OWASP AppSec Germany 2009 Conference
http://www.owasp.org/index.php/Germany

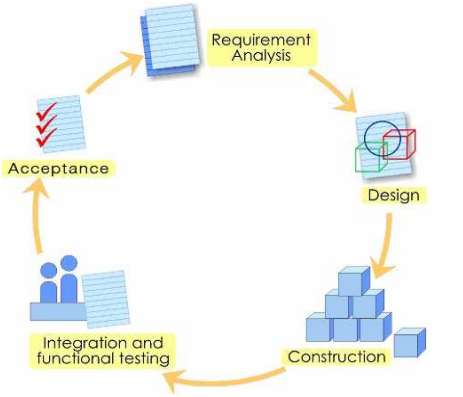
The Secure SDLC

Dr. Bruce Sams
OPTIMAbit GmbH
bruce.sams (at) optimabit.com
+49 8165 65095

OWASP
Nürnberg, 13.10.09

The Software Development Life Cycle

- Software development takes place within a "Software Development Life Cycle" (SDLC)

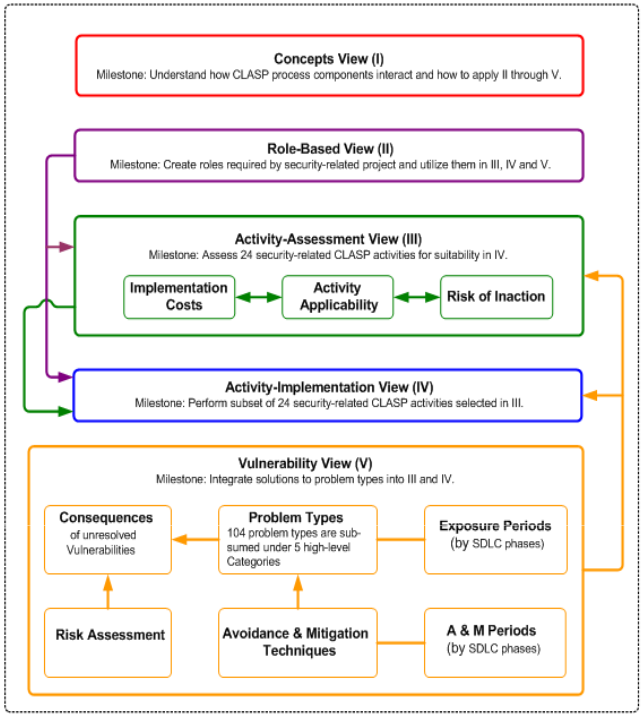


- *Security should be integrated into the SDLC, so that security is "built in" from the beginning and can be maintained over the lifetime of the software.*

- There is no "standard" for the secure SDLC.
  - Several attempts at a "standard" have been made, e.g. CLASP, BSI, ISO, etc.
  - Each company must create a secure SDLC that fits into their development process (V, RUP, Agile)

CLASP

- The Common Lightweight Application Security Process (CLASP) was originally a product of IBM/Rational.
  - It was NOT „lightweight"! It called for many roles, views and artifacts, much like the Rational Unified Process (RUP).
  - But… The basic idea was right: Define a process for creating secure applications rather than leaving it to chance.



Microsoft SDL

- Microsoft has developed the "Security Development Lifecycle" for internal use.
  - They provide some tools for assistance and integration with VisualStudio.
  - The SDL is best suited to development for Boxed Software products.

BSI

- Build Security In (BSI) is a project of the National Cyber Security Division (NCSD) of the U.S. Department of Homeland Security.
  - BSI is a set of non-binding "best practices".
  - The best practices and methods described are applicable to any and all development approaches as long as they result in the creation of software artifacts.

Build Security In

Setting a Higher Standard for Software Assurance

Sponsored by DHS National Cyber Security Division

ISO 12207

- ISO 12207 is a standard for software lifecycle processes.
  - It does not cover security explicitly, but it references other security standards that can be applied.
  - It establishes a process of life cycle for software, including processes and activities applied during the acquisition and configuration of the services of the system.
  - There are 23 Processes, 95 Activities, 325 Tasks and 224 Outcomes.

THE OPTIMABIT SECURE SOFTWARE LIFECYCLE

OWASP AppSec Germany 2009 Conference
Secure SDLC – Dr. Bruce Sams, OPTIMA bit GmbH

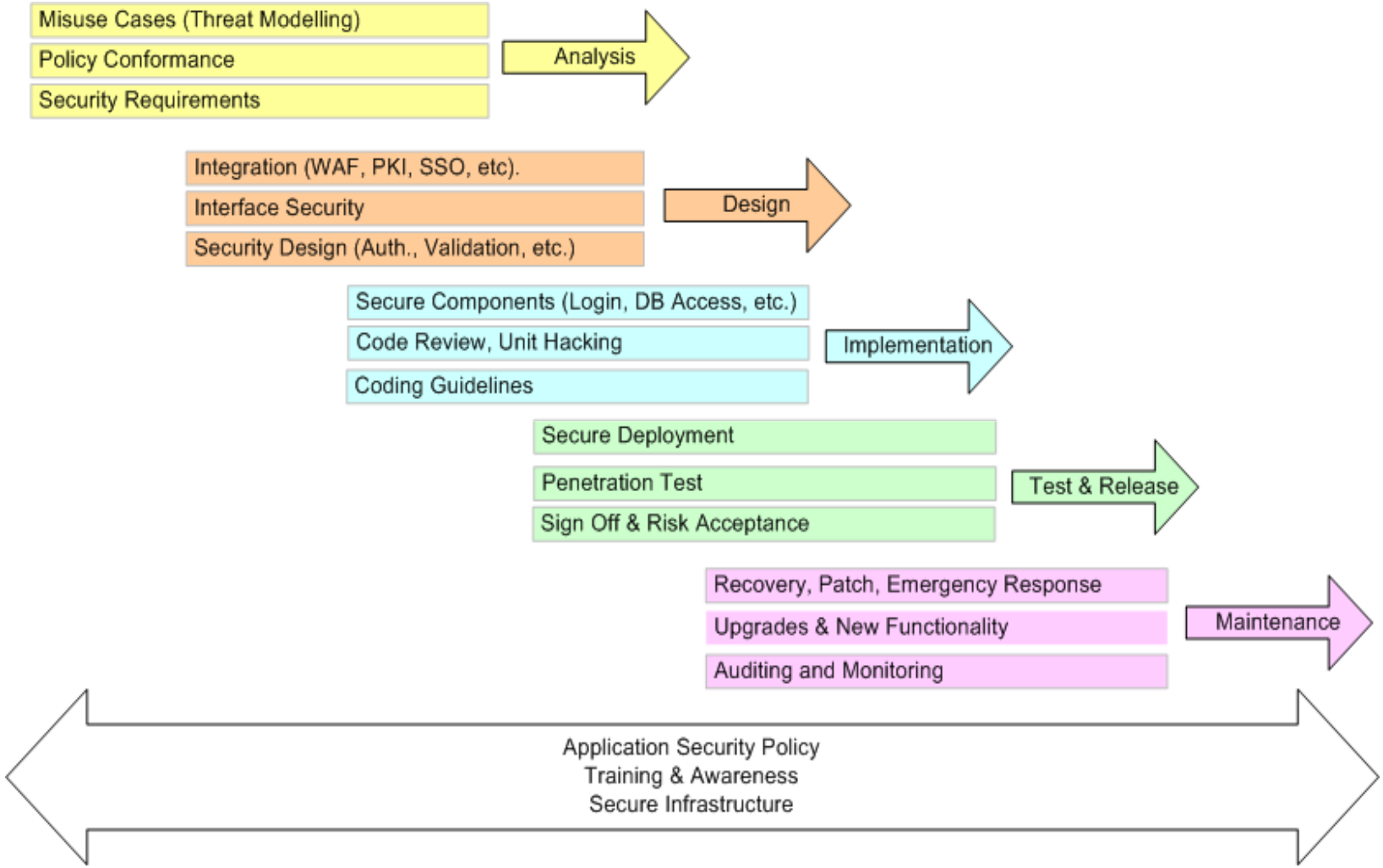
The philosophy behind the SSDL

- The OPTIMAbit process is based on the following principles:
  - The processes is as simple and direct as possible
  - The process is iterative and not all steps are required.
  - Software development is always performed under time and budget pressure; respect the development teams
  - The security effort must be in proportion to the application; provide enough security, but not "too much".
  - Every company is different; the process must be adapted to each one.

Some Development Lifecycle Issues

- Development methodology (RUP, Agile, Scrum, etc)
- How are projects applied for and approved?
- Where does management support come from?
- Where does the money come from? (project, central budget, external)
- What about different project sizes? (10 v. 100 v. 1000 MD)
- Who manages & maintains software in production?
- Outsourcing partners: How will they understand the security requirements? Who controls the security of their code?

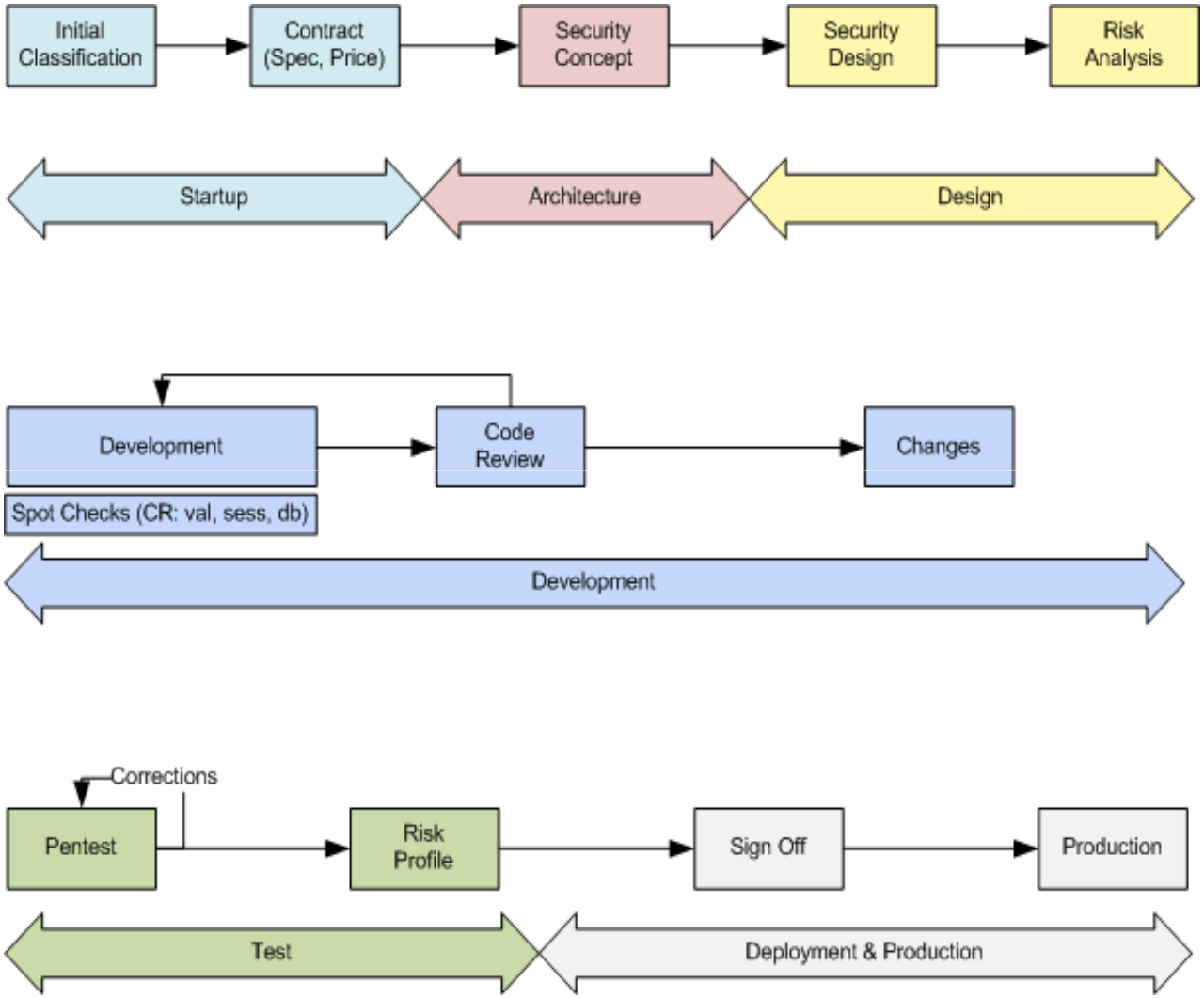
Diagram of foundation elements



Key Facets of a Secure SDLC Framework

- Architecture Review
- Application Security Policy
- Code Review
- Hardening Guides
- Penetration Testing
- Training
- Awareness
- Security Concept/Design
- Required Budget & Plan for Security (depends on protection requirements)
- Matrix of Security Assurance Milestones & consequences
- Security Risk Acceptance
- Migration strategy
- Metrics
- Make others do the work!

A generic view of a secure SDLC



BSI MM

The BSI maturity model

- The BSI (Build Security In) Maturity Model (BSIMM) is a simple method of measuring the maturity of software security in an organization.
  - Details at www.bsi-mm.com
- BSIMM is a collection of good ideas and activities that are in use today.
- It can help you determine where your organization stands with respect to real-world software security initiatives and what steps can be taken to make your approach more effective.

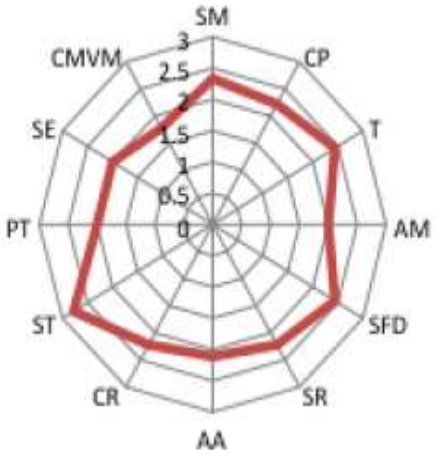
SSF and Domains of the BSIMM

The Software Security Framework (SSF)			
Governance	**Intelligence**	**SSDL Touchpoints**	**Deployment**
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Manage-ment

domain	business goals
Governance	Transparency, Accountability, Checks and Balances
Intelligence	Auditability, Stewardship, Standardization
SSDL Touchpoints	Quality Control
Deployment	Quality Control, Change Management

Values for active companies

- Nine top companies in finance, web and software were surveyed to see what they do for application security according to the BSIMM.
- The average results were at about the level of 2.



CONCLUSION

Conclusions

- The secure SDLC is a reality, and can substantially improve the security of software development.
- There is no Out Of The Box process, because the development process varies from company to company.
- Customizing the process requires sensible policies and templates that are developer friendly.