з техніками MITRE ATT&CK, а також автоматична взаємодія з Threat Intelligence та ручні запити до глобальної бази даних про загрози, ретроспективний аналіз, можливість проактивного пошуку погроз (Threat Hunting).

Кожне рішення EDR покладається на дані як основний елемент для створення “глобальної картини” подій які були під час атак. Тут можна виділити два основні компоненти:

Збір даних: система безпеки EDR повинна постійно контролювати кінцеві точки та збирати телеметрію (запис і передачу показань кінцевої точки) в режимі реального часу, не заважаючи звичайним системним процесам. Ці дані включають широкий спектр процесів які відбуваються на кінцевому пристрої, наприклад, системні процеси, мережеві з’єднання або передача даних. Якщо кінцеві точки проявляють нетипову поведінку, це може вказувати на можливу атаку.

Зберігання даних: оскільки зібрані дані кінцевої точки є об’ємними, більшість малих підприємств повинні планувати зберігати ці дані в хмарі. Хмарна база даних загроз забезпечує належну ємність для зберігання в міру зростання зібраних даних. Вона також дозволяє поєднувати дані кінцевої точки з аналізом загроз або сховищем інформації про загрози безпеки, щоб допомогти визначити ознаки зловмисної діяльності.

Щоб визначити потенційні атаки, системи EDR повинні просіяти зібрані дані кінцевої точки, щоб позначити аномалії. Для цього розслідування потрібна аналітика в режимі реального часу, що виконується за допомогою засобів автоматизації

та експертизи, які використовуються фахівцями з IT-безпеки, такими як пошук загроз або центр операцій безпеки (SOC).

Якщо обсяг даних занадто великий ці дані надходять в автоматизовані механізми виявлення загроз, такі як механізми машинного навчання, щоб корелювати мережеву активність і поведінку загроз. Ця технологія шукає зразки, що означають потенційні загрози, такі як індикатори компроментації (IOC) та індикатори атаки (IOA). IOC — це криміналістичні дані, що сигналізують про можливе порушення безпеки. IOA передбачає дії кіберзлочинців для створення APT, наприклад приховування в пам'яті комп'ютера.

Криміналістичний аналіз передбачає, що люди досліджують елементи, позначені автоматичним аналізом, щоб перевірити наявність загрози. Наприклад, збільшення трафіку веб-сайту в нетипові години або з підозрілих регіонів потребує людського розуміння, щоб підтвердити, що це проблема. Можуть виникати помилкові результати, наприклад, новий комп'ютерний сценарій, створений IT-командою для автоматизації процесів. Рішення EDR повинно підтримувати механізм відмітки законної діяльності, позначеної як потенційна загроза, наприклад додавання їх до білого списку, щоб уникнути подальшого позначення.

Після того, як аналіз підтвердить загрозу, EDR має виконати швидкі дії. Швидке реагування на інциденти безпеки допомагає звести до мінімуму або запобігти збитки, такі як вкрадені фінансові дані або дані клієнтів.

Реакція на інцидент може варіюватися від надсилання автоматизованих сповіщень і автоматичного виходу користувача кінцевої точки до закриття доступу до мережі та ізоляції кінцевої точки до того, як зараження може поширитися. Будь-яка технологія EDR, повинна підтримувати кілька варіантів відповіді, які можна налаштувати відповідно до потреб організації.

Успішна безпека EDR включає в себе можливості виявлення, сортування, дослідження та усунення. Вони представляють етапи фільтрації даних кінцевої точки для реагування на загрозу.

Процес безпеки EDR починається з виявлення загрози. Щоб автоматизовані системи EDR знаходили загрози, встановлюється програмний агент на свої кінцеві точки для збору даних.

Агент постійно відстежує кінцеву точку і збирає дані телеметрії, надсилаючи їх до центральної бази даних, де алгоритми машинного навчання аналізують дані на наявність аномалій. Раптові зміни в процесах кінцевої точки або поведінці користувачів від звичайної поведінки позначаються для подальшого дослідження.

Приклади підозрілих дій включають спробу входу на кінцеву точку з віддаленого клієнту, завантаження певних типів програмних файлів або вимкнення брандмауерів. EDR поєднує ці ознаки нетипової поведінки з ланцюгом подій до і після, щоб створити карту виконуваних процесів. Завдяки цьому більш широкому контексту в поєднанні з розвідкою про загрози системи EDR можуть оцінювати мільярди подій у мережі, щоб звузити активність, яка свідчить про кібератаку.

Далі платформи EDR повідомляють IT-персоналу про підозрілу активність. Вони надсилають сповіщення та надають інформаційні панелі та звіти, що підсумовують результати алгоритмічних висновків. Саме тоді відбувається сортування. IT-команда повинна усунути помилкові спрацьовування. Вони також класифікують сповіщення як відомі шкідливі дії, які негайно запускають етап усунення, або невідомі для розслідування. Фаза сортування є найскладнішою для IT-команд. Вони часто переповнені сповіщеннями, і команда може пропустити діяльність, яка потребує більш глибокого розслідування.

Потім IT-команда перевіряє кожний потенційно атакований об’єкт, використовуючи методи пошуку загроз, щоб зібрати додаткові подробиці. Ці подробиці дозволяють краще зрозуміти діяльність і чому вона відбувається. Наприклад, незнайомий комп’ютерний процес, що виконується на кінцевій точці, може означати атаку або просто те, що працівник завантажив нове програмне забезпечення. Ключ до етапу розслідування – швидкість. Сучасні кібератаки використовують тактику, яка дозволяє інфекціям переміщатися від однієї кінцевої точки до іншої, швидко

заражаючи великі частини мережі. Хороша система EDR прискорює фазу дослідження, що призводить до швидшої реакції та виправлення для стримування таких переміщень.

Підтверджені загрози вимагають відповіді, щоб платформи EDR могли діяти автоматично.

Відповіді включають тактику, як-от зупинку будь-яких комп'ютерних процесів, що виконуються на зараженій кінцевій точці, та ізоляцію кінцевої точки від решти мережі. Деякі рішення EDR можуть автоматично рятувати файли та дані, що зберігаються на кінцевій точці, одночасно видаляючи інфекцію. Розуміння мети кіберзлочинця та того, як сталася атака, дозволяє вжити відповідних дій. Це також дає змогу компаніям збирати конкретні знання для посилення безпеки мережі.

Таким чином, EDR розширюють можливості SOC, оскільки вони виявляють і попереджають як користувача, так і групи реагування на надзвичайні ситуації про нові кіберзагрози. EDR в значній мірі засновані на правилах; тим не менш, машинне навчання або методи штучного інтелекту поступово знайшли свій шлях у ці системи, щоб полегшити пошук нових закономірностей і кореляцій. EDR розширює антивірусні можливості, оскільки EDR ініціює сповіщення, коли виявить аномальну поведінку. Тому EDR може виявити невідомі загрози та запобігти їх до того, як вони стануть шкідливими через поведінку, а не лише через підписи.

ESET Enterprise Inspector (EEI) — це інструмент, який забезпечує безперервний захист і моніторинг безпеки в потужному та простому у використанні рішенні. EEI збирає дані в режимі реального часу на кінцевих пристроях. Дані узгоджуються з набором правил для автоматичного виявлення підозрілих дій. Потім агреговані дані обробляються, а інформація визначається пріоритетом і співвідноситься у формі з можливістю пошуку. Ці агреговані дані дозволяють спеціалісту з безпеки більш ефективно шукати незвичайні та підозрілі дії та дають змогу точно реагувати на інциденти, керувати ними та звітувати. ESET Enterprise Inspector — це рішення, яке включає в себе три такі компоненти [13]:

- EEI Agent встановлюється на кінцевих пристроях, які контролюються EEI і збирають дані для EEI, видаляє шкідливі компоненти та блокує виконання цих компонентів.
- EEI Server постійно об’єднує та зберігає зібрані дані та відображає їх на веб-консолі EEI
- EEI Web Console — це інтерфейс користувача для ESET Enterprise Inspector, створений як веб-додаток HTML5

При вході до серверу ESET Enterprise Inspector Вас зустрічає панель інструментів.

Інструментальна панель (рис. 2.7) надає швидкий огляд стану мережі щодо роботи ESET Enterprise Inspector. Він показує часові рамки виявлення (залежно від їх серйозності), вказуючи, чи перебуває мережа під потенційною/існуючою атакою чи ні, який тип виявлення зініціюється, або чи потрібно впоратися з потоком, налаштувавши виявлення. Він показує карту всіх знайдених виконуваних файлів у мережі, групуючи їх за мережею та популярністю LiveGrid, допомагаючи відфільтрувати безпечні та добре відомі виконувані файли з тих, які можуть бути унікальними та непопулярними взагалі, і які можуть вказувати цілеспрямована атака.

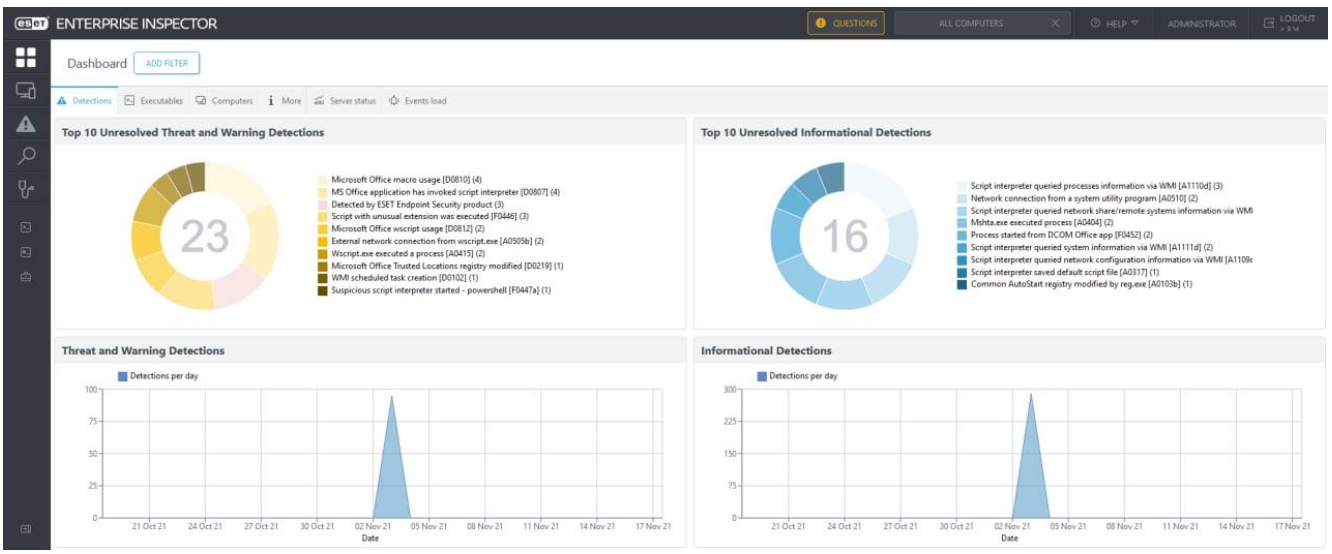

Рис.2.7 Панель інструментів ESET Enterprise Inspector

Панель інструментів також показує виконувані файли з підозрілою поведінкою, згруповані за кількістю виявлень (загальних та унікальних), які вони ініціювали. Другий погляд орієнтований на «комп’ютер» і допомагає вам визначити потенційно небезпечні комп’ютери або комп’ютери, що вказує на підозрілу поведінку, яку варто розслідувати. Також присутня спеціальна інформаційна панель «Огляд керівника», яка показує іншу статистику про різні серйозності, пріоритети, статус вирішеного/невирішеного, статус підключення, статус подій, статус версії агента та стан комп’ютера. Існує також статус сервера, який вказує, чи працює середовище EEI і чи всі системні служби працюють правильно, без надмірного використання системних ресурсів. Доступні такі вкладки:

1. Виявлення
2. Виконувані файли
3. Комп'ютери 4.Більше
4. Статус сервера
5. Навантаження на систему

Основним розділом для виконання аналітичних дій є Detections (рис. 2.8).

Правила, написані виявлення підозрілого і шкідливого поведінки, викликають виявлення з певною мірою серйозності. Кожне виявлення, що спрацювало, відображається в розділі виявлення з чіткою ідентифікацією того, де воно відбулося (комп'ютер), який виконуваний файл викликав його, навіть який конкретний процес викликав його. Він супроводжується інформацією про серйозність, як визначено у правилі, і призначає пріоритет кожному виявленню (пізніше буде доступним як опція фільтрації). Виявлення також відображаються у в вкладці Виявлення в вебконсолі ESET PROTECT.

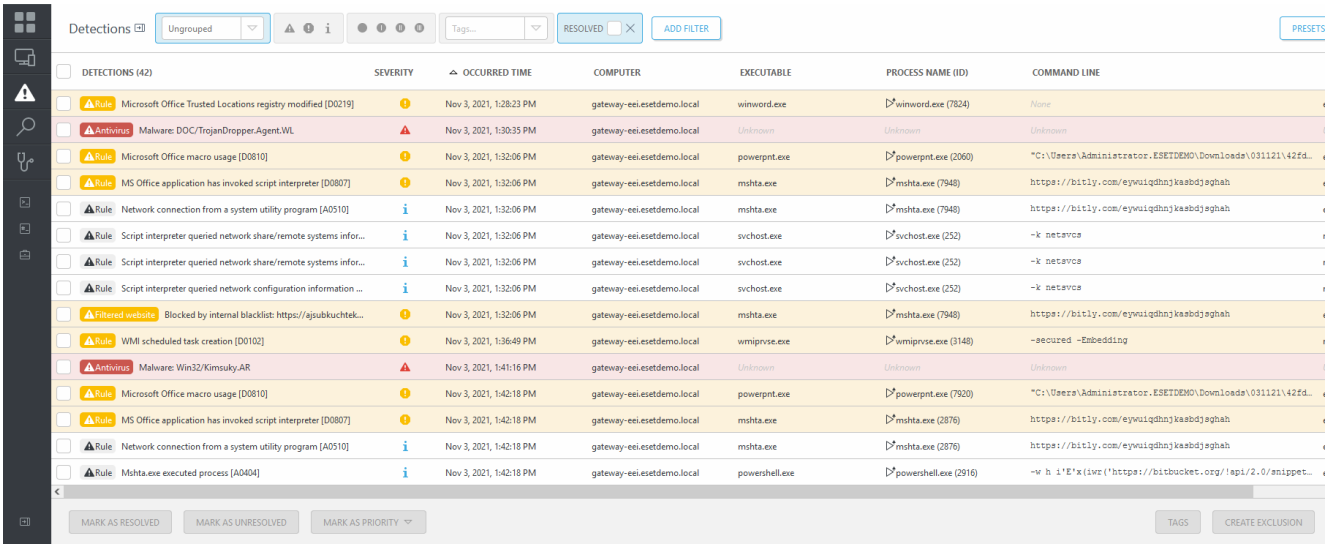

Рис.2.8 Розділ «Detections» веб-консолі ESET Enterprise Inspector

Існує не менш важливий розділ, який надає інформацію про виконувані файли (рис. 2.9). На цій вкладці можливо побачити інформацію про статистику виконуваних файлів по всій інфраструктурі.

В цьому розділі можливо дізнатися:

- Популярність виконуваного файлу — можливо побачити графічний перетин Популярності LiveGrid і Популярності в мережі.
- Популярність LiveGrid —скільки комп'ютерів повідомили про виконуваний файл LiveGrid.
- Популярність мережі — кількість комп'ютерів, які мають цей модуль на підприємстві
- Статус виконуваного файлу — цей розділ показує стан виконуваних файлів на основі невирішених виявлення. Натискання кругової діаграми або назви статусу переспрямує вас до списку виконуваних файлів із вибраним статусом
- Проблемні виконувані файли — у цьому розділі наведено список проблемних виконуваних файлів, які виникли на комп'ютерах, що контролюються. Після натискання імені проблемного виконуваного файлу перенаправляється в розділ «Відомості про виконуваний файл» . Клацніть правою кнопкою миші назву виконуваного файлу або клацніть лівою кнопкою миші будь-де в рядку, щоб відкрити контекстне меню з такими параметрами:

- Seen On — інформація на яких робочій станціях цей процес відбувається або відбувався

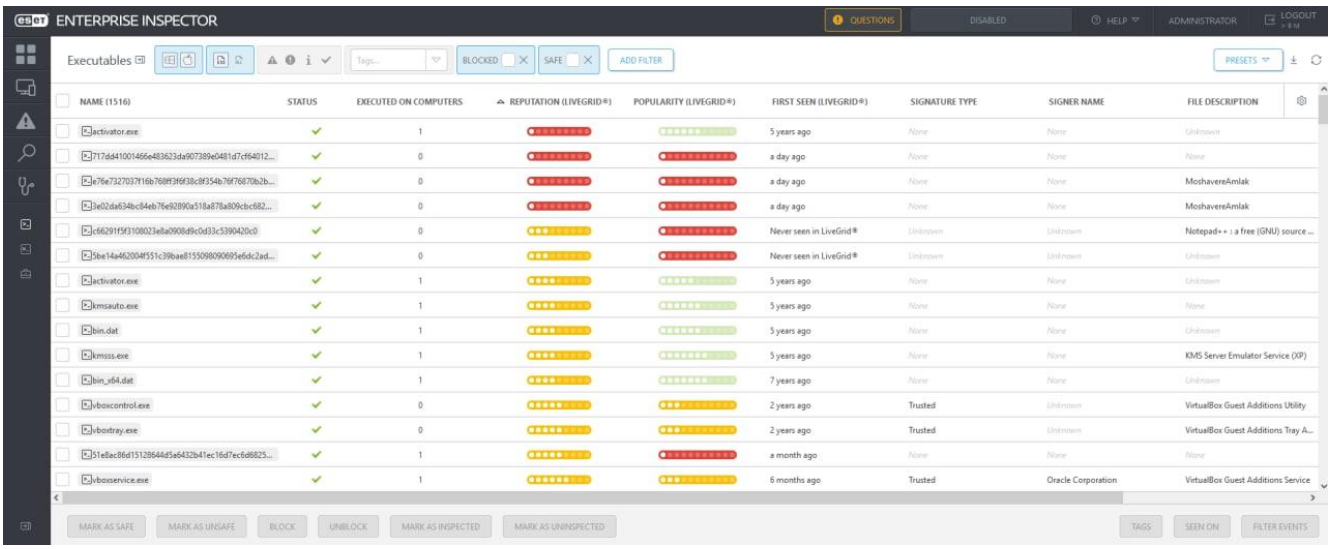

Рис.2.9 Розділ «Executables» веб-консолі ESET Enterprise Inspector

Багато останніх атак/заражень здійснюються за допомогою зловмисного програмного забезпечення «без файлів», яке відбувається шляхом виконання скриптів, які передають шкідливе корисне навантаження або здійснюють будь-яку шкідливу дію.

EEI забезпечує детальну видимість усіх сценаріїв (рис. 2.10), які були виконані в компанії, і показує подробиці про те, які зміни були внесені, а також про те, чи викликав будь-який із сценаріїв специфічне визначення на основі поведінки.

Інженери безпеки можуть побачити деталі події, усе дерево процесів, детальні параметри командного рядка (аргументи) тощо – усі деталі, необхідні для детального криміналістичного розслідування.

Важливою особливістю Scripts View є можливість групувати сценарії за «командним рядком», що дозволяє легко виявляти аномалії або потенційно підозрілі дії. Наразі підтримуються сценарії, написані на Visual Basic і Powershell/ WScript/CScript. Можливо визначити скрипт як:

- безпечний — безпечний стан, який використовується багатьма правилами для визначення ризику. Позначка як безпечна впливає на виявлення. Позначка

як безпечна не обов'язково гарантує, що певний модуль ніколи не буде включено до виявлення. Існує кілька сотень правил, і деякі викликають виявлення, незалежно від того, який модуль виконав підозрілу дію. Наприклад, популярний екземпляр, надійні модулі, як powershell, може зробити це. Інші правила намагаються оцінити ризик на основі модуля. Такі правила враховують прапор «безпечний». Цей прапор означає, що користувач проаналізував модуль, і малоймовірно, що модуль є шкідливим, тому правила припускають, що ризик нижчий під час оцінки.

- Небезпечний**.**
- Створити виключення — створити виключення для сценарію.

Крім цього, можливо завантажити сценарій — відкриває вікно для завантаження сценарію для подальшого вивчення. Тільки якщо скрипт ще доступний у мережі.

Сторінка скриптів надає інформацію:

- про критичність скрипта за допомогою графічного визначення критичності.
- Тіло скрипта
- Користувач, який виконував його
- Комп'ютер на якому виконувались дії

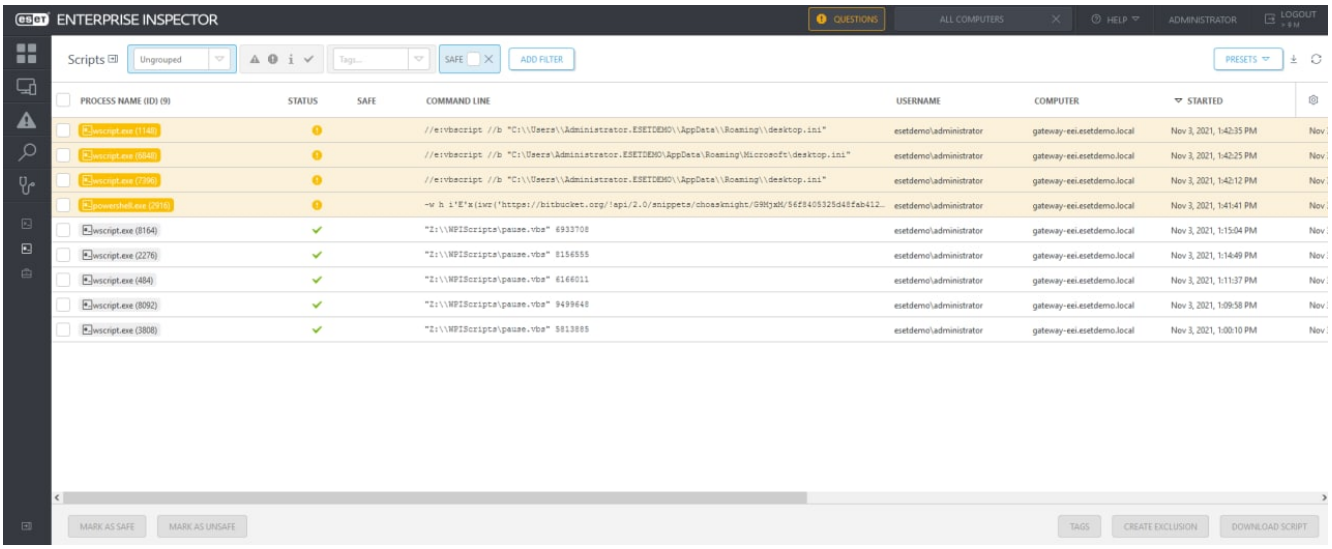

Рис.2.10 Розділ «SCRIPTS» веб-консолі ESET Enterprise Inspector

Вкладка «Адміністратор» (рис. 2.11) використовується для керування правилами та додавання хешів, виконання яких інженери безпеки хочуть заблокувати у своїй мережі. Можливо запустити завдання для подій, що відбулися, створювати виключення для процесів і налаштовувати параметри сервера.

Ви можете перемикатися між такими шістьма вкладками:

1. Правила виявлення
2. Виключення
3. Завдання
4. Заблоковані хеші
5. Налаштування сервера
6. Аудит
7. Запитання

Останній цікавим елементом є правила — це описи поведінки та репутації, які EEI може ідентифікувати з отриманих подій і метаданих.

Інженери з безпеки можуть додавати та редагувати свої правила, але існує також набір правил, наданий ESET, які не можуть бути змінені інженерами з безпеки.

Правило визначається за допомогою мови на основі XML. Правила узгоджуються на сервері асинхронно, тому є певний інтервал часу, коли останні події надсилаються від клієнта до сервера, а потім обробляються правилами. Узгоджене правило може сповістити інженерів безпеки лише шляхом підвищення рівня виявлення.

Виявлення відображається в режимі виявлення, але воно також експортується в ESET PROTECT, а звідти в кінцевому підсумку на підключений інструмент SIEM або електронний лист може бути автоматично надіслано, коли виявлення запускається за допомогою механізму сповіщень ESET PROTECT.

На підставі результатів розслідування інженер безпеки може виконати вручну дію по виправленню.

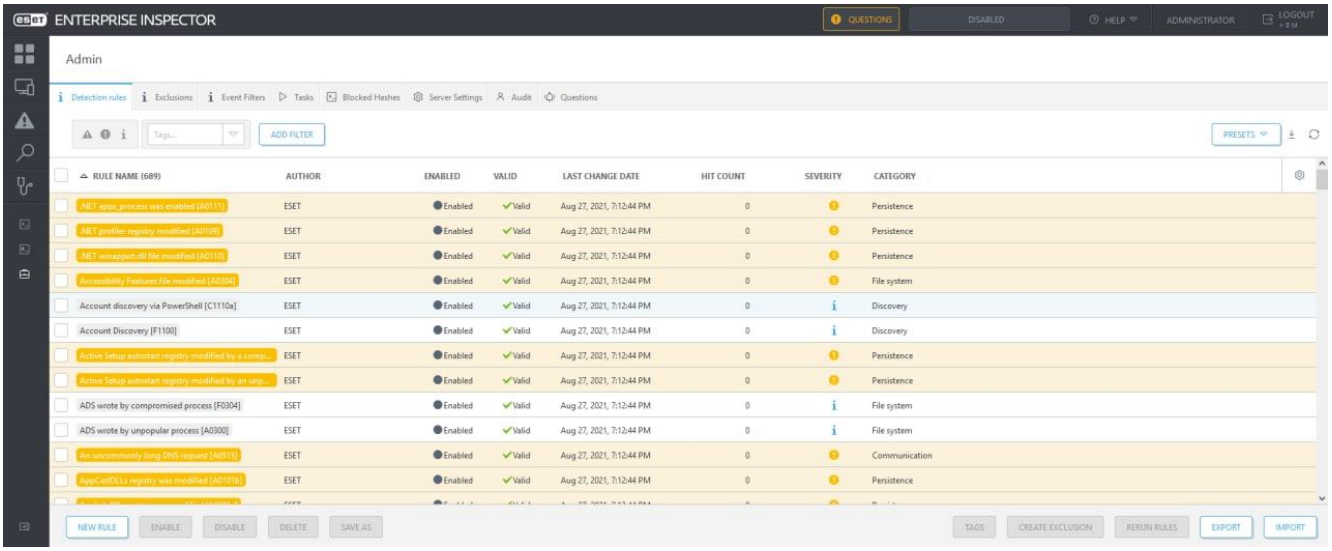

Рис.2.11 Розділ «Detection rules» веб-консолі ESET Enterprise Inspector

2.3.2. Багатофакторна аутентифікація за допомогою технологій ESET Secure Authentication

Загальний процес аутентифікації для MFA вимагає принаймні двох із трьох методів автентифікації, описаних у PCI DSS [14]:

- Щось ти знаєш, наприклад пароль або парольна фраза. Цей метод передбачає перевірку інформації, яку надає користувач, наприклад, пароль/пароль, PIN-код або відповіді на секретні запитання (заклик-відповідь).
- Щось у вас є, наприклад пристрій-токен або смарт-картка. Цей метод передбачає перевірку певного елемента, який є у користувача, наприклад фізичного або логічного маркера безпеки, маркера одноразового пароля (OTP), картки доступу співробітника або SIM-картки телефону. Для мобільної аутентифікації смартфон часто надає коефіцієнт володіння разом із програмою OTP або криптографічним матеріалом (тобто сертифікатом або ключем), що знаходиться на пристрої.
- Щось ти, наприклад біометричний. Цей метод включає перевірку властивих індивіду властивостей, таких як сканування сітківки ока, сканування райдужної оболонки, сканування відбитків пальців, сканування вен пальців, розпізнавання обличчя, розпізнавання голосу, геометрії рук і навіть геометрії мочки вуха.

Інші типи інформації, такі як геолокація та час, можуть бути додатково включені в процес аутентифікації; однак завжди слід використовувати принаймні два з трьох зазначених вище факторів. Наприклад, дані про геолокацію та час можуть використовуватися для обмеження віддаленого доступу до мережі суб'єкта відповідно до робочого графіка особи. Хоча використання цих додаткових критеріїв може ще більше знизити ризик викрадення облікового запису або зловмисної активності, метод віддаленого доступу все одно має вимагати автентифікації за допомогою принаймні двох з наступних факторів: те, що ви знаєте, щось у вас є, і те, що ви є.

Найпоширенішим типом аутентифікації, який використовується сьогодні, є однофакторна аутентифікація, в основному комбінація імені користувача/пароля. Один фактор у цьому випадку є те, що знаєте, тобто пароль. Більшість мереж і більшість Інтернет-ресурсів використовують основну комбінацію імені користувача та пароля, щоб надати доступ до захищеного або приватного ресурсів.

Загальна комбінація імені користувача та пароля є формою однофакторної аутентифікації; єдиним фактором є пароль. Використання двофакторної аутентифікації забезпечує значне підвищення безпеки в порівнянні з традиційною комбінацією імені користувача/пароля.

ESET Secure Authentication (ESA) [15] додає двофакторну автентифікацію (2FA) до доменів Microsoft Active Directory або локальної мережі, тобто одноразовий пароль (OTP) створюється та надається разом із загально необхідними іменем користувача та паролем. Або створюється push-сповіщення, яке має бути затверджене на мобільному телефоні користувача під керуванням ОС Android, iOS або Windows, коли користувач успішно аутентифікується за допомогою своїх загальних облікових даних доступу.

ESA складається з наступних компонентів:

- Плагін ESA Web Application забезпечує 2FA для різних веб-програм Microsoft
- Плагін ESA Remote Desktop забезпечує 2FA для протоколу віддаленого робочого стола

- Плагін ESA Windows Login забезпечує 2FA для комп’ютерів Windows
- Сервер ESA RADIUS додає 2FA до аутентифікації VPN
- Конектор ESA Identity Provider
- Служба аутентифікації ESA включає API на основі REST, який можна використовувати для додавання 2FA до спеціальних програм
- Інструменти управління ESA: oESA, встановлений у середовищі Active Directory:
- Плагін ESA User Management для користувачів і комп'ютерів Active Directory (ADUC) використовується для керування користувачами
- Консоль керування ESA під назвою ESET Secure Authentication Settings використовується для налаштування ESA важливий 2FA увімкнено для користувача адміністратора домену Якщо користувач адміністратора домену увімкнув 2FA під час оновлення ESA 2.7.x або 2.8.x, доступ до екрану «Користувачі та комп’ютери Active Directory» ESET Secure Authentication та ESA Management Console буде видалено. Замість цього потрібно використовувати веб-консоль ESA. Крім того, дозвольте доступ до веб-консолі (також стосується інструментів керування) за допомогою додавання в білий список IP-адрес або вимкнути 2FA для користувача адміністратора домену, створити іншого користувача з вимкненою 2FA та додати користувача до групи адміністраторів ESA або вимкнути 2FA для ESA. Веб-консоль.
- ESA Web Console, універсальний інструмент керування, є кращим способом налаштування ESET Secure Authentication та керування користувачами oESA, встановлений в автономному режимі: ▪ESA Web Console, універсальний інструмент керування, використовується для налаштування ESET Secure Authentication та керування користувачами Якщо ESA інстальовано в середовищі Active Directory, воно зберігає дані в сховищі даних Active Directory. Оскільки дані ESA автоматично додаються до ваших резервних копій Active Directory, немає потреби в додаткових політиках резервного копіювання.

2.3.3. Технологія точного визначення та виявлення шкідливих програмних забезпечень за допомогою хмарної пісочниці ESET Dynamic Threat Defense

Підозрілі зразки, які ще не підтверджені як зловмисні та потенційно можуть містити зловмисне програмне забезпечення, автоматично надсилаються в хмару ESET. Надіслані зразки запускаються в пісочниці та оцінюються вдосконаленими механізмами виявлення шкідливих програм. Шкідливі зразки або підозрілий спам надсилаються в ESET LiveGrid. Вкладення електронної пошти обробляються окремо і підлягають подачі в ESET Dynamic Threat Defense [16] (рис. 2.12). Адміністратори або користувачі можуть визначати обсяг файлів, які надсилаються, а також період зберігання файлу в хмарі ESET. Документи та PDF-файли з активним вмістом (макроси, javascript) за замовчуванням не надсилаються.

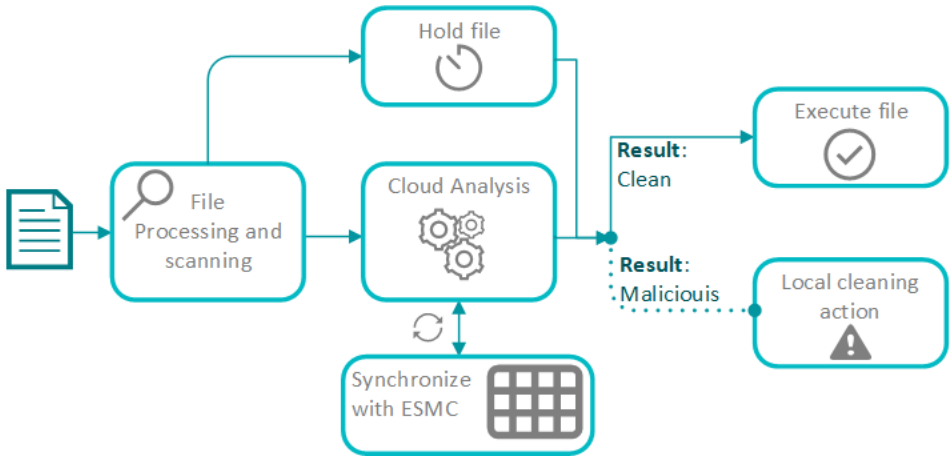

Рис.2.12 Схема роботи хмарної пісочниці ESET Dynamic Threat Defense

Кожен файл, виявлений продуктом ESET Endpoint Security / ESET Server Security, сканується та відкривається. Якщо файл оцінюється як підозрілий, він надсилається на аналіз. Це частина активного захисту. Можливо налаштувати період очікування, протягом якого файл блокується, і користувач повинен дочекатися результату аналізу. Хмара ESET зберігає результати аналізу в хмарній базі даних. Продукт безпеки ESET виконуватиме локальне очищення на основі результатів аналізу та налаштувань політики кожної машини (процес припиняється негайно або при наступному виконанні).

3. РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ЗАХИСТУ ТА АВТОМАТИЗАЦІЇ РЕАГУВАННЯ НА ІНЦИДЕНТИ НА БАЗІ КОМПЛЕКСУ РІШЕНЬ ВІД ESET

3.1 Розроблення топології системи захисту та варіантів автоматизації реагування на інциденти безпеки на кінцевих точках на базі рішень від ESET.

Кіберзагрози загалом найкраще подолати за допомогою багаторівневого підходу, використовуючи серія фільтрів для подолання все більш ухильних форм загроз. ESET використовує багаторівневий підхід, включаючи комплексний захист кінцевих точок та виявлення низькорівневих загроз.

Коли загроза потрапляє на хост, механізм захисту кінцевої точки використовує весь асортимент модулів. Усі ці модулі можливо розділити на три етапи використання.

Перший етап це до виконання файлу. Цей етап включає в себе декілька процесів. Перш за все це включення комп’ютера, серверу (в майбутньому хост). Запуску хосту можна поділити на завантаження декількох розділів, перед завантаження операційної системи – UEFI, інтерфейс між операційною системою і мікропрограмами, які керують низькорівневими функціями комп'ютерного обладнання, далі вже йде завантаження MBR розділу, перший фізичний сектор на жорсткому диску або іншому носії інформації, якщо цей пристрій розподіляється на логічні диски (розділи). MBR містить таблицю розділів (partition table) і невеликий фрагмент виконуваного коду.

Мета MBR — не завантаження ОС, а всього лише вибір, з якого розділу саме відбувається завантаження. При різних рівнях проникнення до системи можливо помістити шкідливе програмне забезпечення на завантажувальні сектори. В цьому випадку є модуль, що перевіряє на вміст такого. Після завантаження операційної системи є різні підходи до потрапляння шкідливого файлу до самої операційної системи.

Коли кажемо про класичний тип вірусів – це виконуваний файл, що робить шкідливі дії в системі. На сьогоднішній день під тип класичних вірусів можливо додати не тільки виконувані файлу, але й документи. В залежності від типу потрапляння їх до системи автоматично реагують відповідні модулі. Першим рівнем аналізу є виявлення на основі цифрових відбитків в системі. Такі та більш складні загрози, що можуть потрапляти через Інтернет, включаючи експлойт вразливостей, реагують модуль Захист від мережевих атак.

Якщо ж файл не може бути визначеним попередніми модулями, є певні критерії оцінки або виведення рейтингу файлу. ESET LiveGrid визначає рейтинг файлу в залежності від критеріїв (повіденки, цифрового підпису та інше) та видимість на інших робочих станціях по світу.

Наступний етап, це етап, коли файл вже виконує свої дії. Для виявлення такого аналіз поведінки в реальному часі, що постійно покращує себе завдяки машинному навчанню. Крім цього, в реальному часі аналізується поведінка за різними критеріями різним компонентами для більш точного виявлення поведінки файлу.

Останній етап – це етап після виконання файлу, тобто коли процес вже працює в системі. Нерідко зустрічаються шкідливі програмні забезпечення, які чекають потрібного випадку, щоб проявити свою активність. Такі віруси базуються на часі, в основному. Тобто, вони запрограмовані на те, що в цей чай виконати шкідливу дію або завантажити додаткові модулі для шкідливих дій. Для виявлення такого є автоматизовані модулі реагування – перевірка трафіку завдяки модулі Захисту від ботнетів та оцінка репутації файлів, які завантажуються.

Відфільтрувавши більшість шкідливих програм за допомогою цих простих і автоматизованих процесів, ресурси можуть бути зосереджені на дуже малій частині, що залишилася. Зазвичай це невиявлені загроз, що належать до складних атак, які здатні ухилятися від виявлення та розширені атаки, які можуть бути звичайно бути максимально шкідливими та руйнівним з усіх ось тут на допомогу приходить EDR.

Одне з головних завдань EDR – забезпечити видимість – допомогти команді безпеки побачити, що насправді відбувається на кінцевих точках. Швидкий доступ

до даних інцидентів, збагачений інформацією та сканування на предмет компрометації (IoCs) є важливими елементами у моніторингу безпеки на кінцевих точках.

Іншим ключовим компонентом діяльності EDR є розслідування.

Навіть якщо EDR відреагувала на – видалення файлу або ін'єкцію процесу в легітимний процес (без шкідливого програмного забезпечення), це не завжди означає, що загроза була розглядатися, особливо в більш складні напади. Розуміння першопричини загрози означає не допускати її залишки компонентів залишаються непоміченими. Наприклад, можна просто видалити шкідливий файл все одно залишати хакера підключеним до хоста за допомогою інших засобів і вбивати один процес не може запобігти повторному зараженню, якщо першопричину не виявлено.

Нарешті, багато сьогоднішні загрози розвиваються дуже швидко, а наслідки їх невиконання. Швидке виявлення компонентів загрози може бути руйнівним (вимагач — це лише один із них приклад). Тому швидка і бажано автоматизована відповідь має вирішальне значення, а не лише виявлення і розуміння загрози, але й нейтралізації її

Аналіз першопричин інциденту цілком може призвести до створення індикатора. Індикатор компрометації (IoC) на основі дій, пов’язаних із виявленою загрозою. Сканування для IoCs є, як вже говорили, важливим захисним механізмом в EDR, що дозволяє зрозуміти, які інші хости могли бути скомпрометовані або де є ознаки присутності загрози.

Відомі IoC (наприклад, надані вам вашим регулюючим органом або зібрані з певного інформаційного бюлетеня або списку розсилки) можна імпортувати в рішення і звичайним автоматичне сканування як для нещодавно створених, так і для імпортованих IoC є важливим для підтримання здоров'я системи. Сканування на наявність IoC, згенерованих з аналізованої загрози на а регулярна основа є цінною, оскільки дуже можливо, що та сама загроза знову виникне майбутнє. І якщо відомо, що конкретна атака відбувається на такі організації, як ваша, і IoC доступні, регулярне сканування цих імпортованих IoC допоможе вам знайти, і реагувати на цю загрозу в найкоротші терміни.

Рішення EDR повинні мати можливість генерувати швидку, автоматизовану відповідь, що може:

- Ефективно обробляється одним із двох способів: за допомогою автоматизації (коли, наприклад, IoC
- Було запущено сканування та знайдено загрози, що потребують негайної реакції) або безпосередньо від картки попередження, якщо, наприклад, співробітнику служби безпеки потрібно ізолювати хост під час аналізу.
- Варіанти відповіді можуть включати запобігання виконання файлу (наприклад, створити правило для
- блокувати файл із певним хешем для запуску на хостах), ізоляції зараженого хоста, видалення
- файл і автоматично сканує інші хости на наявність ознак зараження за допомогою EPP.

3.2 Технологія автоматизованого реагування на інциденти безпеки на кінцевих точках

Автоматизація безпеки – це автоматичне виконання завдань безпеки без втручання людини **.** Це включає будь-які дії безпеки, пов’язані з виявленням, аналізом, запобіганням або усуненням кіберзагроз, які є автоматизованими (тому, машинними) і сприяють забезпеченню безпеки організації та відіграють активну (або ще краще, проактивну) роль у майбутніх стратегіях безпеки. .

До автоматизації багато виснажливих завдань безпеки виконувались практиками та аналітиками, які проходили численні сповіщення, аналізували та вирішували, чи реагувати на них і як.

Завдяки автоматизації безпеки групи безпеки тепер оснащені рішенням, яке може працювати на них і виконувати всі завдання з безпеки, які потребували часу у фахівців з безпеки. Цінний час, який можна використати для залучення до більш стратегічних заходів та роботи над активними заходами безпеки.

Є кілька ознак, які говорять нам, що завдання безпеки слід автоматизувати:

- Повторювані повсякденні завдання : рутинні завдання, які виконуються щоденно або регулярно, наприклад, перегляд сповіщень безпеки та їх аналіз, щоб відрізнити помилкові спрацьовування від справжніх сповіщень і потенційних загроз.
- Набридливі, одноманітні завдання **:** завдання безпеки, які завжди дотримуються подібних правил і кроків. Наприклад, інцидент безпеки, пов'язаний із позначеною електронною поштою та потенційною спробою фішингу, вимагатиме від аналітиків вручну перевіряти URL-адреси, інформацію про власника домену, геолокацію IP тощо.
- Завдання, що забирають багато часу **:** такі завдання безпеки, як кореляція даних і пошук закономірностей у зібраних даних, можуть зайняти багато часу, і цей час може бути неоціненним для виявлення підозрілої діяльності до того, як відбудуться реальні атаки.

Загалом, команди SOC та служби безпеки протягом тривалого часу переважно використовували автоматизацію безпеки . Його введення розглядає кілька ключових проблем, з якими стикаються ці команди, які найкраще відображаються через переваги, які він їм приніс

Розроблення рекомендацій щодо застосування технології управління захистом на кінцевих точках

Беручи до уваги кількість інструментів, поверхню атаки, яку вони відстежують, і кількість інцидентів безпеки, на які ці інструменти реагують, багато з яких є просто помилковими, можливо зробити висновок, що кількість створених сповіщень є значною. Насправді настільки істотні, що звіти показують, що 31,9% спеціалістів із безпеки ігнорують сповіщення, через велику кількість помилкових спрацьовувань.

Втома від оповіщення трапляється з багатьма командами безпеки, тому важко залишатися в тренді під час постійного розвитку кіберзагроз.

Боротьба з проблемою втоми попередження також підвищує продуктивність і ефективність офіцерів безпеки. Автоматизація безпеки візьме на себе процес виявлення, розслідування та посилення попереджень безпеки, тому аналітики безпеки

залишатимуться зосередженими на перевірці та реагуванні на реальні загрози, принципово зупиняючи порушення безпеки .

Іншою перешкодою безпеки є «бонус», який постачається з великою кількістю інструментів і сповіщень, що може призвести до повільної реакції та, у свою чергу, до повільного часу вирішення. Оскільки надходить багато сповіщень, команда безпеки не може проаналізувати кожне з них, тому дії реагування на інциденти неефективні. Це дає зловмисникам важелі впливу.

Швидко ідентифікуючи та розрізняючи небезпечні джерела попереджень безпеки, автоматизація безпеки скорочує час, необхідний для реагування на інцидент. Це вирішує кіберзагрози в режимі реального часу, визначає їх пріоритети, визначає, чи потрібно вживати будь-яких заходів, і, якщо так, передає їх до призначеного аналітика з безпеки, який робить наступні кроки для забезпечення локалізації та вирішення інциденту. Все це робить організацію більш стійкою до різних видів кіберзлочинності .

Ручна робота завжди передбачає, щонайменше, невелику ймовірність людської помилки та, як наслідок, неточних даних. Використовуючи автоматизацію та виключаючи участь людини принаймні в одній області, можливо значно знизити ймовірність помилки, оскільки щоразу дотримуються однакові правила та процедури. Крім того, впровадження в процес рішення для автоматизації безпеки значно покращить точність і узгодженість розслідувань попереджень і даних про загрози, оскільки виснажливі завдання, під час яких можуть виникнути помилки, виконуються за вас.

Усі вищезгадані переваги зводяться до цієї останньої й часто згадуваної переваги автоматизації безпеки — покращення рентабельності інвестицій на автоматизацію та наявні інструменти та рішення безпеки.

Впроваджуючи автоматизацію, організації можуть дозволити своїм аналітикам витрачати більше часу на більш глибокий аналіз і більш стратегічне залучення до процедур безпеки протягом того ж періоду часу, що приносить більшу віддачу від інвестицій в автоматизацію.

Поступове і поетапне впровадження автоматизації безпеки дозволить залишатися під контролем, що дозволить покращити та відстежувати процес і отримати повну перевагу з точки зору безперервності бізнесу та загальної кіберстійкості.

Перш ніж використовувати автоматизацію безпеки, потрібно знати, які завдання слід, а які не слід автоматизувати. Розпізнавання, які типи інцидентів вирішують, і з яких джерел або видів діяльності відбувається більшість інцидентів; а також найбільш трудомісткі завдання, пов'язані з вашою командою безпеки.

Люди чудово вміють робити багато речей, але нудні завдання, які вимагають майже абсолютної точності, все ще не є нашою найсильнішою стороною. Відсутність зосередженості, низька концентрація та помилки знайдуть свій шлях. Якщо ця помилка станеться під час атаки, діяти буде пізно. Деякі незмінні завдання, які забирають час аналітиків (і які зазвичай автоматизовані):

- Визнання
- Виправлення
- Оцінка вразливості
- Моніторинг безпеки
- Пріоритетність сповіщень
- Збагачення даних
- Реакція на інцидент
- Ескалація оповіщення
- Керування ідентифікацією та доступом

Хоча деякі завдання та процеси практично призначені для автоматизації та виконання без участі людини, щоб вони були ефективними, не кожне завдання може або навіть повинно бути повністю автоматизованим.

Прості, повторювані завдання можна легко вирішувати за допомогою широкого спектру доступних інструментів і рішень безпеки, але складні, глибші проблеми та дії, які вимагають критичного мислення, розширеного вирішення проблем і впевненого прийняття рішень, все ж краще довірити вашій команді безпеки.

Ось деякі приклади завдань, які не слід автоматизувати:

- Полювання на загрози

- Тестування на проникнення
- Зворотна інженерія
- Цифрова криміналістична експертиза
- Побудова стратегічного плану безпеки

Зосередивши автоматизацію на завданнях нижчого рівня, групи безпеки можуть зосередитися на завданнях, які потребують їх активної участі та виконання завдань, які справді може забезпечити лише людина.

3.3 Розроблення рекомендацій щодо застосування рішення ESET для автоматизованого реагування на інциденти

Інциденти безпеки – це будь-які події, що можуть вплинути на основні властивості інформації. В такому ключі можливо використати різні підходи в залежності від рівня складності інциденту. Умовно можливо розділити прості інциденти (не встановлено рішення для безпеки, не оновлена операційна система) та більш складні, тобто ті, що включають в себе загрози більш складного характеру (віруси, сценарії та інше).

Автоматизація простих інцидентів можлива за допомогою консолі адміністрування ESET Protect. Можливо створити динамічну групу під багато критеріїв для кожного з унікальних випадків.

1) Машини, які потребують оновлення операційної системи. Хакери люблять вади безпеки, також відомі як вразливості програмного забезпечення. Уразливість програмного забезпечення — це діра або слабкість у безпеці, виявлена в програмній програмі чи операційній системі. Хакери можуть скористатися перевагами слабкості, написавши код для націлювання на вразливість. Код упакований у шкідливе програмне забезпечення — скорочення від шкідливого програмного забезпечення.

Експлойт іноді може заразити ваш комп’ютер без будь-яких дій з вашого боку, окрім перегляду шахрайського веб-сайту, відкриття скомпрометованого повідомлення або відтворення зараженого медіа. Шкідливе програмне забезпечення

може викрасти дані, збережені на вашому пристрої, або дозволити зловмиснику отримати контроль над вашим комп’ютером і зашифрувати ваші файли.

Оновлення програмного забезпечення часто включають виправлення програмного забезпечення. Вони закривають діри в безпеці, щоб не допустити хакерів.

Автоматичне визначення машин, які потребують оновлення можливе за допомогою наперед встановленої динамічної групи «Комп’ютери із застарілою операційною» (рис. 3.1) .

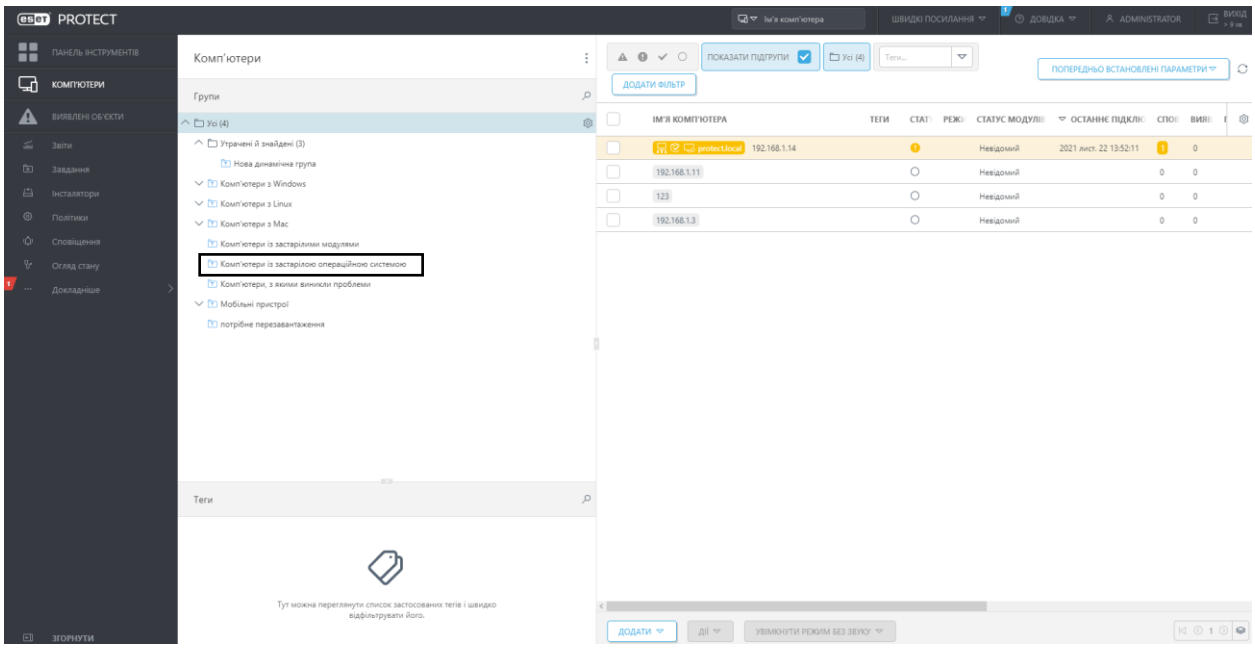

Рис.3.1 Динамічна група «Комп’ютери із застарілою операційною системою»

Після автоматичного визначення можливо назначити автоматичне завдання на оновлення. Переходимо в «Завдання» (рис. 3.2), де можливо створити «Завдання клієнта».

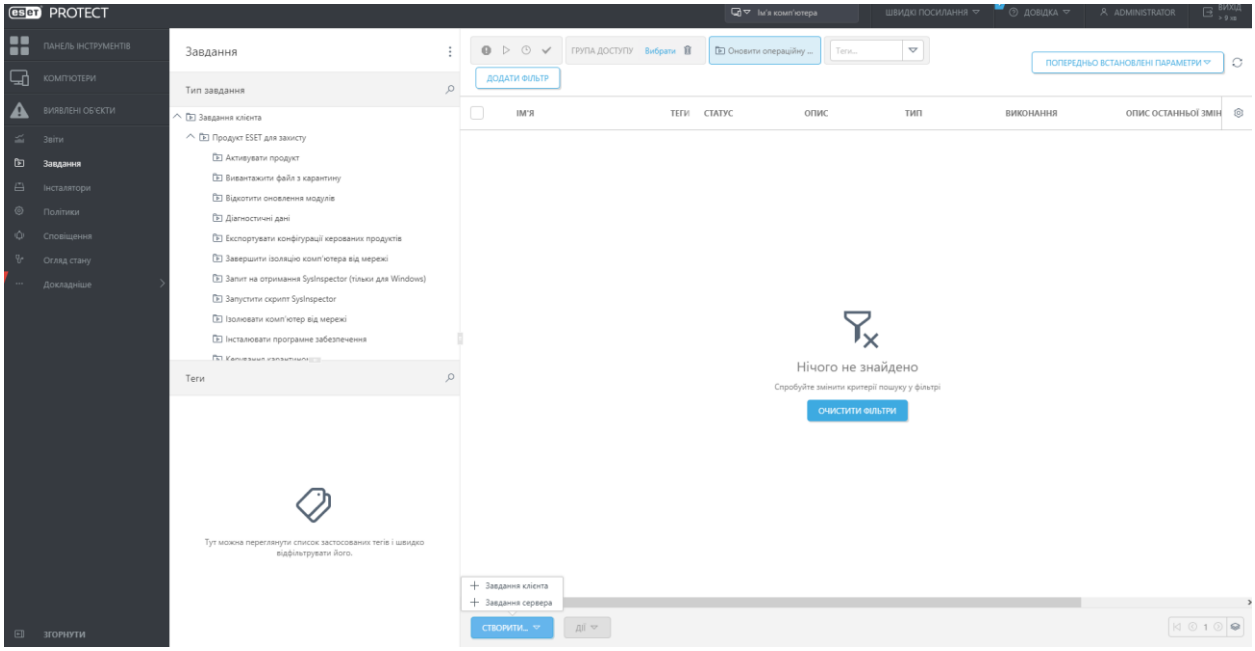

Рис.3.2 Створення завдання клієнта

Для оновлення операційної системи є окреме завдання, що включає в собі такі унікальні параметри (рис. 3.3.) як «автоматичне прийняття ліцензійної угоди», «Інсталяція додаткових оновлень», «Дозволити перезавантаження». Та кожний зможе налаштувати процес оновлення операційної системи з тими параметрами, які йому необхідні.

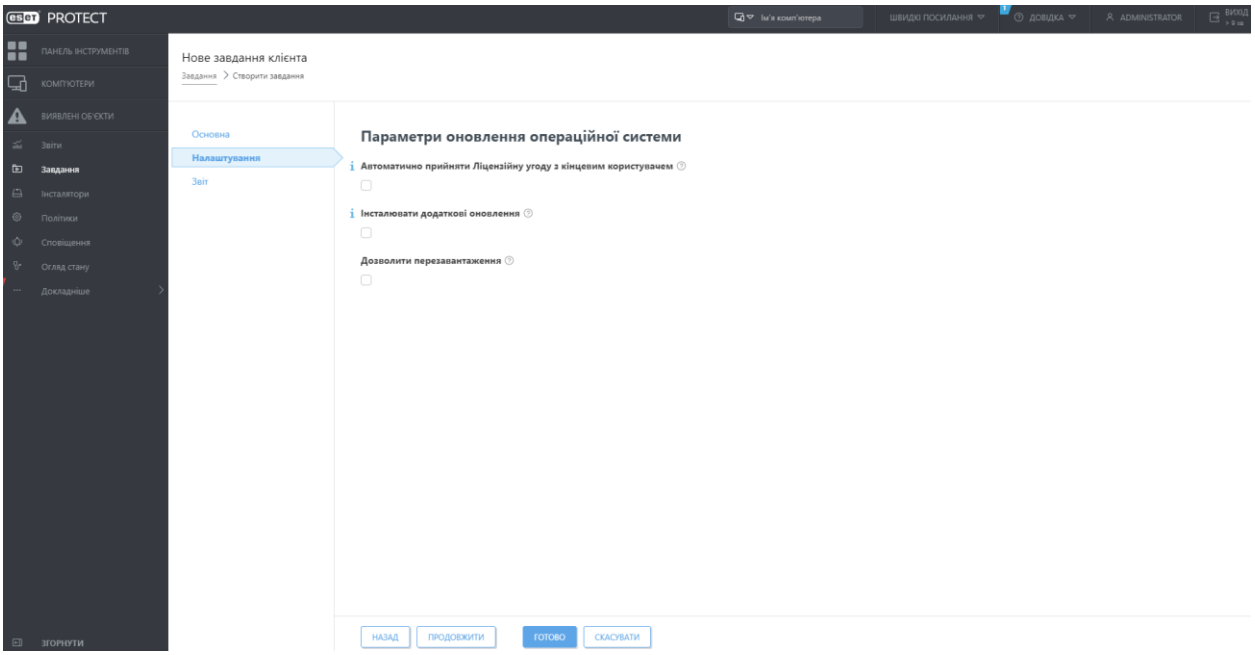

Рис.3.3 Налаштування завдання оновлення операційної системи

Для приєднання завдання клієнта з динамічною групою можливо створити тригер (рис. 3.4)

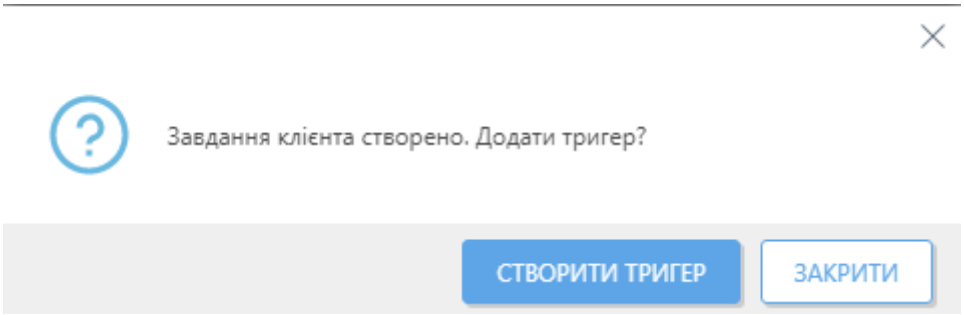

Рис.3.4 Створення тригеру

В якому можливо вибрати необхідну динамічну групу (рис. 3.5)

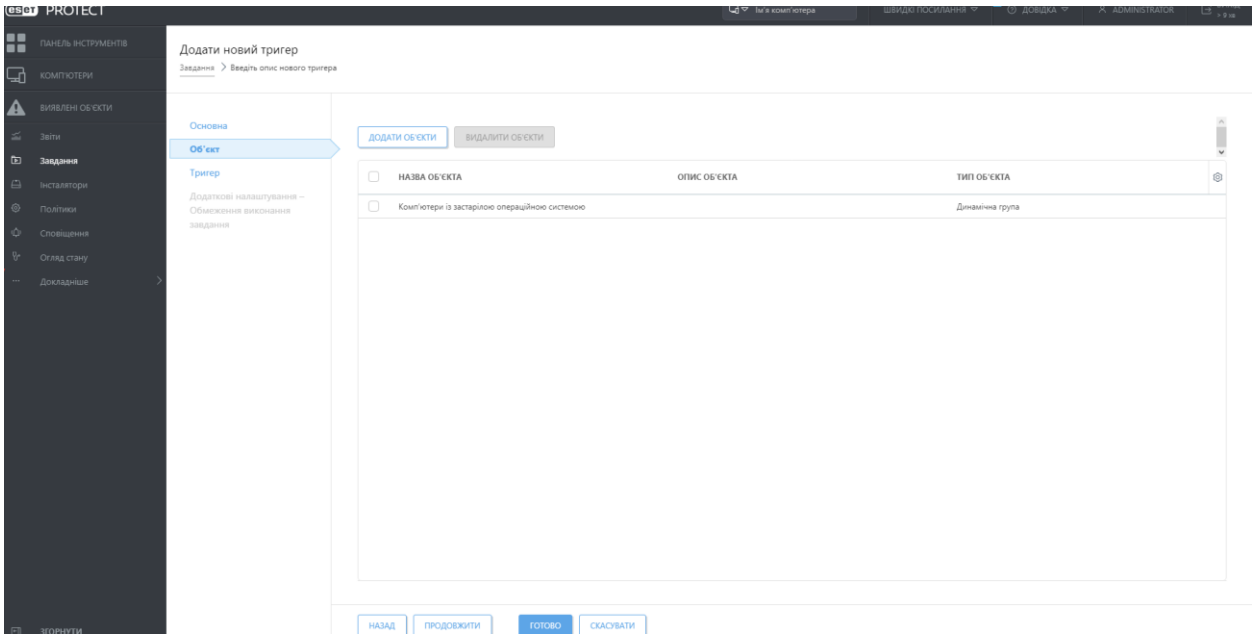

Рис.3.5 Призначення відповідній групі автоматичну дію

Для автоматизації існує тригер «Увійшов до динамічної групи» (рис. 3.6), який зробить створене завдання на тих комп’ютерах, що отримали певний критерій.

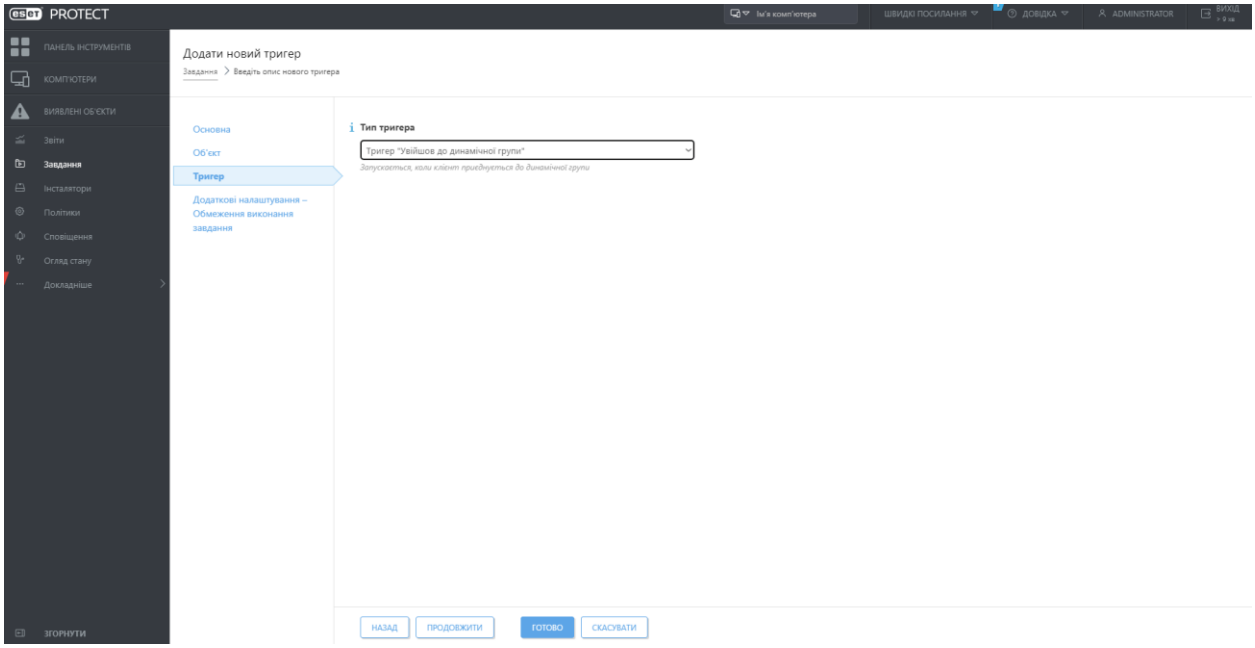

Рис.3.6 Визначення тригеру, коли виконувати дію

Іншим цікавим ключем буде визначення машини, де не встановлено машини, які не маються продукту безпеки (рис. 3.7) – автоматично встановлювати.

Такі машини можливо поділити на ряд:

1) Ті, що не мають агент керування. Коли говоримо про повноцінний захист Active Directory не повинна обходити таку інфраструктури, тому можливо за допомогою AD визначити нові комп’ютери та встановити їх автоматичне встановлення.

2) Ті, що мають агент керування. Для таких комп’ютерів є наперед встановлена група, яка визначає де не встановлено продукт з безпеки. Для автоматичної реакції потрібно створити завдання клієнта за попереднім принципом.

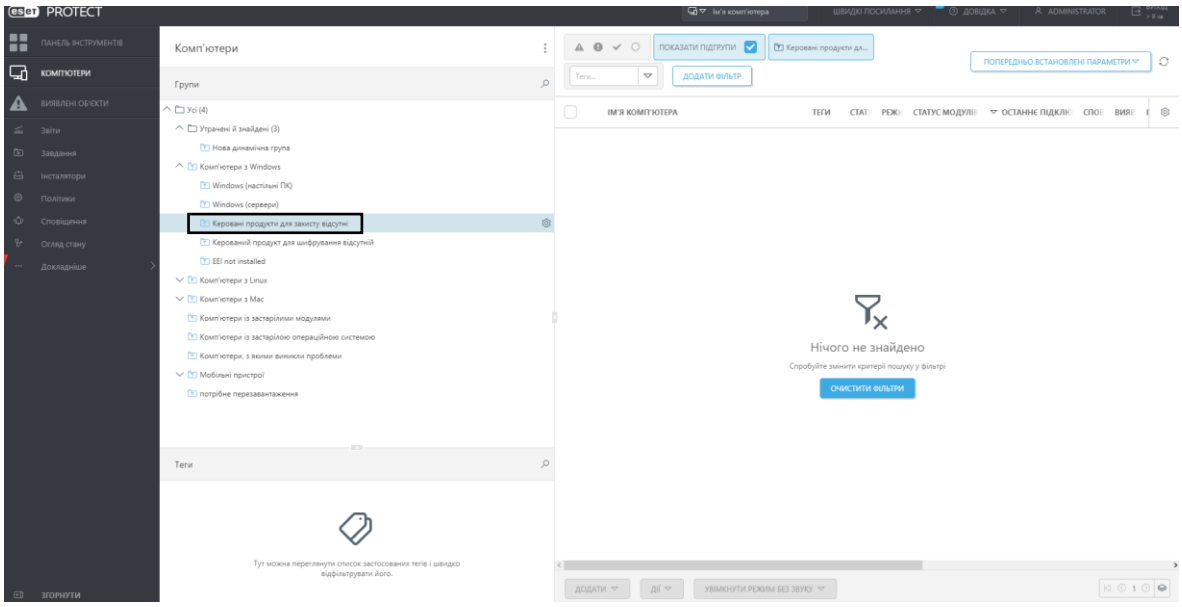

Рис.3.7 Визначення тригеру, коли виконувати дію

Налаштувавши автоматизацію на прості інциденти, можливо перейти до складних інцидентів, що включають в себе віруси та інші загрози. Автоматизацію можливо поділити на декілька етапів:

1) Загрози, що були оброблені. Перший етапов є правильне налаштування кожних модулів за допомогою політики для продукту безпеки, що дозволяє відфільтрувати велику кількість загроз.

Завдяки розділу «Політики» можливо налаштувати параметри продукту з безпеки ESET Endpoint Security. Важливим аспектом є визначення критичності виявлення та захисту. Це можливо визначити в розділі «Ядро виявлення» (рис. 3.8) , в якому можливо існують чотири параметри, які відповідають за детальність виявлення шкідливих програмних забезпечень. Якщо розглядати автоматизацію, то потрібно розглядати максимально можливий захист.

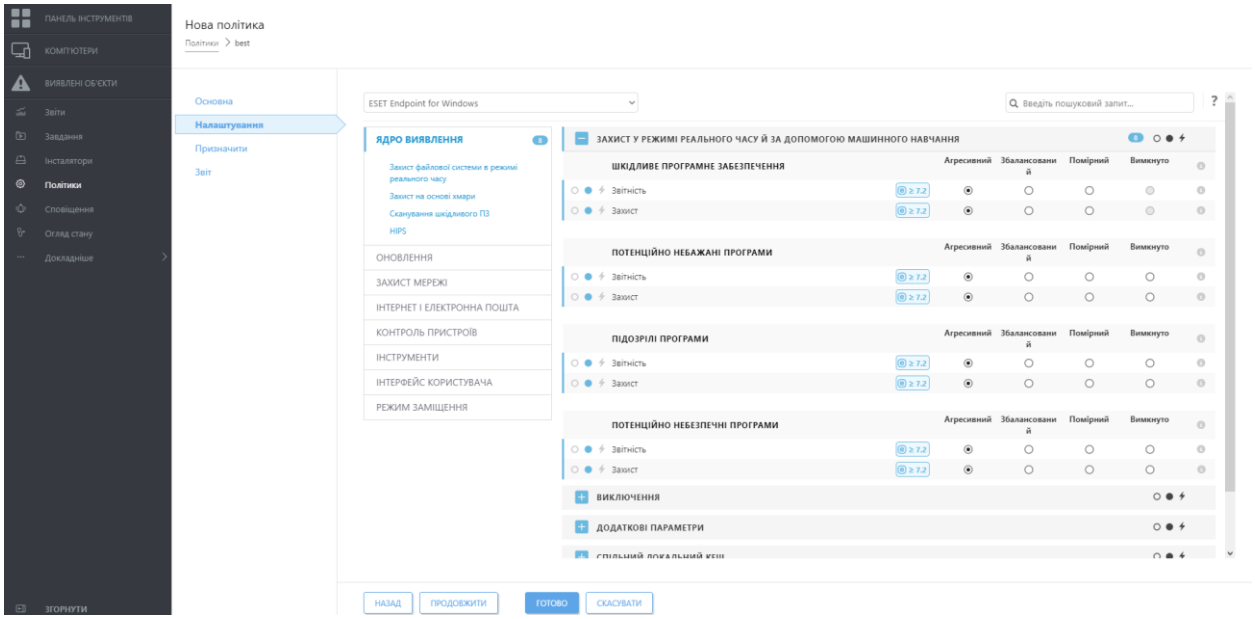

Рис.3.8 Налаштування ядра виявлення

Не меш важливим аспектом є «Захист на основі хмари» (рис. 3.9), де можливо налаштувати такі компоненти як ESET LiveGrid та ESET Dynamic Threat Defense. Найкращим методом є використання обох цих модулів для повної взаємодії продукту безпеки з системою та хмарними комплексами, що дозволяє виявити та знешкодити нові загрози.

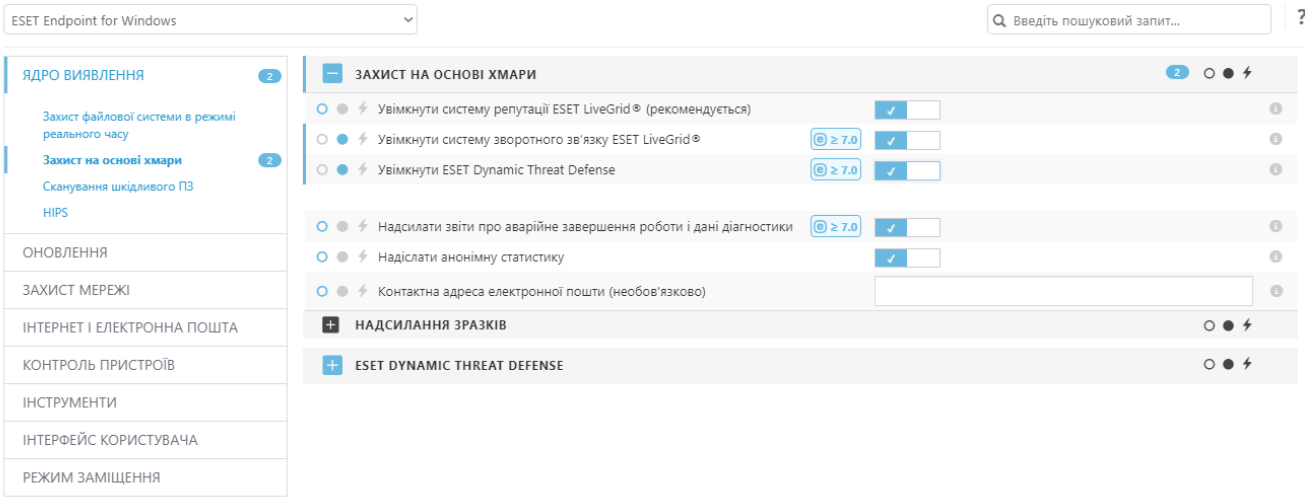

Рис.3.9 Налаштування захисту на основі хмари

Останнім, але не менш критичним є розділ «HIPS» (рис. 3.10), що включає в собі модулі для аналізу процесів в реальному часу.

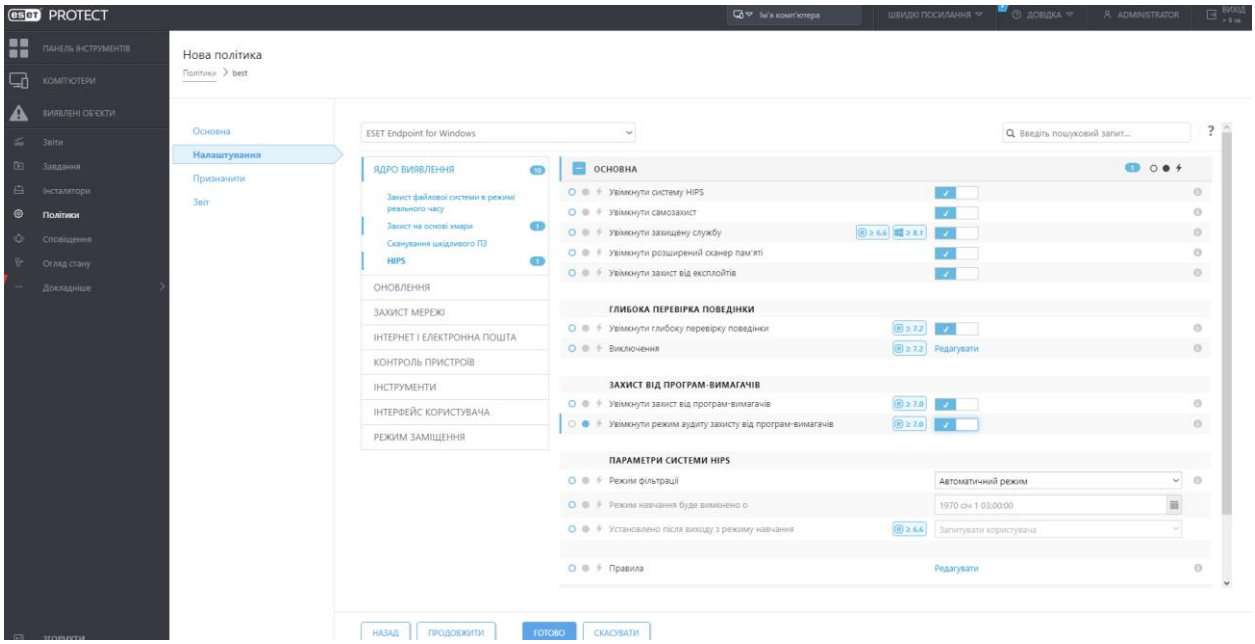

Рис.3.10 Налаштування модулю HIPS

Безсумнівно загрози, що були оброблені цікавлять, але тільки в ключі визначення «слабої точки» інфраструктури. І для цього потрібно зібрати усю необхідну інформацію. Це можливо зробити використовуючи попередній принцип, але в цьому випадку динамічна групу потрібно створити (рис. 3.11).

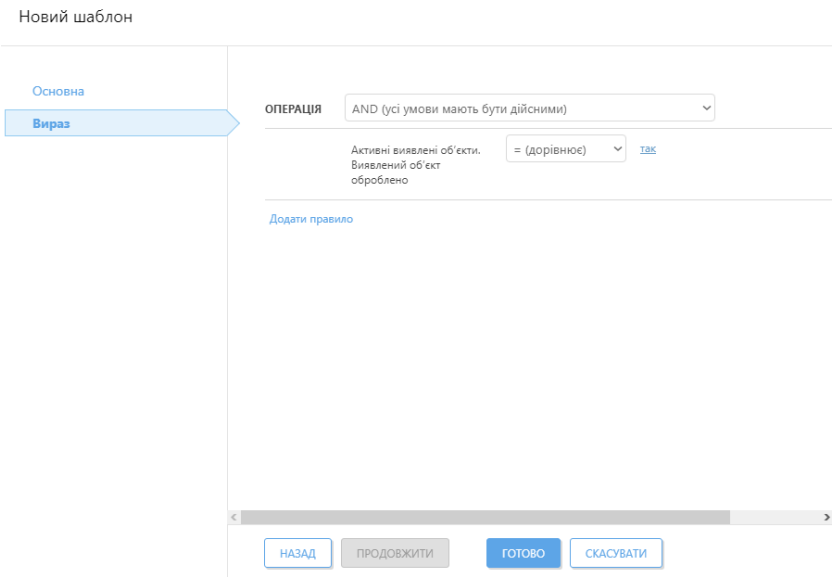

Рис.3.11 Створення шаблону динамічної групи

Для кінцевих точок, на яких загрозу буде заблоковано можливо назначити завдання збирання інформації за допомогою ESET Sysinspector. ESET SysInspector — це безкоштовний, найсучасніший інструмент діагностики для систем на базі Windows. Він перевіряє вашу операційну систему та фіксує такі деталі, як запущені процеси, вміст реєстру, елементи запуску та мережеві підключення.

Що дає змогу без втручання адміністраторів безпеки виконати частину роботи та зібрати усю необхідну інформацію для аналізу.

2) Ті, що не були оброблені (рис. 312). В цьому випадку існують ряд причин, що можуть свідчити про те, що активне виявлення не було оброблене. Основною може свідчити про наявність складної загрози, яку потрібно проаналізувати за допомогою більш складного інструменти – ESET Enterprise Inspector.

Але перед цим потрібно назначити ряд автоматичних дій, що можуть відсортувати кількість кінцевих точок, з якими потрібно робити аналіз.

Можливо назначити завдання «повне сканування операційної системи з очисткою» продуктом для безпеки.

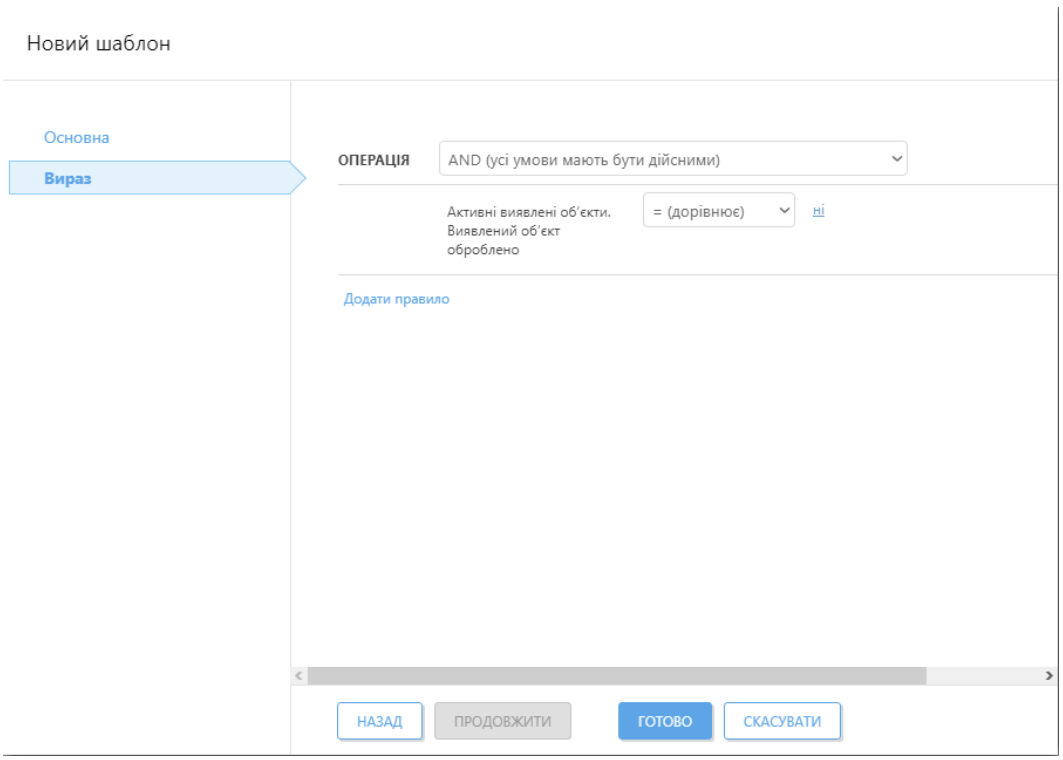

Рис.3.12 Створення шаблону динамічної групи

Більш складні загрози потребують більш складної реакції, що може включати в себе такі дії як поповнення списку IOC. ESET Threat Intelligence рішення, що дозволяє відсортувати ті індикатори компрометації, що необхідні для вашої організації. За допомогою API можливо інтегрувати автоматичне поповнення нових індикаторів до системи ESET Enterprise Inspector.

Відходячи від абсолютної автоматизації, існують покращення та сортування інформації за її важливістю. Саме EST Enterprise Inspector дозволяє фільтрувати великі об'єми інформації того, що відбувається на робочій станції, що дозволяє аналітику безпеки аналізувати тільки ту інформацію, що є ключем для виконання дій відносно того чи іншого інциденту.

Можливо налаштувати повідомлення про будь-які критичні виявлення, що дозволяє офіцеру безпеки після автоматизованих дій зосередитись тільки на важливих виявленнях (рис. 3.12)

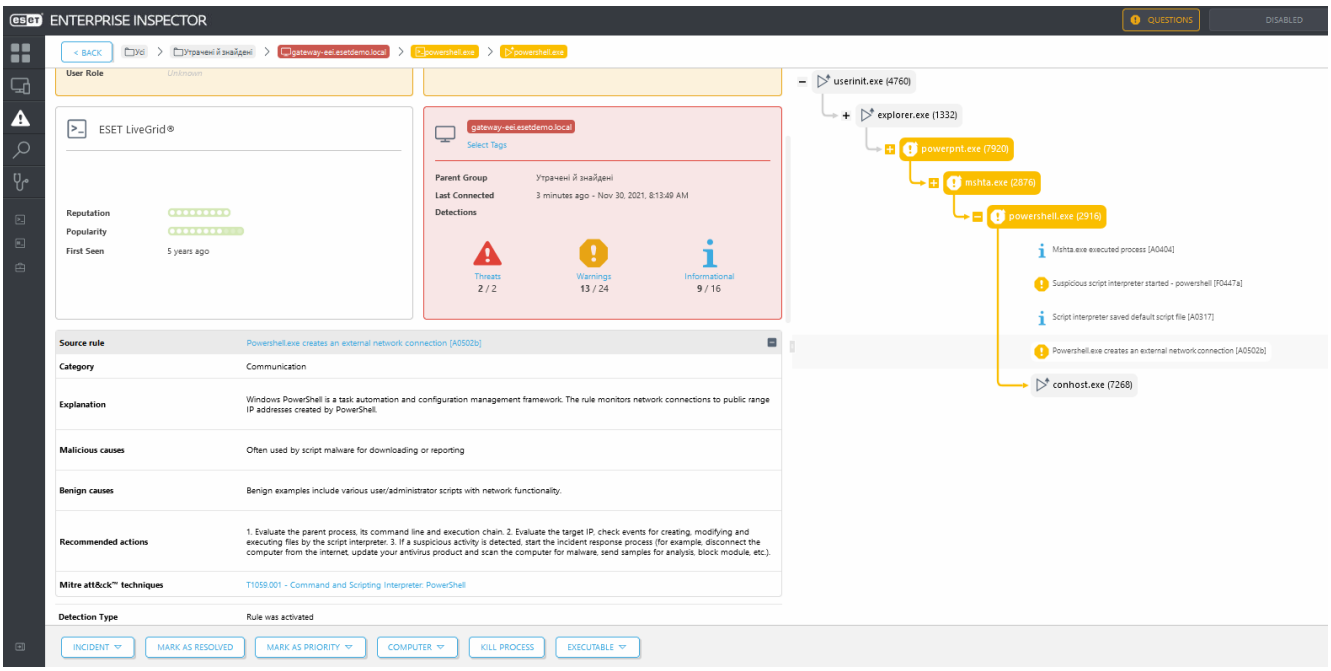

Рис.3.12 ESET PROTECT виявляє атаку HTA

Можливо емалювати два руйнівних сценарії, але реальні, які моделюють сценарії, що використовуються суб'єктами загроз. Емпірична оцінка EDR повинна ві-

дображати поширені моделі атак. Оскільки найбільш часто використовуваним вектором атаки групами APT є електронні листи, як частина соціальної інженерії або фішингу, краще використовувати шкідливі вкладені файли, які заманили б цільову жертву для їх виконання. Крім того, потрібно враховувати, що через високий рівень «шуму» від помилкових спрацьовувань, які повідомляють EDR, необхідно враховувати оцінку, до якої приписується кожна подія.

Зазвичай, атака починається з певних фішингових листів, які намагаються заманити цільового користувача відкрити файл або перейти за посиланням, яке буде використано для компрометації хоста жертви. кілька електронних листів із посиланнями на хмарних постачальників, які ведуть до певного шкідливого програмного забезпечення. Точніше, вектори атаки такі:

- HTA file. Такий тип атаки розрахований на користувача, який відвідає нешкідливу сторінку HTML, що містить IFrame, його буде переспрямовано та запропоновано запустити HTML-файл із виконуваним кодом VBS, який завантажить код .NET і виконає самоін’єкцію в контексті mshta.exe. Такий тип атаки ESET Protect блокує за допомогою ESET Endpoint Security [рис. 3.13]

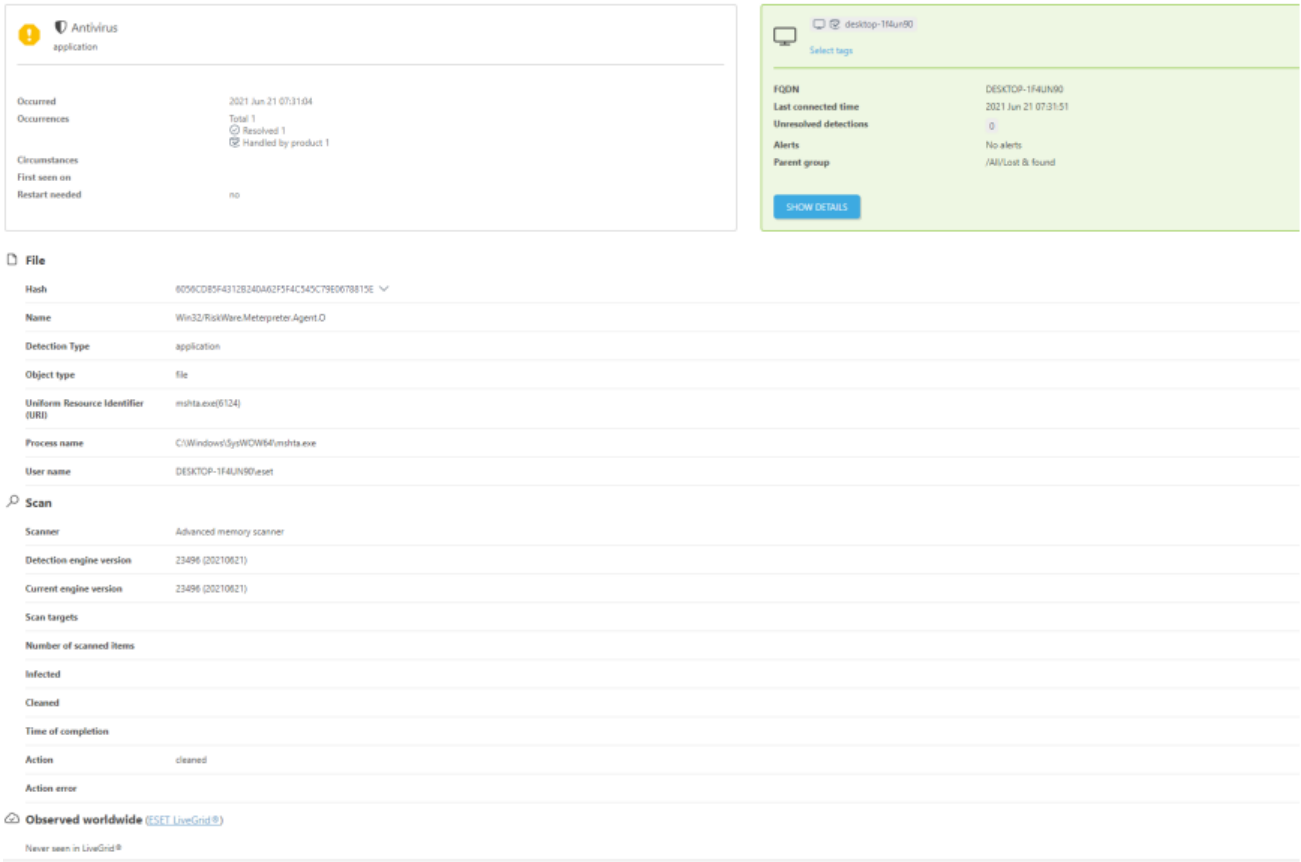

Рис.3.13 ESET PROTECT виявляє атаку HTA

- A .cpl file: файл DLL, який можна виконати подвійним клацанням у контексті файлу rundll32 LOLBINS, який може зловмисно виконувати код у своєму контексті. Файл створено за допомогою CPLResourceRunner. Для цього використаймо сховище шелл-коду техніка з використанням файлів з відображенням пам'яті (MMF) [17], а потім ініціювати. Такий тип атаки ESET Protect блокує за допомогою ESET Endpoint Security (рис. 3.14)

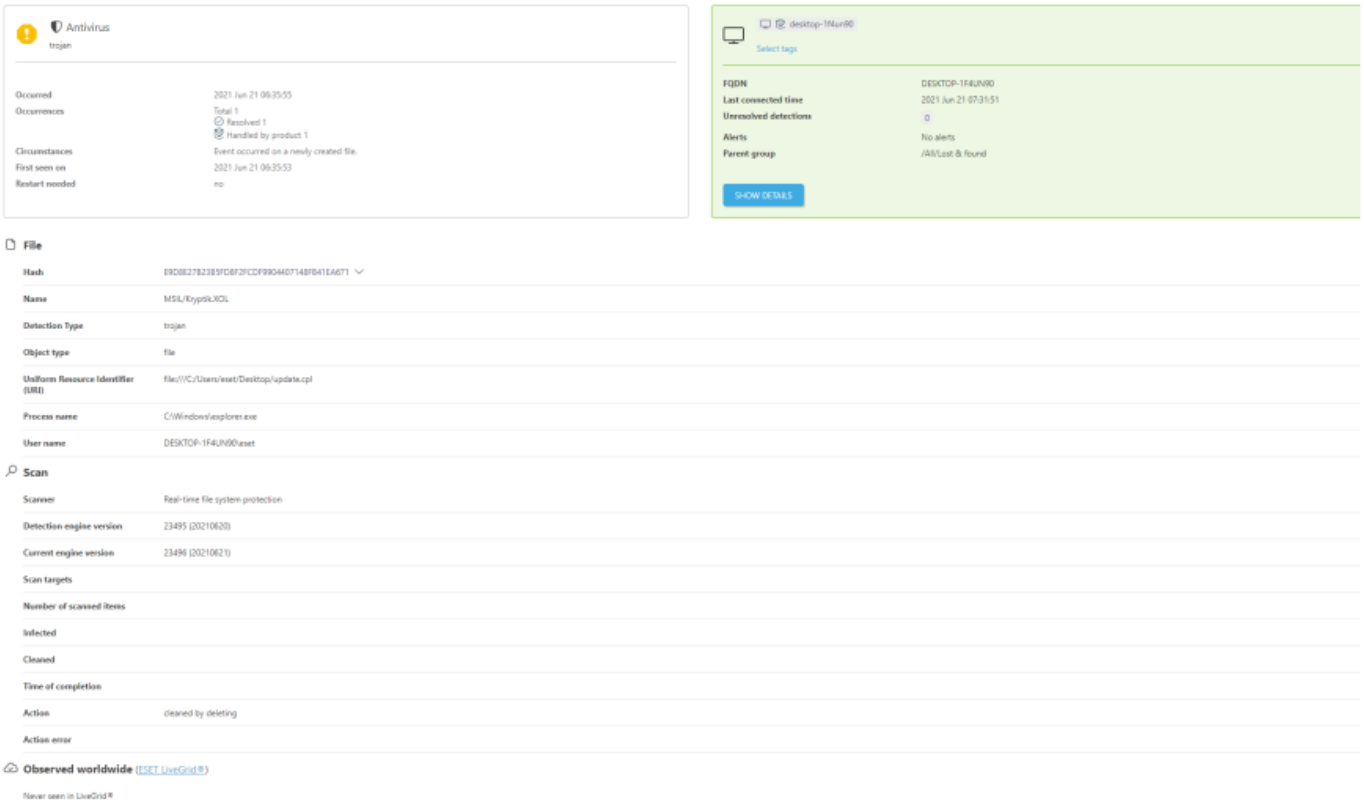

Рис.3.14 ESET PROTECT виявляє атаку CPL

ВИСНОВКИ

У магістерській роботі проведено аналіз сучасних загроз на корпоративну інформацію. Продемонстровано та обґрунтовано зростання складності атак.

Розроблено систему виявлення та протидії сучасним загрозам на прикладі ESET.

У результаті магістерській роботі вирішено такі наукові завдання:

1. Визначено, що звичайні методи забезпечення захисту зазвичай не є ефективними. Складні атаки з хитрими обхідними методами набули більшої популярності.

2. Проаналізовано та досліджено програмні комплекси від ESET, які доцільні до впровадження в державних та приватних установах.

3. Розроблено варіант автоматизації за допомогою програмних комплексів від ESET, що знизить час реакції офіцерів безпеки та допоможе зосередитись на більш важливих завданнях.

4. Доведено на прикладі емуляції атаки ефективність реагування програмних комплексів від ESET.

ПЕРЕЛІК ПОСИЛАНЬ

1. Wild Wide Web [Електронний ресурс] – Режим доступу до ресурсу: https://reports.weforum.org/global-risks-report-2020/wild-wide-web/.
2. Закон України : від 05.07.1994 р. № 81/94–ВР "Про захист інформації в інформаційно–телекомунікаційних системах" [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
3. Chen P. A study on advanced persistent threats / P. Chen, L. Desmet., 2014.
4. Giura P. A Context-Based Detection Framework for Advanced Persistent Threats. In Proceedings of the 2012 International Conference on Cyber Security / P. Giura., 2012.
5. Sood A. K. Targeted Cyberattacks: A Superset of Advanced Persistent Threats. / A. K. Sood., 2013.
6. Brogi G. Terminaptor: Highlighting advanced persistent threats through information flow tracking. In Proceedings of the 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS) / G. Brogi., 2016.
7. Alshamrani A. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. / A. Alshamrani, S. Myneni, A. Chowdhary, A., 2019.
8. Intelligence-driven computer network defenses informed by analysis of adversary campaigns and intrusion kill chains. / E. M. Hutchins, M. J. Cloppert., 2011.
9. ESET Endpoint Security [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/ees/8/uk-UA/.
10. Загальний опис ESET Protect [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/protect_admin/90/uk-UA/.
11. Панель інструментів | ESET Protect [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/protect_admin/90/uk-UA/?dashboard.html.

12. Named: Endpoint Threat Detection & Response [Електронний ресурс] – Режим доступу до ресурсу: https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/
13. ESET Enterprise Inspector [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/eei/1.6/en-US/
14. Multi-Factor Authentication - PCI Security Standards Council [Електронний ресурс] – Режим доступу до ресурсу: https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf.
15. Огляд ESET Secure Authentication [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/esa/30/uk-UA/.
16. ESET Dynamic Threat Defense [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/edtd/uk-UA/.
17. Memory-mapped files [Електронний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/dotnet/standard/io/memory-mapped-files.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)