WELCOME!

Mastering Security Requirements Engineering

February 24, 2021 | with Thomas Kerbl

SEC Consult
an atos company

Thomas Kerbl

Principal Security Consultant

- 20+ years experience in information security
- 50+ speeches
- Service Owner for „Secure Software Development Consulting“
- Teamleader
- Security Analyst, Security Architect

Education

- MSc @ Technikum Vienna, Specialization in Multimedia & Software Development
- Dipl. Ing @ Hagenberg, Specialization in Computer- and Media Security

Certificates

- Accredited ÖNORM A 7700 Auditor
- ISTQB Certified Tester
- ISAQB Certified Professional for Software Architecture
- ISSECO Certified Professional for Secure Software Engineering
- PCiIAA Practitioner Certificate in Information Assurance Architecture

t.kerbl@sec-consult.com
https://twitter.com/dementophobia

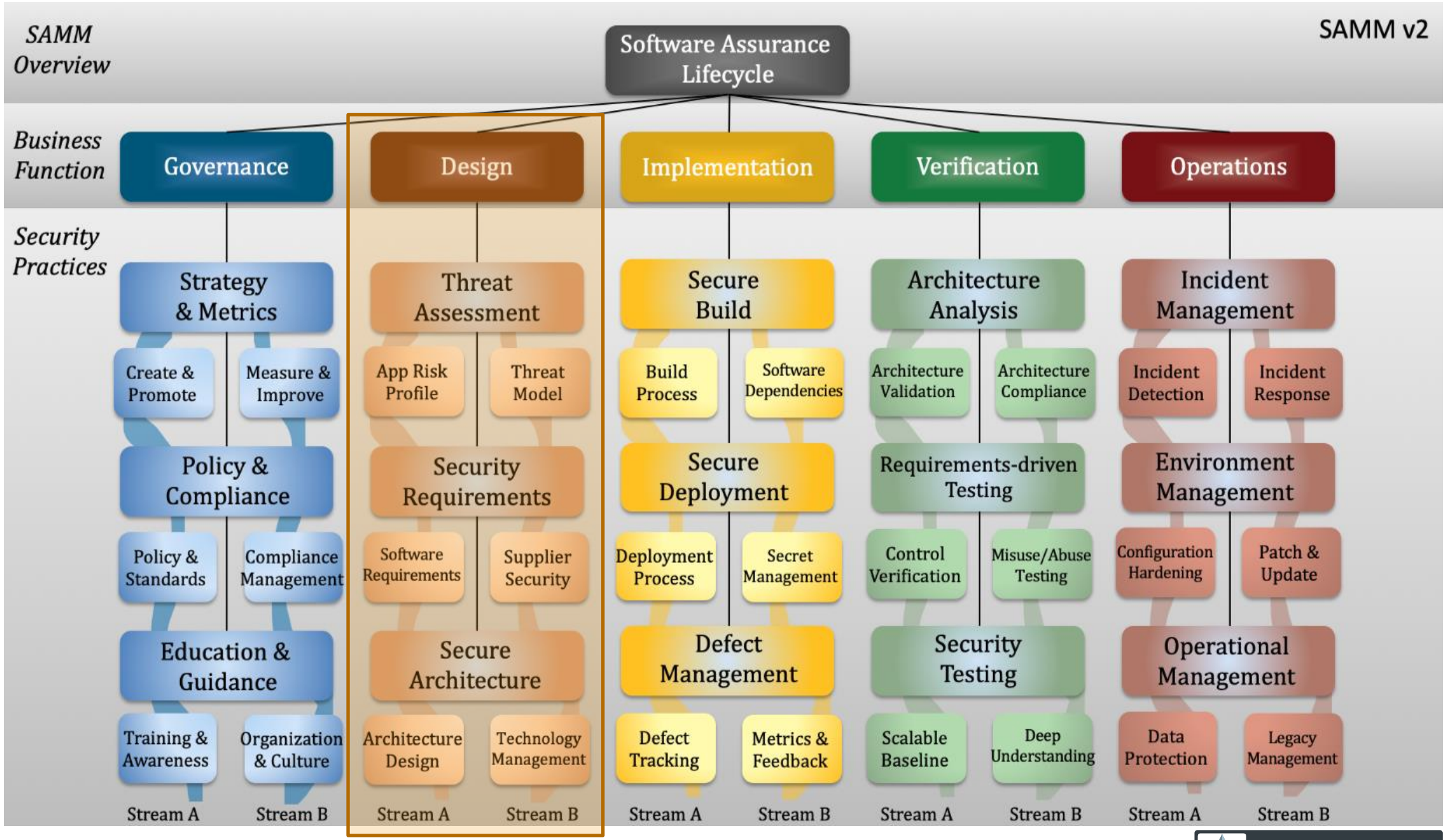
SEC Consult
an atos company

Topics for Today

- Quick **Introduction to OWASP SAMM**
- **From the Early Stages to Mastery** of Security Requirements Engineering
- **Common Pitfalls** to avoid
- Next Steps to **improve your Security Posture**

A quick introduction to OWASP SAMM v2

https://www.owaspsamm.org/



Topics for Today

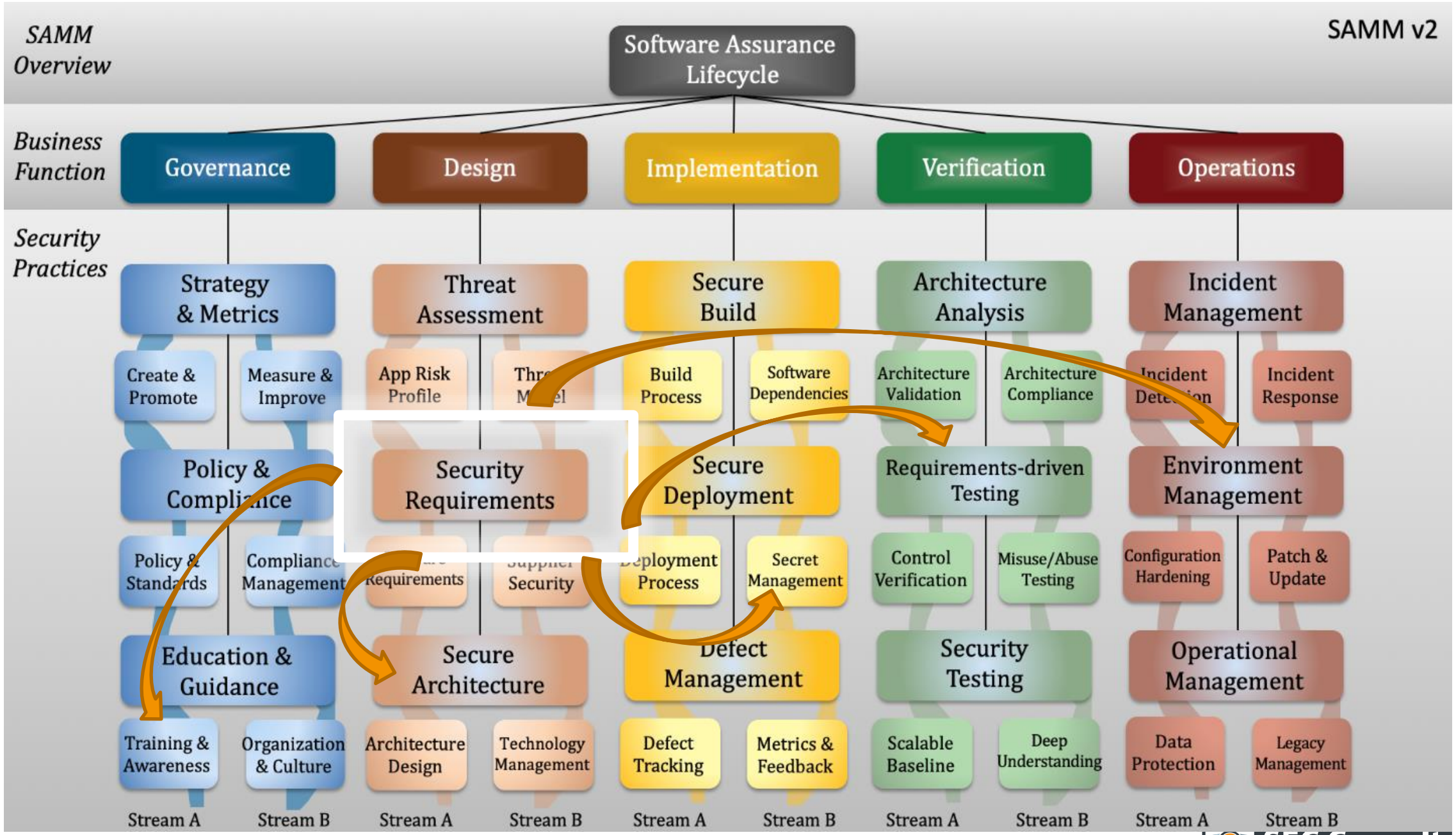
- Quick **Introduction to OWASP SAMM**
- **From the Early Stages to Mastery** of Security Requirements Engineering
- **Common Pitfalls** to avoid
- Next Steps to **improve your Security Posture**

The Power of Security Requirements

- On Paper: Just **1 out of 15** Security Activities in OWASP SAMM
- In Practice: The **Foundation** for many of the other Security Activities

SAMM model overview

Governance	Design	Implementation	Verification	Operations
Strategy and Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Policy and Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Education and Guidance	Security Architecture	Defect Management	Security Testing	Operational Management



Respect the fundamental principles

- Requirements Engineering is an **established craft**
- The fundamentals do apply to **Security Requirements Engineering**
- **Aim for full integration** in your requirements engineering process

Requirements define **WHAT** to do, not **HOW** to do it

Specific	Measurable	Reasonable

Dipping your toe into the water

- Use the OWASP ASVS for **inspiration**
- **Shortcut** for technical requirements
- When in doubt, be **more generic**
- Don’t neglect the **fundamentals**
- This is **not** a long term solution

Warning

This shortcut is no substitute for proper security requirements engineering in the long run!

Ensure proper verification

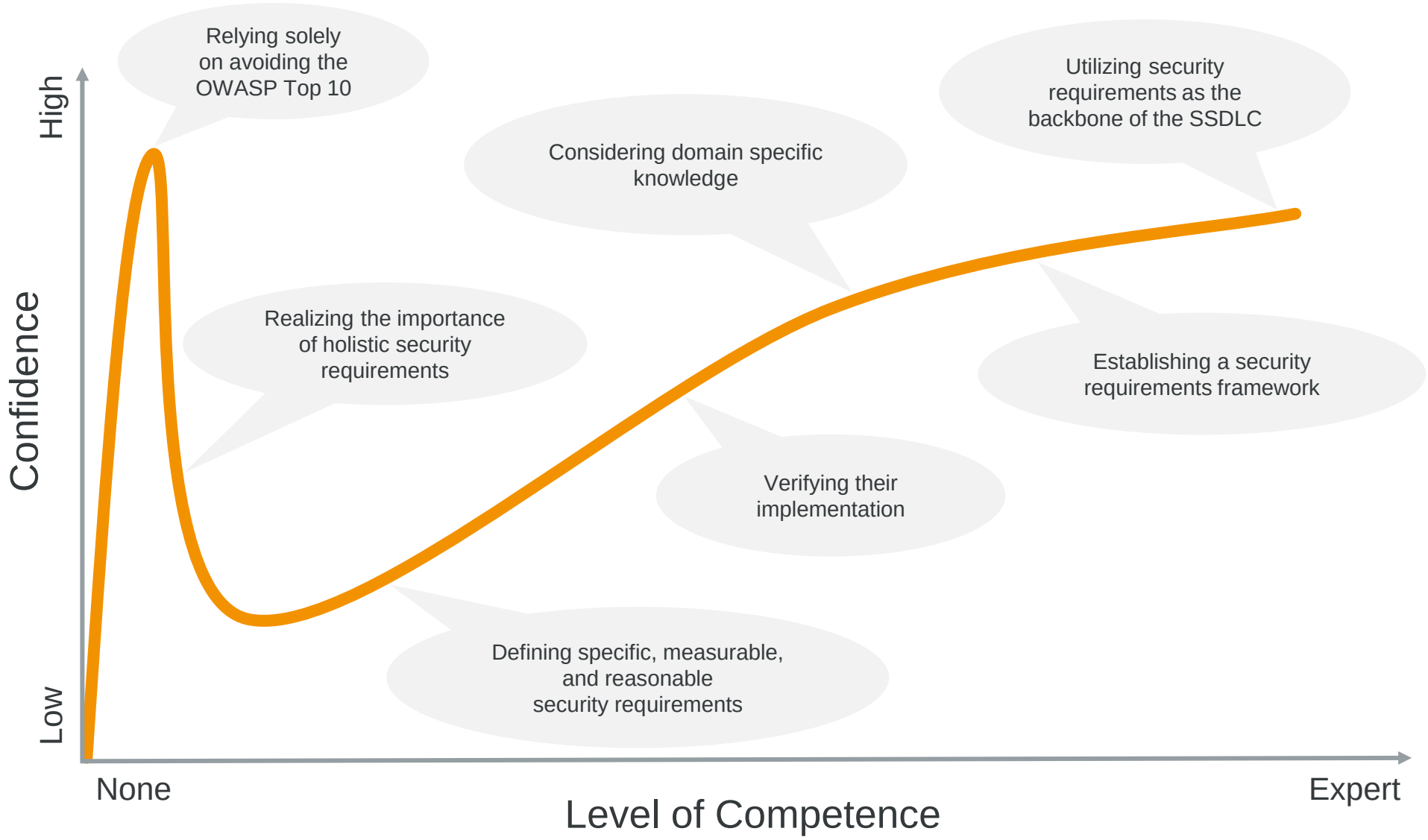
- Don’t force integration into all security activities
- **Ensure verification** of your security requirements **right from the start**
- Security Requirements must **not be treated as optional**
- **Method** of verification **depends on the culture** of the organization

Review Sessions across departments	Requirements-driven Security Testing	Formal Quality Gates

Topics for Today

- Quick **Introduction to OWASP SAMM**
- **From the Early Stages to Mastery** of Security Requirements Engineering
- **Common Pitfalls** to avoid
- Next Steps to **improve your Security Posture**

Pitfall #1: Relying solely on vulnerability classes to avoid



Pitfall #2: Hiding requirements from penetration testers

- Security tests should **focus on the most important areas**
- Providing security requirements helps the test team to **fine-tune their approach**
- This allows you to **get the most out of your available budget**
- Hiding your security requirements creates a **lose-lose scenario**

Hiding your **security requirements** from the **security test team**
is like **going to your doctor** for a general checkout
without mentioning that you are **running a marathon** next week.

Pitfall #3: Not holding vendors to the same standards

- Security requirements must be part of the **contract**
- Do **not** assume a strong level of security is the **default**
- **Verify** the implementation of your security requirements

An **attacker doesn't care** whether the **broken part** of your application has been developed inhouse or not.

A vulnerability is a vulnerability,
no matter who is responsible for this **quality issue**.

Topics for Today

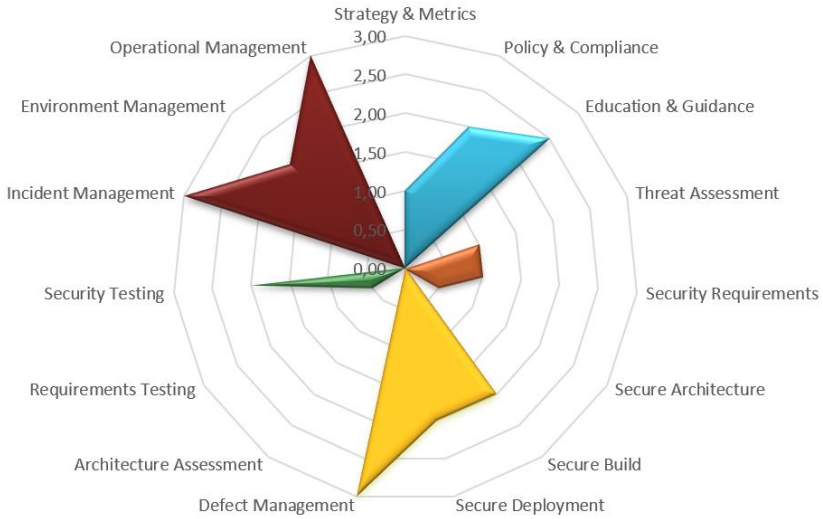
- Quick **Introduction to OWASP SAMM**
- **From the Early Stages to Mastery** of Security Requirements Engineering
- **Common Pitfalls** to avoid
- Next Steps to **improve your Security Posture**

Gap Analysis and Maturity Level Assessment

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

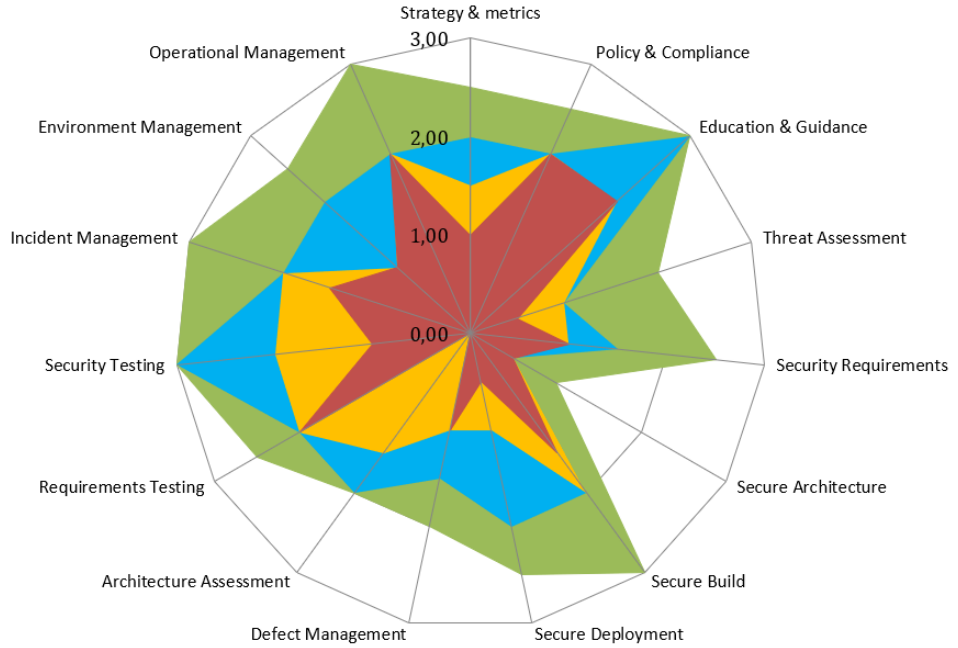
- **Perform Maturity Level Assessments**
  - Assess your current status based on OWASP SAMM
  - Technology and process agnostic

- **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



A deep dive into Secure Software Development based on OWASP SAMM

	WOOD	BRONZE	SILVER	GOLD	DIAMOND
Maturity Level	Zero	Low	Medium	High	Mastery
Approach	Not Implemented	Ad Hoc	Guided	Enforced	Enforced and Audited
Level of Training	None	Self Study	Training on the Job	Regular Generic Trainings	Regular Role Specific Trainings
Quality Gate	No	No	Optional Informal Review	Mandatory Informal Review	Mandatory Formal Review
Protection Profile	Minimal Protection Requirements	Low Protection Requirements	Medium Protection Requirements	High Protection Requirements	Very High Protection Requirements

Quality Levels for your Security Activities SEC Consult

https://www.heise.de/hintergrund/Sichere-Software-entwickeln-mit-OWASP-SAMM-4918292.html

https://r.sec-consult.com/SSDLC

Follow me for Updates!
@Dementophobia

Q&A

ASK ME ANYTHING!

Thomas Kerbl

t.kerbl@sec-consult.com

https://twitter.com/dementophobia

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