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)

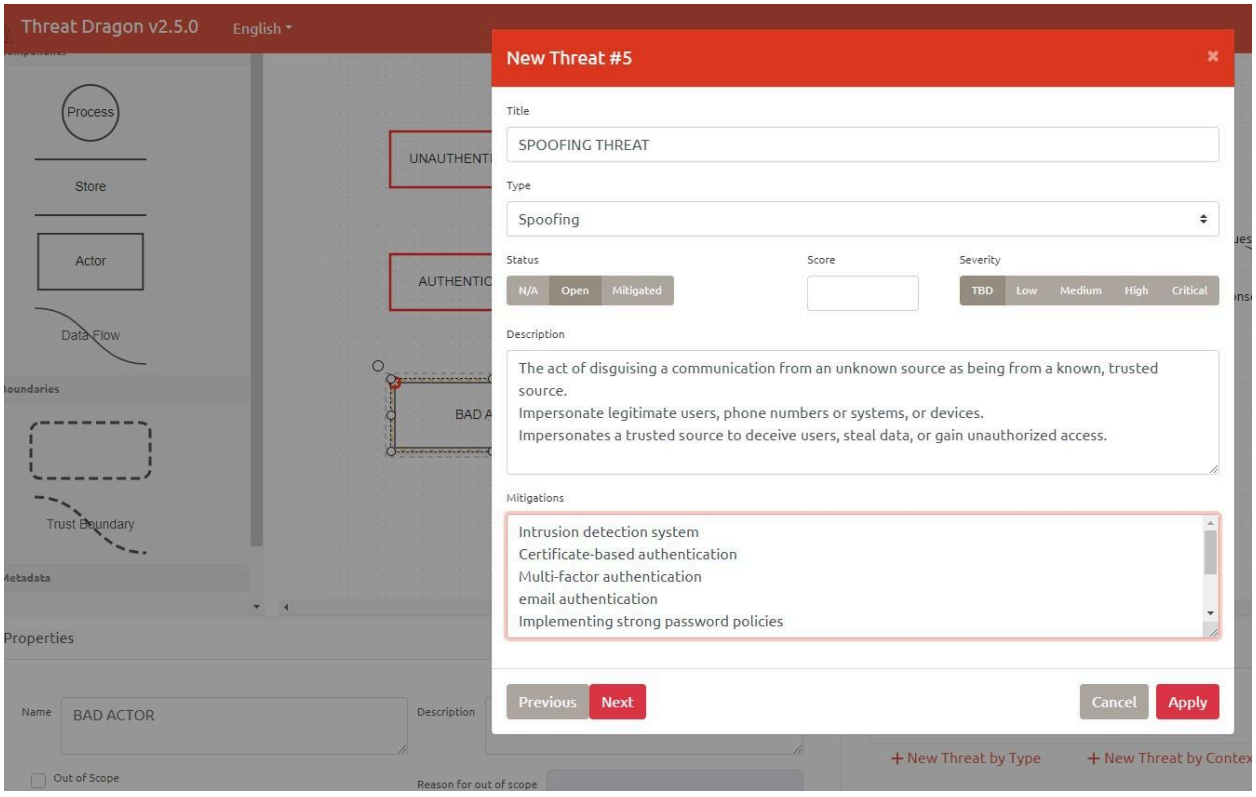
5.1 Spoofing

Threat: Fake user identities
Indicators:

- Weak authentication
- No MFA
- Hardcoded credentials

Mitigations:

- MFA
- OAuth 2.0
- Certificate-based auth



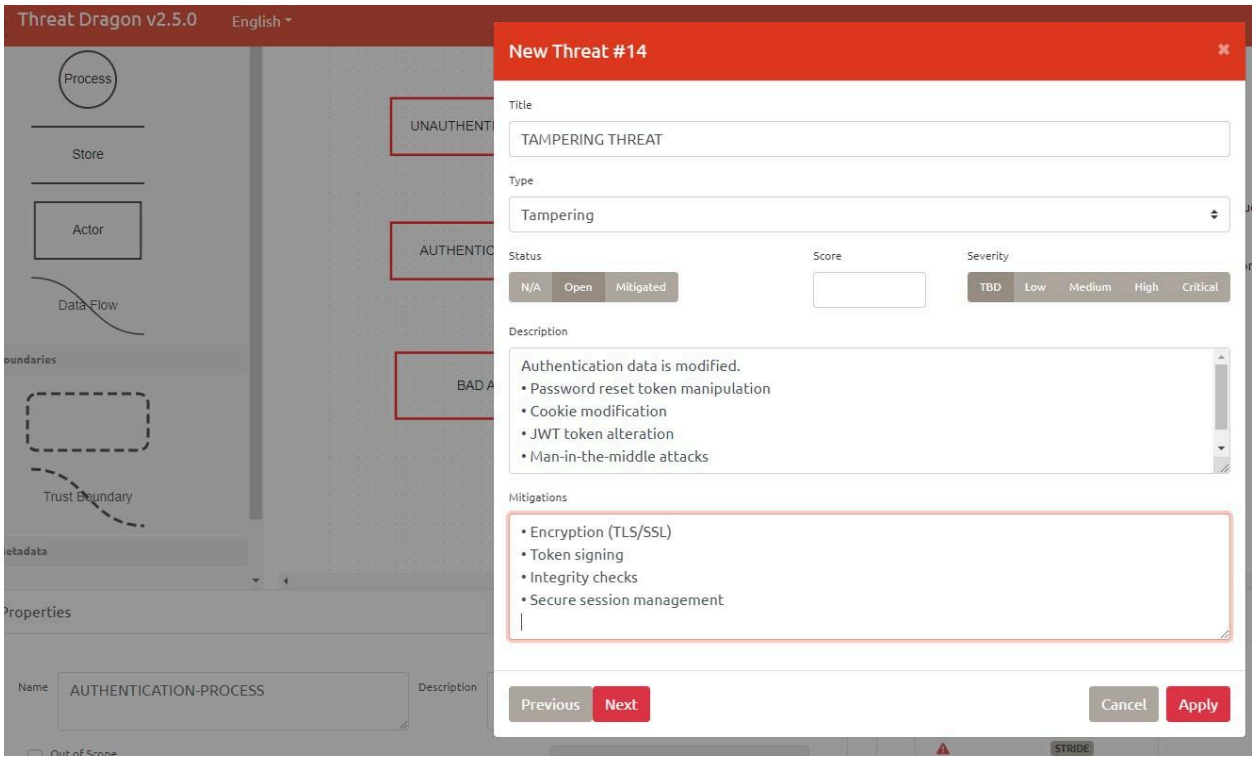
5.2 Tampering (Integrity)

Threat: Modifying requests, data, configs
Indicators:

- No input validation
- Unsigned tokens
- No checksums

Mitigations:

- HMAC
- Digital signatures
- Input validation



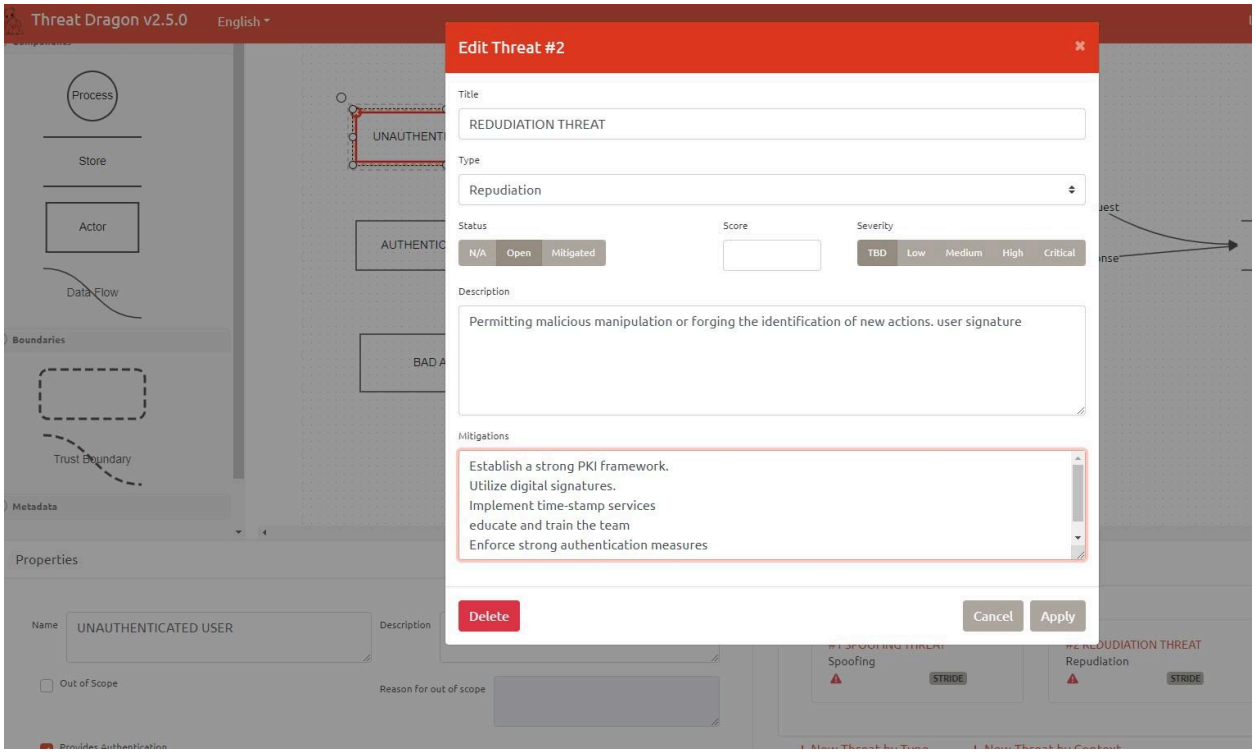
5.3 Repudiation

Threat: Users deny actions
Indicators:

- Missing logs
- No timestamps
- Logs not protected

Mitigations:

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



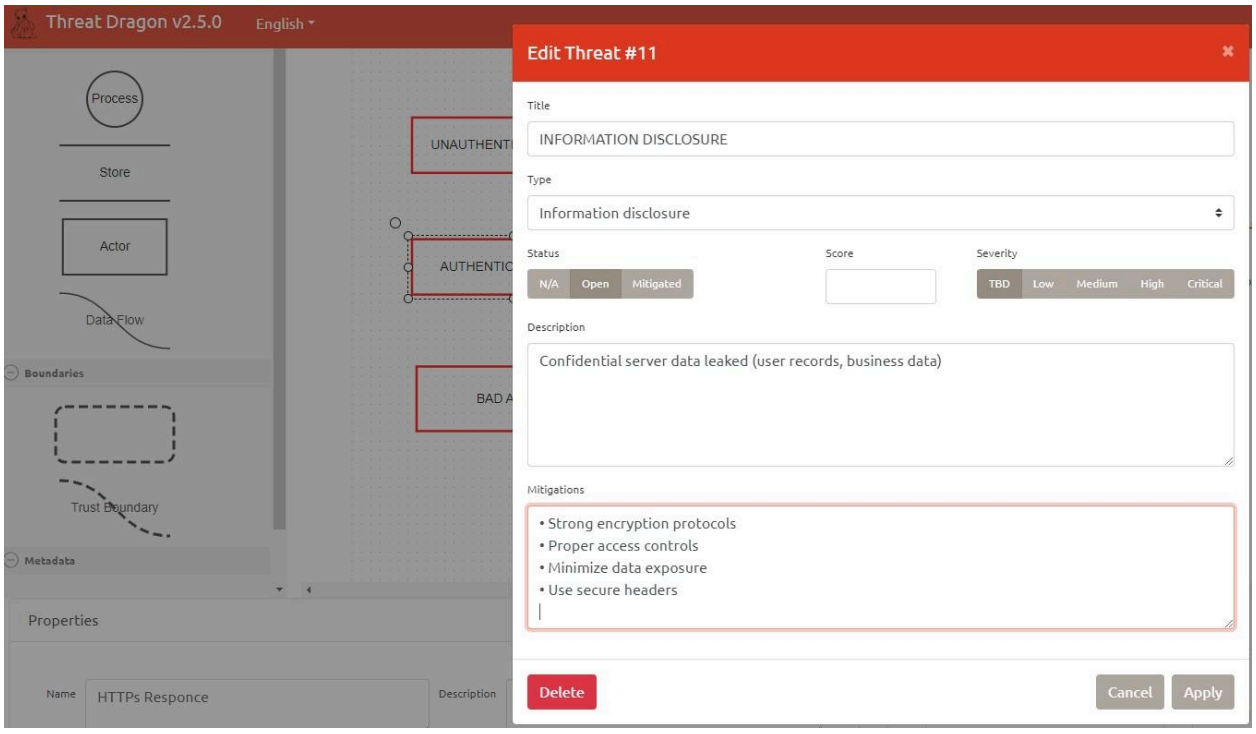
5.4 Information Disclosure

Threat: Sensitive data leaks
Indicators:

- Plaintext storage
- Open S3 buckets
- Verbose error messages

Mitigations:

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



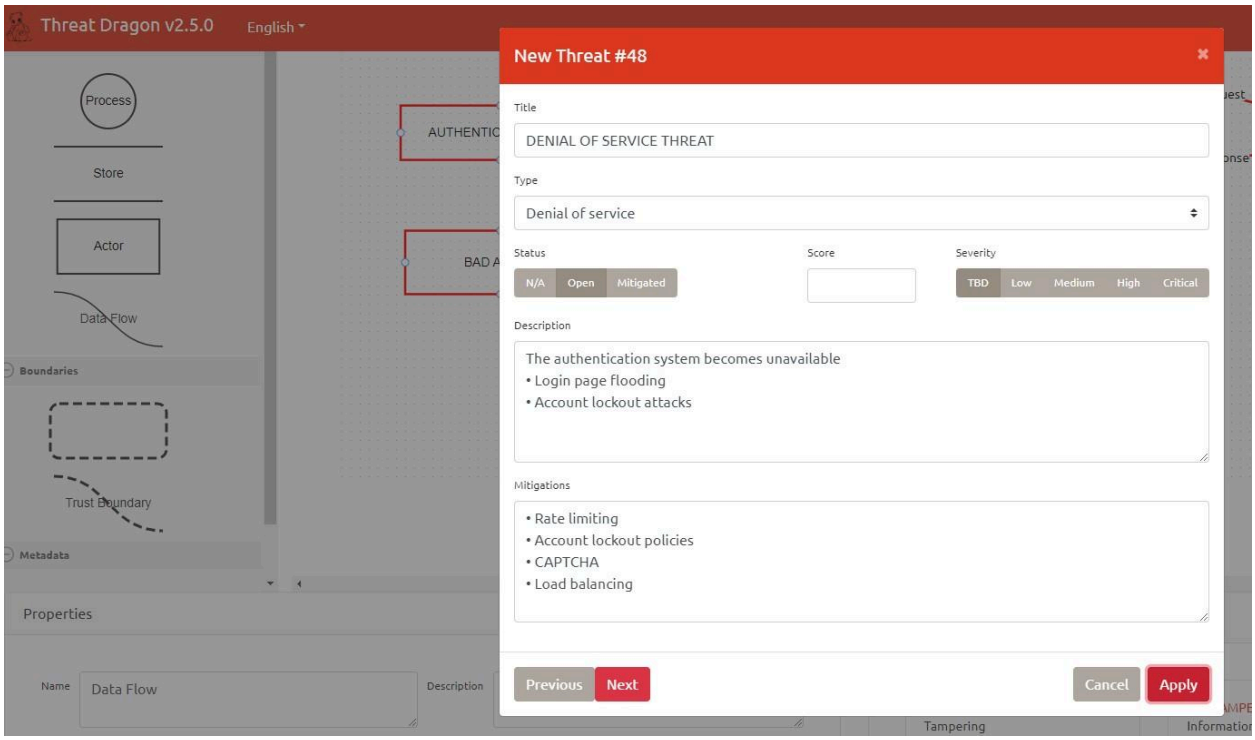
5.5 Denial of Service (Availability)

Threat: Resource exhaustion
Indicators:

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

Mitigations:

- Rate limiting
- Auto-scaling
- Load balancers



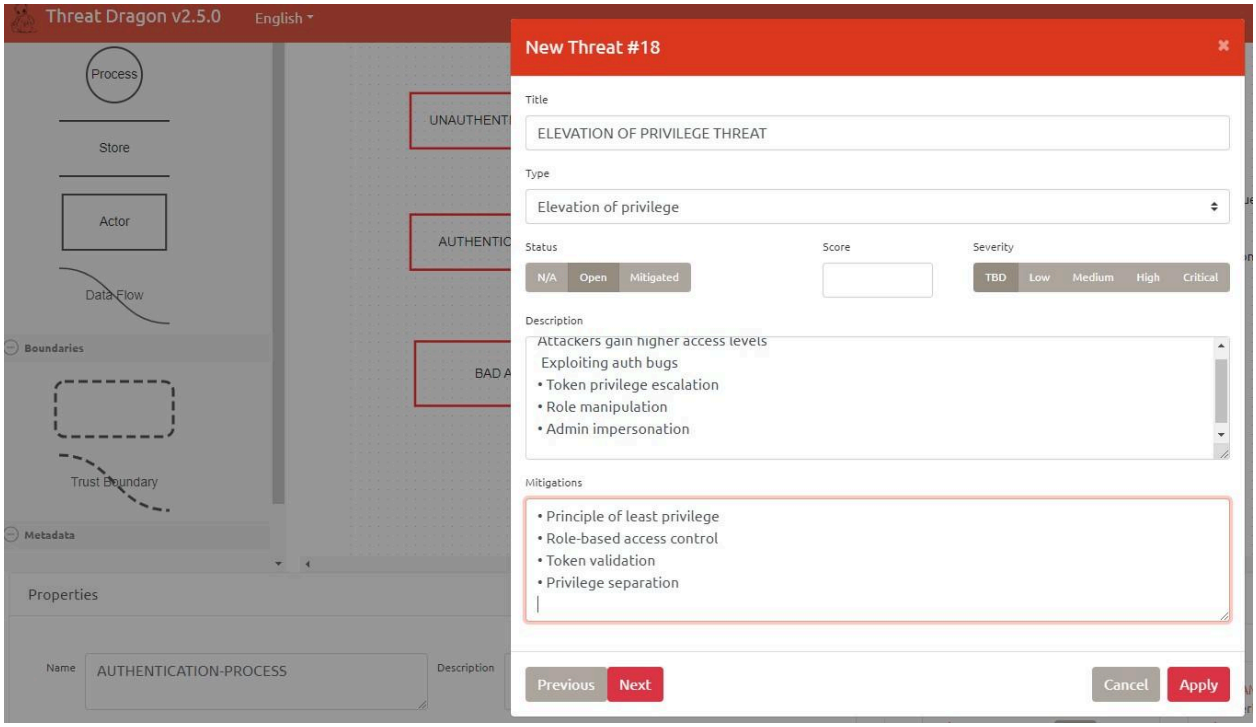
5.6 Elevation of Privilege

Threat: User gains admin access
Indicators:

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

Mitigations:

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



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

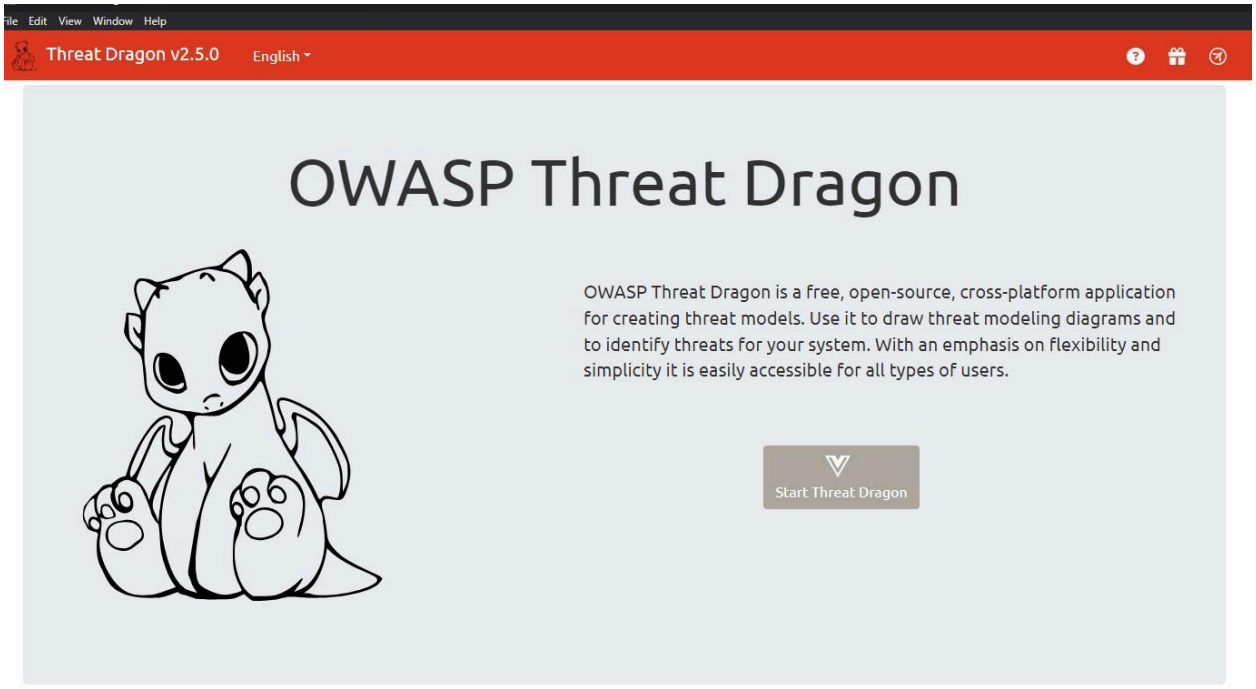
6.1 OWASP Threat Dragon

Tool Overview

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

Installation

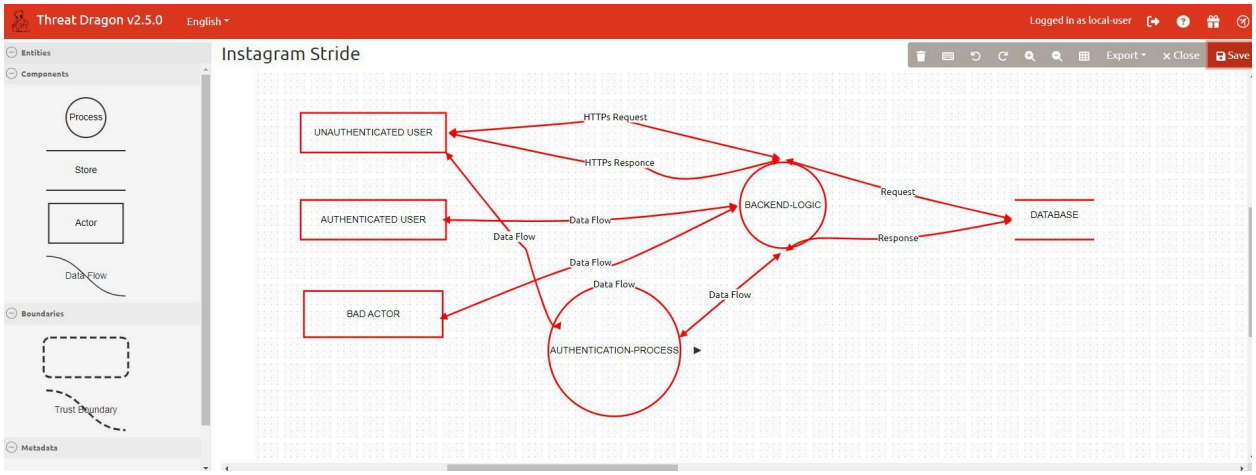
```
git clone https://github.com/OWASP/threat-dragon
cd threat-dragon
npm install
npm start
```



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

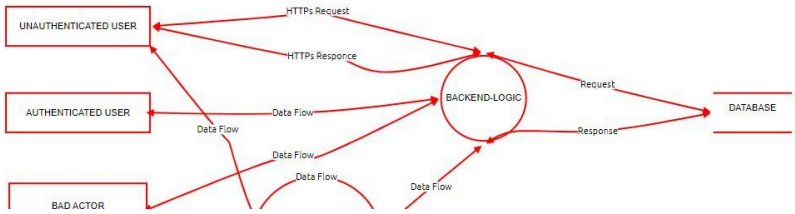
Show model diagrams | Show mitigated threats | Show out of scope elements | Show empty elements | Threat Dragon logo | Show element properties

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



File Edit View Window Help

Threat Dragon v2.5.0 English

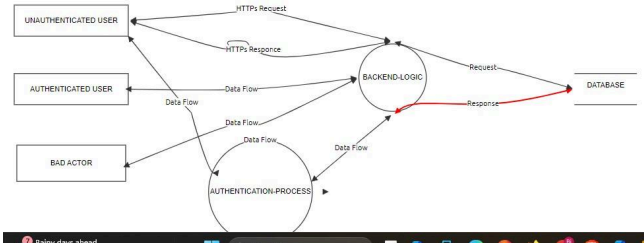
Logged in as local-user

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

PDF Report | Print | Close

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



Rainy days ahead 41°F | Search | 8:52 PM 11/18/2024

Threat Dragon v2.5.0 English

Logged in as local-user

Entities

Components

Process

Store

Actor

Data Flow

Boundaries

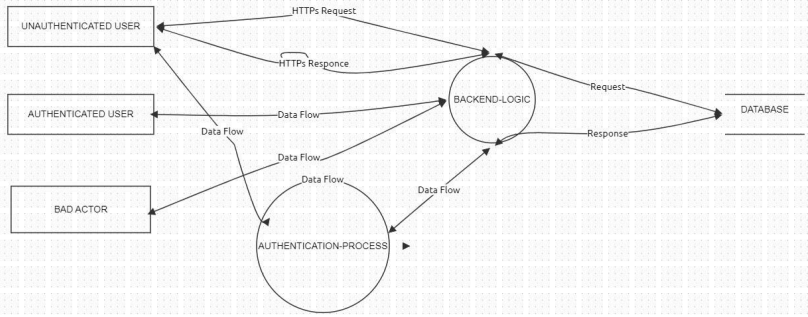
Trust Boundary

Metadata

Descriptive text

Instagram Stride

Export | Close | Save



Properties

Select an element on the graph to edit

Threats

Select an element on the graph to add a threat

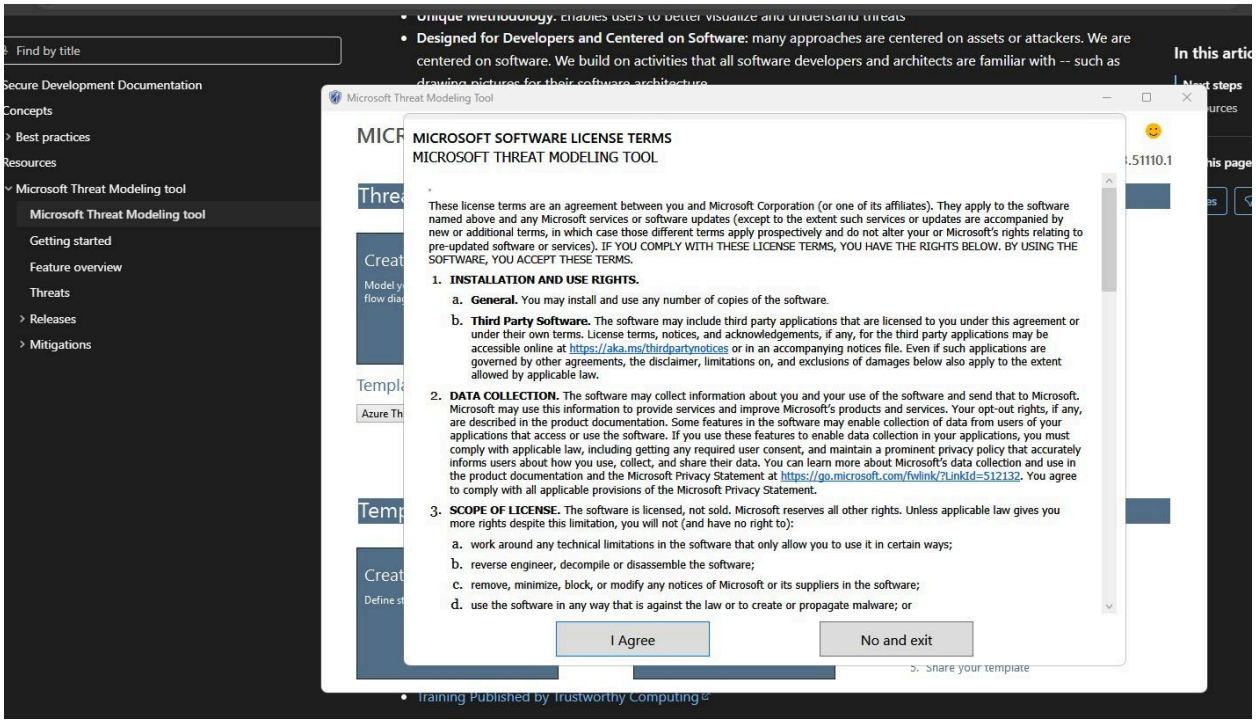
6.2 Microsoft Threat Modeling Tool

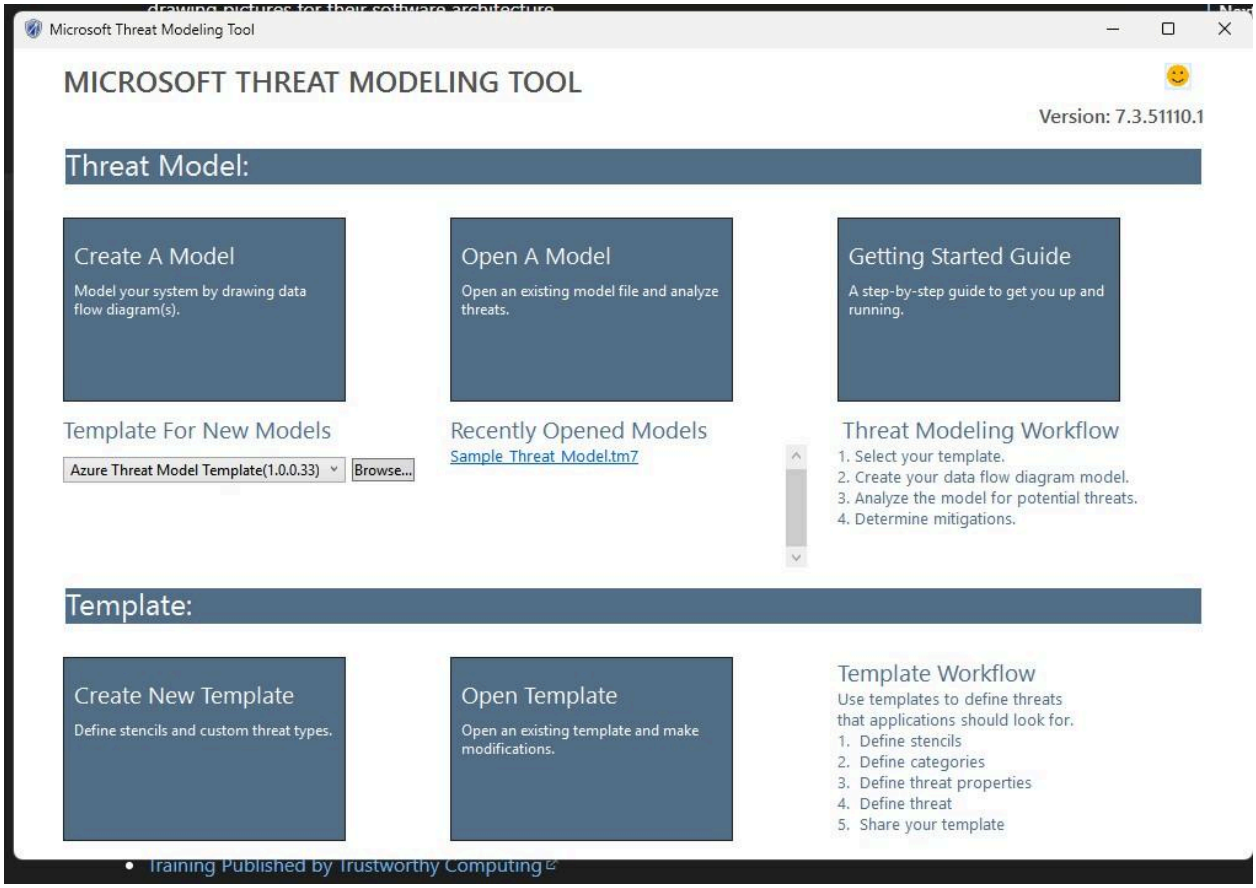
Tool Overview

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




Microsoft Threat Modeling Tool
MICROSOFT THREAT MODELING TOOL
Version: 7.3.51110.1
Threat Model:
Create A Model
Model your system by drawing data flow diagram(s).
Open A Model
Open an existing model file and analyze threats.
Getting Started Guide
A step-by-step guide to get you up and running.
Template For New Models
Azure Threat Model Template(1.0.0.33)
Browse...
Recently Opened Models
Sample_Threat_Model.tm7
Threat Modeling Workflow
1. Select your template.
2. Create your data flow diagram model.
3. Analyze the model for potential threats.
4. Determine mitigations.
Template:
Create New Template
Define stencils and custom threat types.
Open Template
Open an existing template and make modifications.
Template Workflow
Use templates to define threats that applications should look for.
1. Define stencils
2. Define categories
3. Define threat properties
4. Define threat
5. Share your template
Training Published by Trustworthy Computing

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

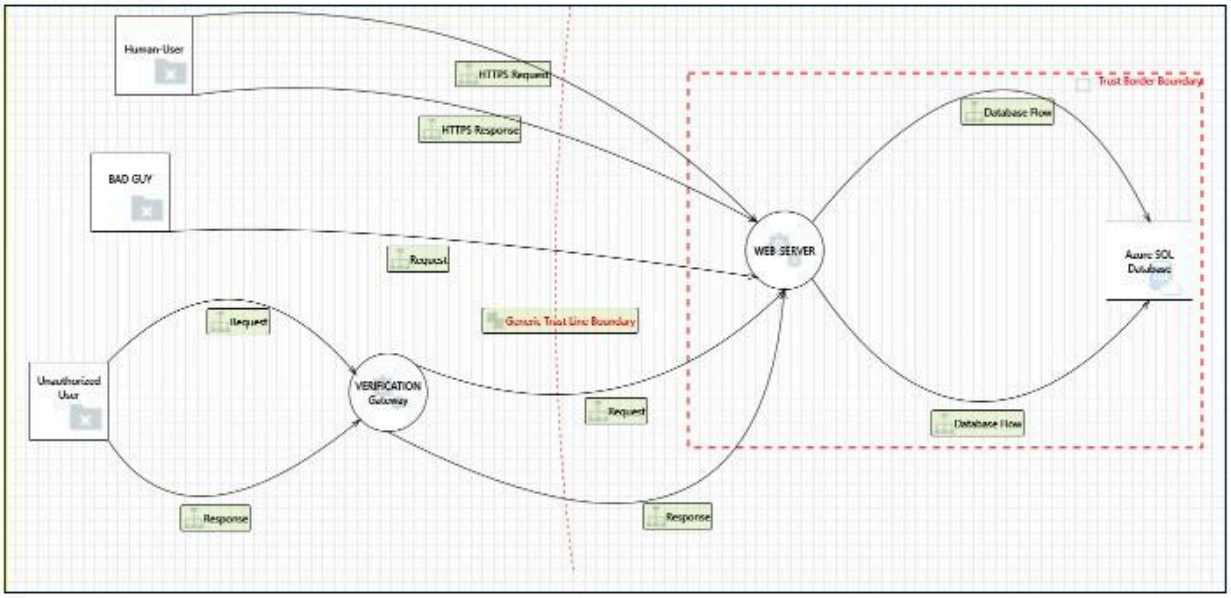
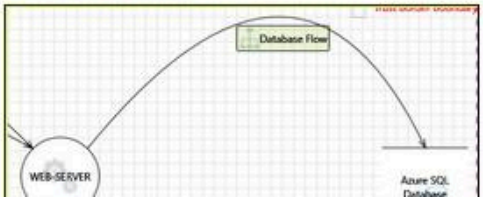


Diagram 1 Diagram Summary:

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.