КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.737
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

Чередниченко Олексій Юрійович
старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
Київ, Україна
ORCID ID: 0000-0002-0816-8321
oleksiy.cherednychenko@viti.edu.ua

Фомкін Денис Валентинович
науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
Київ, Україна
ORCID ID: 0000-0003-0128-9355
denys.fomkin@viti.edu.ua

Бокій Олена Володимирівна
науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
Київ, Україна
ORCID ID: 0009-0006-3459-5665
olenabokiy1971@gmail.com

Куцаєв Павло Володимирович
молодший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
Київ, Україна
ORCID ID: 0000-0002-3235-3316
pavlo.kutsayev@viti.edu.ua

МЕТОДИКА ТЕСТУВАННЯ МОЖЛИВОСТЕЙ ПРОГРАМНИХ РІШЕНЬ ENDPOINT DETECTION AND RESPONSE (EXTENDED DETECTION AND RESPONSE)

Анотація. В умовах функціонування сучасного кіберпростору програмні рішення Endpoint Detection and Response (Extended Detection and Response) є запорукою кіберзахисту. Ці рішення відіграють ключову роль у кіберзахисті кінцевих пристроїв що функціонують в інформаційно-комунікаційних системах та електронних комунікаційних мережах. Однак ефективність цих рішень може суттєво відрізнятись. Саме тому необхідний є комплексний підхід до тестування їх можливостей, що дозволить ефективно їх оцінити. У даній статті розглянуто методику тестування можливостей програмних рішень Endpoint Detection and Response (Extended Detection and Response). Тестування програмних рішень Endpoint Detection and Response (Extended Detection and Response) здійснюється за наступними методиками, що запропоновані авторами статті: перевірка організаційних питань; перевірка можливостей щодо інсталяції, видалення, та роботи в системі; перевірка конфігурування, редагування політик та правил; перевірка функцій консолі; перевірка питань менеджменту індикаторів загроз, виявлення, реагування та блокування загроз; перевірка можливостей проведення аналізу та здійснення збору даних; перевірка додаткових функцій та модулів. Після проведення тестування за переліченими методиками необхідно здійснити оцінку

результатів тестування. Дана оцінка результатів здійснюється окремо по кожному програмному рішенню Endpoint Detection and Response (Extended Detection and Response) для кожної операційної системи та їх порівняльний аналіз за балами та коефіцієнтами. За результатами тестування відпрацьовується звіт, в якому надаються конкретні пропозиції щодо вибору найбільш доцільного програмного рішення для застосування на кінцевих пристроях із врахуванням результатів практичного тестування, організаційно-фінансових питань та наявності експертного висновку Державної служби спеціального зв'язку та захисту інформації України.

Ключові слова: кібератаки; кібербезпека; кіберзахист; кіберінциденти; кінцевий пристрій; рішення.

ВСТУП

На сьогоднішній день, персональна електронна обчислювальна машина (далі — кінцевий пристрій), що немає доступу до електронно комунікаційних мереж (далі — ЕКМ), являється банальною «печатною машиною» початку 20 ст. Тому левова частка кінцевих пристроїв підключених до ЕКМ є потенційними цілями кіберзлочинців в кіберпросторі. Для забезпечення кіберзахисту кінцевих пристроїв слід використовувати програмні рішення Endpoint Detection and Response (Extended Detection and Response) (далі — рішення EDR (XDR)).

Рішення EDR (XDR) є складовою кіберзахисту інформаційно-комунікаційних систем (далі — ІКС), а також ЕКМ. Рішення EDR (XDR) забезпечує кіберзахист ІКС (ЕКМ), шляхом виявлення шкідливого програмного забезпечення (далі — ШПЗ) та підозрілої діяльності на серверному обладнані та кінцевих пристроях (далі — кінцеві пристрої), що підключені до них [1].

Постановка проблеми. Однією із найактуальніших проблем — є саме кібератаки на ІКС та ЕКМ та виникнення кіберінцидентів [2]. Дану проблему в тій чи іншій мірі вирішують Security Operations Center (далі — SOC) та аналітики з їх складу, за допомогою підходів із кіберзахисту. Але де є гарантія того, що ІКС та ЕКМ не попадуть під кібервплив за допомогою підключеного до них кінцевого пристрою, який не знаходиться під захистом рішень EDR (XDR).

Для вибору більш оптимального та необхідного рішення EDR (XDR), що буде використовуватись для захисту кінцевих пристроїв в ІКС та ЕКМ слід використовувати запропоновану нами в статті Методику тестування можливостей програмних рішень EDR (XDR).

Аналіз останніх досліджень і публікацій. В статті [3] відображено практичні підходи до кіберзахисту мобільних комунікаційних пристроїв за допомогою рішення EDR, а також відображення результатів проведених досліджень за даним напрямком. Можна прослідкувати в статті [3] певну методику тестування можливостей програмних рішень EDR для мобільних комунікаційних пристроїв. Але нічого не зазначається про рішення XDR та про методику проведення тестування можливостей програмних рішень EDR (XDR) для захисту кінцевих пристроїв в ІКС та ЕКМ. Тому авторський колектив здійснив комплексне дослідження даного питання та запропонував Методику тестування можливостей програмних рішень EDR (XDR).

Мета статті. Метою даної статті є розроблення Методики тестування можливостей програмних рішень EDR (XDR) для кіберзахисту кінцевих пристроїв в ІКС та ЕКМ.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Практичне тестування можливостей програмних рішень EDR (XDR) слід здійснювати відповідно до розробленої Методики тестування можливостей програмних рішень EDR (XDR), з використанням мережевої інфраструктури відповідно до заздалегідь розроблених схем тестування [4].

При проведені тестування слід використовувати кінцеві пристрої що підключені до ЕКМ із встановленими на них відповідних операційних систем (Windows 10 Pro, Windows 11, Windows Server 2022; Ubuntu 22.04 LTS, тощо), а також хмарні обчислювальні потужності, які надані виробниками рішень EDR (XDR), вони повинні мати окремий відведений простір для проведення тестування та окремий доступ адміністратора для налаштування та керування кінцевими пристроями.

Тестування рішень EDR (XDR) слід здійснювати в наступній послідовності (окремо по кожному рішенню, що цікавить [5]).

Перед початком проведення тестування необхідно отримати або ж придбати ліцензії у виробників рішень EDR (XDR).

Здійснити активацію облікових записів, встановити логін та пароль, і за можливісті, якщо це передбачено виробником, встановити двохфакторну аутентифікацію.

В хмарному середовищі виробника створити віртуальний контекст з панеллю адміністрування програмного рішення. Виробник рішень EDR (XDR) в свою чергу повинен надати віддалений доступ до панелі адміністрування кінцевого пристрою адміністратору безпеки, який здійснює створення та налаштування політик безпеки.

Після одержання ліцензій проводиться інсталяція програмних рішень на кінцеві пристрої, які задіяні у тестуванні. Наступним кроком є перевірка доступності кінцевих пристроїв у віддаленій панелі адміністрування, після чого необхідно здійснити застосування політик безпеки до цього пристрою. Перевіряємо за допомогою хмарних обчислювальних потужностей можливість здійснення координування оповіщень та реагування на безпосередні кіберзагрози.

Провівши дані заходи щодо налаштувань та підготовки проводимо тестування можливостей встановлених рішень EDR (XDR). Тестування можливостей програмних рішень EDR (XDR) здійснюється за наступними методиками:

- перевірка організаційних питань;
- перевірка можливостей щодо інсталяції, видалення, та роботи в системі;
- перевірка конфігурування, редагування політик та правил;
- перевірка функцій консолі;
- перевірка питань менеджменту індикаторів загроз, виявлення, реагування та блокування загроз;
- перевірка можливостей проведення аналізу та здійснення збору даних;
- перевірка додаткових функцій та модулів.

Під час перевірки організаційних питань перевіряються:

- вартість впровадження та підтримки рішення EDR (XDR);
- можливість функціонування клієнт-серверу в електронних комунікаційних мережах через проксі;
- складнощі впровадження, простота розгортання та початкового конфігурування;
- складнощі у підтриманні функціонування, необхідність у додатковому навчанні персоналу;

- наявність дозволу Державної служби спеціального зв'язку та захисту інформації України (далі — ДССЗЗІ України);
- підтримка зовнішнім SOC;
- якість та швидкість реагування технічної підтримки виробника рішення EDR (XDR).

Під час перевірки можливостей інсталяції, видалення та роботи в системі перевіряється:

- інсталяція через командний рядок;
- наявність інсталяції через графічний інтерфейс користувача та легкість даної інсталяції;
- захист від несанкціонованого видалення агента користувачем;
- можливість віддаленого видалення агента за допомогою консолі;
- авторизоване видалення агента власноруч користувачем;
- підтримка операційної системи;
- швидкість і безпроблемність з'єднання нововстановленого агента з консоллю;
- можливість паралельної роботи з антивірусним програмним забезпеченням, що встановлене (далі — АВПЗ);
- конфігурування інсталяційного пакету специфічними параметрами;
- прийнятні системні вимоги до кінцевого пристрою;
- навантаження на кінцевий пристрій на яке встановлено дане рішення в момент «простою» та під час збору даних чи реагування на інцидент;
- сумісність роботи з налаштованими локальними політиками безпеки.

Під час конфігурування, редагування політик та правил перевіряється:

- наявність правил та політик за замовчуванням;
- створення, редагування політик безпеки (правил детектування);
- наявність мінімального набору правил детектування DNS, IP, URL, HASH, File Name, File Path;
- наявність бази даних сигнатур та її оновлення;
- зменшення використання ресурсів;
- можливість налаштування різних політик для різних груп агентів;
- інтеграція з відповідною Security information and event management (далі — SIEM);
- наявність журналу аудиту, у якому повинно відстежуватись і реєструватись всі зміни в конфігурації та всі дії, які виконуються користувачами;
- необхідність використання сторонніх програм для роботи агентів.

Під час перевірки можливостей та функцій консолі перевіряється:

- можливість розподілення агентів по відповідним групам або ж тегам;
- наявність диспетчера користувачів, який дозволяє створювати різних користувачів сервера адміністрування та призначати їм різні права доступу до окремих розділів, груп комп'ютерів;
- список заблокованих EXE/DLL та інших файлів з можливістю їх відновлення у разі неправдивого спрацювання;
- можливість визначення статусу хосту, системної інформації, дати встановлення та останнього підключення агенту;
- простота використання, зручність графічного інтерфейсу для адміністрування;
- наявність аналітичних звітів;
- наявність вбудованого функціоналу для аналізу Triage безпосередньо в консолі.

Під час перевірки питань менеджменту індикаторів загроз, виявлення, реагування та блокування загроз перевіряється:

- ізоляція від мережі;
- доступ девайс менеджера (тобто список підключених флеш носіїв);
- віддалений доступ до кінцевого приристрою;
- блокування файлів (хешів, назв тощо);
- можливість рішень EDR (XDR) забезпечувати автоматичне (по запиту) блокування процесів, які визначені як шкідливі;
- можливість перевірки аномалій у файловій системі;
- виявлення виконання специфічних та невідповідних команд на системі;
- можливість виявлення додавання/видалення нових правил до host-based firewall;
- наявність функції сканування флеш-носіїв на наявність ШПЗ;
- можливість створення білих/чорних списків EXE/DLL файлів;
- можливість переміщення в карантин виявленого ШПЗ.

Під час перевірки можливостей здійснення аналізу та збору даних перевіряється:

- загальна інформація про систему (system information);
- завантаження набору даних Triage;
- завантаження окремого файлу;
- завантаження декількох файлів/папок;
- розумне сортування даних Triage (наприклад Persistence);
- перегляд основних ключів реєстру;
- можливість перевірки та відображення запланованих завдань;
- перегляд процесів;
- перегляд сервісів;
- перегляд файлової системи ($MFT);
- перегляд Event Logs;
- перегляд IPv4\IPv6 (мережевих) подій, активності;
- перегляд Internet History, Form History;
- можливість створення кастомних наборів даних;
- відображення даних в реальному часі та їх аналіз;
- можливість перевірки файлів prefetch;
- можливість перевірки jump list (історія дії користувача на комп’ютері, яка може включати відкриті файли, програми та операції);
- можливість перевірки списку програм чи задач, які були додані до автозавантаження;
- можливість перегляду детальної інформації про виявлений файлів чи процесів;
- можливість перевірки налаштованих політик безпеки та внесення змін до них;
- повнота зібраних даних по інциденту;
- можливість дослідження ШПЗ, яке знаходиться в карантині.

Під час перевірки додаткових функцій та модулів перевіряється:

- сповіщення користувача про ізоляцію/блокування;
- кастомні сповіщення користувача;
- завантаження логів агенту;
- можливість виконання додаткових команд/скриптів на робочих місцях з встановленим агентом;
- наявність спеціального компоненту, що здійснює виявлення незахищених АРМ у мережі за допомогою АРМ, на яких вже встановлено агент EDR;

– можливість віддаленої активації агенту та відображення використаних ліцензій;
– можливість використовувати двофакторну автентифікацію для облікових записів адміністраторів;
– наявність whitelists при ізоляції хосту.

Після проведення тестування за переліченими вище методиками тестування можливостей програмних рішень EDR (XDR) необхідно здійснити оцінку результатів тестування. Здійснюється оцінка результатів (окремо по кожному рішенню EDR (XDR) для кожної операційної системи) та їх порівняльний аналіз за балами та коефіцієнтами.

Кожна технічна функція (можливість) що перевіряється оцінюється наступним чином:

– виконується повністю — 2 бали;
– виконується частково — 1 бал;
– не виконується — 0 балів;
– «-» — дана функціональність відсутня.

Ступінь критичності технічної функції (можливості) визначається коефіцієнтами наступним чином:

– критична/critical — коефіцієнт 1 (К1);
– висока/high — коефіцієнт 0,8 (К2);
– середня/normal — коефіцієнт 0,5 (К3);
– низька/low — коефіцієнт 0,2 (К4).

Оцінка відповідності технічним вимогам (Коефіцієнт ефективності К_ефективності) програмних рішень EDR (XDR) для кожної операційної системи розраховується за формулою 1:

$$К_{ефективності} = n \times \left(\sum_{критична} \times К_1 + \sum_{висока} \times К_2 + \sum_{середня} \times К_3 + \sum_{низька} \times К_4 \right) \quad (1)$$

де, n — часткова доля кінцевих пристроїв з відповідною операційною системою із загальною кількістю кінцевих пристроїв в цілому. Для серверних систем, у зв'язку з критичністю сервісів, що надаються n=1.

$\sum$ критична — це загальна кількість балів по функціях з позначкою критична;
$\sum$ висока — це загальна кількість балів по функціях з позначкою висока;
$\sum$ середня — це загальна кількість балів по функціях з позначкою середня;
$\sum$ низька — це загальна кількість балів по функціях з позначкою низька.

Розрахунок сумарного коефіцієнта ефективності К_Σ для кожного програмного рішення проводимо за формулою 2:

$$К_Σ = К_{еф1} + К_{еф2} + \ldots + К_{ефn} \quad (2)$$

де, $К_{еф1}$ — $К_{ефn}$ — це коефіцієнти ефективності рішення EDR (XDR) для відповідних операційних систем (наприклад $К_{еф1}$ — операційна система Windows 10 Pro, $К_{еф2}$ — операційна система Windows 11 $К_{ефn}$ — n операційна система).

За результатами тестування відпрацьовуються Звіт, в якому надаються конкретні пропозиції щодо вибору найбільш доцільного рішення EDR (XDR) для застосування на кінцевих пристроях із врахуванням результатів практичного тестування, організаційно-фінансових питань та наявності експертного висновку ДССЗЗІ України.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Використання запропонованої в статті методики тестування можливостей програмних рішень EDR (XDR), наддасть можливість адміністраторам безпеки а також аналітикам SOC здійснити підбір найбільш доцільного рішення EDR (XDR) для захисту кінцевих пристроїв, що працюють в ІКС та ЕКМ.

Подальшими дослідженнями є проведення практичного відповідно до зазначеної методики тестувань можливостей програмних рішень EDR (XDR) FireEye (Trellix) Endpoint Agent HX, Sentinel One Singularity XDR, Cisco Secure Endpoint, ESET Inspect, Crowd Strike Falconпрограм на операційних системах Windows 10 Pro; Windows 11; Windows Server 2022, що встановлені на кінцевих пристроях [6].

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

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Overview of endpoint detection and response.* (n. d.). https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-endpoint-detection-response?view=o365-worldwide
2. Oleksenko, V., Shtonda, R., Chernish, Y., & Maltseva, I. (2022). Modern approaches to providing cyber security in radio relay communication lines. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 1(17),* 57–64. https://doi.org/10.28925/2663-4023.2022.17.5764
3. Shtonda, R., Chernish, Y., Maltseva, I., Tsykalo, Y., Chaika, Y., & Polishchuk, S. (2023). Practical approaches to cyber protection of mobile devices with the help of a solution endpoint detection and response. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 1(21),* 17–31. https://doi.org/10.28925/2663-4023.2023.21.1731
4. [Shtonda, R. M., Ostapchuk, V. M., & Radzivilov, H. D. (2023). Using the Endpoint Detection and Response solution for cyber defence of mobile devices. *Cyber warfare: intelligence, protection and counteraction: Proceedings of the First International Scientific and Practical Conference*.
5. Shtonda, R.M., & Chaika, Ye. I. (2023). Cybersecurity of mobile devices using Endpoint Detection and Response solution. *Information Technologies in Culture, Art, Education, Science, Economics and Business: Materials of the VIII International Scientific and Practical Conference*, 94–95.
6. Shtonda, R. M, Tereshchenko, T. P., Chernysh, Yu. O., & Maltseva, I. R. (2023). Investigation of the capabilities of the CrowdStrike Falcon platform to provide cyber security for endpoint devices. *Principles of Science. Ideals, Norms, Values in Science and Style of Scientific Thinking: XVI International Scientific and Practical Conference,* 20–22.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

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

Oleksii Cherednychenko
Senior Researcher
Kruty Heroes Military Institute of Telecommunications and Information Technology
Kyiv, Ukraine
ORCID ID: 0000-0002-0816-8321
oleksiy.cherednychenko@viti.edu.ua

Denys Fomkin
Research Scientist
Kruty Heroes Military Institute of Telecommunications and Information Technology
Kyiv, Ukraine
ORCID ID: 0000-0003-0128-9355
denys.fomkin@viti.edu.ua

Olena Bokii
Research Scientist
Kruty Heroes Military Institute of Telecommunications and Information Technology
Kyiv, Ukraine
ORCID ID: 0009-0006-3459-5665
olenabokiy1971@gmail.com

Pavlo Kutsaiev
Junior Research Scientist
Kruty Heroes Military Institute of Telecommunications and Information Technology
Kyiv, Ukraine
ORCID ID: 0000-0002-3235-3316
pavlo.kutsayev@viti.edu.ua

METHODOLOGY FOR TESTING THE CAPABILITIES OF SOFTWARE SOLUTIONS ENDPOINT DETECTION AND RESPONSE (EXTENDED DETECTION AND RESPONSE)

Abstract. In the conditions of modern cyberspace, Endpoint Detection and Response (Extended Detection and Response) software solutions are the key to cyber protection. These solutions play a key role in the cyber protection of end devices operating in information and communication systems and electronic communication networks. However, the effectiveness of these solutions can vary significantly. That is why a comprehensive approach to testing their capabilities is necessary, which will allow them to be effectively evaluated. This article discusses the methodology for testing the capabilities of Endpoint Detection and Response (Extended Detection and Response) software solutions. Testing Endpoint Detection and Response (Extended Detection and Response) software solutions is carried out according to the following methods proposed by the authors of the article: checking organizational issues; checking the capabilities of installation, removal, and operation in the system; checking the configuration, editing of policies and rules; checking console functions; checking the management of threat indicators, detection, response and blocking of threats; checking the capabilities of analysis and data collection; verification of additional functions and modules. After testing using the listed methods, it is necessary to evaluate the test results. This evaluation of the results is carried out separately for each Endpoint Detection and Response (Extended Detection and Response) software solution for each operating system and their comparative analysis by points and coefficients. Based on the testing results, a report is prepared, which provides specific proposals for choosing the most appropriate software solution for use on end devices, taking into account the

results of practical testing, organizational and financial issues, and the availability of an expert opinion from the State Service for Special Communications and Information Protection of Ukraine.

Keywords: cyberattacks; cybersecurity; cyberdefense; cyberincidents; endpoint; solutions.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *Overview of endpoint detection and response*. (n. d.). https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-endpoint-detection-response?view=o365-worldwide
2. Oleksenko, V., Shtonda, R., Chernish, Y., & Maltseva, I. (2022). Modern approaches to providing cyber security in radio relay communication lines. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 1(17),* 57–64. https://doi.org/10.28925/2663-4023.2022.17.5764
3. Shtonda, R., Chernish, Y., Maltseva, I., Tsykalo, Y., Chaika, Y., & Polishchuk, S. (2023). Practical approaches to cyber protection of mobile devices with the help of a solution endpoint detection and response. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 1(21),* 17–31. https://doi.org/10.28925/2663-4023.2023.21.1731
4. [Shtonda, R. M., Ostapchuk, V. M., & Radzivilov, H. D. (2023). Using the Endpoint Detection and Response solution for cyber defence of mobile devices. *Cyber warfare: intelligence, protection and counteraction: Proceedings of the First International Scientific and Practical Conference*.
5. Shtonda, R.M., & Chaika, Ye. I. (2023). Cybersecurity of mobile devices using Endpoint Detection and Response solution. *Information Technologies in Culture, Art, Education, Science, Economics and Business: Materials of the VIII International Scientific and Practical Conference,* 94–95.
6. Shtonda, R. M, Tereshchenko, T. P., Chernysh, Yu. O., & Maltseva, I. R. (2023). Investigation of the capabilities of the CrowdStrike Falcon platform to provide cyber security for endpoint devices. *Principles of Science. Ideals, Norms, Values in Science and Style of Scientific Thinking: XVI International Scientific and Practical Conference,* 20–22.