SAMM 2.0 - Changing the Role of App. Security

Yan Kravchenko,

CISSP, CSSLP, CISA, CISM

yan.kravchenko@concordusa.com

yan.kravchenko@owasp.org

@yanfosec

CONCORD

Agenda

1

- Evolution of Programming Languages

2

- Evolution of Development Methodologies

3

- Why OWASP SAMM?

4

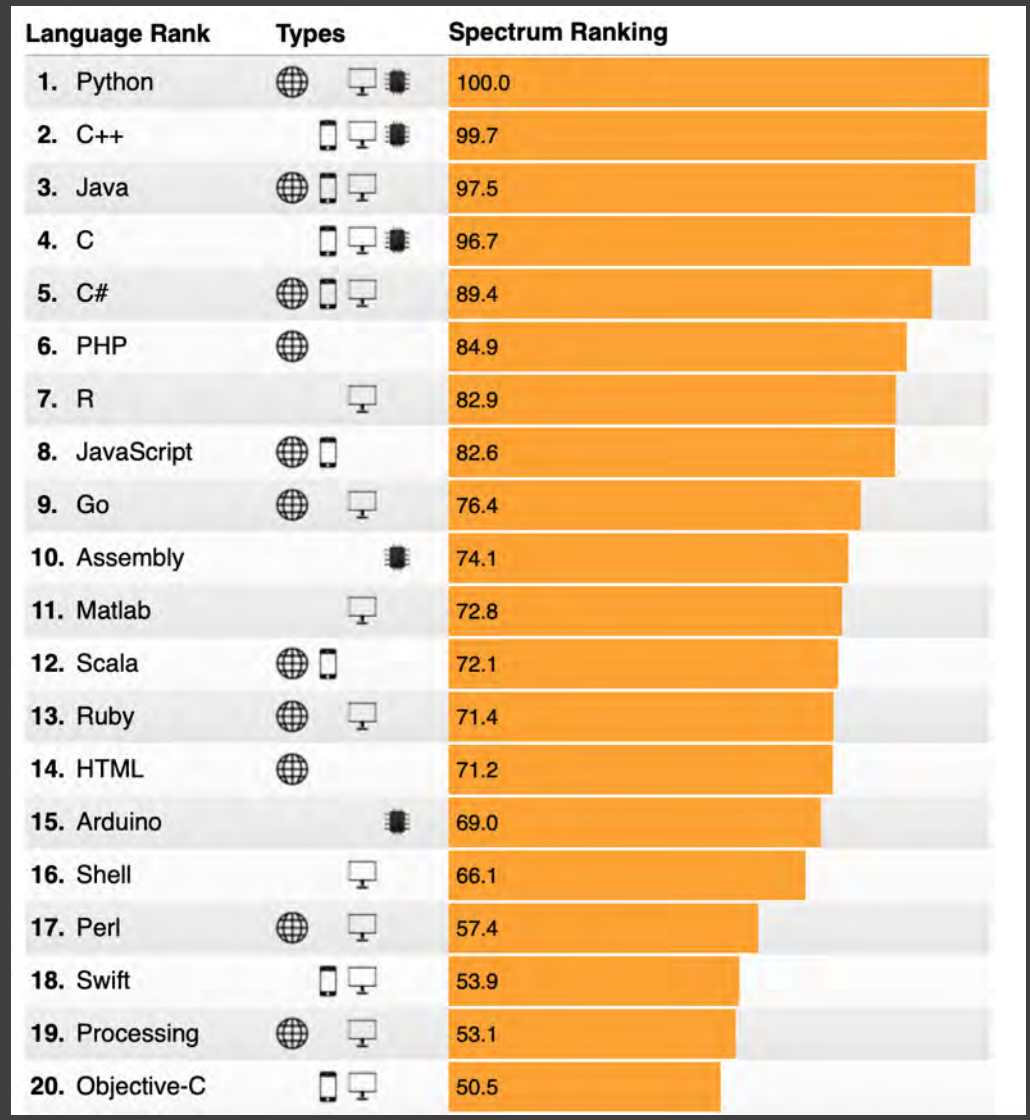
- OWASP SAMM 2.0 Overview

Application Security Challenges

- Software development experience is rare among information security professionals
- Application security programs focus too much on post deployment testing
- Evolving cloud technologies create new opportunities and risks
- Programs still focus too much on individual vulnerabilities

Evolution of Programming Languages

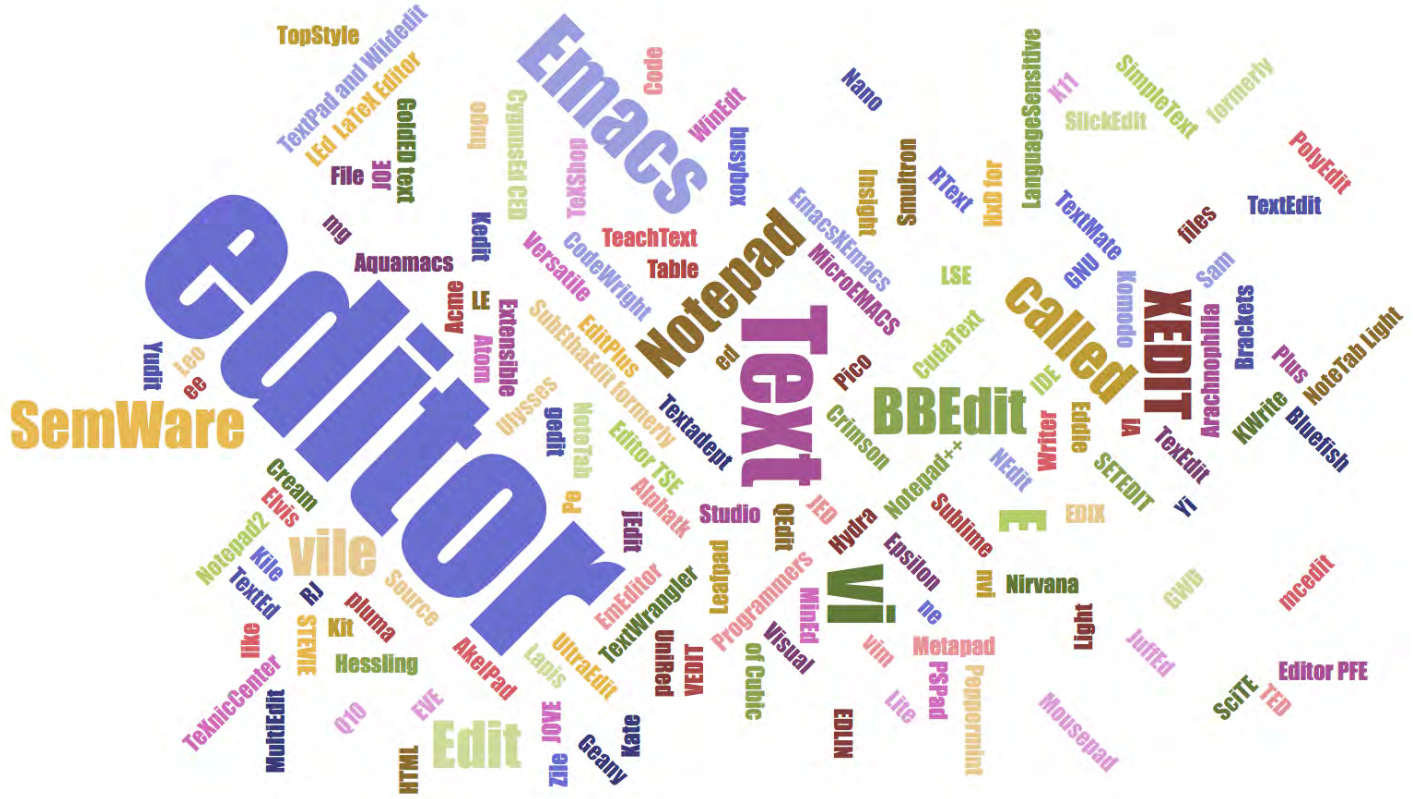
Why do we need so many?



Language Rank	Types	Spectrum Ranking
1. Python	Web, Desktop, Embedded	100.0
2. C++	Mobile, Desktop, Embedded	99.7
3. Java	Web, Mobile, Desktop	97.5
4. C	Mobile, Desktop, Embedded	96.7
5. C#	Web, Mobile, Desktop	89.4
6. PHP	Web	84.9
7. R	Desktop	82.9
8. JavaScript	Web, Mobile	82.6
9. Go	Web, Desktop	76.4
10. Assembly	Embedded	74.1
11. Matlab	Desktop	72.8
12. Scala	Web, Mobile	72.1
13. Ruby	Web, Desktop	71.4
14. HTML	Web	71.2
15. Arduino	Embedded	69.0
16. Shell	Desktop	66.1
17. Perl	Web, Desktop	57.4
18. Swift	Mobile, Desktop	53.9
19. Processing	Web, Desktop	53.1
20. Objective-C	Mobile, Desktop	50.5

What’s your favorite text editor?

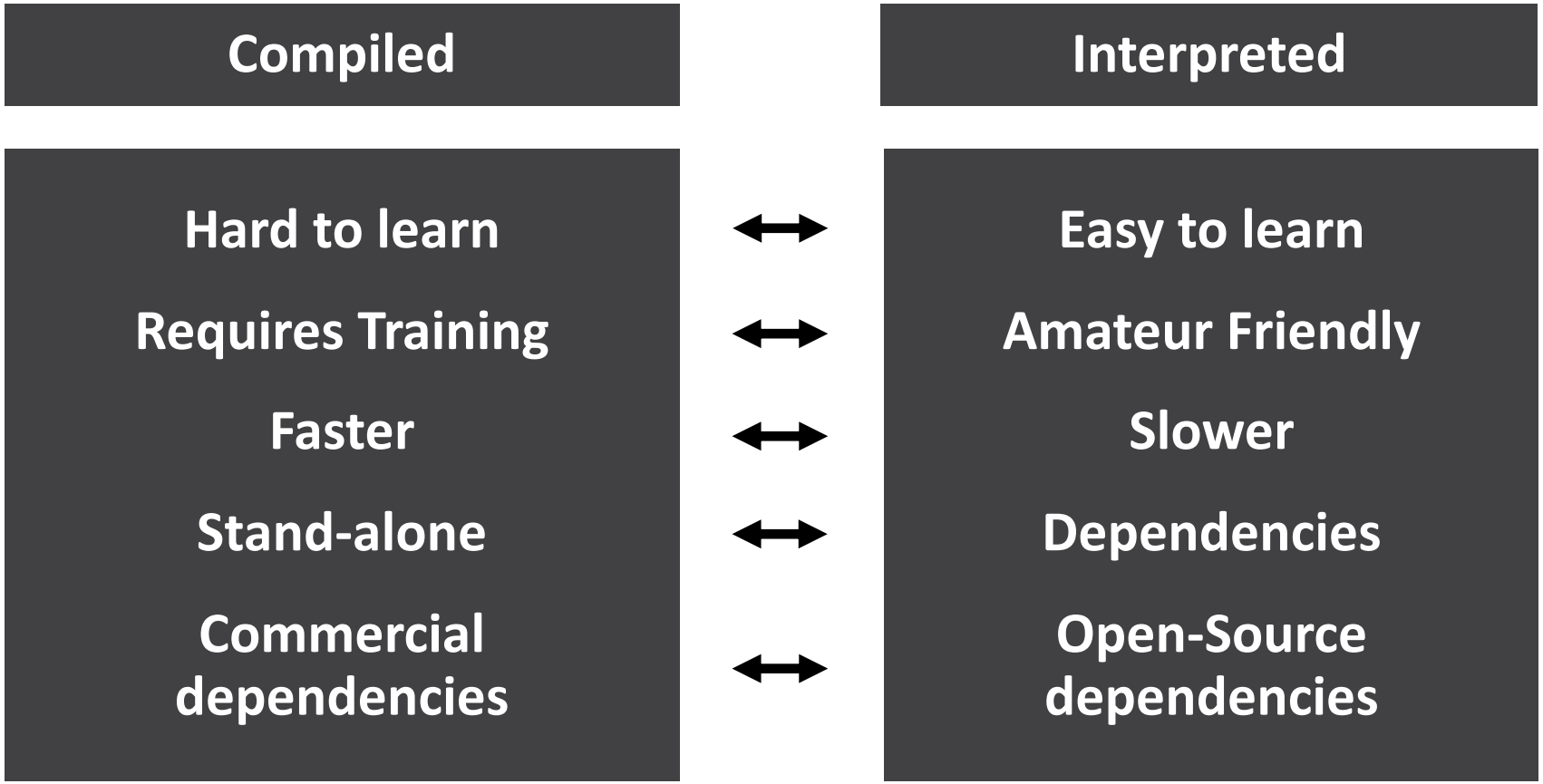
Go ahead… shout them out…



There are over 120…

Over 730 Programming Languages!!!

Interpreted vs. Compiled Languages



Interpreted Language Modules

- Subject to Open-Source Licensing
- Developed by enterprises, professional developers, and amateurs
- Software Supply-Chain is a new Threat Vector

How Many Modules Do We Need?

Repository	First Released	Total Count	Avg. Growth per Day
CPAN (Perl)	1987	39,908	3
PyPI (Python)	1991	179,176	131
Rubygems (Ruby)	1995	152,473	27
Maven Central (Java)	1995	280,028	124
Npm (node.js)	2009	818,768	560

Updated on 5/9/2019 from http://www.modulecounts.com/

Evolution of Computing Architecture

amazon web services™

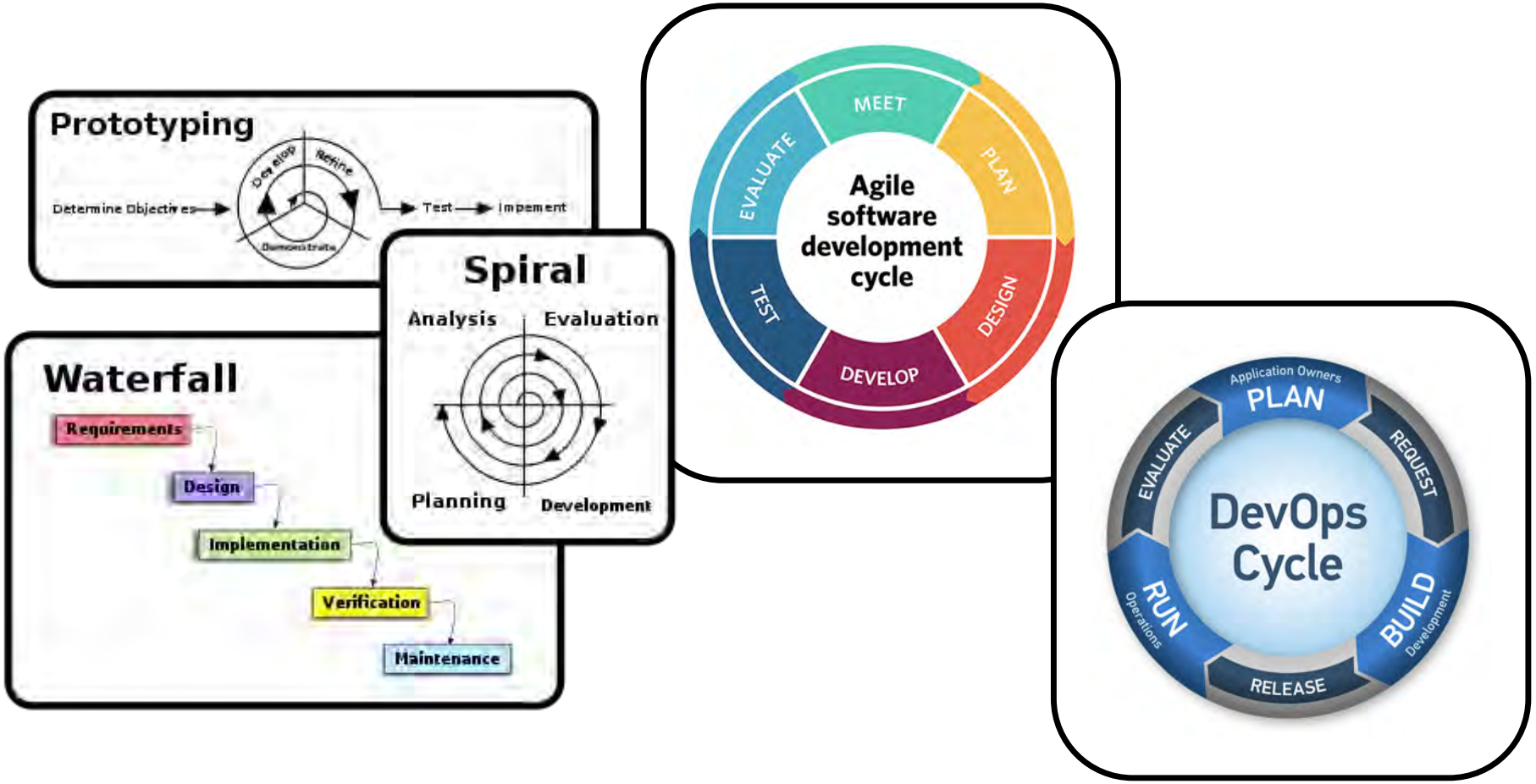
docker

kubernetes

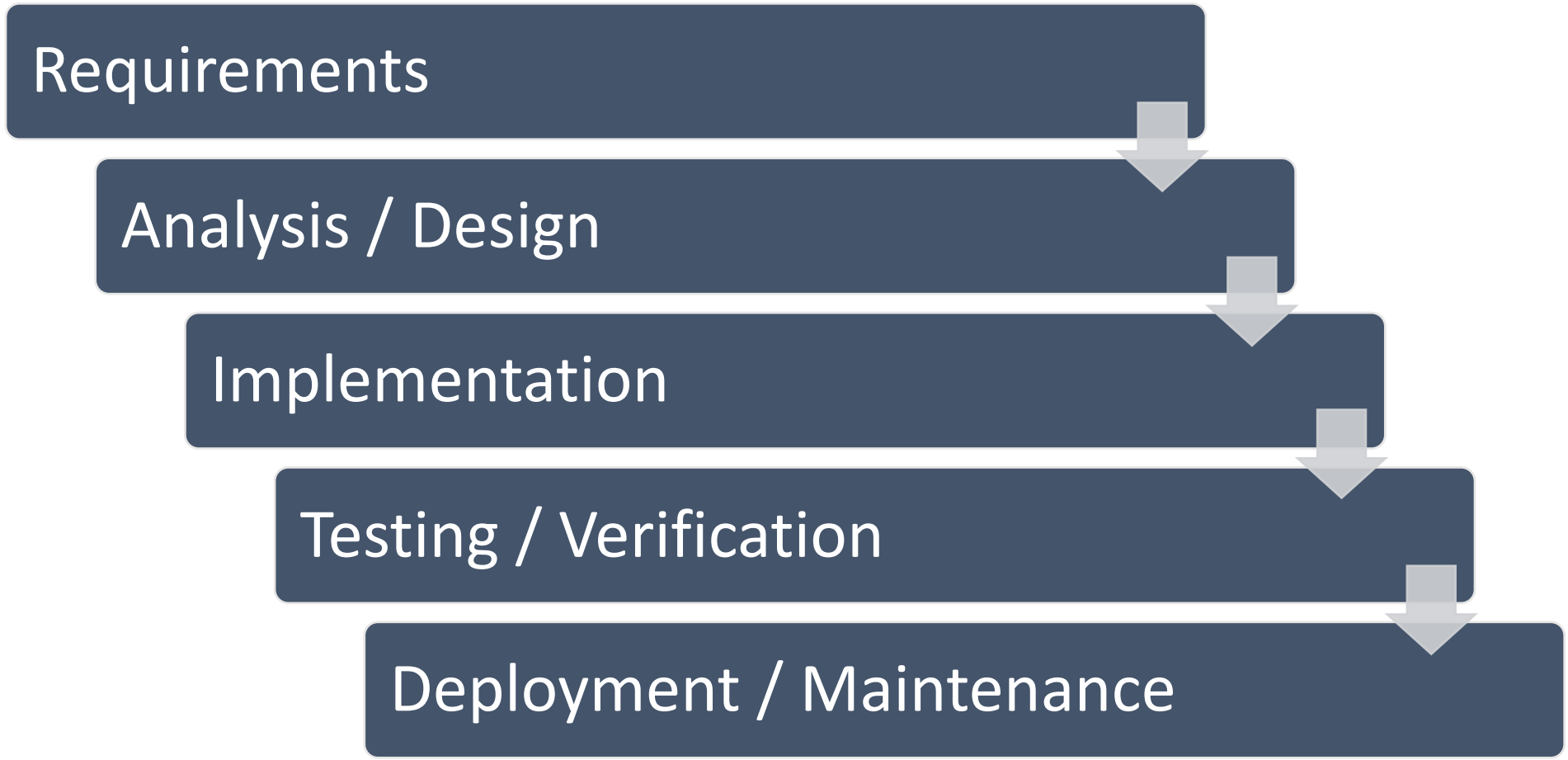
vmware

Microsoft Azure

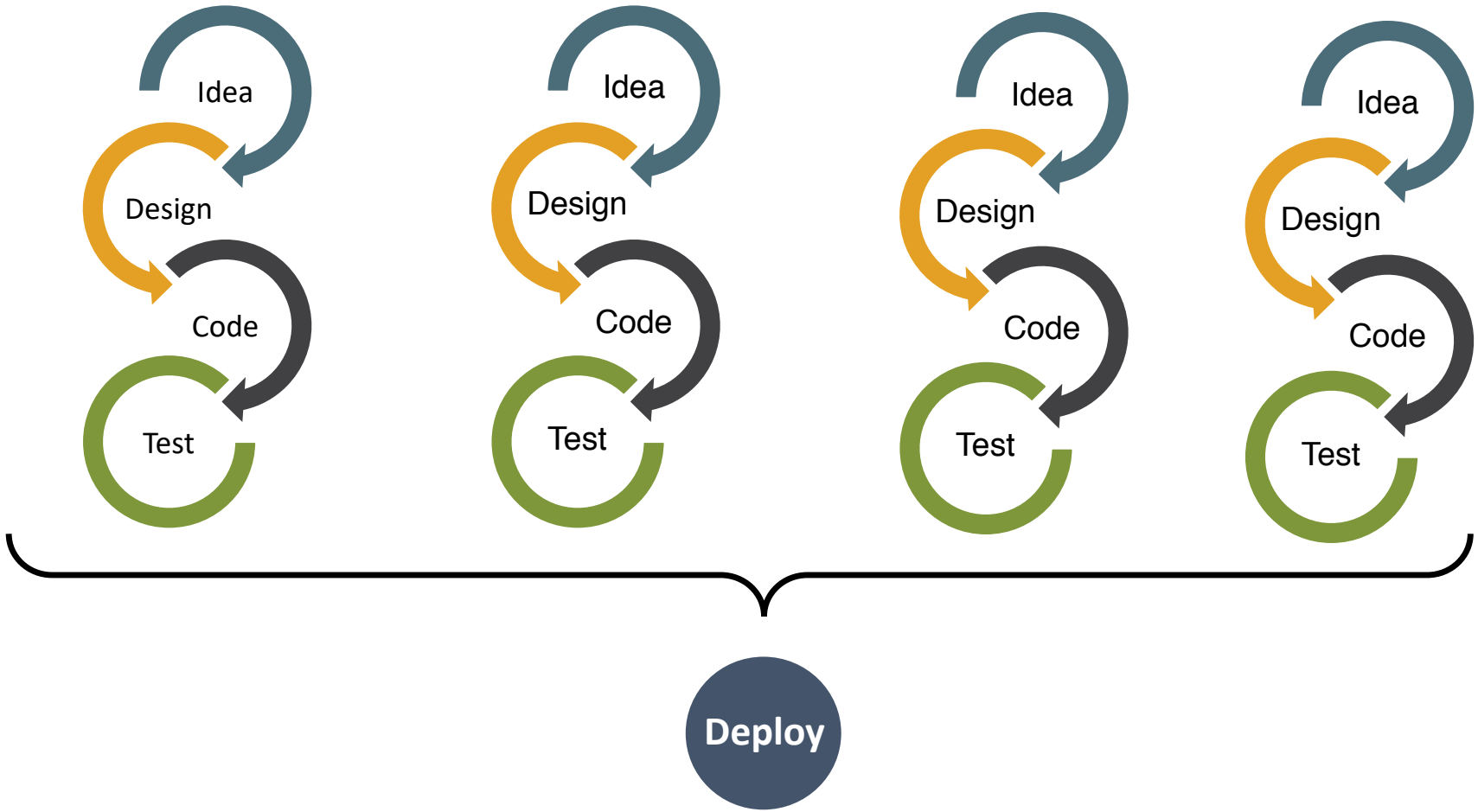
Evolution of Methodologies



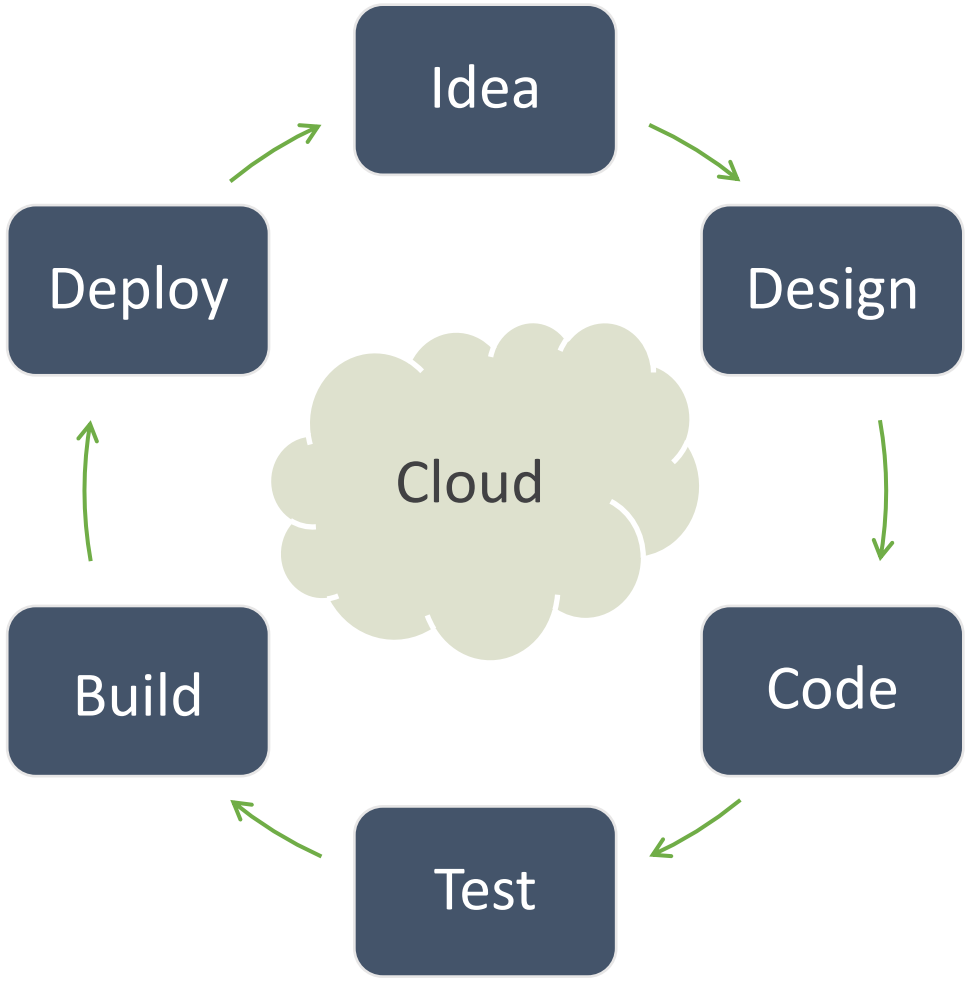
Waterfall


Requirements
Analysis / Design
Implementation
Testing / Verification
Deployment / Maintenance

Agile


Idea
Design
Code
Test
Idea
Design
Code
Test
Idea
Design
Code
Test
Idea
Design
Code
Test
Deploy

DevOps



How Different Are They?

Waterfall

Agile

DevOps

Open Security Summit

OPEN SECURITY SUMMIT

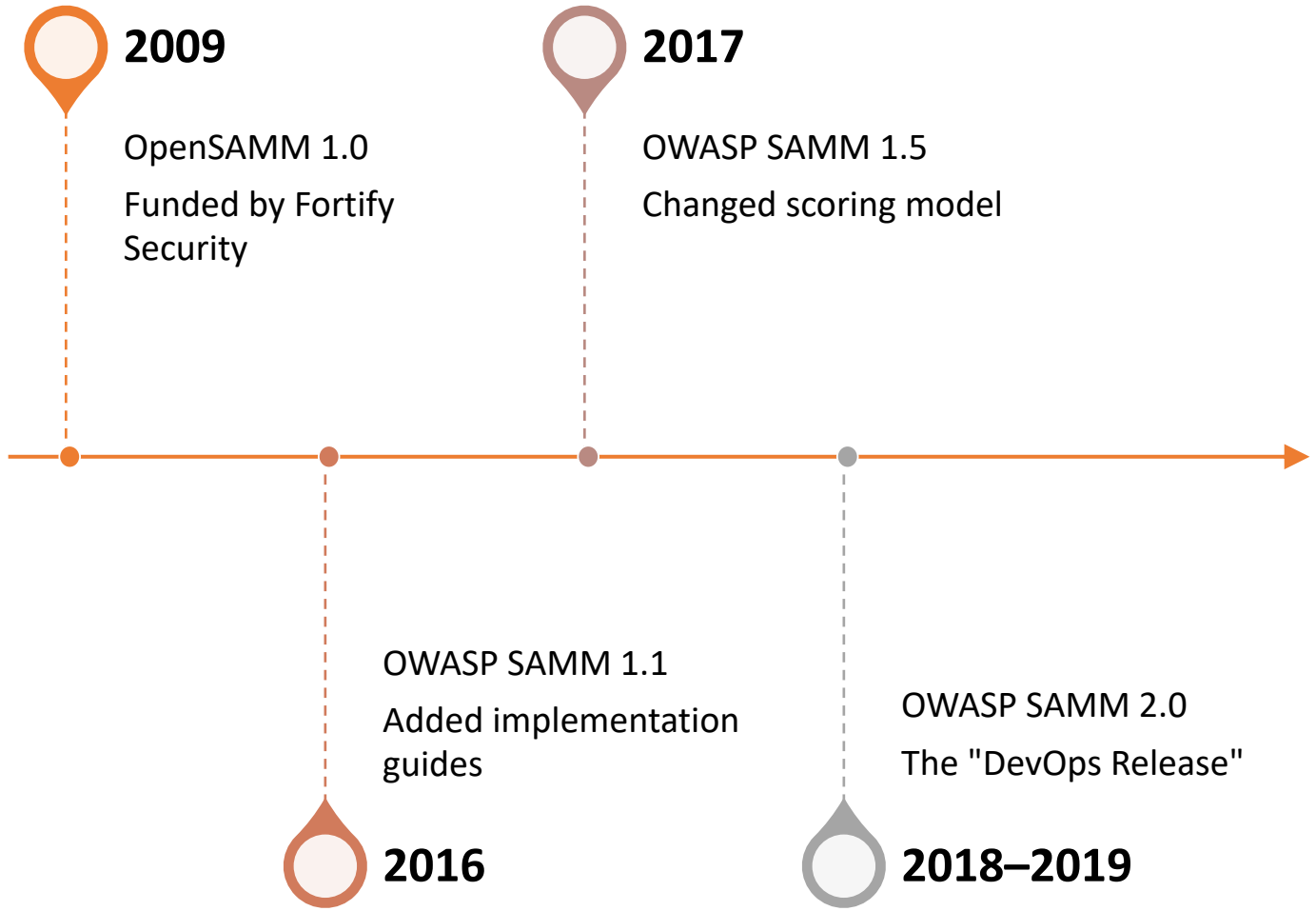
Supported by OWASP

What is OWASP SAMM?

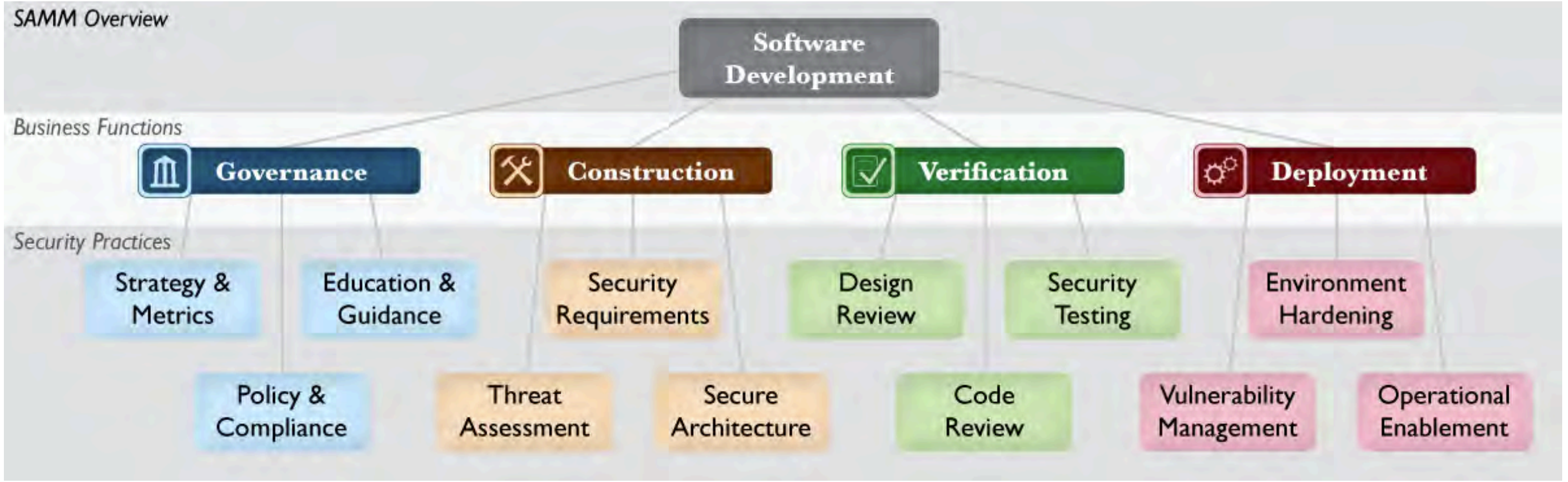
OWASP
Open Web Application Security Project

https://owaspsamm.org

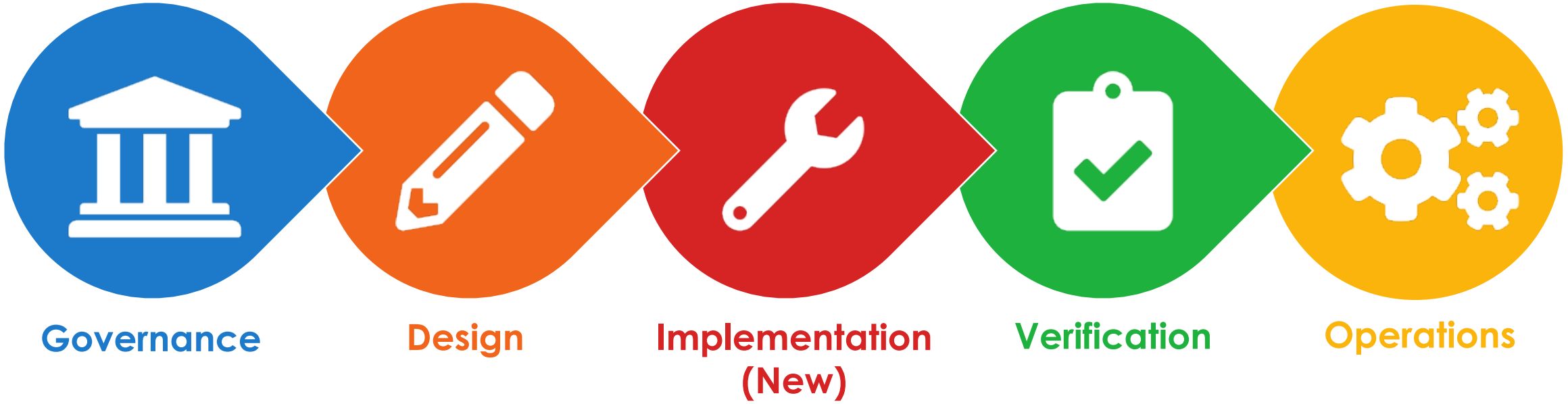
A Little OWASP SAMM History



OWASP SAMM 1.5 - Stable



SAMM 2.0 Structure



What is Shifting Left?

- Consider the actual workflow of a developer
- Studies by NIST and Ponemon Institute provide a clear ROI
- Better and more frequent testing improves quality of each release

SAMM 2.0 - Governance

Governance

Strategy & Metrics

- Create and Promote
- Measure and Improve

Policy & Compliance

- Policy and Standards
- Compliance Management

Education & Guidance

- Training and Awareness
- Organization and Culture

SAMM 2.0 - Governance

Start measuring something other than defect counts

Re-write policies and compliance requirements as test scripts or runbooks

Product Champions, not just Security Champions

SAMM 2.0 - Design

Design

Threat Assessment

- Application Risk Profile
- Threat Modeling

Security Requirements

- Software Requirements
- Supplier Security

Security Architecture

- Architecture Design
- Technology Management

SAMM 2.0 - Design

Build	• Build granular application risk profiles
Make	• Make requirements transparent and accessible
Develop and document	• Develop and document architectural standards

SAMM 2.0 - Implementation

Implementation

Secure Build

- Build Process
- Software Dependencies

Secure Deployment

- Deployment Process
- Secret Management

Defect Management

- Defect Tracking
- Metrics and Feedback / Learning

SAMM 2.0 - Implementation

Make sure all application security team members can build a simple CI/CD Pipeline *(https://www.owasp.org/index.php/OWASP_DevSecOps_Studio_Project)*

Improve defect tracking analytics to identify trends

SAMM 2.0 - Verification

Verification

Architecture Assessment

- Architecture Validation
- Architecture Compliance

Requirements Driven Testing

- Control Verification
- Misuse / Abuse Testing

Security Testing

- Scalable Baseline
- Deep Understanding

SAMM 2.0 - Verification

Whenever possible, automate architecture checks

Invest in tools to identify vulnerability as the code is written or committed

Balance automated and manual penetration testing for the most effective and efficient results

SAMM 2.0 - Operations

Operations

Incident Management

- Incident Detection
- Incident Response

Environment Management

- Configuration Hardening
- Patching and Updating

Operational Management

- Data Protection
- System Decommissioning / Legacy Management

SAMM 2.0 - Operations

Plan for security incidents one application at a time

Configuration hardening and patching may look different, but are still necessary

Review test data routines

The DevOps Release…

- CI/CD pipeline publishes changes in minutes
  - https://owaspsamm.org
- Developed and maintained in Markdown
  - https://github.com/OWASP/samm/tree/master/v2.0/beta/core
- We want your feedback!
  - https://github.com/OWASP/samm/issues

Questions / Discussion

Thank you!