SAMM Grant Request 2023

Our mission is to provide an effective and measurable way for all types of organizations to analyze and improve their software security posture. We want to raise awareness and educate organizations on how to design, develop, and deploy secure software through our self-assessment model. SAMM supports the complete software lifecycle and is technology and process agnostic. We built SAMM to be evolutive and risk-driven in nature, as there is no single recipe that works for all organizations.

To expand our impact on software security and help organizations worldwide improve their security posture, we seek to accelerate our SAMM project significantly. Our proposal is to augment our current team of volunteers with additional paid project contributors and infrastructure. By investing in the SAMM project, SAMM will become even more effective and accessible, supporting organizations in their journey towards secure software development.

We are seeking funding in the order of of 800,000 USD for 2023, which we will use to cover the following tracks (numbers in brackets for the first year):

- Benchmarking Track - (135K USD) - Visibility into how other organizations are managing secure development is critical for driving overall maturity and improvement across the globe.
- Benchmark data collection platform - (100K USD) - This part of the SAMM grant would fund the pilot for the first of many OWASP data collection and analysis projects. SAMM Benchmark will be the pilot project for the new OWASP wide Data Management project.
- Education Track - (200K USD) - By improving the educational delivery of the project we are convinced that we can create a success story not only for SAMM, but also for OWASP and all OWASP projects.
- Communication Track - (35K USD) - To be heard in the crowded security marketplace that we experience today, SAMM (and OWASP) needs to build its authority and appetite to present a faster momentum for change by being more dynamic with the community that supports it.
- Funding Track - (207K USD) - This portion of the grant is dedicated to securing funding to support both the parts of the grant itself and the operational expenses of the OWASP SAMM project.
- Others Track - (124K USD) (including translations, PDF, website)

Each of these tracks is detailed below in our grant request to the OWASP Foundation board.

OWASP SAMM project leaders
Sebastien Deleersnyder
Bart De Win

With the support of our SAMM core team.

Benchmarking Track

Short-term

In order to deliver the first milestones in the benchmark project, we need the following roles in the coming 12 months. Some of which are already picked up by the volunteers in the team, some we still need to source.

If we are to source these efforts on the open market, the average cost in the coming 12 months would be **172K USD** and would total around **630K USD over a period of three years.**

Role	**Person Days (Year 1 of 3)**	**Avg of rates/role (USD)**	**Total Estimate (USD)**
Project Manager	15	105	12.6K
Data Scientist / Researcher	60	150	72K
Technical Writer (+part graphics design)	20	112.5	180K
Marketing Specialist / Growth Expert	10	135	10.8K
Infrastructure engineer and/or developer	10	160	64K
(Benchmark) Product Manager	20	112.5	18K
Grants manager	30	105	25.2K
Subtotal			163K

* 1 day = 8hrs

In addition, the following (yearly recurring) costs are foreseen

Type	**Total Estimate**

	(USD)
Hosting in Azure (estimated)	2.5k USD
Data platform (2 Tableau creator licenses)	2k USD
Subtotal Platform	4.5k USD

Benchmark Context

At some point, every organization seeking to improve its security posture must ask itself, "How do we compare to others in our industry?" Currently, there is no open benchmark available that provides this data. We believe that SAMM can serve as a platform for creating an open benchmark that can help organizations better understand their security posture compared to others in their industry.

Visibility into how other organizations are managing secure development is critical for driving overall maturity and improvement across the globe. The SAMM Benchmark is uniquely positioned to establish a median bar for organizations based on several different factors. By providing visibility into this bar and examples of how organizations are exceeding it, we can drive healthy competition between organizations to improve their security posture. This can help organizations promote their secure development processes and practices as a competitive advantage, ultimately leading to a more secure environment for everyone.

In addition to developing the SAMM benchmark, we are adding guidance to SAMM through an ongoing initiative that provides hands-on information to practitioners and links OWASP projects and resources to SAMM practices. This can increase the reach of OWASP to a whole new audience and help organizations develop a more mature and effective approach to software assurance.

The changing landscape and urgency surrounding software security present an opportunity for OWASP to establish a benchmark for software assurance. Both the EU and US are putting in place legislation that will hold companies accountable for the security of their organization and products. Having a standardized benchmark can help organizations meet these obligations. By mapping ISO and SAMM standards, OWASP can offer a comprehensive tool for organizations to assess their security posture, identify areas for improvement, and demonstrate their commitment to security.

Another quick win for OWASP through the SAMM Benchmark Initiative is raising awareness about the OWASP community and projects. It will allow the foundation to reach a wider audience, especially those who may not be as tech-savvy or familiar with the OWASP Top Ten. By providing hands-on guidance to practitioners and linking OWASP resources to SAMM practices, OWASP can expand its reach and influence beyond its traditional audience. This can help to build awareness and trust in OWASP

and its mission, while also empowering organizations to improve their security posture and promote secure development practices as a competitive advantage.

By being proactive and taking the lead on this initiative, OWASP can establish itself as a thought leader and trusted resource in the software assurance space, helping drive overall maturity and improvement in secure development practices across the globe.

Please refer to the Core Principles Document for a more detailed overview of the project.

Stakeholders and Use Cases

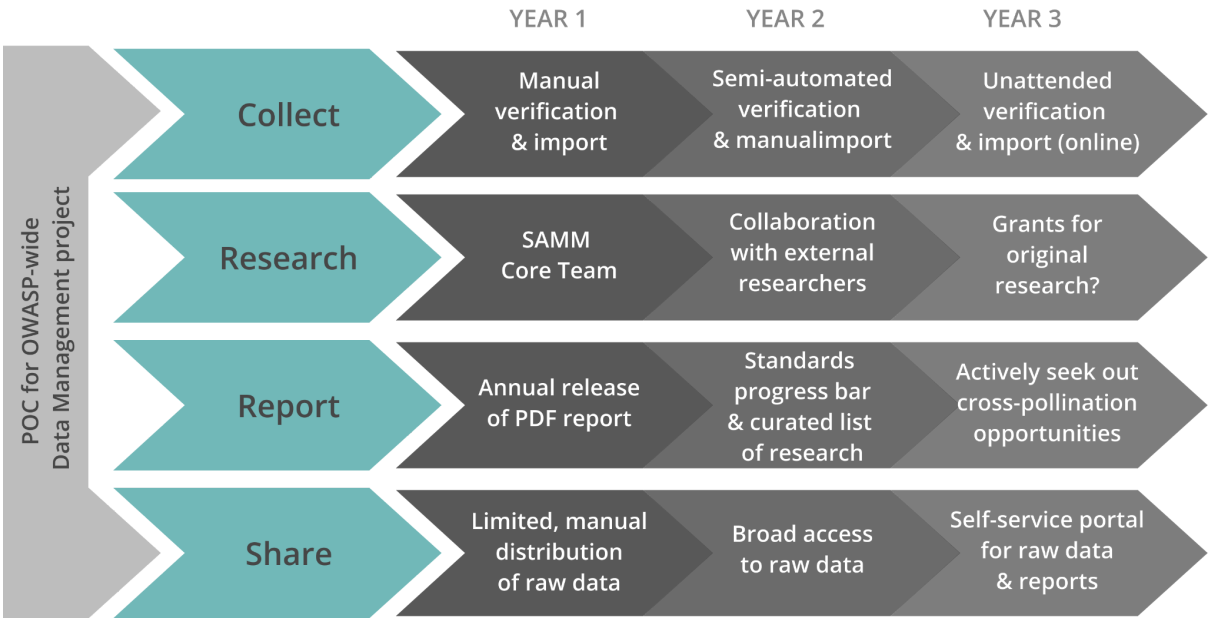
We discern three main stakeholder types for this project.

- SAMM Core Team Members use the benchmarking data to drive improvement of the core SAMM model.
- Assessors contribute data to the benchmark database and use the benchmark data to compare the security posture of their clients or employers to the rest of their industry.
- Independent Researchers use the benchmarking data for original research, leading to independent (from the SAMM core team) publications.

A complete overview of the stakeholders and the use cases we foresee can be found in the Use Cases Document.

Benchmark Roadmap

The following roadmap proposal describes the steps towards long term success.
The 4 streams are able to move in parallel. For 2023, our goal is to achieve the first level of each stream. The work in coming years will build on these efforts, driving towards further automation and integration possibilities in each step.



Funding makes the difference

The core team, with support from many other volunteers, has been working on the Benchmarking initiative since 2015. A lot of work has been done already, and we have a solid foundation to start from, but we still have a long way to go on our roadmap.

During the grant request exercise we polled the core team on the amount of time members are spending on SAMM on average, how much time can be spent during spikes and whether funding would impact the prioritization of SAMM work.
On average, core team members are already spending about 4-6 hours per week on the project.
About half of the core team members would be able to spend more time on the project if they were able to do paid work for (parts!) of the project.

Not all required skills are currently covered by members of the core team, so even if all of the core team members manage to find time, we can not make dependable progress.

Funding will help us align priorities within the core team, source expert support on the open market and deliver on the ambitions for the project.

Supporting Roles

#DISCLAIMER: Market rates have been guesstimated by chatgpt 🙂
#DISCLAIMER: Efforts have been guesstimated by Maxim and to be further refined with the whole group!

Glossary
ROM PD = Rough Order of Magnitude estimate of PersonDays
BOE=basis of estimate

Title	**Responsibilities**	**Main deliverable**	**Market Rate (USD)?**	**YEAR 1 ROM PD**	**YEAR 2 ROM PD**	**YEAR 3 ROM PD**	**Comments/BOE**
Project Manager	“Cat herding” a mix of paid and volunteer contributors against the goals described in this proposal	Dependable progress	70-140/hr	15	30	30	The amount of effort and stakeholders in Y1 are limited, compared to Y2-Y3
Data Scientist / Researcher	Vet, clean and help interpret the benchmarking data. Provide reports or even research papers based on the benchmark data	Insights in the data, technical input for publications	100-200/hr	60	90	120	We expect a lot more data every year
Technical Writer (+part graphics design)	Streamline various technical or high-level inputs and condense them into well-structured	SAMM Benchmark PDF	75-150/hr	20	30	40	With the increased data, comes more insights and a

	“whitepaper” type content and blog posts Help with community communications						longer report
Marketing Specialist / Growth Expert	Helping the initiative to collect the maximum amount of contributions, and helping to ensure consistent contributions year over year. Preparing communications to a target audience with content in the right format to attract visitors and interaction.	Review of content, and manage external communications, building a PR network, posting content.	90-180/hr	10	10	10	Y1 - 3 will be pretty stable in terms of effort, building on previous years to grow and keep the network engaged, prevent churn and grow domain authority and requests for comments / input as specialists in the field.
Infrastructure engineer and/or developer	Architecting and coding tooling that	Self-service platform (Later: unified data platform)	100-220/hr	5	30	60	Y1 will start with the infra that Brian had developed, Y2-Y3 we build on that infra
(Benchmark) Product Manager	Liaison with the SAMM community. SPOC for benchmark. Working with the various other roles to line up external wants (eg. features) with internal needs and	“Productization” of the benchmark	75-150/hr	20	40	40	The amount of effort and stakeholders in Y1 are limited, compared to Y2-Y3

	plans						
Grants manager	Seeking out sponsors and building long-term partnerships with interested 3rd parties.	Ensure an income stream for the project	70-140/hr	30	30	30	

OWASP SAMM Benchmark Timeline

(Milestones are to be completed by the end of month listed)

- April 2023
    - Complete initial draft infrastructure design for review.
    - Draft initial legal agreement and data governance process documents.
- May 2023
    - Complete test environment with the data management infrastructure.
    - Complete second draft of legal agreement and data governance process documents.
- June 2023
    - Complete the production environment for the data management infrastructure.
    - Complete the final draft of the legal agreement and data governance process documents.
    - Complete Awareness campaign for the SAMM Benchmarking initiative.
- July 2023
    - Start data collection using the new production infrastructure.
    - Design initial data visualizations and metrics.
- August 2023
    - Support the data management processes.
    - Refine the collection and analysis processes to streamline.
    - Create additional data visualizations and metrics.
- September 2023
    - Support the data management processes.
    - Refine the data visualizations and metrics.
    - Initial research findings from the gathered data.
- October 2023
    - Support the data management processes.
    - Finalize the data visualizations and metrics for the inaugural report.
    - Identify additional research findings from the data.
- November 2023
    - Support the data management processes.
    - Draft inaugural SAMM Benchmark State of Software Assurance Report
- December 2023
    - Support the data management processes.
    - Publish the SAMM Benchmark State of Software Assurance Report
- January 2024
    - Support the data management processes.

    - Define processes for data access and sharing.
- February 2024
    - Support the data management processes.
    - Document what is needed to enable similar data management capabilities for other OWASP projects.
- March 2024
    - Support the data management processes.

Detailed Milestones

Collect

1. Manual Verification And Import
    a. (Maxim/?) Publish supporting documentation
        i. How to submit data & to whom
        ii. Relationship between core team & practitioners
        iii. Info on vetting process
        iv. Data retention policy & how to remove / transfer / … ?
    b. (Brian?) Use existing methods to import collected data
    c. (Brian?) Publish existing code on public repo, solicit review and pull requests from community
2. Semi-Automated verification & Manual Import
    a. (Dev?) Implement data verification & error handling to support automated benchmark data import
        i. EXAMPLES: conflicting ID's, boundary checking, suspicious scores, suspicious evolution of scores over time, amount of submissions, …?
    b. (Dev?) Streamline import of data and refactor or amend existing codebase to support a self-service portal in the future
3. Unattended Verification and Import
    a. (Dev?) Publish SAMM Benchmark self-service portal that allows

Research

1. SAMM Core Team
    a. (???) 2 or 3 core team members to do research on the first set of data and provide input for PDF in Q3 2023 → focus on high-level insights that can be deduced from a relatively small initial dataset (eg. like questionnaire insights)
2. Collaboration with external researchers
    a. (Maxim) Publish supporting documentation
        i. How to request data
        ii. Acceptable use?
    b. (Maxim?) SPOC for external collaboration
3. Grants for original research **#MBAE freewheel idea, feel free to shoot this down**

Report

1. Annual Release of PDF Report
    a. (Core team researchers) to write down insights

    b. (Core team) peer review + additional input
    c. (Pat?) format in a standalone document
    d. (John?) marketing / hype (Before, during and after release)
    e. (Community Mgr) Make rounds on conferences & solicit feedback from community
2. Standards Progress Bar & Curated list of research
    a. (Aram??) Publish howto or provide tooling to measure progress against 3rd party models and standards (eg. SSDF / ISO / CMM)
    b. (???) Publish and maintain a list of research mentioning OWASP SAMM and/or SAMM benchmark
3. Actively seek out cross-pollination opportunities
    a. (Community Manager) Reach out to OWASP Projects

Share

1. Limited, manual distribution of raw data
    a. (Community Manager) Act as SPOC for individual data requests and provide data to 3rd parties
2. Broad Access to raw data
    a. (Community Manager) Provide raw data to the community for download (eg. blob?)
    b. (dev?) Build on work in stream “Collect” to prepare self-service portal for data, for use by community manager at this stage
3. Self-Service Portal
    a. (Dev?) Build full self-service experience (API or portal?) to submit data, get data, transfer ownership of data or delete data

SAMM Benchmark data collection platform

This part of the SAMM grant would fund the pilot for the first of many OWASP data collection and analysis projects. SAMM Benchmark will be the pilot project for the new OWASP wide Data Management project. Once SAMM Benchmark implementation is completed in the new infrastructure, additional projects can be supported.

There are numerous benefits that can be realized by creating this data management system for OWASP SAMM Benchmark as a pilot for additional OWASP projects in the future:

- Data Consistency and Integrity: A centralized system ensures that data across all projects follows the same data governance standards, thus increasing data integrity and consistency.

- Simplified Data Management: A centralized system streamlines data management processes, reducing the burden of each OWASP project managing data individually. Lessons learned from each project can be applied to future projects when they are on-boarded and consistency can be ensured.

- Time and Cost Savings: A centralized system reduces the time spent on data management and maintenance, resulting in cost savings across projects. Consolidating data in one location minimizes redundancy and promotes quicker data retrieval, improving the overall efficiency of OWASP projects.

- Better Decision-Making: Access to comprehensive and consistent data enables data-driven decision-making, leading to more accurate and effective outcomes for OWASP projects and organizations that rely on them.

- Scalability: A centralized data management system can easily accommodate new projects, ensuring seamless integration and scalability.

- Compliance and Auditing: A centralized system simplifies compliance and auditing processes by providing a unified platform to track and monitor data access and usage.

- Enhanced Data Visibility: A centralized system improves data visibility, making it easier to identify trends, patterns, and insights that can drive innovation and improvement in OWASP projects.

OWASP SAMM Benchmarking is an ideal pilot project to implement the centralized data management system as it deals with the collection, analysis, and reporting of maturity data for various organizations. Implementing the centralized system will streamline data management processes, improve data quality, and facilitate more effective benchmarking results for organizations. The successful implementation of this system will serve as a strong foundation for future OWASP projects, driving innovation and impact in the application security community.

Resource Requirements

Data Architect/Researcher - 500hrs @ $150 per hour = $75,000 USD

Developer - 100hrs @ $100 per hour = $10,000 USD

Product Manager - 150 @ $100 per hour = $15,000 USD

Total = $100,000 USD

Timeline
(Milestones are to be completed by the end of month listed)

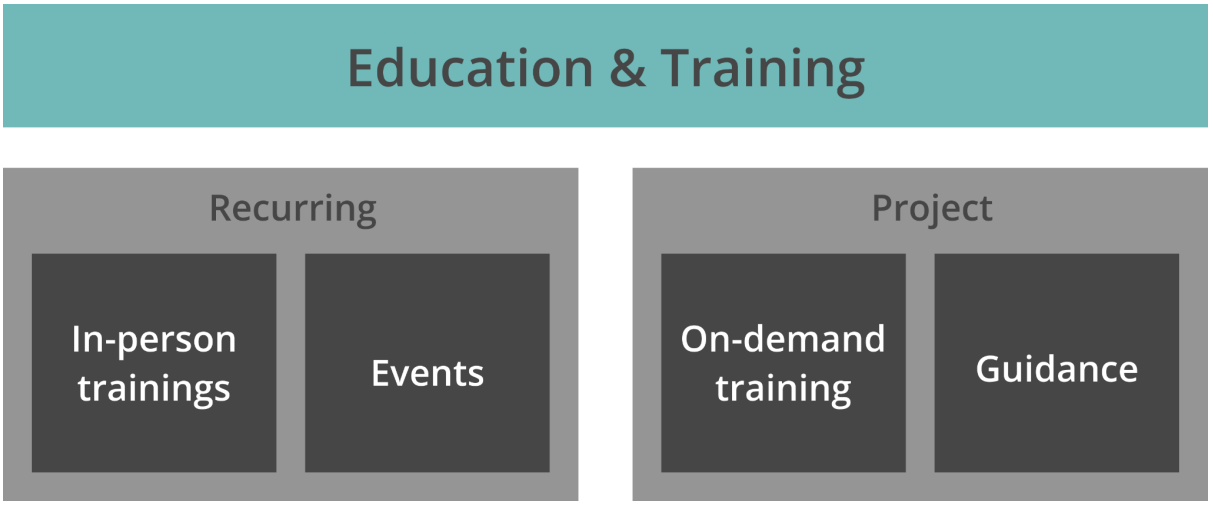
- April 2023
    - Complete initial draft infrastructure design for review.
    - Draft initial legal agreement and data governance process documents.
- May 2023
    - Complete test environment with the data management infrastructure.
    - Complete second draft of legal agreement and data governance process documents.
- June 2023
    - Complete the production environment for the data management infrastructure.
    - Complete the final draft of the legal agreement and data governance process documents.
    - Complete Awareness campaign for the SAMM Benchmarking initiative.
- July 2023
    - Start data collection using the new production infrastructure.
    - Design initial data visualizations and metrics.
- August 2023

    - Support the data management processes.
    - Refine the collection and analysis processes to streamline.
    - Create additional data visualizations and metrics.
- September 2023
    - Support the data management processes.
    - Refine the data visualizations and metrics.
    - Initial research findings from the gathered data.
- October 2023
    - Support the data management processes.
    - Finalize the data visualizations and metrics for the inaugural report.
    - Identify additional research findings from the data.
- November 2023
    - Support the data management processes.
    - Draft inaugural SAMM Benchmark State of Software Assurance Report
- December 2023
    - Support the data management processes.
    - Publish the SAMM Benchmark State of Software Assurance Report
- January 2024
    - Support the data management processes.
    - Define processes for data access and sharing.
- February 2024
    - Support the data management processes.
    - Document what is needed to enable similar data management capabilities for other OWASP projects.
- March 2024
    - Support the data management processes.

Education & Training Track

OWASP SAMM is an Application Security programme gaining momentum across organizations worldwide. Organizations like Microsoft, Zebra Technologies and others are either already using or considering SAMM. As SAMM is an umbrella project for - and advocate of - many other OWASP projects, it plays a key role in the promotion of the entire OWASP community.

However, SAMM comes with a challenging learning curve. By improving the educational delivery of the project we are convinced that we can create a success story not only for SAMM, but also for OWASP and all OWASP projects.



We've split the SAMM Education & Training track into 2 categories. In-person training and events are ongoing and recurring. For these, we need a budget to improve what we're already doing. On-demand training and Guidance can be considered projects themselves. Although we have a basis for both of them, we aim to formalize them and have a clear roadmap with defined phases, and the budget associated with those.

Education & Training Recurring aspects Roadmap

In-person Trainings

The SAMM Core team has been active in evangelizing the project by participating in and organizing SAMM Trainings at global events, including OWASP conferences. Unfortunately, the costs for travel and accommodation are not always fully covered by

the organizers. Smaller events that only charge a nominal fee for the training to the participants are especially impacted by this. This grant initiative would like to bridge that gap and make sure that SAMM trainers can rely on expense reimbursement.

What we plan

We will expand the in-person training to encompass smaller events. With 3 trainers, our goal is to run approximately 10 training sessions per year. That makes a total of 30 in-person training sessions per year.

What we need

Our 3 trainers are geographically spread across the US, Europe and New Zealand, providing opportunities to reach a global audience. Our estimated budget per training is $2000 on average, including flights and accommodation. We would also include paying trainers' opportunity cost, at 1000$ / day, to compensate for paid work they would forego.

Events

To evangelize SAMM, we need to create events and opportunities for SAMM experts, practitioners, and users to get together and share. The current initiatives fall short of making an impact. The monthly community calls we organize are not always convenient for everyone worldwide to join the call, since timing is inconvenient for Europe, Africa and Asia. The last SAMM User Days were organized in 2020. SAMM Core Team summit has been a huge success resulting in more progress over a weekend compared to the past couple of years.

What we plan

In addition to the current events (monthly online community calls and yearly SAMM Core Team summit) we would like to organize a bi-yearly SAMM User Day collocated with a security themed conference (e.g., OWASP SAMM Global AppSec). The goal of the User Day is to invite speakers to share their experiences with SAMM adoption.

What we need

Travel and accommodation budget for the core team members who will be helping with the organization of the User Day. 1500$ for flights and accommodation per person. We would expect 2-5 core team members attending each event.
Marketing / PR budget (1 man-month per event).

Education & Training Projects Roadmap

On-demand Trainings

An online self-study course for SAMM represents an opportunity to increase the project's reach towards the broader community. Here are a list of some benefits an online course would offer:

- Overcome the scaling limitations of in-person training
- Eliminate time constraints and cover SAMM activities in more depth
- Localization to reach a broader global audience
- Improved course quality by including several SAMM trainers
- Expansion of the SAMM guidance
- More reach since larger organizations can provide training to a greater number of key stakeholders tailored to their schedule

What we plan

We would like to create an online course based on the existing in-person training programme with a number of enhancements.

- Include at least 1 case study. Each case study will represent a specific organization profile. Throughout the course we would apply each SAMM activity to the case study in scope and provide concrete examples of how to realize a certain maturity level in a given security practice. We will provide a copy of a completed assessment as well as a phased roadmap as part of the course. Participants would be able to select the course that most closely aligns with their profile.
- We will incorporate pertinent OWASP flagship projects into the curriculum and integrate them into the broader AppSec framework. This will provide visibility and promotion for other projects.
- Each section of the course will have a set of questions designed to assess the understanding of the material covered.
- Our plan is to conduct an online exam and issue an official SAMM certificate upon completion. This will differentiate our course offerings from other non-authoritative providers.

While we plan on providing some introductory material free of charge, the full course will have a cost. We plan to charge 100$ for OWASP members and 150$ for non-members as a fee for the course. Based on an informal survey, we believe we will

have at least 100 to 300 paying users for this course. These estimates are based on an official certification, though.

Course contents

The course will consist of roughly 8 chapters.

1. Introduction to SDLC
2. Governance
3. Design
4. Implementation
5. Verification
6. Operations
7. Roadmap and improvements
8. Summary

Each chapter except for the summary will be approximately 2 to 3 hours long. Hence we expect to create approximately 24 hours of video footage.
Largely based on the first chapter, we will also create a free introductory course about 3 hours long. The course material will be split in small and easy to digest sections of at most 10 minutes each.

3-year plan

What we need

We will need about 15 hours of preparation, recording, and editing per every hour of recorded material.
A SaaS platform for hosting courses - who does OWASP recommend?
We will need about 1 PM for PR and marketing.
Graphic designer resource for visuals.
=> 4 PM in total.

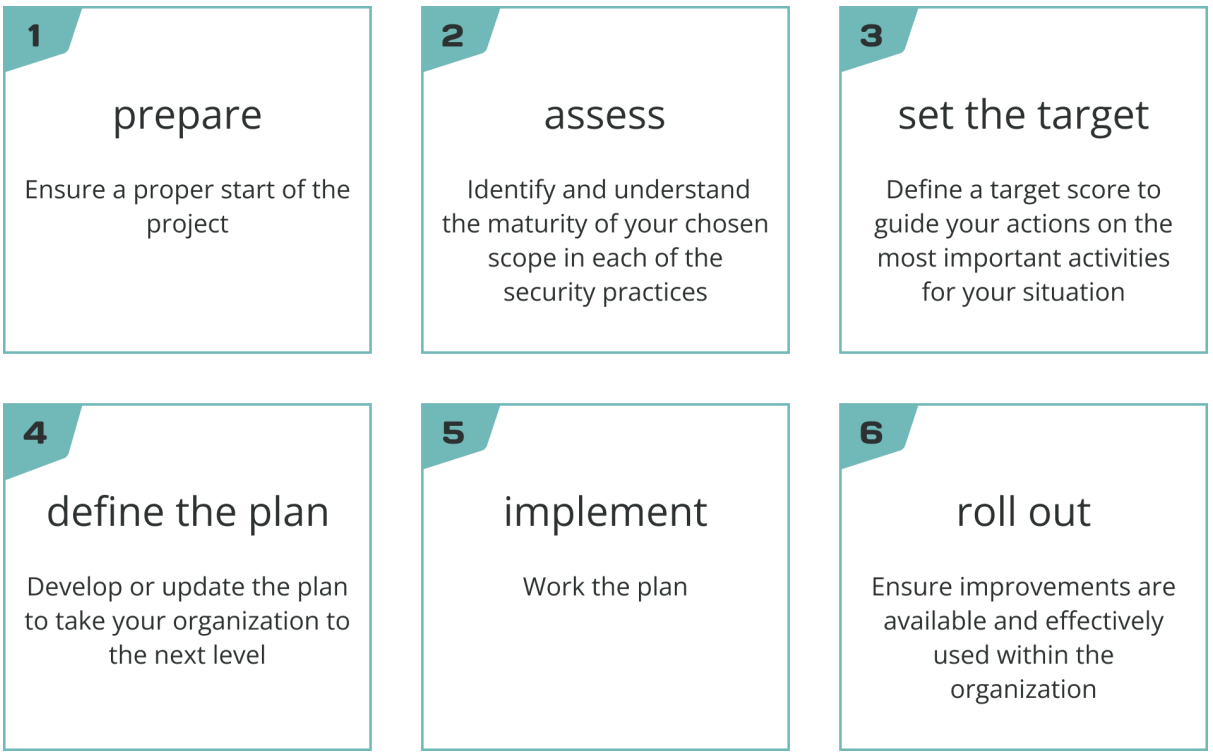
Guidance

Our website is the go-to place for SAMM users to seek references. Apart from having the model available there, we have a Getting Started guide and we've added Stream Guidance, including references to other OWASP projects.

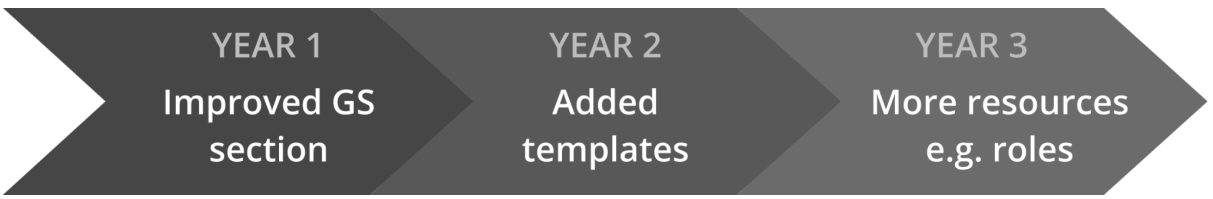
Our aim is to improve the Getting Started guide based on user questions and feedback, adding templates and other resources, and to continue to grow the Stream Guidance.

What we plan

We intend to improve the Getting Started section of the website, which provides clear steps for anyone in the early stages of SAMM adoption. This section also will also include valuable resources, even for experienced SAMM practitioners, such as Roles involved in each stage and templates.



3-year plan



What we need

- Design person hours
- Web development person hours
- Core team members person hours for content input

Supporting Roles

#DISCLAIMER: Market rates have been guesstimated by chatgpt 🙂
#DISCLAIMER: Efforts have been guesstimated and to be further refined with the whole group!

Glossary:
ROM PD = Rough Order of Magnitude estimate of PersonDays
BOE=basis of estimate

Title	**Responsibilities**	**Main deliverable**	**Market Rate (USD)**	**In-Person ROM PD**	**Events ROM PD**	**On-Demand ROM PD**	**Guidance ROM PD**	**Comments / BOE**
Project Manager	“Cat herding” a mix of paid and volunteer contributors against the goals described in this proposal	Dependable progress	70-140/hr	15	(N/A see first column)	(N/A see first column)	(N/A see first column)	4 tracks are relatively easy to manage in parallel as most of the same group will be involved.
Technical Writer (+part	Contribute with information architecture, editing and visuals for the training	Training materials	75-150/hr	50	25	200	N/A	m.patricia.duarte@gm...

visual design)	materials							
UX Writer + visual design + web dev	Design and implement the Getting Started section of the website	Getting Started section on the website	75-150/hr				160	
Marketing Specialist / Growth Expert	Helping the initiative to collect the maximum amount of contributions, and helping to ensure consistent contributions year over year. Preparing communications to a target audience with content in the right format to attract visitors and interaction.	Review of content, and manage external communications, building a PR network, posting content.	90-180/hr	10	10	10	10	john.kennedy@kenned...

Core Team Trainer	Deliver in-person training and talks. Present the content for the ondemand track.	Training	100-220/hr	30	10	40	N/A	

Communication Track

This document provides input to the SAMM Grant request for 2023

Summary

OWASP SAMM is an Application Security program and plays a key role in promoting best practices to a growing community of users and interested parties globally, at a time of heightened security awareness. SAMM as an open source program has a mission to provide an effective and measurable way for organizations to analyze and improve their secure development lifecycle (SDLC).

SAMM supports the complete software lifecycle and is technology and process agnostic, a message that needs to be communicated and elevated to a wider audience than SAMM is presently touching. But this needs to be developed into a two way conversation, where the SAMM best practices can reach a wider audience, building authority in SAMM. And at the same time the community through outreach can actively contribute to the development of the program, what it offers and how it is used.

However SAMM comes with a challenge, to be able to be heard in the crowded security marketplace that we experience today, SAMM needs to build its authority and appetite to present a faster momentum for change by being more dynamic with the community that supports it.

SAMM is an open framework, free for organizations to use for software security assurance, we want to remain as the “go to” source for information on security practices.

With regards application security we are convinced that this project could create awareness not just for SAMM, but also for OWASP. The number of followers amongst the SAMM social networks is growing, visitors to the corporate website increase month on month and feedback from the monthly Community calls is very positive.

We want to elevate our communication and messaging to meet the needs of the SAMM community and visitors to the website, to understand more about what users want from SAMM and provide information in the format that is most easy to digest for the community.

In the context of this initiative we would like to propose 2 complementary tracks for improving the communication aspects of SAMM:

- SAMM quarterly user survey;
- SAMM annual “State of the Nation” report;

Project deliverables

Quarterly user survey

- Get a clear understanding of the pains and challenges of the community of users
- Understand who our audience are and how they find information and use it
- Generate insights on the type of companies and organizations that are interested / using SAMM
- Build on the OWASP SAMM 2022 survey that we did to generate more value for users
- Get an unbiased view on how SAMM can improve its communication, messaging, tone, etc.

State of the Nation report

- Collate data, prepare a report based on the quarterly survey and publish an annual report with commentary around SAMM/ AppSec, etc.

Budget

What resources do you need to create these deliverables?
- Survey, forum, 1:1 interviews
- Technical writer to prepare an annual report

What are the related estimated costs in terms of people and/or tools?
- There are tools that can be used for doing the survey
- Skill is in doing more in-depth interviews to dig more into "technical" needs

- Plus graphics, design, copywriting of a "state of the nation" report

Assume that we can get what we ask - how can we speed up our SAMM project?
We will establish a 3-year funding objective based on the project's needs and break it down into quarterly and annual targets for the next three years.

What are the steps to achieve the project of securing funding for the OWASP SAMM project, with estimated milestones and costs in man-days and USD:

Budget - about $35K
Preparing survey, sending out the survey, collating results, analyzing and providing a commentary.

- Software costs i.e. surveymonkey $1000 - 2000
- Preparation (data prep, emailing, survey set-up, question setting, data collection, creating a report, publishing and any 1:1 interviews) $2000 x 4 = Total approx $8,000
- Frequency 4x times per year on a quarterly basis
- Total approx $10,000

Preparing a “State of the Nation” report, collating results, analyzing and providing a summary of trends and findings.

- Software costs i.e. use of indesign files or equivalent $2000 - 3000
- UX design and layout of a report $2000
- Prepare a summary report of findings and trends $5000
- Technical writer to articulate findings in a way suitable for the target audience $5000
- Publish and post report findings $3000
- Send out to a targeted media list / audience of industry specialists $3000
- Ongoing outreach to get backlinks and discussion around the report $4000
- Total approx $25,000

Overall cost estimate for Communications: Total approx $35,000

Translations Track

This portion of the funding grant is focused on the translation of the OWASP SAMM materials into different languages in order to maximize reachability and coverage throughout the world. Indeed, the success of the model is dependent on the availability of different languages to facilitate adoption. Languages that typically are important to cover include Spanish, Portuguese, French, German, Chinese, Japanese, and so forth.

The internationalization of the model is a complex endeavor. We need to support different model versions in different languages, and this impacts several linked artifacts (e.g., the model on the website, the assessment sheets, the PDF, the website itself, …). Language readiness and uptake can have (and currently has) different speeds depending on the availability of translators. By professionalizing this, we will be able to better align the translation efforts, and further extend the coverage of translation (currently only translation of the model itself is being looked into). For this matter, extra monetary support will help us reach these goals.

We see the following tasks to part of the grant

- Translation manager
    - A person responsible for managing the translation of the model in all its aspects and to make sure that translations are available and timely.
    - Estimated time: 1d/w during active translation periods ; 1d/m otherwise
- Translation (fullstack) engineer
    - A technical profile that is very familiar with Github, CrowdIn and other relevant technologies to perform and maintain the translation setup and automate as much as possible all relevant tasks (upload of new model versions, filtering relevant translation content, auto-generating artifacts from the translated content, …)
    - Estimated time: 30 MD initially + 5MD for new model versions
- Actual translation and QA of the core model to (at least) 10 languages
    - Approach defined
    - Translation of 1 model version into 1 language is approx. 5000 USD (so translating 1 model version in 10 languages is 50K USD) ; separate time for QA is needed.
- Actual translation and QA of other artifacts, including website/guidance/… for different languages
    - Approach to be looked into
    - Effort unclear
- Adaptation of the website to support internationalization
    - Estimated time: 10 MD

Budget

Current estimated budget is

Translations core model = 64,000 USD (10 languages)

Translations web site = 30,000 USD (10 languages)
Translations management and integration: 30,000 USD
= 124,000 USD

Overview of tasks

- Translation of core model for 10 languages (current version) -
    - Approach defined
    - 5 words = 1 USD (32K words 6.400 USD per language)
- Translation of website/guidance for 10 languages (current version)
    - Approach to be looked into (estimate half of the words = 3,000 USD per language)
- Continued translation ?
- Translation manager
    - 20 man days = 20,000 USD
- Integration in website
- PDF generation

Funding Track

This portion of the grant is dedicated to securing funding to support both a portion of this grant itself and the operational expenses of the OWASP SAMM project.

Seba and Bart, the SAMM Product Owners, are responsible for attracting sponsors for the project. Currently, the SAMM project has a number of sponsors, as outlined in the sponsor brochure available here: https://owaspsamm.org/sponsors/.

Estimated outcome: An Account Executive and SDR should generate at least 4 times their cost as of year 2. We aim for an income of $200.000 in year 1 (Q2-Q4). And $600.000 as of year 2.

We will need to integrate this with the OWASP sponsor process and align with the yearly SAMM User Days.

While we anticipate that some of the grant costs will be covered through project sponsors, it is unlikely that all expenses will be covered. To maximize sponsorship income, we will establish a sponsorship process and hire a Sponsor Account Executive (SAE) and a Sponsor Development Representative (SDR) (on a part-time basis, we might also consider a portion of the enumeration to depend on getting the target sponsorship budget). We will also implement a Sponsor Relationship Management tool (a CRM).

We will establish a 3-year funding objective based on the project's needs and break it down into quarterly and annual targets for the next three years. We will evaluate and adjust the sponsor options available to the project to meet our funding objectives.

In addition, we will define the responsibilities of the SAE and SDR and conduct a search for qualified candidates to fill this role. Lastly, we will select and configure a Sponsor Relationship Management tool and process to support SAMM sponsorship activities.

Here are the steps to achieve the project of securing funding for the OWASP SAMM project, with estimated milestones and costs in man-days and USD:

- Define the 3-year funding objective and break it down into quarterly and annual targets - Estimated time: 5 man-days, Estimated cost: $5,000
- Analyze and restructure the sponsor options for the project to meet funding objectives - Estimated time: 5 man-days, Estimated cost: $5,000
- Define the roles of SAE and SDR and conduct a search for qualified candidates - Estimated time: 5 man-days, Estimated cost: $5,000

- Hire the roles - Estimated time: 3 man-days, Estimated cost: $3,000
- Develop a sponsorship process - Estimated time: 10 man-days, Estimated cost: $10,000
- Select and set up a Sponsor Relationship Management tool and process - Estimated time: 5 man-days, Estimated cost: $5,000
- Launch the sponsorship process per quarter - Estimated time: 30 man-days, Estimated cost: $15,000
- Monitor and evaluate the sponsorship program quarterly - Estimated time: 9 man-days, Estimated cost: $9,000
- Total estimated time to start (1 quarter) and run for 3 quarters: 150 man-days, Total estimated cost: $150,000

Milestones:

- Definition of funding objectives and restructuring of sponsor options: End of Month 1
- Hiring of the roles: End of Month 2
- Development of sponsorship process and set up of Sponsor Relationship Management tool: End of Month 3
- Launch of the sponsorship process: Q2-Q4
- Monitoring and evaluation of the sponsorship program: Ongoing quarterly as of Q2

Note that these estimates are rough and may vary depending on the specific circumstances of the project, as well as the availability and qualifications of the Sponsor Account Executive and Sponsor Development Representative.

Other tracks

Website

The goal of the website is to be the source of information for SAMM and to bring people to the community, increasing SAMM adoption.

The objective for 2023 is to update the website, improving its usability and adding more value, interacting with other tracks in many cases. Some of the tasks include:

- revamp of visual design
- improvement of sections (e.g. Getting Started)
- new sections (e.g. Resources, Team)
- Model translations

PDF

The PDF version of SAMM is something many users have requested. We finally got a professional-looking version out in 2022. To cater to our users' needs, we want to have at least one more version of the document, in line with widely used standards.

Core

Though there are no plans for major changes in the core model, there are some improvements we are already considering. These include making the tone and vocabulary more cohesive and adding a glossary.

Toolkit

Some of the goals for the track regarding SAMM tools are

- Getting away from proprietary tools
- Having a web app supported by the team with dedicated developers
- Creating a dashboard
- Having our tools connected to the benchmark track

Mappings

In 2022 we worked hard on delivering the SAMM-NIST SSDF mapping. This is of great value to our community and we want to continue creating these mappings.