简译版

网络安全解决方案的整合

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	Converging on a Better Approach to Security		
原文作者	Ashley Arbuckle	原文发布日期	2019 年 6 月 13 日
作者简介	Ashley Arbuckle 是思科全球安全客户体验副总裁兼总经理。		
原文发布单位	Security Week		
原文出处	https://www.securityweek.com/converging-better-approach-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。		

网络安全解决方案的整合

Ashley Arbuckle

2019 年 6 月 13 日

安全企业通常使用 5 到 50 多个不同的安全供应商和解决方案。这些产品都会生成自己的一组告警，很快就会使企业无法招架。

在 2019 年 CISO 基准研究中，思科采访了约 3000 名受访者。其中，41%的受访者表示其企业每天会收到超过 1 万条告警；其中 30%的受访者已进入“告警淹没”（cyber fatigue）的状态。更重要的是，企业只核实了这些告警中的一半；在被核实的告警中，只有 24%被证明是真实告警；而在这些真实告警中，只有不到一半被修复了。由此可见，安全专家面临大量“噪音”（noise）的干扰，承担着巨大的风险。虽然自动化和机器学习技术对他们的工作有所帮助，但是大部分工作仍然要靠人类智能来解决。他们需要了解这些告警对企业来说意味着什么，以便合理利用手头上的大量数据。

显然，购买单独的安全产品和服务的传统方法已经不再那样有效了——这就是企业开始整合产品和服务的原因。企业希望获得整体性的解决方案，包括从工具和技术中攫取最大价值所需的功能。例如，安全团队不仅采用端点检测和响应（EDR）技术，还执行主动威胁猎杀、向企业发出事件告警并提供修复指导。

企业可以将高级分析平台、身份鉴别和访问管理工具与咨询服务相结合，快速启动网络分段计划。该方法能够减轻内部员工的工作负担，并快速发现新加入的网络设备和流量模式、不同的网络分段，以及与其他网络分段建立不同的信任策略。我们以旨在加强防御和响应的“紫队演习”（Purple Teaming）为例，这种演习由事件就绪和响应（IRR）团队牵头，将基础设施分析平台、应用性能管理和安全仪器平台等新技术与专家团队相结合。

产品和服务的整合是一个颇受欢迎的发展，能够增强企业的安全态势。要想成功利用这一发展趋势，请务必遵循以下三个步骤。

1. 预测

首先，企业应越过特定技术、环境，甚至流程，来审查其安全态势。企业负责人和 IT 人员应根据企业计划和期望结果共同定义安全要求。企业应使其安全策略与业务战略保持一

致，以便于安全团队做好快速响应企业需求的准备，同时降低风险，保护数据、应用和系统。实现这一步有助于企业完成接下来的两个步骤——整合和创新。

2. 整合

企业正在减少与其合作的供应商数量——他们使用架构式的方法进行整合，集成多个单独的产品和平台。通过整合，企业可以提高运营效率，增强安全态势；而非挣扎于各自产生告警的单个产品——在这种情况下企业难以清楚地了解其面临的风险。此外，我们还看到了供应商方面的整合。专注于网络安全的投资银行 Momentum Cyber 指出，在 2018 财年，安全市场的合并和收购活动依然强劲，达到 155 亿美元。随着安全市场的成熟，以及由于收购和合并导致安全市场条块分割的减少，这些并购能够达到 1 + 1 = 3 的效果。通过这种合并和收购，企业可以从安全工具中攫取指数级的价值。

3. 创新

安全行业的一个典型标志是 新兴技术不断涌现以抵御新兴威胁。目前，最新的趋势是：企业使用机器学习、人工智能和自动化工具来剔除告警，聚焦真正的风险并采取针对性的行动。但是，企业对这些技术的采用率正在下降，原因可能是对这些自动化的工具抱有不确定性或缺乏信心。要想成功创新，企业应寻求整体性的解决方案而不仅仅是采用新工具。只有这样，企业才能真正提高安全性，而非生成更多告警，反而增加发现真实威胁的复杂性并浪费资源。

安全行业和企业正在整合更好的安全方法，他们早就该这样做了。将技术和人类智能相整合，能够提高解决方案的成功率并降低风险，帮助企业从安全投资中获取更大的价值，使其充满信心地进行创新——这是一个很有吸引力的目标。

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（APT）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，已连续五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