



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



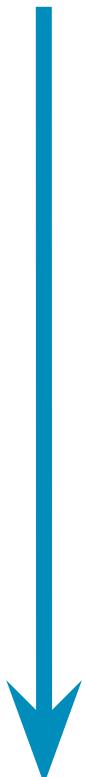
Timo Pagel

Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



High Level

ISMS



Doing

Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



High Level



ISMS



OWASP SAMM

...

SAMM
Practices



Implementation



Governance



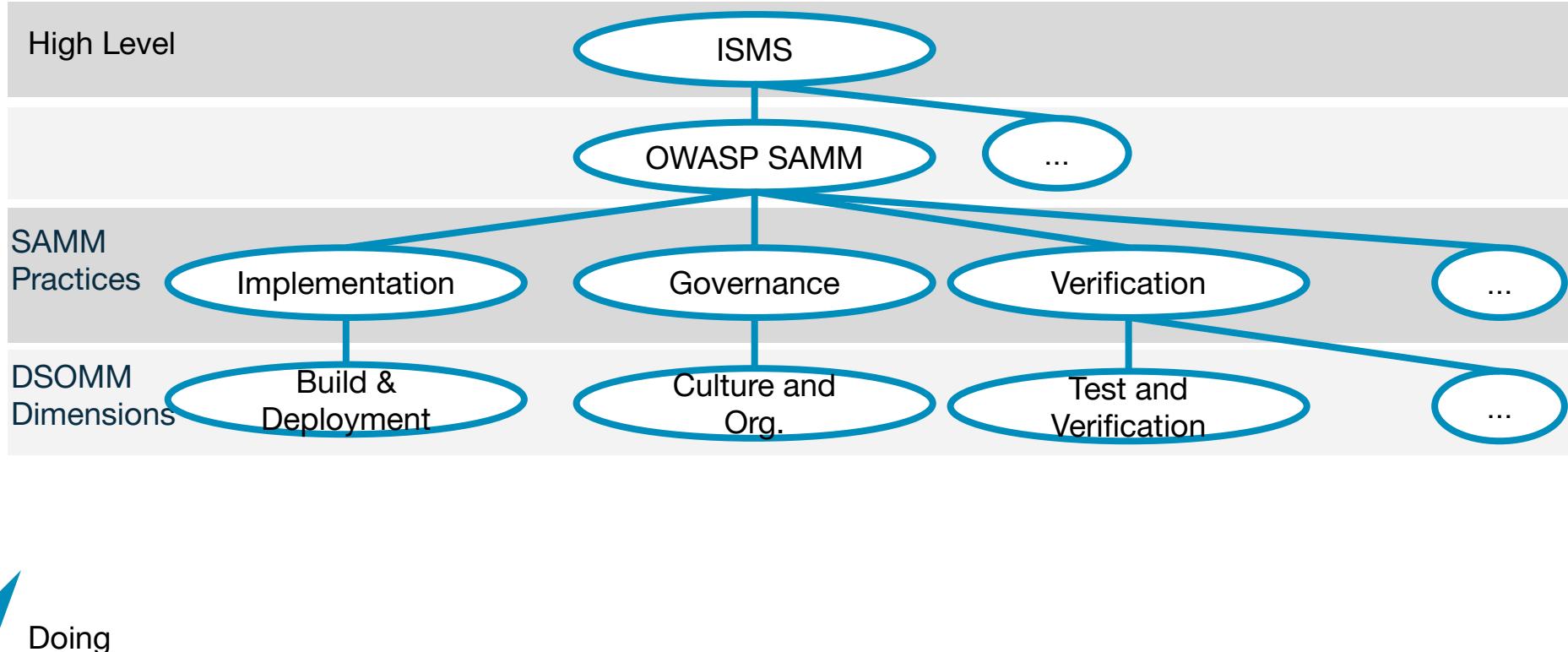
Verification

...



Doing

Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



High Level



...

SAMM Practices



...

DSOMM Dimensions



...

DSOMM Dynamic Depth Activities



...



...

Doing

SAMM and DSOMM

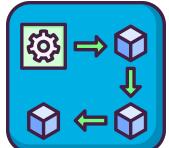


- “Standard”
 - > High level overview
 - Management topics like compliance and governance
 - Planning of high level targets
 - Mapping to ISO in the future



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

DevSecOps Dimensions



Build and Deployment



Culture and Organisation



Information Gathering



Hardening

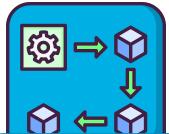


Test and Verification



DSOMM

DevSecOps Dimensions



Build and Deployment



Culture and Organisation



Information Gathering



Hardening



Test and Verification



DSOMM

Security Champions playbook



Identify teams

Define the role

Nominate champions

Comm channels

Knowledge base

Maintain interest

Knowledge Through Training



*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 A blue outline icon of a hand with fingers spread, representing a high-five gesture.



Possible Rewards / Motivations



- High-Fives 
- Pins



Pro/Con Pins



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



Pro/Con Pins



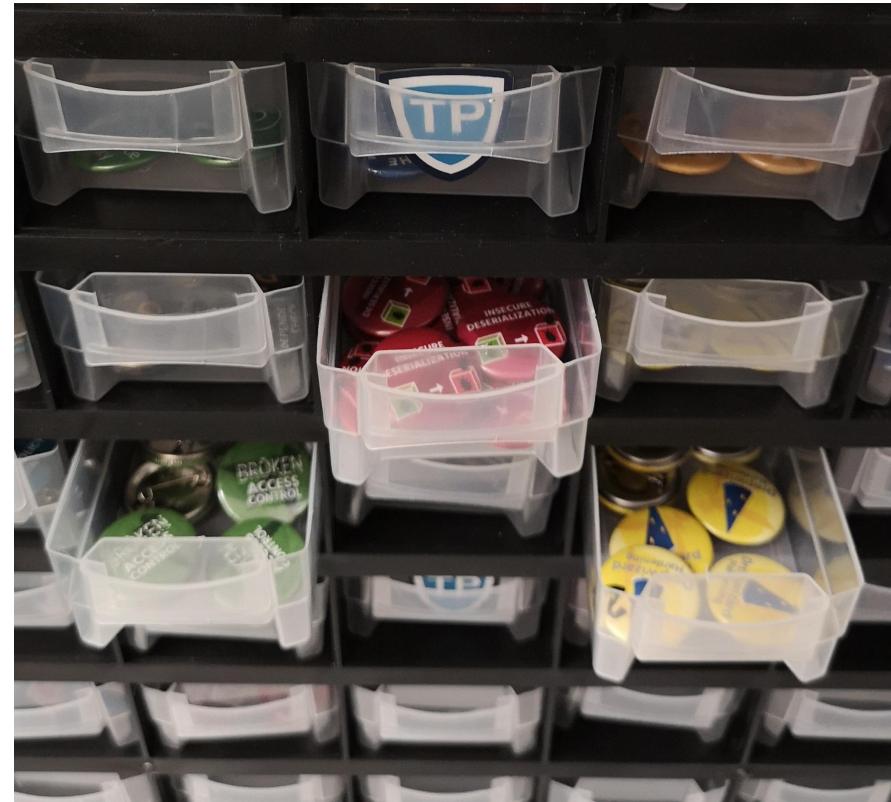
- Reminder
 - Fast achievements
 - Gamification: “We want to collect all pins”
 - Transforms non touchable security into
touchable security
-
- Needs to be designed and produced



Implementation



Implementation



Virtual COVID-19 way: Backstage at SDA SE



backstage.sda-se.io

GROUP — TEAM
team-dock-marshals ☆

Owner unknown Lifecycle unknown

OVERVIEW

Team Dock Marshals
Team Dock Marshals

TD [sda_se_open_industry_solutions]

Security Champions

SECURITY CHAMPION
Dominik Henneke (Oliver Sand)

SECURITY PINS (38)

Learn more →

Ownership

2 Services	0 Documentation	0 APIs
0 Libraries	2 Websites	0 Tools

Members (3)
of Team Dock Marshals

Domík Henneke (TD)
Oliver Sand (PE)
Philipp Ermisch (PE)

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

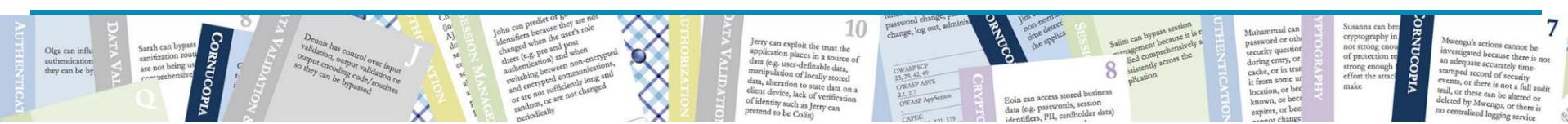
Embed TM
in your
organization

Train your
people to
TM

Strengthen
your TM
processes

Innovate
with TM
technology

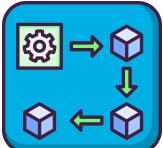
Threat Modeling: What can go wrong?



- 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

DevSecOps Dimensions



Build and Deployment



DSOMM



Culture and Organisation



Information Gathering



Hardening

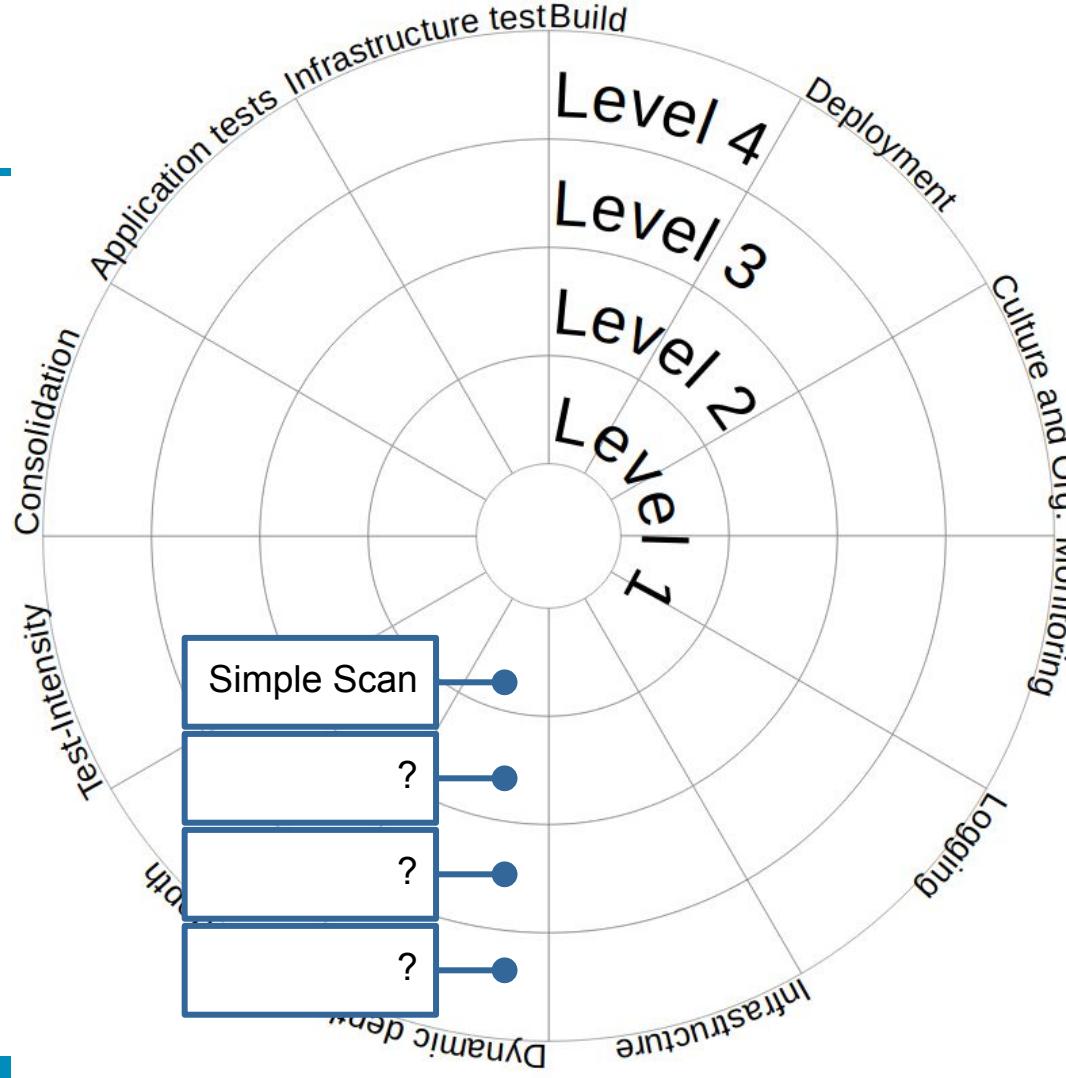


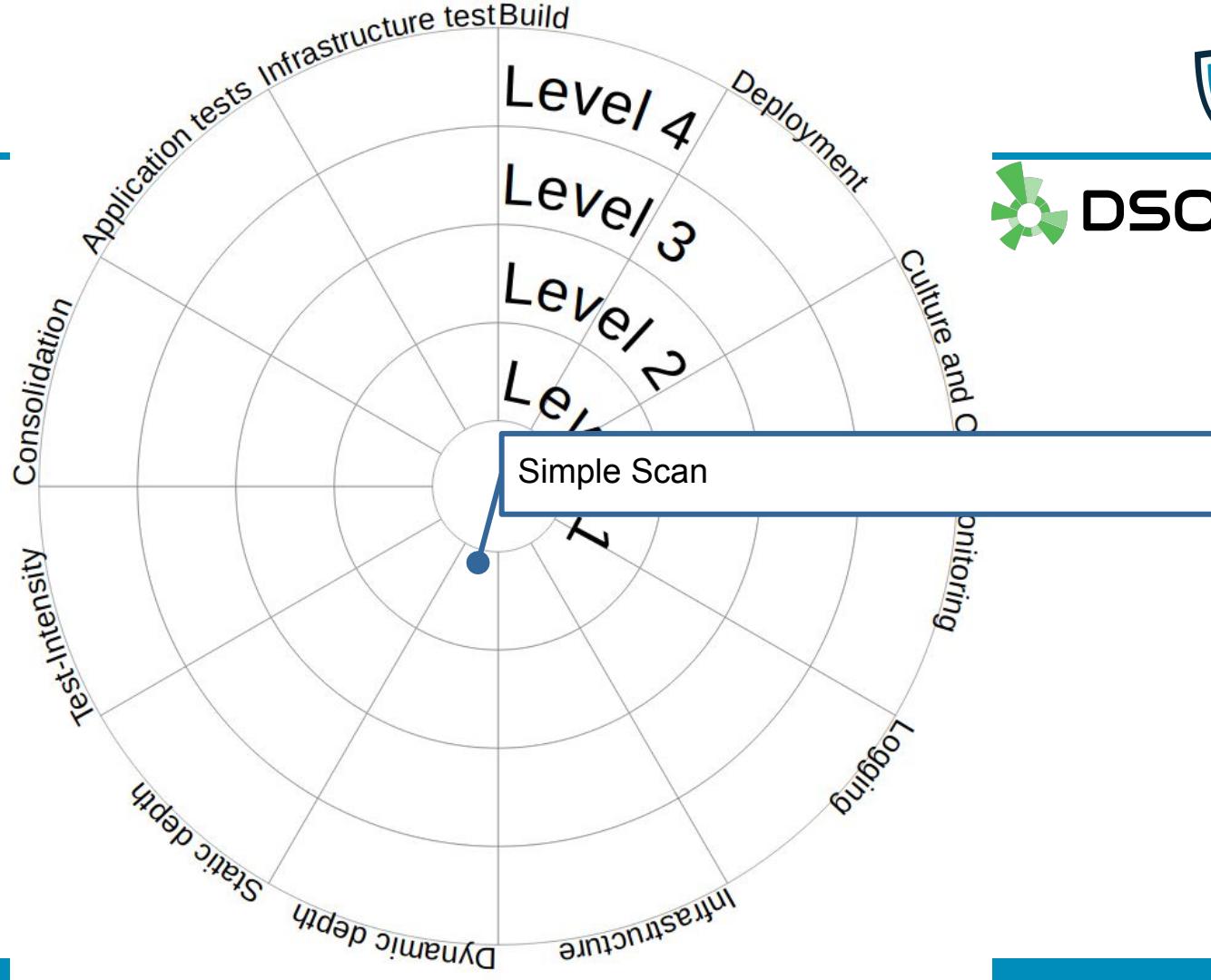
Test and Verification

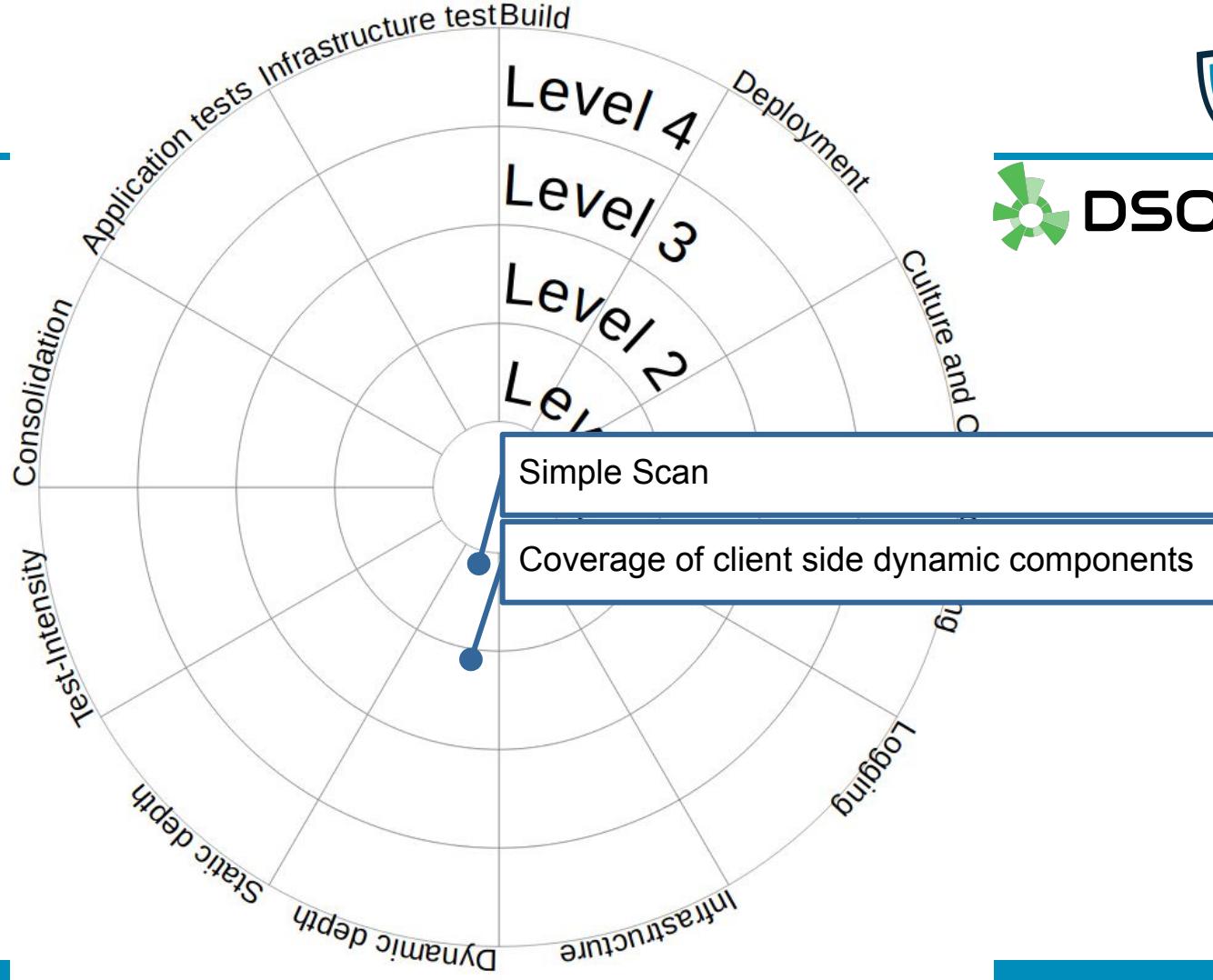
Dynamic depth for applications

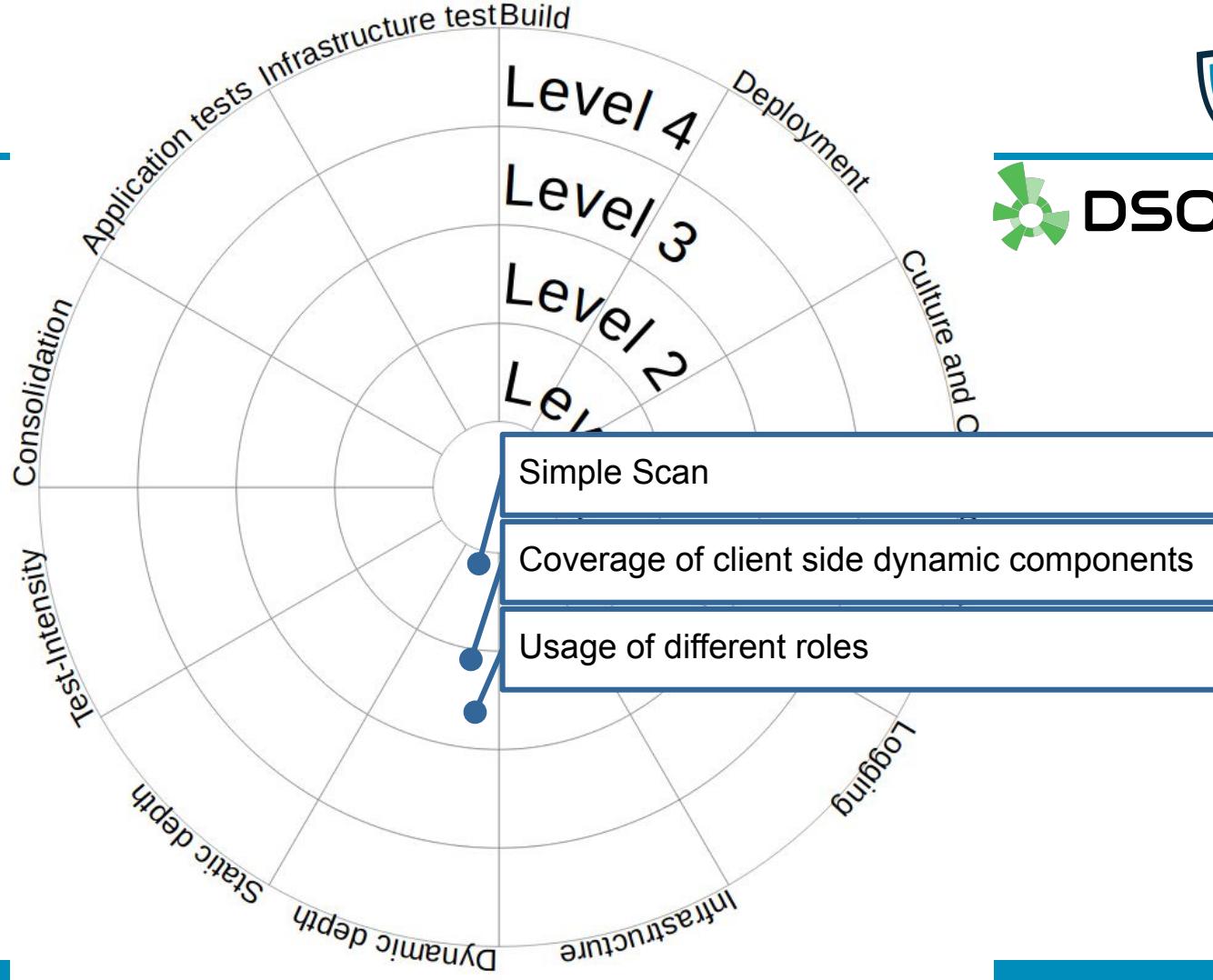


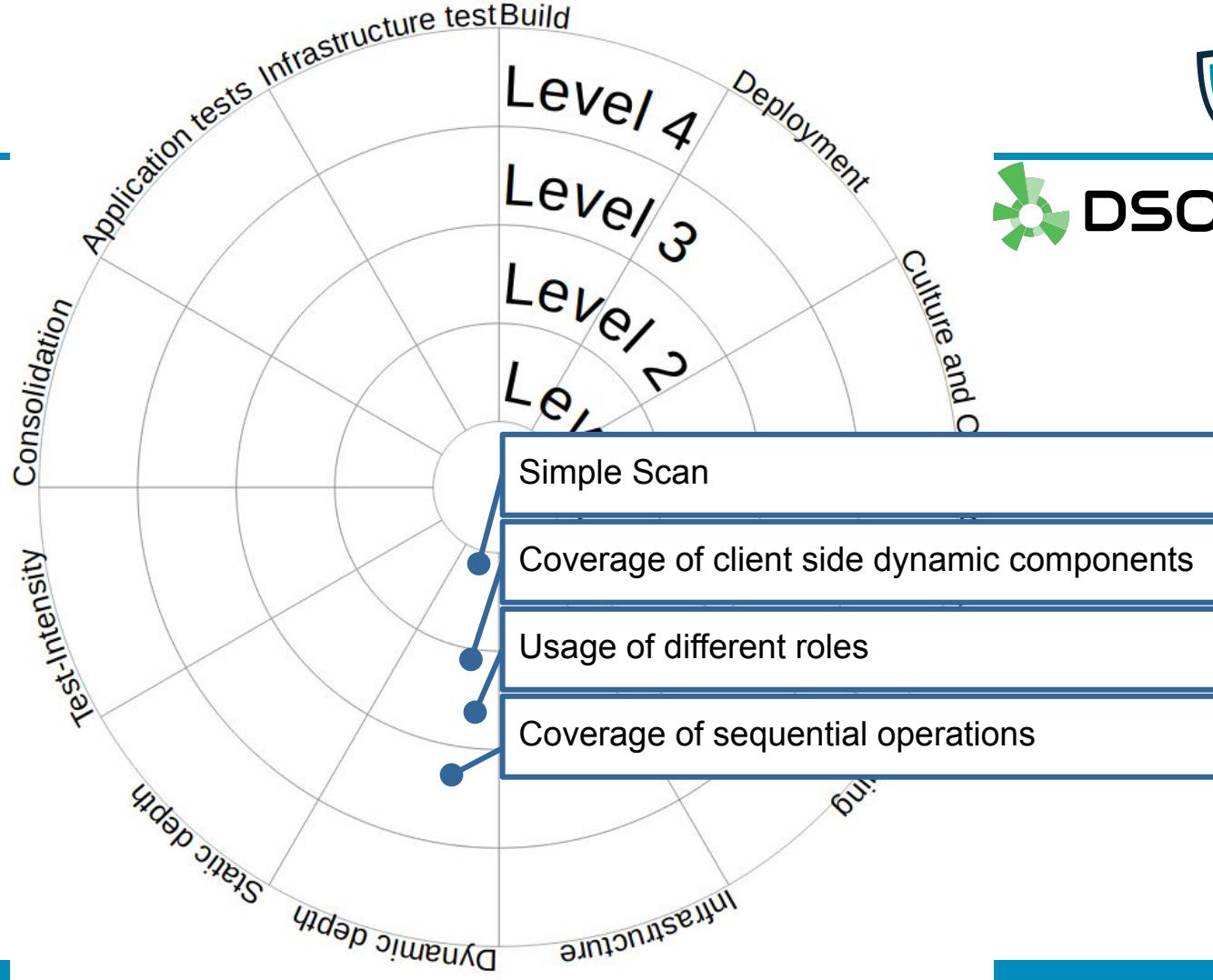
DSOMM

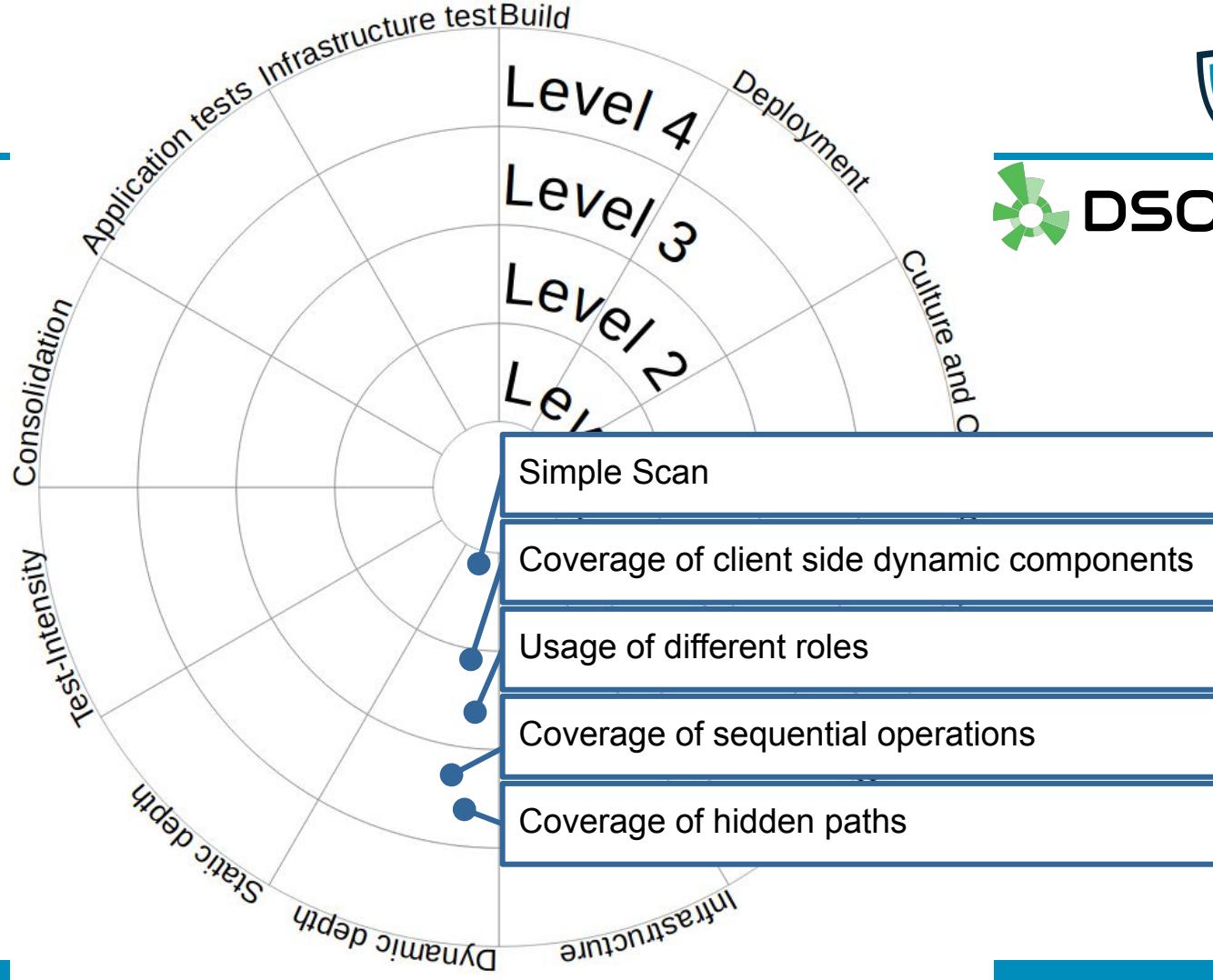


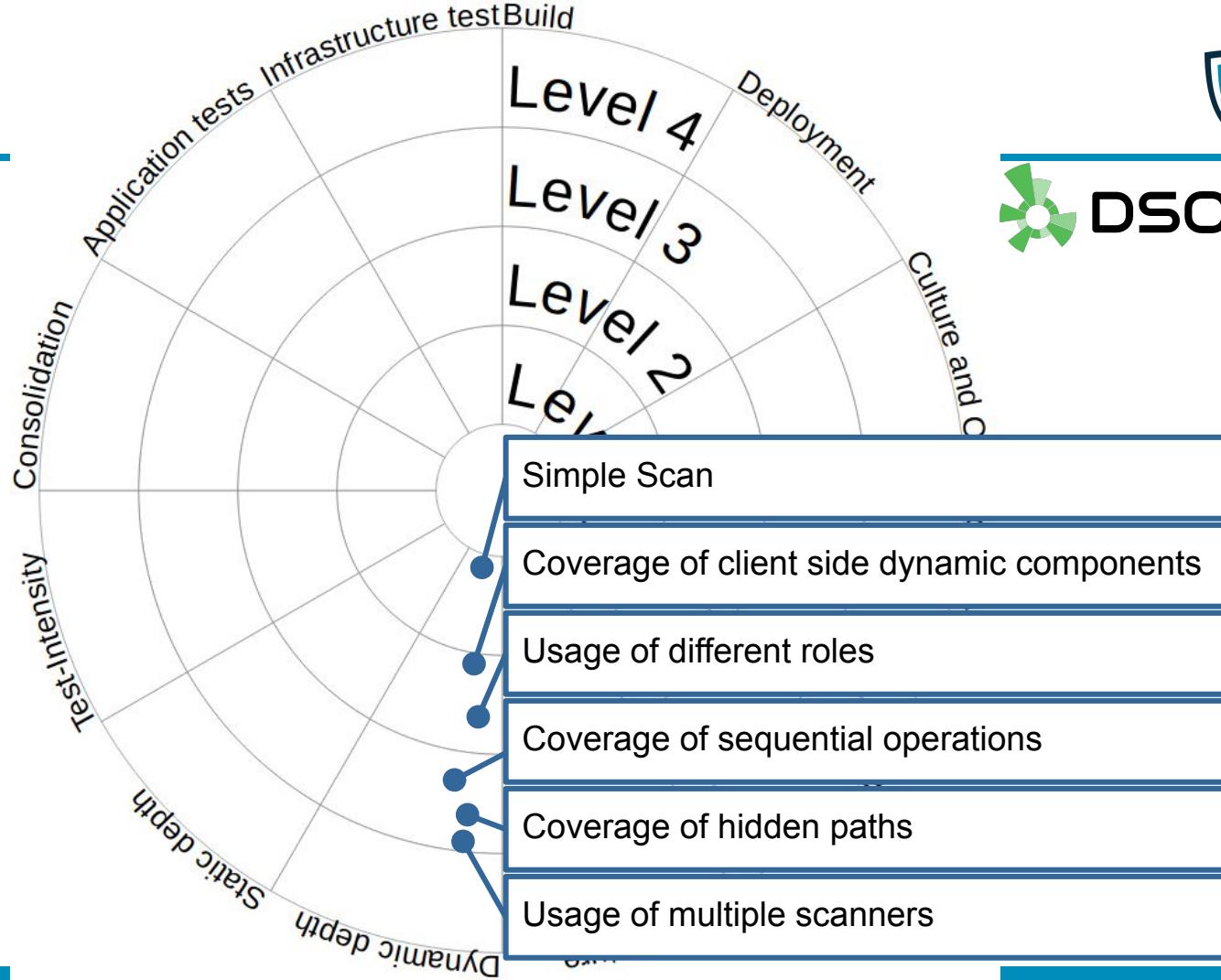




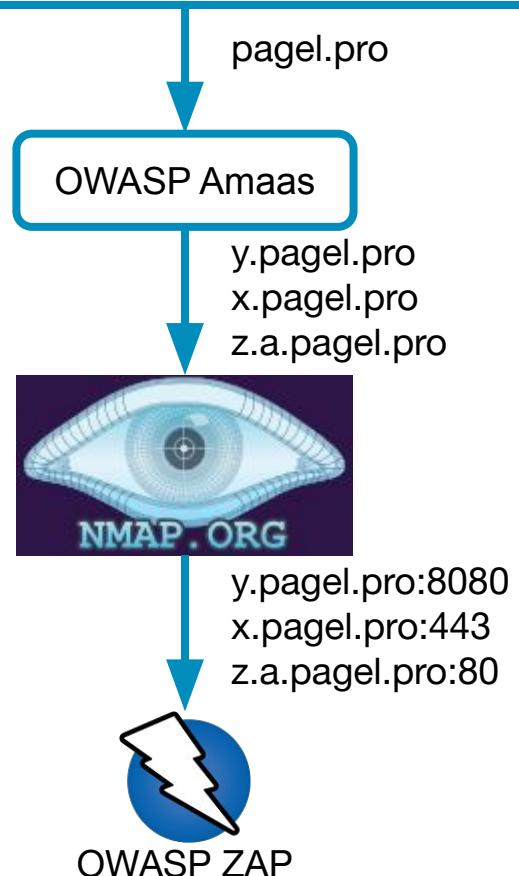


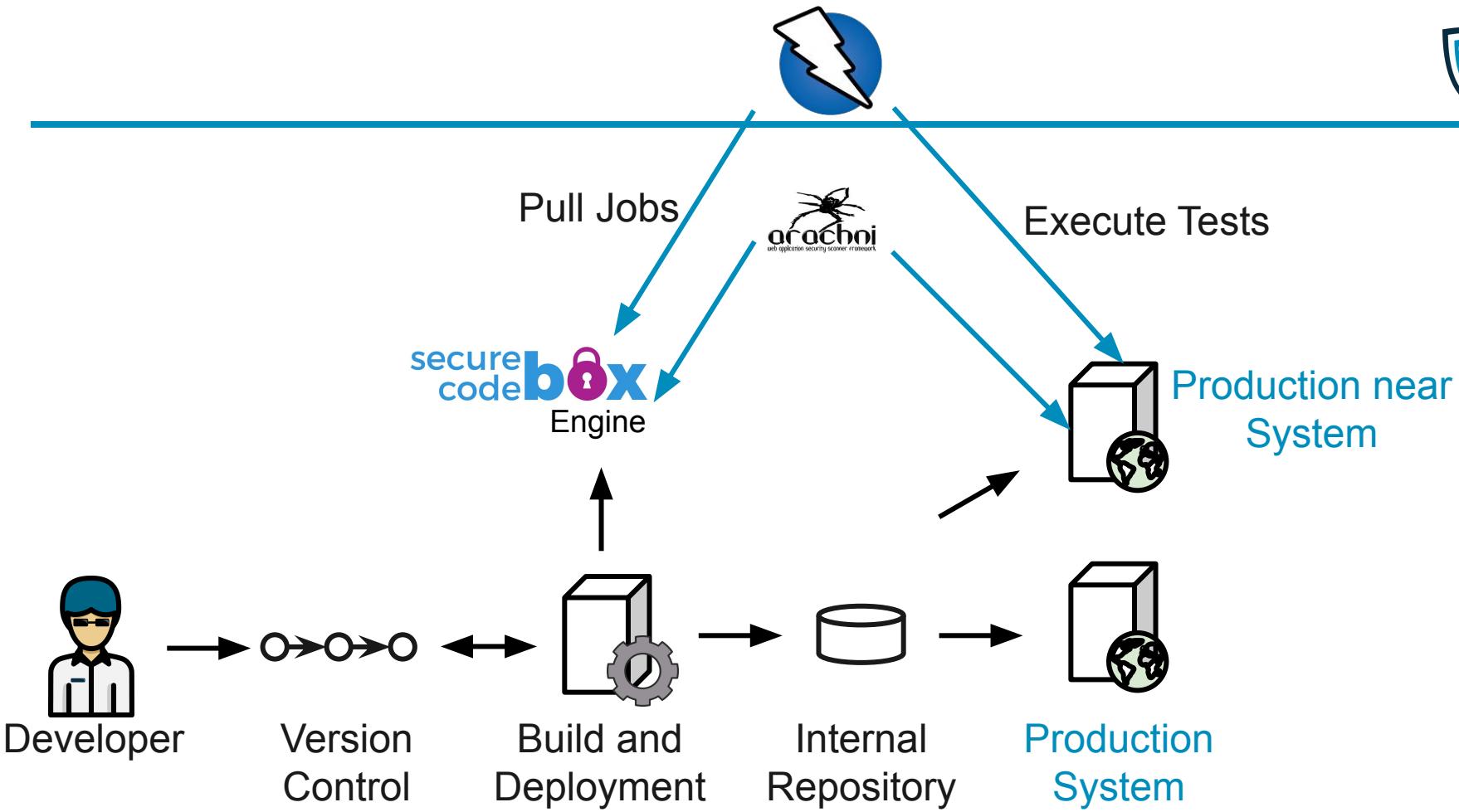






Web Security Testing of (an unknown) Enterprise World

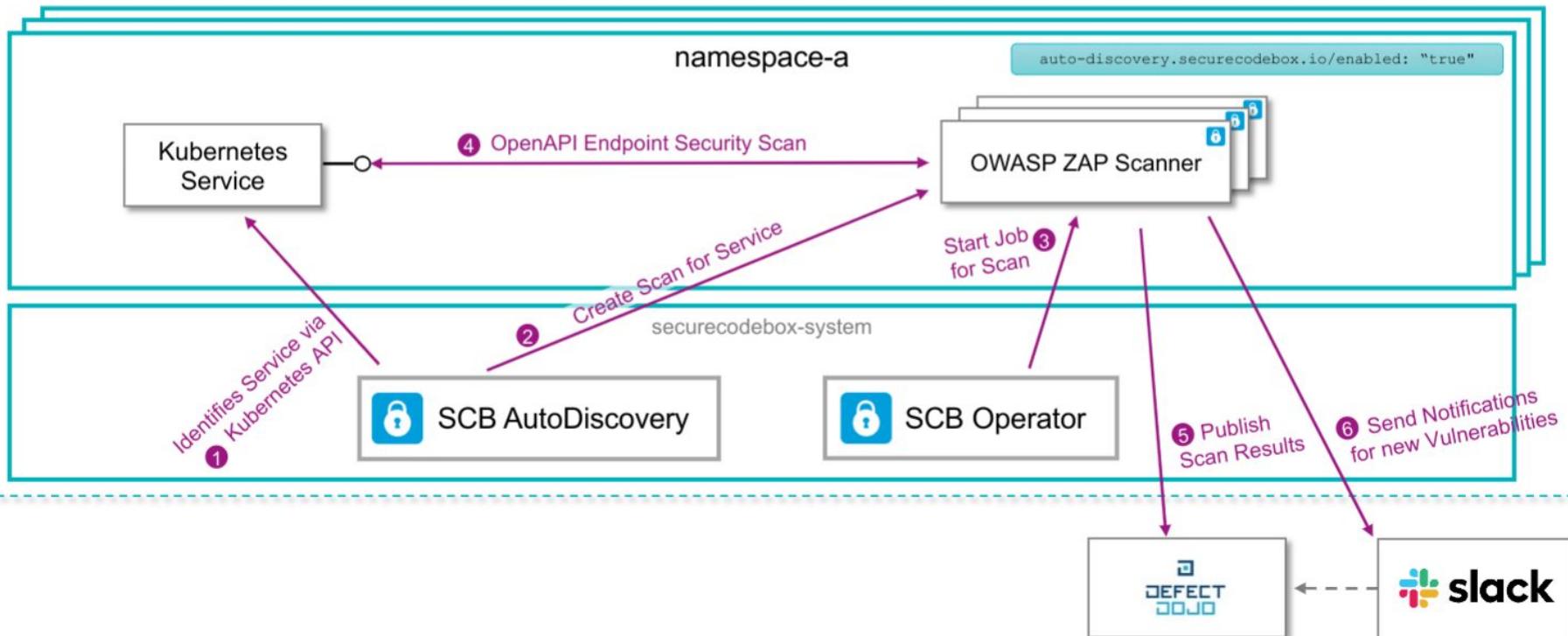




OWASP securecode**box**: New Way



Target Cluster (DEV)



Vulnerability Management System: Deduplication



● Handle Findings

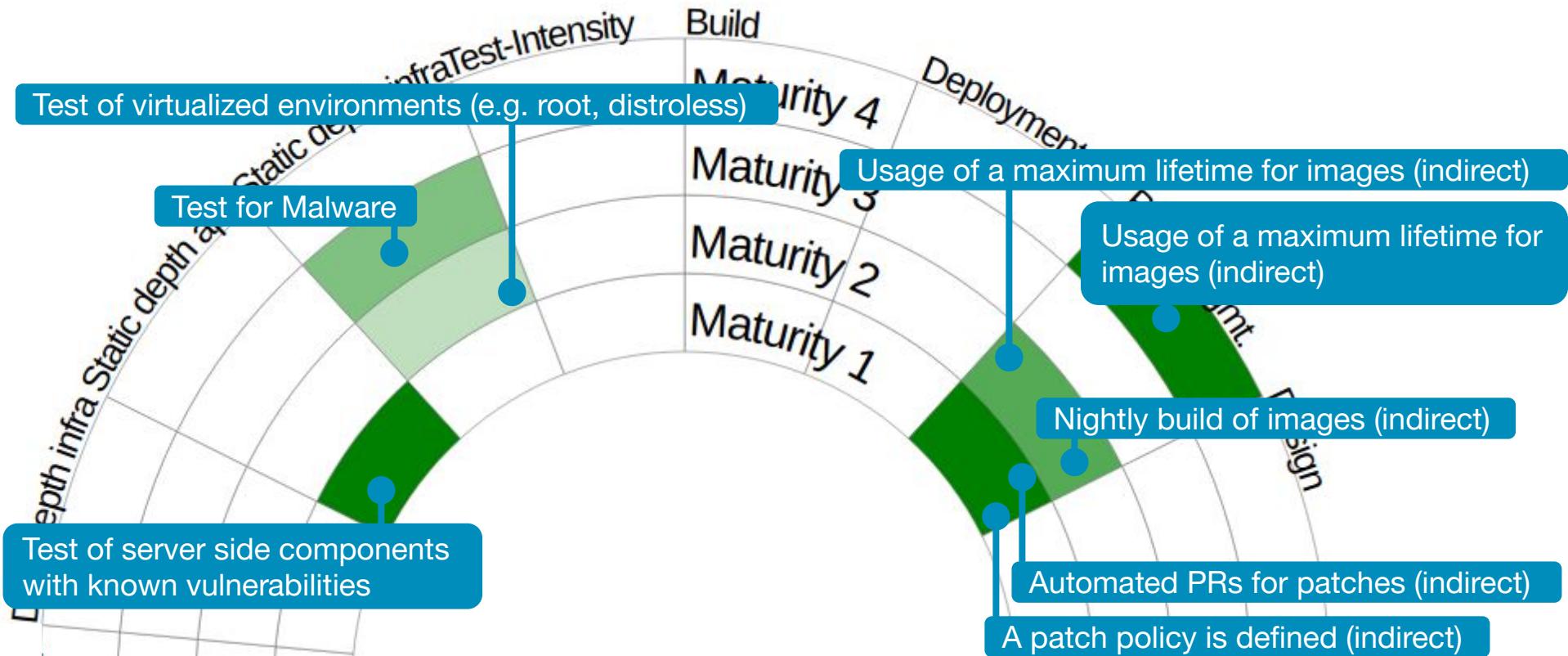


Decision*

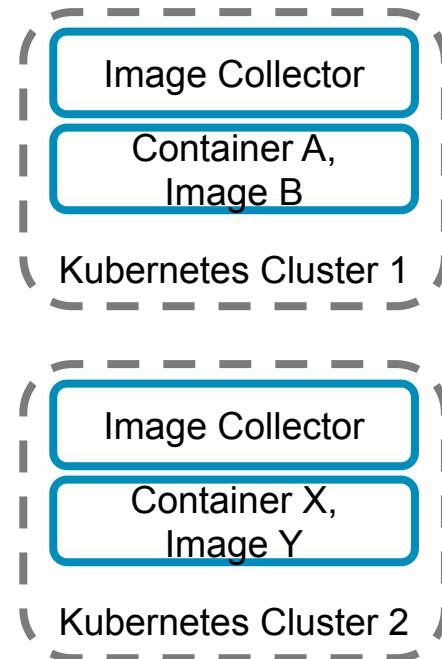
- Accept (The risk is acknowledged, yet remains)
- Avoid (Do not engage with whatever creates the risk)
- Mitigate (The risk still exists, yet compensating controls make it less of a threat)
- Fix (The risk is eradicated)
- Transfer (The risk is transferred to a 3rd party)

● Deduplicate Findings to detect handled findings

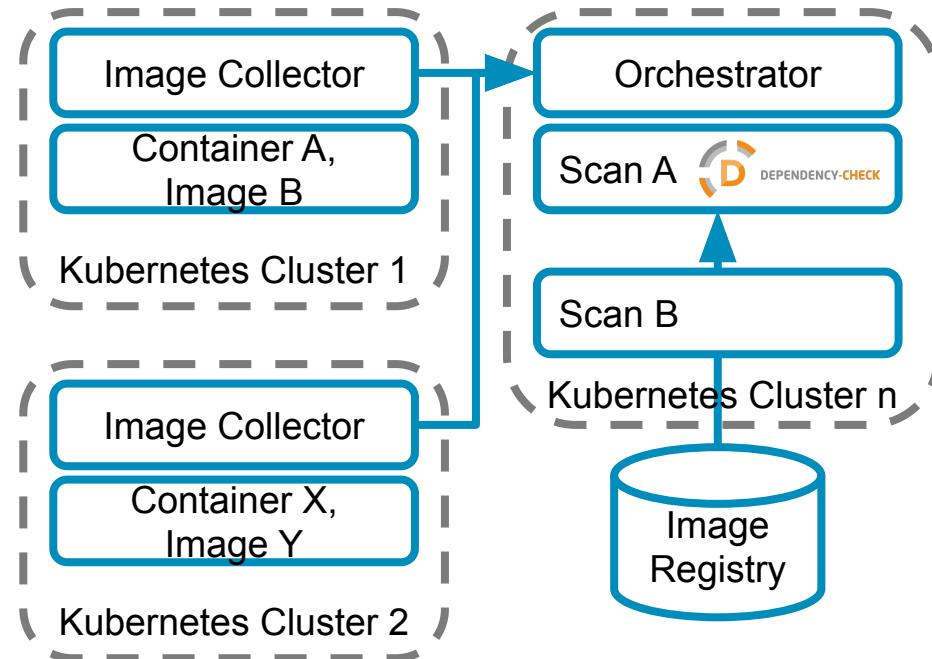
SDA SE ClusterScanner in DSOMM



SDA SE ClusterScanner Overview



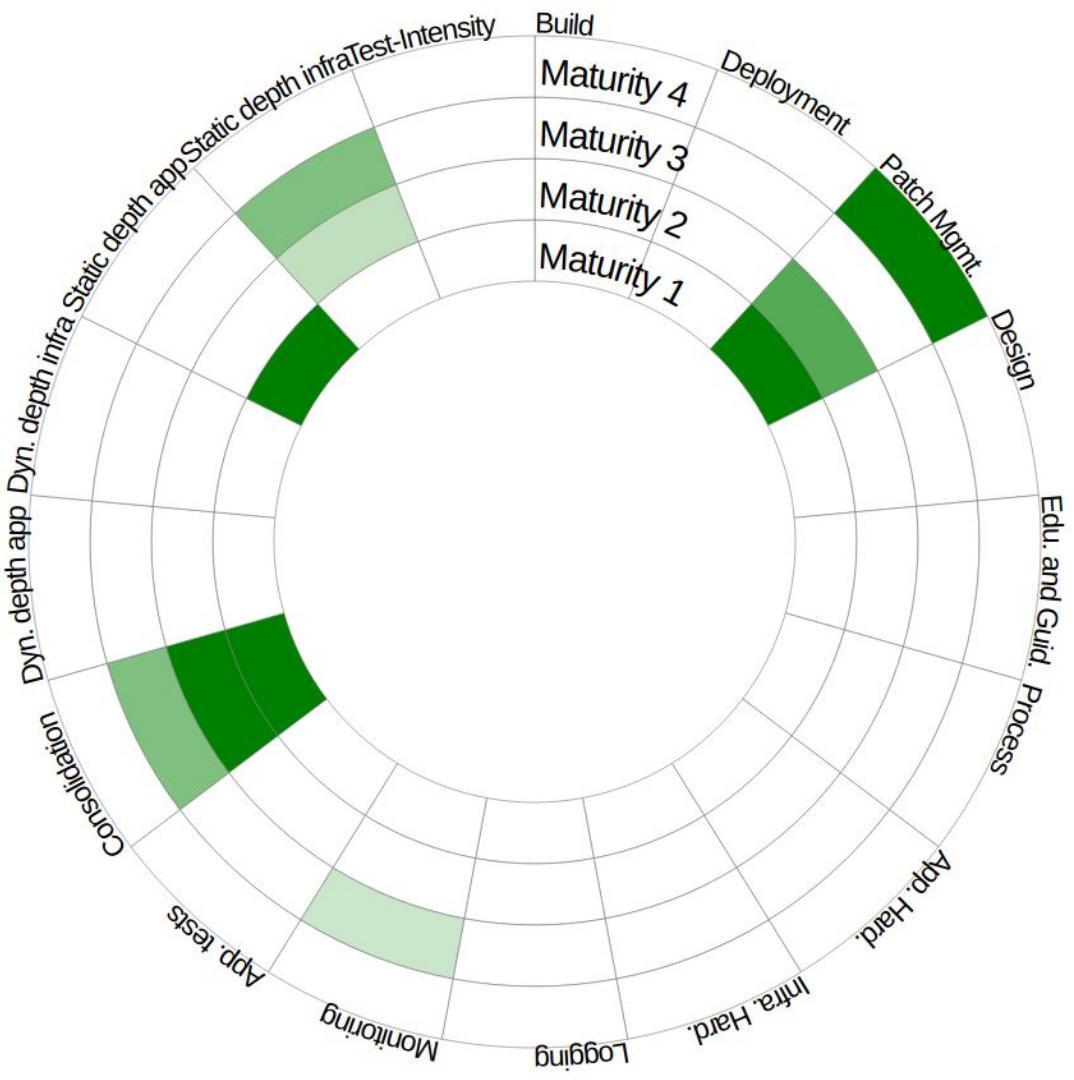
SDA SE ClusterScanner Overview



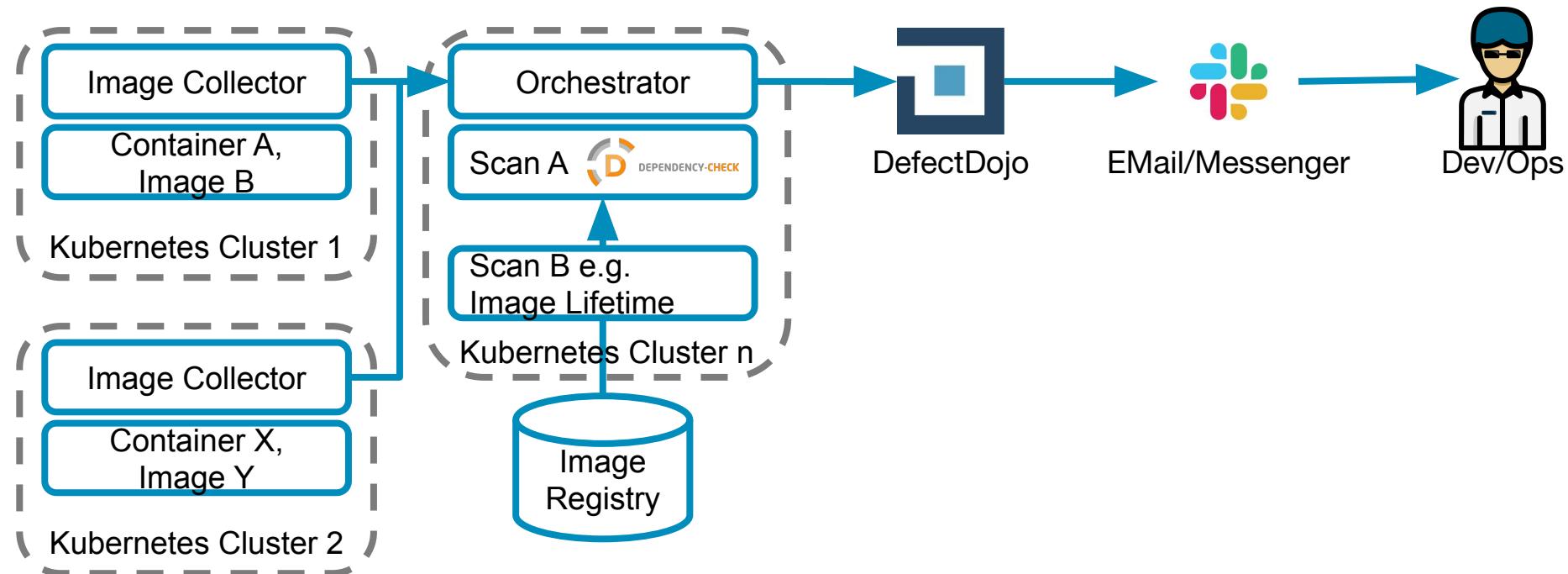
Cluster Scanner

+

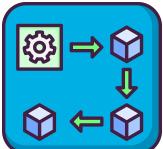
DefectDojo



SDA SE ClusterScanner Overview



DevSecOps Dimensions



Build and Deployment



DSOMM



Culture and Organisation



Information Gathering



Hardening



Test and Verification

OWASP AppSensor: What/When



Logged information	Property	Logged information	Property
When	Event date/time Log date/time	AppSensor detection	Sensor ID Sensor location AppSensor Detection Point ID(s) Description Message
Security event	Type Severity Confidence Custom classification(s) Owner	Optional supporting details	Request headers Request body Response headers Response body Error stack trace Error message Other system response
Location	Host Service/application name Port Protocol HTTP method Entry point Request number	Result (including AppSensor response)	Status Reason for status HTTP status code AppSensor Result Response ID(s) Description Message
Request	Purpose Target	Record integrity	Identity Hash
User	Source Identity HTTP user agent Client fingerprint		

OWASP AppSensor: Detection Points



Category	Detection Point	
Detection Point Category	ID	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

Conclusion



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

Questions?



OWASP Amaas

OWASP: timo.pagel@owasp.org

Business: owasp21@pagel.pro

