КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.21.1731
УДК 004.056

Штонда Роман Михайлович
Начальник науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0001-5986-0847
roman.shtonda@viti.edu.ua

Черниш Юлія Олександрівна
Старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0002-6626-5656
yuliia.chernysch@viti.edu.ua

Мальцева Ірина Робертівна
Старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0001-6073-4637
iryna.maltseva@viti.edu.ua

Цикало Юрій Григорович
Слухач
Національний університет оборони України імені Івана Черняховського, Київ, Україна
ORCID ID: 0009-0006-9698-3276
ab3366bk@ukr.net

Чайка Євген Іванович
Слухач
Національний університет оборони України імені Івана Черняховського, Київ, Україна
ORCID ID: 0000-0002-1937-8228
geniachauka84@gmail.com

Поліщук Сергій Анатолійович
Слухач
Національний університет оборони України імені Івана Черняховського, Київ, Україна
ORCID ID: 0009-0006-9110-7576
0988528103@ukr.net

ПРАКТИЧНІ ПІДХОДИ ДО КІБЕРЗАХИСТУ МОБІЛЬНИХ ПРИСТРОЇВ ЗА ДОПОМОГОЮ РІШЕННЯ ENDPOINT DETECTION AND RESPONSE

Анотація. У даній статті розглянуто практичні підходи щодо кіберзахисту мобільних пристроїв за допомогою рішення Endpoint Detection and Response та наведено отримані результати за проведеною роботою. З метою надійного захисту мобільних пристроїв авторами статті було проведено тестування програмних засобів CrowdStrike Falcon; Sophos Intercept X; Palo Alto Cortex XDR, що входять до рішення Endpoint Detection and Response. Дослідження проводилось на особистих мобільних пристроях співробітників нашої установи, які працюють на основі операційних систем Android та iOS. Комплексний збір даних моніторингу дозволяє Endpoint Detection and Response складати повне уявлення про потенційні кібератаки. Постійний моніторинг усіх мобільних пристроїв – онлайн та офлайн – полегшує аналіз кібербезпеки та реагування на кібератаки/кіберінциденти. Це дозволяє проводити глибокий аналіз кібербезпеки та надає розуміння, адміністраторам безпеки щодо аномалій та вразливостей, які виникають в мережах для усвідомлення майбутніх кіберзагроз. Виявлення кожної загрози виходить за рамки встановленого антивірусного програмного забезпечення, а отже здатність Endpoint Detection and Response забезпечувати реакцію в режимі реального часу на широкий спектр кіберзагроз дозволяє адміністраторам безпеки візуалізувати потенційні кібератаки/кіберінциденти, навіть коли вони здійснюють вплив на

хости та мобільні пристрої, і все це в режимі реального часу. Рішення Endpoint Detection and Response можна вважати набором традиційних антивірусних програмних засобів. Антивірусні програмні засоби самостійно обмежені в області застосування в порівнянні з більш новими рішеннями Endpoint Detection and Response. Таким чином, антивірусні програмні засоби є частиною Endpoint Detection and Response. Оскільки зловмисники вдосконалюють свої атаки та використовують передові технології для отримання доступу до мереж та даних користувачів, простий антивірусний програмний засіб, не в змозі своєчасно виявити загрози "нульового дня" або багатошарового рівня, а от системи Endpoint Detection and Response можуть виявляти всі типи кіберзагроз.

Ключові слова: кібератаки, кібербезпека, кіберзахист, мобільний пристрій, Endpoint Detection and Response, CrowdStrike Falcon; Sophos Intercept X; Palo Alto Cortex XDR.

ВСТУП

На сьогоднішній день, мобільний пристрій (далі – МП), використовує майже кожна друга людина в світі. Робота МП, які працюють за допомогою операційних систем (далі – ОС) Android та iOS, позиціонується на рівні сучасних технологій, а отже і кожен МП в тій чи іншій мірі позиціонується в мережі Інтернет. Будь то використання месенджерів, завантаження програм, розташування МП, карткові рахунки або навіть банально прослуховування музики та читання електронних книг вимагає підключення МП до мережі Інтернет. Дане підключення зазвичай здійснюється за допомогою можливостей SIM-карт із надання Інтернет послуг або через модулі Wi-Fi. Також МП мають можливість з'єднуватись з іншими пристроями за допомогою модуля Bluetooth. Всі ці дії можуть призвести до втрати важливої інформації користувачів та виникнення кібервпливів на самі МП [1].

Постановка проблеми. Однією із найактуальніших проблем, державних установ та організацій, є саме кібератаки на корпоративні інформаційно-комунікаційні системи та комунікаційні мережі, а також виникнення кіберінцидентів в цих системах та мережах [2]. Дану проблему в тій чи іншій мірі вирішують певні організації та призначені адміністратори безпеки за допомогою підходів із кіберзахисту. Але де є гарантія того, що інформаційно-комунікаційні системи та комунікаційні мережі, не попадуть під кібервплив за допомогою підключеного до них МП користувача, що немає відповідних налаштувань із кіберзахисту.

Аналіз останніх досліджень і публікацій. На сьогоднішній день існує велика кількість публікацій щодо наданих пропозицій, які вирішуються за допомогою Endpoint Detection and Response (далі – EDR). Але повноцінного відображення того, що може на практиці виконати EDR в них не відображено. Тому ми здійснили комплексне дослідження, даного питання, яке дозволить надійно протидіяти кіберзагрозам та кібератакам на МП користувачів під час їх підключення до корпоративних інформаційно-комунікаційних систем, комунікаційних мереж з метою недопущення витоку та втраті цінної інформації.

Мета статті. Метою даної статті є доведення до спільноти практичних підходів до кіберзахисту МП за допомогою рішення EDR, а також відображення результатів проведених досліджень за даним напрямком.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Кібератаки та кіберінциденти завдають нищівних проблем інформаційно-комунікаційним системам, комунікаційним мережам, побудованим лініям зв'язку та обладнанню із подекуди критичними наслідками.

На даний час під кібервплив переважно попадають в тій чи іншій мірі державні установи та організації. Але ніхто не гарантує пересічному споживачеві, що його МП не потрапить під вплив цих кібератак. Для того щоб зменшити кібервплив на особисті МП користувачів, інформаційно-комунікаційні системи, комунікаційні мережі, побудовані лінії зв'язку, обладнання та унеможливити подальше його розповсюдження, рекомендовано застосовувати рішення EDR [3].

EDR – це рішення, що виявляє, досліджує підозрілу діяльність та забезпечує кібербезпеку, як на хостах, так і на МП. EDR включає в себе моніторинг та збір даних про безпеку МП у режимі реального часу, за допомогою автоматизованих підходів реагування на кіберзагрози [4].

Дане рішення використовує високий ступінь автоматизації, яке дозволяє інформувати адміністраторів безпеки про виявлення кіберзагроз та забезпечує швидке реагування на порушення висунутих правил кібербезпеки.

EDR забезпечує п'ять основних функцій, які полягають у:

активному відстеженні МП та збору/отримані даних активності, які можуть свідчити про кіберзагрозу;

проведені аналізу зібраних даних для виявлення будь-яких відомих моделей кіберзагроз;

створені автоматичних відповідей на всі виявлені кіберзагрози, з метою видалення або відправлення їх в карантин;

автоматичному сповіщені адміністраторів безпеки про виявлені кіберзагрози;

використані інструментів аналізу та спеціальних досліджень з метою проведення досліджень виявлених кіберзагроз, які могли б призвести до інших підозрілих дій.

За допомогою EDR розгортається місце/пункт для створення сучасних команд кібербезпеки, які відображаються в якості контрольного списку. EDR захищає "цифровий периметр" від кіберзагроз та проблем кібербезпеки кількома ключовими способами.

Комплексний збір даних моніторингу дозволяє EDR скласти повне уявлення про потенційні кібератаки. Постійний моніторинг усіх МП – онлайн та офлайн – полегшує аналіз кібербезпеки та реагування на кібератаки/кіберінциденти. Це дозволяє проводити глибокий аналіз кібербезпеки та надає розуміння адміністраторам безпеки, щодо аномалій та вразливостей, які виникають в мережах, для усвідомлення майбутніх кіберзагроз. Виявлення кожної загрози виходить за рамки встановленого антивірусного програмного забезпечення, а отже здатність EDR забезпечувати реакцію в режимі реального часу на широкий спектр кіберзагроз дозволяє адміністраторам безпеки візуалізувати потенційні кібератаки/кіберінциденти, навіть коли вони здійснюють вплив на хости та МП, і все це в режимі реального часу.

Дані можливості дозволяють запобігти втратам, відсікаючи кібератаки на їх початкових стадіях до того, як відбудуться критичні втрати або компроміси. Реагування в режимі реального часу також дозволяє виявити підозрілу або несанкціоновану поведінку в мережі, дізнавшись про першопричину кіберзагрози, перш ніж вона зможе вплинути на роботу.

ISSN 2663 - 4023

Також EDR можна інтегруватися з іншими інструментами безпеки, що дозволяє корелювати дані з МП, мережі та SIEM для розвитку більш глибокого розуміння практик та методів, що застосовуються кіберзловмисником, який намагається отримати несанкціонований доступ до цифрових активів.

Дослідження здійснювалось шляхом аналізу інформації з відкритих джерел, вимог нормативних актів України у сфері захисту інформації та кібербезпеки, інсталяції, налаштування та тестування технічних та організаційних рішень щодо централізованого налаштування та захисту МП, аналізу/обробки результатів тестування, формування висновків та рекомендацій. Схема дослідження наведена на рис. 1.

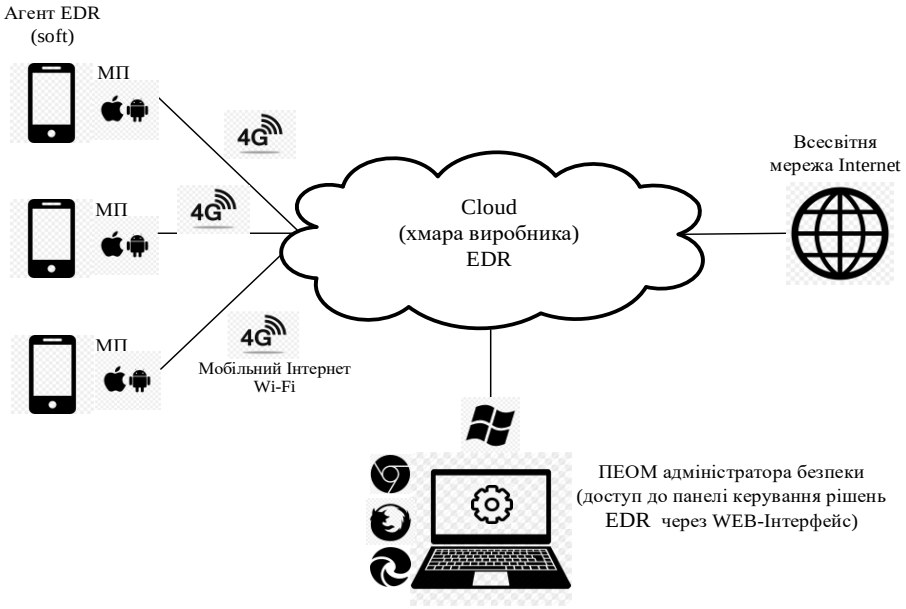

Рис. 1. Схема дослідження

Для проведення дослідження, використовувались особисті МП користувачів нашої організації, які позиціонувалися в мережі Інтернет та могли потрапити під вплив шкідливого програмного забезпечення (далі – ШПЗ) без відома цих користувачів.

Використовуючи EDR, була надана можливість вирішити ці проблеми шляхом:

виявлення та блокування потенційно небезпечних файлів, які могли б призвести до виникнення кіберзагроз на МП;

запобігання використанню USB-пристроїв для несанкціонованого доступу до даних або завантаження конфіденційної інформації;

блокування безфайлових методів атаки шкідливих програмних засобів, які можуть вплинути на МП;

управління виконанням скриптів;

запобігання кібератакам/кіберінцедентам, що могли виникнути при використанні особистої електронної пошти;

захист від “атак нульового дня” та запобігання нанесенню ними шкоди.

Виявлення та реагування на кіберзагрози для МП, здійснювалось шляхом моніторингу трафіку в мережі на цих МП, збору інформації, яка може стосуватися питань кібербезпеки. Далі було здійснено формування зібраної інформації в центральну базу даних та проведено аналіз кібербезпеки.

Під час виконання дослідження ключові компоненти типового рішення EDR включали:

агенти збору даних. Агентами збору даних в нашому випадку виступали антивірусні програмні засоби, що входять до рішень EDR.

Ці агенти, встановлені на МП, відстежували та виконували збір даних про запущені процеси, підключення до мереж і пристроїв, обсяг активності і передачу даних;

центральний хаб. Центральним хабом в нашому випадку виступали хмарні інформаційно-обчислювальні потужності, які були надані виробником EDR. За допомогою цього інтегрованого хабу здійснювалось збирання та аналіз даних в МП. Центральний хаб також координував оповіщення та реагування на безпосередні кіберзагрози;

автоматизація повідомлень. EDR використовував зазвичай попередньо налаштовані правила, які розпізнавали коли зібрані дані свідчать про кіберзагрозу, тоді запускалось автоматичне повідомлення призначене для адміністраторів безпеки або користувача викидало з системи;

виявлення та аналіз. До складу EDR входили інструменти виявлення шкідливого програмного забезпечення, які допомагали виявляти та знешкоджувати кіберзагрози, а також виконувати аналіз після обчислення, а аналітичні процеси в режимі реального часу допомагали швидко виявляти кіберзагрози, які не відповідали існуючим попередньо налаштованим правилам.

Розрахунок МП був розподілений наступним чином: МП із ОС Android – 20 комплектів; МП із ОС iOS – 10 комплектів.

Саме дослідження проводилось за наступними питаннями перевірки:

забезпечення захисту від витоку інформації з МП;

централізований облік МП та їх користувачів;

централізоване налаштування політик безпеки МП;

забезпечення захисту МП від ШПЗ;

виявлення вразливостей ОС та програмних засобів МП;

забезпечення захисту мережевого трафіку МП;

забезпечення захисту від фішингу на МП;

забезпечення можливості логування мережевого трафіку МП;

забезпечення можливості логування та збору інформації про інциденти кібернетичної безпеки, що відбулися на МП;

інтеграція з рішеннями SIEM;

можливість розділення персональної інформації, та інформації, шо мас відношення до службової діяльності на МП;

можливість управляти налаштуваннями месенджерів та контролювати наявність у них сторонніх підключень (сесій);

можливість контролювати наявність сторонніх підключень (сесій) у Google та Apple акаунтах;

можливість контролю наявності двофакторної автентифікації у Google та Apple акаунтах, у месенджерах, що використовуються МП;

можливість додавання власних індикаторів компрометації у базу системи налаштування та захисту МП;

можливість виявлення додатку чи процесу ОС, який звертається на шкідливі веб-ресурси чи здійснює інші підозрілі (незвичайні) дії;

налаштування політики паролів;

примусове встановлення паролю;

примусове змінення паролю МП;

шифрування даних на МП;

знищення даних на МП (через СМС, Інтернет, у разі спроби підбору паролю або невикористання пристрою під час деякого часу);

блокування МП;

побудова VPN тунелю;

примусове вимкнення геолокації, камери, мікрофону, Bluetooth, Wi-Fi МП;

надсилання повідомлень на МП;

блокування та видалення програмного забезпечення на МП;

встановлення та оновлення програмного забезпечення на МП;

перевірка відповідності технічних рішень системи централізованого налаштування та захисту МП вимогам чинного законодавства у сфері захисту інформації, наявність експертних висновків Державної служби спеціального зв'язку та захисту інформації України або перспективи їх отримання;

Дослідження проводились відповідно до керівних документів у сфері кіберзахисту МП [5].

Під час дослідження колективом було проведено перевірку антивірусних програмних засобів, що входять до топ-10 найкращих рішень EDR, серед них: CrowdStrike Falcon; Sophos Intercept X; Palo Alto Cortex XDR [6-8].

CrowdStrike Falcon.

Компанія CrowdStrike для захисту МП запропонувала своє головне рішення CrowdStrike Falcon. Платформа CrowdStrike Falcon – це перше хмарне рішення в галузі, яке захищає МП шляхом об'єднання антивірусного програмного забезпечення нового покоління, системи EDR (виявлення і реагування на кіберзагрози в МП), а також цілодобової керованої служби пошуку кіберзагроз [9].

Платформа CrowdStrike Falcon базується на штучному інтелекті (AI) і об'єднує технології, інтелект та досвід в одне просте рішення, яке надійно зупиняє будь-які кіберзагрози. Платформа за лічені хвилини забезпечує кіберзахист у реальному часі, а ефективні алгоритми штучного інтелекту дозволяють побачити результат вже з першого використання. Хмарна інфраструктура та архітектура усувають складність у роботі з різними додатками, забезпечують керованість та швидкість рішення.

Платформа CrowdStrike Falcon гнучка та масштабована і містить різноманітні модулі для кіберзахисту паролів доступу та локальних мереж з різними кінцевими пристроями (ноутбуки, ПК, сервери, МП). Кожен модуль доступний на платформі CrowdStrike Falcon реалізований за допомогою єдиної хмарної консолі управління та єдиного агента для МП.

Модулі рішення:

Falcon Prevent (головний компонент). Становить собою антивірусне програмне забезпечення нового покоління Crowdstrike Falcon на основі платформи NGAV. Це дозволяє виявляти підозрілу активність, запобігати та усувати порушення в системі кібербезпеки, поки вони не відбулися;

Falcon Insight. EDR, забезпечує постійну та всеосяжну видимість МП, яка охоплює виявлення, реагування та розслідування кіберзагроз, що виникають;

Falcon Device Control, продукт, що надає повну видимість використання USB-пристроїв;

Falcon Overwatch, механізм виявлення кіберзагроз, який здійснює постійний пошук та вживає заходів щодо нейтралізації найскладніших прихованих кіберзагроз. Також даний механізм дозволяє попереджати людський фактор;

Falcon Discover, рішення з IT гігієни, яке дозволяє в режимі реального часу визначати несанкціоновані системи та програми у МП, а також швидко виправляти проблеми для покращення загального стану кібербезпеки;

Falcon Spotlight, продукт для оцінки вразливостей, який допомагає адміністраторам безпеки визначати пріоритети, знаходити та виправляти вразливості раніше, ніж вони призводять до порушень;

Falcon X, рішення для проведення автоматизованого розслідування інцидентів, прискорення сортування сповіщень та здійснення негайного реагування;

Falcon Search Engine, рішення, у якому поєднується швидкий та всебічний пошук шкідливого програмного забезпечення з CrowdStrike Falcon Intelligence, дає значну перевагу адміністраторам безпеки щодо випередження зловмисників.

Платформа CrowdStrike Falcon є у вільному доступі в Google Play для Android та App Store для iOS. Для активації CrowdStrike Falcon необхідна ліцензійна підписка. Станом на час дослідження лютий 2023 року ліцензування здійснюється на основі переплати для кожного МП.

Для встановлення CrowdStrike Falcon на МП, ОС Android повинна бути не нижче версії 8.0, а ОС iOS не нижче версії 13.0.

Результати досліджень можливостей CrowdStrike Falcon наведені в таблиці 1.

Таблиця 1

Результати досліджень можливостей CrowdStrike Falcon

Питання, що досліджувалися		Операційна система	
		Android	iOS
1.	Забезпечення захисту від витоку інформації з МП	-	-
2.	Централізований облік МП та їх користувачів	+	+
3.	Централізоване налаштування політик безпеки МП	+	+
4.	Забезпечення захисту МП від ШПЗ	+	+
5.	Виявлення вразливостей ОС та ПЗ МП	+	+
6.	Забезпечення захисту мережевого трафіку МП	+	+
7.	Забезпечення захисту від фішингу на МП	+	+
8.	Забезпечення можливості логування мережевого трафіку МП	-	-
9.	Забезпечення можливості логування та збору інформації про інциденти кібернетичної безпеки, що відбулися на МП	+	+
10.	Інтеграція з рішеннями SIEM	+	+
11.	Можливість розділення персональної інформації, та інформації, шо мас відношення до службової діяльності на МП	-	-
12.	Можливість управляти налаштуваннями месенджерів та контролювати наявність у них сторонніх підключень (сесій)	-	-
13.	Можливість контролювати наявність сторонніх підключень (сесій) у Google та Apple акаунтах	-	-
14.	Можливість контролю наявності двофакторної автентифікації у Google та Apple акаунтах, у месенджерах, що використовуються МП	-	-
15.	Можливість додавання власних індикаторів компрометації у базу системи налаштування та захисту МП	-	-
16.	Можливість виявлення додатку чи процесу ОС, який звертається на шкідливі веб-ресурси чи здійснює інші підозрілі (незвичайні) дії	+	+
17.	Налаштування політики паролів	-	-
18.	Примусове встановлення паролю	-	-
19.	Примусове змінення паролю МП	-	-

20	Шифрування даних на МП	-	-
21.	Знищення даних на МП (через СМС, Інтернет, у разі спроби підбору паролю або невикористання пристрою під час деякого часу)	-	-
22.	Блокування МП	-	-
23.	Побудова VPN тунелю	-	-
24.	Примусове вимкнення геолокації,, камери, мікрофону, Bluetooth, Wi-Fi МП	-	-
25.	Надсилання повідомлень на МП	+	+
26.	Блокування та видалення програмного забезпечення на МП	-	-
27.	Встановлення та оновлення програмного забезпечення на МП	-	-
28.	Перевірка відповідності технічних рішень системи централізованого налаштування та захисту МП вимогам чинного законодавства у сфері захисту- інформації, наявність експертних висновків Державної служби спеціального зв'язку та захисту інформації України або перспективи їх отримання	+	+

Після встановлення CrowdStrike Falcon на МП, система автоматично отримує дозволи до додатків та програм з метою централізованого налаштування, а саме: встановлювати ярлики; показувати на екрані блокування; увімкнути WLAN; увімкнути Bluetooth; використовувати камеру; читати список інстальованих програм.

Sophos Intercept X.

Sophos Intercept X забезпечує кіберзахист МП від шкідливого програмного забезпечення та інших мобільних загроз.

Встановлений Sophos Intercept X відразу приступає до сканування вашого МП. Провівши сканування МП Sophos Intercept X виводить звіт про проведену роботу на екран. У разі виявлення загроз Sophos Intercept X сповіщає про це, відобразивши де є загрози червоним кольором, а у разі відсутності загроз виділяється зеленим кольором.

Відкривши Device unsafe (пристрій небезпечний), на екрані відображається де виникли загрози.

За допомогою Device security (безпека пристрою), Sophos Intercept X постійно стежить за справністю пристрою та сповіщає вас, якщо пристрій зламано, щоб ви могли вжити заходів щодо виправлення проблеми або автоматично скасувати доступ до конфіденційної інформації. Адміністратори безпеки мають змогу виявляти кіберзагрози і можуть інформувати користувача про необхідні оновлення ОС.

За допомогою Network security (безпека мережі) є можливість створити першу лінію захисту на рівні мобільної мережі на Android та iOS. Мережеві з'єднання перевіряються в режимі реального часу на наявність підозрілих характеристик, які можуть ідентифікувати кібератаку. Це допомагає знизити ризик атак типу "людина посередині" (MitM). Веб-фільтрація та перевірка URL-адрес припиняє доступ до завідомо шкідливих сайтів на МП, а функція виявлення фішингу SMS виявляє шкідливі URL-адреси.

За допомогою Application security (безпека програми), Sophos Intercept X виявляє шкідливі та потенційно небажані програмні засоби, встановлені на пристроях Android та iOS, використовуючи технологію пошуку нових шкідливих програмних засобів. Користувачі та адміністратори безпеки мають можливість отримувати сповіщення про зміну статусу загрози МП. Інтеграція з Microsoft Intune дозволяє адміністраторам безпеки створювати політики умовного доступу, обмежуючи доступ до програм і даних у разі виявлення кіберзагрози [10].

Даний програмний засіб є у вільному доступі в Google Play для Android та App Store для iOS.

Платформа Sophos Intercept X є у вільному доступі в Google Play для Android та App Store для iOS. Для активації Sophos Intercept X необхідна ліцензійна підписка. Станом на час дослідження лютий 2023 року ліцензування здійснюється на основі переплати для кожного МП.

Для встановлення Sophos Intercept X на МП, ОС Android повинна бути не нижче версії 7.0, а ОС iOS не нижче версії 14.0.

Результати досліджень можливостей Sophos Intercept X наведені в таблиці 2.

Таблиця 2

Результати досліджень можливостей Sophos Intercept X

Питання, що досліджувалися		Операційна система	
		Android	iOS
1.	Забезпечення захисту від витоку інформації з МП	-	-
2.	Централізований облік МП та їх користувачів	+	+
3.	Централізоване налаштування політик безпеки МП	+	+
4.	Забезпечення захисту МП від ШПЗ	+	+
5.	Виявлення вразливостей ОС та ПЗ МП	+	+
6.	Забезпечення захисту мережевого трафіку МП	+	+
7.	Забезпечення захисту від фішингу на МП	+	+
8.	Забезпечення можливості логування мережевого трафіку МП	-	-
9.	Забезпечення можливості логування та збору інформації про інциденти кібернетичної безпеки, що відбулися на МП	+	+
10.	Інтеграція з рішеннями SIEM	+	+
11.	Можливість розділення персональної інформації, та інформації, шо мас відношення до службової діяльності на МП	-	-
12.	Можливість управляти налаштуваннями месенджерів та контролювати наявність у них сторонніх підключень (сесій)	-	-
13.	Можливість контролювати наявність сторонніх підключень (сесій) у Google та Apple акаунтах	-	-
14.	Можливість контролю наявності двофакторної автентифікації у Google та Apple акаунтах, у месенджерах, що використовуються МП	-	-
15.	Можливість додавання власних індикаторів компрометації у базу системи налаштування та захисту МП	-	-
16.	Можливість виявлення додатку чи процесу ОС, який звертається на шкідливі веб-ресурси чи здійснює інші підозрілі (незвичайні) дії	+	+
17.	Налаштування політики паролів	-	-
18.	Примусове встановлення паролю	+	+
19.	Примусове змінення паролю МП	-	-
20	Шифрування даних на МП	+	-
21.	Знищення даних на МП (через СМС, Інтернет, у разі спроби підбору паролю або невикористання пристрою під час деякого часу)	-	-
22.	Блокування МП	+	+
23.	Побудова VPN тунелю	-	-
24.	Примусове вимкнення геолокації,, камери, мікрофону, Bluetooth, Wi-Fi МП	+	+
25.	Надсилання повідомлень на МП	+	+
26.	Блокування та видалення програмного забезпечення на МП	-	-
27.	Встановлення та оновлення програмного забезпечення на МП	+	-

28.	Перевірка відповідності технічних рішень системи централізованого налаштування та захисту МП вимогам чинного законодавства у сфері захисту- інформації, наявність експертних висновків Державної служби спеціального зв'язку та захисту інформації України або перспективи їх отримання	-	-

Після встановлення Sophos Intercept X на МП, система автоматично отримує дозволи до додатків та програм з метою централізованого налаштування, а саме: встановлювати ярлики; показувати на екрані блокування; увімкнути WLAN; доступ до даних про місцезнаходження; використовувати камеру; читати список інстальованих програм; використовувати пам'ять телефону.

Palo Alto Cortex XDR.

Компанія Palo Alto Networks розробила додаток Cortex XDR для розширеного захисту від ШПЗ в МП.

Додаток Cortex XDR для Android та iOS запобігає проникненню на МП відомого ШПЗ та невідомих файлів APK.

Додаток Cortex XDR застосовує політику безпеки для блокування відомого ШПЗ та невідомих файлів, завантаження невідомих файлів для глибокого огляду та аналізу, обробки сірого програмного забезпечення, як ШПЗ та проведення локального аналізу, щоб визначити ймовірність того, що невідомий файл є ШПЗ або не являється таким. Також надається можливість додавати до списку, довірених користувачів, щоб дозволити використовувати невідомі додатки, перш ніж програма Cortex XDR отримає офіційний висновок стосовно цих невідомих додатків.

Особливості Cortex XDR:

автоматичне виявлення прихованих і складних загроз мережі за допомогою штучного інтелекту;

швидка фільтрація помилкових алертів, що скорочує навантаження на персонал;

аналіз ШПЗ за рахунок механізму на основі AI, який навчається протистояти новим методам кібератак;

визначення і блокування ШПЗ, експлойтів і безфайлових атак в наслідок поєднання локального і хмарного аналізу на основі AI;

поведінкова аналітика;

виявлення реальних загроз серед нормальних "аномалій".

За допомогою Cortex XDR є можливість забезпечити кіберзахист МП, автоматичного аналізу зібраних даних з різних джерел, що значно пришвидшує роботу адміністраторів безпеки.

Cortex XDR забезпечує:

безпеку МП за допомогою NGAV, брандмауера хоста, шифрування диска та контролю USB-пристроїв;

виявлення ШПЗ за допомогою технології ML. За допомогою аналітики поведінки надається можливість знайти приховане ШПЗ, як-от зловживання інсайдерами, атаки на облікові дані та викрадання;

управління інцидентами. Забезпечується можливість скоротити час аудиту за допомогою інтелектуального групування сповіщень. Підрахунок кібератак/кіберінцидентів дає змогу зосередитися на важливих кіберзагрозах;

автоматизований аналіз основної причини. Надана можливість швидко перевіряти кіберзагрози, переглядаючи першопричину, послідовність подій, дані аудиту та деталі аудиту в одному місці;

глибинні дослідження. Надана можливість проводити перевірки стану кібербезпеки на МП, навіть якщо ці МП не підключені до мережі;

гнучке реагування. Здійснюється блокування кібератак, забезпечується ізоляція МП, виконується сценарій та охоплюється все середовище, щоб стримати кіберзагрози в реальному часі.

Платформа Cortex XDR є у вільному доступі в Google Play для Android та App Store для iOS для існуючих клієнтів Palo Alto Networks Cortex XDR. Для активації Sophos Intercept X необхідна ліцензійна підписка на послугу управління Cortex XDR або Traps. Станом на час дослідження лютий 2023 року ліцензування здійснюється на основі переплати для кожного МП.

Для встановлення Palo Alto Networks Cortex XDR на МП, ОС Android повинна бути не нижче версії 6.0, а ОС iOS не нижче версії 10.0.

Результати досліджень можливостей Palo Alto Networks Cortex XDR наведені в таблиці 3.

Таблиця 3

Результати досліджень можливостей Palo Alto Networks Cortex XDR

Питання, що досліджувалися		Операційна система	
		Android	iOS
1.	Забезпечення захисту від витоку інформації з МП	+	+
2.	Централізований облік МП та їх користувачів	+	+
3.	Централізоване налаштування політик безпеки МП	+	+
4.	Забезпечення захисту МП від ШПЗ	+	+
5.	Виявлення вразливостей ОС та ПЗ МП	+	+
6.	Забезпечення захисту мережевого трафіку МП	–	–
7.	Забезпечення захисту від фішингу на МП	–	–
8.	Забезпечення можливості логування мережевого трафіку МП	–	–
9.	Забезпечення можливості логування та збору інформації про інциденти кібернетичної безпеки, що відбулися на МП	–	–
10.	Інтеграція з рішеннями SIEM	–	–
11.	Можливість розділення персональної інформації, та інформації, шо мас відношення до службової діяльності на МП	–	–
12.	Можливість управляти налаштуваннями месенджерів та контролювати наявність у них сторонніх підключень (сесій)	–	–
13.	Можливість контролювати наявність сторонніх підключень (сесій) у Google та Apple акаунтах	–	–
14.	Можливість контролю наявності двофакторної автентифікації у Google та Apple акаунтах, у месенджерах, що використовуються МП	–	–
15.	Можливість додавання власних індикаторів компрометації у базу системи налаштування та захисту МП	+	+
16.	Можливість виявлення додатку чи процесу ОС, який звертається на шкідливі веб-ресурси чи здійснює інші підозрілі (незвичайні) дії	+	+
17.	Налаштування політики паролів	–	–
18.	Примусове встановлення паролю	–	–
19.	Примусове змінення паролю МП	–	–
20	Шифрування даних на МП	–	–
21.	Знищення даних на МП (через СМС, Інтернет, у разі спроби підбору паролю або невикористання пристрою під час деякого часу)	–	–
22.	Блокування МП	+	+
23.	Побудова VPN тунелю	+	+

24.	Примусове вимкнення геолокації,, камери, мікрофону, Bluetooth, Wi-Fi МП	–	–
25.	Надсилання повідомлень на МП	–	–
26.	Блокування та видалення програмного забезпечення на МП	–	–
27.	Встановлення та оновлення програмного забезпечення на МП	–	–
28.	Відповідність технічних рішень системи централізованого налаштування та захисту МП вимогам чинного законодавства у сфері захисту- інформації, наявність експертних висновків Державної служби спеціального зв'язку та захисту інформації України або перспективи їх отримання	+	+

Перелік даних про МП та користувача, до яких отримує доступ Palo Alto Networks Cortex XDR, після встановлення є наступним: інформація про процеси, які запущені на МП; інформація про файли та директорії, що знаходяться на МП; інформація про мережеві з'єднання та використання мережі на МП; інформація про систему та апаратне забезпечення МП; журнали подій, що стосуються дій користувача та системних процесів на МП; інформація про активних користувачів на МП; інформація про права доступу користувачів на МП; інформація про виконувані користувачами процеси на МП; інформація про мережеві з'єднання, які встановлюють користувачі на МП.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

За результатами тестування, всі рішення можуть інтегруватись з рішеннями SIEM, крім Palo Alto networks Cortex XDR. Експертний висновок Державної служби спеціального зв'язку та захисту інформації України відповідності технічних рішень вимогам чинного законодавства у сфері захисту інформації мають, Palo Alto networks Cortex XDR, CrowdStrike Falcon. Рішення CrowdStrike Falcon може повністю розгортатись на обладнанні замовника.

Враховуючи, що немає 100% відповідних рішень, доцільно з метою впровадження системи централізованого налаштування та захисту МП, розробити та затвердити політику безпеки організації/установи, а вже потім на її основі вибрати найбільш відповідні програмні рішення.

Подальшими дослідженнями є проведення тестувань програм, що входять до рішення Mobile Device Manager та за результатами даних тестувань, надання пропозицій щодо поєднання даних рішень.

Боремося з кібертерором разом! Разом до перемоги! Слава Україні!

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Штонда, Р. М., Остапчук, В. М., Радзівілов, Г. Д. (2023). Використання рішення Endpoint Detection and Response для кіберзахисту мобільних пристроїв. У Кіберборотьба: розвідка, захист та протидія (с. 56).

2 Oleksenko, V., Shtonda, R., Chernish, Y., Maltseva, I. (2022). MODERN APPROACHES TO PROVIDING CYBER SECURITY IN RADIO RELAY COMMUNICATION LINES. Cybersecurity: Education, Science, Technique, 1(17), 57–64. https://doi.org/10.28925/2663-4023.2022.17.5764.

3 Штонда, Р.М., Чацка, Є.І. (2023). Кіберзахист мобільних пристроїв за допомогою рішення Endpoint Detection and Response. У Інформаційні технології в культурі, мистецтві, освіті, науці, економіці та бізнесі (с. 34–35).

4 Overview of endpoint detection and response. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-endpoint-detection-response?view=o365-worldwide.

5 NIST SP 1800-22 Mobile Device Security: Bring Your Own Device (BYOD). https://www.nccoe.nist.gov/publications/practice-guide/mobile-device-security-bring-your-own-device-nist-sp-1800-22-practice-0.
6 One platform. complete protection. https://www.crowdstrike.com/falcon-platform/.
7 The World's Best Endpoint Protection. XDR, EDR, ZTNA, MDR Services. https://www.sophos.com/en-us/products/endpoint-antivirus.
8 What is Cortex XDR? https://live.paloaltonetworks.com/t5/blogs/what-is-cortex-xdr/ba-p/251610.
9 Штонда, Р.М, Терещенко, Т.П., Черниш, Ю.О., Мальцева, І.Р. (2023). Дослідження можливостей платформи CrowdStrike Falcon щодо забезпечення кіберзахисту кінцевих пристроїв. У Principles of science. Ideals, norms, values in science and style of scientific thinking. (с. 20–22).
10 Mobile Threat Defense for Android, iOS, and Chrome OS. https://www.sophos.com/en-us/products/mobile-control/intercept-x.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023

Roman M. Shtonda
Head of Research Department
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0001-5986-0847
roman.shtonda@viti.edu.ua

Yuliya O. Chernish
Senior Researcher
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-6626-5656
yuliia.chernysch@viti.edu.ua

Irina R. Maltseva
Senior Researcher
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0001-6073-4637
iryna.maltseva@viti.edu.ua

Yurii G. Tsykalo
Listener
National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID ID: 0009-0006-9698-3276
ab3366bk@ukr.net

Yevhen I. Chaika
Listener
National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID ID: 0000-0002-1937-8228
geniachauka84@gmail.com

Serhiy A. Polishchuk
Listener
National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID ID: 0009-0006-9110-7576
0988528103@ukr.net

PRACTICAL APPROACHES TO CYBER PROTECTION OF MOBILE DEVICES WITH THE HELP OF A SOLUTION ENDPOINT DETECTION AND RESPONSE

Abstract. In this article, practical approaches to cyber protection of mobile devices using the Endpoint Detection and Response solution are considered and the results of the work carried out are given. In order to reliably protect mobile devices, the authors of the article conducted testing of CrowdStrike Falcon software; Sophos Intercept X; Palo Alto Cortex XDR included in the Endpoint Detection and Response solution. The research was conducted on personal mobile devices of employees of our institution, which work on the basis of Android and iOS operating systems. Comprehensive collection of monitoring data allows Endpoint Detection and Response to create a complete picture of potential cyber attacks. Continuous monitoring of all mobile devices – online and offline – facilitates cybersecurity analysis and response to cyber attacks/cyber incidents. This enables deep cybersecurity analysis and provides security administrators with insight into anomalies and vulnerabilities that occur in networks to anticipate future cyber threats. The detection of each threat goes beyond the scope of installed antivirus software, so Endpoint Detection and Response's ability to provide real-time response to a wide range of cyber threats allows security administrators to visualize potential cyber attacks/cyber incidents even as they impact hosts and mobile devices, and all it's in real time. The Endpoint Detection and Response solution can be considered a set of traditional antivirus software tools. Antivirus software alone is limited in scope compared to newer Endpoint Detection and Response solutions. Thus, antivirus software is part of Endpoint Detection

and Response. As attackers improve their attacks and use advanced technologies to gain access to networks and user data, simple antivirus software cannot detect zero-day or multi-layer threats in a timely manner, but Endpoint Detection and Response systems can detect all types of cyber threats.

Key words: cyber attacks, cyber security, cyber defense, mobile device, Endpoint Detection and Response, CrowdStrike Falcon; Sophos Intercept X; Palo Alto Cortex XDR.

REFERENCES

1 Shtonda, R. M., Ostapchuk, V. M., Radzivilov, H. D. (2023). Vykorystannia rishennia Endpoint Detection and Response dlia kiberzakhystu mobilnykh prystroiv. In Kiberborotba: rozvidka, zakhyst ta protydiia (p. 56).
2 Oleksenko, V., Shtonda, R., Chernish, Y., Maltseva, I. (2022). MODERN APPROACHES TO PROVIDING CYBER SECURITY IN RADIO RELAY COMMUNICATION LINES. Cybersecurity: Education, Science, Technique, 1(17), 57–64. https://doi.org/10.28925/2663-4023.2022.17.5764.
3 Shtonda, R.M., Chatska, Ye.I. (2023). Kiberzakhyst mobilnykh prystroiv za dopomohoiu rishennia Endpoint Detection and Response. In Informatsiini tekhnolohii v kulturi, mystetstvi, osviti, nautsi, ekonomitsi ta biznesi (p. 34–35).
4 Overview of endpoint detection and response. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-endpoint-detection-response?view=o365-worldwide.
5 NIST SP 1800-22 Mobile Device Security: Bring Your Own Device (BYOD). https://www.nccoe.nist.gov/publications/practice-guide/mobile-device-security-bring-your-own-device-nist-sp-1800-22-practice-0.
6 One platform. complete protection. https://www.crowdstrike.com/falcon-platform/.
7 The Worlds Best Endpoint Protection. XDR, EDR, ZTNA, MDR Services. https://www.sophos.com/en-us/products/endpoint-antivirus.
8 What is Cortex XDR? https://live.paloaltonetworks.com/t5/blogs/what-is-cortex-xdr/ba-p/251610.
9 Shtonda, R.M, Tereshchenko, T.P., Chernysh, Yu.O., Maltseva, I.R. (2023). Doslidzhennia mozhlyvostei platformy CrowdStrike Falcon shchodo zabezpechennia kiberzakhystu kintsevykh prystroiv. In Principles of science. Ideals, norms, values in science and style of scientific thinking. (p. 20–22).
10 Mobile Threat Defense for Android, iOS, and Chrome OS. https://www.sophos.com/en-us/products/mobile-control/intercept-x.