SYNOPSYS®

2023年全球DevSecOps现状调查

影响软件安全的策略、工具和实践

概述

关于Synopsys《2023年DevSecOps现状调查》报告

2023年初，Synopsys网络安全研究中心(CyRC)联合国际市场研究咨询公司Censuswide，对负责安全事务的1,000名IT专业人士开展了一项调查。受访者包括开发人员、AppSec专业人员、DevOps工程师、CISO以及在技术、网络安全和应用/软件开发领域担任各种职务的专家。受访者来自美国、英国、法国、芬兰、德国、中国、新加坡和日本。

所有的受访者都有资格参与调查，与其所属行业和公司规模无关。开发本次调查面临的挑战之一是“DevSecOps”一词涵盖了多个学科，其中许多学科都有自己独特的角色。本次调查希望覆盖不同专业背景的人士，既包括“直接”编写代码的开发者，也包括从事软件安全相关工作的CISO级别的人员

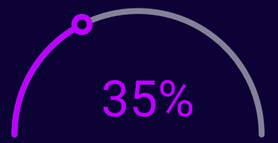
关于DevOps和DevSecOps

加速开发、持续交付、管道弹性、可扩展性和端到端透明度是实现DevOps的关键原则。满足这些标准需要开发、安全和运维人员共同努力。

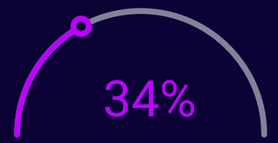
DevSecOps是DevOps方法论的延伸，旨在向多个团队灌输安全文化，并且尽早在DevOps环境中通过一致的方式来解决安全问题。通过将安全实践集成到软件开发生命周期(SDLC)和CI管道中，DevSecOps旨在将安全性从一个独立的阶段转变为开发生命周期的一部分。

DevSecOps在涉及软件开发的各个组织中都广受欢迎。SANS《2023年DevSecOps现状调查》显示，DevSecOps已经成为一种重要的业务实践和风险管理方法。但在过去，当安全团队和开发团队试图把安全性纳入他们的流程时，经常会有不同意见，这很大程度上是因为这种做法会把传统的应用安全测试(AST)工具引入软件开发生命周期(SDLC)。开发者经常抱怨AST工具太复杂、难以学习、性能低下以及产生大量“噪音”，这些都会给DevOps带来“摩擦” —— 也就是，那些在软件开发过程中阻止开发人员轻松快速构建代码的各种东西。

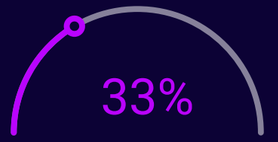
大多数受访者表示，他们对自己使用的AST工具普遍感到不满



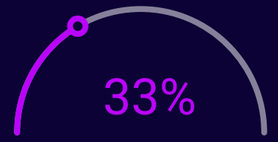
工具不能根据漏洞的暴露程度、可利用性和严重程度来确定修复顺序



因速度太慢而无法适应快速的发布周期/持续部署



性价比低



不准确/不可靠

自动化的好处

DevOps的核心原则是在SDLC的每个阶段都自动执行手动流程。对任何组织而言，自动化都是通过持续集成或持续部署来加速开发和交付代码的基本前提。

成功的DevSecOps需要集成和自动化的相互作用，以及标准和策略的指导。这样，既能让安全团队相信安全利益得到了保障，又能让DevOps团队保持工作状态，相信不会发生管道中断的情况。

与手动测试不同，自动安全测试可以快速一致地执行，使开发人员能够在开发过程的早期阶段发现问题，不会影响到交付进度或工作效率。

一致性

自动测试可确保对每一次的构建和部署一致地进行安全检查。手动测试可能会导致测试过程和覆盖范围不一致。

可扩展性

随着软件复杂性的增长，手工测试将变得不切实际。自动测试容易扩展，以便跨越不同组件进行大量测试。

持续集成和持续部署(CI/CD)

自动测试在CI/CD管道中至关重要，因为这些管道中会发生快速而频繁的代码变更。自动测试可以快速验证变更，防止错误代码进入生产环境。

持续改进

自动测试提供数据和洞察，可以帮助开发和安全团队随时间的推移改进安全实践，允许他们系统地分析和处理漏洞模式。

记录

自动测试可以记录整个测试过程，从而更容易跟踪和审计安全措施与合规要求。

减少人为错误

由于疲劳或疏忽，手动测试容易出错。自动测试遵循预定义的脚本，能够降低人为错误的风险。

节省时间和成本

在开发过程的后期或生产过程中识别和修复安全问题既耗时又昂贵。自动测试可将这些费用降至最低。

改进开发者体验

自动的应用安全测试允许开发者采取主动的、全面的、有助于学习和提高安全知识和技能的方式来解决安全问题，从而增强开发者体验，最终提高软件安全性并提升整个开发过程的效率。.

ASOC/ASPM在 DevSecOps中的应用日益增长

本报告对处于DevSecOps不同成熟阶段的组织进行了考察，包括他们的特征，以及他们采用的安全工具/实践。我们将根据调查结果为其提供指导性建议，帮助他们进一步提高软件安全的成熟度。

有趣的是，从调查结果中可以看出，应用安全编排与关联(ASOC) — 现在一般称为“应用安全态势管理”(ASPM) — 的使用越来越普遍。根据Gartner的说法，对于使用多种开发和安全工具的任何组织而言，ASPM都应该是优先考虑的重要事项。

从开发到部署，ASPM解决方案能够持续管理各种应用风险，包括安全问题的检测、关联和优先级排序。ASPM工具可以从多个来源获取数据，然后关联并分析它们，以实现更轻松的解释、分类和补救。

ASPM还充当安全工具的管理和编排层，支持安全策略的控制与实施。ASPM拥有应用程序安全结果的综合视角，从而提供了整个应用程序或系统的安全与风险状态的完整视图。

鉴于这1,000名受访者中的大多数人都对其正在使用的AST工具普遍感到不满 — 抱怨这些工具无法根据业务需求确定修复的优先级 (35%)，也无法合并/关联数据来帮助解决问题(29%) — 因此，ASOC/ASPM的使用呈现快速增长趋势也在情理之中。

28%的受访者表示，他们的组织使用了ASOC工具

Synopsys《2023年DevSecOps现状调查》的主要发现

大多数DevOps团队都在某种程度上采用了DevSecOps

共有91%的受访者表示，他们已将开展DevSecOps活动的某些安全措施纳入到了软件开发管道中。可以肯定地说，采用DevSecOps方法论现已成为软件开发的一部分。

拥有更成熟的安全计划的组织有专人负责安全事务

29%的受访者表示，他们拥有跨职能部门的DevSecOps团队 — 由开发、安全和运维部门成员构成的协作团队，这是安全计划取得成功的重要因素。专注于安全、与开发人员/软件工程师和/或 QA 和测试合作的人员可能处于拥有成熟安全计划的组织中安全测试的第一线。

有效实施DevSecOps存在许多障碍

超过33%的受访者指出，缺乏安全培训是主要障碍。紧随其后的是安全人员短缺(31%)、开发/运维工作缺乏透明性(31%)以及优先事项的不断变化(30%)。

超过三分之一的受访者表示，将自动安全测试集成到构建/部署工作流中是安全计划取得成功的关键

其他的主要成功因素还包括通过基础架构即代码来执行安全/合规策略，在开发和运维团队中培养安全支持者(security champions)，以及加强开发、运维和安全团队之间的沟通等。

在SDLC后期处理重大漏洞，会极大地削弱收益

超过80%的受访者表示，2022-2023年间，已部署软件中的重大漏洞/安全问题以某种形式影响了他们的工作进度。

28%的受访者表示，他们的组织需要长达三周的时间来修补已部署应用程序中的重大安全风险/漏洞；另有20%的受访者表示，这可能需要一个月的时间

考虑到现在的漏洞利用速度比以往任何时候都要快，这些数字尤其令人感到不安。最新研究表明 超过一半的漏洞在披露后的一周内即被利用。

超过70%的受访者表示，通过自动扫描代码来查找漏洞或编码缺陷是一种有用的安全措施，34%的受访者认为自动AST“非常有用”

对代码进行安全漏洞和其他缺陷的自动化扫描，在“工具/流程的有用性”类别中排名第一，紧随其后的是“在SDLC的需求挖掘阶段明确安全需求”以及“通过BSIMM和SAMM等模型对软件安全计划进行正式评估”。

几乎所有的受访者都认为AST工具与其业务需求不符

在1,000名受访者中，大多数人都认为AST工具存在各种各样的问题是他们面临的主要挑战，包括这些工具无法根据业务需求对修复措施进行优先级排序(35%)，也无法合并/关联数据来帮助解决问题(29%)。

52%的安全专业人员已经开始在DevSecOps活动中积极使用AI，但超过四分之三的人担心AI的使用问题

调查结果表明，安全团队正在积极使用AI、机器学习、自然语言处理和神经网络。然而，随着生成式AI工具（如AI驱动的编码建议）的使用日益增多，引发了围绕AI所生成代码的一系列知识产权、版权和许可问题，某些情况下甚至引起了诉讼。

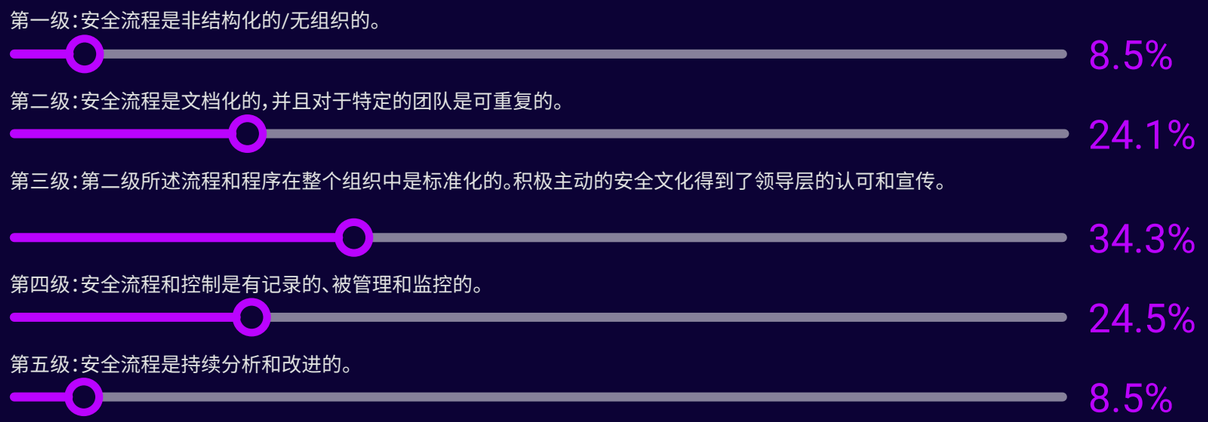
2023年DevSecOps现状调查

DevSecOps部署

在1,000名受访者中，超过三分之一的受访者认为其安全计划已经达到了成熟度的第三级，即整个组织的安全流程都是文档化的、可重复的和标准化的。另有25%的受访者认为其安全计划已经达到了第四级，即安全流程也被记录，同时还被监控和评估。

共有91%的受访者表示，他们已将某种类型的DevSecOps活动应用到软件开发管道中，采用DevSecOps似乎已成为DevOps的既定组成部分。

图 A 您认为贵组织当前的软件安全项目/计划的成熟度处于哪一级?



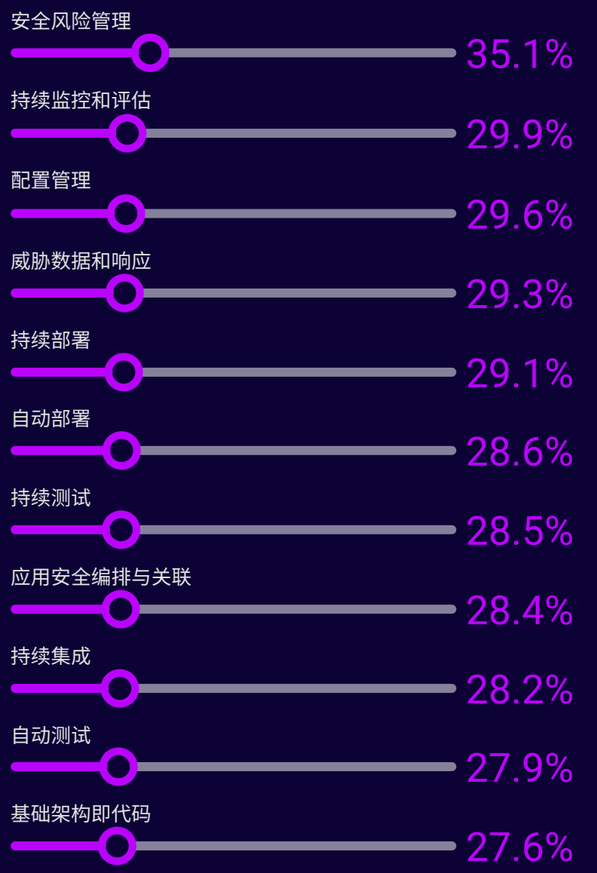
安全实践的实施代表更高级别的成熟度

DevSecOps成熟度的另一个衡量标准如图B所示，表明受访者已经采用了广泛的安全实践，从持续监控和评估(30%)到自动测试(28%)。

作为被358名受访者(35.1%)提及的最佳实践，“安全风险管理”涉及在开发过程中的每个阶段整合安全考虑因素，以识别、评估和减轻与软件应用相关的潜在安全风险。在SDLC的框架下，整体安全风险管理涵盖以下活动：

- **需求分析。在SDLC中尽早识别安全需求和限制，并定义安全目标。**
- **设计。将安全原则纳入到系统架构和设计中，以确保应用程序的设计包含针对常见漏洞的适当防护措施。**
- **开发。实施安全编码实践，并遵守解决安全问题的编码标准。使用集成的安全测试工具，如静态应用安全测试(SAST)和软件组成分析(SCA)，在编写代码和引入开源或第三方代码时捕获漏洞。**
- **测试。执行各种类型的安全测试来识别应用程序中的漏洞，如SAST、动态应用安全测试(DAST)、SCA和渗透测试。**
- **部署。安全地配置应用程序的运行环境。实施访问控制、网络安全以及适当的身份验证和授权机制。**
- **监控与评估。持续监控生产环境中的应用程序，以发现安全事件和异常情况。实施日志记录和监控解决方案，以检测和响应潜在的违规行为。30%的受访者表示，这是其组织采用的主要安全实践。**
- **响应和补救。制定事件响应计划，以快速有效地处理安全事件。修复在测试阶段检测到的问题。**
- **透明度和安全性。建立明确的规范、标准和策略，并报告安全风险和风险容忍度。**
- **培训。为开发团队提供安全编码实践、常见漏洞和最佳安全实践方面的培训，以使开发人员能够主动解决安全问题。遗憾的是，34%的受访者认为，“开发人员/工程师的安全培训不足/无效”是导致其组织无法有效实施DevSecOps的主要障碍之一。**
- **持续改进。定期审查和改进SDLC中的安全流程和实践。**

图 B 贵组织采用哪些安全实践？(选择所有的适用项)



评估安全计划

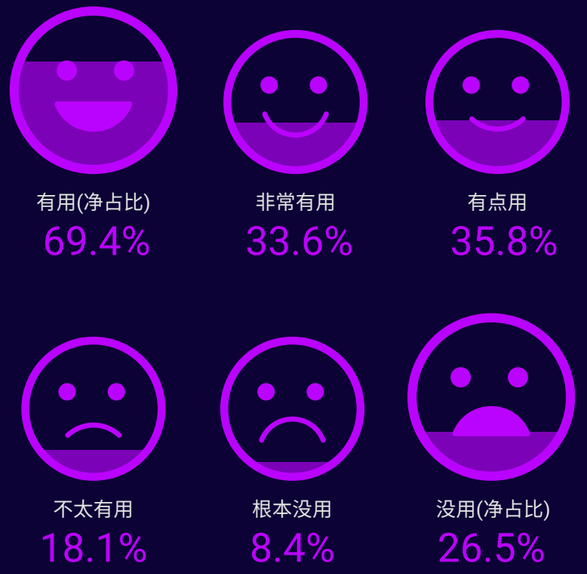
近70%的受访者表示，通过软件安全构建成熟度模型(BSIMM)等评估工具来评估其安全计划是有用的，超过三分之一的受访者认为此类评估“非常有用”。

对安全态势进行外部评估，有助于您分析软件安全计划，并将其与其他组织和同行进行比较。BSIMM等工具能够提供数据驱动的客观分析，可以帮助您在此基础上做出资源、时间、预算和优先级决策。无论您是刚开始实施安全计划，还是想让现有计划适应不断变化的业务和安全需求，与其他软件安全计划进行比较都能为您的策略提供指导。

如果您正在负责软件安全计划或刚刚开始制定软件安全计划，了解同行的AppSec趋势可以帮助您对自己的安全工作做出战略性的改进。如果您从技术角度来管理安全计划，可以借助BSIMM或软件保障成熟度模型(Software Assurance Maturity Model, SAMM)评估所获得的信息，为人员和流程制定战术性的改进方案，例如制定安全支持者(Security Champions)计划。

事实上，根据 BSIMM报告 许多软件安全团队首先要做的事情之一就是找出那些在软件安全方面起到推动作用但与软件安全团队没有直接联系的人员。这些人统称为“软件安全支持者”，能够支持和推动软件安全工作。例如，工程团队中的安全支持者可以鼓励工程师对自己的软件交付件的安全负责。33%的受访者认为，制定安全支持者计划是软件安全计划取得成功的关键因素之一。

图 C 通过BSIMM和SAMM等模型对软件安全性进行正式评估的有效性.



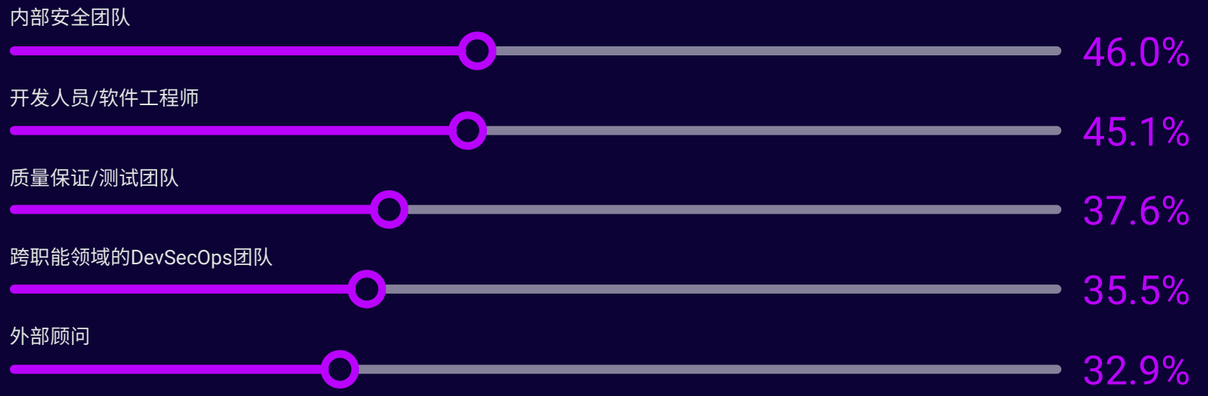
跨职能团队对DevSecOps取得成功的重要性

29%的受访者指出，跨职能的DevSecOps团队 — 由开发、安全和运维人员组成的协作团队 — 是安全计划取得成功的关键（见附录Q16）。安全专业人员，与开发人员/软件工程师及/或质量保证和测试团队协作（无论是正式加入DevSecOps团队还是其他方式），都可能成为安全测试的第一道防线，助力组织打造更成熟的安全计划。

在部署前后仅由安全团队进行单一的流水线式测试已成为过去式。在当今的软件开发环境中，安全测试是整个工程团队的责任，包括质量保证、开发和运维团队，并且大多数团队都会在软件开发生命周期的不同阶段将安全性构建到他们的软件中。

33%的受访者表示，他们的组织也会聘请外部顾问进行安全测试。这里的最佳实践是定期进行安全审计。委托第三方审计人员或渗透测试人员开展此类测试，有助于客观了解整个组织的安全态势，这是非常宝贵的。

图 D 贵组织由谁负责安全测试？（选择所有的适用项）

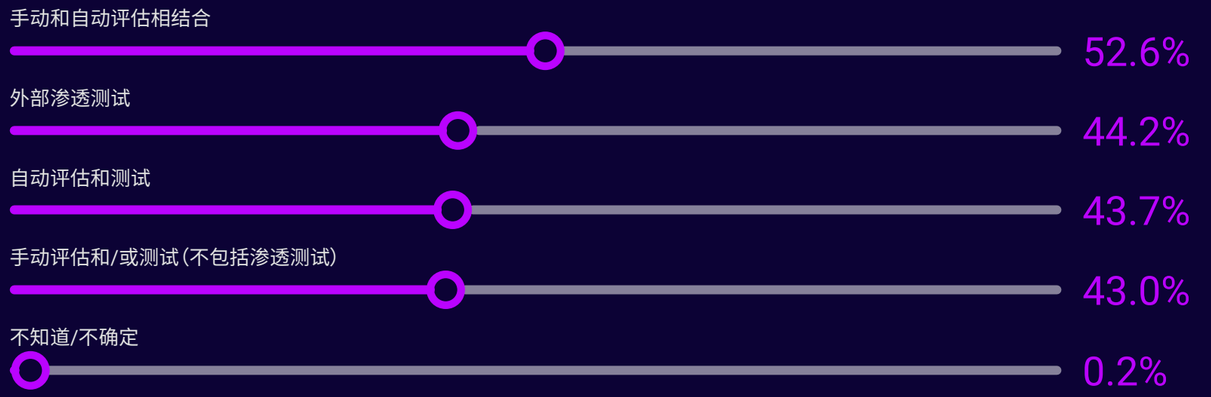


手动和自动测试相结合，以取得最佳结果

调查结果显示，大多数受访者认为，将手动和自动安全测试相结合，可以提供一个更全面的方法来评估关键业务应用的安全性。自动测试虽然对于保持一致性、可扩展性以及节省时间和成本很重要，但人工参与可以增加一层洞察力和适应性，这对识别复杂和微妙的安全问题是必不可少的。例如，作为“黑盒”测试（即，在不了解应用内部结构的情况下开展测试），DAST就需要开发者和安全专家对测试结果进行验证和分类。

同样，44%的受访者将外部渗透测试视为其安全测试的关键组成部分，这一事实证明了渗透测试对内部测试起到重要的补充作用。外部渗透测试通常是为了符合行业规范和标准，能够带来额外的好处，例如提供有关贵组织安全态势的客观评估，以及对外部攻击者可能利用的潜在威胁和漏洞的准确模拟。

图 E 您如何评估或测试关键业务应用的安全性？（选择所有的适用项）



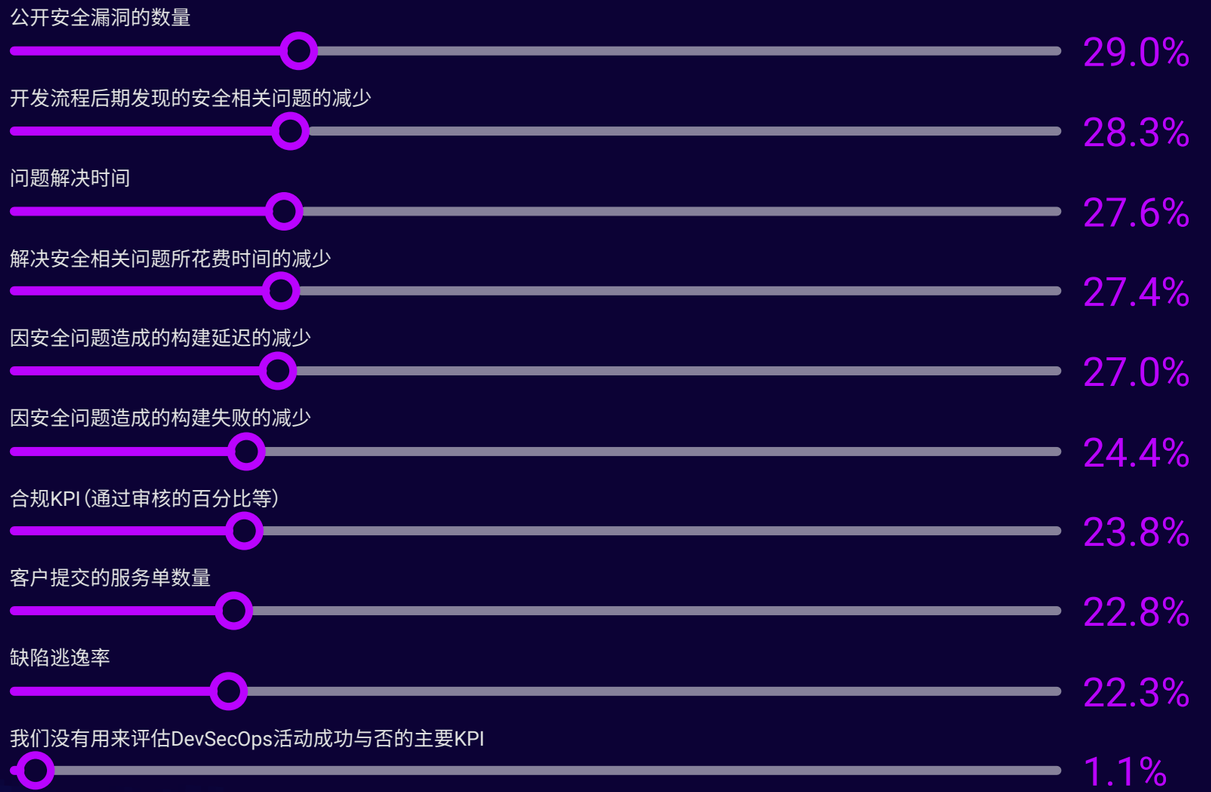
关键绩效指标

本次调查要求受访者选择评估其DevSecOps计划成功与否的前三个关键绩效指标(KPI)。首当其冲的是“公开漏洞的总体减少”，被295名受访者提到(29%)，紧随其后的是“SDLC后期发现的安全相关问题的减少”，被288名受访者提到(28%)，排在第三位的“问题解决时间”，有281名受访者提到了这一点(28%)。

正如调查结果所示，时间、生产率和成本是前面几个KPI的三个共同点，也是组织在实现安全SDLC时面临的挑战。或者，换句话说，DevSecOps参与者面临的三个主要问题是：

- **我们如何减少遇到的漏洞/问题的数量?**
- **我们如何在SDLC中更早地发现漏洞?**
- **我们如何缩短解决问题所需的时间，以减少构建延迟并提高开发效率?**

图 F 您用来评估DevSecOps活动成功与否的主要KPI是什么?(最多可选3项)



您正在使用哪些AST工具?它们有用吗?

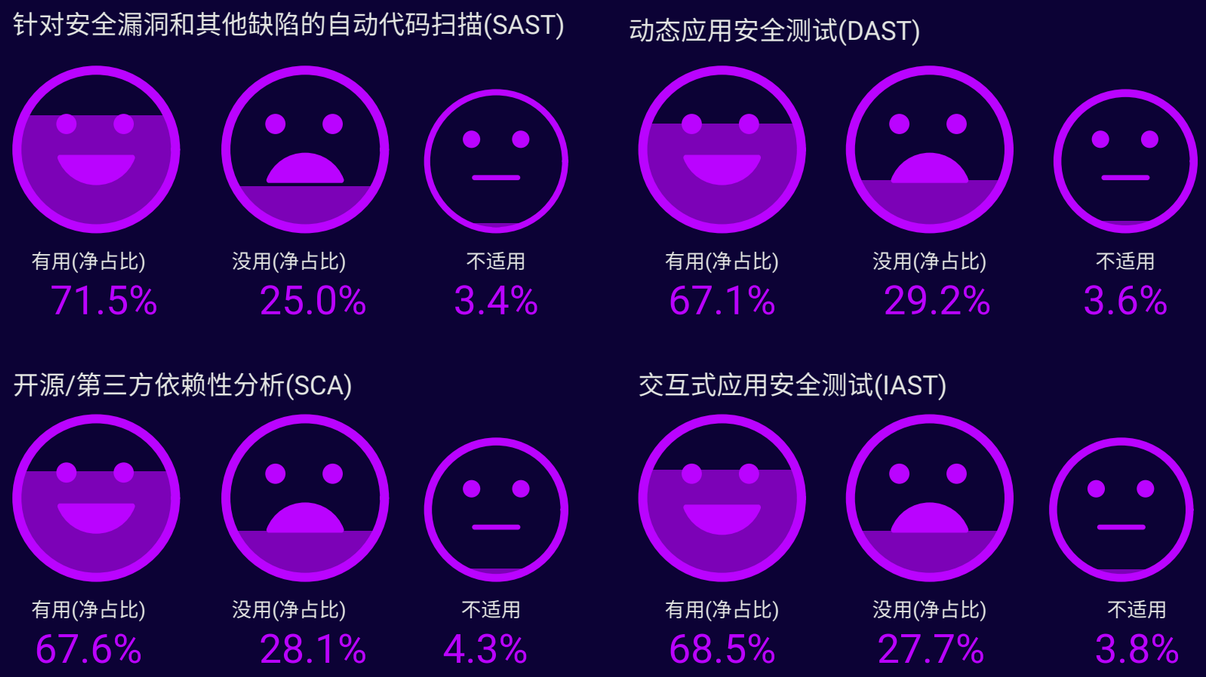
调查结果显示，成功的DevSecOps策略使用完整的安全工具集来处理整个软件开发生命周期中的代码质量和安全问题，包括动态应用安全测试(DAST)、交互式应用安全测试(IAST)、静态应用安全测试(SAST)和软件组成分析(SCA)工具。

调查结果显示，SAST是最欢迎的AST工具，72%的受访者认为它很有用。紧随其后的是IAST(69%)、SCA(68%)和DAST(67%)。

SAST和DAST采用不同的测试方法，适用于不同的 SDLC阶段。SAST对于在SDLC早期（即应用部署之前）发现和消除专有代码中的漏洞至关重要。而DAST则适用于在部署之后发现运行过程中出现的问题，如身份验证和网络配置缺陷。IAST则结合了SAST和DAST的某些功能，适用于检测无法被其他类型的测试识别到的重大安全缺陷。

SCA适用于识别和管理开源安全和许可风险，这是现代软件开发中的一个关键需求，尤其是在任何给定应用中可能都有超过四分之三的代码是开源代码的情况下。由于许多组织都在使用从独立软件供应商处购买的打包软件，以及物联网(IoT)设备和嵌入式固件，因此，他们可能还需要在其AST工具箱中开展某种形式的SCA二进制分析。

图G 贵组织使用的下列应用安全工具有用吗（如果有的话）？



何时进行测试?何时打补丁?这对我们的工作进度有何影响?

应用安全测试的频率取决于多个因素，包括应用程序的业务关键性、行业和威胁情况等。正如我们的调查结果所示，对于非常重要的应用程序，应定期进行评估（图H）。参与本次调查的大多数受访机构都表示，他们平均每周对业务关键型应用进行两到三天的漏洞扫描。

乍看之下，调查结果显示有28%的组织需要花费长达三周的时间来修补重大漏洞（图I），这可能令人担忧，但这要结合其他因素来考虑。有种误解，以为传说中的开发者能够修复所有漏洞，但没有人会无端地要求开发者去深入研究那些不重要的漏洞。

值得注意的是，关于实施DevSecOps的主要障碍，31%的受访者认为是“开发/运维工作缺乏透明性”，29%的受访者认为是“开发、运维和安全之间的组织孤岛”（图K）。这两项都表明了安全和开发团队之间的风险沟通问题，以及安全策略快速告警和自动化的需求。

在任何情况下，漏洞修补的优先级排序都要与待修补资产的业务重要性、关键性和资产被利用的风险相一致，尤其是最后一点。研究表明，超过一半的漏洞在披露后一周内被利用。

图 H 贵组织平均多久对关键业务应用的安全性开展一次评估或测试?

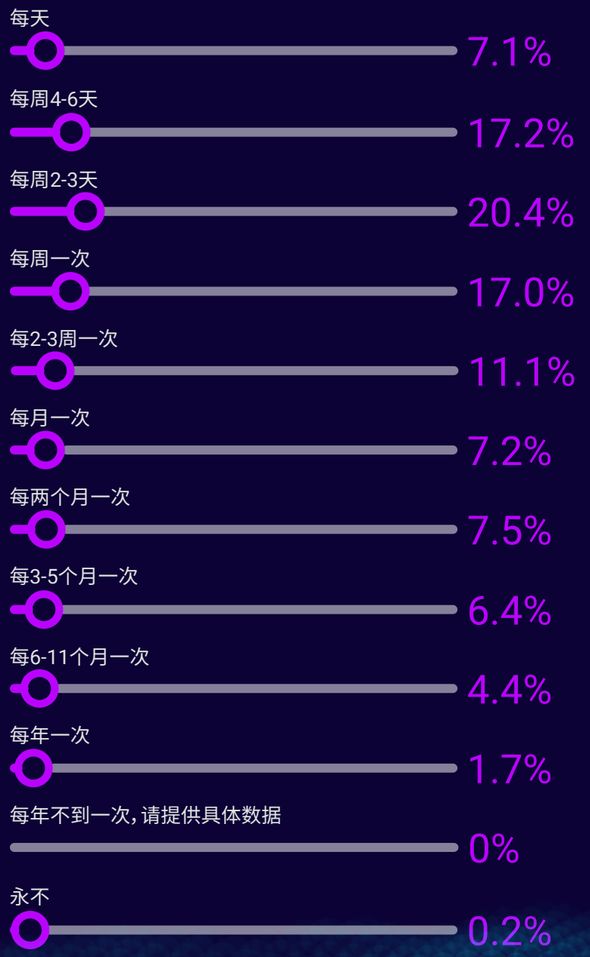
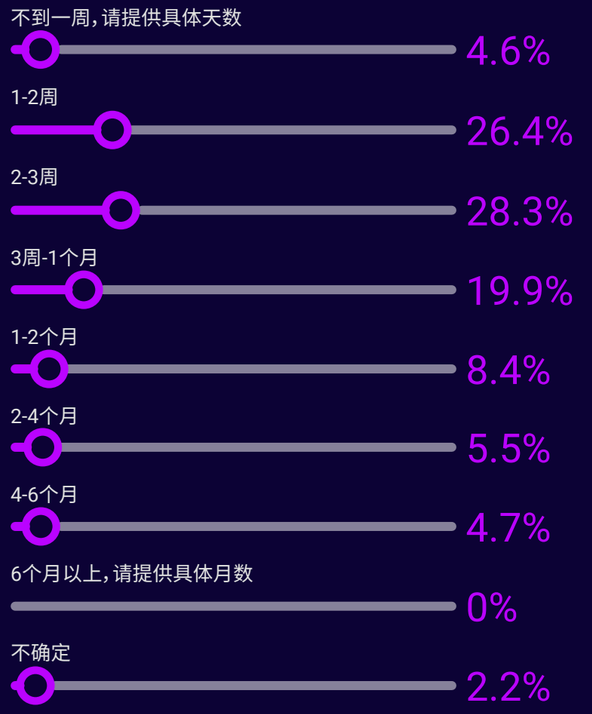


图 I 贵组织平均需要多长时间才能修补/处理已部署的或正在使用的应用程序中的重大安全风险/漏洞?



鉴于此，组织需要根据通用漏洞评分系统(CVSS)的分数、通用弱点枚举(CWE)信息以及漏洞可利用性等因素对漏洞修复进行优先级排序，这一原则不仅适用于漏洞披露的“第零天”，还适用于应用程序的整个生命周期。

CVSS分数是评估危险严重性的一个工业标准。国家漏洞数据库(NVD)中的每个漏洞都有一个基本分数，可以帮助计算漏洞的严重性，并为漏洞修复的优先级排序提供指导。CVSS分数是在结合考虑漏洞可利用性和影响的基础上给出的一个综合性基础分数。

时间分数考虑由于漏洞外部事件而随时间变化的指标。修复水平（是否有官方的修复方案?）和报告置信度（报告是否经过确认?）可以帮助将CVSS的总体分数调整到适当的风险水平。

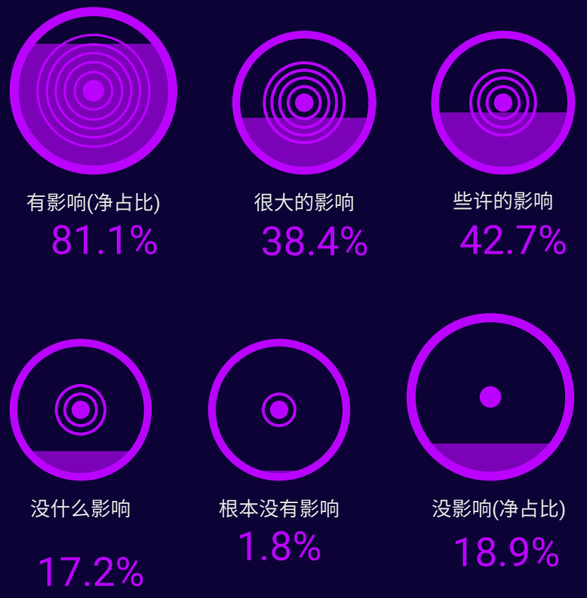
CWE信息列出了具有安全影响的软件或硬件缺陷。CWE告诉开发人员哪些缺陷可以被利用（如果有可用的漏洞）。这些信息可以帮助安全和开发团队了解开发人员安全培训的重点，在SDLC和生产中实施哪些额外的安全控制，以及是否需要添加风险严重性评估机制。例如，开发团队可能会根据应用程序所接触的数据情况、部署位置以及其他环境和安全因素，对SQL注入、缓冲区溢出或拒绝服务分配不同的优先级。

漏洞的存在会提高风险分数，有助于工作团队优先安排修复风险最高的漏洞。在评估了总体风险之后，还需要了解是否有现成的补丁、缓解措施或补偿控制，这是您需要考虑的另外一些关键信息。例如，如果您有两个中等风险但未被利用的漏洞，那么，先修复哪一个漏洞最终可能取决于它们是否存在现成的补丁或解决方案。

在已部署的应用程序中，重大的安全或漏洞问题往往会产生连锁效应，不仅会影响组织（或其客户）的业务运营，还会对整个SDLC造成影响，如图J所示。

如果问题在开发早期就被发现，那么，这些问题可能只是小问题，但如果是在部署后的应用程序中被发现，则这些问题可能会演变成“全员参与”的重大问题。集成到IDE和CI管道中的自动安全测试工具可以在代码提交后立即（甚至在提交之前）识别出代码中的漏洞和缺陷，使开发人员能够在问题传播到下游之前解决它们。

图 J 在过去的一年（2022-2023年），解决一个重大安全/漏洞问题对贵组织的软件交付计划产生了多大的影响（如果有的话）？



有效DevSecOps面临的挑战

网络安全人才短缺是DevSecOps面临的一个重大挑战，如图K所示，许多组织的关键网络安全岗位都无法招聘到合格人员。一些研究显示，全球有350万个网络安全职位空缺。随着市场对训练有素的网络安全专业人士的需求日益增长，供应的稀缺将导致熟练从业人员的工资上涨，使许多政府机构和中小企业无法负担。但是，正如图K所显示的那样，“开发人员/工程师的安全培训不足”仍是排在首位的最大挑战。

经证实，建立安全支持者计划是解决这些问题行之有效的策略，即从组织内部的各个部门挑选出对安全有着高于平均水平的兴趣或技能的人员（这些人员已经开始利用自己的专业知识为开发、质量保证和运维团队提供支持）。安全支持者可以为新项目出谋划策和提供反馈，也可以在新兴或快速变化的技术领域，帮助安全或工程团队将软件安全技能与他们可能欠缺的领域知识相结合。敏捷教练(Agile coaches)、敏捷项目管理人员(scrum masters)和DevOps工程师都是非常适合的安全支持者人选，特别是在发现和消除流程中的摩擦方面。

图 K 贵组织实施DevSecOps的挑战/障碍是什么？（选择所有的适用项）

如本报告前面所述，SAST、DAST、IAST和SCA等AST工具都已被受访者广泛使用，但将这些工具与业务需求有效挂钩仍然是一个挑战（图L）。

许多受访者都抱怨说，他们使用的安全测试工具无法根据安全漏洞的暴露程度、可利用性和严重程度等因素对修复工作进行优先级排序；因为速度太慢而无法适应快速发布周期/持续部署；不准确且不可靠。

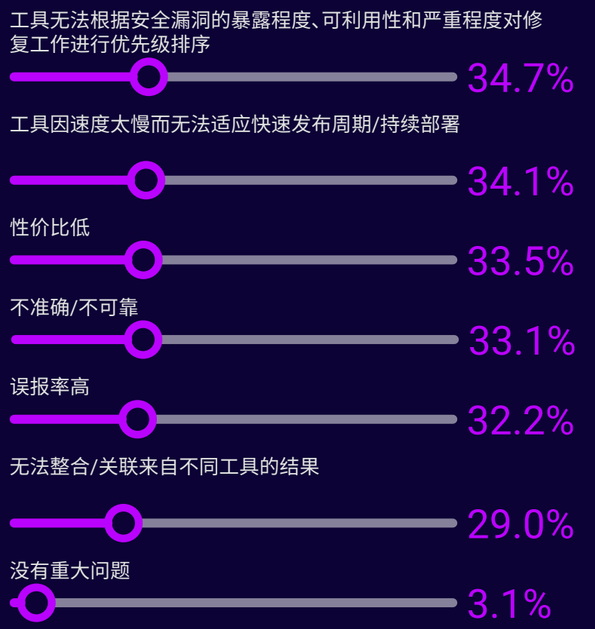
由于无法整合或关联不同安全测试的结果，安全和DevOps团队花费了太多时间来确定需要率先修复的漏洞 — 这可能是近四分之三的受访者指出他们的组织需要两周到一个月的时间来修补已知重大漏洞的原因之一（图I）。

不能迅速修补漏洞会影响到根本利益。超过80%的受访者表示，2022-2023年间，处理已部署软件中的重大漏洞或相关安全问题影响了他们的工作进度（图J）。

AST工具碎片化和修复速度缓慢正是应用安全编排与关联(ASOC)和应用安全态势管理(ASPM)旨在解决的问题。Gartner指出ASOC/ASPM可以作为管理层来编排多个AST工具，自动对发现的问题进行关联和上下文分析，以加快和优化修复过程。

ASOC/ASPM可以提取并整合多个来源的结果，就整个应用环境提供统一风险视图，从而允许您基于业务背景（如严重程度）对修补工作进行数据驱动的优先级排序，以促进对最高风险漏洞的更快修补。ASOC/ASPM还能提供生产环境的可视化，从而解决已部署应用中漏洞修复时间过长的问题，帮助有效避免漏洞利用（大多数的漏洞利用都发生在漏洞披露后的几天内）。.

图 L 贵组织使用的应用安全测试工具的主要问题是什么?（最多可选3项）



AI的承诺和陷阱

调查结果显示，AI的使用已经深入到许多组织的软件安全计划中，超过50%的受访者表示，他们正在DevSecOps实践中积极使用AI。54%的受访者希望通过AI来提高其安全措施的效率和准确性。48%的受访者希望通过AI来帮助他们减少对安全测试的人工审查。

考虑到AI可能为DevSecOps提供的主要优势，您会觉得这是很有道理的。AppSec团队经常陷入两难的境地，一方面需要进行完整和一致的安全测试，另一方面需要跟上使用DevOps方法论和CI管道的开发团队的节奏。当截止日期紧迫时，开发人员很容易跳过关键的安全风险评估过程。

本次调查的受访者表示，“提高安全措施的准确性和效率”(54%)以及“降低安全数据的人工审查和分析需求”(48%)是他们将AI引入安全SDLC的两个主要目的。

然而，请注意，受访者还表示，他们预计AI会“增加软件安全的复杂性和技术要求”，也许有一天，唯一能对AI生成的代码进行充分审查的实体只有AI自己。

图 M 贵组织目前是否正在使用AI工具来加强软件安全措施?

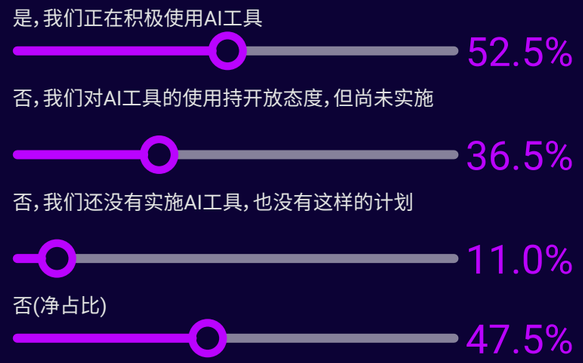


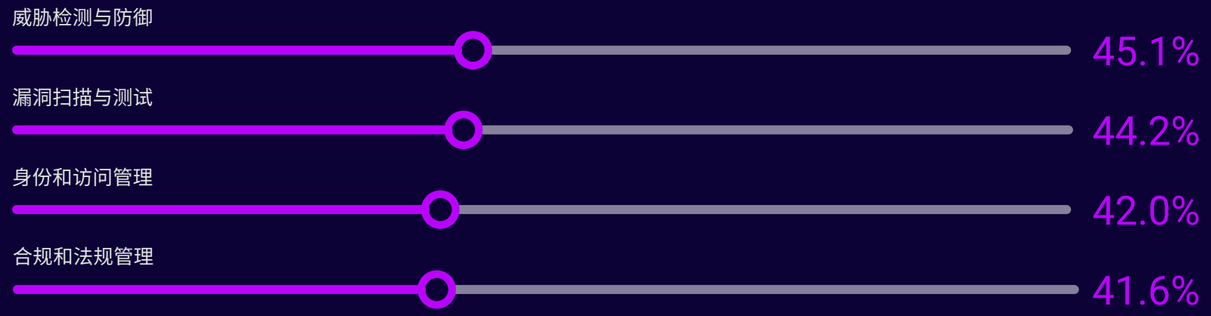
图 N 您预计使用AI工具将对贵组织的DevSecOps流程和工作流有何影响?(选择所有的适用项)

在DevSecOps中实施AI还面临着额外的挑战，例如确保数据质量以及解决安全和隐私问题。随着AI工具越来越多地集成到DevOps管道中，它们几乎肯定会成为安全威胁的主要目标。处理用于训练AI的敏感数据也会引发隐私问题。

AI的使用会带来一些潜在风险，例如AI辅助编码可能会围绕着AI创建的代码产生所有权、版权和许可问题。

2022年底，GitHub、Microsoft和OpenAI遭到集体诉讼，指控GitHub Copilot — 一款为开发者在编码时提供自动补全式建议的云端AI工具 — 侵犯了版权法和软件许可要求，并且训练Copilot服务所使用的开源代码也侵犯了开发者的权利。该诉讼还声称，Copilot建议的代码使用了有许可的材料，但没有注明出处、版权声明或遵守原始许可条款。

图 0 您认为AI工具可以有效加强哪些特定领域的软件安全?



基于大型语言模型的生成式AI聊天机器人，如ChatGPT和Google Bard，也存在随机产生“幻觉”的问题，即它们的回复虽然看起来可信和自信，但实际上是错误的 — 用通俗的说法，就是“说谎”。

AI幻觉显然会威胁到软件供应链安全。研究人员发现，ChatGPT可能会为您推荐虚幻的、根本不存在的代码库或软件包。恶意行为者可以创建具有相同名称的软件包，在其中填充恶意代码，然后将其分发给听从AI建议的毫无戒心的开发人员。这可能会对网络犯罪分子产生颠覆性的影响，让他们能够避开更传统和容易被发现的技术，如拼写错误或伪装。事实上，研究人员发现，根据 ChatGPT 的幻觉建议创建的恶意软件包已经存在于 PyPI 和 npm 等流行的软件包管理程序中。

这种威胁不是理论上的；而是真实存在的，正在发生的。无论供应链攻击是源自AI幻觉还是恶意行为者，要想对其进行防御，就必须了解代码来源、验证开发人员和维护人员的身份、并且只从可靠的供应商或来源下载软件包，这些都是至关重要的。.

图 P 您对基于AI的安全解决方案中潜在的偏差或错误有多担心（如果有担心的话）？

担心(净占比)	非常担心	有些担心	中立/没感觉	不太担心	一点都不担心	不担心(净占比)
76.6%	25.4%	51.3%	16.2%	6.0%	1.2%	7.2%

经验教训

虽然大多数组织在很大程度上采用了某些DevSecOps实践，但在有效实施方面仍然面临挑战。本次调查显示，问题主要集中在两个领域。

- **集成和调整多个应用安全测试(AST)工具的结果，使其与业务优先级相一致**
- **减少处理重大漏洞所需的时间**

28%的受访者表示，他们的组织需要长达三周的时间来修补已部署应用中的重大安全风险/漏洞。另有20%的受访者表示，修补漏洞可能需要长达一个月的时间，但大多数漏洞都会在披露后的几天内被利用。受访者表示，他们最不能忍受的是AST工具无法根据业务需求对漏洞修补进行优先级排序。

正如本报告在引言部分所述，编写调查问卷的挑战之一是术语“DevSecOps”涵盖多个不同学科，其中许多学科都有自己独特的角色。就“业务优先级”而言，不同的角色可能对其有不同的理解。

例如，业务主管最希望了解AppSec工具的效力，他们希望全面了解其流程及其能给整个团队带来怎样的绩效提升。开发和运维团队希望AppSec能够帮助他们集中查看所有问题，以确定最有价值的安全活动。安全专业人士则希望借此来消除噪音，以便优先安排迅速处理重大问题。

对于那些在满足业务需求的同时，努力使各种孤立的安全工具形成合力的组织来说，应用安全态势管理(ASPM)可以提供必要的增强效果。ASPM可以自动协调孤立的工具、提供上下文并确定优先级，以使组织能够专注于对业务最重要的应用安全问题。

- **ASPM可与开发和安全测试工具以及运维监控工具相集成，以提供整合好的单一视图来展示组织中各方面的安全相关信息。**
- **通过关联和分组来自分析特定应用程序和漏洞的不同工具的数据，ASPM 可以提供应用程序整体安全状况的全面视图。DevSecOps团队可以生成与其角色和职责相关的数据，而ASPM可以将这些数据以对业务线经理及其他需要更广阔视角的人有意义的方式展现出来。**
- **ASPM允许您针对特定应用和漏洞可能带来的特定风险制定并执行安全策略。当与开发或运维基础设施集成时，ASPM还允许您尽早地发现并解决安全问题。**

2021年的Gartner报告指出。大约有5%的受访组织采用了ASPM或其前身 — 应用安全编排与关联(ASOC)工具。Gartner预计其采用速度将会迅速提升，这一预测在2023年的调查结果中得到了印证 — 28%的受访者已经开始使用ASOC/ASPM。Gartner还指出，早期采用者往往是拥有成熟的DevSecOps计划和使用多种安全工具的团队，这些都是我们DevSecOps调查受访者的特征。

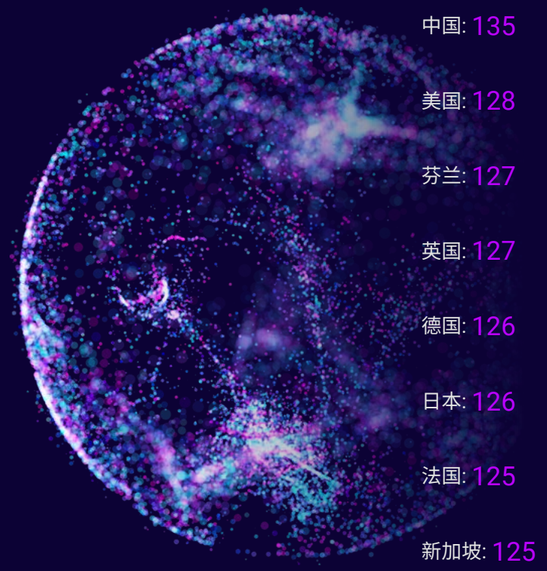
本报告探讨的调查有力地表明，安全工具提供的碎片化结果、不堪重负的工作团队和缓慢的漏洞修复速度是阻碍DevSecOps取得成功的根本挑战。对于那些拥有多元化DevSecOps团队并使用多种应用安全测试工具的组织来说，ASPM可能是有效应对这些挑战的关键。

受访者的行业分布

受访者的工作角色

应用安全架构师 应用安全经理 CISO 开发人员 DevOps工程师 应用安全总监 网络安全总监 IT风险管理总监 IT共享服务总监 产品安全总监 安全保障总监 产品安全执行总监
事故和安全经理 信息保障总监 软件安全工程经理 运维工程师 AppSec产品安全人员 程序员 QA/测试人员/测试经理 发布工程师/经理 安全管理员/安全分析师 安全架构师
安全总监 安全工程经理 产品安全高级总监 产品安全和技术高级副总裁 技术主管 产品和应用安全副总裁 安全架构副总裁 安全合规副总裁

受访者的国家/数量



中国: 135
美国: 128
芬兰: 127
英国: 127
德国: 126
日本: 126
法国: 125
新加坡: 125

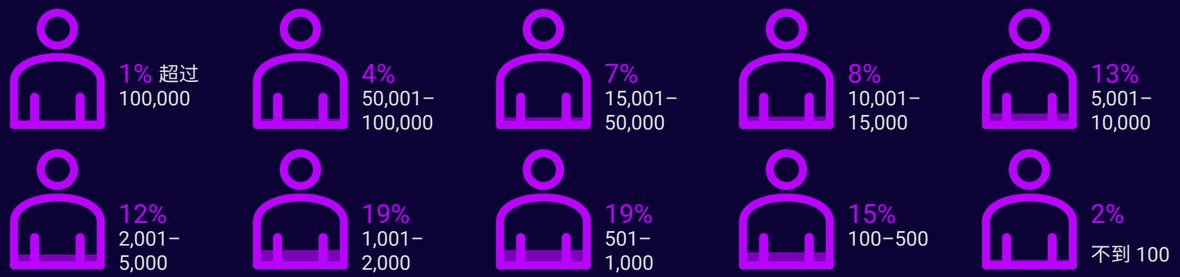
该组织创建/管理的软件/应用

应用软件	46%
系统软件	44%
Web应用	42%
产品软件	38%
人工智能软件	37%
工程/科学软件	35%
嵌入式软件	31%

该组织采用的安全实践

安全风险管理	35%
持续监控和评估	30%
配置管理	30%
威胁数据和响应	30%
持续部署	29%
自动部署	29%
持续测试	28%
应用安全编排与关联	28%
持续集成	28%
自动测试	28%
基础架构即代码	28%

组织规模（员工/临时工人数）



1% 超过 100,000
4% 50,001–100,000
7% 15,001–50,000
8% 10,001–15,000
13% 5,001–10,000
12% 2,001–5,000
19% 1,001–2,000
19% 501–1,000
15% 100–500
2% 不到 100

Q1. 贵组织主要属于哪个行业?

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
技术	18.45%	10.24%	34.38%	14.40%	12.60%	9.52%	42.96%	12.00%	9.52%
网络安全	14.52%	17.32%	13.28%	20.00%	14.96%	10.32%	7.41%	18.40%	15.08%
应用/软件开发	12.66%	4.72%	7.03%	20.00%	14.17%	1.59%	26.67%	5.60%	20.63%
制造	7.26%	3.94%	3.13%	4.00%	5.51%	9.52%	13.33%	8.80%	9.52%
金融科技	6.87%	6.30%	7.03%	4.80%	10.24%	11.11%	2.22%	8.80%	4.76%
教育	5.59%	6.30%	5.47%	7.20%	6.30%	3.97%	0.00%	9.60%	6.35%
银行/金融	5.50%	7.09%	3.91%	5.60%	4.72%	11.11%	0.74%	4.00%	7.14%
电信/ISP	5.10%	5.51%	3.13%	6.40%	8.66%	7.14%	2.22%	3.20%	4.76%
医疗保健	4.12%	6.30%	7.03%	4.00%	3.94%	3.17%	1.48%	4.00%	3.17%
零售	4.02%	7.09%	5.47%	4.00%	3.94%	5.56%	0.00%	3.20%	3.17%
媒体	3.63%	3.15%	2.34%	0.80%	3.94%	5.56%	0.74%	4.80%	7.94%
政府	3.14%	5.51%	3.13%	2.40%	3.15%	4.76%	0.74%	4.00%	1.59%
保险	2.85%	5.51%	3.13%	1.60%	3.15%	4.76%	0.00%	3.20%	1.59%
交通运输	2.55%	3.94%	0.00%	3.20%	1.57%	6.35%	0.74%	3.20%	1.59%
非盈利机构/协会	1.67%	3.94%	0.78%	0.80%	1.57%	3.17%	0.00%	2.40%	0.79%
公用事业	1.57%	2.36%	0.78%	0.00%	0.79%	2.38%	0.74%	4.00%	1.59%
其他(请注明)	0.49%	0.79%	0.00%	0.80%	0.79%	0.00%	0.00%	0.80%	0.79%

Q2. 贵组织有多大?包括员工和临时工?

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
不到100，请注明	1.57%	1.57%	0.00%	2.40%	0.00%	0.00%	3.70%	1.60%	3.17%
100–500	15.11%	11.02%	16.41%	20.80%	12.60%	19.05%	14.81%	6.40%	19.84%
501–1,000	19.04%	14.96%	23.44%	23.20%	14.96%	21.43%	8.89%	16.00%	30.16%
1,001–2,000	18.65%	15.75%	17.19%	15.20%	19.69%	15.87%	37.78%	16.00%	10.32%
2,001–5,000	12.37%	22.83%	10.94%	16.00%	18.11%	7.14%	5.93%	8.80%	9.52%
5,001–10,000	13.05%	18.11%	11.72%	7.20%	15.75%	6.35%	20.00%	17.60%	7.14%
10,001–15,000	8.44%	10.24%	9.38%	3.20%	8.66%	5.56%	2.96%	16.80%	11.11%
15,001–50,000	6.67%	3.94%	4.69%	4.00%	6.30%	17.46%	0.74%	10.40%	6.35%
50,001–100,000	4.42%	1.57%	5.47%	4.00%	3.15%	7.14%	5.19%	6.40%	2.38%
超过100,000，请注明	0.69%	0.00%	0.78%	4.00%	0.79%	0.00%	0.00%	0.00%	0.00%

Q3. 贵组织创建或管理哪些类型的软件/应用?(选择所有的适用项)

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
应用软件	46.03%	40.94%	61.72%	48.00%	37.01%	34.13%	70.37%	36.80%	37.30%
系统软件	44.06%	42.52%	54.69%	40.00%	30.71%	34.92%	67.41%	39.20%	41.27%
Web应用	41.71%	27.56%	45.31%	40.80%	44.09%	37.30%	68.89%	39.20%	28.57%
产品软件	38.27%	29.13%	47.66%	28.80%	39.37%	30.16%	65.19%	30.40%	33.33%
人工智能软件	36.60%	30.71%	41.41%	32.00%	32.28%	33.33%	57.04%	35.20%	29.37%
工程/科学软件	35.23%	25.20%	39.84%	27.20%	31.50%	38.89%	57.04%	30.40%	30.16%
嵌入式软件	30.91%	29.13%	34.38%	20.80%	29.92%	30.16%	42.22%	29.60%	30.16%
其他，请注明	0.20%	0.79%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.79%

Q4. 贵组织采用哪些安全实践？(选择所有的适用项)

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
安全风险管理	35.13%	35.43%	40.63%	33.60%	32.28%	19.84%	56.30%	32.80%	28.57%
持续监控与评估	29.93%	25.20%	34.38%	29.60%	32.28%	22.22%	44.44%	25.60%	24.60%
配置管理	29.64%	19.69%	31.25%	24.80%	23.62%	23.02%	49.63%	30.40%	33.33%
威胁数据和响应	29.34%	22.83%	39.84%	31.20%	28.35%	19.84%	41.48%	27.20%	23.02%
持续部署	29.05%	27.56%	35.16%	21.60%	29.13%	28.57%	41.48%	20.80%	26.98%
自动部署	28.56%	18.90%	28.91%	32.80%	28.35%	23.81%	48.15%	24.80%	21.43%
持续测试	28.46%	22.05%	32.03%	24.80%	30.71%	23.02%	48.15%	17.60%	27.78%
应用安全编排与关联	28.36%	29.13%	39.84%	20.00%	19.69%	18.25%	51.85%	28.00%	18.25%
持续集成	28.16%	23.62%	30.47%	24.80%	25.98%	19.84%	47.41%	28.00%	23.81%
自动测试	27.87%	19.69%	33.59%	28.00%	24.41%	15.08%	48.15%	20.00%	32.54%
基础架构即代码	27.58%	23.62%	41.41%	22.40%	20.47%	22.22%	48.15%	25.60%	15.08%
其他，请注明	0.10%	0.00%	0.00%	0.00%	0.79%	0.00%	0.00%	0.00%	0.00%

Q5. 贵组织使用的以下应用安全工具、实践或技术是否有用？(如果有的话)

在SDLC的需求挖掘阶段明确安全需求	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有用(净占比)	71.25%	66.93%	78.91%	73.60%	81.10%	62.70%	97.04%	55.20%	52.38%
非常有用	32.09%	25.20%	46.88%	32.00%	35.43%	24.60%	54.07%	17.60%	19.05%
些许有用	39.16%	41.73%	32.03%	41.60%	45.67%	38.10%	42.96%	37.60%	33.33%
不太有用	16.78%	15.75%	12.50%	16.80%	13.39%	20.63%	2.96%	26.40%	26.98%
根本没用	7.56%	11.02%	3.13%	8.00%	3.15%	11.90%	0.00%	14.40%	9.52%
没用(净占比)	24.34%	26.77%	15.63%	24.80%	16.54%	32.54%	2.96%	40.80%	36.51%
N/A	4.42%	6.30%	5.47%	1.60%	2.36%	4.76%	0.00%	4.00%	11.11%

通过BSIMM和SAMM等模型对软件安全性进行正式评估	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有用(净占比)	69.38%	55.91%	79.69%	71.20%	70.87%	57.94%	94.81%	67.20%	55.56%
非常有用	33.56%	24.41%	47.66%	25.60%	30.71%	26.98%	57.04%	28.80%	25.40%
些许有用	35.82%	31.50%	32.03%	45.60%	40.16%	30.95%	37.78%	38.40%	30.16%
不太有用	18.06%	25.20%	10.94%	17.60%	25.20%	23.02%	3.70%	16.80%	23.02%
根本没用	8.44%	11.81%	7.03%	8.80%	2.36%	16.67%	0.74%	10.40%	10.32%
没用(净占比)	26.50%	37.01%	17.97%	26.40%	27.56%	39.68%	4.44%	27.20%	33.33%
N/A	4.12%	7.09%	2.34%	2.40%	1.57%	2.38%	0.74%	5.60%	11.11%

通过自动扫描代码来查找安全漏洞和其他缺陷，例如静态应用安全测试(SAST)	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有用(净占比)	71.54%	62.20%	76.56%	76.00%	78.74%	65.87%	94.07%	54.40%	62.70%
非常有用	34.35%	29.13%	46.09%	33.60%	38.58%	27.78%	54.07%	21.60%	22.22%
些许有用	37.19%	33.07%	30.47%	42.40%	40.16%	38.10%	40.00%	32.80%	40.48%
不太有用	17.37%	22.05%	10.94%	16.80%	18.11%	17.46%	5.93%	29.60%	19.05%
根本没用	7.65%	13.39%	8.59%	5.60%	2.36%	11.90%	0.00%	12.80%	7.14%
没用(净占比)	25.02%	35.43%	19.53%	22.40%	20.47%	29.37%	5.93%	42.40%	26.19%
N/A	3.43%	2.36%	3.91%	1.60%	0.79%	4.76%	0.00%	3.20%	11.11%

开源/第三方依赖性分析(SCA)	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有用（净占比）	67.62%	50.39%	75.00%	73.60%	74.80%	61.11%	94.81%	53.60%	55.56%
非常有用	30.32%	22.05%	33.59%	32.00%	30.71%	23.81%	60.74%	20.00%	17.46%
些许有用	37.29%	28.35%	41.41%	41.60%	44.09%	37.30%	34.07%	33.60%	38.10%
不太有用	19.73%	25.98%	16.41%	18.40%	22.05%	22.22%	5.19%	27.20%	21.43%
根本没用	8.34%	14.17%	5.47%	6.40%	1.57%	11.90%	0.00%	12.80%	15.08%
没用（净占比）	28.07%	40.16%	21.88%	24.80%	23.62%	34.13%	5.19%	40.00%	36.51%
N/A	4.32%	9.45%	3.13%	1.60%	1.57%	4.76%	0.00%	6.40%	7.94%

内部或第三方渗透测试	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有用（净占比）	67.91%	53.54%	71.88%	72.00%	80.31%	56.35%	96.30%	54.40%	56.35%
非常有用	30.23%	18.11%	37.50%	35.20%	43.31%	23.02%	48.89%	17.60%	16.67%
些许有用	37.68%	35.43%	34.38%	36.80%	37.01%	33.33%	47.41%	36.80%	39.68%
不太有用	19.33%	29.13%	19.53%	16.80%	16.54%	20.63%	3.70%	24.80%	24.60%
根本没用	8.64%	10.24%	7.03%	7.20%	3.15%	17.46%	0.00%	15.20%	9.52%
没用（净占比）	27.97%	39.37%	26.56%	24.00%	19.69%	38.10%	3.70%	40.00%	34.13%
N/A	4.12%	7.09%	1.56%	4.00%	0.00%	5.56%	0.00%	5.60%	9.52%

模糊测试	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有用（净占比）	62.32%	50.39%	75.00%	58.40%	68.50%	53.97%	88.15%	55.20%	46.83%
非常有用	25.02%	19.69%	35.94%	17.60%	23.62%	27.78%	42.96%	18.40%	12.70%
些许有用	37.29%	30.71%	39.06%	40.80%	44.88%	26.19%	45.19%	36.80%	34.13%
不太有用	19.73%	18.90%	12.50%	22.40%	18.90%	23.02%	10.37%	25.60%	26.98%
根本没用	9.52%	14.96%	4.69%	4.80%	9.45%	18.25%	0.74%	12.00%	11.90%
没用（净占比）	29.24%	33.86%	17.19%	27.20%	28.35%	41.27%	11.11%	37.60%	38.89%
N/A	8.44%	15.75%	7.81%	14.40%	3.15%	4.76%	0.74%	7.20%	14.29%

Q6. 贵组织使用的以下应用安全工具、实践或技术是否有用（如果有的话）？

动态应用安全测试 (DAST)	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有用（净占比）	67.12%	48.82%	74.22%	76.80%	74.80%	62.70%	91.11%	49.60%	57.14%
非常有用	29.44%	16.54%	38.28%	36.80%	29.92%	27.78%	46.67%	20.00%	18.25%
些许有用	37.68%	32.28%	35.94%	40.00%	44.88%	34.92%	44.44%	29.60%	38.89%
不太有用	19.63%	32.28%	16.41%	16.80%	17.32%	20.63%	7.41%	28.80%	18.25%
根本没用	9.62%	12.60%	6.25%	5.60%	6.30%	12.70%	0.74%	18.40%	15.08%
没用（净占比）	29.24%	44.88%	22.66%	22.40%	23.62%	33.33%	8.15%	47.20%	33.33%
N/A	3.63%	6.30%	3.13%	0.80%	1.57%	3.97%	0.74%	3.20%	9.52%

交互式应用安全测试(IAST)	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有用（净占比）	68.50%	60.63%	72.66%	75.20%	77.17%	53.97%	96.30%	53.60%	56.35%
非常有用	31.11%	22.05%	35.16%	34.40%	37.01%	18.25%	54.07%	24.00%	22.22%
些许有用	37.39%	38.58%	37.50%	40.80%	40.16%	35.71%	42.22%	29.60%	34.13%
不太有用	18.06%	18.11%	20.31%	15.20%	18.11%	21.43%	3.70%	24.80%	23.81%
根本没用	9.62%	14.17%	6.25%	9.60%	3.15%	18.25%	0.00%	14.40%	11.90%
没用（净占比）	27.67%	32.28%	26.56%	24.80%	21.26%	39.68%	3.70%	39.20%	35.71%
N/A	3.83%	7.09%	0.78%	0.00%	1.57%	6.35%	0.00%	7.20%	7.94%

Web应用防火墙(WAF)	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有用（净占比）	68.99%	62.99%	78.13%	66.40%	78.74%	55.56%	97.78%	51.20%	58.73%
非常有用	33.17%	33.86%	39.84%	32.00%	36.22%	21.43%	52.59%	21.60%	26.19%
些许有用	35.82%	29.13%	38.28%	34.40%	42.52%	34.13%	45.19%	29.60%	32.54%
不太有用	18.25%	19.69%	14.84%	20.00%	15.75%	23.02%	2.22%	32.80%	19.05%
根本没用	8.73%	11.02%	6.25%	10.40%	3.94%	14.29%	0.00%	12.80%	11.90%
没用（净占比）	26.99%	30.71%	21.09%	30.40%	19.69%	37.30%	2.22%	45.60%	30.95%
N/A	4.02%	6.30%	0.78%	3.20%	1.57%	7.14%	0.00%	3.20%	10.32%

容器安全测试	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有用(净占比)	66.93%	48.82%	79.69%	73.60%	74.80%	57.94%	91.11%	57.60%	50.00%
非常有用	29.93%	20.47%	38.28%	29.60%	39.37%	24.60%	49.63%	21.60%	14.29%
些许有用	37.00%	28.35%	41.41%	44.00%	35.43%	33.33%	41.48%	36.00%	35.71%
不太有用	18.65%	29.13%	13.28%	14.40%	17.32%	19.84%	6.67%	24.00%	25.40%
根本没用	9.42%	14.96%	3.91%	8.80%	6.30%	18.25%	1.48%	12.80%	9.52%
没用(净占比)	28.07%	44.09%	17.19%	23.20%	23.62%	38.10%	8.15%	36.80%	34.92%
N/A	5.00%	7.09%	3.13%	3.20%	1.57%	3.97%	0.74%	5.60%	15.08%

使用安全漏洞/风险管理工具，如XDR和SRM等	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有用(净占比)	69.77%	58.27%	82.81%	74.40%	74.02%	57.14%	97.78%	53.60%	57.94%
非常有用	32.58%	24.41%	47.66%	35.20%	41.73%	22.22%	50.37%	20.00%	17.46%
些许有用	37.19%	33.86%	35.16%	39.20%	32.28%	34.92%	47.41%	33.60%	40.48%
不太有用	17.86%	21.26%	8.59%	19.20%	22.05%	19.05%	1.48%	27.20%	25.40%
根本没用	9.62%	16.54%	7.03%	5.60%	1.57%	20.63%	0.74%	16.00%	9.52%
没用(净占比)	27.48%	37.80%	15.63%	24.80%	23.62%	39.68%	2.22%	43.20%	34.92%
N/A	2.75%	3.94%	1.56%	0.80%	2.36%	3.17%	0.00%	3.20%	7.14%

对修复工作进行优先级排序	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有用(净占比)	67.12%	53.54%	82.81%	67.20%	71.65%	53.97%	96.30%	56.80%	52.38%
非常有用	29.83%	21.26%	40.63%	24.80%	36.22%	21.43%	54.07%	21.60%	16.67%
些许有用	37.29%	32.28%	42.19%	42.40%	35.43%	32.54%	42.22%	35.20%	35.71%
不太有用	18.45%	28.35%	7.81%	19.20%	22.05%	19.84%	3.70%	24.00%	23.81%
根本没用	9.91%	9.45%	7.03%	10.40%	5.51%	17.46%	0.00%	12.00%	18.25%
没用(净占比)	28.36%	37.80%	14.84%	29.60%	27.56%	37.30%	3.70%	36.00%	42.06%
N/A	4.51%	8.66%	2.34%	3.20%	0.79%	8.73%	0.00%	7.20%	5.56%

软件供应链管理/监控	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有用(净占比)	69.28%	59.84%	72.66%	71.20%	77.95%	58.73%	95.56%	56.00%	60.32%
非常有用	32.29%	24.41%	36.72%	33.60%	32.28%	25.40%	57.04%	19.20%	27.78%
些许有用	37.00%	35.43%	35.94%	37.60%	45.67%	33.33%	38.52%	36.80%	32.54%
不太有用	18.84%	22.83%	17.19%	17.60%	18.11%	23.81%	3.70%	31.20%	17.46%
根本没用	8.34%	11.81%	7.81%	10.40%	1.57%	10.32%	0.74%	11.20%	13.49%
没用(净占比)	27.18%	34.65%	25.00%	28.00%	19.69%	34.13%	4.44%	42.40%	30.95%
N/A	3.53%	5.51%	2.34%	0.80%	2.36%	7.14%	0.00%	1.60%	8.73%

Q7.您认为贵组织当前的软件安全项目/计划的成熟度属于哪一级

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
第一级：非结构化/无组织	8.54%	11.02%	3.91%	4.80%	11.02%	12.70%	2.22%	10.40%	12.70%
第二级：安全流程是文档化的，并且对于特定的团队是可重复的	24.14%	28.35%	23.44%	16.00%	29.13%	26.19%	9.63%	34.40%	26.98%
第三级：第二级所述流程和程序在整个组织中是标准化的。积极主动的安全文化得到了领导层的认可和宣传	34.25%	33.07%	38.28%	40.00%	35.43%	36.51%	21.48%	33.60%	36.51%
第四级：安全流程和控件是有记录的、被管理和监控的	24.53%	22.05%	20.31%	28.00%	14.96%	21.43%	48.89%	20.00%	19.05%
第五级：安全流程是持续分析和改进的	8.54%	5.51%	14.06%	11.20%	9.45%	3.17%	17.78%	1.60%	4.76%
其他，请注明	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q8.贵组织平均多久对关键业务应用的安全性进行一次评估或测试？

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
每天	7.07%	3.94%	8.59%	19.20%	4.72%	3.17%	3.70%	2.40%	11.11%
每周4-6天	17.17%	15.75%	16.41%	15.20%	11.81%	11.11%	37.04%	11.20%	17.46%
每周2-3天	20.41%	18.90%	21.09%	28.00%	14.96%	20.63%	27.41%	14.40%	17.46%
每周一次	16.98%	16.54%	15.63%	14.40%	18.11%	16.67%	17.78%	19.20%	17.46%
每2-3周一次	11.09%	11.02%	12.50%	5.60%	18.11%	12.70%	5.19%	14.40%	9.52%
每月一次	7.16%	6.30%	4.69%	5.60%	12.60%	7.94%	5.19%	5.60%	9.52%
每两个月一次	7.46%	7.87%	7.81%	3.20%	11.02%	3.97%	2.22%	18.40%	5.56%
每3-5个月一次	6.38%	7.87%	10.16%	5.60%	3.15%	7.14%	1.48%	7.20%	8.73%
每6-11个月一次	4.42%	7.87%	2.34%	1.60%	4.72%	10.32%	0.00%	6.40%	2.38%
每年一次	1.67%	2.36%	0.78%	1.60%	0.79%	6.35%	0.00%	0.80%	0.79%
每年不到一次，请提供具体数据	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
永不	0.20%	1.57%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q9. 您如何评估或测试关键业务应用的安全性？(选择所有的适用项)

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
手动和自动评估相结合	52.61%	50.40%	65.63%	44.80%	50.39%	51.59%	68.89%	47.20%	40.48%
外部渗透测试	44.15%	37.60%	39.06%	40.00%	43.31%	47.62%	63.70%	45.60%	34.92%
自动评估和测试	43.66%	40.00%	46.88%	39.20%	42.52%	45.24%	68.15%	29.60%	35.71%
手动评估和/或测试(不包括渗透测试)	43.07%	36.00%	46.88%	37.60%	46.46%	44.44%	58.52%	33.60%	39.68%
不知道/不确定	0.20%	0.00%	0.00%	0.80%	0.79%	0.00%	0.00%	0.00%	0.00%
其他，请注明	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q10. 在过去一年(2022-2023年)，解决一个重大安全/漏洞问题对贵组织的软件交付计划产生了多大的影响(如果有的话)？

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
有影响(净占比)	81.06%	72.44%	86.72%	80.00%	92.91%	89.68%	79.26%	80.80%	66.67%
很大的影响	38.37%	24.41%	41.41%	33.60%	33.86%	54.76%	60.74%	24.80%	31.75%
些许影响	42.69%	48.03%	45.31%	46.40%	59.06%	34.92%	18.52%	56.00%	34.92%
没什么影响	17.17%	25.20%	12.50%	17.60%	7.09%	7.94%	20.00%	18.40%	28.57%
根本没影响	1.77%	2.36%	0.78%	2.40%	0.00%	2.38%	0.74%	0.80%	4.76%
没影响(净占比)	18.94%	27.56%	13.28%	20.00%	7.09%	10.32%	20.74%	19.20%	33.33%

Q11. 贵组织由谁负责安全测试？(选择所有的适用项)

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
内部安全团队	46.03%	39.37%	50.00%	36.80%	41.73%	38.89%	67.41%	46.40%	46.03%
开发人员/软件工程师	45.14%	34.65%	53.13%	33.60%	44.88%	42.86%	63.70%	44.00%	42.86%
QA/测试团队	37.59%	41.73%	35.94%	32.80%	33.86%	38.89%	51.11%	34.40%	30.95%
跨职能的DevSecOps团队	35.53%	31.50%	44.53%	28.80%	39.37%	30.95%	48.15%	32.00%	27.78%
外部顾问	32.88%	29.92%	46.09%	28.00%	28.35%	38.10%	32.59%	31.20%	28.57%
不确定	0.10%	0.00%	0.00%	0.00%	0.00%	0.79%	0.00%	0.00%	0.00%
其他，请注明	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q12. 贵组织平均需要多长时间才能修补/处理已部署的或正在使用的应用程序中的重大安全风险/漏洞

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
不到一周，请提供具体天数	4.61%	0.00%	7.81%	11.20%	5.51%	0.00%	6.67%	3.20%	2.38%
1-2周	26.40%	14.96%	21.88%	40.80%	25.98%	14.29%	57.04%	10.40%	23.81%
2-3周	28.26%	33.86%	28.91%	24.80%	26.77%	23.02%	29.63%	28.00%	30.95%
3周-1个月	19.92%	22.83%	19.53%	16.00%	21.26%	32.54%	4.44%	26.40%	17.46%
1-2个月	8.44%	9.45%	5.47%	3.20%	11.81%	11.90%	1.48%	14.40%	10.32%
2-4个月	5.50%	3.94%	5.47%	3.20%	4.72%	11.11%	0.74%	8.80%	6.35%
4-6个月	4.71%	9.45%	10.16%	0.80%	1.57%	4.76%	0.00%	8.00%	3.17%
6个月以上，请提供具体月数	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
不确定	2.16%	5.51%	0.78%	0.00%	2.36%	2.38%	0.00%	0.80%	5.56%

Q13. 您用来评估DevSecOps活动成功与否的主要KPI是什么？(最多可选3项)

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
公开安全漏洞的数量	28.95%	27.56%	32.81%	28.80%	27.56%	24.60%	40.00%	26.40%	23.02%
开发流程后期发现的安全相关问题的减少	28.26%	33.07%	33.59%	24.00%	24.41%	29.37%	30.37%	30.40%	20.63%
问题解决时间	27.58%	24.41%	30.47%	28.00%	24.41%	23.02%	31.11%	25.60%	33.33%
解决安全相关问题所花费时间的减少	27.38%	27.56%	30.47%	24.00%	21.26%	34.13%	32.59%	24.80%	23.81%
因安全问题造成的构建延迟的减少	26.50%	25.98%	28.91%	28.80%	26.77%	19.84%	27.41%	26.40%	27.78%
因安全问题造成的构建失败的减少	24.44%	22.05%	24.22%	21.60%	25.20%	27.78%	25.93%	25.60%	23.02%
合规KPI(通过审核的百分比等)	23.75%	30.71%	28.91%	17.60%	22.83%	26.98%	24.44%	23.20%	15.08%
客户提交的服务单数量	22.77%	29.13%	28.91%	25.60%	21.26%	22.22%	15.56%	25.60%	14.29%
缺陷逃逸率	22.28%	22.83%	17.19%	16.00%	30.71%	23.81%	28.15%	17.60%	21.43%
我们没有用来评估DevSecOps活动成功与否的主要KPI	1.08%	0.00%	0.00%	0.00%	1.57%	0.00%	0.00%	0.80%	6.35%
其他，请注明	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q14. 贵组织中实施DevSecOps的挑战/障碍是什么？(选择所有的适用项)

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
开发人员/工程师的安全培训不足/无效	33.86%	33.07%	42.97%	27.20%	31.50%	35.71%	32.59%	35.20%	32.54%
应用安全人员/技能短缺	31.40%	25.98%	29.69%	28.80%	23.62%	31.75%	46.67%	32.80%	30.95%
开发/运维工作缺乏透明性	31.31%	27.56%	37.50%	28.80%	35.43%	29.37%	36.30%	28.00%	26.98%
不断变化的需求和优先级	30.42%	25.20%	30.47%	27.20%	29.13%	27.78%	43.70%	32.80%	26.19%
安全计划和工具的预算/资金不足	29.44%	30.71%	39.06%	32.80%	37.01%	23.02%	22.96%	21.60%	28.57%
开发、运维和安全团队之间的组织孤岛	29.05%	31.50%	42.19%	24.80%	28.35%	29.37%	29.63%	22.40%	23.81%
安全团队缺乏编码技能	28.95%	24.41%	30.47%	26.40%	31.50%	30.95%	28.89%	29.60%	29.37%
没有遇到挑战障碍	2.06%	4.72%	3.13%	1.60%	2.36%	0.79%	1.48%	0.00%	2.38%
其他，请注明	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q15. 贵组织使用的应用安全测试工具的主要问题是什么?(最多可选3项)

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
工具无法根据安全漏洞的暴露程度、可利用性和严重程度对修复工作进行优先级排序	34.74%	35.43%	41.41%	40.00%	37.01%	34.13%	35.56%	22.40%	31.75%
工具因速度太慢而无法适应快速发布周期/持续部署	34.15%	26.77%	42.97%	33.60%	28.35%	30.16%	47.41%	40.00%	23.02%
性价比低	33.46%	29.92%	34.38%	32.00%	38.58%	34.92%	33.33%	30.40%	34.13%
不准确/不可靠	33.07%	25.20%	39.84%	28.80%	36.22%	33.33%	31.85%	32.00%	37.30%
误报率高	32.19%	38.58%	39.06%	21.60%	31.50%	35.71%	29.63%	36.00%	25.40%
无法整合/关联来自不同工具的结果	28.95%	23.62%	28.91%	22.40%	26.77%	30.95%	34.07%	28.00%	36.51%
没有严重问题	3.14%	6.30%	3.13%	4.00%	2.36%	0.00%	5.19%	0.00%	3.97%
其他,请注明	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q16. 您认为哪些因素对安全计划取得成功最重要?(最多可选3项)

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
通过基础架构即代码来执行安全/合规策略	33.56%	36.22%	37.50%	39.20%	26.77%	26.98%	40.74%	29.60%	30.95%
在开发和运维团队中培养安全支持者	32.58%	22.05%	39.06%	32.80%	28.35%	38.89%	28.15%	40.00%	31.75%
改善开发、运维和安全团队之间的沟通	32.48%	34.65%	42.97%	27.20%	31.50%	34.13%	32.59%	34.40%	22.22%
将自动安全测试集成到构建/部署工作流中	32.29%	28.35%	36.72%	32.00%	36.22%	33.33%	32.59%	28.00%	30.95%
通过自动化来最大限度地降低漏洞修复时间/成本	30.03%	32.28%	31.25%	31.20%	23.62%	27.78%	40.74%	27.20%	25.40%
创建跨职能领域的DevSecOps团队	28.95%	29.92%	32.03%	21.60%	37.01%	28.57%	35.56%	26.40%	19.84%
对开发人员/工程师进行安全编码培训	27.58%	25.20%	28.91%	20.80%	35.43%	26.98%	33.33%	21.60%	27.78%
我不认为有什么重要成功因素	0.79%	2.36%	0.00%	0.80%	0.00%	0.79%	0.74%	0.00%	1.59%
其他,请注明	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q17.贵组织目前是否正在使用AI工具来加强软件安全措施?

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
是,我们正在积极使用AI工具	52.50%	38.58%	64.06%	47.20%	47.24%	69.84%	57.04%	47.20%	48.41%
否,我们对AI工具的使用持开放态度,但尚未实施	36.51%	39.37%	23.44%	42.40%	47.24%	22.22%	40.00%	35.20%	42.06%
否,我们还没有实施AI工具,也没有这样的计划	10.99%	22.05%	12.50%	10.40%	5.51%	7.94%	2.96%	17.60%	9.52%
否(净占比)	47.50%	61.42%	35.94%	52.80%	52.76%	30.16%	42.96%	52.80%	51.59%

Q18.您预计使用AI工具将对贵组织的DevSecOps过程和工作流有何影响?(选择所有的适用项)

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
提高安全措施的效率和准确性	53.69%	51.52%	58.93%	49.11%	44.17%	43.97%	68.70%	57.28%	54.39%
增加软件安全的复杂性和技术需求	52.04%	51.52%	64.29%	42.86%	50.83%	54.31%	61.83%	47.57%	41.23%
降低安全数据的人工审查和分析需求	48.40%	50.51%	45.54%	42.86%	50.83%	45.69%	64.12%	42.72%	42.11%
没有重大影响	0.88%	0.00%	0.00%	0.89%	0.83%	2.59%	0.00%	0.00%	2.63%
其他,请注明	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q19.您认为AI工具可以有效加强哪些特定领域的软件安全?

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
威胁检测与防御	45.09%	42.42%	50.00%	46.43%	46.67%	41.38%	44.27%	46.60%	42.98%
漏洞扫描和测试	44.21%	39.39%	46.43%	45.54%	46.67%	37.07%	52.67%	42.72%	41.23%
身份和访问管理	42.01%	43.43%	50.00%	44.64%	38.33%	37.93%	54.20%	33.98%	31.58%
合规和监管管理	41.57%	47.47%	46.43%	31.25%	42.50%	36.21%	45.04%	37.86%	45.61%
其他,请注明	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q20.您对基于AI的安全解决方案中隐藏的偏差或错误有多担心（如果有的话）？

	全球	英国	美国	法国	芬兰	德国	中国	新加坡	日本
担心（净占比）	76.63%	76.77%	83.93%	74.11%	77.50%	84.48%	55.73%	82.52%	81.58%
非常担心	25.36%	27.27%	33.04%	16.96%	15.83%	50.00%	7.63%	28.16%	27.19%
有些担心	51.27%	49.49%	50.89%	57.14%	61.67%	34.48%	48.09%	54.37%	54.39%
中立/没感觉	16.21%	15.15%	10.71%	22.32%	18.33%	8.62%	28.24%	12.62%	11.40%
不太担心	5.95%	6.06%	4.46%	2.68%	3.33%	6.03%	13.74%	3.88%	6.14%
一点都不担心	1.21%	2.02%	0.89%	0.89%	0.83%	0.86%	2.29%	0.97%	0.88%
不担心（净占比）	7.17%	8.08%	5.36%	3.57%	4.17%	6.90%	16.03%	4.85%	7.02%

Synopsys与众不同

Synopsys提供的集成解决方案，可以改变您构建和交付软件的方式，在应对业务风险的同时加速创新。与Synopsys同行，您的开发人员可以在编写代码的时候快速兼顾安全。您的开发和DevSecOps团队可以在不影响速度的情况下在开发管道中自动进行安全测试。您的安全团队可以主动管理风险并将补救工作聚焦在对贵组织最重要的事情上。我们无与伦比的专业知识可以帮助您规划和执行所需安全计划。只有Synopsys能够满足您构建可信软件的一切需求。

有关Synopsys软件完整性小组的更多信息，请访问：www.synopsys.com/software.