DevSecOps 的六大支柱：集体责任

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

CSA cloud security alliance®

DevSecOps 工作组官方网址：

https://cloudsecurityalliance.org/research/working-groups/devsecops

© 2025 云安全联盟 —— 保留所有权利。你可以在你的电脑上下载、储存、展示、查看及打印，或者访问云安全联盟大中华区官网(https://www.c-csa.cn)。须遵守以下：（a）草案仅限个人、信息性及非商业用途；（b）不得以任何方式修改或改动草案；（c）不得重新分发草案；（d）不得移除商标、版权或其他声明。根据中华人民共和国著作权法合理使用条款，您可以引用草案部分内容，但须注明该部分内容源自云安全联盟。

云安全联盟

创立于2009年，作为世界领先的独立、权威国际产业组织，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识和全面发展。

云安全联盟大中华区

在香港注册并在上海登记备案的国际NGO组织，旨在 立足中国，连接全球，推动 中国数字安全技术标准与产业的发展及国际合作。

4 大区
大中华区、美洲区、欧非区、亚太区

180+ 分会
英国、法国、加拿大、旧金山、马来西亚等覆盖50多个国家和地区

2.5K+ 成员单位
世界500强科技公司、安全厂商、中小型企业、研究机构

20W+ 社区专业人员
研究工作组专家、社区志愿者、从业人员、CSA认证学员

前沿研究

#云安全 #AI安全
#零信任 #数据安全
#5G安全 #区块链安全
#量子安全 #物联网安全
#金融安全 #医疗安全
#智能座舱安全
#关键基础设施安全
.....

培训与认证

CCSK 云安全知识认证
CDSP 数据安全认证专家
CAISP人工智能认证专家
CZTP 零信任认证专家
CCPTP 云渗透测试认证专家
CCAK 云计算审计知识认证
.....

会议活动

CSA summit@RSAC
CSA GCR Congress
CSA研讨会
AI For GOOD峰会
.....

评估与认证

AI STR AI安全、可信、负责任认证
STAR 云安全评估认证
CAST 云应用安全可信认证
CNST 云原生安全可信认证
.....

1000+研究成果 **10W+认证学员** **1000W+传播量**

成员单位(部分)

企业合作微信号:csagcr　认证培训微信号:CSAlynn　邮箱:info@c-csa.cn

致 谢

中文版翻译专家

翻译组成员：

张坤　谢绍志　贺志生　江泽鑫　余晓光

审校组成员：

李 岩

（以上排名不分先后）

© 2025云安全联盟大中华区版权所有

英文版翻译专家

主要作者:

John Martin

Stacy Simpson

Ashleigh Buckingham

Altaz Valani

Melissa Riley

贡献者:

Dennis Bush

Glenn Leifheit

Steve Lipner

Mathew Lyon

Sam Sehgal

Souheil Moghnie

Xiping Song

Sean Heide

在此感谢以上专家及单位。如译文有不妥当之处，敬请读者联系CSA GCR秘书处给予雅正！联系邮箱research@c-csa.cn； 国际云安全联盟CSA公众号。

© 2025云安全联盟大中华区版权所有

行业合作伙伴

云安全联盟（CSA）作为全球领先的组织，致力于定义和提升对最佳实践的认识，以帮助确保云计算环境的安全。CSA 利用行业从业者、协会、政府及其企业和个人会员的主题专业知识，提供针对云安全的研究、教育、培训、认证、活动和产品。https://cloudsecurityalliance.org/

软件保证卓越代码论坛（SAFECode）是一个非营利性组织，主要致力于通过改进有效的软件保证方法以提高人们对信息与通信技术产品和服务的信任度。SAFECode 是一项全球性的、由行业主导的工作，旨在确定和推广最佳实践，以研发和提供更安全、可靠的软、硬件和服务。

https://safecode.org/

© 2025云安全联盟大中华区版权所有

目 录

致 谢 4

行业合作伙伴 6

简介 8

概述 8

高层支持与参与 10

计划设计与实施 11

将冠军带到挑战中 14

通过安全意识和培训加强该计划 15

计划持续运维与成效评估 17

总结 19

附录一：健康问题与讨论要点 21

附录二：延伸阅读 22

© 2025云安全联盟大中华区版权所有

简介

云安全联盟（Cloud Security Alliance）和 SAFECode 都坚定地致力于改善软件安全成果。2019 年 8 月发布的论文《DevSecOps 的六大支柱》提供了一套高层次的方法和成功实施的解决方案，作者通过这些方法和解决方案来快速构建软件，并尽量减少与安全相关的错误。这六大支柱是

支柱1：集体责任

支柱2：培训和流程整合

支柱3：务实的实现

支柱4：建立合规与发展的桥梁

支柱5：自动化

支柱6：测量、监控、报告和行动

云安全联盟（Cloud Security Alliance）和SAFECode将联合出版一套更为详细的出版物，介绍支撑上述每个支柱的成功解决方案。本报告是这些后续出版物中的第一份。

概述

DevSecOps 将安全原则、流程和技术整合到持续的软件开发和 IT 运营文化中，从而影响其实践和工作流程。它将传统上相互隔离的开发、基础设施运营和信息安全领域汇聚在一起，通过一套共同的流程、程序和工具自动化，促进安全软件的开发。

对 DevSecOps 兴趣的增加，部分是由于云计算优先的软件开发环境推动的，这种环境具有越来越短的产品生命周期、更迭代的开发方法以及开发

© 2025云安全联盟大中华区版权所有

和 IT 运营的日益集成。传统的安全开发方法往往难以满足那些在云环境中工作的人快速采用的持续开发方法的需求。将安全开发实践集成到 DevOps 中需要一种更敏捷的安全方法，包括增加安全流程的自动化、更周到和务实的安全实施规划、更明确地列举风险和合规要求，以及更具操作性的监控和测量方法。此外，要使所有这些元素作为一个整体的 DevSecOps 方法协同工作，需要每个接触该流程的人都有集体安全责任意识。

鉴于对 DevSecOps 的兴趣增加，云安全联盟（CSA）和软件保证卓越代码论坛（SAFECode）组成了一个 DevSecOps 工作组，以识别和分享开发和维持 DevSecOps 项目的最佳实践。作为第一步，工作组根据 CSA 的反射性安全框架中描述的六大支柱，确定并定义了将 DevSecOps 集成到组织中的六个关键关注领域。随着时间的推移，我们将重新审视并建立每个 DevSecOps 支柱的更详细的研究和指导，以维护特定行业的标准。本文是计划中的系列文章的一部分，将重点关注 arguably 其他所有支柱基础的领域 —— 集体责任。

培养集体安全责任意识不仅是将安全融入 DevOps 环境的重要组成部分，也是最具挑战性的任务之一。这需要培养组织在软件安全方面的思维方式、理念、习俗和行为的转变。在本报告中，我们将这种努力称为构建支持安全的文化。这种文化的一些显著特征包括以下特点：

- 实施安全设计的心态：在软件开发和运营的每个阶段都考虑和解决安全问题。安全不是事后的想法，也不是仅仅通过审计发现来处理的问题。
- 一种全员参与——从开发到 IT 运营再到高层管理——在确保软件安全方

© 2025云安全联盟大中华区版权所有

面发挥作用，并作为组织应对当今复杂威胁环境的第一道防线的意识。

• 强调个人责任和信任。这种方法使自主性和敏捷性得以增强，提供必要的安全信息和工具，以便进行知情的分散式行动和决策。这与传统上限制性较强、手动密集且相互隔离的安全流程有所不同。

• 明确认识到安全并非与业务目标分开或截然不同，因此，积极的安全行为和激励措施之间存在明确且可识别的一致性，并且相信团队成员在其安全工作中会得到支持。

尽管关于培养支持安全的文化的必要性已有大量著作，但它仍然是 DevSecOps 执行过程中最常被提及的挑战之一。文化通常被描述为组织的一个关键但无形的要素。不幸的是，这可能导致一种相当临时的文化变革方法。在软件安全方面，这通常表现为偶尔的黑客马拉松或漏洞清理活动，或者可能是关于软件安全实践价值的年度培训课程。这并不是说这些活动没有价值，而是说如果它们没有在团队目标的背景下呈现、没有得到加强，或者没有包括正确的受众，它们的影响是有限的。在周期开始时引入安全知识和培训可以帮助避免这些临时会议的需要。

高层支持与参与

用于创建和维持支持安全的文化的方法各不相同，但几乎所有成功的组织都共享的一个基本要素是支持和参与型的领导团队。管理层的支持不仅是确保对DevSecOps进行足够的时间和资源投入的必要条件，也是确保这些努力得到实地支持的关键。员工能够分辨出对安全计划的象征性支持或勉强支持与严肃承诺之间的区别，并且他们的这种认识不可避免地会反映在他们执行计划部分

© 2025云安全联盟大中华区版权所有

的方式上。

为了获得管理层对安全文化发展的支持，通常需要提出一个全面的、以结果为导向的计划，而不是一系列临时性的活动。设计一个计划级的方法至少需要制定一个与业务战略紧密相关的商业案例、一个详细的实施计划以及关键的项目指标。参与云安全联盟（CSA）和SAFECode等组织也有助于了解类似组织是如何处理安全文化发展的，这同样可以支持商业案例的提出。

计划设计与实施

建立安全文化应被视为一项重要且持续的计划级工作，而不仅仅是一系列临时性活动的简单集合。这需要对旨在培养集体安全责任感的新举措进行精心规划和周密部署。以下是那些希望采用计划管理方法的人需要考虑的一些常见问题。

当一个企业设计一个支持安全文化的计划时，任务是将安全意识和集体责任感融入现有的组织文化中。这要求安全领导者在计划设计中考虑其组织和开发团队的现有文化和业务实践。一个有用的方法是研究过去需求或流程变更的例子，以尝试找出有效的沟通和社交化方法，并将其应用于安全开发工作。

例如，安全领导者可能会考虑财务和会计团队如何与开发团队合作，以促进和庆祝其新发票和费用报告系统在全公司的推出，初步威胁模型如何有助于简化产品设计并降低成本和风险，或者为什么尽管增加了工作量，产品管理的新文档要求却如此迅速地被接受？其他一些常见问题包括以下问题：

- 团队是更倾向于响应公司高层的指令，还是更倾向于接受来自工程内部的更基层的方法？

© 2025云安全联盟大中华区版权所有

- 哪些类型的激励措施更有助于促进行为改变?
- 组织中的关键影响者是谁，他们是否有可能在这方面提供帮助?
- 集体安全责任文化与工程团队以及整个公司的目标和愿景之间有什么关系?
- 安全要求和实践在哪些方面与开发流程相冲突，如何最小化这些目的冲突?
- 中高层管理人员应该如何参与?
- 现有的文化和相关流程是否仍然与业务目标保持一致，还是已经过时？如果过时了，是否还有价值/可以改进？你的团队可以使用的内部讨论要点包括这些考虑因素：

预定义的结构和流程通常内部聚焦，服务于组织结构本身而非更广泛的业务需求（例如无效的变更控制流程，管理层和工程师都对流程不满意，看不到其中的价值，但流程仍未改变，开始充当阻碍者而没有增加太多价值）。

- 在部门隔离的模式下，跨层级的沟通可能会缓慢且低效。信息从上到下以及从下到上流动缓慢。是否可以通过简化流程或补充一些举措，如共享安全责任（授权）、使用自动化工具进行控制和度量，以及向管理层清晰报告有意义的度量数据（数据驱动的业务决策），来改善这一点。
- 政策、规则和程序阻碍了战略决策的快速制定。我们看到了去中心化控制的趋势，借助自动化的安全“缓冲器”和个体责任，并通过更好的安全培训和诸如“安全冠军”等计划的支持。
- 人们固守旧习，害怕失去权力和地位。如果我们反复依靠少数几个可

© 2025云安全联盟大中华区版权所有

信赖的人来领导关键举措，而非从更广泛的利益相关者群体获取意见，文化和进步可能会受到抑制（这再次强调了授权和改进沟通/协作的重要性）。

- 快速创新和颠覆是否存在正当的业务需求，以及更高的风险偏好，或者相反，业务需求是否更倾向于规避风险或由合规驱动？

安全团队往往与开发过程相距甚远，无法被视为合作伙伴；他们被认为在周期后期介入，下达指令或要求更改，但对工程环境的实际情况没有充分考虑。事实上，软件安全领域的早期先驱者学到的最深刻的教训之一是，忽略开发者的成功需求是最快失败的方式。在DevOps环境下，这一挑战可能更为严峻，因为开发团队非常重视自动化和迭代的速度。

乍一看，DevSecOps方法似乎将安全性完全集成到开发和运营团队中，消除了对单独安全组的需求。虽然这可能是许多人所期望的未来状态，但实际上大多数组织都发现需要维持一个专门的软件安全团队，以确保所需的专业知识并专注于安全问题。在实践中，最大的组织挑战是如何以支持所需安全文化特征的方式整合安全、开发和运营团队的工作。

在早期的软件开发模型中，安全人员和开发人员之间存在着天然的紧张关系。安全人员通常认为软件管理在道德上是模棱两可的，“现在发布，以后再修复”，而业务目标只是实现构建下一个更好的增量软件版本所需的收入流。DevSecOps允许合并这两种思维方式。安全成为产品的组成部分，用户的安全和隐私要求成为明确的功能要求。

这并不意味着使用独立安全团队的组织注定要失败。这也不一定意味着将安全完全纳入发展是正确的做法。事实上，这两种模式都有成功的组织。重要的是要考虑人员配置计划和周围的组织结构图支持或阻碍文化发展的方式，以

© 2025云安全联盟大中华区版权所有

便减轻任何一种方法带来的任何挑战。

此外，这不需要是一场要么全有要么全无的讨论。事实上，使用混合方法的势头越来越大，即使用安全冠军来弥合安全与发展之间的差距。

将安全冠军带到挑战中

安全冠军是开发团队的成员，他们有权持续参与帮助指导和执行日常安全活动。与可用性有限或受限的安全团队专家不同，安全冠军可以可靠地支持开发团队级别的DevSecOps执行和安全活动。许多组织发现安全冠军计划是扩展其软件安全工作的关键。此外，安全冠军对组织文化有直接影响。事实上，他们经常站在将集体安全责任社会化的任何努力的第一线，并有权在需要时将问题上报给安全团队和管理层。

当SAFECode努力比较其成员之间成功的安全冠军计划时，它发现它们有一些共同的特点。软件安全需要一个冠军——构建和维护成功的安全冠军计划的简短指南

首先，安全卫士的角色应被视为主要职责，最好是全职或接近全职的工作。仅仅将已经不堪重负的软件开发人员标记为新的常驻安全专家是不够的。安全冠军需要与更广泛的安全团队密切合作，并能够根据风险优先考虑安全问题。通过这种方式，它们是工程团队中上下文感知的安全驱动程序，也是安全团队的接口。

其次，虽然安全冠军最初可能需要在工程团队中担任战术安全职位，但目标应该是随着团队安全知识的增长而发展他们的角色。安全冠军不应该为开发人员做安全工作，而应该充当培训开发人员的导师，这样他们就可以自己解决

© 2025云安全联盟大中华区版权所有

安全问题，在需要时寻求额外的澄清或帮助。理想情况下，安全冠军将与首席架构师和利益相关者密切合作，拥有威胁和隐私模型，并成为由此产生的活动（识别安全相关功能、组件选择等）的主要焦点。如果没有这种心态，不仅难以扩大其影响，而且安全可能会继续被视为其他人的工作（在这种情况下是安全冠军的工作），而不是每个开发人员的集体责任。

第三，仅仅找到一个安全冠军并告诉他们去解决安全问题是行不通的。要取得成功，安全冠军需要一个正式的、管理层支持的计划的支持，该计划具有明确的组织和专业目标，以及一个支持性的组织生态系统。这样，安全冠军计划的成功与安全文化发展计划的努力密切相关，因此许多组织应该将其视为一项工作。至少，如果同时推行安全冠军和文化发展计划，就应该一并考虑。

通过安全意识和培训加强该计划

培训是任何成功的DevSecOps计划的重要组成部分。事实上，鉴于安全开发实践很少被纳入软件工程教育，它长期以来一直是软件安全领域的一个重点。CSA DevSecOps工作组认为培训是必不可少的

DevSecOps规划的支柱，正在制定更详细的指导方针，稍后分享。SAFECode在其最新版本的《安全软件开发基本实践》[3]中还谈到了培训的重要性，指出“整个组织都应该意识到安全的重要性，必须为开发团队提供更详细的技术培训，明确阐述个人和团队的具体期望。”

虽然为直接负责实施安全开发方法的人员提供详细技术培训的必要性是相当明显的，但许多组织在意识培训工作中可能没有接触到足够广泛的受众。为了使DevSecOps取得成功，整个团队——架构师/设计师、技术作家、项目经

© 2025云安全联盟大中华区版权所有

理、开发工程师、服务和质量保证（QA）工程师、IT运营等——都应该具备扎实的基础安全知识。培养对安全重要性和每个团队在安全方面所扮演的具体角色的认识，对于建立支持安全的文化至关重要。

考虑其他形式的外展活动，如午餐和学习课程、与安全专家安排的开放时间以及安全指导计划。安全的游戏化也越来越受欢迎，作为一种让安全知识更加触手可及和引人入胜的方式，可以通过在外展组合中添加定期的黑客马拉松来实现。

据了解，培训课程和外联活动的时间有限，因此组织者一定要提供一种方法来获取参与人数，并收集参与者和外联负责人的反馈。这些评估将有助于确定最受欢迎和最有影响力的外联活动，以便可以复制，而不太有用的活动则可以放弃。

此外，考虑如何利用其他现有的团队和面向同行的活动来进一步建立安全意识和发展安全专业知识。已建立的开发方法，如对等编程和配对，可用于安全代码审查。如果定期使用bug抨击，可能有机会邀请一个通常不会参加此类活动的额外团队参与。

威胁建模应该已经作为一项团队活动进行，包括多个角色。重要的是要确保这些会议的参与率保持较高水平，不会因日程安排问题而牺牲。威胁建模会议也可以战略性地扩展，以包括传统上可能不会被邀请的其他人，以增加安全利益。值得注意的是，那些喜欢并在威胁建模课程中表现良好的人通常是安全冠军和其他安全外展角色的优秀候选人。

最后，考虑除了安全意识和技术之外的其他技能是否有助于提高安全计划的影响。例如，提供一组已识别的安全影响者或者接受过领导力培训的安全冠

© 2025云安全联盟大中华区版权所有

军可能会提高他们在团队中的效率。提供演示培训的机会可能会鼓励其他人挺身而出，自愿领导内部棕色袋子会议。

虽然培训计划和外联活动的确切组合因组织而异，甚至可能因团队而异，但在文化发展计划的背景下，对这些举措采取整体和全面的方法非常重要。这并不一定需要采用集中的方法来规划培训和外联计划。事实上，有时，当在团队层面确定需求并采取行动时，外联工作可能是最有效的。然而，了解整个组织正在做什么很重要。这不仅有助于确保培训和外联保持相关性和影响力，但也将确定执行中的差距，优化资源，为其他领域的工作提供信息，并为培养安全文化提供额外的机会。

计划持续运维与成效评估

制定监视和报告策略是 DevSecOps 规划的一个不可或缺的元素。可操作的指标通过度量进度和及时检测故障来启用 DevSecOps 计划。度量是 DevSecOps 的重要组成部分，它也是 CSA-SAFECode DevSecOps 工作组确定的 DevSecOps 策略的六个关键支柱之一4，并且是即将发布的指南的主题。因此，本文不会尝试涵盖 DevSecOps 度量和报告实践的全部范围。但是，它将解决两个与文化相关的关键度量问题

- 如何度量文化驱动的内容
- 度量像文化这样无形的东西的挑战

首先必须认识到，公司的度量标准会驱动其行为方式。这样，组织选择用于监控其 DevSecOps 计划成功的指标将对其安全文化产生直接影响。考虑到许多组织将激励措施直接与项目绩效指标挂钩，度量与行为之间的联系变得更

© 2025云安全联盟大中华区版权所有

加明显。

例如，如果生产时间是唯一重要的指标，那么几乎没有动力去放慢速度来解决已识别的风险。或者，如果最有价值的指标侧重于功能交付而不是质量，那么这可能会促使组织生产被未来技术债务和推卸责任的文化所淹没的软件。相反，如果优先考虑有意义的质量指标，那么就更有可能创造一种丰富的产品owner文化和著降低的递延债务水平。

当集体责任得到适当实施时，所有安全例外都必须在执行级别具有一定程度的明确问责制。安全指标不再只是用于衡量安全程序的性能/有效性。鉴于安全性在文化和技术上都嵌入到 DevSecOps 中，因此每个人都参与检测和收集安全指标，并共同拥有和跟踪安全性能。

此外，组织文化从来都不是一成不变的;它会随着组织的发展而改变，而最初推出 DevSecOps 时有效的方法可能不如项目成熟时有效。安全和开发实践也在不断发展，可用于支持它们的工具也在不断发展，这反过来会影响 DevSecOps 运营的环境并创造文化变革。正如没有一种单一的方法来构建支持安全文化一样，今天有效的方法可能与明天有效的方法不同。

在衡量计划有效性、识别失败点并确保实现持续改进所需的任何变革的过程方面，必须有一个精心设计的方法。拥有强大的衡量计划将有助于指导任何必要的变革，并使组织能够维持和建立其最初的成功。正如本文前面所讨论的，保持高管的支持是长期项目维持的基本要素。衡量文化发展计划影响的能力将使安全团队能够向高级领导者提出更强有力的商业案例，以继续组织对这些活动的投资。

毫无疑问，衡量像文化这样无形的东西会带来挑战。使用的具体指标将取

© 2025云安全联盟大中华区版权所有

决于组织的不同目标。例如，一个专注于确保管理支持工程工作的文化计划可以衡量在计划推出之前和之后请求的风险异常数量。如果它是衡量开发人员对采用安全工程实践的兴趣，那么衡量开发人员对自愿安全活动（如培训和 bug 攻击）的兴趣的社会衡量标准将是有效的。

总结

DevSecOps 是云原生软件开发的自然演变。如果执行得当，它可以利用自动化、更多迭代的开发方法以及开发和 IT 运营的日益增长的集成，更快地将产品交付给客户。

本文确定了创建和维护高管支持和参与的方法，根据我们积累的经验构建包容性文化计划，通过安全冠军建立深度参与，以及如何使用指标来维持、构建和帮助发展该计划。

最后，我们想根据我们的经验分享一些观察结果：

- 没有内置坚实安全性的 DevOps 只会增加技术债务。将 Sec 放入 DevOps 必须深思熟虑。
- 所有成功的 DevSecOps 计划都与参与该过程的每个人共享一种集体安全责任感。这可能是 DevSecOps 实施中最重要和最具挑战性的方面
- 让领导者发挥领导作用。为他们提供该项工作的工具
- 为了让DevSecOps发挥作用，领导层必须允许变革。对结构化的创造力会反对
- 文化将与时俱进。正如先前的行动创造了当前的文化一样，即使不是有意的，一系列不同的行动也可以改变文化

© 2025云安全联盟大中华区版权所有

- 由于文化在不断变化，因此必须始终制定一个计划来维持积极影响，并本着持续改进的精神随着时间的推移衡量这种影响

© 2025云安全联盟大中华区版权所有

附录一：健康问题与讨论要点

在评估软件安全计划的组织时要问的问题

- 您目前是否使用威胁建模来帮助构建功能需求?
- 您是否使用功能安全要求来指导软件组件的选择?
- 发现漏洞的原因是否反馈到设计和开发过程中?
- 产品安全事件响应人员（SIRT 或蓝军）是否直接或通过安全冠军参与安全设计、流程和培训?
- 您的执行团队对开发计划的安全问题的承诺是否会影响产品“构建”运营?
- 安全冠军是否应拥有威胁模型和隐私模型?
- 你的产品团队是否应该在每个组中都有安全支持者，或者这可以是一个共享资源?
- 个人和团队对安全知识的访问是否允许他们独立于安全支持者工作?
- 没有关联异常的未修复安全 bug（来自扫描工具输出）是否应获得批准（或可批准）？
- 在什么时候，当前版本或先前版本中已批准的异常应该变得不可接受?
- 您能够构建和重用参考库吗？以及访问威胁和隐私模型?

© 2025云安全联盟大中华区版权所有

附录二：延伸阅读

对安全文化的讨论需要对软件和 IT 安全有多学科的理解，本文建立在以下工作中提出的许多概念之上。对于任何有兴趣了解有关 DevSecOps、安全文化和管理软件安全程序的更多信息的人来说，这些论文都是有用的阅读材料

1．Fundamental Practices for Secure Software Development Essential Elements of a Secure Development Lifecycle Program: https://safecode.org/wp-content/uploads/2018/03/SAFECode_ Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf

2．安全软件开发的基本做法 安全开发生命周期计划的基本要素：https://safecode.org/wp-content/uploads/2018/03/SAFECode_ Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf

3．The Six Pillars of DevSecOps: Achieving Reflexive Security through the Integration of Security, Development and Operations: https://cloudsecurityalliance.org/artifacts/six-pillars-of-devsecops/

4．DevSecOps 的六大支柱：通过集成安全、开发和运营来实现反射性安全性: https://cloudsecurityalliance.org/artifacts/six-pillars-of-devsecops/

5．Information Security Management Through Reflexive Security: Six Pillars in the Integration of Security, Development and Operations: https://cloudsecurityalliance.org/artifacts/information-security- management-through-reflexive-security/

6．通过反射性安全进行信息安全管理：安全、开发和运营集成的六大支柱：https://cloudsecurityalliance.org/artifacts/information-security- management-through-reflexive-security/

7．Software Security Takes a Champion A Short Guide on Building and Sustaining a Successful Security Champions Program: http://safecode.org/wp-

© 2025云安全联盟大中华区版权所有

content/uploads/2019/02/Security-Champions-2019-.pdf

8．软件安全需要冠军 关于构建和维持成功的安全冠军计划的简短指南:

http://safecode.org/wp-content/uploads/2019/02/Security-Champions-2019-.pdf

© 2025云安全联盟大中华区版权所有

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网:https://c-csa.cn 电话:0755-86548359
地址:上海市浦东新区东育路255弄5号3FB30(前滩国际经济组织集聚区)/
中国广东省深圳市南山区高新技术产业园(南区)高新南环路深圳湾科技生
态园二区9栋B座6层603单元