简译版

SOC 缺失的链条：保护大型机

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 missing link in your SOC: Secure the mainframe		
原文作者	克里斯托弗·佩里（Christopher Perry）	**原文发布日期**	2020 年 5 月 21 日
作者简介	克里斯托弗·佩里是 BMC Software 首席产品经理。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2020/05/21/secure-the-mainframe/		
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。		

SOC 缺失的链条：保护大型机

克里斯托弗·佩里

2020 年 5 月 21 日

企业的安全可见性能否涵盖其基础架构的每个关键角落？好的安全信息和事件管理（SIEM）解决方案将跨防火墙、服务器、路由器和端点设备提取数据。但是，如果有一个漏洞——一台包含关键业务数据的设备无法监控——会怎样呢？这听起来像是企业安全运营中心（SOC）愿景中的一个严重漏洞，尤其是如果这台设备会被黑客、恶意内部人员利用或偶然使用。

我知道，我这是在白费唇舌。企业已经知道 SOC 需要立即访问所有关键基础架构，以确保快速有效地响应任何事件。但是我敢打赌，许多企业仍然存在着这样一个问题——大型机是否受到与服务器相同水平的最佳实践和自动化保护？我认为答案是否定的，或者说企业根本不知道答案。

考虑大型机安全

我们先来讨论一下大型机。你是否知道，大型机占企业 IT 生产工作负载的 68%，并且是整个企业的骨干？

长期以来，就像 macOS 一样，大型机被认为是安全的，没有遭受攻击或破坏的风险。

因此，大多数安全工程师都忽略了大型机——他们要么赞成上述观点，要么根本不理解这种观点，因此毫不质疑。

现实情况是：企业可以采取措施保护大型机，但无法保证它一定是安全的。进入企业网络的攻击者可以从管理员 Windows 或 Linux 平台访问大型机，获得更高的权限并收集敏感数据。一旦获得初始访问权限，他们就可以通过几种常用方法来提权。利用这些权限，他们可以运行许多有害脚本来控制大型机并隐藏踪迹。

开展培训

企业是时候将大型机当作网络上的另一台计算机了。这意味着，要将大型机的信息和事件日志实时同步到 SIEM 中。即使企业已经具备实时大型机可见性，他们可能仍然缺乏成功利用和响应这种可见性的知识和专业技能。举例来说，如果企业的安全团队不了解 RACF 和 ACF2（译者注：RACF，Resource Access Control Facility，资源访问控制设备。ACF2，Access Control Facility 2，访问控制设备 2）这样的首字母缩写词，他们该如何区分误报和灾难事件呢？因此，数据必须是可见的并且可以转化为行动。

企业该怎么做呢？大多数安全分析师需要接受更多的培训，将他们已经拥有的安全知识付诸实践，以更好地理解和保护大型机。但是，他们很快就会面临大型机告警挑战。为了快速启动此过程，成功的公司通常采取如下关键措施：

- 雇用具有大型机背景且对大型机安全感兴趣的人员；
- 开展培训计划，使员工学习渗透测试并保护大型机；
- 咨询大型机托管服务提供商。

1.雇用合适的人才

雇用合适的人才看起来很简单。但实际上，雇用具有大型机或网络安全技能的人才越来越难了，这是因为职位空缺程度远远超过了此类人才的数量。即使企业能够以最高薪资相竞争，可能也无法找到具有这两种技能的人才。因此，很多成功的企业开始投资于现有人才资源，以防御其关键系统。

2.开展培训计划

这些企业的在职培训形式通常是：(1)高级技术人员进行内部培训；(2)聘请行业专家开展技术课程。一个很好的例子是：聘请具有丰富网络安全基础知识的安全分析师来教授大型机基础知识。

同样的安全原则也将适用。有才华的分析师将能够迅速理解新操作系统的细微差别，从而为 SOC 提供保护整个企业（而不仅仅是最普遍的 Windows 和 Linux 系统）所需的技能。对员工进行培训和投资，不仅可以提高企业的安全运营水平，还可以提高接受培训的员工的忠诚度。

3.使用大型机托管服务

如果员工由于时间和个人能力不足无法发挥其技能专长，则企业可能需要考虑使用大型机托管安全服务。将安全责任转移给专门防御大型机的专家，可以确保关键大型机服务器得到充分的保护。使用大型机托管安全服务能够降低业务风险，是实现安全目标的最快方法。幸运的是，这种服务可以按需使用，同时企业员工也能逐渐上手，将安全功能重新集成到 SOC 中。

保护大型机是更广泛的自主数字企业框架的一部分，它不仅是安全或运营需求，还是业务需求，以实现自适应安全。成功的自适应网络安全计划需要有训练有素的安全专家，他们可以建立主动的安全功能，以自动感知、检测和响应安全事件。如果企业考虑一下大型机对于其关键功能有多么重要，就不会想当然地认为大型机是安全的了。

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