OWASP Threat Dragon

Cristian Souza

https://cristian.sh

AGENDA

1. Introdução
2. Instalação
3. Visão geral
4. Exemplos
5. Conclusão

Introdução

Introdução

- **Modelagem de ameaças:** prática de desenvolvimento seguro de sistemas que visa identificar contra-medidas de segurança para mitigar ameaças ao s*oftware*.

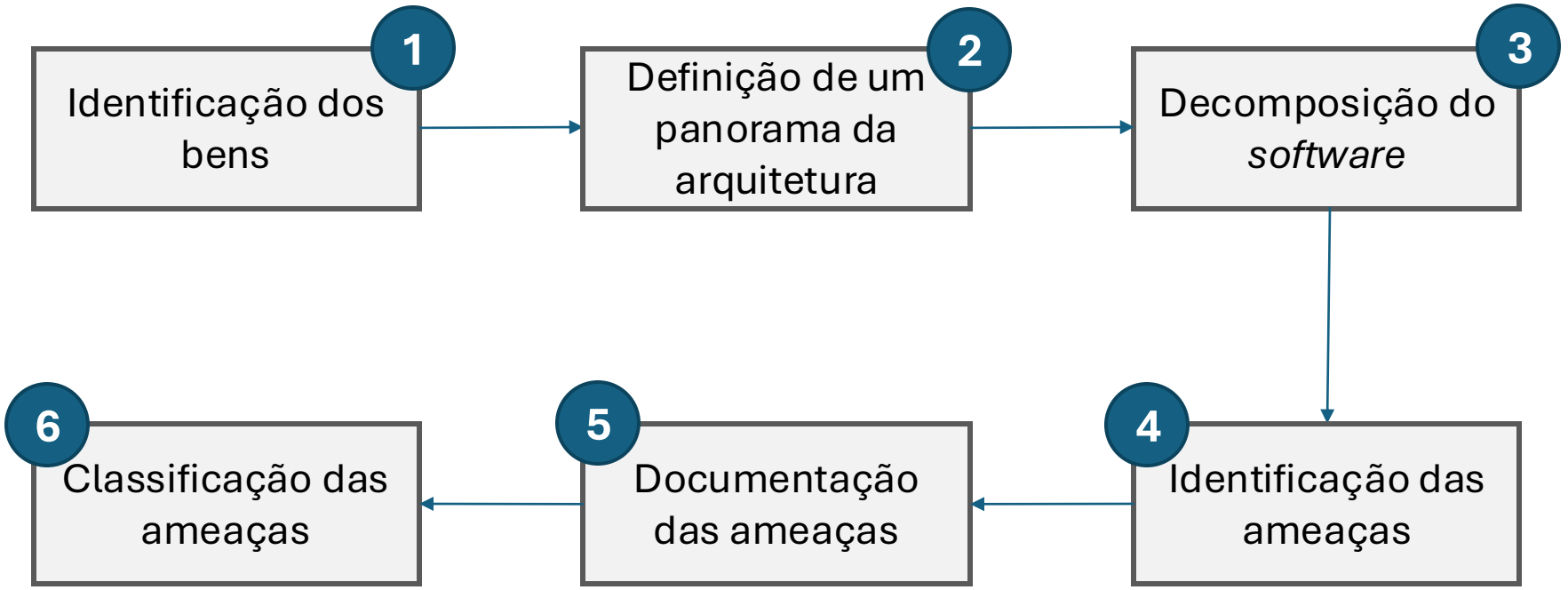
- Pode ser incorporada ao desenvolvimento do produto durante a fase de *design*.

- Método eficaz para proteção de sistemas, redes, aplicações e serviços.

- Permite lidar com ameaças antecipadamente e evitar problemas em ambiente de produção.

Introdução

- **Processo de modelagem:**



Introdução

1. **Identificação dos bens:** recursos que serão protegidos.
   - **Exemplos:** informações confidenciais, bancos de dados, páginas na Internet.

2. **Panorama da arquitetura:** funções da sua aplicação.
   - O que ela faz? Quais os casos de uso? Quais tecnologias e *softwares* de terceiros estão sendo utilizados?

3. **Decomposição do *software*:** identificação das vulnerabilidades individualmente.
   - **Exemplos:** funções do programa, servidor web, sistema operacional, etc.

Introdução

4. Identificação das ameaças: mapeamento dos riscos que podem ser causados por usuários mal-intencionados.

- Métodos STRIDE e DREAD.

5. Documentação das ameaças: evidencie as ameaças identificadas e qual o dano causado por cada uma.

- Qual é o ativo? Qual é o risco? Qual é o ataque? Qual medida de defesa será empregada?

6. Classificação das ameaças: atribuição de um nível de risco com base nos danos que causados no caso de um ataque.

- Os padrões CVSS e CWE são reconhecidos internacionalmente.

Introdução

OWASP Threat Dragon:

- Ferramenta gratuita e *open-source* para diagramação e modelagem de ameaças.
- Suporta os modelos STRIDE, LINDDUN e CIA.
- Multiplataforma.
- Documentação: https://threatdragon.github.io

Instalação

Instalação

- O OWASP Threat Dragon possui as versões web e desktop.

- https://github.com/mike-goodwin/owasp-threat-dragon
- https://github.com/mike-goodwin/owasp-threat-dragon-desktop

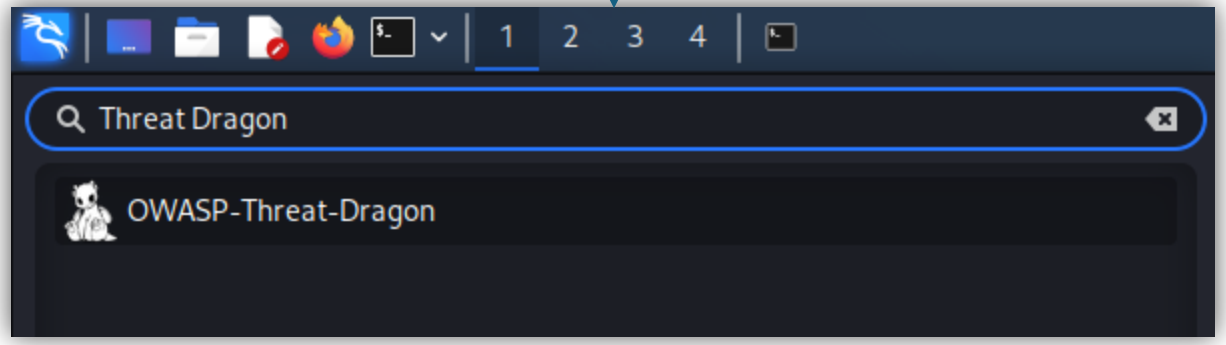
- A versão desktop é baseada no Electron.

- Pacotes para Windows, Linux e MacOS podem ser obtidos em: https://github.com/mike-goodwin/owasp-threat-dragon-desktop/releases/

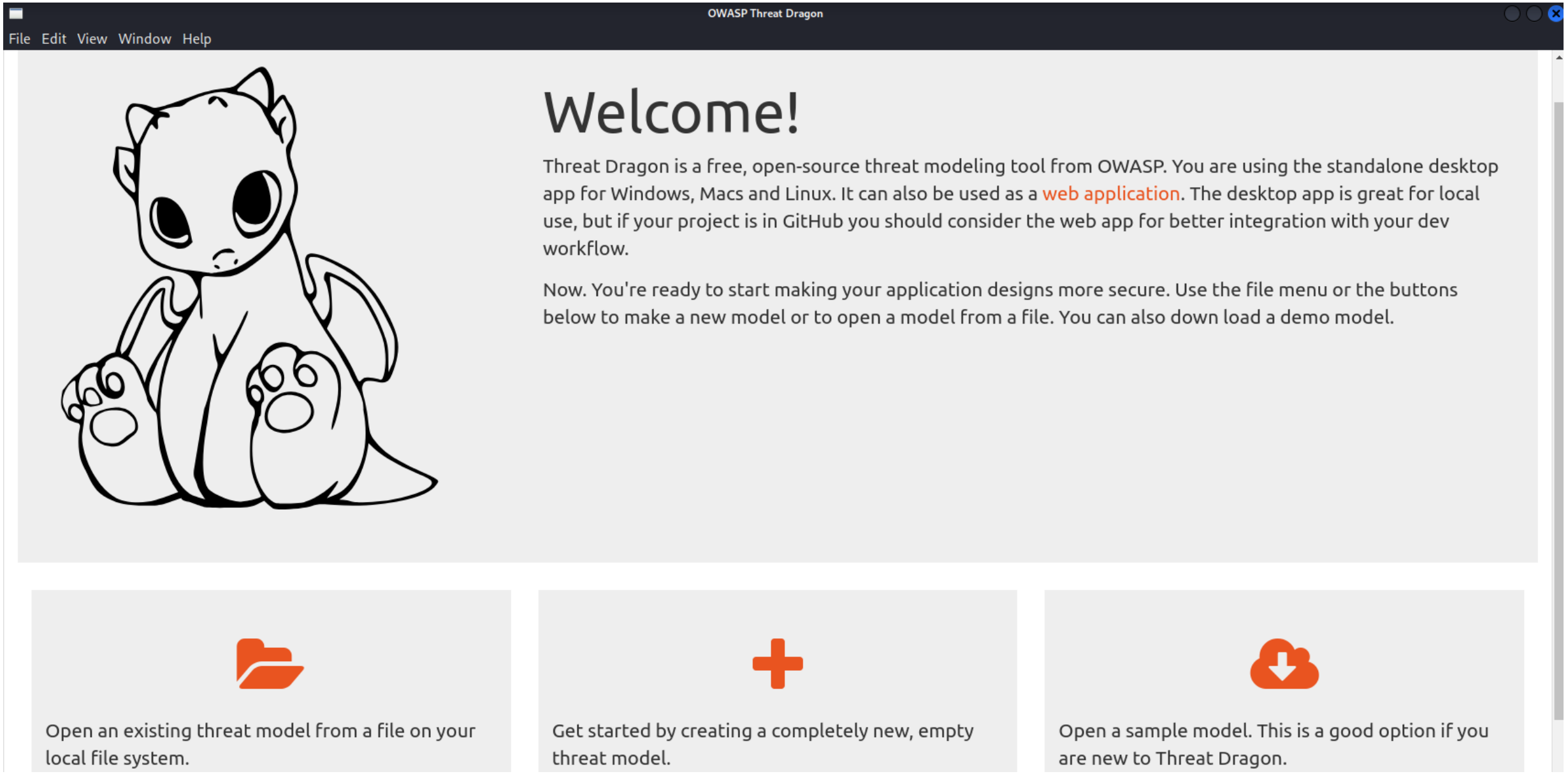
Instalação

```
┌──(kali㉿kali)-[~/Downloads]
└─$ wget https://github.com/mike-goodwin/owasp-threat-dragon-desktop/releases/download/v1.2/threatdragon_1.2.0_amd64.deb

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i threatdragon_1.2.0_amd64.deb
Selecting previously unselected package threatdragon.
(Reading database ... 298561 files and directories currently installed.)
Preparing to unpack threatdragon_1.2.0_amd64.deb ...
Unpacking threatdragon (1.2.0) ...
Setting up threatdragon (1.2.0) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for mailcap (3.70+nmu1) ...
```



Instalação


OWASP Threat Dragon
File Edit View Window Help
Welcome!
Threat Dragon is a free, open-source threat modeling tool from OWASP. You are using the standalone desktop app for Windows, Macs and Linux. It can also be used as a web application. The desktop app is great for local use, but if your project is in GitHub you should consider the web app for better integration with your dev workflow.
Now. You're ready to start making your application designs more secure. Use the file menu or the buttons below to make a new model or to open a model from a file. You can also down load a demo model.
Open an existing threat model from a file on your local file system.
Get started by creating a completely new, empty threat model.
Open a sample model. This is a good option if you are new to Threat Dragon.

Visão geral

Visão geral

Templates:

Demo Threat Model

Owner:
Mike Goodwin

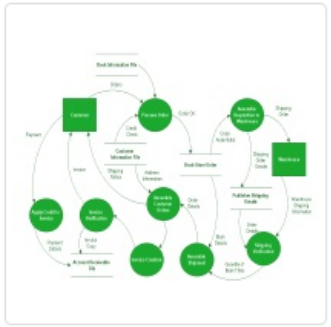
Reviewer:
Jane Smith

Contributors:
Tom Brown; Albert Moneypenny

High level system description

A sample model of a web application, with a queue-decoupled background process.

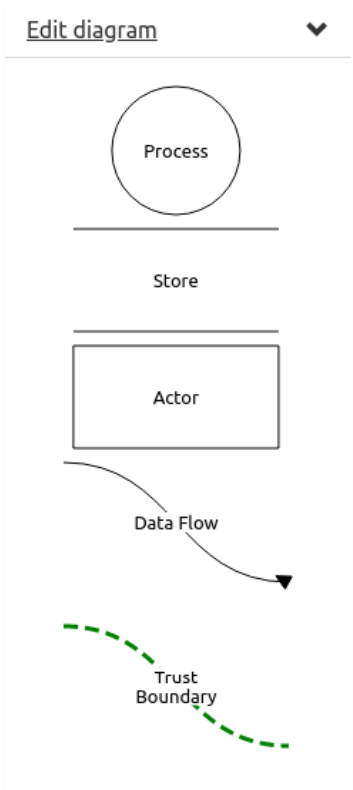
Main Request Data Flow



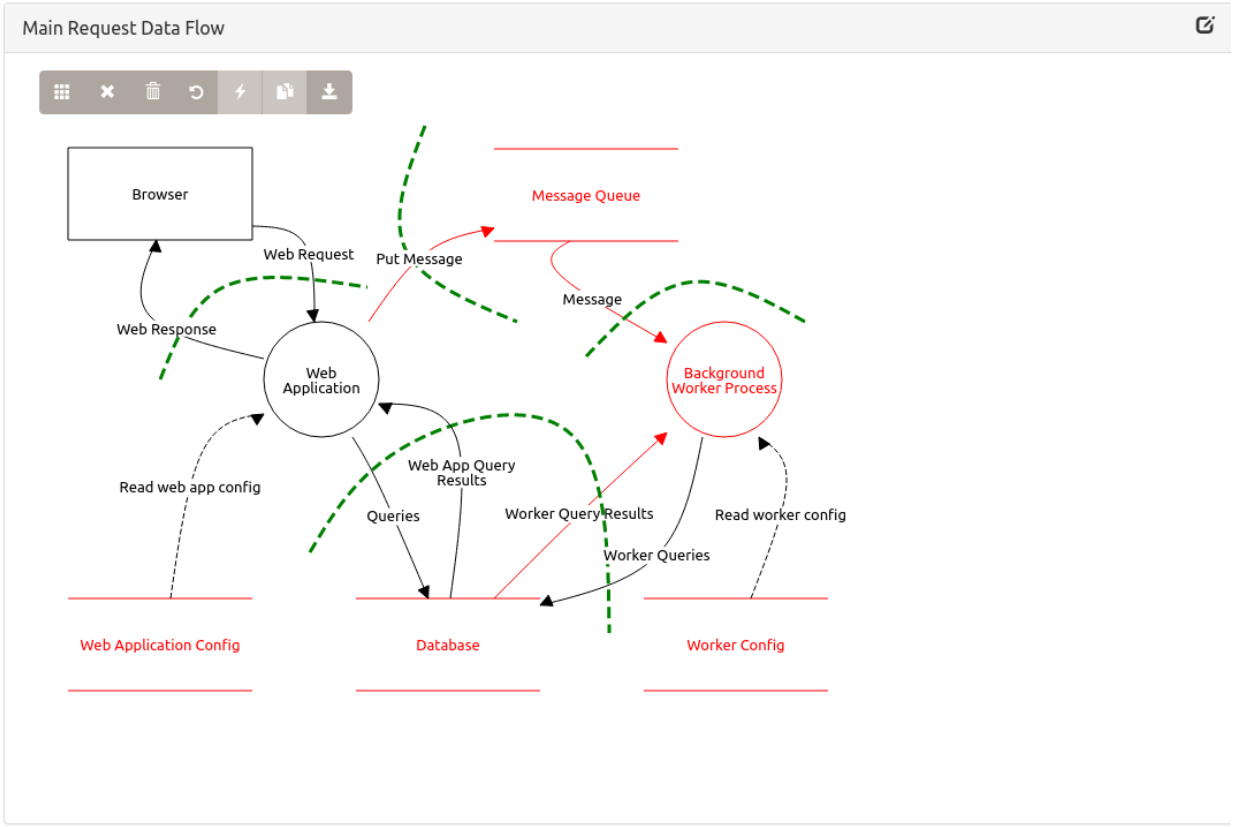
Edit Report Delete

Visão geral

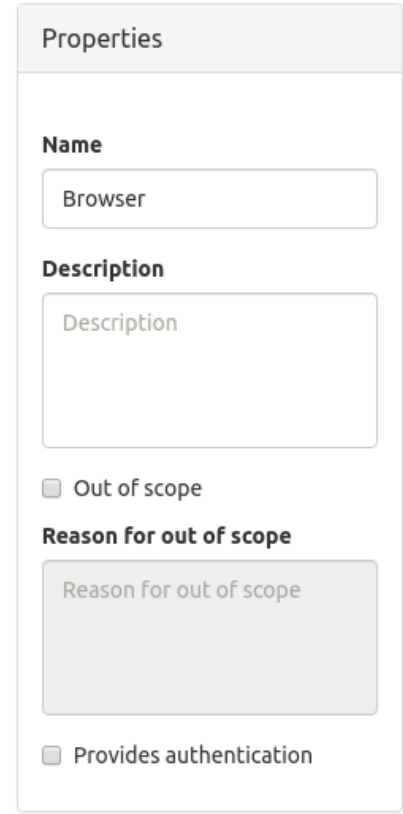
Menu principal:



Área de trabalho:



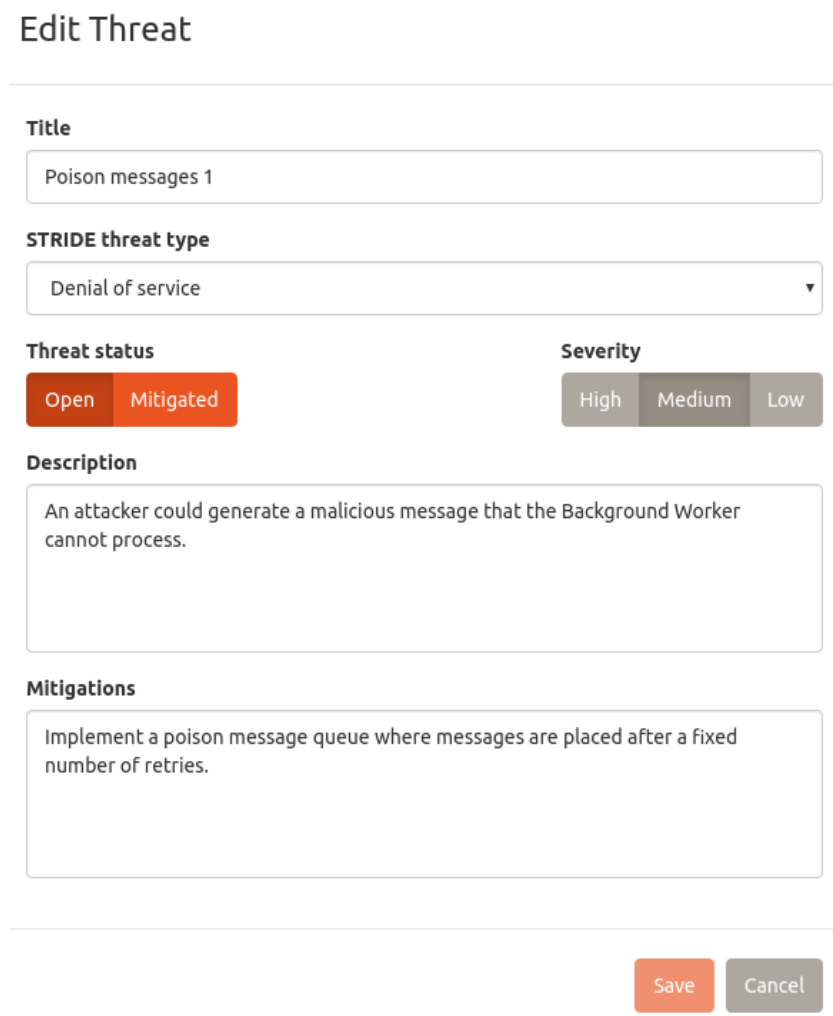
Propriedades:



Visão geral

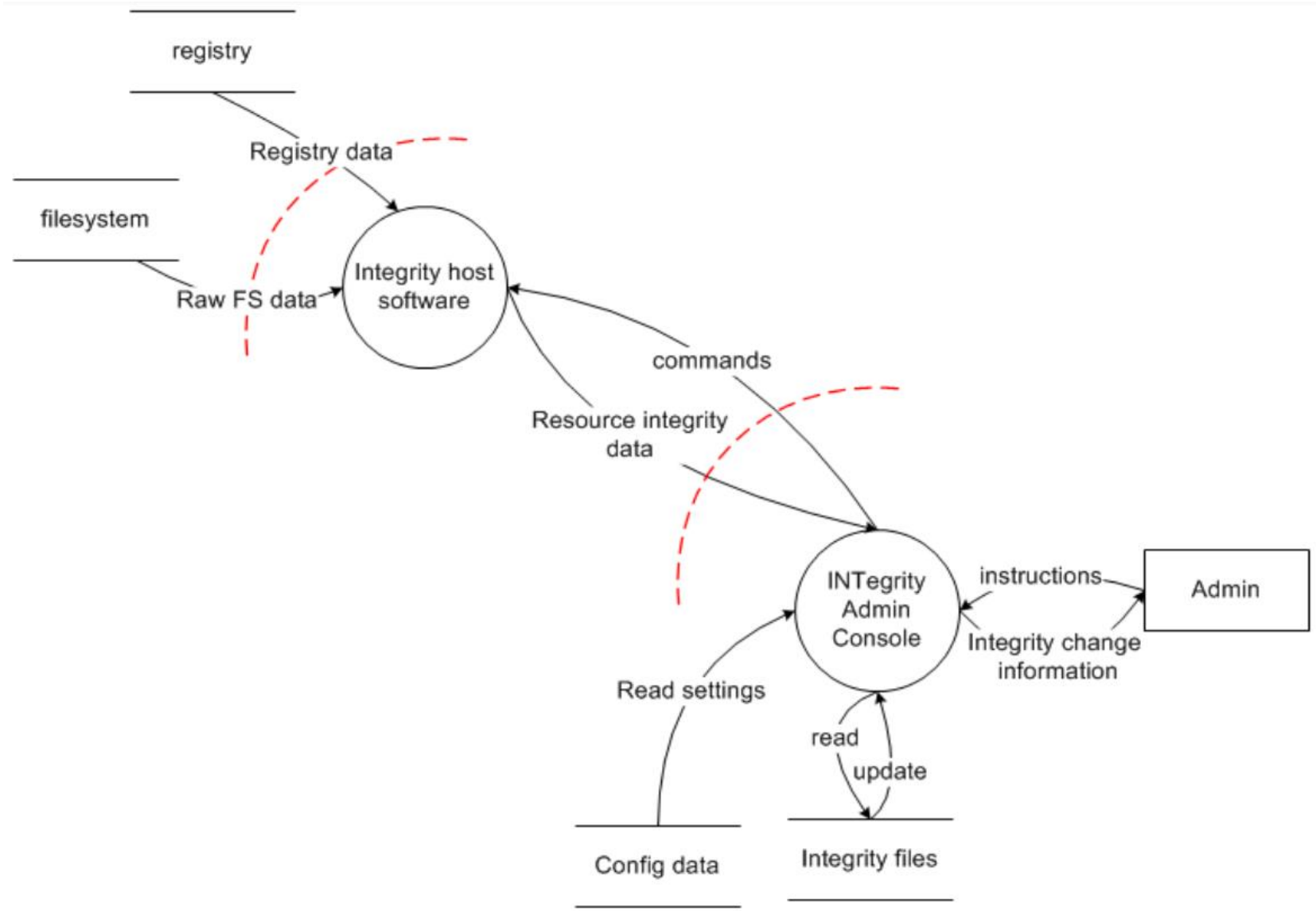
Alguns recursos:

- Cadastro de ameaças para os elementos do diagrama.
- Cadastro e acompanhamento das mitigações implementadas.
- Exportação de diagramas em JSON.

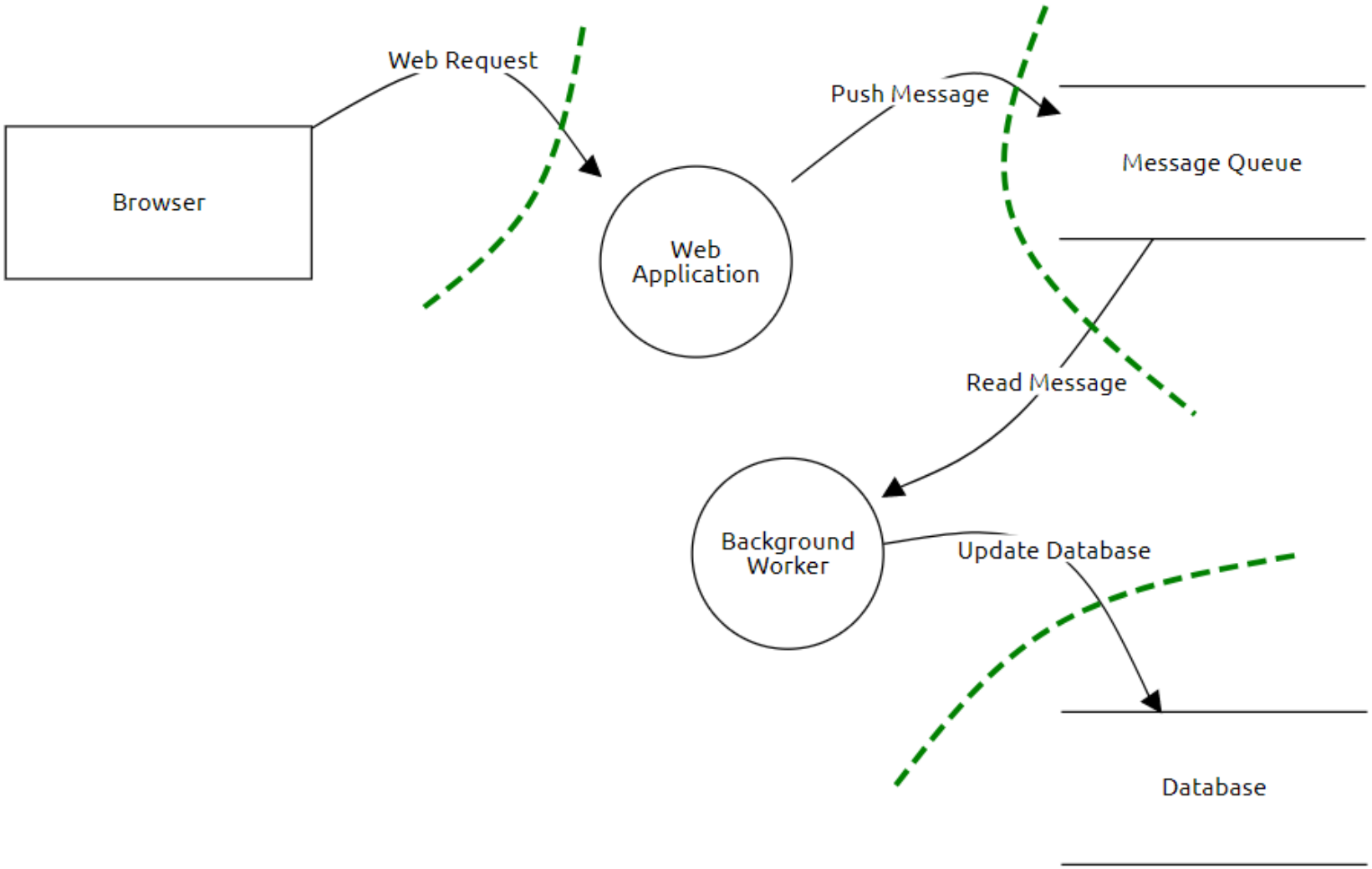


Exemplos

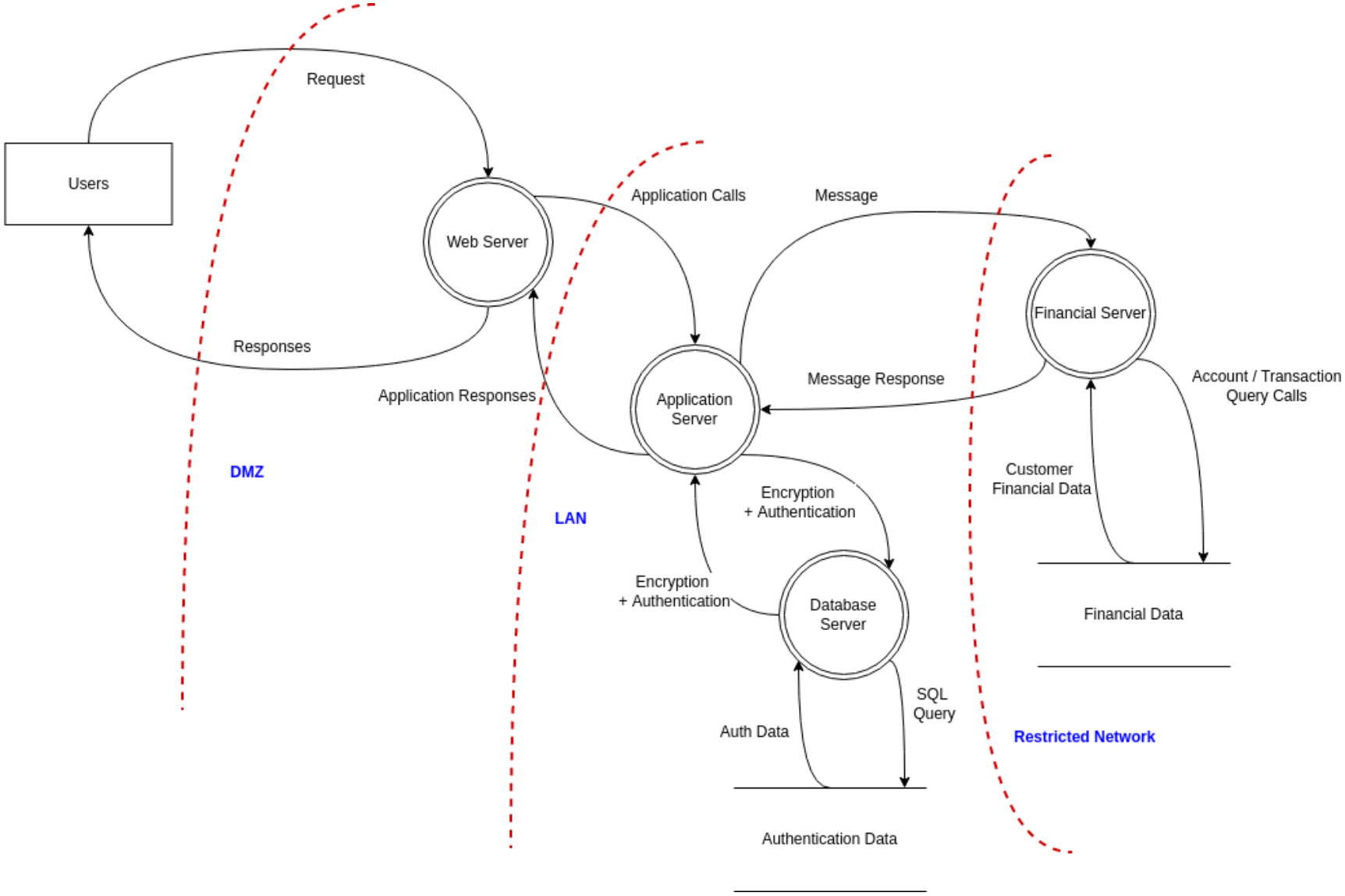
Exemplos


registry
Registry data
filesystem
Raw FS data
Integrity host software
commands
Resource integrity data
INTegrity Admin Console
instructions
Admin
Integrity change information
Read settings
read
update
Config data
Integrity files

Exemplos


Web Request
Browser
Web
Application
Push Message
Message Queue
Read Message
Background
Worker
Update Database
Database

Exemplos


Request
Users
Web Server
Application Calls
Message
Financial Server
Responses
Application Responses
Application Server
Message Response
Account / Transaction Query Calls
DMZ
LAN
Customer Financial Data
Encryption + Authentication
Encryption + Authentication
Database Server
Financial Data
SQL Query
Auth Data
Restricted Network
Authentication Data

Conclusão

Conclusão

- O OWASP Threat Dragon facilita a identificação de ameaças, diagramação e acompanhamento das correções aplicadas.

- A modelagem pode ser realizada para aplicações web, mobile, redes de computadores e outros sistemas.

- Os projetos podem ser exportados e compartilhados com membros da equipe.

OWASP Threat Dragon

Cristian Souza

https://cristian.sh