15 JUNE, 2018

Getting benefits of OWASP ASVS at initial phases

NDS {OSLO} 2018

OLEKSANDR KAZYMYROV

EVRY

Introduction

Introduction

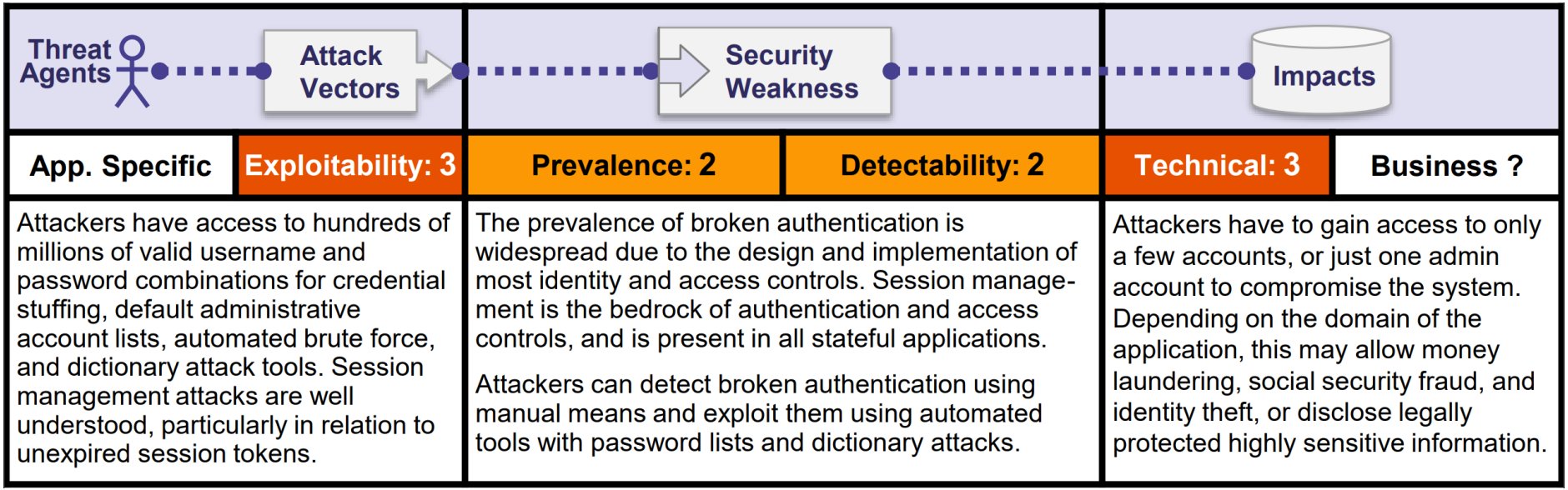
Security Development Lifecycle (SDL)

What is a secure application?

S.M.A.R.T. criteria

Specific	• Is it clearly described and understandable?
Measurable	• How will you know when you are reached it?
Achievable	• Are you able to accomplish it?
Relevant	• Is the web application criterion in line with business needs?
Time Limited	• When do you want to achieve it?

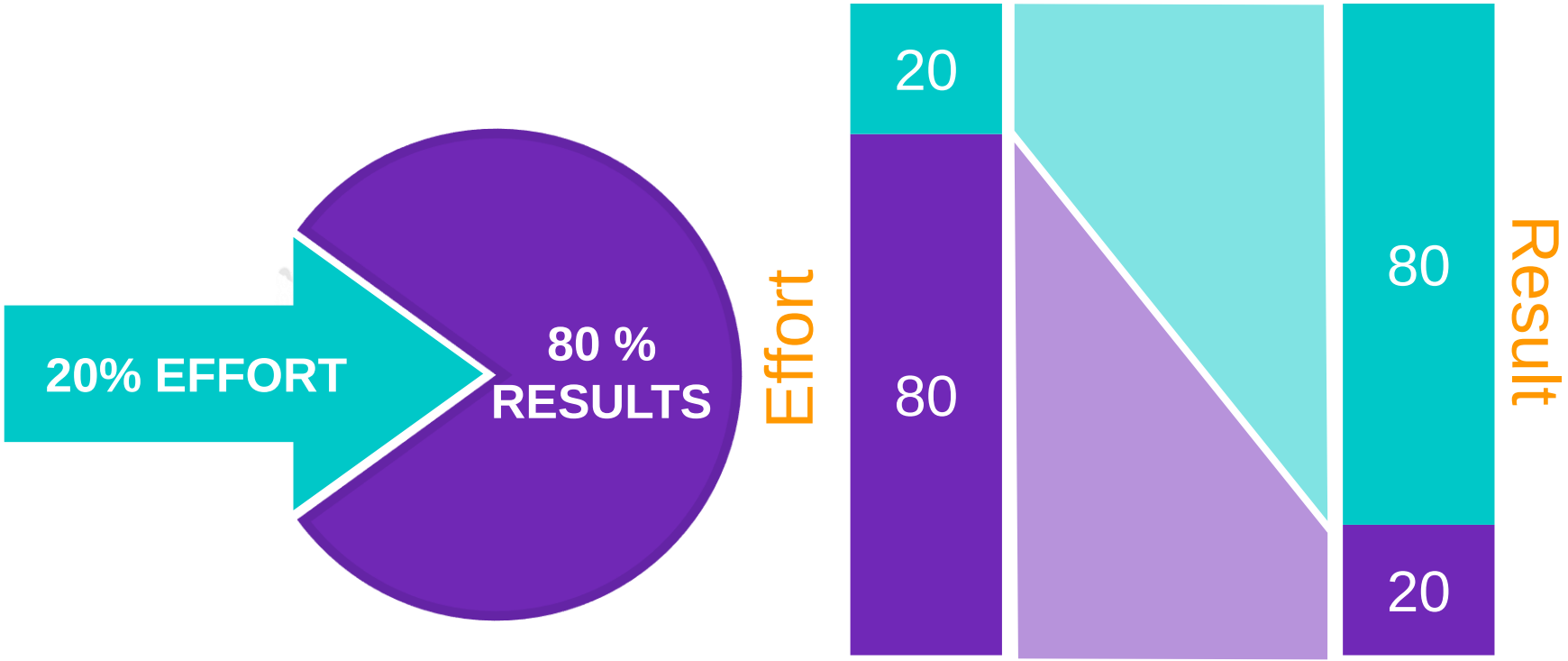
Achievability



OWASP Top 10 2017 – A2 Broken Authentication

EVRY

Achievability and Pareto principle

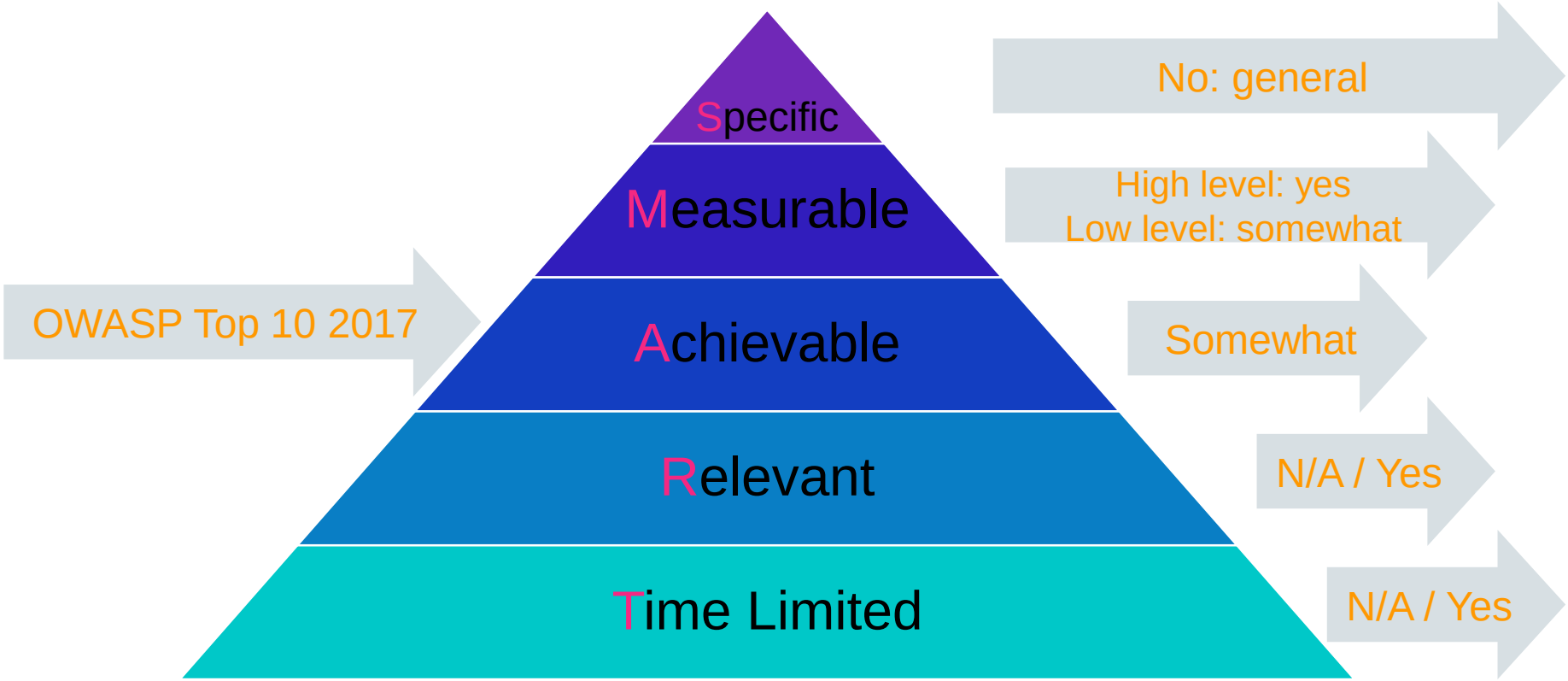


What changed from 2013 to 2017?

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Deserialization vulnerability

OWASP Top 10 2017 through the S.M.A.R.T. prism



OWASP Top 10 2017

"The OWASP Top 10 is a powerful awareness document for web application security. It represents a broad consensus about the most critical security risks to web applications."

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP Application Security Verification Standard (ASVS)

From PCI DSS to OWASP ASVS

Penetration Test Guidance

- NIST SP-800-XXX
- OWASP
- SANS
- …

- NIST SP 800-115
- OWASP Testing Guide
- OSSTMM
- ...

- PCI DSS mapping
- MITRE CWE
- OWASP Top 10
- …

Key parts of OWAS ASVS (v3.0.1)

Scope for the application security verification standard

Description of security verification levels

Requirements / Controls

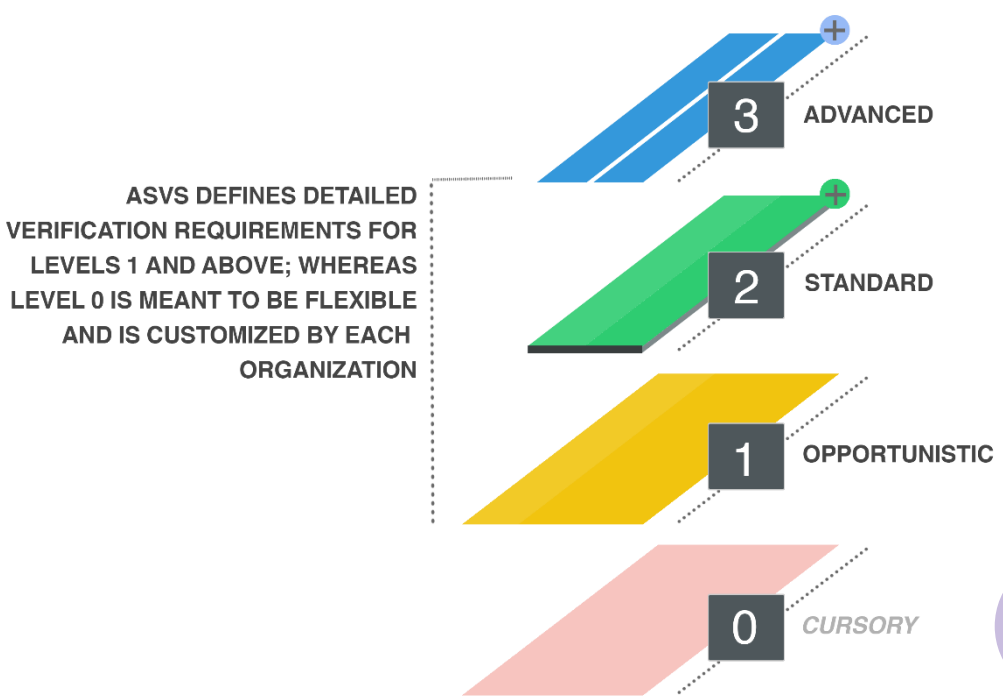
Standards Mappings

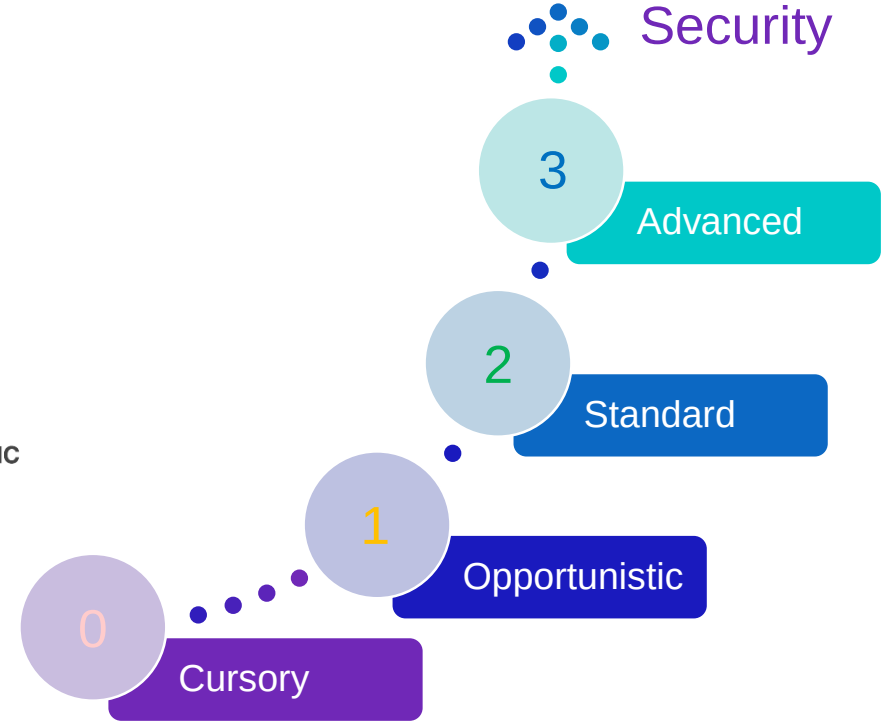
What is covered by OWAS ASVS?

- Web Applications
- Server Configuration
- Mobile Clients
- Web Services
- Communication

EVRY

OWASP ASVS Levels





OWAS ASVS verification controls (v3.0.1)

Category	Level 1	Level 2	Level 3
V1: Architecture, design and threat modelling	1	8	11
V2: Authentication Verification Requirements	18	25	27
V3: Session Management Verification Requirements	11	13	13
V4: Access Control Verification Requirements	7	11	12
V5: Malicious input handling verification requirements	10	20	21
V7: Cryptography at rest verification requirements	2	7	10
V8: Error handling and logging verification requirements	3	9	13
V9: Data protection verification requirements	4	8	11
V10: Communications security verification requirements	7	9	13
V11: HTTP security configuration verification requirements	6	8	8
V13: Malicious controls verification requirements	0	0	2
V15: Business logic verification requirements	0	2	2
V16: Files and resources verification requirements	7	9	9
V17: Mobile verification requirements	7	10	11
V18: Web services verification requirements	7	10	10
V19: Configuration	1	5	10
Total:	91	154	183

EVRY

General level profiles

Industry	Threat Profile	L1 Recommendation	L2 Recommendation	L3 Recommendation
Healthcare	Most attackers are looking for sensitive data that can be used to directly or indirectly profit from to include personally identifiable information and payment data. Often the data can be used for identity theft, fraudulent payments, or a variety of fraud schemes. For the US healthcare sector, the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, Breach Notification Rules and Patient Safety Rule (http://www.hhs.gov/ocr/privacy/=.	All network accessible applications	Applications with small or moderate amounts of sensitive medical information (Protected Health Information), Personally Identifiable Information, or payment data.	Applications used to control medical equipment, devices, or records that may endanger human life. Payment and Point of Sale systems (POS) that contain large amounts of transaction data that could be used to commit fraud. This includes any administrative interfaces for these applications

OWAS ASVS verification controls

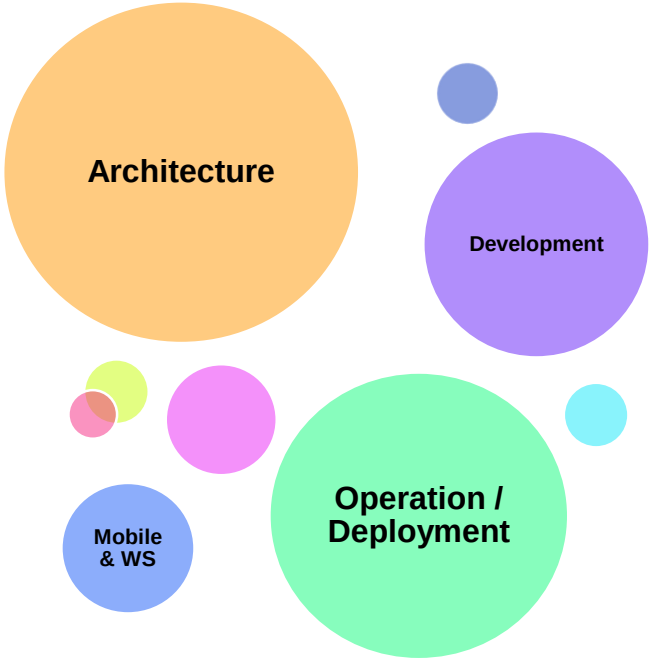
V2: Authentication Verification Requirements

#	Description	1	2	3
2.1	Verify all pages and resources by default require authentication except those specifically intended to be public (Principle of complete mediation).	✓	✓	✓
2.2	Verify that forms containing credentials are not filled in by the application. Pre-filling by the application implies that credentials are stored in plaintext or a reversible format, which is explicitly prohibited.	✓	✓	✓
2.4	Verify all authentication controls are enforced on the server side.	✓	✓	✓
2.6	Verify all authentication controls fail securely to ensure attackers cannot log in.	✓	✓	✓
2.7	Verify password entry fields allow, or encourage, the use of passphrases, and do not prevent password managers, long passphrases or highly complex passwords being entered.	✓	✓	✓
2.8	Verify all account identity authentication functions (such as update profile, forgot password, disabled / lost token, help desk or IVR) that might regain access to the account are at least as resistant to attack as the primary authentication mechanism.	✓	✓	✓

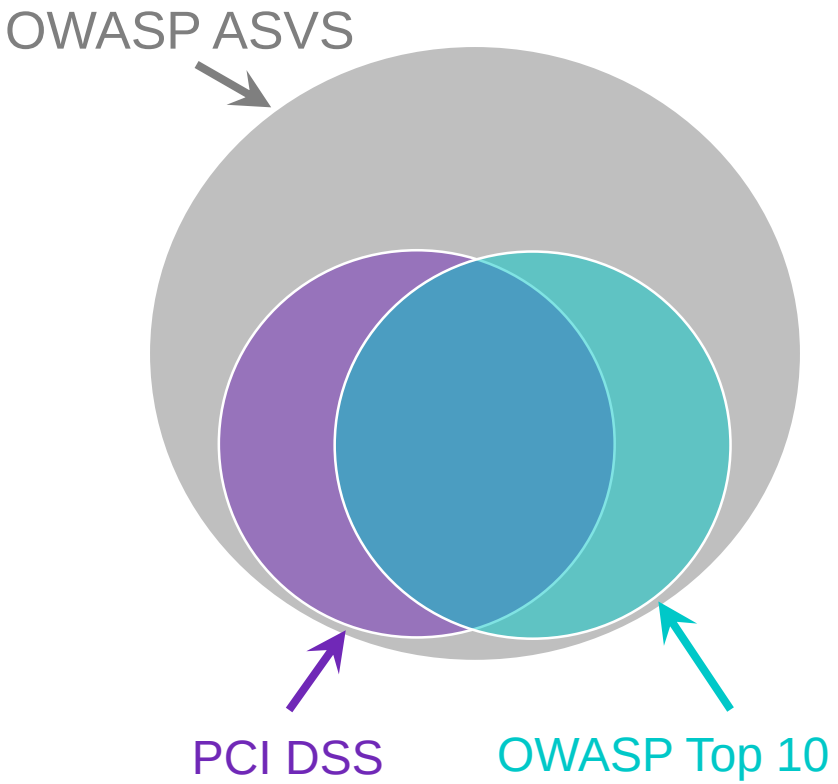
V3: Session Management Verification Requirements

#	Description	1	2	3
3.1	Verify that there is no custom session manager, or that the custom session manager is resistant against all common session management attacks.	✓	✓	✓
3.2	Verify that sessions are invalidated when the user logs out.	✓	✓	✓
3.3	Verify that sessions timeout after a specified period of inactivity.	✓	✓	✓
3.4	Verify that sessions timeout after an administratively-configurable maximum time period regardless of activity (an absolute timeout).		✓	✓
3.5	Verify that all pages that require authentication have easy and visible access to logout functionality.	✓	✓	✓
3.6	Verify that the session id is never disclosed in URLs, error messages, or logs. This includes verifying that the application does not support URL rewriting of session cookies.	✓	✓	✓
3.7	Verify that all successful authentication and re-authentication generates a new session and session id.	✓	✓	✓
3.10	Verify that only session ids generated by the application framework are recognized as active by the application.		✓	✓

EVRY


Architecture
Development
Operation /
Deployment
Mobile
& WS

OWASP ASVS


OWASP ASVS
PCI DSS
OWASP Top 10

OWASP Top 10 2017 vs OWASP ASVS

	Top 10	ASVS
Coverage	Web applications*	Full stack
Perspective	Black box	White box
Measurable	Somewhat	Yes
Product size	Small / Medium	Medium / Large
Scalability	Flat	Flexible

Application of OWASP ASVS

EVRY

Level definition for LS2 and CHC

LoginSevice2

- LS2 stays in front of almost all applications
- It is the first major security barrier
- LS2 helps to retrieve tokens (i.e., Secure Object) and hand over it to the 3rd party applications
- Available through the Internet

Cardholder Client

- CHC is a part of EVRY's NetBank (online banking)
- It can be integrated with any 3rd party web application
- EVRY's NetBank is protected by LoginsService2 in front of CHC
- After logging in CHC uses SO as the main parameter in session management
- Available through the Internet

OWASP ASVS Level 3

OWASP ASVS Level 2 (3)

Compliance selection at EVRY Financial Services

FINODS	Highly Sensitive	Moderate Sensitive	Low Sensitive
SWW - Self Service Non-Portal Applications over Internet	L3	L2	L2
SSP - Self Service Portal Applications over Internet	L3	L2	L2
CSW - Non-Portal Applications over dedicated Office Channel	L3	L2	L1
CSP - Portal Applications over dedicated Office Channel	L3	L2	L1
ESI - Web Services Applications over Internet	L3	L2	L2
ESS - Integrated customer solutions over service layer	L3	L2	L2

Non-OWASP ASVS security methodology

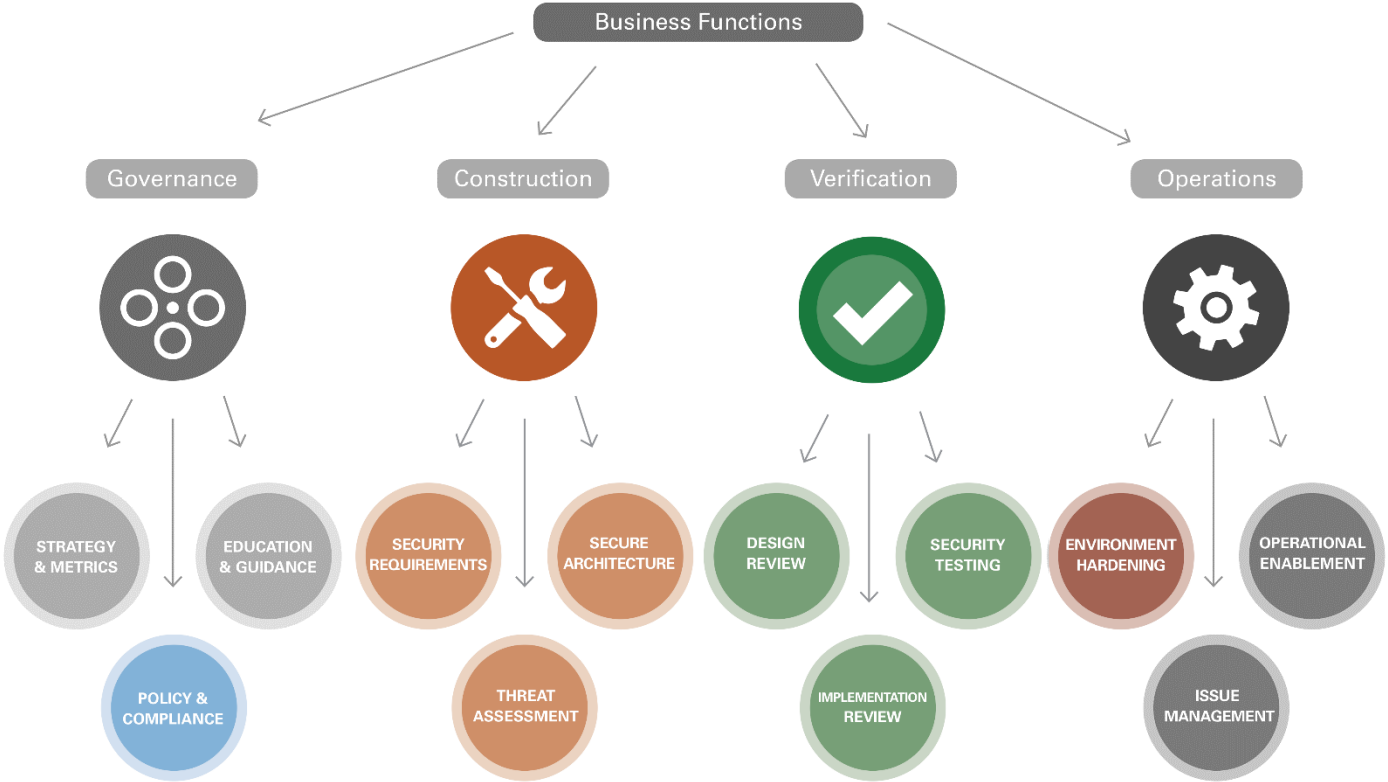
1.3	Verify that a high-level architecture for the application has been defined.		✓	✓
2.32	Verify that administrative interfaces are not accessible to untrusted parties.	✓	✓	✓
5.22	Make sure untrusted HTML from WYSIWYG editors or similar are properly sanitized with an HTML sanitizer and handle it appropriately according to the input validation task and encoding task.	✓	✓	✓
10.4	Verify that backend TLS connection failures are logged.			✓

EVRY

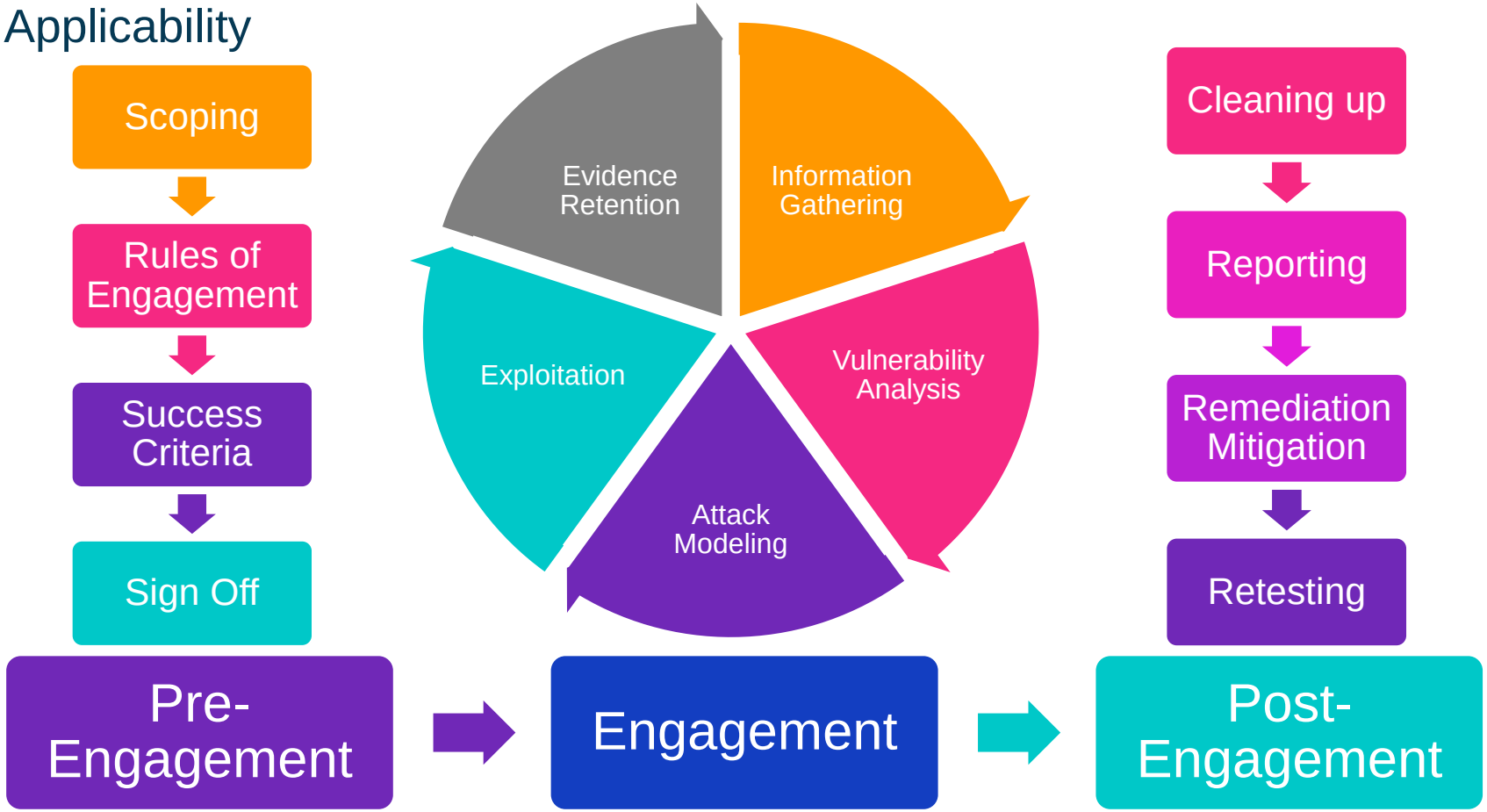
Product owners / architects & technical testing team

Product Owner / Architect	Security Testing Department
Define security requirements for AUT	Perform security assessment to verify defined requirements
Prepare the software architecture document (SAD), NFR checklist and security risk analysis document.	Verify SAD, NFR and SRA to be compliant with defined security expectations
Identify particular focus areas for code review, and participate follow-up meetings.	Complete security code review to verify source code do not contain vulnerabilities
Ensures that business and project goals are met	Report on deviations from security expectations
Gather results in the form of new or updated standards, guidelines and best practices	Keep up-to-date knowledge on new threads, vulnerabilities trends

OWASP Software Assurance Maturity Model (SAMM) and ASVS



Applicability



Conclusions


Security Development Lifecycle (SDL)
Is the application secure?
S.M.A.R.T. criteria
OWASP ASVS

EVRY


EVRY
Digital
+\dvantage