Agenda for the day

Threat Dragon Threat Analysis

1. Investigate the threat posed by the dragon
2. . Develop a model for its creation
3. . Document the Data Flow Diagram (DFD)
4. Apply STRIDE threat analysis methodology
5. . Generate a report
6. Hand-On lab

OWASP Threat Dragon

What is Threat Dragon?

Threat Dragon is a free, open-source threat modeling application designed to help security teams identify and mitigate potential risks in software systems. It allows users to create data-flow diagrams to visualize how information moves through a system, pinpoint security threats, and document necessary remediations.

Key Features:

Cross-platform: Works across different operating systems.

Threat modeling: Supports structured frameworks for identifying security risks.

Diagram-based analysis: Uses visual models to map out potential vulnerabilities.

What is Threat Dragon?

Supported Frameworks:

Threat Dragon incorporates several established threat modeling methodologies:

STRIDE: Focuses on six security threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

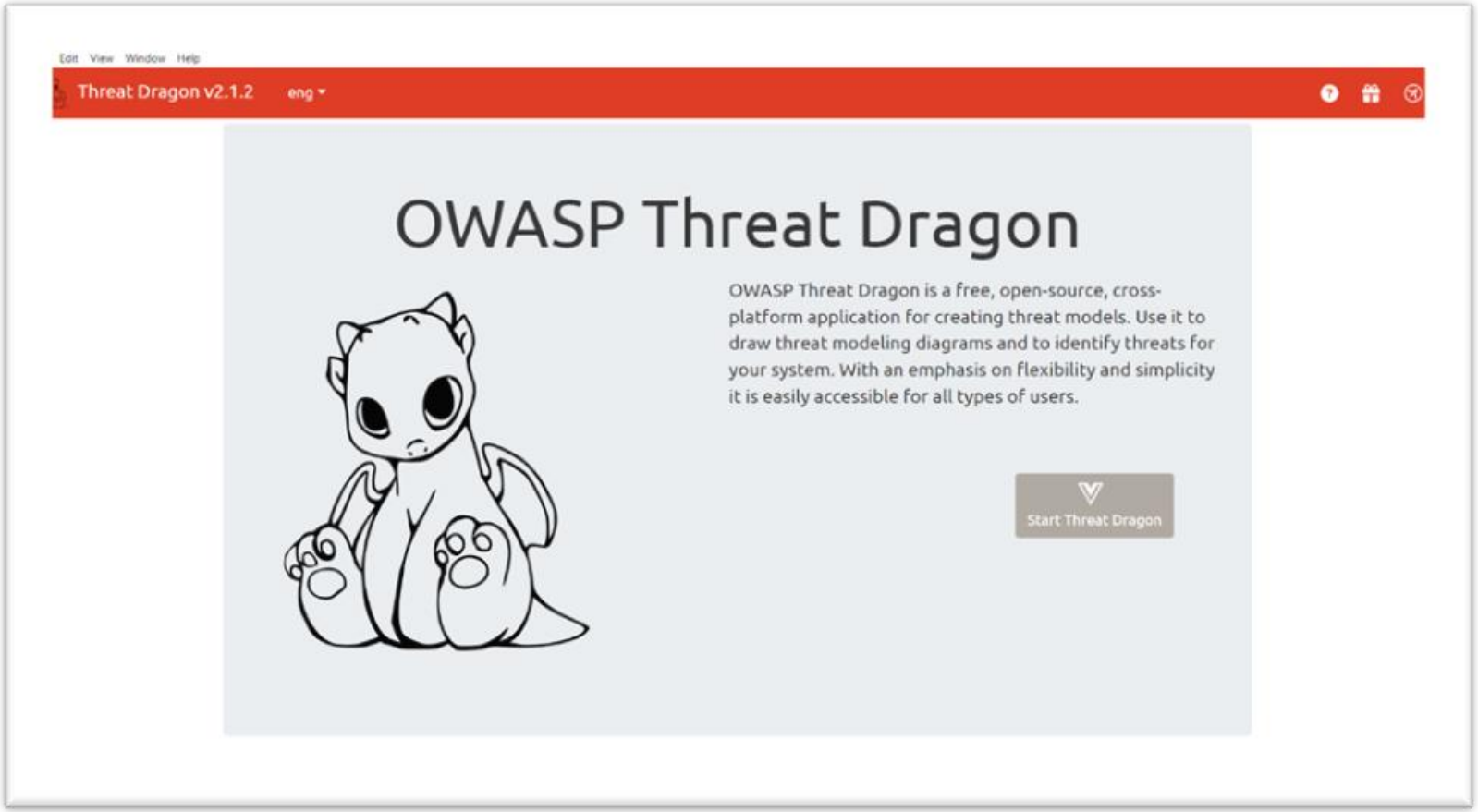
LINDDUN: Specialized for privacy threat modeling.

CIA: Evaluates threats based on Confidentiality, Integrity, and Availability.

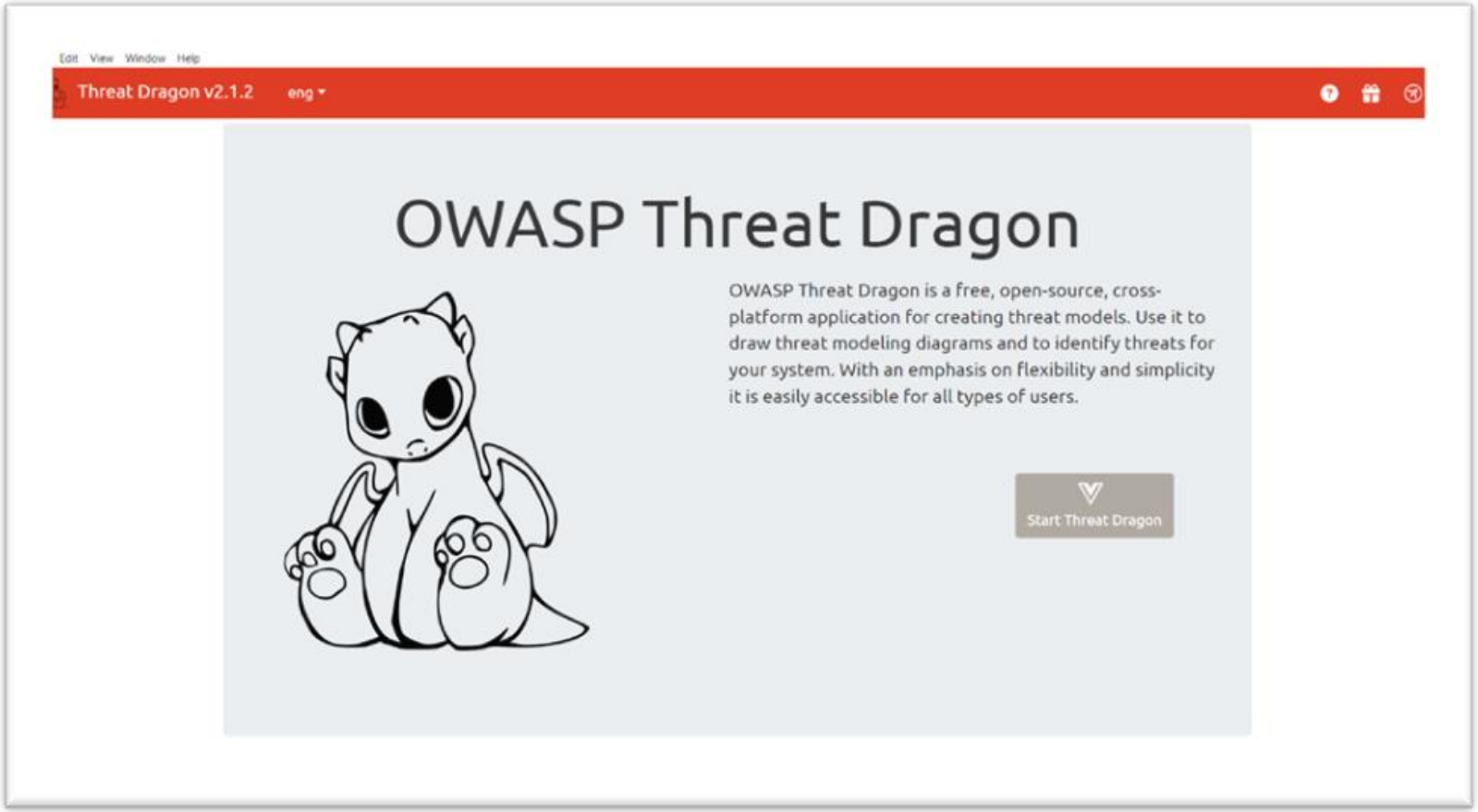
DIE: Distributed security model emphasizing security durability.

PLOT4ai: Security considerations tailored for AI-driven systems.

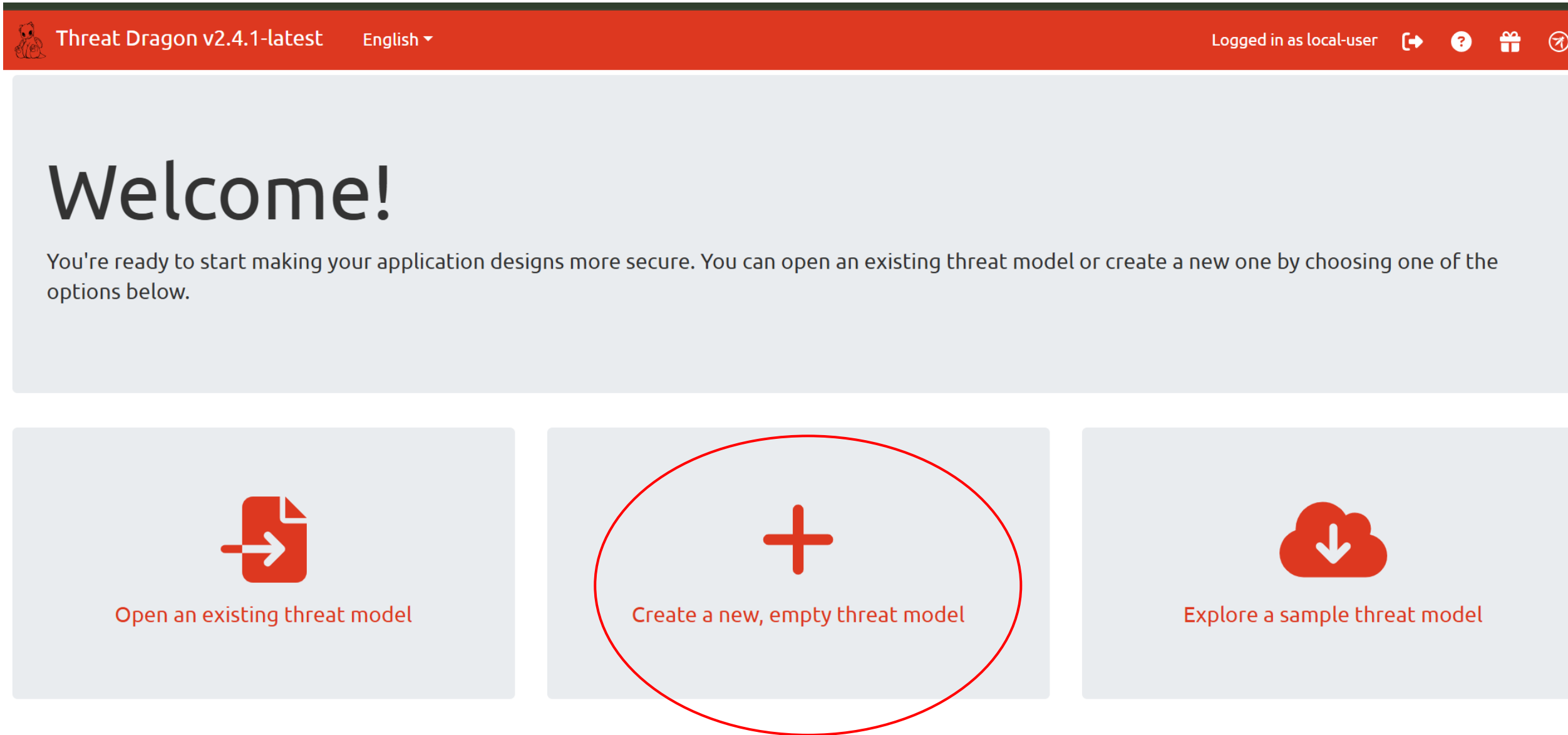
Main screen


Edit View Window Help
Threat Dragon v2.1.2
eng
OWASP Threat Dragon
OWASP Threat Dragon is a free, open-source, cross-platform application for creating threat models. Use it to draw threat modeling diagrams and to identify threats for your system. With an emphasis on flexibility and simplicity it is easily accessible for all types of users.
Start Threat Dragon

Main screen - Online



Welcome screen - Online



Creating a Threat Model

Threat Model Edit Page

The Title field is required, while the others are optional but offer valuable context for future reference. Click the **Edit** button to modify the threat model details.

Title - required, other fields optional
Owner - usually a development team or individual
Reviewer - currently limited to one
High-level system description - adds context to your model
Contributors - acknowledges those involved

Threat Model Edit Page

Editing: New Threat Model

Title

New Threat Model

Owner

Reviewer

High level system description

Contributors

Start typing to add a contributor

Diagrams

+ Add a new diagram...

Save Reload Cancel

Threat Model Edit Page

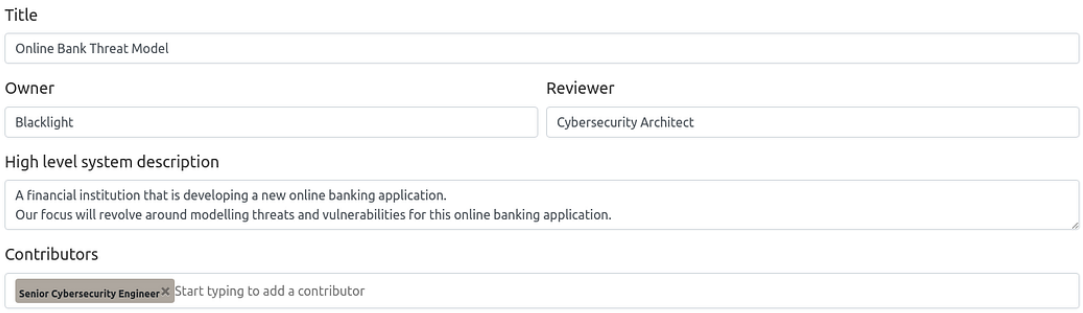
“Title” — Online Bank Threat Model

“Owner” — Blacklight

“Reviewer” — Cybersecurity Architect

“High Level System Description” — A financial institution that is developing a new online banking application. Our focus will revolve around modelling threats and vulnerabilities for this online banking application.

“Contributors” — Senior Cybersecurity Engineer



Add Diagram

Title

Online Bank Threat Model

Owner

Blacklight

Reviewer

Cybersecurity Architect

High level system description

A financial institution that is developing a new online banking application.
Our focus will revolve around modelling threats and vulnerabilities for this online banking application.

Contributors

Senior Cybersecurity Engineer × Start typing to add a contributor

Diagrams

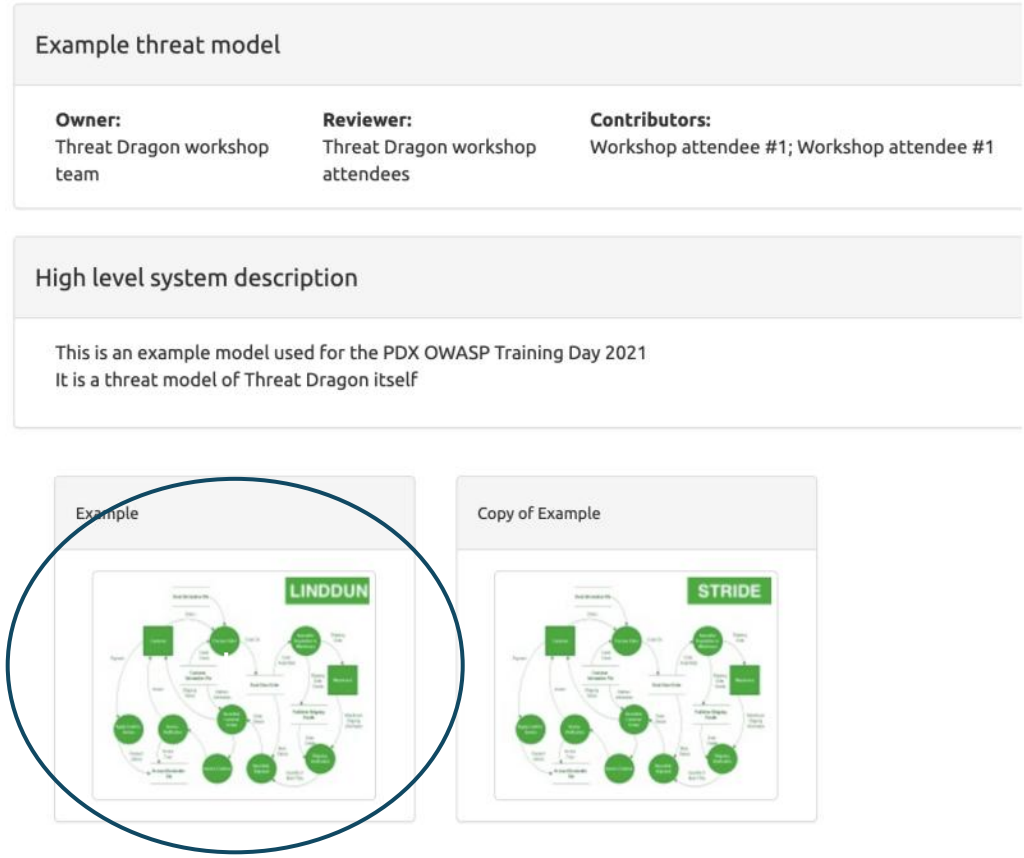
STRIDE ▾ | e-bank | e-bank STRIDE | × Remove

+ Add a new diagram...

Save | Reload | × Close

After save

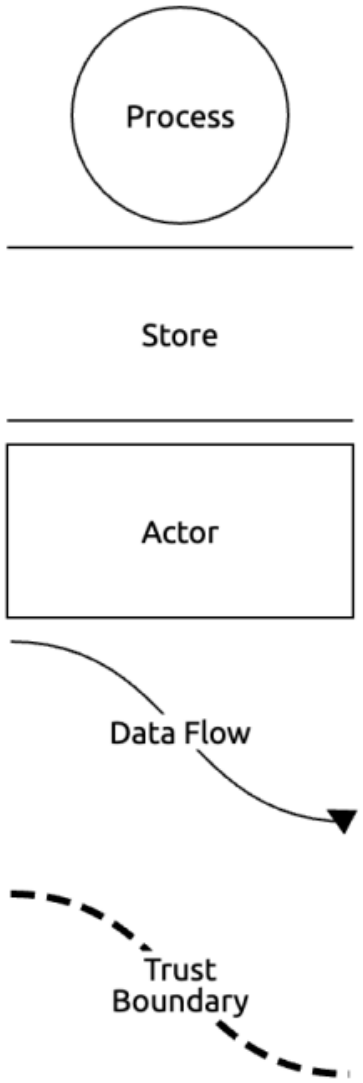
Select the A diagram to begin constructi ng your model.



Diagrams

Threat, not system, perspective

- Process
- Store
- Actor
- Data flow
- Trust boundary



Process

Usually a component under our control

- Name
- Description
- Out of scope? Reasoning

Context properties

- Privilege level

Store

Data at rest, almost always within the system but can be external

- The usual Name, Description, Out of scope? & Reasoning

Context properties

- Is a log?
- Stores credentials?
- Is encrypted?
- Is signed?

This could be regarded as an asset

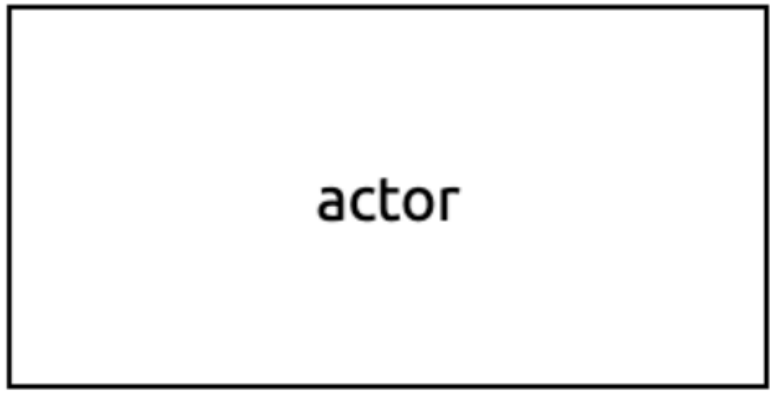
Actor

Commonly a component outside of our system

- The usual Name, Description, Out of scope? & Reasoning

Properties

- Provides authentication?



Data Flow

Data in transit, often cross trust boundaries

- The usual Name, Description, Out of scope? & Reasoning

Properties

- Protocol
- Is encrypted?
- Is over a public network?

Two ways to create data flow

Data Flow

Data in transit, often cross trust boundaries

- The usual Name, Description, Out of scope? & Reasoning

Properties

- Protocol
- Is encrypted?
- Is over a public network?

Two ways to create data flow

Trust Boundary

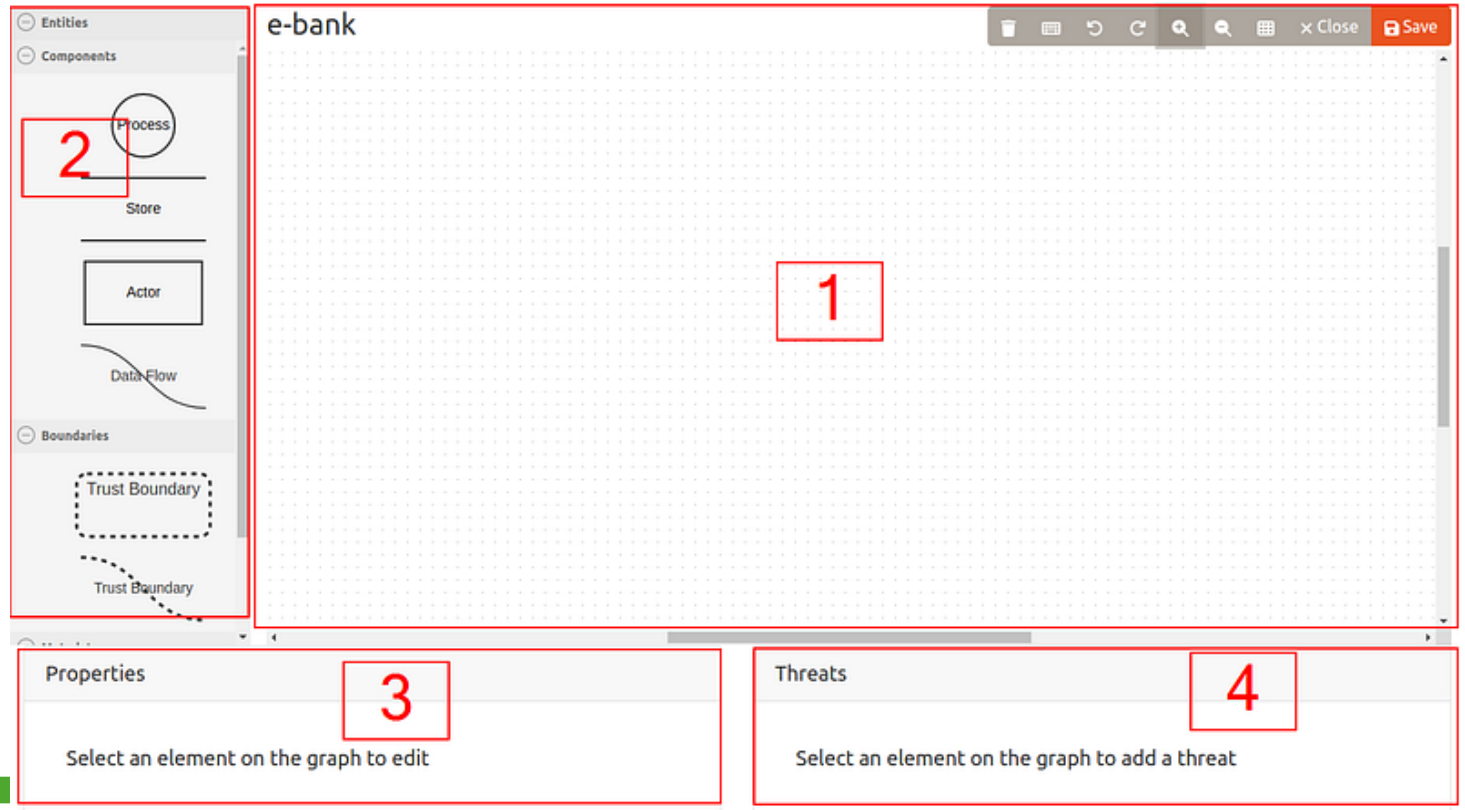
- Name is optional in this case
- No other properties
- It is not a box (yet)
- *The most important of the elements*

Scope

Scope for diagram components

- Components can be declared out of scope
- Useful for focussing on important components
- Boundaries never out of scope
- Try and give a reasoning
- *Helps incremental*

Diagram



1. The canvas where you'll construct the model

2. The **"entities"** pane where you can find the **"components"**, **"bound aries"** and **"metadata".**

3. The **"properties"** pane where you can tweak the properties of entities including their names, descriptions and if they are out of scope.

4. The **"threats"** pane; where we'll add new threats to the entities

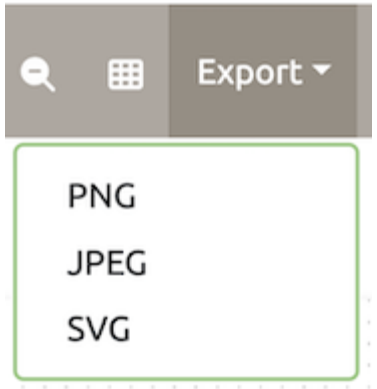
Threats

The reason for the threat model

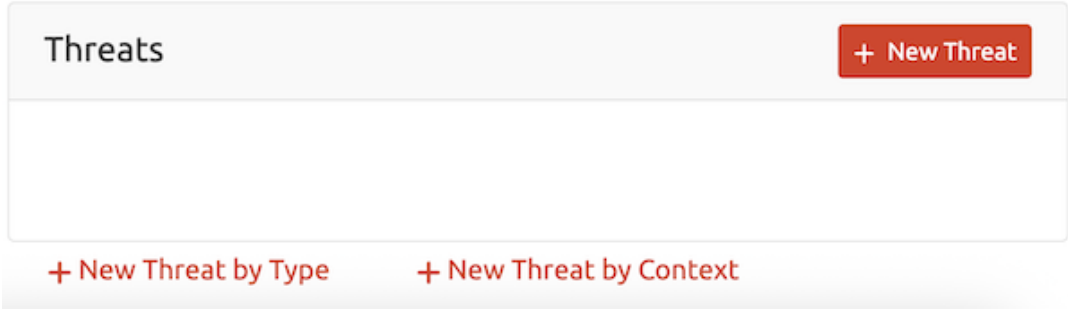
- STRIDE / CIA / LINDDUN
- You can mix and match
- Status: NA / Open / Mitigated
- Priority: Low / Medium / High
- Description of threat
- Mitigation or even prevention

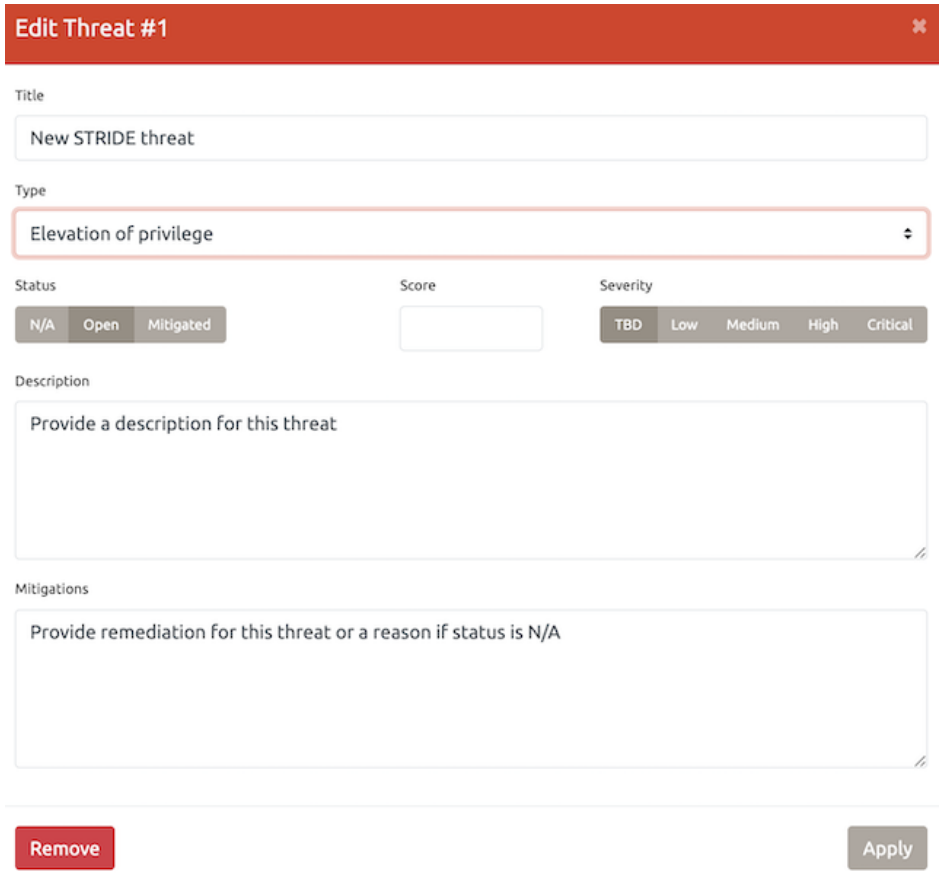
Toolbar

1. Delete the selected element(s)
2. Configure the keyboard shortcuts from the defaults
3. Undo and Redo edits
4. Zoom In and Zoom Out
5. Toggle gridlines on/off, allowing for neater models
6. Close the diagram and return to the threat model details view
7. Save the threat model



Threat generation





Threat properties

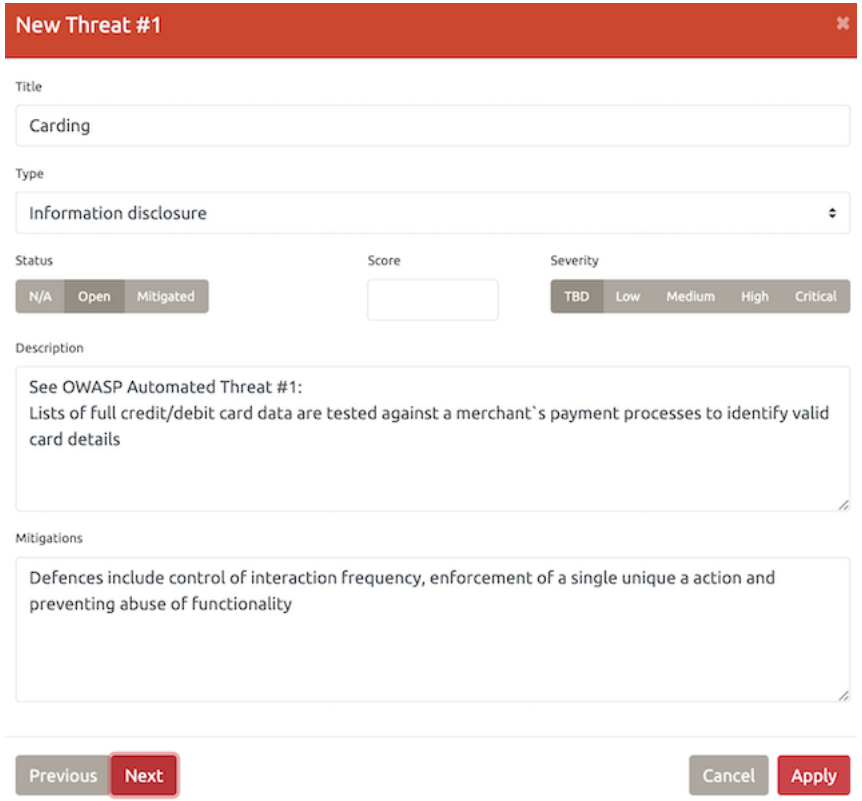
- All threats have the following properties:
- **Title** is free form test, usually a short descriptive title
- **Type** is a category selection determined by the diagram type (STRIDE / LINDDUN / PLOT4ai / CIA / CIA-DIE / Generic)
- **Status** is one of N/A / Open / Mitigated
- **Score** contains a free text field, often used to score the threat from 0.0 to 10.0 but can be any text or CVSS score
- **Severity** is one of TBD / Low / Medium / High / Critical, similar to CVSS
- **Description** of the threat and possible impact
- **Mitigations** for the threat, probably a remediation from TAME (Transfer / Accept / Mitigate / Evade)

Threats by element type -Threats by context

The components on the diagram have type-specific properties,

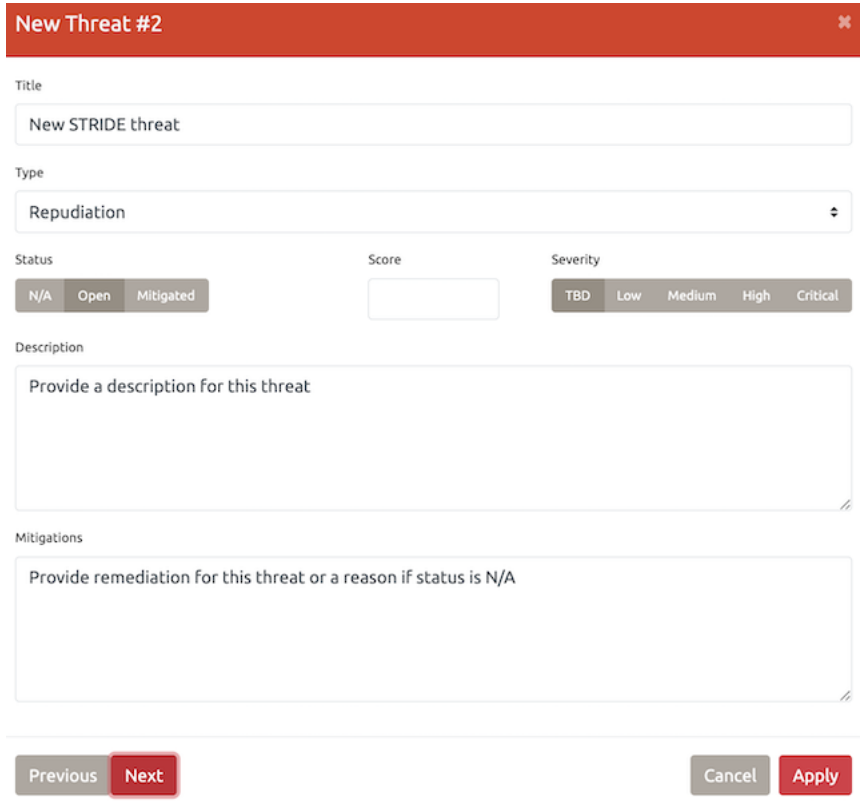
for example the Actor component has a property ‘Provides Authentication’ via a check-box. These properties are used to determine context-specific threat suggestions using ‘New Threat by Context’.

At present the suggestions are based on the OWASP Automated Threats to Web Applications, commonly known as OATS. The threat suggestion can be accepted using **Apply** and cycle through the threats using the **Previous** and **Next** buttons. Use **Cancel** to exit the suggestion sequence.



Threats by element type

The threat model can have different types of threats added to it according to the diagram type. Currently the supported types are STRIDE, LINDDUN, CIA, CIA-DIE and PLOT4ai; these are configured as part of the diagram attributes when editing the model. A ‘Generic’ type is provided so that you can select any type of threat from any of the categories.



Report

Threat Dragon v2.4.1-latest English

Logged in as local-user

Show model diagrams | Show mitigated threats | Show out of scope elements | Show empty elements | Threat Dragon logo | Show element properties

Print | Close

Wed May 28 2025

Threat model report for Online Payments Processing Platform

Owner:
A development team

Reviewer:
A security architect

Contributors:
development engineers, product managers, security architects

Executive Summary

High level system description

This threat model has been provided by the OWASP Threat Model Cookbook:
threat-model-cookbook/Flow Diagram/payment

Summary

Metric	Total
Total Threats	0
Total Mitigated	0
Total Open	0
Open / Critical Severity	0
Open / High Severity	0
Open / Medium Severity	0

Hands-On Lab

Exercise: Threat Modeling with OWASP Threat Dragon