КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3(19), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.19.6982
УДК 004.056

Журавчак Даниїл Юрійович
аспірант, асистент кафедри “Захисту Інформації”
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0000-0003-4989-0203
danyil.y.zhuravchak@lpnu.ua

Дудикевич Валерій Богданович
доктор технічних наук, професор кафедри “Захисту Інформації”
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0000-0001-8827-9920
valerii.b.dudykevych@lpnu.ua

Толкачова Анастасія Юріївна
Студент спеціальності “Кібербезпека”
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0000-0002-8196-7963
anastasiia.tolkachova.mkbst.2022@lpnu.ua

ДОСЛІДЖЕННЯ СТРУКТУРИ СИСТЕМИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ АТАКАМ ВІРУСІВ-ВИМАГАЧІВ НА БАЗІ ENDPOINT DETECTION AND RESPONSE

Анотація. У досліджені розглядаються проблеми та обмеження сучасних систем виявлення та запобігання атакам з вимогами до цих систем, а також потенційний розвиток у цій сфері в майбутньому. Однією з ключових проблем є постійно еволюціонуючий характер атак з використанням програм-вимагачів, що вимагає регулярного оновлення та адаптації систем для забезпечення їхньої ефективності. Іншим викликом є необхідність того, щоб системи могли розрізняти легітимне та шкідливе програмне забезпечення, а також різні типи програм-вимагачів. Для вирішення цих проблем у статті запропоновано низку функціональних та нефункціональних вимог до систем виявлення та протидії програмам-вимагачам. До них відносяться можливість виявлення та реагування на атаки в режимі реального часу або близькому до нього, можливість аналізу та класифікації різних типів програм-вимагачів, а також можливість інтеграції з іншими системами та інструментами безпеки. Крім того, слід також враховувати нефункціональні вимоги, такі як масштабованість, продуктивність та безпека. У статті також представлено детальний аналіз різних типів систем виявлення та протидії програм-вимагачів, що існують на сьогоднішній день, включаючи системи виявлення вторгнень (IDS), системи виявлення та реагування на кінцевих точках (EDR) та сучасні антивіруси. У ньому також представлено порівняння їх сильних і слабких сторін, а також класифікація існуючих рішень відповідно до їх схожості. У роботі представлено алгоритм оцінки якості продуктів для виявлення та протидії програмам-вимагачам. Алгоритм базується на комплексі функціональних та нефункціональних вимог і покликаний забезпечити комплексну та об'єктивну оцінку можливостей різних систем. Алгоритм підтверджено серією тестів та експериментів, які демонструють його ефективність у визначенні найкращих рішень для виявлення та протидії програмам-вимагачам. В цілому, ця стаття містить цінну інформацію та практичні рекомендації для організацій, які прагнуть вдосконалити свій захист від атак з використанням програм-вимагачів.

Ключові слова: віруси-вимагачі, несанкціонований доступ, методи виявлення

ВСТУП

За останні кілька років кількість атак програм-вимагачів на корпоративні мережі та комп'ютери значно зросла, що створює великі проблеми для підприємств та організацій. Програми-вимагачі є однією з найбільш поширених загроз кібербезпеці, які можуть привести до втрати даних, витоку конфіденційної інформації, порушення роботи системи та навіть шкоди для фінансової діяльності компанії.

Для ефективного захисту від програм-вимагачів необхідно розуміти їхню структуру та розповсюдження, а також мати належні методи виявлення та протидії. Отже, дослідження структури системи виявлення та протидії програмам-вимагачам у контексті безпеки корпоративних мереж та кінцевих станцій є актуальним та важливим завданням.

Метою даної роботи є дослідження структури системи виявлення та протидії програмам-вимагачам, а також розробка та валідація методів їхнього виявлення та протидії у режимі реального часу. В рамках цієї роботи будуть вирішені такі завдання: дослідження методів виявлення та аналізу програм-вимагачів, розробка нових методів виявлення та протидії, аналіз та порівняння ефективності розроблених методів, а також валідація їхньої працездатності на реальних даних.

Отже, результати цієї статті дозволять зробити внесок у покращення методів захисту від програм-вимагачів, зменшення ризиків кібератак та забезпечення безпеки корпоративних мереж та кінцевих станцій.

Крім того, зростання використання облікових записів в мережі Інтернет і популярності онлайн-платіжних систем також робить користувачів більш вразливими перед вірусами-вимагачами. У разі зараження комп'ютера вірусом-вимагачем, кіберзлочинці можуть вимагати від користувача виплатити велику суму грошей, щоб розблокувати доступ до його файлів. Втрата важливих даних, таких як фінансові звіти, інтелектуальна власність, особисті фотографії та інші конфіденційні дані, може призвести до значних фінансових втрат та порушення репутації компанії.

Одним із найважливіших викликів для сучасних систем безпеки є захист корпоративних мереж та кінцевих станцій від вірусів-вимагачів. Ця проблема стає особливо актуальною в контексті зростання кількості пристроїв, що підключаються до корпоративної мережі, збільшення кількості шкідливих програм та вдосконалення методів атак кіберзлочинців.

Отже, розробка ефективних методів виявлення та протидії вірусам-вимагачам у режимі реального часу стає дуже важливою задачею для забезпечення безпеки корпоративних мереж та кінцевих станцій. У даній статті досліджено структуру системи виявлення та протидії програмам-вимагачам з метою розробки нових методів та алгоритмів для забезпечення більш ефективного захисту корпоративних мереж та кінцевих станцій від цих загроз.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Існує багато систем виявлення вірусів-вимагачів, кожна з яких має свої переваги та недоліки. Ці системи можуть працювати окремо або в комбінації між собою, залежно від потреб користувача та особливостей застосування. Нижче наведено кілька прикладів таких систем:

1. Антивірусні програми - це програми, призначені для виявлення та блокування вірусів та інших шкідливих програм. Вони здатні сканувати файли та систему на наявність загроз, а також мають функцію блокування виконання шкідливого коду.
2. Системи перехоплення та аналізу поведінки - це системи, які аналізують дії програм на комп'ютері та виявляють зміни в поведінці, що можуть бути зв'язані з дією вірусів-вимагачів. Наприклад, якщо програма починає шифрувати файли на комп'ютері, система перехоплення поведінки може сприймати цю дію як потенційно шкідливу та зупиняти її.
3. Системи інтелектуального аналізу даних - це системи, які використовують алгоритми машинного навчання та інші методи аналізу даних для виявлення шкідливих програм. Вони здатні розпізнавати нові загрози, які не були відомі раніше, та приймати рішення про їх блокування.
4. Системи контролю доступу - це системи, які контролюють доступ до ресурсів комп'ютера та можуть блокувати доступ до файлів та інших ресурсів, які використовуються вірусами-вимагачами. Наприклад, система контролю доступу може блокувати доступ до зовнішніх жорстких дисків, які використовуються для зберігання зашифрованих файлів.
5. EDR (Endpoint Detection and Response) - це система, яка забезпечує збір інформації з кінцевих точок (комп'ютерів, ноутбуків, мобільних пристроїв тощо), що дозволяє здійснювати аналіз та виявлення аномалій у поведінці кінцевих точок. EDR також забезпечує захист кінцевих точок від вірусів-вимагачів шляхом виявлення та блокування шкідливого програмного забезпечення.

У цьому досліджені не враховані ціни, чи цінові політики комерційних рішень. Хоча ціна на нашу думку і є найважливішим у виборі рішення безпеки, зробити порівняльний аналіз в край важко, тому що практично всі вендори пропонують гнучкі системи оплати, чи суттєві знижки. Подальше порівняння продуктів буде відбуватися виключно по функціональних, та нефункціональних атрибутах продуктів, які можна кількісно, якісно, або емпірично виміряти та порівняти.

Аналіз EDR-рішень проводився для визначення ефективності цих продуктів у виявленні та відповіді на кібератаки в режимі реального часу. В умовах постійно зростаючої кількості кібератак та загроз, EDR-системи стають все більш важливими для забезпечення безпеки комп'ютерних систем. Аналіз EDR-рішень дозволяє визначити найбільш ефективні продукти та рекомендувати їх для використання організаціями. Дослідження також допомагає виявити переваги та недоліки різних EDR-рішень, що дозволяє організаціям зробити свідомий вибір при виборі продукту для забезпечення безпеки.

МЕТОДИКА ДОСЛІДЖЕННЯ

Первинне дослідження проведене, щоб скласти список постачальників, які відповідають нашим критеріям оцінки на теперішньому ринку продуктів EDR (Endpoint Detection and Response). З цього початкового пулу постачальників звужується остаточний список. Постачальники обираються на основі таких критеріїв: 1) відповідність продукту; 2) успіх клієнтів; і 3) клієнтський попит. Постачальники включаються, які мають обмежену кількість рекомендацій від клієнтів та продукти, які не відповідають сфері нашої оцінки. Вивчивши попередні дослідження, оцінки потреб користувачів, а також інтерв'ю з постачальниками та експертами, було розроблено початкові критерії оцінки. Щоб оцінити постачальників та їхні продукти за нашим

набором критеріїв, ми збираємо детальну інформацію про кваліфікацію продуктів за допомогою лабораторних досліджень, демо-версій та/або пошуку публічних відповідей клієнтів, які дали публічні рекомендації. Вагові коефіцієнти встановлюються за замовчуванням, щоб відобразити наш аналіз потреб великих компаній-користувачів - та/або інших сценаріїв, а потім оцінюємо постачальників за чітко визначеною на основі чітко визначеної шкали.

Наступні критерії також можуть бути враховані при виборі продуктів безпеки для захисту від вірусів-вимагачів:

1. Функціональність: продукт повинен мати достатньо функцій для виявлення, блокування та відновлення від вірусів-вимагачів, а також бути сумісним з іншими продуктами безпеки, що використовуються в компанії.
2. Ефективність: продукт повинен бути ефективним у виявленні та блокуванні вірусів-вимагачів, а також повинен мати низький рівень помилкових спрацювань.
3. Надійність: продукт повинен бути надійним та має мати доказану історію успіху в захисті від вірусів-вимагачів.
4. Легкість використання: продукт повинен бути легким у використанні та налаштуванні, щоб забезпечити максимальний захист з мінімальними зусиллями.
5. Підтримка та оновлення: компанія-виробник повинна забезпечувати регулярну підтримку та оновлення продукту, щоб забезпечити захист від нових загроз та вразливостей.
6. Сумісність з компаній: продукт повинен бути сумісним з існуючими системами та програмним забезпеченням компанії, щоб забезпечити належну інтеграцію та управління загрозами.
7. Доступність: продукт повинен бути доступним для компанії за розумною ціною та не повинен надмірно обтяжувати бюджет компанії.

Для аналізу EDR систем пропонується методика, яка базується на використанні таких функцій, як:

1. Моніторинг подій: система повинна моніторити всі події, що відбуваються на кінцевих точках та в корпоративній мережі. Це дозволить виявляти аномальну поведінку та вчасно реагувати на них.
2. Аналіз поведінки: система повинна використовувати машинне навчання та аналізувати поведінку користувачів та процесів на кінцевих точках. Це допоможе виявляти підозрілі активності, що можуть свідчити про наявність вірусів-вимагачів.
3. Виявлення підозрілих файлів: система повинна аналізувати файли на кінцевих точках та в корпоративній мережі, щоб виявляти підозрілі файли та програми, які можуть бути вірусами-вимагачами.
4. Виявлення змін конфігурації: система повинна моніторити зміни конфігурації кінцевих точок та інфраструктури мережі. Це дозволить виявляти підозрілі зміни, які можуть бути наслідком дій вірусів-вимагачів.
5. Виявлення спроб вторгнення: система повинна моніторити спроби вторгнення в корпоративну мережу та кінцеві точки. Це допоможе виявити спроби атак вірусів-вимагачів та вчасно реагувати на них.

Використання цих функцій дозволить ефективно виявляти віруси-вимагачі та запобігати їх поширенню в корпоративній мережі та на кінцевих точках.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Наступна Таблиця 1 ілюструє вибраний конкретний продукт від вендора. Для дослідження було включено в оцінку 12 постачальників: Carbon Black, Cisco Systems, CrowdStrike, Cybereason, Cylance, Digital Guardian, Endgame, ESET, FireEye, RSA, SentinelOne та Symantec.

Таблиця 1

Оцінені постачальники: Інформація про продукти

Вендор	Оцінений продукт
Carbon Black	Cb Response
Cisco Systems	Advanced Malware Protection (AMP) for Endpoints
CrowdStrike	CrowdStrike Falcon
Cybereason	Cybereason Hunt
Cylance	CylanceOPTICS
Digital Guardian	Digital Guardian Data Protection Platform
Endgame	Endgame
ESET	ESET Enterprise Inspector
FireEye	FireEye Endpoint Security
RSA	RSA NetWitness Endpoint
SentinelOne	SentinelOne
Symantec	Symantec Advanced Threat Protection(ATP)

Список критерій, за якими здійснювався відбір вендорів:

1. Впровадження на підприємстві. Постачальник повинен мати значну кількість корпоративних клієнтів, що вимірюється наявністю понад 100 корпоративних клієнтів (1 000+ співробітників).
2. Масштабованість підприємства. Зріла пропозиція EDR вимагає від постачальника подолання певних технічних викликів щодо масштабованості. Пороги, необхідні для включення в цю оцінку, становлять 800 000 загальних розгорнутих кінцевих точок, причому за одне розгортання має бути розгорнуто щонайменше 100 000 кінцевих точок.
3. Видимість кінцевих точок. Визначальною особливістю EDR є збір операцій, пов'язаних з безпекою, або телеметрії на кінцевій точці. Розуміючи, що це дослідження не є еталоном для виявлення, необхідно зібрати мінімальний набір телеметричних даних, щоб гарантувати, що продукти можуть виявляти складні типи складних атак, для боротьби з якими підприємства інвестують в технології EDR.

Оцінка поточної пропозиції

Оцінка поточної пропозиції включає оцінку можливостей кожного з 12 провідних EDR-рішень на даний момент. Для цього використовуються такі критерії:

1. Потужність рішення: оцінюється ефективність рішення виявлення та відповіді на кібератаки.
2. Широкий спектр функцій: відображає, які функції включені в рішення, такі як виявлення загроз, аналіз поведінки, автоматизація відповіді на загрози тощо.

3. Клієнтський досвід: оцінюється, наскільки простим та зручним є користування рішенням для виявлення та реагування на кібератаки.
4. Робота у реальному часі: оцінюється здатність рішення виявляти та відповідати на кібератаки в режимі реального часу.
5. Відкритість та інтеграція: оцінюється здатність рішення працювати в комплексі з іншими засобами забезпечення безпеки та можливість інтеграції з ними.
6. Вартість та прозорість: оцінюється вартість рішення та його прозорість, включаючи вартість підтримки та інших додаткових послуг.
7. Видимість на ринку та стратегія: оцінюється видимість та стратегія розвитку рішення на ринку.

Це допоможе зробити свідомий вибір при виборі продукту для забезпечення безпеки, враховуючи поточні можливості кожного продукту. Крім того, оцінка поточної пропозиції EDR дозволяє розробникам продуктів отримати зворотний зв'язок від клієнтів та зрозуміти, як можна вдосконалити свій продукт для підвищення ефективності та задоволення потреб клієнтів. Вдосконалення продуктів може включати додавання нових функцій, поліпшення інтерфейсу користувача, збільшення швидкості реакції на кібератаки тощо.

Отже, оцінка поточної пропозиції в даному досліджені про EDR є важливим етапом у виборі EDR-рішень для забезпечення безпеки та дозволяє забезпечити максимальну захищеність комп'ютерних систем в умовах постійно зростаючої кількості кібератак. Результати оцінювання наведені у Таблицях 2 та 3.

Після оцінки кожного з цих критеріїв, кожному EDR-рішенню присвоюється бал від 0 до 5, де 5 - найвища оцінка. Загальний бал розраховується шляхом обчислення середнього значення всіх балів за кожним з критеріїв.

Таблиця 2

Картка показників продуктів EDR: Оцінка поточної пропозиції.

Атрибути	Вага	Carbon Black	Cisco Systems	Crowd Strike	Cybereason	Cylance	Digital Guardian
Ефективність агентів кінцевих точок	20%	2.8	4.6	4.4	2.4	2	3
Ефективність виявлення	40%	4	1.8	4.8	4	2	4.2
Ефективність протидії	20%	3.8	2.2	4.6	2.2	3.8	4.2
Легкість використання	20%	2.8	3.8	4.2	3	3.4	3.4
Висновок: Поточна пропозиція	100%	3.48	2.84	4.56	3.12	2.64	3.80

З Таблиці 2 видно, що за атрибутом Ефективність агентів кінцевих точок найбільший показник має Cisco Systems. З несильним розривом після нього CrowdStrike. Найнижчий показник у Cylance. Якщо ж дивитися за атрибутом Ефективність виявлення, то тут найвищий показник у CrowdStrike. Після нього йдуть Carbon Black та Cybereason з однаковим значенням. Найменші у Cylance та Cisco Systems відповідно.

Таблиця 3

Картка показників продуктів EDR: Оцінка поточної пропозиції. (продовження)

Атрибути	Вага	Endgame	ESET	FireEye	RSA	Sentinel One	Symantec
Ефективність агентів кінцевих точок	20%	2.4	2.4	2.4	2	4.6	2.4
Ефективність виявлення	40%	3.4	3.8	3	2.2	2.2	2
Ефективність протидії	20%	1.4	1.8	3.4	4.2	3.4	4.2
Легкість використання	20%	1.8	1.8	3.6	1.8	4.2	3
Висновок: Поточна пропозиція	100%	2.8	2.72	3.08	2.48	3.32	2.72

Оцінка стратегії

Оцінка стратегії в The Forrester Wave про EDR, звіт Q3 2018, включає оцінку планів та стратегій розвитку кожного з 15 провідних EDR-рішень. Це включає такі критерії:

1. Візія: оцінюється, яка є візія компанії щодо розвитку та покращення продукту.
2. Ресурси та інвестиції: оцінюється, які ресурси та інвестиції компанії спрямовані на розвиток продукту.
3. Стратегія розвитку: оцінюється, які кроки планується здійснити компанією для покращення продукту та збільшення свого ринкового впливу.
4. Відкритість та стандарти: оцінюється, наскільки компанія відкрита для співпраці та які стандарти використовуються для покращення продукту.
5. Партнерська екосистема: оцінюється, які партнерські взаємини має компанія, що може допомогти у покращенні продукту та розвитку екосистеми.
6. Виконання стратегії: оцінюється, наскільки успішно компанія виконує свою стратегію розвитку.
7. Вартість та цінова стратегія: оцінюється, які цінові стратегії використовує компанія та яка вартість продукту в порівнянні з іншими продуктами на ринку.

Ці критерії дозволяють оцінити, наскільки ефективно кожна компанія планує розвивати свій продукт EDR та які кроки вона збирається здійснити для збільшення свого ринкового впливу. Оцінка стратегії також допомагає визначити, які компанії мають перспективи для довгострокової співпраці та які продукти

Таблиця 4

Картка показників продуктів EDR: стратегія

Атрибути	Вага	Carbon Black	Cisco Systems	CrowdStrike	Cybereason	Cylance	Digital Guardian
Візія продукту	30%	5	5	5	3	3	3
Заплановані вдосконалення	20%	3	1	3	3	5	5
Ринковий підхід	50%	5	1	5	3	5	3
Висновок: Стратегія	100%	4.6	2.2	4.6	3	4.4	3.4

Таблиця 5

Картка показників продуктів EDR: стратегія (продовження)

Атрибути	Вага	Endgame	ESET	FireEye	RSA	SentinelOne	Symantec
Візія продукту	30%	3	3	3	3	3	3
Заплановані вдосконалення	20%	3	3	3	1	3	3
Ринковий підхід	50%	3	5	1	1	1	1
Висновок: Стратегія	100%	3	4	2	1.6	2	2

Оцінка присутності на ринку

Оцінка присутності на ринку включає оцінку рівня присутності на ринку кожного з 15 провідних EDR-рішень на даний момент. Це включає такі критерії:

1. Рівень популярності: оцінюється, який рівень популярності має продукт в індустрії забезпечення безпеки.
2. Ринковий вплив: оцінюється, який ринковий вплив має продукт на ринку забезпечення безпеки.
3. Кількість клієнтів: оцінюється, скільки клієнтів має продукт на даний момент.
4. Географічна присутність: оцінюється, в яких регіонах світу продукт має значний ринковий вплив.
5. Компанійний ресурс: оцінюється, які ресурси має компанія, що може допомогти у збільшенні її ринкового впливу.
6. Міжнародна присутність: оцінюється, наскільки успішно компанія працює в міжнародних ринках.
7. Партнери: оцінюється, які партнери має компанія, які можуть допомогти їй у збільшенні її ринкового впливу.

Ці критерії дозволяють оцінити, наскільки ефективно кожна компанія працює на ринку забезпечення безпеки та який рівень її ринкового впливу. Оцінка присутності на ринку також допомагає визначити, які компанії мають широку базу клієнтів та наскільки їх продукти популярні серед користувачів. Отже, оцінка присутності на ринку є важливим етапом у виборі EDR-рішень для забезпечення безпеки та допомагає організаціям зробити свідомий вибір продукту, який вже має певну популярність та довіру в індустрії забезпечення безпеки. Оцінка присутності на ринку також допомагає розробникам продуктів оцінити свій ринковий вплив та робити кроки для його збільшення.

Таблиця 6

Картка показників продуктів EDR: ринкова доля

Атрибути	Вага	Carbon Black	Cisco Systems	CrowdStrike	Cybereason	Cylance	Digital Guardian
Кількість клієннтів	50%	5	3	5	2	2	1
Загальна кількість розгорнутих кінцевих точок	50%	3	3	5	1	1	1
Висновок: Стратегія	100%	4	3	5	3	3	1

Таблиця 7

Картка показників продуктів EDR: ринкова доля (продовження)

Атрибути	Вага	Endgame	ESET	FireEye	RSA	SentinelOne	Symantec
Кількість клієнтів	50%	1	1	3	5	3	3
Загальна кількість розгорнутих кінцевих точок	50%	1	1	5	3	1	5
Висновок: Стратегія	100%	1	1	4	4	2	4

Аналіз результатів

CrowdStrike. CrowdStrike є лідером. Він розуміє і формулює проблему боротьби з кіберзагрозами краще, ніж будь-хто інший. Компанія, яка займається розробкою продуктів EDR як основним продуктом, підкріплених аналітикою загроз та цифровими криміналістичними послугами, які користуються широкою повагою в галузі. Вони здійснюють системну класифікацію на основі процесів, що виконуються класифікацію на основі процесів, що виконуються на комп'ютері, для коригування пріоритетності сповіщень, а пошук загроз здійснюється за допомогою мови запитів Splunk (SPL), що може розглядатися як конкурентною перевагою для організацій, які утримують аналітиків з таким набором навичок.

Carbon Black. Цей продукт є надзвичайно ефективним рішенням, яке широко використовується цифровими криміналістами та постачальниками послуг безпеки, щоб забезпечити цілісність для своїх клієнтів. Це дуже складний продукт для пошуку загроз, призначений для досвідчених користувачів, і йому бракує деяких з найбільш поширених можливостей запобігання, які є у його аналогів. Користувачі, які шукають більш доступний продукт, можуть звернути увагу на рішення Cb Defense.

Digital Guardian. Digital Guardian - новачок на цьому ринку, який розробив надзвичайно цікаве рішення EDR на основі технології запобігання втраті даних (DLP). Хоча ефективність DLP з точки зору правозастосування піддавалася численним критичним зауваженням, можливості файлового аналізу вирішують одну з найбільших проблем для команд безпеки у виявленні конфіденційних даних в їхніх середовищах. Digital Guardian вирізняється тим, що використовує цю аналітику файлів, щоб допомогти вам зрозуміти чутливість даних, до яких був наданий доступ в рамках виявлення та оповіщення. Це критична функція виявлення та протидії вірусам-вимагачам.

Сильні виконавці:

Cylance. Cylance, компанія, що не одноразово наробила галасу, застосовуючи свій досвід машинного навчання до наборів поведінкових даних, щоб випереджати технології зловмисників, за допомогою свого рішення CylanceOPTICS. Функціонал полювання на загрози обмежений, коли справа доходить до побудови складних запитів, але клієнти часто називають здатність продукту швидко визначати, де ще існують не виявлені артефакти компрометації у корпоративному середовищі [11].

ESET. ESET пропонує комбіноване рішення EDR/EP на базі одного агента з функціями звітності та пошуку загроз, доступними через єдину панель віддаленого адміністратора, яка забезпечує єдиний доступ до всіх продуктів ESET. Інформація подається в продуманому вигляді за допомогою інтуїтивно зрозумілих елементів керування. Це не найкращий інструмент для цифрової криміналістики, але він чудово підходить для розслідувань у більшості випадків на підприємствах. Так, як історія продуктів ESET починається з просто антивіруса, усі інші продукти є максимально простими у користуванні, але при цьому є обмежені у складних ситуаціях [1].

Cybereason. Cybereason ввів поняття "malop" - сукупності декількох подій, які окремо можуть не бути поганими, але якщо їх розглядати як послідовність подій, то вони вказують на зловмисну операцію. Cybereason надає найкрасивіший користувальницький інтерфейс з графічними можливостями пошуку загроз, які полегшують аналітикам молодшого рівня створення запитів і дослідження оповіщень. Його поведінкове виявлення і здатність автоматично виправляти інциденти високо цінується клієнтами, які також визнають, що Cybereason знаходиться на стадії зростання, оскільки стартап знаходиться в стадії розвитку, а багато корпоративних функцій все ще знаходяться в розробці і будуть імплементованими у майбутньому. [12]

Endgame. Рішення Endgame, орієнтоване на протидію вірусам-вимагачам та загрозам, засноване на баченні підвищення рівня SOC-аналітиків першого рівня та прискорення роботи аналітиків третього рівня за допомогою автоматизації. У ньому є захоплюючий чат-бот на ім'я Artemis, який допомагає в розслідуванні простою англійською мовою і прив'язує сповіщення до структури MITRE ATT&CK, щоб забезпечити кращу видимість життєвого циклу атаки.

Учасники:

SentinelOne. SentinelOne надає можливість виявлення та автоматизованого реагування корпораціям, які хочуть покращити рівень безпеки своїх кінцевих точок без додаткових адміністративних витрат. Хоча компанія прийняла дизайнерські рішення, які вказують на те, що вона хотіла б охопити більш вибагливих клієнтів, можливості продвинутого користування ще не реалізовані, і продукту бракує зручності в усуненні вірусів-вимагачів, що ускладнює прийняття обґрунтованих рішень щодо запровадження даного рішення. цей продукт є гарним вибором для замовників, які прагнуть підвищити стійкість організації, додавши поведінкове виявлення з автоматизованим реагуванням і не є вибагливими у ручному аналізі загроз та вразливостей [3].

FireEye. FireEye пропонує платформу, орієнтовану на аналіз даних з кінцевих точок, який забезпечує захист від шкідливого програмного забезпечення та поведінкового виявлення в інструменті, призначеному для корпоративного пошуку та цифрової криміналістики. Здатність виявляти загрози, які на перший погляд не є простими до виявлення, та інтегруватися з іншими продуктами FireEye, що є суттєвою перевагою.Це рішення є хорошим вибором для організацій, які шукають платформу, що об'єднує кілька продуктів в FireEye Helix, але це рішення саме по собі не являється хорошим для задач EDR.

Cisco Systems. Компанія Cisco розуміє, що важко запобігти усім загрозам, тому створила продукт для кінцевих точок, який запобігає всім можливим загрозам, забезпечуючи при цьому видимість виявлених загроз, але при цьому цей продукт

обмежений у аналізі мережевого трафіку. Наразі можливості пошуку обмежуються пошуком окремих артефактів компрементації, або використанням оповіщення лише окремих аналітиків. Розширені функції, такі як пошук кінцевих точок у реальному часі не є імплементованими зараз, а натомість планується впровадження у майбутньому. Їх інформаційні панелі та можливості візуалізації даних диференціюються, а партнерство з Apple дозволяє Cisco запропонувати рішення для пристроїв iOS, яке є унікальним на ринку для організацій, що віддають перевагу єдиній інформаційній панелі, яка включає мобільні пристрої. [2]

Symantec. Продукт Symantec Advanced Threat Protection (ATP) має спільного агента та інсталятора з Symantec Endpoint Protection (SEP), що створює з однієї сторони перевагу для користувачів Symantec, але не являється додатковою цінністю для користувачів, що не мають продуктів Symantec.З точки зору стратегії, до кінця 2018 року Symantec інтегрує своє хмарне рішення EDR (EDRC), яке дозволить хмарно керувати кінцевими точками ATP, додаючи розширені можливості реагування і криміналістики за допомогою кросплатформеного агента - навіть для пристроїв у корпоративній мережі, які не управляються іншими продуктами Semantec. Клієнтам наявних рішень Symantec , які бажають розширити можливості виявлення загроз вірусів-вимагачів і придбати рішення EDR варто розглянути наступні рішення Рішення ATP від Symantec, але це буде включено як додаткова вартість і оцінюватися, як окремий продукт, що піднімає ціну впровадження рішення захисту від вірусів-вимагачів.

RSA. RSA добре розуміє ринок EDR та специфіку його покупців. Сильною стороною цього рішення є збір даних і доступність цих даних для кінцевого користувача для проведення розслідувань. На жаль, дизайн інтерфейсу користувача є поганим і неінтуїтивно зрозумілим, тому для того, щоб стати досвідченим користувачем, аналітикам з питань безпеки знадобиться навчання, щоб набути компетентності, що є нейпринятним у питанні навчання виявлення вірусів-вимагачі . Окрім того, незважаючи на те, що компанія активно продає і просуває цей продукт на основі інтеграції зі своєю платформою аналітики безпеки, RSA NetWitness Platform, багато конкретних переваг інтеграції є пріоритетними до розробки, але не впровадженні сьогоденні, що не дає можливості оцінити рішення.

Виходячи з результатів даного дослідження, дуже важко підібрати конкретне рішення продукту або продуктів для боротьби з вірусами-вимагачами. Дуже часто висока ціна може бути причиною відмови створення стратегії боротьби з загрозою вірусів-вимагачів у багатьох корпоративних та державних структур. Рекомендується ознайомитися

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Наукова стаття розглядає перспективи використання EDR-рішень для забезпечення безпеки комп'ютерних систем. Відзначається, що EDR-системи забезпечують миттєву відповідь на загрози та дозволяють організаціям швидко реагувати на кібератаки.

У статті проаналізовано 12 провідних EDR-рішень, серед яких Carbon Black, CrowdStrike, Cybereason, Endgame, McAfee та Symantec. Кожен з них має свої переваги та недоліки. Автори статті зазначають, що використання EDR-рішень в комплексі з іншими засобами забезпечення безпеки дозволяє забезпечити максимальну захищеність комп'ютерних систем. Також вони відзначають зростаючу популярність EDR-систем та їхню значущість для забезпечення безпеки в умовах постійно зростаючої кількості кібератак.

Отже, стаття підтверджує важливість використання EDR-рішень у сучасних умовах та рекомендує їх використання у комплексі з іншими засобами забезпечення

безпеки для досягнення максимальної ефективності.

Дослідження виявило, що кожен з перерахованих продуктів має свої переваги та недоліки, і немає універсального рішення, яке б підходило для всіх організацій. Однак, усі EDR-системи забезпечують миттєву відповідь на загрози, що дозволяє організаціям швидко реагувати на кібератаки та мінімізувати їхні наслідки.

Також, дослідження підтверджує зростаючу популярність EDR-систем та їхню значущість для забезпечення безпеки в умовах постійно зростаючої кількості кібератак. Використання EDR-рішень в комплексі з іншими засобами забезпечення безпеки дозволяє забезпечити максимальну захищеність комп'ютерних систем.

Отже, результати дослідження підкреслюють важливість використання EDR-рішень для забезпечення безпеки в сучасних умовах, а також необхідність їхнього використання у комплексі з іншими засобами забезпечення безпеки для досягнення максимальної ефективності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 ESET - офіційний сайт. Антивірусні програми Ісет в Україні. ESET. https://www.eset.com/ua/
2 Now Available: Cisco Security Connector for iOS. Cisco Blogs. https://blogs.cisco.com/security/now-available-cisco-security-connector-for-ios
3 SentinelOne. Autonomous AI Endpoint Security Platform. SentinelOne DE. https://www.sentinelone.com/
4 Majors, C., Miranda, G., Fong-Jones, L. (2022). Observability Engineering: Achieving Production Excellence. O'Reilly Media, Incorporated.
5 A New Paradigm For Cyber Threat Hunting. (2018, 11 червня). The Hacker News. https://thehackernews.com/2018/06/cyber-threat-hunting.html
6 MITRE ATT&CK. https://attack.mitre.org/wiki/Main_Page
7 Mohamad Fadli Zolkipli Jantan, A. (2011). An approach for malware behavior identification and classification. У 2011 3rd International Conference on Computer Research and Development (ICCRD). IEEE. https://doi.org/10.1109/iccrd.2011.5764001
8 Defensive Security Handbook: Best Practices for Securing Infrastructure. (2017). O'Reilly Media.
9 Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Technical Series Publications. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf
10 Liu, L., Wang, B.-s., Yu, B., Zhong, Q.-x. (2017). Automatic malware classification and new malware detection using machine learning. Frontiers of Information Technology & Electronic Engineering, 18(9), 1336–1347. https://doi.org/10.1631/fitee.1601325
11 Cylance AI from BlackBerry. BlackBerry – Intelligent Security. Everywhere. https://www.blackberry.com/us/en/products/cylance-endpoint-security/cylance-ai
12 Cybersecurity Software. Cybereason. Cybersecurity Software. Cybereason. https://www.cybereason.com/

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023

Danyil Y. Zhuravchak
Postgraduate student, assistant of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0003-4989-0203
danyil.y.zhuravchak@lpnu.ua

Valerii B. Dudykevych
Doctor of Technical Sciences, Professor of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0001-8827-9920
valerii.b.dudykevych@lpnu.ua

Anastasiia Y. Tolkachova
Cybersecurity student
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8196-7963
anastasiia.tolkachova.mkbst.2022@lpnu.ua

STUDY OF THE STRUCTURE OF THE SYSTEM FOR DETECTING AND PREVENTING RANSOMWARE ATTACKS BASED ON ENDPOINT DETECTION AND RESPONSE

Abstract. The paper discusses the challenges and limitations of current ransomware detection and prevention systems, as well as potential future developments in the field. One key challenge is the constantly evolving nature of ransomware attacks, which requires systems to be regularly updated and adapted to stay effective. Another challenge is the need for systems to be able to distinguish between legitimate and malicious software, as well as different types of ransomware. To address these challenges, the paper proposes a number of functional and non-functional requirements for ransomware detection and counteraction systems. These include the ability to detect and respond to attacks in real time or close to it, the ability to analyze and classify different types of ransomware, and the ability to integrate with other security systems and tools. Additionally, non-functional requirements such as scalability, performance, and security should also be considered.The paper also presents a detailed analysis of the different types of ransomware detection and counteraction systems currently available, including intrusion detection systems (IDS), endpoint detection and response (EDR), and modern antiviruses. It also provides a comparison of their strengths and weaknesses, and a classification of existing solutions according to their similarity. Finally, the paper presents an evaluation algorithm for assessing the quality of products for detecting and countering ransomware. The algorithm is based on a set of functional and non-functional requirements and is designed to provide a comprehensive and objective assessment of the capabilities of different systems. The algorithm is validated through a series of tests and experiments, which demonstrate its effectiveness in identifying the best solutions for detecting and countering ransomware. Overall, this paper provides valuable insights and practical guidance for organizations looking to improve their defenses against ransomware attacks.

Keywords: ransomware, unauthorized access, detection methods

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 ESET - official website. Eset antivirus programs in Ukraine. ESET. https://www.eset.com/ua/
2 Now Available: Cisco Security Connector for iOS. Cisco Blogs. https://blogs.cisco.com/security/now-available-cisco-security-connector-for-ios
3 SentinelOne. Autonomous AI Endpoint Security Platform. SentinelOne DE. https://www.sentinelone.com/
4 Majors, C., Miranda, G., Fong-Jones, L. (2022). Observability Engineering: Achieving Production Excellence. O'Reilly Media, Incorporated.
5 A New Paradigm For Cyber Threat Hunting. (2018, 11 of June). The Hacker News. https://thehackernews.com/2018/06/cyber-threat-hunting.html
6 MITRE ATT&CK. https://attack.mitre.org/wiki/Main_Page

7 Mohamad Fadli Zolkipli Jantan, A. (2011). An approach for malware behavior identification and classification. In 2011 3rd International Conference on Computer Research and Development (ICCRD). IEEE. https://doi.org/10.1109/iccrd.2011.5764001
8 Defensive Security Handbook: Best Practices for Securing Infrastructure. (2017). O'Reilly Media.
9 Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Technical Series Publications. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf
10 Liu, L., Wang, B.-s., Yu, B., Zhong, Q.-x. (2017). Automatic malware classification and new malware detection using machine learning. Frontiers of Information Technology & Electronic Engineering, 18(9), 1336–1347. https://doi.org/10.1631/fitee.1601325
11 Cylance AI from BlackBerry. BlackBerry – Intelligent Security. Everywhere. https://www.blackberry.com/us/en/products/cylance-endpoint-security/cylance-ai
12 Cybersecurity Software. Cybereason. Cybersecurity Software. Cybereason. https://www.cybereason.com/