ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2024. No. 2 (28)*

УДК 004.056.5 DOI: https://doi.org/10.30837/2522-9818.2024.2.182

К. Шуліка, Д. Балагура, А. Смірнов, Д. Непокритов, А. Литвин

МЕТОД ВИКОРИСТАННЯ СУЧАСНИХ СИСТЕМ ЗАХИСТУ КІНЦЕВИХ ТОЧОК (EDR) ДЛЯ УБЕЗПЕЧЕННЯ ВІД КОМПЛЕКСНИХ АТАК

Предметом дослідження в статті є архітектура систем захисту кінцевих точок (EDR) та агентів EDR як їх базового складника з погляду механізмів виявлення комплексних атак на інформаційно-комунікаційні системи (ІКС) та протидії загрозам. **Мета роботи** – розроблення методу підвищення ефективності використання систем захисту кінцевих точок для зниження ризиків компрометації ІКС інформаційних, промислових та інфраструктурних об’єктів щодо ефективного перерозподілу та використання механізмів EDR, команди з кібербезпеки та інших ресурсів для здійснення заходів з організації безпеки на підприємстві, в установі чи організації. У статті розв’язуються такі **завдання**: огляд та аналіз систем EDR; дослідження архітектури EDR-рішень та агентів EDR, особливостей їх використання, логіки побудови методів і механізмів виявлення загроз для системи з боку зловмисників та зловмисного коду; надання рекомендацій щодо організації ІКС для її захисту загалом та окремих елементів, а також з огляду на наявні сили (команда із кіберзахисту, її кваліфікація та рівень обізнаності в архітектурі EDR-рішень) та засоби (елементи EDR-систем) для організації захисту. Упроваджуються такі **методи**: моделювання механізмів атак, моделювання поведінки зловмисника. **Досягнуті результати**: сформульовано загальні та конкретні рекомендації щодо оптимізації роботи EDR-систем та забезпечення ефективного використання елементів EDR-систем у інформаційно-комунікаційних мережах підприємств чи організацій різного типу та спрямованості залежно від ресурсів і наявної інформації з погляду необхідності її захисту. **Висновки**: запропоновані рекомендації щодо застосування EDR-механізмів для захисту інформаційних систем і мереж дають змогу оптимізувати витрати на створення інфраструктури захисту та здійснення відповідних заходів з огляду на особливості наявного інструментарію, навченості та обізнаності команди з кібербезпеки як щодо часу реакцій на загрози, так і з погляду складності та вартості виконання завдань із захисту.

Ключові слова: інформаційно-комунікаційні системи (ІКС); EDR-система; операційний центр безпеки SOC; EDR-агент; аналіз загроз; політика EDR; виявлення атак.

Вступ

Комп’ютерна мережа будь-якого промислового підприємства завжди є під загрозою проникнення з боку зловмисників для отримання чи знищення конфіденційної інформації, руйнування мережі чи інших зловмисних дій, зокрема вимагання коштів за збереження даних недоторканими. Наприклад, відповідно до *Statista* [1], незважаючи на певне зниження темпів зростання за останні два роки, кількість організацій, що постраждала від атак програм-вимагачів, продовжує впевнено зростати впродовж останніх шести років (рис. 1). Зауважимо, що це тільки офіційно зареєстровані атаки, тобто ті, які вдалося виявити. Кількість атак, що встановити не вдалося, підрахувати неможливо.

Зазначений графік відтворює тільки один з безлічі варіантів, які зловмисники можуть використовувати для власного збагачення або знищення інформації, що належить якій-небудь компанії, і, відповідно, самої компанії.

Тому нині неможливо уявити функціонування будь-якої інформаційно-комунікаційної системи організації чи промислового підприємства без систем захисту інформації.

Водночас захист даних у будь-яких мережах, починаючи від відкритих інтернет-мереж та IoT [2] і завершуючи мережами промислових об’єктів, без застосування комплексних антивірусних рішень є достатньо складним, оскільки кількість загроз збільшується щодня й тільки проактивний підхід до безпеки дає змогу ефективно виявляти та протистояти сучасним кіберзагрозам [3]. Рішення EDR наразі є лідерами ринку для протидії сучасним кіберзагрозам. На їх основі було створено XDR- та XSOAR-системи, що доповнюють та автоматизують захист кінцевих точок мереж.

Використання EDR-систем потребує достатнього рівня знань у сфері кібербезпеки, навичок розслідування та реагування на інциденти [4], а також високого рівня обізнаності про архітектуру рішення та розуміння "сліпих зон", особливостей

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №2 (28)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

та недоліків типового EDR-рішення для попередження комплексних атак на інфраструктуру, зокрема від DOS/DDOS-атак і до XSS-атак [5]. Аналіз архітектури агента EDR необхідний, щоб зрозуміти особливість типового рішення та висунути низку рекомендацій, що дадуть змогу ефективно виявляти й протидіяти комплексним атакам на ІКС у майбутньому.

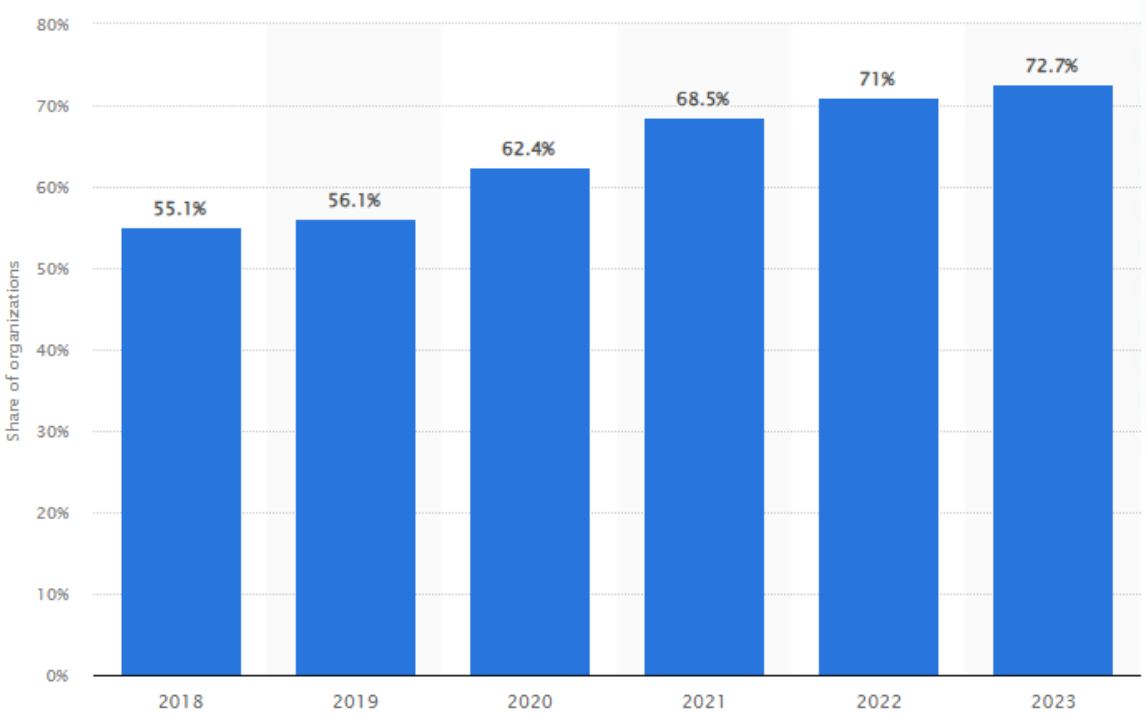

Рис. 1. Річна частка організацій, постраждалих від атак програм-вимагачів у всьому світі впродовж 2018–2023 рр.

Постановка завдання

Метою статті є розроблення методу підвищення ефективності використання EDR для зниження ризиків компрометації ІКС інформаційних, промислових та інфраструктурних об’єктів з погляду ефективного перерозподілу та використання наявних механізмів систем захисту кінцевих точок EDR, команди з кібербезпеки та інших ресурсів, призначених для здійснення заходів з організації безпеки на підприємстві, в установі чи організації.

Для реалізації окресленої мети виконуються такі завдання: огляд та аналіз наявних систем EDR, аналіз архітектури EDR-рішень та агентів EDR, особливостей їх використання, логіки побудови методів і механізмів виявлення загроз для системи з боку зловмисників і зловмисного коду. Окремо надаються рекомендацій щодо організації ІКС для її захисту загалом та окремих елементів, а також з огляду на наявні сили (команда із кіберзахисту, її кваліфікація та рівень обізнаності в архітектурі EDR-рішень) та засоби (елементи EDR-систем) для організації захисту.

Аналіз публікацій

Рішення EDR – це достатньо нова технологія, основана на механізмах так званих "класичних антивірусів" NGA (*Next Generation Antivirus*), що отримав таку назву з 2013 р. [7]. Оскільки цей клас рішень надавав небачену до цього можливість у реальному часі реагувати на загрози (*Prevention*), EDR швидко стали популярними в різних сегментах економіки.

Технологія показала свою ефективність завдяки застосуванню сенсорів – програмних давачів, що EDR розподіляє в операційній системі та надалі використовує для моніторингу активності [7].

У цьому разі впровадження технології за умови ігнорування рекомендацій призводить до того, що зловмисники можуть здійснювати атаки різних типів для обходу EDR: обхід конфігурації, обхід сприйняття, логічний обхід та обхід класифікації [3, 7]. Додаткові рекомендації до експлуатації EDR зазвичай подаються у вигляді звітів про обхід конкретного рішення та містять інструкції для команд з кібербезпеки про виправлення поданої

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 2 (28)

вразливості [4, 6]. Недолік такого підходу полягає в тому, що рекомендації в цьому разі точкові й не допоможуть захистити себе всебічно. Для значного посилення безпеки використання EDR недостатньо убезпечити себе від одного типу обходу EDR – необхідно починати посилювати безпеку з моменту встановлення рішення в межах корпоративної інфраструктури.

Системи захисту кінцевих точок

Системи захисту кінцевих точок EDR (*Endpoint Detection and Response*) [6–8] – це корпоративні антивірусні рішення, що забезпечують багаторівневий підхід до захисту кінцевих точок у межах корпоративної інфраструктури та набули значного поширення в останні роки. Вони використовуються для виявлення та реагування на загрози на кінцевих точках, таких як настільні ПК, ноутбуки, сервери. Також для забезпечення безпеки хмарних сховищ і мобільних пристроїв було створено XDR-рішення, що фактично є розширеннями класичних EDR.

Особливістю, що відрізняє EDR-рішення від EPP (*Endpoint Protection Platform*) – гілки розвитку класичних антивірусів, – є здатність до реагування на інцидент безпеки: блокування процесів та ізоляції зараженого пристрою. Ізоляція означає, що EDR забороняє хід трафіку по всіх портах, окрім виділеного, зазвичай 443, що спілкується з вебконсоллю EDR. Фактично в момент ізоляції доступ зловмисника до пристрою переривається, як і будь-які інші під'єднання, і обмежений віддалений доступ до хоста може мати тільки оператор консолі EDR.

За останнє десятиліття рішення EDR значно вдосконалилися. Сучасні EDR зазвичай інтегровані з іншими рішеннями безпеки, такими як SIEM і платформи аналізу загроз (*threat intelligence*), щоб забезпечити більш повне покриття для корпоративної інфраструктури.

Архітектура EDR

EDR-рішення містять серверну частину та агентів – невеликих за розміром програм, що встановлюються на кінцеві точки (ПК та сервери). Серверна частина рішення, що забезпечує доступ до менеджменту всіх агентів у форматі вебсторінки, може бути розгорнута в хмарному рішенні або на окремому сервері (*on-prem*). Друге рішення є дорожчим і здебільшого підходить для компаній закритого типу або державних установ та об'єктів критичної інфраструктури.

Наразі EDR конкурують з XDR, що фактично є їх розширеною версією, але щодо бізнесу вони ефективні для різних типів компаній. Якщо EDR більш призначені для захисту фізичних і віртуальних кінцевих точок (робочих станцій фахівців, серверів, віртуальних станцій у контейнерах), то XDR розширюється ще на хмарне середовище, смартфони тощо.

Також варто зауважити, що 2024 р. такі інструменти, як EDR, містять достатню кількість додаткових модулів, що дають змогу розширити це базове корпоративне антивірусне рішення в бік, необхідний бізнесу. Для прикладу, додатково до базового функціоналу *Crowdstrike*, призначеного саме для захисту кінцевих точок, можна докупити модулі моніторингу внесення критичних змін, моніторингу USB-пристроїв, пошуку загроз, менеджменту застосунків тощо. Сучасні EDR дають змогу легко масштабувати рівень видимості в умовах корпоративної інфраструктури, будучи певним "конструктором" інструментарію для команди з кібербезпеки.

EDR є класом корпоративних рішень, що активно використовуються в сучасних операційних центрах безпеки (SOC) [9]. SOC є пунктом, де оцінюється кожна подія, що стосується безпеки кінцевих точок і збирається агентом EDR, в якому аналітики з кібербезпеки всебічно розглядають зібрану інформацію та приймають остаточне рішення про інцидент безпеки. Для кожного із спрацювань, що було сформовано з цих подій, аналітики SOC мають вирішити, як їх класифікувати та як діяти надалі.

Архітектура агентів EDR як базових елементів EDR-систем

Агент EDR – це невелика програма, що є базовим складником системи. Вона контролює та споживає дані з компонентів сенсора, виконує базовий аналіз і визначає, чи відповідає активність або серія подій поведінці зловмисника. Далі агент EDR пересилає телеметрію на головний сервер, який аналітик надалі бачитиме як хмарний складник EDR-рішення, далі – вебконсоль, що аналізує події від усіх агентів, розгорнутих в інфраструктурі

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2024. №2 (28) ISSN 2524-2296 (online)

бізнесу. Якість інформації, що отримується агентами, багато в чому визначає якість захисту за допомогою EDR, тому їх налаштування, параметри та особливості використання є базовими для ефективного застосування EDR загалом.

Більшість EDR-рішень спрямована на те, щоб навантажувати кінцеві точки менше, ніж на 1–5% CPU. Також варто зауважити, що розгортання рішення типу EDR можливе тільки після аналізу та оптимізації локальної мережі компанії, впорядкування всіх наявних активів, укладання списків використовуваних програм і створення моделі загроз, моделі порушника та написання внутрішніх політик. Основна мета створення переліченої документації – не завадити бізнес-процесам компанії, оскільки, як побачимо далі, агент має здатність блокувати процеси без можливості легко обійти блокування.

Якщо агент вважає, що певна активність є аномальною і варта уваги, він може виконати одну з таких дій [10]:

– зареєструвати зловмисну активність у вигляді сповіщення про інцидент, надісланого до консолі – інформаційної панелі EDR, або перенаправити сповіщення в центр агрегації даних SIEM;

– заблокувати виконання зловмисної операції, повернувши програмі, яка виконує дію, значення, що вказують на збій;

– увести в оману зловмисника, повернувши йому неправильні значення, такі як неправильні адреси пам’яті або модифіковані маски доступу, що змусить зловмисне програмне забезпечення вважати, що операція завершилася успішно, навіть якщо подальші дії не вдається виконати.

Кожен давач, що є складником агента EDR на хості, слугує загальній меті: збору телеметричних показників. Простіше, телеметрія – це необроблені дані, що генеруються компонентом агента або самим хостом, та фахівці SOC-центру можуть аналізувати їх як вручну, так і за допомогою вбудованих аналітичних механізмів EDR (як машинне навчання та динамічний аналіз), щоб визначити, чи мала місце зловмисна активність. Кожна дія в системі – від відкриття файлу до створення нового процесу – генерує певну форму даних для поповнення телеметрії. Ця інформація є відправною точкою у внутрішній логіці сповіщення про інциденти безпеки.

Можна порівняти телеметрію з показниками, що збирає радіолокаційна система: радари використовують електромагнітні хвилі для виявлення присутності, курсу та швидкості об’єктів у певному діапазоні. Коли радіохвиля відбивається від об’єкта й повертається до радіолокаційної системи, вона створює точку на дисплеї радару, яка вказує на те, що там щось є [11]. Використовуючи ці точки даних, процесор радарної системи може визначити такі параметри, як швидкість, місце розташування та висоту об’єкта, а потім обробляти кожен випадок по-різному. Наприклад, система може реагувати на об’єкт, що летить на низькій швидкості на малій висоті, інакше, ніж на об’єкт, що летить на значній швидкості на великій висоті. Це дуже схоже на те, як EDR обробляє телеметрію, зібрану його сенсорами. Сама по собі інформація про те, як було створено процес або отримано доступ до файлу, рідко забезпечує достатній контекст для прийняття обґрунтованого рішення щодо подальших дій. Крім того, процес, виявлений радаром, може припинитися будь-якої миті. Тому важливо, щоб телеметрія, яка надходить до EDR, була якомога повнішою.

EDR передає інформацію телеметрії до агента, а потім, якщо необхідно, до хмарного сховища, у компонентах яких прописана комплексна логіка виявлення загроз. Алгоритми логіки виявлення аналізують всю доступну телеметрію й за допомогою внутрішніх методів, зокрема евристики навколишнього середовища або бібліотеки статичних сигнатур, установлює, чи була активність зловмисною і чи досягла вона порогу критичності для створення повідомлення про атаку для аналітиків або блокування процесу для запобігання комплексній атаці.

Якщо телеметрія – це виявлені об’єкти на радарі, то сенсори – це передавач, дуплексор і приймач, тобто компоненти, що відповідають за виявлення об’єктів і формування їх у повідомлення для аналітиків, що працюють з консоллю EDR. Тоді як радіолокаційні системи постійно відправляють повторні сигнали до об’єктів, щоб відстежувати їх переміщення, давачі EDR працюють трохи пасивніше, перехоплюючи дані, що проходять крізь внутрішній процес, витягуючи інформацію та пересилаючи її центральному агенту. Оскільки ці давачі мають бути вбудовані в якийсь системний процес, також необхідно, щоб вони працювали неймовірно швидко. Середньостатистичний давач, який відстежує запити до реєстру, виконує свою роботу за 5 мс, перш ніж операція з реєстром буде дозволена та зможе продовжуватись. Це не здається значною проблемою, доки не буде взято до уваги, що в сучасних системах за секунду можуть відбуватися тисячі запитів до реєстру.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 2 (28)

Маленька затримка у 5 мс, що виникне в процесі оброблення 1 тис. подій, призведе до п'ятисекундної затримки в роботі системи. Більшість користувачів вважатимуть це неприйнятним, що відштовхне клієнтів від використання EDR взагалі. Хоча *Windows* має численні джерела телеметрії, продукти EDR, як правило, використовують лише деякі з них. Це пов'язано з тим, що багатьом джерелам бракує якості або кількості даних, вони можуть не відповідати вимогам безпеки комп'ютера або бути важкодоступними.

Деякі компоненти сенсора вбудовані в операційну систему, наприклад, у журнал подій ОС. EDR також можуть впроваджувати в систему драйвери, DLL, що перехоплюють функції, і мініфільтри, що будуть компонентами сенсорів. Фахівці атакуючих команд *(red team*), що превентивно виконують пошук вразливостей організації для того, щоб зменшити ризик успішної кібератаки, здебільшого дбають про запобігання, обмеження або нормалізацію (наприклад, змішування з потоком) зібраної сенсором телеметрії. Метою цієї тактики є зменшення кількості "точок на радарі", тобто показників, які алгоритми EDR можуть зіставити та використати для створення детального сповіщення про атаку для аналітика, що міститиме всю інформацію про активність зловмисника, а також попередить виконання зловмисних дій, блокуючи їх запуск. Власне, ми намагаємося згенерувати *False Negative* алерт, що згадувався раніше як тип алертів у SOC-центрі. Розуміючи кожен компонент давача EDR і телеметричні показники, які він збирає, можемо приймати обґрунтовані рішення щодо реагування на підтверджені інциденти безпеки та запобігання обходу корпоративного EDR.

Виявлення інцидентів безпеки – це логіка, що пов'язує окремі фрагменти телеметрії з певною поведінкою, поміченою в системі. Механізм виявлення може перевіряти окрему умову (наприклад, наявність файлу, геш якого збігається з гешем відомого шкідливого програмного забезпечення) або складну послідовність подій, що надходять із багатьох різних джерел (наприклад, що був створений дочірній процес *chrome.exe*, який потім зв'язався через TCP-порт 88 з контролером домену).

Як правило, інженер, що проєктує механізм виявлення, пише правила на основі наявних сенсорів. Вони мають ретельно зважати на масштаб, оскільки виявлення, вірогідніше за все, вплине на значну кількість організацій. З іншого боку, інженери з виявлення, які працюють в організації клієнта, який замовляє EDR для своєї компанії, найчастіше члени команди захисників (*Blue Team*), можуть створювати правила, що розширюють можливості EDR за межами тих, що надає постачальник ПЗ, щоб пристосувати виявлення інцидентів безпеки до потреб інфраструктури (створення списків, дозволених і заборонених для виконання програм, створення списку власних індикаторів компрометації, написання специфічних для організації правил тощо).

Логіка виявлення EDR зазвичай існує в агенті та підпорядкованих йому давачах або у внутрішній системі збору даних (системі, якій підпорядковуються всі агенти організації), до якої аналітики мають доступ за допомогою вебконсолі. Іноді вона функціонує в певній комбінації цих двох систем. У кожного підходу є переваги й недоліки. Виявлення, реалізоване в агенті або його давачах, може дозволити EDR вжити негайних превентивних заходів (блокування, ізоляція тощо), але не дасть йому змоги проаналізувати складну ситуацію, коли дій зловмисника багато й наявна значна кількість індикаторів компрометації. І навпаки, виявлення, реалізоване у внутрішній системі збору даних, може підтримувати величезний набір правил виявлення, але призводить до затримок у вжитті будь-яких попереджувальних заходів.

Усі EDR-продукти, що є на ринку, побудовані за однією логікою, яка відрізняється від платформи до платформи, на якій встановлено рішення [12, 13]. У цій роботі розглядаємо алгоритми й методи, що використовуються на платформі *Windows*, оскільки наразі вона залишається найбільш популярною операційною системою у світі (69% всіх користувачів; для порівняння – *macOS* застосовують лише 21% користувачів), а це приблизно 1,4 більйона активних пристроїв.

"Крихкі" та "надійні" методи виявлення спрацювань

Одним із способів задовольнити потреби клієнтів є використання комбінації так званих "крихких" і "надійних" методів виявлення інцидентів безпеки.

Крихкі засоби призначені для виявлення певного артефакту, наприклад простого рядка або геш-підпису, який зазвичай асоціюється з відомим шкідливим програмним забезпеченням. Надійні

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2024. №2 (28) ISSN 2524-2296 (online)

методи спрямовані на виявлення поведінки й можуть підтримуватися моделями машинного навчання, навченими для певного середовища. Обидва типи виявлення мають місце в сучасних системах сканування, оскільки вони допомагають збалансувати хибні спрацювання (*False Positive*) та хибні негативні спрацювання (*False Negative*).

Наприклад, виявлення, побудоване на основі гешу шкідливого файлу, дуже ефективно визначає певну версію цього файлу, але будь-яка незначна зміна файлу змінить його геш, що призведе до збою в роботі правила виявлення. Ось чому такі правила називають "крихкими" – вони дуже специфічні, часто спрямовані на один артефакт. Це означає, що ймовірність хибнопозитивного спрацювання майже відсутня, тоді як ймовірність хибнонегативного спрацювання дуже висока.

Незважаючи на недоліки, ці системи виявлення пропонують явні переваги для команд кібербезпеки. Їх легко розробляти та підтримувати, тому інженери можуть швидко змінювати їх відповідно до потреб організації. Вони також можуть ефективно виявляти деякі поширені атаки. Наприклад, єдине правило для виявлення немодифікованої версії інструменту експлуатації *Mimikatz* має величезну користь, оскільки його рівень помилкових спрацювань майже нульовий, а ймовірність зловмисного використання інструменту висока.

Попри це інженер з виявлення має ретельно продумати, які дані застосовувати для створення правил для "крихких" спрацювань. Якщо зловмисник може простими способами змінити індикатор, уникнути виявлення стає набагато легше. Наприклад, якщо програма перевіряє наявність файлу *mimikatz.exe*, зловмисник може просто змінити ім’я файлу на *mimicats.exe* та обійти логіку правила. З цієї причини найкращі правила "крихких" виявлень спрямовані на атрибути, які або незмінні, або їх важко модифікувати.

З іншого боку, надійний набір правил, підкріплений моделлю машинного навчання, може позначити змінений файл як підозрілий, оскільки він є унікальним для середовища або містить певний атрибут, якому алгоритм класифікації надає велике значення. Більшість надійних засобів виявлення – це просто правила, які ширше намагаються бути спрямованими на метод. Ці типи виявлень обмінюють свою особливість на здатність виявляти атаку в більш загальному вигляді, зменшуючи ймовірність хибнонегативних результатів унаслідок збільшення ймовірності хибнопозитивних.

Хоча індустрія схильна надавати перевагу "надійним" методам виявлення, вони мають недоліки. Якщо порівняти з "крихкими" сигнатурами, "надійні" правила набагато важче розробити через їх складність. Крім того, інженер з виявлення має брати до уваги терпимість організації до хибнопозитивних спрацювань і задатися питанням: яку кількість хибнопозитивних спрацювань може обробити внутрішній SOC-центр, аби не знизити свою продуктивність і не заробити так звану *alert fatigue*, тобто нездатність аналітика, що постійно витрачає час на закриття неінформативних спрацювань, відреагувати на справді важливу аномалію в системі. Через це більшість EDR застосовують гібридний підхід, упроваджуючи "крихкі" методи для виявлення очевидних загроз і "надійні" – для виявлення тактик і технік зловмисників у більш загальному плані.

Одним із небагатьох постачальників EDR, який публічно розкриває свої правила виявлення, є *Elastic Stack*. Правила SIEM публікуються в репозиторії *GitHub*, і ці правила містять чудові приклади як крихких, так і надійних виявлень.

Наприклад, розглянемо правило *Elastic* для виявлення спроб *Kerberoasting*, які використовують *Bifrost*, інструмент *macOS* для взаємодії з *Kerberos*. *Kerberoasting* – це метод отримання квитків *Kerberos* і злому їх для розкриття даних службових облікових записів.

Це правило перевіряє наявність певних аргументів командного рядка, які підтримує *Bifrost*. Зловмисник може банально обійти це виявлення, перейменувавши аргументи у вихідному коді (наприклад, змінивши *-action* на *-dothis*), а потім перекомпілювавши інструмент. Крім того, хибне спрацювання може статися, якщо не пов’язаний з ним інструмент підтримує аргументи, перелічені в правилі.

Із зазначених причин правило може здатися поганим детектором. Але варто пам’ятати, що не всі зловмисники діють на одному рівні й чимало груп загроз продовжують використовувати готові інструменти, доступні в популярних фреймворках, як *Metasploit*. Це правило слугує для виявлення тих, хто застосовує базову версію *Bifrost* і не більше.

Через вузьку спрямованість правила *Elastic* має доповнити його більш надійним виявленням, яке закриває очевидні прогалини. Розв’язанням проблеми

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 2 (28)

в цьому разі стає додаткове правило, створене розробником, яке закриває сліпі місця першого.

Це правило спрямоване на нетипові процеси, що створюють вихідні з'єднання з TCP-портом 88, стандартним портом *Kerberos*. Хоча це правило містить деякі прогалини для усунення помилкових спрацювань, загалом воно більш надійне, ніж крихке правило запуску *Bifrost*.

Більшість агентів EDR прагнуть до балансу між крихким і надійним виявленням, але роблять це непрозоро, тому організаціям може бути дуже складно забезпечити покриття, особливо з рішеннями, що не підтримують створення окремих налаштованих користувацьких правил. Із цієї причини інженери команди безпеки мають тестувати та перевіряти виявлення за допомогою таких інструментів, як *Atomic Test Harnesses* від *Red Canary*.

Типи агентів EDR

Як зловмисники, так і інженери команди безпеки мають приділяти пильну увагу типу агенту EDR, розгорнутому на кінцевих точках. Розглянемо типи (або ж побудови) агентів.

1. Базовий

Агенти містять окремі частини, кожна з яких має свою мету й тип телеметрії, яку вона може збирати. Найчастіше агенти мають такі компоненти:

– статичний сканер: застосунок або компонент самого агента, що виконує статичний аналіз зображень, таких як *Portable Executable* (PE) файли або довільні діапазони віртуальної пам'яті, щоб визначити, чи є їх вміст шкідливим. Статичні сканери зазвичай становлять основу антивірусних сервісів;

– DLL-функція перехоплення: DLL, що відповідає за перехоплення викликів певних функцій інтерфейсу прикладного програмування (API);

– драйвер ядра: драйвер режиму ядра, що відповідає за впровадження перехоплюючої DLL у цільові процеси та збір специфічної для ядра телеметрії;

– служба агента: ПЗ, відповідальне за агрегування телеметрії, створеної двома попередніми компонентами. Воно корелює дані або генерує сповіщення, щоб потім передати зібрану інформацію на централізований сервер EDR.

На рис. 2 зображено найпростішу архітектуру агентів, яку нині застосовують комерційні продукти.

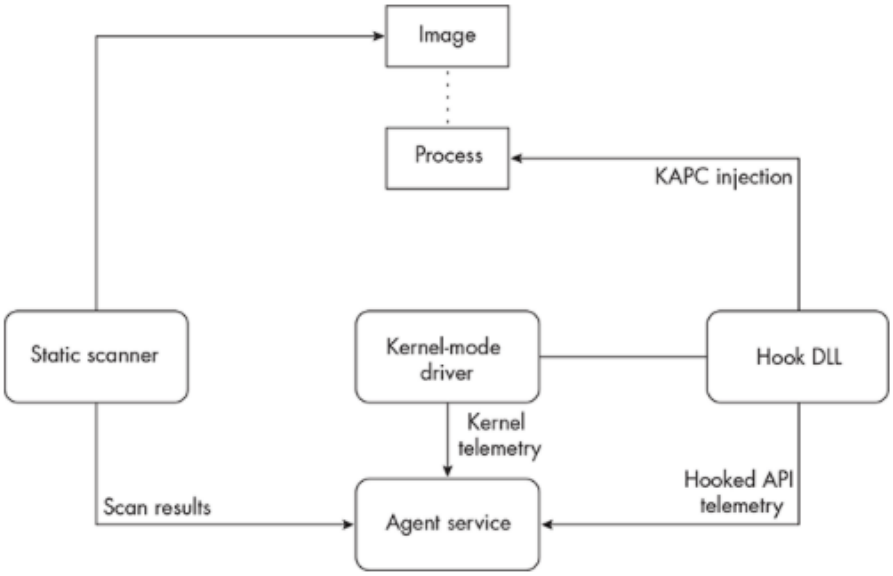

Рис. 2. Базова архітектура агента

Як бачимо, ця базова побудова має небагато джерел телеметрії. Три давачі (сканер, драйвер і DLL-функція перехоплення функцій) надають агенту дані про події створення процесів, виклики функцій, які вважаються чутливими до атак (наприклад, k*ernel32! CreateRemoteThread*), сигнатури файлів і часто віртуальну пам'ять процесу. Така схема може забезпечити достатнє покриття для деяких випадків використання, але більшість комерційних продуктів EDR нині виходять далеко за межі цих можливостей. Наприклад, цей базовий EDR не зможе виявити файли, що створюються, вилучаються або шифруються на хості.

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №2 (28)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

2. *Проміжний*

Хоча базовий агент може збирати значну кількість цінної інформації, на основі якої можна створювати виявлення, ці дані можуть не давати повної картини дій, що виконуються на комп'ютері [15]. Програмні продукти для захисту кінцевих точок, що нині розгортаються в корпоративних середовищах, вже істотно розширили свої можливості для збору додаткової телеметрії.

Більшість агентів EDR наразі належать до середнього рівня складності [16]. Ці агенти не лише впроваджують нові давачі, але й використовують джерела телеметрії, властиві операційній системі. Доповнення на цьому рівні можуть містити:

– драйвери мережних фільтрів: виконують аналіз мережного трафіку для виявлення ознак зловмисної активності;

– драйвери фільтрів файлової системи: спеціальний тип драйверів, що можуть відстежувати операції у файловій системі комп'ютера;

– споживачі ETW: компоненти агента, які можуть слідкувати за подіями, створеними операційною системою хоста або сторонніми програмами;

– компоненти раннього запуску антивірусного програмного забезпечення (ELAM): функції, що надають підтримуваний *Microsoft* механізм завантаження драйвера антивірусного програмного забезпечення перед іншими службами запуску завантаження, щоб контролювати ініціалізацію інших драйверів завантаження. Ці компоненти також дають змогу отримувати *Secure ETW* події, спеціальний тип подій, що генеруються групою захищених постачальників подій.

Хоча сучасні EDR можуть не реалізовувати всі перелічені компоненти, зазвичай використовується драйвер ELAM, розгорнутий разом з основним драйвером ядра.

На рис. 3 показано, як може виглядати більш сучасна архітектура агента.

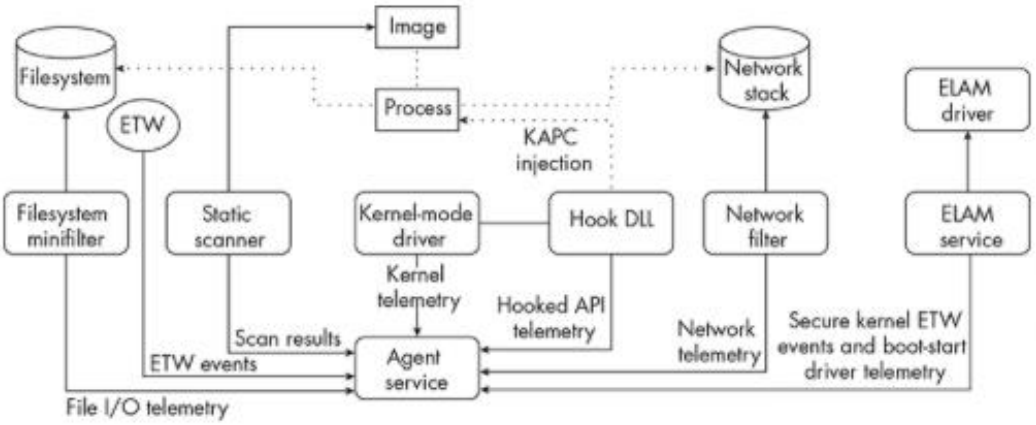

Рис. 3. Архітектура проміжного агента

Ця побудова основана на базовій архітектурі та додає багато нових давачів, з яких можна збирати телеметричні показники. Наприклад, EDR з проміжною архітектурою може відстежувати події файлової системи, зокрема створення файлів, отримувати інформацію від провайдерів ETW, що надають дані, які агент інакше не зміг би зібрати, і спостерігати за мережним зв'язком на хості крізь драйвер фільтра, що потенційно дає змогу агенту виявляти активність маячків командного рядка й команд, що запускаються через неї. Це також додає рівень відмовостійкості, щоб у разі виходу з ладу одного давача інший міг замінити його.

3. *Розширений*

Деякі рішення EDR реалізують більш просунуті функції для моніторингу ділянок системи, які їх цікавлять. Ось два приклади таких функцій:

– гіпервізори: забезпечують перехоплення системних викликів, віртуалізацію певних компонентів системи та ізольоване виконання коду. Вони також дають агенту змогу відстежувати переходи у виконанні між гостьовою машиною та хостом. Зазвичай вони використовуються як компонент захисту від програм-вимагачів та експлойтів;

– обман зловмисника: надає неправдиві дані замість того, щоб запобігти виконанню шкідливого коду. Це може призвести до того, що зловмисник зосередиться на налагодженні свого інструментарію,

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 2 (28)

не усвідомлюючи, що інформація, яку він отримав від системи, була підроблена.

Це досить специфічні для конкретного продукту доповнення і наразі вони не є загальновживаними. Крім того, багато компонентів цієї категорії більше пов'язані зі стратегіями запобігання, ніж із виявленням. Однак з часом деякі розширені функції можуть стати більш поширеними, а нові, ймовірно, будуть винайдені.

Недоліки сучасних EDR

Говорячи про слабкі місця сучасних EDR, не можна обійти теми їх довіри репутації файлу та наскільки структура файлу впливає на процес. Якщо ми розуміємо логіку роботи сенсорів EDR, то легко зможемо проаналізувати, наскільки репутація файлу, сформована іншими вендорами на сервісах як *VirusTotal*, впливає на кінцевий результат аналізу конкретного постачальника ПЗ. І навпаки, якщо файл ще ніде не був проаналізований і його геш не відомий, це означає що він не має поганої репутації, то яка вірогідність його блокування навіть просунутими рішеннями EDR. Нині навіть розрекламовані EDR, такі як *SentinelOne, Trellix, ESET* тощо, що продаються за тисячі доларів, підлягають обходу, якщо зловмисник добре знається на логіці їх сенсорів.

Чимало сучасних рішень EDR не можуть належним чином аналізувати бінарні файли, розроблені за допомогою нового покоління розробки, або, якщо перефразувати, – нетипових мов програмування. Оскільки антивірусні модулі EDR зазвичай розробляються для статичного аналізу зловмисного програмного забезпечення, написаного мовами C, C++ і C#, вони, коли стикаються з файлом зі структурою та виразами, що не є типовими, не можуть застосувати для нього звичні методи аналізу та пропускають далі, що б цей файл не робив далі. У кращому випадку будуть заблоковані дочірні процеси, такі як запуск командного рядка, в гіршому – вони будуть зчитані як нормальна поведінка, оскільки EDR не виявив достатньо індикаторів, що вказували б на хід атаки.

Друга річ, на яку необхідно звернути увагу, це те, наскільки нормально виглядає програма та дії, які вона виконує, для конкретного середовища [17]. Нормалізація, частково пов'язана з репутацією файлів, посідає дуже важливе місце серед методів обходу EDR. Для прикладу візьмемо кейс із простою програмою виведення *MsgBox* за допомогою скриптингової мови *AutoIt*, що часто використовується в сценаріях скриптингу, і спробу перевірити її за допомогою *VirusTotal*, як зробили дослідники сервісу *Secunnix* – отримано результат, що в багатьох рішеннях EDR показники виявлення різняться залежно від того, 32-розрядний чи 64-розрядний файл, а також, чи має файл піктограму, чи ні. Програмне забезпечення, що має значок і скомпільоване як 64-розрядне, рідше спостерігалося *VirusTotal* як зловмисне, а 32-розрядне програмне забезпечення, скомпільоване без піктограм, вважалося більш ризикованим і отримало більше спрацювань.

Тож, найпростіші речі, які можна зробити, щоб зменшити рівень виявлення ПЗ антивірусом, це:

– компіляція зловмисного ПЗ до x64;

– підготовка піктограми;

– якщо можливо, створення ПЗ, що буде застосунком GUI замість CLI;

– уникнення високої ентропії;

– використання дуже популярних, відомих вебсайтів, як C2 для крадіжки даних.

Кожен з перелічених пунктів необхідно брати до уваги під час експлуатації EDR, аби не припустити обходу рішення зловмисником [18].

Метод підвищення ефективності роботи EDR та посилення безпеки ІКС

Тепер, знаючи про особливості побудови агентів EDR та про слабкі місця типового EDR-рішення, можемо сформувати метод використання EDR. Це дасть змогу підвищити ефективності застосування цього рішення.

Для найкращих показників працеспроможності EDR важливо підготуватись до його розгортання в корпоративному середовищі заздалегідь. Перед закупівлею та початком розгортання важливо виконати певні дії.

1. Оптимізувати ресурси локальної мережі та сегментувати мережу, якщо це не було виконано раніше.

2. Ввести стандарт іменування хостів у мережі.

3. Оцінити масштаби й навички фахівців наявного SOC-центру.

4. Провести інвентаризацію всіх активів і програмного забезпечення.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2024. №2 (28) ISSN 2524-2296 (online)

5. Дослідити доцільність обраного рішення та його інтеграцію з уже присутніми інструментами.

6. Протестувати рішення в межах тест-драйву.

Безпосередньо метод, що дасть змогу покращити ефективність використання EDR-систем, передбачає послідовність дій, наведених нижче. У певних аспектах він перегукується із заходами, що мають відбутися до початку впровадження запропонованого методу.

1. ***Сегментація мережі*** дасть змогу розмежувати критично важливі відділи компанії від відділів, що підпадають під ризик зараження шкідливим ПЗ (всі відділи, що спілкуються із зовнішнім світом: технічна підтримка, рекрутери, маркетологи тощо). Також критично важливо створити окрему мережу для будь-яких пристроїв, що не є корпоративними, – смартфонів, особистих ПК тощо.

2. ***Оптимізація ресурсів локальної мережі*** дасть змогу їй працювати без затримок і значно покращить працездатність EDR, тому що, як говорили раніше, хмарна частина рішення є не менш важливою за частину агента на хості. Оскільки EDR має відповідати на запити в реальному часі, будь-яка затримка може бути критичною – від часу передачі телеметрії, повернення результату аналізу від хмарного середовища до часу блокування процесу та ізоляції кінцевої точки. Також якщо агент EDR стикнувся зі збоєм, необхідно, щоб інформація про несправність агента була якомога швидше надана аналітикам у вебконсолі.

3. ***Деактивація інших антивірусних рішень.*** Під час встановлення агента EDR на хости необхідно переконатися, що на них деактивовані всі інші антивірусні рішення, наприклад *Windows Defender*. Через особливості роботи сенсорів агента EDR вони будуть сприйняті як зловмисні іншим антивірусним ПЗ. Також таке сусідство може викликати колізію та призвести до несправності ПК.

4. ***Розроблення політик EDR.*** Розробленню політик EDR (виявлення та реагування окремо) приділяється особлива увага на початку розгортання рішення.

Зазвичай створюються три політики:

– легка – створена для високочутливих хостів, на яких небажано блокувати процеси;

– середня – створена за найкращими практиками, що пропонує постачальник ПЗ; зазвичай всі характеристики усереднені та видають найкращий баланс ефективності та продуктивності агентів;

– строга – політика, яку часто іменують "режимом атаки на компанію"; вона вмикається, коли компрометація хостів підтверджена та аналітики хочуть бачити всі аномалії, що можуть доповнити картину руху зловмисника по середовищу. Ця політика також ефективна під час тестування самого рішення та його чутливості до спроб його обходу.

Крім того, компанії часто утворюють окремі політики для різних відділів, щоб наголосити на особливості налаштувань безпеки для критичних відділів і структур. Можна створити полегшену політику, виняток, білий список, якщо EDR "заважає" працювати, але не уникати встановлення агента на пристрій.

5. ***Створення білого та чорного списків ПЗ*** необхідно для того, щоб під час такої глобальної дії, як розгортання рішення для захисту кінцевих точок, не заважати нормальним процесам бізнесу. ПЗ, дозволене для використання в компанії, має бути додано у виняток, якщо створює хибнопозитивні спрацювання. Варто зауважити, що білий список має застосовуватися з підвищеною обережністю. Використання чорного списку не обмежене. Білий та чорний списки основані на класичних сигнатурах, таких як геш, IP-адреса, домен. Винятки зі свого боку відрізняються від них тим, що прив'язуються до конкретного шляху або поведінки файлу, що робить їх більш застосовуваними й не такими критичними для загальної видимості агента. Також деякі вендори пропонують обмежити видимість певних файлів для агента на хості, але такі винятки вважаються занадто ризикованими й можуть використовуватися лише в окремих випадках, затверджених керівництвом компанії.

6. ***Застосування останніх версій програмного забезпечення*** агентів EDR. Упровадження практики оновлення програмного забезпечення є класичним підходом для будь-якого ПЗ. На жаль, часто ця практика не застосовується в багатьох системах захисту. Опція автоматичного оновлення має бути додана для всіх складників EDR.

7. ***Розроблення плейбуків з реагування на інциденти.*** Плейбуки з реагування на інциденти мають бути розроблені в межах керівництва SOC-центру й підлягають щорічному переоцінюванню їх ефективності, а також впроваджуються з огляду на нові можливості, що надає EDR, і нових методів реагування. Плейбуки мають брати до уваги особливість конкретного обраного EDR-рішення та час реагування на інцидент безпеки, а також

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 2 (28)

можливості активного блокування зловмисних дій з вебконсолі EDR.

8. ***Інвентаризація встановлених агентів і встановлення додаткових інструментів*** проводиться після завершення розгортання рішення та виконується для того, щоб отримати статистику з покриття рішенням усіх кінцевих точок компанії, та оцінити поточний рівень видимості та безпеки корпоративного середовища, і підвищити цей рівень за допомогою додаткових інструментів.

9. ***Постійне тестування та оновлення правил і конфігурацій EDR***. Виконання цього правила дасть змогу пришвидшити впровадження додаткових механізмів виявлення та реагування на найновіші методи, засоби та механізми, що використовуються зловмисниками для атак на ІКС.

Під час роботи з EDR у межах корпоративної інфраструктури важливо зважати на описані вище методи обходу EDR та особливості їх архітектури.

Розглянемо, як метод підвищення ефективності роботи EDR дає змогу попередити різні варіанти обходу EDR зловмисниками.

Обхід конфігурації можна попередити, якщо інженери SOC-центру коректно налаштують політики відповідно до потреб компанії та кращих практик індустрії. На цьому етапі важливо дати бізнесу розуміння, що безпека інформації – це завжди битва між зручністю та швидкістю й безпекою. Варто переоцінювати політики щоразу, коли постачальник ПЗ випускає відповідні оновлення, і тестувати нові опції для підтвердження їх ефективності. Також варто тримати рівень підозрілості агента до процесів на середньому або високому рівні для виявлення, і низькому або середньому – для блокування.

Обхід сприйняття можна попередити використанням додаткових інструментів, окрім EDR, наприклад зовнішніх сканерів вразливостей, IDS/IPS-систем, застосуванням SIEM тощо. Якщо один інструмент не відстежує певні процеси (виявити їх можна під час первинного тестування й далі під час експлуатації рішення), то варто переконатися, що ці процеси відстежуються іншим інструментом, який може генерувати спрацювання для SOC-команди.

Обхід логіки EDR можна попередити регулярним тестуванням правил EDR і кастомних правил за допомогою взаємодії з командою пентестерів в організації. Також обов'язковою практикою є оновлення сенсорів для автоматичного закриття відомих прогалин. Хорошою практикою є моніторинг даркнету для пошуку відомих методів обходу конкретного рішення та створення правил, що закриють для потенційного зловмисника шлях експлуатації цих методів.

Обхід класифікації можна попередити, налаштовуючи політики EDR-рішення на достатньому рівні чутливості для того, щоб більше подій ставилися під сумнів. Також у цьому разі доцільним буде участь інших інструментів безпеки, навіть якщо корпоративний EDR не побачить аномалії в трафіку, то IDS-система або DLP відправить повідомлення про перевищення ліміту надсилання інформації для користувача.

Висновки

У статті описано побудову типових рішень EDR та схеми їх агентів різної складності; проаналізовано методи обходу EDR та висунуто пропозиції з підходу до експлуатації рішення з огляду на сучасні архітектурні особливості EDR-рішень та на основі добутої інформації; сформовано відомості про специфіку цих рішень та наведено рекомендації щодо кращих практик, які можуть бути застосовані в командах фахівців із кібербезпеки для оптимізації та покращення роботи з EDR у мережах організацій різного типу, починаючи від державних органів і завершуючи промисловими об'єктами.

Подані рекомендації можуть бути застосовані під час формування процесів у команді з кібербезпеки, для покращення роботи з наявним рішенням EDR, а також у проведенні менеджменту ризиків та оцінюванні профілю інформаційної безпеки організації, зважаючи на особливості наявного інструментарію команди з кібербезпеки. Це дасть змогу ефективно використовувати наявні програмні, апаратні та людські ресурси, а також здійснювати ефективне планування подальшого розвитку системи кібербезпеки підприємств.

Список літератури

1. Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023 URL: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/ (дата звернення 24.05.2024).

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №2 (28)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

2. Журило О., Ляшенко О. Архітектура та системи безпеки IoT на основі туманних обчислень, *Сучасний стан наукових досліджень та технологій в промисловості,* 2024, Вип. (1(27), С. 54–66. DOI: 10.30837/ITSSI.2024.27.054
3. Когут Ю. Кібервійна та безпека об’єктів критичної інфраструктури. Сідкон, 2021. 336 с.
4. Matt Hand. Evading EDR: The Definitive Guide to Defeating Endpoint Detection Systems. No Starch Press. 2023. 312 p.
5. Мерзлікін Є., Бабешко Є. Аналіз кібербезпеки веборієнтованих індустріальних IOT-систем. *Сучасний стан наукових досліджень та технологій в промисловості.* 2023. Вип. 2(24). С. 131–144. DOI: 10.30837/ITSSI.2023.24.131
6. Forrester Wave October 2023, URL: https://www.forrester.com/ (дата звернення 24.05.2024).
7. Баклан Я. А., Сєвєрінов О. В. Аналіз систем захисту кінцевих точок від складних загроз EDR (Endpoint Detection and Response). Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: матеріали дванадцятої міжнар. наук.-практ. конф. 2022. Баку–Харків–Жиліна. 141 р. URL: https://openarchive.nure.ua/handle/document/24142
8. ISO/IEC 27035:2011 Information technology. Security techniques. Information security incident management, 2011.
9. Crowdstrike October 2023, URL: https://www.crowdstrike.com/ (дата звернення 24.05.2024).
10. Arfeen A., Ahmed S., Khan M. A., Jafri, S. F. A. Endpoint Detection and Response: A Malware Identification Solution. *International Conference on Cyber Warfare and Security (ICCWS).* 2021. DOI: 10.1109/ICCWS53234.2021.9703010
11. Сєвєрінов О. В., Хрєнов А. Г., Поляков А. О. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі. *Системи обробки інформації.* 2015. Вип. 9. С. 101–104. URL: http://nbuv.gov.ua/UJRN/soi_2015_9_24
12. Exploring the History of Antivirus: Fusion Computing. URL: https://fusioncomputing.ca/history-of-antivirus/ (дата звернення 21.03.2024).
13. Сєвєрінов О. В., Шевцов В. О., Сокол-Кутиловська А. С. Аналіз сучасних методів атак на електронні ресурси органів управління. *Системи озброєння і військова техніка*. 2017. Вип. 1. С. 65–67. URL: http://nbuv.gov.ua/UJRN/soivt_2017_1_13 (дата звернення 21.03.2024).
14. Ушатов В., Сєвєрінов О. В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки *Global Cyber Security Forum: матеріали Першого міжнародного науково-практичного форуму*, 2019 С. 104–105. URL: https://openarchive.nure.ua/bitstreams/c2575d95-c877-47e6-aef8-2c19e286d900/download (дата звернення 21.03.2024).
15. FZE B. B. History of antivirus software. UKEssays. 2023. URL: https://us.ukessays.com/essays/information-technology/history-of-antivirus-software.php
16. Zhuravchak D., Dudykevych, V., Tolkachova, A. Дослідження структури системи виявлення та протидії атакам вірусів-вимагачів на базі endpoint detection and response. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2023.* Вип. 3(19), С 69–82. DOI: https://doi.org/10.28925/2663-4023.2023.19.6982
17. Зубок В. Ю., Гончар С. Ф., Єрмошин В. В., Карасюк Г. О. Архітектурно-функціональне порівняння відомих платформ та систем кіберзахисту промислових об’єктів. *Електронне моделювання*, 2022, Вип. 44. Том 3. 65 с. DOI: 10.15407/emodel.44.03.065
18. Коробейнікова Т., Федорченко В. Системний моніторинг мережевої безпеки в тріаді SIEM-EDR-NDR. *Grail of Science*. 2023 Вип. 27. С. 354–360. DOI: https://doi.org/10.36074/grail-of-science.12.05.2023.055

References

1. "Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023", available at https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/ (last accessed 24.05.2024).
2. Zhurilo, O. and Lyashenko, O. (2024), "Architecture and security systems of IoT based on fog computing", ["Arkhitektura ta systemy bezpeky IoT na osnovi tumannykh obchyslen"], *Modern State of Scientific Research and Technologies in Industry*, No 1(27), P. 54–66. DOI: 10.30837/ITSSI.2024.27.054
3. Kogut, Y. (2021), *Cyber warfare and security of critical infrastructure objects, [Kiberviina ta bezpeka obiektiv krytychnoi infrastruktury]*, Sidkon, 336 p.
4. Hand, M. (2023), *Evading EDR: The Definitive Guide to Defeating Endpoint Detection Systems*, No Starch Press, 312 p.
5. Merzlikin, Y., Babeshko, Y. (2023), "Cybersecurity analysis of web-oriented industrial IoT systems" ["Analiz kiberbezpeky veboriientovanykh industrialnykh iot-system"], *Modern State of Scientific Research and Technologies in Industry*, No. 2(24), P. 131–144. DOI: 10.30837/ITSSI.2023.24.131
6. "Forrester Wave October 2023", available at: https://www.forrester.com/ (last accessed: 24.05.2024).

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2024. No. 2 (28)*

7. Baklan, Y. and Severinov, O. (2022), "Analysis of endpoint protection systems against complex threats EDR (Endpoint Detection and Response)" ["Analiz system zakhystu kintsevykh tochok vid skladnykh zahroz EDR (Endpoint Detection and Response)"], Modern Trends in the Development of Information and Communication Technologies and Management Tools: materials of the twelfth international scientific-practical conference 2022, Baku Kharkiv Zhilina, 141 p., available at: https://openarchive.nure.ua/handle/document/24142
8. "ISO/IEC 27035:2011 Information technology. Security techniques. Information security incident management", 2011.
9. "Crowdstrike October 2023", available at: https://www.crowdstrike.com/ (last accessed: 24.05. 2024)-
10. Arfeen, A., Ahmed, S., Khan, M., Jafri, S. (2021), "Endpoint Detection and Response: A Malware Identification Solution". *International Conference on Cyber Warfare and Security (ICCWS).* DOI: 10.1109/ICCWS53234.2021.9703010
11. Severinov, O., Khrenov, A. and Polyakov, A. (2015), "Analysis of modern attack methods on automated control systems and information networks", ["Analiz suchasnykh metodiv atak na avtomatyzovani systemy upravlinnia viiskamy ta informatsiini merezhi"], *Information Processing Systems*, No. 9, P. 101–104. available at: http://nbuv.gov.ua/UJRN/soi_2015_9_24
12. "Fusion Computing 'Exploring the History of Antivirus: Fusion Computing", available at: https://fusioncomputing.ca/history-of-antivirus/ (last accessed: 21.03.2024).
13. Severinov, O., Shevtsov, V., Sokol-Kutilovska, A. (2017), "Analysis of modern attack methods on electronic resources of management bodies" ["Analiz suchasnykh metodiv atak na elektronni resursy orhaniv upravlinnia"], *Weapons and Military Equipment Systems*, No 1, P. 65–67. available at: http://nbuv.gov.ua/UJRN/soivt_2017_1_13 (last accessed 21.03.2024).
14. Ushatov, V. and Severinov, O. V. (2019), "Problems of prompt detection and response to information security incidents" ["Problemy operatyvnoho vyiavlennia i reahuvannia na intsydenty informatsiinoi bezpeky"], Global Cyber Security Forum: materials of the First International Scientific and Practical Forum, P. 104–105. available at: https://openarchive.nure.ua/bitstreams/c2575d95-c877-47e6-aef8-2c19e286d900/download (last accessed 21.03.2024).
15. FZE, B. B. "History of antivirus software, UKEssays". 2023, available at: https://us.ukessays.com/essays/information-technology/history-of-antivirus-software.php
16. Zhuravchak, D., Dudykevych, V. and Tolkachova, A. (2023), "Research on the structure of the system for detecting and countering ransomware attacks based on endpoint detection and response", ["Doslidzhennia struktury systemy vyiavlennia ta protydii atakam virusiv-vymahachiv na bazi endpoint detection and response"], *Electronic Professional Scientific Publication "Cybersecurity: Education, Science, Technology"*, No 3(19), P. 69–82. DOI: 10.28925/2663-4023.2023.19.6982
17. Zubok, V., Honchar, S., Yermoshyn, V. and Karasyuk, H. (2022), "Architectural and functional comparison of known platforms and industrial cybersecurity systems", ["Arkhitekturno-funktsionalne porivniannia vidomykh platform ta system kiberzakhystu promyslovykh obiektiv"], *Electronic Modeling*, No 44, Vol. 3, 65 p. DOI: 10.15407/emodel.44.03.065
18. Korobeinikova, T., Fedorchenko, V. (2023), "System network security monitoring in the triad SIEM-EDR-NDR", ["Systemnyi monitorynh merezhevoi bezpeky v triadi SIEM-EDR-NDR"], *Grail of Science*, No. 27, P. 354–360. DOI: 10.36074/grail-of-science.12.05.2023.055

Надійшла 05.06.2024

Відомості про авторів / About the Authors

Шуліка Катерина Максимівна – Харківський національний університет радіоелектроніки, магістр кафедри безпеки інформаційних технологій, Харків, Україна; e-mail: kateryna.shulika@nure.ua; ORCID ID: https://orcid.org/0000–0003–2560–7426

Балагура Дмитро Сергійович – кандидат технічних наук, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Харків, Україна; e-mail: dmytro.balahura@nure.ua; ORCID ID: https://orcid.org/0009-0006-9839-3317

Смірнов Антон Олександрович – кандидат технічних наук, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Харків, Україна; e-mail: anton.smirnov@nure.ua; ORCID ID: https://orcid.org/0000-0003-4121-3902

Непокритов Дмитро Миколайович – Харківський національний університет Повітряних Сил імені Івана Кожедуба, доцент кафедри радіоелектронних систем пунктів управління Повітряних Сил, Харків, Україна; e-mail: ndn_ndn@ukr.net; ORCID ID: https://orcid.org/ 0000-0003-1752-8496

Литвин Андрій Володимирович – Харківський національний університет Повітряних Сил імені Івана Кожедуба, старший викладач кафедри радіоелектронних систем пунктів управління Повітряних Сил, Харків, Україна; e-mail: ravshan73@ukr.net; ORCID ID: https://orcid.org/0000-0003-1962-6356

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2024. №2 (28) *ISSN 2524-2296 (online)*

Shulika Kateryna – Kharkiv National University of Radio Electronics, M.Sc. at the Department of Information Technology Security, Kharkiv, Ukraine.

Balagura Dmytro – PhD (Engineering Sciences), Kharkiv National University of Radio Electronics, Associate Professor at the Department of Information Technology Security, Kharkiv, Ukraine.

Smirnov Anton – PhD (Engineering Sciences), Kharkiv National University of Radio Electronics, Associate Professor at the Department of Information Technology Security, Kharkiv, Ukraine.

Nepokrytov Dmytro – Ivan Kozhedub Kharkiv National Air Force University, Associate Professor at the Department of Radioelectronic Systems of Control Points of Air Forces, Kharkiv, Ukraine.

Lytvyn Andrii – Ivan Kozhedub Kharkiv National Air Force University, Senior Instructor at the Department of Radioelectronic Systems of Control Points of Air Forces, Kharkiv, Ukraine.

A METHOD OF USING MODERN ENDPOINT DETECTION AND RESPONSE (EDR) SYSTEMS TO PROTECT AGAINST COMPLEX ATTACKS

The **subject** of the research in this article is the architecture of Endpoint Detection and Response and the EDR agent as their base parts in terms of mechanisms for detecting and countering complex attacks on information and communication systems (ICS). The **aim** of the work is to develop of method for improving the efficiency of using Endpoint Detection and Response (EDR) to reduce the risks of compromising ICS information, industrial, and infrastructure objects by effectively redistributing and utilizing the available EDR mechanisms, the cybersecurity team, and other resources available for implementing security measures in an enterprise, institution, or organization. The article addresses the following **tasks**: reviewing and analyzing existing EDR systems, analyzing the architecture of EDR solutions and EDR agents, the features of their use, the logic behind the construction of methods and mechanisms for detecting threats to the system from malicious actors and malicious code. The task of providing recommendations for the organization of ICS is also separately addressed in terms of the need to protect the entire ICS and its individual elements, as well as in terms of the available resources (the cybersecurity team, their qualifications and level of awareness of the architecture of EDR solutions) and means (available EDR system elements) for organizing protection. The following **methods** are used: modeling attack mechanisms, modeling attacker behavior. The following **results** were obtained: general and specific recommendations were formulated for optimizing the operation of EDR systems and ensuring the effective use of EDR system elements in the information and communication networks of enterprises, organizations, and institutions of various types and orientations depending on the available resources and the information requiring protection. **Conclusions**: The identified recommendations for the application of EDR mechanisms for protecting information systems and networks allow optimizing the costs of creating a protection infrastructure and implementing security measures, taking into account the characteristics of the available tools and the training and awareness of the cybersecurity team both in terms of response time to threats and the complexity and cost of performing protection tasks.

Keywords: information and communication systems (ICS); EDR system; Security Opertion Center; EDR agent; threat intelligence; EDR policy; detection of vulnerabilities.

Бібліографічні описи / Bibliographic descriptions

Шуліка К. М., Балагура Д. С., Смірнов А. О., Непокритов Д. М., Литвин А. В. Метод використання сучасних систем захисту кінцевих точок (EDR) для убезпечення від комплексних атак. *Сучасний стан наукових досліджень та технологій в промисловості*. 2024. № 2 (28). С. 182–195. DOI: https://doi.org/10.30837/2522-9818.2024.2.182

Shulika, K., Balagura, D., Smirnov, A., Nepokrytov, D., Lytvyn, A. (2024), "A method of using modern endpoint detection and response (EDR) systems to protect against complex attacks", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (28), P. 182–195. DOI: https://doi.org/10.30837/2522-9818.2024.2.182