Usage of the OWASP DevSecOps Maturity Model

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 *University of Applied Sciences Wedel*

About Me

- DevSecOps Consultant
- Lecturer for *Security in Web Applications* at *University of Applied Sciences Wedel*
- Open Source / Open Knowledge Enthusiast

OWASP DevSecOps Maturity Model

OWASP Juice Shop

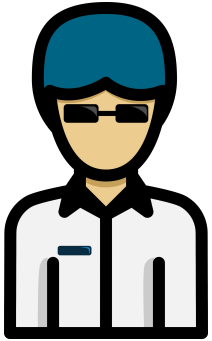
OWASP Security Pins

OWASP DefectDojo

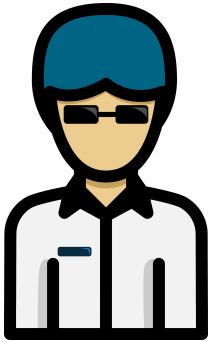
SAMM OWASP Software Assurance Maturity Model

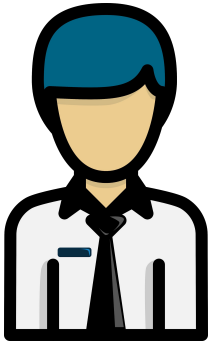
Target Audience

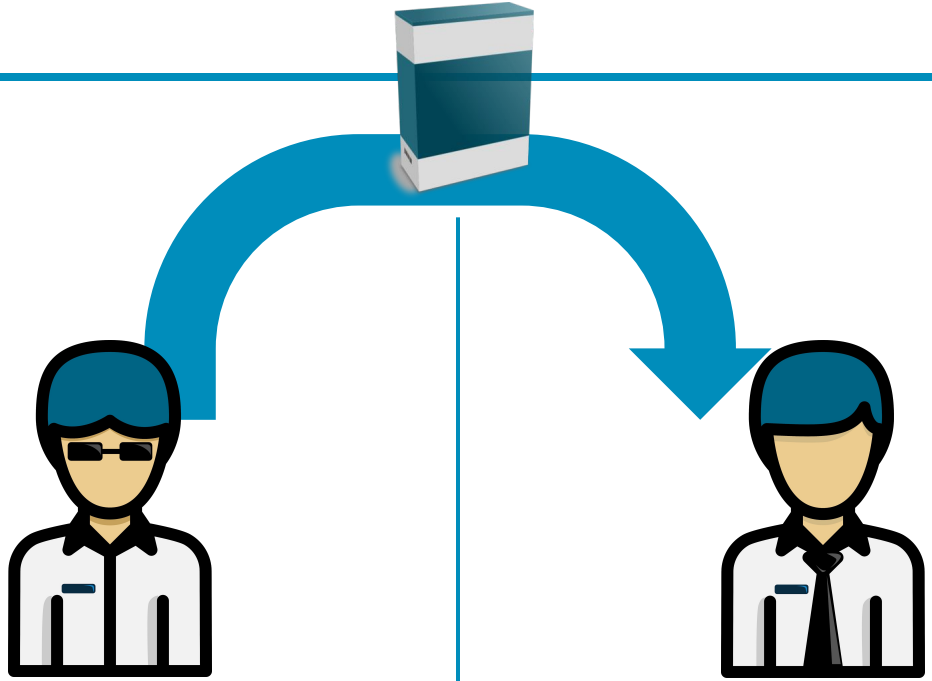
- Security People (Information- and Technical Security)
- Technical Upper Management (CTO)
- Enthusiastic Developers, Operator, C-Level

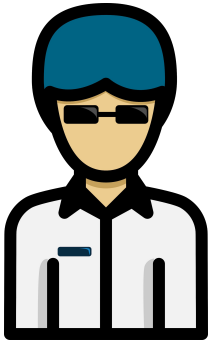


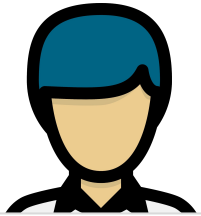
Wall of Irritation



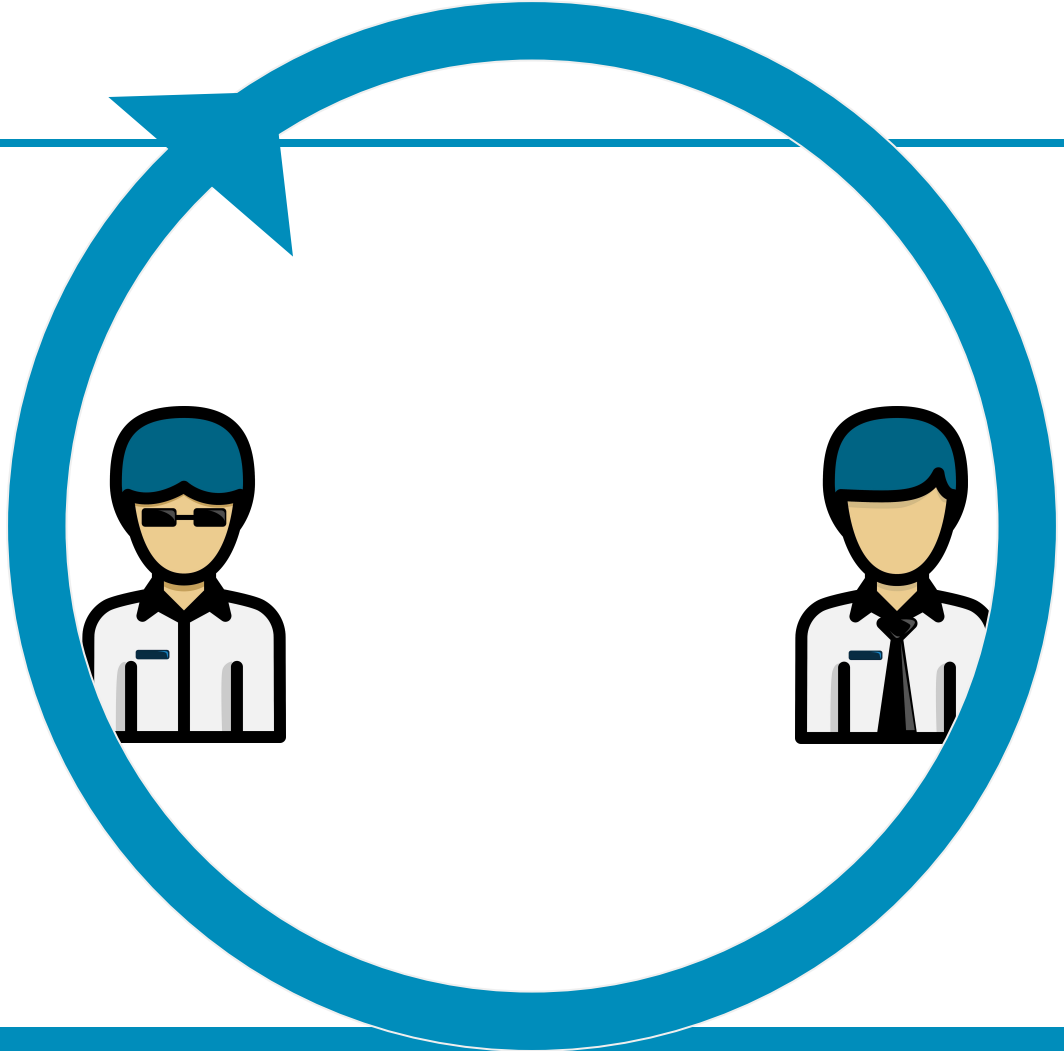




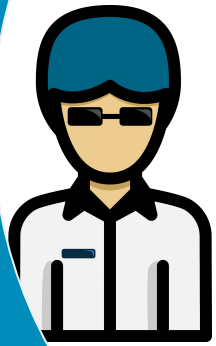


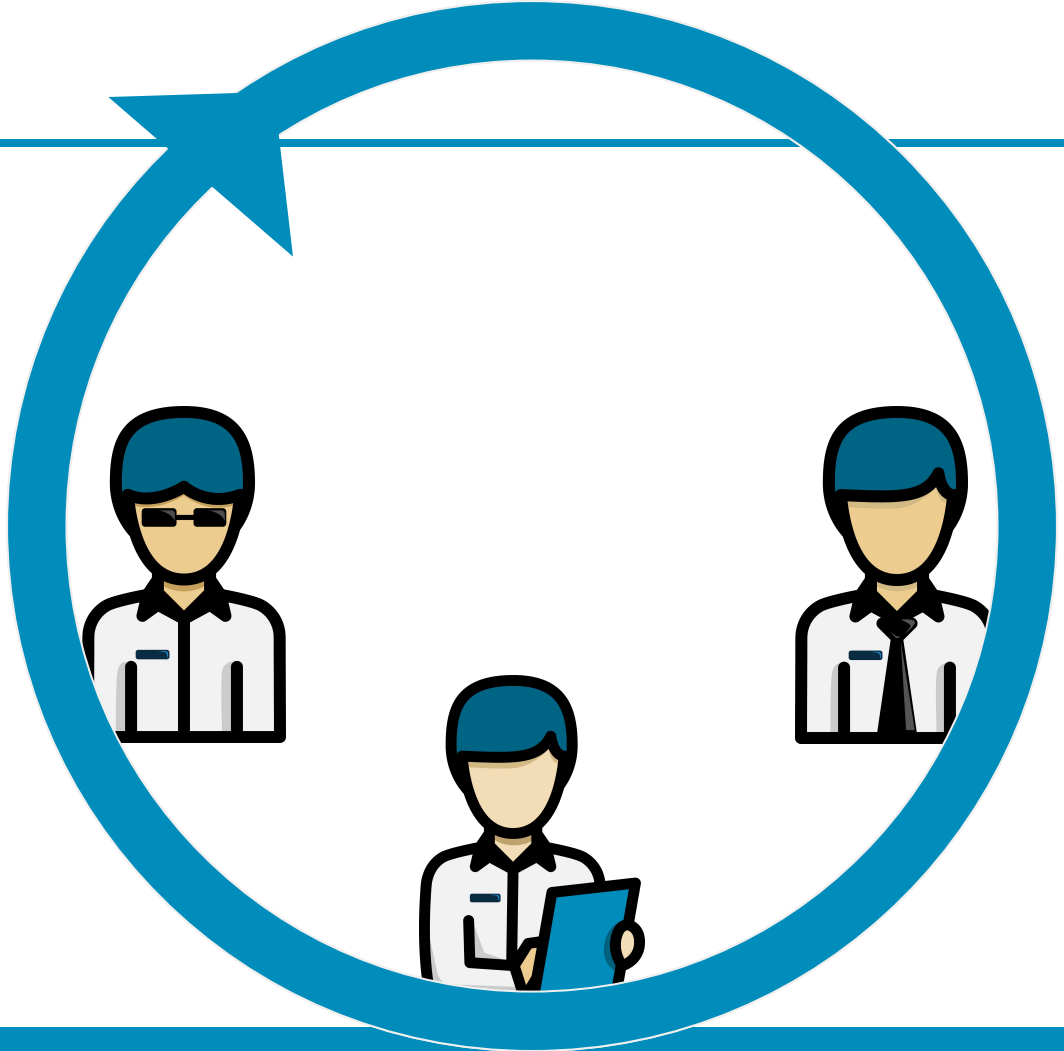



Sardonic Server
@sadserver
"Goddamn developers not testing their changes" he said while sudoing to root in production.
RETWEETS
376
LIKES
343

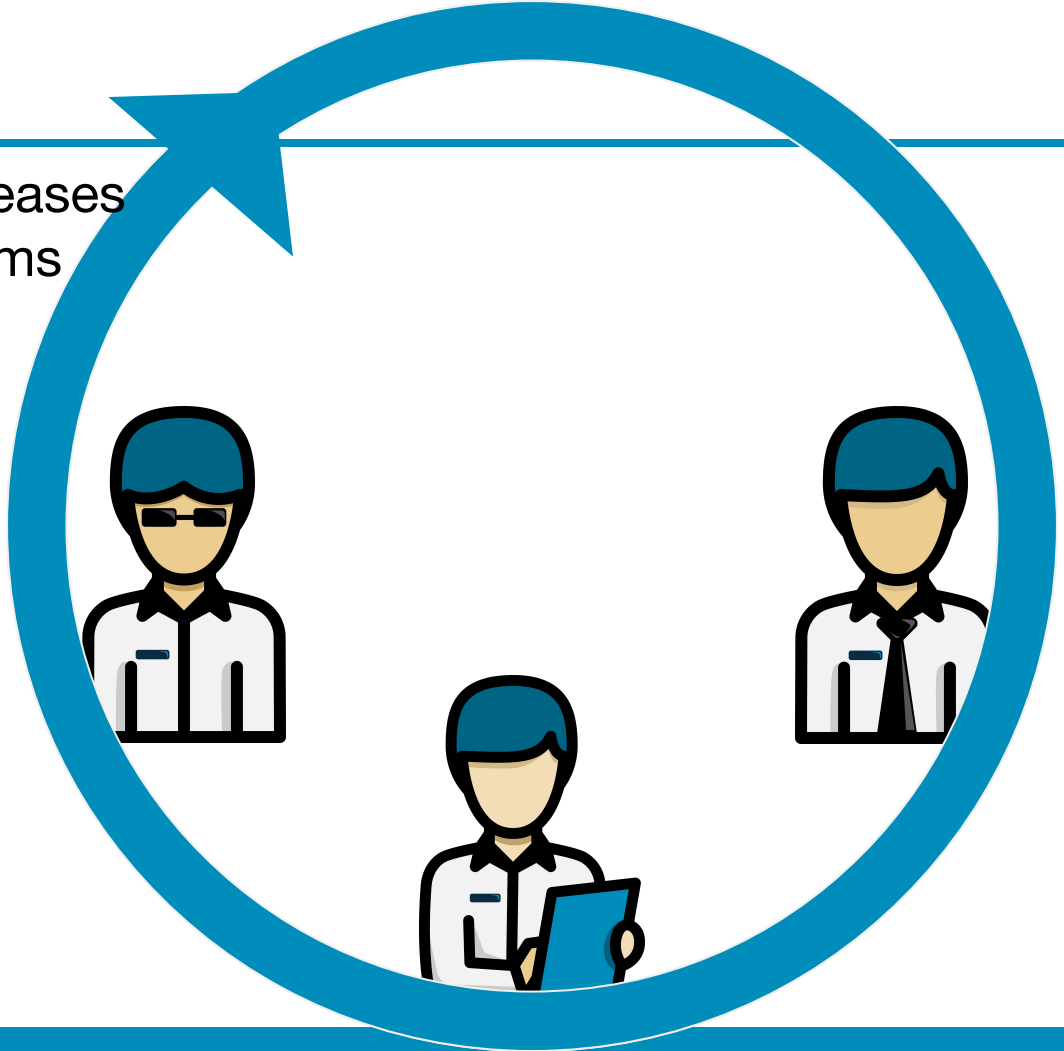


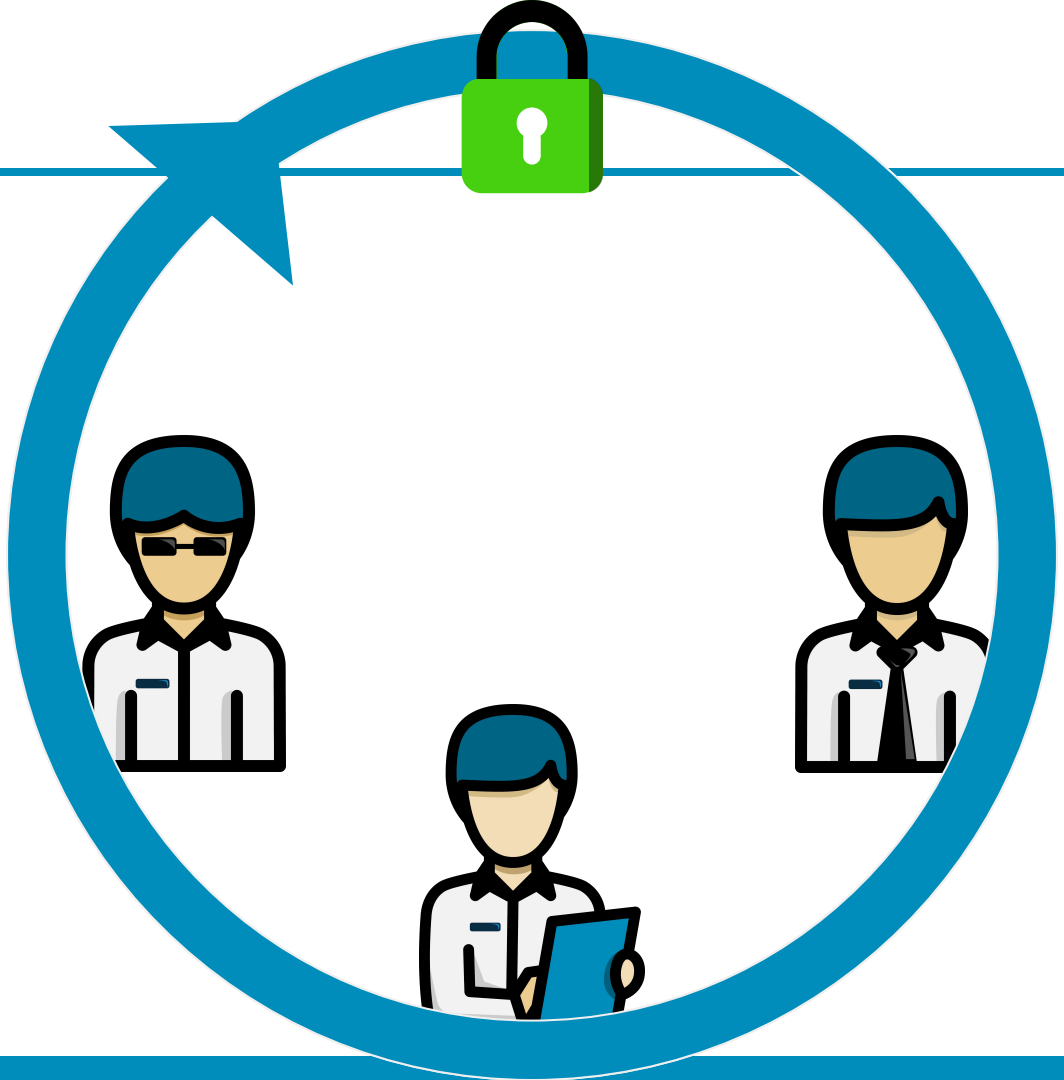
What about quality when deploy automatically multiple times a day?





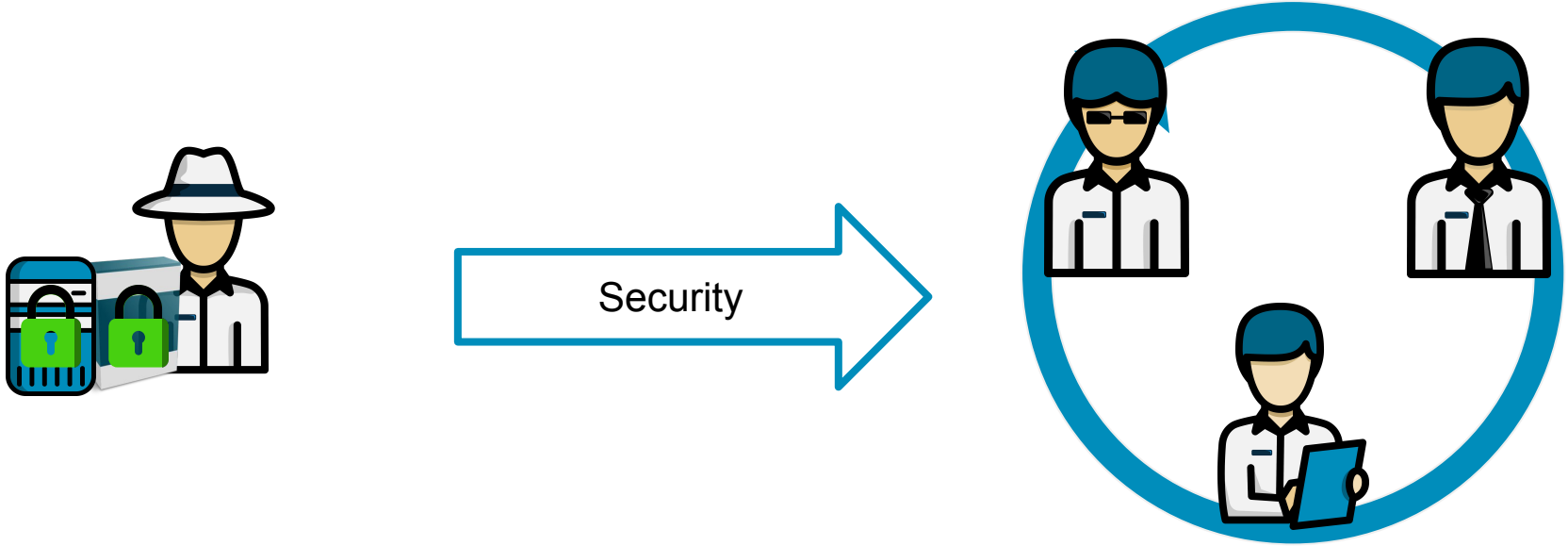
Speed / Fast Releases
Independent Teams
Different Skills
Automation





Problem Statement

- How to enhance security?



Problem Statement

- How to enhance security?
  - In DevOps-Strategies

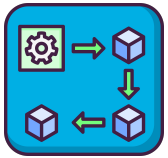
Problem Statement

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

Problem Statement

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

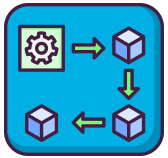
DevOps Dimensions



Build and Deployment

Culture and Organisation

DevOps Dimensions



Build and Deployment

Culture and Organisation

Information Gathering

Infrastructure

Test and Verification

Agenda

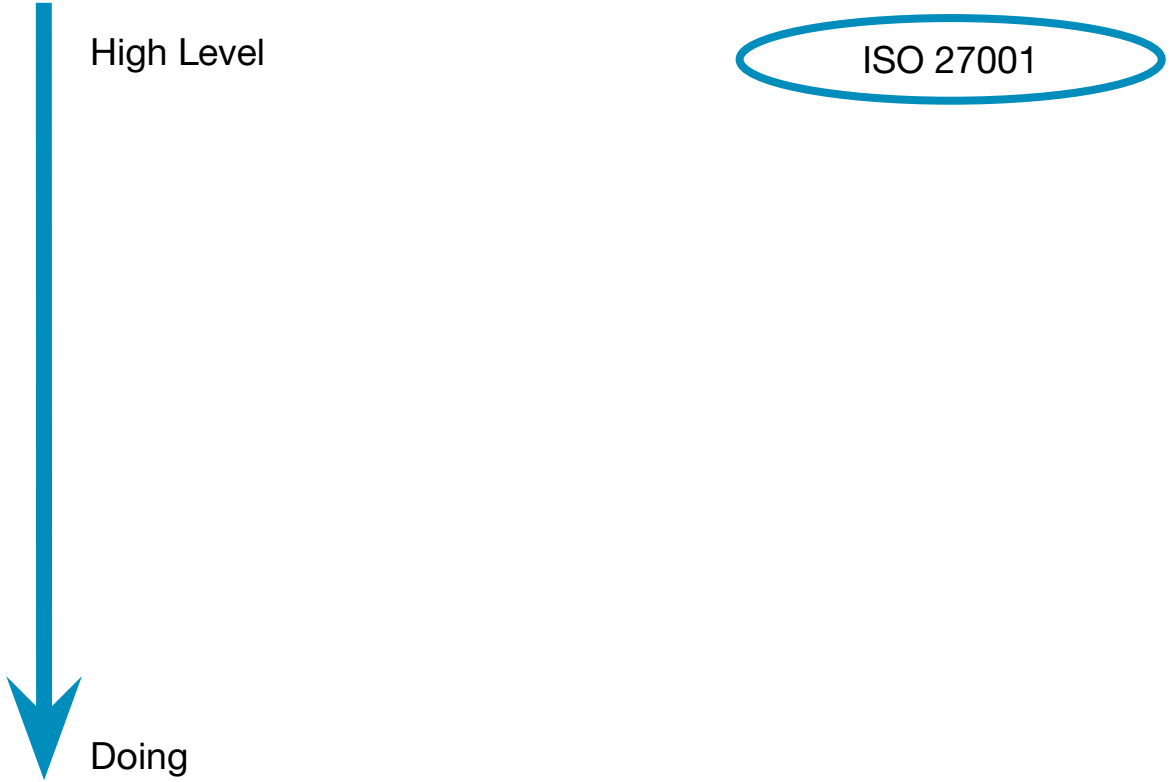
- Introduction/Motivation
- High Level Approaches
- Detailed Usage
- Conclusion

Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM

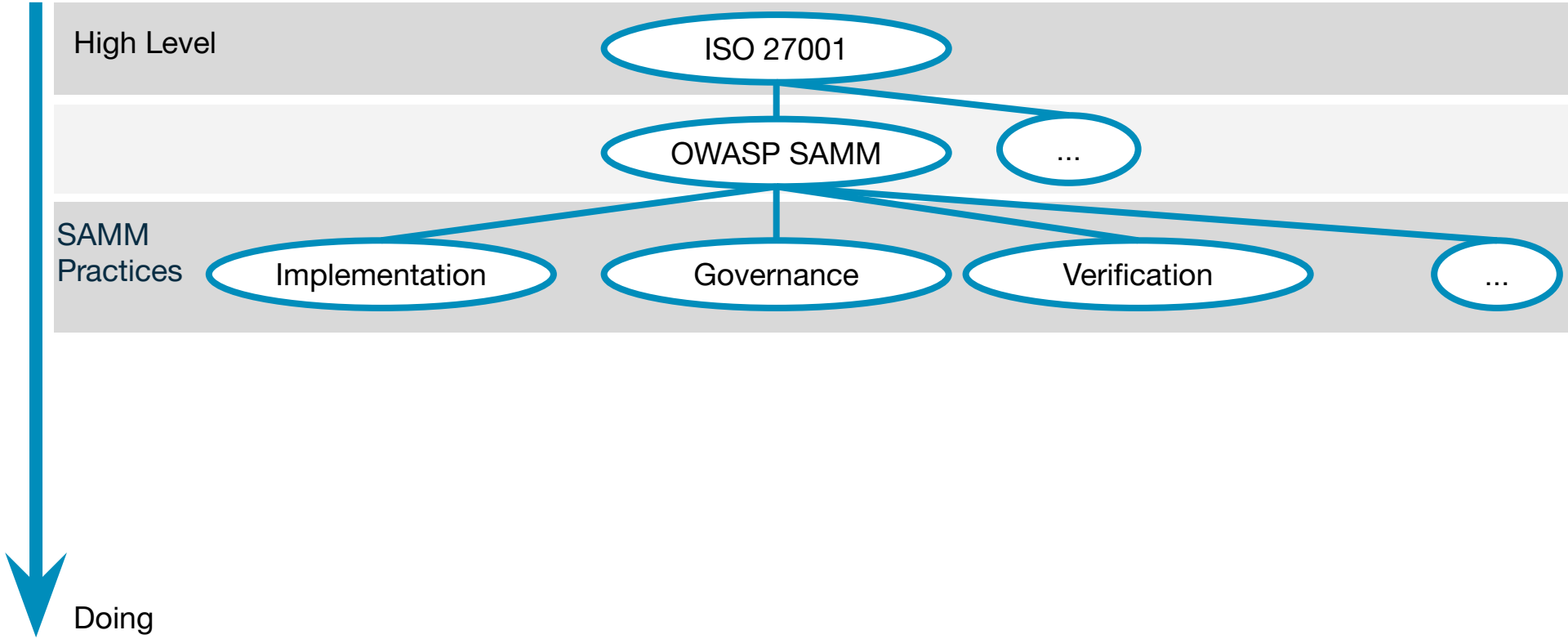
High Level

Doing

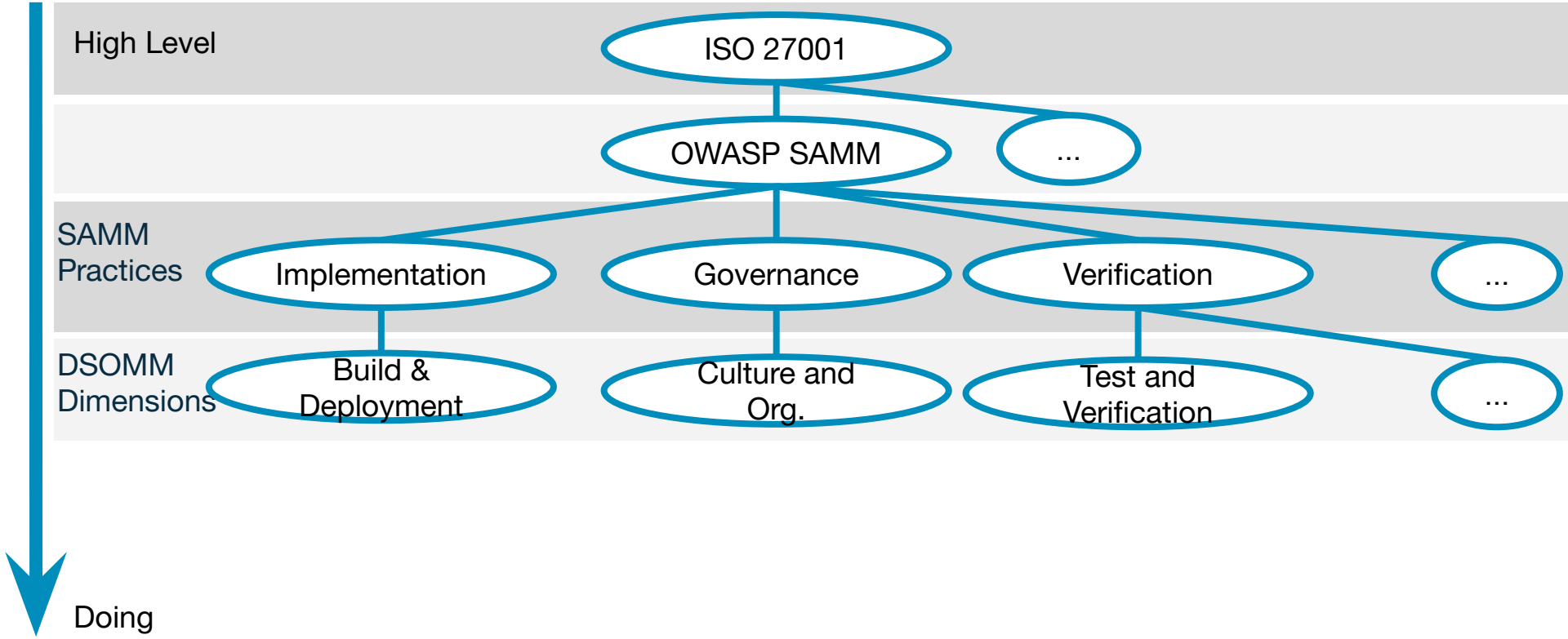
Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



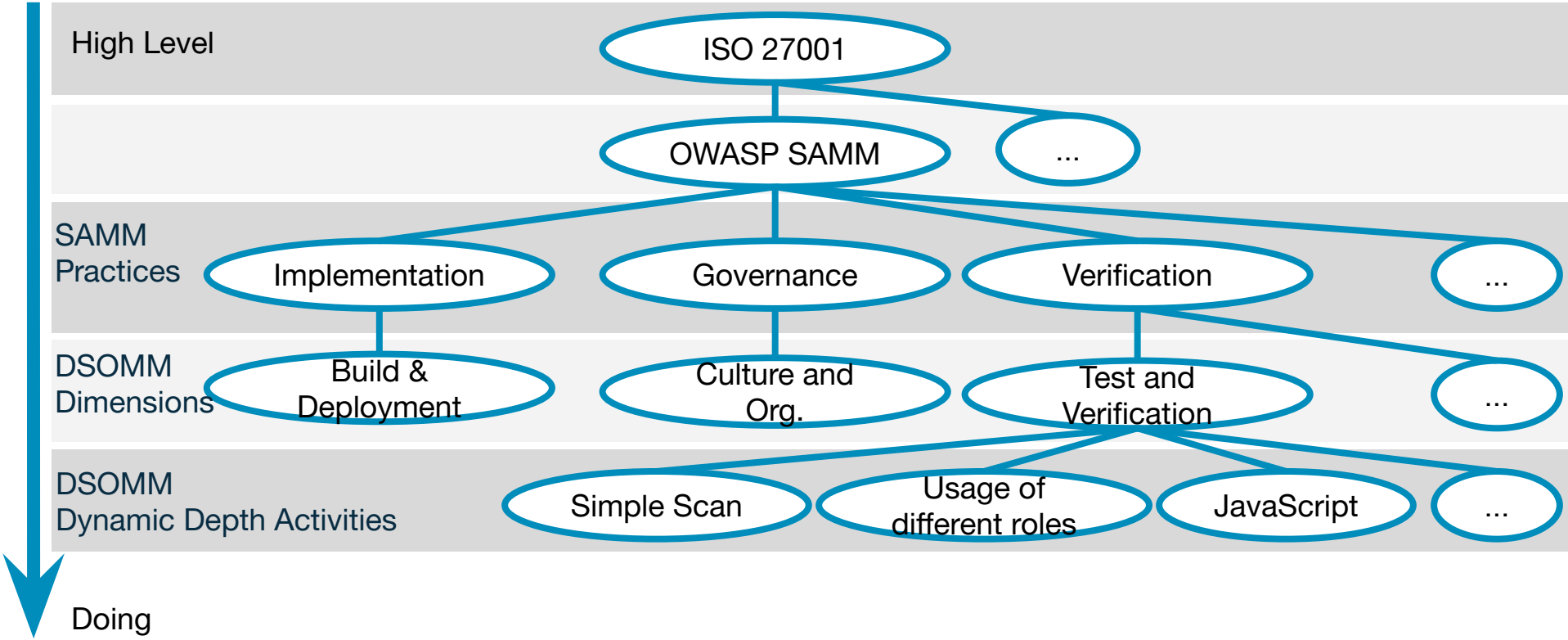
Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



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

DSOMM <> SAMM Mapping

Each Activity has a mapping to OWASP SAMM 2

https://dsomm.timo-pagel.de/report-samm.php

Sample Target Groups

- SAMM 2.0:
  - 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: Definition of targets with the management for the next 3-24 month
- OWASP DevSecOps Maturity Model 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

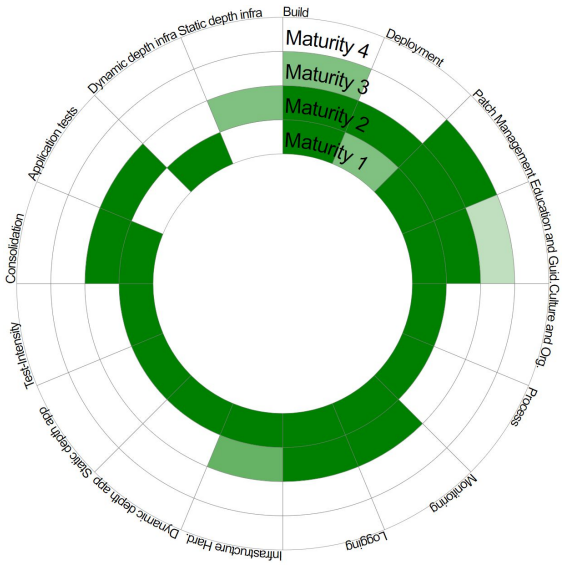
DSOMM Adoption

- 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)



Maturity of Implementation

Green = Done

Blue = Outstanding

Matrix | Implementation Levels | Ease and Value of Implementation | Dependencies | Full Report | About this project

Dimension	Sub-Dimension	Level 1: Basic understanding of security practices	Level 2: Adoption of basic security practices
Build and Deployment	Build	• Defined build process	• Regular tests
Build and Deployment	Deployment	• Defined deployment process • Inventory of running artifacts	• Backup before deployment • Environment depending configuration parameters • Usage of trusted images

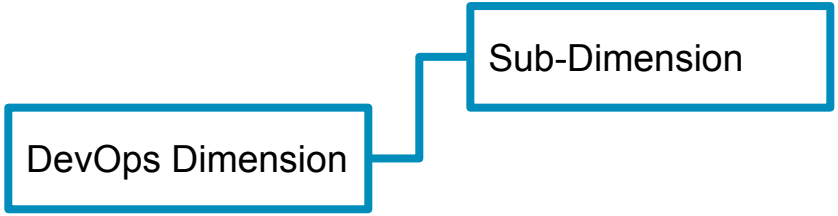
Agenda

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

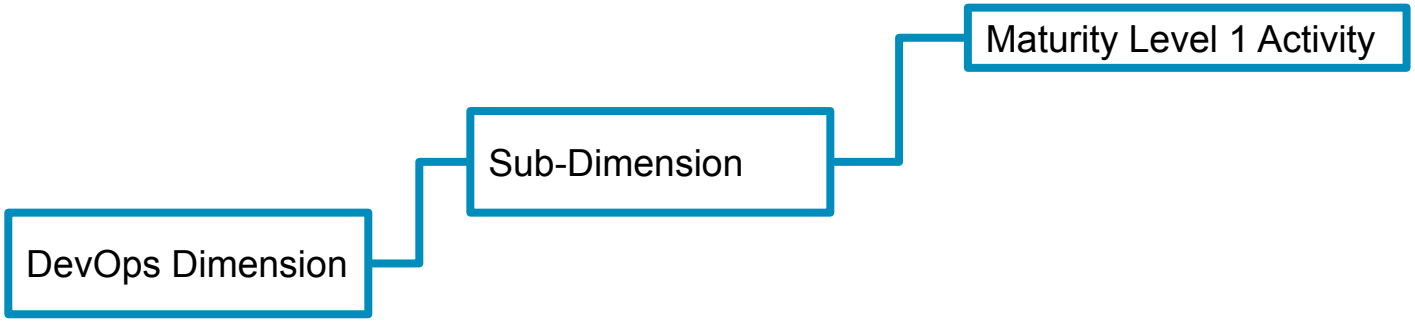
DSOMM Structure

DevOps Dimension

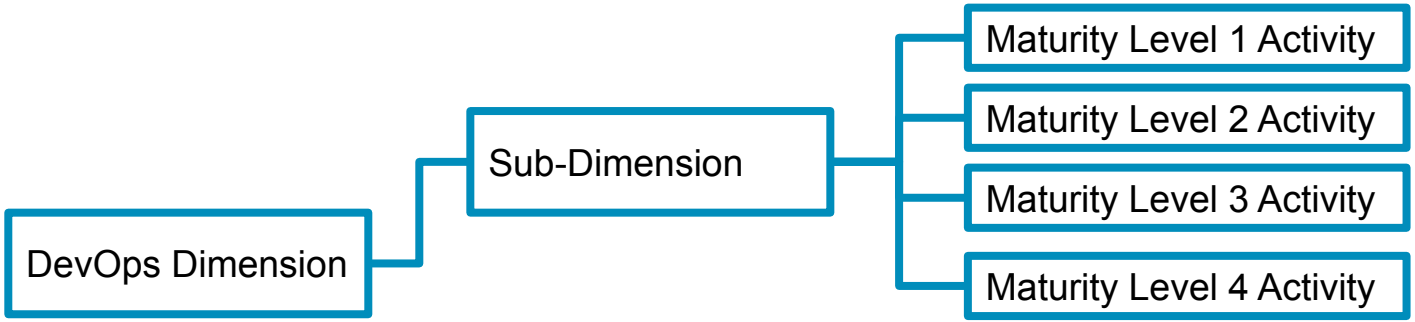
DSOMM Structure



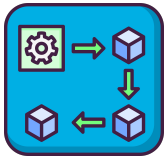
DSOMM Structure



DSOMM Structure



DevSecOps Dimensions



Build and Deployment

Culture and Organisation

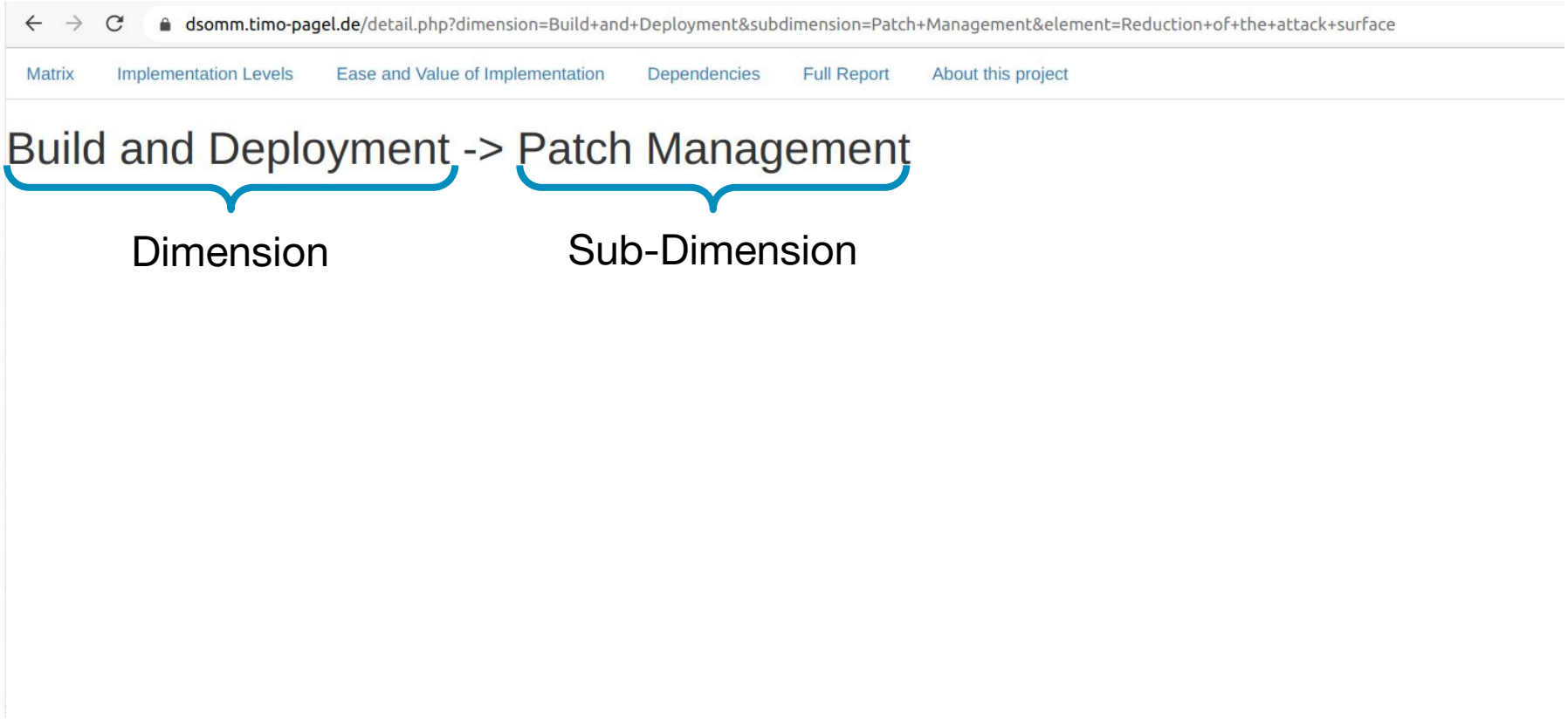
Information Gathering

Infrastructure

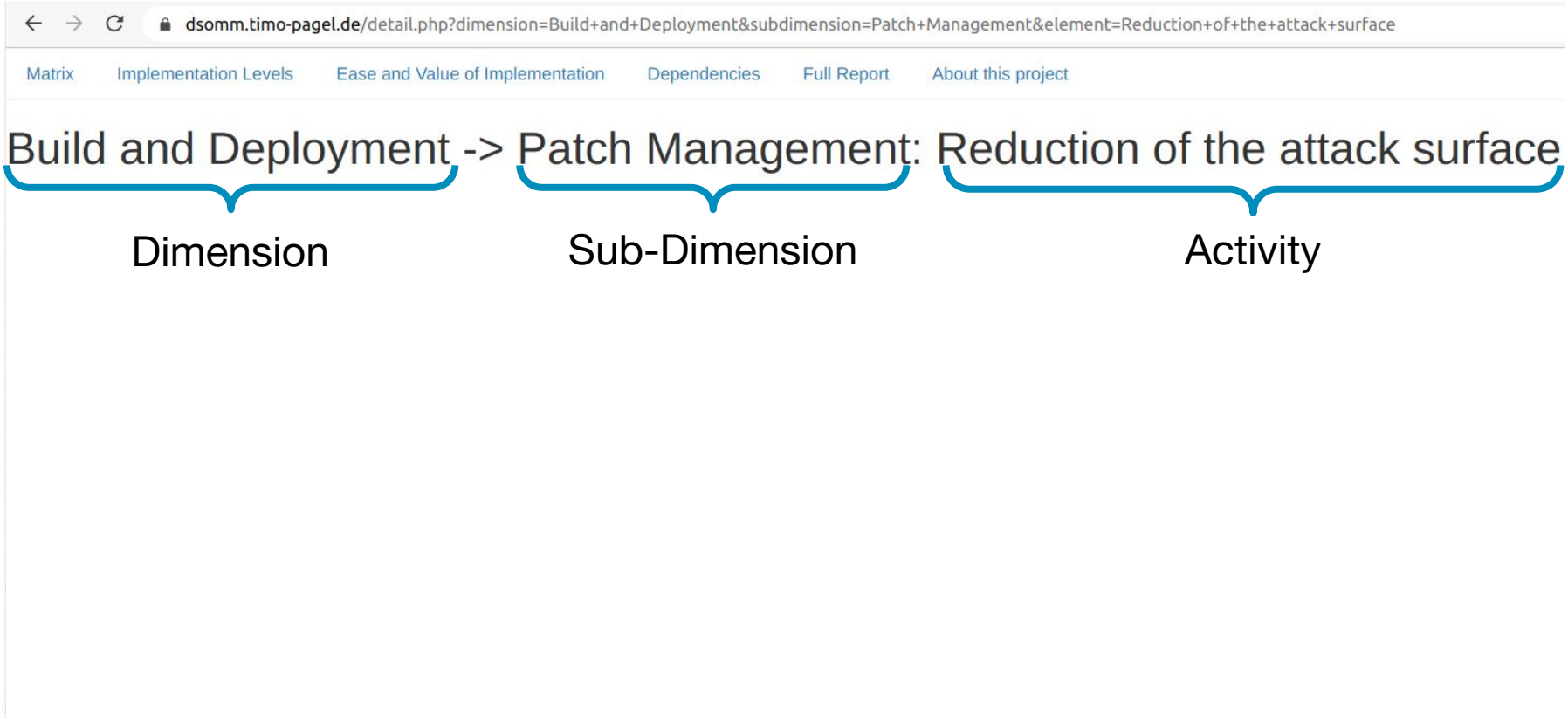
Test and Verification

Build and Deployment: Example Reduction of the attack surface

Build and Deployment: Example Reduction of the attack surface



Build and Deployment: Example Reduction of the attack surface



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

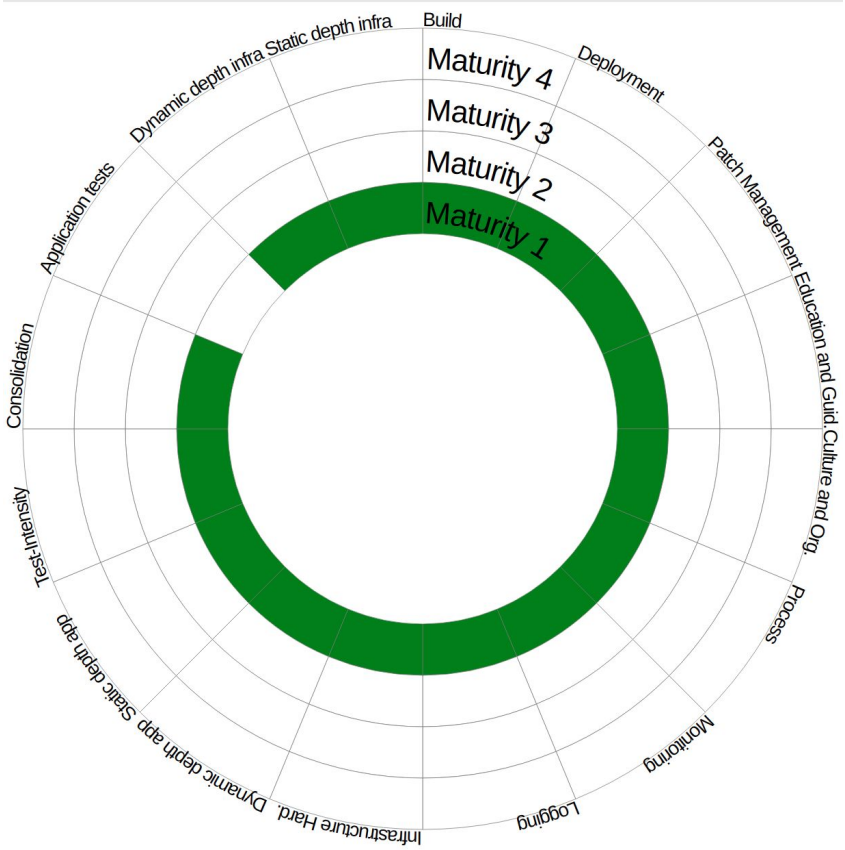
Build and Deployment -> Patch Management: Reduction of the attack surface

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.

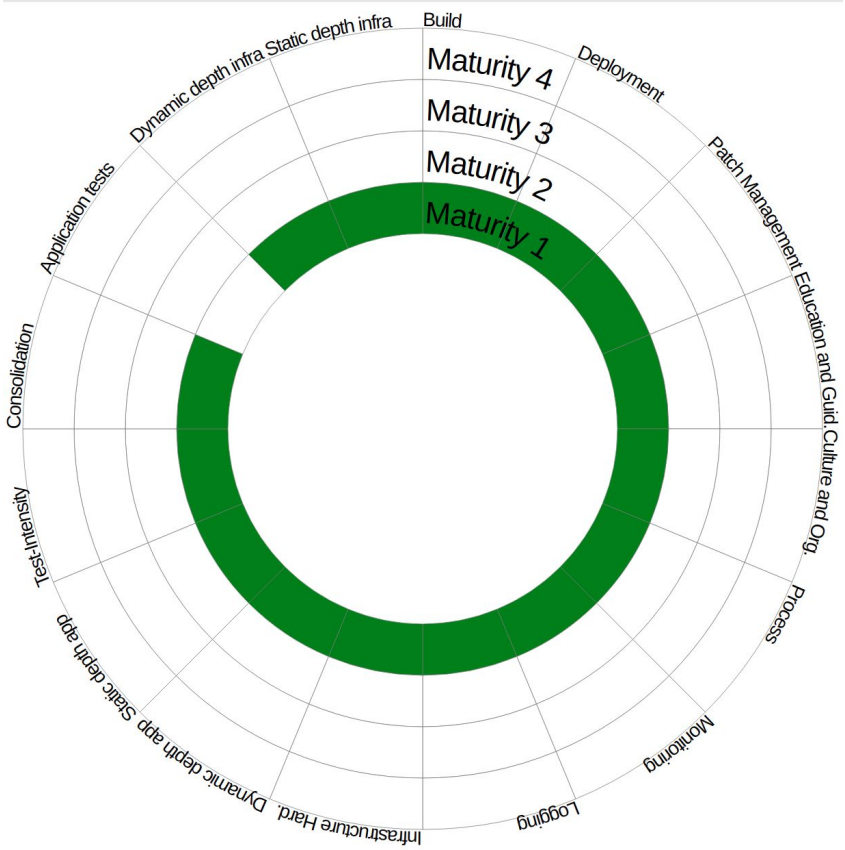
OWASP SAMM 2 Mapping: o-environment-management|B|1

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

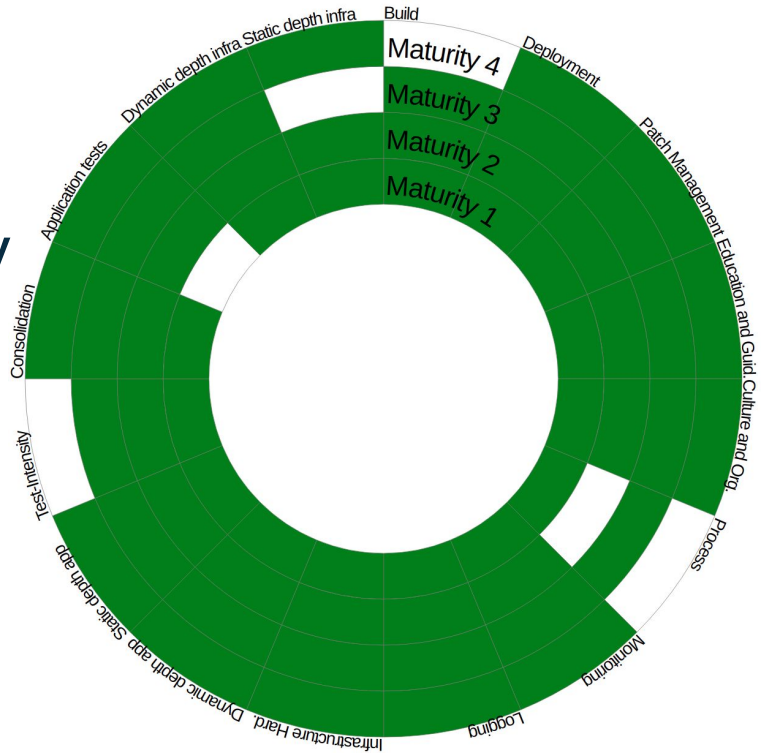
Maturity Levels

Level 1: Basic understanding of security practices

Level 2: Adoption of basic security practices

Level 3: High adoption of security practices

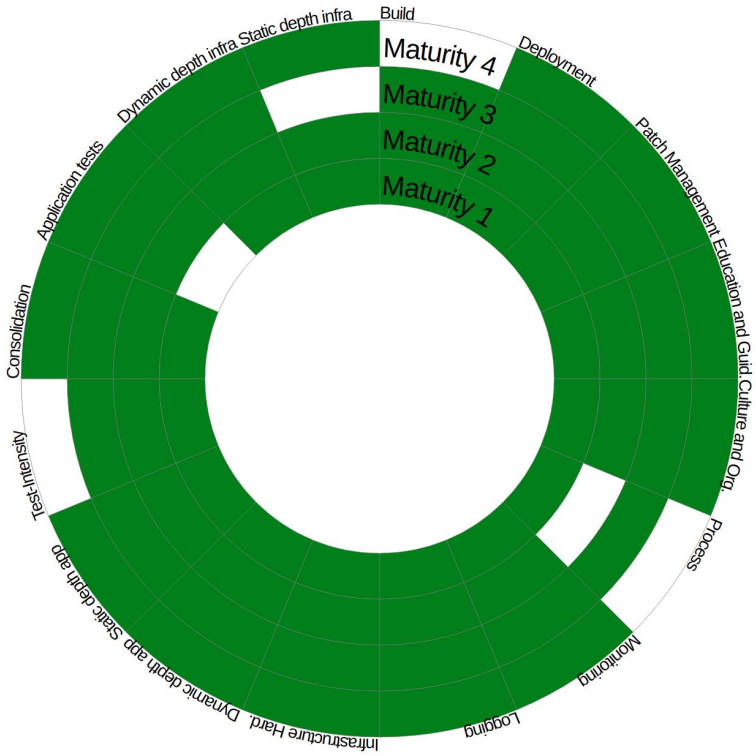
Level 4: Advanced deployment of security practices at scale



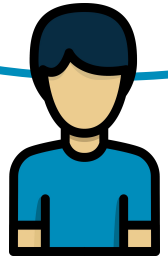
White Spots

Activities where important

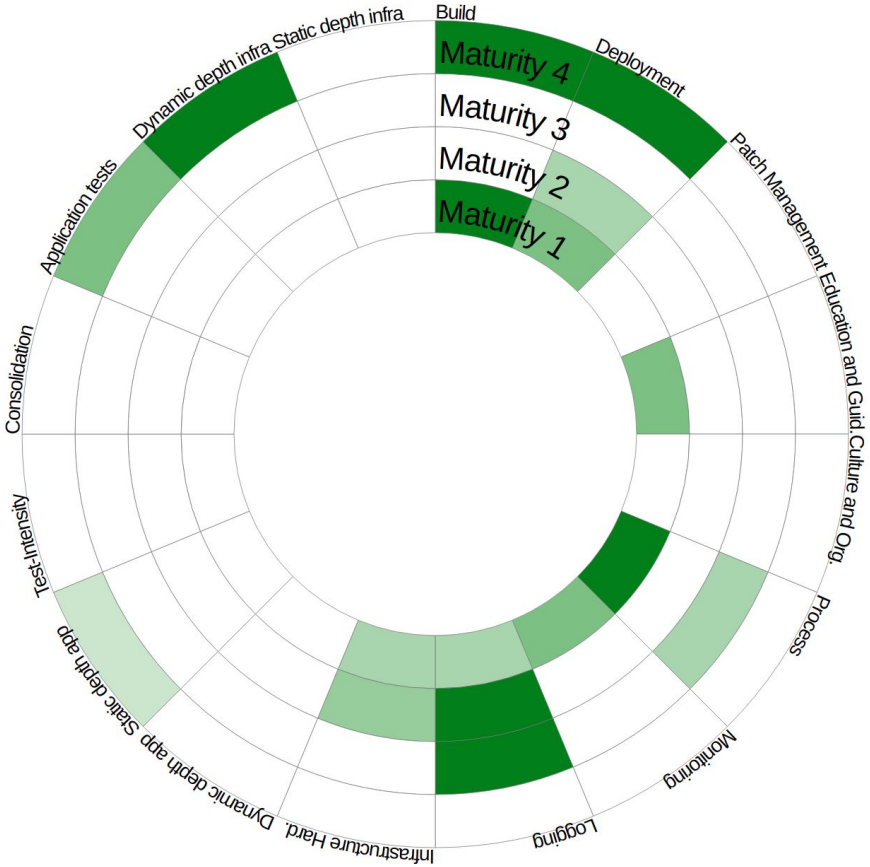
-> No Activity



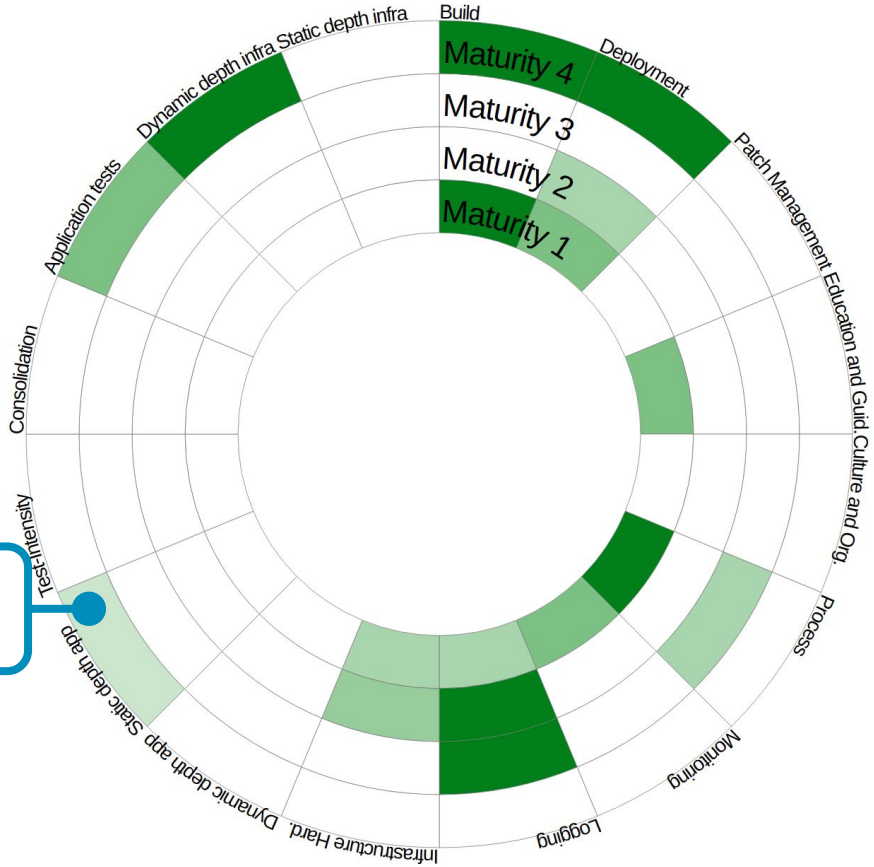
Why spider web with heat map?



Typical Start of a DevOps oriented Organization without Security-Focus



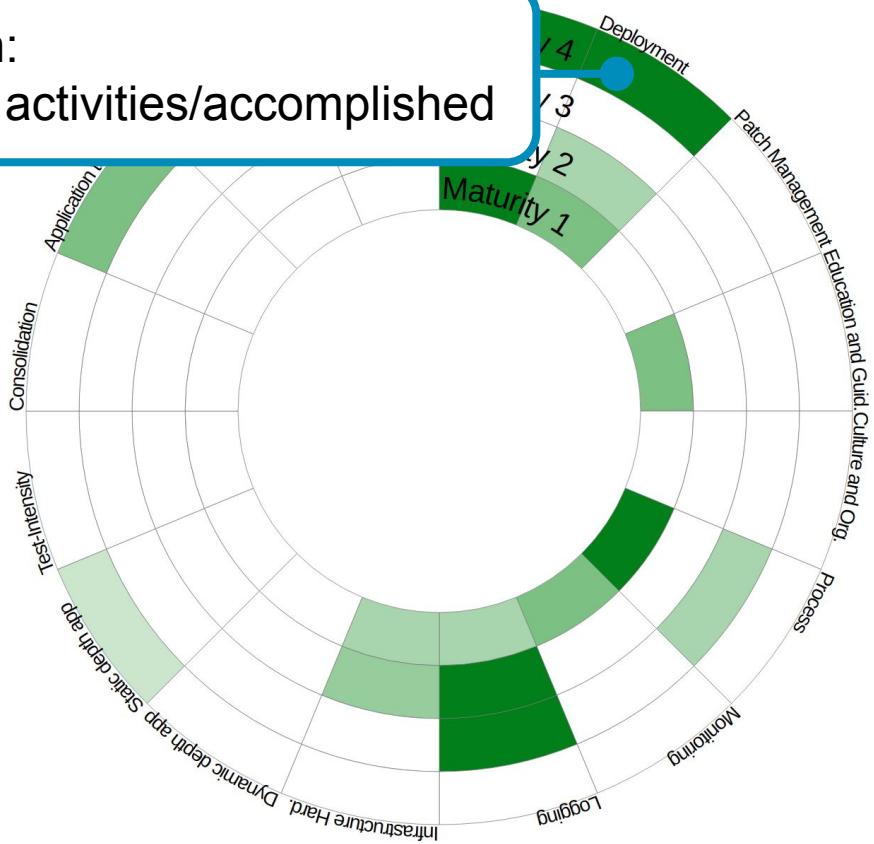
Typical Start of a DevOps oriented Organization without Security-Focus



Often low value,
e.g. *stylistic analysis*

Typical Start of a DevOps oriented Organization without Security-Focus

Calculation:
Number of activities/accomplished



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

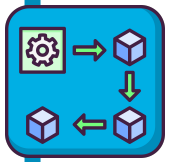
- Usage of distroless images and a small operating system

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

How Deep?

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

- Tests for known vulnerabilities in components of the backend/middleware are performed.
  Implementation Hint: OWASP Dependency Check

- Test with the OWASP Dependency Check in components of the backend/middleware are performed by starting dependency check with ...

Where does DevSecOps starts/ends?

- “Normal” Operations Tasks?
  - Backup of a database
  - Backup before deployment
- “Normal” Application Security Considerations?

-> Would app. security requirements be the outcome of a threat modeling?

-> The model is often misunderstood

-> Introduction of “something”

Application Security: Activity vs. Mapping vs. Nothing

www.menti.com

- Introduction of an activity to define application security requirements

Application Security: Activity vs. Mapping vs. Nothing

www.menti.com

- Introduction of an activity to define application security requirements
- Introduction of a dimension “application” with sample mapping to OWASP ASVS, e.g.

DSOMM	Level 1	Level 2	Level 4
ASVS	Level 1	Level 2	Level 3

Application Security: Activity vs. Mapping vs. Nothing

www.menti.com

- Introduction of an activity to define application security requirements
- Introduction of a dimension “application” with sample mapping to OWASP ASVS, e.g.

DSOMM	Level 1	Level 2	Level 4
ASVS	Level 1	Level 2	Level 3

- No need to add application security directly

Application Security: Activity vs. Mapping vs. Nothing

www.menti.com, Code 95 06 85 9:

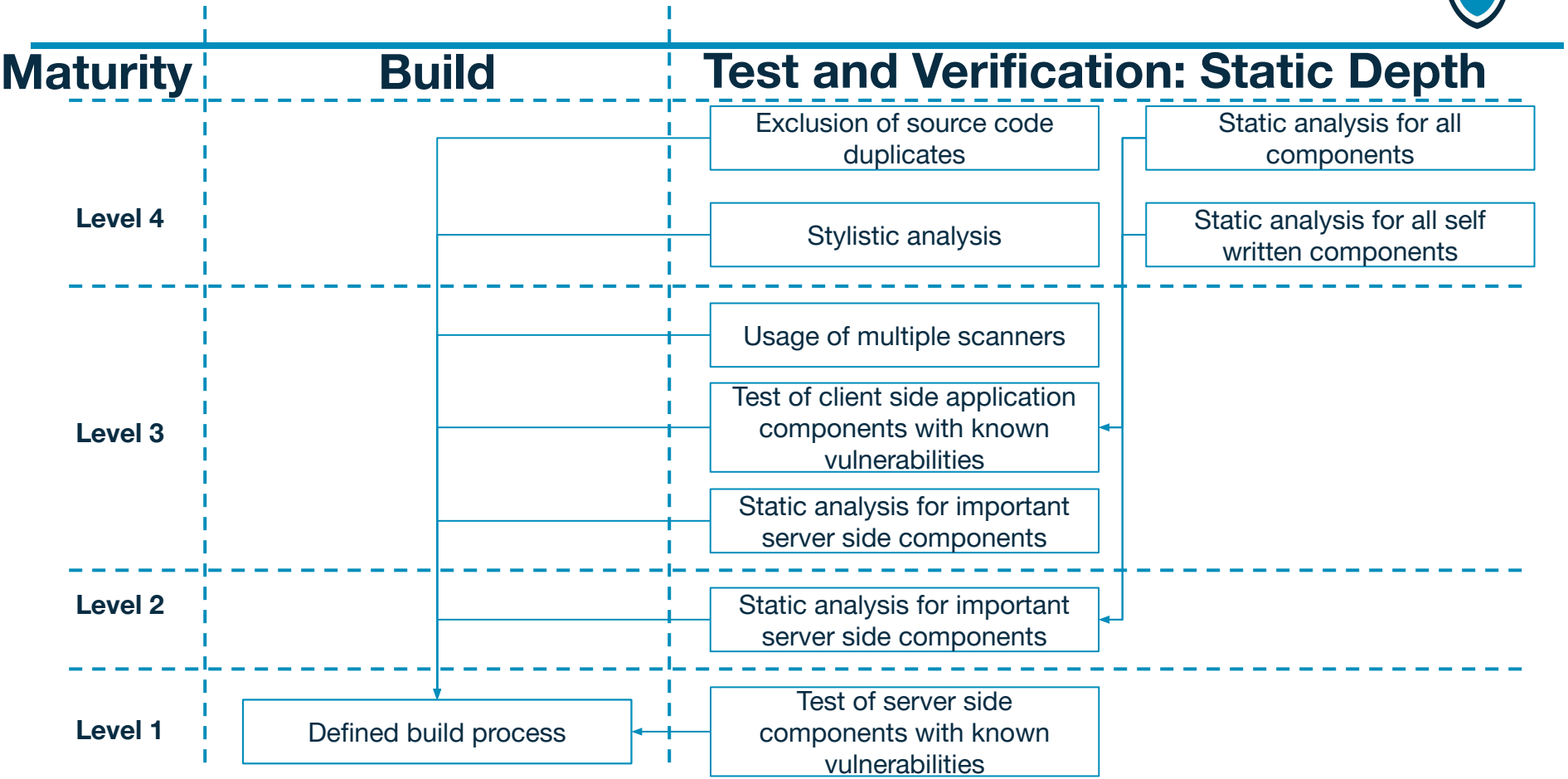
- Introduction of an activity to define application security requirements
- Introduction of a dimension “application” with sample mapping to OWASP ASVS, e.g.

DSOMM	Level 1	Level 2	Level 4
ASVS	Level 1	Level 2	Level 3

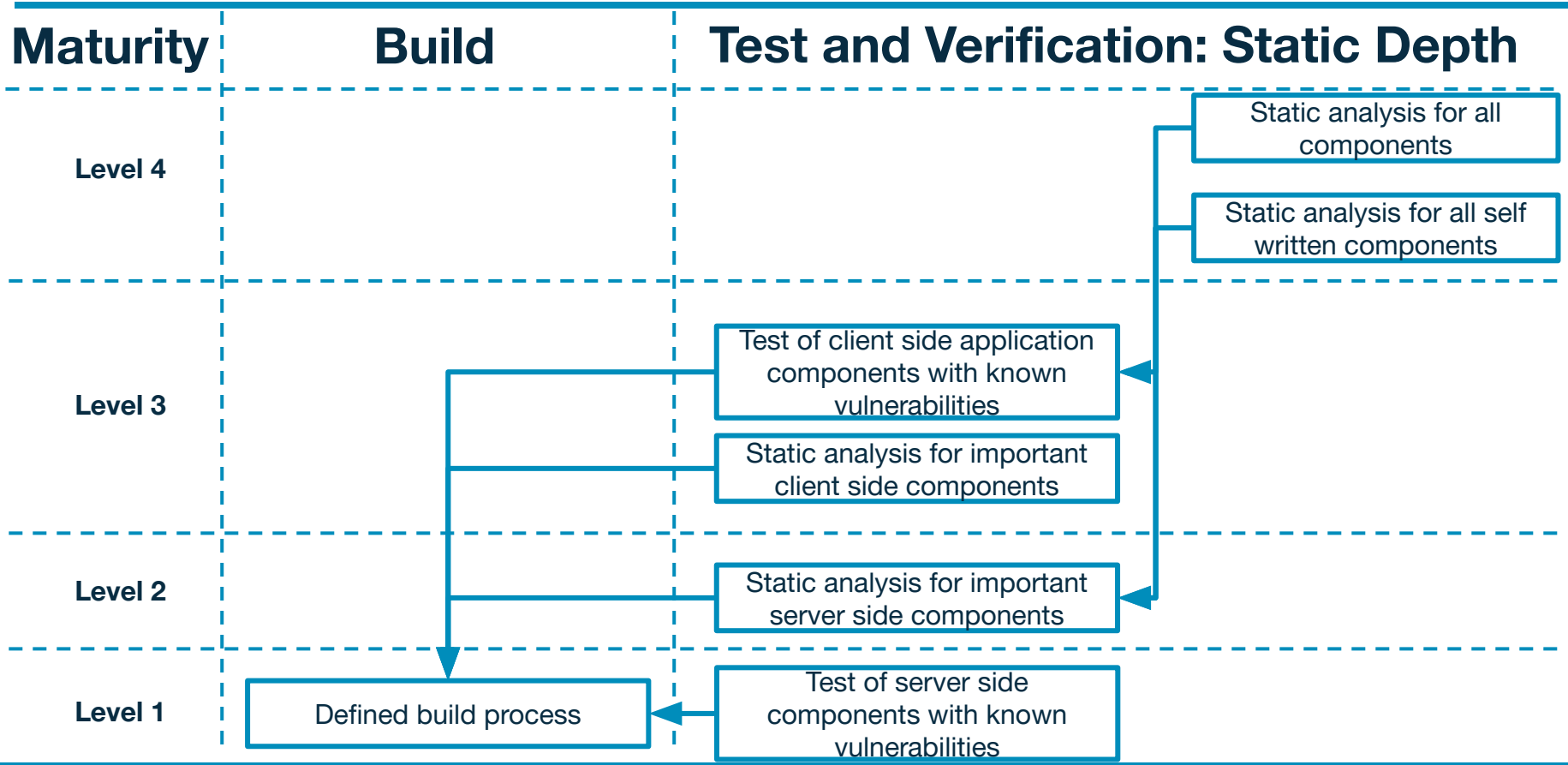
- No need to add application security directly

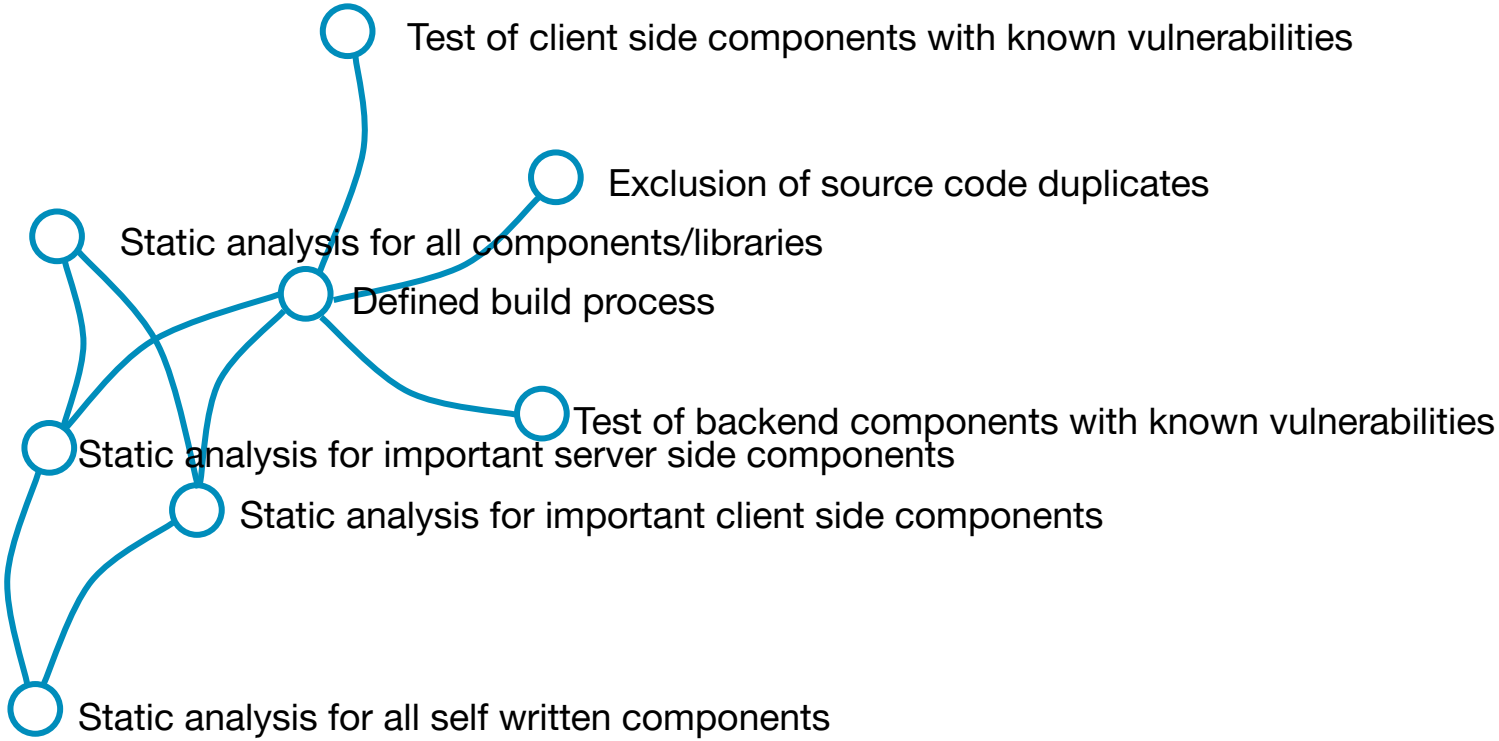
Attributes of an Activity

- Risk
- Opportunity
- Usefulness for Security / Difficulty of Implementation
- Dependencies
- Implementation Hints
- OWASP SAMM Mapping

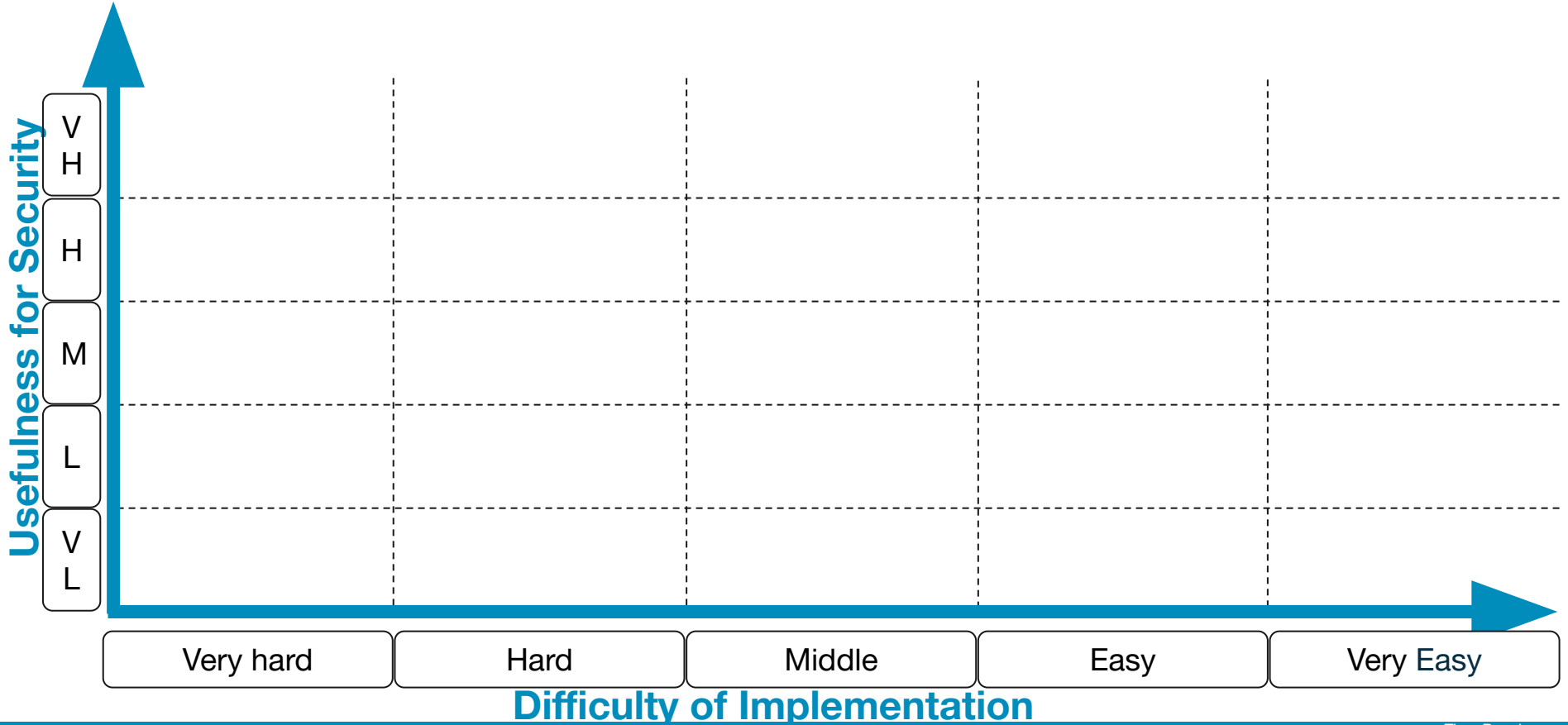

Maturity
Build
Test and Verification: Static Depth
Level 4
Level 3
Level 2
Level 1
Exclusion of source code duplicates
Stylistic analysis
Usage of multiple scanners
Test of client side application components with known vulnerabilities
Static analysis for important server side components
Static analysis for important server side components
Test of server side components with known vulnerabilities
Static analysis for all components
Static analysis for all self written components
Defined build process

Simplified View of Dependencies




Test of client side components with known vulnerabilities
Exclusion of source code duplicates
Static analysis for all components/libraries
Defined build process
Test of backend components with known vulnerabilities
Static analysis for important server side components
Static analysis for important client side components
Static analysis for all self written components

Assigning of Activities



Matrix | Implementation Levels | Ease and Value of Implementation | Dependencies | Full Report | About this project

Toggle Label

Show total values

- Build and Deployment - Build
- Build and Deployment - Deployment
- Build and Deployment - Patch Management
- Culture and
- Culture and Org. - Culture and Org.
- Culture and Org. - Process
- Information Gathering - Monitoring
- Information
- Infrastructure - Infrastructure Hardening
- Test and Verification - Dynamic depth for applications
- Test and Verification - Static depth for applications
- Test and V
- Test and Verification - Consolidation
- Test and Verification - Application tests
- Test and Verification - Dynamic depth for infrastructure
- Test and V

Usefulness for Security

6, 5.5, 5, 4.5, 4, 3.5, 3, 2.5, 2, 1.5, 1

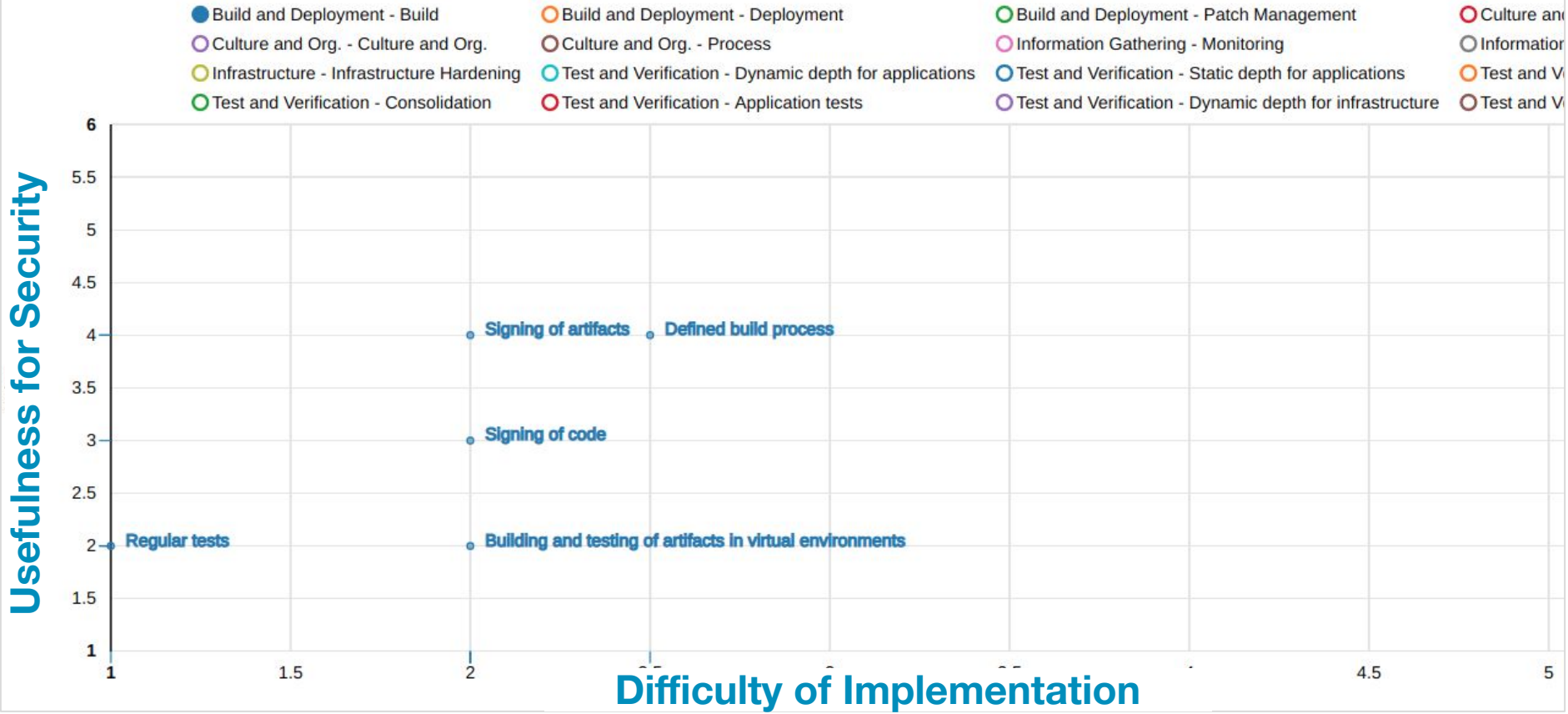
1, 1.5, 2, 4.5, 5

Difficulty of Implementation

Matrix | Implementation Levels | Ease and Value of Implementation | Dependencies | Full Report | About this project

Toggle Label

Show total values

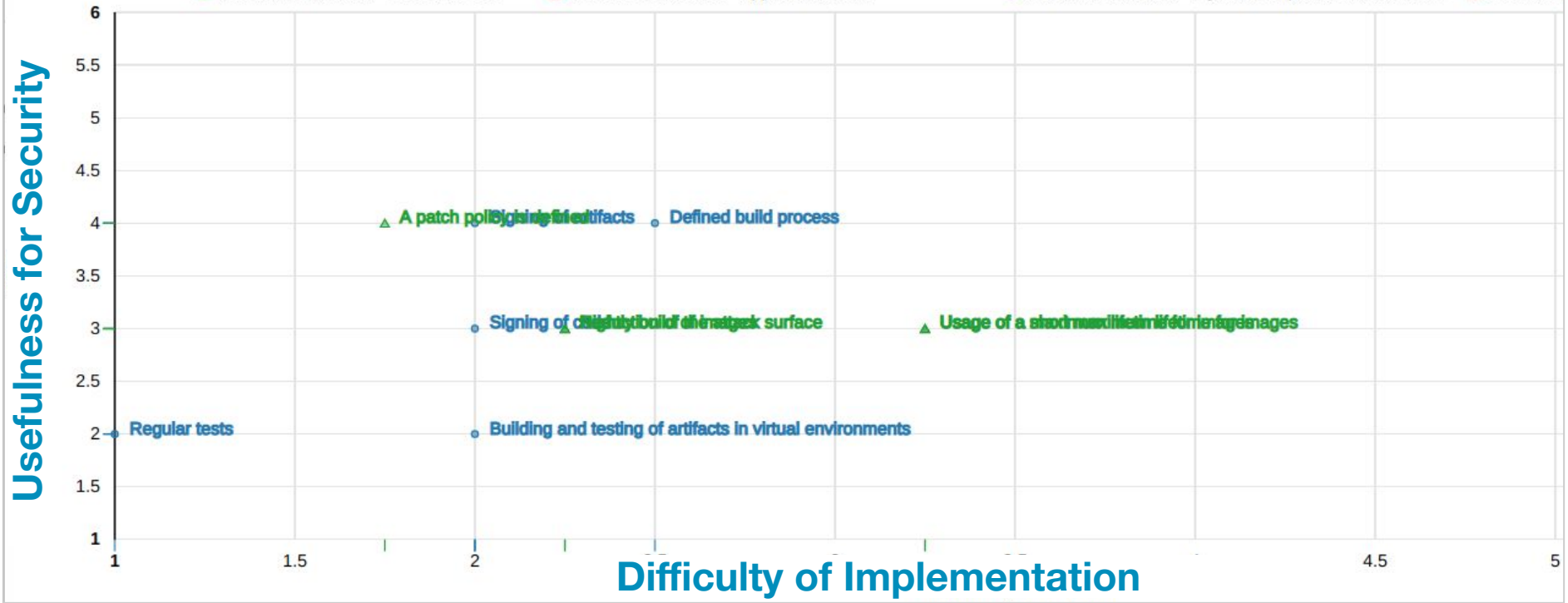


Matrix | Implementation Levels | Ease and Value of Implementation | Dependencies | Full Report | About this project

Toggle Label

Show total values

- Build and Deployment - Build
- Build and Deployment - Deployment
- Build and Deployment - Patch Management
- Culture ar
- Culture and Org. - Culture and Org.
- Culture and Org. - Process
- Information Gathering - Monitoring
- Informatic
- Infrastructure - Infrastructure Hardening
- Test and Verification - Dynamic depth for applications
- Test and Verification - Static depth for applications
- Test and V
- Test and Verification - Consolidation
- Test and Verification - Application tests
- Test and Verification - Dynamic depth for infrastructure
- Test and V



Creation of New of Activities

Take into account:

- Dimension (no redundancy)
- Level
  - Dependencies
  - Outcome for Security
  - Ease of implementation

Creation of New of Activities

Take into account:

- Dimension (no redundancy)
- Level
  - Dependencies
  - Outcome for Security
  - Ease of implementation
    - Needed Knowledge (1,2,3,4 Disciplines)
    - Needed Time
    - Needed Resources (Systems)

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.

Exploit details

Usefullness: Medium
Required knowledge: Medium (two disciplines)
Required time: Medium
Required resources (systems): Low

Additional Information

Implementation hints:

- Distroless
- Fedora CoreOS

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

Agenda

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

Conclusion

- Plan security strategy
- Adapt DSOMM
- DSOMM might be 80% of your secure DevOps strategy

Next Steps, be involved!

- Better OWASP SAMM mapping visualization
- Address application security?
- More and optimized activities
- OWASP Project Lab Status -> Review needed
- DevSecOps Toolchain Categorization

Pull Requests with suggestions are welcome

Questions

DSOMM

https://owasp.org/www-project-devsecops-maturity-model/

https://dsomm.timo-pagel.de

Community contact:

timo.pagel@owasp.org

Business contact:

devsecops@pagel.pro

https://pagel.pro