回顾

默安科技
企业信赖的安全伙伴

[视频回放]

第3讲 5分钟看完安全开发大讲堂之“威胁建模”

[视频回放]

第4讲 默安DevSecOps落地实况

默安科技
企业信赖的安全伙伴

不同企业，SDL差异几何？

不同企业的SDL建设Roadmap分析

何乐乐

目录

Catalog

默安科技
企业信赖的安全伙伴

01如何评估SDL做的好坏

02 不同的SDL建设Roadmaps

03 到DevSecOps ?

可参考的评估标准 BSIMM-10

BSIMM内置安全成熟度模型在软件安全框架中被分为 119 项活动（反映指标）。该框架中共分为 12 个实践模块的 4 个区域

活动级别仅用于区分组织中观察活动的相对频率。经常观察到的活动被指定为“第 1 级”，较少观察到的活动被指定为“第 2 级”，不经常观察到的活动被指定为“第 3 级。

数据显示，高成熟度的计划都是全面的，涵盖该模型所描述的全部 12 项实践中各种各样的活动。

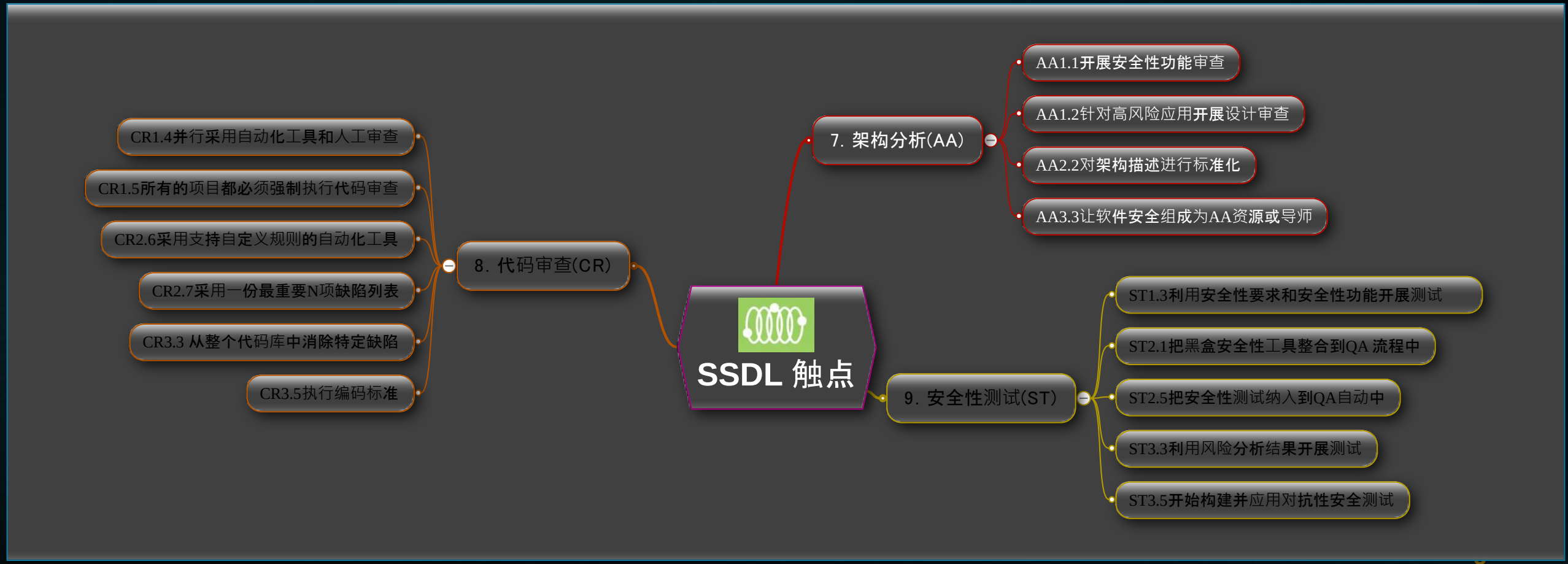
此外，该数据还描述了成熟的软件安全计划是如何随时间的推移而演进、改变和提升的。

可参考的评估标准 BSIMM-10

默安科技
企业信赖的安全伙伴

可参考的评估标准 BSIMM-10

默安科技
企业信赖的安全伙伴



可参考的评估标准 BSIMM-10

默安科技
企业信赖的安全伙伴

可参考的评估标准 SAMM-2.0

默安科技
企业信赖的安全伙伴

SAMM 2.0

软件保证成熟度模型是企业分析和提升软件安全的有效、可度量的方法。分为4部分。

模型基于具有安全保证实践的软件开发的核心业务功能，可以将其集成到现有的软件开发生命周期（SDLC）中。

支持开发模式：瀑布、迭代、 敏捷、DevOps

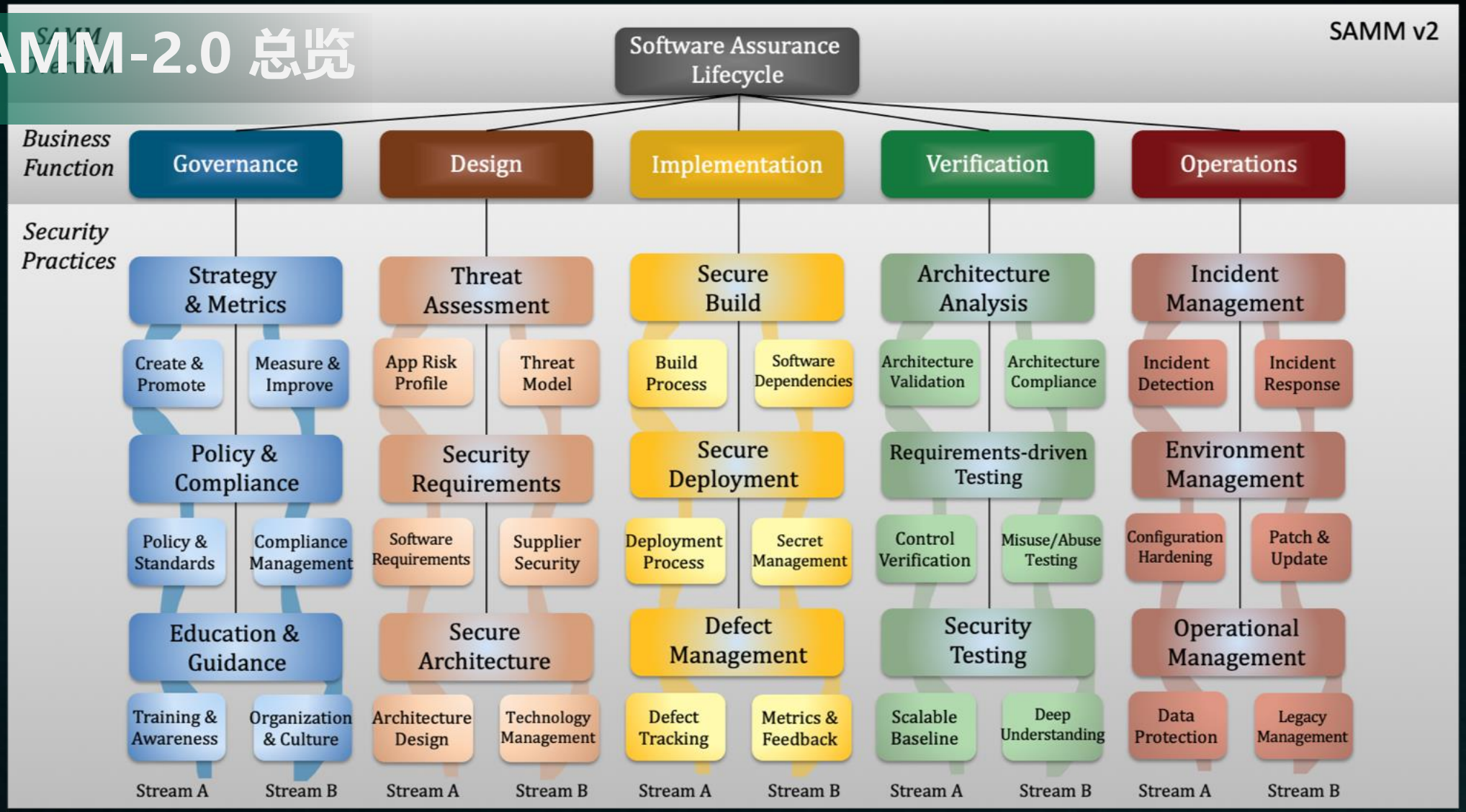
比先前版本增加了：

新业务功能：实施

新的安全实践：运营管理

- SAMM的概述和介绍、详细说明
- 快速入门指南与步骤来改善安全软件的做法
- 更新的SAMM工具箱，用于执行SAMM评估并创建SAMM路线图
- SAMM基准测试，可以自己的成熟度和进步与其他类似组织和团队进行比较

SAMM-2.0 总览



战略和指标	威胁评估	安全构建	架构评估	事件管理
策略和合规	安全需求	安全部署	需求驱动的测试	环境管理
教育和指导	安全架构	缺陷管理	安全测试	运营管理

SAMM-2.0 ToolBox

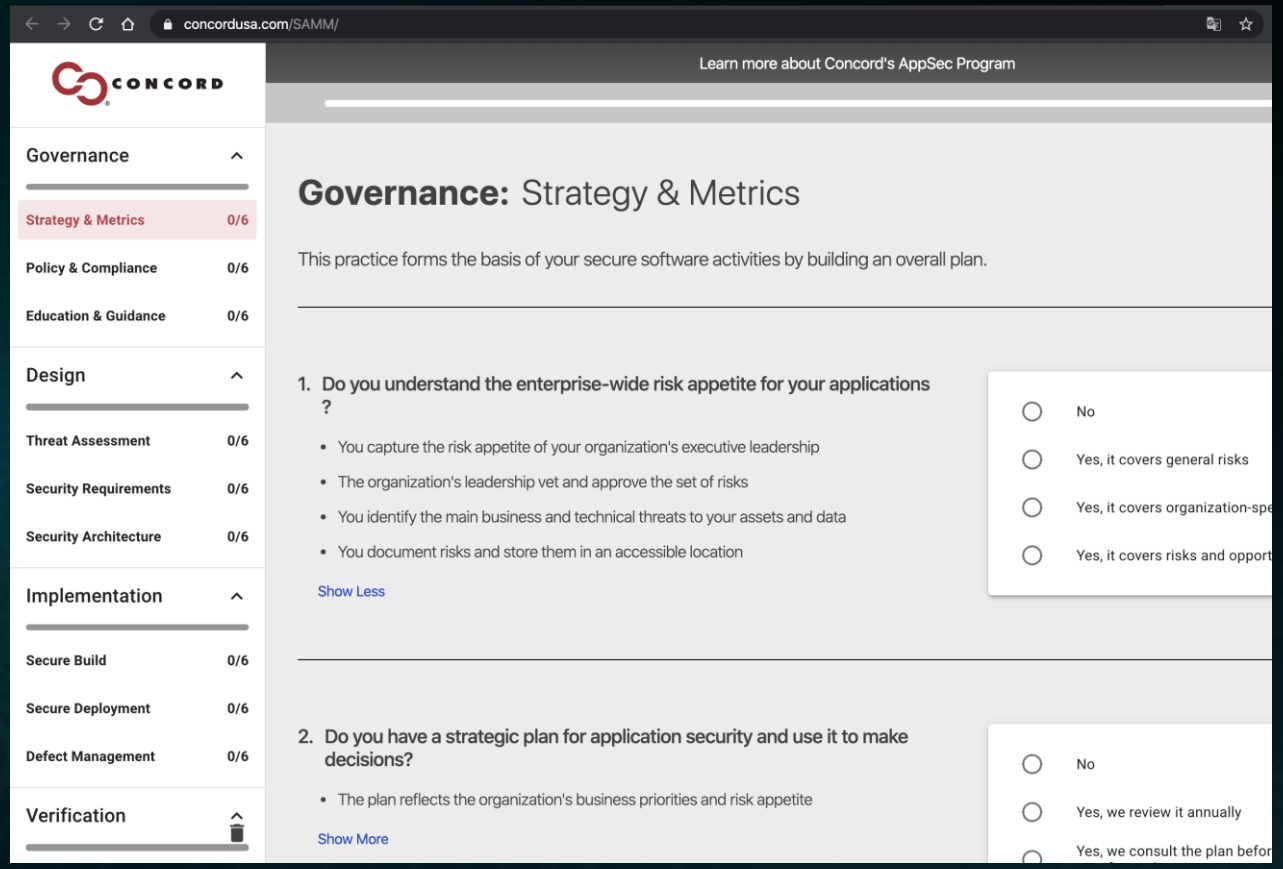
默安科技
企业信赖的安全伙伴

Instructions
Interview an individual based on the questions below organized according to SAMM Business Functions and Security Practices.
Select the best answer from the multiple choice drop down selections in the answer column.
Document additional information such as how and why in the "Interview Notes" column.
The formulas in hidden columns F-H will calculate the scores and update the Rating boxes and other worksheets as needed.
Once the interview is complete, go to the "Scorecard" sheet and follow instructions.

Organization:	
Team/Application:	
Interview Date:	
Team Lead:	
Contributors:	

		Governance
Stream	Level	Strategy & Metrics
Create and Promote	1	**Do you understand the enterprise-wide risk appetite for your applications ?**
		You capture the risk appetite of your organization's executive leadership The organization's leadership vet and approve the set of risks You identify the main business and technical threats to your assets and data You document risks and store them in an accessible location
	2	**Do you have a strategic plan for application security and use it to make decisions?**
		The plan reflects the organization's business priorities and risk appetite The plan includes measurable milestones and a budget The plan is consistent with the organization's business drivers and risks The plan lays out a roadmap for strategic and tactical initiatives You have buy-in from stakeholders, including development teams
	3	**Do you regularly review and update the Strategic Plan for Application Security?**
		You review and update the plan in response to significant changes in the business environment, the organization, or its risk appetite Plan update steps include reviewing the plan with all the stakeholders and updating the business drivers and strategies You adjust the plan and roadmap based on lessons learned from completed roadmap activities You publish progress information on roadmap activities, making sure they are available to all stakeholders
Measure and Improve	1	**Do you use a set of metrics to measure the effectiveness and efficiency of the application security program across applications?**
		You document each metric, including a description of the sources, measurement coverage, and guidance on how to use it to explain application security trends Metrics include measures of efforts, results, and the environment measurement categories Most of the metrics are frequently measured, easy or inexpensive to gather, and expressed as a cardinal number or a percentage Application security and development teams publish metrics
	2	**Did you define Key Perfomance Indicators (KPI) from available application security metrics?**
		You defined KPIs after gathering enough information to establish realistic objectives You developed KPIs with the buy-in from the leadership and teams responsible for application security

https://raw.githubusercontent.com/OWASP/samm/master/Supporting%20Resources/v2.0/toolbox/SAMM_Assessment_Toolbox_v2.0.xlsx



https://concordusa.com/SAMM/

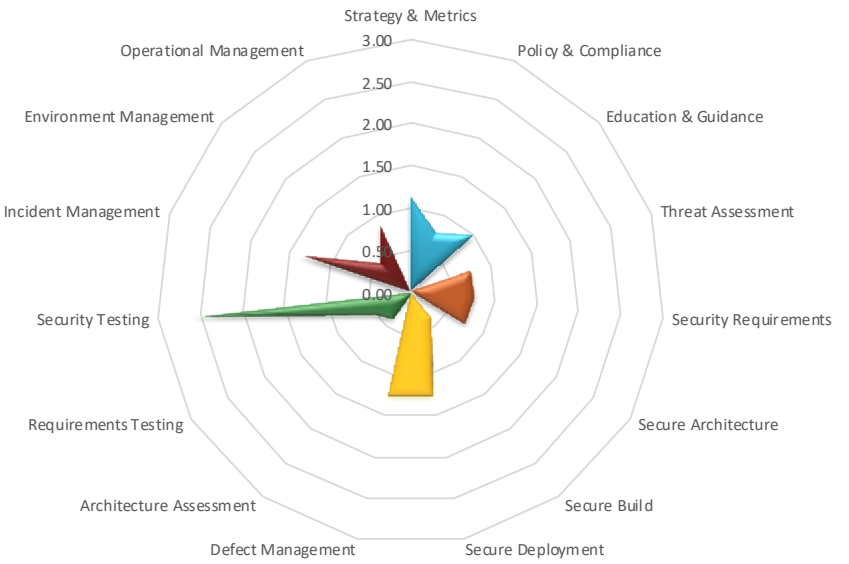
SAMM-2.0 ToolBox

默安科技
企业信赖的安全伙伴

Current Maturity Score

Functions	Security Practices	Current	Maturity 1	Maturity 2	Maturity 3
Governance	Strategy & Metrics	1.13	0.25	0.25	0.63
Governance	Policy & Compliance	0.75	0.38	0.25	0.13
Governance	Education & Guidance	1.00	0.25	0.50	0.25
Design	Threat Assessment	0.75	0.25	0.25	0.25
Design	Security Requirements	0.75	0.25	0.25	0.25
Design	Secure Architecture	0.75	0.25	0.13	0.38
Implementation	Secure Build	0.38	0.13	0.13	0.13
Implementation	Secure Deployment	1.25	0.75	0.38	0.13
Implementation	Defect Management	1.25	0.63	0.25	0.38
Verification	Architecture Assessment	0.38	0.00	0.25	0.13
Verification	Requirements Testing	0.50	0.13	0.25	0.13
Verification	Security Testing	2.63	1.00	1.00	0.63
Operations	Incident Management	1.38	1.00	0.25	0.13
Operations	Environment Management	0.50	0.25	0.25	0.00
Operations	Operational Management	0.88	0.25	0.25	0.38

Functions	Current
Governance	0.96
Design	0.75
Implementation	0.96
Verification	1.17
Operations	0.92



SAMM Current Score

目录

Catalog

默安科技
企业信赖的安全伙伴

02 不同的SDL建设Roadmaps

01如何评估SDL做的好坏

03 到DevSecOps ？

企业如何不同

默安科技
企业信赖的安全伙伴

视角	A	B	C
安全角色在哪里？	运维部、测试部	相对独立 开发部	完全独立 平级或高层岗位
安全人员有多少？	内部单角色 外部供应商	自建小团队	完整安全团队
安全需求来源	直接风险	业务、合规	行标、内建安全
想要达成什么效果	检测风险、遏制影响	保护重要资产	高度/全面的安全保证
平台化程度	主要靠人工和工具	重要流程自动化	大量内外部安全平台
成熟度要求	1初始	2结构化	3优化

A类SDL RoadMap

浅黄色：A类初步实施的安全工作
深黄色：A类应进行的安全工作

默安科技
企业信赖的安全伙伴

A类SDL RoadMap 实践

默安科技
企业信赖的安全伙伴

想做更多，又没有支持/预算/人员怎么办？

日常工作自动化（包括产品工具的嵌入、内部开放）
定制安全指南，兄弟部门协作
制定关键流程，做卡点

每年都做那么测试工作，还是有很多漏洞？

继续左移，总结漏洞到需求中
定制一些初步的基线（需求、开发、上线）

B类SDL RoadMap

浅蓝色：B类初步实施的安全工作
深蓝色：B类应进行的安全工作

默安科技
企业信赖的安全伙伴

威胁建模实践

默安科技
企业信赖的安全伙伴

到底用什么工具？
工具生成的威胁列表能看么？
威胁库怎么积累？
Pen、行业流传、组织共享、前沿

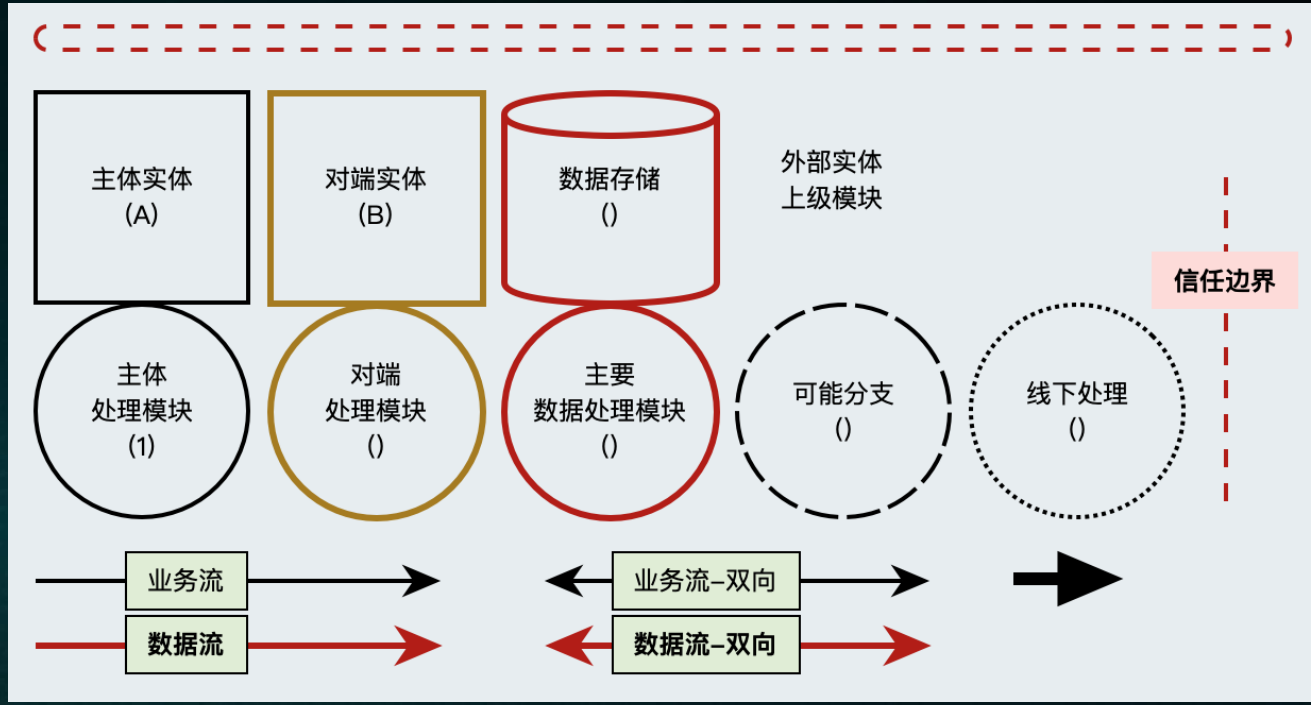
什么评估方法？
STREAD/DREAD/CIA/OWASP/CVSS

谁去做更合适？
系统建模：开发
威胁分析：安全（Pen testers）

项目太紧，来不及？
提前建模，扒设计图、文档、代码

得到大量潜在威胁？
评级、简化，收敛到1个周期能做到的

这样做完整么？
没有客观的完整，经验&方法论



https://capec.mitre.org/data/definitions/3000.html
https://capec.mitre.org/data/definitions/1000.html
https://github.com/izar/pytm
https://github.com/izar/pytm/blob/master/pytm/threatlib/threats.json

安全需求评审实践

默安科技
企业信赖的安全伙伴

谁去参加？
有威胁建模经验的

积累了大量的安全需求？
基于特点和场景简化
要有相关的设计落地方法

没有发现很多问题？
不重要，关注主要风险

需要跟踪么？
记录在内部 和 开发的需求管理系统

NO.	业务流程	细节场景	风险等级	面临的安全威胁	安全需求	安全设计	研发负责人	测试验证结果

C类SDL RoadMap

浅绿色：C类初步实施的安全工作
深绿色：C类应进行的安全工作

默安科技
企业信赖的安全伙伴

C类SDL RoadMap 实践

默安科技
企业信赖的安全伙伴

要干的事情太多了？
先定流程，试点系统
与开发流程深度集成

平台化、统一管理？
目前从项目角度的流程管理

安全控制太多了？
剔除重复工作、结果，重新编排

人员变动大？
需求知识库、测试验证知识库、设计库
入门培训

SDL RoadMap Overview

流程文档规范 | 安全工具 | 安全活动 | 工作目的 | 工作说明 | 主流程

默安科技 企业信赖的安全伙伴

目录

Catalog

默安科技
企业信赖的安全伙伴

03 到DevSecOps ?

01如何评估SDL做的好坏

02 不同的SDL建设Roadmaps

一些疑问

默安科技
企业信赖的安全伙伴

我SDL建设效果还不够理想，可以直接实践DevSecOps么？

SDL重在整体流程治理，DevSecOps重在工具链落地
SDL重在安全开发和安全设计，DevSecOps包括了Ops
两者并不冲突，都是安全治理的方法
都是需要长期持续的建设过程，重点保证核心系统

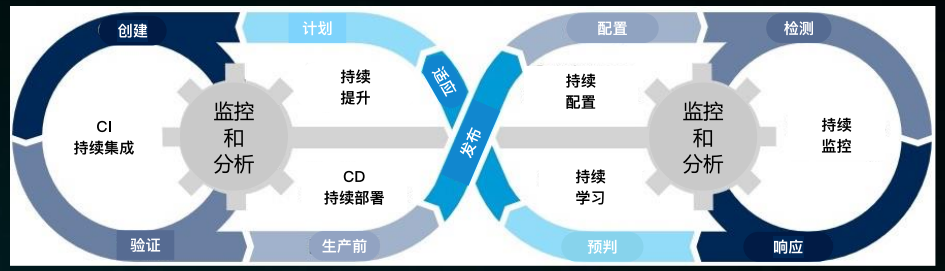
如何选择平台、工具？

为了长远考虑：集成嵌入、自动触发、稳定靠谱

DevSecOps的一些最佳实践参考：

devsecops-security-checklist

DevSecOps对比SDL



默安科技
企业信赖的安全伙伴

适应 计划 创建 验证 生产前 发布 配置 检测 响应 预判

安全需求
需求评审
威胁建模
安全编码规范
安全组件库
SCA 软件成分分析
SAST 静态检查
IAST 交互检查
DAST 动态检查
缺陷管理
资产安全检查
安全防护设备
应急响应
安全培训

培训 需求 设计 实施 验证 发布 响应

攻击树分析
代码审计
渗透测试
安全功能验证
上线前的评审

默安科技
企业信赖的安全伙伴

THANK YOU