ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК НА БАЗІ РІШЕННЯ SYMANTEC ENDPOINT PROTECTION»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Васильченко Д.І.
(прізвище та ініціали)
Керівник Марченко В.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____ 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ
СТУДЕНТУ

Васильченку Дмитру Ігоровичу
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технологія захисту кінцевих точок на базі рішення Symantec Endpoint Protection»

керівник магістерської роботи Марченко Віталій Вікторович, ст. викладач
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «12» жовтня 2022 року №122.

2. Строк подання студентом магістерської роботи 15.12.2022 р.

3. Вихідні дані до магістерської роботи
інформаційна система;
програмний комплекс забезпечення захисту кінцевих точок;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми забезпечення захисту кінцевих точок.
2. Можливості та призначення програмних комплексів для захисту кінцевих точок.
3. Методи та засоби забезпечення захисту кінцевих точок.
4. Варіант технології забезпечення захисту кінцевих точок.

5. Перелік графічного матеріалу
1. Тема магістерської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу проблеми забезпечення захисту кінцевих точок.
4. Результати аналізу методів та засобів захисту кінцевих точок.
5. Призначення, функції та можливості рішення Symantec Endpoint Protection.
6. Компоненти та архітектура рішення Symantec Endpoint Protection.
7. Технології виявлення та захисту у рішенні Symantec Endpoint Protection.
8. Варіант технології забезпечення захисту кінцевих точок.
9. Рекомендації щодо застосування технології забезпечення захисту кінцевих точок.
10. Висновки за результатами роботи.

6. Дата видачі завдання 26.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми забезпечення захисту кінцевих точок.	26.09.2022 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	14.10.2022 р.	
3.	Аналіз методів та засобів захисту кінцевих точок.	05.11.2022 р.	
4.	Розроблення варіанту технології забезпечення захисту кінцевих точок.	18.11.2022 р.	
5.	Розроблення рекомендацій щодо застосування технології забезпечення захисту кінцевих точок.	27.11.2022 р.	
6.	Оформлення результатів дослідження.	04.12.2022 р.	
7.	Підготовка доповіді до захисту.	15.12.2022 р.	

Студент Васильченко Д.І.
(підпис) прізвище та ініціали

Керівник магістерської роботи Марченко В.В.
(підпис) прізвище та ініціали

РЕФЕРАТ

Текстова частина магістерської роботи: 69 сторінок, 44 рисунків, 21 джерело.

Об'єкт дослідження — процес забезпечення кіберзахисту кінцевих точок.

Предмет дослідження — технологія захисту кінцевих точок.

Мета роботи — розробити варіант технології впровадження системи забезпечення захисту кінцевих точок та рекомендації щодо її застосування.

Методи дослідження — аналіз джерел інформації за темою роботи, вивчення документації по експлуатації, відтворення процесу забезпечення захисту кінцевих точок.

У даній роботі обґрунтовано проблему необхідності захисту кінцевих точок. Проаналізовано основні загрози для безпеки кінцевих точок, статистику поширення цих загроз. Досліджено існуючі програмні продукти щодо захисту кінцевих точок.

Визначено призначення та можливості рішення Symantec Endpoint Protection. Показано архітектуру, компоненти та вбудовані технології у рішенні Symantec Endpoint Protection.

Впроваджено варіант технології забезпечення захисту кінцевих точок. Встановлено рекомендації щодо застосування даної технології.

Галузь використання — кіберзахист кінцевих точок.

КІНЦЕВА ТОЧКА, ЗАХИСТ КІНЦЕВИХ ТОЧОК, ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, АТАКИ НА КІНЦЕВУ ТОЧКУ, УРАЗЛИВОСТІ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК, ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК

ABSTRACT

Master’s thesis: 69 pages, 44 figures, 21 sources.

Object of research – the process of ensuring cyber protection of endpoints.

Subject of research – endpoint protection technology.

The aim of research – develop a variant of the technology for implementing the system for ensuring the protection of endpoints and recommendations for its application.

Research methods – analysis of sources of information on the topic of work, study of documentation for operation, modeling of the process of ensuring the protection of endpoints.

This work substantiates the problem of the need to protect endpoints. The main threats to the security of endpoints, the statistics of the spread of these threats are analyzed. Researched existing endpoint security software products.

The purpose and capabilities of the Symantec Endpoint Protection solution are defined. The architecture, components, and embedded technologies in the Symantec Endpoint Protection solution are shown.

Implemented a variant of endpoint protection technology. Recommendations for the use of this technology have been established.

Field of use – endpoint cyber protection.

ENDPOINT, ENDPOINT PROTECTION, INFORMATION SYSTEM, CYBER SECURITY, ENDPOINT ATTACKS, ENDPOINT VULNERABILITIES, METHODS AND MEANS OF ENDPOINT PROTECTION, ENDPOINT SECURITY TECHNOLOGY

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

APT – Advanced Persistent Threat

BYOD – Bring Your Own Device

CPE – Customer Premises Equipment

GUP – Group Update Provider

IoCs – Indicators of Compromise

IoT – Internet of Things

PAC – Proxy Auto-Configuration

PET – Post-Exploitation Toolkit

POS – Point of Sale

SEP – Symantec Endpoint Protection

SIEM – Security Information and Event Management

SOC – Security Operations Center

VPN – Virtual Private Network

АЗ – Апаратне Забезпечення

БД – База Даних

ОС – Операційна Система

ПЗ – Програмне Забезпечення

ШІ – Штучний Інтелект

ВСТУП

Актуальність дослідження. Сьогодні компанії та окремі користувачі покладаються на використання широкого спектру кінцевих точок, таких як мобільні пристрої, планшети, ноутбуки, ПК та інші пристрої для виконання різних функцій. Проте всі ці IT-пристрої, системи та мережі можуть бути уразливими до кібератак.

Кінцеві точки можуть слугувати дверима для входу кіберзлочинців, які намагатимуться отримати доступ до мережі компанії чи окремого кінцевого пристрою користувача. Оскільки компанії ростуть та підключають до власної мережі ще більше пристроїв, то також пропорційно зростає ризик кібератаки на дані кінцеві точки.

Справді, статистика показує, що впродовж останніх кількох років, особливо у 2022 році, відбувається значне збільшення кількості зловмисних атак на кінцеві точки. Збільшенню тенденції поширення атак на кінцеві точки сприяє також перехід багатьох компаній на віддалений режим роботи своїх співробітників. Зловмисники намагаються атакувати кінцеві точки задля доступу та викрадення даних, що там зберігаються, використовувати їх як точки входу до мережі, або порушити роботу системи.

Забезпечення безпеки кінцевих точок передбачає використання розширених інструментів безпеки та процесів для захисту різних кінцевих точок, таких як сервери, робочі станції та мобільні пристрої, які підключаються до мережі. Сучасні інструменти захисту кінцевих точок поєднують у собі функції антивірусних та засобів захисту від шкідливих програм із можливостями сучасних технологій, таких як автоматизація, хмарні обчислення та віддалений моніторинг, щоб забезпечити повну безпеку мережі та кінцевих точок.

Ось чому компаніям та окремим користувачам слід відстежувати та аналізувати всі свої кінцеві точки на наявність аномалій чи підозрілої поведінки, щоб стримувати загрози, перш ніж вони переростуть у вдалу кібератаку та

порушать діяльність системи чи зачеплять конфіденційність, цілісність та доступність даних, що зберігаються.

Наведені аргументи актуалізують тему даної роботи, зміст якої становить дослідження технології забезпечення захисту кінцевих точок на базі рішення Symantec Endpoint Protection.

Об'єкт дослідження – процес забезпечення кіберзахисту кінцевих точок.

Предмет дослідження – технологія захисту кінцевих точок.

Мета роботи – розробити варіант технології впровадження системи забезпечення захисту кінцевих точок та рекомендації щодо її застосування.

Наукові завдання:

дослідити значення проблеми необхідності забезпечення захисту кінцевих точок;

проаналізувати можливі загрози для кінцевих точок;

дослідити технології та продукти забезпечення захисту кінцевих точок;

розробити варіант технології забезпечення захисту кінцевих точок та рекомендації щодо застосування даної технології.

Методи дослідження – аналіз джерел інформації за темою роботи, вивчення документації по експлуатації, відтворення процесу забезпечення захисту кінцевих точок.

Практичне значення одержаних результатів полягає у розробці варіанта технології забезпечення захисту кінцевих точок та рекомендацій щодо застосування даної технології.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КІНЦЕВИХ ТОЧОК

1.1. Призначення та необхідність захисту кінцевих точок

Перш ніж починати досліджувати проблему захисту кінцевих точок, слід з’ясувати, що взагалі мається на увазі під терміном «кінцева точка». Тому, кінцева точка являє собою будь-який фізичний пристрій, який можна підключити до мережі, включаючи комп’ютери, ноутбуки, мобільні телефони, планшети та сервери. Згідно рис. 1.1, список можливих кінцевих точок продовжує досить швидко розширюватись, та починає включати багато інших різноманітних пристроїв, таких як принтери, камери, побутова техніка, смарт-годинники, фітнес трекери, навігаційні системи та будь-які інші пристрої, які можна підключити до Інтернету.

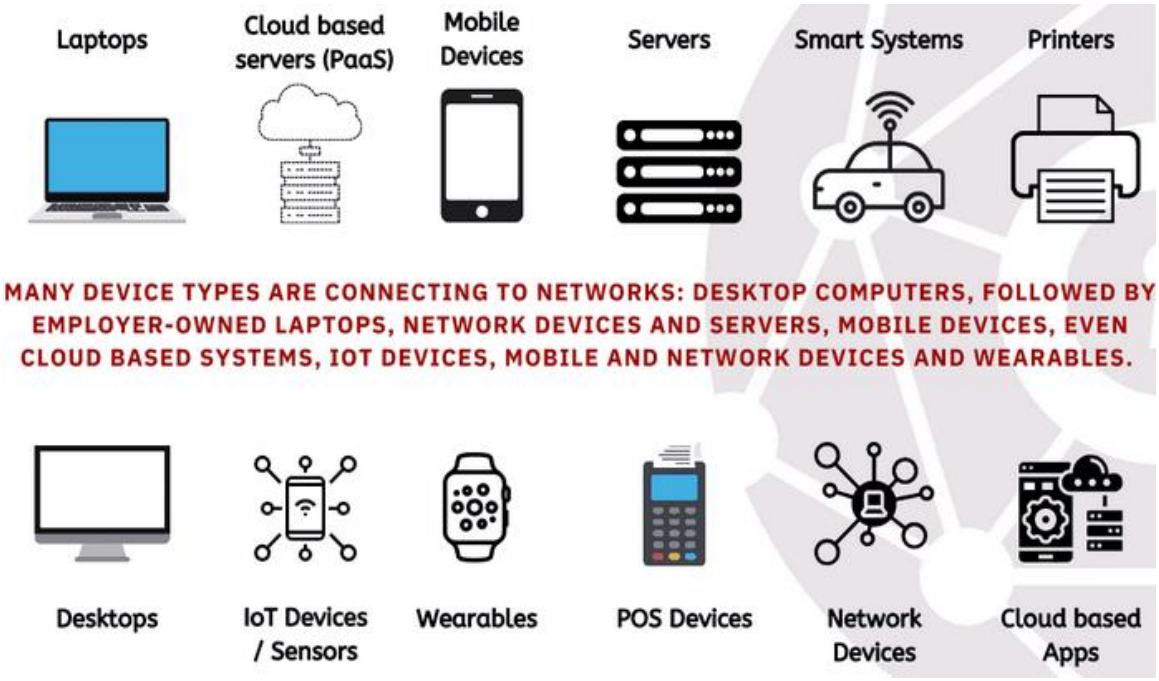

Рис. 1.1. Різноманітність кінцевих точок [2]

Для прикладу, коли Боб та Аліса розмовляють по телефону, то їх зв’язок поширюється від однієї людини до іншої, а кінцевими точками з’єднання є їхні

відповідні телефони. Так само в мережі пристрої «розмовляють» один з одним, тобто вони передають інформацію з однієї точки в іншу. Проте, коли Боб та Аліса спілкуються по телефону, вишка стільникового зв'язку, яка передає їхню розмову, не є кінцевою точкою для обміну даними — це середовище, за допомогою якого відбувається обмін. Пристрої інфраструктури, на яких працює мережа, вважаються CPE, а не кінцевими точками. CPE включає:

- маршрутизатори;
- перемикачі;
- мережеві шлюзи;
- брандмауери;
- балансувальники навантаження.

Як ще один приклад, візьмемо типовий магазин техніки, який має кілька касових апаратів, які підключаються до мережі магазину та запускають POS, маршрутизатор, який з'єднує мережу магазину з Інтернетом, внутрішній сервер, який зберігає записи про щоденні транзакції та кілька співробітників, які підключають свої особисті смартфони до Wi-Fi магазину. Маршрутизатор вважатиметься CPE. Решта цих пристроїв є кінцевими точками в мережі магазину, навіть персональні смартфони, якими безпосередньо не керує магазин [1].

Примітивну схему функціонування кінцевих точок «A» та «B» та проміжних засобів у мережі розглянуто на рис. 1.2.

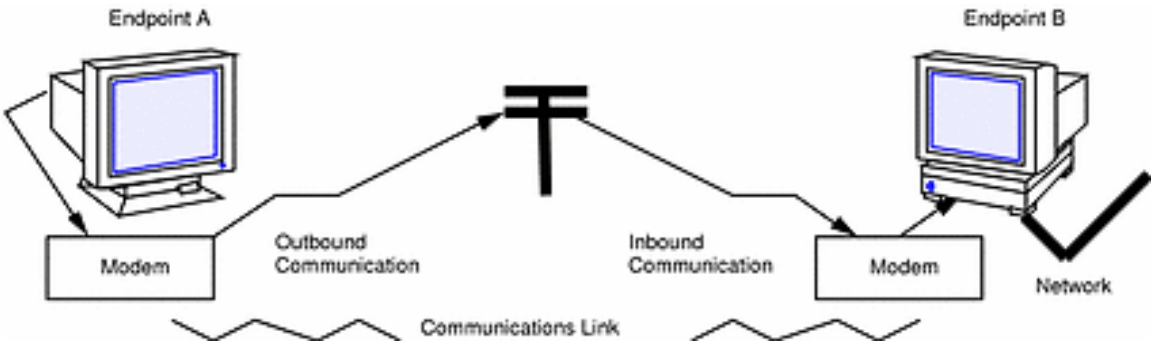

Рис. 1.2. Схема-приклад зв'язку між кінцевими точками [5]

Користувачі в контексті кінцевої точки можуть бути анонімними особами (наприклад, у торговому терміналі) або можуть бути промисловими власниками

датчиків або систем керування, призначених для їхніх цілей. Користувачі й надалі залишаться людьми, які використовують такі інструменти, як веб-браузери на настільних комп'ютерах, ноутбуках та на постійно зростаючому діапазоні мобільних пристроїв.

З ростом застосування BYOD та IoT кількість відокремлених приладів, що підключені до мережі, вже досягає десятків тисяч. Оскільки вони є точками входу для загроз та зловмисного ПЗ, кінцеві точки (особливо віддалені точки) є улюбленою мішенню зловмисників. Зараз мобільні кінцеві точки являються набагато більшими, аніж звичайні пристрої Android та iPhone. Згадаймо найновіші розумні пристрої, годинники, помічники з керуванням голосом та інші розумні кінцеві точки за підтримки IoT. З ростом різноманітності типів кінцевих точок рішення щодо їх безпеки мають бути адаптованими до стійкості перед найновішими загрозами.

Зловмисники регулярно намагаються захопити або зламати кінцеві пристрої. Для цього вони можуть мати на меті будь-яку кількість цілей [1]:

- ✓ зараження пристрою зловмисним ПЗ;
- ✓ відстеження дій користувачів на пристрої;
- ✓ утримання пристрою з метою отримання викупу;
- ✓ використання пристрою як частини ботнету;
- ✓ використання пристрою як відправної точки для компрометації інших пристроїв у мережі.

У бізнес-контексті зловмисники часто націлюються на кінцеві точки, оскільки скомпрометована кінцева точка може бути точкою входу в безпечну корпоративну мережу. Зловмисник може не мати змоги пройти через корпоративний брандмауер, але ноутбук співробітника може стати дещо легшою ціллю [1].

Кінцеві точки важко захистити в бізнес-налаштуваннях, оскільки IT-команди мають менше доступу до них, ніж до внутрішньої мережевої інфраструктури. Кінцеві пристрої також значно відрізняються за виробником, моделлю, ОС, встановленими програмами та станом безпеки (готовність до атаки). Заходи

безпеки, які успішно захищають смартфони від атак, можуть не працювати, наприклад, для серверів. І хоча один працівник компанії може регулярно оновлювати свій ноутбук та уникати ризикованої поведінки в Інтернеті, інший може уникати оновлення ПЗ та завантажувати небезпечні файли на свій ноутбук. Проте компанія має знайти спосіб захистити обидва ноутбуки від атак та запобігти скомпрометації мережі [1].

Через складність забезпечення безпеки кінцевих точок та важливість їх захисту безпека кінцевих точок є окремою категорією кібербезпеки (разом з безпекою мережі, безпекою хмари, безпекою веб-додатків, безпекою IoT та контролем доступу тощо).

Більшість ІТ-команд покладаються на спеціалізоване ПЗ для керування та захисту кінцевої точки, яка є основним робочим інструментом для сучасної робочої сили будь-де. Керування кінцевими точками залишається основоположним компонентом стратегії корпоративної інфраструктури будь-якої ІТ команди [12].

Встановлюючи контроль видимості та безпеки на кінцевих точках, фахівці з ІТ безпеки повинні розуміти, що кожна кінцева точка несе часткову або повну відповідальність за власну безпеку. Це відрізняється від традиційного підходу до безпеки мережі, у якому встановлені заходи безпеки застосовуються до всієї мережі, а не до окремих пристроїв та серверів. З цього випливає, що забезпечення стійкості кожної кінцевої точки має першочергове значення для реалізації успішної стратегії захисту.

Тому організації повинні як мінімум розгорнути прості форми керування кінцевими точками та безпеки, як-от уніфіковане керування кінцевими точками, а також антивірусне ПЗ на всіх пристроях. Багато організацій сьогодні виходять за рамки цих простих заходів та використовують технологію безпеки кінцевих точок, яка охоплює шифрування, виявлення вторгнень та елементи блокування поведінки, щоб ідентифікувати та блокувати загрози, а також ризиковану поведінку як кінцевих користувачів, так й зловмисників. Однак, оскільки величезна кількість пристроїв на підприємстві, а також середня кількість додатків, встановлених у цих системах, різко зросла, складність, з якою доводиться мати справу ІТ-командам і

командам безпеки, також зросла. У свою чергу, адміни часто сприймають керування кінцевими точками як процес, який забирає надто багато часу та не дозволяє їм зосередитися на інших стратегічних пріоритетах [12].

У той же час користувачі очікують постійної та високоякісної роботи незалежно від того, де вони знаходяться. Зрештою, користувачі хочуть, щоб технологія, якою вони користуються, належно працювала, тому їм байдуже, що відбувається на сервері, якщо вони можуть надійно та постійно отримувати доступ до необхідних ресурсів. Це означає, що IT-спеціалістам потрібен вищий рівень видимості, коли користувачі працюють з будь-якого місця, щоб забезпечити стабільну роботу незалежно від місця розташування.

Багато молодих спеціалістів з кібербезпеки стикаються з концепцією безпеки мережі та безпеки кінцевих точок, а також з приводу того, чому обидва необхідні кожному підприємству. Безпека мережі — це процес захисту корпоративної мережі на мережевому рівні за допомогою рішень, які називаються брандмауерами [2].

Сучасні брандмауери не тільки захищають від тривіальних атак 4 рівня, але й надають розширені функції, такі як: глибока перевірка пакетів та фільтрація веб-проксі, які допомагають виявити атаку на прикладному рівні. Брандмауери також контролюють, якому трафіку «дозволено» входити та виходити з мережі. Це також допомагає обмежити трафік між різними зонами одного підприємства [2].

Безпека кінцевої точки також є процесом захисту корпоративної мережі через захист кінцевих пристроїв у мережі від зараження шкідливим ПЗ. Оскільки Endpoint-протектори встановлені в системі, вони мають більше видимості та контролю над запобіганням та стримуванням компроментацій у разі порушення безпеки [2].

Підхід до безпеки мережі, заснований на політиці, має першорядне значення для захисту мережі. Політика повинна вимагати, щоб кінцеві пристрої відповідали певним критеріям, перш ніж отримати доступ до мережевих ресурсів. Архітектура безпеки розроблена для обробки кінцевих пристроїв, щоб захистити активи даних, доступ до яких здійснюється через ці системи.

Компанії, які дозволяють співробітникам мати з собою власні пристрої, як-от ноутбуки чи смартфони, часто стикаються з проблемами безпеки кінцевих пристроїв. Без продуманої політики використання власного пристрою (BYOD) пристрої, що належать працівникам, можуть поставити під загрозу безпеку інформації компанії або мережі.

Організації вважають, що близько 45% корпоративних даних зберігається на кінцевих пристроях. Ці ноутбуки, планшети та смартфони становлять величезний ризик для безпеки даних.

Зростання вразливості кінцевих пристроїв у всій галузі означає, що дані піддаватися ризику легше, ніж будь-коли. Щоразу, коли працівник підключається через загальнодоступний Wi-Fi, завантажує підозрілу програму або стає мішенню фішингового шахрайства, ризик зростає.

Це особливо важливо, оскільки пристрої кінцевої точки не лише піддають свої дані можливому вилученню, вони також служать потенційним каналом для порушення безпеки всієї мережі.

Політики безпеки, особливо в тому, що стосується захисту BYOD, є важливою частиною захисту кінцевих пристроїв від нападу. Але найбільшою причиною вразливості є якість навчання та поінформованості працівників. Необережні дії можуть серйозно вплинути на цілісність безпечної мережі [13]:

- Втрачені або неправильно виведені з експлуатації пристрої: працівники, які втрачають пристрої, підключені до мережі компанії, можуть піддати цю мережу атакам.
- Погане застосування оновлень безпеки: застарілі ОС та програми можуть призвести до будь-якої кількості уразливостей у пристрої, якому надано доступ до конфіденційної інформації компанії.
- Співробітники вимикають/вмикають шифрування: люди, швидше за все, налаштують засоби безпеки на своїх пристроях та перероблять налаштування відповідно до своїх потреб. Це може призвести до небажаних точок доступу.

Завдяки проактивній, постійно ввімкненій технології ІТ-спеціалісти можуть уникнути таких проблем, зберігаючи при цьому відповідність вимогам безпеки й знижуючи ризики [13].

1.2. Аналіз основних атак на кінцеві точки

Кінцеві точки становлять собою унікальну загрозу для організацій, оскільки вони:

- найпоширеніший тип активів на підприємстві;
- найбільш затребувана мішень для супротивників на різних етапах атаки;
- можливо, ціль кількох типів загроз, яким, як очікується, можуть запобігти інші засоби безпеки [14].

Загрози, з якими стикаються організації чи кінцеві користувачі, застосовують на уразливості. Уразливості можуть стосуватися ОС, апаратного забезпечення у фізичній системі або стороннього ПЗ. Як показав останній час, іноді уразливості містяться в бібліотеках, вбудованих у стороннє ПЗ, що наражає кінцеву точку на загрозу. Функція кінцевої точки також може змінити її профіль ризику. Зловмисники можуть шукати дірки у зовнішньому ПЗ, допоміжній бібліотеці або відкритому порту. Як видно з останніх розкриттів уразливостей, зловмисники абсолютно не витрачають час на масове сканування Інтернету, коли з’являється нова уразливість.

Серед найпоширеніших загроз безпеки для кінцевих точок виділяють наступні зловмисні атаки та небезпечні дії, які наведені нище.

Фішингові атаки

Атаки по типу фішингу виникають, коли хакери надсилають шахрайські електронні листи чи повідомлення на кінцеві пристрої користувачів, намагаючись змусити нічого не підозрюючих юзерів переходити за гіперпосиланнями на скомпрометовані веб-сайти, викрадати їхні конфіденційні дані, завантажувати зловмисне ПЗ або надавати дозволи на пристрій неавторизованим користувачам.

Шкідливі документи, електронні таблиці, PDF-файли та реклама призначені для відкриття або перегляду користувачем на кінцевій точці.

Вони маскуються під законні організації, маніпулюють жертвами, змушуючи їх виконувати певні дії, наприклад натискати шкідливі вкладення чи посилання. Іншим способом здійснення фішингових атак є спуфінг веб-сайтів, коли зловмисники маскуються під надійні веб-сайти та запитують облікові дані для входу.

Наприклад, розглянемо фішинговий електронний лист, відкритий на кінцевому пристрої користувача. Хоча очікується, що засоби безпеки електронної пошти унеможливлюватимуть доставку цих фішингових електронних листів, проте тепер це загроза, яку кінцева точка повинна виявити та вчасно заблокувати. На жаль, деякі зловмисники покладаються на цю складність, створюючи фішингові листи, які уникають захисту електронної пошти та кінцевої точки. Це не є виправданням для неналежної безпеки електронної пошти; швидше це розширює профіль загрози для кінцевих точок в організації. Це дає підстави для сильної можливості EDR. Без цього служби безпеки не зможуть протистояти ворогам. Дані загрози часто проходять через окрему лінію контролю безпеки, перш ніж досягти кінцевої точки [14].

Інструменти EDR повинні мати можливість отримувати й аналізувати телеметрію, пов’язану з мережевим трафіком, електронною поштою, виконанням процесів, дозволами на файли, системними змінами, поведінкою користувачів та багатьом іншим.

Файлове та безфайлове шкідливе ПЗ

Кіберзлочинці постійно розробляють передові методи, щоб уникнути виявлення службами захисту кінцевих точок. Безфайлове зловмисне ПЗ є одним із таких шкідливих методів. Він використовує рідні законні програми для встановлення та виконання кібератак на цільові системи. На відміну від традиційних зловмисних програм, зловмисникам не потрібно встановлювати шкідливі коди на кінцеві пристрої жертв. Безфайлове зловмисне ПЗ базується у пам’яті та не покладається на файли. Це призводить до атаки з нульовим слідом,

яку важко виявити та видалити традиційними методами на основі сигнатур. Ця загроза цифрового проникнення може отримати доступ до ПЗ кінцевого пристрою, програм та протоколів системи через різні точки входу, включно з фішинговими листами, шкідливими завантаженнями. Безфайлове зловмисне ПЗ може бути важко ідентифікувати, але його не можна повністю виявити. Можна розгорнути багаторівневий підхід або підхід до глибокого захисту, щоб усунути весь життєвий цикл загрози та захистити свої пристрої.

Зайві права користувача

Іншою високопріоритетною загрозою для кінцевої точки, якою зловмисники завжди прагнуть скористатися, є невід'ємні дозволи, які надаються обліковим записам користувачів. Такі дозволи включають вхід на кінцевий пристрій або перевірку електронної пошти. Наприклад, усі дії, які відбуваються в системі Windows, прив’язані до облікового запису. Будь то запуск веб-браузера, відкриття PDF-файлу чи проведення відеоконференції, дозволи користувача визначають, що користувачі можуть, а що не можуть робити. Крім того, під час звичайних операцій домену облікові записи входять та виходять із систем без будь-якої взаємодії з користувачем. На жаль, користувачі часто отримують занадто багато дозволів. Під час надання облікових записів — локальних, користувачів домену чи служби — часто існує певний набір дозволів, які потрібно надати обліковим записам. Однак, оскільки політикою доступу користувачів може бути важко керувати та підтримувати, організації надають користувачам набагато більше дозволів, ніж потрібно [14].

Набори інструментів після експлуатації (PET)

Однією з загроз, яка часто впливає на кінцеві точки, є використання широко відомих та добре зарекомендованих PET. Звичайно, перше, що спадає на думку, це незмінні Cobalt Strike та Metasploit. Хоча продаються як інструменти симуляції супротивника або агресивні засоби безпеки, комплекти після експлуатації є одними з найпоширеніших інструментів супротивника. У статті Threatpost за червень 2021 року повідомлялося, що використання Cobalt Strike зросло на 161% порівняно з аналогічним періодом минулого року в кібератаках, причому цей інструмент

використовувався як APT, так й суб'єктами загальних товарів або програм-вимагачів.

PET також становлять значну загрозу для кінцевих точок організації, оскільки вони постачаються в комплекті з десятками (якщо не сотнями) можливостей експлуатації. Зловмисники можуть отримати початковий доступ до системи та проходити через десятки атак, експлойтів, ескалації привілеїв та спроб бокового переміщення, поки не знайдуть щось, що працює. Ці набори інструментів також містять елемент автоматизації, який, використовують багато загрозливих суб'єктів на свою користь. Cobalt Strike, наприклад, має можливість для зловмисників завантажувати сценарії агресора, які є автоматизованою серією дій, які виконуються на кінцевому пристрої жертви. Це може дати супротивникам значну перевагу, якщо вони зможуть зібрати сценарій, який переносить їх від 0 до 100 за мінімальний час [14].

Атаки нульового дня

Атаки нульового дня використовують уразливості в системах, які розробники ще не усунули або про які розробники навіть не підозрюють. Назва походить від того факту, що користувачі щойно дізналися про недолік або не знають про нього, тобто у них є «нуль днів», щоб його виправити. Не дивно, що атаки нульового дня мають надзвичайно високий рівень успішності, оскільки немає реальної можливості виправити невідомий недолік і немає конкретних заходів для його компенсації. Часто розробники змушені намагатися зупинити атаки, коли вони вже почалися, або намагатися відновити збитки, завдані після них [14].

Криптоджекінг

Криптоджекінг — це нова кіберзагроза, яка передбачає несанкціоноване використання ресурсів обробки пристроїв для таємного видобутку криптовалюти. Він може скомпрометувати всі види пристроїв, включаючи настільні ПК, ноутбуки, смартфони, мережеві сервери. Це часто відбувається через фішингові електронні листи, які обманом змушують користувачів натискати шкідливі посилання або завантажувати файли, які можуть завантажувати коди для майнінгу криптовалюти на цільовий кінцевий пристрій. У деяких випадках веб-сайти або онлайн-реклама

заражаються кодом JavaScript, який автоматично виконується після завантаження у браузері жертви.

Про ці атаки не так багато заголовків, як про інші, оскільки більшість ПЗ для криптозлому розроблено таким чином, щоб залишатися прихованим від пристроїв жертви. Крім того, на відміну від інших форм зловмисного ПЗ, дане ПЗ для криптомайнінгу не є таким руйнівним та не пошкоджує дані користувачів. Однак це сповільнює ресурси та продуктивність кінцевого пристрою, збільшує витрати на електроенергію та скорочує термін служби пристроїв.

З вищеперерахованого робиться висновок, що кожна кінцева точка, яка під'єднана до мережі, є потенційним входом зловмисника для порушення її безпеки та витоку даних. Дуже важливо мати відповідне рішення безпеки кінцевої точки, щоб зменшити ці ризики та контролювати свої кінцеві пристрої.

1.3. Аналіз статистики загроз кінцевим точкам

Безумовно, у сьогоднішні часи відбувається стрімке збільшення активності кіберзлочинців, особливо на фоні подій 2022 року. Провідні організації продовжують проводити різноманітні дослідження та публікують звіти, насамперед, щодо статистики атак на кінцеві точки.

Згідно статистики щодо зміни рівня ризику небезпеки для кінцевих точок за 2022 рік (рис. 1.3), стверджується, що більшість організацій, а саме 66%, відчули збільшення кіберзагроз для своїх кінцевих точок. Двадцять відсотків фахівців з кібербезпеки повідомляють, що їхня організація зазнала «успішної» атаки на кінцеву точку протягом останніх 12 місяців, яка скомпрометувала дані та/або IT-інфраструктуру. Кількість невиявлених атак, ймовірно, може бути значно вища. [6]

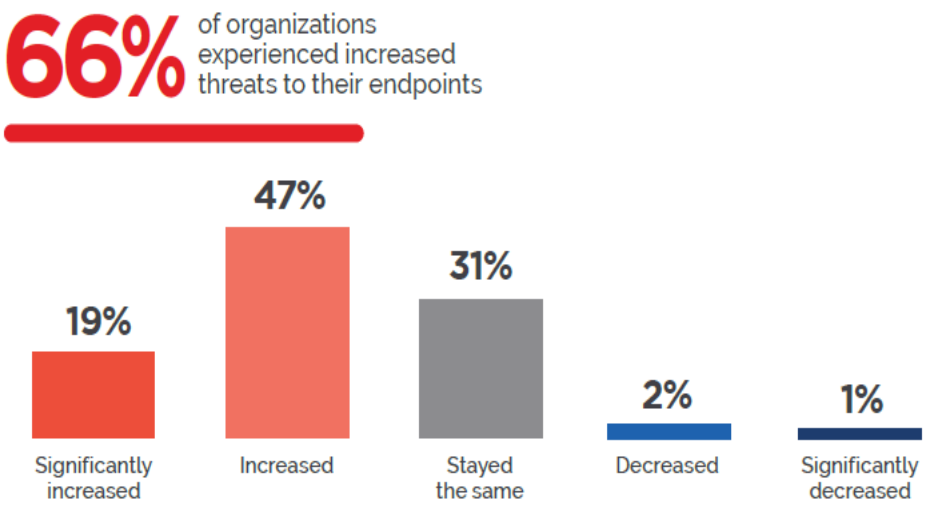

Рис. 1.3. Зміна рівня небезпеки для кінцевих точок за 2022 рік [6]

Згідно з думкою фахівців з кібербезпеки, для їхніх організацій у 2022 році, зловмисне ПЗ (включаючи програми-вимагачі, набори експлойтів, трояни) вважається найбільшою загрозою безпеці (38%), за нею йдуть помилки людини (23%) та експлойти нульового дня (18%). Це підкреслює зростаючу загрозу від зловмисного ПЗ, зокрема програм-вимагачів [6].

Відповідно до дослідження, яке було проведено Ponemon Institute, було виявлено, що близько 70% організацій пережили одну або кілька кібератак на кінцеві точки, які, нажаль, успішно скомпроментували дані та/або їхню IT-інфраструктуру. У тому ж звіті було встановлено, що близько 70% IT-спеціалістів виявили, що частота атак на кінцеві точки продовжує зростати порівняно з минулими роками [9].

Подальше дослідження Ponemon показало, що атаки на кінцеві точки є одними з найпоширеніших, з якими стикалися фахівці: 81% компаній стикалися з атаками з використанням певної форми зловмисного ПЗ, а 28% – з атаками зі зламаними або викраденими пристроями.

Результати дослідження від Check Point щодо кількості щотижневих атак на організацію за галузями (рис. 1.4), які опубліковані в серпні 2022 року, зазначають, що сектор освіти зазнавав більше атак на тиждень порівняно з іншими галузями.

У третьому кварталі цього року освітній/дослідницький сектор щотижня стикався з 2148 атаками на організацію, що на 18% більше, ніж у третьому кварталі минулого року.

Наукові заклади стали популярним джерелом для кіберзлочинців після швидкої оцифровки, яку розпочали у відповідь на пандемію COVID-19. Багато з них були погано підготовлені до несподіваного переходу до онлайн-навчання, що створило широкі можливості для хакерів проникнути в мережі будь-якими засобами. Школи та університети також стикаються з унікальною проблемою роботи з дітьми чи молодими людьми, багато з яких використовують власні пристрої, працюють у спільних місцях та часто мають підключення до загальнодоступного Wi-Fi, не думаючи про ризики для безпеки [8].

Другою найбільш атакованою галуззю була державна/військова сфера з 1564 середньо-тижневими атаками, що на 20% більше, ніж за той самий період минулого року. У секторі охорони здоров'я відбулися найбільші зміни порівняно з минулим роком, у середньому 1426 атак на тиждень – значне зростання на 60% порівняно з минулим роком [8].

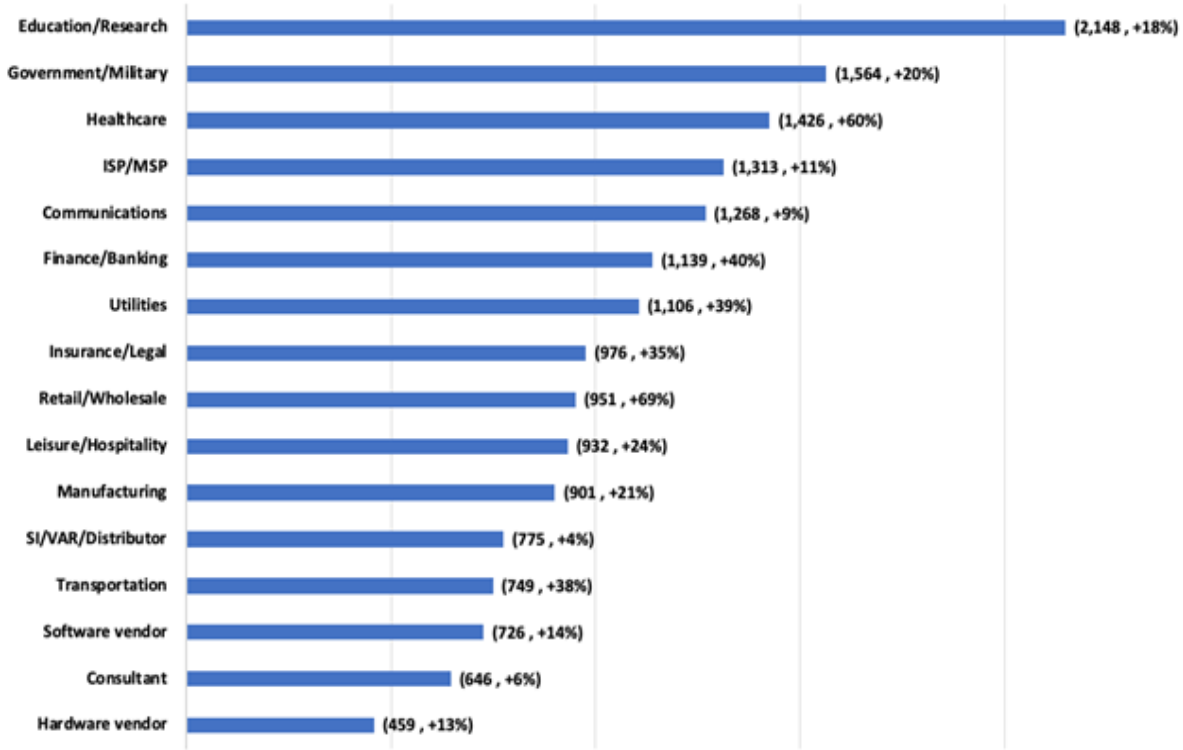

Рис. 1.4. Середньо-тижнева кількість атак на організацію за галузями [8]

Кожен третій співробітник США (33%) використовує персональний комп'ютер та смартфон для віддаленої роботи, тоді як лише 17% використовують корпоративний комп'ютер й смартфон. Згідно зі результатами опитування Ponemon Institute, 55% професіоналів вважають смартфони однією з найбільш вразливих кінцевих точок. 50% вважають ноутбуки особливо вразливими, 24% вважають планшети та 48% вважають вразливими інші мобільні пристрої. Лише 34% вважають настільні комп'ютери одними з найбільш вразливих кінцевих точок [9].

Нещодавній звіт від Webroot показав, що понад 40% пристроїв Android використовують версію ОС, старішу за v9. Це робить їх більш сприйнятливими до атак, тому повинно викликати занепокоєння у власників цих пристроїв.

Дослідження Webroot показують, що 83% шкідливих програм зберігаються в одному з чотирьох місць: %temp%, %appdata%, %cache% та %desktop%. Зловмисне ПЗ також можна встановити за допомогою «juice jacking», тобто методу, який передбачає зміну USB-портів для встановлення шкідливого ПЗ на пристрій жертви. Ці порти часто маскуються під безкоштовні зарядні пристрої в громадських місцях. Цей спосіб встановлення підходить для організацій із великою кількістю віддалених працівників, або працівників, які регулярно переміщуються у зв'язку зі своєю роботою. 79% людей, які переміщуються по справах, підключаючи свої пристрої до загальнодоступного порту USB або зарядної станції, несвідомо відкривають двері для потенційного зловмисника [9].

Згідно з даними компанії SANS за підтримки компанії BlackBerry було встановлено статистику щодо різноманітних векторів атак на кінцеві точки (рис. 1.5), з якими більш всього спідкалися організації. Так, згідно з статистики, виявляється, що найчастіше всього спроби порушення безпеки кінцевої точки були у вигляді завантаження небезпечних файлів з Інтернету (60%), використання фішингу (54%), компрометація облікових даних (49%), використання відомих уразливостей (31%) та інших методів [7].

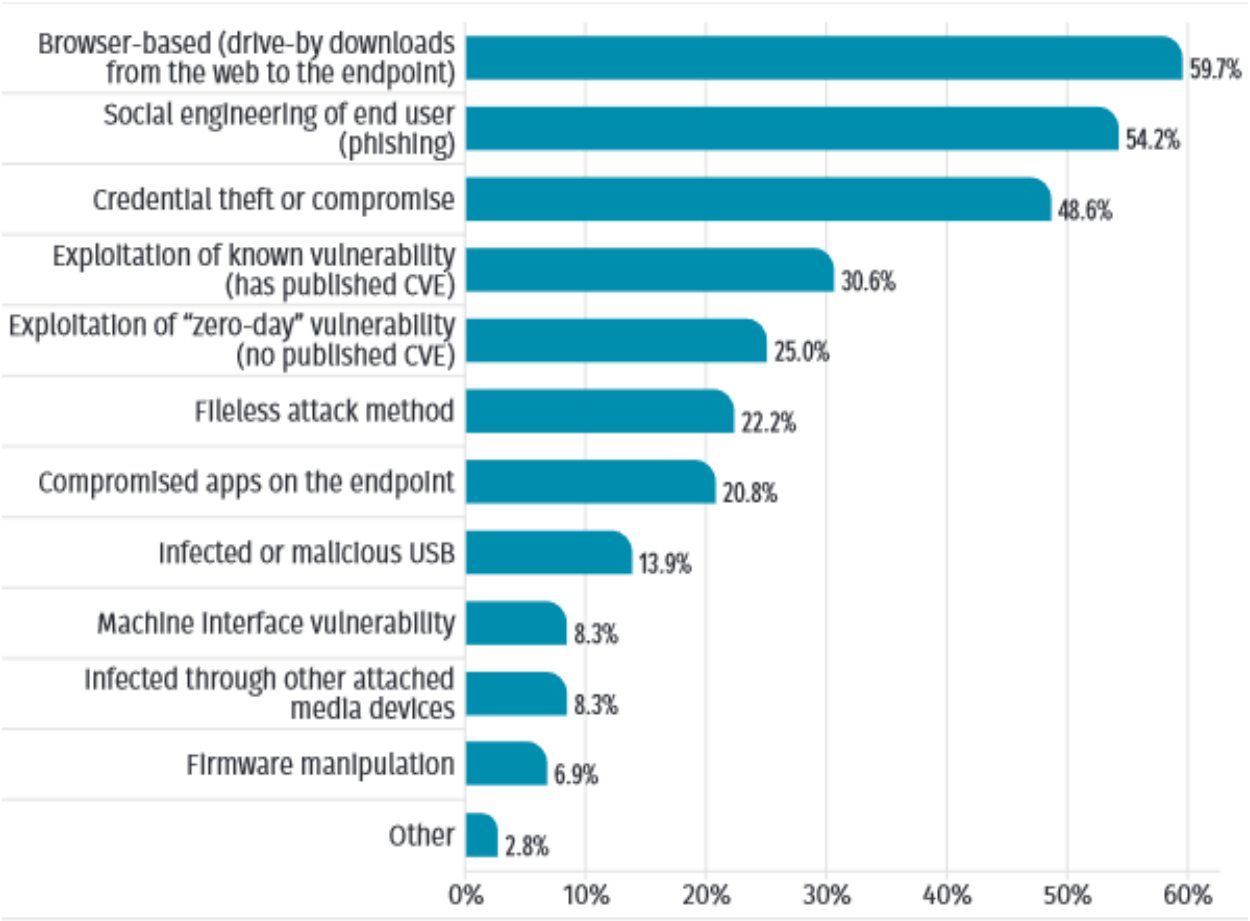

Рис. 1.5. Статистика поширеності різних векторів атак на кінцеві точки [7]

Згідно з дослідженням Sophos, програми-вимагачі найімовірніше (29%) потрапляють в організацію через завантаження файлу або електронний лист із шкідливим посиланням. За цією технікою фішингової доставки йдуть віддалені атаки на сервери, на які припадає 21% атак програм-вимагачів, та електронні листи зі шкідливим вкладенням, на які припадає 16% атак [9].

Встановлено, що 59% атак програм-вимагачів пов'язані з даними у загальнодоступній хмарі, наприклад Office 365 або Amazon Web Services. Це стосується як того, звідки вкрадено дані, так й того, як зловмисник їх використовує. Зловмисник зазвичай надсилає викрадені дані до хмарної служби зберігання, що ускладнює виявлення активності. Google Drive, Amazon S3 та Mega.nz є найпоширенішими службами хмарного сховища для зберігання викрадених даних [9].

Також, згідно звіту від компанії SANS було встановлено відсоток потенційних загроз, виявлених за допомогою методу активного пошуку загроз (рис. 1.6). Цифри різко змінюються в бік меншої кількості інцидентів, виявлених за допомогою активного пошуку загроз. Хоча було зафіксовано несподіваний зріст: шість організацій (9%) вказали, що вони мають 81–90% успіху з пошуком загроз у своїх кінцевих точках [7].

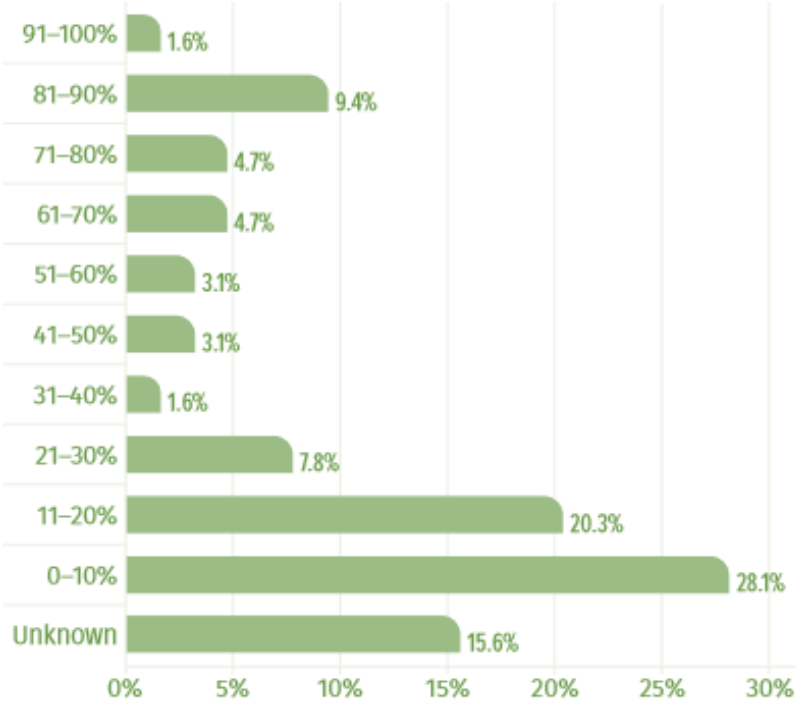

Рис. 1.6. Відсоток потенційних загроз для кінцевих точок, виявлених за допомогою активного пошуку загроз [7]

Згідно звіту від Verizon було встановлено, що програми Windows та документи Office є одними з найпопулярніших типів файлів, у яких міститься зловмисне ПЗ, а електронна пошта та Інтернет є переважними методами доставки шкідливого ПЗ.

Також компанією SANS було оцінено рівень складності для певних процесів відновлення скомпрометованих кінцевих точок (рис. 1.7). Приблизно 12% вважають пошук скомпрометованих кінцевих точок без IoCs неможливим завданням, а пошук за допомогою відомих IoCs – найпростішим завданням (58%). У цих результатах виявляється, що багато організацій все ще залежать від IoCs, або від сповіщень, або від сторонніх джерел, щоб керувати виявленням. Це може бути

сигналом про те, що виявлення інцидентів сильно покладається на відомі IoCs, тому зловмисники можуть прослизнути [7].

	Impossible	Difficult	Easy
Detecting and remediating compromised endpoints in the cloud	7.3%	41.5%	29.9%
Determining scope of a threat across multiple endpoints	3.7%	51.8%	33.5%
Scanning for compromised endpoints with known IoCs	3.7%	29.3%	57.9%
Hunting for compromised endpoints without known IoCs	12.2%	48.2%	26.8%
Identifying what data has been impacted on breached endpoints	8.5%	59.1%	20.1%
Preventing inadvertent data loss during wipe	6.7%	40.9%	31.7%
Removing all malicious artifacts on endpoints	4.3%	43.3%	38.4%
Ensuring full remediation across all impacted endpoints	5.5%	53.7%	25.6%
Other	0.6%	5.5%	3.7%

Рис. 1.7. Статистика складності певних процесів виявлення та відновлення скомпроментованих кінцевих точок [7]

Зацікавленість організацій в оновленні власних рішень безпеки кінцевих точок до нового покоління зумовлена низкою факторів. Основним фактором є те, що багато встановлених застарілих продуктів безпеки (AV, NGAV, HIPS, EPP тощо) не можуть зупинити зростаючу кількість нових загроз (46%). І навіть організації, які вважають, що вони мають надійні інструменти захисту, все ще стурбовані тим, що загрози прослизають через їхній захист (41%) [6].

Згідно звіту компанії Adaptiva, було підраховано, що щомісяця IT-команди витрачають, у середньому, 36 годин на моніторинг безпеки кінцевих точок.

Однак, незважаючи на зростання ризиків безпеки, лише 47% організацій контролюють свої мережі цілодобово та без вихідних, та лише 50% шифрують конфіденційні дані, які зберігаються на пристроях. Крім того, менше половини підприємств відстежують свою мережу та захищають корпоративні кінцеві пристрої за допомогою найновішого антивірусного ПЗ, EDR, шифрування, брандмауерів та інших методів.

За даними сервісу Statista було встановлено, що у 2022 році найбільше всього організації для захисту власних кінцевих точок використовують антивіруси або захист від шкідливого ПЗ, як показано на рис. 1.8. Проте більшість (57%) все ж

використовує EDR та планує для придбання (32%) [10]. Також непогано, що, окрім вище перерахованого, фахівці також застосовують інші методи захисту, такі як шифрування дисків, віртуалізація, моніторинг поведінки та інше.

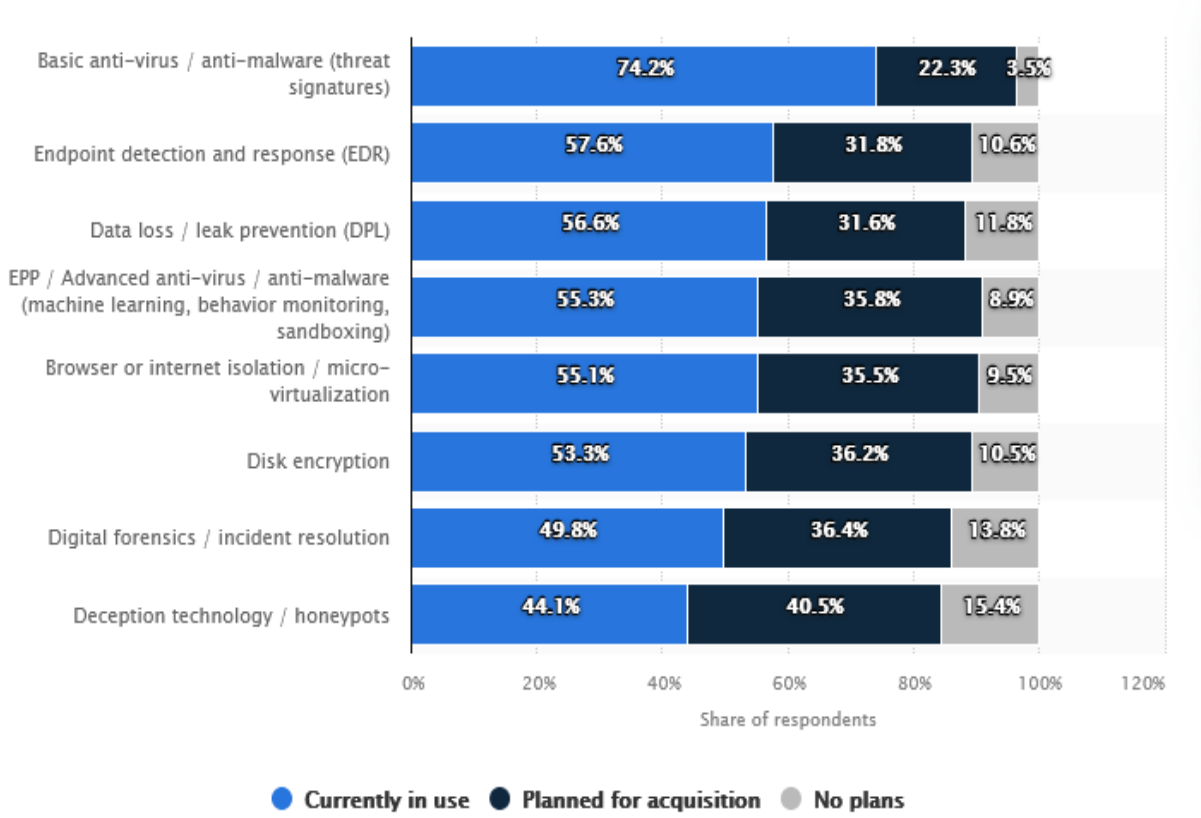

Рис. 1.8. Статистика використання організаціями різних технологій для захисту за даними 2022 року [10]

На даний момент близько 58% організацій у всьому світі працюють дистанційно. З одного боку, віддалена робота забезпечує гнучкість співробітників, проте також створює низку проблем безпеки. Коли респондентів опитування Ponemon запитали, які з цих ризиків безпеки їх найбільше турбують, то вони відповіли [9]:

- відсутність фізичної безпеки на робочому місці (47%);
- ризик зараження шкідливим ПЗ (32%);
- злочинці отримують контроль над віддаленими пристроями, щоб викрасти конфіденційні дані (24%);
- захист зовнішніх комунікацій (23%);
- безпека мережі (20%);

- злочинці використовують пристрої для отримання доступу до мережі (17%);
- фішинг й атаки соціальної інженерії (15%);
- втрачені або вкрадені пристрої (12%);
- захист зовнішнього доступу до внутрішніх ресурсів (8%).

Тут чотири з дев'яти головних проблем, які стосуються атак на кінцеві точки.

Ціна порушення безпеки кінцевої точки

За даними компанії IBM, в середньому, витік даних коштує 4,27 мільйона доларів. Атаки програм-вимагачів або інші небезпечні атаки, які знищують або стирають дані деструктивним способом, коштують у середньому 4,62 мільйона доларів й 4,69 мільйонів доларів відповідно, тоді як вартість успішної атаки на кінцеву точку зросла з 7,1 мільйона доларів до 8,94 мільйона.

Згідно з дослідженням Coveware, середня виплата за атаки програм-вимагачів залишалася досить стабільною між 2-м і 3-м кварталами 2021 року, але середня виплата подвоїлася. Це може бути пов'язано з тим, що зловмисники уникають великих цілей, які можуть спричинити національно-політичну чи правоохоронну реакцію, та, натомість, націлюються на організації середнього ринку [9].

У звіті Cybereason за 2022 рік було виявлено, що 67% компаній, які постраждали від атак програм-вимагачів, зазнали загальних збитків від 1 до 10 мільйонів доларів, а ще 4% оцінюють збитки від 25 до 50 мільйонів доларів [9].

На додаток до фінансових витрат від атаки програм-вимагачів є (дедалі поширеніший) наслідок втрати даних: понад 80% атак програм-вимагачів у третьому кварталі 2021 року включали загрозу викрадання даних. Однак, незважаючи на цю загрозу, все менше компаній погоджуються платити викуп. У 3 кварталі 47,8% компаній обрали варіант сплатити; це знизилося до 59,6% у 4 кварталі.

Час простою — ще одна величезна вартість від атак програм-вимагачів. У четвертому кварталі 2021 року середня компанія, яка постраждала від програм-вимагачів, переживала приблизно 21 день простою.

У відповідь на атаку програм-вимагачів завжди безпечніше спробувати відновити свої дані з резервних копій, ніж платити зловмисникові викуп, якщо є резервні копії. Дослідження Sophos показало, що вдвічі більше (56%) компаній вдалося відновити свої дані з резервних копій, ніж заплативши викуп (26%). Проте сплата викупу не завжди означає, що кіберзлочинець поверне дані назад. Ще 1% компаній сплатили викуп, але не отримали дані назад [9].

Крім того, дослідження Sophos виявили, що сплата викупу подвоює вартість боротьби з атакою програм-вимагачів. Ця вартість становить у середньому 761 106 доларів США по всьому світу; 505 827 доларів для компаній з 100-1000 співробітниками; та 981 140 доларів для компаній з 1000-5000 співробітників.

З усього вищеперерахованого випливає, що за захистом власних кінцевих точок необхідно ретельно доглядати, вчасно оновлювати механізми захисту, щоб не допускати тих негативних наслідків.

1.4. Аналіз технологій для забезпечення безпеки кінцевих точок

Основним призначенням захисту кінцевих точок є захист окремих пристроїв, підключених до мережі, шляхом перевірки файлів під час їх надходження. Для захисту кінцевих точок можна запропонувати як локальні, так й хмарні рішення, причому хмара є більш сучасним підходом, який є масштабованим, легшим для інтеграції та забезпечує швидшу продуктивність [21].

Різниця між антивірусом та Endpoint Protection

Антивірусне ПЗ дозволяє виявляти шкідливі програми на кінцевих точках та запобігати їх запуску. Антивірус встановлюється безпосередньо для захисту кінцевих точок, та виявляє наявність зловмисного ПЗ, скануючи файли за списком попередньо визначених сигнатур [2].

Основним недоліком традиційного антивірусного ПЗ є те, що БД сигнатур потрібно регулярно оновлювати для виявлення останніх загроз, та навіть у цьому випадку певне шкідливе ПЗ уникає виявлення антивірусом. Також антивірусні рішення не контролюються дистанційно ІТ-персоналом або фахівцями з безпеки, а

з ізольованими/індивідуальними кінцевими точками дослідження проблем та потенційних загроз є виснажливим й трудомістким завданням.

Захист Endpoint Security має зовсім інший підхід порівняно з традиційним антивірусом. Замість того, щоб захищати одну кінцеву точку, системи безпеки кінцевих точок захищають всю мережу підприємства, включаючи всі кінцеві точки та сервери в ній. Це дозволяє проводити централізоване адміністрування та забезпечувати кращий захист від загроз [2].

EPP проти EDR проти XDR

Рішення для захисту кінцевих точок зараз зазвичай називають EPP, які являють собою набори хмарних рішень безпеки кінцевих точок, які забезпечують більш надійний захист, ніж окремі продукти безпеки кінцевих точок, такі як антивірусне ПЗ. Оскільки загрози кібербезпеці стають все більш складними, одних лише антивірусних рішень недостатньо, щоб зупинити передові методи зловмисного ПЗ та програм-вимагачів, які більше не базуються лише на сигнатурах, а тому їх важче виявити. EPP забезпечують запобігання та захист від загроз кібербезпеці, таких як: файлове або безфайлове зловмисне ПЗ, відомі та невідомі загрози, шкідливі сценарії та загрози на основі пам’яті. Захист від поведінкових загроз та аналіз на основі ШІ за допомогою машинного навчання допомагають завчасно ідентифікувати, виявляти та зупиняти нові загрози [11].

EPP також можуть надавати можливість виявляти та блокувати зловмисну діяльність, а також досліджувати та виправляти будь-які інциденти, які ухиляються від контролю захисту. Це відоме як EDR. EDR постійно відстежує пристрої кінцевих користувачів, щоб виявляти та реагувати на кіберзагрози, такі як: програми-вимагачі та зловмисне ПЗ. Телеметрія кінцевої точки, зібрана EDR, дозволяє сортувати та досліджувати виявлені загрози за допомогою процесів, які є високоавтоматизованими, що дозволяє командам SOC швидко виявляти загрози та реагувати на них.

Наступна еволюція захисту кінцевих точок відома як XDR. XDR — це новітній підхід до безпеки кінцевих точок, який пропонує покращений захист, виявлення та реагування завдяки інтеграції не лише даних кінцевих точок, а й

даних із будь-якого джерела, наприклад мережі, хмарних даних або даних третіх сторін. Потім усі дані аналізуються з однієї консолі, а не з різних систем, щоб краще розслідувати інциденти та зняти навантаження з операцій SOC. Бажаним результатом для ефективного рішення XDR є не тільки забезпечення надійного захисту кінцевих точок, але й уможливлення більш спрощеного підходу до реагування на інциденти та створення цілеспрямованих, високоефективних виявлень. Консолідація цих рішень допомагає краще керувати ризиками та підвищити продуктивність операцій безпеки [21].

Можливості та порівняння програмних рішень

Деякі аналітичні агентства, наприклад The Radicati Group, порівнюють комплексні підходи щодо протидії складним загрозам кінцевим пристроям, а також у своєму звіті «Endpoint Security 2022» оцінюють постачальників комплексних рішень відповідно до списку основних функцій та можливостей. Окремо виділяються критерії порівняння з наданням рішень EDR-функціональності або можливості взаємодії зі сторонніми продуктами класу EDR. Особлива увага приділяється можливостям системи EDR щодо передачі зібраної інформації з кінцевих пристроїв у централізовану БД для додаткового аналізу та об’єднання цієї інформації з даними, отриманими від інших засобів виявлення загроз, наприклад, у мережі для отримання повної картини розвитку загроз, що виникають на всій інфраструктурі [3].

Radicati Group відзначає на ринку рішень щодо захисту від загроз на кінцеві точки за стратегічним баченням та функціональністю наступні компанії: Broadcom (Symantec), ESET, Cisco, Bitdefender, Kaspersky, Sophos, Trellix, Palo Alto Networks, VMware Carbon Black, Microsoft (рис. 1.9).

Очікується, що світовий дохід від рішень Endpoint Protection зросте з 6,9 мільярдів доларів США у 2022 році до майже 15,2 мільярдів доларів США до 2026 року.

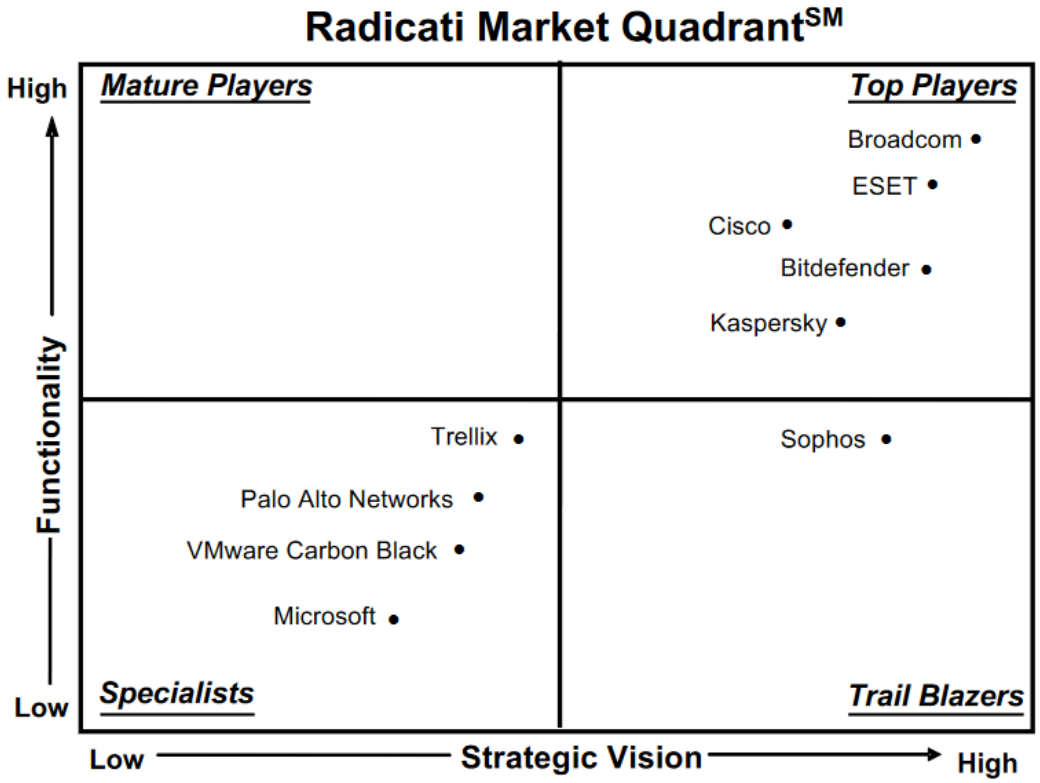

Рис. 1.9. Топ виробників продуктів для захисту кінцевих точок станом на 2022 рік за даними Radicati [4]

На ринку продуктів безпеки є велика різноманітність компаній та їхніх програм безпеки. Тому далі буде проаналізовано найбільш популярні рішення від провідних компаній щодо захисту кінцевих точок.

ESET Endpoint Security

ESET є провідним постачальником ПЗ для захисту кінцевих точок та антивірусного ПЗ, відомим своїми потужними, але легкими рішеннями для кібербезпеки. Їхній продукт ESET Endpoint Security являє собою хмарну та локальну програму, що захищає кінцеві пристрої від зловмисної діяльності, яка може проникнути через мережу. ESET Endpoint Security поєднує технології машинного навчання та краудсорсинговий аналіз загроз для виявлення та запобігання цільовим атакам зловмисного ПЗ та програм-вимагачів. Рішення відстежує всі запущені програми на наявність шкідливого вмісту на основі їх відомої поведінки та репутації. Він також сканує поведінку зловмисних файлових

процесів у пам’яті кожної кінцевої точки, щоб виявити та усунути безфайлові загрози [15].

Також продукт проводить блокування підключень зловмисного ПЗ до мережі. Це є «двостороннім брандмауером» та є другою лінією захисту. Першою лінією захисту є система запобігання вторгненням на основі хоста (HIPS), що відслідковує меседжі про події в файлах журналу на кінцевих пристроях [15].

ESET Endpoint Security встановлюється на Windows, Linux, Mac та Android системи. Проте, багато функцій адаптовано до мереж середнього та великого розміру, менші домашні мережі використовують не всі доступні функції.

Bitdefender GravityZone

Bitdefender GravityZone захищає від повного спектру складних кіберзагроз. Він забезпечує багаторівневий захист із незмінно високими показниками виявлення в провідних незалежних тестах. Завдяки платформі з одним агентом та єдиною консоллю для фізичних, віртуальних, мобільних, хмарних кінцевих точок та електронної пошти, - це рішення мінімізує накладні витрати на керування, забезпечуючи послідовну видимість та контроль. Рішення забезпечує сучасний захист від широкого спектру атак із покращеною видимістю та контролем за допомогою експертизи та візуалізації атак, забезпечуючи основні переваги рішень EDR за нижчої вартості володіння та розкриваючи повний вплив атак. Це дозволяє зосередитися на конкретних загрозах та вжити заходів для їх усунення. Він включає в себе можливості захисту від програм-вимагачів, зменшення площі атак, оцінки надійності, захист від безфайлових та мережевих атак, а також параметри хмарного або локального керування в інтегрованій централізованій консолі керування [15].

GravityZone також відслідковує регулярні дії на кінцевій точці, щоб встановити базовий рівень поведінки. Аномальна активність, яка не схожа на базовий рівень, спонукає заходи захисту. Дані заходи містять відслідковування явної активності експлойтів, яка характеризує атаки нульового дня. Також дозволяє шифрувати усі диски, щоб дані стали нечитабельними для злочинців.

Sophos Endpoint Protection

Sophos Endpoint Protection забезпечує захист від зловмисного ПЗ та шкідливого веб-трафіку. Це також дає адміністраторам більший контроль над веб-вмістом, програмними пристроями та елементами керування даними, а також комплексне застосування правил. Платформу можна розгорнути як хмарну консоль або встановити на місці. Sophos сканує всі каталоги на наявність зловмисного ПЗ, а також перевіряє всі USB-накопичувачі, коли вони підключені [15].

У січні 2019 року Sophos викупила DarkBytes, постачальника криміналістики кінцевих точок. Цю послугу включено в платформу керованого виявлення та реагування Sophos. Клієнти Sophos хвалять запропоновані функції безпеки, стверджуючи, що вони «зупиняють зловмисне ПЗ нульового дня» та забезпечують розширені функції захисту від програм-вимагачів.

Клієнти також хвалять Sophos за простоту використання. Sophos надає єдину консоль адміністратора, з якої можна керувати всіма кінцевими точками, що, на думку Gartner, є візуально привабливим. Однак як відгуки клієнтів, так й звіт Gartner показують, що деякі клієнти стикалися з повільним встановленням та оновленнями ПЗ. Sophos є хорошим варіантом для компаній середнього ринка та підприємств.

Microsoft Endpoint Protection

Endpoint Protection від Microsoft тісно інтегрована з Windows 10. Корпорація Майкрософт описує її як уніфіковану платформу для захисту пристроїв за допомогою поведінкової антивірусної програми, виявлення після злому, автоматизації та реагування. Корпорація Майкрософт також надає консоль реагування на інциденти, яка надає сповіщення та реагування на інциденти в програмі Defender ATP, а також ATP, Office 365, Azure та Active Directory. Також Defender автоматично вимикає інше ПЗ для захисту від зловмисного ПЗ та EDR, наявне на кінцевій точці [15].

Defender ATP працює з Windows, але також доступний у різних середовищах із версією для Mac та Linux. Gartner повідомляє, що Windows Defender Anti-Virus став найпопулярнішою платформою для захисту кінцевих точок бізнесу, що робить його лідером на ринку в цьому просторі. Windows Defender є хорошим вибором для

клієнтів Windows, які шукають рішення для керування своїми кінцевими точками, не бажаючи використовувати інструмент захисту кінцевих точок сторонніх розробників [15].

Symantec Endpoint Protection

Symantec Endpoint Protection використовує методи ШІ для відстеження зловмисної активності. Система є у доступі як програмний модуль, так й як хмарна служба. Локальне ПЗ працює на Windows, Windows Server, Android, Mac OS та Linux. Система застосовує методи SIEM задля перевірки підозрілих подій, що записуються у файли журналу. Він також проводить створення шаблону типової поведінки на кінцевому пристрої та подає сповіщення, коли процес на кінцевому пристрої відхиляються від типової поведінки. Symantec також безперервно проводить сканування пам’яті на наявність підозрілих дій. SEP зберігає записи усіх моделей активності задля аналізу довгостроково. Також, окрім попередження, система проводить запуск автоматичних дій задля блокування зловмисних процесів, щойно їх помічає.

Висновки до розділу

Було розібрано поняття, що являє собою кінцева точка. Визначено актуальність та необхідність захисту кінцевих точок.

Досліджено різноманітність основних загроз та атак на кінцеві точки, а також як вони реалізовуються.

Проаналізовано статистику останніх років щодо атак на кінцеві точки, їх вектори та поширеність.

Розглянуто різноманітність технологій для захисту кінцевих точок, різницю між ними, їхні можливості, а також Symantec Endpoint Protection, який є об’єктом цього дослідження та далі буде проаналізований більш детально.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК НА БАЗІ РІШЕННЯ SYMANTEC ENDPOINT PROTECTION

2.1. Можливості та призначення Symantec Endpoint Protection

У минулому розділі було з’ясовано, що захист кінцевих точок є дуже важливим, чутливим та необхідним процесом для забезпечення їхнього безпечного функціонування. Саме для цього у даній роботі буде використовуватися продукт Symantec Endpoint Protection, що показує гарні результати у різних тестах щодо ефективності захисту.

Symantec Endpoint Protection (SEP) являє собою комплексне рішення безпеки, яке захищає ноутбуки, настільні ПК та сервери від зловмисного ПЗ, а також інших небезпечних атак. SEP поєднує захист від вірусів із розширеним захистом від загроз, щоб проактивно захищати клієнтські кінцеві точки від відомих та невідомих загроз, таких як віруси, хробаки, троянські програми та рекламне ПЗ. SEP забезпечує захист навіть від найскладніших атак, що обходять традиційні заходи безпеки, наприклад руткітів, атак нульового дня та шпигунського ПЗ, яке змінюється.

У останній версії SEP перейшов до нового класу NGEP. Також організація Symantec викупила активи у організації Blue Coat, які займаються мережевими пристроями для кешування даних, що дало змогу додати нові можливості та технології всій лінійці продуктів Symantec, для прикладу, аналізування зашифрованого SSL-трафіку, а також сприяло збільшенню загального обсягу баз репутації. У SEP вдало реалізовано новітні механізми захисту від експлуатації уразливостей нульового дня, а також від невідомих загроз. Сюди відносяться технологія захисту від експлойтів Generic Exploit Mitigation, поновлена модифікація модуля для аналізу поведінки додатків SONAR та технологія

машинного навчання Advanced Machine Learning для аналізу файлів, що виконуються [17].

Основна перевага SEP полягає в тому, що він забезпечує захист кінцевих точок шляхом регулярного сканування даних кінцевих точок на наявність загроз безпеці. Він також зупиняє неавторизовані програми та реалізує суворі політики брандмауера для моніторингу мережевого трафіку. Шкідливий трафік із корпоративних мереж або браузерів автоматично блокується. ПЗ використовує сукупну інформацію від інших користувачів, щоб виявити потенційні загрози. Він також ефективно використовує переваги передового ШІ та машинного навчання, щоб забезпечити низький рівень виявлення помилкових спрацьовувань [19].

Якщо говорити більш узагальнено, то SEP займається та відповідає за виявлення, розширений захист від зловмисного ПЗ, EDR, контроль ізоляції программ, запобігання експлойтам (рис. 2.1.).

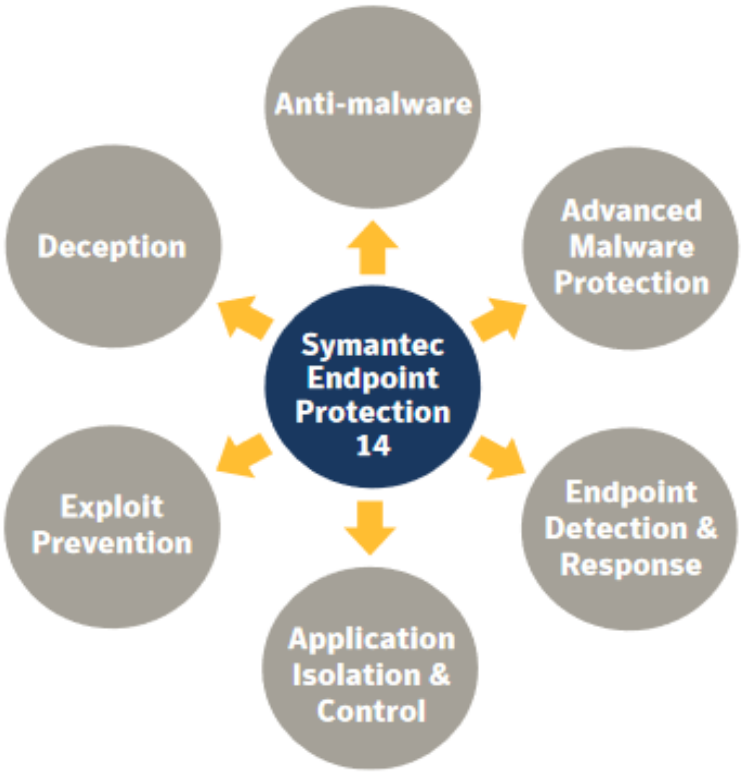

Рис. 2.1. Основні можливості SEP [20]

Незалежна тестова фірма AV-Test Institute надіслала через SEP майже 22 000 зразків зловмисного ПЗ. Продукт SEP виявив їх усіх. Інший тест піддав SEP

загрозам нульового дня. Ці атаки використовують уразливості ПЗ, щоб обійти захист. SEP припинив роботу на 100%, забезпечивши продукту ідеальний бал із захисту.

Забезпечуючи низькі витрати на обслуговування та високу потужність, SEP обмінюється даними через мережу, щоб автоматично захищати фізичні та віртуальні системи від атак. SEP пропонує ефективні та прості в розгортанні та використанні рішення для керування [16].

Програмний продукт SEP використовує кілька рівнів безпеки для захисту IT-мережі. Антивірус у Symantec на основі ШІ становить основу SEP, а кілька інших функцій доповнюють його функціональність.

SEP блокує загрози, які намагаються проникнути через пристрої, підключені до кінцевої точки, наприклад USB-накопичувачі. Також SEP надає «інструмент обману (приманка)», який представляє собою пастку або приманку для кібератак. Його суть полягає у тому, що запускається фіктивні процеси або програми, на які буде цілитись потенційний вірус чи зловмисник. Це допоможе безпечно визначити вторгнення ще до його основної реалізації.

SEP знижує схильність до загроз декількома способами. Він ізолює привілейовані програми, щоб на них не потрапили жодні атаки. Створюються так звані «білі та чорні списки», які контролюють дозволене встановлення ПЗ. Також SEP переглядає конфігурацію Windows Active Directory, щоб запропонувати покращення безпеки, а оцінка уразливості визначає, чи є у нас старі версії ПЗ, які потребують оновлення [18].

SEP забезпечує найповніший захист кінцевих точок, будучи розгорнутим як локальним або хмарним рішенням, одноагентна платформа Symantec дозволяє захищати традиційні та мобільні кінцеві пристрої, забезпечуючи взаємозалежний захист на рівні пристрою, програми та мережі, а також використовує ШІ для оптимізації безпеки.

У клієнті SEP для Windows доступно три види розгортання – стандартний, dark network та embedded/VDI. Стандартний клієнт для Windows має усі функціональні можливості рішення та розрахований для роботи на кінцевих

пристроях усередині локальної мережі компанії. Dark network — являється версією для віддалених кінцевих точок, які не мають можливості постійно з'єднуватися з приватною чи глобальною хмарою Symantec, а також сервером керування. У цьому виді клієнта вимкнено перевірку, що об’єднана з аналізом потенційно-небезпечних файлів у хмарі, проте інші функціональні можливості працюють подібно стандартному виду клієнта, включно з базами репутації. Embedded/VDI являється зменшеним у об’ємі дистрибутивом, який застосовує більшу можливість хмари, ніж попередні клієнти, та застосовується у системі, що вбудовується, а також у інфраструктурі віртуального робочого столу [17].

Symantec пропонує інноваційний підхід до адаптивного захисту, щоб зосередитися на посиленні захисту в усьому ланцюжку атак — з акцентом на запобіганні для швидкого стримування. Адаптивний захист автоматизує конфігурацію безпеки, щоб без зусиль забезпечити індивідуальний захист для кожної організації. Проактивне зменшення площі атак та інноваційні технології запобігання атак забезпечують найсильніший захист від найважчих для виявлення загроз, які покладаються на приховане зловмисне ПЗ, крадіжки облікових даних, безфайлових атак.

Symantec також запобігає повномасштабним порушенням до того, як може статися ексфільтрація. Складна аналітика атак, аналіз поведінки, автоматизовані посібники з розслідування, а також запобігання крадіжці облікових даних забезпечують точне виявлення атак та проактивний пошук загроз для стримування зловмисника та вирішення постійних загроз у режимі реального часу [16].

SEP заздалегідь налаштовує стандартні параметри, такі як захист від вірусів та програм-шпигунів, які автоматично застосовуються до кінцевих точок. Ці попередньо налаштовані параметри суттєво заощаджують час та дозволяють негайно розгортати SEP. При бажанні можна налаштувати параметри після того, як система безпеки буде запущена.

Можливості SEP великі, але жодна платформа не може реалізувати їх усі. SEP інтегрується з іншими продуктами безпеки Symantec, тому у міру зростання

власних потреб у безпеці можна безперешкодно розширювати можливості безпеки, створюючи додатковий набір засобів захисту.

SEP також інтегрується з ПЗ для безпеки від затверджених зовнішніх постачальників через відкриті API (інтерфейс програмування програм) в рамках партнерської програми з інтеграції технологій (TIPP) [18].

2.2. Архітектура та компоненти продукту Symantec Endpoint Protection

Архітектура SEP використовує три функціональні групи компонентів, які разом захищають компанію від загроз безпеці. Деякі з компонентів належать до кількох груп, оскільки вони багатофункціональні. Функціональні компоненти архітектури SEP продемонстровано на рис. 2.2.

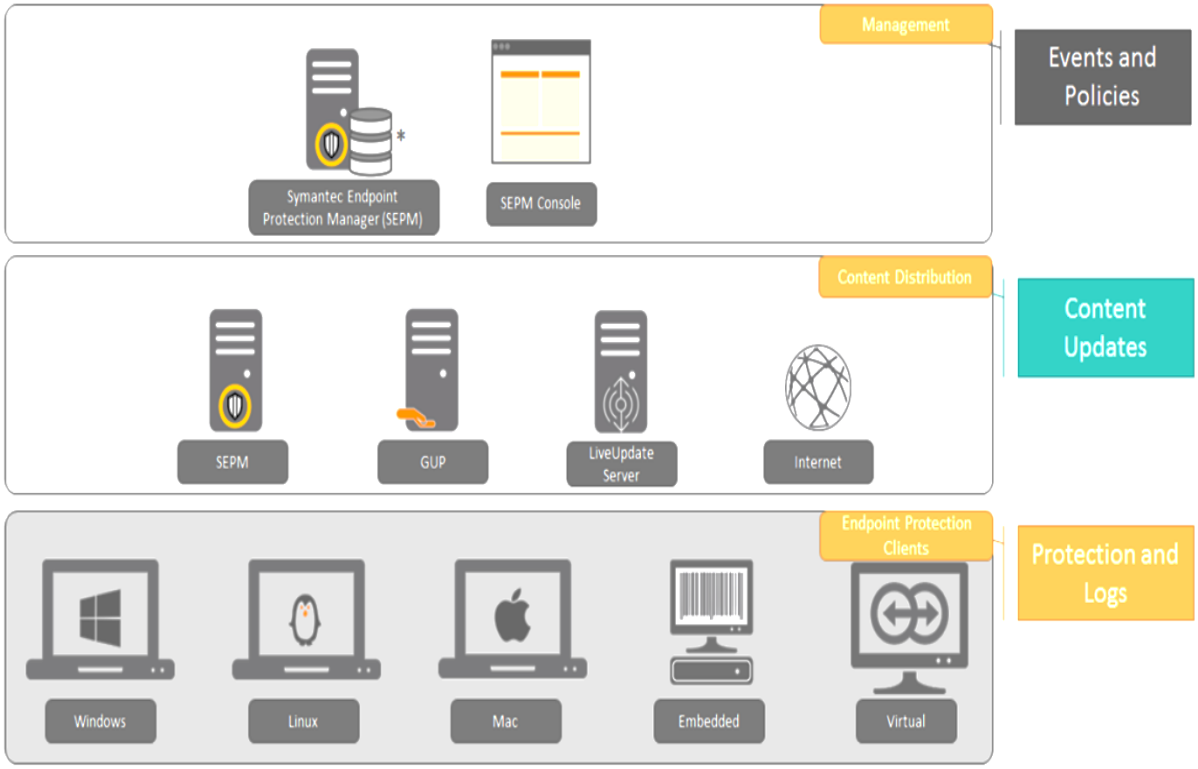

Рис. 2.2. Компоненти архітектури SEP [16]

Нижче розглянемо дані компоненти трохи детальніше.

Symantec Endpoint Protection Manager – це сервер керування, який керує подіями, політиками та реєстрацією клієнтів для клієнтських комп'ютерів, які

підключаються до мережі компанії. Даний компонент включає наступні підкомпоненти:

o ПЗ сервера керування забезпечує безпечний зв’язок між клієнтськими комп’ютерами та консоллю.

o Консоль є інтерфейсом до сервера керування. ПЗ консолі координує та керує політиками безпеки, клієнтськими кінцевими точками, звітами, журналами, ролями та доступом, адміністративними функціями та безпекою. Також консоль встановлюється віддалено та використовується для входу на сервер керування з будь-якої кінцевої точки, що підключена до мережі.

o БД зберігає політики та події безпеки та встановлюється за допомогою Symantec Endpoint Protection Manager. Також дозволяється інсталювати БД Microsoft SQL Server, щоб використовувати її замість автоматично встановленої Microsoft SQL Server Express (починаючи з версії 14.3 RU1) або вбудованої БД (14.3 MP1 та ранішої версії). SQL Server рекомендовано для великих організацій із 5-ма тисячами та більше кінцевих точок. Symantec Endpoint Protection Manager взаємодіє з локальною або віддаленою БД Microsoft SQL Server [16].

Symantec Endpoint Protection client – клієнт Symantec Endpoint Protection надає частину рішення, яке забезпечує захист. Даний клієнт завантажує політики та інколи вміст із Symantec Endpoint Protection Manager та працює на Windows, Mac та Linux ОС.

SEP також дозволяє клієнту завантажувати вміст із сервера керування, постачальника групових оновлень, внутрішнього сервера LiveUpdate або Інтернету.

Клієнта можна встановити як керованого, так й як некерованого. Керований клієнт зв’язується з сервером керування у власній мережі. Адміністратор налаштовує захист та параметри за замовчуванням. Сервер керування сповіщає клієнта, після цього клієнт завантажує налаштування. Залежно від налаштувань зв’язку сервера керування, якщо адміністратор вносить зміни до захисту, клієнт майже негайно завантажує зміни. Доступність налаштувань клієнта, а також значення самих налаштувань можуть періодично змінюватися. Наприклад,

параметр може змінитися, коли адміністратор оновить політику, яка керує захистом клієнта [16].

Некерований клієнт не зв’язується з сервером керування, а адміністратор не керує клієнтом. Під час першого встановлення клієнт має налаштування за замовчуванням. Після встановлення клієнта можна змінити всі налаштування клієнта та виконати всі завдання захисту.

Тепер розберемо додаткові компоненти та їх функції.

LiveUpdate Administrator – адміністратор LiveUpdate завантажує підписи, визначення та інший вміст із внутрішнього сервера LiveUpdate та розповсюджує оновлення на клієнтські кінцеві пристрої. Внутрішній сервер LiveUpdate можна використовувати у дуже великих мережах, щоб зменшити навантаження на Symantec Endpoint Protection Manager. Також слід використовувати внутрішній сервер LiveUpdate, якщо у організації використовується декілька продуктів Symantec, які також використовують LiveUpdate для оновлення безпекових компонентів на клієнтських кінцевих точках [16].

LiveUpdate також може вносити покращення у встановлений клієнт за необхідності. Ці покращення зазвичай створюються для розширення сумісності ОС або обладнання, вирішення проблем із продуктивністю або виправлення помилок продукту. Ці оновлення можуть надходити через сервер керування, якщо він налаштований на це. LiveUpdate отримує нові файли вмісту із сайту Symantec в Інтернеті, а потім замінює старі файли вмісту на оновлені.

За замовчуванням, LiveUpdate запускається автоматично через заплановані інтервали часу. Проте також можна змінити розклад, щоб LiveUpdate запускався автоматично через заплановані проміжки часу. Можна запланувати запуск LiveUpdate на той час, коли користувач не використовує кінцевий пристрій.

На керованих клієнтах дозволяється лише налаштувати LiveUpdate для запуску за розкладом або змінити існуючий розклад, якщо це дозволено адміністратором. Якщо відображається піктограма замка, а параметри виділені сірим кольором, то значить, що заборонено оновлювати вміст за розкладом або

змінювати існуючий розклад. На некерованому клієнті можна вимкнути або змінити графік LiveUpdate.

Проте LiveUpdate слід запускати вручну з наступних причин [16]:

- Клієнтське ПЗ було встановлено нещодавно.
- Пройшло багато часу з моменту останнього сканування.
- Якщо було запідозрено, що намагається або проник вірус чи інше шкідливе ПЗ.

Group Update Provider – постачальник групових оновлень допомагає поширювати вміст всередині організації, особливо корисно для груп у віддалених місцях із мінімальною пропускною здатністю. Організації, які мають багато клієнтів, можуть використовувати GUP для клієнтів Windows. GUP зменшує навантаження на сервер керування та їх легше налаштувати, ніж внутрішній сервер LiveUpdate.

До переваг GUP відносяться [16]:

- Зберігає смугу пропускання та ресурси сервера керування, перекладаючи обчислювальну потужність на GUP.
- Ефективно доставляє оновлення клієнтам з обмеженим або повільним підключенням до мережі.
- Простіше настроїти, ніж внутрішній сервер LiveUpdate.

Тип настроюваного GUP залежить від мережі та клієнтів у цій мережі. Типи GUP не є взаємовиключними. Для кожної політики можна налаштувати один або кілька типів GUP.

Один GUP являє собою виділений клієнтський комп'ютер, який надає вміст для однієї або кількох груп клієнтів. Налаштування одного GUP перетворює одного клієнта на GUP. Один GUP може бути клієнтським комп'ютером у будь-якій групі. Також слід використовувати єдину політику параметрів LiveUpdate, щоб вказати статичну IP-адресу або ім'я хоста для одного GUP. Однак якщо клієнт, який є єдиним GUP, змінює розташування, необхідно змінити IP-адресу в політиці. Якщо хочеться використовувати різні постачальників оновлень для окремих груп, то необхідно створити окрему політику параметрів LiveUpdate для кожної групи.

Декілька GUP використовують набір правил або критеріїв, щоб обрати себе для обслуговування груп клієнтів у власних підмережах. Всі комп'ютери клієнта знаходяться в одній підмережі. Вказуються критерії, яким повинні відповідати клієнтські комп'ютери, щоб вважатися GUP. Якщо клієнтський комп'ютер відповідає критеріям, сервер керування додає його до глобального списку GUP. Потім сервер управління робить глобальний список доступним для всіх клієнтів у мережі. Клієнти перевіряють список та вибирають GUP, які знаходяться у їхній власній підмережі [16].

Symantec Endpoint Security cloud console – це консоль керування, яка використовується для керування клієнтськими кінцевими точками з хмари. Дана консоль є версією локальної SEP, яка повністю керується хмарою. Керувати кінцевими пристроями дозволяється за допомогою будь-якого з таких варіантів:

- Symantec Endpoint Protection Manager (тільки локально).
- З Symantec Endpoint Protection Manager та Symantec Endpoint Security (гібридно: локально та хмарно).
- Symantec Endpoint Security (лише хмара).

Symantec Endpoint Security працює на Symantec Integrated Cyber Defense Manager (ICDm), хмарній платформі, яка об’єднує хмарні та локальні продукти в одному місці [16].

SEP постачається з кількома інструментами, які допоможуть підвищити рівень безпеки та керувати продуктом.

2.3. Технології виявлення та захисту Symantec Endpoint Protection

У SEP використовується багаторівневий підхід до захисту. Комплексний підхід забезпечує захист мережі до, під час та після атаки. SEP знижує ризик викриття, надаючи інструменти для підвищення рівня безпеки перед будь-якою атакою. Щоб мати достатній рівень захисту для кінцевих пристроїв у мережі, необхідно, щоб усі засоби захисту були увімкнені завжди. SEP використовує

наведені нижче основні технології для захисту від відомих та невідомих загроз на різних етапах атаки (рис. 2.3).

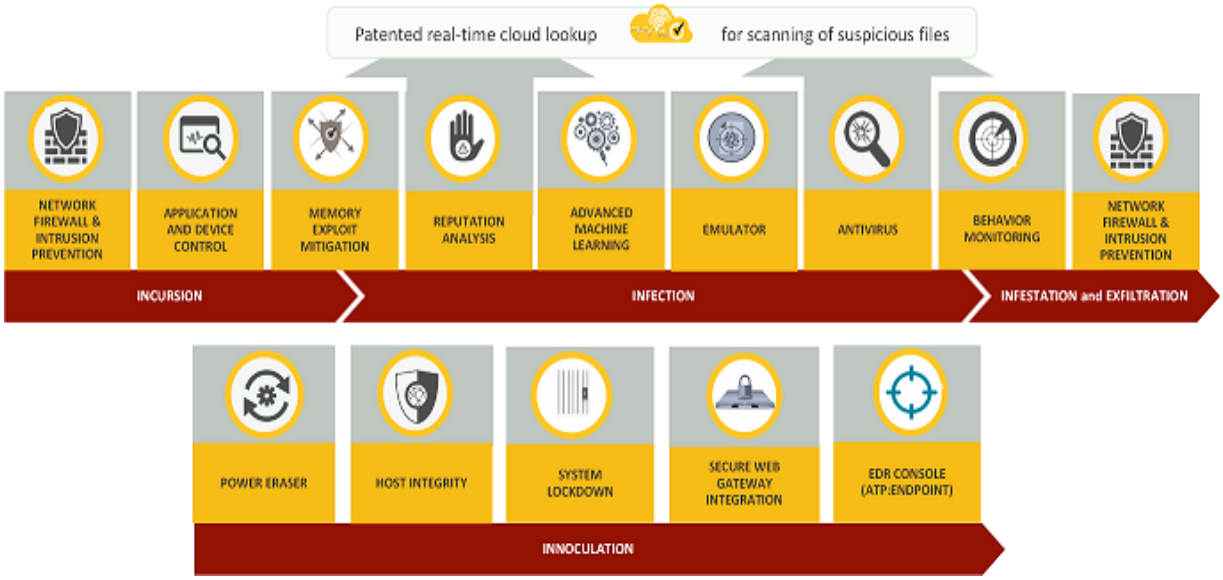

Рис. 2.3. Основні технології Symantec Endpoint Protection [16]

SEP використовує наступний цілісний підхід до забезпечення безпеки для захисту середовища по всьому ланцюжку атак, під час наступних етапів: вторгнення, інфекціонування, зараження та ексфільтрація, а також виправлення. Розберемо їх детальніше.

Етап 1: Вторгнення

Під час етапу вторгнення хакери зазвичай проникають у мережу, використовуючи цільові атаки, такі як соціальна інженерія, уразливості нульового дня, впровадження SQL, цільове шкідливе ПЗ або інші методи.

SEP захищає від атак до того, як вони проникнуть у систему, використовуючи такі технології:

- *Запобігання вторгненням/брандмауер (захист від мережевих загроз):* проводить аналіз усього вхідного та вихідного трафіку, а також пропонує захист браузера для блокування таких загроз, перш ніж вони можуть бути виконані на кінцевому пристрої. Брандмауер на основі правил та захист браузера забезпечують захист від веб-атак.

- *Контроль додатків*: дає змогу створювати різного роду правила для контролювання доступу додатків до елементів реєстру, а також пуску/виключення процесів та загрузки бібліотек. Дане правило щодо заборони дозволяється забезпечити описом, що буде відображатись юзеру під час блокування доступу.

- *Контроль пристроїв*: створюються так звані білі та чорні списки пристроїв, які обмежують доступ до вибраного обладнання та контролюють, які типи пристроїв можуть завантажувати інформацію. Для Windows-клієнтів дозволяється вказувати лише тип свого пристрою (для прикладу, усі USB-пристрої) [17].

- *Запобігання експлойтів пам'яті*: являє собою механізм для контролювання пам'яті, та може забезпечувати захищеність від експлуатації уразливостей нульового дня у ПЗ та ОС. Цей механізм застосовується ще до початку процесу аналізування файлів, що використовуються SONAR-системою чи будь-якими другорядними компонентами захисту, що у результаті збільшує основний рівень захисту системи.

- *Захист доступу до Інтернету та хмари:* контролює мережевий трафік через усі порти та протоколи, незалежно від того, де знаходяться корпоративні користувачі [16].

Етап 2: Інфікування

Під час цілеспрямованих атак хакери зазвичай проникають у мережу організації, використовуючи ту ж саму соц інженерію, уразливості нульового дня, ін’єкції, шкідливе ПЗ та подібні методи. Symantec використовує такі наступні технології для виявлення та запобігання цим атакам до того, як вони заразять систему:

- *Захист від використання пам’яті:* запобігає доступу процесу до нерозподіленої пам’яті в ОС, оскільки він не дозволяє ПЗ захопити контроль над надмірним об’ємом пам’яті та може спричинити пошкодження, яке вплине на інше ПЗ, яке зараз використовується, або призвести до втрати збережених даних. Ці засоби захисту пам'яті також допомагають виявляти зловмисні або шкідливі програми, які можуть пошкодити процеси в ОС.

- *Аналіз репутації файлів:* на основі ШІ, який використовує глобальну інтелектуальну мережу Symantec. Цей розширений аналіз вивчає мільярди корельованих посилань від користувачів, веб-сайтів та файлів, щоб ідентифікувати шкідливе ПЗ, яке швидко змінюється, а також захиститися від нього. Аналізуючи ключові атрибути (наприклад, вихідну точку завантаження файлу), Symantec може точно визначити, чи є файл хорошим або поганим, та призначити оцінку його репутації ще до того, як файл дійде до клієнтського кінцевого пристрою [16].

- *Розширене машинне навчання:* аналізує трильйони прикладів хороших та поганих файлів, які містяться в глобальній інтелектуальній мережі. Розширене машинне навчання — це безсигнатурна технологія, яка може блокувати нові варіанти зловмисного ПЗ на етапі попереднього виконання. Даний механізм за функціонуванням має схожість з аналізатором сигнатур, проте забезпечує захищеність від невиявлених загроз [17].

- *Високошвидкісна емуляція:* виявляє приховане зловмисне ПЗ за допомогою поліморфних спеціальних пакувальників. Сканер запускає кожен файл за мілісекунди у спрощеній віртуальній машині, яка спонукає до виявлення загроз, покращуючи рівень виявлення та продуктивність.

- *Антивірусний захист файлів (захист від вірусів та шпигунського ПЗ):* використовує антивірус на основі сигнатур та файлову евристику для пошуку та знищення зловмисного ПЗ в системі, для захисту від троянів, вірусів, руткітів, хробаків, ботів, шпигунського та рекламного ПЗ. Він також має драйвер раннього запуску для додаткової захищеності, який запускається першим у системі, що дає змогу виявляти, а також знешкоджувати шкідливі носії, що виконуються під виглядом драйвера.

- *Поведінковий аналіз (SONAR):* використовує машинне навчання, щоб забезпечити захист від нульового дня, зупиняючи нові та невідомі загрози. Даний ШІ може аналізувати більше 1390 моделей поведінки загроз на основі мільйонів зразків загроз, класифікуючи їх по, приблизно, 1000 внутрішніх правил, щоб визначити ризик. Параметри за замовчуванням залежать від типу політики захисту від вірусів та програм-шпигунів. Можна використовувати збалансовану політику,

політику високої безпеки або політику високої продуктивності. Евристичні загрози SONAR класифікує як шкідливі з більшою ймовірністю (високий ризик) або меншою ймовірністю (низький ризик). Для виявлення з низьким рівнем ризику можна вимкнути будь-яку дію, тому потім SONAR виявляє лише ті програми, які, швидше за все, є шкідливими [16].

Етап 3: Зараження та ексфільтрація

Після того, як зловмисники отримають контроль над цільовими системами, вони можуть викрасти інтелектуальну власність або інші конфіденційні дані. Зловмисники використовують отриману інформацію для аналізу та подальшої експлуатації чи шахрайства. Для захисту від цього SEP застосовує наступні технології:

- *Поведінковий аналіз:* допомагає зупинити поширення інфекції.
- *Запобігання вторгненням/брандмауер:* блокує загрози під час їхнього проходження через мережу.

Етап 4: Виправлення

SEP містить єдину консоль та агент, який забезпечує захист ОС, платформ та підприємств будь-якого розміру. На цьому етапі застосовуються наступні технології захисту:

- *Power Eraser:* агресивний інструмент, який можна запустити дистанційно, щоб усунути постійні загрози та виправити стійке шкідливе ПЗ. Можна обрати, чи виконувати аналіз Power Eraser з виявленням руткітів чи без нього. Також слід запускати Power Eraser на якомога меншій кількості кінцевих точок, бо якщо виконувати аналіз на багатьох комп’ютерах одночасно, то це може негативно вплинути на продуктивність власної мережі [16].
- *Цілісність хосту:* гарантує, що кінцеві точки захищені та відповідають вимогам, застосовуючи політики, виявляючи неавторизовані зміни та проводячи оцінку збитку. Тоді система цілісності хосту виділяє керовану систему, яка не відповідає вимогам.
- *System Lockdown:* дозволяє запускати програми (завідомо як хороші) або блокує роботу програм (завідомо як погані). У будь-якому режимі System

Lockdown використовує контрольну суму та параметри розташування файлів, щоб перевірити, схвалено додаток чи не схвалено. Блокування системи корисне для випадків, де потрібно запускати лише одну програму [16].

- *Інтеграція безпечного веб-шлюзу:* використовує програмовані REST API, щоб зробити можливою інтеграцію з безпечним веб-шлюзом, щоб допомогти швидко зупинити поширення інфекції на клієнтському кінцевому пристрої [16].
- *Інтеграція консолі EDR:* SEP інтегрований із Symantec EDR та призначений для швидшого виявлення, реагування та блокування цілеспрямованих атак та розширених постійних загроз шляхом визначення пріоритетів атак. Функція EDR (виявлення та реагування кінцевих точок) вбудована в SEP, що робить непотрібним розгортання додаткових агентів.

Висновки до розділу

Досліджено призначення та можливості продукту SEP, переваги його використання, а також його підходи до забезпечення захисту на встановленому кінцевому пристрої.

Проаналізовано структуру SEP, а також компоненти його архітектури, завдяки яким забезпечується надійний рівень захисту.

Визначено основні вбудовані технології, що має та застосовує SEP для захисту кінцевих точок на різних етапах зловмисного втручання.

3 РОЗРОБЛЕННЯ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК НА БАЗІ РІШЕННЯ SYMANTEC ENDPOINT PROTECTION

3.1. Технологія забезпечення захисту кінцевих точок на базі Symantec Endpoint Protection

Для початку роботи з SEP, проводимо його інсталяцію. Для цього завантажуємо з офіційного веб-сайту Symantec (зараз Broadcom) інсталяційний архів та проводимо інтуїтивно-зрозумілу інсталяцію клієнта на комп'ютер. Після успішного встановлення переходимо до роботи з SEP.

У першу чергу, застосовуємо модуль LiveUpdate для оновлення вмісту та забезпечення надійності захисту кінцевої точки від нових типів зловмисних атак (рис. 3.1.). LiveUpdate завантажує нові файли описів вірусів для захисту від вірусів та програм-шпигунів, та файли описів IPS для захисту від мережевих загроз. LiveUpdate також може, в міру потреби, надавати удосконалення для встановленого клієнта. Ці вдосконалення, як правило, випускаються для покращення сумісності з ОС та АЗ, підвищення швидкодії або виправлення помилок.

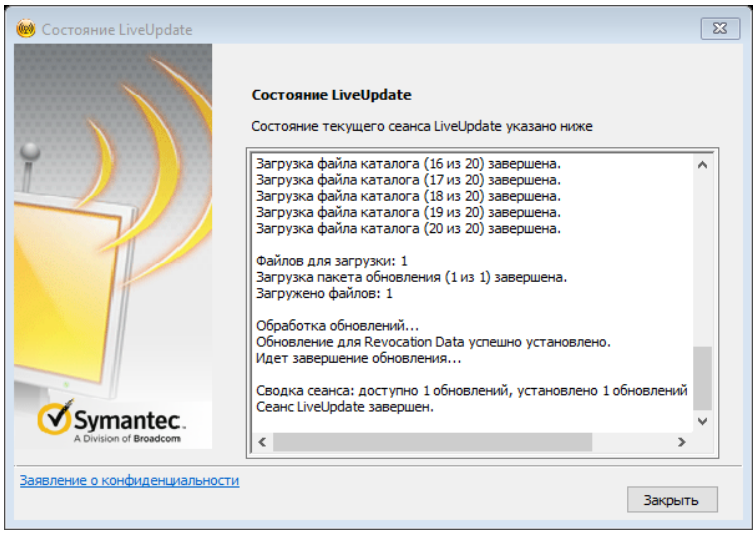

Рис. 3.1. Застосування модулю LiveUpdate

Після успішного оновлення розберемося з можливостями, що надає SEP, по його вкладках.

Вкладка «Стан»

На даній вкладці показується попередній стан кінцевого пристрою (у даному випадку комп'ютера), а також вбудовані компоненти для захисту (рис. 3.2.), такі як: захист від вірусів та програм-шпигунів, превентивний захист від загроз, попередження наслідкам використання експлойтів мережі та хоста, перенаправлення мережевого трафіку. Додаткові компоненти будуть розглянуті трохи далі.

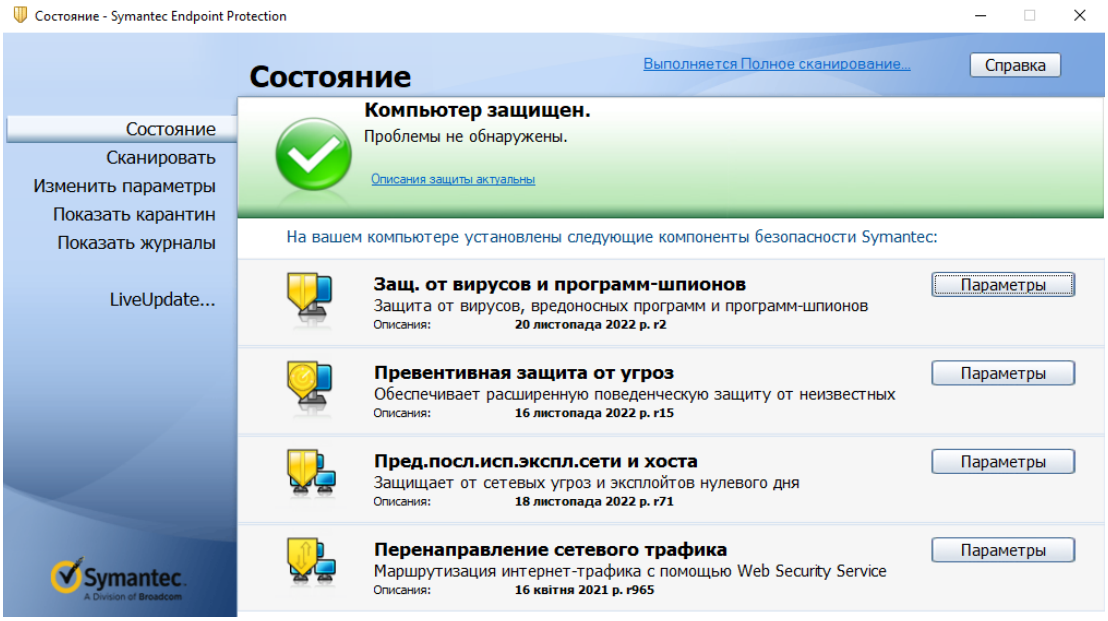

Рис. 3.2. Структура вкладки «Стан»

Захист від вірусів та програм-шпигунів

Згідно з назви, даний компонент надає захист від вірусів, інших зловмисних програм та програм-вимагачів. У параметрах дозволяється запустити сканування, змінити параметри та показати журнали (розглянемо далі у вкладці «Змінити параметри» та «Показати журнали»), а також отримати статистику сканування автоматичним захистом (рис. 3.3.), згідно якої на даному пристрої не було знайдено загроз, проте це буде перевірено згодом шляхом сканування.

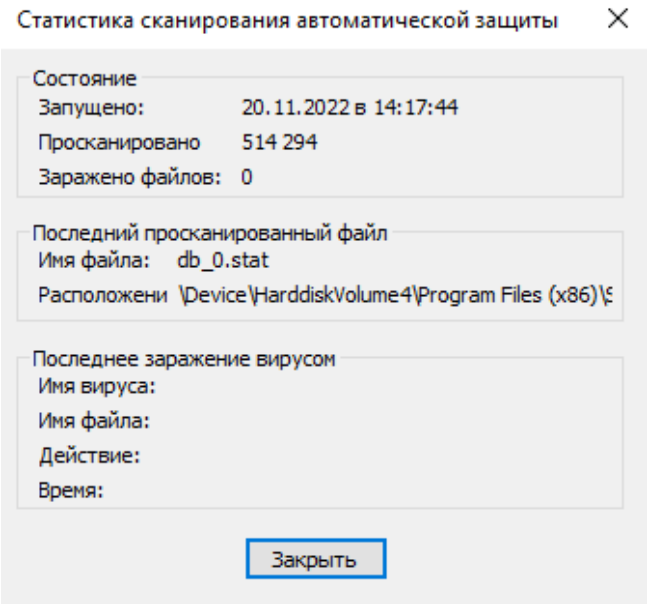

Рис. 3.3. Статистика сканування авто-захистом

Превентивний захист від загроз

Даний компонент забезпечує розширений поведінковий захист від невідомих загроз. У параметрах дозволяється змінити параметри та показати журнали, що зробимо далі.

Попередження наслідкам використання експлойтів мережі та хоста

Цей модуль відповідає за захист від мережевих загроз та експлойтів нульового дня. У параметрах дозволяється проводити зміну налаштувань, що зробимо пізніше. Проте тут доступне вікно «Мережеві операції» (візуально схоже на Диспетчер задач), яке дає змогу переглянути, дозволити або заблокувати програми та служби, які працюють на клієнті та з'єднуються з мережею (рис. 3.4.).

Рис. 3.4. Структура вікна мережевих операцій

Вікно дозволяє проаналізувати об’єм вхідного та вихідного трафіку, динамічні дані щодо цього трафіку за останні дві хвилини. Тут зелений колір показує дозволений трафік, а червоний заблокований. Також тут розташовано графік хронології атак, що показує кількість атак на комп’ютер. Панель запущених додатків містить список усіх запущених додатків та служб, які звертаються на даний момент до мережі. Їх можна перервати або заблокувати, а також додати їм можливість запускатися після запиту.

Також даний компонент містить можливість налаштувати правила брандмауера (рис. 3.5.). За допомогою цього діалогового вікна можна додати, змінити, активувати, видалити та перевпорядкувати створені правила брандмауера. Брандмауер автоматично перевіряє весь вхідний та вихідний трафік на відповідність цим правилам та дозволяє або блокує трафік згідно з правилами. Кожне правило визначає умови, при дотриманні яких воно повинно застосовуватися, а також дію правила. До умов включаються призначені програми, порти та протоколи, а також хости та призначені періоди часу.

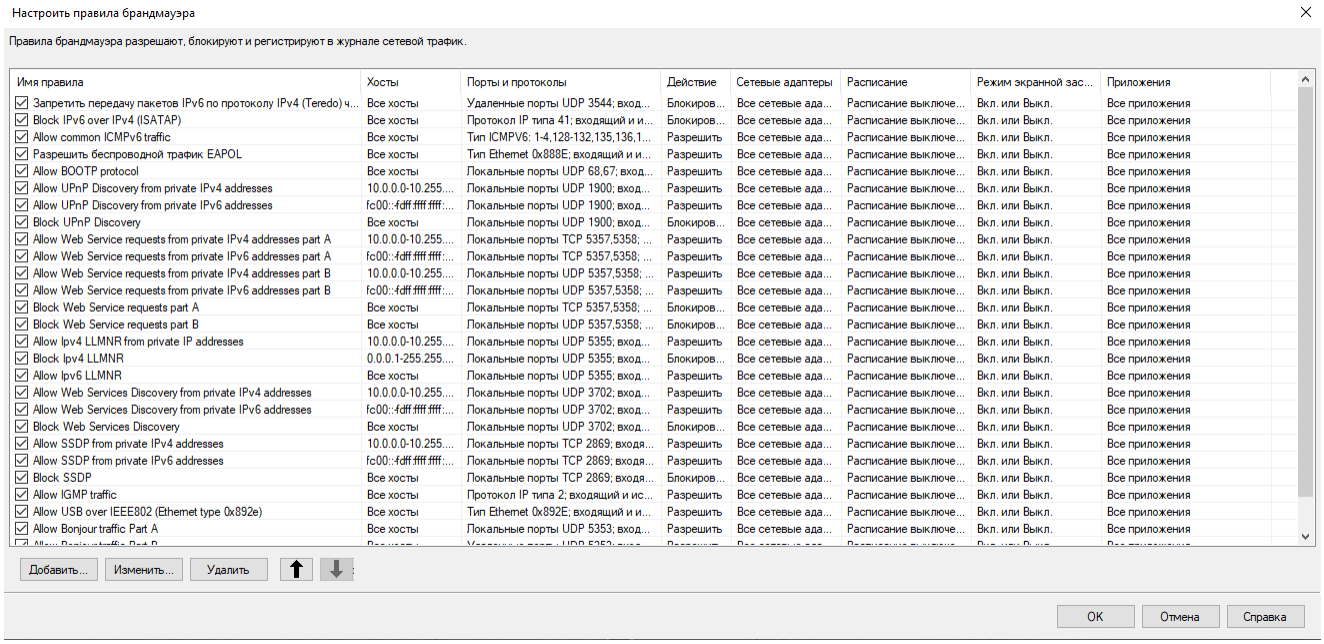

Рис. 3.5. Вікно правил брандмауера

Правила брандмауера обробляються послідовно, від найвищого до нижчого пріоритету у списку правил. Якщо у першому правилі не зазначено, як має оброблятися пакет, то перевіряється наступне друге правило. Обробка правил продовжується до виявлення першого збігу. Після виявлення відповідного правила брандмауер виконує вказану в ньому дію. Усі наступні правила з нижчим пріоритетом ігноруються. Наприклад, якщо на початку списку вказано правило, яке блокує весь трафік, за яким слідує правило, яке дозволяє весь трафік, то клієнт все ж таки заблокує весь трафік.

Правила впорядковуються відповідно до рівня конкретності. І тут першими перевіряються найсуворіші, а вкінці — найзагальніші правила. Наприклад, правила, які блокують трафік, повинні бути розташовані у верхній частині списку правил. Правила, розташовані далі за списком, можуть дозволяти трафік.

Для відстеження поточних з'єднань захист брандмауера використовує функцію перевірки з урахуванням стану. Функція перевірки з урахуванням стану відслідковує вихідні та цільові IP-адреси, порти, додатки та іншу інформацію про з'єднання. Перед обробкою правил брандмауера клієнт приймає рішення щодо передачі трафіку з огляду на інформацію про з'єднання. Наприклад, якщо правило брандмауера дозволяє комп'ютеру підключатися до веб-сервера, то брандмауер

збереже інформацію про таке з'єднання. Отримавши відповідь сервера, брандмауер виявить, що відповідь веб-сервера комп'ютера очікується. Він дозволить трафік веб-сервера у відповідь на вихідний запит комп'ютера без перевірки бази правил. Правило повинно дозволити початковий вихідний трафік до реєстрації підключення до брандмауера [16].

Перевірка з урахуванням стану усуває необхідність створення нових правил. Якщо трафік передається в одному напрямку, то не слід створювати правила, які дозволяють трафік в обох напрямках. Функція перевірки з урахуванням стану автоматично дозволить зворотній трафік у відповідь на вихідний трафік. Оскільки принцип дії брандмауера ґрунтується на обліку стану, необхідно створювати лише ті правила, що встановлюють з'єднання, а не характеристики конкретних пакетів.

До складу клієнта SEP входять стандартні правила брандмауера для захисту комп'ютера. При цьому, для забезпечення додаткового захисту, все ж таки можна змінити ці правила брандмауера або додати нові. У політиці має бути хоча б одне правило. Проте кількість правил не обмежується. У міру потреби правила можна вмикати та вимикати. Наприклад, можливо, потрібно вимкнути правило на час усунення несправностей, а потім знову включити його.

Тепер створюємо нове правило для брандмауера, як показано на рис. 3.6.

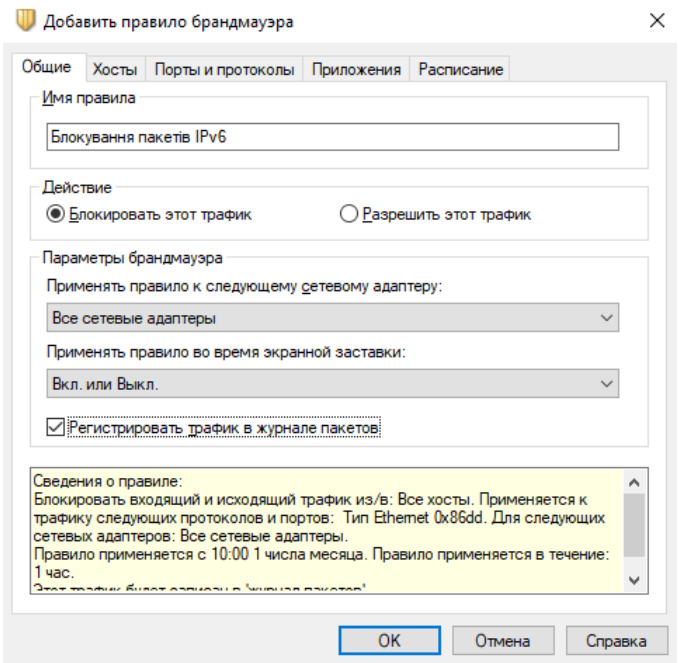

Рис. 3.6. Створення правила брандмауера

У діалоговому вікні «Загальні»:

- Прописується назва правила, яка повинна його максимально точно описувати для полегшення його подальшого використання.
- Обирається варіант його дії щодо трафіку.
- Обирається його дія щодо мережевих адаптерів.
- Дозволяємо або ні регіструвати трафік в журналі пакетів.

У діалоговому вікні «Хости»: налаштовуються параметри хоста, де задається джерело трафіку, для якого буде діяти дане правило. Наприклад, можна дозволити трафік лише із комп'ютерів, IP-адреси яких входять до окремого діапазону.

У діалоговому вікні «Порти та протоколи»: визначаємо мережеву службу, для якої призначено правило брандмауера. Для цього потрібно вказати протокол, порт та напрямок передачі трафіку.

У діалоговому вікні «Програми»: вказується програма, для якої буде діяти правило брандмауера. Додаються усі програми, які використовують мережеве з'єднання або які мають часто виконуватися.

У діалоговому вікні «Розклад»: вказується, у який час повинне чи не повинне застосовуватися дане правило. Наприклад, правило можна вимкнути на час інсталяції програм.

На цьому процес створення, редагування та впровадження правил завершується.

Перенаправлення мережевого трафіку

Компонент дозволяє перенаправити мережевий трафік від клієнта SEP до Служби веб-безпеки Symantec (WSS), яка пропускає або блокує трафік відповідно до правил, які встановлює адміністратор WSS. Безпечне підключення до Служби веб-безпеки Symantec дозволяє клієнту здійснювати фільтрацію вмісту та захист від загроз для всіх мережевих взаємодій.

Даний компонент використовує наступні способи перенаправлення:

- У спосіб PAC-файл на WSS перенаправляється лише веб-трафік за допомогою файлу автоматичної конфігурації проксі (PAC). WSS забезпечує

безпечні параметри проксі для веб-браузерів. На WSS перенаправляється лише веб-трафік. Щоразу, при переході на веб-сайт за допомогою веб-браузера, останній відправляє весь трафік веб-браузера через найближчу службу WSS, визначену у файлі PAC. В залежності від попередньо заданої конфігурації проксі-сервер Symantec WSS може перенаправляти, дозволяти або блокувати трафік [16].

- У способі тунель WSS через VPN перенаправляється весь мережевий трафік для перевірки. Відразу після встановлення клієнт SEP підключається до VPN, який перенаправляє весь мережевий трафік через проксі-сервер Symantec WSS. Тунель VPN налаштовується таким чином, що він завжди увімкнений та автоматично відновлює підключення у разі відключення через перезавантаження системи або переходу в режим сну.

Застосування наступної вкладки «Сканувати» проведемо після налаштування або зміни параметрів у вкладці «Змінити параметри».

Вкладка «Змінити параметри»

У даній вкладці налаштовуються параметри, розглянутих раніше, компонентів, а також додаються виключення, як показано на рис. 3.7.

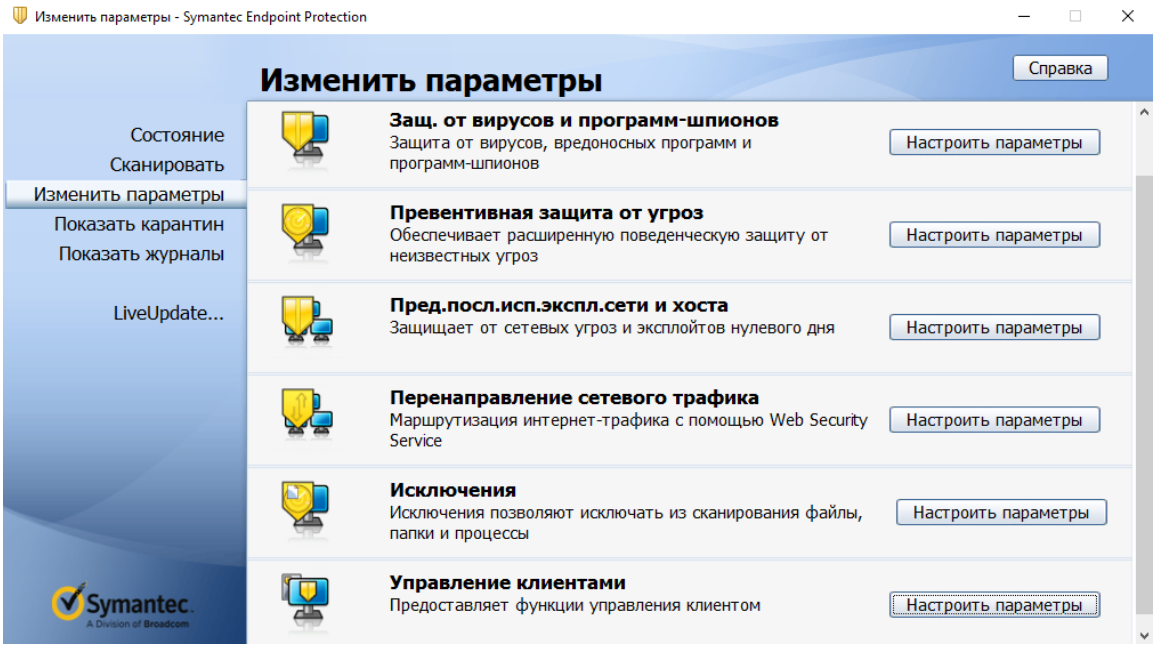

Рис. 3.7. Структура вкладки «Змінити параметри»

Проаналізуємо налаштування параметрів більш детально.

У компоненті «Захист від вірусів та програм-шпигунів» доступні такі налаштування:

- *Глобальні налаштування*

Тут налаштовуються параметри сканування. Для цього можна та слід ввімкнути компонент Insight, який дозволяє пропускати під час сканування файли з цифровим підписом та надійні файли. Тут же налаштовується рівень надійності, який використовується Insight під час використання даних про репутацію для пропуску файлів.

Також тут дозволяється увімкнути евристичне виявлення вірусів технологією Bloodhound, яка ізолює логічні області файлів для виявлення значної частини невідомих вірусів. При виявленні підозрілих дій клієнт не дозволить їх продовжувати. Тут же задається один із наступних рівнів виявлення: автоматичний (за замовчуванням) або агресивний (збільшує чутливість автоматичного виявлення технологією). Інші параметри налаштувань показано на рис. 3.8.

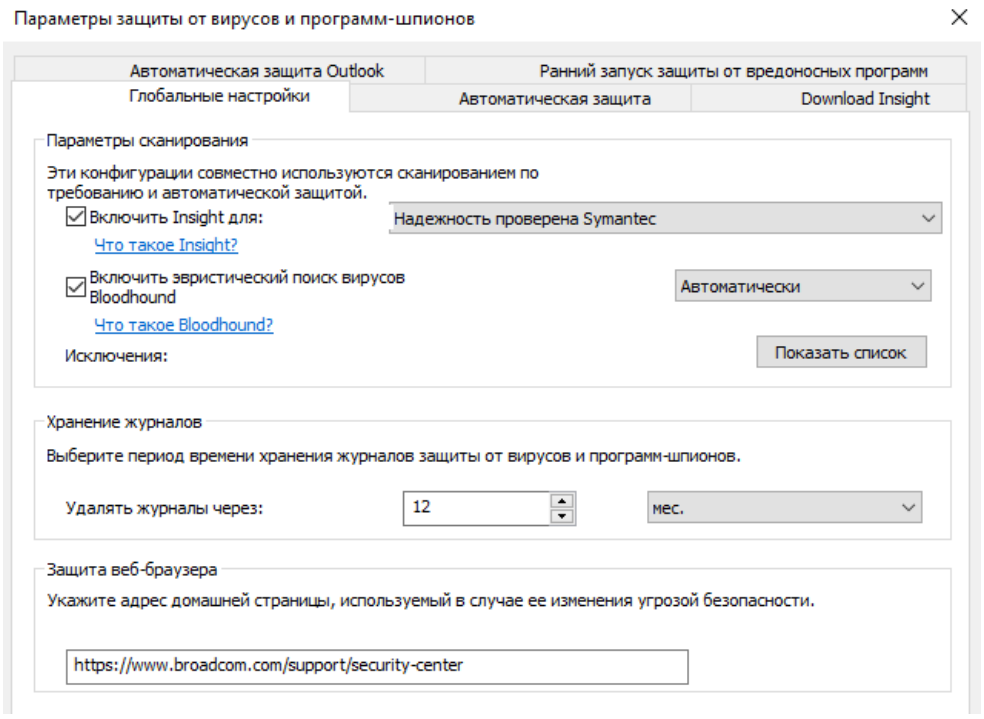

Рис. 3.8. Глобальні налаштування

- *Автоматичний захист*

Дана функція забезпечує постійний захист файлів комп’ютера. При кожному збереженні, копіюванні, переміщенні, відкритті/закритті файлу вона перевіряє його

на наявність вірусів та загроз безпеки. Проте, при її вмиканні компонент Download Insight перестає функціонувати, навіть якщо він був увімкнений.

Тут також обираються типи та розширення файлів, що підлягають скануванню авто-захистом, а також інші параметри, як показано на рис. 3.9.

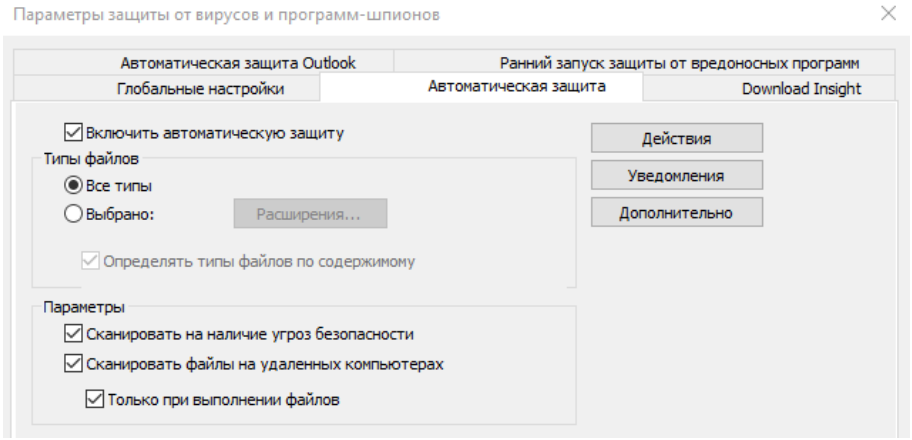

Рис. 3.9. Налаштування параметрів авто-захисту

Проте тут, через кнопку «Дії», налаштовуються дії, що будуть виконуватися при виявленні певного зловмисного ПЗ або загроз безпеці, як на рис. 3.10.

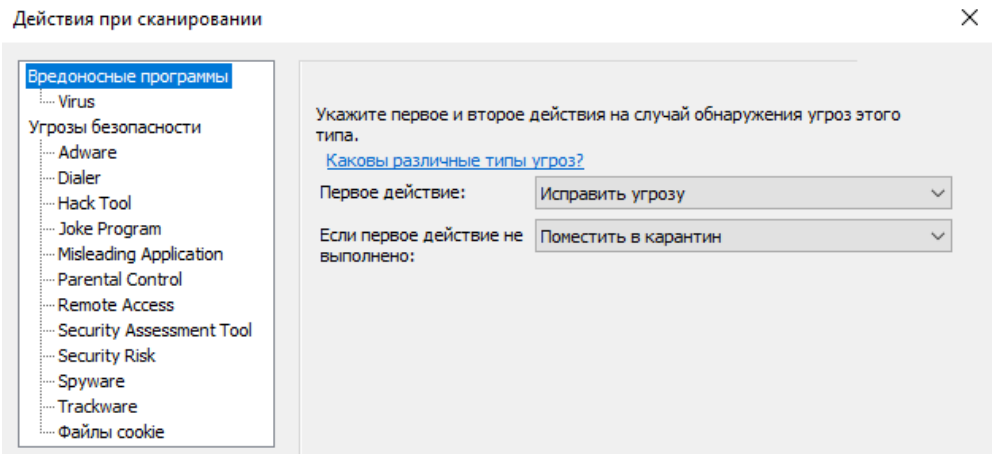

Рис. 3.10. Налаштування дії при виявленні певного зловмисного ПЗ

Через кнопку «Сповіщення» дозволяється/забороняється показувати вікно результатів авто-захисту та текст при виявленні підозрілого, як на рис. 3.11.

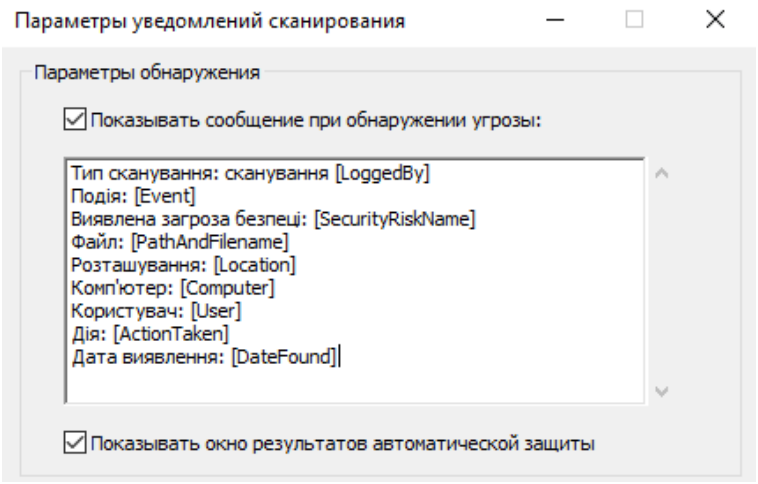

Рис. 3.11. Налаштування параметрів сповіщення

За допомогою кнопки «Додатково» налаштовуються додаткові параметри авто-захисту, а саме: у яких випадках необхідно перезавантажувати авто-захист, коли саме сканувати файли, чи завжди видаляти нові заражені файли, кеш файлів, трасувальник загроз (ідентифікує IP-адреси, з яких здійснюються атаки, але не блокує їх), повторна активація через певний період часу, як показано на рис. 3.12.

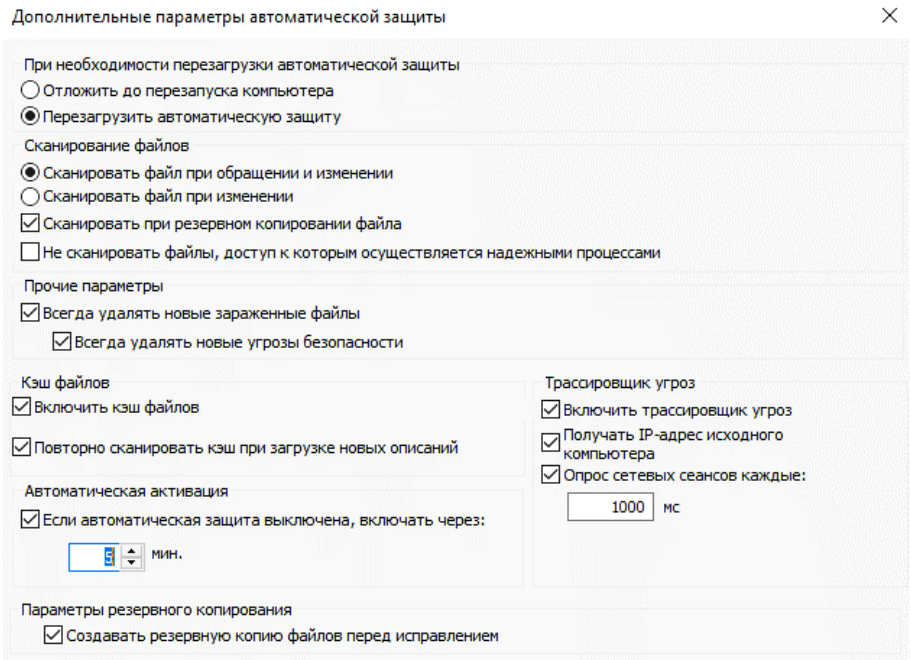

Рис. 3.12. Налаштування додаткових параметрів авто-захисту

- *Download Insight*

Цей компонент виявляє шкідливі та потенційно шкідливі файли під час спроби завантажити їх браузером або клієнтом обміну текстовими

повідомленнями. Налаштування даного компоненту проводиться для виявлення потенційних загроз на основі репутації файлів. Також тут встановлюється рівень чутливості при виявленні підозрілих файлів (чим вище рівень, тим більше виявляється файлів, проте зростає кількість помилкових спрацьовувань), а також інші налаштування, як показано на рис. 3.13.

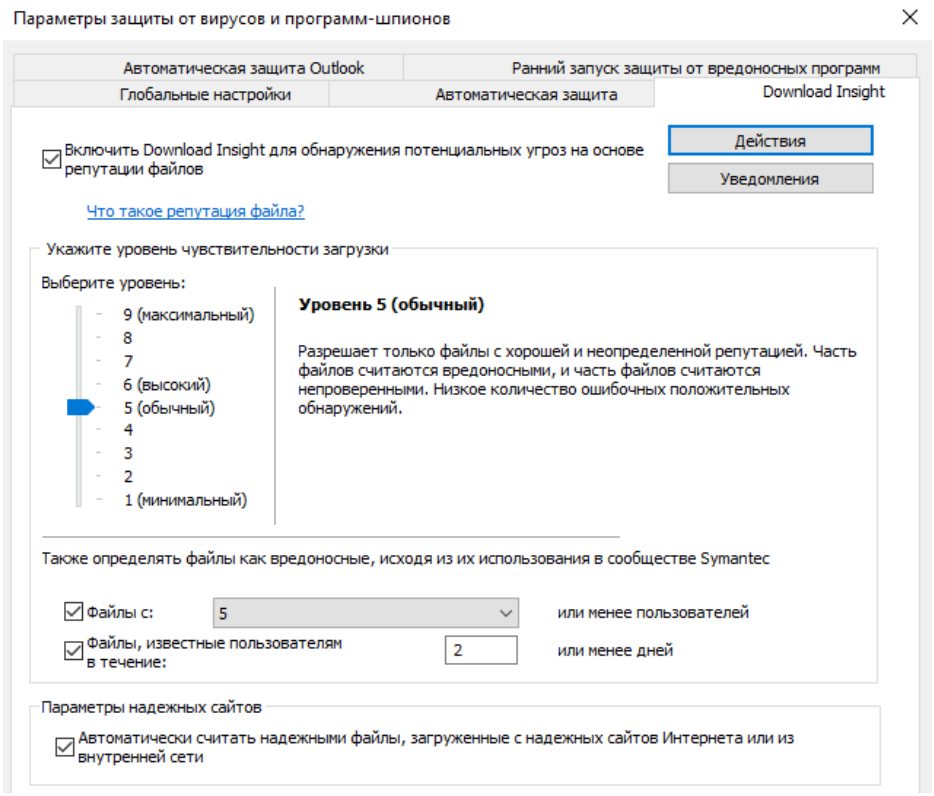

Рис. 3.13. Налаштування Download Insight

Тут же налаштовується дія Download Insight при виявленні зловмисних або неперевірених файлів, як на рис. 3.14.

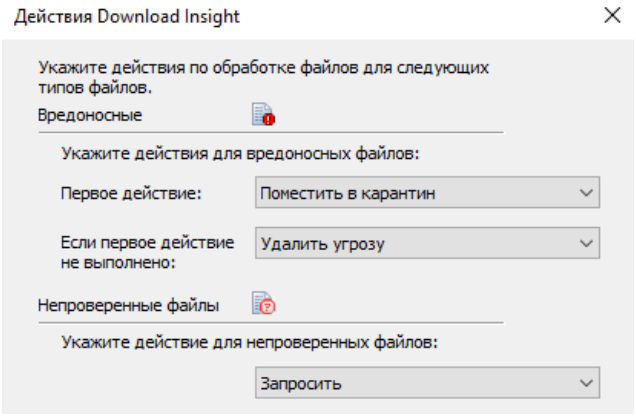

Рис. 3.14. Налаштування дії Download Insight при виявленні

- *Автоматичний захист Microsoft Outlook*

Дана функція дозволяє сканувати вкладення повідомлень Microsoft Outlook. Тут так само є варіація ввімкнути/вимкнути функцію, налаштувати типи файлів, що скануватимуться, дії та повідомлення при виявленні зловмисних файлів в Outlook, як на рис. 3.15. Також дозволяється додати функцію надсилання повідомлення-попередження відправнику, що у його вкладенні міститься зловмисний файл.

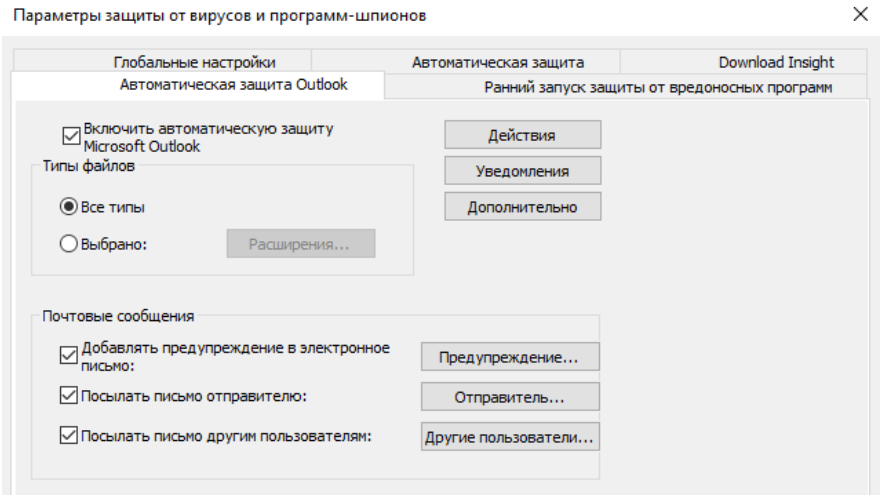

Рис. 3.15. Налаштування авто-захисту Outlook

- *Ранній запуск захисту від зловмисних програм*

SEP містить драйвер раннього запуску захисту від шкідливих програм (ELAM), який працює спільно з драйвером Microsoft ELAM та захищає комп'ютери в мережі під час їх запуску до ініціалізації драйверів інших виробників (рис. 3.16.).

При виявленні потенційно-небезпечного драйвера SEP налаштовується так, щоб повідомляти Windows про неблагонадійні драйвери як про невідомі. SEP вносить виявлення в журнал як неблагонадійний драйвер, а потім Windows використовує дію, передбачену політикою для невідомих драйверів.

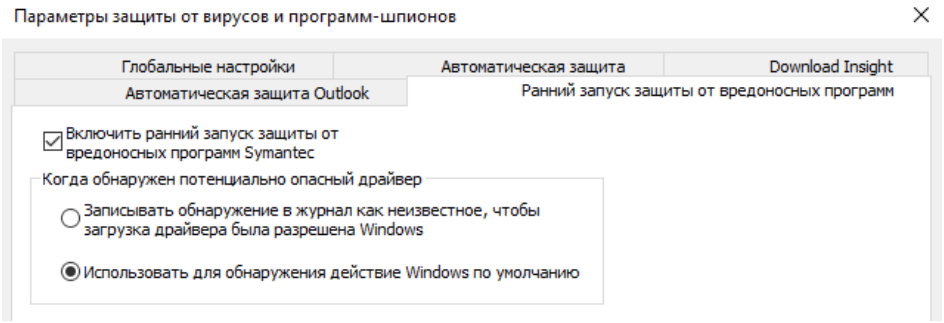

Рис. 3.16. Налаштування раннього запуску захисту

Далі проводимо налаштування параметрів у компоненті «Превентивний захист від загроз». Тут проводимо наступні налаштування:

- *SONAR*

Тут обов’язково вмикаємо модуль SONAR, який відповідає за захист у реальному часі та виявляє потенційно шкідливі програми під час їх запуску на комп'ютері з використанням евристичних методів та даних про репутацію. Тут же вказуємо дії, які будуть виконуватися, якщо SONAR виявить загрозу високого та низького ступеня ризику, як на рис. 3.17.

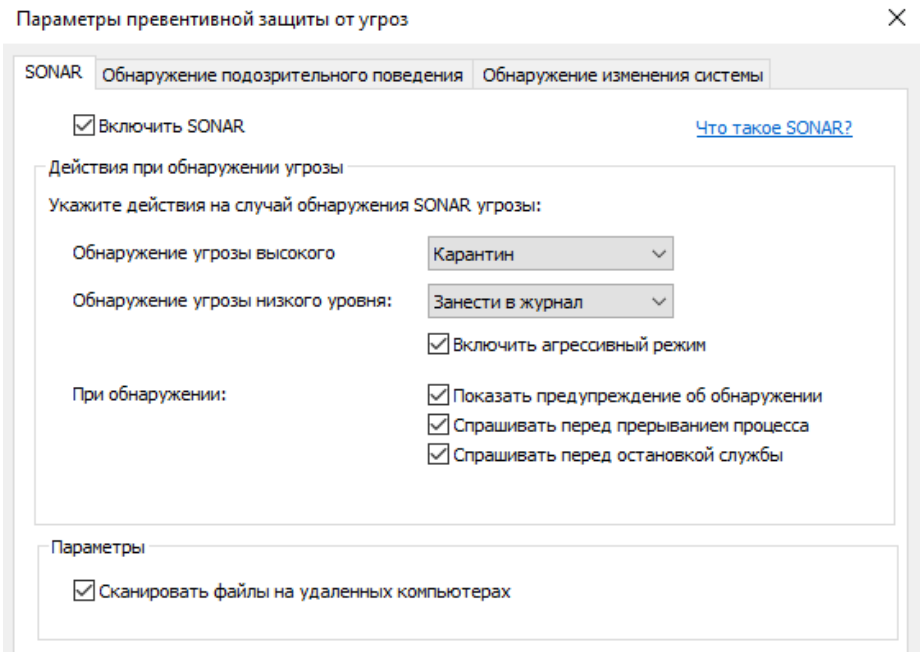

Рис. 3.17. Налаштування модулю SONAR

- *Виявлення підозрілої поведінки*

Дане вікно використовується для налаштування дій, що виконуються модулем SONAR при виявленні надійної програми з підозрілою поведінкою. Наприклад, надійна програма може намагатися створити виконувані файли, або завантажити ненадійний драйвер. Тут налаштовуємо дію, що виконуватиметься SONAR-ом при виявленні підозрілої поведінки високого та низького ступеня ризику у програмі (рис. 3.18.).

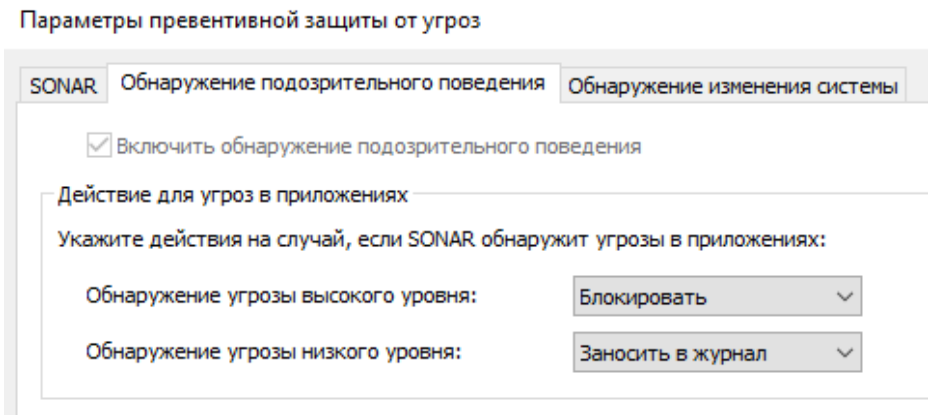

Рис. 3.18. Налаштування виявлення підозрілої поведінки

- *Виявлення змін системи*

У даному вікні налаштовуємо поведінку модулю SONAR при виявленні змін у DNS або файлу hosts. Проте важливо, що SONAR не робить жодних дій, якщо об'єкт намагається відкрити файл хоста або отримати доступ до нього. SONAR діє тільки у тому випадку, коли об'єкт, наприклад браузер, змінює файл хоста.

У вікні налаштувань вказуємо дії на випадок, якщо модуль SONAR виявить будь-які зміни у DNS та окремо файлу hosts. Обираємо дію «Запитати», щоб мати змогу самостійно дозволяти або блокувати зміни (рис. 3.19.), оскільки, якщо блокувати зміни DNS, то можливе блокування доступу до, наприклад, клієнта VPN, а якщо блокувати зміну файлу hosts, то можуть виявитися заблокованими програми, які потребують доступу до файлу hosts.

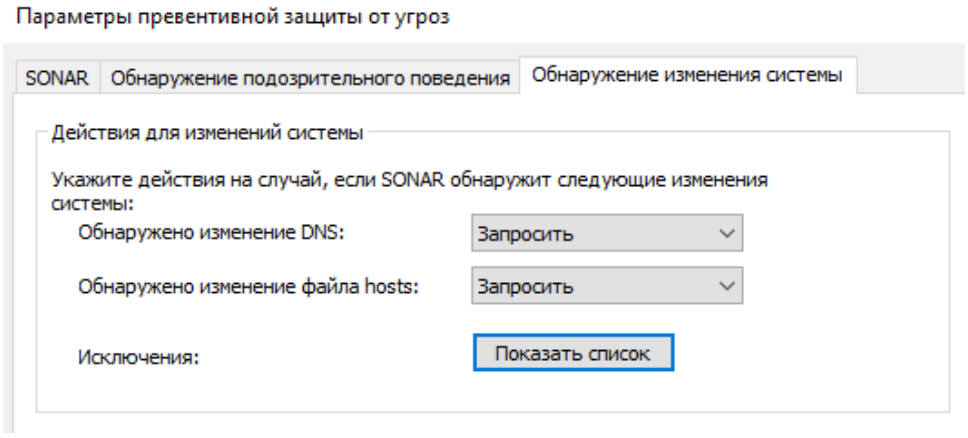

Рис. 3.19. Налаштування параметрів виявлення змін у системі

Тепер проводимо налаштування параметрів попередження наслідків використання експлойтів мережі та хоста. Тут робимо наступні налаштування:

- *Брандмауер*

Що являє собою брандмауер, як він функціонує та його правила було проаналізовано трохи вище. Тепер проведемо загальні налаштування його параметрів.

У даному вікні, окрім увімкнення брандмауера, вмикаємо вбудовані правила, які забезпечують захист від атак з мережі на DHCP, WINS та DNS. Також налаштовуємо параметри трафіку, параметри трафіку IP, для якого не знайдено жодного правила, параметри часу активної відповіді та параметри прихованого режиму, як на рис. 3.20.

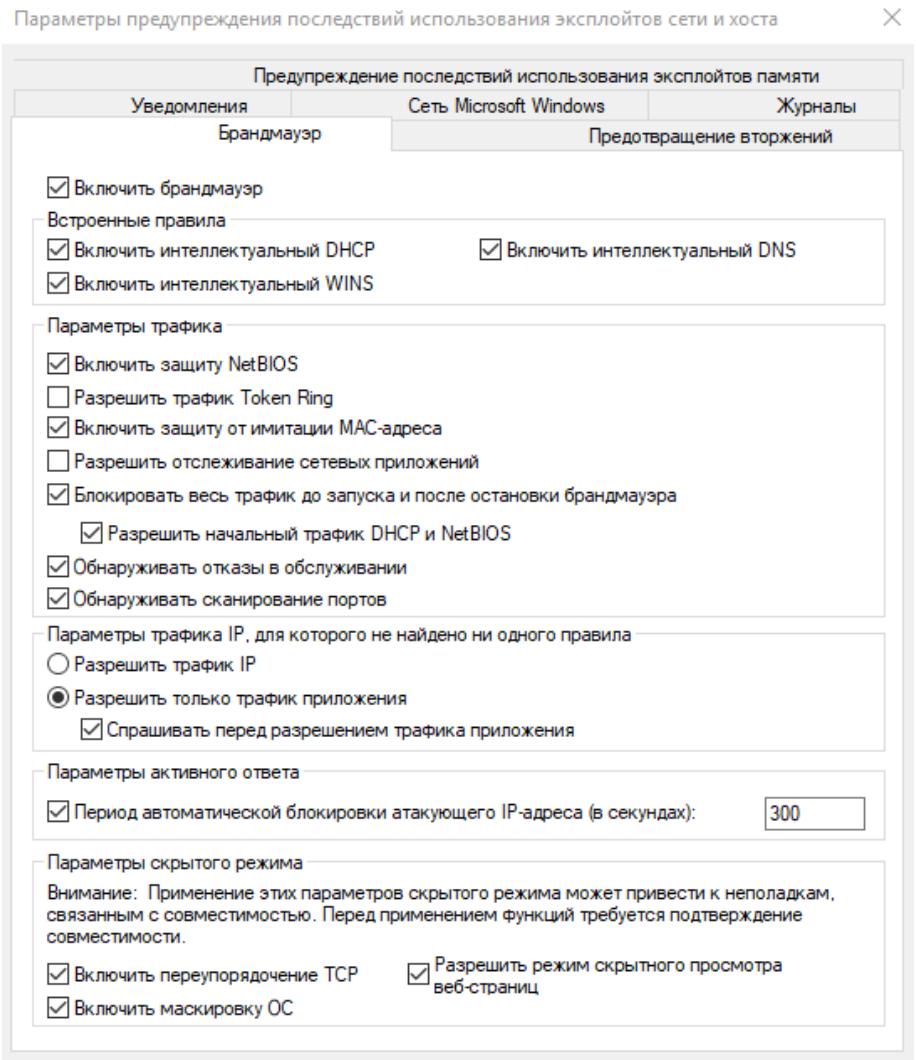

Рис. 3.20. Загальні налаштування параметрів брандмауера

- *Запобігання наслідкам використання експлойтів пам'яті*

У даному вікні тільки вмикаємо модуль запобігання наслідкам використання експлойтів пам'яті, який допомагає захистити ПЗ від використання його уразливостей. Для виявлення спроб використання експлойтів використовуються різноманітні методи. Деякі з них блокують експлойт, а інші завершують роботу уразливої програми.

- *Запобігання вторгнень*

Налаштування параметрів у даному вікні допомагає виявити загрози та захистити клієнта від атак, відповідних відомим шаблонам вторгнення (рис. 3.21.). Тут вмикаємо систему запобігання вторгненням для мережі, яка застосовує мережеві IPS-сигнатури та виключення для IPS-сигнатур до вхідного та вихідного трафіку клієнта. Також систему для браузера, яка порівнює сигнатури браузера з вхідним та вихідним трафіком браузерів. Наостанок вмикаємо службу репутації URL, яка визначає загрози від доменів та URL-адрес, де може знаходитися шкідливий контент та блокує доступ до веб-адрес, які відомі як джерела шкідливого контенту.

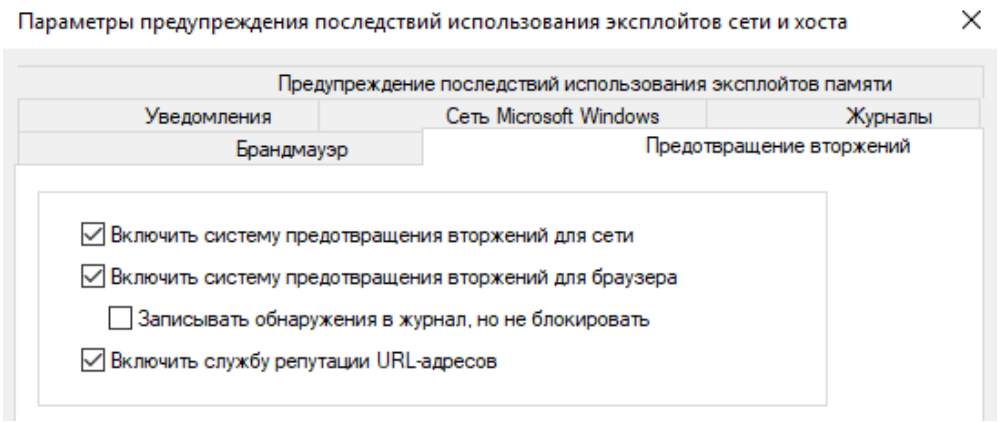

Рис. 3.21. Налаштування параметрів запобігання вторгнень

- *Сповіщення*

У цьому діалоговому вікні вмикаємо відображення сповіщень щодо попередження вторгнень та використання експлойтів пам’яті, як на рис. 3.22.

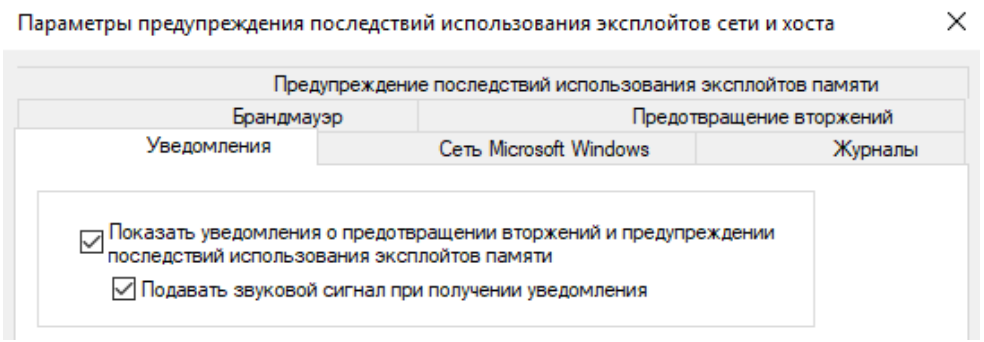

Рис. 3.22. Налаштування сповіщення

- *Журнали*

У даному вікні налаштовуємо журнал безпеки, системний журнал, журнал трафіку, журнал керування та додаємо журнал пакетів (рис. 3.23.). Для кожного журналу вказуємо його розмір (від 64 КБ до 15 МБ) та термін зберігання записів у днях. За необхідності, дозволяється очистити ці журнали.

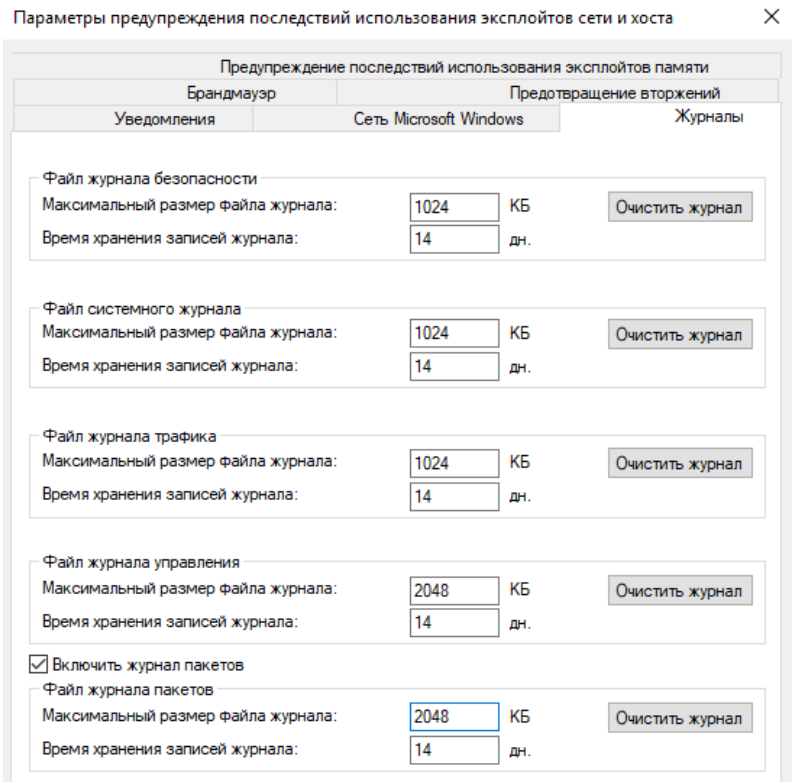

Рис. 3.23. Налаштування журналів

Переходимо до налаштування компоненту «*Виключення*».

Тут є можливість, за необхідності, виключити зі сканування відомі загрози, файли, папки, розширення, веб-домен та процеси. Наприклад, може знадобитися

виключити файл, у безпеці якого вже впевнені. Виключення файлу з процедури сканування, як правило, підвищує продуктивність цього процесу.

Успішне додавання виключень загроз безпеці, SONAR, змін DNS чи файлу хоста для файлів, розширень, програм показано на рис. 3.24.

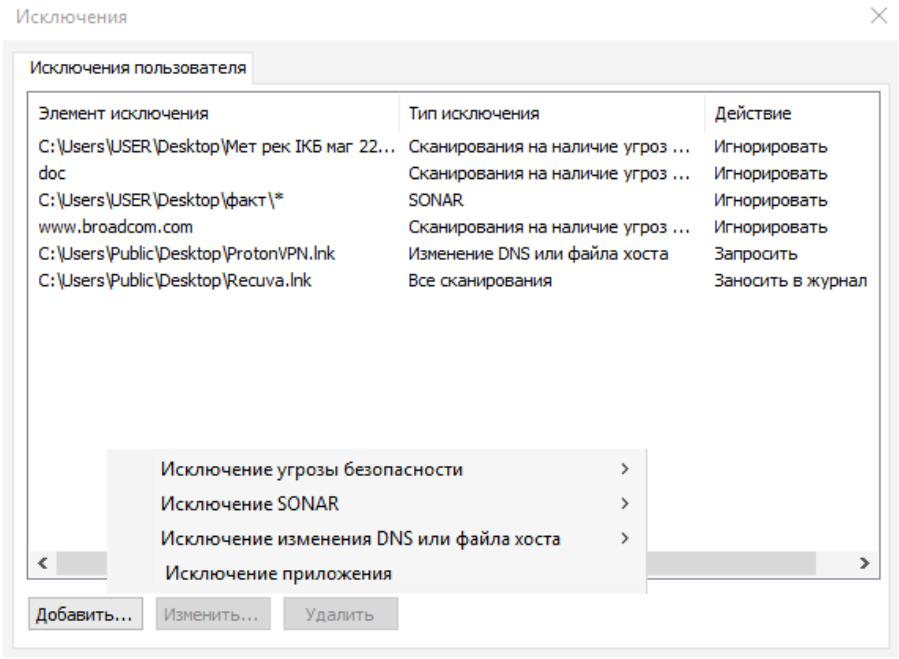

Рис. 3.24. Додавання виключень зі сканувань

Останнім налаштуванням є параметри у модулі «*Керування клієнтами*».

У вікні «Загальні» дозволяємо відображення сповіщень щодо роботи SEP та виявлення критичних попереджень. Також тут вмикаємо керування програмами та пристроями. Керування програмами захищає комп'ютер, контролюючи поведінку програм на клієнтському комп'ютері. Керування пристроями дозволяє захистити комп'ютер від пристроїв, які можуть підключатися до комп'ютера, таких як USB-пристрої.

У вікні «Захист від змін» вмикаємо функцію захисту продукта SEP, яка блокує та заносить у журнал усі спроби змінити процеси Symantec або внутрішні об'єкти, які відповідають за синхронізацію потоків та процесів Symantec.

У вікні «LiveUpdate» вказуємо, коли та як виконувати оновлення вмісту, наприклад описів вірусів та сигнатур IPS, як на рис. 3.25.

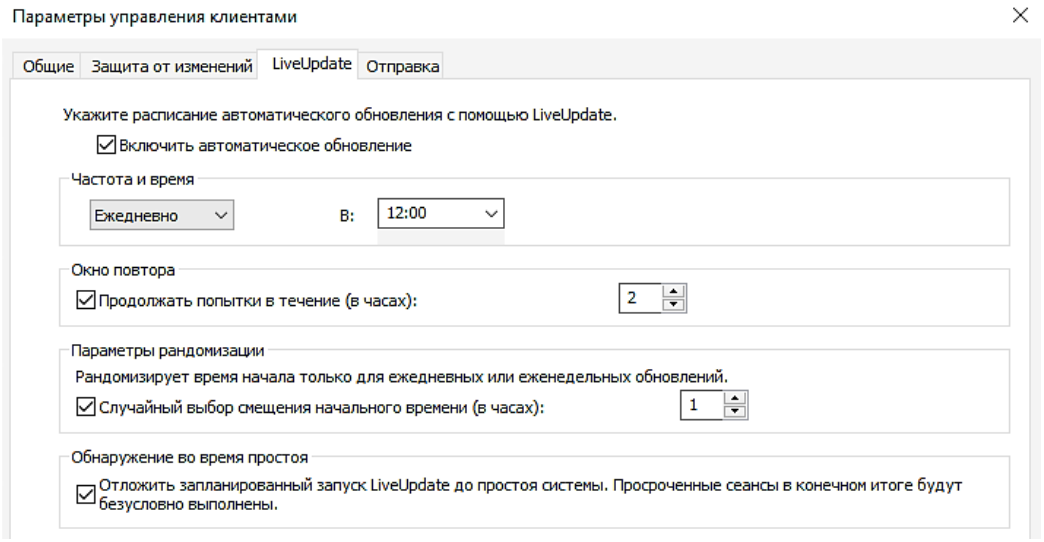

Рис. 3.25. Налаштування роботи компоненту LiveUpdate

У останньому вікні налаштувань «Відправка» дозволяємо відправку даних у Symantec (рис. 3.26.), що включають відомості про знайдені загрози, про мережу та конфігурацію. Symantec використовує цю інформацію для підвищення ефективності захисту за рахунок запобігання хибним спрацьовуванням та швидшого реагування на атаки шкідливого коду.

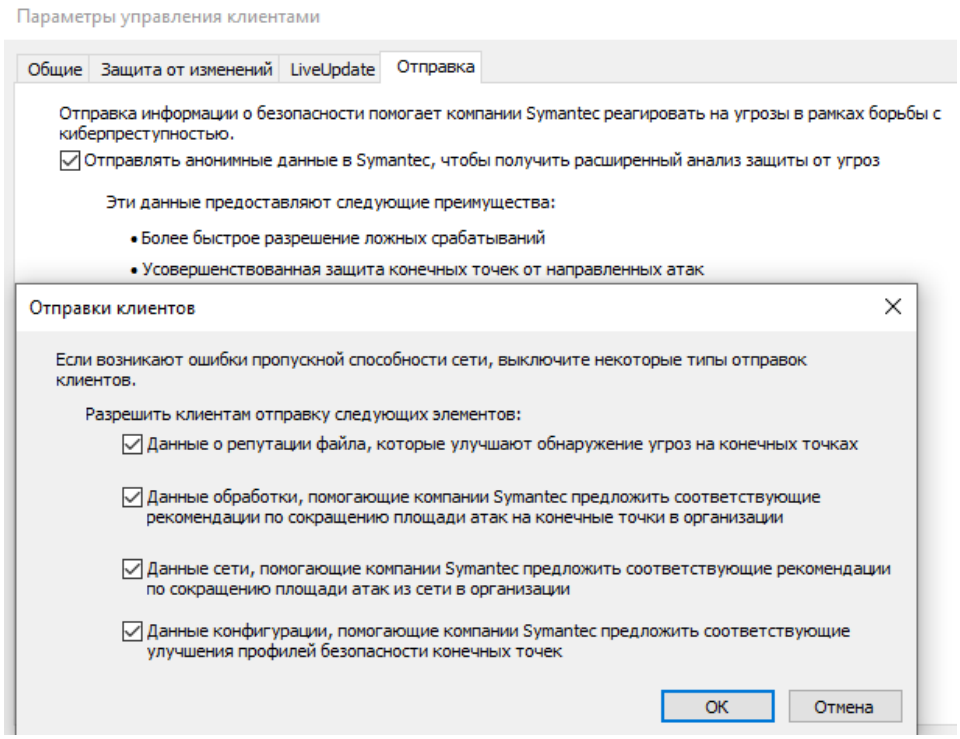

Рис. 3.26. Налаштування відправки даних у Symantec

Після проведення повного налаштування продукту, повертаємось у вкладку «Сканувати» та запускаємо «Повне сканування», оскільки воно, хоч й займає декілька годин часу, проте має найбільшу ефективність у виявленні, у порівнянні з «Активним скануванням», яке перевіряє тільки найбільш можливі місця розташування зловмисного ПЗ, яке вже може знаходитися на кінцевому комп'ютері. Далі обираємо для сканування усі типи файлів, а також встановлюємо додаткові параметри сканування, як на рис. 3.27.

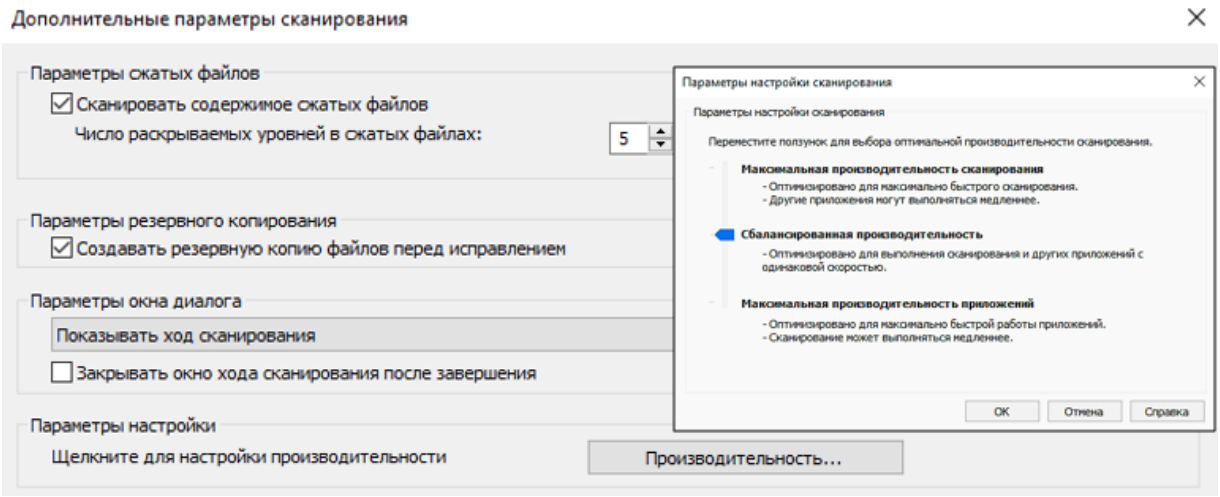

Рис. 3.27. Налаштування додаткових параметрів сканування

На завершення до підготовки сканування, даємо назву скануванню та одразу запускаємо, та чекаємо результатів. Процес повного сканування показано на рис. 3.28.

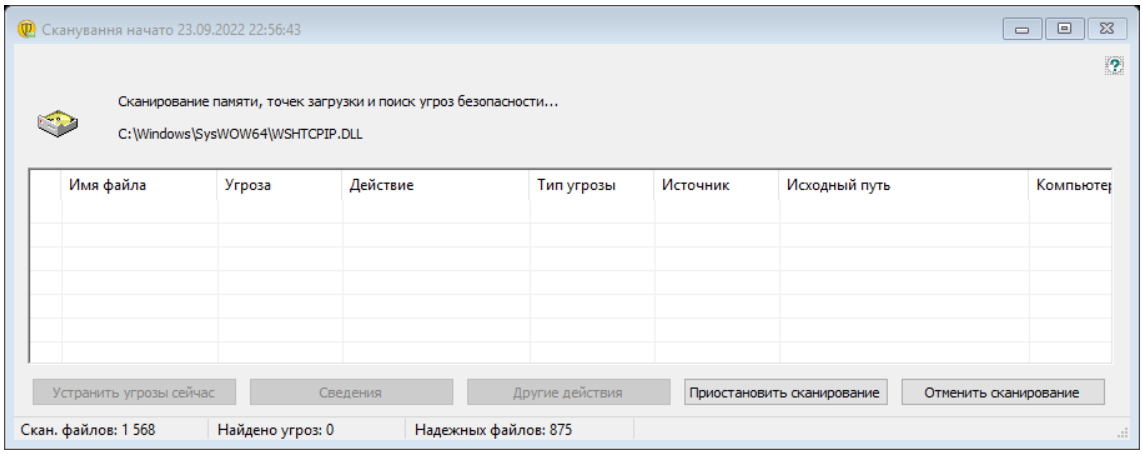

Рис. 3.28. Процес повного сканування

Процес повного сканування на даному комп’ютері зайняв близько 3-х годин. Результатом даного сканування є виявлення SEP-ом низки зловмисних файлів різних розширень, що проникли на кінцевий комп’ютер ще до інсталяції продукту. SEP намагається очистити заражений файл від виявленого вірусу, проте, якщо очистити файл не вдається, то операція сканування поміщає файл у карантин комп'ютера та зашифровує його. У карантині зловмисний файл не зможе заразити інші файли, проте буде залишатися загрозою, допоки не буде видалений. Усі виявлені зловмисні файли SEP одразу помістив у карантин, як на рис. 3.29.

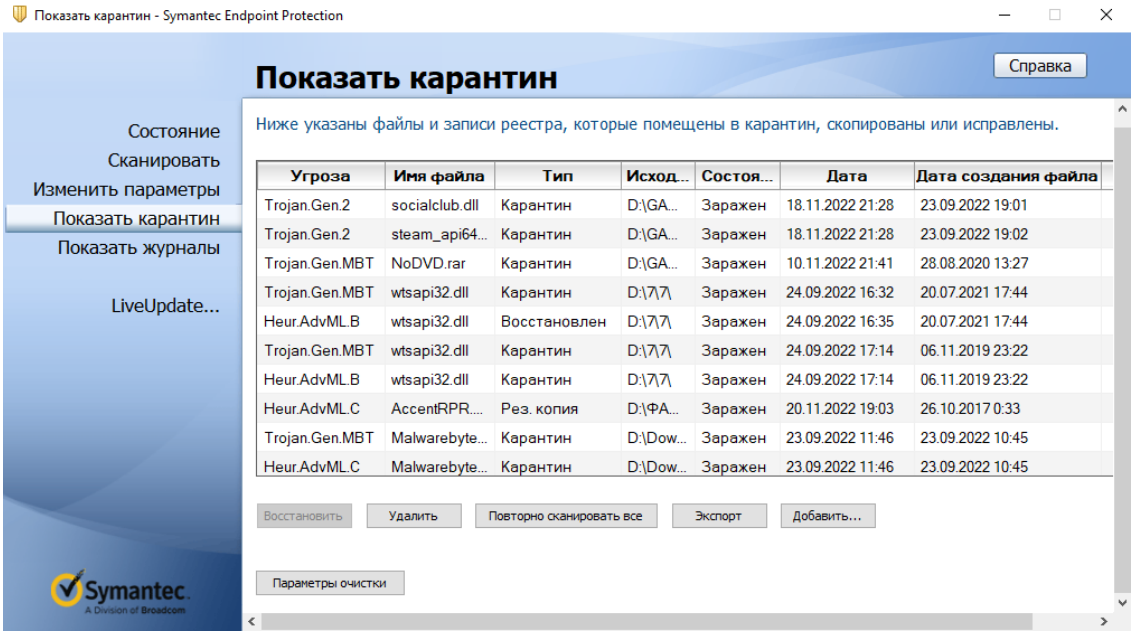

Рис. 3.29. Карантин виявлених зловмисних файлів

Результат виявлення такої кількості зловмисного ПЗ говорить про високу ефективність, та надійність алгоритмів виявлення та реагування SEP, а також про необхідність вчасного правильного налаштування параметрів безпеки та проведення регулярного сканування.

Більш детальну інформацію щодо знайденого зловмисного файлу дозволяється отримати, якщо клацнути по ньому двічі. Наприклад, при відкритті детальних даних про загрозу «Heur.AdvML.C» повідомляється, що це евристичний вірус з категорії зловмисних програм, який був завантажений з Інтернету. Також додаються дані щодо дати виявлення, його місцезнаходження, репутації та поширеності, як показано на рис. 3.30.

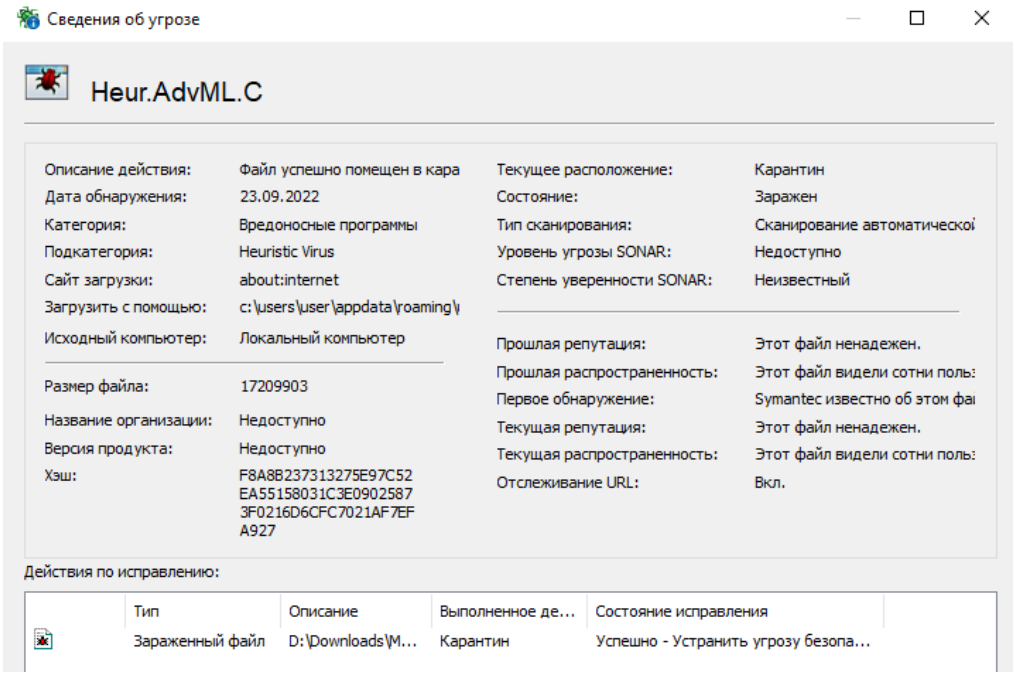

Рис. 3.30. Детальна інформація щодо одного з виявлених зловмисних файлів

Наостанок, статистична інформація надається у вкладці «Показати журнали». Тут є можливість проаналізувати інформацію у наступних журналах:

Системний журнал

У нього щодня записуються події та операції з вірусами та загрозами безпеці, пов'язані з захистом комп'ютера. Ці записи відображають зміни конфігурації, помилки, інформацію про файли описів вірусів та загроз (рис. 3.31). Відомості про заборонені адміністратором дії не зберігаються в цьому журналі.

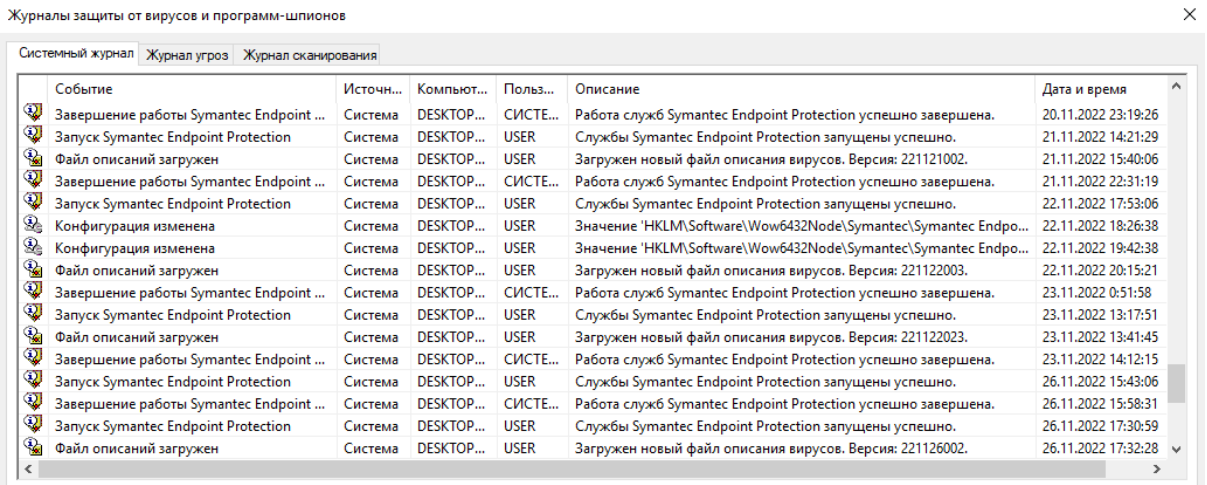

Рис. 3.31. Системний журнал

Журнал сканування

Для нього використовуються дані з системного журналу задля повного розуміння стану сеансів сканування. У журналі подаються дані щодо дат та типу проведеного сканування, кількість проаналізованих та виявлених заражених файлів, а також різновид виявленого зловмисного файлу, як на рис. 3.32.

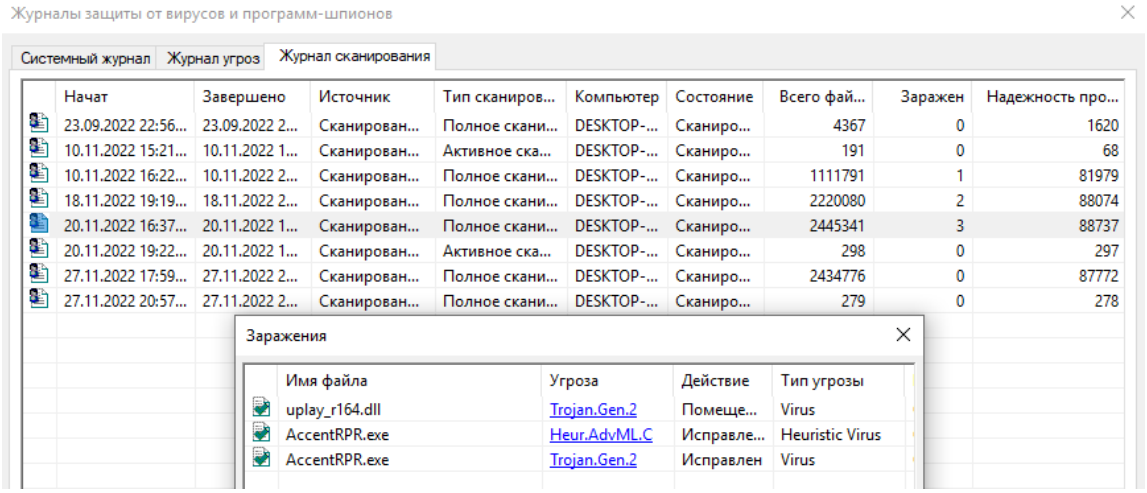

Рис. 3.32. Журнал сканування

На основі вище-проаналізованої інформації робиться висновок, що SEP є потужним інструментом у сфері захисту кінцевих точок, а саме – комп'ютера. Він хоч й має на перший погляд простий інтерфейс, проте містить велику різноманітність функцій, механізмів для виявлення, реагування та забезпечення захисту пристрою, на якому він інстальований.

3.2. Рекомендації щодо застосування технології забезпечення захисту кінцевих точок

Уже довгий час антивірусне ПЗ обирається як де-факто рішення для захисту кінцевих точок. Антивірус відповідає усім вимогам нормативних та управлінських аудитів, проте надає організаціям не дуже великі реальні переваги щодо безпеки. Хоча антивірусні рішення захищають майже усі кінцеві точки та сервери у світі, проте порушення їхньої безпеки продовжуються з загрозливою швидкістю. Багато в чому це пов'язано з тим, що традиційний антивірус є інструментом безпеки на

основі сигнатур, який фокусується на виявленні та реагуванні на відомі загрози після того, як вони вже проникли у систему. Досвідчені зловмисники можуть обійти антивірус за допомогою недорогих автоматизованих онлайн-інструментів, які виробляють безліч унікальних невідомих атак. Зрештою, традиційний антивірус виявляється не завжди надійним рішенням для захисту систем та кінцевих точок від порушень їх безпеки.

Оскільки забезпечення безпеки функціонування кінцевої точки є одним з пріоритетних завдань для компаній чи окремих юзерів, то необхідно дотримуватись наступних рекомендацій щодо впровадження та використання систем захисту, того самого SEP, розглянутого вище.

1. Першим кроком треба проаналізувати доступні різноманітні продукти від провідних компаній з кібербезпеки, а саме продуктів для захисту кінцевих точок. Після обрання та отримання готового продукту необхідно провести його інсталяцію провідним фахівцем на кінцеві пристрої компанії або власний кінцевий комп’ютер чи інший девайс.

2. Продукт для захисту кінцевих точок повинен дозволяти кінцевим користувачам вести свою повсякденну роботу та використовувати мобільні та хмарні технології, не побоюючись невідомих кіберзагроз. Користувачі повинні мати можливість зосередитися на своїх обов'язках, а не турбуватися про виправлення та оновлення безпеки, а також повинні бути впевнені, що захищені від ненавмисного запуску шкідливих програм або експлойтів, які можуть поставити під загрозу їхню систему.

3. Слід провести каталогізацію та оцінку можливих уразливостей. За допомогою цих даних налаштовуємо та дозволяємо доступ до мережі лише для схвалених пристроїв та встановлюємо пріоритет для найбільш ризикованих, а також чутливих кінцевих точок.

4. Щоб запобігти порушенням безпеки, повинен відбутися перехід від виявлення та реагування на інциденти після того, як вони вже сталися, до запобігання порушенням безпеки в першу чергу. Кінцеві точки повинні бути захищені від відомих, невідомих загроз та загроз нульового дня, що доставляються

за допомогою шкідливого ПЗ та експлойтів, незалежно від того, чи знаходиться машина в мережі чи в автономному режимі, локально чи поза нею, підключена до мережі організації чи ні. Ключовим кроком у досягненні цього є включення локального або хмарного аналізу загроз для виявлення та запобігання відомим та невідомим можливим загрозам.

5. Інформація про загрози, отримана від інших постачальників розвідувальних послуг, повинна дозволяти продукту захисту миттєво запобігати зараженню кінцевого пристрою шкідливим ПЗ.

6. Слід перевірити, щоб продукт безпеки не сильно навантажував системні ресурси, такі як ОЗУ, ЦП або сховища. Інструмент захисту не повинен вимагати значних системних ресурсів, інакше він незмінно знижуватиме продуктивність системи та погіршуватиме роботу кінцевого користувача.

7. Пристрої IoT часто мають налаштування та паролі за замовчуванням, що робить їх легкою мішенню для зловмисників. Щоб обмежити цю вразливість, необхідно змінювати паролі, регулярно проводити оновлення ПЗ, та обслуговувати АЗ та ПЗ на всіх системах та комп’ютерах.

8. Кожен користувач кінцевого пристрою повинен бути обізнаним щодо безпечного відвідування веб-ресурсів. За більш безпечний перегляд повинен відповідати контроль доступу до веб-ресурсів. Саме для цього слід забороняти доступ до потенційно-небезпечних категорій веб-сайтів та посилань, відкриття яких може одразу стати точкою входу для зловмисника чи його зловмисного ПЗ.

Висновки до розділу

Досліджено схему роботи продукту SEP, його основні структурні компоненти. Проведено повне налаштування програми та її вбудованих модулів, завдяки яким забезпечується виявлення зловмисної активності та захист від неї. Визначено стан кінцевого комп’ютера шляхом його повного сканування налаштованим продуктом SEP.

Виокремлено рекомендації, які можуть допомогти забезпечити збереження цілісності та недоторканності даних, що функціонують на кінцевому пристрої.

ВИСНОВКИ

У даній магістерській роботі досліджено проблему необхідності забезпечення захисту кінцевих точок. Доведено, що питання забезпечення захисту кінцевих точок є важливою складовою для будь-якої організації з наявністю власних кінцевих пристроїв, а також для звичайного користувача, оскільки використання кінцевих точок породжує чисельні потоки даних, які завжди можуть бути цікаві для зловмисника.

Проаналізовано основні зловмисні атаки, що використовуються кіберзлочинцями, та способи їх реалізації на кінцевій точці. Виявлено, що найчастіше всього зловмисники використовують: зараження кінцевого пристрою шкідливим ПЗ, фішингові атаки, атаки нульового дня, уразливості у зайвих наданих правах користувачам, а останнім часом також набувають популярності атаки на незаконне встановлення майнерів, тобто криптоджекінг. Простежено статистику та вектори цих загроз за останні декілька років та виявлено тенденцію щодо зростання кількості вдалих кібератак на кінцеві точки, особливо на концепцію BYOD, пристрої якої можуть не мати надійного рівня забезпечення захисту.

Проаналізовано також найбільш популярні рішення від провідних організацій щодо забезпечення захищеності кінцевих точок, їх можливості, та обрано продукт Symantec Endpoint Protection для захисту ним кінцевого пристрою.

Досліджено можливості, структуру та вбудовані функції рішення Symantec Endpoint Protection, а також проаналізовано його архітектуру, компоненти та низку вбудованих технологій, які продукт застосовує для виявлення, реагування та забезпечення захисту.

Показано процес застосування рішення Symantec Endpoint Protection від моменту його повного налаштування до забезпечення постійного захисту. Розроблено рекомендації, що підвищать ефективність застосування технології забезпечення захищеності кінцевих точок.

ПЕРЕЛІК ПОСИЛАНЬ

1. What is an endpoint? [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudflare.com/learning/security/glossary/what-is-endpoint/.
2. What is Endpoint Security? Learn about various services and solutions [Електронний ресурс] – Режим доступу до ресурсу: https://thecyphere.com/blog/endpoint-security/.
3. Обзор рынка Endpoint Detection and Response (EDR) [Електронний ресурс] – Режим доступу до ресурсу: https://www.anti-malware.ru/analytics/Market_Analysis/endpoint-detection-and-response-edr.
4. Advanced Persistent Threat (APT) Protection - Market Quadrant 2022 [Електронний ресурс] – Режим доступу до ресурсу: https://go.kaspersky.com/rs/802-IJN-240/images/Licensed_APT_Protection_Market_Quadrant_2022.pdf.
5. Point-to-Point Communications Links [Електронний ресурс] – Режим доступу до ресурсу: https://docs.oracle.com/cd/E19504-01/802-5753/6i9g71m3s/index.html.
6. ENDPOINT SECURITY REPORT [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://adaptiva.com/resources/report/endpoint-security-report.
7. SANS 2021 Endpoint Monitoring in a Dispersed Workforce Survey [Електронний ресурс] – Режим доступу до ресурсу: https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/sans-2021-endpoint-monitoring-in-a-dispersed-workforce-survey.pdf.
8. Check Point Research: Third quarter of 2022 reveals increase in cyberattacks and unexpected developments in global trends [Електронний ресурс] – Режим доступу до ресурсу: https://blog.checkpoint.com/2022/10/26/third-quarter-of-2022-reveals-increase-in-cyberattacks/.

9. 50 Endpoint Security Stats You Should Know In 2022 [Електронний ресурс] – Режим доступу до ресурсу: https://expertinsights.com/insights/50-endpoint-security-stats-you-should-know/.

10. Endpoint security deployment status [Електронний ресурс] – Режим доступу до ресурсу: https://www.statista.com/statistics/1319760/endpoint-security-deployment-status-worldwide/.

11. EPP vs. EDR vs. XDR: Endpoint Security Comparison [Електронний ресурс] – Режим доступу до ресурсу: https://www.altexsoft.com/blog/endpoint-security/.

12. The Future of Endpoint Management [Електронний ресурс] – Режим доступу до ресурсу: https://www.securityweek.com/future-endpoint-management.

13. Endpoint Device [Електронний ресурс] – Режим доступу до ресурсу: https://www.barracuda.com/glossary/endpoint-device.

14. SANS Protects: The Endpoint Whitepaper 2022 SANS Protects: The Endpoint [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/dam/en/us/products/collateral/security/endpoint-security/sans-protects-endpoint-wp.pdf.

15. The Top 11 Endpoint Security Solutions For Business [Електронний ресурс] – Режим доступу до ресурсу: https://expertinsights.com/insights/the-top-endpoint-security-solutions-for-business/.

16. Symantec Endpoint Protection [Електронний ресурс] – Режим доступу до ресурсу: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all.html.

17. Обзор Symantec Endpoint Protection 14 [Електронний ресурс] – Режим доступу до ресурсу: https://www.anti-malware.ru/reviews/Symantec_Endpoint_Protection_14.

18. Symantec Endpoint Protection Review [Електронний ресурс] – Режим доступу до ресурсу: https://www.fool.com/the-ascent/small-business/endpoint-security/symantec-endpoint-protection-review/.

19. Symantec Endpoint Protection Benefits [Електронний ресурс] – Режим доступу до ресурсу: https://comparecamp.com/symantec-endpoint-protection-review-pricing-pros-cons-features/.

20. Symantec Endpoint Protection 15 [Електронний ресурс] – Режим доступу до ресурсу: https://docs.broadcom.com/doc/endpoint-protection-en.

21. Endpoint Protection [Електронний ресурс] – Режим доступу до ресурсу: https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-protection.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)