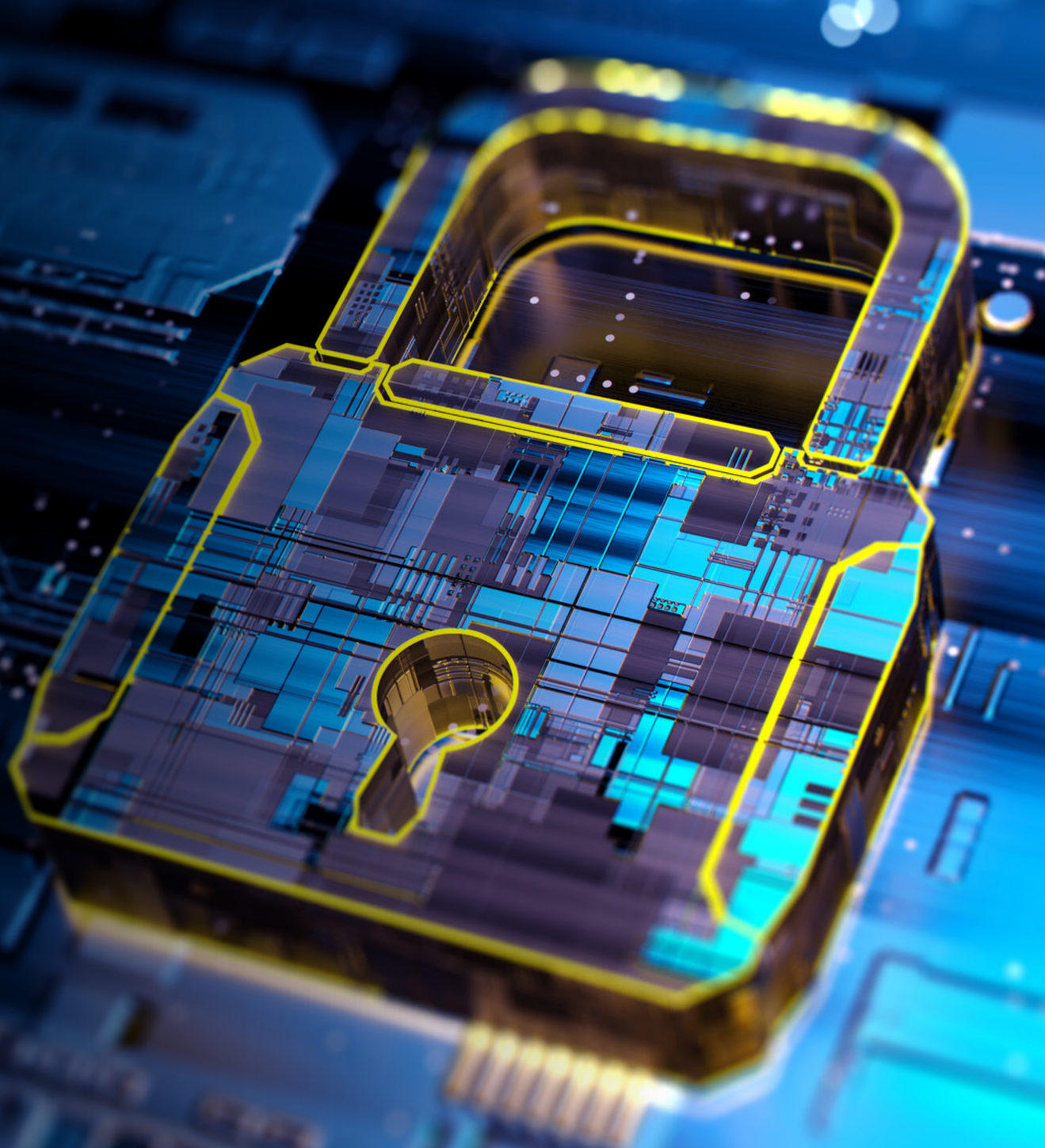
Enterprise Strategy Group | 了解更重要的事实。™

研究重点

现代应用程序开发安全



Dave Gruber, ESG 高级分析师

2020 年 8 月

目录

研究目标

DevSecOps 已在现代开发应用程序时优先考虑安全性并围绕确保安全展开开发活动，然而，驱动并衡量安全团队或开发团队的指标是不一致的，因此实现此目标仍然备受挑战。再加上大多数安全团队缺乏对现代应用程序开发实践的了解，这使得挑战进一步加剧。向微服务架构的转型以及对容器，无服务器模式的使用，转变了开发人员构建、测试以及部署的方式。

因而，应用安全工具的整合可以说是早已启动。众多测试工具催生了大量问题，许多问题又彼此重叠，使得各个组织不堪重负，确定优先次序和缓解问题变得复杂化，因此，集成式的应用安全平台可以说是众望所归。

为了深入了解这些趋势，ESG 对北美（美国和加拿大）地区各个组织参与确保应用程序开发工具和流程安全的 378 名负责 IT、网络安全和应用程序开发的专业人员进行了调研。

本项研究旨在：

考察购买意向。即考察应用安全团队在开发过程中对应用程序的安全程度的把控，并预测买家对于不同类型供应商的应用安全解决方案的偏好。

确定了解程度。确定安全团队对于现代开发和部署实践的了解程度，以及在何处实施安全控制以便降低风险。

了解触发点。即决策者会根据什么来进行应用安全投资，以及如何把握投资的优先级和时机。

深入了解。即了解开发团队和网络安全团队对于应用安全解决方案的部署与管理方面的协同工作方式。

返回目录

研究重点

尽管许多组织仍会提交易受攻击的代码，但大多数组织认为他们的应用安全计划都是可靠的。

拥有良好的应用安全计划并不意味着组织将不再提交易受攻击的代码。区别在于提交此类代码的人完全知情并清楚地了解他们所承担的风险。要想实现应用程序安全就需要持续对潜在风险进行分类处理，这其中就涉及到如何制定优先级决策，使得开发团队既能在规定日期前交付应用程序，同时还能降低风险。

为了确保如今种类繁多的应用程序开发与部署模型的安全，需要使用各种各样的安全测试工具。

随着应用安全日趋成熟，任何单一的测试技术都无法帮助开发团队降低全部安全风险。这就需要安全团队运用通常由多个供应商提供的多种工具来确保 SDLC 的安全。尽管使用情况各不相同，组织认为最重要的工具也有所不同，但大多数组织最终都会混合使用众多工具来满足他们的安全需求。

开发人员安全培训质量参差不齐，缺乏提高开发人员安全技能的计划。

尽管大多数组织为开发人员提供某一级别的安全培训，但超过 50% 的组织仅仅每年培训一次或者更少。虽然开发经理通常负责此类培训，但是在大多数组织中，应用程序安全分析师都肩负重任，需要对跟踪记录显示引入了过多安全问题的开发团队或单个开发人员，执行补救式的培训。

AppSec 测试工具激增为许多人带来了问题，超过三分之一的人将投资重点放在了整合上。

与其他类别的安全控制相似，许多组织使用了太多工具，以致于他们难以集成和管理它们。这就降低了计划的有效程度，并需要安排过多资源来管理工具。近三分之一的组织都遇到了这一问题，并因此计划将未来的投资用于整合与简化大量的工具。

各个组织都在投资，超过半数的组织都计划较前一年相比，大幅增加在应用安全方面的支出。

44% 的组织计划将应用安全投资瞄准云端，三分之一的组织将整点放在工具整合上，以便简化流程。其他组织则计划投资扩大测试工具的使用范围，使更大比例的开发团队和应用程序能使用这些工具。

返回目录

尽管许多组织仍会提交易受攻击的代码，但大多数组织认为他们的应用安全计划都是可靠的。

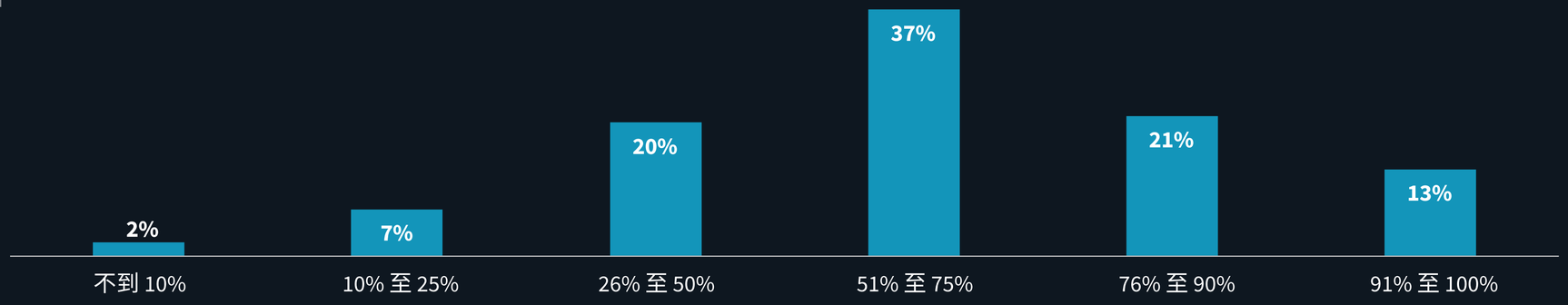
大多数组织认为他们的应用安全计划相当不错

大多数组织认为他们的应用安全计划相当不错，超过三分之一的组织给其计划打 9 或 10 分，整体平均分为 7.92 分。这一好评反映了各组织在过去几年对于应用安全计划的不断投资效果和覆盖水平。尽管如此，离完全覆盖代码库还相去甚远，仅 34% 的组织在其超过四分之三的代码库中使用 AppSec 工具。

36%

的组织给其应用安全计划打 9 或 10 分

受 AppSec 工具保护的代码库

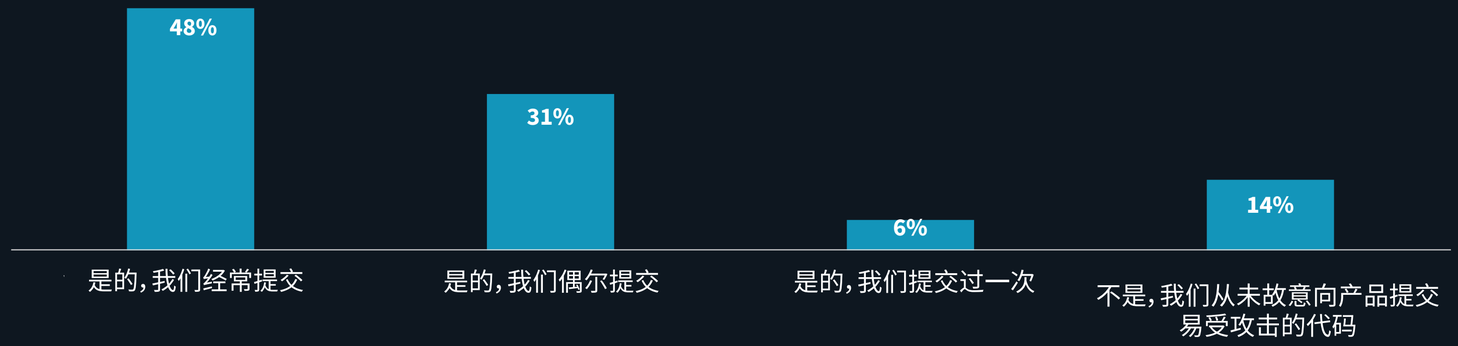


返回目录

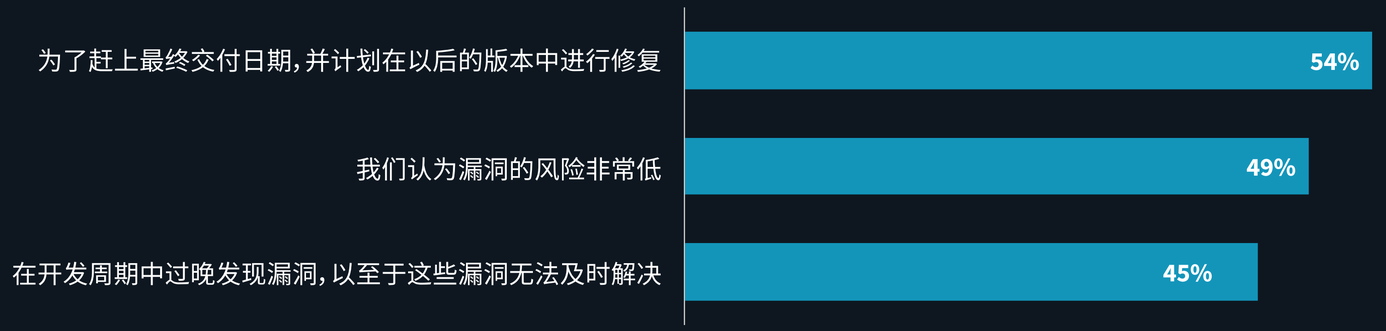
无论程序有多么完善，大部分组织仍会定期提交易受攻击的代码

拥有良好的应用安全计划并不意味着组织将不再提交易受攻击的代码。区别在于提交此类代码的人完全知情并清楚地了解他们所承担的风险。要想实现应用程序安全就需要持续对潜在风险进行分类处理，这其中就涉及到如何制定优先级决策，使得开发团队既能在规定日期前交付应用程序，同时还能降低风险。请注意，如果在开发周期中过晚发现漏洞，那么这些漏洞通常将无法得到解决。这也进一步强调了尽早注重应用程序安全的重要性。因为只有尽早发现漏洞才能留出足够的时间及时解决关键问题，不影响按时交付。

组织会提交易受攻击的代码吗？



为什么组织会提交易受攻击的代码



返回目录

大多数组织仍在遭受漏洞利用导致的攻击

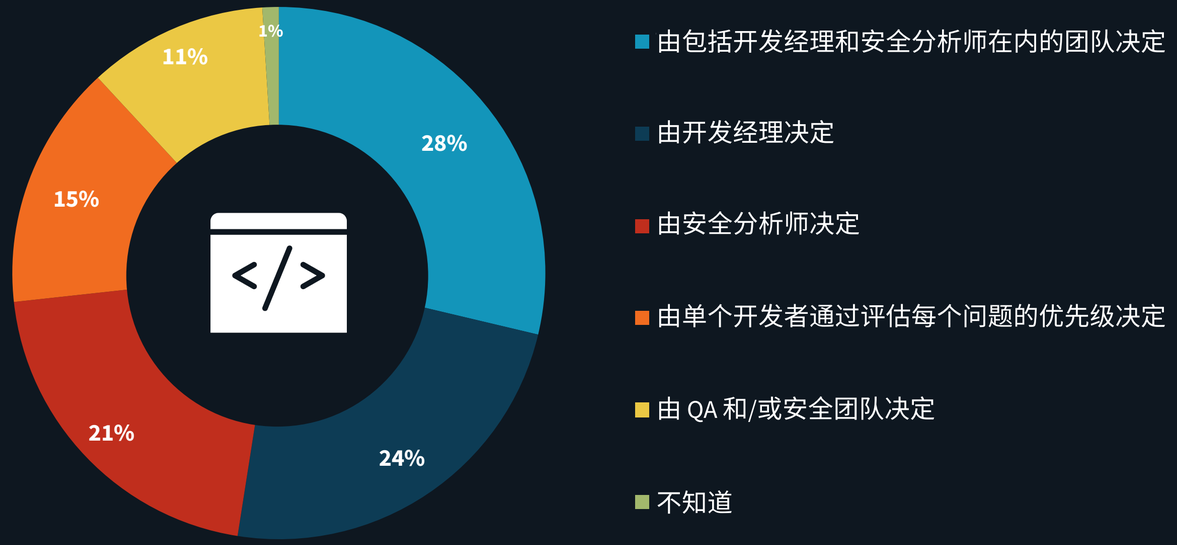
尽管增加对 AppSec 计划的投资能够降低风险，但 60% 的组织仍然表示他们遭受了 OWASP top-10漏洞入侵。尽管某些已知漏洞的攻击利用原因不一定直接对应到到代码缺陷，但这也强调了尽职调查（包括代码覆盖范围、整个 SDLC 中的测试频率以及确定已识别漏洞的优先级）的必要性。

60%

的组织在过去 12 个月遭受到 OWASP top-10 漏洞入侵其生产应用程序

那么谁会决定发布具有已知漏洞的代码？尽管众多组织是由开发经理和安全分析师共同作出此决定的，但也有不少团队是由一个负责人作出最终决定的。这反映了不同的开发组织管理整个应用安全流程方面的差异，一些组织将所有权交给安全团队，而其他组织则让开发经理负责。

谁决定提交代码？

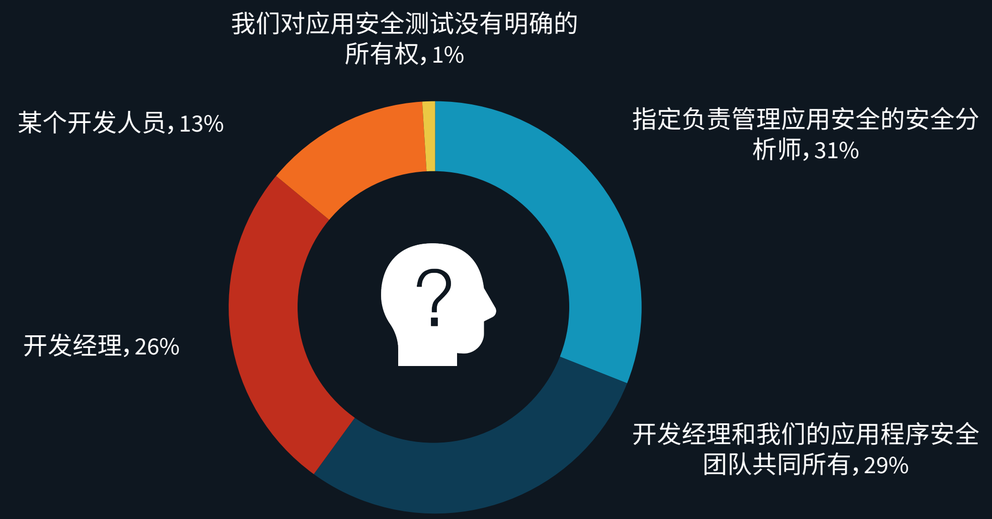


返回目录

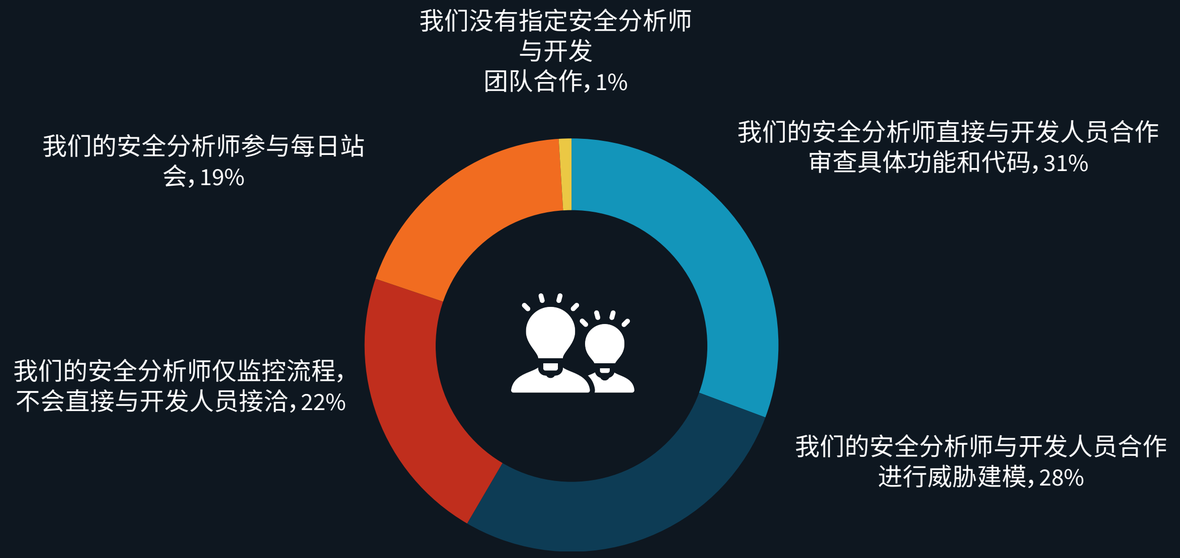
安全分析师越来越多的参与到 AppSec 测试过程中

大部分组织由开发经理或应用安全分析师单独负责管理测试计划，同时也有 29% 的组织报告称由上述双方共同负责管理此计划。安全分析师在帮助开发人员安全构建应用程序方面起着主要的作用。78% 的组织报告称，他们的安全分析师直接与开发人员接洽：31% 的安全分析师直接与开发人员合作审查具体功能和相关代码，28% 的安全分析师与开发人员合作进行威胁建模，还有 19% 的安全分析师会参与每日站会。这种高度参与能够推动双方相互学习与监督，从而确保应用程序得以安全构建。

应用安全测试所有权



安全分析师如何帮助改进项目



返回目录

最为有效的

AppDev 安全计划的 10 大要素

1.应用程序安全控制高度集成到 CI/CD 工具链中。

2.正式记录应用安全最佳实践。

3.应用安全培训包含在持续进行的开发安全培训计划中。

4.开发经理负责向开发人员传达最佳实践。

5.大量开发人员参与到正式的应用安全培训计划中。

6.追踪各个开发团队引入的安全问题。

7.持续改进影响应用安全的正式流程和指标追踪。

8.追踪各个开发团队的持续改进指标。

9.在代码开发过程中追踪安全问题。

10.通过工具自动汇总风险，并让高级开发主管随时了解情况。

返回目录

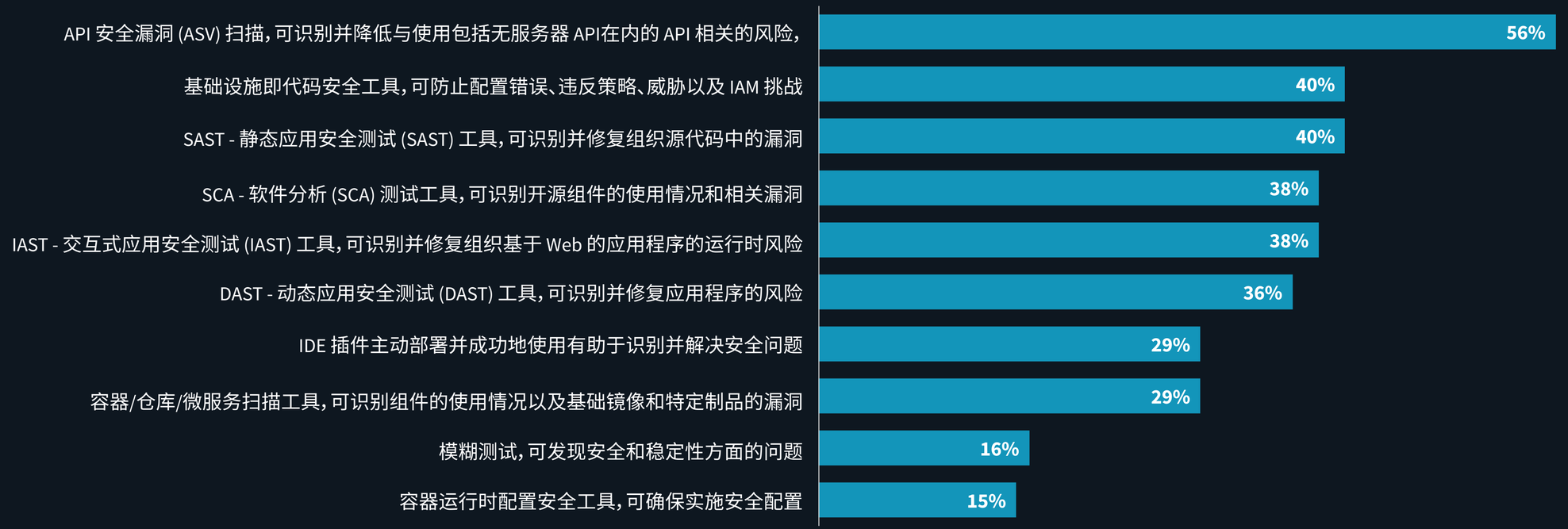
为了确保如今种类繁多的应用程序开发与部署模型的安全，需要使用各种各样的安全测试工具。

各种各样的 AppSec 测试工具正在投入使用

随着应用程序安全日趋成熟，任何单一的测试技术都无法帮助开发团队降低全部安全风险。这就需要安全团队运用通常由多个供应商提供的多种工具来确保 SDLC 的安全。尽管使用情况各不相同，组织认为最重要的工具也有所不同，但大多数组织最终都会混合使用众多工具来满足他们的安全需求。

随着新的开发和部署模型不断出现，为确保它们的安全性，新的测试工具应运而生。一些工具会融入到规模更大的测试平台中，而另一些则长期独立存在。

应用程序安全测试所有权

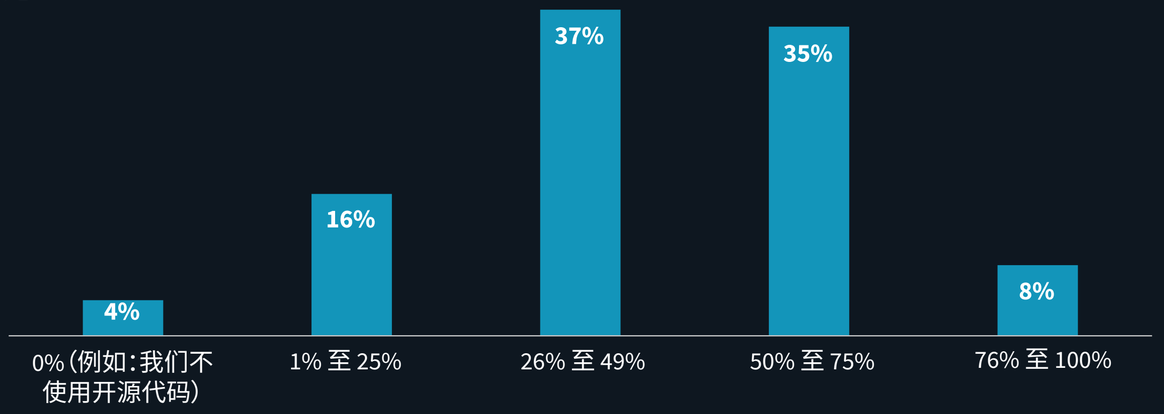


返回目录

现代代码库严重依赖开源代码，但是目前运用开源安全控制的代码库不足一半

尽管各种类型的测试工具已经存在多年，但采用程度还不理想。例如，尽管在现代应用程序开发中使用开源软件至关重要，但是目前报告使用针对开源安全测试工具的开发团队仍然不足一半。虽然许多团队有这样的计划，但这一不确定的趋势也表明了当下众多公司目前对应用安全测试工具的采用情况。

从开源代码中拉取的代码库所占百分比



48%

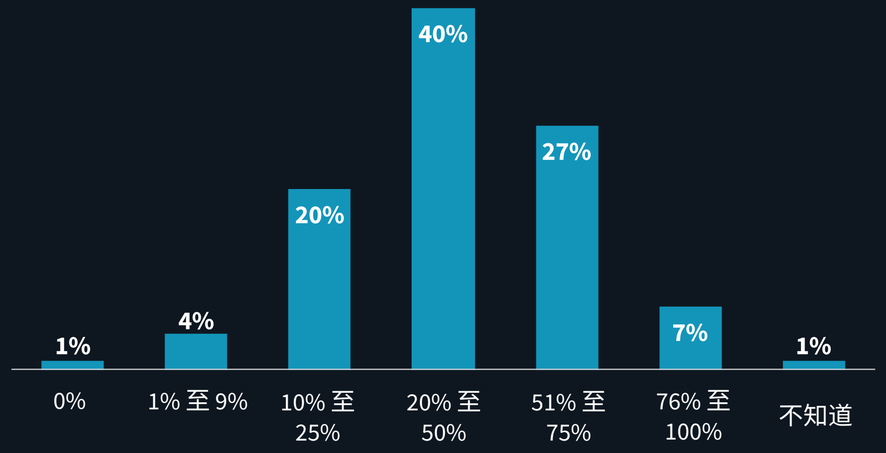
投资于特定的安全控制手段针对开源代码漏洞扫描。

返回目录

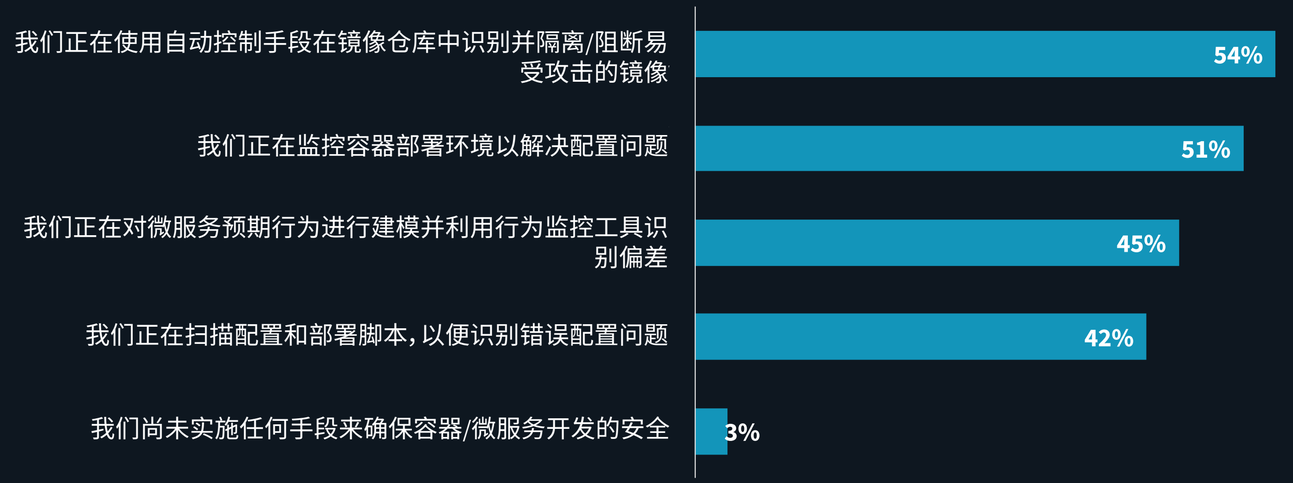
微服务容器开发势头强劲

在某些情况下，更现代化的开发和部署模型会更早开始注重安全程度。在这里我们看到微服务容器开发在相对短的时间内已经得到了广泛采用，特定安全控制手段也随之而来。其他云开发和部署模型也采用了类似模式。

使用容器的开发团队所占百分比



确保容器安全的控制手段



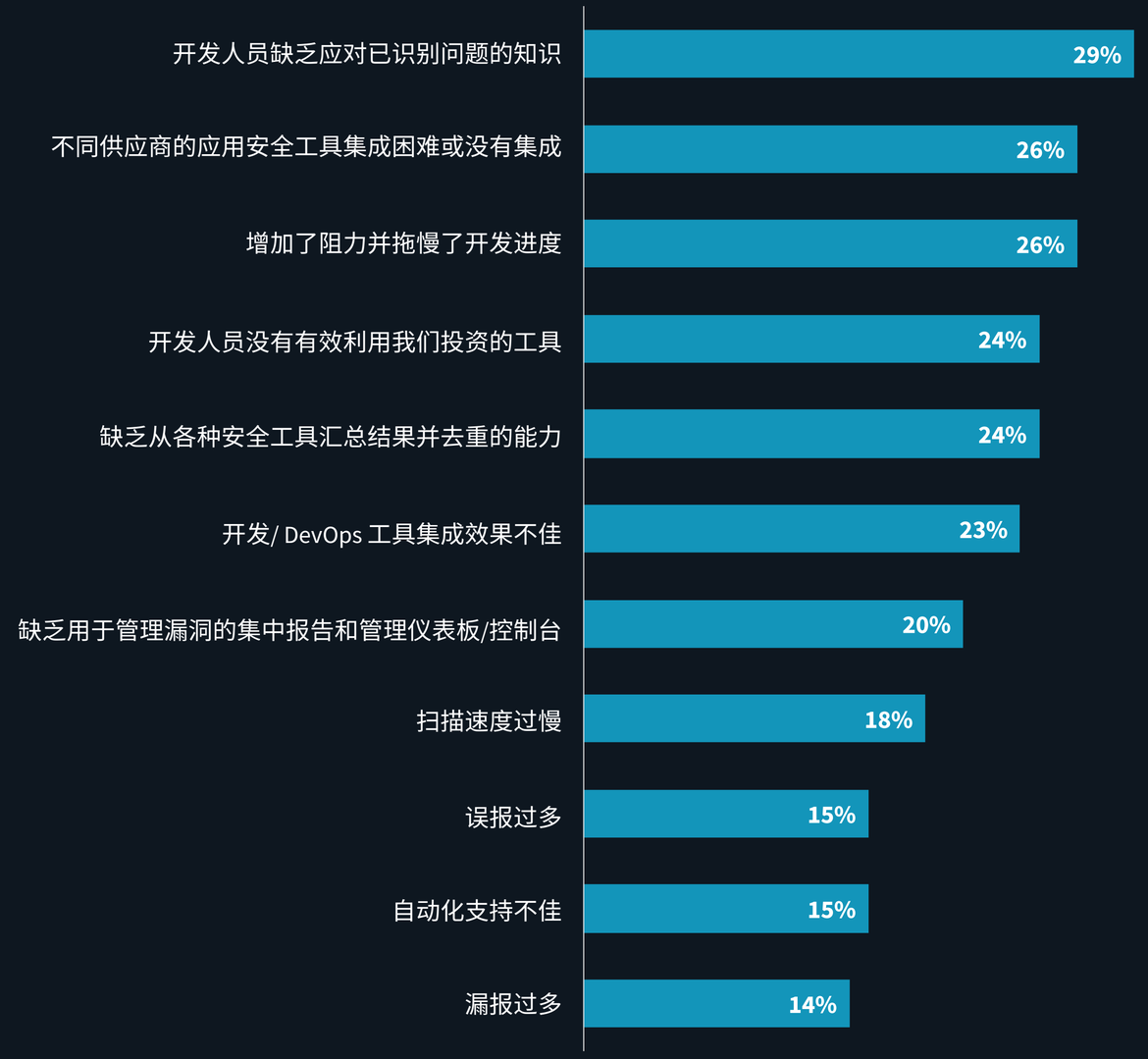
返回目录

目前测试工具面临的挑战

已识别的安全问题归根结底需要由开发人员来解决，然而，大多数组织报告称目前工具使用所面临最普遍的挑战是：开发人员缺乏使用工具解决安全问题的知识。安全工具供应商会推出即时的培训或推荐修复方案来为开发人员提供指导，但是最终还是需要开发人员来完成这项工作。开发人员越能充分理解某些代码引入问题的方式和原因就越能减少问题产生，因此为提供开发人员安全培训应当能逐步解决此类问题。

还有一些组织在集成其它 AppSec 工具方面费尽心思，而大多数人还是担心 AppSec 添加的阻力会拖慢整个开发进程。

目前测试工具面临的主要挑战

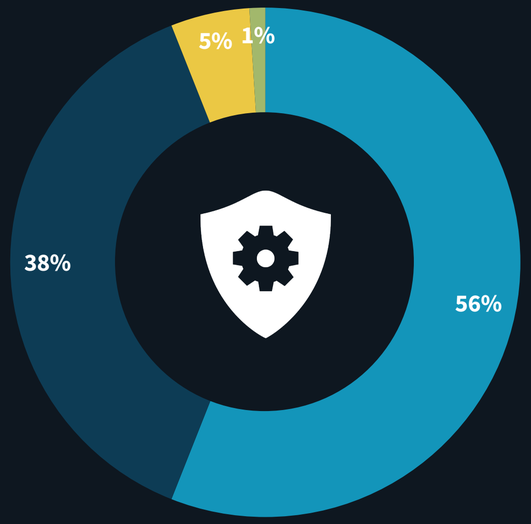


返回目录

DevOps 集成对于改善应用安全计划至关重要

大部分参与调查人员认为，如果项目能够获得成功最重要是得益于在整个 SDLC 中自动执行应用安全测试。DevOps 集成减少了阻力并尽早注重安全问题，可帮助组织尽早识别安全问题。尽管开发人员的培训与工具和流程的改进无疑也会改进项目，但自动化仍是现代应用程序开发实践的重中之重。

DevOps 和 AppSec 集成水平



- 我们在整个 DevOps 流程中使用了一系列高度集成的安全手段
- 我们对安全手段选择性使用，但还会继续集成其它安全手段
- 我们的应用安全工具没有很好地集成到流程中
- 我们尽可能把安全推进到更早的阶段

43%

的组织认为 DevOps 集成对于改进 AppSec 项目至关重要。

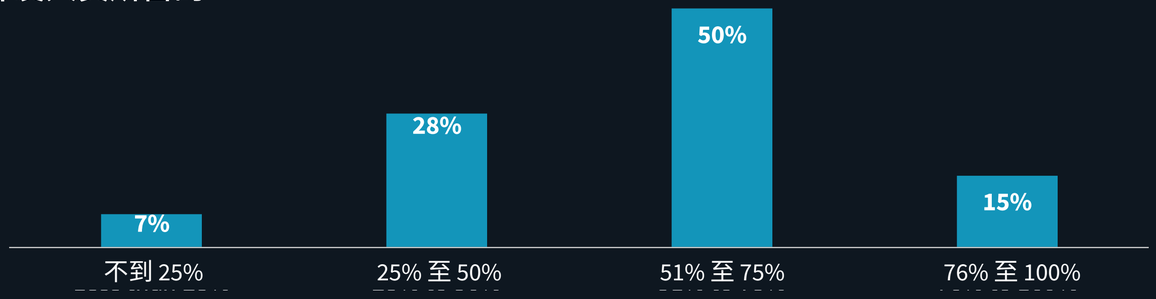
返回目录

开发人员安全培训质量参差不齐，缺乏提高开发人员安全技能的计划。

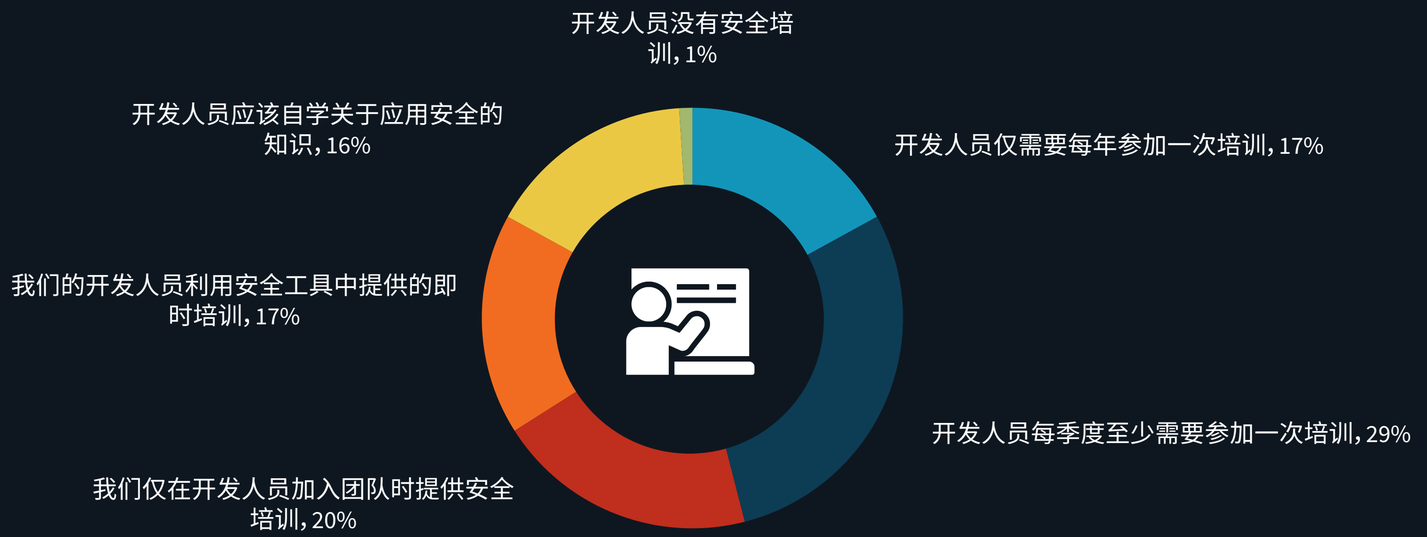
大多数组织都要求开发人员参加 AppSec 培训

大多数组织都要求开发人员参与一定量的应用安全培训，但是有 35% 的组织表示，参与正式培训的开发团队不足一半。仅有 15% 的组织表示，所有开发人员都会参与培训。至于参与培训的频率，不足一半的组织要求开发人员每年参与一次以上的正式培训。

参与正式安全培训的开发人员所占的百分比



应用程序开发人员的安全培训要求

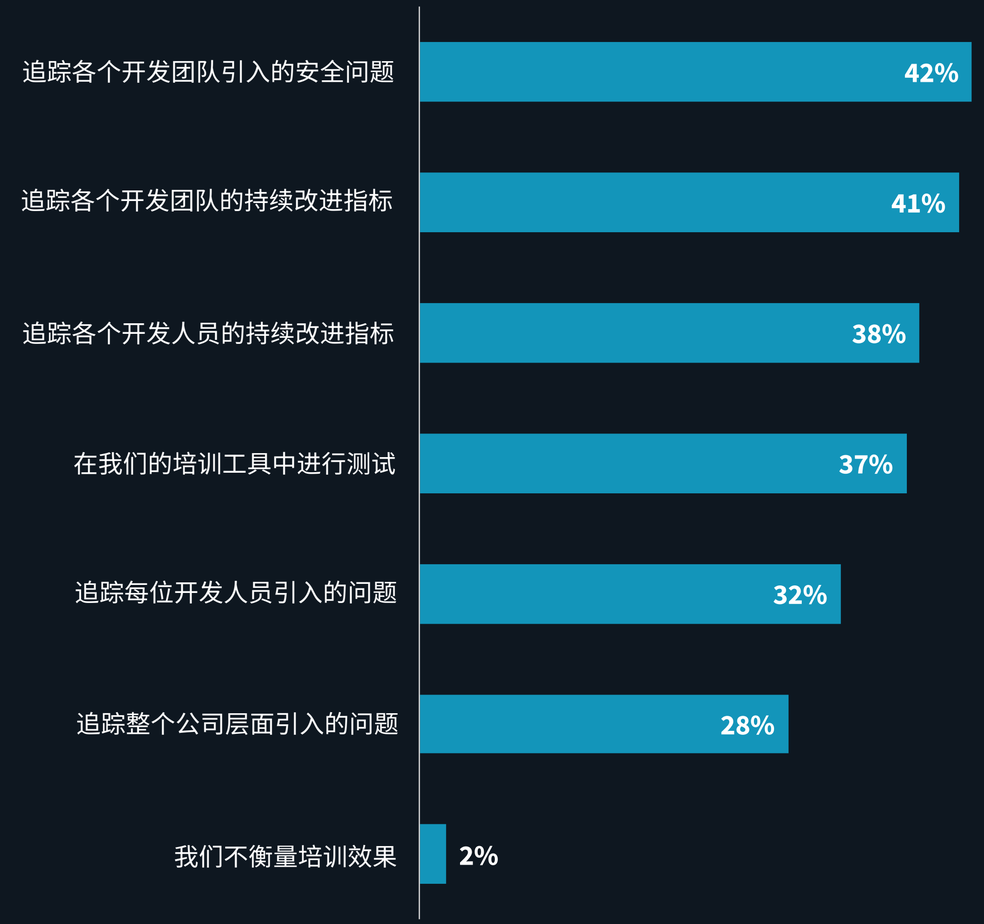


返回目录

大多数组织缺乏衡量开发人员安全培训效果的计划

持续改进安全计划要求衡量开发团队和单个开发人员引入问题的情况。稍多于 40% 的组织报告称，他们会同时追踪问题引入和持续改进指标，从而有针对性地改进那些引入问题最多的团队和单个开发人员。

如何衡量应用程序开发团队的安全培训效果



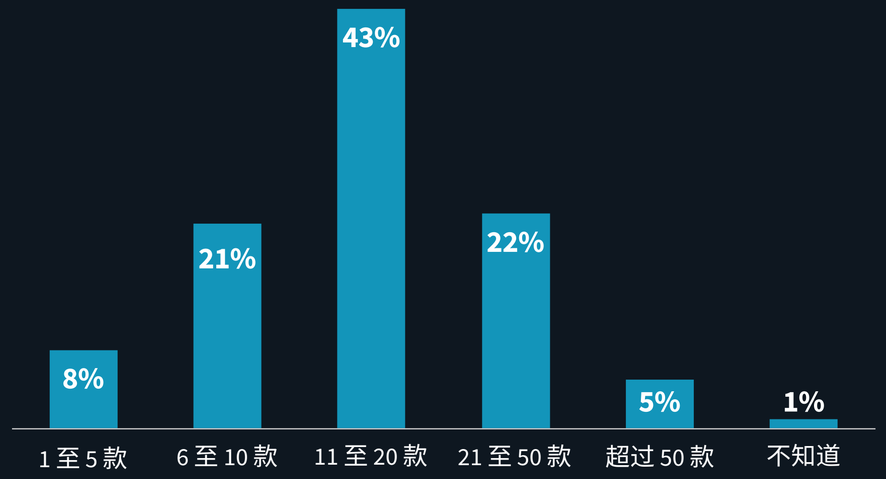
返回目录

AppSec 测试工具激增为许多人带来了问题，超过三分之一的人将投资重点放在了整合上。

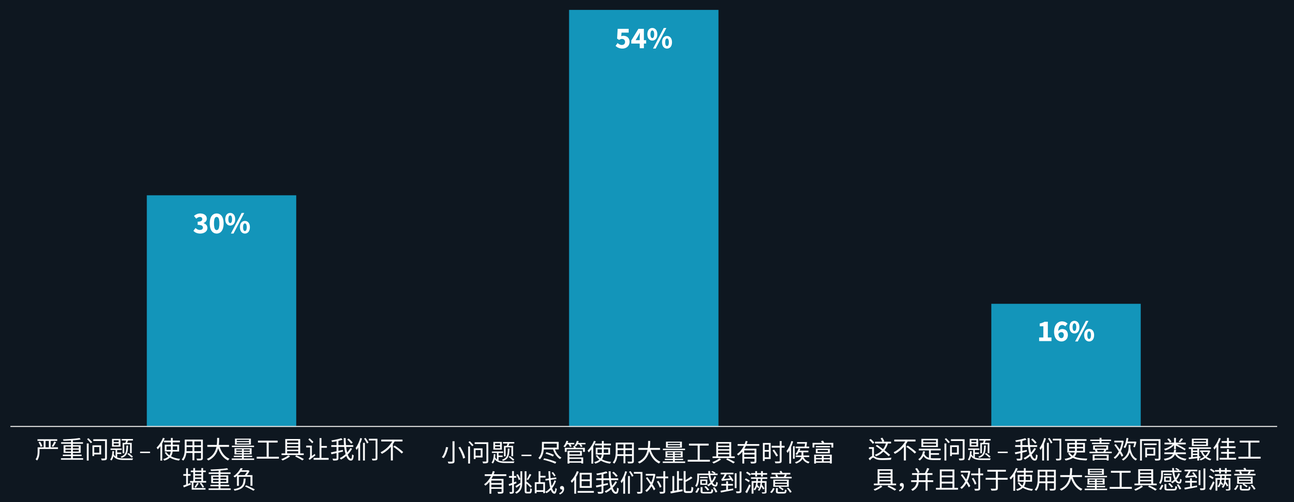
AppSec 工具激增推动组织投资于工具整合

与其他类别的安全控制相似，许多组织使用了太多工具，以致于他们难以集成和管理它们。这往往会导致降低计划的有效程度，并需要安排过多资源来管理工具。72% 的组织使用的工具超过十种，复杂性成为了一个关键问题。

使用的 AppSec 工具数量



工具数量激增本身带给组织的问题

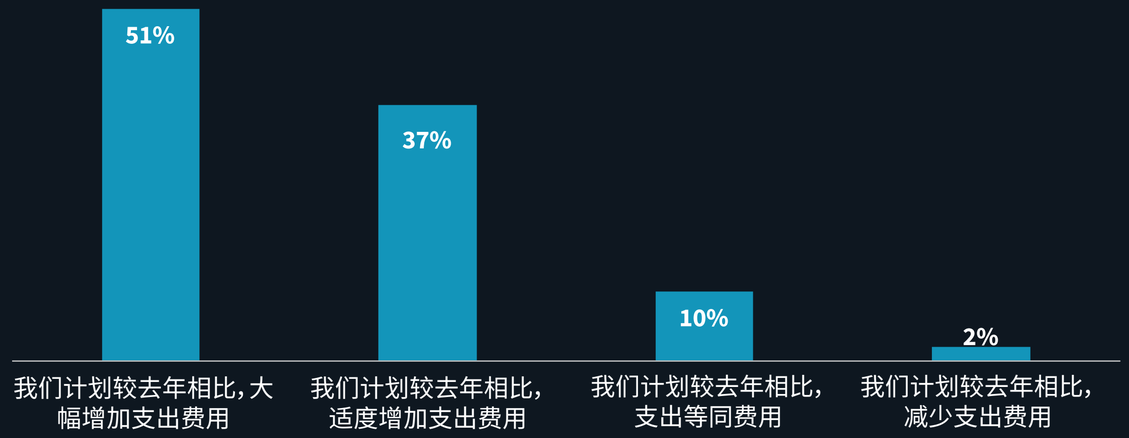


返回目录

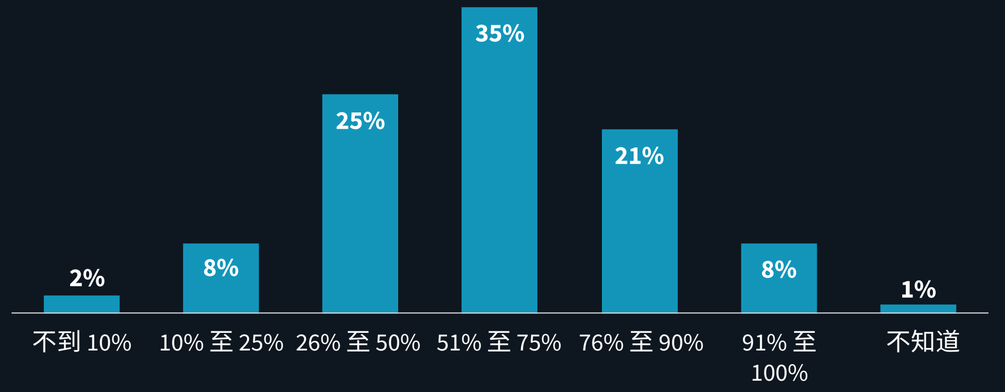
AppSec 方面的支出会继续增加，但对代码的覆盖范围仍不足

尽管大多数组织预计与去年相比将大幅增加应用安全支出，但仅有 30% 的组织在一年内预计能够保护其超过四分之三的代码库。

AppSec 工具在未来 12 个月的预期预算变化



预期在 12 个月内受 AppSec 工具保护的代码库所占的百分比

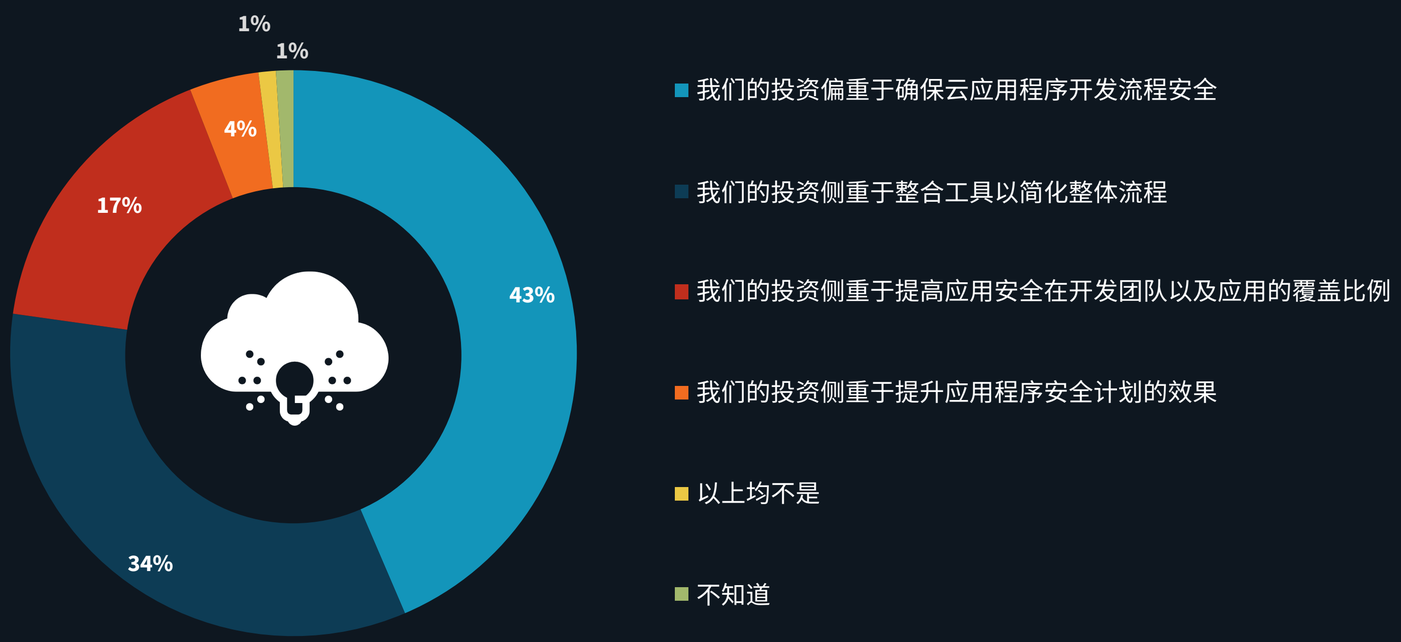


返回目录

AppSec 工具投资方向各异，总体倾向于确保云应用程序开发安全

44% 的组织计划将应用安全投资瞄准云端，三分之一的组织将整点放在工具整合上，以便简化流程。其他组织则计划投资扩大测试工具的使用范围，使更大比例的开发团队和应用程序能使用这些工具。

未来 12 个月内应用安全投资优先级



返回目录

SYNOPSYS®

Synopsys帮助开发团队构建安全、高质量软件，可以最大限度地降低风险，同时最大限度地提高速度和工作效率。Synopsys，公认是应用安全领域的佼佼者，提供静态分析、软件组成分析和动态分析解决方案，支持团队快速发现并修复似有代码、开源组件以及应用程序行为的漏洞和缺陷。Synopsys 结合了行业领先的工具、服务和专业知识，只有它才能帮助组织在 DevSecOps 以及整个软件开发生命周期中优化安全和质量。

了解更多信息

关于 ESG

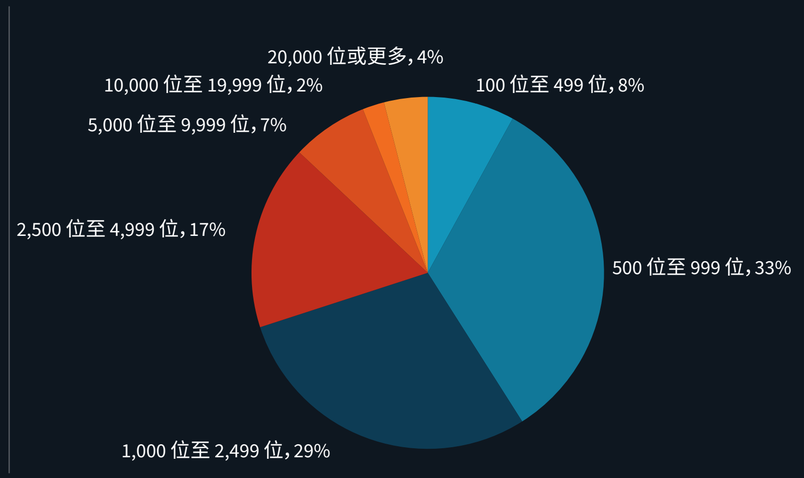
Enterprise Strategy Group 是一家从事 IT 分析、研究、验证并提供战略的公司，我公司致力于向全球 IT 社区提供市场情报和可行见解。

研究方法

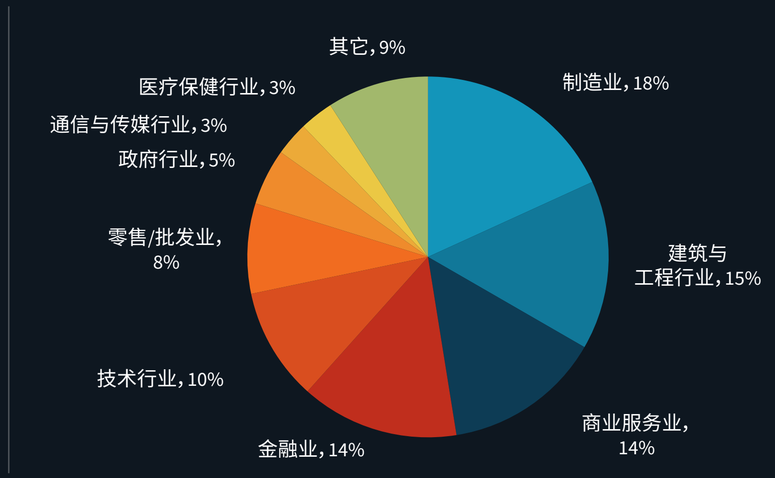
为收集报告数据，ESG 在 2020 年 6 月 12 日至 2020 年 6 月 20 日期间对北美（美国和加拿大）的私营和公共部门组织的 IT 和网络安全专业人员进行了全面的在线调研。当时只有了解或负责确保 AppDev 技术和流程安全的 IT 或网络安全专业人士，或者是涉及确保应用程序开发工具和流程安全的应用程序开发专业人士才有资格作为受访人员，参与本次调研。我们为所有受访人员提供了现金和/或现金等价奖励，鼓励他们完成调研。

在根据多重标准剔出不合格的受访人员、除去重复回复并筛选剩余完整回复以确保数据的完整性之后，我们最终留下共 378 名 IT、网络安全以及应用程序开发专业人员的回复样本。

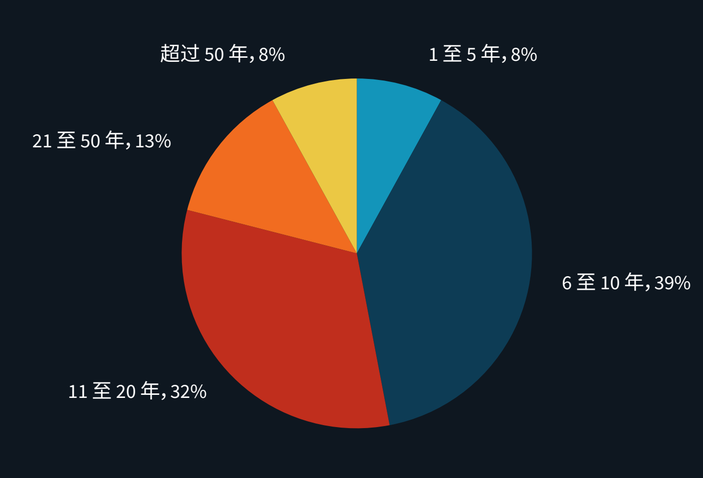
按员工人数划分受访人员



按行业划分受访人员



按组织年限划分受访人员



返回目录

Enterprise Strategy Group 是一家从事 IT 分析、研究、验证并提供战略的公司，我公司致力于向全球 IT 社区提供可行见解和情报。