ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ РЕАГУВАННЯ НА ІНЦИДЕНТИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА БАЗІ ПЛАТФОРМИ ESET PROTECT»

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

КИЇВ – 2022

ЗМІСТ

Стор.

ВСТУП 4

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ 7

1.1. Призначення, структура, функції та умови функціонування корпоративної інформаційної системи 7

1.2. Аналіз проблеми реагування на інциденти в корпоративній інформаційній системі 16

1.3. Мета та завдання реагування на інциденти в корпоративній інформаційній системі 22

1.4. Аналіз технології реагування на кіберінциденти в корпоративних інформаційних системах 24

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РЕАГУВАННЯ НА ІНЦИДЕНТИ НА БАЗІ ПЛАТФОРМИ ESET PROTECT 33

2.1. Призначення, можливості та функції ESET Protect 33

2.2. Компоненти та архітектура рішення ESET Protect 36

2.3. Призначення та архітектура рішення ESET Dynamic Threat Defense 47

2.4. Призначення та архітектура рішення ESET Endpoint Security 53

2.5. Вимоги до системи для інсталяції ESET Protect 56

2.6. Можливості щодо адміністрування ESET Protect 60

3 РОЗРОБЛЕННЯ ПОРЯДКУ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ РЕАГУВАННЯ НА ІНЦИДЕНТИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА БАЗІ ПЛАТФОРМИ ESET PROTECT 63

3.1. Розроблення порядку застосування технології реагування на інциденти в корпоративній інформаційній системі на базі платформи ESET Protect 63

3.2. Розроблення рекомендацій щодо застосування технології реагування на інциденти кібербезпеки в межах підприємства 81

ВИСНОВКИ 88

ПЕРЕЛІК ПОСИЛАНЬ 90

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ) 93

ВСТУП

Актуальність дослідження. З кожним днем до глобальної мережі під'єднується все більше пристроїв. Ця тенденція відбувається внаслідок характеру посиленого технологічного розвитку останніх десятиліть. Суспільство, як окремо, так і в виді корпоративних структур, дедалі більше користується складними комп'ютерними пристроями та опирається на інформацію, що представлена у цифровому вигляді. Таким чином, виникає сильна залежність побутових та бізнес процесів від інформації, що надається цифровими каналами зв'язку. Ця залежність призводить до необхідності вести посилений контроль каналів передачі даних, а також формувати спеціальні департаменти, що спеціалізуються на захисті інформації.

Витрати на утримання команд та розробку програмного забезпечення для протидії небажаному втручанню в роботу інформаційних ресурсів хоч і значні, але значно менші, чим потенціальні втрати в разі викрадення, модифікації або несанкціонованого розкриття важливих даних. Шкоду від вдалих атак, здійснених на інформаційні системи, можна розцінювати як з точки зору матеріальних втрат, так і з точки зору репутаційних втрат, які в свою чергу тісно взаємопов'язані між собою в корпоративному світі.

Необхідність масштабування корпоративних інформаційних систем є тим самим чинником, що робить саму інформаційну структуру підприємства складнішою з технічної точки зору та створює безліч розгалужень в середині самої системи, які потребують чіткого контролю. Вміщуючи все більше цінних та стратегічно важливих даних, ці системи викликають посилений інтерес конкурентів та угрупувань зловмисників. Реагування на інциденти в корпоративних інформаційних системах потребує достатньо високої кваліфікації відповідних спеціалістів, а також професійного програмного комплексу, що відповідає ключовим параметрам захисту в сучасному кіберпросторі.

Реалії сьогодення демонструють, що процес захисту від втручання в інформаційну систему підприємства вимагає від спеціалістів проведення великої кількості дій та надзвичайної пильності, яку часом неможливо досягти без спеціалізованих програмних рішень. Шляхом впровадження програмних засобів можна досягти найвищих показників в якості підготовки установи до можливих кібератак, а також в запобіганні втручанням та виявленні вразливих місць. Наведені фактори мають значний вплив на зменшення частоти появи інцидентів кібербезпеки інформаційних систем та ступеню тяжкості наслідків їх впливу на підприємство.

Важливо мати розуміння того, що в будь-який момент приватна або державна структура може стати мішенню для кібератаки. Тому важко переоцінити важливість розробки та підготування превентивних заходів, які можуть перетворити потенційну кризову ситуацію кібербезпеки у черговий недопущений кіберінцидент. Швидкість і якість, з якою корпоративна структура здатна відреагувати на інциденти, є ключовим фактором впливу на рівень заподіяної шкоди підприємству, витрати, а також лідерську позицію підприємства у корпоративному світі.

Об'єкт дослідження – процес забезпечення кібербезпеки корпоративної інформаційної системи.

Предмет дослідження – технологія реагування на інциденти в корпоративній інформаційній системі.

Мета роботи – розробити порядок застосування технології реагування на інциденти в корпоративній інформаційній системі та рекомендації щодо застосування технології реагування на інциденти в корпоративній інформаційній системі на базі платформи ESET Protect.

Наукові завдання:

дослідити існуючі проблеми реагування на інциденти корпоративних інформаційних систем;

встановити сутність завдань реагування на інциденти в корпоративній інформаційній системі;

проаналізувати існуючі технології реагування на інциденти в корпоративній інформаційній системі;

проаналізувати методи та засоби реагування на інциденти в корпоративній інформаційній системі;

дослідити можливості застосування програмного комплексу ESET Protect з метою розробки порядку застосування технології реагування на інциденти в корпоративній інформаційній системі.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, відтворення процесу реагування на інциденти кібербезпеки за допомогою платформи ESET Protect.

Ступінь наукової розробки. Встановлення та запуск системи виявлення і реагування на інциденти ESET Protect відбувається на основі тієї інформаційної бази, що надана виробником продукту, але чітких комплексів рекомендацій щодо впровадження та розгорнення захисту через використання платформи ESET Protect у доступі немає. Для даного продукту вперше одержано покрокову методику захисту в мережі, а також методику захисту файлової системи кінцевих точок. Удосконалено процедуру запуску системи з наданням практичних рекомендацій з порядку дій при роботі з локальним сервером ESET Protect. Також, в рамках проведення даної роботи, вдосконалено роботу системи реагування для можливості її використання на підприємствах різного масштабу без втрати якості реагування.

Практичне значення одержаних результатів полягає в розробці порядку застосування технології реагування на інциденти в корпоративній інформаційній системі та наданні рекомендацій щодо його впровадження. Впровадження розроблених методів захисту надає змогу підприємству вчасно, а головне, якісно реагувати на інциденти в інформаційній системі, що значно покращить загальний рівень безпеки компанії та виведе її на високий рівень довіри серед суспільства.

Результати магістерської роботи були апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2021 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

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

Традиційно корпоративні інформаційні системи створювалися для підтримки конкретних бізнес-функцій, і, таким чином, вони розроблялись у повній відповідності з функціональною структурою організації. Це призвело до того, що в одній організації було розгорнуто широкий спектр систем, кожна з яких покладається на окрему технологію, що слугує конкретній цілі в певній функціональній сфері (наприклад, логістика, людські ресурси, управління роботою з клієнтами, управління ланцюгом поставок тощо).

Ранні системи часто мали проблеми в налаштуванні та масштабуванні, а заміна чи вдосконалення їх складових була практично неможливою. Залежність систем від платформи та технологій призвела до бажання організацій розробляти та впроваджувати довгострокові технологічні рішення.

Вимоги бізнесу створили додатковий тиск на технічну інфраструктуру, вимагаючи оперативності та кращого узгодження між бізнесом та інформаційними технологіями (ІТ). Зростаюча складність і динаміка бізнес-середовища вимагає створення надійної ІТ-інфраструктури для забезпечення інтелектуального спільного використання ресурсів і динамічного створення та розподілу послуг.

Реалізація повного потенціалу корпоративної інфраструктури інформаційних систем полягає не тільки в доданні нових послуг до існуючих систем, а все більше в перехресній інтеграції, тобто в посиленні сумісності між собою додатків для підтримки бізнес-функцій, які охоплюють традиційні процеси взаємодії з клієнтом та всередині організації. Це призвело до гострої потреби у ширшому внутрішньому та міжорганізаційному співробітництві, а з роками призвело до розвитку та поширення систем, які розглядають технічні, ділові та адміністративні додатки в

корпоративній перспективі. Цей підхід надав перевагу відкритим сучасним системним архітектурам, на відміну від застарілих закритих монолітних систем.

Під тягарем виникаючих потреб та з урахуванням того, що організації все більше прагнуть впорядкувати та покращити свою діяльність, прийняття комплексної стратегії інтеграції інформаційних систем стає обов'язковим, а саме стратегії, яка поєднує корпоративну діяльність, яка традиційно між собою не перетинається для того, щоб мати можливість пропонувати ринку нові послуги. Інформаційна система повинна дозволяти організаціям швидко реагувати на зміни в бізнесі та підлаштовуватись під стрімкий економічний та технологічний прогрес.

Існують різні типи інформаційних систем, і кожна з них виконує свою роль. Системи бізнес-аналітики (BI), наприклад, можуть перетворити дані на цінну інформацію. Така технологія дозволяє швидше та точніше звітувати, приймати кращі бізнес-рішення та ефективніше розподіляти ресурси.

Іншою важливою перевагою є візуалізація даних, яка дозволяє аналітикам інтерпретувати великі обсяги інформації, передбачати майбутні події та знаходити закономірності в історичних даних. Організації також можуть використовувати програмне забезпечення планування ресурсів підприємства (ERP) для збору, керування та аналізу даних у різних сферах, від виробництва до фінансів та бухгалтерського обліку. Як і інші інформаційні системи, ERP надає корисну інформацію та допомагає прийняти рішення щодо подальших кроків. Це також полегшує дотримання нормативних вимог, підвищує безпеку даних і покращує обмін інформацією між відділами. Крім того, це допомагає переконатися, що всі фінансові записи є точними та актуальними. У довгостроковій перспективі програмне забезпечення ERP може знизити експлуатаційні витрати, покращити співпрацю та підвищити дохід підприємства.

Важливою тенденцією використання корпоративних інформаційних систем є можливість компаній використовувати інструменти аналізу даних для збору інформації про споживчі покупки та інші економічні тенденції, в тому числі вже згадані системи BI. Це дозволяє керівництву трансформувати цю інформацію в цілі

та напрямки майбутніх операцій, а також допомагає в визначенні та прийнятті стратегічного плану розвитку підприємства.

Окрім всього іншого, інформаційні системи слугують для своєчасного надання інформації менеджерам, в якості допомоги в прийнятті обґрунтованих бізнес-рішень, наприклад, для прогнозу продажів на квартал, або для вибору підходящого моменту в пропозиції послуг клієнтам.

Хоч тенденція йде на спад, але й сьогодні деякі дрібні підприємства можуть обійтися без програмного забезпечення та інформаційних систем, як явища, але, роздивляючись корпоративну інфраструктуру глобально, важко уявити роботу організацій без потужного програмного забезпечення, на яке часом виділяються цілі дата-центри, оскільки важливість швидкої обробки великих обсягів даних в сучасних мегакорпораціях важко переоцінити.

Насправді, сьогодні можна дешево зберігати та опрацьовувати величезні обсяги інформації, використовуючи хмарні рішення. Навіть дрібні підприємства, котрі ще не користуються інформаційними системами можуть дозволити собі зберігати купу детальних записів і використовувати їх для вивчення моделей купівлі покупцями та для контролю поставок, а також інших виробничих потреб.

Оскільки інформаційні системи здобули широке розповсюдження, та мають низький технічний та фінансовий поріг входу для їх експлуатації, то питання імплементації та підтримки таких програмних рішень в дрібних організаціях є більше питанням готовності керівництва в переведенні підприємства на нову інфраструктуру та зв’язаних з цим трудових витрат, а також достатньої кваліфікованості людського ресурсу підприємства.

Функціонал інформаційних систем завжди повинен базуватись на вимогах тих працівників, хто буде їх використовувати. Правильна корпоративна інформаційна система повинна пропонувати наступні функції:

гнучкість: система повинна дозволяти здійснювати аналіз та оцінку даних з декількох джерел у міру необхідності та кількома способами залежно від виробничих потреб;

простота у використанні: працівникам не потрібні глибокі професійні навички в області інформаційних систем, щоб успішно користуватись та отримати те, що їм потрібно;

універсальність: інформаційні системи повинні однаково зручно використовуватись і професіоналами, і рядовими працівниками, тобто бути адаптованими до різних за рівнем навичок, потреб та знань;

співпраця: система повинна сприяти зручному та якісному спілкуванню між керівництвом та персоналом по всій компанії.

Інформаційні системи використовують дані, внесені працівниками, або автоматично згенеровані системами бізнес-аналітики, що зберігаються в комп'ютерних базах даних, для надання необхідної інформації за запитом. В даному випадку база даних розглядається в якості організованої сукупності взаємопов'язаних даних, що відображають основний аспект діяльності підприємства. До функціональних обов'язків інформаційної системи можна віднести [1]:

фіксацію внутрішніх даних організації та середовища її існування, іншими словами, зовнішніх даних;

збереження елементів бази даних протягом тривалого періоду часу;

маніпулювання відповідними елементи даних за потреби, та отримання користувачем необхідної інформації;

представлення вихідної інформації в різних формах, в залежності від запиту, результату опрацювання, рекомендацій системи, або транзакцій.

Інформаційна система, по суті, складається з п'яти компонентів: апаратного забезпечення, програмного забезпечення, бази даних, мережі та людей [2] (рис. 1.1). Ці п'ять компонентів об'єднуються для введення даних, обробки даних, їх експорту, зворотного зв'язку та здійснення операцій всередині системи.

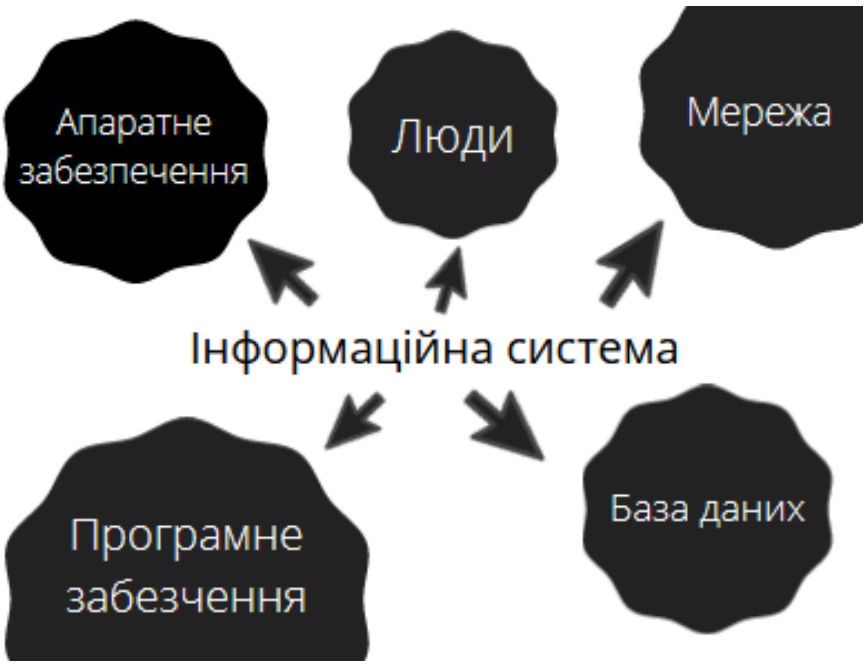


Рис. 1.1. Ключові елементи інформаційної системи

Великі організації зазвичай використовують розподілені комп'ютерні системи, від потужних серверів паралельної обробки даних, розташованих в центрах обробки даних, до широко розсіяних по світу персональних комп'ютерів і мобільних пристроїв, інтегрованих в інформаційні системи організації.

Датчики все ширше поширюються у фізичному та біологічному середовищі для збору даних і, у багатьох випадках, для здійснення контролю за допомогою приводів. Разом з периферійним обладнанням, таким як магнітні або твердотільні диски, пристрої введення-виведення та телекомунікаційне обладнання, вони становлять апаратне забезпечення інформаційних систем.

Вартість обладнання з кожним роком статистично знижується, а швидкість обробки та ємність зберігання значно зростає. Такий розвиток описує закон Мура, що стверджує двократний зріст потужності мікропроцесорів, які є центрами обчислювальних пристроїв, приблизно кожні 18-24 місяці. Проте, використання електроенергії обладнанням та його вплив на навколишнє середовище викликають занепокоєння, особливо варто відмітити зростаючий дефіцит напівпровідників, що використовуються в мікропроцесорах та постачаються виробникам обчислювальної та побутової техніки, а також в автомобільну промисловість, де цей дефіцит найбільш помітний користувачеві.

Все частіше комп’ютерні послуги та послуги сховища надаються в якості хмарного рішення — із спільного обладнання, доступ до якого здійснюється шляхом телекомунікаційних мереж.

Така складова інформаційних систем як комп’ютерне програмне забезпечення поділяється на два широкі класи: системне програмне забезпечення та прикладне програмне забезпечення.

Основним системним програмним забезпеченням є операційна система. Вона керує апаратним забезпеченням, файлами даних і програмами, а також іншими системними ресурсами і надає користувачеві засоби для керування комп’ютером, як правило, через графічний інтерфейс користувача.

Прикладне програмне забезпечення — це програми, призначені для виконання конкретних завдань користувачів. Додатки для смартфонів стали звичайним способом доступу людей до інформаційних систем. Іншим прикладом можуть бути пакети програм загального призначення з їх електронними таблицями та програмами обробки текстів, наприклад, Microsoft Office 365, а також «вертикальні» програми, які обслуговують певний галузевий сегмент, наприклад, програму, яка планує, маршрутизує та відстежує доставку пакетів для поштових підприємств.

Великі фірми використовують готові ліцензовані програми від постачальників програмного забезпечення, налаштовуючи їх відповідно до своїх конкретних потреб, а також розробляють свої особисті додатки власними силами чи на сторонній основі. Компанії також можуть використовувати програми, що поставляються як програмне забезпечення як послуга (модель SaaS) з хмари через доступ до Інтернету. Приватне програмне забезпечення, яке підтримується його постачальниками, зіштовхується з проблемою наявності програмного забезпечення з відкритим кодом, доступним в мережі для безкоштовного використання та модифікації за ліцензією, яка захищає його майбутню доступність.

Багато інформаційних систем є засобами доставки даних, що зберігаються в базах даних. Типовими прикладами баз даних є записи про співробітників та каталоги продуктів. Бази даних підтримують операції та функції управління

підприємства. Сховища даних містять архівні дані, зібрані протягом тривалого часу, які можна використати для розробки та пропозиції нових продуктів, покращеного обслуговування існуючих клієнтів або зв'язку з потенційними клієнтами. Такі бази створюються шляхом накопичення даних про тих, хто оплачував карткою товари виробника, телефонував на гарячі лінії за консультацією, залишав свої дані в формах на сайті чи у відділеннях, також існує практика передачі та обміну персональними даними клієнтів між організаціями, яка може бути прописана в політиці користування сервісом, або здійснюється нелегально, без дозволу клієнтів, що є кримінальним порушенням.

Масовий збір і обробка структурованих числових даних, а також текстових даних, які часто збираються в Інтернеті, переросли в широкий термін, відомий публіці як «великі дані», або «Big Data», оскільки термін часто не перекладається, а використовується в оригіналі. Рішення, прийняті на основі вивчення великих даних, дають серйозні переваги в роботі з клієнтською базою. Ринок «Big Data» росте з року в рік, аналітики прогнозують його ріст майже вдвічі до 2025 року [3] (рис. 1.2).

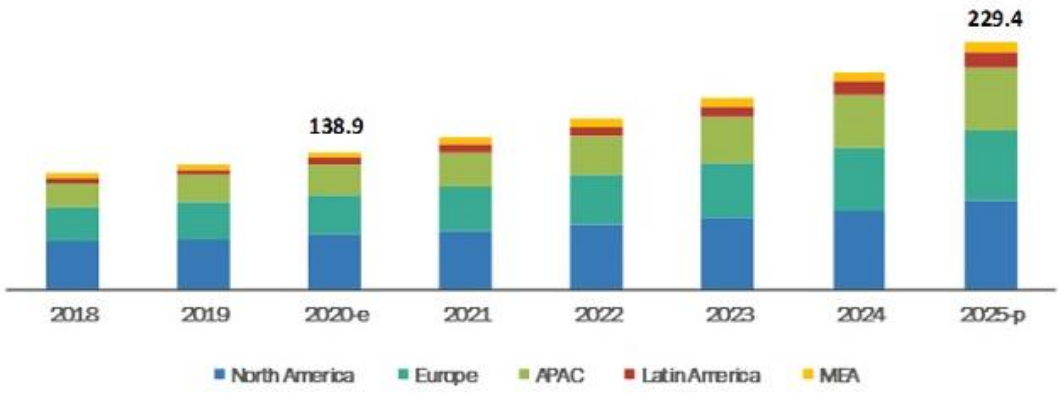


Рис. 1.2. Фактичні та прогнозовані об'єми вартості ринку «великих даних» за регіонами (виражені у мільярдах доларів США) [3]

Перевагами використання «великих даних» може бути економія ресурсів у результаті уникнення марнотратства організації на неробочі методи пошуку шляхів зацікавлення клієнтів, також основною перевагою є надання рекомендацій щодо

нових продуктів на основі інтересів конкретного користувача. Великі дані дають змогу підприємству створювати інноваційні бізнес-моделі.

Мережа, як складова структури інформаційних систем, використовується для з'єднання комп'ютерних систем і портативних пристроїв та для передачі інформації. З'єднання встановлюються за допомогою дротового або бездротового зв’язку. Дротові технології включають коаксіальний кабель і оптоволокно. Бездротові технології, переважно засновані на передачі мікрохвиль і радіохвиль, підтримують мобільні обчислення, без прив’язки до місця з’єднання. Розповсюдження інформаційних систем відбувається ще в наслідок їх взаємодії з обчислювальними пристроями, вбудованими в фізичні об’єкти. Прикладом слугують RFID-датчики, що приєднані до пакунків, які рухаються ланцюгом поставки, для відстеження їх поточного місцезнаходження та стану.

Залежно від потреб організації можливі різні конфігурації комп’ютерної мережі [4]:

локальні мережі: об’єднують комп’ютери на певній території, наприклад, в офісній будівлі чи академічному просторі;

мережі міського району: охоплюють обмежену густонаселену територію і є електронною інфраструктурою «розумних міст»;

глобальні мережі: з’єднують центри обробки даних, якими часто керують різні організації.

Однорангові мережі без централізованого контролю забезпечують широкий обмін даними. Через мережу користувачі отримують доступ до інформаційних ресурсів, таких як великі бази даних, а також здійснюють контакт з колегами, клієнтами, друзями або людьми, які розділяють їх професійні чи особисті інтереси. Послуги Інтернет-типу можуть надаватися в межах організації для виключного використання нею різних інтранетів, які доступні через браузер. Наприклад, інтранет може бути розгорнутий як портал доступу до спільної корпоративної бази документів. Щоб зв’язатися з діловими партнерами через Інтернет приватним і безпечним способом, в екстранеті, шляхом шифрування повідомлень, створюються, так звані, віртуальні приватні мережі.

Сучасна мережева інфраструктура демонструє зростаючу тенденцію переходу до хмарних обчислень (рис. 1.3). Ресурси інформаційної системи розподіляються між кількома компаніями, що призводить до ефективності використання та свободи локалізації центрів обробки даних. Програмно-визначена мережа забезпечує гнучкий контроль над телекомунікаційними мережами за допомогою алгоритмів, які реагують на потреби та доступність ресурсів в режимі реального часу.

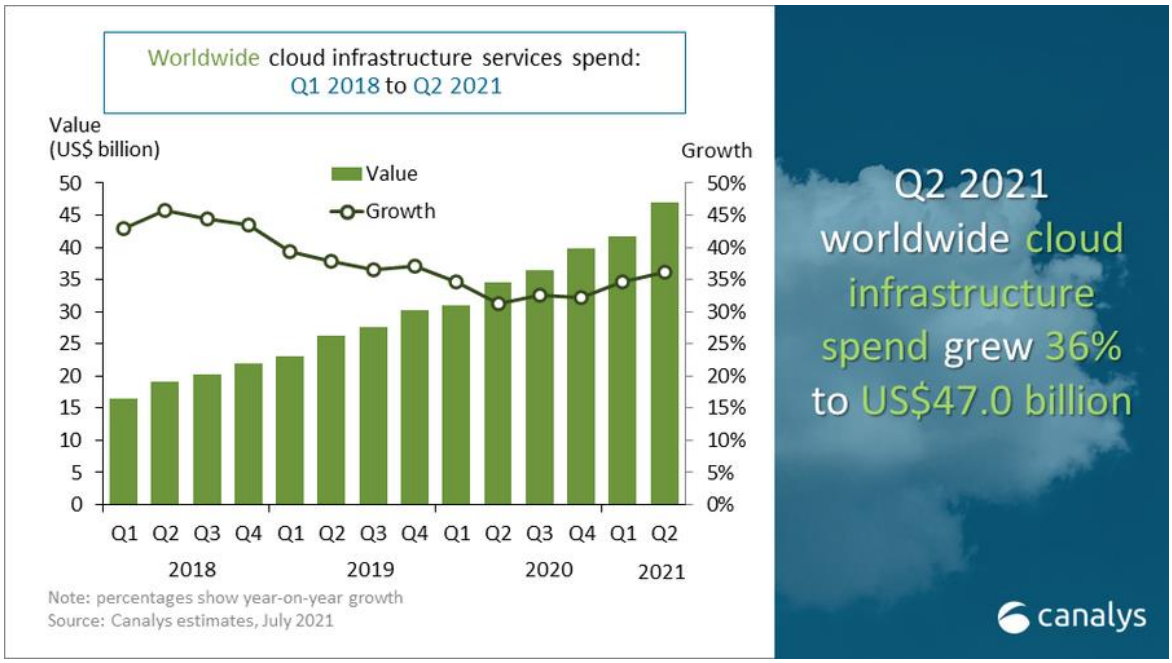


Рис. 1.3. Графік приросту вартості ринку хмарних обчислень періоду 2018-2021 років (виражений у мільярдах доларів США) [5]

На прикладі розвитку сервісів хмарних обчислень в Європі, можна помітити, що великі корпорації все ж не так активно використовують локальні рішення для забезпечення потреб своїх інформаційних систем, віддаючи перевагу, здебільшого, хмарними рішеннями, а сама тенденція набуває розвитку, порівняно з періодом 2020 року [6] (рис. 1.4).

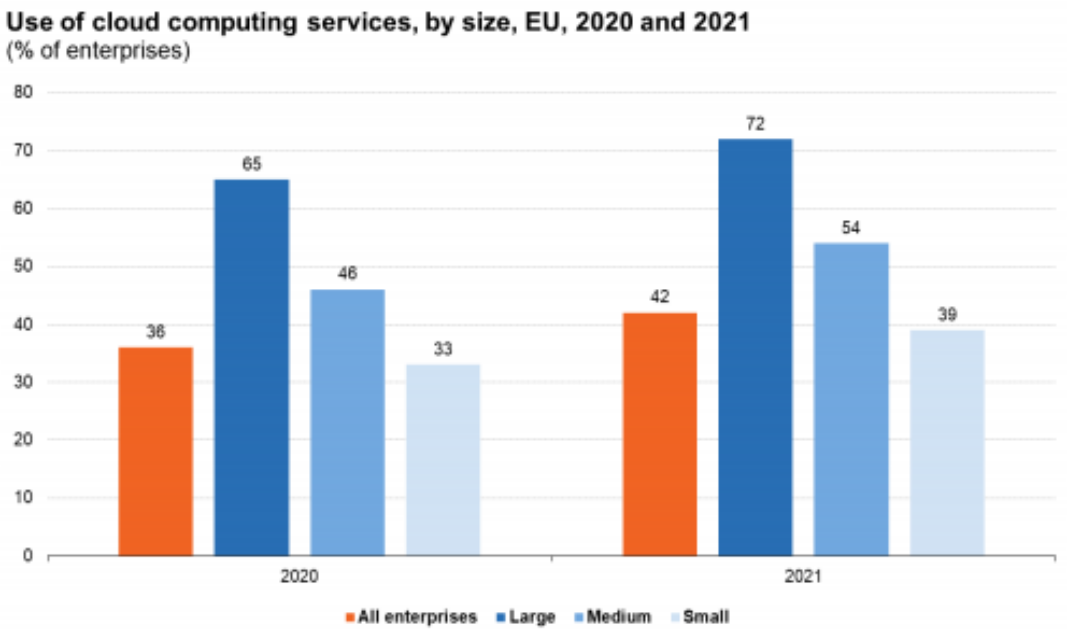


Рис. 1.4. Використання хмарних обчислень серед компаній різного масштабу у Європі [6]

Кваліфіковані кадри є важливою складовою будь-якої інформаційної системи. Технічний персонал включає операційних менеджерів, системних аналітиків, менеджерів з розробки продукту, дизайнерів, бізнес-аналітиків, адміністраторів баз даних, програмістів, спеціалістів з кібербезпеки та операторів комп'ютерів. Крім того, всі працівники організації повинні мати навички використання повного потенціалу інформаційних систем.

Процедури керування, експлуатації та обслуговування інформаційної системи є частиною її технічної документації. Наприклад, необхідно встановити процедури для запуску програми оплати податків чи нарахування коштів за відпустку, зокрема, коли її запускати, хто уповноважений на її запуск і хто має доступ до результатів.

1.2. Аналіз проблеми реагування на інциденти в корпоративній інформаційній системі

Інтернет змінює спосіб ведення бізнесу: кількість даних, які ми передаємо через Інтернет, і наша залежність від їх доступності постійно збільшуються.

Зрозуміло, що зв’язок зі світом не тільки приносить великі можливості, але й породжує нові ризики. Кіберзлочинність – це великий бізнес, і навіть найменша зловмисна атака може серйозно зашкодити репутації організації, продуктивності, цілісності інформаційної системі тощо. Жодна організація не повинна думати, що вона захищена від кіберзлочинності.

Кіберзлочинці націлені не лише на великі організації. Навпаки, невелика організація може бути більш цікавою жертвою через інформацію, яку вона обробляє, або навіть через партнерів, з якими вона працює. Варто завжди пам’ятати, що кожна організація відрізняється.

Коли справа доходить до кібербезпеки, не існує універсального рішення. Те, що буде працювати для однієї організації, буде залежати від її місії та цілей, типу інфраструктури та інформації, яка захищається, доступних ресурсів тощо. А деякі методи захисту можна буде впровадити тільки з плином часу, зіштовхнувшись з неприємною практикою реагування на інциденти.

Інциденти кібербезпеки – це ризик, який необхідно враховувати в загальній політиці управління ризиками організації. Крім того, управління інцидентами кібербезпеки означає не лише застосування технологій. Це також вимагає розробки плану, інтегрованого в існуючі процеси та організаційні структури, щоб він сприяв, а не перешкоджав критично важливим бізнес-функціям. Тому вище керівництво має брати активну участь у визначенні плану запобігання та реагування на інциденти, оскільки чітка підтримка вищого керівництва через відповідну внутрішню комунікацію та розподіл персоналу та фінансових ресурсів є ключем до успіху плану. Добре проінформований топ-менеджер буде усвідомлювати як ризики кіберзлочинності, так і свою власну зразкову роль у заохоченні всіх членів організації взяти на себе відповідальність за дотримання процедур з забезпечення кіберзахисту, наприклад, не нехтуючи базовими принципами безпечної поведінки в мережі та дотриманням рекомендацій з інформаційної безпеки.

Існує думка, що люди є найслабшою ланкою, коли йдеться про кібербезпеку організації, але важливо усвідомлювати, що члени організації мають великий потенціал в допомозі виявлення та ідентифікації інцидентів кібербезпеки. Часто

підприємства нехтують базовим принципом інформування всіх працівників організації про діючий план реагування на інциденти кібербезпеки та про їх власну роль у ньому, навіть коли це означає лише інформування окремої особи з конкретної аномалії в роботі інформаційної системи, з якою вона скоріше за все може зіткнутися.

Це може здатися банальним, але потрібно мати на увазі, що при виникненні інциденту кібербезпеки, організація не завжди можете мати доступ до файлів на корпоративних комп'ютерах. Сьогодні збереження та резервне копіювання даних не є рекомендацією, а необхідністю, без якої життєвий процес організації може зупинитись за лічені години в разі успішного вторгнення в систему зловмисниками. Навіть корисно робити друковані чи офлайн-копії будь-якого документа, який, ймовірно, знадобиться під час інциденту або кризи кібербезпеки. Коли справа доходить до резервних копій, важливо не тільки мати їх. Також дуже важливо мати резервну копію, яка жодним чином не пов'язана з рештою системи. Якщо існуюча резервна копія пов'язана зі всією системою, є ймовірність, що зараження інформаційної системи також поширеться на резервну копію, що робить резервну копію марною. Варто пам'ятати, що саме в банальних речах часто зустрічаються проблеми в кібербезпеці, оскільки про них наче б то всі знають, функції виконуються, але пильність в дотриманні їх належної якості буває дуже низька, якраз внаслідок їх базовості.

Проблемою вчасного та якісного реагування може стати вплив інциденту на існуючі канали зв'язку, наприклад, втручання в роботу системи електронної пошти. У організації мають бути альтернативні безпечні канали зв'язку в постійному доступі. Повинен бути доступ до кількох методів комунікації, і вибір методу, котрий буде найбільш ефективним для конкретного випадку, має залежати від організації, а краще, прописаним у внутрішній політиці реагування на інциденти.

Поширеною практикою серед багатьох організацій є використання номера мосту конференції, який можна налаштувати миттєво. Група реагування на інцидент і всі зацікавлені сторони повинні отримувати інформацію про номери доступу, але не про контрольний номер, необхідний для організації конференції.

Зазвичай це робить кризовий менеджер, який відповідає за керування, контроль та організацію кризових викликів.

Ще одною з проблем реагування на інциденти може виявитись недостатньо детальне ведення журналу процесів, що відбуваються в корпоративній інформаційній системі. Журнали, що фіксують дії в системі, допомагають команді з реагування та розслідування відстежити походження інциденту кібербезпеки. Це важливо не тільки для ідентифікації кіберзлочинця, а також може допомогти організації якнайшвидше повернутися до роботи та здійснити превентивні заходи щодо усунення подібного втручання зловмисників у майбутньому, що також є частиною реагування на інцидент, але тою його частинною, що здійснюється безпосередньо після самого інциденту, гарантуючи захищеність та протидію подібним атакам в подальшій перспективі.

Варто пам’ятати, що докази кіберзлочину будуть прийняті в суді лише в тому випадку, якщо вони були зібрані відповідно до всіх застосовних законів і правил. Тому, у разі процедури розслідування інциденту, варто збирати якомога більше корисних даних, такі дані можуть привести до виграшного становища, навіть після невдалого захисту, оскільки, наприклад, можуть привести до конкуруючої організації, яка здійснювала кібератаку та яка, внаслідок рішення суду, втратить позитивну репутацію, можливо втратить керівників і, як наслідок, клієнтів, а ваша організація позбудеться серйозного конкурента. Це ще один неочевидний вектор розгляду процесу реагування на кіберінциденти.

Складена документація з аналізу вразливостей дає змогу озирнутися назад і оцінити, де і чому з’явилась проблема. Крім того, документування реагування на інциденти кібербезпеки гарантує, що знання про те, що відбувається чи відбулося, буде не лише в головах кількох людей, які зараз працюють в команді реагування.

Розмір компанії визначає розмір та структуру групи реагування на інцидент. Менші компанії, які не мають ресурсів для фактичної команди, повинні хоча б призначити особу, яка буде реагувати першою, в ідеалі – когось із можливістю прийняття ділових рішень. У разі інциденту кібербезпеки він або вона повинні

звернутися до зовнішньої допомоги, але все ще залишатись тією особою, що відповідає за реагування на інциденти в організації.

Склад групи реагування на інцидент має визначатися різноманітними навичками, які необхідні для врегулювання інциденту. Для невеликих компаній деякі з цих навичок, можливо, доведеться знайти у кваліфікованих кадрів за межами організації, з якими повинна зв'язатись людина, що реагує першою на інцидент, як описувалось трохи раніше.

Чим більша організація, тим більш диференційованим повинен бути склад групи реагування на інциденти. Для більших організацій, поряд із групою реагування на інциденти, може бути створена група з кризового управління, що складається з представників корпоративного керівництва, щоб взяти на себе відповідальність за стратегічні та пов'язані з бізнесом рішення та комунікації, коли стикаються з серйозними інцидентами. Це дозволить менеджеру з реагування на інцидент більше зосередитися на технічних питаннях інциденту.

Учасниками процесу реагування може бути не лише команда реагування підприємства, оскільки цей процес досить широкий та включає в себе різні сфери діяльності: від пошуку загроз до висвітлення в медіа просторі. Загальний склад учасників процесу реагування зображений на рисунку нижче (рис. 1.5).

Рис. 1.5. Загальний склад можливих учасників процесу реагування

Незалежно від того, чи відноситься організація до малого чи середнього бізнесу, або є великим підприємством, для розробки та підтримки всіх необхідних технологій та навичок реагування на інциденти потрібні чималі кошти, в тому разі, якщо захист не перекладається на аутсорсингові підприємства. Це найбільш точно відноситься щодо навичок реагування на інциденти кібербезпеки з точки зору питань судової та юридичної консультації. Тож для швидшого реагування на інциденти з мінімальними втратами якості в роботі, іноді варто звернутися до зовнішніх партнерів з реагування на інциденти, щоб заповнити прогалину у досвіді реагування вашої організації.

До плюсів співпраці з організаціями, що надають послуги аутсорс-реагування на кіберінциденти можна віднести:

їх професійних кадрів з великим багажем знань про можливі загрози та сценарії атак, що може скоротити час на діагностику інциденту;

роботу в рамках судового поля для того щоб всі докази втручання та інформація про порушника були захищені та задокументовані відповідно до юридичного процедурного ланцюга. Ці докази можуть бути представлені пізніше в суді, якщо буде необхідність;

досвід правильного порядку роботи з інцидентами та інструменти відновлення слідів атаки з оперативної пам'яті, з віртуальних машин, з жорстких дисків і з мереж;

вони допоможуть визначити причини інциденту і запропонують поради щодо того, як стримувати, ліквідувати та усунути подібні інциденти.

Комунікація є життєво важливим компонентом кожного кроку реагування на інциденти кібербезпеки, тож нехтування нею є сильною проблемою реагування. Організації необхідно контролювати потік зв’язку, щоб забезпечити передачу потрібної інформації в потрібний момент від правильних відправників потрібним одержувачам. Це справедливо як для внутрішнього спілкування, так і для комунікацій із зовнішнім світом. Якщо з внутрішньою комунікацію все зрозуміло, то для зовнішньої варто привести такий приклад: коли інвестори, клієнти та засоби масової інформації отримують певну інформацію про інцидент, що відбувся в

компанії, її представникам слід чітко розуміти та координувати комунікацію з пресою, оскільки необачність може призвести до небажаного витоку даних, важливість яких буде перебільшена публікою та, в цілому, можуть виникнути сильні репутаційні втрати, оскільки компанія може бути необачною в комунікації та продемонструвати свою слабкість на прес-конференціях після інциденту кібербезпеки.

1.3. Мета та завдання реагування на інциденти в корпоративній інформаційній системі

Будь-який інцидент кібербезпеки, який не ліквідується належним чином або ігнорується з різних причин, рано чи пізно переросте у більшу проблему, котра в перспективі призведе до зупинки в роботі системи, її краху, або великих витрат підприємства. Кількість організацій, скомпрометованих хоча б однією успішною атакою на інформаційну систему дуже велика: майже кожна організація зіштовхувалась з успішними атаками їх систем [7] (рис. 1.6).

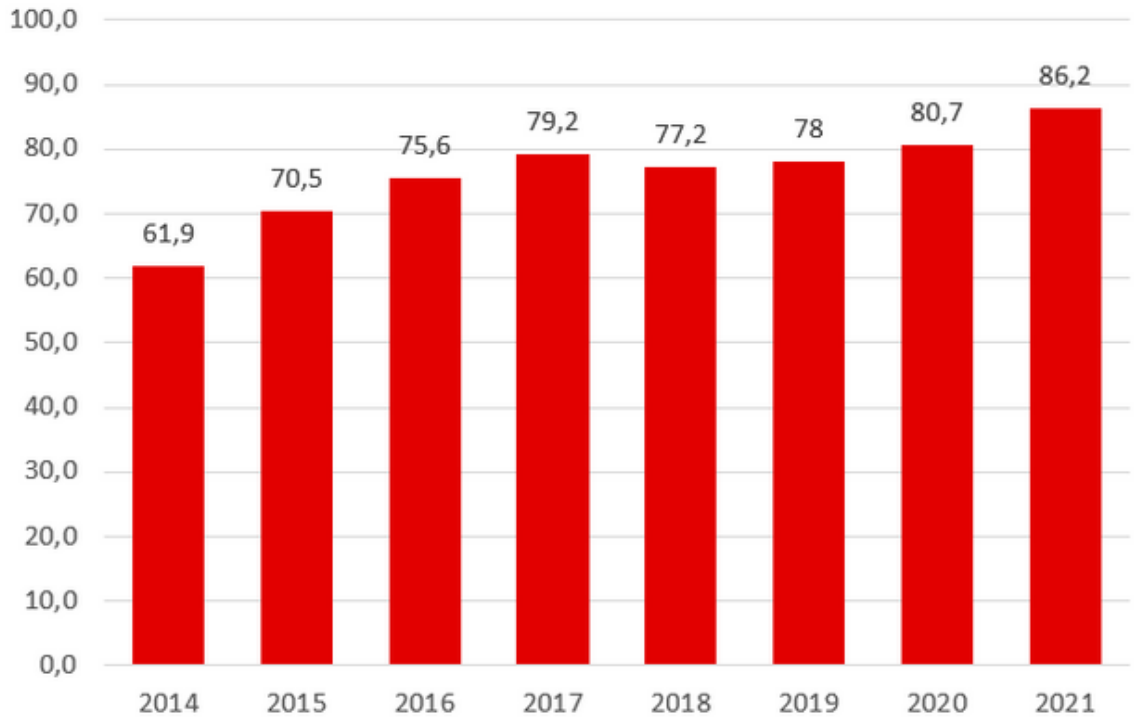


Рис. 1.6. Відсоток організацій, скомпрометованих хоча б однією успішною атакою [7]

Процес реагування на вразливості дозволяє організації не тільки здійснювати фактичну ліквідацію загроз, а й займатись підготовкою до нових для неї викликів в сфері інформаційної безпеки, базуючись на попередньому досвіді усунення вразливостей та протидії зловмисникам. Він також дає змогу започаткувати нові, або покращити старі методи припинення атаки, перш ніж вона розповсюдиться системою та заподіє шкоду активам компанії.

Реагування на події та кіберінциденти здійснюється шляхом, визначеним у корпоративному плані реагування, який формує структурованість та стратегію захисту. Він містить мету, опис можливостей, визначення та елементи реагування на інцидент. Ролі, відповідальність та кроки ескалації є загальними елементами, які розглядаються в плані реагування на інциденти.

Опис можливостей підкреслює повноваження, надані групі реагування на інциденти для вживання необхідних заходів під час боротьби з подіями. Прикладом обмеження дій команди може бути заборона переведення системи в автономний режим до підтвердження того, що стався серйозний інцидент, що не буде правильним рішенням, якщо бізнес-операції при цьому будуть перервані.

Ролі та відповідальність визначають, хто входить до групи реагування та які дії від неї очікуються під час розслідування подій. Визначення також важливі, наприклад, що таке подія, інцидент чи порушення внутрішньої політики безпеки. Викладення їх у плані позбавляє від здогадок та розбіжностей в тлумаченнях. Обговорення цих визначень на ранніх етапах усунення інциденту витрачає дорогоцінний час.

Плани реагування на інциденти розроблені для захисту організації, збереження конфіденційності, цілісності та доступності даних та інших активів, для уникнення збоїв у бізнесі та насамперед втрати репутації. Активи даних включають інтелектуальну власність, комерційні таємниці, стратегії, фінансові дані компанії та інформацію про клієнтів. Ці елементи, якщо на них впливає інцидент, можуть мати різний ступінь впливу на підприємство.

У плані реагування на інциденти викладено стратегію програми протидії атакам на інформаційну систему. Це включає цілі, ролі та відповідальність, способи аналізу та сортування подій та вимоги до ескалації.

Мета та завдання реагування на інциденти відрізняються в кожній організації, але загальні цілі такі:

захист інфраструктури, активів та бізнес-операцій організації;

зведення до мінімуму незручностей для клієнтів;

зведення до мінімуму можливості негативного інформаційного фону в новинах;

запобігання або мінімізація фінансових зобов'язань;

дотримання федеральних, державних та місцевих регуляцій.

Незалежно від того, що цілі можуть відрізнятись в різних установах, важливою залишається співпраця керівництва з командою реагування на інциденти та відділом кібербезпеки для документування цілей, які відповідають потребам організації.

В сучасному світі організаціям неможливо звести шанси кібератаки до нуля, але правильні стратегії та процеси реагування в сукупності з провідним програмним забезпеченням дозволяють мінімізувати ризики виникнення кризових ситуацій та успішних втручань в роботу систем.

1.4. Аналіз технології реагування на кіберінциденти в корпоративних інформаційних системах

Усунення загроз - це справа людини і техніки - неможливо реалізувати якісну процедуру реагування тільки за допомогою людського потенціалу або тільки за допомогою одного програмного забезпечення. Робота з загрозами починається зі збору даних, які прямо або опосередковано можуть бути пов'язані з їх метою.

Важливо визначити цілі та підхід реагування до початку процесу для попередньої оцінки успіху та приблизного розуміння необхідного часу для

усунення загрози. Без чітких цілей ліквідація інциденту може дуже сильно розтягнутись у часі та привести до втрат ресурсів компанії.

Коли команда реагування починає спостерігати за цільовим середовищем, вона спостерігає за активністю. Використовуючи свої знання про інформаційну систему та додатки в цільовому середовищі, спеціалісти починають фільтрувати нормальну робочу активність, залишаючи для дослідження тільки аномальну. Фільтруючи дані одні за іншими, все, що залишається під прискіпливим поглядом - це зловмисники та їх дії в системі. Наприклад, команда реагування може перевіряти використання командного рядку в організації, знаючи нормальні сценарії його використання, вона фільтрує всі допустимі варіанти експлуатації консолі. Якщо будь-які варіанти використання залишаються, вони можуть відноситись до додаткових допустимих варіантів, або до потенційних атак інформаційної системи. Дії, які залишаються нез'ясованими, розслідуються далі.

Організації може знадобитися звернутися за допомогою до експертів з операційної системи, розробників інформаційної системи, додатків, або інших аспектів аномальної активності. Часто, при таких перевірках, з’ясовуються нові елементи регламентного функціонування системи, які раніше були невідомі, або просто не зустрічались. Іноді, таким чином, виявляються компоненти системи, які представляють собою неправильну чи недосконалу її технічну реалізацію.

У випадку, коли була знайдена та підтверджена нетипова активність, що виявилась атакою системи, спеціалісти з кіберзахисту продовжують розслідування, для з'ясування її впливу, а також умов та місця її виникнення. По своїй суті, це аналіз першопричин, який, залежно від атаки, може звузитися до початкової фази вторгнення, але він також може перерости в розслідування широкомасштабної атаки на велику кількість систем.

Після того, як масштаб атаки стає відомим, команда реагування, зазвичай разом з мережевими, системними інженерами, розробниками програмного забезпечення та іншими, починають роботу з виправлення функціонування системи та її стабілізації.

Конкретні дії розрізняються залежно від характеру нападу, але загальні принципи наступні [8]:

видалення шкідливого програмного забезпечення та відновлення усіх змінених та видалених системних файлів;

оновлення конфігурації, дозволів та версій програмного забезпечення для запобігання подібним атакам у майбутньому;

впровадження виправлень в системі безпеки.

Організації необхідно оновити свою політику захисту, для того, щоб подібні атаки більше не виникали, або вимагали набагато більших зусиль з боку зловмисників. Оновлення включають автоматизовані системи пошуку відомих тригерів та маркерів спроб втручання. Спектр заходів може включати:

нові або оновлені правила брандмауера та IPS;

нові або оновлені сповіщення в системі керування інцидентами безпеки та подіями;

покращені процедури реагування на інцидент;

оновлення інфраструктури, додатків або архітектури безпеки;

зміни в інструментах і процесах розробки додатків, тестування, забезпечення та контролю якості;

нові правила попередження в системі моніторингу або подібних інструментах виявлення та реагування на кінцевих точках.

Інвестиції в інструменти для пошуку та усунення загроз, а також в персонал, здебільшого даремні, якщо у компанії не має взаємозв’язку між оновленням системи захисту та підсумками отриманого досвіду після реагування на інциденти. Моніторинг системи в пошуку зовнішніх втручань може виявити також інсайдерські загрози, які не менш страшні за наслідками, а інколи навіть гірші. Варто розцінювати інсайдера в компанії як зовнішнього зловмисника та відповідно з ним боротись.

Існує загальний шлях, який відомий як цикл реагування на інциденти, саме ним проходять всі виявлені вразливості інформаційних систем протягом періоду свого існування. Якщо організація володіє сформованою тактикою та

інструментами реагування на інциденти, вона вживає заходів для забезпечення готовності до вирішення інциденту на кожному етапі циклу.

Процес реагування розбитий на кілька етапів. Залежно від того, як складено план реагування, може існувати від трьох до шести етапів [25] (Рис.1.7).

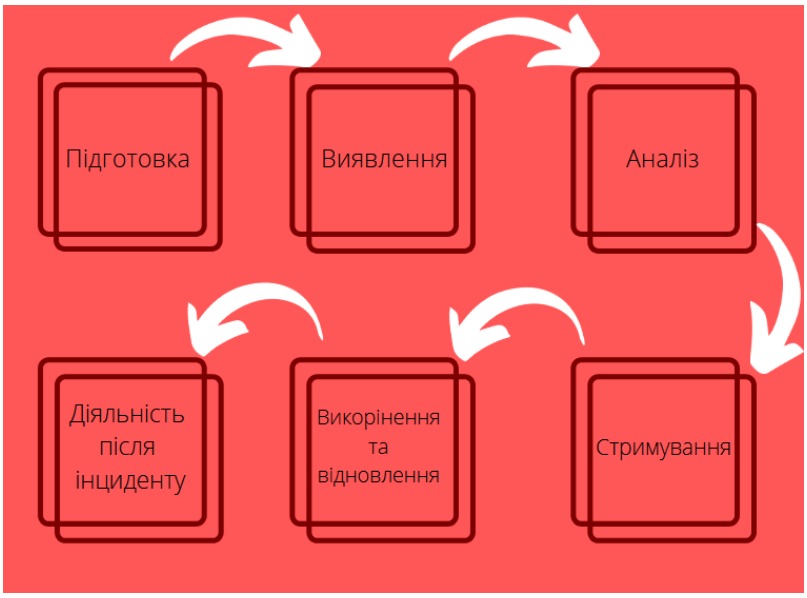


Рис. 1.7. Фази реагування на кіберінциденти

Розглядаючи перший крок циклу усунення загрози, а саме підготовку до реагування, можна зазначити, що без належної підготовки будь-яка подальша реакція на інцидент буде неорганізованою і може сильно погіршити саму ситуацію, яка була викликана атакою.

Одним із важливих компонентів підготовки є створення плану реагування на інцидент, важливість котрого вже згадувалась раніше. Після створення плану та збору команди реагування слід переконатись, що персонал пройшов належну підготовку. Це може бути досвід роботи з прийнятими на підприємстві процедурами та методикою, необхідною для розслідування інциденту.

Окрім плану, такі інструменти, як апаратне та програмне забезпечення для експертизи мають знаходитись в розпорядженні компанії та функціонувати справно. Слід проводити регулярні тренування, або майстер-класи для впевненості, що організація підготовлена до захисту інформаційної системи та повністю ознайомлена з процесом.

Такий етап реагування як виявлення потенційних інцидентів є складною роботою. Залежно від розміру організації, може проводитись мільйони окремих подій на день. Ці події можуть бути записами дій, зроблених під час звичайної діяльності, або індикаторами потенційно зловмисної діяльності.

Поєднуючи цю гору даних про події з іншими засобами контролю безпеки, які постійно сповіщають про ту чи іншу активність, цілком реально отримати ситуацію, коли аналітики переповнені даними та повинні відсівати цінні сигнали від величезного системного шуму. Навіть сучасні передові інструменти керування інцидентами та подіями безпеки, що відомі як SIEM-системи, втрачають свою ефективність, якщо вони не обслуговуються належним чином із регулярними оновленнями наборів правил, що визначають, які події кваліфікуються як потенційний інцидент, наприклад, синхронізуючи роботу SIEM-систем з базою даних MITRE ATT&CK або IBM X-Force.

Фаза виявлення є тією частиною процесу реагування на інцидент, коли організація вперше дізнається про низку подій, які, можливо, вказують на зловмисну активність. Події, які були виявлені та вказують на шкідливий вплив, класифікуються як інцидент. Наприклад, обліковий запис менеджера використовувався під час його перебування у відпустці, що викличе занепокоєння та додаткову увагу.

Сигналізація про події також може надходити із зовнішніх джерел, таких як інтернет-провайдер або кіберполіція, вони можуть виявити зловмисну активність у мережі, в якій діє організація та зв’язатися з нею для повідомлення ситуації. В деяких випадках першими, хто вкаже на потенційний інцидент кібербезпеки, можуть бути працівники компанії. Наприклад, працівник зв’яжеться зі службою підтримки та повідомить про отримання документу з невідомого джерела, після відкриття котрого, файли локальної системи почали шифруватись. Подіям такого типу слід надавати рівень інциденту та починати відповідно їх вирішувати.

Після виявлення інциденту команда реагування підприємства, або компанія, що надає послуги забезпечення інформаційної безпеки, розпочне фазу аналізу. На цьому етапі починається збір доказів атаки з уражених систем. Доказами можуть

бути файли журналів, мережеві з’єднання, запущені програмні процеси та аномальне використання оперативної пам’яті.

Залежно від складності інциденту, збір інформації може зайняти від кількох годин до кількох днів. Після того, як докази зібрані, їх необхідно дослідити. Для проведення такого аналізу існує безліч інструментів, за допомогою яких аналітики намагаються з’ясувати, що саме сталося, на що вплинуло втручання, чи були заражені будь-які інші системи і додатки та чи були викрадені, або модифіковані конфіденційні дані. Кінцева мета аналізу – визначити першопричину інциденту та реконструювати дії зловмисника, а також шкідливого програмного забезпечення від початкового втручання до моменту виявлення та ліквідації.

Як тільки буде чітко зрозуміло, що являє собою інцидент і які системи атакуються, з’явиться змога перейти до етапу стримування. На цьому етапі організації вживають заходів щодо обмеження можливостей зловмисників продовжувати компрометувати ресурси, взаємодіяти з корпоративною інфраструктурою та змінювати або викрадати конфіденційні дані.

Стратегії стримування можуть варіюватися від блокування портів і IP-адрес на брандмауері до простої зупинки мережевого з’єднання кінцевої точки. Кожен тип інцидентів передбачає свою власну стратегію стримування, але варіативність методів реагування дозволяє спеціалістам оперативніше зупинити поширення атаки, якщо інцидент виявили до або під час, крадіжки даних.

Під час фази викорінення організація ліквідує загрозу в зараженій мережі. Бувають різні випадки ліквідації, інколи можна обмежитись використанням утилітами для захисту від шкідливого програмного забезпечення, а інколи доводиться стерти уражені машини та відновити або створити їх заново. Якщо організація виявила вразливість системи, то в подальшому її закривають пакетами виправлень від постачальників програмного продукту або оновленням програмного забезпечення.

Заходи з відновлення часто опираються на плани забезпечення безперервності роботи бізнесу або плани аварійного відновлення роботи організації. Ця фаза включає в себе встановлення нових операційних системи або

додатків на заміну враженим, а також відновлення даних локальних систем із резервних копій. До фази відновлення включений етап перевірки існуючих облікових записів користувачів і адміністраторів для переконання у відсутності облікових записів, які були активовані зловмисниками. Наприкінці, проводиться комплексне сканування вразливостей для впевненості у тому, що будь-які уразливі місця системи, які зловмисники могли б експлуатувати, були виправлені.

Після кульмінації реагування на кіберінцидент проводиться повний огляд інциденту з основними зацікавленими сторонами, якими можуть виступати керівники організації, команда реагування, аналітики безпеки, команда криміналістів та інші. Діяльність після інциденту включає повний огляд усієї активності, що здійснювалась під час інциденту. Ті методи та засоби реагування, що спрацювали, і, що набагато важливіше, ті, котрі не зреагували на загрозу, є важливими темами для обговорення та для створення плану модернізації системи реагування.

Аналіз проведеної процедури усунення загрози важливий, оскільки він може висвітлювати конкретні завдання та дії, які мали позитивний або негативний вплив на результат роботи з інцидентом безпеки. На цьому етапі процесу складається письмовий звіт. Документування дій, виконаних під час інциденту, має вирішальне значення для фіксації того, що сталося, і того, чи дійде справа конкретного інциденту до розгляду суду. Для ефективності складеної документації, вона повинна бути детальною і показувати чіткий хронологічний ланцюг подій з акцентом на першопричину, якщо вона була визначена. Персонал, який бере участь у підготовці цього звіту, повинен розуміти, що матеріал повинен бути викладений у такій формі, щоб люди, які не мають поглиблених знань в сфері інформаційної безпеки, могли зрозуміти його зміст та оцінити інформативність. Якщо у звіті використовувались спеціальні терміни, професійний жаргон або вузькі концепції, їх слід пояснити.

В кінці циклу реагування на інциденти, спеціалісти з кіберзахисту повинні переглянути та оновити власні та корпоративні процеси боротьби з вразливостями, використовуючи всю нову інформацію, отриману під час аналізу та після складання

звітності. Завдяки винесенню цінних уроків, механізм реагування значно покращується, а професіоналізм команди виходить на новий рівень.

Виявлення вторгнення в систему. Організації використовують глибокий оборонний підхід і складні технічні інструменти в інформаційних системах і мережі, підключаючи операційні процеси та визначаючи потрібних людей для керування цими процесами. Сьогодні стратегія виявлення у багатьох компаніях включає внутрішні та зовнішні ресурси. Можливості виявлення включають численні компоненти, наприклад [9]:

виявлення вторгнення по периметру;

шлюзи електронної пошти та блокування спаму;

запобігання втрати даних;

виявлення кінцевої точки та реагування;

кореляція та аналіз журналу.

Ефективні стратегії ведення журналів вимагають збір журналів подій з багатьох різних джерел, таких як додатки, мережеві пристрої, бази даних та сервери. Все це необхідно, щоб отримати видимість всієї інфраструктури.

Стримування атаки відбувається шляхом визначення всіх уражених пристроїв та вимагає пошуку індикаторів на кінцевих точках і пристроях, ідентичних тим, що були, на вперше вражених компонентах системи. При взаємодії з компанією, що надає послуги в сфері захисту інформації, відповідальність за пошук усіх кінцевих точок, а також заражених серед них, може бути покладена на неї, як на постачальника послуг. Головне — швидко та ретельно скласти список уражених пристроїв. Після ідентифікації пристроїв, переведення їх у автономний режим не дозволяє їм підключатися або залишатися на зв’язку з іншими компонентами системи, які поширюють вразливість.

Усунення проблем передбачає видалення будь-якого шкідливого програмного забезпечення та файлів, завантажених в уражені системи. Це також веде за собою зміну конфігурацій, що використовувались як вразливості та призвели до проблем. Після видалення всіх шкідливих файлів та програм із уражених кінцевих точок і пристроїв системи повертаються в мережу, і робочий

процес відновлюється. Команда з кібербезпеки повинна уважно стежити за цими системами та рештою мережі, щоб виявити ознаки наявності шкідливого програмного забезпечення в мережі.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РЕАГУВАННЯ НА ІНЦИДЕНТИ НА БАЗІ ПЛАТФОРМИ ESET PROTECT

У цьому розділі досліджено платформу ESET Protect, що розроблена та підтримується міжнародною компанією ESET, яка є партнером кафедри Інформаційної та кібернетичної безпеки Державного університету телекомунікацій.

Звернуто увагу на такі аспекти, як архітектурні особливості платформи та її компонентів, способи використання, можливості в реагуванні на інциденти та адміністрування.

2.1. Призначення, можливості та функції ESET Protect

Компанія ESET розробила програмну платформу, що дозволяє адмініструвати низку їх продуктів на пристроях, що використовуються в робочих процесах організації. До таких пристроїв можна віднести серверне обладнання, мобільні пристрої та, звичайно, робочі станції. Дана платформа покриває потреби підприємства у сфері реагування на кіберінциденти в інформаційній системі, налаштування політики безпеки, моніторингу стану комп’ютерної мережі організації та виявлення потенційних вразливостей, що виникають на кінцевих точках.

Використовуючи одне комплексне рішення від ESET компанія збирає низку програмних утиліт циклу роботи з загрозами в одному зручному інтерфейсі та з цілковитою взаємодією компонентів між собою, що дає змогу економити кошти підприємства, оскільки не виникає потреби в придбанні окремих рішень під кожен етап забезпечення безпеки системи, наприклад, рішення для шифрування дисків, пошуку вразливостей на підключених комп’ютерах, реагування на вразливості, відновлення системи тощо.

Саме по собі рішення ESET Protect не надає захист від злоякісного програмного забезпечення. Оскільки це платформа, то вона об’єднує під собою та використовує інші продукти ESET для виконання функцій захисту, але формально розуміється, що ці продукти входять до складу ESET Protect, хоч їх встановлення відбувається окремо на кінцевих точках автономним способом, або віддалено через консоль управління платформою. Консоль також використовується для запуску скриптів та віддалених команд, створення списку процесів, конфігурації комплектуючих тощо.

Існує два варіанта використання даного програмного забезпечення: в якості хмарного рішення, відомого під назвою ESET Protect Cloud, та безпосереднього розгорнення на апаратному забезпеченні самої організації. Розгорнення програмного комплексу в будь-якому з представлених варіантів дозволяє отримати доступ організації до постійного оновлення інформації про стан систем та мережі, а також покращує рівень роботи адміністраторів безпеки, оскільки з’являється змога оперативно реагувати на будь-які виклики безпеки.

Програмний продукт ESET постачається з розробленими політиками безпеки, якими можна скористатись зразу після його встановлення, але особливо важливо скористатись можливостями програмного забезпечення та провести детальне налаштування політики безпеки відповідно до потреб підприємства, а також створити автоматизовані задачі, що допоможуть не витрачати зайвий час адміністраторів і дати змогу їм зосередитись на забезпеченні та розробці найкращих варіантів захисту корпоративних систем.

До програмного комплексу також включена можливість подання звітностей на широкий спектр потреб. Розробниками платформи вже передбачені численні шаблони звітностей, генерувати котрі можна одним натиском кнопки, відповідно до запитів керівництва, а також можна створити власний шаблон звітності та визначити графік, за яким звітність буде автоматично створюватись та надсилатись. Це також допомагає зберегти час та використовувати потенціал спеціалістів в правильному напрямку, а не на повсякдення складання статистичних звітів, що, звісно, є необхідною, але рутинною справою.

В цілому, розробники платформи намагались максимально облегшити рутинні дії для адміністраторів безпеки та звести часові затрати на них до мінімуму. Це простежується навіть в таких дрібницях, як створення виключень з правил безпеки або надсиланні файлів для аналізу в один клік. Представлені можливості створення виключення за посиланням, адресою, найменуванням загрози та хешем.

У застосунку використовується широкий спектр сортувань, наприклад, динамічне сортування груп пристроїв, котре регулярно моніторить систему та відбирає пристрої на основі різних критеріїв, наприклад, їх доступності, схожості виявлених проблем або інших заданих параметрів. В подальшому це дозволяє планувати та здійснювати процедури оновлення чи встановлення спеціального програмного забезпечення, або зміни політики безпеки для вибраних груп тощо.

Групи також представлені серед персоналу, що взаємодіє з утилітою. Підтримується функція призначення адміністраторів на окремі ділянки мережі, а також детальне розподілення прав доступу користувачів. В якості опції для входу платформа надає можливість використовувати багатофакторну автентифікацію.

В ESET Protect реалізовано автоматичну підтримку інфраструктури віртуальних робочих столів, яка виражена у розробленому алгоритмі виявлення апаратного забезпечення, завдяки якому визначається ідентичність пристрою на основі його комплектуючих. Ця функція дозволяє автоматизувати створення образів та клонування непостійних систем зберігання даних. Також при розгортанні нового образу є змога додати агент ESET Protect, який при створенні нових робочих столів з іншим апаратним відбитком буде автоматично створювати нові записи про роботу системи в базі даних платформи.

Завдяки даному рішенню від ESET можна переглядати встановлене програмне забезпечення на кінцевих точках та його версії. Окрім цього, можна переглядати інформацію про апаратне забезпечення підключених пристроїв: виробника, серійний номер, доступну пам'ять на носіях та інше. На основі звітів про комплектуючі, можуть складатись плани оновлень апаратного забезпечення.

ESET Protect оперативно реагує на загрози, наприклад, при отриманні листа з потенційно шкідливим для системи вмістом, команда реагування отримує

повідомлення, що в системі знайдена загроза, яка знаходиться на конкретному комп'ютері, після чого виконується віддалене сканування вибраного пристрою. Коли сканування підтверджує шкідливість файлу, він відправляється в компонент платформи під назвою ESET Dynamic Threat Defense, котрий реагує та стримує загрозу від поширення мережею організації. Також для фіксації загроз використовується хмарна пісочниця ESET, завдяки високій потужності, вона швидко знаходить програми-вимагачі.

ESET Protect може взаємодіяти з SIEM-системами, що вже встановлені в організації, та використовуватись в якості доповнення системи захисту організації. Процес взаємодії включає обмін інформацією з журналів подій у форматах JSON або LEEF, таким чином даний продукт інтегрується з існуючими центрами безпеки підприємства [10].

2.2. Компоненти та архітектура рішення ESET Protect

Програмний продукт ESET Protect складається з багатьох модулів, які взаємодіють як одне ціле всередині нього та відповідають за конкретні окремі функціональні частини забезпечення захисту корпоративної інформаційної системи. Саме з цієї причини, для асоціації з ESET Protect, в роботі використовується термін «платформа», що якомога краще підкреслює його масштабність та функціональні перспективи для використання на підприємстві.

В залежності від потреб організації, існують різні комплекти поставки платформи ESET Protect. До того ж продукт представлений не тільки в локальній, а й в хмарній формі, яка дозволяє так само керувати всіма продуктами платформи з єдиного центру, виключаючи необхідність фізичних або віртуальних серверів, які повинні підтримуватись підприємством.

До кожного окремого рішення ESET Protect входить той чи інший набір програмних продуктів для вирішення індивідуальних задач компанії. На рисунку нижче представлено всі можливі версії продукту та включені в них компоненти на момент написання даної роботи (рис. 2.1).

		PROTECT ESSENTIAL	PROTECT ENTRY	PROTECT ADVANCED	PROTECT COMPLETE	PROTECT ENTERPRISE	PROTECT MAIL PLUS
Консоль управління	локальна	✓	✓	✓	✓	✓	
	хмарна та локальна	✓	✓	✓	✓	✓	✓
Класичний захист робочих станцій*		✓	✓	✓	✓	✓	
Комплексний захист робочих станцій**			✓	✓	✓	✓	
Захист файлових серверів		✓	✓	✓	✓	✓	
Хмарна пісочниця				✓	✓	✓	✓
Повнодискове шифрування				✓	✓	✓	
Захист поштових серверів					✓		✓
Захист хмарних додатків (Office 365)					✓ (тільки хмарне управління)		
Виявлення та відслідковування загроз (EDR)						✓ (тільки локальне управління)	

* До складу входить ESET Endpoint Antivirus
** До складу входить ESET Endpoint Security

Рис. 2.1. Таблиця варіантів продукту ESET Protect та їх комплектуючих [11]

Для використання платформи інсталюються необхідні компоненти, а також можна інсталювати додаткові для забезпечення максимальної продуктивності захисту та розкриття всього потенціалу даного програмного забезпечення. До необхідних компонентів архітектури належать: сервер та веб-консоль ESET Protect, а також агент ESET Management. Додатковими ж являються такі компоненти як проксі-сервер HTTP чи Apache HTTP, Rogue Detection Sensor і Mobile Device Connector. Необхідно пройтись по кожному з компонентів та визначити за що вони відповідають в рамках платформи [12].

Сервер ESET Protect, як і прийнято, оброблює вхідні запити та дані, що на нього поступають від клієнтів мережі, що в свою чергу підключаються через агент ESET Management, або за допомогою HTTP проксі-сервера. Сервер бази даних ESET, на якому знаходяться мережеві дані, рекомендується встановлювати на окремому пристрої, оскільки це допоможе підвищити продуктивність роботи системи захисту. Також необхідно стежити за якісним та постійним підключенням між серверами бази даних та ESET Protect. На рисунку нижче зображена топологія підключення між сервером та кінцевими точками мережі (рис. 2.2).

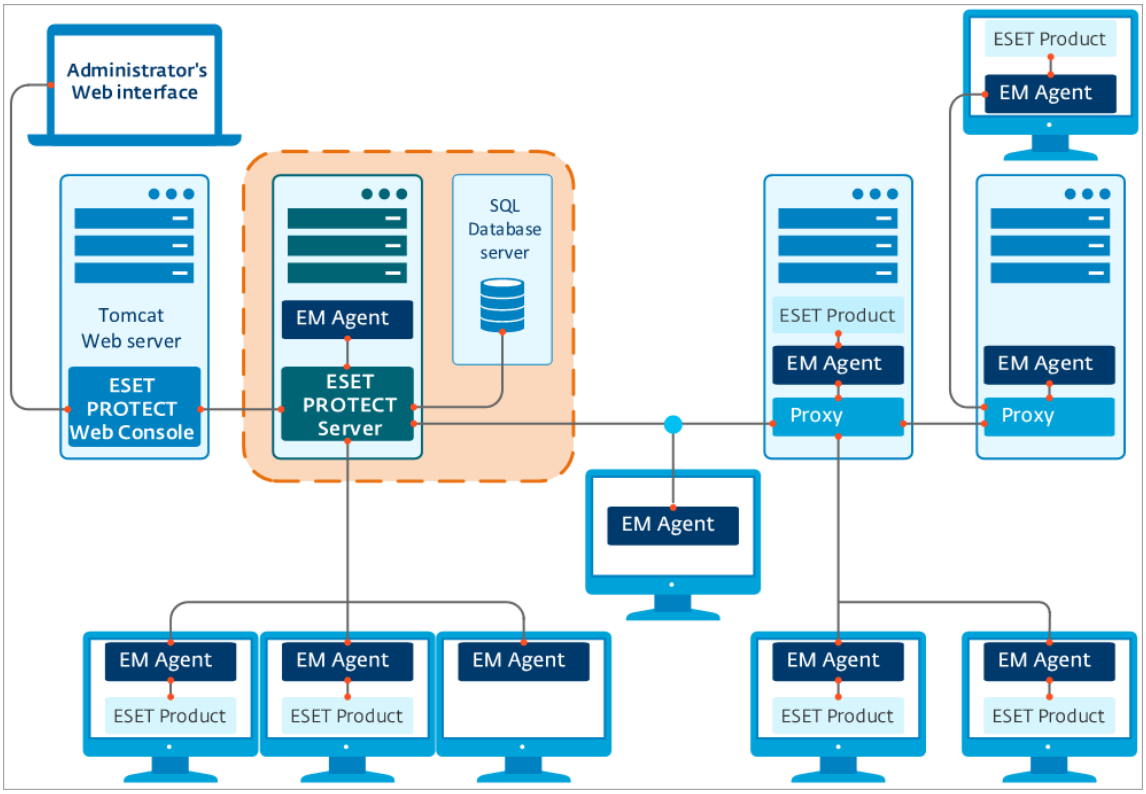


Рис. 2.2. Топологія підключення пристроїв до серверу ESET Protect [13]

Наступним обов'язковим компонентом архітектури платформи є веб-консоль, яка надає користувацький інтерфейс для зручної взаємодії з системою, а саме для керування рішеннями ESET та налаштування системи під потреби організації. Консоль використовує веб-інтерфейс Webmin, котрий застосовується для спрощеного керування системами Linux. В ній відображається поточний стан складових мережі, а також її можливо використовувати для дистанційного встановлення програмного забезпечення на комп'ютерах компанії. Вона дає змогу використовувати ESET Protect з любого куточку світу, оскільки відкривається у браузері, але для цього необхідно відкрити доступ до серверу через Інтернет. В якості веб-серверу для консолі використовується Apache Tomcat.

Клієнти мережі, що здійснюють обмін інформацією про стан з ESET Protect, передають її через агента ESET Management. Попередні версії агента були відомі під назвою ESET Remote Administrator, але хоч назва й змінилась, функціонально це той самий продукт. Для з'єднання та обміну даними між агентом та платформою використовується новий протокол зв'язку gRPC (протокол віддаленого виклику процедур), а для передачі інформації через проксі-сервер – HTTP2 та TLS. Задача

агента полягає у зборі інформації з робочого пристрою та надсилання її на головний сервер платформи, а також в отриманні завдань від серверу та їх виконання.

Всі утиліти ESET, що установлені на пристрої, відсилають дані не напряму на сервер, а агенту, який в свою чергу контактує з платформою. Робочі машини, на яких встановлений агент, з точки зору інформаційної безпеки, повністю керуються продуктом ESET Protect. Агент також має власні збережені сценарії забезпечення кібербезпеки, що, в деяких випадках, дозволяє прискорити реакцію на інцидент, навіть в випадку, коли агент не підключено до головного серверу.

Використання проксі-серверу є необов'язковим, але рекомендованим компонентом ESET Protect. Проксі-сервер слід використовувати для забезпечення зв'язку у разі обслуговування віддалених робочих місць, а також при виникненні проблем в прямому підключенні комп'ютерів через агента до головного сервера.

Платформа використовує спеціалізовану версію проксі-серверу Apache HTTP, він відповідає лише за пересилання даних, без функцій кешування та ініціалізації зв'язку. Налаштований проксі-сервер має змогу кешувати результати роботи утиліти ESET Dynamic Threat Defense, оновлення модулів ESET та пакети інсталяцій.

Apache HTTP Proxy економить трафік мережі, використовуючи кеш для завантажень програмного забезпечення, або його оновлення, це особливо помітно у великих мережах робочих пристроїв, коли необхідно оновити багато пристроїв, оновлення звантажується тільки один раз, а потім береться з кешу, а не завантажується для кожного пристрою окремо.

У системі можливе використання глобальних проксі та окремих проксі для служб. В глобальних - один проксі-сервер буде використовуватись для кешування та відправки даних, а в окремих – використовуються різні проксі для цих самих функцій. Також можливе використання ланцюгів проксі-серверів, якщо ті не потребують автентифікації [14]. Нижче зображено приклад роботи проксі-серверу в інфраструктурі ESET Protect (рис. 2.3).

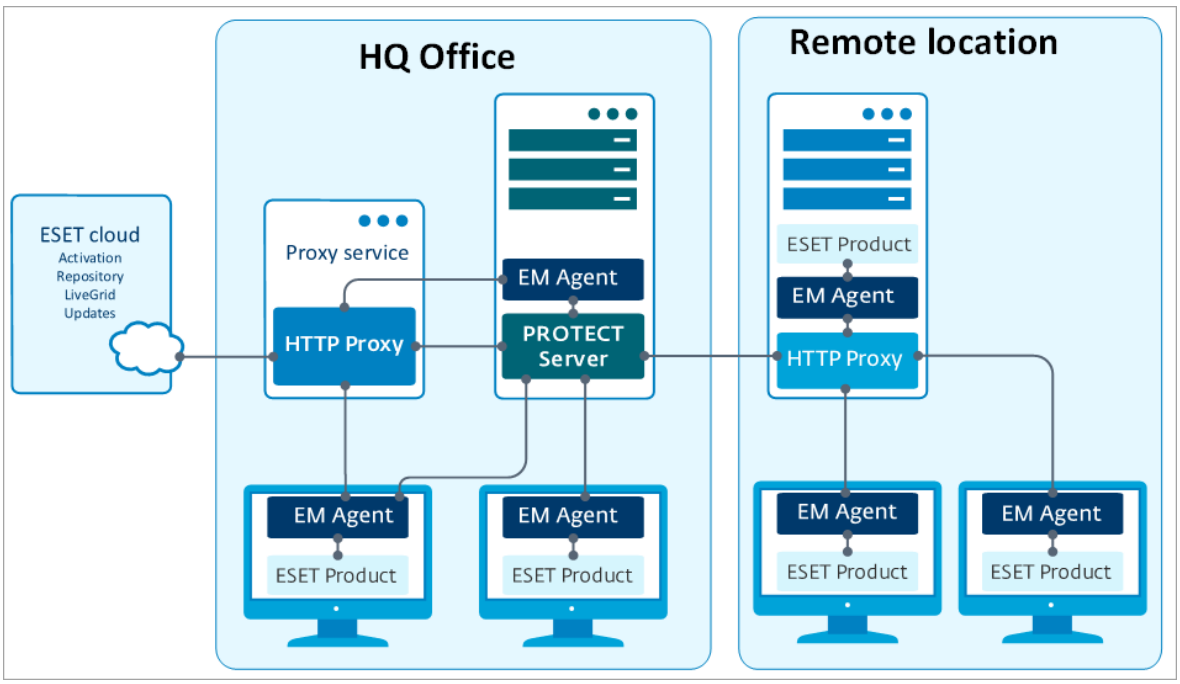


Рис. 2.3. Проксі-сервер Apache HTTP в інфраструктурі ESET Protect [14]

Одним з опціональних архітектурних компонентів платформи є Rogue Detection Sensor, котрий є відповідальним за виявлення неавторизованих систем (рис. 2.4).

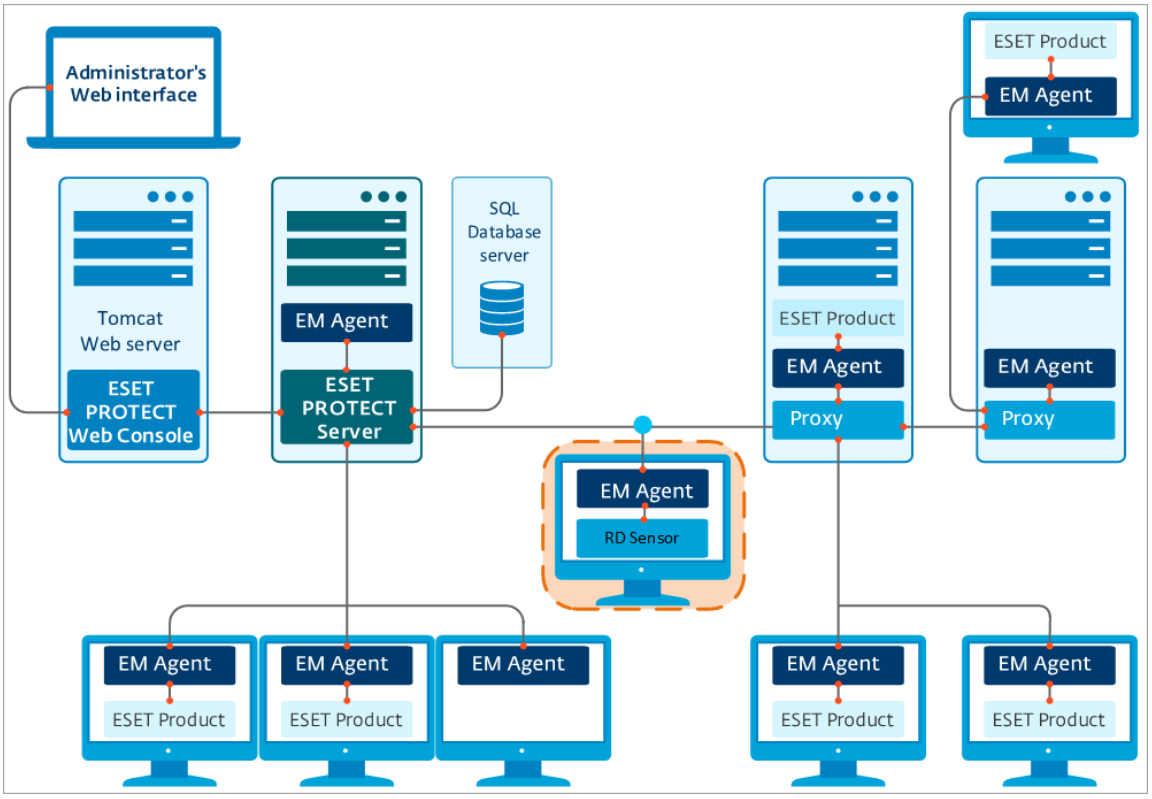


Рис. 2.4. Схема інтеграції Rogue Detection Sensor в систему [15]

Rogue Detection Sensor здійснює регулярний моніторинг комп'ютерів у мережі ESET Protect та додає нові пристрої, точно так, як видаляє неактуальні. Це все здійснюється в автоматичному режимі, без втручання спеціаліста в роботу додатку. Іншими словами, це засіб обліку пристроїв, що надсилає дані на головний сервер для обробки. Робота сенсору в інфраструктурі платформи зображена нижче.

За інтеграцію платформи з мобільними пристроями відповідає компонент Mobile Device Connector. Він надає змогу здійснювати адміністрування ними за допомогою ESET Endpoint Security для мобільних систем. Принцип взаємодії такий самий, як з агентом для комп'ютерних систем: ESET Endpoint Security здійснює збір інформації та надсилає її на сервер, де вона оброблюється, а сервер відсилає команди на пристрій. Схема роботи Mobile Device Connector зображена нижче (рис. 2.5).

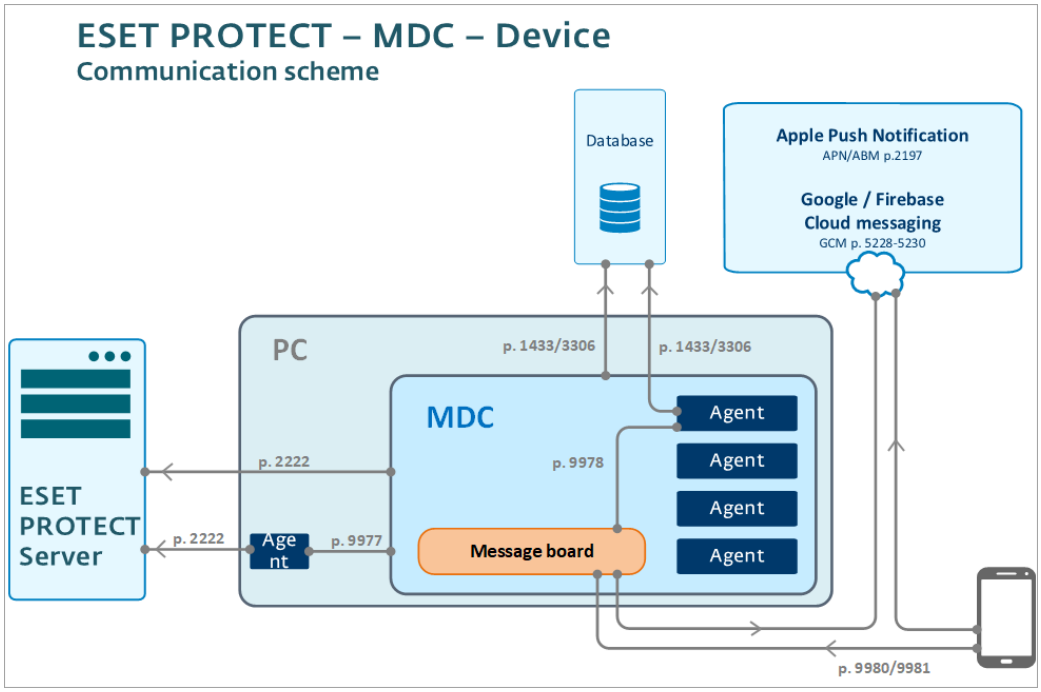


Рис. 2.5. Схема комунікації Mobile Device Connector [16]

Компоненти платформи контактують з головним сервером за наявності ліцензійних сертифікатів, що надаються центром сертифікації ESET для кожного програмного рішення окремо. Сертифікати можна експортувати, переносити на новий сервер у разі міграції, відтворювати їх на основі прив'язаних до них облікових даних, а також відкликати.

На схемі нижче продемонстровано використання сертифікатів в інфраструктурі ESET Protect, яке показує, що сертифікати окремих типів використовуються та перевіряються різними компонентами системи та тісно пов'язані між собою, аж до того, що відсутність будь-якого одного сертифікату потенційно призведе до некоректної роботи всієї системи, а не її частини, а в окремих випадках до зупинки експлуатації системи (рис. 2.6).

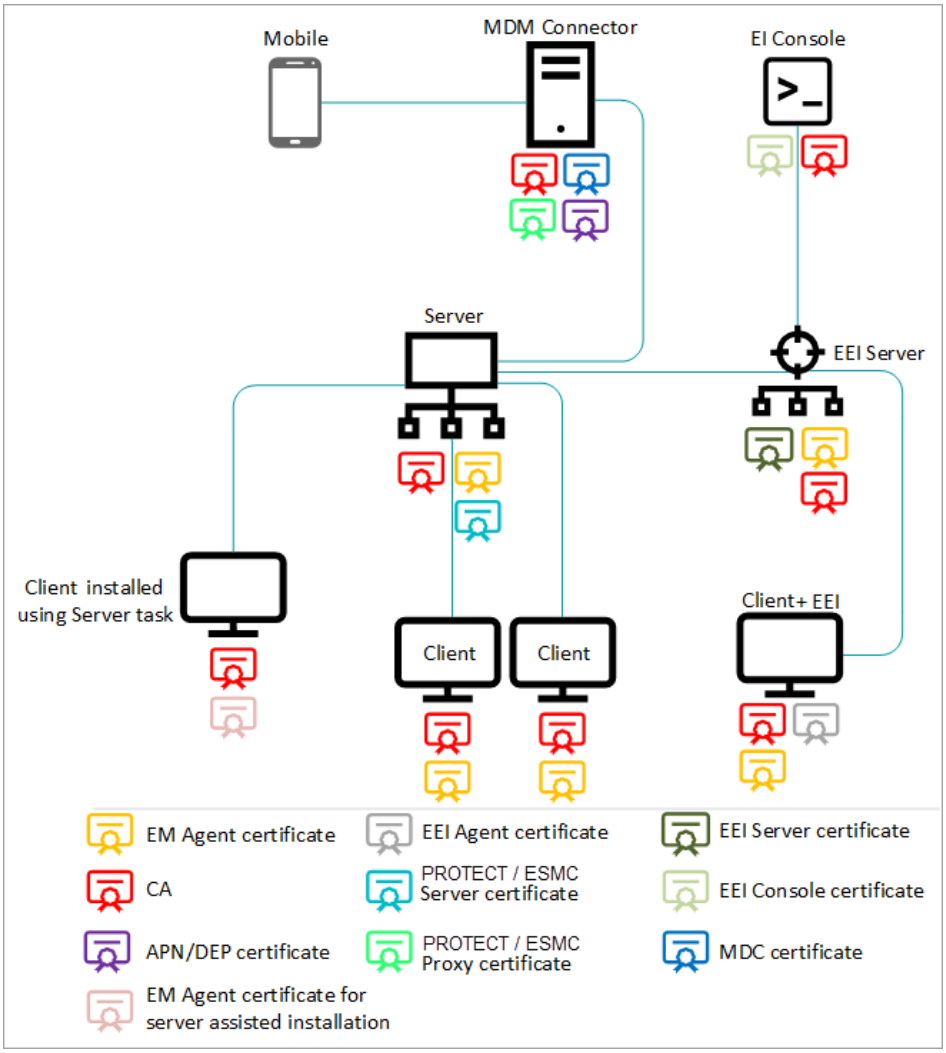


Рис. 2.6. Використання сертифікатів в інфраструктурі системи [17]

Зображення нижче коротко резюмує функціонал описаних компонентів архітектури ESET Protect (рис. 2.7).

Функція	Сервер ESET PROTECT	Агент ESET Management	Продукт захисту ESET	Проксі-сервер HTTP	Сервери ESET	Mobile Device Connector
Віддалене керування продуктами ESET для захисту (створення політик, завдань, звітів тощо)	✓	x	x	x	x	x
Обмін даними із сервером ESET PROTECT та керування продуктами ESET для захисту на клієнтському пристрої	x	✓	x	x	x	✓
Надання оновлень, перевірка ліцензій	x	x	x	x	✓	x
Кешування та переадресація оновлень (ядро виявлення, інсталятори, модулі)	x	x	✓	✓	x	x
Переадресація мережевого трафіку між агентом ESET Management і сервером ESET PROTECT	x	x	x	✓	x	x
Захист клієнтського пристрою	x	x	✓	x	x	x
Віддалене керування мобільними пристроями	x	x	x	x	x	✓

Рис. 2.7. Огляд елементів інфраструктури ESET PROTECT та їх основних функцій [12]

Невід'ємною частиною системи ESET Protect є веб-сервіс ESET Business Account. Саме за допомогою нього підключаються та керуються ліцензії ESET. Це, свого роду, єдиний центр управління бізнес-функціями продуктів ESET, що також веде журнал подій та сповіщає важливу інформацію про стан системи. Додавши в ньому ліцензії, з'являється змога ділитись ними з усіма відділеннями компанії, а також реєструвати ліцензії за конкретними довіреними особами. Також, використовуючи цей сервіс, можна ввімкнути двофакторну автентифікацію, яка має назву ESET Secure Authentication. Вона також функціонує завдяки використанню спеціальної ліцензії.

В веб-додатку також можна ввімкнути захист ESET Cloud Office Security, котрий необхідний для забезпечення захисту файлів OneDrive та електронної пошти Office 365. Саме через ESET Business Account здійснюється доступ до хмарної версії платформи ESET Protect.

Сам ESET Protect Cloud містить аналогічні компоненти системи, що й його локальна версія, але є більш спрощеною версією для використання. Він включає компонент ESET PROTECT Live Installer, який відповідає за встановлення агенту на комп'ютери мережі, що є спрощеною версією ESET Management, оскільки

принцип дії такий самий, але програмний пакет для інсталяції постачається у спрощеній та легкій для використання формі. Пакет інсталяції не потрібно налаштовувати, він йде налаштованим зразу після його створення, а сам встановлений з нього продукт автоматично підключається до серверу та активує себе ліцензією. Взаємодія з користувачем мінімальна. Нижче представлена схема взаємодії ESET Protect Cloud з ключовими елементами системи (рис. 2.8).

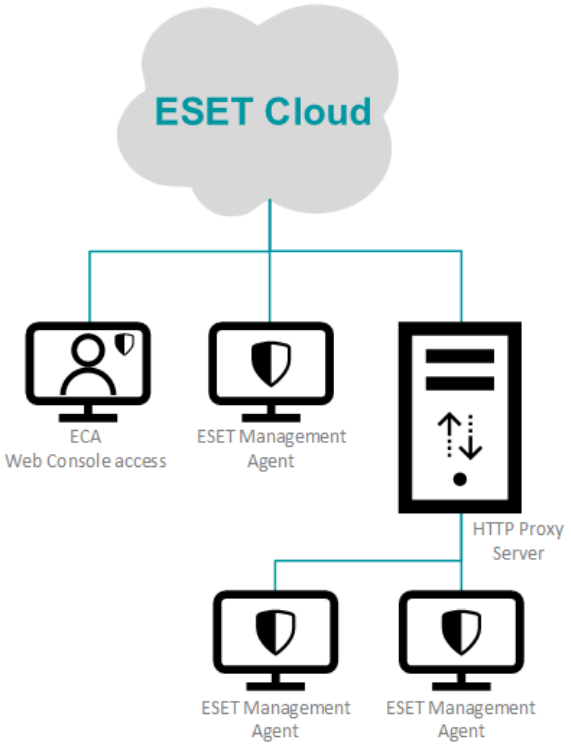


Рис. 2.8. Взаємодія ESET Protect Cloud з ключовими елементами системи [18]

Існує ще один інструмент, котрий не є обов'язковим, але розширює можливості програмного продукту. Він носить назву «Дзеркало», використовується для оновлення інструменту виявлення загроз, а саме для оновлення його програмного ядра. За допомогою «Дзеркала» можна зберігати оновлення ESET локально та встановлювати їх без доступу до мережі. Для того, щоб використовувати даний інструмент необхідно створити автономну ліцензію, котру можна створити самому, використовуючи дійсні ліцензії в ESET Business Account. Інструмент використовується через командний рядок та створює папки, в яких міститься оновлення ядра інструменту виявлення. Автоматичне завантаження

оновлень «Дзеркалом» також налаштовується через командний рядок. Для підтримки інструменту, необхідно створити спеціальну політику та налаштувати сервер оновлень для клієнтів мережі, де необхідно вказати адресу «Дзеркала», або спільних папок з оновленнями.

Досить важливим з точки зору використання платформи є компонент під назвою ESET Remote Deployment Tool. Цей компонент допомагає розповсюдити пакети інсталяторів ESET Management Agent серед підключених до мережі організації комп'ютерів для подальшого їх адміністрування. Компонент сканує мережу компанії та виявляє ще не додані до платформи пристрої для того, щоб відправити н них інсталяційні пакети. Також комп'ютери для розповсюдження пакетів можна додавати вручну, або імпортом списку їх IP-адрес. Цей інструмент використовується без спеціальних ліцензій та знаходиться у вільному доступі, а саме, у списку компонентів ESET Protect, доступних для завантаження окремо.

В список ліцензій доступних для ESET Protect входить ліцензія ESET Server Security. Цей компонент системи представляє з себе рішення для захисту середовища Microsoft Windows Server, пропонуючи захист від шпигунського та шкідливого програмного забезпечення. Цей компонент також може використовуватись як окреме програмне рішення, але в великих мережах він керується через ESET Protect. Його функції наступні [19]:

сканування файлів OneDrive;

сканування віртуальних дисків Hyper-V без встановлення агентів ESET Management для цих дисків;

автоматичне виключення критичних системних файлів з процесу сканування, оскільки це може призвести до некоректної їх роботи;

тісна взаємодія з ESET Dynamic Threat Defense, що використовується для захисту від шкідливого ПЗ;

ведення журналів програмних подій;

можливість ізоляції серверу шляхом обмеження мережевого з'єднання, але не його припинення, оскільки підключення до контролера домену зберігається, що

дає змогу обмінюватись даними про стан серверу та про знайдені вразливості через ESET Management Agent;

використання ESET RMM для керування декількома серверами з одного місця;

використання ESET eShell в якості інтерфейсу командного рядка, що містить параметри управління серверними продуктами ESET.

Для використання в локальній версії продукту ESET Protect доступна утиліта ESET Enterprise Inspector. Це інструмент виявлення та відслідковування загроз системі. До її привілеїв входить постійний моніторинг процесів на кінцевих точках та аналіз цих процесів на рахунок потенційної небезпеки, а вразі її виявлення – швидка реакція. Додаток має можливість надання API-ключа для взаємодії зі сторонніми SIEM та SOAR системами, а також доступний віддалено, оскільки надає змогу налаштовуватись через PowerShell. Інструмент одночасно взаємодіє напряму з кінцевими точками, а також з платформою ESET Protect.

Окрім всього сказаного, ESET Enterprise Inspector співвідносить знайдені вразливості з базою даних MITRE ATT&CK, що допомагає в один клік отримати глибоку інформацію про загрозу та шляхи її усунення. Додаток має відкриту архітектуру, що дає змогу його персоналізації під конкретну інформаційну систему підприємства, а також підтримується гнучке редагування правил безпеки, оскільки вони написані в форматі XML та можуть легко персоналізуватись адміністратором безпеки для досягнення тих цілей безпеки, які ставить перед собою підприємство.

За безпеку електронної пошти клієнтських пристроїв відповідає ESET Mail Security, так саме як ESET Cloud Office Security, він забезпечує захист від фішингу, спаму та шкідливого ПЗ в файлах листів. Відмінним є можливість використання інструменту не тільки в Microsoft Exchange Server, але й в IBM Domino. Також ESET Mail Security пропонує створення кластерів, що допомагають продуктам взаємодіяти між собою та підвищувати таким чином рівень безпеки. Продукт використовує машинне навчання, має можливість відправляти підозрілі листи в веб-карантин, а також підтримує впровадження пісочниці ESET Dynamic Threat Defense для перевірки загроз, в якості додаткового шару захисту.

Розглядаючи наступні компоненти, варто зазначити, що вони є основними програмними додатками, які включені до пакету поставки ESET Protect та доступні зразу після розгортання платформи. Такими продуктами є: ESET Dynamic Threat Defense, ESET Endpoint Security та ESET Full Disk Encryption.

ESET Dynamic Threat Defense спеціалізується на захисті пристроїв від загроз нульового дня. Захист відбувається завдяки відкриттю та запуску підозрілих файлів в хмарному середовищі, де стає можливим оцінити рівень їх небезпеки для системи, а також проаналізувати їх за допомогою інших програмних засобів ESET та зрівняти отримані дані з базами знань про атаки.

За комплексний захист кінцевих точок відповідає ESET Endpoint Security. Захист здійснюється через аналіз поведінки роботи програмного забезпечення, а також через сканування та відслідковування активності системи, що дає змогу нейтралізувати загрози як до їх запуску, так і на його початкових стадіях. Робота даного додатку забезпечує захист від програм-вимагачів, цільових атак на систему та нівелює крадіжки даних.

Для шифрування даних на підключених до ESET Protect пристроях використовується ESET Full Disk Encryption. Шифрування дисків та розділів відбувається на пристроях з операційною системою Windows та macOS та не потребує особливих зусиль, так як передбачені спеціальні команди, які дозволяють в пару кліків запустити процес шифрування.

2.3. Призначення та архітектура рішення ESET Dynamic Threat Defense

Продукт ESET Dynamic Threat Defense це важлива складова екосистеми ESET Protect, а основним поставленим завданням даного продукту є забезпечення додаткового рівня безпеки системи, доповнюючи вже розгорнуті рішення та створюючи ще один шар захисту, через який не пройшла б жодна загроза.

Принцип роботи досить цікавий з точки зору дослідження, оскільки цей інструмент самостійно виявляє підозріле програмне забезпечення або файли в системі підключеного клієнту та перенаправляє їх до хмари. Під хмарою мається

на увазі хмарна пісочниця, яка слугує майданчиком для запуску та тестування відібраних підозрілих файлів. В ній досліджується характер поведінки потенційно небезпечних зразків та збираються відповідні дані.

Дослідження зразків відбувається за допомогою ядер з розширеного виявлення шкідливого ПЗ. Саме про оновлення цих ядер йшлось в описі такого компоненту платформи як «Дзеркало» в попередньому підрозділі. Інструмент також обробляє підозрілі електронні листи, екземпляри яких надсилаються до ESET LiveGrid. ESET LiveGrid, в свою чергу, є компонентом, що дозволяє вчасно отримувати інформацію про актуальні зараження системи. Він використовується для оновлення модулів реагування на загрози на основі досліджених даних, а також для анонімного надсилання даних про загрози в компанію ESET для того, щоб нові продукти розроблялись з урахуванням всіх актуальних прийомів зловмисників.

Хоч зразки листів й надсилаються до ESET LiveGrid, тим не менш, вкладені файли в листах проходять дослідження за допомогою інструментів ESET Dynamic Threat Defense. Варто зазначити, що документи з активним вмістом, таким як макроси всередині PDF файлу, не надсилаються до хмарної пісочниці. Кількість файлів, що надсилається до хмари, та термін їх зберігання визначається адміністраторами або, в деяких випадках, користувачами системи. Також, якщо система не виявила файл підозрілим, користувач може сам, вручну, надіслати цей файл до хмари для перевірки на загрозу.

Архітектурно важливим елементом ESET Dynamic Threat Defense є консоль керування. Вона приймає метадані підозрілих файлів та надає до них доступ адміністратору безпеки, поки файл досліджується в хмарній пісочниці. Доступ до ESET Dynamic Threat Defense можна отримати як з допомогою локальних, так і за допомогою хмарних консолей керування (ESET Protect, ESET Protect Cloud).

Після завершення аналізу файлу пісочницею, результат передається на консоль, а в разі виявлення загрози в файлі, результат надається всім комп’ютерам мережі та іншим компаніям, які працювали з цим файлом. У разі тимчасової відсутності підключення до серверу ESET Protect, ESET Dynamic Threat Defense продовжує працювати та збирати інформацію офлайн, а при відновленні

підключення, програма синхронізується з сервером та повідомляє про знайдені загрози. Інструмент використовує глобальну базу даних, а саме центри обробки Azure, що є у власності компанії ESET, для збереження хеш-файлів та результатів аналізу загроз. На серверах ESET зберігаються всі надіслані файли та виконується аналіз підозрілих файлів.

ESET Dynamic Threat Defense, як вже згадувалось, надає додатковий рівень безпеки системі, але сам він складається з чотирьох рівнів виявлення загроз, на кожному з яких створюється окремий висновок про рівень безпеки досліджуваного файлу. Розберемо кожен рівень окремо [20].

На першому рівні підозрілі файли потрапляють в ESET Dynamic Threat Defense для порівняння їх з базою даних загроз та пошуку схожих випадків реагування. Оскільки для приховання ядра зловмисного програмного коду часто використовується багатократне пакування файлу, необхідно провести розпакування вмісту файлу. Цю функцію виконує рівень під назвою «Розширене розпаковування й сканування» (рис. 2.9).

Рис. 2.9. Перший рівень ESET Dynamic Threat Defense у виявленні загроз [20]

Після розпакування, зразки коду зіставляються зі схожими зразками, що знаходяться в базі даних. За результатами порівняння зразку, він класифікується як шкідливе ПЗ, безпечний файл, потенційно небажаний або потенційно небезпечний елемент. Саме для уникнення ризиків, що зв'язані з тісним дослідженням функціональності файлу, ESET Dynamic Threat Defense використовує хмарну інфраструктуру.

На другому рівні використовується модуль машинного навчання для проведення аналізу підозрілих файлів, щоб отримати більше даних про характеристики зразка. Поверхневий аналіз коду дозволяє тільки узагальнити розуміння про знайдену вразливість, тому на цьому рівні відбувається поглиблене вивчення файлу, а також пошук інструкцій та принципу роботи програмного коду, так зване знаходження ДНК коду (рис. 2.10). Таким чином, можна зрозуміти ступінь небезпеки зразка та його функціонал, навіть не запускаючи його в безпечному середовищі.

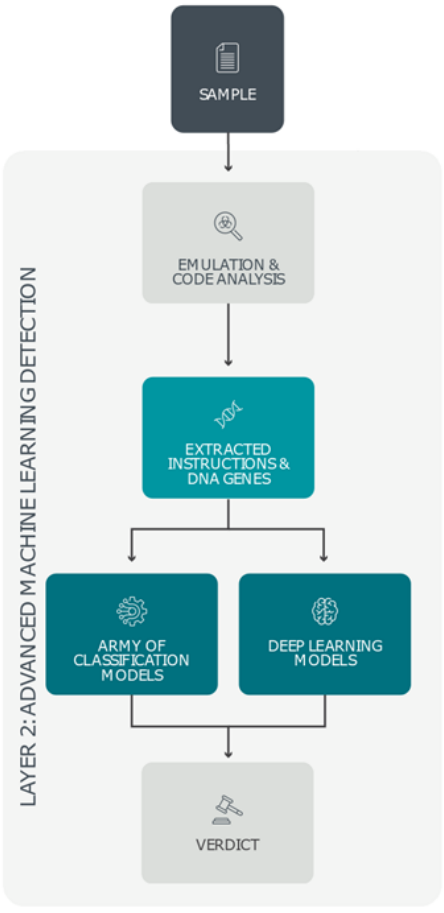


Рис. 2.10. Другий рівень ESET Dynamic Threat Defense у виявленні загроз [20]

Вся зібрана інформація оброблюється алгоритмами машинного навчання, після чого аналізується нейронною мережею та надає заключення: був даний файл загрозою чи ні. Рівень може не використовуватись, оскільки потребує значних ресурсних затрат для обробки, які не завжди є у кінцевого користувача. У випадку, коли рівень не використовується, він буде видавати результат «аналіз не потрібний».

Третій рівень має назву «Експериментальне ядро виявлення». На цьому рівні поглиблено аналізується поведінка підозрілого зразка шляхом додавання його в симулятор робочої системи з різними операційними системами, який в ESET називають пісочницею на стероїдах. Такі робочі системи містять алгоритми виявлення ESET та аналізують всі дії, що відбуваються в системі та до яких змін приводить запуск підозрілого файлу. Отримані дампи пам'яті системи скануються та порівнюються з базою даних загроз для знаходження відповідностей (рис. 2.11).

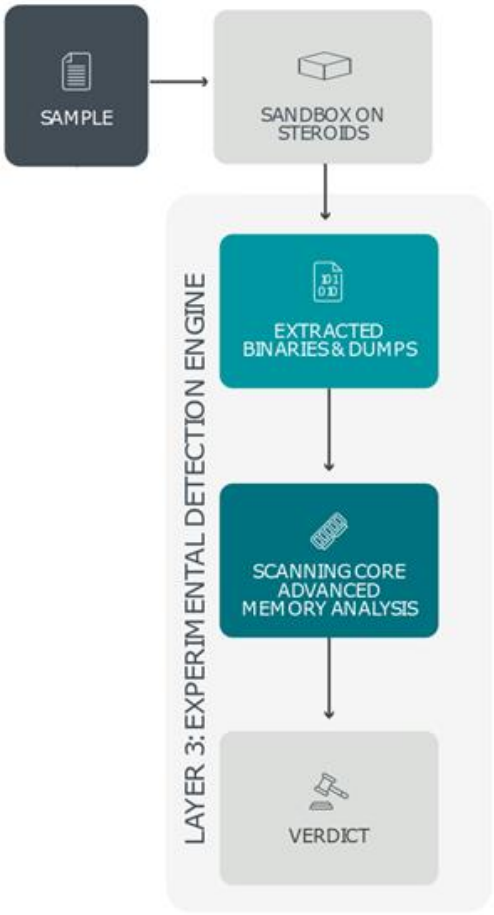


Рис. 2.11 Третій рівень ESET Dynamic Threat Defense у виявленні загроз [20]

Четвертий рівень носить назву «Детальний аналіз поведінки». На цьому рівні аналізуються всі надані пісочницею дані про підозрілий файл та дані про системи, на яких запускався зразок, наприклад, зміни в реєстрі, спроби мережевого зв'язку, запуск скриптів, робота з файлами на жорстких дисках. Згенеровані пісочницею дані розбиваються на логічні блоки, які зіставляються з базою раніше проаналізованих ланцюгів роботи шкідливого ПЗ (рис. 2.12).

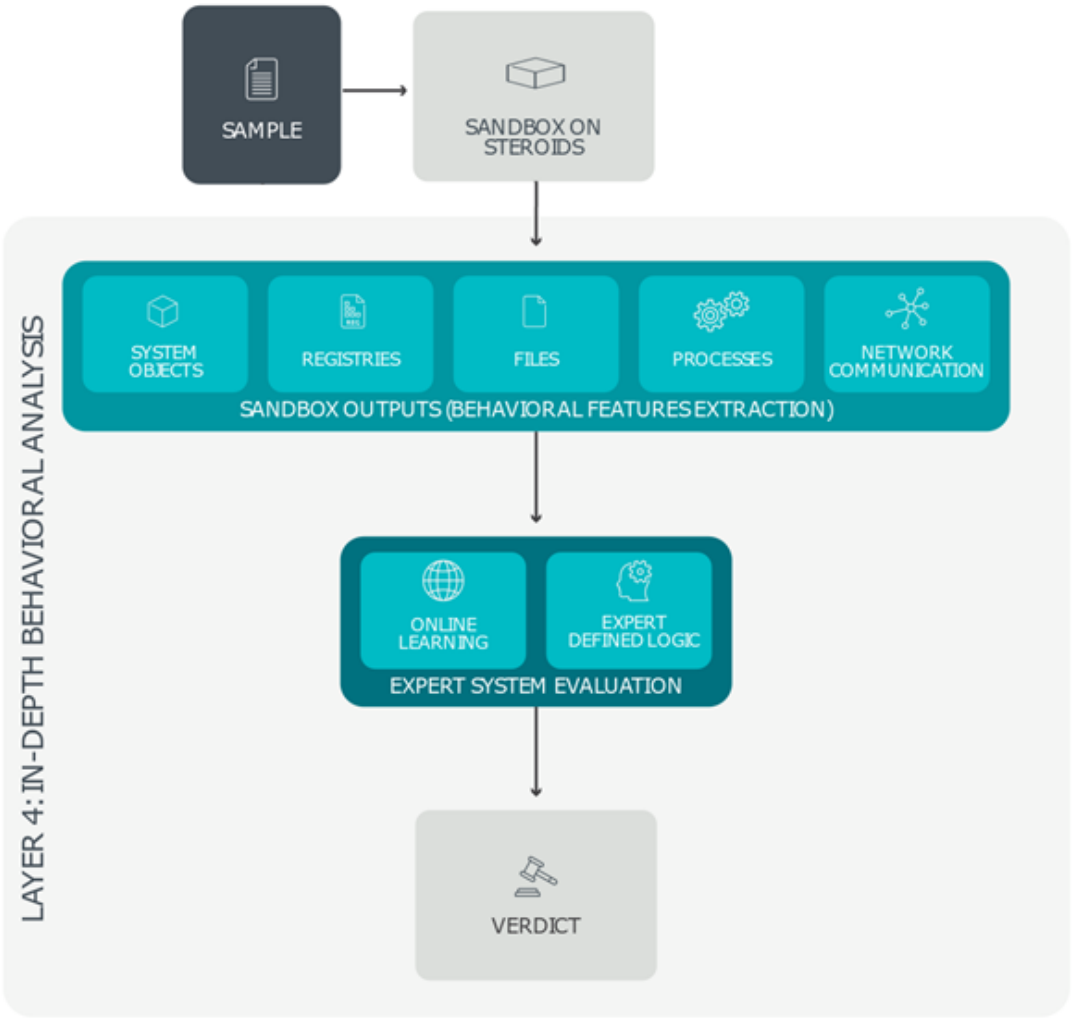


Рис. 2.12 Четвертий рівень ESET Dynamic Threat Defense у виявленні загроз [20]

ESET Dynamic Threat Defense групує всі надані висновки на кожному рівні виявлення про підозрілий файл, а потім надсилає дані в ESET Protect для забезпечення захисту корпоративної інформаційної системи, після чого ділиться

даними з спільною базою знань ESET. Загальна картина рівнів реагування та взаємодії їх між собою зображена нижче (рис. 2.13).

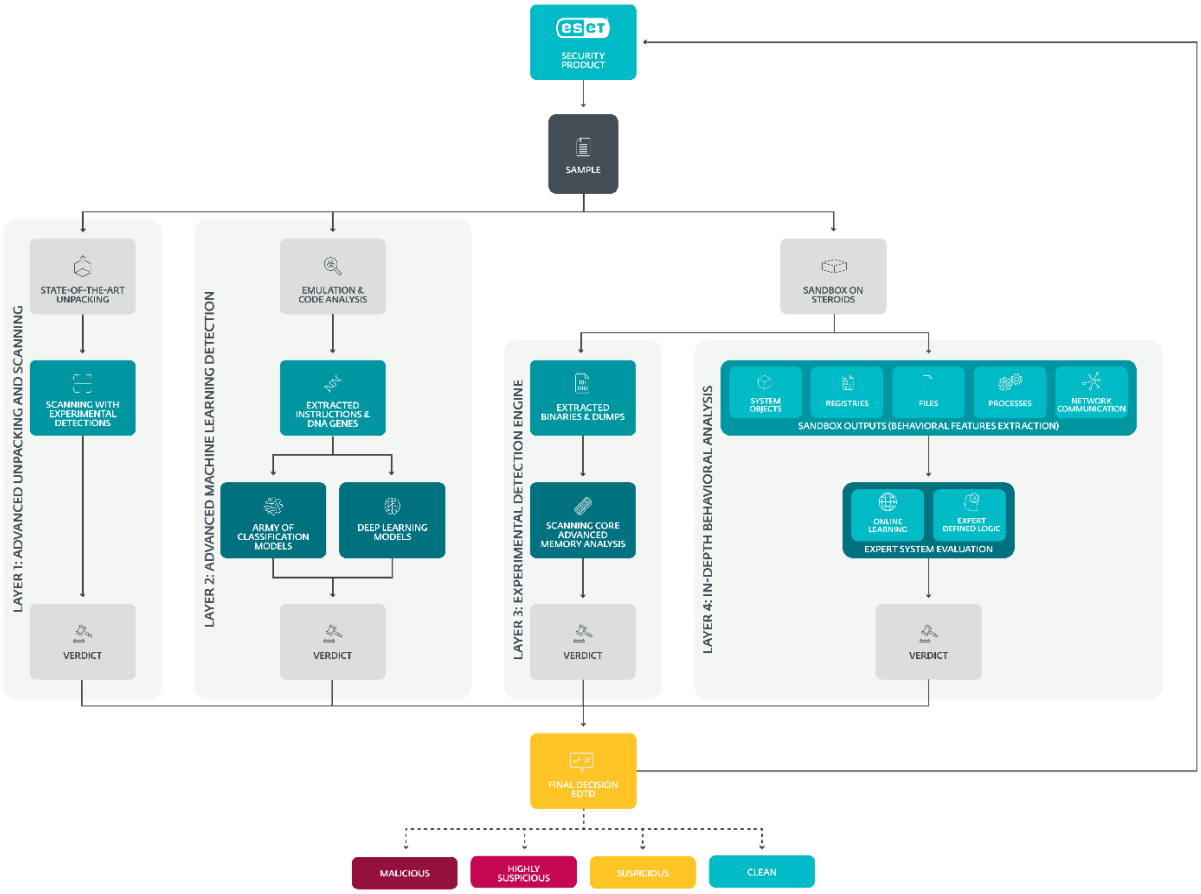


Рис. 2.13. Загальна картина рівнів виявлення загроз ESET Dynamic Threat Defense [20]

2.4. Призначення та архітектура рішення ESET Endpoint Security

Коли виникає необхідність захистити кінцеві точки від таких загроз як трояни, черв'яки, руткіти, постійна реклама та інших відомих типів атак з мережі, ESET пропонує використати додаток ESET Endpoint Security.

Використання штучного інтелекту допомагає завчасно блокувати шкідливе програмне забезпечення, при цьому використовуючи якомога менше системних ресурсів. Інструмент містить антивірусне та антишпигунське забезпечення, що допомагає в ліквідації більшості масово відомих та нових загроз. Базуючись на прийомах та методах, що спрощують вирішення конструктивних та практичних

завдань ідентифікації шкідливого ПЗ, знаходяться нові інциденти та застосовується комплекс захисту системи.

За допомогою перевірки SSL сертифікатів здійснюється захист від фішингових атак, а поштова передача відбувається виключно через POP3S та IMAPS. ESET Endpoint Security регулярно автоматично оновлюється, що допомагає зберігати актуальність алгоритмів реагування та відповідати останнім версіям ESET Protect.

Так само, як і в ESET Dynamic Threat Defense, існує можливість надсилати та переглядати дані про загрози через ESET LiveGrid. Програма надає звітність, котра налаштовується відповідно до встановленого користувачем рівня чутливості, при рівні «агресивний» чутливість максимальна та програма буде надавати велику кількість сповіщень про загрози, що може призвести до помилкового реагування на безпечні файли.

Ядро виявлення ESET Endpoint Security містить технологію виявлення руткітів, які здатні приховати своє знаходження в системі. Ця технологія нова та поки не широко поширена серед сучасних засобів реагування, що безперечно, є перевагою даного додатку. Використання цього програмного засобу в операційній системі Windows 10 дає змогу увімкнення розширеної перевірки Antimalware Microsoft Scan Interface, котра надає додаткові інструменти для пошуку шкідливого ПЗ та захисту від нього. Версія 9.0 принесла можливість захисту від атак перебору комбінацій паролів для віддалених робочих столів та блоку серверних повідомлень.

До архітектурних особливостей інструменту відноситься можливість впровадження спільного кешування для покращення ефективності роботи, оскільки повторне сканування буде усунуто, а дані перш початкового сканування будуть відправлені та доступні у спільному кеші платформи ESET Protect.

ESET Shared Local Cache це компонент, що відповідає за кешування в ESET Endpoint Security. Він завантажується окремо та налаштовується за такими параметрами: ім’я хоста на котрому розміщений програмний продукт, порт для обміну даними та пароль ESET Shared Local Cache. Окрім сканування комп’ютерів, підтримується сканування таких змінних носіїв як диски та USB-накопичувачі.

Модуль сканування підтримує опцію вибіркової перевірки. Ця опція дозволяє виконувати перевірку таких об’єктів [21] (рис. 2.14):

об’єкти, визначені у готовому профілі сканування;

змінні носії;

локальні сховища;

мережеві сховища.

Також можливе сканування таких елементів:

системний реєстр;

оперативна пам’ять;

завантажувальні сектори;

база даних Windows Management Instrumentation.

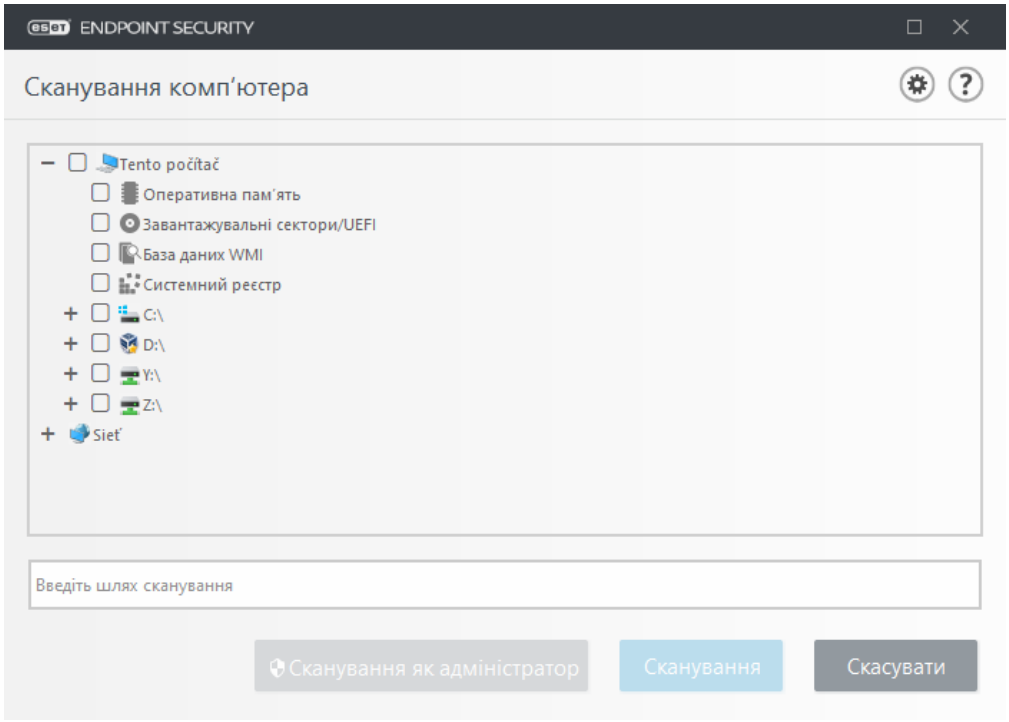


Рис. 2.14. Вікно вибору об’єктів сканування [21]

ESET Endpoint Security використовує власну технологію «ThreatSense», що вміщає в себе багато алгоритмів виявлення загроз, наприклад, емуляція коду, перевірка підписів, аналіз коду тощо. Технологія підтримує багатозадачність та дозволяє перевіряти одночасно декілька потоків інформації. Технологія використовується для захисту поштових клієнтів, доступу до мережі, фонового

сканування, файлової перевірки, а налаштовується за типом файлів для сканування, вибором необхідних методів перевірки та рівнями усунення загроз.

Використовується два типи сканування: евристичний та розширений. Евристичний, маючи ймовірність помилкових сигналів про загрози, хоч і незначну, виявляє шкідливе ПЗ, яке ще не було зареєстроване ні в одній базі загроз. Розширене сканування виявляє черв'яків та трояни, перевіряє сигнатури атак. Недоліком розширеного сканування є можливість виявлення тільки вже відомих загроз, або їх модифікацій. Технологія також дає змогу перевіряти альтернативні потоки даних у файлових системах, тобто асоціативний зв'язок файлів у системі. Вона реєструє всі дії у журналі та може вмикати Smart-оптимізацію для балансу між швидкістю та якістю сканування.

До складу ESET Endpoint Security входить ESET SysInspector та ESET SysRescue Live. ESET SysInspector перевіряє клієнтський пристрій та збирає інформацію в журнал про встановлені драйвери, програмне забезпечення, підключення та реєстр, додатково оцінюючи ризики, які ці елементи можуть нести для системи в моменті. ESET SysRescue Live це інструмент, що дає змогу створити образ системи для її подальшої інсталяції на інший пристрій та перевірки й ліквідації загроз. Інструмент запускається на будь-якій операційній системі та має повний доступ до її файлової системи.

2.5. Вимоги до системи для інсталяції ESET Protect

Безперечною перевагою використання рішення ESET є підтримка всіх популярних операційних систем, в тому числі серверних й мобільних, а також пропонується використання спеціальних пакетів для розгортання рішення на віртуальних машинах.

Платформа встановлюється на комп'ютерні системи під керуванням таких операційних систем як Microsoft Windows, macOS, Ubuntu та RedHat. Якщо мова йде про використання хмарної версії продукту, то її запуск можливий через популярні браузери, до списку котрих входять:

Mozilla Firefox;

Microsoft Edge;

Google Chrome;

Safari;

Opera.

Цікаво, що Internet Explorer не підтримується, при першій спробі запуску хмарної консолі в Internet Explorer чи іншому браузері, що не підтримується платформою, буде сповіщено про несумісність. Важливо вчасно оновлювати версії браузерів для найефективнішої роботи системи.

Комп'ютери, що використовуються платформою ESET Protect можуть бути як фізичними пристроями, так і віртуальними. Віртуальні пристрої працюють лише з IPv4 інтернет-протоколами, тоді як інші використовують також IPv6. Віртуальні робочі столи запускаються за допомогою гіпервізорів. Для платформи передбачена підтримка гіпервізорів від таких постачальників як Citrix (XenServer, XenDesktop), Microsoft (Hyper-V, інструмент Microsoft SCCM), VMware (vSphere, ESXi, Workstation, View), Oracle (VirtualBox).

Для взаємодії ESET Protect з гіпервізором не потрібний спеціальний конектор, оскільки з'єднання відбувається за допомогою агенту ESET Management, так само як і для фізичних пристроїв. Кожен віртуальний робочий стіл має свій власний ідентифікатор, який зміниться після переустановлення пристрою. Пристрій клієнта мережі звертається до каталогу віртуальних робочих столів, які надаються головним гіпервізором (рис. 2.15).

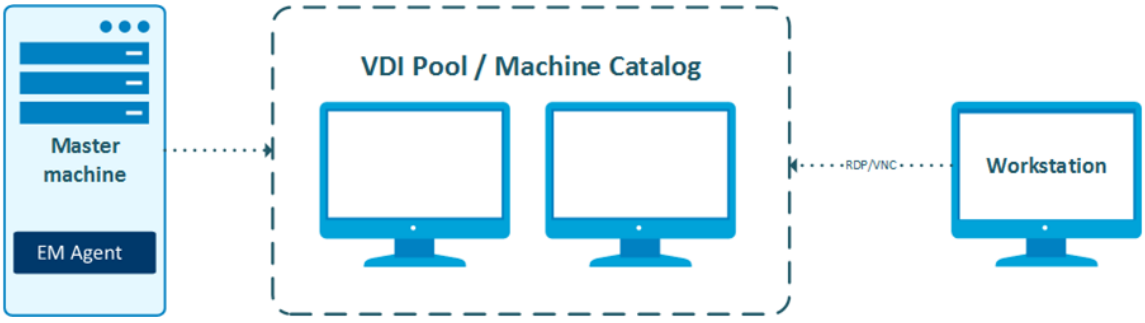


Рис. 2.15. Схема надання віртуального робочого столу [22]

Апаратні вимоги до комп'ютера, на який встановлюється ESET Protect, в комплекті з SQL Server, для кращої продуктивності, залежать від кількості клієнтів, що обслуговуються даною платформою та приведені нижче (рис. 2.16).

Кількість клієнтів	Сервер ESET PROTECT + сервер бази даних SQL			
	Ядра ЦП	ОЗП (ГБ)	Диск[1]	Диск IOPS[2]
До 1000	4	4	Одиночний	500
5.000	8	8		1.000
10,000 [3]	8	16	Окремий	2.000
50.000	16	32		10.000
100.000	16	32+		20.000

Рис. 2.16. Вимоги до апаратних характеристик системи [23]

Також компанія ESET розробила апаратні рекомендації щодо розгорнення систем розміром 10000, 20000 та 40000 клієнтів, де надані дані щодо кількості ядер процесору, частоти їх роботи та об'єму оперативної пам'яті та оцінка продуктивності роботи системи для кожного рішення від «дуже низька» до «висока» [24] (рис. 2.17).

CPU cores	CPU clock speed (GHz)	RAM (GB)	Performance		
			10,000 clients	20,000 clients	40,000 clients
8	2.1	64	High	High	Normal
8	2.1	32	Normal	Normal	Normal
4	2.1	32	Normal	Low	Low
2	2.1	16	Low	Low	Insufficient
2	2.1	8	Very low (not recommended)	Very low (not recommended)	Insufficient

Рис. 2.17. Рекомендації апаратного забезпечення для різних конфігурацій [24]

При обслуговуванні системи з кількістю клієнтів понад 10000, рекомендується встановлювати базу даних на окреме локальне сховище на базі SSD накопичувачів. Загалом, необхідно забезпечити швидкість обробки даних на один клієнт, яка буде дорівнювати не менш ніж 0,2 операцій вводу-виводу даних, що

вимірюється в IOPS одиницях. Використання хмарних сховищ допустиме, але воно не надає максимальну продуктивність.

ESET Protect підтримує Microsoft SQL Server і MySQL в якості серверу бази даних. В базі даних MS SQL Express діє обмеження в 5000 підключених клієнтів, більшу здатність підтримки клієнтів має MySQL, розміром в 10000 клієнтів, тоді як MS SQL Server не має обмежень в кількості підключених пристроїв. Версії Microsoft SQL Server підтримуються платформою, починаючи з версії «2012», а MySQL, починаючи з версії «5.6».

Необхідним компонентом ESET Protect є Apache Tomcat, який підтримується, починаючи з версії «9». Для коректної роботи Apache Tomcat потрібно встановити 64-розрядну версію Java/OpenJDK.

Захист мобільних систем виконується за допомогою ESET Mobile Security, програмний засіб виступає в ролі агента, що пов'язує мобільні пристрої з ESET Protect та має наступні вимоги до системи, на якій він встановлюється: операційна система має бути Android 5 чи iOS 9, або новіша, а мінімальна роздільна здатність екрану 240 на 320 пікселів, мінімальна потужність центрального процесору повинна бути понад 500 МГц, архітектура процесору ARM7, або краще, а мінімальна вимога до об'єму оперативної пам'яті складає 512 мегабайт.

Не підтримуються пристрої з двома SIM-картами та неофіційними версіями програмного забезпечення. Якщо пристрій не підтримує дзвінки або повідомлення, що актуально для планшетів, функції анти крадіжки та фільтру дзвінків не будуть працювати.

Для інструменту ESET PROTECT Mobile Device Connector, що відповідає за керування мобільними пристроями на окремому сервері, надаються такі апаратні рекомендації: процесор має містити 4 ядра з тактовою частотою в 2,5 ГГц, об'єм жорсткого диску має бути понад 100 гігабайт, а об'єм оперативної пам'яті понад 4 гігабайти [16]. Варто зазначити, що ці рекомендації були розроблені за умови керування вісімдесятьма мобільними пристроями.

2.6. Можливості щодо адміністрування ESET Protect

Керування платформою ESET Protect здійснюється за допомогою веб-консолі адміністратора, яка доступна після інсталяції локального рішення або зразу після отримання ліцензії продукту, у разі використання хмарної версії продукту.

Після інсталяції продукту, адміністратору безпеки необхідно виконати дії з налаштування системи для того, щоб створити робочу інфраструктуру. Таке налаштування зазвичай складається з отримання ліцензій всіх продуктів, що входять до складу платформи, додавання клієнтських пристроїв з подальшим створенням для їх агентів політик безпеки або використання вже визначених політик, що постачаються компанією ESET в складі продукту.

Адміністраторам необхідно налаштувати динамічні групи пристроїв, до яких будуть використовуватись політики безпеки, а також використати можливості ESET Protect для керування програмним забезпеченням кінцевих точок, що включає в себе видалення або встановлення додатків сторонніх виробників, а також встановлення продуктів безпеки ESET.

Користуючись платформою ESET Protect, адміністратор безпеки має можливість відстежувати статус комп’ютерів, що знаходяться в мережі компанії, за допомогою генерації звітів, у режимі реального часу та за допомогою сповіщень, що надаються системою.

Звіти можна створювати як за розробленими ESET шаблонами, так і за власними критеріями. Звіти, зазвичай, містять інформацію про комп’ютери, карантин, оновлення та виявлені інциденти чи підозрілі об’єкти. Користувач системи має право використовувати тільки ті звіти, до яких у нього є доступ згідно політики дозволів. Навіть у разі звіту, який спільно використовують декілька користувачів платформи, звіт буде персоналізованим для кожного з них, оскільки буде містити тільки ту інформацію, до якої, згідно політики, їм надано доступ головним адміністратором.

Всередині платформи ESET Protect існують власні користувачі та користувачі домену, які отримують доступ до веб-консолі та створюються

головним адміністратором. Для цих користувачів обов'язково існують набори дозволів, які визначають, яка інформація доступна користувачам для перегляду та які дії вони можуть здійснювати.

Статичні групи користувачів користуються визначеними наборами дозволів, які закріплюються за ними. За допомогою налаштування статичних груп створюються дозволи для локальних адміністраторів безпеки, які отримують доступ до всіх підгруп у визначеній для них статичній групі. Можливо навіть призначати такі набори дозволів, які сам користувач, якому вони були надані, не зможе переглядати, а тільки користуватись ними.

Типи дозволів, що надаються користувачам у платформі є стандартними та поділяються на читання, використання та запис. Дозвіл читання використовується для проведення аудиту. Дозвіл використання об'єктів забороняє проводити зміну та видалення файлів, але виконувати завдання, пов'язані з ними дозволено. Копіювання та зміна даних дозволяється правом на запис в системі. Також дозволи надаються для окремих процесів, наприклад, експорту та імпорту звітів, розгорнення агентів, використання панелі адміністратора у додатку ESET Enterprise Inspector, зміни параметру сервера, створення сповіщень тощо.

Для стабільної роботи системи у перспективі, адміністраторам необхідно використовувати функцію створення резервних копій бази даних, або налаштувати її автоматичне створення. Говорячи про обліковий запис адміністратора у системі, варто зазначити, що при інсталяції платформи він створюється автоматично, але використовувати рекомендується окремо створений обліковий запис, оскільки, у разі неполадок створеного облікового запису, завжди можна буде перейти до використання основного профілю адміністратора системи та усунути проблемні місця у системі.

Керування клієнтами мережі ESET Protect здійснюється за допомогою агента ESET Management. Це головний засіб адміністрування пристроїв платформи. За допомогою нього можливо перезаписувати та впроваджувати окремі політики безпеки пристроям, а також керувати пристроями за допомогою завдань, котрі

створюються через веб-консоль платформи, але виконуються безпосередньо агентом на самій машині.

До завдань, якими виконується адміністрування пристроїв в мережі ESET Protect можна віднести запуск сканування пристрою, отримання його конфігурації або встановленого на ньому додатку, виконання спеціальних команд на пристрої, створених адміністратором безпеки, а також запуск модулю оновлення вірусних баз даних. Для виконання завдань необхідно мати доступ, згідно політики дозволів, до об'єктів з якими вони пов'язані.

Самі завдання є, свого роду, методами автоматизації рутинних процесів у системі та визначаються за допомогою шаблонів завдань або створюються вручну. Завдання призначаються як групам, так і окремим пристроям чи користувачам системи. Завдання виконується за допомогою тригерів, які спрацьовують відповідно до визначених адміністратором параметрів та є індикаторами, що підтверджують наявність потрібних параметрів для проведення завдання. Для клієнтських завдань можливе визначення багатьох тригерів, в той час, коли для серверного завдання – тільки одного.

У політиці агента можна змінити час, протягом якого сервер буде отримувати оновлену інформацію про стан пристроїв, стандартний показник - одна хвилина, але можна встановити як коротший інтервал, для невеликої мережі пристроїв, так і довший, для великих корпорацій, щоб не перевантажувати роботу системи, наприклад, пів години.

Для адміністрування мобільних пристроїв ESET Protect з'єднується з ними за допомогою ESET Endpoint Security для Android або iOS. З'єднання здійснюється через всі можливі канали, наприклад, локальну мережу, мережу мобільного зв'язку тощо. Для коректного підключення необхідно щоб об'єкти взаємодії були правильно налаштовані та не використовували проксі-сервер. Адміністрування мобільних пристроїв передбачає підключення модулю анти крадіжки, фільтру дзвінків, а також захист від фішингу та програмних вірусів.

3 РОЗРОБЛЕННЯ ПОРЯДКУ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ РЕАГУВАННЯ НА ІНЦИДЕНТИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА БАЗІ ПЛАТФОРМИ ESET PROTECT

У цьому розділі детально описано розроблений порядок застосування технології захисту корпоративних інформаційних систем від кіберінцидентів, а саме, їх виявлення та процедура реагування на базі платформи ESET Protect.

3.1. Розроблення порядку застосування технології реагування на інциденти в корпоративній інформаційній системі на базі платформи ESET Protect

Для початку роботи з програмним забезпеченням та розроблення методу реагування на інциденти створено обліковий запис в сервісі ESET Business Account для отримання пробних версій ліцензії з повним доступом до всіх функцій ESET Protect та програмних компонентів платформи.

До програмних компонентів, котрі використовуються в даній роботі та на котрі розповсюджується пробна ліцензія, відносяться ESET Full Disk Encryption, ESET Dynamic Threat Defense в комплекті з Server Security та ESET Endpoint Security в комплекті з ESET File Security. Після проходження даного етапу, можна користуватись хмарною версією платформи ESET Protect та починати розгортання мережі пристроїв, але було вирішено встановити локальну версію продукту, а саме, версію для розгортання в віртуальному середовищі.

В якості програмного продукту, який надає можливості віртуального середовища, обрано Oracle VirtualBox. Локальна версія платформи була обрана в зв'язку з її ширшими функціональними здатностями, а також з більш професійним підходом до впровадження ESET Protect як основного інструменту забезпечення захисту інформаційних систем. В даному випадку віртуальне середовище виступає

окремим головним сервером ESET Protect, який працює на базі операційної системи CentOS 7, що базується на дистрибутиві Linux «Red Hat Enterprise Linux».

Запуск пакету інсталяції створює доступ до веб-сторінки швидкого налаштування ключових параметрів, таких як пароль бази даних, ім’я та пароль адміністратора системи, ім’я домену, мова продукту, а також, за необхідності, підключення проксі-серверу, визначення IP-адреси вручну та введення даних для роботи менеджера мобільних пристроїв.

В якості робочого клієнту ESET Protect, обрано пристрій на базі 32-розрядної операційної системи Windows 10.

Робочий клієнт підключено за допомогою згенерованого інсталяційного пакету, до якого входили програмні компоненти ESET. Інсталяційний пакет містив вже налаштоване підключення до серверу ESET Protect, а саме, дані про адміністратора, компанію, сервер та ліцензії.

Після встановлення пакету програм ESET, до якого входять ESET Management Agent та ESET Endpoint Security, клієнти автоматично починали перевірку оновлень та сканування своєї системи, а також відразу відображались у веб-консолі ESET Protect як підключені пристрої (рис. 3.1).

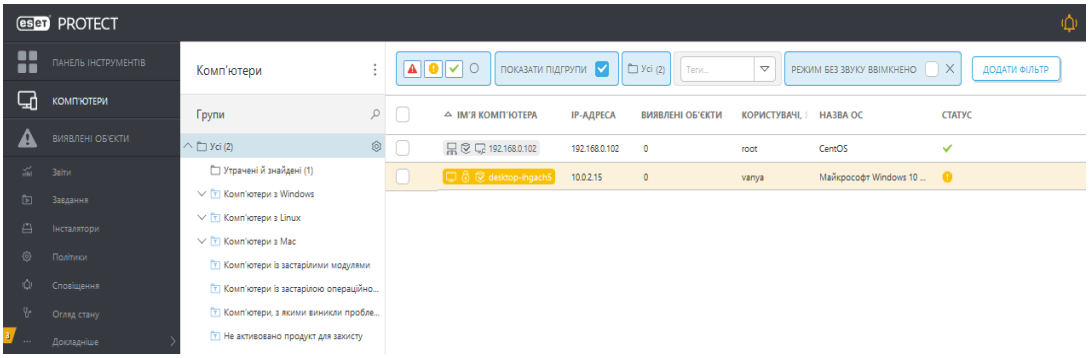


Рис. 3.1. Вікно підключених до ESET Protect пристроїв

Після виявлення клієнтів мережі, створено профіль користувача та пов’язано його з підключеним пристроєм (рис. 3.2 та рис. 3.3).

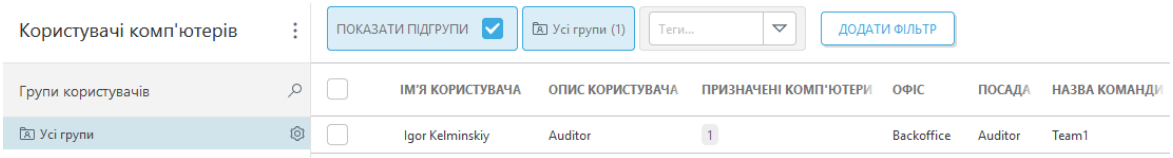


Рис. 3.2. Параметри створеного користувача

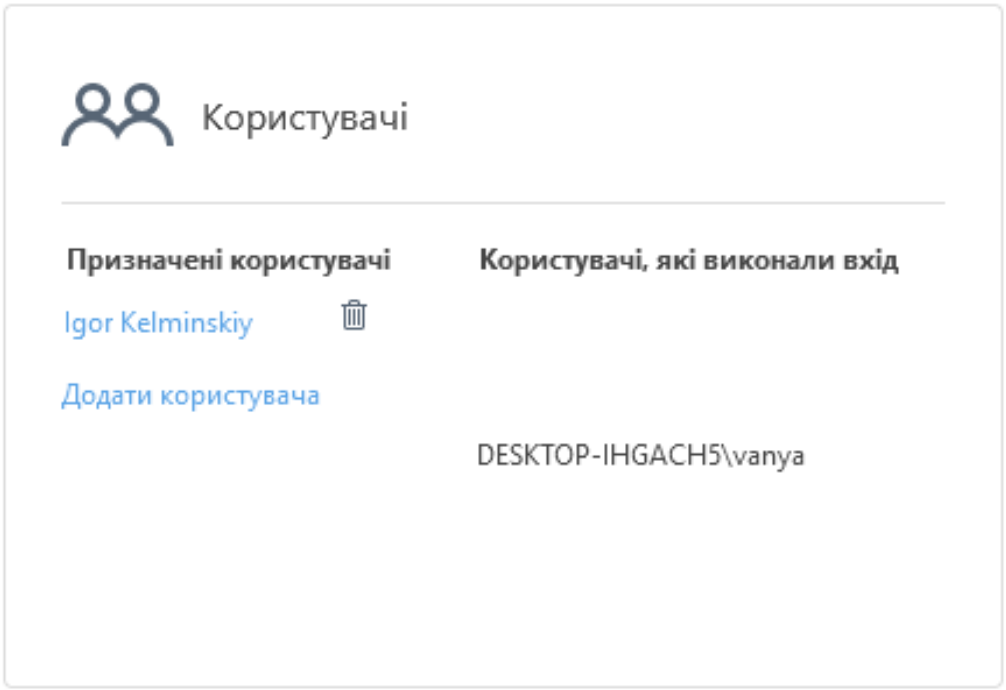
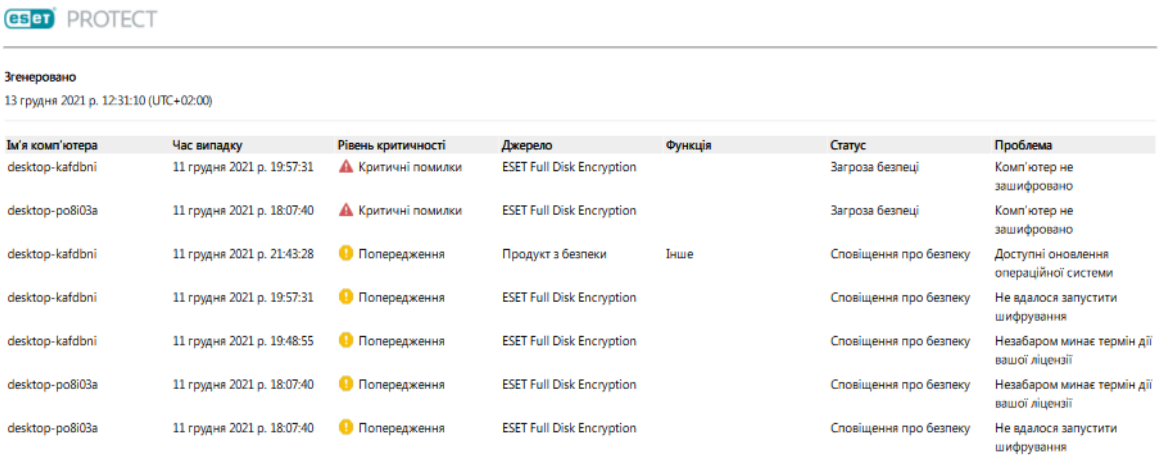


Рис. 3.3. Призначені користувачі пристрою

Після створення користувача комп’ютера, створимо користувача платформи ESET Protect. Для прикладу, створений користувач буде аудитором безпеки та буде мати доступ до платформи лише для читання інформації. Створення користувача та надання йому прав доступу відбувається в меню «Докладніше» - «Права доступу» - «Користувачі». Для прав читання, системою передбачений набір прав «Рецензент», його і застосуємо.

Першим кроком який буде здійснено для підготовки системи до здатності реагувати на загрози та протистояти їм є базовим, а саме – вирішити знайдені вразливі місця під час сканування пристроїв утилітою ESET Endpoint Security. Серед знайдених проблем є дві основні: незашифровані диски та неактуальна версія операційної системи (рис. 3.4).



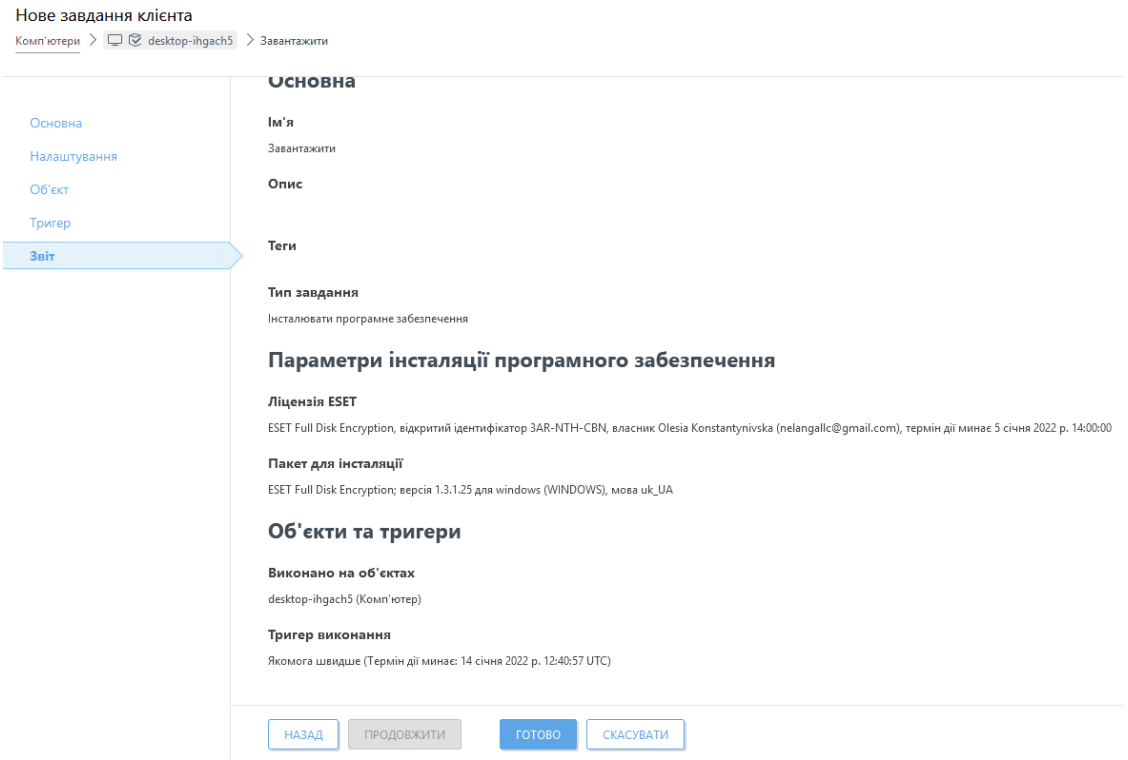
PROTECT

Згенеровано
13 грудня 2021 р. 12:31:10 (UTC+02:00)

Ім'я комп'ютера	Час випадку	Рівень критичності	Джерело	Функція	Статус	Проблема
desktop-kafdbni	11 грудня 2021 р. 19:57:31	Критичні помилки	ESET Full Disk Encryption		Загроза безпеці	Комп'ютер не зашифровано
desktop-po8i03a	11 грудня 2021 р. 18:07:40	Критичні помилки	ESET Full Disk Encryption		Загроза безпеці	Комп'ютер не зашифровано
desktop-kafdbni	11 грудня 2021 р. 21:43:28	Попередження	Продукт з безпеки	Інше	Сповіщення про безпеку	Доступні оновлення операційної системи
desktop-kafdbni	11 грудня 2021 р. 19:57:31	Попередження	ESET Full Disk Encryption		Сповіщення про безпеку	Не вдалося запустити шифрування
desktop-kafdbni	11 грудня 2021 р. 19:48:55	Попередження	ESET Full Disk Encryption		Сповіщення про безпеку	Незабаром минає термін дії вашої ліцензії
desktop-po8i03a	11 грудня 2021 р. 18:07:40	Попередження	ESET Full Disk Encryption		Сповіщення про безпеку	Незабаром минає термін дії вашої ліцензії
desktop-po8i03a	11 грудня 2021 р. 18:07:40	Попередження	ESET Full Disk Encryption		Сповіщення про безпеку	Не вдалося запустити шифрування

Рис. 3.4. Дані згенерованого звіту про знайдені слабкі місця безпеки

Оскільки до пакету інсталяції не входив продукт ESET Full Disk Encryption, тому у веб-консолі створено завдання для клієнта на встановлення даного додатку, а також завдання на його активацію і створення паролю для шифрування (рис. 3.5).



Нове завдання клієнта

Комп'ютери > desktop-ihgach5 > Завантажити

Основна
Налаштування
Об'єкт
Тригер
Звіт

Основна

Ім'я
Завантажити

Опис

Теги

Тип завдання
Інсталювати програмне забезпечення

Параметри інсталяції програмного забезпечення

Ліцензія ESET
ESET Full Disk Encryption, відкритий ідентифікатор 3AR-NTH-CBN, власник Olesia Konstantynivska (nelangallc@gmail.com), термін дії минає 5 січня 2022 р. 14:00:00

Пакет для інсталяції
ESET Full Disk Encryption; версія 1.3.1.25 для windows (WINDOWS), мова uk_UA

Об'єкти та тригери

Виконано на об'єктах
desktop-ihgach5 (Комп'ютер)

Тригер виконання
Якомога швидше (Термін дії минає: 14 січня 2022 р. 12:40:57 UTC)

НАЗАД | ПРОДОВЖИТИ | ГОТОВО | СКАСУВАТИ

Рис. 3.5. Звіт завдання з розгортання ESET Full Disk Encryption на клієнті мережі

Варто зазначити, що ESET Full Disk Encryption відмовлявся виконувати шифрування диску віртуального комп'ютеру, оскільки вимагав встановлення віртуальної операційної системи Windows з використанням UEFI (розширеного інтерфейсу вбудованої мікропрограми), після переустановлення операційної системи, шифрування диску клієнта, об'ємом 33 гігабайти, зайняло близько півгодини часу та було завершено успішно (рис. 3.6).

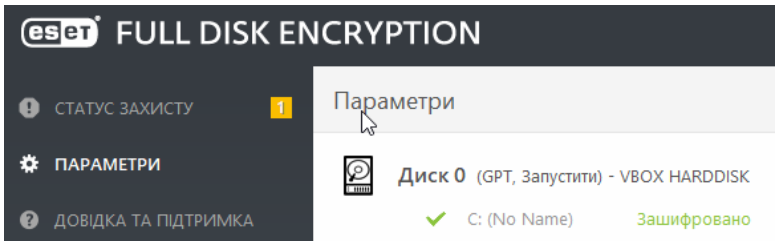


Рис. 3.6. Результат шифрування диску клієнта

Рекомендоване оновлення операційної системи вирішило такі проблеми безпеки системи (рис.3.7):

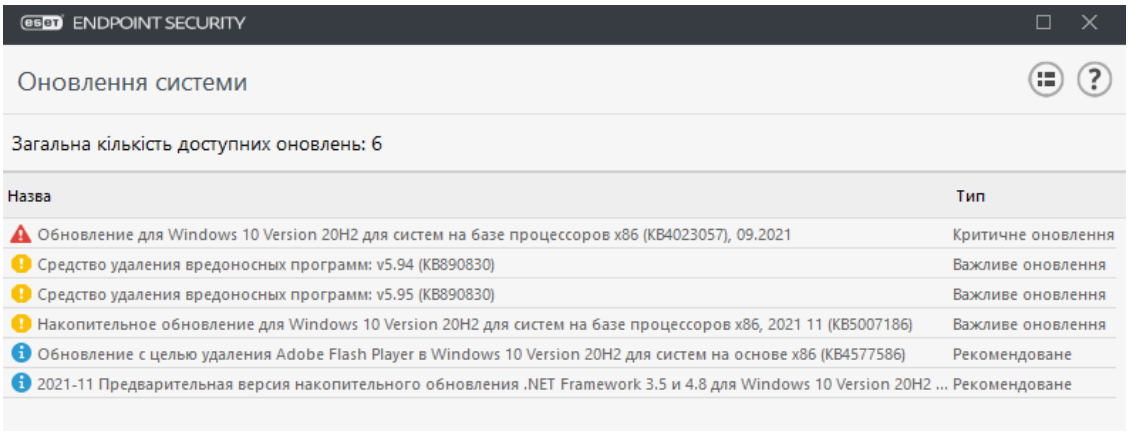


Рис. 3.7. Перелік виявлених проблем безпеки після встановлення операційної системи

Окрім оновлення операційної системи клієнта, необхідно оновити CentOS, на котрій знаходиться сервер ESET Protect.

Після виконання рекомендованих системою дій, варто підключити використання ESET Dynamic Threat Defense для перевірки файлів у хмарній пісочниці та пошуку загроз нульового дня. Це можна здійснити, перейшовши у меню підключених пристроїв та вибрати бажаний клієнт, в меню «Огляд»

підключається ESET Dynamic Threat Defense. Також можливо застосувати політику активації в розділі політик платформи для розгортання додатку на клієнті мережі, що й було зроблено.

Після активації ESET Dynamic Threat Defense, необхідно застосувати політику автоматичного надсилання сценаріїв та виконання файлів для дослідження рівня їх загрози, але перед застосуванням проведемо її налаштування, відповідно до власної методики виявлення та реагування на інциденти.

Налаштовуючи ядро виявлення загроз, вказано здебільшого збалансовану чутливість елементів виявлення (рис. 3.8). Для звітності з наявності шкідливого програмного забезпечення встановлено рівень «агресивний», що може призвести до помилкового спрацювання, але, поєднуючи цю чутливість зі збалансованою чутливістю захисту від шкідливого ПЗ, можна отримувати максимальну інформацію про виявлене шкідливе ПЗ, а автоматичне очищення буде відбуватись за менш суворими критеріями, щоб випадково не видалити з системи елементи, які помилково спрацювали на тригер.

Рішення з очищення файлів, виявлених на рівні «Агресивний» та не видалених на рівні захисту «Збалансований» буде приймати адміністратор безпеки. Потенційно небажані програми можуть спрацьовувати дуже часто та просто надавати багато зайвої інформації , що буде створювати «шум», тому рівень для них виставлено «Помірний».

Підозрілі програми є вже, так званим, «дзвоником» до початку інциденту безпеки інформаційної системи, тому рівень для них виставлено «Збалансований», оскільки рівень «агресивний» потенційно буде спрацьовувати занадто часто у великих клієнтських мережах.

Ситуація з виявленням потенційно небезпечних програм аналогічна ситуації зі шкідливим ПЗ, адміністратор буде сам вирішувати, що робити з файлами, котрі виявила система, але не усунула. Можливість користувача самостійно змінювати параметри чутливості на своєму пристрої надана тільки для розділу потенційно небажаних програм.

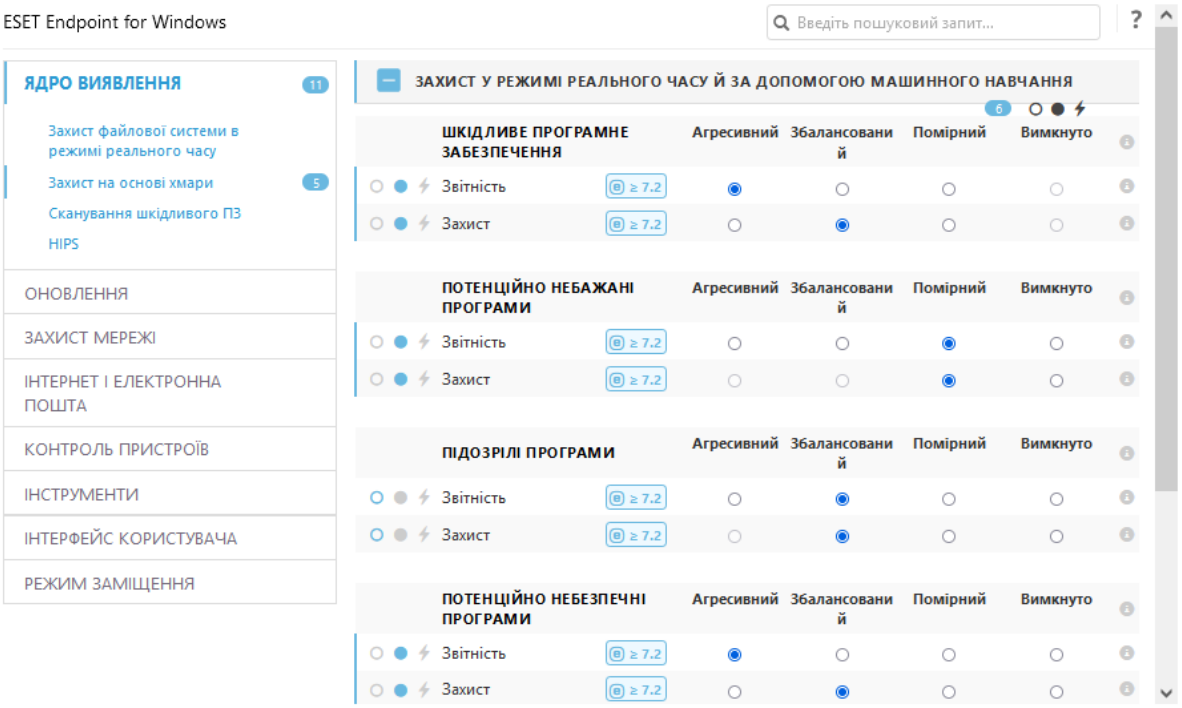


Рис. 3.8. Параметри налаштування захисту ядра ESET Endpoint

Налаштовуючи вкладку «Виключення», заблоковано для користувача самостійне додавання директорій, що не будуть скануватись ядром. Таким чином, користувачі не зможуть обмежувати роботу сканера та дозволяти роботу додатків, що могли б бути виявлені, якби не були додані до виключень (рис. 3.9). Ніколи не можна бути впевненим, що людина не захоче запустити сторонній додаток в робочій системі чи приховати його від адміністраторів безпеки.

Інші параметри ядра залишаються стандартними, а саме, використання локального кешу для ізольованих машин та ввімкнені функції антируткіту, перевірки AMSI та запуск першого сканування після оновлень.

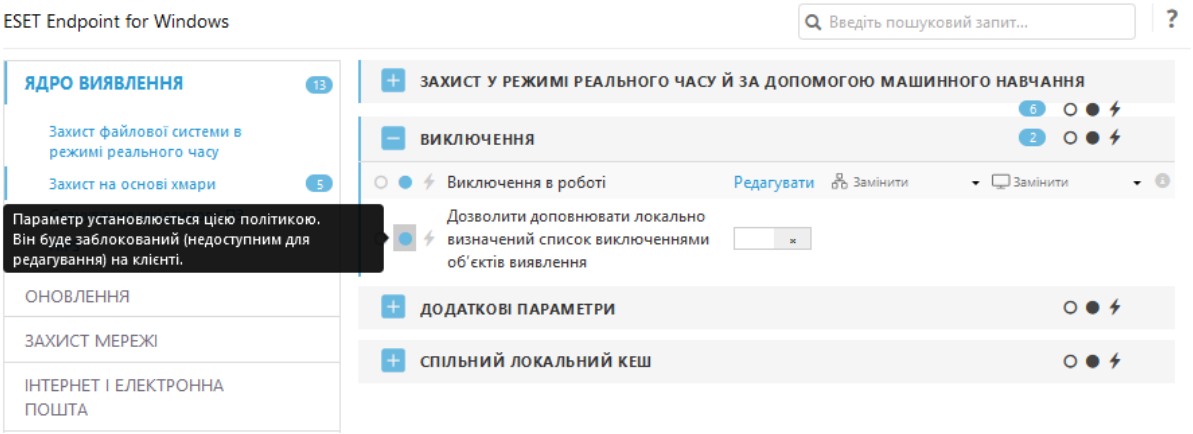


Рис. 3.9. Налаштування вкладки «виключення» ядра ESET Endpoint

Продовжуючи налаштування ESET Endpoint Protection та перейшовши до розділу захисту файлової системи, вмикаємо у розділі «Threatsense» перевірку упакованих програм та розширений евристичний аналіз, що допомагає у виявлені троянів, написаних на мовах програмування високого рівня.

Також необхідно ввімкнути редагування усіх параметрів в розділі «Захист файлової системи» тільки даною політикою, а не кінцевим користувачем. Наступним кроком необхідно налаштувати захист на основі хмари.

У даному розділі редагуємо пункт автоматичного надсилання зразків для надсилання усіх без виключень виявлених потенційно шкідливих файлів та блокуємо цей пункт від налаштування клієнтом мережі, а всі інші параметри залишаємо без змін, оскільки за замовчуванням надсилання файлів, статистики та перевеірка розширень ввімкнена.

В розділі «сканування шкідливого ПЗ» вимкнено пункти сканування архівів та фалів електронної пошти, виправляємо це та вмикаємо. Знаходяться вони у гілці «Threatsense» (рис. 3.10).

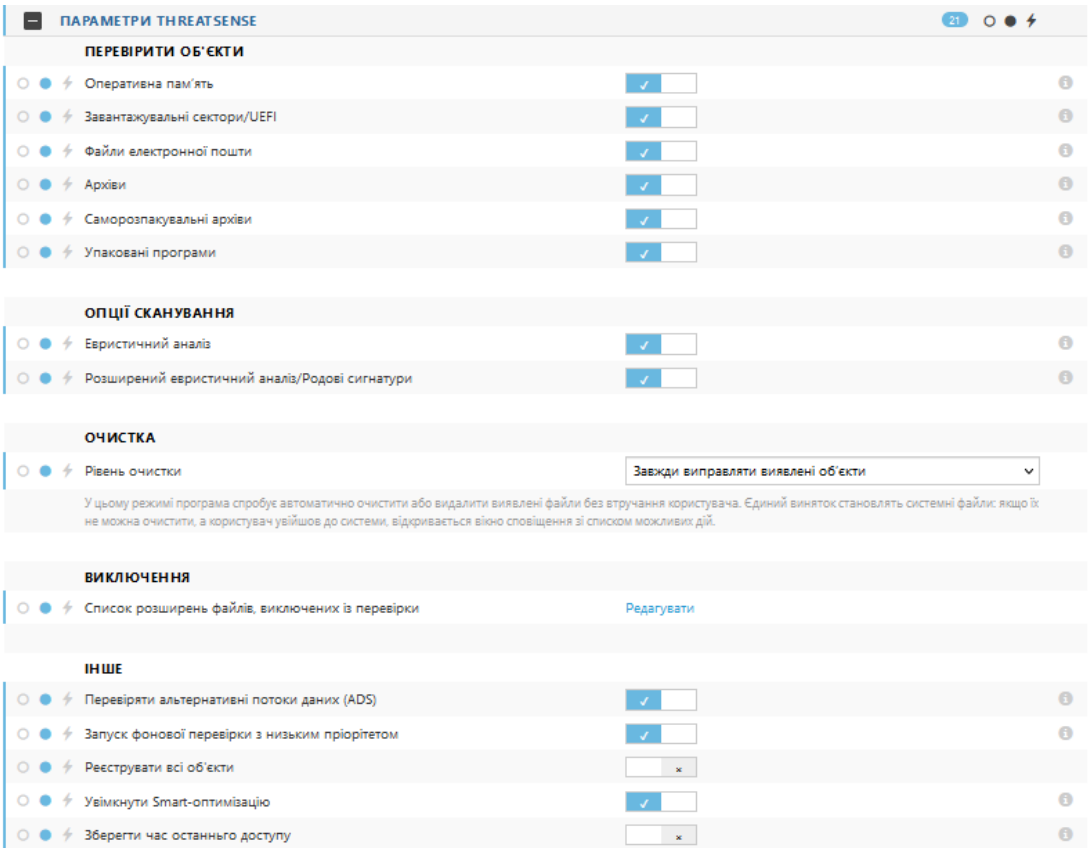


Рис. 3.10. Параметри Threatsense

Також потрібно ввімкнути сканування бази даних WMI та системного реєстру, що буде шукати посилання на інфіковані файли у вигляді даних. Ці дії, а також обмеження доступу до параметрів Threatsense для клієнтів необхідно налаштувати для усіх станів сканування, таких як «Сканування за вимогою», «Сканування в режимі очікування» та «Сканування під час запуску».

В розділі «HIPS» ядра виявлення, обмежуємо доступ клієнтів до усіх параметрів, окрім реєстрації заблокованих операцій, а також вмикаємо повідомлення про зміни в програмах, що виконуються в системі автоматично (рис. 3.11).

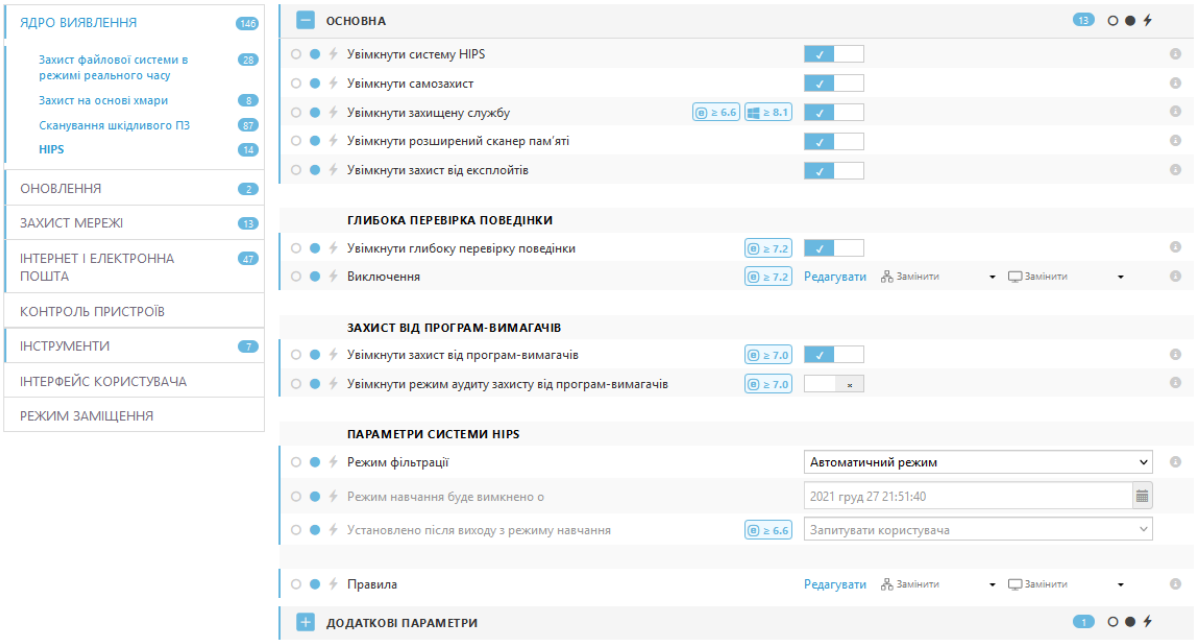


Рис. 3.11. Параметри налаштування HIPS

Переходячи до наступного пункту налаштувань політики захисту ESET Endpoint, налаштовуємо оновлення продукту. Потрібно ввімкнути автоматичне оновлення та заблокувати зміну даного параметру для користувачів у основній гілці налаштувань. Гілку «Профілі» залишаємо без змін, оскільки там за замовчуванням оптимізовано параметри для регулярного оновлення. Функція автоматичного оновлення компоненту підгримується, починаючи з версії «9.0» продукту. Блокуємо зміну клієнтами мережі параметру автоматичної зміни терміну дії ядра виявлення.

Переходячи до зміни параметрів захисту мережі від атак, змінюємо доступ клієнтів до налаштування усіх параметрів, окрім відображення сповіщень про атаки на слабкі місця системи, а також налаштовуємо правила IDS як вказано на рисунку нижче (рис. 3.12). Також перевіряємо, щоб в додаткових параметрах були ввімкнені всі пункти захисту окрім останнього, він не є обов'язковим чи критичним (рис. 3.13).

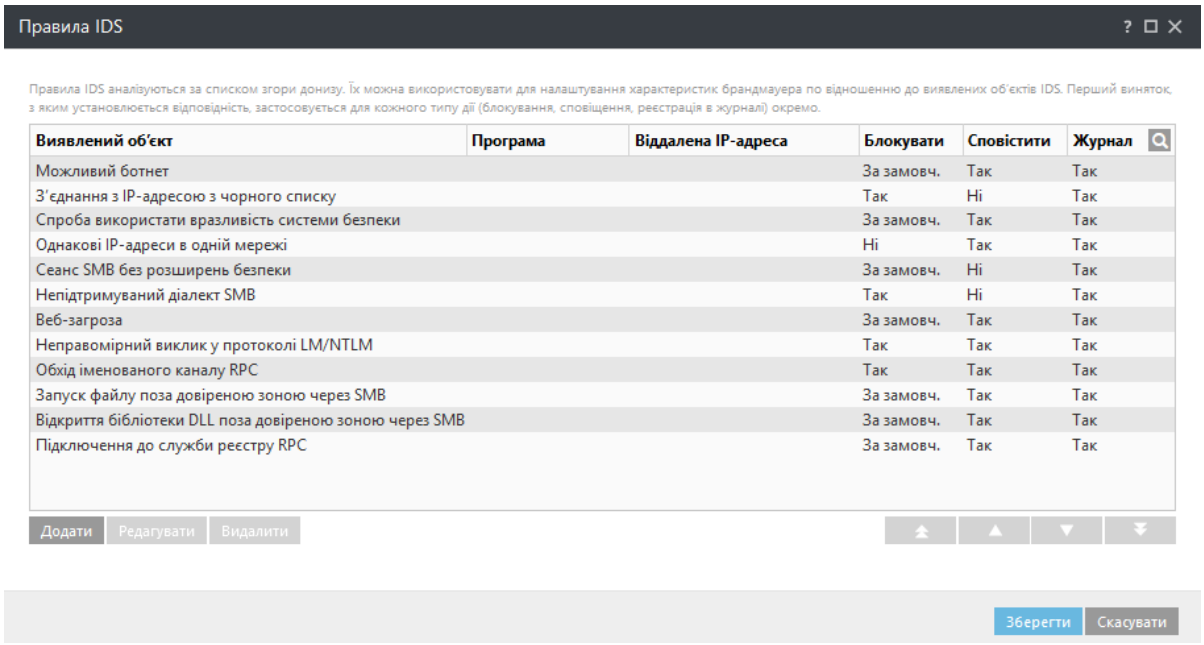


Рис. 3.12. Додавання правил IDS

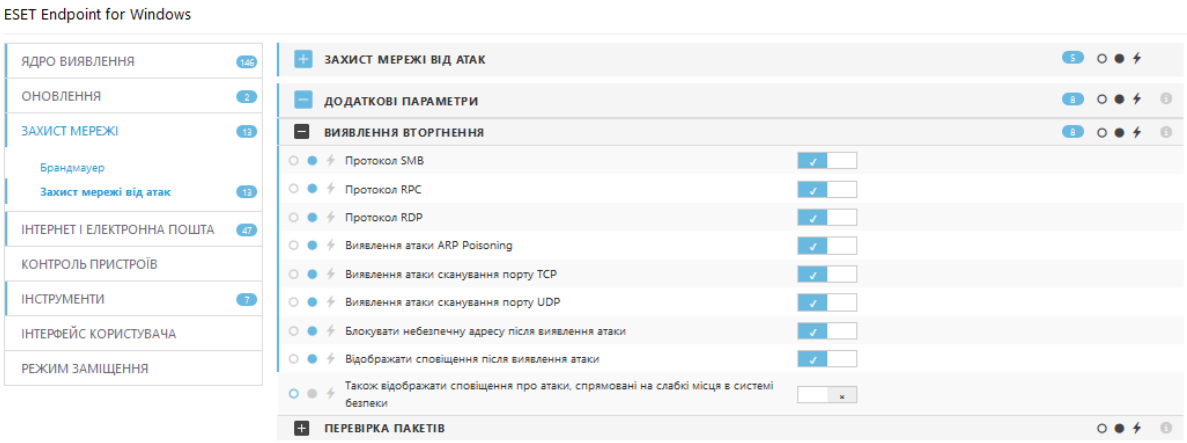


Рис. 3.13. Додаткові параметри захисту від мережевих атак

Рухаючись далі, налаштовуємо доступ до зміни параметрів захисту електронної пошти, забороняючи користувачам відключати фільтрацію вмісту протоколів HTTP(S), POP3(S), IMAP(S), фільтрацію протоколів SSL\TLS, а також фіксуючи для клієнтів мережі блокування зв'язку з використанням пошкодженого

сертифікату. В параметрах захисту поштового клієнту необхідно вказати перенесення інфікованого листа в папку «видалені», а не фактичне видалення, на випадок хибного спрацювання та заблокувати зміну параметру. Виконуємо блокування зміни всіх параметрів роботи «Threatsense».

В гілці «Антиспам» дозволяємо розширену перевірку спаму та блокуємо від зміни параметру, а також вмикаємо відмітку спам-повідомлень як прочитаних. В параметрах захисту доступу до Інтернету не змінюємо прапорці активації, але блокуємо всі функції від зміни клієнтами. Те ж саме робимо й для захисту від фішинг-атак. Вмикаємо веб-контроль для клієнту мережі та налаштовуємо правила контрою, блокуючи доступ до підозрілих ресурсів, що відносяться до вибраних категорій, а також попереджуючи про потенційну небезпеку веб-сторінок (рис. 3.14 та рис. 3.15).

Останнім пунктом захисту в Інтернеті та поштових клієнтах є ввімкнення функції «Захищений браузер», яка захищає роботу з банківськими сервісами та приховує дані, що введені з клавіатури комп'ютера.

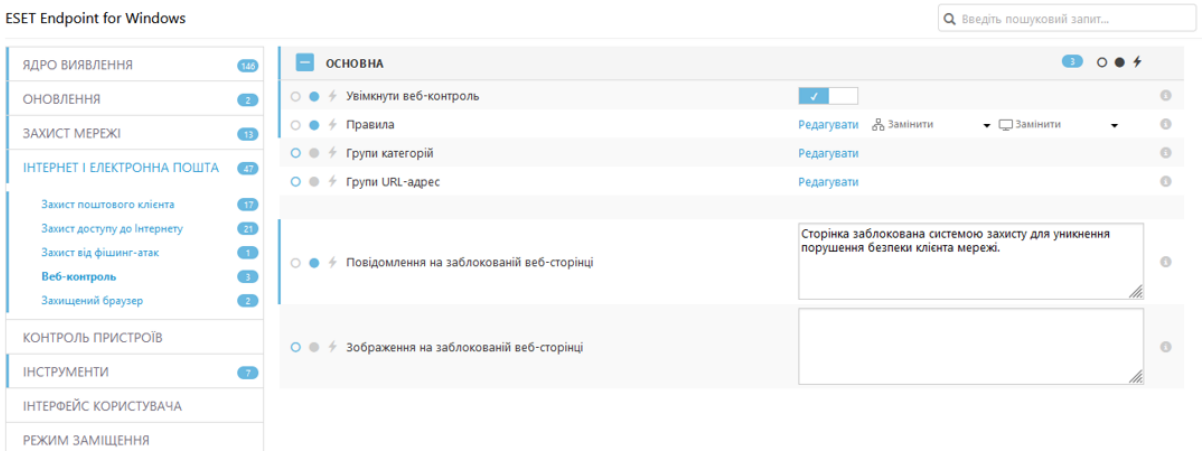


Рис. 3.14. Налаштування веб-контролю ESET Endpoint

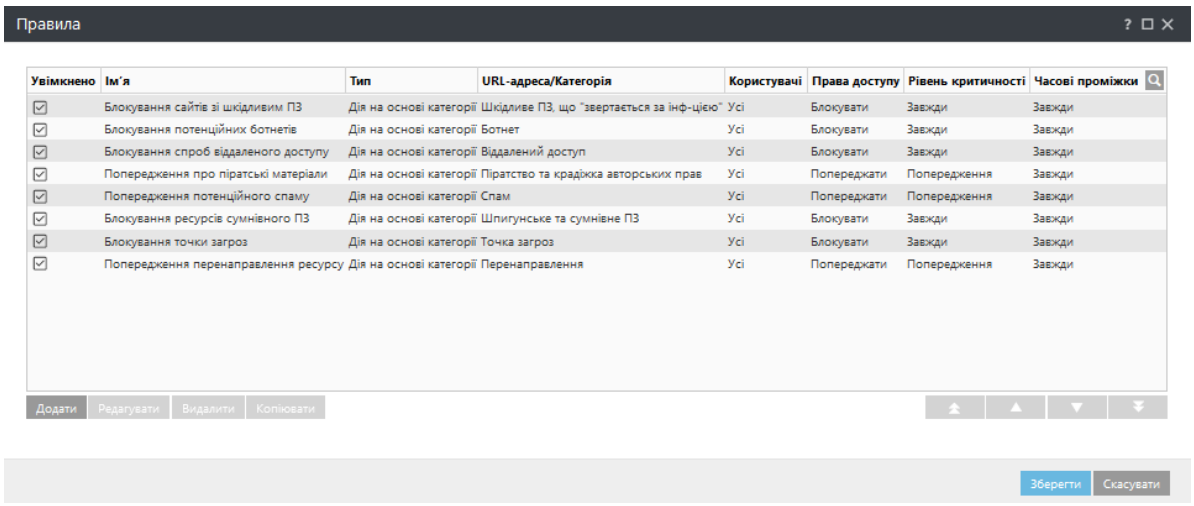


Рис. 3.15. Створені правила контролю доступу до ресурсів

Одразу ж і перевіряємо роботу налаштованих правил контролю доступу до веб-ресурсів на основі категорій. Відкрито ресурси з завантаження сумнівного ПЗ, рекламні ресурси, що перенаправляють на інші сторінки, ресурси з піратськими матеріалами. Всі вони були заблоковані для подальшого користування (рис. 3.16).

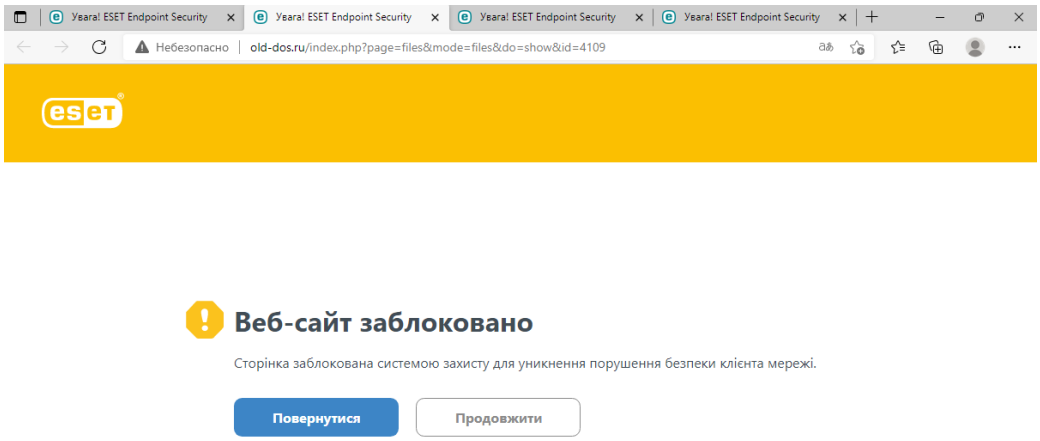
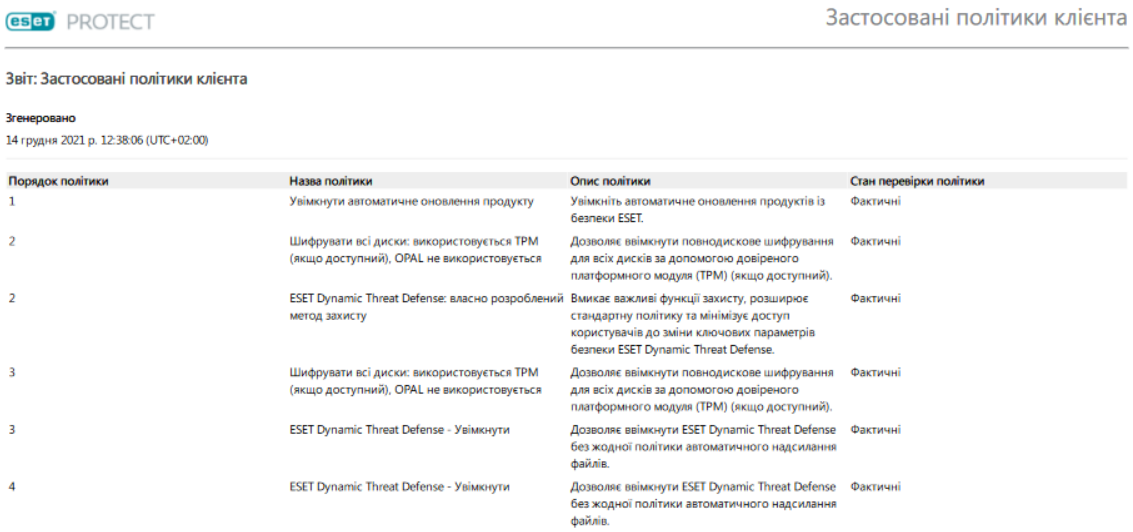


Рис. 3.16. Блокування доступу до ресурсів, згідно до визначених правил контролю

В розділі «Інструменти», гілці «Оновлення MS Windows», налаштовуємо сповіщення про доступні оновлення операційної системи починаючи з важливих оновлень, а не критичних, як виставлено за замовчуванням.

На цьому параметри політики захисту ESET Enpoint Security можна вважати налаштованими. Після налаштування політики її необхідно застосувати, що й робимо.

Згенеруємо звіт активних політик клієнту (рис. 3.17). Оскільки звіту за даними параметрами не передбачено платформою ESET Protect, його довелось створити за власними критеріями відбору (рис. 3.18).



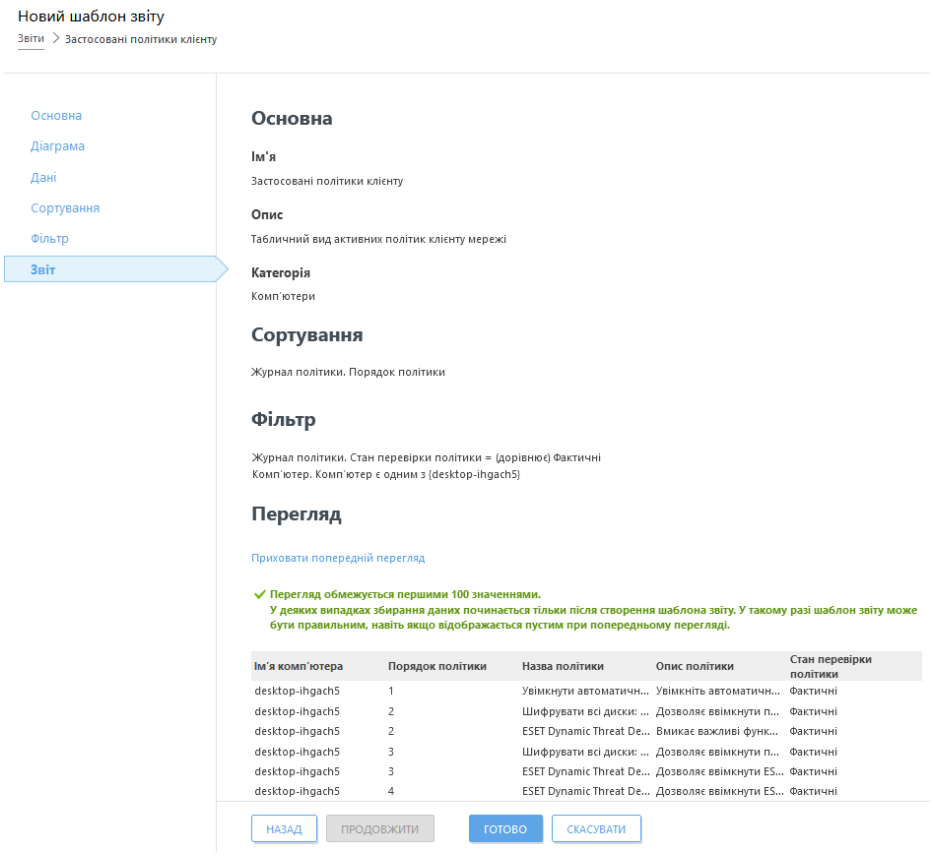
PROTECT Застосовані політики клієнта

Звіт: Застосовані політики клієнта

Згенеровано
14 грудня 2021 р. 12:38:06 (UTC+02:00)

Порядок політики	Назва політики	Опис політики	Стан перевірки політики
1	Увімкнути автоматичне оновлення продукту	Увімкніть автоматичне оновлення продуктів із безпеки ESET.	Фактичні
2	Шифрувати всі диски: використовується TPM (якщо доступний), OPAL не використовується	Дозволяє ввімкнути повнодискове шифрування для всіх дисків за допомогою довіреного платформного модуля (TPM) (якщо доступний).	Фактичні
2	ESET Dynamic Threat Defense: власно розроблений метод захисту	Вмикає важливі функції захисту, розширює стандартну політику та мінімізує доступ користувачів до зміни ключових параметрів безпеки ESET Dynamic Threat Defense.	Фактичні
3	Шифрувати всі диски: використовується TPM (якщо доступний), OPAL не використовується	Дозволяє ввімкнути повнодискове шифрування для всіх дисків за допомогою довіреного платформного модуля (TPM) (якщо доступний).	Фактичні
3	ESET Dynamic Threat Defense - Увімкнути	Дозволяє ввімкнути ESET Dynamic Threat Defense без жодної політики автоматичного надсилання файлів.	Фактичні
4	ESET Dynamic Threat Defense - Увімкнути	Дозволяє ввімкнути ESET Dynamic Threat Defense без жодної політики автоматичного надсилання файлів.	Фактичні

Рис. 3.17. Перелік активних політик комп’ютеру мережі



Новий шаблон звіту
Звіти > Застосовані політики клієнту

Основна
Діаграма
Дані
Сортування
Фільтр
Звіт

Основна

Ім'я
Застосовані політики клієнту

Опис
Табличний вид активних політик клієнту мережі

Категорія
Комп'ютери

Сортування
Журнал політики. Порядок політики

Фільтр
Журнал політики. Стан перевірки політики = (дорівнює) Фактичні
Комп'ютер. Комп'ютер є одним з {desktop-ihgach5}

Перегляд
Приховати попередній перегляд

✓ Перегляд обмежується першими 100 значеннями.
У деяких випадках збирання даних починається тільки після створення шаблона звіту. У такому разі шаблон звіту може бути правильним, навіть якщо відображається пустим при попередньому перегляді.

Ім'я комп'ютера	Порядок політики	Назва політики	Опис політики	Стан перевірки політики
desktop-ihgach5	1	Увімкнути автоматичн...	Увімкніть автоматичн...	Фактичні
desktop-ihgach5	2	Шифрувати всі диски: ...	Дозволяє ввімкнути п...	Фактичні
desktop-ihgach5	2	ESET Dynamic Threat De...	Вмикає важливі функ...	Фактичні
desktop-ihgach5	3	Шифрувати всі диски: ...	Дозволяє ввімкнути п...	Фактичні
desktop-ihgach5	3	ESET Dynamic Threat De...	Дозволяє ввімкнути ES...	Фактичні
desktop-ihgach5	4	ESET Dynamic Threat De...	Дозволяє ввімкнути ES...	Фактичні

НАЗАД ПРОДОВЖИТИ ГОТОВО СКАСУВАТИ

Рис. 3.18. Параметри створення нового звіту системи

Для налаштування агенту ESET Management виберемо вже існуючу політику, яка виконує з’єднання та обмін даними з сервером кожну хвилину (рис. 3.19). Для великої мережі пристроїв (до 10000 клієнтів) рекомендується інтервал з’єднання 20 хвилин, а для мережі до 50000 клієнтів – 60 хвилин.

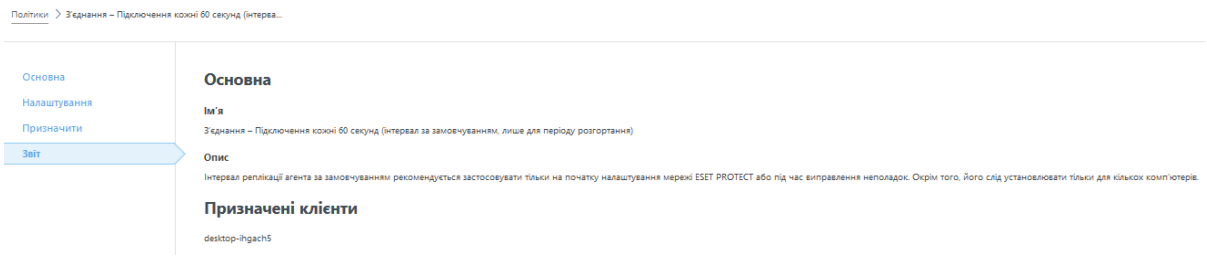


Рис. 3.19. Призначення політики ESET Management

Для перевірки налаштованого захисту клієнта мережі вирішено провести завантаження підозрілих файлів, їх виконання, а також здійснення веб-серфінгу потенційно небезпечними веб-сторінками.

При спробах перейти на веб-сторнінку, де можливо завантажити неофіційне програмне забезпечення, такі сторінки майже завжди блокувались, а перехід посиланнями завантаження блокувався кожен раз з 8 спроб переходу різними посиланнями завантаження ПЗ з сумнівною репутацією. Блокувались також веб-сторінки з сумнівною репутацією, незалежно від характеру наповнення, оскільки репутація перевіряється в базі знань ESET (рис. 3.20), а вибір блокування відповідних категорій ресурсів налаштовується правилами дозволу користування мережею в ядрі реагування.

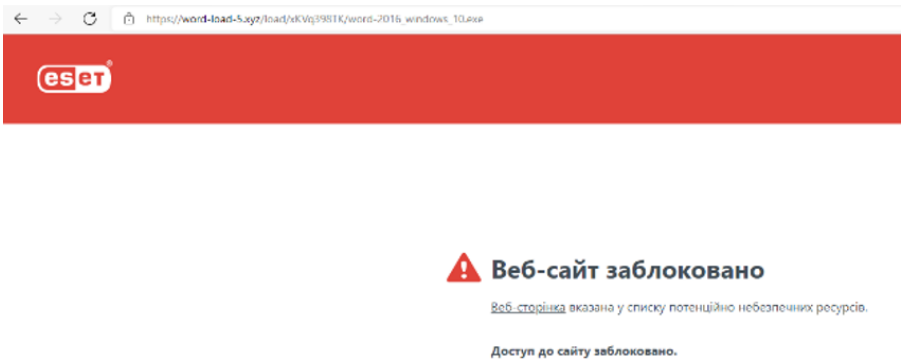


Рис. 3.20. Сповіщення про блокування спроби переходу на ресурс

Програмне забезпечення, яке завантажувалось на клієнт, як правило, бралось з бази даних найновіших виявлених шкідливих додатків «MalwareBazaar» (рис. 3.21).

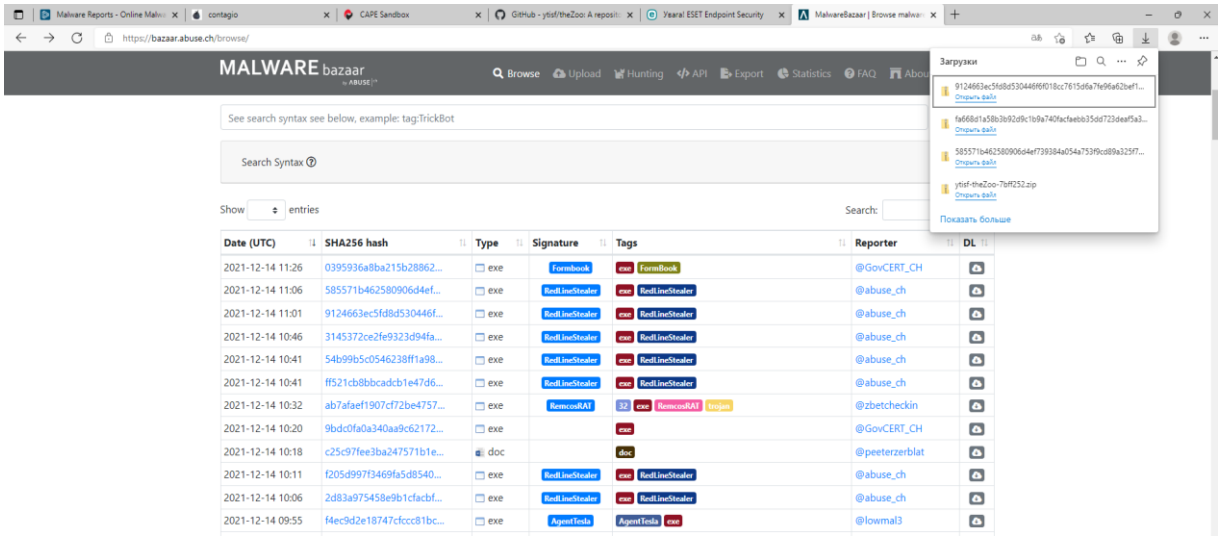


Рис. 3.21. Завантаження вірусних файлів з бази даних «MalwareBazaar»

Загалом завантажено та запущено 45 шкідливих елементів, до яких входили файли різних розширень та призначення. Серед шкідливих файлів, що були протестовані системою, були такі файли та розширення:

документи: «.doc», «.xslx», «.js», «.rtf»;

архіви: «.jar», «.zip», «.gz», «.rar», «.cab», «.ace», «.r05», «.7z»;

скрипти: «.ps1», «.vbs»;

виконуючі файли: «.exe»;

образи дисків: «.img», «.iso»;

файли бібліотек та посилань: «.dll», «.lnk»;

файли пакетів інсталяції: «.msi».

Шкідливе ПЗ, що завантажувалось з бази даних вірусів, було запаковане в архіви та проходило завантаження, а при спробах завантажити виконуючі файли напряму, файли блокувались та не завантажувались в систему. Наприклад, завантажено архів з «.vbs» скриптом, який після розпакування та спроби запуску відразу видалявся системою захисту, але за допомогою текстового редактору

відкрито тіло скрипта та знайдено посилання на шкідливий елемент «bts.ps1». Вручну скопійовано посилання та вставлено в браузер для завантаження, але, оскільки файл шкідливий, він не пропускався до завантаження в систему (рис. 3.22).

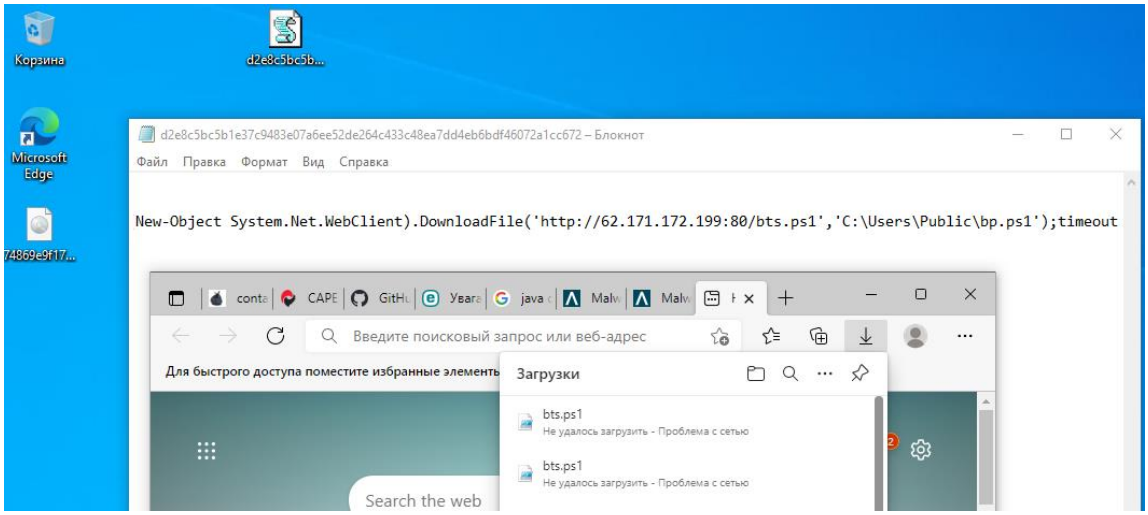


Рис. 3.22. Захист від завантаження шкідливого скрипта Windows PowerShell

Всі шкідливі «.exe» файли видалялись системою відразу після розпакування архіву, ще до їх запуску користувачем.

Образи дисків «.iso» та «.img» монтувались системою, але не були доступні, оскільки їх вміст перевірявся та блокувався для взаємодії з одночасним видаленням шкідливого компоненту (рис. 3.23).

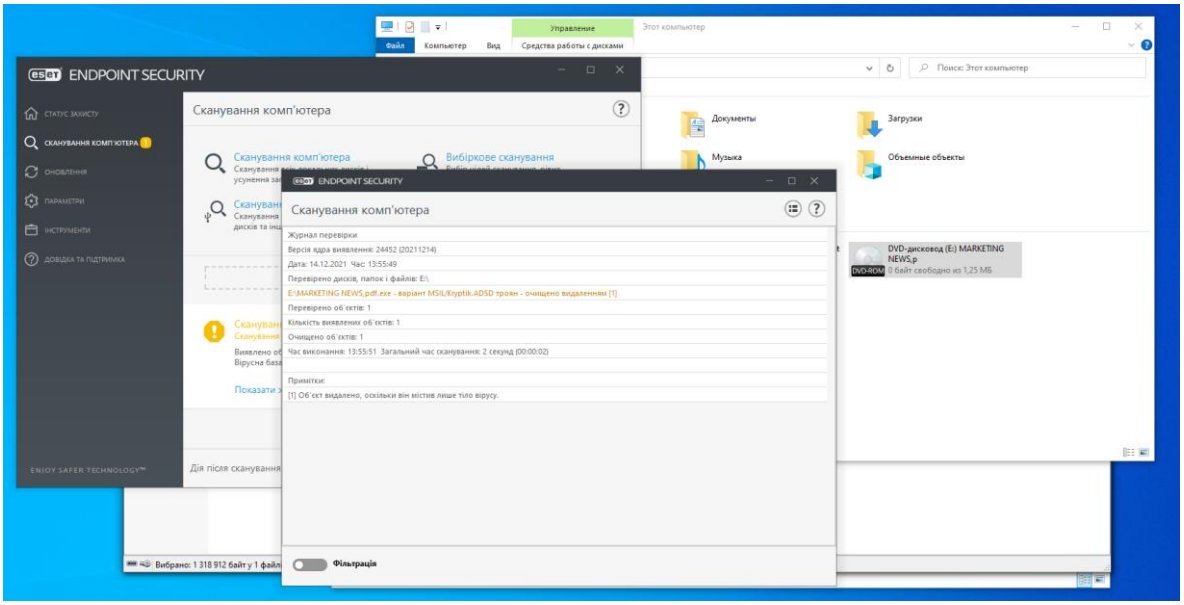


Рис. 3.23. Виявлення трояну у файлі образу диска «.iso»

Файли також можна відправляти на перевірку знаходження у базі шкідливого ПЗ через ESET LiveGrid (рис. 3.24).

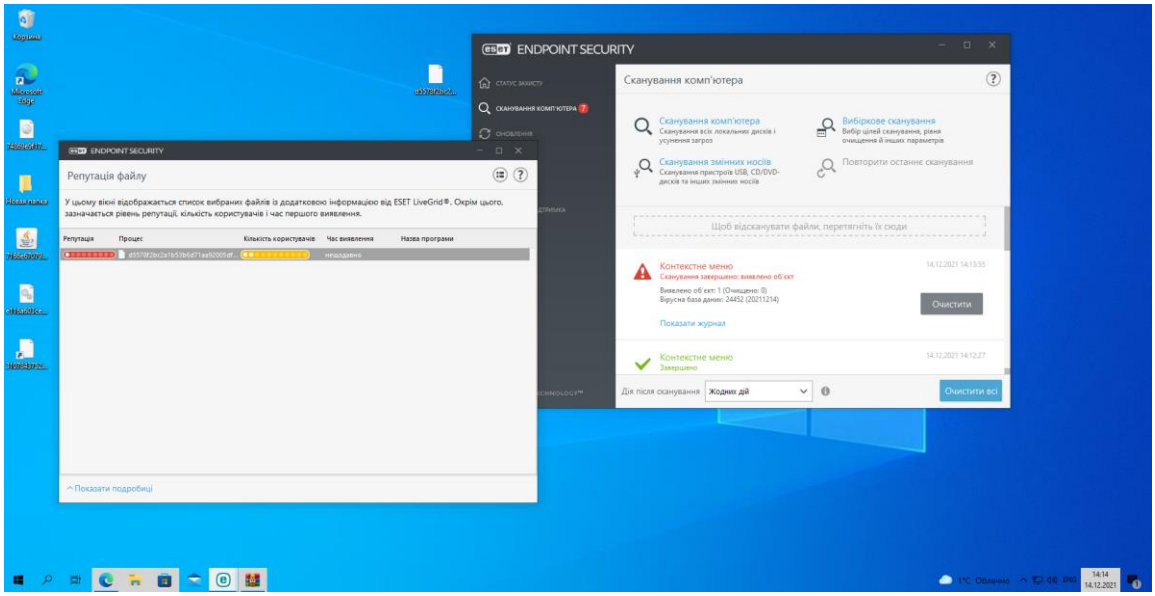


Рис. 3.24. Перевірка ПЗ на рівень шкідливості за допомогою ESET LiveGrid

Відкриття шкідливих файлів документів супроводжувалось їх автоматичним видаленням та пропозицією створити новий пустий текстовий файл з такою ж назвою.

Архіви, файли бібліотек, пакетів інсталяції та інші елементи вели себе однаково: при спробі запуску виникала помилка відкриття та файл відразу видалявся системою.

Після тестування клієнту на вразливість до атак, проведено його сканування на характер появи підозрілих елементів в системі. Відсканована всю систему та не знайдено жодного шкідливого компоненту (рис. 3.25).

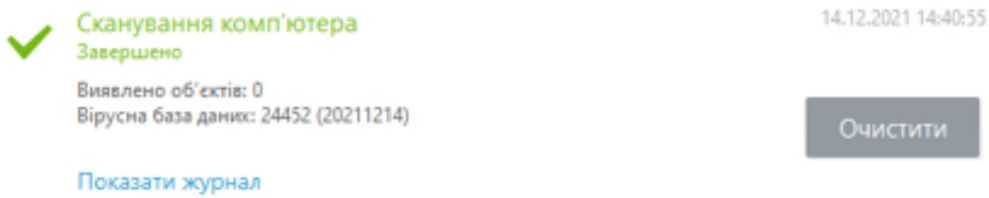


Рис. 3.25. Результат сканування системи після спроб встановлення та запуску шкідливого ПЗ

Переглянути дані про роботу системи з загрозами можливо у веб-консолі ESET Protect, а саме – в панелі інструментів. Аналізуючи дані роботи налаштованого ядра реагування на інциденти, переглянемо інформацію про роботу ESET Dynamic Threat Defense (рис. 3.26).

Рис. 3.26. Результати роботи ESET Dynamic Threat Defense з вразливостями.

Як видно на рисунку, майже всі надіслані зразки виявились безпечними, але два зразки, серед яких один файл та один веб-елемент, мали критичний рівень загрози та були заблоковані системою реагування. Також можливо переглянути інформацію по кожному проаналізованому інциденту (рис. 3.27).

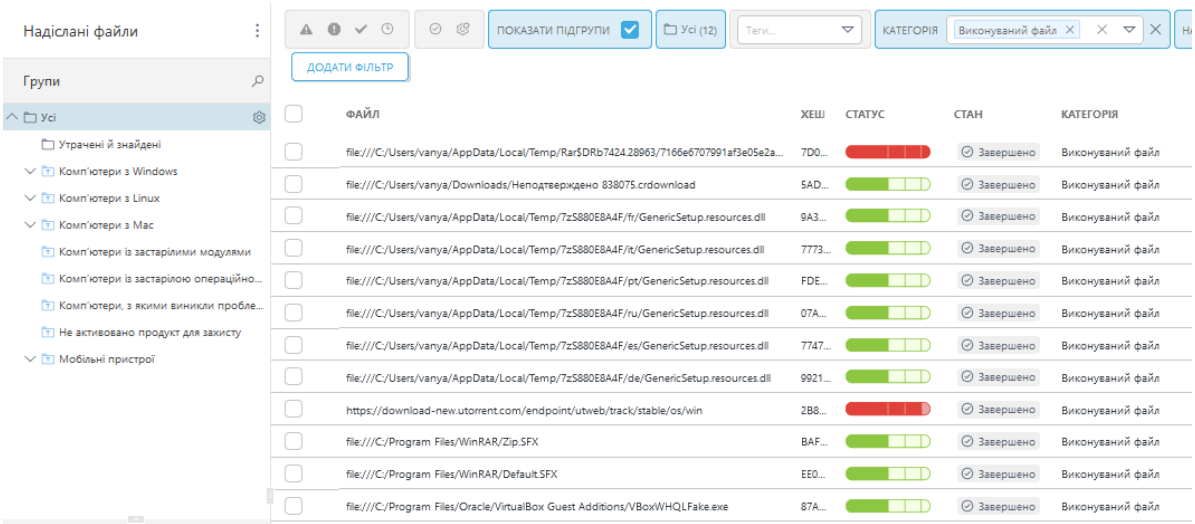


Рис. 3.27. Список проаналізованих ESET Dynamic Threat Defense інцидентів

Як вже було сказано, аналізувалась поведінка налаштованої системи реагування на інциденти на прикладі 45 найновіших вразливостей, взятих з бази

даних «MalwareBazaar». Система реагування усунула всі шкідливі елементи, що виникли внаслідок спроб запуску та тестування вірусних файлів, а також заблокувала доступ до шкідливих веб-ресурсів. Загалом картина реагування на інциденти в клієнті інформаційної системи, після налаштування ядра виявлення, виглядає наступним чином (рис. 3.28):

Згрупувати (Ім'я виявленого об'єкта)	Кількість (Ім'я виявленого об'єкта)
JS/Vjworm.DI	13850
MSIL/Adaware.A	19
MSIL/Kryptik.ADSD	13
Dynamic Threat Defense	6
Win32/Exploit.CVE-2017-11882.BOR	5
MSIL/Adaware.D	5
Win32/Formbook.AA	5
Linux/CoinMiner.TN	5
Win32/TrojanDownloader.Banload.YST	4
Win32/Spy.Numando.AL	4

Рис. 3.28. Усунуті інциденти кібербезпеки клієнта інформаційної системи

3.2. Розроблення рекомендацій щодо застосування технології реагування на інциденти кібербезпеки в межах підприємства

Якість процесу реагування на інциденти залежить від того, наскільки вміло використовуються інструменти та як саме реалізується технологія реагування.

Перш за все необхідно зрозуміти конкретні потреби організації, оскільки для великих організацій краще підходить розгортання локального серверу ESET Protect, а для малих, з невеликою, або взагалі відсутньою командою реагування – ESET Protect Cloud, хмарна версія, що нівелює більшість складнощів. Окрім особливостей вибору платформи, необхідно зрозуміти на що акцентувати увагу: на мережевий захист чи на локальний файловий, чи знаходити баланс серед них.

Після з'ясування для організації згаданих параметрів, варто здійснити перегляд всіх робочих інформаційних пристроїв, що використовуються в бізнес процесах компанії, та розповсюдити на них пакети інсталяції ESET Protect, попередньо його згенерувавши. Найкращим варіантом буде генерування повного інсталяційного пакету програм, до якого входитимуть:

ESET Endpoint Security;

ESET Management Agent;

ESET Dynamic Threat Defense;

ESET Full Disk Encryption;

ESET Enterprise Inspector Agent.

Звичайно, кількість доступних компонентів ESET Protect буде залежати від вибраних та куплених ліцензій програмного забезпечення. Мінімально допустимим пакетом для забезпечення захисту інформаційної системи є наявність ESET Endpoint Security та ESET Dynamic Threat Defense, ESET Management Agent за замовчуванням буде входити в комплект поставки платформи. Але рекомендується використання усіх вказаних компонентів системи.

Після встановлення пакетів ПЗ, необхідно провести перше сканування та вирішити вже наявні проблеми в системах клієнтів мережі, шляхом створення задач з їх виявлення. Більшість задач вже передбачена розробниками продукту, але їх модифікація, наприклад, планування відстроченого запуску, налаштування тригерів спрацювання можлива в розділі «Завдання» (рис. 3.29).

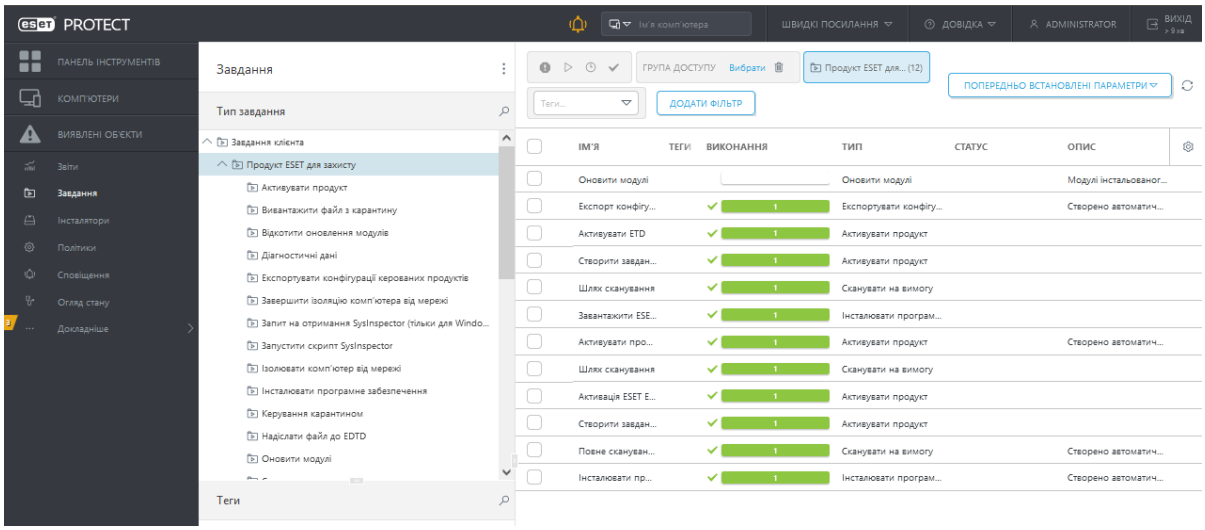


Рис. 3.29. Сторінка створення та налаштування завдань для виконання на клієнтах мережі

Окрім завдань для ліквідації слабких місць клієнту, необхідно підключити політику, що активує захист ESET Dynamic Threat Defense на комп’ютерах мережі. Це необхідно зробити з тієї причини, що після встановлення пакету програм ESET

на кінцевий пристрій, інфраструктура для роботи ESET Dynamic Threat Defense готова, але сам продукт не функціонує, оскільки не активований та не налаштований. Зробити це можна у розділі «Політики» (рис. 3.30).

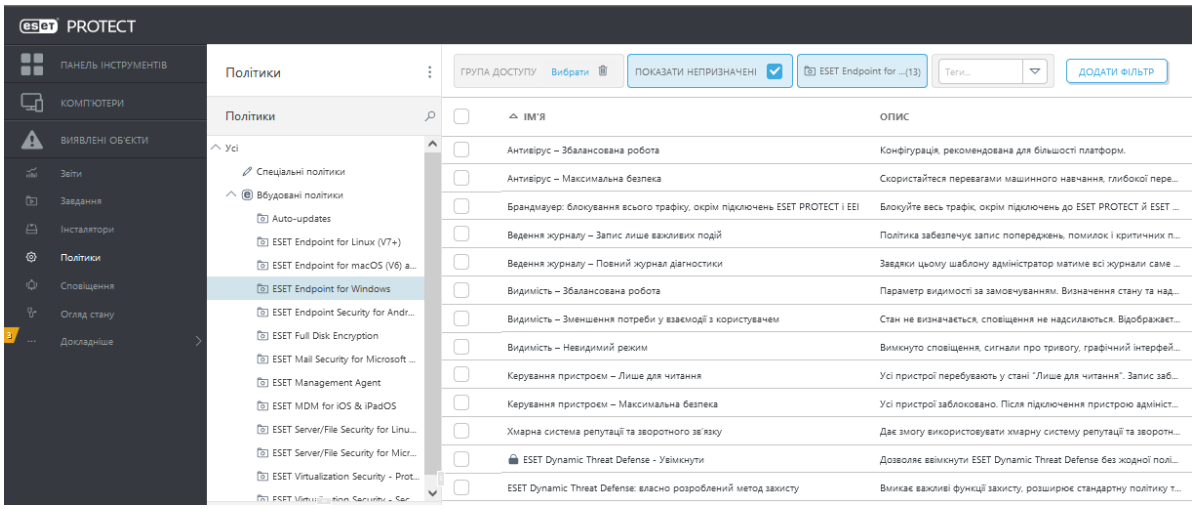


Рис. 3.30. Вибір політики для застосування на клієнті мережі

Після першого сканування необхідно створити користувачів або їх групи, які можна буде пов’язати з клієнтами мережі для подальшого налаштування захисту політик безпеки на базі груп клієнтів чи груп користувачів.

Далі всі дії, пов’язані з реагуванням на інциденти, базуються на налаштуванні політики безпеки для комп’ютерів мережі. Оскільки основним засобом захисту клієнту є ESET Endpoint Security, він і буде налаштовуватись, а точніше його ядро реагування. Для цього найкращим рішенням буде створення нової політики захисту та подальше її конфігурування «з нуля».

Основний принцип розробленого порядку застосування технології реагування полягає в налаштуванні політики виявлення та ліквідації загроз з прицілом на обмеження доступу користувачів до зміни ключових параметрів захисту системи та розширення її стандартних можливостей.

Ядро виявлення налаштовується за принципом максимального виявлення шкідливих та потенційно небезпечних програм, але видалення цих програм буде відбуватись тільки за умови достатніх причин. Іншими словами, сповіщення про шкідливе ПЗ налаштовано на максимальну чутливість, а усунення шкідливого ПЗ має збалансовану чутливість. Різницю між видаленими шкідливими додатками та

ті, про які система сповістила та не очистила, буде контролювати адміністратор вручну, оскільки максимально чутливий рівень виявлення може давати хибне спрацювання та видаляти системні файли, або файли, що важливі для робочих процесів. Рівень виявлення потенційно небажаних програм може редагуватись користувачем клієнту, так як він не є критичним. Виявлення підозрілих програм у системі налаштоване на збалансований рівень чутливості. Такі параметри захисту як захист від руткітів, перевірка AMSI є обов’язковими для даної технології.

Рекомендується використовувати максимальний захист файлової системи, що включає в себе перевірку таких типів носіїв:

локальні диски;

змінні носії;

мережеві диски.

Сканування на вразливості повинне мати дозвіл на перевірку файлу під час його відкриття, створення чи запуску, а також повинен бути наданий доступ до завантажувального сектору змінного носія.

Сканування, що використовується для виявлення загроз у файловій системі рекомендується налаштовувати для перевірки UEFI та упакованих програм, а також надавати дозвіл модулю сканування на використання евристичного аналізу та його розширеної версії з використанням родових сигнатур. Об’єкти, що виявлені сканером, повинні виправлятись автоматично, це означає очищення, тобто відправку у карантин, або видалення файлу з пристрою.

Рекомендується увімкнути систему репутації ESET LiveGrid. Це дасть змогу перевіряти окремі файли на рівень їх небезпеки, порівнюючи з існуючими даними про нього в базі знань ESET. Також обов'язковим аспектом активного захисту інформаційної системи є ввімкнення компоненту ESET Dynamic Threat Defense у ядрі реагування. Автоматичне надсилання зразків в хмарну пісочницю повинне бути ввімкнене, а можливість ручної відправки визначається самим користувачем. До ESET Dynamic Threat Defense рекомендується надсилати такі типи об’єктів:

виконувані файли;

архіви;

сценарії;

повідомлення електронної пошти з підозрою на спам;

інші: файли бібліотек, образи дисків, файли пакетів інсталяції.

Рівень ідентифікації об’єкту як загрози, рекомендується виставити при наданні оцінки «вкрай підозрілий», яку визначає ESET Dynamic Threat Defense після перевірки. Виконання файлу повинне бути заблоковано до отримання оцінки його безпеки.

Усі параметри захисту HIPS повинні бути ввімкнуті, оскільки вони забезпечують захист від експлойтів, програм-вимагачів та виконують глибоку перевірку поведінки файлів та використовують розширений сканер пам’яті пристрою.

Не рекомендується вмикати ведення розширених журналів подій безпеки, оскільки це буде перевантажувати сам журнал ,а пошук потрібної інформації буде займати дуже багато часу. Можливе підключення розширених журналів для одного чи двох найважливіших модулів, наприклад, модуля «Захист файлової системи в режимі реального часу», або модуля веб-контролю. Кожна організація повинна визначити важливі модулі сама для себе.

Ввімкнення брандмауеру є необхідною частиною захисту клієнту мережі. Рекомендується увімкнути захист від ботнетів, мережевих атак, атак повним перебором. Якщо правила захисту від атак перебором ввімкнено за замовчуванням, то правила IDS потрібно налаштувати для покращеного захисту інформаційної системи від мережевих атак. Згідно запропонованого порядку застосування технології захисту та реагування на інциденти, рекомендується налаштувати такі правила IDS:

блокувати з’єднання з IP-адресами з чорного списку;

блокувати ресурси можливих ботнетів;

блокувати ресурси, що намагаються використати вразливості системи безпеки;

повідомляти про однакові IP-адреси в одній мережі;

блокувати сеанс SMB без розширень безпеки;

блокувати передачу повідомлень чи команд з використанням непідтримуваного діалекту SMB;

блокувати веб-загрози;

блокувати неправомірні виклики у протоколі LM\NTLM;

блокувати спробу обходу каналу RPC;

блокувати запуск файлу поза довіреною зоною через SMB;

блокувати відкриття бібліотеки DLL поза довіреною зоною через SMB;

блокувати підключення до служби реєстру RPC.

В додаток до цих правил, необхідно ввімкнути всі параметри виявлення вторгнення.

Запропонований порядок застосування технології передбачає повний захист поштових клієнтів, включаючи такі параметри:

фільтрація вмісту програмних протоколів;

фільтрацію вмісту SSL/TLS;

блокування шифрованого зв'язку, що використовує старий протокол SSL v2;

при пошкодженні сертифікату, блокування з'єднання з ресурсом;

захист електронної пошти за допомогою плагінів клієнта;

сканування всіх папок повідомлень електронної пошти;

перевірка протоколів IMAP(S), POP3(S);

розширена перевірка спаму.

Захист доступу до Інтернету, захист від фішинг-атак та перевірка сценаріїв браузеру повинні бути активними, а протокол HTTP(S) повинен перевірятись системою.

Рекомендується увімкнути функцію захищеного браузеру, включаючи безпеку інтернет-банкінгу, що буде захищати конфіденційні користувацькі дані, а також увімкнути веб-контроль та налаштувати для нього наступні правила за категоріями:

блокування сайтів зі шкідливим ПЗ;

попередження про піратські матеріали;

блокування потенційних ботнетів;

блокування спроб віддаленого доступу;

попередження перенаправлення ресурсу;

блокування ресурсів сумнівного ПЗ;

попередження потенційного спаму;

блокування точки загроз.

За замовчуванням система пропонує до оновлення тільки критичні пакети оновлення Microsoft Windows. Рекомендується понизити планку до важливих оновлень.

Даних рекомендацій достатньо для налаштування коректного, а головне, безпечного функціонування інформаційної системи підприємства та виявлення будь-яких спроб втручання в роботу клієнтів мережі, з подальшим реагуванням на знайдені інциденти безпеки в автоматичному режимі.

ВИСНОВКИ

В даній роботі проведено аналіз проблеми реагування на інциденти в корпоративній інформаційній системі. Також розглянуто функції та умови функціонування інформаційних систем підприємств. Розглянуто загальну структуру інформаційної системи та кожен її структурний компонент окремо. Проаналізовано роль мережі в роботі інформаційних систем, а також ступінь важливості команди реагування, її склад та завдання в процесі забезпечення та підтримки безпечного стану корпоративної інформаційної інфраструктури.

Під час аналізу встановлено сутність завдання з реагування на інциденти. Визначено інтереси та причини атак зловмисників на інформаційні системи підприємств. Визначено чому організації потрібно відповідально ставитись до питання власної інформаційної безпеки та чим їй може обернутись нехтування впровадженням процедури захисту. Встановлено помилки в політиці організацій відносно забезпечення стабільно захищеного комп'ютерного інформаційного середовища та надано рекомендації щодо їх виправлення.

Проведено аналіз технології реагування на кіберінциденти в корпоративних інформаційних системах. Розглянуто процес підготовки та налаштування системи захисту до протидії загрозам. Досліджено такі етапи як: підготовка, виявлення, аналіз, стримування, викорінення, відновлення та діяльність після інциденту. Також звернуто увагу на процес кримінальної експертизи після того, як інцидент безпеки стався та надано рекомендації щодо підготовки до неї, а також дій, яких необхідно дотримуватись в процесі її проведення.

В ході роботи, проаналізовано методи та засоби реагування на інциденти в корпоративній інформаційній системі. Розглянуто компоненти платформи ESET Protect та їх призначення. Досліджено їх функціональні особливості та можливості використання в якості засобів реагування.

Досліджено можливості застосування програмного комплексу ESET Protect в сфері реагування на інциденти та виявлення загроз в інформаційній системі.

Розглянуто всі архітектурні компоненти платформи ESET Protect та приницп їх роботи. Також досліджено взаємодію компонентів між собою та їх поєднання в єдину систему захисту.

В роботі розроблено порядок застосування технології реагування на інциденти в корпоративній інформаційній системі на базі платформи ESET Protect та надано рекомендації щодо його застосування в межах корпоративної структури. Наданий порядок застосування технології є універсальним за своїми характеристиками та може використовуватись у компаніях різного масштабу, а також він надає можливість повної автоматизації реагування на інциденти в корпоративних інформаційних системах. Підприємству залишається тільки визначити пріоритетні загрози, від яких воно буде захищатись, та поглибитись в налаштування журналів подій та налаштування конкретних обмежень, виключень та правил, згідно з визначеними індивідуальними потребами.

ПЕРЕЛІК ПОСИЛАНЬ

1. PERSPECTIVES ON INFORMATION SYSTEMS [Електронний ресурс] – Режим доступу: https://paginas.fe.up.pt/~acbrito/laudon/ch1/chpt1-2main.htm.
2. Information Systems Components [Електронний ресурс] – Режим доступу: https://courses.lumenlearning.com/santaana-informationsystems/chapter/definition-and-components-of-information-systems/.
3. Big data Framework In The Cloud Computing. Comparing Big Data Frameworks [Електронний ресурс] – Режим доступу: https://kitrum.com/blog/big-data-framework-in-the-cloud-computing-comparing-big-data-frameworks/.
4. Types of Computer Network: What is LAN, MAN and WAN [Електронний ресурс] – Режим доступу: https://www.guru99.com/types-of-computer-network.html.
5. Global cloud services market Q2 2021 [Електронний ресурс] – Режим доступу: https://canalys.com/newsroom/global-cloud-services-q2-2021.
6. Cloud computing - statistics on the use by enterprises [Електронний ресурс] – Режим доступу: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises&oldid=546731#Use_of_cloud_computing:_highlights.
7. Alarming Cybersecurity Statistics for 2021 and the Future [Електронний ресурс] – Режим доступу: https://www.retarus.com/blog/en/alarming-cybersecurity-statistics-for-2021-and-the-future/.
8. The Three Elements of Incident Response: Plan, Team, and Tools [Електронний ресурс] – Режим доступу: https://www.exabeam.com/incident-response/the-three-elements-of-incident-response-plan-team-and-tools/.
9. A survey of emerging threats in cybersecurity [Електронний ресурс] – Режим доступу: https://www.sciencedirect.com/science/article/pii/S0022000014000178.

10. Експорт журналів у syslog [Електронний ресурс] – Режим доступу: https://help.eset.com/protect_cloud/uk-UA/admin_server_settings_export_to_syslog.html.

11. Compare new business bundles [Електронний ресурс] – Режим доступу: https://www.eset.com/fileadmin/ESET/UA_NEW_4/Pages/For_bussiness/Compare_for_business/Compare-new-business-bundles.pdf.

12. Архітектура ESET Protect [Електронний ресурс] – Режим доступу: https://help.eset.com/protect_install/80/uk-UA/architecture.html.

13. Сервер ESET Protect [Електронний ресурс] – Режим доступу: https://help.eset.com/protect_install/80/uk-UA/arch_server.html.

14. Проксі-сервер Apache HTTP [Електронний ресурс] – Режим доступу: https://help.eset.com/protect_install/80/uk-UA/apache_http_proxy.html.

15. Rogue Detection Sensor [Електронний ресурс] – Режим доступу: https://help.eset.com/protect_install/81/uk-UA/arch_rd_sensor.html.

16. Mobile Device Connector [Електронний ресурс] – Режим доступу: https://help.eset.com/protect_install/80/uk-UA/mdm_core.html.

17. [KB6715] Certificates in ESET remote management platforms [Електронний ресурс] – Режим доступу: https://support.eset.com/en/kb6715-certificates-in-eset-security-management-center-7.

18. Загальний опис ESET PROTECT Cloud [Електронний ресурс] – Режим доступу: https://help.eset.com/protect_cloud/uk-UA/index.html.

19. ESET SERVER SECURITY Key Features [Електронний ресурс] – Режим доступу: https://help.eset.com/efsw/8.0/ru-RU/key_features.html.

20. Принцип роботи рівнів виявлення [Електронний ресурс] – Режим доступу: https://help.eset.com/edtd/uk-UA/?how_detection_layers_work.html.

21. Модуль запуску вибіркового сканування [Електронний ресурс] – Режим доступу: https://help.eset.com/ees/9/uk-UA/idh_page_scan.html?idh_scan_target.html.

22. VDI, клонування та виявлення обладнання [Електронний ресурс] – Режим доступу: https://help.eset.com/protect_admin/80/uk-UA/support_vdi.html.

23. Обладнання [Електронний ресурс] – Режим доступу: https://help.eset.com/protect_smb/80/uk-UA/hardware.html.

24. Hardware [Електронний ресурс] – Режим доступу: https://help.eset.com/protect_smb/80/en-US/hardware.html.

25. Красноштан Іван Вікторович. Технологія реагування на інциденти в корпоративній інформаційній системі на базі платформи ESET Protect. ВСЕУКРАЇНСЬКА НАУКОВА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ». Державний Університет Телекомунікацій, 27 жовтня 2021. Тези доповідей. С. 87 - 88. [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/uploads/p_2099_79407917.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)