

ThreatModeler Quick Start Guide

Table of Contents

Introduction:.....	2
Prerequisites:.....	2
Starting Evaluation	3
Identifying a Web Application:.....	3
Identify Data Elements:	3
Identify Roles:.....	3
Identify Components:	3
Putting it all together:	4
Managing and Analyzing Threats:	5
References:.....	5

ThreatModeler Quick Start Guide

Introduction:

ThreatModeler™ allows users to capture the entire flow of the application, and define certain properties based on which it automatically generates threats and classifies them under various risk categories. It's simple to use navigation wizard help users to enter the required information they will need to get started with their application and create the threat profile of the application. ThreatModeler™ provides a mind mapping approach to threat modeling, allowing the user to decompose the application just like they do it on the drawing board but at the same time provide features that a drawing board cannot. User can define the communication channel (protocols) between different components; assign data elements and technical controls (like Form, URL, Cookie, Session, etc) to these components.

Once a user has completed the component diagram, ThreatModeler™ has an intelligent threat engine, (ThreatSense), which automatically identifies threats based on the information provided and automatically prioritizes the threats based on risk.

This document helps you create a threat model using ThreatModeler and evaluate how it meets your application security needs.

Prerequisites:

- Microsoft Windows:
 - XP
 - Vista (32-bit and 64-bit)
 - Windows 7 (32-bit and 64-bit)

.NET Framework 3.5 / 4.0

ThreatModeler Quick Start Guide

Starting Evaluation

Identifying a Web Application:

Identify a small to medium sized web application which typically can be designed in a week or two. Things to identify at this step include:

- URL
- Web Application Owner
- Risk Category
- Technology Framework (.NET/Java)

Identify Data Elements:

- Click Admin -> Manage Data Elements
- Review all the Data elements that are provided by ThreatModeler to make sure everything you need is available
- If you have data elements not in the list, click on Add Data Elements. You can add as many Data Elements to the list. When you add a Data Element, please specify the classification of that data for ThreatModeler to apply appropriate rules on that data.

Identify Roles:

1. Identify the various roles in your organization which may have access to the web application.
2. Below are the various roles typically associated with most applications –
 - a. Registered User,
 - b. Unregistered User,
 - c. Admin,
 - d. Maintenance. (Clarify if the maintenance is done under admin account in which case we won't need the maintenance role).
3. If a role doesn't exist in the list, you can add a new role by Click Admin -> Manage Roles for others that you would like to add.

Identify Components:

- Identify the various components that provide functionality to your application. ThreatModeler comes bundled with a list of components like Login, Logout, Registration, etc. these components represent individual feature of your application.
- If a required component does not exist, you can add a new component by
 - Select Admin -> Manage Components menu option.
 - Enter the name of the component
 - Select an icon to represent the component. You can use the default icon for now in order to do the pilot. However, ThreatModeler does provide you a feature by which you can upload an icon which represents that component more appropriately.
 - Select the Rules (Security Requirements) for that component. For reference, see Login component. If a Rule does not exist, you can go to Admin->Manage Rules and add a new rule and associate it with threats.

ThreatModeler Quick Start Guide

Putting it all together:

- To create a threat model, click on the Add button or through the menu File -> New Threat Model. The wizard guides you through a three step process to collect information about the application
 - Step 1 - Threat Model Details – Enter in the details requested
 - Step 2 - Data Elements – Select all the data elements that will be used in your application
 - Step 3 - Security Assessment Checklist – This is a comprehensive checklist to review security controls that are or should be implemented. This step can be skipped and reviewed later.
 - Finish Screen – Press the finish button. This will take you to the diagramming interface (Whiteboard).
- The Whiteboard is a simple drag-and-drop diagramming interface. The user creates a high level architecture of the application by using various components and interconnecting them by arrows which represent the communication protocol between them.
- To the left of the screen is the Component Palette. The various icons in the Palette are the components that represent a feature of an application. The user can drag a component onto the canvas from this palette
- Once several components are placed on the canvas, they can be linked to each other. Take the mouse cursor at the center of a component and it changes into a hand pointer. Click and drag the mouse to the other component.
- Right-click the interconnecting arrows to change the communication protocol. Double click a component to bring up the properties window. Property window has 5 tabs
 - Select the data elements that are used by this associated with the component in the first tab.
 - Select the roles that with permission to access or use this component. – These are security requirements associated with the component.
 - Select the Technical Control (widgets) that will be a part of this component along with the backend they will interact with. For e.g. A login page will have a Form that might interact with the database at the backend to validate the password.
 - You can also view Rules (Security Requirements) for this component in the fourth tab.
 - Fifth tab is where you can write notes for this component. Free flowing thoughts that will be stored for you to come back and read later.
 - After you are done with it, you can click on save button which will update the threats for this component. You can view those threats by clicking on View Threats button. If you don't want to view threats, you can just click on "Save and Close" button. If you click on View Threats button in the properties window, it shows up another screen with all the threats listed in tabular format for this component.
 - You can double click on any of the threats to bring up window which will display list of steps to mitigate that particular threat.

ThreatModeler Quick Start Guide

- You can double click on any of the mitigation steps to see the details for that mitigation step.
- Right click a component and select View Attack Trees to display threats for this component in a graphical representation.

Managing and Analyzing Threats:

- Once you have built the component diagram and defined properties, you can go to View->Threat Management Console. This will bring up a screen which will show you all the threats to the entire application.
- You can group them by components or by threats via Group by drop down menu at the top right corner of the screen.
- You can change the status, add or review comments to a threat through this interface.

References:

[Getting Started with ThreatModeler](#)

[Comparison between ThreatModeler and Microsoft TAM](#)

[ThreatModeler FAQ](#)

[ThreatModeler Key Features](#)

[ThreatModeler Data Sheet](#)

If you have any further questions or need any additional information feel free to contact us at sales@myappsecurity.com