Desafio Zé Delivery

É nítido que a transformação digital já é uma realidade e não há como evitar os comportamentos que ela afeta no aumento da demanda por tecnologias, ferramentas e metodologias de desenvolvimento de software dentro das empresas. Há de se ressaltar também que com esse aumento, como consequência positiva há uma maior visibilidade da empresa devido à utilização de ferramentas de mercado atuais, em contrapartida, o crescimento de incidentes relacionados à segurança tem sido notado substancialmente à medida que novas tecnologias são implantadas sem o devido cuidado. Este é só um exemplo de que a segurança deve ser considerada e contemplada desde a sua fase inicial de concepção de ideias e requisitos e não somente quando já se encontra em ambiente produtivo.

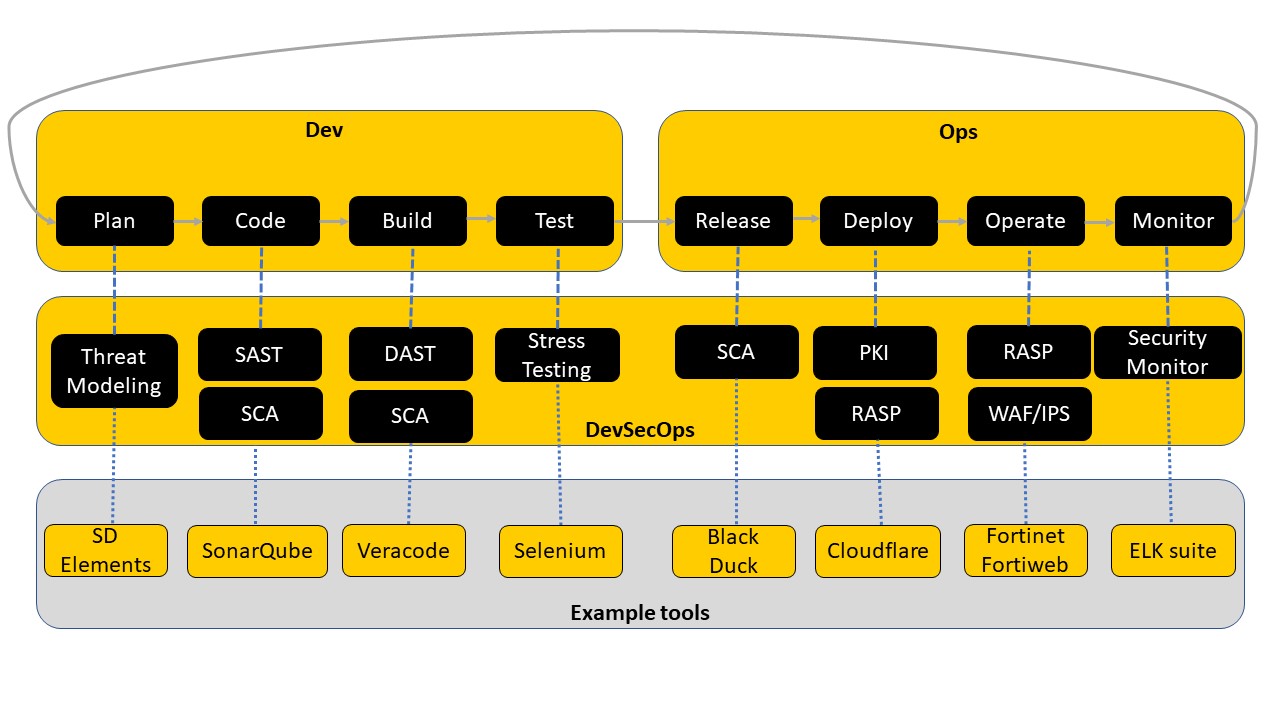
Muitas empresas ainda utilizam uma abordagem reativa, ou seja, somente atuam em demandas de segurança da informação quando são envolvidas por algum incidente ou ataque à algum ativo dela, o que onera e muito os custos para reparação. Para o aplicativo Zé Connect, minha proposta é utilizar o conceito de **Security by Design (SbD)**, a qual aborda de maneira proativa boas práticas de segurança da informação para diminuir o volume e aumento de vulnerabilidades, realizando um follow-up desde a fase de concepção e análise de requisitos até o momento de lançar para produção. Esta abordagem irá proporcionar segurança e adaptabilidade para as novas features, proporcionando integração e harmonia entre os times envolvidos (Marketing, Operações, Negócios, Produto, Desenvolvimento, etc).

Incluído neste mesmo conceito, pode-se aplicar a **Modelagem de Ameaças (Threat Modeling)**, a qual ajudará todo o time na previsibilidade e mapeamento dos cenários possíveis aonde um possível ataque poderá ocorrer, afetando dados sensíveis dos clientes e da companhia. Vale ressaltar que isso poderá ser aplicado não somente no Zé Connect, mas também nos processos (Leis e regulamentações), nas tecnologias (Vulnerabilidades) e nas pessoas (Engenharia Social).

Para que essa transformação ocorra, a companhia deverá ter um engajamento e colaboração de todas as áreas na conscientização de que o dado (dos Clientes, Fornecedores e da própria cia.) é o bem mais valioso que eles deverão se atentar e proteger e colocar os riscos que a LGPD afetará num possível vazamento de dados ou incidente que possa ocorrer. Atualmente, há empresas que fornecem treinamentos de conscientização de segurança para as áreas-chave da companhia, como a **Eskive**, por exemplo. Como alternativa, poderá ser usado também os frameworks que o mercado disponibiliza e aplica-lo e adaptá-lo à necessidade do negócio, como os da **SANS** e **NIST**.

Uma vez os requisitos sendo bem definidos e considerando a segurança como fundamental na sua concepção, os times de desenvolvimento precisam estar alinhados também com essa abordagem. É notável a eficiência de frameworks de mercado quanto a automatização de processos integrados na esteira **CI/CD** de aplicações usando containers num ambiente cloud, então o Zé Delivery também deve surfar nesse momento. Durante o ciclo de desenvolvimento de um software (**SDLC**), a segurança deve ser considerada e poderá ser aplicada usando também a prática de **SecDevOps** numa metodologia ágil. Os guias que a **OWASP** recomenda para desenvolvimento seguro também é uma boa referência para o time atuante, como o **ASVS**, por exemplo. Novos frameworks vêm surgindo para otimizar os processos e falhas de segurança também aparecem como consequência. O Zé Connect sendo o principal produto da companhia, não pode ser um ponto de falha e precisa manter a disponibilidade, escalabilidade e resiliência para os clientes, entregadores e distribuidores.

Abaixo segue uma sugestão de como aplicar técnicas, ferramentas e frameworks de segurança nas etapas de desenvolvimento numa esteira DevOps:



Com a Lei Geral de Proteção de Dados vigorando, o Zé Delivery deve também se adequar ao que se propõe afim de garantir que seu principal produto fique livre de ameaças e possíveis fraudes. Pensando na reputação, na imagem da companhia, seus ativos e os dados gerando valor e informação, este deve ser protegido para que não haja não somente qualquer vazamento, mas também eleve sua maturidade em relação ao mercado. A cibersegurança nesse sentido pode aplicar uma estratégia de defesa em profundidade (**DiD**) como uma forma de mitigar os riscos que possam ocorrer. Mecanismos como **DMZ, Firewall, Hashing e Salting, Autenticação forte baseada em Zero Trust, IPS, VPN, Antivírus e Malware (UTM), DLP** são alguns exemplos de uma boa defesa em profundidade estruturada.

A Zé Delivery deve se preocupar com esses mecanismos de segurança e também possuir um bom plano de resposta de Incidentes para qualquer imprevisto. Um time de **CSIRT** com um SIEM coletando e analisando logs de diversas fontes pode ajudar a prever, detectar e mitigar um possível ataque. Uma forma de evitar retrabalho é utilizar guias e frameworks de mercado para realizar o monitoramento constante de possíveis incidentes, como o **SP-800-61** da **NIST**. Este guia é uma boa referência para realizar a preparação, identificação, contenção, erradicação, recuperação e ao final, rever os processos do que deu certo e errado em lições aprendidas.