[ThreatsManagerPlatform:ModelName]

Threat Model

Prepared by

[ThreatsManagerPlatform:ModelOwner]

Preparation Date

16 May 2021

Contributors

[ThreatsManagerPlatform:ModelContributors]

Table of Contents

[Introduction 3](#_Toc56252524)

[Executive Overview 4](#_Toc56252525)

[The Model 6](#_Toc56252526)

[Assumptions 6](#_Toc56252527)

[The Severities 6](#_Toc56252528)

[Diagrams 6](#_Toc56252529)

[[ThreatsManagerPlatform:ListDiagrams] 6](#_Toc56252530)

[External Interactors 6](#_Toc56252531)

[[ThreatsManagerPlatform:ListExternalInteractors] 6](#_Toc56252532)

[Processes 6](#_Toc56252533)

[[ThreatsManagerPlatform:ListProcesses] 6](#_Toc56252534)

[Data Store 6](#_Toc56252535)

[[ThreatsManagerPlatform:ListStorages] 6](#_Toc56252536)

[Flows 6](#_Toc56252537)

[[ThreatsManagerPlatform:ListFlows] 6](#_Toc56252538)

[Trust Boundaries 6](#_Toc56252539)

[[ThreatsManagerPlatform:ListTrustBoundaries] 6](#_Toc56252540)

[Threat Types 7](#_Toc56252541)

[[ThreatsManagerPlatform:ListThreatTypes] 7](#_Toc56252542)

[Mitigations 8](#_Toc56252543)

[[ThreatsManagerPlatform:ListMitigations] 8](#_Toc56252544)

[The Roadmap 9](#_Toc56252545)

# Introduction

The present document describes a security assessment performed on the design of a solution called [ThreatsManagerPlatform:ModelName], using the Threat Modeling approach.

OWASP[[1]](#footnote-1) defines Threat Models as “structured representations of all the information that affects the security of an application. In essence, [a Threat Model] is a view of the application and its environment through security glasses”[[2]](#footnote-2).

Continuing with its description, OWASP defines “Threat Modeling [as the] process for capturing, organizing, and analyzing all of this information. Threat Modeling enables informed decision-making about application security risk. In addition to producing a model, typical threat modeling efforts also produce a prioritized list of security improvements to the concept, requirements, design, or implementation”.

[ThreatsManagerPlatform:ModelDescription]

This document includes the following sections:

* The **Executive Overview**, which represents a summary view of the solution and its risks.
* **The Model**, which describes how the Solution in scope has been understood.
* The **Threat Types**, describing the identified risks.
* The **Mitigations**, which lists the activities that could address the identified risks.
* **The Roadmap**, which describes a potential plan for improving the security of the Solution.

For a non-technical view, it is recommended to focus on the **Executive Overview**. Architects, Security Experts and other technical roles may find value in the whole Report.

This document assumes a good understanding of the main characteristics of the Solution in scope.

# Executive Overview

The Threat Model describes the main risks identified for the solution in scope and what can be done to address them. The analysis has identified a total of [ThreatsManagerPlatform:CounterThreatEvents] potential issues, called Threat Events, which can be categorized under [ThreatsManagerPlatform:CounterThreatTypes] categories, called Threat Types. The following pie chart shows the distribution of the Threat Types by Severity. It is notable that the analysis has identified [ThreatsManagerPlatform:CounterCriticalThreatTypes] Critical and [ThreatsManagerPlatform:CounterHighThreatTypes] High Severity Threat Types.

[ThreatsManagerPlatform:ChartThreatTypes]

Figure - The Threat Types by Severity chart.

To address those Threat Types, the analysis has identified a total of [ThreatsManagerPlatform:CounterMitigations] Mitigations. The following pie chart shows the distribution of the Mitigations by Status.

[ThreatsManagerPlatform:ChartMitigations]

Figure - The Mitigations by Status chart.

The meaning of the potential States is:

* **Existing**, which indicates a mitigation that already exist, when the Threat Model is performed.
* **Proposed**, used to indicates new Mitigations you are proposing, as a Threat Modeler.
* **Implemented**, which is used for existing Mitigations which have been introduced as a consequence of your Threat Model.
* **Approved**, to indicate a Mitigation that is known (for example it is tracked in the Backlog), but it has not been planned, yet.
* **Planned** is to be used for Mitigations that are known and have been planned for implementation.

The Threat Types identified during the Threat Modeling exercise do not necessarily correspond to vulnerabilities which will necessarily be exploited by attackers. This means that the Threat Model and this report do not describe a prescriptive set of activities that must be necessarily done, but a guidance to understand the risk represented by the analyzed solution and a starting point to decide how to address it. Thus, the recommended approach is to start a conversation to define what to do for each Threat Type. In fact, the main Stakeholders of this initiative have various options:

* Simply accept the risk, track it and do not implement any action.
* Select one or more Mitigations, picking from the proposed list or identifying additional options not included in this document, to mitigate the risk.
* Avoid the risk, by completely removing the functionality that is causing it.
* Transfer the risk to someone else, for example by getting an Insurance.

Ultimately, it is important to understand that the goal of Security is not to nullify the Risk, but to make it acceptable.

# The Model

The present Chapter represents the understanding related to the analyzed Solution, through a representative diagram.

## Assumptions

Assumptions are used to indicate conditions or information that you are using as part of the Threat Model. They are particularly important, because the Threat Model relies on them to be true. In other words, if they are false, then the Threat Model would be in whole or in part be false.

The Threat Model has been created under the following Assumptions.

[ThreatsManagerPlatform:ModelAssumptions]

## The Severities

Threat Type and Events have been assigned different Severities, to represent their importance, in accordance with the following table.

[ThreatsManagerPlatform:TableSeverities]

Table - The definition of the various Severity levels.

## Diagrams

The analysis has produced the following diagrams, representative of the Solution in scope.

### [ThreatsManagerPlatform:ListDiagrams]

## External Interactors

The External Interactors identified by the analysis are represented here.

### [ThreatsManagerPlatform:ListExternalInteractors]

## Processes

The Processes identified by the analysis are represented here.

### [ThreatsManagerPlatform:ListProcesses]

## Data Store

The Data Stores identified by the analysis are represented here.

### [ThreatsManagerPlatform:ListStorages]

## Flows

The Flows identified by the analysis are represented here.

### [ThreatsManagerPlatform:ListFlows]

## Trust Boundaries

The Trust Boundary identified by the analysis are represented here.

### [ThreatsManagerPlatform:ListTrustBoundaries]

# Threat Types

This section represents the various issues identified as part of the Threat Modeling analysis.

For each Threat Type, you have represented here various details, including:

* The **Name** of the Threat Type, as title.
* The **Severity** of the finding, calculated as maximum of the related Threat Events. The meaning of the various levels is described in the table below.

[ThreatsManagerPlatform:TableSeverities]

Table 2 - Definition of the Severities.

* The **Description** of the Threat Type.
* The list of **Affected Objects**, which are the Entities, Flows or the Threat Model itself. For each of them, the related type is expressed through the short form[[3]](#footnote-3) as a prefix between square brackets, and the related severity for the associated Threat Event.
* A list of **Mitigations** split by Status. This list is expressed by a table
	+ The **Object** to which the mitigation applies.
	+ The Name of the **Mitigation**.
	+ The specific **Severity** for the object.
	+ The **Strength** of the Mitigation, in accordance with the following table.[[4]](#footnote-4)

[ThreatsManagerPlatform:TableStrengths]

Table 3 - Definition of possible Strengths for the Mitigations.

Threat Types are sorted by Severity.

## [ThreatsManagerPlatform:ListThreatTypes]

# Mitigations

This section describes the possible actions identified as already included as part of the Solution, or that have been proposed as additional activities as possible improvements.

For each Mitigation, you have represented here various details, including:

* The **Name** of the Mitigation, as title.
* The **Control Type** for the Mitigation, as defined by the following table.

[ThreatsManagerPlatform:TableControlTypes]

Table 4 - Definition of the Control Types adopted by the document.

* A **Description** of the Mitigation.
* The list of **Affected Findings**, that contains the list of the Threat Events associated to the Mitigation, described with a table including the following information:
	+ The associated **Object** to which the specific Threat Event refers.
	+ The **Threat Type** associated to the Threat Event.
	+ The **Strength** of the Mitigation, in accordance with the following table.[[5]](#footnote-5)

[ThreatsManagerPlatform:TableStrengths]

Table 5 - Definition of possible Strengths for the Mitigations.

* The **Status** of the Mitigation, in accordance with the following table.

[ThreatsManagerPlatform:TableMitigationStatus]

Table 6 - Definition of the Status of the Mitigation.

* The **Directives**, which contain information related on how the mitigation should be applied to specific scenarios.

Mitigations are sorted alphabetically.

## [ThreatsManagerPlatform:ListMitigations]

# The Roadmap

The Threat Model has split the recommended Mitigations to be implemented in three phases:

* Short Term, which represent activities that could be done immediately.
* Mid Term, which represent activities that could be done at a later stage.
* Long Term, which includes activities that are more complex or less urgent than the previous categories, and for this reason may be implemented even later.

This list should not be considered as a prescriptive guidance, but just as a starting point.

Based on this list, it is possible to evaluate the effect of each phase on the Residual Risk. The following chart represents this evaluation.

[ThreatsManagerPlatform:ChartRoadmap]

Figure - The effects of the Roadmap on the Residual Risk.

The previous chart applies different colors to the bars depending on the fact that the Residual Risk may be considered acceptable or not. This is achieved considering an Acceptable Risk corresponding to 0 Critical or High Severity, 10 Medium Severity, 20 Low Severity and 20 Information level Threat Events.

The following table describes the Roadmap by listing the Mitigations selected for each phase.

[ThreatsManagerPlatform:TableRoadmap]

1. OWASP is a not-profit organization and “open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted”. It has been founded in the United States in December 2001 and has rapidly asserted itself as one of the most important players in the Application Security field. [↑](#footnote-ref-1)
2. Ssee.: <https://www.owasp.org/index.php/Threat_modeling>. [↑](#footnote-ref-2)
3. Please refer to <https://threatsmanager.com/training/intro/basic/short-form/> for a description of the various values. [↑](#footnote-ref-3)
4. The Mitigation Strength is relative to the Threat: in other words, the same Mitigation may have different strengths for different Threats. [↑](#footnote-ref-4)
5. The Mitigation Strength is relative to the Threat: in other words, the same Mitigation may have different strengths for different Threats. [↑](#footnote-ref-5)