IriusRisk

Place security front and centre and empower your teams

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

ebook

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 organisations, 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 life cycle, reducing costs and solidifying security in all products.

Collaborative. Comprehensive. Effective.

Organisations 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, to make the practice of threat modeling as simple, complete and reliable as possible. Ensure security is intrinsic across your departments with IriusRisk.

Threat modeling used to be a top-level additional extra for code creation, but recently became a minimum standard for vendor or developer verification of code so 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.

01.

Ease of use

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 easier this can be achieved.

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.

03.

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.

Developer expertise

The growing role of developers in the enterprise is increasing the importance of this area when it comes to vendor selection. Quick time to value, easy experimentation through the community edition and a truly self-service offering contribute to IriusRisk's smooth and seamless experience.

Adopting a start left approach

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. The National Institute for Standards and Technology (NIST) has estimated that correcting code once an application is in production can take thirty times the time required for remediation and re-design.

As a result, there has been a move towards adopting a 'Start Left' approach – one that starts earlier on in the development cycle. Automated threat modeling at design time is an activity recommended by NIST1 and OWASP2 (Open Web Application Security Project) to ensure that engineering teams build adequate security controls into a product.

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.

[1] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standard-vendor-or-developer

[2] https://owasp.org/Top10/A04_2021-Insecure_Design/

What is threat modeling?

Modern threat modeling has moved on from manual processes. It 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 Software Development Lifecycle (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:

01.

The OWASP 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.

02.

NIST references it as the first step in their Recommended Minimum Standard for Vendor or Developer Verification of Code.

03.

Gartner places it within the Application Security Requirements and Threat Management (ASRTM) category.

How to build a threat model

Technology organisations want threat modeling to be easy to use for everyone, and to be so well embedded in the development cycle that there's no need to even think about it.

One typical way of building an embedded threat model is based on the basic principles of Adam Shostack's four-question scheme. This model allows the user to detect security deficiencies during the design phase of the application.

01.

Build
the diagram

What are we building?

02.

Pinpoint
the threats

What can go wrong?

03.

Identify
the mitigations

What are we doing to protect ourselves against the threats?

04.

Validate
the model

Did we do a good job?

Validate steps 1-3.

Document the process.

A successful Threat Modeling tool will:

- Be a single point of management for the security team. This allows them to work with an updated view of the risks within their portfolio
- Use automation to generate security requirements based on the application architecture model and the relevant standards
- Have enough flexibility to adopt either industry-specific risk models or customized security policies based on a pre-regulatory triage
- Establish a two-way communication with the Application Lifecycle Management (ALM) tools that the development teams use
- Enable API access that allows automation
- Allow dynamic updates to the risk model and implementation strategy
- Integrate with the main security tools used throughout the development cycle
- Generate a visual diagram of the architecture that can act as an active document for the stakeholders

Bring change to life

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

01.

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.

02.

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.

Finally, Security Champions should remember that security requirements are not exclusively their preserve. The requirements should be published, challenged, improved and adapted to the agreed business risk appetite and regulatory compliance needs.

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.

The alternative?
Do nothing and cross the corporate fingers until the organization has no choice but to act.

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 easy-to-use automated 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 delays 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.

A smart investment

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.

IriusRisk

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

iriusrisk.com