Welcome

OWASP June 28 Meeting

OWASP Los Angeles Dinner Meetings the Fourth Wed of Every Month

7-19 @ Verizon, Playa Vista
8-23 @ Riot Games
9-27 @ Verizon, Playa Vista
10-4 @ Riot Games (Special Training)
10-25 @ Riot Games
11-29 @ Verizon, Playa Vista
12-20 @ Microsoft Playa Vista

Join OWASP LA Today

- Yearly Membership is only $50
- 2-Year membership is $95
- Lifetime membership is $500

https://myowasp.force.com/CPBase__store?site=a1e0B000007AckPQAS

Thank you to all Volunteers from AppSec California 2017

https://appseccalifornia.org

Call for Volunteers for AppSec California 2018

- January 29-31, 2018
- We need planners
- We need volunteers at the conference
- Free admission
- Contact:

  appsec-cali-2018-info@owasp.org

OWASP Top 10

- 10 most critical web application security risks
- One of the foundations of application security compliance
- Last updated in 2013
- Release candidate for the 2017 revision published for public comment
- Email OWASP-TopTen@lists.owasp.org, by the June 30, 2017 deadline

Proposed Entry "A7 – Insufficient Attack Protection"

- A prescriptive security control is not appropriate for the Top 10 list
- The Top 10 is a list of risks
- OWASP has always been about "Openness"
- Prescribing one control casts doubt on this "Openness"
- Attack Protection" is not an accepted type of security control

Proposed Entry "A10-Underprotected APIs"

- Also not an application security risk
- Security risks of APIs are included in other Top 10 items
  - If the API is unprotected, then that is either an A2 - Authentication issue, or an A4 - Authorization issue
  - If the API contains vulnerabilities such as known vulnerable software, then that is covered by A9
  - If the API exposes sensitive data, then that is covered by A6
  - If the APIs are vulnerable to injection, then that is covered by A1
- No need to create a specific category for APIs

Panel Discussion: What DOES it Take to Produce Secure Software?

June 28, 2017

Edward Bonver
Cybersecurity Leader

Richard Greenberg
Leader, OWASP LA
Moderator

Stuart Schwartz
Application Security
Specialist

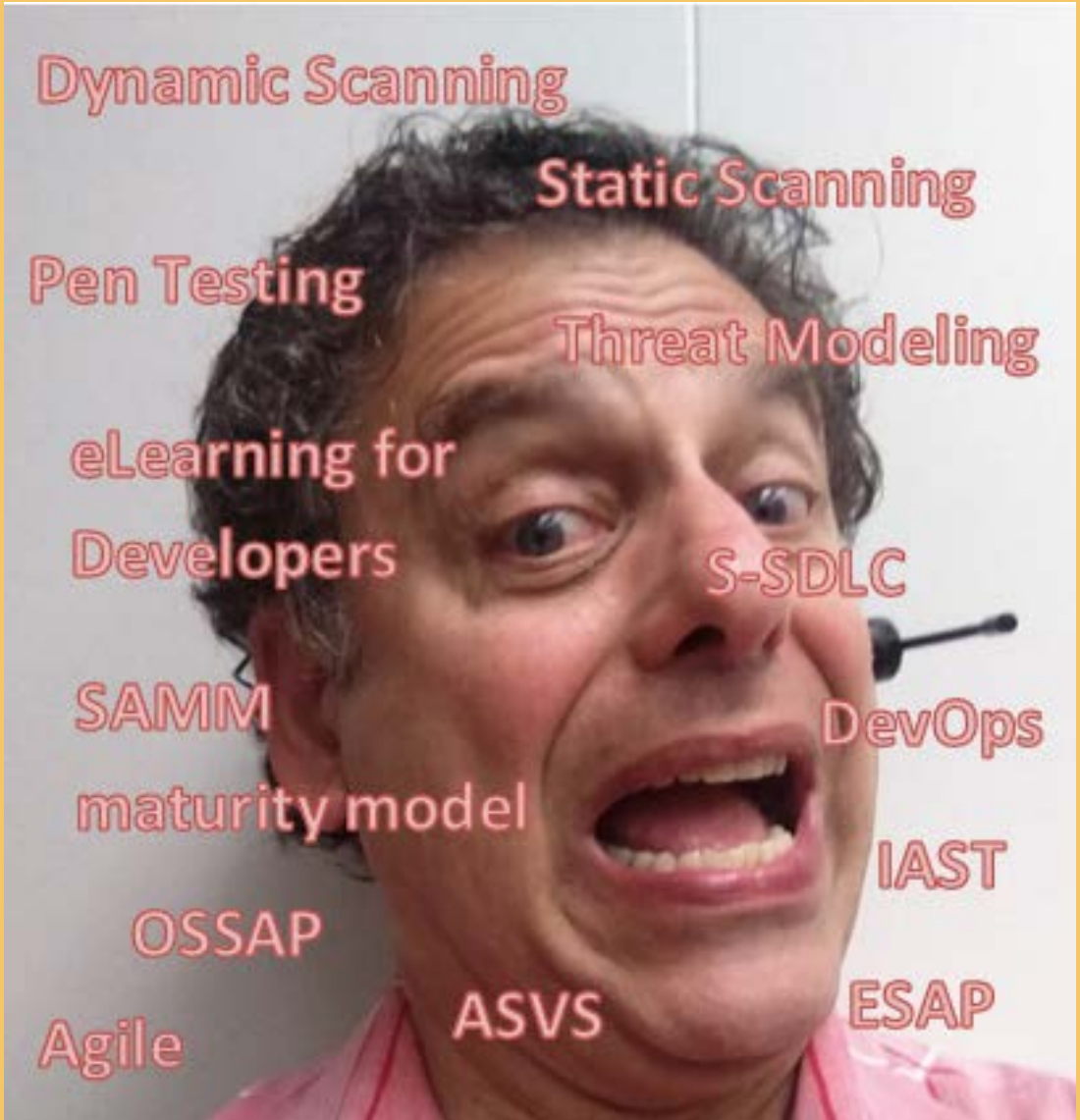
Aaron Guzman
Manager at Gotham
Digital Science

Tony Trummer
Director of Security
Engineering at Tinder

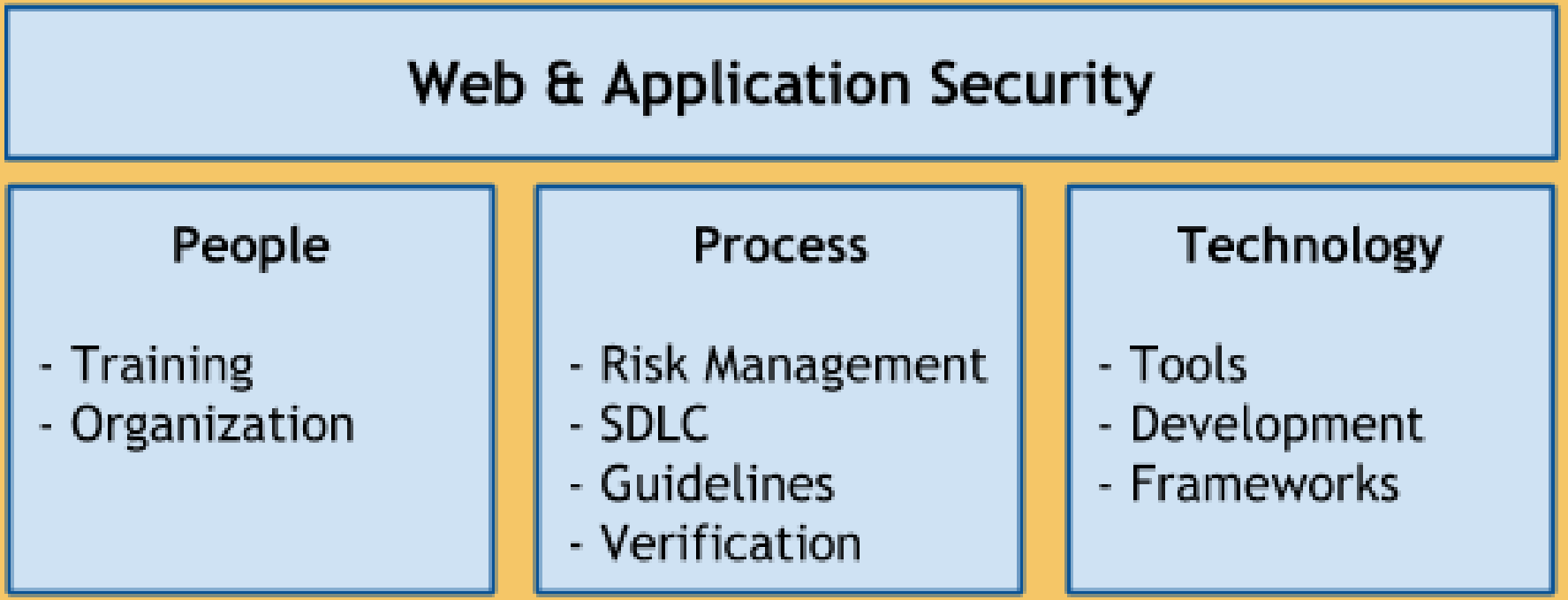
How Do You Ensure Your Software is Secure?

- Where do you begin?
- What do you really need to focus on?
- Are tools enough?
- What is your company's culture?

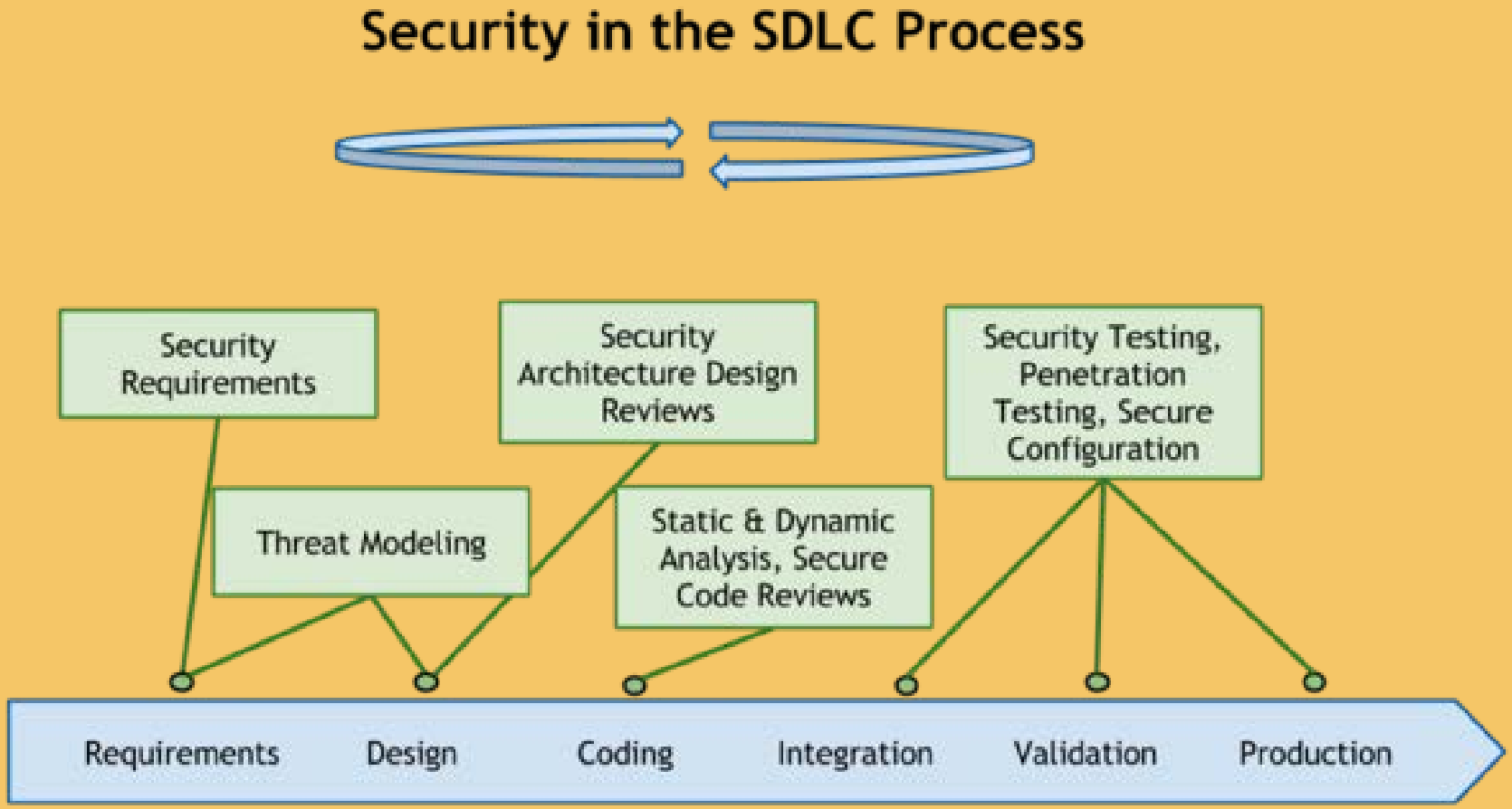
How Do You Make Sense of it all?



People, Process, and Technology



Secure Software Development Life Cycle



OWASP Links

- ASVS https://github.com/OWASP/ASVS
- OWASP testing guide

  http://www.owasp.org/index.php/OWASP_Testing_Project
- MASVS https://github.com/OWASP/owasp-masvs
- OWASP mobile security testing guide

  https://github.com/OWASP/owasp-mstg/

OWASP Links (cont'd)

- Embedded Application Security Project

  https://www.owasp.org/index.php/OWASP_Embedded_Application_Security
- AppSec pipeline project

  https://www.owasp.org/index.php/OWASP_AppSec_Pipeline
- Defect Dojo

  https://www.owasp.org/index.php/OWASP_DefectDojo_Project

Audience Questions

Thank you!

Owaspla.org