Security By Design

Maturity Model for DevSecOps

kakugo.ch

Security by Design

Security by Design embeds security principles early in the IT system development, reducing breach risks, costs of later fixes, and ensuring regulatory compliance.

Benefits

Reduce costs

By not creating vulnerabilities in the first place, therefore avoiding incidents, additional communication and more.

Reduce risks

By reducing the potential impact of a security breach, including financial loss, downtime, and damage to reputation.

Speed Time-to-Market

Secure systems enable businesses to nimbly adapt to market changes and innovate confidently, knowing systems are safe.

Security by Design Maturity Levels

Level	Name	Resources	Pros	Cons
0	Not initiated			
1	Policy Only	Checklists and Company Wiki	Provide directions	High friction; Less chance of being adopted; Non dev-friendly
2	Manual without process	Threat modeling specialist	Contextual assessment; tailored risks and controls	Non-reproducible; Very time-consuming
3	Manual with process	Threat modeling specialist + Playbook	Reproducible process	Very time-consuming
4	Automated	Threat modeling specialist + devops.security	High-quality risks, controls and requirements identification	Despite taking less time it doesn't scale yet
5	Scaled	Developer (Security champion) + devops.security	Security is not a bottleneck anymore	Setup time

Policy Only

Security requirements can be found on checklists handed to developers or company wiki.

It's the starting point to assist developers with security revised checklists.

It's also helpful during procurement to request a given list of requirements to be fulfilled.

Resources

- OWASP Application Security Verification Standard (ASVS) contains general requirements for applications https://threatmodeling.fyi/posts/policy-only/

Manual without process

A security consultant (internal or external) performs a brainstorming together with the development tech lead to identify threats and ultimately security controls to mitigate relevant threats.

The brainstorm is usually based on the STRIDE framework and the outputs depend highly on the consultant knowledge and the ability of the tech lead to describe the application.

Resources

- Microsoft Threat Modeling Tool to draw diagrams and identify threats automatically
- Draw diagrams using tools listed on https://threatmodeling.fyi/posts/manual-without-process/

Manual with process

A security consultant (internal or external) follows a threat modeling playbook with the development tech lead to identify threats and ultimately security controls to mitigate relevant threats.

The playbook includes guidance on what questions to ask, which tools to use and when. The output highly depends on the quality of the playbook.

Resources

- Step-by-step threat modeling process (also explains STRIDE)
- Step-by-step threat modeling using PASTA
- Resources can be found at https://threatmodeling.fyi/posts/manual-with-process/

Automated

A security consultant using a threat modeling tool such as https://ds.kakugo.ch describes the application and the threat modeling is automatically generated.

The process is reproducible and requires less specific knowledge from the consultant but more quality of the tool.

Resources

- devops.security by Kakugo GmbH https://ds.kakugo.ch

Scaled

A developer, after going through a training to become a Security Champion uses the threat modeling tool such as https://ds.kakugo.ch to describe the application.

This process enforces security requirements from the beginning, produces secure products and prevents vulnerabilities from being created.

Resources

- Setting up a Security Champion program for developers https://threatmodeling.fyi/posts/scaled/

Questions?

hello@kakugo.ch