OWASP
Open Web Application
Security Project

OWASP SAMM

OWASP SAMM

Benchmarking Update

November 2023

Brian Glas

Introductions

Assistant Professor of Computer Science &
Department Chair at Union University

Co-Lead of OWASP Top Ten, OWASP SAMM Benchmark, and OWASP Data Analysis, Visualization, and Ingestion Domain (DAVID)

Benchmark Initiative

Trust is key

GUIDANCE

- Competence of the practitioners
- Quality and completeness of the data

INSIGHT

- Anonymization of the data
- Reporting and analysis of the results

Benchmarking

“How important is it for your organization to compare against peers?”

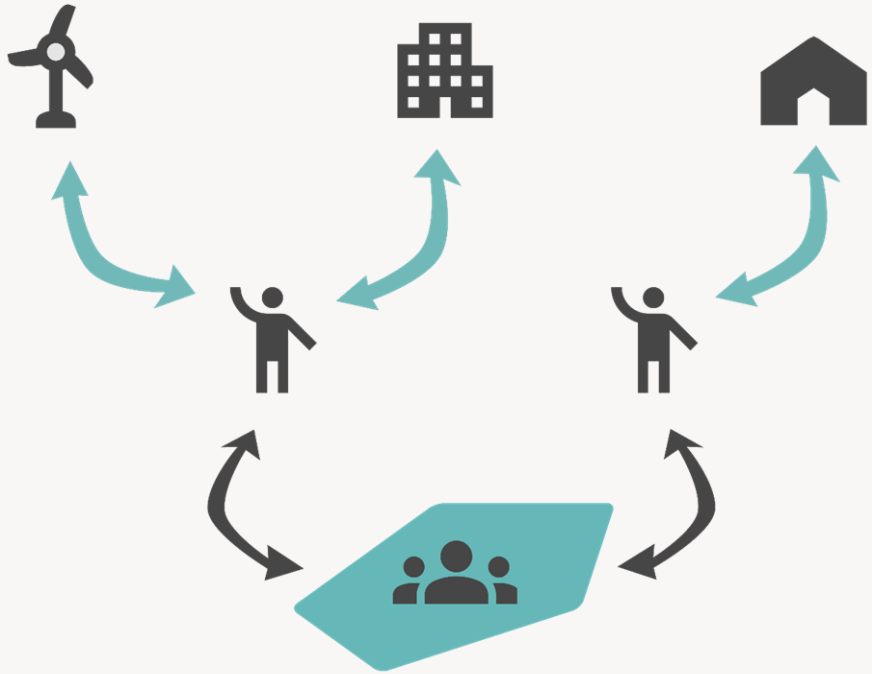
69% answered 7/10 or higher

Answers from the SAMM 2022 Questionnaire

Most frequent question we receive is about benchmarking

SAMM core team’s number 1 priority

SAMM Benchmark Roles



Industries - clients

Practitioners

Collect (& anonymize) data
Consume research

SAMM Team

Guard data
Keep DB
Do research

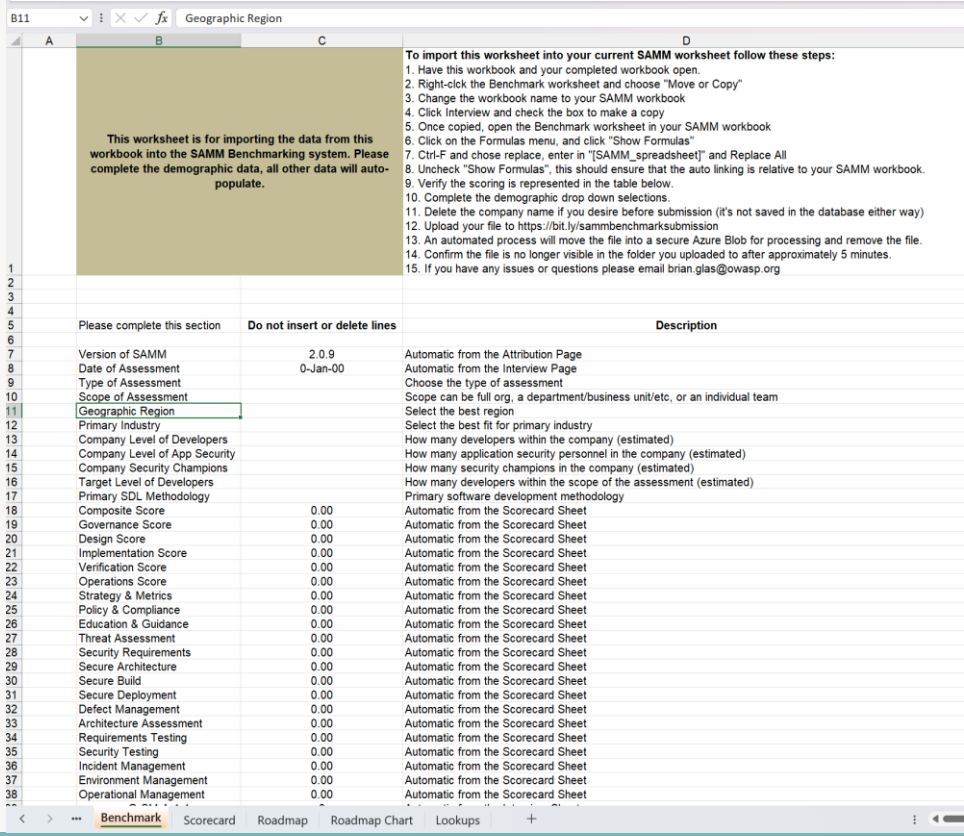
Expectations - Practitioner (Phase I)

SAMM Toolkit is updated
- Benchmark worksheet
- Organizes the data for upload

Submission link goes to OneDrive
https://bit.ly/sammbenchmarkingsubmissions

Consumed within minutes into Azure Data Factory for processing

Tableau Public Visualizations



B11 | Geographic Region

	A	B	C	D
1		**This worksheet is for importing the data from this workbook into the SAMM Benchmarking system. Please complete the demographic data, all other data will auto-populate.**		**To import this worksheet into your current SAMM worksheet follow these steps:** 1. Have this workbook and your completed workbook open. 2. Right-click the Benchmark worksheet and choose "Move or Copy" 3. Change the workbook name to your SAMM workbook 4. Click Interview and check the box to make a copy 5. Once copied, open the Benchmark worksheet in your SAMM workbook 6. Click on the Formulas menu, and click "Show Formulas" 7. Ctrl-F and chose replace, enter in "[SAMM_spreadsheet]" and Replace All 8. Uncheck "Show Formulas", this should ensure that the auto linking is relative to your SAMM workbook. 9. Verify the scoring is represented in the table below. 10. Complete the demographic drop down selections. 11. Delete the company name if you desire before submission (it's not saved in the database either way) 12. Upload your file to https://bit.ly/sammbenchmarksubmission 13. An automated process will move the file into a secure Azure Blob for processing and remove the file. 14. Confirm the file is no longer visible in the folder you uploaded to after approximately 5 minutes. 15. If you have any issues or questions please email brian.glas@owasp.org
2				
3				
4				
5		Please complete this section	**Do not insert or delete lines**	**Description**
6				
7		Version of SAMM	2.0.9	Automatic from the Attribution Page
8		Date of Assessment	0-Jan-00	Automatic from the Interview Page
9		Type of Assessment		Choose the type of assessment
10		Scope of Assessment		Scope can be full org, a department/business unit/etc, or an individual team
11		Geographic Region		Select the best region
12		Primary Industry		Select the best fit for primary industry
13		Company Level of Developers		How many developers within the company (estimated)
14		Company Level of App Security		How many application security personnel in the company (estimated)
15		Company Security Champions		How many security champions in the company (estimated)
16		Target Level of Developers		How many developers within the scope of the assessment (estimated)
17		Primary SDL Methodology		Primary software development methodology
18		Composite Score	0.00	Automatic from the Scorecard Sheet
19		Governance Score	0.00	Automatic from the Scorecard Sheet
20		Design Score	0.00	Automatic from the Scorecard Sheet
21		Implementation Score	0.00	Automatic from the Scorecard Sheet
22		Verification Score	0.00	Automatic from the Scorecard Sheet
23		Operations Score	0.00	Automatic from the Scorecard Sheet
24		Strategy & Metrics	0.00	Automatic from the Scorecard Sheet
25		Policy & Compliance	0.00	Automatic from the Scorecard Sheet
26		Education & Guidance	0.00	Automatic from the Scorecard Sheet
27		Threat Assessment	0.00	Automatic from the Scorecard Sheet
28		Security Requirements	0.00	Automatic from the Scorecard Sheet
29		Secure Architecture	0.00	Automatic from the Scorecard Sheet
30		Secure Build	0.00	Automatic from the Scorecard Sheet
31		Secure Deployment	0.00	Automatic from the Scorecard Sheet
32		Defect Management	0.00	Automatic from the Scorecard Sheet
33		Architecture Assessment	0.00	Automatic from the Scorecard Sheet
34		Requirements Testing	0.00	Automatic from the Scorecard Sheet
35		Security Testing	0.00	Automatic from the Scorecard Sheet
36		Incident Management	0.00	Automatic from the Scorecard Sheet
37		Environment Management	0.00	Automatic from the Scorecard Sheet
38		Operational Management	0.00	Automatic from the Scorecard Sheet

Benchmark | Scorecard | Roadmap | Roadmap Chart | Lookups

Expectations - Practitioner (Phase II)

Initial Submission:

- Submit a dataset to the Benchmark System through a SAMM tool
- Benchmark API creates a new entry when processing the data
- Practitioner receives a UUID in response if processed
- Practitioner maintains the records between the UUID and customer

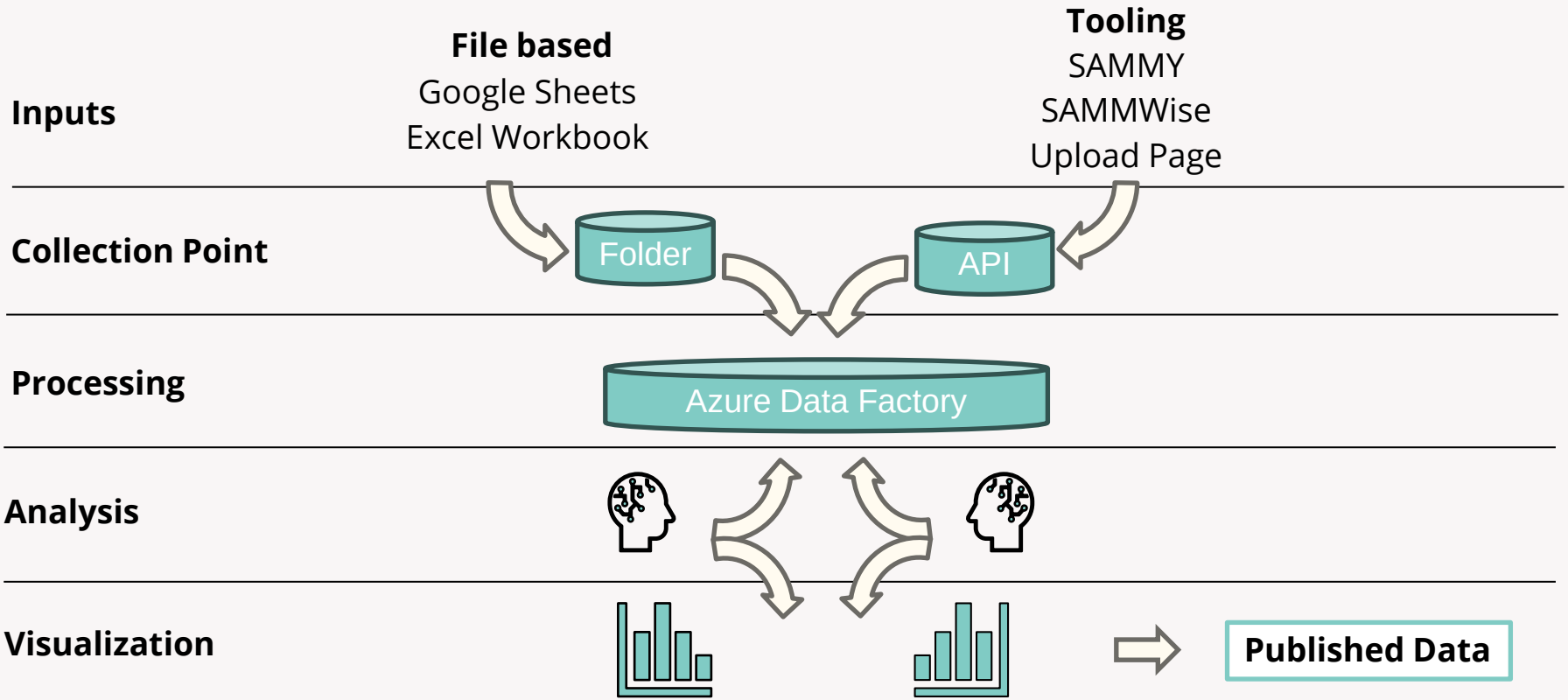
Update Submission:

- Submit a dataset with the UUID to the Benchmark API
- Benchmark will create an update record with the UUID
- Practitioner receives a confirmation if processed

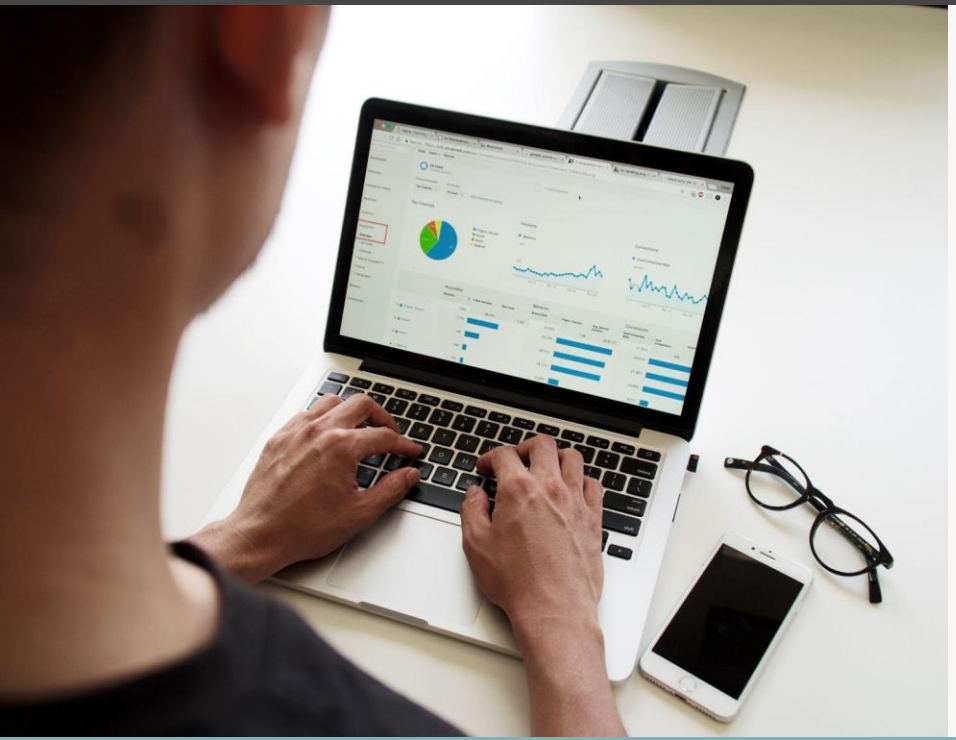
Access Benchmarking Visuals

- Compare with others, learn about different profiles, see industry progression

SAMM Benchmark Infrastructure



Assessment tools



Spreadsheets

Google Sheets (Google Drive)
Excel (GitHub)

SAMMY

Free, online tool
https://sammy.codific.com/

SAMMWise

Open source, self-hosted solution
https://github.com/owaspsamm/sammwise

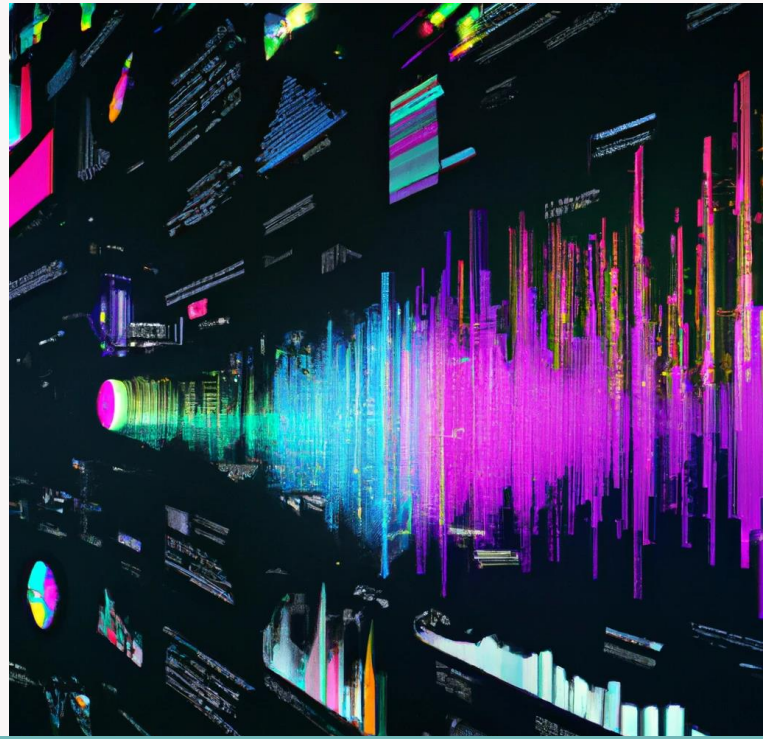
Expectations - Analysis & Visuals

Population Level:

- Overall Low/Median/High scores for organizations
- Aggregate scoring from Business Function to Questions

Comparison:

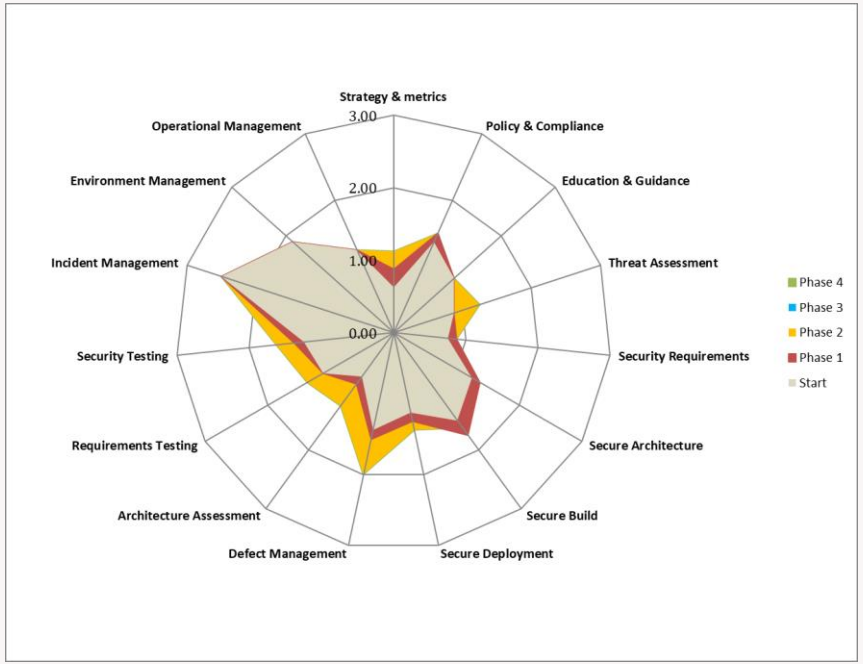
- By size, region, industry, etc
- Predictive: Given current scores what are the most common areas of focus

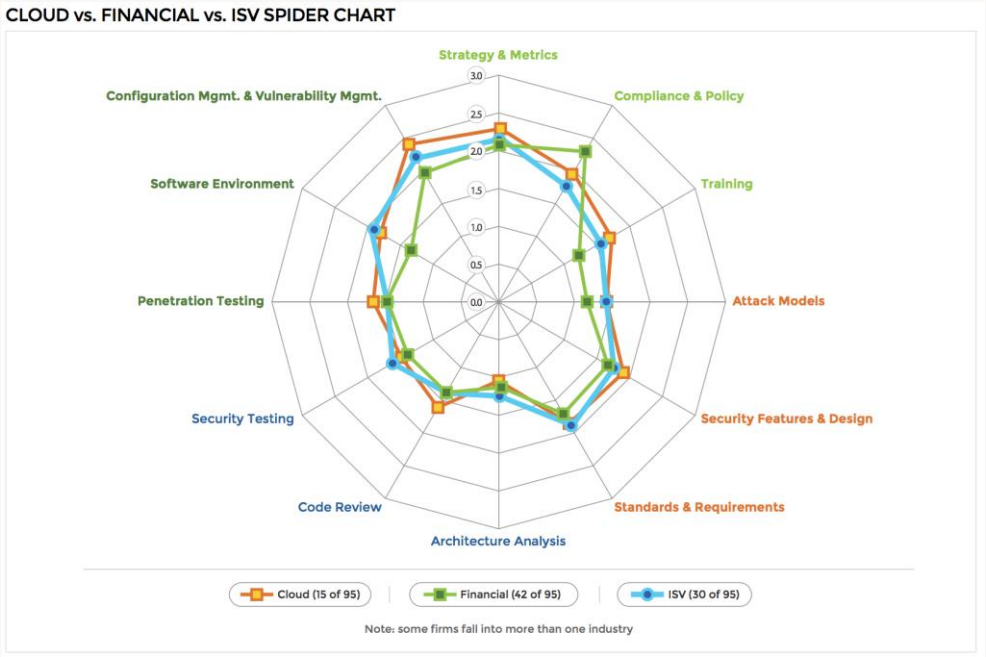


Global Benefits - SAMM Benchmark

- Drive improvement in software security
- Help organizations learn from each other
- Provide data to improve the models
- Accessible data for all organization sizes
- No other comprehensive dataset like this exists today

BSIMM - SAMM Benchmark





BSIMM - SAMM Benchmark

DOMAINS			
GOVERNANCE	**INTELLIGENCE**	**SSDL TOUCHPOINTS**	**DEPLOYMENT**
Practices that help organize, manage, and measure a software security initiative. Staff development is also a central governance practice.	Practices that result in collections of corporate knowledge used in carrying out software security activities throughout the organization. Collections include both proactive security guidance and organizational threat modeling.	Practices associated with analysis and assurance of particular software development artifacts and processes. All software security methodologies include these practices.	Practices that interface with traditional network security and software maintenance organizations. Software configuration, maintenance, and other environment issues have direct impact on software security.
PRACTICES			
GOVERNANCE	**INTELLIGENCE**	**SSDL TOUCHPOINTS**	**DEPLOYMENT**
1. Strategy & Metrics (SM)	4. Attack Models (AM)	7. Architecture Analysis (AA)	10. Penetration Testing (PT)
2. Compliance & Policy (CP)	5. Security Features & Design (SFD)	8. Code Review (CR)	11. Software Environment (SE)
3. Training (T)	6. Standards & Requirements (SR)	9. Security Testing (ST)	12. Configuration Management & Vulnerability Management (CMVM)

BSIMM - SAMM Benchmark

BSIMM COMMUNITY NUMBERS OVER TIME								
	BSIMM13	BSIMM12	BSIMM11	BSIMM10	BSIMM9	BSIMM8	BSIMM7	BSIMM1
Firms	130	128	130	122	120	109	95	9
SSG Members	3,342	2,837	1,801	1,596	1,600	1,268	1,111	370
Satellite Members	8,508	6,448	6,656	6,298	6,291	3,501	3,595	710
Developers	408,999	398,544	490,167	468,500	415,598	290,582	272,782	67,950
Applications	145,303	153,519	176,269	173,233	135,881	94,802	87,244	3,970
Average SSG Age (Years)	5.00	4.41	4.32	4.53	4.13	3.88	3.94	5.32
SSG Average of Averages (SSG per Developers)	3.01 / 100	2.59 / 100	2.01 / 100	1.37 / 100	1.33 / 100	1.60 / 100	1.61 / 100	1.13 / 100

TABLE 3. BSIMM COMMUNITY NUMBERS OVER TIME. The chart shows how the BSIMM study has grown over the years.

BSIMM - SAMM Benchmark

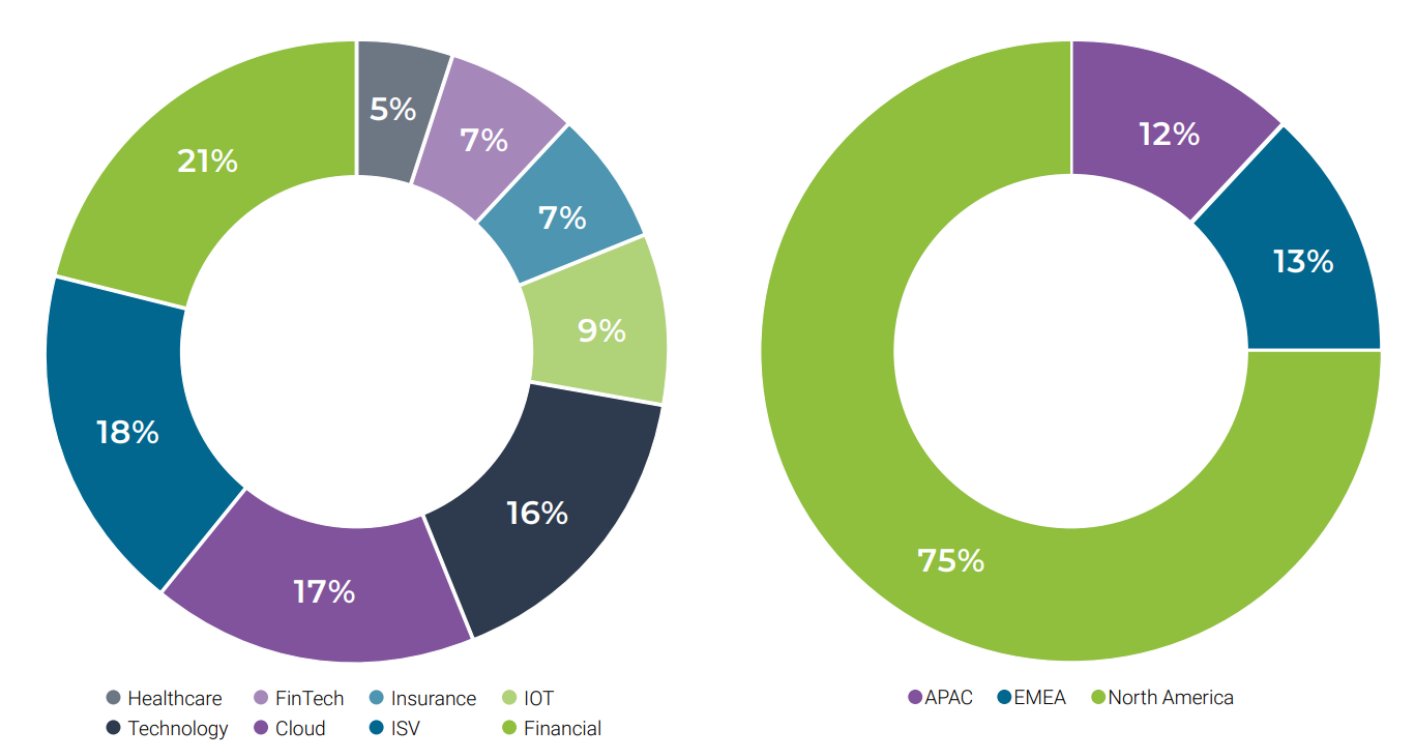
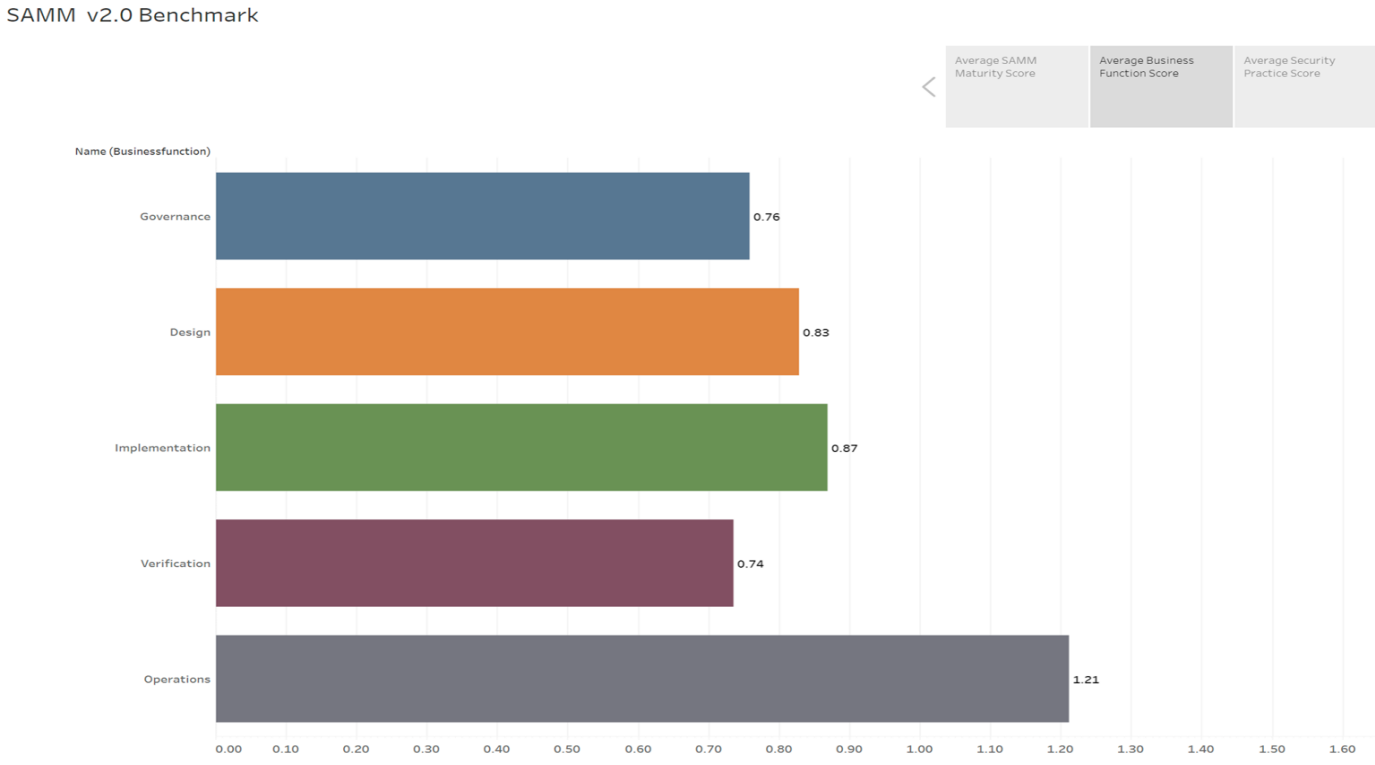


FIGURE 2. BSIMM13 COMMUNITY PARTICIPANTS. Participant percentages per tracked vertical and region.

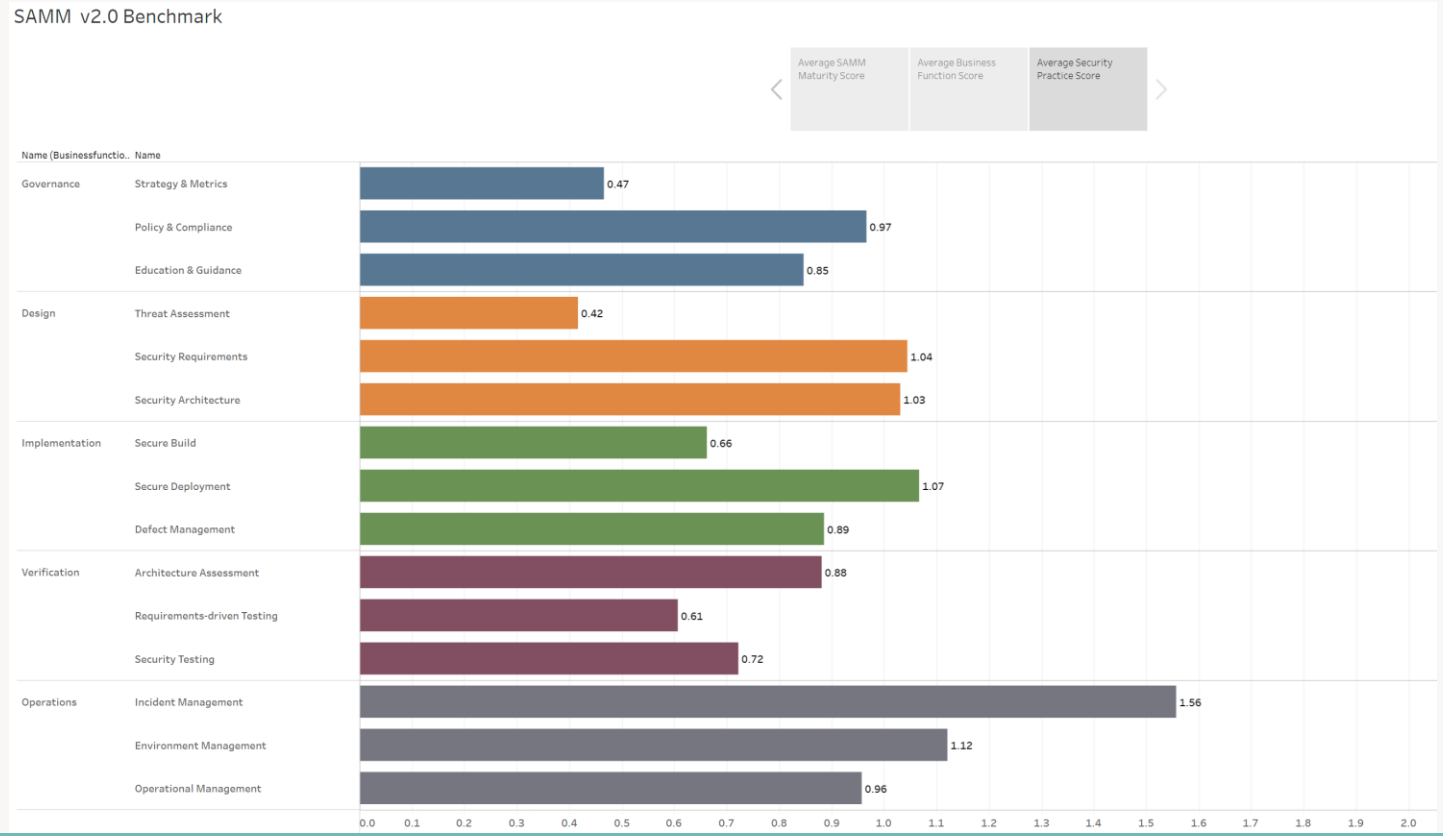
BSIMM -

GOVERNANCE			INTELLIGENCE			SSDL TOUCHPOINTS			DEPLOYMENT		
ACTIVITY	BSIMM13 FIRMS (OUT OF 130)	EXAMPLE FIRM	ACTIVITY	BSIMM13 FIRMS (OUT OF 130)	EXAMPLE FIRM	ACTIVITY	BSIMM13 FIRMS (OUT OF 130)	EXAMPLE FIRM	ACTIVITY	BSIMM13 FIRMS (OUT OF 130)	EXAMPLE FIRM
STRATEGY & METRICS			**ATTACK MODELS**			**ARCHITECTURE ANALYSIS**			**PENETRATION TESTING**		
[SM1.1]	98	1	[AM1.2]	80		[AA1.1]	113	1	[PT1.1]	114	
[SM1.3]	82		[AM1.3]	42		[AA1.2]	53	1	[PT1.2]	102	1
[SM1.4]	117		[AM1.5]	76	1	[AA1.4]	69		[PT1.3]	88	1
[SM2.1]	73		[AM2.1]	16		[AA2.1]	31		[PT2.2]	38	
[SM2.2]	63		[AM2.2]	11	1	[AA2.2]	32	1	[PT2.3]	45	
[SM2.3]	69		[AM2.5]	16	1	[AA2.4]	38	1	[PT3.1]	26	1
[SM2.6]	71		[AM2.6]	16		[AA3.1]	20		[PT3.2]	15	
[SM2.7]	64	1	[AM2.7]	14		[AA3.2]	4				
[SM3.1]	27		[AM3.1]	9		[AA3.3]	15				
[SM3.2]	18		[AM3.2]	5							
[SM3.3]	26		[AM3.3]	11							
[SM3.4]	5										
[SM3.5]	0										
COMPLIANCE & POLICY			**SECURITY FEATURES & DESIGN**			**CODE REVIEW**			**SOFTWARE ENVIRONMENT**		
[CP1.1]	101	1	[SFD1.1]	104	1	[CR1.2]	83	1	[SE1.1]	87	
[CP1.2]	115	1	[SFD1.2]	90	1	[CR1.4]	107	1	[SE1.2]	115	1
[CP1.3]	98	1	[SFD2.1]	39		[CR1.5]	62		[SE1.3]	79	1
[CP2.1]	58		[SFD2.2]	64		[CR1.7]	54		[SE2.2]	57	1
[CP2.2]	59		[SFD3.1]	17		[CR2.6]	28	1	[SE2.4]	39	
[CP2.3]	73		[SFD3.2]	18		[CR2.7]	20		[SE2.5]	52	1
[CP2.4]	62		[SFD3.3]	7		[CR2.8]	34	1	[SE2.7]	42	1
[CP2.5]	82	1				[CR3.2]	14		[SE3.2]	19	
[CP3.1]	30					[CR3.3]	8		[SE3.3]	11	
[CP3.2]	28					[CR3.4]	2		[SE3.6]	18	
[CP3.3]	11					[CR3.5]	3		[SE3.8]	0	
TRAINING			**STANDARDS & REQUIREMENTS**			**SECURITY TESTING**			**CONFIG. MGMT. & VULN. MGMT.**		
[T1.1]	71	1	[SR1.1]	96	1	[ST1.1]	108	1	[CMVM1.1]	114	1
[T1.7]	58	1	[SR1.2]	101		[ST1.3]	97	1	[CMVM1.2]	100	
[T1.8]	53		[SR1.3]	103	1	[ST1.4]	56		[CMVM2.1]	95	1
[T2.5]	38		[SR2.2]	80	1	[ST2.4]	25		[CMVM2.2]	98	
[T2.8]	28	1	[SR2.4]	92		[ST2.5]	31		[CMVM2.3]	62	
[T2.9]	33	1	[SR2.5]	63	1	[ST2.6]	21		[CMVM3.1]	11	
[T2.10]	28		[SR2.7]	53		[ST3.3]	12		[CMVM3.2]	19	
[T2.11]	27		[SR3.2]	19		[ST3.4]	4		[CMVM3.3]	18	
[T3.1]	9		[SR3.3]	17		[ST3.5]	4		[CMVM3.4]	26	1
[T3.2]	16		[SR3.4]	19		[ST3.6]	3		[CMVM3.5]	13	1
[T3.5]	22								[CMVM3.6]	3	
[T3.6]	7								[CMVM3.7]	20	
									[CMVM3.8]	0	

Benchmark Project



Benchmark Project



Benchmark Project Milestones

Nov/Dec

- Azure infrastructure for ETL functionality
- Initial visualizations
- Awareness campaign

Jan/April

- Collect all the data
- Start analysis of datasets

May/June

- Draft state of Software Assurance based on the data

Future Benchmark Infrastructure

OWASP Projects

Mod Security
Top 10(s)
SAMM

Other OWASP Projects
Dependency Track
OWASP ZAP

OWASP DAVID

Data Analysis, Visualization, and Ingestion Domain

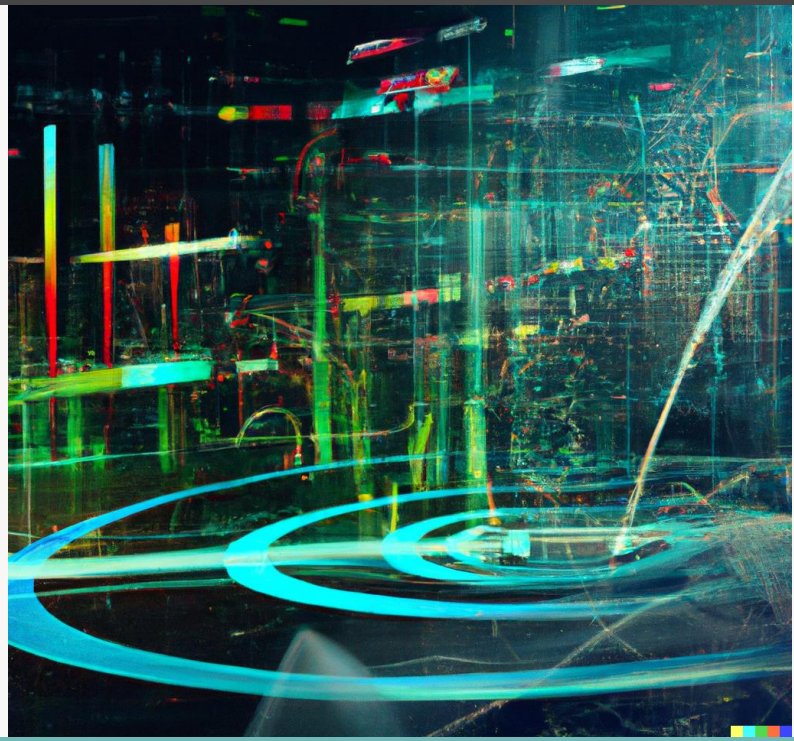
DAVID

Larger scale to manage data for multiple types of projects

Early-Mid 2024

Building the team and requirements

SAMM and OWASP Top 10 initial projects



Contribute to the project

Preliminary data
- 12+ Datasets

Expect to build more quickly in
Late 2023 – Early 2024

Donate data sets
owaspsamm.org/benchmarking/
https://bit.ly/sammbenchmarkingsubmissions

Benchmark

What features would be valuable for you?

Questions?

Feedback?

OWASP SAMM

OWASP
Open Web Application
Security Project

OWASP
SAMM

owaspsamm.org