

Project: Threat Modeling

Project Title

Threat Modeling Using STRIDE with OWASP Threat Dragon & Microsoft Threat Modeling Tool

1. Introduction

What is Threat Modeling?

Threat Modeling is a **structured approach to identifying, analyzing, and mitigating security threats** early in the system design lifecycle.

Why Threat Modeling Matters

- Finds security issues **before deployment**
- Reduces cost of fixing vulnerabilities
- Improves system architecture security
- Required by **NIST, ISO 27001, SOC 2, PCI DSS**

2. Threat Modeling Lifecycle (STEP Methodology)

STEP Phases Used in This Project

1. **DFD (Data Flow Diagram)**
2. **Identify Threats**
3. **Mitigate Threats**
4. **Validation & Review**

3. STEP 1 – DFD (Data Flow Diagram)

Definition

A **DFD visualizes how data moves** through a system and identifies trust boundaries.

DFD Components

- **External Entities** (Users, APIs)
- **Processes** (Application logic)
- **Data Stores** (Databases)
- **Data Flows** (HTTP, SQL, API calls)
- **Trust Boundaries** (Internet vs Internal Network)

What to Look Out For

- Unencrypted data flows
- Direct database access
- Missing authentication boundaries
- Excessive privileges between components

DFD created in OWASP Threat Dragon / Microsoft Tool

4. STEP 2 – STRIDE Threat Identification

STRIDE Model Overview

Category	Description
S – Spoofing	Impersonating identities
T – Tampering (Integrity)	Unauthorized data modification
R – Repudiation	Denying actions
I – Information Disclosure	Data leakage
D – Denial of Service (Availability)	Service disruption
E – Elevation of Privilege	Gaining higher access
Evasion	Avoiding detection & controls

5. STRIDE Threat Analysis (Detailed)

5.1 Spoofing

Threat: Fake user identities

Indicators:

- Weak authentication
- No MFA
- Hardcoded credentials

Mitigations:

- MFA
- OAuth 2.0
- Certificate-based auth

The screenshot shows the Threat Dragon v2.5.0 application interface. A 'New Threat #5' dialog box is open, allowing the user to define a new threat. The background shows a partial view of a threat model diagram with components like 'Process', 'Store', 'Actor', 'Data Flow', 'Boundaries', 'Trust Boundary', and 'Metadata'. The 'Properties' panel at the bottom shows a 'BAD ACTOR' entity.

New Threat #5

Title: SPOOFING THREAT

Type: Spoofing

Status: ☐ N/A ☐ Open ☐ Mitigated

Score:

Severity: ☐ TBD ☐ Low ☐ Medium ☐ High ☐ Critical

Description:

The act of disguising a communication from an unknown source as being from a known, trusted source.
Impersonate legitimate users, phone numbers or systems, or devices.
Impersonates a trusted source to deceive users, steal data, or gain unauthorized access.

Mitigations:

- Intrusion detection system
- Certificate-based authentication
- Multi-factor authentication
- email authentication
- Implementing strong password policies

Previous Next Cancel Apply

+ New Threat by Type + New Threat by Context

5.2 Tampering (Integrity)

Threat: Modifying requests, data, configs

Indicators:

- No input validation
- Unsigned tokens
- No checksums

Mitigations:

- HMAC
- Digital signatures
- Input validation

Threat Dragon v2.5.0 English

New Threat #14

Title: TAMPERING THREAT

Type: Tampering

Status: N/A Open Mitigated

Score:

Severity: TBD Low Medium High Critical

Description: Authentication data is modified.
• Password reset token manipulation
• Cookie modification
• JWT token alteration
• Man-in-the-middle attacks

Mitigations: • Encryption (TLS/SSL)
• Token signing
• Integrity checks
• Secure session management

Previous Next Cancel Apply

Process

Store

Actor

Data Flow

Trust Boundary

Properties

Name: AUTHENTICATION-PROCESS

Description:

UNAUTHENTICATED

AUTHENTICATED

BAD AUTHENTICATION

STRIDE

5.3 Repudiation

Threat: Users deny actions

Indicators:

- Missing logs
- No timestamps
- Logs not protected

Mitigations:

- Centralized logging
- Immutable logs
- Time synchronization (NTP)

Threat Dragon v2.5.0 English

Edit Threat #2

Title: REDUDIATION THREAT

Type: Repudiation

Status: N/A Open Mitigated Score: Severity: TBD Low Medium High Critical

Description: Permitting malicious manipulation or forging the identification of new actions. user signature

Mitigations: Establish a strong PKI framework.
Utilize digital signatures.
Implement time-stamp services
educate and train the team
Enforce strong authentication measures

Delete Cancel Apply

Process
Store
Actor
Data Flow
Boundaries
Trust Boundary
Metadata
Properties
Name: UNAUTHENTICATED USER Description: Reason for out of scope: Out of Scope

UNAUTHENTICATED USER
AUTHENTICATED USER
BAD A
Spoofing STRIDE
Repudiation STRIDE

5.4 Information Disclosure

Threat: Sensitive data leaks

Indicators:

- Plaintext storage
- Open S3 buckets
- Verbose error messages

Mitigations:

- Encryption at rest & transit
- Least privilege
- Secure error handling

The screenshot displays the Threat Dragon v2.5.0 application interface. The main window shows a threat model diagram with various components: a 'Process' circle, a 'Store' rectangle, an 'Actor' rectangle, a 'Data Flow' arrow, a 'Trust Boundary' dashed line, and 'Boundaries' and 'Metadata' sections. The 'Edit Threat #11' dialog box is open, showing the following details:

- Title:** INFORMATION DISCLOSURE
- Type:** Information disclosure
- Status:** N/A, Open, Mitigated (selected)
- Score:** (empty field)
- Severity:** TBD, Low, Medium, High, Critical (selected)
- Description:** Confidential server data leaked (user records, business data)
- Mitigations:**
 - Strong encryption protocols
 - Proper access controls
 - Minimize data exposure
 - Use secure headers

At the bottom of the dialog, there are buttons for 'Delete', 'Cancel', and 'Apply'. The background diagram also includes labels for 'UNAUTHENTICATED', 'AUTHENTICATED', and 'BAD Actor'.

5.5 Denial of Service (Availability)

Threat: Resource exhaustion

Indicators:

- No rate limiting
- No WAF
- Single points of failure

Mitigations:

- Rate limiting
- Auto-scaling
- Load balancers

The screenshot displays the Threat Dragon v2.5.0 application interface. A 'New Threat #48' dialog box is open, allowing the user to define a new threat. The dialog includes the following fields and options:

- Title:** DENIAL OF SERVICE THREAT
- Type:** Denial of service
- Status:** N/A, Open, Mitigated (radio buttons)
- Score:** (empty input field)
- Severity:** TBD, Low, Medium, High, Critical (radio buttons)
- Description:** The authentication system becomes unavailable
 - Login page flooding
 - Account lockout attacks
- Mitigations:**
 - Rate limiting
 - Account lockout policies
 - CAPTCHA
 - Load balancing

At the bottom of the dialog are 'Previous', 'Next', 'Cancel', and 'Apply' buttons. The background shows a threat model diagram with components like Process, Store, Actor, Data Flow, Boundaries, Metadata, and Properties.

5.6 Elevation of Privilege

Threat: User gains admin access

Indicators:

- Over-permissioned roles
- Missing RBAC
- Shared admin accounts

Mitigations:

- RBAC
- Privileged Access Management
- Just-in-Time access

The screenshot displays the Threat Dragon v2.5.0 interface. In the background, a threat model diagram is visible with components like 'Process', 'Store', 'Actor', 'Data Flow', 'Boundaries', 'Trust Boundary', 'Metadata', and 'Properties'. The 'Name' field in the Properties section is set to 'AUTHENTICATION-PROCESS'. Overlaid on this is a 'New Threat #18' dialog box. The dialog has a red header and contains the following fields:

- Title:** ELEVATION OF PRIVILEGE THREAT
- Type:** Elevation of privilege
- Status:** N/A, Open, Mitigated (N/A is selected)
- Score:** (Empty text box)
- Severity:** TBD, Low, Medium, High, Critical (TBD is selected)
- Description:** Attackers gain higher access levels
Exploiting auth bugs
• Token privilege escalation
• Role manipulation
• Admin impersonation
- Mitigations:** • Principle of least privilege
• Role-based access control
• Token validation
• Privilege separation

At the bottom of the dialog are buttons for 'Previous', 'Next', 'Cancel', and 'Apply'.

5.7 Evasion

Threat: Bypassing detection

Indicators:

- Disabled alerts
- Weak SIEM rules
- No behavioral detection

Mitigations:

- SIEM tuning
- UEBA
- Defense in depth

6. Tools Used

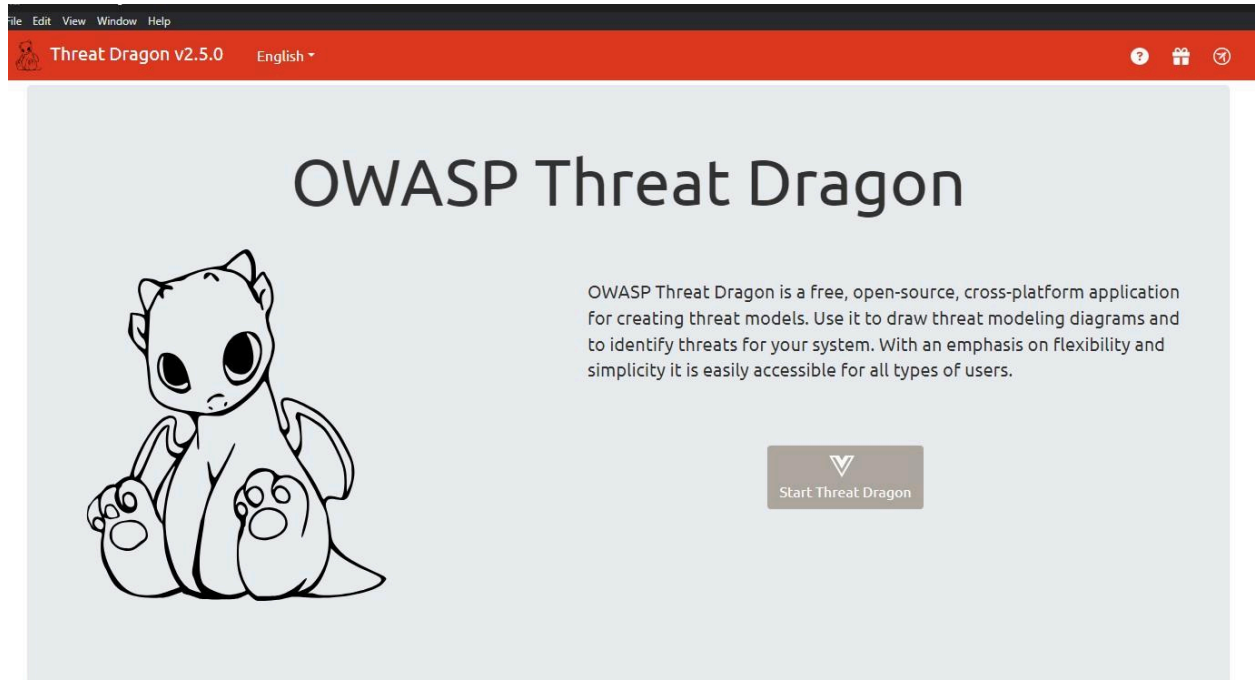
6.1 OWASP Threat Dragon

Tool Overview

Open-source threat modeling tool for creating DFDs and STRIDE threats.

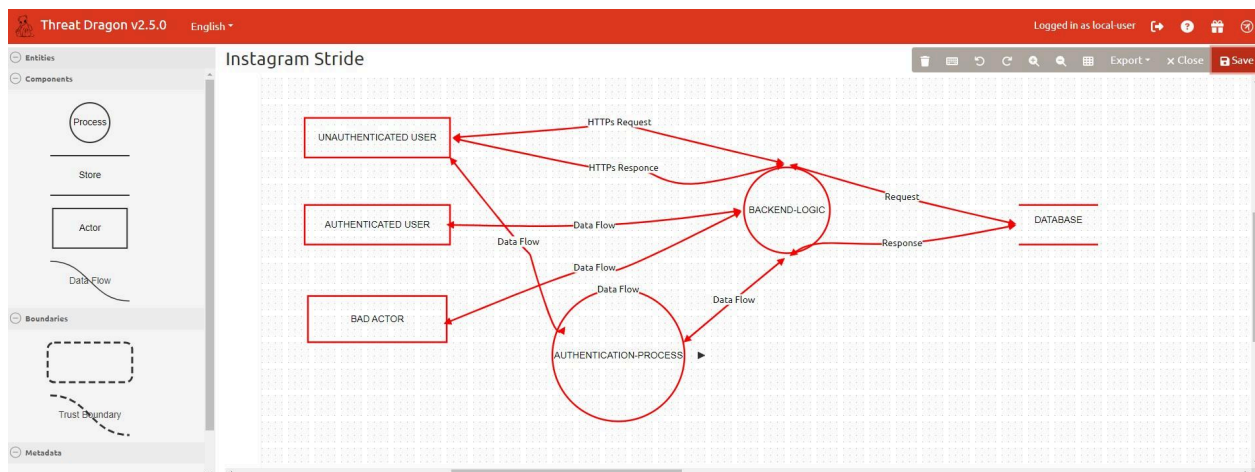
Installation

```
git clone https://github.com/OWASP/threat-dragon
cd threat-dragon
npm install
npm start
```



Step-by-Step Usage

1. Create new model
 2. Add processes, data stores, flows
 3. Assign STRIDE threats
 4. Export report
- Creating model
 - Adding threats
 - Generated report



Threat Dragon v2.5.0 English

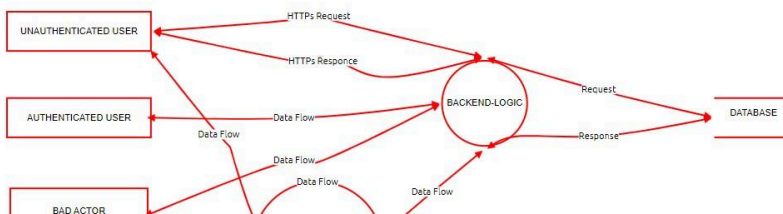
☒ Show model diagrams
 ☒ Show mitigated threats
 ☒ Show out of scope elements
 ☒ Show empty elements
 ☐ Threat Dragon logo
 ☐ Show element properties

Not provided

Summary

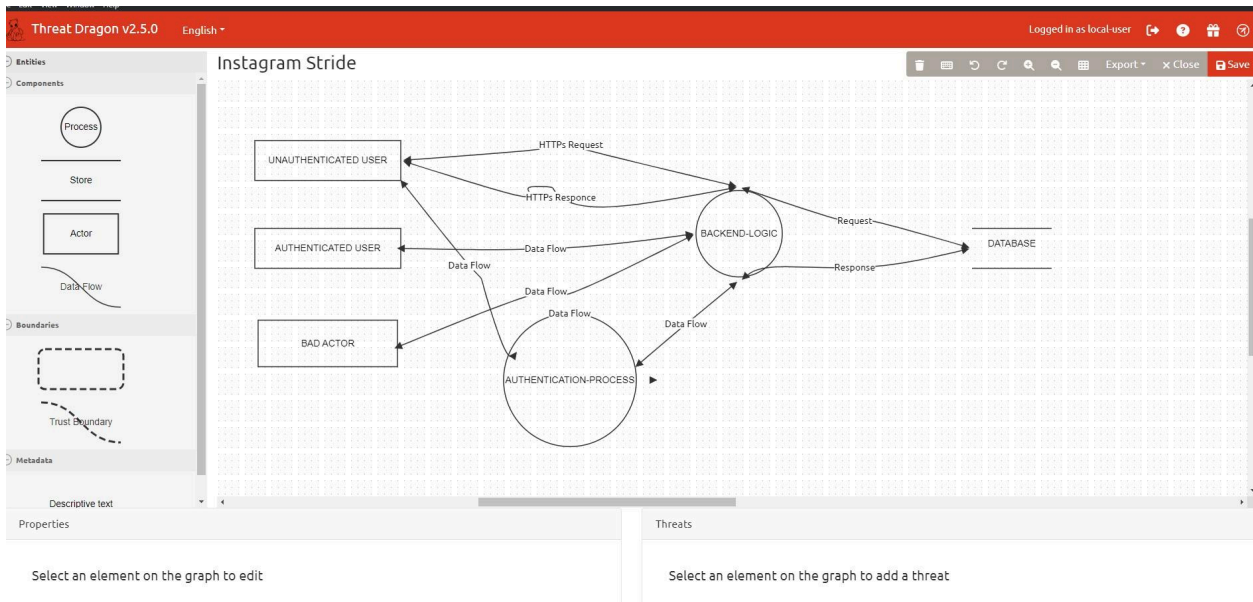
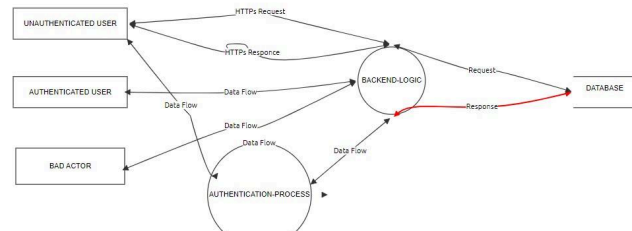
Metric	Total
Total Threats	66
Total Mitigated	0
Total Open	66
Open / Critical Severity	0
Open / High Severity	0
Open / Medium Severity	0
Open / Low Severity	0
Open / TBD Severity	66

Instagram Stride



Threat Dragon v2.5.0 English		Logged in as local-user	PDF Report	Print	Close
<input checked="" type="checkbox"/> Show model diagrams	<input checked="" type="checkbox"/> Show mitigated threats	<input checked="" type="checkbox"/> Show out of scope elements	<input checked="" type="checkbox"/> Show empty elements	<input type="checkbox"/> Threat Dragon logo	<input type="checkbox"/> Show element properties
Metric		Total			
Total Threats		66			
Total Mitigated		60			
Total Open		6			
Open / Critical Severity		0			
Open / High Severity		0			
Open / Medium Severity		0			
Open / Low Severity		0			
Open / TBD Severity		6			

Instagram Stride



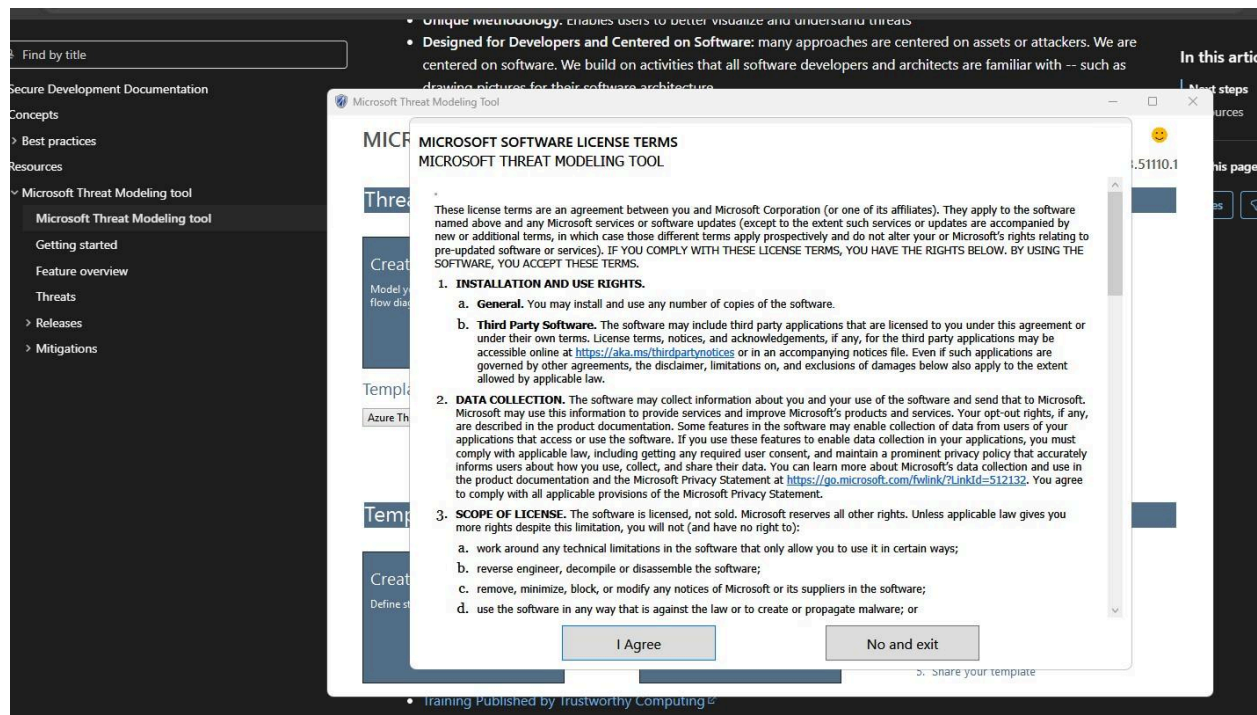
6.2 Microsoft Threat Modeling Tool

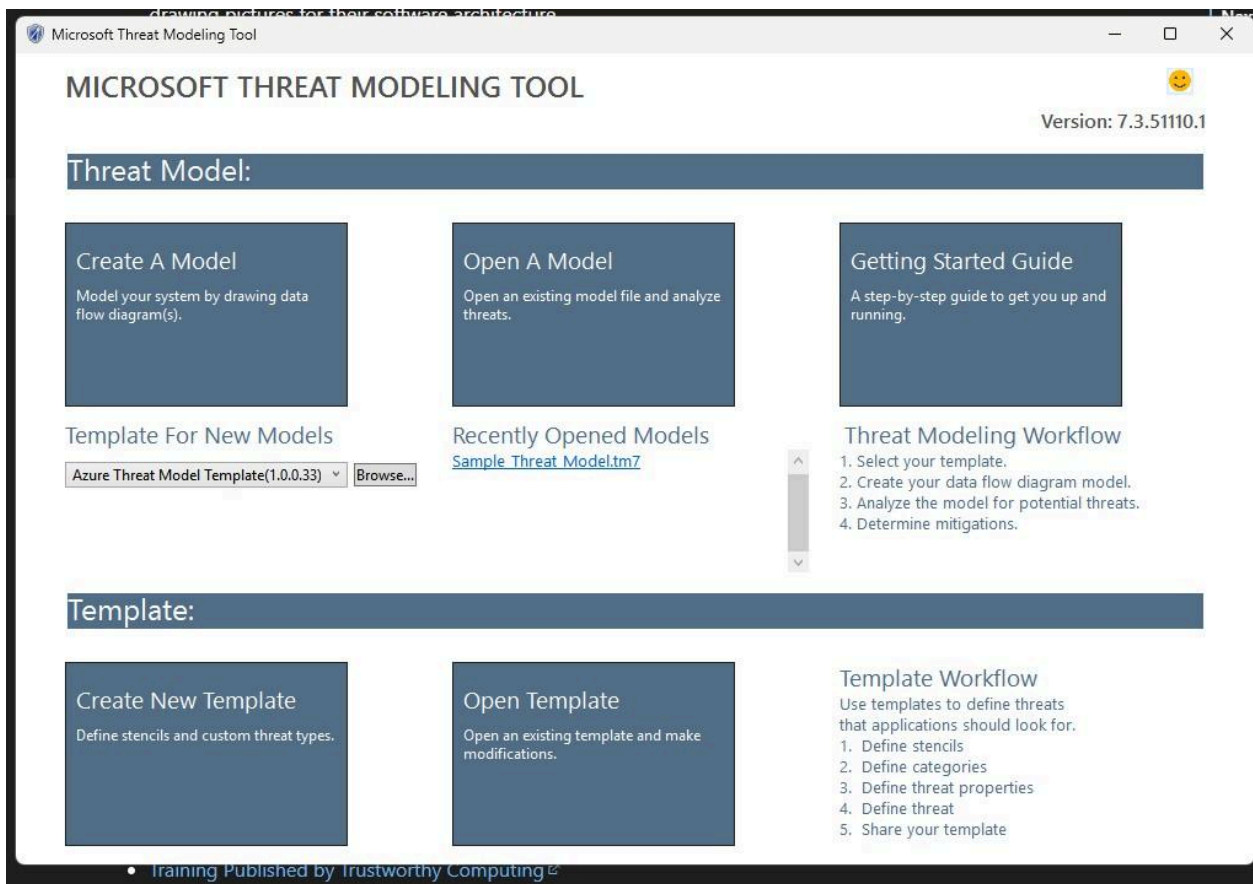
Tool Overview

Microsoft desktop tool for STRIDE-based threat modeling.

Steps

1. Create new model
2. Define architecture
3. Auto-generate STRIDE threats
4. Review mitigation suggestions





Threat Modeling Report

Created on 11/20/2025 8:39:14 PM
Threat Model Name:
Owner:
Reviewer:
Contributors:
Description:
Assumptions:
External Dependencies:

Threat Model Summary:

Not Started	25
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	25
Total Migrated	0

Diagram: Diagram 1

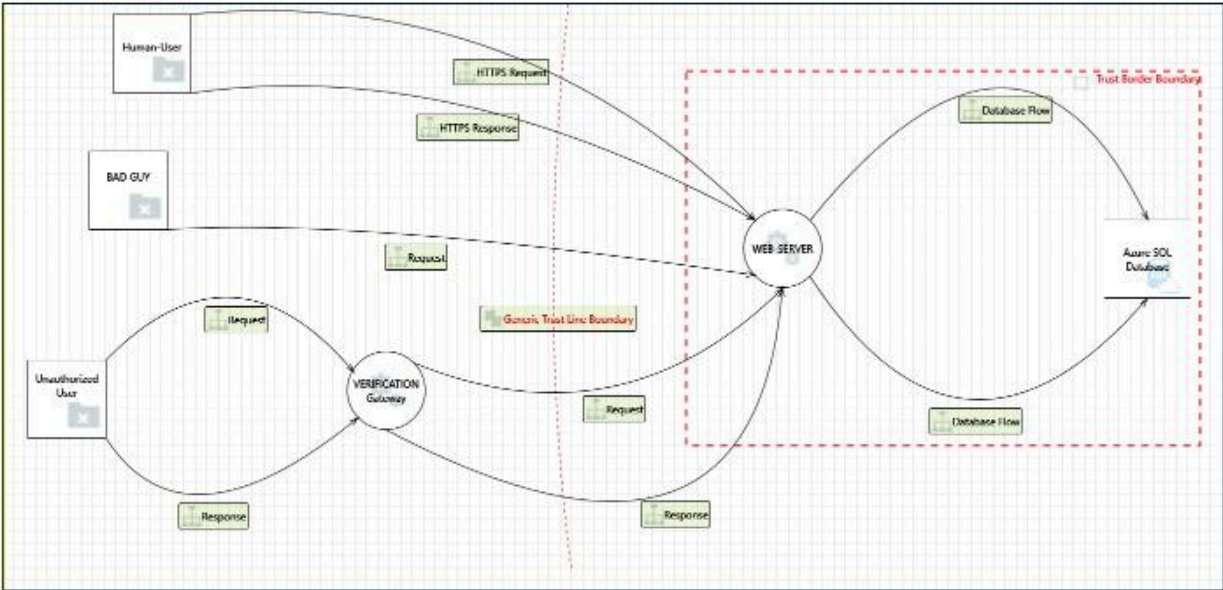
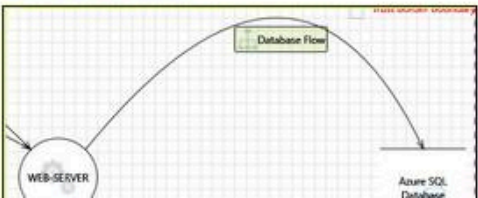


Diagram 1 Diagram Summary:

Not Started	25
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	25
Total Migrated	0

Interaction: Database Flow



- Architecture view
- Threat list
- Mitigation panel

7. Validation & Security Testing (SAFE)

How to Validate Findings

- Review logs
- Configuration review
- Access control testing
- Architecture walkthroughs
- Secure code review

What to Analyze After Modeling

- Attack paths
- Trust boundary violations
- High-risk STRIDE categories
- Unmitigated threats

8. How to Identify Vulnerabilities (Without Exploitation)

Indicators of Vulnerabilities

- Outdated versions
- Weak authentication
- Missing encryption
- Misconfigured IAM

Sources of Evidence

- Application logs
- Cloud audit logs
- Configuration files
- Threat model reports

9. Mapping to NIST CSF

NIST Function	Threat Modeling Mapping
Identify	Asset & threat identification
Protect	Mitigation controls
Detect	Logging & monitoring
Respond	Incident response planning
Recover	Resilience & availability

10. ISO 27001 Annex A Mapping

Control	Description
A.5	Information security policies
A.8	Asset management
A.9	Access control
A.12	Logging & monitoring
A.14	Secure system development
A.16	Incident management

11. Security Best Practices

- Least privilege everywhere
- Zero Trust architecture
- Encrypt everything
- Centralized logging
- Regular threat model reviews
- Update threat models after changes

12. Analysis & Recommendations

Key Findings

- Most risks originate at trust boundaries
- IAM misconfigurations are critical
- Logging gaps increase repudiation risks

Recommendations

- Perform threat modeling during design
- Integrate into CI/CD
- Combine with secure code reviews
- Reassess quarterly

13. Conclusion

Threat modeling using STRIDE, OWASP Threat Dragon, and Microsoft TMT provides a proactive security mindset. This project demonstrates real-world AppSec, Blue Team, and GRC skills aligned with NIST CSF and ISO 27001.