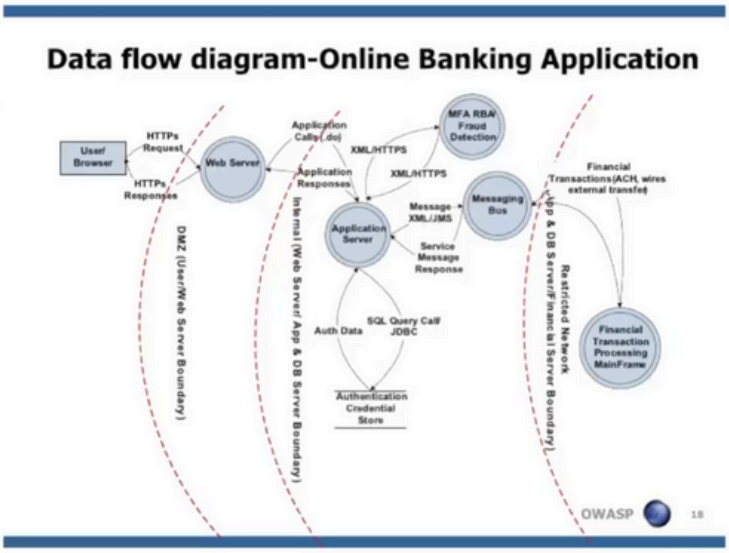
Threat Modeling

pytm

https://github.com/izar/pytm

```python
#!/usr/bin/env python3

from pytm.pytm import TM, Server, Datastore, Dataflow, Boundary, Actor, Lambda, Data, Classi

tm = TM("my test tm")
tm.description = "another test tm"
tm.isOrdered = True

User_Web = Boundary("User/Web")
Web_DB = Boundary("Web/DB")

user = Actor("User")
user.inBoundary = User_Web

web = Server("Web Server")
web.OS = "CloudOS"
web.isHardened = True
web.sourceCode = "server/web.cc"

db = Datastore("SQL Database (*)")
db.OS = "CentOS"
db.isHardened = False
db.inBoundary = Web_DB
db.isSql = True
db.inScope = False
db.sourceCode = "model/schema.sql"
```

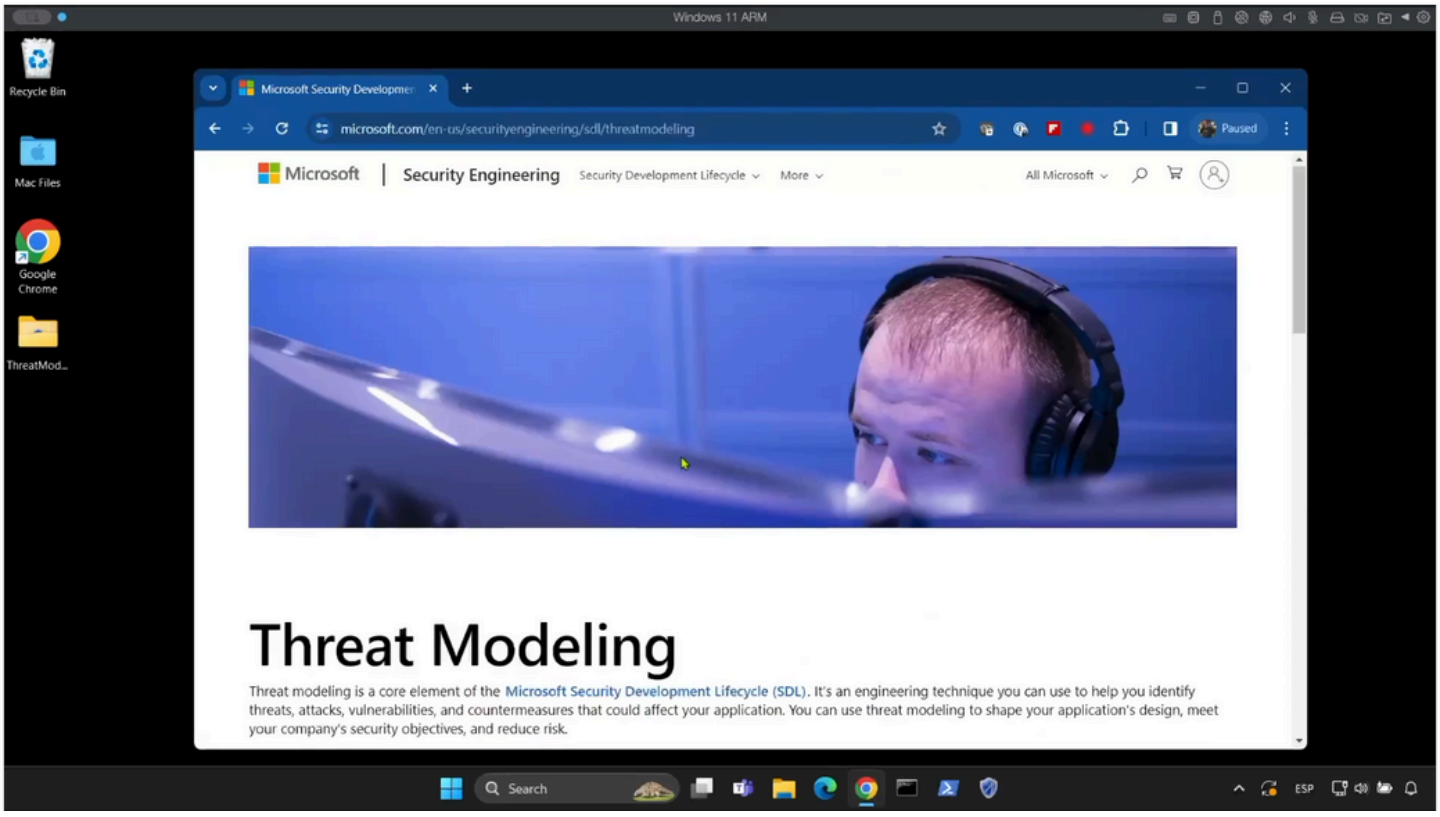
Threat Modeling

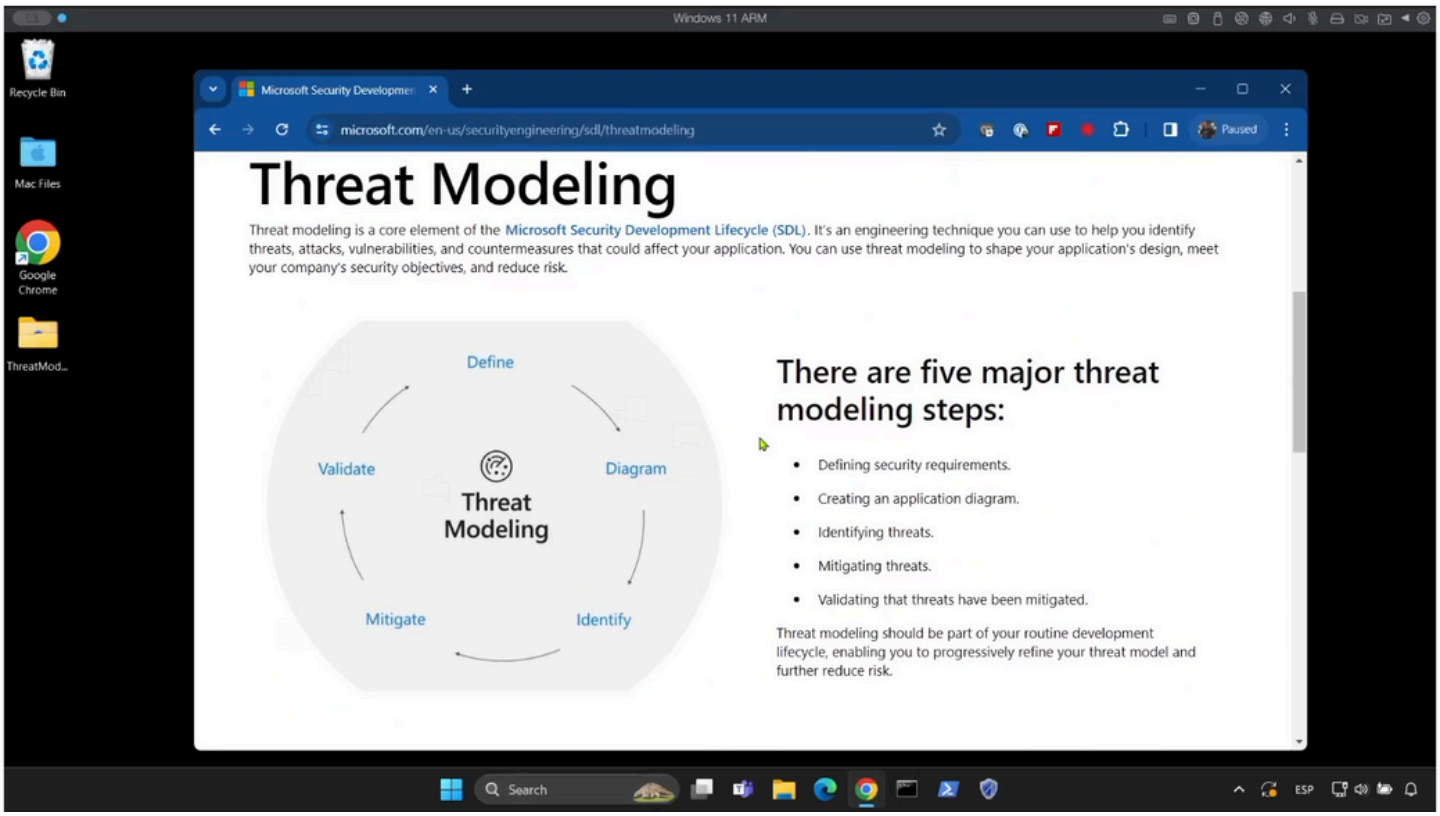


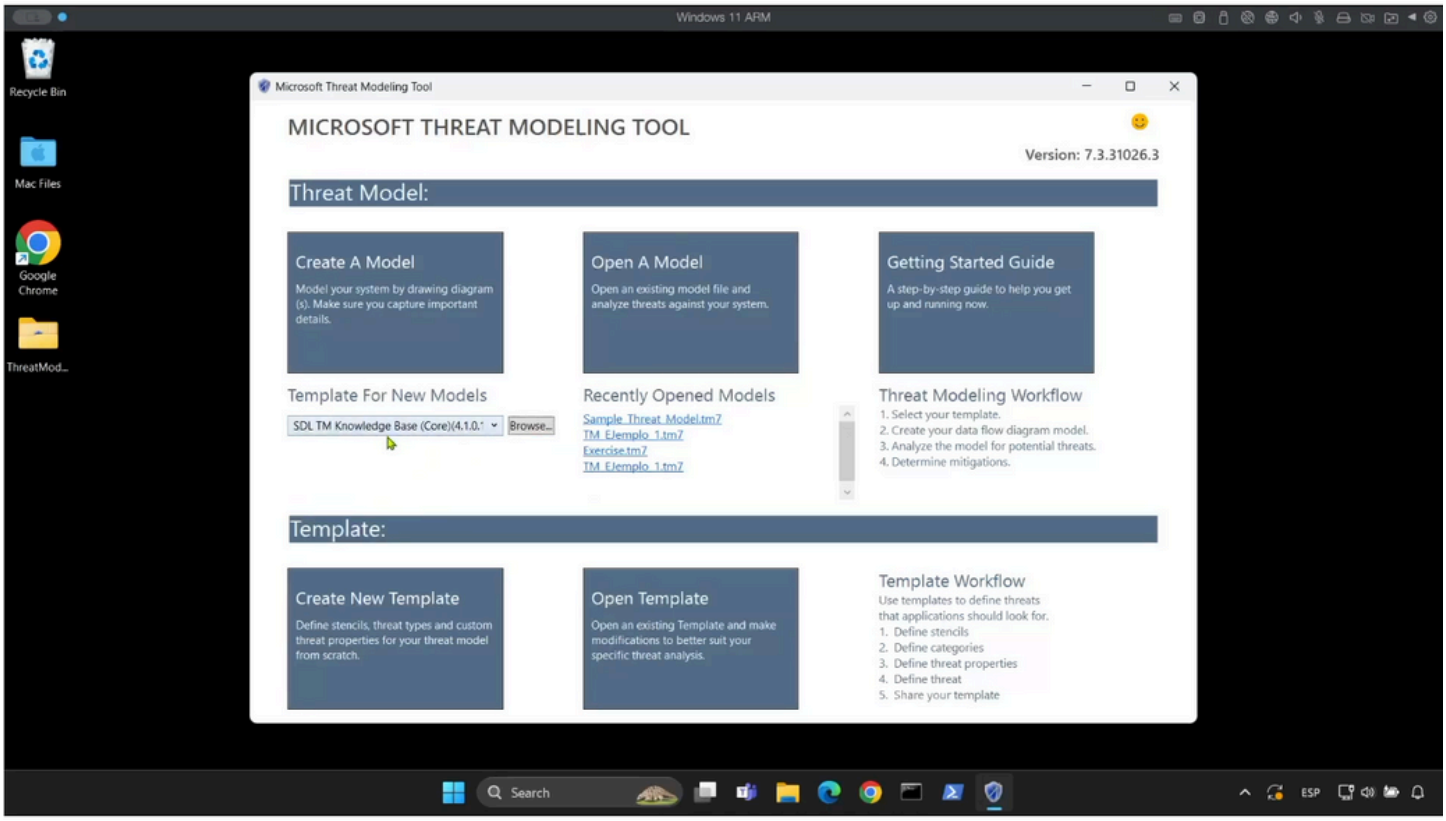
Picture source: Wei Zhang & Marco Morana OWASP Cincinnati, U.S.A.
https://en.wikipedia.org/wiki/Threat_model#/media/File:Data_Flow_Diagram_-_Online_Banking_Application.jpg

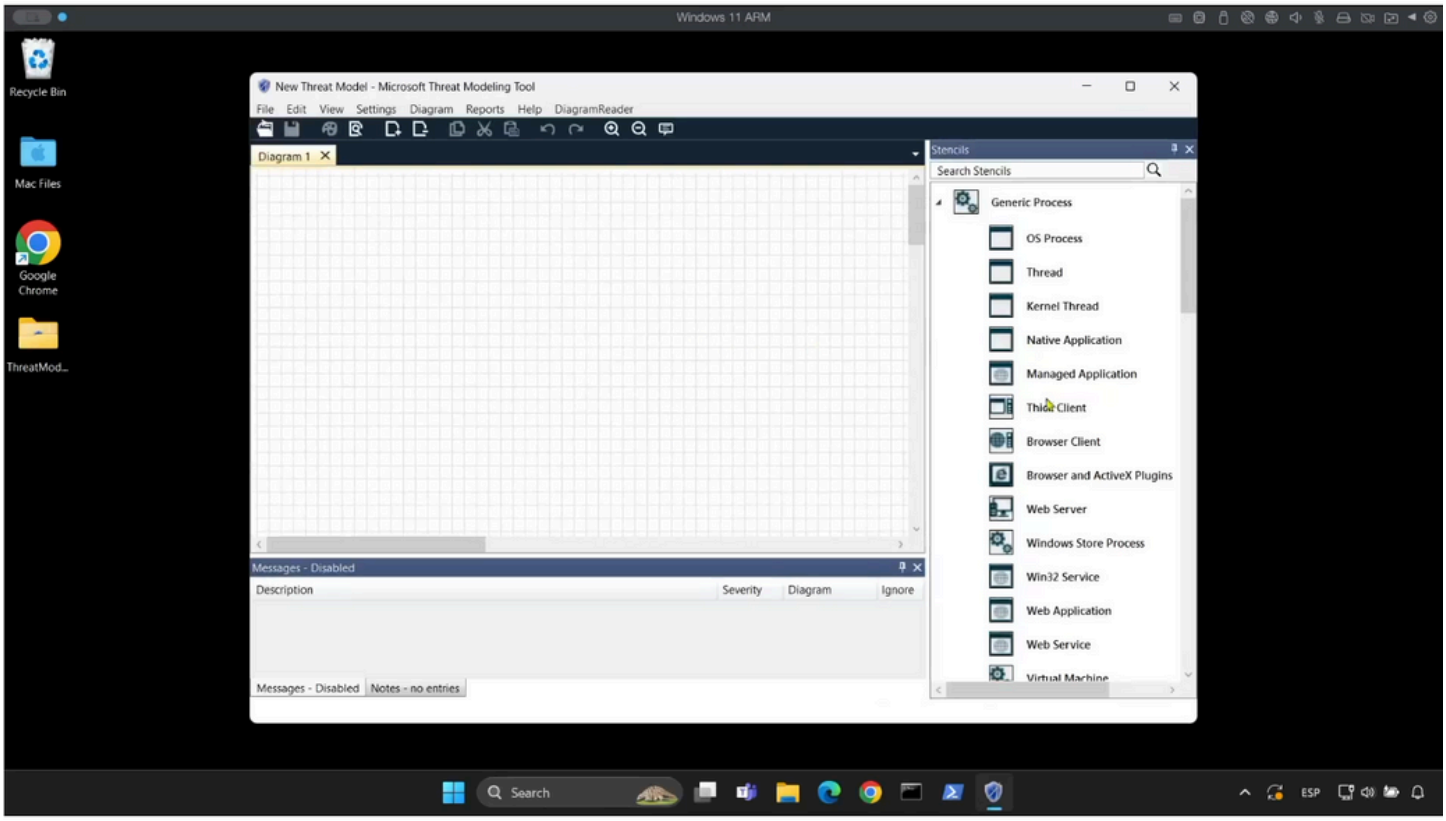
Threat Modeling

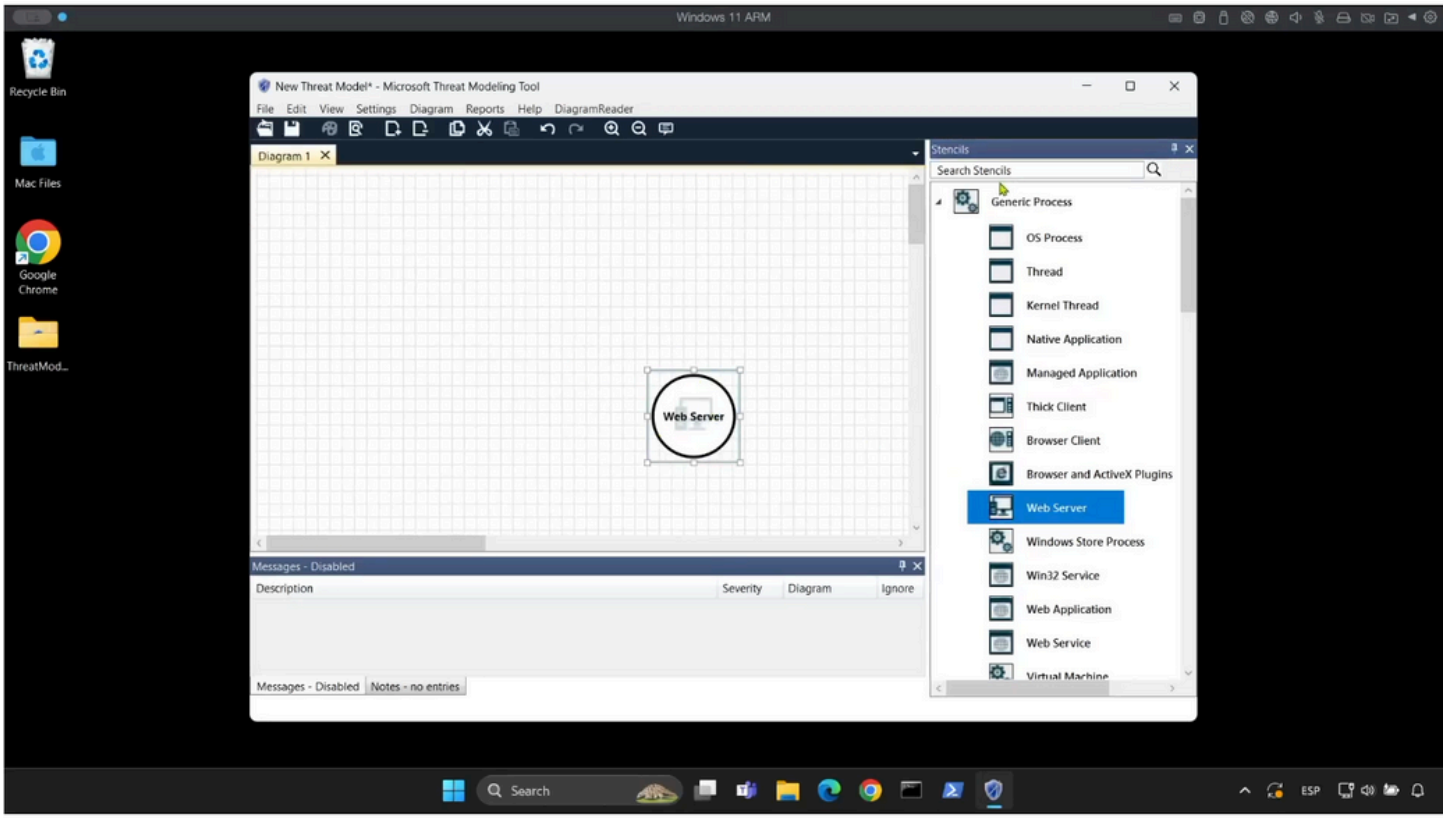
Microsoft Threat Modeling Tool

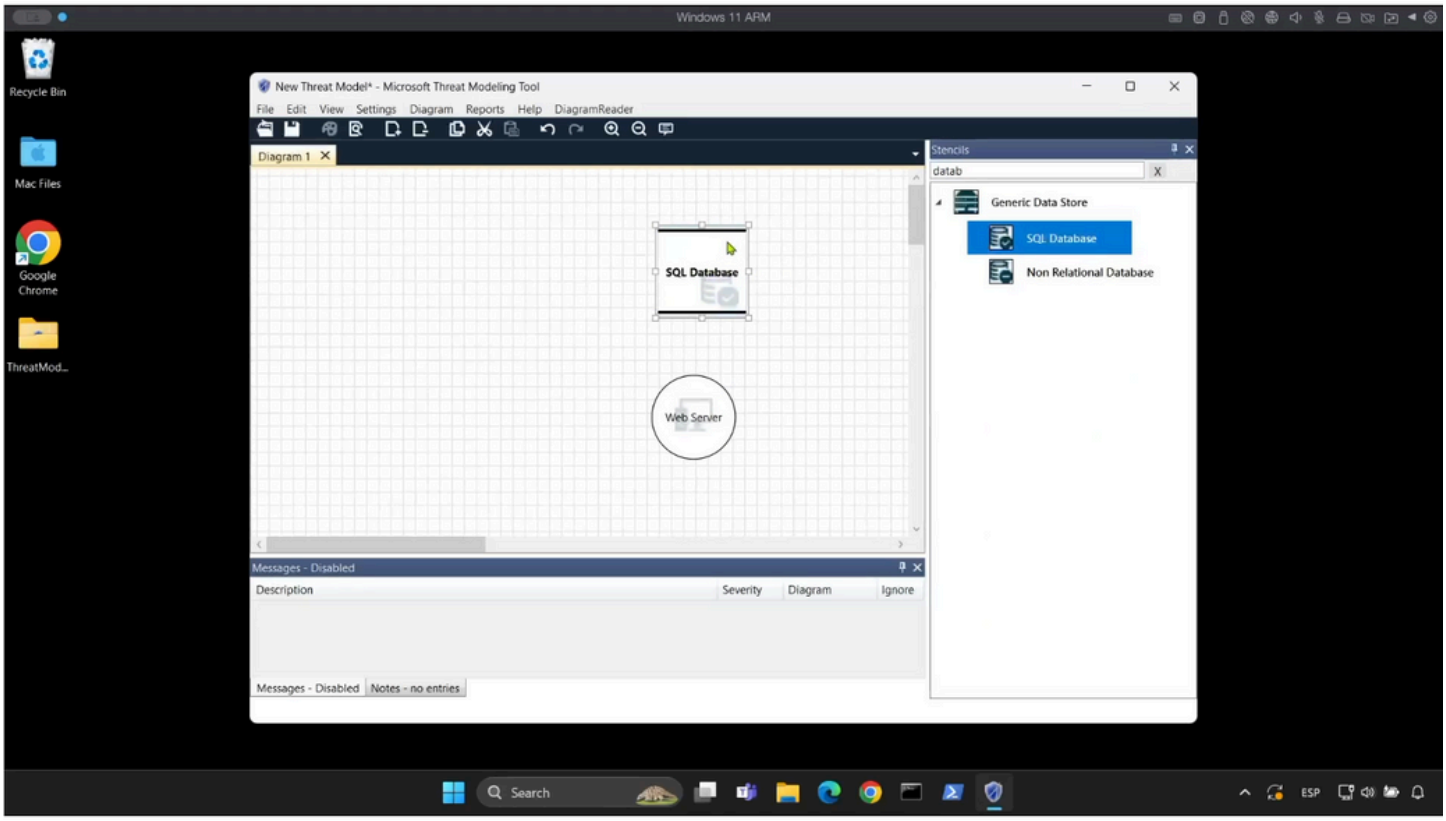


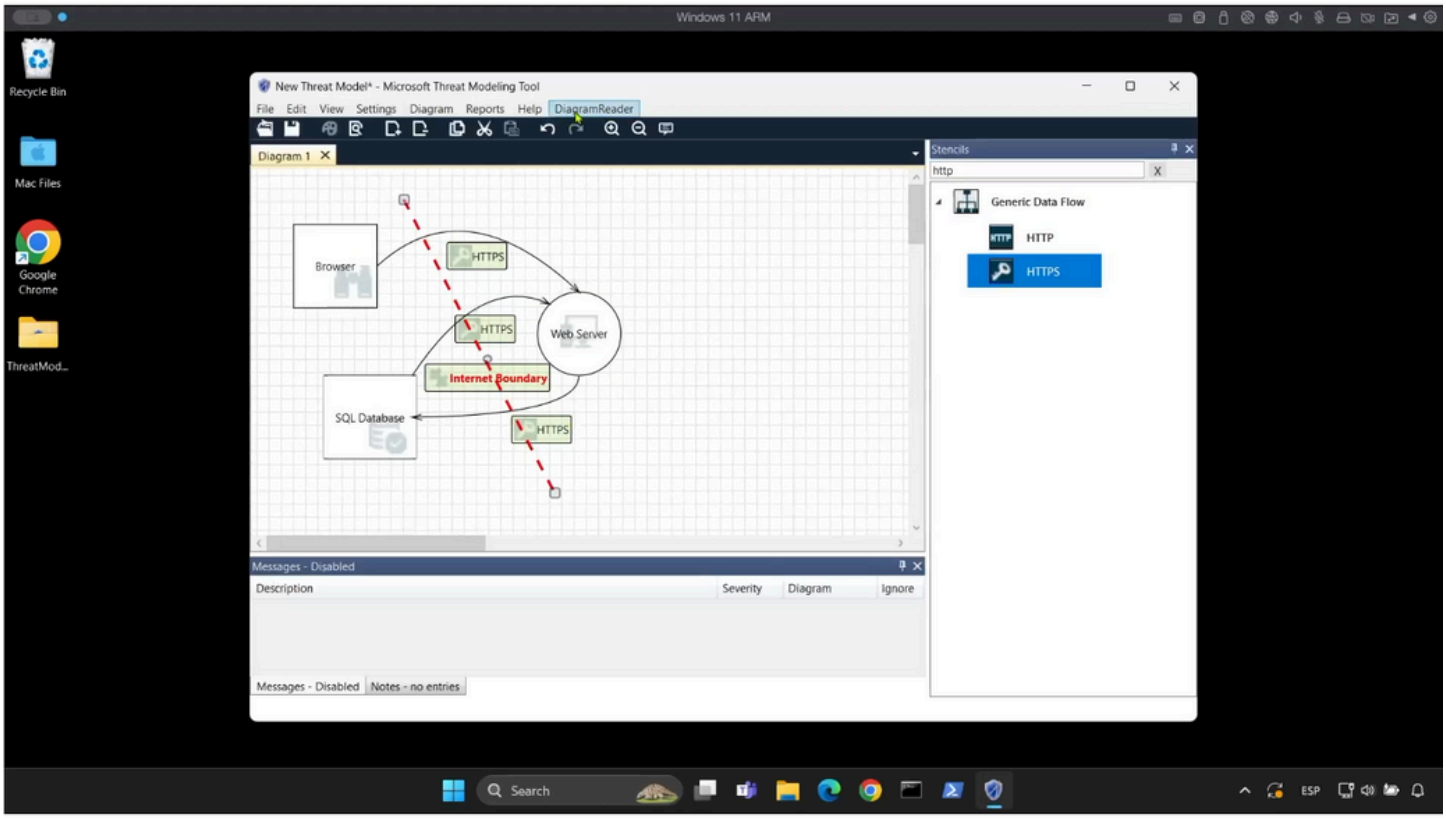

Windows 11 ARM
Recycle Bin
Mac Files
Google Chrome
ThreatMod...
Microsoft Security Developmer
microsoft.com/en-us/securityengineering/sdl/threatmodeling
Paused
Threat Modeling
Threat modeling is a core element of the Microsoft Security Development Lifecycle (SDL). It's an engineering technique you can use to help you identify threats, attacks, vulnerabilities, and countermeasures that could affect your application. You can use threat modeling to shape your application's design, meet your company's security objectives, and reduce risk.
Define
Diagram
Identify
Mitigate
Validate
Threat Modeling
There are five major threat modeling steps:
Defining security requirements.
Creating an application diagram.
Identifying threats.
Mitigating threats.
Validating that threats have been mitigated.
Threat modeling should be part of your routine development lifecycle, enabling you to progressively refine your threat model and further reduce risk.
Search
ESP

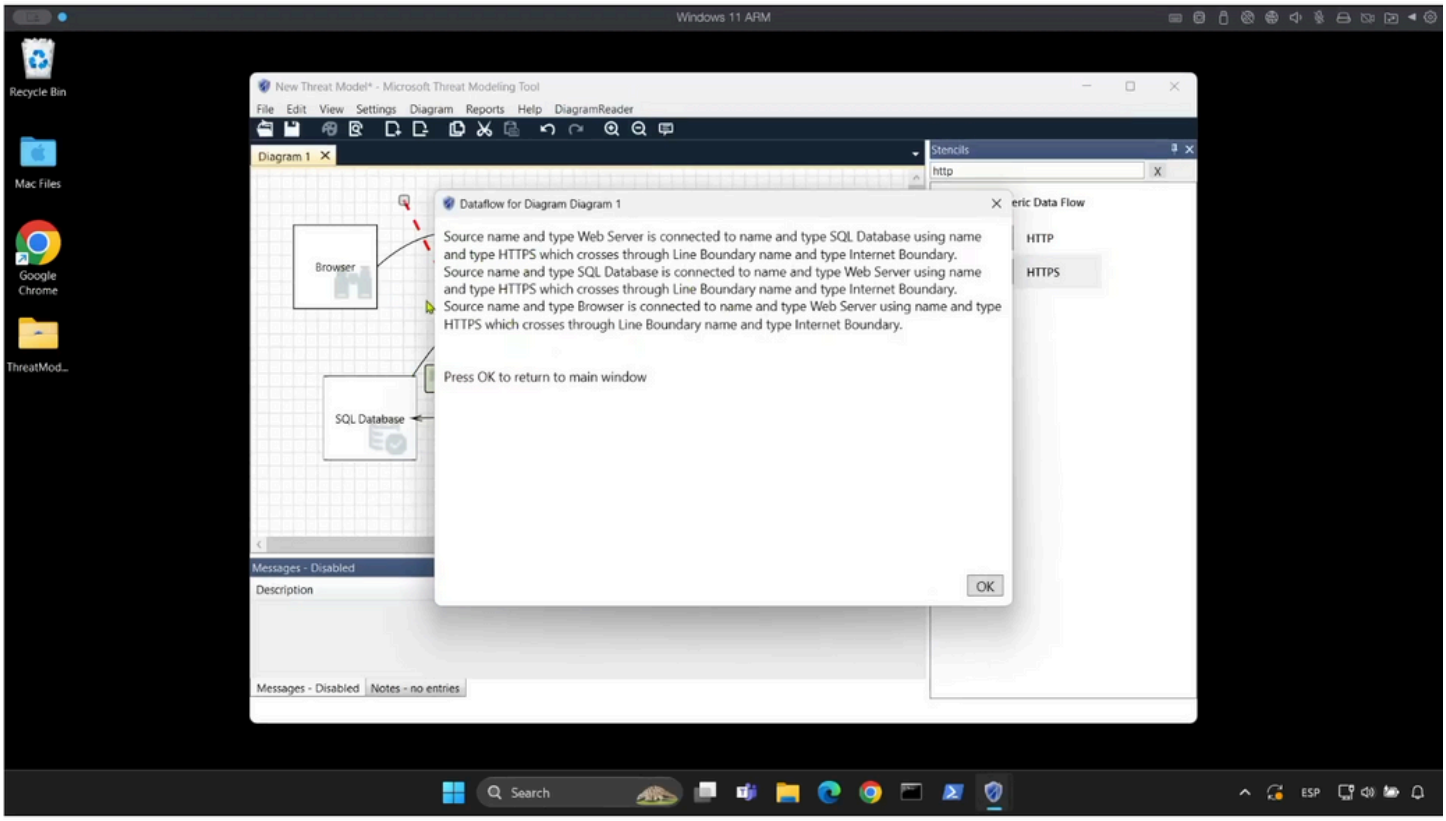

Windows 11 ARM
Recycle Bin
Mac Files
Google Chrome
ThreatMod...
Microsoft Threat Modeling Tool
MICROSOFT THREAT MODELING TOOL
Version: 7.3.31026.3
Threat Model:
Create A Model
Model your system by drawing diagram (s). Make sure you capture important details.
Open A Model
Open an existing model file and analyze threats against your system.
Getting Started Guide
A step-by-step guide to help you get up and running now.
Template For New Models
SDL TM Knowledge Base (Core)(4.1.0.
Browse...
Recently Opened Models
Sample_Threat_Model.tm7
TM_EJemplo_1.tm7
Exercise.tm7
TM_EJemplo_1.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, threat types and custom threat properties for your threat model from scratch.
Open Template
Open an existing Template and make modifications to better suit your specific threat analysis.
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
Search
ESP

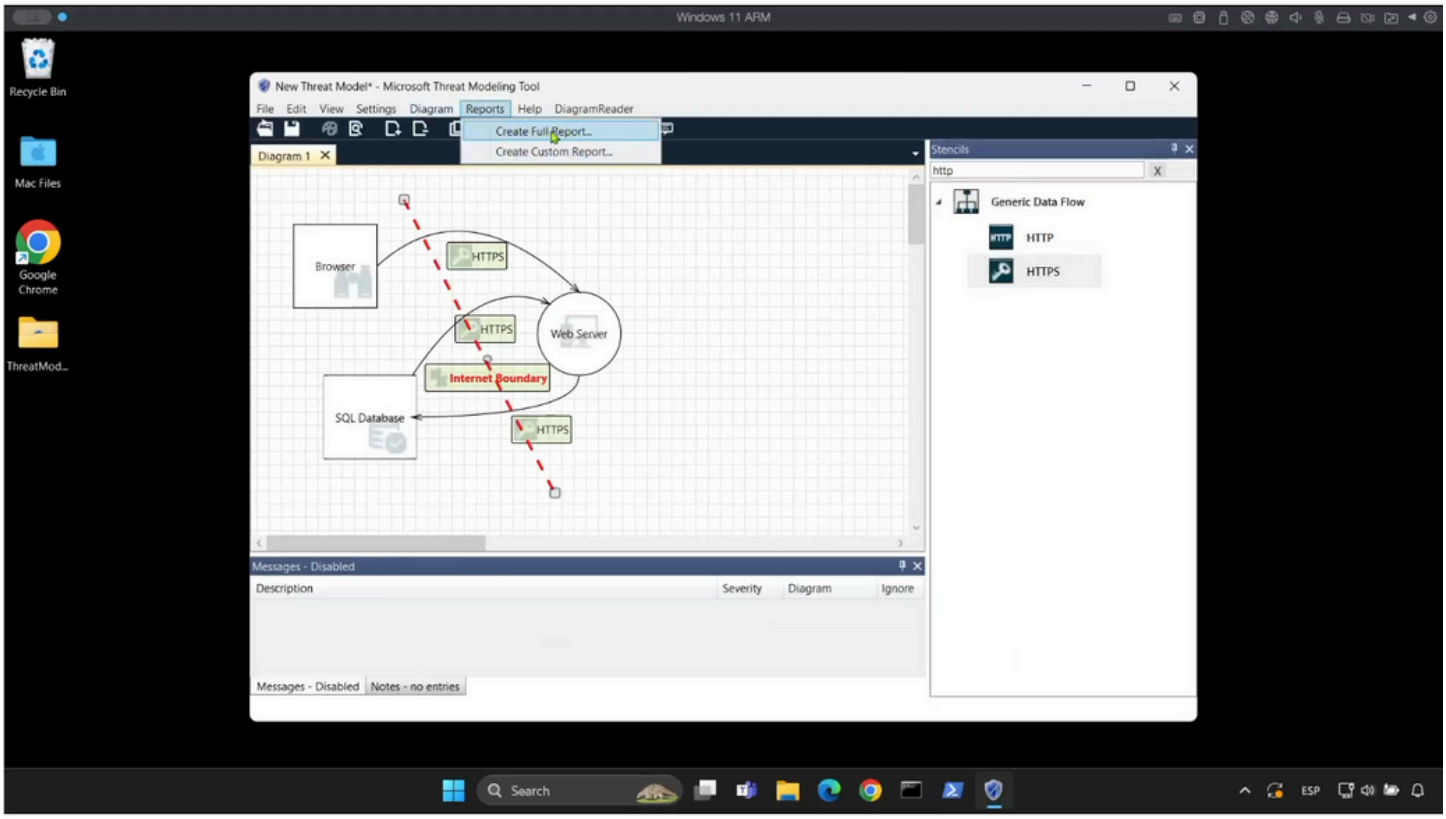

Windows 11 ARM
Recycle Bin
Mac Files
Google Chrome
ThreatMod...
New Threat Model - Microsoft Threat Modeling Tool
File Edit View Settings Diagram Reports Help DiagramReader
Diagram 1
Stencils
Search Stencils
Generic Process
OS Process
Thread
Kernel Thread
Native Application
Managed Application
Thick Client
Browser Client
Browser and ActiveX Plugins
Web Server
Windows Store Process
Win32 Service
Web Application
Web Service
Virtual Machine
Messages - Disabled
Description
Severity
Diagram
Ignore
Messages - Disabled
Notes - no entries
Search
ESP


Windows 11 ARM
Recycle Bin
Mac Files
Google Chrome
ThreatMod...
New Threat Model* - Microsoft Threat Modeling Tool
File Edit View Settings Diagram Reports Help DiagramReader
Diagram 1
Web Server
Stencils
Search Stencils
Generic Process
OS Process
Thread
Kernel Thread
Native Application
Managed Application
Thick Client
Browser Client
Browser and ActiveX Plugins
Web Server
Windows Store Process
Win32 Service
Web Application
Web Service
Virtual Machine
Messages - Disabled
Description
Severity
Diagram
Ignore
Messages - Disabled
Notes - no entries
Search
ESP


Windows 11 ARM
Recycle Bin
Mac Files
Google Chrome
ThreatMod...
New Threat Model* - Microsoft Threat Modeling Tool
File Edit View Settings Diagram Reports Help DiagramReader
Diagram 1
Stencils
datab
Generic Data Store
SQL Database
Non Relational Database
SQL Database
Web Server
Messages - Disabled
Description
Severity
Diagram
Ignore
Messages - Disabled
Notes - no entries
Search
ESP


Windows 11 ARM
Recycle Bin
Mac Files
Google Chrome
ThreatMod...
New Threat Model* - Microsoft Threat Modeling Tool
File Edit View Settings Diagram Reports Help DiagramReader
Diagram 1
Stencils
http
Generic Data Flow
HTTP
HTTPS
Browser
HTTPS
HTTPS
Web Server
Internet Boundary
SQL Database
HTTPS
Messages - Disabled
Description
Severity
Diagram
Ignore
Messages - Disabled
Notes - no entries
Search
ESP


Windows 11 ARM
Recycle Bin
Mac Files
Google Chrome
ThreatMod...
New Threat Model* - Microsoft Threat Modeling Tool
File Edit View Settings Diagram Reports Help DiagramReader
Diagram 1
Stencils
http
Generic Data Flow
HTTP
HTTPS
Browser
SQL Database
Dataflow for Diagram Diagram 1
Source name and type Web Server is connected to name and type SQL Database using name and type HTTPS which crosses through Line Boundary name and type Internet Boundary.
Source name and type SQL Database is connected to name and type Web Server using name and type HTTPS which crosses through Line Boundary name and type Internet Boundary.
Source name and type Browser is connected to name and type Web Server using name and type HTTPS which crosses through Line Boundary name and type Internet Boundary.
Press OK to return to main window
OK
Messages - Disabled
Description
Messages - Disabled
Notes - no entries
Search
ESP


Windows 11 ARM
Recycle Bin
Mac Files
Google Chrome
ThreatMod...
New Threat Model* - Microsoft Threat Modeling Tool
File Edit View Settings Diagram Reports Help DiagramReader
Create Full Report...
Create Custom Report...
Diagram 1
Stencils
http
Generic Data Flow
HTTP
HTTPS
Browser
HTTPS
HTTPS
Web Server
Internet Boundary
SQL Database
HTTPS
Messages - Disabled
Description
Severity
Diagram
Ignore
Messages - Disabled
Notes - no entries
Search
ESP

Threat Modeling

- STRIDE
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure
  - Denial of service
  - Elevation of privileges

Threat Modeling

- Ignore the risk – Not advisable
- Avoid the risk – Architectural redesign
- Accept the risk – Documentation without action
- Transfer the risk – Transfer to another team
- Confront the risk – Implementation of the fix

Threat Modeling

Reports

https://owasp.org/www-project-web-security-testing-guide/v42/5-Reporting/README

Picture source: own creation