OWASP

Austria - Vienna Chapter

Secure Software Development with OWASP SAMM

Virtual Chapter Meeting 2020-04-20

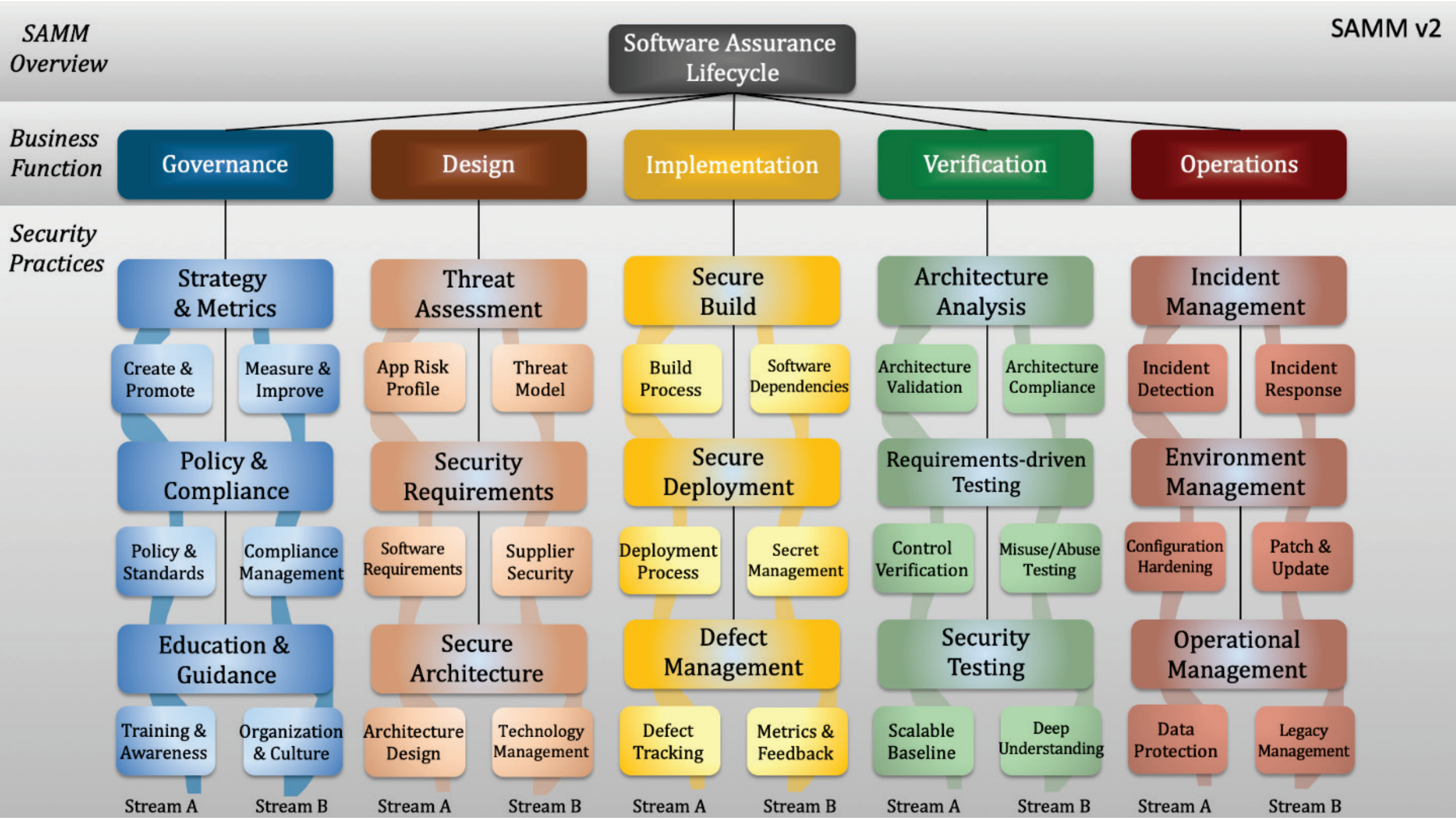
Speaker: Thomas Kerbl (@Dementophobia)

What this talk is all about

- Short introduction to OWASP SAMM 2.0
- How to implement a Secure Software Development process
- The most important areas to focus on
- Common pitfalls to avoid
- Answer YOUR most burning questions

Short introduction to OWASP SAMM 2.0

https://www.owaspsamm.org/


SAMM Overview
SAMM v2
Software Assurance Lifecycle
Business Function
Governance
Design
Implementation
Verification
Operations
Security Practices
Strategy & Metrics
Create & Promote
Measure & Improve
Policy & Compliance
Policy & Standards
Compliance Management
Education & Guidance
Training & Awareness
Organization & Culture
Threat Assessment
App Risk Profile
Threat Model
Security Requirements
Software Requirements
Supplier Security
Secure Architecture
Architecture Design
Technology Management
Secure Build
Build Process
Software Dependencies
Secure Deployment
Deployment Process
Secret Management
Defect Management
Defect Tracking
Metrics & Feedback
Architecture Analysis
Architecture Validation
Architecture Compliance
Requirements-driven Testing
Control Verification
Misuse/Abuse Testing
Security Testing
Scalable Baseline
Deep Understanding
Incident Management
Incident Detection
Incident Response
Environment Management
Configuration Hardening
Patch & Update
Operational Management
Data Protection
Legacy Management
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B

Example Question: Training & Awareness Maturity Level 1

Question

Do you require employees involved with application development to take SDLC training?

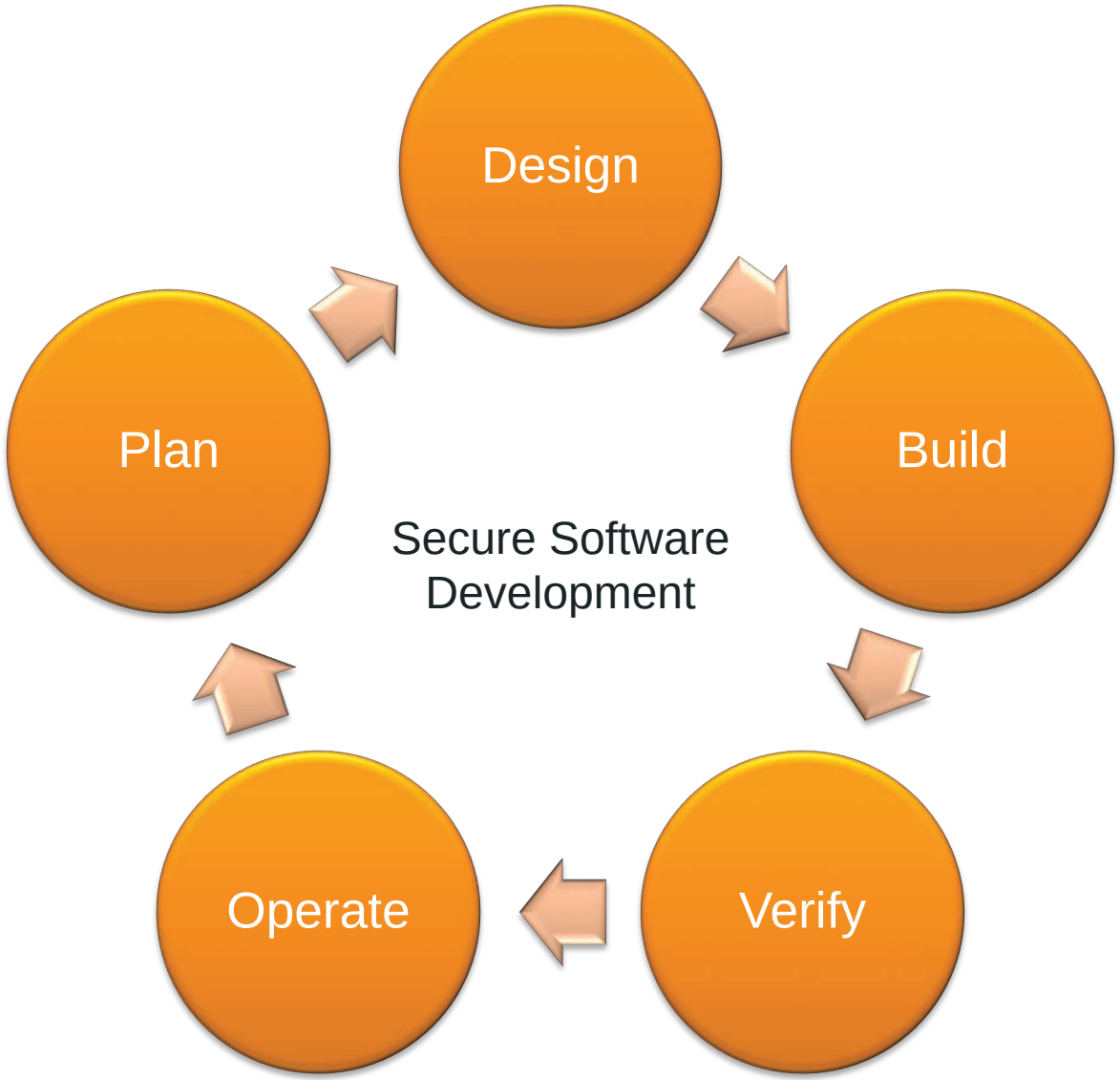
Quality criteria

Training is repeatable, consistent, and available to anyone involved with software development lifecycle
Training includes the latest OWASP Top 10 if appropriate and includes concepts such as Least Privilege, Defense-in-Depth, Fail Secure (Safe), Complete Mediation, Session Management, Open Design, and Psychological Acceptability
Training requires a sign-off or an acknowledgement from attendees
You have updated the training in the last 12 months
Training is required during employees' onboarding process

Answers

No
Yes, some of them
Yes, at least half of them
Yes, most or all of them

Security Challenges in the Software Development Lifecycle (SDLC)



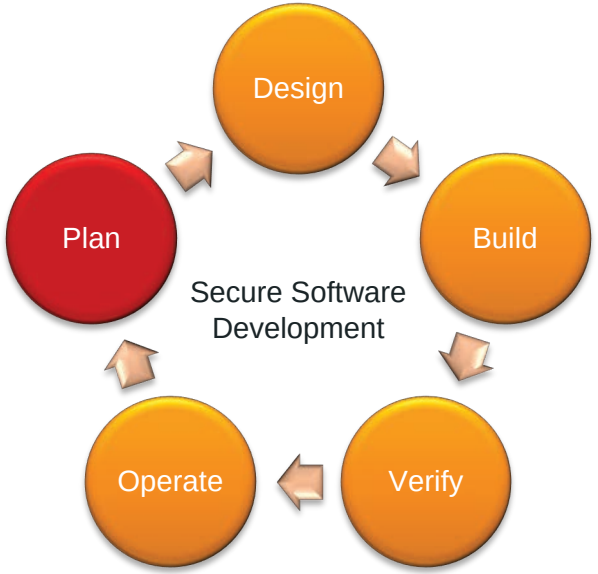
- Secure software is the result of a security aware SDLC
- Security must be addressed at every stage
- Failure results in vulnerable software and applications open to malicious attacks
- Regulators pay close attention to your security posture

Security in the Planning Stage

- **Define your Security Strategy**
  - Align goals and communicate
  - Define how to measure success

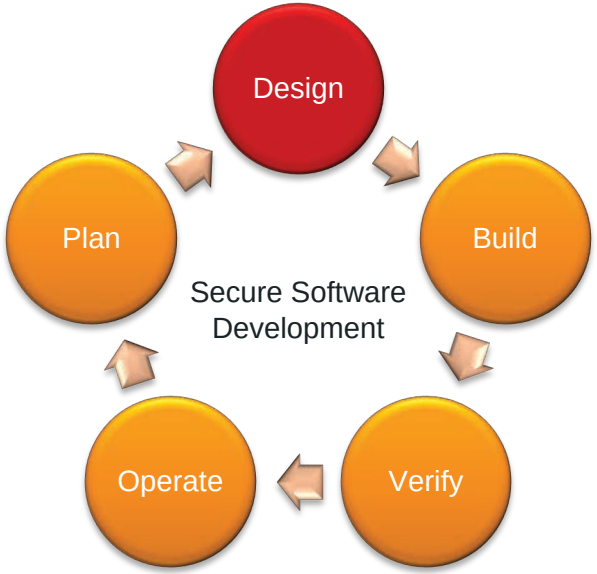
- **Address Policy and Compliance**
  - Know relevant policies and standards
  - Manage and track their implementation

- **Educate Key Personnel**
  - Provide trainings and guidance
  - Build a culture of security



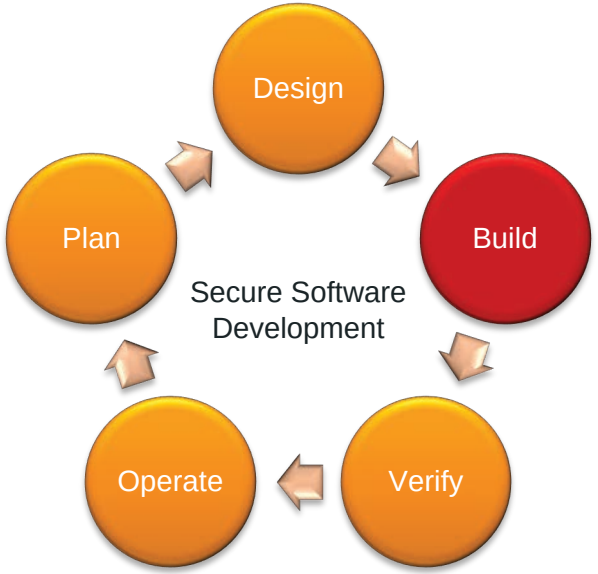
Security in the Design Stage

- **Define Security Requirements**
  - Establish requirements framework for the development team
  - Consider supplier management from a security perspective
- **Design a Secure Architecture**
  - Build on established security design pattern and solutions
  - Manage the technology stack
- **Perform Threat Assessment**
  - Create and maintain an application risk profile
  - Use threat modeling to improve the security design



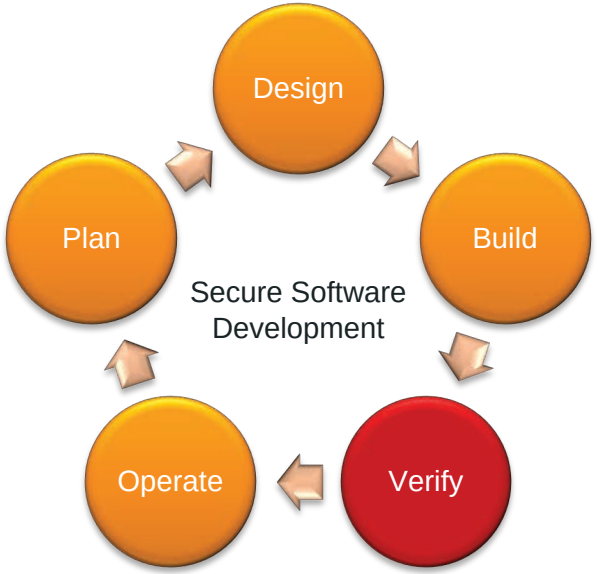
Security in the Build Stage

- **Establish a Secure Build Process**
  - Integrate security tools into pipeline
  - Analyze and manage software dependencies
- **Establish a Secure Deployment Process**
  - Automate deployment und integrity checks
  - Manage secrets within the lifecycle
- **Manage Security Defects**
  - Track, rate and handle security defects
  - Measure defect tracking and improve process



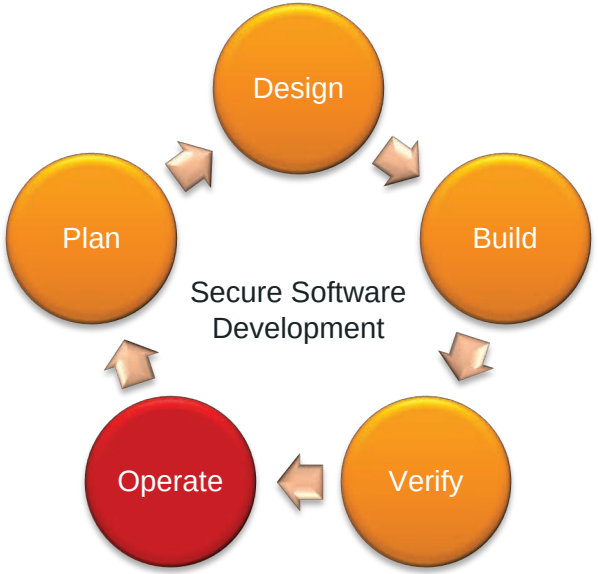
Security in the Verification Stage

- **Assess Security Architecture**
  - Validate implemented security mechanisms
  - Use feedback to improve process and artifacts
- **Perform Security Tests based on Security Requirements**
  - Test security functionality and establish regression tests
  - Address application-specific misuse and abuse cases
- **Static and Dynamic Security Testing**
  - Integrate and automate security testing into pipeline
  - Integrate penetration testing and code reviews in SDLC



Security during Operations

- **Manage Incidents**
  - Detect incidents proactively
  - Employ and enable an incident response team
- **Manage Environment Security**
  - Perform system hardening and monitor deviations
  - Integrate patch management
- **Manage Secure Operations**
  - Address data protection and detect non-compliance
  - Manage migration roadmaps for end-of-life and legacy systems

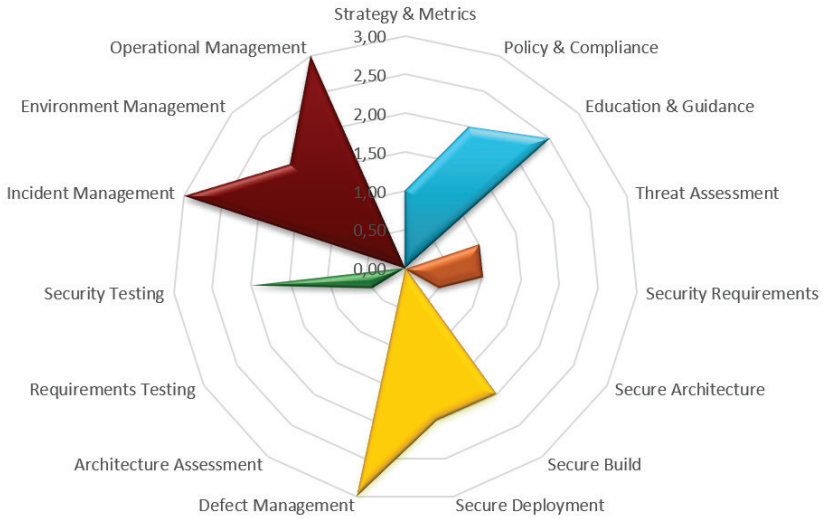


Gap Analysis and Maturity Level Assessment

- **Analyze your Software Development Lifecycle**
  - Based on established security standards
  - Workshop based walk-through

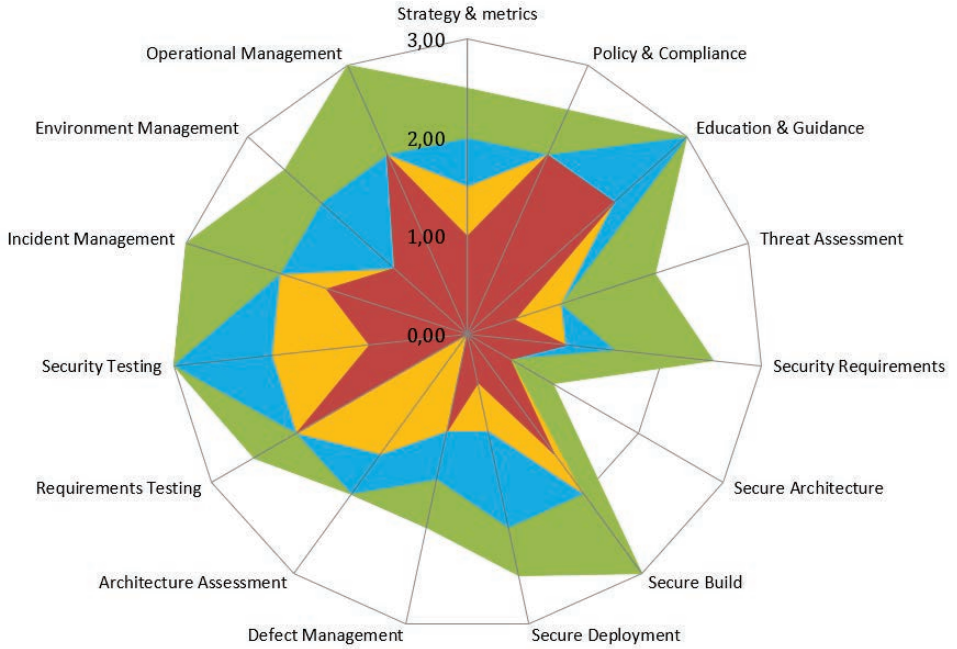
- **Perform Maturity Level Assessments**
  - Assess your current status based on OWASP SAMM
  - Technology and process agnostic

- **Identify potentials to improve your security practices**
  - Know your weak spots and improve them
  - Invest in those areas with the most security leverage



Roadmap to higher Software Assurance

- **Define an implementation roadmap**
  - Roadmap with defined checkpoints
  - Make improvements measurable
- **Increase the maturity level over time**
  - Integrate security step by step
  - Use success stories to drive improvements
- **Perform checkpoint assessments to track progress**
  - Regular assessments verify that you are still on track
  - Course correction can be done early



Contact Information

Further Questions? Let‘s talk!

DI Thomas Kerbl, MSc

SEC Consult Unternehmensberatung GmbH

Principal Security Consultant / Teamleader

ISTQA, ISAQB, CPSSE, PCiIAA

E t.kerbl@sec-consult.com

T https://twitter.com/dementophobia

X https://www.xing.com/profile/Thomas_Kerbl

L https://at.linkedin.com/in/thomas-kerbl-2ab81648