提高企业威胁可见性

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	Enterprise Threat Visibility Versus Real-World Operational Constraints		
原文作者	甘特·奥尔曼（Gunter Ollmann）	**原文发布日期**	2020 年 9 月 17 日
作者简介	甘特·奥尔曼是微软云和 AI 安全部门的首席安全官。		
原文发布单位	Security Week		
原文出处	https://www.securityweek.com/enterprise-threat-visibility-versus-real-world-operational-constraints		
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有方式，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。		

提高企业威胁可见性

甘特·奥尔曼

2020 年 9 月 17 日

近几年，“假设发生攻击”这一观念促使企业进行安全投资并部署防御策略。但现在，这一观念可能要退出舞台了。

如果企业的绝大部分信息安全支出集中在边界防御和反应性响应上，那么企业应进行内部威胁检测，采用零信任网络分段，广泛部署多因子身份鉴别系统和条件访问控制。

鉴于企业在可见性上进行了巨额投资，旧的观念“防御者必须面面俱到，而攻击者只需要找到防御者的一个漏洞就行”应该可以被扭转了，转变为“攻击者必须面面俱到，而防御者只需要找到攻击者的一个漏洞就行”。不幸的是，安全运营和威胁猎杀团队发现，现在的漏洞实在太多了，他们需要付出大量的时间和精力进行猎杀。对于资源贫乏的安全团队（大多数安全团队都是如此）来说，要想增强企业的威胁可见性， 在他们从未完成过的安全任务中，每天还要再加上数百个告警。

要想预先检测、阻止和缓解更多威胁，企业需要将更多的预算和资源分配到增强可见性上。

这就相当于，在房屋内外安装数十个闭路电视（CCTV）探头，这些探头的监控范围彼此覆盖，能够保证监控的全面性，旨在防止入室抢劫的情况发生。但是，这需要建立在“有人一直盯着监控画面，一旦有人入侵就能发现，并采取措施阻止窃贼”的基础之上。

通过上述类比，我们可以很清楚地了解这种策略的后果：

1. 全天候的监控费用昂贵，因此需要部署自动检测措施。但是，自动检测会带来较高的误报率，需要不断调整基线。以家用 CCTV 探头来说，我们需要排除兔子、高尔夫球和送货员等情况，针对不同的运动方式，调整不同的报警阈值，并设置报警热区。不幸的是，即使是罕见的误报事件（例如暴风雨中的雷击或过往飞机的阴影），也足以让安全团队应接不暇，心惊胆战，导致他们浪费大量时间进行调查。为了解决这些问题，企业应至少使用两种不同的检测技术来检测和确认威胁（例如，CCTV 运动和玻璃破碎传感器）。

2. 如果企业的自动检测解决方案不具备自动响应功能，则它只能在攻击发生之后进行

清理和分类，无法进行预防，其价值就大打折扣了。由于存在误报的可能性，在告警响应期间，自动响应也应该是可逆的。如果有什么东西触发了 CCTV 的运动和玻璃破碎传感器，则它可能会自动报警。同时，原始告警接收者可以查看录像，并在明显误报的情况下取消报警（例如，邻居家的孩子在踢球，球飞过了围墙，打碎了窗户玻璃）。

3. 检测与预防之间的平衡至关重要，并且会随着时间发生变化。全天候 CCTV 监控是一项关键的检测功能，但不应忽视给所有外门上锁这一方法——虽说这种方法可能无法阻止未来的威胁，例如窃贼花 50 美元买一架微型无人机，操控无人机从烟囱上飞下来，偷走主人放在厨房桌子上的备用钥匙。预防投资倾向于威胁响应，而现代检测技术则倾向于异常检测。

“假设发生攻击”的目的是改变企业对安全技术（和运营计划）的思考和投资方式。与许多好方法一样，企业的安全措施可能会有些矫枉过正，因此应采取平衡的补救措施。

我认为，将云-安全信息和事件管理（Cloud-SIEM）和高级机器智能平台结合到自动检测方案中，能够满足大多数企业的全天候可见性和检测需求，但是安全运营团队仍会被大量告警淹没。我希望，安全行业未来五年的关注点是“自动缓解风险”。

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