MICROSOFT THREAT MODELING

25-7-2023

Cyber Evangelists

TABLE OF CONTENT

OVERVIEW

Microsoft Threat Modeling Tool 2016 is an easy-to-use tool that can:

- Create data flow diagrams (DFDs) for products or services.
- Analyze data flow diagrams to automatically generate a set of potential threats.
- Suggest potential mitigations to design vulnerabilities.
- Produce reports on the identified and mitigated threats.
- Create custom templates for threat modeling.

MICROSOFT THREAT MODELING

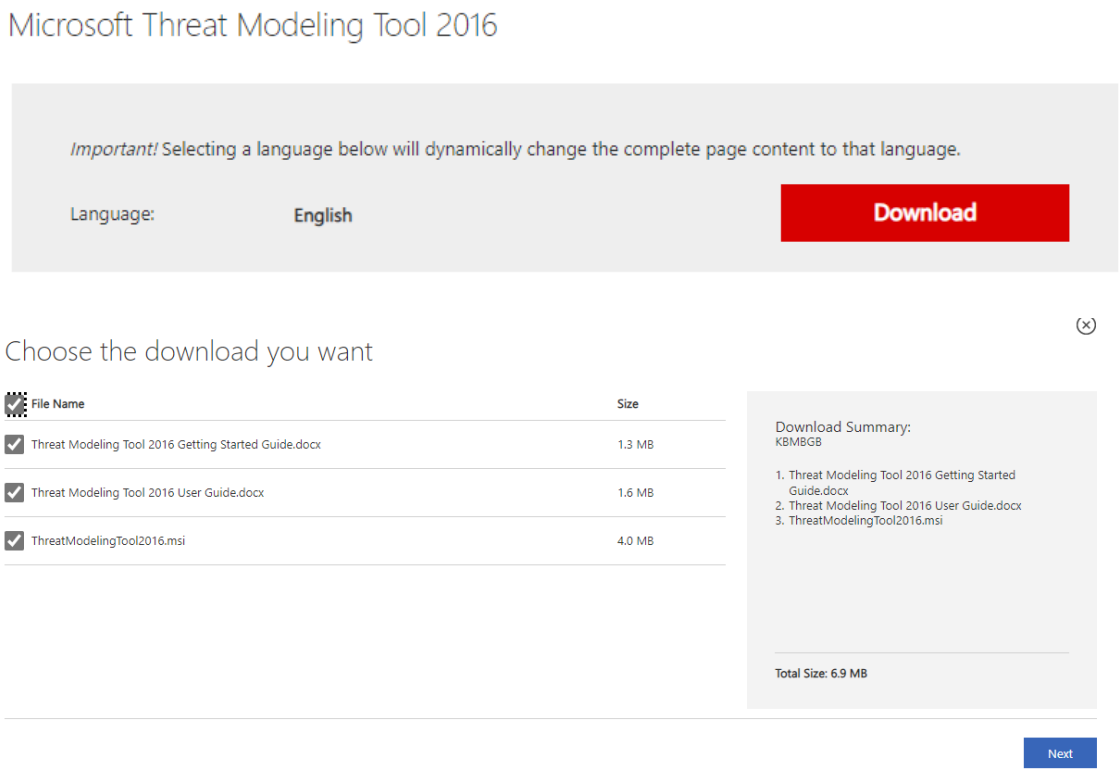
Microsoft Threat Modeling is a structured approach and toolset for identifying and addressing security threats in software applications and systems, promoting proactive cybersecurity.

Why do we use it?

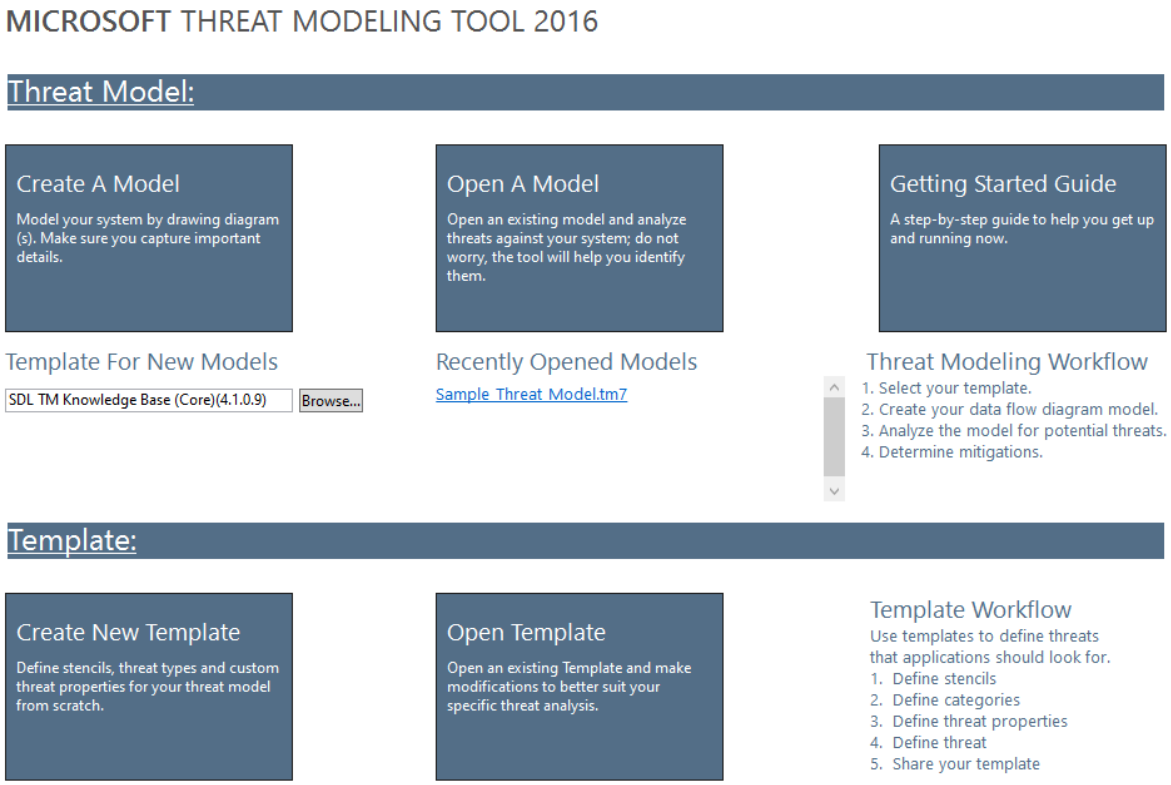
These tools help security professionals and developers visualize, analyze, and mitigate risks early in the development process, resulting in more secure and robust software. Additionally, Microsoft Threat Modeling Tools integrate well with other Microsoft security solutions, making them a convenient and effective choice for threat modeling in Microsoft environments.

How do we use it?

1. Download and install the Microsoft Threat Modeling Tool on your computer.



2. Create a new model: Launch the tool and start a new threat model project.



3. Define the System: Define the boundaries of your system, including components, data flows, and interactions. In this scenario, we create a simple design of a web application developed to interact with third-party service in between internet boundaries defined (External or Internal network)

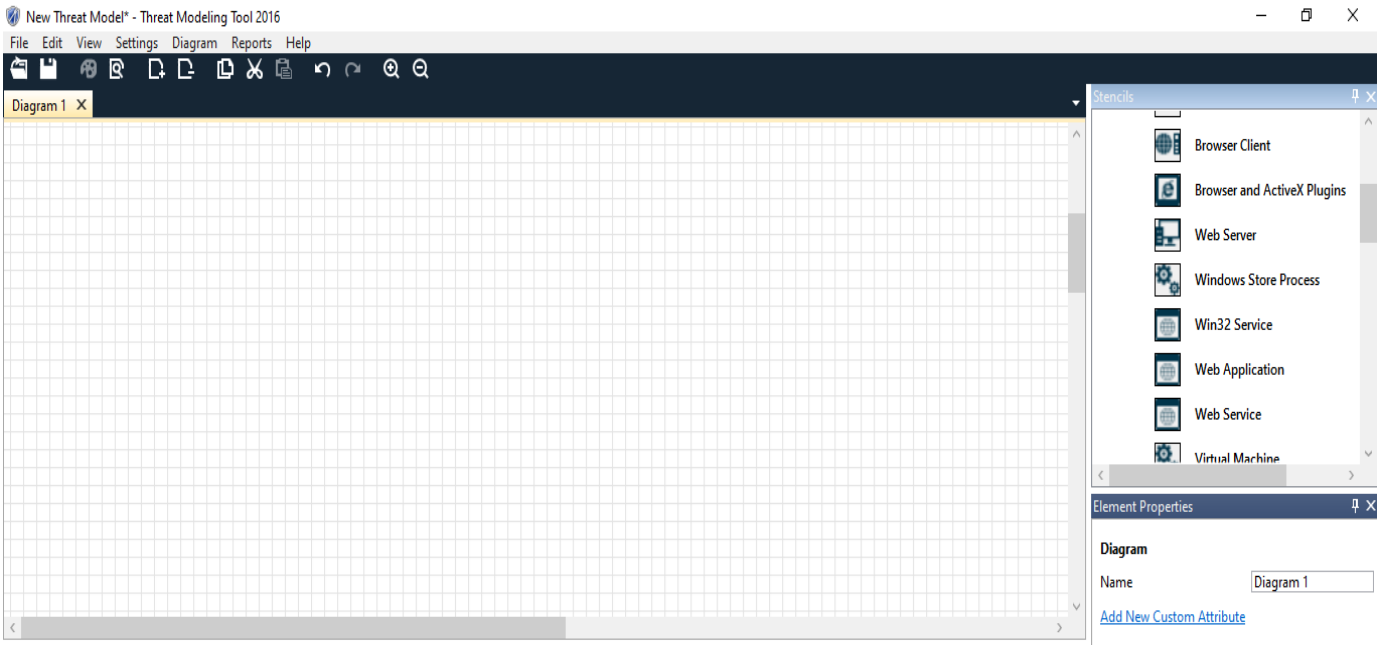


Figure 1Design view

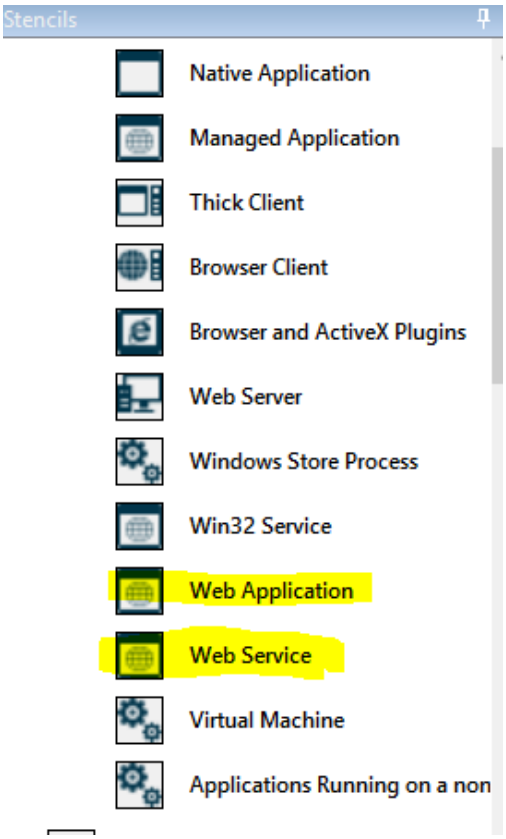


Figure 2 Select web Applications and Web services.

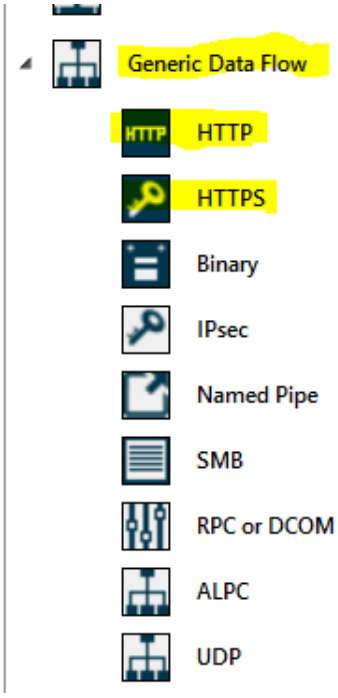


Figure 3: Go to Generic Data Flow and Select HTTP or HTTPS

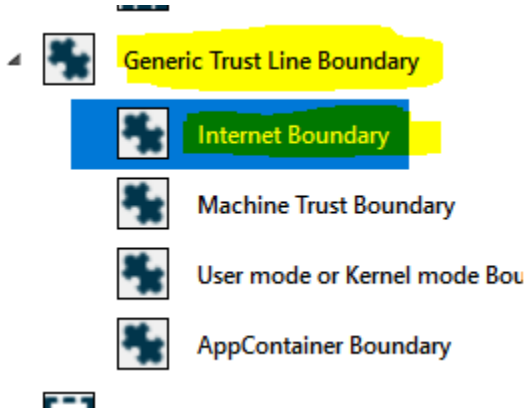


Figure 4 Goto generic Trust Line Boundary and select the Internet Boundary.

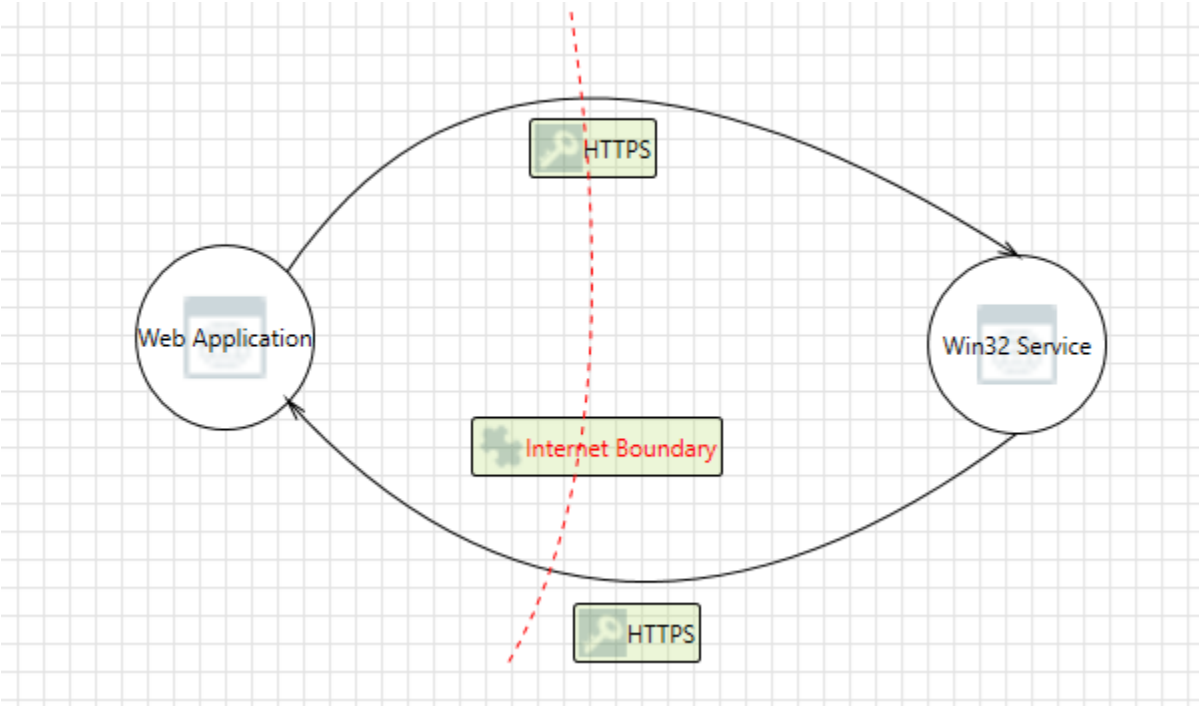


Figure 5 System Design

4. Analyze Design: After creating the design analyze potential threats that might occur.

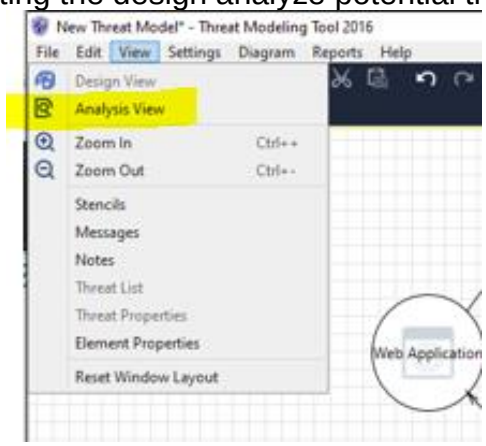


Figure 6 Click View and then Analyze View.

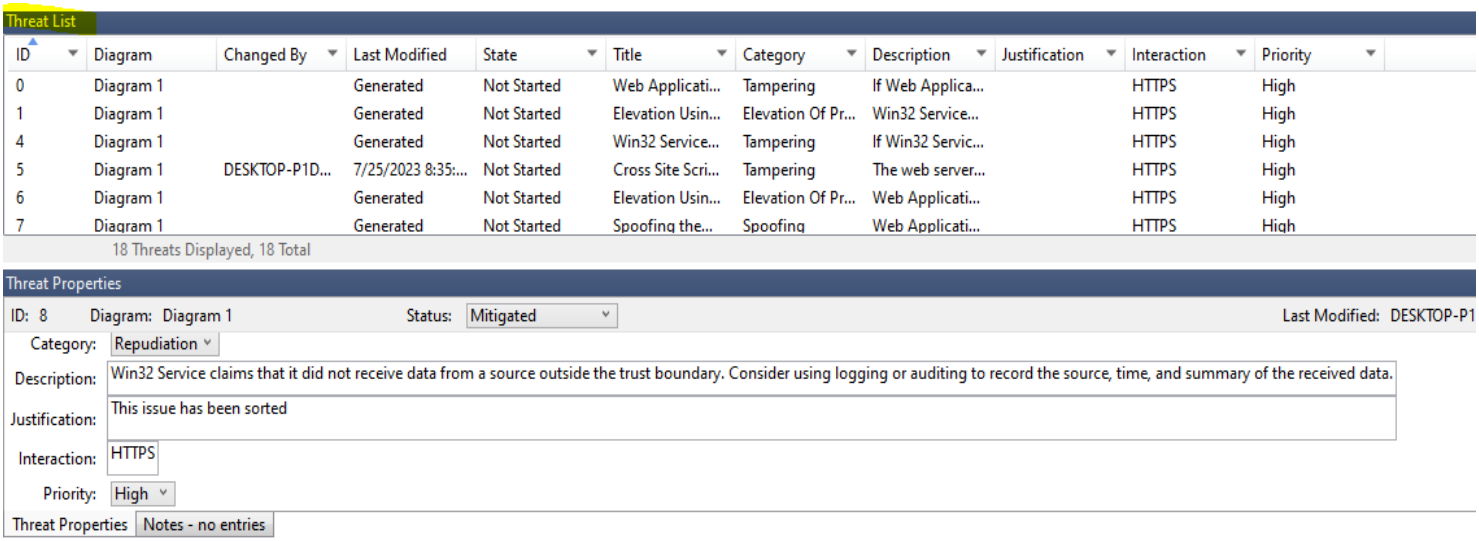
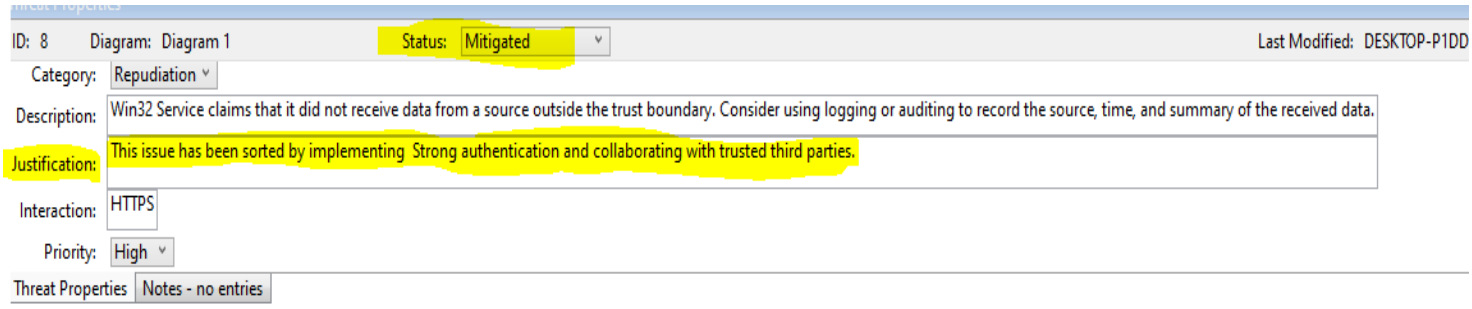
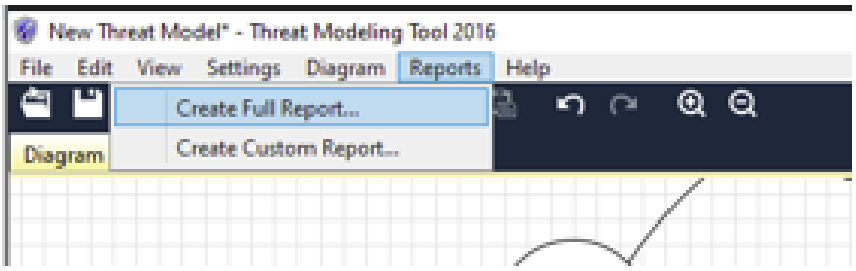


Figure 7 Threat List with Description

5. Mitigate: A risk can be mitigated with proper justification after analysis by security teams.



6. Generate Report: Now you can download full or custom reports after analyzing lists of threats.



Threat Modeling Report

Created on 7/25/2023 10:43:06 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	17
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	1
Total	18
Total Migrated	0

Diagram: Diagram 1

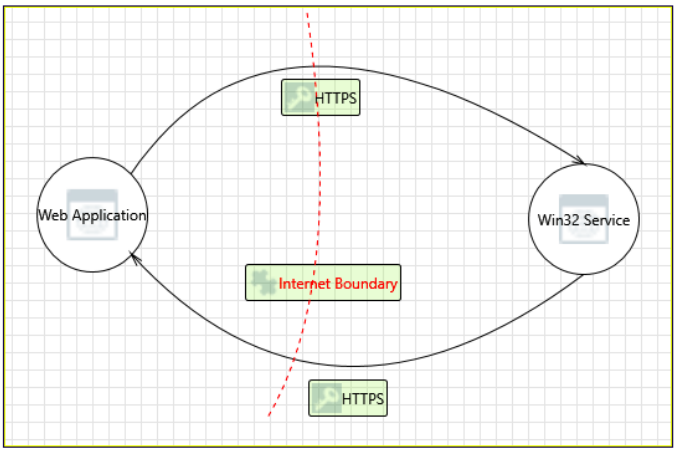
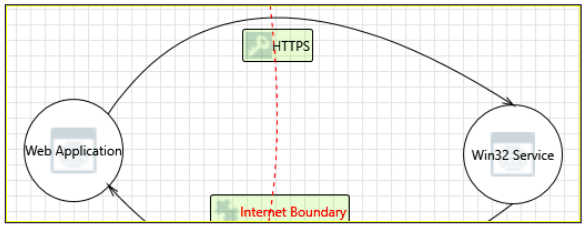


Diagram 1 Diagram Summary:

Not Started	17
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	1
Total	18
Total Migrated	0

Interaction: HTTPS



1. Web Application Process Memory Tampered [State: Not Started] [Priority: High]

Category: Tampering
Description: If Web Application is given access to memory, such as shared memory or pointers, or is given the ability to control what Win32 Service executes (for example, passing back a function pointer.), then Web Application can tamper with Win32 Service. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.
Justification: <no mitigation provided>

2. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Win32 Service may be able to impersonate the context of Web Application in order to gain additional privilege.
Justification: <no mitigation provided>

7. Review and Iterate: Review the model with stakeholders and iterate as necessary to improve security.

By following these steps, you can effectively use the Microsoft Threat Modeling Tool to enhance the security of your software applications and systems.

CONCLUSION

Microsoft Threat Modeling Tool 2016 is an easy-to-use tool for creating data flow diagrams, identifying threats, suggesting mitigations, and producing reports. It promotes proactive cybersecurity and helps visualize and address risks during software development. Integrates well with Microsoft security solutions for convenience.