Strategic Usage of the OWASP SAMM and DSOMM

Timo Pagel

Agenda

- Introduction/Motivation
- High Level Approaches
- Detailed Usage
- Conclusion

Agenda

- Introduction/Motivation
- High Level Approaches
- Detailed Usage
- Conclusion

About Me

- DevSecOps Consultant
- Lecturer for *Security in Web Applications* at different *Universities*

About Me

- DevSecOps Consultant
- Lecturer for *Security in Web Applications* at different *Universities*
- Open Source / Open Knowledge Enthusiast

OWASP DevSecOps Maturity Model

OWASP Juice Shop

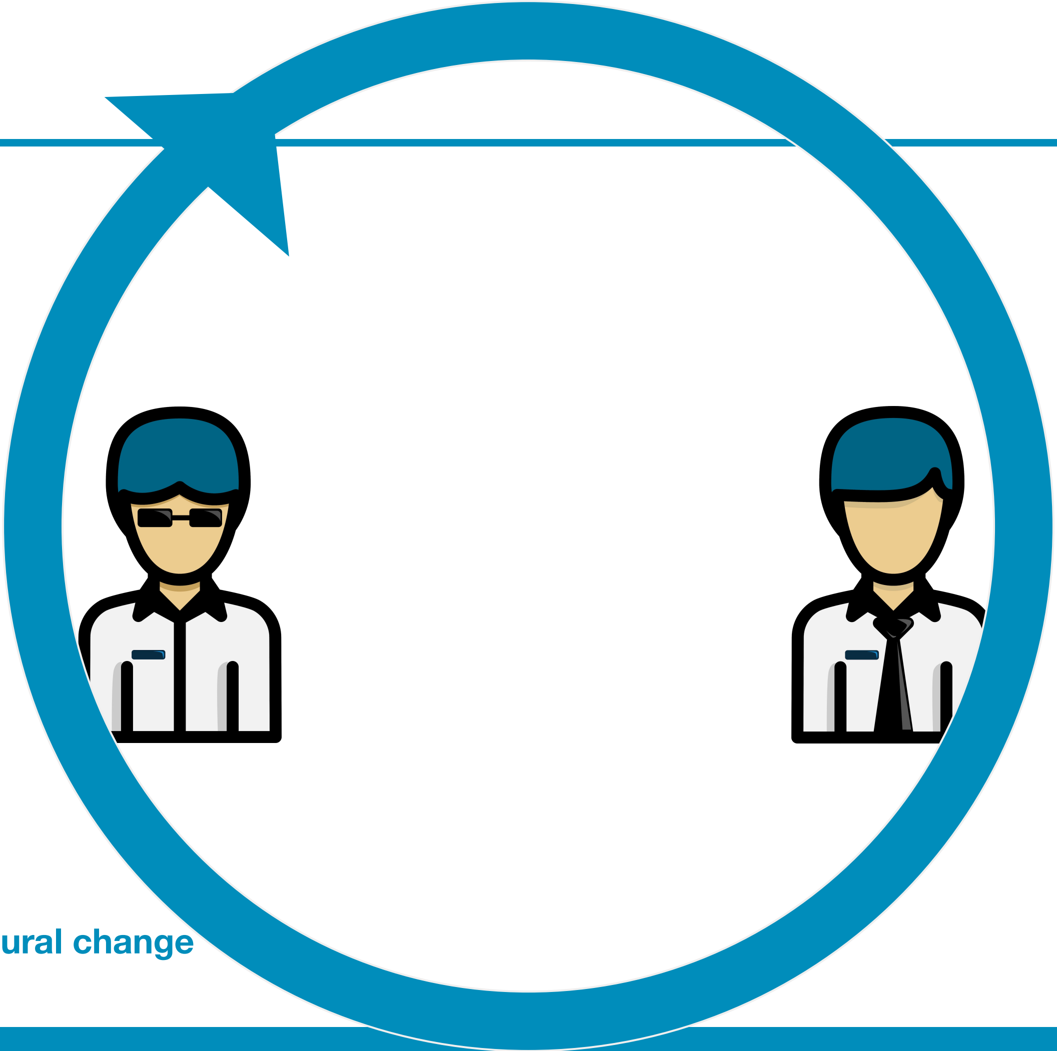
OWASP Security Pins

OWASP DefectDojo

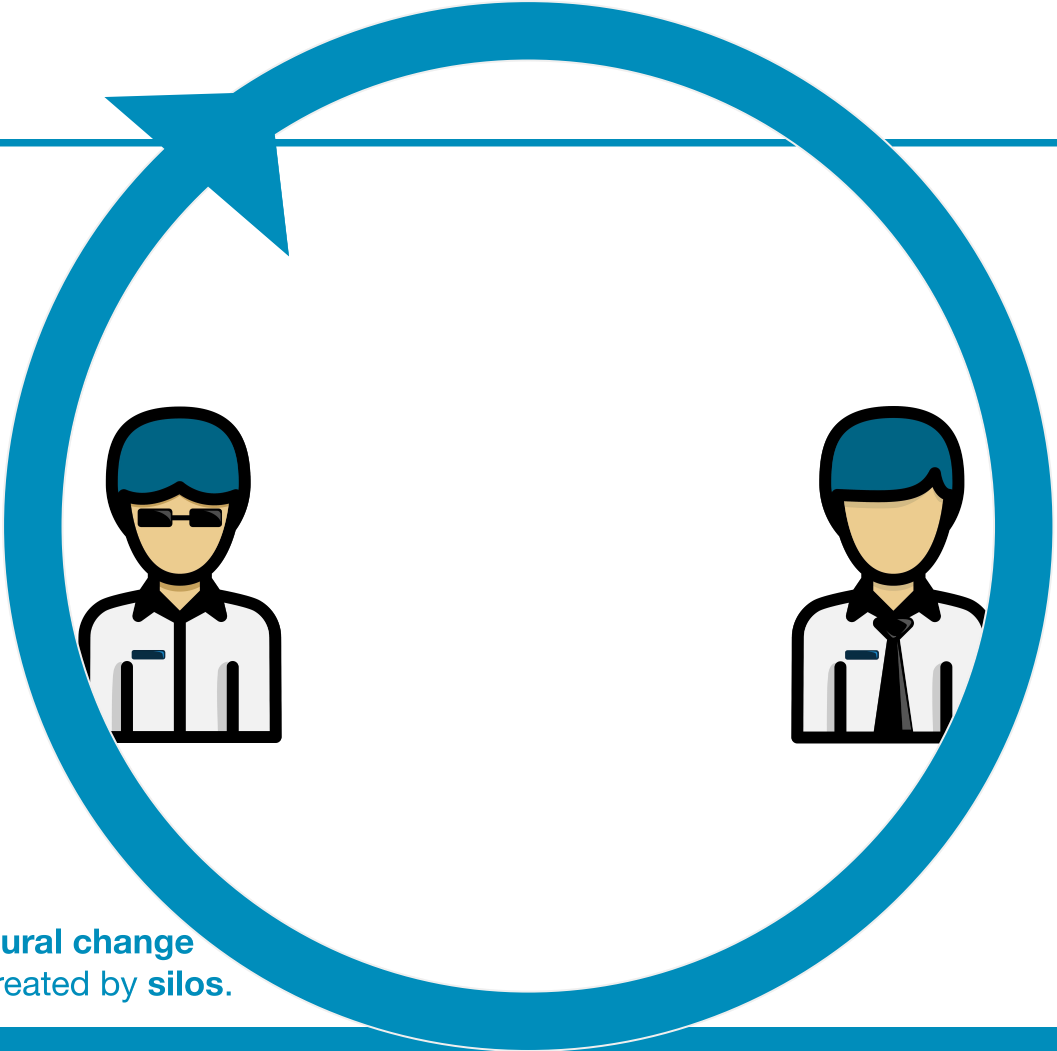
OWASP Software Assurance Maturity Model

Target Audience

- Security People (Information- and Technical Security)
- Technical Upper Management (CTO)
- Enthusiastic Developers, Operator, C-Level

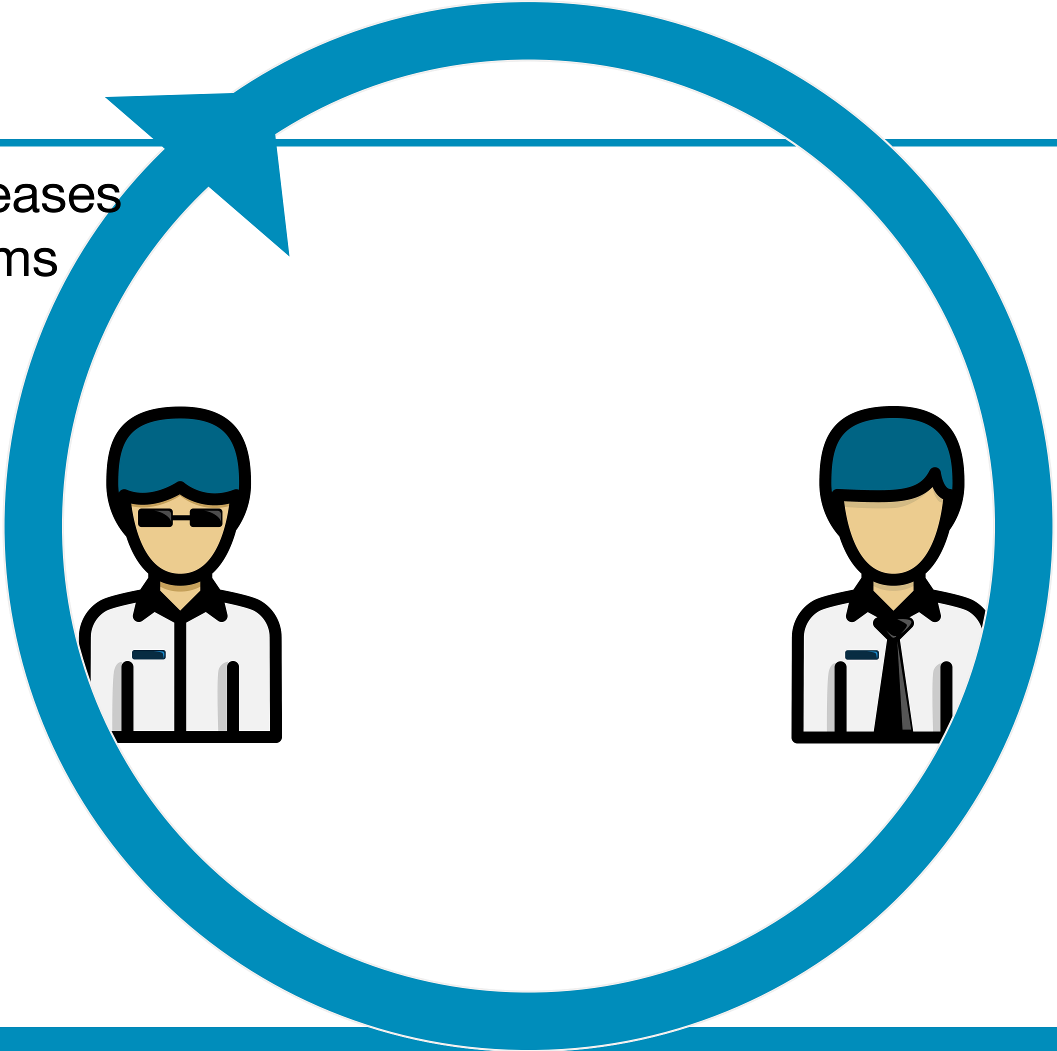


DevOps encourages a **cultural change**



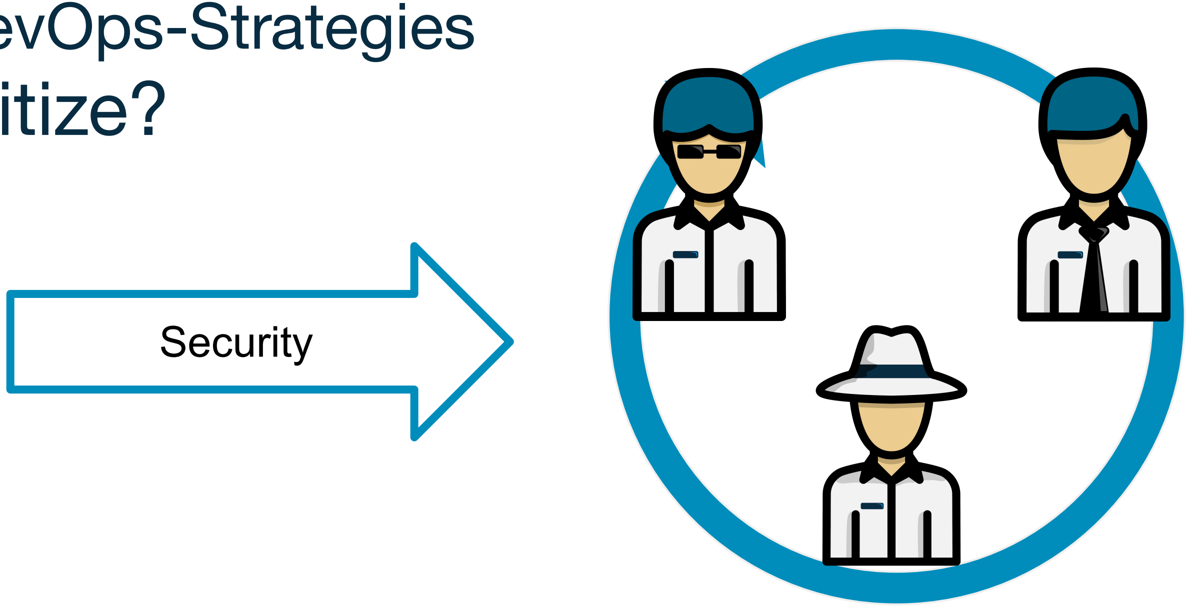
DevOps encourages a **cultural change**
to overcome the **friction** created by **silos**.

Speed / Fast Releases
Independent Teams
Different Skills
Automation



Problem Statement

- How to enhance security?
  - In DevOps-Strategies
  - Through DevOps-Strategies
- How to prioritize?



Security

DevOps Dimensions

Build and Deployment

Culture and Organisation

DevOps Dimensions

- Build and Deployment
- Culture and Organisation
- Information Gathering
- Hardening
- Test and Verification

Target of Security Maturity Models

Analyse **current** software security **practices**,
build a security program in defined iterations,
show **progressive improvements** in secure practices,
and define and measure security-related activities.

Based on Brian Glas, https://owaspsamm.org/blog/2020/10/29/comparing-bsimm-and-samm/

Agenda

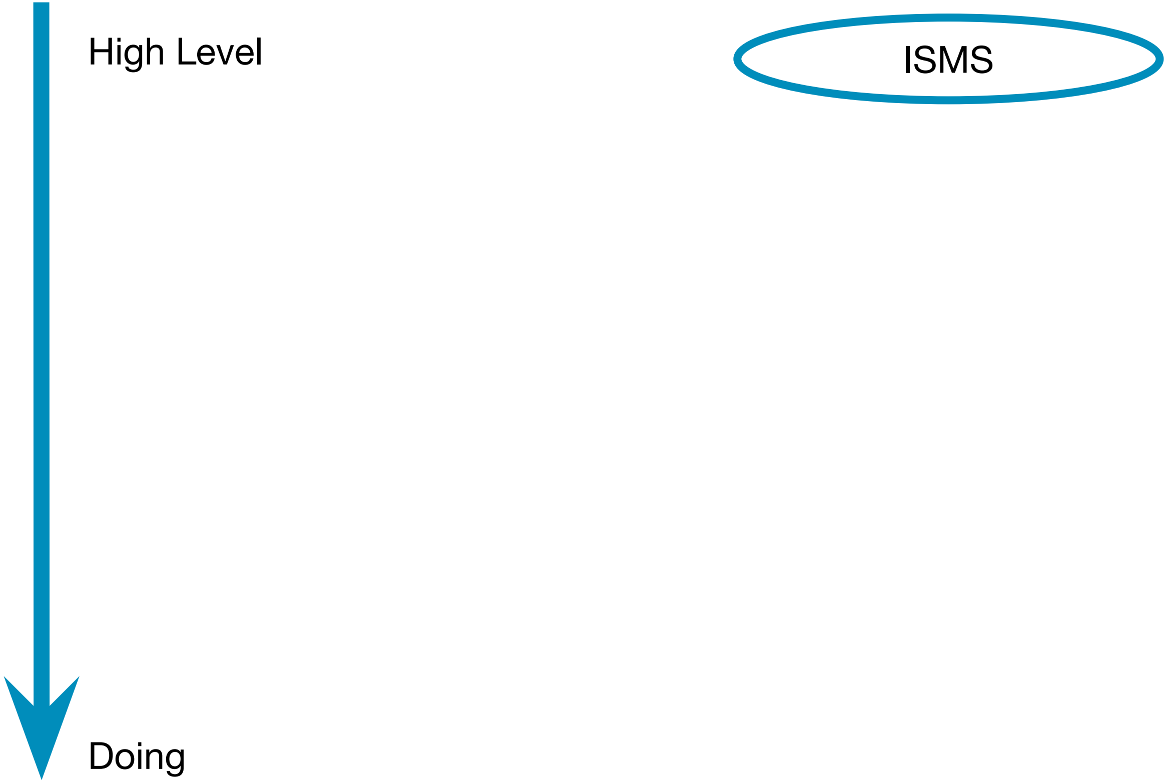
- Introduction/Motivation
- High Level Approaches
- Usage
- Conclusion

Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM

High Level

Doing

Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM

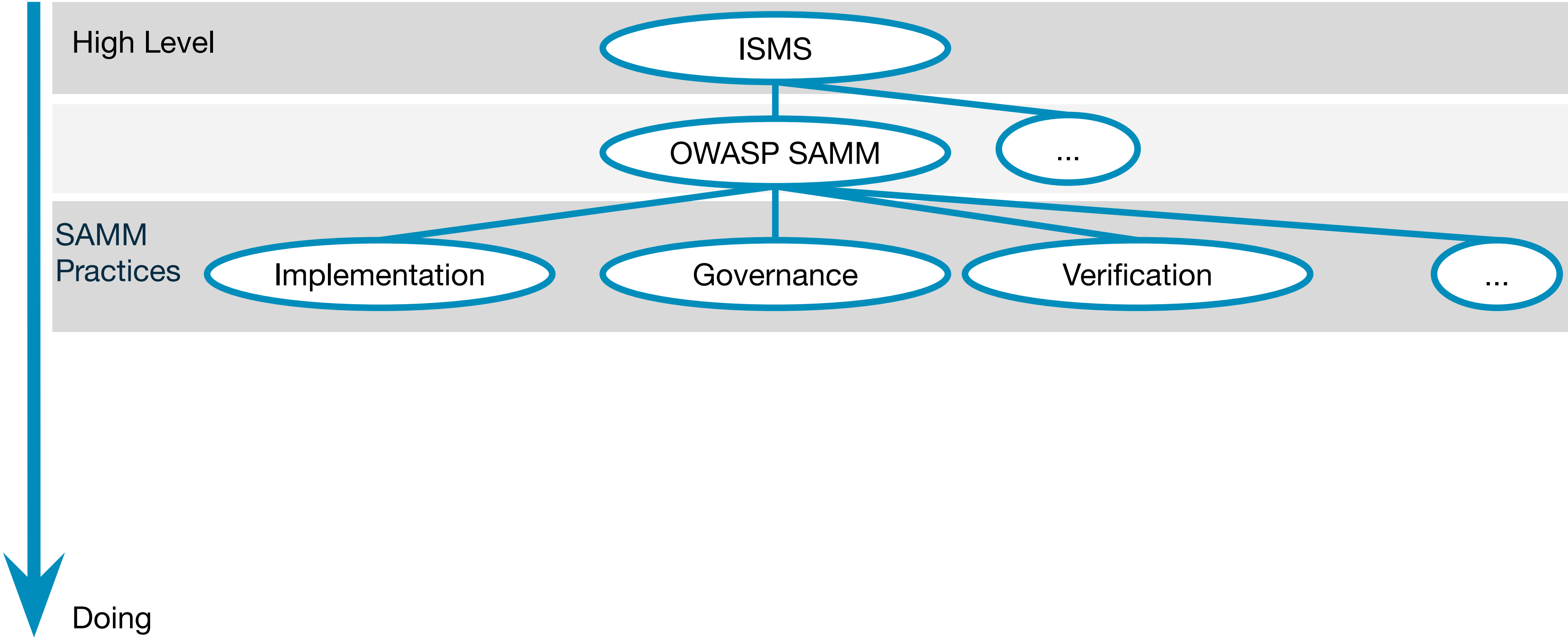


High Level

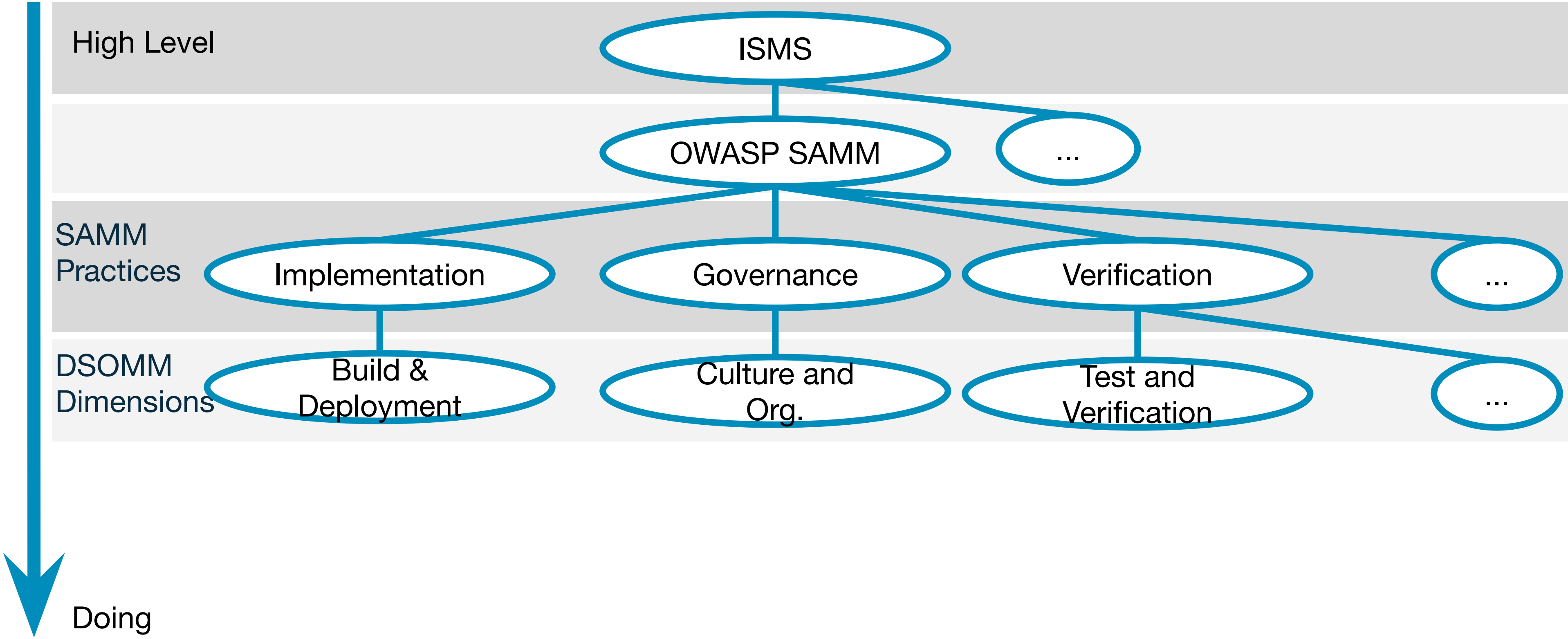
ISMS

Doing

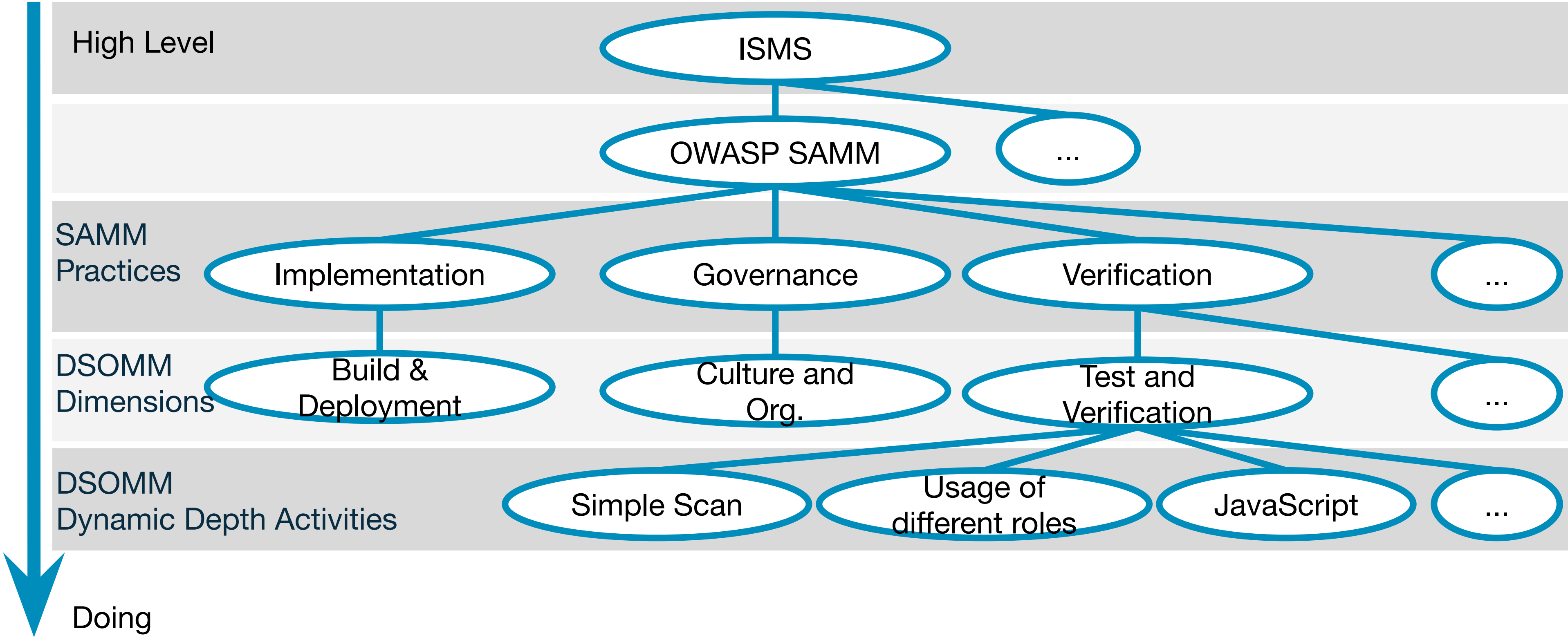
Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



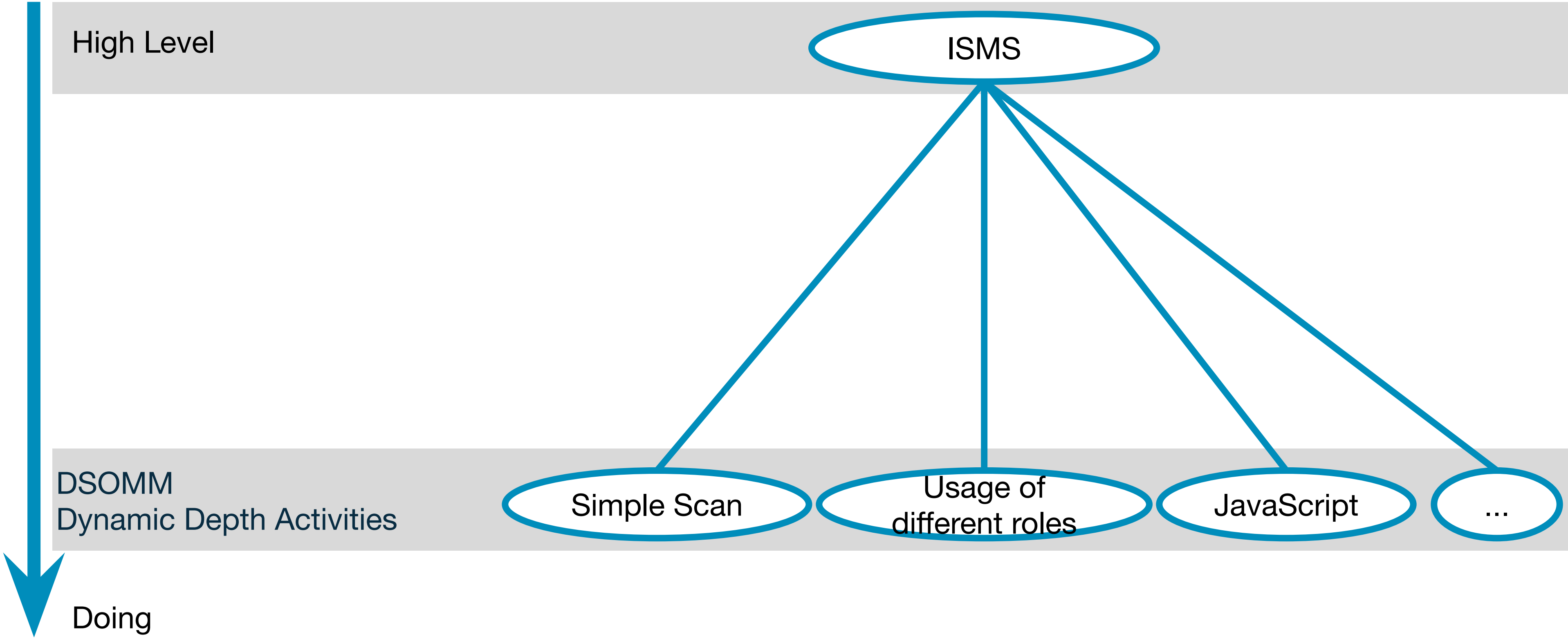
Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



Target Groups

- SAMM 2.0: SAMM
  - Security: Assessment
  - Engineers/CTO: Spider web
  - C-Level Management: Spider web and definition of targets

Audit / Compliance View



SAMM and DSOMM

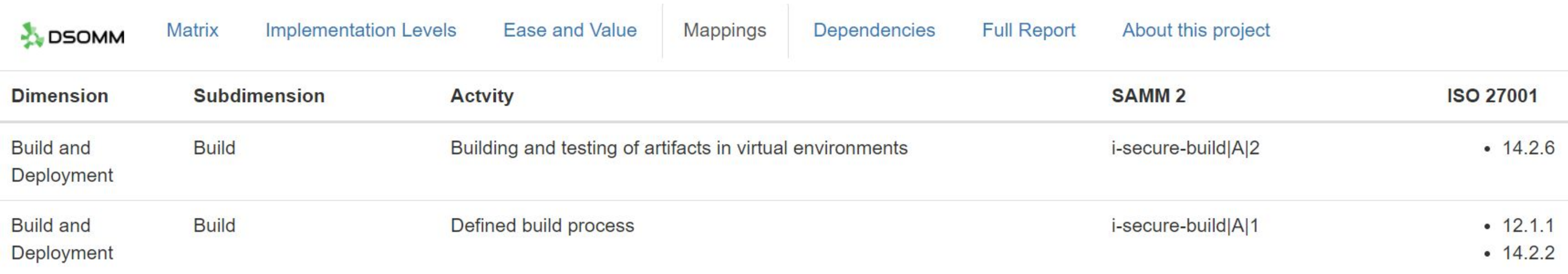
SAMM

- “Standard”
  -> High level overview
- Management topics like compliance and governance
- Planning of high level targets
- Mapping to ISO in the future

DSOMM

- Emerging
  -> Low level overview
- Only DevSecOps topics
- Planning of concrete targets
- Mapping to ISO/SAMM
- ISMS: documentation in DSOMM

Mapping DSOMM to SAMM and ISO 27001



Dimension	Subdimension	Actvity	SAMM 2	ISO 27001
Build and Deployment	Build	Building and testing of artifacts in virtual environments	i-secure-build|A|2	• 14.2.6
Build and Deployment	Build	Defined build process	i-secure-build|A|1	• 12.1.1 • 14.2.2

Sample Target Groups

SAMM

- Security: Assessment
- Engineers/CTO: Spider web
- C-Level: Spider web and definition of targets

DSOMM

- Security: Assessment & Pre-Selection of targets
- Engineers/CTO: Discussion of how to implement
- All: Heatmap/number of planned/implemented activities

Strategic Approaches

- Top-to-Bottom
- Team Independency by Maturity
- Interactive with Teams

Approach: Top-to-Bottom

- Management Support
- SAMM to define targets with the management for the next 3-24 month
- DSOMM to define activities

Approach: Team Independency by Maturity

- Pre-Requirement: C-Level is convinced
- Definition of maturity levels for teams and their "independency"
  - Is a team allowed to roll out software on their own
  - Is a pentest required for each rollout
- Show maturity: Belts

Approach: Interactive with Teams

- Definition of targets with the team
- What is your plan for the next 6 month

Hint: Developers/Operations are not security people

-> explanation of each activity is time consuming

-> reduction of activities needed

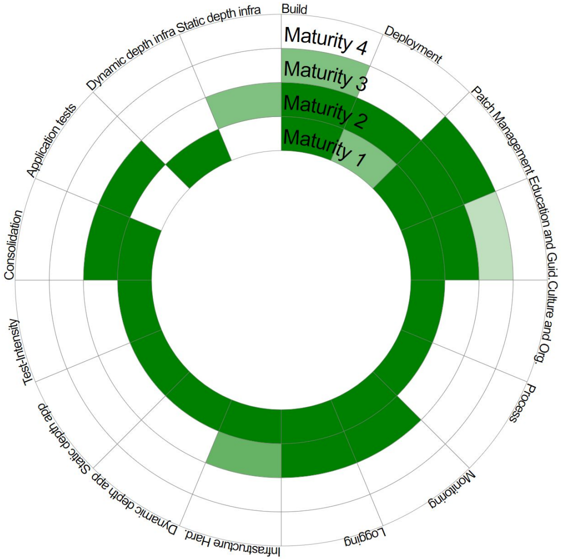
DSOMM Adoption

- DSOMM needs to be customized
- Remove/Add planned activities and present the targets to the teams from the *data/<dimension>yaml’s*

DSOMM Communication ACTUAL/TARGET

Spider Web Diagram with Heatmap

Start a container with customized on *selectedData.csv* (ro)



Requirements / Level 0

- Onboard Product Owner, Manager in Security
- Get to Know Security Policies
- Continuously Improve your Security Belt Rank
- Review Security Belt Activities
- Utilize Pairing when Starting an Activity

Based On: AppSecure-nrw White Belt, https://github.com/AppSecure-nrw/security-belts/tree/master/white

Agenda

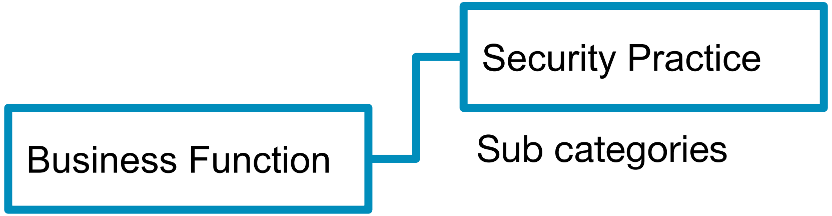
- Introduction/Motivation
- High Level Approaches
- Usage
- Conclusion

SAMM Structure

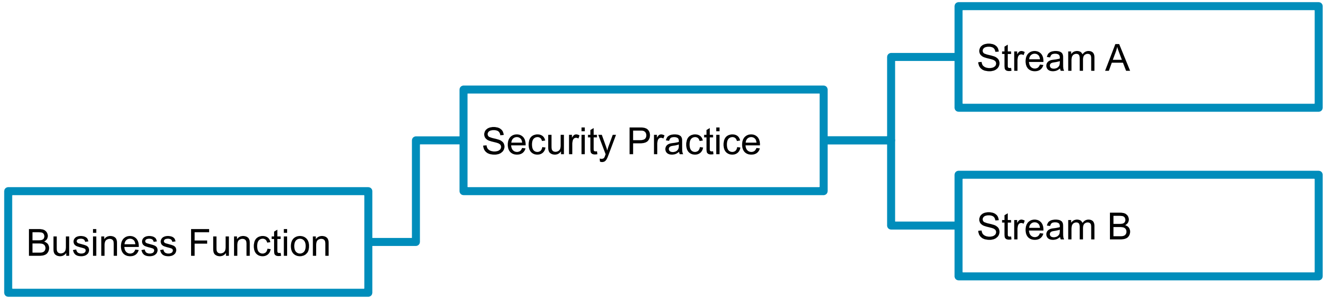
Business Function

Category of activities

SAMM Structure

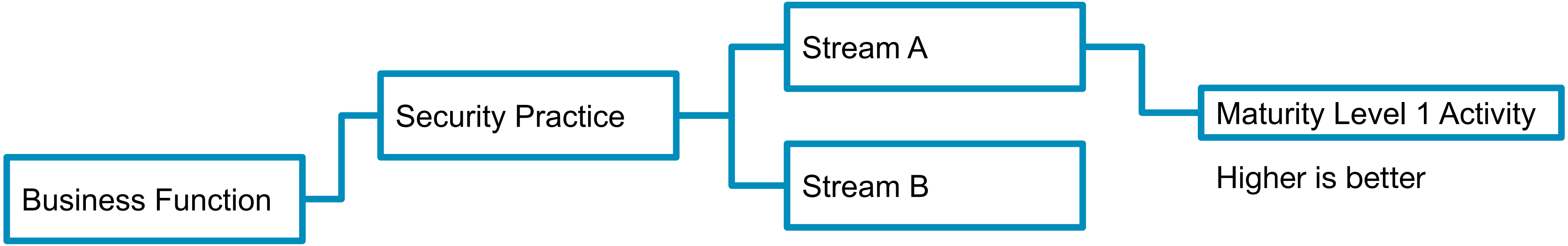


SAMM Structure



Logical flows and divided into two streams

SAMM Structure



Business Function

Security Practice

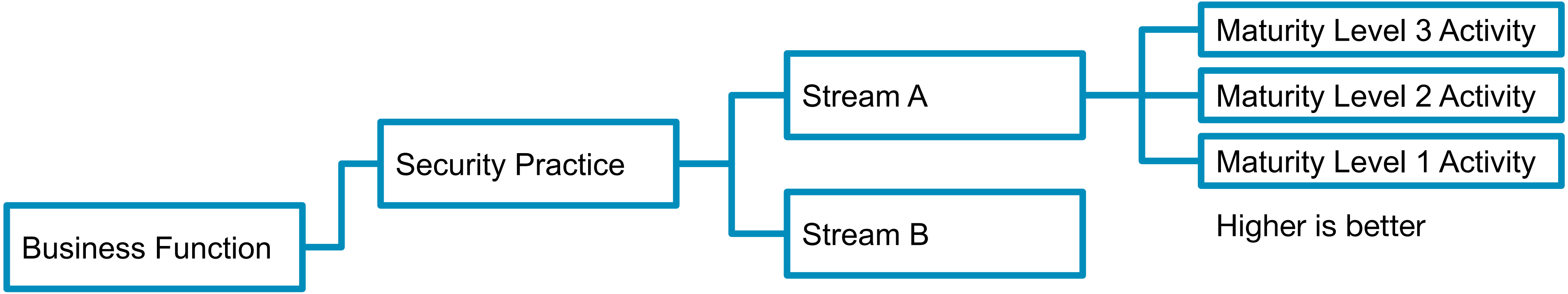
Stream A

Stream B

Maturity Level 1 Activity

Higher is better

SAMM Structure


Business Function

Security Practice

Stream A

Stream B

Maturity Level 3 Activity

Maturity Level 2 Activity

Maturity Level 1 Activity

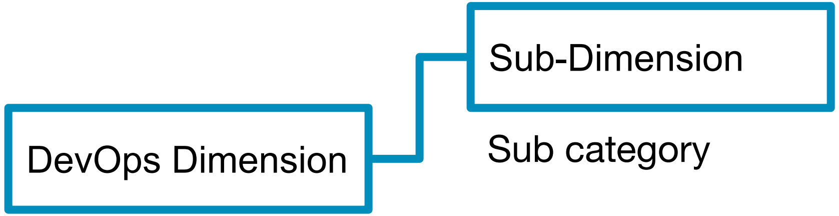
Higher is better

DSOMM Structure

DevOps Dimension

Category

DSOMM Structure

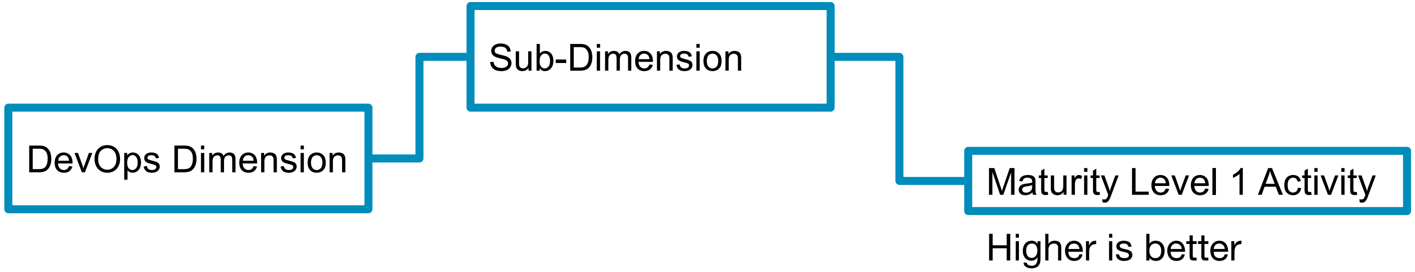


DevOps Dimension

Sub-Dimension

Sub category

DSOMM Structure



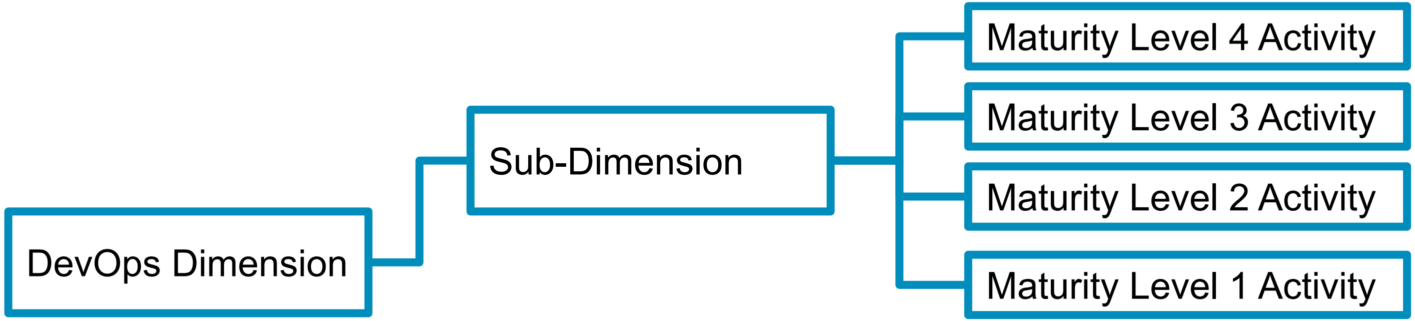
DevOps Dimension

Sub-Dimension

Maturity Level 1 Activity

Higher is better

DSOMM Structure



DevOps Dimension

Sub-Dimension

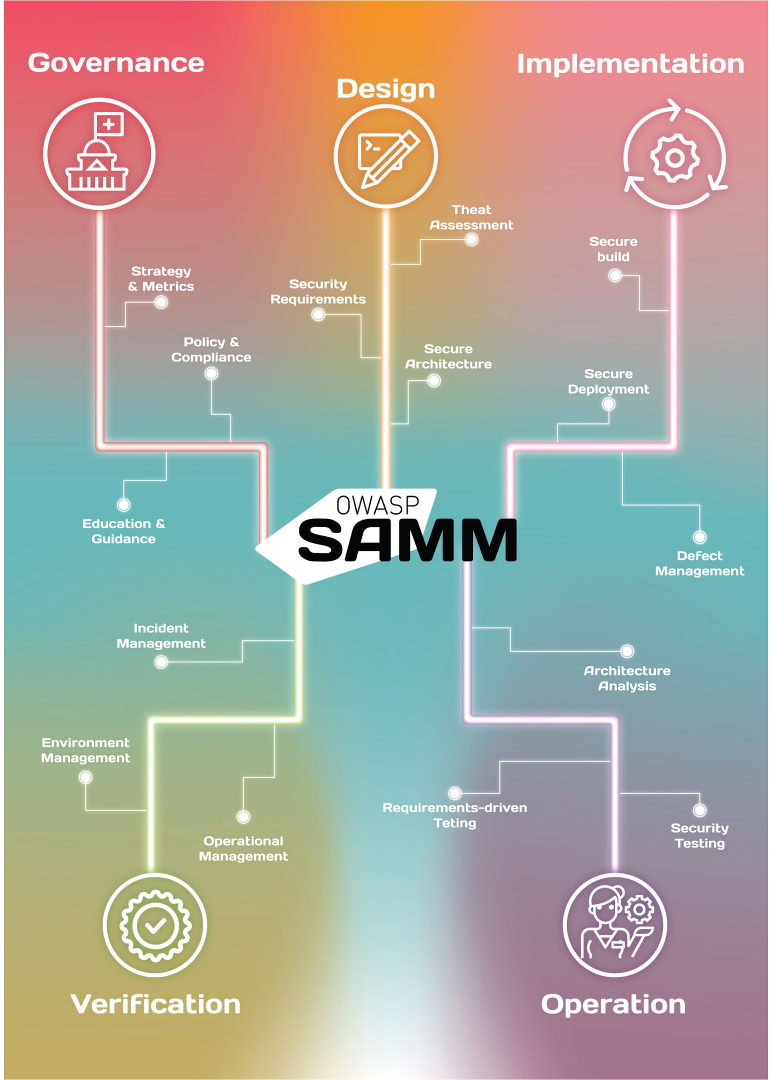
Maturity Level 4 Activity

Maturity Level 3 Activity

Maturity Level 2 Activity

Maturity Level 1 Activity

Higher is better



Governance

Strategy & Metrics

Policy & Compliance

Education & Guidance

Design

Theat Assessment

Security Requirements

Secure Architecture

Implementation

Secure build

Secure Deployment

Defect Management

OWASP SAMM

Incident Management

Environment Management

Operational Management

Verification

Architecture Analysis

Requirements-driven Teting

Security Testing

Operation

DevSecOps Dimensions

Build and Deployment

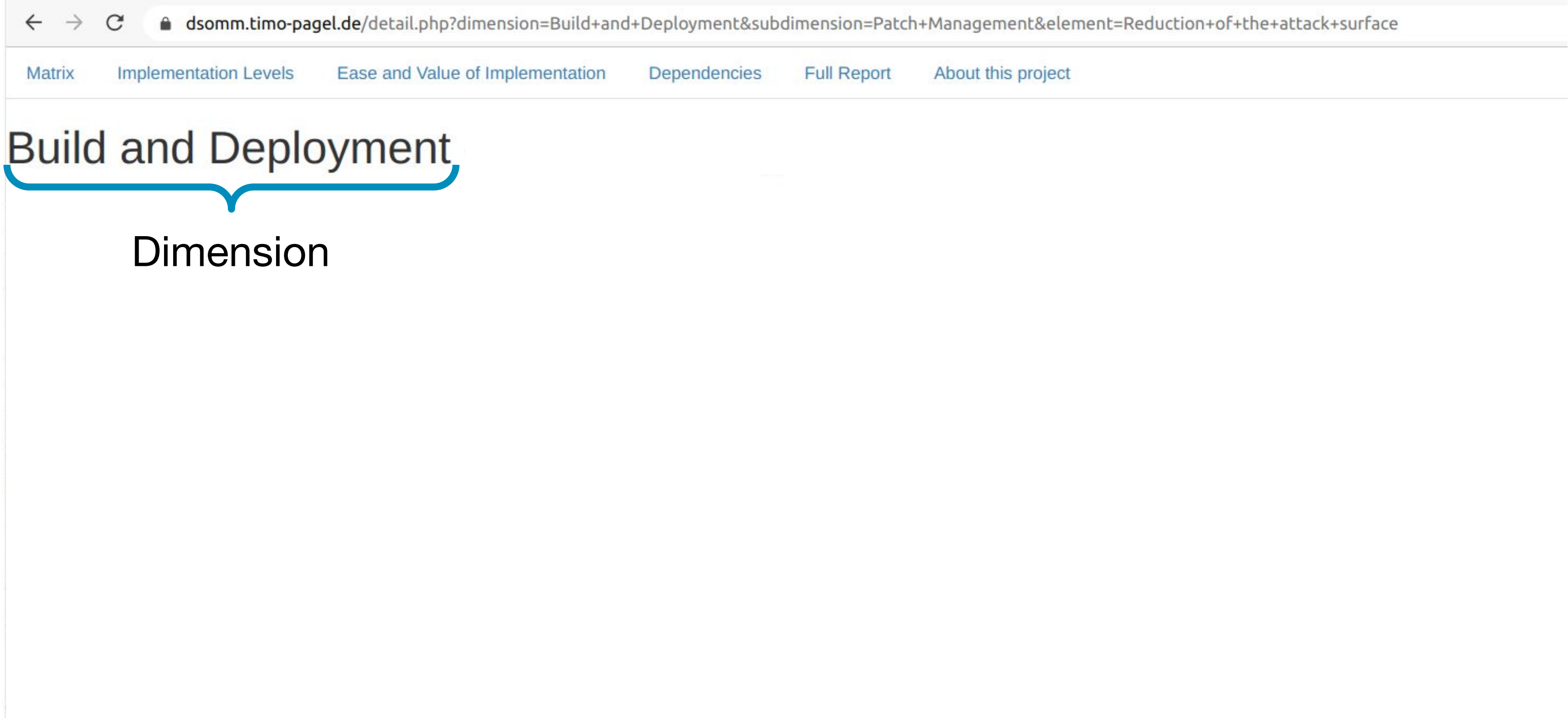
Culture and Organisation

Information Gathering

Hardening

Test and Verification

Build and Deployment: Example Reduction of the attack surface

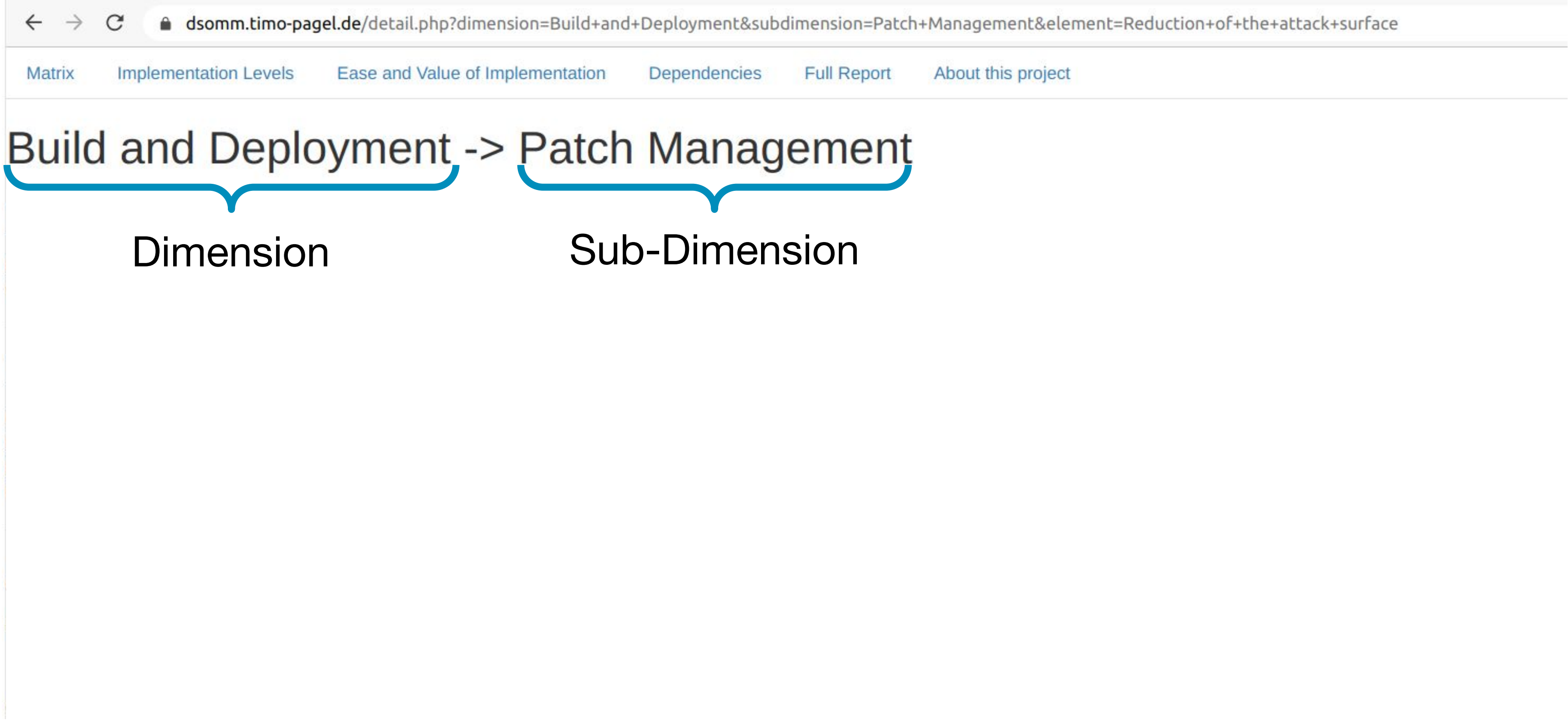


dsomm.timo-pagel.de/detail.php?dimension=Build+and+Deployment&subdimension=Patch+Management&element=Reduction+of+the+attack+surface

Build and Deployment

Dimension

Build and Deployment:
Example Reduction of the attack surface



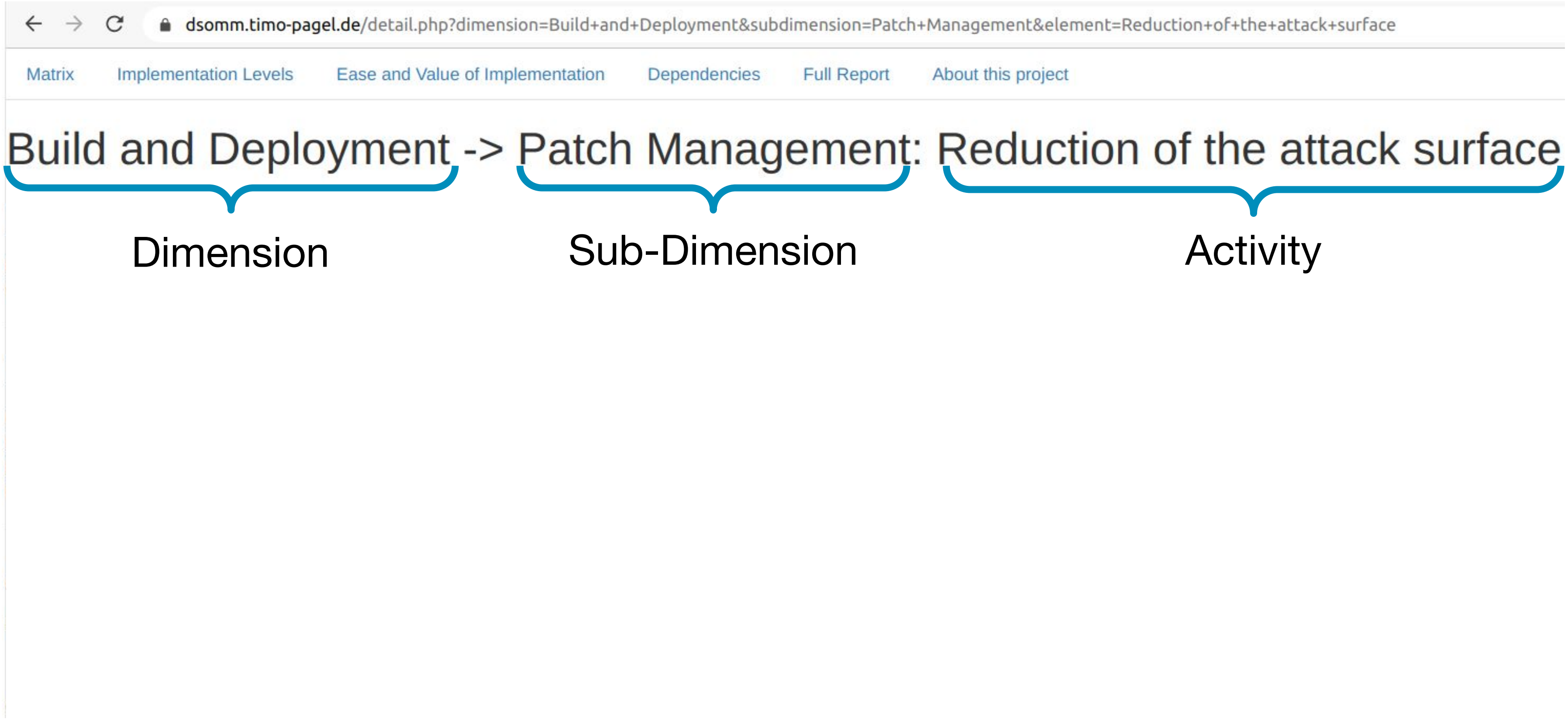
dsomm.timo-pagel.de/detail.php?dimension=Build+and+Deployment&subdimension=Patch+Management&element=Reduction+of+the+attack+surface

Build and Deployment -> Patch Management

Dimension

Sub-Dimension

Build and Deployment: Example Reduction of the attack surface



dsomm.timo-pagel.de/detail.php?dimension=Build+and+Deployment&subdimension=Patch+Management&element=Reduction+of+the+attack+surface

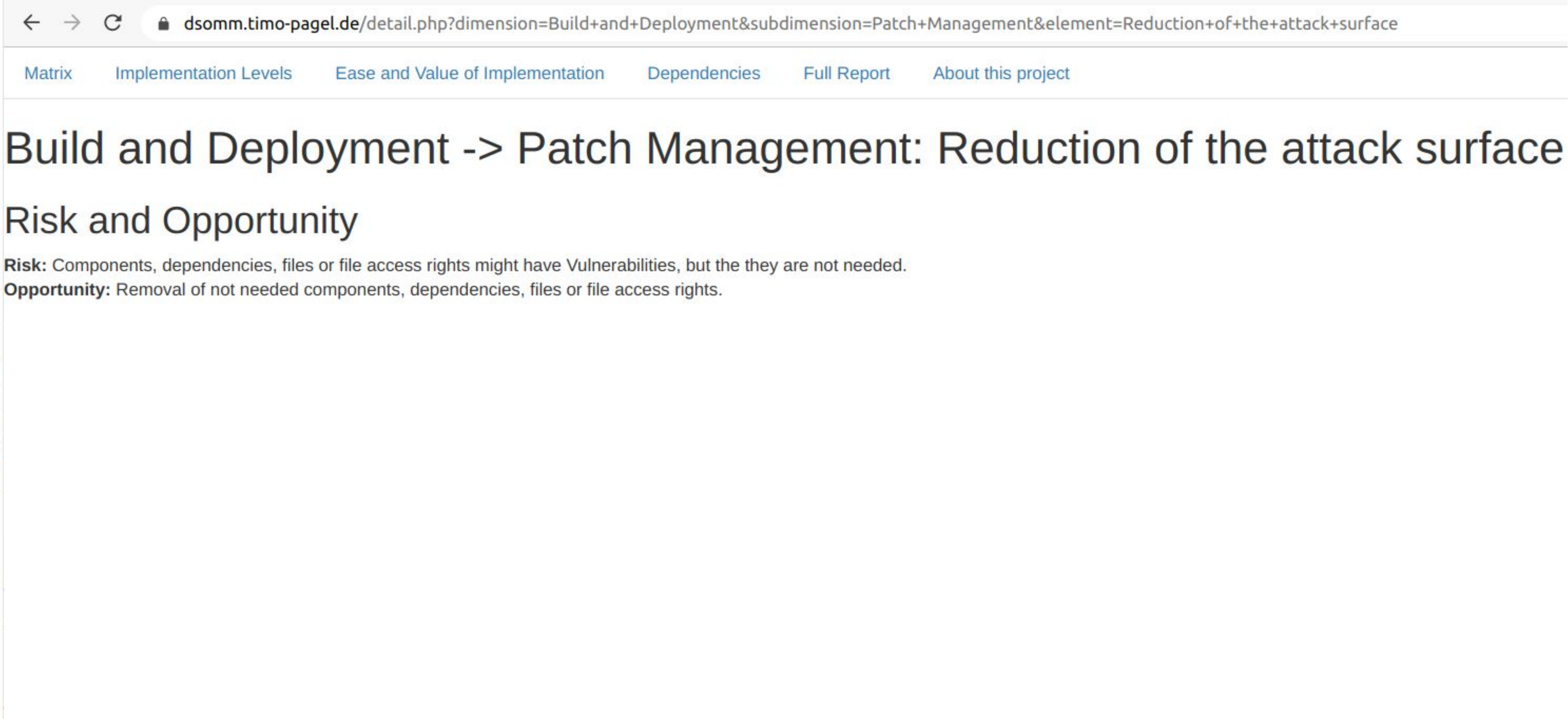
Build and Deployment -> Patch Management: Reduction of the attack surface

Dimension

Sub-Dimension

Activity

Build and Deployment:
Example Reduction of the attack surface



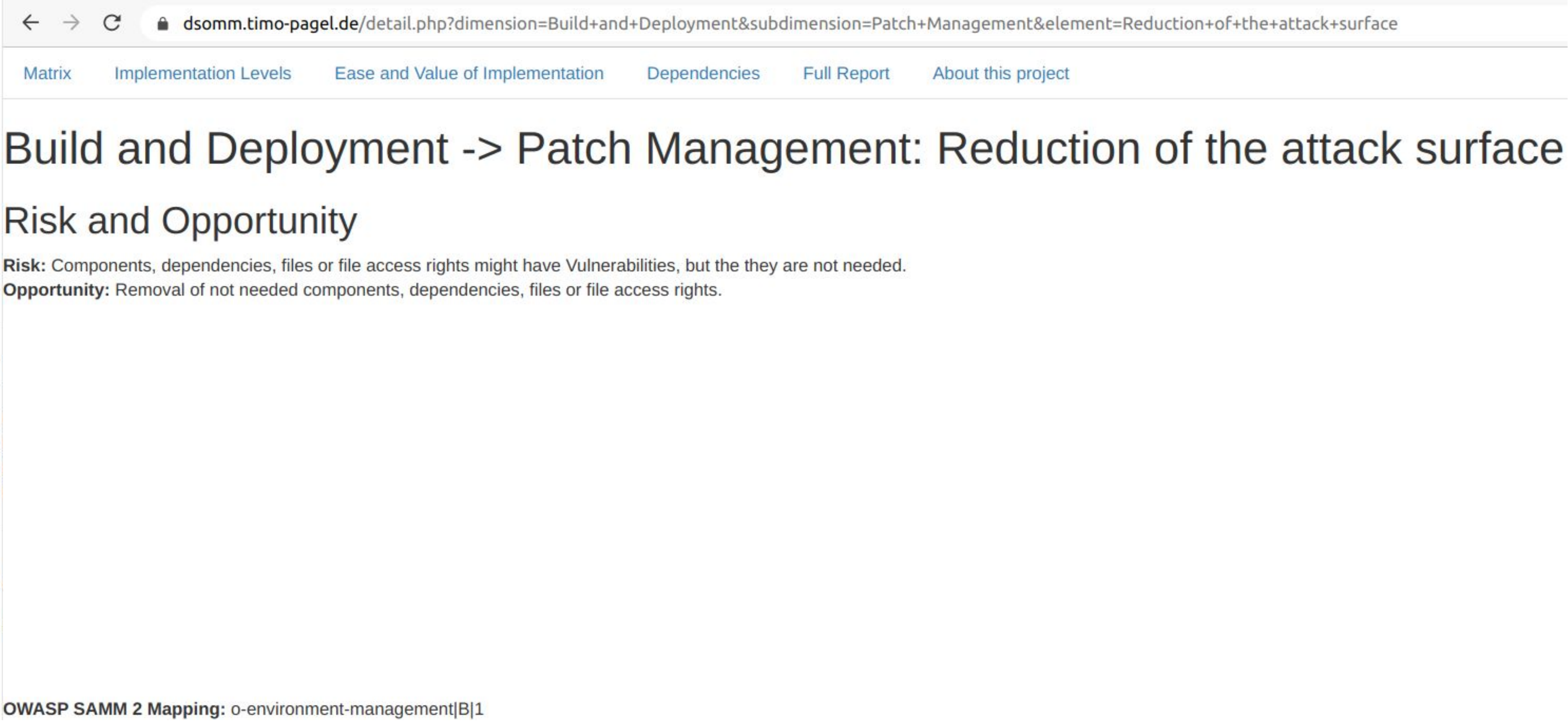
dsomm.timo-pagel.de/detail.php?dimension=Build+and+Deployment&subdimension=Patch+Management&element=Reduction+of+the+attack+surface
Matrix
Implementation Levels
Ease and Value of Implementation
Dependencies
Full Report
About this project

Build and Deployment -> Patch Management: Reduction of the attack surface

Risk and Opportunity

Risk: Components, dependencies, files or file access rights might have Vulnerabilities, but the they are not needed.
Opportunity: Removal of not needed components, dependencies, files or file access rights.

Build and Deployment:
Example Reduction of the attack surface



dsomm.timo-pagel.de/detail.php?dimension=Build+and+Deployment&subdimension=Patch+Management&element=Reduction+of+the+attack+surface
Matrix
Implementation Levels
Ease and Value of Implementation
Dependencies
Full Report
About this project

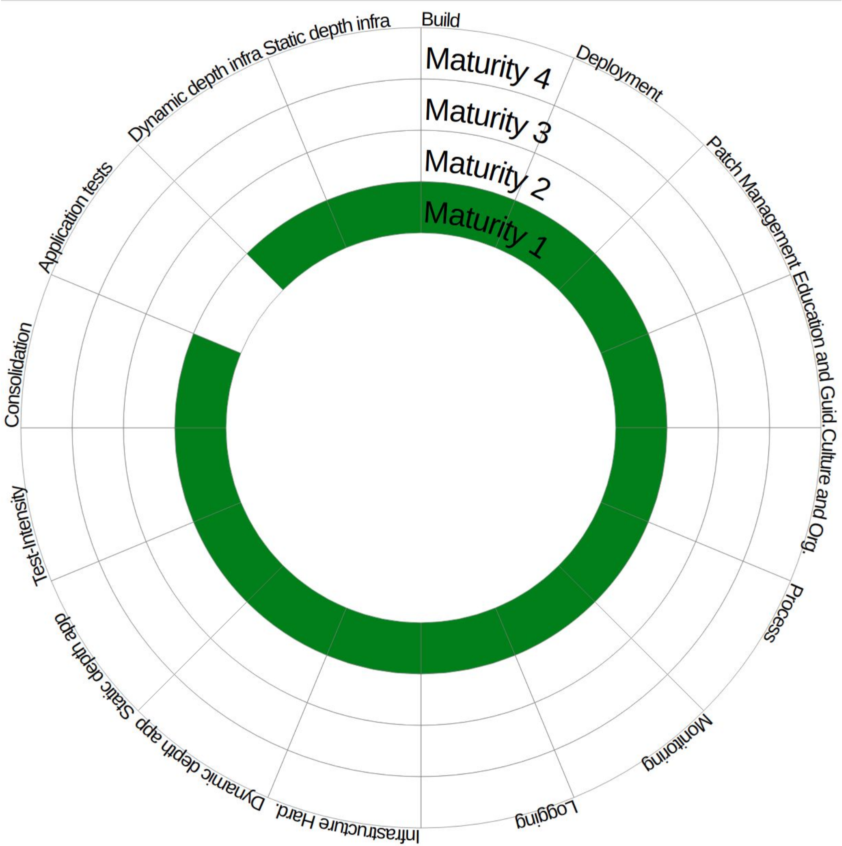
Build and Deployment -> Patch Management: Reduction of the attack surface

Risk and Opportunity

Risk: Components, dependencies, files or file access rights might have Vulnerabilities, but the they are not needed.
Opportunity: Removal of not needed components, dependencies, files or file access rights.

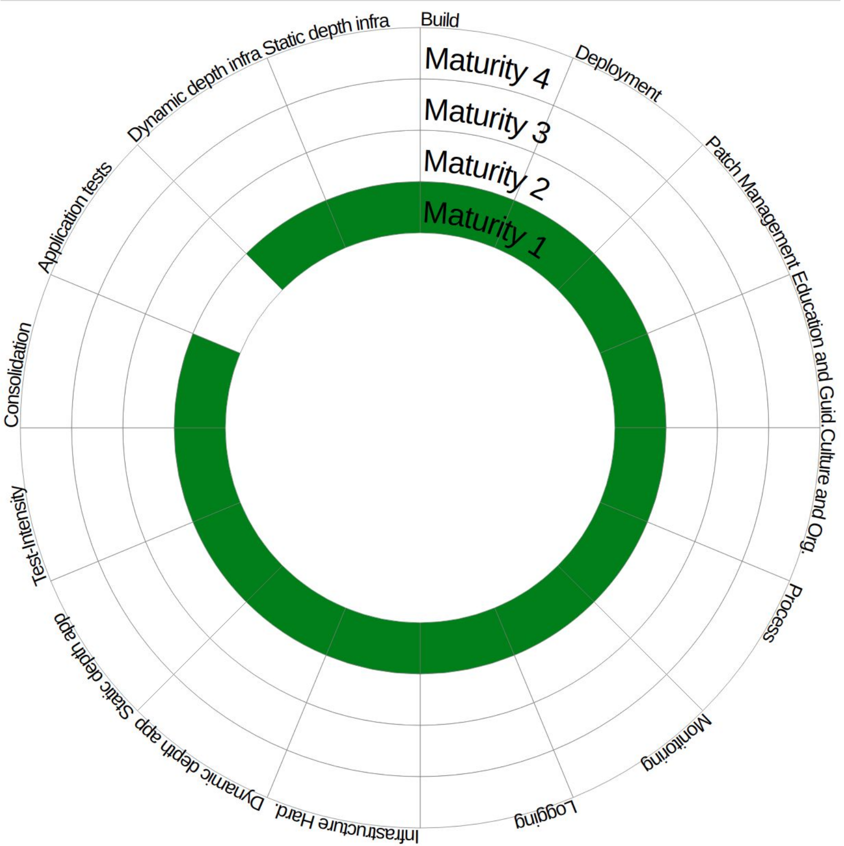
OWASP SAMM 2 Mapping: o-environment-management|B|1

Maturity Levels



Maturity Levels

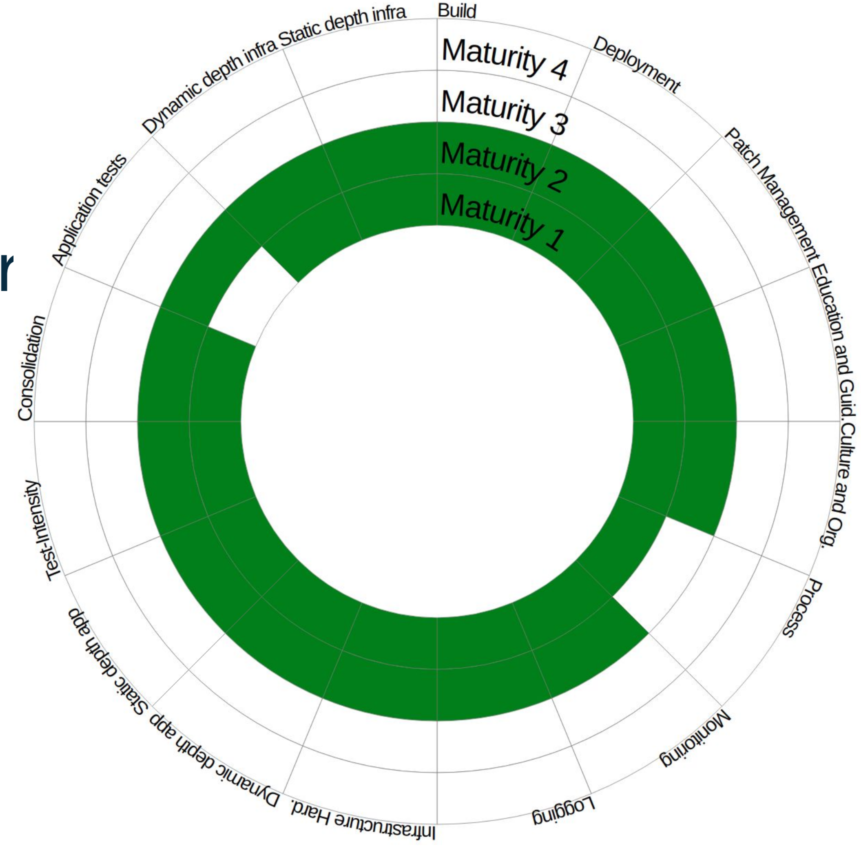
Level 1: Basic understanding of security practices



Maturity Levels

Level 1: Basic understanding of security practices

Level 2: Adoption of basic secur practices

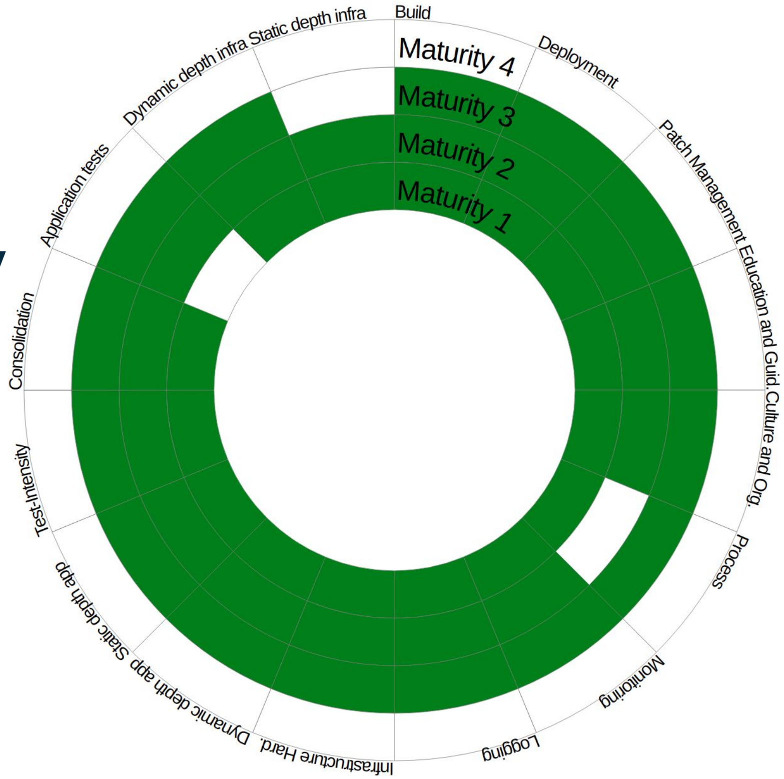


Maturity Levels

Level 1: Basic understanding of security practices

Level 2: Adoption of basic security practices

Level 3: High adoption of security practices



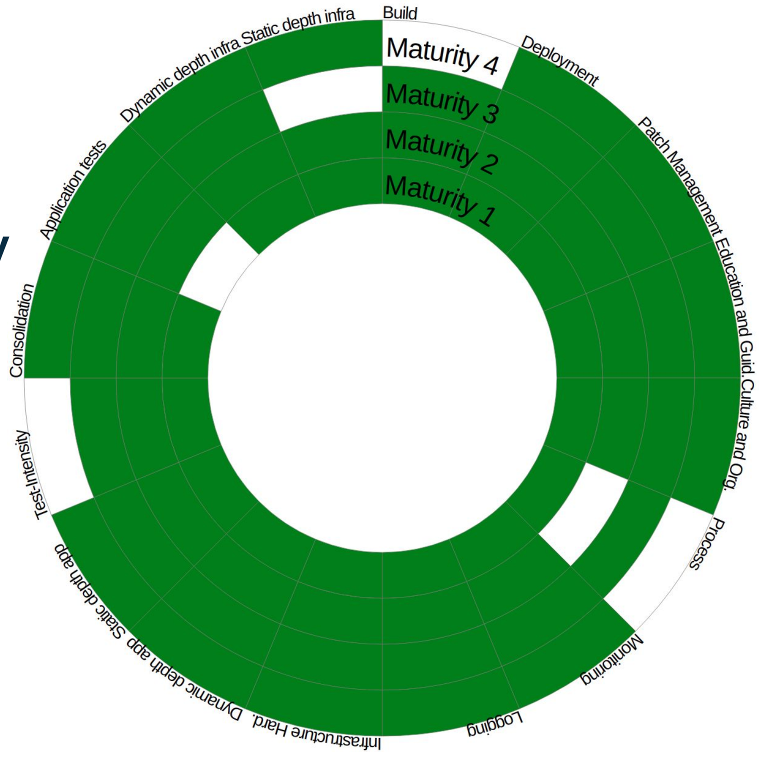
Maturity Levels

Level 1: Basic understanding of security practices

Level 2: Adoption of basic security practices

Level 3: High adoption of security practices

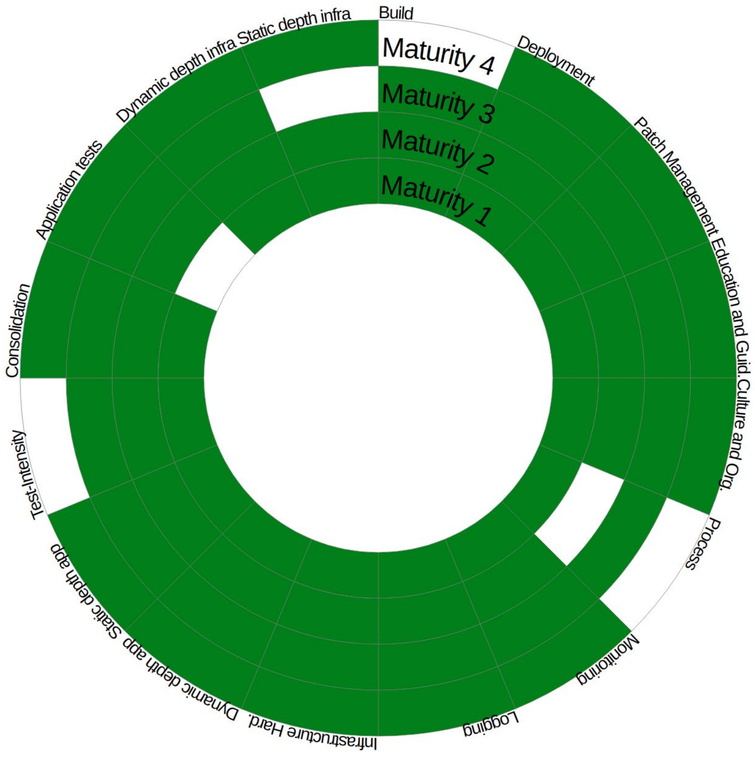
Level 4: Advanced deployment of security practices at scale



White Spots

Activities where important

-> No Activity



Implementation | Secure Build | Build Process

Level 1:

Determine a value for each generated artifact that can be later used to verify its integrity [...]

Level 2:

The automated process [...] code signing certificate or access to repositories.

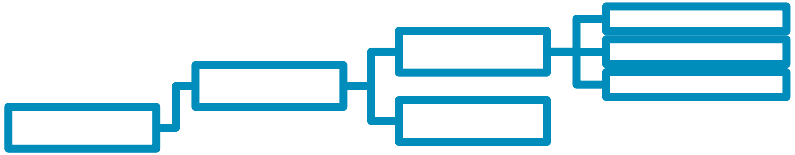
DSOMM and SAMM Structure in Detail

SAMM

Made for management, very *schematic*

Always follows the scheme

No empty levels

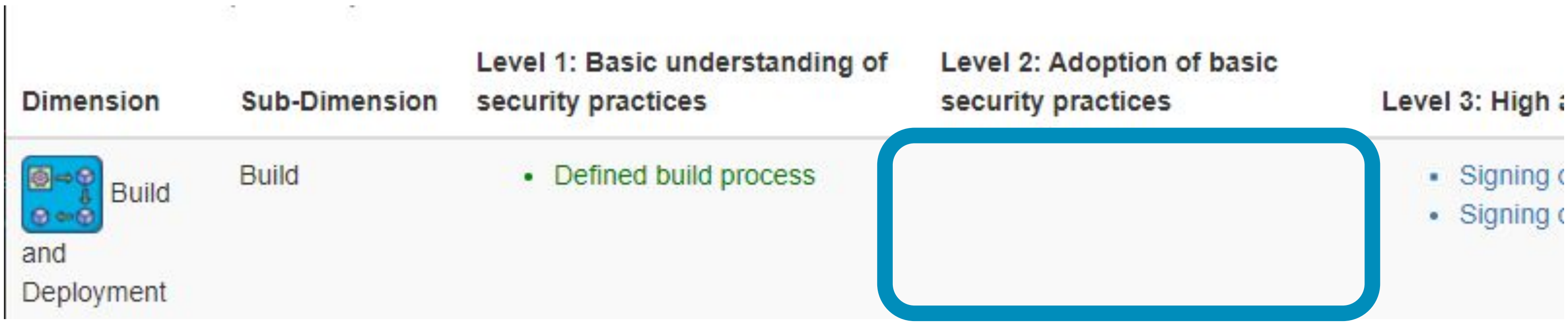


Verification | Security Testing

Implementation | Defect Management

DSOMM and SAMM Structure in Detail

DSOMM



Dimension	Sub-Dimension	Level 1: Basic understanding of security practices	Level 2: Adoption of basic security practices	Level 3: High
Build and Deployment	Build	• Defined build process		• Signing • Signing

Missing In DSOMM

```
+-------+----------+--------------+--------------------------+----------+-------------------------------------------+
| index | id       | function     | practice                 | maturity | stream                                    |
+-------+----------+--------------+--------------------------+----------+-------------------------------------------+
|    36 | G-PC-1-A | Governance   | Policy & Compliance      | 1        | Policy & Standards                        |
|    44 | G-PC-1-B | Governance   | Policy & Compliance      | 1        | Compliance Management                     |
|    31 | G-PC-2-A | Governance   | Policy & Compliance      | 2        | Policy & Standards                        |
|    33 | G-PC-2-B | Governance   | Policy & Compliance      | 2        | Compliance Management                     |
|    24 | G-PC-3-A | Governance   | Policy & Compliance      | 3        | Policy & Standards                        |
|    67 | G-PC-3-B | Governance   | Policy & Compliance      | 3        | Compliance Management                     |
|     9 | O-OM-1-A | Operations   | Operational Management   | 1        | Data Protection                           |
|     2 | O-OM-1-B | Operations   | Operational Management   | 1        | System Decomissioning / Legacy Management |
|    63 | O-OM-2-A | Operations   | Operational Management   | 2        | Data Protection                           |
|    19 | O-OM-2-B | Operations   | Operational Management   | 2        | System Decomissioning / Legacy Management |
|    41 | O-OM-3-A | Operations   | Operational Management   | 3        | Data Protection                           |
|    68 | O-OM-3-B | Operations   | Operational Management   | 3        | System Decomissioning / Legacy Management |
[...]
```

Based on dsomm-orm https://github.com/ioggstream/dsomm-orm/blob/main/mysql-queries.yaml from Roberto Polli

Comparison of Models

Count in DSOMM	**SAMM Governance**	**SAMM Design**	**SAMM Implementation**	**SAMM Verification**	**SAMM Operations**
SAMM 1	0	3	8	12	32
SAMM 2	0	0	12	24	11
SAMM 3	0	0	1	5	1

Based on dsomm-orm https://github.com/ioggstream/dsomm-orm/blob/main/mysql-queries.yaml from Roberto Polli

Comparison of Models

Count/ Level	**D-TA***	**I-DM***	**I-SB***	**I-SD***	**O-EM***	**O-IM***	**O-SR***	**V-ST***	**G***
1	3	3	2	3	23	8	1	12	0
2	0	7	2	3	0	10	1	24	0
3	0	0	1	0	0	0	1	5	0

Based on dsomm-orm https://github.com/ioggstream/dsomm-orm/blob/main/mysql-queries.yaml from Roberto Polli

Analysis of Models

Count in DSOMM	**SAMM Governance**	**SAMM Design**	**SAMM Implementation**	**SAMM Verification**	**SAMM Operations**
SAMM 1	0	3	8	12	32
SAMM 2	0	0	12	24	11
SAMM 3	0	0	1	5	1

Based on dsomm-orm https://github.com/ioggstream/dsomm-orm/blob/main/mysql-queries.yaml from Roberto Polli

Analysis Operations | Environment Management | Patching and Updating

- DSOMM needs to align level 1/2
- SAMM Level 3:

Develop and use management dashboards/reports to track compliance with patching processes and SLAs [...]

-> DSOMM Information Gathering

How Deep?

- SAMM: *Perform best-effort hardening of configurations, based on readily available information.*

How Deep?

- SAMM: *Perform best-effort hardening of configurations, based on readily available information.*

- Removal of not needed components, dependencies, files or file access rights.

  Implementation hint: Distroless, Fedora CoreOS

How Deep?

- SAMM: *Perform best-effort hardening of configurations, based on readily available information.*

- Removal of not needed components, dependencies, files or file access rights.

  Implementation hint: Distroless, Fedora CoreOS

- Usage of distroless images and a small operating system

How Deep?

- SAMM: *Perform best-effort hardening of configurations, based on readily available information.*

- Removal of not needed components, dependencies, files or file access rights.

  Implementation hint: Distroless, Fedora CoreOS

- Usage of distroless images and a small operating system

Agenda

- Introduction/Motivation
- High Level Approaches
- Detailed Usage
- Conclusion and Outlook

Conclusion

- Assess and plan security strategy (with SAMM)
- Adapt DSOMM
- DSOMM might be 80% of your secure DevOps strategy

Next Steps, be involved!

- Better OWASP SAMM mapping visualization
- More and optimized activities
- DevSecOps Toolchain Categorization

Pull Requests with suggestions are welcome

Thank you
Questions?

SAMM https://owaspsamm.org

DSOMM https://dsomm.timo-pagel.de

timo.pagel@owasp.org
sammdsomm@pagel.pro