IriusRisk

# The Security Champion's Guide to Threat Modeling

How IriusRisk turbo-charges your organization's fight against cybercrime

# If the Cape Fits, Wear It

In a business context, a champion advocates best practices. But it's also a title that conjures up a superhero image, someone everyone else can rely upon to protect the business and carry the fight against the bad guys.

While you might not see yourself as the security ops equivalent of a DC Comic hero, your decisions and actions should and will, significantly impact the health and success of your business.

By introducing robust threat modeling into your software development cycle, you'll save time and money, and bring teams together so that everyone is invested in success. While achieving this sounds heroic, it's basically just doing your job well.

This guide introduces the steps you should take as a Security Champion to begin world-leading threat modeling - with IriusRisk.

Read on to discover how your whole organization will benefit and how you'll get buy-in from management for a threat modeling program. But if you're already familiar with the process and positives (you're a superhero, after all), jump right ahead and contact us to book a demo.

# The Growing Cyber Threat

The cost of cybercrime is expected to top $10.5 trillion globally by 2025.
This covers everything from phishing links on personal emails to ransomware attacks on some of the world's largest corporations.

That eye-watering figure is up from 'just' $3 trillion in 2015 and represents the biggest-ever transfer of economic wealth, in this case, from good guys to bad.

And it's why your role as your organization's Security Champion has become so important. Security development and operations are now critical to the success of any new software launch or device that's hooked up digitally to a network.

Cybercrime is so sophisticated that it infects all sectors. Some industries are more susceptible than others, which is why IriusRisk threat modeling is used across financial services, ecommerce, and technology, as well as medical device manufacturers, for example.

But what is threat modeling, and why does it matter to you?

**Pearson** chose IriusRisk as its automated threat modeling platform to add consistency, reduce man-hours, and scale.

**Axway** integrated automated threat modeling into its Secure Software Development Lifecycle, Continuous Security Review and CICD processes.

**European Bank** built a self-service threat modeling process for DevOps and scaled secure design across its organization.

# Identify Risks and Mitigate Against Them

As a Security Champion, your primary concern is bullet-proof products and processes that cannot be exploited.

Whether you make devices for the Internet of Things or provide services that collect private information like customer emails, your systems must be robust.

The best way to avoid issues is to expose potential risk from the very outset of the product lifecycle, then continuously stress test through design, production, and updates down the road.

A superior threat-modeling system, like the platform from IriusRisk, delivers. The more you put into it, from team buy-in as much as in data and code, the more you take out in terms of success.

The benefits include:

- Faster time to market, saving on development costs. Risks are identified before your dev teams go too far down the road. Rather than finding issues after the fact and then starting again, they start development ops in the right way.
- Threats are identified throughout the lifecycle, including after-market patching and update processes.
- Foster a culture of collaboration between security and DevOps, working together for a common goal, creating effectively "DevSecOps," where the whole is greater than the separate parts.
- Regulatory compliance is more straightforward with IriusRisk. If you work in a regulated capacity (such as finance or medicine), your threat-modeling platform collates full auditing trails, issues reports, and even enables you to align to industry standards.

These top-level benefits encourage a better organizational culture and bring cost savings before, during, and after development.

And let's not forget, your business will avoid the extraordinary cost of a cyber security breach in real terms and reputational damage. Don't let your team make up part of that $10.5 trillion global cybercrime bill in 2025!

# Getting Organizational Buy-In

Now that you see the benefits of threat modeling, the next stage is bringing others on board.

Ultimately, you'll want management sign-off as the process shifts how your teams will work. Then, of course, there is the budget to consider. But the cost is insignificant compared to the risk of not correctly assessing loopholes in coding and architecture.

It might be better to get the buy-in from all teams – dev, architecture, design – before seeking management approval. A united front is more impactful; those with their hands on the finances will see how money can be saved from collaborative working.

Bringing department heads together to explain how threat modeling will save them time and effort (and all for the organization's greater good) is, therefore, paramount.

If they're invested from the outset, the results will be well received and acted upon. Perhaps they might recognize the following issues with existing company processes:

- Dev is creating software that has the potential for security breaches.
- Your Security team is overloaded with a backlog of code to approve from Dev.
- You have no system for Dev to build secure software from the outset, let alone for updates/patches.
- There is a lack of consistency in secure design in all application code.

# The Top-Level Sell

If you need an elevator pitch to explain why cloud-based threat modeling is so good, consider this:

*A threat-modeling platform analyzes security weaknesses in cloud native designs without drawing an architecture diagram.*

Assuming your audience understands DevOps, you can add the following:

It generates a threat model from an IaC descriptor, and as DevOps configure multiple versions of these during a product development process, the automated element is invaluable.

If you get any pushback (although unlikely, given the common goal), the National Institute of Standards and Technology in the US has your back.

**According to NIST**: *"We recommend using threat modeling early to identify design-level security issues and focus verification. Threat modeling methods create an abstraction of the system, profiles of potential attackers, including their goals and methods, and a catalog of potential threats."*

# Why IriusRisk?

From the public sector and tech companies to medical and financial services, we're trusted by Chief Information Security Officers (CISOs), Security Champions, developers, and designers – all these departments benefit from reliable, collaborative, and easy-to-use threat modeling solutions.

A collaborative diagramming tool with questionnaire and template capability

Extensive knowledge base of security patterns - including the ability to add your own

Import existing diagramming or cloud orchestration files to automatically generate a threat model

Integrate with Issue Trackers to support your Development Teams

Ability to threat model multiple areas of your supply chain

# Reasons not to ignore IriusRisk

- Shortlisted in the Security Excellence Awards for 'DevSecOps Award' (March 2023).
- Shortlisted for the DevSecOps Excellence Awards for 'Best DevSecOps Security Tool' (January 2023).
- Winner of the Best Technology Company in Aragon by the Official College of Telecommunications (COIT) (January 2023).
- First-of-its-kind threat modeling community, free for all members: **Threat Modeling Connect** (November 2022).

# The Decision of Champions

Having assessed why you need threat modeling, how you can get buy-in from your organization, and why IriusRisk should be your preferred partner, it's time to learn more about us.

You can try the free **Community Edition** version to find out more details at your own pace.

But we thoroughly recommend joining an introductory call to get started with a platform demonstration. Our team will address your questions and add context to your business needs.

It's time to release your inner Security Champion superhero.

**BOOK NOW**