IriusRisk

Place security front and centre and empower your teams

A Guide to Holistic Threat Modeling for Organizations in the Technology Industry

Digital transformation is driving greater demands on technology companies.

The adoption of modern architectures has increased the complexity of the IT infrastructure in many technology organizations, consequentially increasing the number of potential attack vectors exponentially. This has led to traditional labour-intensive threat modeling techniques becoming untenable and a growth in popularity for automated tools that are deeply embedded in the software development life cycle (SDLC).

IriusRisk integrates threat modeling into the native SDLC, meaning engineers and developers become their own security experts and can correct any faults then and there – streamlining the whole lifecycle, reducing costs and solidifying security in all products.

> **“*We have found that performing Threat Modeling in a structured and repeatable way is the best process to identify what could go wrong, to plan what we are going to do about it, and implement relevant controls, whatever they may be.***
>
> Director of Security Architecture, **US-based Software Company**

Usually, technology companies are at the forefront of innovation, being the first to adopt new technologies and approaches to have a competitive edge, while serving their end users with the best possible products. They can be more willing than other industries to use open architecture and can have a complex supply chain. All of which can create an ideal environment for attackers to exploit and find vulnerabilities.

What is threat modeling?

If security flaws and design errors are not identified until after an application goes into testing, corrections can be expensive, both in resources and in time invested. Modern threat modeling doesn't wait until the application goes into production. Instead, it takes place in the design phase of a system or application and automates the process of threat modeling throughout the SDLC, subsequently accelerating the time to market and dramatically reducing the cost of re-design. Current authorities class it as being an essential part of application design.

Where is threat modeling recommended or mandated?

1. The National Institute for Standards and Technology (NIST) recommends threat modeling as an important security practice within their secure software development framework, particularly for identifying security requirements and potential vulnerabilities early in the development lifecycle.[4]
2. The OWASP (Open Web Application Security Project) Top Ten calls for increased use of threat modeling, particularly when dealing with the problem of insecure design, listed as the fourth most critical security risk to applications; Insecure Design.
3. Gartner[5] places it within the Application Security Requirements and Threat Management (ASRTM) category.
4. Gartner6 states, *"Threat modeling is a critical component of any security-by-design program. When approached correctly, it increases system security, resiliency and long-term ease of management by creating an architecture-level system for reviewing code design, enumerating threats and mitigations and mapping out the attack surface of a system."*

The key to scaling this activity across a large portfolio of applications is to move the responsibility for software security from the central security team to the engineering teams and to empower them with a self-service automated threat modeling solution. This removes the central security team as a bottleneck to the product release process, allowing faster releases that still meet the security and compliance requirements of the organisation.

Collaborative. Comprehensive. Effective.

Organizations across sectors continuously demand the latest software, processes, and systems to keep them competitive, so technology companies are required to build and develop quickly and at scale. However, embedded security is paramount, and a proactive approach to threat modeling is the best way to identify and reduce threats from the beginning.

IriusRisk's threat modeling platform takes a holistic view of your architecture, alongside comprehensive threat analysis and effective countermeasures out of the box. It makes the practice of threat modeling simple, repeatable and reliable. It ensures security is intrinsic across your departments with IriusRisk.

Threat modeling is recommended in multiple standards such as the NIST Guidelines on Minimum Standards for Developer Verification of Software[1], and PCI DSS 4.0[2]. IriusRisk ensures your software developments are security compliant, end-to-end. But there are a number of other factors that technology organisations must consider before implementing their threat modeling practices.

> **“**
>
> ***I think that transition has been quite seamless. In terms of adoption, having it cloud-based gives the ability for anyone to access it, whether their role is a developer, product owner or a risk manager. I think people find the automation part really valuable. We can re-prioritise that time we would usually spend with the team into continuous improvement tasks which helps the business move forward while creating autonomy.***

Tom Ling, Team Lead, **ClearBank**

Ease of use

Organizations across sectors continuously demand the latest software, processes, and For threat modeling to be effective, it needs to be implemented throughout the software development lifecycle and be used confidently by Architecture, Development, and Security teams. Their ideal goal is for the threat modeling process to be intuitive and so well-embedded in the SDLC that they don't even have to think about it. The easier the threat modeling solution is to use, the more effectively this can be achieved. To support this, our users can import existing architecture from other sources such as Lucidchart, Visio, and HashiCorp Terraform. The platform also offers **AI-augmented threat modeling** to create diagrams from a description, Jira task or even meeting transcript notes.

Connected collaboration

The ability to collaborate between teams, in person or remotely, throughout the threat modeling process is a key factor when choosing a solution. Organizations want a seamless experience across their Architecture, Development, and Security teams. This is why we allow real-time collaboration in our tool, and the ability to change roles and create Business Units to collaborate efficiently on the applications or systems that your teams are involved in.

Valuable support

Given that automated, scalable threat modeling is a relatively new area of security and one that will prove highly beneficial to the technology sector, a supportive and experienced threat modeling provider can close secure design gaps and work on long-term, continuous security improvements. At IriusRisk we offer a comprehensive onboarding and training program; **IriusRisk Academy**, with free online courses, as well as in-person and virtual workshops for geographically dispersed teams. Onboarding is included as standard, with the chance to upgrade for additional configurations if needed.

Speed of scale

Longevity of the tools you choose is imperative. You need to select software that integrates into your existing technology stack, and has the ability to grow and scale as your business does. IriusRisk does just that by integrating into CI/CD pipelines and developer processes. It integrates with popular cloud and issue tracker tools such as ServiceNow and Jira.

> ***The integration between IriusRisk and Jira has been invaluable to our workflow. Speeding up our processes and removing the need to create lengthy documentation. Jira tickets are created seamlessly for any controls which need to be put in place making the process flow smoothly for all teams.***

Chris Ramirez, Principal Software Security Engineer, **Axway**

Bring change to life

Implementing a security program that includes threat modeling involves a cultural and organizational change rather than a technical change.

Start with a pilot project that applies only to a specific set of applications to confirm there are enough resources and support to make the end result a success. Any threat modeling tool should be collaborative. This involves explaining what will take place, why it will benefit each stakeholder and what the overall effect will be.

"Although Threat Modeling isn't a new process to Axway, bringing together international teams of people to carry out manual threat modeling was never an easy task. With IriusRisk, we've been able to carry on our threat modeling practices across our existing products with much greater ease - to the point where it is now a systematic process which alleviates any SPOC bottlenecks that we used to have." **Sandy Blackwell, Director of Software Security, Axway**

Organizational change must always be communicated, even when the project is a pilot. Adapt the corporate development procedures to include threat modeling once the application architecture is defined to make sure your project succeeds. Understanding how averse to risk the business is in relation to each application is essential to creating a risk-based security strategy. A threat modeling tool helps you manage resources more efficiently so you can make better decisions.

Undertaking a threat modeling strategy offers significant business benefits. Not only does it present a demonstrable ROI, but it's also not a complex activity to undertake. Threat modeling underpins other types of security testing, reviewing and auditing, and increases the productivity of business processes. It also improves time to market and instills an appetite for security all the way up to the C-suite. See more guidance on this in the independent **Forrester Study**[7].

Introducing IriusRisk - proactive software security by design

Secure doesn't have to be slow. By partnering with IriusRisk, you'll have the support of our automated and AI-augmented threat modeling platform to help you identify architectural security flaws before you start building. The IriusRisk platform can be delivered either as an on-premises solution or through SaaS. Powerful, scalable, and collaborative, it's designed to help your engineering and security teams identify architectural security flaws during design, saving you time, avoiding delay,s and accelerating your time to market by baking security earlier into your development process.

Automated threat modeling
IriusRisk helps you beat the complexity of manual threat modeling with its powerful automation engine, providing a reliable self-service tool for designing secure applications that's simple for your engineers to use.

Security starts with design
Half of today's software flaws are in the design. Our platform lets you generate threat models in minutes, along with recommended and required countermeasures and specific, actionable advice for your engineering teams.

Automated threat modeling
Smart threat modeling requires smart, targeted investments. Know how much to invest in security and where to invest it to get maximum return on your investment.

“

> ***Making the change to IriusRisk has significantly improved our threat modeling process. The platform’s stability, combined with essential features like versioning and questionnaire integration, has enabled us to enhance security practices while preparing for future growth.***

Senior Threat Modeling Architect, **Fortune 500 Technology Organization**

Experience our platform first-hand

Book a consultation with our threat modeling specialists to see the tangible benefits that IriusRisk can deliver for your business.

Book now

References

1. https://www.nist.gov/publications/guidelines-minimum-standards-developer-verification-software
2. https://blog.pcisecuritystandards.org/pci-dss-v4-0-resource-hub
3. https://owasp.org/Top10/A04_2021-Insecure_Design/
4. https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standard-vendor-or-developer
5. https://www.gartner.com/en/documents/3772095
6. Gartner, An Introduction to Threat Modeling Best Practices, Giles Williams, Manjunath Bhat, Dale Gardner, Mark Horvath, 30 May 2024
7. https://www.iriusrisk.com/forrester-tei-study