ADDO

ALL DAY DEVOPS

NOVEMBER 6, 2019

Seba Deleersnyder

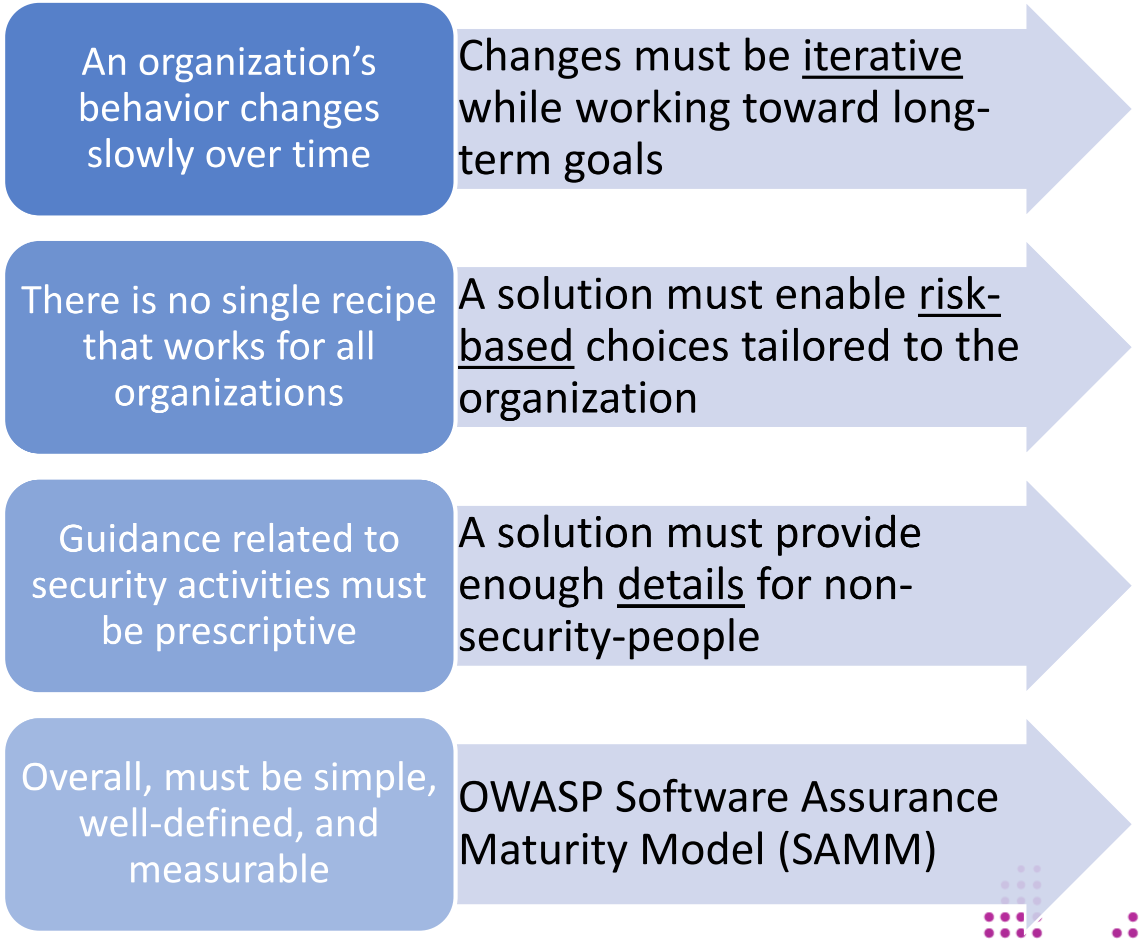
DevOps Assurance With OWASP SAMMv2

What is SAMM?

OWASP Software Assurance Maturity Model

"The prime maturity model for software assurance that provides an effective and measurable way for all types of organizations to analyze and improve their software security posture.”

Why a maturity model?



An organization's behavior changes slowly over time

Changes must be iterative while working toward long-term goals

There is no single recipe that works for all organizations

A solution must enable risk-based choices tailored to the organization

Guidance related to security activities must be prescriptive

A solution must provide enough details for non-security-people

Overall, must be simple, well-defined, and measurable

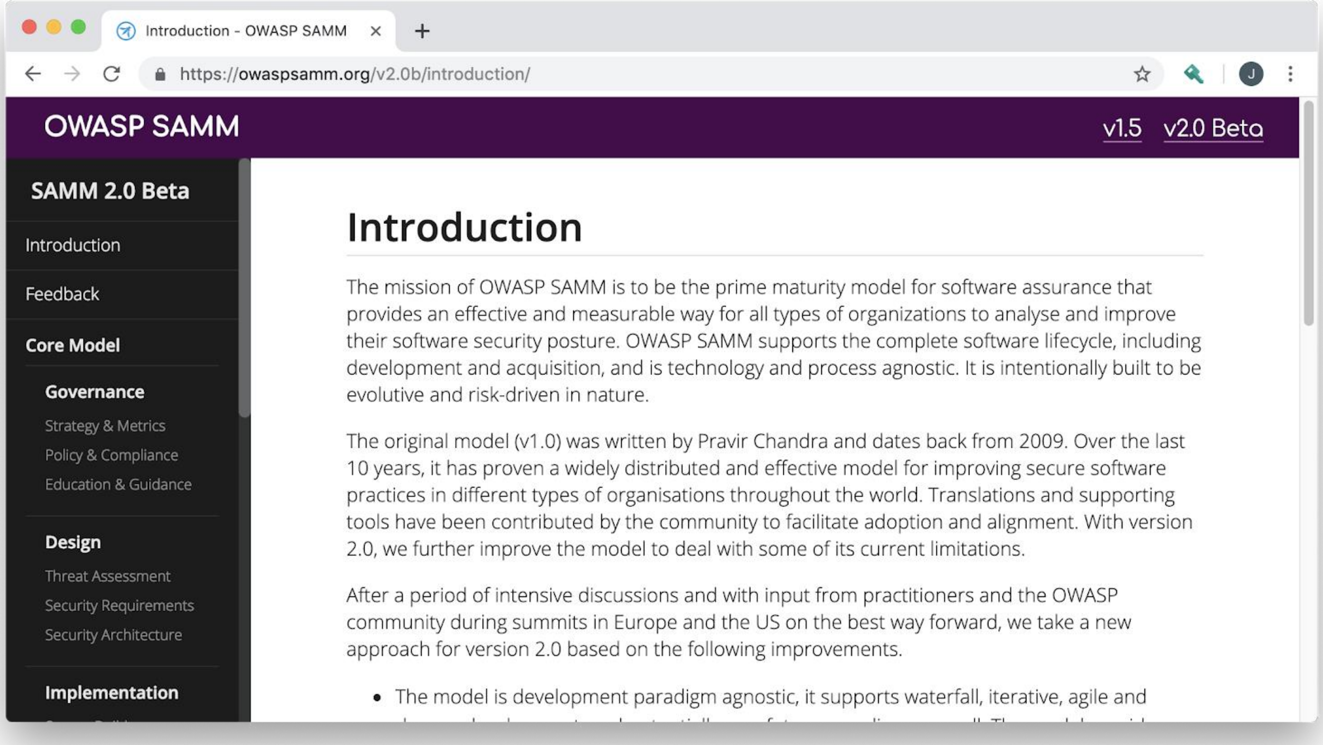
OWASP Software Assurance Maturity Model (SAMM)

Measurable

Actionable

Versatile

OWASP SAMM



Introduction

The mission of OWASP SAMM is to be the prime maturity model for software assurance that provides an effective and measurable way for all types of organizations to analyse and improve their software security posture. OWASP SAMM supports the complete software lifecycle, including development and acquisition, and is technology and process agnostic. It is intentionally built to be evolutive and risk-driven in nature.

The original model (v1.0) was written by Pravir Chandra and dates back from 2009. Over the last 10 years, it has proven a widely distributed and effective model for improving secure software practices in different types of organisations throughout the world. Translations and supporting tools have been contributed by the community to facilitate adoption and alignment. With version 2.0, we further improve the model to deal with some of its current limitations.

After a period of intensive discussions and with input from practitioners and the OWASP community during summits in Europe and the US on the best way forward, we take a new approach for version 2.0 based on the following improvements.

- The model is development paradigm agnostic, it supports waterfall, iterative, agile and

https://owaspsamm.org/

SAMM2 security practices

Governance	Design	Implementation	Verification	Operations
Strategy & Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Policy & Compliance	Security Requirements	Secure Deployment	Requirements Testing	Environment Management
Education & Guidance	Security Architecture	Defect Management	Security Testing	Operational Management

Defect Management

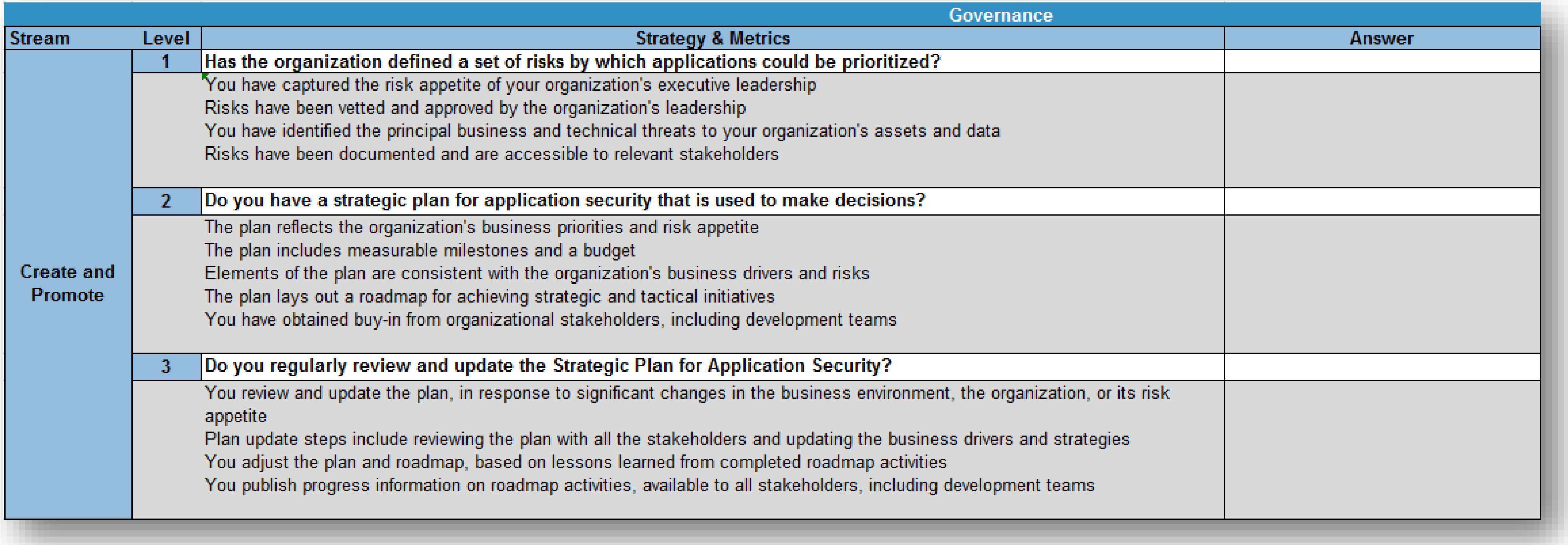
Streams

Maturity

Activities

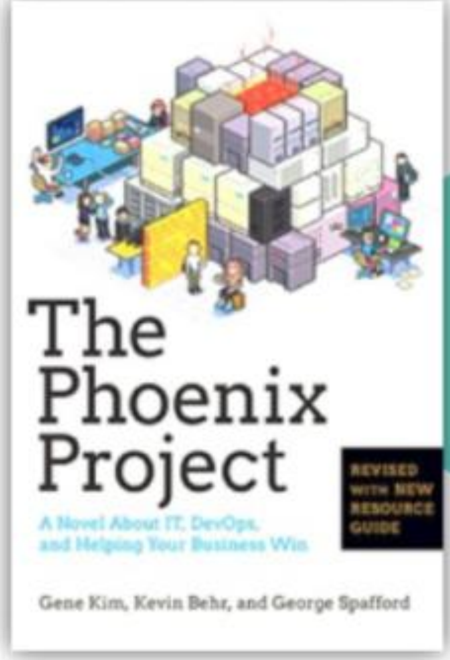
	A: Defect Tracking (Flaws/Bugs/Process)	B: Metrics and Feedback/Learning
Maturity 1 - All defects are **tracked** within each project	Track all defects	Calculate and share basic metrics, such as total counts
Maturity 2 - Defect tracking used to **influence** the deployment process	Agreed upon fix timings based on security rating of the defect	Calculate more advanced metrics that include new issue velocity, remediation speed metrics, and trends.
Maturity 3 - Defect tracking **across multiple components** is used to help reduce the number of new defects	Measure and enforce compliance with an SLA	Use trend analysis to influence changes in the Design and Implementation phase across multiple projects.

SAMM2 assessments

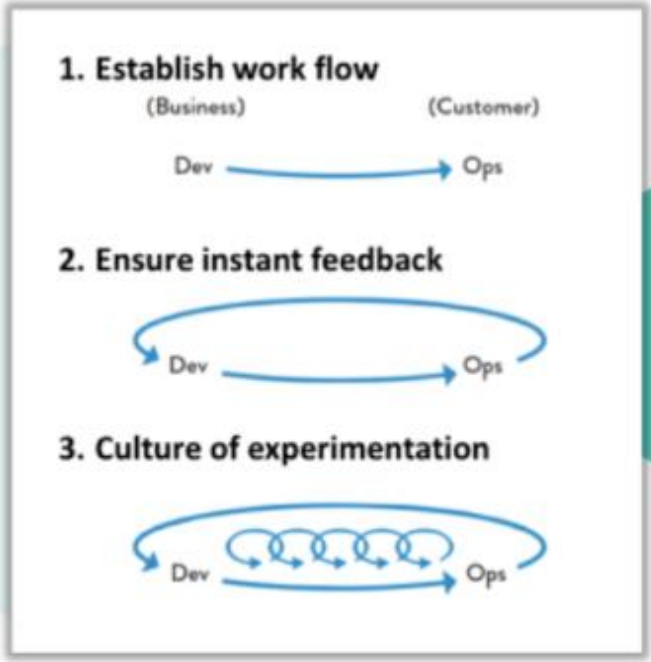


		Governance	
Stream	Level	Strategy & Metrics	Answer
Create and Promote	1	**Has the organization defined a set of risks by which applications could be prioritized?**	
		You have captured the risk appetite of your organization's executive leadership Risks have been vetted and approved by the organization's leadership You have identified the principal business and technical threats to your organization's assets and data Risks have been documented and are accessible to relevant stakeholders	
	2	**Do you have a strategic plan for application security that is used to make decisions?**	
		The plan reflects the organization's business priorities and risk appetite The plan includes measurable milestones and a budget Elements of the plan are consistent with the organization's business drivers and risks The plan lays out a roadmap for achieving strategic and tactical initiatives You have obtained buy-in from organizational stakeholders, including development teams	
	3	**Do you regularly review and update the Strategic Plan for Application Security?**	
		You review and update the plan, in response to significant changes in the business environment, the organization, or its risk appetite Plan update steps include reviewing the plan with all the stakeholders and updating the business drivers and strategies You adjust the plan and roadmap, based on lessons learned from completed roadmap activities You publish progress information on roadmap activities, available to all stakeholders, including development teams	

SAMM2 Toolbox:
https://github.com/OWASP/samm/tree/master/Supporting%20Resources/v2.0/toolbox


The Phoenix Project
A Novel About IT, DevOps, and Helping Your Business Win
REVISED WITH NEW RESOURCE GUIDE
Gene Kim, Kevin Behr, and George Spafford

DEVOPS


1. Establish work flow

(Business) (Customer)

Dev → Ops

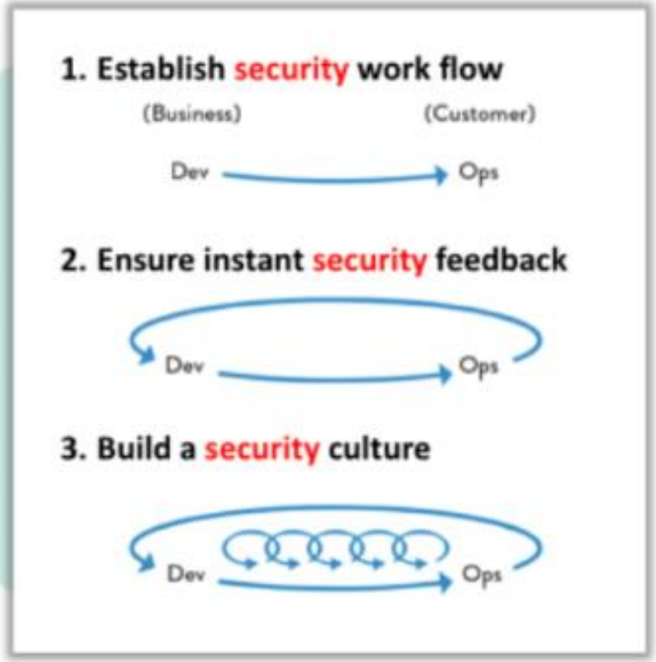
2. Ensure instant feedback

Dev → Ops

3. Culture of experimentation

Dev → Ops

DEVSECOPS


1. Establish security work flow

(Business) (Customer)

Dev → Ops

2. Ensure instant security feedback

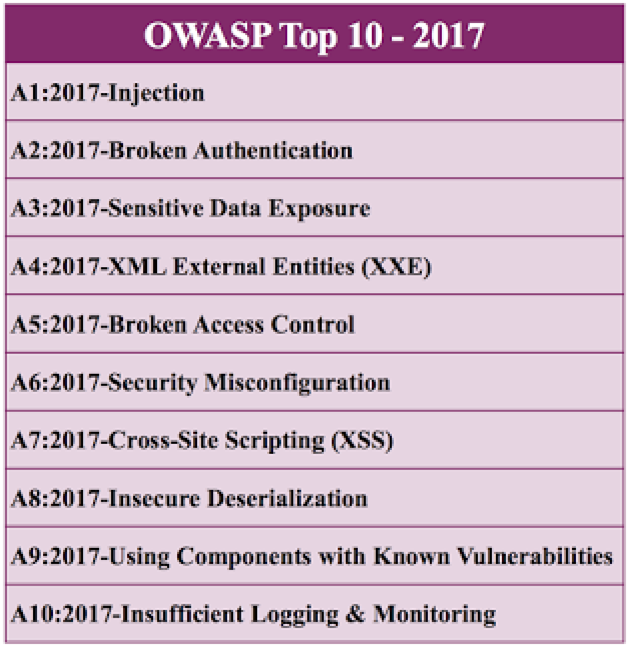
Dev → Ops

3. Build a security culture

Dev → Ops

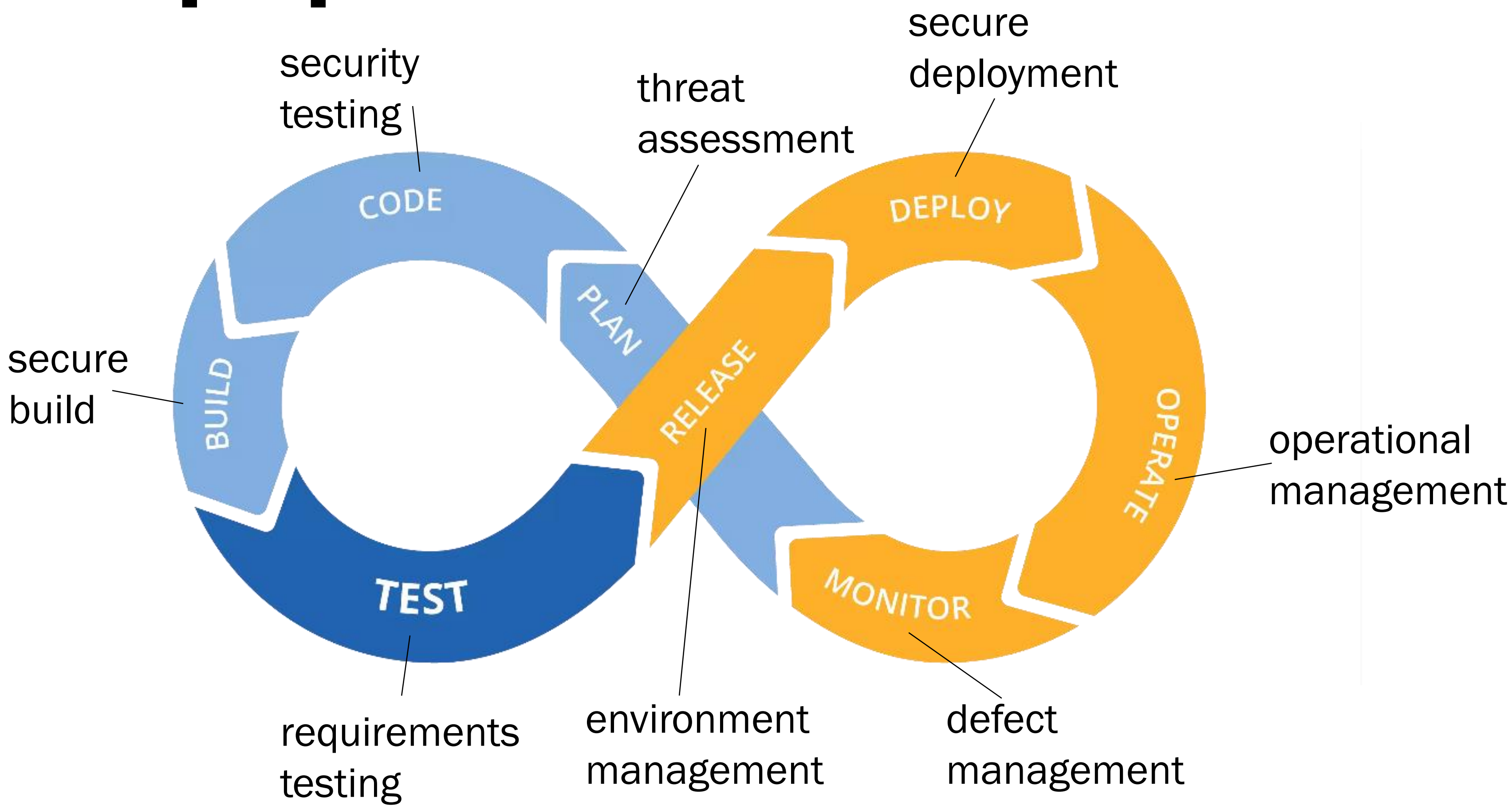
DevSecOps people

1. Awareness training
2. Security champions
3. Security culture

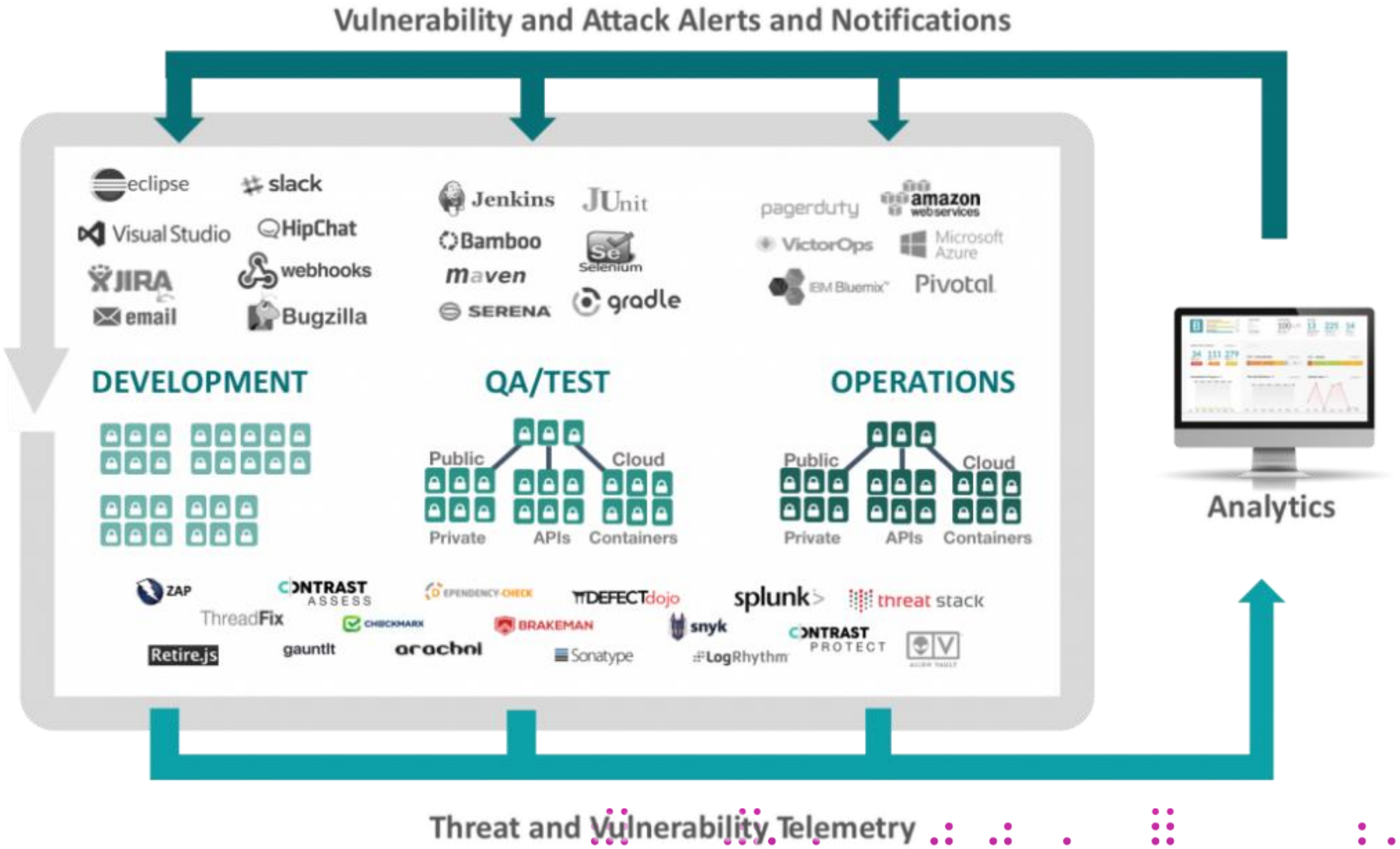


OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

DevSecOps process

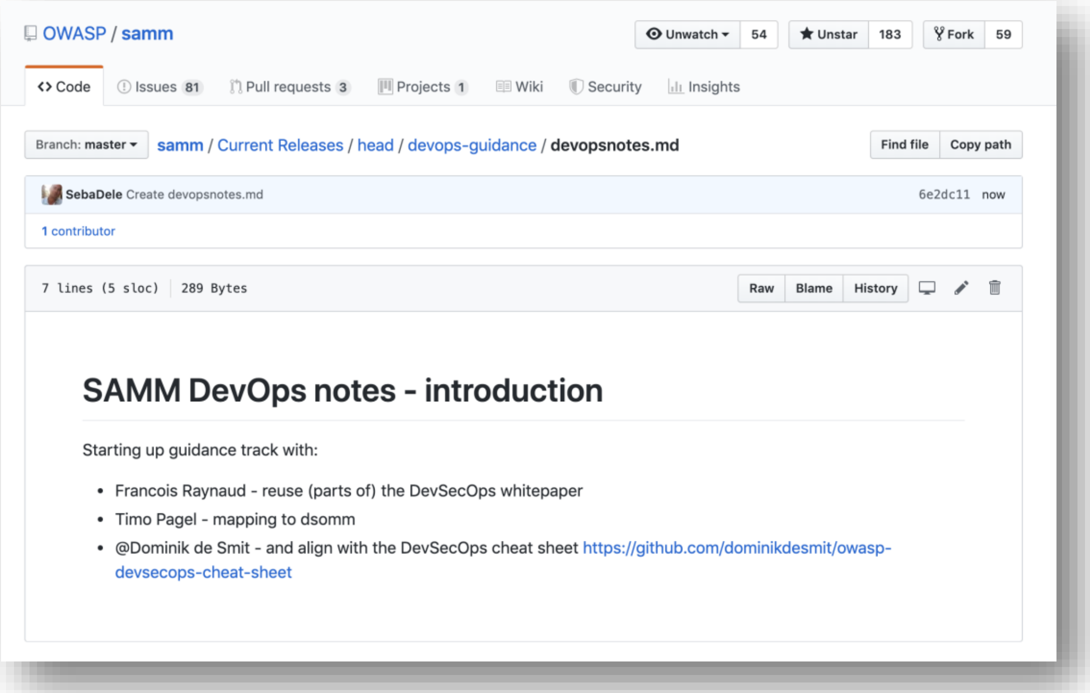


DevSecOps technology



SAMM DevOps guidance

- Extends SAMM model
- Collaborative
- Join this discussion?



SAMM DevOps notes - introduction

Starting up guidance track with:

- Francois Raynaud - reuse (parts of) the DevSecOps whitepaper
- Timo Pagel - mapping to dsomm
- @Dominik de Smit - and align with the DevSecOps cheat sheet https://github.com/dominikdesmit/owasp-devsecops-cheat-sheet

SAMM2 and beyond

- faster & iterative improvements
- community driven
- OWASP references
- process & technology guidance
- online assessments and roadmaps
- benchmark

Questions? Feedback? Input?

#project-samm

tinyurl.com/owaspslack

github.com/OWASP/samm

SAMM newsletter

mailchimp

eepurl.com/gl9fb9

Credits

Bart De Win – Project Co-Leader, Belgium
Sebastien (Seba) Deleersnyder – Project Co-Leader, Belgium
Brian Glass – United States
Daniel Kefer – Germany
Yan Kravchenko – United States
Chris Cooper – United Kingdom
John DiLeo – New Zealand
Nessim Kisserli – Belgium
Patricia Duarte - Uruguay
John Kennedy - Sweden
Hardik Parekh - United States
John Ellingsworth - United States
Sebastian Arriada - Argentina
Brett Crawley – United Kingdom
...

SAMM Sponsors

MICRO FOCUS
Fortify
CONCORD
nccgroup
splunk>

support SAMM: info@owaspsamm.org

Seba Deleersnyder

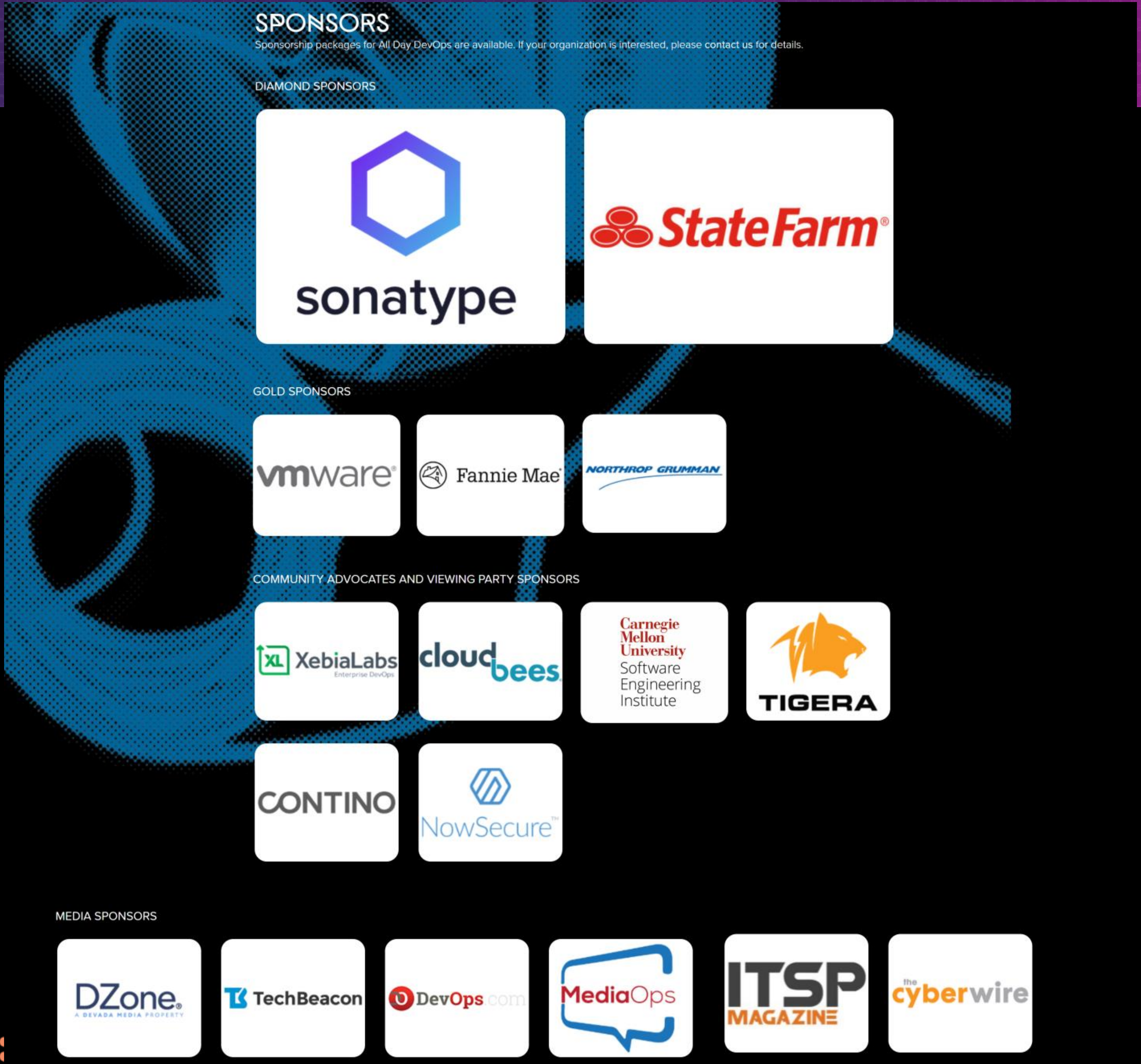
CEO Toreon

Belgian OWASP chapter founder

SAMM project co-leader

seba@toreon.com
seba@owasp.org
@sebadele

ADDO
ALL DAY DEVOPS



SPONSORS

Sponsorship packages for All Day DevOps are available. If your organization is interested, please contact us for details.

DIAMOND SPONSORS

sonatype

State Farm®

GOLD SPONSORS

vmware®

Fannie Mae

NORTHROP GRUMMAN

COMMUNITY ADVOCATES AND VIEWING PARTY SPONSORS

XL XebiaLabs Enterprise DevOps

cloudbees

Carnegie Mellon University Software Engineering Institute

TIGERA

CONTINO

NowSecure™

MEDIA SPONSORS

DZone. A DEVADA MEDIA PROPERTY

TechBeacon

DevOps.com

MediaOps

ITSP MAGAZINE

the cyberwire