简译版

企业需要可扩展的 OT 网络安全解决方案

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 need for scalable OT security		
原文作者	Elad Ben-Meir	**原文发布日期**	2019 年 7 月 26 日
作者简介	Elad Ben-Meir 是 SCADAfence 公司的首席执行官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2019/07/26/scalable-ot-security/		
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。		

企业需要可扩展的 OT 网络安全解决方案

Elad Ben-Meir

2019 年 7 月 26 日

随着制造企业和其他工业网络所有者越来越注重安全性，他们开始面临安全性能问题。生产（OT）网络日益成为攻击目标，但现有的许多 OT 网络安全解决方案并非针对这些高流量的网络而设计。

近期的攻击事件（如挪威铝业巨头 Norsk Hydro 攻击事件）再次证明，任何 OT 网络，无论是制造工厂、关键基础设施还是智能建筑，都可能成为网络攻击的下一个目标。因此，这些网络的所有者需要保护自己。

网络攻击可能导致企业全面停产，使企业收入减少，而且通常需要很长时间才能恢复。如果商业机密被盗，企业可能会失去竞争优势，甚至可能危及生命——因为这些关键系统通常与物理过程、有害物质、高压等人类生命危险因素息息相关。

大多数 OT 网络安全解决方案最初是为石油和天然气、公用事业或供水等行业设计的。在这些行业中，OT 基础设施通常分布在广泛的地域中，但每个单独的 OT 网络通常具有相对较少的资产，低带宽和可确定、可预测的行为。因此，现有的许多 OT 网络安全解决方案倾向于支持非常具体的用例，如具有简单通信模式的单供应商、相对安静的环境。

我们的想法是，对这些解决方案进行扩展，以应对制造和楼宇管理系统（BMS）的大型、复杂、多供应商网络。鉴于这些网络中通常有数千个设备进行复杂和多样化的通信，这种扩展是非常困难的。仅仅几年前设计的安全解决方案，已无法应对当今自动化制造工厂和 BMS 环境产生的复杂流量。

如果企业部署了不恰当的安全系统，则会产生“网络受到保护”的错觉。由于性能问题，这些系统不会处理关键信息。它们只能管理部分资产，无法管理影子 OT 资产。此外，它们只能处理部分数据包，因此无法提供全面的告警。在复杂、多供应商的大型网络中，各种协议和设备的错误配置和维护，导致网络“噪音”问题更加突出。如果系统未采用专门的算法来区分正常事件和应采取行动的异常事件，则一些正常事件也会触发告警，造成安全团队疲于应付一些“误报”事件。

人们通常认为，实验室测试能够预防这些问题；其实并不能。在小型实验室网络中测试解决方案时，无法准确地模拟监控生产网络面临的挑战。在大多数情况下，OT 网络安全解决方案能够成功通过实验室测试；然而在实际生产环境中却不能起到应有的安全保障作用。

保护大规模环境的挑战

大多数 OT 网络安全供应商只是尝试扩展现有系统(这些系统并不是为具有数千个资产的大型网络设计的)，而非重新设计系统。虽然这些解决方案能够胜任最初的小型网络，但它们无法很好地扩展，因此无法对大型生产网络，提供足够的安全和监控功能。

这些解决方案无法支持大规模 OT 网络，存在低性能、难以使用、低检测率和总体拥有成本（ TCO ）过高等问题。

我们通过以下三点予以说明：

- 要真正支持具有数千个 (甚至数万个) 设备的环境，安全解决方案必须能够收集和分析大量数据，且不会遗漏单个字节、设备、配置或任何其他数据点。
- 正确收集和分析数据之后，最终用户需要通过可用的响应界面来访问它们，以便评估实际的安全风险并做出响应。
- 这些解决方案可能存在准确性问题。并且由于大型环境的不断变化和噪音问题，会受到大量误报的干扰。这最终会导致安全团队疲惫不堪，无法关注重点问题。

为了解决这些问题，安全团队通常需要部署昂贵的硬件、增加维护成本，以及雇用额外的人员来处理正在进行的安全操作，这些都会导致 TCO 增加。

为未来做准备

即使目前 OT 环境还未被认为是大规模的，未来也一定会。随着工业 4.0 推动数字化转型和工业物联网的采用，许多企业正在扩展其工业运营的规模、复杂性和自动化程度。他们在 OT 网络中部署传感器，以从现场收集更多数据，并通过改进决策流程来提高效率。

这推动了各个行业的互联和自动化水平的提高。为了安全地支持这些高级功能，企业需要采取适当的安全措施，以促进他们在工业 4.0 时代的发展之旅。

如何为大型网络选择 OT 网络安全供应商

以下是一些建议和最佳实践：

1. 不要只在非活跃生产线或实验室中测试生产系统。
2. 执行误报测试——有多少告警是基于真实事件的？可以对哪些告警采取行动？哪些告警需要立即采取行动？
3. 执行漏报测试——在供应商不知情的情况下，在生产网络上执行测试。检查供应商检测到的内容以及他们是否监控了所有数据包。然后，确定能否通过系统的图形用户界面（GUI）找到有关事件的准确信息。
4. 验证检测到的资产数量，并对资产清单进行抽样，以确定检测的准确性和深度。
5. 系统在实际生产中运行几天后，验证系统用户界面能否做出响应，以及所有 GUI 功能是否可用。
6. 如果您计划管理多个站点，请采用能够提供多站点管理门户和 SIEM 集成的解决方案。

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，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十五亿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