ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІС –інформаційна система

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

ШІ – штучний інтелект

AMP – Advanced Malware Protection

API – Application Programming Interface

APT – Advanced Persistent Threats

DLP – Data Loss Prevention

EDR – Endpoint Detection and Response

ERP – Enterprise Resource Planning

EPP – Endpoint Protection Platform

IOC – Indicator of Compromise

IPS – Intrusion Prevention System

HIPS – Host-Based Intrusion Prevention System

ML – Machine Learning

SOC – Security Operations Center

UEM – Unified Endpoint Management

VPN – Virtual Private Network

ВСТУП

Актуальність дослідження. Один з векторів для проведення кібератак і розповсюдження шкідливого програмного забезпечення є кінцеві точки корпоративної інформаційної системи. Тому, захист кінцевих точок є найважливішою складовою забезпечення кібербезпеки корпоративної інформаційної системи. Сьогодні класичні підходи до захисту кінцевих точок корпоративної інформаційної системи вже не забезпечують належний рівень захищеності від сучасних кіберзагроз.

Для забезпечення ефективного захисту кінцевих точок і користувацьких даних використовуються нові підходи й рішення, що забезпечують комплексний захист.

Фахівцям із кібербезпеки, які відповідальні за захист кінцевих точок, необхідно приділяти особливу увагу можливостям виявлення передових безфайлових загроз, а також можливостям розслідування і виправлення.

Об’єкт дослідження – процес забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи.

Предмет дослідження – технологія забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи.

Мета роботи – запропонувати варіант технології забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, дослідження алгоритму процесу забезпечення кібербезпеки кінцевих точок.

Практичне значення одержаних результатів полягає в розробці варіанта технології забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи на базі рішення Cisco AMP for Endpoint та рекомендації щодо її застосування на підприємстві.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КІНЦЕВИХ ТОЧОК В ІНФОРМАЦІЙНИХ СИСТЕМАХ

1.1. Аналіз проблеми забезпечення безпеки в інформаційних системах

Розглядаючи питання, наскільки важлива компанії інформаційна безпека і значаючи бюджет її забезпечення, необхідно чітко орієнтуватися у цьому понятті. Тільки так можна намітити пріоритетні напрями та скласти план відповідних дій.

Інформаційна безпека в мережах включає широкий спектр проблем. Для благополуччя бізнесу інформаційна безпека має основне значення, тому розглянемо всі завдання, які вона рішує, докладно.

Отже, перший напрямок – це забезпечення цілісності даних. Сьогодні вся комерційна інформація, бухгалтерські дані, фінансова звітність, клієнтські бази, договори, новаторські ідеї співробітників фірми, плани та стратегія її розвитку зберігаються в локальній інформаційно-комп'ютерній мережі. Не завжди і всі документи дублюються на паперових носіях, бо обсяг інформації дуже великий. У таких умовах інформаційна безпека передбачає систему заходів, що покликані забезпечити надійний захист серверів та робочих станцій від збоїв та поломок, що ведуть до знищення інформації або її часткової втрати. Серйозний підхід до цього питання означає, що інформаційна безпека має базуватися на професійному аудиті усієї IT-інфраструктури фірми. IT аудит дозволяє провести оцінку стану мережі та обладнання, зробити аналіз потенційних загроз, виявити та вчасно усунути «слабкі» місця кабельної системи, серверних та робочих станцій, дискових систем та порушень у конфігурації обладнання. Таким чином, знижуються технічні ризики можливої втрати інформації.

До пошкодження даних призводить і некоректна робота систем архівації, мережного та прикладного ПЗ. Забезпечуючи інформаційну безпеку компанії, співробітники проводять тестування програмного забезпечення та перевіряють його відповідність сучасним вимогам.

Наступне найважливіше завдання – забезпечення конфіденційності інформації. Захист комерційних секретів безпосередньо впливає конкурентоспроможність фірми та її стійкість над ринком. Тут інформаційна безпека та захист мереж стикається із зовнішніми та внутрішніми навмисними загрозами, спрямованими на розкрадання даних. Хакери, промислове шпигунство і витік інформації з вини співробітників становлять найбільшу загрозу. Спокуса продати цінну комерційну інформацію велика не тільки у працівників, що звільняються, але й у тих, амбіції яких на робочому місці незадоволені. В даному випадку, інформаційна безпека вживає превентивних заходів, спрямованих на контроль інсайдерів та багатоступінчастий захист серверів від хакерських атак.

Тому заходи щодо протидії несанкціонованому доступу мають бути спрямовані на досягнення двох цілей:

• Створення умов, коли випадкові або навмисні дії, що призводять до втрати даних, стають неможливими. Інформаційна безпека вирішує цю проблему шляхом створення системи аутентифікації та авторизації користувачів, поділу прав доступу до інформації та контролю доступу.

• Також важливо створити систему, за якої співробітники або зловмисники не змогли б приховати скоєних дій. Тут на допомогу спеціалісту з ІБ приходить система контролю подій безпеки, аудит доступу до файлів та папок.

Ефективними засобами захисту, як від зовнішніх загроз, так і від внутрішніх, є також: введення системи паролів користувачів, застосування криптографічних методів захисту (шифрування) для особливо важливої інформації, обмеження доступу в приміщення, застосування індивідуальних цифрових ключів і смарт-карт, використання міжмережевих екранів, встановлення систем захисту від витоку інформації через електронну пошту, FTP-сервери та Інтернет-месенджери, захист інформації від копіювання.

Останнім часом набули великого поширення такі способи зламування мереж, як поширення шкідливих комп'ютерних програм, що виконують функції збору та передачі інформації (троянські програми), програм-шпигунів. Для того, щоб

усунути подібні зовнішні ризики, інформаційна безпека передбачає встановлення потужного антивірусного програмного забезпечення та серверного захисту.

Інформаційна безпека мережі передбачає також захист від атак ззовні, спрямованих припинення працездатності серверів, комп'ютерів чи компонентів мережі. Йдеться про DDos-атаки, спроби підбору паролів (bruteforce-атаки). Для захисту від подібних загроз інформаційна безпека потребує застосування спеціального програмного забезпечення – міжмережевих екранів та систем проактивного захисту.

І найголовніше, для чого потрібна інформаційна безпека – доступність інформації для легітимних користувачів. Всі заходи забезпечення інформаційної безпеки є марними, якщо вони ускладнюють роботу легітимних користувачів або блокують її. Тут на перший план виходить надійно працююча аутентифікація та грамотно реалізований поділ прав користувачів. [1]

1.2. Аналіз проблеми захисту кінцевих точок

Безпека кінцевих точок визначається як практика безпеки, яка використовується для захисту кінцевих точок у мережі, включаючи пристрої користувачів, такі як ПК, ноутбуки, сервери, смартфони, планшети та віртуальні середо ща, від шкідливих програм, шпигунських програм, комп’ютерних вірусів та онлайн/офлайн-загроз.

Безпека кінцевих точок — це захист мереж організації від загроз, які надходять від локальних або віддалених пристроїв. Кінцевою точкою може бути будь-який пристрій, наприклад смартфон, планшет, ноутбук, сервер, ПК або пристрій Інтернету речей, який служить точкою входу до активів і програм підприємства. Ці пристрої є векторами атаки, які кіберзлочинці використовують для використання потенціалу вразливості кібербезпеки.

Оскільки підприємства перейняли культуру віддаленої роботи, мобільні додатки та хмарні послуги, їхні мережеві периметри стали ще вразливішими, ніж будь-коли раніше. Крім того, різко зросла кількість крадіжок пристроїв, що

призвело до величезної втрати корпоративних даних. Крім того, кіберзловмисники використовують складні рішення, які можуть легко обійти багато традиційних заходів безпеки, які використовують підприємства.

Щоб вирішити ці проблеми, організації впроваджують безпеку кінцевої точки за допомогою передо х інструментів, оснащених функціями, подібними до машинного навчання (ML), штучного інтелекту (AI), хмари, віртуальної приватної мережі (VPN), шифрування та детального контролю програм. Ці інструменти є сучасними та захищають компанії від постійно зростаючого ландшафту загроз. Вони захищають організації від атаки шкідли х програм, уразливості нульового дня та інші потенційні кіберзагрози.

Основна мета рішення безпеки кінцевої точки полягає в моніторингу та захисту кожної робочої кінцевої точки в мережі. Це досягається за допомогою централізованої консолі керування, встановленої в корпоративній мережі або на сервері. Ці інструменти безпеки кінцевих точок пропонують такі функції, як явлення вразливих кінцевих точок, багатофакторна аутентифікація, моніторинг у реальному часі, аналіз поведінки користувачів та інші для виявлення розширених загроз безпеки та, у свою чергу, керування ними.

Згідно зі звітом Statista за 2021 рік, очікується, що світо й ринок безпеки кінцевих точок досягне оцінки в 9,51 мільярда доларів у 2021 році. У звіті також прогнозується, що ринок продовжуватиме ш дко роз ватися з оцінкою в 15 мільярдів доларів до 2024 року.

Як працює безпека кінцевої точки?

Щоб пройти шлях безпеки кінцевої точки, підприємствам важливо розуміти, як інструменти безпеки кінцевої точки взаємодіють з іншими елементами безпеки, які вже існують.

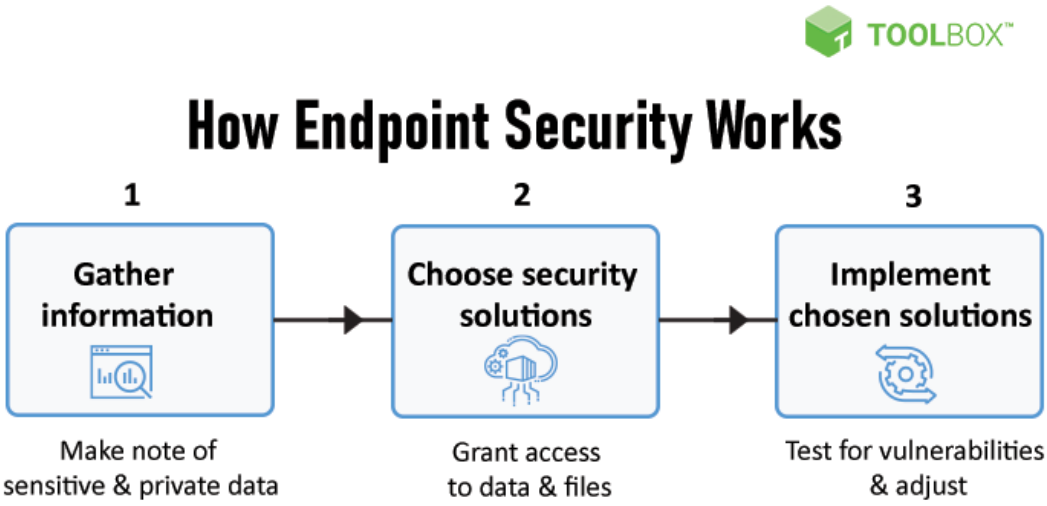

Рис. 1.1. Процес безпеки кінцевої точки

Процес безпеки кінцевої точки

Крок I: Збирати інформацію.

На першому етапі компанія повинна зібрати всю необхідну інформацію. Щоб краще захистити свою мережу від потенційних атак, потрібно знати про всі точки доступу, до яких вона підключається. Це також передбачає запис конфіденційних та конфіденційних даних разом із управління ідентифікацією та доступом (IAM). Ця активність дозволить знати, яку інформацію потрібно захищати і кому надано доступ до яких даних.

Крок II: Вибір рішення безпеки.

Після опитування та збору відповідної інформації про різні кінцеві точки потрібно вибрати відповідне рішення безпеки для кожного рівня кінцевої точки. Це може включати хмарний захист, захист мережі та захист апаратного та програмного забезпечення.

Крок III: Реалізація рішень безпеки.

На останньому кроці потрібно реалізувати вибране рішення безпеки та почати моніторинг кінцевих точок. На даному епаті потрібно виміряти продуктивність вибраного рішення та значити, чи все ще існує вразливість мережі.

Якщо відповідь ствердна, потрібно почати весь процес заново. Для цього можна перевірити всі вразливості та за потреби налаштувати рішення безпеки.

5 ключових компонентів безпеки кінцевих точок

З огляду на зростаючу популярність культури «принесіть свій власний пристрій» (BYOD) та збільшення кількості мобільних пристроїв Інтернету речей, які використовуються, організаціям важливо подумати, чи є рішення безпеки кінцевої точки достатньо комплексним, щоб протистояти загрозам на всіх фронтах. Таким чином, підприємства повинні розуміти фундаментальні компоненти рішення безпеки кінцевої точки.

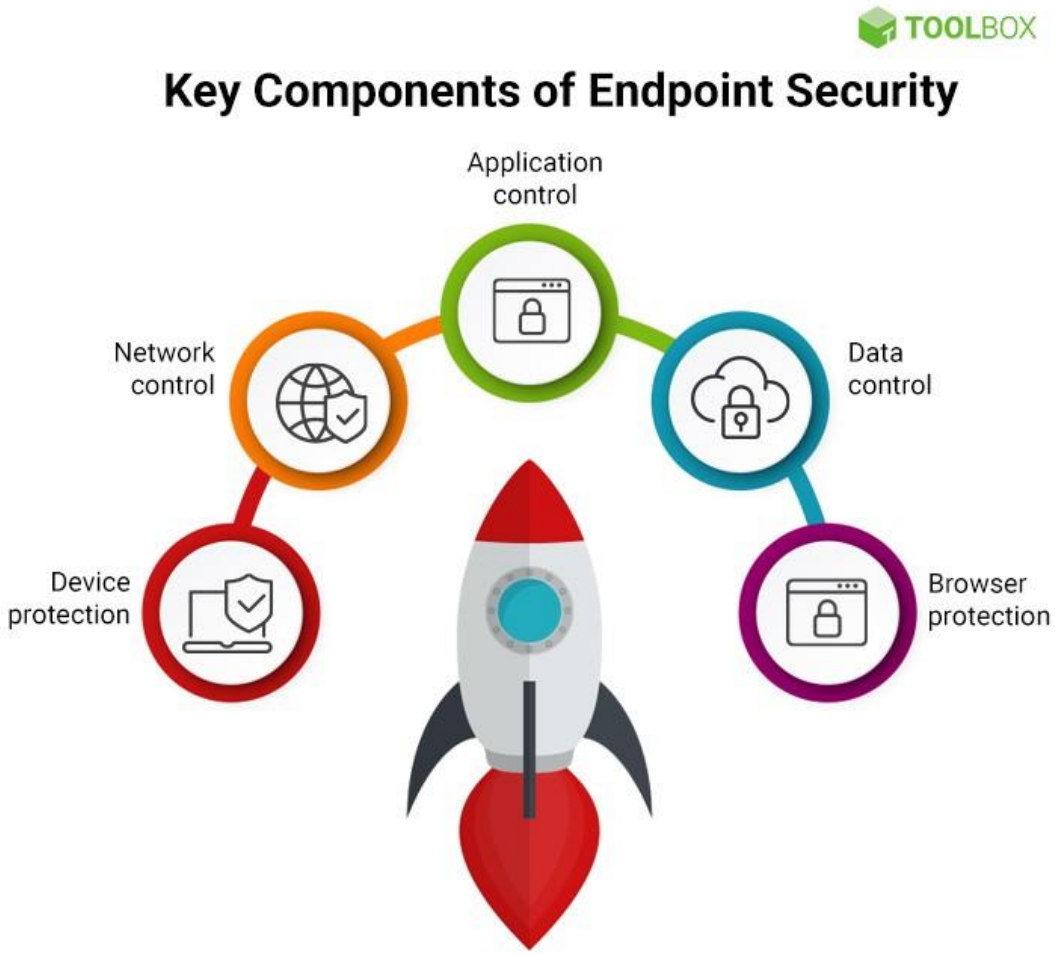

Рис. 1.2. Основні елементи рішення безпеки кінцевої точки

Компоненти Endpoint Security

1. Захист пристрою

Компонент захисту пристрою визначає та досліджує підозрілі дії на кінцевих пристроях. До них належать EDR (Endpoint Detection and Response) інструменти, які відстежують події кінцевої точки, від моніторингу та запису до аналізу подій. Це допомагає командам з IT-безпеки ефективно виявляти потенційні загрози й боротися з ними завчасно.

Рішення безпеки кінцевих точок забезпечують захист від вірусів (наступного покоління) та шкідли х програм для всіх видів пристроїв, щоб видалити нові форми зловмисного програмного забезпечення. В якості антивірусів нового покоління користовують розширену аналітику та ML, вирішення проблем нових програм-вимагачів і розширених фішингових атак, які обходять традиційне антивірусне програмне забезпечення.

2. Контроль мережі

Компонент керування мережею відстежує та фільтрує весь вхідний мереже й трафік. Це комплексний засіб, подібний до брандмауера, який допомагає виявляти, ідентифікувати та обробляти потенційні ризики безпеки, які можуть заразити мережу організації.

3. Контроль додатків

Компонент керування додатками відноситься до типу контролю, який кінцеві точки мають над додатками, що використовуються в мережі. Для цього характерна інтеграція із серверами додатків, оскільки вона допомагає визначати, контролювати та обмежувати доступ кінцевої точки до цих самих програм.

Крім того, цей компонент також включає виправлення додатків, де ризики безпеки, пов’язані з окремими програмами, повністю усуваються. Таким чином, підприємства можуть користуватися покращеним захистом, підтримуючи всі кінцеві точки, включаючи настільні комп’ютери, сервери та програми, в актуальному стані.

4. Контроль даних

Компонент керування даними керує тим, як дані обробляються в мережі. Це включає дані, які циркулюють в системі, а також дані, що зберігаються. Інструмент контролю даних запобігає витоку даних і покращує загальну безпеку даних шляхом

шифрування конфіденційних або цінних даних. Шифрування робить дані нечитаними та віддаленими для кіберзловмисників.

5. Захист браузера

Системи безпеки кінцевих точок забезпечують захист браузера за допомогою веб-фільтрів. Ці фільтри дозволяють вибирати, до чого можуть отримати доступ користувачі або які сайти вони можуть відвідувати, коли вони підключені до мережі.

Цей компонент пропонує функції керування привілеями, також відомі як принцип найменших привілеїв (POLP). Це дозволяє підприємствам надавати користувачам і обробляти мінімальний набір ресурсів, необхідних для виконання своїх завдань. POLP обмежує права доступу авторизованим користувачам і додаткам, видаляючи права локального адміністратора на серверах і ПК. Це значно знижує ризики безпеки корпоративної мережі.

Основні переваги безпеки кінцевих точок для підприємств

Безпека кінцевих точок відіграє вирішальну роль у захисті підприємств від зростаючого числа загроз безпеки, які спостерігаються сьогодні. Деякі з ключових переваг безпеки кінцевих точок для підприємств включають:

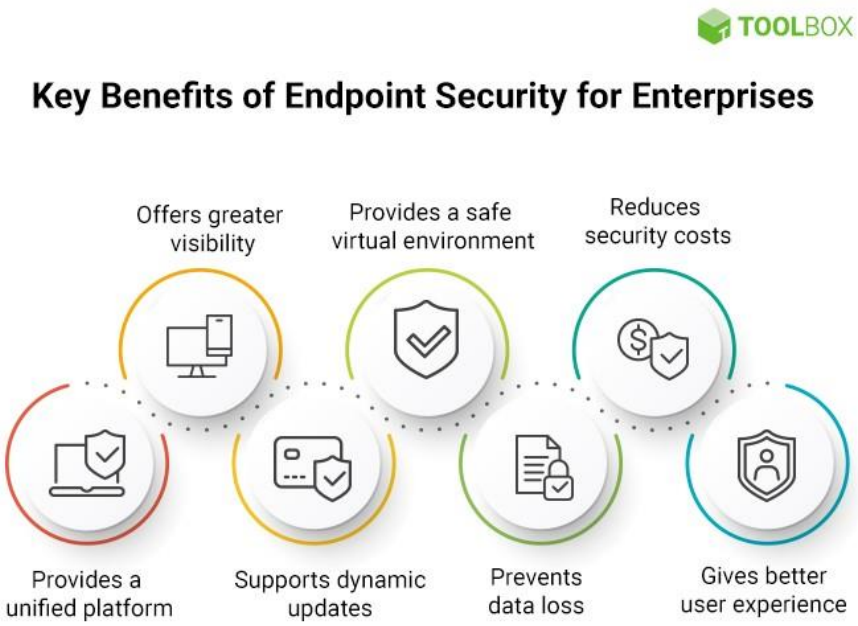

Рис. 1.3. Переваги Endpoint Security для підприємств

1. Забезпечення уніфікованої платформи

Встановлення окремих рішень безпеки може бути громіздким. Безпека кінцевої точки забезпечує єдину систему безпеки, яка підключається до всіх пристроїв і серверів. Ця уніфікована характеристика дозволяє рішенням безпеки динамічно оновлюватися, тим самим ефективно протидіючи загрозам нульового дня та багатовекторним загрозам.

2. Забезпечення кращої видимісті

Безпека кінцевої точки — це інструмент безпеки для всіх пристроїв, мереж і даних, якими вони обмінюються. Інструмент дозволяє постійно відстежувати та відстежувати програми в мережах. Це дає бізнесу більшу видимість до подій у своїх мережах.

3. Підтримка динамічних оновленнь

Безпека кінцевої точки використовує потужність хмари для забезпечення безпеки на всіх пристроях. Це означає, що будь-яке невелике оновлення в хмарі обов’язково відобразиться на всіх пристроях і мережах, підключених до нього.

4. Забезпечення безпечного віртуального середо ща

Безпека кінцевої точки створює локальний інтерфейс користувача, який нагадує оригінальні програми в мережі. Хоча ці інтерфейси є недійсними, вони діють як пісочниця, яка перенаправляє будь-які загрози, які порушують брандмауер рішення безпеки. Перевага такого налаштування пісочниці полягає в тому, що воно захищає сервери та пристрої підприємства, і зловмисники не можуть завдати йому шкоди.

5. Запобігання втраті даних

База даних є важливим активом будь-якої організації. Його компрометація може розкрити всі цінні дані компанії, тим самим зашкодивши її перспективам бізнесу та зашкодивши її репутації в галузі. Захист кінцевої точки надає функцію наскрізного шифрування даних, яка захищає дані компанії та захищає їх від кіберзлочинців. таким чином, запобігання втраті даних є однією з головних переваг безпеки кінцевої точки.

6. Зменшення витрати на захист

Безпека кінцевої точки використовує централізовану систему безпеки для керування всіма пристроями, що працюють у мережі. Це зменшує потребу наймати команду IT-безпеки, яка спеціалізується на обробці або керуванні окремими пристроями. Таким чином, централізовані операції значно знижують витрати на безпеку при безпеці кінцевих точок.

7. Забезпечення кращої роботи користувача

Кілька процедур безпеки можуть відштовхнути клієнтів від ваших бізнес-пропозицій. Однак відомо, що безпека кінцевої точки контролює програми та поведінку користувача таким чином, щоб вони могли переміщатися по мінімальній кількості процесів безпеки.

10 найкращих методів впровадження та керування безпекою кінцевих точок у 2021 році

Після початку пандемії COVID-19 компанії почали широко використовувати дистанційну роботу. В результаті все більше людей працює поза традиційними офісами. Таке робоче середо ще відкриває все більше і більше кінцевих пристроїв, які зараз діють як найбільші потенційні слабкі сторони в безпечних мережах.

Згідно зі звітом за 2020 рік, опублікованим Інститутом Ponemon, близько 68% компаній зазнали більше однієї атаки на кінцеві точки лише за останні 12 місяців.

Пристрої кінцевих точок забезпечують вхід до несанкціонованого доступу з боку зовнішніх учасників. Таким чином, система має першорядне значення для організацій, які хочуть захистити свої мережі від потенційних порушень безпеки.

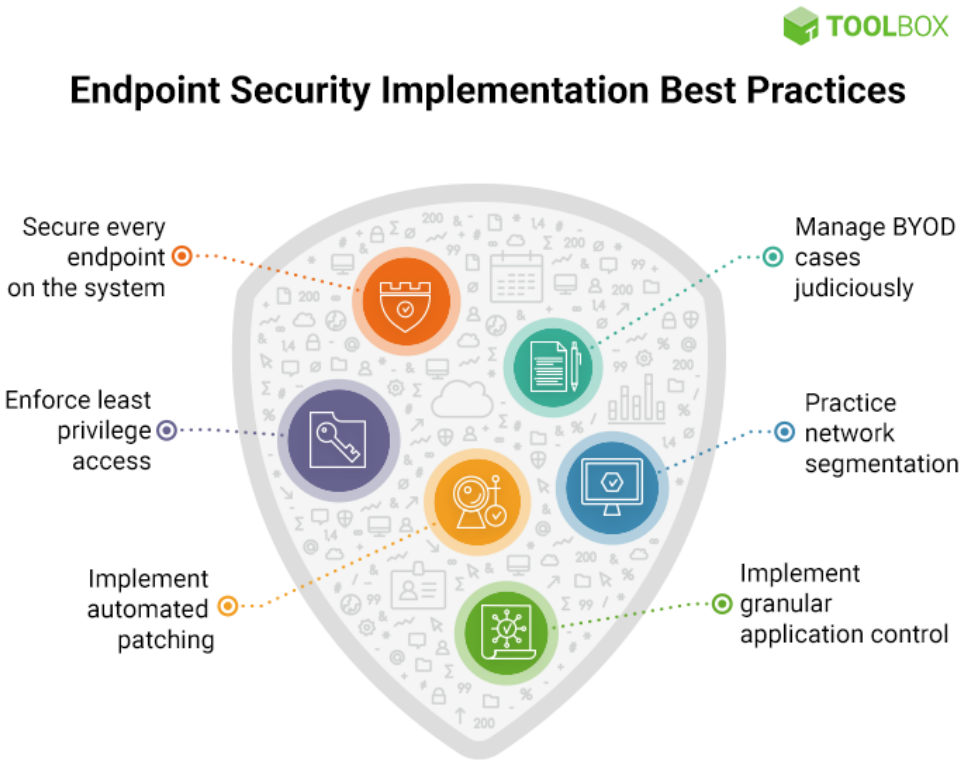

Рис. 1.4. Найкращі методи безпеки кінцевих точок

1. Захист кожної кінцевої точки в системі

Пристрої кінцевої точки діють як шлюз до мережі. Таким чином, захист і відстеження кожного пристрою, який підключається до системи, може добре служити підприємству.

Організації можуть підтримувати інвентаризацію всіх кінцевих точок мережі та оновлювати її, коли до неї підключаються нові пристрої. Крім того, вони по нні переконатися, що кожен кінце й пристрій обладнано необхідними засобами захисту, щоб захистити їх від загроз безпеці, і таким чином застосувати останні правлення відповідно до потреб.

2. Застосування надійної політики паролів і шифрування кінцевої точки

Як тільки пристрої кінцевої точки стануть безпечними в рамках заходів безпеки кінцевих точок, компанії по нні заохочувати своїх користувачів до користання надійних паролів.

Компанії можуть зробити довгі та складні паролі обов’язко м для всіх своїх користувачів. Вони також можуть заохочувати практику періодичної зміни пароля. Також організація по нна заборонити з чку повторно використовувати старі паролі. Крім паролів, компаніям може знадобитися додати додатко й рівень захисту за допомогою шифрування.

Однією з найкращих практик може бути шифрування диска або пам’яті кінцевої точки. Це гарантує, що дані пристрою залишаються нечитабельними або недоступними під час передачі на інший пристрій або в безпеці, навіть якщо пристрій викрадено чи втрачено.

3. Забезпечення доступа з найменшими привілеями

Обмеження доступа і привілеї пристрою є гарною практикою для забезпечення безпеки кінцевих точок. Права адміністратора не слід призначати з чайним користувачам. Така політика доступу з найменшими привілеями може запобігти неавторизованим користувачам завантажувати конуваний код на кінцеві точки.

4. Використання інструментів SIEM і регулярне сканування кінцевих точок

Рішення безпеки кінцевих точок повинні використовувати SIEM нструменти для забезпечення моніторингу мережі в режимі реального часу. Із зростанням кількості кінцевих пристроїв рішення SIEM тепер є частиною стандартів компанії для забезпечення загальної безпеки. Хороше рішення SIEM повинно реєструвати всі події мережі. Таке рішення також повино мати політику, яка може позначати потенційні інциденти та негайно вживати заходів щодо них.

Крім того, регулярне сканування кінцевих точок може дозволити організаціям відстежувати всі пристрої, підключені до мережі, в режимі реального часу. Це можна ще покращити, використовуючи методи постійного визначення місцезнаходження для кінцевих пристроїв, таких як смартфони та планшети, які вразливі до втрати або крадіжки.

5. Впровадження автоматизованого виправлення

Безпека кінцевої точки ефективна з автоматизованими методами правлення. За допомогою них можна динамічно запускати оновлення виправлення під час

простоїв. Організації повинні подбати про те, щоб такі автоматизовані системи також застосовувалися до виправлень сторонніх розробників.

Згідно з дослідженням Інституту Ponemon, 60% порушень, виявлених у 2019 році, були викликані не правленим програмним забезпеченням. Тут уразливості були відомі, але необхідні патчі не були застосовані.

6. Практика суворої політику доступу до VPN разом із MFA

Сьогодні, коли робоча група переходить до моделі віддаленої роботи, VPN широко використовуються більшістю корпоративних компаній. Однак VPN залишаються підданими спуфінгу, сніфінгу, DDoS та іншим зовнішнім атакам.

Таким чином, більш доцільно обмежити використання VPN, дозволяючи тим самим доступ до VPN лише на прикладному рівні. Це може значно звузити ризик безпеки на рівні мережі.

Крім того, реалізація багатофакторної аутентифікації (MFA) може запобігти крадіжці облікового запису з різних джерел. Крім того, запровадження вторинного рівня перевірки, коли система ідентифікує вхід із нерозпізнаних або невідомих місць, може підвищити загальну безпеку.

7. Керування BYOD

Дозволяючи співробітникам користуватися власними пристроями, компанії повинні мати політику, яка значає необхідні протоколи безпеки. У багатьох падках організації також можуть розглянути можливість використання політики гостьового доступу.

Підприємства повинні акцентувати увагу та зосередитися на інформуванні кінцевих користувачів про їхню відповідальність і нагадати їм про правила, що стосуються втрати чи крадіжки пристроїв. Слабка або неправильна політика BYOD може коштувати компаніям мільярдів доларів, оскільки користувачі можуть зламати мережу організації за допомогою власних пристроїв.

Подібний випадок спостерігався у 2017 році, коли стався збій даних найбільшої біржі біткойн у Південній Кореї. До цього інциденту призвела нечітка політика BYOD, коли всього за кілька годин було вкрадено 30 мільйонів доларів (у криптовалюті), що поставило під загрозу дані близько 32 000 користувачів.

8. Практика модифікації системи та використання хмарного сховища

Організації можуть обмежити доступ до конфігурації та налаштувань пристрою, щоб зменшити IT-вразливості і потенційні вектори атак. Зміцнення системи може встановити еталон для різних пристроїв і операційних систем. Він також може визначати шляхи трафіку між кінце ми точками та мережею. Як наслідок, усі інші відкриті порти (UDP або TCP) можуть бути закриті.

Крім того, компанії по нні пам’ятати, що хмара діє як ще одна кінцева точка, яка легко доступна для зовнішніх організацій. Тому для кожного користувача важливо надати окремі облікові дані. Крім того, використання протоколу TLS (HTTPS) для транспортування даних має бути стандартною практикою.

9. Впровадження детального контролю додатків

Запровадження цієї практики безпеки дозволить зосередитися на обмеженні несанкціонованого виконання програм, які становлять ризикований елемент для безпеки організації.

Компанії можуть використовувати програми керування додатками, які обмежують виконання програм на основі таких факторів, як хеш. Вони можуть підтримувати список програм, файлів і програм, які можна виконувати. Крім того, коли програмі надається доступ,потрібно переконатися, що також реалізуються правила, які блокують зв’язок з іншими невідповідними сегментами мережі.

10. Сегментація мережі

Загальну єфективність рішення безпеки кінцевих точок можна подвоїти, якщо розділити свою мережу на підмережі.

Це можна розпочати зі створення привілейованої зони та створення чітко визначеної системи за ієрархією привілеїв. Також потрібно пам’ятати про міжособистісні, міжвідомчі залежності та організаційні фактори під час сегментації мережі. Це гарантує, що звичайні бізнес-процеси не постраждають. Крім того, слід регулярно керувати та оновлювати привілейовані ресурси.

Міністерство внутрішньої безпеки США розглядає сегментацію мережі як стандартну практику безпеки, яка відіграє ключову роль у безпеці мережі будь-якої організації.

Сьогодні рішення безпеки кінцевих точок далеко від традиційних антивірусів і брандмауерів. Вони забезпечують ширший набір засобів захисту для подолання відомих і невідомих атак зловмисного програмного забезпечення, зловживань безпеки та наслідків після вторгнення.

Із значним збільшенням кількості віддалених і мобільних працівників все більше кінцевих точок піддаються зловмисникам. Це збільшує «поверхню захисту» від традиційних офісних середовищ до кінцевих точок, розподілених по всьому світу. Таким чином, запровадивши систему безпеки кінцевих точок, можна гарантувати, що всі кінцеві точки, включаючи пристрої, що належать співробітникам, захищені від несанкціонованого доступу та потенційних кібератак. Це захистить цінні дані компанії та допоможе зберегти її репутацію в галузі [2].

1.3. Аналіз основних атак на кінцеві точки

Еволюція векторів кібератак та розвиток шкідливого програмного забезпечення пояснює необхідність передового рішення захисту кінцевих точок мереж.

Загрози та вектори атак на кінцеві точки підприємства

Безфайлові шкідливі програми та атаки нульового дня

Саме шкідливе програмне забезпечення розвивається у відповідь на посилення захисту від кіберзагроз, також збільшується кількість шкідливих програм. Наприклад, за даними Інституту Ponemon, 41% атак здійснюються за допомогою «безфайлового шкідливого ПЗ», яке використовує процеси операційних систем замість завантаження файлу, подібного до класичної шкідливої програми. Тому коли негативний процес активується, з чайні антивірусні рішення не запускають моніторинг, а вбудований шкідливий код запускається і зникає без сліду.

Також підприємства мають боротися із атаками нульового дня. Вони характерні тим, що не мають сигнатури або можуть використовувати вразливість до виходу патчу. Фактично атаки нульового дня можуть обійти антивірусні

рішення за допомогою машинного навчання; вони можуть отримати атрибути, які відсутні в наборі зразків.

Сучасне рішення для захисту кінцевих точок повинно мати можливість захисту від шкідливих програм, так і від атак нульового дня.

Загрози хмари

У нещодавній статті для Dark Reading головний технічний директор WatchGuard Technologies Корі Нахрейнер передбачив, що програми- магачі скоро націляться на хмару.Він надав кілька причин для цього:

- по-перше, рутинні робочі процеси підприємств стають все більш залежними від хмари, і хакери стежать за тим, щоб максимізувати свій прибуток в умовах, коли модель spray-and-pray більше не приносить доходу. У зв'язку з цим більш цілеспрямована атака зараз перебуває на підйомі і збільшує шанси на більший прибуток у цілому.
- по-друге, Нахрейнер зазначає, що багато компаній помилково вважають, що їхні хмарні провайдери керують своєю кібербезпекою.

Таким чином, хмара є одним з нових вразливих векторів атак на кінцеві точки підприємства, які не можуть захистити ні застарілі платформи захисту кінцевих точок, ні антивірус.

В ідеалі сучасне рішення для захисту кінцевих точок має містити поведінко й моніторинг та машинне навчання, а також конфігураційну безпеку та деяку форму управління ідентифікацією.

Інтернет речей

Інтернет речей рідко поставляється з елементами кібербезпеки; вони можуть мати жорстко запрограмовані основні паролі адміністратора. Традиційні методи безпеки рідко мають можливості, необхідні моніторингу для пристроїв IoT. Навіть рішення виявлення та реагування (EDR) для кінцевих точок можуть не бачити пристрої IoT, що дозволяє їм непомітно увійти до мережі та вийти з неї. Тому IoT дає можливість хакерам створювати загрози або переміщатися по всій мережі без виявлення.

Експлойти

Далеко не всі компанії своєчасно оновлюють ПЗ та операційні системи у парку обладнання. В результаті це може призвести до того, що хакери користовують відомі (і вже виправлені в нових версіях) уразливості, щоб увійти до системи. За цим сценарієм роз валася ситуація з програмою-шифрувальником WannaCry, яка поширювалася через вразливість у протоколі SMB. Причому вразливість ця була відома Microsoft і усунена у нових патчах, які просто не були встановлені на заражених комп'ютерах.

Атаки із застосуванням мобільних додатків

Багато користувачів завантажують програми зі сторонніх джерел, щоб отримати їх безкоштовно або позбутися надокучливої реклами. Але разом з такими програмами вони можуть отримати бонус у вигляді шкідливого ПЗ, троянських модулів і процесів, що стежать за активністю користувача. Причому шанс скачати небажане ПЗ є і при використанні офіційних магазинів Play Market і App Store, які не завжди здатні виявити його до публікації. Найчастіше хакери використовують для поширення своїх шкідливих програм найпопулярніші категорії додатків, наприклад, VPN.

Атаки із застосуванням соціальної інженерії

Зловмисники під виглядом партнерів або керівництва компанії надсилають листи електронною поштою співробітникам із фінансових служб та вимагають переказати кошти на свої рахунки. Такі атаки працюють через постійну завантаженість співробітників та керівництво цих відділів та мімікрію «троянських» листів під звичайне ділове листування [6].

В цілому помітна певна тенденція: хакери відходять від традиційних типів атак, а одним з головних векторів все частіше стають не лише пристрої та ПЗ, але й користувачі, які порушують елементарні принципи інформаційної безпеки. І для захисту корпоративного периметра потрібні нові інструменти, які здатні не лише блокувати стандартні атаки, але й розпізнавати нові види, аналізувати інформацію та відслідковувати стан інфраструктури безпеки в комплексі.

Нові засоби захисту

Платформи для захисту кінцевих пристроїв типу EPP (Endpoint Protection Platform) – це класичні антивіруси, ПЗ для захисту від шкідливих програм, системи шифрування даних, файрволи та рішення для захисту від вторгнень та втрати даних. Вони справляються з відомими загрозами, але нові та незвичайні вектори атак іноді здатні їх заплутати. Зокрема, вони не мають ефективних інструментів для аналізу атак і не можуть значити, що окремі інциденти, зафіксовані в логах, — це частина комплексної кібератаки на інфраструктуру, а безфайлові віруси можуть просто не помітити.

Більш сучасні рішення відносяться до класу EDR (Endpoint Detection and Response), і їхня головна перевага — це поєднання класичних інструментів з арсеналу EPP та ефективної системи аналізу, виявлення та попередження атак (включаючи і так звані «атаки нульового дня»). Завдяки застосуванню нових технологій, наприклад, технологій ШІ, а також інтелектуальному відстеженню та фіксації всієї активності системи та її компонентів, рішення EDR набагато частіше виявляють та знешкоджують комплексні кіберзагрози та атаки без використання «прямих» методів, наприклад, безфайлові атаки.

Розгорнуте рішення класу EDR може бути доповнено службою MDR (Managed Detection & Response), тобто послугою управління виявленням загроз та реагуванням на них. Такі служби найчастіше працюють за підпискою і займаються моніторингом безпеки замовника в цілодобовому режимі. Вони дозволяють знизити навантаження на IT-фахівців компаній, взявши на себе аналіз подій, відсіювання неправдивих спрацьовувань та розстановку пріоритетів при отриманні нових даних, виявлення потенційних загроз та автоматичний підбір інструментів для захисту від них. Ці ж служби допомагають сформувати плани заходів щодо усунення загроз та запобігання повторним атакам, що особливо важливо для компаній з недоукомплектованим або мінімальним штатом фахівців з інформаційної безпеки.

В ідеальній ситуації всі ці інструменти для зручності клієнтів об'єднуються в один програмний комплекс, який здатний працювати з будь-якими платформами; реагувати на виявлені небезпеки без участі користувачів; використовувати

поведінковий аналіз та виявляти нові типи загроз, за необхідності обмінюючись інформацією з централізованою базою даних; контролювати конання додатків на кінцевих пристроях та керуватися з єдиного центру.

Такий підхід у реалізації своїх рішень дозволяє вендорам створити багаторівне й захист як від класичних шкідливих, так і від нових і просунутих типів атак. Також подібні комплекси сильно полегшують роботу IT-фахівцям і набагато краще захищають корпоративні мережі від користувачів, які не надто замислюються про те, які програми завантажують та які сайти відвідують у робочий час. [5]

1.4. Аналіз технологій із забезпечення безпеки кінцевих точок

Служба безпеки EDR - це інструмент, який використовується для постійного моніторингу та реагування на інтернет-загрози.

Агенти встановлюються на кінцевих точках для збору та надсилання даних про поведінку до центральної бази даних з метою аналізу. Пізніше, використовуючи інструменти аналітики, виявляються закономірності та виявляються аномалії.

EDR постійно контролює події на кінцевих точках. Інструмент записує інформацію в центральну базу даних. Потім дані аналізуються та проводиться розслідування. Звітування та зміни будуть базуватися на цьому розслідуванні. Хост-система матиме програмний агент. Цей програмний агент здійснює моніторинг подій та звітування.

Відповідно до досліджень, проведених Гартнер, Ринок EDR подвоїв свій дохід за один рік, і 60% підприємств перейшли від локальної EPP до керованих служб безпеки Endpoint [3].

Ця технологія виявлення та реагування на кінцеві точки користовує статичний ШІ, що позбавить від необхідності повторюваних сканувань. Ця технологія замінила користання традиційного підпису. Кожна послуга EDR працює по-різному і матиме різні можливості.

Метою служб EDR є здійснення постійного моніторингу та аналізу для виявлення, виявлення та попередження передових загроз. Захист EDR - це інструмент, який використовується для виявлення та розслідування підозрілої діяльності в кінцевих точках. Ця нова технологія може виявляти та реагувати на передові загрози.

Рис. 1.5. Квадрант Gartner [4]

Порівняння рішень EDR

Microsoft (лідер)

Партнерство з Microsoft було логічним вибором для команди в Datashield. Сумісність наборів інструментів, які використовється щодня, а саме Microsoft Defender для кінцевої точки та Azure Sentinel. Хмарна основа є ключовим моментом, і можливість використовувати озеро даних Azure має очевидні переваги.

Crowdstrike (лідер)

Crowdstrike продовжує робити величезний фурор на ринку. Цікаво відзначити недавнє оголошення Crowdstrike та іншого партнера Datashield Google Chronicle про інтеграцію платформи захисту кінцевих точок Falcon в аналітичну платформу безпеки Google Cloud Chronicle, платформу збору зловмисного програмного забезпечення VirusTotal Enterprise і платформу управління ризиками Security Command Center (SCC).

SentinelOne (лідер)

SentinelOne є єдиним постачальником, який забезпечує 100% видимість із нульовим значенням пропущених виявлення у всіх протестованих операційних системах.

SentinelOne забезпечив найякісніші аналітичні виявлення, щоб забезпечити автоматизований і миттєвий контекст.

VMware Carbon Black (Visionary)

Mware Carbon Black Cloud — це рішення, що надається за моделлю «ПЗ як послуга» (SaaS), яке забезпечує антивірусний захист нового покоління (NGAV), виявлення кінцевих точок та реагування (EDR), розширений пошук загроз та управління вразливістю в єдиній консолі за допомогою одного датчика [7].

Bitdefender

Bitdefender - нішевий гравець ринку, в 2021 році компанія представлена Magic Quadrant. Вона розробила платформу GravityZone, основні функції платформи - виявлення та реагування на кінцеві точки (EDR) та мережевий аналіз у вигляді хмарного чи локального рішення. Bitdefender також пропонує послугу керованого виявлення та реагування (MDR). В Bitdefender працює численна команда розробників, яка займається дослідженням загроз і є постійним лідером у тестах захисту від файлових та безфайлових шкідливих програм.

Check Point

Check Point – нішевий представник у Magic Quadrant. На початку 2021 року Checkpoint провела ребрендинг рішення It's SandBlast Agent під брендом Harmony. Harmony забезпечує автоматизоване усунення виявлених загроз та можливості захисту, включаючи машинне навчання, поведінковий аналіз та автоматизований

аналіз. Нещодавня розробка покращила інтеграцію з брандмауером Check Point, об'єднавши моніторинг та пошук загроз у кількох продуктах. Check Point є у всіх регіонах, а її продукти підходять для всіх типів організацій, які є існуючими клієнтами Check Point.

Fortinet

Fortinet – також нішевий учасник у цьому магічному квадранті. Fortinet є постачальником платформ для забезпечення безпеки міжмережевих екранів, захисту електронної пошти, пісочниць та програмного забезпечення для захисту кінцевих точок тощо. Придбання в 2019 році enSilo забезпечило таку необхідну можливість EDR з телеметрією для розширення можливостей XDR. Інвестиції у 2019/2020 роках були спрямовані на вдосконалення придбаної системи EDR enSilo, інтеграцію у Fortinet Security Fabric та впровадження FortiXDR. Удосконалення FortiEDR включають скорочення поверхні атаки, сканування вразливостей та інструменти виявлення програм/підприємств Інтернету речей (IoT). Компанія Fortinet представлена у всьому світі, її продукти добре підходять для організацій типу B та типу C, які шукають інтегровану платформу безпеки XDR. Клієнти, які використовують кілька продуктів Fortinet, отримують єдину консоль для моніторингу та керування різними пристроями Fortinet. FortiClient легко інтегрується у цю екосистему.

ESET

ESET є претендентом у Magic Quadrant. Колекція продуктів ESET включає системи захисту кінцевих точок (EPP), Enterprise Inspector (EDR), Dynamic Threat Defense (пісочниця), Threat Intelligence та керовані послуги. Флагманський продукт ESET, ESET PROTECT Enterprise, був доповнений функціями управління хмарою, захисту браузера від несанкціонованого доступу, сканування Windows Management Instrumentation (WMI) та управління шифруванням Apple FileVault 2. ESET сподобається в основному невеликим організаціям типу B та типу C, які шукають надійне EPP та EDR з легким агентом, яким можна керувати з локальних серверів. ESET містить надійний механізм захисту від шкідливого програмного забезпечення, який показує стабільно високі результати тестування ефективності

шкідливого програмного забезпечення. Компанія була одним із перших розробників методів машинного навчання.

Symantec

Компанія Symantec належить до категорії Visionary у Magic Quadrant. Позиція Symantec відображає її стратегію виходу на ринок, тисячі її клієнтів змушені були шукати підтримку або альтернативи. Сфокусувавшись на найбільших клієнтах, Symantec досягла певного успіху, пропонуючи великим підприємствам ширший набір продуктів. В обслуговуванні клієнтів малого та середнього бізнесу (SMB) компанія спирається на глобальну мережу партнерів. Флагманські рішення Symantec, Symantec Endpoint Security Enterprise (SESE) та Symantec Endpoint Security Complete (SESC) надають керовані з хмари EPP та EDR. Багато рішень Symantec мають спільну хмарну консоль.

F-Secure

F-Secure – ще один нішевий представник Магічного квадранта. F-Secure має досвід надання захисту кінцевих точок за допомогою експертних керованих послуг, додавши EDR та послугу Countercept MDR у 2018 році та впровадивши пошук загроз у 1 кварталі 20 року. Основним ринком F-Secure є регіон EMEA, компанія представлена у решті регіонів світу. Клієнтами F-Secure зазвичай є середні та малі підприємства типів B та C, а клієнтами Countercept MDR service та Consulting – великі підприємства. Компанія F-Secure внесла додаткові покращення на захист Linux, використання ресурсів агентами та варіанти розгортання у своєму хмарному рішенні. Агенти для Windows і Mac тепер мають додаткові можливості реагування, включаючи автоматизацію, ширші можливості виявлення для Mac та Linux, а також покращене управління оновленнями. Захист серверів також був посилений, забезпечуючи контроль додатків, захист від несанкціонованого доступу та здирництва в комплексі DataGuard, а також гнучкі щомісячні підписки на основі використання[8].

Cisco

Cisco AMP пропонує безкоштовну пробну версію. Відповідно до онлайн-оглядів, його ціна залежить від планів підписки. Ціна визначатиметься залежно від кількості кінцевих точок та кількості років, на які підписалися.

Cisco AMP (розширений захист від зловмисного програмного забезпечення) надає послуги захисту кінцевих точок. У ньому використовуються різноманітні антивірусні технології для сканування файлів. Він забезпечує антивірусний механізм Cisco. Він буде постійно контролювати кожен файл у мережі.

Чотири основні можливості Cisco AMP включають наступне:

Розвідка про загрози: Talos (Cisco Security Analyst Engineers) аналізує мільйони загроз і терабайти даних на день і передає ці дані до AMP для кінцевих точок, щоб користувачі були захищені 24/7. Хороша розвідка загроз дає змогу зміцнити оборону на передовій.

«Пісочниця»: розширені можливості «пісочниці» на основі механізму Threat Grid дозволяють виконувати автоматичний статичний та динамічний аналіз файлів на основі більше 550 поведінкових індикаторів, щоб виявляти приховані загрози.

Виявлення та блокування зловмисного програмного забезпечення на певний момент. Використовуючи індивідуальне співставлення сигнатур, машинне навчання та нечіткі відбитки пальців, AMP аналізує файли в точці входу, щоб ловити та блокувати відомі та невідомі шкідливі програми в режимі реального часу.

Постійний аналіз, ретроспективна безпека та виправлення: як тільки файл потрапляє у мережу, AMP продовжує переглядати, аналізувати та записувати його активність, незалежно від розташування файлу. Якщо пізніше буде виявлено шкідливу поведінку, AMP надсилає команді безпеки сповіщення, яке містить повну записану історію загрози: звідки прийшло зловмисне програмне забезпечення, де воно було та що воно робить. Потім AMP надає контроль, щоб утримувати та виправляти його за допомогою кількох кліків. [5].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КІНЦЕВИХ ТОЧОК НА БАЗІ CISCO AMP FOR ENDPOINT

2.1. Аналіз функцій та можливостей для забезпечення безпеки кінцевих точок на базі Cisco AMP for Endpoint

Кібератаки вражають бізнес щодня. Програми-вимагачі є особливо проблематичними, оскільки кількість успішних атак програм-вимагачів зростає з року в рік. Очевидно, що організації повинні захищатися від програм-вимагачів, якщо вони хочуть уникнути великих збитків. Cisco Secure Endpoint захищає від кібератак за допомогою хмарного рішення з одним агентом. Це єдине рішення безпеки кінцевої точки, яке має вбудовану платформу розширеного виявлення та реагування (XDR), що дозволяє бачити більше загроз, блокувати більше атак і швидше усувати.

Радикальне спрощення безпеки компанії починається з уніфікації стека безпеки, зменшення навантаження з агентів і досягнення розширеного виявлення та реагування (XDR), Secure Access Service Edge (SASE) і результатів з нульовою довірою шляхом консолідації безпеки кінцевих точок, хмарної безпеки та агентів віддаленого доступу. У Cisco є вдосконалений єдиний агент, яким можна легко керувати в хмарі за допомогою вбудованої платформи SecureX.

Максимізація операцій безпеки компанії включає два ключових інгредієнта: фокус і швидкість. Рішення Cisco допомагає зосередитися на найважливіших вразливостях за допомогою інтегрованого управління вразливими місцями на основі ризиків від Kenna Security, щоб швидко прогнозувати, розставляти пріоритети та керувати усуненням вразливостей.

Досягти повного контролю в безпеці кінцевих точок може бути важко, але це не неможливо. Cisco допомагаємо отримати необхідну впевненість у безпеці, пропонуючи можливості виявлення вразливостей кінцевих точок і реагування на інциденти, якими повністю керує команда відданих фахівців Cisco, які зосереджені

на скороченні часу, одночасно зміцнюючи позицію безпеки за допомогою постійних операцій безпеки.

Інші ключові функції включають:

Виявлення загроз від хмари до кінцевої точки за допомогою Secure Device Insights і Secure Cloud Insights, які надають розширене уявлення про локальні та хмарні активи.

Спрощений пошук загроз і розслідування безпеки за допомогою розширеної можливості розширеного пошуку та запитів у реальному часі, щоб швидко та впевнено знаходити загрози на кінцевих точках у середовищах Windows, Mac і Linux.

Прискорене реагування на загрози та усунення загроз шляхом автоматичного просування та визначення пріоритету інцидентів із Secure Endpoint до SecureX.

Зменшення рівень атак за допомогою надійного поведінкового захисту, який відображає виявлені вразливості на найновішій платформі MITER ATT&CK, одночасно покращуючи здатність зупиняти безфайлові атаки зловмисного програмного забезпечення до того, як будь-які або подальші інциденти вплинуть на кінцеві точки.

Програми-вимагачі продовжують завдавати хаосу, зачіпаючи окремих осіб, підприємства та уряди, шифруючи їхні файли та тримаючи їх у «заручниках», доки не буде сплачено викуп за ключ дешифрування. Оскільки учасники програм-викупів успішно ставлять своїх жертв у становище, коли сплата викупу є найпростішим способом відновити доступ до своїх файлів, цій тенденції атак не видно кінця.

Тим часом, інший прихований тип загроз – безфайлові атаки зловмисного програмного забезпечення – за останні пару років зазнав експоненційного зростання, а його поширеність зросла на 900% лише у 2020 році. Спочатку ця цифра може здатися сюрреалістичною, тобто поки розглянути, наскільки ефективним може бути безфайлове шкідливе програмне забезпечення, коли справа доходить до надання кіберзлочинцям легкого способу заразити середовище, не залишаючи сліду. Цей тип зловмисного програмного забезпечення уникає виявлення,

виконуючи його в пам’яті. Безфайлове зловмисне програмне забезпечення не має сигнатур, тому його особливо важко запобігти.

Оскільки з’являються програми-вимагачі, безфайлові зловмисні програми та низка нових загроз, організації вдаються до розгортання безлічі засобів контролю безпеки, що призводить до складності та неефективності на цьому шляху. Сьогодні середній центр операційної безпеки підприємства (SecOps) використовує 45 різних інструментів безпеки від 13 різних постачальників, одночасно борючись із постійною нестачею кадрів у сфері кібербезпеки, та іншими проблемами SecOps. Не дивно, що галузь вимагає простоти, консолідації, а в деяких випадках і повністю керованого варіанту безпеки.

Захист кінцевих точок від будь-якої загрози є головним пріоритетом для організацій. Важливе значення має комплексне хмарне рішення з одним агентом, яке забезпечує найвищий рівень безпеки та здатність зменшувати складність за допомогою простого уніфікованого захисту.

Підхід Cisco до безпеки кінцевих точок

Коли справа доходить до захисту ваших кінцевих точок, потрібно зосереджуватись на тому, щоб ефективно зупиняти загрози, водночас прискорюючи та максимізуючи операції безпеки. Cisco надає можливості, які потрібні, щоб побачити більше загроз, блокувати більше атак і виправляти їх швидше і повніше, допомагаючи максимально підвищити рівень безпеки.

Постійна увага до спрощення кібербезпеки дозволяє клієнтам підвищити ефективність своїх операцій безпеки за допомогою хмарного підходу з одним агентом, яким легко керувати за допомогою вбудованої платформи SecureX.

Видимість більшості загроз може стати ключем до того, щоб стати «переможцем, а не жертвою» порушення. Рішення Cisco допомагаємо шукати приховані загрози, виявляючи та досліджуючи перші ознаки програм-вимагачів та інших передових атак на 95% швидше за допомогою найширшої інформації про загрози від Talos і досвіду фахівців Cisco. Знайти наявні та нові загрози стало легше завдяки цілодобовим моніторингом, виявленням та реагуванням від команди з

понад 2200 експертів Центру операцій безпеки (SOC), включаючи дослідників загроз, дослідників та спеціалістів із реагування на інциденти.

Блокування нових атак убереже від компрометації чутливих даних. Це досягається завдяки вчасному реагуванню на загрози, зменшуючи поверхню атаки за допомогою багатогранних методів запобігання, оцінки положення та управління вразливістю на основі ризиків.

Останнім ключовим компонентом є реагування на інциденти швидше і більш обширно. За допомогою Cisco for Endpoints можна досягти скорочення часу реагування на інциденти на цілих 97% завдяки вдосконаленим EDR і вбудованим XDR з платформи SecureX. Рішення безпеки кінцевих точок просте, але воно дає необхідну гнучкість, щоб зробити це самостійно, з партнером або повністю керованим Cisco. Останній варіант дає доступ до спеціалістів Cisco, які зосереджені на тому, щоб різко скоротити середній час на виявлення загроз і реагування на них за допомогою поглибленої телеметрії, визначених сценаріїв та інтегрованої архітектури безпеки для швидкого дослідження та усунення загроз.

2.2. Архітектура та компоненти Cisco AMP for Endpoint

Cisco Secure Endpoint (раніше AMP for Endpoints) об’єднує можливості запобігання, виявлення, пошуку загроз та реагування в єдине рішення, використовуючи потужність хмарної аналітики. Secure Endpoint захистить пристрої Windows, Mac, Linux, Android та iOS за допомогою загальнодоступного або приватного хмарного розгортання.

Переваги

У світі шкідливих програм, що швидко розвивається, виявити загрози стає все важче. Найпоширеніший 1% із цих загроз, які в кінцевому підсумку ввійдуть у мережу та спричинять хаос у мережі, потенційно можуть залишитися непоміченими. Однак Secure Endpoint забезпечує комплексний захист від цього 1%. Це програмне забезпечення безпеки запобігає зловживанням, блокує зловмисне програмне забезпечення на місці входу, а також безперервно відстежує й аналізує

активність файлів і процесів, щоб швидко виявляти, стримувати та усувати загрози, які можуть уникнути оборони на передовій.

Профілактика

Припинення загроз на найранішому етапі гарантує мінімальну шкоду кінцевим точкам і менше часу простою після порушення. Secure Endpoint використовує надійний набір профілактичних технологій, щоб зупинити зловмисне програмне забезпечення в режимі реального часу, захищаючи кінцеві точки від найпоширеніших атак сьогодення.

Репутація файлу: Secure Endpoint містить повну базу даних кожного файлу, який коли-небудь бачили, і відповідну хорошу чи погану позицію. У результаті відоме шкідливе програмне забезпечення швидко та легко поміщається на карантин на місці входу без будь-якого сканування, що вимагає інтенсивного використання процесора.

Антивірус: Secure Endpoint містить постійно оновлювані антивірусні системи на основі сигнатур для кінцевих точок Windows, Mac або Linux. Усі кінцеві точки мають переваги завдяки виявленню загроз на основі сигнатурного методу аналізу, що дозволяє адміністраторам надавати надійні можливості контролю та застосовувати чорні списки. База даних антивірусних сигнатур знаходиться локально на кожній кінцевій точці, тобто вона не покладається на підключення до хмари для роботи. Це гарантує, що кінцеві точки захищені як в режимі онлайн, так і в автономному режимі.

Виявлення поліморфного зловмисного програмного забезпечення. Зловмисники часто пишуть різні варіанти одного і того ж зловмисного програмного забезпечення, щоб уникнути поширених методів виявлення. Secure Endpoint може виявити ці варіанти або поліморфне зловмисне програмне забезпечення за допомогою зіставлення даних. Ця функція шукає схожість між вмістом підозрілого файлу та вмістом відомих сімейств шкідливих програм і поміщає в карантин, якщо є значне збіг.

Аналіз машинного навчання: Secure Endpoint навчається за допомогою алгоритмів, щоб «навчитися» ідентифікувати шкідливі файли та дії на основі

атрибутів відомих шкідливих програм. Можливості машинного навчання в Secure Endpoint забезпечуються повним набором даних Cisco Talos, щоб забезпечити кращу та точнішу модель. Разом машинне навчання в Secure Endpoint може допомогти виявити ніколи раніше не бачене зловмисне програмне забезпечення на місці входу.

Запобігання експлойту: атаки можуть проникати в кінцеві точки, а зловмисне програмне забезпечення ухиляється від захисту безпеки, використовуючи вразливості програм і процесів операційної системи. Функція запобігання експлойту захищатиме кінцеві точки від атак з використанням пам'яті, заснованих на експлойті.

Захист сценаріїв: Secure Endpoint забезпечує покращену видимість у сценаріїв, що виконуються на ваших кінцевих точках, і допомагає захистити від атак на основі сценаріїв, які зазвичай використовуються зловмисними програмами. Керування сценаріями забезпечує додатковий захист, дозволяючи механізму запобігання експлойту запобігати завантаженню певних DLL деякими часто використовуваними настільними програмами та їхніми дочірніми процесами.

Захист поведінки: розширений поведінковий аналіз Secure Endpoint постійно відстежує всю активність користувачів і кінцевих точок, щоб захистити від зловмисної поведінки в режимі реального часу, зіставляючи потік записів активності з набором моделей атаки, які динамічно оновлюються в міру розвитку загроз. Наприклад, це забезпечує детальний контроль та захист від зловмисного використання інструментів.

Виявлення

Хоча методи запобігання шкідливому програмному забезпеченню необхідні для повного рішення безпеки кінцевих точок наступного покоління, боротьба з розширеними загрозами вимагає додаткових заходів. Secure Endpoint постійно контролює кінцеві точки, щоб допомогти виявити нові та невідомі загрози.

Захист від шкідливої діяльності: Secure Endpoint постійно відстежує всю активність кінцевої точки та забезпечує виявлення під час виконання та блокування ненормальної поведінки запущеної програми на кінцевій точці. Наприклад, коли

поведінка кінцевої точки вказує на програмне забезпечення-вимагач, процеси, що порушують, припиняються, запобігаючи шифрування кінцевої точки та зупиняючи атаку.

Хмарні індикатори компромісу: провідна в галузі організація Cisco з розвідки загроз, Talos, постійно аналізує зловмисне програмне забезпечення, щоб виявити нові типи загроз і створити поведінкові та криміналістичні профілі для нових загроз, інакше відомих як індикатори компромісу (IoCs). Чутливі дані, такі як розташування файлів або зміни значень розділів реєстру, — це всі дані, які Secure Endpoint може використовувати, щоб допомогти адміністраторам ідентифікувати системи, які були зламані.

IoCs на базі хоста: адміністратори можуть створювати власні індивідуальні IoCs для використання в реагуванні на інциденти для сканування посткомпромісних індикаторів у кінцевої точки. Спеціальні IoCs написані у відкритому стандартному форматі (OpenIOC), що дозволяє легко використовувати дані з будь-яких існуючих розвідувальних каналів.

Уразливості: Secure Endpoint визначає вразливе програмне забезпечення у середовищі, щоб зменшити поверхню атаки. Кінцеві точки, на яких запущено вразливе програмне забезпечення, перераховані, і їм надається пріоритет на основі галузевої оцінки CVE (Загальні вразливості та ризики): чим серйозніша вразливість, тим більш помітною вона буде у списку. Це надає адміністраторам список усіх хостів, які потрібно виправити, щоб запобігти майбутнім експлойтам.

Низька поширеність: Secure Endpoint автоматично визначить виконувані файли, які існують у невеликій кількості на кінцевих точках, і проаналізує ці зразки в хмарній пісочниці, щоб виявити нові загрози. Цільове зловмисне програмне забезпечення або розширені постійні загрози часто залишаються поза радаром і починаються лише на кількох кінцевих точках, але з низькою поширеністю Secure Endpoint автоматично шукатиме загрози, щоб допомогти легко виявити 1% загроз, які інакше залишилися б непоміченими.

2.3. Аналіз додаткових можливостей Cisco AMP for Endpoint

Полювання на загрози

SecureX Threat Hunting — це проактивний підхід, орієнтований на аналітику, для виявлення прихованих розширених загроз. Ця можливість пропонується виключно як частина нового рівня ліцензії Premier у Secure Endpoint. Ця функція показує особам, які реагують на інцидент, як була помічена атака або як вона розвивалася, і що робити далі з точки зору реакції. Мета полягає в тому, щоб виявити та зупинити атаки, перш ніж вони завдадуть будь-якої шкоди. Як побічний ефект від регулярного та постійного пошуку загроз, організація розширює свої знання про вразливості та ризики, що ще більше дозволяє посилити середовище безпеки.

SecureX Threat Hunting використовує досвід Talos і групи досліджень та ефективності Cisco, щоб допомогти визначити загрози, виявлені в середовищі клієнта. Cisco надає високоавтоматизовані пошуки, керовані людьми, на основі підручників, які створюють високоточні оповіщення. Цей процес унікально поєднує технологію Orbital Advanced Search з досвідом від елітних мисливців за загрозами з 20-річним досвідом роботи в галузі, щоб завчасно знаходити більш складні загрози.

Відповідь

Оскільки кількість та різноманітність розширених загроз, призначених для того, щоб уникнути запобіжних заходів, збільшуються, можливість порушення слід розглядати як можливий випадок. З таким мисленням слід розгорнути потужний набір інструментів, який допоможе легко ідентифікувати заражені кінцеві точки та зрозуміти масштаб атаки. На додаток до різноманітних можливостей запобігання та виявлення, Secure Endpoint пропонує детальну видимість кінцевої точки та інструменти реагування для швидкої та ефективної обробки порушень безпеки.

Інформаційні панелі та папка вхідних: звіти не обмежуються перерахуванням та агрегацією подій. Практичні інформаційні панелі, вбудовані в Secure Endpoint, забезпечують спрощене керування та швидшу відповідь. Події та

кінцеві точки класифікуються за пріоритетом і пов’язані з робочими процесами для відстеження прогресу під час розслідування.

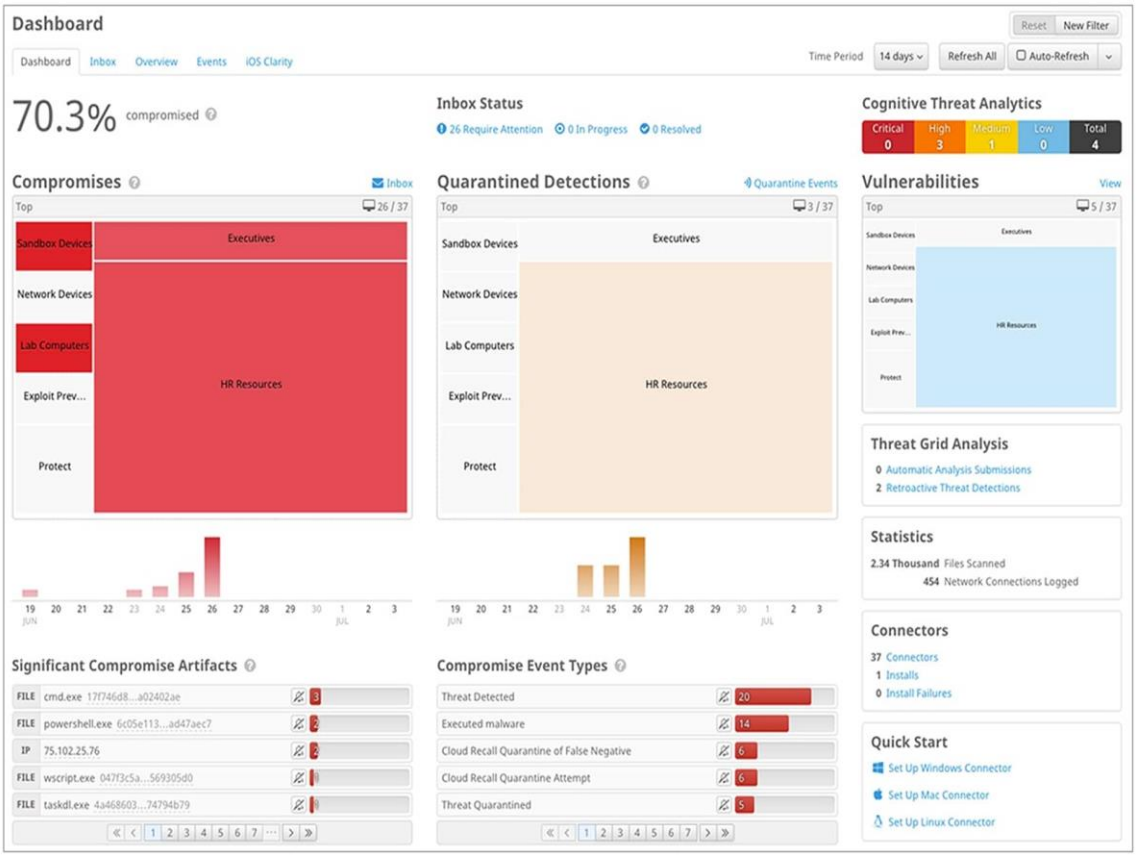

Рис. 2.1. Інформаційна панель безпечної кінцевої точки

Криміналістична експертиза кінцевої точки: потужні інструменти, такі як траєкторія файлів і траєкторія пристрою, використовують можливості безперервного аналізу Secure Endpoint, щоб показати повний обсяг загрози. Secure Endpoint ідентифікує всі уражені програми, процеси та системи, щоб визначити нульового пацієнта, а також метод і точку входу. Ці можливості допомагають швидко зрозуміти масштаб проблеми, визначаючи шлюзи зловмисного програмного забезпечення та шлях, який зловмисники використовують, щоб закріпитися в інших системах.

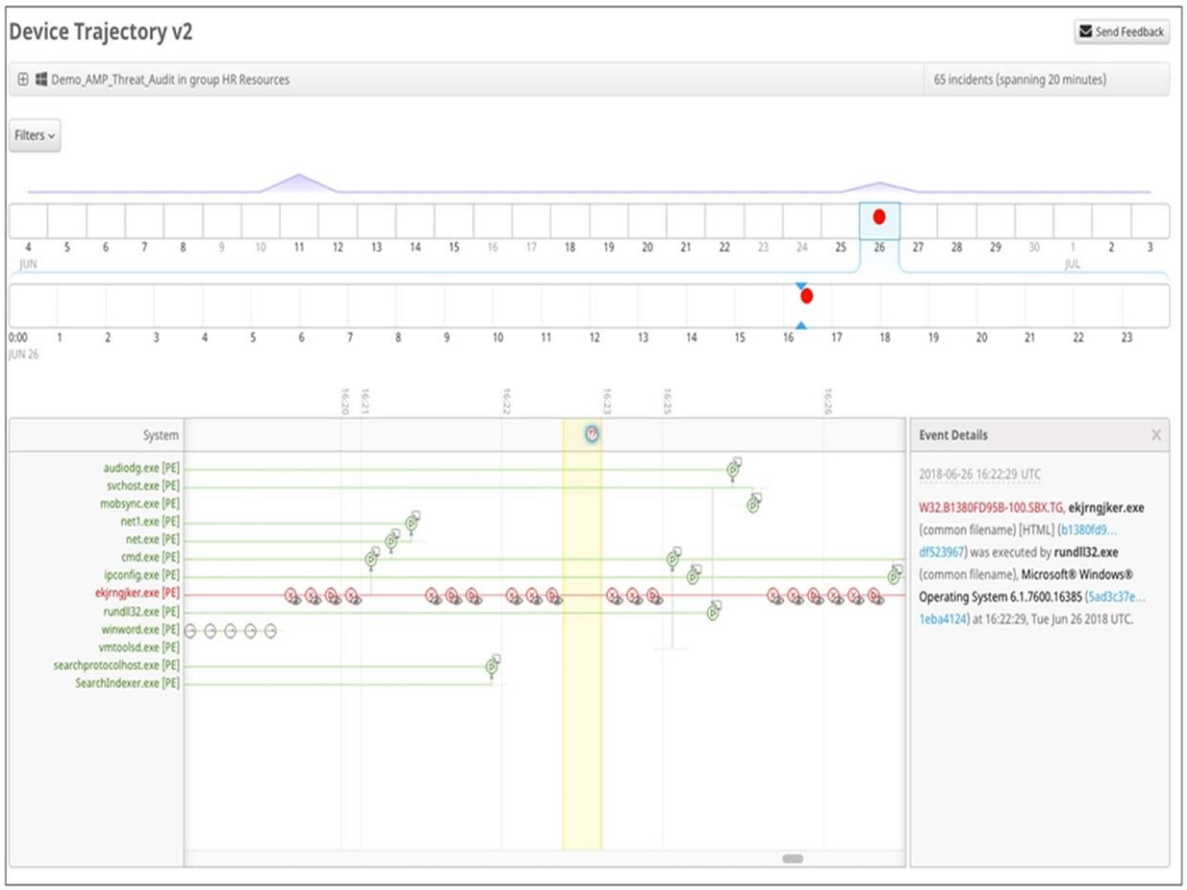

Рис. 2.2. Захищена траєкторія пристрою кінцевої точки

Динамічний аналіз: Secure Endpoint містить вбудоване високобезпечне середовище пісочниці, що працює на основі Cisco Threat Grid, для аналізу поведінки підозрілих файлів. Аналіз файлів дає детальну інформацію про файли, включаючи серйозність поведінки, оригінальне ім'я файлу, знімки екрана запуску шкідливого програмного забезпечення та зразки захоплення пакетів. Озброївшись цією інформацією, можна краще зрозуміти, що необхідно для стримування спалаху та блокування майбутніх атак.

Ретроспективна безпека: Secure Endpoint використовує запатентовану технологію, яка автоматично виявляє розширені загрози, які потрапили у середовище. Завдяки безперервному моніторингу Secure Endpoint співвідносить нову інформацію про загрози з минулою історією та автоматично поміщає файли на карантин, як тільки вони починають проявляти шкідливу поведінку. Ця автоматична реакція на останні загрози забезпечує швидший час для виявлення та значно зменшує поширення шкідливого програмного забезпечення.

Видимість командного рядка: отримання видимості аргументів командного рядка допомагає визначити, чи використовуються законні програми, включаючи утиліти Windows, у зловмисних цілях. Secure Endpoint може виявити поведінку, яку важко виявити, наприклад використання vssadmin для видалення тіньових копій або вимкнення безпечного завантаження; Експлойти на основі PowerShell; посилення привілеїв; модифікації списків контролю доступу; і спроби перерахувати системи.

Ізоляція кінцевих точок: дуже важливо ізолювати кінцеві точки, які були скомпрометовані, щоб зупинити поширення загроз і запобігти їх комунікації з їх C&C, водночас дозволяючи обмін інформацією з надійними ресурсами, такими як хмара Secure Endpoint. Ізоляція кінцевої точки дозволяє одним клацанням миші ізолювати інфіковану кінцеву точку разом із можливістю внесення в білий список надійних мережевих ресурсів. Кінцеву точку можна деізолювати одним клацанням миші адміністратором або за допомогою коду розблокування користувачем.

Розширений пошук: розширений пошук — це розширена функція в Cisco Secure Endpoint, розроблена для того, щоб спростити розслідування безпеки та пошук загроз, надаючи понад сотню попередньо підготовлених запитів, що дозволяє швидко виконувати складні запити на будь-якій або всіх кінцевих точках. Це дає змогу отримати більш глибоке уявлення про те, що сталося з будь-якою кінцевою точкою в будь-який момент часу, зробивши знімок її поточного стану. Незалежно від того, чи проводиться розслідування в рамках реагування на інциденти, пошуку загроз, операцій IT чи вразливості та відповідності, розширений пошук швидко надасть потрібні відповіді щодо кінцевих точок.

3 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ТА ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ CISCO SECURE ENDPOINT

Розглянемо основні способи захисту від шкідливого програмного забезпечення з рішенням Cisco AMP for Endpoints [14].

3.1. Основні технології захисту кінцевих точок Cisco Secure Endpoint

Програми-вимагачі проникають в організації кількома способами і стають особливо проблематичними, оскільки кількість атак зростає з року в рік. Cisco захищає проти програм-вимагачів із інтегрованим платформним підходом у широкому спектрі захисту критичних кінцевих точок, підкріплені найкращою в своєму класі розвідкою про загрози та дослідженнями від Talos. Захист від програм-вимагачів вимагає швидкого запобігання і найкраще працює, коли є орієнтований на розвідку для боротьби з загрозами на багатьох фронтах.

Захист від експлойтів

Атаки на пам'ять проникають через кінцеві точки, а зловмисне програмне забезпечення ухиляється від захисту безпеки, використовуючи вразливості в програми та процеси операційної системи. Більшість цих атак здійснюються в пам'яті програми і залишаються недоторканими для більшості рішень безпеки, як тільки вони отримають доступ до пам'яті. AMP for Endpoints Exploit Prevention забезпечує цілісний превентивний рівень безпеки для захисту кінцевих точок, серверів і віртуальних середовищ від атак без файлів і атак з ін’єкції пам’яті, а також захищеного зловмисного програмного забезпечення. Це рішення робить це, змінюючи статичний характер оборонного ландшафту на динамічний і ускладнює зловмисникам планувати та виконувати успішні атаки.

Можливості захисту Cisco AMP for Endpoints включають кілька технологій, які працюють разом, щоб запобігти, виявляти та виправляти шкідливий код на кінцевій точці. Основні технології запобігання в пам'яті включають:

● Exploit Prevention захищає кінцеві точки від атак на пам'ять, які зазвичай використовуються прихованим зловмисним програмним забезпеченням і використовує, орієнтуючись на вразливості програмного забезпечення захищених процесів.

● System Process Protection захищає важливі системні процеси Windows від маніпуляцій або скомпрометовані через атаки ін'єкції пам'яті іншими небезпечними процесами.

Основні технології виявлення на диску включають:

● AMP Cloud блокує зловмисне програмне забезпечення за допомогою глобального аналізу загроз, який постійно доповнюється новими знання про загрози з досліджень Cisco Talos, Cisco Threat Grid і Cognitive Intelligence.

● TETRA – це традиційний антивірусний механізм на основі сигнатур, розташований на кінцевій точці та надає на диску можливості виявлення шкідливих програм; TETRA є частиною AMP Connector для Windows.

● Захист від зловмисної активності (MAP) пропонує виявлення під час виконання та блокування ненормальної поведінки пов’язаної із запущеним файлом або процесом (наприклад, поведінка, пов’язана з програмним забезпеченням-вимагачем).

● Спеціальні виявлення надають надійних можливостей контролю аналітикам безпеки, також надання можливості визначати власні підписи та застосовувати чорні списки за допомогою стандартних форматів.

Основні технології постінфекційного виявлення включають:

● Кореляція потоків пристрою перевіряє вхідні та вихідні мережеві комунікації процесу/файлу на кінцевій точці та дозволяє застосувати обмежувальні дії відповідно до політики.

● Хмарні індикатори компромісу допомагають виявити підозрілу активність, що спостерігається на кінцевих точках розпізнавання образів; відповідні сповіщення служать тригером для більш глибоких розслідувань і реагування.

● IOC кінцевих точок — це потужна функція пошуку загроз для сканування посткомпромісних індикаторів у кількох кінцевих точок і можуть бути імпортовані з користувацьких відкритих файлів на основі IOC.

Когнітивний інтелект ще більше підвищує ефективність AMP для кінцевих точок завдяки зусиллям групи машинного навчання Cisco. Завдяки цьому продукт збагачується файлами і агентами, що дають можливість виявлення на основі аналізу телеметрії мережі (веб-журнали, NetFlow). Результатом такого аналізу є знання про загрози на основі контексту, пристосовані до певної організації. Когнітивний інтелект також дозволяє корелювати поведінку загроз і активність у кількох контрольованих наборах даних (мережа, кінцева точка, модель зловмисника), таким чином забезпечуючи підвищеного рівня ефективності безпеки (міжрівневий аналіз). Крім того, інші спеціальні моделі працюють, вбудовані в продукти AMP і Threat Grid, щоб забезпечити можливість статичного аналізу файлів на основі ML.

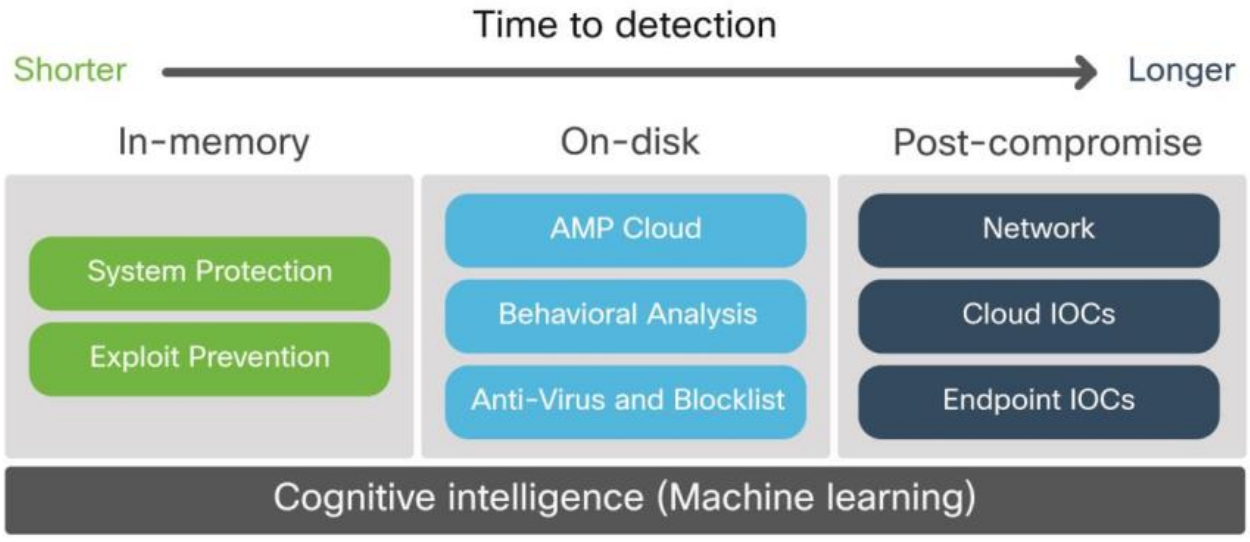

Рис. 3.1. Когнітивний інтелект

Ці можливості безпеки є основою загального підходу до розширеного захисту від шкідливих програм. Хоча Cisco рекомендує використовувати всі ці механізми в поєднанні один з одним, щоб використовувати повні можливості продукту, також клієнти можуть вибрати, увімкнути чи вимкнути ту чи іншу функцію за допомогою політики.

Технологія запобігання експлойту

Exploit Prevention захищає від зловмисного програмного забезпечення та експлойтів, спрямованих на запуск невиправлених вразливостей або вразливостей нульового дня. Дане рішення використовує глибоке розуміння того, як працює процес Windows, і слідує його різні механізми. У поточній версії (AMP Connector версії 6.2.1 і новішої для Windows) Exploit Prevention захищає набір попередньо налаштованих 32-розрядних і 64-розрядних програм. Дослідницька та інженерна команда постійно шукає шляхи підвищення очікуваного рівня захисту та надає підтримку для розширеного списку процесів. Exploit Prevention — це система профілактичної безпеки, яка надає широкі можливості захист від різних типів загроз. Це робиться за допомогою маніпуляцій із пам’яттю захищеного процесу як описано нижче.

Розглянемо, як працює функція запобігання експлойту поділивши на три прості кроки.

Крок 1: Щоразу, коли користувач відкриває захищену програму, завантажувач Windows завантажує в пам'ять усі необхідні ресурси щоб запустити цю програму. Exploit Prevention додає крихітну DLL (бібліотеку динамічних посилань) до завантажувача Windows, який проактивно змінює структуру процесу. Іншими словами, розташування бібліотек, змінних, функцій та інших даних елементи змінюються узгоджено. Exploit Prevention перевіряє всі розташування ресурсів у пам'ять. У більшості випадків скремблювання виконується в односторонній рандомізації без ключа. Це означає, що немає спосіб зворотної інженерії розташування ресурсів у новій зашифрованій пам'яті, яка створює пам'ять непередбачуваний для зловмисників.

Крок 2: Після створення нової структури пам'яті наступним кроком є інформування про законний код програми та нові місця розташування необхідних ресурсів. Програма продовжує працювати в звичайному режимі і працює без будь-яких проблем без зміни своєї поведінки. У той же час Exploit Prevention створює приманку з оригінальної структури пам’яті, яку можна використовувати як пастку для шкідливого коду. Через це DLL, додана Exploit Prevention, перестає працювати, практично не проявляє активності.

Крок 3. Коли шкідливий код націлений на оригінальну структуру пам'яті, він не знає про зміни, внесені Exploit Prevention. Код буде шукати оригінальну, передбачувану мету, для виконання якої він був розроблений, але натомість потрапить до приманки і в результаті нейтралізується. Легко виявляється доступ до пам’яті лише для читання, редагування або запису, і програма, що робить це, є шкідливим програмним забезпеченням за визначенням, і, таким чином, його негайно зупиняють і блокують. Він не може виконуватися та припиняється якомога раніше в ланцюжку знищення: до обміну командами та управлінням і до того, як корисне навантаження буде скинуто на диск.

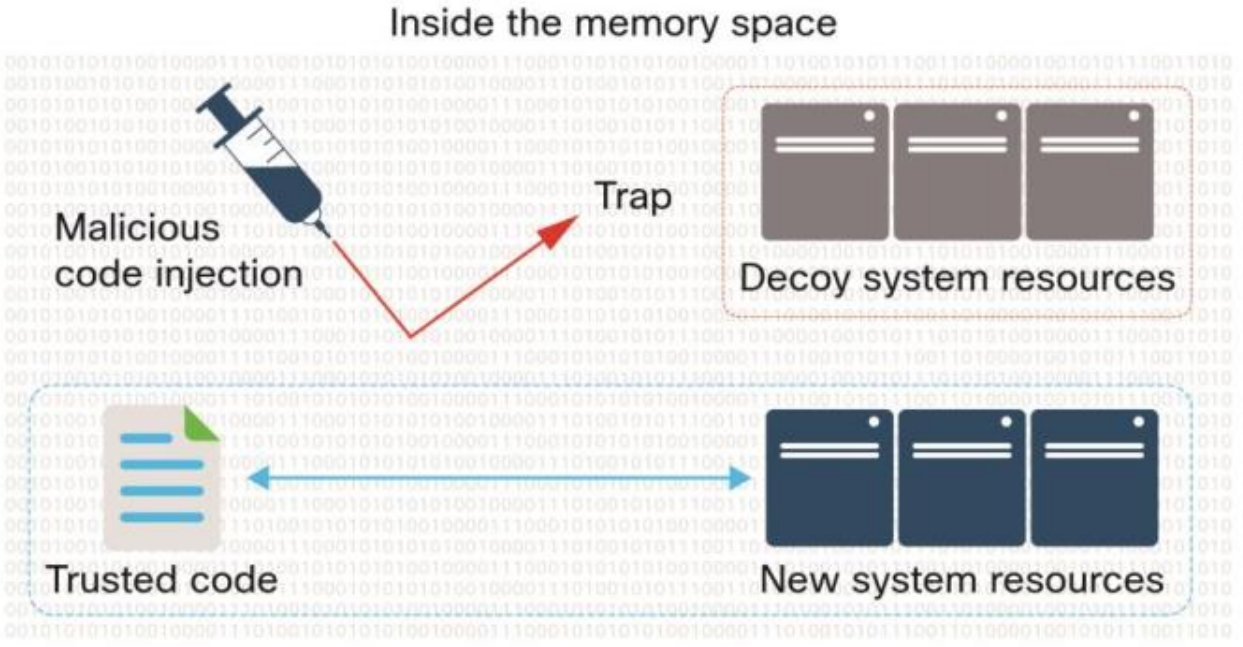

Рис. 3.2. Робота Exploit Prevention

Підводячи підсумок, Exploit Prevention пропонує справжню превентивну систему безпеки, яка не вимагає налаштування політики або попереднє знання загроз або письмових правил роботи. Як тільки процес перебуває під захистом, захист буде продовжувати до завершення процесу. Коли Exploit Prevention зупиняє атаку, він зупиняє програму яка виконується та реєструє контекстні дані разом із класифікацією подій у AMP for Endpoints Device Trajectory та перегляду подій кінцевих точок (який також можна запитувати через API AMP). Варто також зазначити, що поняття режиму аудиту відсутнє із запобіганням експлойту, на відміну від деяких інших механізмів AMP для кінцевих точок. Exploit Prevention є частиною AMP Connector для Windows.

Захищені процеси

Починаючи з AMP для Windows Connector версії 6.2.1, Exploit Prevention захищає такі 32- і 64-розрядні версії процесів. Дочірні процеси захищених програм успадковують захист.

- Програма Microsoft Excel
- Програма Microsoft Word
- Програма Microsoft PowerPoint
- Програма Microsoft Outlook
- Браузер Internet Explorer
- Браузер Mozilla Firefox
- Браузер Google Chrome
- Програма Microsoft Skype
- Програма TeamViewer
- Програма медіаплеєра VLC
- Хост сценаріїв Microsoft Windows
- Програма Microsoft Powershell
- Програма Adobe Acrobat Reader
- Сервер реєстрації Microsoft
- Microsoft Task Scheduler Engine
- Редактор формул Microsoft

План захисту також включає наступні критичні системні процеси. У цьому випадку вводиться протектор запущені процеси.

● Підсистема місцевих органів безпеки

● Провідник Windows

● Підсистема спулера

Виконання

Виконання є великою частиною критеріїв вибору безпеки кінцевої точки. AMP для кінцевих точок додає трохи впливає на продуктивність системи. Механізм запобігання експлойту не передбачає жодного зниження продуктивності чи будь-яких змін досвід кінцевого користувача. Після того, як двигун завершив скремблювання пам'яті, кількість виконань і кількість стрибків для досягнення певної DLL або виконання певної функції (наприклад) зберігається в тій же самій кількості. Єдиний вплив, який можна розглянути, це вплив на пам’ять, спричинений приманкою. Однак, оскільки уповноважений код програми не використовує ці ресурси приманки під час нормальної діяльності, вони повертаються в ядро і тому не впливають на продуктивність. Ці ресурси відсутні в робочому наборі користувача; отже, це не є реальним навантаженням для віртуальної пам'яті (якщо шкідливе програмне забезпечення блокується через доступ до приманки). Іншим можливим впливом є час завантаження програми через виконується скремлінг. Як наслідок, захищена програма може завантажуватися трохи (на 5-10%) повільніше, ніж зазвичай, але не передбачає жодних покарань під час виконання або впливу на роботу користувачів. Запобігання експлойту не впливає на продуктивність процесора.

Сумісність

Сумісність із програмним забезпеченням, встановленим на кінцевій точці, є важливим аспектом будь-якого рішення безпеки кінцевої точки. Увімкнення механізму запобігання експлойту може мати потенційні проблеми з сумісністю лише з деякими продуктами, які запобігають експлойту виконувати маніпуляції з пам’яттю над тими ж процесами. Хоча Cisco не рекомендує запускати більше одного водночас рішення захисту пам’яті, деякі обхідні шляхи можуть допомогти

співіснувати. Виключаючи несумісне процесів зі списку додатків, які захищають інші продукти для боротьби з експлуатацією, є ключем до успішного розгортання і тестування. Microsoft Enhanced Mitigation Experience Toolkit (EMET) включено в Windows 10 і новіших версіях за замовчуванням і доступний як завантажуваний додаток для Windows 7. Щоб покращити сумісність між захистом від експлойтів компонент Cisco AMP for Endpoints і Microsoft EMET, розглянемо наступне:

● Для кінцевих точок Windows 7 вимкніть правило EAF (Експорт фільтрації доступу до таблиці адрес) для процесів захисту AMP для механізму запобігання експлойту кінцевих точок.

● Для кінцевих точок Windows 10 вимкніть EAF (Експорт фільтрації доступу до таблиці адрес), IAF (Імпорт адреси Фільтрація доступу до таблиці) і правила ACG (Arbitrary Code Guard) для процесів, захищених AMP для Механізм запобігання експлойту кінцевих точок.

Порівняйте запобігання експлойту з ASLR

Рандомізація макета адресного простору (ASLR) – це техніка комп'ютерної безпеки, яка передбачає випадкове позиціонування базової адреси виконуваного файлу та положення бібліотек, купи та стеку в адресному просторі процесів. Випадкове змішування адресу пам'яті, що виконується ASLR, означає, що атака більше не знає на якій адресі потрібного коду (наприклад, функції гаджетів Returned-Oriented Programming [ROP]) насправді розташований. Таким чином, замість того, щоб усувати вразливості системи, ASLR намагається зробити її більше важко використовувати наявні вразливості.

ASLR має певні обмеження, подолати які допомагає Exploit Prevention:

● Рандомізація на основі часу завантаження: базові адреси DLL рандомізуються лише під час завантаження; що може використовуватися шляхом поєднання таких вразливостей, як розкриття пам'яті або атаки грубої сили.

● Непідтримувані виконувані файли/бібліотеки: виконуваний файл має бути створений з підтримкою ASLR; інакше немає захисту. Це обмеження здебільшого спостерігається у старіших версіях Windows (до Windows 8).

● ASLR не затримує атаку: ASLR намагається запобігти атаці досягти цільової пам'яті. Однак, як тільки шелл-код переходить на неправильну адресу під час експлойту (через рандомізацію пам’яті), поведінка програми не визначена (можливий виняток — збій).

● ASLR не попереджає у разі атаки: коли вразливість експлуатується і виходить з ладу через ASLR рандомізацію пам’яті, жодних сповіщень або індикаторів атаки не отримано.

● ASLR не надає інформацію про атаку: докази, які часто мають вирішальне значення для судово-медичної експертизи дослідження (наприклад, експлуатовані процеси, дампи пам'яті, стеки викликів) не надається з ASLR

● Зловмисники розробили ряд методів атаки для обходу ASLR, включаючи використання Ланцюги ROP в модулях без ASLR, розпилення JIT/NOP (Just-In-Time або NO-OP), розкриття пам'яті вразливості та інші методи. Підхід Exploit Prevention відрізняється від ASLR. Хоча концепції можуть звучати схожими, ASLR бракує кілька важливих елементів, щоб зробити його успішним у протидії експлойтам нульового дня та цілеспрямованим атакам.

Порівняння Exploit Prevention з EMET Microsoft EMET (Enhanced Mitigation Experience Toolkit) — це набір інструментів для Windows, який спрямований на той самий проблемний простір; однак EMET шукає лише відомі атаки за допомогою настроюваних правил.

Таблиця 3.1. Порівняння EMET та Exploit Prevention

EMET	Exploit Prevention
EMET, що використовується для виявлення експлойтів, має кілька недоліків: ● Визначено явні правила для виявлення конкретних типів атак (правило за набір атак), що означає, що	Exploit Prevention використовує зовсім інший підхід спрямована на профілактику: ● Повністю проактивна профілактика, яка не ґрунтується на правилах; немає можливості змінити

зловмисники можуть обійти EMET, якщо вони зрозуміти ці правила	розташування ресурсів у новому зашифрованому пам'ять

Продовження Табл. 3.1.

● Програми мають бути налаштовані для роботи з EMET явно ● Має проблеми з сумісністю з кількома програмами, оскільки блокуються поведінки, яких вимагають ці програми. Тому багато з правила в EMET слід вимкнути, зменшуючи захист ● Потрібен великий обсяг оперативної пам’яті; для цього потрібно перезавантажити систему застосовувати зміни, які впливають на продуктивність ● Немає криміналістичних даних щодо заблокованих атак ● Можна обійти в Windows 7, 8, 10 ● Пропонує захист лише для експлуатації	● Попередні знання про атаку не потрібні: будь-який доступ до неморфованої області вважається шкідливою ● Сумісний з більшістю рішень безпеки і не має проблеми сумісності ● Тільки без компонентів під час виконання та без зниження продуктивності під час виконання час завантаження ● Надає детальну судово-медичну інформацію через консоль AMP для кінцевих точок; можна отримати через API ● Частина рішення безпеки корпоративного рівня ● Захищає від експлуатації, після експлуатації та зловмисного програмного забезпечення

EMET можна обійти різними методами. Наприклад:

- Виконання 64-розрядного шелл-коду всередині 32-розрядних процесі
- Зняття з охорони EMET методами відчеплення
- Використання EMET .dll для обходу ASLR та підключення

Загрози, шкідливі програми та методи використання

Як невід'ємна частина AMP для кінцевих точок, Exploit Prevention реалізує механізм глибокого захисту, який спрямовані на запобігання різним векторам атаки на початкових етапах ланцюга атаки. В результаті двигун зупиняється наступні загрози, зловмисне програмне забезпечення та методи використання (коли використовуються для використання процесів у списку захисту), які часто розглядаються як складові складних кампаній загроз. Список не є вичерпним і представляє приклади, які представлені в трьох категоріях:

- Експлуатація
- Після експлуатації
- Шкідливе програмне забезпечення

Exploit Prevention вводить інший стек безпеки, набагато раніше на фазі атаки, який доповнює захисна решітка AMP для кінцевих точок. Перевага полягає в тому, що це відбувається на початку ланцюга знищення, зменшуючи залежність від нього знання інтерфейсу про атаку та налаштування правил, а також виправлення вразливостей та очищення. Cisco досі рекомендує запровадити процес для своєчасної оцінки вразливості та виправлення для забезпечення більшої безпеки постава. Метод Exploit Prevention для перепризначення модулів пам'яті в адресному просторі захищених процесів і зміна ключових структур пам'яті дозволяє Exploit Prevention успішно запобігати різноманітним сучасні та складні методи експлуатації, постексплуатації та шкідливих програм [12].

Захист поведінки

Розширений поведінковий аналіз Secure Endpoint постійно відстежує всю активність користувачів і кінцевих точок, щоб захистити від зловмисної поведінки в режимі реального часу, зіставляючи потік записів активності з набором моделей атаки, які динамічно оновлюються в міру розвитку загроз. Наприклад, це дає змогу

детально контролювати та захищати від зловмисного використання інструментів, що не були виявлені.

MITER ATT&CK: Магія захисту кінцевої точки

Розглянемо, що є ключем до початку роботи MITER ATT&CK: Behavior Prevention on Endpoint (M1040), Exploit Protection (M1050) та Execution Prevention (M1038). На швидкий погляд усі вони можуть звучати приблизно однаково. Тож давайте уточнимо їх за допомогою швидкого встановлення рівня:

Behavior Prevention on Endpoint. Гаразд, «на кінцевій точці» — це найпростіше. Це пом'якшення чітко зосереджено на активності кінцевої точки, а не, скажімо, на активності мережі. З огляду на це, «профілактика поведінки» спрямована на виявлення та припинення дивних речей, наприклад, коли системний процес починає запускати неочікуваний код. Наприклад, якщо svchost.exe виконує код у DLL, якого ніколи раніше не виконував. Є велика ймовірність, що код є шкідливим, тому перевіримо його, перш ніж запускати. Отже, можна побачити, це пом'якшення стосується пошуку та запобігання дивовижної активності на кінцевих точках. Історія дещо змінюється, коли активність є відомим експлойтом, тож це переносить до наступного рішення.

Захист від експлойтів. Деякі підозрілі дії в системі можуть виявитися нормальними, але потрібно спершу дослідити і з'ясувати. Однак, без сумніву, потрібно негайно припинити всі відомі експлойти. Термін Індикатори компромісу, означає, що точно знаємо, що шукати. Ось що стосується захисту від експлойтів. Це рішення радить знайти всі відомі подвиги і захиститися від них. Подумавши про Drive-by Compromise ситуація, коли шкідливий код досягає ваших кінцевих точок через звичайний перегляд, іноді з законних, але зламаних веб-сайтів. Звичайно, сам веб-сайт міг бути законним, але не потрібно довіряйти йому сліпо! Захист від експлойтів зупиняє всі відомі шкідливі програми, наприклад, незалежно від того, на якому сайті їх обслуговують.

Execution Prevention. Що відбувається, коли система встановлює програму, завантажену із сумнівного джерела? Що робити, якщо зловмисник використовує непотрібну підтримку настільного комп'ютера або програмне забезпечення

віддаленого доступу, інструменти, які спочатку не слід було залишати? Вони можуть не відображатися як підозріла поведінка або відомий експлойт. Тому Execution Prevention — це видимість і контроль додатків кінцевої точки. Йдеться про виявлення та блокування. Це дозволяє кінцевим точкам запускати санкціоновані програми та сценарії — ті, що вимагає завдання, і ті, що дозволяє політика безпеки — одночасно блокуючи все інше. Execution Prevention також стосується «Обмежити встановлення програмного забезпечення (M1033)», який контролює схвалене/незатверджене програмне забезпечення та кому що дозволено встановлювати.

Ці три рішення охоплюють велику частину MITRE ATT&CK TTPs. Behavior Prevention охоплює 2 прийоми та 15 підтехнік, захист від експлойтів охоплює 9 прийомів, а Execution Prevention охоплює 18 прийомів — і набагато більше підтехнологій.

Ці групи об’єднуються під загальним заголовком «Захист кінцевої точки», хоча насправді MITER не позначає їх таким чином. Основні принципи Zero Trust також використовуються в даній технології. Один з них, відповідно до «Архітектура нульової довіри NIST (NIST SP 800-207)», це: «Підприємство контролює та вимірює цілісність і безпеку всіх належних і пов’язаних з ними активів. Жодному активу не можна довіряти».

З огляду на це, виникає питання: як можна довіряти кінцевим точкам, які:

(а) запускають несанкціоноване або непотрібне програмне забезпечення,

(б) демонструють явні ознаки компромісу

(в) демонструють підозрілу чи незвичайну поведінку.

Аналізуючи ці три твердження, можемо дійти висновку, що не можна. Ось чому ці три рішення захисту кінцевих точок настільки важливі.

Розглянемо, яким чином ці три технології реалізовані в Cisco AMP for Endpoints.

Behavior Prevention on Endpoint. AMP для кінцевих точок використовує багато можливостей даної технології, але виділимо лише одну з його можливостей: захист поведінки. Його назва майже ідентична ATT&CK Mitigation, оскільки

навмисно використовуються прості терміни, щоб описати, що насправді робиться. Захист поведінки в AMP виявляє та зупиняє загрози на основі поведінки системи, як рекомендується. Він поміщає файли в карантин, завершує процеси і, коли потрібна додаткова інформація, завантажує файл у AMP Cloud для подальшого аналізу. Якщо доведиться, що поведінка файлу є зловмисною, то програма також автоматично зупиняє його.

Exploit Prevention. AMP для кінцевих точок має ще одну схожу за звучанням функцію під назвою Exploit Prevention, або скорочено ExPrev. ExPrev захищає кінцеві точки від пошкодження пам'яті та атак із впровадженням процесів, які часто використовуються прихованими шкідливими програмами, а також системних експлойтів, спрямованих на вразливості програмного забезпечення захищених процесів. На хостах Windows він працює разом із системним захистом процесів AMP, щоб захистити системні процеси від підробок або скомпрометації.

Execution Prevention. AMP для кінцевих точок також керує програмами, які працюють на кінцевих точках. Він запобігає запуску неавторизованих програм і вимикає вразливі програми, доки не можна буде їх виправити. Якщо є підозра, що файл кінцевої точки є зловмисним, але потрібен час для дослідження, він просто обмежує використання файлу, не видаляючи його. Таким чином, якщо все гаразд, то можна просто звільнити фіксацію. Якщо це шкідливо, то файл видаляється.

Вбудований ATT&CK. AMP for Endpoints відображає індикатори компромісу безпосередньо в ATT&CK [9].

Захист від шкідливої діяльності

Secure Endpoint постійно відстежує всю активність кінцевої точки та забезпечує виявлення під час виконання та блокування аномальної поведінки запущеної програми на кінцевій точці. Наприклад, коли поведінка кінцевої точки вказує на те, що це програмне забезпечення-вимагач, злочинні процеси буде припинено, запобігаючи шифрування кінцевої точки та зупиняючи атаку.

Розглянемо механізм, доданий до Cisco Advanced Malware Protection for Endpoints як частина AMP Connector версії 6.1.5 для Windows — захист від шкідливої діяльності.

Атаки програм-вимагачів можуть приймати різні форми та форми. Програми-вимагачі – це тип зловмисного програмного забезпечення, яке зазвичай намагається зашифрувати файли на комп'ютері жертви. Після успішного шифрування він вимагає оплати перед розшифруванням викуплених даних і поверненням доступу жертві.

Атаки програм-вимагачів зазвичай здійснюються з використанням шкідливого корисного навантаження, яке розповсюджується як законний файл, який обманом змушує користувача завантажити або відкрити, коли він надходить як вкладення електронної пошти. Проте були приклади атак програм-вимагачів, які розповсюджувалися без взаємодії з користувачем. Мотивація для зловмисників, які використовують програмне забезпечення-вимагач, майже завжди грошова, і на відміну від інших типів атак, жертва зазвичай повідомляється про те, що сталася атака. Потім жертві дають інструкції, як оговтатися від нападу. Платіж часто вимагають у віртуальній валюті, щоб особу кіберзлочинця було нелегко визначити. Важливим моментом тут є те, що сплата викупу не гарантує розшифровки даних, і це також спонсорує розробку наступного покоління програм-вимагачів.

Механізм захисту від шкідливої активності AMP для кінцевих точок (MAP), включений до AMP Connector версії 6.1.5 для Windows, захищає кінцеві точки, відстежуючи систему та виявляючи процеси, які виявляють шкідливі дії під час їх виконання, і зупиняє їх роботу. Оскільки механізм MAP виявляє загрози, спостерігаючи за поведінкою процесу під час виконання, він може загалом визначити, чи система піддається атаці з боку нового варіанта програм-вимагачів або шкідливих програм, які могли уникнути інших продуктів безпеки та технологій виявлення, наприклад, застарілих підписів. -виявлення шкідливих програм на основі. Перший випуск механізму MAP спрямований на виявлення, блокування та карантин атак програм-вимагачів на кінцеву точку.

AMP для решітки захисту кінцевих точок

Можливості захисту AMP для кінцевих точок включають кілька технологій, які працюють разом для запобігання, виявлення та усунення шкідливого коду на кінцевій точці.

Основні технології запобігання в пам'яті включають:

Запобігання експлуатації: захищає кінцеві точки від атак ін'єкції пам'яті, які зазвичай використовуються шкідливими програмами, і атак нульового дня на невиправлені вразливості програмного забезпечення в захищених процесах.

Захист системних процесів: захищає важливі системні процеси Windows від компрометації через атаки ін'єкції пам'яті іншими процесами.

Основні технології виявлення на диску включають:

Хмара AMP надає доступ до глобальної розвідувальної бази даних, яка постійно оновлюється та доповнюється новими виявленнями, а також надає широкий спектр знань для конектора AMP за допомогою хеш-пошуку один на один, загальний механізм підписів і механізм машинного навчання.

TETRA є традиційним антивірусним механізмом на основі сигнатур, який знаходиться на кінцевій точці та забезпечує можливості виявлення шкідливих програм на диску; TETRA є частиною AMP Connector для Windows (ClamAV є автономним двигуном для Mac і Linux).

Захист від шкідливої діяльності: забезпечує виявлення під час виконання та блокування ненормальної поведінки запущеної програми на кінцевій точці (наприклад, поведінки, пов’язаної з програмним забезпеченням-вимагачем).

·Спеціальні виявлення: служать задля надання надійних можливостей контролю адміністратору безпеки, дозволяючи визначати власні підписи та застосовувати заблоковані списки.

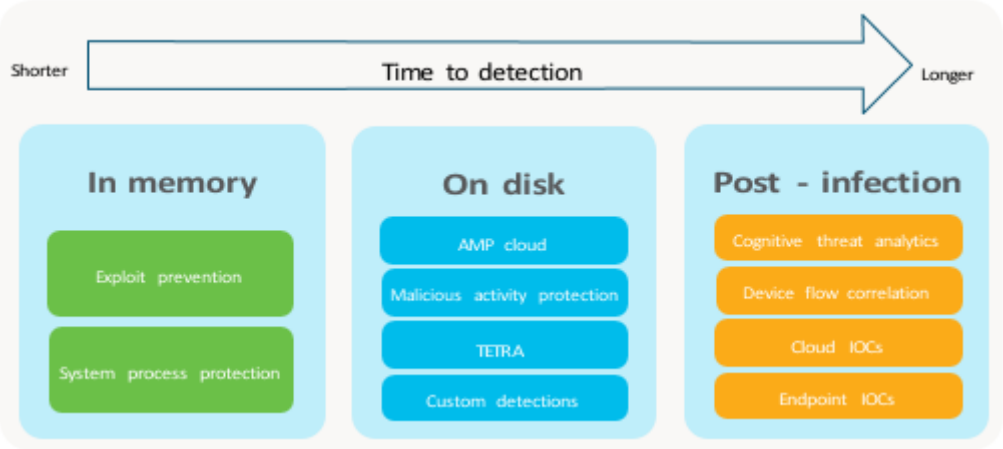

Рис. 3.3. AMP для кінцевих точок – решітка захисту

Основні технології постінфекційного виявлення включають:

Аналітика когнітивних загроз: використовує машинне навчання та штучний інтелект для кореляції трафіку, створеного користувачами, для надійного визначення трафіку команд і керування, ексфільтрації даних і, можливо, небажаних програм, які вже працюють у середовищі; для цього потрібен проксі-сервер, який надає веб-журнали, або Cisco Stealthwatch Flow Collector, що постачає NetFlow.

Кореляція потоків пристрою: дозволяє відстежувати мережеву активність і визначає, які дії повинен виконувати конектор AMP, коли виявлено підключення до шкідливих хостів.

Хмарна індикація компромісу (IOC): функція, яка дозволяє виявляти підозрілу поведінку, що спостерігається на кінцевих точках, і шукає шаблони зловмисного програмного забезпечення та сповіщень на таких; Хмарні IOC не передбачають активне блокування.

Кінцева точка IOC: є потужним інструментом реагування на інциденти для сканування посткомпромісних індикаторів на кількох комп'ютерах, і його можна імпортувати з відкритих файлів на основі IOC, які записуються для активації властивостей файлу.

Ці функції безпеки є основою загального підходу до розширеного захисту від шкідливих програм. Хоча Cisco рекомендує використовувати всі ці механізми в поєднанні один з одним, щоб використовувати повну цінність продукту, клієнти можуть вибрати, увімкнути чи вимкнути ту чи іншу функцію за допомогою політики. MAP (Malicious activity protection), який є предметом технічної документації, сам по собі є лише одним із важливих елементів функціональності, які надає AMP для кінцевих точок. Хоча ці технології перераховані окремо, ці технології працюють разом як решітка виявлення, щоб забезпечити покращену видимість та покращений контроль у всьому континуумі атаки.

Технологія захисту від шкідливої діяльності

Механізм MAP — це механізм виявлення на основі поведінки, який визначає шкідливі дії, які відбуваються на кінцевій точці під час виконання. Після обширних

досліджень із багатьма варіантами зразків програм-вимагачів, які спостерігалися в дикій природі, команда досліджень і розробників AMP for Endpoints приписала поширену поведінку, пов'язану з такими загрозами, для створення набору правил, який є частиною механізму, що знаходиться на самому конекторі AMP.

Як це працює

Механізм MAP постійно перевіряє певні зміни у захищеній системі, щоб визначити процеси, які мають бути визнані винними, коли дії, описані в наборі поведінкових правил, збігаються.

Відповідно до конфігурації політики щодо процесів, виявлених MAP, можна виконати такі дії:

— Журнал виявлення: у цьому режимі ідентифікований шкідливий процес не блокується MAP, але виявлення реєструється на консолі AMP для кінцевих точок. (Це режим аудиту, де не відбувається блокування чи карантин, але виявлення реєструється).

— Блокувати виконання процесу: у цьому режимі шкідливий двійковий файл ідентифікується та блокується, і більше не може виконуватися (подібно до того, як працює функція блокування додатків).

— Процес карантину: цей режим припиняє процес, що порушує порушення, і поміщає файли в карантин.

Набір правил виявлення в движку MAP шукає відхилення в системі. Наприклад, якщо процес читає, записує та перейменовує набір файлів протягом короткого проміжку часу, то правило може ініціювати дії щодо цього процесу. Крім того, якщо процес читає та записує вміст файлу в інший файл, а потім видаляє вихідні файли, то механізм MAP може запустити дію, визначену в політиці. Це лише кілька прикладів правил, присутніх у наборі правил. Правила є внутрішніми для розробників і ніколи не доступні користувачам, а також не налаштовуються користувачами. Інженерні та дослідницькі групи AMP for Endpoints постійно оцінюють методи, які використовуються шкідливими програмами та програмами-вимагателями в дикій природі, щоб підвищити очікуваний рівень захисту.

Для боротьби з хибнопозитивними виявленнями процеси, ідентифіковані механізмом MAP як такі, що виявляють зловмисну активність, перевіряються на огорожі, щоб запобігти випадковому блокуванню або карантину законних програм і компонентів операційної системи.

Незважаючи на те, що конектор AMP може виявляти та запобігати повній загрозі компрометації системним програмним забезпеченням-вимагачем, можливо, деякі файли будуть зашифровані процесом-порушником, доки механізм MAP не визначить, що процес відповідає критеріям для позначення зловмисного. Конектор AMP повідомить про файли, які були змінені порушенням процесу, щоб у разі потреби їх можна було швидко відновити з резервних копій.

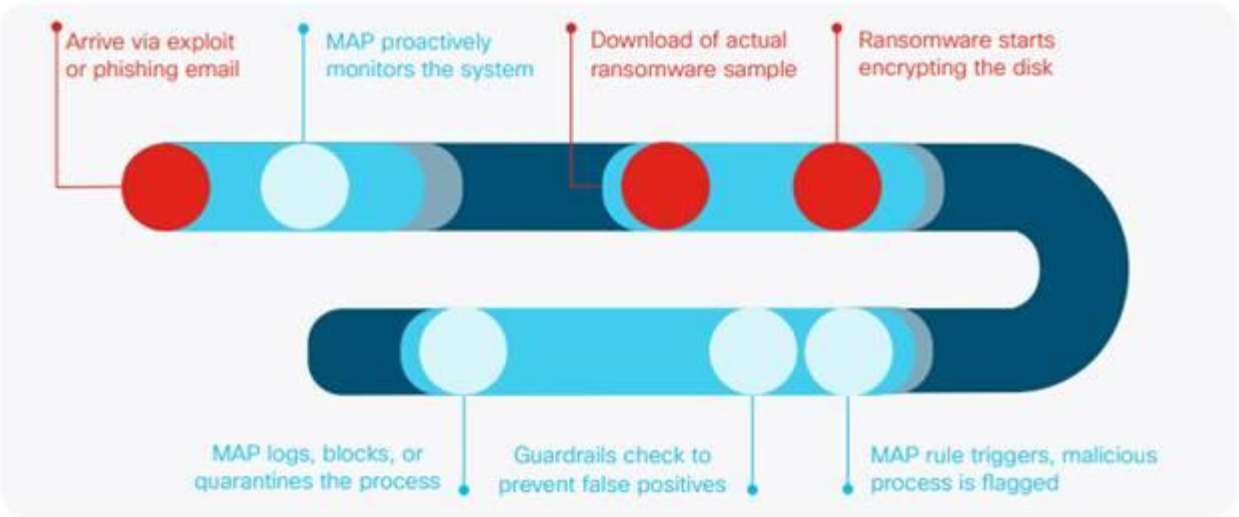

Рис. 3.5. Процес виявлення MAP

MAP є частиною AMP for Endpoints Connector для Windows.

Продуктивність і сумісність

Вплив на продуктивність є великою частиною критеріїв вибору безпеки кінцевої точки. AMP для кінцевих точок додає незначні витрати на продуктивність системи. Увімкнення механізму MAP не означає значного зниження продуктивності або змін у роботі кінцевого користувача. Очікуване збільшення використання ЦП, пов’язане з увімкненням механізму MAP, становить приблизно 5%, а вплив на продуктивність пам’яті, диска та мережі близький до нуля.

Сумісність із програмним забезпеченням, встановленим на кінцевій точці, є важливим аспектом будь-якого рішення безпеки кінцевої точки. Механізм MAP спеціально не має жодних відомих проблем сумісності зі стороннім програмним забезпеченням безпеки.

Законні програми, що використовуються в середовищі клієнта, які демонструють поведінку, подібну до програм-вимагачів, можливо, потрібно буде виключити з моніторингу MAP. Простим прикладом є програмне забезпечення для архівації. Виключення процесів можна застосувати, щоб запобігти моніторингу програм AMP для кінцевих точок і, за бажанням, їхніх дочірніх процесів на наявність зловмисної активності механізму MAP. Зауважте, що дочірні процеси, створені виключеним процесом, не виключаються за замовчуванням.

Загалом, виключення також можна використовувати для вирішення конфліктів з іншими продуктами безпеки або для пом’якшення проблем з продуктивністю, виключаючи каталоги, що містять великі файли, до яких часто записується, наприклад бази даних.

Хоча MAP є механізмом, здатним загалом зупиняти програму-вимагач під час виконання (без урахування вектора експлуатації, можливостей поширення, хешування зразка, цільових файлів, розширень файлів тощо), для цілей тестування може бути корисно зв’язатися з кількома приклади атак, які можуть бути заблоковані або поміщені на карантин двигуном. Тестування проводилося з використанням інфраструктури, автоматизованої для тестування з використанням різних середовищ віртуалізації, а також голих машин з підтримуваними операційними системами. Інженерні та дослідницькі групи AMP for Endpoints постійно оцінюють методи, які використовуються авторами програм-вимагачів для підвищення рівня захисту.

Деякі сімейства програм-вимагачів, які були заблоковані або поміщені на карантин під час виконання MAP, включають SamSam, WannaCry, JigSaw, Jaff, Cerber, TeslaCrypt, CryptoFortress та багато інших.

Оскільки механізм MAP використовує захист на основі поведінки для пошуку дій, неможливо уникнути виявлення за допомогою простих змін до хешів файлів або обфускації з користувачем пакувальників.

Атаки програм-вимагачів суттєво впливають на багато організацій у всьому світі. Протягом багатьох років цей бізнес різко зріс, і найпоширеніші атаки програм-вимагачів минулого гідно розповідають про те, як він зріс. Як і у випадку з великою кількістю порушень, вина може полягати в тому, як організації будують та підтримують свою IT-інфраструктуру. Також завжди існує людський фактор — багато атак програм-вимагачів починаються з простого фішингового електронного листа, навіть не завжди націленого та добре підготовленого зловмисниками.

MAP запроваджує інший підхід до захисту від шкідливих програм і програм-вимагачів, який більше зосереджений на виявленні під час виконання для блокування та карантину. Цей підхід кращий у визначенні варіантів програм-вимагачів під час виконання без залежності від підходів на основі сигнатур і не вимагає попередніх знань про те, як була створена загроза. Cisco настійно рекомендує використовувати цю можливість у поєднанні з архітектурним підходом до безпеки та найкращими практиками інформаційної безпеки, які сприятимуть ефективному вирішенню або запобігання, або серйозного обмеження впливу таких загроз. Наявність надійної, багатошарової стратегії глибокого захисту гарантує, що організації зможуть обмежити поширені відключення системи [13].

3.2. Додаткові технології захисту кінцевих точок Cisco Secure Endpoint

Динамічний аналіз

Secure Endpoint включає вбудоване високобезпечне середовище пісочниці, на основі Cisco Threat Grid, щоб проаналізувати поведінку підозрілих файлів. Аналіз файлів дає детальну інформацію про файли, включаючи серйозність поведінки, оригінальне ім’я файлу, знімки екрана запуску зловмисного програмного забезпечення, та захоплення зразків пакетів. Озброївшись цією інформацією, буде

краще розуміння того, що необхідно для стримування спалаху та блокування майбутні атаки.

Secure Malware Analytics швидко аналізує файли та підозрілу поведінку у середовищі. Команди безпеки отримують аналітику зловмисного програмного забезпечення та інформацію про загрози на основі контексту, тому вони озброєні розумінням того, що робить файл, і можуть швидко реагувати на загрози.

Secure Malware Analytics аналізує поведінку файлу щодо мільйонів зразків і мільярдів артефактів шкідливого програмного забезпечення. Це дає можливість отримати глобальне та історичне уявлення про зловмисне програмне забезпечення, те, що воно робить, і яку загрозу воно становить для організації.

Secure Malware Analytics визначає ключові поведінкові індикатори шкідливого програмного забезпечення та пов'язаних з ними кампаній. Групи безпеки можуть заощадити час, швидко розставляючи пріоритети атак із найбільшим потенційним впливом.

Прискорити розслідування інциденту та швидше розуміти загрози та реагувати на них. Це досягається перевагами надійних пошукових можливостей Secure Malware Analytics, кореляції та детального статичного та динамічного аналізу. Використання таких інструментів, як Glovebox, дає безпечно взаємодіяти із зразками та безпосередньо спостерігати за поведінкою шкідливих програм.

Прискорене виявлення загроз зловмисного програмного забезпечення та реагування на них за допомогою потужного API, який інтегрує та автоматизує існуючі продукти та процеси безпеки [10].

Полювання на загрози SecureX

Проактивний підхід, орієнтований на аналітику для виявлення прихованих передових погрози. Ця можливість пропонується виключно в рамках нового Premier рівень ліцензії в Secure Endpoint. Він повідомляє реагуючим на інцидент а розповідь про те, як був помічений напад або як він розвивався і що робити зробити наступне з точки зору відповіді. Мета – виявити та перешкодити атаки до того, як вони завдадуть будь-якої шкоди.

Розслідування програм-вимагачів і відповідь

Cisco SecureX — це вбудована в хмарі платформа, яка з’єднує Cisco Secure та інфраструктура системи компанії. Це дозволяє радикально скоротити час перебування і виконання людських завдань. Cisco Talos Incident Response розробив спеціально план дій щодо програм-вимагачів (PoA). Для реагування на інцидент, яке було перевірено та підтверджено кількома, скомпрометовані середовища.

Реагування на надзвичайну ситуацію

У разі таких інцидентів, як злом даних або програмне забезпечення-вимагач, SecureX швидко вирішуємо найнагальніші проблеми. В першу чергу – ізолювати зловмисника, обстежити та локалізувати ситуацію, виявити першопричину та розробити стратегії для усунення основних проблем.

З ретейнером команда буде доступна ще до інциденту з проактивними послугами для посилення безпеки організації. Якщо потрібна невідкладна допомога, команда Cisco завжди готова, щоб почати роботу практично до того, як вони виїдуть на місце[11].

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми забезпечення кібербезпеки кінцевих точок. Проаналізовано існуючі технології забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи. Досліджена технологія забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи на базі Cisco AMP for Endpoints.

Визначено методи та засоби забезпечення кібербезпеки кінцевих точок, які реалізовані в Cisco AMP for Endpoints.

Встановлено основні функції та принципи роботи програмного комплексу Cisco AMP for Endpoints. Cisco Advanced Malware Protection (AMP) — система, яка захищає бізнес під час і після атак, що робить її найбільш надійною формою захисту від шкідливих програм. Cisco AMP використовує глобальний аналіз загроз для використання захисту мережі ще до того, як відбувається проникнення. Під час взлому мережа ідентифікує та блокує атаку, використовуючи потужну комбінацію інтелекту, реєструючи файли та розширений аналіз шкідливих програм. Після того, як зловмисник проник у мережу, Cisco AMP представляє групі безпеці компанції чіткі представлення про походження шкідливого ПО, його метод і точку входу, де він знаходився та його поточної траєкторії. Ця комбінація захисту на певний момент часу та ретроспективи дозволяє досить швидко виявляти, обмежувати та утримувати загрозу, щоб захистити бізнес від збитку.

Використання Cisco AMP надає компанії доступ до широкого набору функцій безпеки в тому числі:

– Фільтрування файлів, що порушують політику з Інтернету, електронної пошти і т.д.

– Виявлення та захист від спроб експлойтів на стороні клієнта та спроб експлойтів, спрямованих на клієнтські програми, такі як Java та Flash.

– Розпізнавання, блокування та аналіз шкідливих файлів.

– Виявлення шкідливих програм та виявлення потенційно зламаних пристроїв.

– Відстеження поширення шкідливих програм та комунікацій.

– Зниження загроз повторного зараження.

У роботі запропоновано варіант технології забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи на базі Cisco AMP for Endpoints.

Розроблено рекомендації фахівцям із кібербезпеки щодо застосування технології управління захистом кінцевих точок інформаційної системи на підприємстві.

ПЕРЕЛІК ПОСИЛАНЬ

1. Информационная безопасность: Основные проблемы [Електронний ресурс] – Режим доступу: https://www.easy-tech.ru/articles/informatsionnaya_bezopasnost_osnovnye_problemy/

2. WHAT IS ENDPOINT SECURITY? HOW ENDPOINT PROTECTION WORKS [Електронний ресурс] – Режим доступу: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/

3. 10 найкращих служб безпеки EDR у 2021 році для захисту кінцевих точок [Електронний ресурс] – Режим доступу: https://uk.myservername.com/10-best-edr-security-services-2021

4. Endpoint Detection and Response (EDR) Solutions Reviews and Ratings [Електронний ресурс] – Режим доступу: https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

5. Защита конечных точек в современных условиях: инструменты и основные проблемы [Електронний ресурс] – Режим доступу: https://ko.com.ua/zashhita_konechnyh_tochek_v_sovremennyh_usloviyah_instrumenty_i_osnovnye_problemy_129548

6. Эволюция векторов атак на конечные точки предприятия [Електронний ресурс] – Режим доступу: https://cis.bakotech.com/news/evolyuciya-vektorov-atak-na-konechnie-tochki-predpriyatiya/

7. Strong Showing For Datashield Partners In 2021 Gartner Magic Quadrant [Електронний ресурс] – Режим доступу: https://www.datashieldprotect.com/blog/partners-gartner-magic-quadrant-2021

8. Лучшие решения по безопасности устройств: обзор по версии Gartner(EDR & EPP) [Електронний ресурс] – Режим доступу: https://softlist.com.ua/articles/luchshie-resheniya-po-bezopasnosti-ustroistv-obzor-po-versii-gartner/

9. Steve Caimi. MITRE ATT&CK: The Magic of Endpoint Protection [Електронний ресурс] – Режим доступу: https://blogs.cisco.com/security/mitre-attck-the-magic-of-endpoint-protection

10 Cisco Secure Malware Analytics (Threat Grid) [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/security/threat-grid/index.html

11 Incident Response Services [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/security/sas-incident-response.html#~news-events

12. Cisco Advanced Malware Protection for Endpoint [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/c11-742008-00-cisco-amp-for-endpoints-wp-v2a.pdf

13 Cisco Advanced Malware Protection for Endpoints [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/amp-for-endpoints/white-paper-c11-740980.html

14 Top 6 Ways Cisco Prevents Ransomware with EPP & EDR [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/dam/en/us/products/se/2021/7/Collateral/top-6ways-prevents-ransomware-epp-edr.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)