

Threat Modeling Template

Threat modeling is a risk assessment approach for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects it. Threat modeling helps identify relevant threats to a particular application scenario, key vulnerabilities in an application's design, and improve security design.

Details of the Application

Organization Name:	
Application Name:	
Application Type:	
Developer's Lead Contact:	
<i>Additional App Details:</i> 	

Details of the Incident Handler/Administrator

Name:			
Title:			
Contact Number:			
Email Address:		Reporting Manager:	
Department:		Case Number:	
<i>Additional Details (If any):</i>	 		

Identifying Security Objectives

[To identify security objectives, administrators should ask the following questions:]

1. What data should be protected?

[List out the data that needs protection]

2. Are there any compliance requirements?

[YES or NO; give reasons]

3. Are there specific quality-of-service requirements?

[Provide details of the required QoS]

4. Are there intangible assets to protect?

[List out the intangible assets that need protection]

Application Overview - I

Identify the components, data flows, and trust boundaries. First, the administrator should draw a rough diagram that explains the workings and structure of the application, its subsystems, and its deployment characteristics. Add a copy of the deployment diagram in the below space and ensure that the diagram should contain the following:

Deployment Diagram Components	
<input type="checkbox"/>	<i>End-to-end deployment topology</i>
<input type="checkbox"/>	<i>Logical layers</i>
<input type="checkbox"/>	<i>Key components</i>
<input type="checkbox"/>	<i>Key services</i>
<input type="checkbox"/>	<i>Communication ports and protocols</i>
<input type="checkbox"/>	<i>Identities</i>
<input type="checkbox"/>	<i>External dependencies</i>

[Space for deployment diagram]

Application Overview- II

Role	Name	Actions Performed	App Use Cases	Technology Used	Security Mechanism

Decomposing the Application

The administrator needs to break down the application to identify the trust boundaries, data flows, entry points, and exit points.

Outer System Boundaries	Access Control Points	Data Flow Entry	Data Flow Exit	Reviewed By

Identifying Threats and Vulnerabilities

Questions that Need to be Answered	
1. Will the threat affect the application?	
2. What is the source of the threat?	
3. What will be the impact of this threat?	
4. How severe is this threat?	
5. Is there any backup for the application?	
6. Do we have any response plan handy for this?	
7. Who is the potential target of this threat?	
8. Is there any adversary identified? If yes, provide details.	
<i>Additional Information:</i>	

Sr. No.	Application-Level Vulnerability	Vulnerability Details	Business Impact Rating	Potential Impact	Recommendations