

UTILIZE OWASP DSOMM APP TO DEFINE AND DELIVER YOUR OWN PROGRAM


Timo Pagel



- Know production applications
 - Applications
 - Team
 - Contact
 - (Protection requirement)
 - (Regulatory requirements)
- Know security tooling and processes

Inventories



Dimension	Sub-Dimension	Level 1: Basic understanding of security practices	Level 2: Adoption of basic security practices	Level 3: High adoption of security practices
 Build and Deployment	Deployment	<ul style="list-style-type: none">• Inventory of production components <i>[inventory]</i>	<ul style="list-style-type: none">• Inventory of production artifacts <i>[inventory]</i>	<ul style="list-style-type: none">• Inventory of production dependencies <i>[inventory , sbom]</i>

Helpful Information



- Organization chart/diagram
 - Number of dev | security | ops
 - Relation between them
- Technology stack
- Security tooling stack and processes
- Policies, standards, ...
- Pentest reports and open findings



- Consider “includes” for
 - Team activities like security knowledge or security champions
 - Build pipelines
 - Production environments
- Dev/Ops input

Roadmap Planning



Roadmap for Applications



- Maturity Model
- Scorecards

Design of a Maturity Model



Dimension	Level 1	Level 2/...	Level 3/n
A	Light Green	Dark Blue	Red
B	Dark Blue	Bright Green	Dark Blue
C	Red	Blue	Bright Green

Creation of New of Activities



Take into account:

- Dimension (no redundancy)
- Level
 - Dependencies to other activities
 - Existing tools and processes
 - Outcome for security
 - Ease of implementation

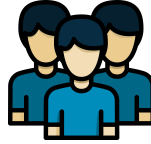


Security Team-Led



- Activities are prioritized by sec. team
- Planned activities needs explanation

Product teams-Led



- Potential activities pre-selected by security team
- Product team selects activities
- All defined activities require explanation
- -> Not recommended due to high effort

Demo



Workshop: Create your own Program



- Focus on the dimension “Test & Verification” for a made up company
- Design at least 4 activities
- Keep existing tools and processes in mind

Summary



- Teams need fast feedback: Automate assessments and metrics
- Planning of activities, communication of the plan, and execution is a key step

Contribution Opportunities

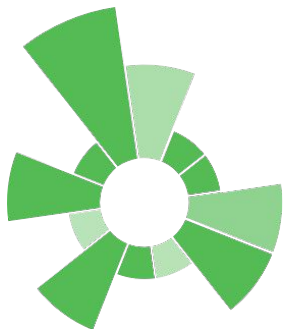


Open PRs

- Add features to the DSOMM application
- Add activities to DSOMM data
- Fix typos in DSOMM data

Sponsor

<https://owasp.org/donate/?reponame=www-project-devsecops-maturity-model&title=OWASP+Devsecops+Maturity+Model>



Timo Pagel

Contact: timo.pagel@owasp.org

Business Contact: dsomm@pagel.pro

Business Website AppSec: <https://appsec-program.com/>

Business Website: <https://pagel.pro>

pagel.pro QR



Join our community in the [OWASP Slack](#) in channel #dsomm

Images



Icons bought via <https://thenounproject.com/> or
copyright by PagelShield GmbH