《代码英雄》第二季（5）：关于 DevSecOps 的故事

代码英雄讲述了开发人员、程序员、黑客、极客和开源反叛者如何彻底改变技术前景的真实史诗。

什么是《代码英雄》

Command Line Heroes

代码英雄是世界领先的企业开源软件解决方案供应商红帽（Red Hat）精心制作的原创音频播客，讲述开发人员、程序员、黑客、极客和开源反叛者如何彻底改变技术前景的真实史诗。该音频博客邀请到了谷歌、NASA 等重量级企业的众多技术大牛共同讲述开源、操作系统、容器、DevOps、混合云等发展过程中的动人故事。

本文是《代码英雄》系列播客第二季（5）：关于 DevSecOps 的故事的音频脚本。

导语：不良的安全和可靠性实践会导致影响数百万人的中断。现在是时候让安全加入 DevOps 运动了。并且，在 DevSecOps 的世界中，我们可以创造性的提升安全性。

每月发现一个漏洞曾经是常态。而现在，由于敏捷流程和 DevOps 团队，软件开发的进展迅速。Vincent Danen 告诉我们，这如何导致被认为是漏洞的东西急剧增加。前亚马逊灾难主管 Jesse Robbins 介绍了公司如何为灾难性故障和漏洞做好准备。而 Elastic 的产品安全主管 Josh Bressers 则展望了科技领域安全的未来。

我们不应该把安全团队当成脾气暴躁的妖怪。听听 DevSecOps 团队如何将英雄们聚集在一起，以实现更好的安全。

00:00:01 - 众议院小组委员会代表：

1991 年 6 月 26 日，在华盛顿特区，马里兰州和西弗吉尼亚州的大部分地区，以及我的家乡的大部分地区都因公共电话网络的大规模故障而瘫痪了。然而，随着技术变得越来越复杂，网络系统越来越相互依存，反复发生故障的可能性也会增加。似乎并没有警告说会发生这种情况。

00:00:23 - Saron Yitbarek：

在 20 世纪 90 年代初，有 1200 万美国人遭受了大规模的电话网络故障。人们不能给医院打电话，企业不能给客户打电话，父母不能打电话给托儿所。对于一个基础设施严重依赖于万物互联的计算机系统的国家来说，这是一场混乱也是一记警钟。这些计算机网络变得越来越大，然后当它们出现故障时，故障时间就会很长。

00:01:01：

电脑故障会导致电话系统崩溃。在今天代码中的一行小错误的后果比以往时候都要严重。

00:01:15：

我是 Saron Yitbarek，这里是是红帽公司的原创播客节目《代码英雄》。

00:01:24：

因此，软件安全性和可靠性比以往任何时候都重要。传统的瀑布式开发方法，安全性只是一个附加流程而已，已经不再适用。我们生活在一个 DevOps 的世界里，一切都变得更快、更敏捷、扩展性更强，这在电话网络崩溃时是他们无法想象的。这意味着我们的安全和可靠性标准必须不断改进，以应对这些挑战。

00:01:55：

在本集中，我们将研究如何将安全性集成到 DevOps 中，我们还将探索在运营中构建可靠性和弹性的新方法。即使在介绍了所有这些之后，我们知道还有很多东西可以讨论，因为在 DevSecOps 的世界里，对于开发人员和运营人员来说，事情都在快速变化。这些变化意

味着不同的事情，这取决于你的立场，但这是我们的看法。我们也很想听到你们的消息——所以如果你认为我们错过了什么，不要害羞——在网上联系我们。

00:02:34：

好了，让我们开始探索这个全新的领域吧。

00:02:43：

事情就是这样，让安全性和可靠性跟上时代的步伐，并为 DevOps 世界做好准备，这意味着我们必须对工作方式进行一些关键的调整。第一，我们必须拥抱自动化。我的意思是，想想双因子认证的逻辑。想想那些难以想象的艰巨任务吧。很显然，你不能仅仅通过增加员工来解决问题，所以第一点就是拥抱自动化。

00:03:15：

然后，第二点，这个可能不是那么明显，那就是它真的改变了文化，使安全不再是一个祸害。稍后我将解释我所说的改变文化的含义。但是让我们一个一个的解释这两点。首先，拥抱自动化。

00:03:42：

以前，应用程序的部署在每个单独的发布之前都涉及到一个人为的安全审查，我不知道你是否注意到了，但是人为的审查可能会有点慢。这就是为什么自动化是在 DevOps 构建安全性的关键部分。以 Verizon 最近的数据泄露报告为例。他们发现，81% 的与黑客相关入侵涉及密码被盗或者弱密码。从表面上看，这是一个非常简单的问题，但是规模却很大。就像我之前所提及到的，你不能用工作人员去解决 3000 万个密码问题，对吧？问题在于解决大规模问题，而每次的答案都是一样的。那就是自动化，自动化。

00:04:36 - Vincent Danen：

如果你等待人参与进来，那么规模就不会扩大。

00:04:41 - Saron Yitbarek：

Vincent Danen 是红帽公司产品安全部门的主管，在过去的 20 年里，他见证了 DevOps 的快速发展。安全团队不得不竞相追赶。

00:04:56 - Vincent Danen：

刚开始的时候，每个月都有漏洞，后来变成了每隔一周，然后是每周都有。现在，每天都能找到几百个漏洞。

00:05:08 - Saron Yitbarek：

有趣的是，Vincent 说，随着安全团队的发展，实际上会出现更多的漏洞，而不是更少。

00:05:17 - Vincent Danen：

我们永远不会说，哦，我们现在安全了，我们做完了，我们的工作结束了。安全审计会一直存在，就像呼吸一样，这是必须要有的。

00:05:27 - Saron Yitbarek：

事实证明，对于安全性和可靠性团队来说，细节的问题变得越来越重要。

00:05:35 - Vincent Danen：

当我们在寻找这些漏洞时，我们会发现更多的东西，而且这个趋势还将继续。因为你会发现新的漏洞类型和一些我们可能认为不太重要的东西，或者以前甚至不知道它们存在的东西。我们会发现这些东西发展的速度很快，而且数量更多，因此规模爆炸性增长。知识、软件的数量、消费者的数量都促进了该领域安全性以及漏洞的增加。

00:06:06 - Saron Yitbarek：

一旦你将安全视为一个不断发展的问题，而不是随着时间的推移而“得到解决”的问题，那么自动化的理由就会变得更加充分。

00:06:18 - Vincent Danen：

嗯，我认为有了自动化，你可以以一种非常快的方式将这些东西集成到你的开发流水线中，这是其一。其二，你不需要人类来做这些工作，对吧？计算机不需要睡觉，所以你可以在处理器允许的情况下以最快速度浏览代码，而不是等待人类通过一些可能相当乏味的命令行来查找漏洞。

00:06:44：

然后通过模式匹配和启发式方法，甚至在开始编写代码的时候，你就可以知道代码中那些地方是易受攻击的。如果在你编写代码的时候，在你的 IDE 或者工具中有一个插件，它能告诉你。嘿，这看起来有点可疑，或者你刚刚引入了一个漏洞。在你提交代码之前你都可以纠正这些可疑点或者漏洞。

00:07:08 - Saron Yitbarek：

安全在进步。这真是一笔巨大的奖励。

00:07:12 - Vincent Danen：

每一天，甚至每一小时，都会有很多东西涌现出来。通过持续集成和持续部署，你写了代码，10 分钟后它就被部署了。因此，在代码被推送之前自动进行验证是非常关键的。

00:07:32 - Saron Yitbarek：

我们可以使用各种各样的工具来完成这个任务，不管是静态代码分析，还是 IDE 的插件，或者是一大堆其他选项。我们将在 redhat.com/commandlineheroes 上分享一些我们最喜欢的片段。

00:07:53：

一旦我们有了这些工具，它们将帮助我们把安全放在首位。结果就是，DevOps 被重新定义为 DevSecOps。安全被纳入到流程中。

00:08:08 - Vincent Danen：

就像开发人员和运维人员结合的方式一样，你将这两个规则合成到了一个规则。现在，你有了 DevOps，并将安全这第三个组件与开发和

运维集成到一起，我认为这非常重要。因为事后才考虑安全性，这会使安全性变得非常被动、昂贵以及可能会损害消费者。当你一开始就把安全代入其中，你就可以完成开发工作，从头到尾进行安全检查并开始运作。

00:08:44 - Saron Yitbarek：

当然，就像我们在这一集的开头提到的，自动化只是一个大蛋糕的一半，而 Vincent 也明白这一点。

00:08:53 - Vincent Danen：

并不仅仅是一部分。不能仅仅在你的 CI/CD 流水线中随便引入一个工具就期望一切都变好。为了达到我们希望看到的最终有益结果，需要使用各种技术和行为。

00:09:15 - Saron Yitbarek：

自动化确实让我们做到了一半，但我们必须记住另一部分 —— 稍微模糊一点的那一部分。让我们一起来说，那就是文化部分，让开发者和运维人员都一起参与进来，这样这些问题就不再是可怕的问题。

00:09:33：

我们必须改变一种文化，而有些人正在学习以一种最不痛苦的方式，通过游戏的方式来做到这一点。

00:09:44：

现在让我们来看看事情的另一面。如今建立庞大的基础设施很容易，但这并不意味着我们应该做粗制滥造的工作。我们仍然应该努力改进我们的系统，确保可靠性，未雨绸缪。这就是 Jesse Robbins 正在努力实现的。

00:10:08：

如今，Jesse 是 Orion Labs 的 CTO，但在此之前，他因在亚马逊被称为灾难大师而名声大噪。在那里，Jesse 特别是在让大家至少意识到这些问题这件事上几乎是个奇才。他通过一个叫做 “游戏日” 的活动

来做到这一点。让其中可能涉及成千上万的员工进行故障演练，通过灾难演练来习惯系统被破坏并了解发生的原因和方式。

00:10:39：

下面是 Jesse 和我在讨论，尤其是在运营方面如何建立可靠性和弹性。

00:10:47：

大家都知道你做了很多非常酷的事情，其中之一就是你在亚马逊做的活动 —— “游戏日”。那是什么? 是什么游戏?

00:10:58 - Jesse Robbins：

“游戏日” 是我创建的一个项目，通过大规模破坏来测试最脆弱系统的运行情况。如果你是 Netflix 的 “混乱猴子” 的粉丝，“游戏日” 则是我的一个可以实现类似的所有事情的东西。实际上，它非常专注于建立一种卓越的运营文化，建立大规模测试系统的能力，当系统崩溃时能了解它们是如何崩溃的以改进它们。然后还要建立一种文化，能够对事件做出反应并能恢复。它是按照事故指挥系统建模的，这是世界各地的消防部门用来处理任何规模事故的系统。

00:11:56：

它的诞生源于...

00:11:58 - Saron Yitbarek：

旁白，Jesse 早在 2005 年就经过训练成为一名消防员。在那儿，他了解了这个事故指挥系统，最终激发了 “游戏日” 的灵感。因此，所有做这些故障演练的开发人员，都要感谢 Jesse 对消防和应急管理的激情。好了，回到我们的谈话。

00:12:22 - Jesse Robbins：

弹性是一个系统的能力，这包括人和这些人建立的适应变化、应对失败和干扰的能力。而建立这种文化最好的方法之一 —— 建立一种文化，能够对这种类型的环境做出反应，并真正理解这些环境是如何工

作的 —— 就是提供人员培训演习。这些演习可以很简单，比如重启服务器，也可以很复杂，比如关闭整个数据中心造成大规模故障等等。所以，“游戏日” 首先是一个过程。在这个过程中，你通过让整个组织聚集在一起，讨论系统如何发生故障，并思考人类对故障发生的预期。而这个演习本身就是 “游戏日” 开始时最有价值的部分之一。

00:13:24：

但是，当你实际对系统做了一个或大或小的破坏后。当你这样做的时候，你就可以看到每个人是如何反应的。你看到系统崩溃了，可能是之前安全的东西崩溃了，一个很容易理解的组件或者是某个东西暴露了一个潜在的缺陷。这些问题隐藏在软件、技术或者大规模的系统中，只有当你遇到极端或者意外事件时，我们才能发现。“游戏日” 的目的是为了训练员工并且建立系统让你了解他们如何在压力下工作。

00:14:12 - Saron Yitbarek：

所以当我听到 “游戏日” 的时候，我就会想，“这是对某个特定事件的回应吗? 它是从哪儿来的?”

00:14:20 - Jesse Robbins：

因此，“游戏日” 刚开始的一段时间内，因为我知道自己的角色以及作为消防员和应急管理人员的背景，因此将文化方法从注重预防失败的观念转变为拥抱失败非常重要，接受失败发生。激发我这样做的部分原因是我自己的经历，你知道，了解系统，比如建筑是如何倒塌的，市政基础设施是如何倒塌的，以及灾难是如何发生的，以及灾难给人们的压力。所以说，如果环顾我所在工作场所所具有的复杂性和运营规模就会知道，想要真的构建成一个高可靠性、持续在线环境的唯一办法就是拥抱消防服务的方法。我们知道失败会发生，这不是如果的问题，而是什么时候的问题。就像我之前的消防队长说的，不是你选择时机，而是时机选择你。你只需要在它发生的时候准备好即可。

00:15:28 - Saron Yitbarek：

哦，这个不错。所以当你第一次开始做 “游戏日” 并思考如何为灾难场景做准备时，每个人都同意了吗？你得到任何反对意见了吗？

00:15:40 - Jesse Robbins：

每个人都认为我疯了。因此，肯定有人反对。有趣的是，有一种非常简单的方法可以克服这种抵制，那就是首先创造出我称之为“冠军”的东西。你要教一小群人，如何以非常安全的方式工作，然后你能够使用一些信服的指标。你能够说，看，让我们只需衡量发生了多少分钟的中断，我的团队经过了这种培训并以这种方式进行操作的停机时间有多少分钟。相反，你的团队没有这个，并且似乎认为进行这种类型的培训和练习没有价值或者不重要。

00:16:25 - Jesse Robbins：

你一旦完成了这种事情，基本上就会有我所说的引人注目的事件。因此，经常会有断电或其他事情让组织突然意识到：哦，我的天哪，我们不能再像以前那样继续做事了。这就是你用来说服怀疑论者的方法。你一方面使用数据和性能数据，再结合指标，然后讲故事，然后等待一个大的故障或者可怕的事情发生。然后，你就可以说，如果我们要在 web 规模或者互联网规模上运维，整个组织都需要这种应变能力。

00:17:06 - Saron Yitbarek：

嗯嗯。所以我喜欢它的原因是它不只是停留在亚马逊内部。相反，它在传播。很多其他公司也在这么做。很多人最终接受了要为故障做好准备这个知识和过程。那下一步是要做什么？我们如何将从“游戏日”中学到的知识继续运用到未来的项目和公司中？

00:17:31 - Jesse Robbins：

我喜欢把它称为趋同进化。每个在 web 上运行的大型组织现在都采用了我提倡的事件管理基础的一个版本，并创建了他们自己的“游戏日”测试。比如，Netflix 将其称为“混乱猴子”。谷歌有他们的 Dirt 计划。

00:17:57 - Saron Yitbarek：

那么你对未来的“游戏日”有什么寄望呢？

00:18:00 - Jesse Robbins：

首先让我感到兴奋的是，我们可以看到人们从闭门造车思维的转变。系统从根本上是相互联系，相互依赖的，而且由世界各地试图有所成就的聪明人构建和运行的。

00:18:22：

几年前，当我刚参加工作时，对运维工作毫不关心，我觉得那非常无趣。然后突然的，我们发现自己能够传播这样一种理念：开发人员和运营人员一起工作是在互联世界中构建和运行有意义的技术的唯一途径。

00:18:44：

所以我对未来的希望是，第一，我们看到越来越多的人接受这些想法并学习它。明白了当你建造了人们依赖的东西时，你有义务确保它是可信赖的、可用的、可靠的，它是人们可以作为日常生活的一部分来使用的东西。

00:19:05：

而且我们也看到了一种新的学科的诞生。“游戏日” 的这种思维模式正在被研究，也有博士正基于这个撰写博士学位论文。它正在不断建立中。

00:19:16 - Saron Yitbarek：

这真的是太棒了。

00:19:16 - Jesse Robbins：

也有写这方面的书，但是包含这些新资源的没有。只有少数人在会议上谈论他们认为世界应该怎么运转。所以我的那种鼓舞人心的希望是，你要明白如果你正在构建软件和技术，那么你真的成为了社会基础设施的一部分。所以作为一名消防员，我所努力贡献的一系列技能和正在出现的技术，这些技术将使它走得更远，它们是建造人们日常生活所依赖的东西的基础的一部分。

00:19:53 - Saron Yitbarek：

很好。这是一个很好的结束方式。Jesse，谢谢你抽出时间来。

00:19:56 - Jesse Robbins：

是的，谢谢。

00:11:59 - Saku Panditharatne：

我认为所有这些因素都不利于采用最佳软件。

00:20:02 - Saron Yitbarek：

在 Jesse 看来，像 “游戏日” 或者 “混乱猴子” 这样的演习是我们不断发展的科技文化的重要组成部分，但它们对于整个社会也至关重要。我很喜欢他很重视这个，因为他是对的。我们的世界取决于我们所做的工作。早在 90 年代，当电话网络开始崩溃时，这一点就很明显了。

00:20:26 - 众议院小组委员会代表：

我们所知道的现代生活几乎陷于停顿。

00:20:31 - Saron Yitbarek：

这是一种伴随的责任。我们有责任关心安全和可靠性，关心我们所建造东西的弹性。当然，当谈到在 DevOps 中的构建安全性时，我们才刚刚开始。

00:20:53 - Saron Yitbarek：

这是 Josh Bressers。他是数据搜索软件公司 Elastic 的产品安全主管。对 Josh 来说，尽管计算机行业已经成熟了半个世纪左右，但我们在这里讨论的安全问题却让人觉得它是刚刚才出现的。

00:21:11 - Josh Bressers：

实际上，就像我想说也行作为一个专业，安全仍然是非常新的东西，有很多事情我们还不是很了解。

00:21:19 - Saron Yitbarek：

但我们确实明白，在 DevSecOps 的世界中，有一些非常好的机会可以创造性的思考安全能达到什么成就。

00:21:29 - Josh Bressers：

我最近和一些人讨论了一个概念，他们利用用户行为来决定用户是否应该能够访问系统。每个人都有特定的行为，比如他们来自哪里，他们访问系统的时间，他们打字的方式，他们移动鼠标的方式。所以我认为，如果我们做得好，他们的这些行为，可以产生一些非常强大结果，如果我们能做到这一点，我们可以注意到有人在做什么。然后假设我表现的很奇怪，因为我刚刚扭伤了手臂。但你知道，另一端并不知道。

00:22:05 - Josh Bressers：

因此，它可能会说，这种行为就有些奇怪，我们就会希望你使用双因子认证登录，并且还会向您发送条短信或其他内容，对吧？这就从用户名和密码变成了更有趣的东西。所以我认为用新的和独特的方式来看待这些问题将是关键。在很多情况下，我们只是还没到那一步。

00:22:27 - Saron Yitbarek：

实现这一目标需要我们所描述的两大步骤。第一步，就是自动化，这很重要，因为……

00:22:35 - Josh Bressers：

人类很不擅长重复地做同一件事。

00:22:38 - Saron Yitbarek：

很公平。然后，我们有了第二步，就是文化，无论我们的职称是什么，我们所有人都有不安全感和责任感。

00:22:49 - Josh Bressers：

当大多数人想到安全团队时，他们不会认为那是一群快乐的好好先生，对吧？一般来说，这些人都很可怕，脾气暴躁，令人讨厌，如果他们出现了，就会毁了你的一天。没有人想要这样，对吧？

00:23:10 - Saron Yitbarek：

但我认为我们可以克服这种偏见，因为我们必须这样想——每天都有更多的安全威胁发生，而且 IT 基础设施每天都在变得更大、更强。把这两个事实放在一起，你最好可以生活在一个被安全环绕的世界里。一个非常 DevSecOps 的世界，在这个世界里，开发人员和运营人员都在提升他们的安全，提高他们的可靠性。我所谈论的是一个自动化被整合到每个阶段的未来，每个人对这些问题的态度变得更加全面。这就是我们保护未来系统安全的方法。这是我们保持电话响，灯开，所有现代生活健康强壮的方法。如果你查一下《福布斯》全球 2000 家公司的名单，也就是前 2000 家上市公司，你会发现其中整整四分之一的公司都采用了 DevOps。集成的敏捷工作场所正在成为规则。并且在几年之内，关于 DevSecOps 的思考可能会成为第二天性。我们希望尽可能快，但是当团队中的每个成员都齐心协力时，长距离比赛实际上会更快。

00:24:40 - Saron Yitbarek：

下一集，我们将面临数据的大爆炸。人类已经进入了泽字节（Zettabyte）时代。到 2020 年，我们将在服务器上存储大约 40 泽字节的数据，而这些信息大部分甚至现在还不存在。但是我们该如何让这些数据有用呢？我们如何使用高性能计算和开源项目让我们的数据为我们所用呢？我们会在 Command Line Heroes 第 6 集中找到答案。

00:25:13 - Saron Yitbarek：

提醒一下，我们整季都在致力于《代码英雄游戏》的开发。这是我们自己的开源项目，我们很喜欢看着它的诞生，但是我们需要你来帮助我们完成。如果你点击 redhat.com/commandlineheroes，你可以发现如何贡献。你也可以深入了解我们在这节课中讨论过的任何内容。

00:25:39 - Saron Yitbarek：

《代码英雄》是红帽原创播客。你可以在 Apple Podcast、Google Podcast 或任何你想做的事情上免费收听。我是 Saron Yitbarek。坚持编程，下期再见。

什么是 **LCTT SIG** 和 **LCTT LCRH SIG**

LCTT SIG 是 LCTT Special Interest Group 特别兴趣小组，LCTT SIG 是针对特定领域、特定内容的翻译小组，翻译组成员将遵循 LCTT 流程和规范，参与翻译，并获得相应的奖励。LCRH SIG 是 LCTT 联合红帽（Red Hat）发起的 SIG，当前专注任务是《代码英雄》系列播客的脚本汉化，已有数十位贡献者加入。敬请每周三、周五期待经过我们精心翻译、校对和发布的译文。

欢迎加入 LCRH SIG 一同参与贡献，并领取红帽（Red Hat）和我们联合颁发的专属贡献者证书。

---

via: https://www.redhat.com/en/command-line-heroes/season-2/the-one-about-devsecops

作者：Red Hat 选题：bestony 译者：mrpingan 校对：bestony, wxy

本文由 LCRH 原创编译，Linux 中国 荣誉推出