简译版

自动化安全的障碍和对策

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Improving the Adoption of Security Automation		
原文作者	Dan Koloski	原文发布日期	2018 年 6 月 20 日
作者简介	Dan Koloski 是 Oracle 系统管理和安全产品部门副总裁。 https://www.darkreading.com/author-bio.asp?author_id=3780		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/vulnerabilities---threats/improving-the-adoption-of-security-automation/a/d-id/1332037		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

自动化安全的障碍和对策

Dan Koloski

2018 年 6 月 20 日

本文将介绍安全自动化应用的四大障碍以及如何克服这些障碍。

通过自动化运行，IT 在很多领域都能获得增值。但是对于安全领域而言，自动化程度一直较低。例如，在刚刚发布的《Oracle 和 KPMG 2018 年云威胁报告》中，只有 35%的受访者表示“我们公司致力于安全自动化并积极投资于自动化解决方案”。调查还显示，在保护启用了云的工作场所时，一个重要挑战是自动化要跟上规模。

自动化应该成为 IT 工具包的重要组成部分，这样一来，企业无需手动执行某些工作，能够大大提高工作效率。但是目前，大多数企业尚未广泛应用自动化技术。为了解决这个问题，我们需要了解应用自动化技术的障碍以及如何克服这些障碍。

障碍 1：对自动化的决策没有信心

客户经常说，他们无法保证自己的分析结论是正确的，在特定场景中，其自动化的修复措施能否起作用存在不确定性，因此无法将修复过程自动化。但这其实是上游分析问题，而非自动化问题。克服这一障碍的措施包括：提高上游数据和分析（上游数据和分析是制定决策的依据）的质量，并将这些决策的结果提供给协作/自动化框架（这意味着你需要一个分析平台，用于处理数据和监测系统生成的大量数据）。

障碍 2：不是所有的都适合自动化处理

平台选择很重要，即使这种选择并非总是由安全团队来决定。现在，安全团队大力倡导，为即将到来的项目选择的技术平台必须能够实现自动化，在理想情况下尽可能自主地进行自我保护。任何企业都有各种云、本地和混合场景，这些场景正在以不同的速度演变，因此考虑平台选择问题永远不会“太晚”。对于安全专家来说，了解哪些平台可以降低应用程序的风险，并积极与应用程序开发人员共享这些信息，是非常重要的。

障碍 3：担心失去控制

这一点受文化影响，可以理解。自计算出现以来，安全要么是手动进行的，要么分析报告不能提供足够的、可转变为具体行动方案，因此许多有经验的分析师对这两者都不信任。企业可以从小处着手。不要一开始就将整个修复周期自动化，可以从取证和小规模修复（如分析师的部分调查和简单的修复措施）的自动化开始，例如采用一次性多因子身份验证（ MFA）。

如果分析算法在一个系统上发现了用户的异常行为模式，那么下一步就可以在其他系统上自动收集类似的用户行为，并通过 MFA（向用户的智能手机发送短信验证码）进一步进行验证。这种方法并未采取极端的防御措施——暂停用户帐户，但确实使一部分调查实现了自动化，并且实现了初步防御。

障碍 4：安全与运维开发的自动框架冲突

在过去的几年里，IT 行业的自动化趋势帮助了开发人员，无处不在的 DevOps（运维开发）自动化加快了创新进入市场的步伐。开发人员和业务线管理人员自然不希望另外的一个所谓自动化安全方案的加入，因为这可能会减慢或破坏 DevOps（开发到上线运营）流水线。在这种情况下，需要将安全与运维开发结合起来.....换句话说，采用 DevSecOps！

DevSecOps 需要一定程度的跨团队协作、设备联合和自动化。当企业对开发、安全和运维的基础数据/分析/自动化系统进行标准化时，这些是有可能实现的。尽管开发、安全和运维用户形态各异，但是实际上背后的平台都是统一的。一个好的解决方案能为这三者（开发、安全和运维）提供一个基础公共知识平台，来弥补它们之间的差异。

做出改进

自动化是 IT 行业最古老的武器之一，使安全工作能够跟上当前攻击面和威胁向量的速度和规模，但是大多数安全团队在这方面的投资还很不足。进一步研究发现，自动化在安全方面的低应用率受上述四个因素的影响，但是，这些因素与自动化本身无关——安全团队可以通过解决这些问题来改善企业的自动化现状。

关注更好的分析，为新项目选择平台，克服团队中的文化阻力以及与其他团队合作，这些措施都可以增加自动化的应用，最终将帮助我们改善安全态势。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队，为用户提供端点防护、流量监测、快速处置、深度分析等产品，以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门，提供高级威胁和新兴威胁解决方案和能力体系，产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。安天是中国应急响应体系中重要的企业节点，在红色代码、口令蠕虫、心脏出血、破壳、魔窟等重大安全威胁和病毒疫情方面，提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动，进行了深度的解析，对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上，安天创始人、首席技术架构师作为网络安全领域的发言代表，向习总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了位于哈尔滨科技创新城的安天公司，对安天负责人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*