

Tutorial - Modelagem de Ameaças

1. Acesse o site <https://www.threatdragon.com/#/>
2. Escolha a forma de login
3. Clique em “Create e new, empty threat model”
4. Defina o título (nome da equipe), o autor do modelo, o revisor (qualquer um da equipe, de preferência o consultor de segurança escolhido)
5. Pode deixar as duas próximas caixas em branco
6. Clique em “Add new diagram”
7. Verifique que a opção “STRIDE” esteja selecionada
8. Escolha um nome para o diagrama. Por exemplo: “Modelagem de Ameaças - *Nome do Grupo*”
9. Clique em “save” e depois em “close”
10. Abra o diagrama recém criado

The screenshot shows the Threat Dragon v2.4.1-latest web application interface. The browser address bar shows the URL <https://www.threatdragon.com>. The application header is red and contains the text "Threat Dragon v2.4.1-latest", "English", and "Logged in as local-user". The main content area is titled "Editing: New Threat Model" and contains several form fields:

- Title:** A text input field with the value "New Threat Model".
- Owner:** A text input field.
- Reviewer:** A text input field.
- High level system description:** A large text area.
- Contributors:** A text input field with the placeholder text "Start typing to add a contributor".
- Diagrams:** A section with a red plus icon and the text "+ Add a new diagram...". A curved arrow points from this section to the "Contributors" field.

At the bottom right of the form, there are three buttons: "Save" (red), "Reload" (grey), and "Close" (grey).

Threat Dragon v2.4.1-latestEnglish

Logged in as local-user

Editing: New Threat Model

Title

New Threat Model

Owner

Reviewer

High level system description

Contributors

Start typing to add a contributor

Diagrams

STRIDE

New STRIDE diagram

New STRIDE diagram description

Remove

+ Add a new diagram...

Save

Reload

Close

1

2

Threat Dragon v2.4.1-latestEnglish

Logged in as local-user

New Threat Model


Owner:

Reviewer:

Contributors:

High level system description

New STRIDE diagram



Edit

Report

Close Model

Como Preencher

1. Crie um modelo do fluxo de dados da aplicação. Exemplo:



2. Atribua a cada elemento do diagrama (ator/processo/fluxo de dados) as ameaças nas quais este elemento pode estar vulnerável. Para isso, clique no elemento, e depois em “New Threat”. Preencha as informações da janela que se abre. O campo “score” pode ser ignorado. Exemplo para o processo de “Login”:

Edit Threat #3

Title

Acesso por força bruta

Type

Spoofing

Status

N/A

Open

Mitigated

Score

Priority

TBD

Low

Medium

High

Critical

Description

Um atacante pode executar um algoritmo que tenta diversas senhas até conseguir autenticar ao sistema.

Mitigations

Aplicar proteções ao processo de autenticação, como limitação de tentativas ou captcha.

Remove

Apply

3. Repita o processo para todas as ameaças pensadas para cada um dos 3 requisitos de segurança definidos.
4. Clique em “save” e entregue o arquivo json gerado.

Dica: Para cada funcionalidade de segurança determinada, releia os 6 tipos de ameaças STRIDE enumeradas no material disponibilizado. Procure identificar quais tipos de ameaças podem estar relacionadas ao requisito. Então, para cada tipo de ameaça relacionada ao requisito, pense em todas as formas possíveis de concretizar esta ameaça. Então, passe tudo para o modelo criado no Threat Dragon.

Para o exemplo da imagem acima:

- **Requisito de segurança:** Broken Access Control
- **Tipo de falha:** Spoofing
- **Forma de concretizar a falha:** ataque de força bruta