

**SteelCon 2025**

**Threat Modelling Workshop  
Using Microsoft Threat Modelling Tool**

**Andrea Jones**



## Contents

Introduction to Threat Modelling .....	1
Data Flow Diagrams .....	2
Trust Boundaries .....	4
Threat Modelling Frameworks .....	5
STRIDE .....	5
LINDDUN .....	5
DREAD .....	5
PASTA .....	5
OCTAVE .....	6
Threat Identification Using STRIDE .....	6
Mitigating Threats .....	8
Creating Threat Modelling Tool Templates .....	9
Creating Stencils .....	12
Modifying the Threats Form .....	15
Creating Threats .....	16
Creating a Model .....	17
Bi-directional data flows .....	19
Recalculating Threats .....	20
Creating a Report .....	20



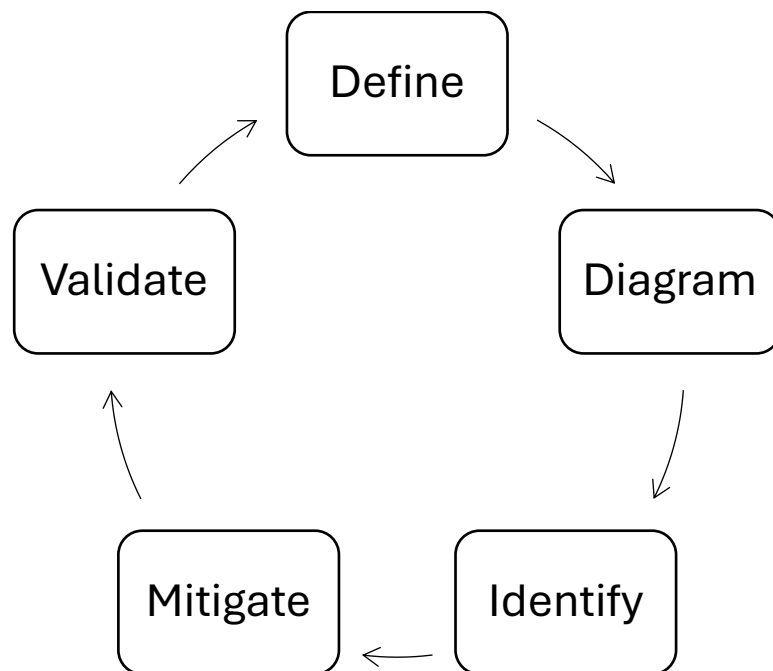
## **Introduction to Threat Modelling**

This workshop will give a brief overview of threat modelling and show how you can customize Microsoft's free Threat Modelling Tool to build a library of potential threat information.

The Threat Modelling Manifesto [www.threatmodelingmanifesto.org](http://www.threatmodelingmanifesto.org) describes the four steps of threat modelling:

Diagram	What are we building?
Threats	What can go wrong?
Mitigations	What are we going to do about it?
Evaluate	Did we do a good enough job?

Microsoft represent the threat modelling process as a continuous cycle, aligning it more with the development lifecycle:


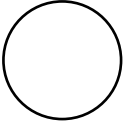
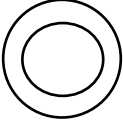





This workshop is based on the OWASP Threat Modelling Process available at [https://www.owasp.org/www-community/Threat\\_Modeling\\_Process](https://www.owasp.org/www-community/Threat_Modeling_Process).

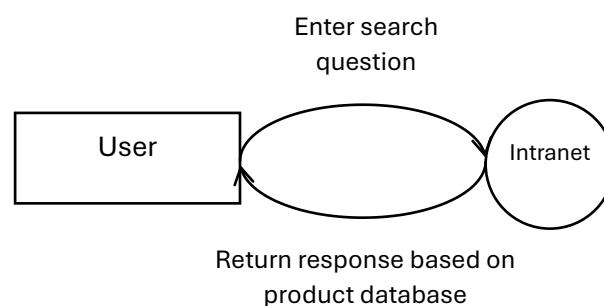
For this workshop we are going to consider a company intranet with search functionality provided by Azure AI Search, this can index information from sources such as databases or document repositories and present answers to questions submitted through prompts to the search facility on the intranet site.

## Data Flow Diagrams

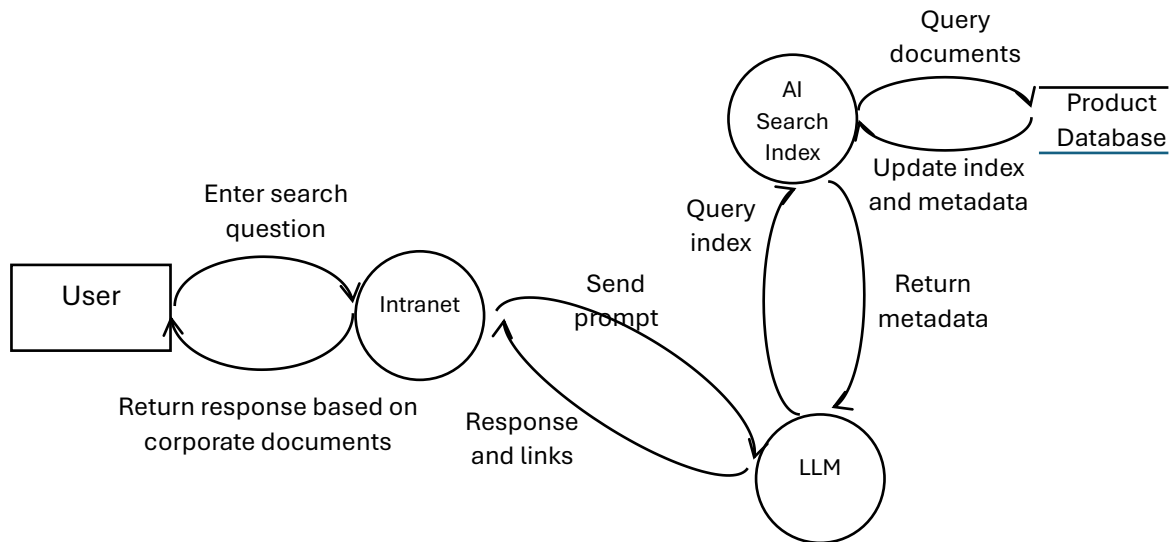
Data flow diagrams are created to represent the components of a system and help discover potential things that can go wrong. There are 5 symbols used in a data flow diagram:

Name	Symbol	Description
External entity		Entities outside the application that interact with the system, can be another application or a person.
Process		Tasks that process data or perform actions based on the data, e.g. web app, API.
Multiple Process		Represents a collection of sub-processes that can be broken down in another data flow diagram
Data Store		A location where data is stored (this does not modify the data)
Data Flow		Used to show the movement of data in the application.
Trust Boundary		Represents a change in trust levels as data flows through an application, this may be a point where the application could be attacked.

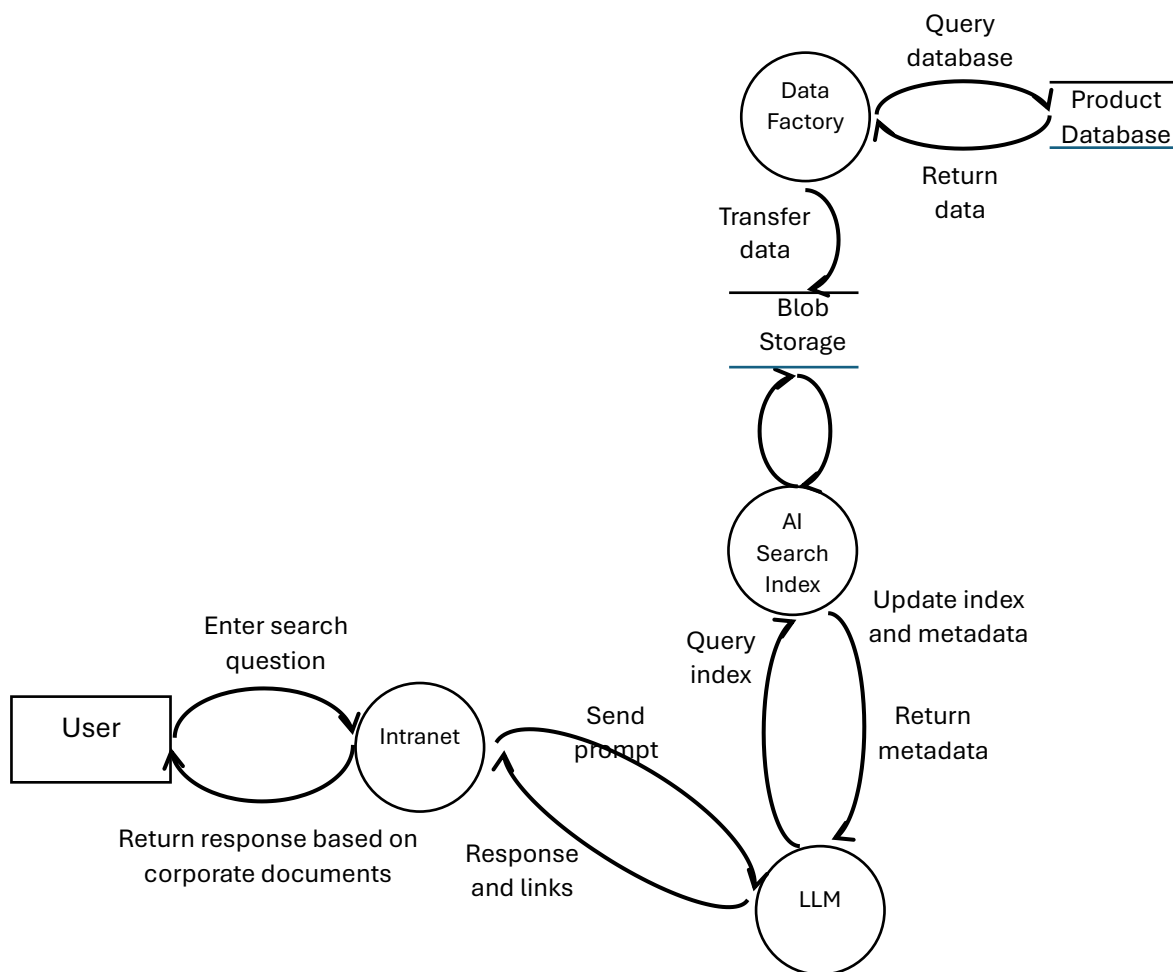
Data flow diagrams are produced to represent different levels of detail as you work through the process. The highest level (DFD 0) is called the 'contextual DFD' and gives an overview of the main functions of the application. Here is a DFD 0 diagram for our scenario:



This can be broken down further to produce a level 1 DFD:



Since Azure AI Search cannot index the database directly, the content is first extracted into Azure Storage using Azure Data Factory. Here is a level 2 DFD showing this extra detail:



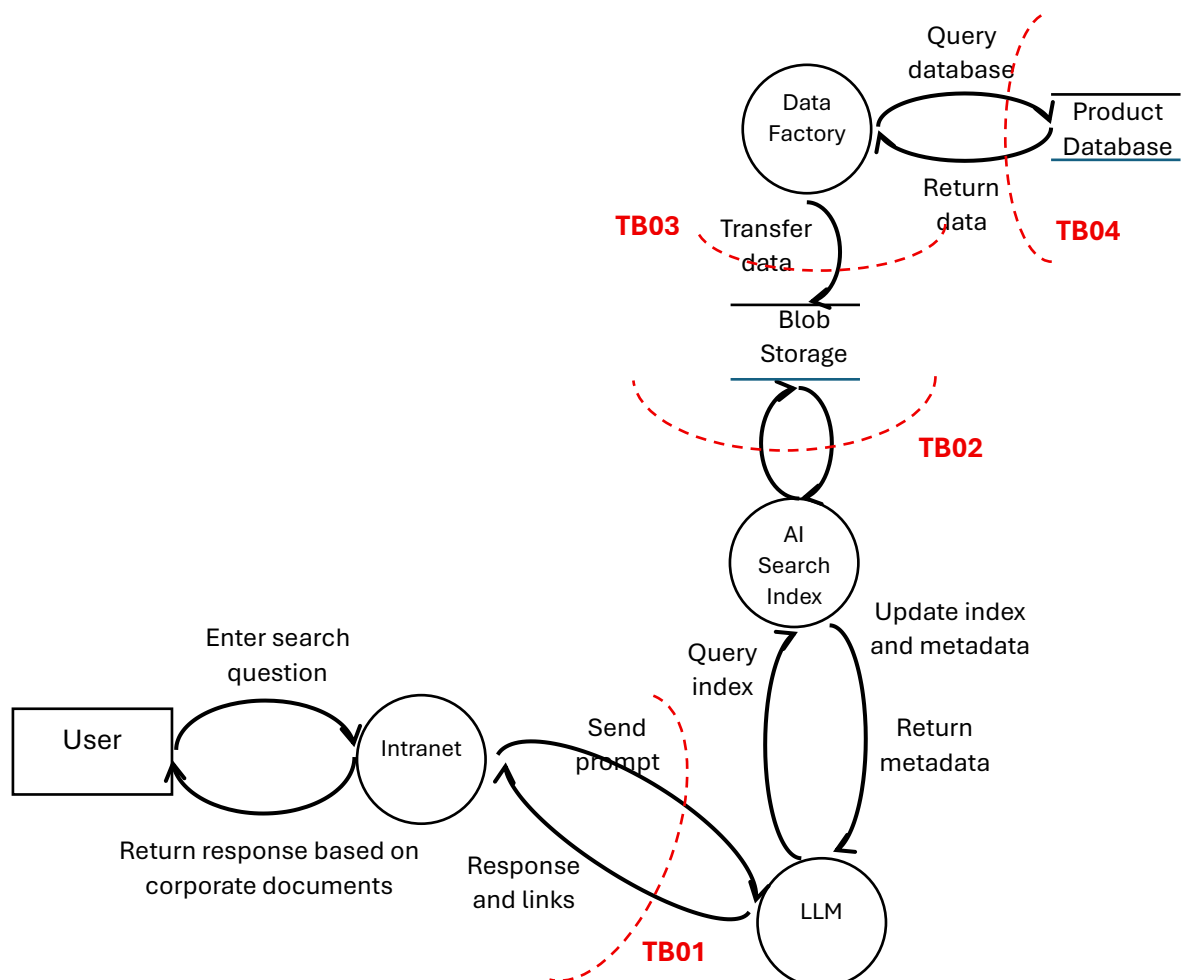
If necessary, you can break processes down even further, it is best to limit a DFD to a maximum of about 6-9 processes. Each process should be numbered according to the level of DFD diagram it appears on. Here is how we would number our processes:

Process	DFD 0 ID	DFD 1 ID	DFD 2 ID
Intranet	1	1.1	1.1.1
LLM		1.2	1.2.1
AI Search Index		1.3	1.3.1
Data Factory			1.3.2

## Trust Boundaries

These are points in a system where trust levels change, processes talking across a network always have a trust boundary.

We can now add trust boundaries at the points in the diagram where there is a change in trust levels and an attack may be attempted. The trust boundaries are numbered to help identify them.





## **Threat Modelling Frameworks**

There are many different threat modelling frameworks you can when identify threats:

**STRIDE** <https://www.microsoft.com/en-us/security/blog/2007/09/11/stride-chart/>

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of privileges

Sometimes STRIDE is referred to as STRIDE-LM where the Lateral Movement category is added to the framework.

**LINDDUN** – [www.linddun.org](http://www.linddun.org)

- Linking
- Identifying
- Non-repudiation
- Detecting
- Data Disclosure
- Unawareness
- Non-compliance

LINDDUN follows a similar process to STRIDE but is more privacy focused.

**DREAD** [https://download.microsoft.com/download/d/8/c/d8c02f31-64af-438c-a9f4-e31acb8e3333/Threats\\_Countermeasures.pdf](https://download.microsoft.com/download/d/8/c/d8c02f31-64af-438c-a9f4-e31acb8e3333/Threats_Countermeasures.pdf)

- Damage potential – how big would the damage be?
- Reproducibility – How easy is it to reproduce a working attack?
- Exploitability – How much time, effort and expertise is needed?
- Affected users – What percentage of users would be affected?
- Discoverability – How easy is it for an attacker to discover this threat?

DREAD hasn't been used by Microsoft since 2010.

**PASTA** <https://versprite.com/cybersecurity-listings/offsec/threat-models/>

Process for Attack Simulation and Threat Analysis

- Define objectives
- Define technical scope
- Decompose application
- Analyse threats
- Identify vulnerabilities
- Enumerate attacks
- Analyse impact and develop countermeasures

**OCTAVE** <https://insights.sei.cmu.edu/library/operationally-critical-threat-asset-and-vulnerability-evaluation-octave-framework-version-10/>

### Operationally Critical Threat, Asset, and Vulnerability Evaluation

- Phase 1 – Build Enterprise-Wide Security Requirements
  - Process 1 – Identify enterprise knowledge
  - Process 2 – Identify operational area knowledge
  - Process 3 – Identify staff knowledge
  - Process 4 – Establish security requirements
- Phase 2 – Identify Infrastructure Vulnerabilities
  - Process 5 – Map high-priority information assets to information infrastructure
  - Process 6 – Perform infrastructure vulnerability evaluation
- Phase 3 – Determine Security Risk Management Strategy
  - Process 7 – Conduct multi-dimensional risk analysis
  - Process 8 – Develop protection strategy

## **Threat Identification Using STRIDE**

Many of the above frameworks use STRIDE for the vulnerability identification stage of their processes and we will use this in our workshop. The web page provided above for STRIDE has a useful table which includes the security properties we are trying to implement when considering each category of STRIDE:

Property	Threat	Definition
Authenticity	Spoofing	Impersonating something or someone else.
Integrity	Tampering	Modifying data or code.
Non-repudiation	Repudiation	Claiming to have not performed an action
Confidentiality	Information Disclosure	Exposing information to someone not authorised to see it.
Availability	Denial of Service	Deny or degrade service to users.
Authorisation	Elevation of Privilege	Gain capabilities without proper authorization.

It is also possible to apply STRIDE in an Artificial Intelligence/Machine Learning (AI/ML)-specific way:

Property	Threat	AI/ML-Specific Definition
Authenticity	Spoofing	The output of a model has been verifiably produced by it.
Integrity	Tampering	Information used throughout the model's lifecycle cannot be changed by unauthorised users.
Non-repudiation	Repudiation	It is not possible to deny that an output has been produced by the model.
Confidentiality	Information Disclosure	No other information is disclosed in use apart from the model's input and output.
Availability	Denial of Service	The model produces reliable information not polluted by noise.
Authorisation	Elevation of Privilege	Only authorised users can interact with the model.

When considering what could go wrong it is good to involve a number of different people to get a wide variety of ideas. However, threat modelling should be a continuous process so don't be surprised if you don't identify everything at the start and be open to someone noticing potential new threats later on. We're going to be building a template for Microsoft's Threat Modelling Tool which can be downloaded from <https://aka.ms/tmt>, this template can be added to as you become aware of threats you hadn't considered before to create a library of potential threat information.

The STRIDE elements don't necessarily affect all DFD elements, you can't control tampering on an external entity and elevation of privilege is only applicable to processes. The table below shows how STRIDE normally applies to DFD elements (repudiation may only apply to a data store if it contains logs but many cloud data stores provide repudiation controls):

	External Entity	Process	Data Store	Data Flow
Spoofing	✓	✓		
Tampering		✓	✓	✓
Repudiation	✓	✓	✓ (?)	
Information Disclosure		✓	✓	✓
Denial of Service		✓	✓	✓
Elevation of Privilege		✓		

You can create a table to help you record the identified threats, shading any cells that are not applicable for that element. Here is a sample of identified threats for TB03:

Threat Type	Azure Data Factory	TB04	Product Database
Spoofing	Stolen credentials may be used to access Data Factory and connected data sources.		
Tampering	Configuration may be tampered introducing vulnerabilities.		Insufficient controls may allow database information to be changed.
Repudiation	Lack of logging may hinder incident response.		
Information Disclosure	Incorrect configuration may lead to sensitive data being added to index.		Lack of encryption may lead to information disclosure.
Denial of Service	Code may be lost if there are no backups.		Data may be lost if there are no backups.
Elevation of Privilege	Failure to implement suitable role-based access controls may lead to unauthorized users accessing privileged functionality.		

The following scores can be used to prioritise issues found at trust boundaries, you can adjust the categories and scores to suit (add the scores together if more than one option applies to a trust boundary):

Cloud environment	+2
Compliance or regulatory requirements	+2
Exposed to a non-trusted area	+3
High availability requirements	+1
High source of hostility	+2
Operates on mobile equipment	+1
Component will stay as it is	-2
Transactional system	+2
Web	+1
Operates in a trusted environment	-1

## **Mitigating Threats**

The table below shows some of the mitigations that can be used to counteract the various categories of threat in STRIDE.

Threat Type	Mitigations
Spoofing	<ol style="list-style-type: none"> <li>1. Authentication</li> <li>2. Protecting secrets</li> <li>3. Not storing secrets</li> </ol>
Tampering	<ol style="list-style-type: none"> <li>1. Authorisation</li> <li>2. Hash verification</li> <li>3. MACs</li> <li>4. Digital signatures</li> <li>5. Tamper resistant protocols</li> </ol>
Repudiation	<ol style="list-style-type: none"> <li>1. Digital signatures</li> <li>2. Timestamps</li> <li>3. Audit trails</li> </ol>
Information Disclosure	<ol style="list-style-type: none"> <li>1. Authorisation</li> <li>2. Privacy-enhanced protocols</li> <li>3. Encryption</li> <li>4. Protecting secrets</li> <li>5. Not storing secrets</li> </ol>
Denial of Service	<ol style="list-style-type: none"> <li>1. Authentication</li> <li>2. Authorisation</li> <li>3. Filtering</li> <li>4. Throttling</li> <li>5. Quality of Service</li> </ol>
Elevation of Privilege	<ol style="list-style-type: none"> <li>1. Principle of least privilege</li> </ol>

As you can see from the above, there is some overlap between Spoofing and Information Disclosure, similar overlaps can be found when considering threats such as malware or network boundary weaknesses. Do not get too hung up on where a threat belongs, just make sure it's identified and mitigated.

## **Creating Threat Modelling Tool Templates**

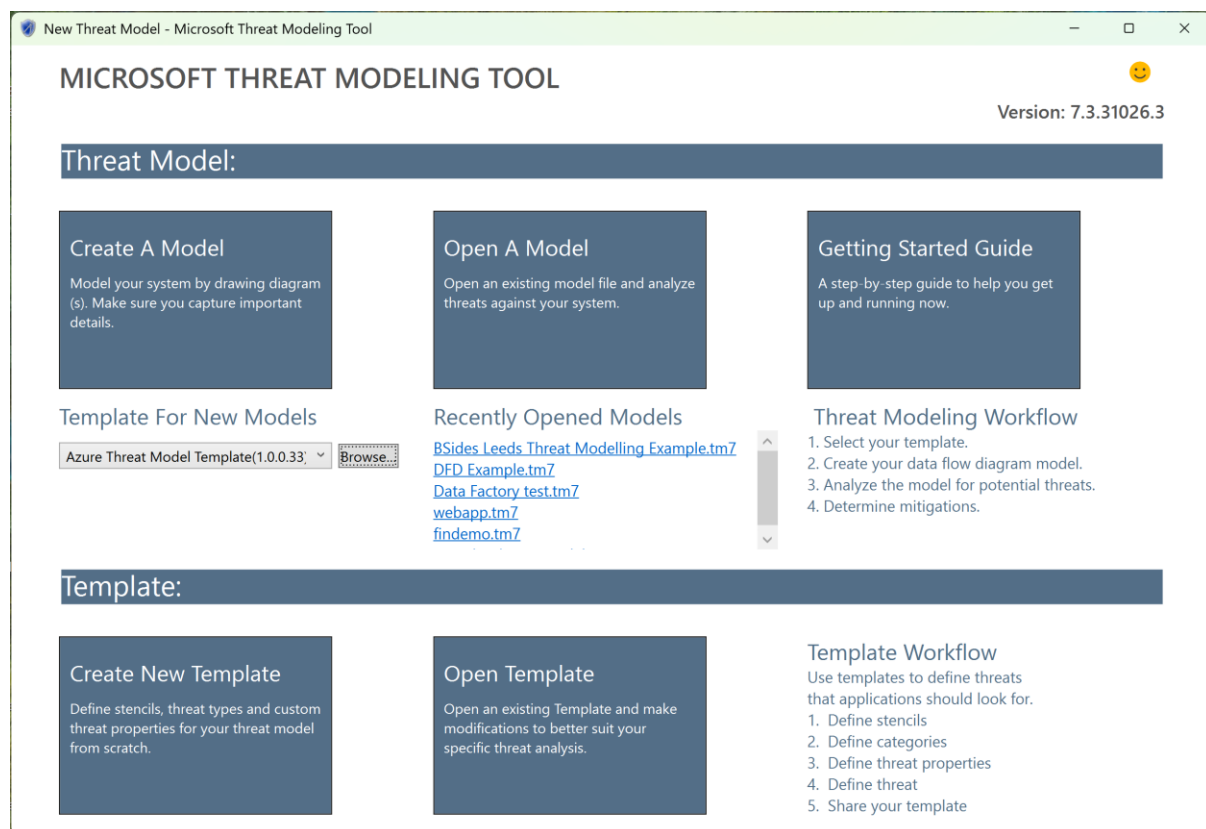
Download and install Microsoft's Threat Modelling Tool from <https://aka.ms/tmt> . When you have installed it you will need to add a shortcut to your desktop to help you locate it in future. Click on the Windows Start menu and type 'Threat modeling' to search for the app. When the Microsoft Threat Modeling Tool option appears in the menu, right-click it and choose 'Open File Location'. Now right-click the application file and send it to your desktop to create a shortcut.

A few basic templates are provided with Microsoft's Threat Modelling Tool when you download and install it:

- SDL TM Knowledge Base (Core)
- Azure Threat Model Template
- Medical Device Model

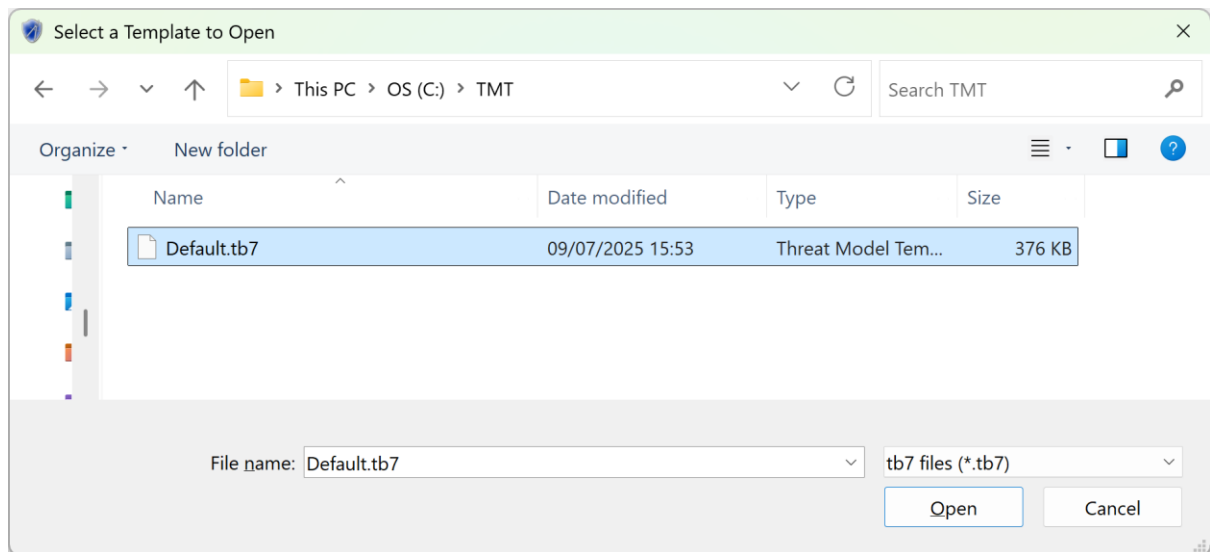
These templates are stored in your user profile when you install TMT, you may want to copy them to another location as TMT tends to overwrite existing templates when it updates.

To copy templates, click the Browse button in the opening menu and then use Windows Explorer to copy templates to a new folder.

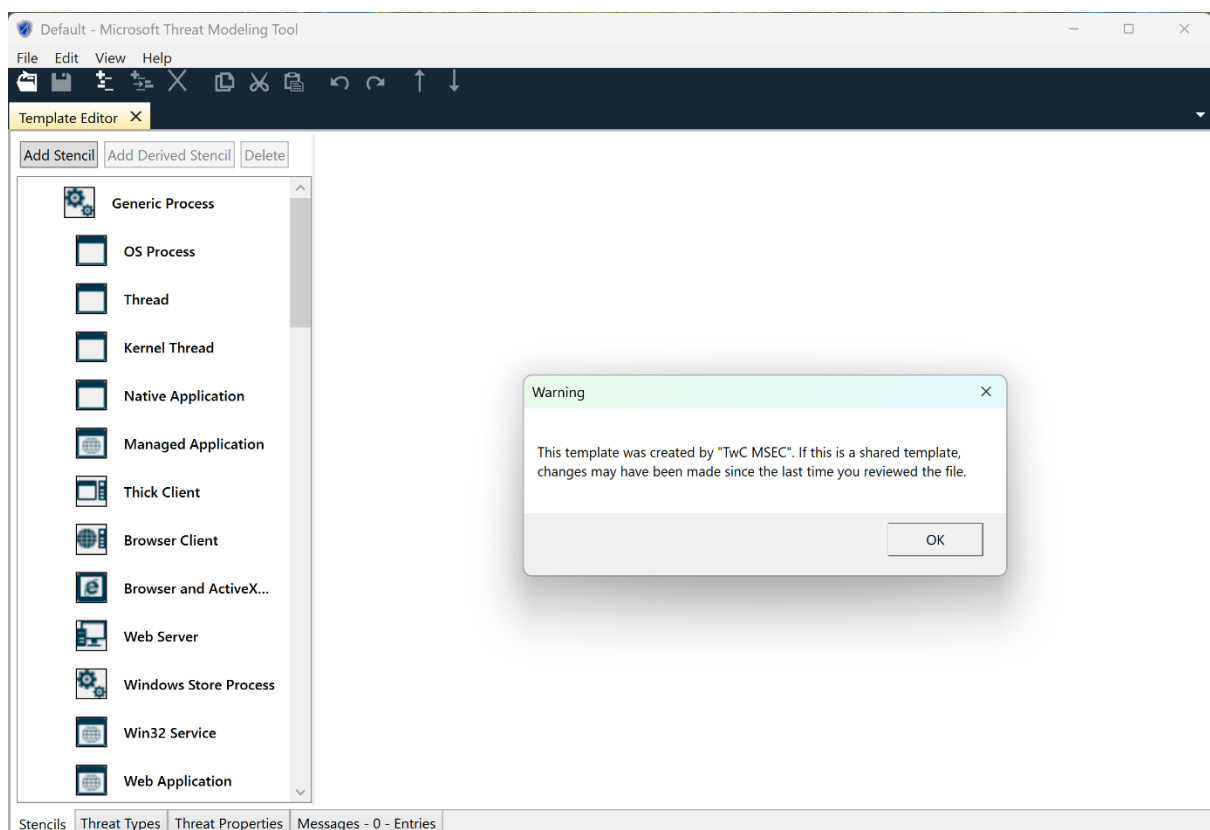


I have copied the default.tb7 file (which is the SDL TM Knowledge Base (Core) template) to C:\TMT and will now open this to use it as the basis for a new template.

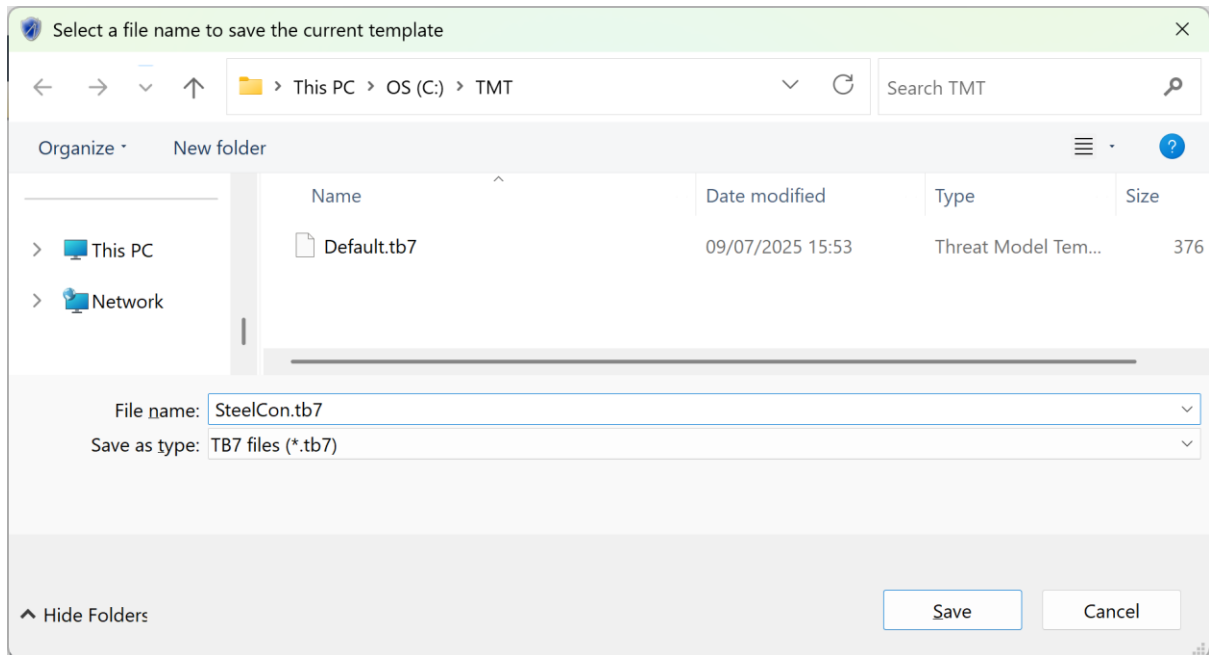
Click the Open Template tile on the main menu and navigate to the location where your template is stored.



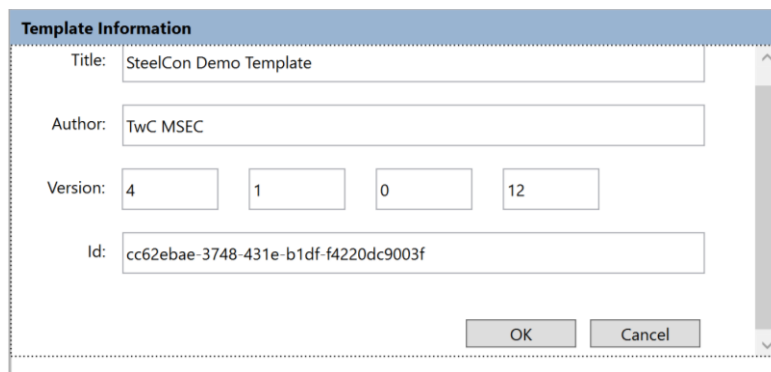
Open the template and click the OK button to dismiss the message.



Now click on File → Save As and save the template with a new name in the same folder, I am calling our template ‘SteelCon’.



If you now click on File → Template Information you can customise the template’s name.



Unfortunately, if you leave the template as it is, the version number will not function correctly and your template is likely to crash. To correct this, save your new template and open it in a text editor.

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <KnowledgeBase xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
3   <Manifest name="SteelCon Demo Template" id="cc62ebae-3748-431e-b1df-f4220dc9003f" version="System.String[]" author="TwC MSEC" />
4   <ThreatMetaData>
5     <IsPriorityUsed>true</IsPriorityUsed>
6     <IsStatusUsed>true</IsStatusUsed>
7     <PropertiesMetaData>
```

Change the “System.String[]” value to “1.0.0.0” to start a new version and then save the file.

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <KnowledgeBase xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
3   <Manifest name="SteelCon Demo Template" id="cc62ebae-3748-431e-b1df-f4220dc9003f" version="1.0.0.0" author="TwC MSEC" />
4   <ThreatMetaData>
5     <IsPriorityUsed>true</IsPriorityUsed>
6     <IsStatusUsed>true</IsStatusUsed>
7     <PropertiesMetaData>
```

You could, of course, create brand new template but there would be a lot more work to do setting up stencils and threats.

## Creating Stencils

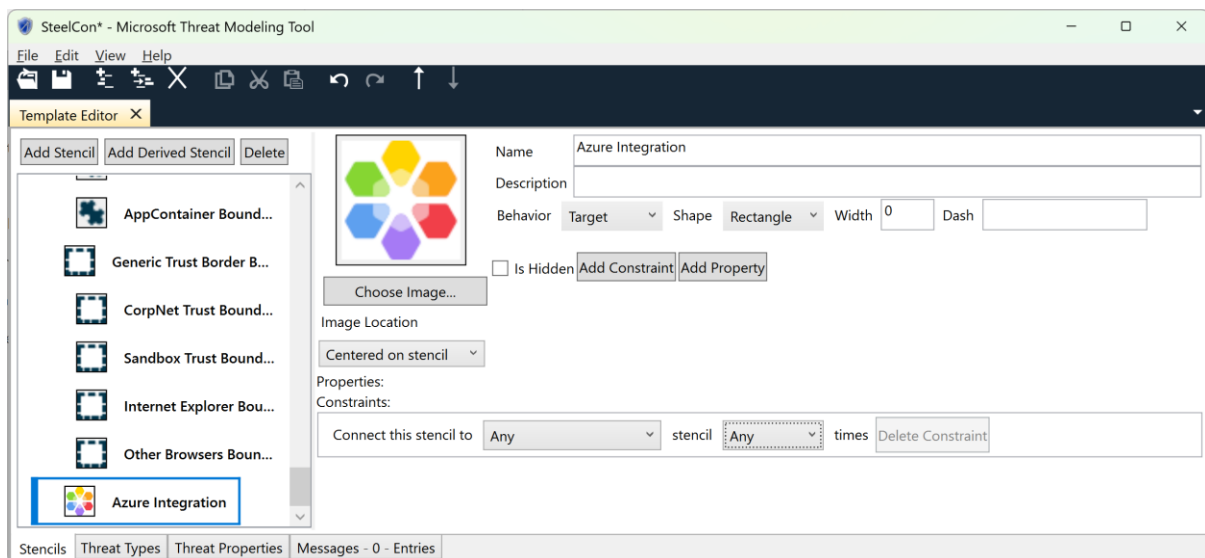
In order to create a threat, the relevant resource stencil(s) must exist. It is best to organise stencils in groups according to type, e.g. put all Azure storage templates together. You can download Microsoft's Azure icons from

<https://learn.microsoft.com/en-us/azure/architecture/icons/>

but note that these are in .svg format and will need to be converted to .png for use with TMT. I use GIMP and resize the image to 72x72 pixels when importing, adding a white background before exporting to .png. AWS icons can be downloaded at <https://learn.microsoft.com/en-us/azure/architecture/icons/>.

The Azure Data Factory icon is found in the Integration category so we will create an Azure Integration stencil group by clicking the Add Stencil button.

Enter a name for the stencil group and then click the 'Choose Image' button to select a suitable icon. For most stencils you should set the 'Behaviour' box to 'Target' and the 'Shape' drop-down to 'Rectangle'. Also don't forget to set the Image Location to 'Centered on stencil' or you will get an error. Don't worry about setting any constraints, this is something you could consider using later to further control creation of diagrams from the stencils if you wish.



Now we have our stencil group we can add Azure Data Factory as a derived stencil. Click on the 'Azure Integration' stencil to select it and then click the 'Add Derived Stencil' button.

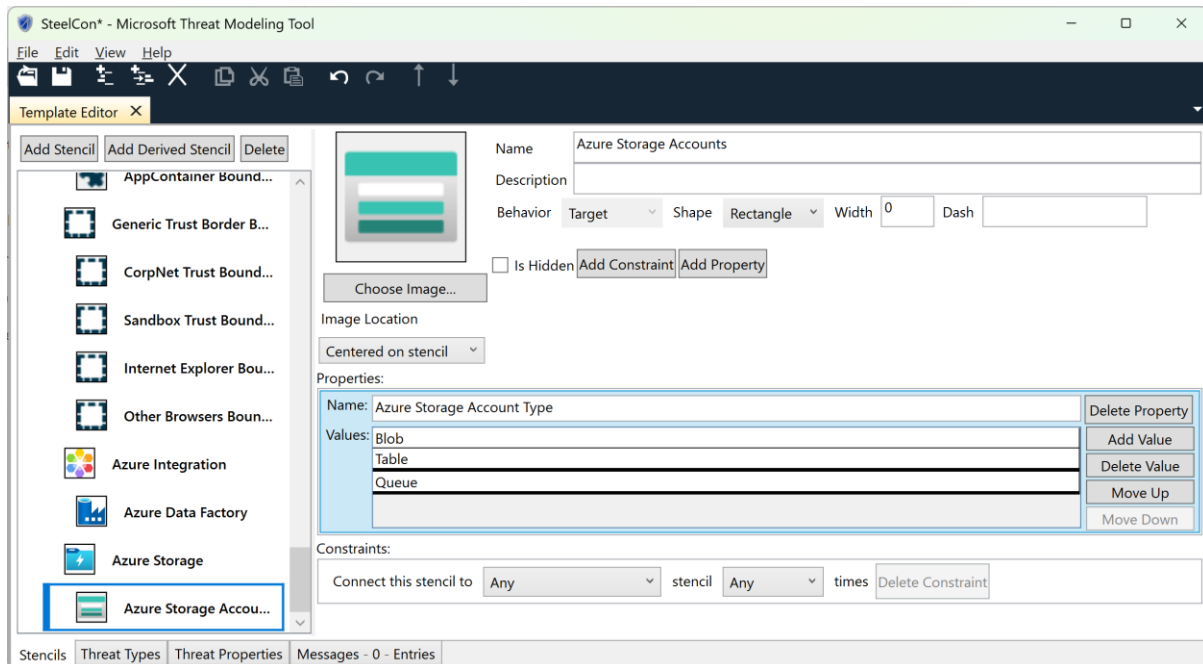
Set up the new stencil in the same way as above, note that you can't change the 'Behavior' drop-down for a derived stencil, it will always inherit the parent stencil's setting. This means you will need to use separate stencil groups for network boundaries and network infrastructure.

The 'Is Hidden' box can be used to hide stencils from users until you are ready for them to be used.

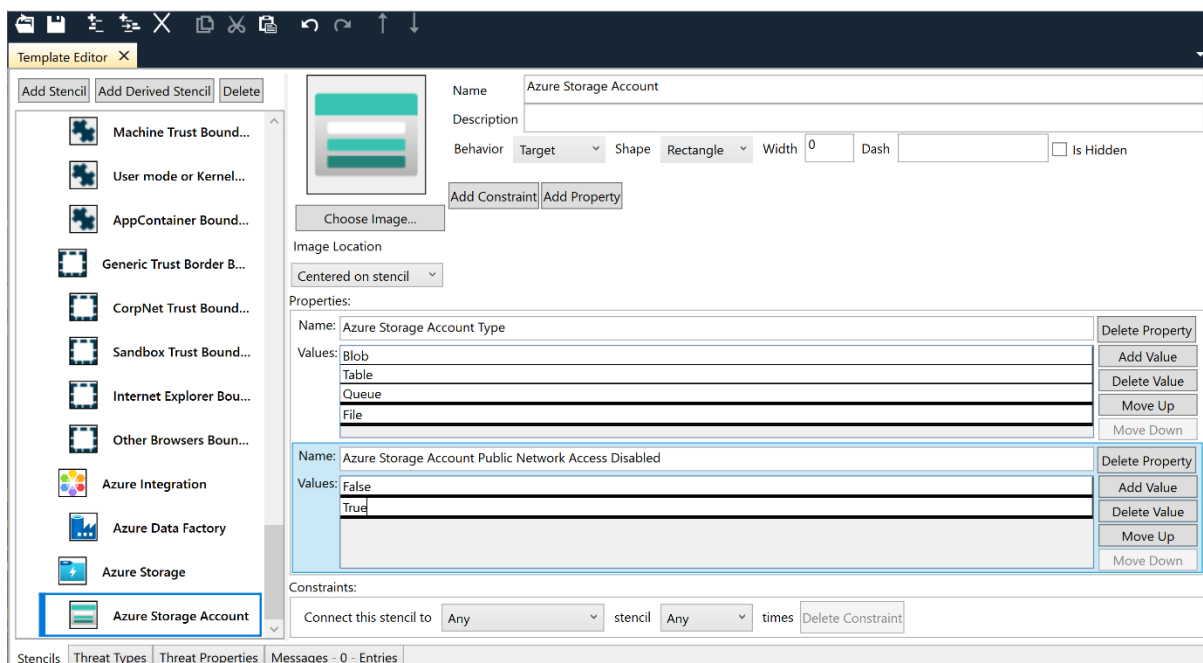
I have also created an Azure Storage stencil group and started to create an Azure Storage Accounts stencil within it. Since Azure Storage can have many forms (blob, table, queue, file) we are going to add some properties to allow users to select the storage type.



Click the 'Add Property' button to set the storage type, it is advisable to always start your property name with the name of the stencil to make it easier to reference when creating threats. TMT is also very particular about duplicate names. Click the 'Add Value' button to add new rows for the property attributes.



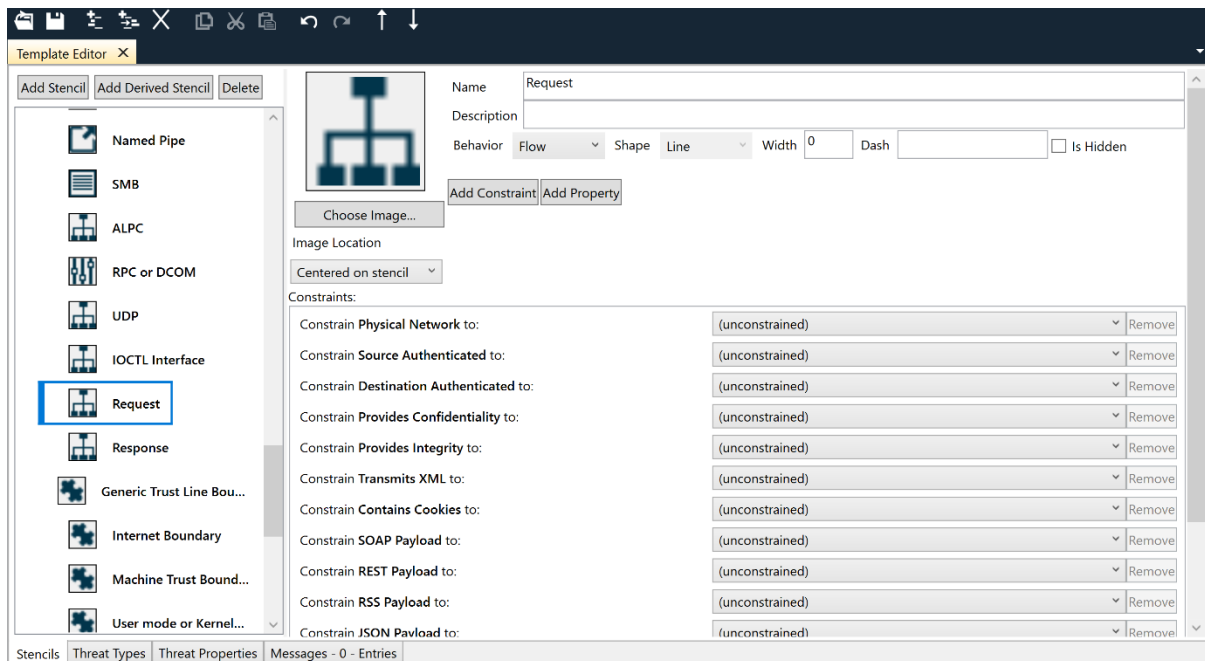
You can also use the Add Property to allow users to select what type of controls are already in place. Here we have added properties so the user can select whether public network access is disabled (the default is enabled).



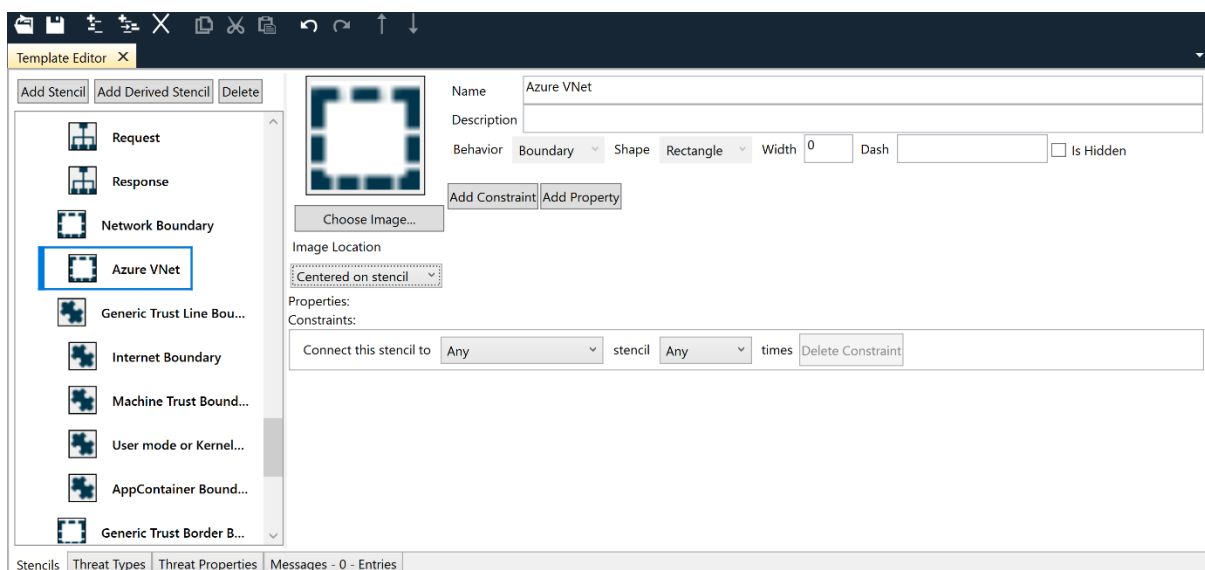
We will now add some data flow icons to the Generic Data Flow stencil group to cover request and response actions. You can use any icon for these, but the 'Shape' drop-down needs to be set to 'Line' (therefore it must be a member of a stencil group that uses lines). There is a set of provided icons in the folder called 'Images' under the folder with a name starting tmt7..tion\_ in

your user profile (look under AppData → Local → Apps → 2.0 etc. I would use the ImageDataFlow7.png image for data flows and ImageGenericTrustBoundaryArc7.png for line trust boundaries.

Our Generic Data Flow group stencil has a number of properties set. When creating the derived 'Request' stencil we can select whether any of these properties should be restrained to specific values (e.g. if you look at the HTTPS data flow stencil in this group you will see that 'Destination Authenticated', 'Provides Confidentiality' and 'Provides Integrity' are all constrained to 'Yes' so the user won't be able to change these values.



Finally, we will create a boundary icon to represent an Azure virtual network. We will create a new stencil group for this using the ImageGenericTrustBoundaryBorder7.png image from our profile.

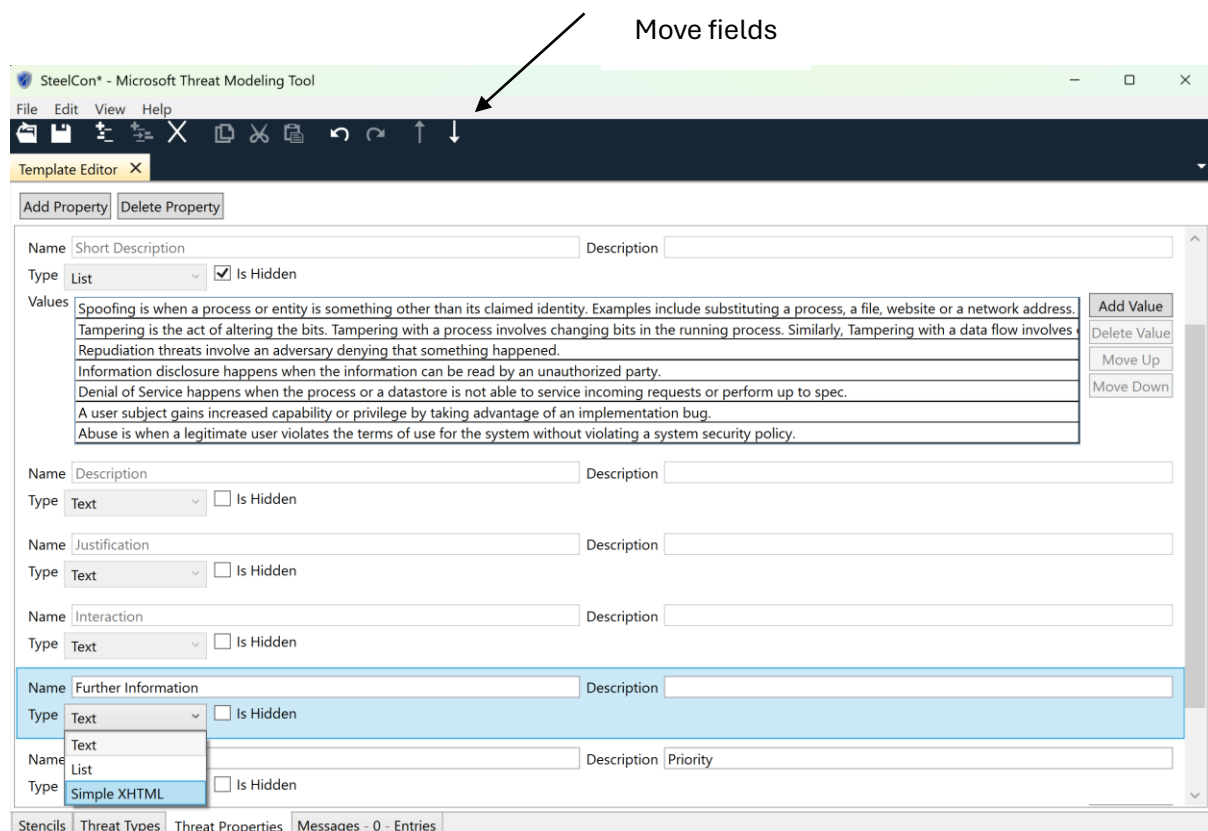


A similar stencil can be created to represent your on-prem corporate network for a hybrid scenario.

## Modifying the Threats Form

We are now going to customise our threats template to add some more fields. As your template grows in size you may wish to add a unique reference for each threat so you can keep a master record of threats you have added (e.g. in a spreadsheet). Since the 'memo' fields are restricted in size I find it helpful to create one to provide further information about the threat and another where I list helpful references.

Click on the 'Threat Properties' tab at the bottom of the window to customise the template and then click the 'Add Property' button to add a new field. Enter a name for the field (we have called the new field 'Further Information' and set the field type. Simple XHTML allows you to create a longer text field and add basic HTML formatting to create paragraphs in the field – without this all your text will run together.



It is a good idea to create a separate 'References' field to hold links to useful information otherwise you are likely to run out of space in a single XHTML field. You can use a basic Text field if you want to add your own threat references. The arrows at the top of the window can be used to move the selected field up or down the template.

These custom fields could also be used to add information such as the name of the relevant resource, links to corporate policies, information security framework references (e.g. NIST, ISO 27001), etc.

If you change to the 'Threat Types' tab and add a new threat then it will include all the new fields. Existing threats won't have the new fields added until you close and re-open the template (but of course these fields will be empty).

## **Creating Threats**

You need to give each threat a unique title, so it can be good to include the relevant resource name in the title to prevent creation of duplicates. You can also use the field code {target.name} in your threat template to automatically include the stencil's name.

To ensure a threat is only listed when it is applicable you need to create suitable threat generation expressions in the 'Include' field, you can also add optional 'Exclude' expressions to ignore items. These conditions can look at whether a resource is the source of the interaction, the target, or whether a flow crosses a trust boundary. If you look at the 'Threat Types' tab in our template you will see that they are organised by STRIDE category. The top threat in each category has an 'Include' value of 'source is [ROOT]'. ROOT is the parent stencil for all the stencils in the template, this threat has been created as a placeholder to provide information about each STRIDE category.

As well as creating specific threats for when an interaction crosses a trust boundary, it can also be useful to include threats simply based on the target to provide best practice configuration information. You can indicate that threats aren't applicable at a later stage if necessary.

Examples of Threat Generation Expression syntax:

Condition	Expression
Data flows terminates at Azure Storage	target is [Azure Storage Account]
Data flows from Azure Storage	source is [Azure Storage Account]
Data flows to Azure Storage which has type 'Blob' and does not have 'Azure Storage Account Public Network Access Disabled' set to 'True'	Target is [Azure Storage Account] and target.[Azure Storage Account Type] is 'Blob' and not target.[Azure Storage Account Public Network Access Disabled] is 'True'
Data flows to Azure Data Factory and crosses a trust boundary	Target is [Azure Data Factory] and flow crosses [Generic Trust Line Boundary]

Here is an example of a completed Spoofing threat for Azure Data Factory. Notice that our HTML characters <p> and </p> have been sanitised to &lt;p&gt; and &lt;/p&gt; - this is an irritation with TMT and we will deal with it later.

The screenshot shows the 'Template Editor' window with a sidebar on the left containing a list of threat types under the 'Spoofing' category. The main area is divided into several sections for defining the threat model.

**Threat Title:** Azure Data Factory access may be spoofed using stolen credentials

**Threat Generation Expressions:**

Generation expressions determine when an instance of a threat type gets created for a threat model. An example of generation expression is: flow.[Authenticates Destination] is 'Yes'.

**Include:** target is [Azure Data Factory] and flow crosses [Generic Trust Line Boundary]

**Exclude:**

**Threat Property Presets:** (Enter text that will be included in each instance of the threat that is created in a diagram. You can use macros to refer to elements of the diagram. Threats are always created on flow stencils. Macros can refer to any stencil property of the flow or the source or target of the flow. Use curly braces to insert a macro, for example "Look for issues with the (flow.name) flow". You can also use macros in the threat title.)

<b>Description</b>	Azure Data Factory access may be spoofed using stolen credentials
<b>Justification</b>	Security Requirement
<b>Further Information</b>	<p>Simplest XHTML that has a length less than 4000, only supports &lt;a/&gt; &lt;p/&gt;. Scripts are not allowed and will be sanitized. Hyperlinks can only start with http:// or https://</p> <p>Value are sanitized.</p>
<b>References</b>	<p>Simplest XHTML that has a length less than 4000, only supports &lt;a/&gt; &lt;p/&gt;. Scripts are not allowed and will be sanitized. Hyperlinks can only start with http:// or https://</p> <p>Value are sanitized.</p>
<b>Priority</b>	High

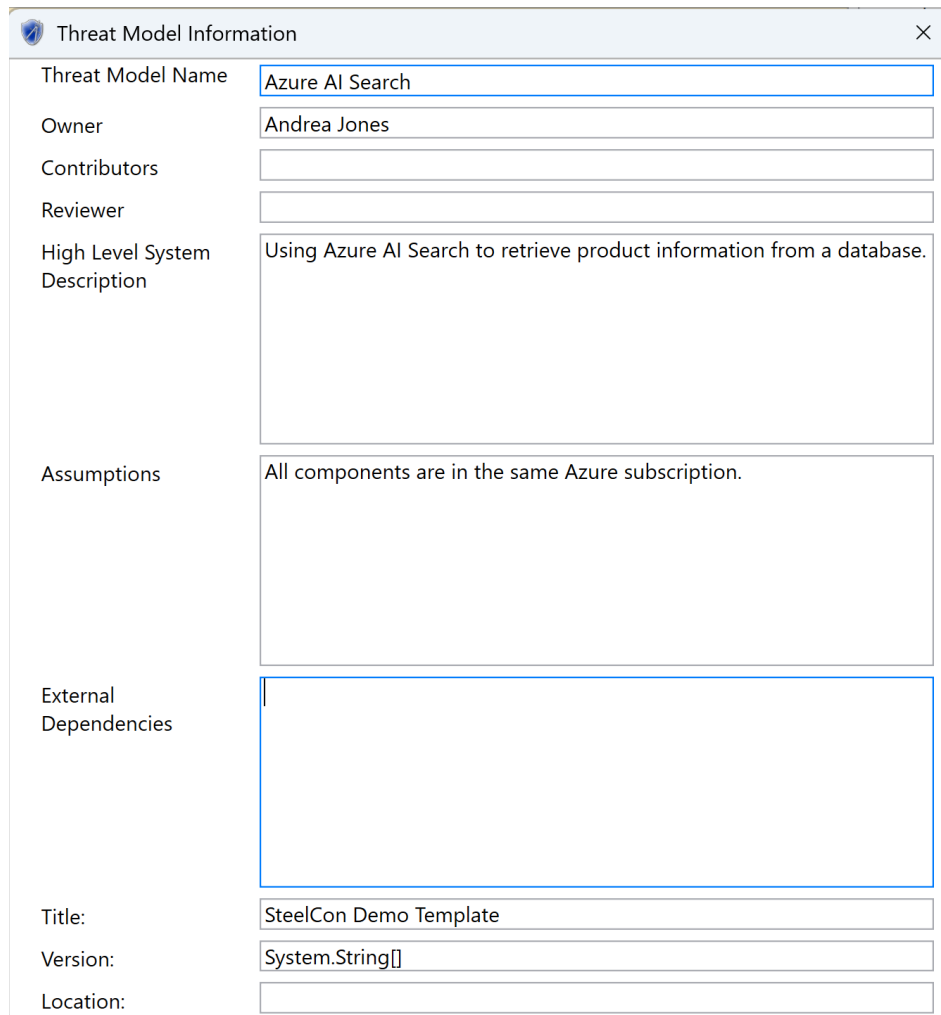
The bottom of the window shows tabs for 'Stencils', 'Threat Types', 'Threat Properties', and 'Messages - 0 - Entries'.

You can find Azure best practice information in the version 3.0 security benchmarks files at <https://github.com/MicrosoftDocs/SecurityBenchmarks/> and the AWS Foundational Security Best Practices information can be found at <https://docs.aws.amazon.com/securityhub/latest/userguide/fsbp-standard.html>.

## Creating a Model

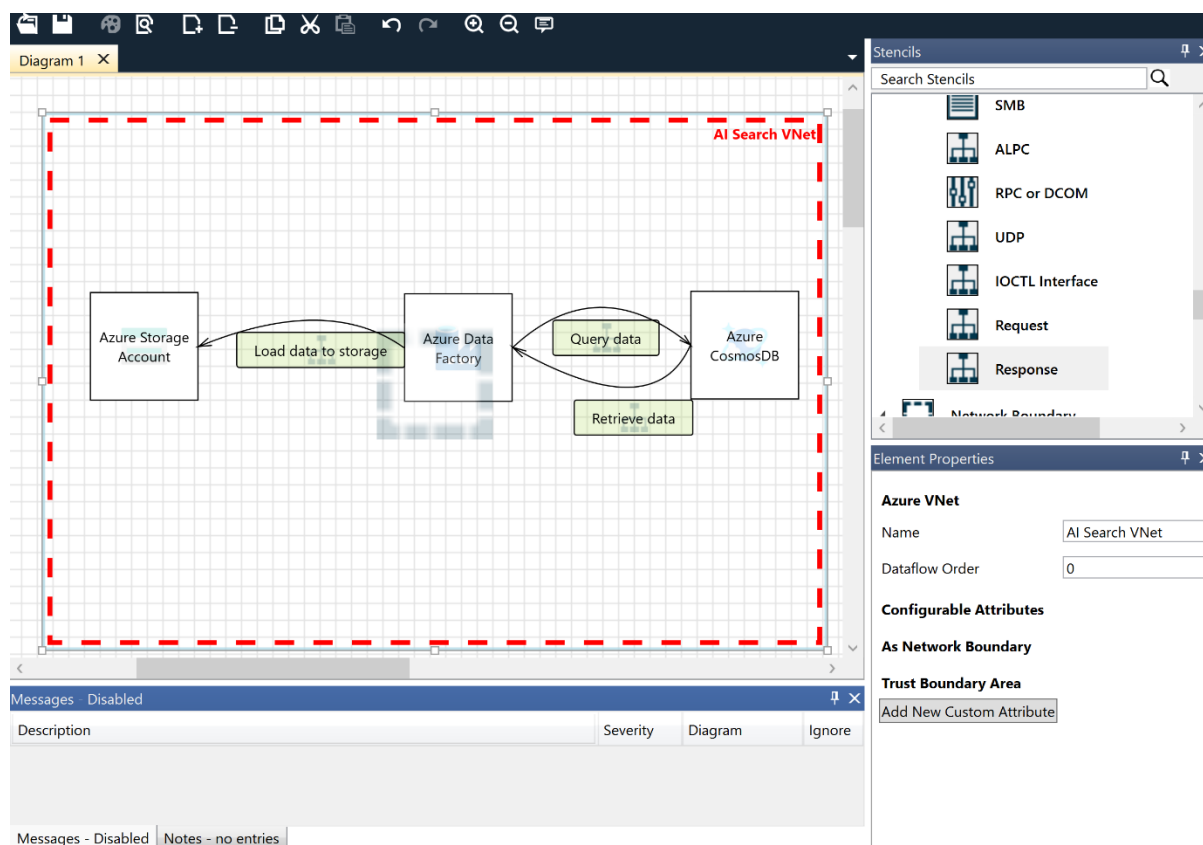
When you have finished editing your template, ensure there are no errors indicated in the 'Messages' tab at the bottom of the window and save your template. To use this for a model, click the 'Browse' button in the 'Template For New Models' drop-down box in the main menu and find the template you have created. Now click the 'Create a Model' tile and you will see the template's stencils on the right-hand side of your screen.

To set information about your model, click on File → Threat Model Information and enter the relevant information in the boxes provided. This information will be printed on your exported model later.

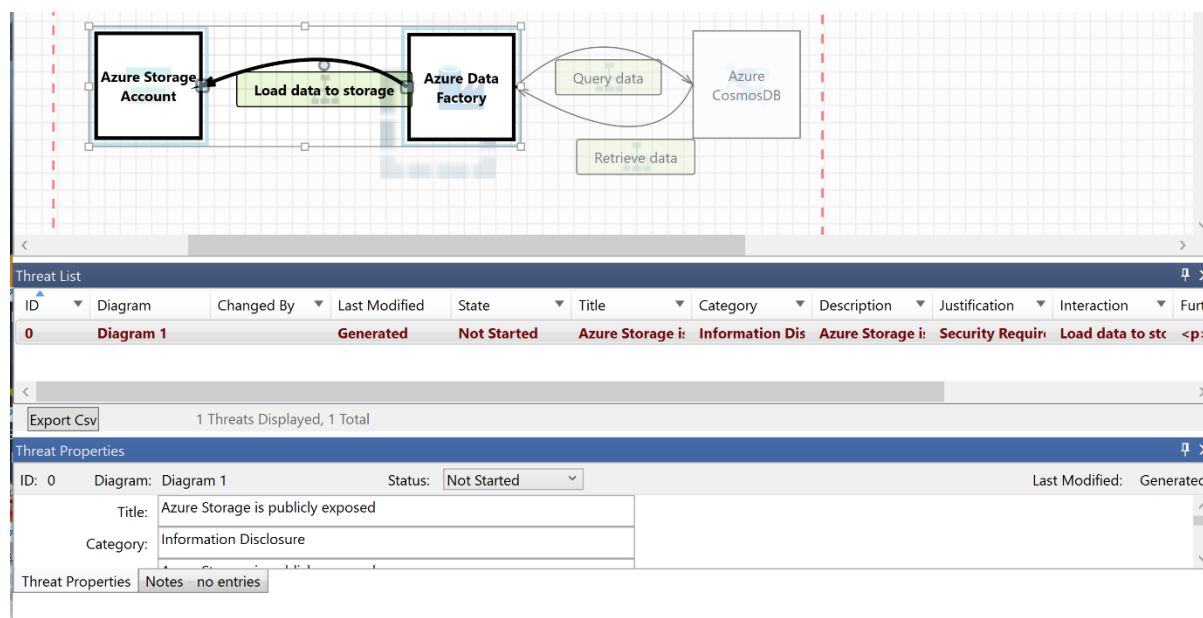


Threat Model Information	
Threat Model Name	Azure AI Search
Owner	Andrea Jones
Contributors	
Reviewer	
High Level System Description	Using Azure AI Search to retrieve product information from a database.
Assumptions	All components are in the same Azure subscription.
External Dependencies	
Title:	SteelCon Demo Template
Version:	System.String[]
Location:	

You can now draw a diagram to represent your infrastructure, when creating diagrams you can click on the 'Diagram x' tab at the top of the screen to change the name of the diagram and you can click on Diagram → Add New Diagram to add extra diagrams, this can be very useful for large infrastructures.



While you create a diagram you are in 'Design View'. If you click on the 'View' menu you can change to 'Analysis View' where you will see a table containing any threats that have been identified. If you click a threat to select it you can then change the 'Status' box to change information such as whether the threat is not applicable or whether it has been mitigated.



## Bi-directional data flows

If you have a situation where either side can initiate a data flow then you can create a bi-directional connection by holding down your Shift key while selecting the two resources that

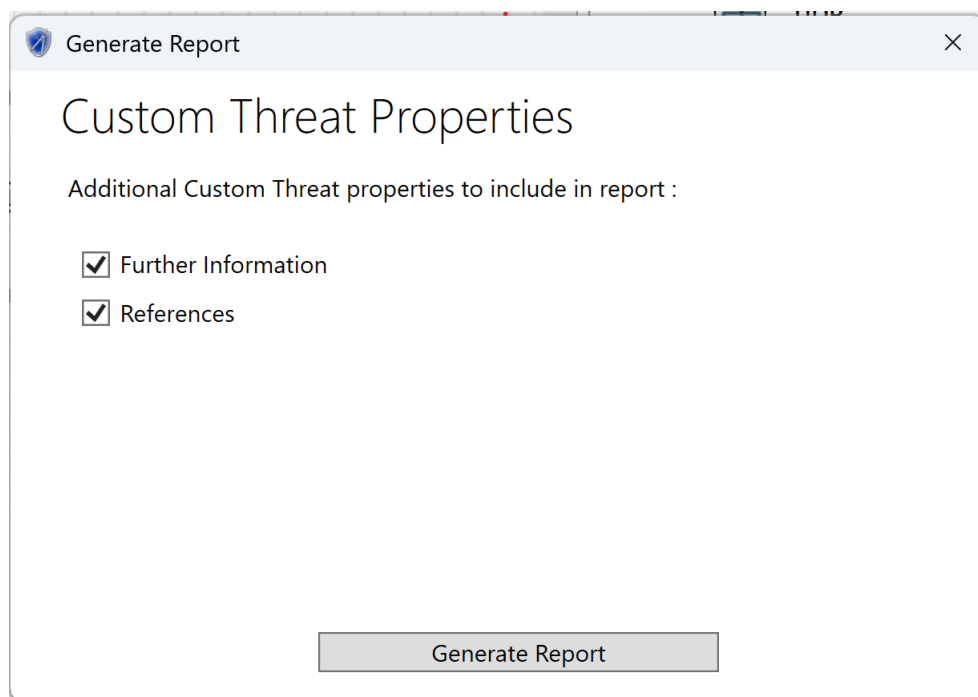
need to be connected. When they are both connected, let go of Shift, right-click one of the resources and select 'Bi-Directional Connect'

## Recalculating Threats

If you update a template and then re-open a model which uses that template you can update all the threats. Sometimes this may put the threat ID numbering out of sync so you end up not starting at 0. To rectify this you can click on Settings → Disable Threat Generation followed by Settings → Enable Threat Generation to reset the identified threats.

## Creating a Report

When you are happy that the analysis view shows the relevant threats you can create a report. Click on Reports → Create Full Report and you will see a window where you can select whether to include the extra template fields we have created.

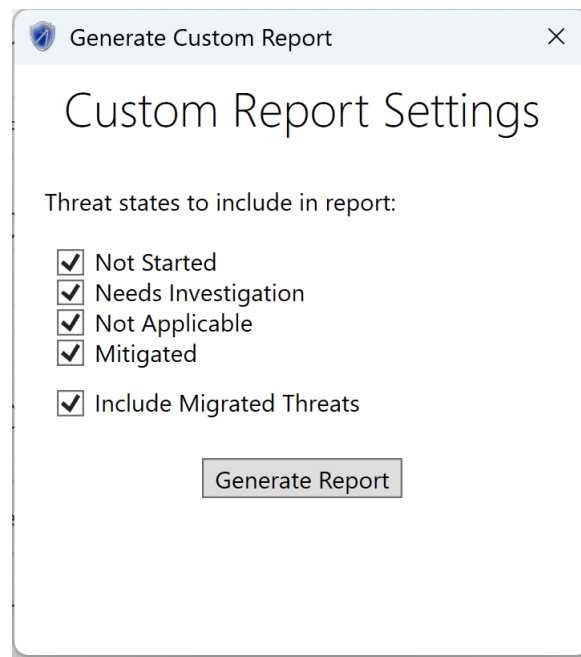


Click the Generate Report button and save the report as an .htm file, it should now open in your browser.

You will notice that any HTML tags you have entered in your threat template will have been sanitised. To resolve this, open the .htm file in a text editor and use find and replace to first replace any instances of **&amp;** with **&** until no more remain and then replace **&lt;** with **<** and replace **&gt;** with **>**. Save the file and you should now find it is formatted correctly (you may also need to replace other special characters such as apostrophes and quotation marks if you have used them).

You can now use your threat model to track progress on mitigations and can refresh the threats if the base template changes. If you use the 'Generate Custom Report' option on the Reports menu you can select which threat states to include.





Generate Custom Report

## Custom Report Settings

Threat states to include in report:

- ☒ Not Started
- ☒ Needs Investigation
- ☒ Not Applicable
- ☒ Mitigated
- ☒ Include Migrated Threats

Generate Report