悬镜 XMIRROR | FreeBuf 咨询

2022 DevSecOps 行业洞察报告

法律声明

ABOUT

关于悬镜

悬镜安全，DevSecOps 敏捷安全领导者。起源于北京大学网络安全技术研究团队“XMIRROR”，创始人子芽。专注于以代码疫苗技术为内核，通过原创专利级“ 全流程软件供应链安全赋能平台 + 敏捷安全工具链”的第三代 DevSecOps 智适应威胁管理体系，持续帮助金融、车联网、泛互联网、能源等行业用户构筑起适应自身业务弹性发展、面向敏捷业务交付并引领未来架构演进的内生积极防御体系。

悬镜安全官网：https://www.xmirror.cn/

关于 FreeBuf 咨询

FreeBuf.COM 网络安全行业门户，每日发布专业的安全资讯、技术剖析，分享国内外安全资源与行业洞见，是网络安全从业者与爱好者广泛关注的行业社区平台。

FreeBuf 咨询集结安全行业经验丰富的安全专家和分析师，常年对信息安全技术、行业动态保持追踪，洞悉安全行业现状和趋势，呈现最专业的研究与咨询服务。

导语

INTRODUCTION

数字化时代，软件定义万物，已逐渐成为支撑社会正常运转的最基本元素之一。随着软件开发过程中开源应用的使用越来越多，开源应用事实上逐渐成为了软件开发的核心基础设施，混源软件开发也已成为现代应用主要软件开发交付方式，开源应用的安全问题也已被上升到基础设施安全和国家安全的高度来对待。

软件供应链开源化，导致影响软件全供应链的各个环节都不可避免受到开源应用的影响。尤其是开源应用的安全性问题，将直接影响采用开源应用的相应软件供应链的安全。除了开源应用开发者因疏忽导致的开源应用安全缺陷，还可能存在具有非法目的开发者故意预留的开源应用安全缺陷，甚至还有恶意攻击者伪造的含有隐藏性恶意功能的异常行为代码被故意上传到上游开源代码托管平台，实施定向软件供应链攻击。上述开源应用中存在的众多安全问题，导致软件供应链的安全隐患大大增加，安全形式更加严峻。

与此同时，随着云计算、微服务和容器技术的快速普及，不仅 IT 基础架构发生了巨大的变化，IT 组织的业务交付模式也迎来巨大变迁——从传统瀑布式开发和一次性全量交付逐渐趋向 DevOps 敏捷开发和持续性交付模式。在业务应用交付规模不断扩大、交付效率要求不断提高、研发及运营场景走向一体化的大环境下，如何在保证快速交付节奏的前提下保障业务安全性是安全部门最大的难题。DevSecOps 敏捷安全应运而生，它通过一套全新的方法论及配套工具链将安全能力完整嵌入整个 DevOps 体系，在保证业务研发效能的同时又能够实现敏捷安全内生和自成长。DevSecOps 敏捷安全的起源、演进和广泛应用，标志着保障软件供应链安全开始进入一个全新的时代。将安全作为 IT 管理对象的一种属性，从软件 SDLC 早期开始安全管理直到覆盖整个软件开发全生命周期，将彻底改善企业和机构在软件供应链和开发基础设施的安全现状。

作为国内 DevSecOps 的主要推动力量之一，从 2016 年初开始，我和悬镜创始团队就一直希望能有机会结合自身在这几年的前沿技术创新研究和行业应用实践沉淀，可以对 DevSecOps 敏捷安全体系的演进做一个系统性的梳理，并分享我们这些年在不同典型用户场景探索的落地实践经验，这也是为何我们花费近 5 年时间沉淀《DevSecOps 敏捷安全》书籍的主要初衷。希望在这个新涌现新变化的前沿技术领域，我们悬镜团队和业界同行一起，凭借长期的技术积累和突破来推动中国自己的安全产业向新的未知空间做更深层次的探索。

2022 年 8 月

目录

CONTENTS

调查篇

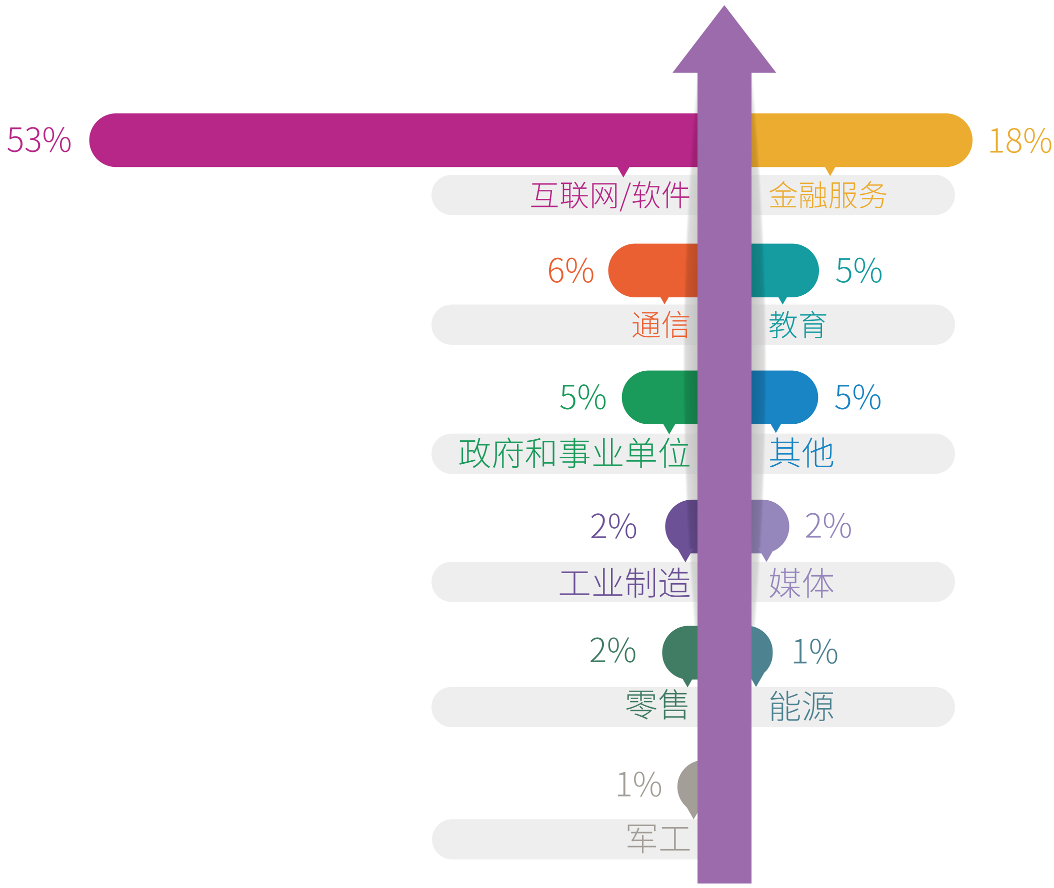
调查篇通过问卷调查、资料收集、交流访谈等形式开展相关调研工作，共收到 1639 条有效调研数据，旨在了解 DevSecOps 实践者和潜在实践者的想法、做法以及遇到的问题。

1

DevSecOps 行业调查

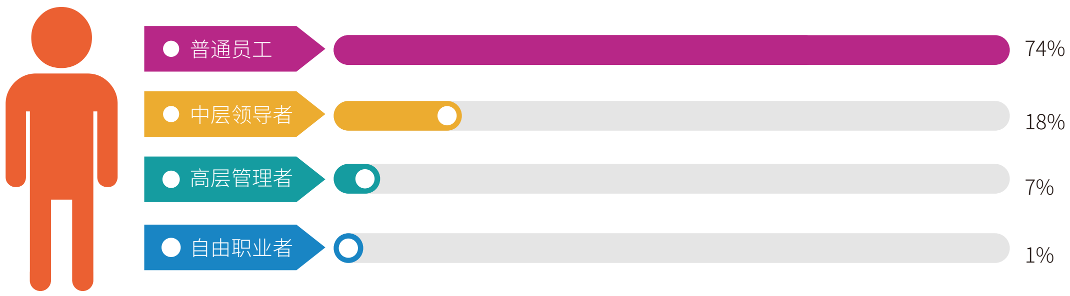
1.1 调研对象及行业领域

您所在组织所属行业领域是？



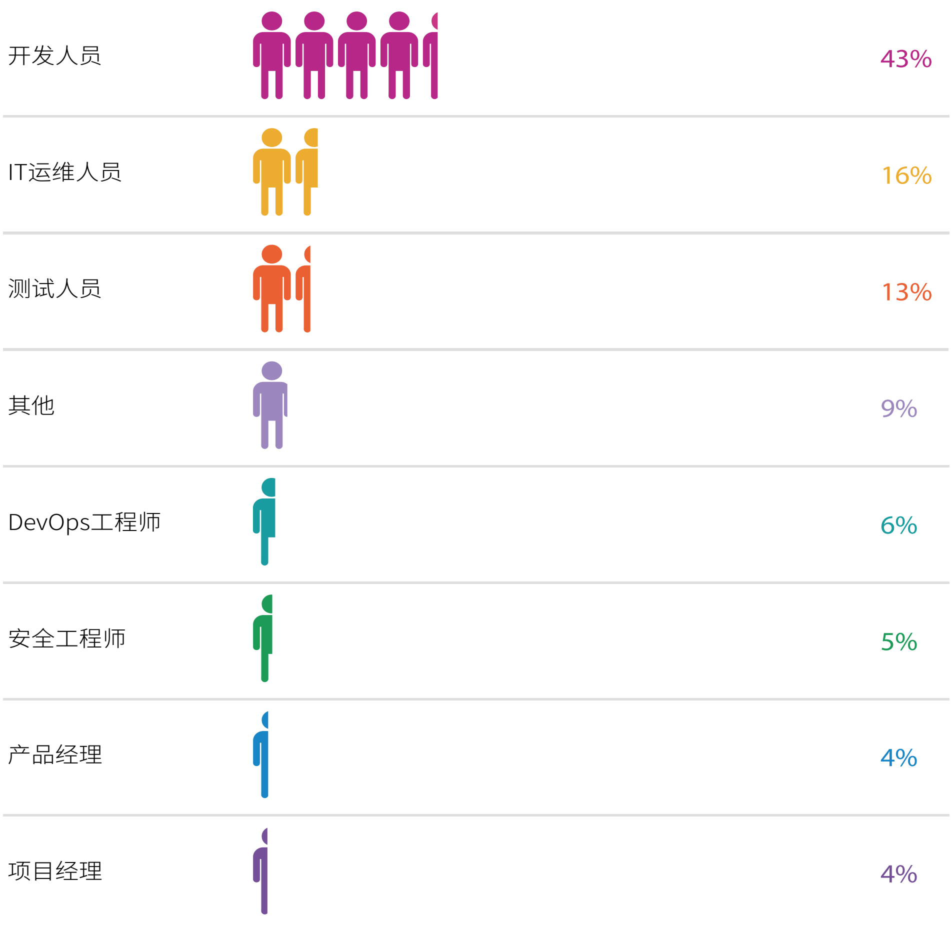
受调者所处行业：本次调查人员共 1639 名，在所有受调者中，来自软件 / 互联网行业的受调者占 53%，来自金融服务行业的受调者占 18%，此两行业受调者总计占比 71%，在其余 29% 的受调者中，教育行业、政府和事业单位各占 5%，通信行业占比为 6%。相较于 2020 年 DevSecOps 洞察分析报告，金融行业、教育行业、通信行业等占比增多，说明越来越多的各类行业开始逐渐关注软件安全领域。

您所在组织中的角色是?



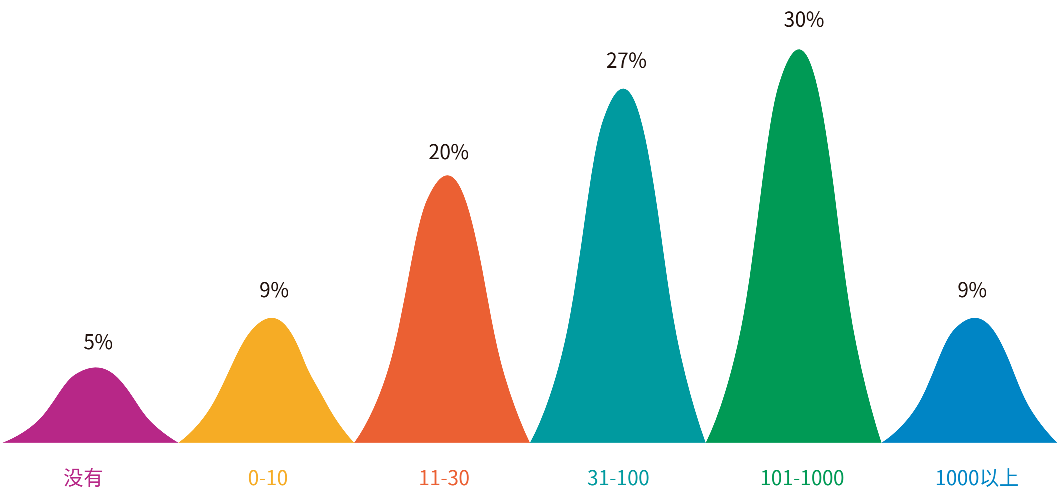
受调者角色: 在受调者中，普通员工的占比最多，占比为 74%，中层管理者占比为 18%，高层管理者占比为 7%，自由职业者占比为 1%，在实际工作中，普通 IT 员工和中层管理者与 DevSecOps 实践联系依旧最为密切，但相较于 2020 年 DevSecOps 行业洞察分析报告，高层管理者占比有所增加。

您所在组织的职位是?



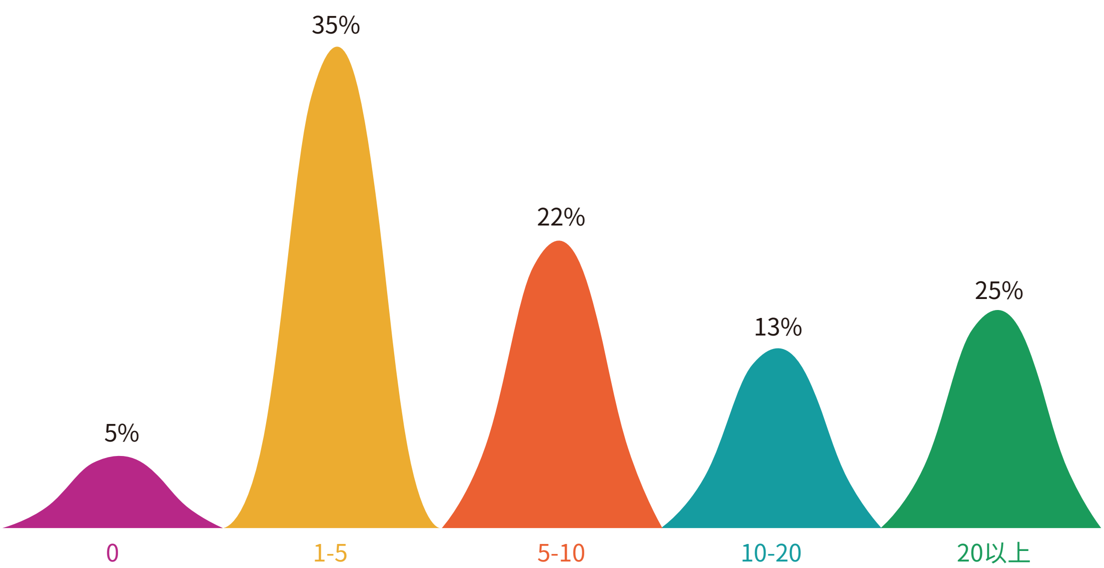
受调者职位：在所有受调者中占比最大的是开发人员，占总人数的 43%，IT 运营人员占 16%，测试人员占 13%，除此之外，其他受调者占比均低于 10%，分别为 DevOps 工程师 6%，安全工程师 5%，产品经理、项目经理各占 4%，其他受调者仅占总人数的 9%。由数据结果可得知，DevSecOps 始终与开发、测试及运维人员的关系更为密切相关。

您所在组织从事开发的人数规模是？



受调者所在组织的开发人员：在所有受调者中，仅有 9% 的受调者所在组织的开发人员人数大于 1000 名，所在组织开发人数在 101-1000 区间范围内的受调者占比为 30%，所在组织开发人员人数规模小于 100 名的受调者占 61%，其中组织开发人员人数规模在 11-30 区间范围内的受调者占比最多，为 20%。

您所在组织安全人员的人数规模是？



受调者所在组织的安全人员：在所有受调者中，25% 的受调者所在组织的安全人员人数大于 20 名，所在组织安全人数在 10-20 区间范围内的受调者占比为 13%，受调者所在组织安全人员人数在 5-10 区间范围内的占 22%，其中组织安全人员人数规模在 1-5 区间范围内的受调者占比最多，为 35%。

小结

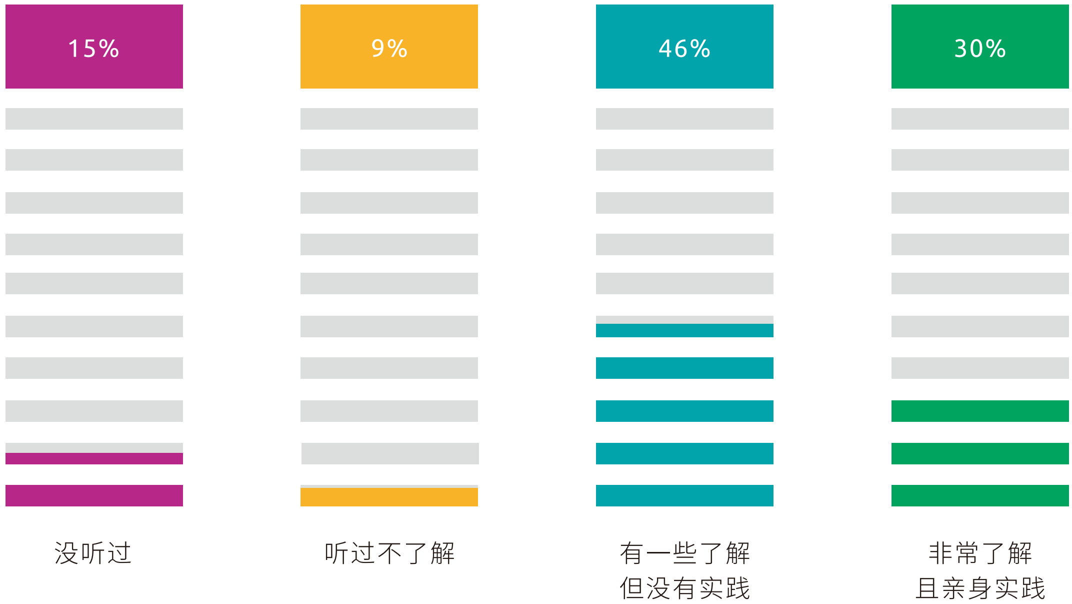
在我国各行各业都离不开软件的支持，所以越来越多的不同行业都开始逐渐意识到软件安全的重要性，但是由于不同行业安全需求不同，其安全侧重点也是不同的。与 2020 年 DevSecOps 行业洞察分析报告相似，互联网行业与金融行业的受调人员的占比依旧较高，但其他行业的占比相比于 2020 年报告有所增加。此外作为 DevSecOps 落地实践者中，开发、测试及运营人员对软件生产及使用过程的安全风险等认知更为深刻，因此本次调查中更多的是开发、测试及运营人员参与其中。

大家说：

安全问题是最容易忽视的问题，对我们金融行业来说，安全一直排在首位。

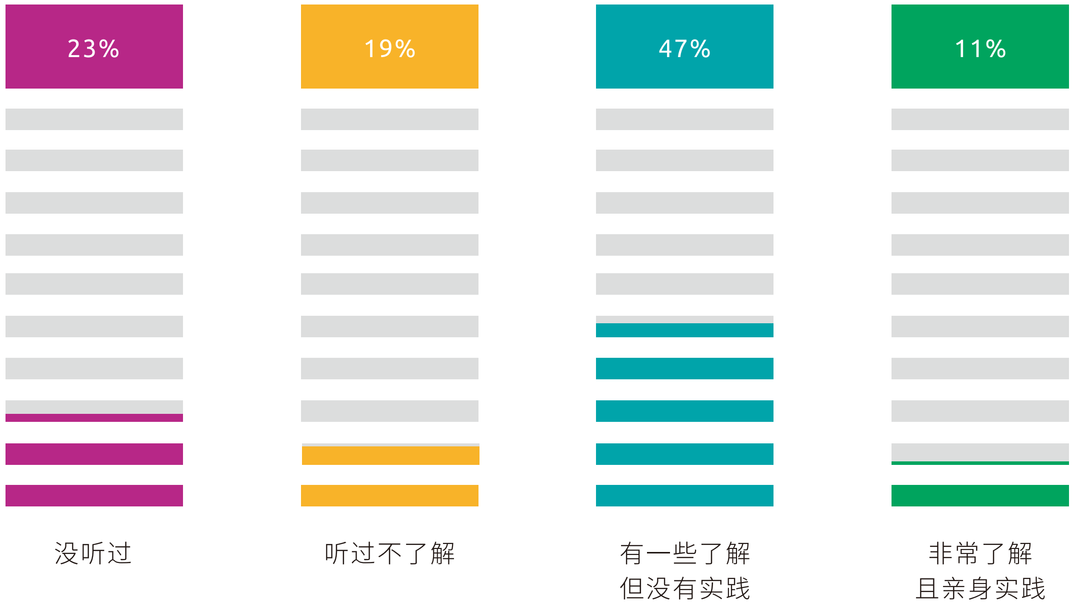
—— 慕斯 金融服务行业 江苏南京

您对 DevOps 的了解程度如何?



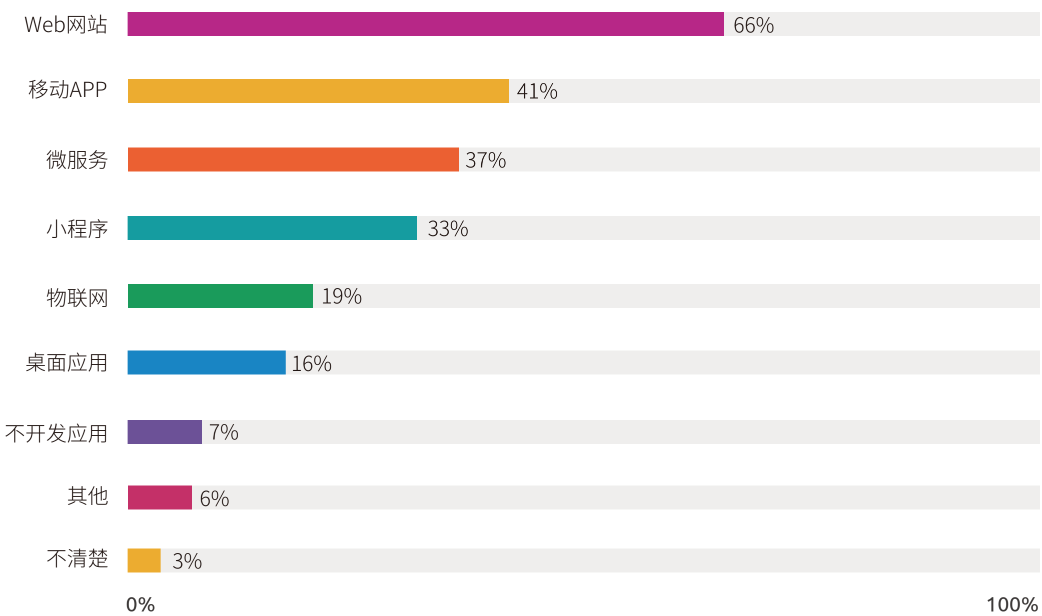
受调者对 DevOps 的熟悉程度：在所有受调者中，有一些了解但没有亲身实践的受调者人数占比最多，为 46%，对于 DevOps 非常了解且有亲身实践的人数占 30%，听过但不了解的受调者占比为 9%，完全没听过的受调人数占比为 15%，通过该数据可以反映出，相较于 2020 年报告，完全没听过和听过但不了解的受调人数比例在下降，对 DevOps 了解的受调人数比例不断增多，说明各企业组织已经逐渐布局 DevOps 模式，但实践部分仍有很大发展空间。

您对 DevSecOps 的了解程度如何?



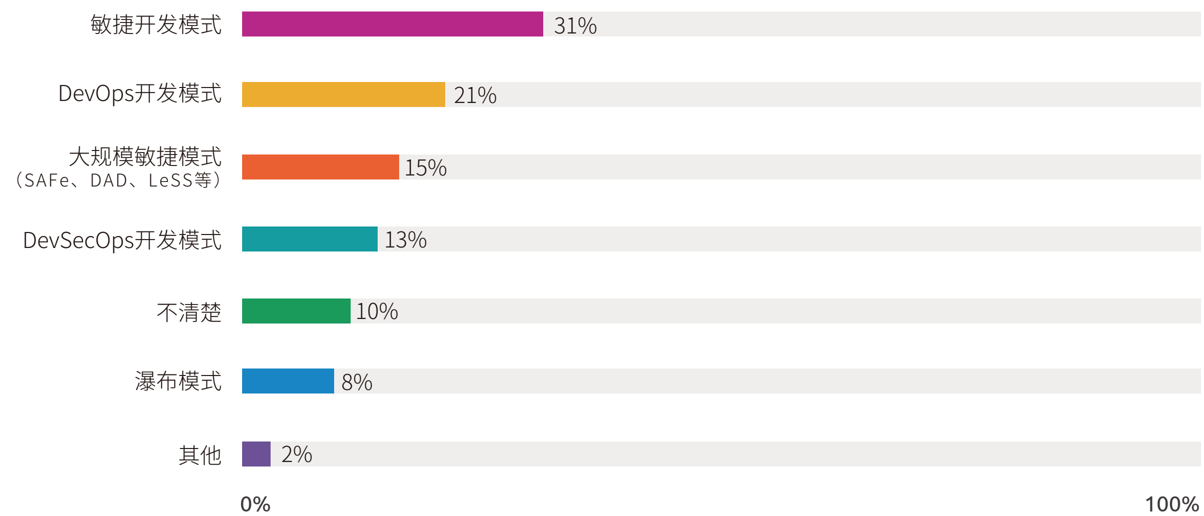
受调者对 DevSecOps 了解程度：在所有受调者中，对 DevSecOps 完全没听过的比重为 23%，相较于 2020 年报告，对 DevSecOps 完全没听过的比重大幅降低，听过但不了解的受调者占比为 19%，有一些了解但没有相关实践经验的受调者占比为 47%，对于 DevSecOps 非常了解且有一定亲身实践的受调者占 11%，这部分数据可以反映出，各企业组织已逐渐开始意识到高效安全开发的重要性，DevSecOps 概念开始深入人心。

您所在组织开发的应用类型是?



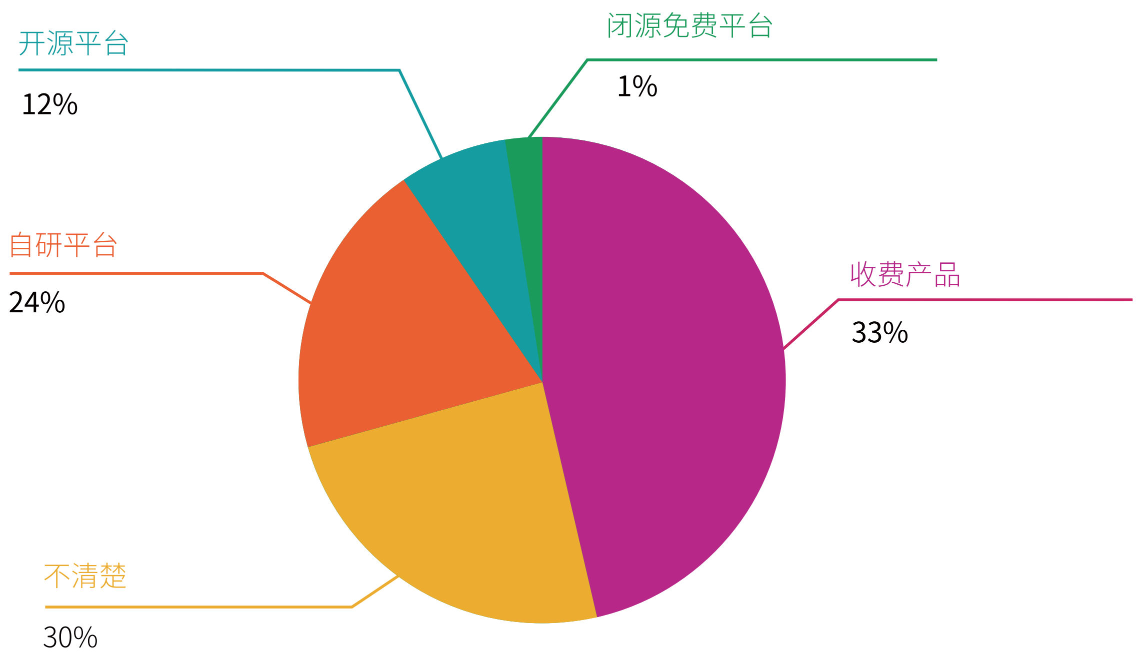
受调者所在组织开发的应用类型：受调者所在的单位中，开发 Web 网页应用的组织占比最高为 66%，其次是移动 APP 占比为 41%，除此之外组织开发类型较多的为小程序占比为 33%、微服务占比是 37%、物联网占比为 19%、桌面应用占比为 16%，可以看到 Web 网站和移动 APP 仍然是目前组织开发的主流应用类型，小程序和微服务占有一定的比重份额。

您所在组织软件产品研发所使用的流程模式?



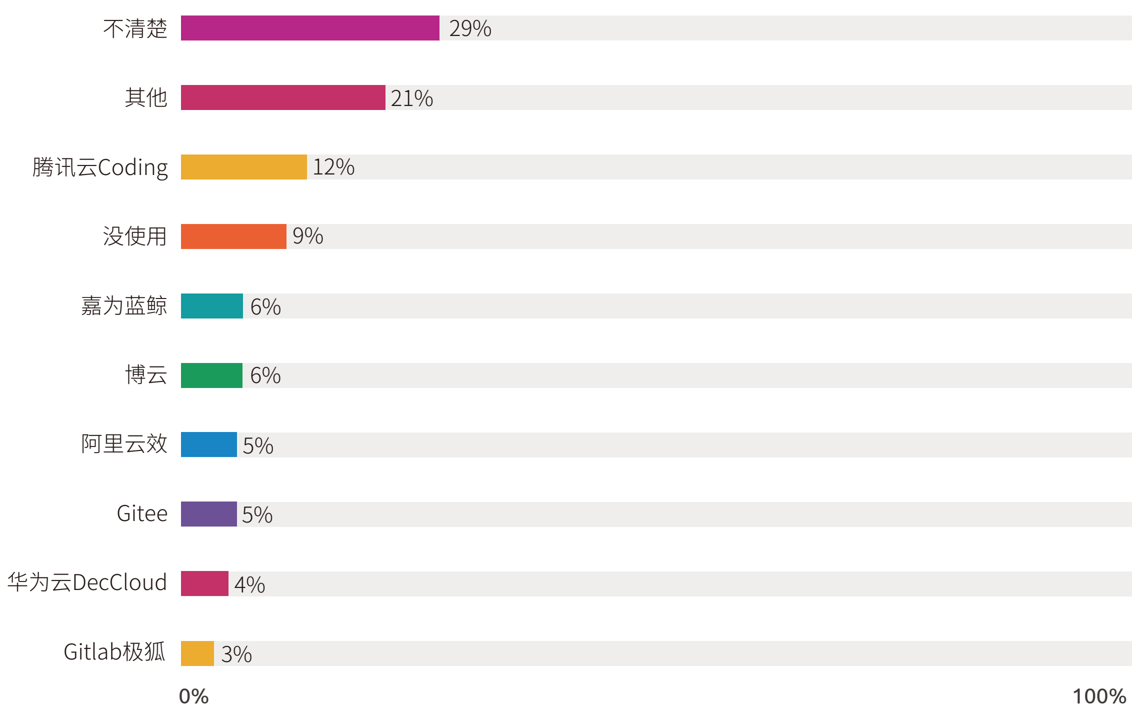
受调者所在组织的软件研发流程模式：在所有受调者中，21% 受调者所在组织在软件开发时已经开始使用 DevOps 开发模式，13% 受调者已经开始使用 DevSecOps 开发模式，31% 受调者所在组织在软件开发时使用敏捷开发模式，而瀑布模式仅占 8%，通过数据可以发现，敏捷开发模式依旧是目前市场上组织进行软件研发的主流选择，但相较于 2020 年报告，选择使用 DevOps 和 DevSecOps 模式的组织逐渐增多。

您所在组织使用的 DevOps 平台的来源是?



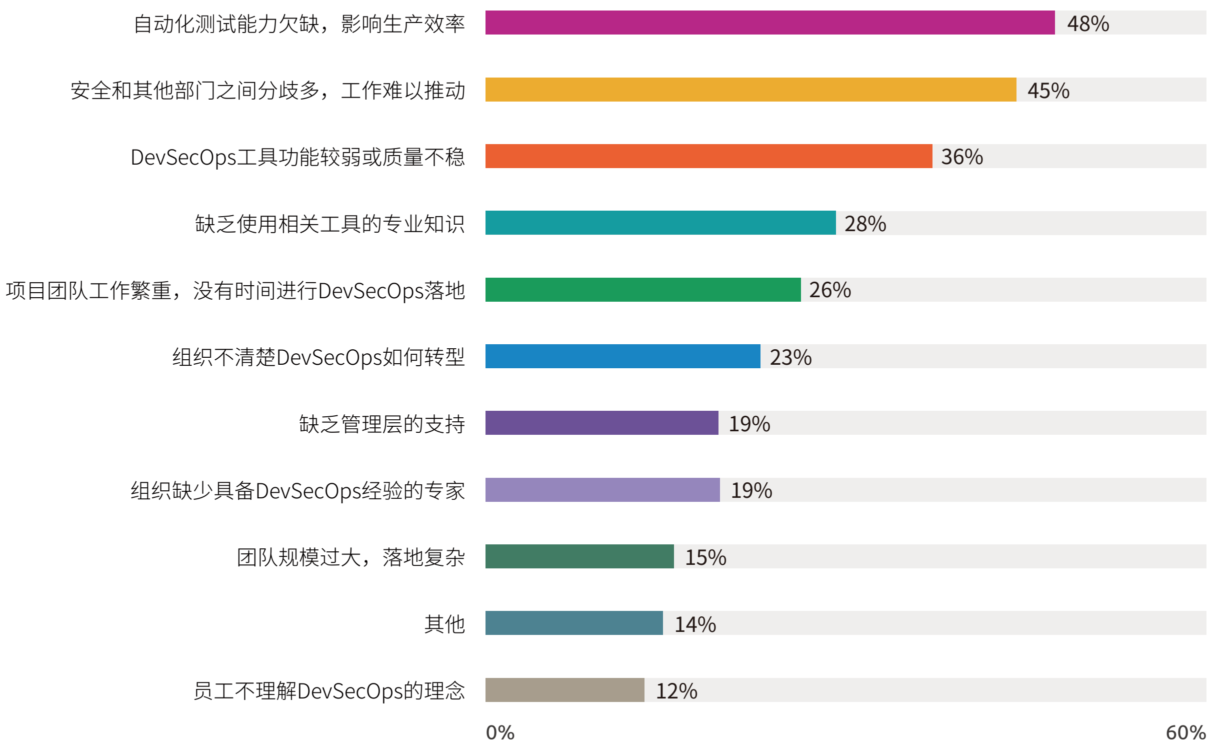
受调者所在组织使用的 DevOps 平台来源：在采用 DevOps 开发模式的组织中，使用收费的 DevOps 平台的受调者所在组织占比最多，为 33%，受调者所在组织选择使用开源平台和自研平台的组织分别占 12% 和 24%，而选择闭源免费平台的组织仅占 1%。

您所在组织使用 DevOps 支撑平台是?



受调者所在组织使用的 DevOps 平台来源：在受调者所在组织中，9% 的组织未使用过 DevOps 平台，在使用 DevOps 平台的组织中，阿里云、腾讯云、华为云自身 DevOps 产品的使用者较多，嘉为蓝鲸也有相当数量的使用量，可以看到，相较于 2020 年 DevSecOps 行业洞察报告，没使用 DevOps 支撑平台的比例大幅减少，此外，组织在选择使用 DevOps 支撑平台时，依旧会优先选择互联网头部厂商的平台。

您所在组织推行 DevSecOps 遇到过哪些障碍？



受调者所在组织推行 DevSecOps 遇到的障碍：在采用 DevSecOps 开发模式的组织中，受调者所在组织不清楚 DevSecOps 以及如何转型占比为 23%，组织缺少具备 DevSecOps 经验的专家以及缺乏管理层的支持的均占比为 19%，组织项目团队工作繁重，没有时间进行 DevSecOps 落地占比为 26%，组织内 DevSecOps 工具功能较弱或质量不稳定占比为 36%，组织团队规模过大，落地复杂占比为 15%，缺乏使用相关工具的专业知识占比为 28%，组织中员工不理解 DevSecOps 的理念占比为 12%，自动化测试能力欠缺，影响生产效率占比为 48%，安全和其他部门之间分歧多，工作难以推动占比为 45%，该数据表明，企业组织在推行 DevSecOps 落地实践时或多或少的都会遇到难以推行的障碍，其中存在的较为严重的问题是自动化能力欠缺，影响生产效率以及以及安全部门和其他部门之间存在分歧。

小结

随着业务的发展以及产品的快速迭代，安全已经无法跟上业务的脚步，因此需要在 DevOps 模式中引入安全要素，在实现快速交付的同时保障软件的安全。相较于 2020 年报告中的数据，各企业组织已经不单单只是将安全停留在被动响应层面上，而是已经越过“救火队员”这一阶段，开始积极主动应对安全问题。但 DevSecOps 落地实践也绝非易事，在实施过程中 DevSecOps 文化如何塑造、自动化工具如何使用、开发运营一体化流程如何依托、DevSecOps 成功落地实施评估标准、DevSecOps 落地实践成熟度等，都是组织落地 DevSecOps 存在的难题。但实践出真知，企业组织也只有在实践过程中才能不断总结经验教训，找到并完善适合于自身的 DevSecOps 模式。

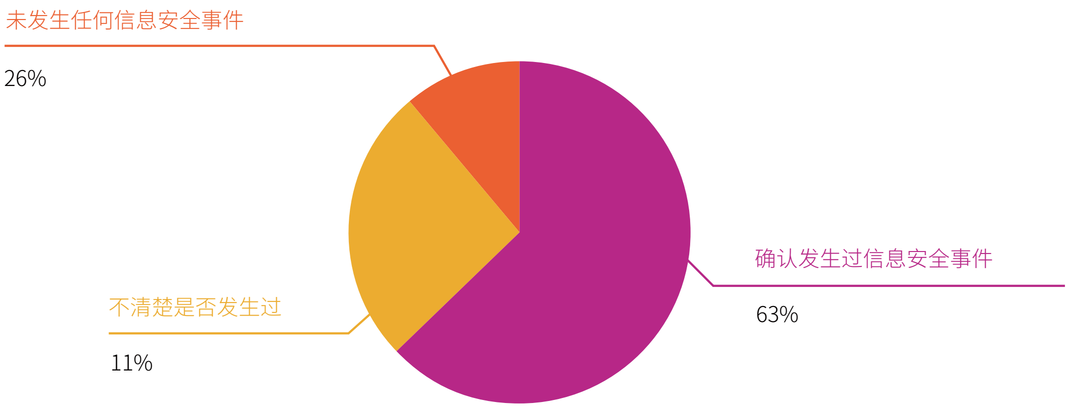
大家说：

DevSecOps的落地重点在于人，安全通过平台与工具对研发与测试团队赋能，同时还需要提升他们的安全意识与安全责任感。

—— Eurekaovo 软件/互联网 广州市深圳

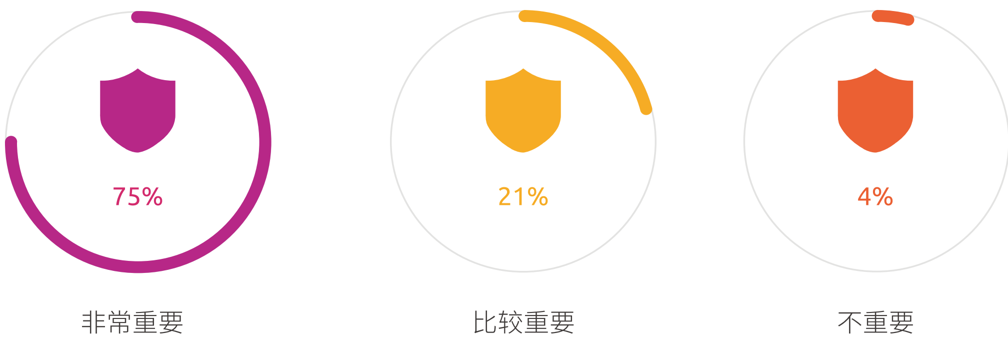
1.3 组织软件应用安全现状

过去一年，您所在组织所开发的软件应用中是否发生过信息安全事件？



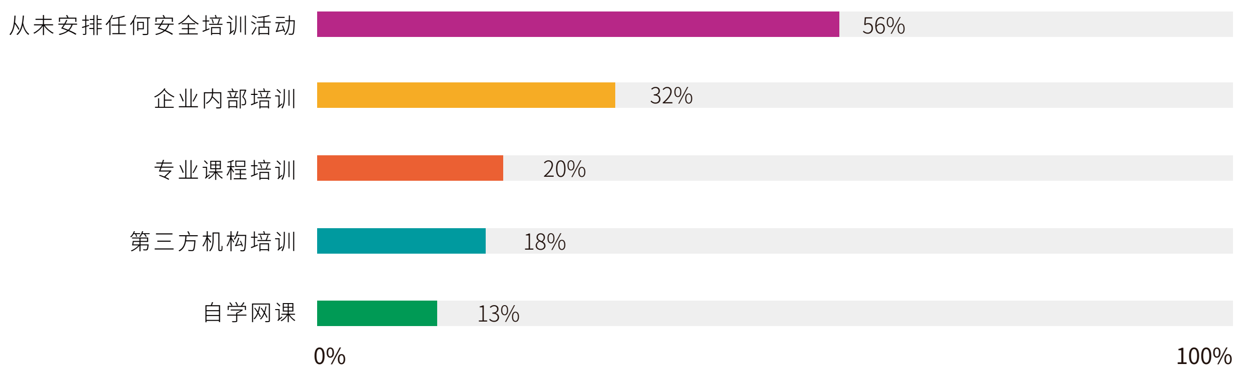
受调者所在组织过去一年发生的信息安全事件：超一半的受调者确认组织在过去一年发生过信息安全事件，占比为 63%，26% 的受调者表示所在组织在过去一年未发生任何信息安全事件，11% 的受调者表示并不清楚是否发生过信息安全事件。

您觉得在软件应用中，安全的重要性是？



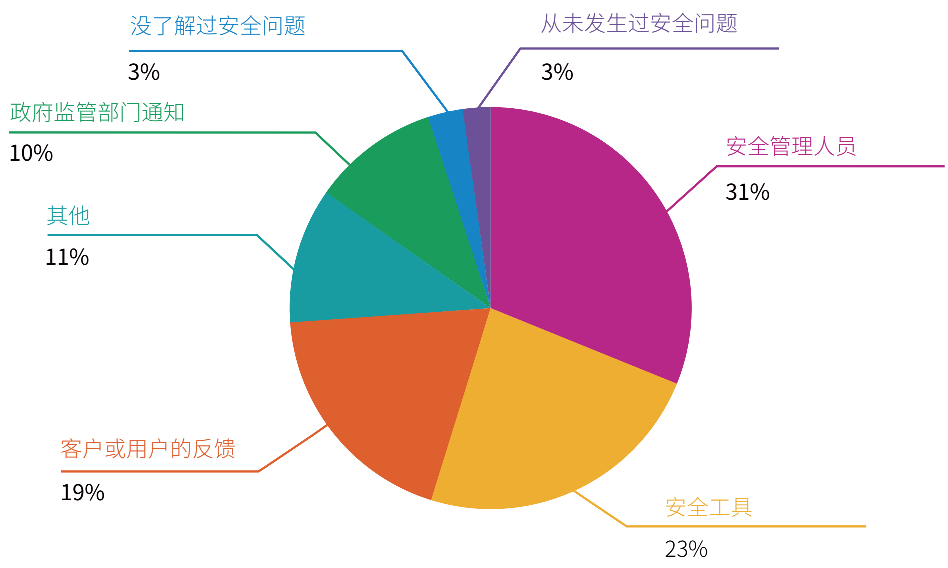
应用安全的重要性：调查数据显示，绝大多数受调者认识到安全在软件应用中的重要性，占比 96%，但仍有 4% 的受调者缺乏相关安全意识。

您所在的组织是否有安排过安全培训活动?



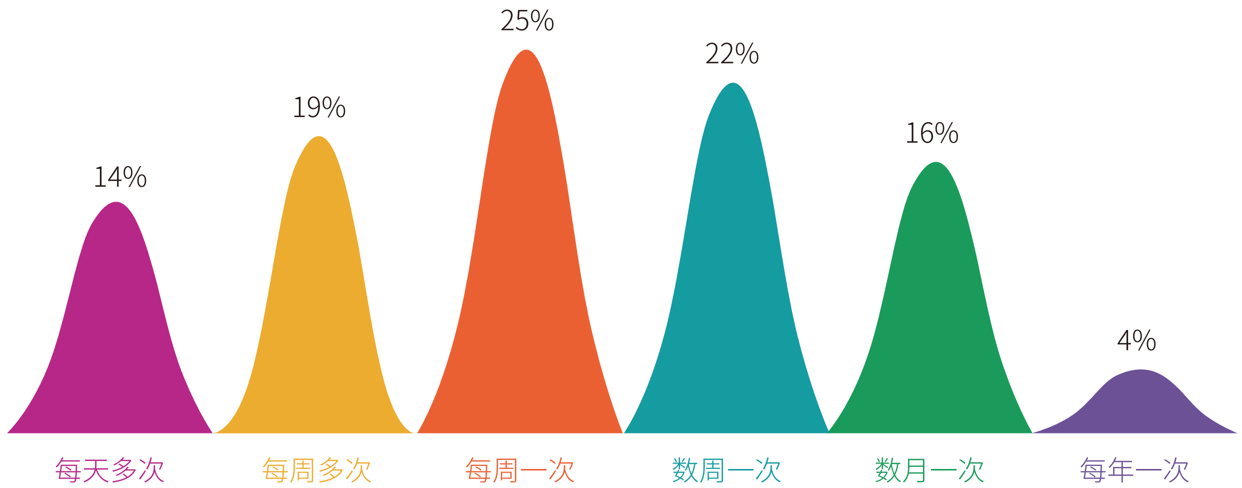
受调者所在组织的安全培训活动情况：调查数据显示，从未安排任何安全培训活动的受调者占比 56%，绝大部分企业组织的安全培训大致分为三种，分别是第三方机构培训、企业内部培训和专业课程培训，占比分别为 18%、32% 和 20%，自学网课占比为 13%，由此得知，各组织企业正逐渐加强培养人员安全意识。

您是通过哪些渠道获知软件应用的安全问题?



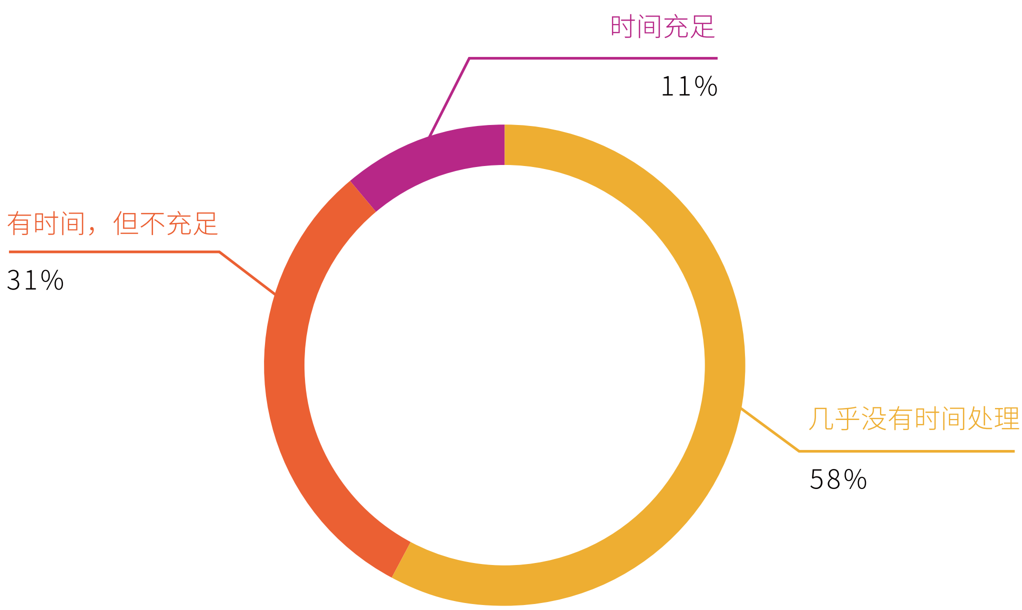
受调者获知应用安全问题的渠道：通过安全管理人员的反馈来获知应用软件安全问题的受调者较多，占比为 31%，受调者通过客户反馈获知安全问题占比为 19%，通过政府监管部门通知以获知安全问题占比为 10%，通过安全工具获知安全问题的受调者占比 23%，从未发生过安全问题或不了解是否发生过安全问题的占比分别为 3% 和 11%。

您所在组织软件应用发布上线的频率是？



受调者所在组织软件应用发布上线频率：58% 的组织每周都会进行软件应用发布，其中每周一次的组织占 25%，每周多次的占 19%，而每天多次上线新版本的组织占 14%，除此之外，数周一次的占 22%，迭代周期为数月的组织占 16%，低于每年一次上线软件版本的组织仅占 4%。

在您所在组织的结构与协作模式下是否有足够的时间处理软件应用中的安全问题？



受调者所在组织处理应用安全问题的时间：调查数据显示，89% 的受调者所在组织用于处理软件应用中安全问题的时间不足，只有 11% 的受调者所在组织有充足的时间用于处理软件应用中安全问题。

小结

近年来软件安全问题一直呈快速增长态势，造成的危害也越来越严重，安全问题不容小觑。对于企业组织来说，从人员上，需要加强开发、运营、安全团队的安全意识，安全已不再仅仅是安全团队的责任，是每个人的责任；从技术上，引入安全自动化工具；从流程上，制定安全度量标准、风险监控机制等，以此保障软件安全。

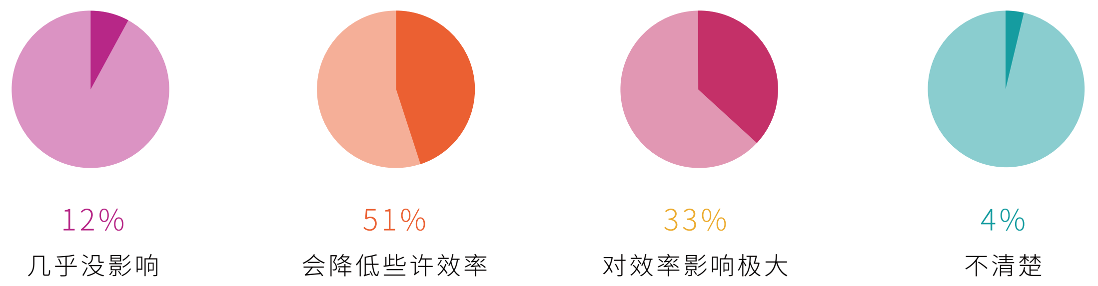
大家说：

安全对于研发团队的素养有较高的要求，如何降低整体的成本是DevSevOps能否大规模推广的重中之重，提供平台化的整体解决方案才能在当前众多产品中杀出重围。

—— Sinky 软件/互联网 北京

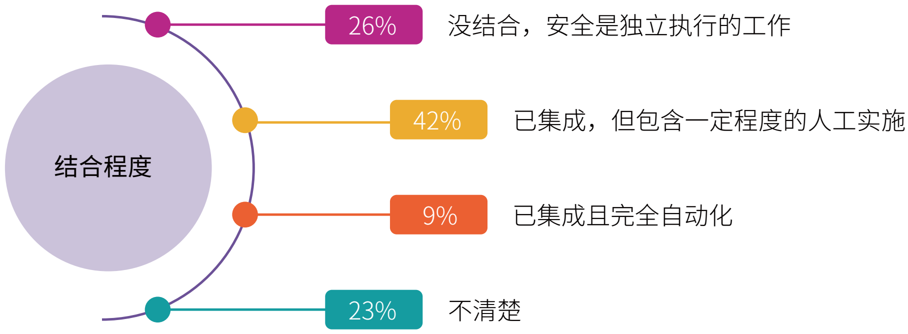
1.4 软件生命周期安全现状

您认为安全工作对软件应用生产效率的影响是？



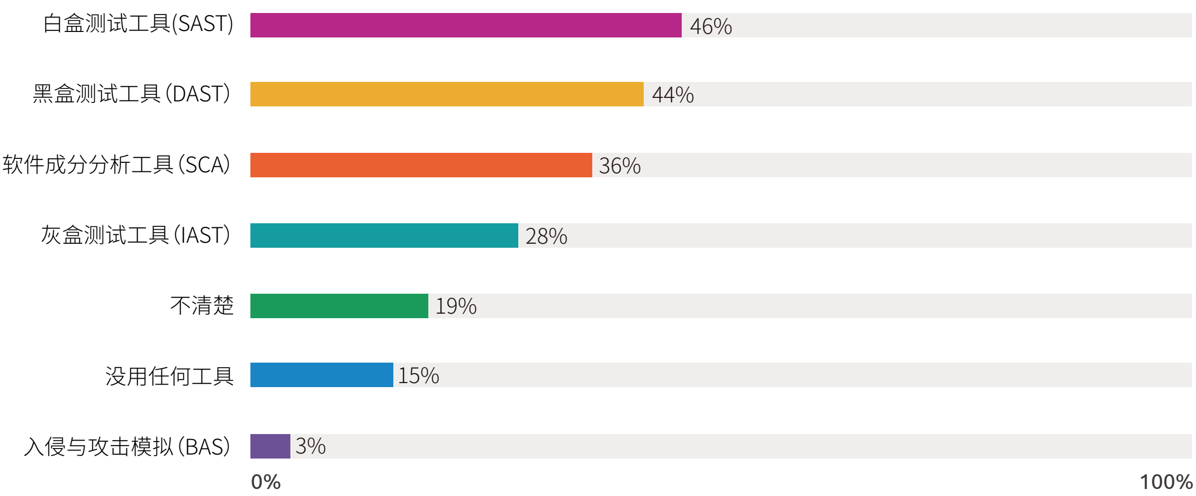
受调者所在组织安全工作对软件应用生产效率的影响：84% 的受调者表示安全工作会影响软件应用生产的效率，其中 51% 的受调者表示会降低些许效率，33% 的受调者表示对效率的影响巨大，除此之外 12% 的受调者表示组织的安全工作对软件应用的生产效率几乎没有影响，4% 的受调者表示并不清楚是否存在影响。

您单位软件运营流程与安全保障工作的结合程度是？



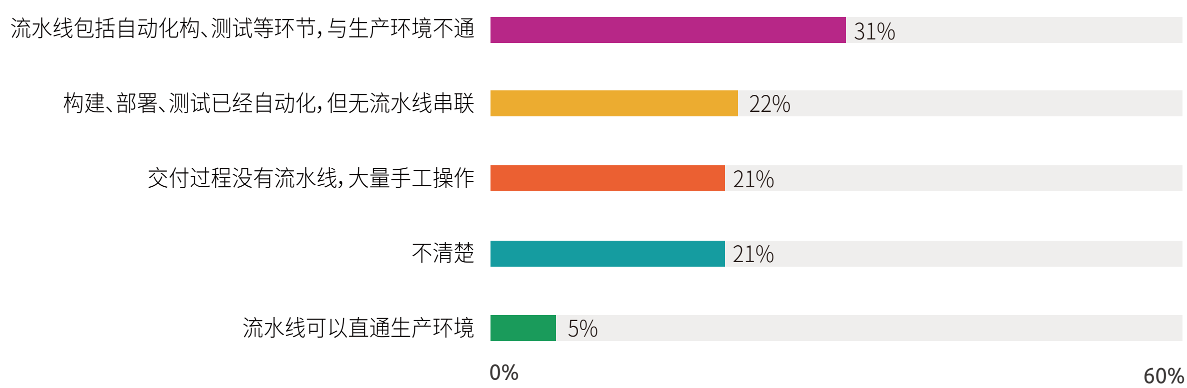
受调者所在组织软件运营流程与安全保障工作的结合程度：26% 的受调者表示安全测试是独立执行的工作，42% 的受调者表示安全测试与开发流程已集成，但仍包含一定程度的人工实施，9% 的受调者表示已集成且完全自动化。

您所在组织软件应用生产过程中，所使用的应用安全检测工具有？



自动化安全测试工具应用：调查数据显示，已使用黑盒测试工具 DAST 的组织占 44%，使用白盒测试工具 SAST 的组织占比为 46%，采用软件成分分析工具 SCA 的组织占比为 36%，采用灰盒测试工具 IAST 的组织占比 28%，采用入侵与攻击模拟 BAS 的组织占 3%，除此之外，没有使用任何工具的组织占比 15%，19% 的受调者表示不清楚所在组织使用了哪些安全检测工具。通过数据分析，使用 DAST 和 SAST 工具的占比依旧很大，但使用 SCA 和 IAST 工具的比例逐渐增多，有的组织已经开始采用 BAS 工具进行安全检测。

以下哪一项更符合您所在团队的持续交付流水线现状？



受调者所在组织的持续交付流水现状：22% 受调者表示所在团队的构建、部署、测试已完成自动化但无流水线串联，21% 受调者表示交付过程仍然靠大量手工操作，31% 受调者表示所在团队已部署流水线可以自动构建、测试等环节，但与生产环境不通，流水线可以直通生产环境占比较少，为 5%。

小结

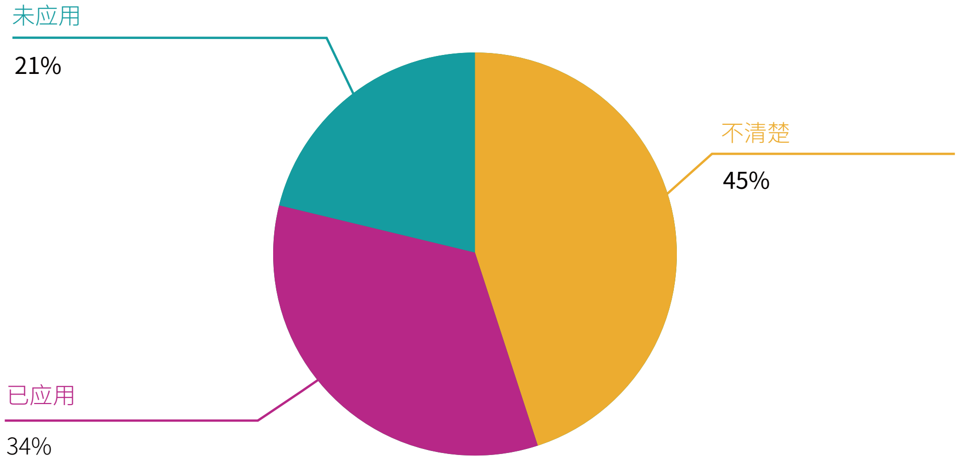
随着各企业组织的开发模式逐渐转变为敏捷开发模式或 DevOps 模式，若仍将安全活动游离在开发、运营流程之外，不仅仅影响应用开发效率还会造成巨大的成本损失。将安全提前介入，集成在软件开发的每一个阶段，实现“安全左移”，才能从根源上避免或减少安全风险。此外，应用程序中安全措施的加入仍然影响着软件应用生产的效率，持续交付是 DevOps 模式的核心要素之一，如何将安全低侵入、柔和地嵌入到流水线管道中，在自动化工具的支持下实现持续的、自动化的安全检查，让安全跟上快速持续交付的速度，是目前我们需要关注的重点问题之一。

大家说：

安全内嵌研发和业务不仅需要底层能力的完善，也需要匹配公司特定的研发流程和运营平台，避免钝化和低效。

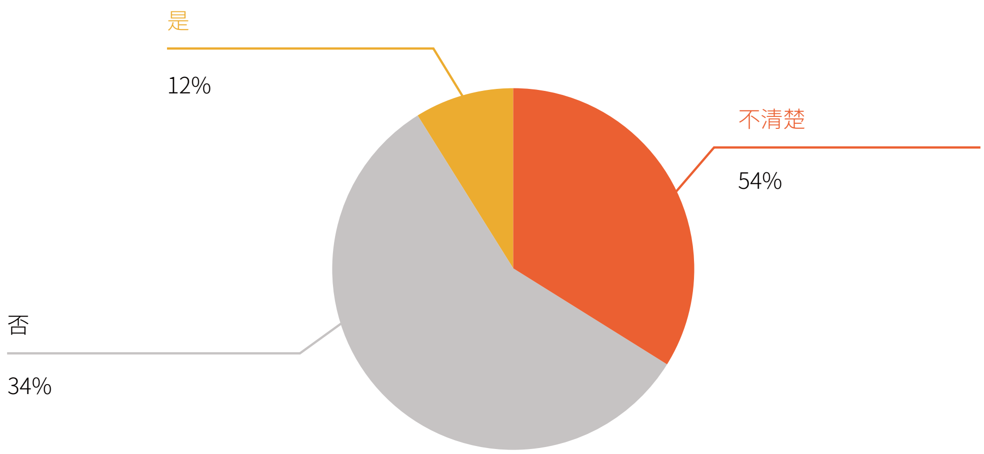
—— lazytricks 软件/互联网 上海

您所在组织是否应用了针对容器的安全解决方案?



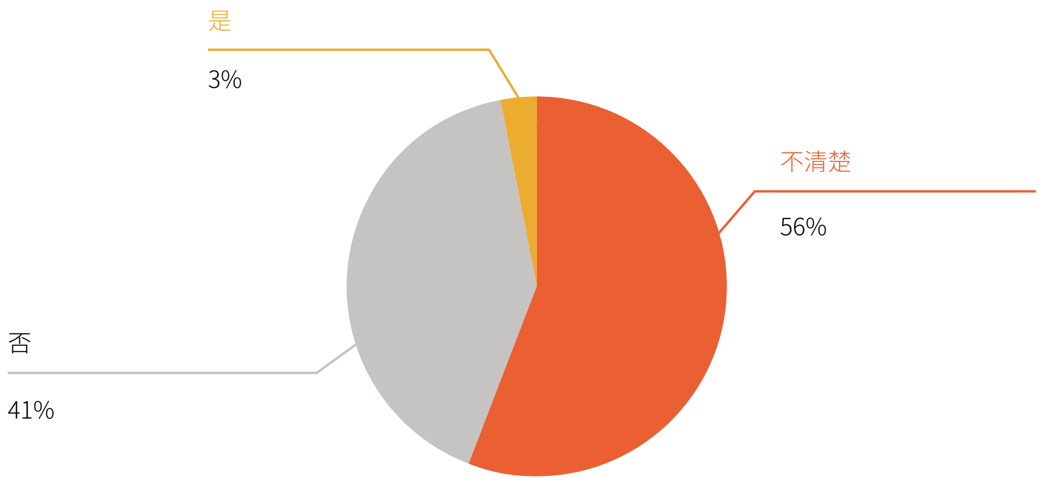
受调者所在组织对容器安全方案的使用：34% 的受调者表示所在组织已应用了容器安全解决方案，有 21% 的受调者表示所在组织并没有应用容器安全解决方案，同时 45% 的受调者表示并不清楚组织是否应用容器安全解决方案。

您所在的组织是否有建立内部的可信开源组件库?



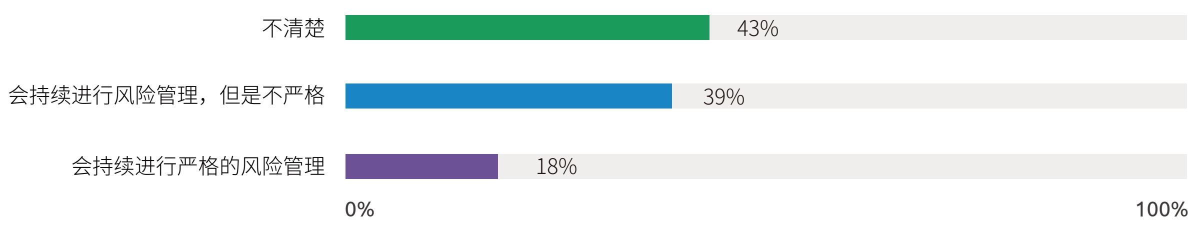
受调者所在组织建立内部的可信开源组件库的情况 ：12% 的受调者表示所在组织已建立内部可信的开源组件库，34% 的受调者表示所在组织没有建立内部可信的开源组件库，超一半受调者表示不清楚。

您所在组织是否为应用程序中使用的开源组件保留了完整的软件材料清单（SBOM）？



软件物料清单（SBOM）的完整性的保留情况：截止目前为止，仅有 3% 的受调者所在企业组织保留了完整的软件物料清单（SBOM），41% 的受调者所在企业组织未保留完整的 SBOM，56% 的受调者不清楚所在组织是否保留完整的 SBOM，SBOM 可以明确软件组件之间的依赖，确保软件供应链安全可追溯，所以完整的 SBOM 保留工作是必要的，现阶段仍处于初步阶段，尚有较大的增长空间。

您所在的组织是否会对软件供应商进行严格的风险管理?



受调者所在组织对软件供应商进行风险管理的情况：所有受调者中，39% 的受调者所在组织会持续进行风险管理，但并不严格，18% 的受调者所在组织会持续进行严格的风险管理，43% 的受调者不清楚该情况。

小结

随着软件产业的快速发展，软件供应链也越发复杂多元化，进而引入一系列的安全问题，近年来软件供应链攻击事件不断爆发，软件供应链安全已成为信息安全中的热门话题，其中开源软件的安全性问题以及软件供应商安全问题已成为软件供应链安全问题增长的重要因素，作为软件供应链的上游，更应该特别关注其安全问题，避免或减少安全问题从上游传递到下游环节导致爆炸式的传播。

大家说：

应该加强对开源软件风险的治理，最大限度的从软件供应链源头保障软件供应链的安全。

—— Miki 软件/互联网 北京

2

调查后记

与许多只关注开源、开发人员或较小组织的调查不同，本报告是基于对 IT、安全、开发和运营等 1639 名 DevSecOps 实践者或潜在实践者的调查。受调者来自不同体量的企业，涉及到多种行业领域。本次调查的目的是为了了解 DevOps 及 DevSecOps 在组织中的实践现状，分析 2022 年软件开发安全新的发展趋势。近年来 SolarWinds Orion 供应链攻击及 Log4j 2.x 开源组件漏洞爆发等事件都在彰显着软件供应链攻击带来的巨大破坏力，软件供应链安全已引起全球的高度重视，成为了近年来热门话题之一。因此相较于 2020 年 DevSecOps 行业洞察报告，本次调查对问题进行了全面优化，并增加了软件供应链安全现状这一新的调查模块。

从调查结果中可以看到，DevOps 依旧持续发挥着重要的流程支撑作用，企业组织的安全措施也正发力追赶，力求实现安全自动化，与 DevOps 更好地融合，从而使企业在持续开发、持续集成、持续发布的运作模式下仍能保持研发效能和应用安全，实现持续创新，进而在激烈的市场竞争中保持领先地位。

希望在今后的调查中，我们能看到 DevSecOps 体系的成熟化和实践的落地化，更多的企业组织能够通过 DevSecOps 帮助他们实现敏捷安全的目标，未来，我们相信一定会有更深层次的技术变革。

本报告在样本分布控制和问卷设置方面，难免存在不成熟之处，望读者见谅并指教。如有更多宝贵建议，欢迎通过邮箱 services@anpro-tech.com 反馈，期待能够得到更多真挚的意见。

洞见篇

洞见篇融合了行业安全专家及咨询师的思考和判断，旨在阐述 DevSecOps 在当下的发展态势，以及预测未来的发展趋势，帮助 DevSecOps 实践者梳理出前瞻性的实践思路。

1

DevSecOps 发展现状

DevOps 作为云原生时代下加速软件开发和部署的核心方法，打破了开发与运营之间的壁垒，引领了流程、文化和交付方式的转变。然而传统的应用程序安全措施无法应对动态复杂的云原生架构和快速的软件发布周期所带来的安全挑战，应用程序安全威胁格局的不断演变要求组织将安全集成到 DevOps 中，由此 DevSecOps 应运而生。从传统的瀑布开发模式演变成新型的软件开发模式的过程中，DevSecOps 是对具有孤立交付管道、充满瓶颈的安全流程的关键响应，是一种在不牺牲安全性的前提下，实现快速且规模交付的安全决策。

2012 年 Gartner 首次提出了 DevSecOps 的概念，即 DevSecOps 是糅合了开发、安全及运营理念以及创建解决方案的全新方法，并于 2016 年 9 月发布的《DevSecOps: How to Seamlessly Integrate Security Into DevOps》报告中首次对该模型及配套解决方案进行详细的分析，核心理念为：“安全是整个 IT 团队（包括开发、测试、运营及安全团队）所有成员的责任，需要贯穿整个业务生命周期的每一个环节”。2017 年美国 RSA（RSA Conference）大会还专门为这个概念和方向设置了议题和讨论会，RSA 大会是信息安全界最有影响力的业界盛会之一，发展到 2021 年，DevSecOps 已成为 RSA 大会上三大核心话题之一，足以见得 DevSecOps 的火热程度以及业界对它的逐渐重视程度。

随着敏捷开发模式的成熟和云原生迅猛发展，加大了业界对 DevSecOps 的需求。在此趋势下，DevSecOps 逐渐形成体系，敏捷安全工具链逐步升级完善，行业头部客户对新一代 DevSecOps 敏捷安全技术解决方案的认知度和接受度相对成熟，加速了 DevSecOps 深度落地实践的步伐。

1.1 DevSecOps 和软件供应链

2020 年人类社会到达虚拟化的临界点，为 2021 年成为元宇宙元年做了铺垫。但元宇宙并不是一种技术，而是一种理念和概念，元宇宙的世界不但涉及到互联网，区块链，物联网，云计算和移动终端产品，也涉及到社交、电商、游戏、信息、金融、AI、社会生活服务、甚至传统行业等各大互联网领域，可以说是目前所有既有的技术和既有的业务模式的有机融合体。在《2020-2021 中国元宇宙产业白皮书》的第一次研讨会中，与会专家、学者就相关技术、应用、政策的现状和未来发展趋势展开对话，并且一致认为，要以安全合规为前提发展元宇宙产业，积极推动我国相关技术发展和应用落地，助力我国产业转型升级。目前元宇宙还处于行业发展的初级阶段，如何把握机会在元宇宙赛道上迅速占领一席之地，保证软件安全是其中关键之一，而软件安全的本质则是开发安全。

从纵深防御和广度防御的角度出发，开发安全也是实现软件供应链安全的纵深防御策略。软件供应链安全可以被理解为软件生产的整个过程中软件设计与开发的各个阶段来自编码过程、工具、设备、供应商以及最终交付渠道所共同面临的安全问题。由此保障软件供应链安全需要从两方面出发：一、保障软件开发生命周期安全；二、保障软件供应链供应过程安全。随着互联网复杂性的增加，攻击者越来越多的转向程序本身已知的安全缺陷和漏洞，为避免软件自身的安全漏洞或缓解受污染的上游软件沿着软件供应链传递到下游造成的危害，就需要在软件开发各个阶段建立可靠的安全措施以改进软件开发的过程。

软件安全开发过程即在软件开发的各个阶段添加安全措施和安全手段，防止在软件开发过程中的缺陷而导致软件出现不该有的软件漏洞和脆弱性。随着现代软件开发需求等的多方面增长，构建一种软件一体化的安全开发方法至关重要。

软件安全开发涵盖了软件的整个生命周期，软件生命周期是从软件生产直到报废的整个过程，一般可以划分为 5 个主要阶段：设计阶段、编码阶段、测试阶段、发布阶段和运营阶段。基于软件生命周期的概念，衍生出软件安全开发生命周期（Secure Software Development Life Cycle，S-SDLC），即从规划到设计、开发、测试和部署阶段将安全性纳入软件开发生命周期的过程，遵循安全的软件开发生命周期标准，以最大限度地保障软件的安全性。

目前较为具有影响力的软件安全开发模型或体系有：微软提出的 SDL（Microsoft Security Development Lifecycle，软件安全开发生命周期）模型、Gartner 基于 DevOps 体系提出的 DevSecOps 框架、OWASP 的 CLASP（Comprehensive，Lightweight Application Security Process，综合的轻量级应用安全流程）方法以及 Gary McGraw 提出的 BSI 模型等。其中 DevSecOps 凭借倡导安全左移和内生安全，强调人人都应为安全负责，将安全嵌入到开发运营的每个阶段，形成一个安全闭环的理念脱颖而出。

DevSecOps 是一种全新的安全理念和模式，由 DevOps 的概念延伸和演变而来。从 RSAC 2017 年第一次设立 DevSecOps day 至今，DevSecOps 体系日趋成熟，相关方法论、技术与实践经验都有了明显的提升，配套工具链技术也日趋完善，但依旧处于摸索和发展阶段。Gartner 于 2019 年提出了一个较为全面的 DevSecOps 工

具链实践清单，如下图所示，Gartner 将 DevSecOps 生命周期分成了计划、创建、验证、预发布、发布、预防、检测、响应、预测和改进这 10 个环节，并且每个环节都具有相应的安全工具和安全活动。

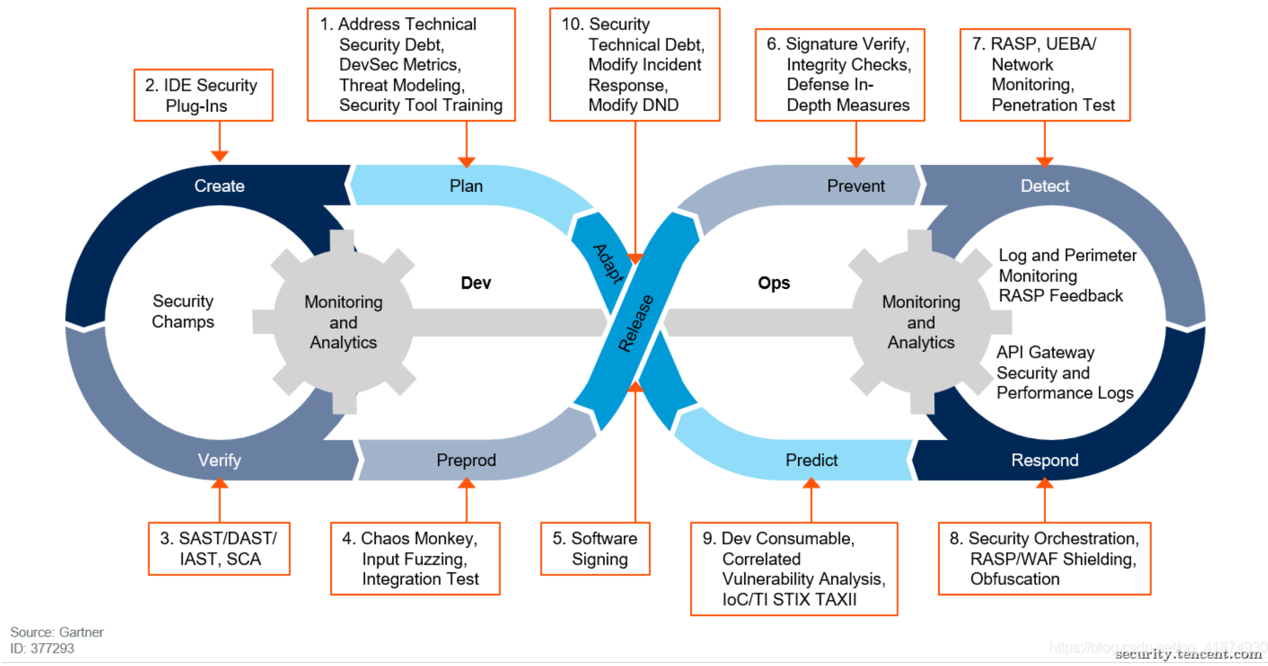


图 1-1 Gartner DevSecOps 工具链

总的来说，DevSecOps 是 DevOps 演进的必然结果，如何把安全无缝柔和地集成到敏捷和 DevOps 开发中，在既能保证高效的前提下保证软件的安全性，是 DevSecOps 重点关注的方向。

随着业内外对软件安全的重视程度越来越高，各种软件安全开发理论、实践和标准相继推出，同时，也形成了多个侧重于评估组织安全开发能力和保障能力的理论和标准，软件或软件系统安全成熟度模型，如：研发运营一体化（DevOps）能力成熟度模型、可信研发运营安全能力成熟度模型、BSIMM、OWASP DSOMM 等。

1、研发运营一体化（DevOps）能力成熟度模型

《研发运营一体化（DevOps）能力成熟度模型》是中国信息通信研究院牵头组织的全球首个 DevOps 标准。DevOps 标准体系旨在帮助组织：

（1）明确概念、框架、能力。DevOps 的概念、框架和能力到达什么程度，做一个非常详细明确的说明；

（2）对于 DevOps 涵盖的流程、组织、实施，有明确的指引，企业可以按照这个标准去提升自己 DevOps 各个环节的能力。

DevOps 标准评估体系主要包括敏捷开发管理、持续交付、技术运营、应用设计、安全及风险管理、系统和工具等部分，如下图所示。

一、研发运营一体化(DevOps)过程														
敏捷开发管理			持续交付							技术运营				
需求管理	计划管理	过程管理	配置管理	构建与持续集成	测试管理	部署与发布管理	环境管理	数据管理	度量与反馈	监控服务	数据服务	容量服务	连续性服务	运营反馈
需求收集	需求澄清和拆解	迭代管理	版本控制	构建实践	测试分级策略	部署与发布模式	环境供给方式	测试数据管理	度量指标	应用监控	数据收集能力	容量规划能力	高可用规划	业务知识管理
需求分析	故事与任务排期	迭代活动	版本可追踪性	持续集成	代码质量管理	持续部署流水线	环境一致性	数据变更管理	度量驱动改进	质量体系管理	数据处理能力	容量平台服务	质量体系管理	项目管理
需求与用例	计划变更	过程可视化及流动			测试自动化					事件响应及处置	数据告警能力	运营成本管理		业务连续性管理
需求验收		度量分析								监控平台				运营服务管理
二、研发运营一体化(DevOps)安全架构														
三、研发运营一体化(DevOps)安全管理														
四、研发运营一体化(DevOps)组织结构														

图 1-2 研发运营一体化（DevOps）能力成熟度模型

2021 年新增开放评估的部分为：第 6 部分安全及风险管理和第 8 部分系统和工具技术要求。截止目前已开放评估的部分分别为：第 3 部分持续交付、第 4 部分技术运营、第 6 部分安全及风险管理以及第 8 部分系统和工具技术要求。

2、可信研发运营安全能力成熟度模型

由中国信息通信研究院牵头编写制订的《可信研发运营安全能力成熟度模型》行业标准规定了面向云计算的可信研发运营安全能力成熟度模型参考框架，强调安全左移，关注需求、设计、研发安全，分为管理制度以及涉及软件应用服务全生命周期的要求阶段、安全需求分析阶段、设计阶段、研发阶段、验证阶段、发布阶段、运营阶段和下线阶段九大部分，每个部分提取了关键安全要素，规范了企业研发运营安全能力的成熟度水平，自低向高依次分为基础级、增强级和先进级。标准适用于企业在落地实践研发运营安全时进行参考与评价，也可为第三方机构对于企业的研发运营安全能力审查和评估提供标准依据，如下图所示。

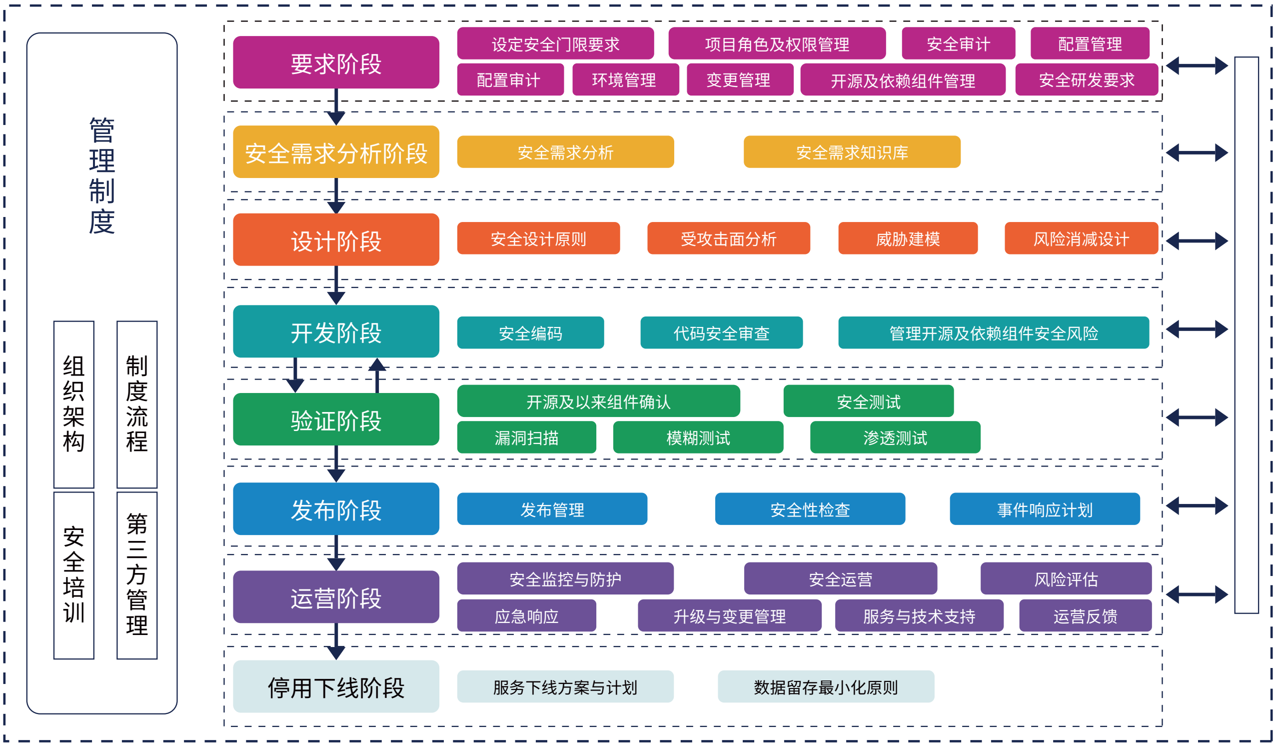


图 1-3 可信研发运营安全能力成熟度模型

信通院依据《可信研发运营安全能力成熟度模型》标准，于 2021 下半年开展了首批面向供应链研发运营安全能力试点评估。

3、BSIMM（BSI 成熟度模型）

BSIMM（Building Security In Maturity Model，软件安全构建成熟度模型）是一个基于软件安全框架（SSF），由十二个安全实践组成并针对多个软件公司的软件安全项目进行研究的模型，该模型对不同软件安全项目所采取的措施和实践进行量化，描述其共性和各自的特点。

BSIMM 研究始于 2008 年，出版了 BISMM 1，当时对来自软件厂商、技术公司和金融服务业界的 9 个顶尖软件安全项目进行了数据收集和分析，随着近年来的快速发展，BSIMM 已经逐渐覆盖了软件构建的整个过程。

2021 年新思科技发布了最新版本 BSIMM12，该模型评估了金融、金融科技、独立软件供应商、科技、物联网、云、零售等众多各类行业在内的 128 家企业，聚焦开源、云、容器及软件供应链安全问题，旨在帮助企业规划、执行、评估和完善其软件安全计划。BSIMM12 报告中提出了新的趋势：

区域			
管理	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及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。授按键配置、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 (AA) 11. 软件环境 (CR) 12. 配置管理和安全漏洞管理 (CMVM)

图 1-4 BSIMM12 的框架

4、OWASP DSOMM（DevSecOps 成熟度模型）

OWASP DSOMM（DevSecOps Maturity Model，DevSecOps 成熟度模型）显示了在使用 DevOps 策略时应用的安全措施以及如何确定这些策略的优先级，如图 1-5 所示。在 DevOps 策略的帮助下，还可以增强安全性。例如：可以测试 Docker 镜像中的应用程序库和操作系统库等每个组件是否存在已知漏洞。在具有前瞻性的 DevSecOps 成熟度模型的指导下，实施了适当的原则和措施帮组织降低安全风险。2021 年就 DevSecOps 成熟度模型召开了开放安全峰会 DSOMM 增强研讨会以及 DSOMM 项目的讨论会。

OWASP DSOMM 主要衡量以下四个方面：

1、静态深度：在 CI 管道中执行的静态代码扫描的全面程度；
2、动态深度：在 CI 管道中运行的动态扫描的全面程度；
3、强度：在 CI 管道中运行的安全扫描的计划频率；
4、整合：用于处理发现和流程完整性的补救工作流程。

此外，DSOMM 模型定义了 DevSecOps 类型的 5 个主要维度，细分成 17 个子维度，以及 4 个不同深度的成熟度级别，如图 1 所示。针对每个维度的不同成熟度级别相对应的活动，DSOMM 也相应的做了解释，包括风险、优点以及此活动的有用性和要求。

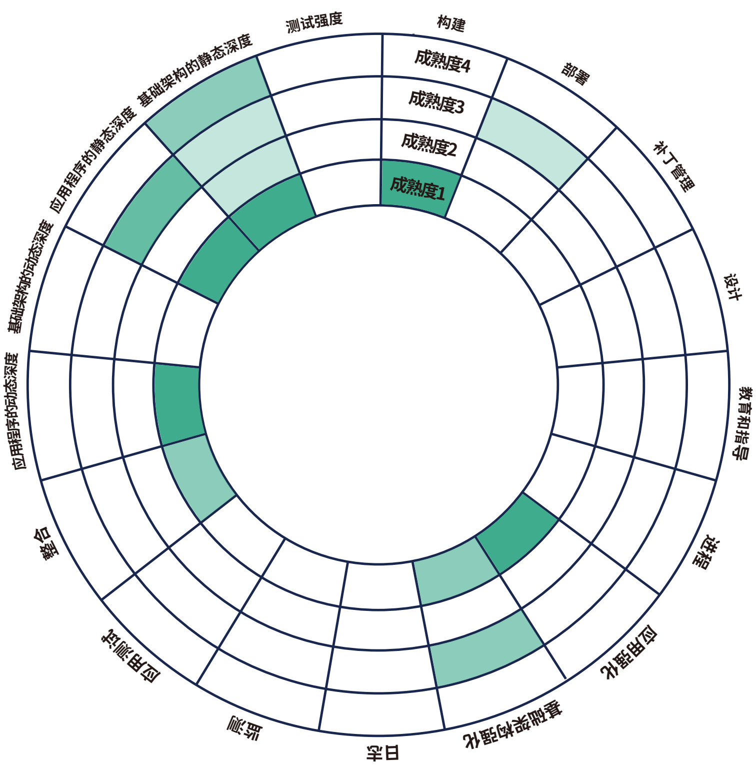


图 1-5 DSOMM 模型

各软件安全成熟度模型的特点：

软件安全成熟度模型的建立和监管实际上可以帮助组织理解安全开发活动的关键要素，从而帮助组织了解当前自身开发安全现状，并且根据软件安全成熟度模型选择适合自身企业的安全活动或措施，制定相应的解决方案，进而使组织的安全开发流程逐渐成熟。

从这些模型包含的内容看，它们之间既有很多相同的特点，也有很多差异，这几种模型各自的特点可以概括如下:

1、研发运营一体化（DevOps）能力成熟度模型

该成熟度模型不同于其他的软件安全方法论或标准，是一套端到端的覆盖软件交付生命周期全流程的方法论、实践和标准的集合，是一套具有体系化的成熟度模型。在一定程度上，为采用 DevOps 开发模式的企业带来了 IT 效能的明显提升，并且能够将应用的需求、开发、测试、部署和运营集合与统一起来，帮助基于整个组织的协作和应用架构的优化，从而实现从敏捷开发到持续交付到应用运营的无缝衔接与集成，在保证软件应用程序稳定运行的同时，能够快速交付高质量的软件及服务，灵活应对快速变化的业务需求和市场环境。

2、可信研发运营安全能力成熟度模型

可信研发运营安全能力成熟度模型具有四大特点：（1）覆盖范围更广，强调安全左移和安全右移延伸至停用下线阶段，覆盖软件应用服务从需求到下线的全生命周期；（2）更具普适性，抽取关键安全要素，不依托于任何开发模式与体系；（3）不止强调安全工具，同样注重安全管理，强化人员安全能力；（4）进行运营安全数据反馈，形成安全闭环，不断优化研发运营流程实践。

该成熟度模型适用于企业在落地实践研发运营安全体系时进行参考与评价，也可为第三方机构对于企业的研发运营安全能力审查和评估提供标准依据。

3、BSIMM12

BSIMM12 收集了很多软件企业在软件安全开发方面的措施和方法，并按照软件安全开发 框架进行描述，找出这些软件企业的共同点和不同点，从而给其他企业提供实践参考。因此，尽管 BSIMM12 本身不提出任何建议，软件企业还是可以根据 BSIMM12 的数据了解常用的软件安全开发措施，同时可以用来和自己的开发方法进行比较。

4、DSOMM

DSOMM 是基于自建的安全框架进行成熟度模型的构造，可扩展性较强，同时作为 OWASP 项目之一的 SAMM 适用于软件安全开发的整个生命周期，包括开发、运营、安全过程，而 DSOMM 适用于 DevSecOps 理念下的软件开发过程，因此，具有 DevOps 开发模式的组织可以将 SAMM 和 DSOMM 模型结合起来，以更好的进行组织自身的改善或提升。

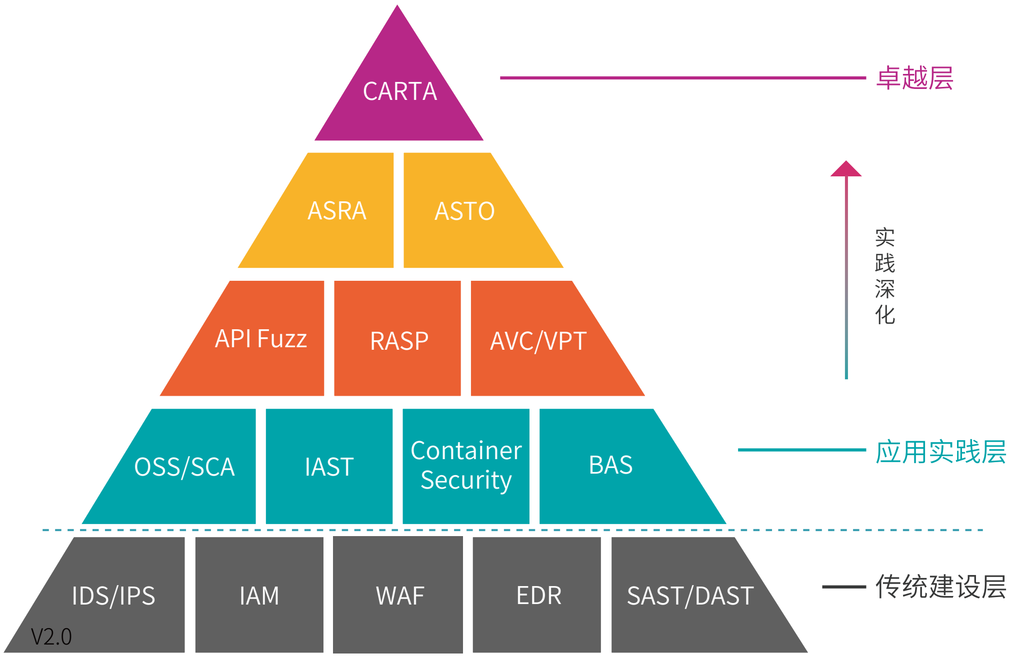


图 1-6 DevSecOps 敏捷安全工具金字塔 2.0

在《2020 DevSecOps 行业洞察报告》中，DevSecOps 敏捷安全技术金字塔被首次提出，随着 DevSecOps 实践的不断发展，目前已迭代至 2.0 版本。该版本的金字塔延续了 1.0 版本的编排原则，即安全工具分层与组织的 DevSecOps 成熟度非正比关系，主要依据该工具的普适性、侵入性、易用性等参考因素。

随着 DevSecOps 实践的不断发展，DevSecOps 敏捷安全技术金字塔 2.0 版本在 1.0 版本的基础上，安全工具进行了部分调整和更新。新增了部分具有创新性且产品成熟度和市场需求度较高的安全工具，删除了部分被边缘化的安全工具，同时调整了部分安全工具的评价。

卓越层

CARTA（持续自适应风险与信任评估）平台

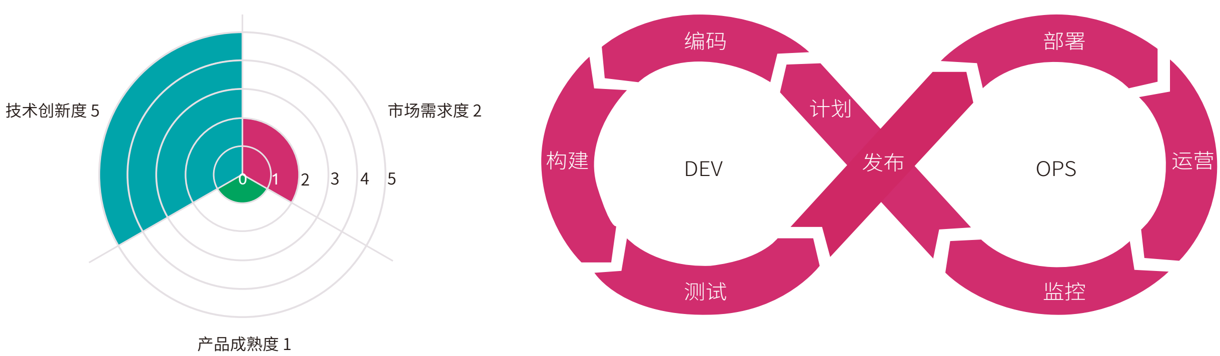


图 1-7 CARTA 调研分析及适用环节

CARTA（Continuous Adaptive Risk and Trust Assessment，持续自适应风险与信任评估）是 Gartner 主推的一种应对当前及未来安全趋势的先进战略方法，该架构促进了一种持续适应不断变化安全形势的方案，而不是试图阻止任何一方或允许特定的交互。作为自适应安全方法，CARTA 可以帮助组织克服应用团队和安全团队之间的障碍，为企业提供风险管理能力。

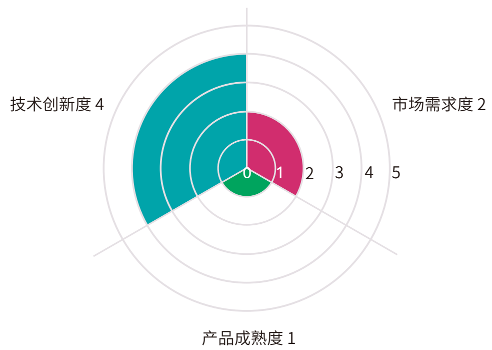
在 CARTA 方法中，决策和安全响应是基于对风险和信任的评估分析，这个评估分析的过程就是一个权衡的过程，拒绝传统允许 / 阻断二进制评估的方式，当信任和风险处于动态时，它会持续评估并通过具有不同风险和响应属性的细粒度度量方式进行管理。CARTA 战略是一个庞大的体系，包括大数据、AI、机器学习、自动化、行为分析、威胁检测、安全防护、安全评估等方面，集主流技术与一体打造出一个自适应自判断安全防护平台。

作为 CARTA 方法的一部分：组织必须克服安全团队和应用团队之间的障碍，安全团队必须将多个点的安全测试集成到 DevOps 工作流程中，这种方式对开发人员很大程序上是透明的，并在 DevOps 和敏捷开发环境的团队合作、敏捷性和速度，提供“DevSecOps”。应用程序的安全性将在开发阶段的早期开始，团队可以将识别组织面临的并在发布应用程序之前消除它们，通过这种方法，开发团队将平衡安全需求和速度需求。

根据调研 CARTA 在 DevSecOps 中的实际应用情况发现其技术创新度、市场需求度和产品成熟度均暂无明显变化，因此 CARTA 的各评级保持不变。

实践深化层

ASRA（自动化安全风险评估）



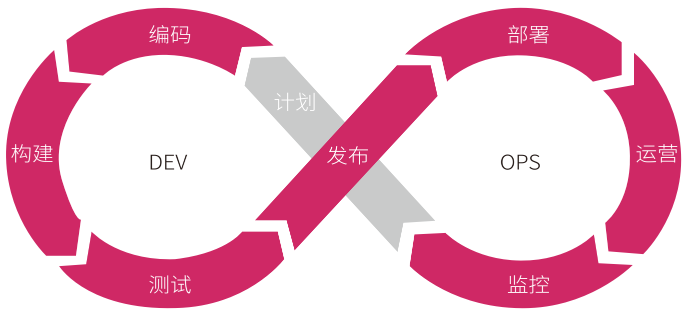


图 1-8 ASRA 调研分析及适用环节

ASRA（Automated Security Risk Assessment，自动化安全风险评估）对于帮助组织理解威胁情报数据、动态更新策略和在系统内实现持续合规性至关重要。通过使用自动化风险评估，可以根据组织的安全性和合规性策略识别安全缺陷并确定其优先级。

ASRA 是全面且自动化的自上而下、自下而上、优先排序和量化的网络安全风险评估。其可以从根本上改变风险管理，除了大幅降低运营成本之外，还可以为风险管理提供新功能，包括将风险控制直接构建到流程中、确定测试和监控领域的优先级、部署具有自定义升级的自动监控、实时解决问题以降低企业面临的安全风险。

虽然 ARSA 拥有较高的技术创新性，但根据其在 DevSecOps 中实际的应用情况及针对市场和产品的调研，最终确定其技术创新度为 4、市场需求度为 2、产品成熟度为 1。

ASTO（应用安全测试自动化编排）

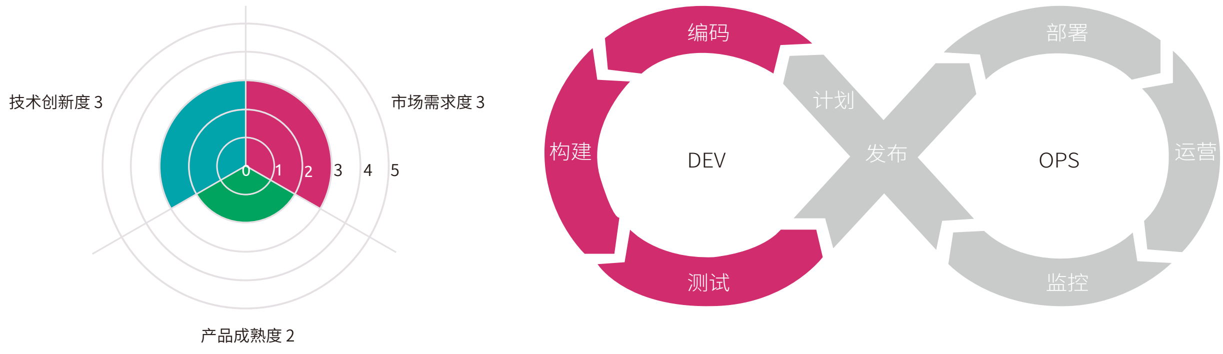


图 1-9 ASTO 调研分析及适用环节

ASTO（Application Security Testing Orchestration，应用安全测试自动化编排）是由 Gartner 在 2017 年首次推出的一款工具。ASTO 的目标是在生态系统中的所有安全测试工具建立一个集中、协调的管理和报告系统。实施自动化和持续的 ASTO 可以帮助组织轻松协调和管理 IAST/SAST/SCA/DAST 等各种安全测试工具，结合从各种安全测试工具收集的相关数据和警报信息，以提高准确和全面的信息和洞察力，并利用它们以最有效和最高效的方式解决安全威胁。

ASTO 在整个软件开发生命周期中集成了安全测试工具，是 DevSecOps 计划中的重要一环。ASTO 通过弥合从检测到补救的差距来提高安全性，由于安全测试工具在开发过程的早期实施，ASTO 可以帮助简化漏洞管理，自动实施策略，帮助开发和安全团队尽早确定和修复安全漏洞。

ASTO 作为实现 DevSecOps 落地实践的重要推动因素，根据调研 ASTO 在行业的实际应用情况，发现其技术创新度和市场需求度并无明显变化，但产品成熟度有显著提升，因此将其提升至 2。

API Fuzz（模糊测试）

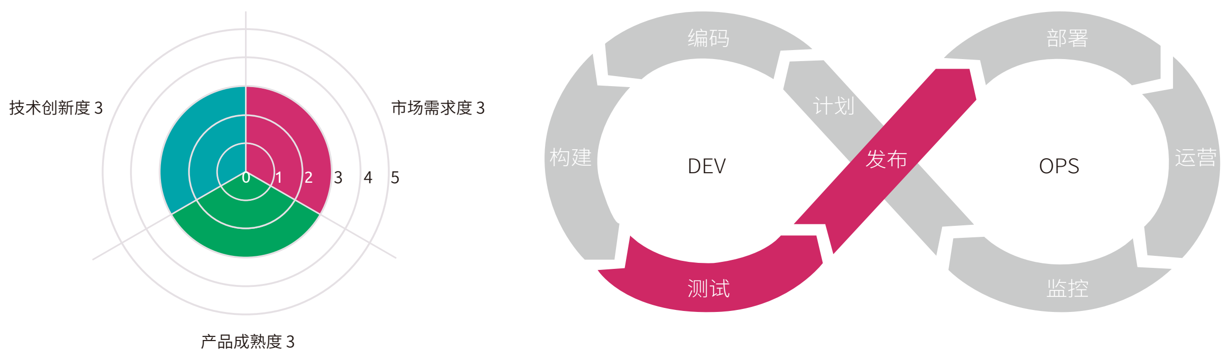


图 1-10 API Fuzz 调研分析及适用环节

API Fuzz（Fuzz Testing，模糊测试）是一种自动化软件测试技术，它试图通过将无效和意外的输入和数据随机输入计算机程序来寻找可破解的软件错误，以发现编码错误和安全漏洞。正确执行的模糊测试技术可以提供一种低成本、高效的发现漏洞的方法，比手动分析在短时间内可以执行的覆盖更多的代码路径和值迭代。

模糊测试通常涉及向被测试的软件或系统输入大量随机数据，以试图使其崩溃或突破其防护。模糊测试可以揭示在编写或调试软件时被忽视的严重缺陷，也可以发现被 SQL 注入、缓冲区溢出、拒绝服务和跨站点脚本利用的漏洞。

根据调研 API Fuzz 在 DevSecOps 中的实际应用情况，发现其市场需求度和产品成熟度并没有发现明显变化，因此其各评级保持不变。

RASP（运行时应用自我保护）

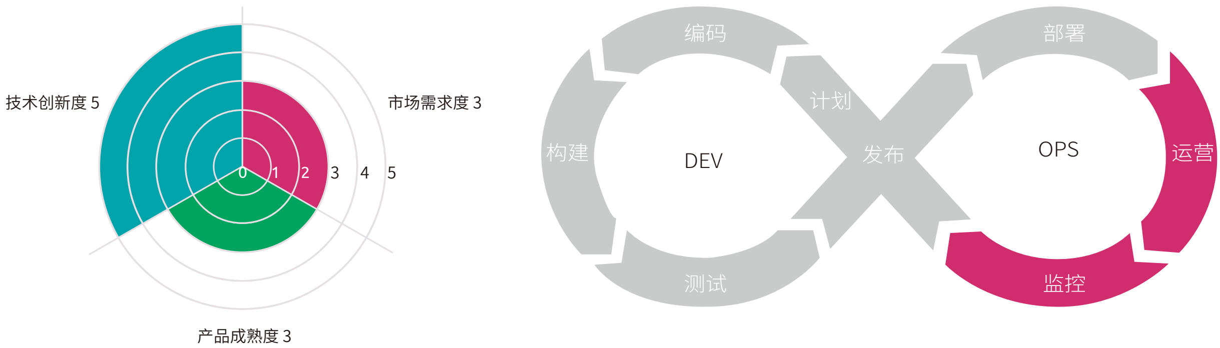


图 1-11 RASP 调研分析及适用环节

RASP（Runtime Application Self-protection，运行时应用自我保护）是由 Gartner 在 2012 年提出的一种新型安全技术。RASP 技术内置于应用程序或应用程序运行环境中，能够控制应用程序执行、检测漏洞并防止实时攻击。RASP 将安全性整合到运行的应用程序中，能够立即检测、阻止和缓解攻击，通过分析应用程序行为和上下文来保护实时运行的应用程序。通过使用该应用程序持续监控其自身行为，RASP 能够保护应用程序免遭数据窃取。

RASP 是应用程序安全生态系统中的一项创新，可通过提供对隐蔽漏洞的更多可见性来应对对软件应用程序层的运行时攻击。它本质上是一种与应用程序或其运行时环境集成的安全软件，并不断拦截对应用程序的调用以检查其安全性。

RASP 可以提供更深入的保护能力，更广泛的覆盖范围，并且可以花费企业更少的时间。因此，根据调研 RASP 在 DevSecOps 中的实际应用情况，其技术创新度并无明显变化，但市场需求度和产品成熟度均存在明显的提升，因此市场需求度由原来的 2 升至 3，产品成熟度由原来的 2 升至 3。

AVC/VPT（应用程序漏洞关联）

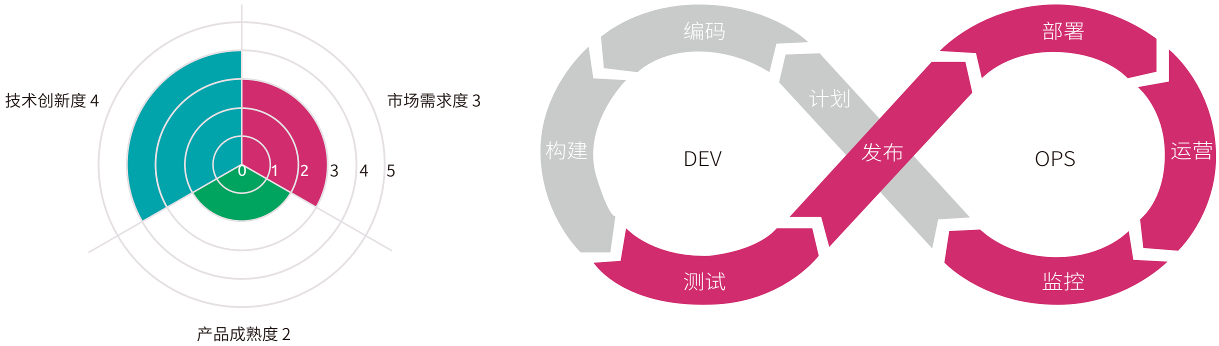


图 1-12 AVC/VPT 调研分析及适用环节

AVC（Application Vulnerability Correlation，应用程序漏洞关联）是由 Gartner 在 2017 年应用安全创新炒作周期中首次提出。AVC 代表应用程序安全工作流和流程管理工具，旨在通过将来自各种安全测试数据源的结构整合到一个集中工具中来简化软件开发生命周期应用程序漏洞的修复。不同的测试工具对它们识别的漏洞的风险评级往往不同，AVC 工具结合这些不同的风险评分，并根据行业标准对它们进行评级。

AVC 通过完全自动化测试工具、集中应用程序安全功能和修复安全缺陷的许多开发团队之间的流程来加速修复易受攻击的应用程序。AVC 和 DevOps 的结合可以使开发人员能够专注于最关键漏洞，同时仍然保持项目所需的速度和创新。随着 DevOps、CI 和 CD 等方法的日益普及，这种工作流自动化变得更加重要。

VPT（Vulnerability prioritization technology，漏洞优先级技术）是在 Gartner 2019 年发布的《漏洞评估市场指南“Market Guide for Vulnerability Assessment”（2019）》报告中提出，主要为了增强在整个漏洞管理上的风险定义和处置优先级，在之后的《漏洞评估市场指南“Market guide for vulnerability assessment”（2021）》被进一步强化，同时在《安全运营技术成熟度模型“Hype Cycle for Security Operations”（2021）》中，Gartner 将 VPT 定义为最具期待性的巅峰技术之一，将在 2-5 年中进入成熟期。

根据 Gartner 对 AVC/VPT 的创新度评价及其在 DevSecOps 中实际的应用情况及针对市场和产品的调研，最终确定其技术创新度为 4、市场需求度为 3、产品成熟度为 2。

应用实践层

OSS/SCA（开源软件 / 软件成分分析）

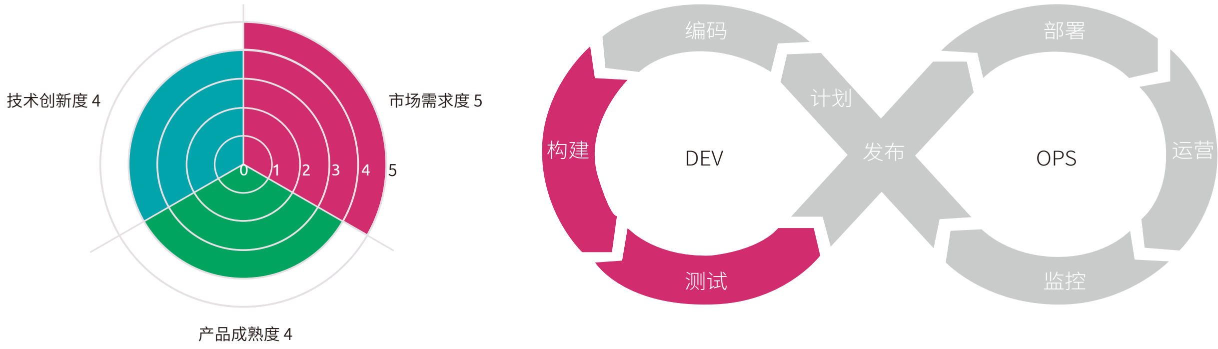


图 1-13 OSS/SCA 调研分析及适用环节

SCA 工具在查找通用和流行的库和组件（尤其是开放源代码）方面最为有效，它们的工作原理是将代码中的已 SCA（Software Composition Analysis，软件成分分析）不仅可以识别第三方组件的开源安全风险和漏洞，还可以提供每个组件的许可和漏洞信息，更先进的工具能够自动化开源选择、批准和跟踪的整个过程，为开发人员节省宝贵的时间并显著提高他们的准确性。

SCA 工具在查找通用和流行的库和组件（尤其是开放源代码）方面最为有效，它们的工作原理是将代码中的已知模块与已知漏洞库进行比较。SCA 工具查找具有已知漏洞并已记录漏洞的组件，并且通常会提示使用者组件是否过时或有可用的补丁修补程序。

SCA 工具生产 SBOM（Software Bill of Materia，软件物料清单），其中包括已识别的源代码，然后针对包括 NVD 在内的多个数据库进行检查。通过将 SBOM 与其他数据库进行比较，可以快速识别和修复任何关键的安全或法律问题。

根据调研 SCA 在 DevSecOps 中的实际应用情况以及 OSS 开源治理成为行业持续关注的新热点，因此 SCA 的市场需求度从 3 增长至 5、产品成熟度从 3 增长至 4。

IAST（交互式应用安全测试）

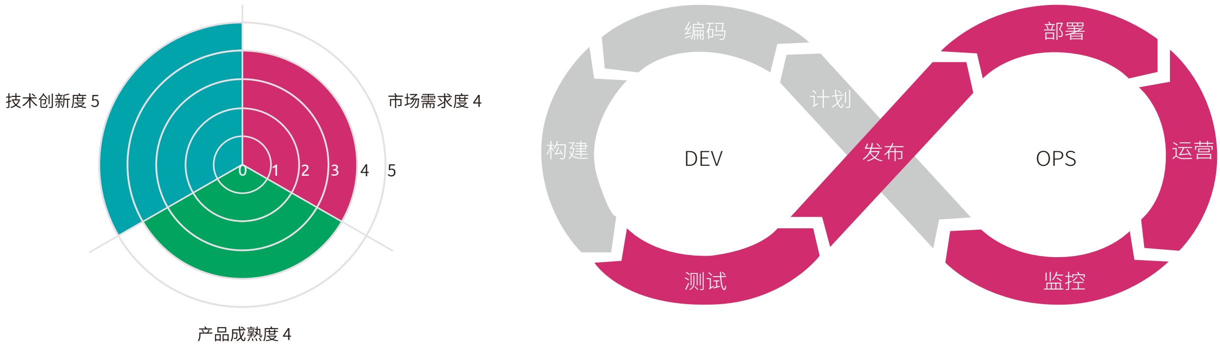


图 1-14 IAST 调研分析及适用环节

IAST（Interactive application security testing，交互式应用安全测试）曾被 Gartner 多次列为十大安全技术，IAST 工具结合了 SAST 和 DAST 技术的优点，可以模拟验证代码中的已知漏洞是否可以真的在运行的环境中被利用。

IAST 工具利用对应用程序流和数据流的了解来创建高级攻击方案，并递归地使用动态分析结果：在执行动态扫描时，该工具将基于应用程序对测试用例的响应方式来了解有关应用程序的知识。一些工具将使用这些知识来创建其他测试用例，然后可以为更多的测试用例产生更多的知识。以此类推，IAST 工具擅长于减少误报数，并且可以很完美地使用在敏捷和 DevOps 环境。在这些环境中，传统的独立 DAST 和 SAST 工具在开发周期中可能会占用大量时间，而 IAST 几乎不会对原有应用生产效率产生任何影响。

根据调研 IAST 在 DevSecOps 中的实际应用情况以及 IAST 持续保持高速发展，因此 IAST 的市场需求度从 3 增长至 4、产品成熟度从 3 增长至 4。

Container Security（容器安全）

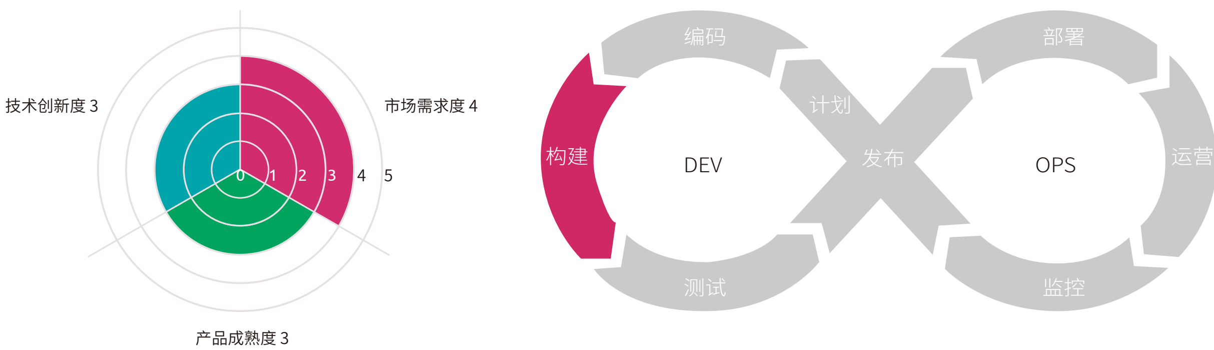


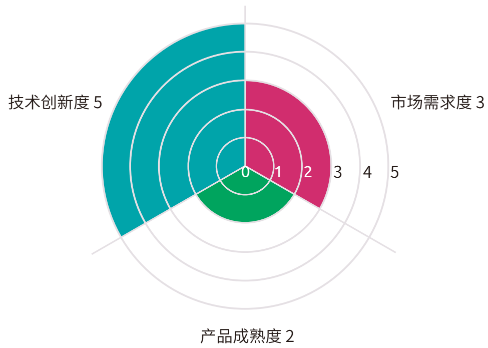
图 1-15 Container Security 调研分析及适用环节

Container Security（容器安全）是一个专注于保护容器化应用程序的各个方面免受潜在风险的领域。容器安全管理整个环境中的风险，包括软件供应链或 CI/CD 管道、基础设施和运行时免受网络安全风险。

容器安全工具可以保护云原生环境免受漏洞和主动攻击威胁，容器安全工具可以完全集成到构建和部署管道中，提供针对容器镜像的漏洞管理功能，实现并强制实施合规性，自动化以消除手动接触点的数量，并扩展到底层基础架构的维护和操作中。这意味着保护组织的构建管道映像和运行时主机、平台和应用程序层。将安全性作为持续交付生命周期的一部分实施意味着您的企业将在不断增长的攻击面中降低风险并减少漏洞。

根据调研容器安全在 DevSecOps 中的实际应用情况以及市场需求度和产品成熟度，将其调整至应用实践层，同时市场需求度从 3 增长至 2，产品成熟度从 2 增长至 3。

BAS（入侵与攻击模拟）



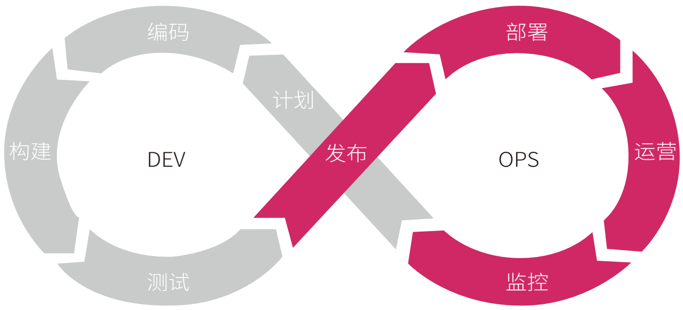


图 1-16 BAS 调研分析及适用环节

BAS（Breach and Attack Simulation，入侵与攻击模拟）在 Gartner2017 年发布的《面向威胁技术的成熟度曲线》中首次提及，并将其归到新兴技术行列。同时，在 2021 年，Gartner 将其纳入“2021 年顶级安全和风险管理趋势”。

BAS 通过模拟对端点的恶意软件攻击、数据泄露和复杂的 APT 攻击，测试组织的网络安全基础设施是否安全可靠，在执行结束时，系统将生成关于组织安全风险的详细报告，并提供相关解决方案。同时结合红队和蓝队的技术使其实现自动化和持续化，实时洞察组织的安全态势。

根据 Gartner 对 BAS 的创新度评价及其在 DevSecOps 中实际的应用情况及针对市场和产品的调研，最终确定其技术创新度为 5、市场需求度为 3、产品成熟度为 2。

传统建设层

IDS/IPS（入侵检测系统 / 入侵防御系统）

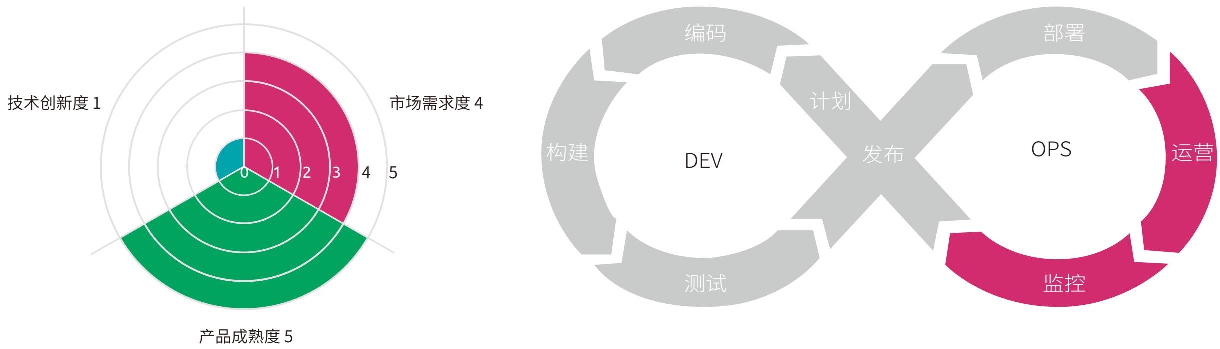


图 1-17 IDS/IPS 调研分析及适用环节

IDS（Instruction Detection System，入侵检测系统）、IPS（Instruction Prevention System，入侵防御系统）是两类传统的安全保障产品，主要用于应对网络安全系统中的黑客攻击事件。

IDS 是依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。

IPS 能够监视网络或网络设备的网络资料传输行为，能够即时的中断、调整或隔离一些不正常或是具有伤害性的网络行为。

由于这两种产品的技术和形态有高度的一致性，因此这里放到同一个分类中阐述。IPS 和 IDS 工具已经非常成熟，甚至可以成为古老。但由于其拥有实时检测和响应的特点，在生产系统中有着高度的实用性，因此现如今依旧是在线应用的网络保护中十分必要的一环。

根据调研 ISD/IPS 在 DevSecOps 中的实际应用情况，发现其市场需求度和产品成熟度并没有发现明显变化，因此其各评级保持不变。

IAM（身份识别与访问管理）

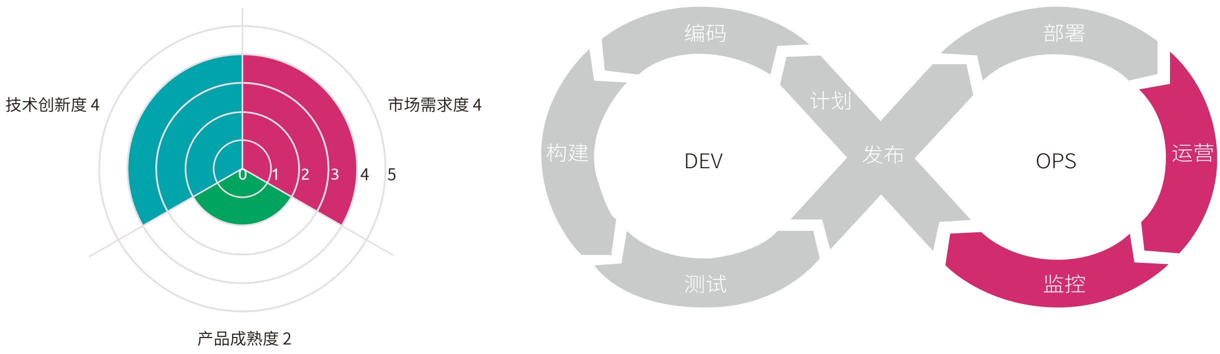


图 1-18 IAM 调研分析及适用环节

IAM（Identity and Access Management，身份识别与访问管理）是一个业务流程、政策和技术框架，可促进电子或数字身份的管理。IAM 具有不断增加的功能列表，包括生物识别、行为分析和人工智能，非常适合新安全环节的严格要求。

IAM 解决了确保在日益复杂的技术环境中适当访问资源并满足日益严格的合规性要求的关键任务需求。IAM 系统可以通过工具来实施全面的安全、审计和访问策略来加强监管合规性。成熟的 IAM 工具可以帮助企业降低身份管理成本，更重要的是，在支持新业务计划方面变得更加敏捷。

IAM 的市场不断增加可归因于数据暴露、数据泄露、数据丢失、内部攻击和不安全的使用。跨组织快速采用新兴技术包括基于云的服务、物联网和自带设备推动了网络攻击的增加。因此，提高安全有效性、提高运营效率和遏制内部威胁的必要性是显而易见的。

根据 IAM 在 DevSecOps 中的实际应用情况及针对市场和产品的调研，最终确定其技术创新度为 4、市场需求度为 4、产品成熟度为 2。

WAF（Web 应用防火墙）

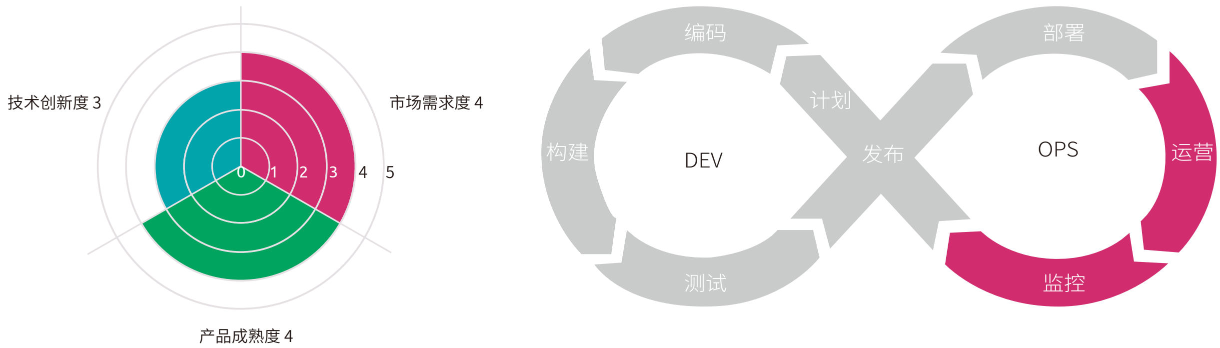


图 1-19 WAF 调研分析及适用环节

WAF（Web Application Firewall，Web 应用防火墙），是通过执行一系列针对 HTTP 和 HTTPS 的安全策略，可以对来自 Web 应用程序客户端的各类请求进行内容检测和验证，确保其安全性和合法性，对非法的请求予以实时阻断，从而对各类网站站点进行有效的安全防护。

WAF 通过增强输入验证，可以在运营阶段有效防止网页篡改、信息泄露、木马植入等恶意网络入侵行为，从而减小 Web 服务器被攻击的可能性。同时，WAF 还可以判断用户是否是第一次访问，将请求重定向到默认登录界面并记录时间，通过检测用户的整个操作行为识别攻击。

根据调研 WAF 在 DevSecOps 中的实际应用情况，发现其市场需求度和产品成熟度并没有发现明显变化，因此其各评级保持不变。

EDR（端点检测与响应）

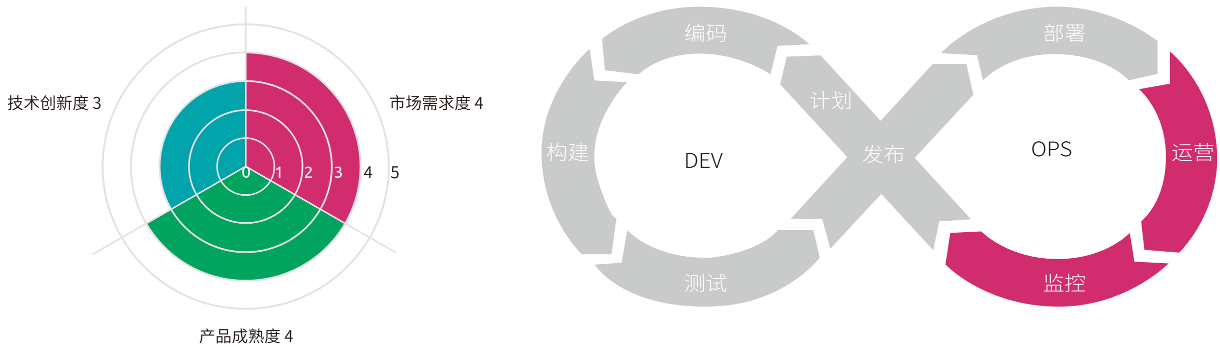


图 1-20 EDR 调研分析及适用环节

EDR（Endpoint Detection & Response，端点检测与响应）是一种集成的端点安全解决方案，将实时连续监控和端点数据的收集与基于规则的自动响应和分析功能相结合。通过使用分析工具促进了持续的检测和检测。这些工具通过识别、响应和转移内部威胁和外部攻击来确定可以改善公司整个安全状态的任务。

EDR 通过监控端点和网络时间并将信息记录在中央数据库中进行工作，在中央数据库中进行进一步的分析、检测、调查、报告和警报。安装在主机系统上的软件代理为事件监控和报告提供了基础。

Gartner 将 EDR 定义为“记录和存储端点系统级行为，使用各种数据分析技术检测可疑系统行为，提供上下文信息，阻止恶意活动，并提供修复建议以修复受影响的系统”的解决方案。

根据调研 EDR 在 DevSecOps 中的实际应用情况发现其市场需求度和产品成熟度，将其调整至应用实践层，同时其市场需求度和产品成熟度并无明显变化，因此其各评级保持不变。

SAST（静态应用程序安全测试）

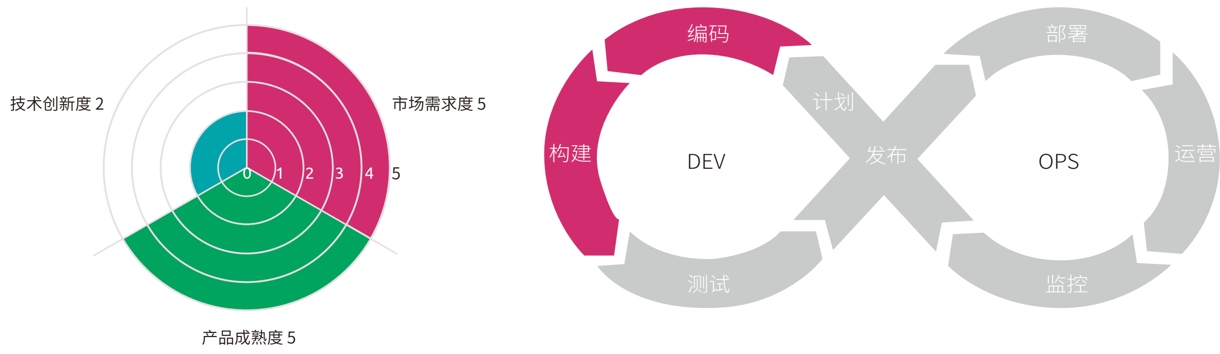


图 1-21 SAST 调研分析及适用环节

SAST（Static Appliaction Security Testing，静态应用程序安全测试）又称为白盒测试，是一种常用的应用程序安全工具，用于扫描应用程序的源代码、二进制代码或直接代码。SAST 工具可以识别漏洞的根本原因并帮助修复潜在的安全漏洞，可以“由内而外”分析应用程序，并且不依赖正在运行的系统来执行扫描。

SAST 可以直接集成到开发环境中，允许开发人员持续监控他们的代码并在发现漏洞时快速缓解。由于 SAST 安全工具在开发人员编写代码时为他们提供实时反馈，因此他们可以在问题进行 SDLC 的下一阶段之前修复问题，从而比在 SDLC 后期更快地检测和修复问题。

根据调研 SAST 在 DevSecOps 中的实际应用情况，发现其市场需求度和产品成熟度并没有发现明显变化，因此其各评级保持不变。

DAST（动态应用安全测试）

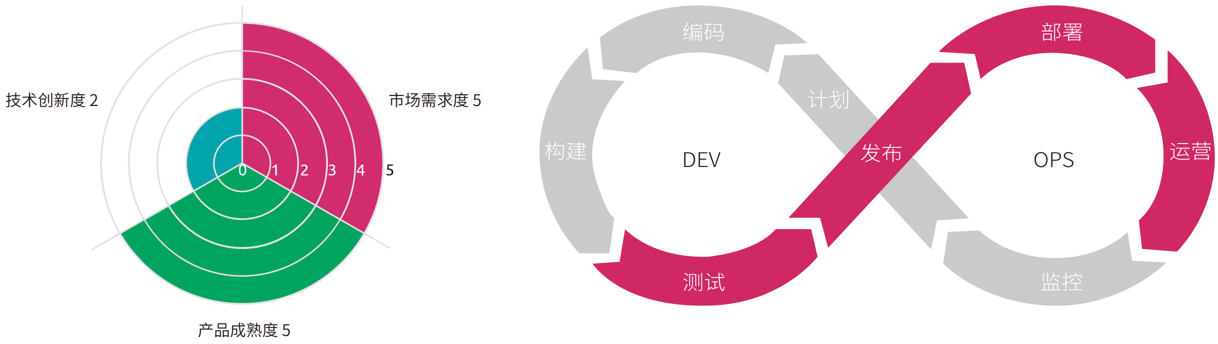


图 1-22 DAST 调研分析及适用环节

DAST（Dynamic Application Security Testing，动态应用安全测试）又称为黑盒测试，是一种漏洞评估工具，用于查找生产中的应用程序漏洞。测试人员无需具备编程能力，无需了解应用程序的内部逻辑结构，也无须了解代码细节。DAST 不区分测试对象的实现语言，采用攻击特征库来做漏洞发现与验证。

DAST 工具针对编译后的可执行程序运行，以检测界面、请求、响应、脚本（即 JavaScript）、数据注入、会话、身份验证等问题。除了可以扫描应用程序本身之外，还可以扫描发现第三方开源组件、第三方框架的漏洞。

根据调研 DAST 在 DevSecOps 中的实际应用情况，发现其市场需求度和产品成熟度并没有发现明显变化，因此其各评级保持不变。

DevSecOps 敏捷安全技术金字塔的不断升级，是为了给业界更好的预测和思考。关于 DevSecOps 敏捷安全技术未来演进方向的预测是开放且持续性的，随着 DevSecOps 实践的不断发展，我们会持续关注 DevSecOps 中安全工具的实际应用情况，并进行不断调整和更新。

1.4 不同行业的 DevSecOps 现状

由于不同行业的安全开发需求不同以及自动化工具使用意愿不同，所以尽管 DevSecOps 的实践广泛适用于各个行业，但不同行业的 DevSecOps 实践成熟度也存在明显差异。

本文选取了三大具有代表性的行业，分析其 DevSecOps 落地实践现状，简要描述其面临的风险和挑战，以及在此背景下构建的 DevSecOps 实践案例。需要说明的是，这里选取的案例并非一定最领先的行业实践，其实践方案是否适合行业参考借鉴是我们的重要选择标准，同时也考虑了其代表性。与之相似的是，我们给出的时间成熟度评价，更倾向于体现行业的中等水平，而非最高水平。

1.4.1 某大型通信运营商 DevSecOps 现状

面临的风险与挑战：某大型通信运营商不断向敏捷及 DevOps 转型，现阶段已初步建立 DevOps 体系。虽然 DevOps 极大的提升了软件的交付速度，实现了 5G 时代下的多网融合，多设备连接以及多业务并发，但也给软件安全性及可靠性带来了极大的挑战。为了弥补 DevOps 流程中安全性缺失的问题，该运营商开始着手进行开发流程的 DevSecOps 建设。

该运营商在互联网业务模式下要求信息系统敏捷开发、快速迭代，云道平台是其 DevOps 理念落地产品化平台，如下图所示，实现了软件从传统线下瀑布式模式到敏捷开发运营一体化的数字化转型，但是由于迭代频率要求较高，该平台依旧面临着安全方面的挑战。以往的安全工作仅在上线前进行安全防护或开展上线后的安全运营工作，已逐渐无法满足和适应新形势下的各种安全威胁。不仅如此，随着网络安全态势的发展，监管部门出台了更加严格和专业的各类监管文件，该运营商作为通信行业重要的研究机构，如何快速有效地实现对监管文件的检查与落实同样是一直困扰企业安全管理部门的难题。

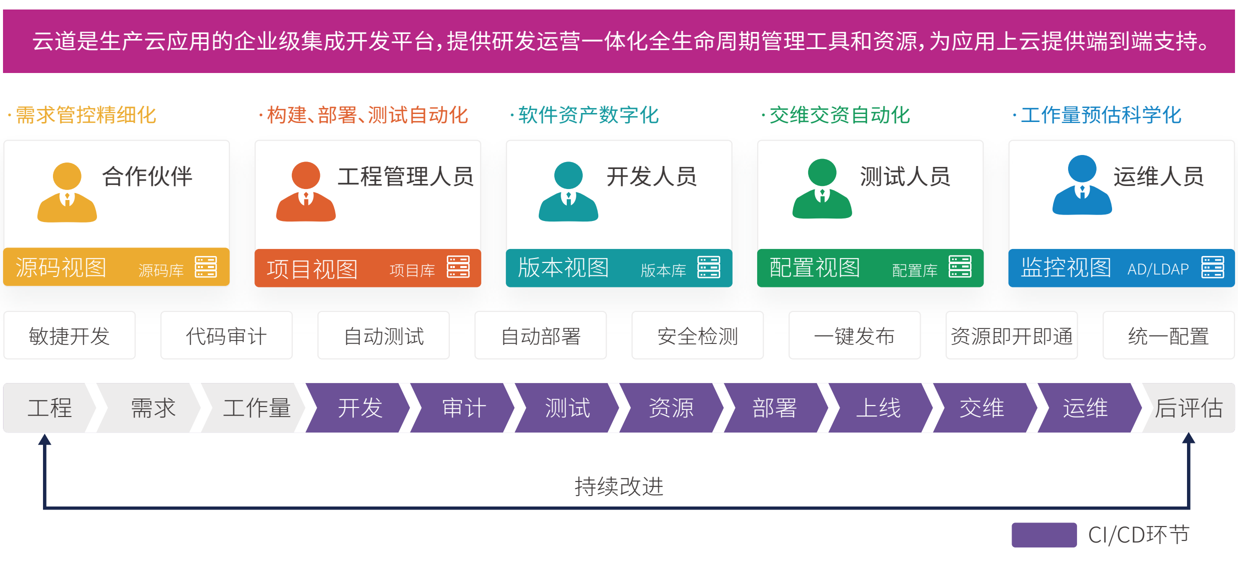


图 1-23 某运营商 DevOps 平台

通信运营商落地实践：该运营商通过在软件开发的不同阶段将安全工具或安全活动进行整合，将各个信息安全孤岛进行串联，实现安全开发、安全测试、安全部署和安全运营的统一融合，有效提升软件系统研发过程的标准化和自动化，降低对效率的影响和安全成本。

该运营商已经初步建立了端到端完整的安全工具链，将各种商业或开源的安全工具，如：IAST 工具、SAST 工具、SCA 工具、DAST 工具、渗透测试等工具通过 API 接口方式集成到 DevOps 平台，对外提供集成安全测试能力支持。DevSecOps 模式下的安全开发实践如下图所示。

图 1-24 DevSecOps 模式下的安全开发实践

同时，该运营商自主研发了人工智能安全态势感知平台，对内部用户进行行为分析及安全威胁发现，通过赋能研发运营一体化过程，助力 DevSecOps 安全运营效能的提升。该运营商落地 DevSecOps 的关键在于嵌入 CI/CD 流程，减少对开发流程的阻碍，通过采用多种自动化测试工具使得安全与业务研发实现更紧密的合作。此外在风险分析阶段采用高并发全分布式技术有效解决了该运营商单线、单业务、单系统风控难以兼容、连通以及实时风控能力低等难题，从而从容应对庞大的业务需求访问量，有效提升数据处理效率。

1.4.2 某互联网企业 DecSecOps 现状

面临的风险与挑战：该互联网知名企业创业早期，安全问题颇多，安全团队又独立于开发团队，对开发项目缺乏可视性，常常是随机审计评估项目，发现问题后提交工单要求修复，导致开发团队收到的每个工单都是紧急高优先级的，打乱了开发计划，也由此与安全团队产生分歧，漏洞问题不能闭环解决，安全团队无法系统性地提升应用安全性。

随后由于系统中断造成的巨大损失后，该互联网企业决定在云中重写整个应用程序以实现云原生，从根本上改变公司的运营方式，并且为了在未来能够应对造成同等或更严重损害的不可见错误，构建了 DevOps 体系，以 DevOps 的方式通过自动化故障和持续测试使该企业的云基础架构更加安全、可靠和可用。

随着该互联网企业订阅人数与日俱增，流媒体播放时间翻倍增长，使得在线应用程序频繁更新，且早期该企业仅依靠其内部安全团队进行移动应用安全测试，无法适应 DevOps 环境，安全越来越不能跟得上其发布的速度，最终考虑引入了 DevSecOps 体系，以期不仅发现传统的安全缺陷，还识别特定于移动设备中的隐私和安全问题。

某互联网企业落地实践：该互联网企业利用 DevSecOps 体系中安全自动化工具链对 Android、IOS 和 Microsoft 的移动应用程序进行静态或动态分析，以寻找安全漏洞和隐私漏洞，帮助该企业检测注入问题、会话管理问题、动态运行时缺陷、易受攻击的第三方 SDK、不安全的开源库以及 PCI、GDPR、HIPAA、FTC 等的合规性差距。另外利用体系中的威胁监控工具对 Apple App 和 Google Play 商店中相关该企业移动应用程序进行持续监控和扫描，并在发现安全或隐私问题时提醒该企业安全团队。

最重要的是，该 DevSecOps 体系提供了 Objective-C，Swift 和 Java 代码以识别和修复该企业应用程序中的各种漏洞问题，再将其上线到公共应用程序商店中，包括：

（1）开源库中的漏洞

DevSecOps 体系中应用安全测试工具识别第三方库，并在发现安全漏洞时及时通知安全团队。

（2）主动安全功能

通过引入 DecSecOps 体系，利用自动化安全工具链保障该企业应用程序，使应用程序更具弹性。

（3）减轻安全人员的负担

该企业通过引入 DevSecOps 体系为移动应用程序提供了安全保障。通过托管门户，该企业的开发人员和安全团队可以随时登录以获取状态更新、审查缺陷和警报，并提出安全的代码建议，从而节省时间、确保数据安全并减轻内部应用程序安全人员的负担。

作为该企业持续交付的平台，Spinnaker 是一个开源的多云持续交付平台，帮助企业完成快速、可靠、安全的交付和部署，下图所示为 Spinnaker 持续交付流程。

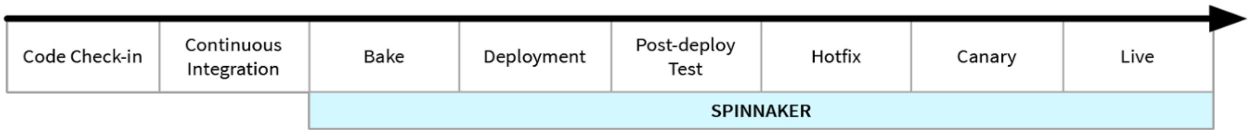


图 1-25 使用 Spinnaker 持续交付流程

Spinnaker 还提供集群管理功能，并提供对应用程序云足迹的深入可见性，如下图所示。通过 Spinnaker 的应用程序视图，您可以调整大小、删除、禁用甚至手动部署新的服务器组，使用蓝绿等策略。您可以创建、编辑和销毁负载均衡器以及安全组。

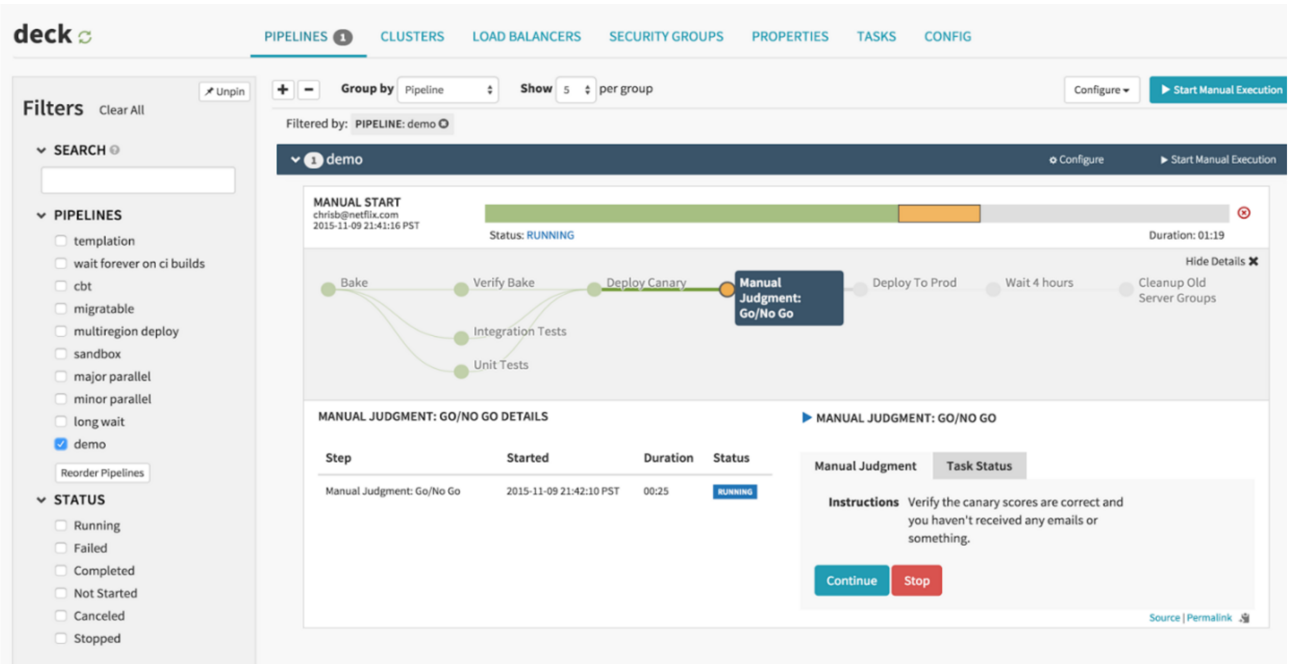


图 1-26 Spinnaker 管道

1.4.3 某智能制造企业 DevSecOps 现状

面临的风险与挑战：互联网时代的快速发展催生了车联网的形成。“软件定义汽车”大行其道，如今智能汽车软件代码行数直逼 1 亿条，从代码数量便可窥见其发展趋势。车联网是新一代网络通信技术与汽车、电子、道路交通运输等领域深度融合的新兴产业形态。随着汽车网联化、智能化的交融发展，安全形势更加复杂严峻，车联网行业面临着数据安全风险、车联网平台服务安全风险、车载应用安全风险等多种安全风险挑战。

（1）数据安全风险：网联汽车普遍搭载多种传感器装置，如在道路行驶中记录的高精度道路测绘数据、车流分布信息数据、公民车内录音录像以及位置轨迹等隐私数据，都会回传至车联网平台进行分析处理。如若数据安全保障能力保障不足，就有可能面临着国家重要数据和个人隐私信息泄露风险；

（2）车联网平台服务安全风险：用户主要通过车联网平台进行信息交互、远程操作，一旦遭受网络攻击控制，如被黑客入侵或除驾驶员以外的人从外部控制，实现远程操控，将造成严重后果；

（3）车载应用安全风险：车辆联网应用日益丰富，如汽车数字钥匙、车载应用等，汽车智能应用大量引用开源软件，且与云端联网，相应的攻击面增多，不仅影响系统运行等功能安全，还会影响网络安全。

智能制造企业落地实践：该企业基于敏捷开发、微服务、容器化和云优先架构等相关云原生技术建立了拥有 600 多个存储库、350 多个微服务应用、10 多种开发语言等的 DevOps 敏捷持续交付体系，以实现高质量的快速交付。为了应对上述安全风险，该企业开始采用 DevSecOps 实践以全程确保行车安全，并通过以下几个原则将安全纳入开发流程中：

（1）围绕软件的整个生命周期进行规划，充分考虑代码的升级、补丁、持续的漏洞测试；

（2）应用 SCA 工具检测第三方组件安全漏洞风险、许可证风险等；应用 SAST、IAST、DAST 等安全测试工具检测安全漏洞并及时修复；

（3）测试阶段进行 API 测试检测 API 中是否存在漏洞；

（4）大范围地实施汽车生态系统威胁建模与架构风险分析，以识别漏洞并减少安全控制漏洞；

（5）在测试阶段进行 ECU 仿真、故障仿真等仿真测试，模拟渗透测试会通过突破安全控制措施，找到应对已知威胁的方法，而无需对实际车辆进行危险的现场测试；

（6）对 CAN 总线（控制器区域网络）进行分析、模糊测试、捕获和逆向工程；

（7）利用签名认证、加密等手段避免第三方应用对汽车产生安全威胁。

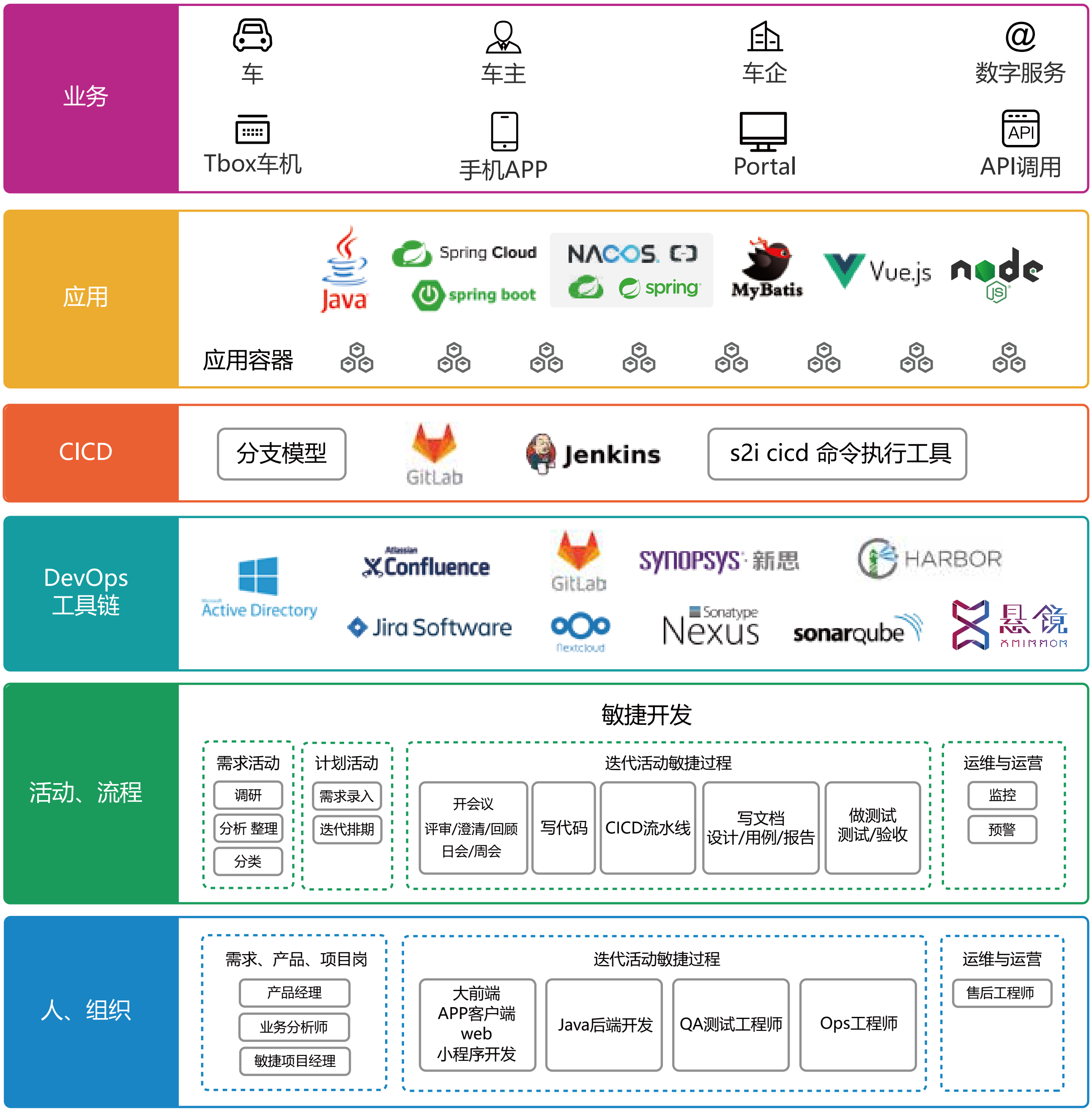


图 1-27 该智能制造企业车联网安全防护实践

如上图所示，上述原则涵盖了从代码选择和分析到发布和生命周期管理的所有阶段，使用 DevSecOps 工具进行自动化安全测试，以确保将风险识别和消除纳入软件安全解决方案中，并随着基于云平台的软件分发日益普及，利用容器以安全、高效地维护车辆内的安全软件环境。

此外该企业在 DecSecOps 开发流程中利用 AI 组件来管理更新调度和部署，并不断进行测试以检测未知的风险漏洞；利用人工智能进行监督流程，以减少因人为决策失误而造成的隐患；利用机器学习用于持续分析软件中可能存在的安全问题，进行预测性维护检查，以提前告知驾驶员或维修团队可能发生的组件故障，或调整编程，以便更高效地解决安全问题。

2

DevSecOps 年度热点

2.1.1 软件成分分析技术（SCA）

在传统意义上，软件平台、框架和库都是使用专有软件实现的。它们将由来自内部开发或第三方商业软件供应商的各种构建块组成。随着时间的推移，公司开始将开源软件整合到他们的平台和软件堆栈中。现如今，开源是帮助组织将其服务数字化并利用其技术在当今竞争激烈的市场中更好地竞争的关键因素之一。开源组件正在成为几乎所有垂直领域软件的主要构建块，但大量使用开源组件同时也导致给软件供应链带来难以预知的安全隐患。为了组织更好的通过开源软件提升生产力，组织需要采用 SCA 技术保证软件供应链的安全性。

SCA（Software Composition Analysis，软件成分分析）是一种对二进制软件的组成部分进行识别、分析和追踪的技术。SCA 可以生成完整的 SBOM，分析开发人员所使用的各种源码、模块、框架和库，以识别和清点开源软件（OSS）的组件及其构成和依赖关系，并精准识别系统中存在的已知安全漏洞或者潜在的许可证授权问题，把这些安全风险排除在软件的发布上线之前，也适用于软件运行中的诊断分析。SCA 允许组织在整个软件供应链中对开源软件的使用进行安全风险管理，保护最终用户免受安全漏洞的影响，在保证组织能够利用开源软件带来的优势的同时，也能保持安全性和合规性。

SCA 主要的两种模式：静态模式和动态模式

1、静态模式：静态模式是使用工具对目标工程文件进行解压，识别和分析各个组件的关系；

2、动态模式：动态模式则是依赖于执行过程，在程序执行的同时收集必要的活动元数据信息，通过数据流跟踪的方式对目标组件的各个部分之间的关系进行标定。

随着开源软件的日益普及，SCA 的重要性逐年增长。这种增长导致了一种新型工具的产生，即 SCA 工具。其正在成为应用程序安全的必备工具，SCA 工具可以精准识别应用开发过程中，软件开发人员有意或违规引用的开源第三方组件，并通过对应用组成进行分析，多维度提取开源组件特征，计算组件指纹信息，深度挖掘组件中潜藏的各类安全漏洞及开源协议风险。同时，SCA 工具还可以对应用程序源代码、支持库、所有相关组件以及它们之间的间接和直接依赖项执行扫描，通过代码扫描可以及早发现漏洞和许可合规问题并降低修复成本，允许自动扫描以更少的成本发现和修复安全漏洞。

从使用成本来看，SCA 工具可分为开源（免费）的开源威胁治理工具和商业化的开源威胁治理工具。其中商业化的 SCA 工具发展较为成熟，更适合在大型企业的场景中使用，在此不再一一列举。开源的 SCA 工具主要包括 Snyk Open Source（Snyk）、OpenSCA（悬镜安全）、Veracode SCA（Veracode）、DependencyCheck（OWASP）等几个代表性的工具，每一款 SCA 工具都各有不同，各具特色，各大企业可以根据自己的实际情况进行选择。

通过使用基于多源 SCA 开源应用安全缺陷检测技术的安全审查工具，开源在整个软件供应链中对开源软件的使用进行安全风险管理，为组织提供具有可操作性的洞察力和详细的补救措施

1、创建准确的软件物料清单（SBOM）：SCA 工具生成软件物料清单（SBOM），其中包括已识别的源代码，然后针对包括 NVD 在内的多个数据库进行检查。SBOM 可帮助安全专业人员和开发人员更好的了解应用程序中使用的组件并深入了解潜在的安全和许可证问题，同时可以快速识别和修复任何关键的安全和法律问题；

2、发现并跟踪所有开源组件：SCA 可以帮助组织跟踪当前运行的程序、源代码、构建依赖项、子组件等所依赖组件的使用情况，检测扫描代码中与知识库中跟踪的已知漏洞相对应的任何安全漏洞和依赖项中的安全漏洞;

3、制定和执行相关开源政策：SCA 工具可以制定细粒度的策略来定义和自动执行关于开源软件组织可接受的安全性和合规性指南，实现快速响应各类安全事件；

4、启用主动和持续监控：为了更好地管理工作负载并提高生产力，SCA 持续监控安全漏洞问题，通过持续监控、扫描和来自强大漏洞数据库的最新 CVE 知识，实现更深入的洞察。同时对关键警报进行优先级排序和自动修复，以帮助开发人员在不中断工作流程的情况下快速解决问题；

5、无缝集成到构建环境中：在 DevOps 环境中集成操作系统安全和许可证扫描，以便扫描代码并识别构建环境中的依赖性。

2.1.2 运行时应用自我保护（RASP）

随着软件行业的迅速发展，容器、IaaS、PaaS、虚拟和弹性环境激增，在不同环境下，快速部署应用程序和 API 成了核心要求。DevOps 的大行其道进一步加速了集成、部署和交付的速度，这使得需要独立部署的 WAF 在灵活性上的欠缺成为其致命弱点，以及近几年的“HW”行动，企业应用安全遭受越来越大的挑战。

随着针对应用程序的黑客攻击威胁的不断发展以及“HW”行动的兴起，仅靠 Web 应用程序防火墙（WAF）已不再是抵御威胁的有效方法。传统 WAF 通过在网络流量到达应用程序服务器之间对其进行分析，完全独立于应用程序进行工作。在门外处理的方式，使其无法真正核实请求的合法性，难以保证其准确性，因此管理员只能使其处于“日志模式”。

为了更好地预防针对应用程序的攻击威胁以及应对“HW”等超大流量超大规模的实战验证，RASP（Runtime application self-protection，运行时应用自我保护）作为 Gartner 提出的一种新型 Web 防护手段，将保护代码注入到应用程序中，与应用程序融为一体，使应用程序具备自我保护能力，通过分析应用程序行为和上下文，对访问应用系统的每一段代码进行检测，保护实时运行的应用程序。通过使用该应用程序持续监控其自身行为，当应用程序遭受到实际攻击和伤害时，RASP 可以实时检测和阻断安全攻击，无需人工干涉。

市面上绝大多数 Java 版 RASP 技术，如 OpenRASP、云鲨 RASP、Imperva RASP 等都是在运行时阶段字节码加载前进行插桩，其优点是无需对源代码进行修改真正做到对应用程序的无侵入。其实现原理：Java 源程序在运行时需要通过编译器编译成为 .class 文件，即字节码文件。JAVA 的跨平台特性是 Java 字节码文件可以直接在 JVM（Java 虚拟机）运行，而 JVM 提供的 Java Agent 参数可以使得在字节码加载前修改字节码，完成 RASP Agent 的注入，当应用程序受到攻击时，就会触发 HOOK 函数，此时 RASP Agent 就可以获取到函数参数，实现对 Java 运行程序的检测。

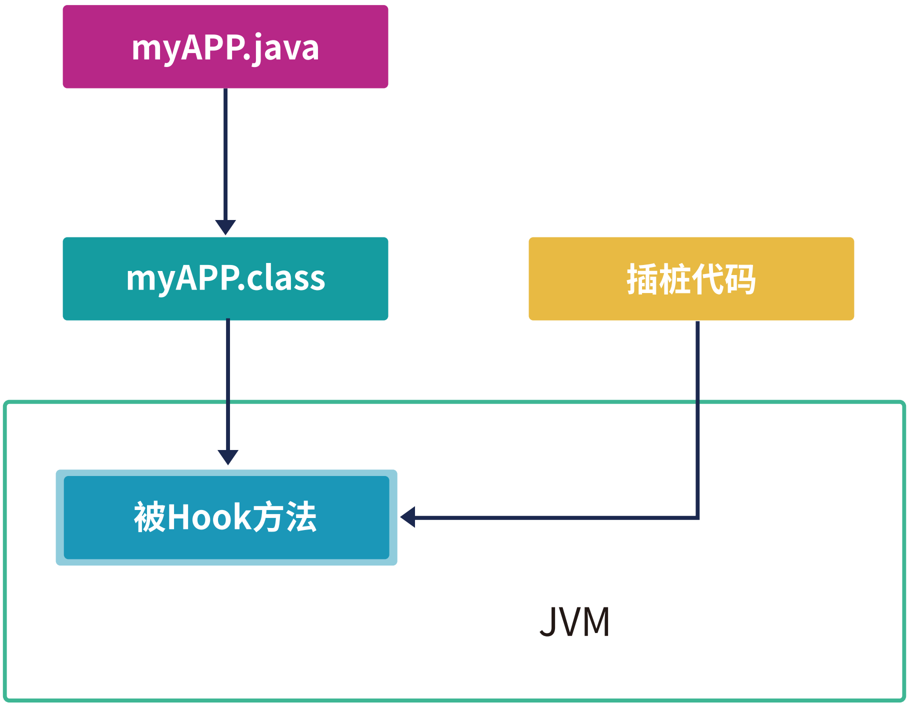


图 2-1 Java 代码中实现 RASP 注入防护

面对应用现代化，安全防护需要“左移”，推动安全战略实现从“传统基于边界防护的安全”向“面向应用现代化的内生安全”模式转变。RASP 作为降低应用风险的一项关键创新技术，弥补了传统边界安全防护产品的先天性防护不足，可应对无处不在的应用漏洞与网络威胁，为应用程序提供全生命周期的动态防护和内生主动安全免疫能力，其必将加快企业数字化转型，推动软件供应链的创新发展。

1、美军发布《国防部企业 DevSecOps 战略指南》2.0 版本

2021 年 3 月，美国国防部发布《国防部企业 DevSecOps 战略指南》等系列战略文件，提出全军应用 DevSecOps 的指导原则。本文对 DevSecOps 的定义、优势、应用原则进行了梳理，并介绍了文件中强调的软件供应链和软件工厂概念。同时要求国防部全面应用 DevSecOps 的原则，为 IT 能力提供方、消费者、应用开发团队和授权官方组织提供教学、最佳方案及实施和运行指南。

美国防部首席信息官以及国防部长下属采办和维护办公室（OUSD A&S）已认识到，亟需利用新的商用途径和最佳方法来重塑美军的软件开发方法和文化。DevSecOps 的优势在于，能够在整个国防部实施软件现代化，从而以较快的速度交付安全的软件。

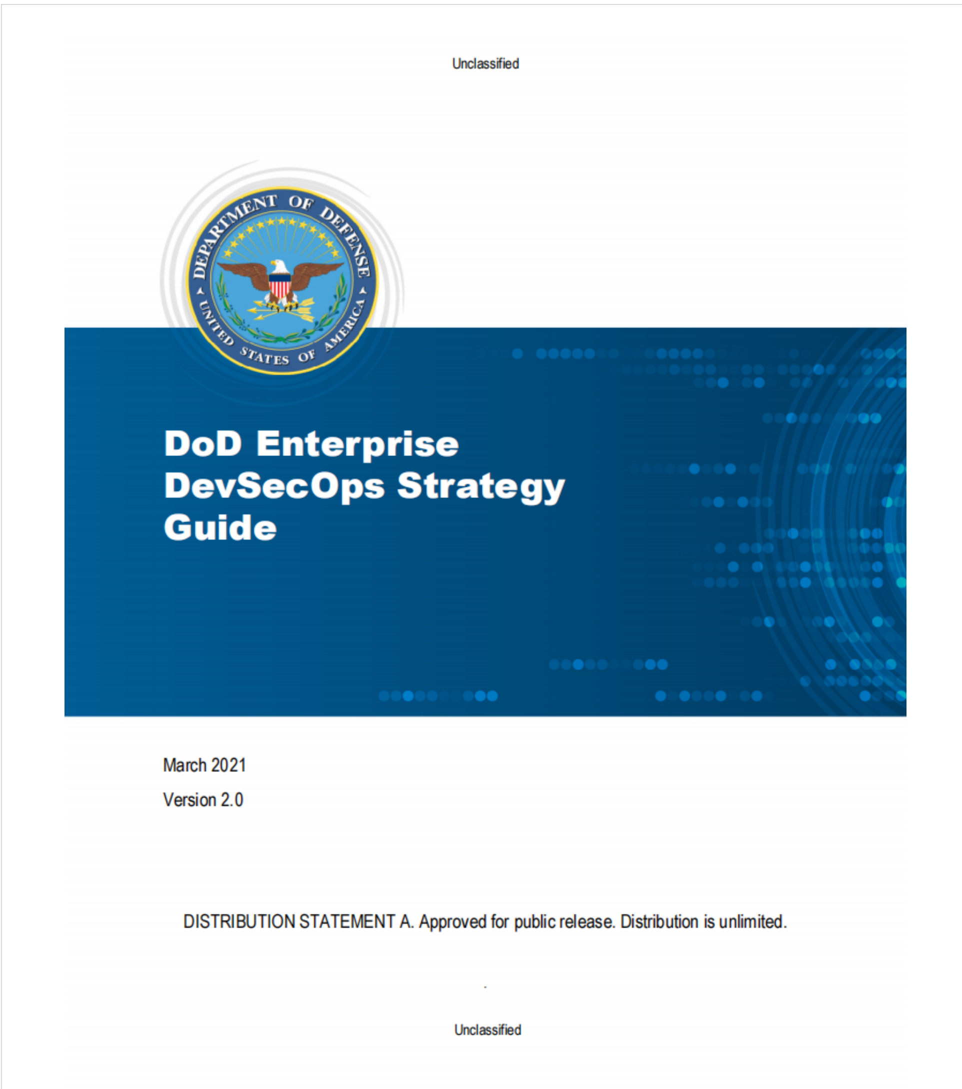


图 2-2 《国防部企业 DevSecOps 战略指南 2.0》报告

2、美国总统拜登签署《改善国家网络安全行政令》

2021 年 5 月 12 日美国总统拜登签署发布了《改善国家网络安全行政令》（Executive Order on Improving the Nation’s Cybersecurity），其中包括九项关键举措，是美国在网络安全方面最详细的行政命令之一。拜登在白宫的声明中指出，近日在美国频发的网络安全事件发人深省，其中包括科洛尼尔管道运输公司被黑客攻击事件等等。美国政府需要采取行动来打击网络犯罪，并从根本上加强网络安全管理。

该行政令是美国联邦政府试图保护美国软件供应链安全采取的最强劲的措施。根据行政令，拜登要求规范和更新商业软件的网络安全标准，并要求联邦政府所使用的所有软件在 9 个月内达到新的标准，与政府有业务往来的软件开发人员必须公开其安全数据。行政令也要求联邦政府开始使用加密验证和身份验证等措施。此外，拜登下令建立网络安全审查委员会来分析网络攻击事件，委员会将由政府和私营部门共同领导。

该行政令明确要求联邦政府出售软件的任何企业不仅需要提供应用程序，而且还必须提供软件物料清单（SBOM），提供组成该应用程序组件的透明度。同时，要求美国商务部下属机构国家标准技术局（NIST）在 6 个月内发布软件供应链安全指南，并在 1 年内发布最终指南，该指南的内容需要包括如何检测漏洞、如何查找缺陷证据、如何确保开源代码和源代码的最新来源，以及如何使用自动化工具验证可信代码的指导。

图 2-3 美国总统拜登签署《改善国家网络安全行政令》

3、Apiiro 公司斩获 RSAC 2021 创新沙盒比赛冠军

2021 年 5 月 19 日，Apiiro 公司在 RSAC 2021 创新沙盒比赛中脱颖而出，斩获最终冠军，获得“RSAC 2021 最具创新初创企业”称号。RSA Conference 2021 的三大核心话题之一，就是供应链安全，同时 2021 年爆出的 Solarwind 供应链污染，造成极其恶劣的影响，也导致大家对软件供应链安全风险的关注度大幅度提升。Apiiro 宣传号称可以发现和阻止类似 SolarWinds 的供应链攻击，非常契合当前的网络威胁主题，作为 DevSecOps 赛道里的一员，Apiiro 可为用户提供完整的业务应用风险可见性来重新定义整个系统开发生命周期（SDLC），识别整个开发过程中的风险，加强应用程序治理和合规性，并防止高级 CI / CD 攻击，所有这些都可以在一个平台上以及在开发生命周期的早期进行。

Apiiro 的夺冠，可以表明未来几年网络安全的风向标，同时 DevSecOps 已成为当下重要赛道，云原生浪潮下安全左移已成为新的发展趋势。随着敏捷开发模式的成熟和云原生的迅猛发展，DevOps 已经成为开发团队常态，而从开发到运营如此长的链条中，安全怎么做始终是一个困难问题。其中涉及到多个团队、多种流程、多种软件协同，Gartner 也是连续多年在提 DevSecOps。2021 年创新沙盒中出现了两家从事 DevSecOps 的公司，可见这个赛道已经有了足够多的玩家，客户认知和接受度也已经相对成熟。

图 2-4 Apiiro 公司斩获 RSAC 2021 创新沙盒比赛冠军

4、亚太区首届 DevSecOps 敏捷安全大会

2021 年 7 月 21 日，亚太区首届 DevSecOps 敏捷安全大会（DSO 2021）在北京成功举办，大会以“安全从供应链开始”为主题，寓意安全基础决定上层建筑，在云原生环境下为软件供应链注入覆盖全流程的安全属性，从源头做风险治理。DSO 2021 由中国信息通信研究院指导，DevSecOps 敏捷安全厂商悬镜安全主办，腾讯安全协办，现场近千位权威学者、安全专家、生态伙伴、技术精英齐聚一堂，近 20 个议题，直击软件供应链安全复杂场景中涉及的管理、流程、技术、工具等问题，为安全产业发展提供创新源动力。

同时，在大会现场正式发布了《软件供应链安全白皮书（2021）》，白皮书着重分析了软件供应链安全，梳理了软件供应链的安全现状，透过现状全面剖析软件供应链的安全风险及面临的安全挑战，有针对性的提出如何对软件供应链的安全风险进行防范与治理，系统阐述了软件供应链安全的防护体系及软件供应链安全的应用实践以供参考，最后白皮书结合现在软件供应链安全的发展趋势进行了全面的分析及展望。软件供应链安全作为国家近几年新提出的网络安全理念，不再是针对软件供应链上单一环节进行安全防护，而是针对软件供应链全链路进行安全监控防护，薄弱环节的安全预防更是重中之重。

图 2-5 DevSecOps 敏捷安全大会

5、新思科技发布软件安全构建成熟度模型 BSIMM12

2021 年 9 月新思科技发布其最新版本的软件安全构建成熟度模型 BSIMM12。自 2008 年起，新思科技的软件安全构建成熟度模型 BSIMM 就作为评估各种类型和规模的组织的有效工具，包括全球一些先进的安全团队正采用其软件安全策略。

每一个版本的 BSIMM 模型都会为了保持数据的“新鲜度”而进行报告内企业的删减和增加，从而准确放映最新的市场软件安全趋势。最新的 BSIMM12 数据反映了企业正调整其方法来应对现代开发和部署实践的新动态，比如增加开源、云、容器方面的安全活动。BSIMM12 反映了观察到的 128 家公司的软件安全实践，覆盖多个垂直行业，包括金融服务、金融科技、独立软件供应商（ISV）、云、医疗保健、物联网等，并且描述了近 3000 名软件安全团队成员和 6000 多名外围小组成员的工作成果，旨在帮助企业规划、执行、评估和完善其软件安全计划。

BSIMM 模型不同于指导性模型，其本质上是一种描述性模型，是对数据和事实的一种陈述，适用于具有软件信息安全、生产软件的流程的企业，衡量其在安全方面的成熟度。通过参与 BSIMM 的评估，企业除了可以横向详细了解自身 SSI 的执行情况，从而改善自身的软件安全计划之外，还可以纵向评估在软件安全计划实施一段时间后具备的成熟度如何，从而有助于重新分配资源或者对外宣传。

图 2-6 新思科技发布 BSIMM12 报告

6、我国五部门联合发布《关于规范金融业开源技术应用与发展的意见》

2021 年 10 月 20 日，中国人民银行办公厅、中央网信办秘书局、工业和信息化部办公厅、银保监会办公厅、证监会办公厅联合发布《关于规范金融业开源技术应用与发展的意见》（以下简称《意见》）就规范金融机构合理应用开源技术，提高应用水平和自主可控能力，促进开源技术健康可持续发展进行工作布局。

近年来，开源技术在金融业各领域得到广泛应用，在推动金融机构科技创新和数字化转型方面发挥着积极作用，但也面临安全可控等诸多挑战。《意见》的出台，有助于规范金融机构合理应用开源技术，提高应用水平和自主可控能力，促进开源技术健康可持续发展。

《意见》要求金融机构在使用开源技术时，应遵循“安全可控、合规使用、问题导向、开放创新”等原则。《意见》鼓励金融机构将开源技术应用纳入自身信息化发展规划，加强对开源技术应用的组织管理和统筹协调，建立健全开源技术应用管理制度体系，制定合理的开源技术应用策略；鼓励金融机构提升自身对开源技术的评估能力、合规审查能力、应急处置能力、供应链管理能力等；鼓励金融机构积极参与开源生态建设，加强与产学研交流合作力度，加入开源社会组织等。《意见》强调要加强统筹协调，建立跨部门协作配合、信息共享机制，完善金融机构开源技术应用指导政策，探索建立开源技术公共服务平台，加强开源技术及应用标准化建设等。

下一步，人民银行、中央网信办、工业和信息化部、银保监会、证监会将继续协同联动，推进《意见》中的各项工作部署落实落地，切实提升金融业开源技术应用水平。

中国人民银行办公厅 中央网络安全和信息化委员会办公室秘书局 工业和信息化部办公厅 中国银行保险监督管理委员会办公厅 中国证券监督管理委员会办公厅关于规范金融业开源技术应用与发展的意见

标题: 中国人民银行办公厅 中央网络安全和信息化委员会办公室秘书局 工业和信息化部办公厅 中国银行保险监督管理委员会办公厅 中国证券监督管理委员会办公厅关于规范金融业开源技术应用与发展的意见

索引号:	HB/2021-4364505	**文号:**	银办发〔2021〕146号
发文机关:	中国人民银行办公厅 中央网络安全和信息化委员会办公室秘书局 工业和信息化部办公厅 中国银行保险监督管理委员会办公厅 中国证券监督管理委员会办公厅	**公文种类:**	
		发布日期:	2021年10月20日
		生效日期:	
主题词:	金融业开源技术		

图 2-7 我国五部门联合发布《关于规范金融业开源技术应用与发展的意见》

7、Apache Log4j2“核弹级”安全漏洞事件被爆出

2021 年 12 月 9 日晚，被全球广泛应用的组件 Apache Log4j 被曝出一个“史诗级 / 核弹级漏洞”。据悉，Apache Log4j2 已存在多种在野利用，且利用方式十分简单，攻击者仅需向目标输入一段代码，不需要用户执行任何多余操作即可触发该漏洞，使攻击者可以远程控制用户受害者服务器，90% 以上基于 Java 开发的应用平台都会受到影响。业内众多人士认为，其危害程度丝毫不弱于 2017 年的“永恒之蓝”漏洞。

Log4j2 作为 Java 代码项目中广泛使用的开源日志组件，它的一个严重安全漏洞对于全球的软件供应链生态来讲不亚于一场新冠病毒的影响，任何企业的代码项目沾上它都有可能给企业带来致命的安全风险。网络安全专家认为，这一漏洞潜在危害极大，甚至可能是“计算机历史上最大的漏洞”。该安全事件披露后官方紧急推出了 2.15.0 和 2.15.0-rc1 新版本修复，依然未能完全解决问题，目前已经更新到 2.16.0。该漏洞被命名为 Log4Shell，编号 CVE-2021-44228。

资料显示，该漏洞在 11 月 24 日就被阿里云安全团队发现并向 Apache 官方进行了报告。目前，漏洞利用细节已公开，Apache 官方已发布补丁修复该漏洞。


访客预约 | RSS订阅

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

统一搜索

看新闻 找文件 查办事 提意见 查数据 要投诉

工业和信息化部 新闻动态 政务公开 政务服务 公众参与 工信数据 专题专栏

首页 > 工业和信息化部 > 机关司局 > 网络安全管理局 > 工作动态

关于阿帕奇Log4j2组件重大安全漏洞的网络安全风险提示

发布时间：2021-12-17 12:09 来源：网络安全管理局

阿帕奇（Apache）Log4j2组件是基于Java语言的开源日志框架，被广泛用于业务系统开发。近日，阿里云计算有限公司发现阿帕奇Log4j2组件存在远程代码执行漏洞，并将漏洞情况告知阿帕奇软件基金会。

12月9日，工业和信息化部网络安全威胁和漏洞信息共享平台收到有关网络安全专业机构报告，阿帕奇Log4j2组件存在严重安全漏洞。工业和信息化部立即组织有关网络安全专业机构开展漏洞风险分析，召集阿里云、网络安全企业、网络安全专业机构等开展研判，通报督促阿帕奇软件基金会及时修补该漏洞，向行业单位进行风险预警。

该漏洞可能导致设备远程受控，进而引发敏感信息窃取、设备服务中断等严重危害，属于高危漏洞。为降低网络安全风险，提醒有关单位和公众密切关注阿帕奇Log4j2组件漏洞补丁发布，排查自有相关系统阿帕奇Log4j2组件使用情况，及时升级组件版本。

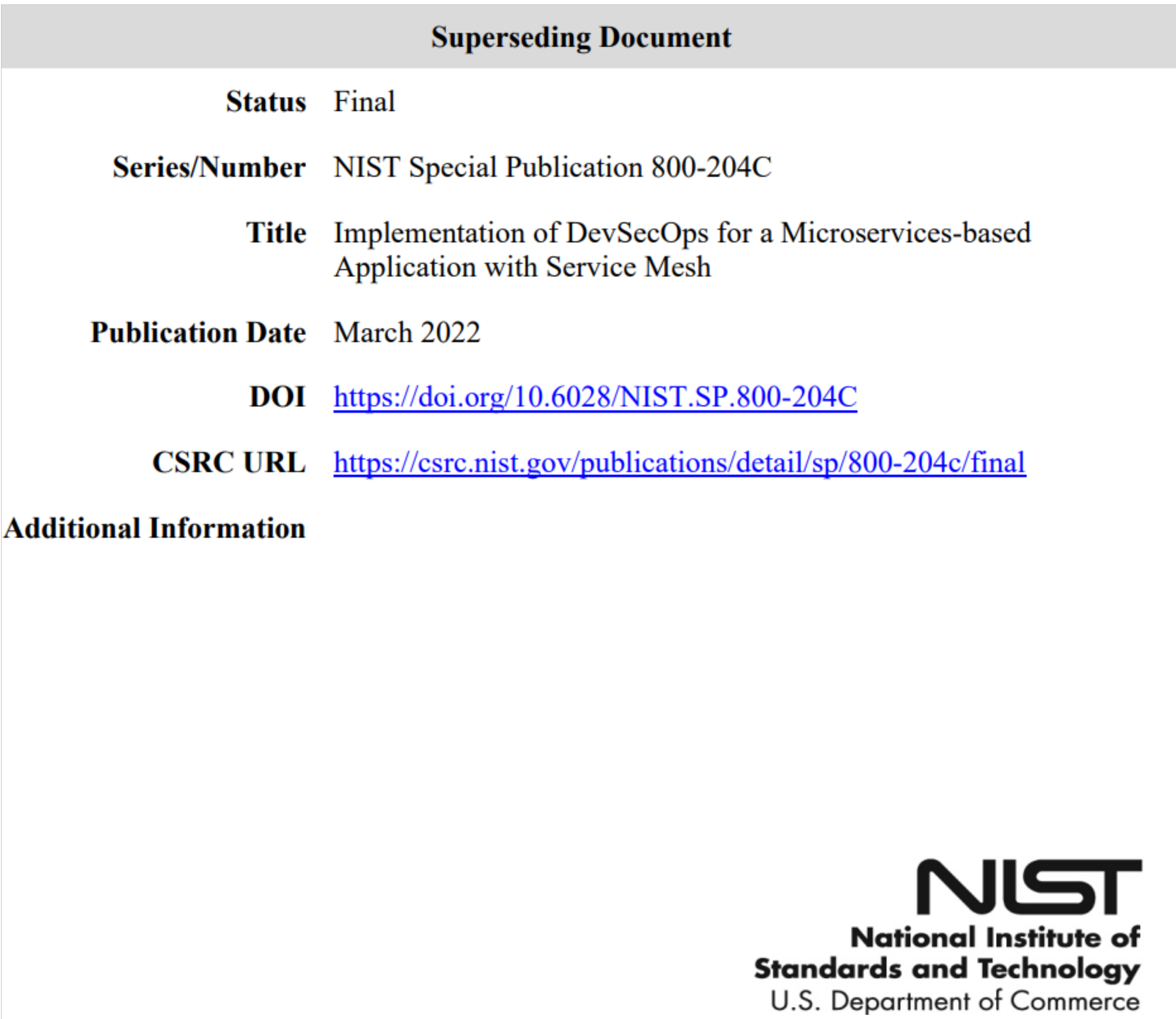
工业和信息化部网络安全管理局将持续组织开展漏洞处置工作，防范网络产品安全漏洞风险，维护公共互联网网络安全。

图 2-8 中华人民共和国工业和信息化部关于阿帕奇 Log4j2 组件重大安全漏洞的网络安全风险提示

8、NIST DevSecOps 项目

NIST 作为美国官方的标准制定机构，成立前瞻性的课题项目是其职责之一。创建关于 DevSecOps 实践的新 NIST 特别出版物 (SP)，将现有指南和实践出版物中的内容汇集在一起并规范化是 2020 年 10 月 NIST 启动的 DevSecOps 项目的主要内容之一。可以看到，其当前的主要工作都围绕着 800 系列特别出版物（SP）进行。NIST 的 800 系列特别出版物 (SP) 提供了计算机安全相关的信息，包括指南、建议、技术规范和 NIST 网络安全活动的年度报告等内容。

2021 年 9 月 29 日发布了 DevSecOps 800 系列特别出版物 SP 800-204C《使用服务网格并基于微服务的应用程序实施 DevSecOps》草案，并于 2022 年 3 月 8 日发布最终版，NIST SP 800-204C 为云原生应用程序实施 DevSecOps 提供了指导，该指南还讨论了这种方法对于安全保障和实现持续运营授权 (C-ATO) 的好处。



Superseding Document	
Status	Final
Series/Number	NIST Special Publication 800-204C
Title	Implementation of DevSecOps for a Microservices-based Application with Service Mesh
Publication Date	March 2022
DOI	https://doi.org/10.6028/NIST.SP.800-204C
CSRC URL	https://csrc.nist.gov/publications/detail/sp/800-204c/final
Additional Information	

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

图 2-9 SP 800-204C《使用服务网格并基于微服务的应用程序实施 DevSecOps》最终版

9、IDC Innovators：安全左移，DevSecOps 创新厂商助力企业构建原生安全

2022 年 5 月 20 日，全球知名咨询机构 IDC 发布了《IDC Innovators: 中国 DevSecOps 技术，2022》（Doc # CHC47745422）报告。据悉，IDC Innovator (IDC 创新者) 榜单旨在为行业用户和投资商介绍拥有创新技术或突破性商业模式的新兴 IT 供应商，该入榜的创新者在其从属的特定细分领域能否为其用户提供创新性的技术实现和解决其面临的业务痛点问题。

在“安全左移”的背景下，IDC 首次在国内启动关于 DevSecOps (开发安全运维一体化) 专项报告，目的就是对这个新兴赛道上的创新企业进行调研后形成专项报告，该类报告通常推荐的入选数量会严格控制在 3-5 家以内。基于对 DevSecOps 生态链中各厂商的分析，从公司规模、产品技术，到行业和客户，生态系统建设以及未来发展战略等方面对该领域的新兴公司进行了考察，最终选择了北京安普诺信息技术有限公司（悬镜安全）、北京升鑫网络科技有限公司（青藤云安全）、杭州孝道科技有限公司（安全玻璃盒）、深圳海云安网络安全技术有限公司（海云安）、思客云 (北京) 软件技术有限公司（思客云）五家厂商（排名不分先后）成为 IDC 中国 DevSecOps 技术创新者。

该报告对上述五家公司的产品和客户案例进行深入的分析，阐明了其差异化特点以及面对的挑战，帮助 IT 技术购买者选择技术供应商时，发现最新的 IT 技术，并找到新产品的评估方法。

图 2-10 《IDC Innovators: 中国 DevSecOps 技术，2022》

10、中国信息通信研究院发布《中国 DevOps 现状调查报告（2022）》

7 月 28-29 日，由中国信息通信研究院、中国通信标准化协会主办的 2022 首届 XOps 产业生态峰会在北京成功举办。在本次论坛上，由中国信息通信研究院云计算与大数据研究所审计与治理部主任杨玲玲重磅发布并解读了《中国 DevOps 现状调查报告（2022）》。中国 DevOps 现状调查报告梳理了国内 DevOps 实践现状，洞察 DevOps 转型新趋势，助力企业 DevOps 落地实践，促进全行业 DevOps 演进与变革。

本次调查由中国信息通信研究院联合超 50 家企业共同发起，在各地 DevOps 实践企业和社会各界的大力支持下，共收到 4280 份有效问卷。问卷以中国信息通信研究院牵头编制的《研发运营一体化（DevOps）能力成熟度模型》系列标准、《研发运营一体化（DevOps）效能度量模型》为参考，聚焦中国 DevOps 实践成熟度现状，对 DevOps 转型现状、未来 DevOps 的发展、企业对政策 / 资质的需求等情况进行了调查。帮助企业和产业侧了解现状、趋势和核心关切。

图 2-11 中国 DevOps 现状调查报告（2022）

3

发展趋势

1、开源软件供应链安全热度只增不减

随着开源技术快速形成生态，开源热度不断升高，开源软件正不断推动深度信息技术的创新发展，因此，企业引入开源软件已成为一种趋势。随着开源软件在推动数字化转型方面所发挥的作用变得越来越明显，已成为企业实现快速开发和科技创新的必要条件，是商业不可或缺的一部分。

作为业务应用程序的重要组成部分，开源软件已成为网络空间的重要基础设施。开源软件的大量使用导致软件供应链越来越复杂化和多样化，开源软件已成为影响软件供应链安全的关键因素之一。据 Synopsys 称，99% 的商业数据库至少包含一个开源组件，其中近 75% 的代码库包含开源安全漏洞。随着开源组件使用的增加，风险面也在不断膨胀，使用包含已知安全漏洞的开源组件很有可能将安全缺陷引入到软件产品中，并随着软件的使用而进行扩散，进而对软件供应链造成巨大的安全威胁。

软件供应链开源化，导致影响软件供应链的各个环节都不可避免受到开源的影响。根据 Sonatype 发布的《2021 年软件供应链状况》报告可知，2021 年旨在利用上游开源生态系统弱点的软件供应链攻击同比增长了 650%。若攻击者通过将恶意代码注入为全球软件供应链提供组件的开源项目中，借助开源软件的“高信任度”和影响力，通过感染软件供应链的“上游”组件加速向“下游”扩散，产生的破坏性进一步加大。

开源软件目前正处于企业信息化的管理盲区，企业往往会忽视掉源代码和使用的基础开源组件的安全性以及各个组件之间的依赖关系。由于开源软件之间的依赖关系非常复杂，一旦出现安全问题将带来十分严重的安全影响，若一款开源软件出现未知的安全漏洞，将会导致所有与之存在关联依赖关系的其他软件出现同样的安全漏洞，软件供应链的攻击面将呈现出爆炸性的放大效果。

开源软件已成为企业创新的基础，推动企业数字化转型，其安全性直接影响着网络重要基础设施的安全性。因此，开源软件的安全性应得到充分关注和重视，未来会更加重视开源软件供应链的安全风险检测，构建开源软件的全生命周期安全风险治理平台。

2、软件供应链精准监管的有力抓手 SBOM

软件物料清单（SBOM）是一份正式规范且机器可读的软件组件清单，清单中包含这些组件的依赖关系、层次关系以及相关信息，旨在跟踪软件组件的详细信息和供应链关系、它们的依赖关系以及它们的层次关系。

2021 年 5 月美国总统拜登签署发布的《改善国家网络安全行政令》要求美国商务部在 60 天内协同美国国家通信和信息管理局（NTIA）发布 SBOM 的“最小元素”。2021 年 7 月 12 日 NTIA 发布了《SBOM 最小要素》，规定了最小要素应包括数据字段、自动化支持、实践和过程等三个方面，其中的实践和过程指为了将 SBOM 集成到安全开发生命周期操作中而需定义其请求的操作、生成和使用等内容，包含频率、深度、已知的未知情况

（known unknowns）、分发和交付、访问控制和容错等。并于同年 11 月 27 日发布的《软件供应商手册：SBOM 生成和提供》是对最小要素中 SBOM 生成的进一步细致讨论和在实施层面的补充，给出了 SBOM 生成的一般性流程及每一步中应关注的重点。

近年来一些重大的软件供应链攻击，如 2021 年的 Apache Log4j2 漏洞攻击和 2022 年的 spring 框架漏洞攻击，越来越多的组织和政府意识到软件供应链安全的重要性。SBOM 已经成为了安全业界公认的遏制软件供应链风险的最佳方案之一，SBOM 的推广应用可以增强软件供应链的可见性，极大地便利软件组件溯源、软件产品依赖关系梳理、已知漏洞的影响范围判断、及时发现恶意软件渗透等，从而有力支撑软件供应链相关监管政策规则的落地实施。

虽然截止目前还没有创建和维护 SBOM 的标准、法规或行业指南，但医疗保健概念验证（Healthcare POC）工作组与美国国家电信与信息管理局（NTIA）软件组件透明度小组共同协作收集了如何生成 SBOM 的简单说明和指南。相信不久的将来将会推行出 SBOM 标准，并通过标准推广实践。

3、RASP 与 IAST 技术实现一体化

IAST 是近几年较为火热的一项应用安全测试新技术。IAST 最显著的特征就是通过运行时部署插桩 Agent 来收集安全信息，当外部扫描器发起扫描测试触发这个 Agent 时，IAST 便持续监测应用程序中的流量信息，一旦检测到漏洞，便实时提供报警并进行漏洞定位。IAST 在检出率、误报率以及成本上都比传统的 SAST 和 DAST 有着明显的优势，曾被 Gartner 列为网络安全领域的 TOP 10 技术之一。

RASP 技术早在 2014 年就被 Gartner 在应用安全报告里列为应用安全领域的关键趋势，并将其定义为：应用程序不应将其大部分运行时保护委派给外部设备，应用程序应能够进行自我保护（即在应用程序运行时环境中内置保护功能）。RASP 代码疫苗技术，如同疫苗一样将自身保护程序注入到应用程序中，与应用程序融为一体，在运行时通过实时监控和分析流量或用户行为以阻断攻击，而不需要人工干预，使程序自身拥有自保护的能力，实现出厂免疫。同时 RASP 在检测到漏洞还会提供实时的热补丁，无需修改源代码，这是 RASP 的优势也是其弊端，因为 RASP 临时提供虚拟补丁，并没有真正解决安全漏洞，当 RASP 停止使用后，这些安全漏洞问题依旧存在。

为解决上述问题，实现 RASP 技术与 IAST 技术一体化的新思路逐渐展露头角，各大安全厂商也纷纷跟进研究，由于 RASP 与 IAST 同样都使用了插桩技术，由此可以实现将 IAST 技术与 RASP 技术使用同一插桩探针，通过插桩来记录应用程序运行时的堆栈数据，分析应用程序健康度。即在测试阶段采用 IAST 插桩探针的检测功能，在应用上线后自动开启 RASP 功能，启动探针的安全防护功能，主要针对测试阶段检测到的没来得及修复的且不影响应用程序正常运行的安全漏洞进行精准防护，实现运行时自我保护机制。

结语

CONCLUSION

从上一次 DevSecOps 行业洞察报告发布至今，已有一年半的光景。从这一次的调查结果中我们看到了很多令人欣喜的变化：更多的受调者了解 DevOps 和 DevSecOps，更多的企业安排了安全相关的培训活动，更多的工具被深度应用到了日常实践当中。虽然调查结果也呈现出了一些问题，例如软件供应链相关的安全工作尚有很长的路要走，但总体上看，DevSecOps 的发展处于高速轨道当中是毋庸置疑的。

斯坦福大学教授福格提出的 Fogg 模型可简单描述为：人的行为由动机、能力和触发条件这三个要素组成，三要素都同时满足后，行为才会发生。正是当前我们所处的环境提供了强大的三要素支撑，使得 DevSecOps 实践呈现着高速发展的状态。

首先从动机上看，近期我们经历了人类历史上最大规模的国家级软件供应链攻击事件 SolarWinds Orion、“核弹级”的开源组件缺陷 Apache Log4j2 漏洞、由修昔底德陷阱带来的二战后最大规模的逆全球化。这一切，让软件应用的安全性保障逐渐脱离了奢侈品的属性，而成为了社会、国家、企业所关注的生存必需品。

其次在能力上，DevSecOps 的实践经过国外早期的探索和国内这两年的落地，已经形成了一系列的行业标准和成熟度模型、诞生出了一整套较为成熟的实践方法、并涌现出了一些领先的解决方案提供商，这些使得企业的 DevSecOps 落地过程更加地成熟可控。我们观察到，如今很多 IT 安全建设相对滞后的传统行业和一些中小型企业也拥有着相当的 DevSecOps 实践能力，例如悬镜正在帮助某国内领先的农场养殖企业搭建 DevSecOps 体系。

最后，针对软件供应链安全逐步出台的一系列行政要求和行业规范是企业打造自身 DevSecOps 实践的触发器。在高强度竞争的环境中，DevSecOps 是保障软件供应链安全的同时不降低生产效率的重要实践方法。通过全面自动化的工具和高度场景化的流程，在安全管理人员的能力上附加乘数效应，用尽可能少的人力，高效全面地覆盖软件应用全生命周期的安全管理，满足软件供应链安全政策要求。

英国哲学家怀海德曾说：文明的进步，就是人们在不假思索中可以做的事情越来越多。DevSecOps 力求通过对文化、流程、工具的重塑，让软件应用的安全保障工作润物细无声地在组织中流转，以实现安全地生产软件及生产安全的软件。无疑，DevSecOps 的这一目标代表着数字文明进步的方向。而作为实践者的我们所要做的，就是脚踏实地地将这一目标变为现实。

出品人 董毅

2022 年 08 月

引用参考

[1]Macdonald N,Head I.DevSecOps: How to Seamlessly Integrate Security Into DevOps[EB/OL].
https://cdn2.hubspot.net/hubfs/1958393/White_Papers/devsecops_how_to_seamlessly__315283.pdf.

[2]Shannon Lietz.What is DevSecOps?[EB/OL].
https://www.devsecops.org/blog/2015/2/15/what-is-devsecops,2015-06-01.

[3]Shannon Lietz.Principles of DevSecOps[EB/OL].
https://www.devsecops.org/blog/2015/2/21/Principles of DevSecOps,2015-02-22.

[4]GSA,DevSecOps Guide[EB/OL].
https://tech.gsa.gov/guides/dev_sec_ops_guide/,.

[5] 悬镜安全 . 从 RSAC 看 DevSecOps 的进化与落地思考 [EB/OL].
https://mp.weixin.qq.com/s/JdV13bsMQTyeYQtf1OQ0RA.

[6]OWASP SAMM[EB/OL].
http://owasp.org/www-project-samm/.

[7]OWASP DSOMM[EB/OL].
https://owasp.org/www-project-devsecops-maturity-model/.

[8]BSIMM12 2021 INSIGHTS &TRENDS REPORT[EB/OL].
http://www.bismm.com/download.html.

[9] 云原生产业联盟 . 云原生架构安全白皮书 [R]. 北京 : 云原生产业联盟 ,2021.

[10]2021 RSAC 精彩汇集 [EB/OL].
https://baijiahao.baidu.com/s?id=1700063565702260249&wfr=spider&for=pc.

[11]Synopsys.2021 Open Source Security And Risk Analysis Report[R].USA:Synopsys,2021.

[12]NCSC.Software Supply Chain Attacks[R].USA:NCSC,2021.

[13]WhiteSource.Software Supply Chain Attacks[EB/OL].

https://www.whitesourcesoftware.com/resources/blog/software-supply-chain-attacks/.

[14] 安全内参 . 美国总统拜登《关于改善国家网络安全的行政令》全文翻译 [EB/OL].
https://www.secrss.com/articles/31267.

[15] 悬镜安全携手中国信通院发布《软件供应链安全白皮书（2021）》[EB/OL].
https://mp.weixin.qq.com/s/nrfem5V-Uw2PrBswHtR7Sg.

[16]Enisa Threat Landscape For Supply Chain Attacks[EB/OL].
ENISA Threat Landscape for Supply Chain Attacks.pdf.

[17]Building a More Effective Strategy for ICT Supply Chain Security[EB/OL].
https://www.bsa.org/files/policy-filings/02162021supplychainsecurity.pdf.

[18]Enisa Threat Landscape 2021[EB/OL].
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

[19] 中国信息通信研究院 .《开源生态白皮书（2021 年）》[R/OL]. 北京：中国信息通信研究院 ,2021.

[20] 云计算开源产业联盟 .《中国 DevOps 现状调查报告（2021 年）》[R]. 北京：云计算开源产业联盟 ,2020.

[21]DOD Enterprise DevSecOps Strategy Guide[EB/OL].
https://dodcio.defense.gov/Portals/0/Documents/Library/DoD%20Enterprise%20DevSecOps%20Strategy%20Guide_DoD-CIO_20211019.pdf.

出品方

悬镜 XMIRROR | FreeBuf咨询