УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.120

ЕФЕКТИВНІСТЬ ТА МАЙБУТНІЙ РОЗВИТОК СИСТЕМ ЗБОРУ МЕРЕЖЕВИХ АРТЕФАКТІВ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

Малахова А. А.
Науковий керівник – Євгеньєв А. М.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
email: anna.malakhova@nure.ua

This report explores the current state, effectiveness, and future development prospects of network artifact collection systems, focusing on their role in cybersecurity. It highlights the importance of evolving these systems to cope with the increasing complexity of cyber threats in our digital world. The discussion encompasses the current landscape of network artifact collection methods, their limitations, and the potential for future improvements. Emphasis is placed on innovative approaches such as automation, artificial intelligence integration, and blockchain technology to enhance the efficiency of these systems. The report concludes by underscoring the necessity of continued research and investment in advancing these technologies to ensure robust cybersecurity measures.

У сучасному цифровому світі, де мережева активність постійно зростає, а загрози кібербезпеки стають все складнішими, ефективні системи збору мережевих артефактів відіграють важливу роль у виявленні та протидії кіберзагрозам. У цієї доповіді розглянемо сучасний стан та майбутні перспективи розвитку таких систем, а також ключові інновації, які можуть забезпечити їхню ефективність та надійність [1].

Сучасні системи збору мережевих артефактів базуються на різноманітних технологіях, включаючи сенсори, журнали подій, системи моніторингу мережевого трафіку тощо [2]. Однак, багато з цих систем мають обмежену масштабованість, низьку швидкість аналізу та виявлення аномалій, а також вимагають значних зусиль для обробки та аналізу отриманих даних.

Ефективність систем збору мережевих артефактів є ключовим аспектом в забезпеченні кібербезпеки та виявленні потенційних загроз. Ці системи відіграють важливу роль у зборі, аналізі та моніторингу мережевої активності, дозволяючи виявляти аномальні зміни та підозрілу поведінку, яка може свідчити про кібератаку або інші загрози безпеці [3].

Майбутні перспективи розвитку систем збору мережевих артефактів досить передбачувані і можуть характеризуватись такими аспектами як:

– автоматизація та інтелектуалізація: застосування штучного інтелекту та машинного навчання для автоматичного виявлення аномалій та відстеження кіберзагроз;

– розширення області застосування: розвиток систем збору мережевих артефактів для виявлення загроз у Інтернеті речей, хмарних середовищах, облікових записах користувачів та інших аспектах цифрового життя;

– безпека та конфіденційність: розробка технологій шифрування, анонімізації та захисту персональних даних для забезпечення конфіденційності та захисту інформації, зібраної системами збору мережевих артефактів.

Якщо говорити за інновації у розвитку збору мережевих артефактів, то використання блокчейн технологій і розвиток нових алгоритмів аналізу даних – це необхідні міри для забезпечення невідворотності, цілісності та автентифікації даних, зібраних системами збору мережевих артефактів, а також для виявлення найбільш складних та витончених атак, які можуть ухилятися від традиційних методів виявлення загроз [4].

Майбутній розвиток систем збору мережевих артефактів відкриває перед нами широкі перспективи для підвищення безпеки та ефективності цифрових мереж. Інновації в області штучного інтелекту, машинного навчання, блокчейн технологій та аналізу даних дозволять побудувати більш реактивні та надійні системи, які забезпечать нам захист від кіберзагроз у майбутньому. Для досягнення цілей необхідно продовжувати інвестувати в дослідження та розробки в цих напрямках, що дозволить забезпечити нам безпеку та стабільність у цифровому середовищі [5].

Список використаних джерел:

1. Arvidsson V., Mønsted T. Generating innovation potential: How digital entrepreneurs conceal, sequence, anchor, and propagate new technology. The Journal of Strategic Information Systems. 2018. Vol. 27, no. 4. P. 369–383. (дата звернення: 05.03.2024).

2. Сєвєрінов О.В., Хрєнов А.Г. Аналіз сучасних систем виявлення вторгнень. // Системи обробки інформації 6 (2014): 122-124.

3. Cybersecurity and Network Security / A. Guha et al. Wiley & Sons, Limited, John, 2022.

4. Staff J. f. A. Cybersecurity Log Book: Cybersecurity Log. Independently Published, 2017.

5. Local Network Security. Cybersecurity. Indianapolis, Indiana, 2018. P. 423–447.