MINDED SECURITY
The Software Security Company

Software Security War: your reports are dead

Matteo Meucci, CEO @ Minded Security

12nd March 2019 - Security Summit Milan

Agenda

(1) OWASP Software Security 5D Framework

1.1. The model

1.2 Assessment results

(2) Software Security Roadmap

2.1 Good practices

2.2 Big Companies Example

(3) Compliance & Software Security

3.1 PCI Software Security Framework

3.2 GDPR

(4) Your reports are dead

4.1 Is the report useful today?

4.2 Security bugs integrated in lifecycle

(5) Top Things to do

5.1 Threat Modeling

5.2 Secure Code Review

5.3 Vendors Requirements

5.4 Conclusions

Who am I?

Informatics Engineer (since 2001)

Research

- OWASP contributor (since 2002)
- OWASP-Italy Chair (since 2005)
- OWASP Testing Guide Lead (since 2006)
- OWASP Sw Security 5D Framework Lead (since 2018)

Work

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

(1) OWASP Software Security 5D Framework

1.1 The model

Why do we need another model?

How can we measure Software Security?

Good reports results? Number of tools?

- Measuring the number of vulnerabilities in your sw is the best way to get an idea of the maturity of secure software development?

- SCR and WAPT are some of the activities to do and if for example they are completely automated → you rely completely on the results of the scans.
  - Software A after scan: X bugs
  - Software B after scan: no bugs.

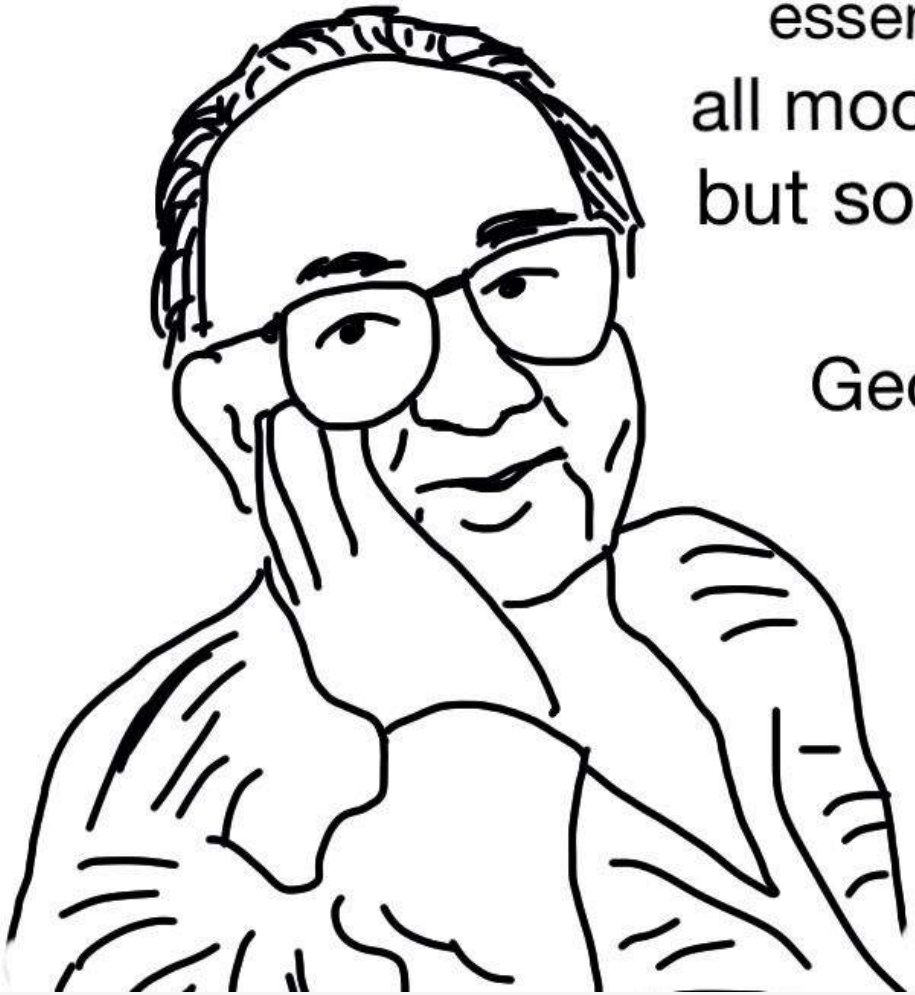
  Is the software secure?

Reports vs S-SDLC

OWASP SwSec 5D Framework and OWASP SAMM measure the level of maturity of the software life cycle. Penetration test is just one of the actions that need to be implemented in the life cycle.

Vulnerabilità	Rischio	Difficoltà di risoluzione	Priorità
SQL Injection	Critico	Media	Alta
Authorization Bypass	Critico	Media	Alta
Remote Code Execution	Critico	Media	Alta
Stored Cross-Site Scripting	Alto	Media	Alta
Reflected Cross-Site Scripting	Alto	Media	Alta
Chiave Crittografia in Codice Sorgente	Alto	Media	Alta
Segreti inseriti nel codice	Alto	Media	Alta
Dati sensibili nei log	Alto	Media	Alta
Arbitrary file upload	Alto	Media	Alta
Sensitive data in querystring	Alto	Media	Alta
Funzione di logout non implementata	Medio	Bassa	Alta
Insecure session cookie	Medio	Bassa	Alta
Mancanza di validazione dei certificati SSL	Medio	Bassa	Alta
Software Obsoleti e Vulnerabili	Medio	Media	Media
Insecure Jackson deserialization	Medio	Media	Media
Web Service di backend esposti senza autenticazione	Medio	Media	Media
Web Service di backend su canale non sicuro	Medio	Media	Media
Contromisure al CSRF incomplete	Medio	Media	Media
Insecure Hashing Algorithm	Medio	Media	Media

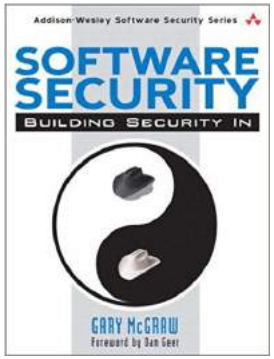
MINDED SECURITY
The Software Security Company

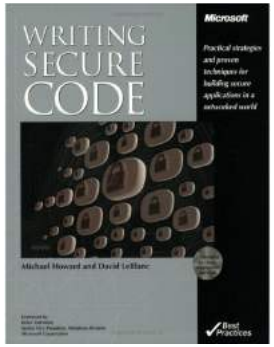


essentially,
all models are wrong,
but some are useful

George E. P. Box

Software Security: a brief history

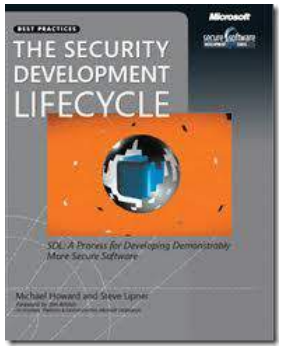




OWASP
Open Web Application Security Project
www.owasp.org

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

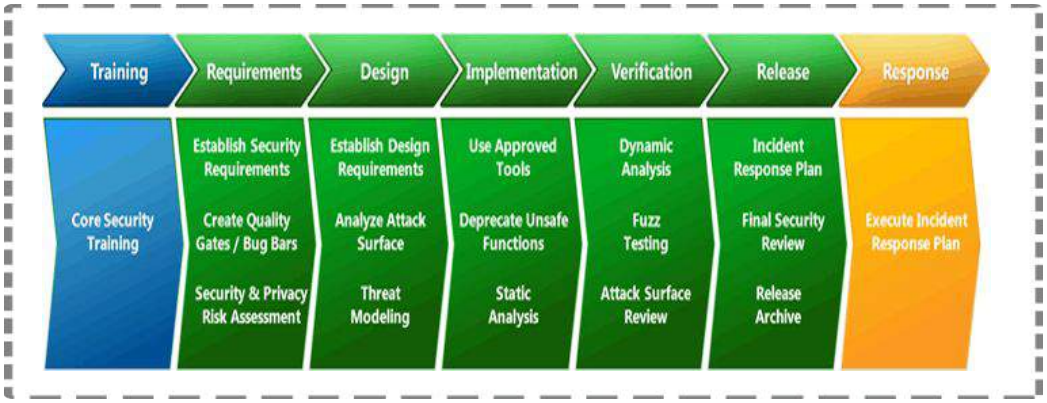
...new capabilities is the fact that it is designed from the ground up to deliver **Trustworthy Computing.**



2001 **2002** **2004** **2005** **2006**

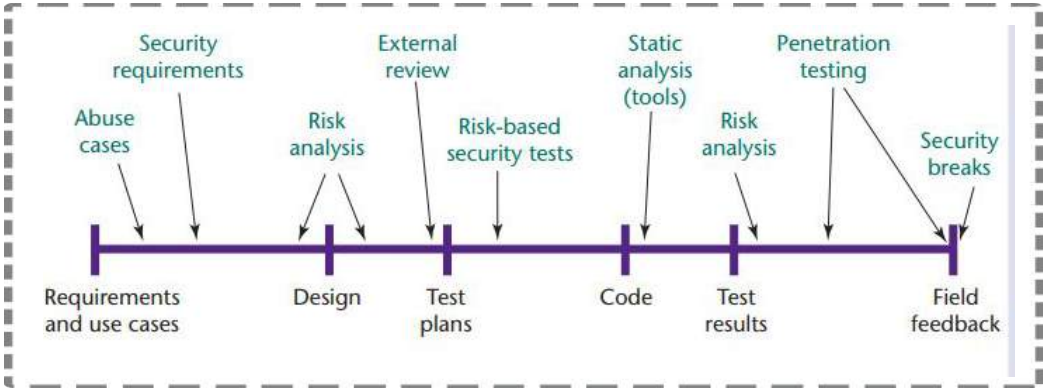
Traditional S-SDLC frameworks

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.

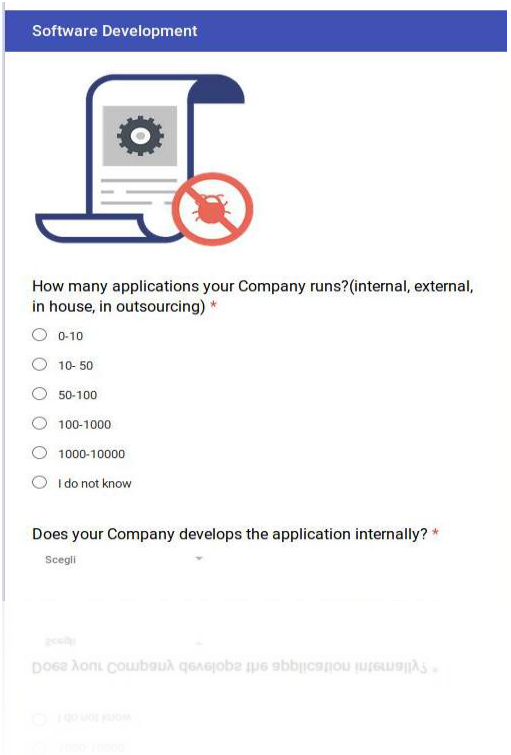


2006: Microsoft Security Development Lifecycle

2006: Building Security In



Software Security Assessment



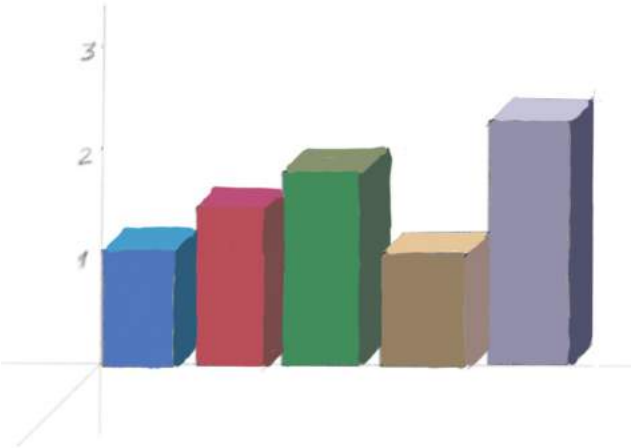
(1) OWASP Software Security 5 Dimension Framework (light assessment)

(2) OWASP Open SAMM is an OWASP Standard

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.

OWASP Software Security 5D framework

OWASP Sw Sec 5D

Sw Sec 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

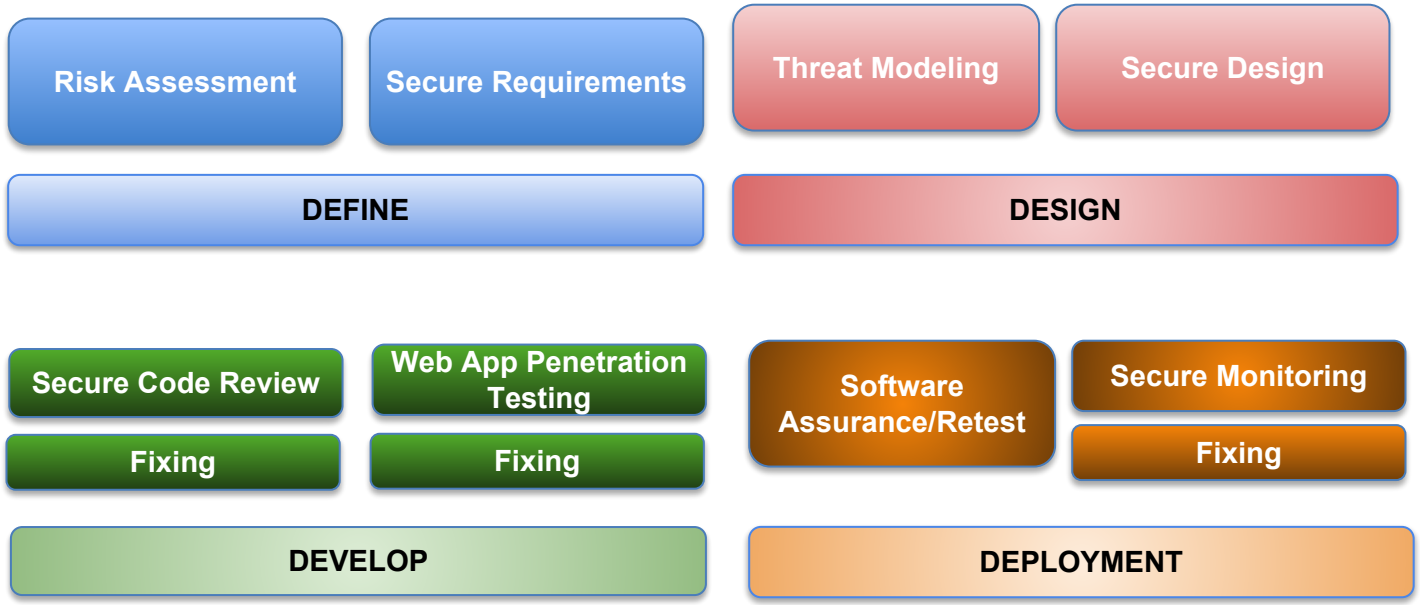
Sw Sec AWARENESS

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

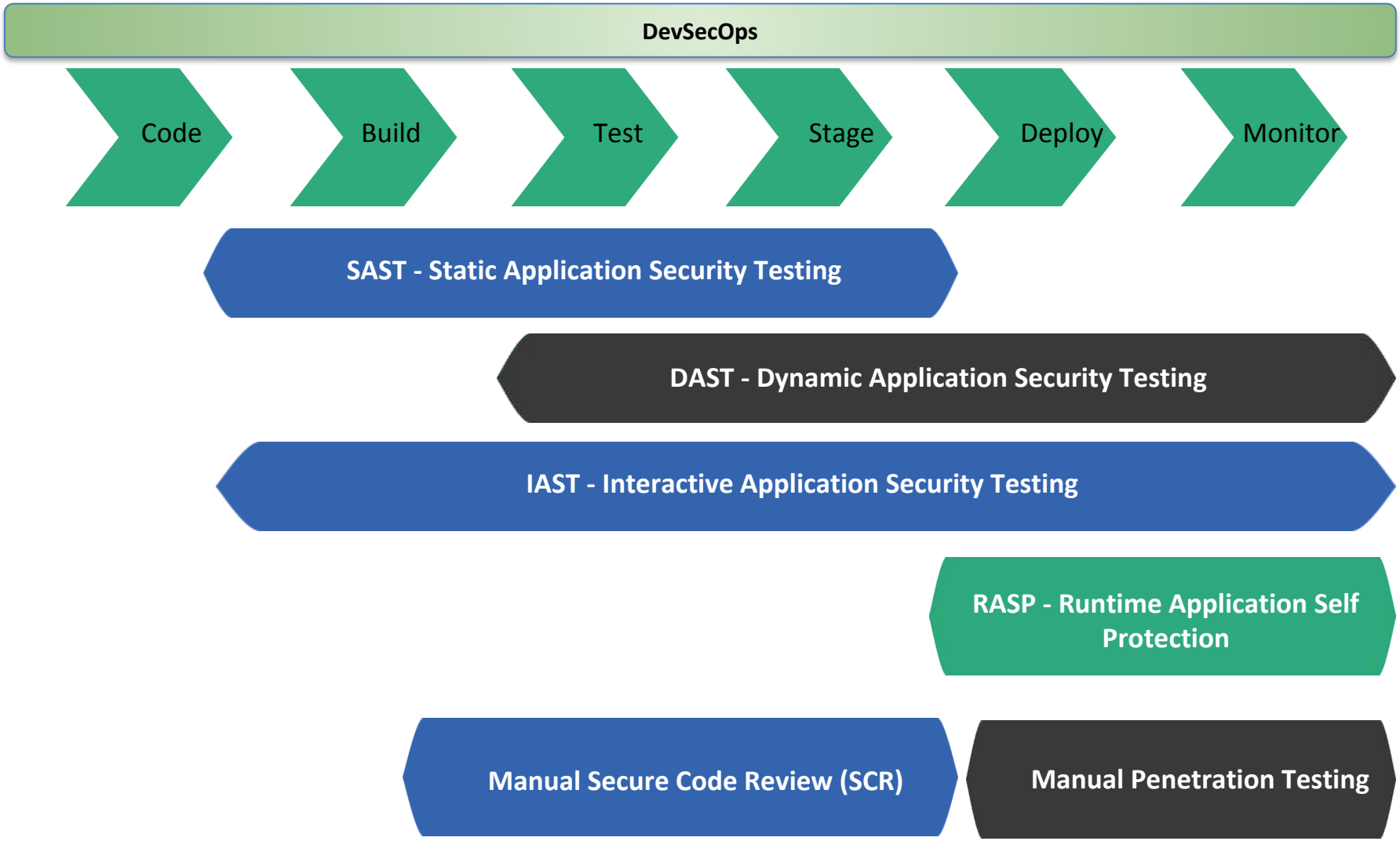
Sw Sec STANDARDS

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

(1) SwSec - Processes dimension



(2) SwSec - Testing dimension



(3) SwSec 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 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

SwSec 5D

SDLC phases	Software Security Processes	Software Security Standards	Software Security Testing	Team	Awareness
Define	Risk Assessment Secure Requirement	Sw Security Roadmap (SAMM) Risk analysis Secure Software Requirements		Management Security Champions	Management, IT Managers,App Owners
Design	Threat Modeling Secure Software Design	Threat modeling use cases Secure Architecture		Analysts Security Champions	Sec Specialists
Develop	Secure Code Review Web Application Testing Security Bug Fixing	Secure Coding Guidelines Outsourcing Governance (Software Assurance)	SAST DAST IAST SCR	DevOps Security Champions	Devs Sec Specialist
Deploy	Secure Software Testing & Acceptance Security Bug Fixing	Security Validation and Testing	RASP SCR/WAPT	DevOps Security Champions	Ops
Maintain	Secure Software Deployment & Maintenance Security Bug Fixing	Secure Deployment	RASP WAPT	Devops Security Champions	Sec Engineers

(1) OWASP Software Security 5D Framework

1.2 Assessment results

Financials and Independent Sw Vendor

SwSec 5D Survey

	FINANCIAL	ISV
AWARENESS	2,1	1
TEAM	1,7	1
STANDARDS	1,8	1,7
TESTING	2,5	1,6
PROCESSES	1,7	1,5

- **12 FINANCIAL institutions**
- **5 Independent Software Vendor**

SwSec 5D Survey results - top mature practices

Financial

Awareness

Management, Auditors, Developers, Engineers

Standards

Risk analysis, Secure Architecture

Testing

SAST, DAST, External manual SCR, WAPT

Team

AppSec Specialists, Satellite Architects

Processes

Risk Assessment, Security Requirements

SwSec 5D Survey results - top mature practices

Independent Software Vendor

Awareness

Architects, Developers, Engineers

Standards

Secure Coding - Software Assurance

Testing

External manual
SCR, WAPT

Team

Satellite Developers

Processes

Security Requirements
Security Design
Security bug Fixing

MINDED SECURITY
The Software Security Company

(2) Software Security Roadmap

2.1 Big Companies examples

What is doing Google?

Google codebase

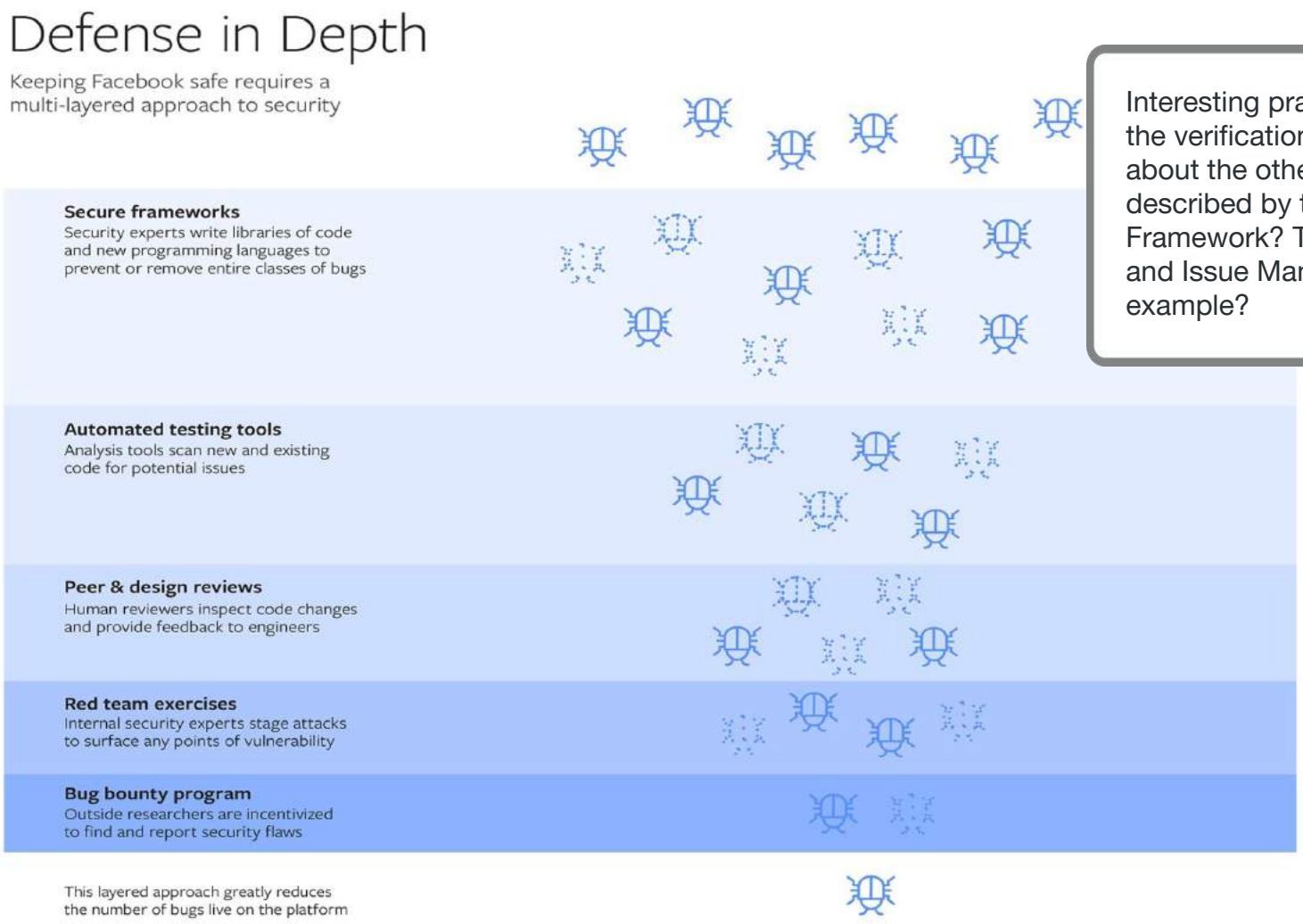
2.000.000.000+ Righe
86 TB, 9.000.000 files
dati del 2015

Google approach:

- Do not detect during developing (testing tools), prevent (use Secure API)
- Automate: humans do not scale

Source: Claudio Criscione - AIEA Venice 2018

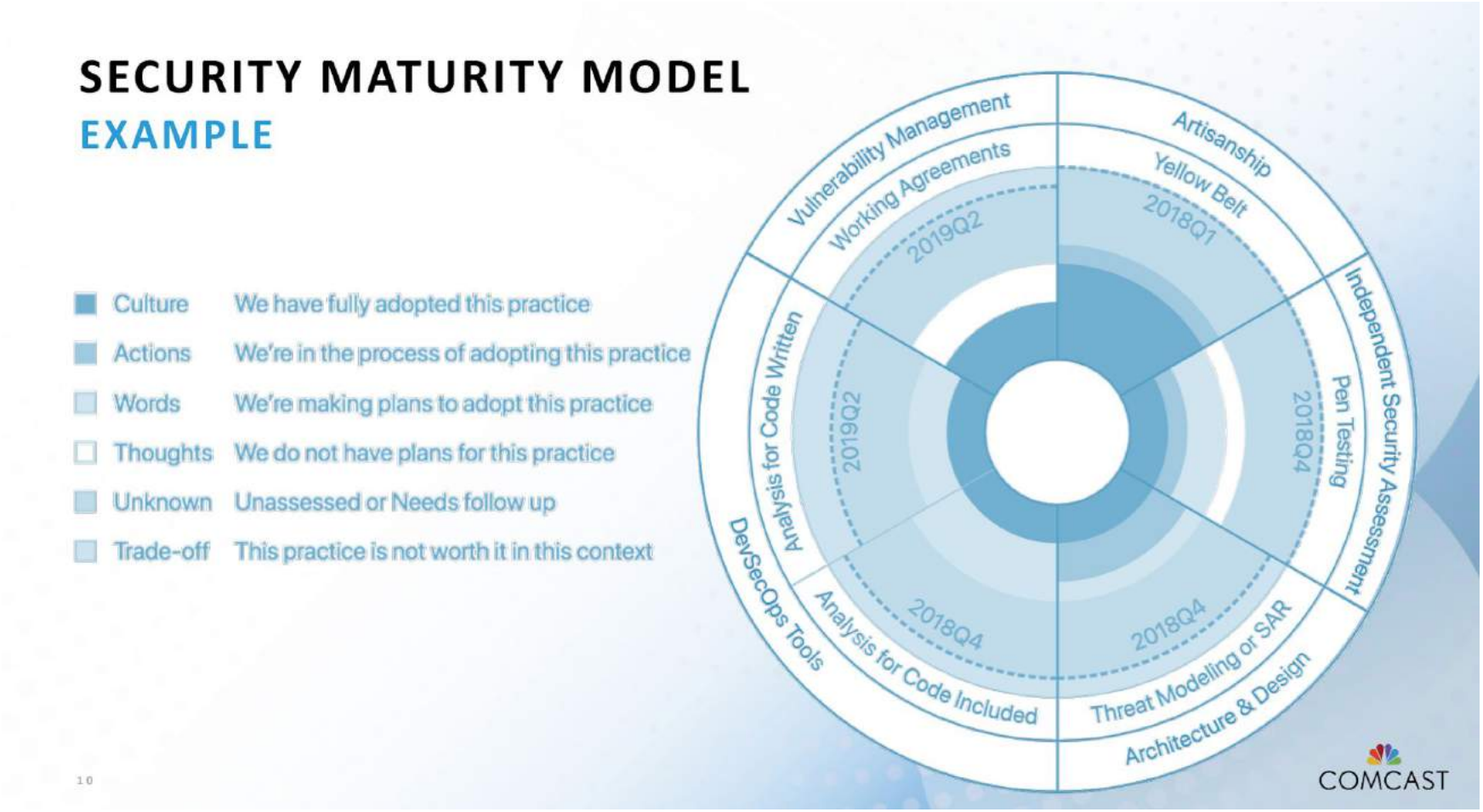
What is doing Facebook?



Interesting practical approach for the verification practices. What about the others security practices described by the OWASP 5D Framework? Threat Assessment and Issue Management for example?

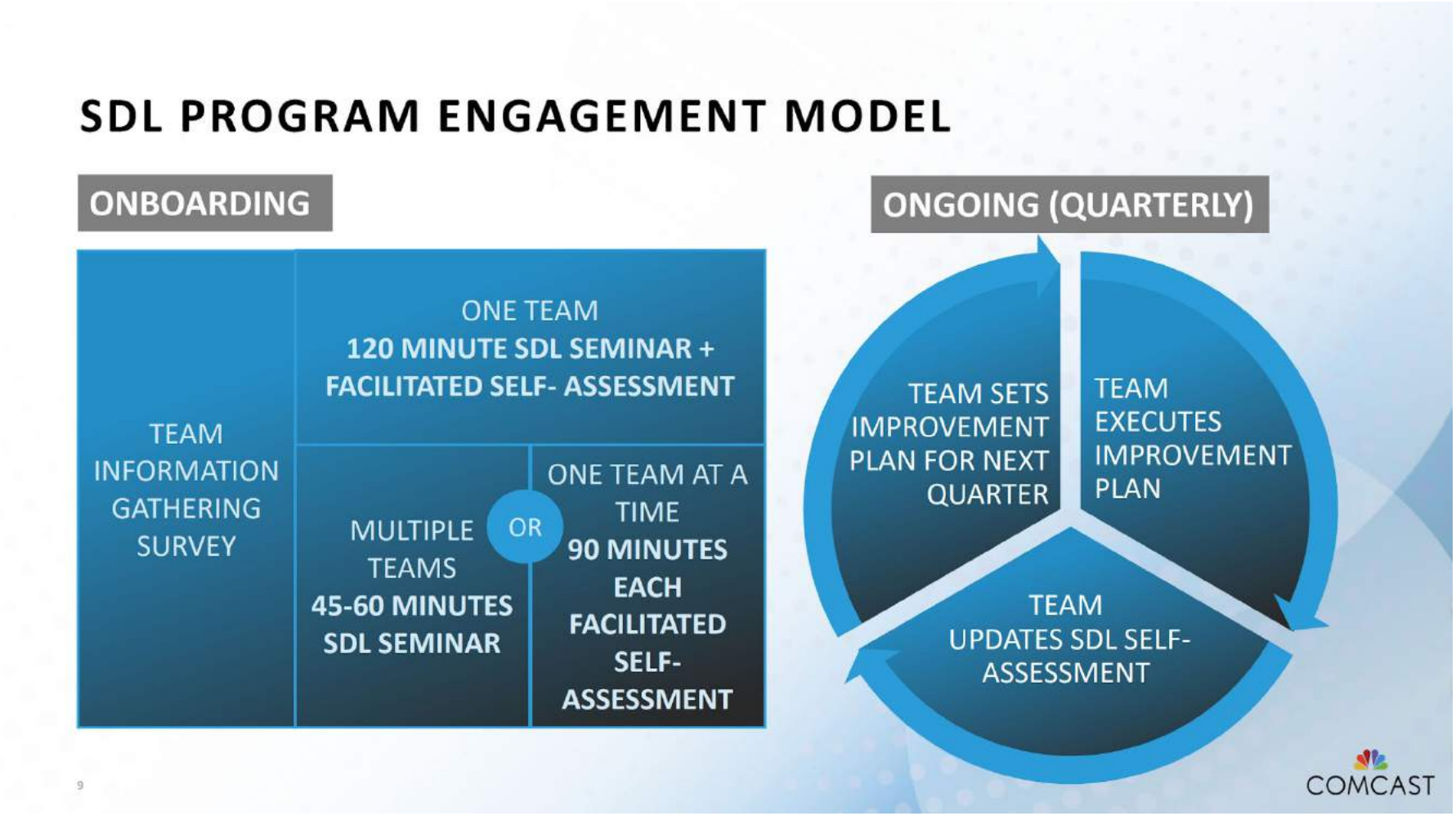
Source: https://newsroom.fb.com/news/2019/01/designing-security-for-billions/

Another example of Security Maturity Model



Source: Noopur Davis "Building Security In – DevSecOps" SVP, Chief Product and Information Security Officer, Comcast - RSAC 2019

Another example of Security Maturity Model



Source: Noopur Davis "Building Security In – DevSecOps" SVP, Chief Product and Information Security Officer, Comcast - RSAC 2019

(3) Compliance & Software Security

3.1 PCI Software Security Framework

PCI Secure Software Standards

Payment Card Industry
Software Security Framework

Secure Software Lifecycle (Secure SLC) Requirements and Assessment Procedures

Version 1.0

January 2019

Payment Card Industry
Software Security Framework

Secure Software Requirements and Assessment Procedures

Version 1.0

January 2019

PCI S-SLC (January 2019) vs SwSec 5D

Secure SLC Requirements
- Security Objective: Software Security Governance
  - Control Objective 1: Security Responsibility and Resources
  - Control Objective 2: Software Security Policy and Strategy
- Security Objective: Secure Software Engineering
  - Control Objective 3: Threat Identification and Mitigation
  - Control Objective 4: Vulnerability Detection and Mitigation
- Security Objective: Secure Software and Data Management
  - Control Objective 5: Change Management
  - Control Objective 6: Software Integrity Protection
  - Control Objective 7: Sensitive Data Protection
- Security Objective: Security Communications
  - Control Objective 8: Vendor Security Guidance
  - Control Objective 9: Stakeholder Communications
  - Control Objective 10: Software Update Information

Sw Sec 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

PCI S-SDL 1st Security Objective

1. Security Objective: Software Security Governance

Control Objective 1: Security Responsibility and Resources
Control Objective 2: Software Security Policy and Strategy

1. PROCESSES: Risk Assessment - Security Requirements
Threat Modeling - Security Design
SCR, WAPT
Software Acceptance - Security bug Fixing

2. TESTING: SAST, DAST, IAST, RASP
External manual SCR, WAPT

3. AWARENESS: Management, Application Owners, Analysts, Auditors, Architects, Developers, Engineers

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

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

PCI S-SDL 2nd Security Objective

2. Security Objective: Secure Software Engineering

Control Objective 3: Threat Identification and Mitigation
Control Objective 4: Vulnerability Detection and Mitigation

1. PROCESSES: Risk Assessment - Security Requirements
Threat Modeling - Security Design
SCR, WAPT
Software Acceptance - Security bug Fixing

2. TESTING: SAST, DAST, IAST, RASP
External manual SCR, WAPT

3. AWARENESS: Management, Application Owners, Analysts, Auditors, Architects, Developers, Engineers

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

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

PCI S-SDL 3rd Security Objective

3. Security Objective: Secure Software and Data Management

Control Objective 5: Change Management
Control Objective 6: Software Integrity Protection
Control Objective 7: Sensitive Data Protection

1. PROCESSES: Risk Assessment - Security Requirements
Threat Modeling - Security Design
SCR, WAPT
Software Acceptance - Security bug Fixing

2. TESTING: SAST, DAST, IAST, RASP
External manual SCR, WAPT

3. AWARENESS: Management, Application Owners, Analysts, Auditors, Architects, Developers, Engineers

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

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

PCI S-SDL 4th Security Objective

1. PROCESSES: Risk Assessment - Security Requirements
Threat Modeling - Security Design
SCR, WAPT
Software Acceptance - Security bug Fixing

2. TESTING: SAST, DAST, IAST, RASP
External manual SCR, WAPT

3. AWARENESS: Management, Application Owners, Analysts, Auditors, Architects, Developers, Engineers

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

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

4. Security Objective: Security Communications

Control Objective 8: Vendor Security Guidance
Control Objective 9: Stakeholder Communications
Control Objective 10: Software Update Information

(3) Compliance & Software Security

3.2 GDPR

GDPR

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

GDPR: impact on Sw Security

Article	Activities
Art. 4: Expansion of definition of "personal data"	The GDPR's definition of the "personal data" that must be protected is more detailed and broad than previous regulations. It can be anything from a **name, a photo, an email address, bank details, posts on social networking websites, medical information or a computer IP address.**
Art. 25: Security by Design	The GDPR includes a requirement to implement "data protection by design and by default." This requirement involves **creating applications from scratch with security and data protection in mind**. For applications, "security by design" incorporates activities like t**hreat modeling, secure design, training developers on secure coding** best practices, and ensuring that developers are not only coding securely, but also identifying and remediating security-related defects in their code **(fixing)**

GDPR: impact on Sw Security

Article	Activities
Art. 28: Third-party vendor security	Article 28 states that, in choosing a data processor(outside vendor), “the controller shall select a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.” **For application security, this means you can’t assume the security of third-party software**. You need “sufficient guarantees” that these externally sourced applications comply with the EU GDPR.
Art. 33: Notification of a personal data breach to the supervisory authority	Under the EU GDPR, breach notification will become mandatory in all member states where a data breach is likely to “result in a risk for the rights and freedoms of individuals.” This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers “without undue delay” after first becoming aware of a data breach.

SDLC and GDPR

Art. 4: Expansion of definition of "personal data"

Define	Design	Develop	Deploy	Maintain
Risk Assessment	Secure Design	Design Review	Software Acceptance	Web Intrusion Monitoring
Secure Requirements	Threat Modeling	Secure Development	Secure Installation	Change Management
Secure Architecture		SCR and WAPT	Hardening	
		Fixing		

SDLC and GDPR

Art. 25: Security by Design

Define	Design	Develop	Deploy	Maintain
Risk Assessment	Secure Design	Design Review	Software Acceptance	Web Intrusion Monitoring
Secure Requirements	Threat Modeling	Secure Development	Secure Installation	Change Management
Secure Architecture		SCR and WAPT	Hardening	
		Fixing		

SDLC and GDPR

Art. 28: Third-party vendor security

Define	Design	Develop	Deploy	Maintain
Risk Assessment	Secure Design	Design Review	Software Acceptance	Web Intrusion Monitoring
Secure Requirements	Threat Modeling	Secure Development	Secure Installation	Change Management
Secure Architecture		SCR and WAPT	Hardening	
		Fixing		

SDLC and GDPR

Art. 33: Notification of a personal data breach to the supervisory authority

Define	Design	Develop	Deploy	Maintain
Risk Assessment	Secure Design	Design Review	Software Acceptance	Web Intrusion Monitoring
Secure Requirements	Threat Modeling	Secure Development	Secure Installation	Change Management
Secure Architecture		SCR and WAPT	Hardening	
		Fixing		

(4) Your reports are dead

4.1 Is the report useful today?

MINDED SECURITY
The Software Security Company

Numbers of vulnerabilities

Level of Security

HIGH

Numbers of vulnerabilities	Level of Security
	**HIGH**
	**MEDIUM**

Numbers of vulnerabilities	Level of Security
	**HIGH**
	**MEDIUM**
	**LOW**

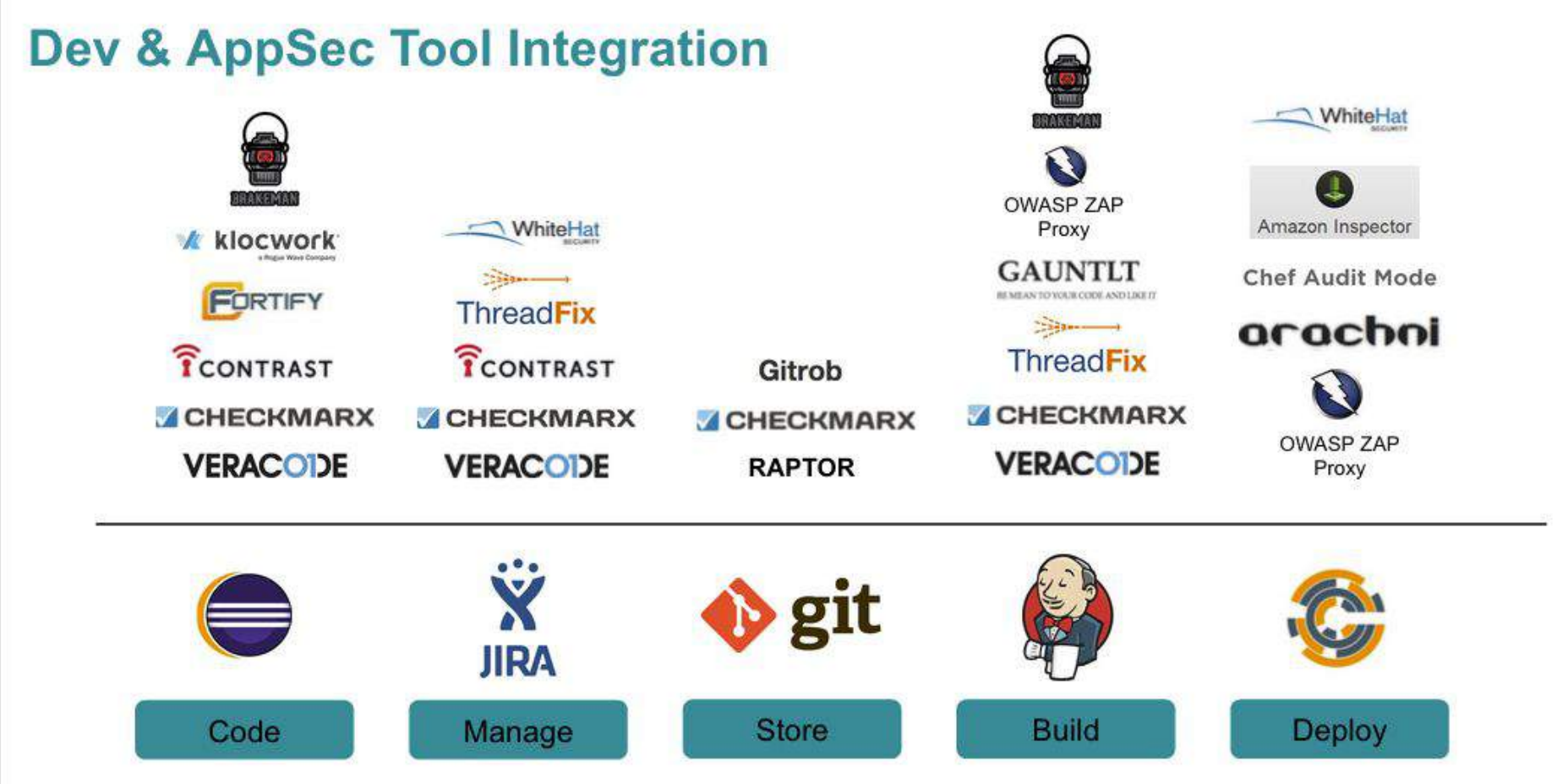

SCORE <1>
000290
HI-SCORE
000000
SCORE <2>
000000
2


WAPT Report
INTERNET BANKING
12 March 2019

(4) Your reports are dead

4.2 Security bugs integrated in lifecycle

Security bugs are bugs



Why it works

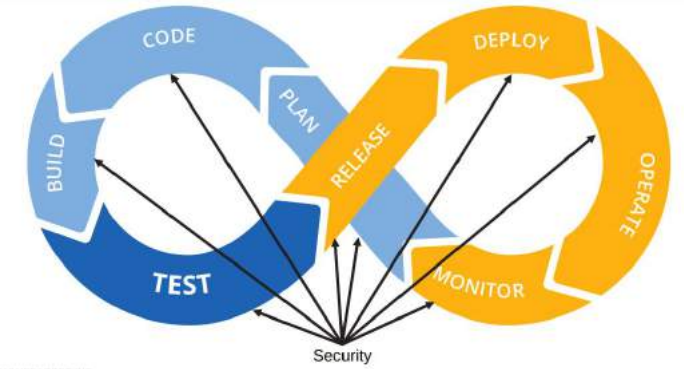
1. Improve the security culture

The purpose and intent of DevSecOps is to build on the mindset that **"everyone is responsible for security"**

2. More security champions

- Security Champions are active members of a team that may help to make decisions about when to engage the Security Team
- Act as the "voice" of security for the given product or team
- Assist in the triage of security bugs for their team or area

3. Less time to implement the fixes of security bugs



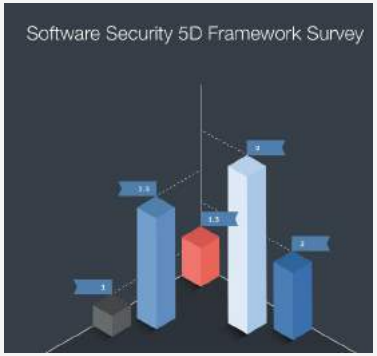
(5) Conclusions

5.1 Top Things to do

5.1 Top Things to do

THREAT MODELING

Threat Modeling and Compliance



Processes and Standards

3.2 Secure Software Engineering

Art. 25 Security by design

What is Threat modeling?

We do threat modeling every day.

Threat modeling answers to the question: what can go wrong?

What is Threat modeling?

The Threat Modeling activity allows the systematic identification and valorization of the threats that could affect the developing system. The goal is to identify the most serious threats and start from these to mitigate the risk.

Terminology:

Asset: a valuable resource (data, systems, functionalities)

Threat: a potential occurrence that can cause damage to assets

Vulnerability: a lack in some feature or system design that makes the threat possible

Attack: action taken by someone who creates damage to an asset

Mitigation: a security measure that manages a threat and mitigates the risk

Methodology:

- Identify application asset
- Assume potential attack scenarios to identify threats
- Document the possible threats and identify mitigation
- Evaluate the risk related to the presence of the threat

May I see a real example?

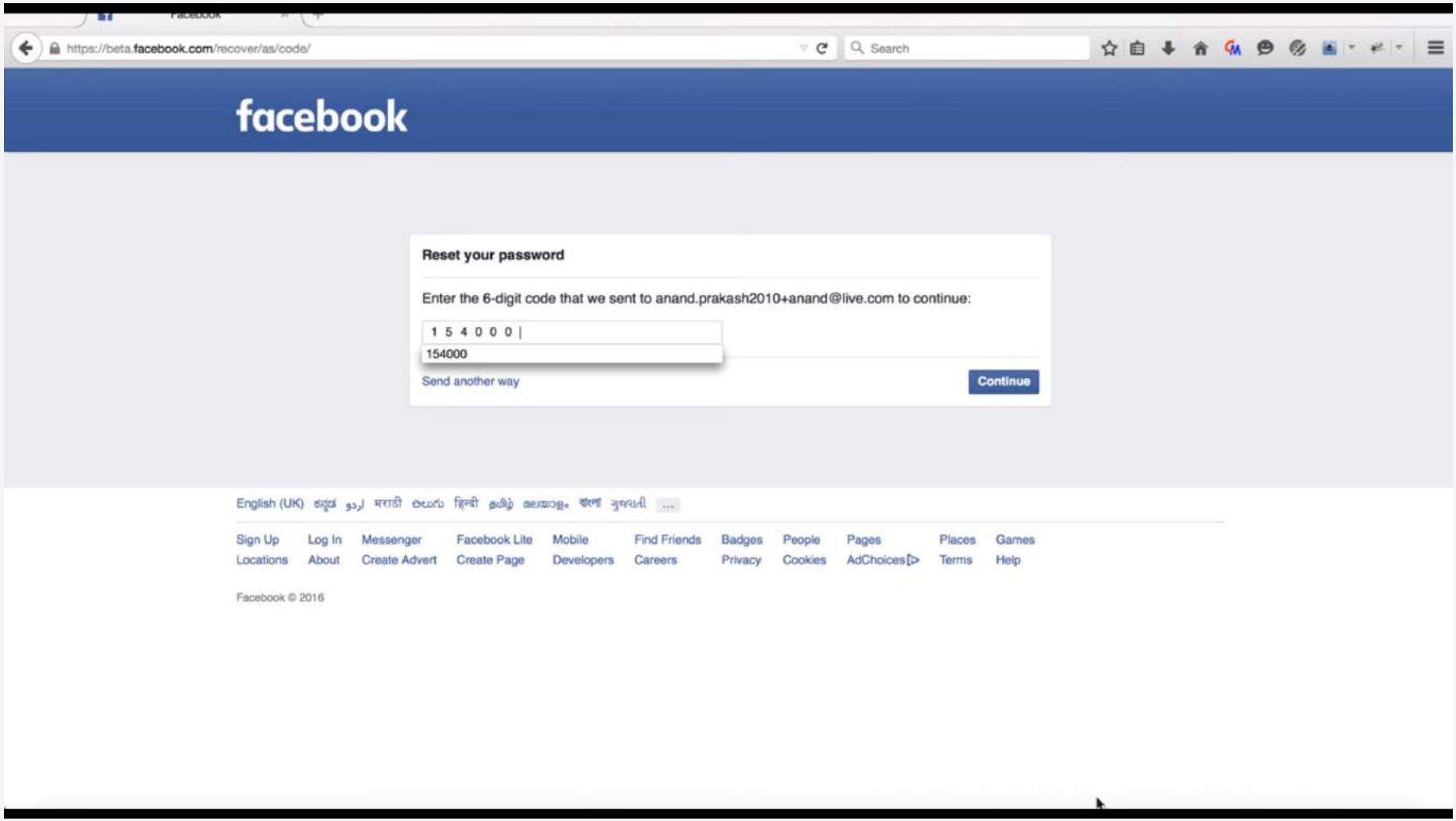
Threat Modeling: reset password functionality

- When user can not login, you have to manage it maybe with a pwd reset.
- Usually you can send to the user email inbox a link which contains an identifier linked to the user:
  www.facebook.com/pwreset/ut=aj32d2828DJJAJD823

What are the possible threats to this model?

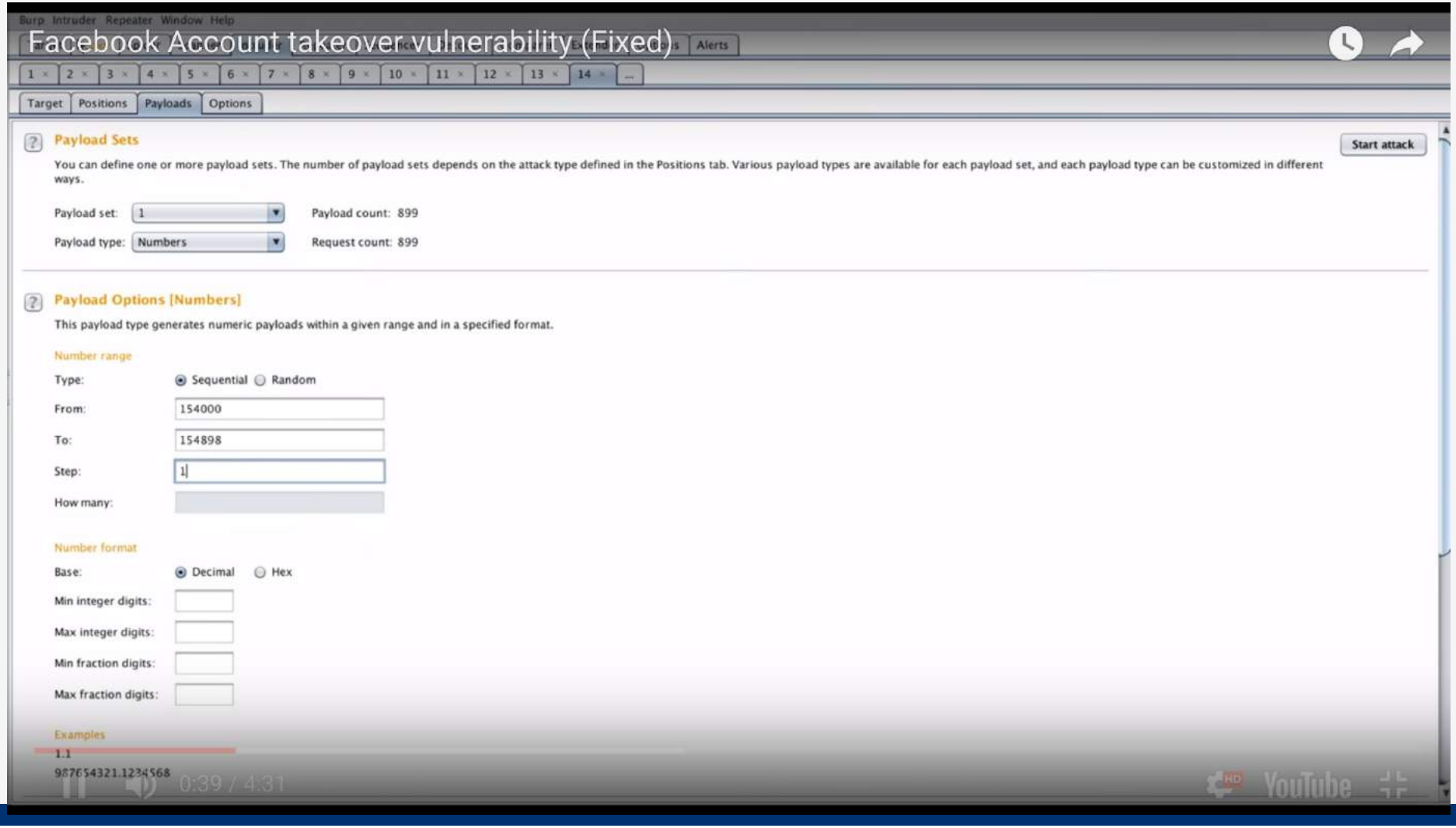
Let's see a real example occurs at Facebook (2017)

Facebook Reset pwd



Source: https://thehackernews.com/2016/03/hack-facebook-account.html

Facebook Reset pwd



Facebook Reset pwd

Attack Save Columns

Results | Target | Positions | Payloads | Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
8	154007	200			42780	
9	154008	200			42742	
10	154009	200			42742	
11	154010	200			42780	
12	154011	200			42782	
13	154012	200			42782	
14	154013	200			42780	
15	154014	200			42742	
16	154015	200			42742	
17	154016	200			42742	
18	154017	200			42782	
19	154018	200			42780	
20	154019	200			42742	
21	154020	200			42742	
22	154021	200			42742	

Request | Response

Raw | Params | Headers | Hex

```
POST /recover/as/code/ HTTP/1.1
Host: beta.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:37.0) Gecko/20100101 Firefox/37.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://beta.facebook.com/recover/as/code/
Cookie: datr=62onVq9hwbhNjy5MXffsO7QQ; fr=0vz212Qg2fhIOfDNv.AWUDclDLAyXnUBRqC-IioQrCsho.BWJ2th.js.AAA.0.AWXDRPit; lu=RA-U-EmXQwpuklzwvV69_Aag; _ga=GA1.2.1350052445.1445425356;
x-referer=%2Fsettings%2Fsecurity%2F%3Fdevice_based_login%26refid%3D72%23%2Fsettings%2Fsecurity%2F; locale=en_GB;
reg_fb_ref=https%3A%2F%2Fwww.facebook.com%2F%3Fstype%3Dlo%26jlou%3DAffyGPonEzegSqgrfTy9U407d2YMYssITVgAf-N1bD9wskz1hYUV7vZP9Fk7YKgMzZAWZtS5AxGXGfDNiiMR_A00pi59cmzoJSH5Fk4mRhYMvg%26smuh%3D3380%261h%3DA
c9eoHLhFF8zi-1t;
reg_fb_gate=https%3A%2F%2Fwww.facebook.com%2F%3Fstype%3Dlo%26jlou%3DAffyGPonEzegSqgrfTy9U407d2YMYssITVgAf-N1bD9wskz1hYUV7vZP9Fk7YKgMzZAWZtS5AxGXGfDNiiMR_A00pi59cmzoJSH5Fk4mRhYMvg%26smuh%3D3380%261h%3D
Ac9eoHLhFF8zi-1t;
sfiu=AYiGPvOeh18M6islm3C3M1VdZShQmuo_5o3CG2pTmeXoho4QKrP-YNQovbX4MBjIbH6RStutenPqYT2pKebSNjkz8bHVphXhmwuNt3obX8exKhc0EUIKFITgJXHklxk031gnBCBV8RMytKcRySFcqgHeNFdEdfCAWIbGpRctuAUFFkFOXPEoG5XLrlVW8x0GhuI
CiKVa7NUoJEc7ByIoqRNm; wd=1440x734
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 21

lsd=AVrvDZBe&n=154010
```

? < + > Type a search term 0 matches

32 of 899

MINDED SECURITY
The Software Security Company

Facebook Reset pwd

Facebook Account takeover vulnerability (Fixed)

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
885	154884	200			42742	
886	154885	200			42742	
887	154886	200			42780	
888	154887	200			42782	
889	154888	200			42742	
890	154889	200			42742	
891	154890	200			42782	
892	154891	200			42742	
893	154892	200			42742	
894	154893	200			42742	
895	154894	200			42782	
896	154895	200			42742	
897	154896	200			42742	
898	154897	200			42820	
899	154898	302			1237	

Request | Response

Raw | Headers | Hex

```
HTTP/1.1 302 Found
Pragma: no-cache
Expires: Sat, 01 Jan 2000 00:00:00 GMT
Location: https://beta.facebook.com/recover/password?u=100005363430566&n=154898
Cache-Control: private, no-cache, no-store, must-revalidate
Content-Security-Policy: default-src * data: blob:;script-src *.facebook.com *.fbcdn.net *.facebook.net *.google-analytics.com *.virtualearth.net *.google.com 127.0.0.1:* *.spotilocal.com:*
'unsafe-inline' 'unsafe-eval' fbstatic-a.akamaihd.net fbcdn-static-b-a.akamaihd.net *.atlassolutions.com blob:;style-src * 'unsafe-inline' data:;connect-src *.facebook.com *.fbcdn.net *.facebook.net
*.spotilocal.com:* *.akamaihd.net wss://*.facebook.com:* https://fb.scanandcleanlocal.com:* *.atlassolutions.com attachment.fbsbx.com blob:;
X-XSS-Protection: 0
X-Content-Type-Options: nosniff
P3P: CP="Facebook does not have a P3P policy. Learn why here: http://fb.me/p3p"
X-Frame-Options: DENY
Set-Cookie: wd=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=-1456165704; path=/; domain=.facebook.com; httponly
Content-Type: text/html
X-FB-Debug: G4m4T6lqgKnSG531ROiLqT8k+Otjq7uAI8qiwNB9fasszHk9sGJiLaRI5eL2DDxJao6ssXNmdFslFWwTaae64w==
Date: Mon, 22 Feb 2016 18:28:25 GMT
Connection: close
Content-Length: 0
```

Settings

3:52 / 4:31

YouTube

MINDED SECURITY
The Software Security Company

Facebook Reset pwd

https://beta.facebook.com/recover/password?u=100005363430566&c=154898

Search

facebook

Choose a new password

A strong password is a combination of letters and punctuation marks. It must be at least 6 characters long.

New password | Hide | ?

Continue | Cancel

English (UK) ಕನ್ನಡ اردو मराठी తెలుగు हिन्दी தமிழ் മലയാളം বাংলা ગુજરાતી ...

Sign Up | Log In | Messenger | Facebook Lite | Mobile | Find Friends | Badges | People | Pages | Places | Games
Locations | About | Create Advert | Create Page | Developers | Careers | Privacy | Cookies | AdChoices | Terms | Help

Facebook © 2016

Threat Modeling: reset password functionality

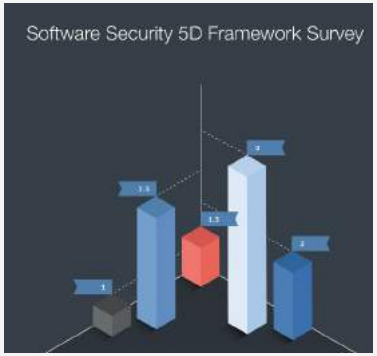
- After a threat modeling analysis you can give to the developers team the following security requirements:

Threat	Objective	Mitigation
UT guessing	User password reset	- Use a random function to generate the UT - The UT must be more than 20 chars length
UT brute forcing	User password reset	- Verify that the same user session will not ask for more than 3 different requests (anti brute forcing functionality)
Email compromised	Obtain a valid UT	- set a timeframe validity of the UT of 30 mins - verify that the IPAddress of the first request is the same of the link with the UT.
…	…	…

5.1 Top Things to do

5.2 SECURE CODE REVIEW

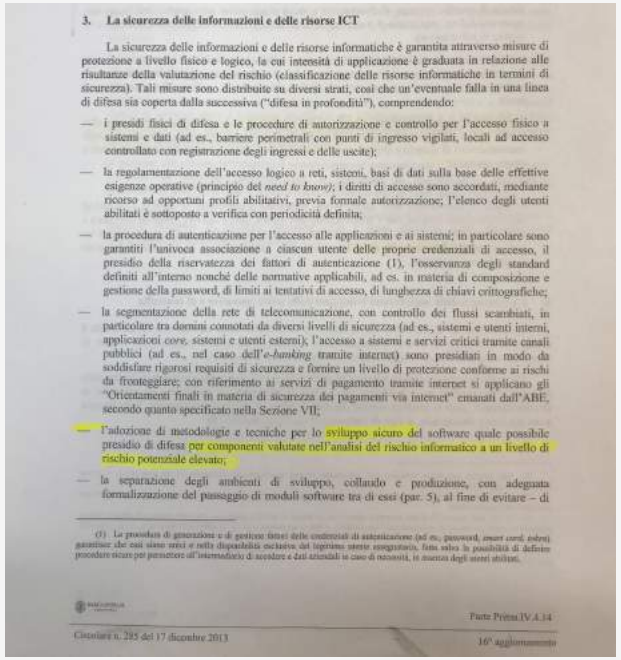
Secure Code Review and Compliance



Processes and Testing

2.4 Software security assurance

Art. 25 Security by design



3. La sicurezza delle informazioni e delle risorse ICT

La sicurezza delle informazioni e delle risorse informatiche è garantita attraverso misure di protezione a livello fisico e logico, la cui intensità di applicazione è graduata in relazione alle risultanze della valutazione del rischio (classificazione delle risorse informatiche in termini di sicurezza). Tali misure sono distribuite su diversi strati, così che un'eventuale falla in una linea di difesa sia coperta dalla successiva ("difesa in profondità"), comprendendo:

— i presidi fisici di difesa e le procedure di autorizzazione e controllo per l'accesso fisico a sistemi e dati (ad es., barriere perimetrali con punti di ingresso vigilati, locali ad accesso controllato con registrazione degli ingressi e delle uscite);

— la regolamentazione dell'accesso logico a reti, sistemi, basi di dati sulla base delle effettive esigenze operative (principio del *need to know*); i diritti di accesso sono accordati, mediante ricorso ad opportuni profili abilitativi, previa formale autorizzazione; l'elenco degli utenti abilitati è sottoposto a verifica con periodicità definita;

— la procedura di autenticazione per l'accesso alle applicazioni e ai sistemi; in particolare sono garantiti l'univoca associazione a ciascun utente delle proprie credenziali di accesso, il presidio della riservatezza dei fattori di autenticazione (1), l'osservanza degli standard definiti all'interno nonché delle normative applicabili, ad es. in materia di composizione e gestione della password, di limiti ai tentativi di accesso, di lunghezza di chiavi crittografiche;

— la segmentazione della rete di telecomunicazione, con controllo dei flussi scambiati, in particolare tra domini connotati da diversi livelli di sicurezza (ad es., sistemi e utenti interni, applicazioni *core*, sistemi e utenti esterni); l'accesso a sistemi e servizi critici tramite canali pubblici (ad es., nel caso dell'*e-banking* tramite internet) sono presidiati in modo da soddisfare rigorosi requisiti di sicurezza e fornire un livello di protezione conforme ai rischi da fronteggiare; con riferimento ai servizi di pagamento tramite internet si applicano gli "Orientamenti finali in materia di sicurezza dei pagamenti via internet" emanati dall'ABE, secondo quanto specificato nella Sezione VII;

— l'adozione di metodologie e tecniche per lo sviluppo sicuro del software quale possibile presidio di difesa per componenti valutate nell'analisi del rischio informatico a un livello di rischio potenziale elevato;

— la separazione degli ambienti di sviluppo, collaudo e produzione, con adeguata formalizzazione del passaggio di moduli software tra di essi (par. 5), al fine di evitare – di

(1) Le procedure di generazione e di gestione fattori delle credenziali di autenticazione (ad es., password, smart card, token) garantiscono che essi siano noti e nella disponibilità esclusiva del legittimo utente assegnatario, fatta salva la possibilità di definire procedure sicure per permettere all'intermediario di accedere a dati aziendali in caso di necessità, in assenza degli utenti abilitati.

Parte Prima IV.4.14

Circolare n. 285 del 17 dicembre 2013

16° aggiornamento

MINDED SECURITY
The Software Security Company

Secure Code Review

The activity of Secure Code Review consists in the security analysis of the source code of the application line by line: it is also called a white box test, to underline the fact that the person performing the verification has complete knowledge of the application (set of sources).

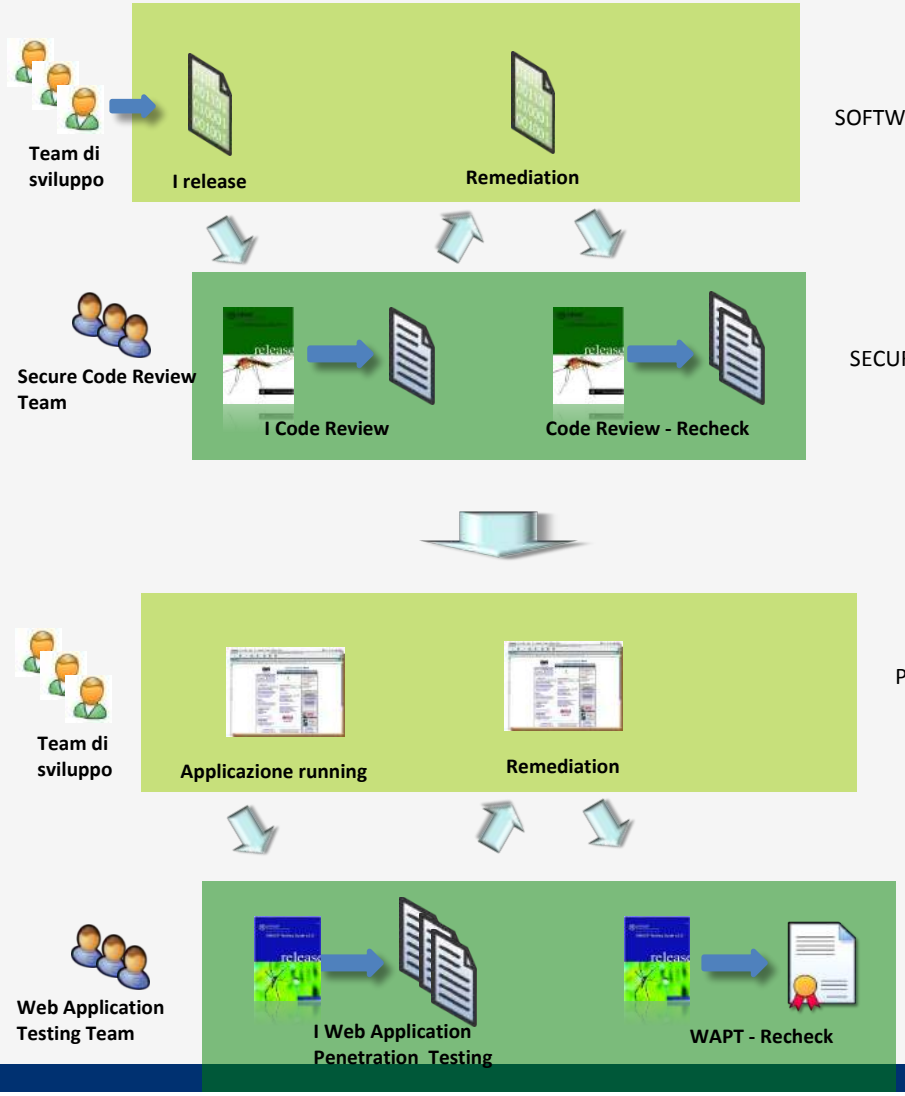
This activity is a manual process: some tools can be used to carry out some analysis activities but these can not understand the application context that is the cornerstone of the code review.

MINDED SECURITY
The Software Security Company

Code Review vs Application Testing

- **Secure Code Review:** The Secure Code Review activity is the security analysis of the source code of an application made line by line: it is also called a white box test, to underline the fact that the person performing the verification has complete knowledge of the application (set of sources).
- **Web Application Penetration Testing (WAPT):** the Web Application Penetration Testing activity is a real simulation of a cyber attack on the application, in order to evaluate the actual level of security. This test is called a "black box" because in this circumstance the user who performs the analysis does not have any knowledge about the software, and wants to ensure that there are no safety issues before the deployment in operation.

SCR & WAPT in the processes



Verification phase during software development

Verification phase during pre-operation start-up

MINDED SECURITY
The Software Security Company

SECURE SDLC phase 0: 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);

}
```

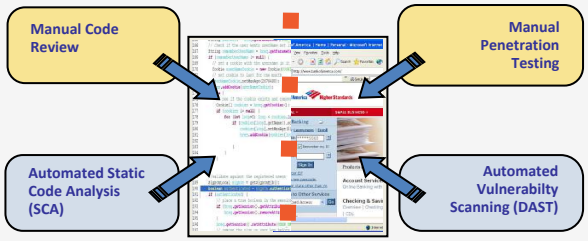
Secure Software

International standards and Manual Secure Code Review

OWASP Secure Code Review Guide:

"Manual secure code review provides insight into the "real risk" associated with insecure code. This contextual, white-box approach is the single most important value. A human reviewer can understand the relevance of a bug or vulnerability in code. Context requires human understanding of what is being assessed. With appropriate context we can make a serious risk estimate that accounts for both the likelihood of attack and the business impact of a breach. Correct categorization of vulnerabilities helps with priority of remediation and fxing the right things as opposed to wasting time fixing everything."

Reference: https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project



The combination of the 4 techniques produces the best results

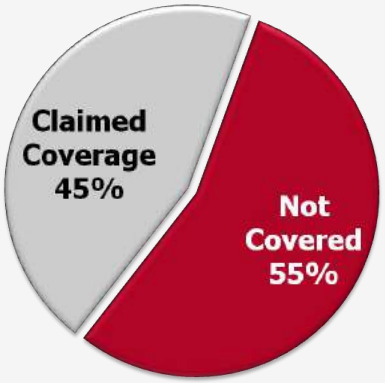
PCI-DSS v3.2.1:

5.10 PCI-DSS Requirements Related to Code Review Specifically, requirement 6.3.2 mandates a code review of custom code. Reviewing custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes)

Reference:
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1539762215120

Wikipedia su Application Security: "The human brain is suited more for filtering, interrupting and reporting the outputs of automated source code analysis tools available commercially versus trying to trace every possible path through a compiled code base to find the root cause level vulnerabilities."

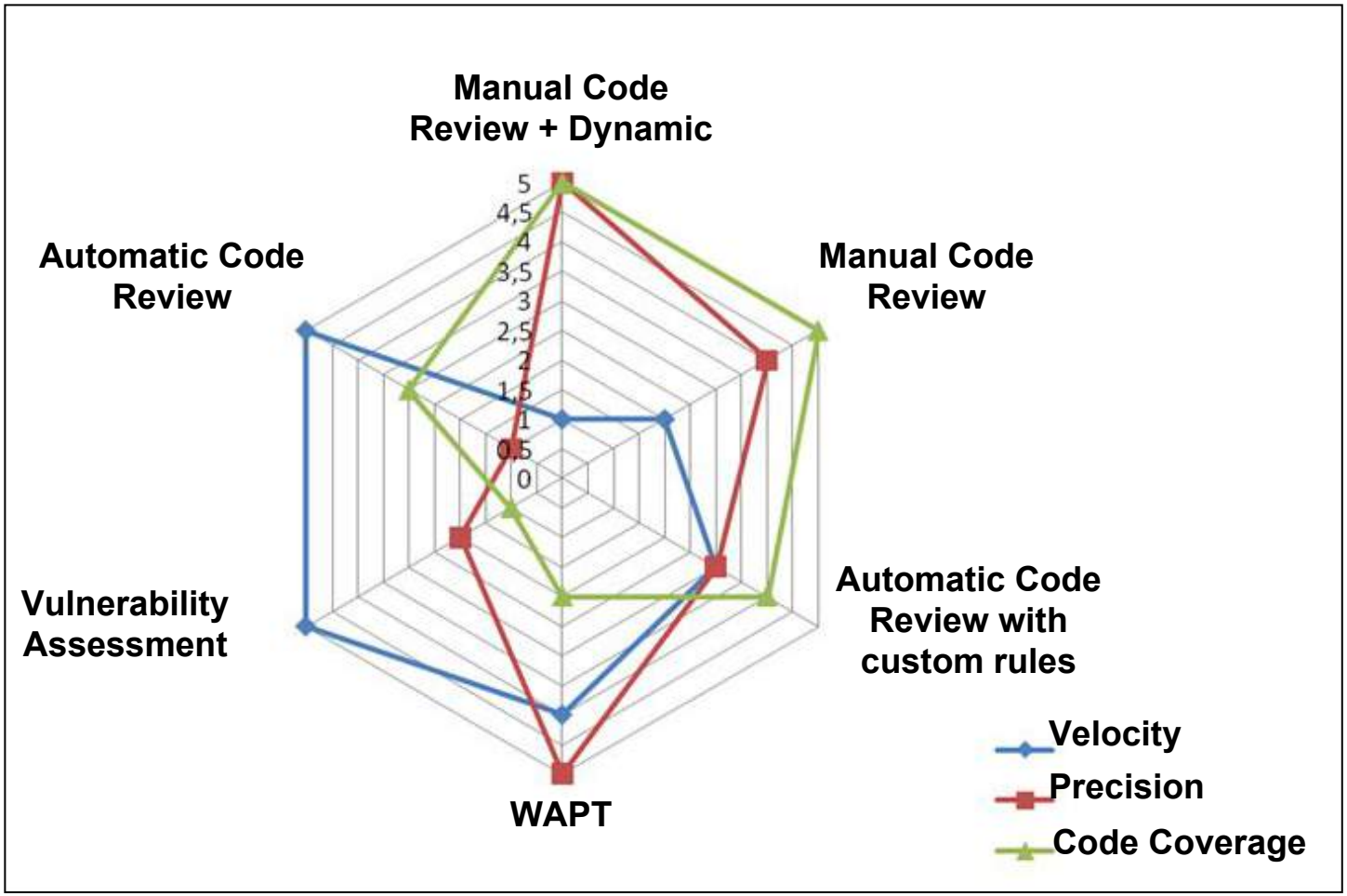
Manual and automated revisions of the source code complement each other, each of which covers areas where the other is generally weak.



MITRE:
MITRE found that all application security tool vendors' claims put together cover only 45% of the known vulnerability types (over 600 in CWE)

They found very little overlap between tools, so to get 45% you need them all (assuming their claims are true)

CR – General comparison



(5) Conclusions

5.3 Vendors requirements

What do you ask to your Sw Vendor?

- lock?
- owasp?
- top10?
- a WAPT report?
- can you show me how you develop secure software?

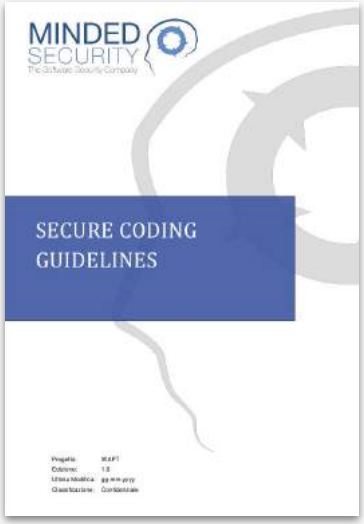
Software suppliers governance

We do not know if the suppliers apply:

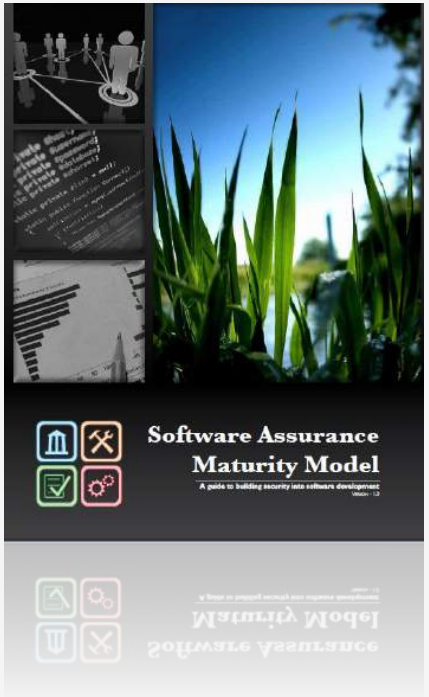
- Secure coding practice;
- Secure Software training;
- Software assurance contract to avoid deploy insecure software.

PCI S-SDL

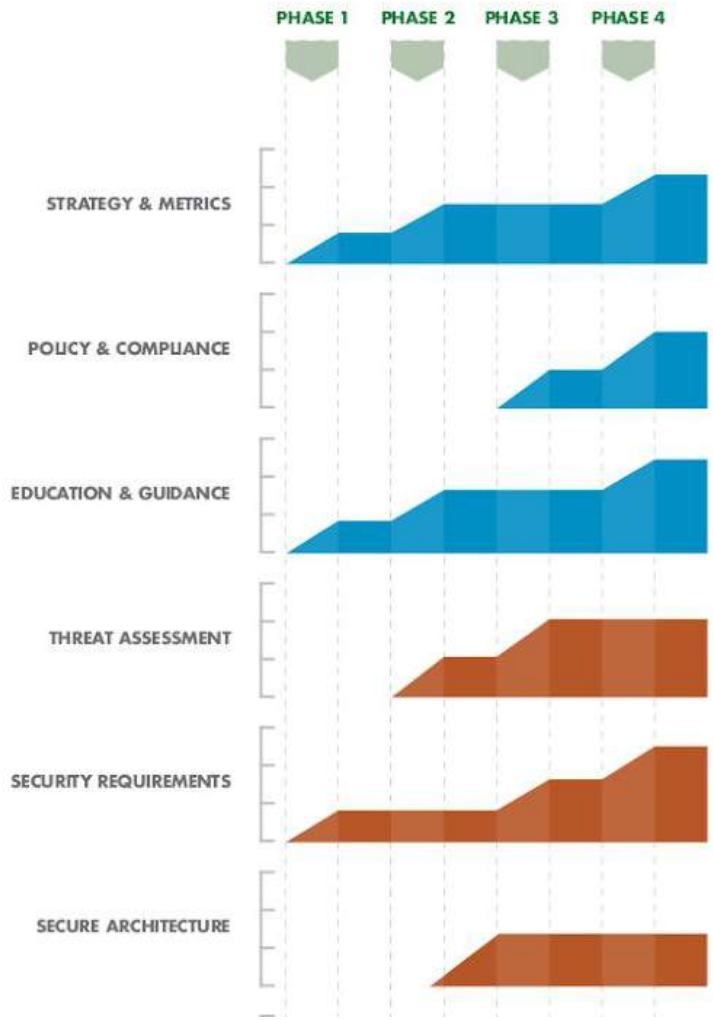
- 2.3 Strategy for sw vendor



Secure Software Assurance Contract



SAMM Independent Software Vendor



ISV example

CERTIFICATE OF ACHIEVEMENT

[redacted] performed an **OpenSAMM** (Software Assurance Maturity Model) assessment and achieved

Target maturity levels for an Independent Software Vendor roadmap - Phase 2

in the following security practices

Security Practices	Target	Achieved
Strategy & Metrics	2	2
Policy & Compliance	n/a	1
Education & Guidance	2	2
Threat Assessment	1	3
Security Requirements	1	3
Secure Architecture	n/a	2
Design Review	1	2
Code Review	2	2
Security Testing	2	3
Vulnerability Management	1	2
Environment Hardening	n/a	-
Vulnerability Management	[illegible]	2

Key Assessment Parameters:	
Date of Period	July 17 - July 20, 2018
Location	[redacted]
Assessment Style	Detailed
SAMM Model	Open SAMM V1.0
Model Scope	Independent Software Vendor roadmap Phase 2
Organizational Unit	[redacted]
Organizational Scope	[redacted] Software release: R12
Coverage Measure	This scope covered more than 50% of people

Assesment Lead:	Affiliation
Gianrico Ingrosso	Minded Security

Matteo Meucci, CEO

Minded Security S.r.l.,
The Software Security Company

I affirm that the information in this certificate is accurate.

OWASP

OPENSAMM

MINDED SECURITY

OWASP and Open SAMM logos are available under the CC-BY 3.0 license

Conclusions: what do we take home?

- "Vulnerabilities in the software development process are expected": hence the need to create a governance process of secure development (Software Security Processes).

- "If you do not require security features, you will not get secure software": hence the need for guidelines and standards for secure development (Software Security Standards e Tools)

- "Everyone is responsible for security": all the people involved in the software development process must be involved in the security aspects and make their own contribution (Software Security Team e Awareness). If you do not have a security team you need it now.

- OWASP SAMM Assessment and 5D Framework are standards that allows to create a Software Security program that involves all the people working in the SDLC in order to create their own S-SDLC. They implement the GDPR requirement “Security by Design“

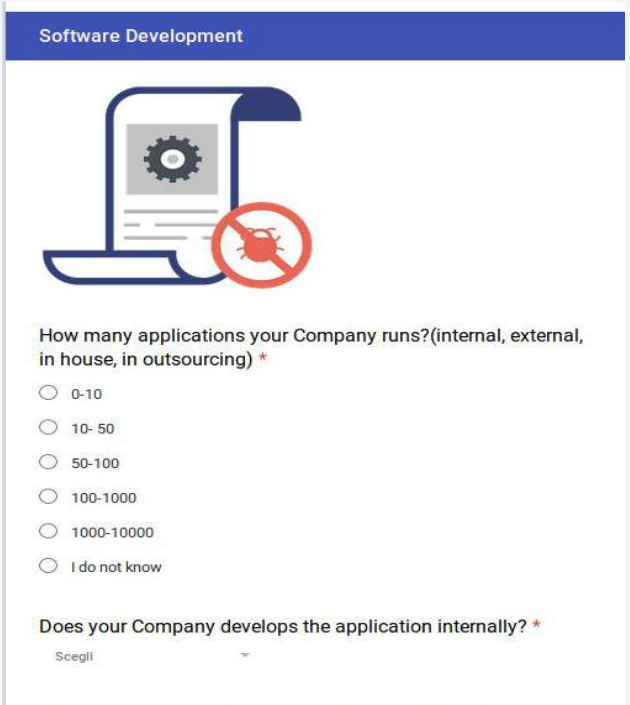
- PCI, GDPR are usually a great driver to start an S-SDLC program

What Minded Security does to improve Companies SwSec

Stand at Security Summit

SwSwec 5D Framework

Take a survey and win an Ipad!



Stickers, brochures, talks

Questions?

Matteo Meucci
matteo.meucci@mindedsecurity.com

Site: http://www.mindedsecurity.com
Blog: http://blog.mindedsecurity.com
Twitter: http://twitter.com/mindedsecurity
BlueClosure: http://www.blueclosure.com

Thanks!

MINDED SECURITY
The Software Security Company

References

(1) Jeff Williams, Contrast Security: "Continuous Application Security at Scale with IAST and RASP"

(2)https://www.csoonline.com/article/2978858/application-security/is-poor-software-development-the-biggest-cyber-threat.html

(3) https://www.spec-india.com/blog/from-waterfall-to-agile-to-devops-a-cultural-and-technological-shift/

(4) Peter Chestna, Veracode: "AppSec in a DevOps World"

(5) XebiaLab: ITRev_DevOps_Guide_5_2015