КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (14), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.14.2635
УДК 004.056

Сусукайло Віталій Андрійович
аспірант кафедри захисту інформації
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0000-0003-4431-9964
vitalii.a.susukailo@lpnu.ua

ВИКОРИСТАННЯ ПІДХОДУ DEVSECOPS ДЛЯ АНАЛІЗУ СУЧАСНИХ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. У даній статті подано дослідження використання підходу DevSecOps для аналізу сучасних загроз. Визначення методології для реалізації та адаптації DevSecOps підходу. DevSecOps у даній статті подано як підхід до культури розробки, автоматизації та дизайну інформаційної платформи, який інтегрує безпеку як спільну відповідальність протягом усього життєвого циклу розробки програмного забезпечення. Підхід, описаний у даній статті, допомагає вирішити проблему впровадження контролей безпеки в процесі розробки програмного забезпечення. Визначений підхід дозволяє організації постійно вбудовувати безпеку в SDLC, щоб команди DevOps могли швидко та якісно розробляти безпечні програми. Досліджується можливість впровадження безпеки на ранніх етапах розробки програмного забезпечення в робочий процес, так як це дозволить швидше виявити та усунути слабкі та вразливі місця безпеки. Ця концепція є частиною «зміщення ліворуч», яка переміщує тестування безпеки до розробників, що дозволяє їм виправляти проблеми безпеки в своєму коді майже в реальному часі, а не чекати до кінця SDLC, де безпека була закріплена в традиційних середовищах розробки. Описано бізнес процеси для мінімізації ризиків пов’язані з сучасними загрозами та вразливостями нульового дня у рамках DevSecOps підходу. Проведено аналіз SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing), SCA (Software Composition Analysis) застосунків для оцінки можливого використання даних технологій для оптимізації процесу безпечної розробки додатків. Подано процес DevSecOps для організацій, що зможуть легко інтегрувати безпеку в свою існуючу практику безперервної інтеграції та безперервної доставки (CI/CD). DevSecOps процес в даній статті охоплює весь SDLC від планування та проектування до кодування, побудови, тестування та випуску, з безперервним зворотним зв’язком в реальному часі та сформовано технічні контролі процесу DevSecOps у відповідності до ISO 27001/02 та NIST стандартів.

Ключові слова: DevSecOps; безпека; інформація; загрози; SaaS, SAST, DAST.

ВСТУП

Форматування кожного структурного елементу статті описано у «Вимогах до оформлення статей». Дана інструкція оформлена згідно цих вимог і може бути використана як *шаблон*. Прохання, перед завантаженням файлу в журнал, перевірити всі деталі готового рукопису, у тому числі і порядок імен авторів. Переконайтеся, що Вами були вказані адреси електронної пошти кожного з авторів, а сторінки статті не пронумеровані. Згідно зі статистикою організації Security Magazine приблизно 50 вразливостей з’являється щодня. Вони представляють серйозну загрозу для урядових та приватних організацій, так як несуть не тільки фінансові а й репутаційні наслідки. Унаслідок вразливостей відбуваються витоки великої кількості конфіденційної інформації - від внутрішніх документів до невипущених продуктів і персональних даних клієнтів (включаючи паролі). Залежно від юрисдикції за витік даних користувачів можуть накладатися серйозні грошові штрафи і юридична відповідальність.

ISSN 2663 - 4023

Незважаючи на все це, команди розробників часто трактують контролі інформаційної безпеки не як можливий актив, а як обтяження. Аудити безпеки, складання звітів - все це уповільнює процес і перешкоджає доставці нових можливостей прямо в руки користувачів. Це мислення допомагає зловмисникам скомпрометувати організацію. Ситуація також ускладнюється тим, що практично будь-яке ПЗ (і з відкритим вихідним кодом, і пропрієтарних) включає залежності, і організація не можете бути впевненою, що сторонній код не містить вразливостей. Раніше завдання безпеки «добудовувалися» в кінці життєвого циклу розробки ПЗ як щось другорядне, при цьому за забезпечення і тестування безпеки відповідали окремі команди фахівців. Проте зараз під час розробки програмного забезпечення компанії все частіше використовується підхід DevSecOps. Згідно з IBM Security, DevSecOps - скорочено від development, security і operations - автоматизує інтеграцію завдань безпеки на всіх етапах життєвого циклу розробки програмного забезпечення, від проектування до інтеграції, тестування, розгортання і доставки ПЗ.

Постановка проблеми. Протягом останніх кількох років технологічна індустрія часто стає свідком компрометації даних, ставлячи під загрозу функції безпеки та конфіденційність даних користувачів через своєчасність виявлення вразливостей та загроз. Існують різні причини, які надають зловмисникам можливість скористатися відсутніми обмеженнями безпеки. Як повідомляє DBIR 2020, 43% компроментації даних минулого року були пов'язані з вразливістю адодатків. Це відбувається тому, що більшість підходів, що використовуються розробниками не мають відповідних засобів безпеки, які могли б перешкодити зловмиснику причаїтися і обійти обмеження. Це працює як основна причина експоненціального зростання порушень даних. Організації повинні впроваджувати питання безпеки в процес розробки своїх додатків, щоб запобігти порушенням та поглибити захист. Існує безліч причин для інтеграції безпеки у ваш SDLC, починаючи від запобігання порушенню даних та зменшуючи вплив порушення/атаки до втрати репутації або довіри зацікавлених сторін. Для цього дана стаття розглядає підхід DevSecOps як безперервний процес безпечної розробки додатків.

Аналіз останніх досліджень і публікацій. Проблеми побудови процесу автоматизованого визначення вразливостей на різних рівнях інформаційних систем досліджуються багатьма науковцями та спеціалістами цієї галузі. Для даної статті було проаналізовано низку зарубіжних та вітчизняних наукових робіт, зокрема проблеми розвитку DevSecOps детально описані у наступних статтях: J. Smeds, K. Nybom and I. Porres, "DevOps: A Definition and Perceived Adoption Impediments", Agile Processes in Software Engineering and Extreme Programming [1] та KUMAR, Rakesh; GOYAL, Rinkaj. Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud (ADOC). Computers & Security [2].

Мета статті. Метою статті є визначення можливостей використання підходу DevSecOps для аналізу сучасних загроз інформаційної безпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Традиційний процес побудови додатків - SDLC розпочинається з дослідження вимог до застосування та цільового користувача чи ринку. Найважливішим чинником у SDLC є розробка багатофункціональних та керованих даними програм/програмного забезпечення якнайшвидше для захоплення ринку та швидкої рентабельності інвестицій. Вимога стосується виключно функцій додатку, дизайну та досвіду користувача. Він включає всебічне планування додатку або фундаменту програмного забезпечення,

наприклад, фінансовий бюджет додатку, зовнішній вигляд, макет, план, архітектурні рішення, передачу та зберігання даних, взаємодію додатку з користувачами та інші системи чи мережі. Безпечний SDLC - це методологія з додаванням найкращих практик безпеки на кожному з етапів життєвого циклу розробки. Вона включає розгляд контролей безпеки під час планування розробки додатків. Безпечний SDLC описує, як повинна бути побудований додаток, щоб дані користувачів залишались захищеними. Дана методологія враховує впровадження вимог інформаційної безпеки під час розробки, проведення аналізу загроз для додатку, процес впровадження перевірок безпеки під час розробки додатків та подальше дослідження інцидентів для розроблених додатків. Частиною процесу безпечний SDLC є інтеграція вимог безпеки у DevOps, тобто DevSecOps процес. Зловмисники завжди шукають найкращі способи розгортання шкідливого програмного забезпечення та інших експлойтів. Під час компрометації компанії SolarWinds зловмисникам вдалось встановити шкідливе програмне забезпечення у додаток під час процесу збірки, під час цього шкідливе програмне забезпечення не було виявлено, поки додаток не було розповсюджено тисячам клієнтів. Збиток як для системи клієнтів, так і для репутації компанії був величезним, так як SolarWinds використовували як приватні так і державні організації. Згідно з організацією SumoLogic, яка є світовим лідером з у SaaS моніторингу, є шість важливих складових підходу DevSecOps. Аналіз коду – код програмного забезпечення повинен доставлятись невеликими фрагментами, щоб вразливі місця можна було швидко виявити. Управління змінами – будь хто повинен мати можливість як подати зміни, так їх і відмінити. Моніторинг відповідності – потрібно вивчати вимоги чинного законодавства та стандартів інформаційної безпеки та бути готовим до аудиту в будь -який час. Розслідування загроз – потрібно моделювати потенційні нові загрози з кожним оновленням коду або ж функціоналу застосунку. Оцінка вразливості – потрібно безперервно визначати нові вразливості за допомогою аналізу коду, а також швидкість їх виправлення. Навчання безпеці – потрібно постійно проводити тренінги з інформаційної безпеки для мінімізації ризиків спричинених людським фактором. Для побудови активної протидії загрозам та швидкого виявлення загроз у за підходом DevSecOp, заходи безпеки можуть бути додані до постійної інтеграції та постійного впровадження (CI/CD). Кожного разу, коли розробник створює код, він запускає інструмент коCI/CD, який виконує весь необхідний процес, тобто передає код у спільне сховище та надсилає сповіщення іншим членам команди. Крім цього, він також може перевіряти наступні речі: якщо будь -яка зовнішня бібліотека, включена до проекту, чи є вона автентичною, ліцензійні ризики та уразливості тощо. Будь -яка секретна інформація, така як пароль/ облікові дані, передається разом з кодом у сховищі git . Він повідомляє. Перш ніж вони потраплять у конвеєр CI/CD, сканування зображень контейнерів за допомогою засобів безпеки перевіряє їх уразливості. Для наведених вище цілей доступні різні інструменти для включення в конвеєр DevOps CI/CD. Типовий Devops процес включав такі етапи, як план, код, збірка, тестування, випуск та розгортання. У DevSecOps до кожної фази конвеєра DevOps застосовуються певні перевірки безпеки. Тут ми можемо зрозуміти перевірки безпеки, які використовуються шляхом прийняття DevSecOps у конвеєрі CI/CD.

План: на етапі планування виконується аналіз безпеки та створюється план для визначення сценаріїв того, як, де та коли буде проводитися тестування.

Надсилання коду: на даному етапі потрібно регулярно проводити перевірку коду на наявність облікових даних користувачів.

ISSN 2663 - 4023

Збірка коду: використання інструментів статичного тестування додатків (SAST) для відстеження вад коду перед його розгортанням у виробництві.

Розгортання: проведення динамічного аналізу (DAST) безпеки додатку.

Моніторинг: дослідження подій та інцидентів інформаційної безпеки пов'язнаних з додатком, шляхом збору системних подій.

Під час дослідження основних аспектів підходу DevSecOps, було розроблено низку блок-схем для узагальнення методології перевірки додатків, що можуть слугувати основою для впровадження DevSecOps процесів у організацію. Зокрема, дані блок схеми зображено на Рисунках 1 та 2.

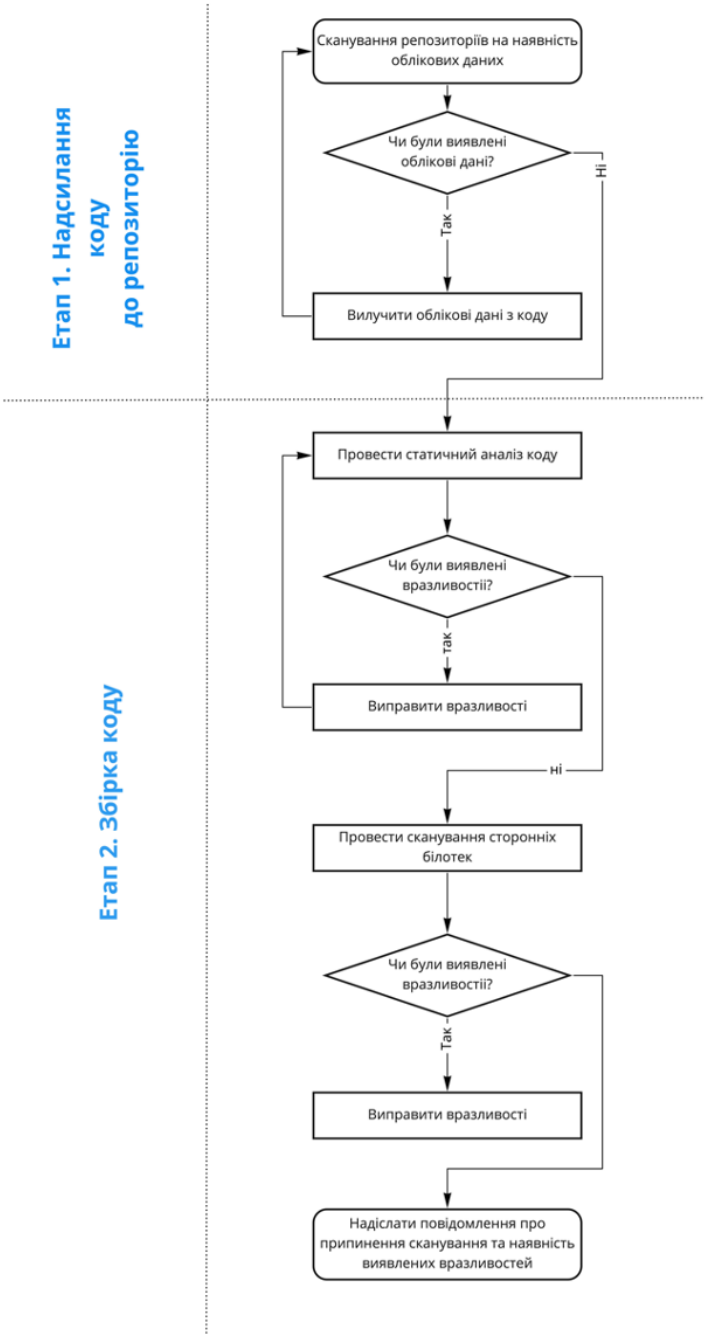

Рис.1 – Перевірка та Збірка Коду

ISSN 2663 - 4023

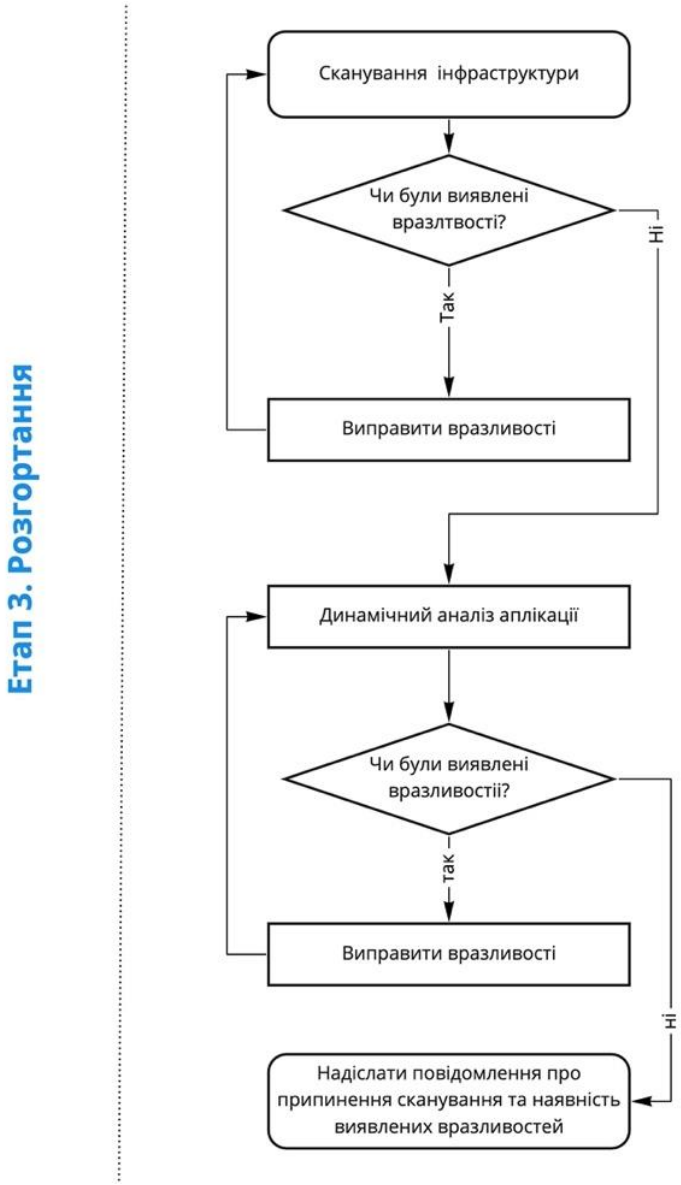

Рис.2 – Етап розгортання

Під час впровадження процесу DevSecOps на етапах надсилання коду, збірки та розгортання організація повинна визначити критерії за яких процес внесення змін буде призупинятись доки не будуть виправлені недоліки. Зокрема в даному дослідженні рекомендовано призупиняти процес внесення змін в додаток до виправлення виявлених проблем інформаційної безпеки, зокрема внесених паролей до вихідного коду або ж наявність вразливостей будь якого типу, окрім інформаційних.

Важливим етапом для безперервного дослідження загроз у підході DevSecOps є також етап моніторингу. Для дослідження усіх подій пов'язаних з додатком та його інфраструктурою потрібно використовувати централізовану систему дослідження загроз типу SIEM. Прикладом систем які можуть використовуватись є Splunk, AlienVault OSSIM, Security Onion та інші. Необхідним кроком під час налагодження моніторингу є приєднання усіх можливих джерел логування до централізованої системи моніторингу, зокрема: подій з інфраструктурних компонентів, додатків, доступу до даних та фаєрволу веб-додатків.

ISSN 2663 - 4023

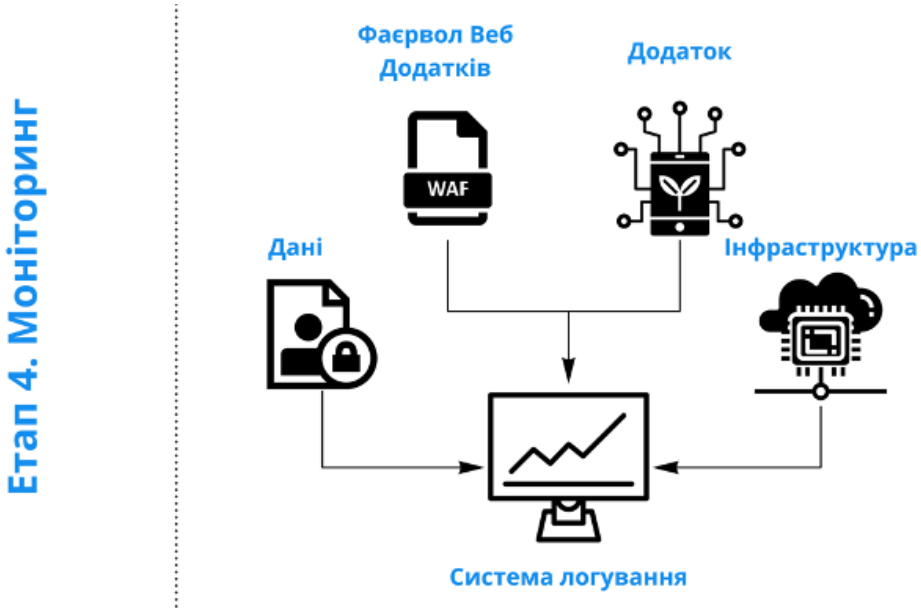

Рис.3 – Моніторинг

Після підключення джерел логування, потрібно приєднати джерела індикаторів компроментації систем, таких як AlienVault OTX чи IBM Xchange XForce. Також необхідно розробити кореляційні правила для дослідження нетипової поведінки у журналах подій. Для автоматизації дослідження подій систему SIEM можна інтегрувати з додатками для комунікацій та для автоматизації реагування на інциденти інформаційної безпеки необзідно інтегрувати SIEM систему з SOAR системою. В даному випадку не лише DevSecOps процес буде повноцінним, а й процес дослідження кіберзлочинів буде автоматизований. Також в даній статті було проаналізовано використання можливих рішень для побудови DevSecOps процесу у різних огранізаціях та подано їх в Таблиці 1.

Таблиця 1

Технічні рішення для побудови DevSecOps процесу

Контроль	Рішення	Ціль використання	Відповідний контроль ISO 27001/2	NIST CSF контроль
Security Orchestration	Patrowl Demisto	Платформи автоматизації використовувати для автоматизації заходів безпеки під час пандемії.	A16.1.2	RS.CO-2
SAST	SonarQube, DerScanner	Інструменти аналізу вихідного коду, які також називаються інструментами статичного тестування безпеки додатків (SAST), призначені для аналізу вихідного коду або складених версій коду, щоб допомогти виявити недоліки безпеки.	A14.2.1	PR.IP-2
DAST	OWASP ZAP, Arachni NIkto	Динамічне тестування безпеки додатків (DAST) досліджує програми на наявність	A14.2.1	PR.IP-2

		уразливостей у розгорнутому середовищі.		
SCA	Npm-audit, OWASP Dependency check	Програмне забезпечення для аналізу композиції програмного забезпечення (SCA) дозволяє користувачам аналізувати та керувати елементами відкритого коду своїх програм.	A14.2.1	PR.IP-2
Cloud Configuration Audit	Scout-suite	Інструмент перевірки безпеки, що дозволяє оцінювати контролі безпеки хмарних середовищ.	A18.2.3	ID.RA-1

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Практично кожна IT -організація так чи інакше використовує автоматизацію. Звіт Business Wire показує, що 61% організацій у США широко використовують автоматизацію. Компанії усвідомлюють потужність та переваги автоматизації та впроваджують її на кожному рівні DevOps - від розробки, до розгортання та управління.

Оскільки організації все більше працюють без серверів, використовуючи Docker, Kubernetes та інші сучасні хмарні технології, безпека, як завжди, буде мати пріоритет, ставши частиною DevOps за замовчуванням.

Як і у випадку з DevOps - об'єднанням команд розробників та IT, DevSecOps стане інтеграцією безпеки у команду розробникі.

Золотим стандартом для дослідження загроз та взаливостей пов'язаних з додатками та інфраструктурою інформаційних систем вважалось тестування на проникнення. Проте, тестування на проникнення не є постійним процесом, що унеможливлює вчасне виявлення вразливостей. Тому, у даній статті подано дослідження використання підходу DevSecOps для аналізу сучасних загроз. Визначений підхід у даній статті дає можливість організаціям реалізувати та адаптувати DevSecOps підхід та мінімізувати ризики пов'язані з сучаними загрозами та вразливостями нульового дня.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Mezak, S. (2018). Data Breaches Compromised 4.5 Billion Records in First Half of 2018.
2 (2018). https://www.sttinfo.fi/tiedote/data-breaches-compromised-45-billion-records-in-first-half-of-2018?publisherId=58763726releaseId=69844038.
3 Smeds, J., Nybom, K., & Porres, I. (2015). DevOps: A Definition and Perceived Adoption Impediments. У *Lecture Notes in Business Information Processing* (с. 166–177). Springer International Publishing. https://doi.org/10.1007/978-3-319-18612-2_14
4 Prates, L., Faustino, J., Silva, M., & Pereira, R. (2019). DevSecOps Metrics. У *Information Systems: Research, Development, Applications, Education* (с. 77–90). Springer International Publishing. https://doi.org/10.1007/978-3-030-29608-7_7
5 Kumar, R., & Goyal, R. (2020). Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud (ADOC). *Computers & Security*, *97*, 101967. https://doi.org/10.1016/j.cose.2020.101967
6 Susukailo, V., Opirskyy, I., & Vasylyshyn, S. (2020). Analysis of the attack vectors used by threat actors during the pandemic. У *2020 IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT)*. IEEE. https://doi.org/10.1109/csit49958.2020.9321897
7 Susukailo, V., Vasylyshyn, S., Opirskyy, I., Buriachok, V., Riabchun, O. (2021). Cybercrimes investigation via honeypots in cloud environments. *CEUR Workshop Proceedingsthis link is disabled*, 2021, *2923*, 91–96.
8 Koskinen, A. (2019). DevSecOps: building security into the core of DevOps.

ISSN 2663 - 4023

9 *12 Things to Get Right for Successful DevSecOps*. (2019). Gartner. https://www.gartner.com/en/documents/3978490/12-things-to-get-right-for-successful-devsecops
10 *What is DevSecOps and Why Is It Important? | Sumo Logic*. (2019). Sumo Logic. https://www.sumologic.com/insight/devsecops-rugged-devops
11 *What is DevSecOps?* Forcepoint. https://www.forcepoint.com/cyber-edu/devsecops
12 *DevSecOps Process and Implementation*. Software Engineering Institute. https://www.sei.cmu.edu/education-outreach/courses/course.cfm?coursecode=P141
13 *The future of DevSecOps*. https://faun.pub/the-future-of-devops-15-trends-for-2021-b3b8c59444ff
14 *What is DevSecOps?* https://www.jetbrains.com/ru-ru/teamcity/ci-cd-guide/what-is-devsecops/

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (14), 2021
ISSN 2663 - 4023

Vitalii Susukailo
PHd student of Information Security Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0003-4431-9964
vitalii.a.susukailo@lpnu.ua

USE OF DEVSECOPS APPROACH FOR INFORMATION SECURITY THREATS ANALYSIS

Abstract. This article presents a study of the use of the DevSecOps approach to analyze modern threats. Defines a methodology to implement and adapt the DevSecOps approach. DevSecOps is presented in this article as an approach to the culture of developing, automating and designing an information platform that integrates security as a shared responsibility throughout the software development lifecycle. The approach described in this article helps to solve the problem of implementing security controls in the software development process. This approach allows organizations to continually integrate security into SDLC so that DevOps teams can quickly and efficiently develop secure applications. The possibility of implementing security in the early stages of software development in the workflow is being investigated, as it will allow to identify and eliminate security vulnerabilities and vulnerabilities faster. This concept is part of the "left shift" that shifts security testing to developers, allowing them to fix security issues in their code almost in real time, rather than waiting until the end of the SDLC, where security has been embedded in traditional development environments.Describes DevSecOps approach as business processes, which minimize the risks associated with modern threats and zero-day vulnerabilities. SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing), SCA (Software Composition Analysis) analysis was used to assess the possibilities of using these technologies to optimize the process of secure software development. The DevSecOps process is presented for organizations that can easily integrate security into their existing practices of continuous integration and continuous delivery (CI / CD). The DevSecOps process in this article covers the entire SDLC from planning and design to coding, testing, and release, with continuous real-time feedback, and defined DevSecOps process technical controls in accordance with ISO 27001/02 and NIST standards.

Keywords:DevSecOps; security; information; threats; SaaS; SAST; DAST.

REFERENCES

1 Mezak, S. (2018). Data Breaches Compromised 4.5 Billion Records in First Half of 2018.
2 (2018). https://www.sttinfo.fi/tiedote/data-breaches-compromised-45-billion-records-in-first-half-of-2018?publisherId=58763726releaseId=69844038.
3 Smeds, J., Nybom, K., & Porres, I. (2015). DevOps: A Definition and Perceived Adoption Impediments. У *Lecture Notes in Business Information Processing* (с. 166–177). Springer International Publishing. https://doi.org/10.1007/978-3-319-18612-2_14
4 Prates, L., Faustino, J., Silva, M., & Pereira, R. (2019). DevSecOps Metrics. У *Information Systems: Research, Development, Applications, Education* (с. 77–90). Springer International Publishing. https://doi.org/10.1007/978-3-030-29608-7_7
5 Kumar, R., & Goyal, R. (2020). Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud (ADOC). *Computers & Security*, *97*, 101967. https://doi.org/10.1016/j.cose.2020.101967
6 Susukailo, V., Opirskyy, I., & Vasylyshyn, S. (2020). Analysis of the attack vectors used by threat actors during the pandemic. У *2020 IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT)*. IEEE. https://doi.org/10.1109/csit49958.2020.9321897
7 Susukailo, V., Vasylyshyn, S., Opirskyy, I., Buriachok, V., Riabchun, O. (2021). Cybercrimes investigation via honeypots in cloud environments. *CEUR Workshop Proceedingsthis link is disabled*, 2021, *2923*, 91–96.
8 Koskinen, A. (2019). DevSecOps: building security into the core of DevOps.
9 *12 Things to Get Right for Successful DevSecOps*. (2019). Gartner. https://www.gartner.com/en/documents/3978490/12-things-to-get-right-for-successful-devsecops

10 *What is DevSecOps and Why Is It Important? | Sumo Logic*. (2019). Sumo Logic. https://www.sumologic.com/insight/devsecops-rugged-devops
11 *What is DevSecOps?* Forcepoint. https://www.forcepoint.com/cyber-edu/devsecops
12 *DevSecOps Process and Implementation*. Software Engineering Institute. https://www.sei.cmu.edu/education-outreach/courses/course.cfm?coursecode=P141
13 *The future of DevSecOps*. https://faun.pub/the-future-of-devops-15-trends-for-2021-b3b8c59444ff
14 *What is DevSecOps?* https://www.jetbrains.com/ru-ru/teamcity/ci-cd-guide/what-is-devsecops/