SECURA SOFTWARE DEVELOPMENT LIFECYCLE

Developing software is a challenging task. Historically, teams used the linear waterfall-approach a lot. Nowadays we see more iterative and cyclic approaches: agile, scrum, dev(sec) ops, continuous integration and continuous delivery (CICD). In all cases, making the software secure is not easy. Secura's -Software Development Lifecycle (Secura-SDL) approach helps you to develop secure software in a way that fits your development process.

IN CONTROL WITH SECURA

Secura has worked in information security and privacy for nearly two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing services varying in depth and scope.

OUR VIEW ON SOFTWARE DEVELOPMENT

Software is often less secure than we want because, by its nature, security is invisible. This makes it difficult to define our security expectations and apply the appropriate technical measures during development. Often we discover our security needs when it is too late or too expensive to repair: such as the result of a security test just before release. Or even worse: if someone successfully attacks our software.

We believe that making security visible throughout the Software Development Lifecycle (SDL) will give a clear picture of our security needs, and lets us make well-informed decisions on what to spend on software security, in line with other business objectives. Therefore we recommend to **'shift left'**: consider security earlier in the software development process, and throughout the SDL:

- When we define our software requirements, we make our security expectations explicit, so that we do not forget them during development.
- When we design our software and pick the right technologies, we analyze what threats we can expect from these technologies, and think of solutions.

- During the implementation, we follow secure coding principles and review our code against them.
- Security testing is not only performed at the end of the process. As soon as we can test or review something, it makes sense to do it, preferably in an automated way.
- A secure development process and secure development knowledge are the engine and fuel of our software security. Defining quality gates and security metrics increases security assurance, while training and learning on the job increases developer security awareness.

By shifting left, you are aware of the security risks of your software earlier. You can choose to ignore security (which makes sense at times), or you can choose to mitigate the risk earlier (which saves costs). In either case, you are better informed to make the right decision.

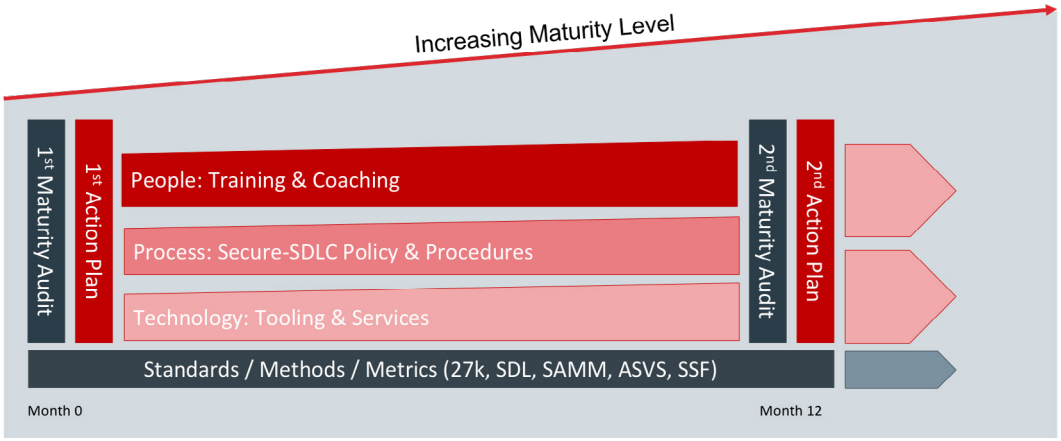
In many cases, a secure SDL program also increases the quality of the code in a number of other aspects, such as the readability and maintainability of the code.

SECURA SDL APPROACH

Many valuable standards, best practices, norms and metrics are available to improve security in your SDL. There is ISO 27034, Microsoft's SDL, OWASP SAMM, OWASP ASVS, COBIT, and many more. They all have their unique focus and while this jungle of standards may seem daunting at first, they all advocate the same goals and practices.

Because no two software projects are alike, you must decide what is important for your project and grow a secure SDL over time.

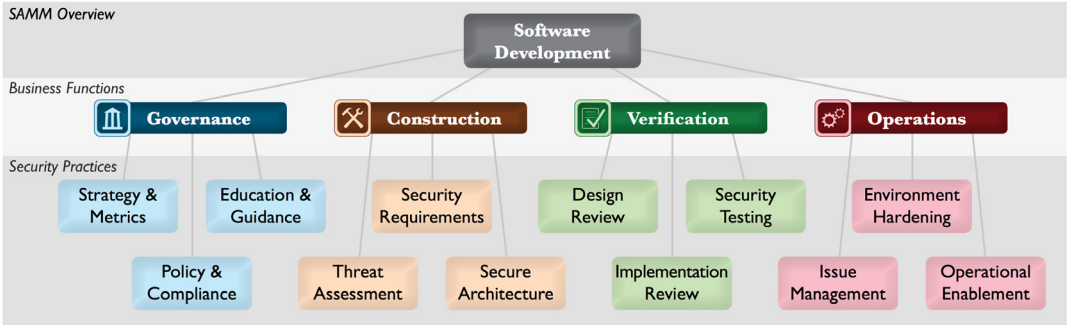
The Secura approach is to **measure, plan and improve**. We will look at how you build your software, what security practices are already in place and make an improvement plan, based on what you desire and what is possible. Repeat this regularly, and the improvement gets clear.



Secura-SDL Approach: Measure & Improve

MEASURE, PLAN, IMPROVE!

A good way to measure the maturity of a secure SDL is via OWASP SAMM (Software Assurance Maturity Model). SAMM measures the various phases of the SDL (construction, verification and deployment) and the SDL process itself (governance).



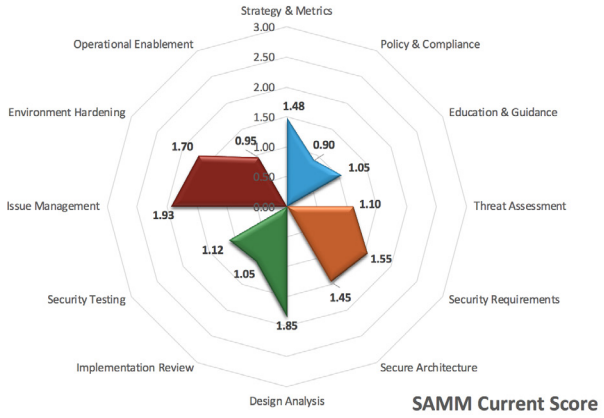
Maturity Audit (based on OWASP SAMM): Multi-dimensional Assessment

The outcome of a SAMM audit is a spider diagram showing (on a high-level) the maturity of your development organisation and process.

Current Maturity Score

Functions	Security Practices	Current	Maturity 1	2	3
Governance	Strategy & Metrics	1,48	0,47	0,67	0,35
Governance	Policy & Compliance	0,90	0,35	0,35	0,20
Governance	Education & Guidance	1,05	0,50	0,35	0,20
Construction	Threat Assessment	1,10	0,20	0,30	0,60
Construction	Security Requirements	1,55	1,00	0,35	0,20
Construction	Secure Architecture	1,45	0,35	0,75	0,35
Verification	Design Analysis	1,85	0,75	0,50	0,60
Verification	Implementation Review	1,05	0,35	0,35	0,35
Verification	Security Testing	1,12	0,57	0,35	0,20
Operations	Issue Management	1,93	0,83	0,75	0,35
Operations	Environment Hardening	1,70	0,75	0,35	0,60
Operations	Operational Enablement	0,95	0,50	0,10	0,35

Current Maturity Score



This output allows you to set goals and create an improvement plan. At Secura, we focus on three pillars for improvement:

- **People**: Via training and coaching, we increase security knowledge and awareness in all phases of the SDL.
- **Process**: By integrating appropriate security practices into the existing SDL, the development team can tackle security when it is most effective. Adopting security into quality assurance ensures that people follow the secure process.
- **Technology**: Automating security activities lets you work faster, and if you do not have the resources to perform all of them, our services can take care of it.

We carefully align the improvement plan with your business needs and possibilities.

PEOPLE: TRAINING & COACHING

Secura offers the following classroom training courses:

- Security Awareness
  - Hacker Mindset / OWASP Top10
  - Hands-on Hacking
- Secure Programming
  - Introductory training
  - OWASP Secure Knowledge Framework
- Design Review & Threat Modeling

We also offer the following eLearning courses:

- Security Awareness for Everyone (SAFE)
- Secure Programming

We also provide workshops and training on the job.

PROCESS: POLICY & PROCEDURES

Secure development knowledge and good tools by itself do not guarantee secure software. In our experience, people tend to take shortcuts under time pressure, resulting in vulnerable software. A good process assures that certain security practices are regularly executed and that the results pass the criteria.

We need metrics to define our software's security, responsibilities need to be defined and incentives need to be created for secure software. Secure software knowledge and experience must be available to the development teams, for example by having a 'Security Champion' in every development team.

You can base processes and procedures on standards like ISO 27.001 and ISO 27.034, or in a less formal way.

Areas of attention include:

- Requirements Management (& Communication with business)
- Threat Management / Design Principles
- (Security) coding principles
- Testing & Issue management
- Deployment, Patch & Release management
- Incidents, Response, Coordinated Vulnerability Disclosure
- Stage-gate processes
- Documentation & archiving
- Metrics & compliance

Secura can be your partner to help you define or refine these procedures.

TECHNOLOGY: TOOLING & SERVICES

When people write software, they focus on the most important thing: making the software run. Security is important, but the time needed for software security can feel uncomfortable. You may not have the expertise or resources to perform all activities. Fortunately, we can take away some of the pain via tooling and our services. In some environments, such as DevOps, automated execution of security practices is even essential. Secura can help you to install and run tools in your SDL:

- Code Analysis (Checkmarx, HPE Fortify, Semmle, AttackFlow, ...)
- Continuous Scanning (IBM Appscan, Netsparker ...)
- Issue Management (Jira, Mantis, Pipefy, Defect Dojo, ...)
- Pen Testing (Burpsuite, Acunetix, ...)

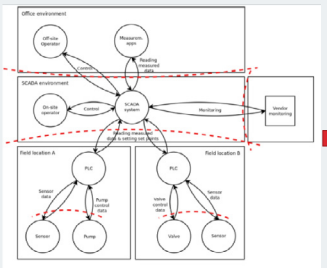
PREVENTION IS BETTER THAN CURE

Secura can help you with measuring and improving the security level within your software development organisation by offering training & coaching of employees, partnering in defining or refining policies and procedures and providing tooling & services. All in line with your business needs and possibilities, saving costs and resulting in more secure code. While direct cost savings from the design phase may seem trivial, optimal operational continuity as well as preventing reputational damage could be of even greater importance to your organisation ànd your stakeholders. Contact us today and be one step ahead!

EXAMPLE: THREAT MODELING

During our system's design, we choose technologies that suit our needs. We may choose an SQL database or a non-SQL database for example. Every technology comes with its own inherent threats. Being aware of these threats can prevent many vulnerabilities before the code is written. We do this via the threat modeling process:

1. ***What are we working on?***
   We create a model of the system that we work on, before we can analyze it. Usually we draw a Data Flow Diagram (DFD). So-called trust boundaries help us to identify where the attackers can be. We then identify the technologies that our system uses.
2. ***What can go wrong?***
   We identify what threats to expect from these technologies. A threat library helps us to select those threats. For web applications, we like to use a threat library based on the OWASP ASVS. We use Microsoft's STRIDE method to find more generic threats
3. ***What are we going to do about it?***
   Our threat library suggests certain mitigations. Blindly implementing these mitigations is not always effective or may be costly. An attack/defense tree can help us pick the most effective mitigations.
4. ***Did we do a good job?***
   For every threat that we identify, we list its mitigation, and how we will verify it. This 'TMV-list' gives us a metric of the threats and also a security test plan.



Data Flow Diagrams to find potential threats

Attack/Defense Tree (mapping onto ASVS Controls)

INTERESTED?
Would you like to learn more about our services?
Please do not hesitate to contact us.

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)88 888 31 00
E info@secura.com
W secura.com

Follow us on