Introdução

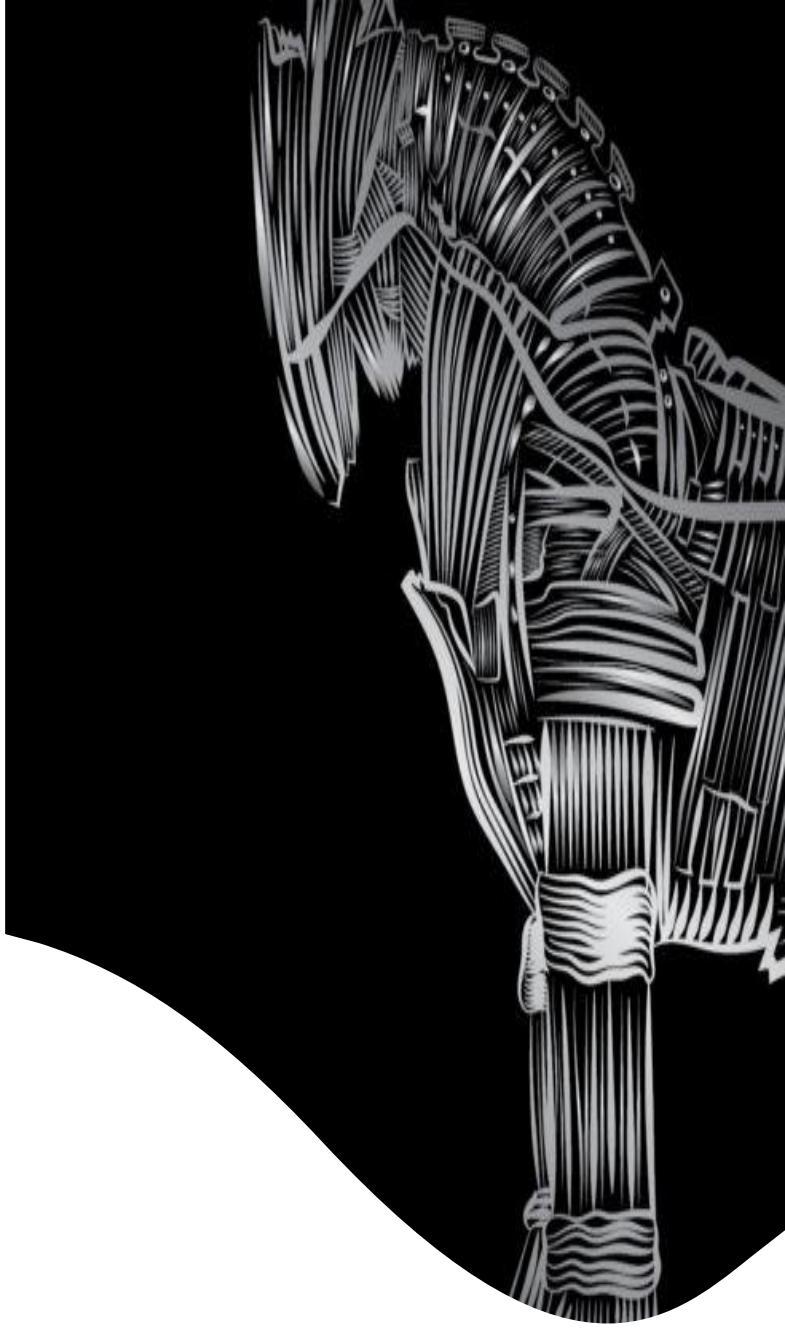
Conceitos gerais

Nossa abordagem

Existem diversos métodos para se modelar de ameaças, mas independente do método, quanto antes ela for aplicada, melhor.

Da modelagem surgem **insights** para o desenho da **arquitetura da solução**, dos **processos de negócio** e, até mesmo, para nortear as escolhas de **tecnologia**. A modelagem de ameaças deve:

1. Prover uma **visão de riscos para a solução sendo desenvolvida**;
2. Prover alinhamento das diversas frentes envolvidas, dentre elas, **área de negócio**, **time de resposta a incidentes**, **time de monitoração**, **desenvolvedores** e **arquitetos de sistemas**;
3. Derivar **requisitos de segurança**, tanto arquiteturais quanto de implementação.



Nossa abordagem

Um dos equívocos mais comuns é a exigência de detalhes técnicos avançados sobre uma solução para se aplicar a modelagem, que começa em **fases iniciais do processo de desenvolvimento**, quando **não estão claros e detalhados uma série de aspectos da solução**.

Uma das coisas sobre a qual se tem clareza quando inicia-se um projeto são os macroprocessos de negócio e os tipos de ativos envolvidos nesse negócio. Portanto, precisamos de um método que **trabalhe melhor com processos de negócio e com insumos macro e tenha a menor exigência de detalhamentos técnicos possível**.

O método de modelagem aqui proposto baseia-se em cenários de ataque. Partindo de "histórias" de desenvolvimento, processos de negócio e do tipo de serviço que se deseja ofertar para o cliente, para criar o modelo de ameaças.