IriusRisk

A new security landscape for the public sector

A Guide to Holistic Threat Modeling for Organizations in the Public Sector

ebook

A state of change in the public sector calls for changing threat protection

The public sector has seen increasing pressure to move towards a product-centric deployment strategy.

Rather than reinventing the wheel, these organizations should look to products and business outcomes with proven technologies, architecture and security models behind them, rapidly increasing the speed of deployment for internal customers with timelines of weeks – not months.

Consequently, a range of public sector organizations are undergoing a change in their structure, approach and cultural behaviour.

The introduction of new products and processes as part of these organizations' digital transformation, aligning their IT services with their business requirements and outcomes and then demonstrating this to wider governing bodies.

Security is paramount in this. Government departments and other public sector bodies are responsible for protecting their own networks and systems. As holders of significant data and providers of services, stringent measures must be put in place by companies in the public sector in order to safeguard this.

The standard bearers of organizational security

The pressure on public sector organizations to deliver products to internal customers faster and most cost effectively has never been higher. Along with strict budget limitations, the challenge is only greater.

Coupled with this is an increased pressure on public sector bodies to maintain cyber security. In 2022, the National Cyber Security Strategy shifted the dial on UK cyber resilience, setting the ambition for government to “act as an exemplar of best practice in cyber security”.

But threat modeling in the public sector is often perceived as hard and complex. This is partly due to many governmental organizations’ experience with free-to-use threat modeling tools, which often require advanced engineering and architecture skills to use effectively.

Another obstacle to this lies in the fact that many organizations are accustomed to seeing large amounts of documentation generated from traditional processes and systems. Moving to a more agile approach from these systems can be challenging. consider before implementing threat modeling practices.

In the same vein, legacy IT systems used by public sector bodies can have a significant impact on vulnerabilities, threat models and security posture.

Despite these obstacles, it is imperative that organizations in the public sector embrace modern threat protection. It's no longer just hackers that pose a threat to these companies.

Central government organizations hold large amounts of national data, and there are numerous foreign agents and bodies that constantly try to access this data. Well-funded and educated in their methodology, these agents pose a significant threat to national security.

But there are a number of other factors that public sector organizations must consider before implementing threat modeling practices.

01.

Ease of use

For threat modeling to be effective, it needs to be implemented throughout the software development lifecycle (SDLC) and be used confidently by AppSec, DevOps and engineering 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.

IriusRisk

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 DevOps, Development and Security teams.

03.

Valuable expertise

Given that automated, scalable threat modeling is a relatively new area of security, not just in the public sector, a supportive and experienced threat modeling provider can close secure design gaps and work on long term continuous security improvements.

IriusRisk

Trusted data protection

The protection of data, whether that be personal information from the general public or system level data, is paramount in choosing a threat modeling partner.

04.

IriusRisk

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 ASRTM (Application Security Requirements and Threat Management) category.

IriusRisk

How to build a threat model

Organizations 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.

IriusRisk

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

IriusRisk

Bring change to life

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

IriusRisk

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.

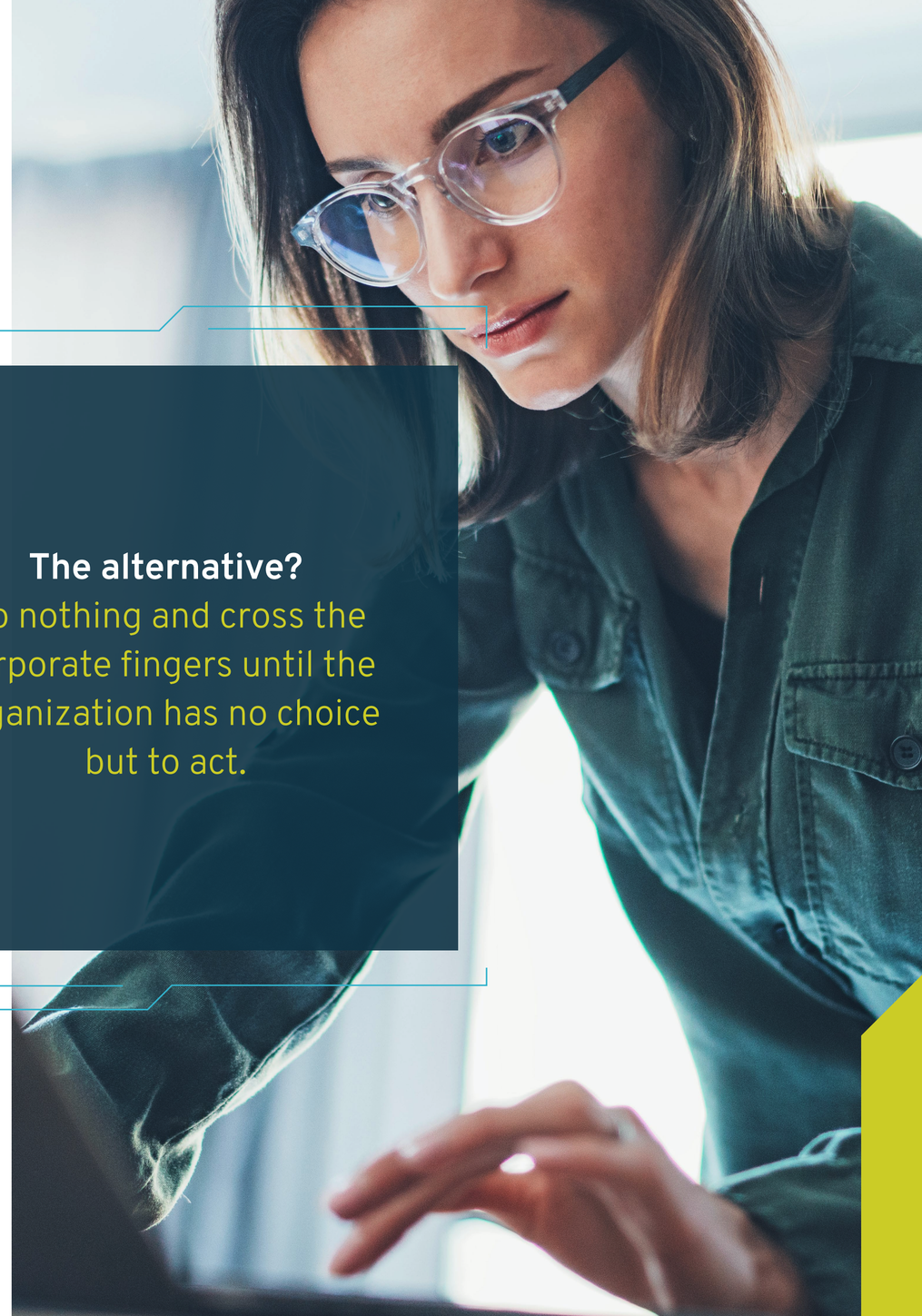
Organizational change must always be communicated, even when the project is a pilot. Adapt the corporate development procedures to include threat modeling once the application architecture is defined to make sure your project succeeds. Understanding how averse to risk the business is in relation to each 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.

IriusRisk

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.



IriusRisk

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.

IriusRisk

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