УДК 004.056.53

ІННОВАЦІЙНІСТЬ У ЗАХИСТІ МЕТОДОМ ВИКОРИСТАННЯ СУЧАСНИХ ІНСТРУМЕНТІВ ДЛЯ КОНТРОЛЯ ЗА КІБЕРБЕЗПЕКОЮ

Малахова А. А.
Науковий керівник – ст. викладач Данилов А. Д.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
email: anna.malakhova@nure.ua

In the rapidly evolving landscape of cybersecurity threats, the importance of innovative approaches to protection cannot be overstated. This whitepaper explores the importance of using modern tools and techniques in cybersecurity control to effectively mitigate risks. By leveraging advanced technologies such as behavioural analytics and threat intelligence platforms, organizations can strengthen their defences against a wide range of cyber threats. This explores the various applications of these tools, from proactive threat detection to rapid incident response and remediation. By embracing innovation and leveraging modern tools for cybersecurity control, organizations can enhance their resilience against cyber attacks and safeguard their sensitive data in a digital environment.

Кібербезпека є динамічною областю, що постійно змінюється. Нові загрози з'являються з непередбачуваною швидкістю. Традиційні методи захисту вже не є достатньо ефективними. Важливо застосовувати інноваційні підходи, що ґрунтуються на використанні сучасних інструментів та методів [1].

Поведінкова аналітика, платформи розвідки загроз та швидке реагування на інциденти та усунення наслідків є важливими складовими для ефективного забезпечення кібербезпеки. Вони сприяють вчасному виявленню, аналізу та відверненню кіберзагроз, допомагаючи організаціям запобігати кібератакам та мінімізувати їхні наслідки. Поведінкова аналітика допомагає ідентифікувати аномальну активність, яка може вказувати на потенційні загрози, тоді як платформи розвідки загроз забезпечують доступ до інформації про потенційні кіберзагрози та дозволяють прогнозувати майбутні атаки. Швидке реагування на інциденти та усунення їхніх наслідків дозволяє організаціям мінімізувати час простою систем та відновити нормальну роботу якнайшвидше, зменшуючи вплив на бізнес та користувачів. Таким чином, ці складові спільно допомагають підвищити рівень захищеності від кіберзагроз та забезпечити стабільність і безпеку цифрового середовища організації.

В роботі буде розглянуто перераховані вище складові для ефективного забезпечення кібербезпеки з наведенням порівняльного аналізу [2].

Система DLP(Data Loss Prevention), як метод поведінкової аналітики займається захистом даних, моніторингом активності користувачів та захистом конфіденційності, GDPR(General Data Protection Regulation), в свою чергу система IDS(Intrusion Detection System) вирішує проблеми захисту мережі та хостів, моніторингу трафіку та журналів, і, звісно, запобігання атакам і швидке реагування на них. Ці системи потребують ретельних налаштувань та постійного моніторингу, а також їх краще використовувати з іншими інструментами кібербезпеки.

Комбінування поведінкової аналітики та платформ розвідки загроз дозволяє створити більш комплексну та ефективну систему кіберзахисту. Поєднання цих методів дозволяє організаціям отримати більш повне уявлення про загрози, з якими вони можуть стикнутися, та вчасно реагувати на них. Використання обох підходів дозволяє зменшити ризик помилкових сигналів тривоги та підвищити ефективність виявлення та запобігання кіберзагрозам. Таким чином, комбінування поведінкової аналітики та платформ розвідки загроз створює більш надійний та комплексний підхід до кіберзахисту, що дозволяє організаціям ефективніше захищати свої цифрові активи.

Платформи розвідки загроз − це централізовані системи, що збирають та аналізують інформацію про потенційні кіберзагрози з різних джерел. Вони дозволяють отримувати доступ до актуальної інформації про загрози та прогнозувати майбутні кібератаки [3].

Платформи розвідки загроз, як CheckPoint Endpoint Security та VirusTotal, стають дедалі важливішими інструментами для захисту від кібератак. Ці платформи збирають та аналізують дані про кіберзагрози з різних джерел, таких як звіти про кіберінциденти, дані про вразливості, інформація про шкідливі програми, дані про ботнети.

CheckPoint Endpoint Security та VirusTotal – це два приклади платформ розвідки загроз, які можуть взаємодіяти для покращення кібербезпеки.

CheckPoint Endpoint Security − це комплексне рішення для захисту кінцевих точок, яке використовує машинне навчання та штучний інтелект для виявлення та блокування кіберзагроз.

VirusTotal − це безкоштовна платформа, яка дозволяє користувачам сканувати файли та URL-адреси на наявність шкідливих програм. Взаємодія CheckPoint Endpoint Security та VirusTotal може покращити виявлення кіберзагроз методом поєднання даних з двох платформ, швидше реагувати на кібератаки, тому що інформація з VirusTotal може допомогти CheckPoint Endpoint Security швидше реагувати на кібератаки а також підвищити рівень кібербезпеки.

Хоча взаємодія платформ є одним із міцних способів покращити кібербезпеку, все одно важливо вживати інших заходів для захисту своїх систем та даних [4].

Ефективний план реагування на кібератаку може мінімізувати шкоду, завдану організації, тож потрібно приділити йому увагу.

Ефективний план включає в себе чотири ключових етапи: виявлення інциденту, розслідування, усунення наслідків та відновлення роботи системи після нейтралізації атаки.

Існує ряд інструментів, які можуть допомогти у реагуванні на кібератаки: SOAR (Security Orchestration, Automation, and Response) та Playbooks.

Системи автоматизованого реагування на інциденти (SOAR) автоматизують рутинні завдання, пов'язані з реагуванням на кібератаки, що може значно економити час.

Playbooks – це документи, які описують дії, які потрібно виконати у разі кібератаки.

Наприклад, платформа розвідки загроз може виявити нову кіберзагрозу. Ця інформація може бути використана для оновлення Playbook для реагування на інциденти, щоб організація була готова до цієї кібератаки.

Швидке реагування на кібератаки є важливим для мінімізації шкоди, завданої організації. Для покращеного результату рекомендується використовувати платформи розвідки загроз та поведінкову аналітику у комбінації з цими інструментами.

Список використаних джерел:

1. A Large Scale Study and Classification of VirusTotal Reports on Phishing and Malware URLs / E. Choo та ін. Proceedings of the ACM on Measurement and Analysis of Computing Systems. 2023. Т. 7, № 3. С. 1–26. URL:https://doi.org/10.1145/3626790(дата звернення: 01.03.2024).

2. CheckPoint Endpoint Security.URL:https://www.checkpoint.com/ (дата звернення: 01.03.2024).

3. I. T. Security Risk Manager. Information Security Program Guide: Company Policies, Departmental Procedures, IT Standards and Guidelines. Independently Published, 2019.

4. Tsukerman E. Objective Selection for NGIDS. Designing a Machine Learning IDS. Berkeley, CA, 2020. URL: https://doi.org/10.1007/978-1-4842-6591-8_6 (дата звернення: 01.03.2024).