

简译版

采用 DevSecOps 下一代威胁建模

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	Is next-gen threat modeling even about threats?		
原文作者	埃桑·福鲁吉 (Ehsan Foroughi)	原文发布日期	2022 年 3 月 28 日
作者简介	埃桑·福鲁吉是 Security Compass 的首席技术官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2022/03/28/modern-threat-modeling/		
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		
摘要	利用现代、全面和自动化的 DevSecOps 威胁建模框架，企业可以部署有限的资源，以产生最大的效益。从一开始就构建强大、安全的代码，不强迫开发人员或 AppSec 团队追溯和纠正漏洞，可以提高生产力。此外，无论威胁源采用何种攻击方法或技术，该方法都能够阻止他们创建“滩头阵地”。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

采用 DevSecOps 下一代威胁建模

埃桑·福鲁吉

2022 年 3 月 28 日

随着技术的发展，威胁形势也在不断演变。随着威胁的复杂性不断增加，人们担心诸如 Colonial Pipeline 勒索软件攻击或 Equifax 黑客攻击等事件会再次上演。主流媒体通常关注运营网络安全、智能应用防火墙等防御性/反应性解决方案，但是《2021 年 Verizon 数据泄露调查报告》显示，软件中不安全的代码和配置才是亟待解决的根本问题。

为应对不安全软件开发/部署的挑战，安全行业开始在软件开发生命周期（SDLC）考虑安全性。许多安全专家尝试使用传统的威胁建模来解决 SDLC 中的安全问题。

但是，如果传统威胁建模是错误的，该怎么办呢？

传统威胁建模标准源自以前的安全专家会议，在该会议中，安全专家齐聚一堂集思广益，讨论可能影响其软件的潜在威胁。这种劳动密集型方法通常导致安全专家和开发人员之间存在沟通问题。该方法的主要缺陷是，只能解决安全专家在开发建模平台期间考虑到的威胁。

威胁建模不断演变

随着 DevSecOps 的发展，现代威胁建模不再专注于对复杂威胁场景的详细分析。乍一看，你可能会认为这是错误的，你可能认为不考虑威胁的威胁模型没有什么用处。但是实际上，通过 DevSecOps 进行威胁建模取得了很好的效果，这是因为该模型“从一开始”就防御威胁。DevSecOps 和“从一开始就构建安全代码”的理念不再强调个体威胁以及它们如何利用漏洞，而是专注于从软件开发的早期就开始进行防御。从某种意义上说，企业可以通过安全设计以及从一开始就编写完善的代码来消除漏洞。

此外，DevSecOps 可以减轻开发人员和安全团队的压力。在威胁建模的早期，耗时、瀑布式的威胁建模意味着它是在有限的范围内执行的，而且很少保持最新状态。这通常会导致开发人员跳过安全计划，直接将代码提交给应用程序安全（AppSec）团队以确定其是否足够安全。然后，安全团队将提供一长串需要进行的更改。由于时间紧迫，开发人员很少有时间实施这些更改。此外，一些公司资源不足，无法在开发新代码的同时进行追溯性修复。在这种情况下，最好的防御方法是使用传统的威胁建模来阻止试图利用已知漏洞的攻击者。

如今，DevSecOps 已成为新威胁建模的黄金标准，它能够主动防止威胁的发生。相较于由人手不足的 AppSec 团队负责安全性，该标准能够帮助开发团队确保安全性，从而构建更强大的安全框架。通过主动开发更安全的代码、规范语言并采用现代化的威胁理念，企业可以大大改善其安全状况。

这就引发了一个问题：如果现代威胁建模与传统威胁建模是不同的，那到底哪种方法更好呢？

采用现代威胁建模框架至关重要

虽然威胁建模方法发生了变化，但是我们需要进行建模的原因是一样的。现代威胁建模仍然涉及识别和预防威胁，只是更加主动。该模型专注于 DevSecOps，能够全方位地预防威胁，而非仅预防当下的热门威胁或漏洞。我们无法预测所有新型的恶意软件传播方案，但我们可以消除恶意软件可能利用的路径和漏洞。

这种“不确定性”会越来越严重。随着复杂 IoT 设备攻击、加密货币和区块链诈骗以及网络钓鱼攻击的不断发展，企业需要担心的威胁越来越多。“可以预测每种攻击方法”的想法太过幼稚。实际上，防御现代威胁的最佳方法是不直接关注威胁本身。

我们还必须考虑到，传统的应用程序安全模型不适用于“与软件风险管理有关的一些问题”。现代威胁建模需要为开发人员提供需要实施的缓解措施清单。

利用现代、全面和自动化的 DevSecOps 威胁建模框架，企业可以部署有限的资源，以产生最大的效益。从一开始就构建强大、安全的代码，不强迫开发人员或 AppSec 团队追溯和纠正漏洞，可以提高生产力。此外，无论威胁源采用何种攻击方法或技术，该方法都能够阻止他们创建“滩头阵地”。

这种现代威胁建模框架应迅速成为新的标准。没有任何企业愿意沦为“下一个 Equifax”或“下一个 Colonial Pipeline”，也没有任何股东或利益相关者愿意看到因建模实践不佳而发生重大系统攻击事件。因此，企业应专注于 DevSecOps，从一开始就构建安全代码，并使用该平台创建更强大、更现代的威胁建模方法。

安天简介

安天致力于全面提升客户的网络安全防御能力，有效应对安全威胁。通过 20 余年自主研发积累，安天形成了威胁检测引擎、高级威胁对抗、大规模威胁自动化分析等方面的技术领先优势，打造了面向服务器、云、虚拟化、容器和传统办公节点等提供全防御能力覆盖的智甲安全产品家族，满足客户对于包括终端杀毒、终端防护 (EPP)、终端检测与响应 (EDR)、云工作安全防护 (CWPP) 等系统安全层面需求；整合强化包括 ATID 威胁情报门户、追影沙箱和捕风蜜罐等产品在内的威胁情报板块产品，有效提升客户情报赋能和自主情报生产能力；基于流量产品探海有效应对客户对于网络威胁检测与响应 (NDR) 和网络流量分析 (NTA) 的安全需求，相关产品可以实现交叉联动，统一管理，形成面向从勒索软件到高级威胁 (APT) 的纵深安全防线。同时打造威胁对抗、威胁猎杀、威胁巡检服务三款主打安全服务，辅以平台支撑、快速到达的轻量级垂直响应服务，以运营模式有效支撑应对综合威胁对抗能力升级。

安天为网信主管部门、军队、部委、保密行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，已连续七届蝉联国家级网络安全应急支撑单位。安天参与了 2005 年后历次国家重大政治社会活动的安保工作，获得杰出贡献奖、安保先进集体等荣誉称号；自 2015 年来，安天的产品与服务为包括载人航天、探月工程、空间站对接等历次重大航天飞行任务，以及大飞机首飞、主力舰护航、南极科考等重大任务提供安全保障支撑。

目前，安天的威胁检测引擎为全球超过一百万台网络设备和网络安全设备、超过三十亿部智能终端设备提供了安全检测能力，已经成为“国民级”引擎。

安天已发展成为以哈尔滨为总部基地，建有六地研发中心、两个控股子公司，参与一个国家工程实验室建设，拥有两个省级工程中心和重点实验室、一个博士后创新创业基地和多个高校联合实验室的集团化创新企业，同时在地多设有办事处和应急响应站，为客户提供全面的安全服务与技术支持。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“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>