ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ РОЗШИРЕНОГО ЗАХИСТУ КОРПОРАТИВНИХ КІНЦЕВИХ ТОЧОК ВІД ЗАГРОЗ НА БАЗІ FORTIEDR»

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

КИЇВ – 2021

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

APIs – Application Programming Interfaces

APT – Advanced Persistent Threat

DNS – Domain Name System

EDR – Endpoint Detection and Response

EPP – Endpoint Protection Platform

IDS – Intrusion Detection System

IoC – Indicator of Compromise

IoT – Internet of Things

IP – Internet Protocol

IPsec – IP security

SaaS – Software as a Service

SOC – Security Operations Center

VPN – Virtual Private Networks

ВСТУП

Актуальність дослідження. Мережі підприємств та організацій, їх інформаційні ресурси всередині повинні бути захищені через можливі атаки зі шкідливих джерел. Типи мережевих атак з часом еволюціонували від пасивного перехоплення даних до активних типів атак, які є більш руйнівними та згубними. Для підвищення безпеки корпоративної мережі спеціалісти застосовують кілька стратегій захисту всіх частин мережі, особливо кінцевих точок. Пристрої в кінцевих точках мережі, що переходять до Інтернету, мають найбільш вразливі шляхи атаки.

Популярним підходом до безпеки кінцевих точок є використання як підходів попередження, так і підходів виявлення. Платформи захисту кінцевих точок (EPP) є запобіжними системами, які ідеально підходять проти великих обсягів загроз від шкідливого програмного забезпечення, включаючи програм-вимагачів. Однак, якщо атака зможе обійти брандмауер та інші системи EPP, загроза може не зафіксуватися. Система виявлення та реагування на кінцевій точці (EDR) забезпечує наступний рівень захисту, оскільки запобігання не може забезпечити повний захист мережі.

Рішення EDR – це програмні системи, розгорнуті для захисту комп'ютерних пристроїв у кінцевих точках мережі. Програми або агенти збирають дані з пристроїв кінцевих точок та аналізують їх для виявлення, ідентифікації та розкриття потенційних загроз та проблем. Програмне забезпечення EDR постійно контролює пристрій, і коли виявляється підозра на загрозу, воно негайно попереджає персонал безпеки, як правило, набором рекомендованих дій. Засоби EDR можуть бути інтегрованими або бути компонентом систем збору інформації про безпеку та управління подіями (SIEM).

EDR система покращує видимість завдяки постійному моніторингу та фіксації діяльності та подій, що відбуваються в кінцевих точках. Іншими важливими особливостями рішень EDR є пошук і розслідування даних про події, виявлення та перевірка підозрілої діяльності, сортування попереджень, пошук

загроз або дослідження даних, а також автоматизовані дії для припинення шкідливої діяльності. Можливості розвідки загроз та хмарні рішення – це деякі сучасні функції, які зараз пропонують постачальники технологій EDR.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження методів та засобів забезпечення розширеного захисту корпоративних кінцевих точок від загроз.

Об'єкт дослідження – розширений захист корпоративних кінцевих точок від загроз.

Предмет дослідження – технологія розширеного захисту корпоративних кінцевих точок від загроз.

Мета роботи – розробити порядок застосування технології розширеного захисту корпоративних кінцевих точок від загроз та рекомендації щодо його реалізації.

Наукові завдання:

проаналізувати сучасні загрози корпоративним кінцевим точкам;

проаналізувати існуючі підходи до захисту корпоративних кінцевих точок;

проаналізувати функціональність рішень класу EDR;

дослідити існуючі методи та засоби розширеного захисту корпоративних кінцевих точок від загроз на базі FortiEDR;

розглянути варіанти застосування рішення FortiEDR;

розробити рекомендації щодо розширеного захисту корпоративних кінцевих точок від загроз.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів полягає в розробці рекомендацій щодо застосування методів та засобів забезпечення розширеного захисту корпоративних кінцевих точок від загроз.

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

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ КОРПОРАТИВНИХ КІНЦЕВИХ ТОЧОК ВІД ЗАГРОЗ

1.1. Аналіз сучасних загроз корпоративним кінцевим точкам

Новою тенденцією сучасних цілеспрямованих атак є обрання зловмисниками в якості своїх жертв не тільки великі організації, а й цілі поменше і все частіше використовують малі організації в ланцюжку атаки на великі компанії. Зловмисники стають більш акуратними до витрат на підготовку атак і прагнуть якомога сильніше мінімізувати витрати, внаслідок чого вартість організації ефективної цілеспрямованої атаки значно знижується, та, відповідно, зростає і загальна кількість атак в світі [1].

У комплексних атаках, спрямованих на конкретні організації, застосовуються: мультівекторний підхід до проникнення, пошук вразливих місць в інфраструктурі, ретельне вивчення існуючих засобів захисту з метою їх обходу, використання спеціально розробленого або модифікованого шкідливого коду, застосування соціальної інженерії, шифрування і подальшої обфускації для виключення ймовірності виявлення [1].

За даними звіту про сучасний ландшафт загроз SANS 2017 Threat Landscape Survey: Users on the Front Line (рис.1.1) [1]:

74% респондентів назвали одним з поширених способів проникнення шкідливих об'єктів в організацію є заражені посилання в тілі електронних листів або виконувані шкідливі файли, що поширюються в вигляді вкладень;

48% респондентів виділили активацію шкідливого коду з заражених веб-сайтів або самостійне завантаження шкідливих файлів при відвідуванні веб-сторінок;

30% вказали на вразливості додатків на кінцевих точках користувача тощо.

За даними цього ж звіту [1], 81% опитаних компаній вважають, що *засоби захисту кінцевих точок стають найбільш затребуваними інструментами*. Спостерігаючи за еволюцією загроз від масових до спрямованих, ми бачимо

потребу в додаванні до автоматичного блокування простіших загроз, просунуте виявлення спрямованих складних загроз і в цілому перебудування ринку і зміні фокусу від захисту окремих робочих місць до забезпечення безпеки цілого підприємства із залученням не тільки фахівців IT -департамента, а й фахівців з інформаційної безпеки і аналітиків для подальшого розслідування інцидентів, оперативного реагування та пошуку новітніх загроз.

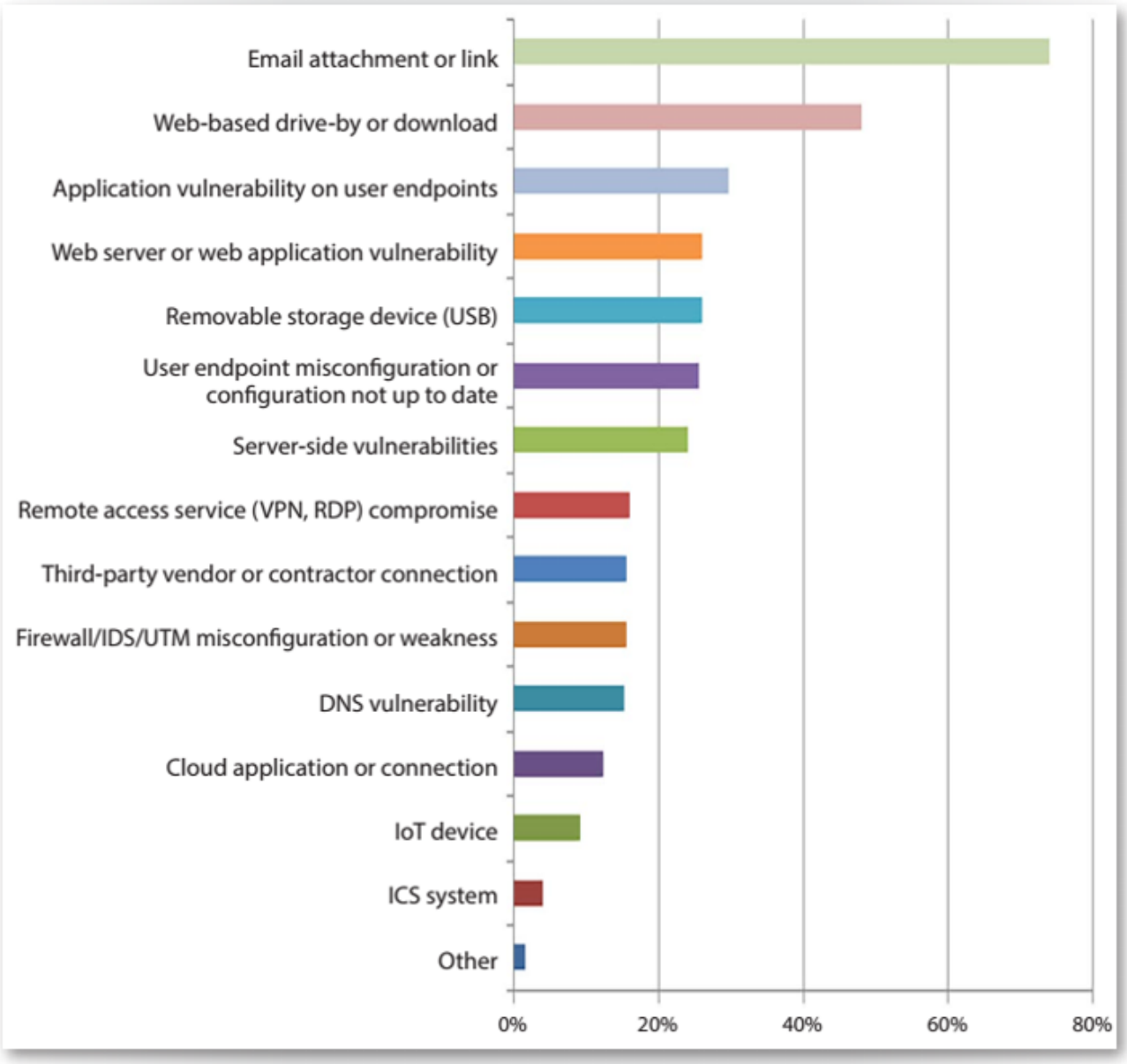

Рис. 1.1. Vectors Threats Use to Enter Organizations, SANS 2017 Threat Landscape Survey: Users on the Front Line

Розглянемо більш докладно ключові тенденції розвитку загроз, що зачіпають кінцеві точки мережі.

Зростання *безфайлових (fileless) атак*. Безфайлові атаки – це атаки, які не

розміщують ніяких файлів на жорсткому диску. Відстежити такого роду активності на порядок складніше.

Зловмисники можуть використовувати експлойти, макроси, скрипти і легітимні інструменти. Можна виділити кілька видів безфайлові атак: розміщення в оперативній пам'яті; збереження в реєстрі Windows; використання довіреного програмного забезпечення: інструментів Windows, різних додатків тощо для отримання облікових даних цільових систем для шкідливих цілей; атаки з використанням скриптів [1].

З кожним роком імовірність зіткнення з спрямованими атаками на кінцевих точках для організацій збільшується. Замість установки шкідливих виконуваних файлів, які антивірусні движки можуть без проблем оперативно знаходити і блокувати, зловмисники використовують різні комбінації із застосуванням безфайлових методів, заражаючи кінцеві точки і не залишаючи при цьому артефактів, які можна було б виявити в ста відсотках випадків антивірусом [1].

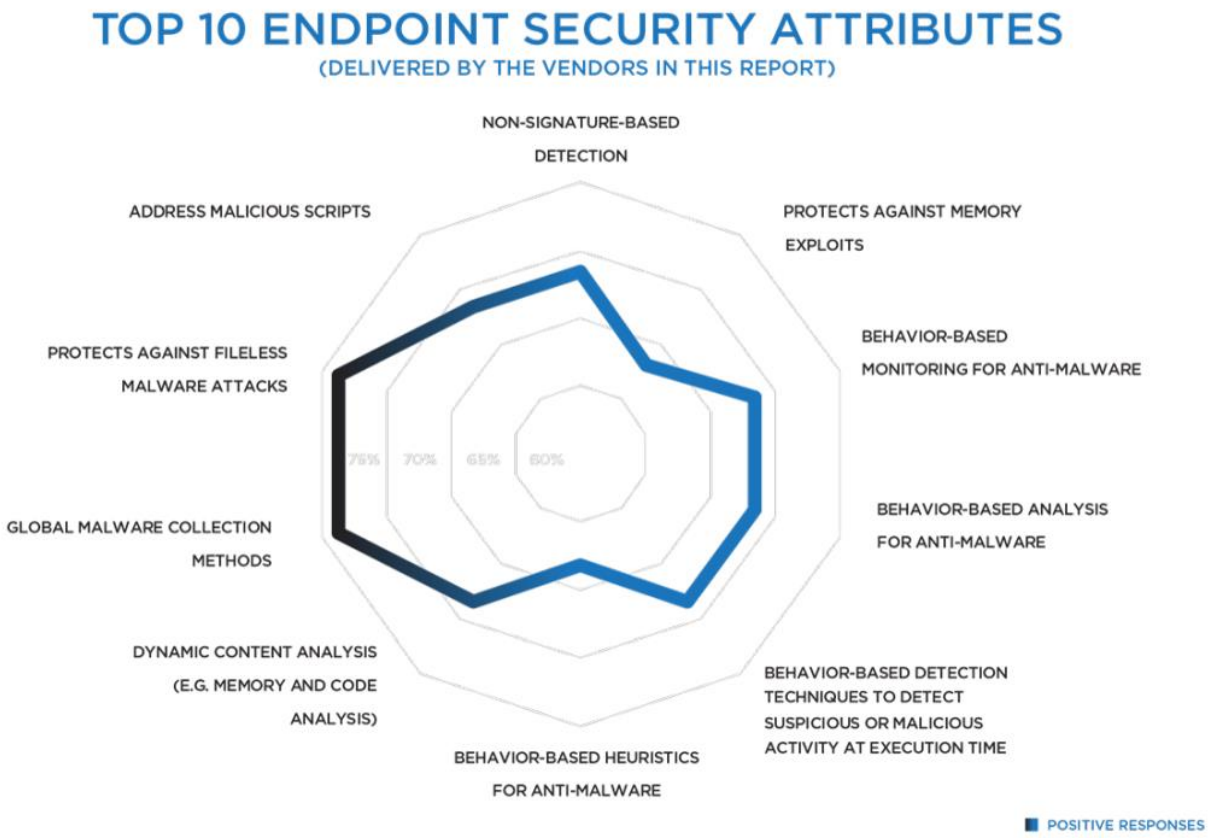

Рис. 1.2. Top 10 Endpoint security attributes, CISOs Investigate: Endpoint Security by Security Current, 2017

Опитування CISOs Investigate: Endpoint Security by Security Current, в якому були включені відгуки керівників з інформаційної безпеки, які вже використовують рішення просунутого захисту кінцевих точок або тільки планують, а також відповіді проанкетованих виробників цих рішень показали, що протидія безфайловим атакам на кінцевих точках є одним з головних атрибутів інформаційної безпеки, на який варто звернути особливу увагу [1].

За даними опитаних організацій, 29% нападів, з якими вони зіткнулися протягом 2017 року, були безфайлові, що на 9% більше, ніж роком раніше. New Ponemon Institute прогнозують, що ця пропорція продовжить рости, і в 2018 році безфайлові атаки складуть 35% від загальної кількості всіх прогнозованих атак.

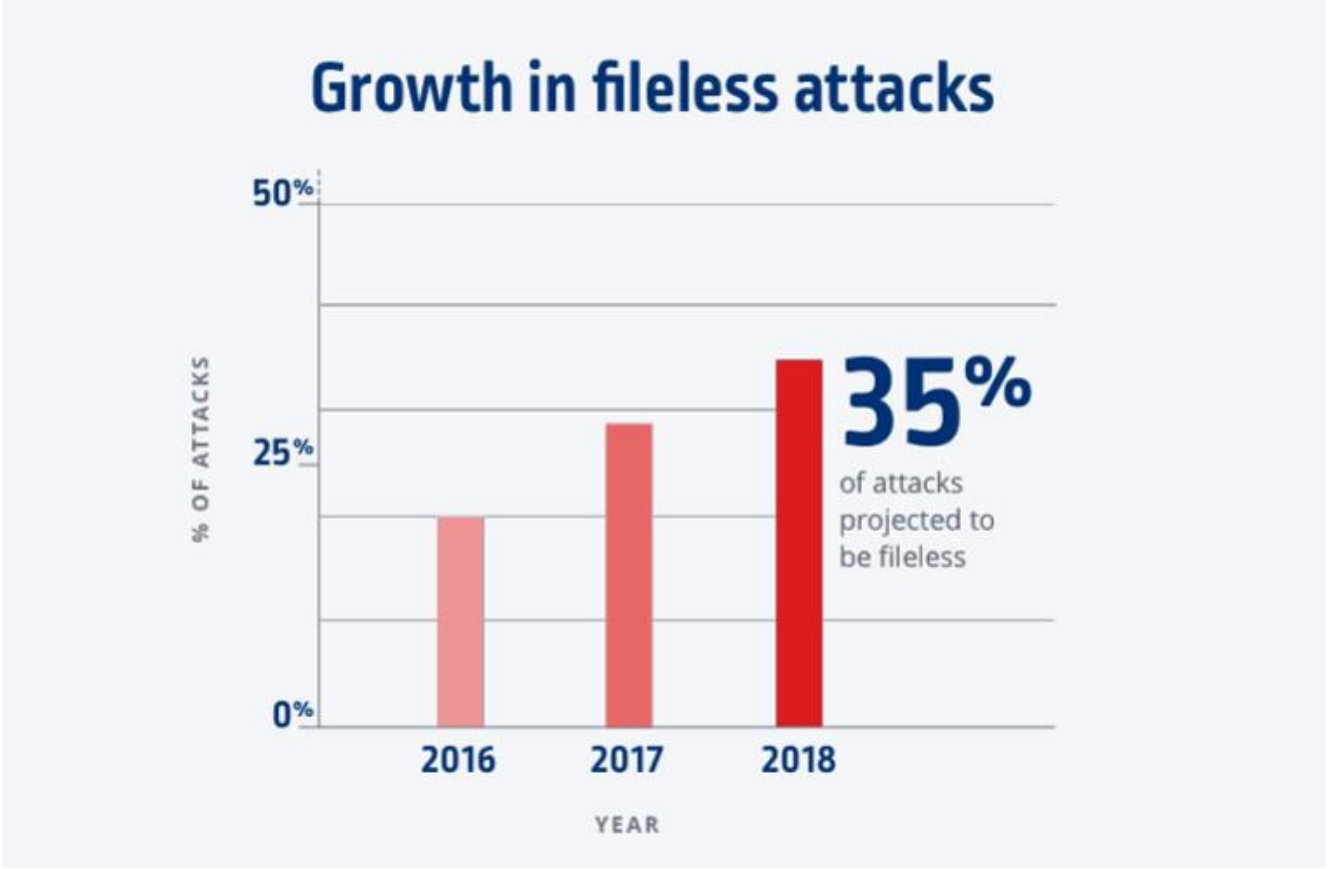

Рис. 1.3. Графік зростання безфайлових атак, New Ponemon Institute 2017

Тобто існує гостра потреба в додатковому захисті кінцевих точок.

Велика кількість успішних безфайлових атак ще більше підриває довіру організацій до їх існуючих захисних засобів. Згідно зі звітом аналітичного агентства Forrester на замовлення Google за 2017 рік Rethink Enterprise Endpoint Security In The Cloud Computing Era, більше половини світових підприємств (53%)

зіткнулися протягом року щонайменше з одним фактом компрометації або порушенням на стороні кінцевих пристроїв, незважаючи на використання технологій захисту. Варто зазначити, що понад три чверті оприлюднених випадків на інфраструктурі, пов'язаних з компрометацією, стосувалися безфайлових методів [1].

Проведене глобальне дослідження також показало, що підприємства почали активно розглядати просунуті інструменти з виявлення та аналітиці складних загроз на кінцевих точках. 48% компаній вважають пріоритетним для себе підвищити ефективність виявлення складних загроз на кінцевих точках, а 42% планують поліпшити аналітику (рис. 1.4). В результаті все більше організацій починають замислюватися про додаткові інвестиції в нові просунуті технології по захисту кінцевих точок, в рішення класу EDR [1].

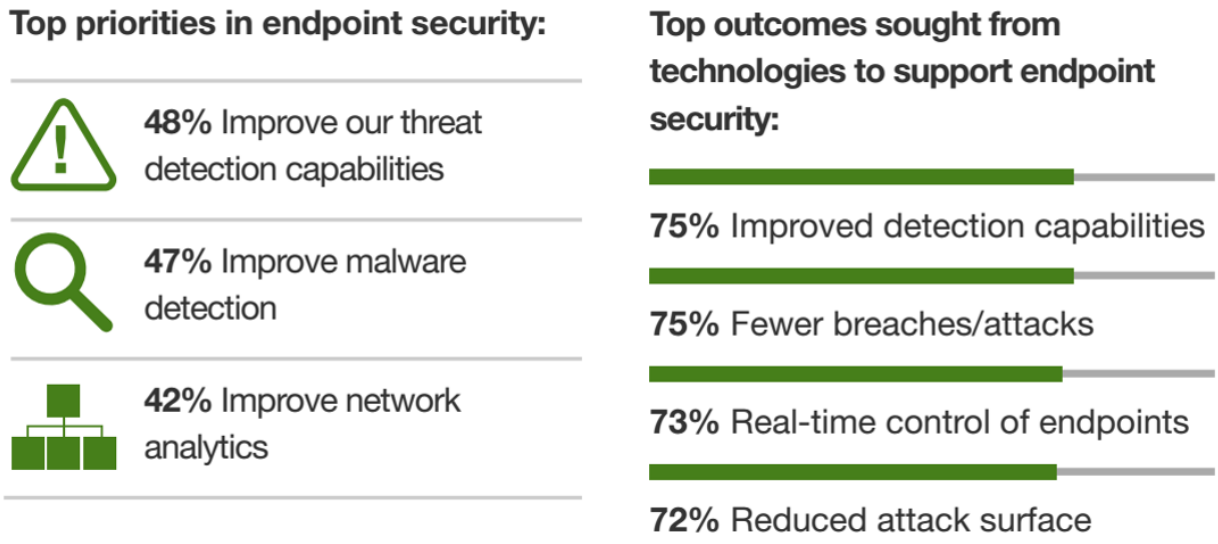

Рис. 1.4. Дані з пріоритетних напрямів захисту кінцевих точок, Rethink Enterprise Endpoint Security In The Cloud Computing Era, Forrester 2017

Відмічається зростання вартості і складності захисту кінцевих точок. Контроль всіх кінцевих точок, що взаємодіють з ресурсами компанії, стає все більш складним процесом, оскільки їх кількість і різноманітність зростає з величезною швидкістю. Майже три з чотирьох респондентів (73%) дослідження New Ponemon Institute відзначили, що для їх організації стало більш складним і трудомістким процесом контролювати кінцеві точки, і при цьому лише третина респондентів вказали, що вони володіють достатньою кількістю власних ресурсів для

моніторингу та управління робочими станціями і серверами і ще менше для розслідування інцидентів та оперативного реагування.

Також існує очевидний брак кваліфікованих фахівців з реагування на інциденти і відсутність у багатьох компаній власних експертів, що змушує вдаватися до сторонньої допомоги для ліквідації наслідків атак.

Компанії, що планують використовувати функціональність по виявленню складних загроз на кінцевих точках, стикаються з тим фактом, що значна частина з них не володіє необхідними знаннями та ресурсами для повномасштабного розгортання EDR-рішення або його належного використання. Перехід від простого адміністрування IT-відділом рішень EPP до необхідності залучення відповідних ресурсів IT-безпеки при використанні EDR-рішень призводить до потреби в інженерах з безпеки і аналітиків загроз з достатнім рівнем знань і досвіду, щоб забезпечити максимальну користь від впровадження EDR. Це можуть бути внутрішні навчені співробітники або залучені експерти в рамках різних сервісів, які розуміють, як отримати вигоду з платформи EDR і організувати ефективний процес реагування на інциденти [1].

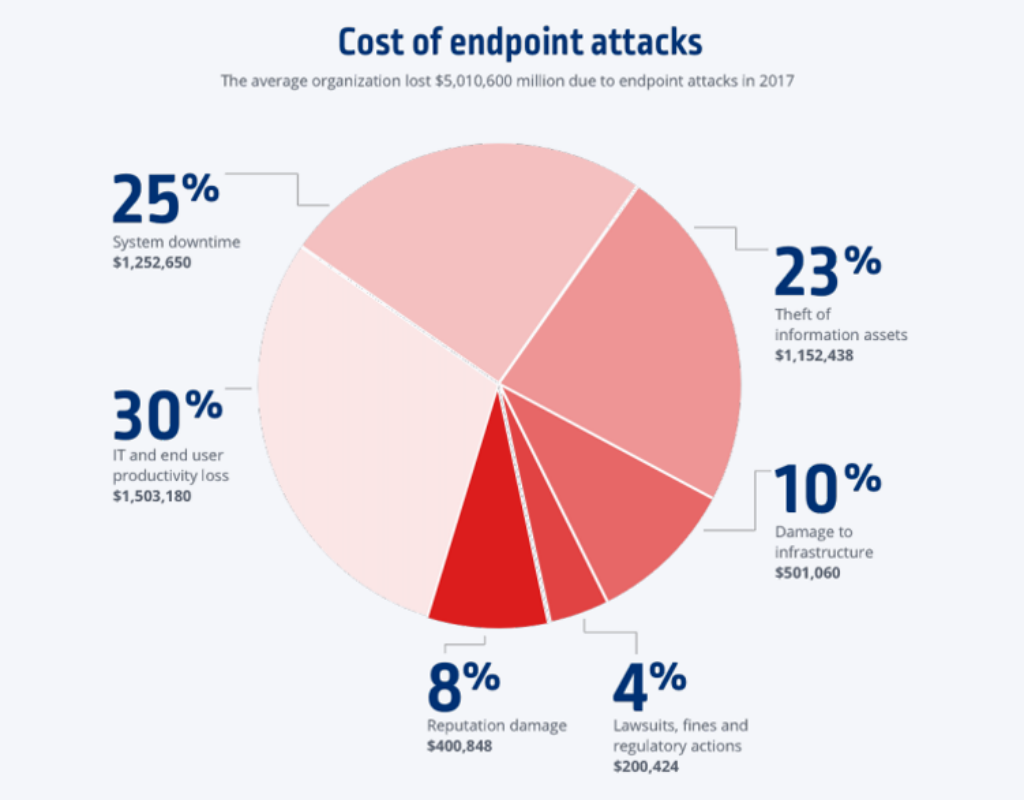

Рис. 1.5. Вартість атак на кінцеві точки мережі, New Ponemon Institute 2017

Відмічається зростання збитків від атак на кінцеві точки Виходячи з цифр, які надає нам New Ponemon Institute [1], в середньому за 2017 рік компанії втратили через успішних атак, в яких зловмисники обійшли існуючі системи безпеки кінцевих точок, в цілому більше 5 мільйонів доларів (середня вартість 301 долар США на одного співробітника), що є значною цифрою і говорить про те, що сучасні компанії потребують перегляду своєї стратегії захисту кінцевих точок.

1.2. Аналіз існуючих підходів до захисту корпоративних кінцевих точок

У разі кібератак, основною метою яких є крадіжка даних, тимчасова проблема в деякій мірі вирішується за допомогою рішень EDR першого покоління. Такі атаки непомітно переміщуються, щоб зібрати інформацію, скласти карту мережі і визначити місцезнаходження цінних активів – процес, який може зайняти тижні. При боротьбі з подібними загрозами для запобігання крадіжки даних багато керівників з інформаційної безпеки вважають достатнім час виявлення та реагування близько 24 годин або навіть декількох днів [10].

Навпаки, метою інших атак, таких як програми-вимагачі, є не крадіжка даних, а саботаж. Ці швидкодіючі загрози виконуються за хвилини і навіть секунди, що значно скорочує часові рамки. Наприклад, вимагачу WannaCry треба було всього кілька секунд, щоб зашифрувати файли і поширитися по всьому світу, заразивши 150 країн і більше 200 000 комп'ютерів за 24 часа [10].

Інший приклад – NotPetya, кіберзброя, замаскована під програму-вимагач, але призначене для знищення. Атака сталася набагато швидше, ніж будь-яка команда безпеки могла б вручну відреагувати і стримати за допомогою рішень EDR першого покоління. Все, що не пов'язане з блокуванням в реальному часі, збільшує ризик успішної атаки для організації [10].

Для багатьох організацій все актуальнішим стає питання перегляду стратегії захисту кінцевих точок. Традиційних засобів вже стає недостатньо для протидії сучасним кіберзагрозам.

Дедалі гострішою проблемою для багатьох організацій з різних сфер діяльності стає ймовірність зіткнення з цілеспрямованими атаками, які все частіше

застосовують поєднання поширених загроз, вразливостей нульового дня, унікальних схем без використання шкідливого програмного забезпечення, безфайлових методів та ін. Використання рішень, побудованих на базі превентивних технологій, а також систем, націлених точково на виявлення складних шкідливих активностей тільки в мережевому трафіку, *не може бути достатнім для захисту підприємства від складені цілеспрямованих атак* [1].

Кінцеві точки, включаючи робочі станції, ноутбуки, сервери і смартфони, також є критично важливими об'єктами контролю, так як вони залишаються для зловмисників в більшості випадків досить простими і популярними точками проникнення, що підвищує значущість контролю за ними.

Платформи захисту кінцевих точок (Endpoint Protection Platform – EPP), які зазвичай присутні в інфраструктурі у більшості організацій, відмінно захищають від масових, відомих, а також і ряду невідомих загроз, але в більшості випадків, побудованих на базі шкідливих програм, які вже раніше зустрічалися [1].

Згодом техніки нападу кіберзлочинців зазнали значних змін. Зловмисники стали агресивніші в своїх атакуючих підходах і більш досконалі в організації всіх етапів процесу. А тому велика кількість компаній, не дивлячись на використання рішень щодо захисту кінцевих точок (EPP), все ж піддаються компрометації [1].

Це означає, що *сьогодні організаціям вже необхідні додаткові інструменти*, які допоможуть їм ефективно виявляти нові, більш складні загрози, з якими вже не в змозі впоратися традиційні засоби захисту, з самого початку не розробляються проти подібного роду загроз. Ці засоби захисту хоча і виявляють інциденти на кінцевих точках, але зазвичай не здатні визначити, що надходять попередження можуть бути складовими частинами більш небезпечною і складної схеми, яка може спричинити за собою значимий для організації збиток [1].

Сучасний захист кінцевих точок потребує адаптації до існуючого ландшафту складних загроз і повинен включати функціональність по виявленню комплексних атак, спрямованих на кінцеві точки, і бути здатним оперативно реагувати на знайдені інциденти (Endpoint Detection and Response – EDR).

Очікуваним результатом від впровадження EDR-рішення щодо протидії складним загрозам буде організація передового захисту кінцевих пристроїв, що призведе до помітного зменшення поверхні комплексних цільових атак і тим самим до скорочення загального числа кіберзагроз.

Незважаючи на популярність традиційних засобів захисту кінцевих точок, багато організацій проте розглядають і додають нові технологічні можливості поверх своїх EPP-рішень, щоб підвищити якість виявлення складних загроз і прискорити процес реагування на них, зменшуючи тим самим ймовірність виникнення успішних атак і руйнівного впливу на бізнес [1].

Як ми бачимо, в забезпеченні безпеки кінцевих точок на ринку присутні дві різні категорії засобів: запобігання/блокування загроз (EPP) і розширене виявлення і реагування (EDR). Об'єднуючим елементом цих рішень, в більшості випадків, виступає антивірусний движок, який для систем класу EPP працює в режимі блокування, а для EDR служить одним з двигунів, орієнтованим на виявлення складних загроз в комплексі з іншими детектуючих механізмами, такими як: IoC-сканування, Yara-правила, пісочниця (підтримують не всі виробники в рамках своїх EDR-рішень), доступ до Threat Intelligence та ін.

Окремо варто відзначити, що в рішеннях класу EPP включена ще функціональність з контролю додатків і пристроїв, веб-контролю, оцінці вразливостей, патч-менеджменту, URL-фільтрації, шифрування, межсетевому екранування і ін.

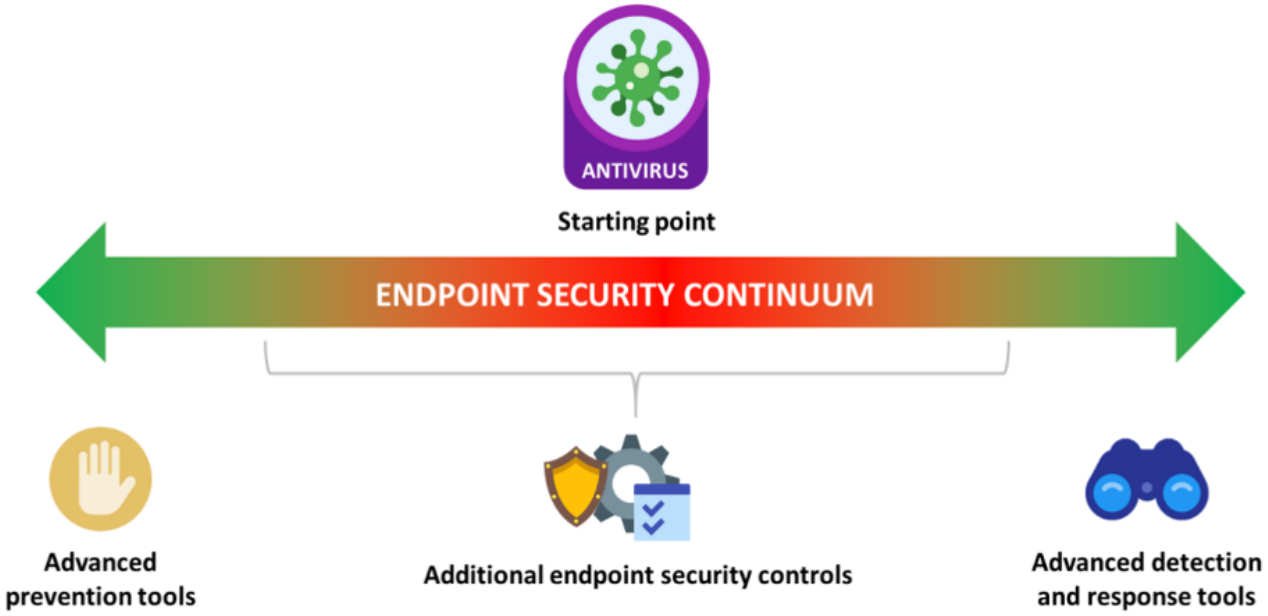

Рис. 1.6. The Endpoint Security Continuum, ESG: Redefining Next-generation Endpoint Security Solutions

Як ми бачимо, кожна з систем EPP і EDR сполучає у собі те, що відсутнє (або частково присутно) в іншій системі і що безумовно призводить до необхідності і важливості взаємодії цих рішень. У EPP і EDR є спільна мета з протидії загрозам, для досягнення якої ці продукти використовують різні підходи та функціональні можливості. Синергія використання цих рішень веде до загального більш глобального підходу захисту кінцевих точок [1].

У момент появи повнофункціональних самостійних систем класу EDR ринок рішень щодо захисту кінцевих точок був розділений на постачальників, які забезпечують автоматичне запобігання, і на тих, які забезпечують просунуте виявлення і реагування. Хоча варто відзначити, що у пари-трійки вендорів на той момент в портфелі вже були присутні обидва класи рішень – і EPP, і EDR, але позиціонувалися вони як зовсім окремі продукти [1].

Згодом відбулися зміни, і більшість постачальників почали об'єднувати свої підходи в забезпеченні як просунутого виявлення, так і запобігання.

Ринок рішень даного класу активно розвивається і формується. Деякі з постачальників рішень класу EPP випустили власні нові продукти класу EDR для отримання повної картини щодо захисту кінцевих пристроїв, інші просто допрацювали рішення для надання можливості взаємодії зі сторонніми

постачальниками, як EPP, так і EDR-рішень відповідно. Тенденція об'єднання рішень EPP і EDR гарна для споживачів цих технологій і, найімовірніше, продовжить розвиватися в цьому напрямку, що має привести до більш глибокої взаємодії цих рішень.

Ринок все ще перебуває на стадії формування. За прогнозом аналітичного агентства Gartner, беручи до уваги зростаючу потребу в швидкому й ефективному виявленні та оперативному реагуванні на передові загрози на кінцевих точках, ринок EDR-рішень буде стрімко рости. В даний час агенти EDR-рішень встановлені приблизно на 40 мільйонах кінцевих точок (менш ніж у 6% від загальної бази кінцевих пристроїв) [1].

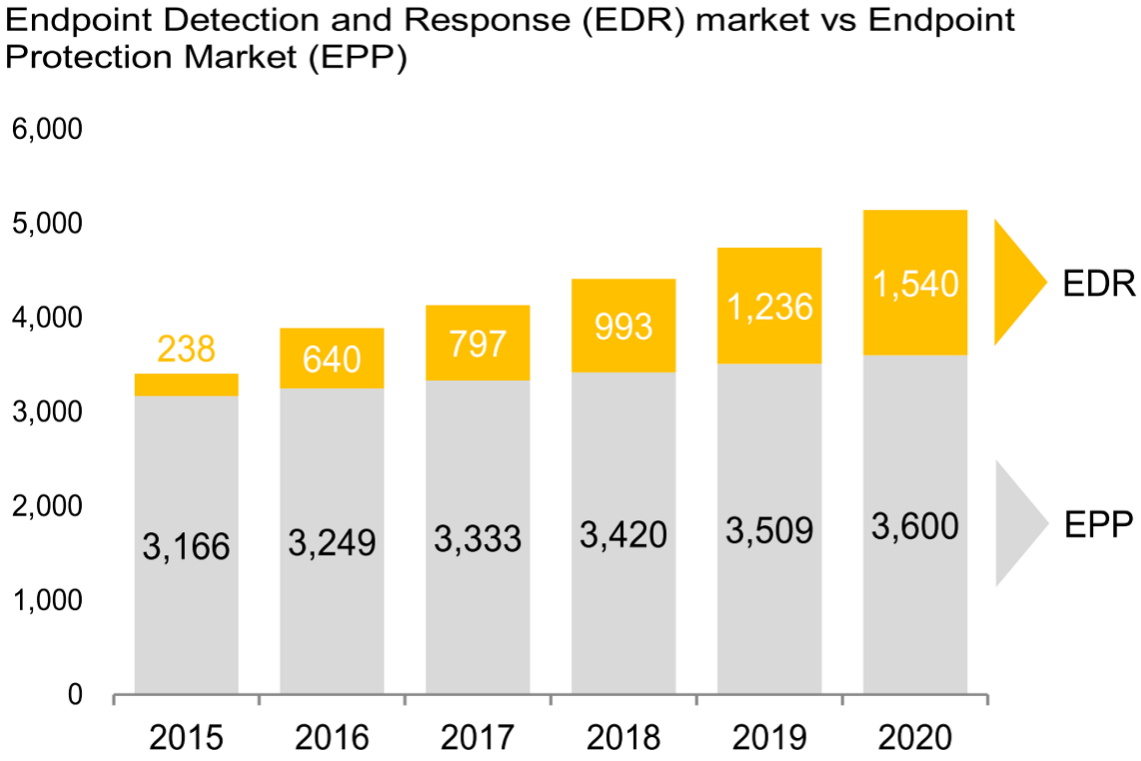

Рис. 1.7. EDR Market vs EPP Market, Gartner, CS Communications Infrastructure Team, Credit Suisse Research

За оцінками Gartner, сукупні витрати організацій на вирішення EDR будуть рости і до 2020 року складуть близько 1,5 млрд доларів США. Це при сукупному середньорічному темпі зростання в 45,3%, що помітно швидше, ніж прогноз сукупного середньорічного темпу зростання в 2.6% для ринку рішень EPP, а також ніж в 7.0% для загального ринку рішень безпеки [1].

Провідні аналітичні агентства в своїх звітах згадують наступних виробників щодо захисту кінцевих точок з включеною EDR-функціональністю.

Аналітичне агентство Gartner в листопаді 2017 році випустило окремий огляд ринку за EDR: Market Guide for Endpoint Detection and Response Solutions, де детально описані напрямки EDR-ринку, розподіл, тренди та інше. У розділі Representative Vendors EDR-огляду Gartner для можливості подання масштабу ринку перераховує наступних представників цього ринку рішень в алфавітному порядку: Carbon Black, Check Point Software Technologies, Cisco, CounterTack, CrowdStrike, Cyberbit, Cybereason, Cynet, CyTech Services, Digital Guardian, Endgame , enSilo, ESET, Fidelis Cybersecurity, FireEye, G Data Software, IBM, Kaspersky Lab, Malwarebytes, McAfee, Microsoft, OpenText (Guidance), RSA Security, Secdo, SentinelOne, Sophos, Symantec, Tanium, Trend Micro, WatchGuard, Ziften [1].

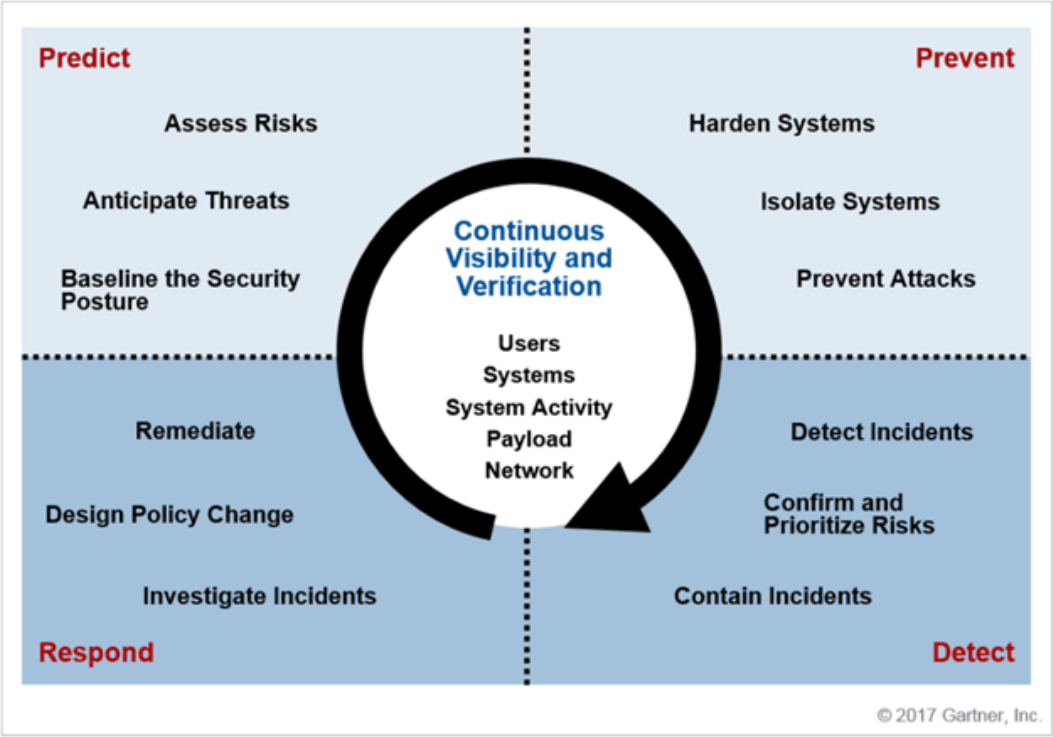

Рис. 1.8. EDR Functionality, Gartner Market Guide for Endpoint Detection and Response Solutions 2017

Також варто відзначити, що в цьому огляді Gartner починає згадувати про важливість взаємодії рішень класів EDR і EPP і, відповідно, про адаптивної

стратегії: Prevent (запобігання), Detect (виявлення), Respond (реагування), Predict (прогнозування) (рис.1.8) [1].

1.3. Аналіз функціональності рішень класу EDR

Розглянемо функціональні можливості рішень Endpoint Detection and Response (EDR).

Сучасні рішення класу EDR дозволяють [1]:

забезпечувати моніторинг кінцевих точок в режимі реального часу і представляти наочну візуалізацію активностей всіх робочих станцій і серверів в корпоративній інфраструктурі з єдиної консолі;

ефективно виявляти і пріоритезувати інциденти інформаційної безпеки в міру їх виникнення на кінцевих точках;

записувати і зберігати інформацію по активностей на кінцевих точках для подальшого розслідування комплексних інцидентів;

надавати необхідну інформацію фахівцям з безпеки для оперативного розслідування інцидентів;

реагувати на інциденти, забезпечуючи їх стримування, а також допомагають у відновленні робочих станцій у вихідне до інциденту стан;

підтримувати можливість взаємодії з рішеннями класу EPP.

Рішення EDR дозволяє проводити спостереження за всіма діями кінцевих точок, наприклад, установка нового програмного забезпечення, скачування файлів, підвищення рівня привілеїв облікових записів, а також зміни в запущених процесах, в мережеву активність, в поведінці користувачів і ін. Детальний моніторинг всіх процесів, запущених на робочих станціях і серверах, а також їх взаємодію, наприклад, з виконуваними файлами і корпоративними додатками, дозволяє організаціям отримувати наочну картину всього, що відбувається. А саме відстежувати підозрілу поведінку, фіксувати несанкціонований доступ і інші зловмисні дії. У разі інциденту можна перевірити ці дані і зрозуміти, на яких користувачів була спрямована атака, які системи могли бути скомпрометовані і яка інформація могла постраждати [1].

Рішення EDR відстежує запуск програм і дозволяє визначати місце розташування шкідливих об'єктів в корпоративній мережі, а також надавати інформацію про виконувані ними дії. Коли файл потрапляє на кінцеву точку, EDR продовжує спостерігати, аналізувати і записувати всю активність файлу, незалежно від його розташування. Якщо в якийсь момент в майбутньому будуть виявлені сліди атаки, рішення може надати всю записану історію поведінки використовуваного в атаці шкідливий: звідки з'явився, де був, що робив і інше. Ця інформація допоможе побачити весь ланцюжок процесу і оперативно вжити заходів по реагуванню [1].

Виявлення. Важливо якомога швидше виявити атаку, що розвивається, перш ніж вона завдасть серйозної шкоди організації. EDR-рішення виявляють складні атаки на ранніх стадіях, використовуючи комбінацію різних механізмів пошуку і методів аналізу невідомих загроз, включаючи машинне навчання і поведінковий аналіз [1].

Методи виявлення [1]:

сканування IoC. EDR шукає та перевіряє компрометуючі індикатори в кінцевих точках, періодично або безперервно скануючи всі кінцеві точки зі списку відомих артефактів (наприклад, хеші, IP-адреси, доменні імена, значення реєстру тощо). Завантаження EDR компрометуючих показників, отриманих з внутрішніх або зовнішніх баз даних загроз або інших джерел, таких як список розсилки від FinCERT, дозволяє організаціям швидко виявляти і реагувати на загрози, а також встановлювати автоматичні правила їх запобігання;

антивірусний модуль. Функціональність антивіруса для перевірки файлів на наявність шкідливого компонента за допомогою сигнатурних, евристичних методів аналізу;

виявлення аномальної поведінки. Нетипові зміни в поведінці або базовій конфігурації можуть свідчити про загрозу. Реєстрація таких подій допомагає виявити загрози і надати, наприклад, інформацію про те, коли стався інцидент і які зміни або наслідки сталися в результаті зловмисних дій, викликаних цілеспрямованою атакою тощо;

пісочниця. Деякі виробники підтримують функціональність пісочниці або взаємодіють з окремими рішеннями у своїх EDR-рішеннях. Підозрілі файли, що вимагають подальшого аналізу, можуть бути автоматично завантажені в спеціально відведене середовище для безпечного їх виконання та досягнення відповідного вердикту на основі поведінки файлу. Якщо пісочниця підтверджена як шкідлива, файл можна відразу заблокувати на всіх робочих станціях мережі;

Threat Intelligence. Залежно від виробника, EARs можуть взаємодіяти з власними службами доступу до Threat Intelligence (TI) та/або сторонніми TI, дозволяючи отримувати дані про загрози, надійні об'єкти та моделі поведінки. Така взаємодія з TI дозволяє швидше реагувати на глобальні загрози;

інші. Наприклад, використання правил YARA для сканування об'єктів, механізм перевірки дійсності підписаних сертифікатів тощо;

ретроспективний аналіз. Пошук інформації про дії шкідливих об'єктів в минулому, про які системи, машини, файли піддавалися шкідливому коду і так далі - ці дані значно полегшують процес всебічного розслідування інцидентів;

кореляція. EDR дозволяє порівнювати різні дані та події з різних кінцевих точок в один інцидент для подальшого розслідування та реагування, використовуючи телеметрію в реальному часі, історичні дані та вердикти виявлення, щоб співвіднести.

Розслідування. Швидкий доступ до всіх даних з кінцевих точок і до інформації про активність дозволяє аналітикам виконувати комплексне розслідування і глибокий аналіз джерел загроз.

EDR може збирати різноманітні дані, наприклад [1]:

метадані з кінцевих точок: IP, MAC, DNS-імена, підключені USB-пристрої;

мережеві дані: таблиці DNS і ARP, відкриті порти і пов'язані процеси, мережеві підключення, популярні URL-адреси;

дані процесів: потоки і метадані запущених процесів, служби Windows, події операційної системи;

події доступу до реєстру і доступу до диска;

інші дані: події завантаження DLL, активні драйвери пристроїв і завантажені модулі ядра, розширення браузера і історія, історія команд CMD і PowerShell.

EDR консолідує дані про події, послідовність яких привела до виявлення діючої атаки на кінцевих точках. Візуалізація всієї хронології подій дозволяє оперативно розслідувати інциденти.

EDR надає докладні відомості про будь-які виявлені загрози, наприклад:

як загроза проникла в інфраструктуру організації;

список порушених робочих станцій і серверів;

інформація про зміни в порушених атакою кінцевих точках;

додатки, які запускаються;

створені в ході атаки файли;

завантажені файли та ін.

EDR надає можливість пріоритезувати інциденти, в залежності від критичності подій, шляхом аналізу отриманих даних і їх кореляції, що дозволяє фахівцям зосередитися в першу чергу на самих релевантних складним атакам інциденти і оперативно реагувати на виявлені загрози.

Реагування. Широкий набір інструментів дозволяє фахівцям з інформаційної безпеки переглядати події, оцінювати масштаб порушень і визначати всі порушені кінцеві точки. Рішення EDR дозволяють забезпечувати стримування складені інцидентів, усуваючи загрози на окремих кінцевих точках, і їх наслідків без впливу на роботу користувачів [1].

У разі виявлення шкідливої активності інформація про інцидент оперативно передається адміністратору. Використовуючи централізовану консоль управління, фахівець може прийняти наступні заходи:

зупинка працюючих шкідливих процесів;

карантин файлів;

ізолювання заражених робочих станцій;

проведення необхідних віддалених дій з файлами та реєстром;

блокування підключень кінцевих точок до зловмисних доменів, URL- і IP-адресами;

збір криміналістичних артефактів (образ оперативної пам'яті, образ жорсткого диска);

відновлення робочих місць в попередній безпечний стан.

Запобігання. Наявність рішень класу EPP, побудованих на базі превентивних технологій, орієнтованих на виявлення та автоматичне блокування відомих загроз, очевидно шкідливих об'єктів, а також частини невідомих загроз, допомагають усунути необхідність аналізу великої кількості інцидентів, які не мають відношення до складних атакам, тим самим підвищуючи ефективність EDR-платформ, спрямованих на виявлення складних загроз. Рішення EDR, в свою чергу, можуть відправляти вердикти в EPP-рішення і тим самим забезпечити дійсно комплексний підхід до протидії передовим загрозам [1].

Інтеграція. Рішення по виявленню складних загроз на кінцевих точках і реагування на них, крім взаємодії з рішеннями класу EPP, повинні бути здатні вбудовуватися в ширшу інфраструктуру інформаційної безпеки організацій. Підтримка можливості взаємодії з існуючими засобами ІБ, наприклад, з системами з виявлення складних загроз на мережі, з пісочницею в разі відсутності вбудованої в рішення EDR, з інструментами з розслідування тощо. Важливо, щоб рішення підтримувало відкритий API для інтеграції з SIEM/SOC для Збагачення цих систем інформацією і надання додаткових можливостей для моніторингу і проведення розслідувань. EDR-рішення допомагають SIEM, виступаючи джерелом логів і подій, надаючи при цьому вже проаналізовану і потрібну інформацію для проведення кореляції з інформацією, одержуваної від інших джерел [1].

Експертиза. Зрозуміло, важливо мати інструменти, необхідні для належного виявлення і реагування, однак і цього в наш час стає недостатньо для протистояння сучасним загрозам, на чолі яких стоять люди, керівні всім процесом підготовки та проведення самих складені спрямованих атак. Організації, що використовують EDR-рішення, також потребують виділених кваліфікованих кадрах. Щоб постійно залишатися в курсі нинішнього ландшафту загроз, застосовувати знання для пошуку загроз всередині мережі та розуміти, як ефективно використовувати

спеціалізовані набори інструментів, потрібна глибока експертиза в цій області, як внутрішня, так і зовнішня [1].

Деякі компанії при використанні інструментів з виявлення та реагування на передові загрози на кінцевих точках віддадуть перевагу задіяти в повному обсязі свої власні ресурси і тільки в разі гострої необхідності частково залучати зовнішніх фахівців і використовувати сторонні сервіси. В цьому випадку посилення експертизи всередині організації може будуватися на проходженні різних навчальних програм з підвищення кваліфікації фахівців ІБ, а також шляхом доступу до інформаційного порталу загроз, отримання потоків даних про загрози і різних аналітичних звітів, які зазвичай надають виробники рішень щодо протидії передовим загрозам [1].

Для перевантажених або недостатньо укомплектованих фахівцями компаній буде привабливим використовувати більшою мірою сторонні професійні послуги, такі як: сервіси реагування на інциденти, активний пошук загроз, аналіз шкідливих програм, використаних в рамках атаки, сервіс по цифровій криміналістиці, усунення наслідків і інші необхідні експертні сервіси [1].

Як висновок, робочі станції та сервери в наш час продовжують залишатися найпопулярнішими точками проникнення в інфраструктуру зловмисниками при організації ними спрямованих атак. Популярних систем класу Endpoint Protection Platform (EPP), які створювалися за часів досконалого іншого ландшафту загроз і були спрямовані в основному на запобігання масових атак, вже стає недостатньо. Ці рішення не орієнтовані на протидію складним і комплексним загрозам на кінцевих точках, що свідчить про необхідність додаткових інвестицій в спеціалізовані продукти класу Endpoint Detection and Response (EDR) для розширеного виявлення на базі передових технологій і подальшого реагування на знайдені складні загрози.

Тільки спільне використання цих двох технологій і балансу між власною експертизою і використанням сторонніх сервісів дозволить організаціям домогтися дійсно високих показників захисту своїх кінцевих пристроїв і тим самим підвищити

безпеку компанії в цілому в епоху швидко зростаючого числа і складності передових загроз і цілеспрямованих атак.

1.4. Роль і місце розширеного захисту корпоративних кінцевих точок від загроз

На малий бізнес все частіше націлюються кіберзлочинці. Торік 66% малого бізнесу зазнали кібератаки. Все частіше компанії звертаються до програмного забезпечення для захисту кінцевих точок для захисту мереж інформаційних технологій [2].

Проте проблема залишається. Кіберзлочинці застосовують таку кількість тактик, щоб обійти захист, і неможливо щоразу зупиняти всі атаки. Сучасна передова технологія безпеки визнає цю реальність і включає можливість вирішення загроз, які проникають крізь захист. Одним з найпопулярніших та найефективніших підходів є виявлення та реагування на кінцеві точки (EDR) [2].

Виявлення та реагування на кінцеві точки (EDR) є все більш популярним заходом безпеки з однієї ключової причини: видимості. Це важливий елемент, необхідний для зупинки кібератаки, що заражає системи.

Для виявлення та припинення атаки, яка проскочила через безпеку кінцевих точок, компаніям потрібно в середньому 197 днів, більше шести місяців. Цей тип кібератаки, який називається передовою стійкою загрозою (APT), є складним і призначеним для зараження мережі, яке стає невиявленим протягом тривалого періоду часу.

Системи виявлення та відповіді кінцевих точок знаходять ці атаки. EDR передбачає постійний моніторинг IT-систем у поєднанні з автоматизованим аналізом даних для виявлення підозрілої діяльності на кінцевих точках (обчислювальних пристроях, що використовуються у мережі, включаючи ноутбуки, мобільні телефони та сервери) [2].

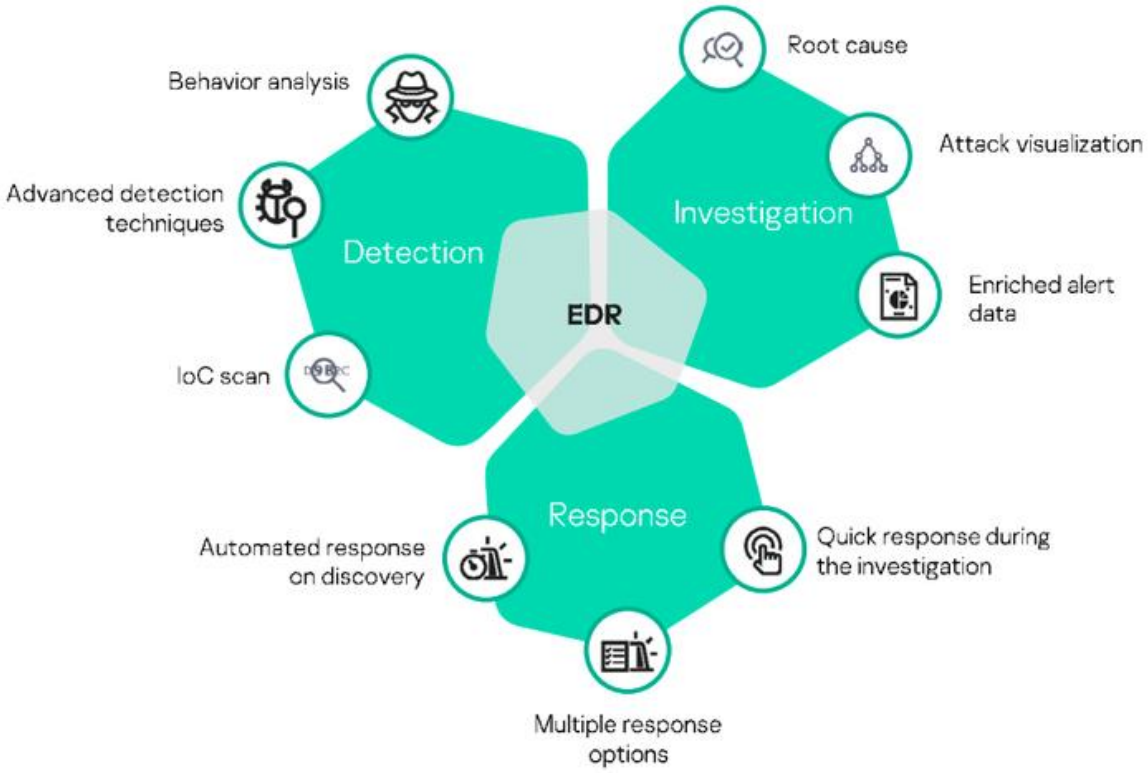

Рис. 1.9. Основні функції рішень класу EDR [2]

З EDR типова поведінка кінцевих точок стає добре зрозумілою. Коли ця поведінка змінюється внаслідок нападу, то отримується попередження і можна діяти, щоб стримати загрозу.

Три важливі елементи ефективного виявлення та реагування на кінцеві точки (EDR). Ці компоненти необхідні для успішного захисту EDR та створюють видимість, необхідну для виявлення порушень безпеки та дії над ними [2].

1. Збір та зберігання даних.

Кожне рішення EDR покладається на дані як основний елемент для створення видимості для лову атак. Два компоненти складають фрагмент даних.

Збір даних: захист EDR повинен постійно контролювати кінцеві точки та збирати телеметрію (запис та передачу показань кінцевої точки) у режимі реального часу, не втручаючись у звичайні системні процеси. Ці дані включають широкий спектр заходів, які виконують кінцеві точки. Системні процеси, мережеві зв’язки та передача даних – це одна із зібраних статистичних даних. Якщо кінцеві точки реалізують несподівану поведінку, це може свідчити про можливу атаку.

Зберігання даних: Оскільки зібраних даних кінцевих точок дуже багато, більшість малих підприємств повинні планувати зберігати ці дані у хмарі. Хмарна база даних загроз забезпечує належний обсяг пам’яті в міру зростання зібраних даних. Це також дозволяє поєднувати дані кінцевих точок із розвідкою загроз , сховищем інформації про загрозу безпеці, щоб допомогти вам визначити ознаки шкідливої діяльності.

2. Аналітика та криміналістичні можливості

Для виявлення потенційних атак системи EDR повинні пробирати зібрані дані кінцевої точки, щоб позначити аномалії. Для цього розслідування потрібна аналітика в режимі реального часу, що виконується за допомогою засобів автоматизації та криміналістичних інструментів, що застосовуються спеціалістами з безпеки, наприклад, мисливцями за загрозами або операційним центром (SOC) [2].

Автоматизована аналітика: для людей неможливо виконати початковий аналіз даних. Обсяг даних занадто масивний. Натомість ці дані подаються в автоматизовані механізми виявлення загроз, такі як механізми машинного навчання, для кореляції мережевої активності та поведінки проти розвідки загроз. Ця технологія шукає моделі, що означають потенційні загрози, такі як показники компромісу (IoC) та показники атаки (IoA). IoC – це дані, що сигналізують про можливе порушення безпеки. IoA передбачає дії, вжиті кіберзлочинцями для створення APT, наприклад, приховування в пам’яті комп’ютера [2].

Криміналістичний аналіз: передбачає вивчення людьми предметів, позначених автоматичним аналізом, для перевірки наявності загрози. Наприклад, збільшення трафіку веб-сайту в непарні години або через підозрілу географію потребує людського розуміння, щоб підтвердити, що це проблема. Можуть виникати помилкові позитивні результати, наприклад, новий комп’ютерний сценарій, створений IT-командою для автоматизації процесів. Рішення EDR повинно підтримувати механізм відмітки законної діяльності, позначеної як потенційна загроза, наприклад, додавання їх до білого списку, щоб уникнути подальшого позначення [2].

3. Швидка реакція

Як тільки аналіз підтвердить загрозу, ваш EDR повинен виконати швидкі дії. Швидке реагування на випадки безпеки допомагає мінімізувати або запобігти пошкодженню, такому як викрадені фінансові дані або дані клієнтів [2].

Реакція на інцидент може варіюватися від розсилки автоматичних сповіщень та автоматичного виходу користувача з кінцевої точки до вимкнення доступу до мережі та ізоляції кінцевої точки до розповсюдження інфекції. Будь-яка технологія EDR, яку ви розглядаєте, повинна підтримувати кілька варіантів відповіді, які ви можете налаштувати відповідно до своїх потреб [2].

Успішна безпека EDR включає можливості виявлення, сортування, розслідування та виправлення. Вони представляють етапи фільтрації даних кінцевих точок для націлювання на кіберзагрозу. Процес функціонування EDR (рис. 1.10) [2]:

Виявлення (Detection)

Процес захисту EDR починається з виявлення загроз. Щоб автоматизовані системи EDR знаходили загрози, ви встановлюєте на кінцеві точки програмний агент для збору даних.

Агент постійно контролює кінцеву точку та збирає дані телеметрії, надсилаючи їх до центральної бази даних, де алгоритми машинного навчання аналізують дані на наявність аномалій. Раптові зміни в процесах кінцевих точок або поведінці користувачів внаслідок нормальної поведінки позначаються для подальшого розслідування [2].

Приклади підозрілих дій включають спробу входу в кінцеву точку з віддаленого місця, завантаження певних типів програмних файлів або відключення брандмауерів. EDR поєднує ці ознаки нерегулярної поведінки з ланцюжком подій до та після, щоб створити карту виконуваних процесів.

Завдяки цьому більш широкому контексту, в поєднанні з розвідкою про загрози, системи EDR можуть оцінювати тисячі подій у мережі, щоб звузити діяльність, що свідчить про кібератаку.

Сортування (Triage)

Платформи EDR повідомляють IT-персонал про підозрілу діяльність. Вони надсилають попередження та надають інформаційні панелі та звіти, що підсумовують результати алгоритмічних знахідок [2].

Це коли відбувається сортування. IT-команда повинна усунути помилкові спрацьовування. Вони також класифікують попередження як відому шкідливу діяльність, яка негайно запускає стадію виправлення, або невідомі для розслідування.

Етап сортування є найскладнішим для IT-команд. Вони часто перевантажені попередженнями, і команда може пропустити діяльність, що вимагає більш глибокого розслідування [2].

Щоб цього не сталося, IT-команди повинні регулярно переглядати критерії виявлення EDR для вирішення наступних питань [2]:

частота помилкових спрацьовувань: Чи надто багато помилкових спрацьовувань? Якщо так, то чому це відбувається? Одним із рішень є використання білих списків;

корисні сповіщення: Точно налаштуйте механізми виявлення та сповіщення про сповіщення, щоб переконатися, що ви отримуєте попередження, необхідне, щоб допомогти вам діяти. Ви не хочете, щоб сповіщення відчували себе як спам, оскільки вони занадто загальні;

структура сортування: важливо створити структуру для чіткої класифікації попереджень та розуміння необхідних дій для ефективного виконання етапу сортування.

Розслідування (Investigation)

Фаза сортування призводить до виявлених аномалій до невідомих, які називаються потенційними. З цього часу пора копатись у потенційних клієнтах, щоб підтвердити доброякісну чи шкідливу діяльність.

Команда IT вивчає кожного потенційного клієнта, використовуючи методи полювання на загрози, щоб зібрати додатковий контекст. Цей контекст дає змогу краще зрозуміти діяльність та те, чому вона відбувається. Наприклад, незнайомий

комп'ютерний процес, який виконується в кінцевій точці, може означати атаку або просто те, що працівник завантажив нове програмне забезпечення [2].

Ключовим для етапу розслідування є швидкість. Ви хочете швидко визначити, чи є невідома діяльність шкідливою, щоб запобігти пошкодженню.

Сьогоднішні кібератаки використовують бічний рух, тактику, яка дозволяє інфекціям переходити від однієї кінцевої точки до інших, швидко заражаючи значні частини вашої мережі. Хороша система EDR прискорює фазу розслідування, що призводить до швидшого реагування та виправлення, щоб стримувати бічні рухи [2].

Відновлення (Remediation)

Підтверджені загрози вимагають відповіді, тому платформи EDR можуть автоматично діяти. Відповіді включають такі тактики, як зупинка будь-яких комп'ютерних процесів, що працюють на зараженій кінцевій точці, та ізоляція кінцевої точки від решти вашої мережі. Деякі рішення EDR можуть автоматично обробляти файли та дані, що зберігаються на кінцевій точці, одночасно видаляючи інфекцію [2].

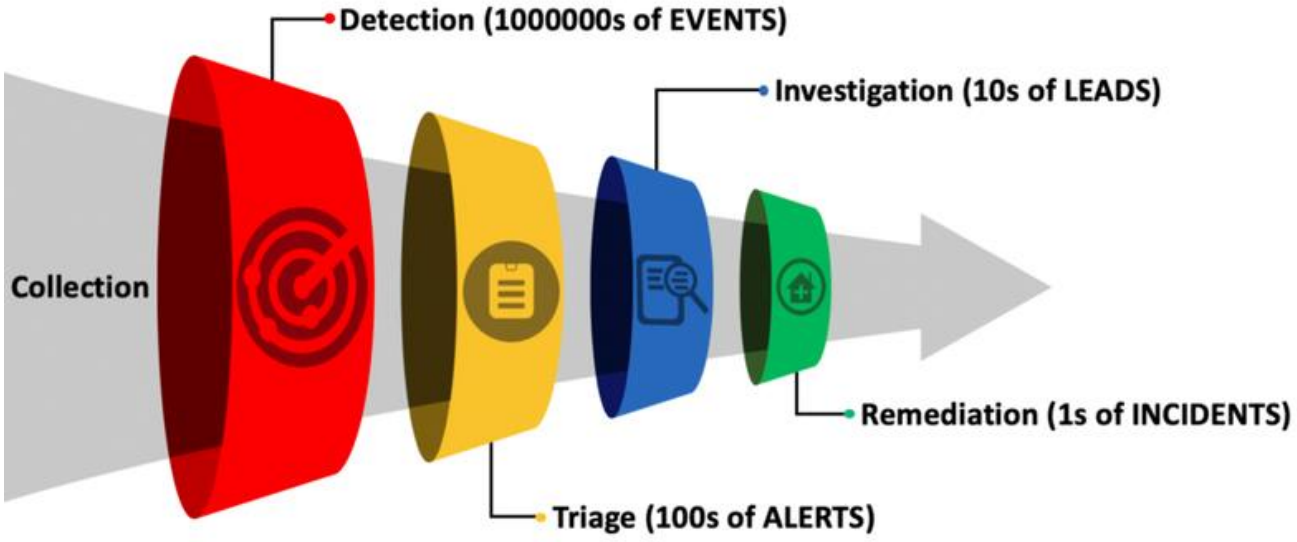

Рис. 1.10. Процес функціонування EDR [2]

Частина зусиль щодо виправлення залучає IT-команду, яка визначає ступінь збитку. Дані клієнтів були вкрадені? Які вразливості мережі потребують усунення?

Розуміння цілі кіберзлочинця та способу нападу дозволяє вжити належних дій. Це також дозволяє вашій команді збирати конкретні знання для посилення

безпеки мережі [2].

Кібератаки розвиваються ускладнено і можуть пройти повз традиційний захист безпеки. Фішинг, програмне забезпечення – вимагач та поліморфне шкідливе програмне забезпечення, здатне змінити себе, щоб уникнути виявлення, є лише деякими загрозами, які обходять системи безпеки. EDR бореться з цим, забезпечуючи покращений огляд стану мережі. Ця видимість дозволяє рішенням EDR швидко знаходити атаки, зупиняючи їх до виникнення збитків.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ РОЗШИРЕНОГО ЗАХИСТУ КОРПОРАТИВНИХ КІНЦЕВИХ ТОЧОК ВІД ЗАГРОЗ НА БАЗІ FortiEDR

Рішення FortiEDR дозволяє в режимі реального часу відстежувати роботу кінцевих точок, автоматично блокує шкідливу активність, а також надає операторам SOC детальну інформацію, необхідну для розслідування складних кіберінцідентов. Можливості рішення FortiEDR дозволяють використовувати її для боротьби з нетиповими, цільовими атаками, мінімізувати шкоду від програм-шифрувальників, швидко усувати наслідки шкідливих дій на корпоративних кінцевих точках [3].

2.1. Призначення та функції системи FortiEDR

Необхідність застосування систем класу Endpoint Detection & Response (EDR) продиктована постійно зростаючої складністю кібератак, спрямованих на корпоративний сектор. З одного боку, продукти, призначені для контролю мережевого трафіку, не покривають весь потенційний фронт нападу, залишаючи поза сферою своєї уваги процеси, що відбуваються всередині кінцевих точок. З іншого боку, класичні антивіруси і рішення рівня Endpoint Protection Platform (EPP) не завжди мають можливість детектувати багатоетапні, цільові атаки [3].

Порівняння сигнатур і евристичний аналіз часто безсилі при виявленні нападів, з використанням безфайлові шкідливої програми, або атак, що розвиваються через легітимні програми і соціальну інженерію. Ще одним аспектом, який ускладнює боротьбу з загрозами для кінцевих точок, є велика кількість спрацьовувань традиційних засобів захисту. При ручній обробці даних про потенційно небезпечною активності з робочих станцій оператори SOC (центру моніторингу і реагування на інциденти в області інформаційної безпеки) будуть перевантажені розбором масових, типових подій [3].

При такому підході уважне розслідування по-справжньому серйозних подій в масштабах організації вимагатиме збільшення штату, а значить, і бюджету SOC,

що не завжди можливо і доцільно. EDR-системи є одним з найбільш ефективних шляхів вирішення проблеми захисту кінцевих точок від складних атак. Вони дозволяють контролювати всі процеси, запущені на робочих станціях, автоматично детектувати, класифікувати і усувати загрози, а також надавати фахівцям детальні відомості для розслідування нетипових інцидентів.

Функціональні можливості EDR-продуктів зазвичай включають в себе розвинені засоби моніторингу, протоколювання і наочного уявлення виявлених загроз. Важливо, що такі системи можуть мати функціональні можливості антивірусних і EPP-рішень або допускати взаємодія з зовнішніми продуктами. Це дозволяє інтегрувати EDR в загальний контур безпеки підприємства без заміни наявних засобів захисту кінцевих точок [3].

Функціональність типової системи класу EDR складається з наступних елементів [3]:

Засоби моніторингу активності кінцевих точок:

контроль запуску нових процесів і внесення змін в існуючі;

відстеження установки і видалення програмного забезпечення;

моніторинг операцій з файлами, виявлення операцій щодо підвищення рівня привілеїв облікових записів;

сканування мережевих з'єднань;

контроль змін ключів реєстру.

Виявлення потенційно шкідливої активності:

власний антивірусний компонент або взаємодія із зовнішньою системою;

аналіз індикаторів компрометації (IoC);

елементи поведінкового аналізу для виявлення аномалій в діях користувачів або роботі запущених процесів;

методи Threat Hunting і Threat Intelligence (проактивний пошук загроз і кіберрозвідку);

перевірка журналів роботи.

Ідентифікація та класифікація виявлених загроз:

збагачення відомостей про інцидент за допомогою власних баз даних або

зовнішніх джерел;

отримання метаданих від кінцевої точки;

аналіз додаткової інформації, пов'язаної з інцидентом – відомостей про мережеву активність, роботі з пам'яттю, історії використання командного рядка тощо.

Реагування на інциденти:

блокування мережевих з'єднань ураженої кінцевої точки;

ізоляція шкідливого процесу в пісочниці;

видалення пов'язаних з атакою файлів;

відновлення змінених записів реєстру.

Рішення FortiEDR є повнофункціональною системою захисту кінцевих точок в режимі реального часу. Розвинені засоби моніторингу та реагування дозволяють їй в упереджувальному режимі знижувати кількість напрямків атак, запобігати ураженню шкідливими програмами, виявляти і знешкоджувати потенційні загрози [3].

FortiEDR забезпечує багаторівневий захист після зараження і до зараження, який зупиняє просунуті шкідливі програми в режимі реального часу. Визнається, що не можна запобігти проникненню зовнішніх загроз в мережі, і замість цього треба зосереджуватися на запобіганні крадіжки і викупу критично важливих даних у разі кібератаки. Унікальна технологія віртуального виправлення FortiEDR, яка блокує тільки шкідливі вихідні повідомлення, дозволяє співробітникам продовжувати працювати в звичайному режимі, навіть якщо їх влаштування заражені [4].

Запобігання виконанню

Антивірус нового покоління (NGAV) – це безсигнатурний підхід, який може виявляти і пом'якшувати атаки нульового дня. FortiEDR зупиняє як відомі, так і невідомі типи шкідливих програм за допомогою NGAV на основі машинного навчання, який відфільтровує відомі варіанти шкідливих програм. Це блокує виконання файлів, які визначені як шкідливі або імовірно шкідливі. Відповідно до цієї політикою кожен файл аналізується на предмет виявлення зловмисних дій.

Запобігання крадіжкам даних

Крадіжка даних – це несанкціонована передача конфіденційної інформації з мережі-мети в місце, контрольоване зловмисником. FortiEDR – це платформа для запобігання крадіжки під час цільових атак в реальному часі. FortiEDR гарантує, що дані не будуть вкрадені зловмисниками, незалежно від використовуваних ними методів. FortiEDR може запобігти спробам зловмисної крадіжки будь-якого типу даних, з будь-якої програми, з будь-якого процесу, використовуючи будь-який протокол або порт [4].

FortiEDR стане останньою лінією захисту в разі спроби крадіжки даних. Всі шкідливі сполуки блокуються, і можна переглянути точну інформацію про заражені пристрої і пов'язані з ними компоненти. FortiEDR це тільки програмне рішення, яке можна встановити на поточному стандартному обладнанні. FortiEDR захищає корпоративні дані від крадіжки як на місці, так і за його межами [4].

Запобігання програмам-вимагачам

Програми-вимагачі – це шкідливі програми, які використовуються зловмисниками для зараження пристрою, захоплення файлів на цьому пристрої та подальшої їх блокування за допомогою шифрування, щоб до них не можна було отримати доступ, поки зловмисник не розшифровує і не звільнить їх. Успішна атака програми-здирника є використання вразливості системи безпеки у середовищі. Платня зловмисникові це тільки короткострокове рішення, яке не усуває корінь проблеми, оскільки може привести до іншої атаки, яка буде ще більш зловмисною і дорожчою, ніж попередня [4].

FortiEDR запобігає в режимі реального часу спроби зловмисника зашифрувати або змінити дані. Потім FortiEDR генерує попередження, яке містить інформацію, необхідну для початку розслідування, щоб можна було виявити корінне порушення і повністю усунути його. Більш того, кінцевий користувач може продовжувати працювати в звичайному режимі навіть на зараженому пристрої [4].

Полювання на загрози (Threat Hunting)

Можливості FortiEDR з пошуку загроз включають набір програмних інструментів і джерел інформації, призначених для виявлення, розслідування,

стримування і пом'якшення підозрілих дій на пристроях кінцевих користувачів.

FortiEDR забезпечує управління захистом кінцевих точок до і після зараження, забезпечуючи високу швидкість виявлення з можливістю блокування і реагування в реальному часі в порівнянні з традиційними інструментами виявлення та реагування кінцевих точок (EDR) [4].

FortiEDR забезпечує класифікацію шкідливих програм, відображає IoC і надає повний огляд ланцюжка атак – і все це, одночасно дозволяє користувачам проводити подальший пошук загроз, якщо і коли це необхідно [4].

Можливості FortiEDR забезпечують блокування в реальному часі для реалізації багаторівневої стратегії захисту, якою можна керувати з хмари.

Дивлячись на те, як діють зовнішні суб'єкти загроз, можна виділити два важливих аспекти. По-перше, зловмисники використовують мережу для виведення даних з організації. По-друге, вони намагаються залишатися якомога більш непомітними, щоб уникнути існуючих заходів безпеки. Це означає, що зловмисники повинні встановлювати вихідні комунікації нестандартним чином.

Технологія FortiEDR запобігає крадіжці даних, виявляючи в режимі реального часу зловмисні вихідні повідомлення, які були створені зовнішніми учасниками загроз. Виявлення зловмисних вихідних повідомлень є результатом досліджень, проведених як щодо внутрішніх компонентів операційної системи, так і щодо методів роботи шкідливих програм [4].

Дослідження показують, що всі законні вихідні повідомлення повинні проходити через операційну систему. Таким чином, відстежуючи внутрішній устрій операційної системи, можна перевірити правильність установки з'єднання.

FortiEDR збирає дані стека ОС, дані, що відносяться до трафіків і процесів, і проводить аналіз виконуваних файлів, щоб визначити характер з'єднання. Крім того, виявляється будь-який тип загрози, яка намагається обійти FortiEDR, оскільки з'єднання не матиме відповідних даних від FortiEDR [4].

Технологія FortiEDR (рис. 2.1) запобігає крадіжці даних, виявляючи в режимі реального часу зловмисні вихідні повідомлення, які були створені зовнішніми учасниками загроз. Виявлення зловмисних вихідних повідомлень є результатом

досліджень, проведених як щодо внутрішніх компонентів операційної системи, так і щодо методів роботи шкідливих програм [4, 9].

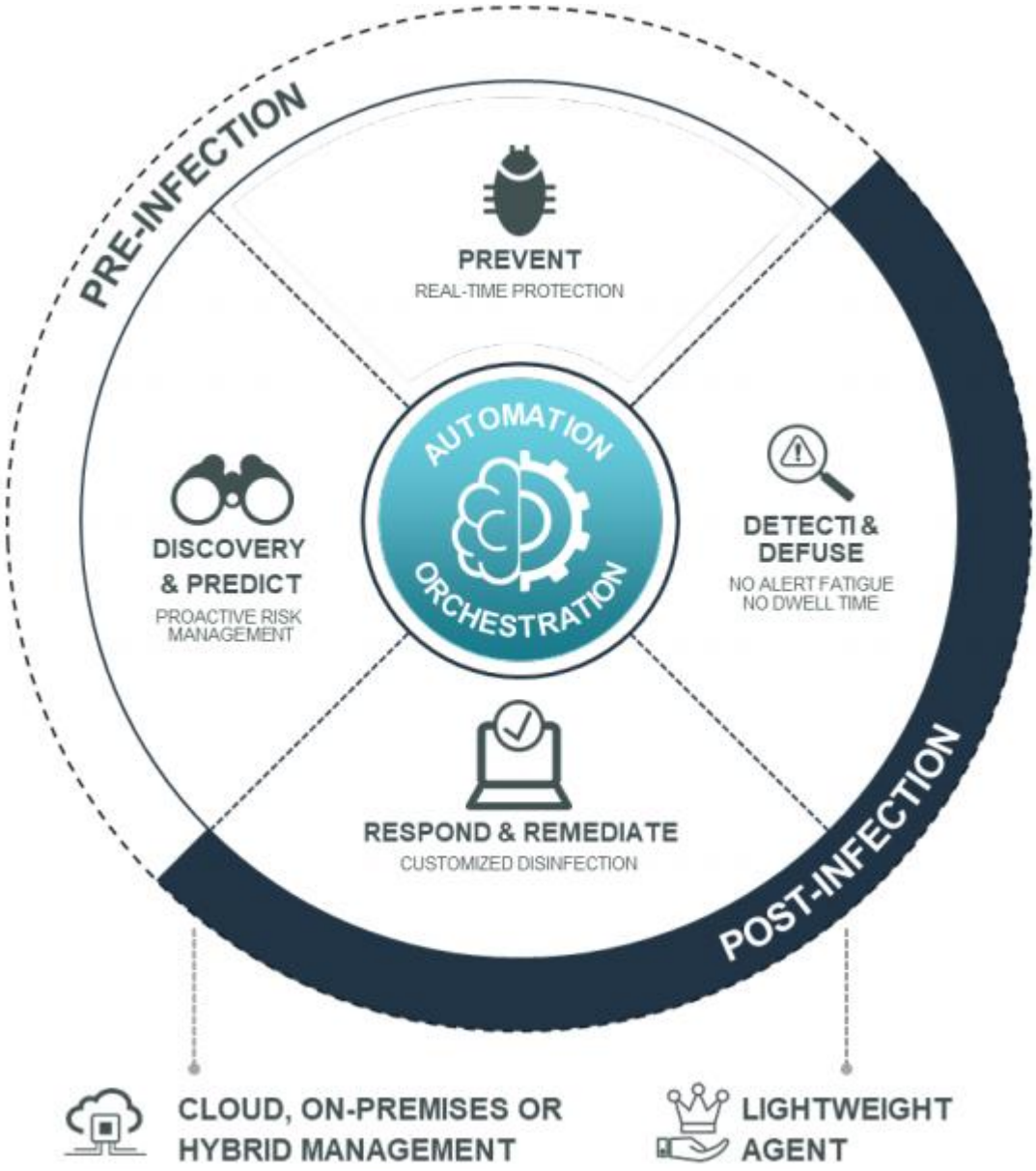

Рис. 2.1. Технологія FortiEDR [4, 9]

FortiEDR має власний антивірусний модуль, оснащений технологією машинного навчання і NGAV-ядром (Next Generation Antivirus, антивірус нового покоління). Крім того, система може взаємодіяти з EPP-рішенням FortiClient або іншим програмним забезпеченням для захисту робочих станцій.

Після виявлення підозрілої активності FortiEDR автоматично блокує потенційні загрози і при необхідності ізолює робочу станцію від мережі. Така політика дозволяє ефективно боротися з атаками, спрямованими на витік даних, а також припиняти роботу програм-шифрувальників. Одночасно з ліквідацією атаки

FortiEDR збирає додаткові відомості про подію, взаємодіючі з хмарним сервісом Fortinet Cloud Services, VirusTotal і базою MITRE [3].

Реакція системи на виявлення загрози визначається набором політик безпеки і автоматичних сценаріїв, які можуть бути налаштовані користувачем. Для кожної групи кінцевих точок може бути призначений свій власний набір політик безпеки. Адміністратор SOC має можливість оперативно перенести обрану кінцеву точку в групу з більш строгими правилами безпеки.

Контроль з'єднань з мережею в розрізі програм, встановлених на робочі станції, дозволяє FortiEDR ефективно протидіяти експлуатації відомих вразливостей. Система автоматично знижує рівень довіри до будь-якого додатка, у якого зафіксовані незакриті проломи, і обмежує його можливості по взаємодії з зовнішніми джерелами [3].

FortiEDR складається з шести базових компонентів [3]:

FortiEDR Collector – агентський модуль, екземпляри якого встановлюються на кінцеві точки (робочі станції і сервери). Колектор здійснює моніторинг діяльності кінцевої точки, передає дані для аналізу центрального компоненту системи, а також самостійно блокує відомі загрози за допомогою вбудованого антивірусного модуля.

FortiEDR Central Manager – центральний компонент відповідає за аналіз даних, отриманих від колектора, збагачення цих відомостей, вибір і виконання сценарію («плейбук») для реагування на інцидент.

Fortinet Cloud Services – сервіс, який містить дані про погрози, необхідні для збагачення зібраної і переданої колектором інформації.

FortiEDR Central Manager – модуль управління системою, що здійснює взаємозв'язок всіх компонентів.

FortiEDR Aggregator виконує функції проксі-сервера, перенаправляючи запити від менеджера до центрального компоненту і назад. Крім того, агрегатор відповідає за видачу ліцензій та конфігураційної інформації колекторам.

Репозиторій Threat Hunting – база даних для зберігання шкідливих файлів, виявлених FortiEDR на кінцевих точках.

При виявленні підозрілої активності колектор передає дані про неї в центральний компонент, який звертається до Fortinet Cloud Services за додатковою інформацією, щоб ідентифікувати загрозу. Визначивши шкідливий характер того, що відбувається, центральний компонент вибирає відповідний плейбук і відсилає на колектор набір команд для блокування і нейтралізації загрози [3].

Надалі центральний компонент створює записи про виявлені шкідливих об'єктах в репозиторії Threat Hunting, а також через агрегатор відправляє інформацію про інцидент в менеджер. Останній формує повідомлення для користувача і при необхідності передає дані в зовнішні системи (наприклад, FortiSOAR).

Варіанти розгортання FortiEDR [3]:

хмарний – всі компоненти, за винятком колекторів, розташовуються на серверах Fortinet. В цьому випадку всі завдання, пов'язані з виділенням ресурсів для безперебійної роботи системи, вирішуються силами виробника;

гібридний - центральний компонент і агрегатор (або ж тільки центральний компонент) можуть бути розгорнуті на серверах користувача, а репозиторій, менеджер і Fortinet Cloud Services - розміщені на ресурсах Fortinet;

локальний – всі модулі системи, за винятком Fortinet Cloud Services, встановлюються на сервери користувача. В цьому випадку FortiEDR звертається до зовнішніх ресурсів тільки для збагачення інформації про інцидент при аналізі чергового сервісного запиту («тікета»);

офлайн – користувачі, які приділяють підвищену увагу автономності роботи системи, можуть відключити функцію звернення до Fortinet Cloud Services. При цьому збагачення даних про інцидент виконуватися не буде. Ліцензування FortiEDR ведеться за кількістю робочих станцій і серверів, на які встановлено систему.

FortiEDR призначена для захисту кінцевих точок від кібератак в режимі реального часу. Система контролює процеси, що запускаються на робочих станціях і серверах, виявляючи підозрілу активність і при необхідності блокуючи її. Робота FortiEDR значно звужує потенційний фронт атаки за рахунок відстеження

мережевих з'єднань і автоматичного переривання шкідливих процесів. Розвинені можливості реагування дозволяють в ручному або автоматичному режимі блокувати несанкціоновані дії і ізолювати заражене пристрій [3].

Моніторинг роботи кінцевих точок (контроль процесів, запущених на пристроях, з метою виявлення підозрілої, шкідливої або потенційно небажаної активності; керування з'єднаннями з мережею в розрізі їх програм; виявлення незахищених або некерованих пристроїв, в тому числі IoT; відстеження та оцінка програм) [3].

Антивірусний захист кінцевих точок (виявлення потенційно шкідливих дій на підконтрольних пристроях за допомогою антивірусного движка NGAV на основі штучного інтелекту, виявлення прихованих атак, безфайлових проникнень, роботи програм-вимагачів; запобігання зміни ключів реєстру і відновлення його в разі атаки; виявлення і блокування відомих загроз на підставі інформації, отриманої з постійно поповнюється хмарної бази даних; ізоляція кінцевих точок в разі зараження; автономна захист пристроїв; контроль USB-пристроїв) [3].

Реагування на інциденти (автоматична класифікація подій з області безпеки; підтримка автоматичних стратегій реагування на інциденти на базі політик безпеки і плейбук; широкий спектр реакцій на інциденти – видалення файлів, переривання шкідливих процесів, відкат постійних змін, повідомлення користувачів, ізоляція додатків і пристроїв, створення запитів; відстеження всіх стадій атак і шкідливих змін за допомогою запатентованої технології трасування коду; автоматичне усунення шкідливих змін і відновлення системи без переривання її роботи; додаткова керована служба виявлення та реагування на загрози (MDR) для підтримки SOC) [3].

Розслідування інцидентів (автоматичний аналіз подій без переривання обслуговування користувача; можливість створення дампів пам'яті, використаної шкідливими процесами; інформаційна підтримка прийняття рішень – відображення критеріїв, на підставі яких подія була визнана підозрілою або шкідливою, і структури атаки по MITRE ATT&CK, а також пропозиція логічно обґрунтованих заходів протидії).

2.2. Архітектура рішення та функціональні компоненти рішення FortiEDR

Платформа FortiEDR являє собою розподілену архітектуру (рис. 2.2), яка збирає потік встановлення з'єднань між пристроями організації, які обмінюються даними, безпосередньо з внутрішніх компонентів операційної системи кожного пристрою. FortiEDR аналізує потік подій, що передували встановленню з'єднання, і визначає, чи був запит на встановлення з'єднання зловмисним. Система може забезпечити дотримання політики організації, заблокувавши запит на встановлення з'єднання, щоб запобігти крадіжці [4].

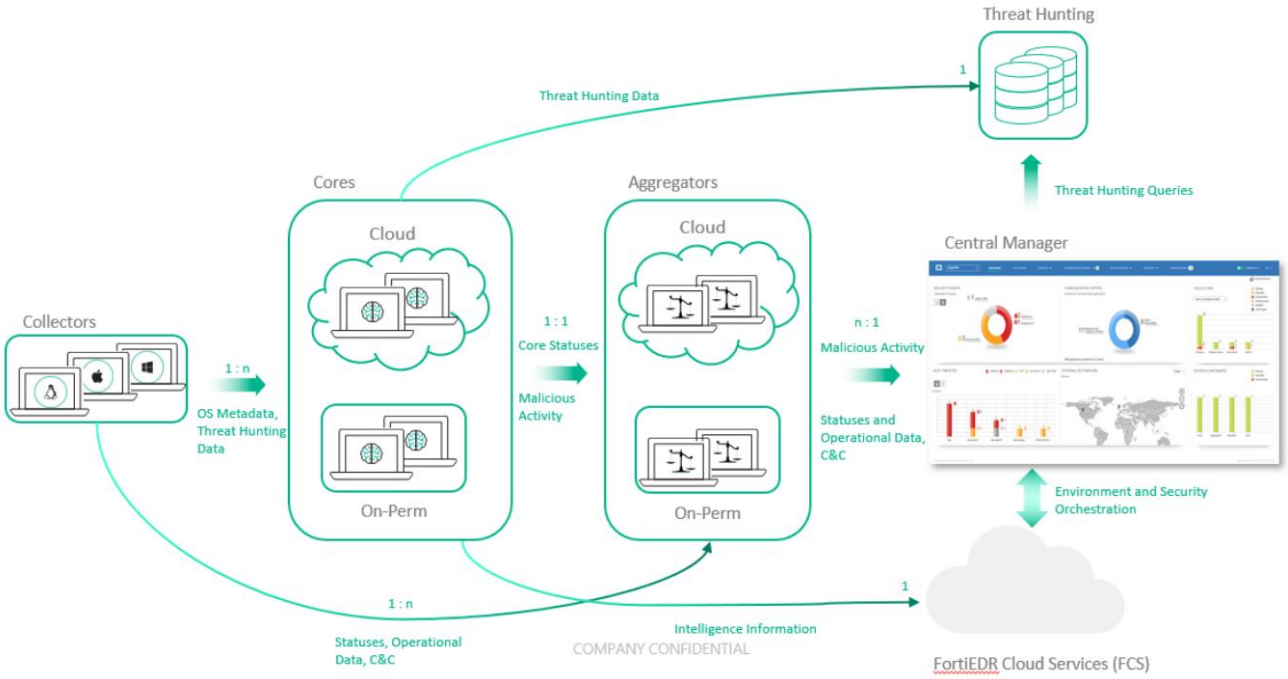

Рис. 2.2. Архітектура FortiEDR [4]

Платформа FortiEDR складається з наступних компонентів [4]:

FortiEDR Collector – це brainless-збирач, який знаходиться на кожному пристрої зв'язку на підприємстві, включаючи настільні комп'ютери, ноутбуки і сервери. FortiEDR Collector знаходиться глибоко всередині операційної системи пристрою обміну.

При кожній спробі підключеного пристрою встановити з'єднання з мережею FortiEDR Collector збирає всі необхідні метадані і відправляє їх в FortiEDR Core

(описане нижче), підписану цифровим підписом FortiEDR. Потім FortiEDR Collector утримує встановлення цього з'єднання до тих пір, поки не буде отримана авторизація від FortiEDR Core:

пройдено: законні запити дозволені з вашої мережі з вкрай незначною затримкою;

блокування: спроби зловмисного крадіжки блокуються.

FortiEDR Collector повинен бути встановлений на кожному пристрої зв'язку в організації. FortiEDR Collector може бути встановлений у всіх системах Windows, Mac і Linux. Нижче наведені зв'язки, встановлені між FortiEDR Collector і іншими компонентами FortiEDR:

У FortiEDR Aggregator: FortiEDR Collector спочатку відправляє реєстраційну інформацію FortiEDR Aggregator через SSL, а потім відправляє поточну інформацію про працездатність і стан.

Від FortiEDR Aggregator: FortiEDR Collector отримує свою конфігурацію від FortiEDR Aggregator.

В FortiEDR Core: FortiEDR Collector відправляє стислі метадані операційної системи в FortiEDR Core, а потім поточну інформацію про працездатність і стан.

Від FortiEDR Core: FortiEDR Collector отримує дозвіл на встановлення з'єднання або відмову (блокування) від FortiEDR Core.

FortiEDR Collector зберігає тільки обмежений обсяг метаданих на пристрої, щоб звести завантаження ЦП до нуля і мінімізувати вимоги до сховища. Вимоги FortiEDR до споживання трафіку низькі, оскільки FortiEDR обробляє тільки початкове встановлення з'єднання. Обсяг метаданих, що відправляються в FortiEDR Core, настільки мінімальний, що затримка на етапі прийняття рішення ядром незначна. Крім того, FortiEDR використовує стиснення повідомлень, щоб ще більше зменшити трафік, що відправляється в мережу [4].

FortiEDR Collector поставляється у вигляді стандартного пакета установника MSI, який легко встановлюється за допомогою стандартних засобів віддаленого автоматичного розгортання, таких як Microsoft SCCM. Ніякої локальної настройки або перезавантаження не потрібно; проте перезавантаження системи гарантує, що

будь-які шкідливі сполуки, які були встановлені раніше до установки, будуть заблоковані та відслідковані через FortiEDR після завершення перезавантаження. Оновлення можна виконувати віддалено, і вони рідко потрібні, тому що весь мозок системи FortiEDR знаходиться в FortiEDR Core.

Переглядач подій (Event Viewer). Засіб перегляду подій Windows записує кожного разу, коли FortiEDR Collector блокує зв'язок з пристроєм.

FortiEDR Core забезпечує дотримання політик безпеки і приймає рішення. Він визначає, чи є запит на встановлення з'єднання законним чи є зловмисною спробою крадіжки, яку, отже, мають бути заблоковано.

FortiEDR збирає дані стека ОС, дані, що відносяться до трафіків і процесів, і проводить аналіз виконуваних файлів, щоб визначити характер кожного запиту на з'єднання, як показано нижче. При роботі в режимі запобігання все запити на встановлення з'єднання у організації повинні бути авторизовані FortiEDR Core, що дозволяє йому блокувати кожен вихідний запит на встановлення з'єднання, який є шкідливим.

Коли FortiEDR Core отримує запит на встановлення з'єднання, він поповнюється метаданими, зібраними FortiEDR Collector, які описують дії операційної системи, які йому передували. FortiEDR Core аналізує потік подій, що передували запитом на підключення, і визначає, чи був запит на підключення шкідливим. Потім система застосовує політику організації, блокуючи (або тільки реєструючи) запит на з'єднання, щоб запобігти крадіжці / log exfiltration.

Збір потоку подій, що передували запитом на з'єднання, дозволяє FortiEDR визначити, де відбулося порушення. Потрібно одне або кілька ядер FortiEDR в залежності від розміру мережі в залежності від розміру розгортання (до 50 ядер FortiEDR). Нижче наведені зв'язку, встановлені між FortiEDR Core і іншими компонентами FortiEDR:

У FortiEDR Aggregator: FortiEDR Core відправляє реєстраційну інформацію при першому підключенні до FortiEDR Aggregator, а потім відправляє події і поточну інформацію про працездатність і стан.

Від FortiEDR Aggregator: FortiEDR Core отримує свою конфігурацію від

FortiEDR Aggregator.

FortiEDR Core знаходиться в точках виходу з організації. Він перевіряє тільки метадані FortiEDR Collector; він не бачить вихідного трафіку. Це центральний програмний об'єкт на базі Linux, який може працювати на будь-якій робочій станції або віртуальній машині, яким призначено статичну IP-адресу.

FortiEDR Aggregator – це програмний об'єкт, який діє як проксі для FortiEDR Central Manager і надає послуги обробки навантаження. Всі колектори FortiEDR і ядра FortiEDR взаємодіють з агрегатором для реєстрації, настройки та моніторингу. FortiEDR Aggregator збирає цю інформацію для FortiEDR Central Manager і передає конфігурації, певні в FortiEDR Central Manager, в FortiEDR.

Для більшості розгортання потрібно тільки один FortiEDR Aggregator, який можна встановити на тому ж сервері, що і FortiEDR Central Manager. Додаткові агрегатори FortiEDR можуть знадобитися для більших розгортання, що включають понад 10 000 колекторів FortiEDR, і їх можна встановити на іншому комп'ютері, а не на FortiEDR Central Manager.

FortiEDR Central Manager – це програмний центральний призначений для користувача веб-інтерфейс і внутрішній сервер для перегляду та аналізу подій і налаштування системи. FortiEDR Central Manager – єдиний компонент, який має призначений для користувача інтерфейс. Це дозволяє здійснювати [4]:

контроль та налаштування поведінки системи FortiEDR;

моніторинг та обробка подій FortiEDR;

глибокий криміналістичний аналіз проблем безпеки;

моніторинг стану і працездатності системи.

Хмарна служба FortiEDR (FCS) збагачує і підвищує безпеку системи, виконуючи глибокий, ретельний аналіз і розслідування класифікації події. FCS – це хмарна, відповідна GDPR, програмна служба, яка визначає точну класифікацію подій і діє відповідно до цієї класифікації – і все це з високим ступенем точності.

Процес класифікації подій FCS здійснюється шляхом збагачення даних і розширеного глибокого, ретельного аналізу і розслідування, що забезпечується автоматизованими і ручними процесами. Вдосконалені процеси можуть включати

(частковий список) інтелектуальні служби, аналіз файлів (статичний і динамічний), пісочницю, аналіз потоку за допомогою машинного навчання, аналіз спільнот, краудсорсінгове вилучення даних та багато іншого [4].

Поряд з потенційним підтвердженням класифікації або рекласифікацією, після підключення FCS може також дозволити кілька наступних дій, які можна розділити на два основних види діяльності [4]:

налаштування: автоматичне виключення подій (занесення в білий список). Після того, як ініційоване подія перекласифікується як безпечне, автоматичне виключення між середовищами може бути передано вниз по потоку і закінчиться термін дії події, запобігаючи його повторне спрацьовування;

дії з плейбуком: всі дії по політиці керівництва засновані на остаточному визначенні FCS.

2.3. Робочий процес рішення FortiEDR

Розглянемо типові варіанти використання рішення FortiEDR:

Безпека операційних технологій

FortiEDR запобігає, виявляє та знешкоджує загрози в середовищах операційних технологій (OT), зберігаючи при цьому машини в мережі, щоб уникнути зупинки виробництва. FortiEDR виявляє вразливості і забезпечує заходи щодо їх усунення, такі як віртуальна установка виправлень для захисту систем від експлойтів до наступного доступного періоду обслуговування. FortiEDR займає мало місця, що дозволяє підтримувати застаріле обладнання та ізольовані системи, не впливаючи на продуктивність пристрою [7].

Безпека торгових точок

FortiEDR захищає інформацію про кредитні картки в точках продажів (POS), запобігаючи атаки у джерела. Сертифікований за Стандартом безпеки даних індустрії платіжних карт (PCI DSS), FortiEDR запобігає крадіжці даних в разі злому системи. FortiEDR надає віртуальні виправлення для захисту POS-систем від вразливостей. FortiEDR пропонує підтримку вбудованих ОС з невеликими розмірами, придатними для застарілого POS-обладнання [7].

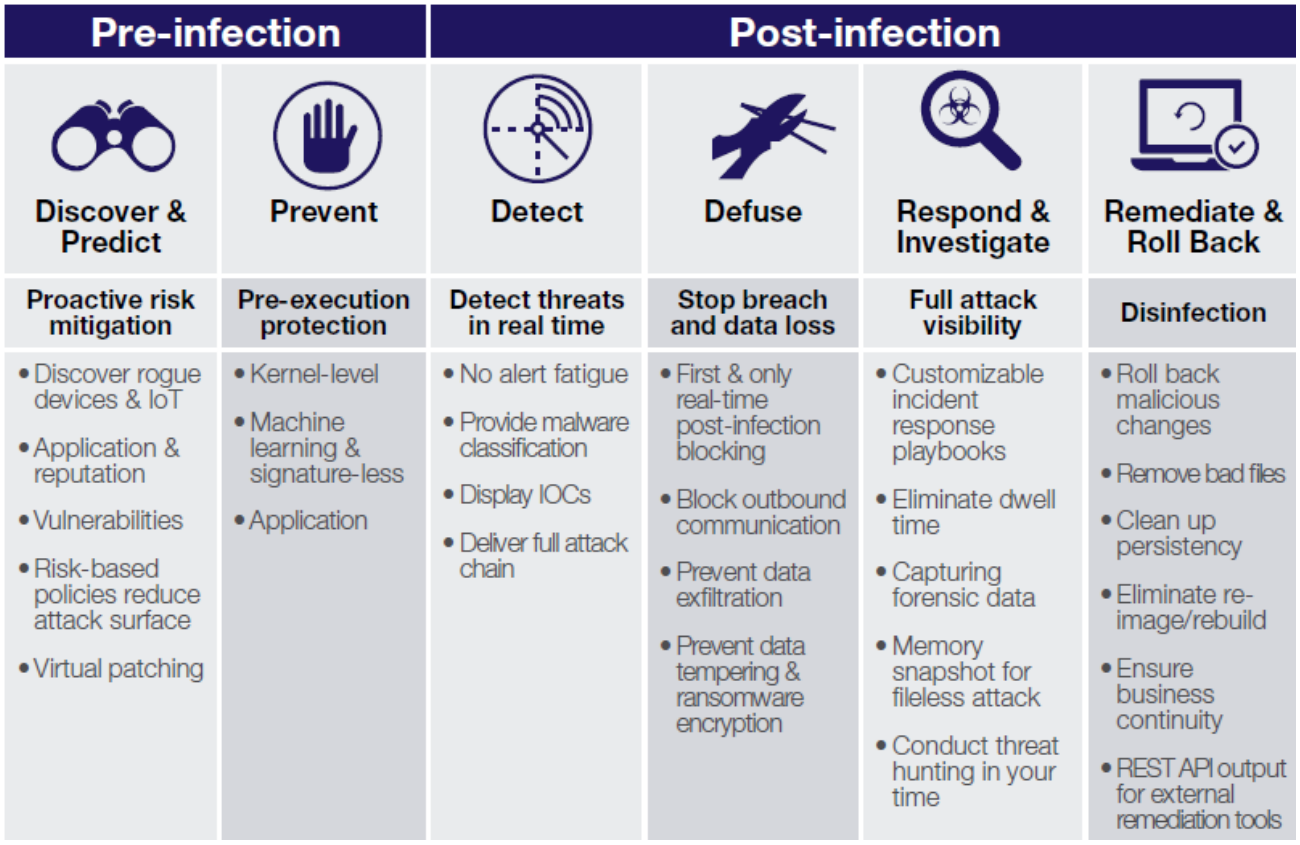

Рис. 2.3. Множина функцій рішення FortiEDR [7]

У міру постійного збільшення кількості та вдосконалення прогресивних загроз – особливо програм-вимагачів - організації повинні посилювати свої заходи безпеки в цілому, включаючи кінцеві точки OT. FortiEDR пропонує захист кінцевих точок наступного покоління, який є легким і простим для розгортання на OT-пристроях з обмеженими ресурсами. За допомогою FortiEDR команди безпеки можуть підвищити рівень безпеки кінцевих точок, тим самим пришвидшивши реакцію на інциденти, впорядкувавши операції з безпеки та уникнувши дорогих збоїв у виробничих лініях та продуктивності користувачів.

Розглянемо робочий процес рішення FortiEDR [4].

Крок 1. FortiEDR Collector збирає метадані ОС. FortiEDR Collector працює на кожному пристрої зв'язку в організації і прозоро збирає метадані ОС на обчислювальному пристрої.

Крок 2, комунікаційний пристрій робить запит на встановлення з'єднання: коли на пристрої виконується будь-який запит на встановлення з'єднання, збирач FortiEDR відправляє моментальний знімок встановлення з'єднання з ОС в FortiEDR

Core, збагачений зібраними метаданими ОС. Тим часом, FortiEDR не дозволяє встановити запит на підключення.

Крок 3. FortiEDR Core виявляє шкідливі запити. Використовуючи запатентовану технологію FortiEDR, FortiEDR Core аналізує зібрані метадані ОС і застосовує політики.

Крок 4, пройти або заблокувати: вихідний зв'язок дозволена тільки законним з'єднанням. Спроби зловмисного вихідного підключення блокуються.

Крок 5, генерація події: кожне порушення політики FortiEDR генерує подія (попередження) в реальному часі, яке упаковано з безліччю метаданих пристрою, що описують внутрішній устрій операційної системи, що веде до зловмисному запитом на встановлення з'єднання. Ця подія ініціюється FortiEDR Core, і його можна переглянути в консолі FortiEDR Central Manager. FortiEDR також може відправляти повідомлення електронною поштою та/або інтегруватися з будь-яким стандартним рішенням для управління інформацією і подіями безпеки (SIEM) через системний журнал.

Крок 6, Криміналістичний аналіз: надбудова аналізу інциденту дозволяє групі безпеки використовувати різні параметри, що надаються консоллю FortiEDR Central Manager, для більш глибокого вивчення фактичної події і даних внутрішнього стека, які до неї привели.

3 ПОРЯДОК ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ РОЗШИРЕНОГО ЗАХИСТУ КОРПОРАТИВНИХ КІНЦЕВИХ ТОЧОК ВІД ЗАГРОЗ

3.1. Варіанти застосування рішення FortiEDR

Прикладами застосування таких рішень як FortiEDR є захист операційних технологій (ОТ) та захист систем POS. Так, промислові, нафтогазові, енергетичні і транспортні організації, що використовують уразливі і застарілі системи, підтримка яких припинена, можуть стати легкою ціллю для зловмисників. Атаки на ОТ-системи несуть загрозу безперервності бізнес-процесів. Вони загрожують можливим руйнуванням важливих інфраструктур і негативними наслідками для населення [5].

FortiEDR – єдине рішення, яке забезпечує високу доступність ОТ-систем навіть у випадку виникнення інциденту безпеки або порушення. Це засіб запобігає, виявляє та знешкоджує загрози без зупинки роботи комп'ютерів. Паралельно з цим запатентована технологія трасування коду фіксує артефакти порушень і автоматизує реагування. За рахунок своєї компактності FortiEDR забезпечує підтримку і захист застарілих і вбудованих систем, що не сповільнюючи їх. У періоди між обслуговуванням FortiEDR захищає від експлойтів ОТ-системи і аналогічні їм структури в середовищах з фізичним поділом за допомогою компонентів управління функціями віртуального виправлення і усунення [5].

Також, FortiEDR забезпечує захист даних користувачів кредитних карт в системах торговельних терміналів (POS). Рішення не тільки сертифіковане відповідно до Стандарту безпеки даних індустрії платіжних карт (PCI DSS), але і запобігає крадіжці даних в разі компрометації системи. Крім того, FortiEDR в періоди між плановими обслуговуваннями усуває уразливості систем POS за допомогою функції віртуального виправлення. В процесі планового обслуговування виконується виправлення систем POS. У разі виникнення невідомих вразливостей в період між регулярними оновленнями FortiEDR

забезпечує безпеку системи. Також рішення надає підтримку вбудованої ОС. За рахунок компактності воно не уповільнює роботу систем [5].

Розглянемо варіанти застосування FortiEDR.

Розглянемо питання налаштування політик безпеки і плейбуків FortiEDR.

Політики визначають реакцію FortiEDR на події безпеки, виявлені на кінцевих точках. Конфігурація політик проводиться в розділі «Security Policies» меню «Security Settings». Користувач може застосовувати встановлені політики, що поставляються «в коробці», або створювати на їх підставі власних наборів правил [3].

У FortiEDR передбачено чотири типи політик безпеки: Execution Prevention (контроль запуску файлів), Exfiltration Prevention (запобігання витоку даних), Ransomware Prevention (протидія програмам-здирникам) і Device Control (контроль роботи пристроїв) [3].

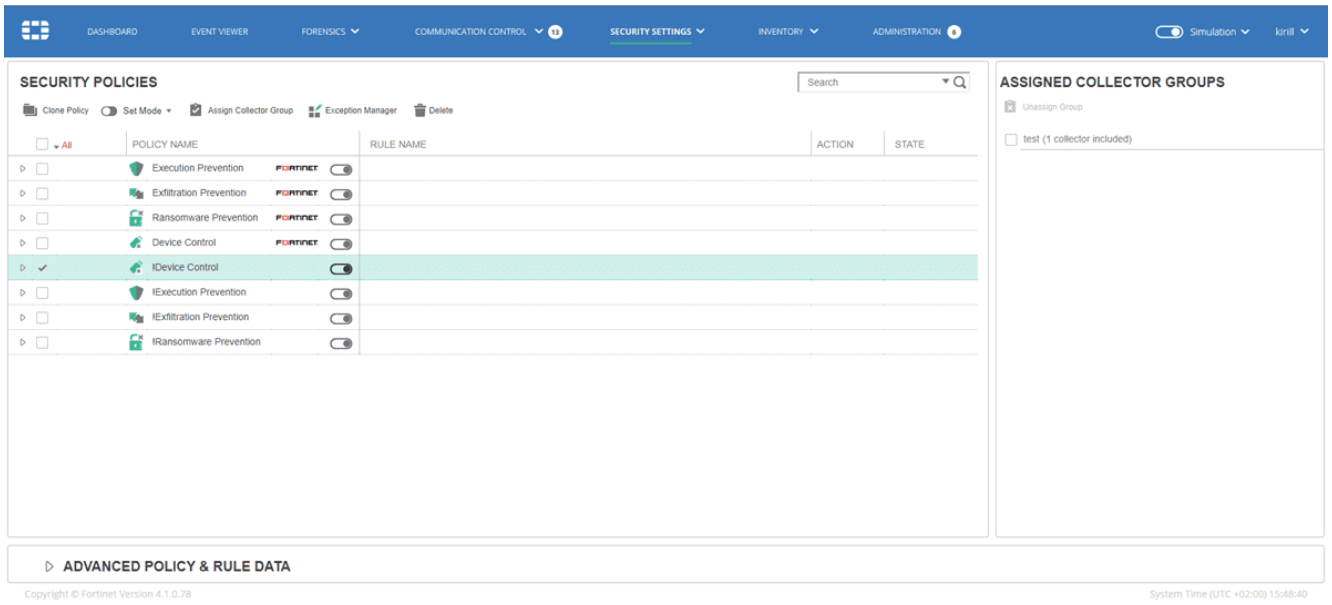

Рис.3.1. Політики безпеки в FortiEDR [3]

Кожна політика може бути налаштована на автоматичне блокування шкідливої активності або протоколювання виявлених дій в журнал для розбору адміністратором SOC. Крім цього на рівні групи політик або всіх об'єктів системи можна активувати режим «Simulation», який відключає автоматичне реагування на інциденти [3].

Політики безпеки можуть бути призначені певним колекторам або їх групам.

Таким чином адміністратор системи може гнучко налаштовувати реакцію FortiEDR на події в залежності від конкретної кінцевої точки [3].

При натисканні на конкретне правило відкривається інформаційне вікно в нижній частині екрана, де крім короткого опису обраної політики відображаються рекомендації з розслідування інциденту. Наприклад, при спробі завантаження підозрілого драйвера система радить видалити файл, перевірити його походження і виявити використання на інших пристроях, а також перейти на вкладку «Forensics» для детального аналізу проблеми [3].

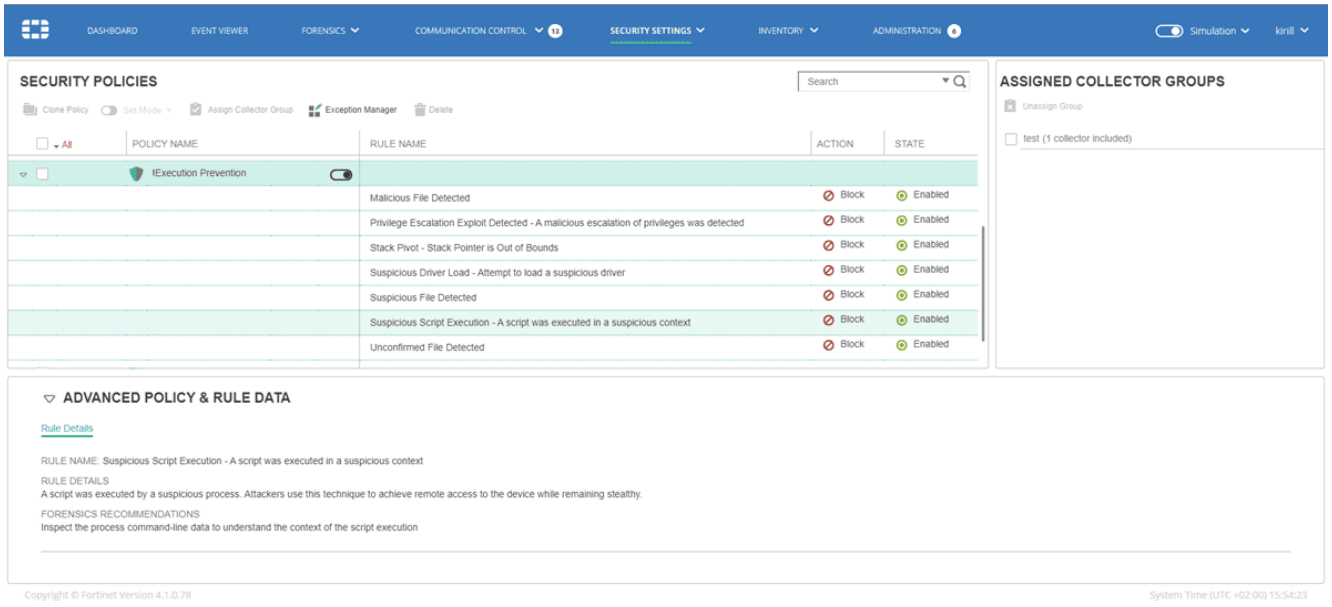

Рис. 3.2. Політики безпеки і рекомендації з розслідування інциденту в FortiEDR

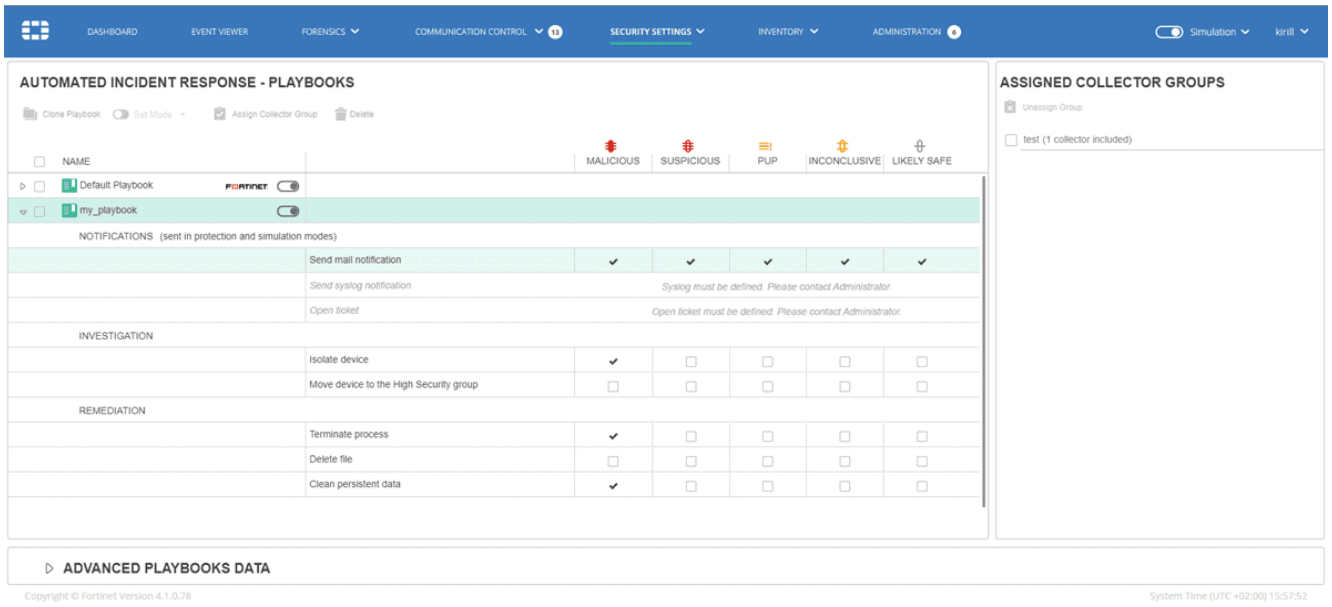

Рис. 3.3. Налаштування сценарію реагування (плейбук) в FortiEDR

За автоматизацію реагування на інциденти в FortiEDR відповідають плейбук – сценарії дій, розташовані в розділі «Playbooks» меню «Security Settings». Плейбук визначає, які саме дії виконає система при виявленні події, описаної в політиках безпеки [3].

Реакція плейбук на інцидент варіюється в залежності від ступеня загрози. FortiEDR дозволяє налаштовувати дії по п'яти градаціях небезпеки події: шкідливе (malicious), підозріле (suspicious), потенційно небажане (PUP), непідтверджені (inconclusive), швидше за все безпечне (likely safe).

Для кожного випадку можна автоматично виконати одну або кілька дій: відправити повідомлення на задану електронну пошту, вислати нотифікацію по syslog, створити тікет, ізолювати пристрій, перенести пристрій в іншу логічну групу, де до нього будуть застосовані більш суворі політики безпеки, завершити небезпечний процес, видалити шкідливий файл, відновити ключі реєстру, які були змінені шкідливою програмою, заблокувати IP-адреса, від якого виходить шкідлива активність, додавши відповідне правило для брандмауера [3].

Розглянемо такі питання розслідування інцидентів як обробка подій з області безпеки.

Всі інциденти, зареєстровані в системі FortiEDR, зберігаються в розділі «Event Viewer» головного меню. Події можуть бути згруповані за робочими станціями / колекторами або по пов'язаних з ними процесів. Вибравши конкретну подію, користувач може побачити додаткову інформацію про нього - ім'я кінцевої точки, наявність або відсутність цифрового підпису, повний шлях до ураженого об'єкту, а також причину, по якій інцидент визнаний шкідливим [3].

Для зручності користувача в нижній частині екрана виводиться графічна інформація про ланцюжок атаки – послідовність запуску шкідливих процесів, звернення до сторонніх ресурсів і інші дані, аж до блокування активності.

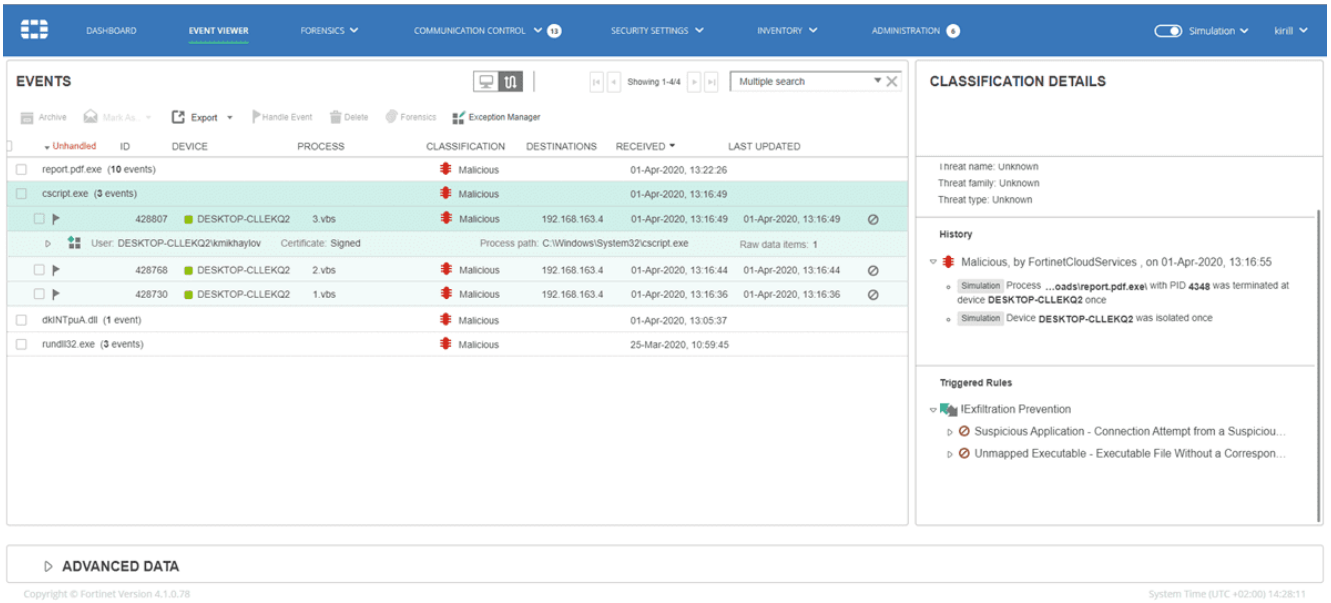

Рис. 3.4. Інформація про подію в розділі «Events» системи FortiEDR

Крім цього користувачеві доступна детальна інформація про подію, яка, зокрема, містить список спрацювали правил безпеки. Відкривши правило, можна побачити його опис, а також перелік рекомендованих дій з посиланням на відповідні техніки MITRE, якщо такі застосовні до конкретної події. Користувач має можливість відредагувати статус події: позначити його як оброблене або змінити рівень небезпеки інциденту, призначений системою.

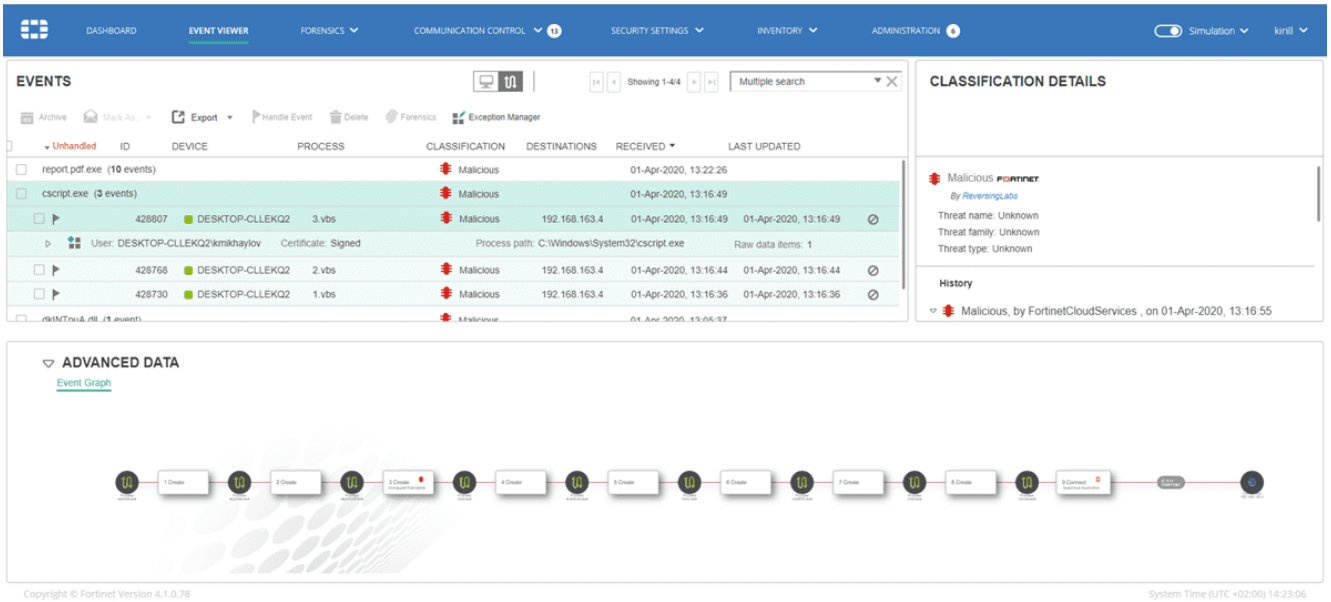

Рис. 3.5. Візуалізація ланцюжка атаки в розділі «Events» системи FortiEDR

Розслідування події зручно проводити в режимі «Forensics», який доступний зі списку інцидентів або у відповідному розділі головного меню. Тут можна

ознайомитися більш детальніше з ланцюжком атаки, кожен вузол якого може бути розкритий для отримання детальної інформації про пов'язані з ним дії.

Крім того, в розділі містяться повні дані, необхідні для аналізу події: імена хоста і користувача, операційна система, котрий ініціював дії процес, класифікація активності, призначення і мета шкідливих дій, дати виявлення і останньої зафіксованої активності, ідентифікатор інциденту, шлях до виконуваного файлу і розрядність запущеного процесу, наявність або відсутність цифрового підпису [3].

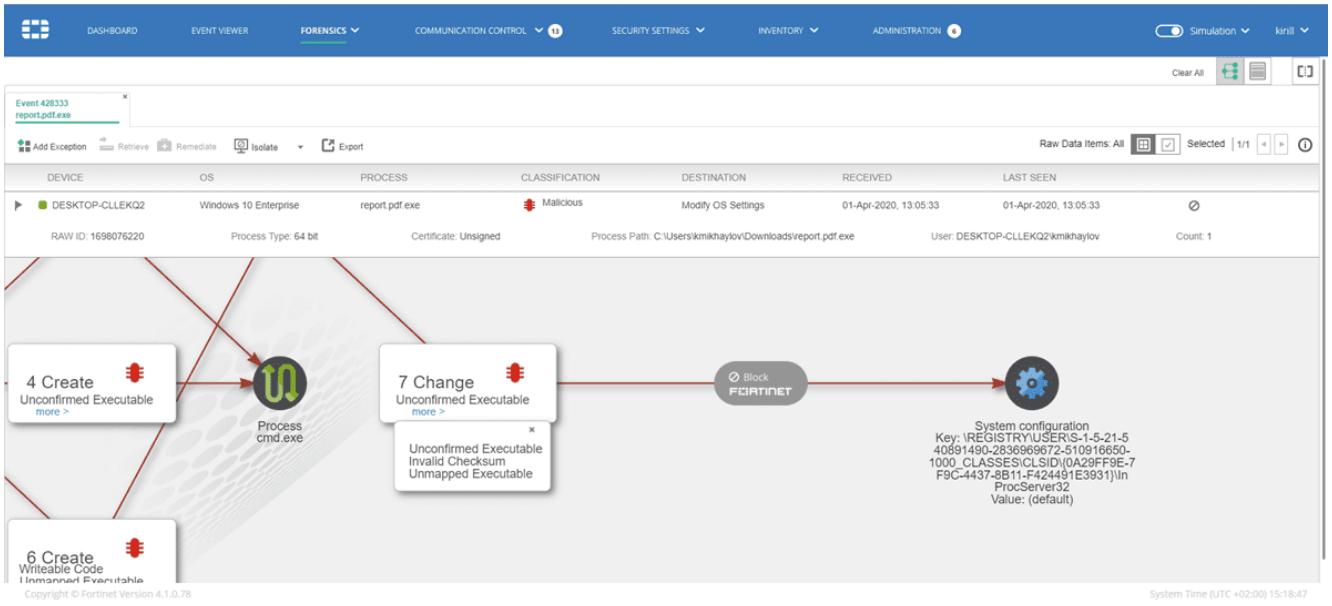

Рис. 3.6. Розділ «Forensics» в FortiEDR

Атака представлена у вигляді послідовності етапів, по кожному з яких можна отримати повну технічну інформацію, включаючи список всіх файлів, до яких звертався шкідливий процес, і адреси областей пам'яті, використані ними. Безпосередньо з розділу «Forensics» оператор SOC може зберегти дамп пам'яті, використовуваної шкідливим процесом в цілому або окремими елементами, порушеними атакою.

Подія або окремі його частини, що не представляють небезпеки, можна додати в виключення. FortiEDR дозволяє гнучко налаштовувати застосовність таких винятків - користувачеві доступні вибір конкретного колектора або групи кінцевих точок, додавання винятків тільки для зовнішніх або тільки для внутрішніх адрес. В виключення можна внести і окремі правила, що спрацювали всередині події, причому користувач має право скасувати виконання політик для конкретного

файлу в певній папці або для всіх аналогічних об'єктів незалежно від їх розташування.

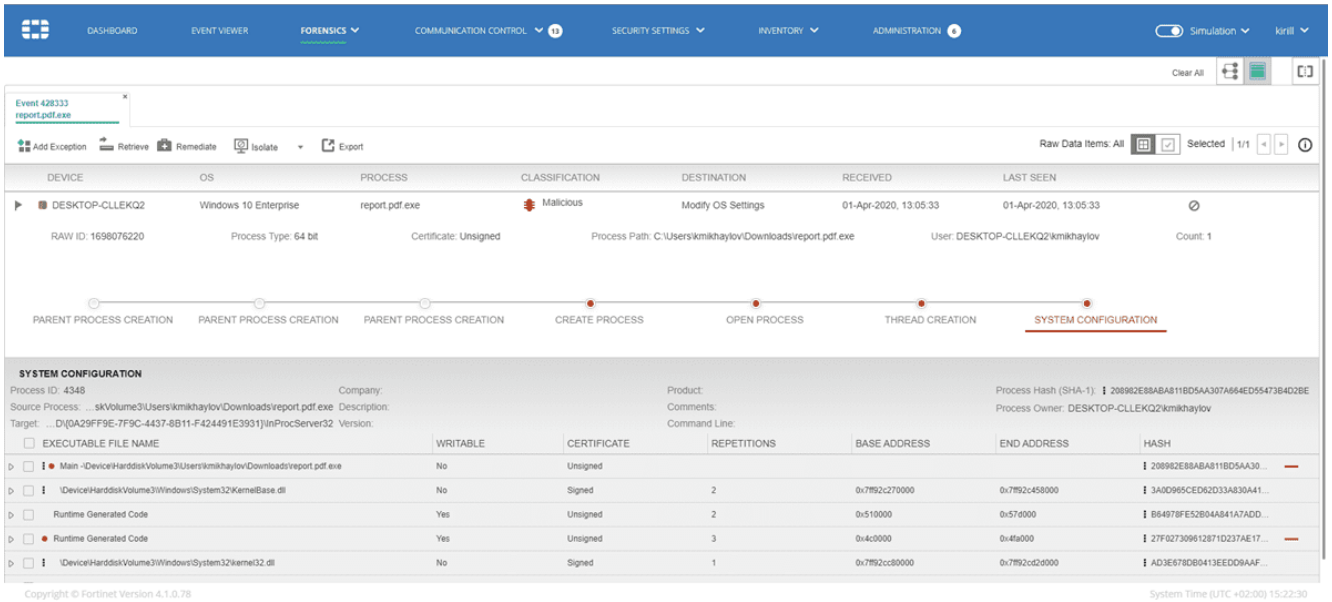

Рис. 3.7. Детальна інформація про етап кібератаки в FortiEDR

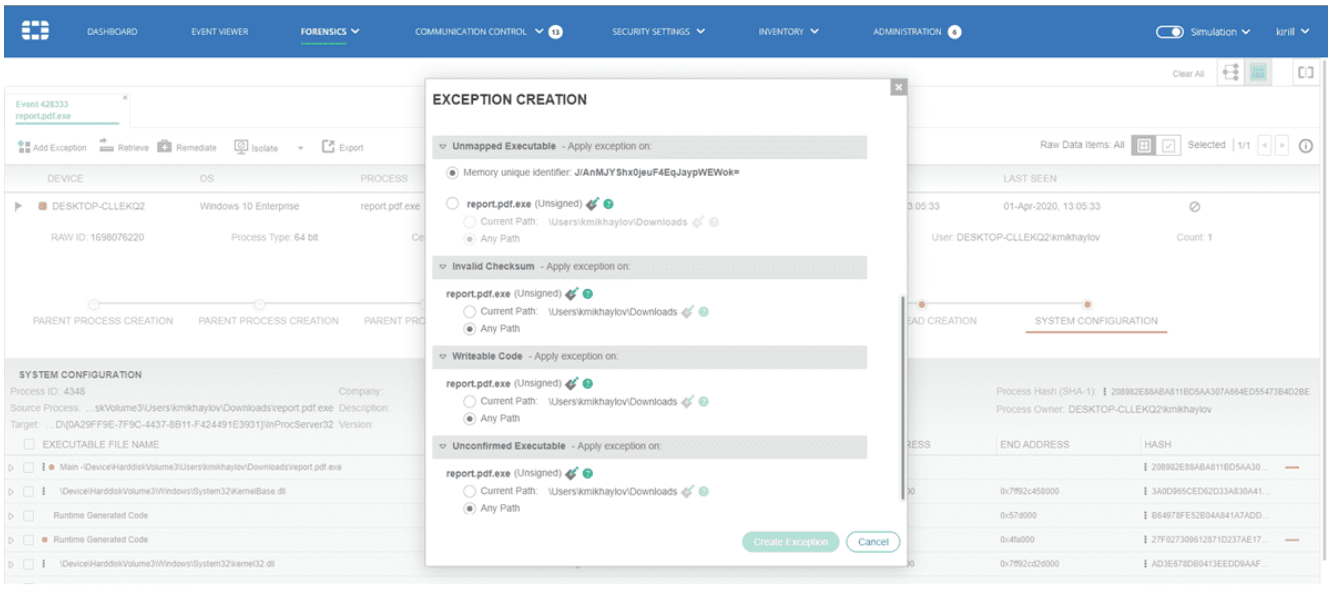

Рис. 3.8. Налаштування виключень в FortiEDR

Система надає користувачеві наступні інструменти для реакції на події [3]:

ізоляція робочої станції від мережі;

завершення шкідливого процесу;

відновлення ключів реєстру, порушених атакою;

видалення файлів, пов'язаних з процесом.

Пошук аналогічних об'єктів на всіх робочих станціях, контрольованих

FortiEDR.

Після завершення розслідування і блокування атаки оператор SOC може безпосередньо з системи запитати додаткову інформацію про подібні інциденти на сервісі VirusTotal.

Розглянемо питання як керувати з'єднаннями з мережею.

FortiEDR дає користувачеві можливість управляти мережевими з'єднаннями, які ініціюють встановлені на кінцевих точках програми. Колектор збирає інформацію про всі додатки, які звертаються до мережі, і встановлює для кожного з них рівень довіри, який отримує автоматично, з хмари. Якщо в будь-якій програмі присутні відомі уразливості, її мережеві комунікації можуть бути обмежені до моменту випуску оновлень. Таким чином експлуатація вразливостей зловмисниками буде утруднена [3].

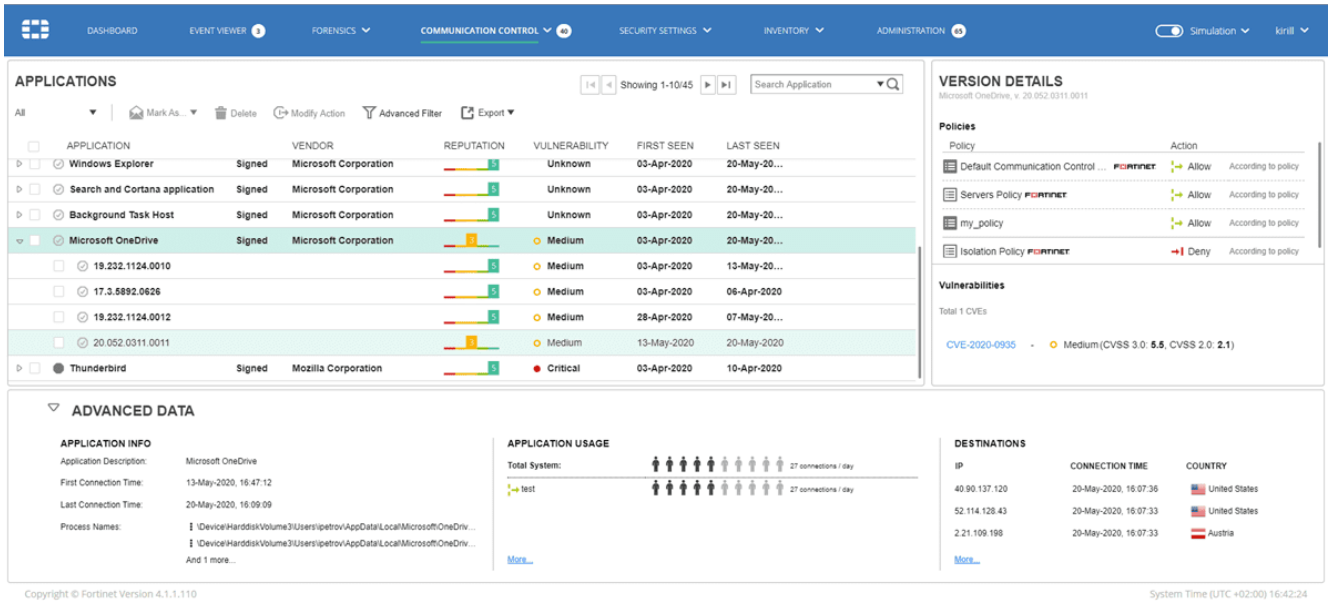

Рис. 3.9. Контроль мережевих з'єднань в FortiEDR

Користувач має можливість самостійно змінювати дії, призначені для конкретного додатка. Наприклад, заблокувати його, навіть якщо воно має статус довіреної. Крім того, є можливість встановлювати правила, що обмежують мережеву активність останнього для різних груп кінцевих точок (колекторів). Наприклад, система може бути налаштована так, щоб браузер міг без обмежень передавати дані з робочих станцій, але був ізольований на сервері [3].

У розділі «Communication Control» представлено список всіх програм, які

здійснюють мережеве взаємодія, а також детальна інформація про їх активності. Користувачеві доступні перелік політик безпеки, які застосовуються до поточної версії програми, список незакритих уразливостей з посиланням на базу даних MITRE, відомості про IP-адреси, з якими комунікувати програма, і про частоту її використання на контрольованих пристроях [3].

Розглянемо питання як управляти кінцевими точками.

У розділі «Inventory» головного меню FortiEDR користувач може включити кінцеву точку в певну групу. Для кожної групи може бути сформований унікальний набір політик безпеки, що дозволяє гнучко управляти правилами спрацьовування системи. Наприклад, можна винести пристрої віддалених користувачів в окремі групи і застосувати до них більш суворих політики безпеки.

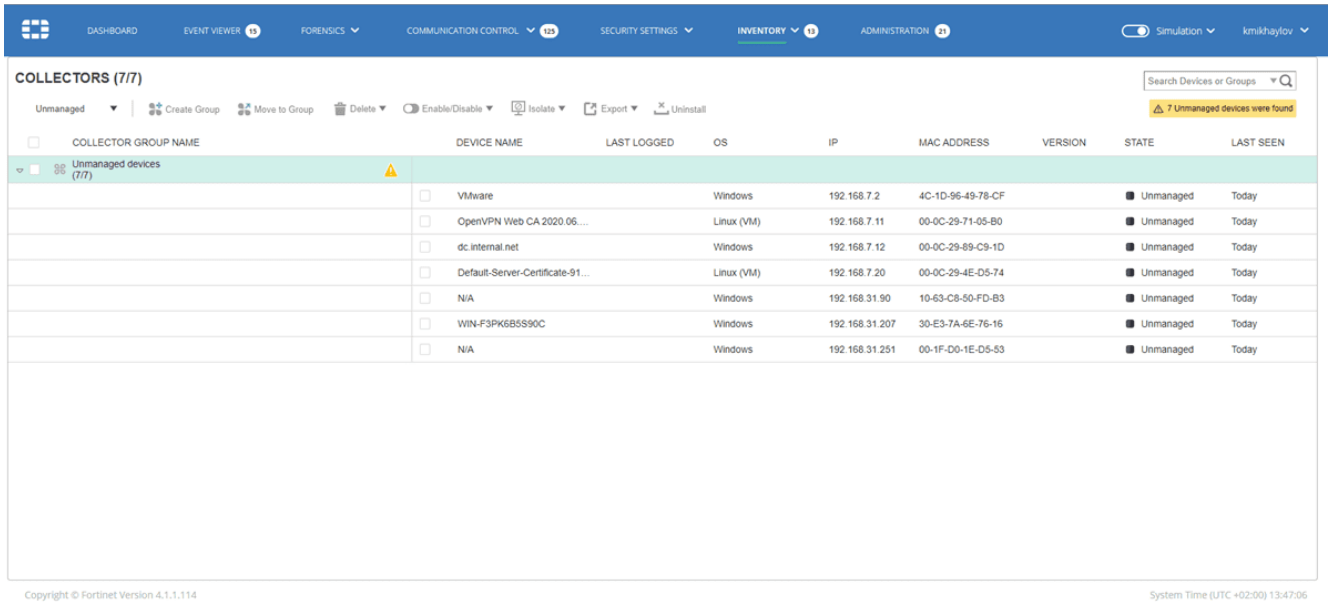

Рис. 3.10. Розділ «Inventory» системи FortiEDR

У цьому ж вікні можна отримати інформацію про поточний статус робочої станції, її MAC-адресу та версію встановленої операційної системи. При необхідності кінцева точка двома клацаннями миші ізолюється від мережі або підключається назад. Для зручності адміністратора можна вивести список комп'ютерів, на які ще не встановлені колектори, щоб визначити план розгортання агентів [3].

Розглянемо панель управління FortiEDR.

Зведена інформація про всі аспекти безпеки кінцевих точок, що знаходяться

під контролем FortiEDR, зібрана в вікні «Dashboard». В цьому розділі розміщуються графічні інформери, які настроюються та представляють у вигляді діаграм інформацію про кількість спрацьовувань системи, проблемні мережеві з'єднання, запущені колектори, згруповані за операційним системам і інші дані. З цього ж вікна можна сформувати ряд звітів, пов'язаних з роботою FortiEDR [3].

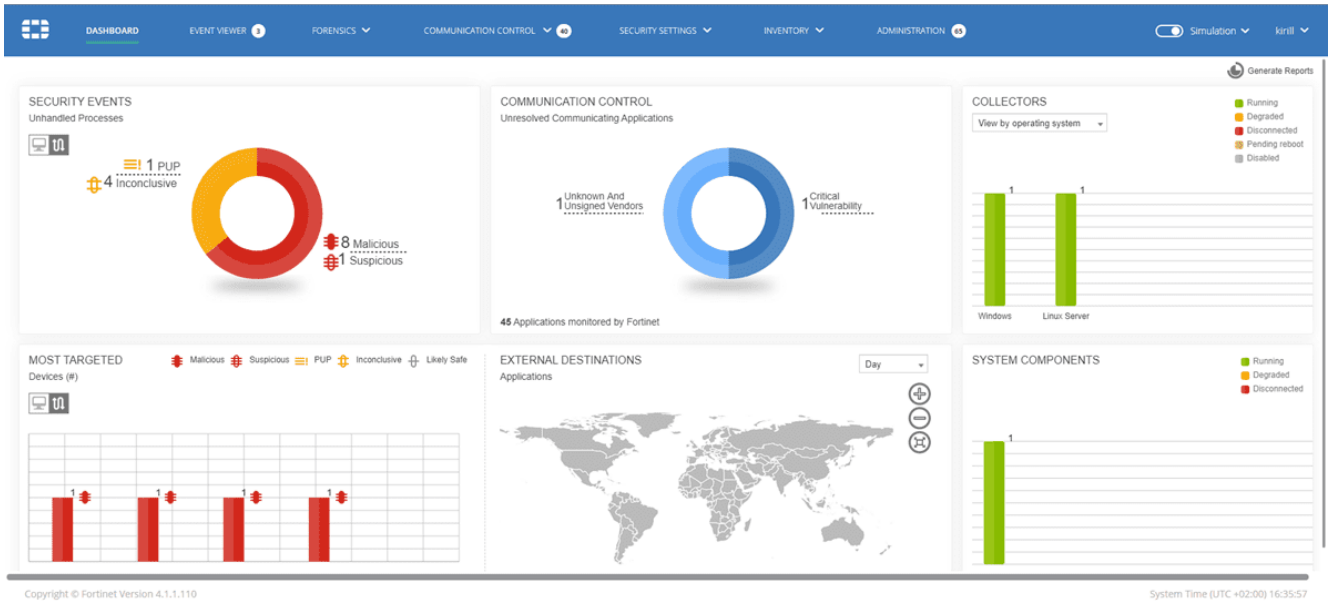

Рис. 3.11. Панель управління FortiEDR

Таким чином, рішення FortiEDR здатне істотно розвантажити операторів SOC за рахунок автоматичної реакції на типові події і надати фахівцям з безпеки можливість сконцентруватися на розслідуванні складних інцидентів.

У разі складної, цільової атаки функціональний інструментарій FortiEDR дозволяє істотно ускладнити її розвиток і в більшості випадків заблокувати шкідливу активність ще на початковому етапі. Це особливо важливо в світлі наростаючою активності програм-шифрувальників, атака яких може привести до серйозних фінансових втрат [3].

Система дає фахівцям з безпеки можливість відстежити і класифікувати активність кіберзлочинців в режимі реального часу, а також швидко вжити заходів у відповідь. Розвинені засоби автоматизації – набори політик і плейбук – дозволяють операторам SOC сконцентруватися в першу чергу на розслідуванні інцидентів, а не на оперативному реагуванні. У разі індивідуалізованої атаки управління реагуванням можна перевести в ручний режим, відключивши

блокування і залишивши тільки повідомлення про виникаючі загрози.

3.2. Рекомендації щодо розширеного захисту корпоративних кінцевих точок від загроз

Системи EDR другого покоління (рис.3.12) пропонують безліч переваг для груп безпеки, включаючи зменшення кількості попереджень, прискорене розуміння загроз і автоматизовані дії реагування на основі правил. Ці рішення EDR другого покоління підсилюють запобігання, знижують рівень шуму, прискорюють реагування і дозволяють більшій кількості аналітиків безпеки перенаправити свої зусилля на зупинку найскладніших загроз [6].

Ці важливі поліпшення в EDR дозволяють групам безпеки швидше ліквідувати прогалини, залишені рішеннями для захисту кінцевих точок, не відставати від зловмисника і зупиняти загрози до того, як станеться пошкодження, при цьому знижуючи навантаження на аналітиків з безпеки [6].

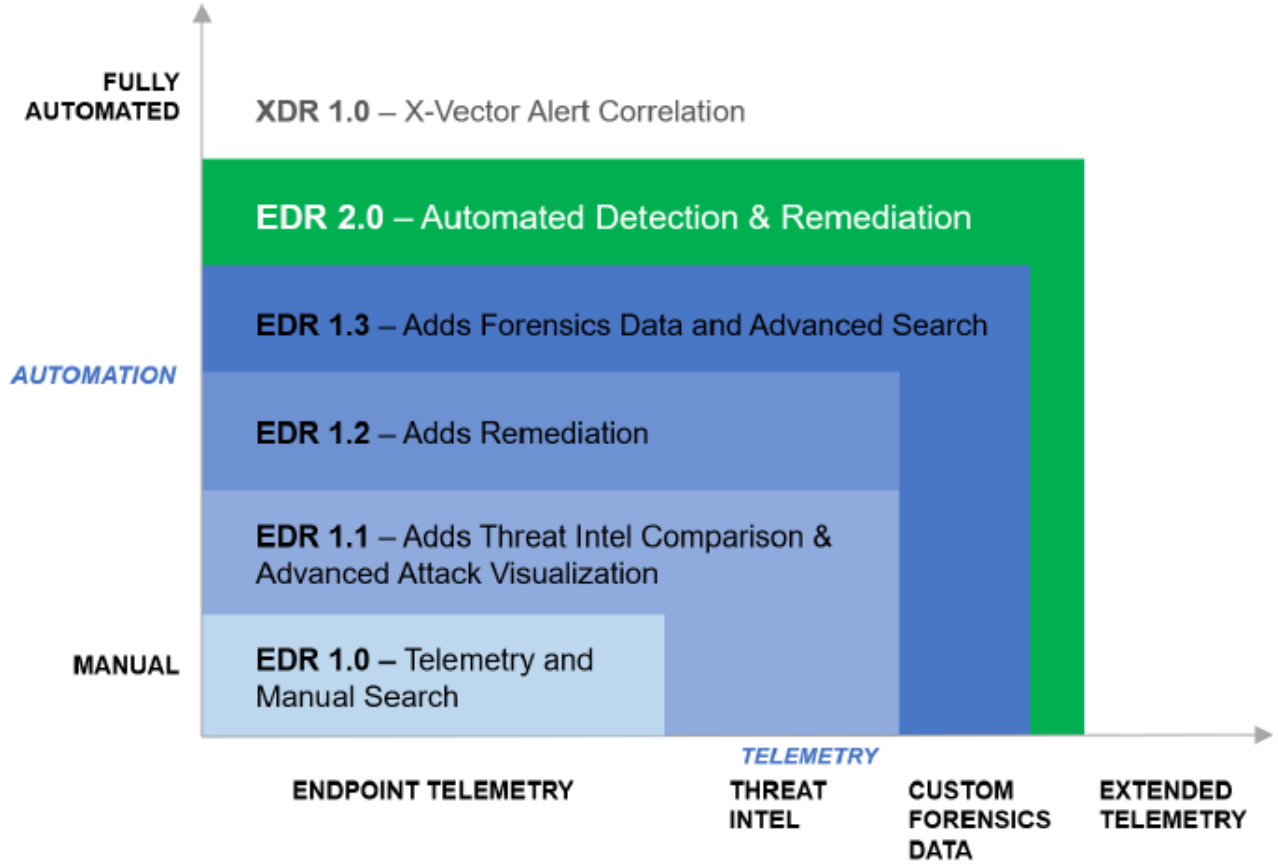

Рис. 3.12. Розвиток систем EDR [6]

Підвищення швидкості та ефективності програм виявлення і реагування вимагає ретельного балансу видимості, дослідницького аналізу і автоматизованих дій, заснованих на всебічному розумінні атаки [6].

Рішення EDR другого покоління більш тісно інтегровані з засобами запобігання, працюючи разом, щоб блокувати шкідливі або підозрілі дії в режимі реального часу. Коли рішення EDR можуть автоматично і вибірково усувати загрози, групи безпеки можуть зупинити збиток, маючи інструменти і час, необхідні для повного розслідування, зводячи до мінімуму перебої в роботі бізнесу [6].

Рішення EDR другого покоління додають керований політиками автоматичний контроль зниження ризиків, використовуючи виявлення на основі поведінки для виявлення підозрілої або зловмисної активності, яке може запускати автоматичне блокування в реальному часі для запобігання досягнення зловмисниками своїх цілей крадіжки даних, шифрування або бокового переміщення в інші цінні активи. Ці рішення часто здатні знешкодити атаку, не перериваючи нормальні бізнес-операції, шляхом вибіркової блокування вихідного зв'язку або доступу до файлової системи без необхідності повної ізоляції системи або повного завершення процесу [6].

Використовуючи автоматизовані сценарії, які настроюються, виправлення може відбуватися як негайно, так і автоматично, зупиняючи атаки до того, як вони зможуть просунутися в інфраструктурі. Коли рішення EDR можуть автоматично і вибірково швидко усувати загрози, організації можуть продовжувати роботу з мінімальним впливом на бізнес-процеси.

EDR другого покоління закладає основу для нових рівнів автоматичного виявлення і реагування, що призводить до створення більш стійкого, самовідновлювального середовища, в якому аналітики безпеки можуть переорієнтувати свій час на усунення найбільш важливих і складних загроз. 34% опитаних IT-фахівців, які нещодавно змінили постачальника засобів захисту кінцевих точок або планують змінити його, вказали на необхідність більш

ефективного виявлення загроз і реагування в якості однієї з рушійних сил переходу [6].

З додаванням цих розширених можливостей автоматизації рішення EDR другого покоління повинні дозволити організаціям швидше виявляти і реагувати, запобігати більше загроз і робити це більш ефективно, вимагаючи менше зусиль з боку висококваліфікованих аналітиків безпеки. А коли події вимагають уваги аналітика безпеки, загрози можуть бути знешкоджені під час розслідування, що обмежує збої в роботі [6].

Організації, що інвестують в EDR, повинні серйозно розглянути рішення другого покоління, які включають в себе більш автоматизовані можливості виявлення, реагування та виправлення, які можуть прискорити реагування, забезпечити відмовостійкість кінцевих точок і дозволити існуючим групам безпеки не відставати від сучасного ландшафту загроз кінцевим точкам [6].

Щоб допомогти керівникам служби безпеки вирішити ці проблеми, Fortinet пропонує послуги FortiGuard Responder Services. Служби FortiGuard Responder Services дозволяють організаціям здійснювати безперервний моніторинг, а також реагувати на інциденти і проводити судово-медичні розслідування [8].

Організації, яким необхідно прискорити зрілість SOC, отримують вигоду від комбінації розширеної безпеки кінцевих точок, що надається через FortiEDR і FortiGuard Responder Services. Вони отримують цілодобове покриття і можливість масштабувати існуючі ресурси SOC. При цьому вони можуть краще реагувати на загрози, вводити в дію процеси реагування на інциденти і уникати втоми від попереджень, не турбуючись про пропущений виявленні. Ці послуги надають стійкість команді SOC, дозволяючи молодшим співробітникам SOC брати на себе більш складні завдання, щоб організації могли робити більше за допомогою вже наявних талантів, усуваючи загрози і зловмисників. Крім того, щоденне покриття від зовнішнього постачальника дає надмірно розгалуженим групам безпеки істотну резервну копію, дозволяючи їм масштабуватися, скорочуючи при цьому середній час на виявлення і реагування [8].

При використанні корпоративних кінцевих точок, особливо під час роботи в

Інтернеті, необхідно пам’ятати, що жодна система захисту від вірусів не здатна повністю усунути небезпеку заражень і віддалених атак. Щоб досягти найвищого ступеня безпеки і комфорту, важливо використовувати рішення для захисту від вірусів належним чином і дотримуватися наступного.

Необхідно регулярно оновлювати програмне забезпечення компонентів корпоративної інформаційної системи, у тому числі засобів захисту та управління ними.

Необхідно відмітити, що фахівцями команд реагування (лабораторій) щодня виявляються тисячі нових унікальних заражень. Вони створені для обходу існуючих заходів безпеки і приносять дохід їх авторам за рахунок інших користувачів. Фахівці лабораторій постачальників засобів кіберзахисту щодня аналізують такі загрози, готують і випускають оновлення для безперервного поліпшення рівня захисту користувачів. Для максимальної ефективності цих оновлень важливо налаштувати їх належним чином на компонентах корпоративних інформаційних систем.

Автори шкідливого програмного забезпечення часто використовують різні вразливості в системі для збільшення ефективності поширення шкідливого коду. Беручи це до уваги, компанії-виробники програмного забезпечення уважно стежать за появою звітів про всі нові вразливості їх додатків і регулярно випускають оновлення безпеки, намагаючись зменшити кількість потенційних загроз. Дуже важливо завантажувати ці оновлення безпеки відразу ж після їх випуску. ОС Microsoft Windows і веб-браузери, такі як Internet Explorer, є прикладами програм, для яких регулярно випускаються оновлення безпеки.

Необхідно постійно проводити резервне копіювання важливих даних та робити копії образів налаштувань критично важливих систем.

Автори шкідливого програмного забезпечення зазвичай не піклуються про користувачів, а дії їх продуктів найчастіше призводять до повної непрацездатності операційної системи і втрати важливої інформації. Необхідно регулярно створювати резервні копії важливих конфіденційних даних на зовнішніх носіях, таких як DVD-диски або зовнішні жорсткі диски. Це дозволяє набагато простіше і

швидше відновити дані у разі збою системи.

Необхідно регулярно сканувати компоненти корпоративної інформаційної системи на наявність вірусів та вразливостей.

Багато відомих і невідомих вірусів, черв'яки, троянські програми і руткіти виявляються модулем захисту файлової системи в режимі реального часу. Це означає, що при кожному відкритті файлу виконується його сканування на наявність ознак діяльності шкідливих програм. Рекомендується виконувати повне сканування корпоративних кінцевих точок принаймні один раз на місяць, оскільки шкідливі програми змінюються, а модуль виявлення оновлюється щодня.

Необхідно дотримуватися основних правил безпеки.

Це найбільш ефективне і корисне правило – завжди треба бути обережним. На даний момент для спрацювання багатьох заражень (їх виконання і розповсюдження) необхідне втручання користувача. Якщо дотримуватися обережності при відкритті нових файлів, можна значно заощадити час і сили, які в іншому випадку будуть витрачені на усунення заражень на корпоративних кінцевих точках. Тому:

необхідно не відвідувати підозрілі веб-сайти з безліччю спливаючих вікон і анімованою рекламою;

треба бути обережним при установці безкоштовних програм, пакетів кодеків тощо. Необхідно використовувати тільки безпечні програми та відвідувати безпечні веб-сайти;

треба бути обережним при відкриванні вкладень в повідомленнях електронної пошти (особливо це стосується повідомлень, що розсилаються масово і відправлених невідомими особами);

треба не використовувати облікові записи з правами адміністратора для повсякденної роботи на корпоративних кінцевих точках.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми розширеного захисту корпоративних кінцевих точок від загроз.

Проаналізовано сучасні загрози корпоративним кінцевим точкам. Встановлено, що зловмисники застосовують багато векторний підхід до проникнення, пошуку вразливих місць в інфраструктурі підприємства та організації, ретельне вивчення існуючих засобів захисту з метою їх обходу, використання спеціально розробленого або модифікованого шкідливого коду, застосування методів соціальної інженерії, шифрування і подальшу обфускацію для виключення ймовірності виявлення.

Проаналізовано існуючі підходи до захисту корпоративних кінцевих точок. Встановлено, що велика кількість підприємств та організацій, не дивлячись на використання рішень щодо захисту кінцевих точок (EPP), все ж піддаються компрометації. Це означає, що сьогодні організаціям вже необхідні додаткові інструменти, які допоможуть їм ефективно виявляти нові, більш складні загрози, з якими вже не в змозі впоратися традиційні засоби захисту.

Проаналізовано функціональність рішень класу EDR. Встановлено, що сучасні методи захисту кінцевих точок потребують адаптації до існуючого ландшафту складних загроз і мають включати функціональність щодо виявлення комплексних атак, спрямованих на кінцеві точки, та бути здатними своєчасно реагувати на інциденти (EDR).

Досліджено існуючі методи та засоби розширеного захисту корпоративних кінцевих точок від загроз на базі FortiEDR. Встановлено, що рішення FortiEDR є повнофункціональною системою захисту кінцевих точок в режимі реального часу. Воно має розвинені засоби моніторингу та реагування, що надає змогу в випереджувальному режимі знижувати кількість напрямків атак, запобігати ураженню шкідливими програмами, виявляти і знешкоджувати потенційні загрози.

FortiEDR контролює процеси, що запускаються на робочих станціях і

серверах, виявляючи підозрілу активність і при необхідності блокуючи її. Робота FortiEDR значно звужує потенційний фронт атаки за рахунок відстеження мережевих з'єднань і автоматичного переривання шкідливих процесів. Розвинені можливості реагування дозволяють в ручному або автоматичному режимі блокувати несанкціоновані дії та ізолювати заражений пристрій.

Розглянуто варіанти застосування рішення FortiEDR. Прикладами застосування таких рішень як FortiEDR є захист експлуатаційних технологій (OT) та захист систем торгівельних терміналів (POS). Розглянуто питання адміністрування системи FortiEDR.

Розроблено рекомендації керівникам підприємств та фахівцям з кібербезпеки щодо розширеного захисту корпоративних кінцевих точок від загроз.

Таким чином, запропоновані в роботі рекомендації мають сприяти розширеному захисту корпоративних кінцевих точок від загроз та ефективному втіленню та застосуванню систем EDR в корпоративній інформаційній системі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Яна Шевченко. Обзор рынка Endpoint Detection and Response (EDR) [Електронний ресурс] – Режим доступу: https://www.anti-malware.ru/analytics/Market_Analysis/endpoint-detection-and-response-edr.

2. Robert Izquierdo. A Beginner's Guide to EDR Security [Електронний ресурс] – Режим доступу: https://www.fool.com/the-blueprint/edr/.

3. Денис Сарычев. Обзор FortiEDR, системы защиты конечных точек от сложных атак [Електронний ресурс] – Режим доступу: https://www.anti-malware.ru/reviews/FortiEDR.

4. FortiEDR Installation and Administration Guide. Version 4.2 [Електронний ресурс] – Режим доступу: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/5e261ba9-cc73-11ea-8b7d-00505692583a/FortiEDR_Installation_and_Administration_Guide_V4.2.pdf.

5. FortiEDR. Современное средство автоматизированной защиты, выявления и реагирования на угрозы безопасности конечных точек [Електронний ресурс] – Режим доступу: https://www.fortinet.com/ru/products/endpoint-security/fortiedr#use-case.

6. Dave Gruber. ESG WHITE PAPER. The Need for Speed: Second Generation EDR. [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources/esg-white-paper.

7. Boosting Endpoint Security with Real-time, Automated Incident Response [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources-content/fortinet/assets/solution-guides/file/sb-boosting-endpoint-security-with-realtime-automated-incident-response.

8. FortiGuard Responder Services Turn Alerts Into Actions [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources-content/fortinet/assets/solution-guides/file/sb-fortiresponder-services-turn-alerts-into-actions.

9. Protecting OT Infrastructures with Real-time, Automated Endpoint Security [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources-content/fortinet/assets/solution-guides/file/sb-protecting-ot-infrastructures.

10. Hidden Costs of Endpoint Security. Ransomware, Fileless Malware, and Other Advanced Cyber Threats Still Challenge Current Endpoint Protection Systems. WHITE PAPER [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources-content/fortinet/assets/white-papers/file/wp-hidden-costs-endpoint-security.

11. Наконечний Максим Юрійович. Технологія розширеного захисту корпоративних кінцевих точок від загроз на базі FortiEDR. ВСЕУКРАЇНСЬКА НАУКОВА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ». Державний Університет Телекомунікацій. 27 жовтня 2021. Тези доповідей. С. 40 – 42. http://www.dut.edu.ua/uploads/p_2099_79407917.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)