简译版

集成 SIEM 工具对于威胁管理至关重要

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	Why integrating SIEM tools is crucial to managing threats		
原文作者	戴夫·费舍尔（Dave Fischer）	**原文发布日期**	2021 年 11 月 8 日
作者简介	戴夫·费舍尔是 Yahoo Small Business 的首席安全架构师。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/11/08/siem-tools/		
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	SIEM 软件并非一个新概念。但是，建议企业选择那些使用云和更新的网络架构构建的应用程序，这样更加明智。众所周知，一些较旧的版本会收集过多误报，比关键的安全工具更令人讨厌。新一代 SIEM 软件使用 AI 技术进行分析，解决了这些遗留问题。在网络威胁持续扩散的今天，SIEM 能够为网络安全专家和 IT 专家提供关键、自动化和可扩展的优势。		
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。		

集成 SIEM 工具对于威胁管理至关重要

戴夫·费舍尔

2021 年 11 月 8 日

如今，远程和混合办公已经成为常态，对企业网络的访问不再局限于实体建筑内的网络，而是扩展到通过不安全的家庭网络和个人设备连接企业网络的员工。这导致维护企业的网络安全非常困难。而这些不安全的网络和设备通常不会被常见的网络安全措施发现，却会被攻击者和恶意软件发现和利用。

但在许多情况下，将“安全信息和事件管理”（SIEM）工具与企业现有的网络安全软件集成有助于识别和减轻恶意网络攻击，防止此类攻击带来灾难性的后果。那些已经集成 SIEM，并用其来检测、分析和响应威胁（包括内外部威胁）的企业领导者和管理人员已经领先一步。

将 SIEM 工具与其他安全层集成，可以实时标记异常行为和潜在问题。即使攻击者的战术、技术和程序（TTP）不断发展，这种自动化的“额外双眼”也能够使用机器学习技术来监控整个企业的数据点和工作流程。

SIEM 可以帮助企业 IT 团队（尤其是中小型企业的 IT 团队）防止代价高昂的安全攻击，这类攻击会消耗企业的时间和精力，并可能对业务构成严重威胁。此外，SIEM 通常是可扩展的，因此可以成为帮助企业安全运营的宝贵资产。

除了新的远程办公场所之外，其他几个因素也会使企业网络的日常监控更加复杂。在大多数情况下，安装 SIEM 软件是管理这些因素的最简单方法。

我们以物联网（IoT）为例。软件，IoT 设备迅速扩增，这意味着网络的潜在入口点呈指数级增长。随着企业向远程办公的转变，这类威胁进一步放大。与远程办公人员共享 Wi-Fi 网络的个人或家庭笔记本电脑、游戏设备、平板电脑甚至连接的设备会产生安全漏洞，而攻击者和恶意软件可以瞄准和利用这些漏洞。SIEM 可以迅速处理 DoS 攻击，或者至少可以识别受感染的设备。

不幸的是，非 IT 部门的员工甚至可能没有意识到他们的家庭 Wi-Fi 和连接设备对企业网络构成了潜在威胁。这就是员工培训的用武之地。当员工清楚地了解全部风险以及他们在

避免网络攻击方面的责任时，网络安全就成为整个企业的共同目标。

即使员工明白他们不应该自行下载软件或禁用已经安装在他们工作站上的安全软件，SIEM 工具也能够起到“附加保险”的作用。在这种情况下，SIEM 软件可以设置为持续监控员工下载操作并在发生异常事件时发送告警。

更严格的跨行业法规为企业带来了另一层安全障碍：他们需要遵守新的、不断发展的隐私和消费者保护法律、法规和标准。例如，《欧盟通用数据保护条例》（GDPR）适用于所有规模的企业，要求中小型企业使用比大型企业更少的资源来管理合规性。

《支付卡行业数据安全标准》（PCI DSS）有助于保护整个支付卡生态系统的安全，适用于处理信用卡/借记卡支付交易的商家和服务提供商。无论企业需要保护客户信用卡数据，还是保护 HIPAA 法案规定的医疗数据，SIEM 软件都可以帮助其管理合规流程，同时降低长期合规和运营成本。

SIEM 软件并非一个新概念。但是，建议企业选择那些使用云和更新的网络架构构建的应用程序，这样更加明智。众所周知，一些较旧的版本会收集过多误报，比关键的安全工具更令人讨厌。新一代 SIEM 软件使用 AI 技术进行分析，解决了这些遗留问题。在网络威胁持续扩散的今天，SIEM 能够为网络安全专家和 IT 专家提供关键、自动化和可扩展的优势。

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