OPUS

White paper

Threat Modeling

A Shift Left Strategy for Building Secure Payment Software



Table of Contents

	Page
Executive Summary	03
Introduction	03
Why Threat Modeling is Mandatory for All Financial Organizations	04
Threat Modeling Methodologies in the Industry	05
Basic Threat Modeling Process	06
Benefits of Threat Modeling	07
Threat Modeling Example	08
Threat Modeling Using Microsoft Threat Modeling Tool – A Guide	10
Challenges and Considerations	13
Best Practices	14
Conclusion	15

© 2026, Opus Technologies

Executive Summary

Threat modeling is a proactive approach to cybersecurity that helps organizations identify, assess, and mitigate potential threats and vulnerabilities in their systems and applications. By systematically analyzing the security of their assets, organiza-tions can make informed decisions about risk management and prioritize security measures effectively. Threat modeling has become an integral part of the modern application development and is embedded as an activity performed during the Design Phase of the DevSecOps lifecycle. This shift left approach of adding security into the design phase is bene fi ting many organiza-tions by improving security and lowering the cost of fi xing vulnerabilities by identifying vulnerabilities early in the Software life-cycle.

Threat modeling aims at answering essential questions, such as:

- What are the critical assets and resources to protect?
- What are the potential threats to these assets?
- How might attackers exploit vulnerabilities?
- What are the potential consequences of a successful attack?

By addressing these questions, application teams can take proactive steps to strengthen their security posture, reduce the attack surface, and allocate resources effectively.

This whitepaper provides an in-depth overview of threat modeling, its importance, methodologies, and best practices, as well as the bene fi ts it offers to organizations by showcasing an actual use case using Microsoft's threat modeling tool.

Introduction

In today's digital age, where cyberthreats are evolving at an alarming rate, organizations must proactively safeguard their information systems and applications. Threat modeling is a structured approach that helps organizations understand their vulnerabilities, anticipate potential threats, and develop strategies to mitigate these risks.

Financial software is most prone to such attacks, which makes security one of the most imperative aspects of software development in the fi nancial domain.

> It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it.
>
> **— Stéphane Nappo, CISO, Société Générale International Banking**

© 2026, Opus Technologies

Why Threat Modeling is Mandatory for All Financial Organizations

According to the Threat Modeling Manifesto, “When you perform threat modeling, you begin to recognize what can go wrong in a system” and this is the most significant reason for this being an essential phase in the financial software development lifecycle.

Furthermore, the adoption of threat modeling in the Software Development practice is fundamental for several other reasons as shown below

Exhibit 1: Factors Driving Adoption of Threat Modeling in the Software Development Practice

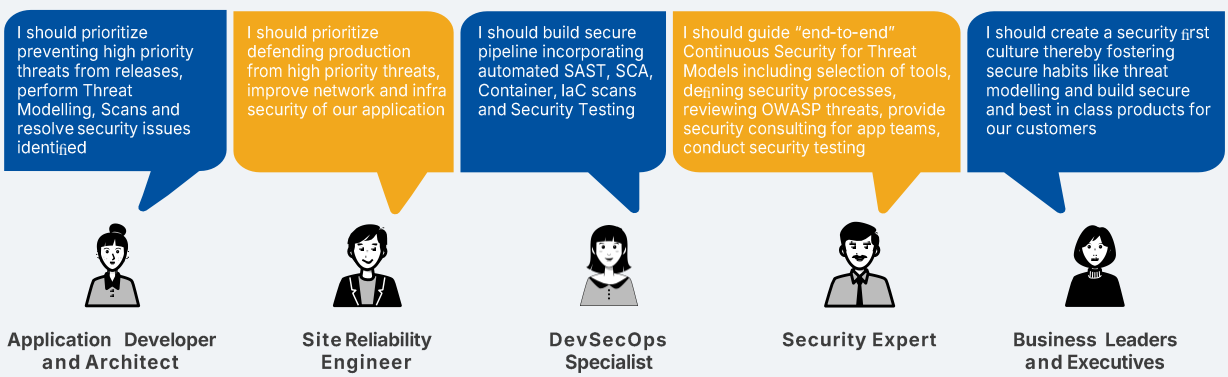
Risk Reduction
It helps prioritize security measures by focusing on high-impact threats and vulnerabilities, reducing the likelihood of successful attacks

Cost Savings
By identifying vulnerabilities early in the development cycle, organizations can save significant resources by addressing issues before they become expensive to fix at a later stage

Compliance
Many regulatory frameworks and standards, such as GDPR and ISO 27001, require organizations to conduct risk assessments and demonstrate proactive security measures. Threat modeling is one such method and introducing it early in the cycle makes companies compliant from the get-go

Security Awareness
Adopting this encourages a security-conscious culture within organizations, wherein all stakeholders, including developers and testers, understand the important of security in software lifecycles

Exhibit 2: Personas involved in Threat Modeling



© 2026, Opus Technologies

Threat Modeling Methodologies in the Industry

There are several threat modeling methodologies that exist today, and they can be employed depending on an organization's specific needs. Some of the widely recognized methodologies are:

Exhibit 3: Threat Modeling Methodologies

Stride
STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) is a framework developed by Microsoft. It segregates threats into six main categories and helps in identifying potential vulnerabilities based on these categories

Dread
DREAD (Damage, Reproducibility, Exploitability, Affected Users, and Discoverability) is a threat modeling approach that assigns scores to each of these categories to assess the severity of a threat

Octave
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk assess-ment methodology developed by the Software Engineering Institute (SEI). It focuses on identifying assets, threats, vulnerabilities, and assessing risks using a structured approach

Attack Trees
Attack trees are graphical representations that illustrate potential attack paths, starting from the root threat and branching out into various attack vectors. This method helps in visualizing complex attack scenarios

Kill Chain
The kill chain model, often associated with military and intelligence, outlines the stages of a cyberattack, from reconnaissance to exfiltration. Understanding the kill chain can aid in threat modeling by identifying points of intervention and disruption

Some of the other notable frameworks are PASTA (process for attack simulation and threat analysis), VAST, NIST (National Institute of Standards and Technology's framework), and Trike.

© 2026, Opus Technologies

Basic Threat Modeling Process

01

Identify Assets

Identify and catalog all the assets, systems, and data that need protection. This includes all the network, hardware, software, data repositories, and resource personnel

02

Identify Threats

According to Stephane Nappo, “Threat is a mirror of security gaps.” Hence, this particularly important step involves teams identifying potential threats and threat actors that could target the specific asset. Consider external threats like hackers and malware and internal threats like human negligence while identifying them

03

Identify Vulnerabilities

Determine vulnerabilities within the system or application, including the infrastructure where its workloads will be running, be it cloud or on-premises. This includes weaknesses in the software, configurations, access controls, and physical security

04

Assess Risks

Evaluate the impact and likelihood of each threat exploiting a vulnerability. Assign risk scores based on methodologies, like DREAD or qualitative assessments, to prioritize them

05

Mitigate Risks

Develop and implement strategies to mitigate identified risks. This may involve implementing security controls, updating software code or configurations, adding new components to the application, like storing keys in vaults instead of config files, training organizational staff, or changing existing processes

© 2026, Opus Technologies

Benefits of Threat Modeling

Robbie Sinclair, Head of Security, Country Energy, NSW said, “Security is always excessive until it’s not enough.” Threat modeling’s biggest benefit is that it ensures you add more security to the “not enough” by building an even more secure product than before.

It offers several significant benefits to organizations. Some of the key benefits of performing Threat Modeling are:

Exhibit 4: Business and Operational Benefits of Threat Modeling



Early Detection of vulnerabilities, leading to significant reduction of cost and effort



Helps teams to prioritize risks and security measures based on the criticality of assets and the severity of potential threats



Improves Decision-Making in risk management and resource allocation



Improves Compliance through risk assessments and proactive security measures



Helps reduce the attack surface of the application by identifying potential risks and their mitigations



Helps improve security awareness in the organization and fosters a security-first culture within the organization through constant communication and collaboration between various teams and stakeholders



Adds to the agility of the organization, by allowing teams to deliver secure apps faster, while teams continuously improve through its adoption

© 2026, Opus Technologies

Threat Modeling Example

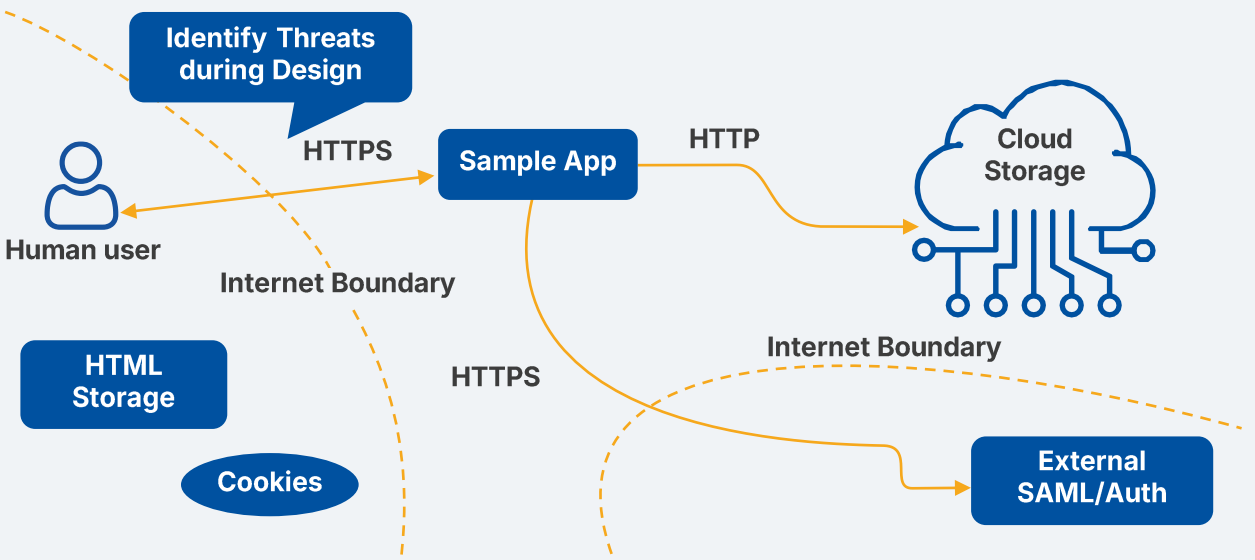
Threat modeling can be explained with a simple scenario as depicted below. This is a simple web application that is exposed over the internet and is accessed by the user over https. The application talks to cloud storage as the datastore and connects with SAML for authorization.

One of the primary activities in threat modeling is to identify the obvious potential threat areas and, in this case, it is the inter-net boundary that can be exploited by malicious parties to gain access to the internal systems. These threats need to be identi-fied during the design phase and solutions to mitigate risks around them need to be put in place.

These mitigations can be as simple as adding basic authorization, token-based authorization, input validation, encryption of the data including redating SPI, adding throttling, metering or a WAF layer on the APIs to make them secure.

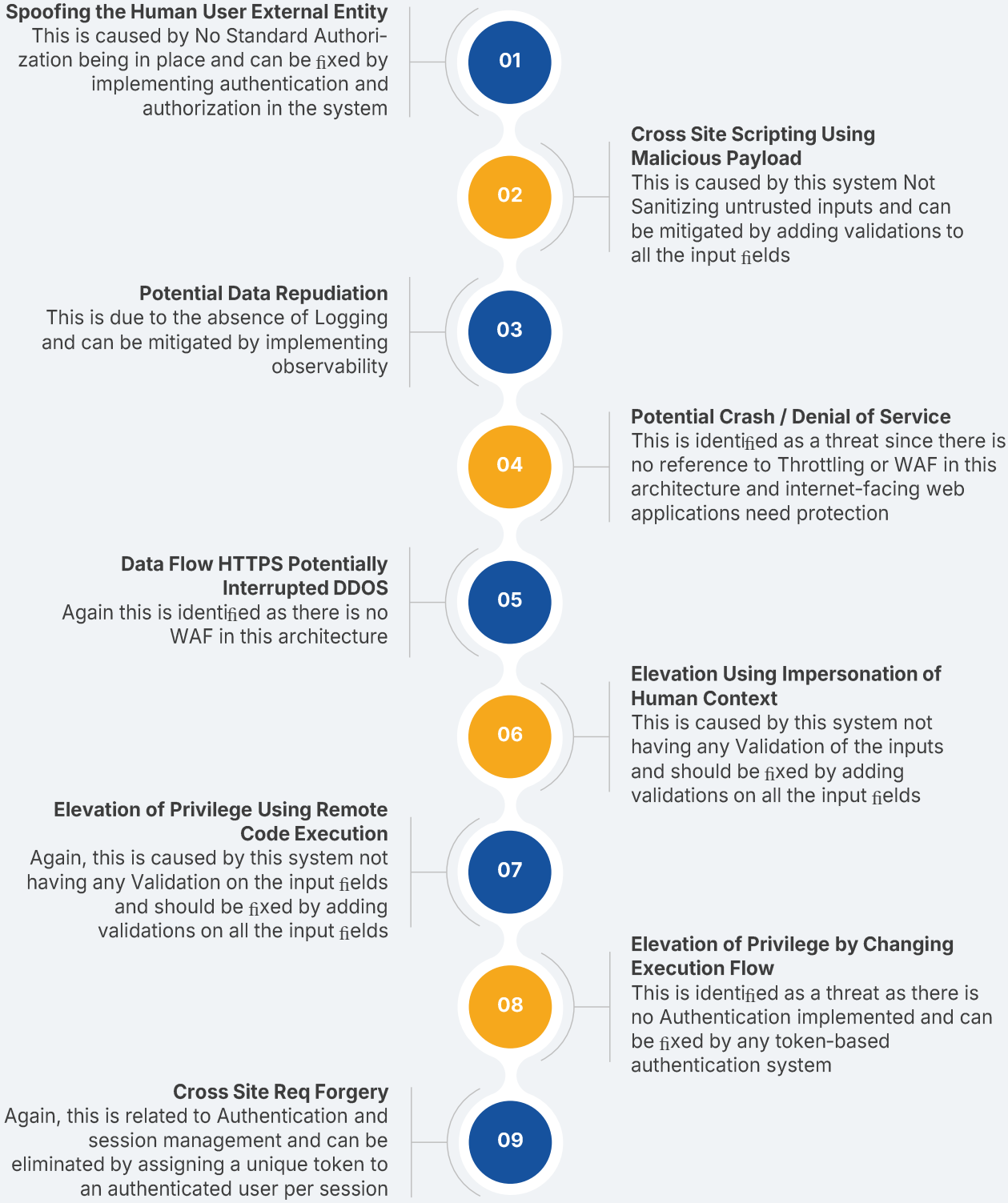
We ran this architecture with a basic threat modeling tool and following are the potential vulnerabilities that were identified in this architecture.

Exhibit 5: Sample Threat Model Diagram



© 2026, Opus Technologies

Exhibit 6: Sample Threat Model Result Derived from the Previous Diagram are Listed Below



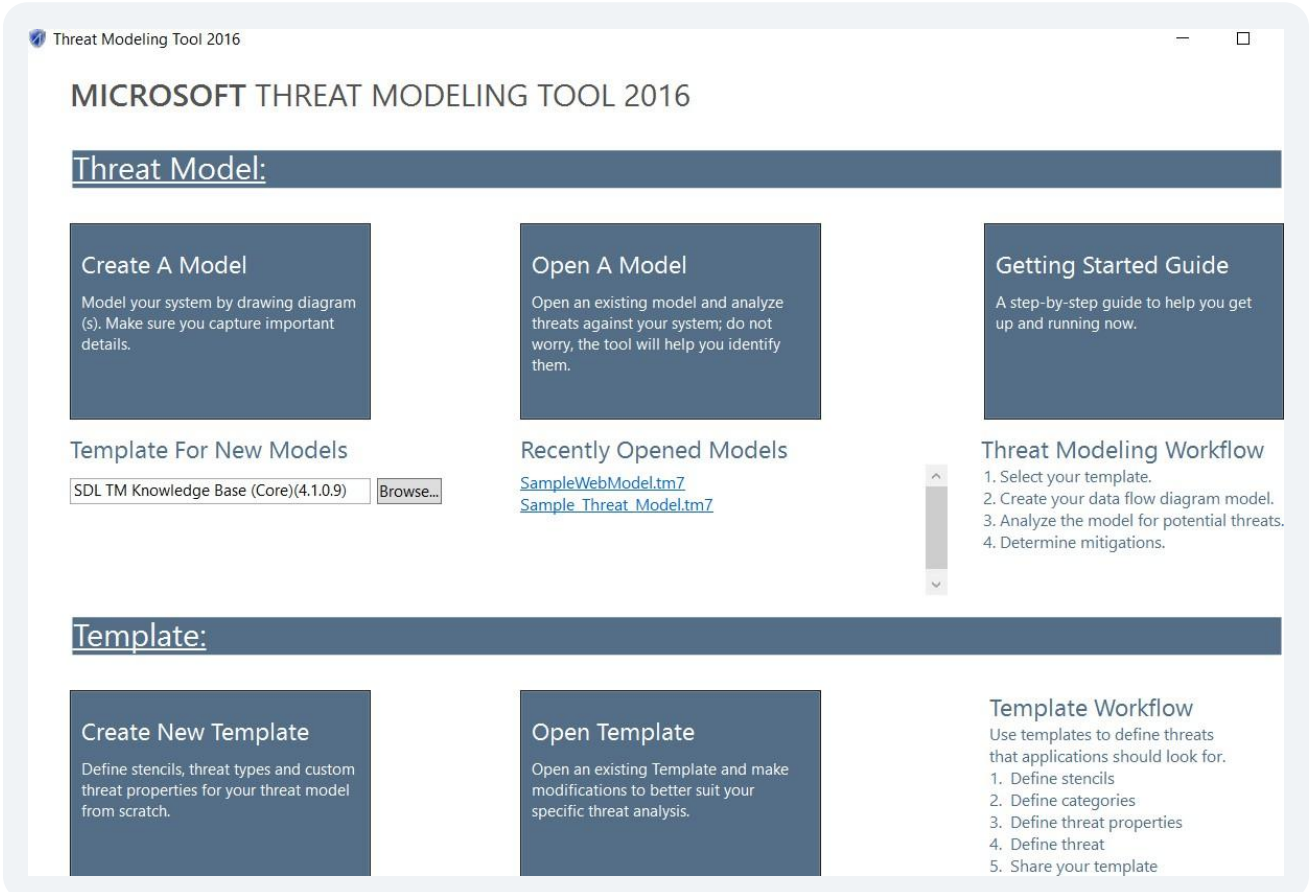
© 2026, Opus Technologies

Threat Modeling Using Microsoft Threat Modeling Tool – A Guide

Microsoft's Threat Modeling tool, although basic, is an immensely powerful tool with a smaller learning curve. It is very popular among developers building applications, and several teams employing Secure Coding Practices use it extensively during the design phase. In this section, let's look at how you can use the tool for threat modeling for your projects.

Download and install the Microsoft package for the tool. When you open the tool, this is what you see, and you can click on 'Create A Model' to build one.

In the Create Model screen, you can drag and drop stencil items from the right menu to build your model. For instance, if you are building a web application and wish to create a threat model for this, click on the 'Web Application' option on the menu as shown and the item appears on the model.



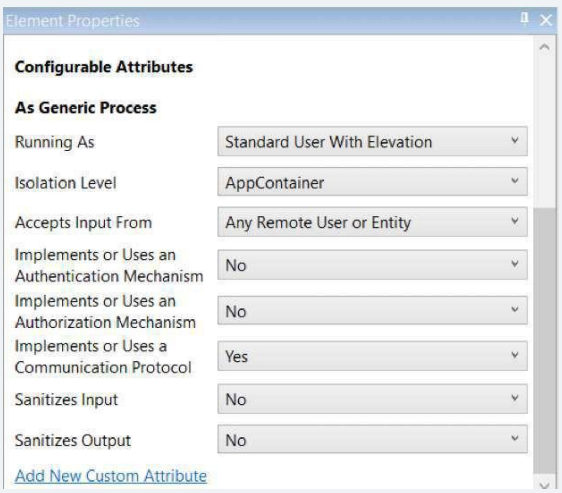


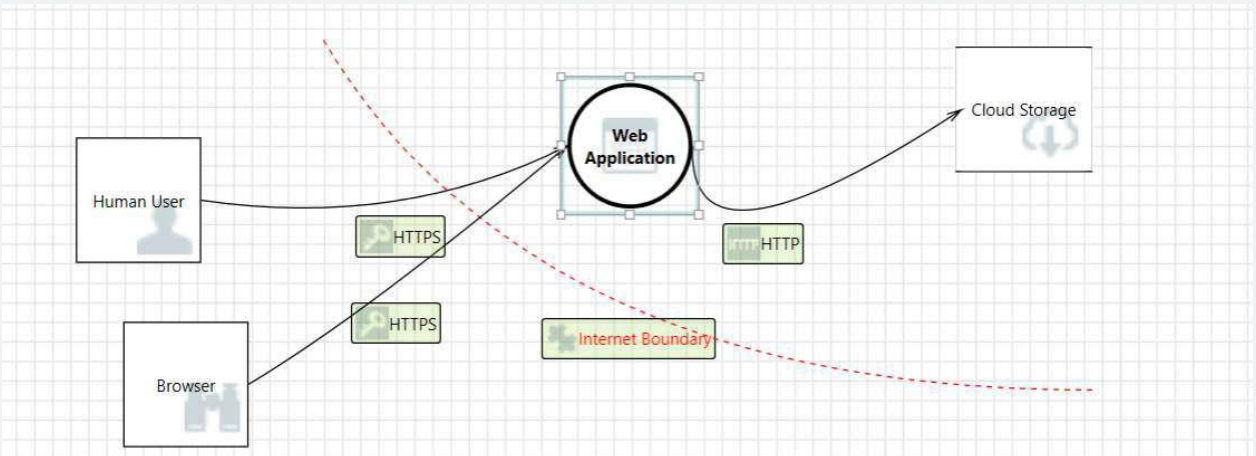
You can also configure the attributes of the component. For instance, for a web application, you can consider aspects like - is it running in a container, does the web app validate input and output, is there an authentication mechanism in place, etc.

These attributes play a key role in analyzing threats. For example, if your web app does not validate Inputs, it would be susceptible to Cross Site Scripting.

Similarly, you can define Internet boundaries, select users like human user, define traffic protocols and databases and build the model for an entire application.

The example threat model below is a complete web application that connects to a cloud storage and is accessed by human users via browsers over the inter-net using https protocol. We have defined the properties with weaker security aspects to demo the vulnerabilities here.

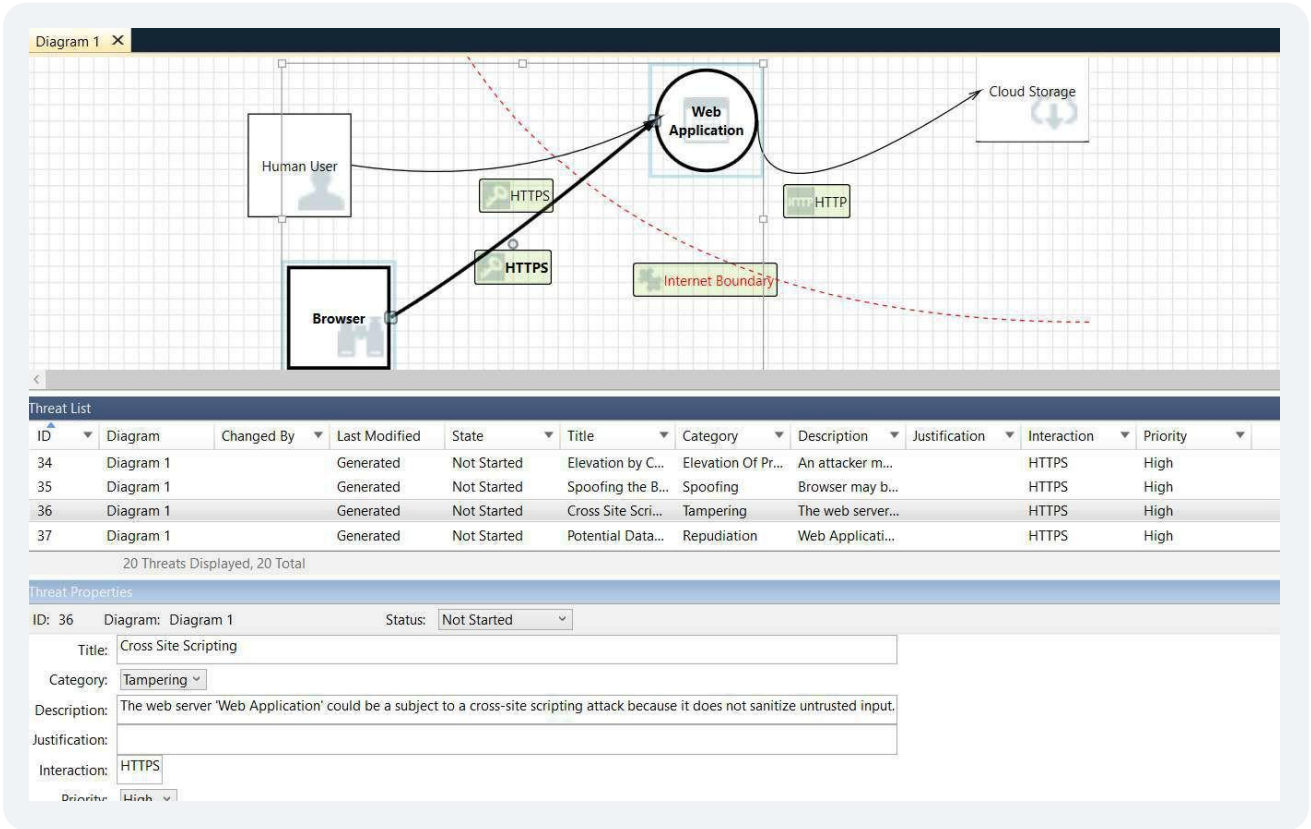




Go to Menu → View → Analysis View to start looking at the Threat Analysis

© 2026, Opus Technologies

The image below shows the Analysis view and how the threats can be viewed and understood based on the description. The description also provides suggestions to resolve the issues.



You can also download the report into your system to further investigate, discuss and make decisions. A sample report for this example case is attached below.

Threat Model Report.htm

Challenges and Considerations

While threat modeling is a valuable practice, it comes with challenges, such as complexity, resource requirements, and the need for expertise. Application teams must also consider that threat landscapes evolve, and threat models should be continu-ously updated to remain effective. Here are some of the major challenges organizations face while implementing threat modeling:

Exhibit 7: Implementation Barriers – Key Challenges and Strategic Considerations

Cultural Change	The people factor is always primary in such initiatives and creating a security-first culture is a big challenge for most organization, as it involves changing the mindsets of the people who constitute the organization. Further, integrating threat modeling in the SDLC cycle also is a substantial change for development teams and needs them to accept and adapt the new process
Skills and Training	This requires resources with Security skillsets that goes beyond the general skills of application development and networking. Hence, finding the right set of resources is always a challenge
Biased Models	Threat models can often create a bias and lead teams to overlook other potential threats that were not identified during this activity. Expert opinions and analysis need to be in place to eliminate biased models
Budget and Effort	Integrating this activity in the SDLC cycle increases the cost of development at the beginning and might be a challenge for teams with limited budget and resources
Time to Market	Although it is supposed to alleviate the process, it often adds to the lead time of the product, due to which the process needs to be reviewed properly and curated to ensure it brings in efficiency to the entire release process
Managing Complexity	Modern systems and architecture are complex and are continuously evolving. Hence, ensuring the right threat model is created for such systems and are updated regularly is a big challenge for large systems. A dedicated centralized team governing application teams is inevitable for larger organizations due to this reason

© 2026, Opus Technologies

Best Practices

Exhibit 8: Strategic Pillars for Effective Threat Modeling

Involve All Stakeholders 01

Collaborate with developers, architects, security experts, and business units to ensure a comprehensive threat model. This also adds diverse perspectives while building the model

Use the Right Methodology 02

Choose a threat modeling methodology that suits your team's goals and expertise

Regular Updates 03

Keep threat models up-to-date to reflect changing technologies and threat landscapes

Integration 04

Integrate threat modeling into the design phase of the software development lifecycle, for maximum effectiveness

Training 05

Train and educate your teams with Secure Coding and continuously appraise them on OWASP top 10 vulnerabilities

Penetration Testing 06

Use threat modeling as an input for designing Penetration testing cases, making them more relevant by targeting the threats

© 2026, Opus Technologies

Conclusion

In February 2023, customers running workloads in VMware ESXi hypervisors became the victims of a deadly attack exploiting a two-year old vulnerability. Post that attack, VMWare said, “The important truth is that virtual infrastructure is a high-value target, precisely because organizations run their most important workloads there, and that threat actors are continuously evolving their tools and tactics to work in those environments.” This statement emphasizes the importance of embedding security early in the financial software ecosystem’s lifecycle to prevent such incidents.

Threat modeling is one of those vital activities. It is deemed as an important component of modern Secure Application Development Methodology and by systematically identifying and mitigating potential threats and vulnerabilities, application teams can enhance their security posture, reduce risks, and protect their critical assets.

Opus: Your Trusted Partner in Building Secure Solutions

At Opus, we consider security as a top priority item while building and transforming your financial software. Our teams are trained to write secure code, consult, and recommend software tools for SAST, Container and SCA scans and are adept at per-forming threat modeling while designing software. This is an integral part of the Agile Software Development Process followed by our team. Opus can help you in your Continuous Improvement journey by establishing and embedding the threat modeling processes within your development cycle and empower your teams with Secure Coding processes.

© 2025, Opus Technologies

Author



Debashis Bhattacharyya
Technology Consulting Leader

Debashis Bhattacharyya has over 18 years of experience planning and delivering technology solutions, specializing in Cloud, API, DevSecOps and Application Modernization. He has been instrumental in Opus' transformational DevOps initiative with FIS that won the prestigious DevOps Dozen Award for 'Best DevOps Industry Implementation' in 2022..

© 2026, Opus Technologies



Opus is a trusted engineering partner to payment providers, banks and fintechs navigating change in a real-time, digital-first world. We solve for business value—accelerating go-to-market, unlocking future readiness, and powering transformation at scale.

Our promise is simple: Business Value Acceleration. Realization. Maximization.

We deliver on this promise through the Opus trifecta—a domain-native engineering skillset, a value-creation mindset, and a toolset that drives business agility. From MVP (Minimum Viable Product to MPT (Maximum Possible Transformation), Opus turns engineering into business advantage.

Contact us

info@opustechglobal.com

www.opustechglobal.com

