TRIANZ℠

Threat Modelling procedure

TRIANZ INTERNAL

trianz.com

Statement of Confidentiality

The information contained in this document is internal to Trianz. It shall not be disclosed, duplicated, or used for any purpose other than that stated herein, in whole or in part, without the express written consent of Trianz.

Information Classification

☐	Public
☒	Internal
☐	Confidential
☐	Restricted

Table of Contents

Glossary

Word/Abbreviation	Description
Risk	the effect of uncertainty on objectives
SDL	Secure Development Life cycle
SDLC	Software Development Life Cycle
Threat	A potential cause of an unwanted incident that may result in harm to a system or organization
Vulnerability	An instance of a weakness as manifested in a specific implementation
Attack	An attempt to damage or gain access to the system
DFD	Data Flow Diagrams

1. Introduction

Threat modeling is an approach for analyzing the security of an application. It is a structured approach that enables you to identify, quantify, and address the security risks associated with an application. The inclusion of threat modeling in the SDLC can help to ensure that applications are being developed with security built-in from the very beginning.

Threat modeling must align with an organization's development practices and follow design changes in iterations that are each scoped to manageable portions of the system.

2. Objective(s)

Threat Modeling objectives are:

1. Defines security of application.
2. Identifies and investigates potential threats and vulnerabilities.
3. Results in finding architecture bugs earlier.
4. Accurately determine the attack surface for the application
5. Assign risk to the various threats.
6. Drive the vulnerability mitigation process.

3. Scope

The scope includes all internal and applicable vendor applications that are owned, operated, maintained, and controlled by Trianz by internally and externally either on premises or on cloud.

4. Threat Modeling Process

Threat modeling is the systematic and strategic approach for identifying and enumerating threats to an application environment with the objective of minimizing risk and the associated impacts.

It is applied continuously throughout a software development lifecycle. The process identifies and prioritize potential threats, then document both the harmful events and what actions to take to resolve them.

Use the Policies & standards, Legal/Compliance directives & business requirements to list the security objectives.

4.1 Identify Asset:

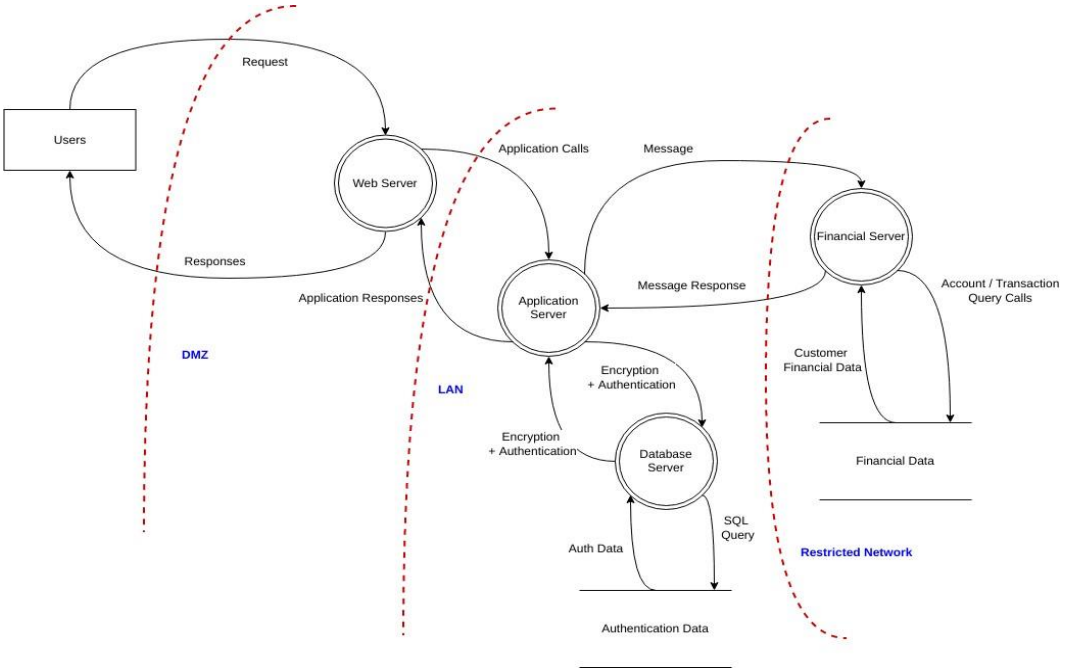
- The first step of threat modeling is to understand how it interacts with internal and external entities.
- Identify entry points, privilege boundaries, access control matrix, data flow, privileged code and technology stacks being used document the security profile.

4.2 Application Overview:

- Threat modeling process is concerned with gaining and understanding of the application and how it interacts with external entities.
- To create an application overview:
- Draw the end-to-end deployment scenario.
- Identify roles.
- Identify key usage scenarios.
- Identify technologies.
- Identify application security mechanisms.
- Ensure creating use-cases to understand how the application is used, identifying entry points to see where a potential attacker could interact with the application. Use and abuse cases can illustrate how existing protective measures could be bypassed, or where a lack of such protection exists.

4.3 Dissect the Application:

- In this step, break down the application to identify trust boundaries, data flows, entry points, and exit points.
- Ensure producing DFDs & Architectural diagrams for the application. A data flow diagram is a depiction of how information flows through your system. It shows each place that data is input into or output from each process or subsystem. It includes anywhere that data is stored in the system, either temporarily or long-term.
- The DFDs show the different paths through the system, highlighting the privilege boundaries. A trust boundary is a location on the data flow diagram where data changes its level of trust. Any place where data is passed between two processes is typically a trust boundary.
- DFDs helps to identify the potential threat targets from the attacker's perspective, such as data sources, processes, data flows, and interactions with users.



4.4 Identify and rank threats.

- Threat analysis identifies the threats to the application and involves the analysis of each aspect of the application functionality and architecture and design to identify and classify potential weaknesses that could lead to an exploit.
- A threat methodology (STRIDE) can be used to define threat categories such as Auditing &
- Logging, Authentication, Authorization, Configuration Management, Data Protection in Storage and Transit, Data Validation, Exception Management. STRIDE helps to identify threats from the attacker.
- The determination of the security risk for each threat can be determined using a value-based risk model such as DREAD.

4.4.1 STRIDE

- The STRIDE threat model is focused on the potential impacts of different threats to a system:
    1. Spoofing
    2. Tampering
    3. Repudiation
    4. Information Disclosure
    5. Denial of Service
    6. Elevation of Privilege.

STRIDE Type	Description	Security Control

Spoofing	An adversary posing as another user, component, or other system that has an identity in the system being modelled. Threat action aimed to illegally access and use another user's credentials, such as username and password	Authentication
Tampering	Threat action aimed to maliciously change/modify persistent data, such as persistent data in a database, and the alteration of data in transit between two computers over an open network, such as the Internet	Integrity
Repudiation	Threat action aimed to perform illegal operation in a system that lacks the ability to trace the prohibited operations.	Non-Repudiation
Information Disclosure	The exposure of protected data to a user that is not otherwise allowed access to that data.	Confidentiality
Denial of Service	Occurs when an adversary uses illegitimate means to assume a trust level than he currently has with different privileges.	Availability
Elevation of Privilege	Threat aimed to gain privileged access to resources for gaining unauthorized access to information or to compromise a system	Authorization

4.4.2 DREAD

- DREAD methodology is used to rate, compare and prioritize the severity of risk presented by each threat that is classified using STRIDE. Threats can be ranked from the perspective of risk factors.
- we rate threats in light of the risks they cast. This leads us to address the threats that are most problematic, and afterwards resolve alternate threats.
- The DREAD model is a form of quantitative risk analysis that involves rating the severity of a cyber threat (DREAD model is used to determine how much damage it has already caused and can cause in the future).

- You must assess various key points of the cyber threat while assigning a numbered rating to each of these points. When finished, you can then compare the total rating to that of the DREAD model's rating system, which should reveal whether the cyber threat has a low, medium or high risk to your business.
- When using the DREAD model to assess the severity of a cyber threat, must scrutinize five key points.
- Ensure assigning a rating of either one, three or nine. A rating of one indicates a low risk. A rating of three indicating a moderate risk. A rating of nine indicates a high risk
- The DREAD model is utilized to figure out the probability of risk, which is abbreviated as:

    1. Damage
    2. Reproducibility
    3. Exploitability
    4. Affected Users
    5. Discoverability

- Following tables will be used to assign the Damage, Reproducibility, Exploitability, Affected Users, Discoverability rating.

Value	**Damage** **(If a threat exploit occurs, how much damage will be caused)**
1	Nothing / Leaking trivial information.
3	Individual or Administrative sensitive user data compromised
9	Complete system or data destruction

Value	**Reproducibility** (How easy is it to reproduce the threat exploit)
1	The attack is very difficult to reproduce, even for administrators of the application or with knowledge of the security hole / Very hard or impossible even for administrators/DBAs.
3	One or two steps required, may need an authorized user
9	Just a web browser and the address bar are sufficient, without authentication.

Value	**Exploitability** (What is needed to exploit this threat)
1	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
3	Malware exists on the Internet, or an exploit is easily performed, using available attack tools.
9	Just a web browser is enough

Value	**Affected Users** (How many users will be affected)
1	Very small percentage of users, obscure feature; affects anonymous users
3	Some users, non-default configuration
9	All users

Value	Discoverability How easy it is to discover this threat
1	Very hard, requires source code or administrative access
3	Can figure it out by querying or by analyzing the application data flow
9	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.

- Prioritizing the threat in the following way to analyze the risk factor from first to last:
    - First High Risk.
    - Second Medium Risk.
    - Last Low Risk.

- **DREAD = (Damage * Reproducibility * Exploitability * Affected Users * Discoverability)**

DREAD	Basis
Low	Value of DREAD Risk<81
Medium	Value of DREAD Risk within the range from > =81 to <=243
High	Value of DREAD Risk >243

- Risk assessment is performed after the threat modeling process in order to map each threat to either a mitigation mechanism or to ignore.
- Risk assessment will be performed if DREAD Risk value is Medium or High (DREAD value is greater than (>) 81)
- If DREAD value is greater than (>) 81 then Identify Vulnerabilities, Impact and probability of occurrence of vulnerabilities.

  Refer to Risk and Opportunity Management Policy for risk assessment.

4.5 Identify Vulnerabilities:

- Identify vulnerabilities by examine the application layer by layer, considering each of the vulnerability categories in each layer.
- Ensure identifying OWASP TOP 10 Vulnerabilities (Authentication, Authorization, Input and data

Validation, Configuration Management, Sensitive Data, Parameter Manipulation, Session Management, Cryptography, Exception Management, Auditing and Logging)

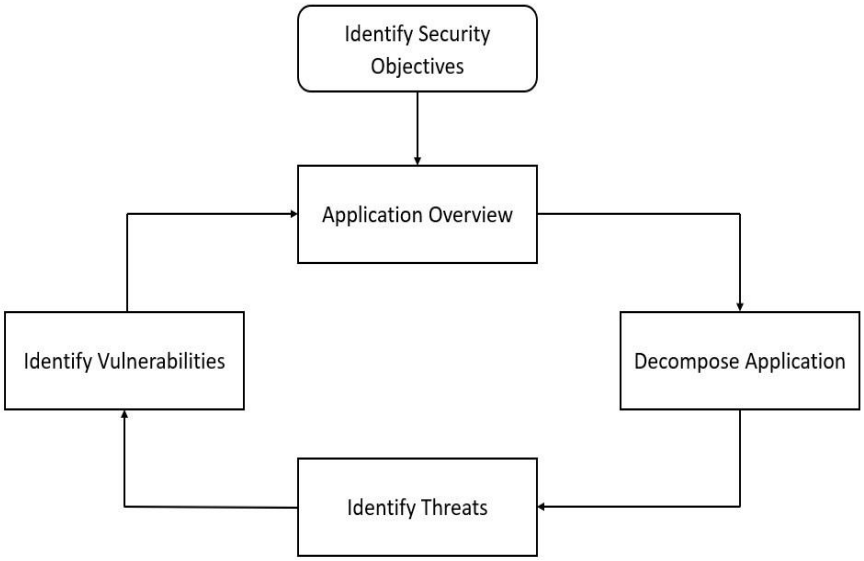
4.6 Conclusion:

- Threat modeling should be incorporated into every stage of the Secure SLDC to ensure that threats are identified and managed from the initial design of software through the final release.

5. Roles and Responsibilities

Role	Responsibility	Internal/External
Internal App Team	• Identify security objectives and create data flow diagram and architectural diagram	Internal
IS Team	• Identify threats and Vulnerabilities to the application and the rank the threats	Internal

6. Process Flow



7. Prerequisites

7.1 Reference Policy, Process, Procedure, Templates, Checklist

Document Name
Secure SDLC Procedure
Risk and Opportunity Management Procedure

8. Standards Addressed

ISO 9001:2015 Standard
ISO 27001:2022 Standard
ISO 20000-1:2018 Standard

9. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Technological Control	8.27 Secure system architecture and engineering principles Control Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	Threat Modeling Procedure

Document Control

Owner:	CISO	**Release ID:**	THRT_MOD_PROC_0163

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.00	30-July-21	Divya G	Karthik N	Phani	Initial Version	None
1.00	30-July-21	Divya G	Karthik N	Phani	Request for Baseline	Baselined
1.00	05July2022	Sanjana	Divya	Siva N	For review	No changes
1.1	25-April-2023	Krutideepta, Rama Madhavan	Vijaya R		For Review	Reviewed with no changes. Migrated to new template
2.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For Approval	Approved and Baselined
2.1	11-Feb-24	Shalini	Vijaya	Srikanth M	For Review	Mapped to new ISO 27k 2022 Control
3.0	23-Feb-24	Shalini	Vijaya	Srikanth M	For Approval	Approved and Baselined

3.1	28-May-25	Kruti	Vijaya		For Review	Migrated to New Template
4.0	29-May-25	Kruti	Vijaya	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com