

DEVSECOPS AS A SERVICE

PROJECT SECDEVIAS

Cesar Marcondes, PhD



<https://www.secdevias.com/>

Instituições Envolvidas

Rede Nacional de
Pesquisa



Instituto Tecnológico de
Aeronáutica



Instituto Federal do
Tocantins



Exército Brasileiro



Netconn Group



INDICE

01

ESTADO ATUAL DE DEVSECOPS

02

SOLUÇÃO SECDEVIAS

04

VISÃO DE FUTURO

05

CALL FOR ACTION (POC)

ESTADO ATUAL DE DEVSECOPS

SECDEVIAS

Solução SecDevias traz processo de desenvolvimento de software seguro automatizado

O mercado de desenvolvimento de software vem amadurecendo rapidamente, passando por um processo de consolidação de automação desde a criação até **entrega de software por meio de esteiras** de desenvolvimento, que são uma solução de desenvolvimento e entrega automatizada do software para o cliente. Entretanto, a **segurança ainda é uma grande preocupação**. Desde o começo da pandemia da covid-19, os **ataques de hackers aos softwares têm crescimento exponencialmente**. Muitas instituições de ensino e pesquisa, e pequenas e médias empresas, **não possuem o know-how tecnológico** para implementar e manter esteiras de desenvolvimento focadas para segurança de código, as chamadas esteiras de DevSecOps.

O DevSecOps é uma prática que **combina os princípios de desenvolvimento de software, segurança e operações** a fim de criar um processo de desenvolvimento de software mais eficiente e seguro. Ele foi projetado para garantir que a **segurança seja integrada ao processo de desenvolvimento de software** desde o início, por meio do uso de automação, testes específicos e outras práticas que visam identificar e abordar potenciais vulnerabilidades de segurança, antes que elas possam ser exploradas por hackers. O objetivo do DevSecOps é **criar um processo de desenvolvimento de software mais seguro e eficiente**, o que pode ajudar a reduzir o risco de ataques cibernéticos e outras ameaças de segurança.

SOLUÇÃO SECDEVIAS

SECDEVIAS – INOVAÇÃO COM RNP

Dessa forma, a solução SecDevias, desenvolvida dentro do **Programa de P&D Serviços Avançados da RNP em 2022**, promete fornecer, dentro de seus serviços, **auto-esteiras de DevSecOps** para qualquer time de desenvolvimento de universidades, centros de pesquisa, e empresas, gerando relatórios de segurança indicando as vulnerabilidades encontradas.

“Essas **auto-esteiras podem ser executadas a cada modificação do código**, inibindo que erros sejam propagados para o ambiente de produção. Bem como, os relatórios são gerados em português, com muita clareza e precisão”, explica Cesar Marcondes, coordenador do SecDevias. “Desse modo, **permite que os desenvolvedores possam corrigir e atualizar os problemas de segurança encontrados** e, conseqüentemente, diminuir a superfície de ataque ao software”.

“OS RELATÓRIOS SÃO
GERADOS EM PORTUGUES,
COM MUITA CLAREZA E
PRECISÃO.

- CESAR MARCONDES, PHD

SOLUÇÃO SECDEVIAS

O MVP foi desenvolvido uma plataforma SaaS (Software como Serviço), que pode ser alimentada de várias formas: desde o desenvolvedor enviar um arquivo compactado com seu código, até mesmo integrar a auto-esteira do SecDevias diretamente no seu ambiente de esteira preferido, Gitlab ou Github.

O MVP realiza então a **varredura de vulnerabilidades nos códigos enviados tratando de vários tipos de “varreduras” de vulnerabilidade, fazendo uma busca holística por problemas de segurança.** Além disso, a ferramenta traz os textos dos relatórios de maneira uniformizada, classificados segundo criticidade e tipo, e esses textos são gerados em português de fácil compreensão. As linguagens de programação suportadas são as mais comuns como Python, Java, Java Script e Microsoft dotNet (.NET). Também foi desenvolvido um dashboard para que o desenvolvedor tenha uma noção temporal e por tipo, sobre as vulnerabilidades.

Os resultados preliminares mostram que o MVP sendo desenvolvido na modalidade SaaS, **tem várias características de segurança de código importantes e que os clientes buscam.** A validação do MVP, bem como formas de viabiliza-lo economicamente, têm sido estudadas e serão colocadas à prova com early adopters.

"Durante o desenvolvimento do MVP, fizemos muitas reuniões com empreendedores (tanto do Brasil quanto de Portugal), diretores de times de desenvolvimento (de empresas privadas e públicas), pessoal de universidades, militares e desenvolvedores de grandes projetos da RNP **para tentar encontrar a aderência correta. E os resultados dos diálogos indicam interesse**", diz Marcondes.

VISÃO DE FUTURO

ROADMAP DE 2023

Em breve, a solução do SecDeviaS irá **expandir seu horizonte de exploração de vulnerabilidades, ao incluir novos testes de segurança dinâmicos (DAST)** nos tipos suportados, bem como outros tipos de **busca semântica por vulnerabilidades**, e busca por problemas de **licenciamento de software**. Finalmente, será explorada a adoção de um **novo recurso da plataforma que faz o aprendizado de máquina profundo das vulnerabilidades e indicação por meio de interpretação**, para mostrar ao programador o local exato no código onde está vulnerável.

Segundo o coordenador do SecDeviaS, os **modelos de aprendizado de máquina são como um "cérebro"** que tenta aprender sobre o mundo através de um conjunto grande de exemplos, como fotos de animais de variadas espécies, desvendando padrões que os diferenciem. "E nesse ínterim, a **inovação em interpretabilidade refere-se à habilidade do modelo tomar decisões assertivas**. Essa interpretação é particularmente importante nos modelos de aprendizado profundo, que podem ser muito complexos e difíceis de entender", complementa.

O projeto é uma parceria entre **RNP, Instituto Tecnológico de Aeronáutica (ITA), Exército Brasileiro, Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO) e a startup Netconn**.

CALL FOR ACTION (POC)

ESTAMOS PROCURANDO INTERESSADOS

No primeiro semestre de 2023, estaremos **em busca de interessados para experimentar o MVP desenvolvido.**

- Se você percebe riscos escondidos no software desenvolvido por seu time?
- Se você pensa que pode ganhar produtividade com melhor entendimento dos riscos no seu software?
- Se desenvolver esteiras não é algo que seu time está capacitado.
- Se os relatórios de ferramentas estrangeiras são difíceis de ler e interpretar.

Se algumas dessas dores fazem parte do seu dia a dia.

Entre em contato por email em: contato@secdevias.com para marcarmos uma reunião.

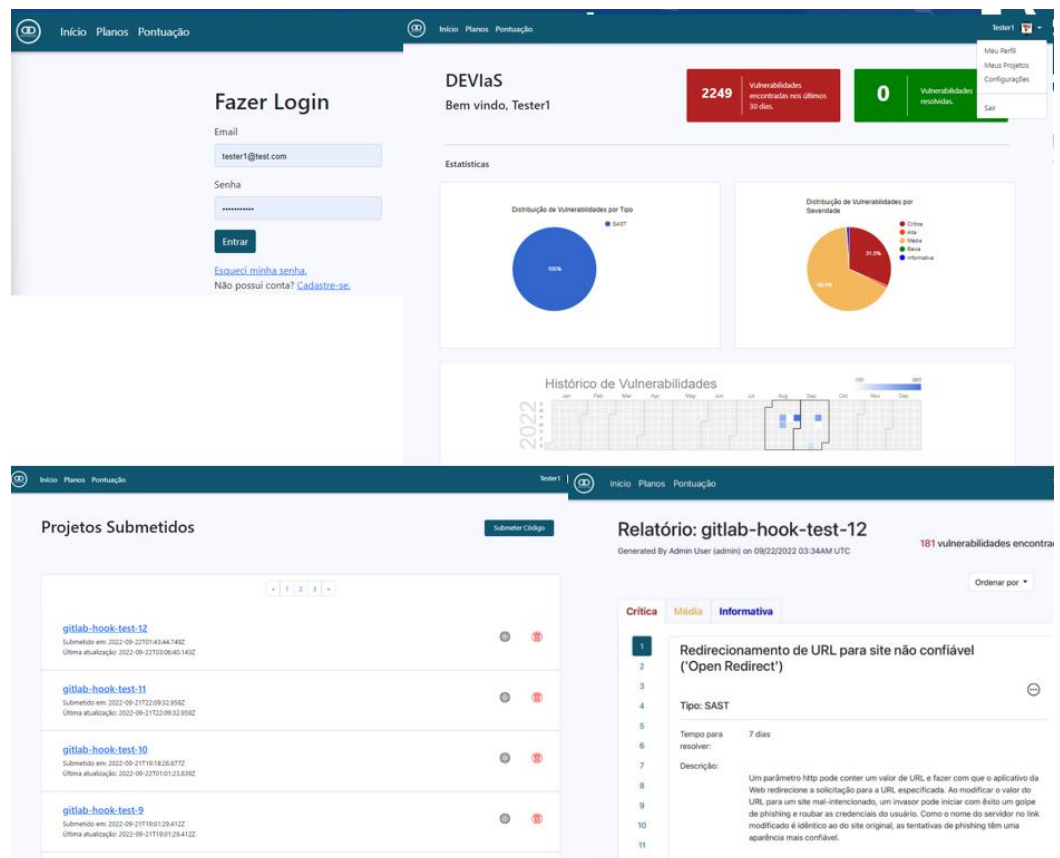


Figura 1 - Screenshots do MVP SecDevias