Proposta para Grupo de Trabalho 2022

DeVIaS - DevSecOps Infrastructure as a Service

Cesar Augusto Cavalheiro Marcondes
Proponente cmarcondes@ita.br

São José dos Campos - SP, 24 de julho de 2021

1 Título

DeVIaS - DevSecOps Infrastructure as a Service

2 Coordenador Acadêmico

Cesar Augusto Cavalheiro Marcondes
Professor do Instituto Tecnológico de Aeronáutica (ITA)
Lattes: http://lattes.cnpq.br/4431183539132719
LinkedIn: https://www.linkedin.com/in/cesarmarcondes/
Google Academico: https://scholar.google.com.br/citations?hl=pt-BR&user=VqUfaJsAAAAJ

Dados de Contato: +55 (16) 997193230 (celular com whatsapp), email: cesar.marcondes@gp.ita.br

3 Assistente de Inovação

Eng. Manuel Correia
Fundador da Netconn Group, executivo de várias empresas TI nos últimos anos e participante da Rede ANSP.br onde foi o responsável pela montagem do seu ecossitema.
Site da Startup: https://www.netconngroup.com.br/
LinkedIn: https://www.linkedin.com/in/mcorreia/
Dados de Contato: +351 913 869 261 (celular com whatsapp), email: mcorreia@gmail.com

4 Tópicos de Interesse

DevOps, DevSecOps, Segurança Cibernética, Desenvolvimento de Software Seguro, Pipelines de Segurança, Análise de Segurança de Código, Computação em Nuvem

5 Parcerias e respectivas contrapartidas

- O Instituto Tecnológico de Aeronáutica (ITA) é uma instituição de ensino superior pública da Força Aérea Brasileira, vinculada ao Departamento de Ciência e Tecnologia Aeroespacial (DCTA), localizado na cidade de São José dos Campos, São Paulo. É considerado uma das melhores instituições de ensino superior do Brasil, com formação em engenharias, incluindo a engenharia da computação. A instituição tem se destacada nos últimos anos na área de segurança cibernética com acordos com empresas e com o Comando de Defesa Cibernético (CComDCiber). O projeto será conduzido no ITA, dando preferencia para a contratação de alunos da instituição.
- O Exercito Brasileiro tem a atividade estratégica de ciberdefesa, através de seus vários órgãos como CDS, ComDCiber e ENADCiber tem prerrogativa de proteger os sistemas de informações e neutralizar a fonte de ataques, tentando inibir possíveis ataques digitais. Integra o Sistema Militar de Defesa Cibernética, que atua em cinco áreas de competência: Doutrina, Operações, Inteligência, Ciência e Tecnologia e Capacitação de Recursos Humanos. Nesse projeto contaremos com a parceria do Tenente Coronel Ricardo Sant'Ana, doutor em computação pelo IME na área de IA para cibersegurança.
- O Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO) é resultante da integração da Escola Técnica Federal de Palmas (ETF) e da Escola Agrotécnica Federal de Araguatins (Eafa), e foi criado por meio da Lei nº 11.892/2008, que instituiu a Rede Federal de Educação Profissional, Científica e Tecnológica. O aluno de doutorado Emerson Barea, atua no Campus Palmas onde oferta ensino médio integrado a cursos técnicos, e cursos técnicos separados concomitantes ou subsequentes ao ensino médio, e cursos superiores nas áreas de informática. Tendo atuado na área de testbeds, nuvem e defesa cibernética no doutorado.

As 3 instituições de ensino e pesquisa serão co-responsáveis pelo design do produto, enquanto a NetConn Group será responsável pela divulgação e comercialização. A NetConn Group vai dedicar horas de trabalho nessas atividades, a custo zero para o projeto.

6 Descrição da Proposta

6.1 Sumário Executivo

Além de fatos anteriores relativos a ataques cibernéticos via sistemas implantados em empresas e entidades, um destaque ocorreu em 2020, que além de ser o ano de pandemia de COVID-19, também foi quando os ataques cibernéticos proliferaram, centenas de ataques de ramsomware ocorreram, milhares de vazamentos de dados foram detectados e, quando parecia que os hackers iam dar uma trégua no final do ano, um dos maiores ataques cibernéticos da história estava para acontecer: o ataque à SolarWinds. Tratou-se do primeiro caso concreto de ataque na chamada cyber supply chain, ou na cadeia de fornecimento do software que é usado por 4/5 das empresas do Fortune 500. A linha de produto deles foi modificada e o software "oficial" - agora modificado - passou a ter um backdoor para hackers, que passaram a ter acesso a milhares de empresas nos EUA e mihares países na Europa, Asia e Latam.

Observa-se que o mundo está mudando rapidamente e a área de desenvolvimento seguro é uma clara necessidade de todos [1]. Estima-se[1] que metade das aplicações vulneráveis hoje em dia não tenham adotado nenhuma abordagem de desenvolvimento seguro, com esteiras automatizadas. Esse é um mercado estimado de USD 15,9 bilhões em 2027, com uma taxa de crescimento composto anual de 30,24%. Sendo que, mais de 68% das empresas em 2022, planejam incluir iniciativas de análise de vulnerabilidades de software de maneira automatizada nos seus processos, porém existe uma grande barreira, pois a maioria dos executivos - 71% dos CISOs - sentem alto risco de colocar recursos nessa área porque a segurança pode impedir a velocidade dos processos normais da empresa.

Dado todo este panorama, de crescimento rápido, mas simultaneamente, medo de que não exista maturidade suficiente nas empresas para processos de esteiras de checagem de segurança de software, esta nossa proposta de projeto de inovação ligada a uma startup, traz a possibilidade de racionalizar os testes de software seguro, por um processo todo automatizado em nuvem, que permita melhor aconselhar os desenvolvedores a tomarem atitudes para fortalecer a segurança de seus sistemas.

Em especial, no ambiente brasileiro, em uma universidade típica, ligada ao ecossistema da RNP, os times de TI de desenvolvimento e infraestrutura ainda não fizeram o passo para a migração do modelo de DevOps para um modelo DevSecOps, que considera aspectos de segurança durante todo processo de desenvolvimento. Os programas acadêmicos, portais das universidades, sistemas de notas, a maioria, em geral, licitados por funcionalidades, não passam por um pente fino de segurança ou simplesmente não foram desenvolvidos considerando a segurança durante todo o processo de desenvolvimento. Assim, uma plataforma de nuvem que a RNP poderá oferecer para seu ecosistema, trará qualidade e desprendimento no processo, fazendo com que sistemas possam ser colocados em uma esteira e seja produzido relatórios em bom português, com exemplos de solução e auditoria do processo, via nuvem o que trará reais benefícios. Estes serviços então, poderão ser utilizados pelos times de programadores das universidades, para consertar as falhas de segurança encontradas, aumentando a resistência a ataques cibernéticos do ecossistema da RNP como um todo.

Em um segundo momento, o projeto pode ser oferecido para entidades de apoio às empresas para fornecer aos seus associados, pequenas e médias empresas, a solução de DevSecOps em nuvem, objeto deste

[1] https://www.veritis.com/blog/14-statistics-that-shed-light-upon-devsecops-opportunities-and-challenges/

projeto, e assim proporcionar melhor a segurança cibernética nacional através do fortalecimento do elo mais fraco, os pequenos empresários que não conseguem contratar pessoal qualificado para construir esteiras de segurança ou mesmo para fazer um pente fino em software que eles produzem ou façam uso. Todos esses cenários são de aplicação da DeVIaS, a plataforma de DevSecOps as as Service que será desenvolvida neste projeto, com excelente potencial social - de melhoria das empresas e seus software e também mercadológico através de um oferecimento freemium, onde os produtos pagos subsidiam produtos grátis para universidades e empresas sem recursos.

No restante do documento serão detalhados aspectos técnicos do produto minimamente viável, também será realizada uma pequena análise de mercado e como será viabilizada a plataforma e os recursos a serem utilizados no projeto.

6.2 Desenvolvimento Tecnológico

A solução DeVIaS é uma solução que fornece, dentro de seus serviços, relatórios de segurança indicando as vulnerabilidades encontradas permitindo, portanto, que estes desenvolvedores possam corrigir e atualizar os problemas de segurança encontrados e, consequentemente, diminuir a superfície de ataque ao software.

Esta solução é composta por 05 (cinco) componentes:

1. Portal WEB;
2. Componente de transferência de código;
3. Pipelines de ferramentas de análise de segurança de código para as principais linguagens de programação como Java, Python e Javascript); 4. Componente de integração de relatórios;
5. Componente de registro de análise.

É importante destacar que estes componentes poderao evoluir de forma a atender necessidades específicas para as entidades alvo, algo a ser tratados posteriormente com a equipe da RNP.

O primeiro componente, Portal WEB, é a interface de comunicação com o usuário. Por meio do Portal WEB o usuário pode submeter um link do repositório do código fonte a ser analisado e obter, como resposta, o relatório da análise de segurança do código. Com este relatório em mãos, o programador pode ser capaz de atualizar e corrigir seu software e, potencialmente, produzir versões de software mais seguras. Conforme veremos no plano de negócios, há dois planos possíveis para os usuários: um plano gratuito, onde há limite do número de linhas máximo de código a ser analisado e também limite máximo de tempo/uso da infraestrutura de nuvem destinada a produzir os relatórios, e os planos pagos, em que, estes limites são bastante ampliados.

Os links de respositórios de códigos devem ser padronizados e devem permitir acesso de maneira uniforme. Uma possibilidade é a definição do github como repositório padrão. A partir do link do repositório de código fonte fornecido pelo usuário, o Componente de transferência de código, irá realizar a transferência do código do repositório para o servidor de análise. Este componente é responsável também por realizar a contagem da quantidade de linhas de código a ser analisada, estimar a quantidade de recursos de TI necessárias e identificar as linguagens de programação utilizadas no código fonte. Com estas informações, o componente poderá verificar as estes valores estão de acordo com o tipo de plano do usuário.

A partir de então, um pipeline utilizando-se de infraestrutura de nuvem e alocado de maneira optimizada, é acionado para que a análise de segurança do código seja realizada. Numa primeira versão do DeVIaS, as linguagens de programação mais comuns como Java e Python estarão implementadas para análise no pipeline em versões específicas. Estas linguagens e versões podem ser expandidas em versões futuras da

solução. As ferramentas instaladas de análise de segurança estarão no estado da arte e serão, em primeiro momento, somente open source. No futuro, poderá ser incorporado ao pipeline ferramentas pagas, para clientes de maior valor, onde estas poderão ser executadas em appliances específicos com licenças de uso, como por exemplo o Fortify Cloud Offering por meio do modelo de marketplace da nuvem.

Conforme as ferramentas do pipeline forem gerando relatórios de segurança, o componente de integração de relatórios, quarto componente, recebe estes resultados para processamento. Este componente é responsável por diversos processamentos a serem realizados nas informações dos relatórios:

- Tradução do relatório para português: é sabido que grande parte dos programadores e desenvolvedores, brasileiros e portugueses, não tem pleno conhecimento de inglês e, portanto, a tradução dos relatórios para português traz benefícios para os desenvolvedores que são responsáveis em realizar a correção do código ao deixar o mesmo mais acessível. Adicionalmente a isso, os relatórios de vulnerabilidades são muito sobrecarregados de informações técnicas que exigem um pré-conhecimento de áreas de segurança, a ideia também é aliviar nessa curva de aprendizado. Finalmente, embora partes de texto possam ter sido traduzidas previamente, a todo momento existem atualizações nas vulnerabilidades sendo descobertas e, portanto, é necessário um processo de tradução não somente offline, como também online, fazendo-se uso de Google Translate API, por exemplo;

- Consulta a um banco de dados de exemplos: é comum que os problemas de segurança apresentados em relatórios de segurança das diversas ferramentas contenha informação confusa, fazendo com que o desenvolvedor não saiba como corrigir o problema. Assim, uma base de dados com textos mais orientativos e exemplos práticos de correção será desenvolvida e, estas informações serão adicionadas à versão em português do relatório para cada problema encontrado. Desta forma, espera-se que o resultado final seja um relatório mais claro do problema encontrado, permitindo que os desenvolvedores possam focar mais esforços no desenvolvimento da solução em si e menos esforço na correção do código. Observando-se que apesar das ferramentas SAST - Static Application Security Testing, como o SonarQube, e DAST - Dynamic Application Security Testing, como o OWASP ZAP, normalmente oferecerem este tipo de feedback, seu conteúdo é predominantemente composto apenas pela indicação do problema com sugestões superficiais de resolução, sem exemplos de códigos ou dados orientativos que possam ser implementados de forma literal pelo desenvolvedor da aplicação. Futuramente, pretende-se testar o uso de inovações como o Github CoPilot para especificar em linguagem natural os aspectos de segurança e ele automaticamente gerar código fonte atendendo aquela necessidade;
- Disponibilização de função de feedback: por meio desta funcionalidade, o desenvolvedor poderá informar se as informações apresentadas em cada item do relatório, texto, orientação e exemplo, foi útil ou não (de 1 a 5). Desta forma, com este feedback, é possível avaliar os pontos fracos da tradução, do texto orientativo e dos exemplos de forma a permitir melhorias em novas versões do DeVIaS. O feedback pode alimentar uma rede de aprendizado por reforço que, automaticamente, poderá escolher dentre os diversos textos orientativos e exemplos, aqueles que melhor respondem a um problema de segurança encontrado. Além desse feedback do qualidade da tradução e do relatório em si, também pretende-se adicionar um feedback do processo: para toda aplicação que passar pela análise será feita uma "assinatura" da mesma com a finalidade de permitir identificar o que mudou entre as submissões, de modo a comparar se as sugestões dadas anteriormente foram utilizadas pelo desenvolvedor. Portanto, verificando se a sugestão resolveu definitivamente a vulnerabilidade e/ou não gerou outro problema no código. Com essas informações, pode-se aumentar o banco de dados de soluções e também manter um ranking das sugestões mais utilizadas e o quanto essas sugestões representam de melhora nas aplicações.

Finalmente, o componente de registro de análise de segurança poderá ser feito em uma blockchain utilizando um smart contract. A intenção é registrar cada fase do proceso de criação do software, que ficará registrado por meio de chaves criptograficas, começando pela chave criptografica do desenvolvedor, assinando o hash do commit do código, após isso, no processo do pipeline a máquina virtual que será a executora dos testes de segurança será criada de uma maneira limpa, como uma imagem fixa, calculando e salvando o hash dela, e finalmente, no final do processo os entregáveis (relatórios, sugestões de código etc) também serão resumidos por hashs criptográficos. E tudo isso, submetido a uma blockchain pública como o Ethereum. Desta forma, futuramente será possível auditar o processo de análise de código e, por exemplo, responder se uma determinada vulnerabilidade encontrada hoje, tinha sido analisada no código na versão 2.0 do DeVIaS já era conhecida na versão 1.0 do DeVIaS. Isso traz confiança ao processo de análise de segurança de código, pois o cliente terá transparência sobre a real efetividade das ferramentas. Outro aspecto interessante é que na blockchain pública estas informações serão encadeadas por meio de uma arvore merkle, árvore criptográfica de encadeamento, de modo a manter uma evolução histórica do código, sendo que cada nó da árvore merkle é formada por uma tupla contendo essas informações criptograficas geradas em cada teste, parecido com os nós da blockchain Bitcoin.

Assim, a inovação do projeto DeVIaS acontece em diversos momentos: (1) ao disponibilizar para os desenvolvedores as diversas ferramentas de análise de segurança já instaladas e atualizadas para as linguagens de programação mais comuns; (2) ao gerar um relatório em português, dando maior acessibilidade ao mesmo; (3) ao disponibilizar uma base de dados de textos orientativos e de exemplos de correção; (4) ao implementar um componente de feedback para melhoria do sistema; (5) ao realizar o registro da análise para auditoria. Vale ressaltar que estas inovações serão implementadas a baixo custo e de forma flexível permitindo que atualizações sejam realizadas.

Ao ser finalizado o MVP deste projeto, teremos um ambiente escalável, desenvolvido em termos de infraestrutura como código e que produzirá a partir de serviços, relatórios, feedback e validação de alta qualidade para os usuários. Entretanto, na etapa inicial do MVP e devido a limitações de orçamento e escopo, o MVP será baseado em um conjunto mínimo de linguagens (python e java) devido a sua enorme popularidade. Entretanto, no roadmap do produto, pretende-se incluir outras linguagens igualmente interessantes com foco na área de desenvolvimento web, como php, javascript e mesmo linguagens como C, C++, C# e Ruby. Além da incorporação de novas linguagens, outro processo para ser incluído é na criação automática de imagens docker para o código do cliente, já com todo o endurecimento de segurança para containers. Desse modo, realizando a análise estática do código de Dockerfile para proteção da imagem e execução da mesma.

Outro plano, para a evolução futura do produto, está nos casos onde o cliente não pode, por política da sua empresa, colocar o seu código disponível via interface web no MVP (em um github, por exemplo) como empresas médias fintechs ou empresas que lidam com crédito via BACEN. Nestes casos, a solução estará na criação de uma imagem criptografada do produto para distribuição remota nas máquinas do cliente. Os detalhes da construção dessa sandbox passam pela preparação de um distro Linux que possa ter o disco parcialmente criptografado e com acesso restrito ao núcleo do produto. Deste modo, é possível realizar o processamento offline do pipeline de segurança e obter o relatório de segurança. Essa imagem criptografada precisará ser produzida como uma golden image específica para cada cliente, com toda a validação por hash, e deverá rodar em ambientes virtuais enterprise baseados em VMWare, Virtualbox, Hyper-V, entre outros. Outro ponto importante é ter uma conexão criptográfica forte, com certificado válido e endereço DNS fixo, para realizar a atualização, sendo o mesmo configurável no proxy da empresa. A imagem em execução, no final do processo, se tornará, um agente específico do pipeline com interface web, para execução exclusiva daquele cliente. Finalmente, isso terá implicações no design da inteligencia do software, pois, certas técnicas de feedback terão somente informação local para tomar decisões.

6.3 Modelo de Negócios

Com o grande crescimento do uso de TIC, nos últimos anos, pelas universidades e pequenas e médias empresas, a aquisição de sistemas bem como o desenvolvimento interno, traz a tona os assuntos fundamentais de eficácia, desempenho, rapidez de entrega e de implementação de segurança. Se este processo não for cuidadoso, metódico e objetivo a empresa certamente terá problemas com relação ao desempenho final, escalabilidade, bugs, correções, evoluções e segurança do programa implantado. Por outro lado, também o foco é o ecossistema da RNP, universidades e entidades, distribuídos, em todo o país, utilizam-se de sistemas onde cada Universidade pode gerenciar e operar adequadamente suas áreas de atuação. Existem várias metodologias para garantir os itens acima citados, em termos de sistemas de informação, as quais são usadas pelas grandes organizações e uma delas é a abordagem DevSecOps (Desenvolvimento e Operação Segura). Entretanto, além do foco básico, é essencial e fundamental, em termos de benefícios para a sociedade, que tal abordagem, seja estendida às Médias-Pequenas empresas, bem como as Universidades onde a RNP presta serviços, tudo isso a custos adequados e facilidade de uso.

Este é o objetivo da metodologia de DevSecOps que, através da aplicação de ferramentas de software estruturadas em um processo inteligente, garantem a entrega segura e em tempo real do produto de TIC originalmente pretendido. A implantação de DevSecOps inclui sempre produtos e serviços para a execução dessa metodologia. A união de pesquisadores de Universidades Brasileiras (ITA, IFTO e EB) , em conjunto com a startup Netconn Group, especializada na interação Universidade - Empresas, tem como objetivo maior o desenvolvimento de um produto-serviço dificilmente encontrado a nível Brasil e mundo, que possa atender a RNP e seu ecossistema, bem como as médias empresas brasileiras, ambas carentes desse tipo de produto para garantir o desenvolvimento rápido, contínuo e seguro de suas aplicações. Dessa maneira o produto a ser desenvolvido, focado no modelo SaaS, em arquitetura na nuvem RNP, irá fornecer às empresas e Universidades parceiras, uma visão consolidada de segurança da sua aplicação, utilizando todo o poder das tecnologias de SAST (static application security testing), SCA (software composition analysis) e DAST (dynamic analysis security testing) combinadas em uma única análise. Além disso, modelos de licenças de uso e em arquitetura on-premises poderão ser considerados. Com isso se pode gerenciar as vulnerabilidades encontradas, armazenar as evidências e possibilitar o trabalho colaborativo na correção de problemas.

No surgimento de alguma vulnerabilidade adicional, o produto poderá interromper o desenvolvimento e entrega da fase em questão e notificar o usuário para que se possa corrigir a mesma antes dela seguir para a fase de produção. Ressaltamos que procuramos inserir nesta pesquisa outros itens que atualmente estão crescendo na área de pesquisa, tais como blockchain, desenvolvimento seguro, IA, processamento nuvem sob-demanda. Isso possibilita que produtos agregados, usando estas tecnologias, sejam desenvolvidos no futuro pelo time atual ou outros times de pesquisa envolvidos com a RNP.

A nossa proposta de valor, orientada para as Universidades e Médias empresas, é fornecer um produto e vários serviços complementares, para que os programas e sistemas desenvolvidos pelas Universidades e Médias empresas sejam testados via nuvem, na modalidade SaaS, e cujo resultado propiciará às entidades acima, orientações para sua correção e otimização a um preço atrativoadequado, para o público alvo, sem similar atualmente no Brasil, pois hoje temos soluções focadas para grandes empresas, onde o preço e as condições tornam-se inviáveis para o público alvo dessa proposta.

Metricas	Universidades Federais e Estaduais Brasil	Empresas micro e médias no Brasil (Sebrae)
Quantidade	100	aprox. 6 milhões
Repositórios Mantidos	20/universidade	10/micro, 100/média
Necessidade mensal testes de pipeline	40.000	600.000 (mix)

Tabela 1: Tamanho do Mercado Potencial

Para uma análise mercadológica inicial, o tamanho do mercado pode ser medido usando-se dados do ecossistema da RNP e de Entidades a serem escolhidas de apoio à pequena-média empresa, conforme Tabela 1. Com base nessa base de potenciais clientes, foi pensado em algumas possibilidades de Modelo de Negócios a serem definidas em conjunto com a RNP, como na composição de um serviço FREEMIUM, onde alguns usuários podem executar o produto FREE, por tempo limitado, e o valor dos demais serviços compensa o FREE e gera lucro. Portanto, esses serviços são explicitados na seguinte oferta na Tabela 2. Multiplicando-se as tabelas 1 e 2 tem-se uma ideia de potencial de faturamento.

FREE (temporário 30 dias)	STANDARD: R$ 80,00/mês(*)	PREMIUM: R$ 150,00/mês(**)
Aplicações: 1 / Usuários: 1	Aplicações: 3 / Usuários: 5	Aplicações: 6 / Usuários: 10
Max Linhas p/App: 100.000	Max Linhas p/App: 150.000	Max Linhas p/App: 300.000
Max Pipelines p/Mes: 10	Max Pipelines p/Mes: 30	Max Pipelines p/Mes: 60

Tabela 2: Freemium e Serviços Pagos.

(*) e (**): a intenção é que os valores sejam posteriormente definidos em conjunto com a RNP,mas o objetivo é que sejam baixos e que assim se possa atingir um número elevado de empresas.

Além dos serviços padrão definidos acima, teremos uma categoria ESPECIAL, a ser definido por cada projeto e empresa, variando do número de análises mensais e de linhas de código a serem verificadas. Adicionalmente, serão verificadas, de tempos em tempos, ociosidades que poderão ser ofertadas para entrantes. Finalmente, as possibilidades de entrega do produto deverão ser analisadas em conjunto, no momento oportuno pelos pesquisadores e startup, com a equipe da RNP. Com este enfoque mercadológico poderemos ter um preço baixo, atrativo e adequado para as universidades parceiras da RNP. Além disso, poderemos, no futuro, oferecer o produto e seus serviços associados a Universidades e parcerias internacionais da RNP e organizações focadas nessas relações.

Outros enfoques também podem ser ofertados, como existem vários tipos de empresas e Universidades, em termos de maturidade de TI, a Netconn pretende adicionar ao produto vários serviços que possam trazer benefícios para essas organizações. Podemos destacar alguns desses serviços:

1. Consultoria para a avaliação da maturidade de sua equipe e seus processos fazendo recomendações estratégicas sobre como obter mais valor no desenvolvimento de sistemas.

2. Consultoria para a análise do processo de desenvolvimento, código e infraestrutura recomendando ações para otimizar custos, adoção das melhores práticas em desenvolvimento seguro, testes de qualidade, identificação e proteção de dados.

3. Quando aplicável e necessário, e se houver interesse, por parte da Universidade ou Média empresa, apoiar na implementação de vários itens de gestão, controle e operação.

Tendo em vista a importância deste tipo de projeto para o mercado, quer academico, quer empresarial (foco na média empresa) propomos que a RNP também estude a necessidade de cursos teóricos e práticos de DevSecOps sejam disponibilizados pela RNP na sua plataforma de cursos, desenvolvidos pela NetConn Group. Acreditamos assim que esse Modelo de Negócios para esse produto e serviços seja o apropriado para o mercado alvo citado com as componentes pesquisa, comerciais, técnicas e operacionais adequadas ao mesmo.

7 Ambiente de validação da solução proposta e documentação dos aprendizados

O ambiente de validação é descrito na figura 1. O processo começa com os desenvolvedores fazendo uso de suas ferramentas típicas de gerencia de versionamento de código (SCM, como github) e o usuário submete ao portal Web do DeVIaS. O projeto DeVIaS começa a funcionar a partir do bloco em AZUL chamado "Web Portal Automation Center", que será oferecido pela infraestrutura da RNP em VM conectada à Internet 24/7 (ver alocações de infraestrutura), e possuirá áreas de dashboard por usuário onde ficarão as atualizações dos processos de segurança. Uma vez o usuário fazendo a submissão de um código por meio de URL do github (ou mesmo de um arquivo zipado com o código), acionará os pipelines. Os pipelines executarão em ambiente de cluster próprio no ITA, eles serão desenvolvidos com estratégia infraestrutura como código para facilmente serem escaláveis. No entanto, no futuro, a parte de security pipeline pode ser usando infraestrutura on-demand de uma nuvem, enquanto que o pipeline report pode ser uma infraestrutura reservada em nuvem. Isso ajudará a reduzir custos da execução dos pipelines.

Mostrando mais em detalhes, na figura 1 verificamos que existem 2 pipelines principais: Pipeline de Segurança e Pipeline do Relatório. O ideia do "Security Pipeline" é ser implementado em containers, utilizando de um orquestrador de pipeline como gitlab ou Zuul, e os agentes remotos também serão containers ou mesmo serverless lambda, onde serão executadas dezenas de ferramentas

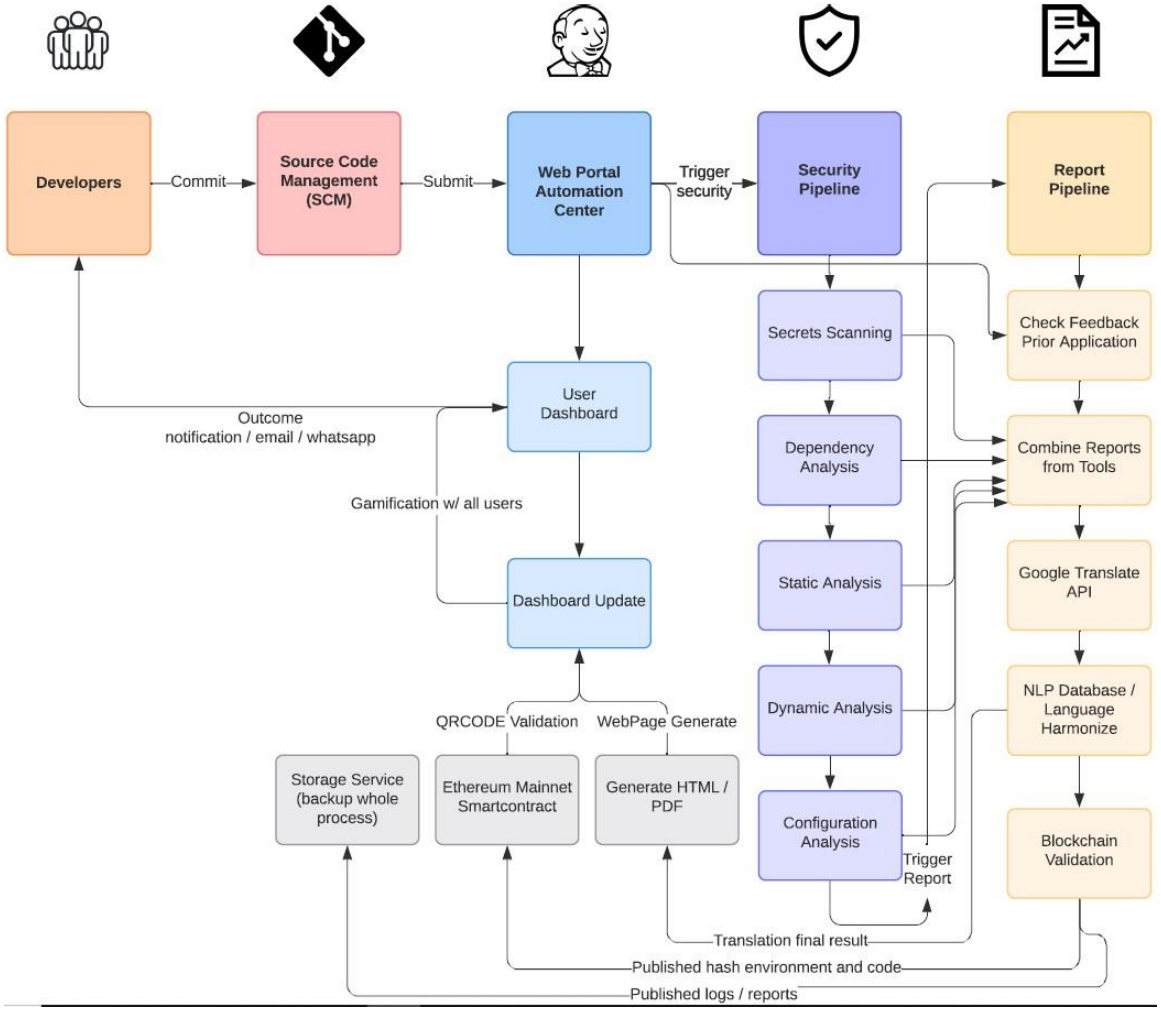

Figura 1: Diagrama do Ambiente de Validação.

opensource, como: trufflehog para a parte de descoberta de senhas no código, OWASP dependency checker para a parte de detecção de vulnerabilidades de dependencias de bibliotecas de código, SonarQube para a análise estática de código, OWASP Zed Attack Proxy (ZAP) e tomcat para a parte de análise dinamica de código, e conjunto de scripts de conformidade NESSUS de configuração, na parte final da análise. Cada processo de segurança produzirá um relatório em formato consumível para o próximo estágio, por exemplo, em formato XML ou JSON.

O “Report Pipeline” também executará no cluster ITA e será composto pelas fases de elaboração do relatório em português, com linguagem clara e incorporação de exemplos de feedback para corrigir os problemas de segurança. A primeira fase do estágio é uma checagem, onde se verificará se o código do usuário incorporou sugestões de uma versão anterior do relatório e pode ser feito por diferenças entre código antigo ou observando-se os commits intermediários. Em seguida, todos os relatórios gerados pelas ferramentas de segurança serão combinados, com um processo de limpeza, de classificação de itens em função da gravidade do erro. Então, o próximo passo envolve acessar uma API do Google Translate para traduzir as partes relevantes dos relatórios e, finalmente, uma etapa onde é acessado um banco de dados dos textos e sugestões a serem incorporados no relatório final. Esse banco de dados e uniformização serão desenvolvidos como um notebook jupyter contendo inteligencia artificial para harmonizar e suavizar a linguagem do relatório final. Esses notebooks jupyter serão convertidos em formato PDF ou HTML para serem incorporados na página web usando Jupyter PaperMill. A última etapa desse pipeline é a validação em blockchain, onde todas as partes (como, chave pública do desenvolvedor - pré-armazenada, hashs das imagens douradas do pipeline, hash do código, hash dos relatórios gerados é incorporado a uma chamada de API para um smartcontract na rede pública da Ethereum.

Os últimos processos, representados em cinza na figura 1, apresentam a consolidação dos pipelines, que não precisam ser acionados em tempo real, e podem ser executados com periodicidade diárias, por exemplo, dependendo do nível de serviço cobrado. Para cada execução do pipeline todos os dados de logs, reports em XML são armazenados para futura melhoria do produto com treinamento de classificadores de IA e Natural Language Processing. O processo de validação na blockchain Ethereum pode levar um tempo de 10 a 15 minutos para realizar o registro de maneira imutável na blockchain. Essa imutabilidade é então registrada e pode ser explorada por ferramentas de Exploração da Chain como etherscan.io, permitindo que se verifique se o processo foi executado de maneira transparente e auditável. Para ficar fácil do cliente verificar os dados, é gerado, ao final do smartcontract, um QRCODE para fácil acesso. Outro componente gera o relatório que é incorporado no site como uma atualização da dashboard do usuário. Dentro do próprio portal web, existirá uma espécie de gamificação onde o usuário vai ganhando pontos de experiencia ao incorporar sugestões do DeVIaS. Esses pontos de experiencia vão aparecendo em um ranking de usuários, como os mais pró-ativos em incorporar melhorias. E finalmente o processo termina notificando o usuário por meio de e-mail ou mensagem instantanea no Whatsapp, por exemplo.

8 Cronograma de marcos

O projeto estará organizado utilizando-se de uma estratégia de desenvolvimento ágil, em 6 sprints. Cada sprint terá duração fixa de 2 meses (60 dias, distribuídos em 8 semanas). No desenvolvimento ágil, cada sprint é composto pelo desenvolvimento, teste e demostração de um conjunto de estórias do produto, os chamados épicos. Para ficar coerente com essa metodologia, algumas estórias dos épicos de períodos mais tardios serão feitas em paralelo, e adiantadas, puxando o mínimo para facilitar a integração das partes e demonstrações mínimas intermediárias. Por exemplo, o portal web poderá demonstrar algumas funcionalidades mínimas de backend, que serão melhor completadas em etapas posteriores. Na tabela na próxima página, descrevemos as principais entregas desses sprints.

É importante ressaltar que poderemos estudar várias antecipacões nas entregas e marcos acima descritos, o qual pretendemos analisar em conjunto com a equipe da RNP.

9 Recursos financeiros

9.1 Pessoal

9.1.1 Equipe alocada com recursos do edital

A equipe de pesquisadores é organizada por pesquisadores especialistas em cibersegurança, das 3 instituições parceiras da Netconn: ITA, EB e IFTO. O coordenador geral é o Cesar Marcondes do Instituto Tecnológico de Aeronáutica, tendo grande experiencia em projetos de P&D. Em seguida destacamos o Tenente Coronel Sant'Ana do Exército Brasileiro, um pioneiro e extremamente qualificado guerreiro cibernético, listado como Jovem Pesquisador 3 com seu doutorado finalizado pelo Instituto Militar de Engenharia (IME). Finalmente, completando a equipe cientifica temos o

Sprint	Descrição do Entregável
#1 Portal Web	Ambiente do Site funcionando com cadastro, login de usuário, autenticação 2FA, e campo de submissão de código (por meio de um upload de arquivo zipado, ou uma URL de site de versionamento como github). Cada usuário terá um dashboard mínimo nesse momento, com as pipelines executados e o link para o relatório gerado.
#2 Reports	Produção de Relatório Único derivado de saídas de múltiplas ferramentas após passar por todas as fases do pipeline. O relatório será mostrado em HTML (na dashboard) e em PDF (para download), consolidado, com marca d'agua, formatado com logo, telas e customizado por usuário.
#3 Translation	Desenvolvimento de engine de tradução automática do relatório, conversão de termos técnicos, explicação suscinta em portugues usando automação com APIs de tradução, ex. Google, no limite do serviço grátis.
#4 Suggestions	Baseando em banco de dados de soluções de problemas de vulnerabilidades, descrições de resoluções no StackOverflow. Incorporação de novas oportunidades como o Github Copilot (programação autonoma). Cada sugestão é incorporada ao relatório, e no caso do usuário ter fornecido acesso ao repositório pode-se fornecer um *pull request*.
#5 Feedback	Checagem se modificações foram realizadas, através da comparação entre execuções do pipeline, como forma de medir a maturidade do usuário. Essa checagem é baseada em diferenças entre *commits* ou armazenamento do código zipado prévio. A medida de maturidade é incorporada ao relatório e ao site como uma gamificação do processo, mostrando o ranking do usuário comparado com os demais.
#6 Blockchain	Adicionar ao relatório e ao site do usuário um QRCode que mostra o conjunto de link na Blockchain Explorer (ex., do Ethereum) onde estão registrados as validações do processo do pipeline.

Emerson Barea, professor do Instituto Federal de Tocantins, atualmente realizando doutorado na área de segurança cibernética através de testbeds de larga escala em containers. O assistente de inovação é o empreendedor, criador da Netconn Group, Sr. Manuel Correia, com sua larga experiencia nacional e internacional em vendas e ex-diretor comercial de empresas de telecomunicações no Brasil. Completando o

time, e ainda a ser definido, foram alocadas bolsas para 2 assistentes de desenvolvimento, do tipo 1 com maior valor por hora, que serão desenvolvedores plenos do projeto.

Nome	Função	Tipo	Data Inicio (d/m/a)	Data fim (d/m/a)	Aloc. hs/mês	Valor M. R$	Total Ano R$
Cesar Marcondes	Coordenador geral	GP	01/01/2022	31/12/2022	40	R$1.960,00	R$23.520,00
Manuel Correia	Ass. de Inovação	GP	01/01/2022	31/12/2022	48	R$ 0.00	R$ 0.00
Ricardo Sant'Ana	Jovem Pesquisador 3	GP	01/01/2022	31/12/2022	40	R$940.00	R$11.280,00
Emerson Barea	Doutorando	GP	01/01/2022	31/12/2022	40	R$900.00	R$10.800,00
a definir	Ass. de desenv. 1	GP	01/01/2022	31/12/2022	160	R$3.600,00	R$43.200,00
a definir	Ass/ de desenv. 1	GP	01/01/2022	31/12/2022	160	R$3.600,00	R$43.200,00
Total (máximo anual R$ 132.000,00)							R$132.000,00

Iremos realizar um processo seletivo dentro das instituições parceiras para selecionar jovens com background mínimo em desenvolvimento seguro e tecnologias de virtualização. Ao longo do processo do desenvolvimento do MVP, o prof. Marcondes disponibilizará ao time, o conteúdo completo do seu curso de Introdução à DevSecOps oferecido pelo ITA, bem como material, labs e experiencias, de suas 2 certificações internacionais de DevSecOps pela empresa Practical DevSecOps [2].

9.2 Infraestrutura

No desenvolvimento do projeto, pretende-se utilizar de cluster próprio do ITA, que possui alguns servidores HP de alto desempenho. Além disso, o grupo possui laptops para os desenvolvedores. Entretanto, temos interesse em utilizar recursos em nuvem para permitir experimentos na Internet pública, demonstrações e testes de carga com infraestrutura virtual da RNP.

9.2.1 IaaS

Foi escolhida dentro do catálogo de infraestrutura de nuvem da RNP [3][4], uma modalidade de máquina virtual relativamente potente, com 4 vCPUs, 14GB de RAM e 50GB disco, para a execução de demonstrações públicas da execução do portal utilizando-se de containers e acionamento remoto do pipeline DevSecOps (no cluster). A VM ficará disponível 24/7 durante um ano.

Categoria	Descrição Config	Mês Ini	Mês Fim	Unid.	Qtd.	Custo M. U. (R$)	Sub em R$ estimado
Servidor Virtual	TIPO 1.4 vCPUs	1	12	1	1	1.192,80	14.313,60
Comunic. Dados	IP Público IPV4	1	12	1	1	30,46	365,52
Comunic. Dados	Trafego Rede	1	12	1	1GB	10,12	121,44
Total							14.800,56

[2] https://www.linkedin.com/in/cesarmarcondes/

[3] https://www.rnp.br/arquivos/documents/Cat%C3%A1logo%20de%20equipamentos%20e%20Servi%C3%A7os%

[4] nuvem%20p%C3%BAblica_IaaS_2021.pdf

9.2.2 Equipamentos, Periféricos e Garantias

O grupo de pesquisa possui cluster com servidores HP de alto desempenho, mas é preciso melhorar a sua capacidade de discos. Portanto, foi realizada uma pesquisa na Internet [5] por um modelo de disco compatível com os equipamentos do grupo.

Modelo	Descrição	Inst. Destino	Qtd.	Valor U. em R$	Sub em R$ estimado
Disco SAS	HP 1.8TB 2,5 SFF 10K RPM Para Servidor 872481-B21	ITA	3	3.222,49	9.667,47
Total					9.667,47

Referências

[1] UR RAHMAN, A. A., AND WILLIAMS, L. Software security in devops: Synthesizing practitioners' perceptions and practices. In Proceedings of the International Workshop on Continuous Software Evolution and Delivery (New York, NY, USA, 2016), CSED '16, Association for Computing Machinery, p. 70–76.

[5] https://www.processtec.com.br/hd-1-8tb-sas-hp-2-5-sff-10k-rpm-para-servidor-872481-b21?origem=gs&gclid=Cj0KCQjwraqHBhDsARIsAKuGZeEkDmX0M_znI40j2jWtu6nnDK5weFW-kaWhxq_9EverFHfzSqV8F0waAjftEALw_ wcB

1. FICHA CADASTRAL DA STARTUP

RAZÃO SOCIAL DA MATRIZ: NETCONN SERVIÇOS LTDA
NOME FANTASIA: NETCONNGROUP

CNPJ: 08.229.397/0001-08	INSCRIÇÃO MUNICIPAL: 4.685.215-8
INSCRIÇÃO ESTADUAL:	INSCRIÇÃO NO CADASTRO NACIONAL DE ATIVIDADES (CNAE): 62.01.5.01

DATA DA FUNDAÇÃO: 2009

CÓDIGO: 02919
RAMO DE ATIVIDADE: Prestação de Serviços Técnicos e de Manutenção de Informática, Promoção e Realização de Eventos E Consultoria.

SITE: WWW.NETCONNGROUP.COM.BR

ENDEREÇO: Rua: Marconi 53 cj 22	Nº53	COMPL.: cj 22

BAIRRO: Republica	CIDADE: São Paulo	UF: SP

CEP: 01047-000	FONE (DDD):011 98208-3723	FAX (DDD):

RAZÃO SOCIAL DA FILIAL: >>>> nao existe filial <<<<<
NOME FANTASIA:

CNPJ:	INSCRIÇÃO MUNICIPAL:
INSCRIÇÃO ESTADUAL:	INSCRIÇÃO NO CADASTRO NACIONAL DE ATIVIDADES (CNAN):

DATA DA FUNDAÇÃO:

CÓDIGO:
RAMO DE ATIVIDADE:

ENDEREÇO:

BAIRRO:	CIDADE:	UF:

CEP:	FONE (DDD):	FAX (DDD):

NOME DO REPRESENTANTE LEGAL:
CARGO DO REPRESENTANTE:
NACIONALIDADE:
ESTADO CIVIL:
FORMAÇÃO:
PROFISSÃO:
RG: ÓRGÃO EMISSOR DO RG:
CPF:
E-MAIL:
ENDEREÇO COMPLETO DO REPRESENTANTE:

2. PRINCIPAIS PRODUTOS

Nome do produto	Descrição
Arquitetura de redes	adequações de redes voz/dados (ANSP,BR ; Telebras ; Unesp ; Unifesp)
Segurança cibernética	varios servicos , em conjunto com parceiro Redbelt > consultoria em seguranca >Threat intelligence >Managed Security Services >Segurança na nuvem >DevSecOps
Apoio na montagem para desenvolvimento de projetos TI em P&D	> inclusão de criptografia nos switches (cliente Datacom) > desenvolvimento do RIS : é uma plataforma SaaS que integra soluçao de : diferentes fabricantes e permite concentrar e correlacionar as informações de segurança necessárias para um plano de ação, viabilizando a gestão do ciclo de vida de vulnerabilidades e incidentes de segurança (Redbelt)
montagem de ecossistema tecnológico TI	> levantamento e montagem de ecossistema, abordagem tecnológica, para várias entidades (cliente : ANSP.BR , Promovetic , etc)
Capacitação	montagem de planos de treinamento específicos para empresas e sua implantação (Exercito Brasileiro, Grupo SDN de varias universidades de SP) etc

3. PRINCIPAIS CLIENTES

Listar os clientes (varios em conjunto com parceiros)

Os principais : Datacom; Telebras; ANSP, Exercito Brasileiro ; UNESP ; UNIFESP ; FAPESP TI, etc

4. RESPONSÁVEL PELAS INFORMAÇÕES
NOME: MANUEL LUIS C F CORREIA linkedin: https://www.linkedin.com/in/mcorreia/
LOCAL E DATA: S.PAULO 26 DE JULHO DE 2021