The research presented in this paper contributes to the field of information communication and offers practical implications for the planning and development of new network connections. Specifically, the method's applicability extends to various network architectures, including corporate intranets and extranets, where ensuring secure communication is paramount.

References

Ibraim DIDMANIDZE, Mikheil DONADZE, Besik BERIDZE, Zebur BERIDZE, Didar DIDMANIDZE, Tengiz DIDMANIDZE. Development of Secure Routing Algorithms in Computer Networks. CHALLENGES TO NATIONAL DEFENCE IN CONTEMPORARY GEOPOLITICAL SITUATION CNDCGS'2024. PROCEEDINGS OF THE 4th INTERNATIONAL SCIENTIFIC CONFERENCE. 11 – 13 September 2024 Brno, Czech Republic. P. 331-340.
ISSN 2538-8959 (online)

https://1drv.ms/b/s!Amo3hJPYM9ezjeZ0d5GCpwgpeOV1KQ

АВТОМАТИЗОВАНІ СИСТЕМИ АНАЛІЗУ, ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ЗЛОВМИСНОЇ МЕРЕЖЕВОЇ АКТИВНОСТІ / AUTOMATED SYSTEMS FOR ANALYZING, DETECTING AND PREVENTING MALICIOUS NETWORK ACTIVITY

Я.І.Вознюк, О.М Вознюк/ Y.I.Vozniuk O.M. Vozniuk
Національний університет Києво-Могилянська Академія
04655, м. Київ, вулиця Григорія Сковороди, 2, НаУКМА, Факультет інформатики, Кафедра інформатики / National University of Kyiv-Mohyla Academy
04655, Kyiv, Skovoroda Street, 2, NaUKMA, Faculty of Informatics, Department of Informatics
Контактні телефони: +38 067 791 59 12
E-mail: vozniuck@ukma.edu.ua

The study presents ways of integrating free and shareware IDS/IPS solutions with ML/AI approaches, which allow you to effectively adapt security systems to the dynamic conditions of modern cyberspace. Further research will focus on automating signature adaptation, leveraging deep neural networks, federated learning, as well as active learning to respond more accurately and quickly to cyber threats.

Зростання складності мережевих інфраструктур, перехід на хмарні платформи, розвиток концепцій Інтернету речей (IoT) та промислового Інтернету речей (IIoT) створюють нові напрямки атак. Класичні сигнатурні системи виявлення загроз поступово втрачають ефективність, оскільки зловмисники використовують складні, багатокрокові та малопомітні техніки, які не завжди можна розпізнати за заздалегідь відомими зразками. Сучасні підходи, які включають поведінковий аналіз, машинне навчання (ML) та штучний інтелект (AI), мають на меті підвищити точність, адаптивність і масштабованість систем виявлення та запобігання вторгненням (IDS/IPS) [1–3, 10].

Передусім доступність безкоштовних та умовно-безкоштовних інструментів (наприклад, Snort, Suricata, Zeek, Wazuh, Security Onion) дозволяє організаціям різного масштабу впроваджувати сучасні рішення без надмірних витрат [4–8].

Метою нашого дослідження був аналіз безкоштовних та умовно-безкоштовних IDS/IPS рішень, що можуть бути інтегровані із технологіями ML/AI. На основі аналізу публікацій та сучасних практик ми виробили набір рекомендацій щодо впровадження згаданих інструментів та окремих методик виявлення втручань у реальних мережевих середовищах.

Коротко охарактеризуємо обраний інстументарій:

- **Snort**: Класичний сигнатурний IDS з великою спільнотою та розгалуженою базою правил, ефективний для відомих патернів загроз [4].
- **Suricata**: Висока продуктивність, паралельна обробка трафіку, підтримка сигнатурних та аномалійних підходів, активна інтеграція з ML-пайплайнами [5].

- **Zeek (Bro)**: Аналізатор мережевого трафіку з акцентом на поведінковий аналіз та логічне представлення даних, що дозволяє зручно застосовувати ML для виявлення аномалій [6].

- **Wazuh**: Інтегрована платформа безпеки з елементами SIEM, контролем конфігурацій, аналізом журналів і можливістю впровадження ML-моделей для аналізу подій та кореляції загроз [7].

- **Security Onion**: Комплексне рішення, що об'єднує Snort, Suricata, Zeek та інші інструменти в єдину платформу. Легко інтегрується з ML/AI-стеками (ELK Stack,

Зазначимо, що сучасні дослідження акцентують увагу на побудові гібридних ML-моделей, які поєднують сигнатурні та поведінкові характеристики [1–3, 9].

Проведений аналіз демонструє, що поєднання відкритих інструментів (Snort, Suricata, Zeek, Wazuh) з ML/AI дозволяє створити продуктивні, гнучкі та масштабовані IDS/IPS системи для різних категорій організацій. Це дає змогу мінімізувати витрати, підвищити ефективність, гнучкість у протидії новим загрозам та оптимізувати роботу аналітиків безпеки. Серед сучасних підходів у виявленні загроз варто відзначити: сигнатурні методи, поведінковий аналіз, кореляція подій та інтеграція даних. Ми також виділили такі найбільш ефективні методології реалізації: впровадження ML через ELK Stack (Elasticsearch, Logstash, Kibana) та інтеграція з Wazuh, Zeek для централізованого збору даних та обробки [7, 8]; використання TheHive та Cortex для оркестрації аналітики та застосування ML/AI-сервісів у реальному часі; застосування глибинних нейронних мереж для складних сценаріїв поведінкового аналізу та виявлення складних стійких загроз (APT) [2, 3].

На наш погляд, найбільш прийнятними є наступні методики впровадження рішень: поетапне впровадження Snort/Suricata/Zeek із поступовою інтеграцією у Wazuh чи Security Onion, адаптація до вимог конкретного середовища [4–8] (модульність та масштабованість); використання ML для автоматичного оновлення сигнатурного набору та поведінкових профілів на основі нових зразків атак [1–3] (адаптивність правил); побудова інфраструктури, де вхідні дані (трафік, логи, події) у режимі реального часу перетворюються, агрегуються та аналізуються ML-моделями з подальшим виведенням індикаторів компрометації для автоматичного чи напівавтоматичного реагування [7, 9] (інтеграція з AI/ML-конвеєром).

Використані джерела:

1. Roy, A., Nourbakhsh, H., & Mashatan, A. (2022). "A Hybrid Deep Learning Model for Network Intrusion Detection and Classification." *Computers & Security*, 113:102552.

2. Zhang, J., Yu, C., Ning, X. et al. (2020). "Building an Effective Intrusion Detection System by Using Hybrid Machine Learning and Ensemble Approach." *IEEE Access*, 8, 170400–170411.

3. Kundari, G., Shakya, S., & Merigó, J.M. (2021). "Deep Reinforcement Learning for Intrusion Detection in Cyber-Physical Systems." *Sensors*, 21(14).

4. Roesch, M. & Green, C. (2013). "Snort Users Manual." *Snort Project*. [Online]. Available: https://www.snort.org/

5. The OISF (Open Information Security Foundation). "Suricata." [Online]. Available: https://suricata-ids.org/

6. Zeek Network Security Monitor. [Online]. Available: https://zeek.org/

7. Wazuh Documentation. [Online]. Available: https://wazuh.com/

8. Security Onion Solutions. [Online]. Available: https://securityonion.net/

9. Milenkoski, A., Vieira, M., Koutroumpouchos, N. et al. (2021). "A Systematic Evaluation of Intrusion Detection Systems via Attack Injection." *IEEE Transactions on Network and Service Management*, 18(1).

10. Salama, M.A., Ezz, M., Mohamed, S.A., et al. (2023). “A Federated Learning-Based Framework for Intrusion Detection in IoT Networks.” *IEEE Internet of Things Journal*, Early Access.

ІНТЕГРАЦІЯ КІБЕРПОЛІГОНІВ В ОСВІТНІЙ ПРОЦЕС / INTEGRATION OF CYBER RANGES INTO THE EDUCATIONAL PROCESS

А.М. Глибовець, Т.А. Бабич / Hlybovets A.M., Babych T.A.
Національний університет Києво-Могилянська Академія
04655, м. Київ, вулиця Григорія Сковороди, 2, НаУКМА, Факультет інформатики, Кафедра інформатики / National University of Kyiv-Mohyla Academy
04655, Kyiv, Skovoroda Street, 2, NaUKMA, Faculty of Informatics, Department of Informatics
Контактні телефони: +38 093 793 94 54
E-mail: t.babich@ukma.edu.ua

The article highlights the theoretical foundations of cyber ranges, including an overview of the main technologies and techniques used to create virtualized cyber environments. Examples of the introduction of cyber ranges into the curriculum of higher education institutions, their impact on student motivation, as well as teaching and assessment methods using these complexes are considered. Further, the article focuses on the practical aspects of using cyber polygons in the educational process on the development and adaptation of cyber polygons for educational purposes. The article also discusses safety and ethical issues related to the use of cyber training grounds in education, as well as legal aspects of their use. Particular attention is given to the analysis of case studies of successful use of cyber training grounds, which demonstrate a significant increase in the level of student training.

Сучасний світ стає дедалі більш цифровим, що спричиняє зростання потреби в захисті кіберпростору. З кожним роком кількість кібератак зростає, що підкреслює необхідність підготовки кваліфікованих фахівців у галузі кібербезпеки. Злочинці стають дедалі винахідливішими у своїх методах, а тому методи захисту мають еволюціонувати ще швидше. Враховуючи це, розуміння та застосування передових практик і технологій в галузі кібербезпеки є критично важливим для захисту особистих, корпоративних та державних інтересів.

Кіберполігон — це спеціалізоване віртуалізоване середовище, призначене для моделювання кібернетичних загроз та атак, що дозволяє користувачам в безпечний спосіб відпрацьовувати реакції на них. Це середовище імітує реальну IT-інфраструктуру з усіма її компонентами, включаючи мережі, сервери та застосунки, дозволяючи таким чином відтворювати атаки і тестувати оборонні механізми без ризику для реальних систем. В освіті кіберполігони використовуються для підготовки студентів, забезпечуючи їм можливість здобути практичний досвід у виявленні, аналізі та відповіді на кіберзагрози. Особливо важливою є роль кіберполігонів у формуванні навичок роботи в команді та розвитку стратегічного мислення, що є критично важливими компетенціями для майбутніх фахівців кібербезпеки.

Інтеграція кіберполігонів у освітній процес вищих навчальних закладів може забезпечити значний прогрес у підготовці фахівців у галузі кібербезпеки [13]. Кіберполігони дозволяють студентам здобувати практичний досвід в ідентифікації, аналізі та відповіді на кіберзагрози в контрольованому і безпечному середовищі. Це допомагає не лише у формуванні технічних навичок, але й розвиває критичне мислення, необхідне для ефективного реагування на інциденти в реальному світі.

Збільшення кількості кіберзагроз, їхнє постійне ускладнення та висока динаміка розвитку кібератак вимагають від освітніх закладів включення інноваційних підходів до навчання. Інтеграція кіберполігонів у освітні процеси є актуальною, оскільки вона дозволяє забезпечити студентам доступ до практичного досвіду [8], що є незамінним в підготовці кваліфікованих фахівців. Практика на кіберполігоні допомагає студентам краще зрозуміти реальні кіберзагрози, відточити свої навички реагування на інциденти та розвинути здатність адаптуватися до мінливого кіберландшафту. Це також створює умови для реалізації прикладного навчання, забезпечуючи студентам розуміння теоретичних знань у практичних реальних ситуаціях [12]. Кіберполігони використовують низку технологій і методологій для створення реалістичних умов, що дозволяють користувачам відпрацьовувати відповіді на кіберзагрози [10].