下一代网络靶场：将事件响应演习迁移到云中

简译版

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	The Next-Gen Cyber Range: Bringing Incident Response Exercises to the Cloud		
原文作者	马修·多布斯（Matthew Dobbs），伊兹克·科特勒（Itzik Kotler）	**原文发布日期**	2021 年 3 月 18 日
作者简介	马修·多布斯是 IBM 安全网络靶场首席集成架构师；伊兹克·科特勒是 Safebreach 联合创始人兼首席技术官。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/posts/next-gen-cyber-range-incident-response-cloud-native/		
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	云原生是什么？这个概念源于向云计算的快速过渡，从根本上改变了构建、部署和保护应用程序和基础架构的方式。随着云原生成为许多企业 IT 基础架构规划的关键部分，我们认识到，所有相关功能都需要扩展为云原生，包括能够影响这些环境的事件检测和响应。		
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。		

下一代网络靶场：将事件响应演习迁移到云中

马修·多布斯，伊兹克·科特勒

2021 年 3 月 18 日

云原生是什么？这个概念源于向云计算的快速过渡，从根本上改变了构建、部署和保护应用程序和基础架构的方式。云原生背后的推动力是 Kubernetes 的普及、快速增长的开源容器编排系统以及云原生计算基金会（Cloud Native Computing Foundation，CNCF）。CNCF 推出了许多厂商中立的、迅速发展的开源项目（包括 Kubernetes）。

我们将云原生应用程序和基础架构定义为“由离散的、可重用的组件（称为微服务）组成，这些组件可以集成到任何云环境中。这些微服务充当构建块，通常包装在容器中。它们作为一个应用程序协同工作，但是每个微服务都可以通过自动化和编排流程独立扩展，不断改进和快速迭代。”

随着云原生成为许多企业 IT 基础架构规划的关键部分，我们认识到，所有相关功能都需要扩展为云原生，包括能够影响这些环境的事件检测和响应。

从物理到虚拟再到云原生

网络靶场的概念诞生于物理时代。如果企业部署服务器，则安全或 IT 管理员需控制物理机箱和机架，包括网络接口卡、硬盘等等。如果企业运行软件，则该软件将控制其安装的代码。在虚拟和云原生领域中，管理员和安全软件几乎无法控制物理硬件，甚至无法控制在云原生应用程序下运行的原始控制面板。这意味着，网络安全方法必须考虑架构、监控和控制方面的重大差异。

从各方面看，虚拟化会带来一些复杂性。当企业以混合模式运作时（有本地资产，也有多个供应商的云资产和数据），会尤其复杂。

为了满足企业现在和将来的需求，我们一直在设计网络靶场的云原生版本。

随着疫情的持续，员工继续远程工作，企业对云中事件响应功能的需求越来越迫切。我们看到，越来越多的攻击者将目标锁定在云原生环境中的薄弱环节，他们利用热门平台和应用程序，在 Linux 和云环境中运行其恶意软件，这些恶意软件通常使用 Go 编程语言编写，

可以在混合基础架构中运行。

举例来说，Amazon Web Services（AWS）的 S3 存储系统是云中最热门的对象存储设备，公司经常将敏感数据存放在 S3 存储桶中，但是该存储系统难以进行保护。使用该存储桶会带来很大的风险：要么无意中将存储桶暴露于开放的互联网，要么遭受诸如 CapitalOne 在 2019 年夏天遭受的破坏性攻击。在该攻击中，一位前 AWS 员工利用配置错误的 Web 应用程序防火墙（WAF）泄露了超过 1.06 亿人的信用卡申请。

云原生安全演习有何不同？

在常规演习中，当检测到问题时，安全团队可以将受影响的服务器与网络隔离，断开连接，但保留物理服务器以进行进一步检查和分析。而在云原生领域，没有物理服务器。安全团队可以从公司的网络中删除虚拟实例，但是他们没有便捷的方法从云提供商的网络中删除物理服务器。实际上，这样做会破坏许多其他客户的应用程序。

鉴于云原生应用程序和体系结构的特殊之处，企业需要以不同的方式来考虑和应对安全威胁。例如，当容器或虚拟机被感染后，安全响应团队应立即冻结并隔离该计算实例以进行适当的取证，这一点至关重要。这与关闭云服务器的初衷背道而驰，该举动可能会阻止攻击，但也会消除进行分析所需的取证线索。

当 DevSecOps 团队跨多重云保护其应用程序和基础架构时，这些差异将成倍增加。不同云之间的安全方法和功能都有很大的差异。例如，诸如 S3 这样的存储服务，其默认配置可能具有不同的安全级别。AWS Cloud Trails 和 Microsoft Azure Sentinel 中用于收集和分析云日志文件的方法不同。在 AWS 和 Azure 上运行的基础级应用程序编程接口（API）也存在根本差异，与这些 API 进行通信的开发人员应在命令脚本和 DevOps 工具中使用不同的语言惯例，以实现持续集成（CI）和持续部署（CD）。

为了检测潜在的安全事件，安全团队应进行适当的监控，以了解他们要保护的整个环境。不幸的是，在复杂的混合基础架构中，难以创建简单易用的单一面板。我们经常在企业和政府客户的安全咨询工作中生成此类仪表板和连接层，这就是原因所在。

除监控障碍外，安全团队在不同云中可用的安全工具和控件也大有不同。例如，AWS 有三种负载均衡器，它们具有不同的（或没有）WAF。在 AWS 和 Azure 上运行的 Kubernetes 服务则不允许配置 WAF。

此外，在本地和云中部署时，安全团队如何使用诸如 SafeBreach 的连续安全控制验证平台，也有很大不同。在云中，大多数应用程序是使用容器技术部署的。容器能够大规模创建长期和短期的基础架构，这使云原生成为可能。因此，在这些演习中，我们针对容器进行攻击模拟，针对它们的网络堆栈、安全流程，以及安全团队在构建和保护多重云环境的过程中必须管理的任何其他攻击面。

向“基于容器的安全性”的转变也扩大了参与者的范围。在这种情况下，开发人员不断部署代码和应用程序，并控制容器中的内容。由于发布周期快，安全审查往往是自动化的。因此，云原生网络靶场包括开发团队和 DevSecOps 团队的参与者，传统事件响应团队则不包括这些人员。

将各种因素整合

在与客户沟通他们对事件响应培训的需求时，他们表示想要搭建一个实践舞台，以便安全团队不仅可以在混合（传统）环境和云之间，而且可以在多重云之间进行分析、监控和编排。这就是 IBM X-Force 云原生网络靶场的推动思想。

在网络靶场中，演习由攻击活动的紧急通知（例如新闻工作者打来的电话或 FBI 发来的电子邮件）触发。攻击可能源于公有云中众多攻击点之一。我们还将不受参与者控制的云包括在内，使参与者了解如何应对这一新现实，以及如何与公有云安全团队进行交互，以最大程度地获得成功、减少攻击影响。

借助 SafeBreach，我们运行了以容器为中心的攻击方法，着眼于潜在的杀伤链，重点分析哪些控制措施有效、哪些控制措施无效。SafeBreach 规定的补救措施，可作为改善参与者云原生安全态势的指南。采取补救措施后，需确保控制措施按预期运行。

我们构建云原生网络靶场的一个目标是，通过更高速的部署，帮助安全组织和开发团队了解在分布式应用程序环境中验证安全性的最佳方法。这是因为，如果将补救措施整合到 CI/CD 管道中，而非将其作为对攻击信标的反应，补救措施能够更好地发挥作用。

大多数安全团队已经了解了这一现实。但是，在内部实现这种转变并更改安全立场（反映新的云原生方式），是实现这一目标的最佳方式。

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，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

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，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

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