ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА ПЛАТФОРМІ HCL BIGFIX»

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

КИЇВ – 2020

РЕФЕРАТ

Текстова частина магістерської роботи: 70 сторінки, 19 рисунків, 14 джерел.

Об'єкт дослідження – процес забезпечення захисту кінцевих точок корпоративної інформаційної системи.

Предмет дослідження – технологія управління захистом кінцевих точок корпоративної інформаційної системи.

Мета роботи – розробити варіант топології системи управління захистом кінцевих точок корпоративної інформаційної системи та рекомендації щодо застосування технології їх захисту на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління захистом кінцевих точок корпоративної інформаційної системи.

В роботі зроблено аналіз проблеми забезпечення кібербезпеки корпоративної інформаційної системи та визначено мета та завдання управління захистом кінцевих точок корпоративної інформаційної системи. Проведено аналіз існуючих технологій управління захистом кінцевих точок корпоративної інформаційної системи.

Досліджено методи та засоби управління захистом кінцевих точок на прикладі HCL BigFix. Визначено призначення, основні функції та склад платформи HCL BigFix.

На основі досліджень проведених в роботі розроблено варіант технології управління захистом кінцевих точок корпоративної інформаційної системи та рекомендації щодо застосування технології управління їх захистом на підприємстві.

Галузь використання – кібербезпека корпоративної інформаційної системи.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ЗАХИСТ КІНЦЕВИХ ТОЧОК, УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК, ТЕХНОЛОГІЯ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КІС – корпоративна інформаційна система

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

ШІ – штучний інтелект

AMP – Advanced Malware Protection

APT – Advanced Persistent Threats

BYOD – Bring Your Own Device

CRM – Customer Relationship Management

DLP – Data Loss Prevention

EDR – Endpoint Detection and Response

EMS – Endpoint Management System

ERP – Enterprise Resource Planning

EPP – Endpoint Protection Platform

IoC – Indicator of Compromise

IPS – Intrusion Prevention System

HIPS – Host-Based Intrusion Prevention System

MDM – Mobile Device Management

MDR – Managed Detection and Response

ML – Machine Learning

RBAC – Role-Based Access Control

SOC – Security Operations Center

UEBA – User And Entity Behavior Analytics

UEM – Unified Endpoint Management

VPN – Virtual Private Network

ВСТУП

Актуальність дослідження. Забезпечення безпеки кінцевих точок в умовах кібернетичних впливів відноситься до методології захисту корпоративної мережі під час доступу через віддалені пристрої, такі як ноутбуки або інші бездротові і мобільні пристрої. Кожен пристрій з віддаленим підключенням до мережі створює потенційну точку входу для загроз безпеки. Безпека кінцевих точок призначена для захисту кожної кінцевої точки в мережі, створеної цими пристроями.

Зазвичай безпека кінцевих точок забезпечується системою, яка складається з програмного забезпечення безпеки, розташованого на центрально керованому і доступному сервері або шлюзі в мережі, на додаток до клієнтського програмного забезпечення, що встановлюється на кожній з кінцевих точок (або пристроїв). Сервер автентифікує логіни з кінцевих точок, а також оновлює програмне забезпечення пристрою при необхідності. Хоча програмне забезпечення для забезпечення безпеки кінцевих точок розрізняється залежно від постачальника, можна очікувати, що більшість пропозицій програмного забезпечення будуть містити антивірусне та антишпигунське програмне забезпечення, міжмережевий екран, а також систему запобігання вторгнень на хост (HIPS).

Безпека кінцевих точок стає все більш поширеною функцією кібербезпеки корпоративних мереж, оскільки все більше співробітників залучають до роботи мобільні пристрої споживачів, а компанії дозволяють своїм мобільним співробітникам використовувати ці пристрої в корпоративній мережі. Також, застосування технології захисту саме кінцевих точок реалізує принцип «розподіленого захищеного середовища».

Це визначає актуальність дослідження щодо управління захистом кінцевих точок корпоративної інформаційної системи на базі HCL BigFix.

Об'єкт дослідження – процес забезпечення захисту кінцевих точок корпоративної інформаційної системи.

Предмет дослідження – технологія управління захистом кінцевих точок корпоративної інформаційної системи.

Мета роботи – розробити варіант технології управління захистом кінцевих точок корпоративної інформаційної системи та рекомендації щодо застосування технології управління їх захистом на підприємстві.

Наукові завдання:

дослідити сутність проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи;

встановити сутність завдань управління захистом кінцевих точок корпоративної інформаційної системи;

проаналізувати існуючі технології управління захистом кінцевих точок корпоративної інформаційної системи;

проаналізувати методи та засоби управління захистом кінцевих точок корпоративної інформаційної системи;

проаналізувати основні функції та принципи реалізації управління захистом кінцевих точок корпоративної інформаційної системи.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесів управління захистом кінцевих точок.

Практичне значення одержаних результатів полягає в розробці варіанта технології управління захистом кінцевих точок корпоративної інформаційної системи на базі HCL BigFix, а також у розробці рекомендацій щодо застосування технології управління захистом кінцевих точок корпоративної інформаційної системи.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

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

У найзагальнішому сенсі термін *корпорація* означає об'єднання підприємств, що працюють під централізованим управлінням та вирішують загальні завдання. Корпорація є складною, багатопрофільною структурою і внаслідок цього має розподілену ієрархічну систему управління [1].

Корпоративне управління визначається як система взаємовідносин між акціонерами, радою директорів і правлінням, визначені статутом, регламентом і офіційною політикою компанії, а також принципом верховенства права на основі прийнятої бізнес моделі.

Бізнес-модель – це опис підприємства, як складної системи, із заданою точністю. В рамках бізнес-моделі відображаються всі об'єкти (сутності), процеси, правила виконання операцій, існуюча стратегія розвитку, а також критерії оцінки ефективності функціонування системи. Форма представлення бізнес-моделі і рівень її деталізації визначаються цілями моделювання і прийнятою точкою зору.

Підприємства, відділення та адміністративні офіси, що входять в корпорацію, як правило, розташовані на достатньому видаленні один від одного. Їх інформаційний зв'язок один з одним утворює комунікаційну структуру корпорації, основою якої є *інформаційна система* [1].

Інформаційна модель – підмножина бізнес-моделі, що описує всі існуючі (в тому числі не формалізовані в документальному вигляді) інформаційні потоки на підприємстві, правила обробки і алгоритми маршрутизації всіх елементів інформаційного поля.

Інформаційна система (ІС) – це вся інфраструктура підприємства, задіяна в процесі управління всіма інформаційно-документальними потоками, що включає в себе такі обов'язкові елементи [1]:

інформаційна модель, яка являє собою сукупність правил і алгоритмів функціонування ІС. Інформаційна модель включає в себе всі форми документів, структуру довідників і даних тощо;

регламент розвитку інформаційної моделі і правила внесення в неї змін;

кадрові ресурси (департамент розвитку, які залучаються консультанти), що відповідають за формування і розвиток інформаційної моделі;

програмне забезпечення, конфігурація якого відповідає вимогам інформаційної моделі (програмне забезпечення є основним рушієм і, одночасно, механізмом управління ІС). Крім того, завжди існують вимоги до постачальника програмного забезпечення, які регламентують процедуру технічної і призначеної для користувача підтримки впродовж усього життєвого циклу;

кадрові ресурси, що відповідають за налаштування і адаптацію програмного забезпечення, і його відповідність затвердженій інформаційній моделі;

регламент внесення змін до структури (специфічні настройки, структури баз даних і т.д.) і конфігурацію програмного забезпечення та склад його функціональних модулів;

апаратна база, яка відповідає вимогам по експлуатації програмного забезпечення (комп'ютери на робочих місцях, периферія, канали телекомунікацій, системне програмне забезпечення та СУБД);

кадрові ресурси, включаючи персонал по обслуговуванню апаратної бази;

правила використання програмного забезпечення і призначені для користувача інструкції, регламент навчання і сертифікації користувачів.

Ресурси корпорацій включають: матеріальні (матеріали, готова продукція, основні засоби); фінансові; людські (персонал); знання (ноу-хау); корпоративна інформаційна система.

Система управління будь-якої компанії включає три основні підсистеми [1]:

планування продажів і операцій. Це загальний план функціонування підприємства, що встановлює обсяги виготовлення готової продукції. Головним тут є планування попиту і оцінка ресурсів, необхідних для задоволення попиту. Тут же створюється основний виробничий план, який визначає, які вироби, в якій

кількості і в які терміни потрібно зробити;

детальне планування необхідних ресурсів (матеріалів, виробничих потужностей, трудових ресурсів тощо). Складений план визначає час і обсяг замовлень для всіх матеріалів і комплектуючих, необхідних для реалізації основного виробничого плану;

управління виконанням планів в процесі виробництва і закупівель (постачання).

Всі ці робочі процеси вищеперелічених підсистем реалізуються на основі корпоративної інформаційної системи.

Корпоративні інформаційні системи (КІС) – це інтегровані системи управління територіально розподіленої корпорацією, засновані на поглибленому аналізі даних, широке використання систем інформаційної підтримки прийняття рішень, електронних документообігу та діловодстві. КІС покликані об'єднати стратегію управління підприємством і передові інформаційні технології [1].

Корпоративна інформаційна система – це сукупність технічних і програмних засобів підприємства, що реалізують ідеї і методи автоматизації.

Комплексна автоматизація бізнес процесів підприємства на базі сучасної апаратної та програмної підтримки може називатися по-різному. В даний час поряд з назвою корпоративні інформаційні системи вживаються, наприклад, такі назви [1]:

автоматизовані системи управління (АСУ);

інтегровані системи управління (ІСУ);

інтегровані інформаційні системи (ІІС);

інформаційні системи управління підприємством (ІСУП).

Головне завдання КІС – ефективне управління всіма ресурсами підприємства (матеріально-технічними, фінансовими, технологічними і інтелектуальними) для отримання максимального прибутку і задоволення матеріальних і професійних потреб усіх співробітників підприємства.

КІС за своїм складом є сукупністю різних програмно-апаратних платформ, універсальних і спеціалізованих додатків різних розробників, інтегрованих в

єдину інформаційно систему, яка найкращим чином вирішує в деякому роді унікальну задачу кожного конкретного підприємства. Тобто, КІС – людино-машинна система і інструмент підтримки інтелектуальної діяльності людини, яка під його впливом повинна [1]:

накопичувати певний досвід і формалізовані знання;

постійно вдосконалюватися і розвиватися;

швидко адаптуватися до мінливих умов зовнішнього середовища і нових потреб підприємства.

Комплексна автоматизація підприємства має на увазі переклад в площину комп'ютерних технологій всіх основних ділових процесів організації. І використання спеціальних програмних засобів, що забезпечують інформаційну підтримку бізнес-процесів, як основи КІС представляється найбільш виправданим і ефективним. Сучасні системи управління бізнес-процесами дозволяють інтегрувати навколо себе різне програмне забезпечення, формуючи єдину інформаційну систему. Тим самим вирішуються проблеми координації діяльності співробітників і підрозділів, забезпечення їх необхідною інформацією і контролю виконавської дисципліни, а керівництво отримує своєчасний доступ до достовірними даними про хід виробничого процесу і має кошти для оперативного прийняття і втілення в життя своїх рішень [1].

Автоматизований комплекс засобів має являти собою гнучку відкриту структуру, яку можна перебудовувати і доповнювати новими модулями або зовнішнім програмним забезпеченням.

Під *корпоративною інформаційною системою* розуміють інформаційну систему організації, що відповідає наступним мінімальним переліком вимог [1]:

функціональна повнота системи;

надійна система захисту інформації;

наявність інструментальних засобів адаптації та супроводу системи;

реалізація віддаленого доступу і роботи в розподілених мережах;

забезпечення обміну даними між розробленими інформаційними системами, програмними продуктами, що функціонують в організації тощо;

можливість консолідації інформації;

наявність спеціальних засобів аналізу стану системи в процесі експлуатації.

Функціональна повнота системи забезпечується [1]:

виконанням міжнародних стандартів управлінського обліку MRP II, ERP, CSRP;

автоматизацією в рамках системи вирішення завдань планування, бюджетування, прогнозування, оперативного (управлінського) обліку, бухгалтерського обліку, статистичного обліку та фінансового-економічного аналізу;

формуванням і веденням обліку за вітчизняними та міжнародними стандартами тощо.

Найбільш розвинені корпоративні інформаційні системи призначені для автоматизації всіх функцій управління організацією: від науково-технічної та маркетингової підготовки її діяльності до реалізації її продукції і послуг. В даний час КІС мають в основному економічну і виробничу спрямованість.

Розглядаючи архітектуру великих організацій, прийнято використовувати поняття «корпоративна архітектура». Її можна представити у вигляді сукупності декількох типів архітектур [2]:

бізнес архітектура (Business architecture);

IT-архітектура (Information Technology architecture);

архітектура даних (Data architecture);

програмна архітектура (Software architecture);

технічна архітектура (Hardware architecture).

Модель корпоративної архітектури представлена на рис. 1.1.

Технічна архітектура є першим рівнем архітектури інформаційної системи. Вона описує всі апаратні засоби, що використовуються при виконанні заявленого набору функцій, а також включає засобу забезпечення мережної взаємодії й надійності. У технічній архітектурі вказуються периферійні пристрої, мережні комутатори й маршрутизатори, жорсткі диски, оперативна пам’ять, процесори, сполучні кабелі, джерела безперебійного живлення тощо.

Рис. 1.1. Модель корпоративної інформаційної системи [2]

Програмна архітектура являє собою сукупність комп'ютерних програм, призначених для рішення конкретних завдань. Даний тип архітектури призначений для опису додатків, що входять до складу інформаційної системи. На даному рівні описують програмні інтерфейси, компоненти й поведінку.

Архітектура даних поєднує в собі як фізичні сховища даних, так і засоби керування даними. Крім того, до неї входять логічні сховища даних, а при орієнтованості розглянутої компанії на роботу зі знаннями, може бути виділений окремий рівень – архітектура знань (Knowledge architecture). На цьому рівні описуються логічні й фізичні моделі даних, визначаються правила цілісності, складаються обмеження для даних.

Слід особливо виділити рівень *IT-архітектури*, оскільки він є сполучним.

На ньому формується базовий набір сервісів, які використовуються як на рівні програмної архітектури, так і на рівні архітектури даних. Якщо будь-яка особливість функціонування для цих двох рівнів не була передбачена, то сильно зростає ймовірність збоїв у роботі, а, отже, втрат для бізнесу. У деяких випадках неможливо розділити IT-архітектуру й архітектуру окремого додатка. Таке можливо при високому ступені інтеграції додатків. Прикладом IT-архітектури може служити SharePoint від Microsoft. Цей продукт надає сервіси для спільної роботи й зберігання інформації, що є дуже важливим аспектом функціонування

будь-якої компанії. Його базові системні модулі відносяться до IT-архітектури, а користувальницькі – до програмного.

Основною функцією IT-архітектури є забезпечення функціонування важливих бізнесів-додатків для досягнення позначених бізнесів-цілей. Якщо деяка функція потрібна відразу в декількох додатках, то її доцільно перенести на рівень IT-архітектури, тим самим підвищивши інтеграцію системи й знизити складність архітектури додатків.

Останнім в ієрархії є *рівень бізнес-архітектури* або *архітектури бізнесів-процесів*. На цьому рівні визначаються стратегії ведення бізнесу, способи керування, принципи організації й ключові процеси, що представляють для бізнесу величезну важливість.

Технологія – комплекс наукових та інженерних знань, втілених в способах і засобах праці, наборах матеріально-речових факторів виробництва, видах їх поєднання для створення певного продукту або послуги [3].

До сучасної технології висуваються наступні вимоги [3]:

високий ступінь поділу процесу на стадії (фази);

системна повнота (цілісність) процесу, який повинен включати весь набір елементів, що забезпечують необхідну завершеність дій людини в досягненні поставленої мети;

регулярність процесу і однозначність його фаз, що дозволяють застосовувати середні величини при охарактеризуванні цих фаз, а отже їх стандартизації і уніфікації;

технологія є нерозривно пов'язаною із процесом – сукупністю дій, які виконуються в часі;

технологічний процес здійснюється в штучних системах, створених для забезпечення реалізації певних потреб.

Зазначені вище властивості визначають характеристики технологічних процесів [3]:

поділ процесу на внутрішні взаємозв'язані стани, фази, операції, що забезпечують оптимальну або близьку до оптимальної динаміку розвитку

процесу, а також визначають раціональні межі вимог до персоналу, що працюватиме з даною технологією;

координування і поетапне виконання дій та операцій, спрямованих на досягнення необхідного результату, причому послідовність дій базується на логіці функціонування і розвитку визначеного процесу;

однозначність виконання наявних в технології процедур і операцій, що є неодмінною і вирішальною умовою досягнення результатів у відповідності з визначеними для цього нормами і нормативами.

Так можна інтерпретувати поняття технології в широкому сенсі. З іншого боку, в більш вузькому сенсі означення технології формулюється наступним чином [3]:

Технологія – це набір способів, засобів вибору і здійснення керуючого процесу з множини можливих його реалізацій.

В основі будь-якого процесу лежить визначена технологія, до компонентів якої відносяться [3]:

мета реалізації процесу;

предмет, що підлягає технологічним змінам;

способи і методи впливу;

засоби технологічного впливу;

впорядкованість і організація, які протиставлені стихійним процесам.

1.2. Аналіз проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи

Сьогодні переважна більшість атак на корпоративні IT-системи здійснюються зловмисниками через використання проломів і вразливостей кінцевих точок – пристроїв, які використовуються кінцевими користувачами: ПК, ноутбуки, планшети, смартфони тощо. Це є логічним та зрозумілим, беручи до уваги факт того як і ким експлуатуються ці пристрої: велика кількість самих пристроїв, багато доступних каналів зв'язку і портів, розмаїття встановленого ПЗ, не надто висока кваліфікація користувачів, низький рівень їх відповідальності

тощо. У результаті кінцеві точки стали найуразливішим місцем будь-якої IT-інфраструктури, через яке здійснюється чотири п’ятих всіх атак, з якими пов’язані майже всі шахрайські дії та ненавмисні події інформаційної безпеки.

Часто, в спробі вирішити проблему, фахівці з кібербезпеки намагаються поза комплексом заходів інформаційної безпеки забезпечити захист кінцевих точок від множини конкретних загроз, встановлюючи на них велике число незалежних агентів: антивірусів, хостових IPS, засобів управління патчами і оновленнями, систем шифрування тощо. Проблема полягає в тому, що вони не працюють як єдина система і вимагають окремих серверів управління, налаштувань профілів і політик, своєчасного оновлення, що є суттєвим навантаженням на адміністративні та обчислювальні ресурси. А їх одночасна робота може приводити до колізій і знижувати стабільність функціонування додатків і операційної системи.

Як зазначається в [4] кінцеві точки користувачів продовжують залишатися постійною проблемою для організацій. Найбільш успішні зломи кінцевих точок пов'язані з людськими чинниками, такими як соціальна інженерія/фішинг, спроби проникнення через Інтернет і програми-вимагачі. Існує можливість заражень через USB-пристрої в якості початкового вектора атаки.

Підкреслюється, що антивірус був найбільш часто використовуваним інструментом для виявлення початкового вектора атаки та тільки 47% атак були виявлені за його допомоги. Інші 32% атак були виявлені за допомогою автоматичних попереджень SIEM і мережевого аналізу, а 26% були виявлені за допомогою платформ EDR (виявлення кінцевих точок і реагування) [4].

Проте, технології виявлення, які відстежують поведінку користувачів і систем або забезпечують обізнаність про контекст, набагато менше брали участь у виявленні порушень. Тільки 23% зломів респондентів були виявлені за допомогою моделювання поведінки атак і тільки 11% зломів за допомогою поведінкової аналітики. Оскільки поведінка користувачів і комп'ютерів є причиною більшості порушень роботи кінцевих точок, ці технології мають вирішальне значення для виявлення кінцевих точок і реагування на них [4].

Однією з проблем є те, що групи безпеки не справляються з задачами з причин коли їх операційний центр безпеки (SOC) завалений такою великою кількістю новітніх інструментів, які б мали скоротити функції кібер-аналітиків, щоб вони могли виконувати аналіз, натомість обмежило їх можливості. для глибокої реалізації або використання доступних опцій [4].

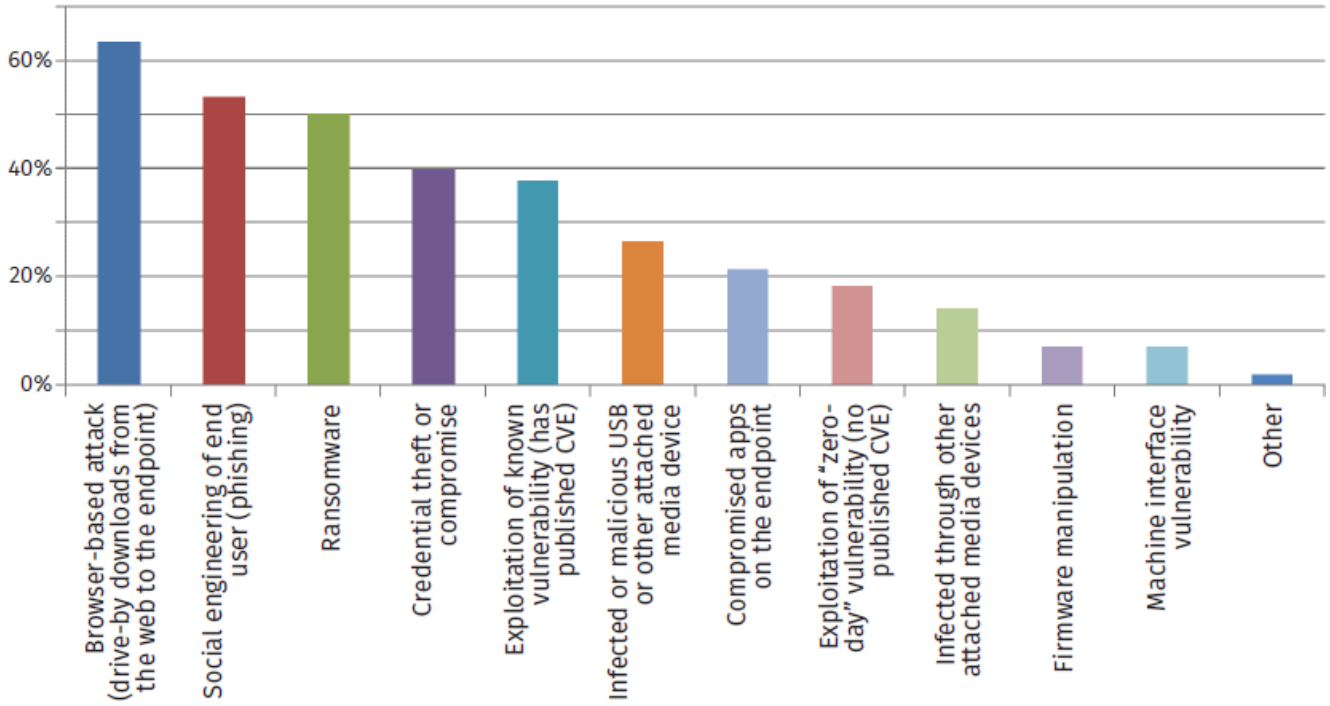

Рис. 1.2. Вектори атак кінцевих точок [4]

Основними векторами атак на кінцеві точки є веб-сервіси (63%), соціальна інженерія (фішинг) (53%) і програми-вимагачі (50%). Крадіжка облікових даних використовувалася в 40% випадків злому (рис. 1.2).

Оскільки основні компрометації залежать від дій користувачів на кінцевих точках, то, відповідно, що операції людини на кінцевій точці повинні контролюватися і стримуватися, а також по можливості треба навчати користувачів. Задля цього треба застосовувати різні інструменти, в тому числі антивірусне програмне забезпечення нового покоління (для виявлення атак без шкідливих програм і файлів) і автоматизований EDR (з антивірусом нового покоління (NGAV), включаючи аналітику поведінки користувачів) [4].

Аналітика загроз кінцевих точок також важлива і повинна автоматично передаватися в системи виявлення та реагування. Це повинно скоротити час на

виявлення, реагування та, в кінцевому підсумку, усунення загрози/вразливості, яку зловмисник намагався використовувати.

Типовий сценарій реагування на інциденти щодо кінцевої точки починається з оповіщення SOC від джерела автоматичного виявлення, що вказує на незвичайну поведінку або дії. Потім аналітик може негайно дослідити цільову кінцеву точку для пошуку будь-яких незвичайних процесів, з'єднань або інших артефактів для попереднього висновку. Якщо це не помилкове спрацьовування, а існує реальна загроза, аналітик ізолює кінцеву точку від доступу до інших кінцевих точок, щоб запобігти поширенню атаки, а також переконатися, що доступ до пов'язаних джерел Інтернету обмежений системою реагування на загрози (відповідь).

Поки фахівець з безпеки визначає джерела і вектори атак, система і будь-які додаткові скомпрометовані вузли виправляються для відновлення роботи. SOC ініціює заходи з блокування джерел зараження, якщо це можливо, і, при необхідності, планується навчання користувачів та виправлення.

За даними [4] 61% респондентів повідомили, що можуть виявити загрозу менш ніж за 24 години, а 46% – за 5 годин. Відповідь займає трохи більше часу, але більшість респондентів (53%) змогли зреагувати за п'ять годин або менше, як показано на рис. 1.3 та 1.4.

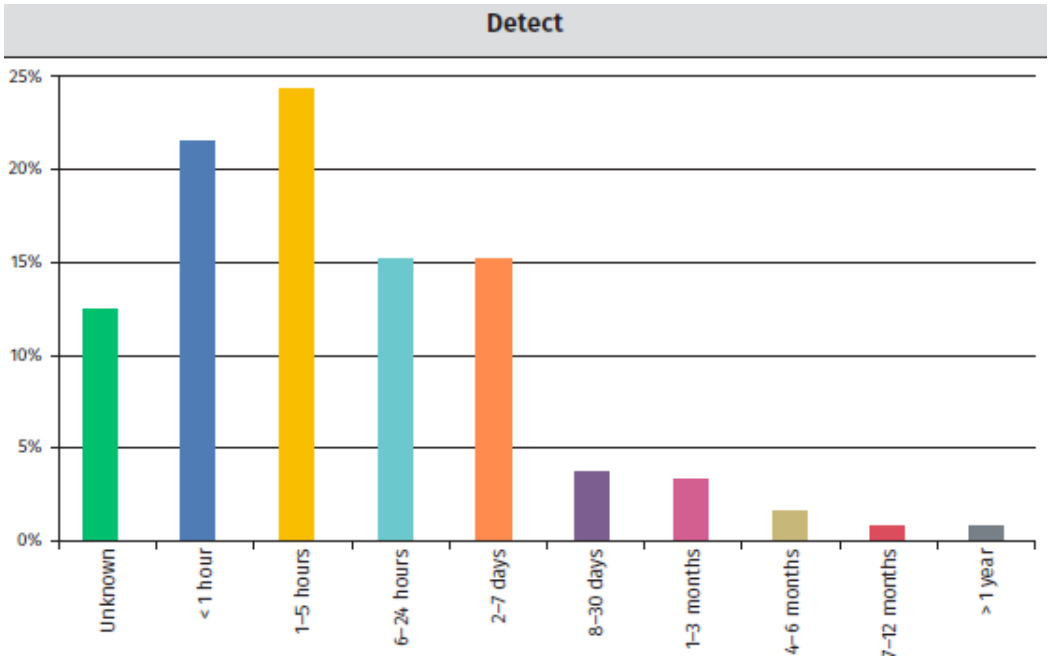

Рис. 1.3. Час виявлення загроз [4]

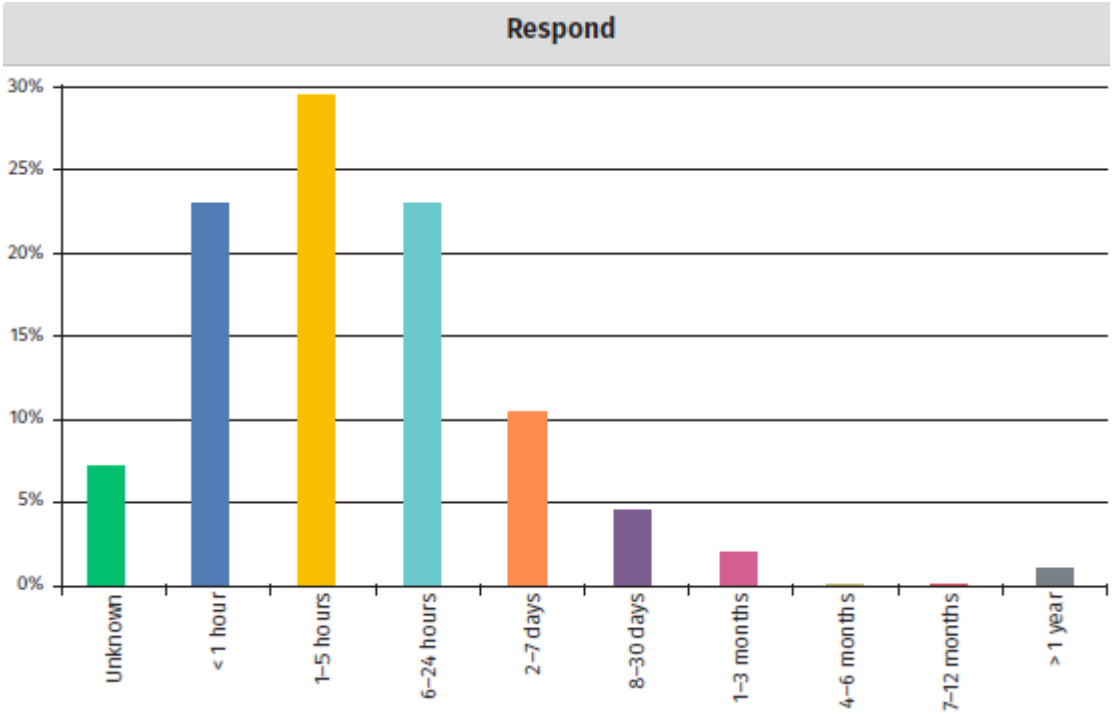

Рис. 1.4. Час реагування на виявлені загрози [4]

Однак, з огляду на те, що 62% респондентів було потрібно до 24 годин, а ще 19% респондентів було потрібно 2-7 днів для виправлення однієї кінцевої точки, все ще існує можливість для подальшого скорочення цього часу. Оскільки зараження поширюється на кінцеві точки за лічені хвилини, час на виявлення та реагування на загрози утворює тривале часове вікно для зловмисників.

Результати [4] показують, що організації використовують ряд технологій і, ймовірно, централізують пошук за допомогою застосування своїх SIEM-систем. У цих випадках SIEM збирає дані про кінцеві точки і мережеві дані, які організації використовують для пошуку подій, пов'язаних з кінцевими точками, аналізуючи їх за допомогою аналітики кінцевих точок і забезпечуючи кореляцію з елементами даних з систем EDR і інших.

32% респондентів повідомили, що *випереджаюче виявлення*, що включає активний запит кінцевої точки, виявляє компрометацію тільки в 10% або менше випадків. Це означає, що виявлення залежить від попереджень від кінцевої точки або мережевого інструменту. Це ще одна область, в якій автоматизація та інтеграція з EDR і іншими платформами оркестровки дозволять значно поліпшити можливості виявлення кінцевих точок і реагування [4].

Приклади попереджувального виявлення включають моделювання поведінки, аналіз загроз і платформи для полювання. Уміння виявляти поведінку атак, а не прості індикатори компрометації, є ключем до *проактивних дій*. Використання Red Team, внутрішнього тестування на проникнення і вивчення поведінки зловмисників – все це допомагає в побудові моделей поведінки.

Коли справа доходить до відстеження артефактів для розслідування компрометації, централізований збір даних охоплює багато ключових елементів, такі як інвентаризація та конфігурація ПЗ, але є прогалини [4]:

найбільша прогалина полягає в виявленні резидентних об'єктів в пам'яті, де не працюють антивірус і традиційні механізми безпеки. Виявлення об'єктів пам'яті – це ключ до виявлення безфайлових шкідливих програм і реагування на них. Респонденти з попередніх опитувань також висловили занепокоєння з приводу відсутності цих артефактів, які самі по собі є ефективним, якщо не найкращим способом проведення аналізу постінфекцій;

виявлення використання конфіденційних даних і відсутність інформації обліку периметру є ключем до розуміння прогалин в охопленні. Такі типи інформації дозволяють зрозуміти, де обробляється інформація, що може викликати занепокоєння, якщо дані були витягнуті. Більш того, коли користувачі звертаються до систем – це ключ до кореляції дій користувача і загроз;

респонденти повідомляють нам, що у них відсутні мережеві дані (між машинного з'єднання і дані протоколу дозволу адрес (ARP)) для кореляції з артефактами кінцевих точок. Така інформація необхідна для отримання повного уявлення про шкідливі програми і про те, як воно використовує або взаємодіє з мережею;

у них також відсутні дані про поведінку користувачів, яких в деяких випадках просто не існує. Такі дані необхідні організаціям для кореляції і належного визначення базових показників. З появою хмарних сервісів організаціям необхідно забезпечити наявність аналогічних сервісів збору даних і переконатися, що дані включені в централізований збір даних.

Щоб переломити ситуацію, організації повинні визначити, встановити й

налаштувати ефективні рішення, а також встановити базові показники. Ключовими факторами успіху, зазначеними респондентами, є простота збору даних (49%), зіставлення даних з корисною інформацією (47%), досвідчені оператори (46%) і сумісність автоматизації / інструментів (43%) [4].

Головний бар'єр – це бюджетна і управлінська підтримка (47%), за якими слід відсутність автоматизації / взаємодії інструментів (43%) і знаходження навичок, необхідних для роботи з інструментами (40%) [4].

З цих результатів ясно, що, крім придбання інструментів, що забезпечують автоматизацію і функціональну сумісність, організаціям необхідно залучити персонал, необхідний для роботи і використання своїх інструментів, або за рахунок виділення ресурсів, або за рахунок зменшення складності наборів інструментів, з якими аналітики повинні безпосередньо взаємодіяти [4].

Аналіз і консолідація. Коли справа доходить до аналізу і консолідації даних кінцевих точок, 63% респондентів заявили, що їх основним інструментом є SIEM, за якими слідують 46%, які вважають за краще платформу централізованого управління журналами [4].

На жаль, 33% аналізу і консолідації даних як і раніше включає ручний пошук з використанням розрізнених інструментів безпеки, аналітики і платформи. Використання централізованого інтерфейсу управління системою EDR слід на 32%. Тому важливо, щоб рішення EDR забезпечували надійну двосторонню інтеграцію API в додатку SIEM, щоб аналітики могли використовувати єдиний інтерфейс для користувачів в кращому додатку [4].

В цілому 57% досягли певного рівня автоматизації; в порівнянні з 52% в 2017 році, тоді як 38% як і раніше покладаються на ручні процеси. Автоматизація являє собою шлях до скорочення часу відгуку, а також до більш швидкому поверненню користувачів в мережу. Це також сприяє узгодженості відповідей і вивільняє ресурси, необхідні для роботи зі зрослим різноманітністю і кількістю пристроїв в корпоративній екосистемі [4].

Перевірка виправлення. З усіх етапів виправлення виявлення порушень з використанням відомих індикаторів компрометації є найменш важким для

респондентів (58%), після чого слід видалення всіх шкідливих артефактів на кінцевих точках (що підкреслює заклик до стирання і повторного створення образу, як зазначено раніше). Найскладнішими завданнями виправлення були визначення того, які дані були порушені на зламаних кінцевих точках, вибраних 71%, з подальшим визначенням масштабу загрози на кількох кінцевих точках, обраними 68%. Відносно висока частота атак програм-вимагачів вказує на необхідність виправлення порушених даних. Для цього потрібна здатність виявляти змінені дані і наявність відомих хороших копій цих даних, досить свіжих, щоб мати мінімальний вплив на бізнес при установці [4].

Практики і можливості нового покоління. Відрадно відзначити, що 65% респондентів використовують технології захисту і шифрування даних, які є ключовими інструментами для ефективного відновлення. Оцінка вразливостей і засоби контролю додатків використовуються в 63% організацій, при цьому 59% використовують панелі централізованого управління, а 54% використовують аналітику кіберзагроз. У чому респонденти, схоже, не справляються, так це в автоматизації робочих процесів і штучному інтелекті (AI)/машинному навчанні, які є ключовими інструментами для поліпшення виявлення, виправлення і реагування, але їх використовують тільки 25% і 21% відповідно [4].

В цілому 58% вказали, що автоматизовані робочі процеси реагування/усунення інцидентів і штучний інтелект/машинне навчання важливі, але вони ще не впровадили ці технології.

Як згадувалося раніше, наявність автоматичних відповідей разом з автоматичним викликом робочого процесу є ключем до ефективного і своєчасного реагування на інциденти. Крім того, без використання автоматизації для виявлення тенденцій і побудови моделей вже перевантажені роботою аналітики повинні вручну виконувати ці обов'язки, а не просто уточнювати результати і мінімізувати або виключати помилкові спрацьовування або негативні результати. Нарешті, коли аналітикам доводиться приділяти увагу великої кількості попереджень, пов'язаний з цим брак часу на аналіз означає, що аналіз першопричин не може бути успішно завершений. Без докладної інформації про

те, як була зламана організація, неможливо отримати корпоративні знання і / або розвіддані про тактику, методи та процедури зловмисників [4].

Організаціям необхідно створити генеральний план або дорожню карту, щоб інтегрувати інструменти, які у них вже є, і розставити пріоритети у витратах, щоб заповнити прогалини. Вони повинні розставити пріоритети у витратах на сучасні можливості виявлення та реагування, що використовують машинне навчання, при цьому намагаючись не схилити чашу терезів і не погіршити здатність аналітиків безпеки убезпечити організацію, додавши занадто багато розрізнених інструментів, які послаблюють їх увагу дані.

Як висновок, основними загрозами для організацій як і раніше є шкідливі програми в Інтернеті, соціальна інженерія та програми-вимагачі, які націлені на кінцеві точки користувачів.

Організації повинні розширити свої можливості, щоб більш активно захищати свої системи і виявляти загрози на більш ранніх етапах ланцюжка кібератак. Їм також необхідно централізовані АРМ для адміністрування безпеки кінцевих точок, у тому числі навіть для кінцевих точок в хмарі. Результати показують деяку плутанину щодо того, чи становлять SIEM, EDR або навіть системи управління журналами цю централізовану можливість. Без центральної точки для аналізу діяльності, пов'язаної з кінцевими точками (включаючи дані, пов'язані з мережею), автоматизація відійде на другий план.

В кінцевому підсумку мета захисту кінцевих точок є скорочення середнього часу на виявлення, реагування та стримування шкідливого ПЗ. Досягнення цієї мети допоможе організаціям рухатися до бізнес-цілей на відповідних рівнях ресурсів, замість того, щоб витрачати час на очищення і повторне відображення кінцевих точок або виконання інших дій, які негативно впливають на життєздатність бізнесу.

1.3. Мета та завдання управління захистом кінцевих точок корпоративної інформаційної системи

У [5] зазначаються три ключові елементи, які впливають на стійкість в

кіберпросторі: гнучкість системи, зменшення поверхні для атак і динамічне реагування на атаки.

Гнучкість в конфлікті кіберпростору в значній мірі буде виникати з створення гнучких людей, хоча хороший дизайн мережі, який дає гнучким операторам кіберпростору більше можливостей, також допоможе. Гнучкість систем кіберпростору буде витратною, а ефективність буде знижена через необхідну надлишкову потужність, яка повинна бути вбудована в більш гнучку систему. Гнучка система кіберпростору також є різнорідною і розбита на захищені анклави, а не в одну велику і просту в адмініструванні мережу, в якій на кожному пристрої працює одне і те ж програмне забезпечення. Персонал гнучкого кіберпростору найкраще росте за допомогою великого навчання і вправ, які включають в себе об'єднання в червоні команди, повномасштабні вправи з грою в кіберпросторі, що дозволяють впливати на фізичні домени і підзвітність для користувачів, які виявилися нездатними прийняти хороші методи безпеки. Багато з цих змін буде дуже важко реалізувати, оскільки вони будуть вкрай незручні для організацій і зажадають значних культурних змін [5].

Зменшення поверхонь для атак – другий елемент забезпечення стійкості кіберпростору.

Першим і надзвичайно важким кроком є усунення непотрібних можливостей в мережі, як програмних, так і апаратних. Користувачі будуть збиті з пантелику тим, що їм доведеться використовувати інструменти, відмінні від тих, до яких вони звикли, але виграш в безпеці може бути значним. Не всяку систему резервного копіювання слід усувати, всюди, де це можливо, повинна бути доступна основна і резервна система для кожної ключової області місії, щоб оператори кіберпростору могли швидко перемикатися з однієї системи на іншу в разі виявлення вразливостей. Прагнення користувача до постійного швидкому вдосконаленню зв'язку і можливостей також має бути збалансовано з вимогами безпеки, оскільки кожна нова можливість або канал зв'язку вводить потенційний вектор атаки. Досягнення правильного балансу між безпекою та можливостями буде складною і постійним завданням, і правильний баланс буде змінюватися в

залежності від організації і середовища, в якій вона працює [5].

Останній елемент стійкості кіберпростору – це здатність динамічно реагувати на атаки. Операторам кіберпростору необхідно поліпшити ситуаційну обізнаність про свої власні мережах і розвинути розвідувальні можливості, щоб зрозуміти, що планує зловмисник. Зловмисникам і захисникам на одній стороні також необхідно знизити бар'єри між ними і обмінюватися додатковою інформацією, щоб захисники кіберпростору могли краще захищати свої мережі, одночасно захищаючи можливості настання. Ефективне управління і контроль в кіберпросторі, при якому оператори кіберпростору розглядаються як маневрені сили, якими потрібно командувати, в порівнянні з проблемою управління IT за допомогою інженерного рішення. Активний захист, включаючи зломи, мережі honeypot, резервне копіювання, режими військового резервування та обладнання для резервного копіювання, сприяє стійкості кіберпростору.

Щоб організація могла створити стійку стійкість кіберпростору, будуть потрібні деякі аспекти всіх трьох елементів, і створення стійкості кіберпростору буде недешево. Додаткові витрати, понесені тільки на резервування та навчання, перевершать будь-яку потенційну економію від оптимізації і скорочення надлишкових потужностей.

Однак, якщо організація серйозно ставиться до захисту своєї здатності виконувати свою місію в кіберпросторі, стійкість до атак буде ключовим фактором [5].

1.4. Аналіз існуючих технологій управління захистом кінцевих точок корпоративної інформаційної системи

Платформа захисту кінцевих точок (EPP) – це рішення, яке розгортається на кінцевих пристроях для запобігання атак шкідливих програм на основі файлів, виявлення шкідливої активності і надання можливостей розслідування і виправлення, необхідних для реагування на динамічні інциденти безпеки і попередження.

Можливості виявлення будуть різними, але в передових рішеннях будуть

використовуватися кілька методів виявлення, від статичних IoC до поведінкового аналізу. Деякі рішення EPP в основному управляються хмарою, що дозволяє здійснювати безперервний моніторинг і збір даних про активність, а також можливість приймати віддалені заходи щодо виправлення становища, незалежно від того, чи знаходиться кінцева точка в корпоративній мережі або за межами офісу. Крім того, в цих рішеннях використовуються хмарні дані, що означає, що агенту кінцевої точки не потрібно підтримувати локальну базу даних з усіма відомими IoC, але він може перевіряти хмарний ресурс, щоб знайти останні вердикти по об'єктах, які він не може класифікувати.

У [6] зазначається, що дуже часто атаки на кінцеві точки йдуть через експлуатацію вразливостей в системному і прикладному програмному забезпеченні. Починаючи від атак на вразливості браузерів, коли користувач завантажує заражену веб-сторінку, і закінчуючи доставкою шкідливого корисного навантаження на кінцеву точку через уразливості мережевих протоколів і операційних систем.

В цьому випадку недостатньо просто перехоплювати і аналізувати заражений файл – необхідно забезпечувати захист мережевих з'єднань, аналізуючи мережевий трафік, що приходить і виходить з кінцевої точки. В рамках такого підходу до функціональності класичного антивіруса додаються технології мережевого захисту, такі як міжмережевий екран, система запобігання вторгнень і система контролю підключаються до кінцевої станції пристроїв. Саме з цього моменту формується новий тип продуктів – платформа захисту кінцевих точок, або Endpoint Protection Platform (EPP).

Endpoint Protection Platform – це система комплексного захисту кінцевої точки, що включає в себе як класичну функціональність антивірусного захисту, так і розширені технології безпеки – персональні міжмережеві екрани, системи запобігання вторгнень, системи контролю портів і пристроїв, що підключаються, системи шифрування дисків та ін. З певного моменту більшість EPP-рішень перестали задовольняти сучасним вимогам до безпеки кінцевих станцій. В першу чергу це було пов'язано з ростом цілеспрямованих атак, які в основному

використовують уразливості нульового дня і відрізняються масовістю завдяки використанню ботнетів і внутрішньої архітектури горизонтального поширення.

Також необхідно відзначити окремий клас загроз – кріптолокерів (або шифрувальників), які в принципі, з точки зору системного програмного забезпечення, не роблять нічого протиправного. Відмінною рисою всіх цих атак є те, що вони не використовують відомі підходи і проломи, а експлуатують ще невідомі вразливості і способи свого поширення. Безумовно, EPP-рішення були змушені еволюціонувати, щоб відповідати сучасним викликам в сфері захисту кінцевих точок. Підсумком такого еволюційного розвитку стала поява нових систем, об'єднаних під загальною назвою NGEPP.

NGEPP (Next Generation Endpoint Protection Platform) – це системи захисту кінцевих станцій, які крім базової функціональності класичного антивіруса, захисту мережі та контролю портів володіють розширеними функціями для боротьби з сучасними загрозами. Додатковими системами, що розширюють можливості класичних EPP-систем, можуть бути [6]:

системи емуляції проходять файлів в пісочниці (sandboxing) для боротьби з загрозами нульового дня;

системи Anti-Bot для боротьби з ботнетами, засновані на аналізі патернів трафіку і визначення в них бот-активності;

EDR-системи (Endpoint Detect and Response) – системи реактивної захисту кінцевих точок, що відповідають за розслідування інцидентів шкідливої активності і подальшого відновлення системи;

системи контролю додатків, які відповідають за блокування недовірених додатків (у тому числі на основі поведінкової аналітики), не дозволяючи останнім впливати на основні процеси та критичні дані;

системи захисту пам'яті, проактивно блокують підозрілу активність при зверненні додатків до оперативної пам'яті;

системи захисту даних, що включають в себе системи резервного копіювання, системи шифрування даних, системи запобігання витокам і системи боротьби з фішингом.

В [6] виділяють такі еволюційні напрямки розвитку EPP-систем:

розвиток класичних антивірусних рішень;

розширення функціональності NGFW (Next Generation Firewall) на кінцеві точки користувачів;

окремі рішення, які використовують нестандартні та унікальні підходи до забезпечення безпеки кінцевих мочок.

Розвиток класичних антивірусних рішень. Цей клас EPP-рішень є прямим нащадком перших антивірусів. І якщо раніше антивірусні виробники боролися в основному за повноту і обсяг сигнатурних баз, то сьогодні боротьба розгортається вже за зручність користування, вбудовані механізми самозахисту і стійкість до технік обходу і новим загрозам. Відмінною особливістю таких систем є наявність як корпоративних рішень з виділеної системою управління і звітності, так і рішень для захисту домашніх комп'ютерів користувачів і мобільних пристроїв, з підтримкою практично всієї Enterprise-функціональності [6].

До представників цього класу EPP-рішень можна віднести TrendMicro Smart Protection Suites, ESET Endpoint Protection, Symantec Endpoint Protection, Dr.Web Enterprise Security Suite та ін.

Розширення функціональності NGFW (Next Generation Firewall) на кінцеві точки користувачів. В рамках комплексного підходу до забезпечення мережевої безпеки виробники NGFW були змушені створювати рішення для захисту кінцевих точок, щоб забезпечити більшу видимість і не допустити розмиття периметра безпеки, особливо в організаціях, що використовують BYOD-підхід. Маючи значний досвід в комплексній мережевій безпеці, виробники NGFW випускають досить конкурентні рішення, багато з яких по праву можна назвати NGEPP.

Зазвичай рішення таких виробників представлені виключно в корпоративному сегменті. До найвідоміших представників цього класу EPP-рішень можна віднести: Check Point Endpoint Security, Fortinet FortiClient, Palo Alto Networks Traps і ін.

Окремі рішення, які використовують нестандартні та унікальні підходи до

забезпечення безпеки кінцевих точок. Класичний підхід інтеграції множини функцій захисту кінцевих точок в одному продукті не завжди є єдино можливим. На доказ цього на ринку EPP стали з'являтися рішення, які виходять за рамки класичної парадигми захисту кінцевих точок, але при цьому можуть скласти конкуренцію піонерам цього ринку.

Яскравим прикладом таких систем можна вважати продукт Cylance PROTECT, який використовує алгоритми машинного навчання для боротьби з відомими і невідомими загрозами, при цьому не вимагаючи регулярних оновлень і не використовуючи сигнатурний підхід.

Ще один приклад нестандартного підходу – рішення BufferZone, що відповідає тільки за контейнерування (запуск в ізольованому системному оточенні) всіх недовірених додатків, таким чином захищаючи системні файли і критичні дані без як такого аналізу активності додатків.

Розглянемо можливості рішень деяких лідерів ринку EPP.

Falcon - це платформа CrowdStrike, спеціально створена для запобігання зломів за допомогою єдиного набору хмарних технологій, які запобігають всі типи атак, включаючи шкідливе ПЗ і багато іншого. Сучасні витончені зловмисники виходять «за рамки шкідливих програм», щоб зламати організації, все більше покладаючись на експлойти, нульові дні і важко виявляються методи, такі як крадіжка облікових даних, і інструменти, які вже є частиною середовища або операційної системи жертви, наприклад PowerShell. CrowdStrike Falcon вирішує ці проблеми за допомогою потужного, але легкого рішення, яке об'єднує антивірус нового покоління (NGAV), виявлення та реагування на кінцеві точки (EDR), аналітику кіберзагроз, можливості керованого пошуку загроз і гігієну безпеки – все це в крихітному, єдиному, легкий датчик з хмарним керуванням і доставкою [8].

Примітна архітектура рішення *Falcon Endpoint Protection (CrowdStrike)*, яка будується на двох сутностях – агенті, що встановлюється на робочій станції і хмарній платформі, що відповідає за розширення функціональності агента за допомогою хмарних додатків (від NGAV до Threat Intelligence і Sandboxing),

управління агентами і надання API для сторонньої інтеграції.

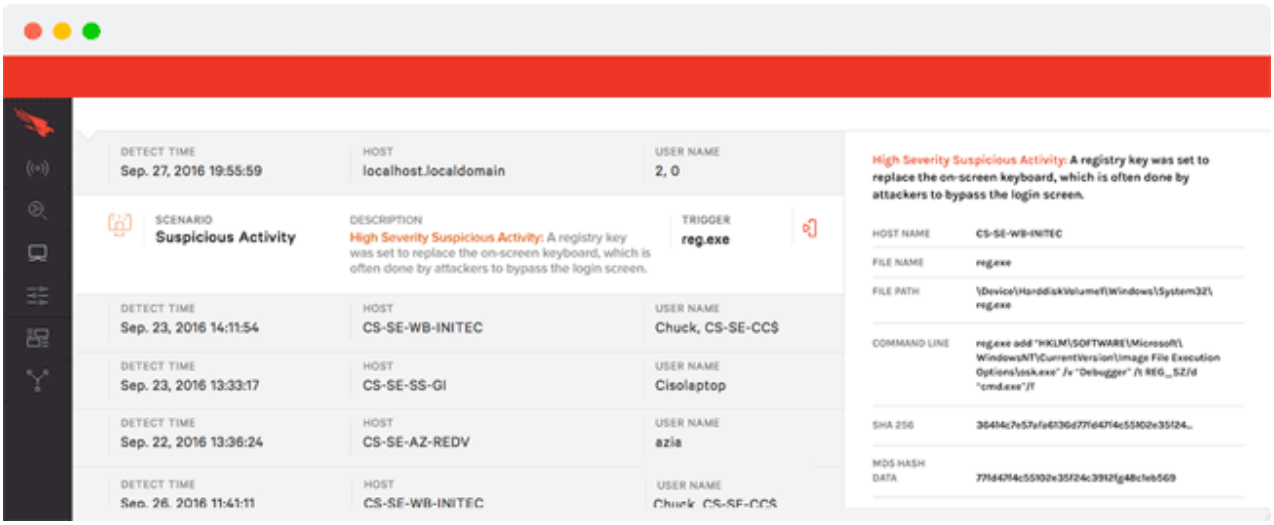

Рис. 1.5. Консоль управління CrowdStrike Falcon

Відмінною рисою рішення (рис. 1.5), безумовно, є cloud-delivered-підхід до захисту кінцевих точок. Також варто окремо відзначити платформу CrowdStrike Threat Graph, яка відповідає за збір даних про атаки, їх збагачення з зовнішніх джерел і індикаторів компрометації (IoC), подальший аналіз із застосуванням технологій машинного навчання і поведінкової аналітики і створення індикаторів атак (IoA), які в подальшому поширюються на кінцеві точки. За рахунок такого підходу компанія значно знижує обсяг і частоту оновлень інформації на агентах, встановлених на кінцевих точках.

Trend Micro Smart Protection Suites.

Ландшафт загроз постійно змінюється, і традиційні рішення безпеки не встигають за ними. Використання декількох точкових продуктів на одній кінцевій точці призводить до того, що занадто багато продуктів не працюють разом, збільшує складність, уповільнює роботу користувачів і залишає прогалини у вашій безпеки. Ще більше ускладнює ситуацію те, що ви переходите в хмару і потребуєте гнучких інструкції з розгортання безпеки, які будуть адаптуватися в міру зміни ваших потреб.

На сьогоднішній день відсутнє рішення, яка зупинить всі виникаючі сьогодні загрози. Вам потрібна інтелектуальна безпеку, яка використовує правильні методи для кожного типу загроз, які не сповільнюючи вас. Безпека, пов'язана з використанням декількох рівнів для запобігання виникаючих загроз і

скорочення накладних витрат на управління.

Продукти для захисту кінцевих точок поставляються в двох комплектаціях Smart Protection for Endpoints Suite і Smart Protection Complete Suite. Обидві комплектації включають в себе централізовану систему управління Trend Micro Control Manager і платформу для захисту кінцевих точок, що включає всі компоненти, властиві NGEPP [9].

У комплекті Smart Protection Complete Suite додатково передбачені можливості захисту поштових серверів, серверів спільної роботи і інтернет-шлюзів. Всі рішення доступні як для десктопних операційних систем (Windows, macOS, Linux), так і для мобільних платформ iOS, Android, Blackberry і Windows Mobile.

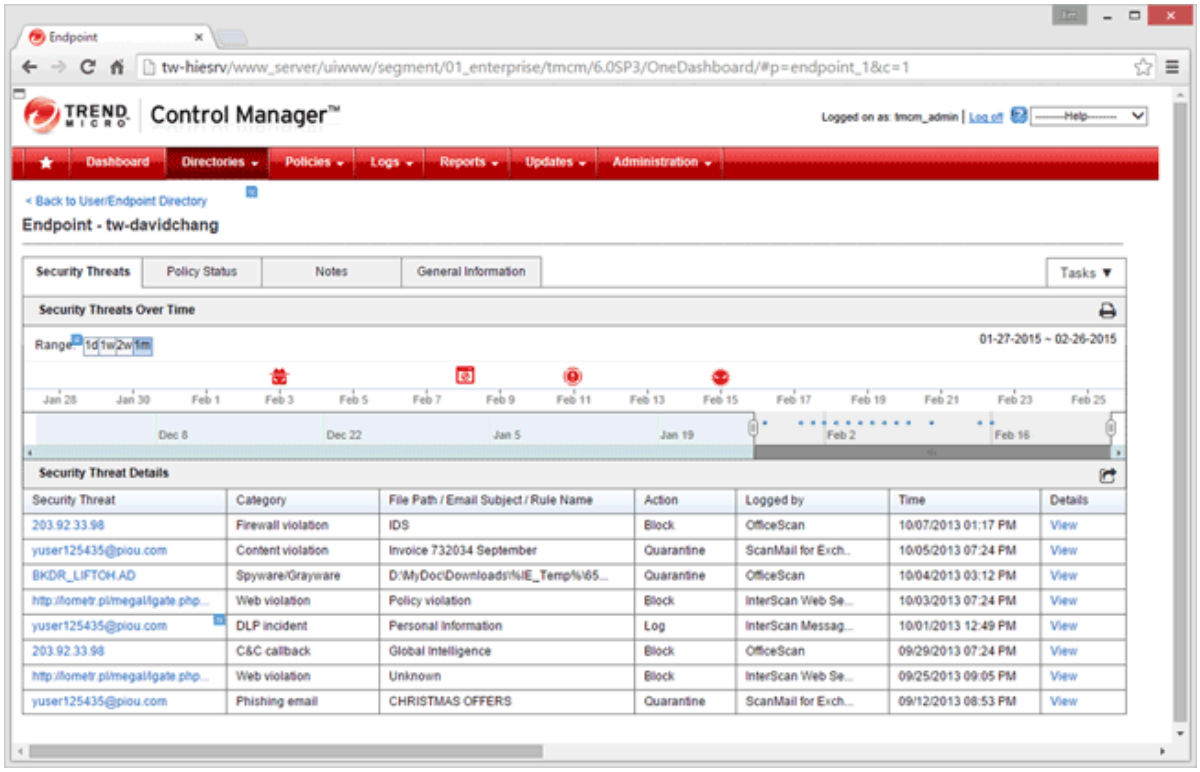

Рис. 1.6. Консоль управління Trend Micro Control Manager

Відмінною особливістю рішень Trend Micro є те, що компанія однією з перших додала в свої продукти механізми високоточного машинного навчання, які включають аналіз файлів до і після запуску. Комплекс розширених технологій для визначення заражених файлів отримав назву XGen Endpoint Security і, крім машинного навчання, включає в себе технології контролю додатків, захисту від експлойтів і поведінкової аналітики.

Traps (Palo Alto Networks). Кібератаки – це атаки, що здійснюються в мережах або кінцевих точках для нанесення шкоди, крадіжки інформації або досягнення інших цілей, які включають в себе отримання контролю над комп'ютерними системами, які не належать зловмисникам. Зловмисники роблять кібератаки, змушуючи користувача ненавмисно запустити шкідливий виконуваний файл або використовуючи уразливість в легітимному виконуваному файлі для запуску шкідливого коду за лаштунками без відома користувача [10].

Один із способів запобігти цим атакам є визначити виконувані файли, бібліотеки з динамічної компонуванням (DLL) або інші фрагменти коду як шкідливі, а потім запобігти їх виконання, протестувавши кожен потенційно небезпечний модуль коду за списком конкретних відомих сигнатур загроз. Слабкість цього методу полягає в тому, що антивірусні рішення на основі сигнатур (AV) вимагають багато часу для виявлення новостворених загроз, відомих тільки зловмисникові (також відомих як атаки нульового дня або експлойти), і додавання їх до списків. відомих загроз, в результаті чого кінцеві точки залишаються уразливими до оновлення сигнатур [10].

Рішення Traps використовує більш ефективний і дієвий підхід до запобігання атак, тим самим усуваючи необхідність в традиційному AV. Замість того, щоб намагатися йти в ногу з постійно зростаючим списком відомих загроз, Traps встановлює серію блокпостів, які запобігають атаки в їх початкових точках входу – тій точці, де законні виконувані файли збираються несвідомо дозволити зловмисний доступ до системи [10].

Traps націлений на вразливості програмного забезпечення в процесах, які відкривають невиконувані файли за допомогою методів запобігання експлойтів. Traps також використовує методи запобігання шкідливих програм для запобігання запуску шкідливих виконуваних файлів. Використовуючи цей подвійний підхід, рішення Traps може запобігати всі типи атак, будь то відомі або невідомі загрози.

Всі аспекти налаштувань безпеки кінцевих точок – кінцеві точки і групи, до яких використовуватимуться, додатки, які вони захищають, певні правила, обмеження і дії – все це легко налаштовується. Це дозволяє кожній організації

адаптувати пастки до своїх потреб, щоб пастки могли забезпечити максимальний захист з мінімальним порушенням повсякденній діяльності [10].

Traps архітектурно схожий з іншими представниками ринку EPP – рішення складається з легкого агента для кінцевих точок і хмарної платформи для аналізу загроз. Крім класичної функціональності EPP, в продукт вбудовані інші технології, такі як Machine Learning, захист від кріптолокерів, контроль запуску дочірніх процесів і блокування різних скриптів всередині документів. Крім цього, агент дозволяє відправляти файли на перевірку як в локальну, так і хмарну пісочницю Wildfire.

Рис. 1.7. Консоль управления Palo Alto Networks Endpoint Security Management (ESM)

Відмінною рисою Traps є глибока інтеграція з пісочницею Palo Alto Networks WildFire і формування усіма замовниками глобальної бази індикаторів роботи шкідливого коду за допомогою алгоритмів машинного навчання і штучного інтелекту, за рахунок чого наповнюється аналітичне ядро Traps, а також поповнюється Threat Intelligence база на мережевій платформі NGFW.

Таким чином, кінцеві точки як були, так і залишаються одним з основних джерел загроз кібербезпеці. При цьому технології їх захисту еволюціонують

разом з техніками зловмисників. Все більше рішень класу [NG] EPP використовують в своїх аналітичних двигунах системи роботи з великими масивами даних, системи машинного навчання і нейронні мережі. Це веде до зменшення ролі класичних сигнатурних, евристичних і навіть поведінкових технік і сприяє розвитку хмарних рішень з мінімальною агентською присутністю безпосередньо на кінцевій точці.

При цьому класичні виробники антивірусних рішень не відстають від своїх конкурентів-новачків, і на базі накопиченого досвіду і знайдених вразливостей формують свої експертні системи, які не поступаються за рівнем аналітикою загроз. Всі без винятку рішення прагнуть блокувати ще не відомі на сьогоднішній день загрози і переходять від вузького file-centric-підходу до виявлення та запобігання більш складних механізмів спрямованих атак [6].

Рішення для захисту кінцевих точок, які не зможуть еволюціонувати і відповідати статусу NGEPP, швидше за все перестануть існувати в найближчій перспективі просто тому, що не зможуть повноцінно протистояти сучасним атакам на кінцеві точки, які можна визначити лише безсігнатурними механізмами детектування і захисту.

Таке розмаїття застосовуваних технологій кібербезпеки актуалізує проблему управління захистом кінцевих точок корпоративної інформаційної системи.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК НА БАЗІ HCL BIGFIX

Рішення EPP HCL BigFix є надійним продуктом для захисту від шкідливих програм, а також має широкі можливості виявлення і реагування, які можуть задовольнити потреби безпеки масового ринку та є надійним, ефективним і доцільним вибором.

2.1. Обґрунтування необхідності дослідження можливостей платформи HCL BigFix

У [7] зазначається, що коли системи управління кінцевими точками ефективно інтегровані з інструментами безпеки та IT-операцій, вони грають важливу роль в підтвердженні відповідності, запобігання загрозам, консолідації інструментів і захисту організацій.

Оскільки в більшості кібератак використовуються відомі вразливості, IT-оператори та служби безпеки повинні співпрацювати, щоб швидко усувати ризики безпеки, які загрожують організації.

Управління виправленнями, конфігурація безпеки і відповідність вимогам, поширення програмного забезпечення та інвентаризація – це основні можливості IT-інфраструктури, які повинні взаємодіяти з іншими операціями IT і набором інструментів безпеки. Необхідно розглянути BigFix через його можливості управління кінцевими точками і здатності легко інтегруватися з іншими інструментами IT і безпеки, допомоги групам IT-операцій і безпеки більш ефективно співпрацювати.

Кінцеві точки являють собою операційний механізм, який дозволяє сучасним працівникам виконувати свої обовязки. Порушення роботи цих систем впливає як на індивідуальну продуктивність, так і на взаємодію команд, сповільнюючи спільні бізнес-операції. Основною причиною збоїв в роботі систем сьогодні є атаки, пов'язані з безпекою, які впливають на роботу всієї системи і

призводять до зниження продуктивності.

Сучасні атаки часто використовують відомі вразливості в програмному забезпеченні, для яких вже існують виправлення та дії щодо виправлення.

Невірно сконфігуровані системи також надають можливості для атаки. Організації можуть запобігти кібератакам і витоку даних, постійно оновлюючи виправлення для операційної системи і додатків, а також впроваджуючи управління конфігурацією для забезпечення дотримання стандартних правил безпеки. Тому IT-командам потрібно безперервний і точний облік всіх кінцевих точок, програмного забезпечення і деталей конфігурації в своєму середовищі. Використовуючи цю інвентаризацію, IT-групи можуть гарантувати, що ці системи підтримуються в актуальному стані з використанням останніх виправлень для ОС і додатків, відповідність ліцензійним і нормативним вимогам і правильно налаштовані [7].

Оскільки групи безпеки зазвичай несуть відповідальність за виявлення вразливостей, а групи IT-операцій – за виправлення, ефективна співпраця між цими групами є обов'язковою умовою безперервності бізнесу. Правильно реалізована *система управління кінцевими точками* може надати платформу для спільної роботи як для IT-операцій, так і для забезпечення безпеки, що підвищує загальну безпеку. Для цього ці рішення повинні бути комплексними, гнучкими і інтегрованими з IT-інфраструктурою та інфраструктурою безпеки. Вони повинні забезпечувати швидке і послідовне усунення загроз на всіх кінцевих точках, безперервно перевіряючи, що все кінцеві точки виправлені і відповідають вимогам [7].

Розглянемо проблеми, пов'язані з управлінням кінцевими точками т а визначимо основні його функції.

У [7] підкреслюється, що захисту периметра вже недостатньо та самі кінцеві точки тепер є частиною поверхні атаки. У зв'язку з постійно зростаючою поверхнею атак, включаючи нові типи кінцевих точок, серверів, пристроїв і додатків, IT-команди з усіх сил намагаються не відставати від управління конфігурацією, виправленнями та відповідністю вимогам. Ця проблема збільшує

ризик компрометації через виявлені вразливості в незахищених і неправильно налаштованих системах. Своєчасне внесення виправлень має вирішальне значення, щоб випереджати зловмисників.

Без ефективної стратегії і процесу управління кінцевими точками організаціям не вдасться захистити своє середовище. У міру того, як групи безпеки все частіше використовують інструменти виявлення загроз і реагування, обсяг роботи, необхідної для усунення виявлених загроз, непомірно великий для багатьох IT-організацій. Наприклад, коли випускаються CVE, командам безпеки спочатку необхідно оцінити рівень ризику, визначивши, скільки систем порушено, і пріорітезувати дії по виправленню, виходячи із серйозності вразливості або загрози. Усунення загроз – це «незапланована» робота для більшості IT-груп, яка часто створює зростаюче число незавершених проектів розширення IT-інфраструктури через відволікання уваги, створюваного усуненням загроз. Питання «як виправити те, що ми знаходимо?» сьогодні надто поширене [7].

Роумінг кінцевих точок і хмарних кінцевих точок не видно для багатьох систем управління кінцевими точками, що створює зростаючу проблему управління ними [7]. Хоча рішення для управління мобільними пристроями пропонують деякі необхідні можливості, лише деякі з них мають масштабованість, необхідну для ефективного управління кінцевими точками, незалежно від того, в якій операційній системі вони працюють, де вони розташовані або як вони підключені.

Забезпечення того, щоб інструменти безпеки були встановлені, актуальні і активні, критично важливо для захисту інфраструктури. Однак постійний моніторинг і автоматичне виправлення систем – завдання непросте, особливо з урахуванням сьогоднішніх високомобільних співробітників.

Управління відповідністю вимагає прозорості конфігурації кінцевих точок і інвентаризації програмного забезпечення. Зі зростаючою різноманітністю кінцевих точок цей рівень консолідованої видимості в кращому випадку є складним завданням [7].

Своєчасне усунення вразливостей безпеки і конфігурації може стати відмінністю скомпрометованої системи від неушкодженої. Коли інструменти безпеки виявляють проблеми, інтеграція з інструментами EMS стає критично важливою для швидкого визначення пріоритетів і усунення вразливостей. Проте, деякі організації інтегрували ці інструменти, що призвело до скорочення часу відновлення.

Зараз все частіше вимагають перевірки відповідності систем та програмного забезпечення певним галузевим нормам. Compliance (відповідність вимогам регуляторів) занадто часто сприймається як подія. Організаціям буде краще перевіряти відповідність на постійній і безперервній основі [7].

Звітність про перевірку відповідності вищому керівництву та аудиторам може бути складним завданням без інструментів безперервного моніторингу. Крім відстеження, аналізу та складання звітів про поточний статус дій по установці виправлень на всіх кінцевих точках, IT-організаціям необхідно відстежувати історію відповідності у вигляді загального відсотка – значимого показника для вимірювання прогресу зусиль щодо забезпечення відповідності в часі.

На думку Enterprise Strategy Group [7] необхідно реалізувати *сім можливостей* управління кінцевими точками (рис. 2.1.), які нададуть допомогу відділам експлуатації та безпеки отримати необхідну прозорість, зупинити загрози і підтвердити відповідність вимогам, при цьому всі інструменти мають бути консолідованими:

1. Всебічна видимість:

швидке і безперервне виявлення кінцевих точок і точна інвентаризація програмного забезпечення і конфігурації;

легка візуалізація звітності з історичними тенденціями (відповідність, інвентаризація і відхилення);

виявлення дрейфу і оповіщення.

2. Легкість керування:

надійне і послідовне поширення програмного забезпечення;

швидке і надійне виправлення з високим відсотком успіху з першого проходу;

оновлення конфігурації і перевірка;

автоматизоване забезпечення програмного забезпечення.

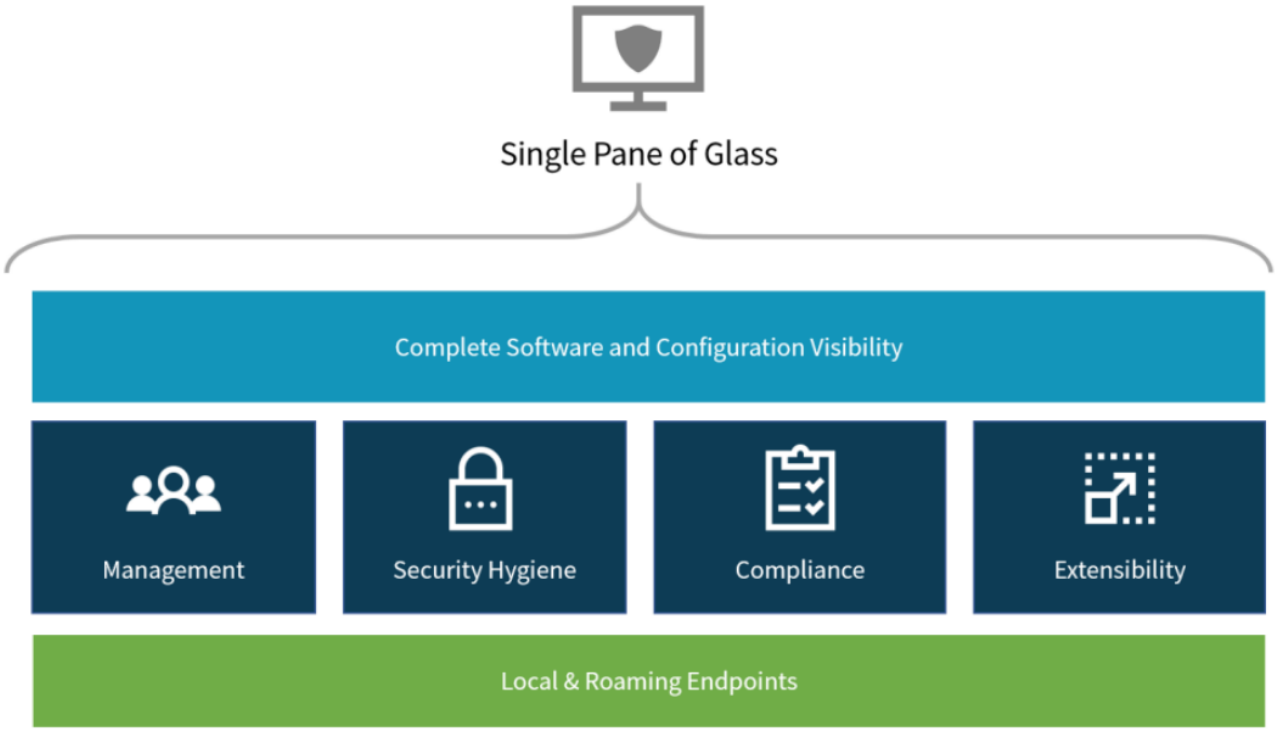

Рис. 2.1. Вимоги до управління кінцевими точками за даними Enterprise Strategy Group [7]

3. Безперервна гігієна безпеки:

постійний моніторинг і виправлення;

виявлення та усунення відхилень конфігурації;

забезпечення дотримання політик безпеки.

4. Постійна відповідність:

безперервний моніторинг і перевірка програмного забезпечення та конфігурації на відповідність політикам і нормам;

забезпечення дотримання регуляторної політики.

5. Управління роумінгом кінцевих точок:

точне управління конфігурацією віддалених кінцевих точок.

6. Можливість розширення та інтеграція з існуючою інфраструктурою:

готова інтеграція з інструментами безпеки, включаючи платформу захисту

кінцевих точок (EPP) і інструменти управління інформацією і подіями безпеки (SIEM);

API-інтерфейси, що розкривають всі аспекти управління кінцевими точками для автоматизації.

7. Єдина панель уявлення для всього парку кінцевих точок:

єдине уявлення про всі системні активи, незалежно від операційної системи, розташування або типу підключення.

HCL BigFix – платформа для спільного управління кінцевими точками і безпекою. Вона забезпечує готовий підхід до виявлення активів, поширенню програмного забезпечення та ініціалізації ОС, що призводить до створення безпечних і сумісних систем, незалежно від операційної системи, розташування або можливості підключення.

HCL BigFix дозволяє швидко виявляти активи (інвентаризація обладнання і програмного забезпечення, ліцензії на програмне забезпечення та їх використання, а також звіти про відповідність):

швидка інвентаризація кінцевих точок в декількох операційних системах, ідентифікація всіх кінцевих точок і надання точної і актуальної інформації про встановлене програмне забезпечення, його використанні і конфігурації;

отримання інформації про кінцеві точки практично в реальному часі з окремого пристрою або від груп кінцевих точок за допомогою BigFix Query;

виявлення некерованих кінцевих точок, включаючи потенційно небезпечні пристрої, підключені до мережі.

HCL BigFix дозволяє легко управляти (установка виправлень, поширення та підготовка програмного забезпечення):

швидке розгортання і виправлення операційних систем і сторонніх програм з високими показниками успіху з першого разу;

скорочення витрат на програмне забезпечення за рахунок оцінки використання додатків і ліцензування;

управління безпечною конфігурацією на всіх кінцевих точках, включаючи віддалені системи в роумінгу;

забезпечення загального уявлення про всі апаратні і програмні активи як для IT-фахівців, так і для фахівців з безпеки.

HCL BigFix забезпечує постійну безпеку (безперервний моніторинг і установка виправлень, дотримання політик безпеки і правильної конфігурації):

постійний моніторинг, виправлення і забезпечення дотримання політик безпеки на всіх кінцевих точках, незалежно від операційної системи, розташування або типу підключення;

підтримка хмарних кінцевих точок, віддалених серверів і кінцевих точок в роумінгу (з виходом в Інтернет) в оновленому, безпечному і завжди правильно налаштованому стані.

HCL BigFix забезпечує дотримання вимог в режимі реального часу:

покращення звітності про відповідність, надаючи готову підтримку тестів безпеки, опублікованих CIS, DISA, STIG, USGCB і PCI-DSS;

забезпечення відповідності кінцевих точок в операційних системах Windows, UNIX, Linux і Macintosh;

постійний моніторинг і забезпечення дотримання конфігурацій безпеки кінцевих точок для забезпечення відповідності нормативним або організаційним політикам безпеки.

HCL BigFix забезпечує керування віддаленими кінцевими точками:

отримання повної видимості серверів, настільних комп'ютерів і ноутбуків, незалежно від їх місця розташування, підключення, типу або статусу;

управління та виправлення як локальних, так і підключених до Інтернету кінцевих точок;

виявлення некерованих активів, щоб швидко привести їх під управління.

HCL BigFix забезпечує повну інтеграцію:

інтеграція з інструментами виявлення та реагування на кінцевій точці (EDR), щоб допомогти командам безпеки краще виявляти загрози, а операційним групам усувати масштабні проблеми з кінцевими точками;

інтеграція з програмним забезпеченням для управління доступом до мережі (VPN-клієнти, брандмауери тощо), щоб ізолювати кінцеві точки і забезпечити

дотримання вимог;

надання командам SOC можливості переглядати дані кінцевих точок в рамках наявних у них засобів управління інформацією і подіями безпеки і реагування на інциденти (SIEM). Прискорення і поліпшення реагування на інциденти за рахунок виявлення, покращення та автоматичного реагування.

використання багатого набору API-інтерфейсів для настройки і автоматизації дій з управління кінцевими точками.

HCL BigFix забезпечує загальний огляд активів:

за допомогою єдиної консолі BigFix і єдиної платформи IT-підрозділу і організації, що займаються безпекою, можуть більш ефективно співпрацювати, щоб скоротити експлуатаційні витрати, скоротити цикли управління кінцевими точками, забезпечити дотримання нормативних вимог в режимі реального часу і підвищити продуктивність.

Використовуючи BigFix, групи безпеки та інфраструктури можуть бачити одні й ті ж дані кінцевих точок і діяти з ними, не перемикаючись між декількома додатками, що економить їх час і прискорює прийняття рішень. Команди IT-операцій і безпеки можуть більш ефективно співпрацювати, щоб скоротити операційні витрати, скоротити цикли управління кінцевими точками і забезпечити дотримання нормативних вимог в режимі реального часу, одночасно підвищуючи продуктивність.

У [7] підкреслюється, що програмне забезпечення для управління кінцевими точками грає важливу роль як в стратегії безпеки, так і в стратегії відповідності. В умовах постійно мінливої поверхні атак в більшості організацій захист кінцевих точок є практично неможливим завданням без автоматизації процесу інвентаризації, установки виправлень і налаштувань.

EMS є основним компонентом IT-інфраструктури і, як такий, повинен сприяти інтеграції з багатьма іншими системами управління ризиками, які працюють в стеці безпеки. Ця інтеграція має першорядне значення для того, щоб IT-відділи та служби безпеки могли не відставати від швидко зростаючого ландшафту загроз.

Незважаючи на те, що сьогодні є безліч рішень для установки виправлень, організаціям слід уважно вивчити варіанти, щоб переконатися, що вони пропонують надійні можливості, що підтримують як вимоги безпеки, так і відповідності, при цьому пропонуючи масштабованість, гнучкість і розширюваність для підтримки зростання і складності організації.

HCL BigFix, широко відомий як провідне програмне рішення для управління кінцевими точками, відповідає вимогам щодо управління кінцевими точками або перевершує їх, тому його слід серйозно враховувати при додаванні або оновленні EMS організацій та підприємств.

2.2. Призначення, можливості та функції платформи HCL BigFix

Зазначається, що команди фахівців з кібербезпеки прагнуть передбачити всі можливі дії кіберзлочинців і для цього можуть використовувати до 85 інструментів від 45 різних постачальників. Це ускладнює визначення пріоритетів змін і виправлень. Крім того, не всі інструменти мають однакові можливості. Якщо відсутня видимість, що відбувається у кінцевих користувачів, інструменти захисту працюють разом неефективно і не можна захистити корпоративні пристрої і дані. Для цього розроблено продукт HCL BigFix – платформа для спільного управління IT-обладнанням та забезпечення безпеки.

Платформа HCL BigFix надає адміністраторам централізовані, автоматизовані і функції, які настроюються, для управління кінцевими точками з наступними можливостями:

управління виправленнями;

поширення програмного забезпечення;

розгортання ОС;

управління мобільними пристроями;

управління енергоспоживанням;

автоматична оцінка кінцевих точок і усунення вразливостей;

захист в реальному часі від шкідливих програм та інших вразливостей;

автоматизація серверів.

BigFix – це набір продуктів, який забезпечує швидке та інтуїтивно зрозуміле рішення для управління відповідністю, кінцевими точками і безпекою і дозволяє організаціям бачити і управляти фізичними і віртуальними кінцевими точками за допомогою єдиної інфраструктури, єдиної консолі і одного типу агента.

Використовуючи BigFix, підрозділи і фахівці з кібербезпеки можуть більш ефективно співпрацювати, щоб скоротити експлуатаційні витрати, цикли управління робочими місцями кінцевих користувачів та IT-обладнанням, забезпечити дотримання вимог в режимі реального часу, підвищити продуктивність і оптимізувати окупність інвестицій.

Рішення HCL BigFix відповідає ключовим потребам фахівців, відповідальних за корпоративну IT-інфраструктуру та кібербезпеку:

швидке виявлення: визначає і надає точну інформацію про ваших кінцевих користувачів та IT-обладнанні в режимі реального часу – незалежно від операційної системи, розташування або підключення;

постійний захист: забезпечує постійний моніторинг, виправлення і застосування політик безпеки:

BigFix Compliance – постійне дотримання і відповідність політиці і звітність;

BigFix Lifecycle – відстеження життєвого циклу програмного забезпечення: виправлення, поширення і надання;

BigFix Inventory – інвентаризація, аудит авторизованого і неавторизованого програмного забезпечення;

BigFix Patch – відстеження і установка патчів: автоматичне виправлення з високим результатом першого проходу;

BigFix Compliance забезпечує постійну відповідність політикам безпеки організації для кожної кінцевої точки як в корпоративній мережі, так і за її межами. Включає в себе вбудовану підтримку більшості популярних тестів безпеки, опублікованих CIS, DISA STIG, USGCB і PCI DSS. Інтелектуальний агент на кожній кінцевій точці відстежує і забезпечує дотримання вимог, повідомляє про стан конфігурації безпеки IT-обладнання в режимі реального часу

незалежно від типу або розташування ОС. Сповіщення про будь-які порушення відповідності надходять негайно, що дозволяє швидко усунути порушення та знизити загальні ризики безпеки.

BigFix Lifecycle допомагає знаходити і усувати проблеми на всіх кінцевих точках за лічені хвилини. Це рішення виявляє, захищає і керує сотнями тисяч одиниць IT-обладнання та пристроїв кінцевих користувачів в більш ніж 90 різних версіях ОС протягом декількох годин або навіть хвилин. Крім того що всі інформаційні системи оновлені і захищені, автоматизація міграції ОС, відстежування робочих місць кінцевих користувачів на наявність шкідливих файлів в режимі реального часу, швидке встановлення програмного забезпечення, здійсення розширеної автоматизації або дистанційного керування за допомогою всього декількох кліків миші, через зручний веб-інтерфейс, використовуючи прості інтуїтивно зрозумілі питання.

BigFix Inventory може значно скоротити час, необхідний для проведення повної інвентаризації активів програмного забезпечення для звірки ліцензій або відповідності вимогам. Це дає цінну інформацію про те, чим організація законно володіє з встановленого програмного забезпечення, як часто його використовує. Завдяки таким можливостям, можна підвищити рівень планування і бюджетування, забезпечити відповідність встановлених ліцензій придбаним у постачальника, зменшити ризик IT-безпеки.

BigFix Patch забезпечує автоматизований, спрощений процес установки патчів, який адмініструється з єдиної консолі в реальному режимі часу для розгортання та управління патчами на IT-обладнанні і робочих місцях користувачів, в корпоративної мережі і за її межами. Клієнти повідомляють про більш ніж 98% успішному установки патча з першого разу. Рішення підвищує ефективність процесу внесення виправлень, знижує експлуатаційні витрати і скорочує час циклу установки патчів, забезпечуючи безпеку кінцевих користувачів.

Додатки BigFix

Рішення BigFix складається з декількох прикладних продуктів, що

забезпечують консолідоване управління безпекою та операціями, спрощене та оптимізоване управління кінцевими точками, одночасно підвищуючи точність та продуктивність.

BigFix Lifecycle – інструмент адміністратора на основі агента, який забезпечує точну видимість стану кінцевих точок та автоматично усуває проблеми.

BigFix Lifecycle включає такі програми:

*OS Deployment – з*абезпечує консолідоване комплексне рішення для швидкого розгортання нових робочих станцій та серверів у мережі через єдине централізоване місце;

Power Management – керує та контролює параметри енергоспоживання на комп'ютерах у мережі. Він також керує та застосовує політику збереження компанії, яка встановлюється за допомогою інформаційних панелей, майстрів та веб-звітів.

Remote Control – дистанційно приймає та контролює робочі станції та сервери під час розгортання;

Server Automation – автоматизує робочі процеси забезпечення. Є можливість автоматизувати послідовність Fixlets, завдань та базових ліній для різних кінцевих точок, таких як сервери або комп'ютери;

Software Distribution – забезпечує консолідоване комплексне рішення для швидкого розгортання програмного забезпечення в мережі з одного централізованого місця. Він забезпечує економічно ефективний оперативний контроль та видимість процесу доставки та встановлення програмного забезпечення.

BigFix Patch – програму призначено, щоб забезпечити автоматизований, спрощений процес виправлення помилок для всіх розподілених кінцевих точок. Він управляє як виправленнями операційної системи, так і програмних додатків.

BigFix Compliance – додаток для захисту кінцевих точок, автоматизації виправлення та гарантування регуляторів щодо відповідності стандартам безпеки.

BigFix Inventory – програма для сканування відстежуваних комп'ютерів для

визначення, яке програмне забезпечення встановлено, а також зіставлення підписів, які виявлені скануванням, з каталогом програмного забезпечення.

Create reports – створення та застосування різних звітів.

Є можливість додавання додатків, що належать до рішення BigFix, придбавши додаткові ліцензії; вони автоматично будуть доступні для використання на консолі BigFix. Не має потріби встановлювати додаткове програмне забезпечення або купувати нове обладнання, коли ви додаєте програми, що належать до рішення. Тільки виявлення активів та інвентаризація вимагають встановлення нових компонентів, але установка здійснюється самим рішенням BigFix.

Додатково: *Asset Discovery* – це компонент платформи BigFix, який дозволяє ідентифікувати некеровані активи у мережі.

Багато клієнтів починають з однієї програми, наприклад Patch, а потім розширюють сферу свого розгортання, купуючи нові ліцензії, оскільки починають цінувати всі можливості продуктового рішення.

Необхідно враховувати, що деякі можливості є спільними для кількох програм у вирішенні продукту BigFix. Наприклад, можливість застосовувати виправлення для ОС та програмного забезпечення доступна в додатку Patch, а також у програмах Compliance та Lifecycle. Можна придбати будь-яку з цих ліцензій для управління виправленнями.

Всі ці програми використовують переваги безперервної оцінки агента і процесу збору для збору даних з репозиторіїв і їх відправки цільовим об'єктах.

2.3. Архітектура та компоненти платформи HCL BigFix

HCL BigFix єдина платформа для управління кінцевими точками, яка дозволяє групам IT-операцій і безпеки повністю автоматизувати виявлення, управління та виправлення – будь-то локально, віртуально або в хмарі – незалежно від операційної системи, розташування або підключення. На відміну від складних інструментів, які охоплюють обмежену частину ваших кінцевих точок і вимагають днів або тижнів на відновлення, BigFix може знаходити і

виправляти кінцеві точки швидше, ніж будь-яке інше рішення, при цьому забезпечуючи понад 98% успішних виправлень з першого проходу.

HCL BigFix єдина платформа для управління кінцевими точками, яка дозволяє групам IT і безпеки повністю автоматизувати процеси виявлення, управління та виправлення будь-то локально, віртуально або в хмарі, незалежно від операційної системи, розташування або підключення. На відміну від складних інструментів, які охоплюють обмежену частину корпоративних кінцевих точок і вимагають днів або тижнів на оновлення, BigFix може знаходити і виправляти кінцеві точки швидше, ніж будь-яке інше рішення, при цьому забезпечуючи понад 98% успішних виправлень з першого проходу [11].

Рішення BigFix є багаторівневою технологічною платформою, яка виступає в якості основної частини глобальної IT-інфраструктури. Платформа являє собою динамічну, керовану контентом систему обміну повідомленнями та управління, яка розподіляє роботу з управління IT-інфраструктурою між самими керованими пристроями, агентами. Всі додатки BigFix працюють на платформі BigFix.

Платформа може керувати до 250 000 фізичними та віртуальними комп'ютерами в приватних або загальнодоступних мережах, включаючи настільні сервери, портативні комп'ютери в роумінгу, мобільні телефони, пристрої для точок продажів, банкомати та кіоски самообслуговування [11].

Розглянемо основні компоненти архітектури рішення HCL BigFix, функціонування яких реалізує технологію управління захистом кінцевих точок корпоративної інформаційної системи, а саме [11]:

Єдиний інтелектуальний агент повинен бути встановлений на кожному комп'ютері, яким необхідно управляти. Він постійно оцінює стан кінцевої точки відповідно до заявленої політики, незалежно від того, чи підключена вона до мережі чи ні. Як тільки агент бачить, що ціль не відповідає політиці або контрольному списку, він інформує сервер, запускає налаштоване завдання виправлення і негайно повідомляє сервер про стан завдання та його результат. У більшості випадків агент працює мовчки, без будь-якого прямого втручання з боку користувача. Однак, якщо виникає необхідність запросити відповідь

користувача, програма також дозволяє відображати підказки на екрані. Комп'ютер зі встановленим агентом BigFix також називається клієнтом.

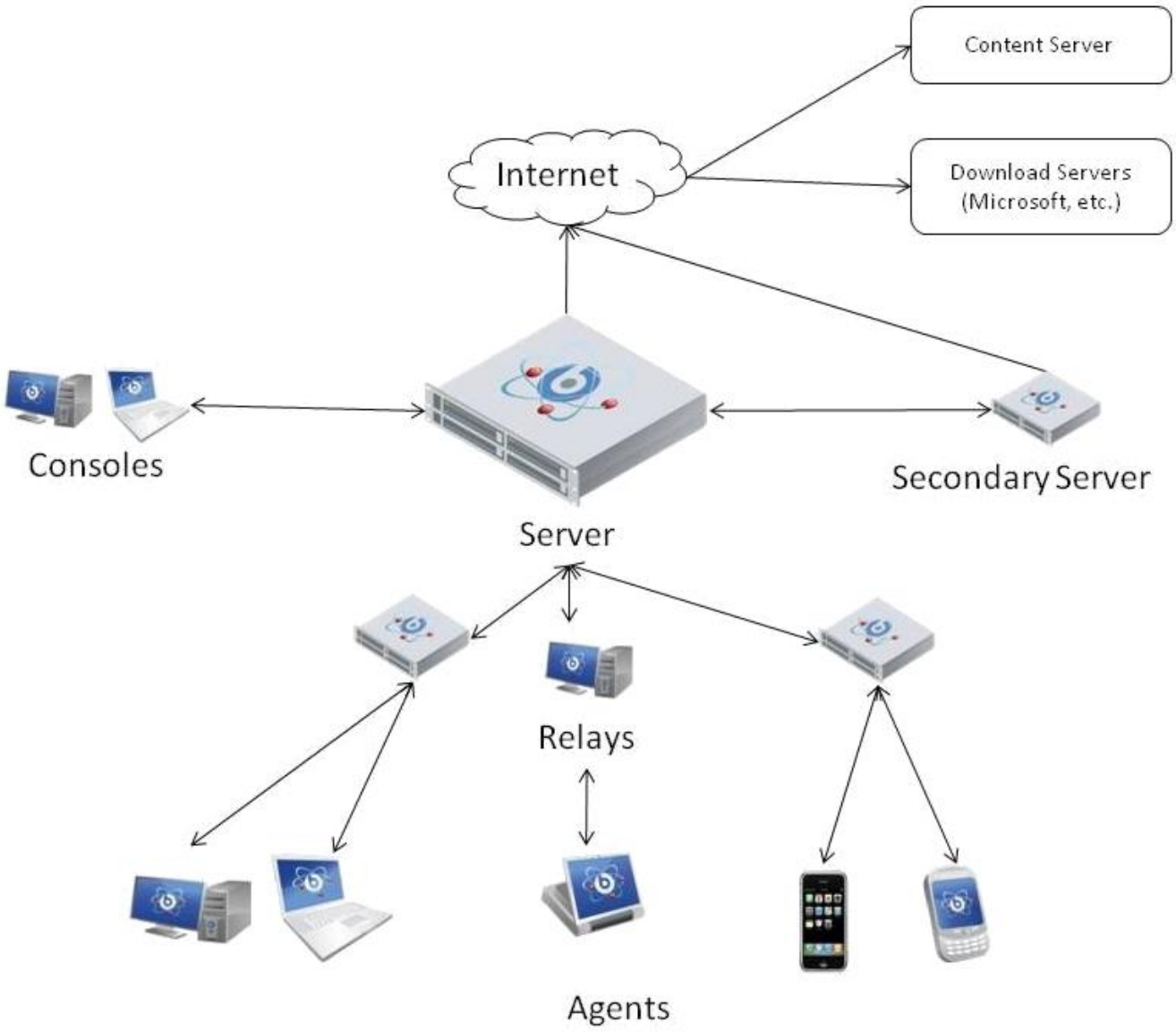

Рис. 2.2. Основні компоненти архітектури рішення HCL BigFix [11]

Розглянемо основні компоненти архітектури рішення HCL BigFix, функціонування яких реалізує технологію управління захистом кінцевих точок корпоративної інформаційної системи, а саме [11]:

Єдиний інтелектуальний агент повинен бути встановлений на кожному комп'ютері, яким необхідно управляти. Він постійно оцінює стан кінцевої точки відповідно до заявленої політики, незалежно від того, чи підключена вона до мережі чи ні. Як тільки агент бачить, що ціль не відповідає політиці або контрольному списку, він інформує сервер, запускає налаштоване завдання виправлення і негайно повідомляє сервер про стан завдання та його результат. У

більшості випадків агент працює мовчки, без будь-якого прямого втручання з боку користувача. Однак, якщо виникає необхідність запросити відповідь користувача, програма також дозволяє відображати підказки на екрані. Комп'ютер зі встановленим агентом BigFix також називається клієнтом.

Єдина консоль забезпечує управління кінцевими точками, наприклад, управління захистом кінцевих точок, управління життєвим циклом системи, налаштуваннями безпеки і управління вразливостями та оновленнями.

Єдиний сервер координує потік інформації до окремих клієнтів та від них, зберігає результати в базі даних. Він керує контентом на основі політик і дозволяє оператору підтримувати видимість і контроль в реальному часі над усіма пристроями в середовищі. Контент доставляється в повідомленнях, які називаються Fixlet, і постійно оновлюється за допомогою хмарної служби доставки контенту. Оскільки велика частина роботи з аналізу, обробки і забезпечення дотримання вимогам виконується агентом, а не сервером, один сервер може підтримувати до 250 000 кінцевих точок. Висока доступність може забезпечуватися за рахунок використання декількох серверів.

Опціональні ретранслятори допомагають керувати розподіленими пристроями і вмістом політик. Ретранслятор – це клієнт, розширений службою ретрансляції. Він виконує всі клієнтські дії для захисту головного комп'ютера і, крім того, доставляє контент і завантаження програмного забезпечення дочірнім клієнтам і ретрансляторам. Замість того, щоб вимагати від кожного мережевого комп'ютера прямого доступу до сервера, можна використовувати ретрансляцію, щоб зняти велику частину навантаження. Сотні клієнтів можуть вказувати на ретранслятор для завантажень, який, в свою чергу, робить тільки один запит до сервера. Ретранслятор також можна підключати до інших ретрансляторів, що ще більше збільшує ефективність. Підвищення рівня агента до ретранслятора займає хвилини і не вимагає зміни спеціального обладнання або конфігурації мережі.

Сервер Disaster Server Architecture (DSA) реплікує інформацію сервера для аварійного відновлення. Якщо сервер BigFix виходить з ладу, інші сервери BigFix автоматично стають повністю функціональними серверами BigFix.

Додаток Web Reports забезпечує створення діаграм та графіків корпоративних даних, надаючи друковані копії; надає допомогу у веденні контрольного журналу всієї активності Fixlet у корпоративній мережі; забезпечує експорт даних для подальшої обробки в електронну таблицю або базу даних; збирає інформацію з додаткових серверів BigFix; забезпечує роботу інтерфейсу в веб-браузері і надає ряду користувачів можливість бачити стан комп'ютерів без права на зміну цих комп'ютерів.

Таким чином, сучасні підходи базуються на комплексному захисті кінцевих точок корпоративної інформаційної системи, у вигляді клієнта зі всіма необхідними компонентами, що є зручним для кінцевого користувача. Централізоване управління захистом кінцевими точками спрощує роботу адміністраторів безпеки із засобами захисту, так як використовується менше додатків безпеки та, відповідно, витрачається менше зусиль щодо забезпечення їх функціонування.

2.4. Додатки платформи HCL BigFix

Рішення BigFix включає кілька прикладних продуктів, які забезпечують консолідоване управління безпекою та операціями, спрощене і оптимізоване управління кінцевими точками, одночасно підвищуючи точність і продуктивність.

Рішення BigFix включає кілька прикладних продуктів, які забезпечують консолідоване управління безпекою та операціями, спрощене і оптимізоване управління кінцевими точками, одночасно підвищуючи точність і продуктивність.

BigFix Lifecycle

Цей додаток використовується для надання адміністраторам інструменту на основі агентів, який забезпечує точну видимість стану кінцевих точок і автоматично усуває проблеми.

BigFix Lifecycle включає в себе наступні програми:

OS Deployment – надає консолідоване комплексне рішення для швидкого розгортання нових робочих станцій і серверів в мережі з єдиного централізованого місця.

Power Management – управляє і відстежує параметри енергоспоживання на комп'ютерах у корпоративній мережі. Він також керує і застосовує політику збереження компанії, яка встановлюється за допомогою інформаційних панелей, майстрів та веб-звітів.

Remote Control – віддалено бере на себе і контролює робочі станції і сервери в корпоративному розгортанні.

Server Automation – автоматизує робочі процеси підготовки. Здійснює автоматизацію послідовностей Fixlets, завдань і базових показників на різних кінцевих точках, таких як сервери або комп'ютери.

Software Distribution – надає консолідоване комплексне рішення для швидкого розгортання програмного забезпечення в мережі з єдиного централізованого місця. Додаток забезпечує операційний контроль і прозорість процесу доставки і установки програмного забезпечення.

BigFix Lifecycle – це технологія з одним агентом та однією консоллю, яка забезпечує видимість стану конечних токів майже в реальному часі.

Основне в технології BigFix це програмне забезпечення, яке забезпечує адміністрування централізованих, автоматизованих та функцій, які налаштовуються, для управління конечними точками. Адміністраторам надається інструмент на основі агентів, який забезпечує точну видимість та автоматичне вирішення проблем.

BigFix Lifecycle забезпечує:

управління кінцевими точками незалежно від їх розташування, підключення, типу або статусу з одного сервера управління;

об'єднання повного життєвого циклу систем, включаючи виявлення та інвентаризацію активів, розповсюдження програмного забезпечення, розширення операційної системи, управління виправленнями та управління удаленим робочим столом;

максимальне використання технології BigFix, виконуючи додаткові спеціальні запити та дії на основі практично будь-яких властивостей комп'ютера за лічені хвилини;

зниження складності управління та затримки при одночасному підвищенні точності та продуктивності.

BigFix Patch

Цей додаток використовується для забезпечення автоматизованого і спрощеного процесу установки виправлень для всіх розподілених кінцевих точок. Він керує виправленнями як операційної системи, так і програмних додатків.

BigFix Compliance

Цей додаток використовується для захисту кінцевих точок, автоматизації виправлень і забезпечення відповідності регулюючих органів стандартам безпеки.

BigFix Inventory

Цей додаток використовується для сканування комп'ютерів, які відслідковуються, щоб:

визначати, яке програмне забезпечення встановлено;

для зіставлення підписів, які виявлені при скануванні, з каталогом програмного забезпечення;

створення звітів;

для порівняння результатів з інформацією про витрати і правах, які вказані в контрактах.

Відповідальні за кібербезпеку приймають рішення про додавання додатків, що належать рішенням BigFix і вони автоматично стають доступними для використання в консолі BigFix. Не має потреби встановлювати будь-яке додаткове програмне забезпечення або купувати нове обладнання при додаванні додатків, що належать рішенням. Тільки Asset Discovery і Inventory вимагають установки нових компонентів, але установка виконується самим BigFix.

Asset Discovery – це компонент платформи BigFix, який дозволяє ідентифікувати некеровані активи в корпоративній мережі.

Багато клієнтів починають з однієї програми, такого як Patch, а потім розширюють обсяг свого розгортання, додаючи відповідні компоненти.

Необхідно враховувати, що деякі можливості є спільними для декількох додатків в продукті BigFix. Наприклад, можливість застосовувати виправлення

для ОС та програмного забезпечення доступна в додатку Patch, а також в додатках Compliance і Lifecycle. Тому, можна обирати відповідні рішення.

2.5. Типова архітектура платформи HCL BigFix

Розглянемо типову архітектури рішення HCL BigFix, яка надасть уявлення про середовище платформи та можливість її правильного планування.

У стандартному розгортанні є один сервер BigFix (рис. 2.3), який збирає Fixlets з Інтернету. Ці повідомлення можуть бути переглянуті оператором консолі та розподілені за трансляціями, які переглядають дані клієнтів. Кожний клієнт перевіряє свій локальний комп'ютер і повідомляє про всі відповідні Fixlets ретрансляторам, які відтворюють дані та передають їх назад на сервери.

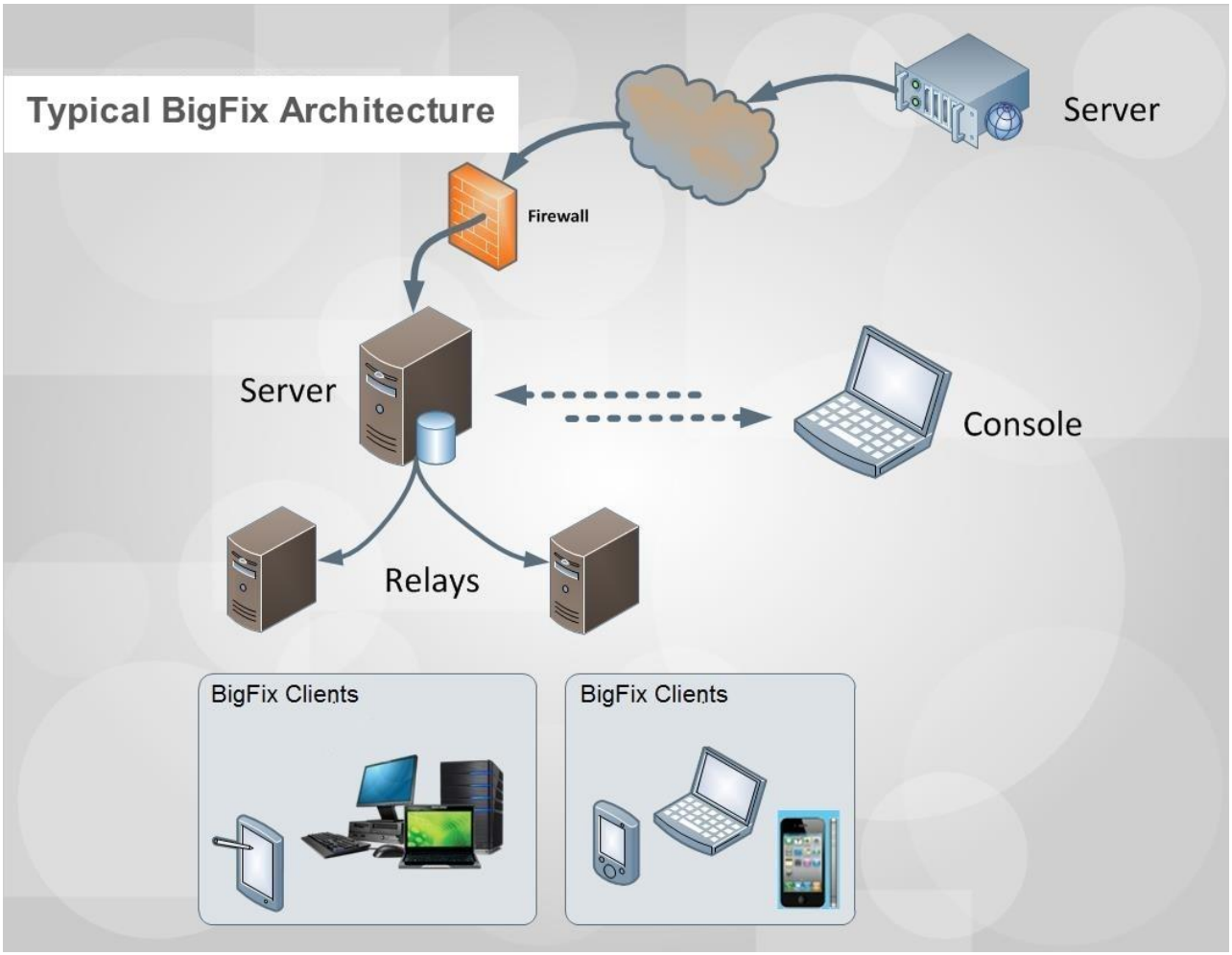

Рис. 2.3. Типова архітектура платформи HCL BigFix

Консоль спостерігає за цією діяльністю. Вона підключається до сервера та періодично оновлює свої презентації, щоб відобразити зміни або нову інформацію

про корпоративну мережу. При виявленні уявного оператора консолі можуть почати виправлення або інші виправлення на відповідних комп'ютерах. За ходом виправлень можна слідувати майже в реальному часі, оскільки вони поширюються на всіх відповідних комп'ютерах і, по-різному, вказують на помилки та уявлення.

BigFix достатньо гнучкий, щоб підключитися до віддаленого офісу через VPN, і навіть дозволяє домашнім працівникам або менеджерам у дорозі підключитися через Інтернет до захищеного брандмауером каналу в демілітаризованій зоні. Цю просту ієрархію можна розширювати і поглиблювати для розміщення мереж практично будь-якого розміру.

Розглянемо типи контенту BigFix.

Функціонування BigFix засноване на контенті. Загальний термін «контент» може представляти дані для розподілу по цілям, інструкції для виконання за програмними цілями або запити для виконання за програмними цілями.

Функціонування BigFix заснована на наступних типах контенту:

Дія – це сценарій, який виконується для обраних цілей. Дії використовуються для виправлення порушень політики і вразливостей, для виконання кроків налаштування або, в загальному, для виконання операцій або команд для цілей. Fixlets, завдання та базові показники містять дії і залежать від дій для виконання своєї місії щодо виправлення.

Fixlet – це документ, що містить інструкції, які агенти BigFix в цільових системах використовують для оцінки свого статусу, виявлення проблем, таких як вразливість або недотримання правил політики, і прийняття коригувальних дій для вирішення.

Завдання – це документ, що містить інструкції, які агенти BigFix в цільових системах використовують для локального виконання команд або дій з налаштування.

Базова лінія – це контейнер для розгортання Fixlets і завдань. Він використовується для одночасного застосування набору вмісту до однієї або декількох цілей. Вміст застосовується відповідно до послідовності, зазначеної в

базовому описі. Наприклад, базова лінія може містити:

fixlet для установки продукту;

fixlet для підвищення його до необхідного рівня;

завдання по налаштуванню встановленого продукту.

Коли базова лінія розгорнута, вміст застосовується в заздалегідь певній послідовності.

Аналіз – це набір виразів властивостей, що дозволяє оператору переглядати і узагальнювати різні властивості клієнтських комп'ютерів BigFix в мережі.

Доступ до цих типів контенту забезпечується з консолі BigFix. Кожна програма, що входить в комплект BigFix, використовує цей контент для виконання своїх завдань. Адміністратор може створити свій власний контент, щоб задовольнити конкретні потреби. Наприклад, адміністратор може створювати власні Fixlets для застосування виправлень до додатків власної розробки або для забезпечення дотримання правил політики. Для цього повинні бути певні повноваження для створення власного контенту.

Контент міститься на інформаційних сайтах і своєчасно оновлюється автоматично. Доступні інформаційні сайти залежить від придбаних ліцензій на продукт BigFix. Якщо є необхідні дозволи, адміністратор може створити власний сайт з налаштованим контентом та для збирання відповідного контенту.

Fixlet є фрагментом контенту BigFix, який містить оператори Relevance і Action Script, об'єднані разом для виконання операції або завдання. Fixlets є основними будівельними блоками контенту BigFix. Fixlet надає агенту BigFix інструкції для виконання дії з управління мережею або складання звітів. Вигляд інтерфейсу HCL BigFix показано на рис. 2.4.

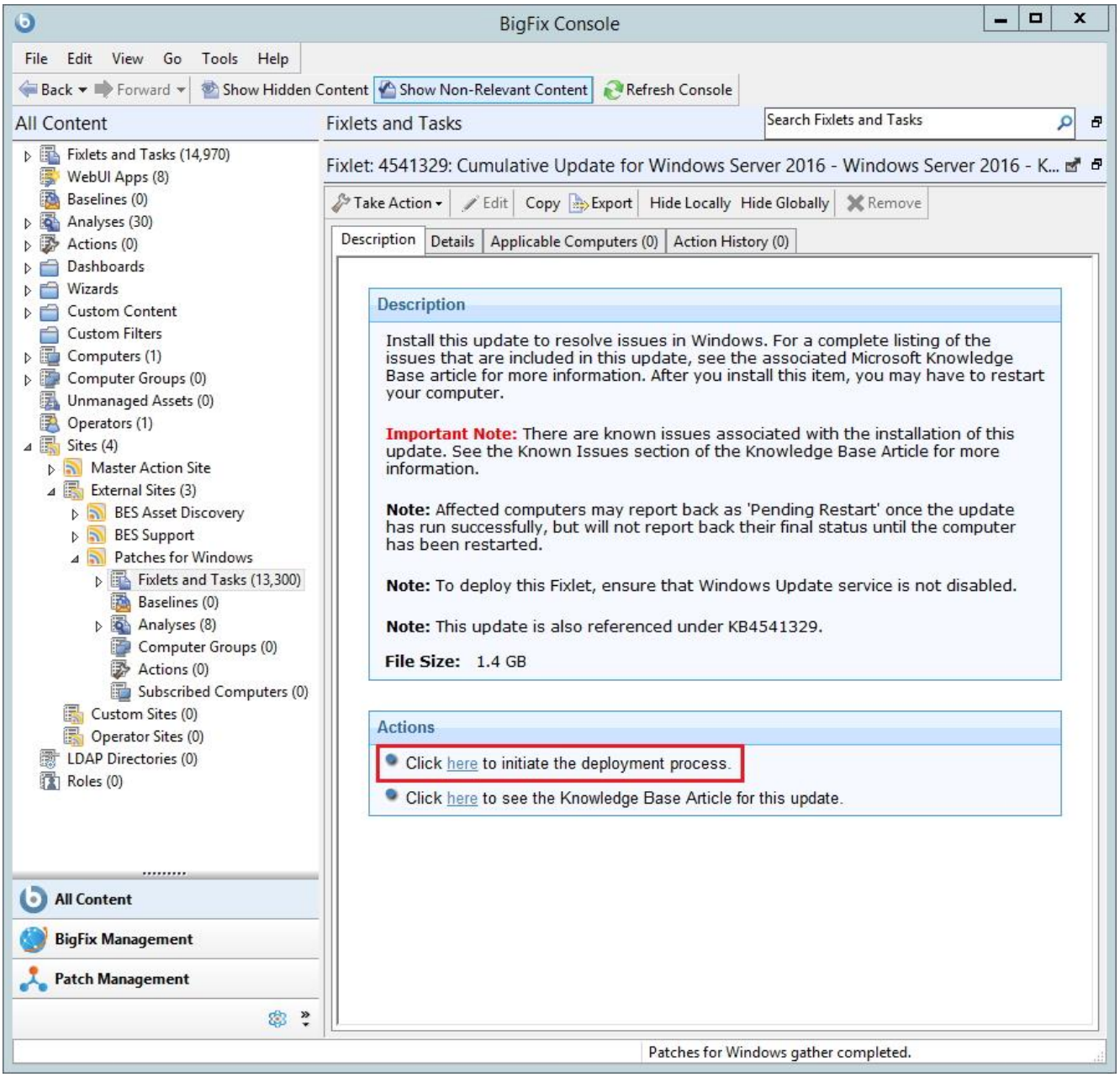

Рис. 2.4. Вигляд інтерфейсу HCL BigFix

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ HCL BIGFIX

3.1. Розроблення варіанта технології управління захистом кінцевих точок корпоративної інформаційної системи на базі HCL BigFix

Необхідно зазначити, що HCL BigFix є потужним і багатофункціональним програмним комплексом. Якщо оператор розуміє типовий робочий процес, операції безпеки стають простими і інтуїтивно зрозумілими.

Розглянемо приклад робочого процесу оператора консолі HCL BigFix [12].

1. Робочий процес оператора починається із запуску консолі BigFix.

2. На панелі домену зліва необхідно натиснути кнопку з написом All Content, яка дозволяє операторові переглядати всі сайти, на які підписані. Потім необхідно натиснути кнопку Fixlets and Tasks у верхній частині панелі Domain. Після цього на панелі списку праворуч відобразиться список Fixlets and Tasks (рис. 3.1), які в даний час застосовуються до мережі.

3. На панелі списку натисніть потрібний Fixlet. Відповідний документ відкриється в Робочій області під списком. Це текст Fixlet, який дає операторові інформацію, необхідну для прийняття рішення про розгортання, а також конкретні дії, які необхідно зробити (рис. 3.2).

4. Внизу повідомлення знаходяться одне або кілька посилань, які ініціюють дії щодо виправлення вразливих комп'ютерів. Необхідно натиснути кнопку дії, яке здається найбільш підходящим. Take Action відкриває діалогове вікно (рис. 3.3).

5. Оператор може використовувати вкладку Target, щоб вибрати будь-яку підмножина порушених комп'ютерів, на яких він налаштовує відповідні дії. Є кілька прийомів розгортання дій:

Конкретні комп'ютери, обрані в списку нижче (рис. 3.3). Перша кнопка Target дозволяє оператору вибрати потрібні комп'ютери на панелі внизу праворуч,

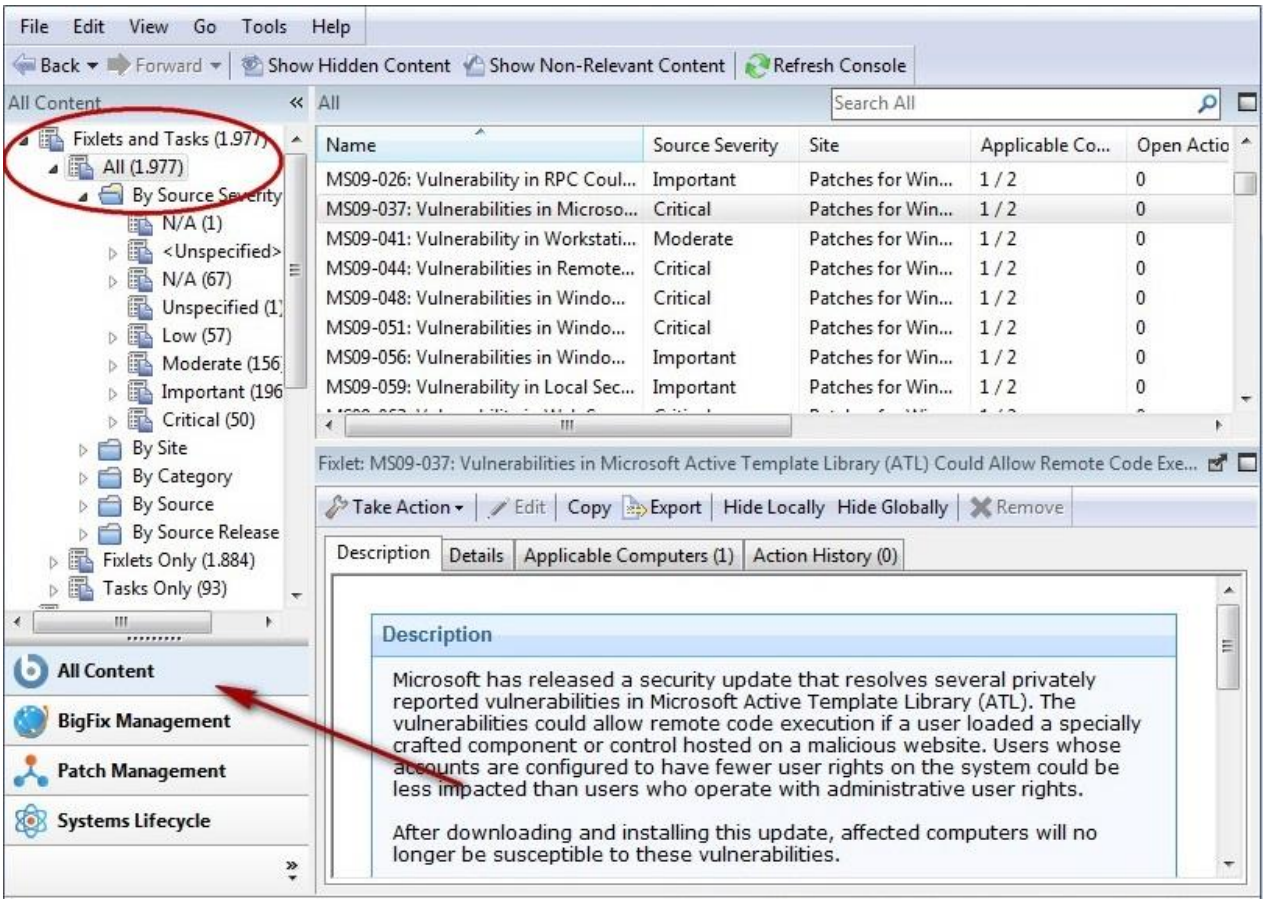

Рис. 3.1. Список Fixlets and Tasks консолі BigFix

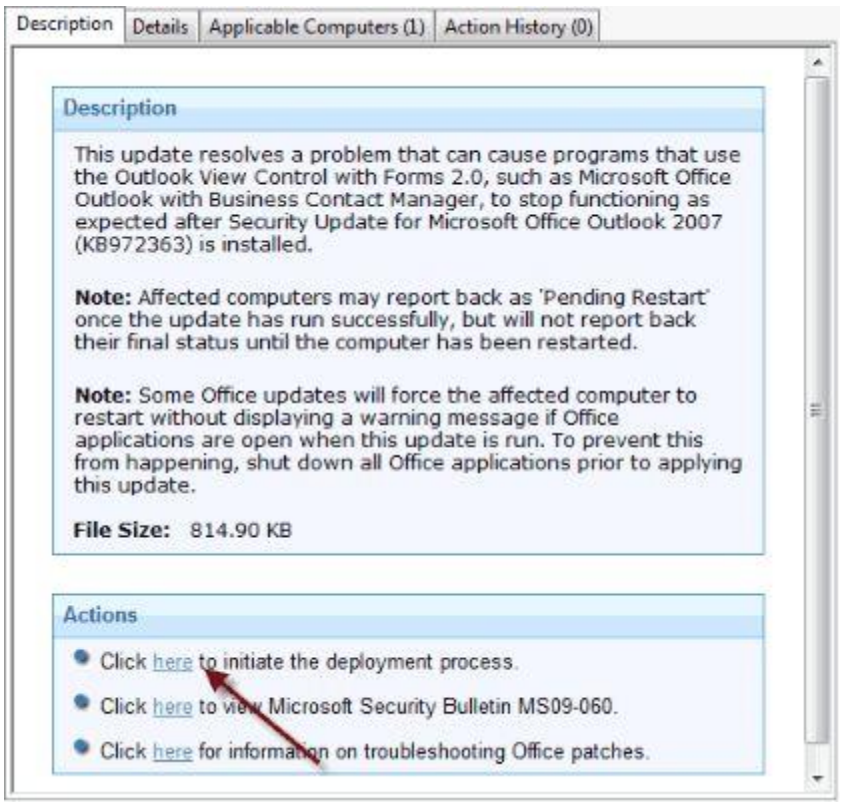

Рис. 3.2. Зміст конкретного Fixlet на консолі BigFix

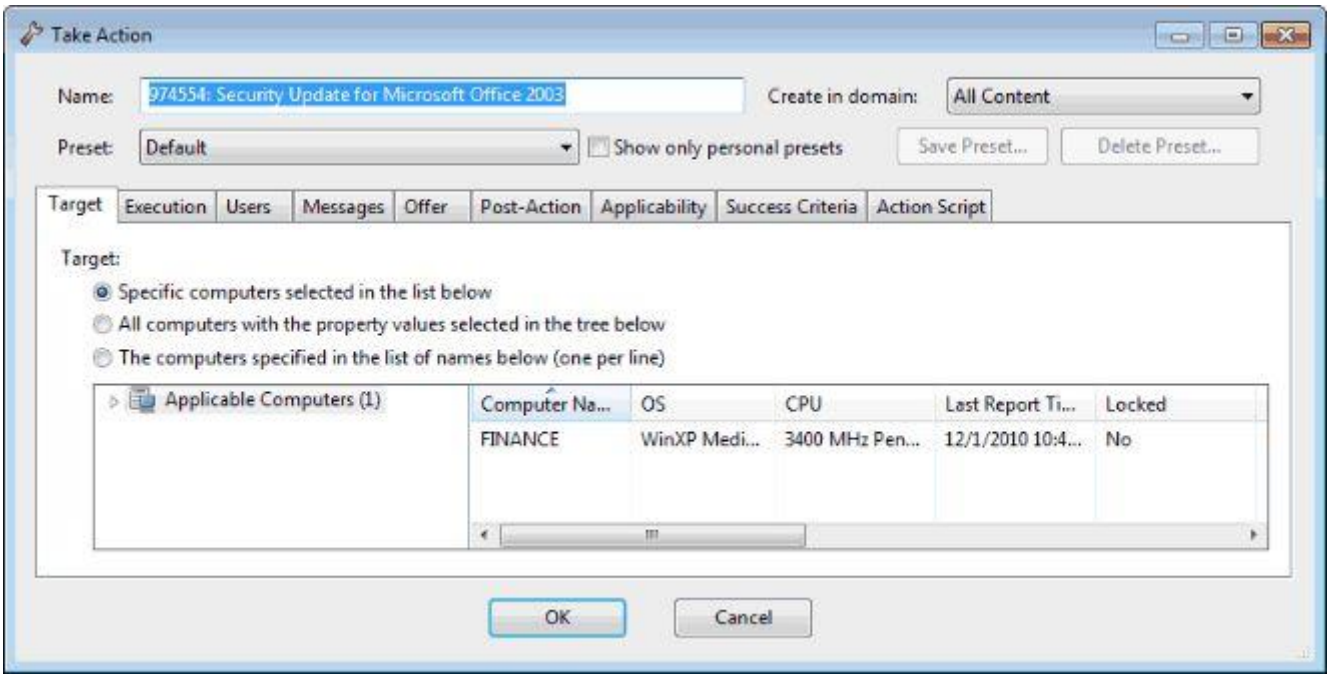

Рис. 3.3. Діалогове вікно Take Action на консолі BigFix

де перераховані всі ті комп'ютери, для яких в даний момент актуальний Fixlet. Меню, яке викликається правою кнопкою миші, дозволяє вибрати всі комп'ютери в списку. Цей метод обмежує дію Fixlet зазначеним списком.

Всі комп'ютери зі значеннями властивостей, обраними в дереві нижче (рис. 3.3). Натисніть другу кнопку, щоб виконувати дії на комп'ютерах з набором зазначених властивостей. До закінчення періоду дії, коли комп'ютер задовольняє заданим властивостям, він стає метою. Як і у випадку з усіма діями, дії фактично отримують тільки порушені комп'ютери.

Комп'ютери, зазначені в списку імен нижче (рис. 3.3). Натисніть третю кнопку, щоб вказати список комп'ютерів.

6. Оператор використовує інші вкладки для підготовки своїх дій, включаючи розклади виконання, клієнтські повідомлення, додаткові сценарії і багато іншого, потім натискає кнопку ОК.

7. Коли оператор вводить свій пароль, дія Fixlet розгортається по всій корпоративній мережі і застосовується спеціально до кожного комп'ютера, який його потребує, з урахуванням всіх встановлених оператором фільтрів.

Розглянутий процес використовує оператор для стандартного обслуговування і виправлення комп'ютера. Вивчивши інтерфейс, оператор

виявляє яким чином усувати проблеми безпеки, проводити інвентаризацію комп'ютерів, управляти користувачами і вести докладний контрольний журнал кожного виправлення та оновлення. Якими б різноманітними не були ці завдання, всі вони виконуються схожим робочим процесом.

3.2. Технологія управління активами корпоративної інформаційної системи на базі BigFix Asset Discovery

BigFix Asset Discovery має кілька ключових застосувань в корпоративних середовищах [13]:

ідентифікація мережевих ресурсів, включаючи такі пристрої, як маршрутизатори, принтери, комутатори, точки бездротового доступу або що-небудь з IP-адресою;

виявлення некерованих і шахрайських комп'ютерів, включаючи комп'ютери, на яких був відключений агент BigFix, або шахрайські комп'ютери, які не керовані компанією.

За допомогою цієї інформації можна відповісти на важливі питання інвентаризації ліцензій щодо того, що це за пристрій, коли він був встановлений і де знаходиться. Крім того, можна відповісти на питання безпеки і проблеми, що стосуються неавторизованих комп'ютерів співробітників, бездротових пристроїв або несанкціонованих пристроїв в мережі.

Рішення BigFix Asset Discovery унікально, тому що сканування виконується іншими агентами найближчих комп'ютерів. Це називається *розподіленим скануванням*.

У цього підходу є кілька ключових переваг:

зберігає пропускну здатність WAN;

сканування можна виконувати паралельно, щоб отримати результати набагато швидше - за лічені хвилини замість тижнів;

легко налаштовується для роботи в складних мережевих конфігураціях, включаючи ізольовані підмережі;

окремі підмережі можуть запускати типи сканування, які настроюються.

BigFix Asset Discovery працює за допомогою Fixlet і Tasks для розгортання точок сканування для зазначених агентів у корпоративній мережі. Потім можна використовувати інші Fixlet і Tasks для запуску сканування Nmap з вибраними оператором інтервалами. Результати сканування автоматично відправляються на сервер BigFix, який імпортує дані в базу даних BigFix (рис. 3.4). Після цього інформацію про сканування можна буде переглянути в консолі BigFix на вкладці «Некеровані ресурси».

BigFix Asset Discovery працює, визначаючи певні комп'ютери як *точки сканування*. Будь-який агент може бути позначений як точка сканування, якщо він працює під управлінням підтримуваної операційної системи. Ці точки сканування запитують некеровані активи в корпоративній мережі. Наступне зображення на рис. 3.4 ілюструє цей процес.

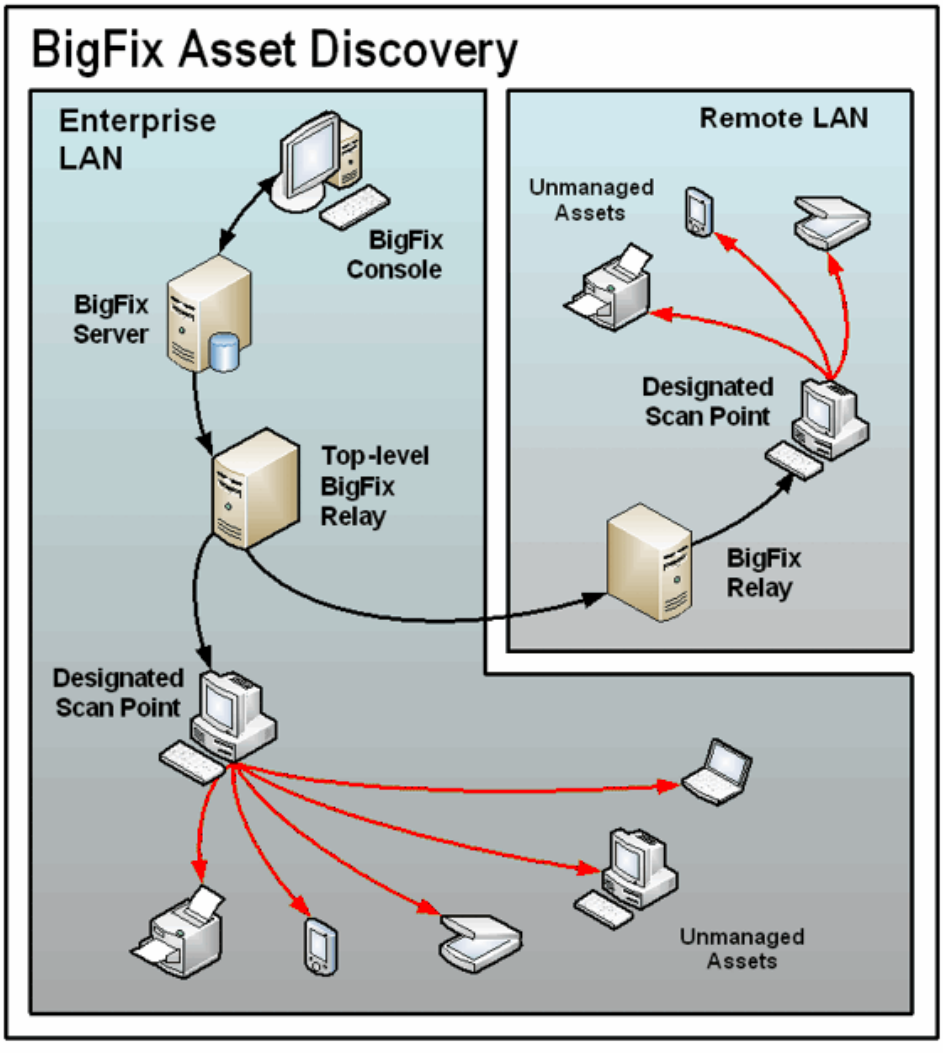

Рис. 3.4. Процес сканування некерованих активів за допомогою BigFix Asset

Discovery [13]

Інформація витягується з цих некерованих активів точками сканування і відправляється назад через реле в базу даних на сервері BigFix. Звідти оператор може ознайомитись з результатами на консолі BigFix (рис. 3.5).

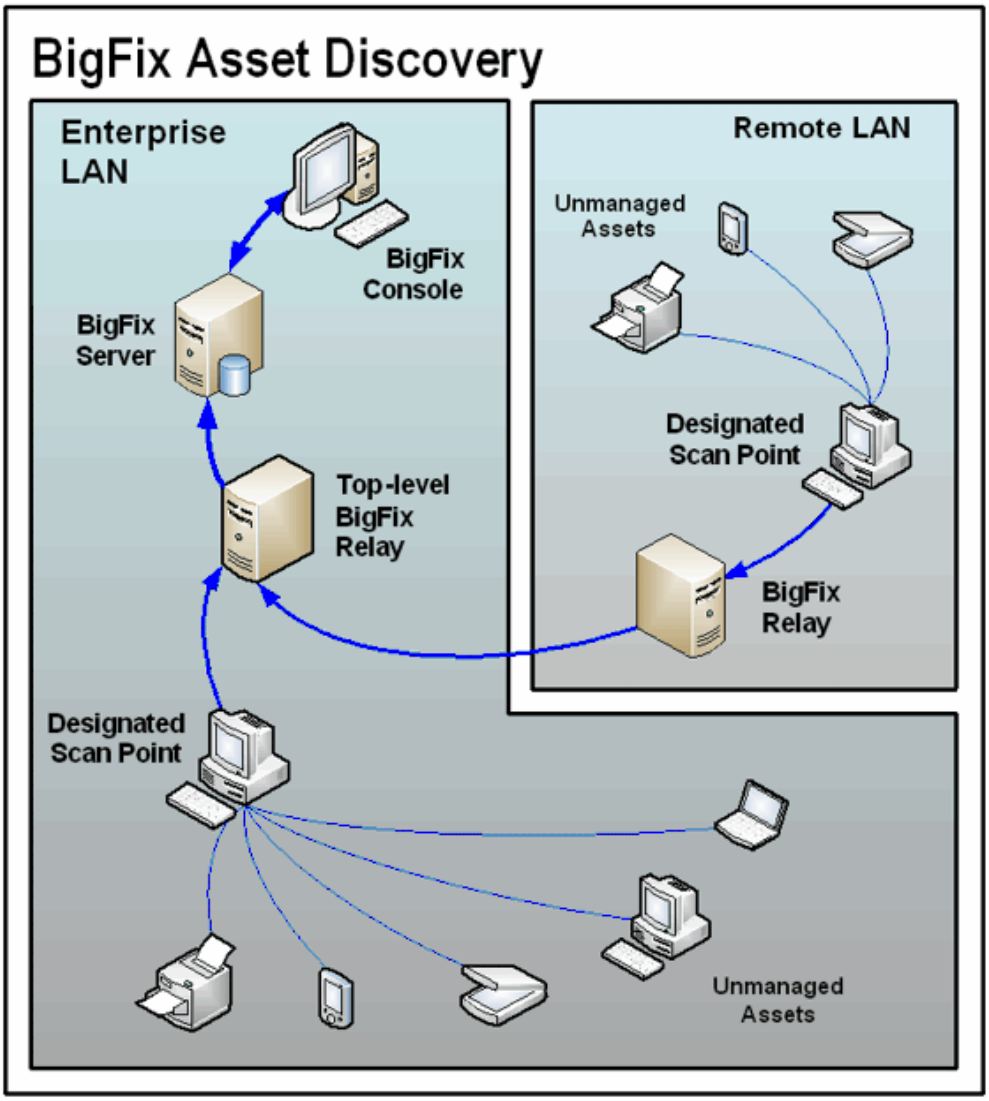

Рис. 3.5. Процеси обміну даними щодо некерованих активів [13]

Розглянемо дії, які виконує оператор з некерованими активами, отриманими з комп'ютерів Scan Point.

Після установки оператор може переглядати всю інформацію про некеровані актии, отриману комп'ютерами Scan Point.

У будь-який момент оператор може активувати статистику точок сканування, щоб переглянути інформацію про призначені точки сканування Nmap. Для цього він використовує Статистика точки сканування під вузлом

«Управління скануванням» в дереві навігації. Оператор може переглядати статистику по статусу, по сайту або по активації.

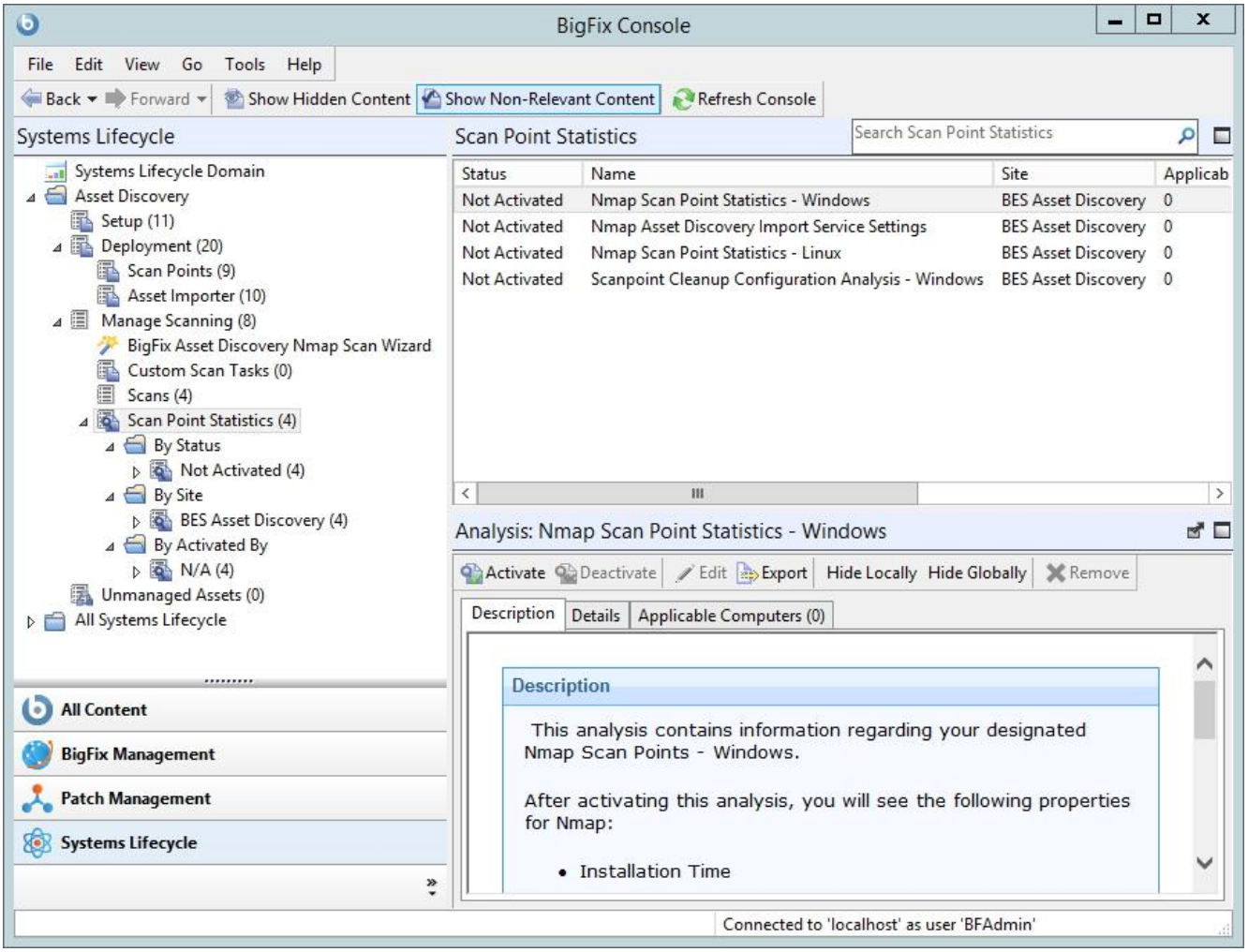

Рис. 3.6. Інтерфейс консолі BigFix [13]

Щоб списати комп'ютер Scan Point, оператор використовує завдання Remove Nmap Scan Point в вузлі Deployment. Щоб отримати доступ до завдань «Видалити точку сканування Nmap», він використовує «Точки сканування» в вузлі «Розгортання» (рис. 3.6).

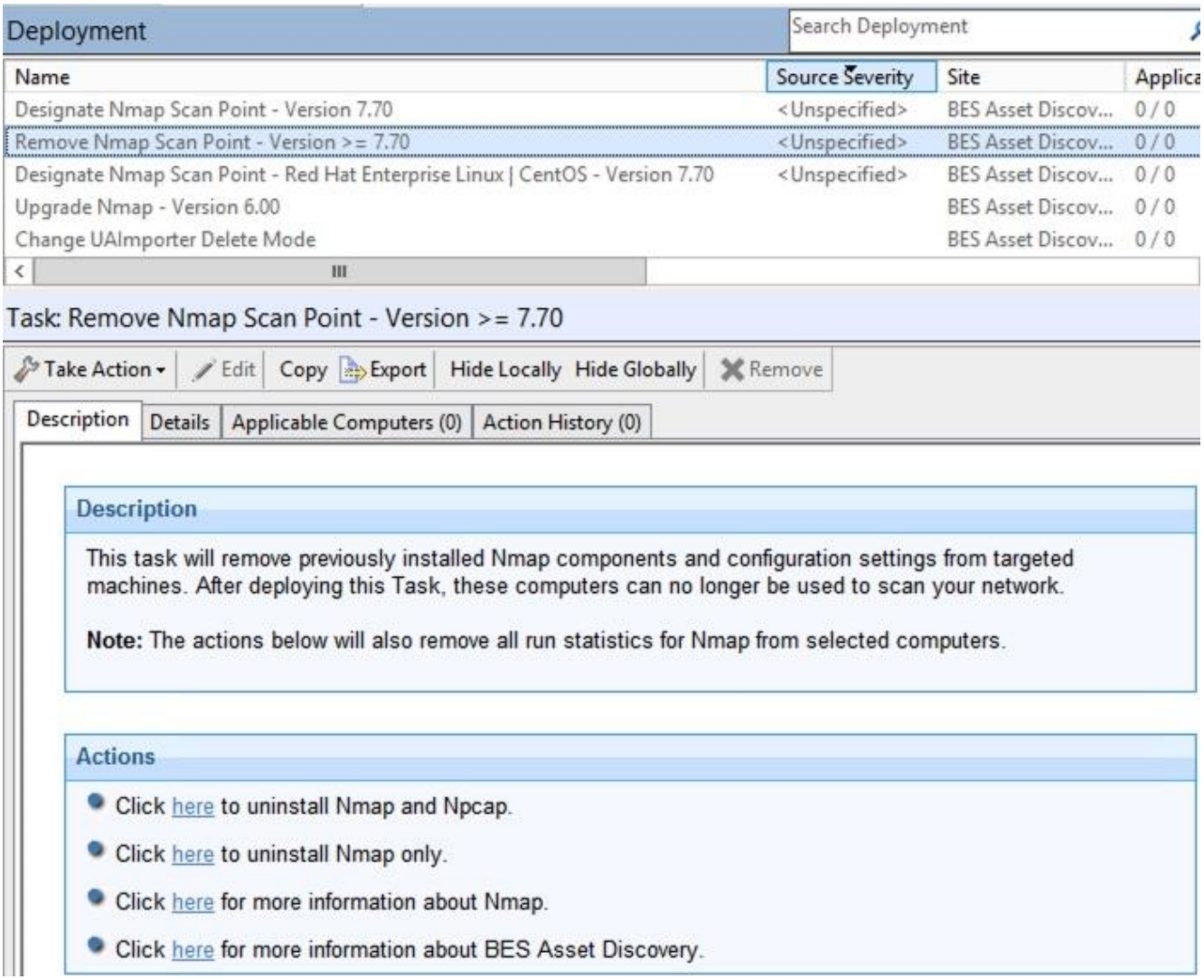

Рис. 3.7. Інтерфейс можливих Дій щодо точки сканування

Це видаляє Nmap з цієї точки сканування (рис. 3.7), а також оператор може видалити WinPcap або Npcap для останньої версії Nmap. Натискаючи поле Дії, щоб відкрити діалогове вікно «Виконати дію», і вибрати комп'ютери Scan Point, які потрібно вивести з експлуатації. Щоб видалити некерований актив, оператор використовує «Некеровані активи» в нижній частині дерева навігації.

3.3. Розроблення рекомендацій щодо застосування технології управління захистом кінцевих точок корпоративної інформаційної системи

В [14] визначено критичні компоненти платформи захисту кінцевих точок наступного покоління (NGEPP), їх роль і завдання, які вони вирішують.

Захист кінцевих точок – одна з найбільш важливих програм безпеки, яку повинні створювати організації будь-якого розміру і спрямованості. Сьогоднішній

ландшафт загроз складається з все більш різноманітного набору складних загроз і жодна кінцева точка або платформа не залишаються без уваги.

Статичні методи (антивірусні рішення), які довгий час були єдиними профілактичними заходами, більше не ефективні проти сучасних складних атак [13]. Новий підхід до захисту кінцевих точок вимагає можливостей, які охоплюють весь життєвий цикл реалізації загрози: від попереднього виконання до подальшого виконання. Крім того, технологія, що лежить в основі, повинна забезпечувати можливість не тільки ідентифікувати загрозу по її суті, а й за її поведінкою, а також забезпечувати інтелектуальне реагування на загрози в реальному часі.

Компоненти платформи захисту кінцевих точок наступного покоління (NGEPP) мають реалізовувати такі функції (рис. 3.8):

до виконання:

запобігання відомих загроз;

внесення додатків в білий і чорний списки;

при виконанні

динамічне виявлення експлойтів;

динамічне виявлення шкідливих програм;

після виконання

пом'якшення;

відновлення;

криміналістична експертиза в реальному часі.

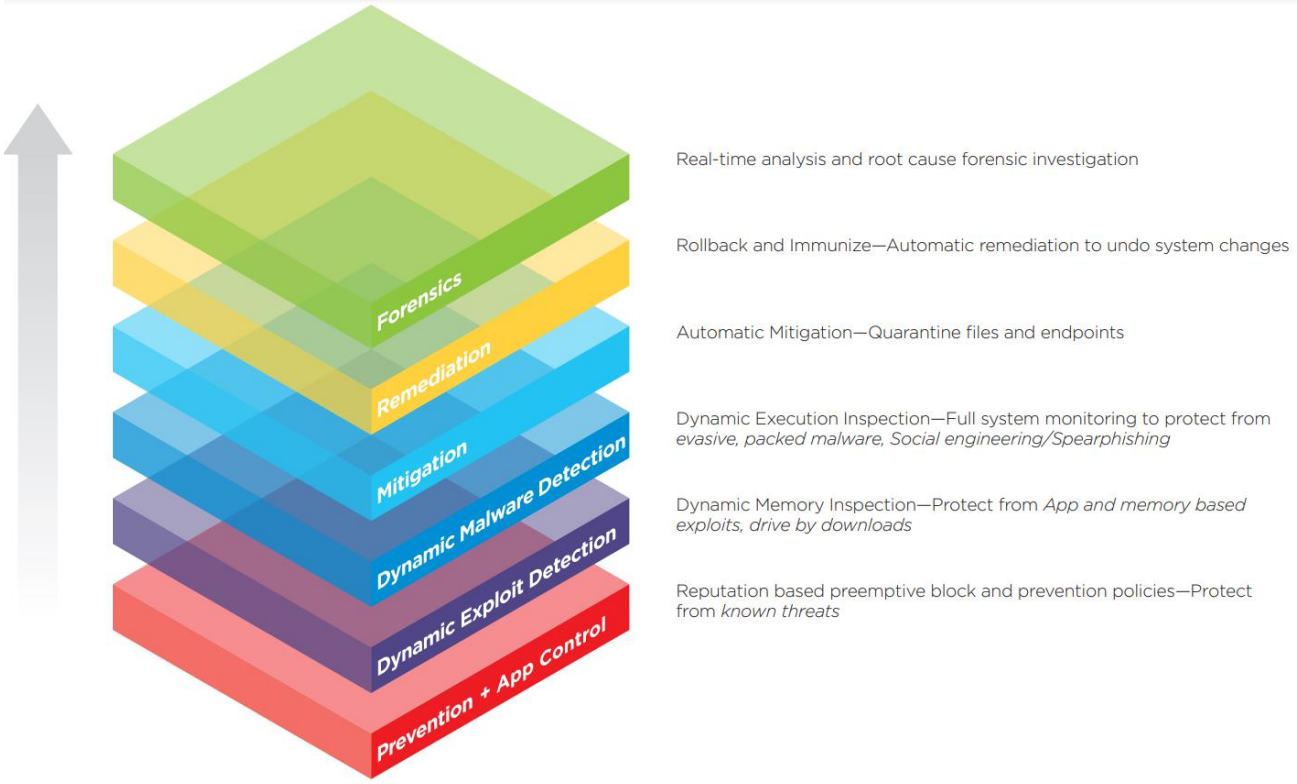

Рис. 3.8. Next Generation Endpoint Protection Platform [14]

На високому рівні рішення для захисту кінцевих точок наступного покоління повинно працювати на самому кінцевому пристрої і бути ефективним проти всіх основних векторів атак протягом всього життєвого циклу реалізації загроз (до виконання, при виконанні і після виконання).

Це вимагає аналізу поведінки і криміналістичної експертизи в режимі реального часу, а також здатності пом'якшувати і усувати загрози зі швидкістю машини.

Для захисту кінцевих точок наступного покоління необхідний принципово новий підхід, щоб зупинити просунуті шкідливі програми і загрози нульового дня, все ж є вагомі причини для використання перевірених методів для блокування відомих загроз.

Можна запобігати запуску файлового шкідливого ПЗ на цільовому пристрої кінцевої точки за умови, що підпис шкідливого файлу або хеш-код збігаються з профільованими в базі даних сигнатур служби репутації. Сьогодні організації можуть скористатися послугами репутації понад сорока провідних постачальників, підключившись до служб хмарної розвідки і скориставшись перевагами більш широкого охоплення.

Крім того, організації почали усувати недоліки свого антивірусного програмного забезпечення, впроваджуючи технології білих і чорних списків в якості додаткового рівня захисту. Ці методи об'єднуються, щоб сформувати метод грубої сили, що визначає, які програми дозволено запускати на конкретному кінцевому пристрої. Ця форма запобігання є ефективним засобом значного зменшення загальної поверхні атаки організації і змушує хакерів і кіберзлочинців старанніше працювати (і витрачати більше грошей) на проникнення в IT-інфраструктуру організації через кінцеву точку.

За сьогоднішніми стандартами, попередній захист повинен розглядатися як основа будь-якого підходу наступного покоління до захисту кінцевої точки.

Рекомендація: необхідно обирати рішення NGEPP, яке не тільки використовує служби репутації декількох постачальників для попереджувального блокування загроз, а й використовує спрощений метод індексації файлів (пасивне сканування або вибіркове сканування) замість тих, які регулярно виконують ресурсномістке сканування системи. Рішення також повинне забезпечувати функціональність управління додатками.

Невідомі загрози (часто ретельно упаковані або змінені варіанти відомих загроз) уникають статичних заходів запобігання і починають виконуватися на кінцевому пристрої. Доцільно застосовувати методи аналізу, засновані на поведінці, що є основою NGEPP. Виявлення складних загроз за допомогою поведінкового аналізу вимагає постійного моніторингу всієї активності на рівні системи на кінцевому пристрої. Такий ступінь моніторингу необхідно для створення контексту нормальної поведінки системи і додатків, що дозволяє швидко виявити серйозну загрозу.

Крім того, глибокий моніторинг активності кінцевих точок необхідний для проведення значущої і докладної криміналістичної експертизи. Як і у випадку з шкідливими програмами на основі файлів, застосування складних алгоритмів, які зіставляють підозрілі процеси з шкідливими шаблонами, забезпечує високоефективне виявлення шкідливих програм на основі пам'яті, розширених експлойтів і атак на основі внутрішніх порушників/сценаріїв.

В цілому, виявлення на основі поведінки виявилося набагато більш ефективним, ніж статичне виявлення. Крім того, воно є більш ефективним, ніж інші рішення нового покоління, в яких використовується математичне моделювання для виявлення подібності між структурою підозрілого виконуваного файлу серед різних варіантів і сімейств шкідливих програм.

Ці методи, як і раніше обмежуються шкідливими програмами на основі файлів і потрапляють в одну гру в кішки-мишки, коли зловмисники і постачальники засобів безпеки намагаються перехитрити один одного.

Рекомендація: динамічний аналіз поведінки і підхід, який не покладається виключно на попереднє знання конкретного індикатора для виявлення атаки, виявляться більш ефективними при роботі з справжніми атаками нульового дня. Атаки нульового дня рідко відображають будь-які статичні індикатори компрометації, хоча поведінка атаки в значній мірі знайома. Рішення NGEPP може динамічно виявляти загрози нульового дня і складні шкідливі програми без необхідності статичних заходів. Крім того, рішення NGEPP повинні вміти виявляти атаки, що використовують уразливості в веб-браузерах і документах, а також атаки на основі пам'яті і атаки на основі сценаріїв, які зазвичай відбуваються інсайдерами.

Після успішного виконання атаки на одній або декількох кінцевих точках організація залишається вразливою до тих пір, поки співробітники служби безпеки не зможуть повністю пом'якшити її, зупинивши її бічне поширення і видаливши з порушених пристроїв.

Кібератаки часто створюють, змінюють або видаляють системні файли і параметри реєстру, а також вносять зміни в параметри конфігурації. Ці зміни або залишки можуть викликати збої в роботі або нестабільність системи і вимагають значних зусиль для очищення без відповідних можливостей. Багато сучасних технологій орієнтовані на виявлення загрози і оповіщення про неї. Це бентежить персонал, відповідальний за реагування на інциденти, озброєний комбінацією точкових інструментів пом'якшення наслідків і криміналістичної експертизи, а також ручних процедур, за допомогою яких робляться спроби знайти і ізолювати

заражені системи.

Іноді залучаються експерти-консультанти з безпеки (за значні гроші), коли внутрішнім групам потрібна допомога в усуненні наслідків, виправленні порушених файлів або створенні та інтерпретації даних експертизи.

В кінцевому рахунку, найбільш ефективним є відповідь, при якому пом'якшення і усунення атак автоматично виконуються в початковій точці виявлення і ґрунтуються на детальних криміналістичних даних в реальному часі. Найбільш повні рішення для захисту кінцевих точок нового покоління засновані на цілісному підході інтеграції можливостей реагування з виявленням та запобіганням загроз. Це усуває будь-які потенційні проблеми взаємодії між інструментами безпеки і забезпечує максимально швидкий час відгуку.

Рекомендація: платформа NGEPP повинна підтримувати автоматичне пом'якшення наслідків на основі політик, яке є досить гнучким, щоб охопити широкий спектр сценаріїв використання. Наприклад: карантин заражених файлів, знищення шкідливих процесів, відключення заражених комп'ютерів від мережі або навіть повне відключення скомпрометованих пристроїв. Усунення наслідків повинно виконуватися своєчасно (наприклад, якщо інструменту необхідно зв’язатися з центральним сервером, щоб отримати команду пом'якшення, атака ще може встигнути поширитися вбік).

Швидке пом'якшення наслідків на початкових етапах життєвого циклу загрози зведе до мінімуму шкоду і мінімізує необхідних зусиль щодо усунення.

Рекомендація: рішення NGEPP має бути здатним легко виправляти порушені файли, відкочуючись їх до останніх відомих довірених станів.

Рекомендація: рішення NGEPP має забезпечувати повну і детальну видимість того, що сталося на кінцевій точці під час атаки в реальному часі, а також забезпечувати можливість пошуку індикаторів компрометації на кінцевих точках. Дані судової експертизи повинні бути представлені як в інтуїтивно зрозумілому графічному форматі, так і в декількох форматах файлів, сумісних з іншими інструментами безпеки, такими як SIEM.

Таким чином, з огляду на зростаюче розмаїття пристроїв і платформ захисту

кінцевих точок в поєднанні з швидко мінливим ландшафтом загроз, захист кінцевих точок стає більш актуальним і важливим, ніж будь-коли раніше. Хоча існує кілька різних підходів і рішень, які підпадають під назву «захисту кінцевих точок наступного покоління», існує чітко визначений набір критичних можливостей і атрибутів, необхідних для реалізації в NGEPP для найкращого обслуговування сучасних корпоративних організацій.

Рішення повинно працювати в спрощеному режимі на самій кінцевій точці, захищати кілька платформ і бути ефективним проти всіх основних векторів атак на протязі всього життєвого циклу реалізації загроз. Воно повинно запобігати відомим загрозам, використовувати динамічне виявлення загроз на основі поведінки, інтелектуально пом'якшувати і усувати загрози в реальному часі, а також генерувати докладну криміналістичну експертизу.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми забезпечення захисту кінцевих точок як складової частини корпоративної інформаційної системи, встановлена сутність завдань їх захисту. Встановлено сутність та зміст управління захистом кінцевих точок корпоративної інформаційної системи.

Проаналізовано існуючі технології управління захистом кінцевих точок корпоративної інформаційної системи. Досліджена технологія управління захистом кінцевих точок корпоративної інформаційної системи на базі платформи HCL BigFix.

Визначено методи та засоби забезпечення управління корпоративними кінцевими точками, які реалізовані в HCL BigFix.

Встановлено основні функції та принципи роботи платформи HCL BigFix. Платформа HCL BigFix – це набір продуктів, який забезпечує швидке та інтуїтивно зрозуміле рішення для управління відповідністю, кінцевими точками і безпекою та дозволяє організаціям бачити і управляти фізичними і віртуальними кінцевими точками за допомогою єдиної інфраструктури, єдиної консолі і одного типу агента.

Досліджено типову архітектуру рішення HCL BigFix, яка надає уявлення про середовище платформи та можливість її правильного планування застосування.

У роботі запропоновано варіант технології управління захистом кінцевих точок корпоративної інформаційної системи на платформі HCL BigFix. для цього було розглянуто приклад робочого процесу оператора консолі HCL BigFix.

У роботі розглянута технологія управління активами корпоративної інформаційної системи на базі BigFix Asset Discovery.

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

Таким чином, правильна реалізація технології управління захистом

кінцевих точок корпоративної інформаційної системи на платформі HCL BigFix має забезпечити ефективний захист корпоративних даних та кібербезпеку корпоративної інформаційної системи підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Брюске, Д.Я., Савельев, А.Ю. Архитектура корпоративных информационных систем (web-формат) [Электронный ресурс. Мультимедиа]. Учебное пособие. Тамбов. Издательство ФГБОУ ВО "ТГТУ", 2018.

2. Моделі і методи проектування інформаційних систем. Проектування інформаційних систем. Архітектура інформаційних систем [Електронний ресурс] – Режим доступу: https://elearning.sumdu.edu.ua/free_content/lectured:de1c9452f2a161439391120eef364dd8ce4d8e5e/20151220200610/170352/index.html#p1.

3. Томашевський О.М. Інформаційні технології та моделювання бізнес-процесів: навч. посіб. / О.М. Томашевський, Г.Г. Цегелик, М.Б. Вітер, В.І. Дубук // – К. : ЦУЛ, 2012. – 296 с..

4. Misty Blowers. Evolution of Cyber Technologies and Operations to 2035. Advances in Information Security. Springer International Publishing Switzerland 2015. – 201 p.

5. Lee Neely. Endpoint Protection and Response: A SANS Survey. June 2018 [Електронний ресурс] – Режим доступу: https://www.sans.org/reading-room/whitepapers/analyst/endpoint-protection-response-survey-38460.

6. Алексей Матвеев. Обзор рынка систем защиты конечных точек (Endpoint Protection Platform) [Електронний ресурс] – Режим доступу: https://www.anti-malware.ru/analytics/Market_Analysis/endpoint-protection-platform.

7. HCL BigFix. Seven Must-have Endpoint Management Capabilities. September 2019. Author: Dave Gruber, Senior ESG Analyst [Електронний ресурс] – Режим доступу: https://www.ciosummits.com/ESG-Solution-Showcase-HCL-Sept-2019.pdf.

8. What is CrowdStrike? Falcon Platform FAQ [Електронний ресурс] – Режим доступу: https://www.crowdstrike.com/endpoint-security-products/crowdstrike-falcon-faq/.

9. Trend Micro. Smart protection suites. Maximum Trend Micro XGen™ security

from your proven security partner [Електронний ресурс] – Режим доступу: https://www.trendmicro.com/ru_ru/business/products/user-protection/sps.html.

10. Traps Endpoint Security Manager [Електронний ресурс] – Режим доступу: https://docs.paloaltonetworks.com/traps.html.

11. HCL Software. Product Documentation. BigFix [Електронний ресурс] – Режим доступу: https://help.hcltechsw.com/bigfix/10.0/platform/Platform/Getting_Started/c_ibm_endpoint_manager_getting_started.html.

12. HCL Software. BigFix. A sample console operator's workflow [Електронний ресурс] – Режим доступу: https://help.hcltechsw.com/bigfix/10.0/platform/Platform/Console/c_operating_basics.html.

13. BigFix. Asset Discovery User's Guide [Електронний ресурс] – Режим доступу: https://help.hcltechsw.com/bigfix/10.0/platform/pdf/BigFix_Asset_Discovery_Users_Guide.pdf.

14. SentinelOne. Next-Generation Endpoint Protection [Електронний ресурс] – Режим доступу: https://www.infosecpartners.com/wp-content/uploads/2017/02/NextGenEndpointProtection_041816.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)