ISACA®
Trust in, and value from, information systems
Venice Chapter

VI Venice AppSeC Conference

In collaborazione con

OWASP
The Open Web Application Security Project

Università Ca'Foscari Venezia

Dipartimento di Scienze Ambientali Informatica e Statistica

Venezia, Università Ca' Foscari

5 Ottobre 2018

Matteo Meucci

OWASP SwSec 5D Framework

<AGENDA>

1. Software Security Introduction
2. SDLC frameworks: how OWASP can help on software security
3. OWASP Software Security 5 Dimension Framework
4. Apply the models to a real case
5. Some wrong approaches
6. Conclusions

</AGENDA>

Who Am I?

Informatics Engineer (since 2001)

Research:

- OWASP contributor (since 2002)
- **OWASP-Italy Chair (since 2005)**
- OWASP Testing Guide Lead (since 2006)

MINDED SECURITY
The Software Security Company

Work:

- 17+ years on Information Security focusing on Software Security
- CEO @ Minded Security – The Software Security Company (since 2007)

What is the subject today

Secure Design

SDLC

Costs to fix

Automation

Software Security

Governance

DevOps

Tools

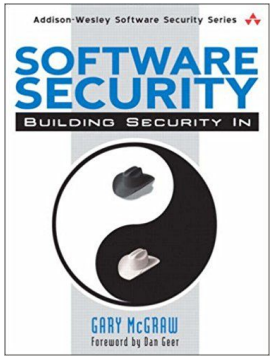
OWASP

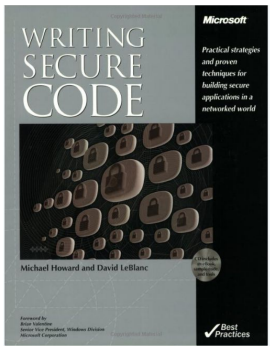
SAST, DAST

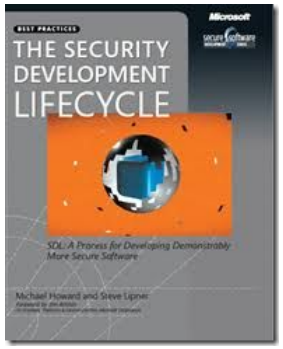
Processes

1. Software Security Intro

Software Security: a brief history



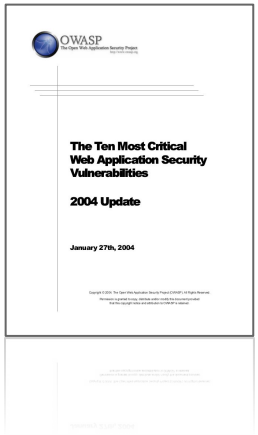




OWASP Open Web Application Security Project

From: Bill Gates
Sent: Tuesday, January 15, 2002 5:22 PM
To: to every full-time employee at Microsoft
Subject: Trustworthy computing

...new capabilities is the fact that it is designed from the ground up to deliver **Trustworthy Computing.**

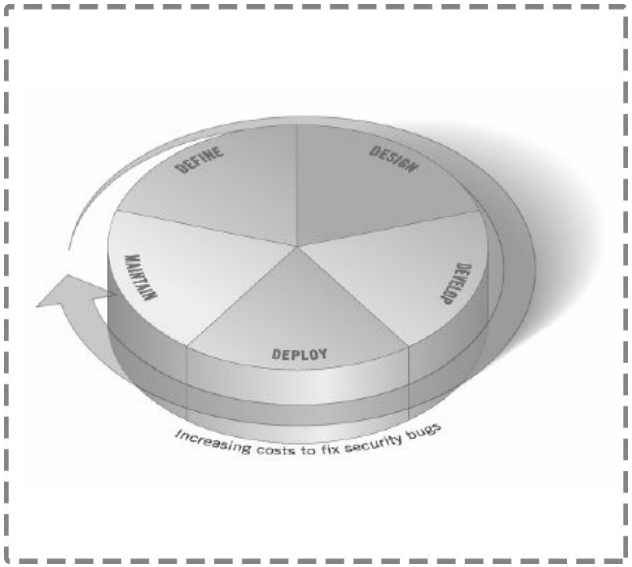


2001 2002 2004 2005 2006

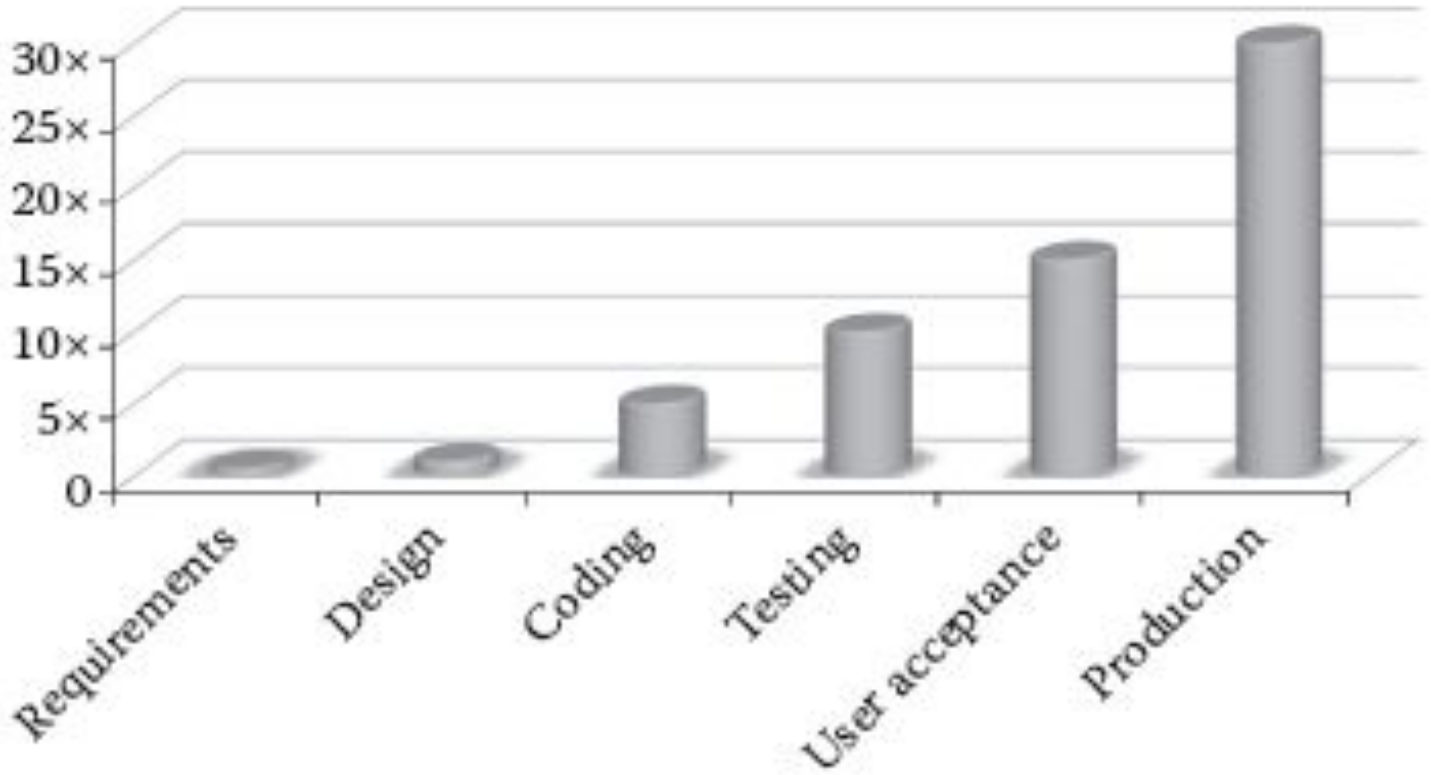
Traditional SDLC (Software Development Life Cycle)

Traditional Software Development Life Cycle has the following phases:

- **Define:** definition of the software specifications and requirements;
- **Design:** identifies general requirements for design;
- **Develop:** software development phase;
- **Deploy:** software goes in production;
- **Maintain:** software change management.



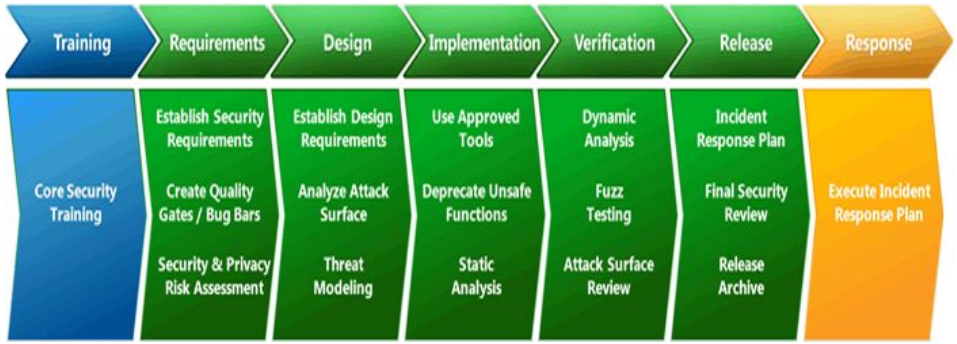
Costs related to fixing a vulnerability



Sources: Official (ISC)2 Guide to CSSLP (2011)

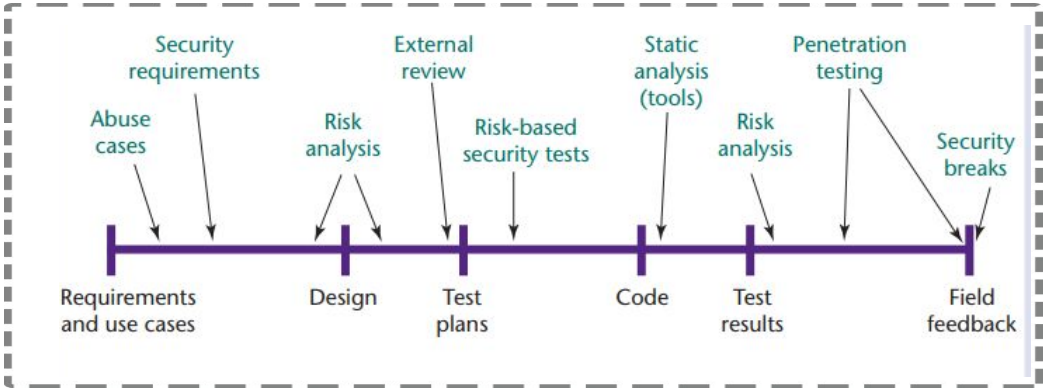
Traditional S-SDLC frameworks

A Software Development Life Cycle (SDLC) is a framework that defines the process used by organizations to build an application from its inception to its decommission. Over the years, multiple standard SDLC models have been proposed (Waterfall, Iterative, Agile, etc.) and used in various ways to fit individual circumstances.



2006: Microsoft Security Development Lifecycle

2006: Building Security In



2006: Microsoft Security Development Lifecycle

The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost.

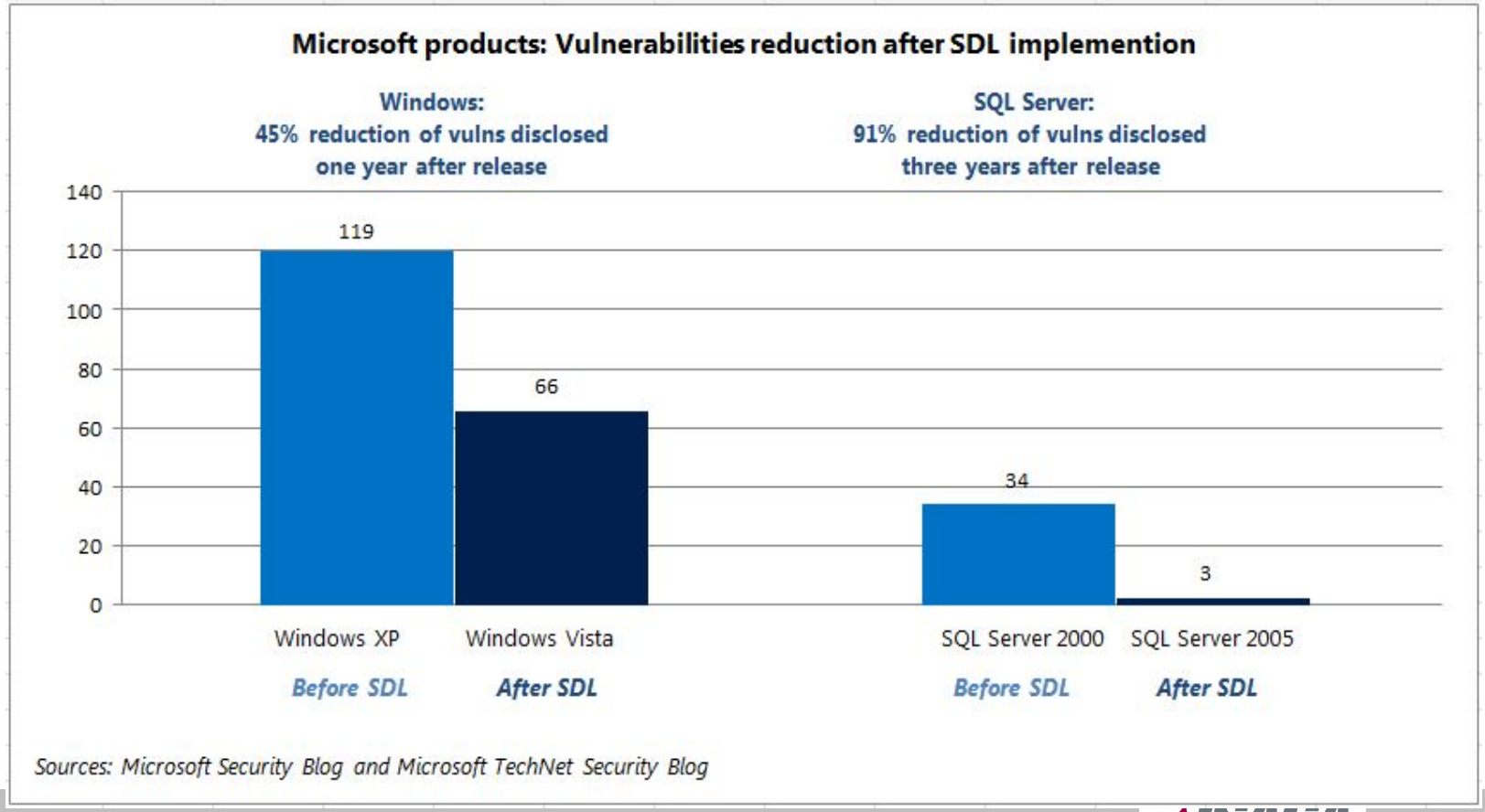
Microsoft created the first SDLC: built internally for MS software.

Released it for public in 2006.

1. TRAINING	2. REQUIREMENTS	3. DESIGN	4. IMPLEMENTATION	5. VERIFICATION	6. RELEASE	7. RESPONSE
1. Core Security Training	2. Establish Security Requirements	5. Establish Design Requirements	8. Use Approved Tools	11. Perform Dynamic Analysis	14. Create an Incident Response Plan	Execute Incident Response Plan
	3. Create Quality Gates/Bug Bars	6. Perform Attack Surface Analysis/ Reduction	9. Deprecate Unsafe Functions	12. Perform Fuzz Testing	15. Conduct Final Security Review	
	4. Perform Security and Privacy Risk Assessments	7. Use Threat Modeling	10. Perform Static Analysis	13. Conduct Attack Surface Review	16. Certify Release and Archive	

SDL Microsoft is an example of a complete and efficient SDLC implementation that perfectly fit to Microsoft SDLC.

The Microsoft SDL Process Guidance illustrates the way Microsoft applies the SDL to its own technologies and software. **Each organization being unique, it is important that you determine your own security requirements and which tools are appropriate for your organization.**



2. How OWASP can help on software security

www.OWASP.org

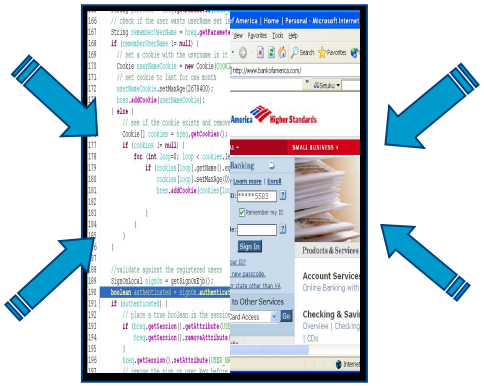
- The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit also registered in Europe as a worldwide charitable organization focused on **improving the security of software**.
- **Our mission is to make application security visible**, so that people and organizations can **make informed** decisions about true application security risks.
- Everyone is welcomed to participate in OWASP and all of our materials are available **under free and open software licenses.**

OWASP: The Open Web Application Security Project

I would like to build secure software

I would like to find all the security bugs in my software

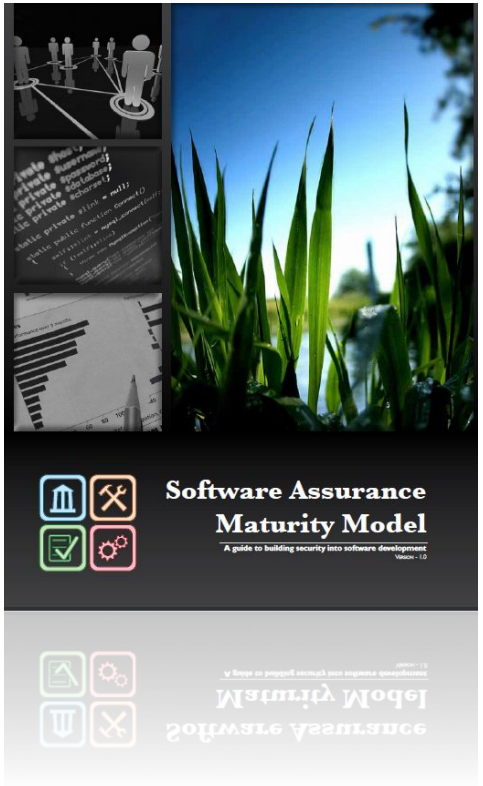
I would like to implement a Roadmap for Software Security



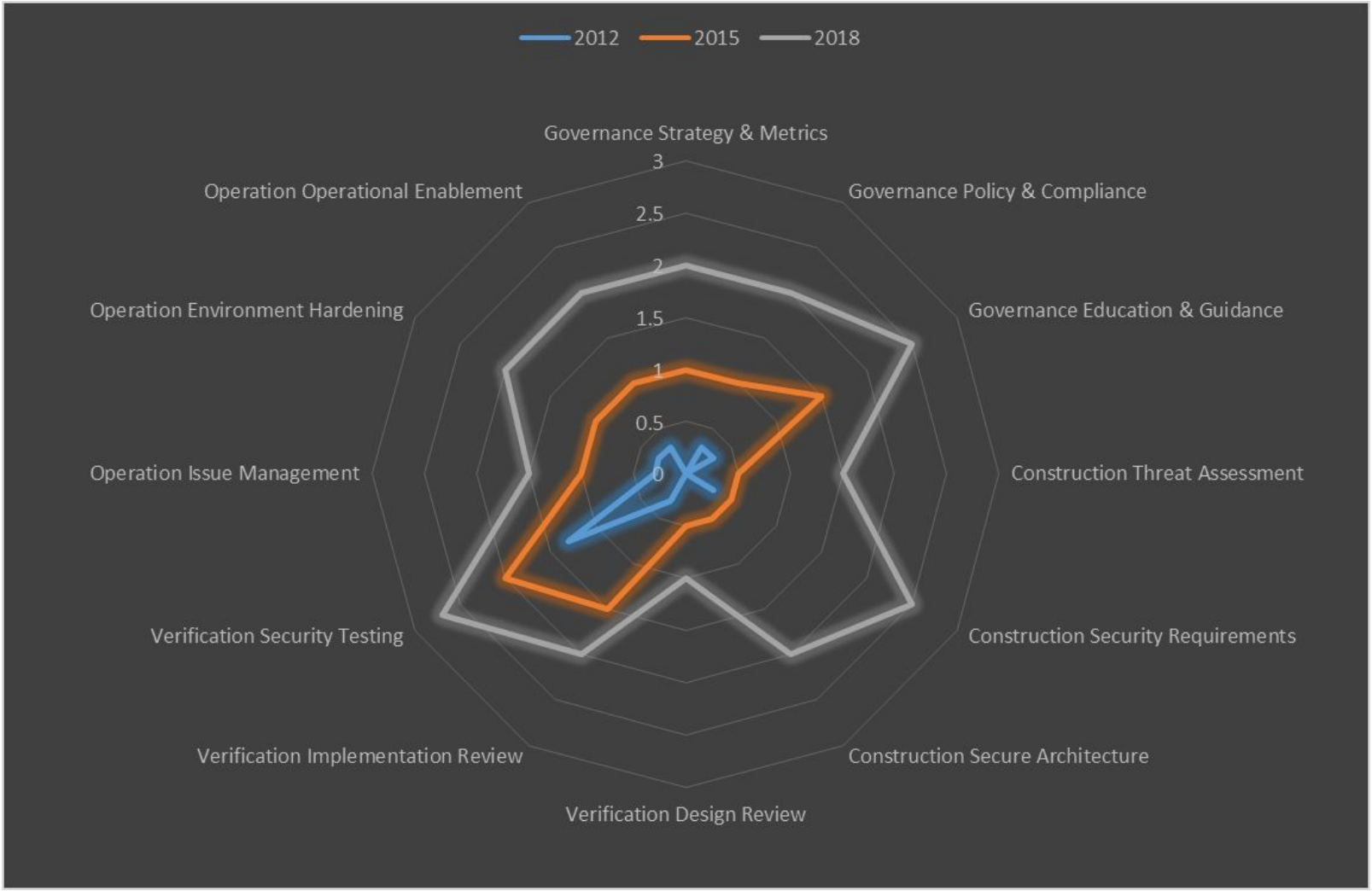
OWASP SAMM

The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is **tailored to the specific risks** facing the organization.

It represents the open standard world wide to create an internal SDLC and a roadmap to improve it.



Case Studies: 2012-2015-2018



Source: Minded Security 2018

3. OWASP Software Security 5 Dimension Framework

Traditional SDLC is not enough

Traditional SDLC frameworks lack of:

- level of awareness
- security team
- security standards
- security testing tools

Minded Security has develop a new and more practical framework that focus on 5 dimensions to evaluate the maturity of a Software Security framework and now have:

OWASP Software Security 5D framework

OWASP SwSec 5D

SwSec PROCESSES

- Risk Assessment - Security Requirements
- Threat Modeling - Security Design
- SCR, WAPT
- Software Acceptance - Security bug Fixing

Sw Sec TESTING

- SAST, DAST, IAST, RASP
- External manual SCR, WAPT

Sw Sec TEAM

- AppSec manager/CISO, Sec Champions, AppSec Specialists, Satellite Architects, Sat Developers,Sat Testers

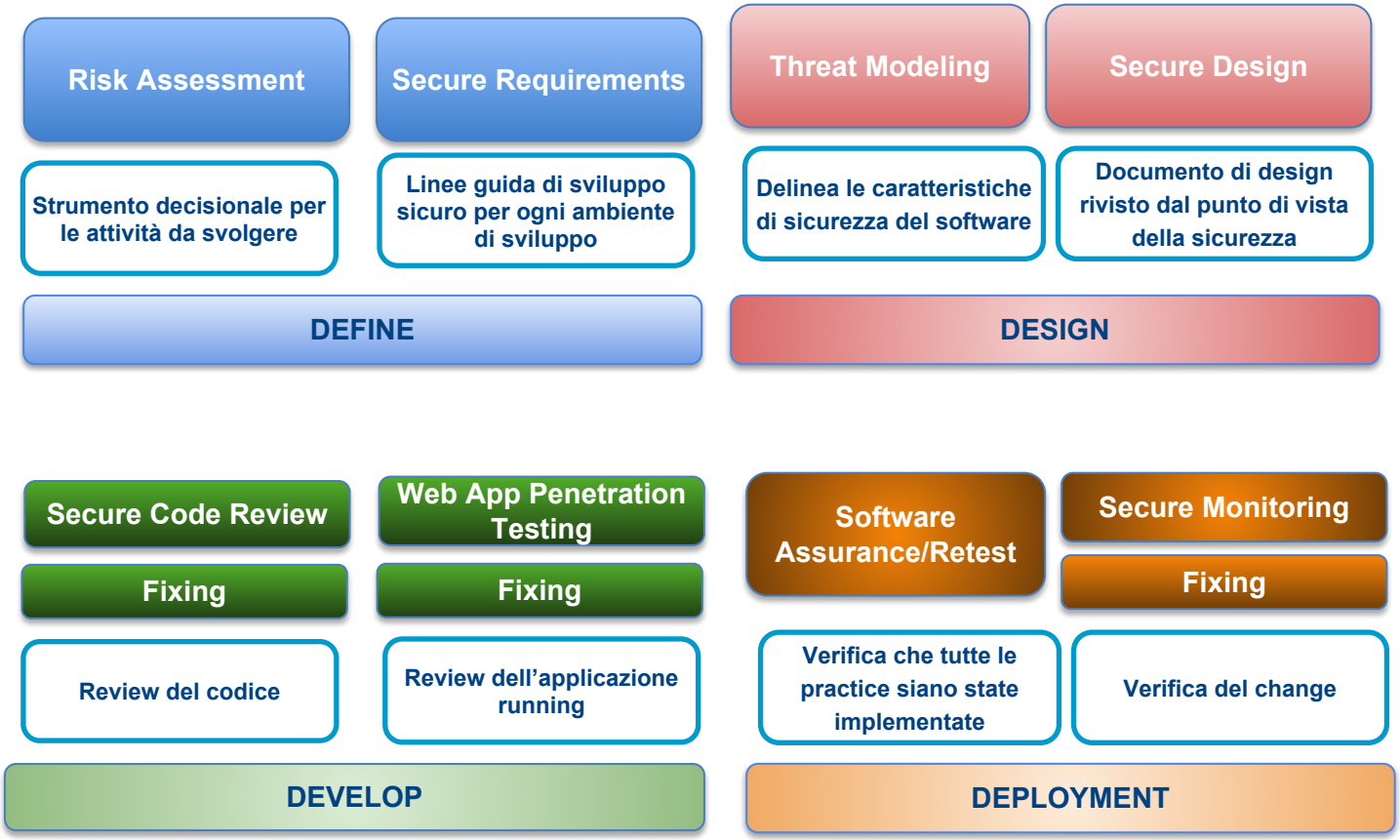
Sw Sec AWARENESS

- Management, Application Owners, Analysts, Auditors, Architects, Developers, Engineers

Sw Sec STANDARDS

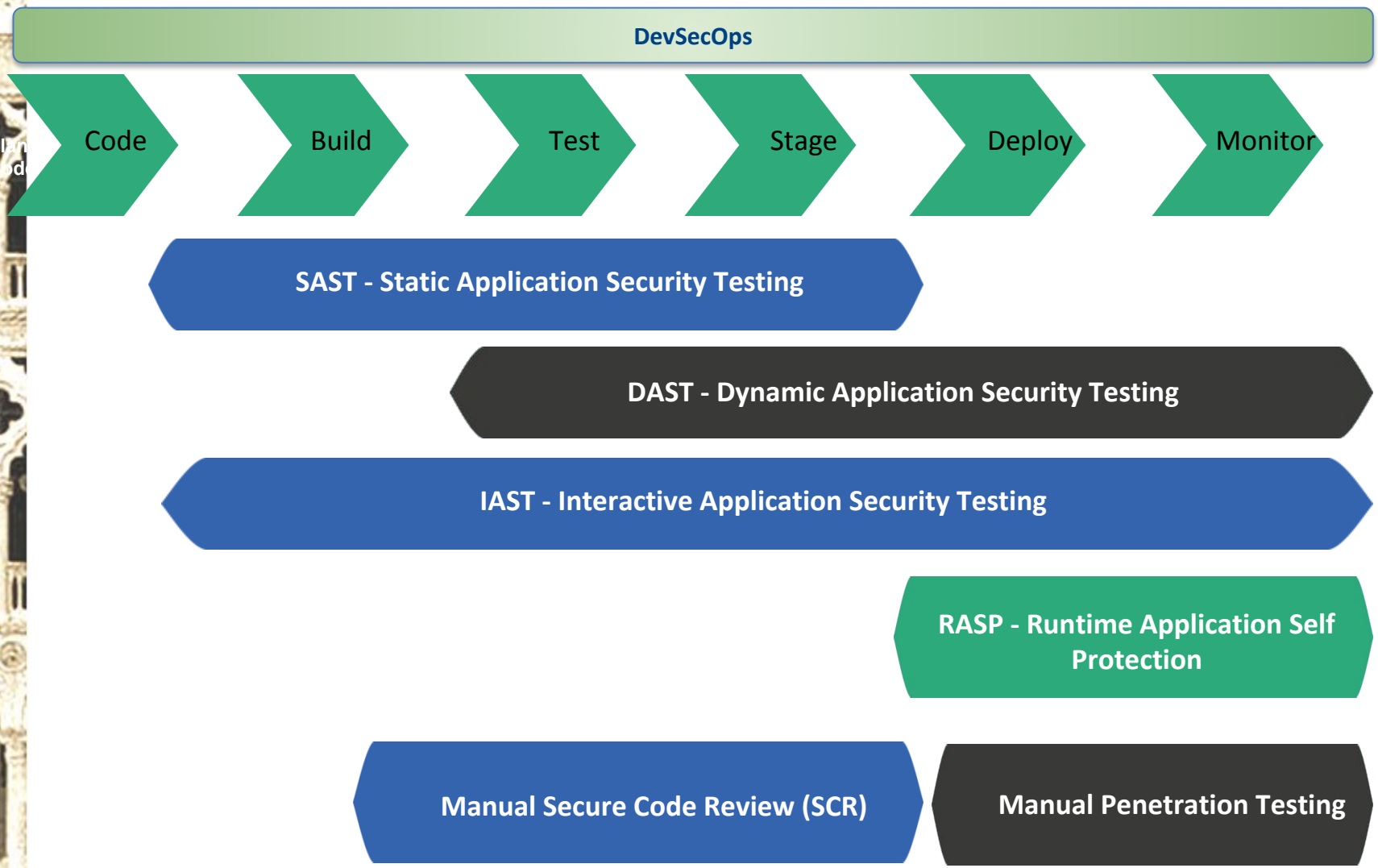
- Sw Security Roadmap (SAMM) - Risk analysis - Threat Modeling - Sec Architecture - Sec Coding - Software Assurance

(1) SwSec 5D - Process dimension

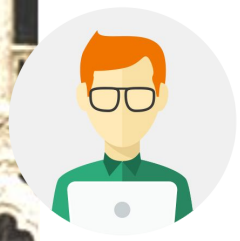


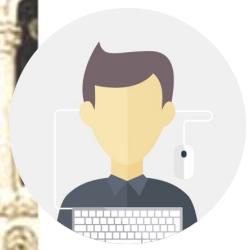
Source: Minded Security

(2) SwSec5D - Testing dimension



(3) SwSec5D - Team dimension





AppSec manager/CISO

Security Champions

AppSec Specialists

Satellite Architects

Satellite Developers

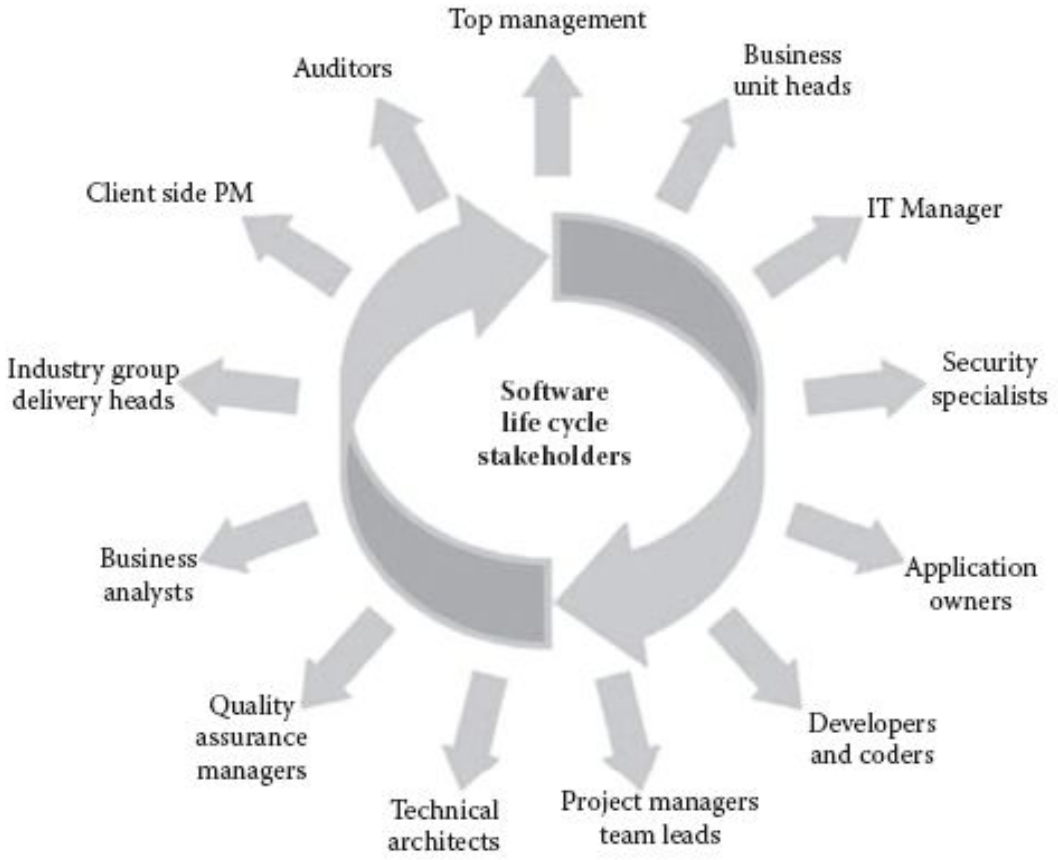
Satellite Testers

A fast fixing process is the key to have a mature SwSec Program:

- Satellite architects: should fix flaws asap
- Satellite developers: should fix bugs asap
- Satellite tester: should test if the remediations are strong enough asap.

A strong satellite is the key of a mature software security initiative.

(4) SwSec 5D - Awareness dimension



Source: Official (ISC)2 Guide to CSSLP (2012)

(5) SwSec - Standards dimension

Sw Security Roadmap (SAMM)

Risk analysis

Secure Software Requirements

Threat modeling use cases

Secure Architecture

Secure Coding Guidelines

Software Assurance

4. Apply the models to a real case

SDLC phase 1

The first implementations of a Secure SDLC started in 2007. The fist results appears as the following:

1) basic training
2) generic secure coding guidelines
3) buy a tool
4) test at the end

Basic trainings: 8hs webinar on xss, sqli, major attacks

what about building specific secure software?

what about management? analysts, auditors? Architects?

Basic guidelines:

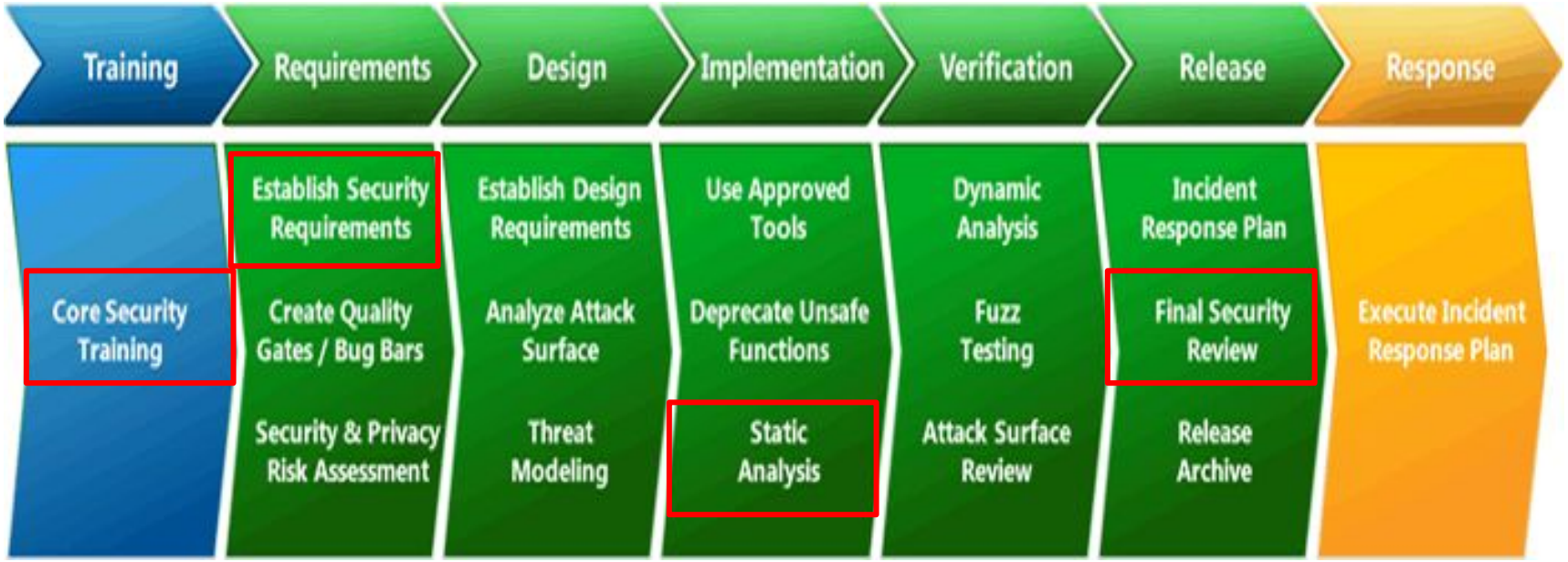
what about how to implement

secure authentication in J2EE?

SECURE CODING GUIDELINES

...
develop secure software following the OWASP Top 10
...

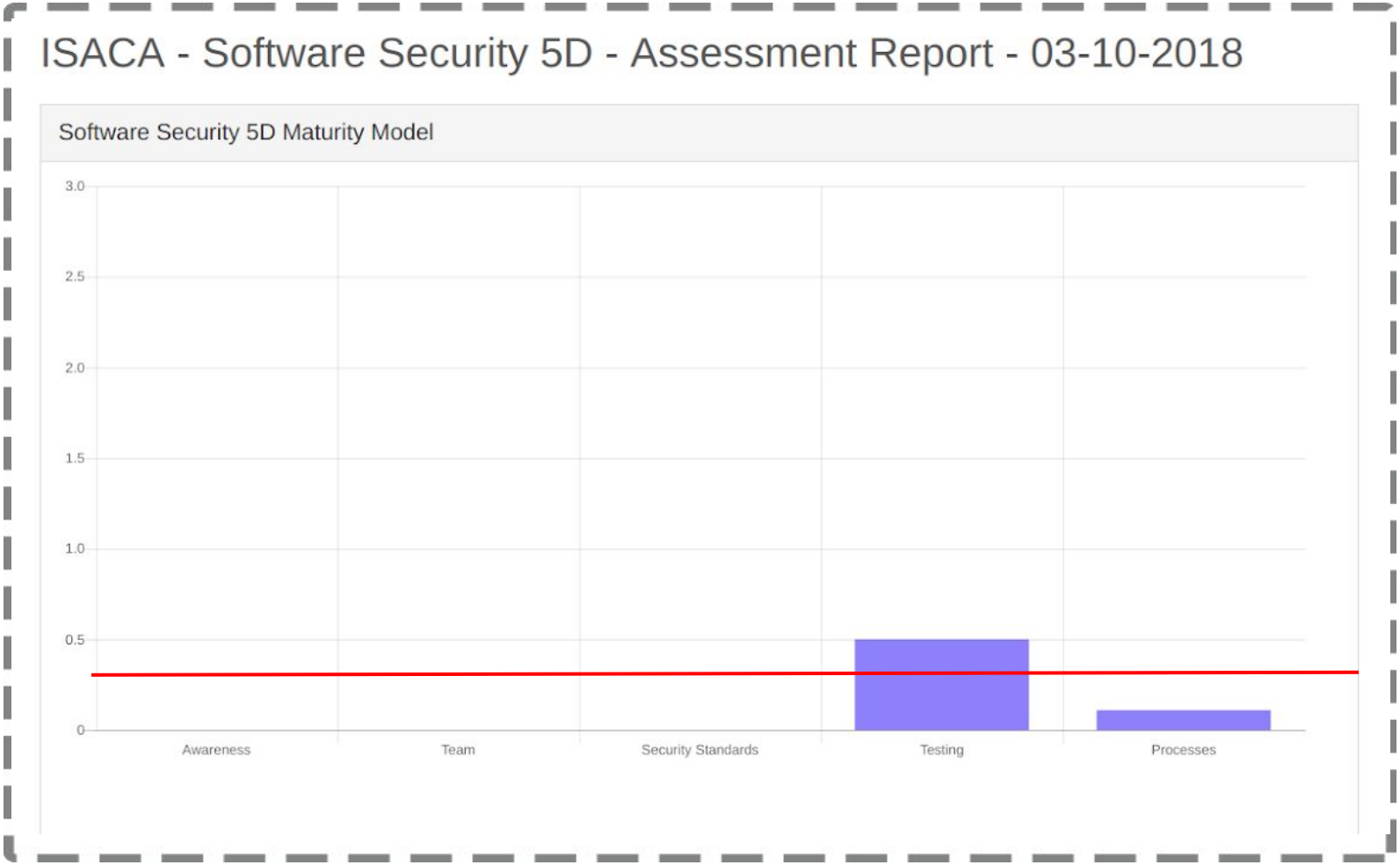
SDLC phase 1: MS SLD



SDLC phase 1: OWASP SAMM

Business Functions	Security Practices	Maturity Level
Governance	Strategy & Metrics	0
	Policy & Compliance	0
	Education & Guidance	0,3
Construction	Threat Assessment	0
	Security Requirements	0.3
	Secure Architecture	0
Verification	Design Review	0
	Code Review	0
	Security Testing	0,6
Deployment	Vulnerability Management	0
	Environment Hardening	0
	Operational Enablement	0

SDLC phase 1: OWASP SwSec 5D



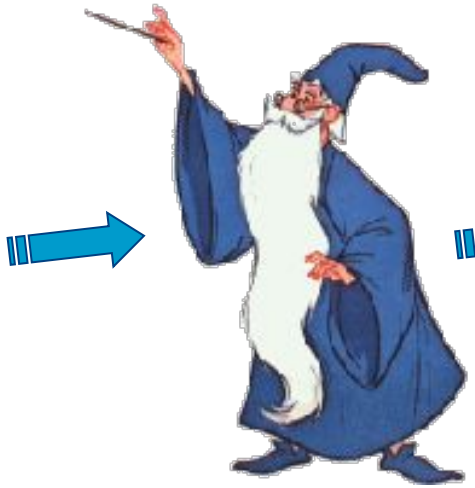
5. Some wrong approaches

1) buy a tool and your software will be secure!

```
public void findUser()
{

boolean showResult = false;
String username =
this.request.getParameter("
username");
this.context.put("username
", username);
this.context.put("showResult",
showResult);

}
```



```
public void findUser()
{

boolean showResult = false;
String username =
this.request.getParameter("
username");
ESAPI.encoder().encodeFor
HTMLAttribute(username));
this.context.put("username
", username);
this.context.put("showResult",
showResult);

}
```

Software | **Security tool in action** | **Secure Software**

1) buy a tool and your software will be secure!

```
public void findUser()
{

boolean showResult = false;
String username =
this.request.getParameter("
username");
this.context.put("username
", username);
this.context.put("showResult",
showResult);

}
```

Software

Security tool in action

```
public void findUser()
{

boolean showResult = false;
String username =
this.request.getParameter("
username");
ESAPI.encoder().encodeFor
HTMLAttribute(username));
this.context.put("username
", username);
this.context.put("showResult",
showResult);

}
```

Secure Software

1) buy a tool and your software will be secure!

```
public void findUser()
{

boolean showResult = false;
String username =
this.request.getParameter("
username");
this.context.put("username
", username);
this.context.put("showResult",
showResult);

}
```

200 High risk vulns

500 Medium risk vulns

650 low risk vulns

Software | **Security tool in action** | **Report**

The model lacks of strategy, skill sets to configure the tools, skill sets to manage the results

2) SECURE SDLC phase 0: Test at the end

A gate to control **at the end** of the development?

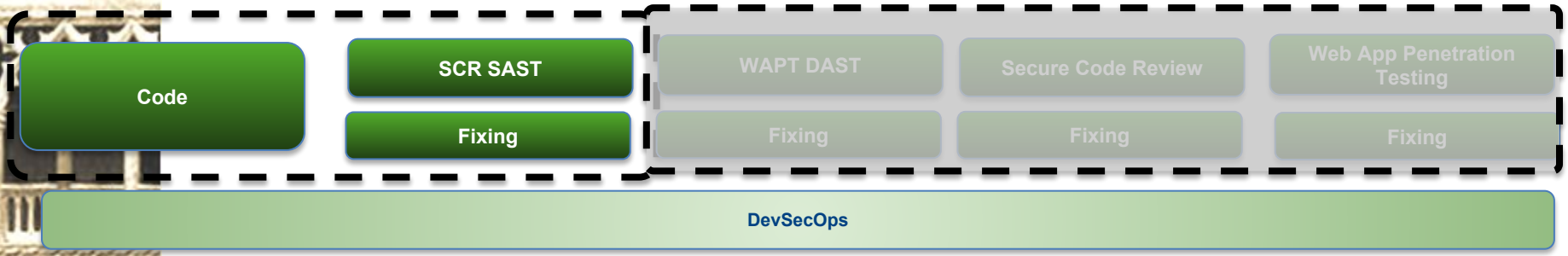
2) SECURE SDLC phase 0: Test at the end

A gate to control **at the end** of the development?

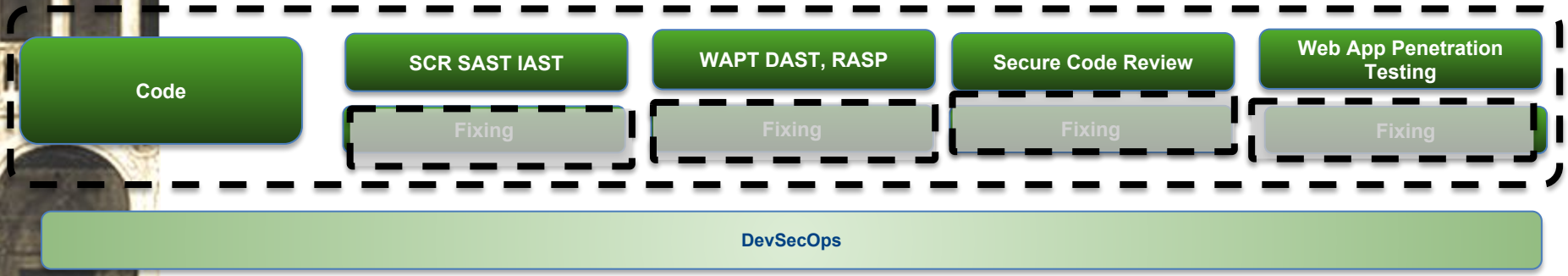
Software is ready and it is coming to the gate...

3) Use the right tools for DevOps

(1) In DevOps only SAST but used by a developer on a set of applications.



(2) In DevOps SAST, DAST, IAST, RASP, manual SCR and WAPT are adopted but more than 1y to fix



SwSec 5D: When it fails

SwSec PROCESSES

- Risk Assessment - Security Requirements
- Threat Modeling - Security Design
- SCR, WAPT
- Software Acceptance - Security bug Fixing

Sw Sec TESTING

- SAST, DAST, IAST, RASP
- External manual SCR, WAPT

Sw Sec TEAM

- AppSec manager/CISO, Sec Champions, AppSec Specialists, Satellite Architects, Sat Developers, Sat Testers

Sw Sec AWARENESS

- Management, Application Owners, Analysts, Auditors, Architects, Developers, Engineers

Sw Sec STANDARDS

- Sw Security Roadmap (SAMM) - Risk analysis - Threat Modeling - Sec Architecture - Sec Coding - Software Assurance

6. Conclusions

Conclusions

- Building a Secure Software Roadmap for SDL is a journey
- The journey is different for each company.
- SDLC frameworks like MS SDL helps to see what MS is doing
- OWASP SAMM helps to manage all the aspects of the path of the roadmap
- OWASP SwSec 5D helps to understand that not only processes and tools are the focus of Companies roadmap.

Companies need to see the maturity growing in 5 Dimensions

OWASP Day: 19th October Cagliari

OWASP
Italy Day - Cagliari
19 October 2018

WELCOME

Introduction

Welcome to the OWASP Italy Day 2018, Cagliari Edition Conference. Following on from the great successes of last OWASP Days, the new conference will take place next **19th October 2018 at the University of Cagliari**. Address: Auditorium of the Faculty of Engineering and Architecture, Piazza d'Armi, Cagliari.

Agenda | Abstracts | Registration | Organization and goals | Sponsors | Call For Papers

The Conference will be in ITALIAN language.

The schedule will be as follow:

10:00h	**"Welcome and opening of the works"** Prof. Giorgio Giacinto, Ing. Davide Ariu - Università di Cagliari, Matteo Meucci OWASP Italy
10.15h	**"Web Application & Cloud Services: What are the new threats? "** David Calligaris, Director of Vulnerability Research & Security Testing Automation Huawei Technologies GMBH
10:45h	**"API Security (or insecurity)"** Marco Pacchiardo
11:15h	**"Let me introduce you the Owasp Mobile App Security Testing: How to test your mobile applications against security vulnerabilities."** Giuseppe Porcu, Minded Security
11.45h	**Coffee Break**
12.10h	**"Are you focusing on the root causes? A Unified Framework for Web Security"** Dr. Igino Corona,Computer Security Researcher, Co-Founder & Security CTO at Pluribus One
12:40h	**"How we turned spaghetti (code) into mHackeroni"** Marco Festa, POLIMI
13:10h	**Light lunch**

{ Thanks!

MATTEO.MEUCCI@owasp.org

https://twitter.com/matteo_meucci

www.OWASP.org