kamstrup

Secure Development Foundations

"The What, The How and The Why"

Yes you usually talk about it in a different order.

The What
The How
The Why
A bit about əɯ

kamstrup

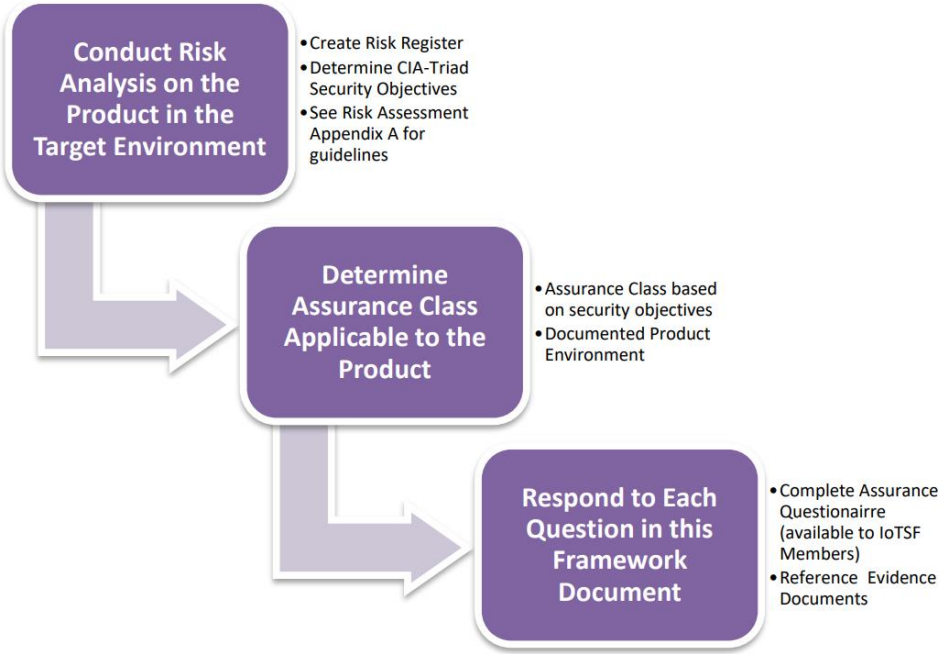
The What

Philosophical and practical.
What are we actually building?
For whom?
What is the use and applicability of it?

Usually the talk is: What - pray tell - are the requirements?

If you do not know what you are building - how will you know which part needs to be secure?

IoTSF



Identify Requirements
Identify Risks
Update Requirements
Build in a secure manner

kamstrup

The How

From SAFECode

“[...] the workflow should include:
1. Identifying threats, risks and compliance drivers faced by this application
2. Identifying appropriate security requirements to address those threats and risks
3. Communicating the security requirements to the appropriate implementation teams
4. Validating that each security requirement has been implemented
5. Auditing, if required, to demonstrate compliance with any applicable policies or regulations”

kamstrup

Identifying risk

How do the trust boundaries look? [Internal/External]
Which actors are in the product? [Internal/External]
How does the information flow?
What classification does the information elements have?
How does the deployment of the product differ from the logical concept?

kamstrup

Overall practices

From NIST:
“Prepare the Organization (PO): Ensure that the organization’s people, processes, and technology are prepared to perform secure software development at the organization level and, in some cases, for individual development groups or projects.
Protect the Software (PS): Protect all components of the software from tampering and unauthorized access.
Produce Well-Secured Software (PW): Produce well-secured software with minimal security vulnerabilities in its releases.
Respond to Vulnerabilities (RV): Identify residual vulnerabilities in software releases and respond appropriately to address those vulnerabilities and prevent similar vulnerabilities from occurring in the future.”

kamstrup

Building securely

Approach / development practice must be:

- Relevant
- Practical
- Agreed upon

Be explicitly aware of which components need extra consideration

kamstrup

The Why

That is a matter of quoting Microsoft regarding the SDL:

"By introducing standardized security and compliance considerations throughout all phases of the development process, developers can help reduce the likelihood of vulnerabilities in products and services and avoid repeating the same security mistakes. Similarly, security integration throughout the operations lifecycle will assist in maintaining the integrity of those products and services."

In short : "There is a business case. It has proven to be cheaper in the long run."

kamstrup

Understand **what** you build and who is going to use it.
Agree on **how** to build it, such that you are sure that you have secured it.
Because providing a secure product will soon not just be a matter of differentiation,
but your license to operate.

kamstrup

So being practical

What is important to secure about a product?

How do you identify Risk?

How do you validate what is being built?

Who does What?

Do you follow any specific guidelines or technological paradigms?

When your product is shown to have a vulnerability, how do you proceed?

kamstrup

What do you need to secure about the product?

Places where to look for this:

- Functionality
- Data
- Social Contract

You should threat model. At every step of your product development.

kamstrup

How do you identify Risk?

To get an overview
How do the trust boundaries look? [Internal/External]
Which actors are in the product? [Internal/External]
How does the information flow?
What classification does the information elements have?
How does the deployment of the product differ from the logical concept?

Identify dependencies

Focus on data

Focus on functionality

kamstrup

How do you validate what you are building?

Is your security described through functional requirements? Do you have the ability to test it?

Is the product you are building relevant in the deployment context?

Is the risk acceptable? How do you evaluate that?

kamstrup

Who does What?

Are you doing DevOps, Agile, prescriptive development?

Who can approve whether a risk is acceptable?

And who can you ask regarding technological or security issues?

kamstrup

Do you have any specific guidelines or technological paradigms?

Do you for instance follow OWASP cheatsheets for guidelines?

Do you have a reference architecture? A common toolchain? Build pipeline?

Is everything FOSS?

kamstrup

Vulnerability disclosure and procedure

Who does what?

How do you evaluate it?

When do you act?

kamstrup

Links and references

SAFECode Fundamental Practices for Secure Development:
https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf

IoTSF Security Assurance Framework:
https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf

OWASP Cheatsheets:
https://cheatsheetseries.owasp.org/

NIST Secure Software Development Framework:
https://csrc.nist.gov/Projects/ssdf

About me

Rasmus Lisby Fruergaard-Pedersen
Directs secure development at Kamstrup A/S, a smart metering developer and manufacturer.

Working professionally in security since 2007.
Security generalist, architect, developer, penetration tester, policy writer, educator …

Education and certifications

Cand.scient in computer science at Aarhus University.
Ongoing Diploma in Business Administration at Aarhus University
GSEC, GPEN, GXPN, GAWN, GCFA.

kamstrup

Rasmus Lisby Fruergaard-Pedersen