OWASP-Stammtisch Hannover

Thema: Sichere Softwareentwicklung mit OWASP

Benjamin Liebe
benjamin.liebe@owasp.org

OWASP-Stammtisch Hannover?

Monatliche Treffen

- https://www.meetup.com/de-DE/OWASP-Germany-Chapter-Stammtisch-Hannover/
- https://owasp.org/www-chapter-germany/stammtische/hannover/

Geplante Vorträge 📅

- 24. März: Vortrag von Dirk Wetter (Docker Top 10 / testssl.sh / OWASP)
- Ende April: Pwning OWASP Juice Shop mit Björn Kimminich


PRESENTING
OWASP
SAMM

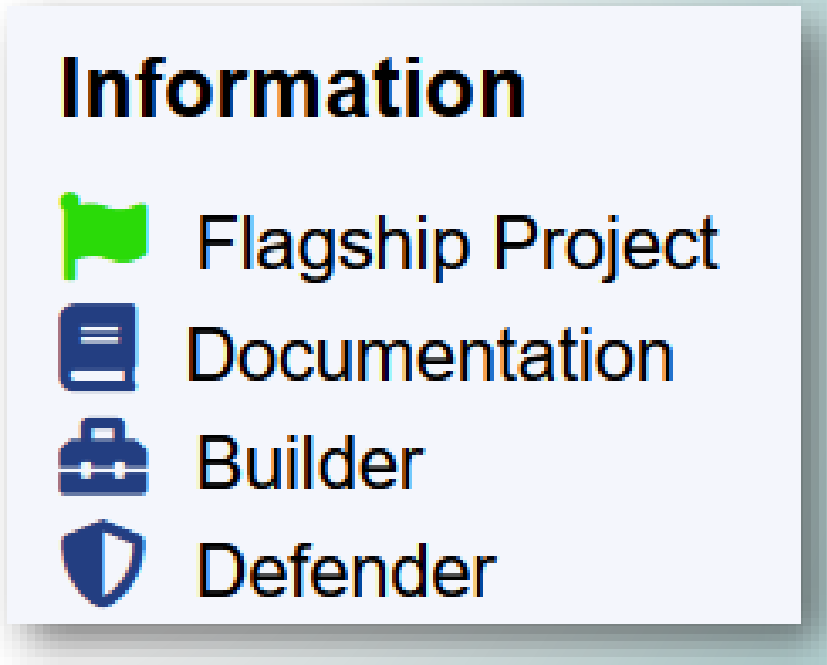
OWASP SAMM

Software **A**ssurance
Maturity **M**odel

- Früher: Open SAMM
- Verwandt mit BSIMM
- owaspsamm.org

Reifegradmodell für

- Bestandsaufnahme
- Planung von Aktivitäten



August 2008: Erste Beta

SAMM Beta Release

Posted by Pravir Chandra in Releases on August 21st, 2008

Thanks to sponsorship and feedback from Fortify, we've finished an initial release of the Software Assurance Maturity Model (SAMM) that is now available on the downloads page. Everyone is encouraged to review and provide feedback either directly to me or through discussion on the OWASP-CMM mailing list. The working goal is to have a solid 1.0 release in a few months after public review and feedback from organizations using the model and vendors in the software security space.

beta, release

No Comments

Januar 2020: V2 Finalisiert

OWASP SAMM VERSION 2 - PUBLIC RELEASE

BY THE SAMM PROJECT TEAM IN RELEASE

January 31, 2020

After three years of preparation, our SAMM project team has delivered version 2 of SAMM! OWASP SAMM (Software Assurance Maturity Model) is the OWASP framework to help organizations assess, formulate, and implement, through our self-assessment model, a strategy for software security they can be integrated into their existing Software Development Lifecycle (SDLC). The new SAMM v2 consists of the following components: The SAMM Model overview and introduction, explaining the maturity model in detail A Quick-start Guide with different steps to improve your secure software practice An updated SAMM Toolbox to perform SAMM assessments and create SAMM roadmaps A new SAMM Benchmark initiative to compare your maturity and progress with other similar organizations and teams What's changed with SAMM v2?

CONTINUE READING

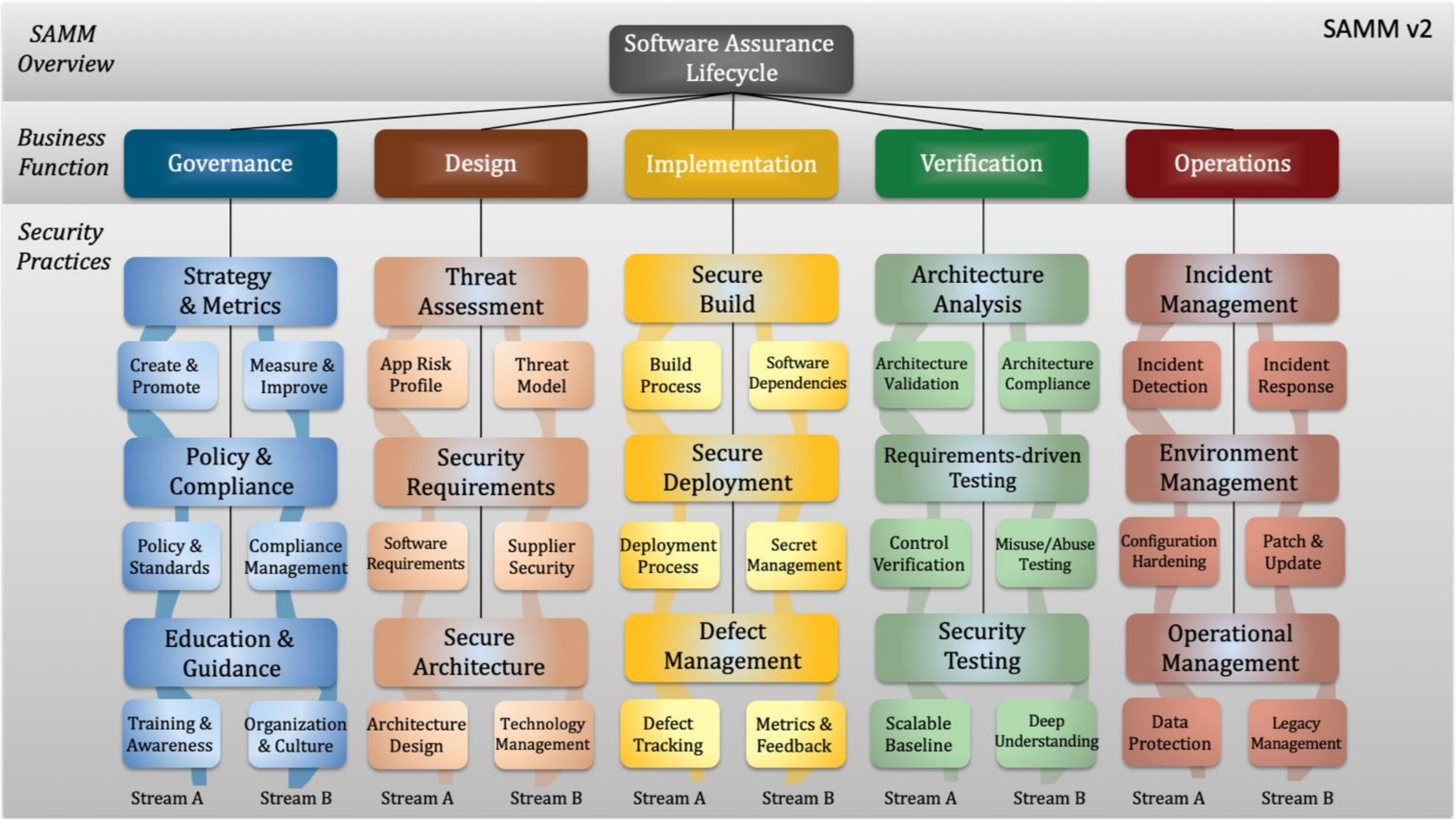
SAMM Benchmark Initiative

Ziel: Vergleichbarkeit

- Wie steht man selbst im Vergleich zu anderen da?
- Was hat sich bewährt?

Status

- Projekt im Aufbau
- Noch keine öffentlichen Daten
- Einreichungen bereits möglich


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

Business Function

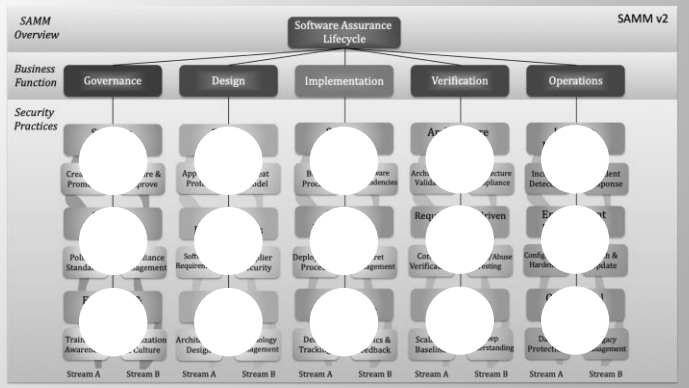
Security Practice

Stream A | Stream B

- Reifegrad 1
- Reifegrad 2
- Reifegrad 3

Project 1

Project 2



Governance

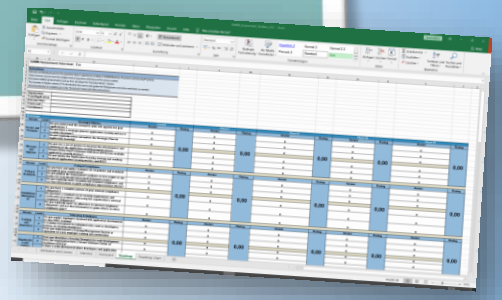
Strategy and Metrics

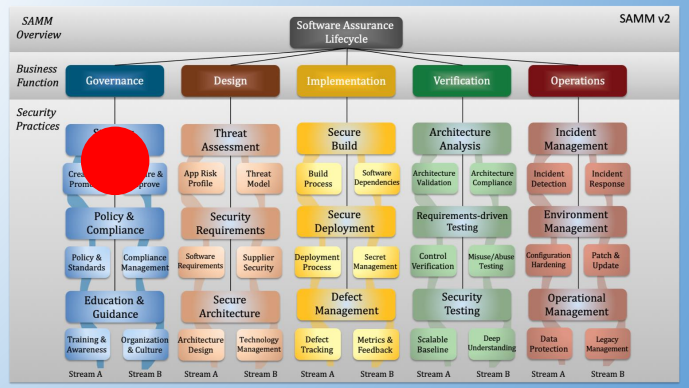
Create and Promote

Measure and Improve

- Ziele und Kennzahlen festlegen
- Roadmap für Aufbau von SW-Sicherheit erstellen (mit SAMM)
- Aktivitäten am Unternehmen ausrichten

OWASP SAMM





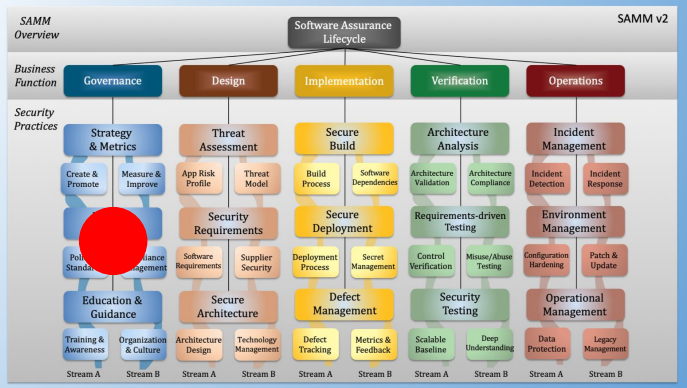
Governance

Policy and Compliance

Policy and Standards

Compliance Management

- Relevante interne und externe Anforderungen identifizieren
- Baseline für Sicherheits-anforderungen schaffen
- Erfüllungsgrad messen



Governance

Education and Guidance

Training and Awareness

Organization and Culture

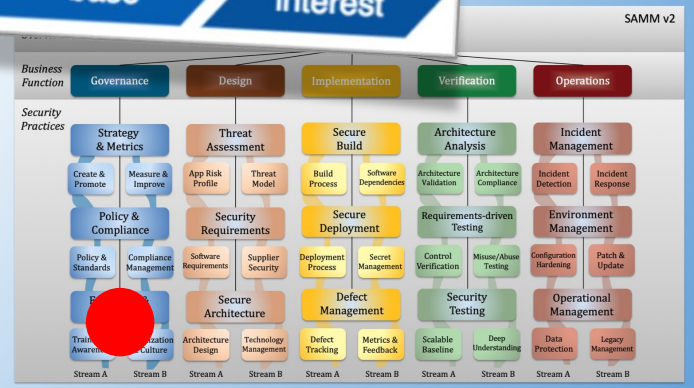
- Wissen über sichere SW-Entwicklung verbreiten
- Rollenspezifische Kenntnisse vermitteln
- Secure Software Community aufbauen

WEBGOAT

Security Knowledge Framework

Security Champions playbook

Identify teams → Define the role → Nominate champions → Comm channels → Knowledge base → Maintain interest



Design

Threat Assessment

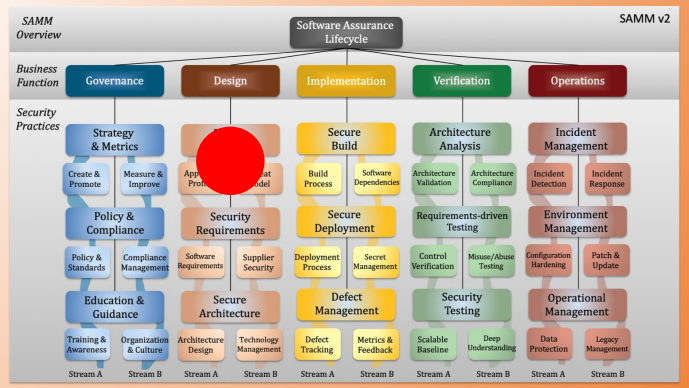
Application Risk Profile

Threat Modeling

- Allgemeine Bedrohungen und Einstufung der Anwendung fließen in Anforderungsprozess ein
- Aufdecken von Designfehlern mit Threat Modeling

{❤} threatspec

OWASP PyTM



Design

Security Requirements

Software Requirements

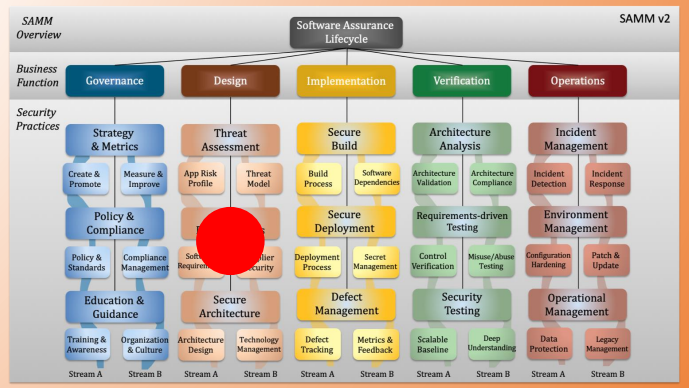
Supplier Security

- Explizite Berücksichtigung von Sicherheit im Anforderungs- oder Beauftragungsprozess
- Verfeinerung der Sec-Anforderungen anhand von Fachlogik und bekannten Risiken
- Verbindliche Sec-Anforderungen für die komplette Entwicklung

OWASP ASVS

OWASP MASVS

OWASP SecurityRAT



Design

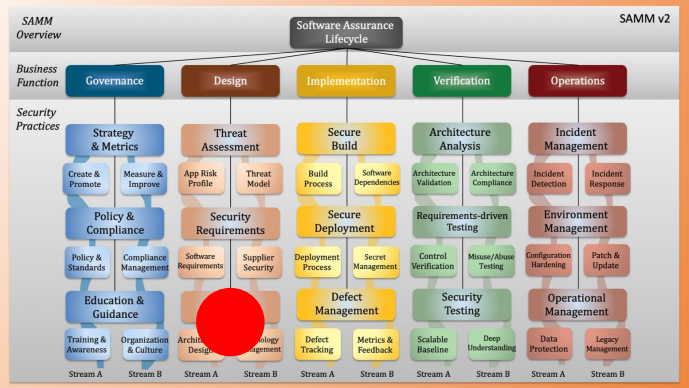
Security Architecture

Architecture Design

Technology Management

- Beachtung von Sicherheitsempfehlungen in der Entwurfsphase
- Im Entwurf wird auf Secure-by-Default und bewährte Sicherheitslösungen geachtet
- Tatsächliche Nutzung sicherer Architekturen wird geprüft.

Security Knowledge Framework



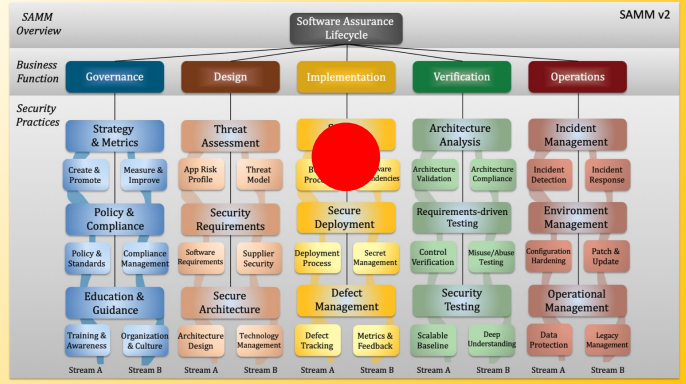
Implementation

Secure Build

Build Process

Software Dependencies

- Build-Prozess ist reproduzierbar
- Automatische Build-Pipeline mit Sicherheits-prüfungen
- Build-Prozess verhindert, dass bekannte Schwachstellen in Produktion kommen



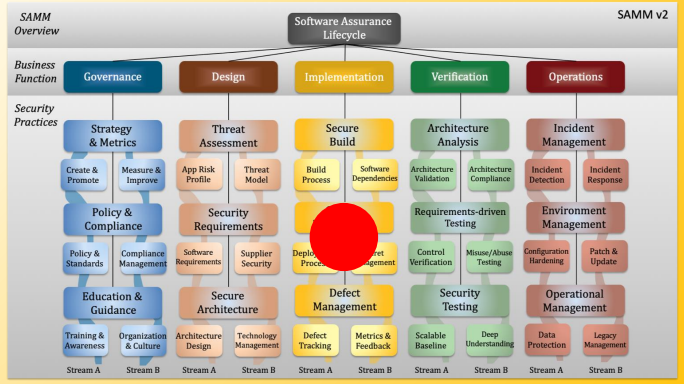
Implementation

Secure Deployment

Deployment Process

Secret Management

- Deployment prüft Sicherheit und ist automatisiert
- Keine Passwörter, Keys etc. im Quellcode



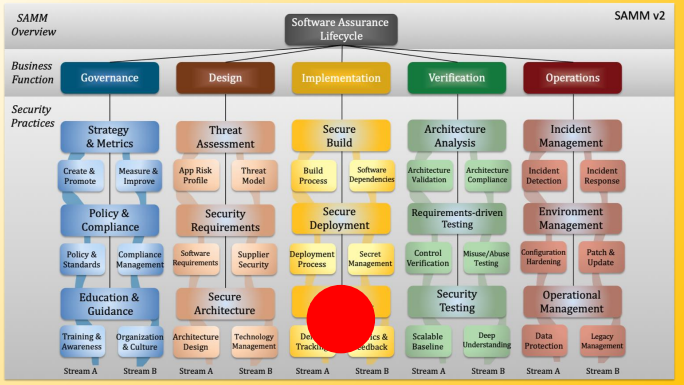
Implementation

Defect Management

Defect Tracking

Metrics and Feedback

- Defects werden strukturiert erfasst und verfolgt.
- Aus Defects wird gelernt, um gleichartige Probleme zukünftig zu vermeiden.



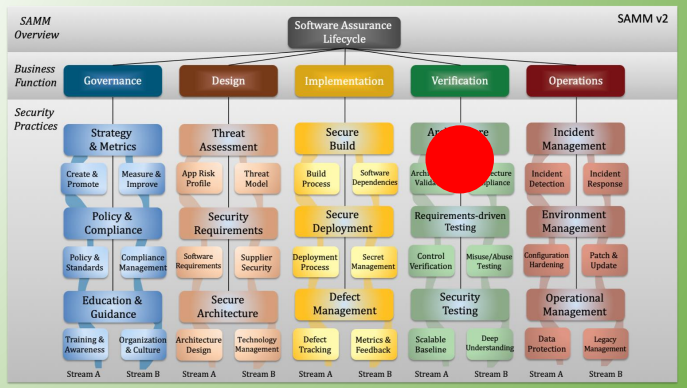
Verification

Architecture Assessment

Architecture Validation

Architecture Mitigation

- Sicherstellen, dass typische Risiken vermieden werden
- Konzeptionelle Prüfung von Sicherheitsmechanismen
- Wirksamkeit der Architektur wird geprüft und diese ggf. nachgebessert



Verification

Requirements-driven Testing

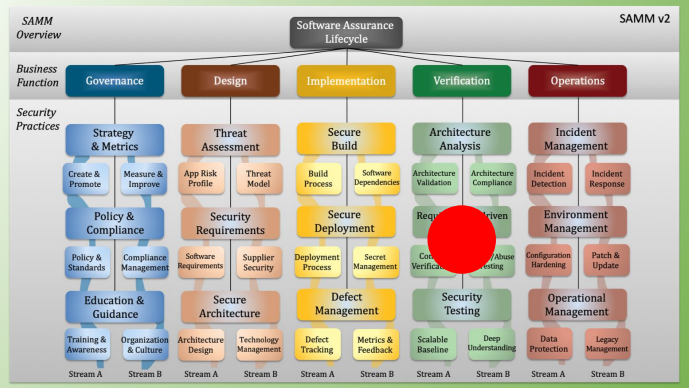
Control Verification

Misuse/Abuse Testing

- Einhaltung der Sec-Anforderungen wird systematisch geprüft.
- Umsetzung von Security Best Practices wird technisch geprüft.

OWASP WSTG

OWASP MSTG



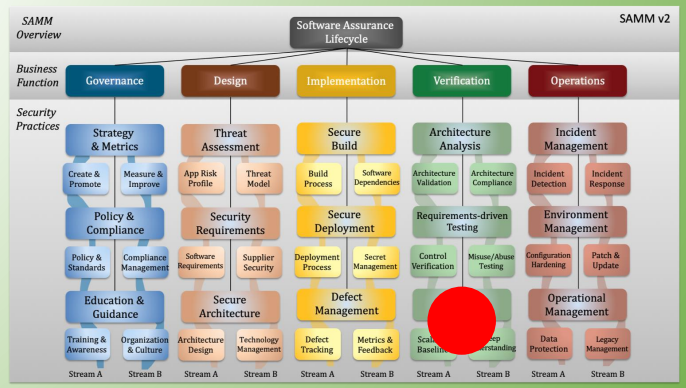
Verification

Security Testing

Scalable Baseline

Deep Understanding

- Flächendeckende automatische Tests in Entwicklung und Deployment
- Vertiefende manuelle Analyse kritischer Module
- Penetrationstests



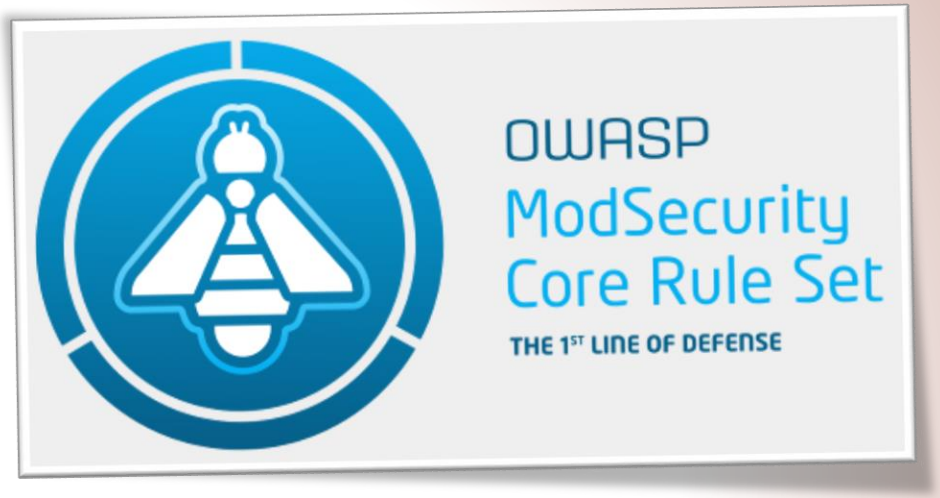
Operations

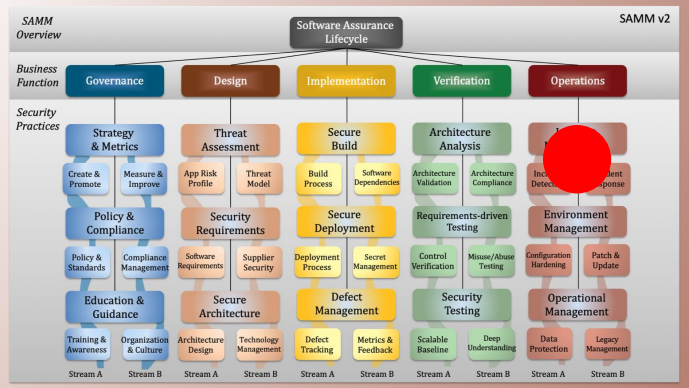
Incident Management

Incident Detection

Incident Response

- Vorfälle werden proaktiv erkannt und gemäß eines Prozesses bearbeitet
- Die Reaktion auf Vorfälle erfolgt durchdacht und diszipliniert





Operations

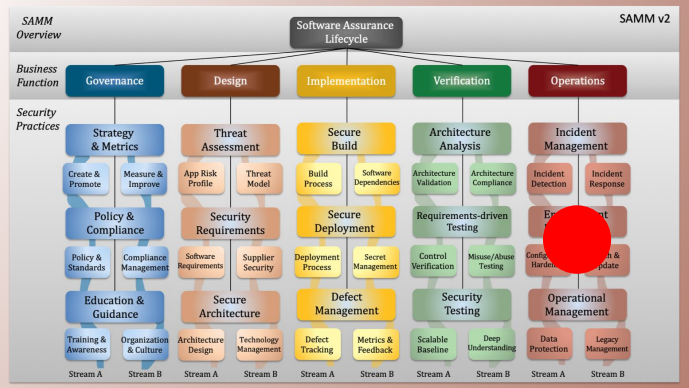
Environment Management

Configuration Hardening

Patching and Updating

- Patchen und Härten gemäß geregeltem Prozess
- Einhaltung der Vorgaben wird überwacht

OWASP Docker Top 10



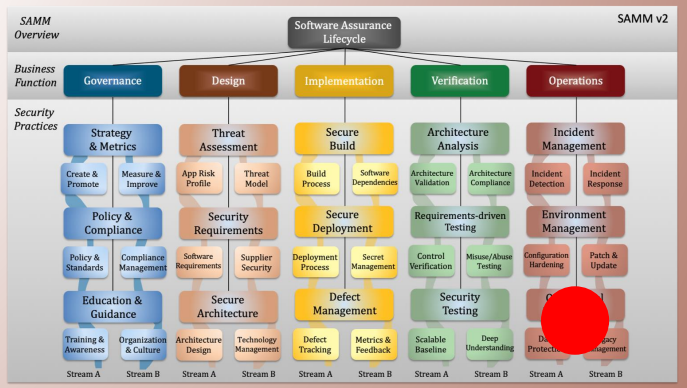
Operations

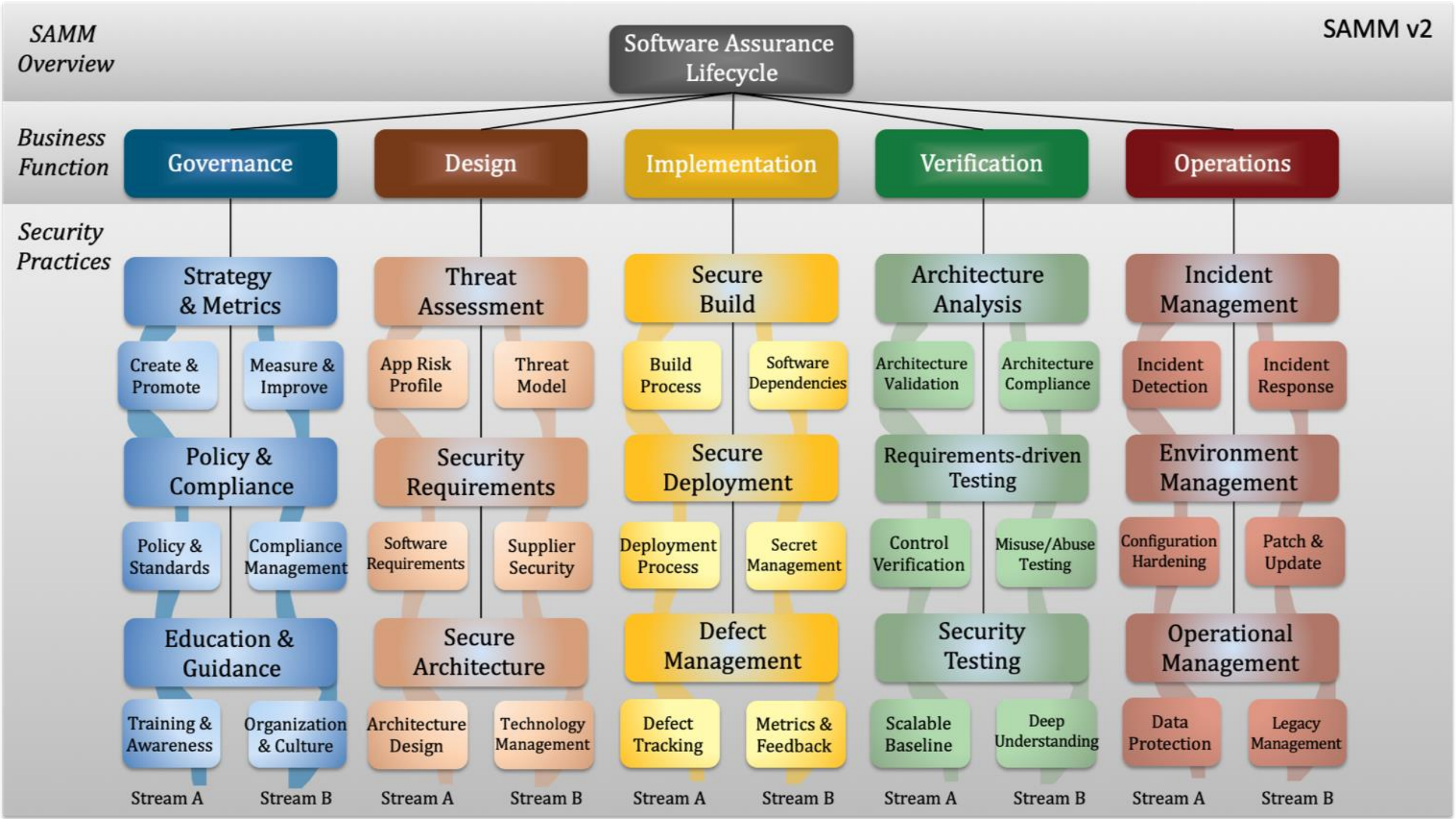
Operational Management

Data Protection

System Decomissioning / Legacy Management

- Strukturierter Umgang mit sensiblen Daten
- Geordneter Umgang mit Altsystemen und deren Abschaltung




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

OWASP Integration Standards

https://github.com/OWASP/www-project-integration-standards

- Projekt ist 2020 gestartet
- Ziel: Roter Faden für OWASP-Projekte