Come valutare la maturità del proprio modello di sviluppo del software

Matteo Meucci

OWASP-Italy Chair

OWASP Day per la PA
Roma
9, Novembre 2010

MEF
Ministero dell'Economia e delle Finanze

The OWASP Foundation
http://www.owasp.org

Agenda

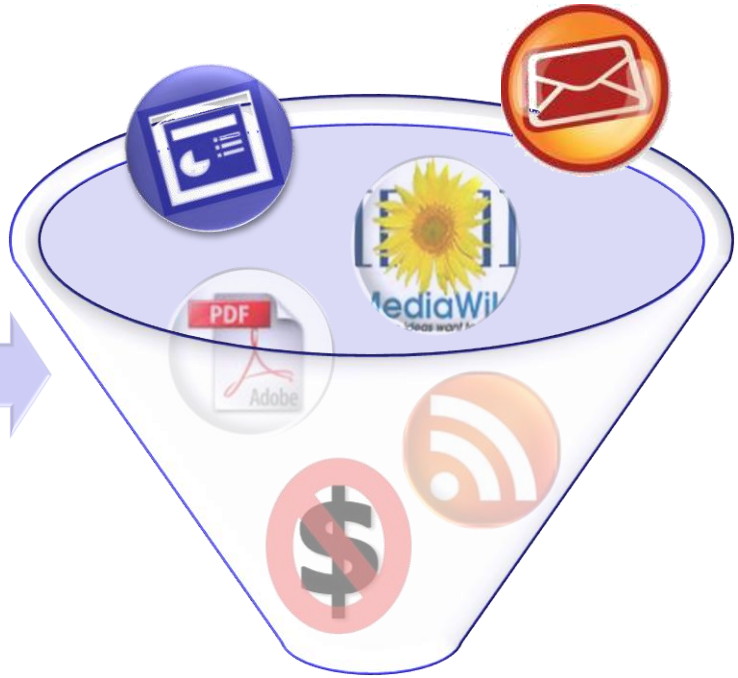
- OWASP news!
- I modelli Open Source per valutare la maturità del ciclo di vita di sviluppo del software
- Quali sono le criticità nel mondo delle Pubbliche amministrazioni

Who am I?

- Research
  - OWASP-Italy Chair
  - OWASP Testing Guide Lead
  - OWASP Vulnerability List Lead
  - OWASP SAMM Contributor
- Work
  - CEO @ Minded Security
    Application Security Consulting
  - 9+ years on Information Security
    focusing on Application Security

OWASP News

OWASP è un gruppo di professionisti

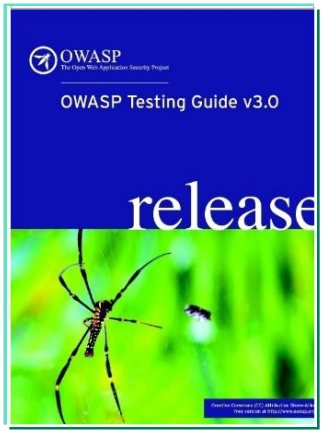


- 6,381 Articoli
- 427 presentazioni
- 200 aggiornamenti/giorno
- 271 mailing lists
- 180 blog monitorati
- Progetti:
  - alfa
  - beta
  - release

Linee Guida OWASP

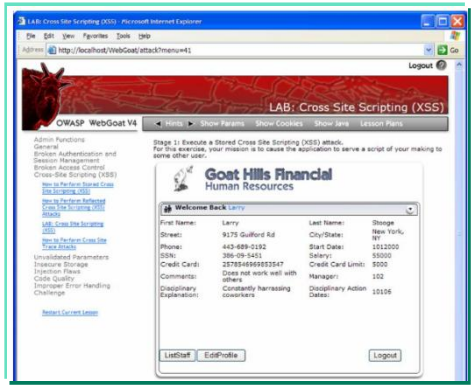
- Gratuite e open source
- Libri a basso costo
- Centinaia di esperti coinvolti
- Coprono tutti gli aspetti di sicurezza applicativa

Principali progetti OWASP



BOOKS

- Owasp top10
- OWASP ASVS
- Building guide
- Code review guide
- Testing guide



TOOLS

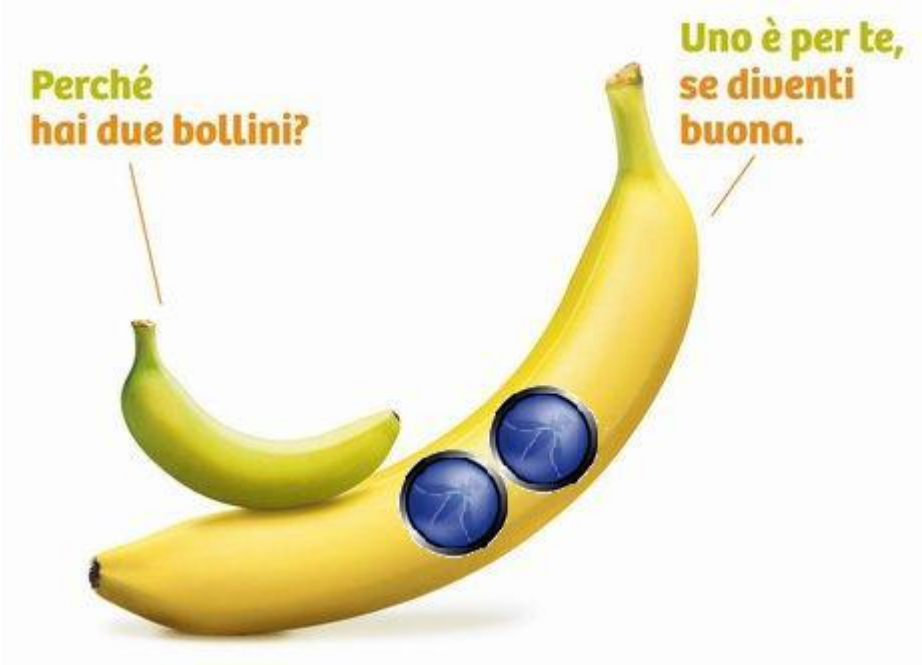
- WebGoat,WebScarab
- ESAPI
- SQLMap – SQL Ninja
- SWF Intruder
- O2
- Orizon
- Code Crawler

Cosa NON è OWASP:

comuni fraintendimenti su OWASP

OWASP collaborator != Superman

OWASP != Bollini !=certificazioni



La certificazione OWASP non esiste


OWASP
The Open Web Application Security Project
OWASP Top 10 - 2010
The Ten Most Critical Web Application Security Risks
Versione in Italiano
release

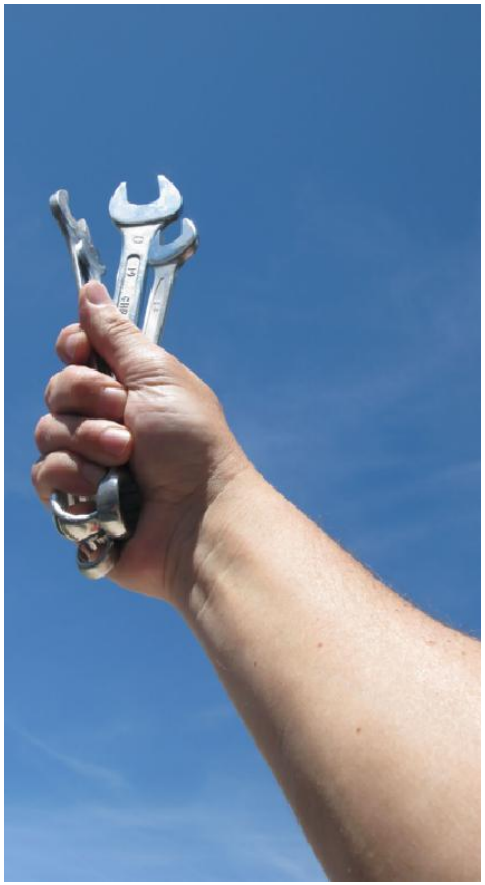
!=


OWASP
OWASP Testing Guide v3.0
release

sponsor OWASP != sviluppare applicazioni sicure!

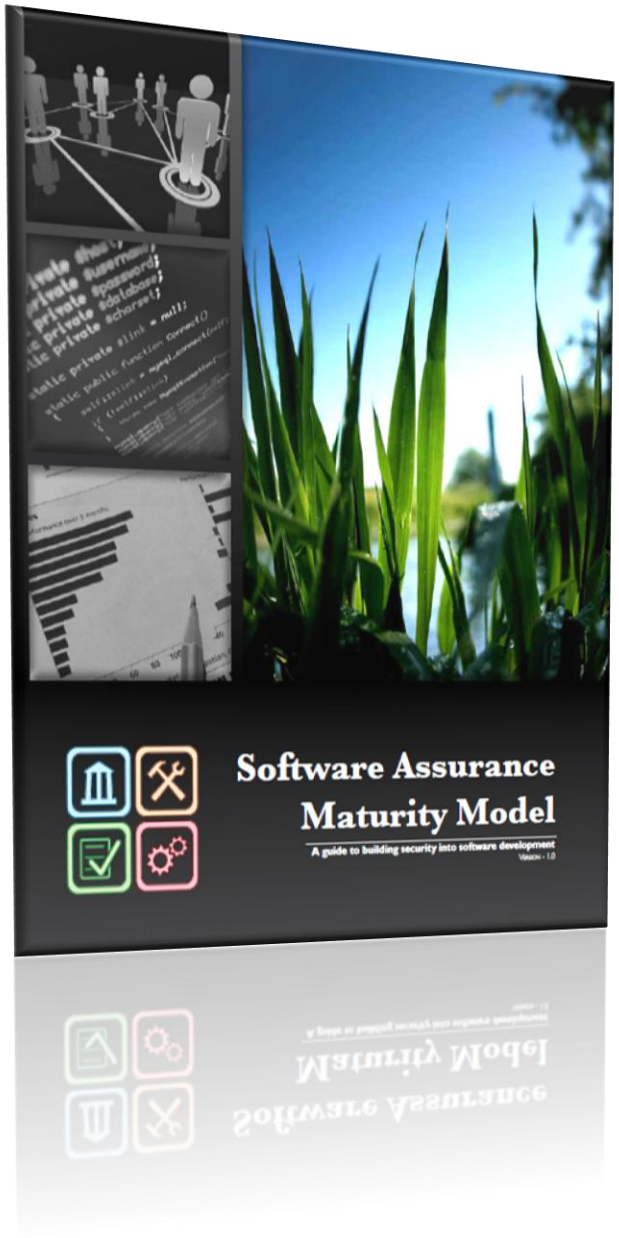

```
public class HelloWorld extends HttpServlet {

    public void doGet(
        HttpServletRequest request,
        HttpServletResponse response)
            throws IOException,
    ServletException
    {
        response.setContentType("text/html");
        PrintWriter out = response.getWriter();
        out.println("<HTML><HEAD>");
        out.println("<TITLE>Hello
    World</TITLE>");
        out.println("</HEAD><BODY>");
        out.println("Hello, " + }
```




acunetix
Adobe
amazon
ASPECT SECURITY
ASTECH
DENIM GROUP
DIGITAL DEFENSE
DREAMLAB
fishnet SECURITY
FORTIFY
GOTHAM
gemalto
IMPERVA
Information Builders
(ISC)
iSEC PARTNERS
Microsoft
Firefox
NOKIA
omega point
ORACLE
PortWise
PROACTIVERISK
protiviti
Qualys
salesforce.com
securestate
SOGETI
symantec.
TENABLE
Trustwave
VERACODE
WhiteHat

Software Assurance Maturity Model: OWASP SAMM


Software Assurance
Maturity Model
A guide to building security into software development

OWASP SAMM è il primo maturity model?

eSourcing Capability Model for Client Organizations (eSCM-CL)

eSourcing Capability Model (eSCM)

Data Management Maturity Model (DMMM)

Capability Maturity Model Integration (CMMI)

Building Security In Maturity Model (BSIMM)

Service Integration Maturity Model (SIMM)

Organizational Project Management Maturity Model: (OPM3)

Information Security Management Maturity Model (ISM3)

E-Learning Maturity Model (eMM)

Progressive HR Business Integrated Model (ProBIM)

Systems Security Engineering Capability Maturity Model (SSE-CMM)

Open Source Maturity Model (OSMM)

Self-Assessment Maturity Model (SAMM)

Usability Maturity Model (UMM)

Enterprise Data Management Maturity Model Integration (EDMMI)

Web Site Maturity Model

PRINCE2 Maturity Model (P2MM)

IT Service Capability Maturity Model (IT Service CMM)

Capability Maturity Model (CMM)

Software Reliability Engineering Maturity Model

Testing Maturity Model (TMM)

Software Acquisition Capability Maturity Model (SA-CMM)

People Capability Maturity Model (PCMM)

Portfolio, Programme and Project Management Maturity Model (P3M3)

eSourcing Capability Model for Service Providers (eSCM-SP)

Outsourcing Management Maturity Model

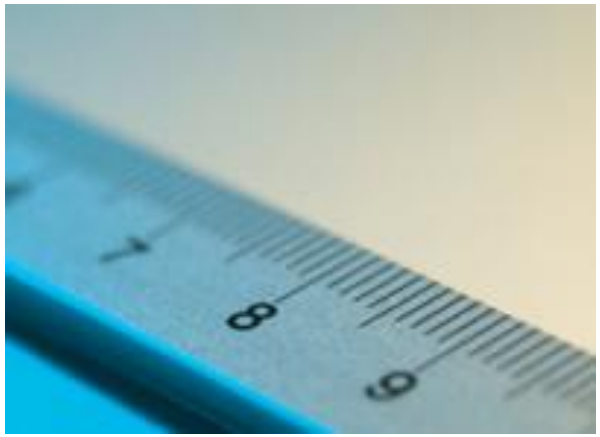
eGovernment Maturity Model (eGMM)

OWASP SAMM e BSIMM

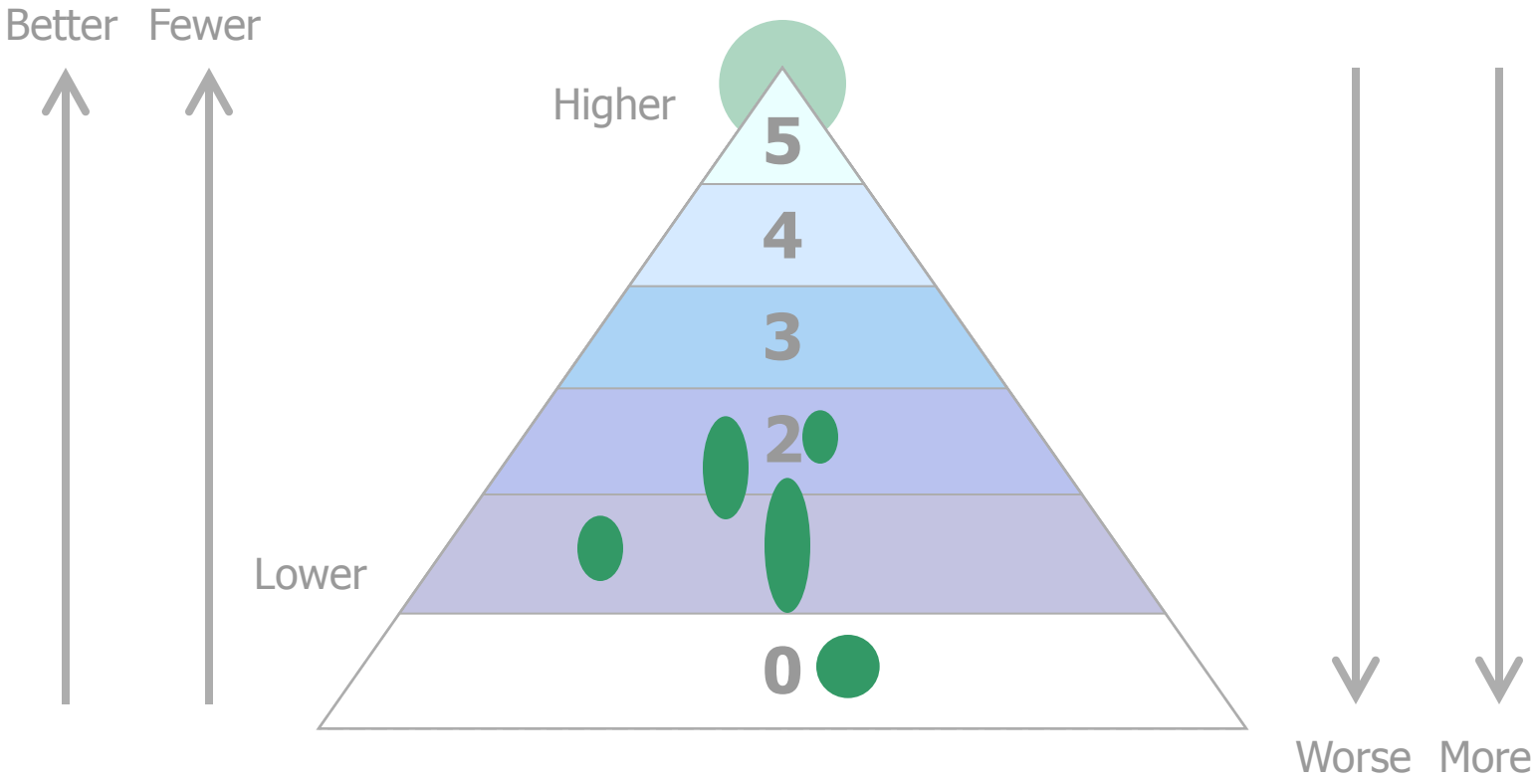
- BSIMM: Lo scopo del BSIMM è quello di documentare le attività comuni a tutte le più importanti attività di software security. Modello descrittivo: a posteriori il modello riflette una fetta crescente di realtà.

- OWASP SAMM: I modelli precedenti sono buoni per gli esperti da utilizzare come una guida, ma difficile per le aziende da utilizzare per migliorare i propri obiettivi. Modello prescrittivo: mostra un percorso comune da seguire.

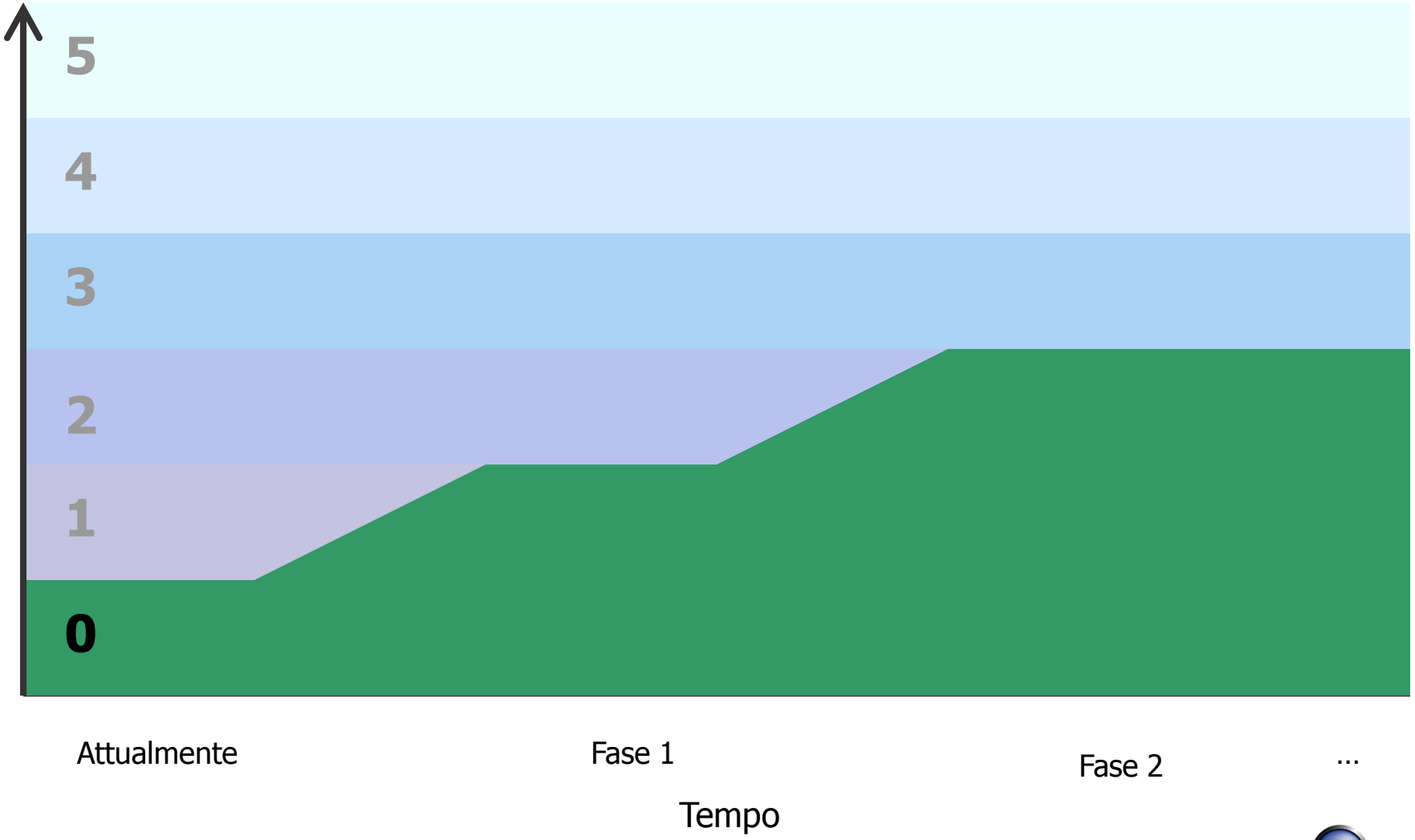
OWASP SAMM: obiettivi



Proprietà di un generico modello di maturità



Un generico processo nel corso del tempo



OWASP SAMM: il modello

SAMM: 4 Funzioni di business critiche

Governance

Software development management activities and organisation-wide business processes

Construction

Goal definition and software creation processes

Verification

Checking, evaluation and testing of software development artifacts

Deployment

Software release management and normal operational management

- Si inizia con le 4 attività di base legate ad ogni azienda che sviluppa o acquista software
- Nomi generici delle funzioni ma dovrebbero essere compresi dagli sviluppatori e manager

Ciascuna area ha 3 Security Practices

Governance	Construction	Verification	Deployment
			
Security & Metrics	Threat Assessment	Design Review	Vulnerability Management
Policy & Compliance	Security Requirements	Code Review	Environment Hardening
Education & Guidance	Secure Architecture	Security Testing	Operational Enablement

Per ogni security practice

- Sono definiti 3 obiettivi per ogni practice che definiscono come questa può essere migliorata nel tempo
  - Ciò stabilisce una nozione del livello al quale un'organizzazione adempie ad una data Practice

- I 3 livelli per una practice in generale corrispondono a:
  - (0: Inizio implicito con la Practice non completata)
  - 1: Inziale comprensione e la disposizione ad hoc della Practice
  - 2: Aumentare l'efficienza e / o l'efficacia della pratica
  - 3: Padronanza completa della pratica

Ad esempio: BF Governance, SP Education

Governance

Security & Metrics

Policy & Compliance

Education & Guidance

Obiettivi

Attività

EG1	EG2	EG3
Offrire allo staff di sviluppo l'accesso alle risorse di sviluppo sicuro	Educare tutto il personale nel SDLC in base al proprio ruolo nello sviluppo sicuro	Training sulla sicurezza mandatori e completi. Personale certificato
A. Condurre Training tecnici su Security Awareness B. Costruire e mantenere linee guida tecniche	A. Condurre training specifici in base al ruolo B. Utilizzare i trainer per migliorare i team di progetto	A. Creare un supporto formale per la application security B. Stabilire esami in base ai ruoli aziendali

Per ogni Security Practice SAMM definisce 3 livelli di maturità

- Obiettivi
- Attività
- Risultati
- Metriche
- Costi
- Personale coinvolto

Activities

A. Conduct technical security awareness training

Either internally or externally sourced, conduct security training for technical staff that covers the basic tenets of application security. Generally, this can be accomplished via instructor-led training in 1-2 days or via computer-based training with modules taking about the same amount of time per developer.

Course content should cover both conceptual and technical information. Appropriate topics include high-level best practices surrounding input validation, output encoding, error handling, logging, authentication, authorization. Additional coverage of commonplace software vulnerabilities is also desirable such as a Top 10 list appropriate to the software being developed (web applications, embedded devices, client-server applications, back-end transaction systems, etc.). Wherever possible, use code samples and lab exercises in the specific programming language(s) that applies.

To rollout such training, it is recommended to mandate annual security training and then hold courses (either instructor-led or computer-based) as often as required based on development head-count.

B. Build and maintain technical guidelines

For development staff, assemble a list of approved documents, web pages, and technical notes that provide technology-specific security advice. These references can be assembled from many publicly available resources on the Internet. In cases where very specialized or proprietary technologies permeate the development environment, utilize senior, security-savvy staff to build security notes over time to create such a knowledge base in an ad hoc fashion.

Ensure management is aware of the resources and briefs oncoming staff about their expected usage. Try to keep the guidelines lightweight and up-to-date to avoid clutter and irrelevance. Once a comfort-level has been established, they can be used as a qualitative checklist to ensure that the guidelines have been read, understood, and followed in the development process.

Results

- Increased developer awareness on the most common problems at the code level
- Maintain software with rudimentary security best-practices in place
- Set baseline for security know-how among technical staff
- Enable qualitative security checks for baseline security knowledge

Success Metrics

- >50% development staff briefed on security issues within past 1 year
- >75% senior development/ architect staff briefed on security issues within past 1 year
- Launch technical guidance within 3 months of first training

Costs

- Training course buildout or license
- Ongoing maintenance of technical guidance

Personnel

- Developers (1-2 days/yr)
- Architects (1-2 days/yr)

Livello 3

Activities

A. Create formal application security support portal

Building upon written resources on topics relevant to application security, create and advertise a centralized repository (usually an internal web site). The guidelines themselves can be created in any way that makes sense for the organization, but an approval board and straightforward change control processes must be established.

Beyond static content in the form of best-practices lists, tool-specific guides, FAQs, and other articles, the support portal should feature interactive components such as mailing lists, web-based forums, or wikis to allow internal resources to cross-communicate security relevant topics and have the information cataloged for future reference.

The content should be cataloged and easily searchable based upon several common factors such as platform, programming language, pertinence to specific third party libraries or frameworks, life-cycle stage, etc. Project teams creating software should align themselves early in product development to the specific guidelines that they will follow. In product assessments, the list of applicable guidelines and product-related discussions should be used as audit criteria.

B. Establish role-based examination/certification

Either per role or per training class/module, create and administer aptitude exams that test people for comprehension and utilization of security knowledge. Typically, exams should be created based on the role-based curricula and target a minimum passing score around 75% correct. While staff should be required to take applicable training or refresher courses annually, certification exams should be required biannually at a minimum.

Based upon pass/fail criteria or exceptional performance, staff should be ranked into tiers such that other security-related activities could require individuals of a particular certification level to sign-off before the activity is complete, e.g. an uncertified developer cannot pass a design into implementation without explicit approval from a certified architect. This provides granular visibility on an per-project basis for tracking security decisions with individual accountability. Overall, this provides a foundation for rewarding or penalizing staff for making good business decisions regarding application security.

Results

- Efficient remediation of vulnerabilities in both ongoing and legacy code bases
- Quickly understand and mitigate against new attacks and threats
- Judge security-savvy of staff and measure against a common standard
- Establish fair incentives toward security awareness

Add'l Success Metrics

- >80% staff certified within past 1 year

Add'l Costs

- Certification examination build-out or license
- Ongoing maintenance and change control for application security support portal
- Human-resources and overhead cost for implementing employee certification

Add'l Personnel

- Developers (1 day/yr)
- Architects (1 day/yr)
- Managers (1 day/yr)
- Business Owners (1 day/yr)
- QA Testers (1 day/yr)
- Security Auditors (1 day/yr)

Applicare il modello

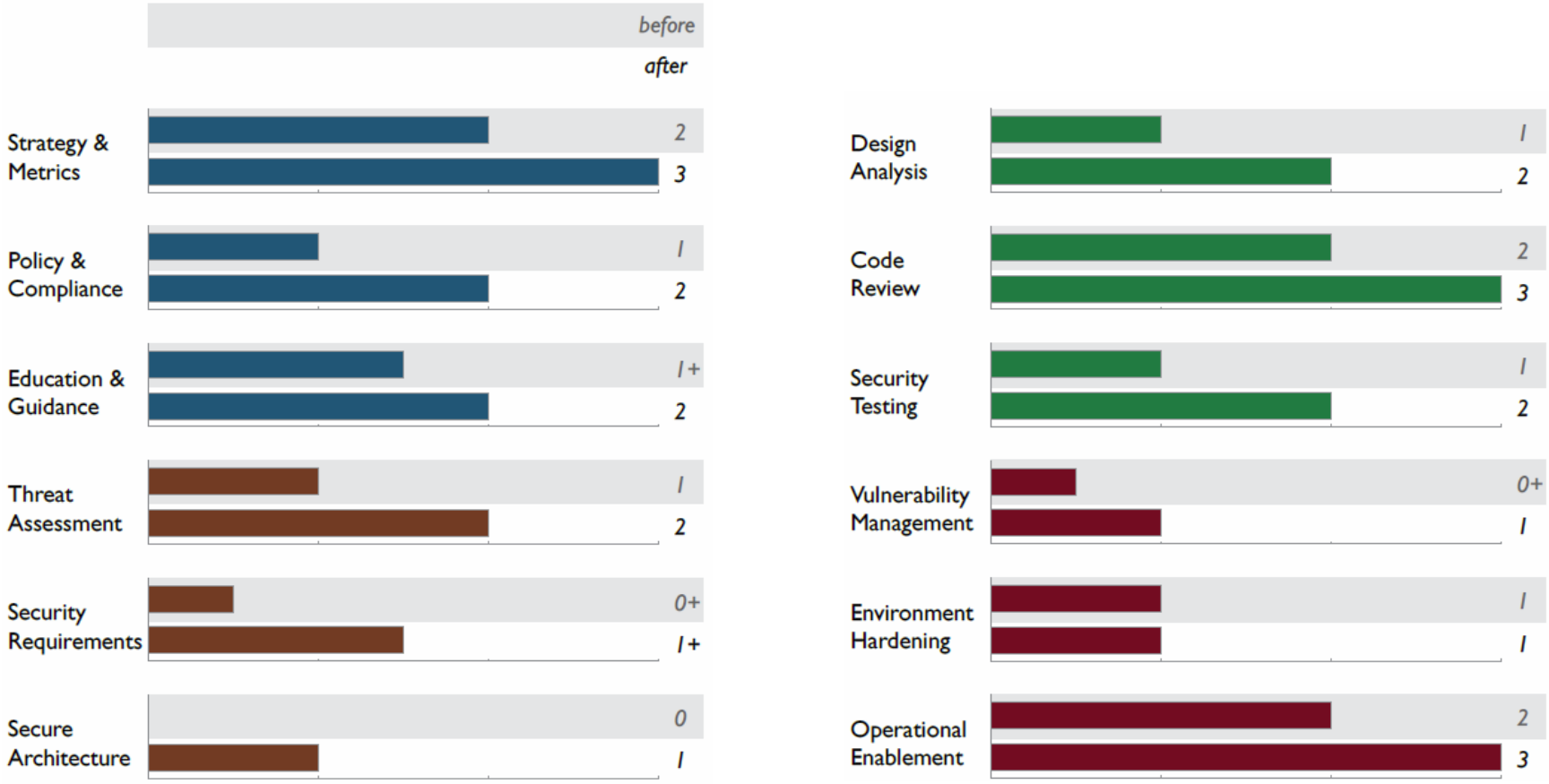
Procedura di assessment

- Condurre un assessment
- Creare uno score card
- Costruire un programma di assurance
  - Metriche
  - Road map
- Implementare gli obiettivi e condurre nuovamente un assessment

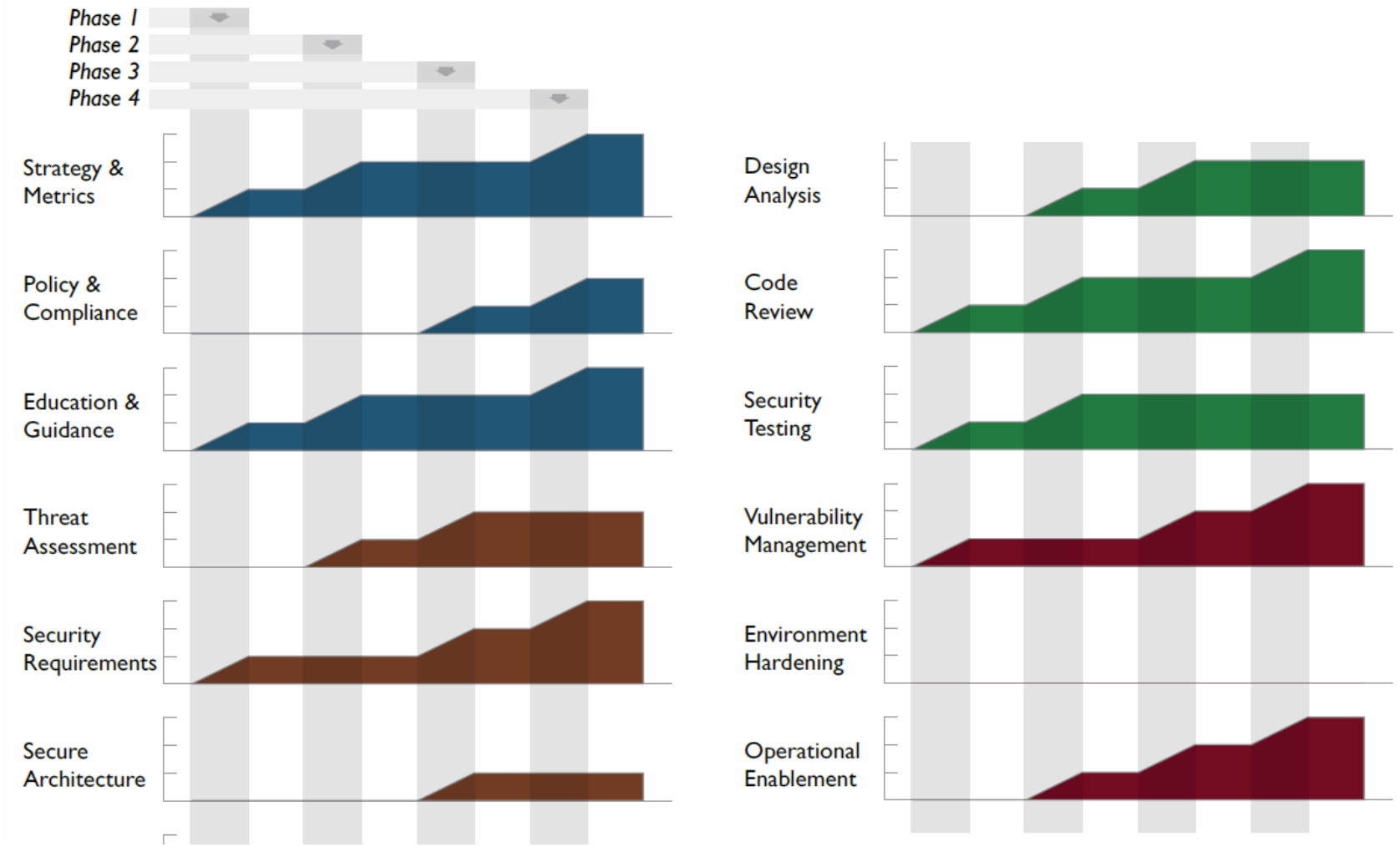
Assessment

Education & Guidance	Yes/No
✦ Have most developers been given high-level security awareness training?	
✦ Does each project team have access to secure development best practices and guidance?	
✦ Are most roles in the development process given role-specific training and guidance?	
✦ Are most stakeholders able to pull in security coaches for use on projects?	
✦ Is security-related guidance centrally controlled and consistently distributed throughout the organization?	
✦ Are most people tested to ensure a baseline skill-set for secure development practices?	

Scorecards


before
after
Strategy & Metrics
2
3
Policy & Compliance
1
2
Education & Guidance
1+
2
Threat Assessment
1
2
Security Requirements
0+
1+
Secure Architecture
0
1
Design Analysis
1
2
Code Review
2
3
Security Testing
1
2
Vulnerability Management
0+
1
Environment Hardening
1
1
Operational Enablement
2
3

Roadmap


Phase 1
Phase 2
Phase 3
Phase 4
Strategy & Metrics
Policy & Compliance
Education & Guidance
Threat Assessment
Security Requirements
Secure Architecture
Design Analysis
Code Review
Security Testing
Vulnerability Management
Environment Hardening
Operational Enablement

Il modello di maturità per le PA

Criticità nel mondo PA

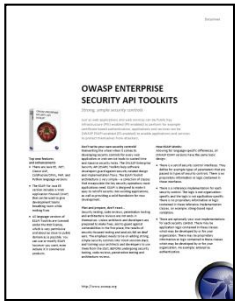
- Outsourcing dello sviluppo: fiducia cieca nel sw acquistato
  - Verifica di sicurezza solo dell'applicazione running (WAPT), non Design e Code Review
  - Open Source != sicuro
  - Aggiunta di componenti da terze parti senza fare review (js, banner)
- Outsourcing dell'infrastruttura: fiducia cieca nella gestione
  - non ci sono contratti di gestione delle problematiche di sicurezza, degli incidenti e delle modalità di deploy.

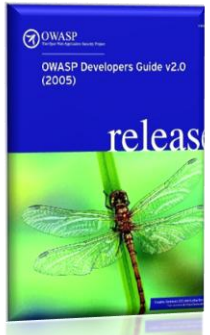
Le aree SAMM da migliorare

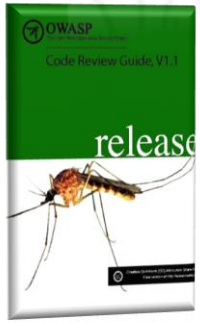
Governance	Construction	Verification	Deployment
			
Security & Metrics	Threat Assessment	Design Review	Vulnerability Management
Policy & Compliance	Security Requirements	Code Review	Environment Hardening
Education & Guidance	Secure Architecture	Security Testing	Operational Enablement

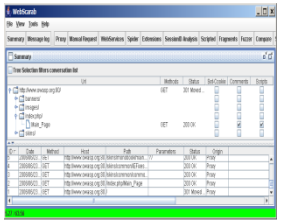
Linee guida e tool OWASP nel modello SAMM

Governance	Construction	Verification	Deployment









Conclusione

- Come affrontare il tema della **Web application security** nelle PA:
  - Implementare un **programma definito di Software Assurance** con linee guida standard, percorsi di formazione, processi di security integrati del ciclo di vita di sviluppo del software
- Prossimi obiettivi:
  - Creare una community per la sicurezza delle PA con l'obiettivo di redigere linee guida comuni e condivise

Grazie!

Domande?

Thanks to Pravir Chandra, Colin Watson and OWASP SAMM team

http://www.owasp.org/index.php/Italy

matteo.meucci@owasp.org