SISTEMAS EMBARCADOS · UFC · 31 DE DEZEMBRO DE 2025

Do invisível ao observável: implementação de uma pipeline DevSecOps em uma empresa de pequeno porte

Fonte: Repositório Institucional UFC · Publicação original

INOVAÇÃO	APLICABILIDADE	POTENCIAL ECONÔMICO	MATURIDADE
7/10	9/10	8/10	Média

Implementação de uma pipeline DevSecOps de baixo custo em uma pequena empresa de segurança da informação, utilizando GitHub Actions para integrar análise estática, dinâmica e verificação de dependências. O estudo demonstrou viabilidade de alta maturidade de segurança com equipe enxuta, obtendo 82% de cobertura de testes e redução significativa de vulnerabilidades.

NÚCLEO DA ANÁLISE

Ideia de startup ou produto

Plataforma SaaS de 'DevSecOps-in-a-Box' focada no mercado de PMEs brasileiras, oferecendo templates prontos de pipelines de CI/CD com ferramentas de segurança pré-configuradas e dashboard simplificado para gestão de riscos sem necessidade de expertise profunda em segurança.

Aplicações práticas

Adaptação de repositórios de GitHub Actions prontos para uso por PMEs; automação de portarias de segurança em processos de desenvolvimento ágil; integração de ferramentas open-source (SonarQube, OWASP ZAP) em fluxos de trabalho contínuos.

Potencial de mercado

Alta demanda por soluções de 'Compliance as Code' e automação de segurança no cenário de LGPD, especialmente por software houses e startups que buscam escala sem inflar custos operacionais. O modelo de DevSecOps acessível é um diferencial competitivo forte no mercado B2B de tecnologia.

FUNDAMENTO CIENTÍFICO

Problema abordado

Dificuldade de pequenas empresas em manter práticas de segurança de software devido a restrições orçamentárias, falta de infraestrutura e impossibilidade de contratar profissionais dedicados, resultando em verificações manuais ineficientes e exposição a vulnerabilidades.

Metodologia

Estudo de caso em uma pequena empresa do setor de segurança da informação. Implementação de pipeline CI/CD utilizando GitHub Actions e ferramentas de automação de segurança (SAST, DAST, SCA) de código aberto, focando em soluções de baixa manutenção compatíveis com recursos limitados.

Principais descobertas

A pipeline automatizada permitiu a detecção de 67 vulnerabilidades de dependência e falhas estáticas/dinâmicas, além de alcançar 82% de cobertura de testes automatizados. A solução eliminou a necessidade de profissionais dedicados a segurança naquele momento, agilizando a entrega e elevando a maturidade de segurança da organização.

LEITURA PARA GESTÃO PÚBLICA

Criação de editais de fomento (via FUNCAP ou FINEP) para incentivar a adoção de boas práticas de segurança em micro e pequenas empresas de tecnologia do Ceará. Implementação de selo de 'Software Seguro' para empresas que adotem pipelines automatizados.

PARCERIA UNIVERSIDADE × EMPRESA

Parceria entre universidades (UFC) e ecossistemas de inovação (como o Núcleo ou TEC4DEV) para desenvolver laboratórios de validação de código seguro, onde a comunidade acadêmica audita pipelines de empresas locais em troca de dados para pesquisa.

OPORTUNIDADES DERIVADAS

3 direções estratégicas identificadas

STARTUP · IMPACTO MÉDIO · CIBERSEGURANÇA

DevSecOps as a Service for SMEs

Startup especializada em configurar e gerenciar pipelines de segurança automatizadas para pequenas empresas que não têm engenheiros de segurança, usando ferramentas open-source.

PRODUTO CORPORATIVO · IMPACTO BAIXO · SOFTWARE

GitHub Actions Security Toolkit

Pacote corporativo de workflows padronizados para GitHub Actions que integram SAST, DAST e SCA, vendido como um produto de valor agregado para agências de desenvolvimento.

POLÍTICA PÚBLICA · IMPACTO ALTO · GOVTECH

Programa de Fortalecimento da Cibersegurança Local

Política pública para capacitar e fornecer infraestrutura baseada nos achados do paper para empresas de tecnologia incubadas no estado, garantindo um nível mínimo de segurança no software produzido.

ABSTRACT ORIGINAL

Título: Do invisível ao observável: implementação de uma pipeline DevSecOps em uma empresa de pequeno porte Autor(es): Silva, Francisco Keven Almeida da Abstract: Software development security is an increasing concern, especially for companies seeking greater agility in delivering new products to the market. However, small companies frequently face significant constraints in budget, infrastructure, and staffing, which hinder the hiring of dedicated security professionals and the adoption of automation mechanisms capable of sustaining a secure development cycle. In such settings, small teams end up accumulating multiple responsibilities, relegating security practices to manual, sporadic, or even nonexistent checks, thereby increasing exposure to vulnerabilities. In this context, the Development, Security, and Operations (DevSecOps) approach emerges as a low operational cost, integrated solution, combining development, operations, and security into a single automated workflow capable of compensating for the absence of a dedicated security team through continuous, automated verification. This study proposes the implementation of a DevSecOps pipeline in a small company operating in the information security sector, with the goal of automating routine activities during the software delivery process, reducing the burden on the development team, and applying security checks throughout the entire software development lifecycle without requiring the hiring of additional specialists. The case study focuses on integrating security tools, such as static and dynamic code analysis, into a Continuous Integration and Continuous Delivery (CI/CD) pipeline using GitHub Actions, prioritizing free, low-maintenance solutions compatible with the company's limited resources. The proposed model is evaluated based on its ability to enhance code efficiency, quality, and security while meeting the company's operational and staffing constraints. The methodology employs security automation tools to promote early vulnerability detection and ensure a more secure and robust development process, even amid a shortage of specialized human resources. The results show that the pipeline enabled the detection of 67 dependency vulnerabilities, 2 static code findings, and runtime security risks via dynamic analysis, while achieving 82% automated test coverage, demonstrating that it is possible to significantly raise the security maturity of a small organization even with a lean team and a limited budget. As a practical impact, the automation introduced by the pipeline reduced thetime spent on manual checks, enabling faster and more frequent delivery of new versions to end customers, while the security embedded into the development process becomes a competitive differentiator for the company, a relevant factor for attracting and retaining customers who demand guarantees regarding the protection of their data and systems. Tipo: TCC

MATÉRIA PARA LEIGOS

Para leigos: Segurança de software automatizada para pequenas empresas

O cenário atual

A segurança no desenvolvimento de software é uma preocupação crescente, especialmente para empresas que buscam maior agilidade na entrega de novos produtos ao mercado. No entanto, pequenas empresas enfrentam restrições significativas de orçamento, infraestrutura e pessoal. Esses obstáculos dificultam a contratação de profissionais de segurança dedicados e a adoção de mecanismos de automação que sustentem um ciclo de desenvolvimento seguro. Nesses ambientes, equipes pequenas acabam acumulando múltiplas responsabilidades, relegando as práticas de segurança a verificações manuais, esporádicas ou inexistentes, o que aumenta a exposição a vulnerabilidades.

O que os pesquisadores fizeram

Este estudo propôs a implementação de uma pipeline DevSecOps em uma empresa de pequeno porte do setor de segurança da informação. O objetivo foi automatizar atividades rotineiras durante o processo de entrega de software, reduzir a carga sobre a equipe de desenvolvimento e aplicar verificações de segurança em todo o ciclo de vida do desenvolvimento sem a necessidade de contratar especialistas adicionais.

Como funciona na prática

A abordagem DevSecOps (Desenvolvimento, Segurança e Operações) surgiu como uma solução integrada de baixo custo operacional. O estudo focou na integração de ferramentas de segurança, como análise estática e dinâmica de código, em uma pipeline de Integração Contínua e Entrega Contínua (CI/CD) utilizando o GitHub Actions. A prioridade foi o uso de soluções gratuitas e de baixa manutenção, compatíveis com os recursos limitados da empresa. A metodologia emprega ferramentas de automação de segurança para promover a detecção precoce de vulnerabilidades.

Resultados e evidência

O modelo proposto foi avaliado com base na capacidade de melhorar a eficiência, qualidade e segurança do código. Os resultados demonstraram que a pipeline possibilitou a detecção de 67 vulnerabilidades de dependências, 2 achados na análise estática de código e riscos de segurança em tempo de execução via análise dinâmica. Além disso, alcançou-se 82% de cobertura de testes automatizados. Isso mostra que é possível elevar significativamente a maturidade de segurança de uma pequena organização mesmo com uma equipe enxuta e orçamento limitado.

Implicações práticas

Como impacto prático, a automação introduzida pela pipeline reduziu o tempo gasto em verificações manuais, permitindo entregas mais rápidas e frequentes de novas versões para os clientes finais. A segurança incorporada ao processo de desenvolvimento torna-se um diferencial competitivo para a empresa, sendo um fator relevante para atrair e reter clientes que exigem garantias sobre a proteção de seus dados e sistemas.

Limitações e próximos passos

O paper não detalha limitações específicas da implementação realizadas ou quais seriam os próximos passos para a continuidade da pesquisa além dos resultados apresentados.

QUEM SÃO OS PESQUISADORES

Quem são os pesquisadores

O estudo foi autoria de Francisco Keven Almeida da Silva, apresentado como Trabalho de Conclusão de Curso (TCC) vinculado à Universidade Federal do Ceará (UFC). O material fornecido não informa afiliações específicas, vínculos prévios, trajetória acadêmica detalhada ou atuação profissional do autor além do contexto deste trabalho.