OWASP SAMM2 – Your Dynamic Software Security Journey

Bart De Win
bart.dewin@owasp.org

Sebastien Deleersnyder
seba@owasp.org

Bart?

Bart De Win, Ph.D.

- 20+ years experience in software security
- Belgian OWASP chapter co-leader
- OWASP SAMM co-leader and evangelist
- Author of >60 publications
- Director & security consultant @PwC BE
- Bart.de.win@pwc.com

pwc

OWASP
Open Web Application Security Project

What is SAMM?

FLAGSHIP mature projects

"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."

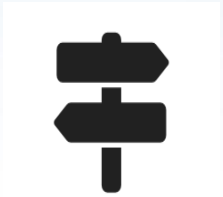
OWASP Open Web Application Security Project

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

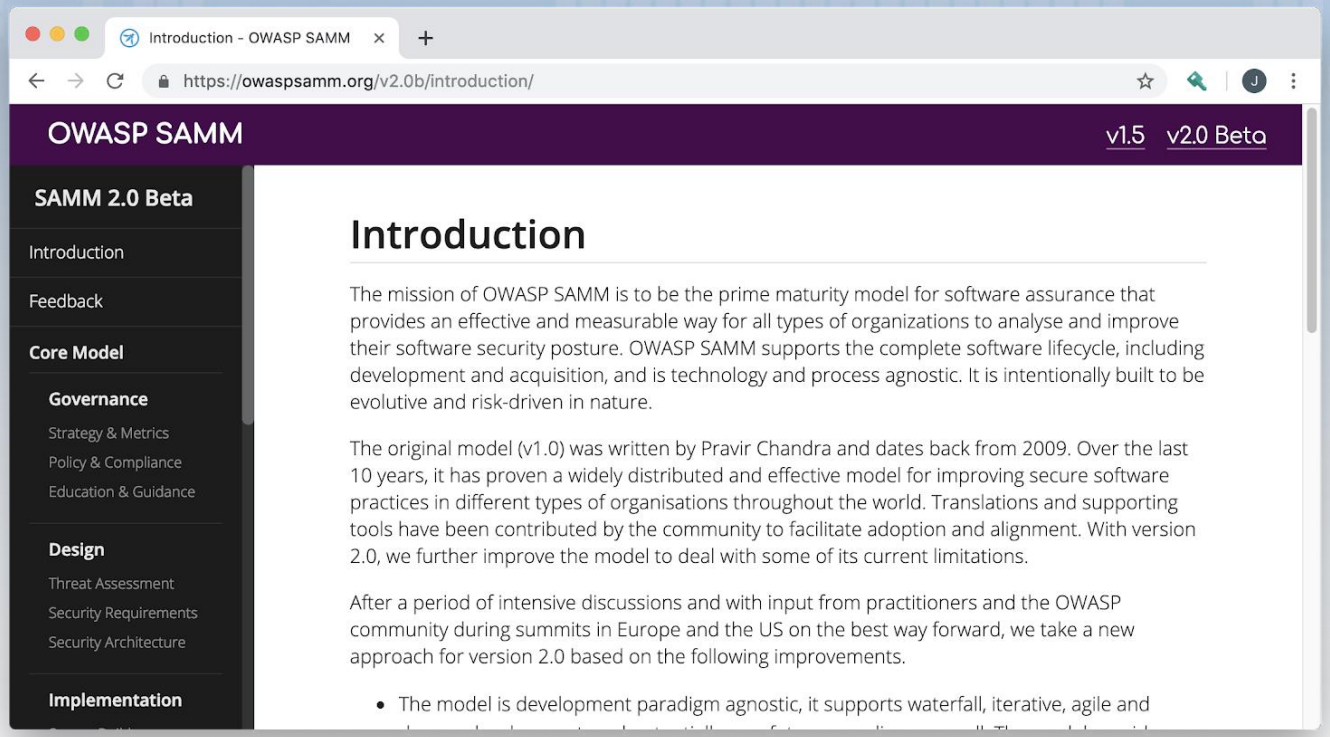
Actionable



Versatile

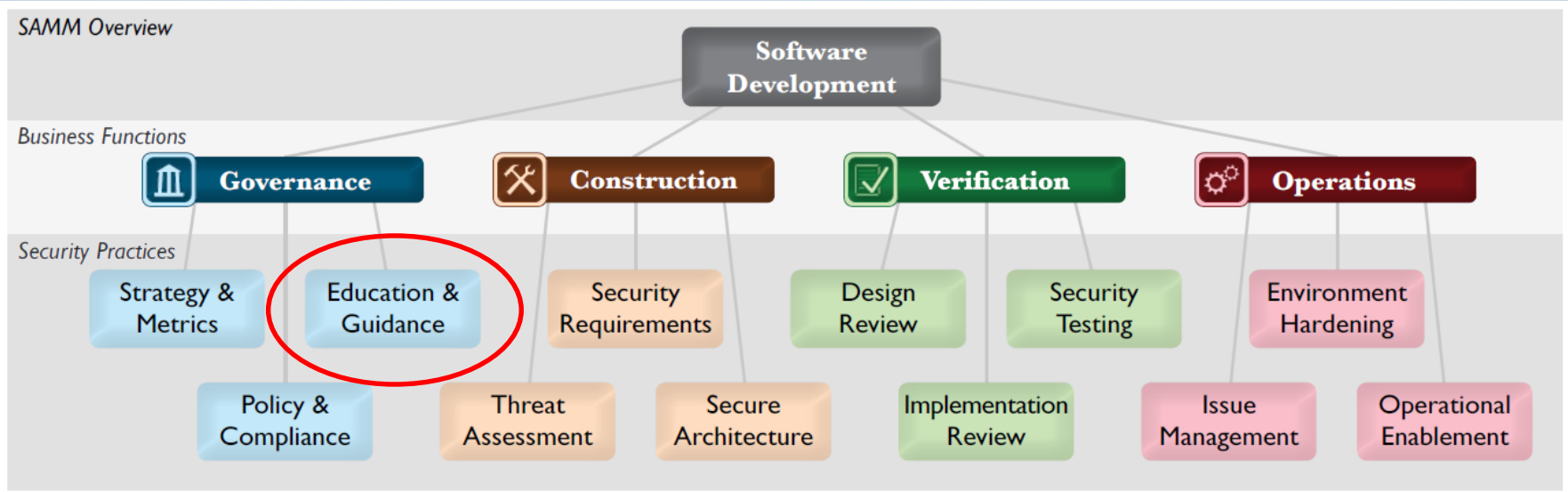
OWASP
Open Web Application Security Project

OWASP SAMM



https://owaspsamm.org/

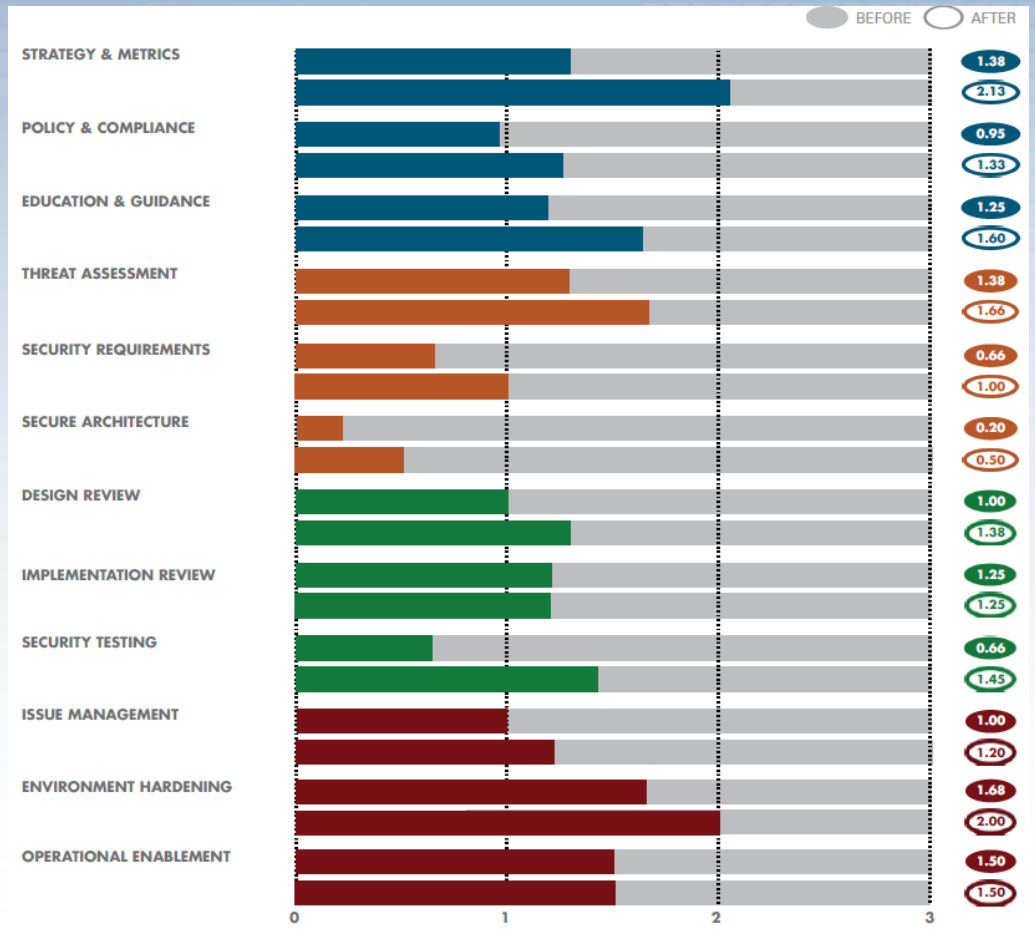
Core structure

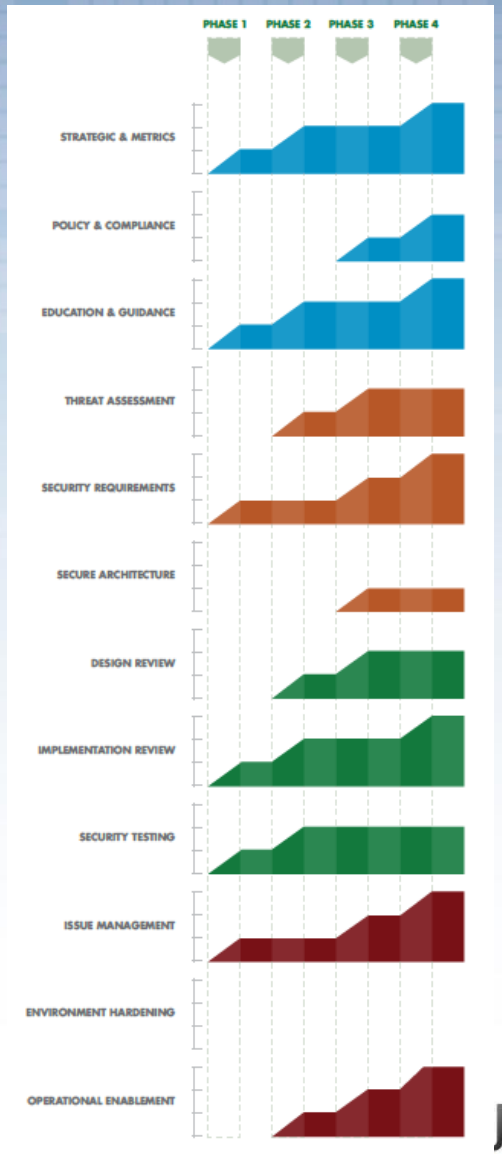


Assessments

Education & Guidance	Score	0.0	0.2	0.5	1.0	
✦Have developers been given high-level security awareness training?		No	Once	Every 2-3 yrs	Annually	
✦Does each project team understand where to find secure development best-practices and guidance?		No	Some	Half	Most	EG 1
✦Are those involved in the development process given role-specific security training and guidance?		No	Some	Half	Most	
✦Are stakeholders able to pull in security coaches for use on projects?		No	Some	Half	Most	EG 2
✦Is security-related guidance centrally controlled and consistently distributed throughout the organization?		No	Per Team	Org Wide	Integrated Process	
✦Are developers tested to ensure a baseline skill-set for secure development practices?		No	Once	Every 2-3 yrs	Annually	EG 3

SAMM output





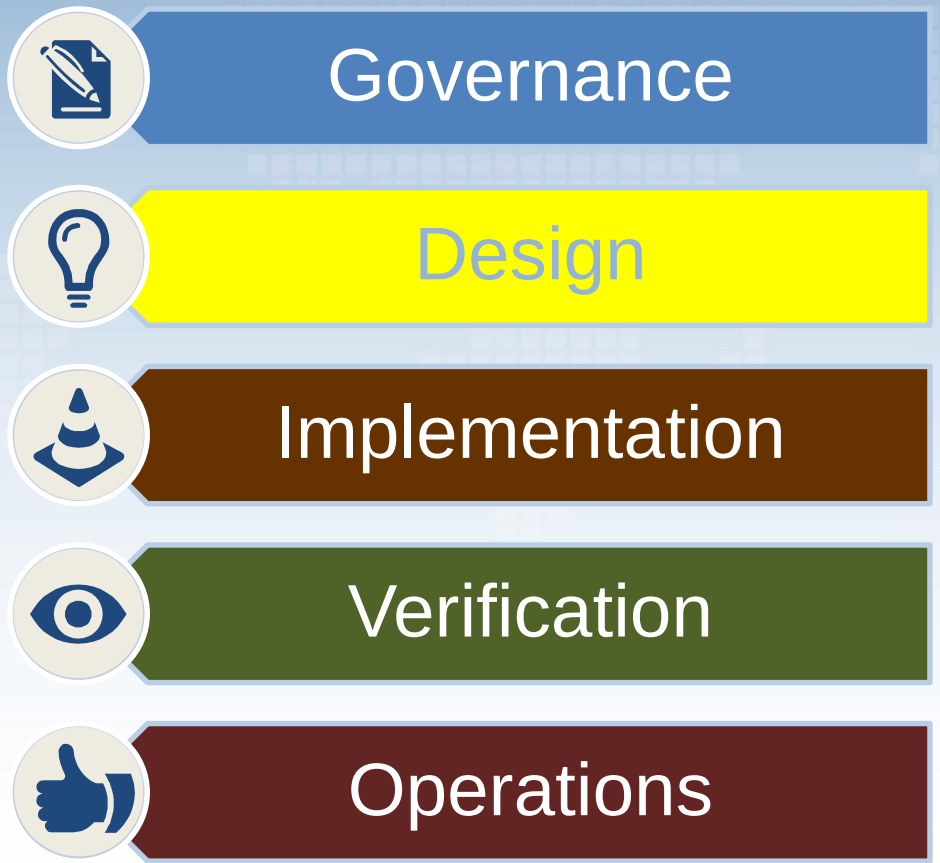
JASP
Open Web Application Security Project

Why a new version?

- ✓Align with recent development practices
- ✓“Orphaned” activities
- ✓Method agnostic
- ✓Improve assessments
- ✓Improve production process

Backwards compatibility was not a goal

SAMM2 business functions

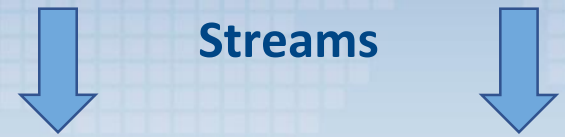


SAMM2 security practices

- Still 3 Security Practices per Business Function

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

SAMM2 security practice structure



Maturity

	A: Control Verification	B: Misuse/Abuse Testing
Level 1 *- Opportunistically find basic vulnerabilities and other security issues.*	Test for standard security controls	Perform security fuzzing testing
Level 2 *- Perform implementation review to discover application-specific risks against the security requirements.*	Derive test cases from known security requirements	Create and test abuse cases and business logic flaw test
Level 3 *- Maintain the application security level after bug fixes, changes or during maintenance*	Perform regression testing (with security unit tests)	Denial of service and security stress testing

Activities

SAMM2 framework overview

Governance		
Strategy & Metrics	Create and Promote	Measure and Improve
Policy & Compliance	Policy and Standards	Compliance Management
Education & Guidance	Training and Awareness	Organization and Culture
Design		
Threat Assessment	Application Risk Profile	Threat Modeling
Security Requirements	Software Requirements	Supplier Security
Secure Architecture	Architecture Design	Technology Management
Implementation		
Secure Build	Build Process	Software Dependencies
Secure Deployment	Deployment Process	Secret Management
Defect Management	Defect Tracking (Flaws/Bugs/Process)	Metrics and Feedback/Learning
Verification		
Architecture Assessment	Architecture Validation	Architecture Compliance
Requirements Testing	Control Verification	Misuse/Abuse Testing
Security Testing	Scalable Baseline	Deep Understanding
Operations		
Incident Management	Incident Detection	Incident Response
Environment Management	Configuration Hardening	Patching and Updating
Operational Management	Data Protection	System decommissioning / Legacy management

Scoring in SAMM v1.5

Strategy & Metrics, Level 1: *Is there a software security assurance program in place?*

Available Responses:

- *No*
- *Yes, it's less than a year old*
- *Yes, it's a number of years old*
- *Yes, it's a pretty mature program*

But, what about…

- Quality of the program?
- Freshness of the program? Has it been reviewed/updated?
- How do you know the program is still relevant?

Multiple dimensions to consider

SAMM2:
Questions

SAMM2:
Quality criteria (mandatory)

OWASP Open Web Application Security Project

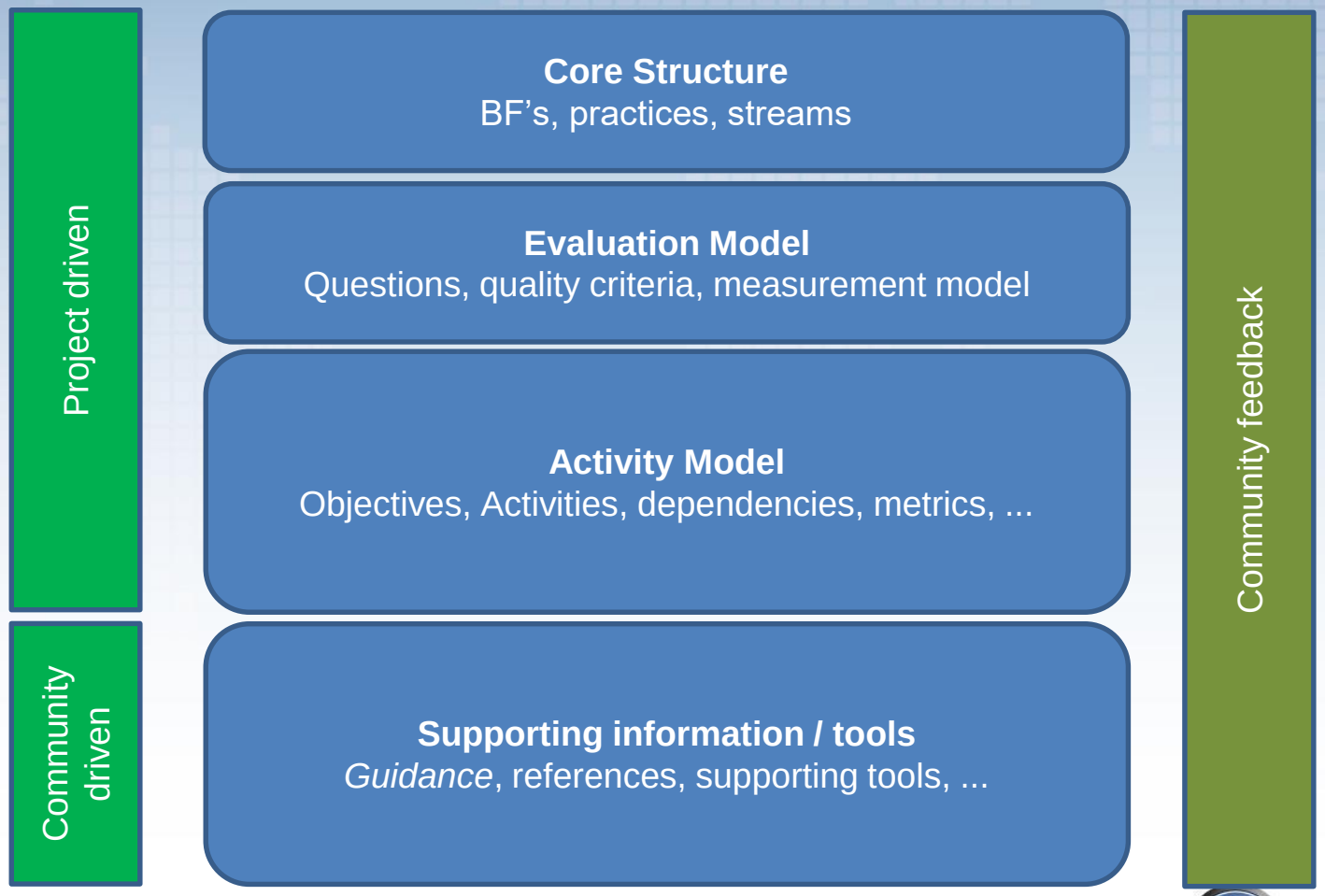
SAMM2 assessments

		Governance	
Stream	**Level**	**Strategy & Metrics**	**Answer**
Create and Promote	1	**Has the organization defined a set of risks by which applications could be prioritized?**	**Yes, covers most significant risks**
		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?**	**Yes, we consult the plan before making significant 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,Äôs 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?**	**Yes, but review is ad-hoc**
		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	

Project: new way of working

- Single source of the truth (Github)
- Used to generate everything *automatically*
  - Document, website
  - Toolbox
  - Applications

Community involvement



How do I compare to?

BusinessWire
A Berkshire Hathaway Company

HOME SERVICES NEWS EDUCATION ABOUT US Search

OpenSAMM Consortium Launches Industry's First Public Benchmarking Data for Improving Software Security

Pragmatic, Open Assessment Process Improves Usability by Enabling Organizations to Parse Data by Industry and Company Size

April 15, 2015 12:15 PM Eastern Daylight Time

SAN ANTONIO--(BUSINESS WIRE)--The Open Software Assurance Maturity Model (OpenSAMM) consortium today announced the industry's first publicly available, anonymized software security benchmarking data that enables organizations to steadily improve their software security posture over time. OpenSAMM is an easy-to-use assessment which provides flexible datasets that can be customized by organization demographics, including sector, development and cultural profile, resulting in pragmatic milestones towards reducing overall security risk.

The expanded access to these datasets makes OpenSAMM available to a larger number of organizations, which previously weren't able to apply valuable benchmarking data to their particular case. Each of the practical, constructive benchmarks within the framework was derived from best practices of leading application security firms. Contributing members of the consortium include Aspect Security, AsTech Consulting, Denim Group, Gotham Digital Science, Security Innovation and Veracode.

"It's critical to have an open framework where people can go to assess data and begin to benchmark their application security practices. Understanding that OpenSAMM was game changing for our industry, we recognized the need for it to be enhanced given the state of today's threat landscape."

As organizations of all sizes and across every industry increasingly rely on web, mobile and cloud applications as a source of strategic differentiation and competitive advantage, the threat surface has dramatically expanded. According to the Verizon DBIR, web applications have become the number one target for cyberattackers, with application-

OWASP
Open Web Application Security Project

Current roadmap

V2.0: end of 2019

2020:

- v2.1, 2.2, ...: iterative releases
- Agile/devops guidance
- Roadshows/trainings

Looking forward

- Online assessments, integrated with benchmark data
- User community contributions
- Support for regulations
- User events
- …

Try it !

Credits

- Sebastien (Seba) Deleersnyder – Project Co-Leader, Belgium
- Bart De Win – 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 - Bolivia
- John Kennedy - Sweden
- Hardik Parekh - United States
- John Ellingsworth - United States
- Sebastian Arriada - Brasil
- Brett Crawley – United Kingdom

https://owaspsamm.org/sponsors/

News / Become involved

Website (https://owaspsamm.org/)

Slack (OWASP - #project-samm)

Newsletter

Mailinglist (info@owaspsamm.org)

Github (https://github.com/OWASP/samm/)

Questions or Feedback ?