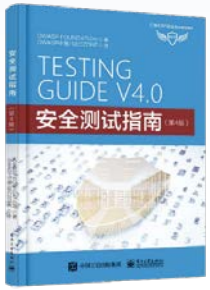
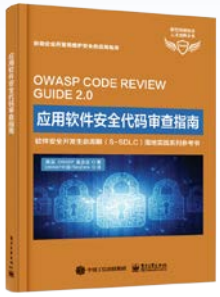
OWASP
Open Web Application
Security Project

OWASP SAMM v2.0
软件保障成熟度模型解析

王颉

关于我





王颉

- 英国拉夫堡大学网络安全博士
- 开源网安副总经理
- 致力于应用安全与软件安全开发理念和技术的推广
- OWASP中国副主席
- OWASP+OWASP China (2009-Now)
  - ✓ OWASP Top 10 2017, 2013, 2010
  - ✓ OWASP Secure Coding Practices - Quick Reference Guide
  - ✓ OWASP ASVS
  - ✓ OWASP Testing Guide
  - ✓ OWASP Code Review Guide
  - ✓ ……

https://www.owasp.org/index.php/User:Jie_Wang

OWASP
Open Web Application Security Project

Open Web Application Security Project

SAMM的背景

发展历程

2009年
V1.0

2016年
V1.1.1

2017年
V1.5

2020年
V2.0

OWASP
Open Web Application
Security Project

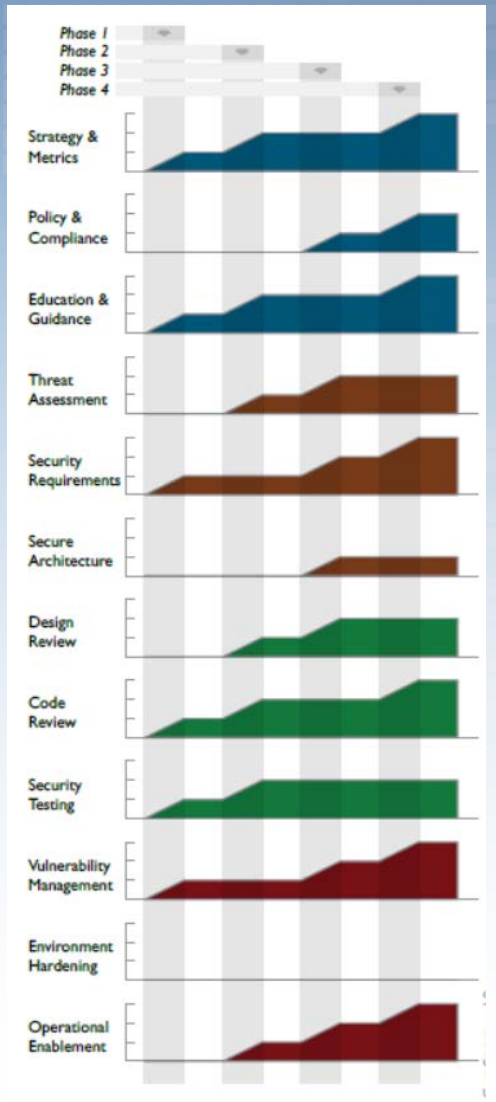
Open Web Application Security Project

什么是“SAMM”?

- SAMM是“Software Assurance Maturity Model”的英文缩写。
- SAMM是一个规范性模型，是一个易于使用、完全定义和可测量的开放框架。

用处

- 评估组织机构当前的软件安全开发能力成熟度。
- 规划组织机构的软件安全开发计划，定义软件安全开发实践。
- 展示组织机构软件安全开发计划的改进态势。
- 适用于瀑布开发和敏捷开发模式下的。



来源：OWASP SAMM v1.0

OWASP
Open Web Application Security Project

用户评价

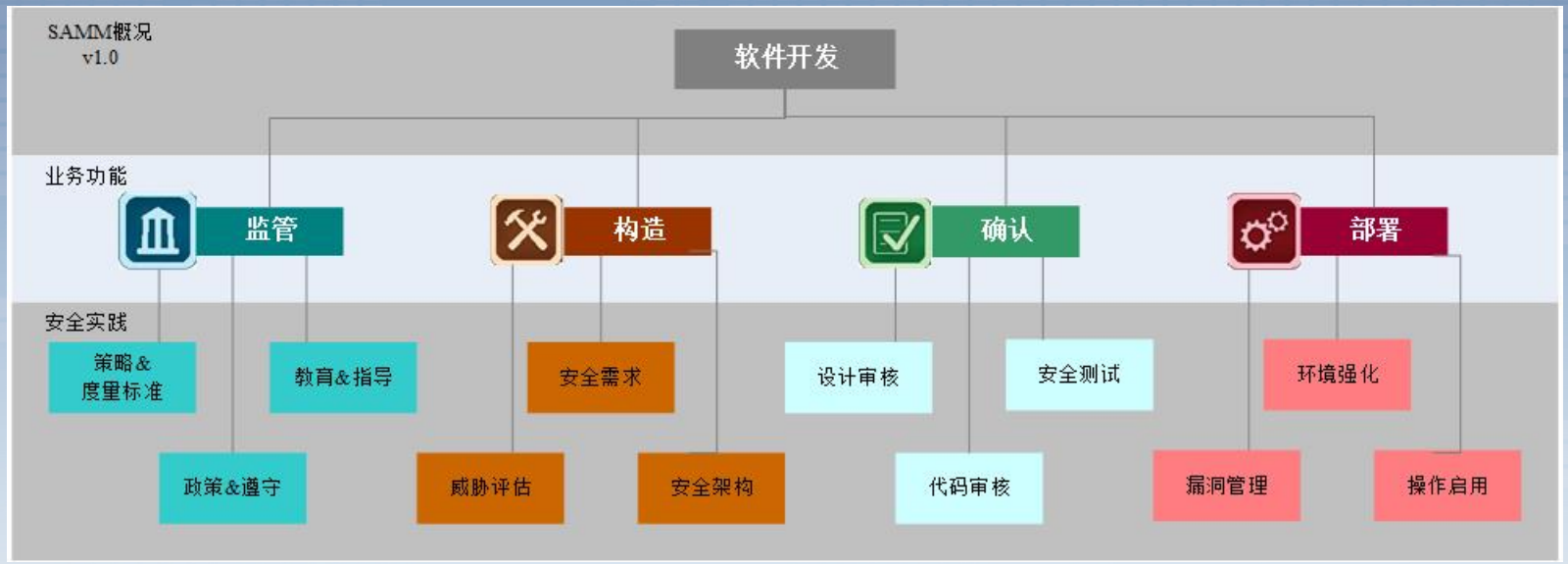
Dell uses OWASP's Software Assurance Maturity Model (OWASP SAMM) to help focus our resources and determine which components of our secure application development program to prioritize.

——Michael J. Craigue

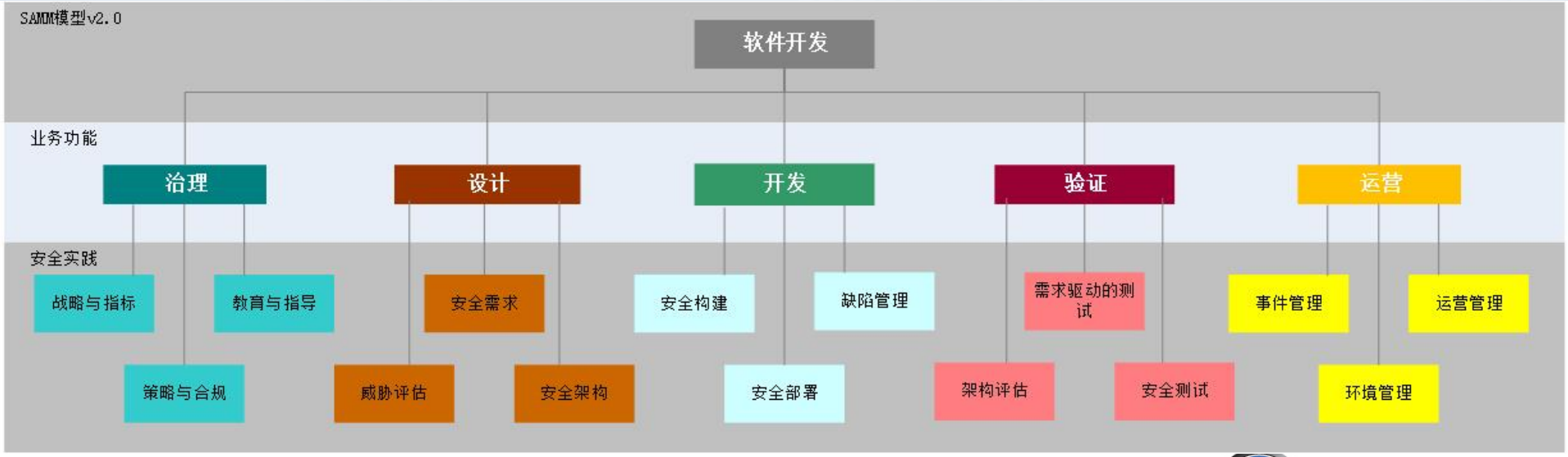
Information Security & Compliance, Dell, Inc

Open Web Application Security Project

SAMM核心模型

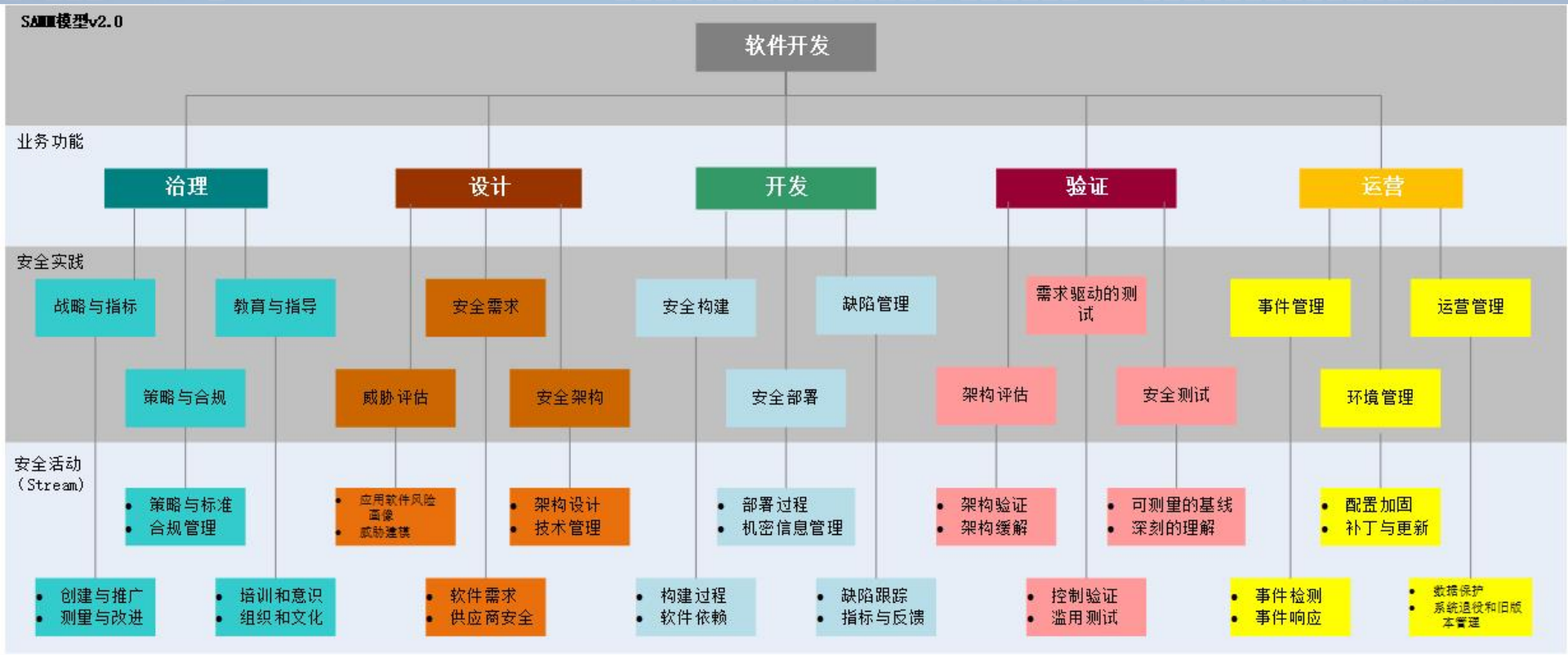


SAMM v1.0/v1.5模型



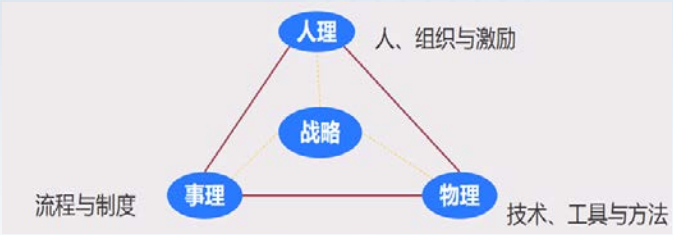
SAMM v2.0模型

OWASP
Open Web Application Security Project



OWASP
Open Web Application Security Project

成熟度等级评估的维度



WSR系统工程方法论

安全开发实践维度
- 人员
- 工具
- 规范
- 实践

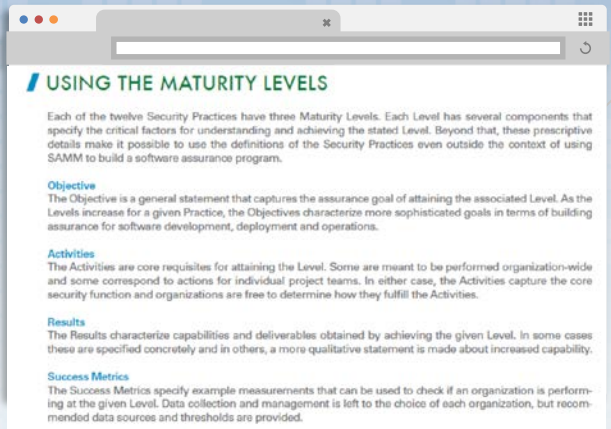
组织机构治理维度
- 战略与指标
- 策略与合规
- 组织与文化

安全开发能力成熟度

OWASP
Open Web Application Security Project

SAMM的成熟度等级

- 设置了3个成熟度等级；并与CMMI的5个级别大致对应



USING THE MATURITY LEVELS

Each of the twelve Security Practices have three Maturity Levels. Each Level has several components that specify the critical factors for understanding and achieving the stated Level. Beyond that, these prescriptive details make it possible to use the definitions of the Security Practices even outside the context of using SAMM to build a software assurance program.

Objective
The Objective is a general statement that captures the assurance goal of attaining the associated Level. As the Levels increase for a given Practice, the Objectives characterize more sophisticated goals in terms of building assurance for software development, deployment and operations.

Activities
The Activities are core requisites for attaining the Level. Some are meant to be performed organization-wide and some correspond to actions for individual project teams. In either case, the Activities capture the core security function and organizations are free to determine how they fulfill the Activities.

Results
The Results characterize capabilities and deliverables obtained by achieving the given Level. In some cases these are specified concretely and in others, a more qualitative statement is made about increased capability.

Success Metrics
The Success Metrics specify example measurements that can be used to check if an organization is performing at the given Level. Data collection and management is left to the choice of each organization, but recommended data sources and thresholds are provided.

隐藏起点，即，安全开发实践没有实现时

对安全开发实践有了初步了解并有了一定的执行

安全开发实践的执行被提高了效率和有效性

安全开发实践得到了综合性的全面落地

OWASP SAMM	CMMI
第1级	能力级别1—非正式执行
	能力级别2—计划跟踪（部分）
第2级	能力级别2—计划跟踪（完整）
	能力级别3—充分定义
第3级	能力级别4—量化控制
	能力级别5—持续优化

1.3 教育与指导

成熟度等级		活动流A 培训和意识	活动流B 组织和文化
1级	为员工提供有关安全开发和部署主题的可访问资源。	为所有软件开发涉及的人员提供安全意识培训。	在每个开发团队中确定一个“安全专家（Security Champion）”。
2级	对软件生命周期中的所有人员提供有关安全开发技术和针对特定角色指导的教育。	提供技术和特定角色的指导，包括每种语言和平台的安全细微差别。	开发一个安全软件中心，以显著促进开发人员和架构师的思想领导力。
3级	开发由不同团队开发人员共同推动的内部培训计划。	围绕组织的安全软件开发标准形成标准化的内部指导。	建立一个软件安全社区，包含所有参与软件安全的组织内部人员。

培训和意识—成熟度等级1

- **收益**

所有相关员工的基本安全意识。

- **活动**

对当前参与软件管理、开发、测试、审计的所有角色进行安全意识培训。目的是提高人们对应用软件安全威胁和风险、安全最佳实践以及安全软件设计原则的认识。在组织内部创建培训，或从外部购买培训。理想情况下，应提供面对面的培训，以便参与者可以进行小组讨论，但是也可以选择基于计算机的上机培训。

- **问题**

您是否要求涉及应用软件开发的员工接受SDLC培训？

- **质量标准**

① 培训是可重复的、持续的，并且对任何参与软件开发生命周期的人员都可用。
② 培训在适当的情况下包括最新的OWASP Top 10，并包括诸如最低权限、纵深防御、安全故障保护、完全消减、会话管理，开放式设计和心理接受性的概念。
③ 培训需要参加者的签字或确认。
④ 您在最近12个月内更新了培训。
⑤ 在员工入职过程中提供了培训。

- **回答**

① 没有；
② 是的，要求其中一些；
③ 是的，要求至少有一半；
④ 是的，要求大多数或全部。

培训和意识—成熟度等级2

- **收益**

根据员工的具体角色对相关员工角色进行培训。

- **活动**

从核心开发团队开始，针对组织的角色和技术进行讲师授课或上机实操安全培训。组织根据每个小组的技术需求为产品经理、软件开发人员、测试人员和安全审核员定制培训。

- 产品经理对与SAMM业务功能和安全实践相关的主题进行培训，重点是安全需求、威胁建模和缺陷跟踪。
- 开发人员对其使用的技术进行编码规范和最佳实践方面进行培训，以确保培训直接有益于应用软件安全。他们对OWASP Top 10安全脆弱点或类似弱点相关的技术和使用的框架（如：移动应用）、以及对每个问题最常见的消除策略，具有扎实的技术理解。
- 测试人员对组织中使用的不同测试工具、相关技术的最佳实践、以及识别安全缺陷的工具进行培训。
- 安全审核员对软件开发生命周期、组织中使用的应用软件安全机制、以及提交安全缺陷进行修复的过程进行培训。
- 安全专家对SDLC各个阶段的安全主题进行培训。他们接受与开发人员和测试人员相同的培训，但也了解威胁建模和安全设计以及可以集成到构建环境中的安全工具和技术。

- **问题**

培训是否对不同角色（如：开发人员、测试人员或安全专家）进行量身定制？

- **质量标准**

① 培训包括“成熟度等级1”中的所有培训主题，并增加了其他特定的工具、技术和演示；
② 所有员工和承包商都必须参加培训；
③ 培训包括组织内部专家和受训人员的输入信息；
④ 培训包括组织内部开发的工具和技术演示；
⑤ 使用培训反馈信息对培训进行优化。

- **回答**

① 没有；
② 是的，对于一些培训；
③ 是的，对于至少一半的培训；
④ 是的，对于大多数或所有培训。

培训和意识—成熟度等级3

- **收益**

在员工执行关键任务前，确保员工具有足够的安全知识。

- **活动**

实施正式的培训计划，该计划要求与软件开发生命周期有关的任何人员在入职过程中完成适当的角色和特定于技术的培训。根据应用软件的重要性和用户角色，考虑限制员工的访问权限，直到完成入门培训为止。尽管组织可以从外部获取一些培训模块，但该计划是在内部进行促进和管理的，并且包括特定于组织的内容，而这些内容超出了常规的安全最佳实践。该计划具有明确的课程表、参训人员参与情况检查，并对学习内容的理解和掌握能力进行测试。培训内容由行业最佳实践和组织内部标准组成，包括对组织使用的特定系统进行培训。

- **问题**

您是否配备了一个学习管理系统或类似系统来追踪员工的培训和认证过程？

- **质量标准**

① 学习管理系统被用于追踪培训和认证过程；
② 培训基于内部标准、政策和程序；
③ 使用认证计划或考勤记录来确定对开发系统和资源的访问。

- **回答**

① 没有；
② 是的，对于一些培训；
③ 是的，对于至少一半的培训；
④ 是的，对于大多数或所有培训。

4.3 安全测试

成熟度等级		活动流A 可测量的基线	活动流B 深入理解
1级	执行安全测试（包括人工的和基于工具的）以发现安全缺陷。	利用自动化安全测试工具。	对高风险组件执行人工安全测试。
2级	通过自动化以及常规的手动安全渗透测试，可以使开发过程中的安全测试更加完整和高效。	采用特定于应用软件的自动化安全测试。	执行人工渗透测试。
3级	将安全测试嵌入到开发和部署过程中。	将自动化安全测试集成到构建和部署过程中。	将安全测试集成到开发过程中。

可测量的基线—成熟度等级1

- **收益**

检测常见的、易发现的脆弱点。

- **活动**

对软件使用自动化的静态和动态安全测试工具，可以提高安全测试的效率和质量。逐渐增加安全测试的频率并扩展代码覆盖范围。

可以通过在不运行应用软件的情况下检查应用软件的源代，以静态地执行应用软件安全测试，也可以仅通过观察各种输入条件下的应用软件行为来动态地执行应用软件安全测试。前一种方法通常称为“静态应用软件安全测试（SAST）”，后一种称为“动态应用软件安全测试（DAST）”。称为“交互式应用软件安全测试（IAST）”的混合方法通过动态测试的方式自动检测的应用软件，并结合了这两种方法的优势（以额外的投入为代价），从而可以响应外部的输入而准确监视应用软件的内部状态。

- **问题**

您是否使用自动化安全测试工具扫描应用软件？

- **质量标准**

① 您可以使用自动化工具动态生成用于安全测试的输入；

② 您选择适合组织架构和技术堆栈的安全测试工具，并在检查的深度和准确性、结果对组织的可用性之间取得平衡。

- **回答**

① 没有；

② 是的，使用了其中一些；

③ 是的，使用了至少有一半；

④ 是的，使用了大多数或全部。

可测量的基线—成熟度等级2

- **收益**

检测特定于组织的、易于发现的脆弱点。

- **活动**

通过对特定技术堆栈和应用软件进行调整和自定义，提高自动化安全测试工具的效率。自动化安全测试工具具有两个重要特征：假阳性错误率（FP），即，对不存在bug和脆弱点的不正确报告；假阴性错误率（FN），即，对存在bug和脆弱点的检测缺失。随着您对自动化测试工具的使用日趋成熟，您将努力降低其假阳性错误率和假阴性错误率。这样可以最大程度地延长开发团队用于审查和解决应用软件中实际安全问题的时间，并减少通常与使用未经调整的自动化安全分析工具相关的摩擦。

- **问题**

您是否为应用软件和技术堆栈自定义了自动化安全工具？

- **质量标准**

① 您可以调整和选择与您的应用软件或技术堆栈相匹配的工具功能；
② 通过沉默或自动过滤无关的警告或低概率的发现，可以最大程度地减少假阳性误报；
③ 通过利用工具扩展或DSL为应用软件或组织标准定制工具，可以最大程度地减少假阴性误报。

- **回答**

① 没有；
② 是的，自定义了其中一些；
③ 是的，自定义了至少有一半；
④ 是的，自定义了大多数或全部。

可测量的基线—成熟度等级3

- **收益**

在尽可能早的阶段识别可自动识别的漏洞。

- **活动**

组织内的项目通常会运行自动化的安全测试，并在开发过程中检查结果。将安全测试工具配置为在构建和部署过程中自动运行，以使其具有较低的开销而可扩展。检查发现的结果。

尽早在需求或设计阶段进行安全测试将是有益的。尽管传统上使用功能测试用例，但这种类型的测试驱动开发方法涉及在开发周期的早期识别并运行相关的安全测试用例。随着安全测试用例的自动执行，项目进入实施阶段，并针对不存在的功能进行了许多失败的测试。所有测试通过后，实施完成。这为开发人员在开发周期的早期提供了明确的前期目标，降低了由于安全问题或在项目截止日期之前强制接受风险而导致发布延迟的风险。

- **问题**

您是否将自动化安全测试集成到构建和部署过程中？

- **质量标准**

① 管理层和业务利益相关者在整个开发周期中跟踪和审查测试结果；
② 您可以将测试结果合并到中央仪表板中，并将其输入到缺陷管理中。

- **回答**

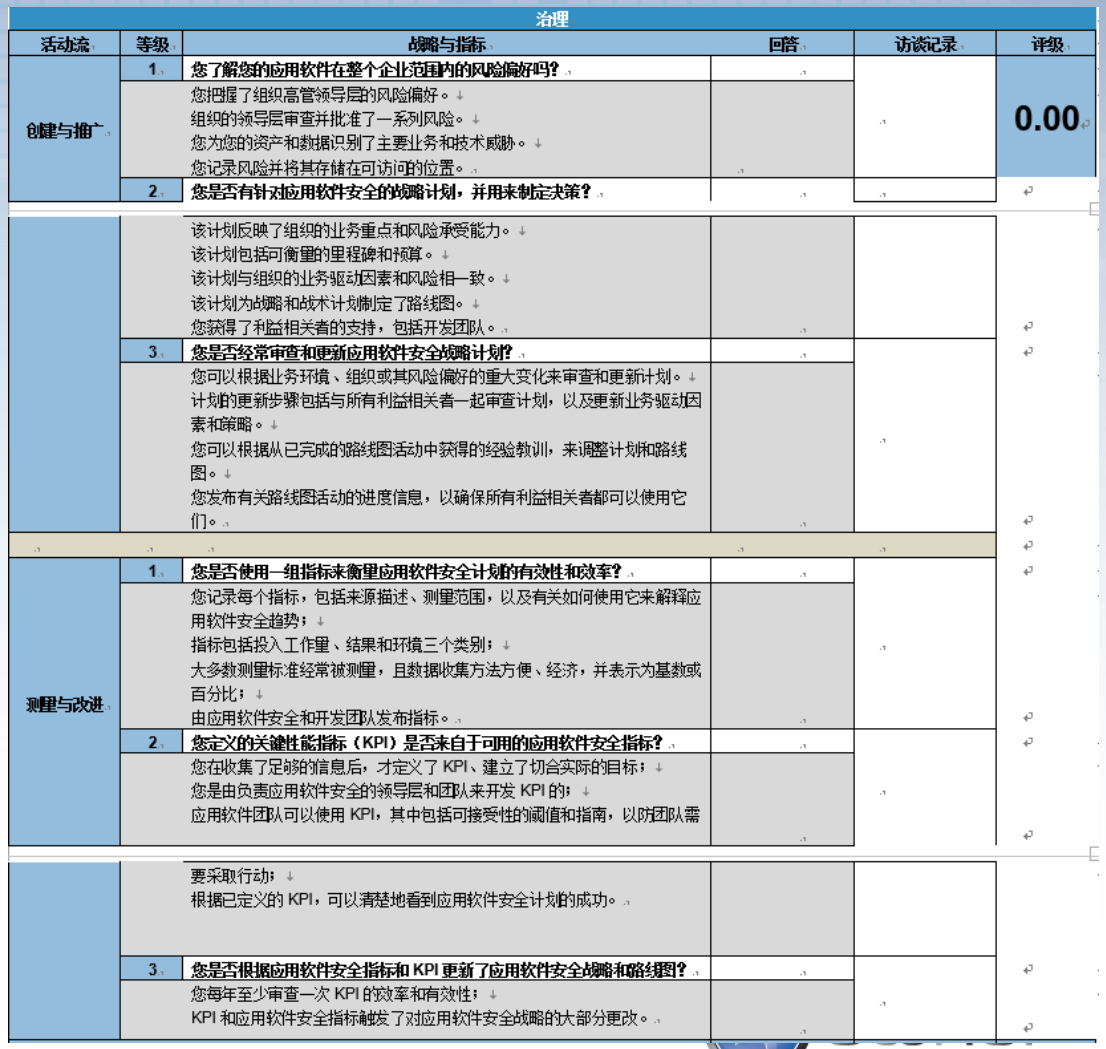
① 没有；
② 是的，集成了其中一些；
③ 是的，集成了至少一半；
④ 是的，集成了大部分或全部。

Open Web Application Security Project

使用方法

评估软件开发组织的能力现状

- 根据SAMM业务功能和安全实践组织访谈。
- 从“答案”列中的多项选择下拉选择中选择最佳答案。



治理					
活动流	等级	战略与指标	回答	访谈记录	评级
创建与推广	1	**您了解您的应用软件在整个企业范围内的风险偏好吗?**			0.00
		您把握了组织高管领导层的风险偏好。 组织的领导层审查并批准了一系列风险。 您为您的资产和数据识别了主要业务和技术威胁。 您记录风险并将其存储在可访问的位置。			
	2	**您是否有针对应用软件安全的战略计划，并用来制定决策?**			
		该计划反映了组织的业务重点和风险承受能力。 该计划包括可衡量的里程碑和预算。 该计划与组织的业务驱动因素和风险相一致。 该计划为战略和战术计划制定了路线图。 您获得了利益相关者的支持，包括开发团队。			
	3	**您是否经常审查和更新应用软件安全战略计划?**			
		您可以根据业务环境、组织或其风险偏好的重大变化来审查和更新计划。 计划的更新步骤包括与所有利益相关者一起审查计划，以及更新业务驱动因素和策略。 您可以根据从已完成的路线图活动中获得的经验教训，来调整计划和路线图。 您发布有关路线图活动的进度信息，以确保所有利益相关者都可以使用它们。			
测量与改进	1	**您是否使用一组指标来衡量应用软件安全计划的有效性和效率?**			
		您记录每个指标，包括来源描述、测量范围，以及有关如何使用它来解释应用软件安全趋势； 指标包括投入工作量、结果和环境三个类别； 大多数测量标准经常被测量，且数据收集方法方便、经济，并表示为基数或百分比； 由应用软件安全和开发团队发布指标。			
	2	**您定义的关键性能指标（KPI）是否来自于可用的应用软件安全指标?**			
		您在收集了足够的信息后，才定义了 KPI、建立了切合实际的目标； 您是由负责应用软件安全的领导层和团队来开发 KPI 的； 应用软件团队可以使用 KPI，其中包括可接受性的阈值和指南，以防团队需			
		要采取行动； 根据已定义的 KPI，可以清楚地看到应用软件安全计划的成功。			
	3	**您是否根据应用软件安全指标和 KPI 更新了应用软件安全战略和路线图?**			
		您每年至少审查一次 KPI 的效率和有效性； KPI 和应用软件安全指标触发了对应用软件安全战略的大部分更改。			

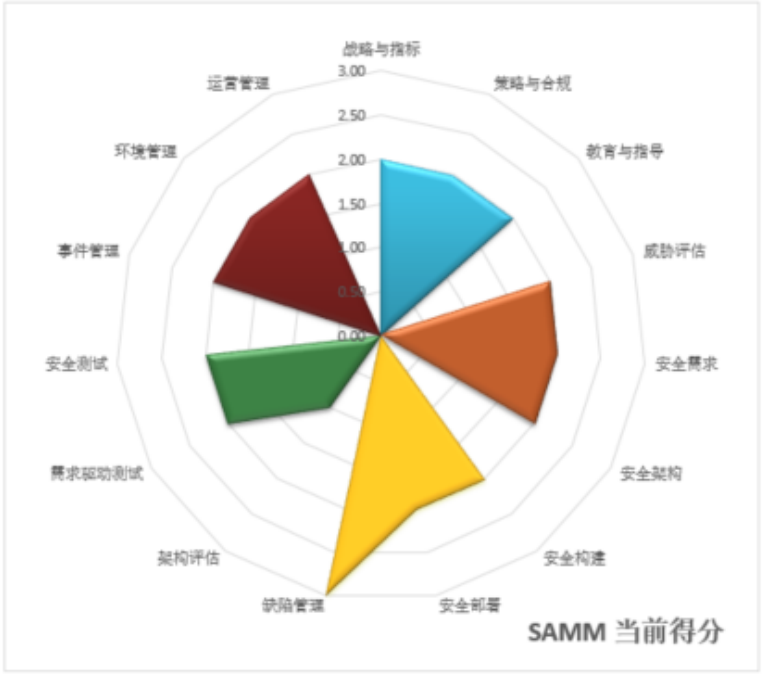
访谈记分卡

当前成熟度得分

业务功能	安全措施	当前	成熟度 1	2	3
治理	战略与指标	2.00			
治理	策略与合规	2.00			
治理	教育与指导	2.00			
设计	威胁评估	2.00			
设计	安全需求	2.00			
设计	安全架构	2.00			
开发	安全构建	2.00			
开发	安全部署	2.00			
开发	缺陷管理	3.00			
验证	架构评估	1.00			
验证	需求驱动测试	2.00			
验证	安全测试	2.00			
运营	事件管理	2.00			
运营	环境管理	2.00			
运营	运营管理	2.00			

业务功能	当前
治理	2.00
设计	2.00
开发	2.33
验证	1.67
运营	2.00

当前成熟度得分



OWASP
Open Web Application Security Project

Open Web Application Security Project

价值与意义

对组织的价值与意义

- 提升组织的软件安全开发能力
- 有助于组织开发安全的软件产品
- 有助于组织在开发过程中的安全合规
  - 《网络安全法》
  - 《等级保护2.0》
  - 《商业银行信息科技风险管理指引》
  - 其他

SAMM vs BSIMM

对比项	SAMM	BSIMM
谁编制的？	OWASP安全组织	美国新思科技公司
怎么编制的？	全球安全专家经验	对全球约130家企业进行调研
编制的维度是什么？	主动描述各个等级（包括但不限于：实践、人员、工具、规范等）	调研的统计结果
怎么使用？	完整的调研访谈材料（提问、回答标准、回答选项）	比对调研统计结果

国内已知的安全开发能力认证

中国信息安全测评中心

- 信息安全服务资质（安全开发类）
- 资质级别分为一级、二级，三级未推出
- 一级最低、二级最高
- 关注信息技术产品研发过程的安全开发，适用于信息技术产品研发单位。
- 典型持证企业：海康威视、绿盟、启明星辰、中软、东软

中国网络安全审查技术与认证中心

- 软件安全开发服务资质认证
- 资质级别分为一级、二级、三级共三个级别
- 三级最低、一级最高
- 关注软件开发过程的控制，适用于软件开发和软件外包单位。

谢 谢

项目Email: project@owasp.org.cn
个人Email: wangj@owasp.org.cn

OWASP
Open Web Application Security Project