SAMM practitioners

SAMM community call
November 9, 2022

We get this question a lot

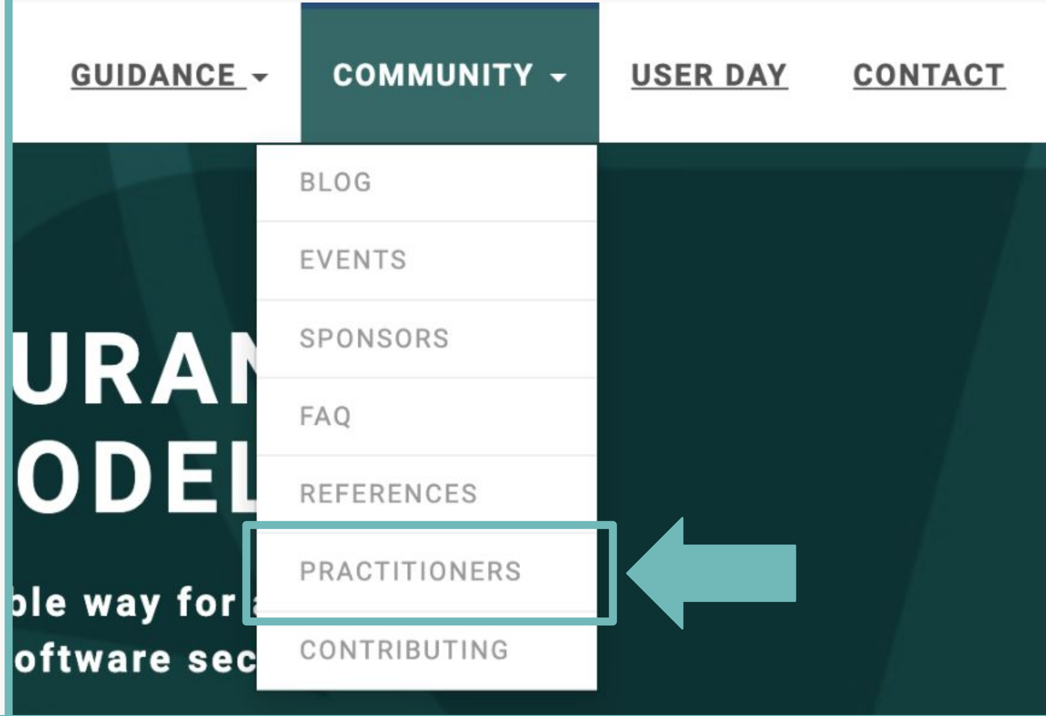
We're looking at adopting OWASP SAMM 2.0 where I work.

Can you recommend a company to do this?

Introducing SAMM Practitioners

Providing

- Assessments
- Roadmap services
- SAMM tools
- Trainings
- ...



GUIDANCE
COMMUNITY
USER DAY
CONTACT

BLOG
EVENTS
SPONSORS
FAQ
REFERENCES
PRACTITIONERS
CONTRIBUTING

Disclaimer

While the OWASP SAMM project is selective about the practitioners we list, it does **NOT** imply we endorse, recommend, or favor any of them.

Full disclaimer at https://owaspsamm.org/practitioners/

Who makes the list

To add SAMM practitioners to the list

- the SAMM practitioner has to request to be on the list.
- the SAMM practitioner has to provide a link to its SAMM related service offering (SAMM assessment, roadmap, or tools).
- the SAMM service offering of the practitioner has to contain a reference and link to https://owaspsamm.org/.

The OWASP SAMM project team reserves the right to reject or remove SAMM practitioners from this list at any time.

Interested in contributing?

Don’t hesitate to contact us!

OWASP SAMM

SAMM Core Team Summit

Summit Debrief
November 6, 2022

Summit Outcomes

- Survey result analysis (see sneak preview later)
- Professionalization of SAMM
- Mapping
- Benchmarking
- Guidance
- Other outcomes

Professionalization of SAMM

Topics

- Project Governance
- Defining Core Processes and Roles
- Product Management
- Future Roadmaps

Professionalization of SAMM

Outcomes

- Leverage Github Projects for SAMM project management
  - Predictive pace of development
  - Increase visibility towards the community
  - Make it easier for community members to identify where they can contribute
- Leverage dedicated identity (info@owaspsamm.org) for community Slack channel
- Explore dedicated roles pros & cons
- Collaborate, share & promote roadmaps with the community

Mapping

Goals

- Leverage SAMM’s capabilities to create a roadmap towards SSDF compliance
- Starting point for further mapping initiatives

NIST SSDF Mapping

2022 Timeline

February

Release of NIST SSDF v1.1, including a mapping to SAMM 1.5

September

Executive Memorandum M-22-18 is released

(Enhancing the Security of the Software Supply Chain through Secure Software Development Practices)

October

First SSDFv1.1 to SAMMv2.0 mapping created, reached out to NIST for feedback

November

We used a more formal and granular mapping scheme to refine the mapping

We have followed up with NIST for further feedback, and plan to iterate

December

Tentative release of final SSDF/SAMM mapping

Benchmarking

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

69% answered 7 or higher

We’ve made the benchmarking initiative SAMM core team’s number 1 priority

Benchmarking 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 Initiative

MVP

- Focus on increasing the number of datasets in the database

  You can help!

- First deliverable

  PDF report with in-depth analysis in 2023

Benchmarking Initiative

What have we done already?

- Consolidated existing benchmarking initiative information into “SAMM Benchmarking Use Cases” to drive further initiative development

  Soon open for review

- Benchmarking data model updated to reflect the use cases (Brian)

- Practitioners page created

Benchmarking Initiative

What’s next?

- Use case community feedback
- Project planning
- Practitioner & assessment guidance
- Documentation on the approach
- Start requesting data and expand the dataset
- … Publish the first SAMM benchmark report!

Guidance

Types

- Practice
- Role

Source

- Community
- Core team

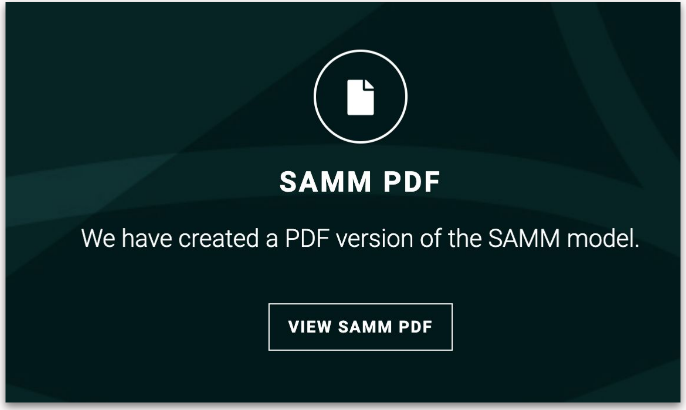
Access

- Resources section on website
- Friendly activity IDs
- Activity URLs

Other Outcomes

- PDF generator
  - https://github.com/owaspsamm/pdf-generator
  - Donated by Codific (thanks!)

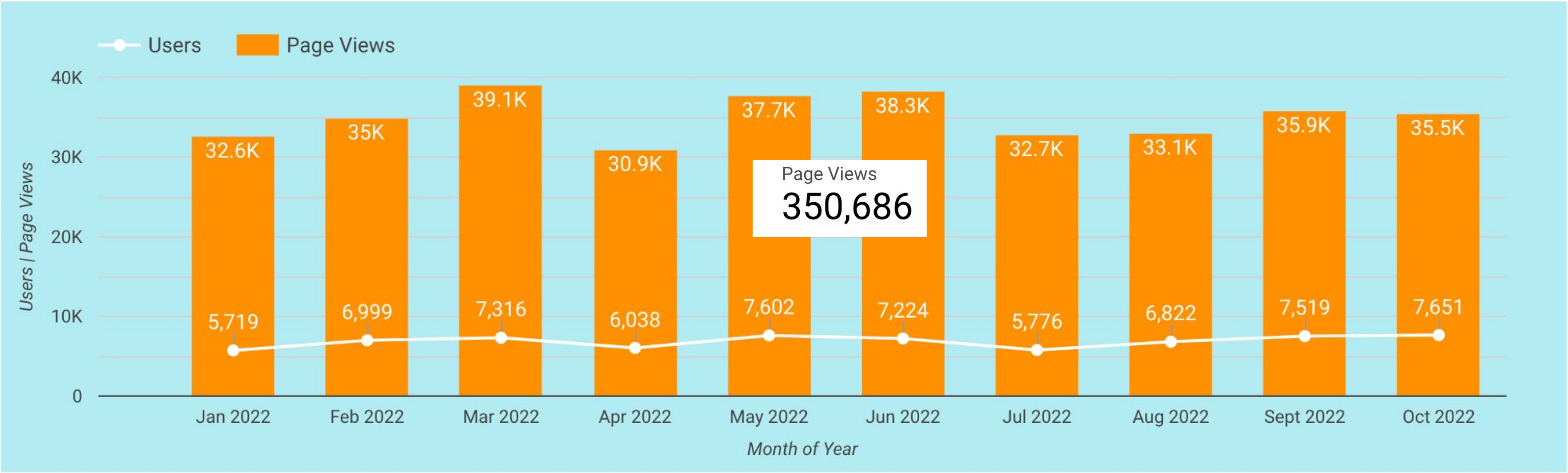
- Translations (approach revisited - see here)
- Marketing outcomes
- “Not applicable” option :-)



SAMM PDF

We have created a PDF version of the SAMM model.

SAMM is getting noticed



OWASP
Open Web Application
Security Project

OWASP SAMM

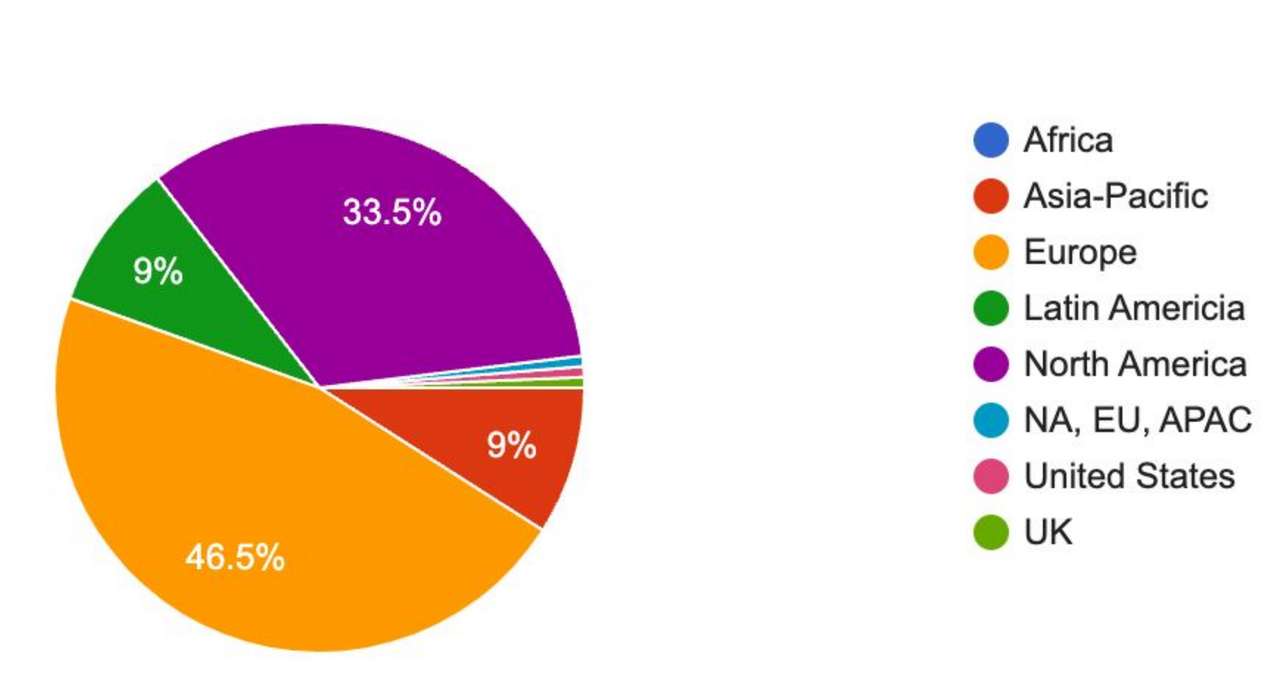
SAMM 2022 Survey (sneak peek)

SAMM community call
November 9, 2022

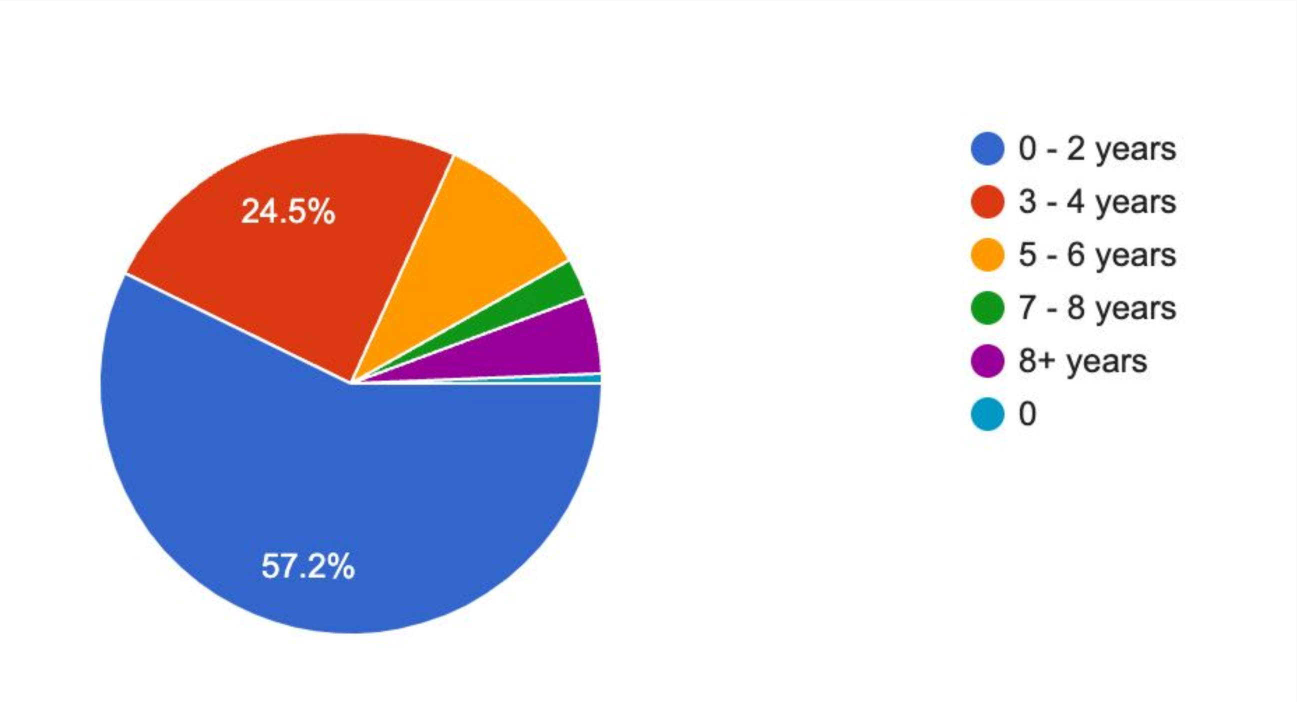
Sneak peek

- 156 participants, survey now closed
- Some preliminary results here
- Full blog post and results analyzed next community call in December

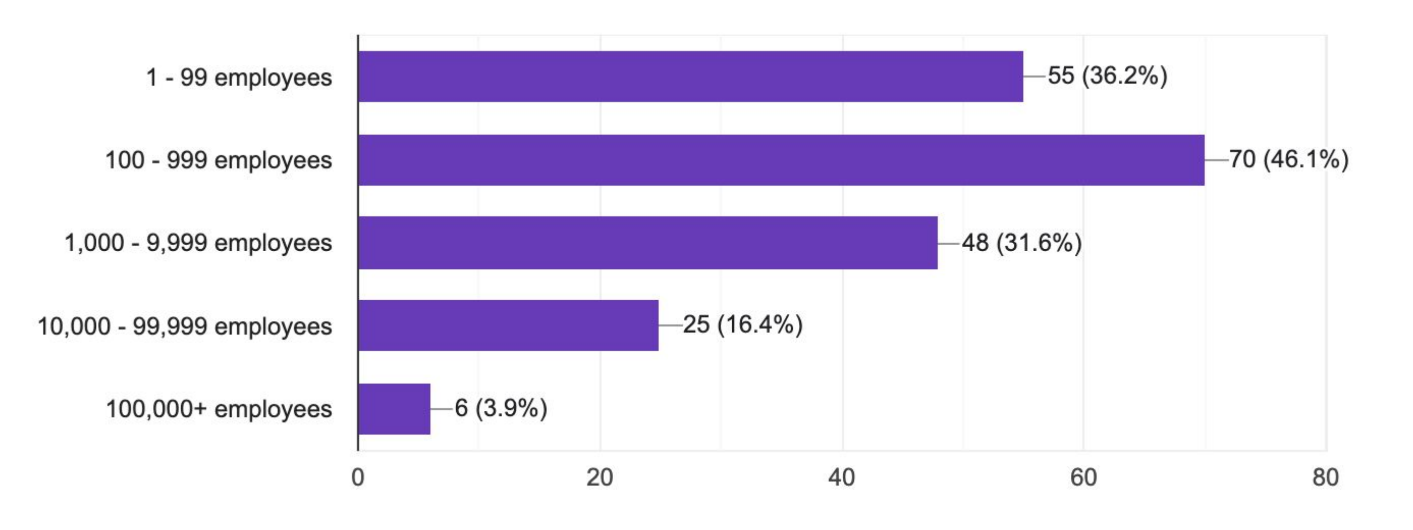
Geographic spread



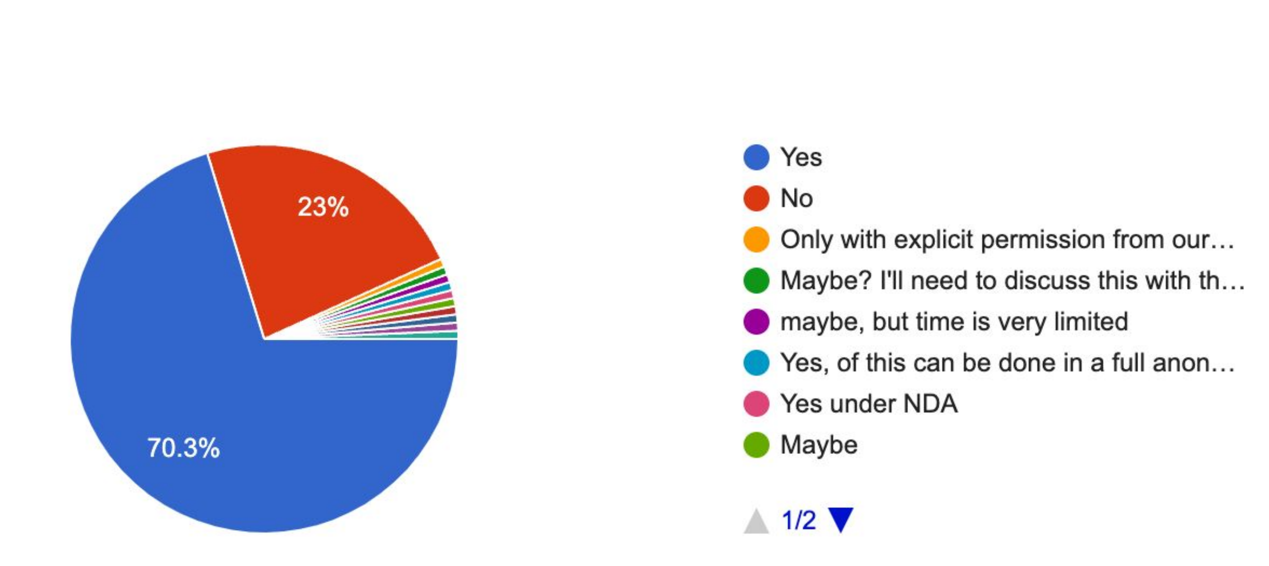
SAMM experience



Organization size



Contribute data to the Benchmark?



Improvements suggested (draft)

- Provide SAMM for teams & products
- Mappings / combination with
  - ISO 27001
  - NIST 800-53
  - NIST CSF
  - NIST SSDF
- Benchmark!
- More guidance

Communication channels

#project-samm

mailchimp

eepurl.com/gl9fb9

OWASP
Open Web Application
Security Project

OWASP
SAMM

Thank you!

owaspsamm.org