Engineer Консультування

Запровадила безперервне сканування безпеки

Запровадила безперервну програму безпеки — сканування коду, DAST, перевірки залежностей і вразливостей, генерацію SBOM, пошук секретів та actions, закріплені за SHA, — поряд із 21 письмовим аудитом безпеки.

2025

21

письмових аудитів безпеки
поряд з автоматичними

Ситуація. Робота з безпеки всередині застосунку — Content-Security-Policy, ролі бази даних із мінімальними привілеями, повторні перевірки прав — захищає платформу під час виконання. Але вона нічого не каже про те, що саме виходить у реліз: чи не підхопила залежність відому вразливість минулого вівторка, чи не потрапили в коміт облікові дані, які потім відкотили, і чи не стала стороння action, закріплена за тегом, непомітно зовсім іншим кодом.

Завдання. Безпека ланцюга постачання та коду мала бути безперервною й автоматизованою, щоб її стан був результатом збірки, а не чиєюсь думкою.

Дія. Статичний аналіз виконує CodeQL, динамічне тестування живого інстансу — ZAP, а залежності Go перевіряє govulncheck. Перелік компонентів програмного забезпечення (SBOM) генерується під час кожної збірки за допомогою Anchore та Syft, тож склад того, що вийшло в продакшн, відомий одразу, а не відновлюється згодом. Gitleaks шукає в історії облікові дані. Кожна стороння GitHub Action закріплена за хешем коміту, а не за тегом, — цей непоказний захід захищає від непомітної підміни коду через переміщення тегу. Dependabot стежить за 6 екосистемами. Автоматизацію доповнює 21 письмовий аудит безпеки, зокрема модель

загроз і оцінка за посібником з тестування OWASP, — адже сканери знаходять типи проблем, які хтось уже описав, а в моделі загроз називають ті, що властиві саме цій платформі.

Результат. Вразливість, яку розпізнають налаштовані перевірки, може зупинити збірку. Справжня ціна — обсяг знахідок: сканер, який повідомляє про все, привчає людей його ігнорувати, і щоб сигнал лишався корисним, потрібен постійний розбір знахідок, а не одноразове налаштування.

Застосуйте цей досвід у своєму проєкті

Використайте «Запровадила безперервне сканування безпеки» як відправну точку для схожого завдання у вашій організації. Послуги, що стоять за цією роботою, доступні й для вашого проєкту. Передавання справ, інструкції з експлуатації і посібники, щоб ваші працівники обслуговували систему без дзвінків тому, хто її створив.

Переглянути наші послуги Зв'язатися з нами →

Дізнайтеся, що привело до результату

Прочитайте про ситуацію, рішення та результат цього прикладу. Ми можемо обговорити, що відповідає вашим умовам, а що потребує іншого підходу. Запровадила безперервне сканування безпеки — 21 письмових аудитів безпеки поряд з автоматичними

Переглянути наші послуги Зв'язатися з нами →

Хочете перевіряти безпеку під час кожної збірки?

Обговоріть свій проєкт з інженером, відповідальним за виконання. Обсяг, основу розрахунку вартості та передачу результатів узгоджуємо письмово до початку робіт.

Роль у цій роботі: Інженер з безпеки. Тут задіяні DevOps, Автоматизація та CI/CD, Надійність і резервне копіювання, Безпека та Документація. І, до речі, ми добре вміємо DevOps та автоматизація CI/CD, Безпека та керування доступом, Безпека ШІ-агентів та Технічна документація.

Зв'язатися з нами Ознайомтеся з нашими послугами

Одна частина **довшого переліку** — і він увесь на цьому сайті.

Кожен запис написано однаково: ситуація, завдання, що ми зробили і що змінилося.

Переглянути весь перелік

Визначте потрібне покращення

Опишіть рішення, людей, яких воно стосується, та вже розглянуті варіанти. Ми можемо явно показати компроміси й залишити документовану рекомендацію.

Дивитися, скільки це коштує Зв'язатися з нами →

Хочете перевіряти безпеку під час кожної збірки?

Запитайте про рішення в роботі «Запровадила безперервне сканування безпеки». Ви говоритимете з людьми, які можуть пояснити роботу й оцінити ваш проєкт.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://advisory.engineer.company/uk/portfolio/ran-a-continuous-security-scanning-programme/