розгорнута система моніторингу успішно зафіксувала спробу атаки, а також коректно визначила час її виникнення.

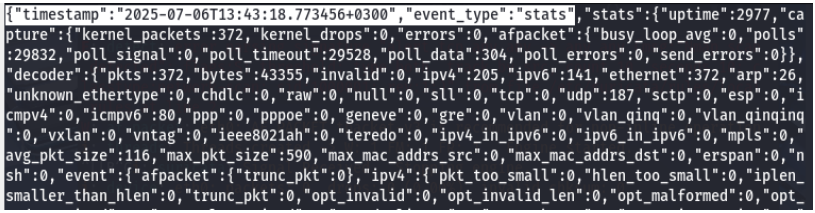
{"timestamp":"2025-07-06T13:43:18.773456+0300","event_type":"stats","stats":{"uptime":2977,"capture":{"kernel_packets":372,"kernel_drops":0,"errors":0,"afpacket":{"busy_loop_avg":0,"polls":29832,"poll_signal":0,"poll_timeout":29528,"poll_data":304,"poll_errors":0,"send_errors":0}},"decoder":{"pkts":372,"bytes":43355,"invalid":0,"ipv4":205,"ipv6":141,"ethernet":372,"arp":26,"unknown_ethertype":0,"chdlc":0,"raw":0,"null":0,"sll":0,"tcp":0,"udp":187,"sctp":0,"esp":0,"icmpv4":0,"icmpv6":80,"ppp":0,"pppoe":0,"geneve":0,"gre":0,"vlan":0,"vlan_qinq":0,"vlan_qinqinq":0,"vxlan":0,"vntag":0,"ieee8021ah":0,"teredo":0,"ipv4_in_ipv6":0,"ipv6_in_ipv6":0,"mpls":0,"avg_pkt_size":116,"max_pkt_size":590,"max_mac_addrs_src":0,"max_mac_addrs_dst":0,"erspan":0,"nsh":0,"event":{"afpacket":{"trunc_pkt":0},"ipv4":{"pkt_too_small":0,"hlen_too_small":0,"iplen_smaller_than_hlen":0,"trunc_pkt":0,"opt_invalid":0,"opt_invalid_len":0,"opt_malformed":0,"opt_

Рис.1. Результати тестування системи моніторингу

В межах роботи написано скрипт для аналізу лог-файлів системи. Захист журналів включає контроль цілісності, резервне копіювання та виявлення несанкціонованих змін, оскільки вони є критичним джерелом інформації про інциденти безпеки. Водночас ефективність такого захисту забезпечується поєднанням автоматизованих засобів, контролю доступу та моніторингу.

У результаті розроблено гнучку та ефективну систему моніторингу безпеки VPN-з'єднання на базі WireGuard, придатну як для забезпечення віддаленого доступу до корпоративних ресурсів, так і для освітніх і дослідницьких цілей у сфері мережевої безпеки. Результати тестування підтверджують здатність системи збирати інформацію про VPN-клієнтів, автоматично виявляти підозрілу активність і своєчасно ідентифікувати потенційні загрози.

1. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T. (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, 1-11.
2. Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote iot system management by integrating firewall configuration into tunneled traffic. Вісник Тернопільського національного технічного університету, 115(3), 122-129.

Ідентифікація STRIDE загроз та пріоритизація засобів захисту SSDF для CI/CD процесів

УДК 004.056+ 004.415

Тарас Лобур[1], Руслан Козак[2]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]taras.lobur@tntu.edu.ua, [2]ruslank@tntu.edu.ua

Галузь IT широко використовує практики DevOps (Development and Operations) і CI/CD (Continuous Integration / Continuous Delivery), які забезпечують безперервну інтеграцію коду, автоматизоване тестування та швидке розгортання продуктів. Однак із ростом рівня автоматизації наслідки потенційних кіберзагроз стають масштабними [1]. Попри значну кількість досліджень, присвячених DevSecOps, CI/CD та інтеграції безпеки в життєвий цикл розробки [2, 3, 4], аналіз вказує на відсутність праць, у яких здійснювалася

б формалізована ідентифікація та пріоритезація засобів захисту відносно специфічних для CI/CD загроз.

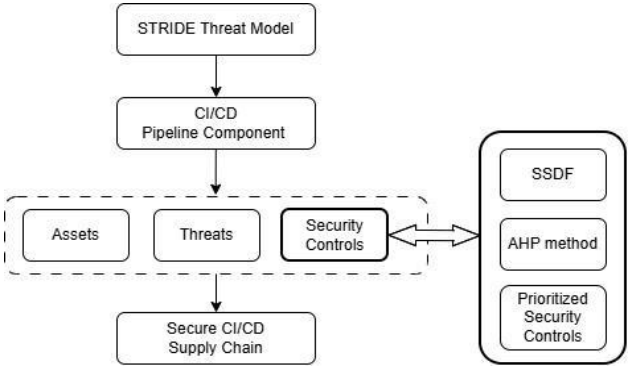

Рис.1. Схема запропонованого підходу для пріоритезації засобів захисту

Для ідентифікації засобів захисту CI/CD було використано NIST Secure Software Development Framework (SSDF) методологію, оскільки вона забезпечує орієнтовані на життєвий цикл практики, що відповідають DevSecOps, та STRIDE методологію, яка пропонує структуровану таксономію для виявлення ризиків у таких середовищах. Разом обидві методології утворюють взаємодоповнюючий підхід, який інтегрує дієві засоби контролю із систематичним моделюванням загроз (Рис. 1).

Конвеєри (CI/CD) стали незамінними в розробці програмного забезпечення, однак автоматизація та взаємозв'язок цих конвеєрів створюють нові вектори атак. Без систематичного моделювання загроз існує ризик пропустити вразливості, які можуть швидко поширюватися по всьому ланцюжку постачання програмного забезпечення. Щоб вирішити цю проблему, було застосовано методологію STRIDE, яка пропонує структуровану таксономію загроз, яку можна відобразити на робочі процеси CI/CD (Рис. 2). Визначення найважливіших категорій в рамках STRIDE, дало змогу визначити пріоритетність засобів захисту та узгодити їх із методами розробки, що визначені в NIST Secure Software Development Framework (SSDF).

Серед шести категорій STRIDE виявлено три, які є визначальними в контексті CI/CD: підробка коду та артефактів, підміна сутності та розкриття інформації. Підробка коду та артефактів є одним з найпоширеніших векторів атак в автоматизованих конвеєрах, що призводить до компрометації ланцюга постачання програмного забезпечення. Зростання атак підміни сутності, такі як крадіжка облікових даних або видавання себе за агентів компіляції, підкреслює необхідність розробки надійних механізмів перевірки ідентичності. Нарешті розкриття інформації також було визначено як повторювану проблему, причому витік секретів із середовищ CI/CD може призводити до виникнення інцидентів у хмарних середовищах.

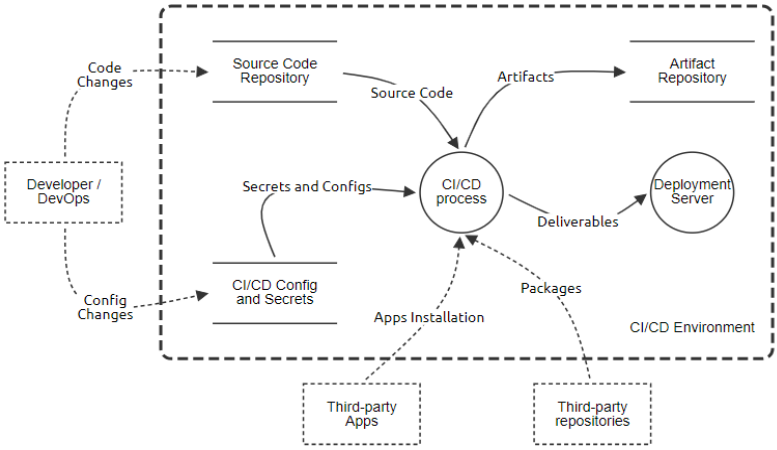

Рис.2. Структура CI/CD процесу в DFD нотації

Запропонована комбінація SSDF та STRIDE методологій забезпечує систематичне виявлення та пріоритизацію загроз в CI/CD процесах.

1. Prates, L., & Pereira, R. (2025). DevSecOps practices and tools. International Journal of Information Security, 24 (1), 11. https://doi.org/10.1007/s10207-024-00914-z
2. Paule, C., Düllmann, T. F., & Van Hoorn, A. (2019, March). Vulnerabilities in Continuous Delivery Pipelines? A Case Study. In ICSA Companion (pp. 102-108). https://doi.org/10.1109/ICSA-C.2019.00026
3. Akbar, M. A., Smolander, K., Mahmood, S., & Alsanad, A. (2022). Toward successful DevSecOps in software development organizations: A decision-making framework. Information and Software Technology, 147, 106894 https://doi.org/10.1016/j.infsof.2022.106894
4. Zhao, X., Clear, T., & Lal, R. (2024). Identifying the primary dimensions of DevSecOps: A multi-vocal literature review. Journal of Systems and Software, 214, 112063 https://doi.org/10.1016/j.jss.2024.112063

Issues of protecting personal data in artificial intelligence systems in education

UDK 37.01:004.8:004.056.5

Zhazira Yerimbetova

Kazakh National pedagogical university named after Abai, Almaty, Kazakhstan
zhazira.erimbetova@gmail.com

Currently, the digital transformation process is characterized by the active introduction of artificial intelligence (AI) technologies at all levels of the education sector. Adaptive learning platforms and intelligent systems are enhancing the