Overview of (DevSecOps) OWASP Projects

OWASP Stammtisch Frankfurt

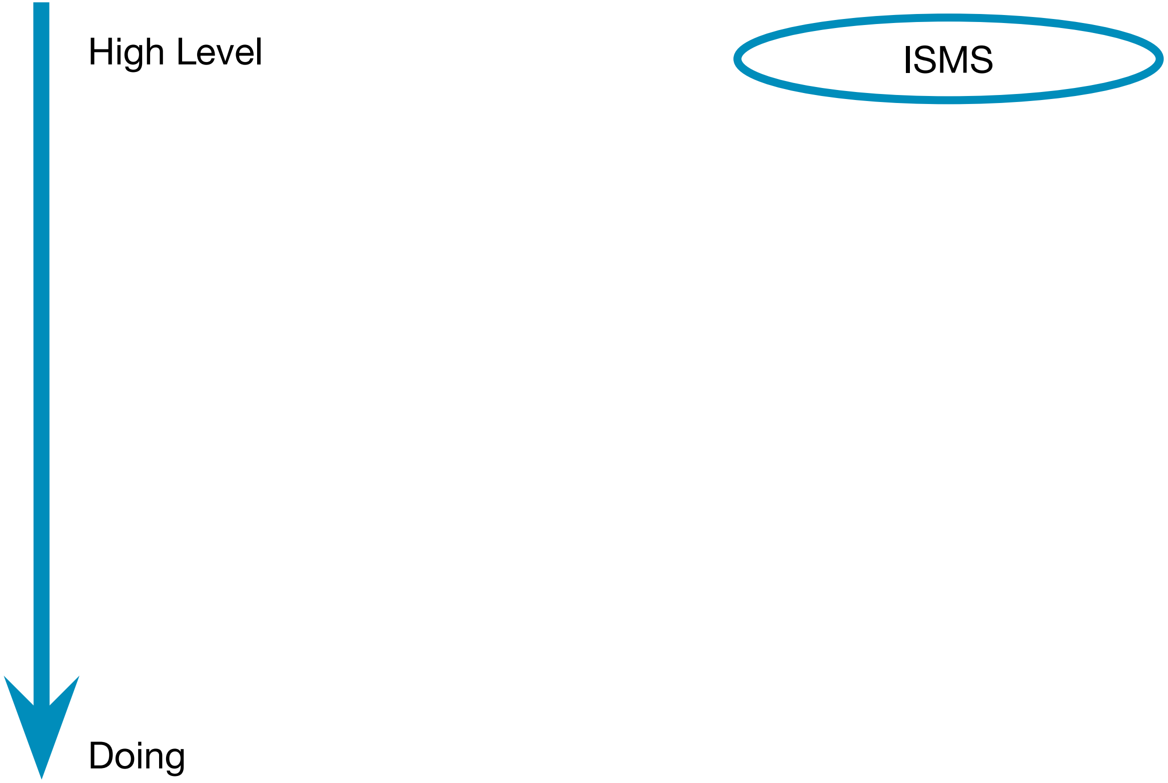
2021-04-28

Timo Pagel

/bin/whoami

- 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

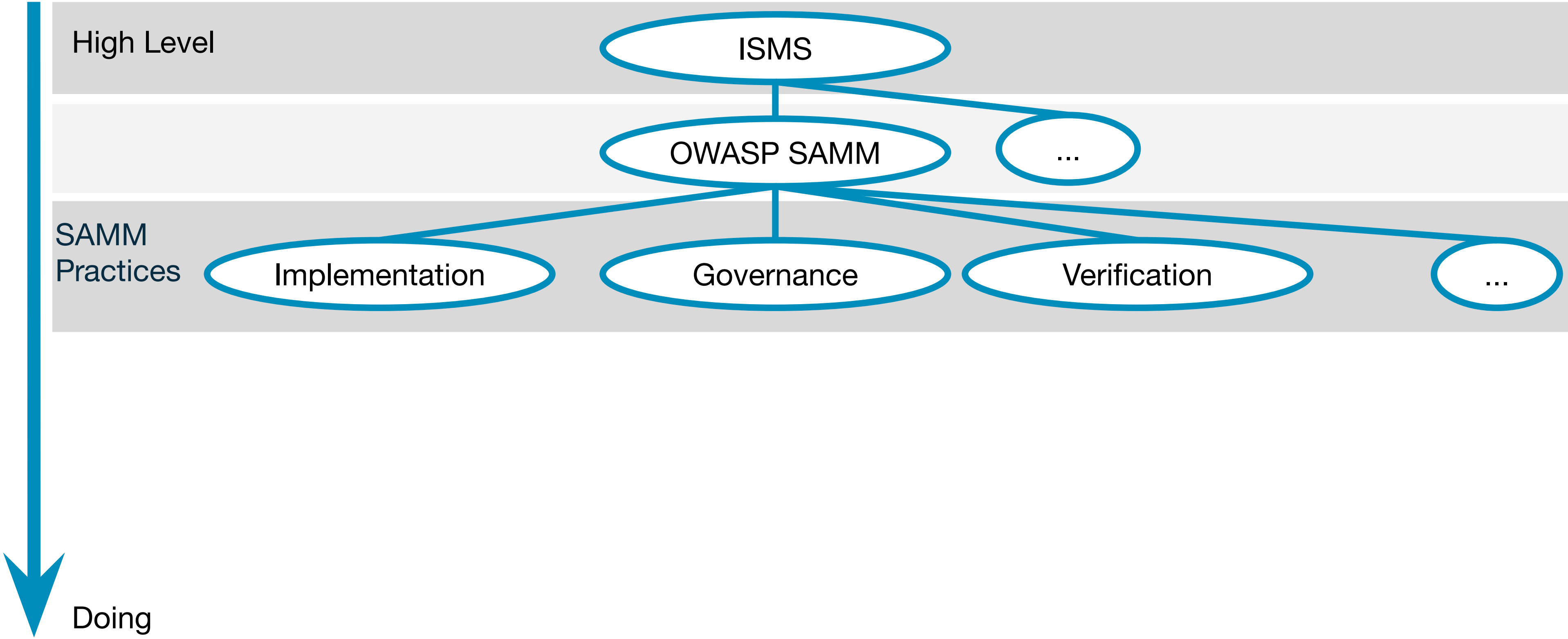


High Level

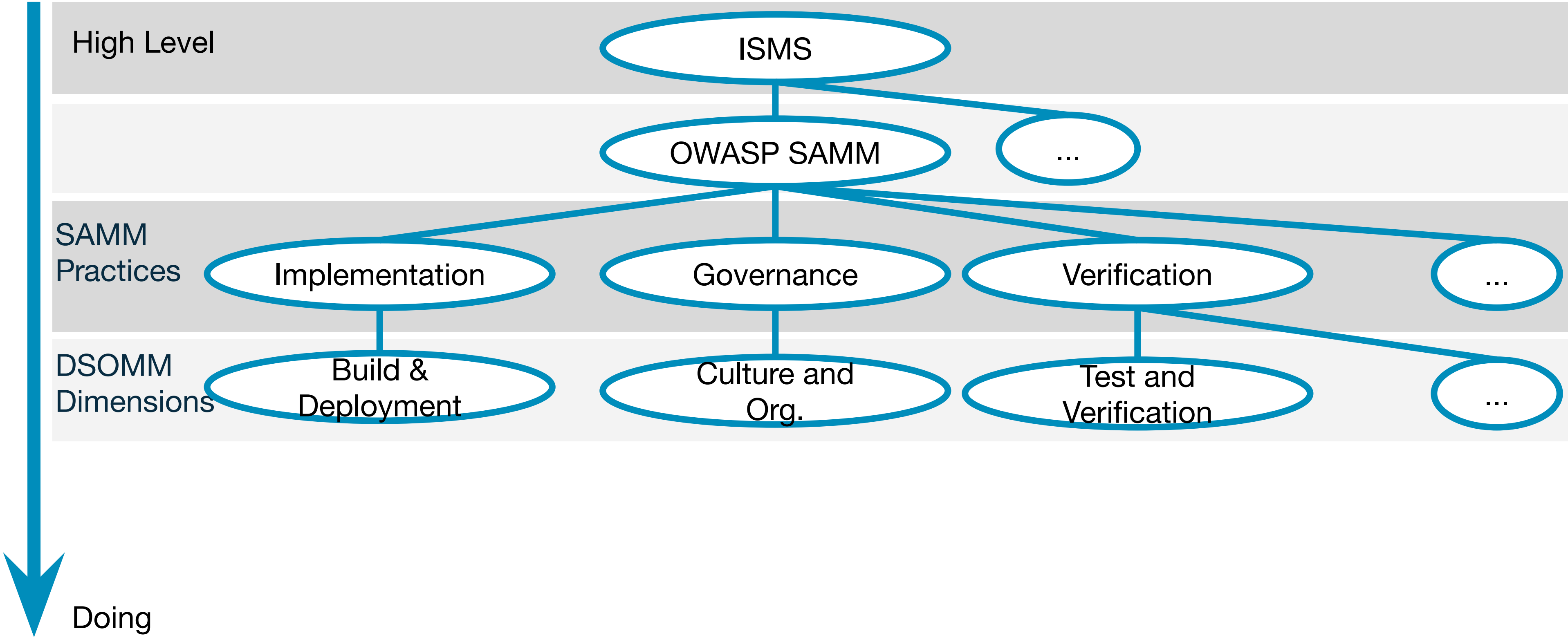
ISMS

Doing

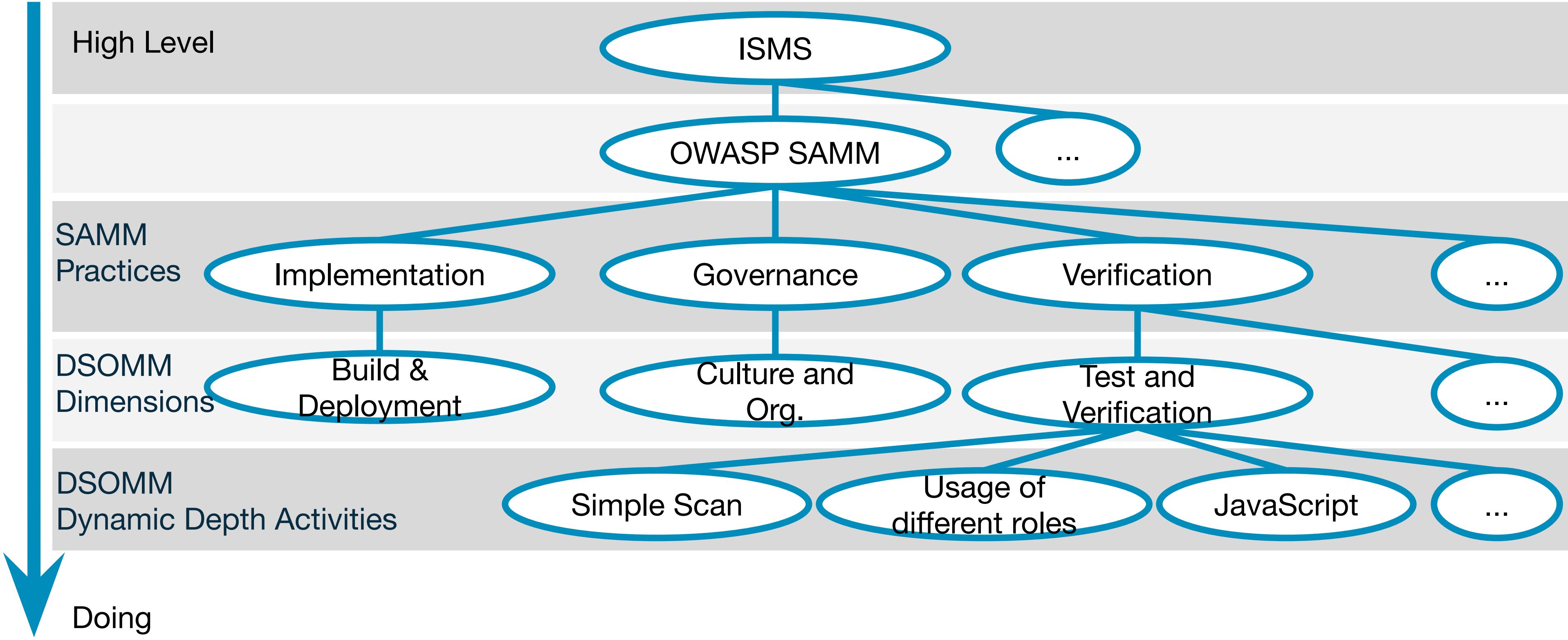
Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM



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

DevSecOps Dimensions

DSOMM

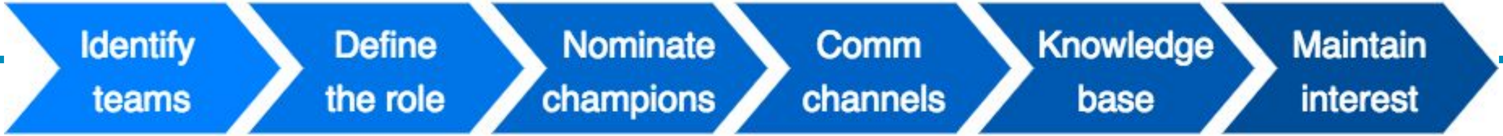
- Build and Deployment
- Culture and Organisation
- Information Gathering
- Hardening
- Test and Verification

DevSecOps Dimensions

DSOMM

- Build and Deployment
- 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

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

OWASP Top 10 2017, German, https://wiki.owasp.org/images/9/90/OWASP_Top_10-2017_de_V1.0.pdf

Possible Rewards / Motivations

- High-Fives ✋

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

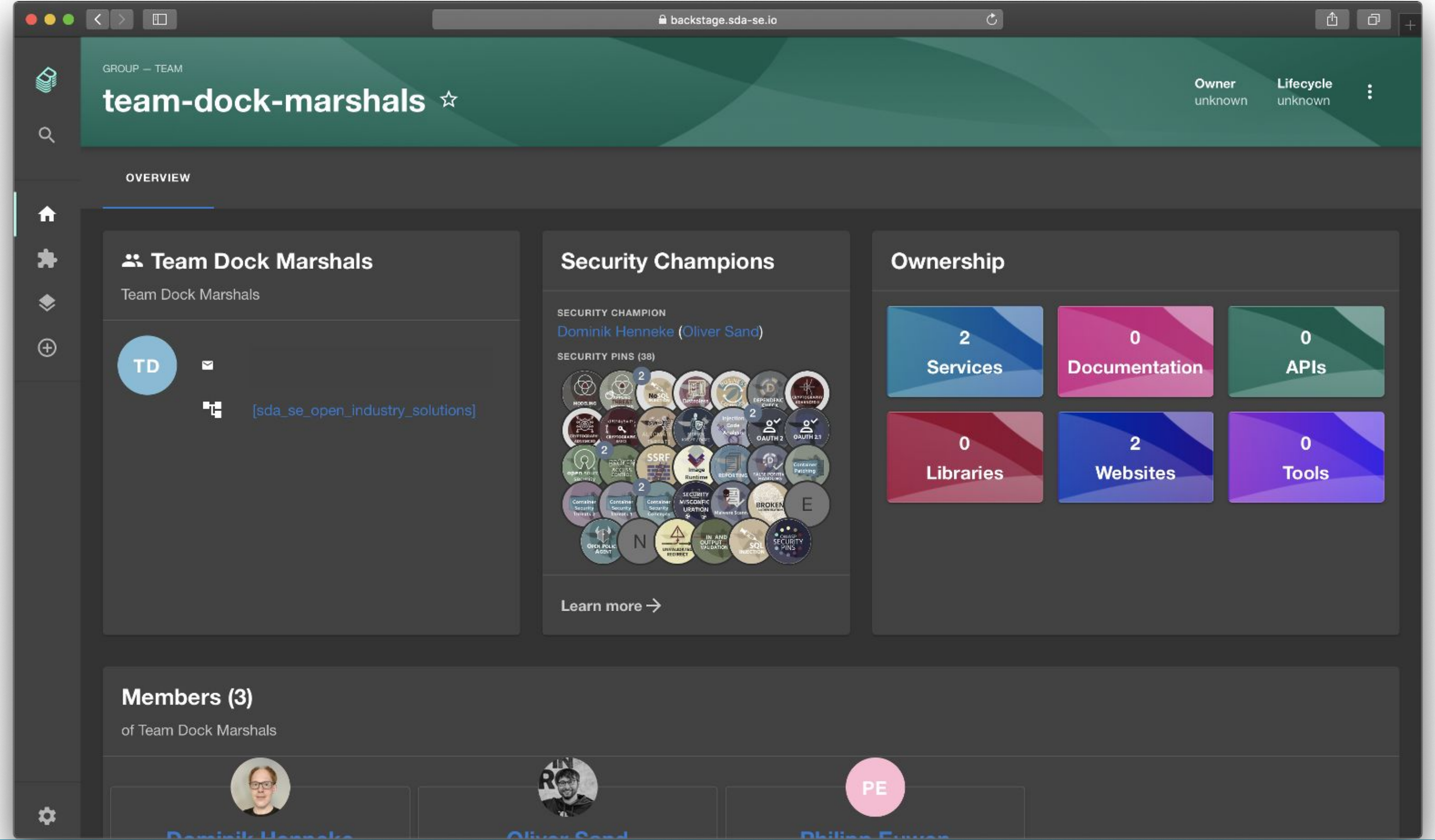
Implementation

OWASP Pins Project: https://owasp.org/www-project-security-pins/

Implementation

OWASP Pins Project: https://owasp.org/www-project-security-pins/

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

Training Rewards

OWASP Pins Project: https://owasp.org/www-project-security-pins/

Nudging (Reminder)

- “Steer people in particular directions”
- E.g. road signs

-> Security pins on a hat

- Reminder of topics

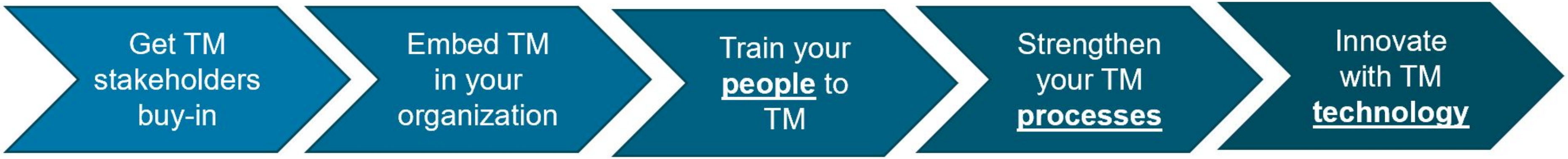
Based on: Nudging: A Very Short Guide, https://dash.harvard.edu/bitstream/handle/1/16205305/shortguide9_22.pdf?sequence=4

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

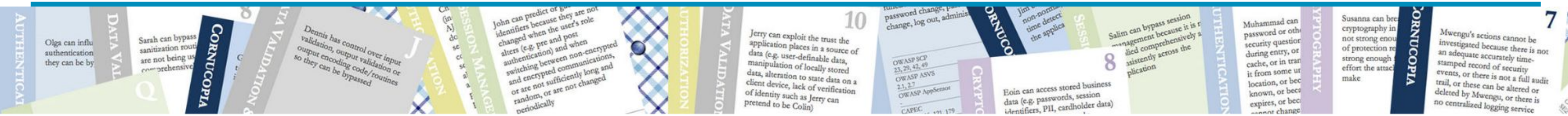
Embed TM in your organization

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

Source: Simon Gibbs, 2020, https://agilestationery.co.uk/blogs/pp/how-to-play-eop-and-cornucopia-remotely, Picture/Project Source https://owasp.org/www-project-cornucopia/

DevSecOps Dimensions

Build and Deployment

Culture and Organisation

Information Gathering

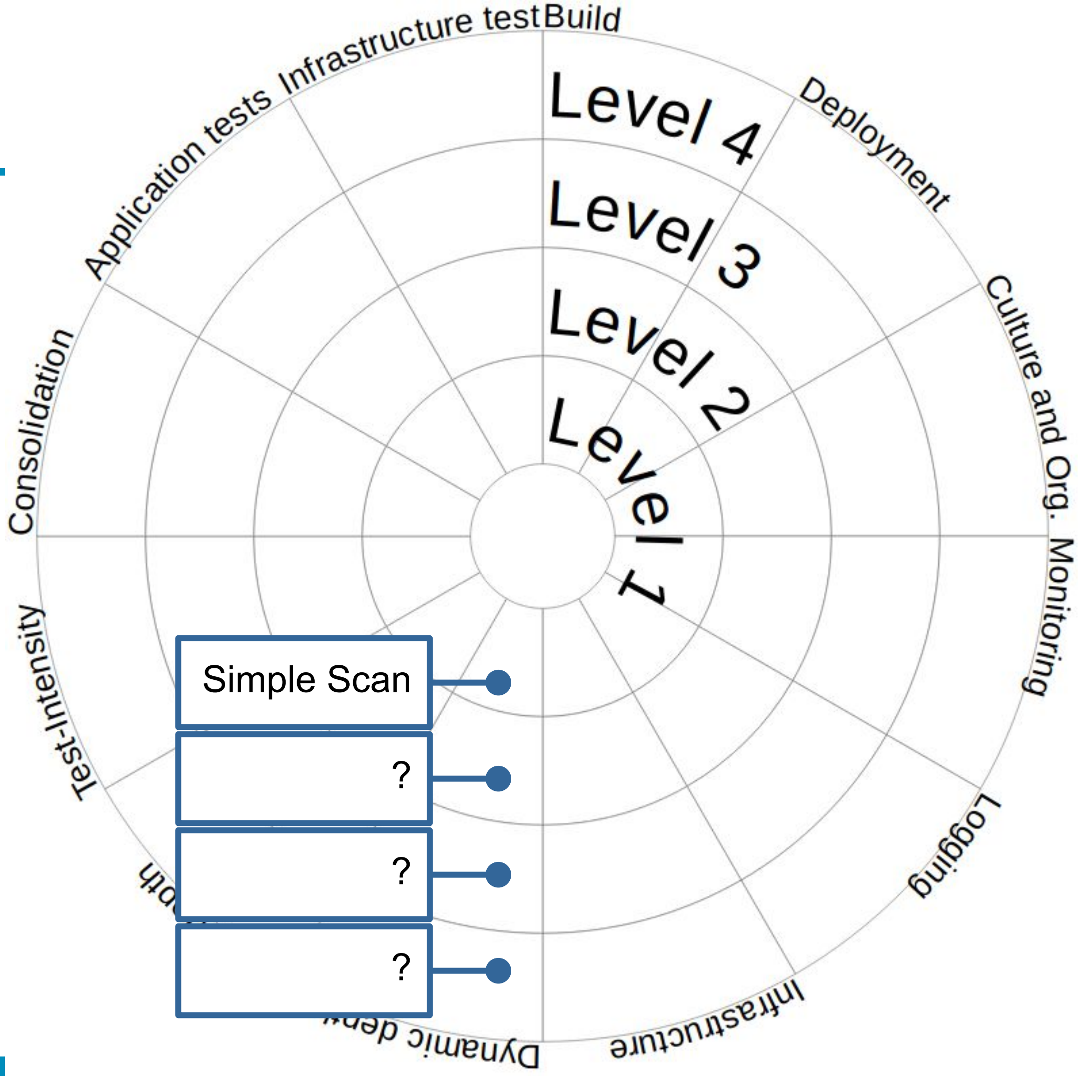
Hardening

Test and Verification

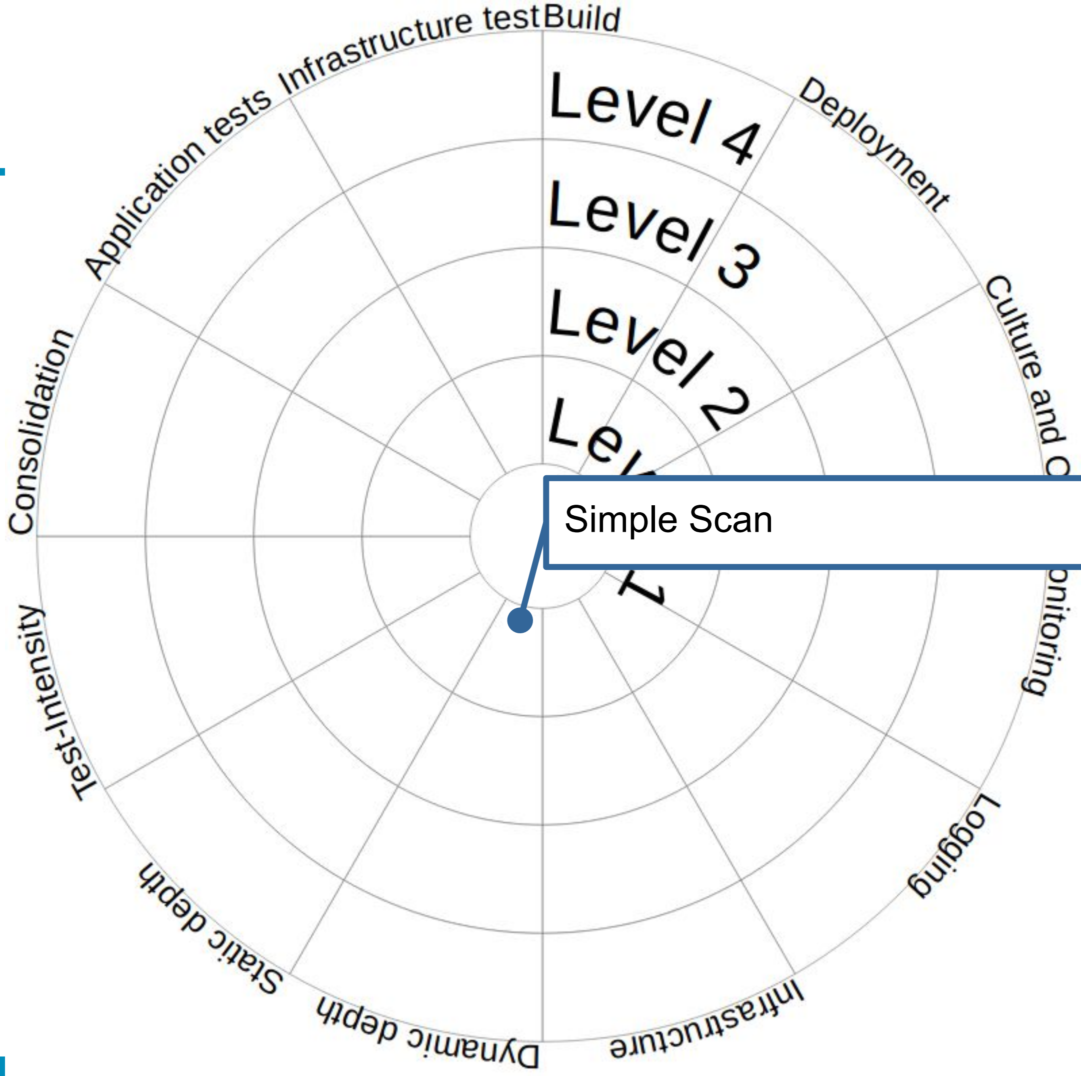
DSOMM

Dynamic depth for applications

DSOMM

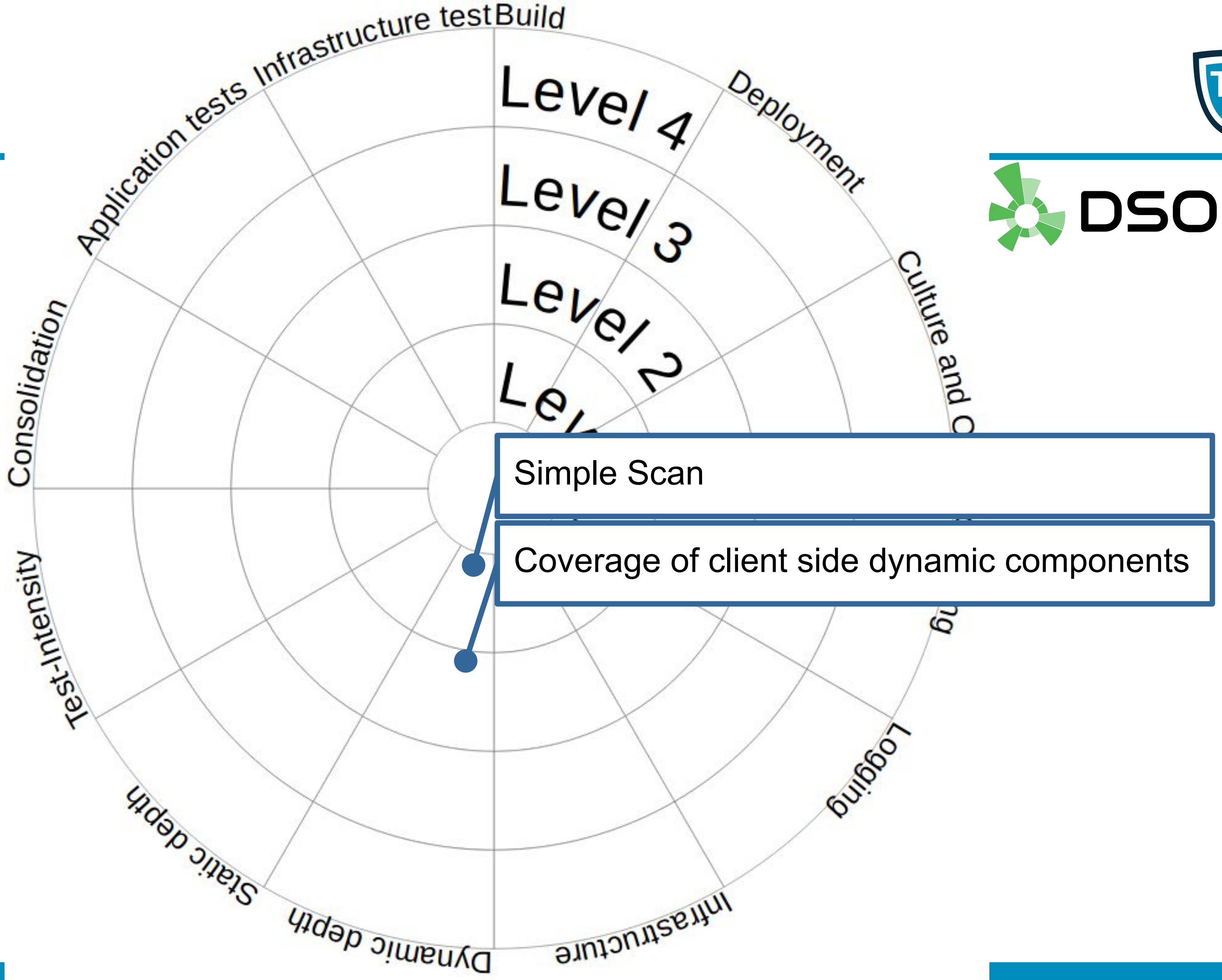


Build
Deployment
Culture and Org.
Monitoring
Logging
Infrastructure
Dynamic dep
pth
Test-Intensity
Consolidation
Application tests
Infrastructure test
Level 4
Level 3
Level 2
Level 1
Simple Scan
?
?
?



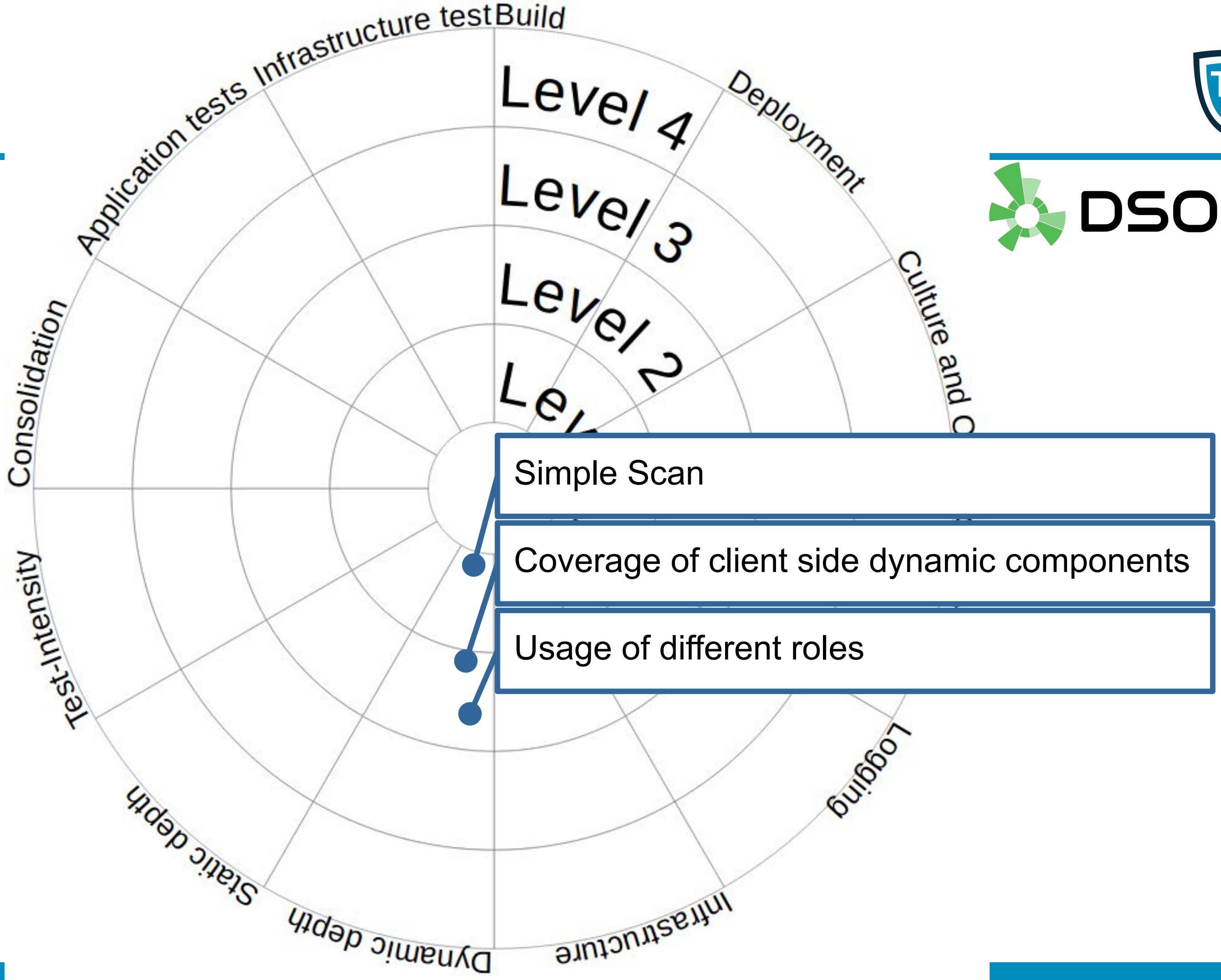
Simple Scan

DSOMM



Simple Scan

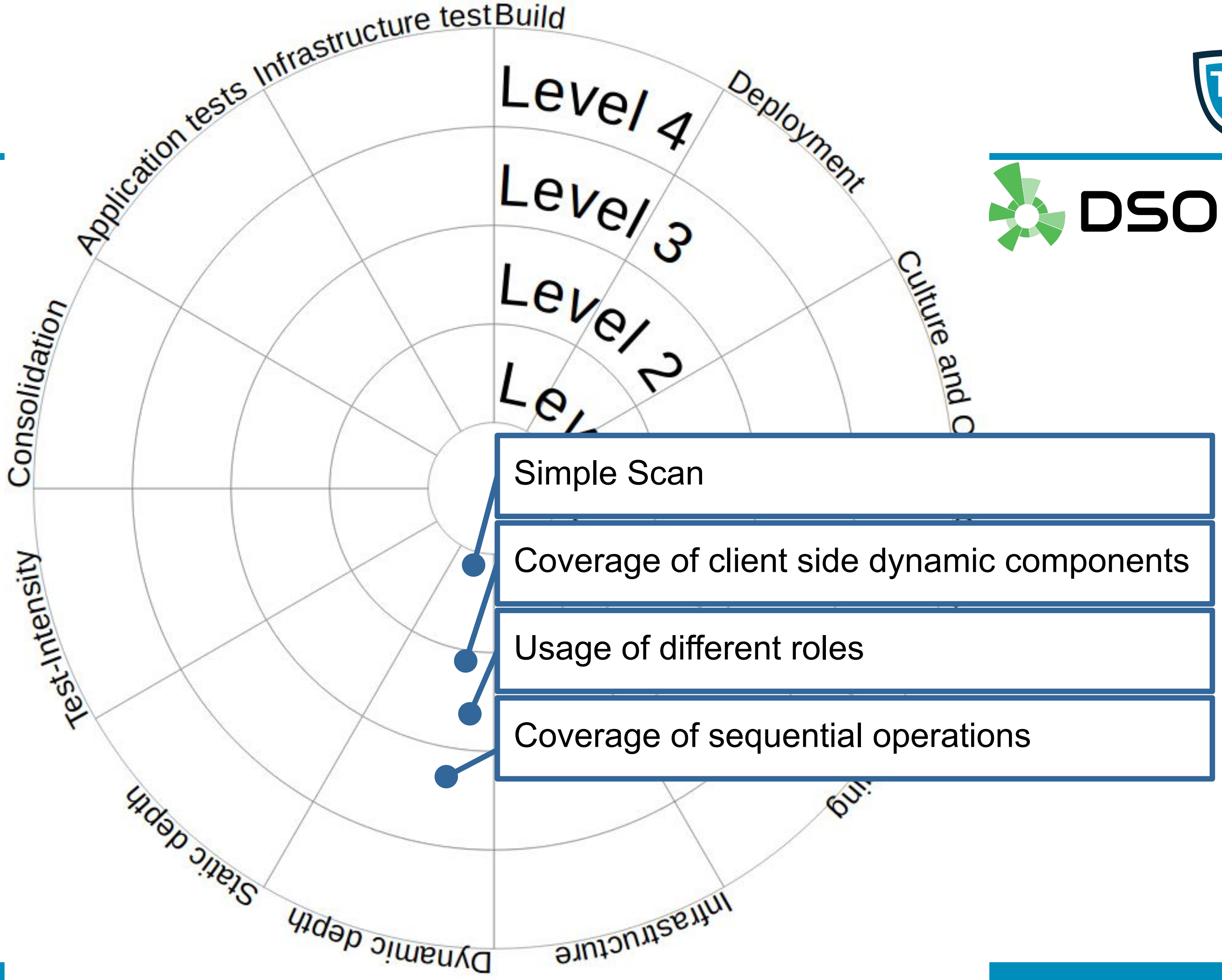
Coverage of client side dynamic components



Simple Scan

Coverage of client side dynamic components

Usage of different roles

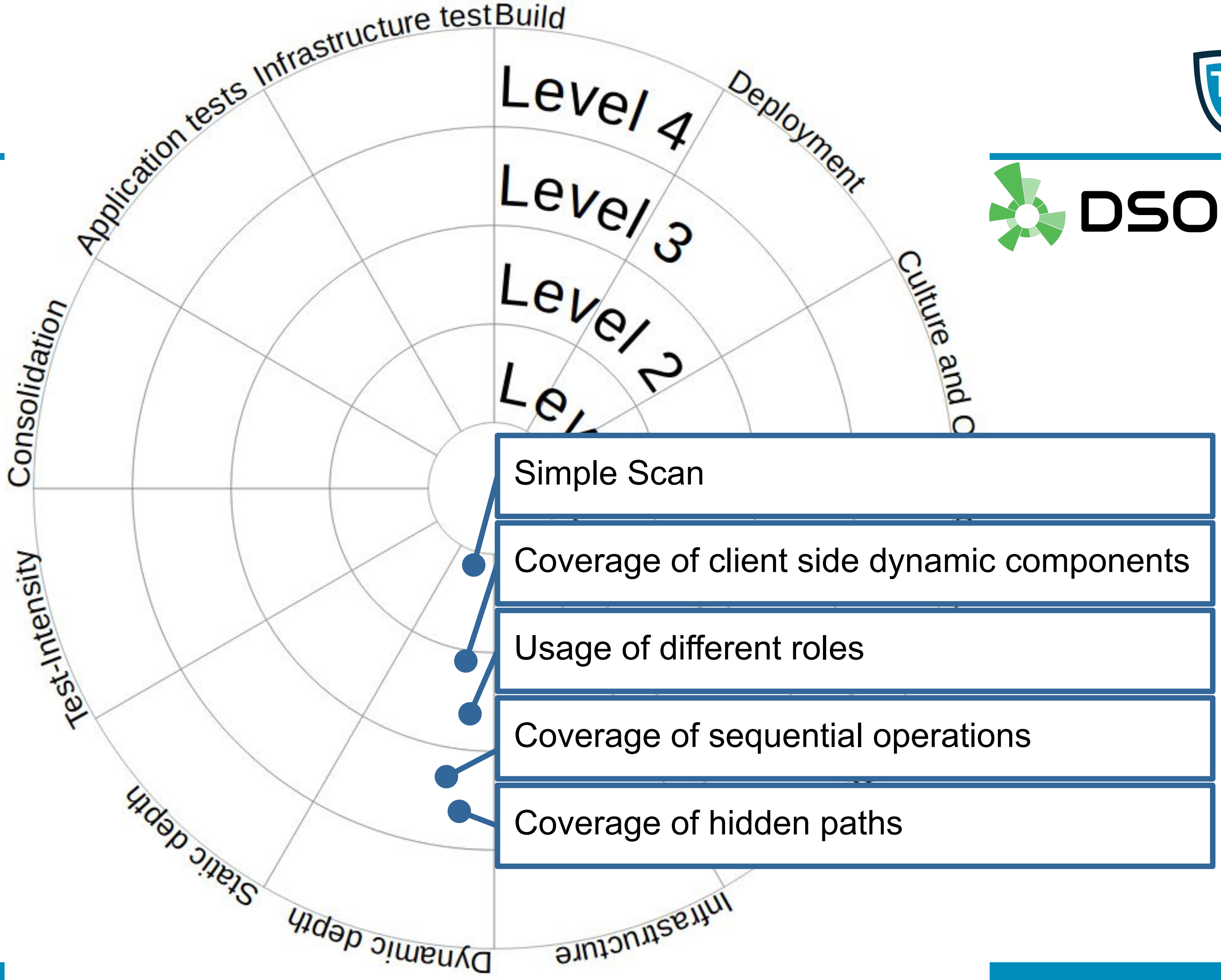


Simple Scan

Coverage of client side dynamic components

Usage of different roles

Coverage of sequential operations



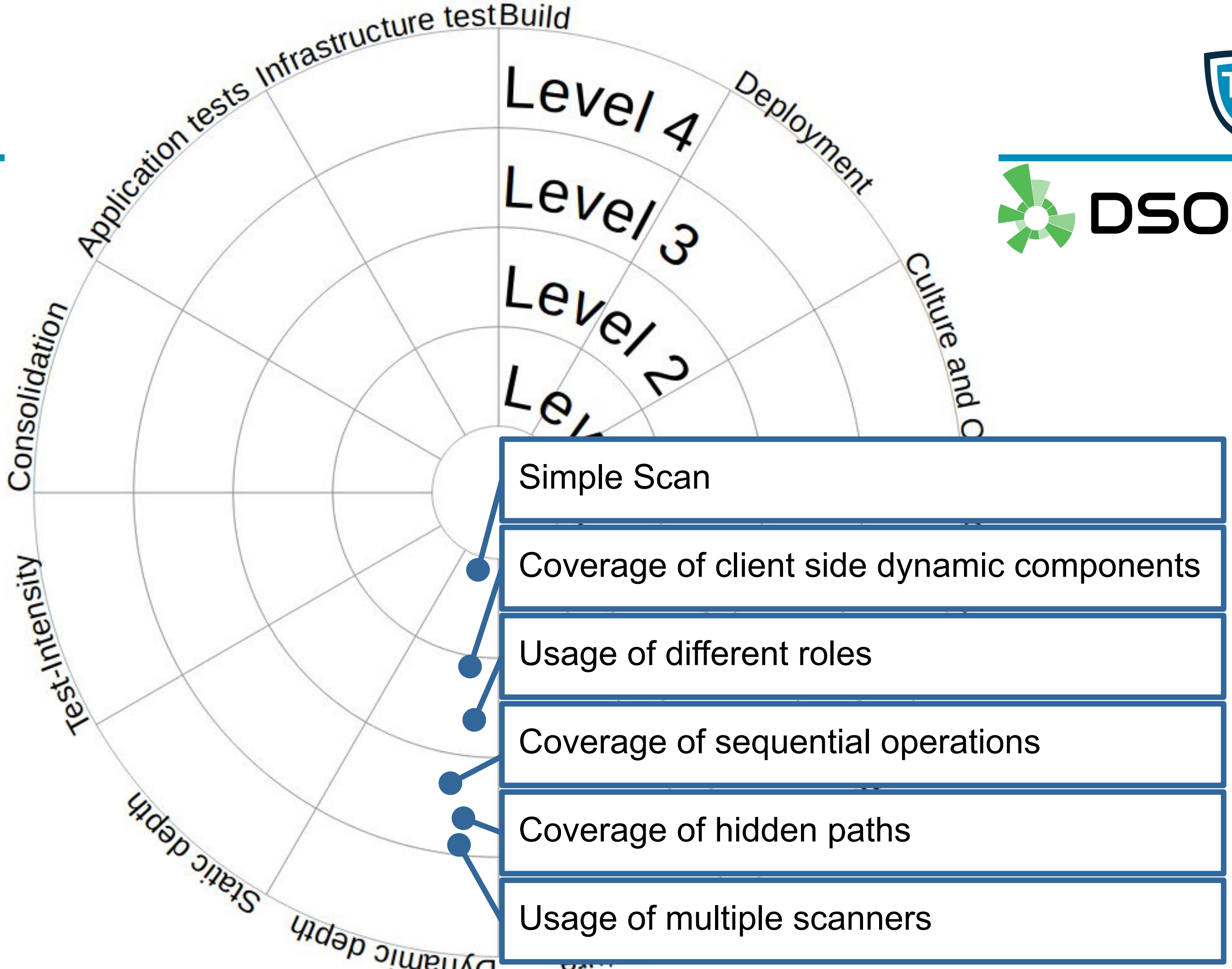
Simple Scan

Coverage of client side dynamic components

Usage of different roles

Coverage of sequential operations

Coverage of hidden paths



Simple Scan

Coverage of client side dynamic components

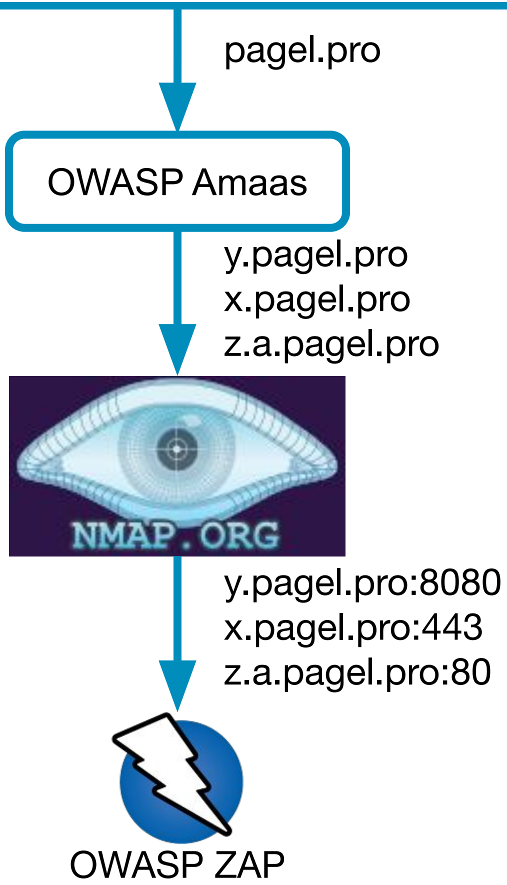
Usage of different roles

Coverage of sequential operations

Coverage of hidden paths

Usage of multiple scanners

Web Security Testing of (an unknown) Enterprise World



pagel.pro

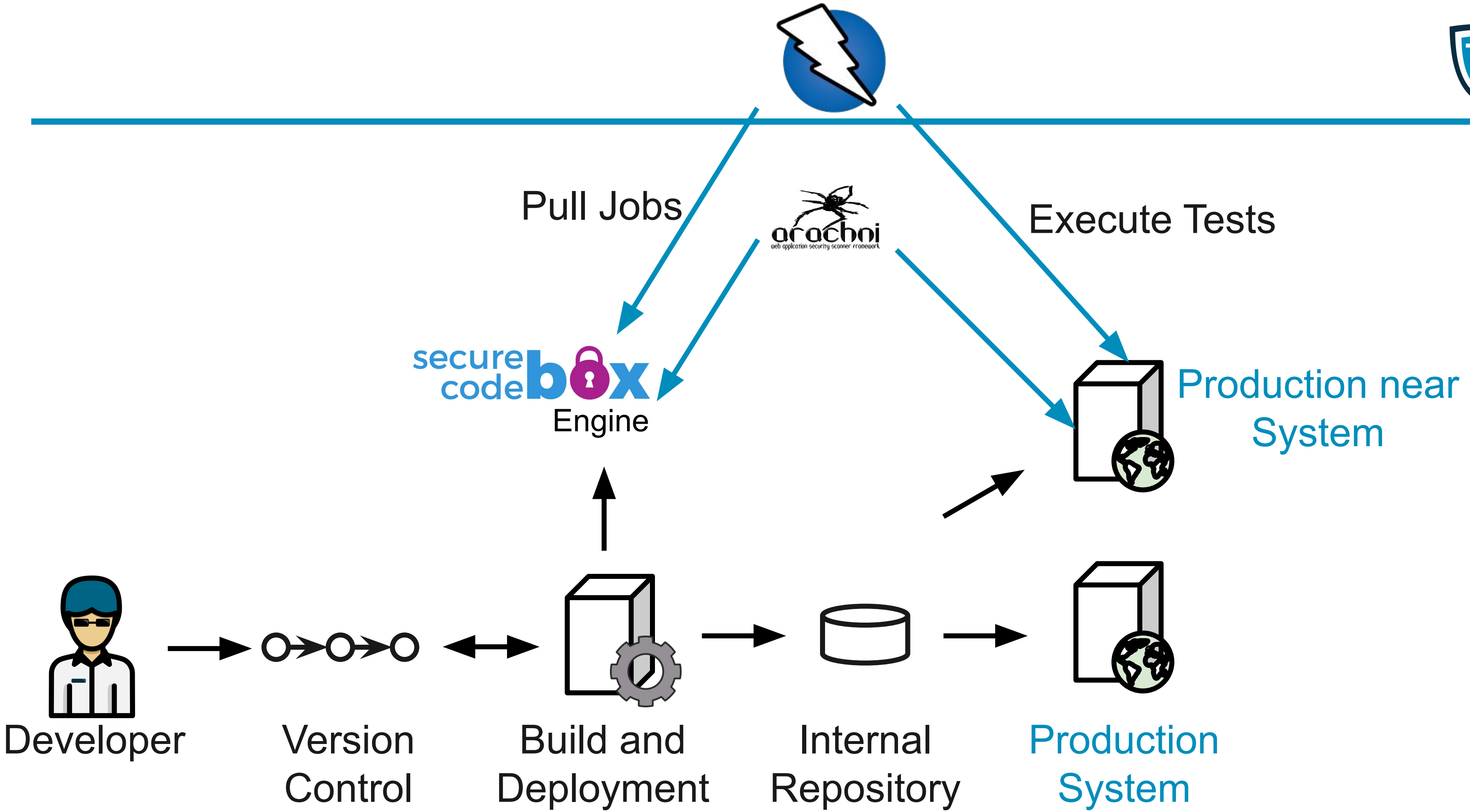
OWASP Amaas

y.pagel.pro
x.pagel.pro
z.a.pagel.pro

y.pagel.pro:8080
x.pagel.pro:443
z.a.pagel.pro:80

OWASP ZAP

OWASP Amaas https://github.com/OWASP/Amass



Pull Jobs

Execute Tests

Engine

Production near System

Developer

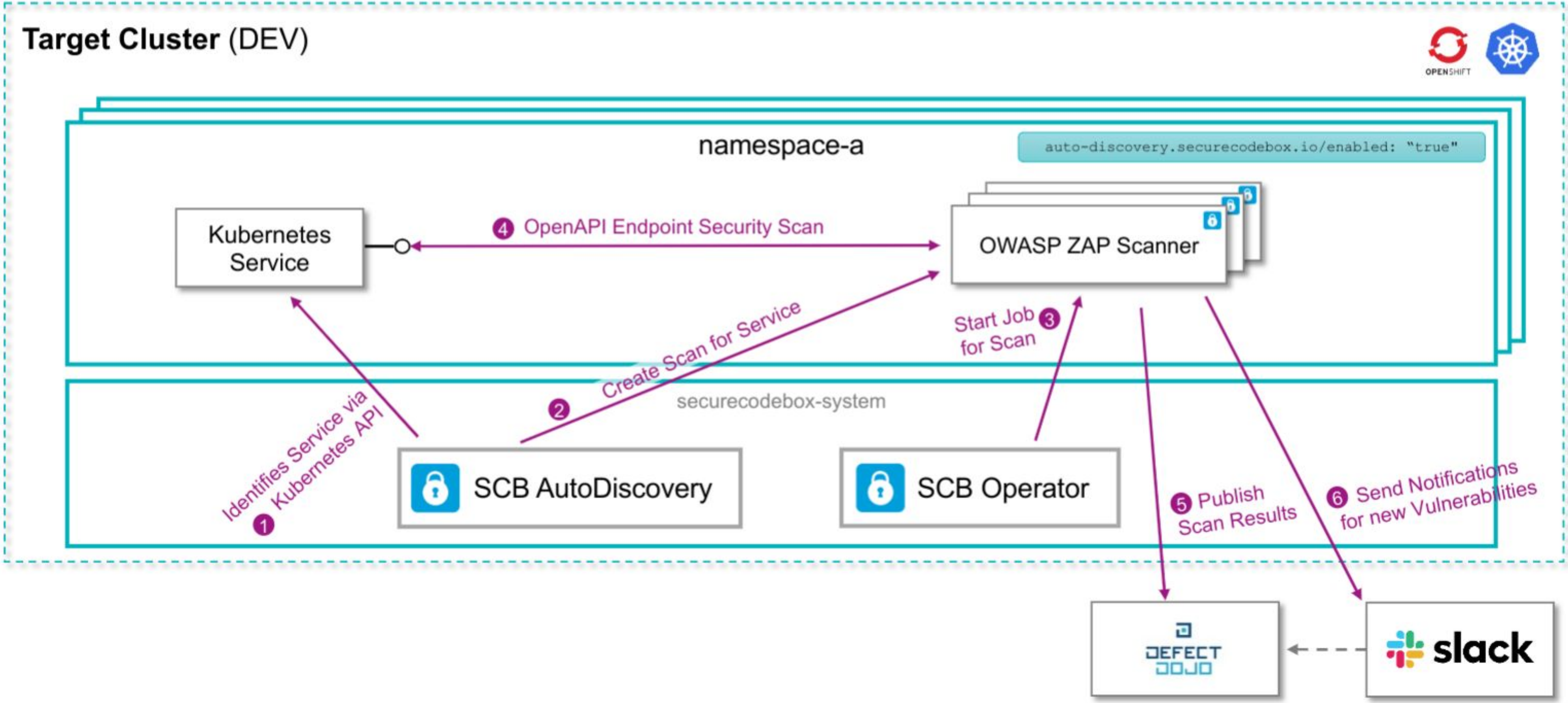
Version Control

Build and Deployment

Internal Repository

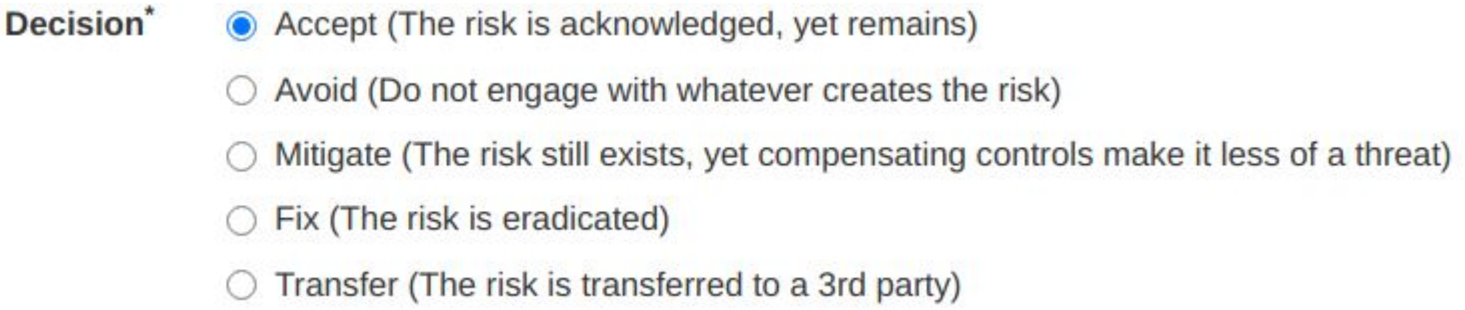
Production System

OWASP securecodebox: New Way



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)

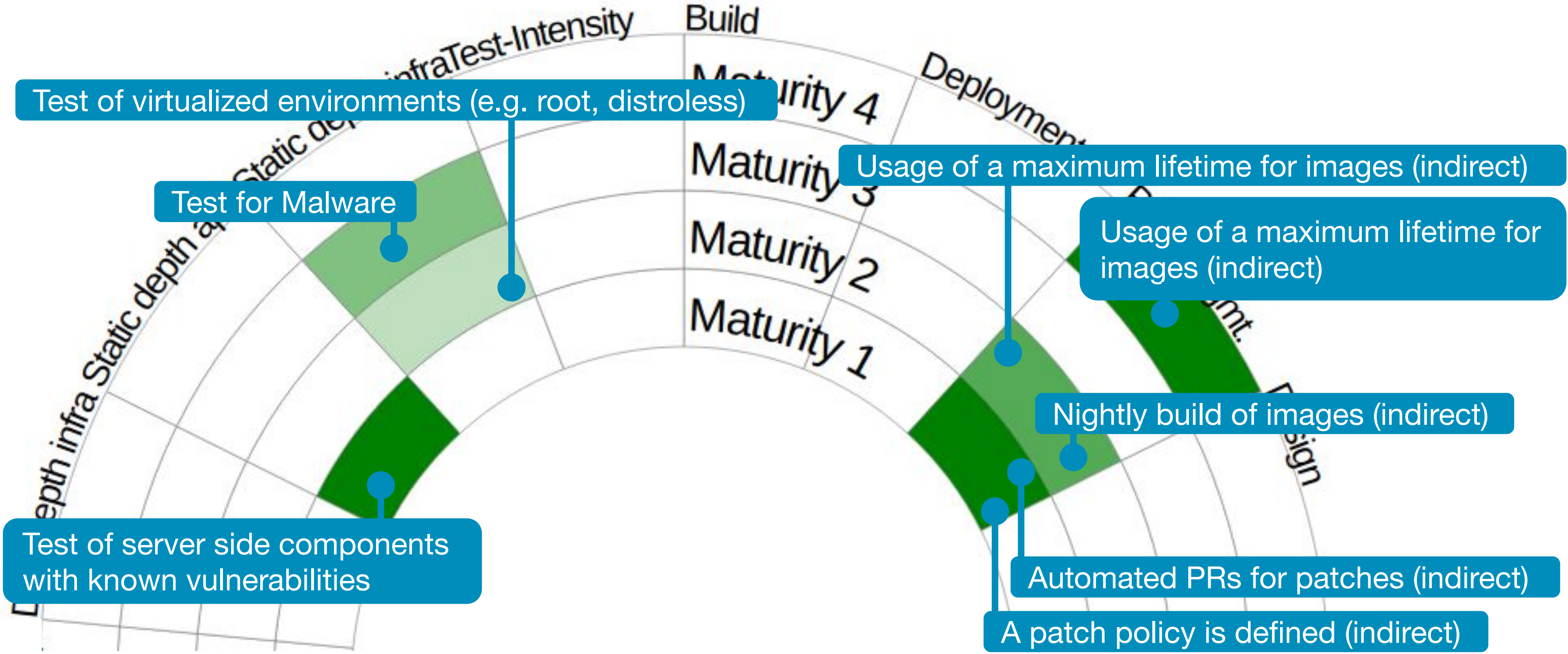
○ Fix (The risk is eradicated)

○ Transfer (The risk is transferred to a 3rd party)

- Deduplicate Findings to detect handled findings

Screenshot OWASP DefectDojo “Add Risk Acceptance”, v 1.13.2, OWASP DefectDojo: https://github.com/DefectDojo/django-DefectDojo

SDA SE ClusterScanner in DSOMM



Test of virtualized environments (e.g. root, distroless)

Test for Malware

Test of server side components with known vulnerabilities

Usage of a maximum lifetime for images (indirect)

Usage of a maximum lifetime for images (indirect)

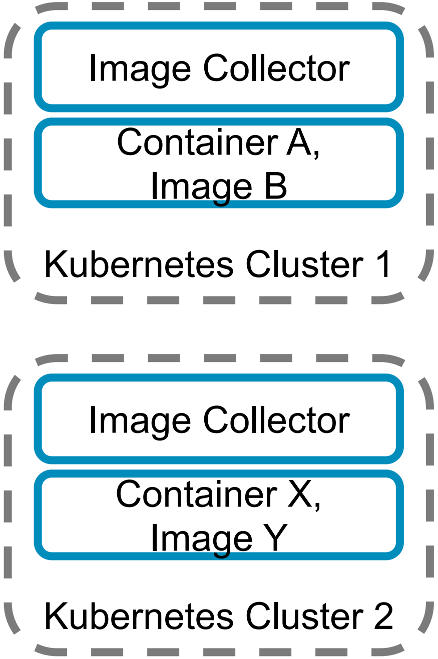
Nightly build of images (indirect)

Automated PRs for patches (indirect)

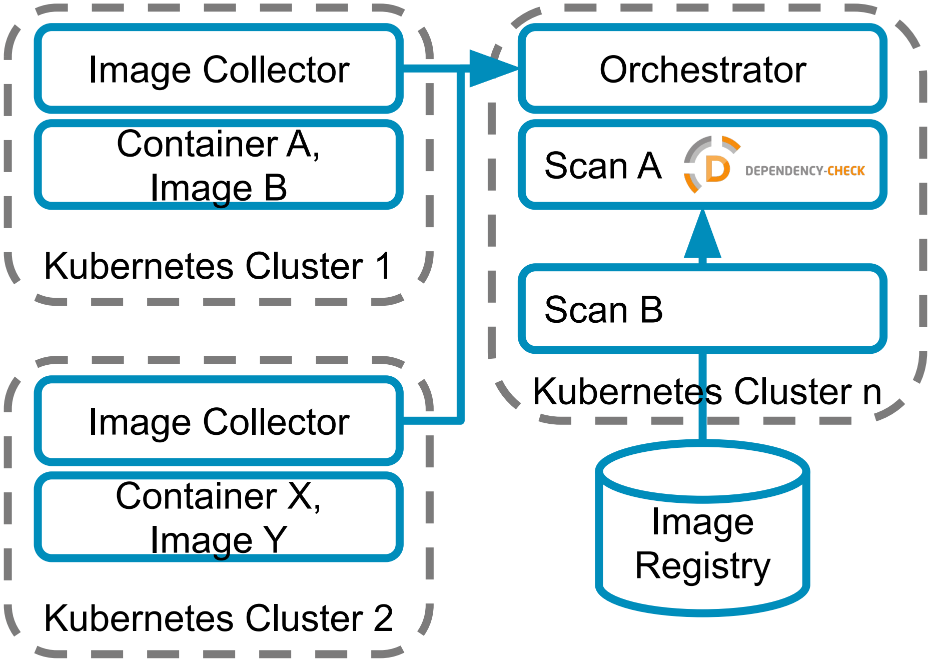
A patch policy is defined (indirect)

SDA SE ClusterScanner Overview

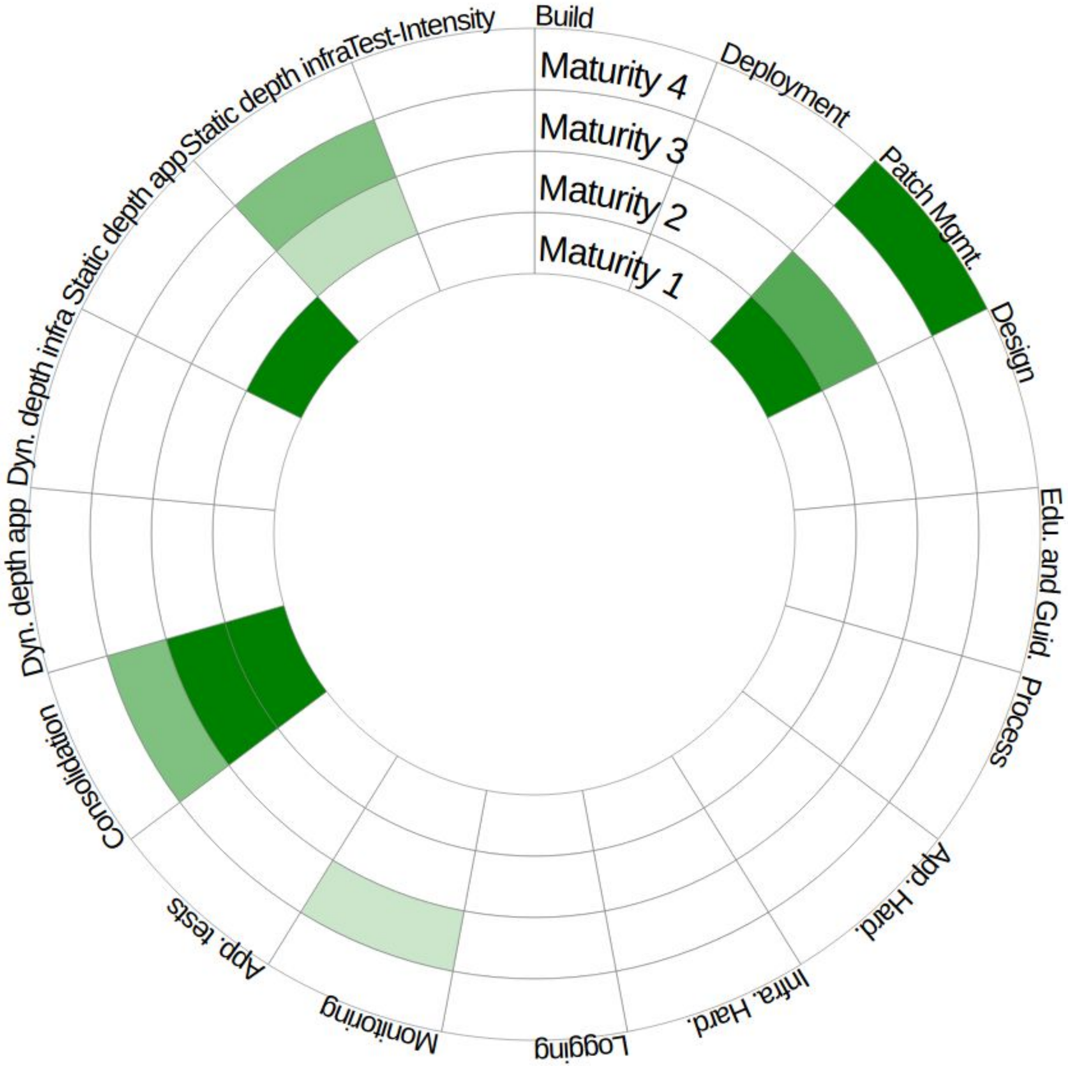
CLUSTER SCANNER



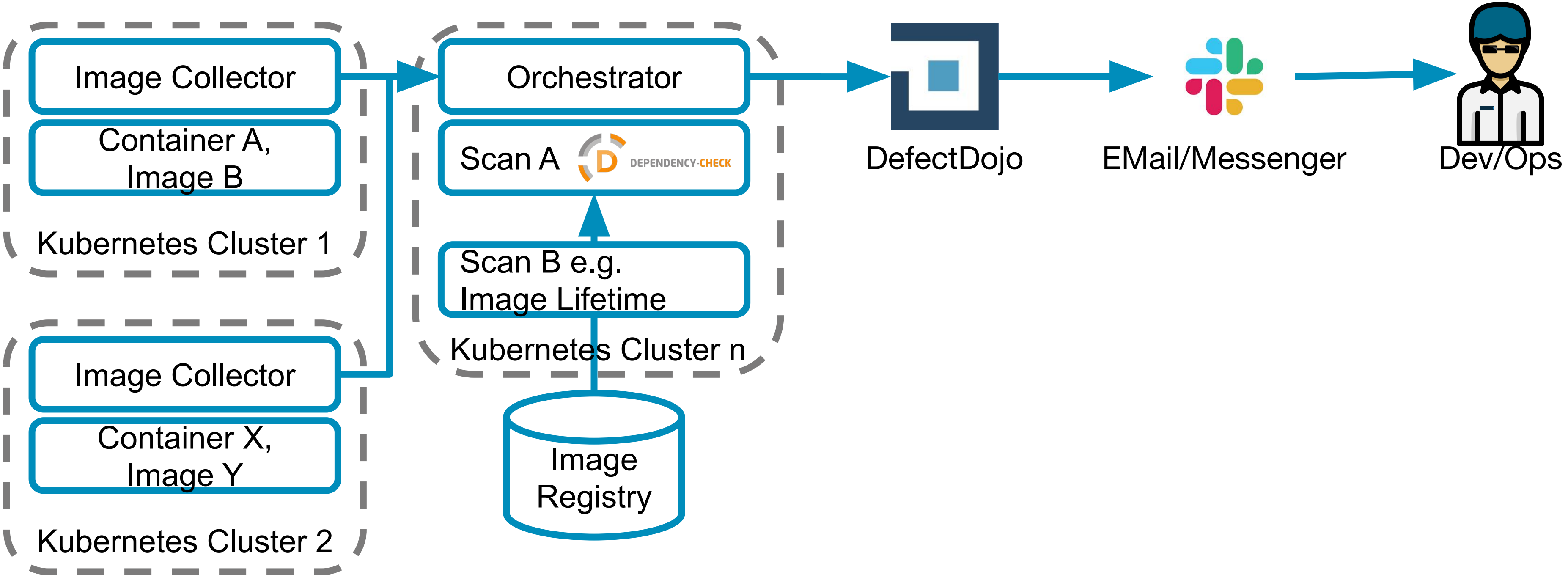
SDA SE ClusterScanner Overview



Cluster Scanner
+
DefectDojo



SDA SE ClusterScanner Overview



DevSecOps Dimensions

DSOMM

Build and Deployment

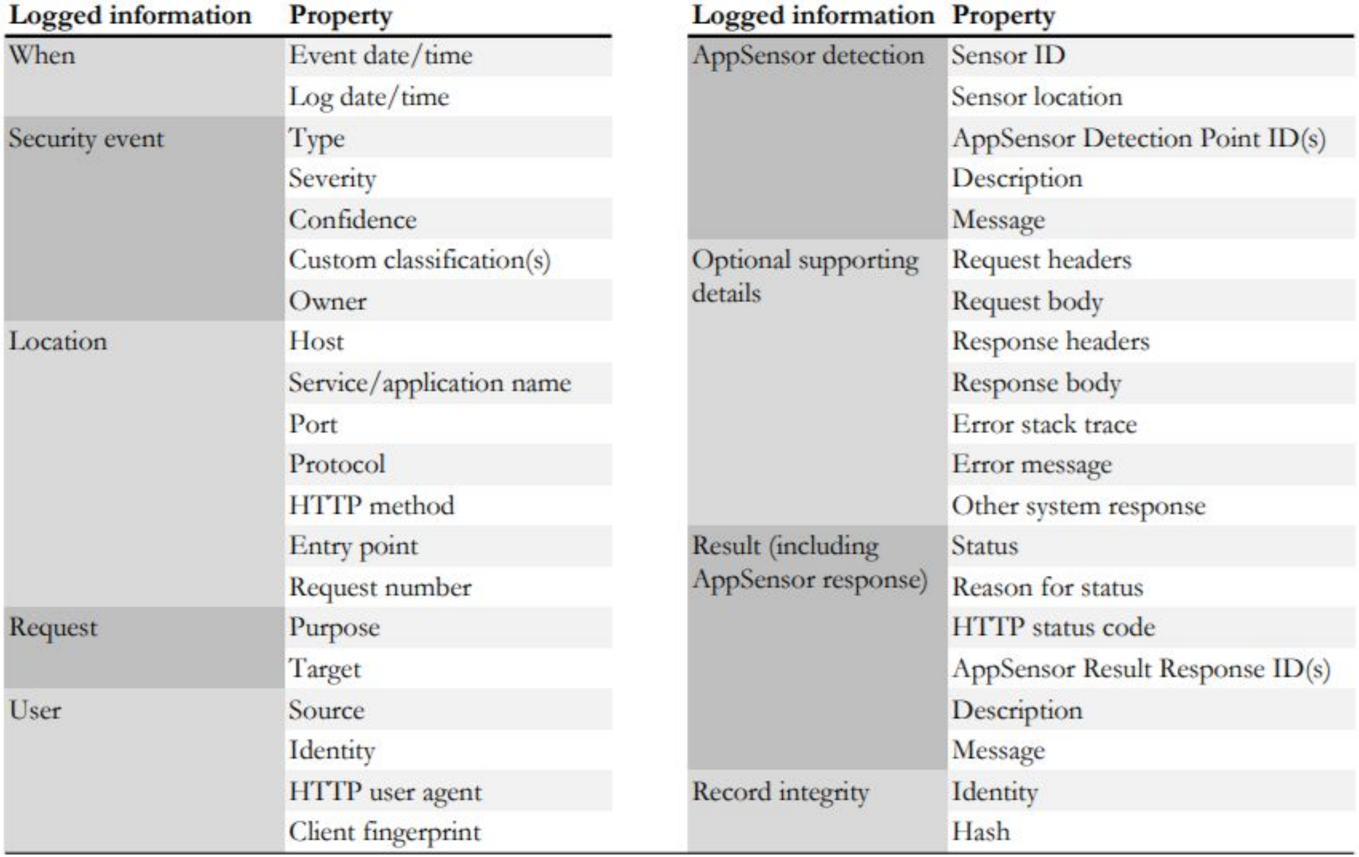
Culture and Organisation

Information Gathering

Hardening

Test and Verification

OWASP AppSensor: What/When

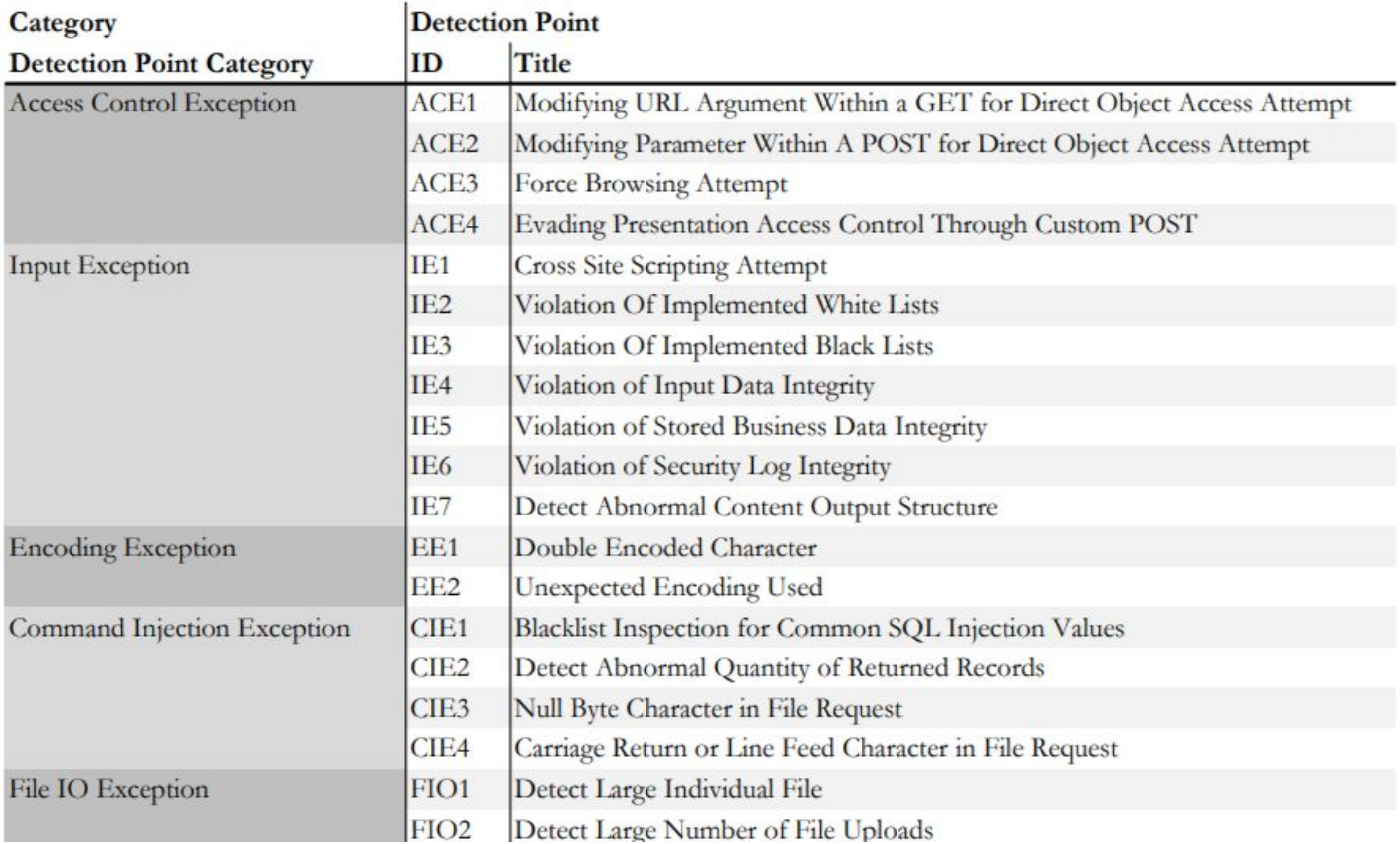


Logged information	Property
When	Event date/time
	Log date/time
Security event	Type
	Severity
	Confidence
	Custom classification(s)
	Owner
Location	Host
	Service/application name
	Port
	Protocol
	HTTP method
	Entry point
	Request number
Request	Purpose
	Target
User	Source
	Identity
	HTTP user agent
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

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

OWASP AppSensor http://www.appsensor.org/, https://www.linuxsecrets.com/owasp-wiki/images/0/02/Owasp-appsensor-guide-v2.pdf

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

OWASP AppSensor http://www.appsensor.org/, https://www.linuxsecrets.com/owasp-wiki/images/0/02/Owasp-appsensor-guide-v2.pdf

Conclusion

- Open Source/Knowledge is startup and enterprise ready

-> Even for security

- OWASP® provides a lot of useful projects

Questions?

secure code box

CLUSTER SCANNER

OWASP TOP 10

OWASP SECURITY PINS

SAMM

DSOMM

OWASP Amaas

OWASP: timo.pagel@owasp.org

Business: owasp21@pagel.pro