BSIMM12
2021年洞察与趋势报告

目录

第一部分：执行概述

第二部分：活动

第三部分：附录

第一部分

执行概述

执行概述

了解BSIMM

2008年，来自新思科技软件质量与安全部门（当时名为“Cigital”）的顾问、研究人员和数据专家开始收集有关企业为应对软件安全挑战而采取的不同途径的数据。他们的目标是调研软件安全计划方面卓越成效的企业，通过面对面访谈的方式来了解这些企业的活动，并发布调查结果。

该结果就是软件安全构建成熟度模型（更广为人知的名称是BSIMM）— 通过观察到的活动为软件安全计划提供基线的描述性模型。由于这些计划通常使用不同的方法和术语，因此，BSIMM还为软件安全计划创建了一个通用词汇表。

BSIMM12参与者

2021版BSIMM报告 - BSIMM12 – 研究了来自不同行业领域的128家企业的软件安全活动的匿名化数据，包括金融服务、金融科技、独立软件供应商(ISV)、物联网(IoT)、医疗健康、云计算和科技公司（见图1）。

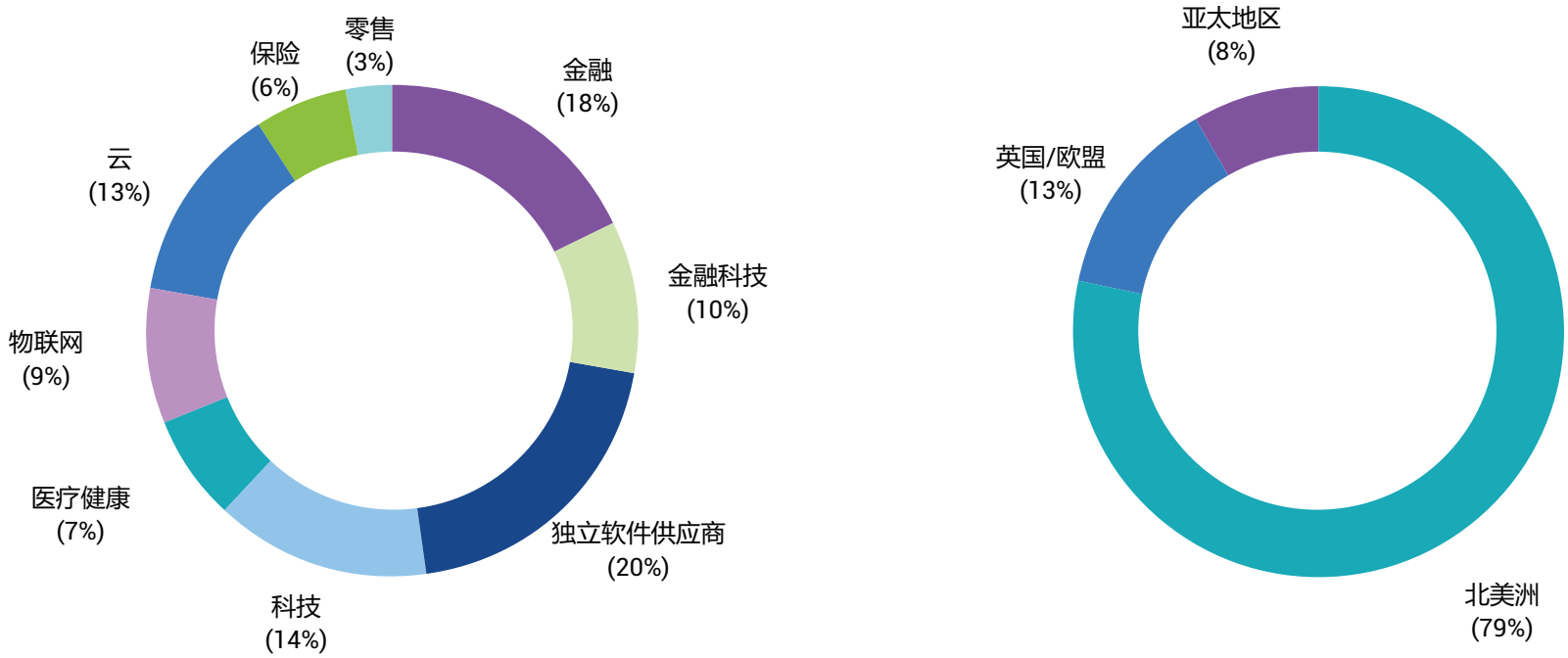


图1.BSIMM12参与企业 *跟踪的参与者在行业市场和地理位置的占比。*

BSIMM框架

BSIMM活动观察使用由12个软件安全实践组成的框架，这些实践分属于四个领域：“治理”、“情报”、“SSDL触点”和“部署”，这四个领域目前包含122项活动。以“治理”领域为例，有关BSIMM领域、实践和活动的说明，请访问 https://www.bsimm.com。《BSIMM12基础》文件提供了有关BSIMM12背景、数据和观察结果的详细信息，请访问 https://www.bsimm.com/resources.html。

从高管的角度来看，您可以将BSIMM活动视为在软件安全风险管理框架中实施的控制措施。您所开展的活动可能会在软件安全计划中起到预防、检测、纠正或补偿控制措施的作用。将这些活动定位为控制措施，便于治理、风险与合规、法律、审计和其他风险管理团队更容易地理解BSIMM的价值。BSIMM活动级别用于区分在参与企业中观察到的活动的频率。经常观察到 的活动被指定为“第1级”，较少观察到的和极少观察到的活动分别被指定为“第2级”和“第3级”。

BSIMM数据的演进

BSIMM项目已从2008年的9家参与企业发展到2021年的128家，目前拥有近3,000名软件安全团队成员和6,000多名外围小组（又名安全拥护者）成员。参与企业的软件安全计划的平均年限为4.4年。如表1所示，随着参与者进/出BSIMM社区，BSIMM相关数据可能会逐年略有波动。

BSIMM数据的演进												
	BSIMM12	BSIMM11	BSIMM10	BSIMM9	BSIMM8	BSIMM7	BSIMM6	BSIMM-V	BSIMM4	BSIMM3	BSIMM2	BSIMM1
公司数	128	130	122	120	109	95	78	67	51	42	30	9
评估次数	341	357	339	320	256	237	202	161	95	81	49	9
第2轮评估公司数	31	32	50	42	36	30	26	21	13	11	0	0
第3轮评估公司数	14	12	32	20	16	15	10	4	1	0	0	0
第4轮评估公司数	4	7	8	7	5	2	2					
SSG*成员数量	2,837	1,801	1,596	1,600	1,268	1,111	1,084	976	978	786	635	370
外围小组成员数量	6,448	6,656	6,298	6,291	3,501	3,595	2,111	1,954	2,039	1,750	1,150	710
开发人员数量	398,544	490,167	468,500	415,598	290,582	272,782	287,006	272,358	218,286	185,316	141,175	67,950
应用程序数量	153,519	176,269	173,233	135,881	94,802	87,244	69,750	69,039	58,739	41,157	28,243	3,970
SSG平均年限（年）	4.41	4.32	4.53	4.13	3.88	3.94	3.98	4.28	4.13	4.32	4.49	5.32

表1.BSIMM数据随时间发生的变化 *该图显示了BSIMM研究多年来的发展情况。（*SSG=软件安全团队）*

BSIMM路线图

在瞬息万变的软件安全领域，通过将自己的软件安全活动与BSIMM数据进行比较，可以了解其它公司对软件安全计划的处理方式，从而为制定自己的软件安全计划策略提供直接参考。

本文提供从BSIMM12收集到的数据中观察到的一些趋势和洞察的高度概述。

BSIMM术语表

- 活动(ACTIVITY)：作为实践的一部分由软件安全团队(SSG)直接开展或协助开展的行动。活动在BSIMM中按观察率划分为三个级别。经常观察到的活动被指定为“第1级”，较少观察到的和极少观察到的活动分别被指定为“第2级”和“第3级”。
- 能力(CAPABILITY)：跨越一个或多个实践的一组BSIMM活动，共同服务于一项内联安全功能。
- 拥护者(CHAMPION)：感兴趣并参与软件安全活动的开发人员、云安全工程师、部署工程师、架构师、软件管理人员、测试人员，以及对提高企业及其软件安全状况做出了贡献的其他人。
- 领域(DOMAIN)：BSIMM框架被划分的4个类别。4个领域包括治理、情报、安全软件开发生命周期(SSDL)触点以及部署。
- 实践(PRACTICE)：BSIMM的活动被划分为12个实践。4个BSIMM领域中的每一个都含有3个实践。
- 外围小组(SATELLITE)：一个小组，有时也被称为“拥护者”，由软件安全团队（SSG）组织和协调。
- 安全软件开发生命周期(SSDL)：
  集成了软件安全检查点及活动的软件生命周期。
- 软件安全框架(SSF)：支撑BSIMM 的基础结构，由4个领域的12项实践组成。
- 软件安全团队(SSG)：负责实施和推动软件安全工作的内部工作团队。
- 软件安全计划(SSI)：一项涵盖整个组织机构的计划，其以协调一致的方式逐步引入、评估、管理并演进软件安全活动。

第二部分

活动

BSIMM12评估的软件安全活动

畅销商业书籍《高效人士的7个习惯》(Habits of Highly Effective People)探讨了成功人士在实现目标方面具有共同品质并且这些品质可以被其他人识别和运用的理论。这一理念也适用于软件安全计划。表2列出了BSIMM12数据池中观察到次数最多的10项活动，所有这些活动都常见于非常成功的软件安全计划中。数据表明，如果组织正在制定自己的软件安全计划，应考虑采取这些活动。

BSIMM12中按观察次数排列的10项最常见活动		
	对128名参与者的观察到的次数	活动描述
1	92% （118名参与者）	实施对开发周期各环节的检测并用于定义治理
2	91% （117名参与者）	确保主机及网络安全性基础就位
3	89% （114名参与者）	确定个人身份信息(PII)责任
4	88% （113名参与者）	开展安全性功能审查
5	87% （111名参与者）	聘请外部渗透测试人员来查找问题
6	84% （108名参与者）	创建事件响应机制或者与事件响应团队交流
7	80% （102名参与者）	集成并交付安全性功能
8	80% （102名参与者）	采用自动化工具
9	78% （100名参与者）	确保QA执行支持边缘/边界值条件测试
10	77% （99名参与者）	把合规约束转变成需求

表2.10项最常见的BSIMM12活动

您的软件安全计划能跟上变化的步伐吗？

1. 您是否维护所有软件资产的当前视图，包括内部代码、第三方代码、开源代码、自动化脚本、基础架构即代码和其它的软件资产？
2. 您是否使用详细记录所有在软件安全计划范围内的软件的物料清单来制定风险管理决策？

10项最常见活动的细分

1 实施开发周期各环节的检测并用于定义治理

BSIMM12发现，软件安全领导者正在大幅转向在整个软件组合中实施基于风险的控制，从而使开发团队能够在软件开发生命周期的早期发现并修复问题。绝大多数—92%—的BSIMM12参与者都以某种形式开展了本活动。

安全的软件生命周期流程是在整个开发过程中将安全性构建到应用程序中的主动式预防性方法。从本质上说，“开发周期各环节检测”倡导者通过在软件开发生命周期的各个阶段收集数据并使用这些数据来创建和实施软件安全策略而将软件安全紧密地融入到应用开发过程中。

2 确保主机及网络安全性基础就位

在主机和网络安全性就位之前尝试实施软件安全就像先穿鞋子后穿袜子。几乎所有的BSIMM12参与者—91%—均通过确保在其数据中心和网络中部署主机和网络安全性基础，作为开展软件安全的好的基础。

3 确定个人身份信息(PII)责任

正如BSIMM12观察结果所示，保护个人身份信息(PII)是许多组织的首要任务，89%的参与者已经确定了他们的PII要求，43%的参与者还建立了PII清单。外包到托管环境并不会减轻组织的PII义务，甚至会增加识别所有相关义务的难度。了解PII所在的位置并防止未经授权披露PII数据是每家具有安全意识的企业都需要采取的行动。

4 开展安全性功能审查

在开始架构分析时，具有安全意识的组织会将流程集中在对安全功能的审查上。例如，安全功能审查将识别确定可能受到提权攻击的系统或错误地将PII放入本地存储系统的移动应用。88%的BSIMM12参与者开始了这项活动。

5 聘请外部渗透测试人员来查找问题

外来的和尚会念经。87%的BSIMM12参与者都认可这个谚语。虽然内部软件安全拥护者的话可能没人会听，但外部渗透测试人员可以清楚地向组织证明其无法避免安全问题。

10项最常见活动的细分 续

6 创建事件响应机制或者与事件响应团队交流

84%的BSIMM12参与者启动了这个流程，将软件安全小组与事件响应团队联系起来，以保持关键安全信息的双向流通。开通与基础设施和软件供应商的沟通-渠道也是软件安全小组的一项非常重要的任务。

7 集成并交付安全性功能

不应当让每个项目组自行实施全部的安全功能，80%的BSIMM12软件安全小组推动或参与了获批安全功能的制定和并发布。项目组可受益于软件安全小组预先批准的实施内容，而软件安全小组则免于重复追踪那些安全功能中常见的错误。

8 采用自动化工具

随着应用程序和网络变得越来越复杂，手工管理安全性和合规变得越来越困难。手工操作可能导致问题检测和修复速度变慢、资源配置错误和策略应用的不一致性，从而使组织容易遇到合规问题和攻击。80%的BSIMM12参与者表示，他们正在使用自动化工具来帮助保护代码和应用程序。值得注意的是，在2021年，多达26家BSIMM12参与企业仍在严重依赖于手动软件安全和合规流程，尽管每个人都可能有正当的理由这样做。

9 确保QA执行支持边缘/边界值条件测试

大多数- 78% - 的BSIMM12参与者认识到超越标准功能测试（仅使用可接受的输入信息）的价值。越来越多的QA团队逐渐开始像对手那样思考问题，采用主动的软件安全思维方式。

10 把合规约束转变成需求

把合规性约束转变为软件需求并传达给开发团队被纳入到77%的BSIMM12参与者的策略中。把这些合规约束转变为软件要求有助于提高审计时的可追溯性和可视性。

活动的增长

活动 — 即软件安全团队采取或协助推动的行动 — 往往会随着软件安全环境和团队优先级的变化而变化。例如，数据表明，在过去两年中，识别开源代码活动增加了61%，这可能是由于现代软件中对开源组件使用量的增加以及将常用开源项目作为途径的攻击的增加。

表3显示了过去24个月BSIMM数据中观察到的增速最高的活动。早在BSIMM7便引入的三项活动 —确保具备云安全基础、对容器和虚拟化环境使用编排功能 以及采用应用程序容器来支持安全目标— 由于对BSIMM项目而言相对较新，因此增长率百分比较高。例如，对容器和虚拟化环境使用编排功能这项活动在BSIMM9首次被引入后的12个月内，仅被观察到5次，而两年后在BSIMM12中则被观察到33次。尽管如此，这些活动的增长表明了云平台和容器技术对企业使用和保护软件的影响越来越大。

活动	观察计数 BSIMM10	观察计数 BSIMM12	增加的 百分比
对容器和虚拟化环境使用编排功能	5	33	560%
确保具备云安全基础	9	59	555%
采用应用程序容器来支持安全目标	14	44	214%
针对高风险应用程序开展设计审查	29	49	69%
在入职培训中加入软件安全性方面的内容	28	46	64%
识别出软件中所使用的开源代码	46	74	61%
创建SLA样板文件	35	55	57%
整合黑盒安全工具到QA流程中	32	50	56%
确保高管人员了解合规性和隐私义务	56	74	32%
统一监管压力	81	98	21%
采用自动化工具	85	102	20%

表3.增长最快的活动 *以观察计数占比的总体变化显示的各项活动从BSIMM10到BSIMM12的增长情况。*

BSIMM12垂直行业比较

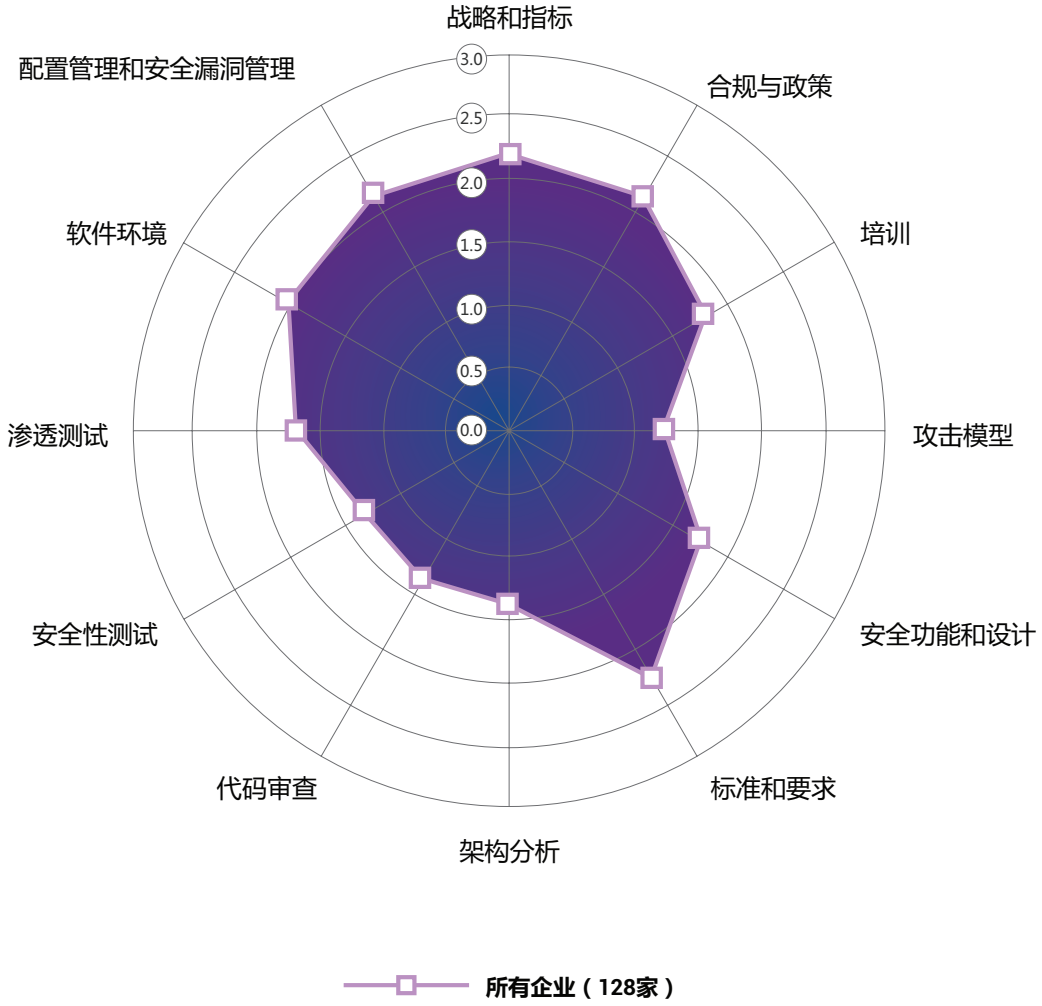


图2.2 级和 3 级活动的观察计数*128 家 BSIMM12 企业在每个实践中共同达到的平均高位标记。*

BSIMM高水位线图提供了基线，用于比较128家公司在每个实践中的主要活动的频率。活动级别代表了参与组织中观察到的活动的频率。经常观察到的活动被指定为“第1级”，较少观察到的和极少观察到的活动分别被指定为“第2级”和“第3级”。

水位线通常表示成熟度，如3级的水位线高，2级的水位线稍低。如上图2所示，在BSIMM12观察的所有公司中，在 “战略和指标”、“合规与政策”和“标准和要求”等实践观察到的第2级和第3级活动数量要比“攻击模型”、“架构分析”、“代码审查”和“安全测试”等实践中多一些。

物联网、云计算和ISV行业

物联网、云计算和ISV公司创建的软件解决方案通常部署方式不同。例如，物联网公司在与前端设计相关的实践中表现出更高水平的成熟度（即，强调设计过程早期阶段的决策），如“培训”、“安全功能和设计”以及“架构分析”等实践。在“架构分析”中，物联网的高水位线明显高于其他行业，这可能是因为许多物联网设备预计会在生产环境中长时间运行。

云计算和ISV公司有着相似的模式，但“代码审查”实践除外，在这个实践中，云计算公司领先于其他两个行业的公司（见图3）。这一趋势可能是由于过去几年云计算公司产生的代码呈现爆炸式增长，从而导致代码审查需求扩大所致。

出现这种情况部分是因为物联网公司对物联网设备滥用和隐私问题的认识不断提高，因此对培训和测试等若干实践的引入部署的速度超过了ISV行业。

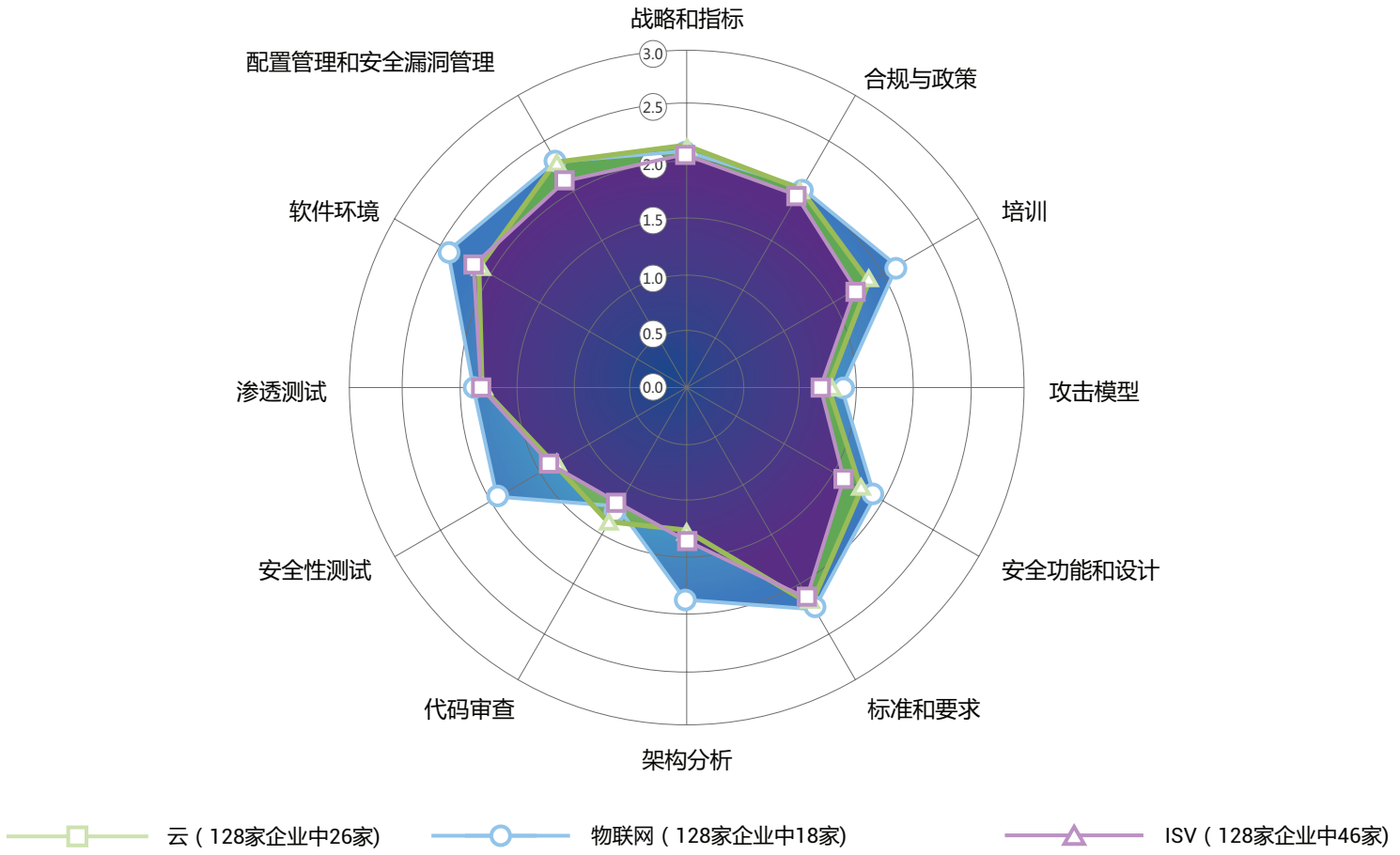


图3.云计算、物联网与ISV行业相比较

物联网和金融科技行业

物联网行业安全计划的重点是保护设备上的软件，例如采用二进制机密性保护和完整性验证活动。有趣的是，物联网和金融科技公司在识别开源代码方面拥有相似的观察率，但金融科技公司在控制开源代码风险方面的观察率却比前者高出两倍多。这可能是因为金融科技公司认为与开源漏洞风险相关的后果更严重，而物联网公司则认为设备软件中的许可证违规风险更大。

如图4所示，查看每个垂直行业认为最有价值的活动也很有趣。据观察，物联网和金融科技行业都认为执行安全功能审查活动很重要，但物联网公司对高风险应用程序执行设计审查的频率却远远高于金融科技公司，而金融科技公司使用风险评估方法对应用程序进行排序的活动频率则远远高于物联网公司。

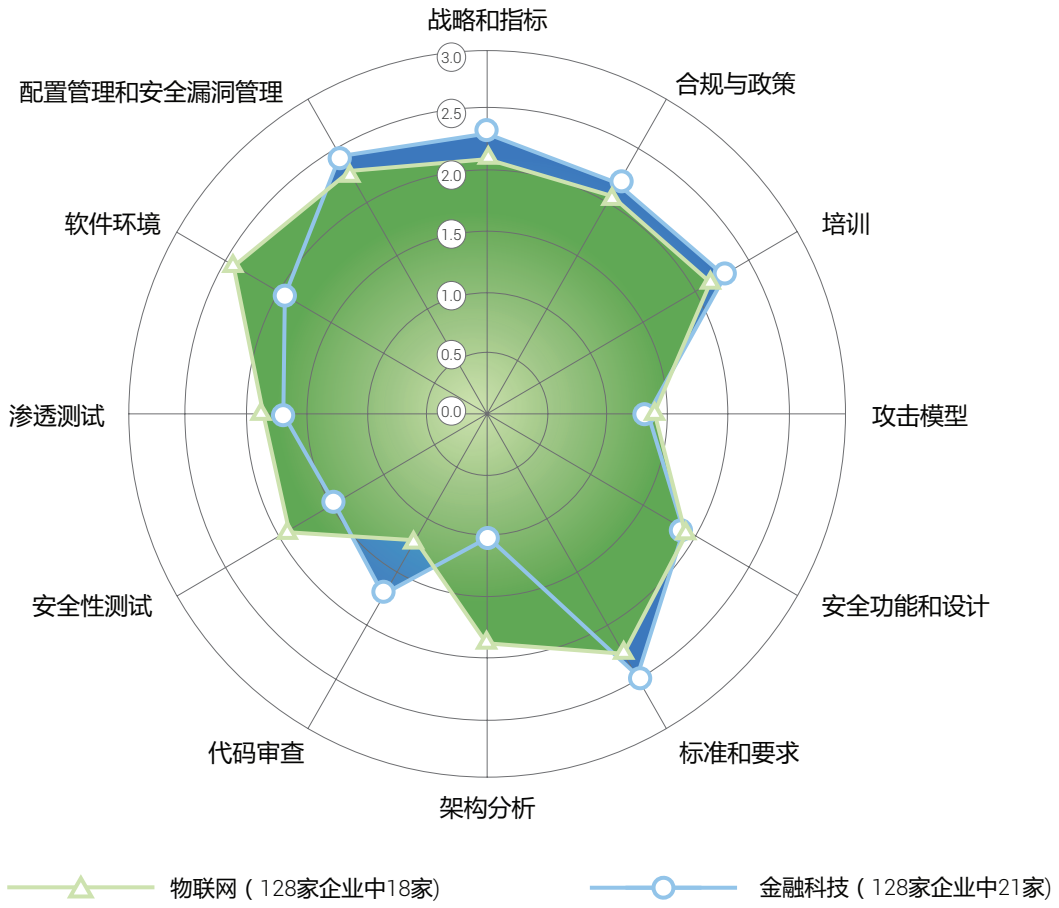


图 4.物联网与金融科技行业相比较

金融服务、医疗健康和保险行业

BSIMM中有三个处于高度监管领域的行业，它们是：金融服务业、医疗健康行业和保险行业（见图5）。根据我们十几年的BSIMM经验，大型金融服务公司通过启动软件安全计划而对监管变化作出反应的速度要比保险企业和医疗健康企业早很多。

尽管BSIMM数据池中的金融服务公司的数量在过去五年中大幅增加，但金融服务行业的软件安全小组在评估时的平均年限为5.4.年，而保险行业为4.4年，医疗健康行业为4.2年。金融服务公司在完善其采用的软件安全计划所花费的时间在并排比较中可清楚地展示出来。

虽然保险行业包括一些成熟的例外者，但这三个受监管的行业的数据表明，保险行业虽然在代码审查和安全性测试实践方面取得领先优势，但在策略和指标、攻击

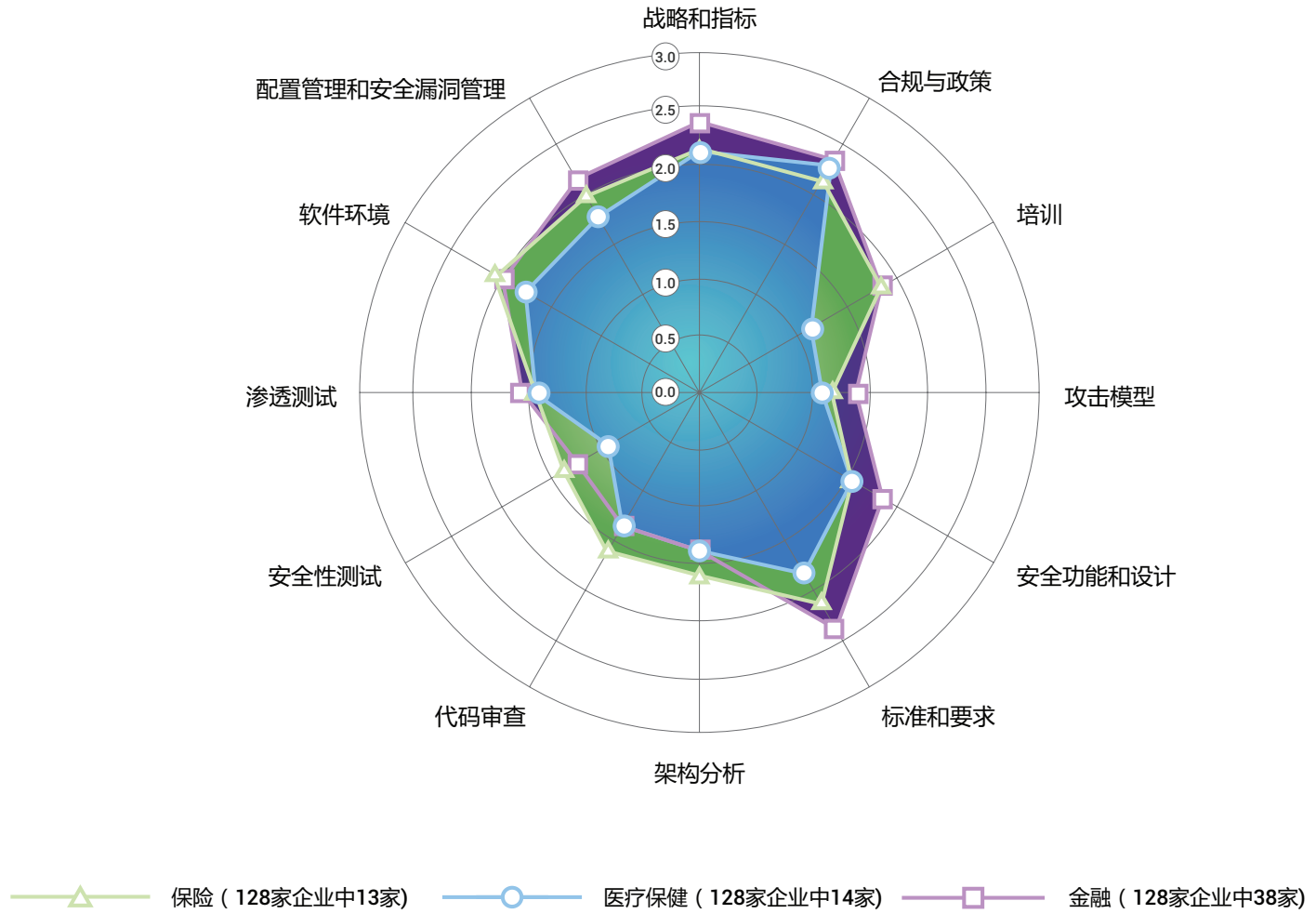


图5.金融服务、医疗健康和保险行业相比较

模型以及安全功能与设计这三个实践方面仍落后其它两个行业。我们看到医疗健康公司的情况与金融服务公司类似，虽然在合规与政策、架构分析、 代码审查和渗透测试方面达到了平均水平，但在其它实践领域仍处于落后状态。

尽管这三个行业的合规和监管驱动因素相似，但医疗健康行业的高水位线通常落后于保险和金融科技行业，这可能是因为他们在开展合规活动之前需要优先考虑满足患者的关切。

BSIMM12 软件安全活动的新兴趋势

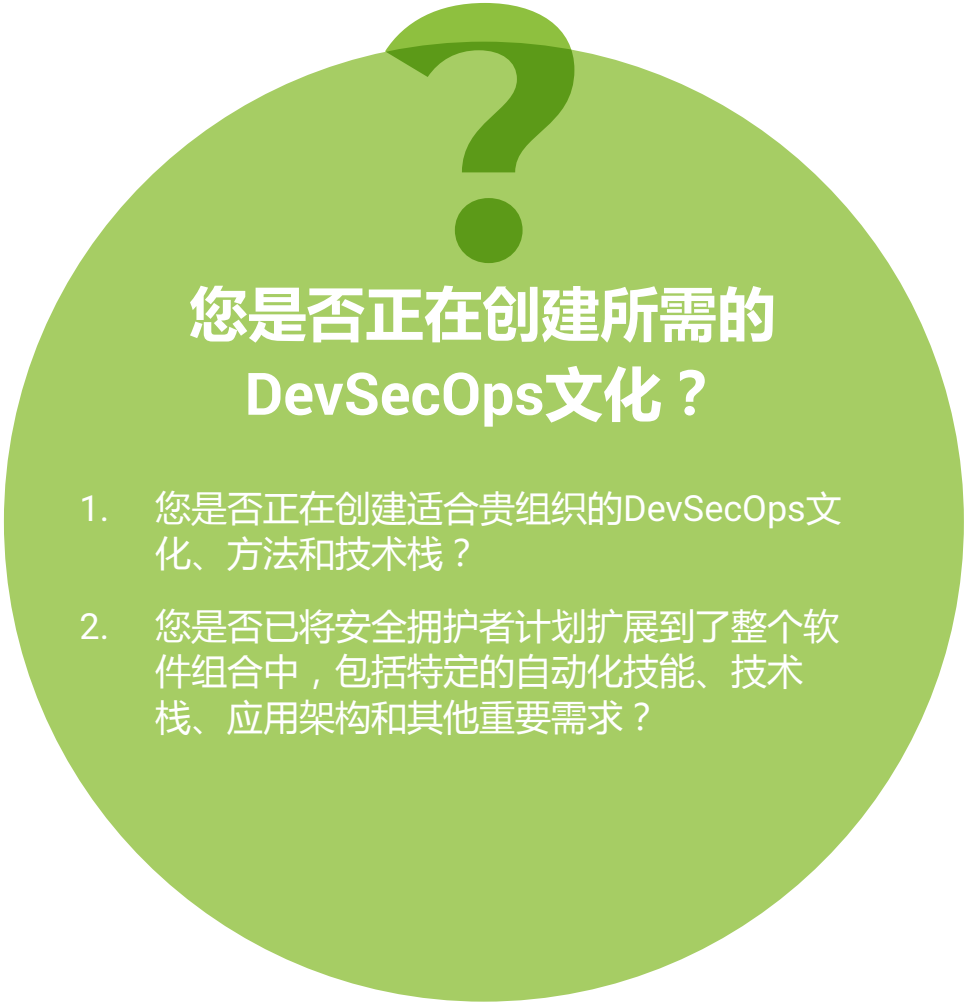
借调资源、人员和知识用于开展 DevSecOps 活动

过去24个月收集的数据表明，软件安全小组正在从强制性的软件安全行为人朝着合作伙伴角色转移 — 为DevSecOps实践提供资源、人员和知识，目的是为关键软件交付路径的安全工作直接做出贡献。

例如， “使用应用程序容器支持安全目标” 这一活动的观察率已从BSIMM10中的14次增加到BSIMM12中的44次。 “对容器和虚拟化环境使用编排功能” 这一活动的观察率也从BSIMM10中的5次大幅增加到BSIMM12中的33次。

治理即代码

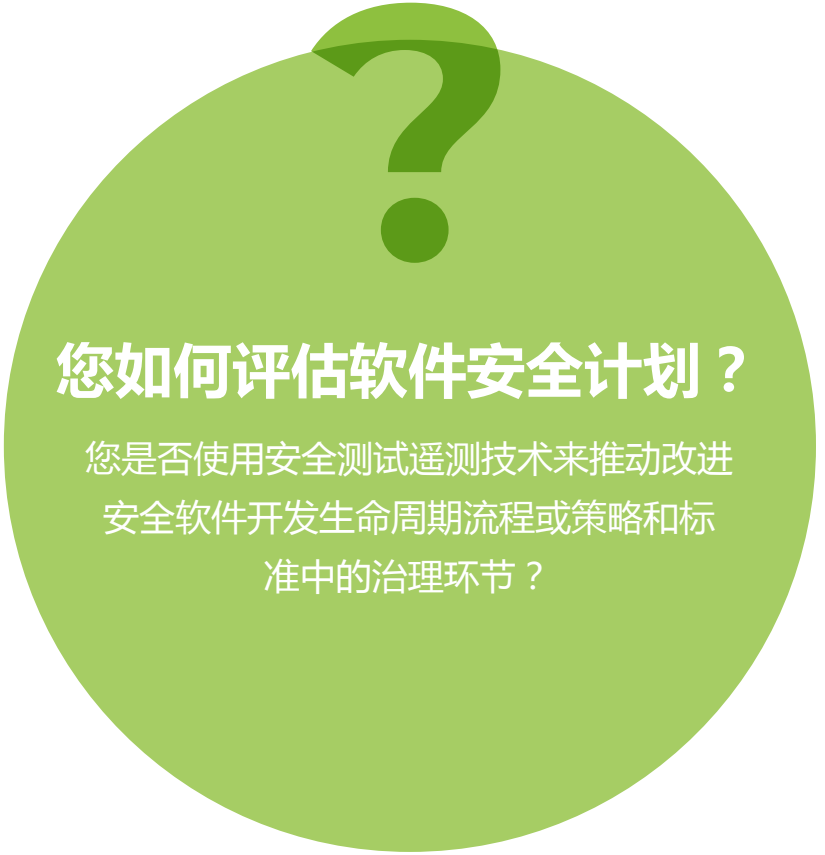
BSIMM10和BSIMM11数据表明，企业已经开始使用自动化来取代由人工驱动的手工治理活动。BSIMM12中的观察计数越来越明确地表明，软件安全标准和策略的唯一来源正在变成人可读的配置代码或进行漏洞发现的简化代码 — 这是软件定义生命周期治理的本质。



持续缺陷发现和持续改进

BSIMM12数据表明，越来越多的公司正在实施先进的缺陷发现方法，并倾向于持续监控和报告，而不仅是针对指定时间点的缺陷发现方法。开展持续测试最初需要额外的人力，从而导致外围小组的发展壮大，例如观察到“战略和指标”活动次数以及 “创建或扩大外围小组”的活动次数有所增加。过去两年中，在 “通过自动化创建的资产能够被监控” 和 “自动验证基础运维设施安全” 这两个方面新观察到的活动次数平均都是8次，随着这一趋势的继续，我们预计外围小组将开展更多的自动化活动。

安全软件开发生命周期和生产环境中的持续测试趋势加剧了需要分类和处理的安全问题。这种新的趋势要您向领导层提供数据以支持他们做出管理决策，从而导致 “在内部发布有关软件安全性的数据”这一BSIMM活动在过去两年中增长了30%。虽然今天的治理流程大部分仍然是手动的，但越来越多的组织倾向于治理即代码，导致BSIMM12中15%的企业观察到了 “整合软件定义的生命周期治理”这一活动。



持续安全软件开发生命周期改进

在及早地、持续地进行较小规模的测试活动时，企业了解到安全遥测必须从生命周期的一个阶段传递到下一个阶段，就像软件工件本身从生命周期的一个阶段传递到下一个阶段一样。这一持续发展的趋势反映在两项新活动中，即BSIMM10中引入的 “自动验证基础运维设施安全”和BSIMM11中引入的 “实施事件驱动的自动化安全测试”。

数据表明，持续改进反映在重要的安全软件开发生命周期工作中，包括通过观察来扩充外围小组、自动化资产发现流程、增量安全设计工作、将手动工作转换为“代码”、以及尽快发现安全和质量问题以加快开发速度等。尽早发现问题仍然是必要的，可促使您将大规模的测试活动分解成小规模的及时检查。但软件安全小组也越来越意识到，有时候，部署编排或部署后的环境是开展某些测试的最早的、最佳的机会。

这种朝着持续工作方式的转变反映在采用怎样的治理颗粒度上（例如，分配应用程序所有者）采用什么测试（SAST门限），并且因为其将简化构建软件清单的方式。相比传统应用程序，现在有更多的代码被使用，并且容易被资产管理工作所疏漏。

安全即弹性和质量

过去两年中，“整合黑盒安全工具到QA流程中”这一活动的观察率增加了50%以上。同样，“把安全性测试纳入到QA自动化中”这一活动的观察率在过去两年中也增加了一倍以上。

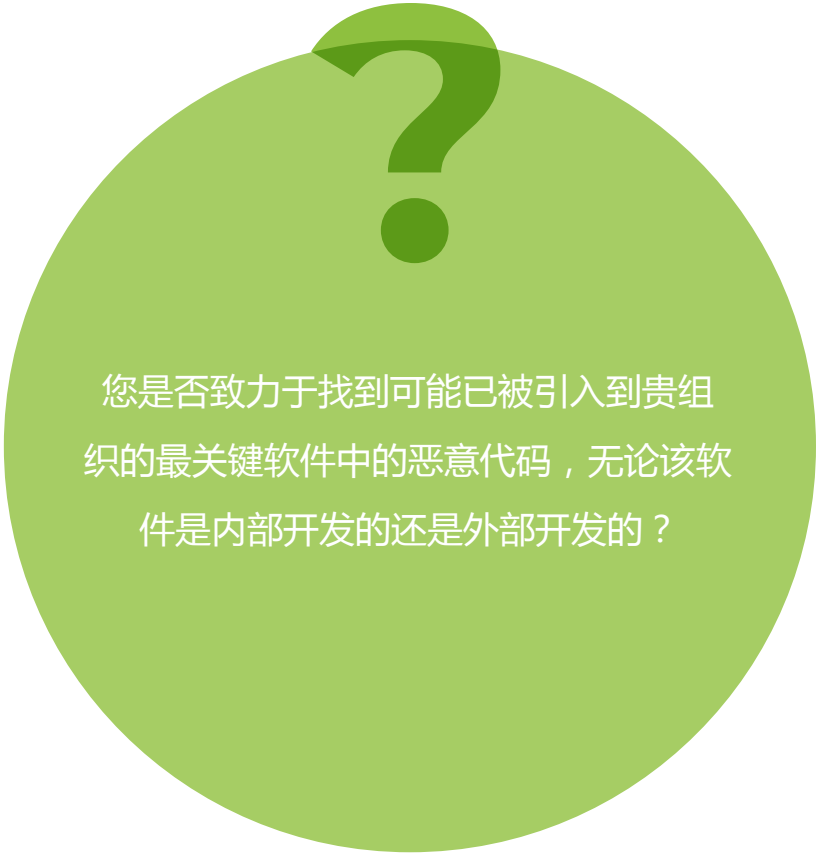
BSIMM参与者一直都在极大地改善功能性质量保证实践，在一些以工程为主导的企业中，弹性实践达到了令人印象深刻的成熟度。这些企业还添加了A/B测试、混沌工程和回滚机制等工程流程，以提高弹性。

就工程技术导向计划而言，许多安全活动自然的适用于质量保证实践。虽然SAST、SCA和DAST等安全测试工具历来都是作为由软件安全小组执行的带外活动来实施的，但这些活动仍有机会整合到质量保证自动化流程中。

软件安全自然也归于弹性实践。我们观察到，以工程主导的安全计划无论是在面对可靠性和可扩展性挑战时还是在面对攻击时，都有能力提供弹性。

这项工作需要专注于盘点软件、创建软件物料清单、了解软件的构建、配置和部署方式，以及企业基于安全遥测技术重新部署软件的能力。详细列出所有生产软件的组件、依赖项、配置和外部服务等事项的清单有助于加强企业安全态势。

与这些能力相关的BSIMM活动 — 通过运维物料清单来增强应用程序库存盘点— 在过去两年中急剧增加，表明许多企业已经开始重视制作全面的实时软件物料清单这一需求。



其他活动趋势

备受瞩目的勒索软件和软件供应链破坏促使软件安全日益受到关注

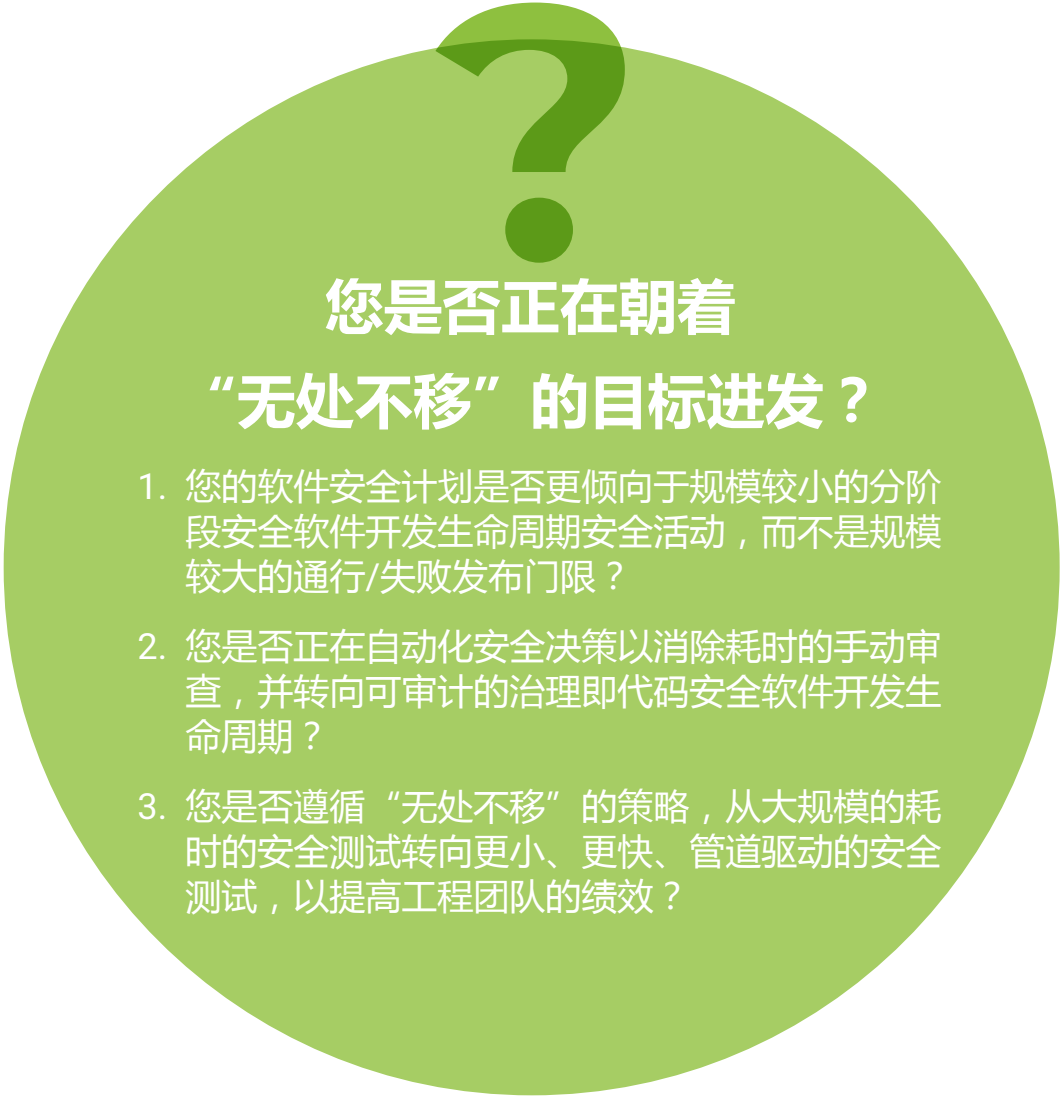
数据显示，在过去两年中，参与企业的 “识别开源代码” 活动增加了61%，“创建SLA样板文件” 活动增加了57%。鉴于媒体对攻击的报道越来越频繁，也许我们也将开始看到恶意代码检测活动的增加，这是目前很少观察到的活动。

管理层的日益关注，再加上工程化的驱动，也导致企业开始培养自己的云安全管理能力以及评估他们的责任分担的模型。过去两年中，通常与云安全相关的活动平均有36个新观察结果。然而，尽管管理层的关注度有所提高，但我们尚未看到直接面向管理层级别的宣导和准备工作得到相应提高。

“左移”变为“无处不移”，以更好地管理风险

如果“左移”侧重于在开发过程中更早地进行安全测试，“无处不移”则是扩展了在整个软件生命周期中持续进行安全测试的想法。这意味着尽早进行更小、更快、管道驱动的安全测试，例如从设计阶段开始，一路过渡到生产阶段。

从维护传统运营库存转向自动资产发现和创建物料清单需要添加“无处不移”活动，例如使用容器来强制实施安全控制、编排和扫描基础设施即代码。“通过运维物料清单来增强应用程序库存盘点”、“对容器和虚拟化环境使用编排功能”以及“通过自动化创建的资产能够被监控””等活动在BSIMM中的观察率的提高，都证明了这一趋势的存在。



企业开始学习如何将风险转化为数字

我们看到企业在收集和发布其软件安全计划数据方面付出了更多的努力，“在内部发布有关软件安全性的数据” 活动在过去24个月中的发布数据增加了30%便是很好的证明。

已经开始采用治理即代码的企业发现，首先构建软件安全指标对于成功实现治理愿景至关重要。

高风险应用的架构分析和设计审查变得越来越普遍

过去24个月中，“对高风险应用程序进行设计审查” 和 “定义/使用架构分析方法” 等活动的观察率增加了65%以上。

结论和建议

无论您是正在制定软件安全计划，还是已经开始维护成熟的计划，都应该已经实施或正在考虑实施以下关键操作：

- 尽可能地使用安全测试遥测技术。收集数据，例如执行了哪些测试以及发现了哪些问题，以推动改进您的软件开发生命周期和管理流程。在生命周期的各个阶段收集数据，并使用这些数据制定和实施软件安全策略。
- 向自动化安全决策转变。目标应是可审查的治理即代码，以便将安全实践与合规活动从手动转变为更一致、更高效、可重复性更强的自动方法。
- 创建全面的软件清单。该清单应包括贵组织资产的软件物料清单，以及开源和第三方代码。Gartner在其2020年《应用程序安全测试魔力象限》中预测，“到2024年，软件供应商提供详细的、定期更新的软件物料清单将成为至少一半企业软件买家不可协商的要求，而这一比例在2019年还不到5%。”[1] 虽然从理论上说，手动创建物料清单是可能的，但维护物料清单需要开展大量的工程和自动化工作。自动化工具生成的物料清单可以提供全面的信息（如特定版本、漏洞信息和所用代码的许可证等），对于开源代码，它还能帮助您更好地了解开源组件可能正在使用的依赖项。
- 在整个软件开发生命周期中实施小规模的、分阶段的安全活动。一开始要从小处着眼，不要使用会延迟管道进程的大规模的、缓慢的通行/失败门限。
- 自动化安全工具到位。这些工具可以识别并帮助您修复关键软件中的缺陷、漏洞和恶意代码，无论该软件是内部开发的、商业第三方软件还是开源软件。

您的安全计划能否跟上变化的步伐？

- 您是否使用数据驱动的证据 — 表示为遥测、测量、指标、KPI、KRI和OKR等 — 来制定软件安全投资成功与否的评估标准并对其进行跟踪？
- 您的软件安全计划是否考虑了云安全、容器安全、编排安全、源内容管理安全、开发管道安全和责任共担模型等规程对软件安全的影响？

如果您尚未制定正式的软件安全计划，请立即行动起来。

首先，为您的安全和开发团队创建可操作的路线图 - 如有必要，请聘请专业的软件安全评估团队来帮助您创建该路线图。评估您的安全计划的当前状态。定义您想要实现的未来目标状态，并确定您现在的状态与目标状态之间的差距。然后，将BSIMM12结果作为基线来考量同行开展的主要软件安全活动，据此制定您的行动计划。

[1] Mark Horvathh、Dionisio Zumerle和Dale Gardner，《应用程序安全测试魔力象限》，Gartner，2020年4月29日。

通过BSIMM提高安全意识和采用率

自1997年以来，Genetec Inc.一直提供一个涵盖安全，情报和运营的广泛的解决方案组合的创新技术。负责制定软件安全计划任务的Genetec首席安全架构师Mathieu Chevalier致力于推行一种安全至上的文化。Mathieu面临的关键问题之一便是证明其策略的明智性并培养广大受众对Genetec软件安全计划的信任，这要求Genetec采用经过验证的方法来制定计划。

Genetec使用新思科技的软件安全构建成熟度模型(BSIMM)评估来帮助Mathieu清楚了解公司当前的软件安全状况，并确定公司软件安全计划的需提高的领域。BSIMM评估为软件安全小组提供了模型和框架，用于对其当前的AppSec活动进行测试、评估和设定基准。BSIMM数据基于120多家企业的安全计划，针对软件安全小组应该在组织内部实施的关键活动、实践和工具提供了洞察。

GENETEC于2016年12月开始与BSIMM合作，在过去五年进行了两次评估

Mathieu表示，他当初决定对公司新兴安全计划进行BSIMM评估，这提供了重要的第三方洞察。他表示：“BSIMM帮助我们评估了我们的产品安全计划，并指导我们去往何处。对于任何制定产品安全计划的人来说，它都是一个宝贵的工具。”

近期，Genetec启动了第二次评估，以深入了解已经改进的领域和亟待改进的领域。第二次评估通过向安全团队以及整个企业展示新计划的好处来帮助Genetec就其正在实施的新计划赢得支持。

> “BSIMM帮助我们评估了我们的产品安全计划并指导我们去往何处。对于任何制定产品安全计划的人来说，它都是一个宝贵的工具。”

Genetec™

BSIMM评估是安全计划的基础

某家世界领先的技术公司十多年来一直都是BSIMM成员。其产品安全团队的高级经理表示：“BSIMM确实是我们安全拥护者和培训计划的基础。BSIMM评估对我们取得成功起到了重要作用，使我们能够知道公司软件安全计划在哪些方面比较成熟，在哪些方面还有待改进。BSIMM是帮助我们评估和提高安全计划成熟度的完美手段。”

安全拥护者和培训

该产品安全经理表示：“三年前当我加入公司时，我正式制定了拥护者计划，为注册参加该计划创建了适当的框架，根据需要对拥护者进行了培训，并通过互动不断为他们提供支持。我们目前有800多名安全拥护者。

我还负责安全培训。我们已经制定了渐进式的“安全段位带”(Security Belt)培训计划，从“黄带”（通过学习获得基本安全意识）开始，穿越“绿带”（安全编码培训和确保软件开发生命周期安全的最佳实践），然后进入更高级别的“蓝带”活动（我们用来构建产品和应用的技术，例如保护 Kubernetes REST API 的技术）。

为了加强安全拥护者计划，我们在制定该计划时考虑了我们从产品安全客户咨询中获得的知识和经验。通过收集这些信息，我们的安全拥护者不仅可以帮助处理客户咨询，而且还能了解客户的安全需求。我们使用这些信息来帮助安全拥护者了解行业现状，以及他们在通过确保产品和服务安全来促进销售方面所发挥的作用。”

> BSIMM是帮助我们评估和提高安全计划成熟度的完美手段。

BSIMM评估有何作用？

- 使您能够通过独立的评估数据向客户、合作伙伴、高管和监管机构展示贵组织的软件安全状况。当您在制定战略计划和做预算时，可以利用BSIMM评估数据让您的高管人员了解贵组织的现状并设定合理的目标。
- 评估您的成熟度，以便您可以分阶段演进的软件安全之旅，首先奠定坚实基础，然后随着时间的推移开展更复杂的活动。
- 提供来自现场的实测数据。BSIMM使您有可能制定长期的软件安全计划并跟踪其进度。
- 提供对BSIMM社区的访问权限。您可以参加年会和加入私人线上小组，就您的软件安全挑战提出问题，并从同行那里获得直接、保密的反馈。

致谢

我们感谢在撰写BSIMM12过程中所研究的全球各地软件安全计划的128位高管，其中包括那些选择保持匿名的人士。

AARP
Adobe
Aetna
Alibaba
Ally Bank
Autodesk
Axway
Bank of America
Bell
Black Duck Software
Black Knight Financial Services
Canadian Imperial Bank of Commerce
Cisco
Citigroup
Depository Trust & Clearing Corporation
Eli Lilly
eMoney Advisor
EQ Bank
Equifax
F-Secure
Fannie Mae
Finastra
Freddie Mac
Genetec
Global Payments
HCA Healthcare
Highmark Health Solutions
Honeywell
HSBC
iPipeline
Johnson & Johnson
Landis+Gyr
Lenovo
MassMutual
McKesson
Medtronic
MediaTek
Morningstar
Navient
Navy Federal Credit Union
NCR
NEC Platforms
NetApp
NewsCorp
NVIDIA
Oppo
PayPal
Pegasystems
Principal Financial Group
RB
SambaSafety
ServiceNow
Synopsys
TD Ameritrade
Teradata
The Home Depot
The Vanguard Group
Trainline
Trane
U.S. Bank
Veritas
Verizon Media

同时，我们感谢为帮助我们构建BSIMM而收集数据的近130名人员。

尤其是感谢Tony Blakemore、Matthew Chartrand、Eli Erlikhman、Jacob Ewers、Stephen Gardner、Iman Louis、Daniel Lyon、Sammy Migues、Alistair Nash、Kevin Nassery、Donald Pollicino、Brendan Sheairs、Denis Sheridan和Li Zhao。

每年安排几十次BSIMM评估活动需要付出巨大的努力，我们十分感谢Maatia Rickard提供的帮助。此外，还特别感谢Kathy Clark-Fisher，其在幕后完成的大量工作使得BSIMM科学项目、会议和社区能够始终运行在正轨上。

BSIMM12由Eli Erlikhman、Jacob Ewers、Sammy Migues和Kevin Nassery编写。

第三部分

附录

附录

BSIMM框架

BSIMM12在软件安全框架中被有组织的分为122项活动。该框架包括4个领域的12项实践，如表A所示。

领域			
 治理	 情报	 SSDL触点	 部署
用于协助组织、管理和评估软件安全计划的实践。人员培养也是一项核心的管理实践。	用于在企业中汇集企业知识以开展软件安全活动的实践。所汇集的这些知识既包括前瞻性的安全指导，也包括组织机构威胁建模。	与分析和保障特定软件开发工件（artifacts）及开发流程相关的实践。所有的软件安全方法论都包含这些实践。	与传统的网络安全及软件维护组织机构打交道的实践。软件配置、维护和其他环境问题对软件安全有直接影响。
实践			
管理	情报	SSDL触点	部署
1. 战略和指标 (SM) 2. 合规与政策 (CP) 3. 培训 (T)	4. 攻击模型 (AM) 5. 安全功能和设计 (SFD) 6. 标准和要求 (SR)	7. 架构分析 (AA) 8. 代码审查 (CR) 9. 安全性测试 (ST)	10.渗透测试 (PT) 11.软件环境 (SE) 12.配置管理和安全漏洞管理 (CMVM)

表A. 软件安全框架 *4大领域的12项实践。*

BSIMM轮廓

治理		
战略和指标 (SM)	合规与政策 (CP)	培训 (T)
第1级	第1级	第1级
• [SM1.1] 公布流程并按需演进。 • [SM1.3] 对高管人员进行软件安全培训教育。 • [SM1.4] 实施对开发周期各环节的检测并用于定义治理。	• [CP1.1] 统一监管压力。 • [CP1.2] 确定个人身份信息(PII)责任。 • [CP1.3] 制定政策。	• [T1.1] 开展软件安全意识培训。 • [T1.7] 提供按需个人培训。 • [T1.8] 在入职培训中加入软件安全性方面的内容。
第2级	第2级	第2级
• [SM2.1] 在内部发布有关软件安全性的数据并驱动改进。 • [SM2.2] 根据评估结果验证产品发布条件并跟踪异常。 • [SM2.3] 创建或扩大外围小组。 • [SM2.6] 要求在软件发布之前签发安全性证明。 • [SM2.7] 设立布道师岗位，开展内部宣传。	• [CP2.1] 确定PII数据清单。 • [CP2.2] 要求签发与合规相关的风险安全证明。 • [CP2.3] 实施并跟踪针对合规的控制。 • [CP2.4] 把软件安全性SLA纳入所有的供应商合同中。 • [CP2.5] 确保高管人员了解合规性和隐私义务。	• [T2.5] 通过培训和活动来提高外围小组的能力。 • [T2.8] 创建并使用与企业具体历史相关的材料。 • [T2.9] 提供与具体角色相关的高级课程。
第3级	第3级	第3级
• [SM3.1] 使用带组合视图的软件资产跟踪应用程序。 • [SM3.2] 将SSI纳入到对外推广计划中。 • [SM3.3] 确定指标并利用指标来要求获得资源。 • [SM3.4] 整合软件定义的生命周期治理。	• [CP3.1] 常态化为满足监管合规要求的信息收集工作。 • [CP3.2] 要求供应商执行政策。 • [CP3.3] 推动把来自软件生命周期数据的反馈纳入到政策中。	• [T3.1] 奖励通过课程的进步。 • [T3.2] 为供应商或外包人员提供培训。 • [T3.3] 举办软件安全性活动。 • [T3.4] 要求参加年度进修课程。 • [T3.5] 确定SSG定期服务答疑时间。 • [T3.6] 通过观察来发现新的外围小组成员。

表B. BSIMM轮廓 *在SSF中按不同级别组织的122项活动。*

情报		
攻击模型 (AM)	安全性功能和设计 (SFD)	标准和要求 (SR)
第1级	第1级	第1级
• [AM1.2] 制定数据分类方案和数据清单。 • [AM1.3] 识别潜在攻击者。 • [AM1.5] 收集并使用攻击情报。	• [SFD1.1] 集成并交付安全性功能。 • [SFD1.2] 让SSG参与到架构设计团队。	• [SR1.1] 制定安全性标准。 • [SR1.2] 创建安全性门户网站。 • [SR1.3] 把合规性约束转变成需求。
第2级	第2级	第2级
• [AM2.1] 构建与潜在攻击者有关的攻击模式和滥用案例。 • [AM2.2] 创建与特定技术相关的攻击模式。 • [AM2.5] 创建并维护前 N 种可能的攻击列表。 • [AM2.6] 收集并发布攻击案例。 • [AM2.7] 建立内部论坛来讨论各种攻击。	• [SFD2.1]利用“通过设计保证安全”（secure-by-design）组件和服务。 • [SFD2.2] 培养解决棘手设计问题的能力。	• [SR2.2] 成立标准审查委员会。 • [SR2.4] 识别出软件中所使用的开源代码。 • [SR2.5] 创建SLA样板文件。
第3级	第3级	第3级
• [AM3.1] 拥有一支开发新攻击方法的研究团队。 • [AM3.2] 创建并使用自动化方法来模拟攻击者。 • [AM3.3] 通过自动化创建的资产能够被监控。	• [SFD3.1] 成立审查委员会或中央委员会来批准并维护安全的设计模式。 • [SFD3.2] 要求采用获得批准的安全性功能和框架。 • [SFD3.3] 从企业中寻找并发布成熟的安全设计模式。	• [SR3.1] 控制开源风险。 • [SR3.2] 同供应商沟通标准。 • [SR3.3] 采用安全编码标准。 • [SR3.4] 为技术栈制定标准。

表B. BSIMM轮廓。*在SSF中按不同级别组织的122项活动。*

SSDL触点		
架构分析 (AA)	代码审查 (CR)	安全性测试 (ST)
第1级	第1级	第1级
• [AA1.1] 开展安全性功能审查。 • [AA1.2] 针对高风险应用程序开展设计审查。 • [AA1.3] 由SSG领导设计审查工作。 • [AA1.4] 使用风险评估方法为应用程序排序。	• [CR1.2] 开展机会性的代码审查。 • [CR1.4] 使用自动化工具。 • [CR1.5] 所有的项目都必须强制执行代码审查。 • [CR1.6] 使用集中报告来构建知识环路。 • [CR1.7] 指定工具辅导人员。	• [ST1.1] 确保QA执行支持边缘/边界值条件测试。 • [ST1.3] 推动结合安全性要求和安全性功能的测试。 • [ST1.4] 整合黑盒安全工具到QA流程中。
第2级	第2级	第2级
• [AA2.1] 定义并使用AA流程。 • [AA2.2] 标准化架构描述。	• [CR2.6] 使用自定义规则运行自动化工具。 • [CR2.7] 采用一份最重要 N 项缺陷列表（最好采用真实数据）。	• [ST2.4]与QA共享安全检查结果。 • [ST2.5] 将安全测试纳入到QA自动化中。 • [ST2.6] 开展专为应用API定制的模糊测试。
第3级	第3级	第3级
• [AA3.1] 让工程团队领导AA流程。 • [AA3.2] 推动把分析结果引入标准架构设计模式。 • [AA3.3] 使SSG能够作为导师指导AA实践。	• [CR3.2] 培养合并评估结果的能力。 • [CR3.3] 培养消除缺陷的能力。 • [CR3.4] 自动进行恶意代码检测。 • [CR3.5] 执行编码标准。	• [ST3.3] 推动结合风险分析的测试。 • [ST3.4] 利用（代码）覆盖分析。 • [ST3.5] 开始构建并应用对抗性安全测试（滥用案例）。 • [ST3.6] 在自动化中实施事件驱动的安全测试。

表B. BSIMM轮廓。 *在SSF中按不同级别组织的122项活动。*

部署		
渗透测试 (PT)	软件环境 (SE)	配置管理和安全漏洞管理 (CMVM)
第1级	第1级	第1级
• [PT1.1] 聘请外部渗透测试人员来查找问题。 • [PT1.2] 把结果反馈至缺陷管理和修复缓解系统中。 • [PT1.3] 在内部使用渗透测试工具。	• [SE1.1] 进行应用程序输入监控。 • [SE1.2] 确保主机及网络安全基础能力就位。	• [CMVM1.1] 创建事件响应机制或者与事件响应团队交流。 • [CMVM1.2] 通过运维监控发现软件缺陷并将其反馈给开发团队。
第2级	第2级	第2级
• [PT2.2] 渗透测试者使用所有可用的信息。 • [PT2.3] 定期开展渗透测试，以提高应用程序覆盖情况。	• [SE2.2] 定义安全部署参数和配置。 • [SE2.4] 保护代码完整性。 • [SE2.5] 使用应用程序容器来支持安全目标。 • [SE2.6] 确保具备云安全基础能力。 • [SE2.7] 对容器和虚拟化环境使用编排功能。	• [CMVM2.1] 建立紧急响应机制。 • [CMVM2.2] 通过修复流程跟踪运维过程中发现的软件错误。 • [CMVM2.3] 制定软件交付价值流的运维清单。
第3级	第3级	第3级
• [PT3.1] 聘请外部渗透测试人员开展深度分析。 • [PT3.2] 定制渗透测试工具。	• [SE3.2] 进行代码保护。 • [SE3.3] 进行应用程序行为监控和诊断。 • [SE3.6] 通过运维物料清单来增强应用程序库存盘点。	• [CMVM3.1] 修复运维过程中发现的所有软件错误。 • [CMVM3.2] 增强SSDL，以防止运维期间再次发生软件错误。 • [CMVM3.3] 模拟软件危机。 • [CMVM3.4] 启动鼓励发现软件错误的计划。 • [CMVM3.5] 自动验证基础运维设施安全。 • [CMVM3.6] 发布可部署工件的风险数据 • [CMVM3.7] 简化外部漏洞报告者与内部相关人员的沟通流程。

表B. BSIMM轮廓。*在SSF中按不同级别组织的122项活动。*

BSIMM在线社区

BSIMM在线社区是一个独特的会员制论坛，可以帮助您应对当今复杂业务环境中的软件安全挑战。

完成BSIMM评估的企业可以访问会员制的BSIMM社区网站。

作为会员，您可以：

- **定期接收探讨最佳实践、技巧和案例研究的博客文章和跟帖。**
- **从这个700名会员的社区中寻找灵感和问题的答案。**
- **参加专属会议。**

从行业领袖创作的内容、到与BSIMM成员进行实际互动，BSIMM在线社区是强大的平台，可以帮助您协同解决问题、培养思维领导力、获得从其他任何地方都无法获得的宝贵资源。

希望了解如何访问引人入胜的BSIMM 会员制社区，包括会议、新闻稿和原创内容。

请访问www.bsimm.com