# ВИКОРИСТАННЯ СИСТЕМ EDR ДЛЯ ПРОТИДІЇ ШКІДЛИВОМУ ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННЮ

Сєвєрінов О.В., Балагура Д.С., Семенова К.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Кіберінциденти з атаками на інформаційні системи українського бізнесу показала, що класичні способи захисту виявляються безсилими проти шкідливого програмного забезпечення, нових вірусів, особливо вірусів-шифрувальників.

**Метою доповіді** є аналіз нових рішень виявлення та реагування на сучасні загрози кінцевим точкам (EDR).

Виявлення та реагування на загрози кінцевим точкам (EDR) - це основний спосіб забезпечення кібербезпеки, який масово використовується на сьогодні [1-3].

EDR пропонується як ідеальна відповідь на швидкозмінну ситуацію загроз, з якою до того часу боролися, насамперед, за допомогою AV-рішень. Ці загрози включали експлойти, шкідливе програмне забезпечення нульового дня та безфайлові атаки.

Попри те, що на сьогодні, традиційні EDR визнано досить ефективним проти багатьох передових загроз, існує нова та покращена категорія рішень "EDR наступного покоління". Окрім звичайних можливостей нове покоління включає додатковий рівень захисту від основних векторів атак (таких як користувачі та мережі) [1-3].

Щоразу, коли зловмисник виявляє активність, виникає аномалія в інформаційній системі. Це основне припущення, яке потрібно взяти до уваги, бо дії, спрямовані на компрометацію даних та ресурсів, не є звичайною діяльністю. Можливість ідентифікувати ці дії - це те, що дозволяє програмним та програмно-апаратним рішенням безпеки та аналітикам загроз ідентифікувати та заблокувати атаку.

Ці аномалії відбуваються в трьох основних місцях: виконання процесів, мережевий трафік або активність користувачів. EDR чудово справляється із цією задачею, оскільки знаходиться на кінцевій точці та контролює поведінку процесу. Це означає, що організація отримує надійний захист від таких видів загроз. Але мережевий трафік та поведінка користувачів також є критичними областями, і основні вектори можуть працювати там, не викликаючи жодних ознак аномалій. EDR майже повністю сліпий до таких видів загроз [4].

Більшість зловмисників, з часом, стають все далі просунутими в підборі сценаріїв, і одна з речей, на яку вони звертають увагу, це те, які заходи захисту застосовуються.

Для протидії цим загрозам необхідно використовувати EDR нового покоління NG EDR, яка є комплексною системою з набором технологій, призначених для моніторингу, зображення і зберігання даних, які відстежують всі дії, що відбуваються в кінцевих точках. Ці дані збираються в

централізованому сховищі, де аналізуються. Захист проводиться в реальному часі, і якщо в процесі аналізу EDR виявить в якійсь із точок ознаки злому, автоматично починають використовуватися можливості швидкого реагування, а після усунення загрози відбувається відновлення до безпечних параметрів функціонування.

Основною метою NG EDR є ефективно та постійно захищати дані та інформаційні системи кінцевого користувача від шкідливого програмного забезпечення.

В роботі отримані результати порівняльного аналізу рішень класу виявлення та реагування на загрози на кінцеві точки наступного покоління (NG EDR) та традиційних антивірусів (Legacy AV) [5].

Включення NG EDR в організаційну архітектуру безпеки розширює можливості виявлення, реагування та відновлення після інцидентів кібернетичного характеру.

Таким чином, враховуючі стрімкий розвиток індустрії розробки шкідливого програмного забезпечення як в комерційних цілях (отримання фінансової вигоди), так в політичних (підміна контенту для дискримінації уряду, кіберрозвідка, кібервійна тощо) можна зробити висновки про необхідність використання передових технологій для захисту кінцевих точок в інформаційних системах з використанням NG EDR.

Цей проактивний підхід дозволяє організаціям нейтралізувати потенційні загрози ще до того, як вони зможуть скористатися наявними вразливими місцями, що значно покращує їхні позиції у сфері безпеки. Це дасть змогу протистояти новим викликам кіберагресії по відношенню не тільки користувача, але і держави в цілому.

**Список літератури**

1. What You Need to Know About Next Gen EDR. URL: https://threatpost.com/next-gen-edr/148626/

2. Баклан Я.А., Сєвєрінов О.В. Аналіз систем захисту кінцевих точок від складних загроз EDR (Endpoint Detection and Response) // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: матеріали дванадцятої міжнар. наук.-практ. конф. 2022. Баку–Харків–Жиліна.

3. Шуліка, К., Балагура, Д., Смірнов, А., Непокритов, Д., Литвин, А. (2024) «Метод використання сучасних систем захисту кінцевих точок (EDR) для убезпечення від комплексних атак», *Сучасний стан наукових досліджень та технологій в промисловості*, (2(28), с. 182–195. doi: 10.30837/2522-9818.2024.2.182.

4. Шуліка, К., Балагура, Д., Сидоренко, З. (2024). Аналіз методів обходу сучасних систем захисту кінцевих точок EDR. *Радіотехніка*, *2*(217), 64–68. https://doi.org/10.30837/rt.2024.2.217.05.

5. What is Next Generation Endpoint Security? URL: https://www.sentinelone.com/cybersecurity-101/endpoint-security/next-generation-endpoint-security/