利用遥测技术监控应用程序，发现源自内部的隐藏威胁

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	Using Application Telemetry to Reveal Insider & Evasive Threats		
原文作者	安迪·霍金斯（Andy Hawkins）	**原文发布日期**	2020 年 4 月 7 日
作者简介	安迪·霍金斯（Andy Hawkins）是 TrueFort 的现场首席技术官，也是 DevOps、IoT、软件工程和站点可靠性/SRE 方面的专家。		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/attacks-breaches/using-application-telemetry-to-reveal-insider-and-evasive-threats/a/d-id/1337438		
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。		

利用遥测技术监控应用程序，发现源自内部的隐藏威胁

安迪·霍金斯

2020 年 4 月 7 日

通常只有在数据渗出成功后，才能正确识别破坏已经造成的指征（IoC）——无论是由误导性的过失、善意的操作更改，还是由恶意的内部人员或外部攻击者通过受损的帐户凭证进行的攻击。

幸运的是，IT 基础设施（尤其是应用程序进程、负载、会话以及网络连接）不会撒谎。它以碎片的形式将威胁展现出来，可以在违规造成破坏之前就将其观察到。要找到并收集这些威胁信息，对 IT 基础设施和应用程序行为进行有针对性的监控仍然是检测和最有希望地阻止正在进行的攻击的最有效方法。

让我们考虑一下哪些威胁碎片或遥测技术最适合使用，以及它们如何帮助企业在杀伤链的早期应对威胁。

进程

所有攻击都源于进程。考虑一个 shell 脚本或 Java 应用程序——时间、进程标识符（PID）、参数和 CRC 校验和都是重要的因素。

例如，在暴力破解或其他更复杂的攻击中，进程行为的异常更改提供了第一个 IoC—就像攻击者发动离地攻击一样。因此，实现具有保真度的技术来检测异常的进程行为是一个关键的防线前置手段，提前预警入侵。

网络负载

企业的网络构架通常比较复杂，涵盖企业内部、数据中心以及云等。由于它们的网络流量在这些不同的环境、它们的 API 之间、物联网平台上流动，现在还使用了容器和微服务，因此，如果没有关联的具体场景信息，这些部分之间的网络指征则会是无用的。为了识别哪些流量是正常的、哪些是恶意的或者攻击者的，就需要深入了解相关背景下的，进程之间、各应用程序之间的网络流量情况。

例如，最近许多引起广泛关注的渗出漏洞利用了特权、非人为和服务帐户凭证进行攻击。检测这种类型攻击的一种方法是绘制进出应用程序或业务服务以及其基础进程活动（即其PID、已执行的命令和参数、甚至是其网络连接的更改）的网络流量图。访问实时警报的时间序列数据，并进行前导和后续取证，可以帮助确保信息安全团队及时响应。

软件

无论是商用现货（COTS）还是运营支持系统（OSS），只观察进程数据是不够的。相反，有必要验证并确认没有 Web 应用程序资源（WAR）文件、二进制文件、机密文件或配置被破坏。这可以通过文件系统扫描和针对清单或校验和的集中测试来完成。

然而，更好的做法是将此功能构建到工具链中。新兴威胁带来了污染构建系统的风险——可能来源于内部，也可能来自上游的供应商。采取适当的措施来监控已构建和部署的软件非常重要。特别是如果核心组件库被置入恶意代码，那将非常危险。一个不幸的例子是针对 Ruby 强密码库的依赖库的攻击。在软件系统进行测试、发布以及运维过程中，企业至少应关注软件的来源、权限以及校验和等因素，以确认其可靠性。

身份

许多企业已开始对用户实施控制措施，甚至可能正在使用 UEBA。然而，许多用户不存在于目录中，也不在用户管理进程内。系统和服务帐户会将企业的系统弄得乱七八糟。然而，它们却是为 Web、应用程序和 RDBMS 服务器提供服务的基础设施的核心。必须对这些系统用户进行监控，以防止其对业务造成影响和破坏。

例如，虽然应该永远不允许 Apache 用户登录，但是应该允许 Oracle 用户登录，且只能允许一小部分白名单用户从预先确定的、受控的位置登录。

系统

信息安全和攻击者的理念是正交的——防护需要全面覆盖，而攻击者最关心的则是目标的数据。任何存在于网络、用户界面、应用程序开发接口 API 或者操作系统中的弱点和漏洞都可能被攻击者利用；作为防守方，就要全面了解整个防护网络的全部服务内容以及这些服务之间是如何协作的。

为了说明这一点，是否应该调查应用程序服务器上的 CPU 峰值，或者相反，它下降了？

唯一的确定方法就是了解上下文。是否有计划的更改，或推出了新产品或地理定位？是否正在举行活动？为了避免误判，必须具有宏观视角，根据系统的不断变化来判断是否出现了异常情况。对变化敏感、对网络背景的深入了解是防护的基础。

再举一个例子。为了准备产品发布，企业在 Web 和应用程序服务器层中预配置了四倍的容量，并使用 HAProxy 重新分配负载。启动之前，不会生成任何安全警报，因此企业不知道现在有额外的容量。在发布当日，数据库服务器的数据量突然有了巨大的增长，这可能表明外围防御已被破坏并且机密客户数据已被访问。

全局视角的防护理念

孤立、单个的指征，如果缺乏其产生的背景，将没有应用价值。从全局掌控应用程序之间的关系、以及这些应用赖以依存的环境：平台、操作系统、网络连接、性能、进程、用户身份、发送的时间等，只有这样才能在威胁发生前，将其检测出来。

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，截止到 2019 年 9 月 30 日，安天的威胁检测引擎为全球超过六十万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，“您们也是国家队，虽然您们是民营企业”。

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*