Threat model report for XXXX

Replace XXXX above with the name of the production / solution for which the threat model report is being prepared.

Version:	0.2
Status:	Draft
Date:	Feb-2023
Contact:	
E-Mail:	

1 **Introduction** 4

This document describes the process and outputs of threat modelling on XXX product/solution. 4

Assumptions 4

Definitions 4

Related Reference Documents 4

2 **Product / solution architecture** 4

3 **Assets** 4

4 **Communication matrix** 4

4.1.1 Service Asset 1 4

4.1.2 Service Asset 2 5

4.1.3 Data asset 1 5

4.1.4 Data asset 2 5

5 **Data flow Diagram** 5

6 **Security Threats identified** 5

7 **Risk analysis / threat mitigation** 5

8 **Consolidated list of Security controls** 6

Document Control

Document Version History

This table shows a record of significant changes to the document.

Version	Date	Author and Email	Description of Change
0.1	31-Jan-2023	Author name (xyz@example.com)	xxxx

Approvals

This table shows the approvals on this document for circulation, use and withdrawal.

Version	Date	Approver	Title/Authority	Approval Remarks
0.1	DD-MMM-YYYY			

Acronyms

STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service and Elevation of Privilege

1 Introduction

This document describes the process and outputs of threat modelling on XXX product/solution.

Assumptions

Provide assumptions made about the product interfaces, deployment, etc…

Definitions

Provide definitions of the terms used in the product context.

Related Reference Documents

Provide reference documents used to perform this threat modelling, risk analysis.

No.	Document Title	Document URL (If Any)

2 Product / solution architecture

Provide brief introduction of products, such as key features and main user scenarios. Provide high-level architecture information detailing the interfaces, sensitive data handling aspects, security functions, security features, existing security controls.

3 Assets

Identify the assets (microservices / data) that are considered for threat modelling in this document.

4 Communication matrix

Provide communication matrix information for the assets including the protocols used, protections planned for the interfaces / data.

If the details are not known yet, but it is in the roadmap, please indicate so.

4.1.1 Service Asset 1

Add a brief description of the service, a sample is provided below. The interface type can be “Public”, “External” or “Internal”. “Public” means the interface is exposed to internet. “External” means the interface is to an entity outside the system being modelled. “Internal” means the interface is from one component of the system being modelled to the other.

Interface name	Interface type	protocols	Ports	Comments

Web interface	Public	HTTPS	443	CA certificates are used

4.1.2 Service Asset 2

Add a brief description of the service and replicate the table above in “service asset 1” to fill relevant details

4.1.3 Data asset 1

Add a brief description of the data, a sample is provided below.

Data	Protected in transit	Protected at rest	Authorization details for data handling	Comments
TLS private key	N/A	Stored in Vault	Vault Kubernetes auth mode	Keys are not transmitted outside the module

4.1.4 Data asset 2

Add a brief description of the data and replicate the table above in “data asset 1” to fill relevant details

5 Data flow Diagram

Attach the generated product/solution DFD using OWASP Threat Dragon here.

6 Security Threats identified

List the identified threats using threat dragon tool. A sample table is provided below.

#	Threat description	Threat category	Impacted assets	Comments
1	Lack of MFA mechanism	Spoofing	Database	Critical data is accessible if the password is compromised.
2	xxxx	xxxx	xxxx	xxxx

7 Risk analysis / threat mitigation

Identify the risk for each threat and map the security control to the threat for mitigation. The risk can be identified based on the impact / likelihood of the threat exploitation to the product /

solution. Once the controls are applied to the threat, the risk will reduce and the residual risk has to be mentioned in the table.

Residual risk is defined as the risk level after mitigation or applying counter measures using defined security controls.

Following Mnemonics can be used to describe the risks

- "L" for low risk
- "M" for medium risk
- "H" for high risk
- "N" for no risk

A sample table is provided below.

#	Threat Description	Threat Category	Impacted assets	Mitigations	Existing Security Controls	Proposed Security Controls	Risk	Residual risk	Comments
1	Privileged containers	Elevation of Privilege	An escape attack can be mounted on a privileged container to gain access to host resources	Isolate the container using a namespace to provide runtime restrictions in case of a breach	None	Namespaces	M	L	
2	xxxx	Information disclosure	xxxx	xxxx	xxxx	xxxx	H	M	xxxx

8 Consolidated list of Security controls

Provide a list of identified security controls that can be used as counter measures for threat mitigation. Mention existing and planned/future security controls.

Sample table provided below.

Security Control	Existing/Planned/Future	Purpose
No security	N/A	Protection not needed for component xyz
Namespace	Future	To provide isolation
Network policies / Firewall	Planned	To provide access control
xxxx	xxx	xxxx

Appendix A

Embed the JSON file created from OWASP threat dragon tool here