



Overview of (DevSecOps) OWASP Projects

OWASP Stammtisch Frankfurt

2021-04-28



Timo Pagel

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



Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM

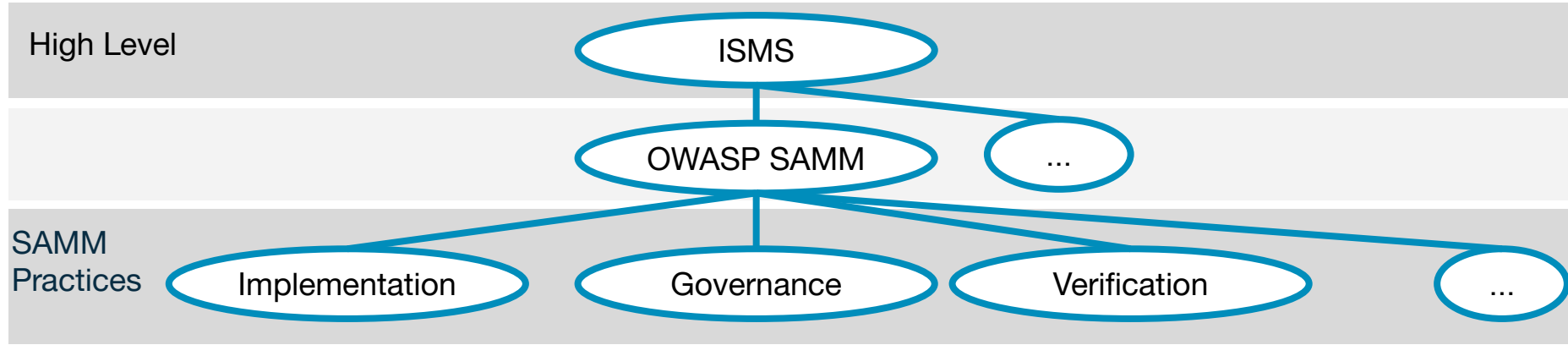


High Level

ISMS

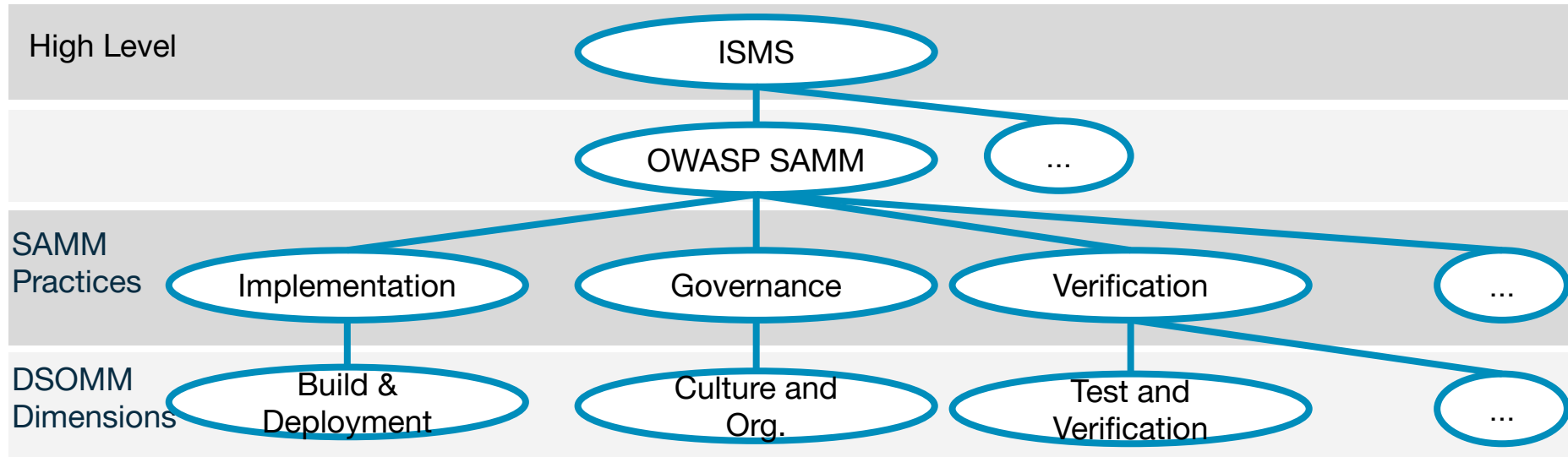
Doing

Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM

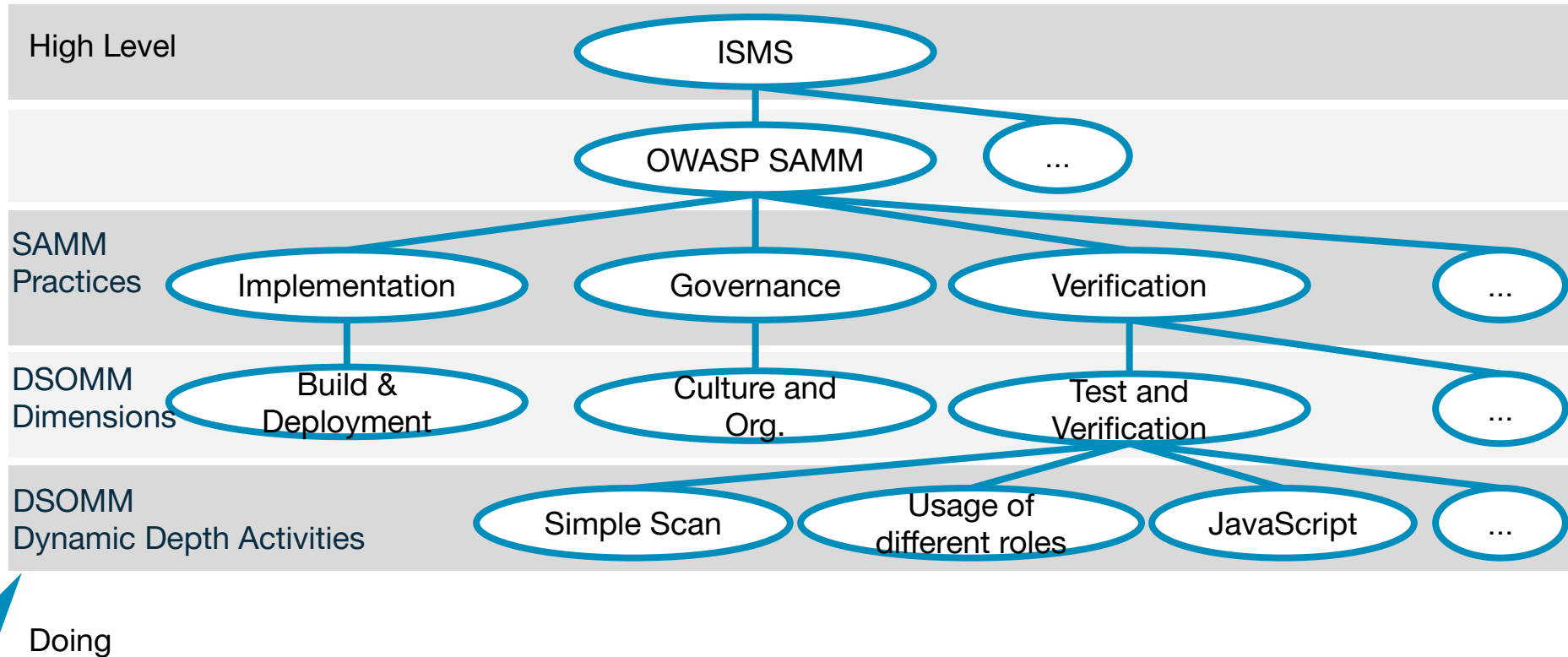


Doing

Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM

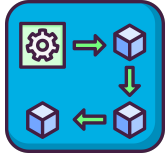


Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



- **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



Build and Deployment



Culture and Organisation



Information Gathering



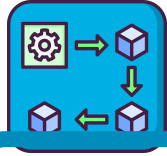
Hardening



Test and Verification



DSOMM



Build and Deployment



DSOMM



Culture and Organisation



Information Gathering



Hardening



Test and Verification

Security Champions playbook



Identify
teams

Define
the role

Nominate
champions

Comm
channels

Knowledge
base

Maintain
interest

OWASP Juice Shop is probably the most modern and sophisticated insecure web application!



“OWASP Top 10 2017 German”



German OWASP Top Ten 2017
Great for an initial training plan





Possible Rewards / Motivations



- High-Fives 



Possible Rewards / Motivations



- High-Fives 
- Pins



- Reminder
- Fast achievements
- Gamification: “We want to collect all pins”
- Transforms non touchable security into touchable security



- Reminder
 - Fast achievements
 - Gamification: “We want to collect all pins”
 - Transforms non touchable security into touchable security
-
- Needs to be designed and produced



Implementation



Implementation



Virtual COVID-19 way: Backstage at SDA SE



The screenshot shows the Backstage.io interface for the 'team-dock-marshals' team. The browser address bar shows 'backstage.sda-se.io'. The team name 'team-dock-marshals' is displayed with a star icon. The 'Owner' and 'Lifecycle' are both listed as 'unknown'. The 'OVERVIEW' tab is selected. The main content area is divided into three sections: 'Team Dock Marshals', 'Security Champions', and 'Ownership'. The 'Team Dock Marshals' section shows a team icon 'TD' and a link '[sda_se_open_industry_solutions]'. The 'Security Champions' section features a grid of security champion avatars and a 'Learn more' link. The 'Ownership' section displays a grid of ownership metrics for various categories.

| Category | Count |
|---------------|-------|
| Services | 2 |
| Documentation | 0 |
| APIs | 0 |
| Libraries | 0 |
| Websites | 2 |
| Tools | 0 |

Members (3)
of Team Dock Marshals

The members section shows three team members: Dominik Henneke, Oliver Sand, and Philipp Furrer.

Training Rewards



Nudging (Reminder)



- “Steer people in particular directions”
 - E.g. road signs
- > Security pins on a hat
- Reminder of topics

Nudging Advanced



Threat Modeling



- What are we building?
- What can go wrong?
- What are we going to do about that?
- Did we do a good enough job?



Threat Modeling Playbook

Get TM
stakeholders
buy-in

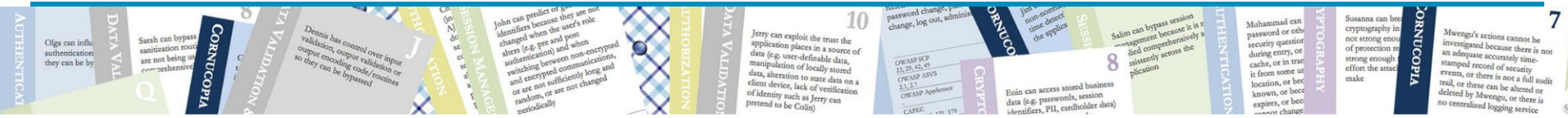
Embed TM
in your
organization

Train your
people to
TM

Strengthen
your TM
processes

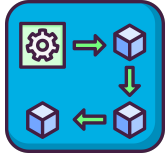
Innovate
with TM
technology

Threat Modeling: What can go wrong?



- Card Games (e.g. OWASP Cornucopia)
- Remote:
 - Online Cue Cards
 - Hybrid
 - > Send out card games before
 - > Send out hand before
 - > Participants might look at it beforehand

Free Cards for German OWASP Members:
Request robert.seedorff@iteratec.com



Build and Deployment



Culture and Organisation



Information Gathering



Hardening



Test and Verification



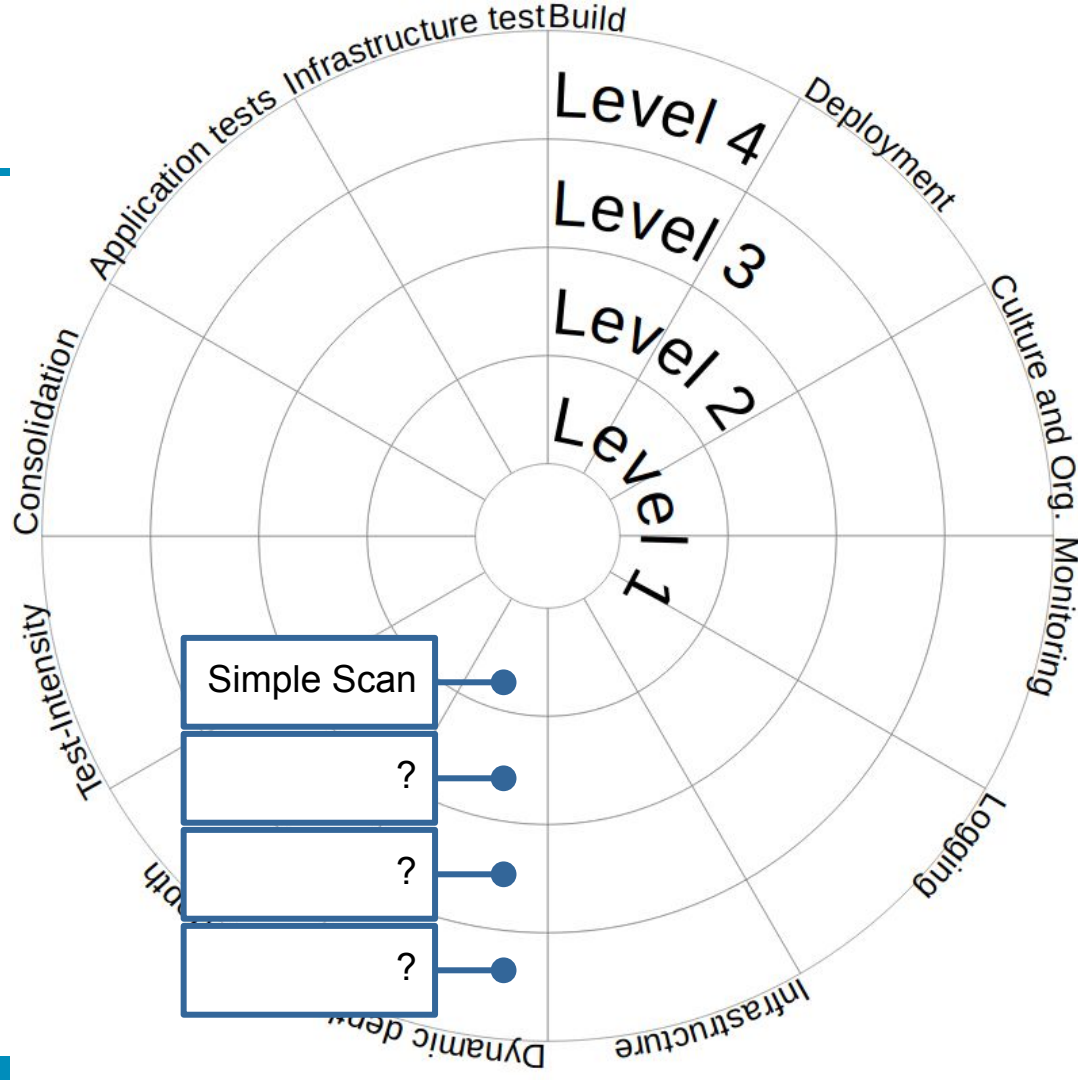
DSOMM



DSOMM

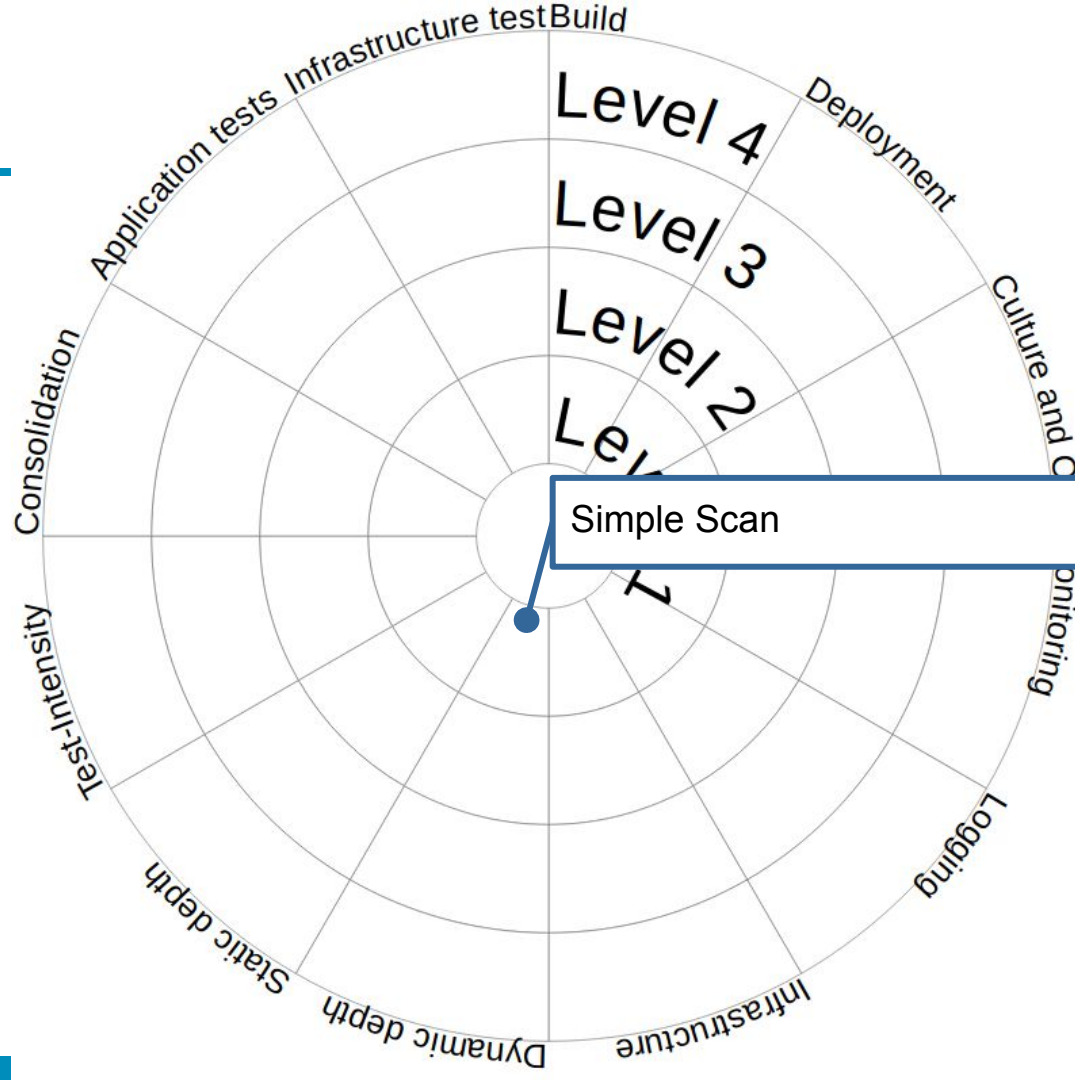


DSOMM



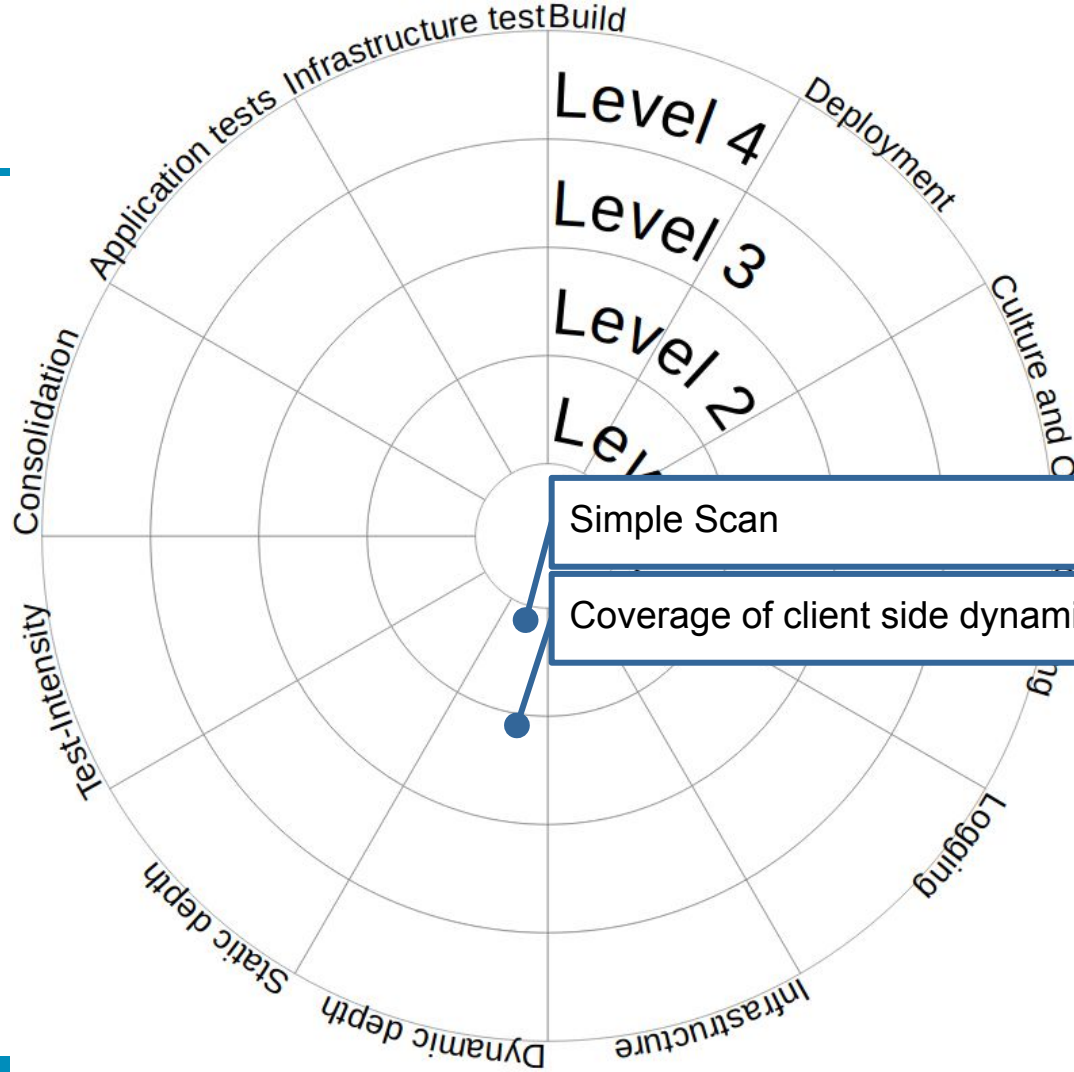


DSOMM



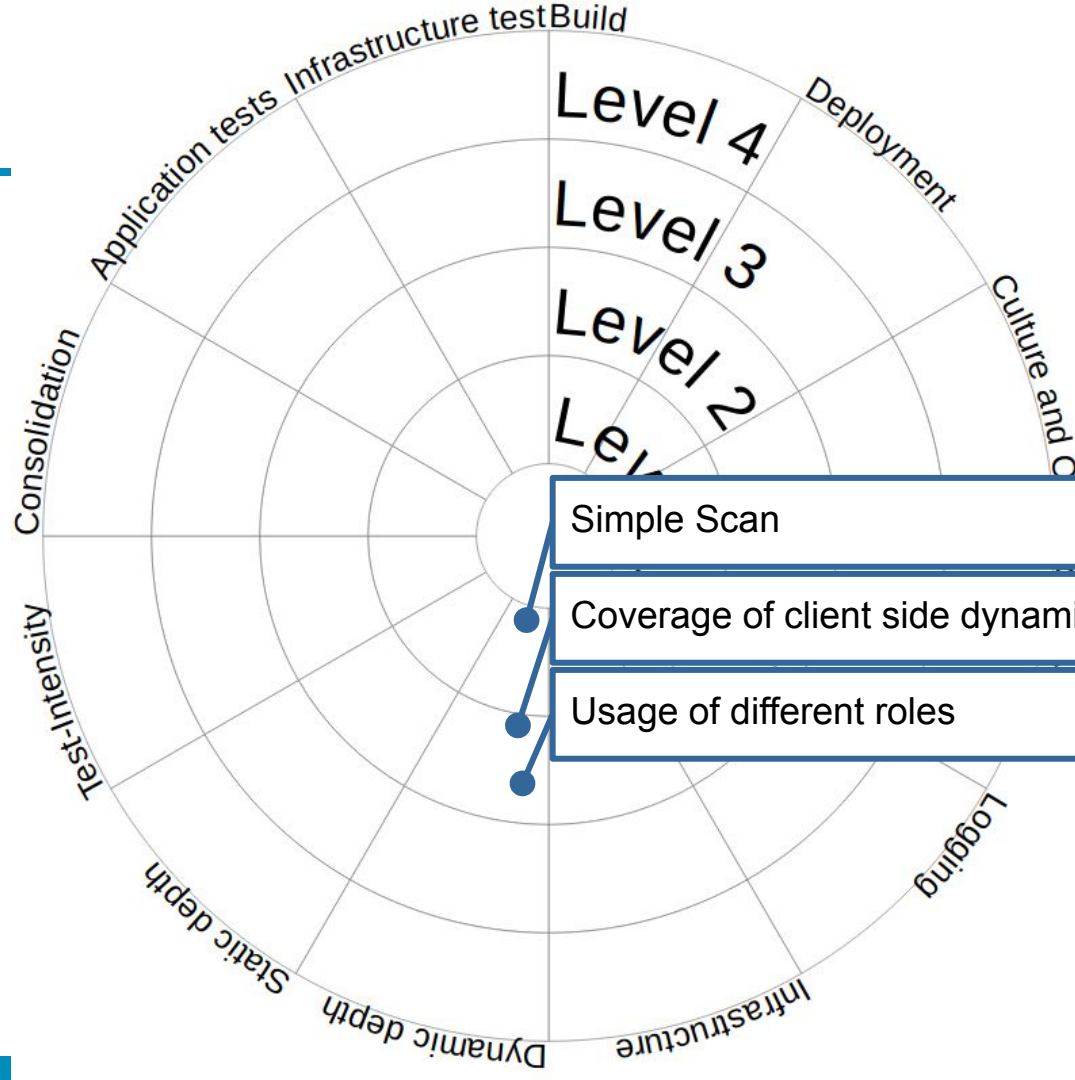


DSOMM



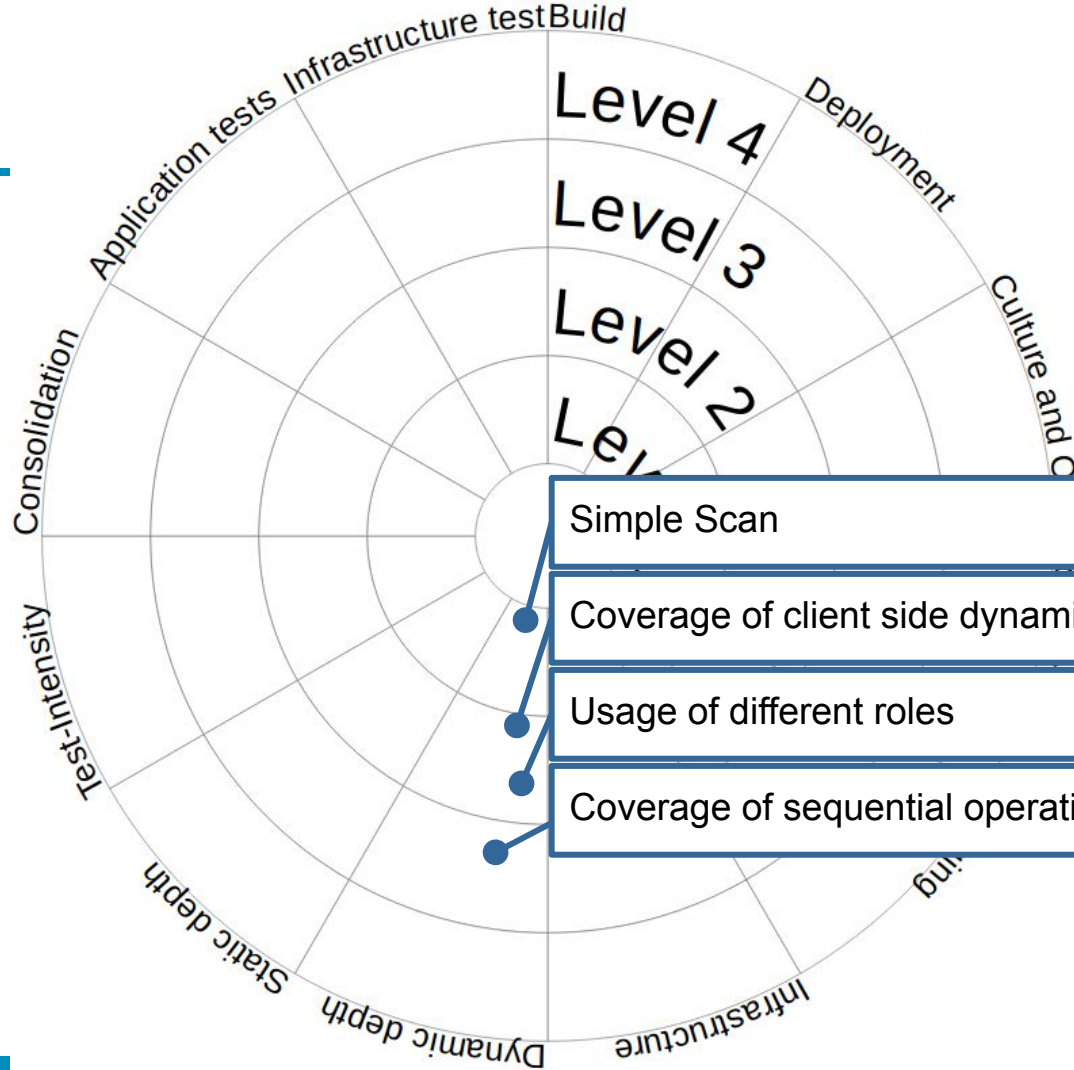


DSOMM





DSOMM



Simple Scan

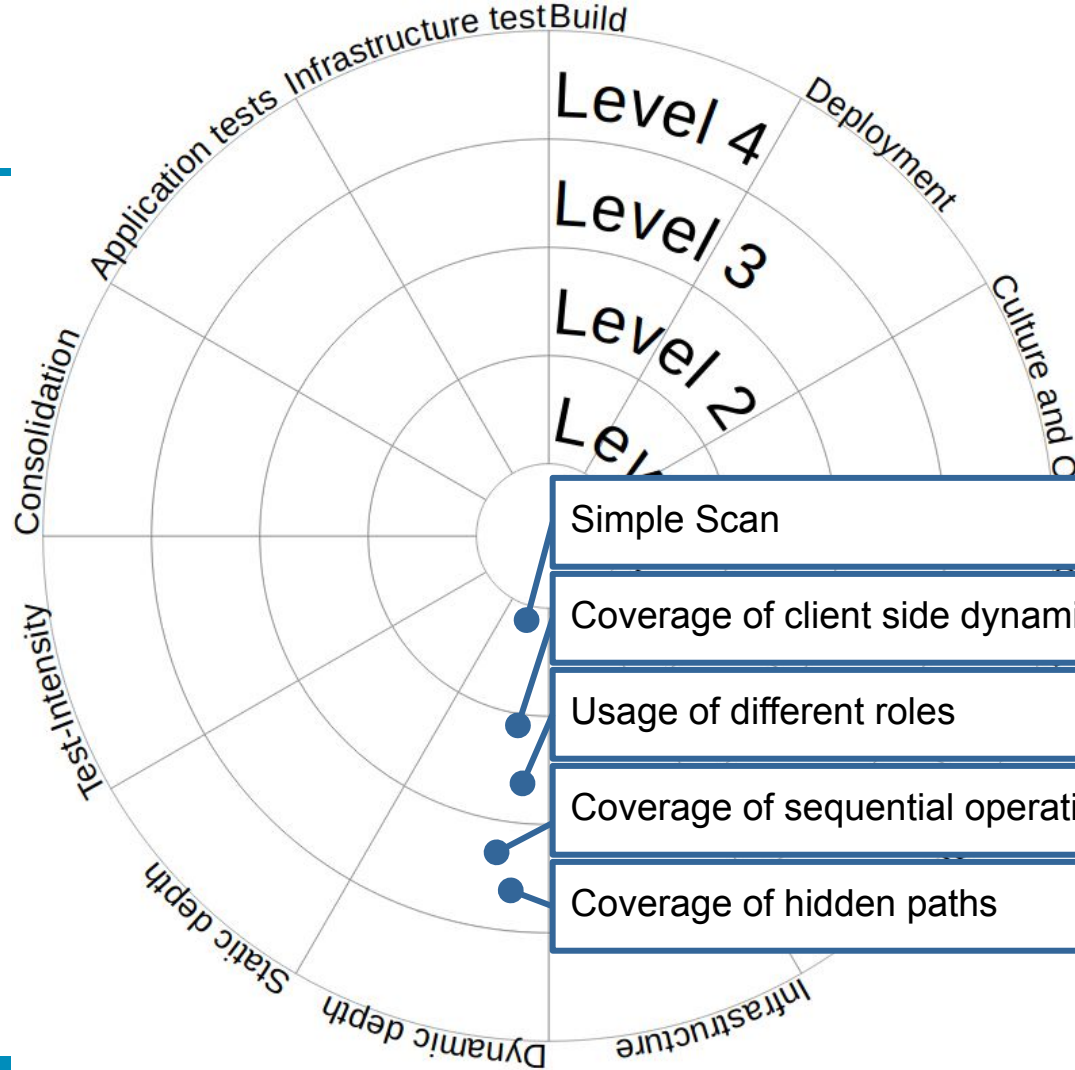
Coverage of client side dynamic components

Usage of different roles

Coverage of sequential operations

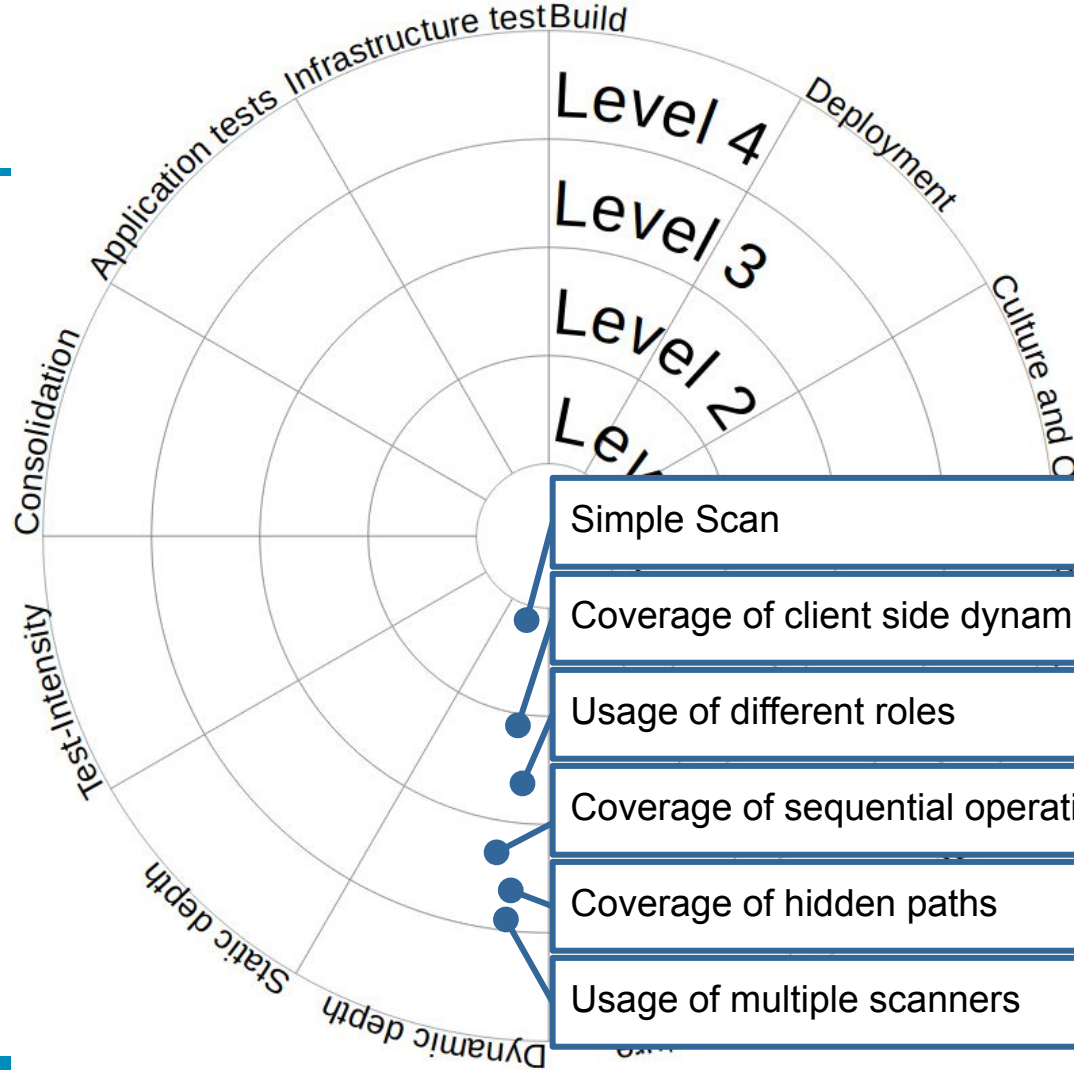


DSOMM

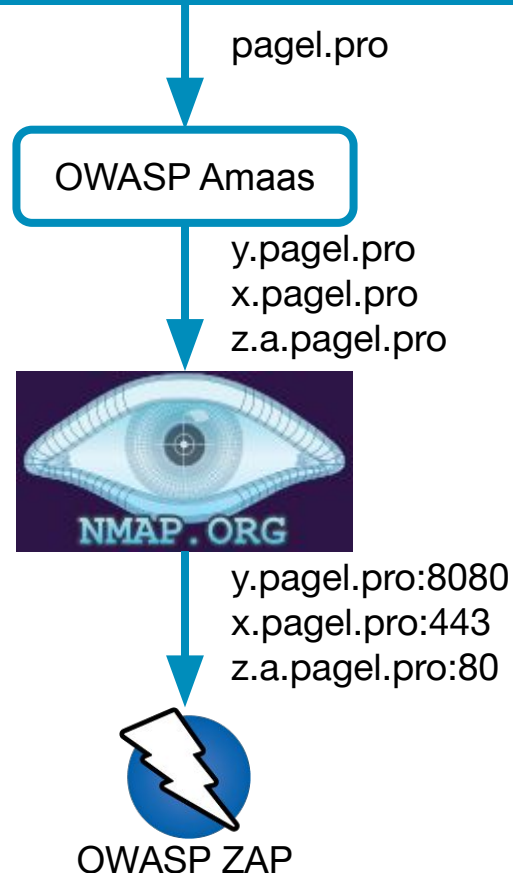


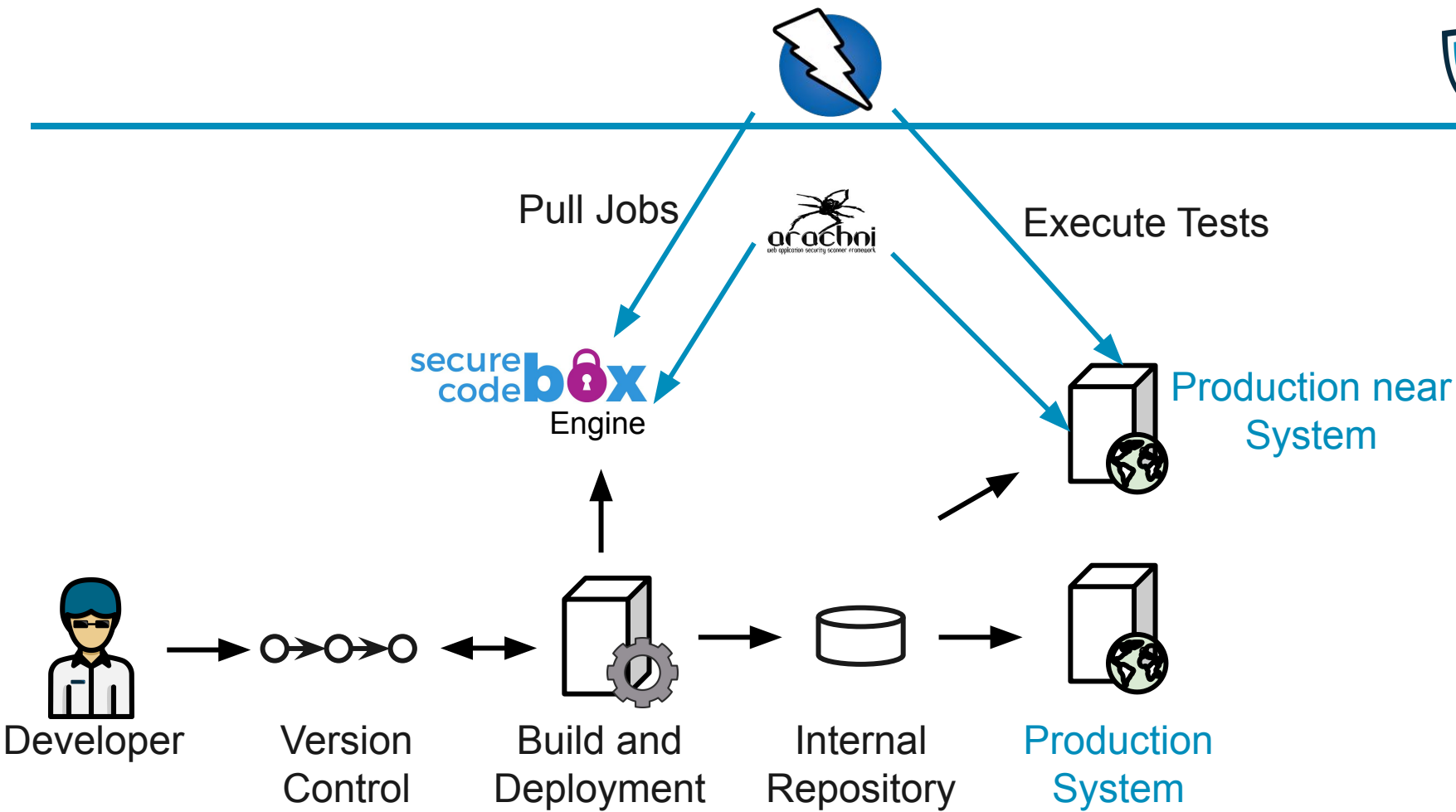


DSOMM

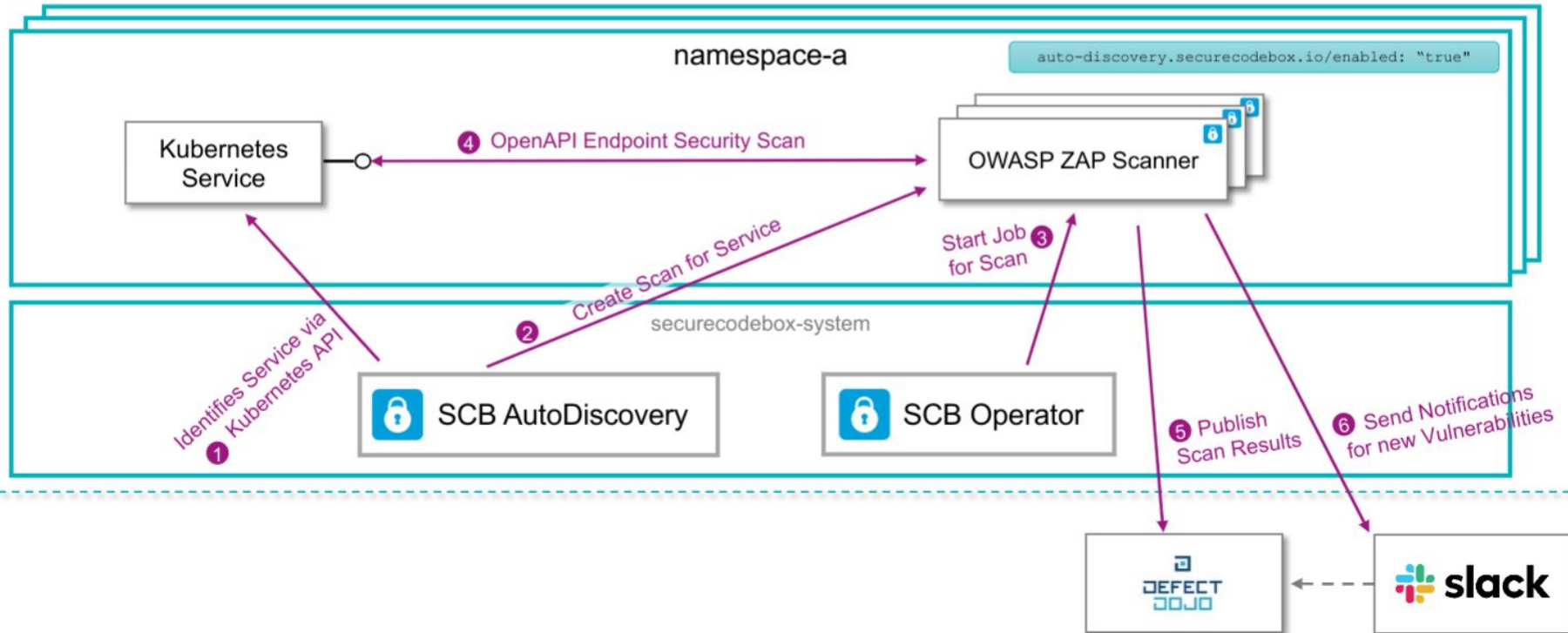


Web Security Testing of (an unknown) Enterprise World





Target Cluster (DEV)



Vulnerability Management System: Deduplication



- Handle Findings

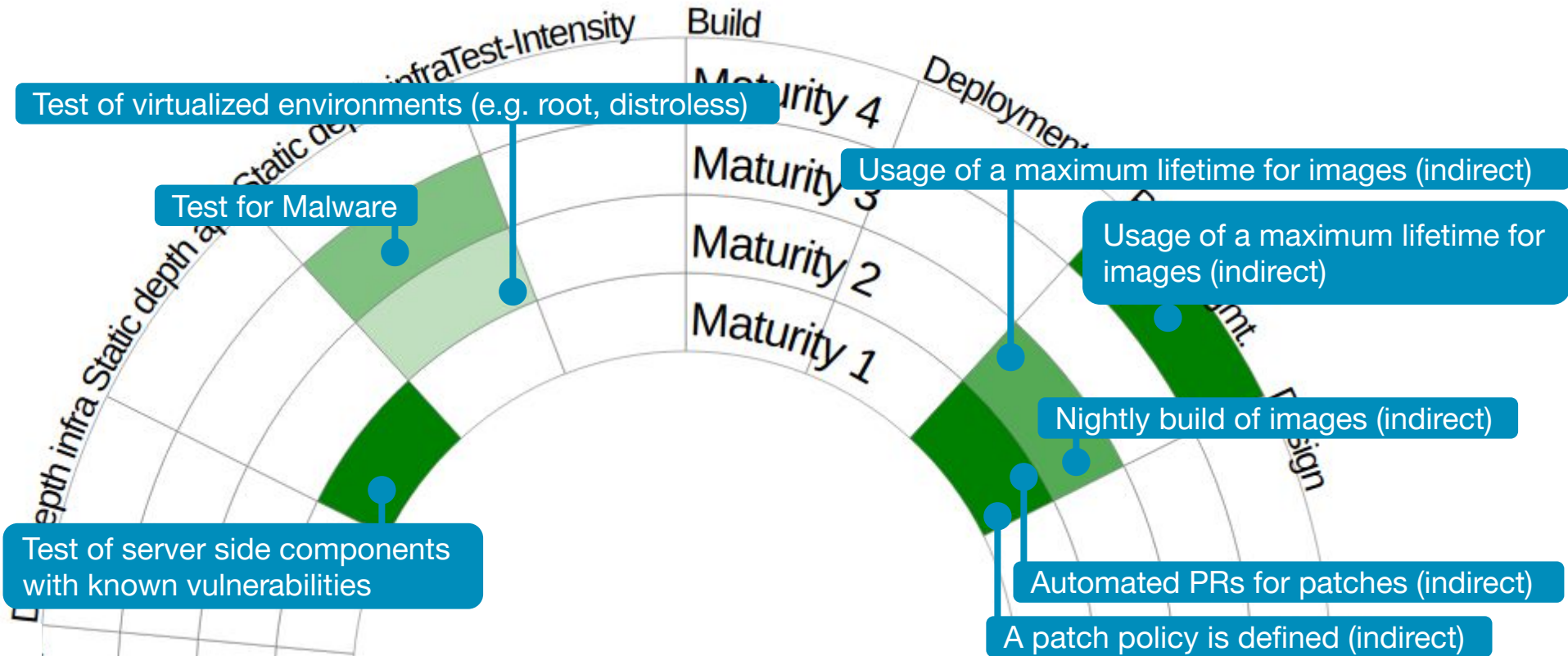


Decision*

- ☒ Accept (The risk is acknowledged, yet remains)
- ☐ Avoid (Do not engage with whatever creates the risk)
- ☐ Mitigate (The risk still exists, yet compensating controls make it less of a threat)
- ☐ Fix (The risk is eradicated)
- ☐ Transfer (The risk is transferred to a 3rd party)

- Deduplicate Findings to detect handled findings

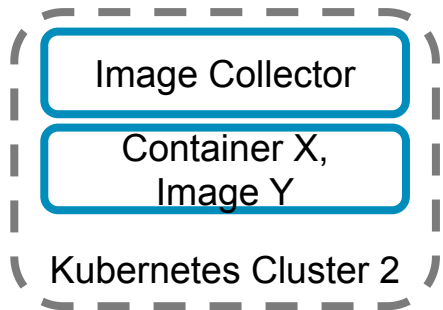
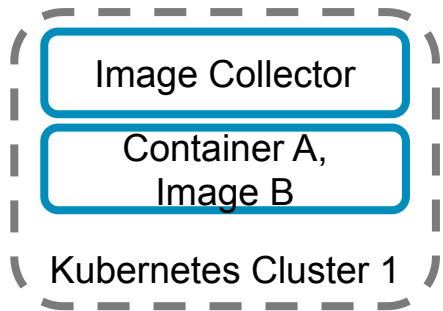
SDA SE ClusterScanner in DSOMM



SDA SE ClusterScanner Overview



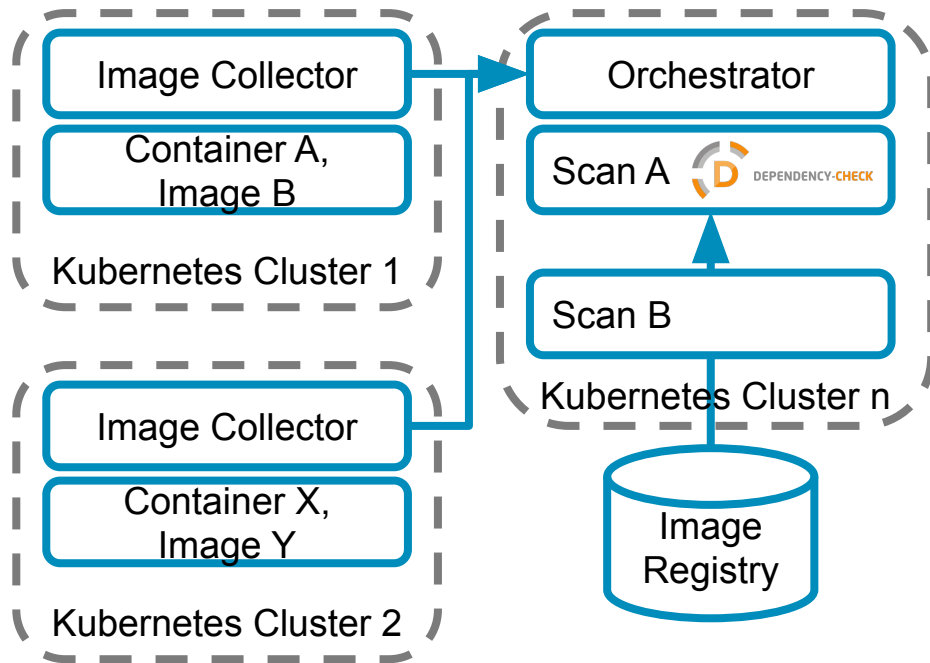
CLUSTER SCANNER



SDA SE ClusterScanner Overview



CLUSTER SCANNER



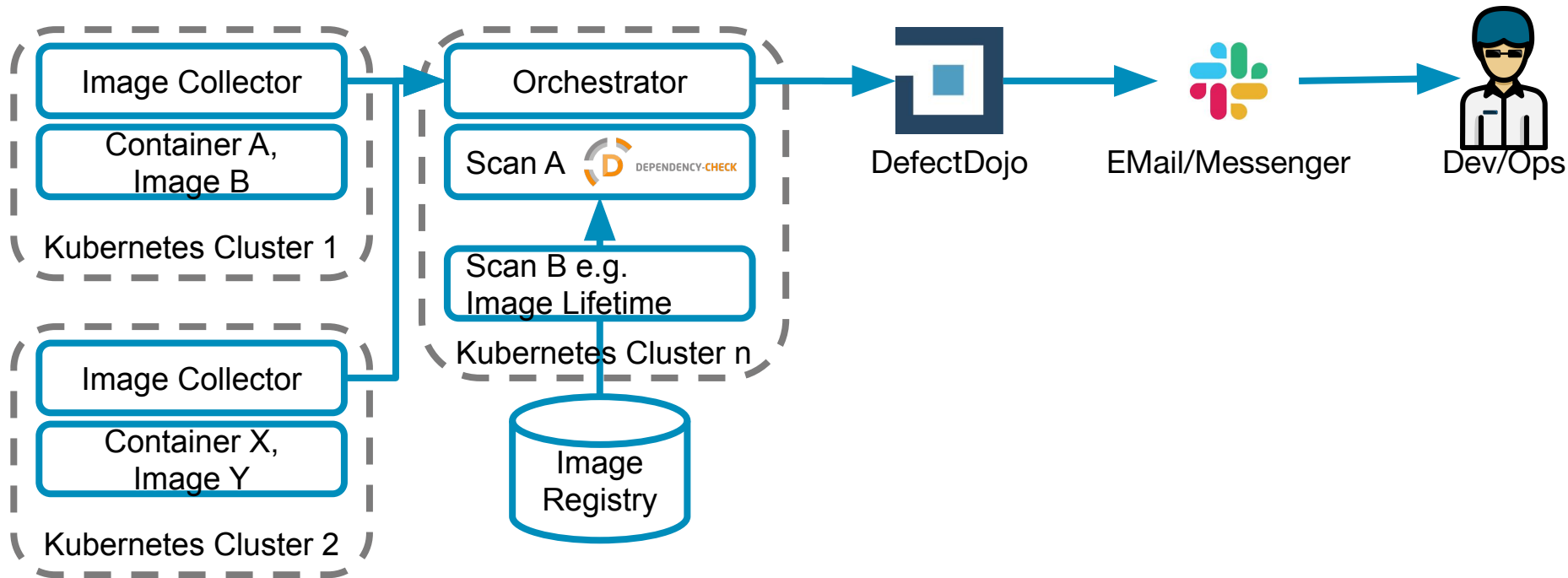
Cluster Scanner + DefectDojo

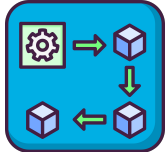


SDA SE ClusterScanner Overview



CLUSTER SCANNER





Build and Deployment



Culture and Organisation



Information Gathering



Hardening



Test and Verification



DSOMM

OWASP AppSensor: What/When




| Logged information | Property |
|--------------------|--------------------------|
| When | Event date/time |
| | Log date/time |
| Security event | Type |
| | Severity |
| | Confidence |
| | Custom classification(s) |
| | Owner |
| Location | Host |
| | Service/application name |
| | Port |
| | Protocol |
| | HTTP method |
| | Entry point |
| | Request number |
| Request | Purpose |
| | Target |
| User | Source |
| | Identity |
| | HTTP user agent |
| | Client fingerprint |

| Logged information | Property |
|---------------------------------------|---------------------------------|
| AppSensor detection | Sensor ID |
| | Sensor location |
| | AppSensor Detection Point ID(s) |
| | Description |
| Optional supporting details | Message |
| | Request headers |
| | Request body |
| | Response headers |
| | Response body |
| | Error stack trace |
| | Error message |
| Result (including AppSensor response) | Other system response |
| | Status |
| | Reason for status |
| | HTTP status code |
| | AppSensor Result Response ID(s) |
| Record integrity | Description |
| | Message |
| | Identity |
| | Hash |

OWASP AppSensor: Detection Points



| Category | Detection Point | |
|-----------------------------|--------------------------|--|
| | Detection Point Category | Title |
| Access Control Exception | ACE1 | Modifying URL Argument Within a GET for Direct Object Access Attempt |
| | ACE2 | Modifying Parameter Within A POST for Direct Object Access Attempt |
| | ACE3 | Force Browsing Attempt |
| | ACE4 | Evading Presentation Access Control Through Custom POST |
| Input Exception | IE1 | Cross Site Scripting Attempt |
| | IE2 | Violation Of Implemented White Lists |
| | IE3 | Violation Of Implemented Black Lists |
| | IE4 | Violation of Input Data Integrity |
| | IE5 | Violation of Stored Business Data Integrity |
| | IE6 | Violation of Security Log Integrity |
| | IE7 | Detect Abnormal Content Output Structure |
| Encoding Exception | EE1 | Double Encoded Character |
| | EE2 | Unexpected Encoding Used |
| Command Injection Exception | CIE1 | Blacklist Inspection for Common SQL Injection Values |
| | CIE2 | Detect Abnormal Quantity of Returned Records |
| | CIE3 | Null Byte Character in File Request |
| | CIE4 | Carriage Return or Line Feed Character in File Request |
| File IO Exception | FIO1 | Detect Large Individual File |
| | FIO2 | Detect Large Number of File Uploads |

- Open Source/Knowledge is startup and enterprise ready
- > Even for security
-  OWASP[®] provides a lot of useful projects

Questions?



DSOMM

OWASP Amaas

OWASP: timo.pagel@owasp.org

Business: owasp21@pagel.pro

