

|  |  |
| --- | --- |
| Microsoft Threat Modeling Tool 2016  User Guide | |
| Microsoft Trustworthy Computing |  |

Contents

[Document History 3](#_Toc431823969)

[Overview 4](#_Toc431823970)

[Threat Modeling with STRIDE 4](#_Toc431823971)

[Standard Threat Mitigations 7](#_Toc431823972)

[Purpose of Tool 8](#_Toc431823973)

[Supported Scenarios 8](#_Toc431823974)

[Creating a New Threat Model 8](#_Toc431823975)

[Modifying an Existing Threat Model 8](#_Toc431823976)

[Upgrading a Threat Model to use a new Template 8](#_Toc431823977)

[Analyzing the Threat Modeling Tool Output - Reports 8](#_Toc431823978)

[Adding or Extending the Threat Knowledge Base 9](#_Toc431823979)

[Installation 9](#_Toc431823980)

[How to Run Threat Modeling Tool 9](#_Toc431823981)

[Analysis of Threat Modeling Tool Output 9](#_Toc431823982)

[How to File Bugs on your Threat Modeling Tool Security Issues 9](#_Toc431823983)

[Features 10](#_Toc431823984)

[The Initial Screen 10](#_Toc431823985)

[Threat Model Section 10](#_Toc431823986)

[Design View 11](#_Toc431823987)

[Automation 28](#_Toc431823988)

[Appendices 29](#_Toc431823989)

[Appendix I — Extending the Threat Template 29](#_Toc431823990)

[Appendix II — Drawing Surface Keyboard Navigation and General Keyboard Shortcuts 58](#_Toc431823991)

# Document History

Document Status: **Approved**

# Overview

Microsoft Threat Modeling Tool 2016 is an easy-to-use tool that can:

* Create data flow diagrams (DFDs) for products or services
* Analyze data flow diagrams to automatically generate a set of potential threats
* Suggest potential mitigations to design vulnerabilities
* Produce reports on the identified and mitigated threats
* Create custom templates for threat modeling

A threat model is (1) a representation of the software or device components in a system, (2) the data flows between them and (3) the trust boundaries in the system. When threat-modeling, potential design vulnerabilities can be discovered by analyzing the system’s security properties and identifying potential threats to the information assets in the system.

Unlike pure verification techniques, such as penetration testing or fuzzing, threat-modeling can be performed before a product or service has been implemented; this helps ensure that a product or service is as much as possible secure by design.

Software-centric threat-modeling can be summarized as:

* Diagram
* Draw the system architecture
* Add details and draw the trust boundaries
* Identify Threats
* Find threats using a methodology, such as STRIDE per interaction
* Address Threats
* Redesign the component to use a standard mitigation
* When necessary, create a custom mitigation
* Validate
* Validate that the threat-model diagram matches what is implemented
* Validate that each potential threat has a mitigation

The SDL threat-modeling approach starts with a data flow diagram. From the diagram, potential threats are identified. For each threat, mitigations are proposed. In some cases, the mitigation takes the form of changing the design itself, in which case the new or changed elements must be analyzed in an additional iteration.

When the mitigations have been implemented, the product or service is validated against the threat model to ensure that the mitigations work and that design functionality and performance are sufficient. If the design has serious security issues, revisiting the design and the threat model may be appropriate.

## Threat Modeling with STRIDE

The Microsoft Threat Modeling Tool applies a particular threat-modeling approach called *STRIDE per Interaction.* STRIDE is an acronym for the threat types of **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of privilege. STRIDE is a way to find a wide variety of threats using these easy-to-remember threat types. Not all threats fit easily into a STRIDE category and some threats may fit into more than one category. More important than fitting a threat to a category is using the model to help you describe the threat and design an effective mitigation. With its matching of threats to mitigating features, STRIDE is also convenient way of moving the focus from threat to mitigation. Each threat is matched to the feature or property that should be present in the software to mitigate the threat, shown in Table 1.

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat** | **Property** | **Threat Definition** | **Examples** |
| **Spoofing** | Authentication | Spoofing threats involve an adversary creating and exploiting confusion about who is talking to whom. Spoofing threats apply to the entity being fooled, not the entity being impersonated. Thus, external elements are subject to a spoofing threat when they are confused about what or whom they are talking to. | * Accounts.contoso.com is spoofed when it thinks that a user is giving it authorized credentials. * An adversary may have poisoned the DNS cache so accounts.contoso.com now points at a malicious system that looks exactly like the real accounts.contoso.com. |
| **Tampering** | Integrity | Tampering threats involve an adversary modifying data, usually as it flows across a network, resides in memory, on disk, or in databases. | * An adversary tampers with network packets, and changes commands after the user has logged in. * An adversary tampers with a registry key, making us run any program they choose. * An adversary tampers with a DLL, inserting the code into executable memory. * An adversary installs an unauthorized program on a computer. |
| **Repudiation** | Non-repudiation | Repudiation threats involve an adversary denying that something happened. | * Joe denies that he clicked on that link, for example to deny that he has benefited from a financial transaction. * Amy receives an email from Joe in which he agrees to a contract between the two. Later, Joe denies ever having sent that email. |
| **Information disclosure** | Confidentiality | Exposing information to someone not authorized to see it. | * Examples include passwords for known or unknown users, copies of emails, and names and social security numbers in a database.   As the last example makes clear, some information disclosure issues are also privacy issues. However, not all privacy issues are information disclosure issues. For example, the “Fair Information Practices” at the heart of most privacy and data protection laws usually include items such as notice, meaning that people should be informed that you are collecting certain data, and choice, meaning that users should get options about what data they provide, and how it will be used. For more on privacy issues, see the [Microsoft Privacy and Foundations of Trustworthy Computing.](http://www.microsoft.com/about/twc/en/us/privacy.aspx) |
| **Denial of service** | Availability | Deny or degrade service to users. | * An adversary prevents customers from connecting to a web site. * An adversary prevents the client from getting a DNS response. * An adversary prevents the client from speaking SSL, and forces a downgrade to an insecure connection. * An adversary can cause a program to crash. |
| **Elevation of privilege** | Authorization | Gain capabilities without proper authorization. | * An adversary who starts as an anonymous internet user can send commands to an application that execute as the web server. * An adversary with a web server can make code run as the local user. * An adversary who has the ability to log onto the machine as a standard user can become an administrator. |

Table 1 STRIDE Definitions and Examples

STRIDE per Interaction is an approach that analyzes threats in the context of the interaction between two elements in the model.

## Standard Threat Mitigations

The following chart gives examples of standard mitigations for the threats in STRIDE. Standard mitigations, if practicable, are preferred over custom mitigations:

|  |  |  |
| --- | --- | --- |
| **Threat** | **Property** | **Mitigations** |
| **Spoofing** | Authentication | To authenticate principals:   * Windows authentication (NTLM) * Kerberos authentication * Windows or Live ID authentication * PKI systems such as SSL/TLS and certificates * IPsec * Digitally signed packets   To authenticate code or data:   * Digital signatures * Message authentication codes * Hashes |
| **Tampering** | Integrity | * Windows Discretionary Access Control Lists * Windows Mandatory Integrity Controls * Digital signatures * Message authentication codes |
| **Repudiation** | Non-repudiation | * Strong authentication * Secure logging and auditing * Digital signatures * Time stamps * Trusted third parties |
| **Information disclosure** | Confidentiality | * Encryption * ACLS |
| **Denial of service** | Availability | * Windows Discretionary Access Control Lists * Filtering * Quotas and rate limits * Authorization * High-availability designs |
| **Elevation of privilege** | Authorization | * Windows Discretionary Access Control Lists * Group or role membership * Privilege ownership * Permissions * Input validation |

Table 2 STRIDE Threat Mitigations

# Purpose of Tool

The Microsoft Threat Modeling Tool is intended to assist in analyzing the design of a system for security risks and assist in mitigating the identified threats.

# Supported Scenarios

## Creating a New Threat Model

For details about how to create and analyze a threat model, see the “How to Run Threat Modeling Tool” section of the *TMT Getting Started Guide*.

## Modifying an Existing Threat Model

Modify an existing model either by selecting the model from the **Recently Opened Models** list on the bottom of the initial screen or selecting **Open** from the **File** menu. Proceed with diagraming and analyzing the model as described in the *TMT Getting Started Guide*.

## Upgrading a Threat Model to use a new Template

If you have a template file that you want to use to upgrade your existing threat model, start the Threat Modeling Tool and select **File** **> Apply Template** and select the appropriate Threat Model Template (.tb7) file.

## Analyzing the Threat Modeling Tool Output - Reports

You can create a report from the **Reports** menu, using the **Create Full Report** item. The full report contains the following information:

* The threat model information, including the name, owner, reviewer, contributors, description, assumptions, and external dependencies.
* All DFDs and a report showing a list of threats and their states.
* An entry for each threat showing the precise interaction, the threat information, and the mitigation information.
* List of validation messages/errors, if there are any present for each diagram.
* Table of notes for the threat model if any entered in the **Notes** section.

To consider your threat model completed, you should aim to have all threats either mitigated and verified, or justified as being not applicable. In some cases, a bug entry may be necessary.

## Adding or Extending the Threat Knowledge Base

Some product or service teams may choose to supplement the Template that is part of TMT.

Creating or customizing a Template article is described in “Appendix I — Extending the Threat ”.

# Installation

For information regarding installation and setup of Threat Modeling Tool please see the *TMT Getting Started Guide*.

# How to Run Threat Modeling Tool

For information regarding running Threat Modeling Tool please see the *TMT Getting Started Guide*.

# Analysis of Threat Modeling Tool Output

For information regarding Analyzing Threat Modeling Tool results, please see the *TMT Getting Started Guide*.

# How to File Bugs on your Threat Modeling Tool Security Issues

For information regarding how to file bugs on your Threat Modeling Tool security issues, please see the *TMT Getting Started Guide*.

# Features

For a walkthrough of TMT, see the *Threat Modeling Tool Getting Started Guide*. That document will identify and explain the basic steps of creating a threat model.

## The Initial Screen

Launch **Microsoft Threat Modeling Tool 2016.** The Initial screen will appear. It consist of primarily two sections, **Threat Model** and **Template**.

From the initial screen, choose the **Create a Model** tile to create a new model. Click **Open a Model** to show the open file dialog so you can select a model to open.

**Create New Template** helps in creating template from scratch. Click on **Open Template** to show the open file dialog so you can select an existing template for edit/view.

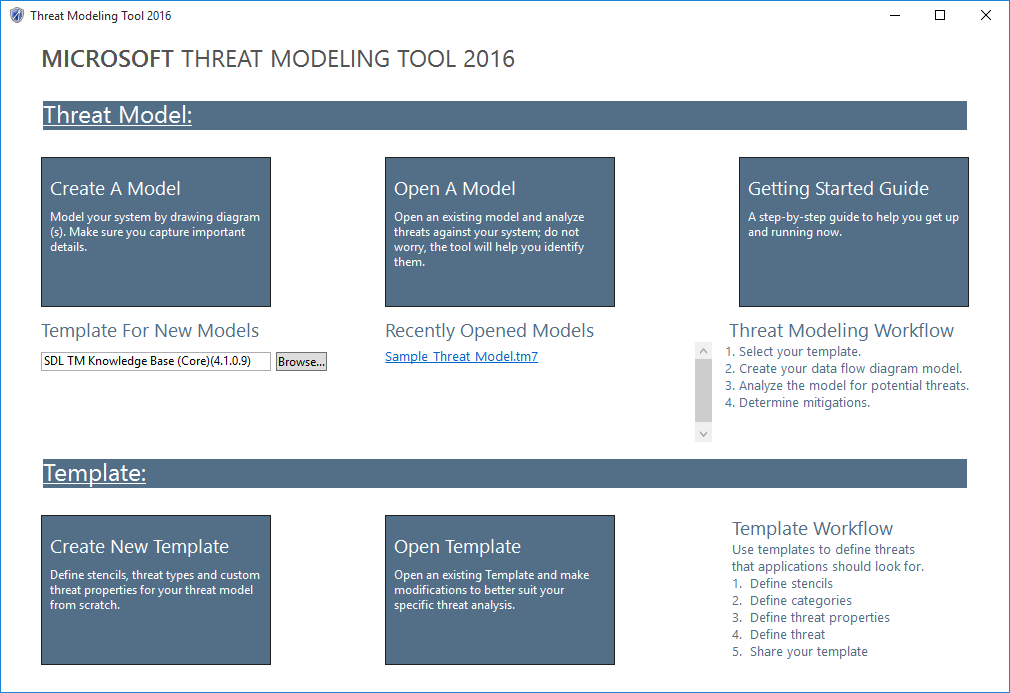


Figure 1 Initial Threat Modeling Tool Screen

## Threat Model Section

Following sections details out the functionalities provided by threat model section.

## Design View

**Design** view allows you to draw your diagram and provides objects and properties to allow you to adequately represent the design of your component.

All diagrams should minimally contain:

* One or more processes.
* The directional data flows between external interactors and processes, and among the processes themselves.
* Important data stores.
* An external interactor (often a user) that communicates with the processes.
* A trust boundary or boundaries

The example below shows a basic diagram:

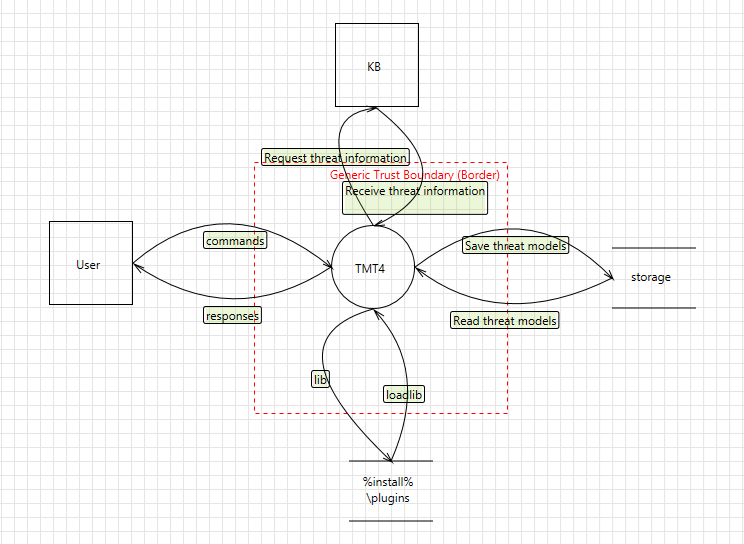


Figure 2 Sample Diagram

To help you create a good diagram, the tool has certain heuristics that are based on a review of many threat models. These heuristics are intended to guide you in drawing the data flow diagram, and when violated, will show warnings or errors in the **Messages** pane.

***Self-check:*** *See if you can tell a story about someone using your product with the diagram. A good diagram will have the key elements you talk about.*

When first instantiated, elements will have names like **Generic Process.** The name should be replaced by a unique, descriptive name that uses a consistent pattern. It is very helpful to use the real technical names where possible. For example, use process names, such as **tmt7.exe**, **AnalysisOutput.xslt**, data store names, such as **HKLM\...\Currentversion\Userdata\** or **HKCU\Software\SDLTm\,** anddata flow names, such as **Read Configuration Data** or **Write Configuration Data**.

Use logical names like **lexical analysis**, **marshal data** when representing functional elements inside a process.

If your design is large or complex, you can represent it using multiple diagrams in the threat model file.

### The Drawing Canvas

The diagram is the basis of all threat information automatically generated by the tool. The recommended process is to begin with a simple diagram and add details to explain the system and show all the trust boundaries. If you use child diagrams, you can extend designs laterally into multiple sheets and expand high level elements into their internal component elements.

### Menu Choices

The **File** menu provides options to create, open, save, or close models:

* **New Model** creates a new model.
* **Open** opens an existing threat model.
* **Save** saves the current model using current name.
* **Save As** saves the current model with option to change name or location.
* **Apply Template** apply selected template to opened threat model
* **Threat Model Information** displays the **Threat** **Model Information** dialog. You should provide the background information and answer the scoping questions.
* **Close Model** closes the current model.
* **Exit** exits the tool.

The **Edit** menu provides options to interact with the clipboard:

* **Undo** undoes the last operation.
* **Redo** redoes the most recent operation.
* **Copy** copies the current selection into clipboard.
* **Paste** pastes the current clipboard contents onto drawing surface.
* **Cut** places the current selection into clipboard and removes from drawing surface.

The **View** menu provides options to view different functional windows within the tool:

* **Design View** switches to **Design** view.
* **Analysis View** switches to **Analysis** view.
* **Zoom In** increases magnification.
* **Zoom Out** decreases magnification.
* **Stencils** show the drawing stencils in **Design** view. (Enabled only if currently hidden).
* **Messages** showthe **Message** window. (Enabled only if currently hidden.)
* **Notes** show the **Notes** window**.** (Enabled only if currently hidden.)
* **Threat List** shows the threat list window in analysis view. (Enabled only if currently hidden.)
* **Threat Properties** shows the Threat Properties window in Analysis view. (Enabled only if currently hidden.)
* **Element Properties** shows the **Properties** window. (Enabled only if currently hidden.)

The **Settings** menu exposes settings for the tool:

* **Enable Threat Generation** enables automatic threat generation. (ON by default.)
* **Disable Threat Generation** disables automatic threat generation. (Improves performance for large models.)

The **Diagram** menu provides options for switching between diagram windows. The menu options are generated dynamically based on your diagram names.

The **Reports** menu provides methods for creating HTML reports for the threat model.

* **Create Full Report** creates a threat model report with information on all threats.
* **Create Custom Report** creates a threat model report for a subset of threats based on state.

The **Help** menu displays options for user assistance.

### Toolbar

|  |  |
| --- | --- |
| **Open** opens explorer file open prompt | **Save** saves current open model file |
| **Design View** switches to **Design** view. | **Paste** pastes the clipboard contents onto surface. |
| **Analysis View** switches to **Analysis** view. | **Cut** cuts the current element from surface. |
| **New Diagram** creates a new blank diagram. | **Undo** undoes the last operation. |
| **Delete Diagram** deletes the current diagram | **Redo** redoes the most recent operation. |
| **Copy** copies the current element to the clipboard. | **Zoom in** increases magnification. |
|  | **Zoom out** decreases magnification. |

### Context (Right–Click) Menu

Right-click on the drawing canvas or an element, to choose from a set of actions will vary depending on the context and whether you are in Design view or Analysis view.

Actions available by right-clicking the drawing canvas:

* **Connect** connects the last two elements from the first to the second element.
* **Bi-directional Connect** creates a two-way connection between last two elements.
* **New Process** adds a new generic process.
* **New External Interactor** adds a new generic external interactor.
* **New Data Store** adds a new generic data store.
* **New Arc Boundary** adds a new generic arc boundary (legacy boundaries).
* **New Border Boundary** adds a new generic border boundary (preferred boundaries).
* **New Data Flow** adds a new generic (unconnected) data flow.
* **Add User-Defined Threat** adds a custom threat unassociated with any interaction.
* **Copy** copies the current selection to the clipboard.
* **Cut** places the current selection into clipboard and removes from drawing surface.
* **Paste** pastes an element onto drawing surface.
* **Add Annotation** adds a free-text annotation on the diagram.
* **Properties** show the properties window.

Actions available by right-clicking an element:

* **Add User-Defined Threat** adds a custom threat.
* **Delete** removes the element.
* **Copy** copies the current selection to the clipboard.
* **Cut** places the current selection into clipboard and removes from drawing surface.
* **Convert To** converts a stencil to a parent stencil type or derived stencil type.
* **Show Related Threats in Threat List** filters threats related to selected element and shows in threat list pane.
* **Properties** show the properties window.

### Elements

The **Stencils** pane displays a large set of icons and drawing tools that help you to intuitively create models that can be evaluated for security vulnerabilities before you begin coding. Using more specific elements allows for more precise threats to be generated.

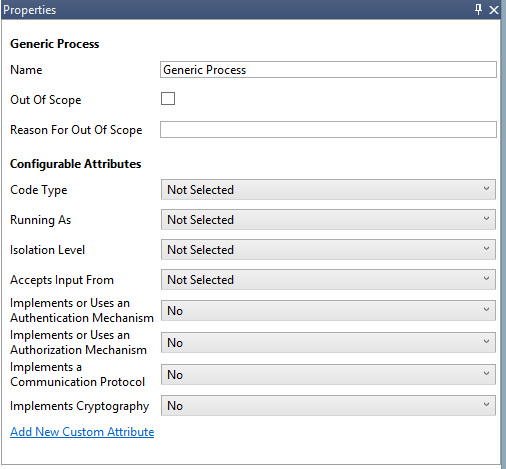
The **Stencils** pane displays tree view of stencils categorized by **Generic Stencils**. The elements available in each tab are listed in the following table.

|  |  |  |
| --- | --- | --- |
| **Element Type** | **Name** | **Description** |
| **Process** | Generic Process | A representation of a generic process. |
| **Process** | Applications Running on a non-Microsoft OS | Microsoft applications running on operating systems from Google or Apple. |
| **Process** | Browser and ActiveX Plug-ins | A representation of a browser plugin. |
| **Process** | Browser Client | A representation of a browser client. |
| **Process** | Kernel Thread | A thread of execution in the Windows kernel. |
| **Process** | Managed Application | A representation of a .NET application. |
| **Process** | Native Application | A representation of a Win32 or Win64 application. |
| **Process** | OS Process | A Windows process. |
| **Process** | Thick Client | A representation of a thick client. |
| **Process** | Thread | A thread of execution in a Windows process. |
| **Process** | Virtual Machine | A virtual machine running in a Hyper-V partition. |
| **Process** | Web Application | Delivers web content to a human user. |
| **Process** | Web Server | A representation of a Web Server Process. |
| **Process** | Web Service | Exposes a programmatic interface. |
| **Process** | Win32 Service | A representation of a network process or service. |
| **Process** | Windows Store Process | A representation of a Windows Store process. |
| **Store** | Generic Data Store | A representation of a data store. |
| **Store** | Cache | A representation of a local data cache. |
| **Store** | Cloud Storage | A representation of a cloud storage. |
| **Store** | Configuration File | A configuration file, such as XML, INI, and INF files. |
| **Store** | Cookies | A representation of cookie storage. |
| **Store** | Device | A representation of device local storage. |
| **Store** | File System | A representation of a file system. |
| **Store** | HTML5 Local Storage | A representation of HTML5 local storage. |
| **Store** | Non-Relational Database | A representation of a non-relational database. |
| **Store** | Registry Hive | A representation of the registry. |
| **Store** | SQL Database | A representation of a SQL database. |
| **Data Flow** | Generic Data Flow | A unidirectional representation of the flow of data between elements. |
| **Data Flow** | ALPC | Inter-process communication using an (Advanced) Local Procedure Call (ALPC) port. |
| **Data Flow** | Binary | A representation of a binary data flow. |
| **Data Flow** | HTTP | A representation of an HTTP data flow. |
| **Data Flow** | HTTPS | A representation of a HTTPS, TLS, or SSL data flow. |
| **Data Flow** | IOCTL Interface | An interface for an application to communicate to a device driver. |
| **Data Flow** | IPsec | A representation of an IPsec dataflow. |
| **Data Flow** | Named Pipe | A representation of a named pipe data flow. |
| **Data Flow** | RPC / DCOM | Remote Procedure Call (RPC) or Distributed COM (DCOM) data flow. |
| **Data Flow** | SMB | A representation of a Server Message Block (SMB) 1.0 or SMB 2.0 data flow. |
| **Data Flow** | UDP | User Data Protocol transport. |
| **External Interactor** | External Interactor | A representation of an external interactor. |
| **External Interactor** | Authentication Provider | A representation of an external authorization provider. Examples include Microsoft ID and Facebook. |
| **External Interactor** | Browser | A representation of an external web browser. |
| **External Interactor** | Human User | A representation of a user. |
| **External Interactor** | Megaservice | A large service that has only one instance on the Internet, such as Outlook.com or Xbox Live. |
| **External Interactor** | External Web Application | A representation of an external web application (such as a portal or front end) that delivers web content to a human user. |
| **External Interactor** | External Web Service | A representation of an external web service that exposes a programmatic interface. |
| **External Interactor** | Windows .NET Runtime | Represents the point where an application calls into the .NET Framework. |
| **External Interactor** | Windows RT Runtime | Represents the point where an application calls into WinRT. |
| **External Interactor** | Windows Runtime | Represents the point where an application calls into an unmanaged runtime library such as the CRT. |
| **Trust Boundary** | Generic Trust Boundary (arc and border) | A border representation of a trust boundary. There is no functional difference between an arc boundary and a border boundary, use whichever one provides the most clarity for your diagram. |
| **Trust Boundary** | AppContainer Boundary | A border representation for a Window Store AppContainer boundary. |
| **Trust Boundary** | CorpNet Trust Boundary (border) | A border representation of a corporate network trust boundary. |
| **Trust Boundary** | Internet Boundary (arc) | An arc representation of an Internet trust boundary. |
| **Trust Boundary** | Internet Explorer Boundaries | Describes the types of trust boundaries implemented by Internet Explorer. |
| **Trust Boundary** | Machine Trust Boundary (arc) | An arc representation of a machine trust boundary. |
| **Trust Boundary** | Other Browsers’ Boundaries | Describes the types of trust boundaries implemented by Google Chrome and Mozilla Firefox. |
| **Trust Boundary** | Sandbox Trust Boundary Border | A border representation of a sandbox trust boundary. |
| **Trust Boundary** | User-mode/Kernel-mode Boundary | A border representation of user-mode/kernel-mode separation. |

Table 3 Elements

### Element Properties

The specific properties vary by element type within the threat model. The only common property for every type in the model is **Name**, which identifies each element. All elements except **Boundary** also have **Out of Scope** property**,** which removes the interaction(s) and element from the threat generation matrix. Use the related **Reason For Out of Scope** property to record why it is excluded.

  
Figure 3 Properties for Generic Process

Here are the additional element properties by element type:

#### Properties for Processes

| Element Type | **Attribute Name** | **Additional Attribute Values** | **Modifiable?** |
| --- | --- | --- | --- |
| Generic Process | **Code Type** | **Managed** | Yes |
| **Unmanaged** |
| **Running As** | **Kernel** | Yes |
| **System** |
| **Network Service** |
| **Local Service** |
| **Administrator** |
| **Standard User With Elevation** |
| **Standard User Without Elevation** |
| **Windows Store App** |
| **Isolation level** | **AppContainer** | Yes |
| **Low Integrity Level** |
| **Microsoft Office Isolated Conversion Environment (MOICE)** |
| **Sandbox** |
| **Accepts Input From** | **Any Remote User or Entity** | Yes |
| **Kernel, System, or Local Admin** |
| **Local or Network Service** |
| **Local Standard User With Elevation** |
| **Local Standard User Without Elevation** |
| **Windows Store Apps or App Container Processes** |
| **Nothing** |
| **Other** |
| **Implements or uses an Authentication Mechanism** | **No** | Yes |
| **Yes** |
| **Implements or uses an Authorization Mechanism** | **No** | Yes |
| **Yes** |
| **Implements a Communication Protocol** | **No** | Yes |
| **Yes** |
| **Sanitizes Input** | **No** | Yes |
| **Yes** |
| **Sanitizes Output** | **No** | Yes |
| **Yes** |
| Applications Running on a non-Microsoft OS | **No additional properties.** | **[None]** | [Not Applicable] |
| Browser and ActiveX Plug-ins | **ActiveX** | **No** | Yes |
| **Yes** |
| **Browser Plug-in Object (BHO)** | **No** | Yes |
| **Yes** |
| Browser Client | **Code Type** | **Unmanaged** | No |
| Kernel Thread | **No additional properties.** | **[None]** | [Not Applicable] |
| Managed Application | **Code Type** | **Managed** | No |
| OS Process | **No additional properties.** | **[None]** | [Not Applicable] |
| Thick Client | **Code Type** | **Unmanaged** | This value cannot be changed |
| Thread | **No additional properties.** | **[None]** | [Not Applicable] |
| Virtual Machine | **No additional properties.** | **[None]** | [Not Applicable] |
| Web Server | **No additional properties.** | **[None]** | [Not Applicable] |
| Web Application | **No additional properties.** | **[None]** | [Not Applicable] |
| Web Service | **No additional properties.** | **[None]** | [Not Applicable] |
| Win32 Service | **Code Type** | **Unmanaged** | Yes |
| **Managed** |
| Windows Store Process | **Code Type** | **Managed** | No |
| **Context** | **Local** | Yes |
| **Web** |
| **'Documents Library' capability** | **Yes** | Yes |
| **No** |
| **'Enterprise Authentication' capability** | **Yes** | Yes |
| **No** |
| **Internet (Client & Server)' capability** | **Yes** | Yes |
| **No** |
| **'Internet (Client)' capability** | **Yes** | Yes |
| **No** |
| **'Location' capability** | **Yes** | Yes |
| **No** |
| **'Microphone' capability** | **Yes** | Yes |
| **No** |
| **'Music Library' capability** | **Yes** | Yes |
| **No** |
| **'Pictures Library' capability** | **Yes** | Yes |
| **No** |
| **'Private Networks (Client & Server)' capability** | **Yes** | Yes |
| **No** |
| **'Proximity' capability** | **Yes** | Yes |
| **No** |
| **'Removable Storage' capability** | **Yes** | Yes |
| **No** |
| **'Shared User Certificates' capability** | **Yes** | Yes |
| **No** |
| **'Text Messaging' capability** | **Yes** | Yes |
| **No** |
| **'Videos Library' capability** | **Yes** | Yes |
| **No** |
| **'Webcam' capability** | **Yes** | Yes |
| **No** |

Table 4 Element Properties for Processes

#### Properties for Data Storage

| Element Name | **Attribute Name** | **Additional Attribute Values** | **Modifiable?** |
| --- | --- | --- | --- |
| Generic Data Store | **Stores Credentials** | **No** | Yes |
| **Yes** |
| **Stores Log Data** | **No** | Yes |
| **Yes** |
| **Encrypted** | **No** | Yes |
| **Yes** |
| **Signed** | **No** | Yes |
| **Yes** |
| **Write Access** | **Yes** | Yes |
| **No** |
| **Removable Storage** | **Yes** | Yes |
| **No** |
| **Backup** | **Yes** | Yes |
| **No** |
| **Shared** | **Yes** | Yes |
| **No** |
| **Store Type** | **SQL Relational Database** | Yes |
| **Non Relational Database** |
| **File System** |
| **Registry** |
| **Configuration** |
| **Cache** |
| **HTML5 Storage** |
| **Cookie** |
| **Device** |
| Cookies | **HTTP Only** | **Yes** | Yes |
| **No** |
| Devices | **GPS** | **Yes** | Yes |
| **No** |
| **Contacts** | **Yes** | Yes |
| No |
| **Calendar Events** | **Yes** | Yes |
| **No** |
| **SMS messages** | **Yes** | Yes |
| **No** |
| **Cached Credentials** | **Yes** | Yes |
| **No** |
| **Enterprise Data** | **Yes** | Yes |
| **No** |
| **Messaging Data (Mail, IM, SMS…)** | **Yes** | Yes |
| **No** |
| **SIM Storage** | **Yes** | Yes |
| **No** |
| **Other Data** | **Yes** | Yes |
| **No** |
| File System | **File System Type** | **NTFS** | Yes |
| **ExFAT** |
| **FAT** |
| **ReFS** |
| **IFS** |
| **UDF** |
| **Other** |

Table 5 Properties for Storage

#### Properties for Data Flow

| Element Name | **Attribute Name** | **Additional Attribute Values** | **Modifiable?** |
| --- | --- | --- | --- |
| Generic Data Flow | **Physical Network** | **Wire** | Yes |
| **Wi-Fi** |
| **Bluetooth** |
| **2G - 4G** |
| **Source Authenticated** | **No** | Yes |
| **Yes** |
| **Destination Authenticated** | **No** | Yes |
| **Yes** |
| **Provides Confidentiality** | **No** | Yes |
| **Yes** |
| **Provides Integrity** | **No** | Yes |
| **Yes** |
| **Transmits XML** | **No** | Yes |
| **Yes** |
| **Contains Cookies** | **Yes** | Yes |
|  | **No** |
| **SOAP Payload** | **No** | Yes |
|  | **Yes** |
| **REST Payload** | **No** | Yes |
| **Yes** |
| **RSS Payload** | **No** | Yes |
| **Yes** |
| **JSON Payload** | **No** | Yes |
| **Yes** |
| ALPC | **No additional properties.** | **[None]** | [Not Applicable] |
| Binary | **No additional properties.** | **[None]** | [Not Applicable] |
| HTTP | **No additional properties.** | **[None]** | [Not Applicable] |
| HTTPS | **No additional properties.** | **[None]** | [Not Applicable] |
| IOCTL Interface | **No additional properties.** | **[None]** | [Not Applicable] |
| IPsec | **No additional properties.** | **[None]** | [Not Applicable] |
| Named Pipe | **No additional properties.** | **[None]** | [Not Applicable] |
| RPC / DCOM | **No additional properties.** | **[None]** | [Not Applicable] |
| SMB | **No additional properties.** | **[None]** | [Not Applicable] |
| UDP | **No additional properties.** | **[None]** | [Not Applicable] |

Table 6 Properties for Data Flow

#### Properties for External Interactors

| Element Name | **Attribute Name** | **Additional Attribute Values** | **Modifiable?** |
| --- | --- | --- | --- |
| External Interactor | **Authenticates Itself** | **No** | Yes |
| **Yes** |
| **Type** | **Not Selected** | Yes |
| **Code** |
| **Human** |
| **Microsoft** | **No** | Yes |
| **Yes** |
| Authentication Provider | **No additional properties.** | **[None]** | [Not Applicable] |
| Browser | **Type** | **Code** | No |
| Human User | **Type** | **Human** | No |
| Megaservice | **No additional properties.** | **[None]** | [Not Applicable] |
| External Web Application | **Type** | **Code** | No |
| External Web Service | **Type** | **Code** | No |
| Windows .NET Runtime | **Type** | **Code** | No |
| Windows RT Runtime | **Type** | **Code** | No |
| Windows Runtime | **Type** | **Code** | No |

Table 7 Properties for External Interactor

#### Properties for Trust Boundaries

| Element Name | **Attribute Name** | **Additional Attribute Values** | **Modifiable?** |
| --- | --- | --- | --- |
| Generic Trust Boundary (arc and border) | **Boundary Type** | **Internet** | Yes |
|  | **Machine Boundary** |
|  | **Kernel Boundary** |
|  | **AppContainer Boundary** |
|  | **Corporate Network** |
|  | **Sandbox Boundary** |
|  | **IE Boundary** |
|  | **Other** |
| AppContainer Boundary | **No additional properties.** | **[None]** | [Not Applicable] |
| Corpnet Trust Boundary (Border) | **No additional properties.** | **[None]** | [Not Applicable] |
| Internet Boundary (arc) | **No additional properties.** | **[None]** | [Not Applicable] |
| Internet Boundaries | **Boundary Type** | **Internet Boundary** | No |
| **Low Integrity Level Sandbox** | **Yes** | Yes |
| **No** |
| **App Container Sandbox** | **Yes** | Yes |
| **No** |
| **JavaScript Sandbox** | **Yes** | Yes |
| **No** |
| **Flash Sandbox** | **Yes** | Yes |
| **No** |
| Machine Trust Boundary (Arc) | **Boundary Type** | **Machine Boundary** | No |
| Other Browser’s' Boundaries | **Boundary Type** | **Other** | No |
| **Chrome JavaScript Sandbox** | **Yes** | Yes |
| **No** |
| **Chrome Sandbox** | **Yes** | Yes |
| **No** |
| **Firefox JavaScript Sandbox** | **Yes** | Yes |
| **No** |
| Sandbox Trust Boundary Border | **Boundary Type** | **Sandbox Boundary** | No |
| User-mode/Kernel-mode Boundary | **Boundary Type** | **Kernel Boundary** | No |

Table 8 Properties for Trust Boundary

In addition to the above built-in properties, additional properties can be added through changes to the Template. For instructions on extending the Template, please see “Appendix I — Extending the Threat ”**.**

### Threat Model Information

The **Threat** **Model Information** dialog contains basic information about the threat model and asks a series of security questions to help establish the risk of the component. You can select this dialog from the **File** menu.

### Messages

The **Messages** window allows the tool to identify any errors, warnings or inconsistencies in the drawing or the Knowledge Base.

### Notes

The **Notes** window provides a place to record notes and comments during the threat model discussion. These are included in the report, but not used for threat generation or analysis.

# Automation

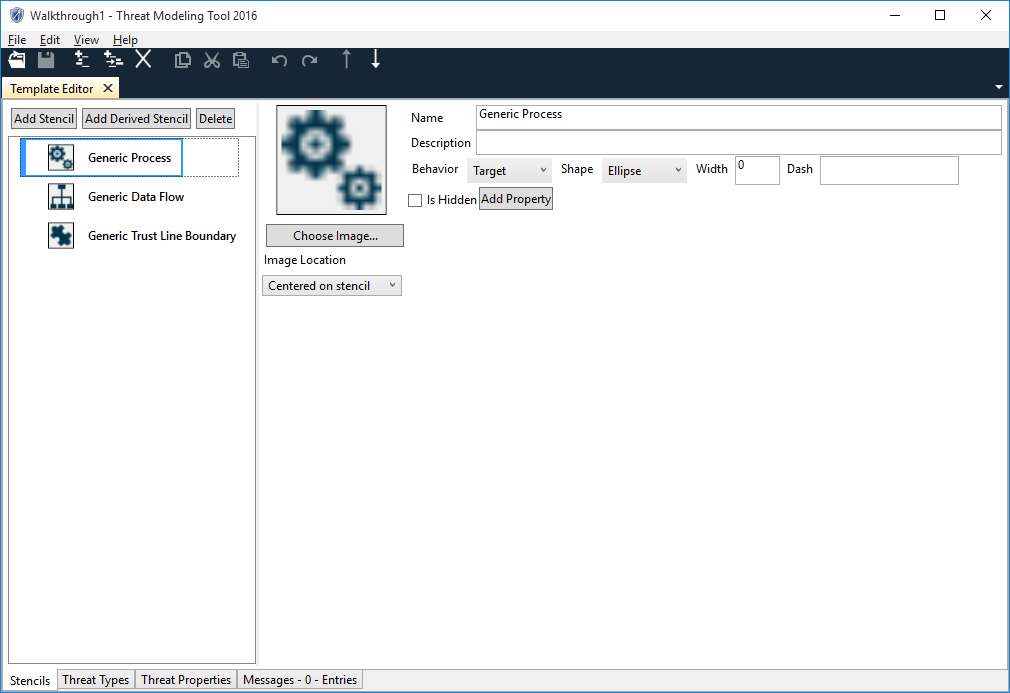
SDL Threat Modeling Tool is not scriptable.

# Appendices

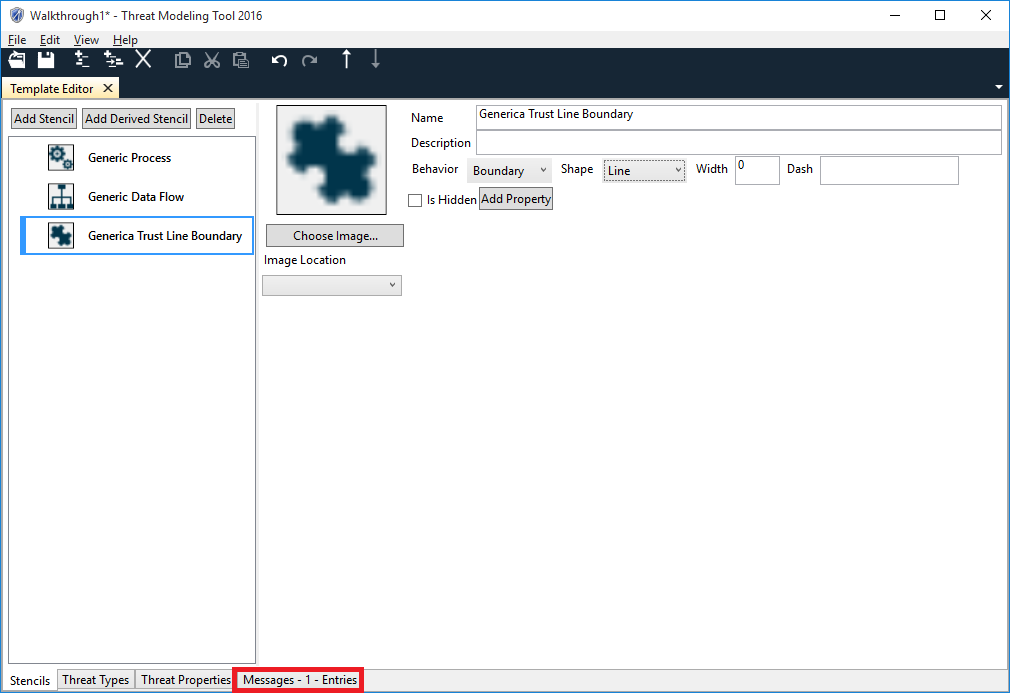
## Appendix I — Extending the Threat Template

### Creating Stencils

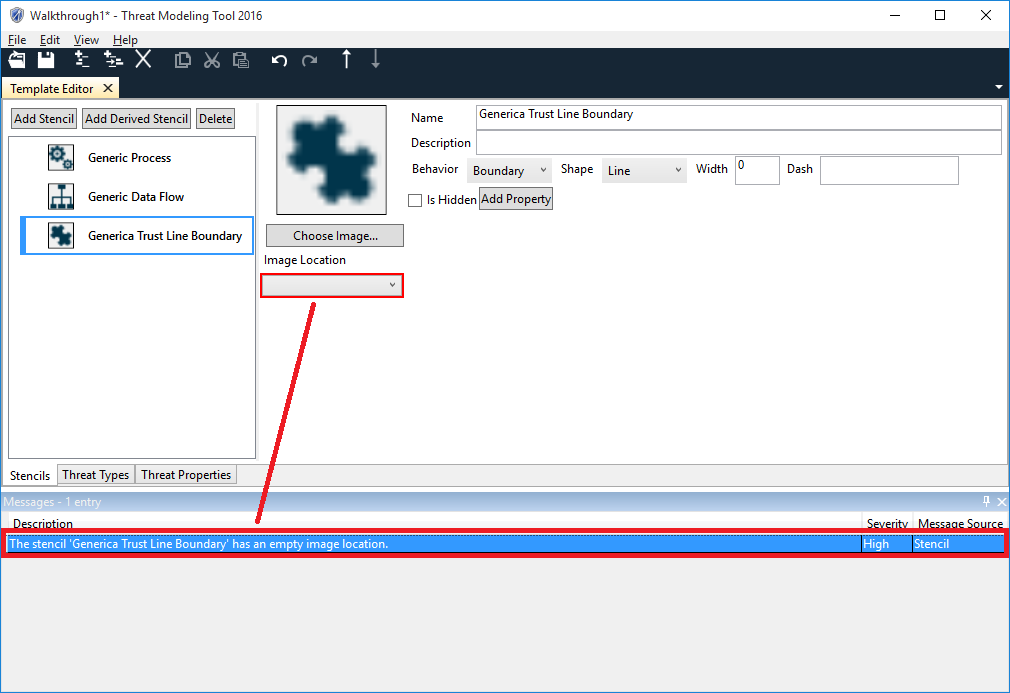
The threat model editor uses a template to guide users as they create threat models. The template defines all the stencils that can be used to create a threat model, such as generic process or OS process. Using the template editor, you can customize the list of stencils that are available in the threat model editor. The template also defines the threats that TMT generates for each threat model. Using the template editor, you can customize the list of threats that apply in the threat model editor.



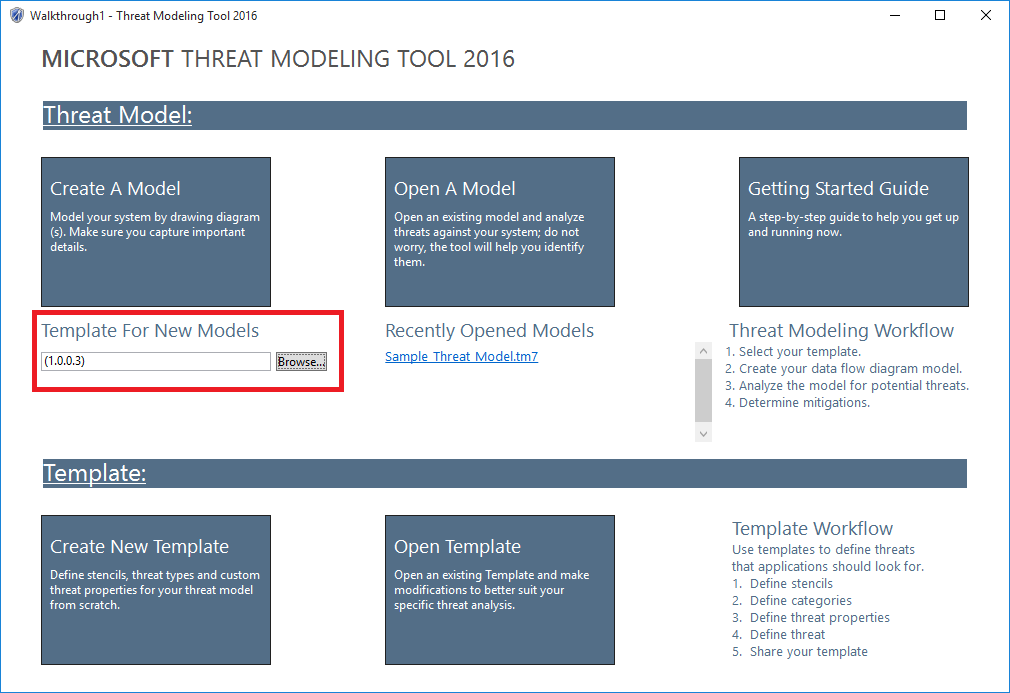
When you select new template, TMT puts you on the stencils tab of a blank template. You can use the Add Stencil button to create new stencils. Each stencil has 5 important controls. The name and image show up in the stencil list in the threat model editor. The behavior and shape determine the kind of stencil. If behavior is set to target, the stencil represents an object, such as a generic process. The shape determines if it is an ellipse, rectangle, or parallel lines. If behavior is set to flow, the stencil represents a flow connecting objects, such as a generic data flow. If behavior is set to boundary, the stencil represents some kind of trust boundary, such as generic trust line boundary. The shape of a boundary can be either line or rectangle. All templates should have at least one stencil with each behavior. You must select a value for the image location control of each stencil. The image location controls where the image will be displayed when a user adds a stencil in the threat model editor. Try the options out and pick the one you like. If you don't set the image location, the template editor gives you an error message. You can't use a template to create threat models till all error messages have been fixed.



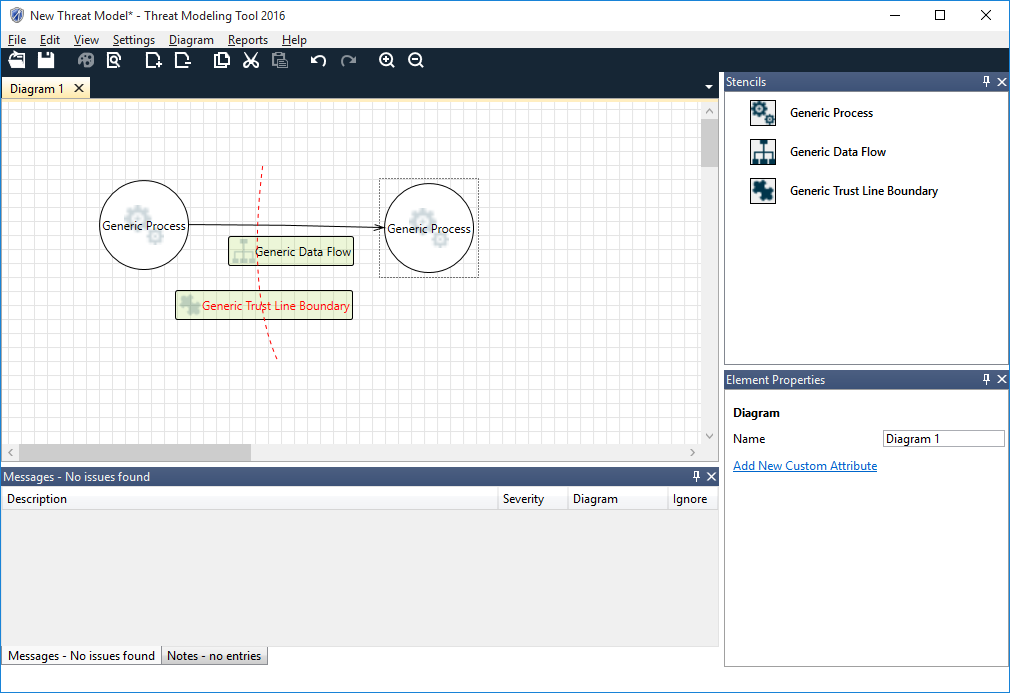
If you select the messages tab and double click, TMT will show you the message pane and the control the message applies to. In this case, the message indicates that the image location hasn't been set. The image location control is highlighted to show you where TMT found the error.



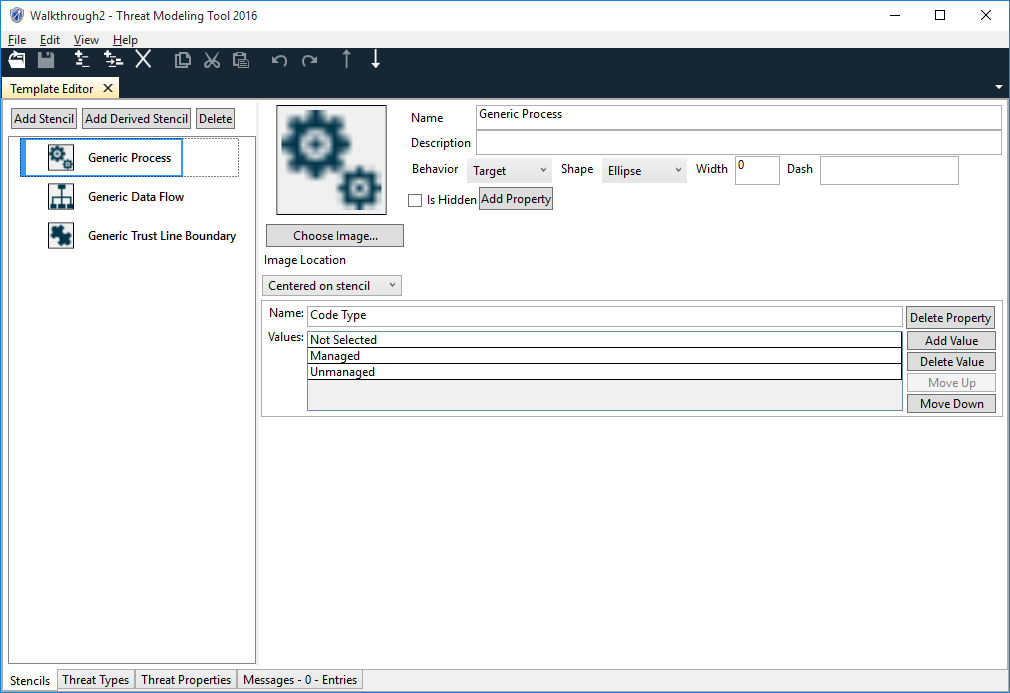
After fixing the error and saving the template, you can use the template to create a new threat model. First close the template to return to the start menu.



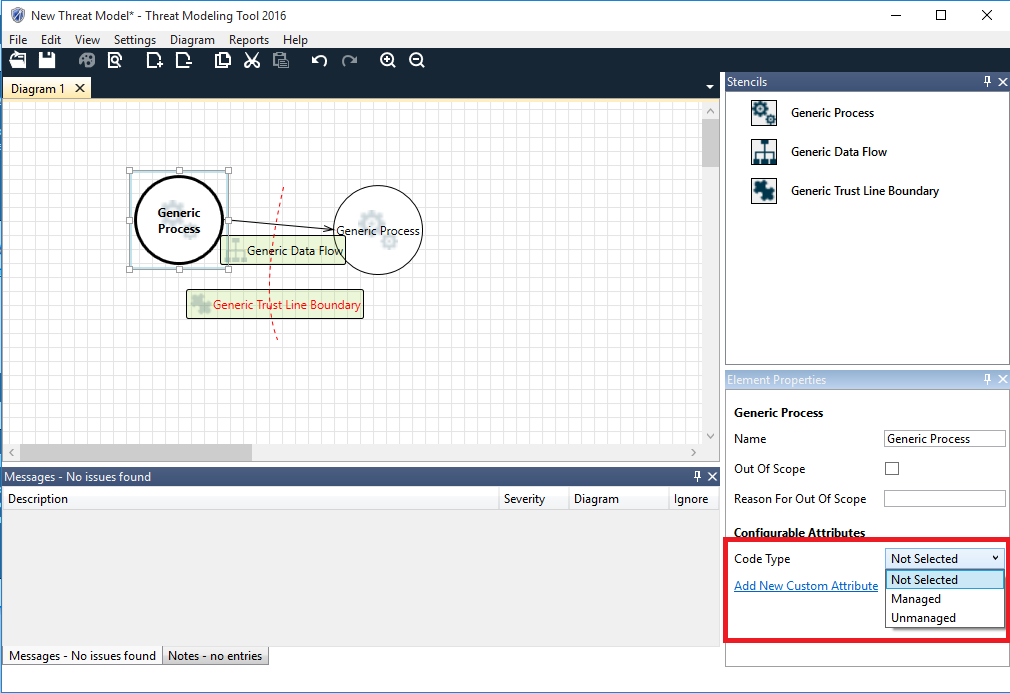
Select the browse button and select the template that you just created. This configures the "Create A Model" button on the start menu. The next time a user selects "Create A Model", your new template will be used.



The stencils that were created in the template are now available in the threat model editor.

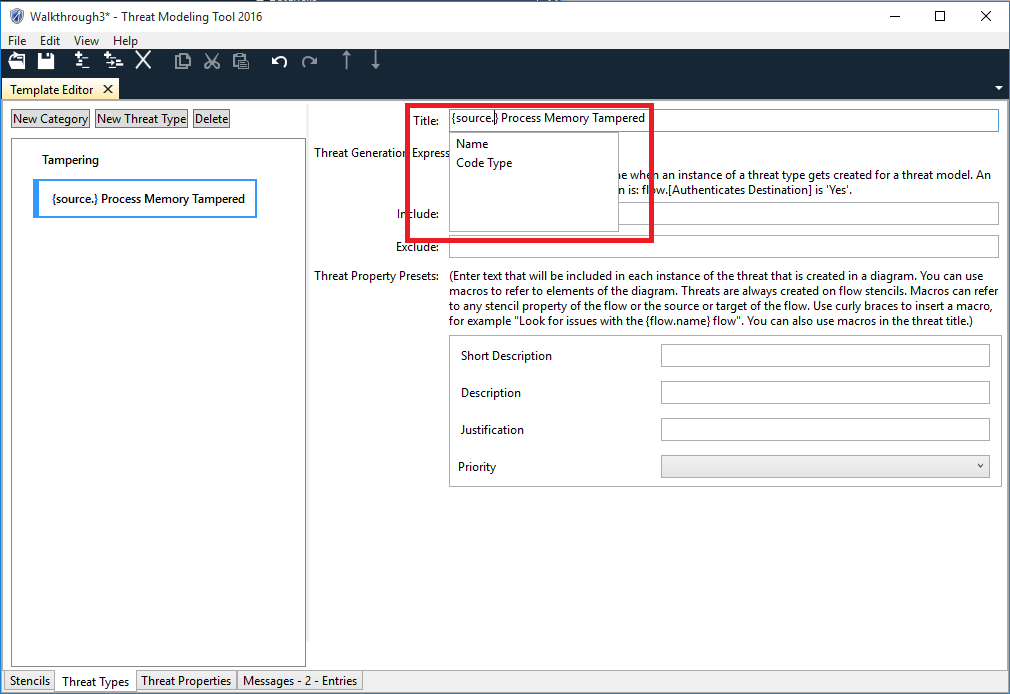


Go back to the template editor and open the template you just created. The add property button can be used to create new stencil properties.

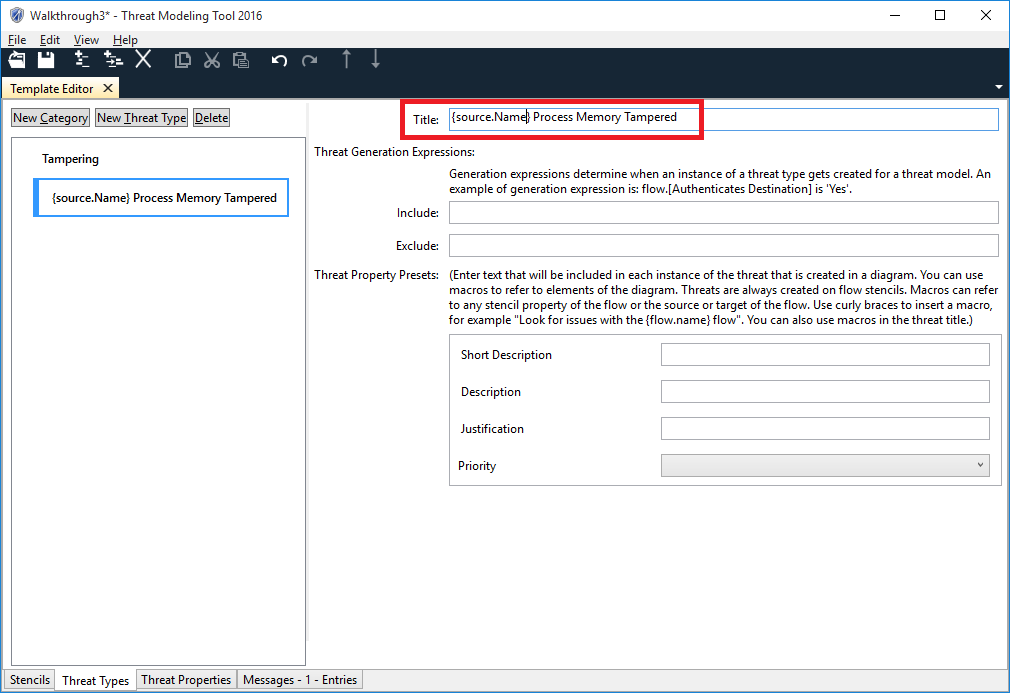


Back in the threat model editor, when you create a new model, the new properties you created are available as stencil properties in the data flow diagram. The first value in the list is the default value for all stencils created in the threat model editor. It's convenient to use "Not Selected" as the first value in the list. In this example, if the property code type didn't have the value "Not Selected", all new generic processes would have code type set to managed by default.

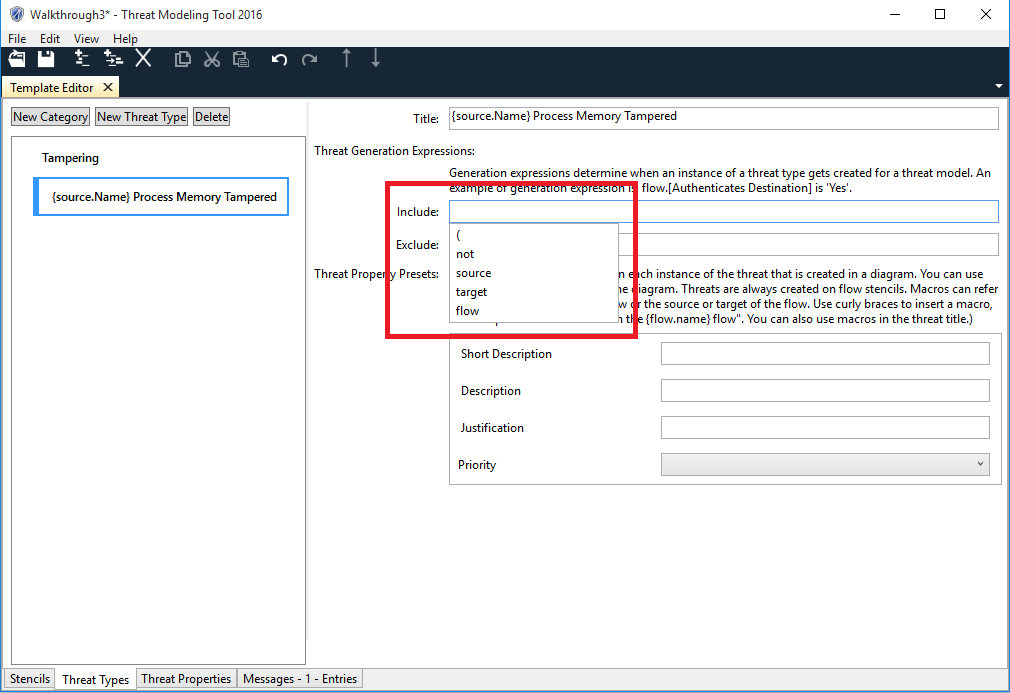
### Creating Threat Types



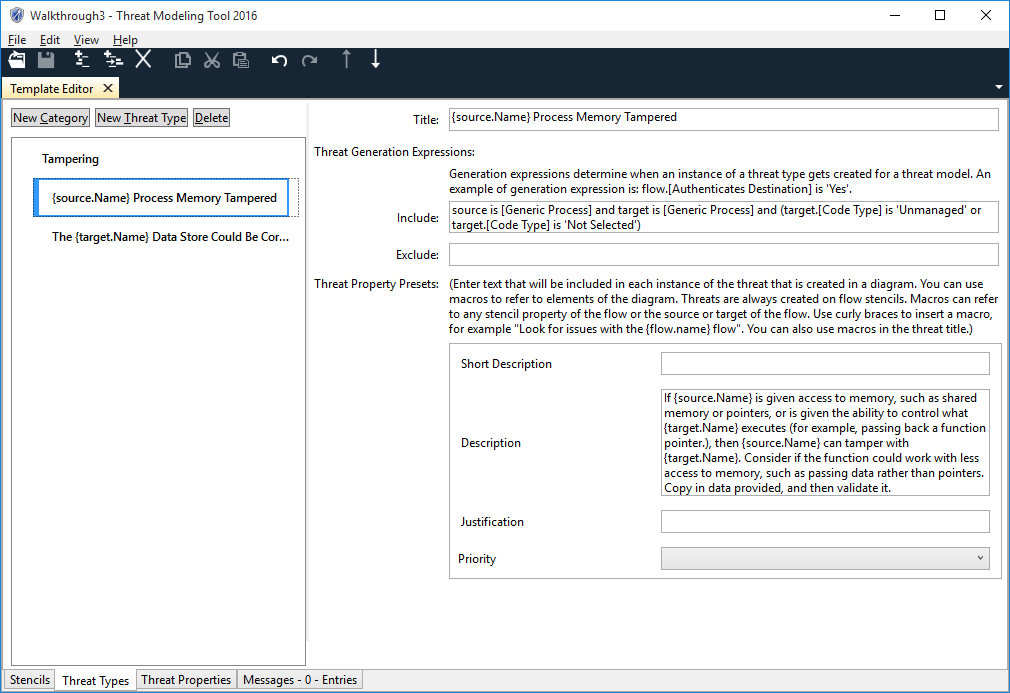
Back in the template editor, the next interesting tab is the threat types tab. This is where you define the threats that TMT will create for threat models. Use the new category button to create a new category. Categories are just used to organize threats. For example, SDL uses the STRIDE categories (spoofing, tampering, etc). The new threat type button creates a new threat type. TMT will look at each threat type and each flow in a DFD. If TMT determines a threat type applies, TMT will create a new threat in the threat list. A threat type has 2 important controls. The value in the name control of the threat type shows up as the title of the threat in the threat list. You can use curly braces to reference stencil properties in the title. Intellisense will list the properties available to you.



All threats are generated against flow stencils in the data flow diagram in the threat model editor. {flow.name} is replaced with the flow's name property. {source.name} is replaced with the name property of the object at the source end of the flow (before the arrow). {target.name} is replaced with the name property of the object at the target end of the flow (after the arrow).



The include control tells TMT when to create the threat. TMT has Intellisense to help you enter the include expression correctly.

  
A simple expression like "source is [Generic Process]" tells TMT to create the threat for any flow if the source end of the flow is connected to a generic process. 3 kinds of equations can be used in an expression.

source is [stencil]

This equation matches any data flow where the source is the specified stencil. This equation can also be used to match the flow or target stencils.

source.[stencil property] is 'stencil property value'

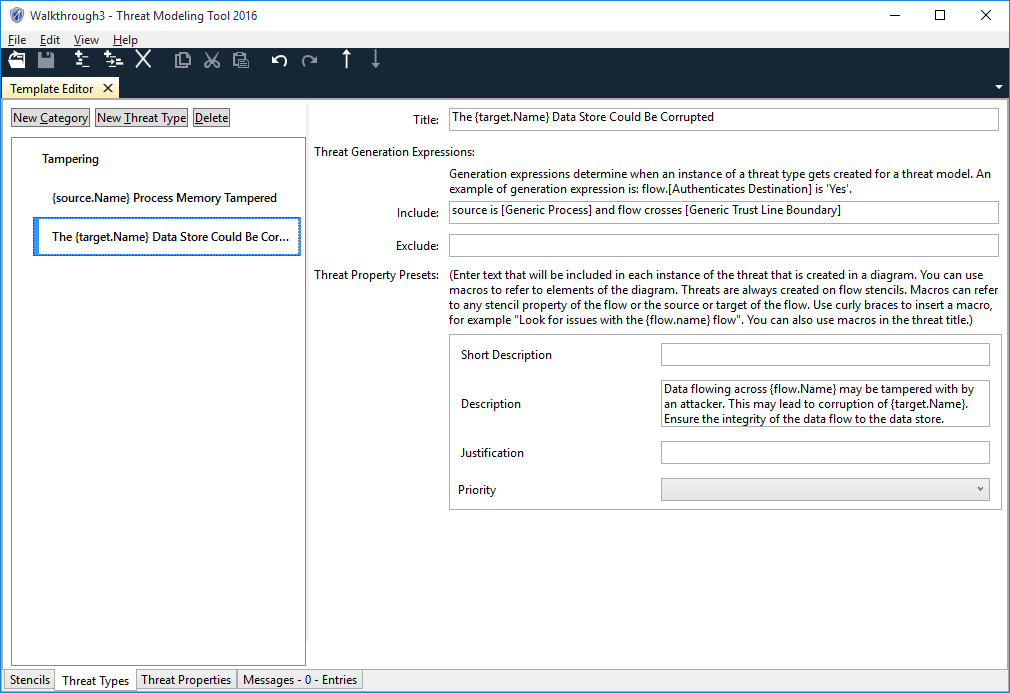
This equation matches any data flow where the source has the specified stencil property value. For example, the equation "target.[Code Type] is 'Unmanaged'" will apply to any data flow if the target object has the property code type and the value of that property is unmanaged. This kind of equation can match stencil property value of the source, target, or flow.

flow crosses [boundary stencil name]

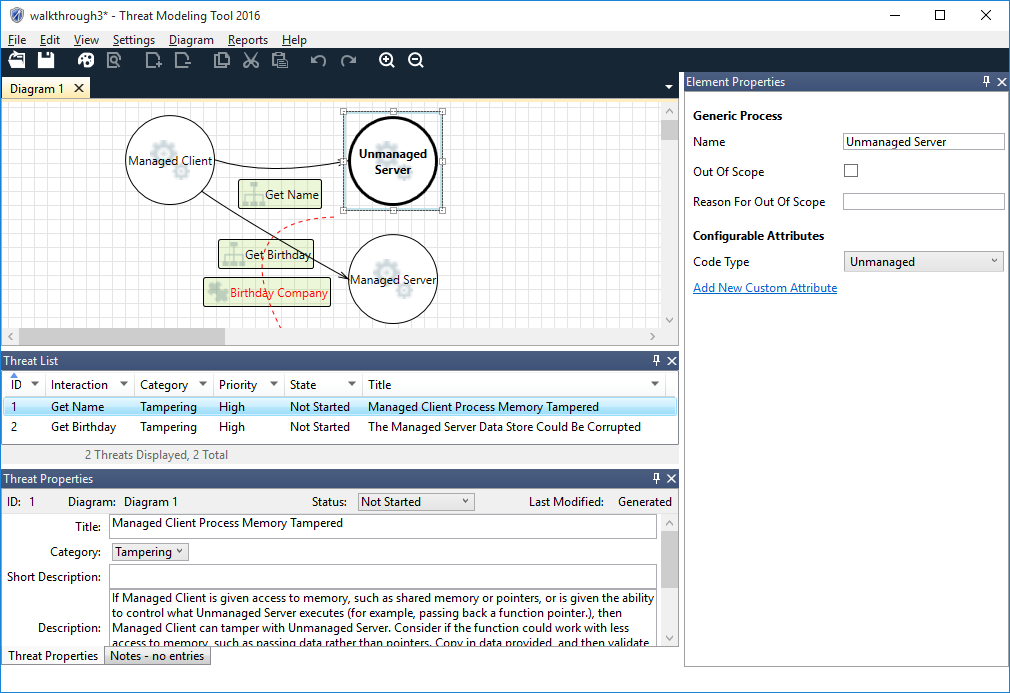
The last kind of equation matches any flow that crosses the specified boundary stencil. For example "flow crosses [Generic Trust Line Boundary]" will match any flow if it there is a generic trust line boundary that crosses over the flow.

If you enter a generic stencil name, TMT will also match all the stencils derived from that generic stencil. For example, in the default template OS process is derived from generic process, so the expression "source is [generic process]" will also match a data flow connected to an OS process. See the section Threat Expressions below for more details.

Any text that is entered into the threat property preset controls will show up in the threat properties pane in the threat model editor. The same curly braces that work in the title can be used to enter replacement strings in the threat property presets.

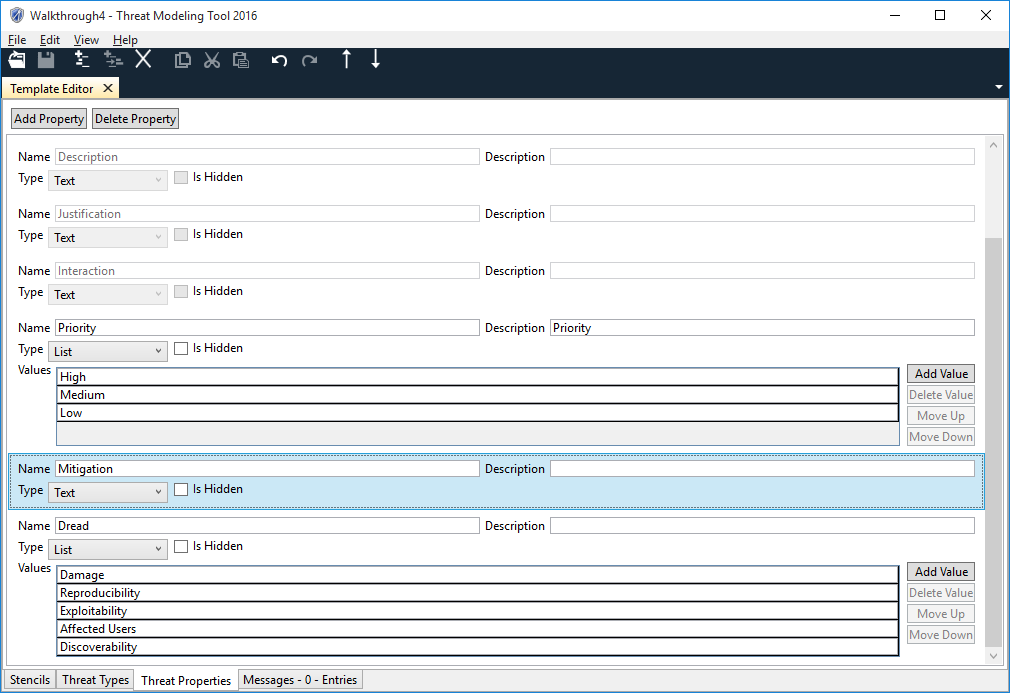


This example demonstrates the crosses equation.

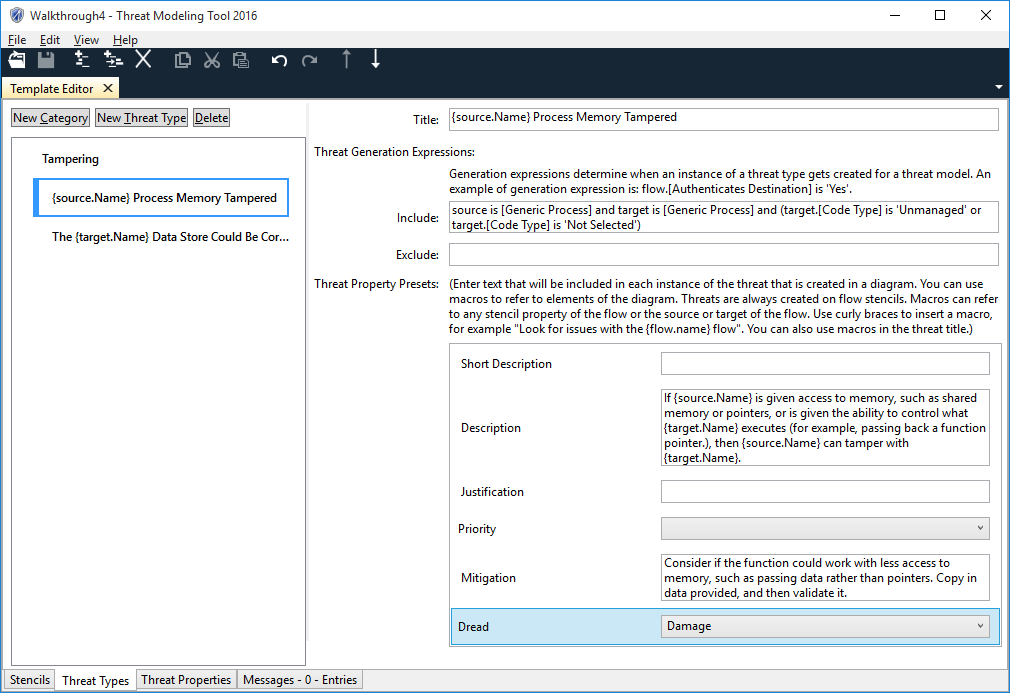


Creating this threat model based on the template will demonstrate 2 threats. The threat "Managed Client Process Memory Tampered" is generated on the flow "Get Name" because the generic process "Unmanaged Server" has the property "Code Type" set to "Unmanaged". The include expression for the threat will be true when "target.[Code Type] is 'Unmanaged'". The threat "The Managed Server Data Store Could Be Corrupted" is generated on the flow "Get Birthday" because the flow crosses the boundary "Birthday Company". The include expression for the threat will be true when "flow crosses [Generic Trust Line Boundary]".

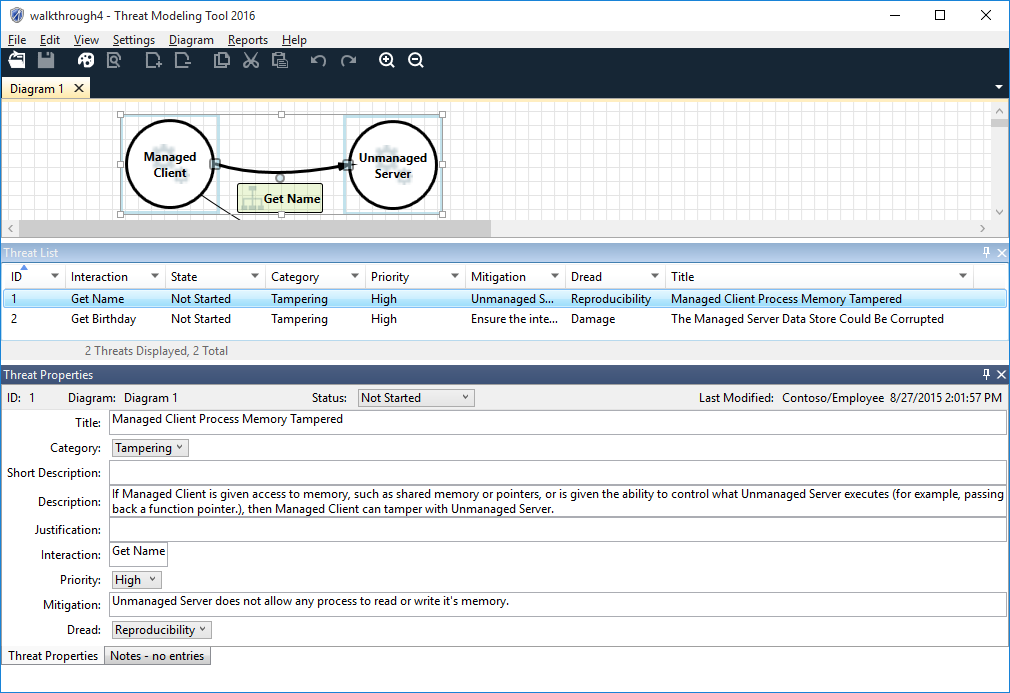
### Adding Threat Properties



The threat properties tab can be used to add and modify threat properties. There are a set of require threat properties that you cannot edit, but you can hide them if they are not useful in your model. Every threat property in this tab will show up in the preset list for every threat type. All threats have the same list of properties. Each threat type defines the initial value for each threat property. In this example, the mitigation threat property is a text control and the dread threat property is a list control.



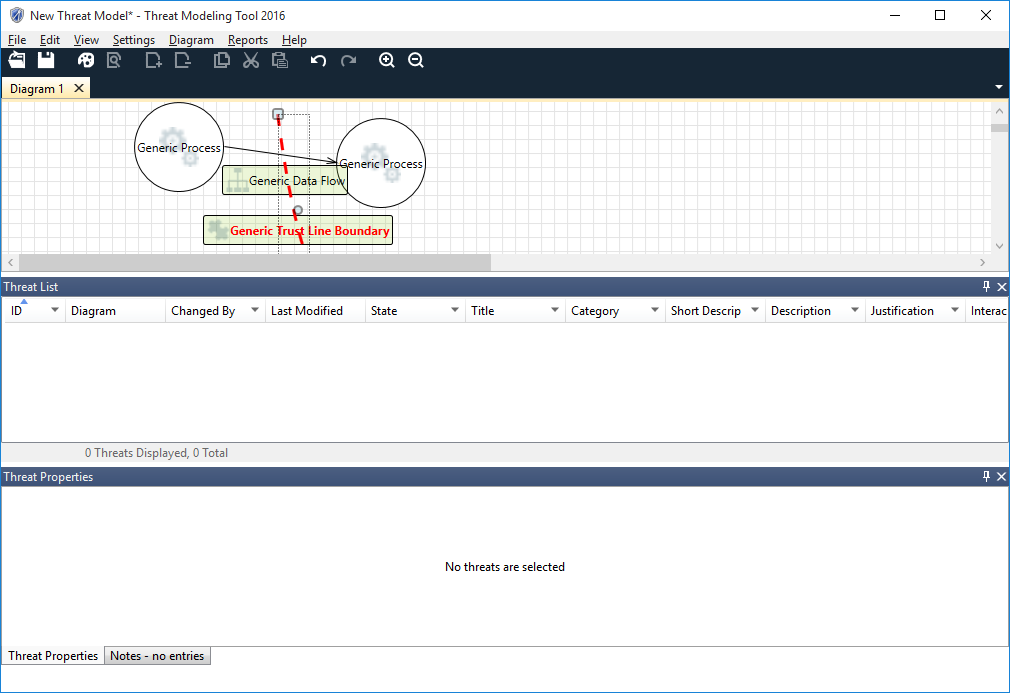
In the threat types tab, the new threat properties now show up in the list of presets. Since mitigation is a text threat property, you can set the default value for this threat to text. In this example I've moved some text from the description into the mitigation. The dread control has a list of values. In this example I've set the default value to damage.



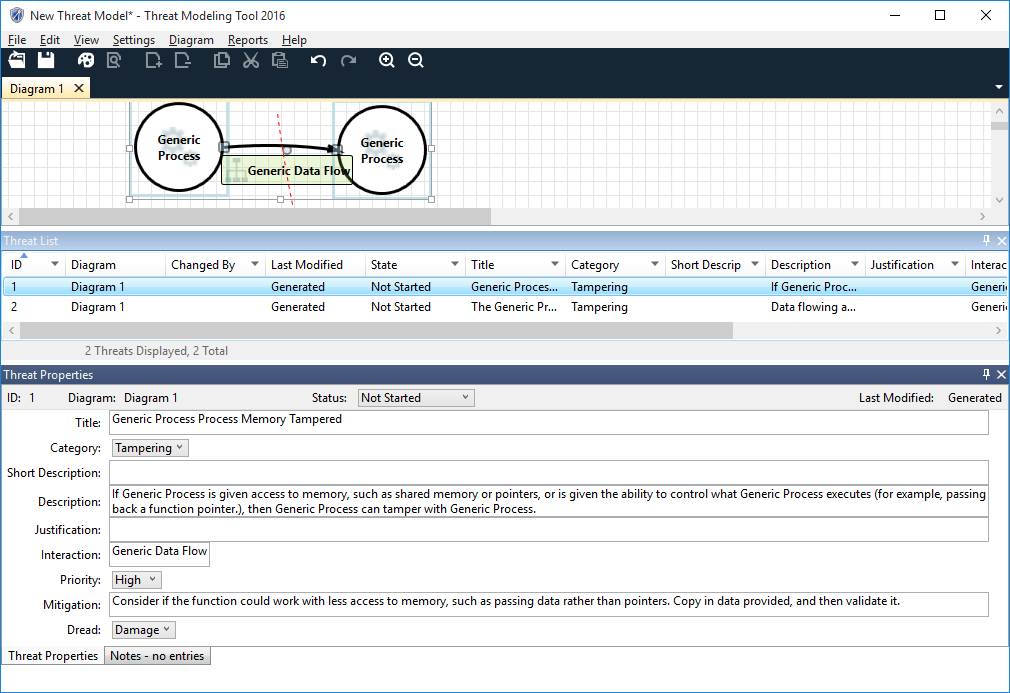
When you create a new threat model with the latest template, the new threat properties will show up in the threat properties pane. The threat properties will have the default value set on the threat types tab, but the user will be able to edit them. In this example, I've edited the values for mitigation and dread.

### Updating Threat Models

When a threat model is created, it makes a copy of the template set on the start page. Updates to the template do not affect the threat model. The function apply template is used to update a threat model to use a newer template. The section Creating Stencils defines a template that just contains stencil. It does not have any threat types.



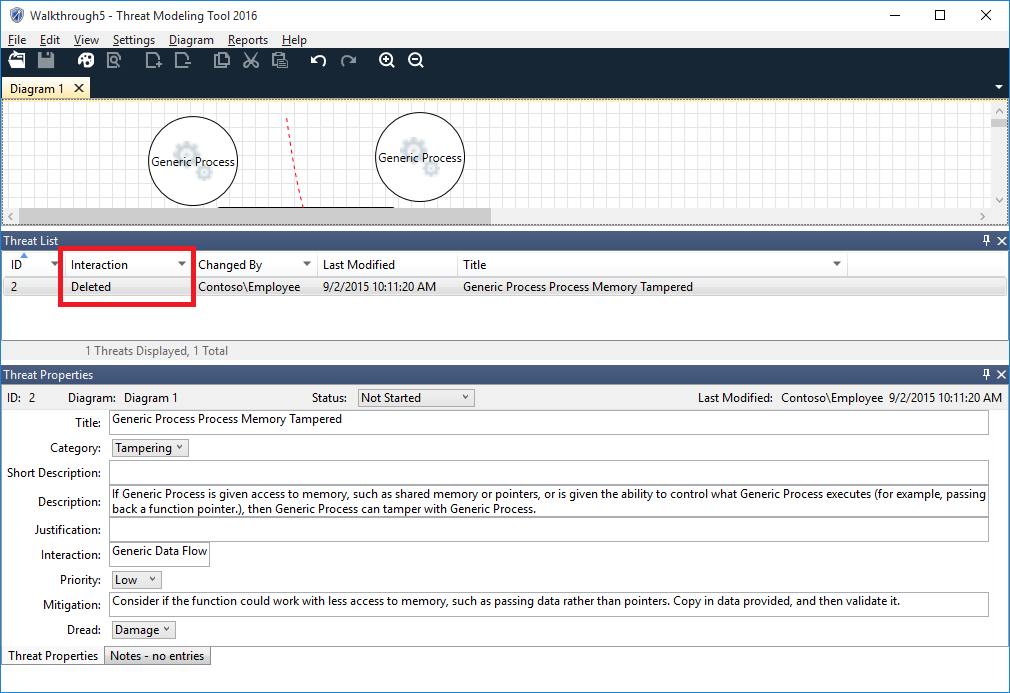
If I create a threat model using that template and switch to the analysis mode, it will look like this.

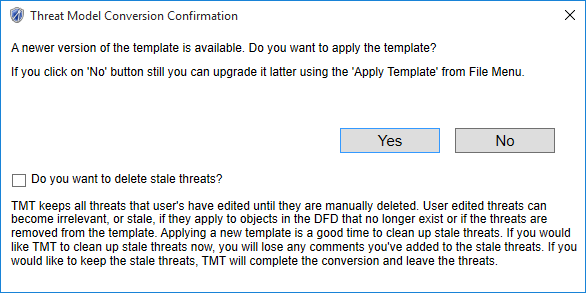


If I use file / apply template and select the template defined in the section Adding Threat Properties, the threat model will look like this. The threats and the threat properties from that template are now part of my threat model.

Adding features to a template makes a straightforward change when you apply the template to a threat model. Any new stencils are available for the threat model authors. Any new stencil properties are added to all the objects on the drawing surface. Any new stencil property values are available to the threat model author. Any new threat properties are added to all the threats in the threat list. TMT examines the DFD and creates threats in the threat list for any new threat types.

Deleting features is almost as simple. Deleted stencil properties, stencil property values, and threat properties are removed. If a derived stencil is deleted, TMT converts all objects of that type into its parent. For example, if I deleted the OS process stencil from the default template, when I applied that template to a threat model, all OS process objects would be converted to generic process objects.

Deleting threat types is a little more complicated. Each threat is in one of 2 states, generated or modified. If a user edits a threat in the threat model editor, the threat list records which user changed the threat in the last modified column. If no user has ever edited a threat, the last modified column shows the word generated. TMT will not delete a user's changes. Once a threat is in the modified state, TMT will never update it. If you rename the target process, TMT won't update the title. If you delete the target process, TMT won't delete the threat. If you apply a template that no longer contains the threat type, TMT won't delete the threat. When a modified threat no longer applies, TMT changes the interaction column to the word deleted. When you apply a template, TMT deletes all generated threats and regenerates them. There is no way for TMT to handle changing the behavior of a stencil. If you change the behavior, TMT will essentially delete the stencil and create a new stencil with the same name.



When you apply a template, the conversion confirmation dialog has a checkbox labeled "Do you want to delete stale threats?" If you check that box, TMT will delete all modified threats that no longer apply to the threat model.

### Menu Choices

The **File** menu provides options to create, open, save, or close templates:

* **New Template** creates a new Template.
* **Open Template** open threat template (.tb7).
* **Save** saves the current Template using current name.
* **Save As** saves the current Template with option to change name or location.
* **Import** a user can import a template from previous versions of TMT
* **Template Information** Open Template information
* **Close Template** closes the current template.
* **Exit** exits the tool.

The **Edit** menu provides options to interact with the clipboard:

* **Undo** undoes the last operation.
* **Redo** redoes the most recent operation.
* **Copy** copies the current selection into clipboard.
* **Paste** pastes the current clipboard contents onto template editor.
* **Cut** places the current selection into clipboard and removes from template editor.
* **Delete**  removes the element
* **Move Up** moves up the current selection.
* **Move Down** move down the current selection
* **Add Stencil** adds a stencil
* **Add Derived Stencil** adds a derived stencil under the selected stencil
* **Add Threat Category** adds a threat category
* **Add Threat Type** adds threat type under selected threat category
* **Add Threat Property** adds a threat property

The **View** menu provides options to view different functional windows within the tool:

* **Stencils** switches to **stencil** view.
* **Threat Types** switches to **Threat types** window.
* **Threat Properties** shows the **Properties** window
* **Messages** show the **Message** window.

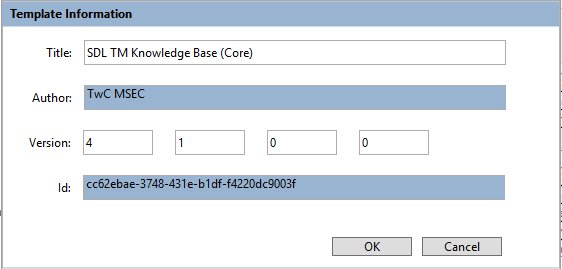
**Intellisense** Features in TMT that help the user by making decisions automatically.

The **Help** menu contains items relating to receiving help with the product:

### Toolbar

|  |  |
| --- | --- |
| **Open** opens explorer file open prompt | **Save** saves current open template file |
| **Add** top level object | **Add** nested object |
| **Delete** selected text | **Copy** copies the current selected text |
| **Cut** cuts current selected text | **Paste** pastes the clipboard contents onto text control |
| **Undo** undoes the last operation | **Redo** redoes the most recent operation |
| **Move Up** selected object | **Move Down** selected object |
| Template Information |  |

**File -> Template Information** brings up below UI. Id field here uniquely identify each template. The Id gets propogated to threat model when a model is created using this template. This keeps the connection between the threat model and the template used to create the threat model. You can upgrade your threat model to other template only if the template has been extended with same id which your threat model is based off. Other than id, version number is another important paratemer in template. Version number keeps track of versioning of template. Whenever there is any change done in the template and you save it, revision number always gets updated automatically. You have an option to change the version number. This ensures that your threat model always convert to latest version of template.



### Context (Right–Click) Menu

### Stencil Window

Right-click on the Stencil window or an element, to choose from a set of actions will vary depending on the context.

Actions available by right-clicking the stencil window in tree area

* **New Stencil** creates a new stencil
* **New Derived Stencil** creates new derived stencil
* **Delete Stencil** removes the stencil
* **Move Up** moves up the current selection
* **Move Down** move down the current selection

Actions available by right-clicking the stencil window in the property area

* **Add New Property** add new property below the selected property list
* **Delete Property** deletes selected property
* **Move Up** moves the current selection up
* **Move Down** move the current selection down

### Threat Types Window

Right-click on the Threat type window or an element, to choose from a set of actions will vary depending on the context.

Actions available by right-clicking the threat type window in tree area:

* **New Threat Category** creates new threat category
* **New Threat Type** creates new threat type
* **Delete** removes the selected threat type or category
* **Move Up** moves up the current selection
* **Move Down** move down the current selection

Actions available by right-clicking in text box in threat Type are

* **Cut** cuts current selection
* **Copy** copies current selection
* **Paste** pastes the current clipboard contents

### Threat Properties Window

Right-click on the Threat Properties window or an element, to choose from a set of actions will vary depending on the context.

Actions available by right-clicking in text box of threat properties window:

* **Cut** places the current selection into clipboard and removes from template editor.
* **Copy** copies the current selection into clipboard.
* **Paste** pastes the current clipboard contents onto template editor

Actions available by right clicking in the threat properties list box window

* **Move Up** moves the current selectionup
* **Move Down** move the current selection down

### General Keyboard Shortcut Keys

|  |  |
| --- | --- |
| Function | Keyboard Shortcut |
| *New Template* | **Ctrl + N** |
| *Open Template* | **Ctrl + O** |
| *Save Template* | **Ctrl + S** |
| *Import Template* | **Alt – F, I** |
| *Template Information* | **Alt – F, T** |
| *Close Template* | **Alt – F, C** |
| *Exit* | **Alt -F, E** |
| *Undo* | **Ctrl + Z** |
| *Redo* | **Ctrl + Y** |
| *Copy* | **Ctrl + C** |
| *Cut* | **Ctrl + X** |
| *Paste* | **Ctrl + V** |
| *Delete* | **Delete** |
| *Move Up* | **Ctrl + Up Arrow** |
| *Move Down* | **Ctrl + Down Arrow** |
| *Intellisense* | **Ctrl + Space** (Only for threat type tab for Include and Exclude Expressions) |
| *Help* | **F1** |
| *New Stencil* | **Shift F10+ S** |
| *New Derived Stencil* | **Shift F10+ D** |
| *New Property (both on Stencil Screen and on Threat Properties Screen)* | **Ctrl+ P** |
| *New Category* | **Shift F10+ C** |
| *New Threat Definition* | **Shift F10+ T** |
| *Right click to bring menu screens* | **Shift + F10** (For menu screens as described in previous sections) |

### Stencils

Stencils are the basic building blocks for creating threat models. Once a stencil is defined in a template, users can directly create those stencils in their threat models. The stencil editor can be used to create **Stencils** and **Derived Stencils**. Each stencil requires user to provide suitable image to recognize purpose of stencil, Name, Description, Behavior, Shape, Width, Dash and multiple properties with list of values against each of the property. Name and Description are free flowing text with restriction of special characters. Behavior can take one of the 3 values namely Target, Flow and Boundary. Shape can be one of Ellipse, Rectangle, Line and Parallel Lines. But not all the possible combinations of these 2 fields are allowed. Upon selection of Behavior, TMT automatically displays allowed valued of shapes in the dropdown.

*\*Note: Applying a template cannot handle changing the behavior of stencils. If the template author changes the behavior of a stencil, any instances of that stencil will be deleted any time a user applies the new template.*

The **Width** default value is set to zero (0) and user can change according to requirement. It accepts only **numeric values.** It does not allow **characters** or **special characters**. Width field can’t be empty.

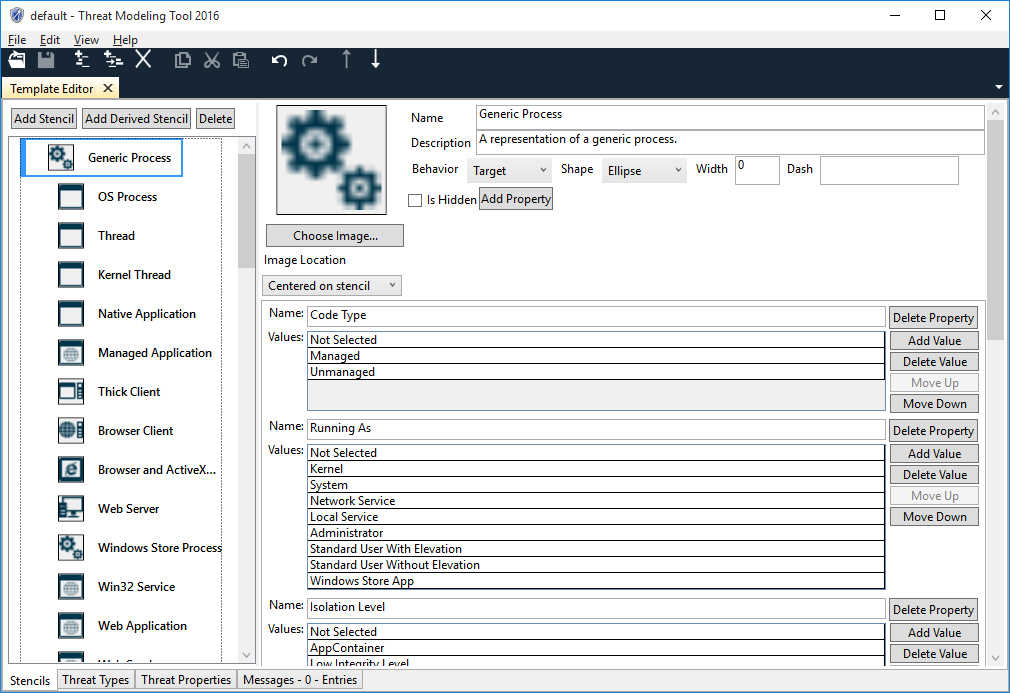
**Dash** accepts only numeric values. Default value for Dash is set blank. It does not allow **character** or special character, system will prompt a validation error message. The Dash can accept numeric values but only in certain formats as given below:

**Format of Dash field**

|  |  |
| --- | --- |
| **Value** | **Representation** |
| # | Yes |
| #.# | Yes |
| # # | Yes |
| #.# #.# | Yes |
| # #.# | Yes |
| #.# # | Yes |

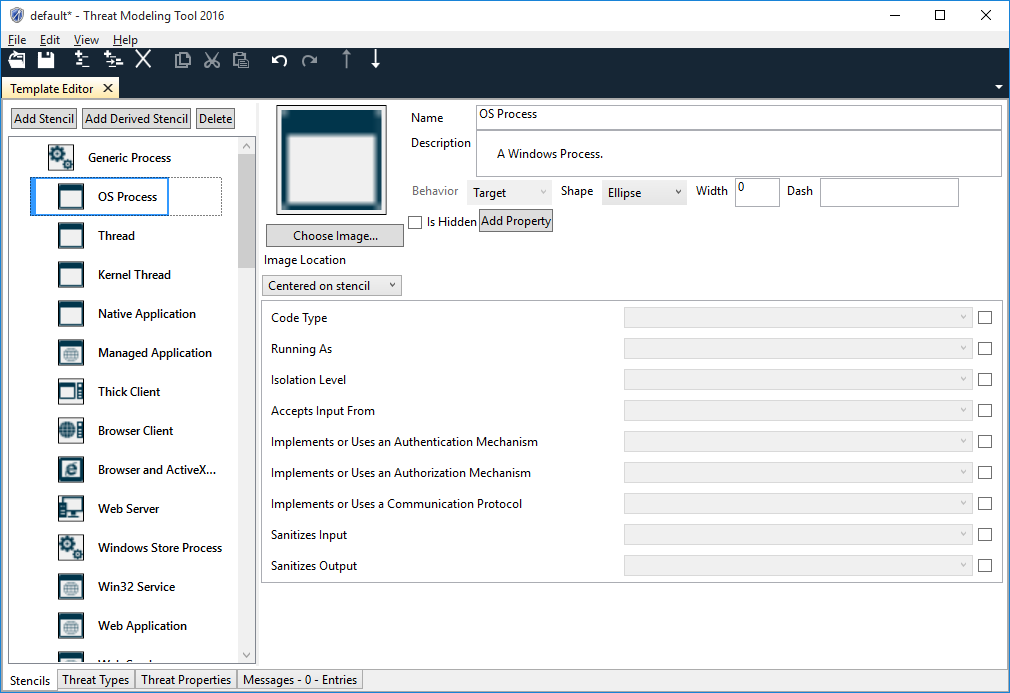
### Stencil Properties

A stencil can have multiple properties with each property able to take multiple values. The property names are unique across all the stencils and if the user does define a duplicate property name, the system will flag this in the Error Message window.

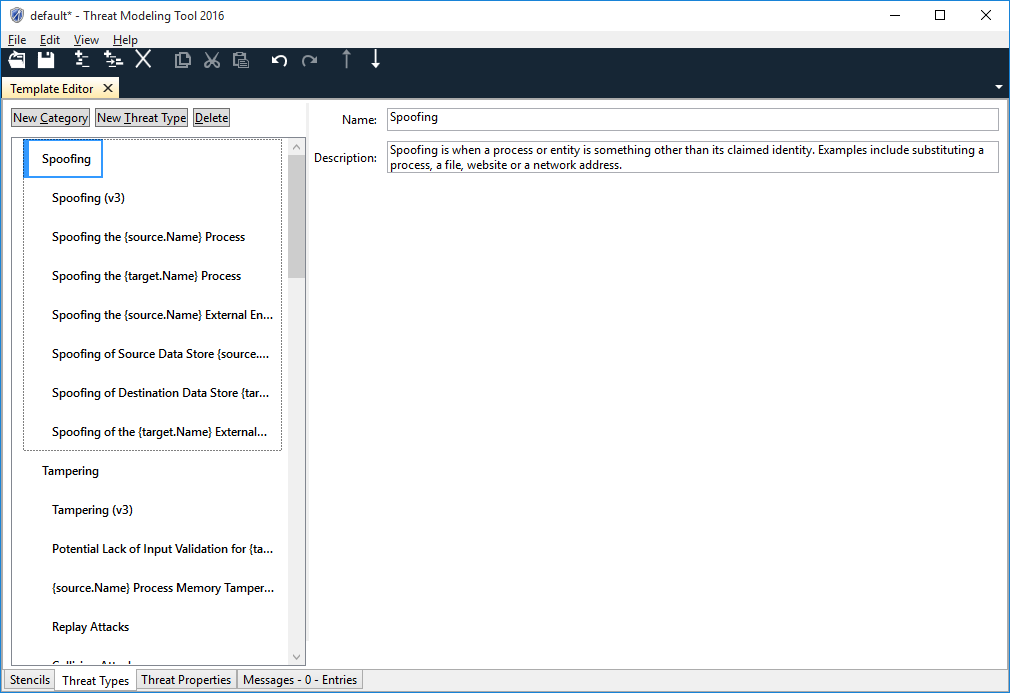


### Derived Stencils

TMT also allows creation of **Derived Stencils.** Derived stencils inherit properties of the parent. Inherited properties can also be constrained to specific values. To constrain, check the constrain box and choose a value to constrain to from the dropdown box. If an inherited property is constrained, when the stencil is created in a threat model, the value for that property will be fixed to this value. If an inherited property is not constrained, when the stencil is created in a threat model, the user may select any value for that property. See threat type generation expressions for more details about the differences between stencils and derived stencils.



### Threat Categories

Generally threat models use STRIDE to define categories of threats. However TMT facilitates creation of any category. 

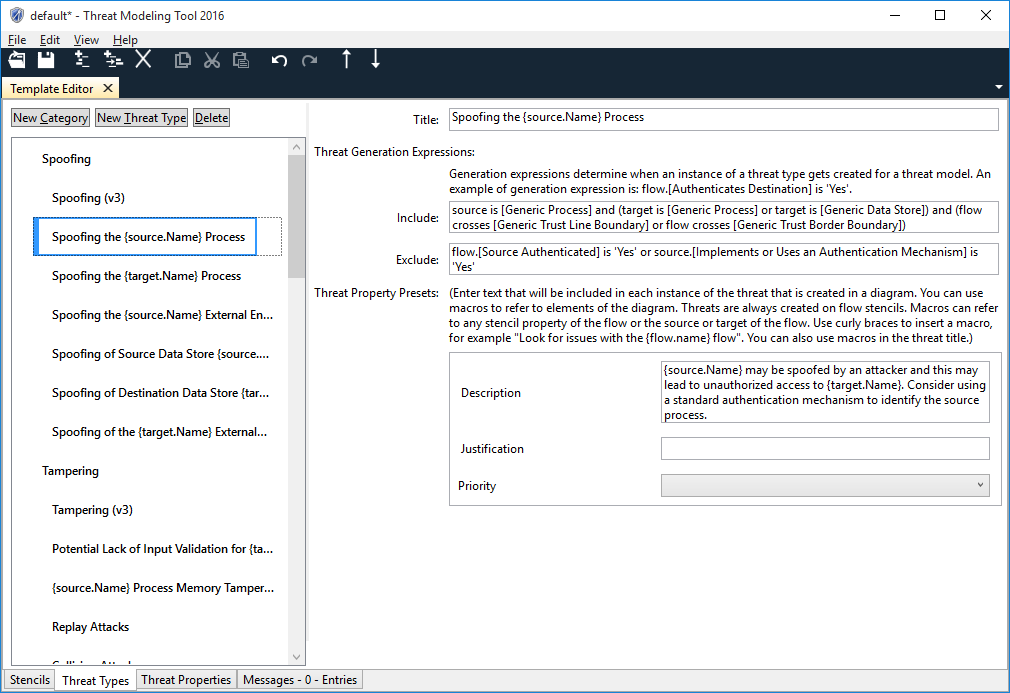
### Threat Types

Threat types are definition of threats. Categories are used to organize threats. When a user creates a DFD in the threat model editor, TMT examines the DFD and the threat types. For each flow on the DFD, TMT looks at all the threat types in the template. If the threat expression matches the flow, TMT creates an instance of the threat.

Threat types consists of Title, Include Expression, Exclude Expression and 4 reserved threat columns **Short Description**, **Description**, **Justification** and **Interaction**. These properties can be left blank if the user does not feel the need to enter any value for them. Short Description and Description are text boxes where what the threat type is all about can be described. Besides these reserved properties that get added to a threat type, new custom properties can be added if required by using the **Threat Properties** tab. Stencil properties can be referenced in these fields to make the threat more meaningful to the user.

A reference to a stencil property is called a preset. **Presets** are of the form {object.stencil property}. The curly braces identify the preset. Object can be one of three values, source, target, or flow. {source.name} will insert the name of the stencil at the source of the flow. Target references properties of the target of the flow and flow references properties of the flow.

**Note** that if presets show up as guids in a threat instance, the preset is referencing a property that does not exist for the stencil.



### Threat Expressions

Include and Exclude sections of Threat Types allow you to model the threats based on the project security requirements by allowing you to create threat expressions. All threat types must have an include expression. Include expression matches against flows in a threat model to determine when a threat instance may be created. The exclude expression determines when a threat instance may not be created. Threat instances are only created when include expression is true and the exclude expression is false or blank.

Grammar for creating the Threat Expression is given below.

<rule> ::= <expression> { <op><expression> }

<expression> ::= <object>[.<property>] IS <value>  |  Flow crosses <entity\_id> | [ NOT ]( <expression> )

<object> ::= Source | Target | Flow

<property> ::= [Stencil Property Name]

<value> ::= ‘Stencil Property Value’

<entity\_id> ::= [Stencil Name]

<op> ::= AND | OR

The following expression matches all flows where the source stencil in a data flow interaction is an instance of New Derived Stencil.

Source is [New Derived Stencil]

The following expression matches all flows where the target stencil is an instance of New Stencil. It also matches flows where the target is any derived stencils under New Stencil. The main difference between stencils and derived stencils is that threat expressions for stencils also match any derived stencil children. This lets you make threats that apply to whole categories of stencils.

Target is [New Stencil]

The following expression matches all flows where the flow crosses New Derived Stencil2. New Derived Stencil2 must be a boundary stencil.

Flow crosses [New Derived Stencil2]

The following expression matches all flows where the value of New Property Attribute is set to New Property Attribute Value.

Flow.[New Property Attribute] is ‘New Property Attribute Value’

A few valid examples of the threat expressions are shown below for reference:

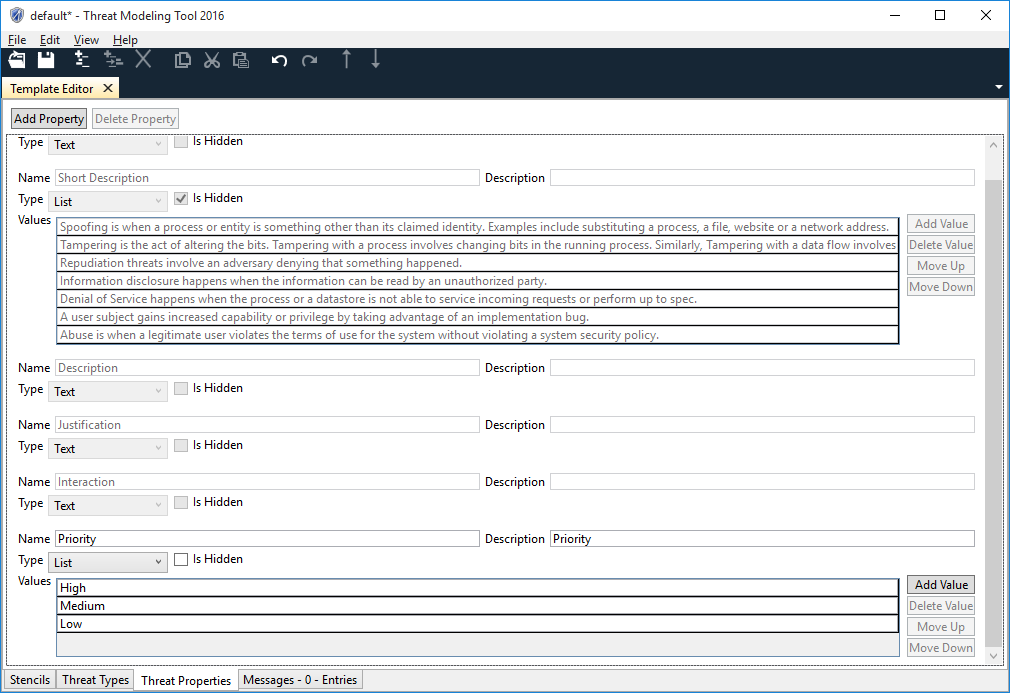
1. **Not** (**source is** [New Stencil2])
2. (**Source is** [New Stencil]) **or** (**source is**[New Stencil3]) **and** (**target is** [New Stencil]) **and** (**flow crosses** [New Stencil2]) **or** (**flow is** [New Stencil1])
3. (**Target is** [New Stencil])
4. (**Flow is** [New Stencil]) **or** (**Flow crosses** [New Stencil])

### Intellisense

Intellisense enabled for Include and Exclude expression fields provide learned behavior to facilitate expression entry and editing. This feature is context sensitive, allowing the user to be shown a more manageable list of options that depend on what has been previously entered. For example, depending on where the user is in an expression, the drop-down list shown may include objects, properties, operators, or types. Intellisense menu normally opens automatically when you edit an expression field but you have an option to press control + space button to force open it and any time.

### Threat Properties

Each threat type has a list of default properties attached to it. These properties as explained in the previous section are displayed as Threat Presets on the Threat Types tab. In addition to the default properties, TMT allows the user to define custom properties. These custom properties are created system wide and are accessible to all Threat types that a user creates. Whether a particular threat type uses a particular custom property or not depends on the requirement and definition of that threat type.



## Appendix II — Drawing Surface Keyboard Navigation and General Keyboard Shortcuts

The Threat Modeling Tool for SDL provides the ability to navigate throughout the tool and the drawing surface by using the keyboard. Keyboard shortcuts provide an accessibility option to those who are impaired, as well as anyone who wants to save time by combining key commands with mouse control.   
Since the windows and panes in Threat Modeling Tool are organized into focus scopes, the drawing surface keeps track of the currently focused element. When keyboard focus leaves a focus scope, the focused element will lose keyboard focus but will retain logical focus. When keyboard focus returns to the focus scope, the focused element will obtain keyboard focus. This allows for keyboard focus to be changed between multiple focus scopes but ensures that the focused element in the focus scope regains keyboard focus when focus returns to the focus scope.

|  |  |
| --- | --- |
| **To do this** | **Press** |
| Move from element to element on the drawing surface. A dotted rectangle indicates the shape that has the focus. The focus is moving in the order the elements were created. No change to the selection state of elements. | TAB |
| Move from element to element on the drawing surface in reverse order. | SHIFT+TAB |
| Select a currently focused element.  **NOTE**: If the focused element is already selected it retains selection. Any other previously selected elements are unselected. | ENTER |
| To select multiple elements, press the TAB key to bring focus to the first element you want to select, and then press ENTER. Press the TAB key to bring focus to another element. When the focus rectangle is over the element you want, press SHIFT+ENTER to add that shape to the selection. Repeat for each element you want to select.  NOTE: Selected element is removed from the selection group if there is more than one element in the group, otherwise the last selected element is kept selected. Focus is preserved on the same element. | SHIFT+ENTER |
| Select all elements on a diagram. | CTRL+A |
| Clear selection of or focus on an element or group. | ESC |

Table 9 Focus Navigation and Element Selection

|  |  |
| --- | --- |
| **To do this** | **Press** |
| Move a selected element or group of elements. | Arrow keys |
| Move a selection group 1 pixel at a time.  **NOTE**: SCROLL LOCK must be turned off. | SHIFT+Arrow keys |
| Delete selected element(s) | DEL |
| Copy/Cut/Paste  **NOTE**: Elements pasted onto a diagram should be selected by default. Previous selection group is cleared. | CTRL+C/X/V |
| Resize selected element(s). | ALT+Arrow keys |
| Switch focus between source anchor/middle point/target anchor of a selected line to allow movement of an individual point of the line. | CTRL+1/2/3 |
| Move the selected source anchor/middle point/target anchor of a selected line. | ALT+Arrow keys |
| Bring focus back to the selected line if in anchor manipulation mode | ESC |
| Connect/disconnect a selected dataflow anchor to/from a border anchor in proximity  **NOTE**: Focus moves immediately to another anchor of the dataflow | ENTER |

Table 10 Manipulating Selected Elements

|  |  |
| --- | --- |
| **To do this** | **Press** |
| Switch between diagrams. | CTRL+TAB |
| Scroll a diagram. | CTRL+Arrow Keys |
| Zoom in. | CTRL+PLUS |
| Zoom out. | СTRL+MINUS |
| Open file. | CTRL+O |
| Zoom in/Zoom out. | CTRL+Mouse wheel up/down |

Table 11 Other Actions

Copyright © 2015 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes