IriusRisk

Threat modeling Playbook

Document Version and Updates

This chapter documents the version history and updates made to this document, ensuring a clear and organised record of all changes.

Version Control Table

Version Number	Date	Author/Editor	Summary of Changes
1.0	01/09/2024	George Makrodimitris	1st Draft - Publish

Detailed Change Log

Version 0.1	
Date	02/08/2024
Author/Editor	George Makrodimtris
Changes	Initial Draft
Version -.-	
Date	
Author/Editor	
Changes	

Table Of Contents:

Chapter 1: Introduction

We are introducing our new Threat Modeling playbook to allow organizations to roll a Threat Modeling function faster and robustly. Threat Modeling is important when it comes to conducting threat models but it is also very important to have the right process, methodologies and structure in place to be conducted efficiently. By following effective Threat Modeling practices[1] organizations can significantly enhance the delivery of the threat models and reduce the friction with relevant stakeholders.

1.1 What is Threat Modeling?

Threat Modeling[2] is a structured approach used in cybersecurity for the purposes of identification, assessment, communication and mitigation of potential security threats to the organizations stakeholders as early as possible. It involves analyzing systems, identifying vulnerabilities, and predicting possible attack vectors. By prioritizing risks and developing countermeasures, Threat Modeling helps strengthen a system's security posture and reduce the likelihood of successful attacks.

Books to study:

- Threat Modeling: Designing for Security by Adam Shostack
- Securing Systems: Applied Security Architecture and Threat Models by Brook S. E. Schoenfield
- Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis by Willey
- Threat Modeling: A Practical Guide for Development Teams by O'Reilly
- Designing Usable and Secure Software with IRIS and CAIRIS by Shamal Faily

Also, we have also created a Threat Modeling Guide that is very compact and easy to read.

---

[1] *What is Threat Modeling by OLC(OpenLearnCreate)*

[2] *What is Threat Modeling*

1.2 Why Threat Modeling?

It has many benefits which can be summarized below:

- Secure by Design (Proactive Risk Identification and Mitigation)
  - Threat Modeling helps in identifying potential security threats and vulnerabilities early in the development process, allowing the organization to address them proactively before they can be exploited.
- Enhanced Security Posture
  - By systematically analyzing and understanding potential threats, a organization can strengthen its overall security measures, reducing the likelihood and impact of security breaches.
- Cost Savings
  - Addressing security issues during the design and development phases is generally much cheaper than fixing them after deployment. Threat Modeling can help avoid costly incident response and remediation efforts.
- Compliance and Regulatory Adherence
  - Threat Modeling supports adherence to industry standards and regulatory requirements (e.g., GDPR), helping the organization avoid legal penalties and maintain customer trust.
- Improved Collaboration and Communication:
  - The Threat Modeling process fosters better communication and collaboration between development, security, and business teams, ensuring that security is integrated into the entire lifecycle of a project.

1.3 Threat Modeling Mandate

Threat Modeling might not always be explicitly required by name in regulations, many industries incorporate it as part of broader risk management and management process mandated by regulations. The specific requirement may vary by the regulatory framework, but the practice is highly recommended or even implicitly required in many critical sectors where security and privacy are of great importance.

In Financial services:

- **PCI DSS (Payment Card Industry Data Security Standard)**[3]: Organizations handling payment data must implement security measures, including Threat Modeling, to identify potential threats and vulnerabilities. Applies to the "Retail" industry as well.
  Key Section: Requirement 12.2 requires organizations to implement a risk assessment process, which can include Threat Modeling.

- **Gramm-Leach-Bliley-Act (GLBA)**[4]: Financial Institutions are required to protect customer data, which often involves Threat Modeling to ensure robust security measures.
  Key Section: The Safeguards Rule requires financial institutions to develop a written information security plan, which involves identifying risks to customer information (often through Threat Modeling).

In Healthcare:

- **HIPAA (Health Insurance Portability and Accountability Act)**[5]: While not explicitly mentioning Threat Modeling, HIPAA reqired covered entities to conduct risk assessments and implement safeguards, which can include Threat Modeling as part of a broader risk management strategy.
  Key Section: The Security Management Process standard (45 CFR § 164.308(a)(1)(ii)(A)) mandates risk analysis, which can include Threat Modeling.

- **HITRUST CSF (Common Security Framework)**[6]: Threat Modeling is recommended for healthcare organizations to comply with this framework, which integrates multiple standards including HIPAA.
  Key Section: HITRUST incorporates controls from HIPAA and NIST, recommending Threat Modeling as part of the risk management process.

---

[3] *PCI DSS Documents*

[4] *Gramm-Leach-Bliley-Act (GLBA)*

[5] *HIPAA (Health Insurance Portability and Accountability Act)*

[6] *HITRUST CSF*

In Telecommunications:

- **5G Security Requirements (e.g. ENISA Guidelines)[7]:** 5G networks are required to follow strict security guidelines, often involving Threat Modeling.
  Key Section: These guidelines discuss Threat Modeling as part of the risk assessment for 5G networks.

In Energy:

- **NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection)[8]:** Requires the protection of the critical electric grid, and Threat Modeling is recommended as part of the cybersecurity standards.
  Key Section: CIP-002 to CIP-011 discuss the identification and protection of critical assets, which often involve Threat Modeling.

In Automotive:

- ISO/SAE 21434 (Road Vehicles – Cybersecurity Engineering)[9]: This is a cybersecurity standard for road vehicles, where Threat Modeling is a requirement to ensure that automotive systems are secure against cyber threats.
  Key Section: The standard explicitly requires cybersecurity risk assessment and threat analysis.

In Software Development and Technology:

- GDPR (General Data Protection Regulation)[10]: While GDPR does not explicitly require Threat Modeling , the need for Data Protection Impact Assessments (DPIA) for high-risk processing activities may involve Threat Modeling as part of identifying and mitigating risks to personal data.
  Key Section: Article 35 requires Data Protection Impact Assessments (DPIAs), where Threat Modeling can be used to identify risks to personal data.

Above are just a few examples of where Threat Modeling is mandated in some industries. In general, in highly regulated sectors with very strong security and privacy requirements, Threat Modeling would be also a requirement.

---

[7] *ENISA 5G Security Recommendations*

[8] *NERC CIP Standards*

[9] *ISO/SAE 21434 (Road Vehicles – Cybersecurity Engineering)*

[10] *GDPR*

1.4 FAQs about Threat Modeling

- **Threat Modeling is not an "one-time" exercise**
  Threat Modeling should be considered a "live"document. With evolving threat landscapes and new internal weaknesses discovered, it is vital to keep threat models up-to-date, especially when crucial components, trust boundaries and connections are changed in the product.

- **Differentiation between Threat Modeling and Penetration Tests**
  Threat Modeling is a proactive process that identifies and assesses potential threats during the design phase, focusing on preventing vulnerabilities/weaknesses. Penetration testing, on the other hand, is a reactive assessment performed after development, simulating attacks to find and exploit existing vulnerabilities. Essentially, Threat Modeling anticipates risks early, while penetration testing verifies security through real-world attack scenarios or simulations.

- **Threat Modeling is complex and difficult to be implemented**
  Threat Modeling isn't inherently complex or difficult to implement; it can be scaled to fit the organization's size and maturity. The process is flexible and can start small, focusing on critical assets and simple methodologies like STRIDE. With collaboration across teams and clear communication, it can be integrated into existing workflows. Automation tools and frameworks are available to simplify the process further. As the organization grows, so can the Threat Modeling process, adapting to new challenges and requirements, making it a practical and essential function in any cybersecurity strategy.

- **Threat Modeling is too time-consuming and expensive[12].**
  In reality, the cost of fixing security issues increases exponentially the later they're discovered. Threat Modeling can actually save time and money in the long run.

- **Threat Modeling is only for big companies with mature security programs[13].**
  False. Organizations of all sizes can benefit from Threat Modeling. It's about making security a priority, not the size of the organization's security budget.

---

[11] *DevSecOps, Threat modeling and You: Get started using the STRIDE method*

[12] *Threat Modeling Guide*

[13] *Threat Modeling Guide*

1.5 Playbook usage

This playbook serves as a guide of how to establish a Threat Modeling function in any organization. However, it is not considered a panacea for establishing a Threat Modeling function. The playbook provides an approach that can be tailored as needed for each organization to meet their needs. The basis of the playbook is that an organization has zero experience on Threat Modeling and they are just starting.

In addition, at the end of the document there will be a checklist (See Appendix) that can be used to guide a Threat Modeling program on the main elements that need to be implemented in order for the Threat Modeling function to operate efficiently and effectively.

1.6 What should be the Vision, Mission and Strategy Approach

1.6.1 About Vision

The Vision of a Threat Modeling function should emphasise on the goal of making Threat Modeling an integral part of the organization's development and operational processes, with the ultimate aim of enhancing security across all products and services, with the driving principle of Secure-by-Design.

An example of a Vision statement could be:
"To proactively secure our products and services by embedding Threat Modeling as a core practice, enabling us to foresee and mitigate security risks, ensuring our systems are resilient, trustworthy and capable of protecting our customers and stakeholders in the continuous evolving threat landscape."

1.6.2 About Mission

The Mission of a Threat Modeling function should focus on the actionable steps the Threat Modeling function will take, which is integrating Threat Modeling into development, fostering collaboration across teams, providing necessary training and resources and continuously improving the security of the organization to achieve its business objectives.

An example of a Mission statement could be:
"Our mission is to implement a structured, collaborative, and continuous Threat Modeling process that identifies and addresses potential security threats early in the development lifecycle. We aim to empower our teams with the knowledge and necessary tools and skills to anticipate and mitigate risks, improve our security posture, and deliver secure, high-quality solutions that guarantee our commitment to protecting our customers and the business."

1.6.3 About Strategy

To ensure an effective Threat Modeling Strategy in a organization, it is crucial to adopt a systematic and comprehensive approach conducting Threat modeling[14]. In addition, the Threat Modeling Strategy should align with the wider CyberSecurity Strategy that the organization has/will develop.

Capturing the current state of Threat Modeling and other relevant security assessments is vital to understand the organization's maturity and it is a prerequisite for the next step which is to create a comprehensive plan to pinpoint how the Threat Modeling function will operate. Also, a crucial step for the success of the Threat Modeling function will be the stakeholder buy-in which will allow the team to operate effectively. A key objective is to provide ongoing training and awareness programs to ensure that relevant stakeholders understand how Threat Modeling is conducted and all team members understand their roles inmaintaining security. Then, prepare to "walk-the-walk".

Capture Current State
Get accurate information about the current state of your company

Create a Plan
Develop a comprehensive plan that will describe the Threat Modeling function

Stakeholder Buy-in
Get buy-in from relevant stakeholders, in particular from senior management

Building a Threat Modeling Team
Create a team that will lead the Threat Modeling program

Expertise and Integration
Train people who will conduct Threat Modeling

Operationalize Threat Modeling Function
Create and integrate the Threat Modeling function in the organization

Optimization of Threat Modeling
Optimization and Improvements

[14] *What is Threat Modeling and How To Choose the Right Framework*

Moreover, establish a Threat Modeling methodology and a clear process of how the products will be threat modeled on IriusRisk. Involve cross-functional teams, including developers, security experts, and stakeholders, to identify potential threats and vulnerabilities from multiple perspectives. Utilize structured methodologies offered in our tool such as STRIDE, to Categorize and prioritize risks.

In addition, develop and implement robust mitigation strategies, incorporating best practices and security controls tailored to address identified threats. Regularly review and update the Threat model to reflect changes in the system and emerging threats.

Finally, validate the effectiveness of the Threat Modeling efforts through continuous testing, monitoring, and iterative improvements, fostering a culture of security throughout the organization.

Chapter 2: Develop a Threat Modeling Plan and a Roadmap

A well-structured Threat Modeling Plan and a Roadmap is essential for establishing an effective Threat Modeling function within a organization. They are slightly different from each other. The Threat Modeling Plan is tactical focusing on the specific, immediate steps needed to perform Threat Modeling effectively. On the other hand, Threat Modeling Roadmap is strategic, outlining the long-term journey and milestones needed to establish and mature the Threat Modeling function over time.

	Threat Modeling Plan	Threat Modeling Roadmap
Purpose	The Threat Modeling Plan is a detailed document that outlines the specific actions, objectives, and strategies for conducting Threat Modeling within an organization. It serves as a blueprint for how the Threat Modeling function will operate, including goals, methodologies, resources, and success criteria.	The Threat Modeling Roadmap is a strategic document that outlines the long-term vision and phased approach for establishing and evolving the threat modeling function within an organization. It guides the growth and maturity of the function over time.
Scope	The plan focuses on the "what" and "how" of Threat Modeling. It includes details on objectives, processes, methodologies (e.g., STRIDE), tools, roles, and responsibilities. The plan also covers how Threat Modeling integrates with other security and development activities.	The roadmap focuses on the "when" and "in what order" aspects. It lays out a sequence of milestones, phases, and timelines, guiding the development of the threat modeling function from initiation to full maturity. It may include plans for scaling the function, integrating new methodologies, and expanding team expertise.
Focus	It is more tactical, dealing with the day-to-day execution of Threat Modeling activities, ensuring that all necessary components are in place for effective threat identification and mitigation.	It is more strategic, dealing with long-term goals, such as building organizational capability, securing stakeholder buy-in, resource planning, and continuous improvement of the Threat Modeling function.
Timeframe	The plan is usually developed for short to medium-term implementation, focusing on current or upcoming projects and immediate goals.	The roadmap typically spans a longer timeframe, often several years, providing a high-level view of the evolution of the threat modeling function.

The Threat Modeling Plan is a tactical document that focuses on the immediate, detailed actions required to perform Threat Modeling effectively. It addresses the “what” and “how” of the Threat Modeling process, emphasising the methodologies, tools, roles, and processes needed to identify and mitigate threats in the short term.

In contrast, the Threat Modeling Roadmap is a strategic document that outlines the long-term vision and phased approach for establishing and evolving the Threat Modeling function. It focuses on the “when” and “in what order” aspects, guiding the growth and maturity of the Threat Modeling capability over time. The roadmap is concerned with building organizational capacity, securing stakeholder alignment, scaling practices, and ensuring continuous improvement, making it a broader, more future-oriented guide compared to the detailed, action-oriented plan.

2.1 Threat Modeling Plan

Key Objectives:

- ✓ Define clear objectives early
- ✓ Align with business goals
- ✓ Identify and Prioritize Products
- ✓ Establish Methodologies and Tools
- ✓ Integrate with Development Processes
- ✓ Define Roles and Responsibilities
- ✓ Document and Report Findings

A well-structured Threat Modeling Plan is essential for establishing an effective Threat Modeling function within a organization. The first step in developing this plan is to define clear objectives early in the process. These objectives should be aligned with the organization’s overall business goals, ensuring that the Threat Modeling efforts directly contribute to the organization’s security posture and strategic initiatives. By setting specific, measurable goals, the organization can focus its resources on addressing the most critical threats, which in turn maximizes the impact of the Threat Modeling function.

Alignment with business goals is crucial because it ensures that the Threat Modeling activities are not conducted in isolation but are integrated into the broader context of the organization’s operations. This alignment helps in prioritizing high-impact threats that could potentially disrupt the business, enabling the security team to allocate resources more effectively. It also ensures that the Threat Modeling function is seen as a value-adding activity by stakeholders across the organization, rather than just a technical exercise.

The primary objective of the Threat Modeling Plan is to identify and prioritize products associated with the organization's systems, applications, and data. This involves a systematic assessment of potential threats and vulnerabilities, focusing on those that could have the most significant impact. By prioritizing products, the plan ensures that resources are directed toward mitigating the most critical products first, thereby maximizing the effectiveness of the Threat Modeling efforts.

In addition to prioritization, it is important to establish measurable success criteria for the Threat Modeling Plan. These criteria should be tied to the objectives set at the outset and should provide a clear way to assess the effectiveness of the Threat Modeling efforts. This could include metrics such as the number of threats identified and mitigated, the reduction in potential attack surfaces, or improvements in the overall security posture of the organization. The metrics should be integrated in the Threat Modeling Roadmap as well so that it can be demonstrated of how the maturity is increasing within the Threat Modeling Function.

Next, the plan seeks to establish methodologies and tools that will guide the threat modeling process. This includes selecting appropriate Threat Modeling frameworks (such as STRIDE) and implementing the tools that will facilitate the analysis. These methodologies and tools must be tailored to the specific needs of the organization, ensuring consistency and accuracy in identifying and mitigating threats. Sometimes this comes hand-in-hand with the tooling that will be selected.

A crucial objective is to integrate Threat Modeling with development processes. By embedding Threat Modeling into the Software Development Life Cycle (SDLC), security becomes a continuous and proactive part of development rather than an afterthought. This integration helps in identifying potential threats early in the development process, reducing the likelihood of costly security issues later on.

The plan also aims to define clear roles and responsibilities within the threat team. This ensures that every team member knows their specific duties, which fosters collaboration and accountability. By having clearly defined roles, the team can operate more efficiently and effectively, with each member contributing to the overall success of the Threat Modeling function.

Finally, the plan emphasises the importance of documenting and reporting findings creating a Standardized process for documenting threats, vulnerabilities, and mitigation strategies is essential for ensuring that all relevant information is captured and communicated to stakeholders. Regular reporting ensures that decision-makers are kept informed of the threat landscape and the effectiveness of the Threat Modeling efforts, enabling them to make informed decisions about resource allocation and risk management.

2.2 Threat Modeling Roadmap

Key Objectives:

- ✓ Build Organizational Capability
- ✓ Achieve Stakeholder Alignment
- ✓ Scale and Evolve Practices
- ✓ Establish Continuous Improvement
- ✓ Measure and Demonstrate Value

The Threat Modeling Roadmap is focused on the long-term development and sustainability of the threat modeling function within the organization. The first objective is to build organizational capability, which involves developing the necessary skills, resources, and infrastructure to support Threat Modeling. This includes training existing staff, hiring specialized personnel, and acquiring the appropriate tools and technologies. The goal is to create a robust and scalable Threat Modeling function that can grow and adapt as the organization and its threat landscape evolve.

Another key objective is to achieve stakeholder alignment for the Threat Modeling function to be successful, it must be supported by key stakeholders, including executives, IT leaders, and business unit managers. The roadmap outlines strategies for securing this support by clearly communicating the value of Threat Modeling and aligning it with the organization's broader strategic objectives. This alignment ensures that Threat Modeling is recognized as a critical component of the organization's security strategy and not just a technical exercise.

As the organization grows, the roadmap must scale and evolve practices to ensure that the Threat Modeling function can keep pace with increasing complexity and new threats. This involves planning for the adoption of new methodologies and tools that can handle larger and more complex systems, as well as continuously refining existing practices to address emerging threats. The objective is to ensure that the Threat Modeling function remains effective and relevant over time.

Establishing continuous improvement is another key objective of the roadmap. This involves creating mechanisms for regularly assessing the effectiveness of the Threat Modeling function and making adjustments as needed. Continuous improvement ensures that the Threat Modeling process remains dynamic and responsive to changes in the threat landscape and business environment.

Finally, the roadmap emphasises the need to measure and demonstrate value by developing metrics and key performance indicators (KPIs) allows the organization to track the effectiveness of its Threat Modeling efforts and demonstrate their impact to stakeholders. This objective ensures that the Threat Modeling function is not only effective but also transparent and accountable, providing clear evidence of its contribution to the organization's overall security posture.

Chapter 3: Stakeholder Buy-in

One of the key tasks for the success of a new Threat Modeling function in an organization is to get on-board all the relevant stakeholders.

Key Objectives:

- ✓ Communicate value to stakeholders early
- ✓ Engage cross-functional teams
- ✓ Address stakeholder concerns proactively
- ✓ Foster a collaborative culture
- ✓ Ensure executive-level support consistently

3.1 Stakeholder Inventory and Needs

One of the first tasks that need to be done is to create a list of stakeholders that need to be closely monitored and engaged.

Consider the following roles:

- Application Domain Owner
- Application Owner
- Project Manager
- Product Owner
- Security Analyst
- Security Architect
- Enterprise Architect
- Software Developer
- Software Security Engineer
- Threat Intelligence

Note: The above titles might be different for each organization. The takeaways here is to create a stakeholder inventory that the Threat Modeling team will keep frequent contact with and will be a vote of confidence to Senior Management for the Threat Modeling function.

3.2 Stakeholder Engagement

Convincing stakeholders of the importance of the Threat Modeling team for security involves a strategic approach. Engage stakeholders and especially Senior Management tackling the following areas:

- **Present the Risks and Consequences**
  - **Identify Specific Threats:** Explain the specific security threats relevant to the organization's industry and organization.
  - **Real-World Examples:** Use real-world case studies of breaches and their impacts on companies that lacked adequate Threat Modeling.
  - **Potential Costs:** Highlight the potential financial losses, compliance and regulatory requirements, and damage to reputation that can result from security breaches.

- **Demonstrate the Benefits** (See Chapter: Why Threat Modeling?)
  - **Proactive Security Measures:** Emphasize that Threat Modeling allows the organization to identify and mitigate potential security issues before they become serious problems.
  - **Cost-Effectiveness:** Show how investing in a Threat Modeling team the organization aims on Security-by-Design by shifting left, and can be more cost-effective in the long run compared to the costs associated with data breaches and reactive measures.
  - **Compliance and Standards:** Point out how Threat Modeling helps in meeting regulatory requirements and industry standards, avoiding penalties and ensuring smoother audits.

- **Provide Clear Metrics** (That might not be available from the beginning but it will be needed later for proof of value. See Chapter: Optimization of Threat Modeling)
  - **Quantifiable Data:** Use metrics and KPIs to demonstrate how Threat Modeling can improve the organization's security posture
  - **ROI Calculations:** Calculate and present the return on investment (ROI) for building and maintaining a Threat Modeling team, considering factors such as reduced incident response costs, minimized downtime, less fixes after product launch.

- **Develop a Strategic Plan**
  - **Implementation Roadmap:** Present a clear, phased plan for implementing the Threat Modeling team, including timelines, resource requirements, and milestones (See Chapter: Create a Threat Modeling Plan/Roadmap).
  - **Roles and Responsibilities:** Define the roles and responsibilities within the Threat Modeling team and how they integrate with existing teams (See Chapter: Embedding the Team in the Organization).
  - **Training and Development:** Outline a training plan for the Threat Modeling team to ensure they are well-equipped with the latest knowledge and tools (See Chapter: Threat Modeling Expertise and Training).

- **Align with Business Objectives**
  - Business Integration: Explain how Threat Modeling supports broader business objectives, such as maintaining customer trust, protecting intellectual property, and ensuring business continuity.
  - Strategic Advantage: Highlight how a strong security posture, supported by Threat Modeling, can provide a competitive advantage.

- **Engage Key Stakeholders**
  - Support from Influencers: Identify and engage key influencers within the organization who can advocate for the importance of Threat Modeling.
  - Cross-Departmental Collaboration: Demonstrate how Threat Modeling involves and benefits multiple departments, not just IT or security, but also business.
  - Presentations and Reports: Create professional presentations and detailed reports that Senior Management can review at their convenience.

3.3 Create a SIPOC Diagram

A SIPOC (Suppliers, Input, Process, Output, Customers) is helping the Threat Modeling team to identify the relevant stakeholders that will be involved with Threat Modeling but also, what input documents are needed and what output documents will be generated. It serves as a guide to know the communication channels and adds value to the final deliverables.

The below paradigm serves as an example of a Threat Modeling Function SIPOC and should be tailored according to the organization needs.

Supplier	Inputs	Process	Outputs	Customers
Security Analysts/Security Engineers	Existing Risk Assessments	Threat Modeling Process (Use of IriusRisk Software)	Threat Model • Data Flows • Threats • Countermeasures • Action Plans Attack Sequences (if applicable)	Security Architecture Security Analysts/Security Engineers Risk Owners Chief Information Security Office Senior Leadership (if required) Product Owner Project Manager Application Owner Application Domain Owner Threat Modeling Team Members
Offensive Security	Existing Penetration Tests			
Threat Modeling Team	Existing Threat Models			
Threat Intelligence/ Threat Research/Incident Response Team	Threat Intelligence			
Product Owner	Requirements			
Project Manager Application Owner Application Domain Owner	Relevant documentation (e.g., existing implemented controls etc.)			
Security Architecture	Architectural References			
Risk Department	Enterprise Risk Management			

Chapter 4: Threat Modeling Expertise and Integration

Threat Modeling may already be conducted already in an organization by existing personnel, or it may be just starting. In any case, proper expertise and training is vital to drive the Threat Modeling Program efficiently and effectively.

Key Objectives:

- ✓ Invest in specialized training.
- ✓ Hire experts to drive Threat Modeling success
- ✓ Encourage continuous learning
- ✓ Certify expertise if applicable
- ✓ Utilize external experts strategically

4.1 Get an Expert

The expert will be able to lead the Threat Modeling program to success utilizing previous experience and knowledge. The expert will also teach how Threat Modeling should be performed to the other team members and product teams in the organization that in the future might want to do their own threat models.

To hire an expert a organization should:

- **Profile the Ideal candidate:** Look for a candidate with extensive experience in Threat Modeling frameworks (e.g. STRIDE, MITRE etc.) and a deep understanding of the organization industry's threat landscape.
- **Recruit Strategically:** Use specialized job boards, professional networks and security communities to find qualified candidates. Consider conducting technical interviews and practical assessments to test their expertise and knowledge.
- **Onboard effectively:** Ensure the expert understands the organization's architecture, existing security capabilities, and risk appetite. Provide access to necessary resources and tools such as IriusRisk.
- **Integrate into Organization:** Position the expert with the cybersecurity department but ensure they collaborate closely with development, operations, architecture.
- **Review and Adapt:** The expert should regularly assess the effectiveness of the Threat Modeling function and make adjustments based on the organization's needs.

Hiring an expert is beneficial for companies that are just starting out with Threat Modeling or for organizations with a small product inventory for Threat Modeling.

4.2 Threat Modeling Training Program

Implementing a Threat Modeling training program involves hiring trainers/instructors to educate a core group of people on Threat Modeling techniques. These individuals could later serve as Threat Modeling experts or advocates within the organization.

This method is beneficial because it can be scaled effectively and increases the likelihood of the organization successfully adopting and integrating Threat Modeling practices and IriusRisk. To establish a Threat Modeling training program:

- **Identify training needs:** Assess current skills and gaps within the Threat Modeling team. Consider specific threats and industry regulations relevant to the organization.
- **Define Objectives:** Set clear learning outcomes, such as mastering Threat Modeling frameworks (e.g., STRIDE) and understanding organization risk profiles.
- **Select Content:** Select training courses and material tailored to the organization's needs. Include theoretical knowledge, practical exercises with IriusRisk, and real-world case studies.
- **Select Trainers:** Engage experienced professionals with expertise in Threat Modeling and can adapt to the organization's needs.
- **Implement Training:** Schedule regular sessions, workshops etc. Ensure training is interactive and includes hands-on exercises to reinforce learning.
- **Evaluate and Iterate:** Collect feedback from team members to assess effectiveness.
- **Integrate into organization's Culture:** Encourage continuous learning by making Threat Modeling a part of the organization's security culture.

The Threat Modeling training program might take time to see results, as the training must be followed by the creation of initial threat models, and combining the two might be overwhelming. In addition, it needs significant investment that might be challenging for organizations that have yet to see the proven benefits of Threat Modeling.
Thus, organizations already convinced of the importance of Threat Modeling but looking to expand and fully integrate it into their processes should consider investing in Threat Modeling.

Chapter 5: Building a team

Without a good team, the Threat Modeling function will struggle to show its value to the stakeholders.

Key Objectives:

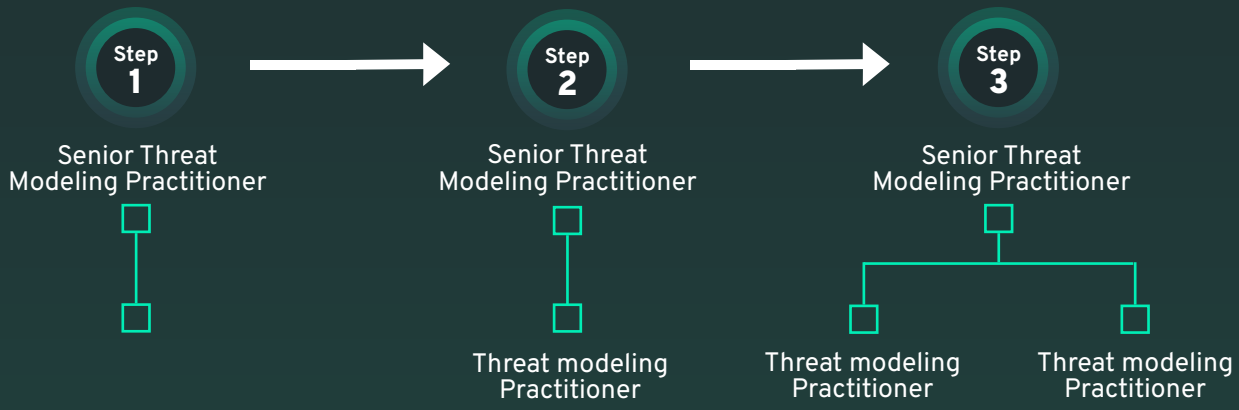
- ✓ Define clear roles and responsibilities
- ✓ Provide continuous support and resources
- ✓ Start small and expand
- ✓ Be close to Senior Management
- ✓ Foster a problem-solving mindset

There are two approaches that can be used to embed a Threat Modeling function.

1. Create a team that is the central beacon of knowledge and the creation of models.
2. Allocate dedicated Threat Modeling Practitioners in each product team or train product team members to conduct threat models.

The second approach can be arduous and costly as big companies have many products and it will be time-consuming to do the corresponding allocation of Threat Modeling Practitioners and follow structurally the Threat Modeling process. Also, the team is split, losing the collaborative elements that are needed in the beginning to foster relationships and problem-solving skills.

Therefore, the recommended approach for a Threat Modeling team that is just starting is Option 1, creation of a dedicated team for Threat Modeling. Next, hire a senior Threat Modeling Practitioner to establish the foundations of the Threat Modeling function. If there is a budget for a second team member, hire an additional Threat Modeling Practitioner that will assist the senior Threat Modeling Practitioner in related tasks. A natural progress of team expansion in 3 steps looks like the picture below.



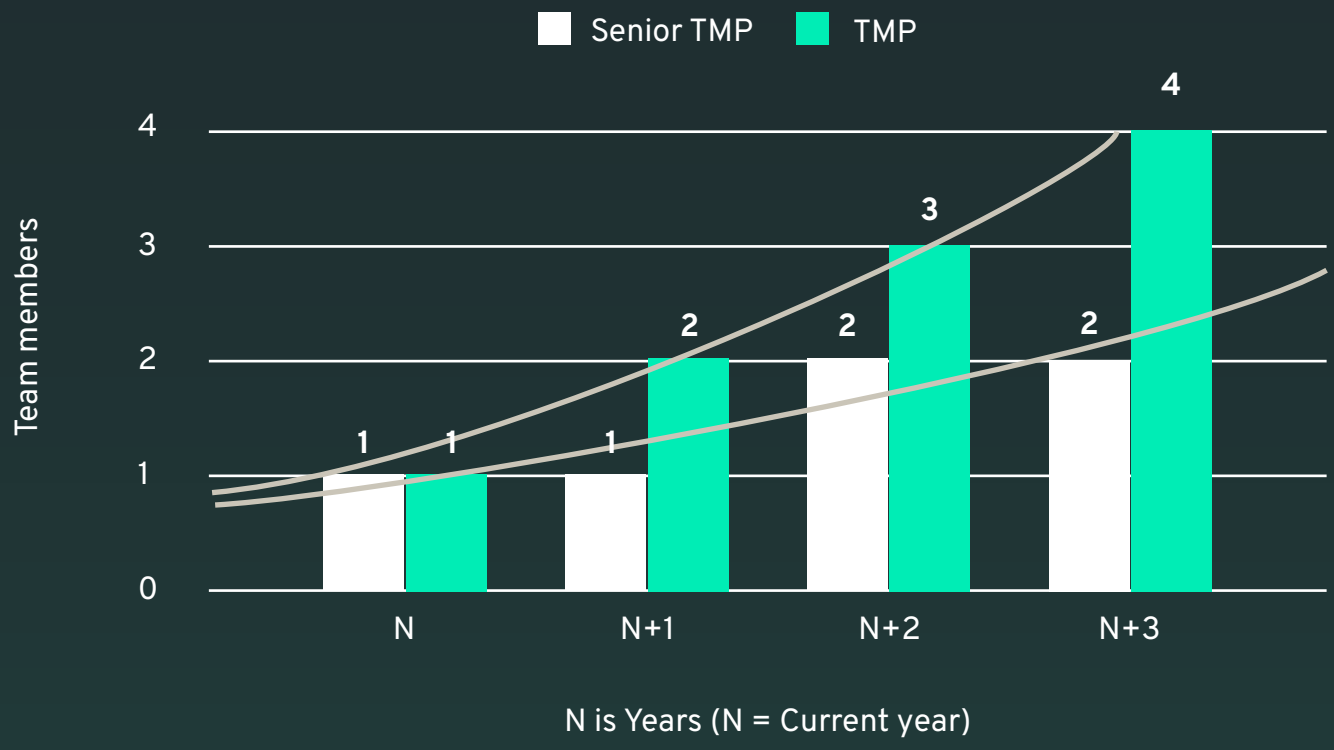
Assuming starting with two members, they should focus on the following things:

- Creating a Threat Modeling Process and a Threat Modeling Methodology.
  Note: Do not hesitate to make assumptions, it is better to have a document describing the process and methodology, than none. The documents can be improved along the way.
- Create a presentation for Senior Management to show the timelines of conducting the threat models and the benefits and mention the blockers.

The next area of focus for the team is the creation of the first threat models:

- Select 5 Products that will be threat modeled starting with the most critical ones.
- Start Threat Modeling one product.
  - During Threat Modeling, the Threat Modeling Practitioner should educate the relevant people about Threat Modeling through specific tailored educational sessions during the initiation of the threat model.
  - Pick a highly motivated individual from every product team and bless them with the role of Threat Modeling Champion (more details next session).

Once the team has proven to the senior manager, through continuous reporting and presentations, that Threat Modeling investment has a positive impact on the product by identifying threats and remediating them, more budget can be allocated and the team can expand to more people as below.

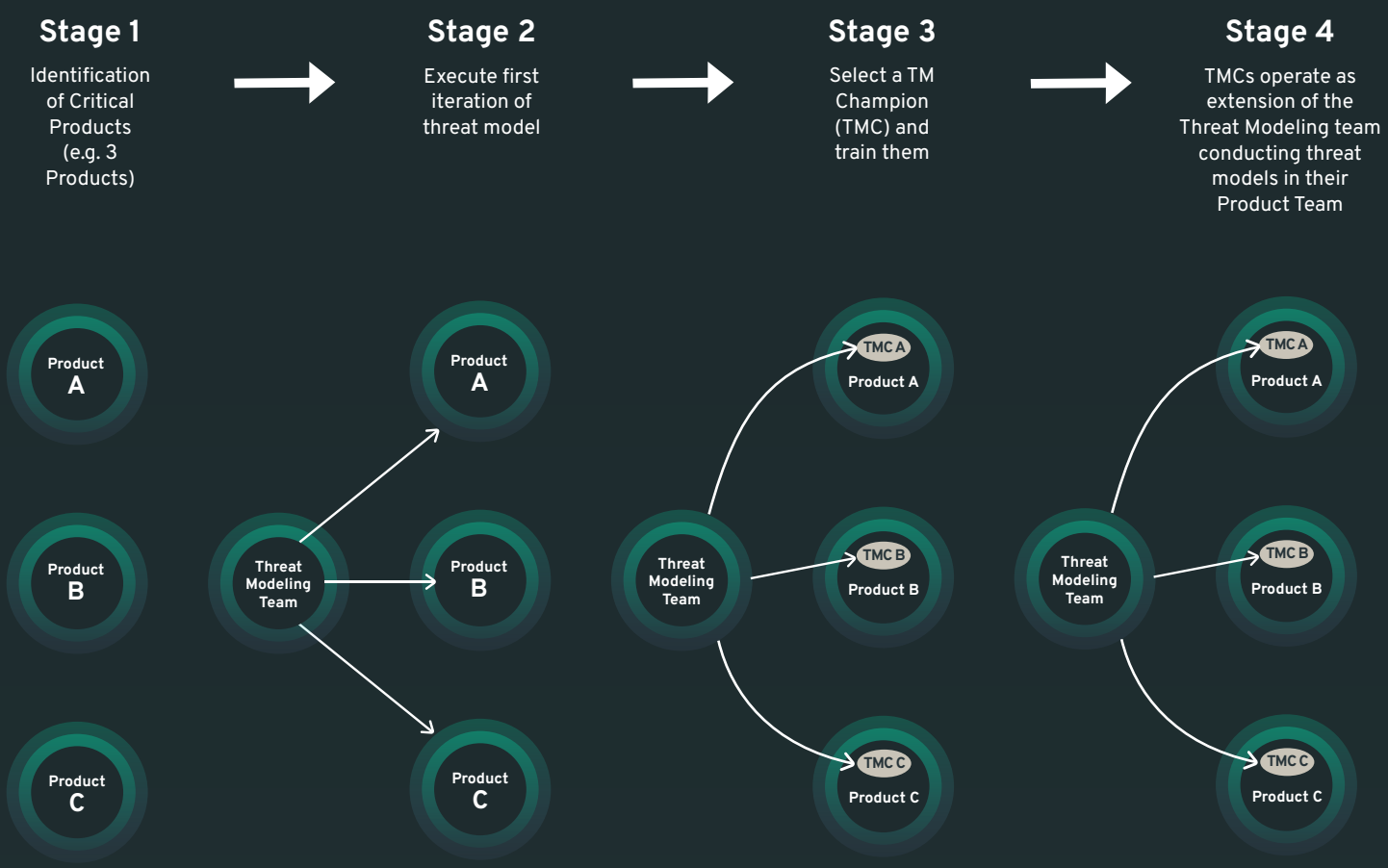


5.1 Threat Modeling Champions

Every time a threat model is done to a product, it is an opportunity to allocate a Threat Modeling Champion within the product team. To allocate a Threat Modeling Champion:

- **Identify the Champion Role:** Define the responsibilities and qualifications for a Threat Modeling Champion. This individual should be a security-focused highly-motivated product team member with a strong understanding of the product, Threat Modeling processes, and security best practices. They should also have good communication and leadership skills to effectively guide and influence the product team.
- **Selection Process:** Choose Champions from within the existing product teams or bring in security experts to fill this role. Ideally, the Champion should be someone already familiar with the product's architecture and development practices to seamlessly integrate security into the development lifecycle.
- **Training and Certification:** Provide specialized training for the selected Champions to ensure they are well-equipped to lead Threat Modeling efforts.
  This could include formal certification in Threat Modeling frameworks like STRIDE and as well as hands-on workshops and simulations on IriusRisk.
- **Integration into Product Teams:** Assign each Champion to a specific product team as their point-of-contact for all Threat Modeling activities. This integration ensures that security considerations are continuously incorporated into the development process, from initial design through deployment and beyond.
- **Regular Updates and Communication:** Establish a routine for regular updates and communication between the Champion, the product team, and the broader security team. This includes scheduled threat model reviews, updates on emerging threats, and adjustments to the threat model as the product evolves.
- **Monitoring and Support:** Set up a support system for the Champions, such as a central security team or a community of practice where Champions can share insights, challenges, and solutions. Regularly review the effectiveness of the Champion system and make adjustments as necessary.

A natural progress of a threat model Champion implementation could look like process below:



As noted above, the TM Champion could be any member of the Product team, however should be someone who is security-focused, highly-motivated and has a strong understanding of the product, Threat Modeling processes, and security best practices (e.g. Senior Software Developer).The end goal is to have a Threat Modeling Champion for each product the organization has and the Threat Modeling team will support them in the threat model creation.

5.2 Embedding the Team in the Organization

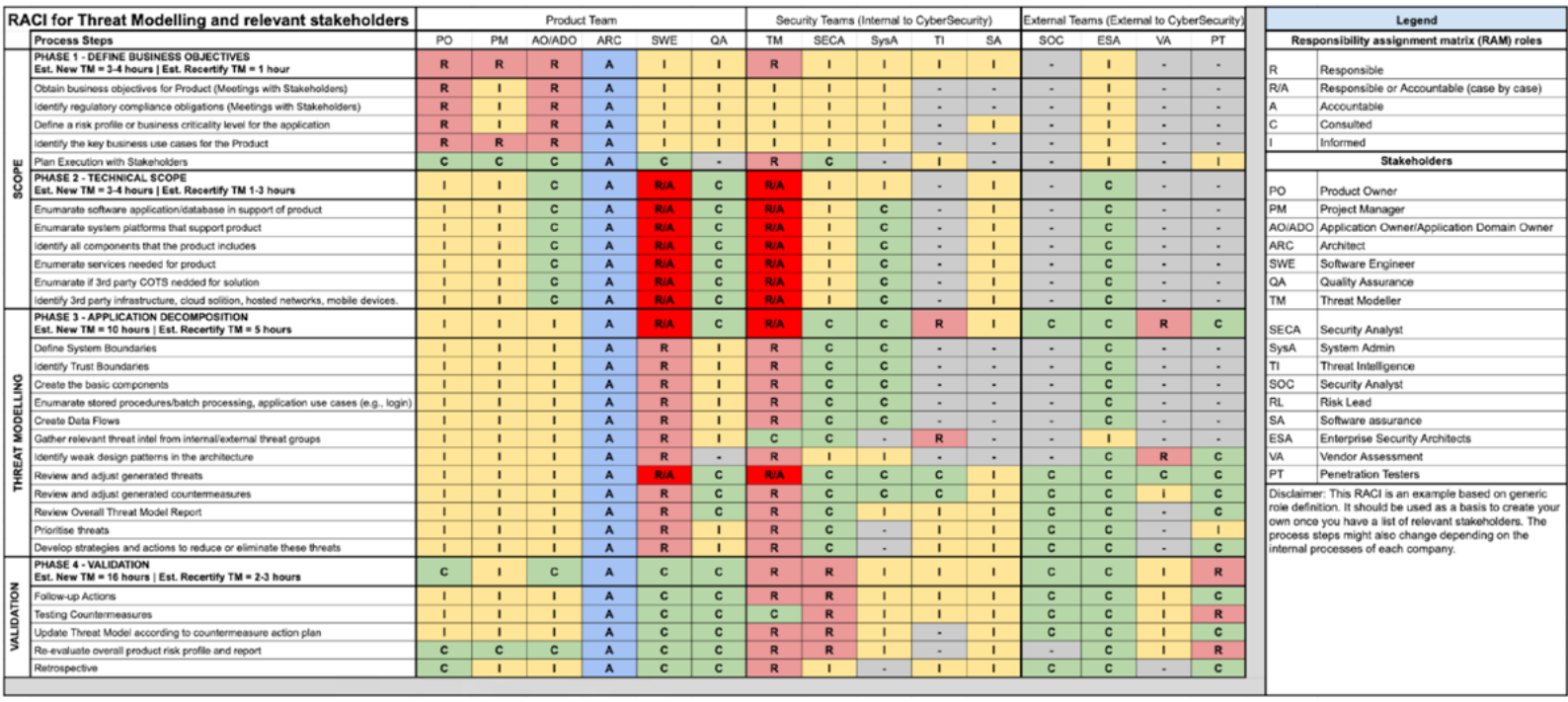
Experience has shown that a good RACI[15] (Responsible, Accountable, Consulted, Informed) is vital as it defines roles and responsibilities with the completion of a threat model, ensuring accountability and streamlined communication. It helps prevent overlaps and gaps in tasks, aligns team members on their specific duties and ensures that all relevant stakeholders are involved appropriately. This structured approach enhances efficiency, reduces confusion and ensures that Threat Modeling is conducted thoroughly and effectively, leading to better risk management and security outcomes.

[15] *Threat Modeling - RACI*

The RACI framework Categorizes roles as:

- **Responsible (R):** The person(s) who does the work to complete the task. They are responsible for carrying out the task.
- **Accountable (A):** The person who is ultimately answerable for the task's completion and the outcome. There should be only one accountable person per task.
- **Consulted (C):** The person(s) who provides input or feedback on the task. These are typically subject matter experts whose opinions are sought.
- **Informed (I):** The person(s) who need to be kept informed about the progress or decisions related to the task. They do not contribute directly to the work.

Below, an example of a RACI table (Click on the image for a larger version of the model).



RACI for Threat Modelling and relevant stakeholders		Product Team						Security Teams (Internal to CyberSecurity)					External Teams (External to CyberSecurity)			
	Process Steps	PO	PM	AO/ADO	ARC	SWE	QA	TM	SECA	SysA	TI	SA	SOC	ESA	VA	PT
SCOPE	**PHASE 1 - DEFINE BUSINESS OBJECTIVES Est. New TM = 3-4 hours | Est. Recertify TM = 1 hour**	R	R	R	A	I	I	R	I	I	I	I	-	I	-	-
	Obtain business objectives for Product (Meetings with Stakeholders)	R	I	R	A	I	I	I	I	I	-	-	-	I	-	-
	Identify regulatory compliance obligations (Meetings with Stakeholders)	R	I	R	A	I	I	I	I	I	-	-	-	I	-	-
	Define a risk profile or business criticality level for the application	R	I	R	A	I	I	I	I	I	-	I	-	I	-	-
	Identify the key business use cases for the Product	R	R	R	A	I	I	I	I	I	-	-	-	I	-	-
	Plan Execution with Stakeholders	C	C	C	A	C	-	R	C	-	I	-	-	I	-	I
	PHASE 2 - TECHNICAL SCOPE Est. New TM = 3-4 hours | Est. Recertify TM 1-3 hours	I	I	C	A	R/A	C	R/A	I	I	-	I	-	C	-	-
	Enumarate software application/database in support of product	I	I	C	A	R/A	C	R/A	I	C	-	I	-	C	-	-
	Enumarate system platforms that support product	I	I	C	A	R/A	C	R/A	I	C	-	I	-	C	-	-
	Identify all components that the product includes	I	I	C	A	R/A	C	R/A	I	C	-	I	-	C	-	-
	Enumerate services needed for product	I	I	C	A	R/A	C	R/A	I	C	-	I	-	C	-	-
	Enumarate if 3rd party COTS nedded for solution	I	I	C	A	R/A	C	R/A	I	C	-	I	-	C	-	-
	Identify 3rd party infrastructure, cloud solition, hosted networks, mobile devices.	I	I	C	A	R/A	C	R/A	I	C	-	I	-	C	-	-
THREAT MODELLING	**PHASE 3 - APPLICATION DECOMPOSITION Est. New TM = 10 hours | Est. Recertify TM = 5 hours**	I	I	I	A	R/A	C	R/A	C	C	R	I	C	C	R	C
	Define System Boundaries	I	I	I	A	R	I	R	C	C	-	-	-	C	-	-
	Identify Trust Boundaries	I	I	I	A	R	I	R	C	C	-	-	-	C	-	-
	Create the basic components	I	I	I	A	R	I	R	C	C	-	-	-	C	-	-
	Enumarate stored procedures/batch processing, application use cases (e.g., login)	I	I	I	A	R	I	R	C	C	-	-	-	C	-	-
	Create Data Flows	I	I	I	A	R	I	R	C	C	-	-	-	C	-	-
	Gather relevant threat intel from internal/external threat groups	I	I	I	A	R	I	C	C	-	R	-	-	I	-	-
	Identify weak design patterns in the architecture	I	I	I	A	R	-	R	I	I	-	-	-	C	R	C
	Review and adjust generated threats	I	I	I	A	R/A	C	R/A	C	C	C	I	C	C	C	C
	Review and adjust generated countermeasures	I	I	I	A	R	C	R	C	C	C	I	C	C	I	C
	Review Overall Threat Model Report	I	I	I	A	R	C	R	C	I	I	I	C	C	-	C
	Prioritise threats	I	I	I	A	R	I	R	C	-	I	I	C	C	-	I
	Develop strategies and actions to reduce or eliminate these threats	I	I	I	A	R	I	R	C	-	I	I	C	C	-	C
VALIDATION	**PHASE 4 - VALIDATION Est. New TM = 16 hours | Est. Recertify TM = 2-3 hours**	C	I	C	A	C	C	R	R	I	I	I	C	C	I	R
	Follow-up Actions	I	I	I	A	C	C	R	R	I	I	I	C	C	I	C
	Testing Countermeasures	I	I	I	A	C	C	C	R	I	I	I	C	C	I	R
	Update Threat Model according to countermeasure action plan	I	I	I	A	C	C	R	R	I	-	I	C	C	I	C
	Re-evaluate overall product risk profile and report	C	C	C	A	C	C	R	R	I	-	I	-	C	I	R
	Retrospective	C	I	I	A	C	C	R	I	-	I	I	C	C	-	C

Legend	
Responsibility assignment matrix (RAM) roles	
R	Responsible
R/A	Responsible or Accountable (case by case)
A	Accountable
C	Consulted
I	Informed
Stakeholders	
PO	Product Owner
PM	Project Manager
AO/ADO	Application Owner/Application Domain Owner
ARC	Architect
SWE	Software Engineer
QA	Quality Assurance
TM	Threat Modeller
SECA	Security Analyst
SysA	System Admin
TI	Threat Intelligence
SOC	Security Analyst
RL	Risk Lead
SA	Software assurance
ESA	Enterprise Security Architects
VA	Vendor Assessment
PT	Penetration Testers

Disclaimer: This RACI is an example based on generic role definition. It should be used as a basis to create your own once you have a list of relevant stakeholders. The process steps might also change depending on the internal processes of each company.

Notes:

- In two phases, there is R/A twice in the process. This means that the roles can be either Responsible for that task or Accountable depending on the current structure and task assignment of the teams. However, keep in mind that there can be only one Accountable person, which means if the one role is Accountable, the other role needs to be Responsible.
- This RACI is an example based on generic role definition. It should be used as a basis to create one based on the organization's list of relevant stakeholders. The process steps might also change depending on the internal processes of each organization.

Chapter 6: Operationalize Threat Modeling Function

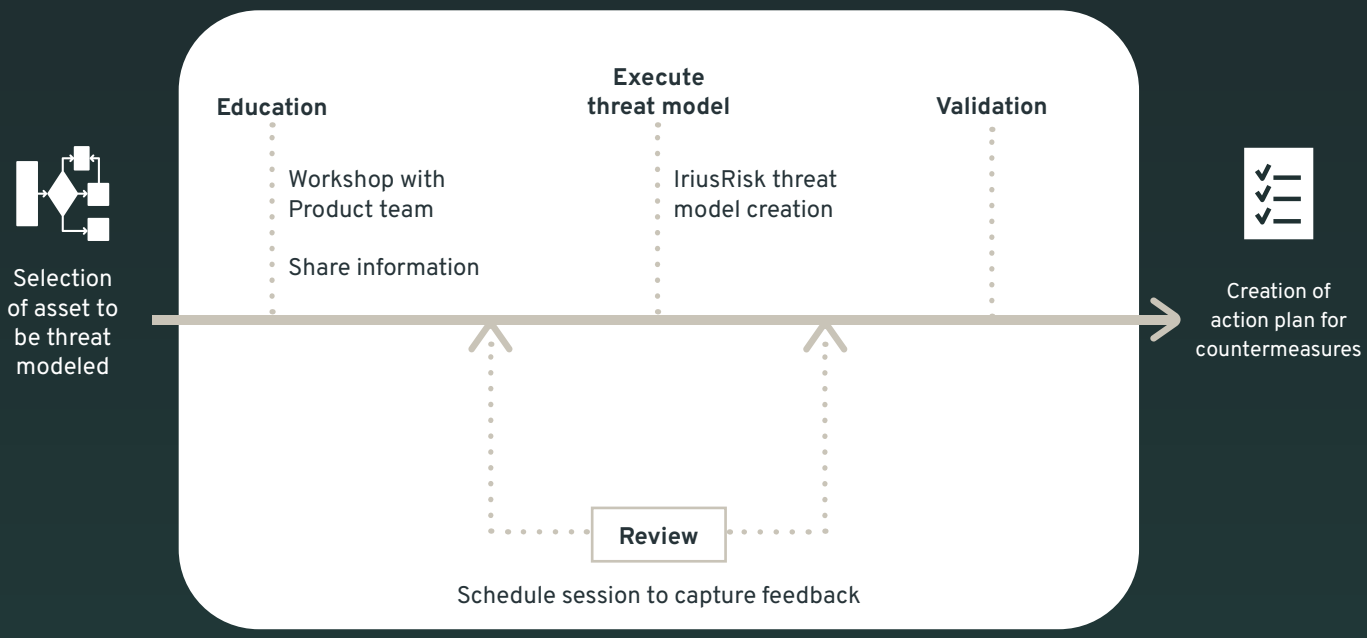
This step is the core of the Threat Modeling function and where the real value is generated.

Key Objectives:

- ✓ Prioritize assets that will be threat modeled based on criticality.
- ✓ Standardize and document processes for consistency.
- ✓ Select comprehensive methodology.
- ✓ Select appropriate modeling frameworks.
- ✓ Incorporate feedback loops continuously.

6.1 Establish a Threat Modeling Methodology and a Process

The organization should develop a comprehensive Threat Modeling process[16][17][18] in order to create a standardized way of creating threat models that will allow the efficient and effective planning, execution and management of threat models.



[16] *Threat Modeling Cheat Sheet by OWASP*
[17] *Threat Modeling Process by OWASP*
[18] *Threat Modeling Explanation by ShellSharks*

Three key answers that will need to be tackled early on are:

- How detailed should the threat models be?
- What documents are needed to initiate a threat model and are they available?
- When is a threat model considered complete?

These questions will equip the team with a projection of the resources needed and a timeline.

6.1.1 Document Current Situation

In order to create a robust process, it is important to document if other elements of security assessments are being carried out in the organization. Once a good understanding of what and how security assessment elements is captured, the Threat Modeling team can start brainstorming, planning and drafting a robust Threat Modeling process.

6.1.2 Prioritization of the Critical Products

The first key recommendation of IriusRisk is to identify the most critical applications/ systems/services of the organization. If there is no database in the organization with the risk profiles of the products, additional steps need to be taken to identify them, such as BIAs (Business Impact Analysis).

A quick start is to define the risk profiles that work for the organization and a classification method, the application can be categorized per criticality.

- **High-Risk:** Products that if Confidentiality, Integrity and Availability is compromised, there will be Major Financial and Reputational impact, and the existence of the organization is at stake.

- **Medium-Risk:** Products that if Confidentiality, Integrity and Availability is compromised, there will be Medium FInancial and Reputation impact to the organization.

- **Low-Risk:** Products that if Confidentiality, Integrity and Availability is compromised, there will be Minor FInancial and Reputation impact.

Another approach which is highly recommended in order to start doing threat models faster is by ad-hoc brainstorming with relevant stakeholders. This will help the organization start faster Threat Modeling critical applications.

1. Assuming that the organization has an accurate Product inventory, then the next step is to identify 5 of the most important/critical products that if the CIA is breached, the financial and reputational of impact of the organization might be at stake (for this the SBIA is a very helpful exercise).
2. To conduct step 1, we recommend collaborating with the offensive security team, security architecture and security analysts and any stakeholder that has good knowledge of the organization's infrastructure and do a brainstorming session to identify the products.
3. Once 5 products are in the list, create a high-level roadmap for the threat models.

6.1.3 How to do Threat Modeling

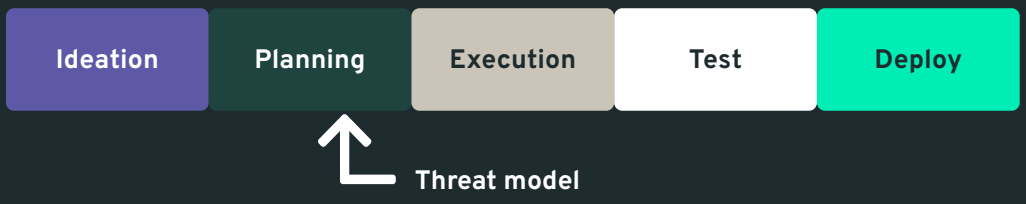
Assuming that a organization has a comprehensive inventory of the Products and a prioritisation list of the threat models that need to be completed, they be done by either doing:

- **Partial threat model**: Partially threat model a Product by performing the most important use cases.
  - By identifying the most critical components of the Product, a partial threat model can be conducted to cover the most important risks.
    - Benefits: Less time consuming, less resources, easy start.
    - Disadvantage: Partially completed, less view on the actual risk.

- **Focus on Changes**: This approach captures the current state of the Product and the changes that are going to affect in any way the Product.
  - This approach allows to conduct a threat model on new components, services etc. that will be embedded in an already existing Product.
    - Benefits: Not that time consuming, and less resources than a full threat model are needed.
    - Disadvantage: Partially completed, less view on the actual risk.

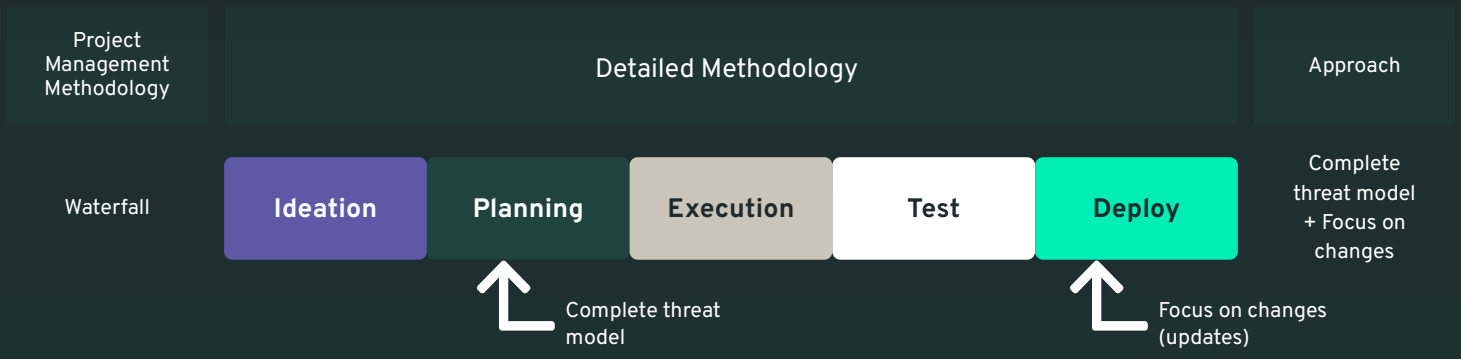
- **Complete threat model**: End-to-end threat model a Product.
  - The reason of doing a complete threat model is to identify all the relevant risks and mitigate the:
    - Benefits: A full representation of the existing risks, easy to be updated.
    - Disadvantage: Time consuming, more resources.

Experience has shown that it is better to start by doing either a **partial threat model** and keep progressing slowly until the full "picture" is captured alongside the changes that are introduced or a **complete threat model**. Every product follows a project methodology to be delivered, such as the picture below:



In the above simple example, a recommended approach is to conduct a **complete threat model** during the planning phase. However, considering that there are many types of project methodologies like Waterfall, Agile and DevOps, this can change.

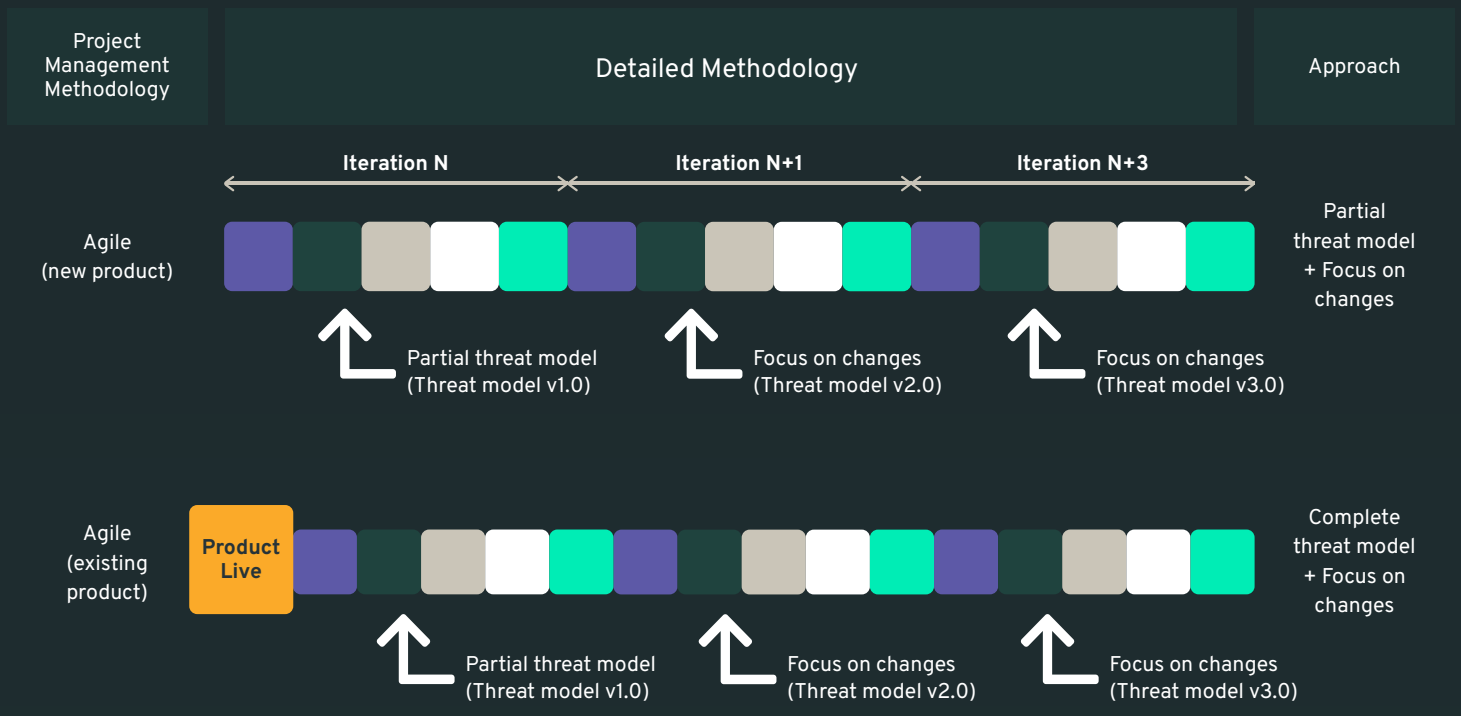
Assuming an organization is following Waterfall (similar to the example above), rationale says that a **complete threat model** needs to be done.



Assuming a organization is following Agile[19], rationale says that can either:

- Do a partial threat model and focus on changes for each iteration.
- Do a complete threat model and update the whole threat model for each change, treating the threat model as a "Live" document.
- Could also do a focus on changes (not presented in the picture below) and update it in every change that is introduced (not recommended because the threat model might never be complete enough to be valuable, but can be done)

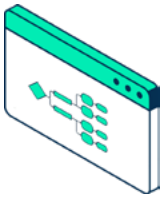
[19] *Agile Methodology by Atlassian*



Important Note: In general, a threat model is a "live" document. There might be cases that the threat models will not be 100% complete, and that should be fine. Whatever is selected from the above, take into account that the threat models need to be updated/recertified often (See Chapter: Treating threat models and Follow-Up), with iterations that work for the organization, and progressively improve the threat models until they reflect reality.

6.2 Determining the Threat Modeling Methodology

There are various methodologies[20] that can be selected to deliver threat models. Whichever methodology an organization picks to deliver threat models, it should answer the following four questions in order to be considered effective.



1. What are we working on?

2. What can go wrong?

3. What are we going to do about it?

4. Did we do a good enough job?

Diving into the above questions in detail:

1. **What are we working on?**
   This question aims to clearly define the system, application, or product being developed. It involves understanding the architecture, components, data flows, user interactions, and the overall purpose of the system. This foundational understanding helps identify the scope of the Threat Modeling exercise and sets the context for identifying potential threats.

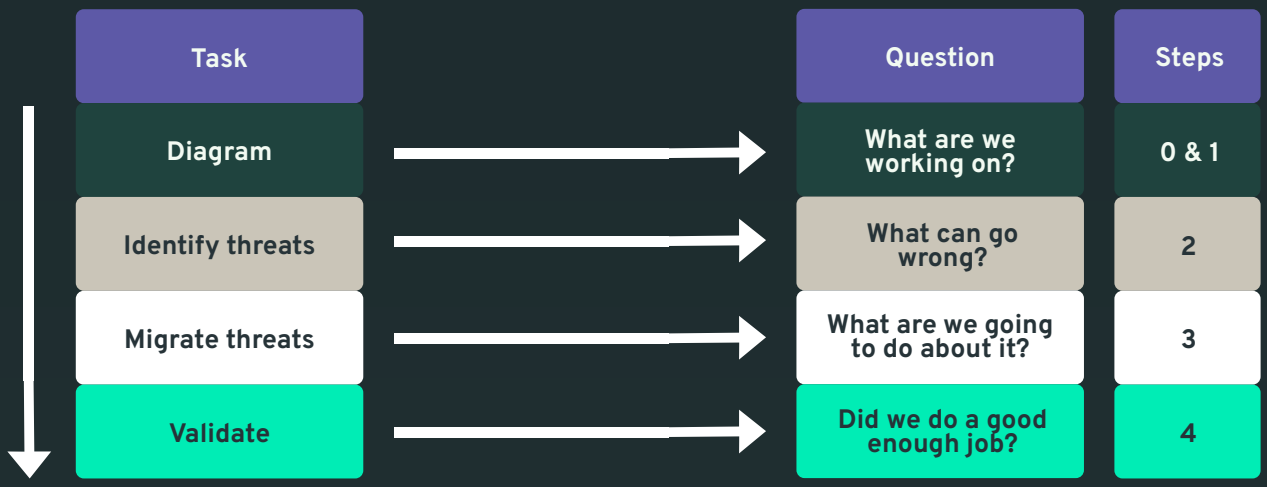
2. **What can go wrong?**
   This question focuses on identifying potential threats and vulnerabilities in the system. It involves brainstorming and analyzing various scenarios where the system could be attacked or fail. Consider different types of threats such as unauthorised access, data breaches, denial of service attacks, and insider threats. This step aims to uncover as many potential security issues as possible.

3. **What are we going to do about it?**
   This question addresses the mitigation strategies and actions to counteract the identified threats. It involves developing a plan to reduce or eliminate the risks associated with each threat. This could include implementing security controls, adding encryption, performing regular security audits, and creating incident response plans. The goal is to enhance the system's security posture and reduce the likelihood and impact of potential threats.

[20] *Threat Modeling - 12 Available Methods*

4. **Did we do a good enough job?**
   This question is about evaluating the effectiveness of the Threat Modeling process and the implemented security measures. It involves reviewing and testing the mitigations to ensure they adequately address the identified threats. This step might include security testing, code reviews, and validating that the security controls are functioning as intended. Continuous assessment and improvement are key to maintaining a robust security posture over time.

To answer the 4 questions above the process of creating a threat model can be split into 5 steps:



➜ **Step 0:** Initiating a threat model it would be wise to engage with the product stakeholders to gather information about the product:

- Understand the business part of the product.
  - Obtain business objectives for Product (Meetings with Stakeholders)
  - Identify regulatory compliance obligations (Meetings with Stakeholders)
  - Define a risk profile or business criticality level for the application
  - Identify the key business use cases for the Product
  - Plan Execution with Stakeholders
- Understand the technical part of the product.
  - Enumerate software application/database in support of product
  - Enumerate system platforms that support product
  - Identify all components that the product includes
  - Enumerate services needed for product
  - Enumerate if 3rd party commercial-off-the-shelf (COTS) needed for solution
  - Identify 3rd party infrastructure, cloud solution, hosted networks, mobile devices.

➜ Step 1: Create a visual representation of the product to understand how it functions and how data flows through it. Using IriusRIsk to:

Notes to take into account[21]: Elements of a Data Flow Diagram (DFD). A DFD consists of four main elements:

1. External entities - these are outside actors that interact with the system, like users or third-party services.
2. Processes - these are the activities that manipulate data within the system.
3. Data stores - these are the places where data is stored, like databases or files.
4. Data flows - these are the paths that data takes as it moves through the system.

Visualizing the product's components and how they interact reveals the path data flows take, exposing potential weak points along the way.

Best Practices for Creating Data Flow Diagrams:
Creating effective DFDs is an art, and there are some insider tips to master it.

- Keep it simple - start with a high-level diagram and add detail as needed.
- Use consistent notation - this makes the diagram easier to understand and maintain
- Focus on the data - the goal is to understand how data moves through the system, so don't get bogged down in implementation details.
- Collaborate with stakeholders - DFDs are a great communication tool, so involve the right people in their creation and review them at least annually.

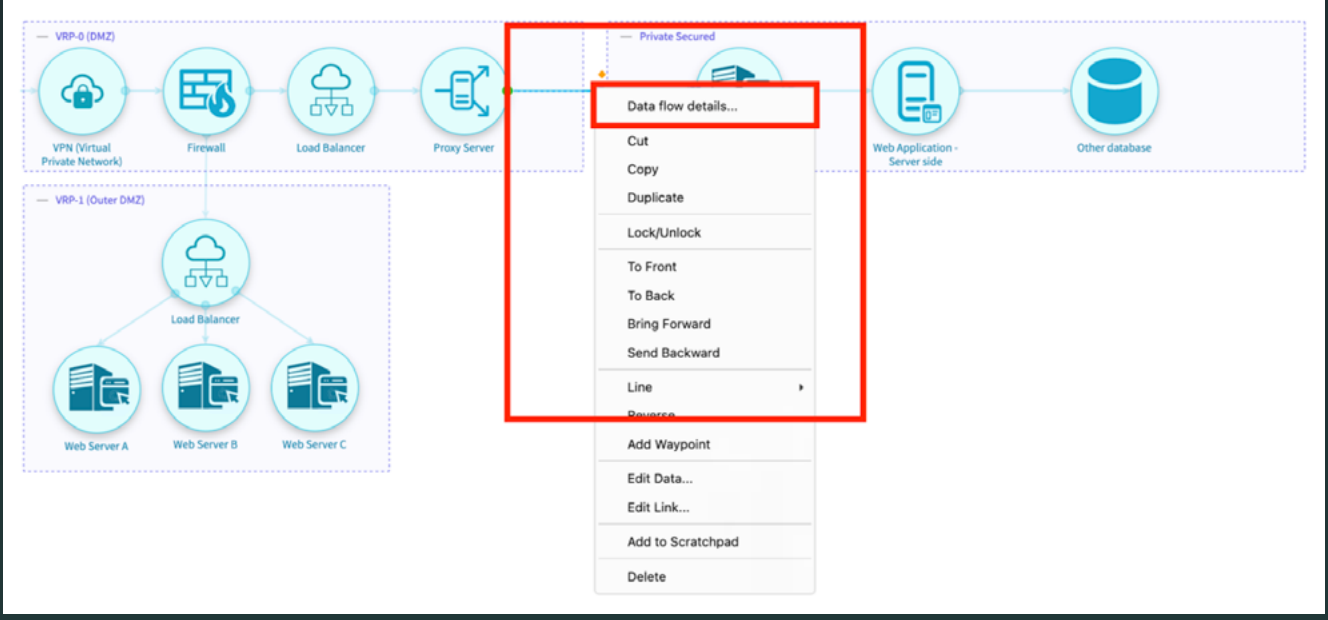
Continue with the steps:

- Define System Boundaries
  - Identify the scope of the Product being modeled.
  - Determine the boundaries between what is inside and outside.
- Identify Trust Boundaries
  - Create the boundaries where data flows between different levels of trust (e.g., user to server).

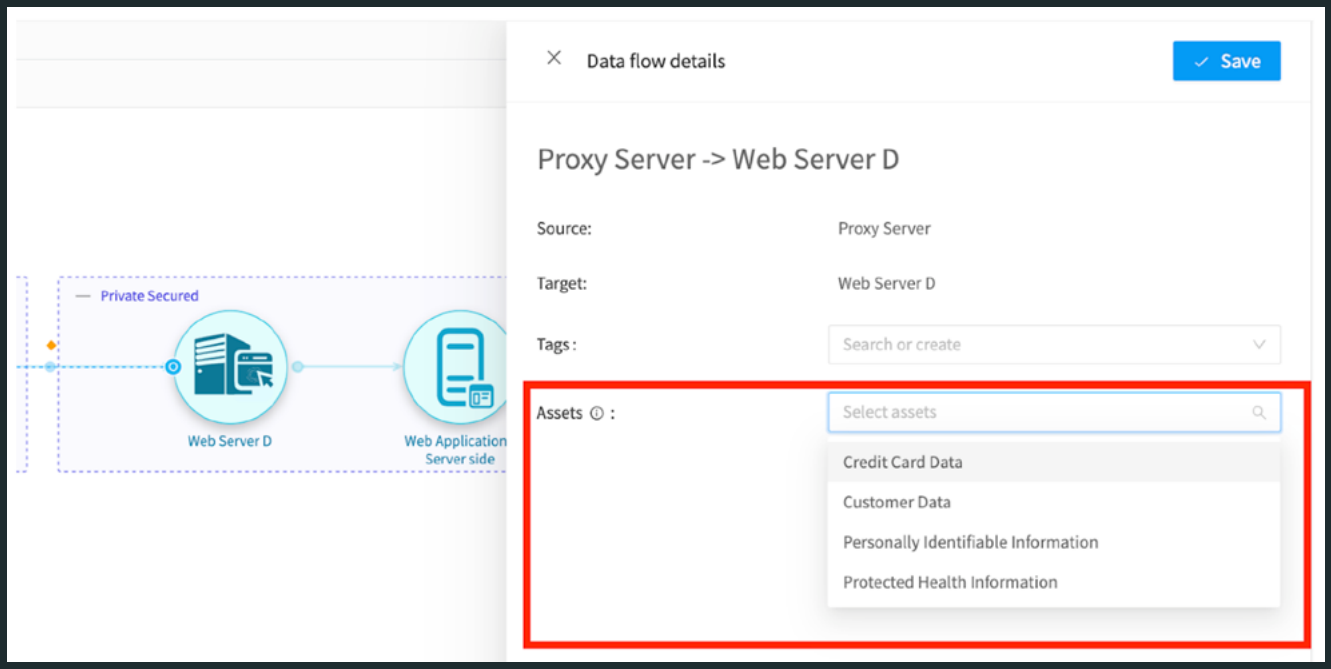
[21] *The Beginners guide to Threat modeling by IriusRisk*

- Create the basic components
  - Break down the Product into smaller components (e.g. databases, modules etc.).
  - Start creating a map of how these components interact with each other and with external entities (that is the start of the next step).
  - After the most important components are placed, dive into a more detailed diagram.

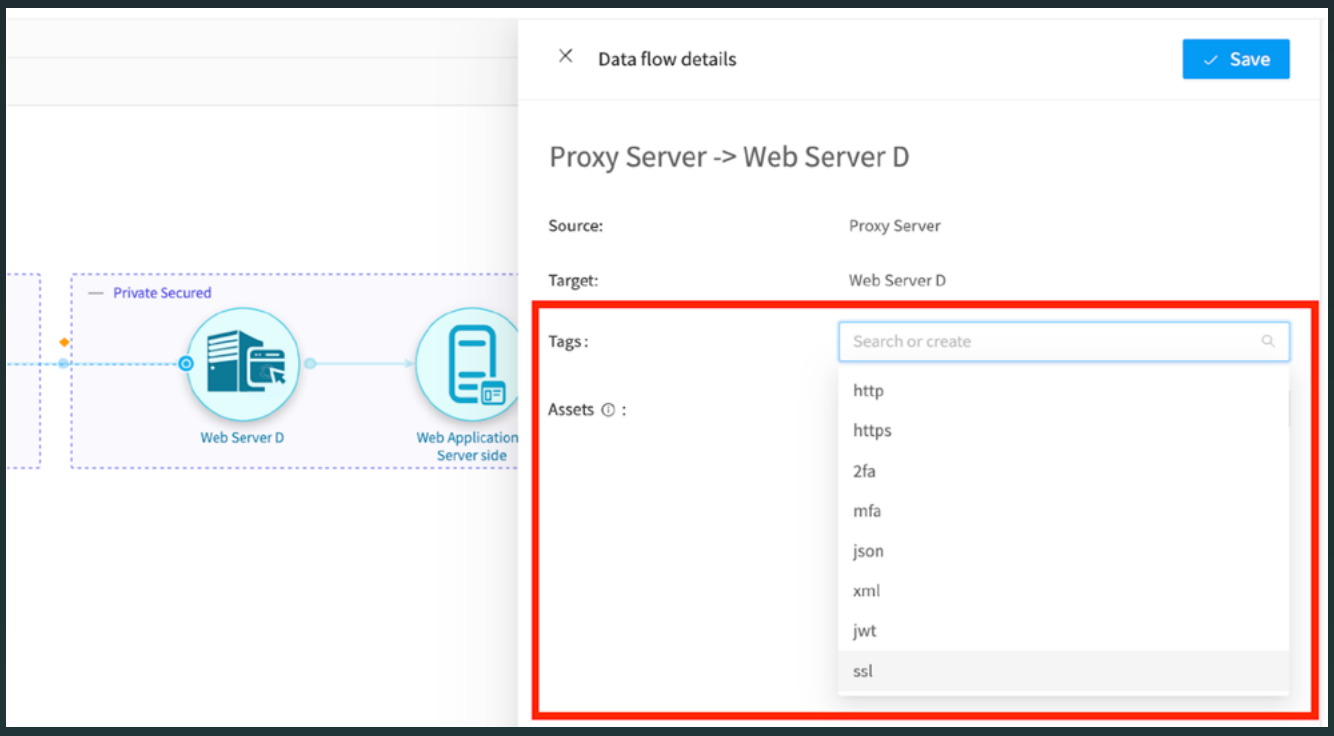
- Create Data Flows
  - Diagram the flow of data within the trust boundaries and with the other trust boundaries.
  - Assign “Assets” and “Protocols” to data flows.



  - Assign “Assets” → Right-Click on “Data Flow Arrow” → Select “Data Flow Details” → Select “Assets”



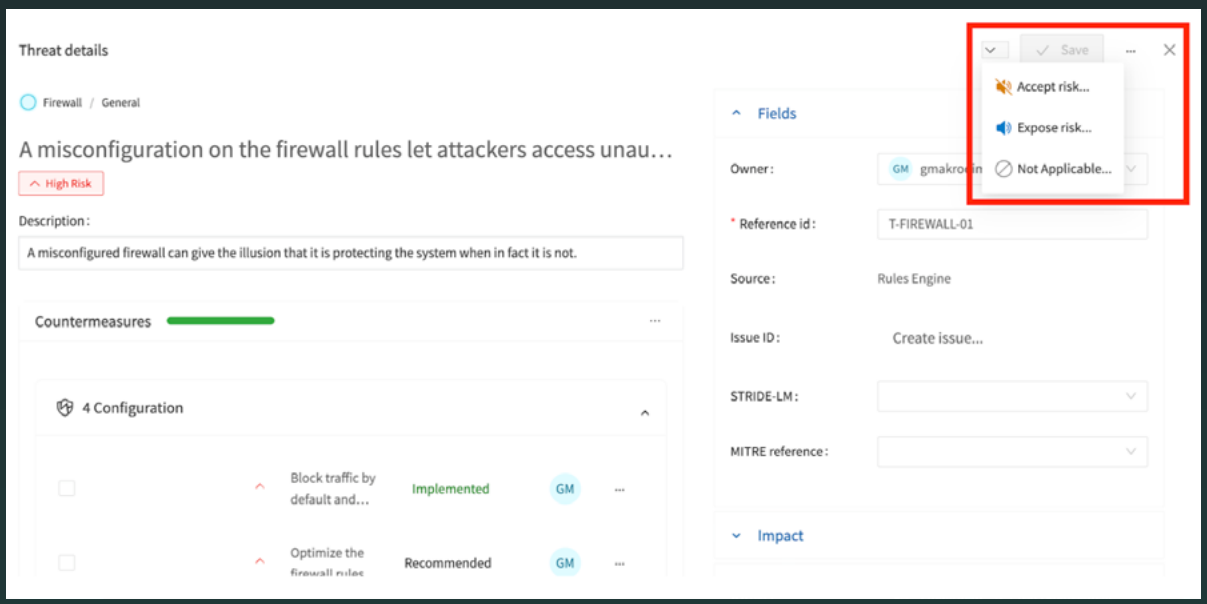
- Assign Protocols (named “Tags”) → Right-Click on “Data Flow Arrow” → Select “Tags”



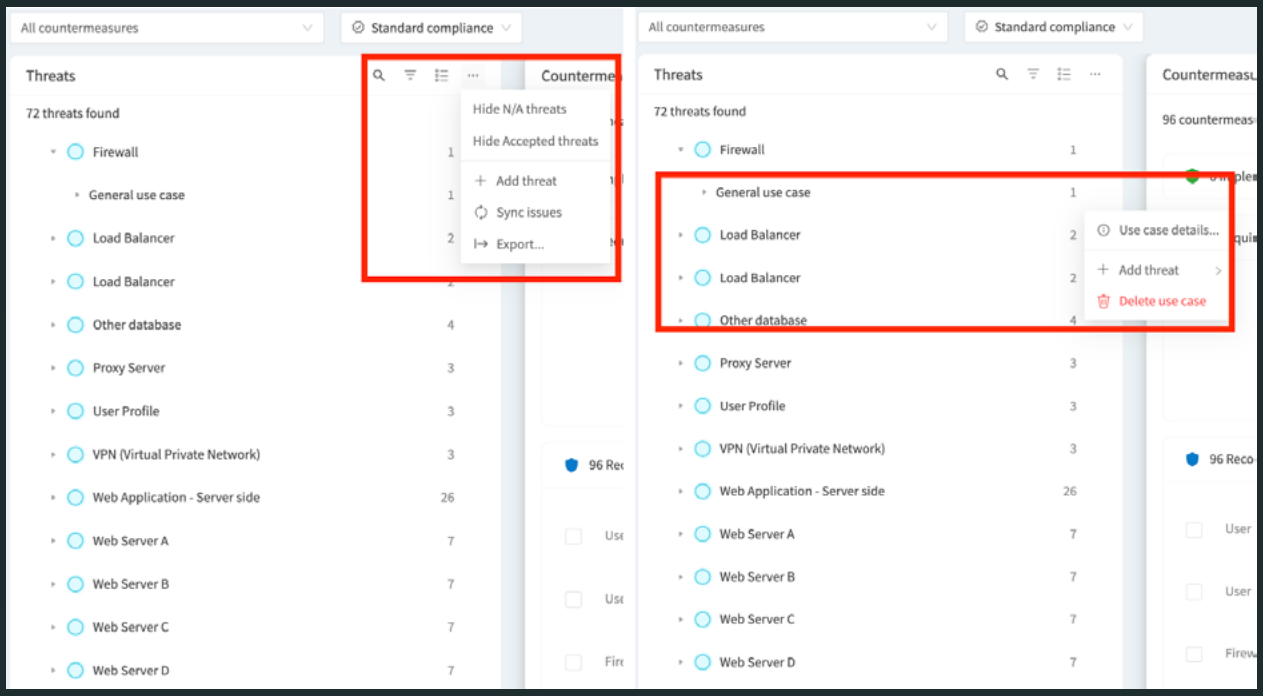
Note: Improve the diagram by adding other components that are identified and show how they interact with each other and with other trust boundaries.

➜ Step 2: Study the threats generated by IriusRisk:

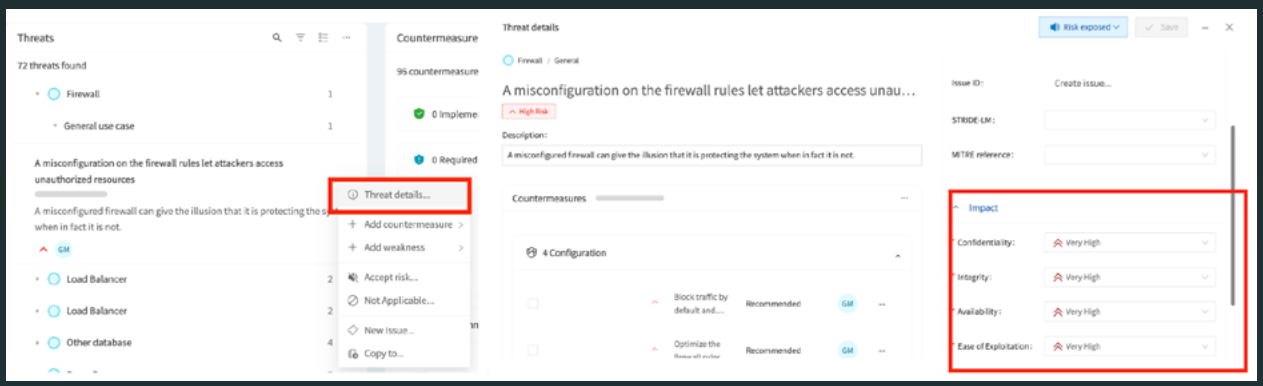
- Review all the generated threats produced by IriusRisk
  - Clicking on “Threats and Countermeasures”.
- Adjust the identified threats by choosing to “Accept Risk”, “Expose Risk”, or remove by choosing “N/A”
  - *Accept Risk: The risks of the threat are Accepted by the organization e.g., within risk appetite of the organization.*
  - *Expose Risk: The risks that are valid, and should be mitigated.*
  - *N/A: Does Not take into account the risk of the threat, a.k.a Not Applicable.*



- Also, there is the option to “Add Threats” if required.

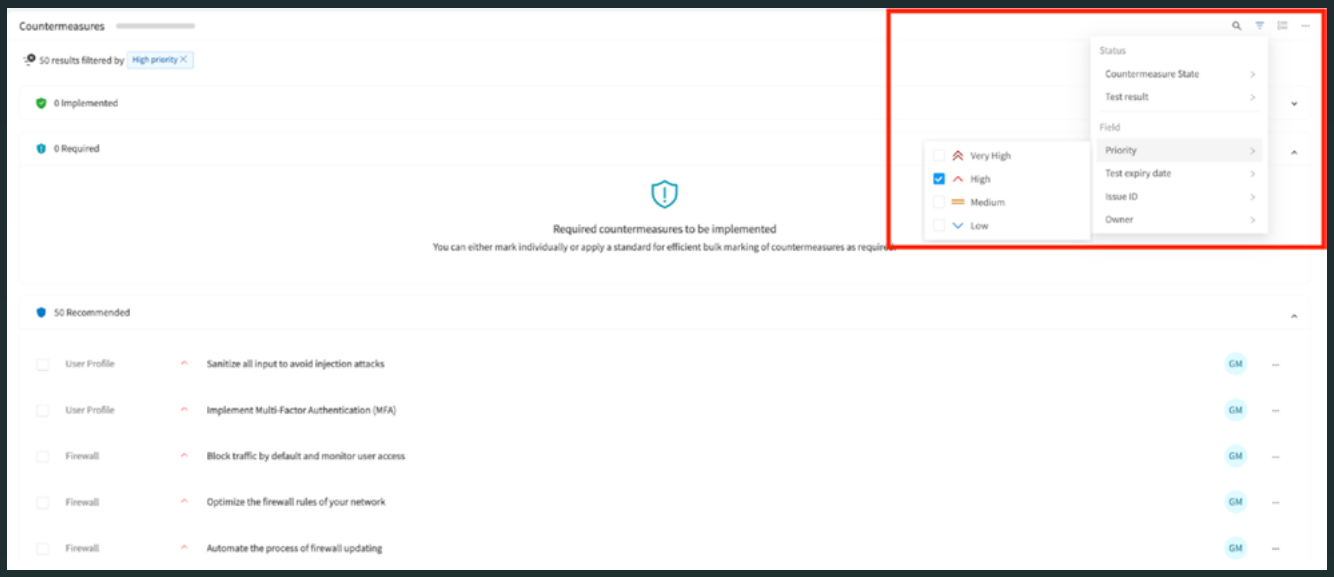


- Adjust fields if required (e.g., Confidentiality, Integrity, Availability, Ease of Exploitation).

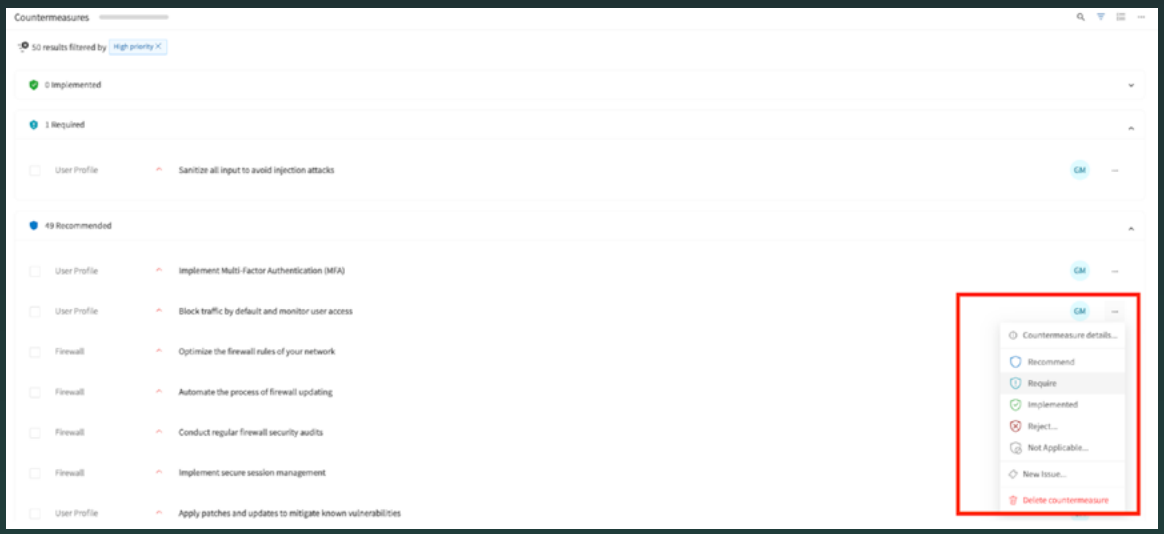


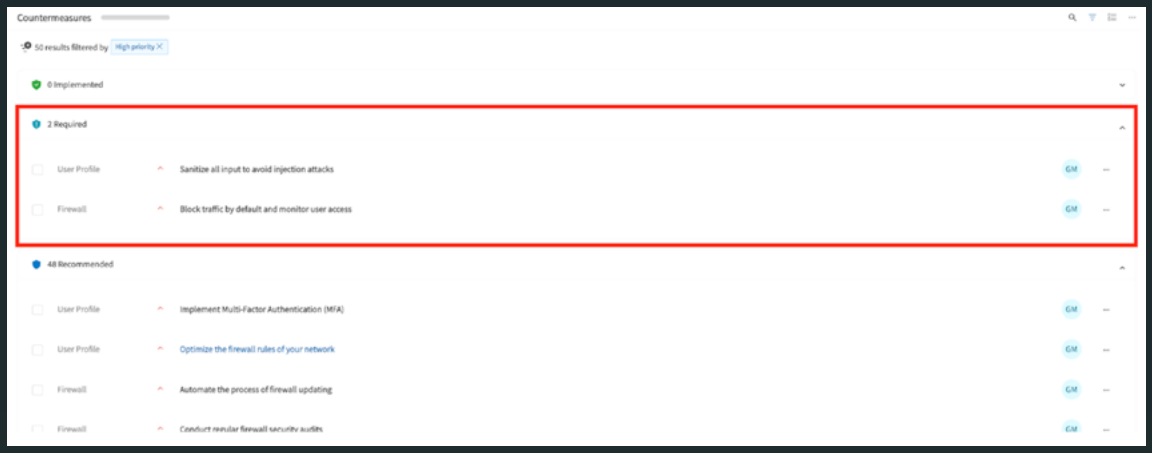
➜ Step 3: Using IriusRisk to identify the relevant countermeasures according to the generated threats, and develop strategies and actions to reduce or eliminate these threats:

- Various approaches can be used to start with the implementation of countermeasures.
  - Prioritize Threats using the filtering option to view what countermeasure based on threat severity.
    Note: For prioritization it is strongly recommended to start with the "Very High" and "High" priority ones. In addition, make sure to check if the threats are "Applicable" or not, as some threats might not be relevant and can quickly remove some from the list. In the end, the user will have a list of the highest priority threats that can start reviewing the recommended countermeasures.

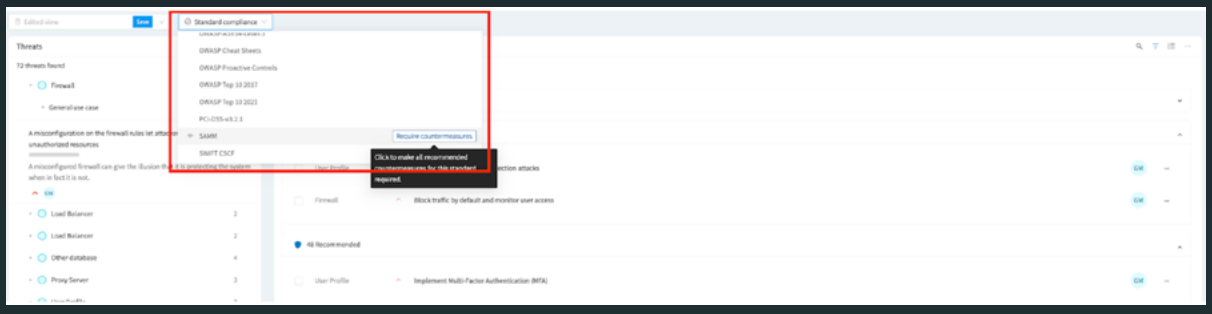


- The user can manually select specific countermeasures to be required (or N/A, or Rejected, depending on the knowledge the user has on the product). This will move the countermeasure to the "Required" Section, or to the corresponding section selected.

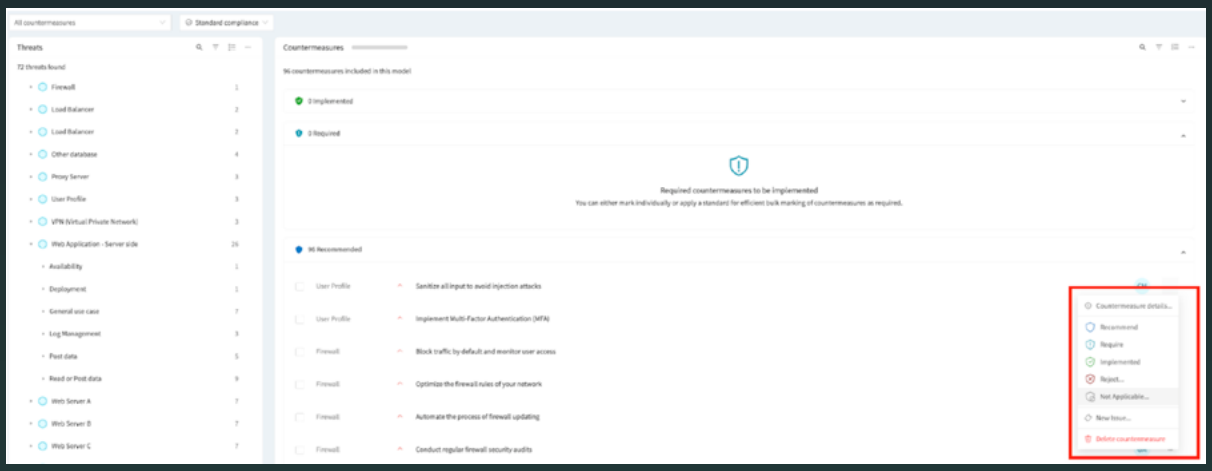




- Or the user can select a Standard in order to force countermeasures to move to “Required” to show what countermeasures are required to be compliant with that Standard.

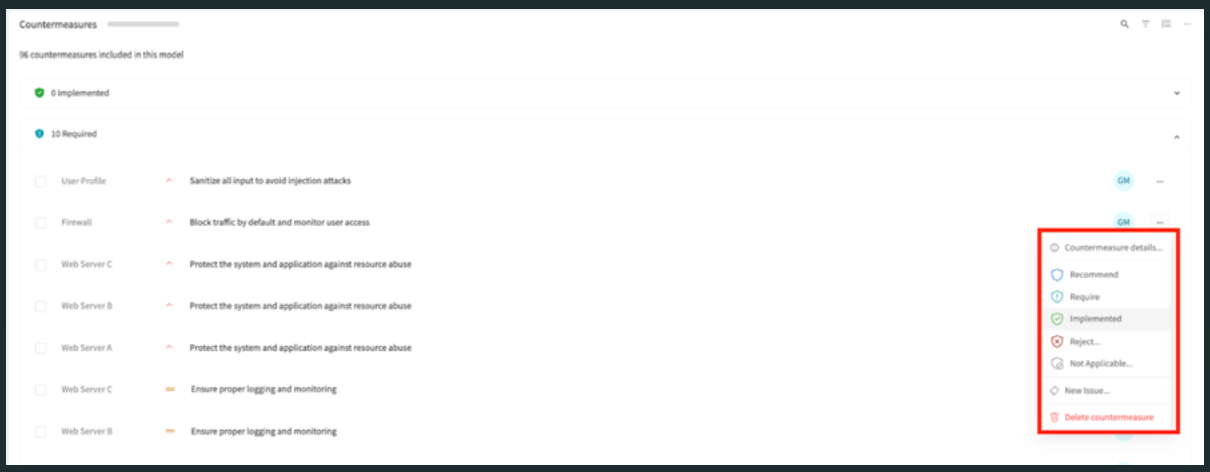


- Review, filter and adjust the details of countermeasures.



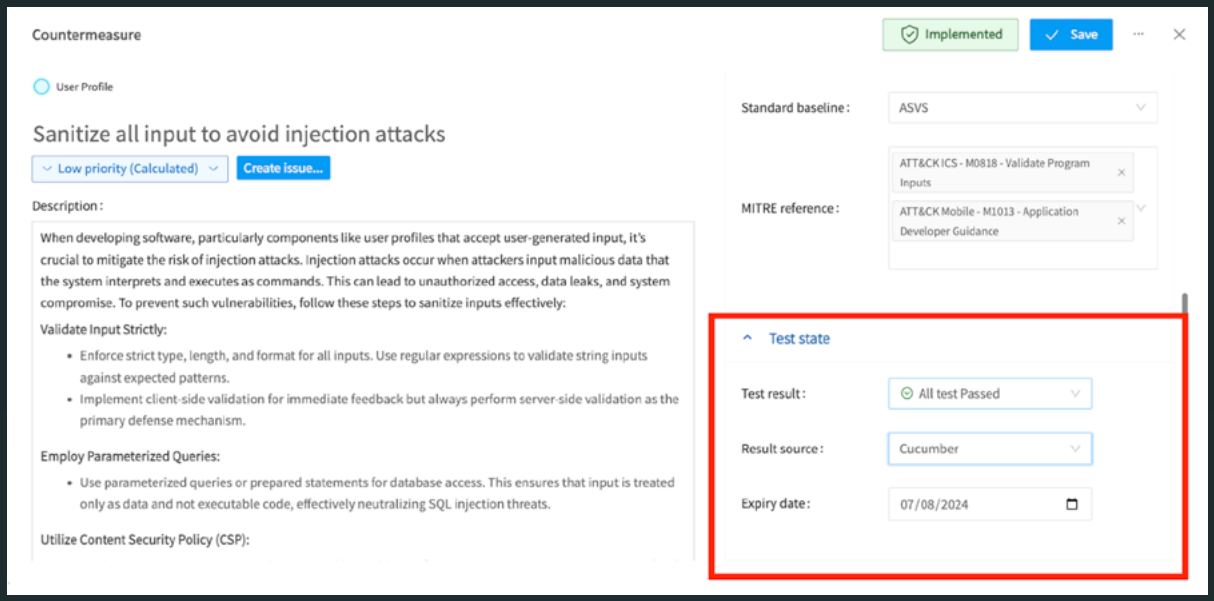
- Once the user has a “Required Countermeasure” list, develop mitigation strategies based on the identified security controls and measures of each threat.
- Implement mitigations by integrating the identified countermeasures into the system design and development process. It is recommended to have a robust process of how the user will share this information with the relevant stakeholders.

- Update the status of mitigations for each countermeasure that is implemented.



➜ Step 4: Validation - This step is very critical as the Threat Modeling Practitioners need to validate the created threat model. They need to make sure that there is a plan to mitigate the threats and that the results are efficiently communicated with the business stakeholders:

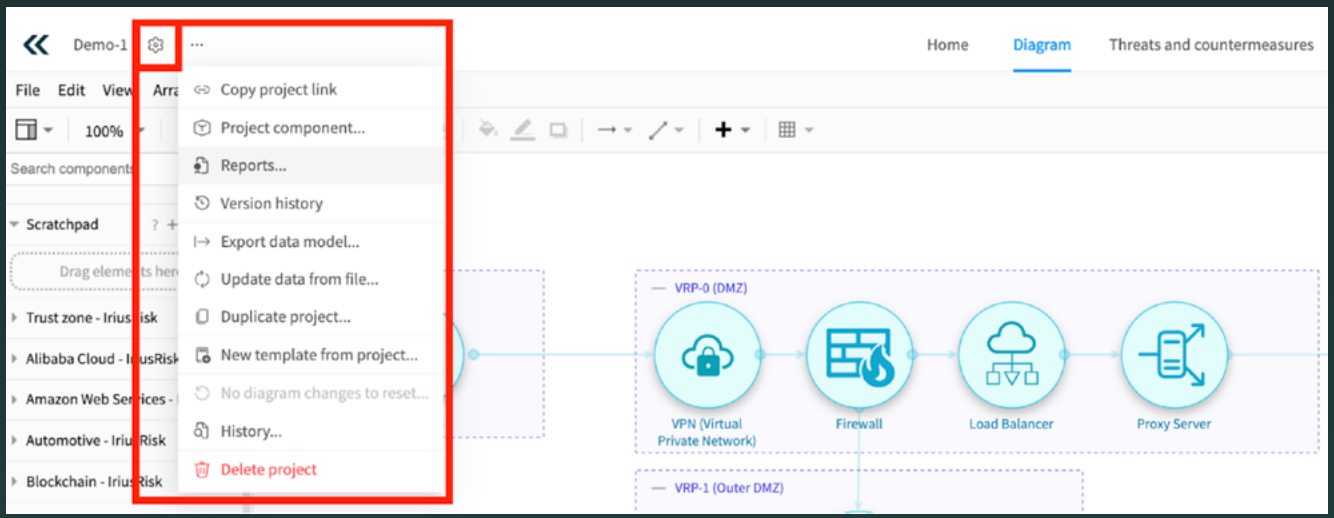
- Review and test mitigations.
  - By conducting security testing such as penetration testing and asking the pentesters to test specific use cases mapped to the identified threats/ countermeasures.
  - Perform simulations and attack scenarios to test how the system responds to threats.
- Peer and expert reviews.
  - Make sure that the threat model will be shared with peers and experts to provide feedback to improve the Threat model and mitigation plans.
- Monitor and update.
  - Continuously monitor the Product for new threats and vulnerabilities.
  - Regularly review and update the threat model and mitigation strategies to address emerging threats and changes.
- Record validation results.



In each validation of a threat model, it is recommended to also assess if the used methodology is robust and it works for the organization. Changes are recommended in order to tailor the methodology for the organization needs. It is advised that an organization should not be worried about changing the methodology and adapting it as it is important to find the right way to reduce friction and costs.

6.3 Reporting

At the end of every threat model, a report describing the key findings to audiences should be created. A comprehensive Threat Modeling report is essential for stakeholders as it clearly communicates risks, enabling informed decision-making and resource allocation. A good report will build trust with/among stakeholders by demonstrating a commitment to security, by facilitating cross-functional collaboration, and by serving as valuable documentation for future reference and training.



The reports that can be generated are:

- Current Risk Management Report
- Technical Threat Report
- Technical Countermeasure Report
- Compliance Report

These reports can be valuable as they are but sometimes they might be either very detailed or missing details. Therefore, in general, it would be preferable for the Threat Modeling team to be able to create their own reports based on the level of detail needed. Consequently, even though the software provides the Report export function, the Threat Modeling team should be able to create the two following documents:

- Threat model digest - For Senior Management Audience → Threat Modeling Digest Report
- Threat model detailed - For Technical Audience → Threat Modeling Detail Report

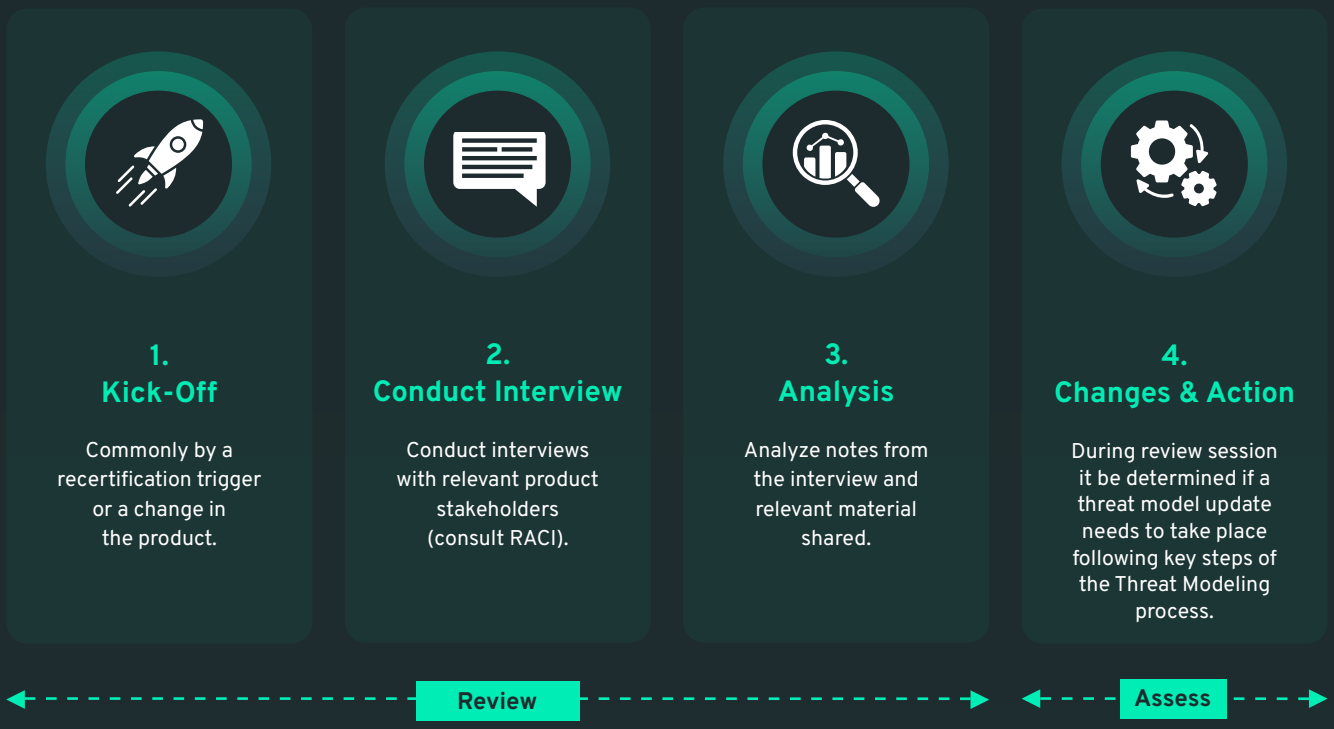
6.4 Treating Threat Models & Follow Up

As previously mentioned, threat models are "live" documents. Best scenario would be that when a change takes place in the product, there should be updates in the threat model, however it is very possible that updates to the threat models will be missed. Therefore, it is recommended to have a structure recertification process in place because even though changes might not trigger an update to a threat model, it would be good to have a structured and frequent review and update the threat models.

According to 6.1.2 Prioritization of the critical products, a way to establish a recertification process is by risk profile category, for example:

- **High-Risk Products:** Recertify **every 3 months**
- **Medium-Risk Products:** Recertify **every 6 months**
- **Low-Risk Products:** Recertify **every 9 months**.

Note: *The above serves as an example, and should be tailored according to organization needs.*



The above serves as a high-level approach when there is a change in the product or the periodic recertification trigger takes place.

6.5 Retrospectives and Optimization

For companies that are starting from zero, it is important to conduct retrospectives, internal feedback, to assess the process and the outcomes of the threat models to determine where and how they can improve.

They should focus on:

- What worked well?
- What didn't go well??
- What can be done to improve?
- What should be changed?

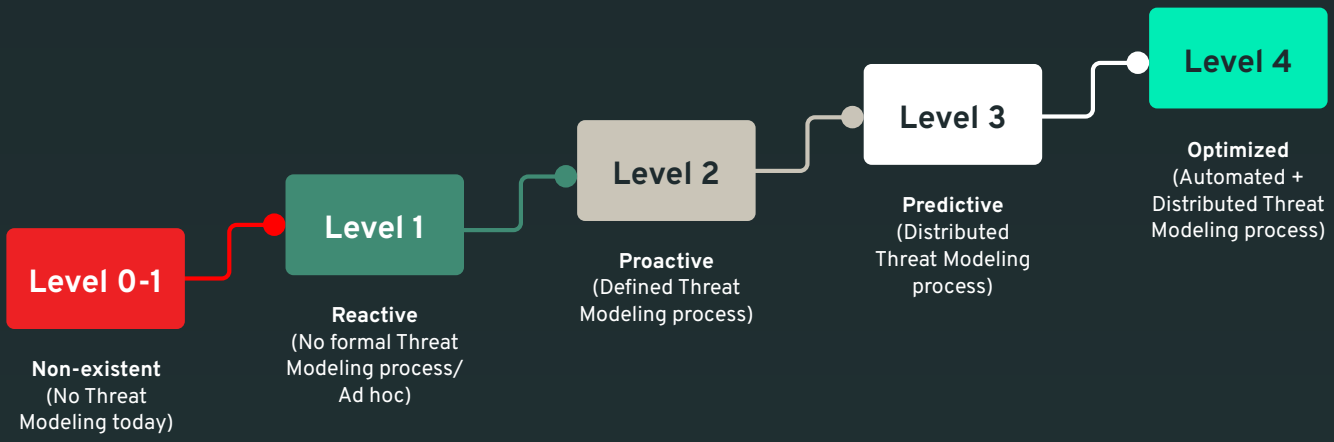
In addition, it is recommended to do external assessments by planning meetings with the Product teams to gather their view of how the threat model affected them (e.g., resources, time etc.). This will provide valuable information on how the interaction with the Product team can be improved and create less friction.

Chapter 7: Optimization of Threat Modeling

The last part of the playbook will discuss Threat Modeling optimization, covering a Threat Modeling Maturity Framework, and Metrics and Reporting. This step is the core of the Threat Modeling function and where the real value is generated.

7.1 Threat Modeling Maturity

The Threat Modeling Maturity Framework (TMMF) helps organizations to understand their current state in terms of Threat Modeling and provides guidance on how to advance to more mature practices.



Description:

- **Level 0 - Nonexistent:** At this stage, the organization does not perform Threat Modeling. Security concerns are not systematically identified or addressed during the software development lifecycle (SDLC). This often results in reactive security measures.
- **Level 1 - Reactive:** Threat Modeling is performed sporadically, typically initiated by the Threat Modeling team, security-conscious developers or in response to specific incidents. There is no standardized approach or documentation.
- **Level 2 - Proactive:** The organization has established a defined Threat Modeling process and a methodology, which is consistently followed across multiple projects. The process is documented, and the results are used to inform security requirements and design decisions.

- **Level 3 - Predictive:** Threat Modeling is distributed across the organization, with multiple teams independently conducting Threat Modeling as part of their standard workflow. The process is scalable and adaptable to different types of projects.
- **Level 4 - Optimized:** The organization has fully automated aspects of the Threat Modeling process and has successfully distributed the practice access to all relevant teams. Threat Modeling is an integral part of the SDLC, and the process evolves continuously to address new threats.

Moving from one maturity level to the next requires a combination of strategic planning, training, process improvement and tooling. The organization should focus on building a strong foundation (as described in the first Chapters) so they can naturally progress to the next levels, ensuring that practices are scalable, sustainable, and continuously evolving to meet new security challenges in the continuously changing threat landscape.

In-depth, the natural progress in the Threat Modeling Maturity Framework should look as below.

Stage 0 - Non existant	
Description	The organization does not perform threat modeling. Security concerns are not systematically identified or addressed during the lifecycle (SDLC). This often results in reactive security measures.
Current Status	• Security issues are identified post-deployment or during testing. • No formal security guidelines or threat identification process. • Lack of security awareness among teams. • No Threat Modeling teams. • No Threat Modeling vision, mission, plan, roadmap etc.
Transition to next step	**Training & awareness:** Initiate basic security awareness and Threat Modeling training for teams. **Pilot project:** Conduct a small, ad-hoc Threat Modeling exercise to demonstrate value. **Build a team:** Indentify or form a Threat Modeling team. **Strategic planning:** Threat Modeling plan and roadmap etc. **Senior leadership acknowledgement:** Show senior leadership the value of Threat Modeling and get buy-in.

Stage 1 - Reactive

Description

Threat Modeling is performed sporadically, typically initiated by the Threat Modeling team, security-conscious developers or in response to specific incidents. There is no standardized approach or documentation.

Current Status

- Manual and inconsistent application of Threat Modeling across projects.
- Organization recognizes value of threat model.
- No standardized documentation or process.
- Relies on individual expertise and ad-hoc methods.

Transition to next step

Champion Programe: Start TM champions programme.
Tooling: Acquisition of IriusRisk TM tool.
Templates: Basic Threat Modeling templates and checklists.
KPIs/KRIs: Define KPIs and KRIs that should be implemented.
Develop Guidelines: Create simple, easy-to-follow guidelines and templates for Threat Modeling.
Standardization: Encourage all teams to follow a basic standardized process.
Document Learnings: Start capturing and sharing lessons learned from each Threat Modeling exercise.

Stage 2 - Proactive

Description

The organization has established a defined Threat Modeling process and a methodology, which is consistently followed across multiple projects. The process is documented, and the results are used to inform security requirements and design decisions.

Current Status

- Use of IriusRisk tool and adapt it organizational standards.
- TM Champions developers running threat models.
- Integrations of automated Threat Modeling in the SDLC, paticularly during the design phase.
- Basic KPIs/KRIs are implemented.
- Practice is integrated into development workflows.
- Documented process with clear roles and responsiblities.
- Consistent use of Threat Modeling methodologies (e.g. STRIDE).

Transition to next step

Expand Integration: Integrate Threat Modeling into additional SDLC phases, such as during code reviews and testing.
Collaboration: Foster cross-functional collaboration amoung developers, architects, and security teams.
Refinement: Continuously refine the process based on feedback.
Metrics & Reporting: Implement advanced metrics to measure effectiveness and quality of Threat Modeling process and be in a form able to be reported to stakeholders.

Stage 3 - Predictive

Description

Threat Modeling is distributed across the organization, with multiple teams independently conducting threat modeling as part of their standard workflow. The process is scalable and adaptable to different types of projects.

Current Status

- Fully established TM Champions Program (all products have at least 1 TM champion).
- Integration with other services (e.g JIRA).
- Threat Modeling is part of the standard workflow for multiple teams.
- Teams adapt the process to specific project needs while following a standard framework.
- Regular collaboration and outcome sharing across teams planned by the Threat Modeling team.
- Advanced KPIs and KRIs.

Transition to next step

Automation: Start automating aspects of the Threat Modeling process to improve efficiency.
Advanced Training: Offer training for complex threat scenarios.
Centralized Coordination: Established a platform for sharing threat models and bes practices.
Continuous Improvement: Implement a feedback loop for ongoing process improvement.

Stage 4 - Optimized

Description

Threat Modeling is fully automated where possible and distributed across all relevent teams. The process is continuously evolving and is and integral part of the SDLC.

Current Status

- Use of automation tools for generating and assessing threat models.
- Integrated into CI/CD pipelines for continuous security assessment.
- High level of collaboration and centralized oversight.
- Continuous updates to address emerging threats.
- Automated and in-depth Threat Modeling.
- Fully established TM Champions Program.
- Detailed analytics shared at exec level.

Transition to next step

Continuous Integration: Integrate Threat Modeling all phases of SDLC.
Emerging technologies: Keep pace with new technologies by integrating Threat Modeling for AI, IoT, etc.
Advanced Analytics: Use data analytics and machine learning for threat prediction and reponse.

7.2 Success Criteria - Defining KPIs and KRIs

When selecting and establishing KPIs (Key Performance Indicators) and KRIs (Key RIsk Indicators) for a Threat Modeling function, it is important to focus on both the effectiveness of the Threat Modeling process (described later) and the impact on overall security posture. These metrics should help the team continuously improve their processes and provide Senior Management with meaningful insights into the organization's security picture and the effectiveness of Threat Modeling activities.

Commonly, the KPIs and KRIs are defined during the development of the Strategy. The earliest they are defined, the quicker the results as some metrics will need to be captured enough times to be understood. In addition, it is important to note that KPIs and KRIs are more efficient when there is more maturity in Threat Modeling. That is how sometimes it comes on Stages 3, 4 and 5. See Chapter: Threat Modeling Maturity). However, this should not create a block from attempting to use KPIs and KRIs earlier when there is low maturity, and improve along the way.

Then according to the Threat Modeling Maturity Framework implementation of KPIs and KRIs should look like this:

At Stage 0: KPIs and KRIs are generally not applicable.

- **At Stage 1:** Selection and definition of **Basic KPIs and KRIs** to measure the initiation of Threat Modeling processes and their outcomes.
- **At Stage 2:** Implementation of **Basic KPIs and KRIs** to cover basic aspects of the Threat Modeling process, integrating them with broader SDLC phases.
- **At Stage 3:** Implementation of **Advanced KPIs and KRIs** to cover advanced aspects of the Threat Modeling process, integrating them with the SDLC phases.
- **At Stage 4:** Mature the KPIs and KRIs to ensure they are aligned with strategic goals and optimize KPIs and KRIs for real-time insights and predictive capabilities, ensuring that they support operational and strategic decision-making.

The following list of KPIs are metrics that measure the effectiveness, efficiency and coverage of the Threat Modeling process, ensuring it successfully identifies and mitigates potential security threats within an organization.

7.2.1 What KPIs and KRI should be developed?

Defining KPIs and KRIs can be difficult at the first steps of the Threat Modeling function. Below, there are a few examples of how to start. Note that to define KPI and KRI effectively, a company should have an up-to-date product inventory and their criticality level recorded.

Basic KPIs	Description	Purpose	Measurement	Calculation Formula	Target/ Benchmark	Considerations	Example
Threat Models Completed.	Number of threat models completed within a specific time frame (e.g., per quarter).	Measures the throughput of the team and helps understand the efficiency of the Threat Modeling process.	Number of threat models completed per quarter.	(Completed Models / Planned Models) * 100.	Target: 90% of planned models completed per quarter.	Ensure that planned models are realistic and resource-allocated.	In Q1, the team planned to complete 10 threat models. By the end of the quarter, they successfully completed 9 models, achieving 90% of the planned target.
Average Time to Complete a Threat Model.	The average duration it takes to complete a threat model from start to finish.	Indicates the efficiency of the process and can highlight bottlenecks.	Average duration (in days) to complete a threat model.	Total Time Spent on Models / Number of Models Completed.	Benchmark: < 30 days.	Track by project phase (e.g. Kick-off, model creation) for deeper insights.	The team completed 9 threat models in Q1, with a total of 270 days spent across all models. The average time to complete each model was 270 / 9 = 30 days.
Average Time in Stage.	The average amount of time a model is being spent in each threat modeling phase.	Determine where teams might be struggling to apply Threat Modeling concept.	Total time spent in diagramming, threats review, countermeasure review, etc.	Total Time Spent Summed.	Variable.	Track by group of projects to observe trends in teams or systems.	In Q2, the teams spent approximately 30% more time in scoping systems of type x. This may be because the supporting teams do not provide sufficient documentation.
Coverage of Critical Products.	Percentage of critical systems, applications, or data assets that have a completed threat model.	Ensures that the most important parts of the organization are adequately covered by threat models.	Percentage of critical products with completed threat models.	(Critical Products Covered / Total Critical Assets) * 100.	Target: 100% Coverage of Critical Products.	Prioritize Products on business impact and risk level.	The organization has 20 critical assets, and 18 of them have a completed threat model. The coverage of critical assets is (18 / 20) * 100 = 90%.
Number of Threats Identified per Model.	Average number of threats identified in each threat model.	Helps understand the depth and thoroughness of the Threat Modeling process.	Average number of threats identified per threat model.	Total Threat Identified / Number of Models Completed.	Target: Increasing trend (year-on-year basis).	Adjust the model complexity or scope based on findings.	Over the course of Q1, 9 threat models identified a total of 63 threats, averaging 63 / 9 = 7 threats per model.

Average Number of Threats Identified Via Automated Threat Modeling vs Manual.							
Types of Threats (e.g. design flaws, authentication based etc.)							
Alignment with Development Life Cycle.	Percentage of threat models that are completed and reviewed within the project timelines.	Ensures that Threat Modeling is integrated into the development life cycle without causing delays.	Percentage of threat models completed within project timelines.	(Models Completed On-Time / Total Models Completed) * 100.	Target: 95% Alignment.	Integrate Threat Modeling checkpoints into development timelines.	Out of 9 completed threat models, 8 were completed within the project timelines, resulting in an alignment rate of (8 / 9) * 100 = 88.9%.

Advanced KPIs	Description	Purpose	Measurement	Calculation Formula	Target/ Benchmark	Considerations	Example
Stakeholder Satisfaction.	Satisfaction level of stakeholders (e.g., development teams, project managers) with the Threat Modeling process and its outputs.	Gauges the perceived value and effectiveness of Threat Modeling from those who rely on its outcomes.	Average satisfaction score (1-5) from stakeholders. Score to be received on retrospectives.	(Sum of Stakeholder Satisfaction Scores / Number of Re-spondents).	Benchmark: ≤ 4.0.	Use anonymous surveys to get honest feedback. Analyze the trends over time.	After completing the threat models, the team conducted a survey of stakeholders during retrospective, who rated the process with an average satisfaction score of 4.2 out of 5.
Risk Reduction Post-Implementation.	Measure the percentage reduction in identified risks after threat mitigation strategies have been implemented.	Indicates the effectiveness of Threat Modeling in reducing overall risk.	Percentage reduction in identified risks after mitigation.	(Initial Risk Score - Post-Mitigation Risk Score) / Initial Risk Scope) * 100.	Target: 75% reduction in risk.	Use Standardized risk scoring models for consistency (offered by IriusRisk).	A system had an initial risk score of 80. After implementing mitigations identified through Threat Modeling, the risk score dropped to 20, resulting in a 75% risk reduction.
Defect Rate Post-Deployment.	Number of security defects found post-deployment in components that underwent Threat Modeling.	Assesses the quality of the Threat Modeling process and its impact on the security of deployed systems.	Number of security defects found post-deployment in components with threat models.	Total Post-Deployment Defects / Number of Deployment.	Benchmark: ≤ 5 defects per release.	Correlate defects with specific threats that were missed or not mitigated.	After deploying a system that underwent Threat Modeling, 2 security defects were found out of 5 releases, resulting in an average defect rate of 2 / 5 = 0.4 defects per release.

In addition, below there is a list of KRIs metrics that assess the potential risks and vulnerabilities in an organization's security posture, highlighting areas where identified threats are not effectively mitigated or where the Threat Modeling process may be inadequate.

Basic KRIs	Description	Purpose	Measurement	Calculation Formula	Target/ Benchmark	Considerations	Example
Unmitigated High-Risk Threats.	Number or percentage of identified high-risk threats that remain unmitigated.	Highlights potential vulnerabilities that could have a significant impact on the organization.	Percentage of high-risk threats that remain unmitigated.	(Unmitigated High-Risk Threats / Total High-Risk Threats) * 100.	Threshold: ≤ 10% of identified high-risk threats.	Escalate unresolved threats to senior management as soon as possible.	Out of 20 high-risk threats identified in Q1, 18 were mitigated, leaving 2 unmitigated. The percentage of unmitigated high-risk threats is (2 / 20) * 100 = 10%.
Frequency of Threat Model Updates.	The average time between updates to threat models for critical products.	Indicates how well the team is keeping up with evolving threats and changes in the environment, but also with the Development Lifecycle.	Average time (in months) between updates to threat models for critical products.	Total Months Since Last Update / Number of Models.	Benchmark: ≤ 6 months.	Regularly review and update models, according to Business Impact and Risk Profile. See Chapter: **Treating Threat Models and Follow Up.**	The last update for a critical asset's threat model was 5 months ago, and it's now due for a review. The team has consistently updated models every 5 months, within the benchmark of 6 months.
Escalation of Unaddressed Threats.	The number of threats that have been escalated to Senior Management due to lack of action.	Measures the effectiveness of the threat mitigation process and responsiveness of management.	Number of threats escalated to senior management due to lack of action.	Total Number of Escalated Threats.	Threshold: ≤ 2 per quarter.	Monitor root causes of escalations and how to address them.	In Q1, 3 threats identified in previous models were not mitigated and had to be escalated to senior management for further action. This is above the threshold of 2 per quarter.
Gaps in Threat Coverage.	Percentage of systems or assets that have not undergone Threat Modeling.	Identifies potential blind spots in the organization's security posture.	Percentage of products not covered by threat models.	(Uncovered Products / All Existing Products) * 100.	Threshold: ≤ 5% of existing Products.	Identify and Prioritize gaps in coverage, especially for high-risk assets.	The organization has 50 total Products, with 3 not covered by threat models. The gap in threat coverage is (3 / 50) * 100 = 6%.

Advanced KRIs	Description	Purpose	Measurement	Calculation Formula	Target/ Benchmark	Considerations	Example
Impact of Missed Threats.	Severity of incidents or breaches related to threats that were not identified during Threat Modeling.	Reflects the accuracy and comprehensiveness of the Threat Modeling process.	Severity (measure in impact score) of incidents or breaches due to missed threats.	Total Severity Scores of Incidents from Missed Threats / Number of Incidents.	Threshold: ≤ 5 on a 10-point severity scale.	Use incidents post-mortems to refine threat identification processes.	A security incident occurred due to a missed threat, resulting in an impact severity score of 6 out of 10. This exceeds the desired threshold of less than 5.
Time to Mitigate Identified Threats.	Average time taken to address and mitigate threats identified during Threat Modeling.	Measures the responsiveness and agility of the organization in addressing security risks.	Average Time (in days) to mitigate identified threats.	Total Days to Mitigate Threats / Number of Threat Mitigated.	Benchmark: ≤ 45 days.	The average time to mitigate 10 identified threats was 40 days, which is within the acceptable benchmark of ≤ 45 days.	The average time to mitigate 10 identified threats was 40 days, which is within the acceptable benchmark of ≤ 45 days.

7.2.1.1 Return on Investment (ROI) of Threat Modeling

Proving the Return on Investment (ROI) of Threat Modeling to senior management involves demonstrating how the process contributes to the organization's bottom line by reducing risks, preventing costly security incidents, and enhancing overall efficiency. Below are three examples of proving ROI to Senior Management:

Quantify Risk Reduction

Quantify the cost avoidance from prevented incidents by estimating the potential cost of security incidents that were avoided due to the threats identified and mitigated through Threat Modeling. This could include data breaches, service disruptions, or regulatory fines. For example, If a threat model identifies a vulnerability that could have led to a data breach, and the average cost of a breach is 4€ million, the threat model effectively avoided this potential loss.

Cost Savings from Improved Security Practices

Show the operational efficiency gains demonstrating how Threat Modeling integrates with and improves the efficiency of the development process by identifying and mitigating threats early, the organization avoids costly rework and delays. For example, early identification of security flaws could save 20% of the costs associated with late-stage fixes or emergency patches.

Calculate ROI with a Financial Model

The following is a very simplified version of how to calculate ROI for Threat Modeling. There are more detailed ways:

- Total Investment in Threat Modeling: Include the costs of tools, training, personnel, and time spent on Threat Modeling activities.
    - **Example:** Annual costs might include €150,000 in personnel, €30,000 in tools, and €20,000 in training.
- Total Savings/Benefits from Threat Modeling: Sum up the avoided costs from incidents, defects, and other efficiencies gained through Threat Modeling.
    - **Example:** If Threat Modeling avoids €500.000 in potential breach costs and saves €50.000 in operational efficiencies, the total benefit is €1.15 million.

- ROI Calculation Formula.

  ROI = ((Total Savings/Benefits - Total Investment)/Total Investment) X 100

- Result:
  - Total Savings/Benefits: €1.150.000
  - Total Investment: €200.000

  ROI = ((1.150.000 - 200.000)/200.000) X 100 = 475%

  This means that for every Euro invested in Threat Modeling, the organization gains €4,75 in benefits.

7.3 Continuous Improvement and Insights for Senior Management

It is very important that Senior Management[22] will have a good understanding and visibility of the Threat Modeling progress. By focusing on the above section KPIs and KRIs, a Threat Modeling team can drive continuous improvement and provide Senior Management with the insights needed to make informed decisions about the organization's security strategy.
In addition, the following insights can be provided to Senior Management:

- **Trend Analysis:** Track KPIs and KRIs over time to identify trends in the effectiveness of Threat Modeling and areas that require improvement.
- **Benchmarking:** Compare internal metrics with industry benchmarks to understand how the Threat Modeling process stacks up against peers.
- **Actionable Insights:** Use the data from KPIs and KRIs to provide Senior Management with actionable insights, such as areas needing more resources or attention.
- **Integration with Overall Risk Management:** Ensure that Threat Modeling metrics are integrated into the organization's broader risk management framework, helping to provide a comprehensive view of risk.

[22] *Presentation to Senior Management Template by IriusRisk*

Appendix

Checklist

In order to create a compact and robust checklist, the following steps will guide the implementation of the Threat Modeling function and the first threat models. Note that some parts in the list below might not be done in the same exact order. General advice is to progress on the parts that can be completed and keep a good plan and structure on how to move ahead.

Phase 0 - Initiation (before Threat Modeling Function creation):

- [ ] Define and document the Business Objectives of the Threat Modeling Function and align with Business Goals (See Chapter 1).
- [ ] Create a concrete business plan and roadmap and present it to Senior Management describing the benefits of a Threat Modeling function. The aim is to get Senior Management Buy-in for the Threat Modeling Function (See Chapter 2).
- [ ] Get Senior Management Buy-in for the Threat Modeling Function (See Chapter 3).
- [ ] Goal is to acquire a budget to start the Threat Modeling team.

Phase 1 - Plan (Step 1):

- [ ] Understand what expertise is needed for a Threat Modeling team (See Chapter 4).
- [ ] Create a Threat Modeling team (See Chapter 5).
    - [ ] Start either with 1 Senior Threat Modeling Practitioner and one Supportive Threat Modeling Practitioner (optional).
- [ ] Operationalize the Threat Modeling function by selecting the Methodology and the required tools.
- [ ] [Optional] Decide Metrics for continuous improvement. This can be done later when the team achieves higher maturity. It is recommended to define Success Criteria. (See Chapter 7).

Phase 1 - Plan (Step 2):

- [ ] Create a threat model methodology document that will describe the methodology of how threat models will be conducted in the organization (See Chapter 6).
- [ ] Create a threat model process document that will describe the process of conducting threat models in the organization (See Chapter 6).
- [ ] Do brainstorming sessions of which Products will be selected for the first threat models (See Chapter 6.1.1).
- [ ] Prioritize few products that wish to be threat modeled first (See Chapter 6.1.1).
- [ ] Create a plan of the execution of the threat models (Product A → 2024 Q3, Product B → 2024 Q4 etc.

Phase 2 - Do:
[Assuming that a Product is selected for a threat model]

- [ ] Proceed with a presentation to the team managing the product in question of how threat models are being conducted, what are the timelines, what resources will be needed, what knowledge is needed and is the benefit of the outcome. The aim is to get Stakeholder Buy-in from the Product Stakeholders.
- [ ] Identify the critical stakeholders in the Product being assessed such as, Security Architect, Product Owner, Application Owner, Business Analyst, Software Developers.
- [ ] Plan frequent meetings with the relevant stakeholders to gather information about the Product.
- [ ] Select a Threat Modeling Champion from that team that will serve as a POC.
  Note: Select a motivated and knowledgeable individual that will assist with all the required information needed.
- [ ] Conduct the threat model in parallel with the meetings you planned with the stakeholders.
- [ ] Present the threat model often to relevant stakeholders and capture feedback.
- [ ] Update the threat model until you reach a consensus of the final result.
- [ ] Generated threat and countermeasures to be explained to the relevant stakeholders

Phase 4 - Act:

- [ ] Create an action plan for the generated countermeasures with dates of completion.
- [ ] Monitor the progress of the countermeasure implementation and update the threat model accordingly.
- [ ] Generate a final threat model report for Senior Management (Threat Modeling Digest Report) and for Technical audiences (Threat Modeling Detailed Report).
- [ ] Plan when the re-certification of the threat model will be conducted according to the criticality of the product.

Phase 5 - Review:

- [ ] Do an internal retrospective in the Threat Modeling team to review what can be improved.
- [ ] Do an external retrospective with the Product stakeholders and gather feedback about their experience and what they recommend as improvements.
- [ ] Report to Senior Management the results and gather feedback and impressions.

NOTE: Following the above checklist, probably you have completed the first threat model. Now, repeat Phases 2 to 5 to conduct more threat models.

Automate Threat Modeling to fit your existing SDLC

Secure design right from the start

Visit **www.iriusrisk.com**

to book your demo

IriusRisk