

# **OWASP Threat Dragon**

Presentation to Bristol (UK) Chapter

# Who am I?

- C/C++ developer for 25 years
- Security engineer for 11 years

Active in OWASP :

- Leader + contributor to OWASP Threat Dragon project
- Co-leader + contributor for OWASP Developer Guide project
- Co-Leader of Bristol (UK) OWASP Chapter

# Did you say Threat Dragon?

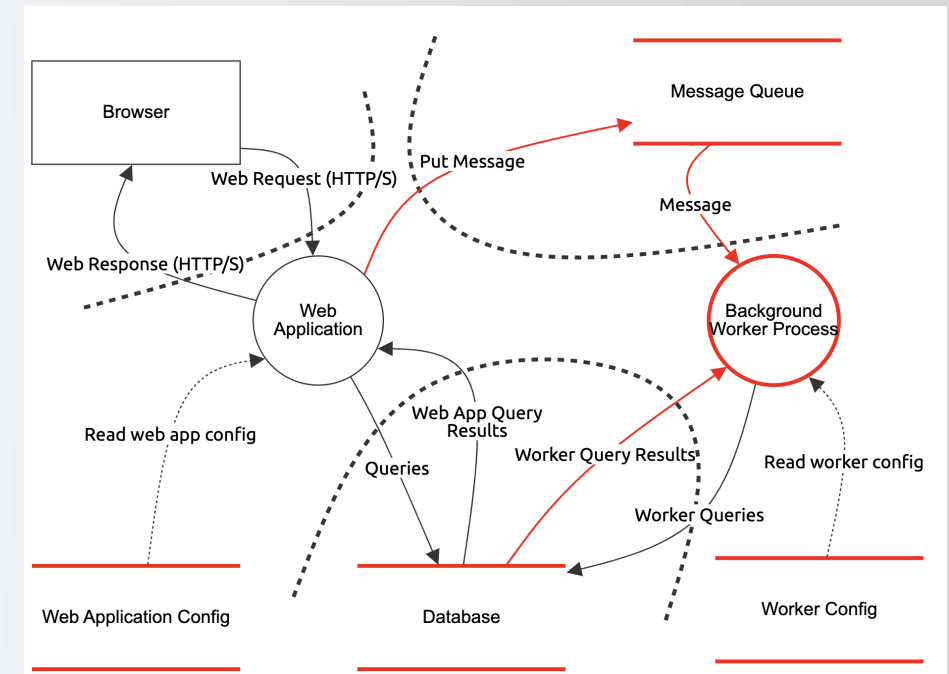
- OWASP Lab Project
- Tactical threat modeling
- Stores threats
- Data flow diagrams
- Always free to download, free to use



# What is Threat Modeling?

- Just **4** simple questions
- What are we considering?
- What can go wrong?
- What to do about that?
- How well did it turn out?

*(Paraphrasing Shostack's Four Questions)*



# Why do Threat Modeling?

- Well, because we are expected to do it
- It is as useful if you make it
- It can be fun!

It may be the only time when a team can sit back and ask: ‘If I was a bad person, what is the worst I can do?’



# Is Threat Modeling painful?

- It can be if you get it wrong
- Tactical threat modeling
- Make it bite size
- Do it early; and its never too late
- No security heroes



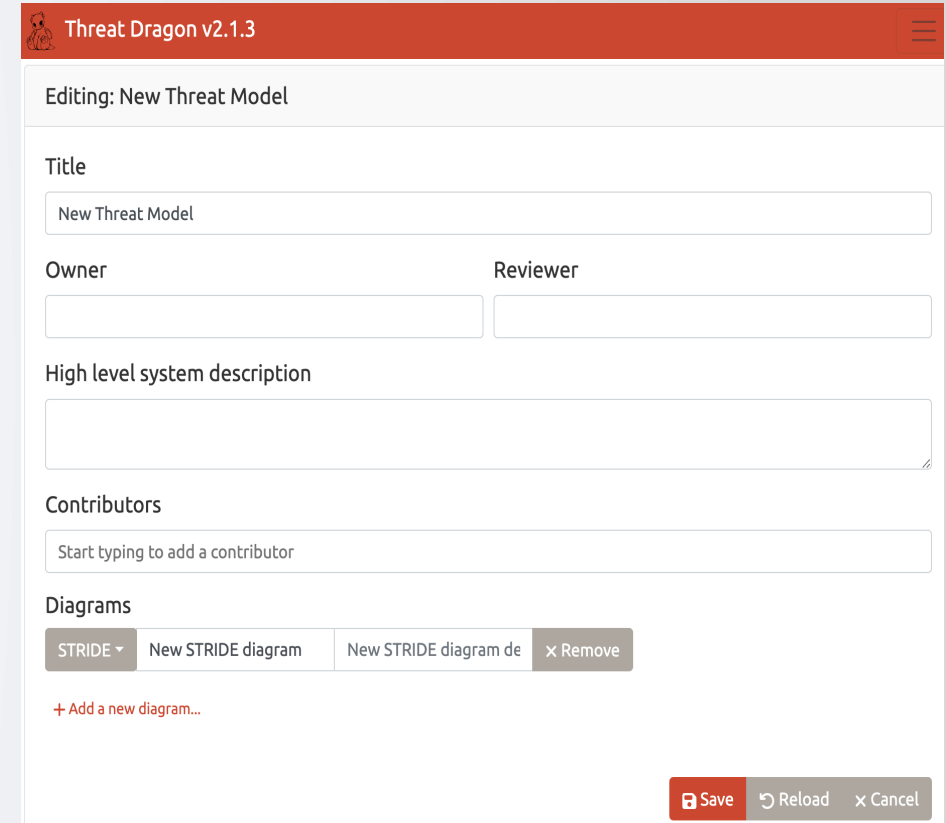
# Where do I get Threat Dragon?

- Download the desktop application for Linux/MacOS/Windows
- Or run your own web application
- Or deploy a docker container
- Or access the demo site:  
[www.threatdragon.com](http://www.threatdragon.com)



# So where do I start?

- Provide high level information
- Add diagrams:
  - STRIDE
  - LINDDUN
  - CIA, PLOT4ai, DIE



The screenshot shows the Threat Dragon v2.1.3 web application interface. The title bar is red with the application name and a hamburger menu icon. The main content area is white and contains the following sections:

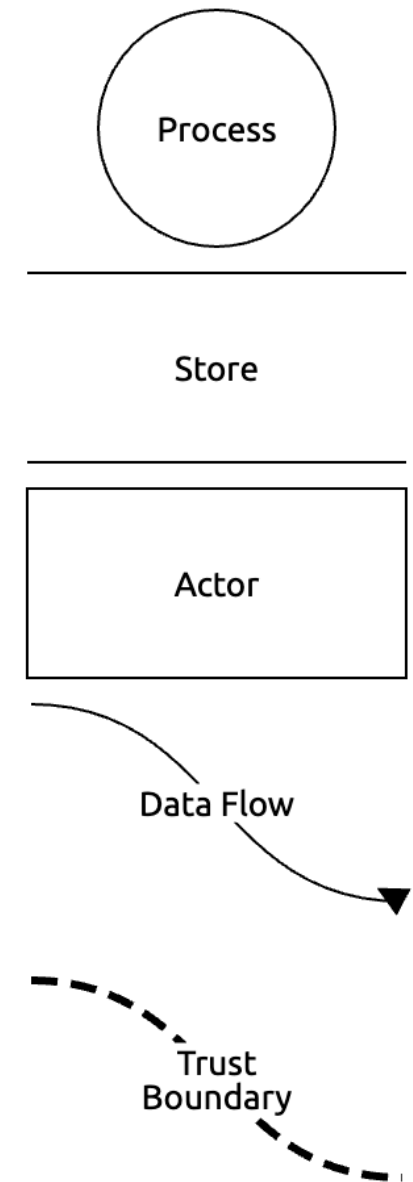
- Editing: New Threat Model**: A header for the current editing session.
- Title**: A text input field containing "New Threat Model".
- Owner** and **Reviewer**: Two text input fields for user information.
- High level system description**: A large text area for describing the system.
- Contributors**: A text input field with the placeholder "Start typing to add a contributor".
- Diagrams**: A section with a dropdown menu showing "STRIDE" and two buttons: "New STRIDE diagram" and "New STRIDE diagram de". There is also a "x Remove" button.
- + Add a new diagram...**: A link to add a new diagram.

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



# Did you say diagrams?

- Data flow diagram components:
  - Processes
  - Actors
  - Stores / Assets
  - Trust boundaries
- Data flow between components



# What about threats?

- The reason for threat modeling
- Stores threats within the model
- Type: according to methodology
- Status: Open / Mitigated / NA
- Priority: High / Medium / Low
- Score: any numeric value
- Mitigation or Remediation?
- TAME the threats

The screenshot shows a web form titled "Edit Threat #1" with a red header bar. The form contains the following fields and controls:

- Title:** A text input field containing "Out of scope threat".
- Type:** A dropdown menu with "Spoofing" selected.
- Status:** Three radio buttons labeled "N/A", "Open", and "Mitigated". "Open" is selected.
- Score:** A text input field.
- Priority:** Three radio buttons labeled "Low", "Medium", and "High". "Medium" is selected.
- Description:** A large text area with the placeholder text "Provide a description for this threat".
- Mitigations:** A large text area with the placeholder text "Provide remediation for this threat or a reason if status is N/A".
- Buttons:** At the bottom, there are three buttons: "Delete" (red), "Cancel", and "Apply".

# Did you say **STRIDE**?

	Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privileges
Process	X	X	X	X	X	X
Store		X	X	X	X	
Actor	X		X			
Data flow		X		X	X	

# Did you say **LINDDUN**?

	Linkability	Identifiability	Non-repudiation	Detectability	Disclosure of information	Unawareness	Non-compliance
Process	X	X	X	X	X		X
Store	X	X	X	X	X		X
Actor	X	X				X	
Data flow	X	X	X	X	X		X

# Questions on Threat Dragon?

- Making Threat Modeling less threatening
- Always free to download, free to use
- Contributions welcomed!



# Time for a demo ?



