What Is Threat Modeling?

Threat modeling is a structured approach used to identify, analyze, prioritize, and mitigate potential security threats within a system, application, or process. It allows security teams and developers to understand *what could go wrong* before attackers exploit vulnerabilities.

At its core, threat modeling helps answer four major questions:

1. **What are we building?**
2. **What can go wrong?**
3. **What are we going to do about it?**
4. **Have we done a good job?**

It helps organizations anticipate attacks, strengthen system design, and build security into products from the earliest stages of development (shift-left security).

Key Benefits

- Identifies design-level vulnerabilities before coding begins
- Saves cost compared to fixing issues later
- Improves system understanding and documentation
- Enhances secure-by-design architecture
- Reduces overall attack surface

Threat modeling isn't tied to one specific methodology, but popular approaches include **STRIDE**, **DREAD**, **PASTA**, and **Kill Chain-based analysis**.

🛠 OWASP Threat Dragon

OWASP Threat Dragon is an open-source, browser-based tool used for creating and managing threat modeling diagrams.

What It Does

- Allows users to design **data flow diagrams (DFDs)** for applications and systems
- Automatically identifies threats based on model elements (STRIDE methodology)
- Helps track threats, mitigations, and risks through a structured interface
- Supports exporting models into reports for documentation

Uses & Advantages

- **Open-source and free** for all security teams and developers

- Useful for secure design reviews in DevSecOps pipelines
- Visual and easy to use, making it excellent for collaboration
- Works across platforms (web app and desktop)
- Helps build repeatable and consistent threat modeling practices

Ideal for developers, architects, and security teams early in the SDLC.

🛠 Microsoft Threat Modeling Tool (TMT)

Microsoft's Threat Modeling Tool is a mature, enterprise-ready solution that helps teams apply the **STRIDE** framework systematically.

What It Does

- Enables creation of high-quality DFDs with Microsoft's standardized modeling symbols
- Automatically generates a list of potential threats based on system components
- Provides mitigation suggestions aligned with Microsoft security guidance
- Supports detailed reporting and model validation

Uses & Advantages

- Strong integration with enterprise development workflows
- Extensive built-in threat libraries
- Excellent for modeling cloud, web, and enterprise applications
- Helps ensure consistency across large security teams
- Ideal for organizations using Microsoft development stacks (Azure, .NET, etc.)

It's particularly valuable for engineering teams that want a repeatable, scalable threat modeling process.

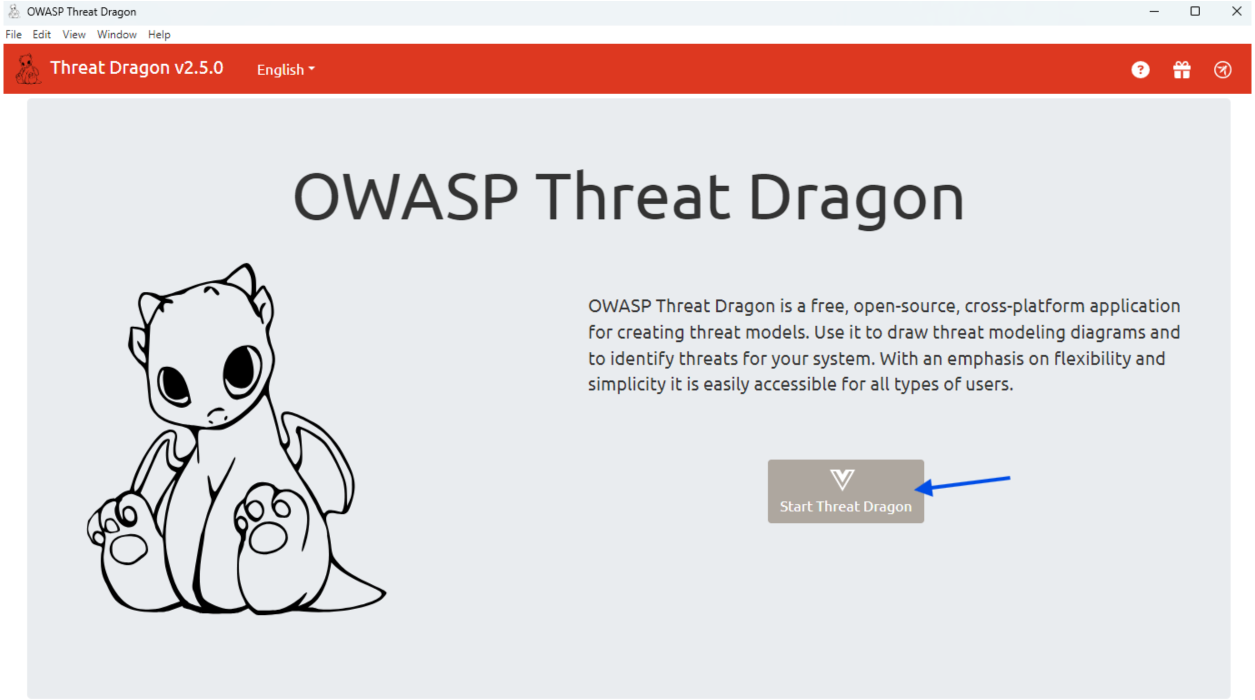
Threat modeling process

We will be simulation the building of a basic mobile app, which can be used to view inventory and place orders.

We will demonstrate with OWASP first then MTMT.

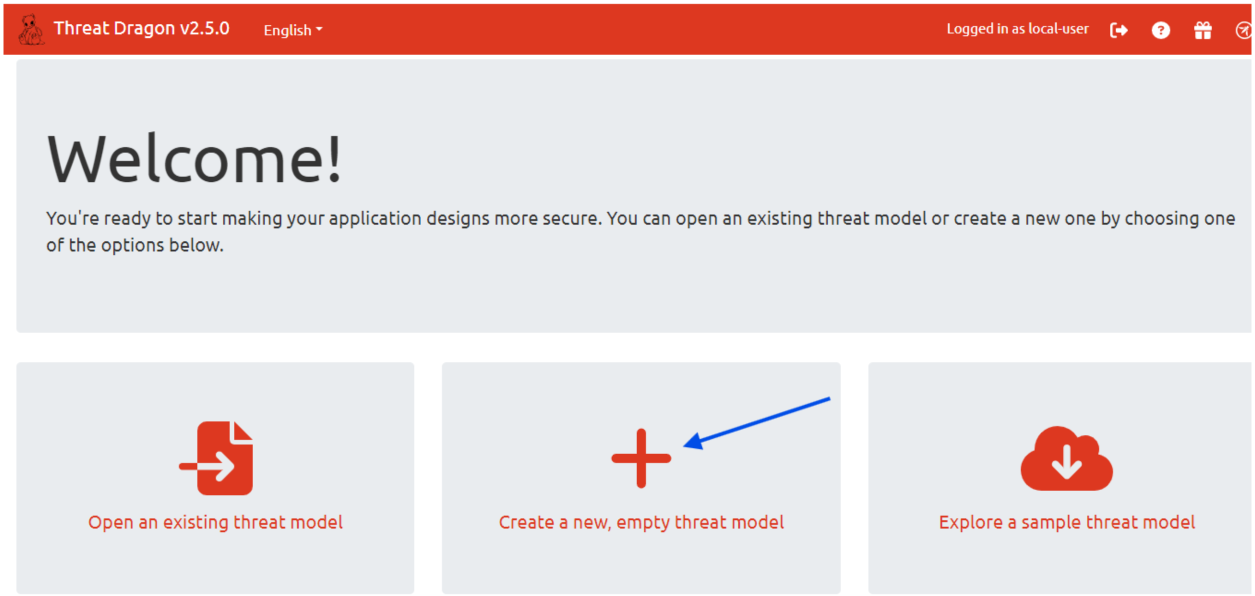
The OWASP app can be downloaded from https://github.com/owasp/threat-dragon/releases.

Upon installation, launch the app and create a new threat model



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.


Threat Dragon v2.5.0
English
Logged in as local-user
Open an existing threat model
Create a new, empty threat model
Explore a sample threat model

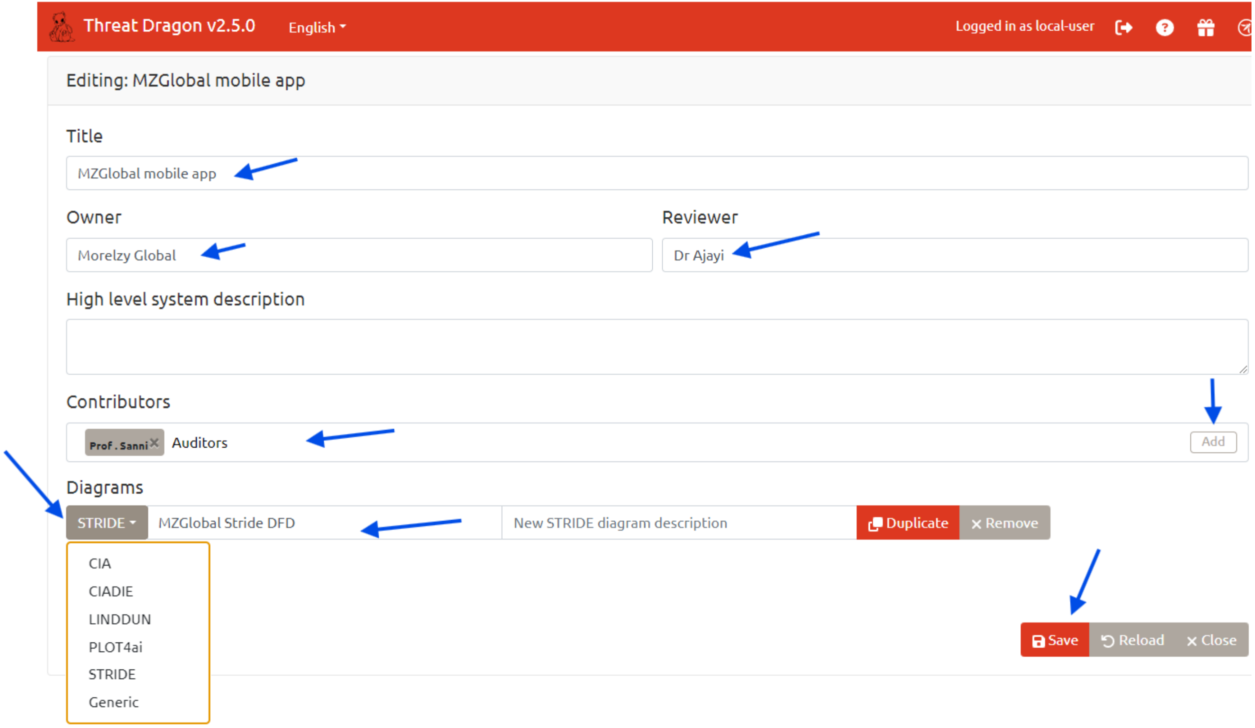
Welcome!

You're ready to start making your application designs more secure. You can open an existing threat model or create a new one by choosing one of the options below.

We give the model a title, define the owner and select the type of diagram.

In this instance we will be using he STRIDE model, click save.

Once its saved, click file and open the saved file



Editing: MZGlobal mobile app

Title

MZGlobal mobile app

Owner

Morelzy Global

Reviewer

Dr Ajayi

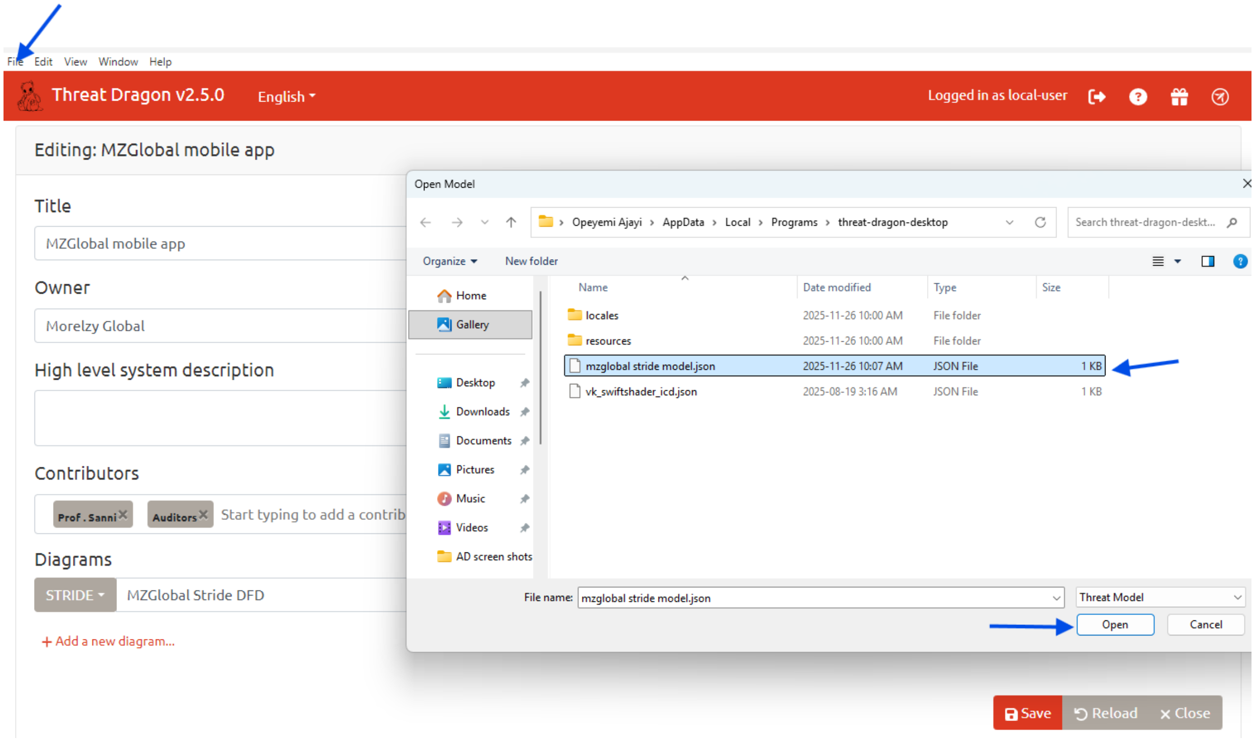
High level system description

Contributors

Prof . Sanni Auditors

Diagrams

STRIDE MZGlobal Stride DFD New STRIDE diagram description



Editing: MZGlobal mobile app

Title

MZGlobal mobile app

Owner

Morelzy Global

High level system description

Contributors

Prof . Sanni Auditors Start typing to add a contrib

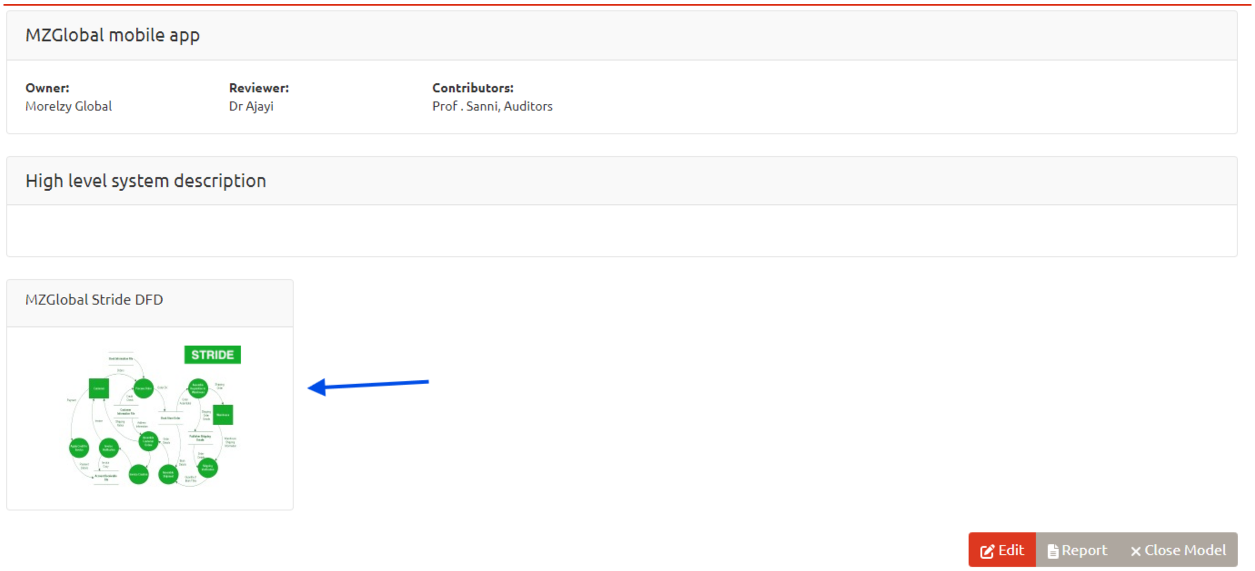
Diagrams

STRIDE MZGlobal Stride DFD

Name	Date modified	Type	Size
locales	2025-11-26 10:00 AM	File folder	
resources	2025-11-26 10:00 AM	File folder	
mzglobal stride model.json	2025-11-26 10:07 AM	JSON File	1 KB
vk_swiftshader_icd.json	2025-08-19 3:16 AM	JSON File	1 KB

File name: mzglobal stride model.json

Threat Model



MZGlobal mobile app

Owner: Morelzy Global

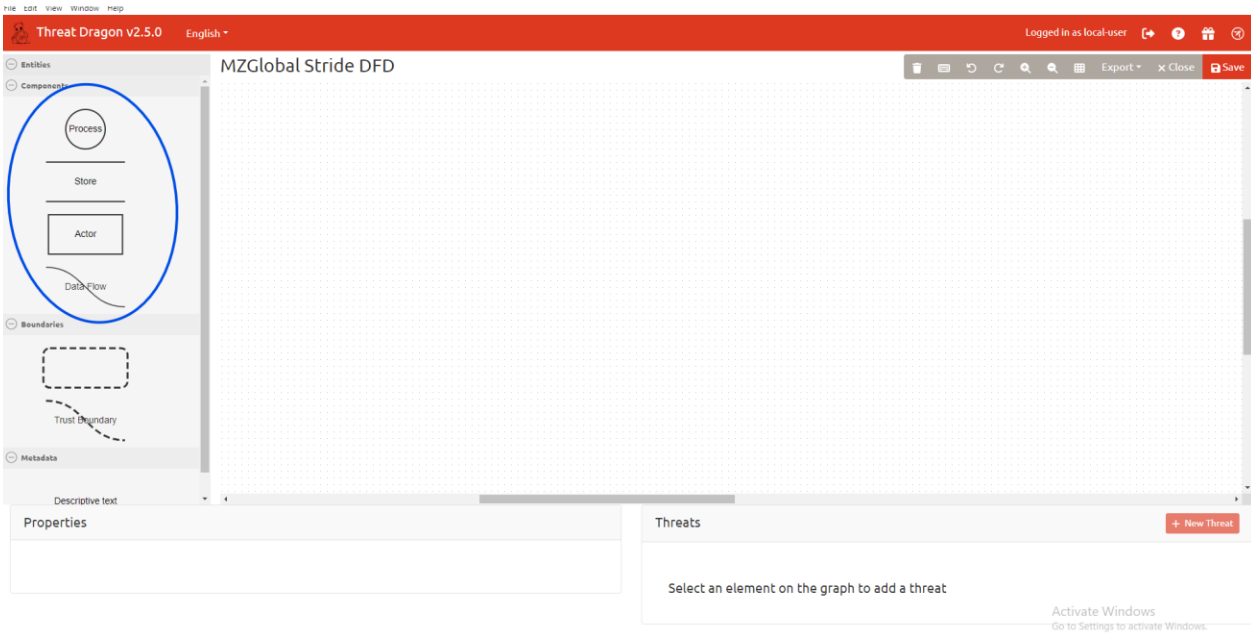
Reviewer: Dr Ajayi

Contributors: Prof . Sanni, Auditors

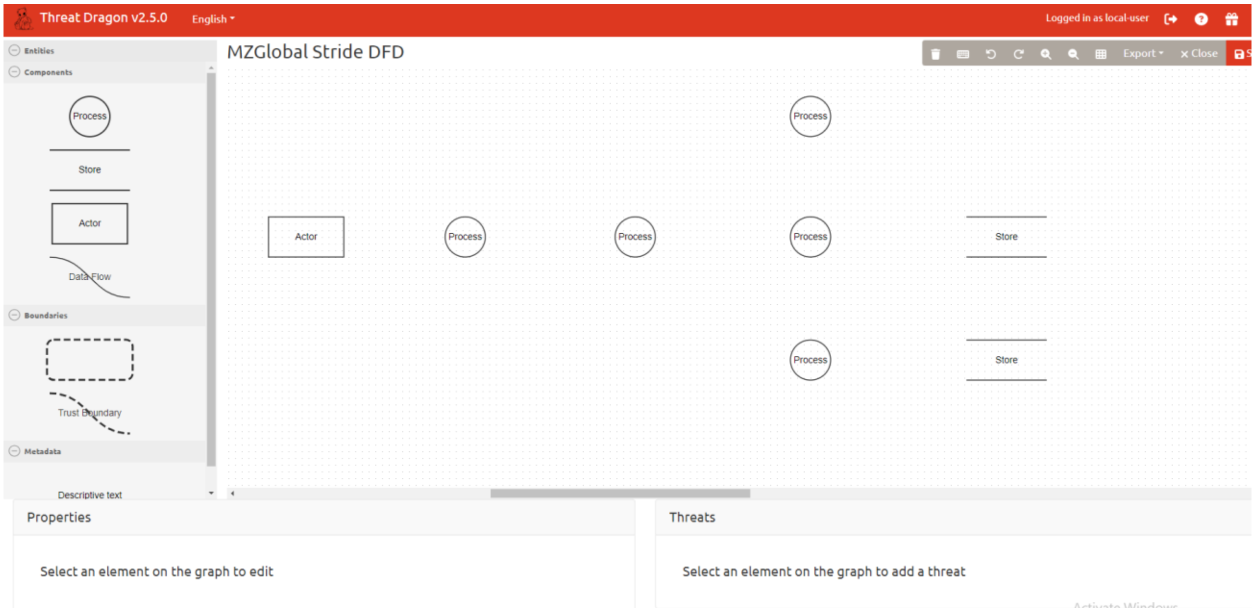
High level system description

MZGlobal Stride DFD

We begin by creating the DFD and use the components to creat the levels and the flow of data

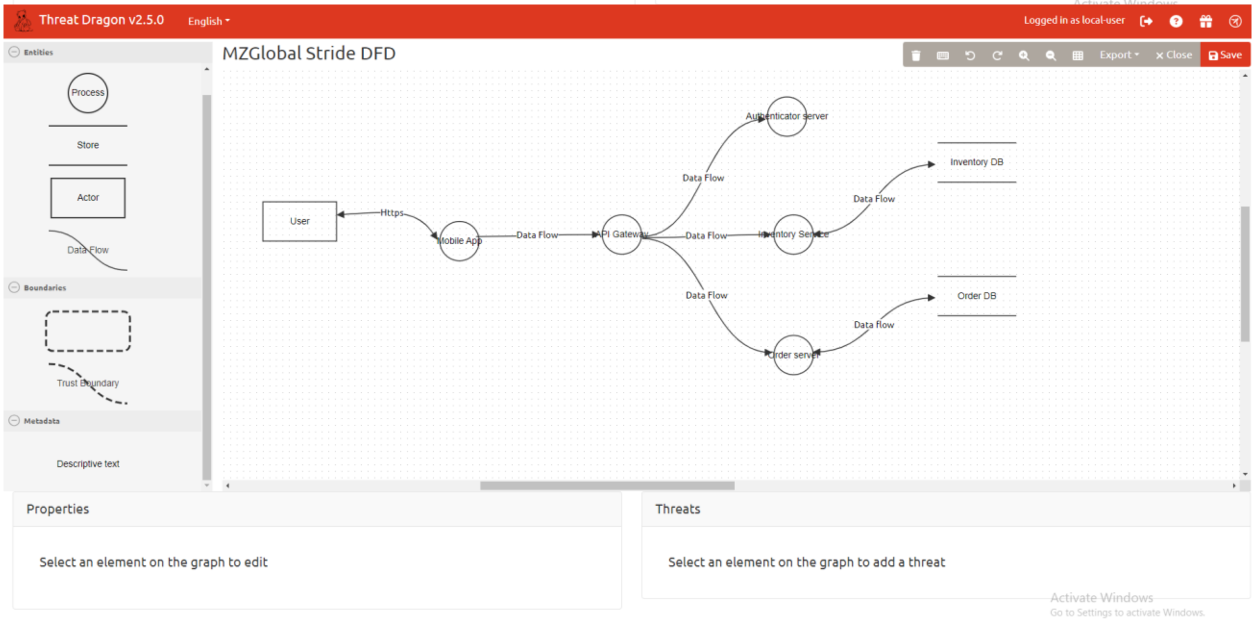


Select an element on the graph to add a threat



Select an element on the graph to edit

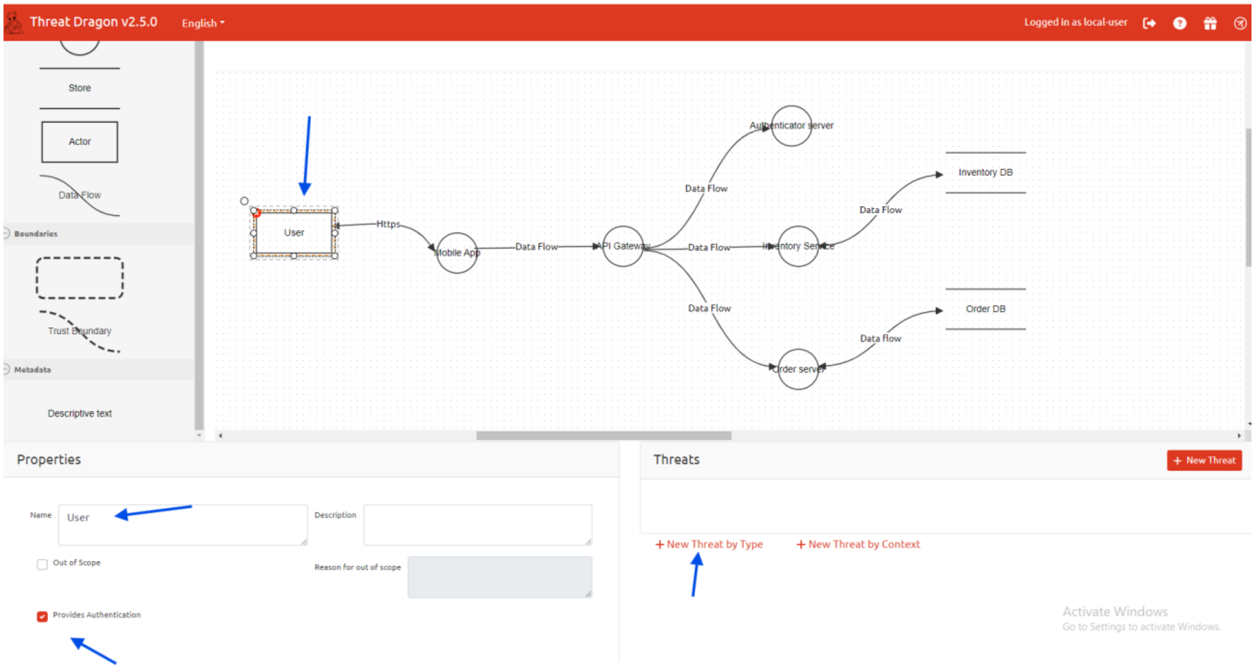
Select an element on the graph to add a threat



Select an element on the graph to edit

Select an element on the graph to add a threat

Once the diagram is done, we begin to define the properties for each level, and define the threats of each process or flow.



Properties

Name: User

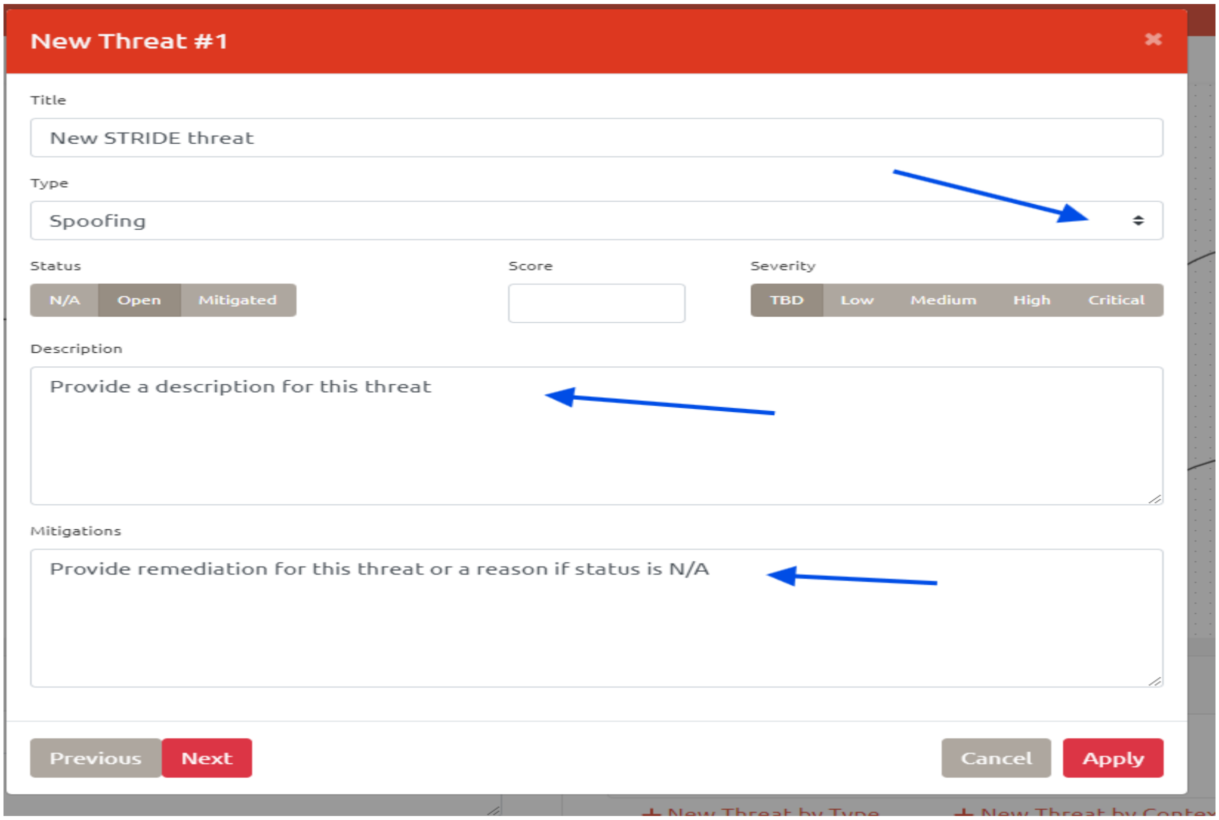
Description:

□ Out of Scope

Reason for out of scope:

☑ Provides Authentication

We describe the threat and define the mitigation for each threat , then save



Title: New STRIDE threat

Type: Spoofing

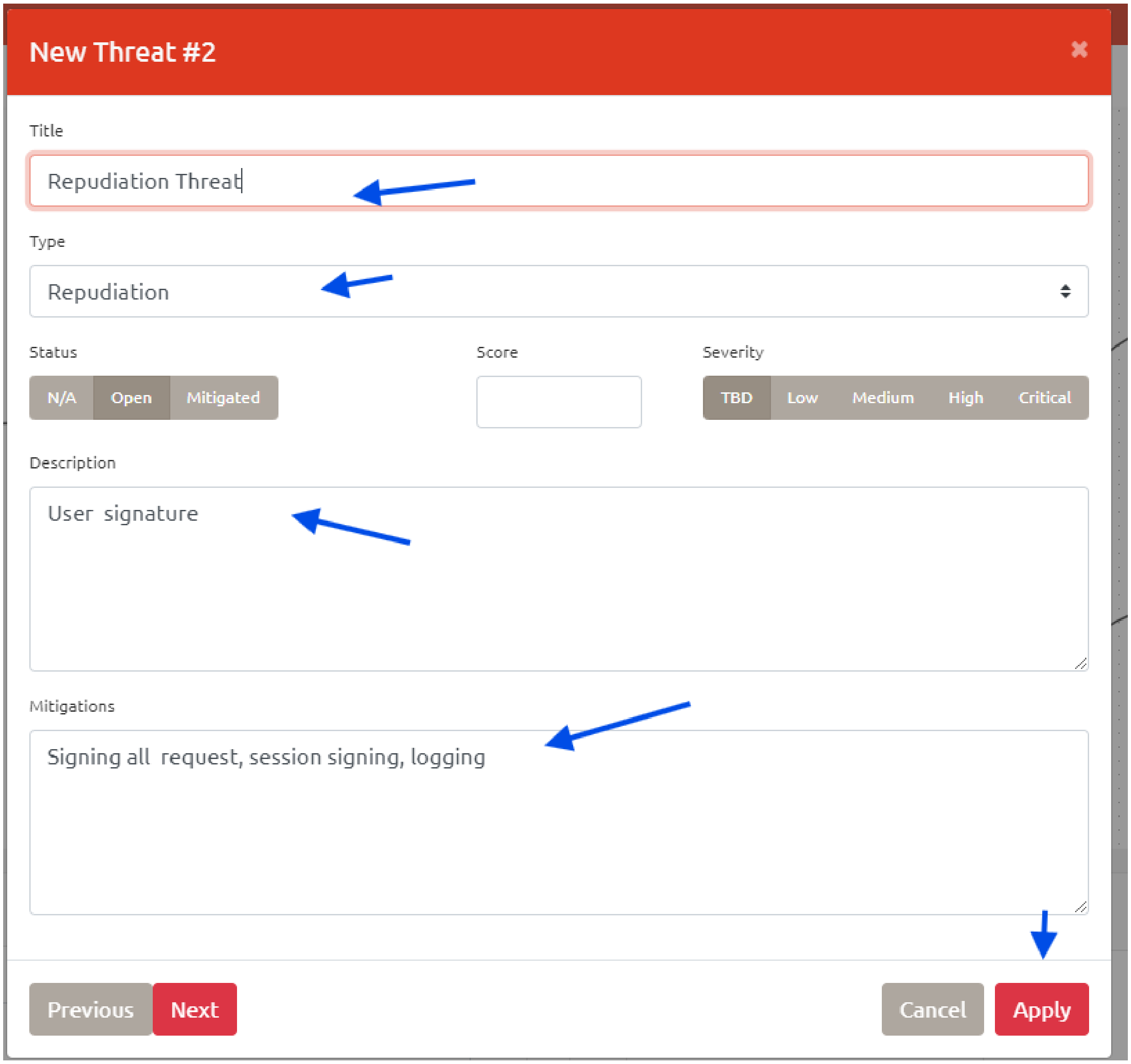
Status: N/A [✓ Open] Mitigated

Score:

Severity: [✓ TBD] Low Medium High Critical

Description: Provide a description for this threat

Mitigations: Provide remediation for this threat or a reason if status is N/A



Title

Repudiation Threat

Type

Repudiation

Status

Score

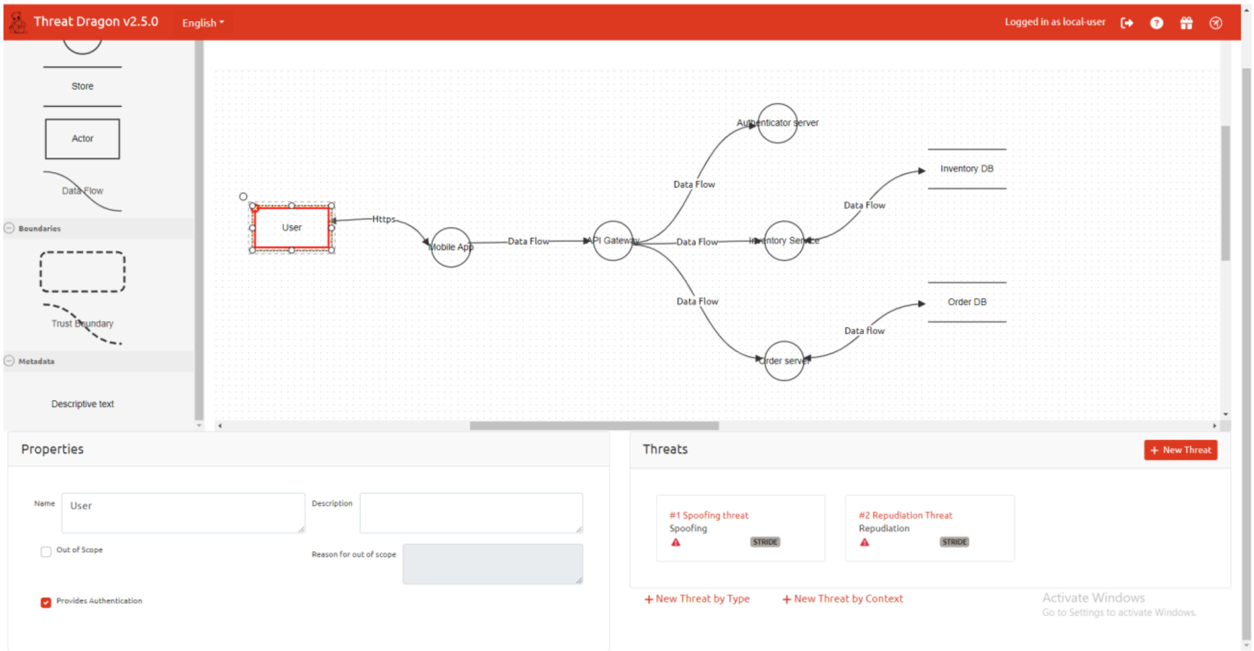
Severity

Description

User signature

Mitigations

Signing all request, session signing, logging



Properties

Name: User

Description:

□ Out of Scope

Reason for out of scope:

☑ Provides Authentication

Threats

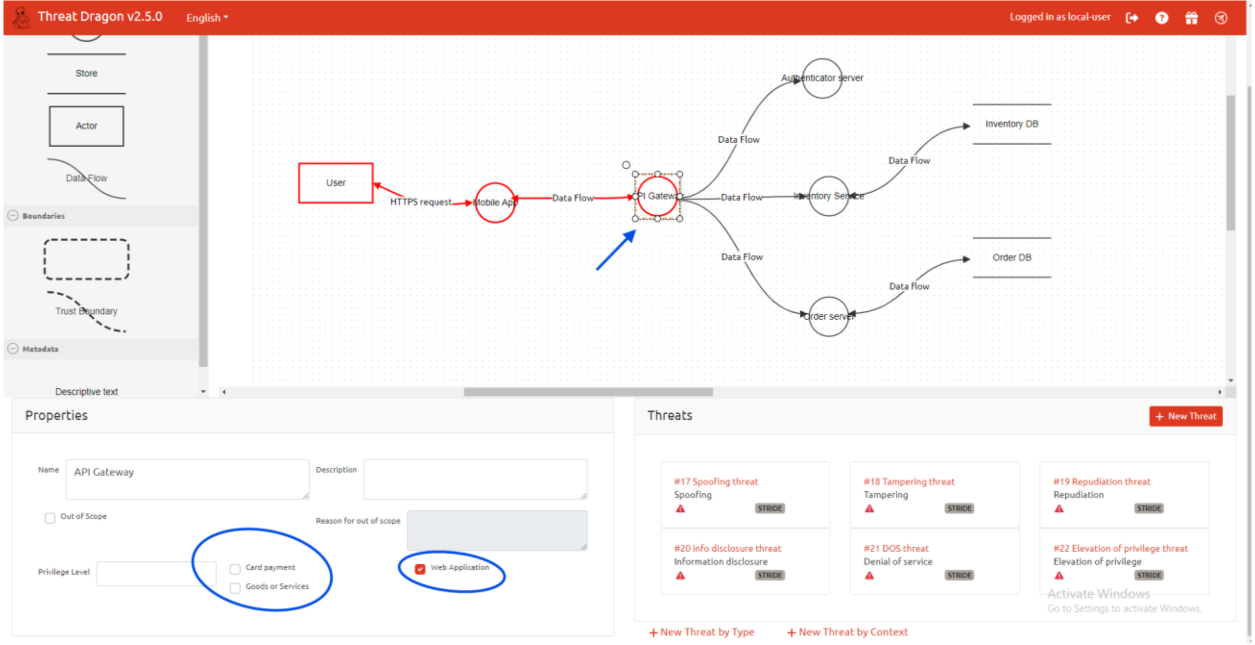
+ New Threat

#1 Spoofing threat
Spoofing
STRIDE

#2 Repudiation Threat
Repudiation
STRIDE

+ New Threat by Type
+ New Threat by Context

Now we repeat the same process for all sections of the DFD



Name: API Gateway

Description:

□ Out of Scope

Reason for out of scope:

Privilege Level:

□ Card payment

□ Goods or Services

☑ Web Application

#17 Spoofing threat — Spoofing — STRIDE

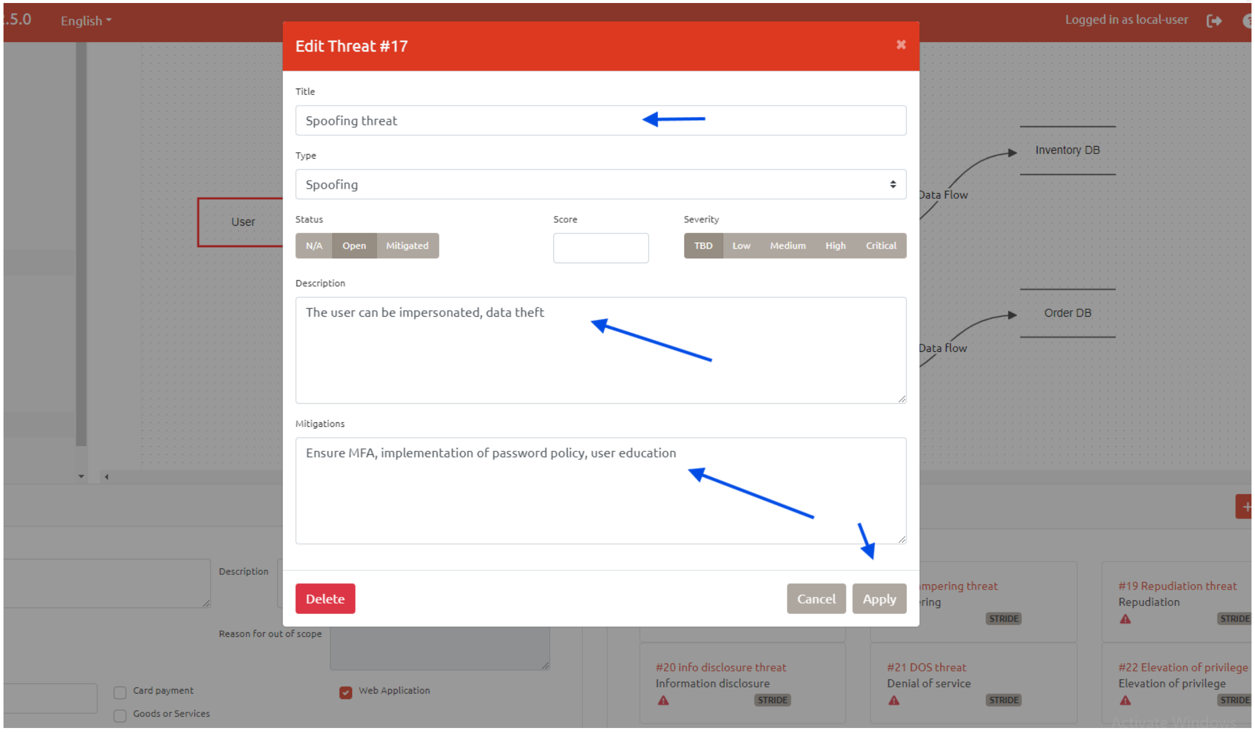
#18 Tampering threat — Tampering — STRIDE

#19 Repudiation threat — Repudiation — STRIDE

#20 info disclosure threat — Information disclosure — STRIDE

#21 DOS threat — Denial of service — STRIDE

#22 Elevation of privilege threat — Elevation of privilege — STRIDE



Edit Threat #17

Title: Spoofing threat

Type: Spoofing

Status: N/A [✓ Open] Mitigated

Score:

Severity: [✓ TBD] Low Medium High Critical

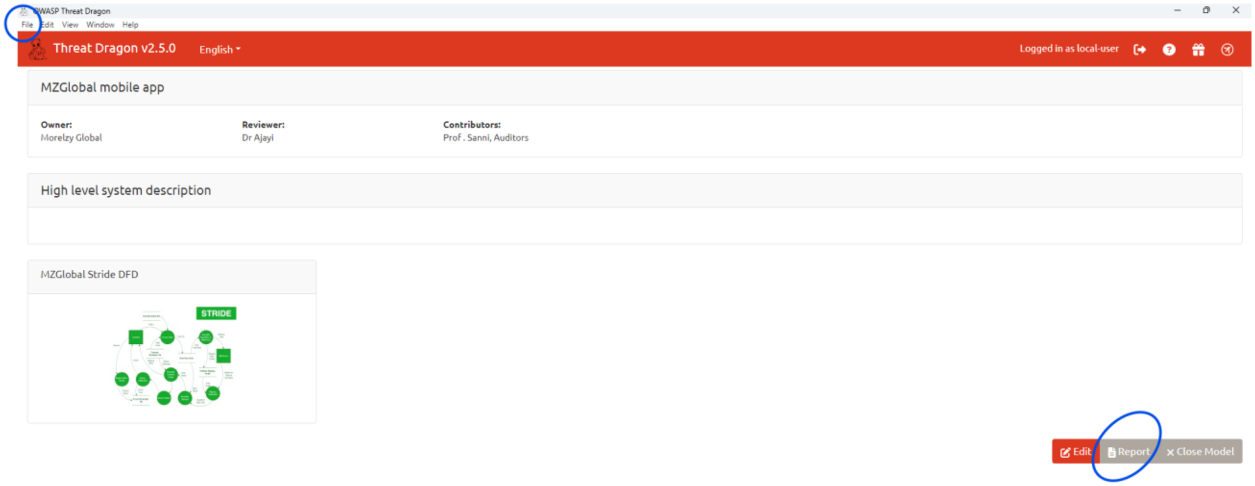
Description: The user can be impersonated, data theft

Mitigations: Ensure MFA, implementation of password policy, user education

Delete | Cancel | Apply

Once all fields and threats are defined, we save and reopen to generate a report.

This report is given to the developers to implement.



MZGlobal mobile app

Owner: Morelzy Global

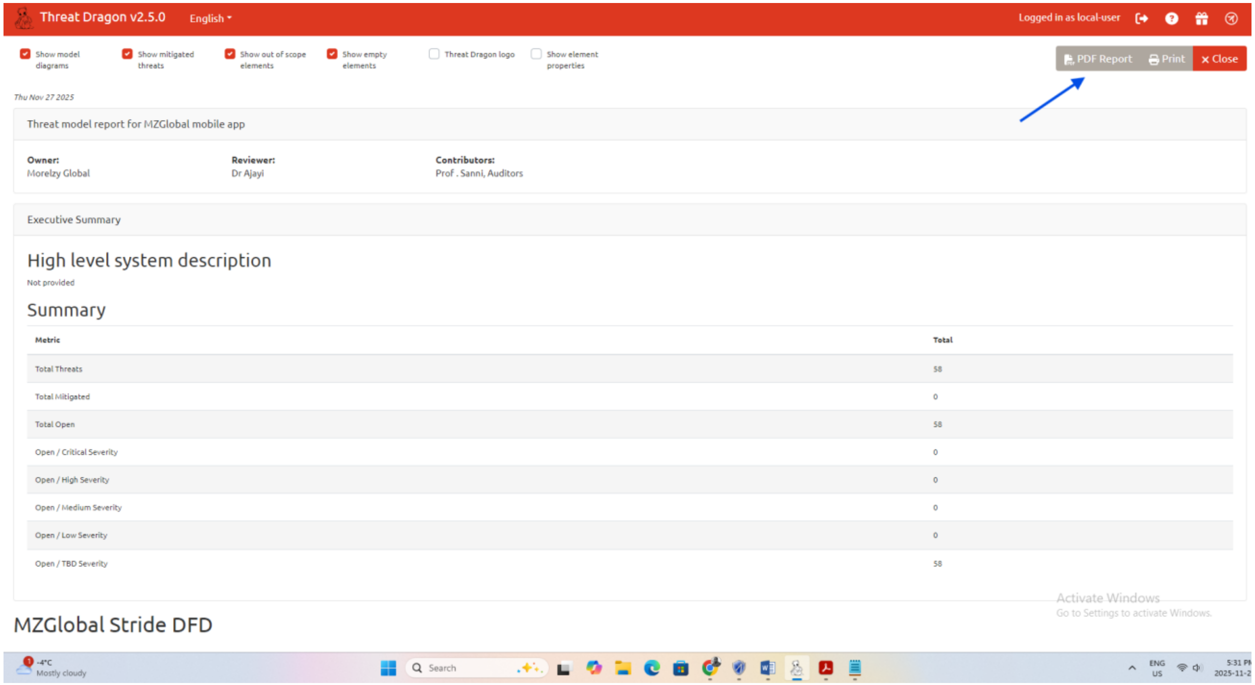
Reviewer: Dr Ajayi

Contributors: Prof . Sanni, Auditors

High level system description

MZGlobal Stride DFD

As of now , we have 58 threats



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

Thu Nov 27 2025

Threat model report for MZGlobal mobile app

Owner: Morelzy Global

Reviewer: Dr Ajayi

Contributors: Prof . Sanni, Auditors

Executive Summary

High level system description

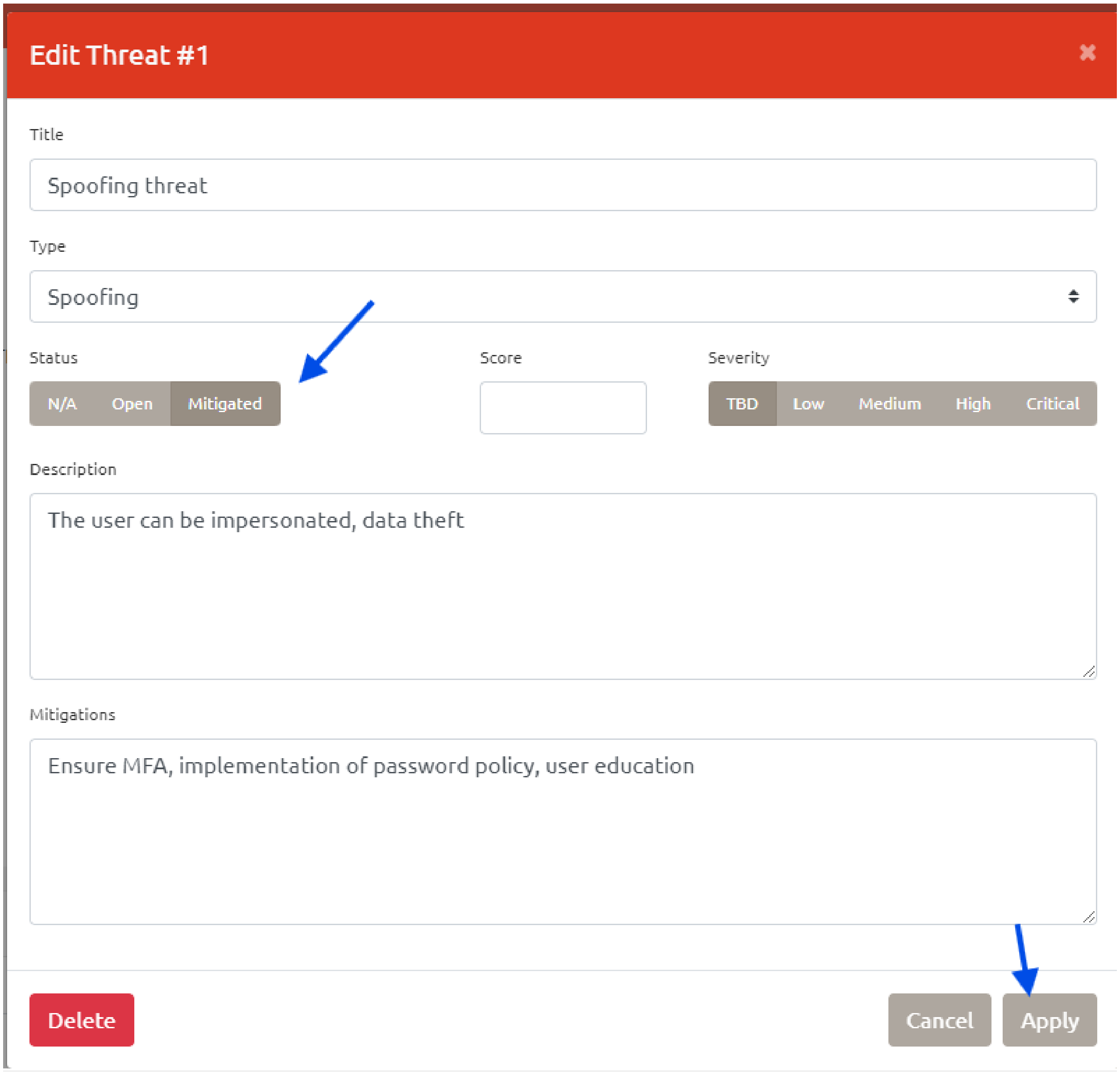
Not provided

Summary

Metric	Total
Total Threats	58
Total Mitigated	0
Total Open	58
Open / Critical Severity	0
Open / High Severity	0
Open / Medium Severity	0
Open / Low Severity	0
Open / TBD Severity	58

MZGlobal Stride DFD

When the threats have been mitigated, we return to the DFD and update the model



Edit Threat #1

Title: Spoofing threat

Type: Spoofing

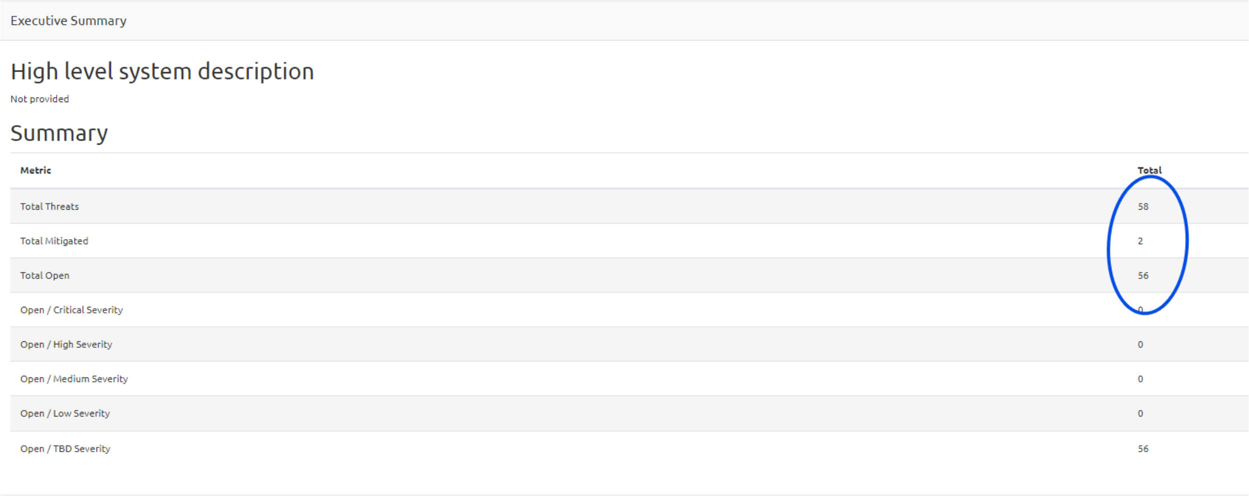
Status: N/A Open [✓ Mitigated]

Score:

Severity: [✓ TBD] Low Medium High Critical

Description: The user can be impersonated, data theft

Mitigations: Ensure MFA, implementation of password policy, user education



Executive Summary

High level system description

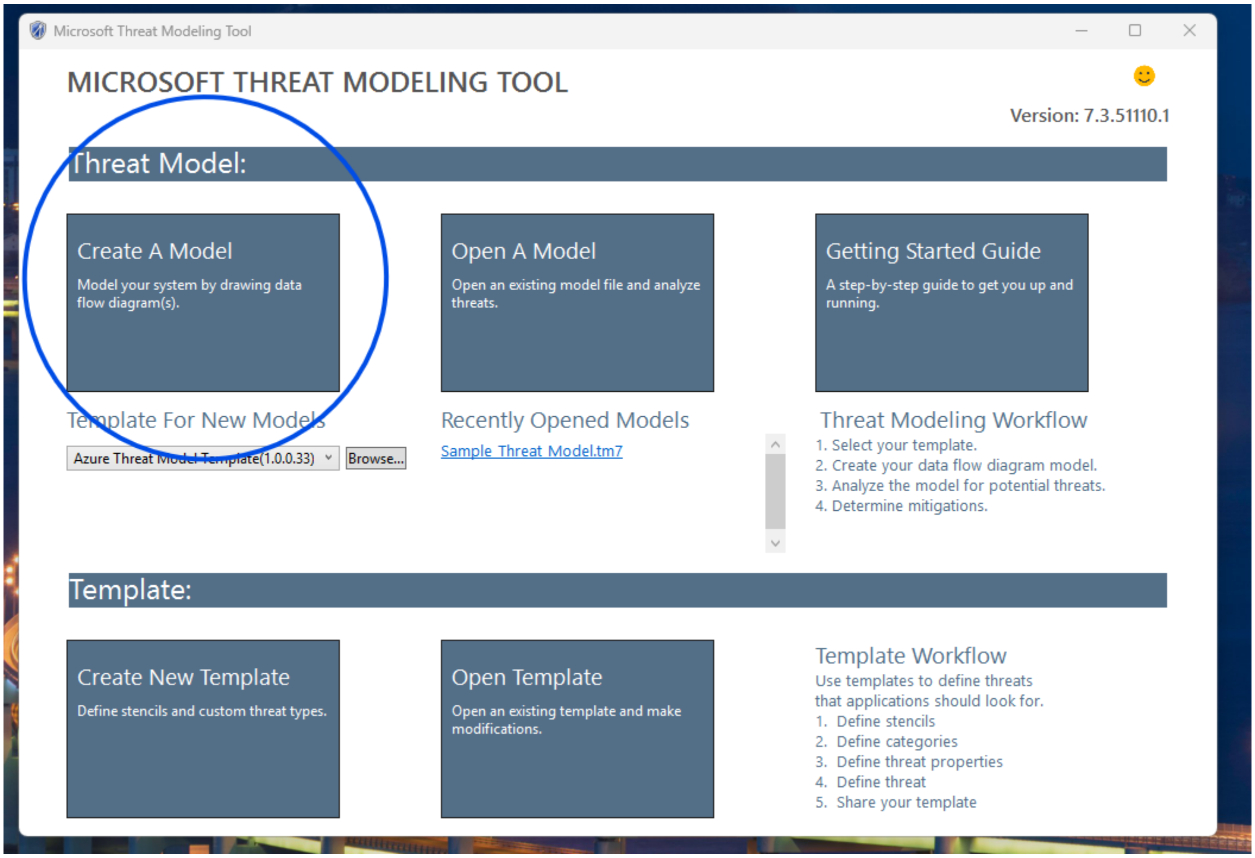
Not provided

Summary

Metric	Total
Total Threats	58
Total Mitigated	2
Total Open	56
Open / Critical Severity	0
Open / High Severity	0
Open / Medium Severity	0
Open / Low Severity	0
Open / TBD Severity	56

The process is similar for the Microsoft threat modeling tool, which can be gotten at https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool

Below are the steps for creating a threat model



MICROSOFT THREAT MODELING TOOL

Version: 7.3.51110.1

Threat Model:

Create A Model

Model your system by drawing data flow diagram(s).

Open A Model

Open an existing model file and analyze threats.

Getting Started Guide

A step-by-step guide to get you up and running.

Template For New Models

Azure Threat Model Template(1.0.0.33)

Recently Opened Models

Sample Threat Model.tm7

Threat Modeling Workflow

1. Select your template.
2. Create your data flow diagram model.
3. Analyze the model for potential threats.
4. Determine mitigations.

Template:

Create New Template

Define stencils and custom threat types.

Open Template

Open an existing template and make modifications.

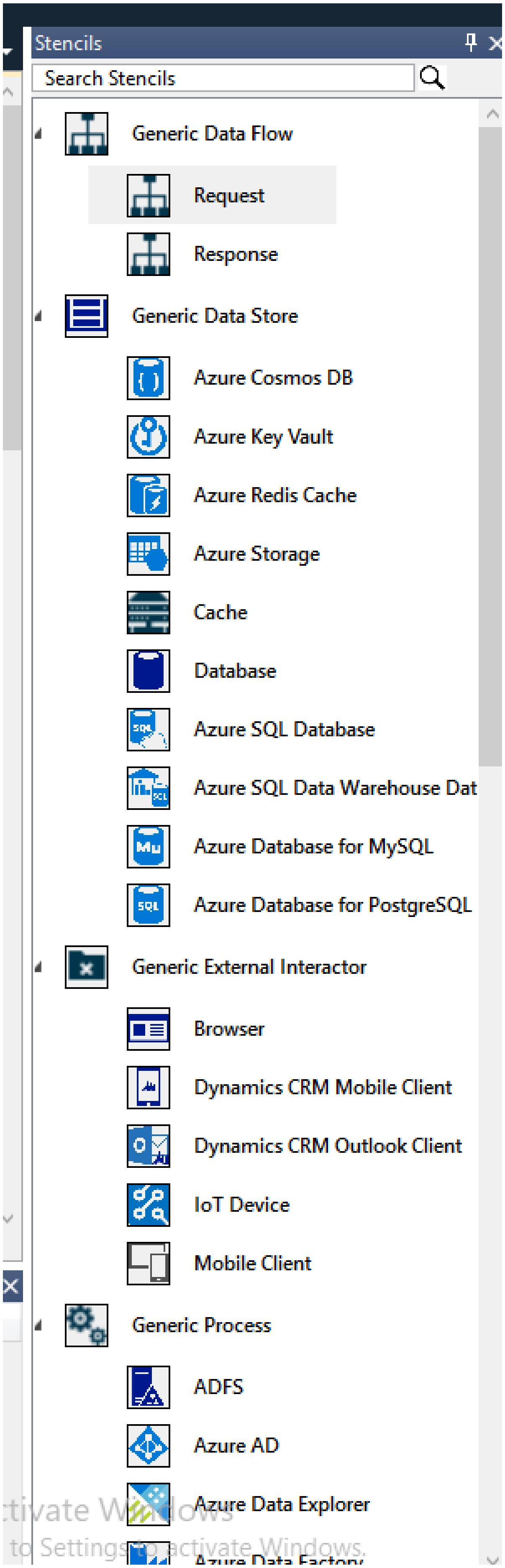
Template Workflow

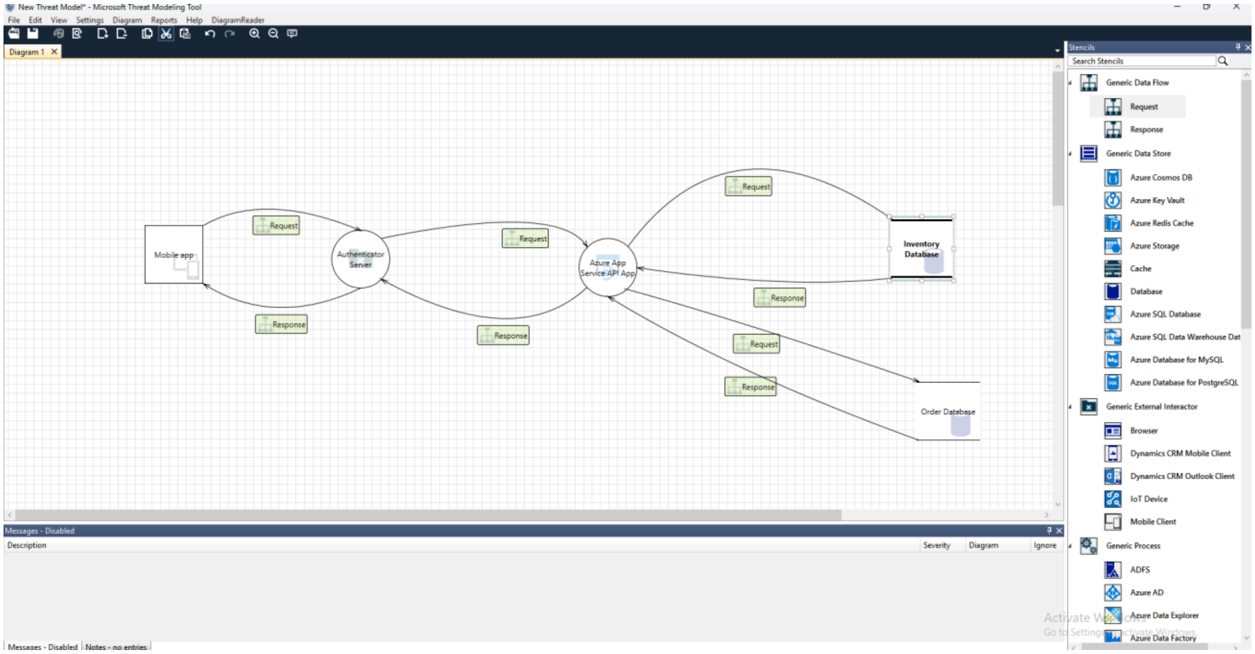
Use templates to define threats that applications should look for.

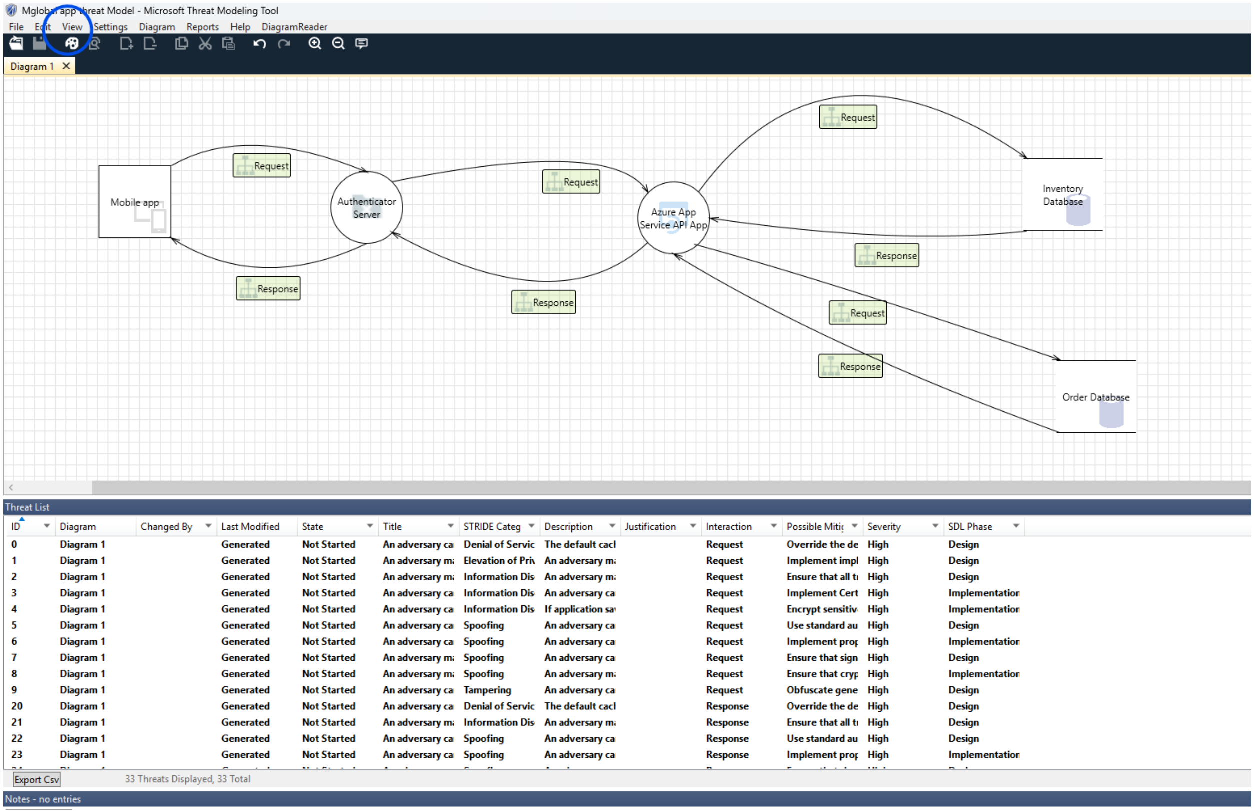
1. Define stencils
2. Define categories
3. Define threat properties
4. Define threat
5. Share your template

The left side of the screen contain tools to crate the DFD.

Once the DFD is complete and the properties of each section has been defined


Stencils
Search Stencils
Generic Data Flow
Request
Response
Generic Data Store
Azure Cosmos DB
Azure Key Vault
Azure Redis Cache
Azure Storage
Cache
Database
Azure SQL Database
Azure SQL Data Warehouse Dat
Azure Database for MySQL
Azure Database for PostgreSQL
Generic External Interactor
Browser
Dynamics CRM Mobile Client
Dynamics CRM Outlook Client
IoT Device
Mobile Client
Generic Process
ADFS
Azure AD
Azure Data Explorer
Azure Data Factory
tivate Windows
to Settings to activate Windows.





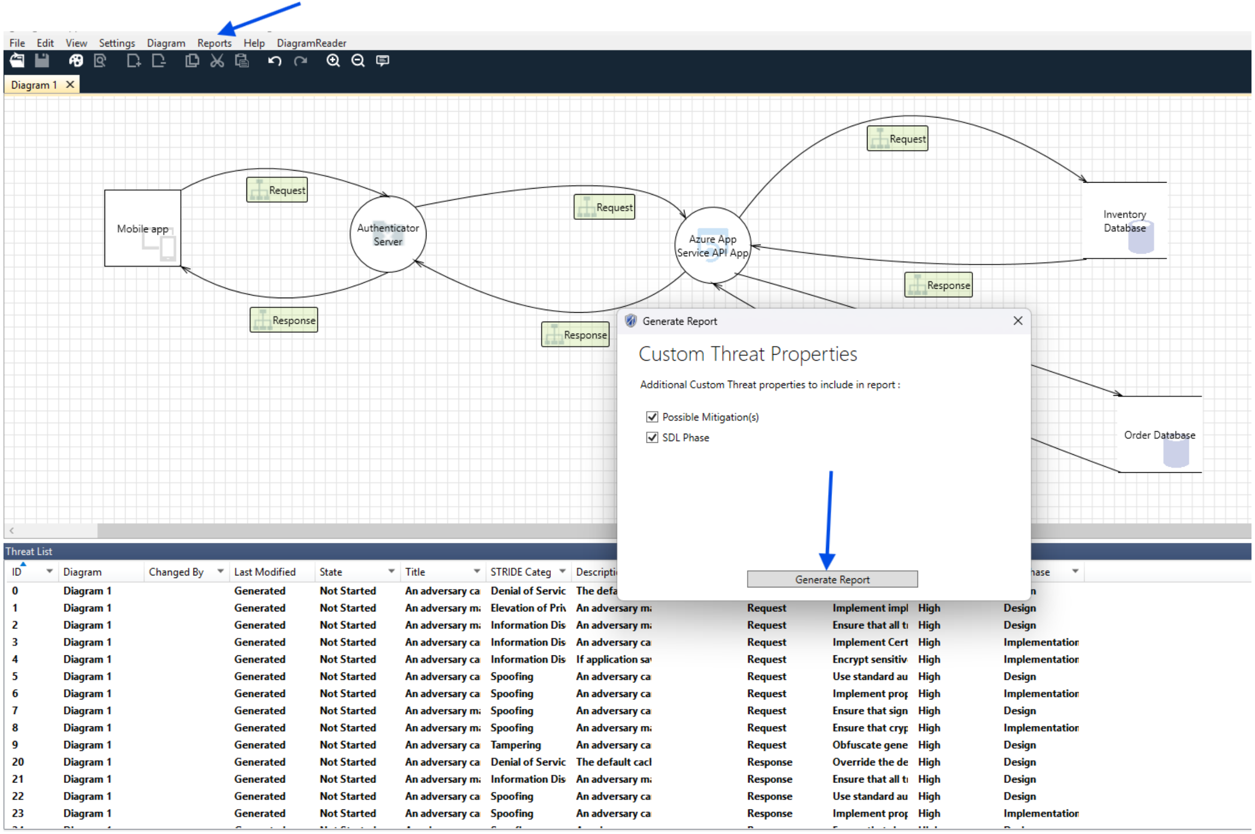
Threat List

ID	Diagram	Changed By	Last Modified	State	Title	STRIDE Categ	Description	Justification	Interaction	Possible Mitig	Severity	SDL Phase
0	Diagram 1		Generated	Not Started	An adversary ca	Denial of Servic	The default cacl		Request	Override the de	High	Design
1	Diagram 1		Generated	Not Started	An adversary ma	Elevation of Priv	An adversary ma		Request	Implement impl	High	Design
2	Diagram 1		Generated	Not Started	An adversary ma	Information Dis	An adversary ma		Request	Ensure that all t	High	Design
3	Diagram 1		Generated	Not Started	An adversary ca	Information Dis	An adversary ca		Request	Implement Cert	High	Implementation
4	Diagram 1		Generated	Not Started	An adversary ca	Information Dis	If application sa		Request	Encrypt sensitiv	High	Implementation
5	Diagram 1		Generated	Not Started	An adversary ca	Spoofing	An adversary ca		Request	Use standard au	High	Design
6	Diagram 1		Generated	Not Started	An adversary ca	Spoofing	An adversary ca		Request	Implement prop	High	Implementation
7	Diagram 1		Generated	Not Started	An adversary ma	Spoofing	An adversary ca		Request	Ensure that sign	High	Design
8	Diagram 1		Generated	Not Started	An adversary ma	Spoofing	An adversary ma		Request	Ensure that cryp	High	Implementation
9	Diagram 1		Generated	Not Started	An adversary ca	Tampering	An adversary ca		Request	Obfuscate gene	High	Design
20	Diagram 1		Generated	Not Started	An adversary ca	Denial of Servic	The default cacl		Response	Override the de	High	Design
21	Diagram 1		Generated	Not Started	An adversary ma	Information Dis	An adversary ma		Response	Ensure that all t	High	Design
22	Diagram 1		Generated	Not Started	An adversary ca	Spoofing	An adversary ca		Response	Use standard au	High	Design
23	Diagram 1		Generated	Not Started	An adversary ca	Spoofing	An adversary ca		Response	Implement prop	High	Implementation

33 Threats Displayed, 33 Total

Click reports and generate a report, this coan then been shared with developers.

Once threats are mitigated , we update the model



Custom Threat Properties

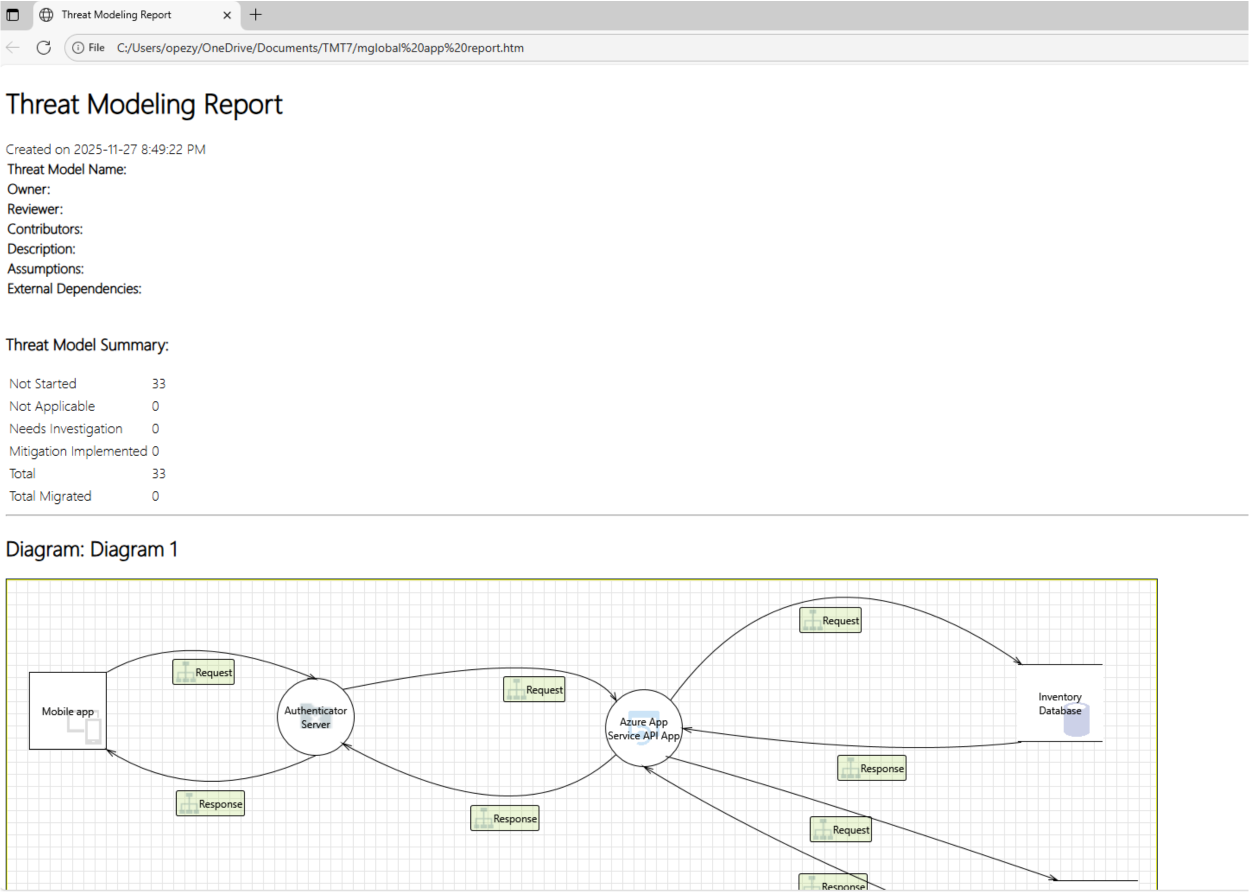
Additional Custom Threat properties to include in report :

☑ Possible Mitigation(s)

☑ SDL Phase

Threat List

ID	Diagram	Changed By	Last Modified	State	Title	STRIDE Categ	Descripti				hase
0	Diagram 1		Generated	Not Started	An adversary ca	Denial of Servic	The defa				n
1	Diagram 1		Generated	Not Started	An adversary m	Elevation of Priv	An adversary m	Request	Implement impl	High	Design
2	Diagram 1		Generated	Not Started	An adversary m	Information Dis	An adversary m	Request	Ensure that all t	High	Design
3	Diagram 1		Generated	Not Started	An adversary ca	Information Dis	An adversary ca	Request	Implement Cert	High	Implementation
4	Diagram 1		Generated	Not Started	An adversary ca	Information Dis	If application sa	Request	Encrypt sensitiv	High	Implementation
5	Diagram 1		Generated	Not Started	An adversary ca	Spoofing	An adversary ca	Request	Use standard au	High	Design
6	Diagram 1		Generated	Not Started	An adversary ca	Spoofing	An adversary ca	Request	Implement prop	High	Implementation
7	Diagram 1		Generated	Not Started	An adversary m	Spoofing	An adversary ca	Request	Ensure that sign	High	Design
8	Diagram 1		Generated	Not Started	An adversary m	Spoofing	An adversary m	Request	Ensure that cryp	High	Implementation
9	Diagram 1		Generated	Not Started	An adversary ca	Tampering	An adversary ca	Request	Obfuscate gene	High	Design
20	Diagram 1		Generated	Not Started	An adversary ca	Denial of Servic	The default cacl	Response	Override the de	High	Design
21	Diagram 1		Generated	Not Started	An adversary m	Information Dis	An adversary m	Response	Ensure that all t	High	Design
22	Diagram 1		Generated	Not Started	An adversary ca	Spoofing	An adversary ca	Response	Use standard au	High	Design
23	Diagram 1		Generated	Not Started	An adversary ca	Spoofing	An adversary ca	Response	Implement prop	High	Implementation



Threat Modeling Report

Created on 2025-11-27 8:49:22 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	33
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	33
Total Migrated	0

Diagram: Diagram 1

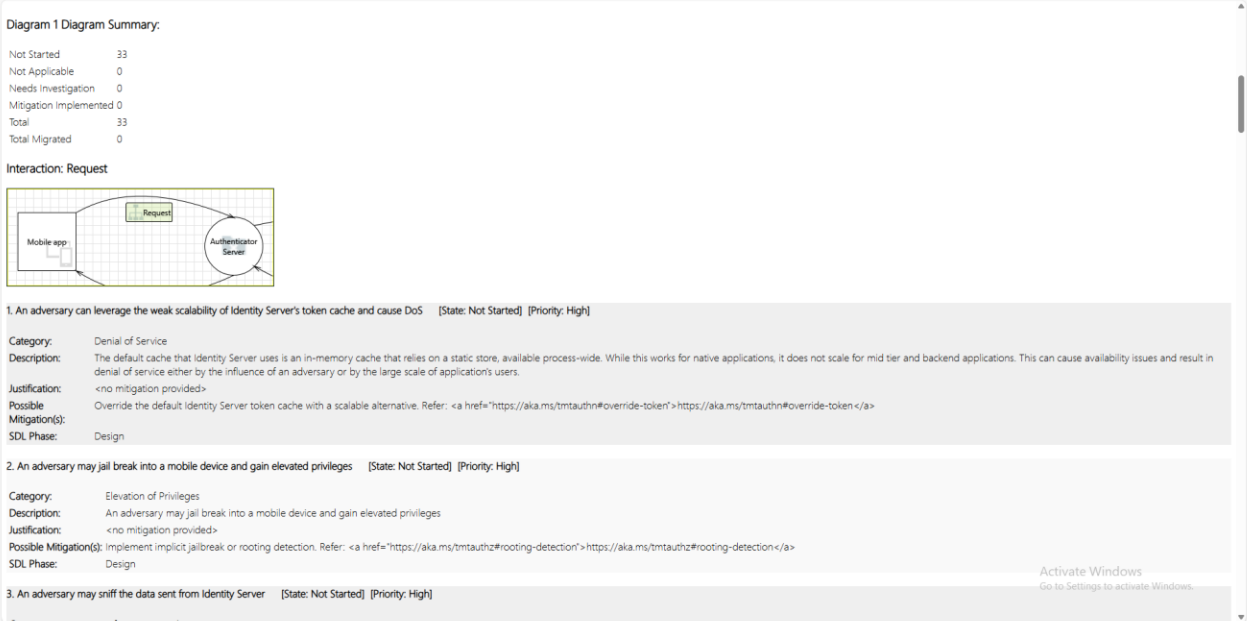


Diagram 1 Diagram Summary:

Not Started	33
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	33
Total Migrated	0

Interaction: Request

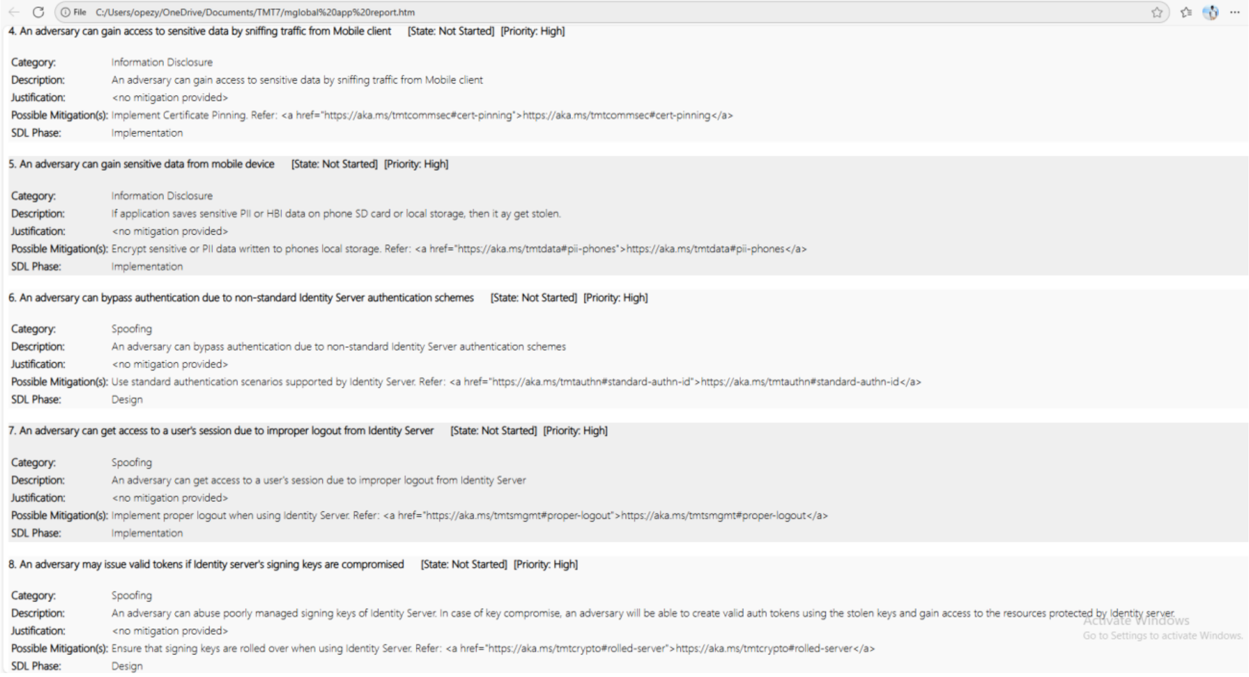
1. An adversary can leverage the weak scalability of Identity Server's token cache and cause DoS [State: Not Started] [Priority: High]

Category: Denial of Service
Description: The default cache that Identity Server uses is an in-memory cache that relies on a static store, available process-wide. While this works for native applications, it does not scale for mid tier and backend applications. This can cause availability issues and result in denial of service either by the influence of an adversary or by the large scale of application's users.
Justification: <no mitigation provided>
Possible Mitigation(s): Override the default Identity Server token cache with a scalable alternative. Refer: <a href="https://aka.ms/tmtauthn#override-token">https://aka.ms/tmtauthn#override-token</a>
SDL Phase: Design

2. An adversary may jail break into a mobile device and gain elevated privileges [State: Not Started] [Priority: High]

Category: Elevation of Privileges
Description: An adversary may jail break into a mobile device and gain elevated privileges
Justification: <no mitigation provided>
Possible Mitigation(s): Implement implicit jailbreak or rooting detection. Refer: <a href="https://aka.ms/tmtauthz#rooting-detection">https://aka.ms/tmtauthz#rooting-detection</a>
SDL Phase: Design

3. An adversary may sniff the data sent from Identity Server [State: Not Started] [Priority: High]


File C:/Users/opezy/OneDrive/Documents/TMT7/mglobal%20app%20report.htm

4. An adversary can gain access to sensitive data by sniffing traffic from Mobile client [State: Not Started] [Priority: High]

Category: Information Disclosure
Description: An adversary can gain access to sensitive data by sniffing traffic from Mobile client
Justification: <no mitigation provided>
Possible Mitigation(s): Implement Certificate Pinning. Refer: <a href="https://aka.ms/tmtcommsec#cert-pinning">https://aka.ms/tmtcommsec#cert-pinning</a>
SDL Phase: Implementation

5. An adversary can gain sensitive data from mobile device [State: Not Started] [Priority: High]

Category: Information Disclosure
Description: If application saves sensitive PII or HBI data on phone SD card or local storage, then it ay get stolen.
Justification: <no mitigation provided>
Possible Mitigation(s): Encrypt sensitive or PII data written to phones local storage. Refer: <a href="https://aka.ms/tmtdata#pii-phones">https://aka.ms/tmtdata#pii-phones</a>
SDL Phase: Implementation

6. An adversary can bypass authentication due to non-standard Identity Server authentication schemes [State: Not Started] [Priority: High]

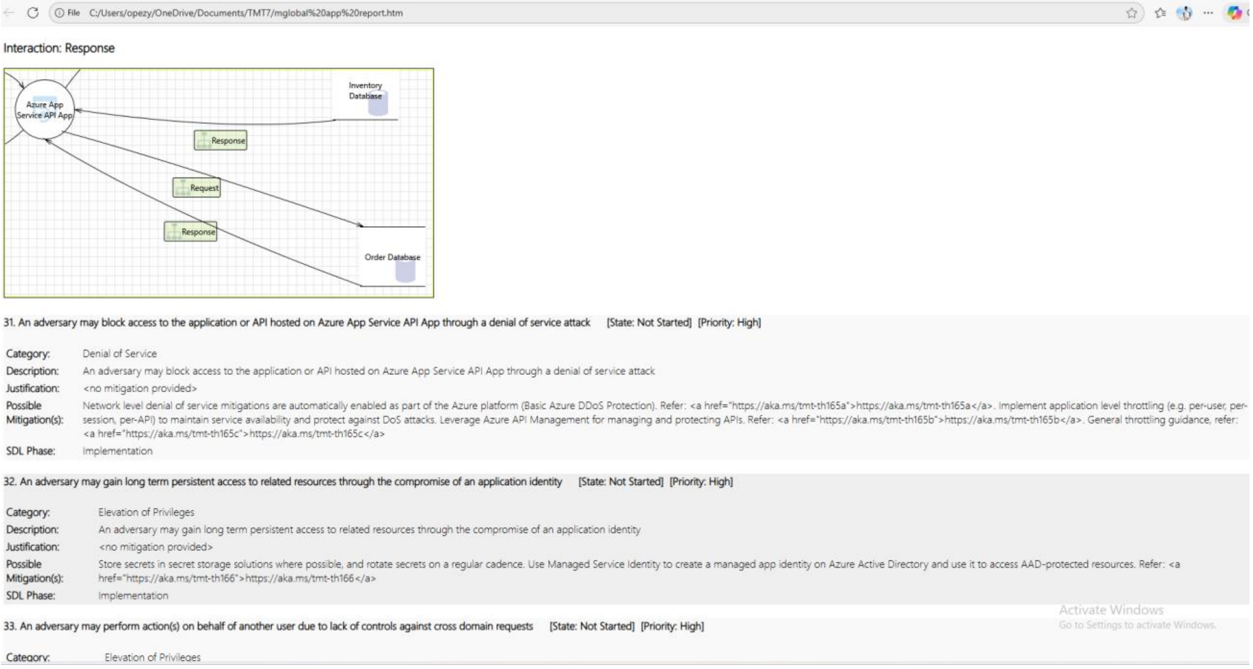
Category: Spoofing
Description: An adversary can bypass authentication due to non-standard Identity Server authentication schemes
Justification: <no mitigation provided>
Possible Mitigation(s): Use standard authentication scenarios supported by Identity Server. Refer: <a href="https://aka.ms/tmtauthn#standard-authn-id">https://aka.ms/tmtauthn#standard-authn-id</a>
SDL Phase: Design

7. An adversary can get access to a user's session due to improper logout from Identity Server [State: Not Started] [Priority: High]

Category: Spoofing
Description: An adversary can get access to a user's session due to improper logout from Identity Server
Justification: <no mitigation provided>
Possible Mitigation(s): Implement proper logout when using Identity Server. Refer: <a href="https://aka.ms/tmtsmgmt#proper-logout">https://aka.ms/tmtsmgmt#proper-logout</a>
SDL Phase: Implementation

8. An adversary may issue valid tokens if Identity server's signing keys are compromised [State: Not Started] [Priority: High]

Category: Spoofing
Description: An adversary can abuse poorly managed signing keys of Identity Server. In case of key compromise, an adversary will be able to create valid auth tokens using the stolen keys and gain access to the resources protected by Identity server.
Justification: <no mitigation provided>
Possible Mitigation(s): Ensure that signing keys are rolled over when using Identity Server. Refer: <a href="https://aka.ms/tmtcrypto#rolled-server">https://aka.ms/tmtcrypto#rolled-server</a>
SDL Phase: Design


File C:/Users/opezy/OneDrive/Documents/TMT7/mglobal%20app%20report.htm
Azure App Service API App
Inventory Database
Response
Request
Response
Order Database

Interaction: Response

31. An adversary may block access to the application or API hosted on Azure App Service API App through a denial of service attack [State: Not Started] [Priority: High]

Category: Denial of Service
Description: An adversary may block access to the application or API hosted on Azure App Service API App through a denial of service attack
Justification: <no mitigation provided>
Possible Mitigation(s): Network level denial of service mitigations are automatically enabled as part of the Azure platform (Basic Azure DDoS Protection). Refer: <a href="https://aka.ms/tmt-th165a">https://aka.ms/tmt-th165a</a>. Implement application level throttling (e.g. per-user, per-session, per-API) to maintain service availability and protect against DoS attacks. Leverage Azure API Management for managing and protecting APIs. Refer: <a href="https://aka.ms/tmt-th165b">https://aka.ms/tmt-th165b</a>. General throttling guidance, refer: <a href="https://aka.ms/tmt-th165c">https://aka.ms/tmt-th165c</a>
SDL Phase: Implementation

32. An adversary may gain long term persistent access to related resources through the compromise of an application identity [State: Not Started] [Priority: High]

Category: Elevation of Privileges
Description: An adversary may gain long term persistent access to related resources through the compromise of an application identity
Justification: <no mitigation provided>
Possible Mitigation(s): Store secrets in secret storage solutions where possible, and rotate secrets on a regular cadence. Use Managed Service Identity to create a managed app identity on Azure Active Directory and use it to access AAD-protected resources. Refer: <a href="https://aka.ms/tmt-th166">https://aka.ms/tmt-th166</a>
SDL Phase: Implementation

33. An adversary may perform action(s) on behalf of another user due to lack of controls against cross domain requests [State: Not Started] [Priority: High]

Category: Elevation of Privileges

Threat modeling helps teams think like attackers to identify weaknesses early in the design process.

- **OWASP Threat Dragon** → *Open-source, lightweight, simple to use; great for collaborative, accessible threat modeling.*
- **Microsoft Threat Modeling Tool** → *Enterprise-grade, detailed, and backed by strong STRIDE automation; ideal for large-scale or Microsoft-based environments.*

Both tools support secure-by-design principles and help organizations build safer software from the ground up.