Threat Modeling

Start where you are now

IriusRisk

« The path to threat modeling

In order to detect design errors in applications, many companies have found that static (SAST) and dynamic (DAST) security analysis tools are simply not enough. The failures found with these tools account for over half the security flaws detected when an application goes through into production, which are often the most expensive to correct in terms of resources and time invested. This is the reason why over the past few years many security teams are trying to adopt a shift left approach that goes further within the development cycle.

« But what is threat modeling?

Threat Modeling takes place in the design phase of a system or application. It focuses on using abstractions to help think and assess risks effectively. Gartner[1] frames this activity within the ASRTM (Application Security Requirements and Threat Management) category, focused on automating the definition of security requirements, risk assessment and Threat Modeling.

« Where do I start?

Implementing a security program that includes Threat Modeling involves a cultural and organizational change rather than a technical change. We want to avoid that this change has a paralyzing effect, so to get started here are some strategies that can help in this transition.

1. Communicate change and involve people

Any Threat Modeling tool should be a collaborative tool. Collaboration is based on trust, which means explaining what we are going to do and why it is in every stakeholders interest to do so. The first objective is to communicate the organizational change needed. This involves adapting the corporate development procedures to include Threat Modeling once the application architecture is defined. If it is not written in the procedures and approved by the PMO, it doesn't exist.

2. Start small

Don't be ambitious, it is important to start small for two main reasons: firstly, to overcome resistance to change; secondly so you can be sure you have enough resources to maintain the new Threat Modeling service. If you are going to ask other areas to get involved but you are not able to give an adequate response time, you run the risk of dying of success. We all know that it is often far easier to promote a new initiative than to revive a dead one. Start with a pilot approach, take a set of applications, and then grow from there.

References

[1] *2017 Hype Cycle for Data Security, https://www.gartner.com/doc/3772083*

3. Establish risk-based security pathways

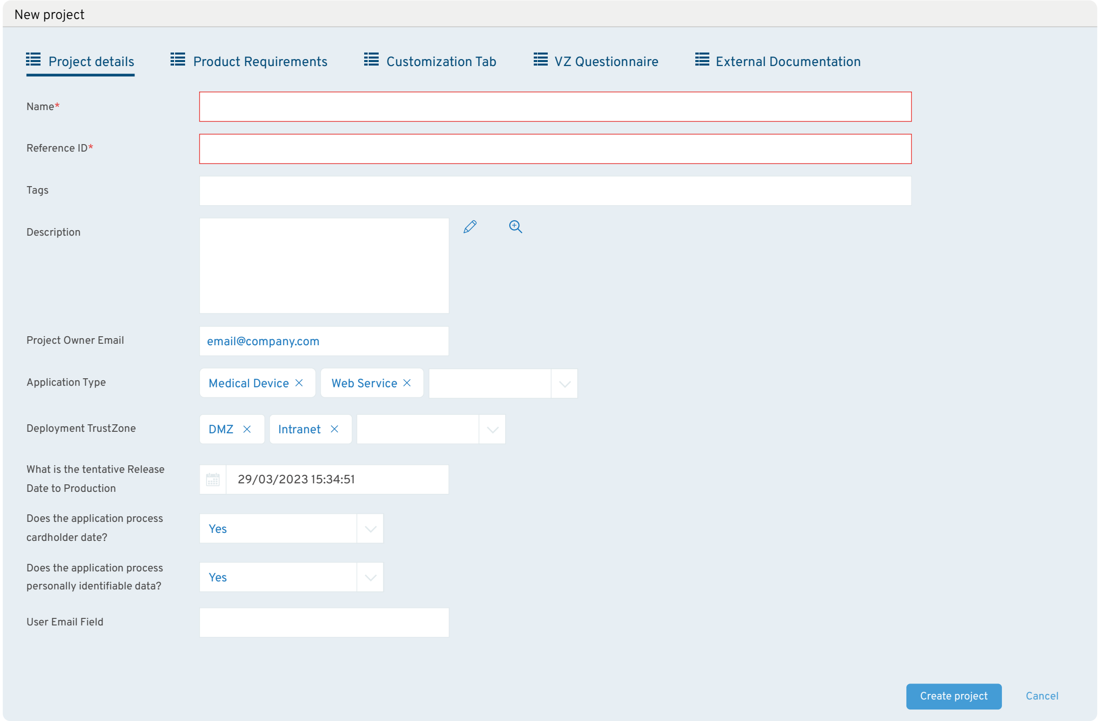
Not all applications are the same or have the same business value. Without a corporate-level understanding of risk appetite, it is not possible to establish a risk-based security strategy to improve the resources that are available.

A Threat Modeling tool can help you manage your resources more efficiently so you can make better decisions. An example of this could be the definition of different security pathways for applications based on a preliminary risk assessment. If it is an internal application based on a corporate archetype which has the approval from security, it may be enough to do security tests in pre-production.

Define the threat path

On the other hand, if an application handles card and customer data, it would be reasonable to require a path in which static code security analysis, unit security control tests, and external security tests are carried out before going into production.

We can define these paths manually, though it is far more useful to automate the process so the project manager can obtain the security pathways for his application without directly involving the security team. An example of this type of initiative with IriusRisk[2] is shown in Figure 1.



Name*	
Reference ID*	
Tags	
Description	
Project Owner Email	email@company.com
Application Type	Medical Device × Web Service ×
Deployment TrustZone	DMZ × Intranet ×
What is the tentative Release Date to Production	29/03/2023 15:34:51
Does the application process cardholder date?	Yes
Does the application process personally identifiable data?	Yes
User Email Field	

Figure 1.

Based on the answers of the project manager, the Threat Modeling tool will automatically generate the necessary tasks in the ALM tool so that traceability of the defined security path is ensured.

References

[2] *IriusRisk - Threat Modeling Tool, https://www.iriusrisk.com/threat-modeling-platform*

4. Automate the delivery security requirements

Security requirements must exist outside the security team. They should be published, challenged, improved and adapted to the agreed business risk appetite and regulatory compliance needs.

IriusRisk can automatically generate threat models and its associated security requirements, without having to rely on a security analyst. For this, the development team must define the architecture of the application. There are mainly two (nonexclusive) ways of achieving this. The first is to draw a diagram of the components, assets as shown in the example in *Figure 2.*

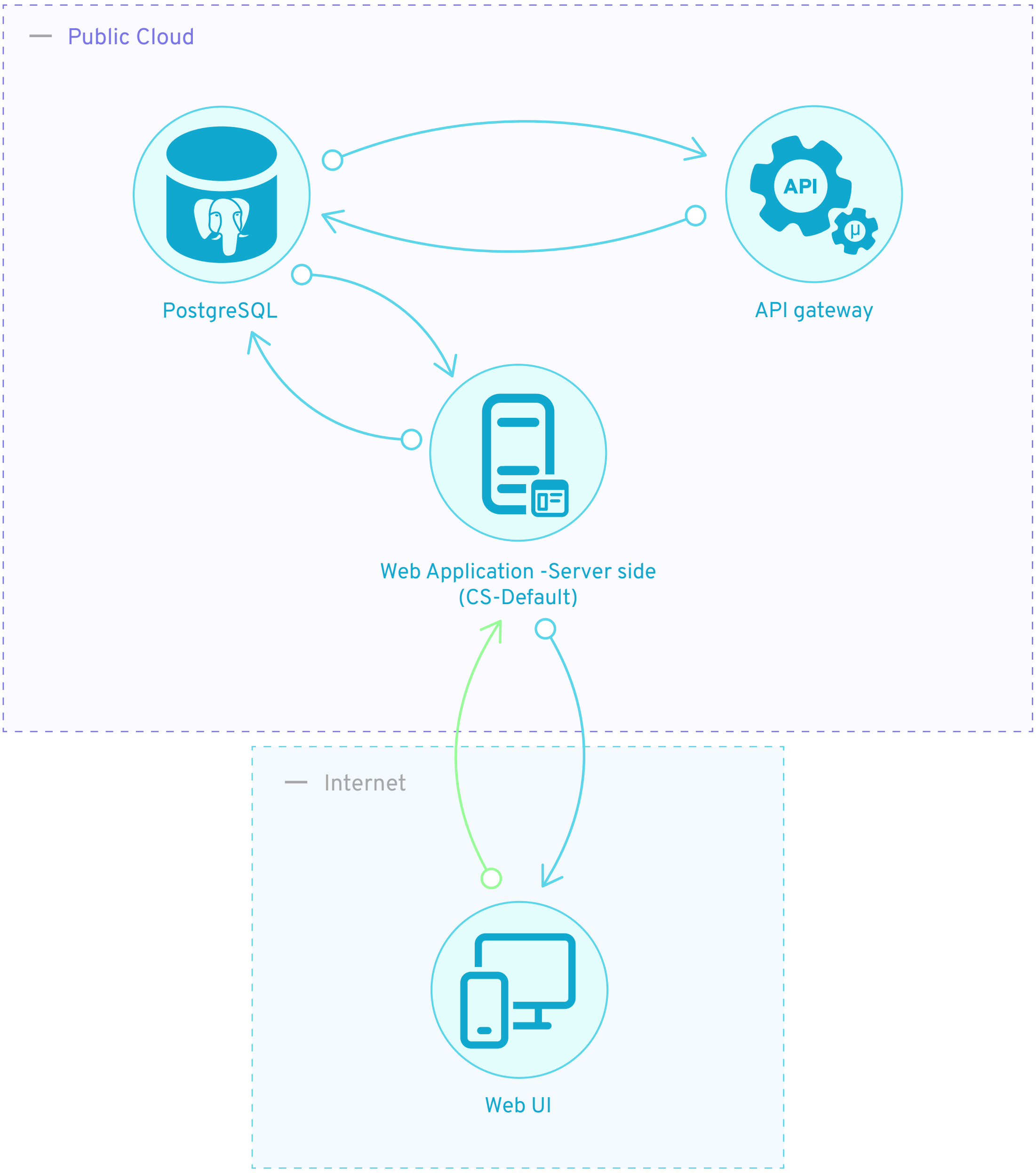
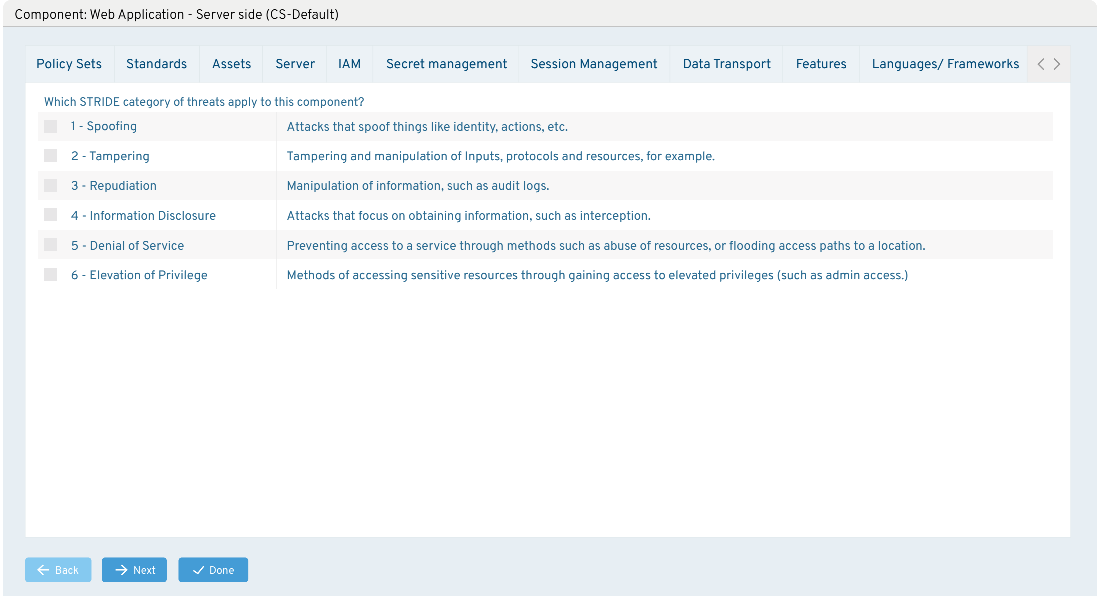


Figure 2.

A second strategy is to define the architecture with a questionnaire that will complement the visual orientation of the diagram, to establish a granularity in the model that allows more relevant threats and their countermeasures to be extracted. In *Figure 3* you can see an example of a form in which you can observe that by adding the details about the assets of the architecture, the standards defined in the security policies are automatically applied.



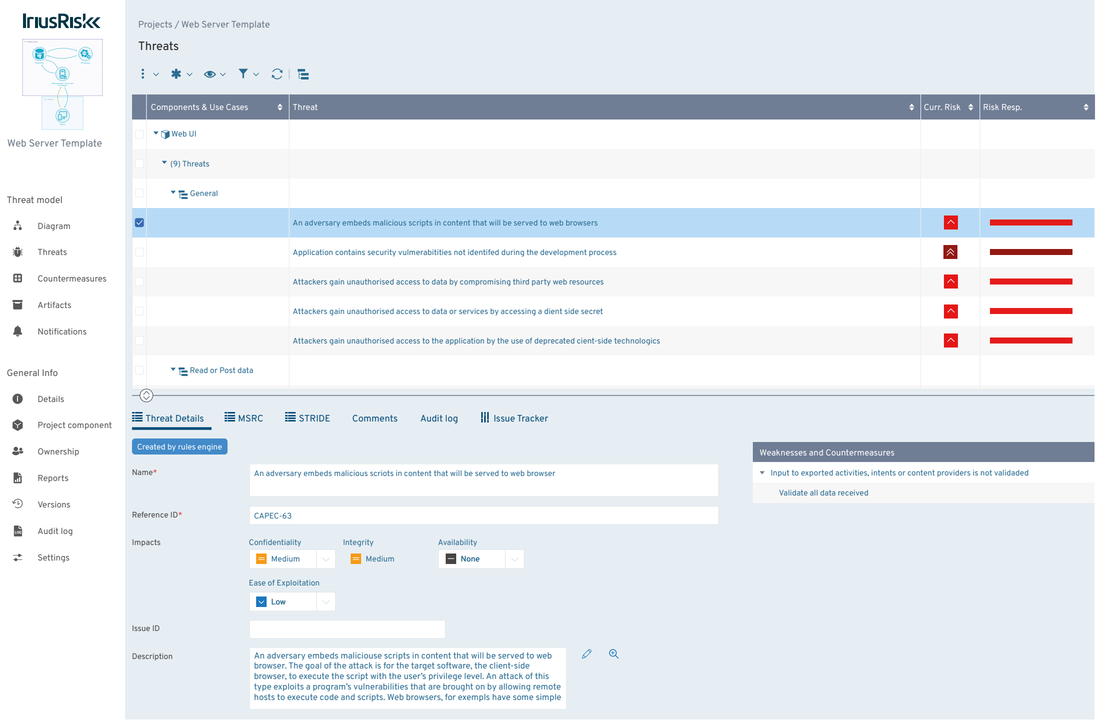
Component: Web Application - Server side (CS-Default)

Which STRIDE category of threats apply to this component?

□	1 - Spoofing	Attacks that spoof things like identity, actions, etc.
□	2 - Tampering	Tampering and manipulation of Inputs, protocols and resources, for example.
□	3 - Repudiation	Manipulation of information, such as audit logs.
□	4 - Information Disclosure	Attacks that focus on obtaining information, such as interception.
□	5 - Denial of Service	Preventing access to a service through methods such as abuse of resources, or flooding access paths to a location.
□	6 - Elevation of Privilege	Methods of accessing sensitive resources through gaining access to elevated privileges (such as admin access.)

Figure 3.

Finally, as shown in Figure 4, the development team can autonomously obtain a set of security requirements that can be automatically (and bidirectionally) synchronized with an ALM tool.



	Components & Use Cases	Threat	Curr. Risk	Risk Resp.
□	Web UI			
□	(9) Threats			
□	General			
☑		An adversary embeds malicious scripts in content that will be served to web browsers	🟥	🟥
□		Application contains security vulmerabitities not identifed during the development process	🟥	🟥
□		Attackers gain unauthorised access to data by compromising third party web resources	🟥	🟥
□		Attackers gain unauthorised access to data or services by accessing a dient side secret	🟥	🟥
□		Attackers gain unauthorised access to the application by the use of deprecated cient-side technologics	🟥	🟥
□	Read or Post data			

Name*: An adversary embeds malicious scriots in content that will be served to web browser

Reference ID*: CAPEC-63

Impacts: Confidentiality: Medium; Integrity: Medium; Availability: None

Ease of Exploitation: Low

Issue ID:

Description: An adversary embeds maliciouse scripts in content that will be served to web browser. The goal of the attack is for the target software, the client-side browser, to execute the script with the user's privilege level. An attack of this type exploits a program's vulnerabilities that are brought on by allowing remote hosts to execute code and scripts. Web browsers, for exempls have some simple

Weaknesses and Countermeasures

- Input to exported activities, intents or content providers is not validaded
  - Validate all data received

Figure 4.

Measure to improve

Metrics will help you assess if you are doing a good job and make it easier to pinpoint what you are not yet doing and why. Security metrics should be handled like any other quality indicator of software artifacts. This makes it easier to spread a security culture and make security a global contribution of all the teams involved in the development cycle. Figure 5 shows an example of risk metrics associated with the assets involved in the Threat Modeling of an application.

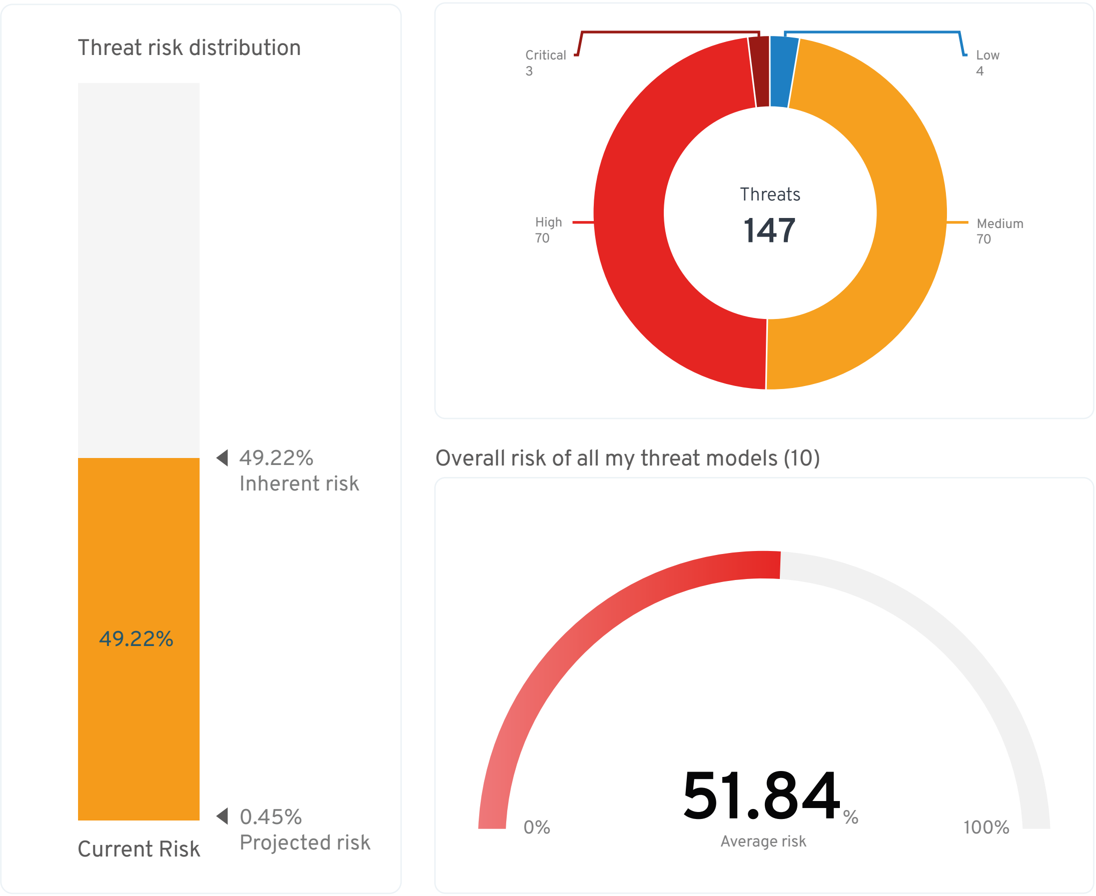


Figure 5.

Automate Threat Modeling to fit your existing SDLC.

Secure design right from the start.

Request a demo

IriusRisk