内置安全成熟度模型 (BSIMM)

软件安全进入“科学”时代

BSIMM 结果可用于评估软件安全计划的现状、寻找差距、确定变革优先次序，以及确定为了立即实现改进而应当如何运用资源。

BSIMM 可帮助您：

1 使用实时数据启动软件安全计划（SSI）

软件安全计划必不可少。无论您身在哪个行业，BSIMM 可在您着手这项工作之前帮助您确定所有成功计划所包含的核心活动。

2 与同行业公司进行 SSI 比较

BSIMM 是帮助您与同行业公司进行 SSI 比较的最佳标杆之一。您能按照您的目标快速确定您在同行业公司中的地位。

3 基准化分析和跟踪您的 SSI 成长

BSIMM 是度量 SSI 效果的最佳和唯一可重复方法。SSI 建立后，您能用它逐年度量您的持续改进。另外它还能够提供具体细节，以便向您的高层团队和董事会展示您在安全方面的工作有何成效。

4 汲取成熟计划的经验教训，发展您的计划

BSIMM 是关于构建和发展软件安全计划的“有效方法”（ what works）报告。BSIMM 包含成熟组织当前正在进行的各种经过实践检验的活动。您可使用您的评估结果、BSIMM 活动和您的目标来制定策略和优先事项，从而取得实实在在的改进。

5 与面临常见问题的专业人士互动

除 BSIMM 外，您还能够加入我们的专属 BSIMM 社区，其相关内容和活动包括每月新闻通讯、季度专题研讨会、在美国和英国召开的年度会议、RSA 会议联谊活动以及一个活跃的在线社区。

BSIMM 是同类唯一的度量工具。

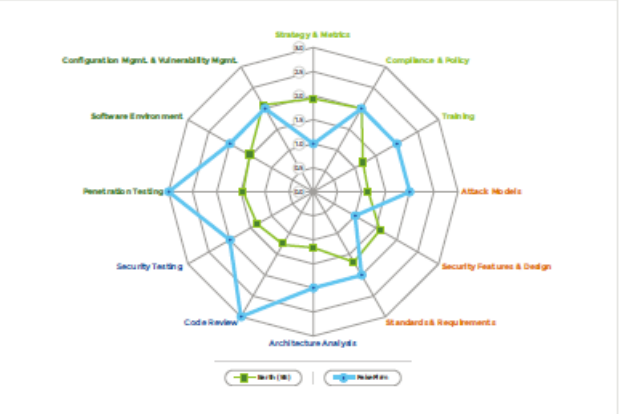
获得个性化报告

每个 BSIMM 都附带一个详细报告，重点列出您的优势领域和需要改进的领域。具体内容包括：

定制式的蜘蛛图。此图概括显示了您的领先和可能落后的领域。当您从度量模式转换到软件安全计划规划模式时，这些结果可提供客观的指导，使您能够立即予以实施。

BSIMM 公司记分卡。此表显示了你的计划与其他所有计划的对比，以便您了解自己处于什么地位。您可用它来考察您的整个计划的推进、您的各业务单元、业务合作伙伴和合作厂商。

虚假公司蜘蛛图



BSIMM7 记分卡：虚假公司 | 观察：37

GOVERNANCE			INTELLIGENCE			SSDL TOUCHPOINTS			DEPLOYMENT		
ACTIVITY	BSIMM7 FIRMS (95)	FAKEFIRM	ACTIVITY	BSIMM7 FIRMS (95)	FAKEFIRM	ACTIVITY	BSIMM7 FIRMS (95)	FAKEFIRM	ACTIVITY	BSIMM7 FIRMS (95)	FAKEFIRM
STRATEGY & METRICS			ATTACK MODELS			ARCHITECTURE ANALYSIS			PENETRATION TESTING		
[SM1.1]	47	1	[AM1.2]	63		[AA1.1]	81	1	[PT1.1]	82	1
[SM1.2]	48		[AM1.3]	34		[AA1.2]	29	1	[PT1.2]	58	1
[SM1.3]	46	1	[AM1.5]	48	1	[AA1.3]	23	1	[PT1.3]	54	
[SM1.4]	81	1	[AM2.1]	8		[AA1.4]	47		[PT2.2]	21	1
[SM2.1]	41		[AM2.2]	8	1	[AA2.1]	15		[PT2.3]	16	
[SM2.2]	35		[AM2.5]	13	1	[AA2.2]	12	1	[PT3.1]	10	1
[SM2.3]	33		[AM2.6]	9	1	[AA2.3]	5		[PT3.2]	6	
[SM2.5]	19		[AM2.7]	9		[AA3.1]	4				
[SM2.6]	33		[AM3.1]	4		[AA3.2]	0				
[SM3.1]	14		[AM3.2]	2							
[SM3.2]	9										
COMPLIANCE & POLICY			SECURITY FEATURES & DESIGN			CODE REVIEW			SOFTWARE ENVIRONMENT		
[CP1.1]	56	1	[SFD1.1]	74		[CR1.2]	58	1	[SE1.1]	46	
[CP1.2]	84		[SFD1.2]	65	1	[CR1.4]	63	1	[SE1.2]	78	1
[CP1.3]	50	1	[SFD2.1]	27		[CR1.5]	28		[SE2.2]	27	1
[CP2.1]	24		[SFD2.2]	40		[CR1.6]	34	1	[SE2.4]	24	
[CP2.2]	31		[SFD3.1]	6		[CR2.5]	22		[SE3.2]	12	
[CP2.3]	34		[SFD3.2]	10		[CR2.6]	15		[SE3.3]	3	
[CP2.4]	36		[SFD3.3]	1		[CR2.7]	19		[SE3.4]	0	
[CP2.5]	38	1				[CR3.2]	3	1			
[CP3.1]	19					[CR3.3]	2				
[CP3.2]	13					[CR3.4]	3				
[CP3.3]	5					[CR3.5]	5				
TRAINING			STANDARDS & REQUIREMENTS			SECURITY TESTING			CONFIG. MGMT & VULN. MGMT		
[T1.1]	69	1	[SR1.1]	60	1	[ST1.1]	78	1	[CMVM1]	82	1
[T1.5]	27		[SR1.2]	66		[ST1.3]	72	1	[CMVM2]	84	
[T1.6]	17	1	[SR1.3]	64	1	[ST2.1]	22	1	[CMVM3]	69	1
[T1.7]	37		[SR2.2]	28	1	[ST2.4]	10		[CMVM2.2]	74	
[T2.5]	13		[SR2.3]	22		[ST2.5]	7		[CMVM2.3]	41	
[T2.6]	14	1	[SR2.4]	21		[ST2.6]	9		[CMVM3.1]	3	
[T2.7]	5		[SR2.5]	22		[ST3.3]	4		[CMVM3.2]	5	
[T3.1]	3		[SR2.6]	17	1	[ST3.4]	2		[CMVM3.3]	8	
[T3.2]	5		[SR3.1]	8		[ST3.5]	4		[CMVM3.4]	6	
[T3.3]	2		[SR3.2]	11							
[T3.4]	7										
[T3.5]	2										

BSIMM 参加者的评论

无论是消费者还是专业人士，软件对我们日常生活的影响越来越大，而且人类正在张开臂膀拥抱数字体验。使用 BSIMM 对软件安全弹性实务进行基准化分析的领先组织在市场上明显具有竞争优势。

~ Jim Routh，首席安全官，Aetna

2009 年以来，BSIMM 的每个新版本都证明软件安全更加成为主流，并被越来越多的组织所采用。BSIMM7 也不例外，并且可能代表一个转折点——亦即软件安全日益包含于开发实务，作为一个独立软件工程领域的事实正在减弱。

~ Eric Baize，高级总监，产品安全办公室，Dell EMC

BSIMM7 是用户在为软件安全计划奠定坚实基础或加以改进（根据有关全球大量组织的实际活动的实时数据以及用于分类和理解这些数据的一致、系统性方案）时可资利用的基础资源。

~ Ivan Arce，安全总监， ICT 项目，Sadosky 基金会

关于我们

Cigital现为Synopsys旗下公司，Synopsys拥有市场上最全面的软件安全解决方案阵容。除传统测试服务以外，我们还帮助客户发现、补救和预防其业务应用中的安全漏洞。我们的整体式应用安全方案追求的是管理和专业服务与针对客户具体需求而定制的产品之间的平衡。我们的努力不会因为测试完成而止步。我们的专家还提供补救指导、程序设计服务以及培训，使您能够构建和保持应用安全。欲知更多信息，请访问www.synopsys.com/software。

新诺普思科技（北京）有限公司
北京市海淀区科学院南路2号
融科资讯中心 A 座 711-718室

中国销售：010-59860681
电子邮件：software-cn-sales@synopsys.com