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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо захисту робочих станцій організації від програм-вимагачів на базі ESET Endpoint Security»

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

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

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Ірина ПАВЛІЙ
(підпис)

Виконала: здобувачка вищої освіти групи БСД-42
ПАВЛІЙ Ірина
(прізвище, ім'я)

Керівник доцент кафедри ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....9

ВСТУП.....10

1. ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ РОБОЧИХ СТАНЦІЙ ВІД ПРОГРАМ-ВИМАГАЧІВ ОРГАНІЗАЦІЇ НА БАЗІ ESET ENDPOINT SECURITY.....12

1.1 Аналіз проблеми забезпечення захисту робочих станцій.....12

1.2 Аналіз підходів до захисту та управління робочими станціями 17

1.3 Аналіз уснуючих засобів захисту робочих станцій.....21

2. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ РОБОЧИХ СТАНЦІЙ ОРГАНІЗАЦІЇ ВІД ПРОГРАМ-ВИМАГАЧІВ НА БАЗІ ESET ENDPOINT SECURITY.....29

2.1 Рішення компанії ESET щодо захисту робочих станцій.....29

2.2 Призначення, основні функції та склад програмного комплексу ESET Endpoint Security.....30

2.3 Процеси функціонування рішення ESET Endpoint Security.....34

3. РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ БЕЗПЕКОЮ РОБОЧИХ СТАНЦІЙ ОРГАНІЗАЦІЇ ВІД ПРОГРАМ-ВИМАГАЧІВ.....39

3.1 Алгоритм реалізації управління захистом робочої станцій оргназації на базі ESET Endpoint Security.....43

3.2 Розроблення рекомендацій щодо управління безпекою робочих станцій організації.....48

ВИСНОВОК.....47

ПЕРЕЛІК ПОСИЛАНЬ.....48

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація).....49

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

FRS – Federal Reserve System

ERS – Emergency Risk Surcharge

WRS – Wide Area Reference Station

ERM – Enterprise Performance Management

PAM – Privileged Access Management

LSASS – Local Security Authority Subsystem Service

SAM – Security Account Manager

SSO – Single Sign-on

XDR – Extended Detection Response

MDR – Manager Detection Response

EDR – Endpoint Detection and Response

SSL – Secure Sockets Layer

ВСТУП

Актуальність дослідження. Проблема захисту робочої станції організації стає все більш актуальною в сучасному цифровому світі, оскільки зростає загроза кібератак, вірусів, шкідливих програм та інших зловмисників. По-перше, зловмисники постійно розривають нові методи атак та використовують вразливості у програмному забезпеченні для доступу до конфіденційної інформації, вимагання викупу, або просто для завдання шкоди. По-друге, зростаюча кількість організацій переходить до цифрових платформ для зберігання та обробки даних, це робить їх уразливими перед новими загрозами, зокрема втратою даних або порушення приватності. По-третє, у багатьох випадках загроз для робочих станцій може виникати зсередини самої організації через нестабільність співробітників або навмисні дії зловмисників. По-четверте захист робочих станцій вимагає постіного оновлення програмного та апаратного забезпечення, а також регулярного навчання персоналу з питань кібербезпеки. Враховуючи ці фактори, можна зробити висновок, що проблема захисту робочих станцій організації є дуже актуальною і потребує постійної уваги та інвестицій з боку керівництва для мінімізації рихиків та забезпечення безпеки даних та інформаційних ресурсів.

ESET Endpoint Security – це комплексне рішення з кібербезпеки, призначене для захисту робочих станцій (комп’ютерів) в корпоративних середовищах віл різних кіберзагроз, включаючи програми-вимагачі. Основні функції які виконує ESET Endpoint Security це антивірусний захист, механізми виявлення в реальному часі, фаєрвол та захист від вторгнень, антифішинг, захист від програм-вимагачів.

Рішенням на основі ESET Endpoint Security для проблеми захисту робочих станцій від програм-вимагачів включаючи декілька кроків. По-перше, постійне оновлення баз даних загроз для виявлення нових варіантів програм-вимагачів. По-друге, створення правил та політик безпеки, які відповідають потребам конкретної організації та допомагають у запобіганні атак програм-вимагачів. По-третє, систематичний моніторинг та аналіз активнсоті системи для виявлення незвичайних змін, що можуть свідчити про наявність програм-вимагачів. По-

четверте, використання регулярних бекапів даних та механізмів відновлення для запобігання втраті даних у разі успішної атаки програм-вимагачів.

Об'єкт дослідження – захист робочих станцій організації від програм-вимагачів.

Предмет дослідження – методи та засоби захисту робоичх станцій організації від програм-вимагачів на базі ESET Endpoint Security.

Мета роботи – розробити рекомендації щодо застосування методів та засобів захисту робочих станцій організації від програм-вимагачів на базі ESET Endpoint Security.

Наукові завдання:

дослідити сутність проблеми захисту робочих станцій організації;

проаналізувати основні підходи до захисту робочих станцій організації;

проаналізувати існуючі рішення із захисту робочих станцій організації;

проаналізувати методи та засоби захисту робочих станцій організації від програм-вимагачів на базі ESET Endpoint Security;

запропонувати варіанти системи захисту робочих станцій організації від програм-вимагачів на базі ESET Endpoint Security;

розробити рекомендації щодо управління безпекою робочих станцій організації.

Методи дослідження – опрацювання література за даною темою, аналіз експлуатаційної документації.

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів та засобів захисту робочих станцій від програм-вимагачів, а також розроблено рекомендації фахівцям з кібербезпеки щодо реалізації.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ РОБОЧИХ СТАНЦІЙ ОРГАНІЗАЦІЇ ВІД ПРОГРАМ-ВИМАГАЧІВ НА БАЗІ ESET ENDPOINT SECURITY

1.1 Аналіз проблеми забезпечення захисту робочих станцій

Робоча станція – це пристрій, особистий чи корпоративний, який містить дані організації.

Згідно річному звіту Trend Micro про кібербезпеку за 2023, можемо отримати статистичні дані про різні загрози. В даному розділі розглянемо декілька загроз для робочих станцій: загрози програм-вимагачів, хмарне технології та загрози для підприємств, виявлення загроз та загроза ландшафту.

Для початку розглянемо що собою являє загрози програм-вимагачів. Наступні тактики спостерігалися в 2023 році, і з кожним роком дії програм-вимагачів стають все більш складними. Постійно зростає використання віддаленого шифрування:

спостерігається в Akira, Black Cat, BlackMatter, LockBit і Royal;

зловмисники активно відображають диски для шифрування на ураженій кінцевій точці замість виконання бокового переміщення. Це може бути стрибком у тактиці, щоб зменшити їх вплив на атаки, щоб уникнути виявлення.

Групи програм-вимагачів також максимально підвищують зручність періодичного шифрування:

зловмисники шифрують фрагменти даних замість того,щоб шифрувати всі дані за один раз, цей процес прискорює шифрування, водночас роблячи уражені дані марними для жертви. А також ускладнює процес шифрування.

Виявлення та реагування на кінцевій точці (EDR) обходить за допомогою неконтрольованих віртуальних машин (VM):

спостерігається у Akira і Black Cat;

зловмисники обходять EDR, створюючи неконтрольовані віртуальні машини для навігації, відображення та шифрування файлів у системах гіпервізора Windows Hyper-V і підключених віртуальних машинах.

Атаки програм-вимагачів:

початковий зловмисник продає свій доступ іншим групам програм-вимагачів, щоб розпочати численні атаки з поєднанням зловмисного програмного забезпечення, крадіжок даних і інструментів стирання, щоб максимізувати маніпуляції та тиск на жертв.

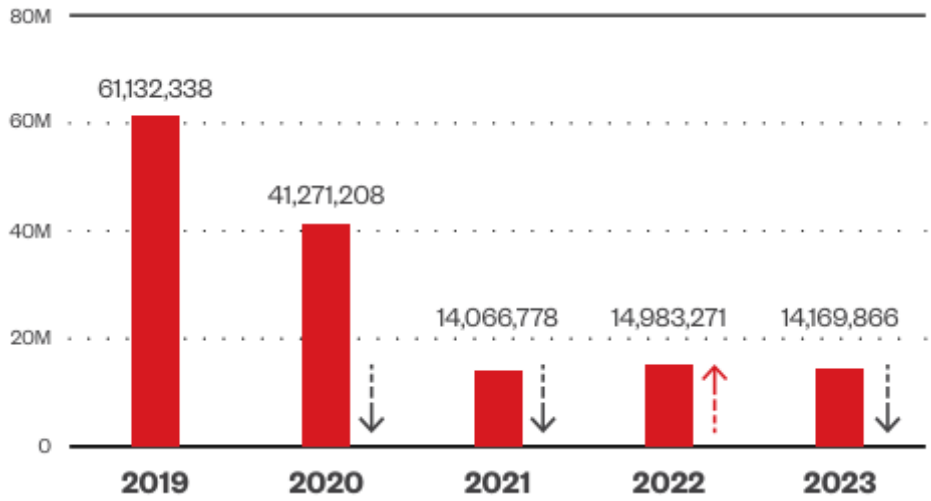

Рис. 1.1 Загальна кількість виявлень програм-вимагачів [1]

Спостерігається загальна тенденція до зниження виявлення програм-вимагачів, причому виявлення програм-вимагачів з 2021 по 2023 рік становить у середньому менше половини зареєстрованих виявлень у 2020 році. Раніше атаки програм-вимагачів запускали «масово», наприклад спам-кампанії зі зловмисними посиланнями, але атаки зосередженні на кількості, можна легше заблокувати. Ці цифри показують загальну тенденцію до зниження, що відповідає загальній кількості виявлень програм-вимагачів.

Однак постійне збільшення кількості виявлень FRS може свідчити про те, що зловмисники використовують ефективніші способи уникнення попереднього виявлення від прибуття та захисту, таких як бінарні файли та сценарії живих поза

межами землі (LOBIN/LOLBA), Bring your Own Vulnerable Driver (BYOVD), експлойти нульового дня та завершення AV.

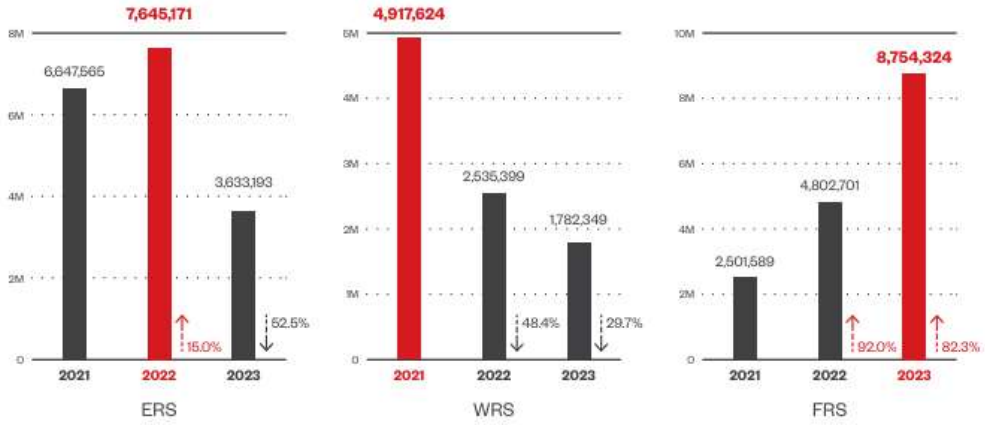

Рис 1.2 Дані ERS, WRS та FRS про програми-вимагачі [1]

Згідно з даними звіту, виявлення клієнтами атак програм-вимагачів, націлених на Linux, у першій половинні 2023 року продовжує затьмарювати атаки MacOS. Це узгоджується з даними, зібраними з 2022 року, який був винятковим роком для виявлення зловмисного програмного забезпечення на базі Linux, що становило 25%, раніше цільові атаки на Linux становили лише два-три відсотки співвідношення ОС. Слід зазначити, що Windows продовжує приймати основну частину наших виявлень програм-вимагачів, лише значне зменшення у 2022 році.

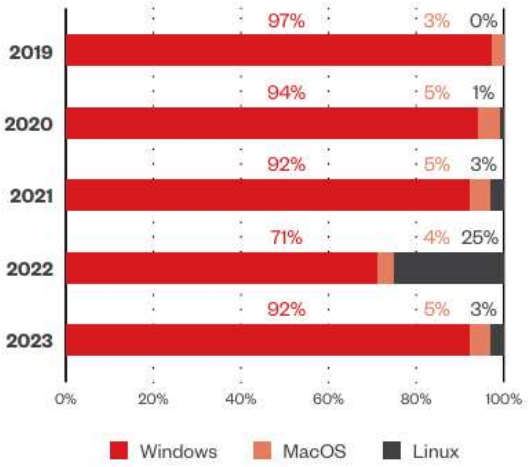

Рис. 1.3 Операційні системи, уражені програмами-вимагачами [1]

Однак, оскільки дані за 2023 рік були звершені, кількість атак програм-вимагачів MacOS виявилася вищою з 9961 виявленням, тоді як виявленням Linux було остаточно визначено 4949. Це може свідчити про те, що атаки, націлені на Linux , стабілізуються після напливу нових варіантів Linux у 2022 році на початку 2023 року, але на це може вплинути загальне зниження активності програм-вимагачів.

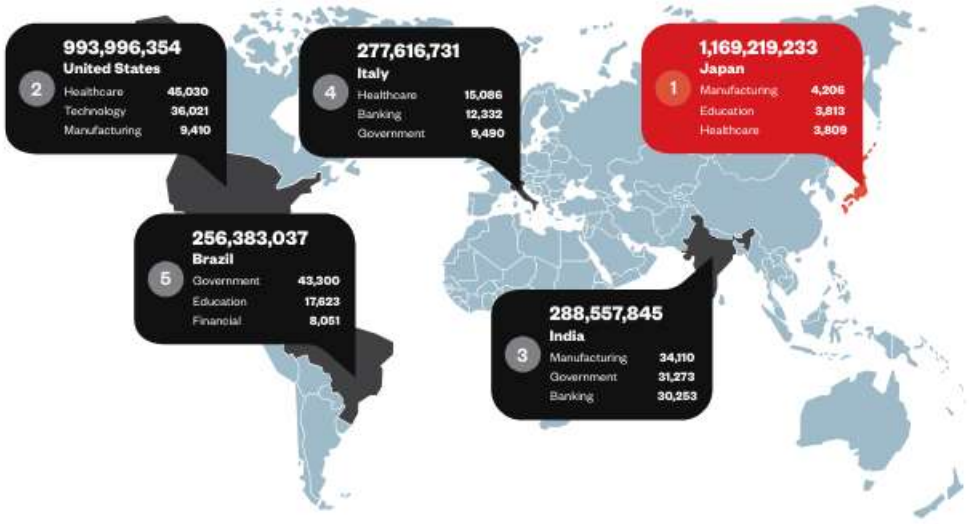

Рис. 1.4 Найпопулярніші країни та регіони за виявлені атаки програм-вимагачів [1]

Галузеві рейтинги та розбивка сегментів на основі унікальних показників виявлення в кінцевій точці показують, що підприємства є основними цілями, причому значний інтерес до банківського сектора у 2023 році.

Найпопулярніші сімейства програм-вимагачів StopCrypt і LockBit зберігають лідируючі позиції з точки зору найбільш плідних сімейств програм-вимагачів у 2023 році, як і в попередньому році, але перший з невеликим відривом обігнав другий цього року. Зауважимо, що ці дані не включають застарілі сімейства програм-вимагачів. Розглянемо трохи функціоналу LockBit яка у 2022 році набула популярності:

створює та використовує шкідливу програму StealBit для автоматизованого викрадення даних;

запускає програму винагороду за помилки у 2022 році;

LockBit 3.0 має спільний код схожість з DarkSide і BlackMatter;

збільшує кількість філій, які купують доступ до цілі від інших суб'єктів загрози.

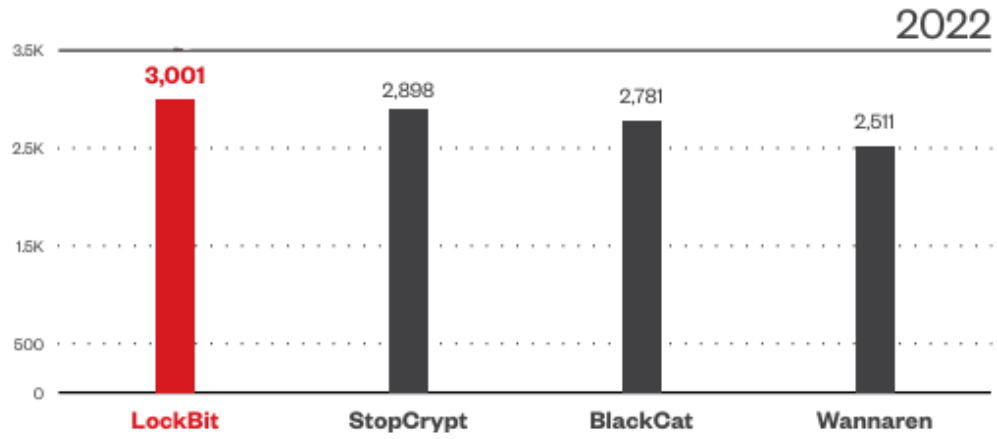

Рис. 1.6 Найпопулярніші сімейства програм-вимагачів у 2022 році [1]

Далі розглянемо передмови використання StopCrypt яка у 2023 році набула популярності, зіштовхнувши LockBit на друге місце порівняно з 2022 роком:

вимагає виконання з певними аргументами або параметрами, додатковими компонентами або в певному середовищі, щоб продовжити свою процедуру;

повідомлялася, що у 2023 році вони були націлені на Індфю разом із LockBit і BlackCat.

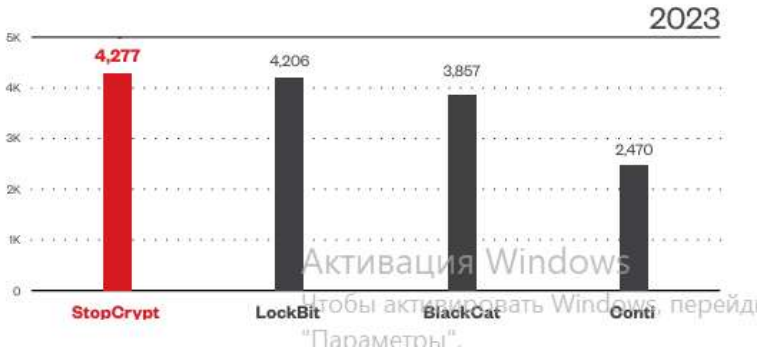

Рис. 1.7 Найпопулярніші сімейства програм-вимагачів у 2023 році [1]

Отже, програми-вимагачі створюють великі проблеми, спричиняючи щначні збитки для користувачів і організації. Вони шифрують важливі дані, порушують робочі процеси та вимагають викуп, що може призвести до сейрозних фінансових втрат. Крім того, ці атаки можуть підірвати репутацію організації та викликати втрату довіри з боку клієнтів.

1.2 Аналіз підходів до захисту та управління робочими станціями

Робочі станції Windows, MacOS, і Linux є улюбленою ціллю для зловмисників. Сучасні співробітники часто працюють вдома або в дорозі, поза захистом корпоратвиної мережі. У світі гібридної робочої сили та хмарних сервісів робочі станції є звичайною точкою входу для зловмисників і новою лінією захисту для більшості компаній. Зловмисники регулярно використовують недостатньо захищені робочі станції для запуску шкідливих програм, проникнення в IT-системи та викрадення конфіденційних даних.

Програмне забезпечення-вимагач та інші атаки можуть порушити ваш бізнес, заплямувати репутацію вашої компанії та коштувати вашому бізнесу чималої суми. Насправді вартість злому програм-вимагачів становить 4.62 мільйона доларів.

Переважна більшість виснажливих кібератак, таких як атаки програм-вимагачів, походять із кінцевих точок загалом і робочих станцій зокрема. Безпека робочої станції є фундаментальною. Але збалансувати безпеку та взаємодію з користувачем може бути складно. Потрібно захищатися від злому, не перешкоджаючи кінцевим користувачам і не створюючи вузьких місць у роботі. Безперебійно надаючи потрібним людям і програмам потрібний доступ до потрібних ресурсів у потрібний час, менеджер привілеїв кінцевих точок може допогти посилити вашу безпеку, не перешкоджаючи продуктивності працівників і не знижуючи задоволеності користувачів.

Безпека робочої станції починається з керування привілеями. Сучасні кмітливі зловмисники використовують привілейовані облікові записи, щоб захоплювати робочі станції та організовувати складні атаки. Менеджер привілеїв

кінцевої точки служить першою лінією захисту вашого бізнесу, захищаючи від зловживань привілеями та зупиняючи зловмисників на їхніх слідах у точці входу. Розглянемо декілька методів захисту робочих станцій за допомогою диспетчера привілеїв кінцевих точок, які пропонує нам CyberARK.

Першим методом є видалення права локального адманістратора. Облікові записи адміністратора Microsoft Windows, MacOS і Linux відкривають двері для загроз. Ці привілейовані облікові записи використовуються для встановлення та оновлення програмного забезпечення робочої станції, налаштування параметрів системи і керування обліковими записами користувачів. Зловмисники часто використовують їх для вимкнення антивірусного програмного забезпечення чи інструментів аварійного відновлення, а аткож для запуску програм-вимагачів та інших типів шкідливих програм. Позбавлення прав локального адміністратора є найшвидшим і найпростішим кроком до зміцнення робочих станцій і відкидання зловмисників. Це обмежує шкоду, яку може завдати зловмисник, якщо йому в руки потраплять облікові дані кінцевого користувача за допомогою фішингової схеми чи ігшого трюку. Крім того, скасування прав локального адміністратора запобігає випадковому встановленню зловмисного програмного забезпечення або виконанню інших привілейованих дій, які можуть спровокувати атаку або створити шлях для загрози.

Другим методом є застосування найменших привілеїв. Користувачі часто мають законну потребу виконати дію, що вимагає адміністративних привілеїв. Найкращі у своєму класі менеджери привілеїв кінцевих точок дозволяють підвищувати дозволи користувачів для виконання певних завдань на основі політики, не вимагаючи дій кінцевого користувача чи втручання служби підтримки. Дотримуючись принципу найменших привілеїв – надаючи кінцевим користувачам і програм мінімальний набір привілеїв, необхідних для виконання своїх завдань – можемо пом’якшити вразливість робочої станції та посилити рівень безпеки.

Третім методом є інститут політики контролю програм. Контроль програм є основоположним для захисту від зловмисного програмного забезпечення та інших

загроз. Багато менеджерів привілеїв кінцевих точок підтримують функції дозволеного та забороненого списків, щоб явно дозволити або заблокувати відомі програми. Відмінність між хорошим контролем програм і відмінним полягає в здатності створювати комплексні правила, що охоплюють не лише конкретні виконувані файли (наприклад, враховуючи хеш, ім'я файлу. Шлях до файлу), але й групу виконаних файлів, таких як програми, що дозволяють за замовчуванням які підписані певним постачальником, мають конкретну назву продукту, пов'язау з ними, і походять із визначеного надійного джерела оновленя.

Деякі менеджери привілеїв кінцевих точок також контролюють поведінку необробленої програми за допомогою функції «сірий список». Наприклад, можете зменшити ризики програм-вимагачів, створивши невідомі програми в ізольованому середовищі, дозволивши їм працювати, але не мати доступу до Інтернету. Провідні менеджери привілеїв кінцевих точок також підтримують розширені умовні політики з вкладеними правилами для блокування складних атак із залученням довірених програм.

Четвертим методом є захист та зміна паролів адміністратора робочої станції. Адміністративні облікові записи є улюбленою мішенню для зловмисників. Навіть якщо позбивити користувачів прав локального адміністратора, скомпроментовані облікові записи адміністратора все одно можна використовувати для здійснення атак. Належна гігієна пароля адміністратора є важливою, а управління на основі політики є найкращим способом забезпечити належну гігієну.

Провідні менеджери привілеїв кінцевих точок інтегруються з рішеннями керування привілейованим доступом (PAM), щоб захистити адміністративні паролі та посилити безпеку робочої станції. З рішенням PAM ви можете безпечно зберігати паролі в безпечному цифровому сховищі, щоб запобігти крадіжці, і автоматично змінювати їх відповідно до політики, прозоро для користувача. Регулярна зміна пароля допомагає зменшити ризик у випадку, якщо пароль якимось чином зламано.

П'ятий метод це захист кешованих облікових даних. Крадіжка облікових даних відіграє провідну роль у більшості кібератак. Не дивно, що кешовані облікові

дані є основною мішенню для загрозливих осіб і кіберзлочинців. Різноманітні служби Windows зберігають різні облікові дані в пам’яті, включаючи службу підсистеми локального центру безпеки(LSASS), диспетчер облікових записів безпеки (SAM) і кеш облікових даних домену. Крім того, багато веб-браузерів, менеджерів паролів і рішень єдиного входу (SSO) локально кешують облікові дані програм і веб-сайтів. Зловмисники часто використовують кешовані облікові дані для викрадення даних, здійснення незаконних дій або атак.

Розширені менеджери привілеїв кінцевих точок автоматично виявляють і блокують дії, які зловмисники зазвичай виконують для збору облікових даних, кешованих операційними системами, веб-браузерами, менеджерами паролів, програмами SSO або іншими програмами. Кешовані облікові дані часто не помічаються організаціями безпеки та часто використовуються зловмисниками.

Шостим методом є обманювання загрозливих суб’єктів і виявлення їх на ранніх стадія ланцюга атак. Найкращі в своєму класі менеджери привілеїв кінцевих точок підтримують функцію обману привілеїв, щоб допомогти заманити й відкинути потенційних зловмисників. Також можемо створювати підроблені привілейовані облікові записи «honeypot» із привабливими іменами користувачів, як-от «admin2», і навмисно слабкими паролями, як от «admin» , щоб накрутити та забокувати зловмисників у точці входу. Менеджер привілеїв кінцевої точки створить сповіщення, щоб повідомити, коли заманили зловмисника.

Останій метод це проактивний моніторинг активності привілейованої робочої станції. Багато диспетчерів привілеїв кінцевих точок надають можливості моніторингу та звітування, щоб допомогти відстежувати діяльність привілейованих робочих станцій, виявляти підозрілу поведінку та потимізувати аудит відповідності та криміналістичні дослідження. Більшість містить стандартні звіти, які дозволяють легко визначити, які робочі станцій та програми захищені, а аткож конкретні політики підвищення привілеїв і бізнес-правила, які застосовуються.

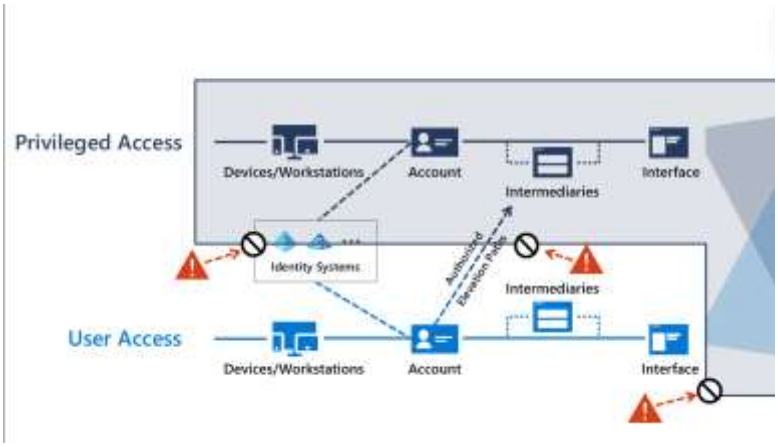

Рис. 1.8 Підхід захисту та управління робочої станцією [2]

Провідні менеджери привілеїв кінцевих точок генерують докладні повідомлення про події кожного разу, коли політика викликається, і містять інформаційні панелі та інструменти для спостереження та вивчення подій і статистики, керованих політикою. Спритні зловмисники часто залишаються поза увагою радарів, досліджуючи захист, плануючи та реалізовуючи свої наступні кроки. Проактивно відстежуючи захист, плануючи та реалізовуючи активність привілейованих робочих станцій, можете ідентифікувати та зупинити супротивників до того, як вони зможуть рухатися вік і завдавати серйозної шкоди.

Отже, ефективний захист та управління робочими станціями є критично важливими для забезпечення безпеки та стабільності в організаціях. Використання передових методів кібербезпеки, регулярне оновлення систем, навчання користувачів та впровадження спеціалізованого програмного забезпечення дозволяють мінімізувати ризик від кібератак і забезпечують безперебійну роботу. Інтегрований підхід до цих завдань допомагає знизити вразливість до загроз та підтримувати високий рівень захисту кібербезпеки, що є ключовим для успішного функціонування сучасних організацій.

1.3 Аналіз існуючих засобів захисту робочих станцій

Захист робочих станцій є важливою частиною загальної стратегії кібербехпеки в будь-якій організації. Існуючі засоби захисту робочих станцій

включають різноманітні технології та методики, що забезпечують захист від зловмисних програм, несанкціонованого доступу та інших кіберзагроз. Існує багато продуктів на ринку платформ захисту інформації, декілька з них ми порівняємо та переглянемо їх функціонал та рішення щодо захисту робочих станцій.

Для початку розглянемо Trellix Endpoint Security Suite – це гнучке уніфіковане рішення, яке захищає пристрої та кінцеві точки на межі мережі, надаючи можливість організації ретельно, ефективно та швидко вирішувати складні розподілені проблеми безпеки. Він використовує аналітику та машинне навчання для досягнення найкращої в галузі ефективності, водночас пропонуючи гнучкість підключення до продуктів інших постачальників. Рішення допоможе уніфікувати дані та захист від загроз із пристрою в хмару, для комплексної безпеки.

Оскільки Trellix об’єднує дані та захист від загроз від пристрою до хмари, можна будувати майбутнє, де безпека буде інтегрованою системою – простішою, розумнішою та широкою, ніж будь-що раніше. Trellix Endpoint Security Suite навчається та розвивається, щоб захистити потреби бізнесу, що змінюються, у динамічному середовищі загроз.

Важливо зазначити, що Trellix Endpoint Security Suite – це інтегрований набір технологій, який використовує аналітику та машинне навчання для забезпечення ефективного захисту, включаючи гнучкість підключення до продуктів безпеки від інших постачальників, ці методики надають декілька рекомендацій для захису вашої робочої станції. Перша рекомендація від Trellix – запобігайте, виявляйте, розслідуйте та реагуйте на загрози, одночасно ефективно керуючи поверхнею для атак. Trellix допомагає передбачити, визначити пріоритети тп призначити найефективнішу відповідь на загрози за допомогою інтегрованих служб виявлення та реагування (XDR), керованих служ виявлення та реагування (MDR), відкритих API та партнерських програм. Та другою рекомендацією від Trellix – підтримувати віддалених співробітників за допомогою провідної галузі безпеки кінцевих точок і єдиного захисту, а також комплексного проактивного аналізу загроз і засобів захисту протягом усього життєвого циклу атак.

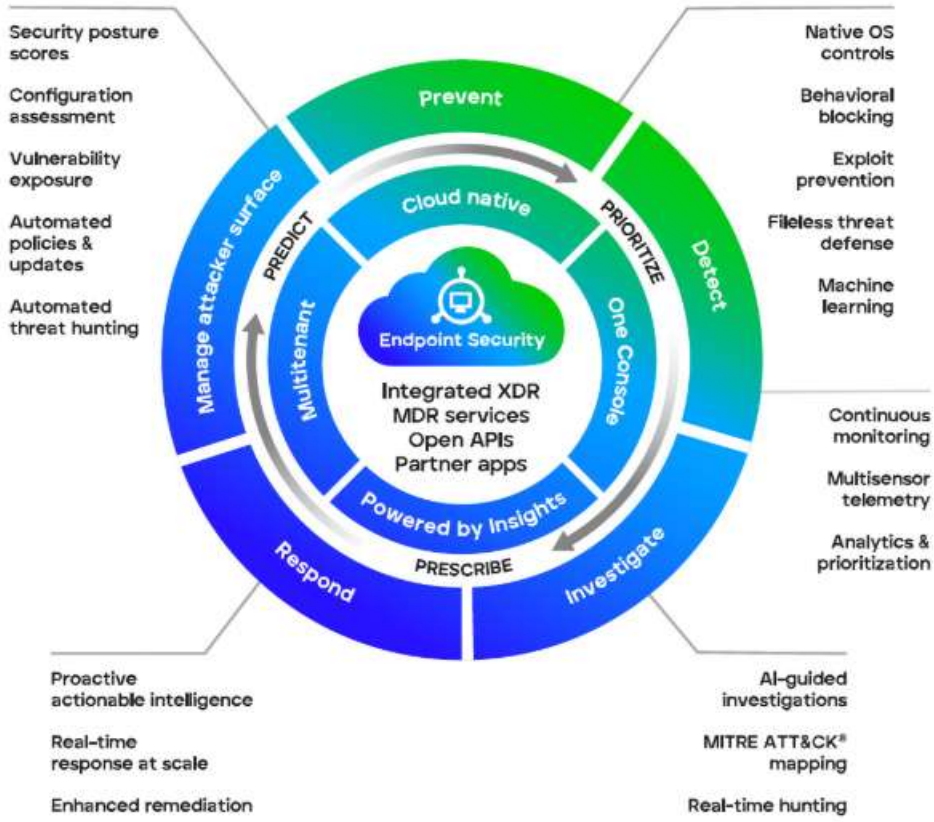

Рис 1.9 Безпека кінцевої точки на базі Trellix [3]

Trellix Endpoint Security Suite складається з 3 важливих компонентів це безпека кінцевої точки (ENS) та виявлення та відповідь кінцевої точки (EDR).

Рішення кінцевої точки, має відповідати пріоритетам, які є найважливіші. Незалежно від ролі Trellix Endpoint Security відповідає конкретним критичним потребам – від запобігання загрозам і полювання на них до адаптації засобів контролю безпеки. Потрібно використовувати рішення, щоб забезпечити безперебійну роботу системи для користувачів, знайти більше можливостей для автоматизації та спростити складніробочі процеси.

Trellix EDR допомагає зменшити втому від сповіщень, надаючи аналітикам усіх рівнів кваліфікації можливість підвищувати, одночасно потсійно відстежуючи та збираючи дані, щоб забезпечити видимість і контекст, необхідний для виявлення загроз і реагування на них.

Унікальним рішенням Trellix EDR є Trellix Insights, яке дозволяє проактивувно визначити пріоритети загроз, прогнозувати, чи зможе існуюча тактика їх зупинити, і призначати ефективні контрзаходи.

Далі розглянемо Sophos Intercept X використовує найсучасніший захист, включаючи глибоке виявлення шкідливих програм, профілактику вразливих місць та технології, призначені для зупинки»програм-вимагачів» та завантаження записів. Створені спеціально для Intercept X, функції Server Lockdown та Cloud Workload Discovery забезпечують збереження конфігурацій серверів не залжено від того, де вони знаходяться.

Експлуатаційні атаки в середовищах сервера можуть бути руйнівними і часто їх не можна виявити за допомогою традиційних технологій захисту серверів. Intercept X призначено для того, щоб зупинити навіть найбільш наполеглевих хакерів від експлуатації вразливостей засобами, які спрямовані на збирання облікових даних, залишаючись при цьому прихованими, або тим, що розроблені для переміщення через мережу системами та додатками.

CryptoGuard захищає сервери, зупиняючи шифрування даних і відновлюючи будь-які зміни до попередньо відомих безпечних станів. З Root Cause Analysis виявлення та виправлення загроз є простим для розуміння та допомагає скоротити час реакції на інцидент експоненціально.

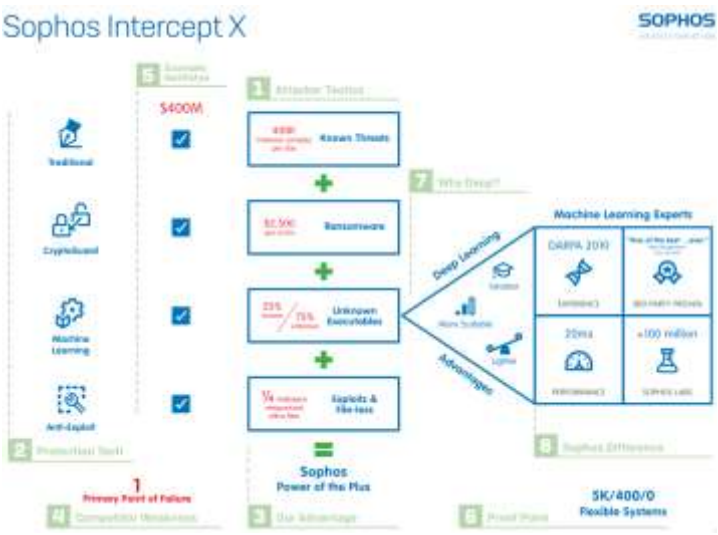

Рис. 1.10 Sophos Central архітектрура [4]

Також Sophos Intercept X for Server пропонує нам розглянути синхронізаційну безпеку та блокування сервера одним кліком. Для початку розглянемо синхронізовану безпеку – є найкращою серед аналогів системи безпеки. вона поєднує в собі інтуїтивно зрозумілу платформу безпеки з продуктами, що мають безліч нагород, які активно працюють разом, щоб блокувати додаткові загрози та надавати унікальний захист. Далі завдяки блокуванню сервера одним кліком можна отримати потужні зміни та контроль управлінськими можливостями шляхом віднесення програм до !білого списку» та недопущення несанкціонованої конфігурації сервера.

Останій компонент Microsoft Defend for Endpoint – це платформа безпеки Microsoft корпоративного рівня для запобігання, виявлення, дослідження та реагування на розширені загрози в корпоративних мережах. Він вбудований у Windows 10 і різні служби Microsoft Azure. Основними функціями Defender for Endpoint:

поведінкові датчики кінцевої точки – вбудовані в Windows 10 ці датчики збирають і обробляють поведінкові сигнали від операційної системи. Ці дані надсилаються до хмарного приватного екземпляра Microsoft Defender for Endpoint;

хмарна аналітика безпеки – рішення збирає інформацію з оптики Microsoft у всій екосистемі, включаючи онлайн-активи та корпоративні хмарні продукти, такі як Office 365. Воно використовує великі дані та навчання пристроїі, щоб перетворити ці поведінкові сигнали на виявлення, статистичні дані та рекомендовані відповіді на загрози;

інтелектуальні дані про загрози – сторонні партнери, мисливці та групи безпеки Microsoft надають дані аналізу загроз Defender for Endpoint.рішення використовує інформацію для визначення конкретних методів, процедур та інструментів зловмисника. Він створює сповіщення, коли спостерігає ці індикатори атаки в зібранихданих датчиків.

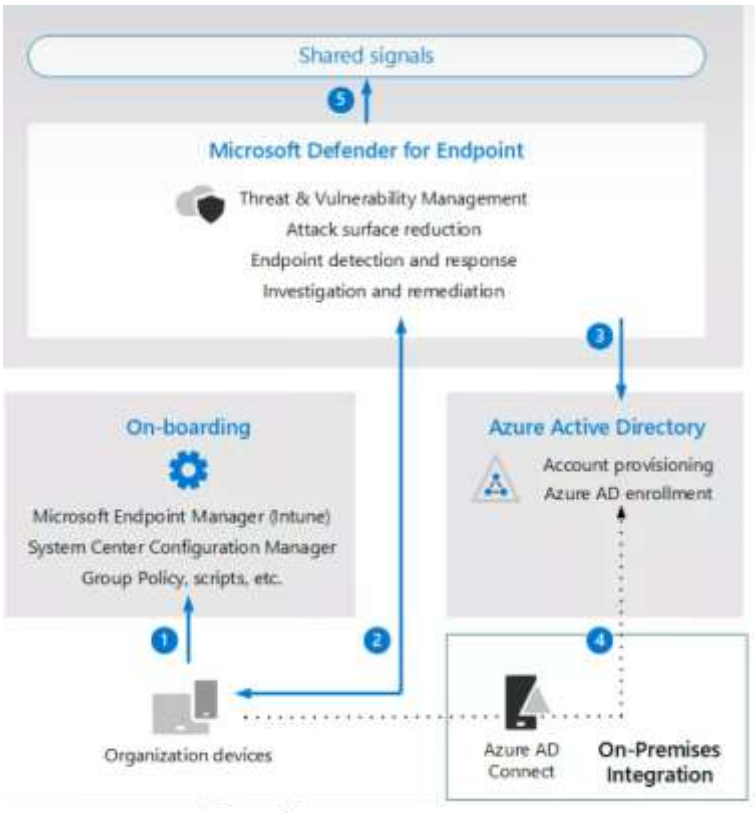

Рис. 1.11 Процес підключення кінцевих пристроїв для захисту Defended for Endpoint [5]

На рисунку продемонтровано процес підключення кінцевих пристроїв, щоб можна була захистити Defended for Endpoint:

вбудовані пристрої за допомогою Microsoft Intune, System Centre Configuration Manager, сценаріїв або інших підтримуваних інструментів керування;

пристрої починають надсилати сигнали Microsoft Defend for Endpoint;

керовані пристроїв приєднується або реєструються в Azure Active Directory (Azure AD);

пристрої Windows, розгорнуті локально та зареєстровані в Windows Active Directory, синхронізуються за допогою Azure AD Connect.

Також існує декілька особливостей роботи Microsoft Defender for Endpoint, які варті уваги кожного кіберфахівця.

Однією з особливостей Microsoft Defender for Endpoint є управління загроза та вразливістю ця функцію допомагає виявляти вразливості та неправильні конфігурації в кінцевих пристроях у режимі реального часу, без необхідності

розгортання спеціальних агентів або сканування вразливсотей. Управління загрозами та вразливістю використовує датчики на кінцевих точках для виявлення вразливостей. Він може визначати пріоритети вразливостей на основі аналізу всіх виявлень у вашій організації, незалежно від того, чи містять кінцеві точки конфіденційні дані чи ні, а також ландшафту загроз. Ця можливість повністю базується на хмарі та інтегрується з рештою стека безпеки кінцевої точки.

Слідуюча особливість Microsoft Defender for Endpoint – зниження поверхні атаки, яка може допомогти автоматично зменшити кількість атак на кінцевих пристроях, блокуючи певні можливості на рівні операційної системи та контролюючи додатки та доступ до Інтернету. Зниження поверхні атаки базуєтьється на правилах, які можуть контролювати поведінку програмного забезпечення, як-от запуск виконуваних файлів і сценаріїв, у тому числі сценаріїв, які є підозрідими, і програмне забезпечення, яке виконує дії, нетипові для звичайної робочої діяльності.

Останьою особливістю Microsoft Defender for Endpoint є Microsoft Secure Score для пристроїв – ця функція забезпечує автоматизовану оцінку всієї корпоратвиної мережі, допомагаючи ідентифікувати незахищені системи та вжити заходів для покращення безпеки. Secure Score for Devices визначає незахищені системи та автоматично виконує дії для покращення стану їх безпеки. Оцінка безпеки для пристроїв показує єдину оцінку для всієї мережі, вказуючи, скільки кінцевих пристроїв захищено від кібератак.

Захисник Microsoft для кінцевих точок спочатку був випущений як повне рішення для виявлення та реагування на кінцеві точки (EDR) і вдосконалене рішення для захисту від загроз. Початкову та нову версію Microsoft Defender for Endpoint було перейменовано так:

Defender for Endpoint Plan 1 – це нова назва для обмеженої версії продукту, призначеного для невеликих компаній;

Defender for Endpoint Plan 2 – це нова назва для повної версії продукту, який раніше називався просто «Microsoft Defender for Endpoint»

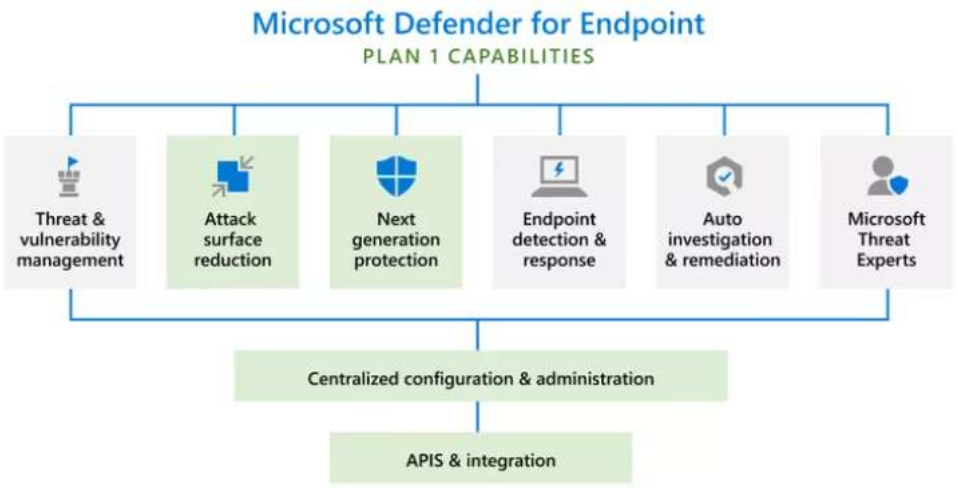

Рис. 1.12 Можливості Microsoft Defender for Endpoint Plan 1[4]

Отже, аналізуючи існуючі засоби захисту робочих станцій, показує, що сучасні рішення забезпечують високий рівень безпеки завдяки інтеграції передових технологій. Вони пропонують багатошаровий підхід до захисту, включаючи виявлення та реагування на загрози в реальному часі, штучний інтелект для прогнозування та попередження атак, а також ефективне управління інцидентами. Загалом, ці платформи значно підвищують безпеку робочих станцій, знижуючи ризики та мінімізуючи потенційні загрози завдяки своїй комплексності та інтеграції з іншими інструментами кібербезпеки.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ РОБОЧИХ СТАНЦІЙ ОРГАНІЗАЦІЇ ВІД ПРОГРАМ-ВИМАГАЧІВ НА БАЗІ ESET ENDPOINT SECURITY

2.1 Рішення компанії ESET щодо захисту робочих станцій

ESET Endpoint Security – потужний багаторівневий захист який використовує унікальну глобальну мережу ESET для виявлення загроз, а також машинне навчання та досвід кваліфікованих фахівців. Для того аби виконати повне розгортання продуктів безпеки ESET потрібно інсталювати деякі компоненти, з якими пізніше ознайомимся більш детально.

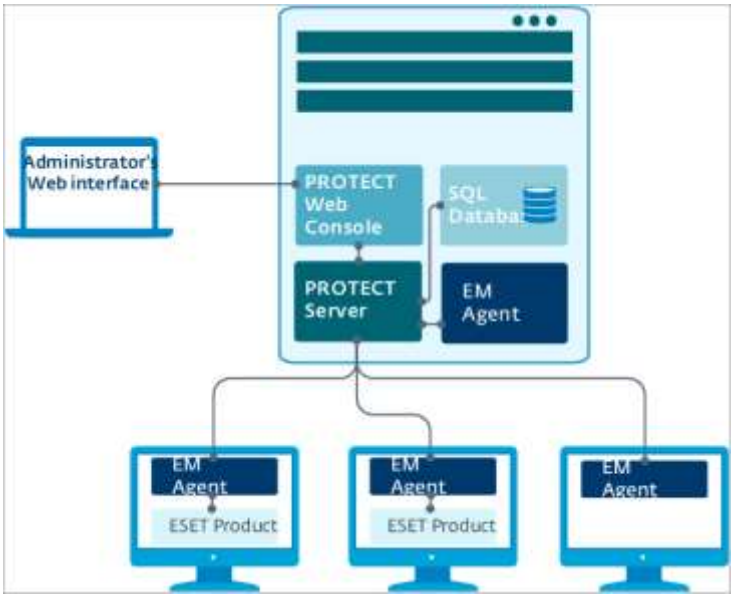

Рис. 2.1 Комопненти й архітектура ESET PROTECT [6]

ESET PROTECT Server – це програма,яка обробляє всі дані, отримані від клієнтів, яка підключаються до сервера(через ESET Management Agent).

Agent ESET Managent – є невід'ємною частиною ESET PROTECT.комп'ютери клієєнтів передають дані на сервер не напряму, а через агнета. Агент забирає інформацію від клієнта та надсилає її на сервер ESET PROTECT. Якщо ESET PROTECT Server надсилає завдання клієнтуЮ воно

потрапляє до агнета, який пересилає завдання до продукту ESET на робочі станції клієнта.

ESET PROTECT Web Console – це інтерфейс користувача в браузері, який дає змогу керування рішеннями ESET у вашому середовищі. У ньому відображається загальна інформація про статус клієнтів у мережі. Окрім того, його можна використовувати для віддаленого розгортання рішень ESET на некеровані комп'ютери. Якщо зробити веб-сервер доступним з Інтернету, ESET PROTECT можна використовувати практично в будь-якому місці й на бідь-якому пристрої.

ESET Bridge (Проксі-сервер HTTP) використовується для завантаження та кешування: оновлення модулів ESET, пакет інсталяції й оновлення, просунуті ESET PROTECT (наприклад, інсталятор MSI ESET Endpoint Security), оновлення продуктів ESET для захисту(оновлення компонентів і продуктів), результати ESET LiveGuard також переспрямовання обміну даними з агентами ESET Management на сервер ESET PROTECT.

Отже, рішення компанії ESET щодо захисту робочих станцій відзначається високою ефективністю та надійністю. ESET пропонує комплексний підхід до кібербезпеки, включаючи проактивний захист від шкідливого програмного забезпечення, вдосконалене виявлення загроз і швидке реагування на інциденти. Їхні продукти забезпечують багаторівневий захист, інтегруючи технології машинного навчання та поведінкового аналізу для виявлення навіть найскладніших атак. Крім того, ESET приділяє велику увагу зручності використання та мінімальному впливу на продуктивність системи, що робить їхні рішення оптимальним вибором для захисту робочих станцій у різних середовищах.

2.2 Призначення, основні функції та склад програмного комплексу ESET Endpoint Security для Windows

ESET Endpoint Security – це новий підхід до розробки повністю інтегрованої системи безпеки комп'ютера. Остання версія ядра сканування ESET LiveGrid у поєднанні зі спеціально розробленим брандмауером і модулем «Антиспам»

забезпечують швидку й точну роботу. А також надійний захист вашого комп’ютера. Таким чином, кожен користувач отримує інтелектуальну систему, яка гарантує постійний захист від атак і зловмисного програмного забезпечення, що загрожують комп’ютеру.

ESET Endpoint Security 9 – повноцінне рішення безпеки, яке стало результатом тривалої роботи, спрямованої на поєднання максимального захисту та використання мінімуму системних ресурсів. Передові технології на базі штучного інтелекту здатні проактивно блокувати проникнення вірусів, щпигунських і троянських програм, черв’яків, нав’язливої реклами, руткітів й інших атак з Інтернету, не зменшуючи продуктивність системи та не порушуючи роботу комп’ютера.

ESET Endpoint Security насамперед призначено для робочих станцій, яуі працюють у середовищі малих фірм.

Використання ESET Endpoint Security і ESET PROTECT у корпоративному середовищі дає змогу легко керувати будь-якою кількістю робочих станцій клієнтів, застосувати політики та правила, стежити за виявленими об’єктами та віддалено налаштовувати клієнти з будь-якого комп’ютера в мережі.

Функції та переваги:

удосконалений інтерфейс користувача: у цій версії інтерфейс користувача було значно змінено та спрощено на основі результатів тестування зручності в користуванні. Усі формування в елементах графічного інтерфейсу та сповіщень ретельно відредаговано, а сам інтерфейс тепер підтримує мови із записом справа наліво, зокрема арабську й іврит;

темний режим: розширення для швидкого переключення екрана в темний режим;

антивірус та антишпигун: завчасне виявлення та видалення більшості зареєстрованих і невідомих вірусів, черв’яків, троянських програм і руткітів. Технологія розширеної евристики дає змогу визначити раніше невідомі шкідливі програми, гарантуючи захист від нових загроз і їх завчасне знешкодження. Захист доступу до Інтернету та Захист від фішингу здійснюється шлязхом контролю

зв’язків між веб-браузерами й віддаленими серверами(включно з протоколом SSL). Захист поштового клієнта забезпечує керування поштовими комунікаціями через протоколи POP3(S) та IMAP(S);

регулярні оновлення: регулярне оновлення оброника виявлення(попередня назва – «вірусна база даних») і модулів програми найкращий спосіб гарантувати максимальний захист комп’ютера;

ESET LiveGrid (репутація у хмарі): відстежуйте репутацію запущених процесів і файлів безпосередньо в ESET Endpoint Security;

віддалене керування: ESET PROTECT дозволяє керувати продуктами ESET на робочих станціях, серверах і мобільних пристроях, які працюють у мережі, з єдиного центру. Веб-консоль ESET PROTECT(вуб-консоль ESET PROTECT) дозволяє виконувати такі операції: розгортати рішення ESET, керувати завданнями, застосовувати політики безпеки, відстежувати стан системи й швидко реагувати на проблеми або загрози на віддалених комп’ютерах;

захист від мережевих атак: аналізує вміст мережевого трафіку й захищає від мережевих атак. Увесь трафік, який вважатиметься шкідливим, буде заблоковано;

веб-контроль (тільки в ESET Endpoint Security): батьківський контроль дає змогу блокувати веб-сторінки, які можуть містити потенційно образливі матеріали. Крім того, керівники підприємств або системні адміністратори можуть заборонити доступ до певних попередньо визначених категорій (більше 27) і підкатегорій (більше 140) веб-сайтів.

Для нормальної роботи ESET Endpoint Security система має відповідати наведеним нижче вимогам апаратного та програмного забезпечення. Підтримувані процесори Intel або AND32-розрядний (x86) із набором інструкцій SSE2 Аабо 64-розрядний (x64), 1 ГБ або вище процесор на базі ARM63, 1ГГц або більше. Операційні системи: Microsoft Windows 11, Microsoft Windows 10. Відповідність усім системним вимогам, пов’язаним з операційною системою й іншим програмним забезпеченням, інстальованим на комп’ютері:

0,3 ГБ вільної системної пам’яті;

1 ГБ вільного місця диску;

мінімальна роздільна здатність:1024 x 768;

підключення до джерела оновлень продукту через Інтернет або локальну мережу.

Якщо дві антивірусні програми одночаснно виконуються на одному пристрої, це спричиняє неминучі системні конфлікти ресурсів, наприклад уповільнення продукту, беручи до уваги вимоги щодо продуктивності. Продукт можна ісінталювати й запускати в системах, які не відповідають цим вимогам однак рекомендується попередньо протестувати зручність використання продукту, беручи до уваги вимоги щодо продуктивності. Продукт може використовувати більше пам’яті, якщо в іншому разі вона не використовуватиметься на сильно інфікованому комп’ютері, а також коли у продукт імпортується дуже великі списки даних (наприклад, білі списки URL-адрес). Місце на диску необхідне для завантаження інсталятора, інсталяції продукту та збереження копії інсталяційного пакета в даних програми, а таклж для збереження резевних копій оновлень продукту для підтримки функції відкочування. Продукт може використовувати більше місця на диску залежно від вибраних параметрів(наприклад, коли сворюються резервні копії нових версій продукту, зберігаються дампи пам’яті або велика кількість записів журналу), а також якщо комп’ютер інфіковано(зокрема через функцію карантину). ESET рекомендує залишати на диску достатньо вільного місця для підтримки оновлень операційної системи,, а також оновлень продуктів ESET.

Отже, програмний комплекс ESET Endpoint Security для Windows призначений для забезпечення всебічного захисту робочих станцій від різноманітних кіберзагроз. Основні функції цього комплексу включають антивірусний та антишпигунський захист, фаєрвол, захист від фішингових атак, контроль пристроїі, веб-контроль та функції захисту в реальному часі. Склад комплексу також передбачає інструменти для управління оновленнями, аналізу поведінки програм, запобігання вторгненням та управління інцидентами. Завдяки своїм можливостям, ESET Endpoint Security для Windows забезпечує надійний та

комплексний захист робочих станцій, сприяючи безперебійній роботі та захисту даних користувачів.

2.3 Процеси функціонування рішення ESET Endpoint Security

ESET Endpoint Security – це платформа, яка захищає кінцеві точки під керуванням Windows, Mac, Linux і Android. Його платформа кінцевих точок має повний набір функцій, але не включає Endpoint Detection Response (EDR). Першим компонентом є сервер ESET PROTECT – це виконавча програма, яка обробляє всі дані, отримані від клієнтів, які підключаються до Сервера(через ESET Management Agent або HTTP Proxy. Для коректної обробки даних Серверу потрібне стабільне з'єднання з сервером бази даних, де зберігаються мережеві дані.

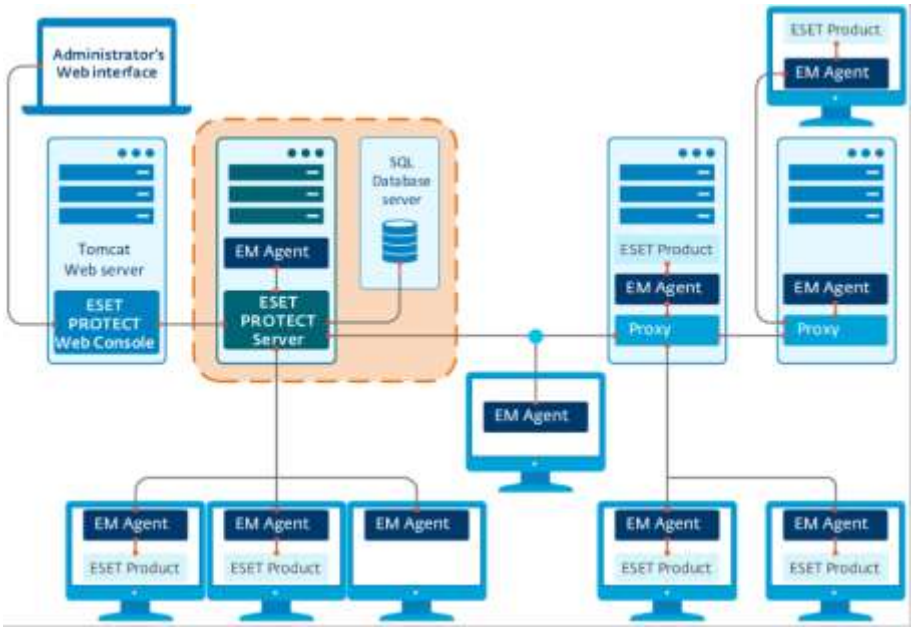

Рис. 2.2 Сервер ESET PROTECT [8]

Другим компонентом є веб-консоль ESET PROTECT – це веб-інтерфейс користувача, який дозволяє керувати рішеннями безпеки ESET у середовищі. Він відображає огляд стану клієнтів у вашій мережі та може використовуватися для віддаленого розгортання рішень ESET на некерованих комп'ютерах. Доступ до веб-консолі здійснюється за допомогою вашого браузера. Веб-консоль використовує

Apache Tomcat як веб-сервер HTTP. Під час використання Tomcat, який входить до інсталятора ESET або Virtual Appliance, він дозволяє лише підключення TLS 1.2 і 1.3 до веб-консолі.

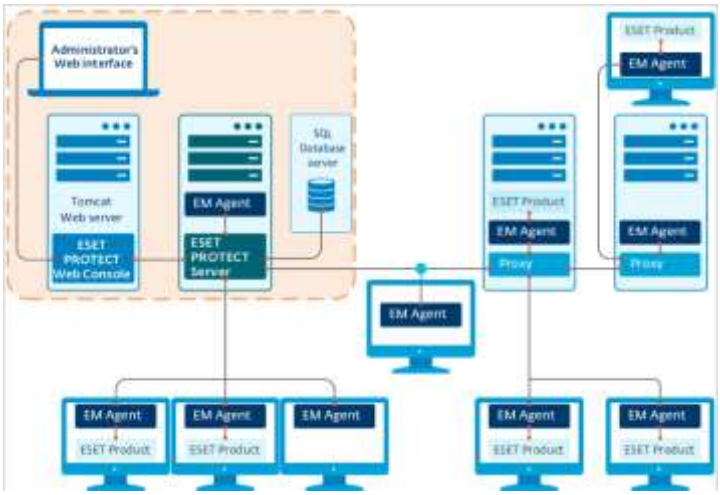

Рис. 2.3 Веб-консоль ESET PROTECT [8]

Наступним компонентом є HTTP-проксі пересилає зв’язок від агентів до сервера ESET PROTECT у середовищах, де комп’ютери агентів не можуть отримати доступ до сервера. ESET PROTECT 9 виконує налаштовану версію Apache HTTP Proxy як компонент Proxy. Після належної конфігурації Apache HTTP Proxy може діяти як проксі для ESET Management Agent. Проксі не кешує та не відкриває повідомлення, він лише пересилає його.проксі-рішення, можна використовувати з ESET Management Agent при наявності таких умов:

може пересилати зв’язок SSL;

підтримує HTTP CONNECT;

не використовує ім’я користувача та пароль.

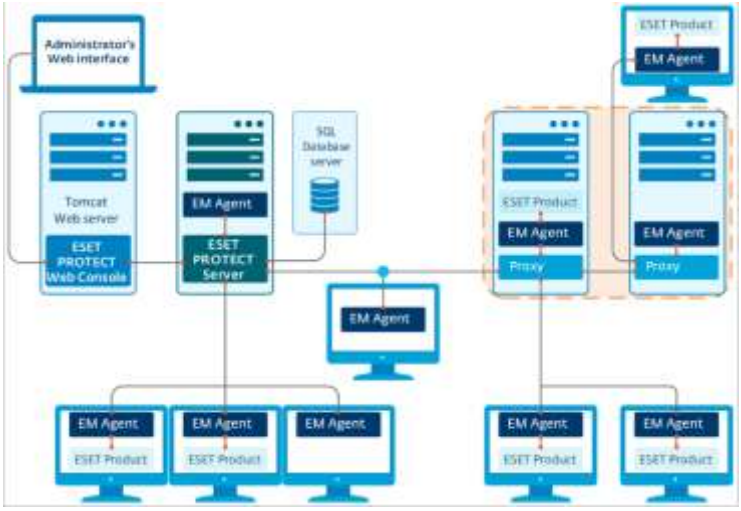

Рис. 2.4 Проксі HTTP ESET PROTECT [8]

Наступний компонет Apache HHTP Proxy – це проксі-служба, яку можна використовувати для розповсюдження оновлень на клієнтські комп'ютери. Apache HHTP Proxy зменшує навантаження на мережу, завантажуючи лише ті дані, які запитують компоненти ESET PROTECT або кінцеві продукти ESET. Якщо клієнт кінцевої точки запитує оновлення, Apache HHTP Proxy завантажує його з серверів оновлення ESET, зберігає оновлення в своєму каталозі кешу, а потім подає його окремому клієнту кінцевої точки. Параметри кешуванняESET Management Agent і Endpoint не ідентичні. ESET Management Agent може керувати налаштуваннями продуктів безпеки ESET на клієнтських пристроях. ESET Endpoint Security можна налаштувати двома способами:

локально з GUI;

із ESET PROTECT Web Console за допомогою політики.

Apache HTTP Proxy можна використовувати для збору та пересилання даних із компонентів ESET PROTECT у віддаленому місці. Одне проксі-рішення можна використовувати для кешування оновлень — Apache HTTP, а інший- для зв'язку між агентом і сервером.

Далі показано проксі-сервер (Apache HTTP Proxy), який використовується для розподілу хмарного трафіку ESET до всіх компонентів ESET PROTECT і кінуевих продуктів ESET.

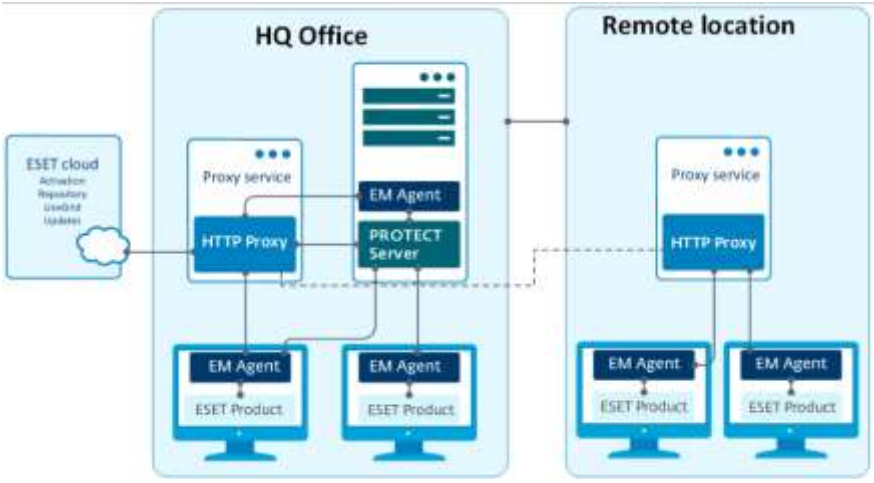

Рис. 2.5 Apache HTTP Proxy в інфраструктурі [8]

ESET Management Agent є важливою частиноюESET PROTECT.клієнти не спілкуються безпосередньо з сервером ESET PROTECT, а агент сприяє цьому зв'язку. Агент збирає інформацію від клієнта та надсилає її на сервер ESET PROTECT. Якщо ESET PROTECT Server надсилає завдання для клієнта, воно надсилається агенту, який потім надсилає це завдання клієнту. Щоб спростити впровадження захисту кінцевої точки, до складу пакету ESET PROTECT включено автономний агент ESET Management Agent. Це проста, високомодульна та легка служба, яка охоплює весь зв'язок між сервером ESET PROTECT і юудб-яким продуктом або операційною системою ESET.

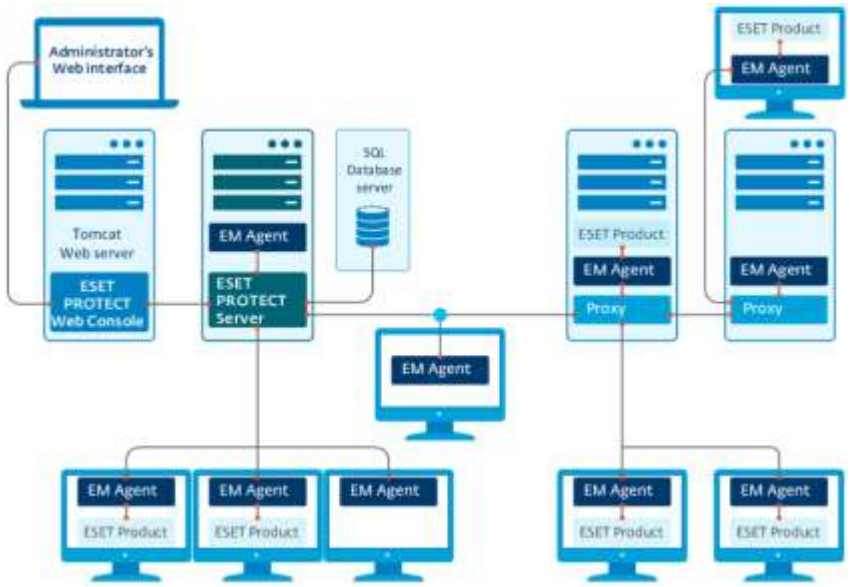

Рис. 2. 6 Архітектура ESET Management Agent [8]

Отже, процеси функціонування рішення ESET Endpoint Security характеризуються високою ефективністю та багатошаровим підходом до захисту. Система використовує машинне навчання та поведінковий аналіз для виявлення підозрілої активнсоті та запобігання невідомим загрозам. Завдяки ефективній координації цих процесів, ESET Endpoint Security забезпечує надійний і всебічний захист робочих станцій, мінімізуючи ризики та забезпечують безпеку користувацьких даних.

3 РОЗРОБЛЕНН РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ БЕЗПЕКОЮ РОБОЧИХ СТАНЦІЙ ОРГАНІЗАЦІЇ

3.1 Алгоритм реалізації управління захистом робочої станції організації на базі ESET Endpoint Security

Для початку розглянемо панель інструментів – це сторінка, яка за замовчуванням відображається після першого входу у веб-консоль ESET PROTECT. У розділі «Панель інструментів» представлено огляд мережі компанії та статуси всіх підключених пристроїв.

Рис. 3.1 Огляд існуючої мережі

На попередньо налаштованих панелях інструментів відображаються різні звіти про мережу, зокрема статус пристроїв, дані про рівень безпеки, виявлені виявлені об’єкти тощо. Можна скористатися швидкими діями, щоб негайно оновити продукт із ESET, інстальований на керованому пристрої, або отримати докладні відомості про повідомлені проблеми. Окрім того, можна створити власні персоналізовані панелі інструментів, які найкраще відповідатимуть потребам.

Далі у розділі «Комп’ютери» можна переглянути інформацію про пристрой, підключені до ESET PROTECT, і керувати ними.

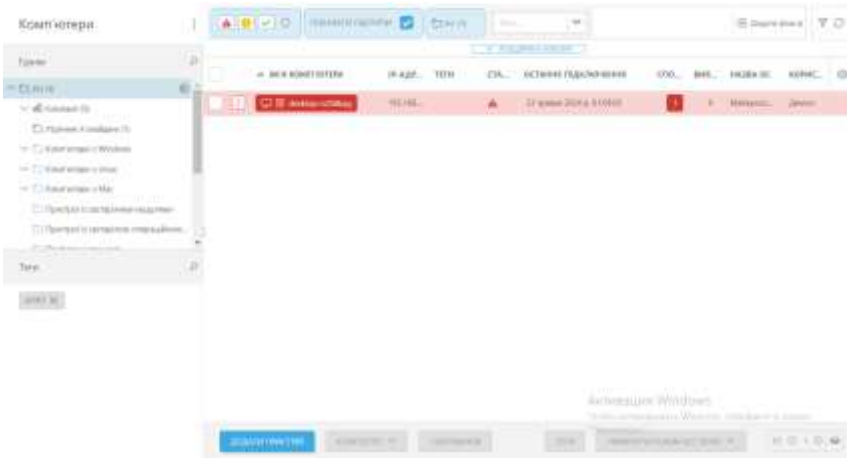

Рис. 3.2. Підключений пристрій до ESET PROTECT

Доступні докладні відомості про кожен пристрій. Зокрема статус захисту, сповіщення, інстальована операційна система, конфігурація інстальованого продукту з безпеки ESET тощо.

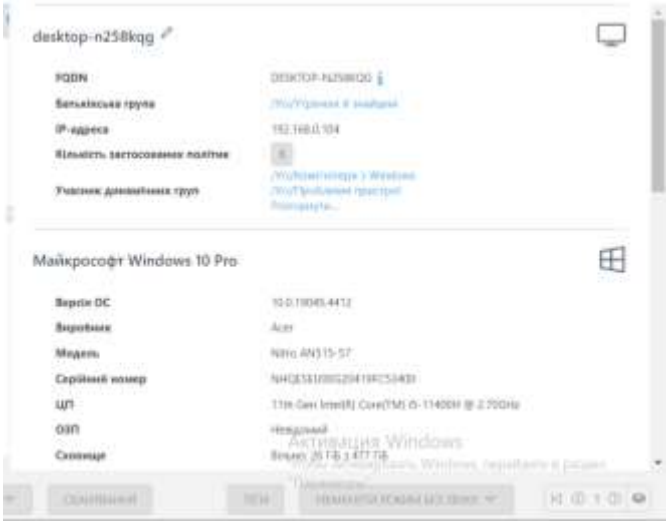

Рис. 3.3 Докладні відомості про пристрій

Також можна впорядкувати пристрої в групи відповідно до Active Directory або вручну позначити найважливіші комп’ютери тегами, щоб створити персоналізовану структуру. Є кілька способів переміщатися між всіма керованими пристроями. Можна скористатися фільтрами над таблицею або динамічними групами. Окрім того, динамічні групи дають змогу автоматизувати виконання загальних дій.

Також ESET PROTECT має ще один розділ «Виявленні об’єкти» на керованих пристроях. Кожний виявлений об’єкт містить інформацію про відповідний пристрій і рівень серйозності. Деякі виявлені об’єкти можуть автоматично оброблюватись продуктом, інші можуть потребувати дій із боку користувача. Якщо виявлений об’єкт ще не вдалося очистити, користувачу потрібно обробити його вручну. Окрім того, можна запустити детальне сканування з очищенням для папки, яка містить виявлений об’єкт. Для певних груп і пристроїів можна виключити сповіщення щодо тих виявлених об’єктів, які ви вважаєте безпечними. Виявлені об’єкти впорядковуються за часом та іншими критеріями для спрощення керування й обробки. Якщо один об’єкт виявляється багаторазового, можна отримати сповіщення лише про одне виявленнящоб полегшити його обробку.

Далі у нас розділ «Завдання» дає змогу виконувати різні дії з керованими пристроями.

Рис. 3.4. Керування пристроєм у розділі «Завдання»

Зокрема, у розділі «Завдання» можна автоматизовувати виконання повсякдених завдань. Нашлатувати ваш пристрій у цьому розділі можна використавши попередньо налаштовані завдання або налаштувати їх за власним бажанням.

Політики дають змогу віддалено налаштовувати продукти з безпеки ESET, інстальовані на керованих пристроях, відповідно до потреб вашої компанії. Можна

також використовувати попередньо визначені конфігурації, доступні в списку політики.

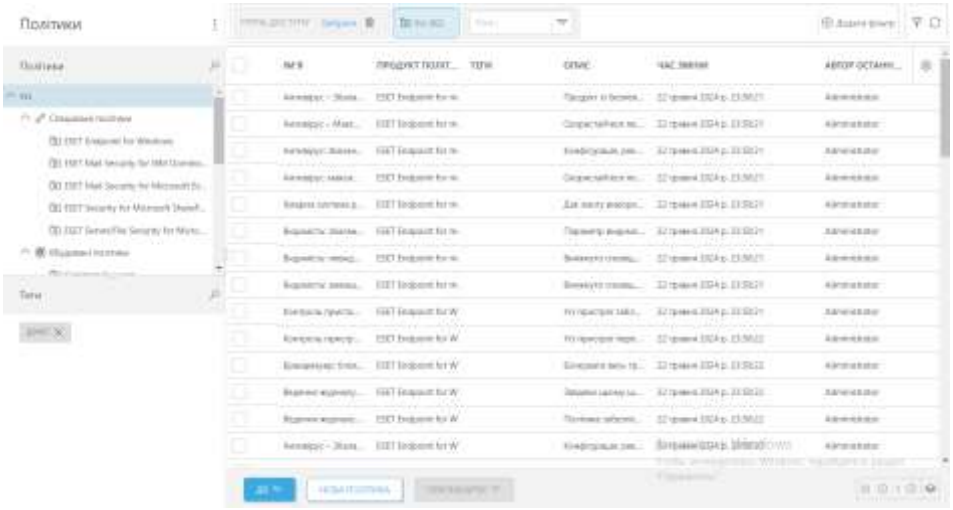

Рис. 3.5 Політики безпеки ESET керованого пристроя

Політику пожна призначати безпосередньо окремим пристроям або групам. Остаточна політика. Яка застосовується до пристрою, може складатися з кількох призначених політик. Це дає змогу керувати різними аспектами конфігурації безпеки окремо.

Також можна розглянути розділ «Сповіщення» який допомагає відстежувати загальний стан мережі та інформують вас про всі проблеми, яким потірбно приділити увагу. Вони надсилаються незалежно від того, чи ввійшли ви в ESET PROTECT.

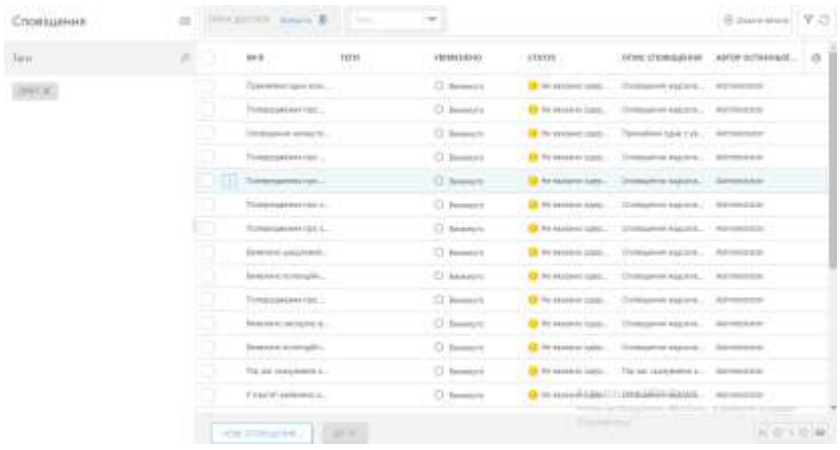

Рис. 3.6 Розділ «Сповіщення» для керованого пристрою

Можна налаштовувати різні сповіщення електронною поштою відповідно до ваших потреб, наприклад сповіщення про виявлені загрози, застарілі продукти з безпеки тощо.

Також існують автоматичні оновлення продутку функцію автоматичного оновлення в продуктах ESET з безпеки для Windows, цю функцію вже впроваджено в продуктах ESET Endpoint Security .

Отже, рішення ESET PROTECT забезпечує багаторівневий захист завдяки своїм функціям, централізована консоль управління дозволяє легко застосовувати політики безпеки до всіх робочих станцій, відслідковувати стан системи і швидко реагувати на потенційні загрози. Загалом, управління робочими станціями за допомогою ESET PROTECT забезпечує надійну та нфнктивну систему кібербезпеки, знижуючи ризики і підвищуючи рівень захисту корпоративних даних і ресурсів.

3.2 Розроблення рекомендацій щодо управління безпекою робочих станцій організації

Робочі станції, такі як комп’ютери та ноутбуки, часто є основною мішенню для кібератак. Ці притсроїв, які використовуються в усіх організаціях, зазвичай містять конфіденційну інформацію. Вони також часто підключаються до мережі, що робить їх уразливими до широкого спектру загроз, включаючи зловмисне програмне забезпечення, віруси та несанкціонований доступ. Тому зловмисники часто націлюються на ці кінцеві точки, намагаючись використовувати їхні слабкі місця.

Перелічені нижче елементи керування є елементарними та основоположними компонентами сильної політики безпеки робочої станції, дотримуючись їх, ви можете покращити безпеку робочих станцій вашої організації.

Політика надійних паролів. Запровадьте політику надійних паролів, яка вимагає користувачів вибирати складні унікальні паролі та регулярно їх змінювати. Також постійно рекомендується використовувати менеджер паролів. Надійні

паролі необхідні для захисту ваших облікових записів онлайн від несанкціонованого доступу. Слабкі паролі, такі як прості комбінації слів або цифр, можуть бути легко розшифровані або зламані хакерами за допомогою автоматизованих інструментів.

Багатофакторна автентифікація. Використовуйте багатофакторну автентифікацію, яка вимагає перевірки кількох факторів для доступу до ресурсу. багатофакторна автентифікація замінює лише одного фактора, наприклад пароля. Увімкнення двохфакторної або багатофакторної автентифікації додає додатковий рівень безпеки вашим обліковим записам в Інтернеті. Вимагання додаткових факторів, таких як код, надісланий на ваш телефон, на додаток до вашого пароля, для входу значно ускладнює для хакерів отримати неавторизований доступ до вашого облікового запису, навіть якщо вони знають ваш пароль. Імовірність того, що зловмисники зможуть надати кілька факторів перевірки, невелика, особливо якщо ви використовуєте такі фактори, як біометрична перевірка.

Захистіть від щловмисного програмного забезпечення. Установіть і регулярно оновлюйте програмне забезпечення для захисту від зловмисного програмного забезпечення та антивірусне програмне забезпечення. Одне зараження шкідливим програмним забезпеченням може вивести з ладу всю мережу, що призведе до простою, втрати продуктивності, фінансових втрат і погіршення репутації. Захист від зловмисного програмного забезпечення може забезпечити захист у режимі реального часу від зловмисного програмного забезпечення, виявляючи та видаляючи зловмисне програмне забезпечення, щоб допомогти зберегти безпеку цифрових активів компанії.

Керування виправленнями операційної системи та додатків. Регулярно оновлюйте операційні системи та додатки останніми виправленнями та оновленнями безпеки. Керування виправленнями допомагає підтримувати програмне забезпечення та системи в актуальному стані за допомогою останніх виправлень безпеки та виправлень. Це допомагає запобігти використанню відомих уразливостей, які можуть використовуватися кіберзлочинцями для компрометації кінцевих точок, мережі та даних організації.

Конфігурація брандмауера. Налаштуйте внутрішні брандмауери робочої станції для обмеження вхідного та вихідного мережевого трафіку. Ефективна конфігурація брандмауера робочої станції забезпечує додатковий рівень захисту від потенційних мережевих загроз. Брандмауери можуть запобігати несанкціонованому доступу, фільтрувати мережевий трафік, виявляти та блокувати підозрілу активність і зупиняти бічне переміщення шкідливих програм. Внутрішній брандмауер допомагає захистити систему та дані від широкого спектру загроз, включаючи віруси, зловмисне програмне забезпечення та хакерські атаки.

Шифрування файлів і папок. Шифруйте жорсткі диски робочих станцій. Це особливо важливо для захисту ноутбуків. Шифрування файлів і папок допомагає захистити конфіденційні дані, які зберігаються локально, від несанкціонованого доступу. Шифрування ускладнює для кіберзлочинців перехоплення та читання конфіденційної інформації, оскільки дані зашифровані та можуть бути розшифровані лише за допомогою ключа дешифрування. Шифрування файлів і папок також може допомогти відповідати нормам захисту даних, а в деяких випадках допомагає захистити від програм-вимагачів.

Навчання користувачів. Навчіть користувачів розпізнавати потенційні загрози безпеці та реагувати на них, а також дотримуватися найкращих методів безпеки. У багатьох випадках люди є найслабшою ланкою кібербезпеки. Підвищуючи обізнаність щодо найкращих практик кібербезпеки та загроз, співробітники можуть стати ефективною лінією захисту від кібератак, таким чином зменшуючи ризик порушення безпеки та інших кіберзагроз. Навчання з підвищення обізнаності користувачів допомагає навчити співробітників розпізнавати кіберзагрози та реагувати на них. Це включає виявлення фішингових електронних листів і повідомлень, уникнення шахрайства соціальної інженерії та безпечну поведінку в Інтернеті.

Адміністрування робочої станції. Переконайтеся, що всіма операційними системами та конфігураціями апаратного забезпечення керовано централізовано. Використовуйте мінімальну кількість облікових записів локальних адміністраторів і переконайтеся, що цими обліковими записами безпечно керувати. Центральне

адміністрування робочих станцій допомагає забезпечити належне керування, оновлення та обслуговування всіх окремих робочих станцій, що полегшує їх захист. Крім того, застосування віддаленого адміністрування також дозволяє швидко виявляти та усувати загрози безпеці, мінімізуючи вплив порушень безпеки. Це зменшує ризик кібератак, таких як зараження зловмисним програмним забезпеченням і витік даних, а також вплив людських помилок, які можуть виникнути під час ручного оновлення та обслуговування.

Блокування робочих станцій. Переконайтеся, що робочі станції заблоковано після встановленого періоду бездіяльності. Вкрай важливо блокувати робочі станції, щоб запобігти несанкціонованому доступу до конфіденційних даних і систем. Коли робоча станція залишається без нагляду та розблокована, до неї може отримати доступ будь-хто, хто має до неї фізичний доступ, потенційно скомпрометувавши конфіденційну інформацію або сприяючи зловмисній діяльності.

Резервне копіювання та відновлення. Регулярностворюйте резервні копії даних робочої станції та впроваджуйте процедури відновлення. Резервне копіювання та відновлення робочих станцій забезпечують доступність і цілісність даних у разі кібератаки, яка спричинила втрату, шифрування або пошкодження даних. За допомогою резервного копіювання копія важливих даних зберігається в безпечному місці, окремо від робочої станції, і може використовуватися для відновлення даних у разі атаки. Регулярно створюючи резервні копії важливих даних із кінцевих точок і маючи план відновлення, організації можуть запобігти втраті даних і забезпечити безперервність бізнесу.

Отже, впровадження цих заходів безпеки може допогти зменшити ризик і радіус вибуху інцидентів безпеки, а також захистити конфіденційні дані, які зберігаються на робоичх станціях.

ВИСНОВОК

В роботі проведено дослідження проблеми захисту робочих станцій від програм-вимагачів на базі ESET Endpoint Security.

Встановлено, що організації все більше застосовують продукти для захисту інформації в своїх організаціях. Разом з тим загострюється проблеми безпеки, такі як фішингові атаки, шкідливе програмне забезпечення, програми-вимагачі, які стають більш поширеними, ніж будь-коли. За останні кількароків кількість кіберзагроз робочим станціям зросла, що робить рішення для безпеки важливим для організацій.

Проаналізовано призначення та основні функції рішення ESET Endpoint Security – це комплексне рішення з кібербезпеки, призначене для захисту робочих станцій(комп'ютерів) в корпоративних середовищах віл різних кіберзагроз, включаючи програми вимагачі. Основні функції які виконує ESET Endpoint Security це антивірусний захист, механізми виявлення в реальному часі, фіpефол та захист від вторгнень, антифішинг, захист від програм-вимагачів.

Рекомендації, розроблені на основі дослідження, спрямовані на підвищення ефективності процесів розробки та забезпечення робочих станцій організації, включають необхідність неперервного навчання персоналу та використання рішення методології ESET Endpoint Security. Реалізація таких рекомендацій дозволить організаціям покращити свої стратегії кіберзахисту, мінімізувати ризики та ефективно реагувати на постійно змінювані кіберзагрози.

Таким чином, правильний захист робочих станцій організації при застосуванні продуктів захисту інформації має забезпечити ефективний захист корпоративних даних та кібербезпеку інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Calibrating expansion: 2023 annual cybersecurity report - security roundup. *Trend Micro (DE) | Branchenführende Plattform für Cybersicherheit*. URL: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/calibrating-expansion-2023-annual-cybersecurity-threat-report#:~:text=Our%20continuous%20surveillance%20and%20research,of%20the%20expanding%20attack%20surface (date of access: 23.05.2024).

2. Securing privileged access overview - Privileged access. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/security/privileged-access-workstations/overview (date of access: 23.05.2024).

3. (URL: https://www.trellix.com/assets/solution-briefs/trellix-endpoint-protection-platform.pdf (дата звернення: 23.05.2024).

4. *Blue Connections IT – We Design IT, Build IT, and Manage IT*. URL:https://www.blueconnections.com.au/wpcontent/uploads/2020/03/sophos_intercept_x_whiteboard.pdf (дата звернення: 23.05.2024).

5. https://www.bluevoyant.com/knowledge-center/microsoft-defender-for-endpoint-architecture-features-and-plans

6. Agent | ESET PROTECT. *ESET Online Help*. URL:https://help.eset.com/protect_install/90/enUS/arch_agent.html?arch_server.html (date of access: 23.05.2024).

7. ESET Endpoint Security | ESET Endpoint Security |. *ESET Online Help*. URL: https://help.eset.com/ees/10.0/uk-UA/ (date of access: 23.05.2024).

8. ESET PROTECT on-prem 11.0. *ESET Online Help*. URL:https://help.eset.com/protect_install/11.0/ruRU/arch_server.html?arch_server.html (date of access: 23.05.2024).

9. Top IT security policies to implement: workstation security copy - cynomi. *cynomi*. URL: https://cynomi.com/blog/top-it-security-policies-to-implement-workstation-security-copy/ (date of access: 23.05.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)