

The background features a stylized landscape. At the top, a large yellow sun is centered in a purple sky. To the left, there are white clouds and several black birds in flight. To the right, there are more white clouds. Below the sun, the text 'S3M2' is written in a bold, dark blue font. Underneath that, the full name 'Scalable Software Security Maturity Model' is written in a smaller, dark blue font. In the center of the image, a purple location pin icon is positioned above a road. The road is dark grey with white dashed lines, leading from the bottom center towards the location pin. The road is flanked by a purple field with a dark green border.

S3M2

Scalable Software Security Maturity Model

S3M2 – Overview

- The Purple Book Community's Scalable Software Security Maturity Model (S3M2) is a framework designed to help organizations assess and improve their software security practices. It provides a structured approach to measuring and enhancing an organization's maturity in software security, focusing on scalability and community collaboration.
- S3M2 emphasizes scalability and community collaboration, meaning it aims to provide a framework that can be adapted and applied to organizations of different sizes and industries. It also encourages organizations to engage with the software security community, share knowledge, and leverage collective expertise to enhance their security practices.
- The materials from these slides was presented in 3 workshops in the 2023 AppSecCon event on June 29, 2023 as Version .5 of the model to gain community awareness and access to the model. If you are interested in joining the efforts to evolve the model and help with improving software security across the globe, please visit <https://www.thepurplebook.club/s3m2>



S3M2 – Applying the Model

To begin, [download this worksheet](#) to record your results and gain a visual representation of your current state of the software security practices.

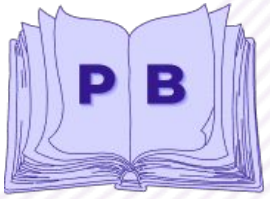
S3M2 is broken down into three major categories with a varied number of sub-categories within them, and 5 levels of maturity defined on each category, as defined on Slide 4:

- **People** – Relates to the people aspect of software development organizations and addresses the needs for awareness, training, and Security Champions.
- **Process** – Describes the relative maturity across internal processes to address software security.
- **Technology** – Covers the selection, procurement, and use of software security and DevOps tools to help operate and report on the effectiveness of a software security program.

To use the model, review each of the summary slides (slides 6, 8, 10, and 11) and check off the attributes along each row that best describes the state of each sub category for your software security practices. Review the row and select the column that best represents the state of your program. Record that value (1-5) on the spreadsheet linked on this page.

At the end of your review and transfer of maturity levels you determined, you'll see a Radar Chart that will dynamically change as you add or update data. You can also use this chart for planning future iterations of your program by determining which attributes are needed to advance to the next level. These will serve as a roadmap for improvements to your program.





Purple Book
Community

S3M2: Section Summaries



Purple Book
Community

AppSecCon 2023

S3M2 – Maturity Level Overview

Dimension	Level 1 Reactive	Level 2 Proactive	Level 3 Managed	Level 4 Optimized	Level 5 Dynamic
	Basic visibility from Ad Hoc tool execution	Prioritization of remediation efforts, automated tool execution	Processes are defined and policies followed	Processes are optimized and automated	Adaptive AppSec (e.g. Threat modeling)
People					
Process					
Technology					



Purple Book
Community

People

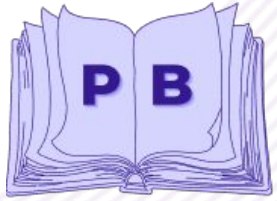


Purple Book
Community

People Section Summary

Dimension	Level 1 Reactive	Level 2 Proactive	Level 3 Managed	Level 4 Optimized	Level 5 Dynamic	Your Rating (1-5)
	Basic Visibility from Ad Hoc tool execution	Prioritization of remediation efforts, automated tool execution	Processes are defined and policies followed	Processes are optimized and automated	Adaptive AppSec (e.g. Threat modeling)	
People / Personas	<ul style="list-style-type: none"> <input type="checkbox"/> Developer led (volunteer program) <input type="checkbox"/> No dedicated software security resources <input type="checkbox"/> No organizational mandate 	<ul style="list-style-type: none"> <input type="checkbox"/> Dedicated AppSec resources 	<ul style="list-style-type: none"> <input type="checkbox"/> Security Champion program. <input type="checkbox"/> Security champions present on every development team 	<ul style="list-style-type: none"> <input type="checkbox"/> Security champions (if present) Community Formed and Operating 	<ul style="list-style-type: none"> <input type="checkbox"/> Security leads/champions contribute reusable code for remediations <input type="checkbox"/> Best practices are documented for sharing across all development efforts 	
Training and Education	<ul style="list-style-type: none"> <input type="checkbox"/> No program in place <input type="checkbox"/> No mandate from the upper management or leadership 	<ul style="list-style-type: none"> <input type="checkbox"/> Some foundational / introductory training. 	<ul style="list-style-type: none"> <input type="checkbox"/> Role-based training introduced. <input type="checkbox"/> Training program needs to account for the identification of security champions 	<ul style="list-style-type: none"> <input type="checkbox"/> Role-based training refined and metrics collected <input type="checkbox"/> Refresher training introduced. <input type="checkbox"/> Badge of honor issue <input type="checkbox"/> Just-in-Time contextual training. <input type="checkbox"/> Customized CTFs (Capture the Flag) 	<ul style="list-style-type: none"> <input type="checkbox"/> Advanced degree/certification encouraged and sponsored. <input type="checkbox"/> Refresher training expanded. 	
Security Champions Program	<ul style="list-style-type: none"> <input type="checkbox"/> No program in place <input type="checkbox"/> No mandate from the upper management or leadership 	<ul style="list-style-type: none"> <input type="checkbox"/> Ad-hoc appearance of security leads. 	<ul style="list-style-type: none"> <input type="checkbox"/> Security Champions are formalized as part of the program. 	<ul style="list-style-type: none"> <input type="checkbox"/> Community / Network of Security Champions is functioning 	<ul style="list-style-type: none"> <input type="checkbox"/> Active contribution from Security Champions <input type="checkbox"/> Reusable Code, Best Practices and Standards. 	
Software Security Awareness	<ul style="list-style-type: none"> <input type="checkbox"/> No program in place <input type="checkbox"/> No mandate from the upper management or leadership 	<ul style="list-style-type: none"> <input type="checkbox"/> Initial / generic security awareness training rolled out 	<ul style="list-style-type: none"> <input type="checkbox"/> Development of tailor-made, role-specific security awareness 	<ul style="list-style-type: none"> <input type="checkbox"/> Exercises - CTFs <input type="checkbox"/> Cyber-ranges <input type="checkbox"/> Guest speakers from the industry <input type="checkbox"/> Brown bags, <input type="checkbox"/> Regular communication channels established. <input type="checkbox"/> Issuing security advisories / bulletins <input type="checkbox"/> Discussions about security breaches are common 	<ul style="list-style-type: none"> <input type="checkbox"/> The Security Champions become the program! 	





Purple Book
Community

Process

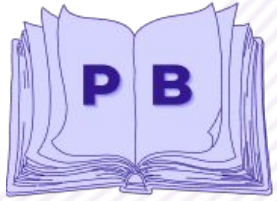


Purple Book
Community

Process Section Summary

Dimension	Level 1 Reactive	Level 2 Proactive	Level 3 Managed	Level 4 Optimized	Level 5 Dynamic	Your Rating (1-5)
	Basic Visibility from Ad Hoc tool execution	Prioritization of remediation efforts, automated tool execution	Processes are defined and policies followed	Processes are optimized and automated	Adaptive AppSec (e.g. Threat modeling)	
Governance	❑ Totally reactive, fighting fires	❑ Focus on finding 'low hanging fruit' external attack vulnerabilities	❑ Governance policies (SLAs) and risk methodology defined	❑ Automated gates to control push to production	❑ Data driven decision making process to drive feedback to improve the workflow	
Asset Inventory and Categorization	❑ Inconsistent tracked inventory, limited thought process and planning	❑ Partial Asset Inventory. Effort continues towards automation	❑ Complete portfolio visibility	❑ Partial Asset Inventory. Effort continues towards automation	❑ 100% correlation with asset inventory systems of record and business functions	
Prioritization	❑ Usual approach is to fight the fire, every single time as a snowflake	❑ Prioritization is done using the scanning solution	❑ Internal application's business context is used for prioritization	❑ Prioritization is done using the scanning solution	❑ Ongoing threat modeling drives updates to prioritization	
Remediation	❑ No established strategy, no established guidance	❑ SLAs defined, strategizing remediation activities, not strictly enforced, not universally applied	❑ Established formalized strategy for remediation with rigor and policy compliance	❑ Enforce SLA compliance to drive down MTTR, also leveraging and integration Threat Intel feeds	❑ Ongoing threat modeling drives updates to prioritization	
Security Debt	❑ No visibility into the technical debt	❑ There is a visibility into the technical debt, but the much needed focus does not exist	❑ Visibility, All new debt is managed/under control aka " <u>stop the bleeding</u> "	❑ Visibility, Debt significantly reduced/managed + new under control	❑ acceptance of prioritization of debt reduction as part of backlog	
Metrics	❑ Reporting done on an ad-hoc basis, not an ideal and usually prone to human error	❑ Reporting done on an ad-hoc basis, not an ideal and usually prone to human error	❑ Consolidation of reporting of security posture on a regular basis	❑ Reporting/Dashboarding "on demand" + self service for specific roles	❑ Operationalizing tool selection/optimization/rationalization	





Purple Book
Community

Technology



Purple Book
Community

Technology Tool Summary

Dimension	Level 1 Reactive	Level 2 Proactive	Level 3 Managed	Level 4 Optimized	Level 5 Dynamic	Your Rating (1-5)
	Basic Visibility from Adhoc tool execution	Prioritization of remediation efforts. Automated tool execution.	Processes are defined and policies followed	Processes are optimized and automated	Adaptive AppSec (Threat modelling etc)	
Tool portfolio/ security stack	<ul style="list-style-type: none"> <input type="checkbox"/> Tools are Open-Source non-enterprise versions (no paid support, all functions not available) <input type="checkbox"/> Usage of SCA tools on high value applications <input type="checkbox"/> Usage of SAST on high value apps (no automation) <input type="checkbox"/> Start of usage of Code Coverage tools <input type="checkbox"/> Lack of Testing tools, lack of testing regime (Ad hoc) 	<ul style="list-style-type: none"> <input type="checkbox"/> Paid Licenses on primary tools. <input type="checkbox"/> Visibility into tools for SCA, SAST, PenTesting, Secrets Detection <input type="checkbox"/> Mandated tool sets without App Teams input creating usability issues. <input type="checkbox"/> Use of CIS hardening Standards <input type="checkbox"/> Use of Security Framework and Libraries <input type="checkbox"/> Use of Testing tools, start of formalizing of testing Regime. <input type="checkbox"/> Start/planning of formal asset catalog. 	<ul style="list-style-type: none"> <input type="checkbox"/> Use of Security Frameworks and Libraries <input type="checkbox"/> Track Dependency tools for 3rd party code <input type="checkbox"/> Infrastructure as code, and automation of deployment <input type="checkbox"/> Risk management tool <input type="checkbox"/> Automated bug tracking <input type="checkbox"/> Tools for tracking dependency in 3rd party code <input type="checkbox"/> Tools for Identification/classification of data <input type="checkbox"/> Normalization of tools for development/testing 	<ul style="list-style-type: none"> <input type="checkbox"/> Strict Policy Enforcement <input type="checkbox"/> Mix of testing methods <input type="checkbox"/> Automation of risk management <input type="checkbox"/> Attack Surface Management <input type="checkbox"/> Threat Model workflow <input type="checkbox"/> Standardized Vulnerabilities/Risk/Findings actively managed 	<ul style="list-style-type: none"> <input type="checkbox"/> Automated Remediation (SOAR) <input type="checkbox"/> Automated policy enforcement <input type="checkbox"/> Orchestration of testing/development process 	

Technology Secure Design Summary

Dimension	Level 1 Reactive	Level 2 Proactive	Level 3 Managed	Level 4 Optimized	Level 5 Dynamic	Your Rating (1-5)
	Basic Visibility from Adhoc tool execution	Prioritization of remediation efforts. Automated tool execution.	Processes are defined and policies followed	Processes are optimized and automated	Adaptive AppSec (Threat modelling etc)	
Secure Design	<ul style="list-style-type: none"> <input type="checkbox"/> No specific and dedicated secure design practices <input type="checkbox"/> Adhoc threat modeling, if it occurs <input type="checkbox"/> Constrained by Developers knowledge base <input type="checkbox"/> Security requirements reactive 	<p>Prioritization of remediation efforts. Automated tool execution.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Basic threat modelling for critical designs/applications. <input type="checkbox"/> The model document will be any convenient form (data flow diagram with attacks and mitigations, picture of white board, etc.) <input type="checkbox"/> There will typically be significant secure design expertise gaps and lack of coverage. 	<ul style="list-style-type: none"> <input type="checkbox"/> Complex and security critical designs must have a threat model. the security requirements from the model are prioritized and built. <input type="checkbox"/> There is a process for engaging secure design expertise. threat modelling is required for security significant changes. <input type="checkbox"/> KPIs will be introduced. <input type="checkbox"/> Secure design expertise is available at least critical design work. <input type="checkbox"/> Security requirements are validated Training program needs to account for the identification of security champions 	<ul style="list-style-type: none"> <input type="checkbox"/> Trainings occur at predictable periodicity. <input type="checkbox"/> There is a standard model document form and modelling methodology. Governance ensures model quality and completeness. <input type="checkbox"/> Security requirement validation must be included in test regime. <input type="checkbox"/> Modelling is widely adopted (nearly all teams), with modelling and design expertise readily available. <input type="checkbox"/> There are secure design patterns, checklists, or standards. modelling is required for security significant changes. <input type="checkbox"/> There is a risk rating methodology. <input type="checkbox"/> There is a way to protect models and to archive them. <input type="checkbox"/> Models are used as a critical input to design decisions 	<ul style="list-style-type: none"> <input type="checkbox"/> Levels of secure design skill: leaders, practitioners, and those who are learning. <input type="checkbox"/> Every development effort/team practices secure design: threat modelling happens as an organic part of the development process. <input type="checkbox"/> Models go through a governance review to ensure quality. There may be automation applied to modeling. <input type="checkbox"/> Models are documented and available influence security decisions during design sessions. <input type="checkbox"/> Penetration test/bug bounty/test regime findings help refine threat models 	