Threat Model Every Story

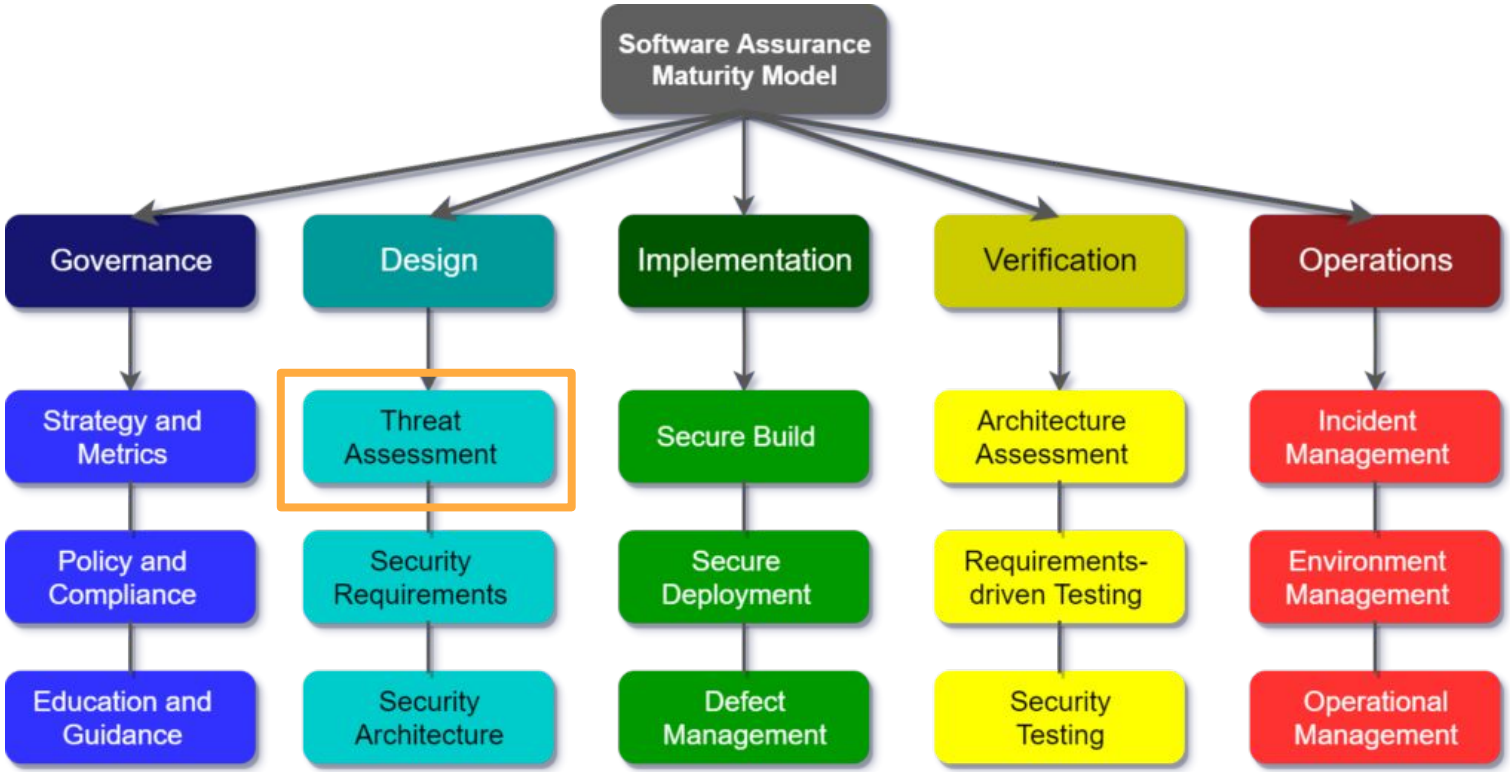
Tiago Zaniquelli
@zani0x03

- Pai da Bia!
- AppSec Specialist na Conviso
- Pós Graduado em Segurança da Informação
- Graduado em Ciência da Computação
- Quase 18 anos atuando como Desenvolvedor de Software
- Apaixonado por Segurança, Desenvolvimento, Software Livre e Métodos Ágeis

O que é modelagem de ameaças?

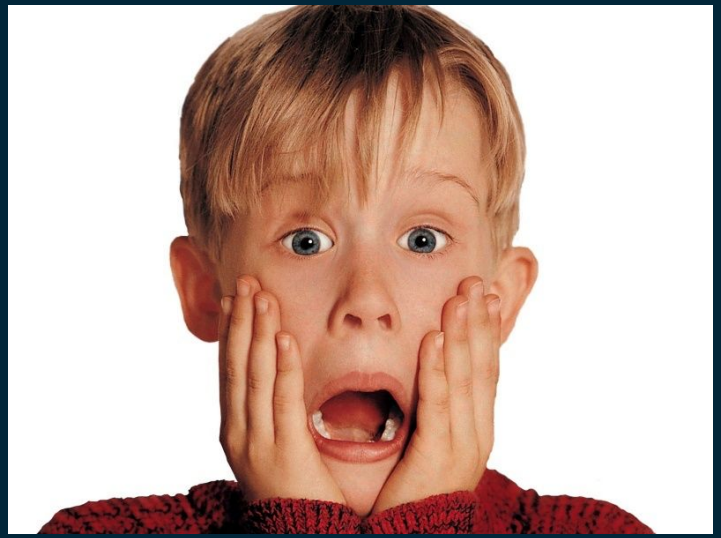
"É uma **técnica efetiva** que ajuda a construir aplicações, sistemas, redes e serviços de **maneira mais segura**. De forma que **identifique ameaças potenciais** e **reduza riscos** estratégicos logo no início do ciclo de desenvolvimento."

OWASP SAMM

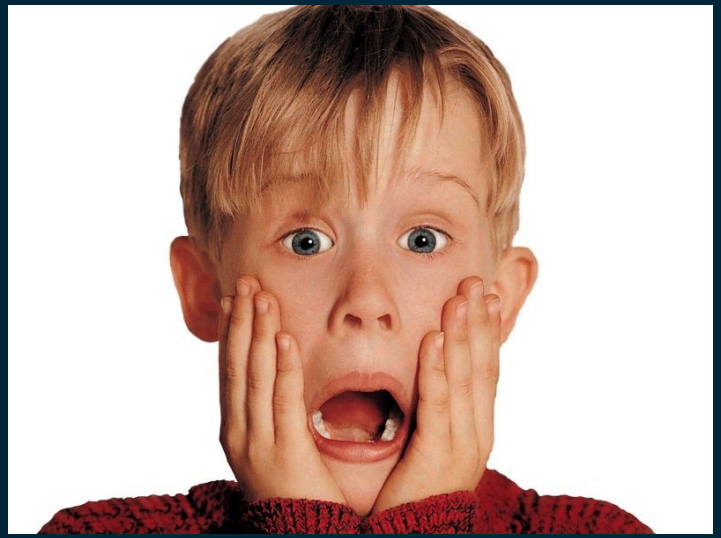

Software Assurance Maturity Model
Governance
Design
Implementation
Verification
Operations
Strategy and Metrics
Policy and Compliance
Education and Guidance
Threat Assessment
Security Requirements
Security Architecture
Secure Build
Secure Deployment
Defect Management
Architecture Assessment
Requirements-driven Testing
Security Testing
Incident Management
Environment Management
Operational Management

Primeira impressão da modelagem de ameaças?

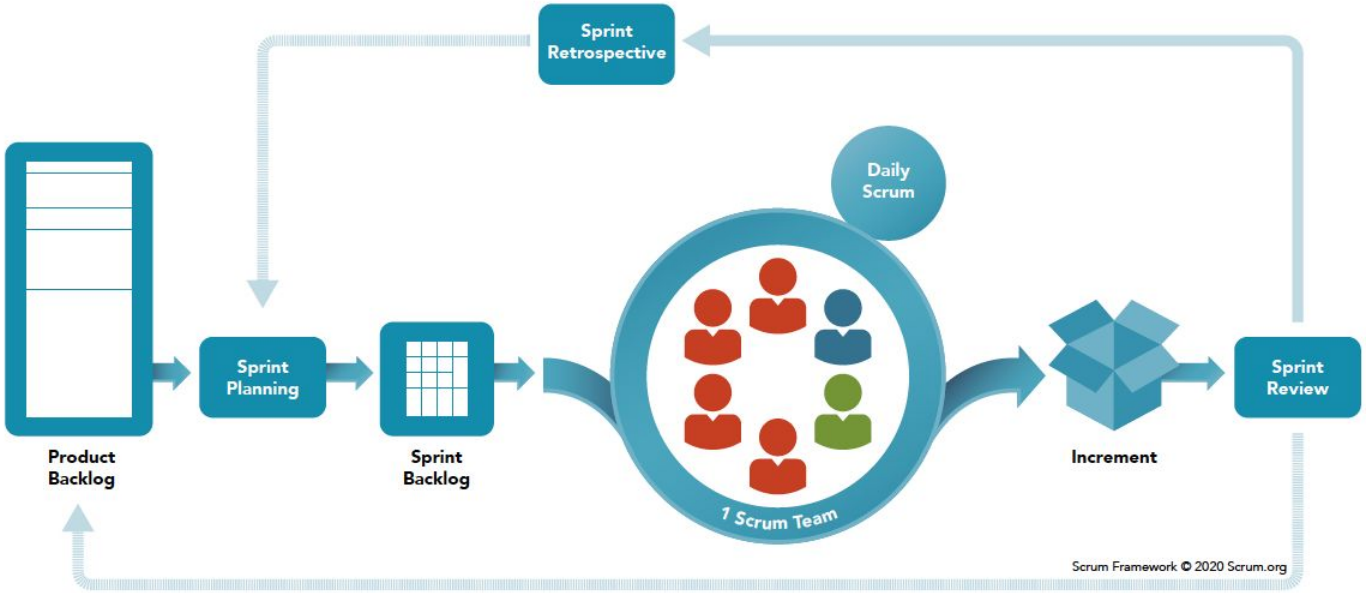
999 requisitos de segurança!



999 requisitos de segurança!

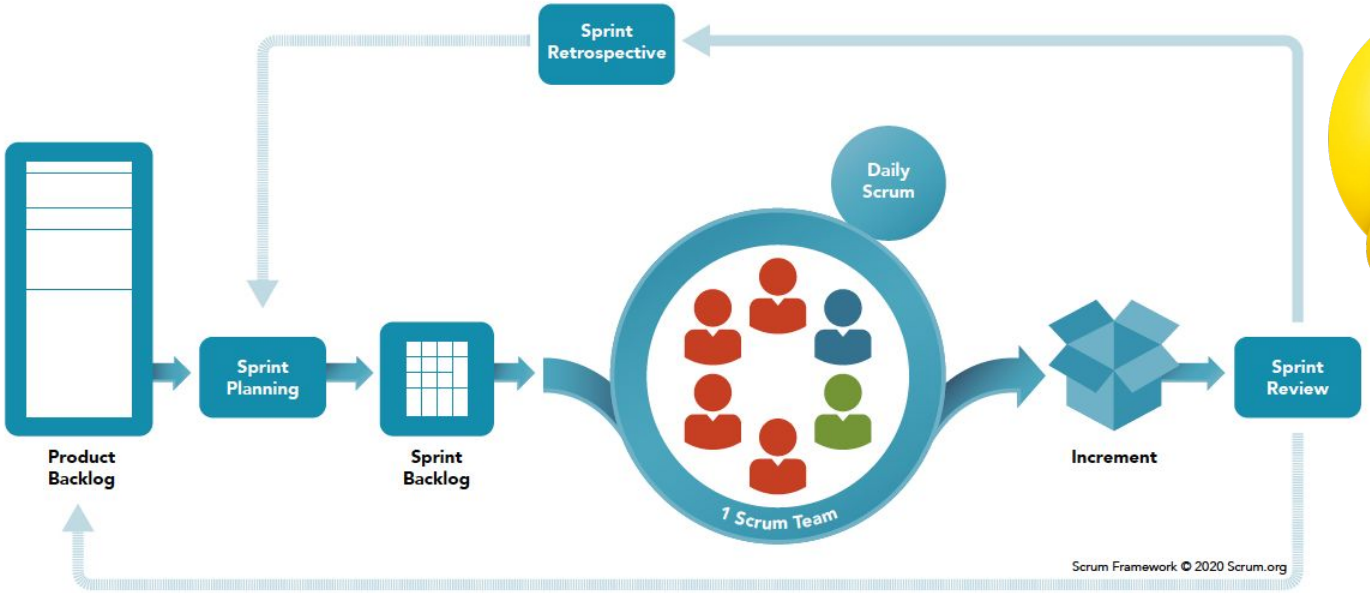


SCRUM FRAMEWORK



Scrum.org

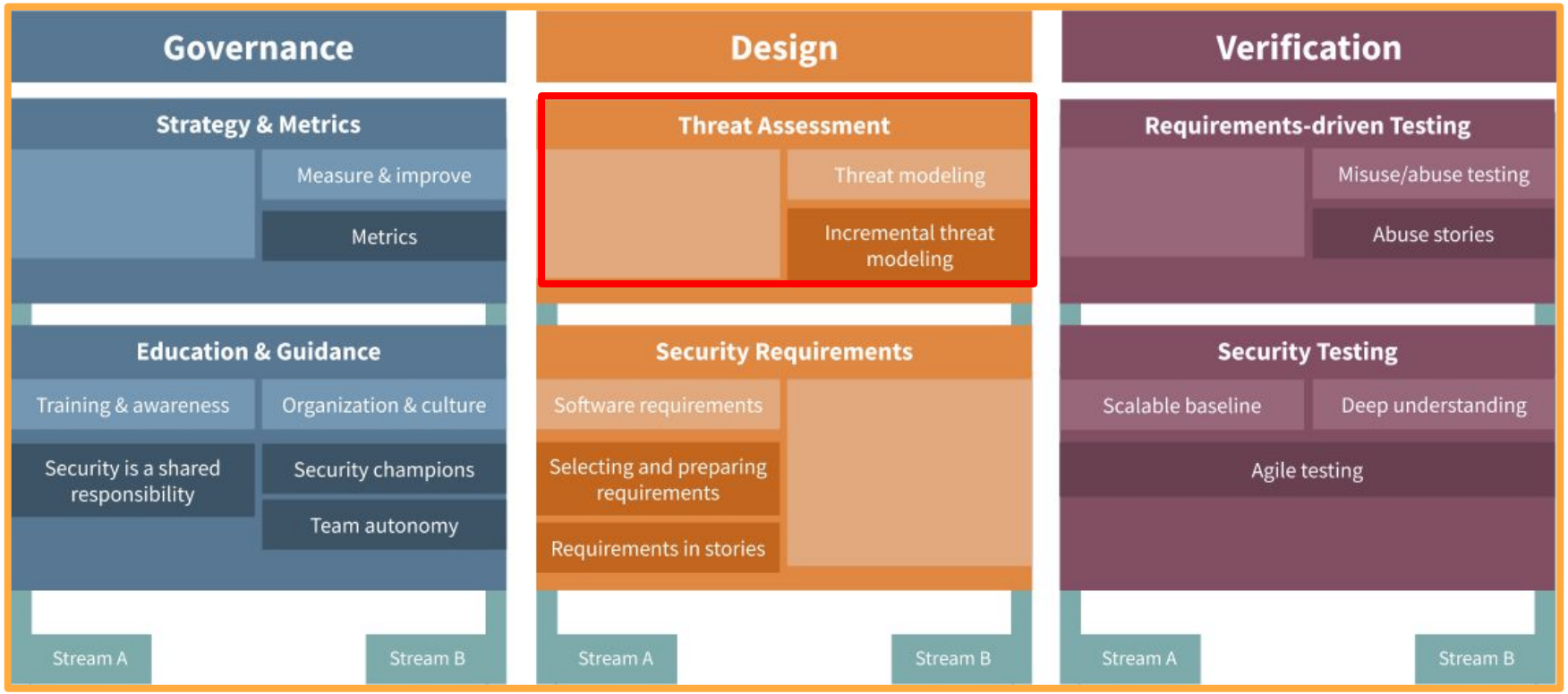
SCRUM FRAMEWORK



Scrum.org

E agora quem poderá
nos ajudar?

OWASP SAMM AGILE



A luta continua...

Tiago Zaniquelli ·

para r.vanderveer

8 de jul. de 2022, 13:16

Hello Rob van der Veer, How are you?

I watched your video (https://www.youtube.com/watch?v=ati80YcVJy8) about Secure Agile Development According To SAMM. I work for Conviso Application Security a Brazilian company that work with AppSec.

So, I thought amazing yout video and I would like to study more about Agile and AppSec.

Do you have any tips for me? What do you indicate to me study about this? Books? Articles? WebSite?

Regards

A luta continua...

Subject: Re: Secure Agile Development According To SAM
Date: Fri, 8 Jul 2022 18:28:21 +0200
From: Rob van der Veer
To: Tiago Zaniquelli <

Hi Tiago,
You could also watch my recent talk on shift left: https://www.youtube.com/watch?v=bxea58oz2RA&t=345
Also OpenCRE might be interesting to you: https://youtu.be/7knF14t0Svg
I love Bruce Schneier's books such as 'Click here to kill everybody'.
Furthermore I recommend these resources:
https://www.youtube.com/c/ContinuousDelivery
https://www.devops-research.com/research.html#capabilities

Good luck!
Software Security is a small community - we'll meet again.
Rob

Modelagem não presta! Parei!

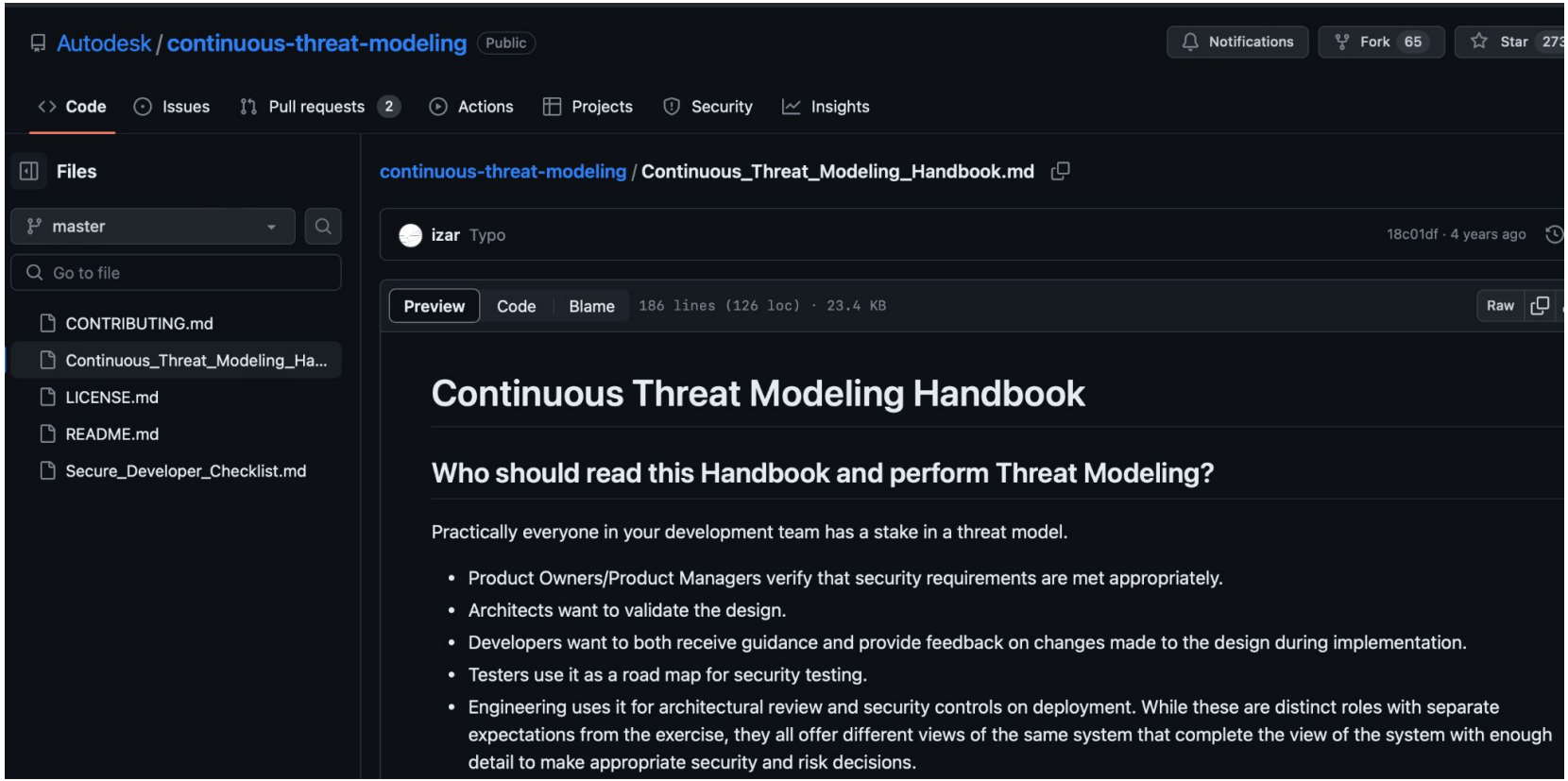
E se pensarmos apenas nos requisitos?

Poxa! Mas modelagem parece ser tão legal

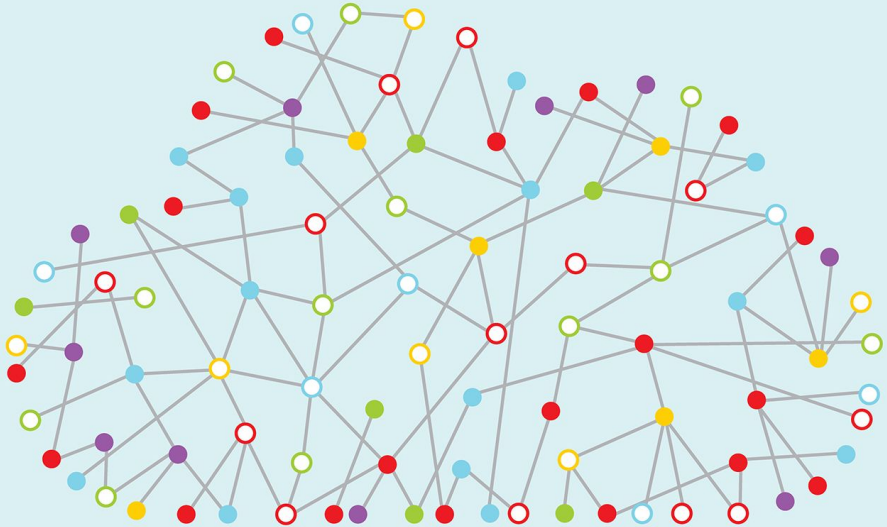
O mundo dá voltas
Não posso mais parar
É só correr atrás
Nem tudo mudou...

O Mundo dá Voltas - CPM22

Threat Model Every Story



Cenário Atual - Muitos sistemas em produção



Motor envenenado
Vou contra o aceitável
Heróis ou rebeldes
Bandeira a meio mastro

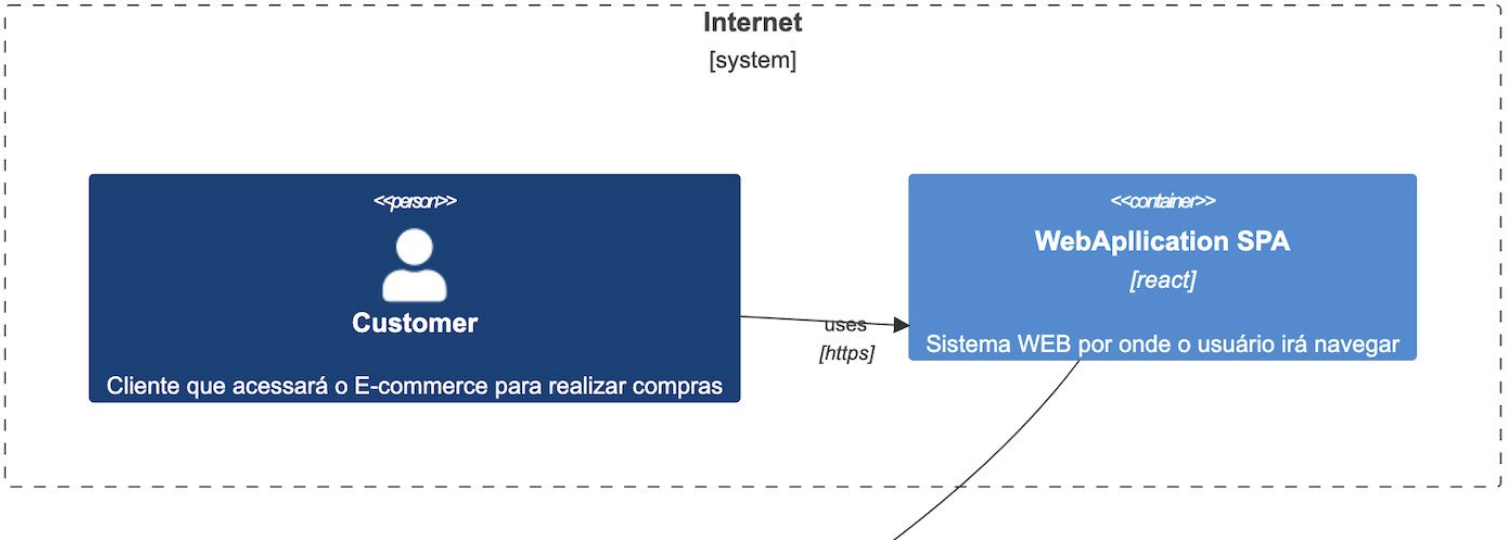
Heróis ou Rebeldes -Blind Pigs

NOVA PROPOSTA

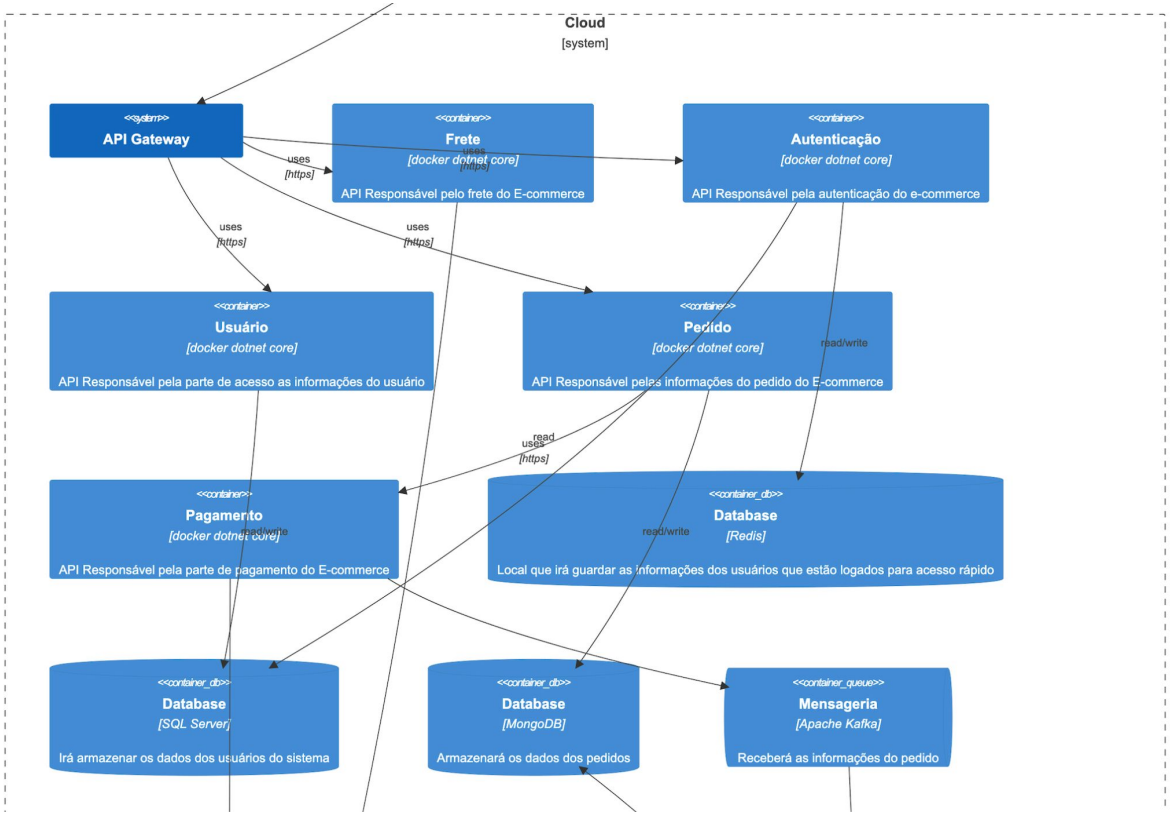
- Primeira modelagem no **TODO**;
- **DREAD** para sinalizar a priorização dos "999 requisitos" gerados;
- Após essa primeira modelagem, **modelagem a cada história**;

talk is cheap
show me the code

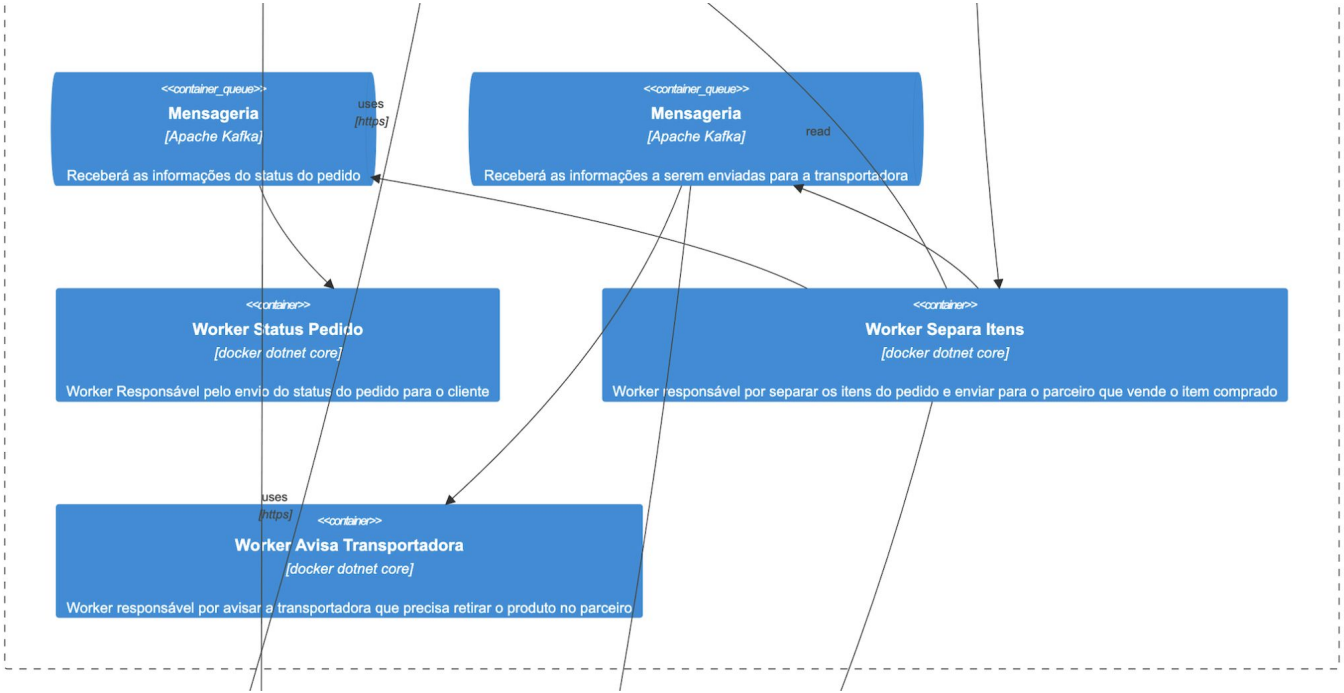
Sistema E-Commerce
Arquitetura



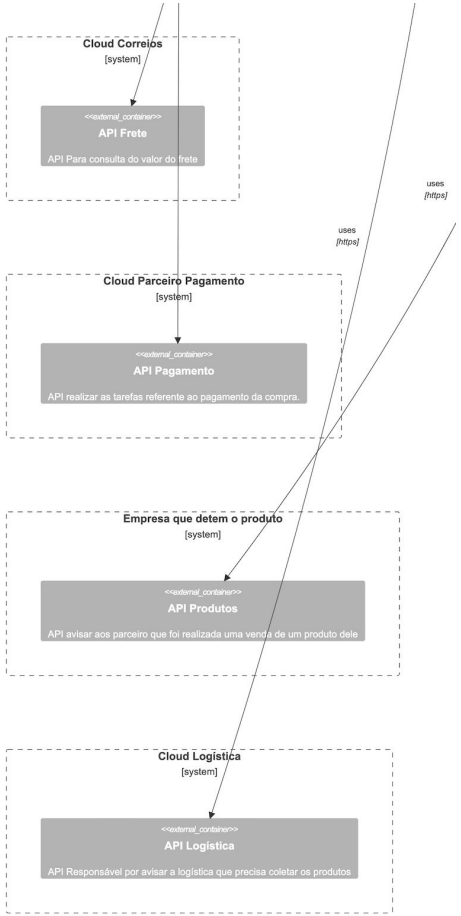
Sistema E-Commerce
Arquitetura



Sistema E-Commerce
Arquitetura



Sistema E-Commerce
Arquitetura



Modelagem de Ameaças "Tradicional"

Modelagem de Ameaças

Ameaças - Ativo Autenticação

Ataque	Capec	CWE
Fuzzing for application mapping	215	532;209
Password Brute Forcing	49	521;262;263;257;654;307;308;309
Authentication Abuse	114	287;1244
Privilege Escalation	233	269;1264;1311;
Use of Known Domain Credentials	560	522;307;308;309;262;263;654;1273

Modelagem de Ameaças

Requisitos de Segurança - Ativo Autenticação

Requisitos de Segurança	CWE
Verify the application only stores session tokens in the browser using secure methods such as appropriately secured cookies (see section 3.4) or HTML 5 session storage.	532
Verify that user set passwords are at least 12 characters in length (after multiple spaces are combined). (C6)	521
Verify that passwords of at least 64 characters are permitted, and that passwords of more than 128 characters are denied. (C6)	521
Verify that password truncation is not performed. However, consecutive multiple spaces may be replaced by a single space. (C6)	521
Verify that passwords are stored with sufficient protection to prevent offline recovery attacks, including local system access.	522
...	

Modelagem de ameaças

Classificar as Ameaças

Classificação		Alto (3)	Médio (2)	Baixo (1)
D	Danos em Potencial	✓		
R	Reprodutibilidade	✓		
E	Explorabilidade			✓
A	Usuários Afetados		✓	
D	Possibilidade de descobrimento			✓
Risco		3+3	+2	+1+1
		= 10 (risco médio)		

Risco:
Baixo: 5 a 7;
Médio: 8 a 11;
Alto: 12 a 15.

Modelagem de Ameaças
"A cada história"

História da Sprint

Como um usuário cadastrado.

Gostaria de recuperar a senha que perdi.

Para que eu possa novamente logar no sistema.

Critérios de aceite:

- Usuário existindo na base de dados, enviar mensagem de "E-mail enviado", usuário não existindo na base de dados, enviar mensagem "usuário não existe na base de dados";
- Enviar um link com código sequencial para o e-mail do usuário;
- Link direciona para tela de alteração de senha;

Modelagem de Ameaças

Ameaças - Recuperação de Senha

Ataque
Brute Force - para descobrir códigos sequenciais válidos
Brute Force - enumeração de usuário
Negação de Serviço - alterar a senha dos usuários
Phishing - através da enumeração de usuários;

História da Sprint

Como um usuário cadastrado.

Gostaria de recuperar a senha que perdi.

Para que eu possa novamente logar no sistema.

Critérios de aceite:

- Usuário existindo ou não na base de dados, enviar mensagem "**Caso conste em nossa base de dados um e-mail será enviado com as instruções de alteração de senha**"
- Enviar um link com **random GUIDs**, para o e-mail do usuário;
- **Rate Limiting** implementado;
- Vincular o **random GUIDs** com o **usuário** que está solicitando a **recuperação de senha**;
- Link direciona para tela de alteração de senha;
- **Senha** precisa seguir o padrão da **Política XYZ**;

Conclusão

- Modelagem voltada **para desenvolvedores**;
- **DoR e DoD**;
- Requisitos de segurança como **critério de aceite** nas histórias;
- Melhoria **contínua**;

Conclusão

- Modelagem voltada **para desenvolvedores**;
- **DoR e DoD**;
- Requisitos de segurança como **critério de aceite** nas histórias;
- Melhoria **contínua**;

MODELAGEM DE AMEAÇAS É UMA ATIVIDADE VIVA

MODELAGEM A CADA HISTÓRIA

Let's empower developers to build secure applications?!

Tiago Zaniquelli

Security Analyst

zani0x03@gmail.com