BLACKDUCK®

软件安全构建成熟度模型 (BSIMM)

让科学为软件安全保驾护航

变化无常。您的SSI能否应对?

- 开发速度加快
- 使用自动化来驱动应用程序生命周期管理流程
- 由工程团队主导软件安全工作
- 转向容器、微服务和虚拟化环境
- 多云部署策略的冲突
- 一切皆代码
- 新应用架构

概述

无论软件安全变革是由工程团队的发展演进而驱动(如敏捷实践、CI/CD和DevOps),还是由软件安全小组 (SSG) 自上而下发起,提高软件安全计划 (SSI) 的成熟度对于成功管理风险都至关重要。但是,如果您的团队既不了解SSI的最新状态,也没有所需的数据来制定改进策略和确定SSI变更事项的优先级,您该如何应对呢?

解决方案就是使用软件安全构建成熟度模型 (Building Security in Maturity Model) — 通过对SSI进行十余年研究而得出的独特行业模型以及衡量SSI的标尺。BSIMM可以量化多家不同组织的软件安全活动,揭示其共同点和不同点,从而反映每个组织的独特性。BSIMM评估计分卡可用于评估SSI的当前状态、找出差距、为变更事项分配优先级、并确定如何以及在哪里分配资源,以实现立即改进。

BSIMM能够帮助您做到以下几点:

1. 使用真实数据启动软件安全计划 (SSI)。

您必须制定SSI。当您开始制定SSI时,BSIMM能够帮助您了解成功计划所必须执行的核心活动,与您的所属行业、公司规模、部署模式或合规需求无关。

2. 将您的SSI与同行业公司进行比较。

BSIMM是目前唯一可以衡量您的SSI并将其执行结果与多个行业进行比较的标准。有了目标,您便可以快速确定距离目标还有多远。

3. 对SSI发展进行基准分析和跟踪。

BSIMM是衡量SSI广度和深度的最佳和唯一可重复的方法。一旦建立了SSI,您就可以使用BSIMM来衡量每年的持续改进情况。BSIMM还能提供具体的细节,向您的管理团队和董事会展示安全工作有何成效。

1. 借鉴成熟计划的经验教训，持续改进您的SSI。

BSIMM是关于如何建立和完善SSI的“有效实践”报告，包含一些成熟组织机构经过验证的有效活动。您可以根据评估结果、BSIMM活动和您的目标，制定出真正能够改进SSI的策略和优先事项。

获得个性化报告

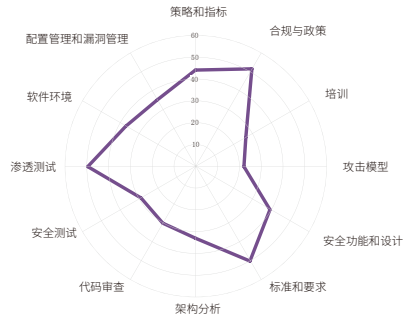
每次BSIMM评估都会生成一份详细的报告，重点列出SSI的优势和弱项。为了方便与管理层和董事会沟通，您还可以获得：

定制化的蜘蛛图。通过这张图表，您一眼就能看出在哪些方面做得很好，哪些方面还有待提高。当您从评估标准模式切换到SSI规划模式时，这些结果可以提供客观的反馈，以使您能够跟踪进步情况。

BSIMM计分卡。该表显示了您的SSI与其他SSI的对比情况。您可以使用它来查看您整个SSI的发展趋势，以及每个业务部门、业务伙伴和供应商的情况。

提取价值

联想基础设施解决方案集团产品安全办公室执行总监 Bill Jaeger 表示：“自2015年加入BSIMM社区以来，我们发现每年更新的观察结果对于我们规划和评估安全计划以及了解客户最关心的实践领域非常有价值。”



GOVERNANCE			INTELLIGENCE			SSDL TOUCHPOINTS			DEPLOYMENT		
ACTIVITY	BSIMM14 FIRMS (OUT OF 130)	EXAMPLE FIRM	ACTIVITY	BSIMM14 FIRMS (OUT OF 130)	EXAMPLE FIRM	ACTIVITY	BSIMM14 FIRMS (OUT OF 130)	EXAMPLE FIRM	ACTIVITY	BSIMM14 FIRMS (OUT OF 130)	EXAMPLE FIRM
STRATEGY & METRICS			**ATTACK MODELS**			**ARCHITECTURE ANALYSIS**			**PENETRATION TESTING**		
[SM1.1]	101	1	[AM1.2]	73		[AA1.1]	108	1	[PT1.1]	114	
[SM1.3]	80		[AM1.3]	49	1	[AA1.2]	59	1	[PT1.2]	102	1
[SM1.4]	118		[AM1.5]	81		[AA1.4]	63		[PT1.3]	85	1
[SM2.1]	73		[AM2.1]	16		[AA2.1]	35		[PT2.2]	42	
[SM2.2]	71		[AM2.6]	16	1	[AA2.2]	34	1	[PT2.3]	55	
[SM2.3]	71		[AM2.7]	15	1	[AA2.4]	40	1	[PT3.1]	30	1
[SM2.6]	77		[AM2.8]	20		[AA3.1]	20		[PT3.2]	21	
[SM2.7]	62	1	[AM2.9]	16		[AA3.2]	8				
[SM3.1]	32		[AM3.2]	8		[AA3.3]	17				
[SM3.2]	23		[AM3.4]	13							
[SM3.3]	32		[AM3.5]	11							
[SM3.4]	8										
[SM3.5]	0										
COMPLIANCE & POLICY			**SECURITY FEATURES & DESIGN**			**CODE REVIEW**			**SOFTWARE ENVIRONMENT**		
[CP1.1]	103	1	[SFD1.1]	100	1	[CR1.2]	84	1	[SE1.1]	88	
[CP1.2]	114	1	[SFD1.2]	95	1	[CR1.4]	112	1	[SE1.2]	113	1
[CP1.3]	101	1	[SFD2.1]	45		[CR1.5]	74		[SE1.3]	92	1
[CP2.1]	58		[SFD2.2]	70		[CR1.7]	55		[SE2.2]	68	1
[CP2.2]	63		[SFD3.1]	18		[CR2.6]	26	1	[SE2.4]	45	
[CP2.3]	72		[SFD3.2]	22		[CR2.7]	20		[SE2.5]	63	1
[CP2.4]	62		[SFD3.3]	9		[CR2.8]	28	1	[SE2.7]	47	1
[CP2.5]	80	1				[CR3.2]	17		[SE3.2]	18	
[CP3.1]	38					[CR3.3]	5		[SE3.3]	18	
[CP3.2]	34					[CR3.4]	3		[SE3.6]	22	
[CP3.3]	15					[CR3.5]	4		[SE3.8]	2	
									[SE3.9]	0	
TRAINING			**STANDARDS & REQUIREMENTS**			**SECURITY TESTING**			**CONFIG. MGMT. & VULN. MGMT.**		
[T1.1]	76	1	[SR1.1]	94	1	[ST1.1]	110	1	[CMVM1.1]	117	1
[T1.7]	64	1	[SR1.2]	103	1	[ST1.3]	91	1	[CMVM1.2]	95	
[T1.8]	59		[SR1.3]	98		[ST1.4]	62		[CMVM1.3]	98	1
[T2.5]	44		[SR1.5]	101	1	[ST2.4]	23		[CMVM2.1]	92	
[T2.8]	27	1	[SR2.2]	75		[ST2.5]	34		[CMVM2.3]	53	
[T2.9]	32	1	[SR2.5]	63	1	[ST2.6]	25		[CMVM3.1]	14	
[T2.10]	26		[SR2.7]	58		[ST3.3]	16		[CMVM3.2]	24	
[T2.11]	30		[SR3.2]	18		[ST3.4]	4		[CMVM3.3]	18	
[T2.12]	28		[SR3.3]	19		[ST3.5]	3		[CMVM3.4]	30	1
[T3.1]	8		[SR3.4]	21		[ST3.6]	6		[CMVM3.5]	16	1
[T3.2]	14								[CMVM3.6]	3	
[T3.6]	8								[CMVM3.7]	35	
									[CMVM3.8]	0	

Black Duck与众不同

Black Duck® 提供业界最全面、最强大、最值得信赖的应用安全解决方案组合。我们拥有无与伦比的专业知识和经验，来帮助世界各地的组织机构快速保护其软件，在其开发环境中高效集成安全性以及使用新技术进行安全创新。作为软件安全领域公认的领导者、专家和创新者，Black Duck拥有您构建可信软件所需的一切。如预了解更多信息，请访问www.blackduck.com。