From Zero to Hero - or how OWASP saved my holiday

Tobias Gondrom

(OWASP Member)

OWASP AppSecEU 15

Amsterdam, The Netherlands

Disclaimer

- *All characters appearing in this work are fictitious. Any resemblance to real persons, living or dead, is purely coincidental.*

- *The views and opinions expressed in this article are those of the author and not of any organisations.*

- *“Everything I say is my own personal opinion. Especially the wrong ones….”*

Tobias Gondrom

- 15 years information security experience
  (Global Head of Security, CISO, CTO)
  CISSP, CSSLP, CCISO
- 12 years management of application security & development exp.
- Sloan Fellow M.Sc. In Leadership and Strategy, London Business School
- OWASP Global Board member, OWASP Project Leader for the CISO Survey, www.owasp.org
- Author of Internet Standards on Secure Archiving, CISO training and co-author of the OWASP CISO guide
- Chair of IETF Web Security Working Group
  http://datatracker.ietf.org/wg/websec/charter/
  Member of the IETF Security Directorate
  Chair of IETF Administrative Oversight Committee (IAOC),
- Cloud Security Alliance, Hong Kong chapter, Vice Chairman
- Previously working for Thames Stanley: Managing Director, CISO Advisory, Information Security & Risk Management, Research and Advisory

The Beginning

You **think you have this**:

- Well fortified. Secure perimeter protection,
- anti-virus,
- secure off-the-shelf software systems customized for your business needs and
- a few self-built system applications.
- Very little budget, but you are doing fine, because you never had a breach….

…… until Today.

The Truth

In truth **you have this**:

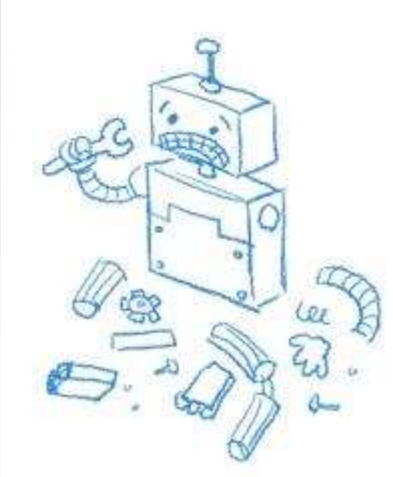
“Hello John.”

- “Hello, my name is John Smith. I am the CISO of a medium sized company. And we had a breach.”

- “Hello John.”

What now?

TOTAL CRISIS
PANIC BUTTON
START RUNNING
Danger Is Imminent
DON'T THINK
Stay Fearful And Alert
FLASHING
OBEY ORDERS



PANIC
BUTTON
FOR EMERGENCY USE ONLY

Now?

- … your Exec Management team is pretty upset,
- … your customers worried,
- … your employees confused,
- … your CEO has you on speed dial
- … and you get the "pleasure" of daily and then weekly briefings on fixing everything and what you do to make sure this never happens again.

Summer holiday???

- Now is May, and you had so nice plans for a relaxing summer holiday on the beach in July….
- Are you crazy???
- All bets are off….

Fix it

- Before you could even think of going on holiday, you need to…

- Have a security strategy?
- Upgrade your Security policy?
- SDLC – do we have one, do we live it? And if yes, why did everything go sideways….?
- How do we benchmark against others?
- Use Risk Management?
- Have a security team / organise it?
- Security training and awareness?
- Secure coding guidelines….

…. All by yesterday

You are not alone….

- Make everything yourself?

- No chance to get there in time....

Learn and copy from the experts

There is this crazy group of experts and everything they do is open source and free….

….. maybe we should take a look. Shall we?

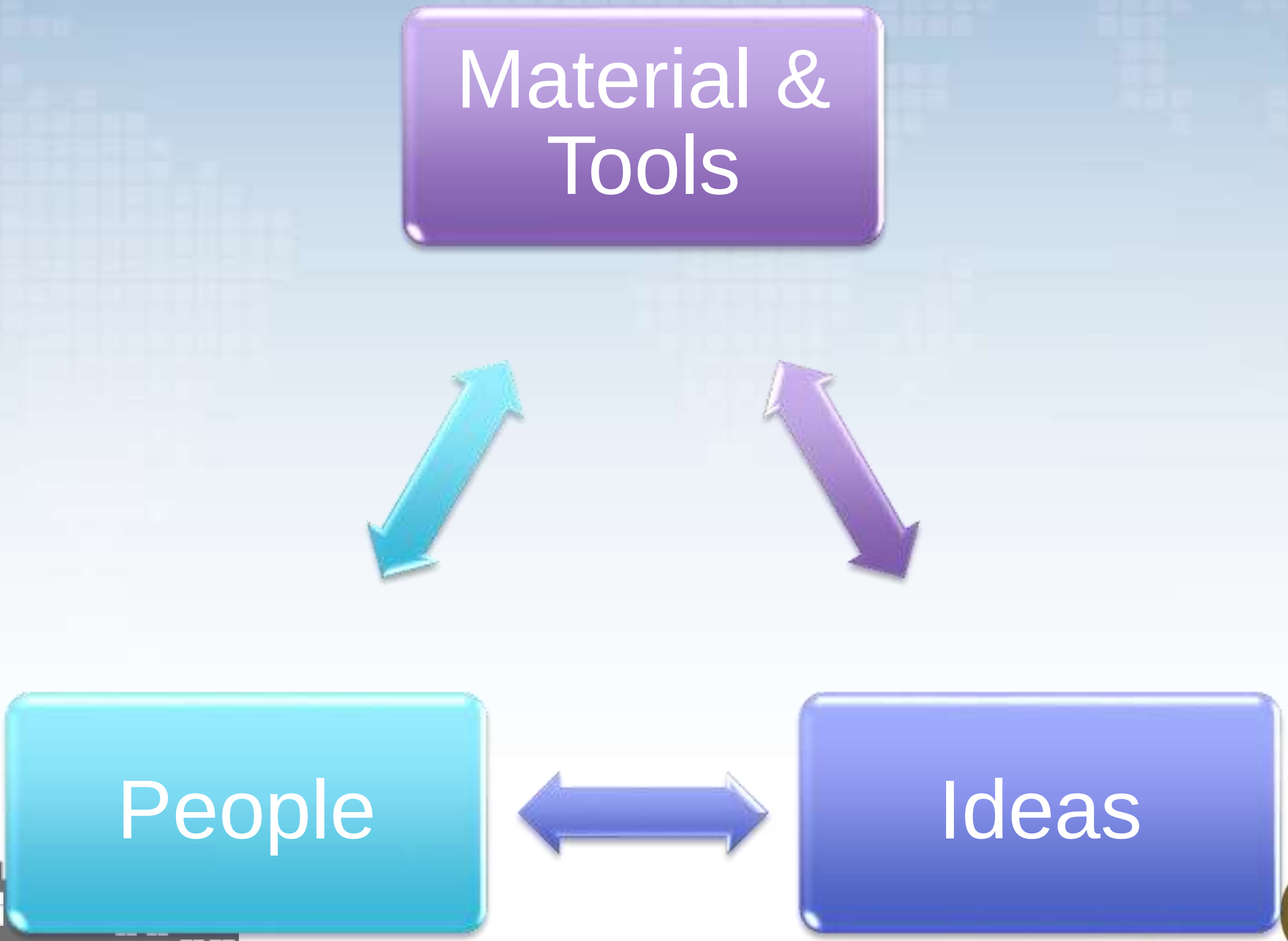
So how do we get there…

- Have a security strategy?
- Upgrade your Security policy?
- SDLC – do we have one, do we live it? And if yes, why did everything go sideways….?
- How do we benchmark against others?
- Use Risk Management?
- Have a security team / organise it?
- Security training and awareness?
- Secure coding guidelines….

…. All by yesterday / all by next month / within 3 months?

OWASP AppSecEU 15
Amsterdam, The Netherlands

How OWASP can help you

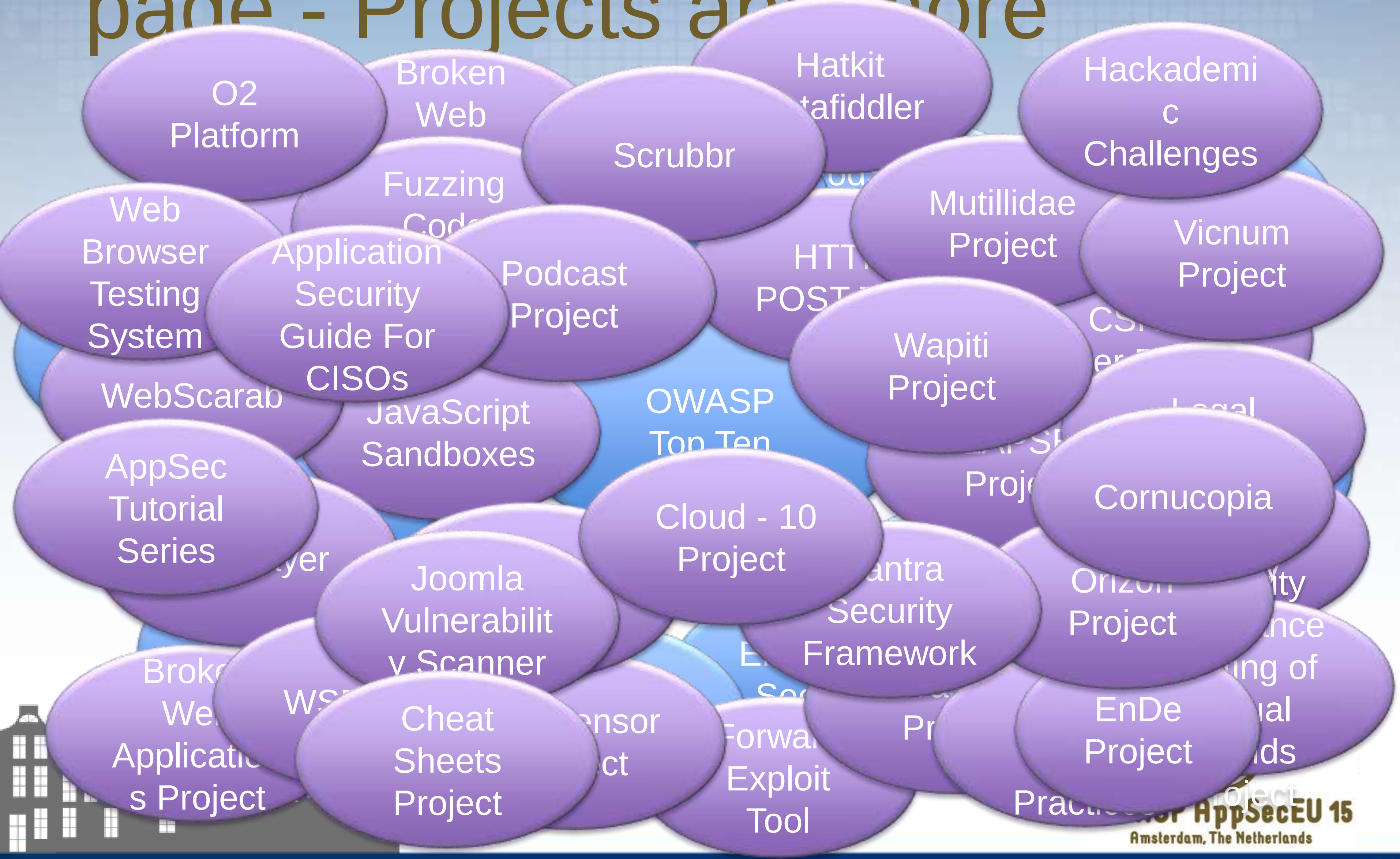


Material & Tools

People

Ideas

You go to the OWASP web page - Projects and more



O2 Platform

Broken Web

Hatkit ...tafiddler

Hackademic Challenges

Scrubbr

Fuzzing Cod...

Mutillidae Project

Vicnum Project

Web Browser Testing System

Application Security Guide For CISOs

Podcast Project

HTT... POST...

CS... er...

Wapiti Project

WebScarab

JavaScript Sandboxes

OWASP Top Ten

Legal

...APSE... Proj...

Cornucopia

AppSec Tutorial Series

...yer

Cloud - 10 Project

Joomla Vulnerability Scanner

...antra Security Framework

Orizon Project

...ity ...nce ...ing of ...ual ...ds ...oject

Brok... We... Applicatio... s Project

WS...

Cheat Sheets Project

...ensor ...ct

Forwa... Exploit Tool

E... Sec...

Pr...

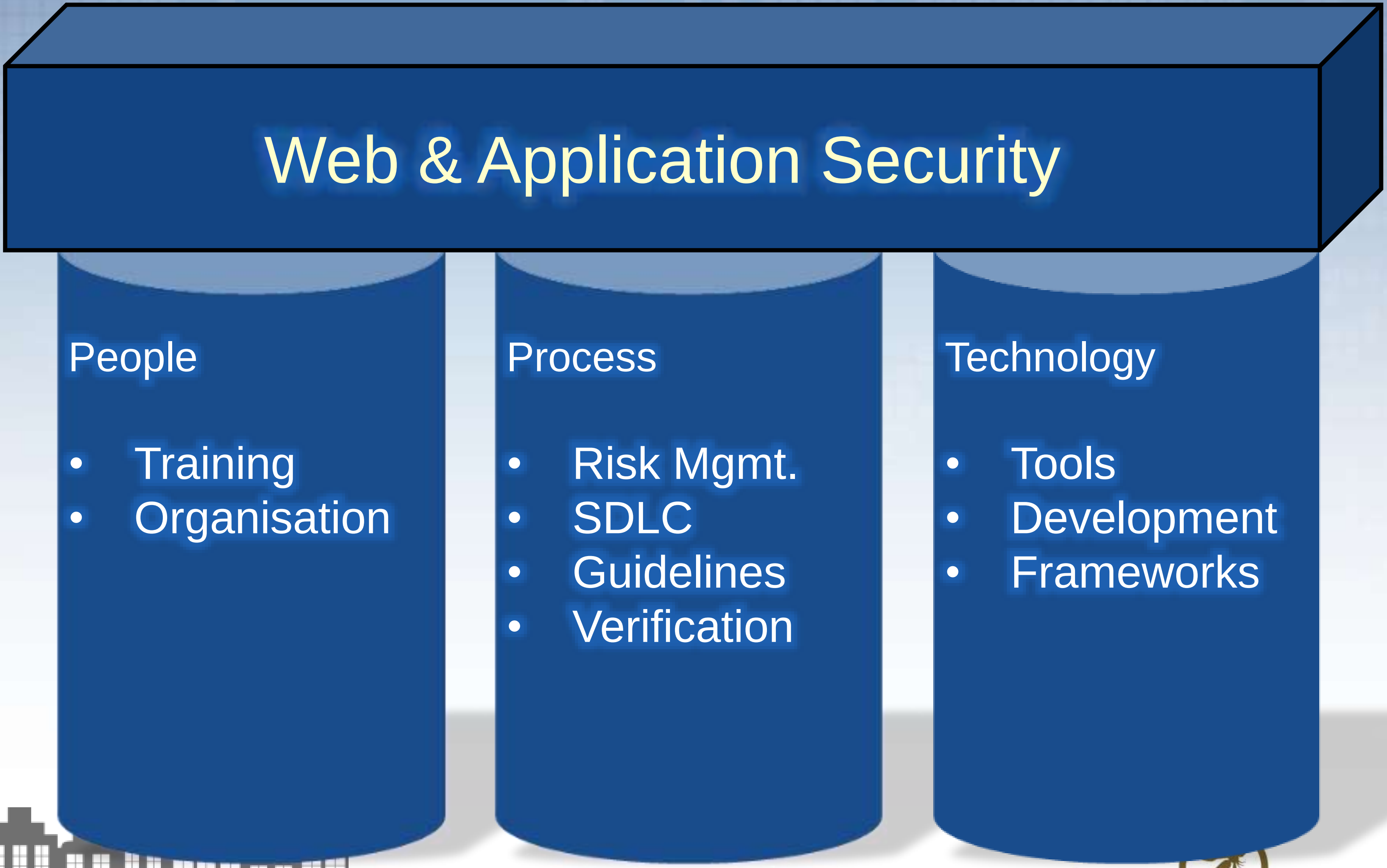
EnDe Project

Practi...

And others?

Multitude of Standards and Documents

- OWASP
- ISO 2700x, ISO 31000
- Cobit, Risk IT (ISACA)
- ITIL, NIST, PCI-DSS, ISF “Standard of Good Practice for Information Security”
- CSA (Cloud Security Alliance)
- ….



Web & Application Security

People

- Training
- Organisation

Process

- Risk Mgmt.
- SDLC
- Guidelines
- Verification

Technology

- Tools
- Development
- Frameworks

OWASP Projects for an industry or development company

OWASP Top Ten

openSAMM - Software Assurance Maturity Model

Application Security Guide For CISOs

Secure Coding Practices - Quick Reference Guide

Cheat Sheets Project

Code Review Guide

Development Guide Project

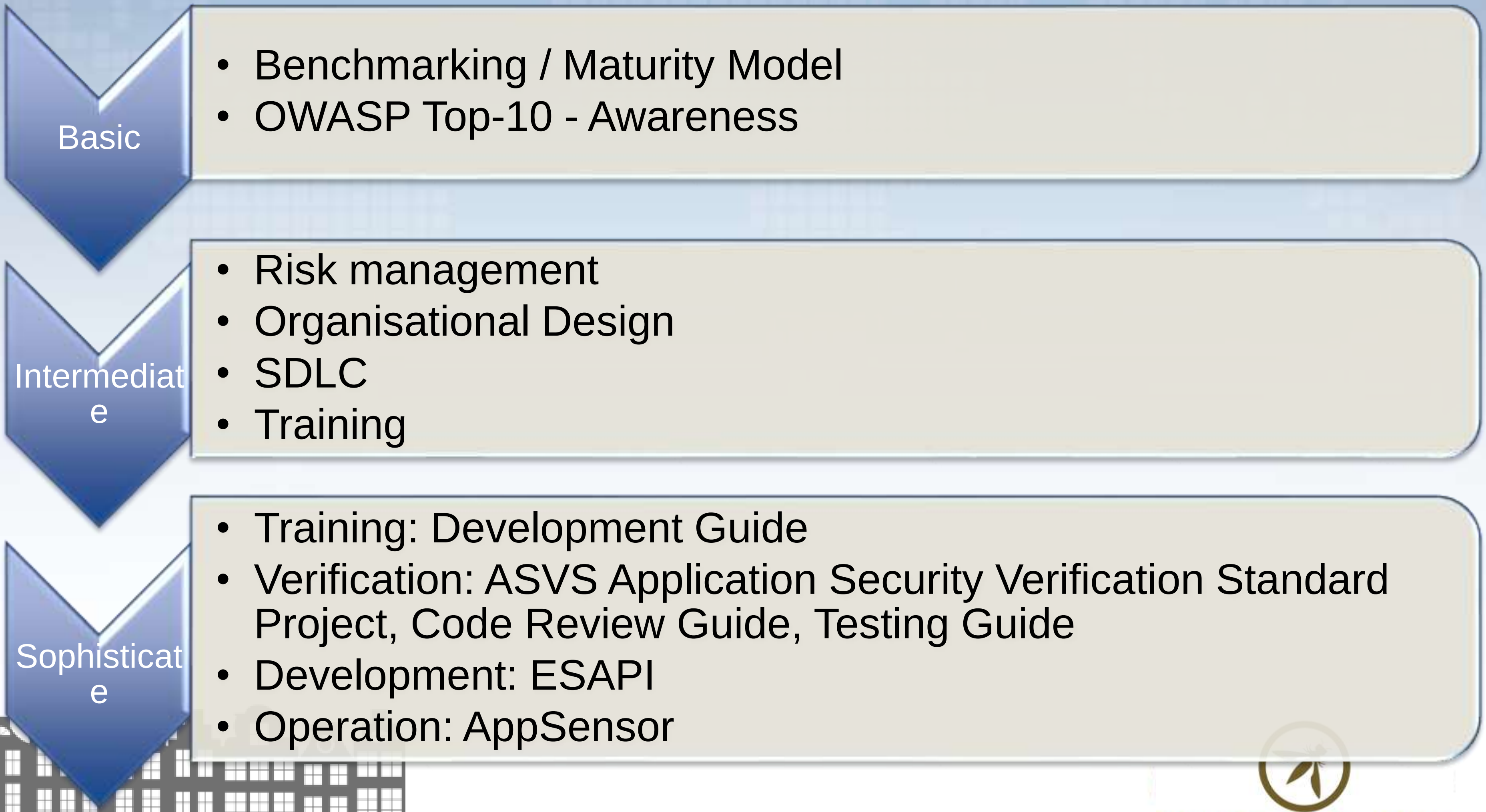
WebGoat Project

Testing Guide

ASVS - Application Security Verification Standard

CISO Survey

One Roadmap Example



Basic

- Benchmarking / Maturity Model
- OWASP Top-10 - Awareness

Intermediate

- Risk management
- Organisational Design
- SDLC
- Training

Sophisticate

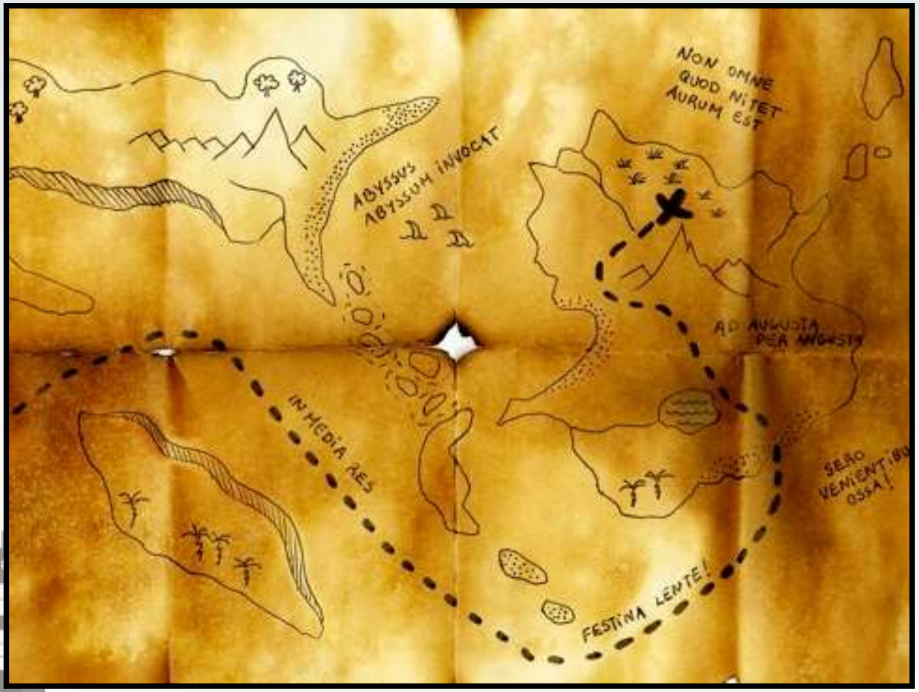
- Training: Development Guide
- Verification: ASVS Application Security Verification Standard Project, Code Review Guide, Testing Guide
- Development: ESAPI
- Operation: AppSensor

Maturity Models & Benchmarking

Benchmarking

Or:

Where are we? – And where are we going?



Maturity Models & Benchmarking

- Review of existing security efforts
- Benchmarking, Measuring Progress and Maturity Models

- Software Assurance Maturity Model (SAMM, http://www.opensamm.org)
- ISO 27000s
- Capability Maturity Model (CMM)
- ...

Your choice

BSIMM, or another x00 page model….

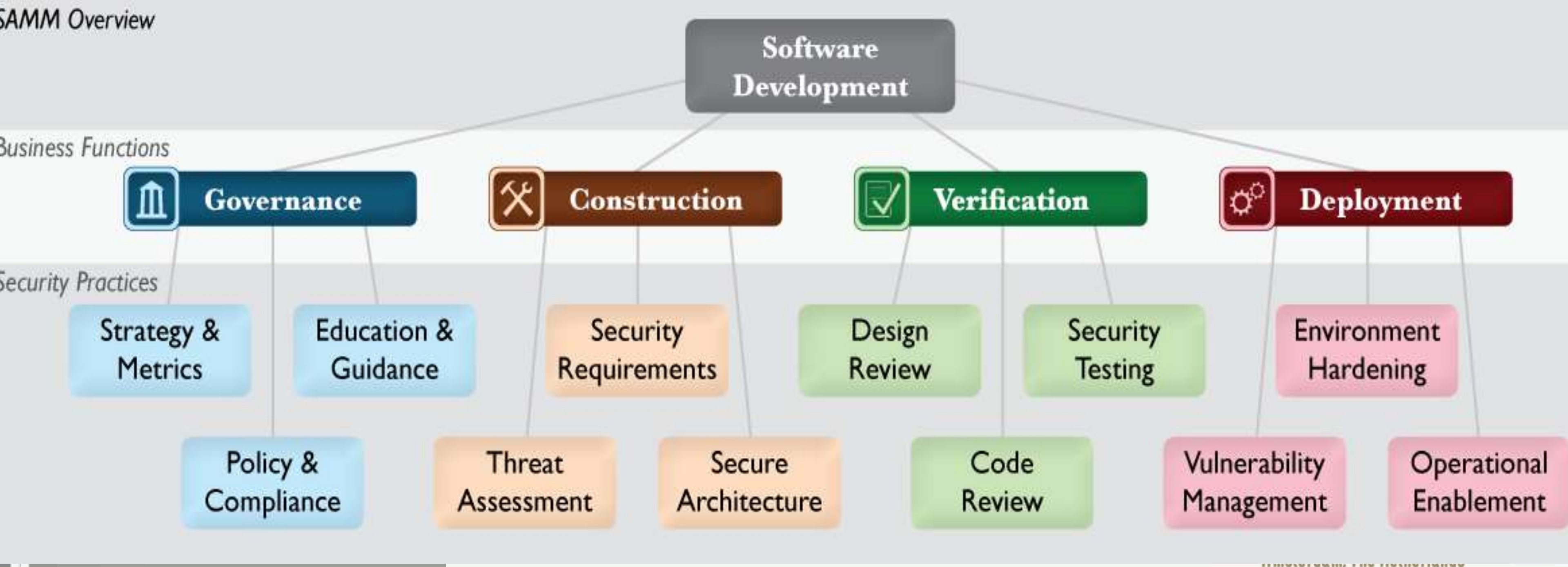
- Sophisticated and detailed, but….

openSAMM

- Short, but easy
- First assessment done in a day….

SAMM Security Practices

- From each of the Business Functions, 3 Security Practices are defined
- The Security Practices cover all areas relevant to software security assurance
- Each one can be targeted individually for improvement



SAMM Overview

Software Development

Business Functions

Governance

Construction

Verification

Deployment

Security Practices

Strategy & Metrics

Policy & Compliance

Education & Guidance

Threat Assessment

Security Requirements

Secure Architecture

Design Review

Code Review

Security Testing

Vulnerability Management

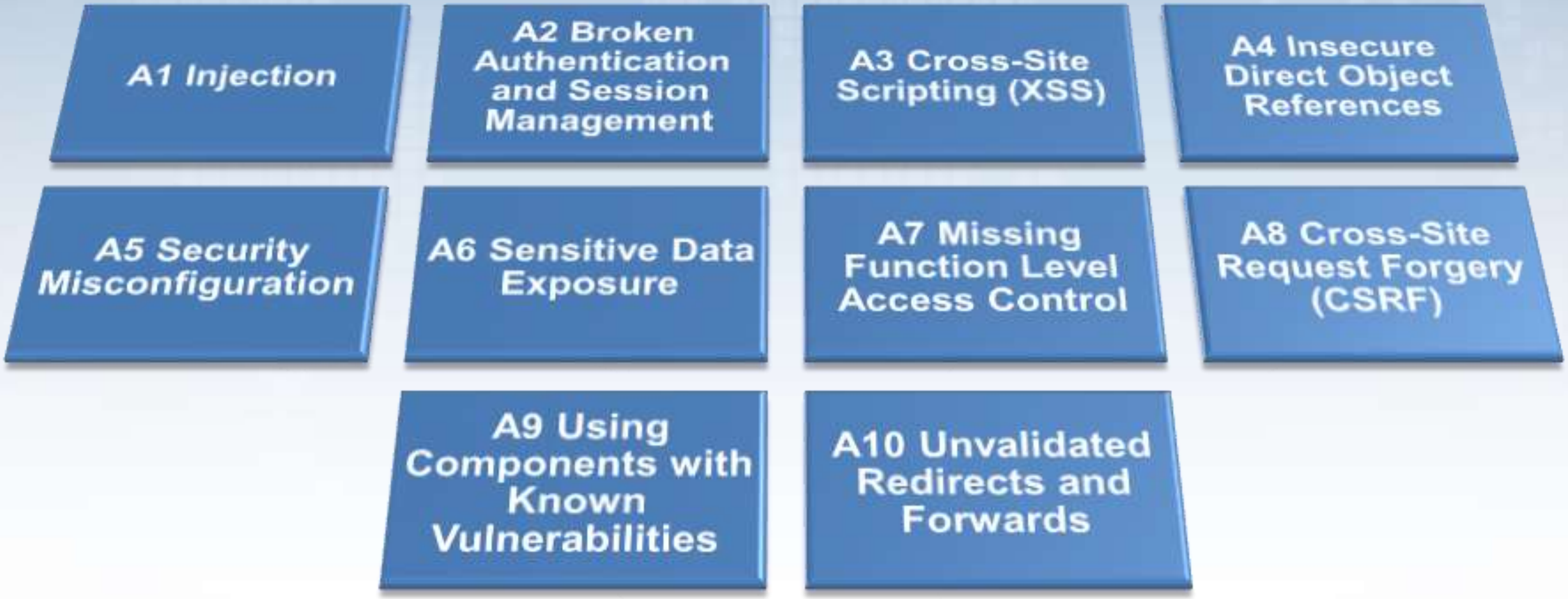
Environment Hardening

Operational Enablement

Basic awareness training….

- Build / Buy / Use….

OWASP Top 10 – Awareness & Training



- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Components with Known Vulnerabilities
- A10 Unvalidated Redirects and Forwards

OWASP Top-10 version 2013 - how

- Easy to use to start a first discussion and awareness
  - Initial developer training (1.5 hours)
  - Management awareness
  - Available in many languages (Spanish, Chinese, Japanese, Korean, Vietnamese, Indonesian, …)
  - Also other Top-10 for cloud, …
- But: there exist more risks beyond top-10!
- Referenced by many external standards, regulation and best practices, e.g. PCI DSS etc.

OWASP Top-10

- Usually a good first awareness training for developers (~1-2 hours)
- Recommend to tailor it to your application landscape: make it meaningful for them as some of the security risks may not be as urgent in your organisation as others
- Enrich with examples / use cases from your applications

… and some more Training

- OWASP Top-10
- Secure Coding Practices
- Cheatsheets
- Webgoat

Secure Coding Practices Quick Reference Guide

- Good next step of “To do” after initial “OWASP Top-10”
- Technology agnostic coding practices
- What to do, not how to do it
- Compact (17 pages), comprehensive checklist format
- Focuses on secure coding requirements, rather then on vulnerabilities and exploits
- Includes cross referenced glossary to get developers and security folks talking the same language
  - Tailor to your application landscape
(not all parts may be equally important for your organisation).

- Goal: Build a secure coding kick-start tool, to help development teams quickly understand secure coding
- Originally developed for use inside The Boeing Company, July 2010, Boeing assigned copyright to OWASP

Secure Coding Practices Quick Reference Guide Summary

Help development teams to quickly understand secure coding practices

Assist defining requirements and adding them to policies and contracts

Context and vocabulary for interactions with security staff

Easy desk reference

OWASP Cheat Sheet Series

- Transport Layer Protection Cheat Sheet
- Authentication Cheat Sheet
- Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet
- DOM based XSS Prevention Cheat Sheet
- Cryptographic Storage Cheat Sheet
- Session Management Cheat Sheet
- Input Validation Cheat Sheet
- XSS (Cross Site Scripting) Prevention Cheat Sheet
- HTML5 Security Cheat Sheet
- SQL Injection Prevention Cheat Sheet
- Forgot Password Cheat Sheet
- Web Service Security Cheat Sheet

Webgoat

- Exercise with Example Web Application to illustrate typical Security Flaws within Web-Applications
- Practice Lessons for Common Vulnerabilities
- Teach a Structured Approach to Testing and Exploiting
- Give Practical Training and Examples

Risk Management

What &
How much
is enough?

Risk Management

Risk: The probable frequency and probable magnitude of future loss

- Why – or where do you put your resources?
- Methods: OWASP, ISO-27005, ITIL, NIST SP 800-30, OCTAVE
- Asset Classification, Threat Analysis & Vulnerability Assessment
- What do you do with Risks?
- Quality vs. quantity, Human behavior & risk

Risk management

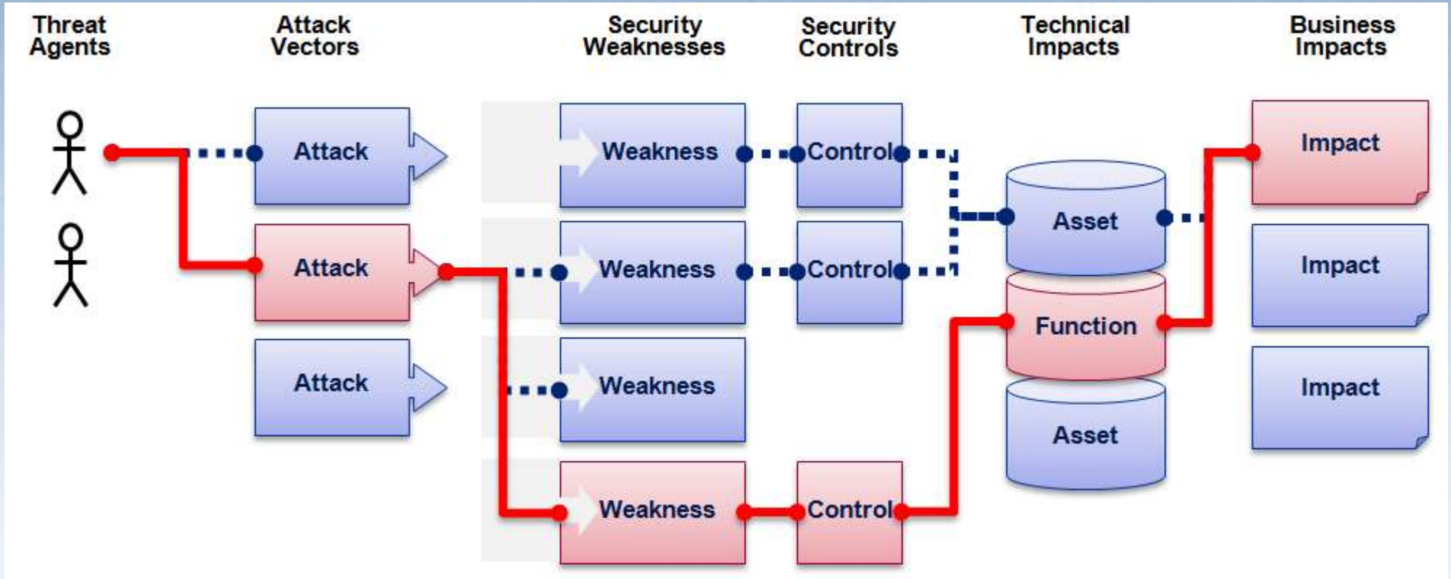
Why / Benefits:

- Allocation of resources
  - Asset Classification and values?
  - Threats Analysis & Scenarios?
- Establish ownership of assets, risk and controls

Methods:

- OWASP
- FAIR (Factor Analysis of Information Risk)
- ISO 27005, ISO 31000
- Risk IT (ISACA)
- …

OWASP Top 10 Risk Rating Methodology

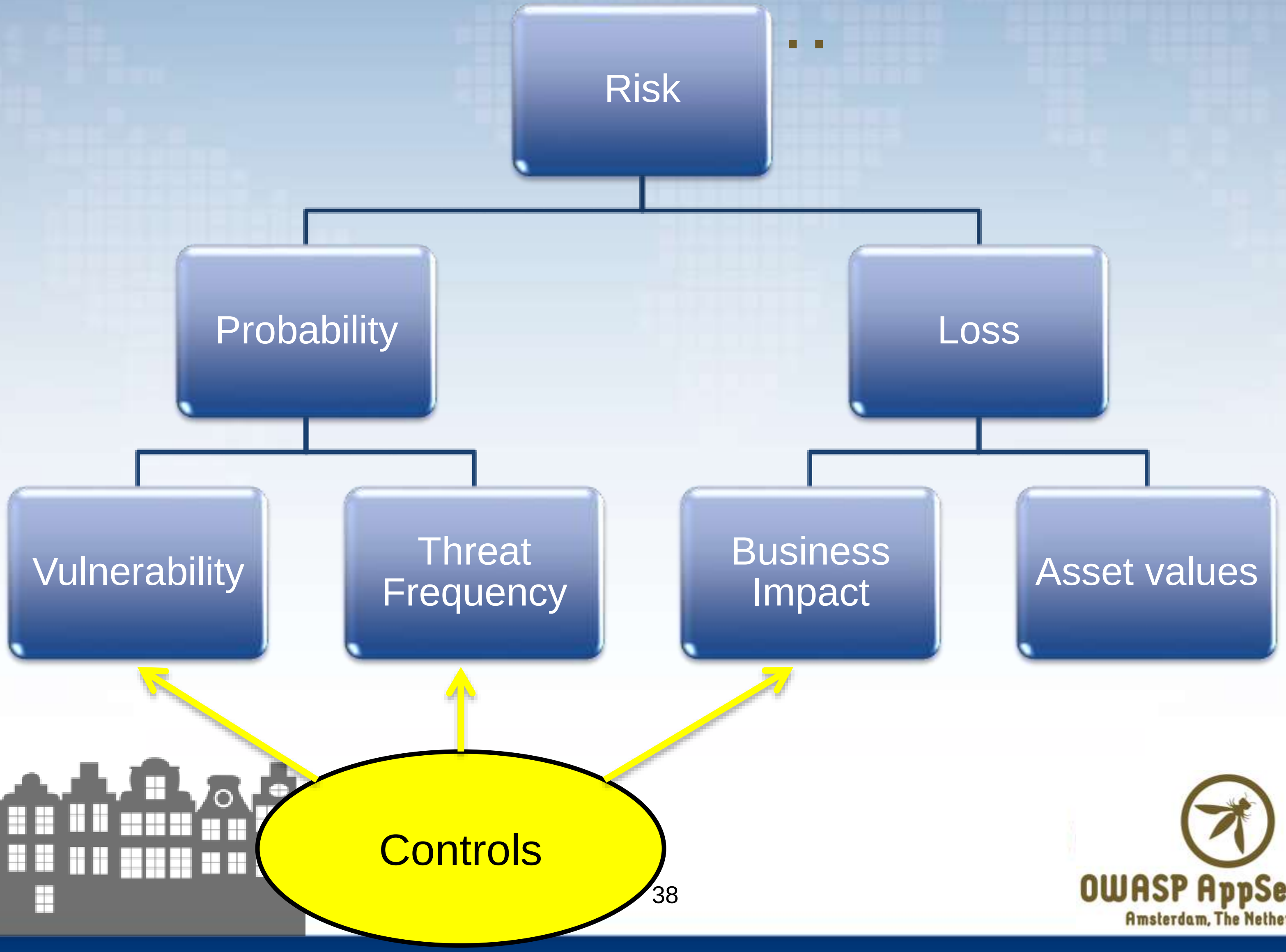


Threat Agent		Attack Vector	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
?	1	Easy	Widespread	Easy	Severe	?
	2	Average	Common	Average	Moderate	
	3	Difficult	Uncommon	Difficult	Minor	
		1	2	2	1	
			1.66	*	1	

Injection Example

1.66 weighted risk rating

Other methods: e.g. ISO 27005, ..



Risk

Probability

Loss

Vulnerability

Threat Frequency

Business Impact

Asset values

Controls

Risk Heat Map – Threat Level

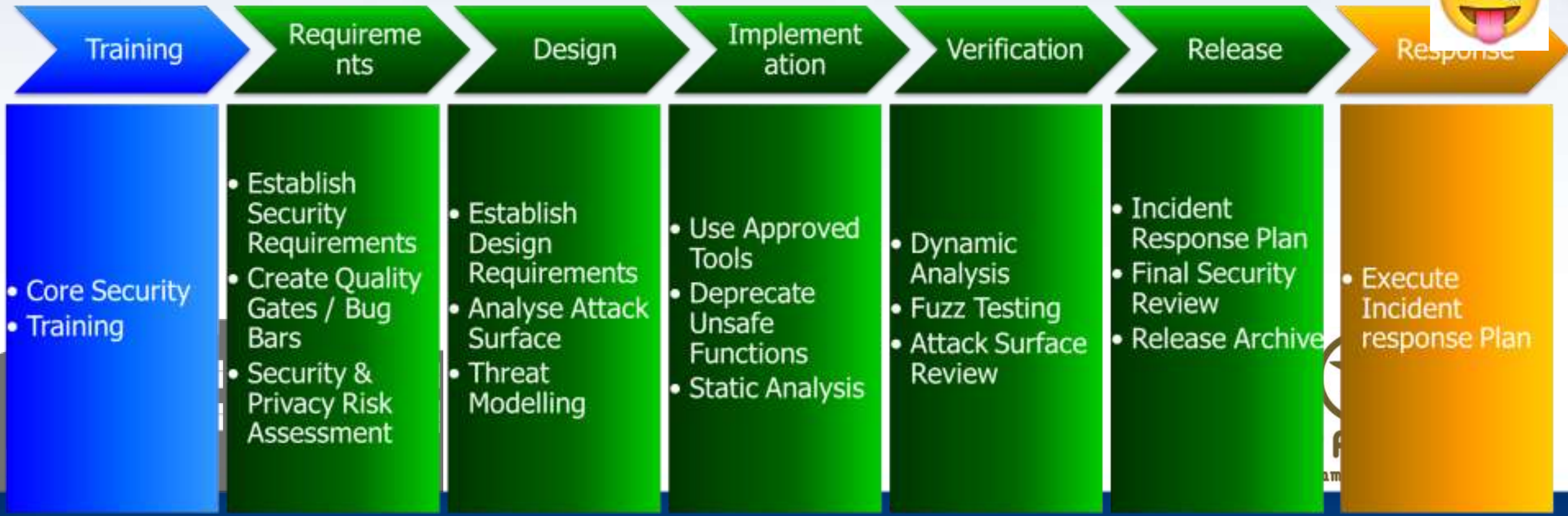
Medium	Medium	High	High	High
Medium	Medium	Medium	High	High
Low	Medium	Medium	Medium	High
Low	Low	Medium	Medium	Medium
Low	Low	Low	Medium	Medium

Likelihood

Impact

Secure Software Development Lifecycle - SDLC

- e.g. Microsoft has a nice one: SDL
  - comprehensive, but heavy. But has some very good ideas; btw. if you don’t like Microsoft, Adobe has a nice one published, too. “Adobe Secure Product Lifecycle”
  - => But if you want to get ready in time for your holiday (read: in the next 2 years) => don’t try to do all of it at once…. – Cherry pick what is good for you…



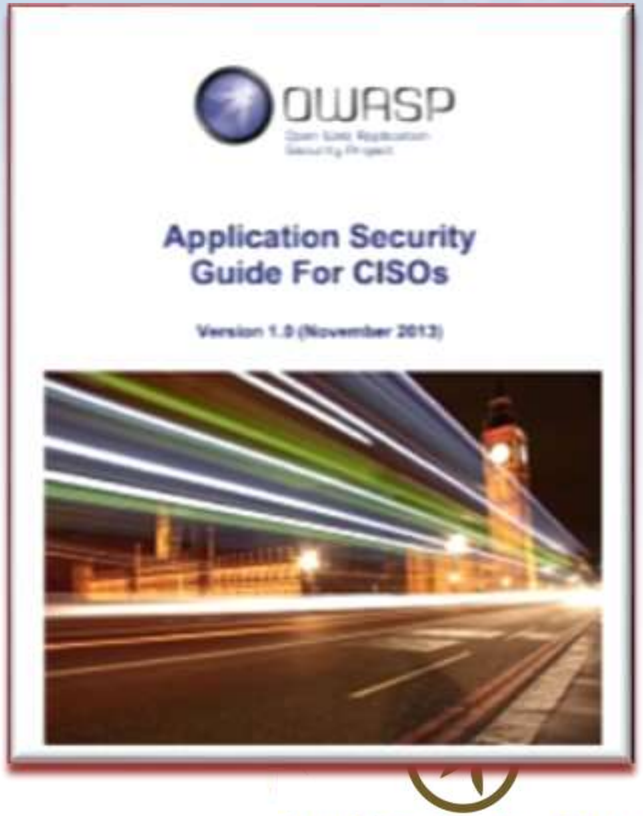
Training	Requirements	Design	Implementation	Verification	Release	Response
• Core Security • Training	• Establish Security Requirements • Create Quality Gates / Bug Bars • Security & Privacy Risk Assessment	• Establish Design Requirements • Analyse Attack Surface • Threat Modelling	• Use Approved Tools • Deprecate Unsafe Functions • Static Analysis	• Dynamic Analysis • Fuzz Testing • Attack Surface Review	• Incident Response Plan • Final Security Review • Release Archive	• Execute Incident response Plan

Security Strategy and want some “high-level stuff”

- E.g. not sure what should be in your security strategy?

=> OWASP CISO Guide

- **OWASP CISO Guide:** https://www.owasp.org/images/d/d6/Owasp-ciso-guide.pdf



OWASP

Open Web Application Security Project

Application Security Guide For CISOs

Version 1.0 (November 2013)

Want some forward looking intelligence? Need some data to justify your proposals?

- Further Resources:
  - OWASP CISO Survey https://www.owasp.org/index.php/OWASP_CISO_Survey

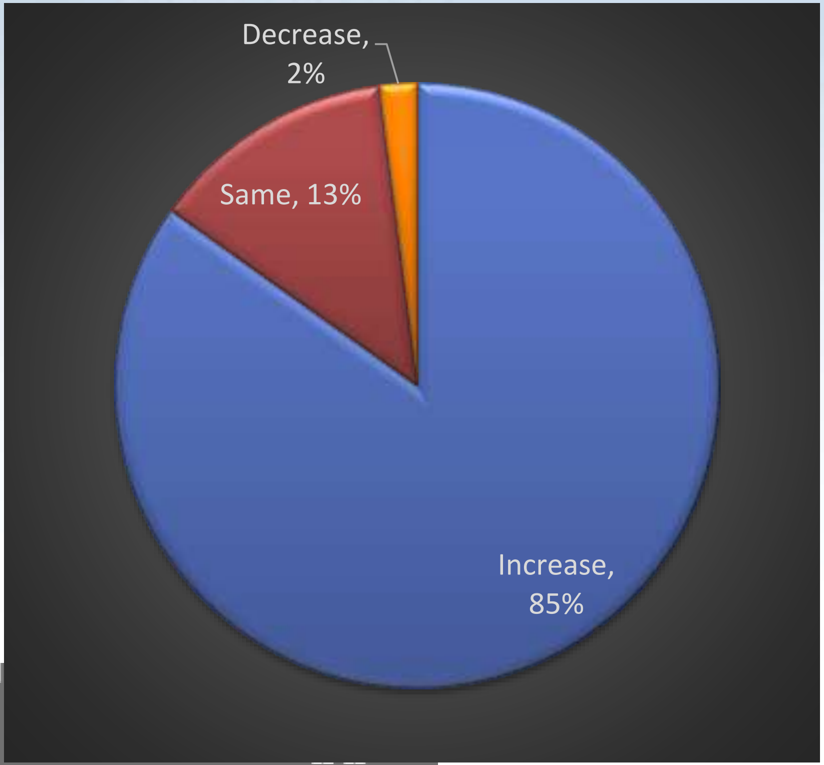
OWASP
Open Web Application Security Project

CISO Survey and Report 2013

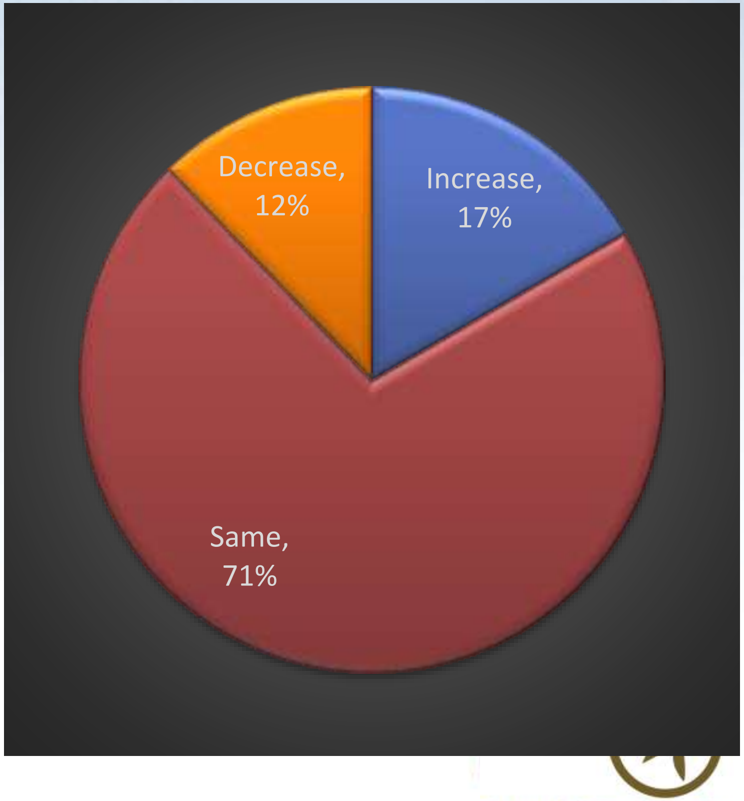
Version 1.0.2 (January 2014)

CISO Survey: External Threats are on the Rise!

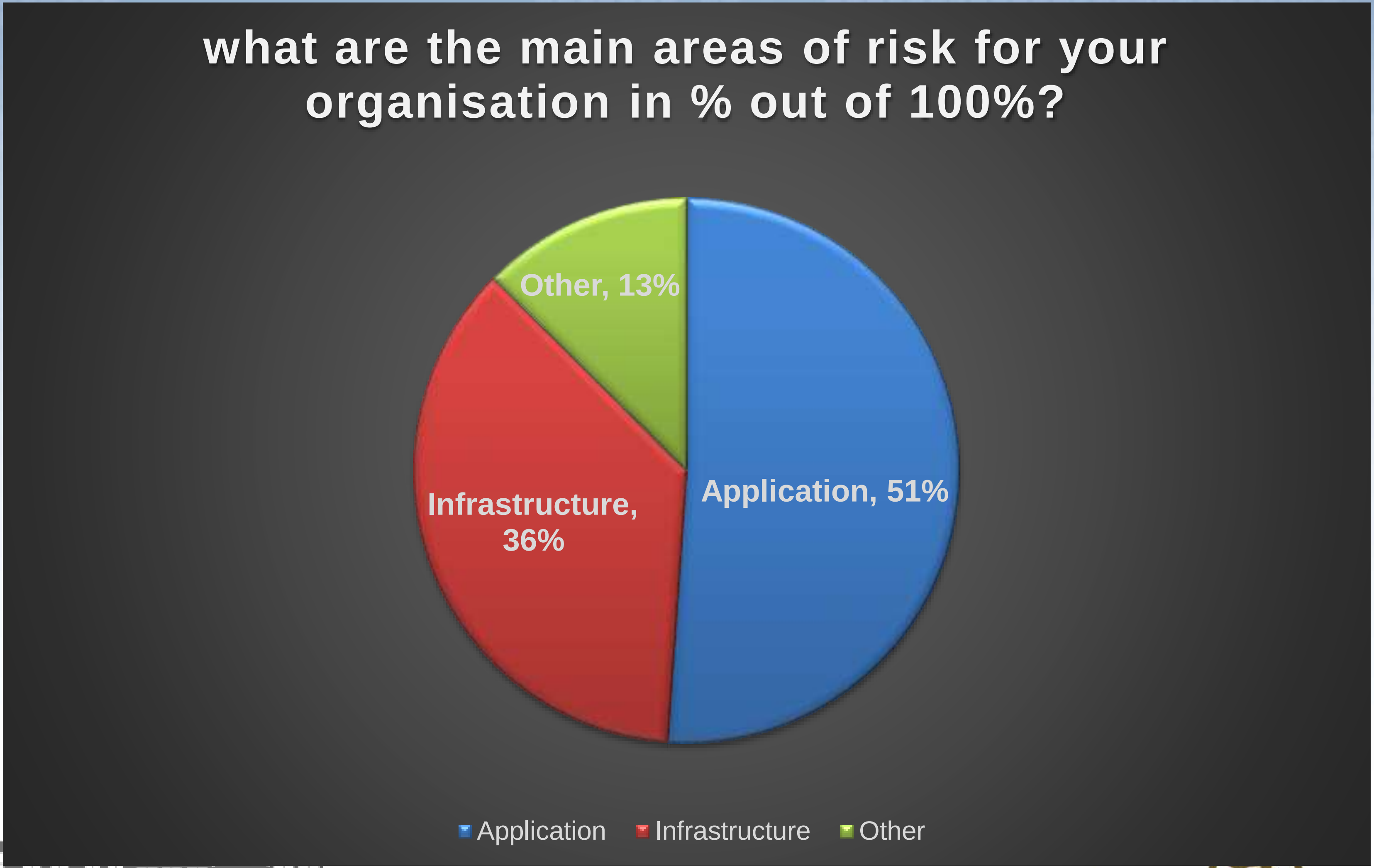
- External attacks or fraud (e.g., phishing, website attacks)



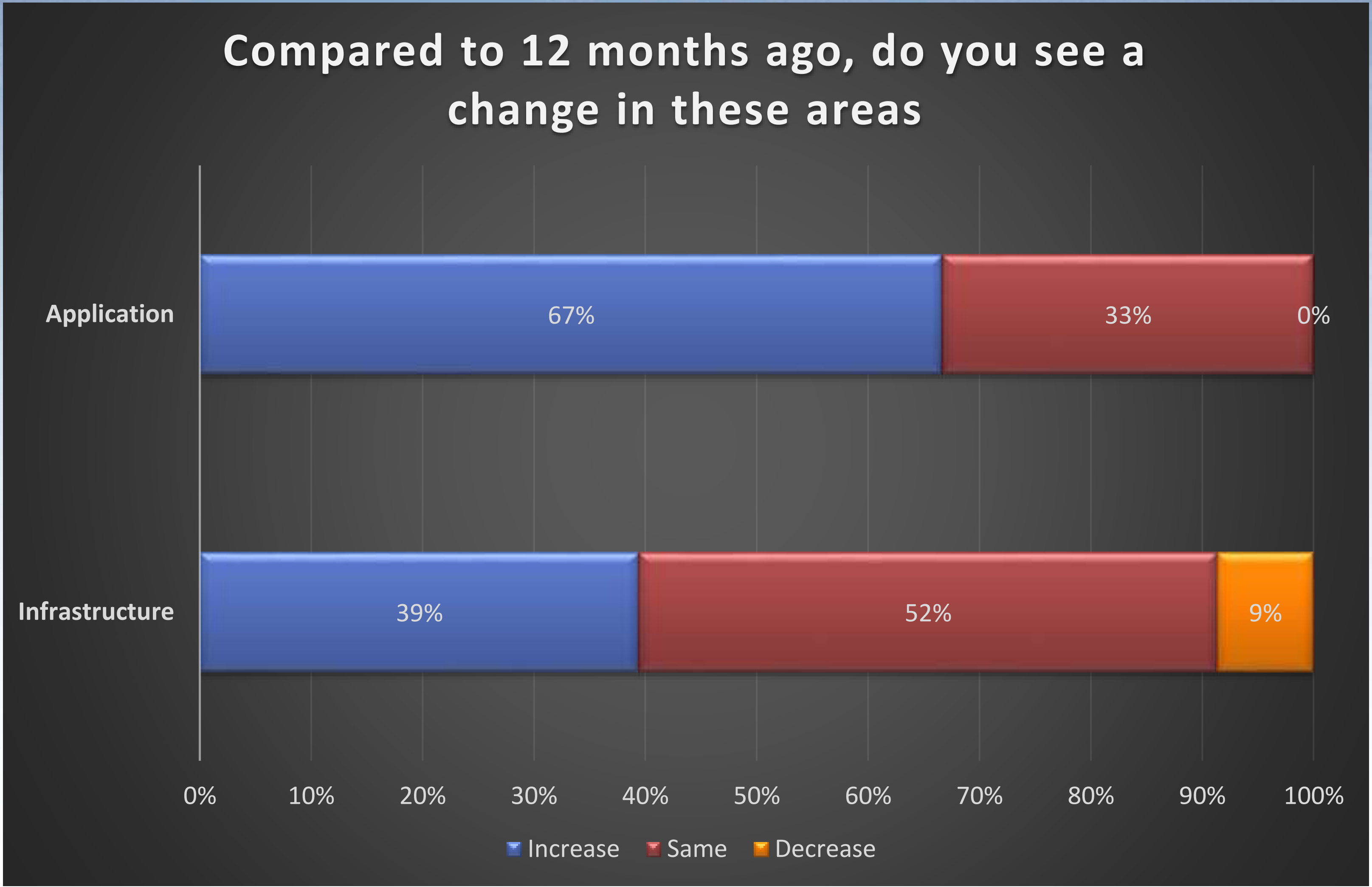
Internal attacks or fraud (e.g., abuse of privileges, theft of information)



CISO Survey: Change in the threats facing your organization



CISO Survey : Change in the Threats

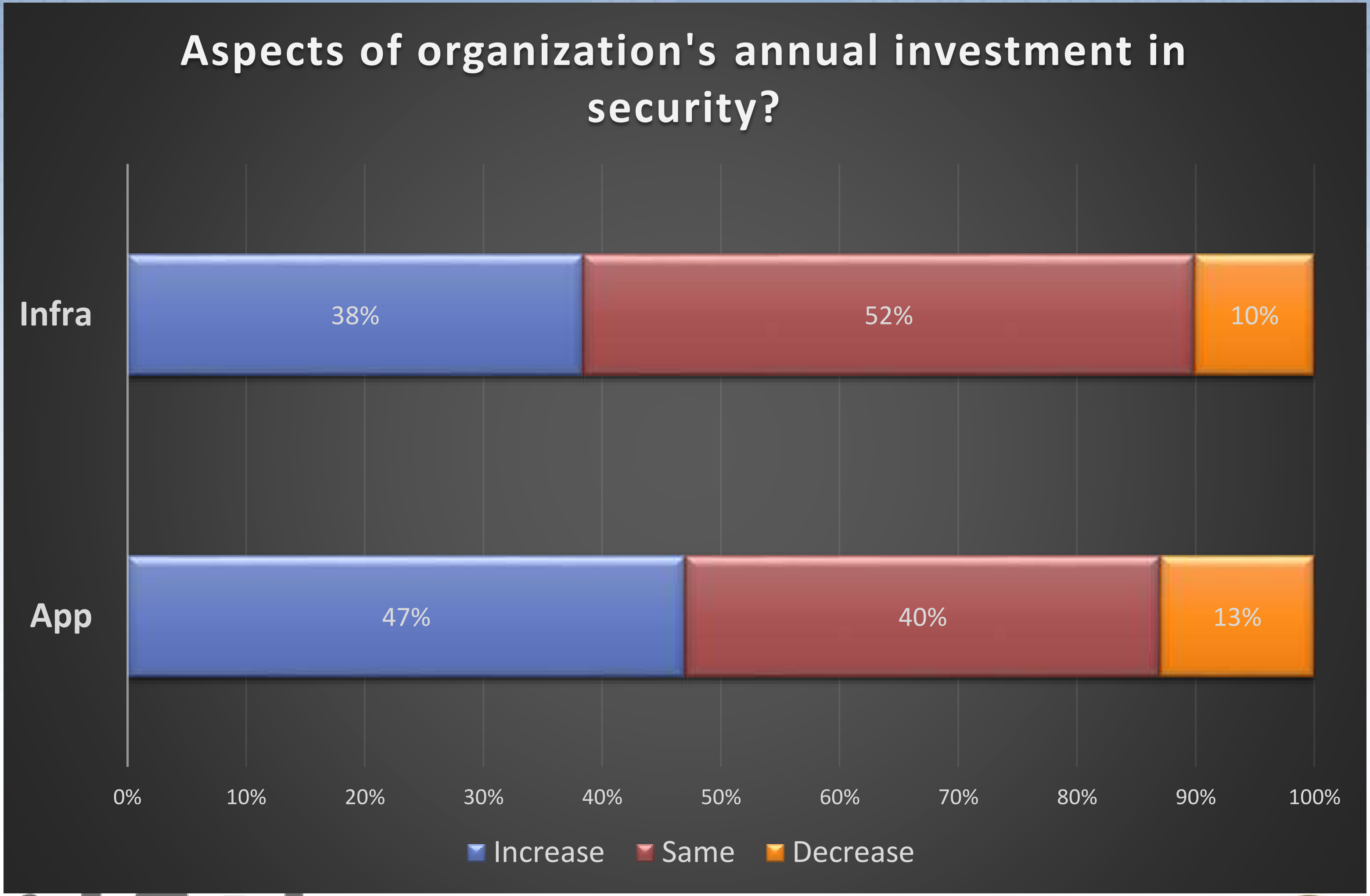


OWASP AppSecEU 15
Amsterdam, The Netherlands

•Top five sources of application security risk within your organization?

- Lack of awareness of application security issues within the organization
- Insecure source code development
- Poor/inadequate testing methodologies
- Lack of budget to support application security initiatives
- Staffing (e.g., lack of security skills within team)

CISO Survey & Report: Investments in Security



OWASP AppSecEU 15
Amsterdam, The Netherlands

- Top application security priorities for the coming 12 months.

Security awareness and training for developers

Secure development lifecycle processes (e.g., secure coding, QA process)

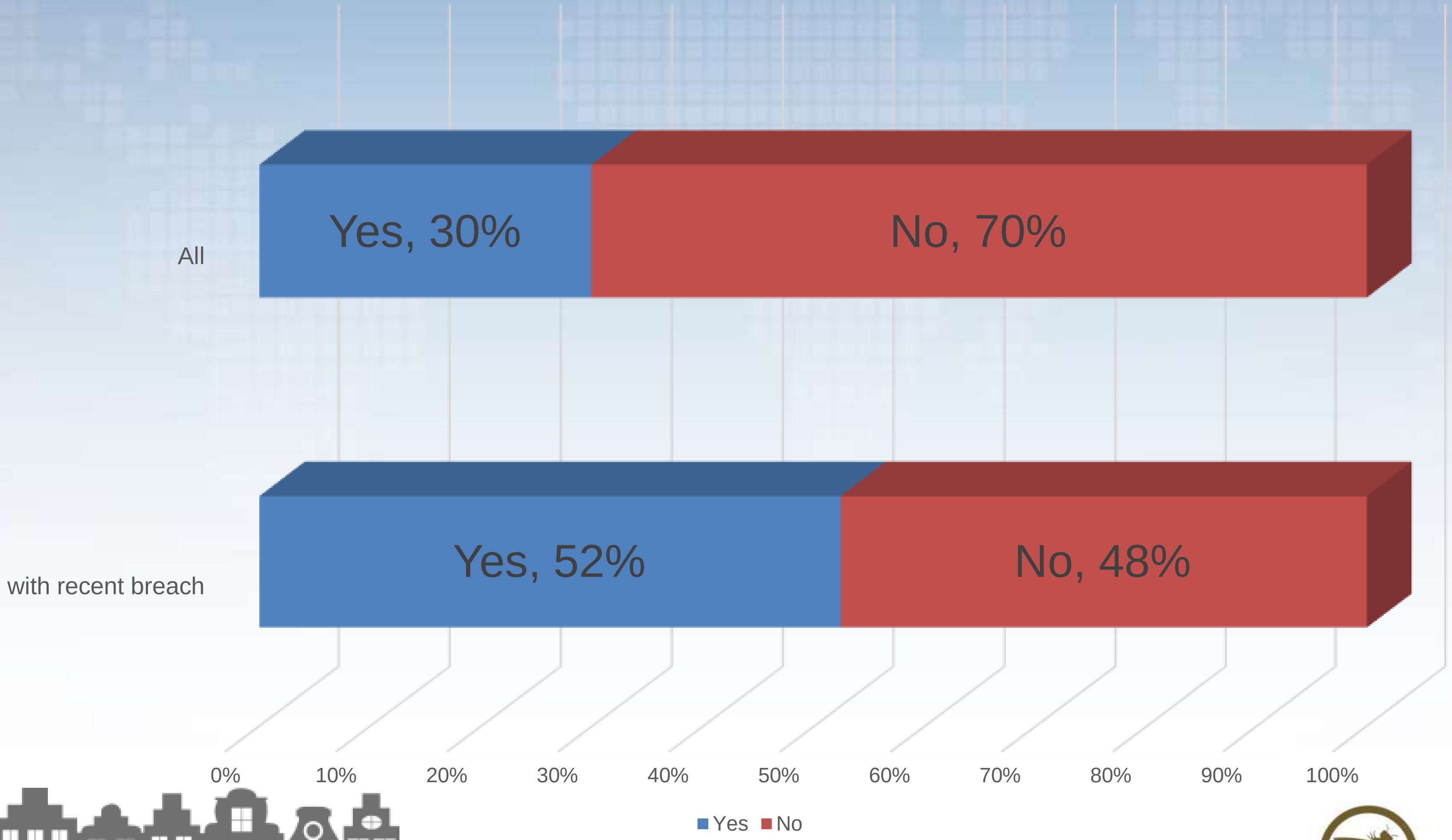
Security testing of applications (dynamic analysis, runtime observation)

Application layer vulnerability management technologies and processes

Code review (static analysis of source code to find security defects)

Spending after security incident

Is your organization spending more on security in response to a security incident?



OWASP AppSecEU 15
Amsterdam, The Netherlands

- Top five challenges related to effectively delivering your organization's application security initiatives

Availability of skilled resources

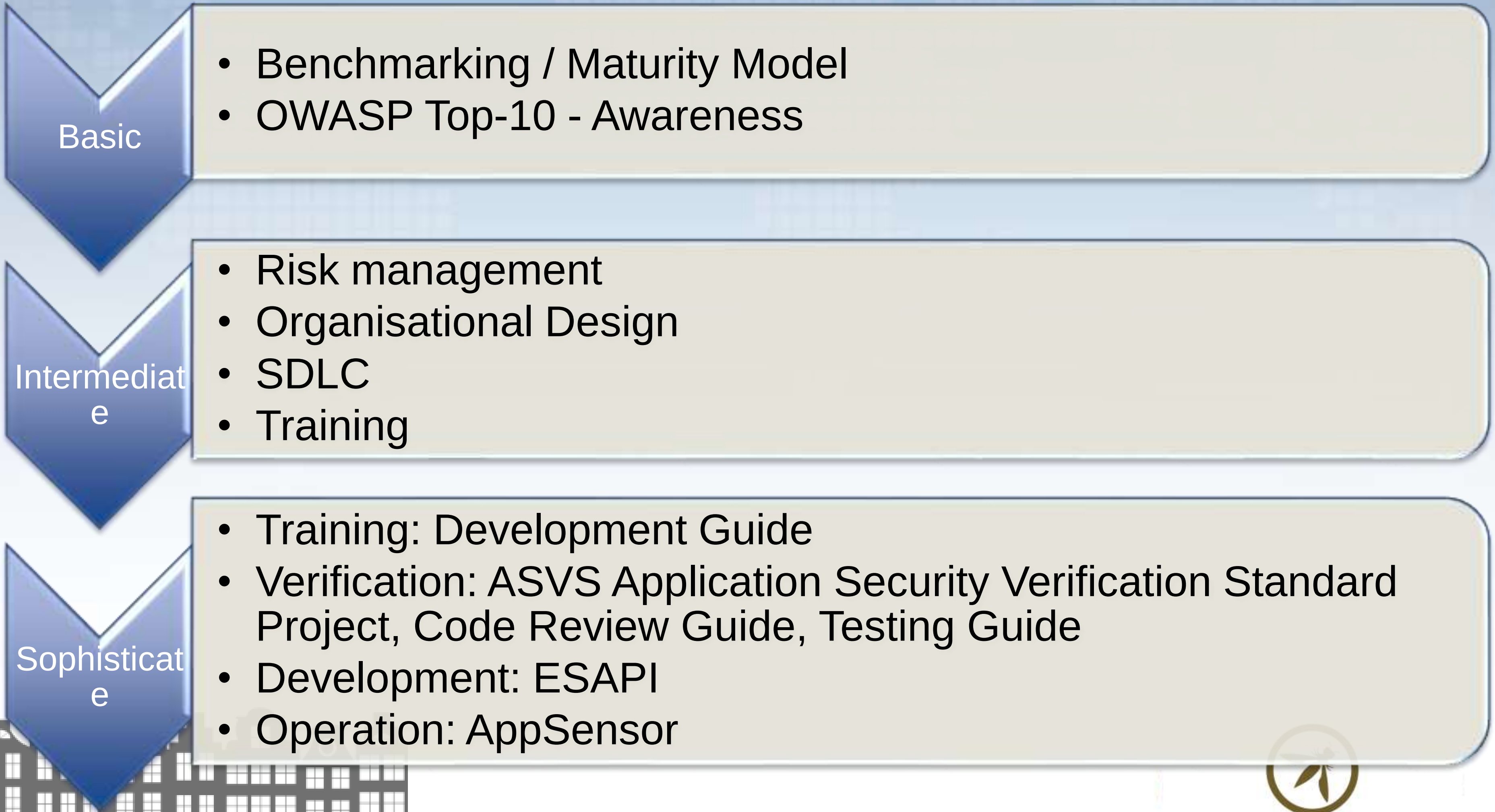
Level of security awareness by the developers

Management awareness and sponsorship

Adequate budget

Organizational change

One Roadmap Example



Basic

- Benchmarking / Maturity Model
- OWASP Top-10 - Awareness

Intermediate

- Risk management
- Organisational Design
- SDLC
- Training

Sophisticate

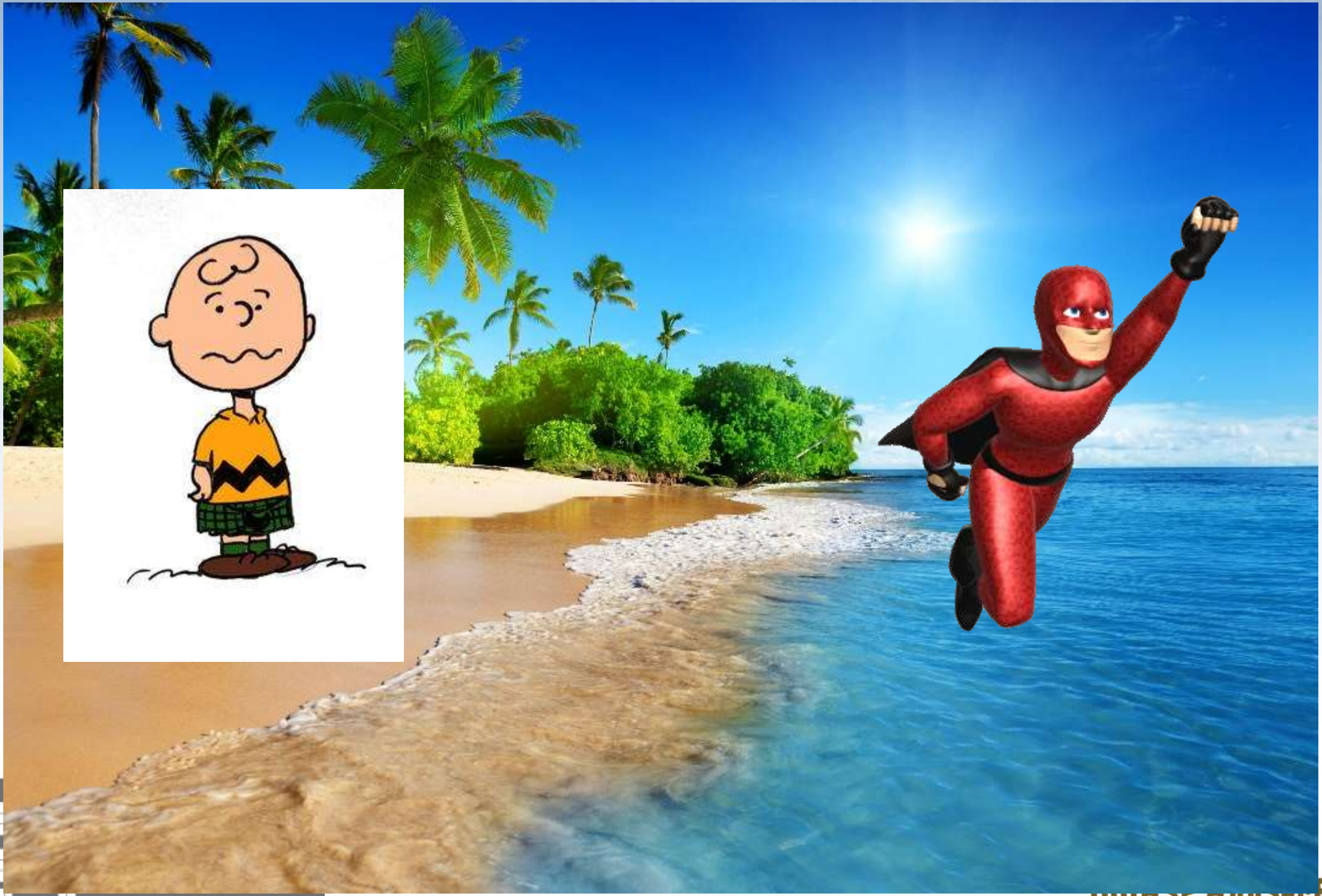
- Training: Development Guide
- Verification: ASVS Application Security Verification Standard Project, Code Review Guide, Testing Guide
- Development: ESAPI
- Operation: AppSensor

So how are we doing?

• Have a security strategy?	Template, write one.	✓
• Upgrade your Security policy?	Guide, Coding guide	✓
• SDLC – do we have one, do we live it? And if yes, why did everything go sideways….?	Learn from Microsoft SDL	✓
• How do we benchmark?	openSAMM, CISO Survey	✓
• Use Risk Management?	ISO 27005	✓
• Have a security team / organise it?	Hey, we need to leave some work also for you…	
• Security training and awareness?	OWASP Top-10, and more	✓
• Secure coding guidelines….	OWASP Secure Coding Quick Reference Guide	✓

…. All within 3 months?

Will your holiday be saved?



- Questions?
  - What OWASP tools do you think will be useful for you right away?
  - What would you like to have in the future?

OWASP AppSecEU 15
Amsterdam, The Netherlands

Thank you