

简译版

优先关注高风险资产：缓解内部人员威胁的四个步骤

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	Prioritizing High-Risk Assets: A 4-Step Approach to Mitigating Insider Threats		
原文作者	大卫·桑德斯 (David A.Sanders)	原文发布日期	2020 年 4 月 2 日
作者简介	大卫·桑德斯是 Fishtech Group 业务部门 Haystax 的内部威胁运营总监。		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/vulnerabilities---threats/prioritizing-high-risk-assets-a-4-step-approach-to-mitigating-insider-threats/a/d-id/1337404		
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	<ul style="list-style-type: none"> 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。 		

优先关注高风险资产：缓解内部人员威胁的四个步骤

大卫·桑德斯

2020 年 4 月 2 日

如果一个公司拥有 2.5 万名员工，但却只有一个四人的内部威胁团队，那么它应该如何检测并缓解内部威胁？或者，简单地说，一个分析师如何持续地监控并处理 6250 名员工的用例？答案是：他们办不到。

企业的首席安全官和首席信息安全官不仅面临着来自政府客户的预算紧缩、人员短缺和日益严格的内部威胁计划要求的挑战，也面临着来自董事会和（或）股东的压力——要采取正确的应对方法以防止内部威胁对企业的人员、财务、系统、数据和声誉的造成威胁。

有什么解决方法呢？唯一合乎逻辑的答案是：将注意力集中在风险最高的员工身上一——也就是那些最有可能进行欺诈、信息披露、职场暴力、间谍活动、蓄意破坏或其他对公司不利事件的受信任员工。

我建议采取以下四个步骤来识别并阻止高风险内部人员。

步骤一：尽早使用所有可用数据建立上下文

上下文对分析过程至关重要。当分析师看到一个或一组告警时，他们会提出以下五个问题：

1. 何人：这个人是谁？他们的工作职责是什么，正在做什么？他们是具有特权访问权限的用户吗？过去是否发生过安全事件？
2. 何事：这个人使用的是什么设备？是否涉及公司 IP 或客户数据？
3. 何地：这些人的实际位置在哪（办公室、VPN、旅行途中、咖啡店）？
4. 何时：发出告警的时间是在周日下午还是工作周的下班时间？
5. 何因：告警涉及活动是否与工作相关，是否在他们的职责和项目范围内？这个人以前这样做过吗？其他类似职责的工作人员会这样做吗？

用户和实体行为分析（UEBA）工具可以提供一些上下文，如名称、标题、开始日期、状态、部门、位置、经理以及观察列表，这些上下文可能表明访问级别或高风险活动。但是，这些属性通常仅在特定技术活动发生时才能促使生成较高的风险评分。

公司应考虑获得包括入职记录、工作经历、工作模式、差旅和费用记录、标识与打印机日志、绩效评级和培训记录等其他相关数据。

最重要的是，上下文数据应在分析过程开始时就可利用，这样就可以立即识别出高风险用户。然后，所有的后续分析都应专注于这些高风险用户的活动，而不是那些针对低风险内部人员的永无休止的告警流。

步骤二：根据访问权限和工作职责确定高风险内部人员

根据内部人员的访问级别和工作职责，很多人可以被判定为潜在的高风险人员（高管、企业管理人员和数据库管理员），而其他人员则为低风险人员（招聘人员、营销人员和联络人员）。

具有相似权限和工作职责的员工之间的风险水平也可能有所不同。假设在财务部门中有一小部分员工（A 组）直接参与编制合并财务报告。同时，B 组员工仅为报告准备独立的信息子集，因此访问权限受限。与 B 组相比，A 组非法披露信息的风险显然更大。除了以上的 A 和 B 组两组人员，在他们的报告对外公布之前，可能需要打印出来，这时行政助理就具有访问该报告的权限（虽然按照级别划分，该助理可能并没有查看该报告的权限）。这个情况类似于国内的领导秘书或助理，这些行政人员的泄密风险同样非常高。

步骤三：收集并评估行为指标

恶意内部人员通常会开发策略和技术，以打破他们在组织机构中因位置和访问级别所受的限制。爱德华·斯诺登（Edward Snowden）就是一个例子。斯诺登其实也暴露出了一些明显的痕迹，现在看来，如果当时把这些痕迹联系到一起，组织机构是能够觉察到安全风险的。

下列行为可能表明内部人员风险的增加：

- 安全事件历史记录
- 行为问题

- 经证实的职业道德/社会伦理问题
- 出勤问题
- 异常休假模式
- 国外旅行/联系记录
- 异常工作/活动时间
- 工作以外的暴力报告
- 酒精/非法药物滥用
- 威胁公司、上级领导、同事、客户
- 感觉被低估/收入过低
- 举止改变
- 拒绝工作分配
- 脱离团队
- 与同事/上级领导发生冲突
- 在社交媒体发表负面帖子
- 财务问题
- 逮捕
- 违反政策
- 数据渗漏
- 访问高风险网站
- 突然删除文件
- 未经授权的访问尝试

对一些公司来说，如果不完全禁止以上行为，那么收集和使用这些行为的证据就会变的非常微妙。也就是说，目标是提供关键的行为指标，为步骤四中描述的风险模型提供信息。

步骤四：根据上下文与行为开发风险评分模型

组织机构需要在专门设计的模型中评估来自步骤一的用户上下文数据、步骤二的内部人员工作职责和访问级别以及步骤三中的行为指标，以评估和确定内部风险的优先级。

我发现，最有效的分析方法是使用与不同主题专家协作开发的概率模型来识别高风险人员。

该模型本质上是一个风险基线，综合了安全、心理学、欺诈、反情报、IT 网络活动等领域主题专家的知识。每个模型节点都代表行为和压力源，当这些行为和压力源分解为最基本的元素时，这些行为和压力源可以用数据度量，这些数据可以作为模型的证据。

此模型的输出是每个人的风险评分，并随着新数据的可用而不断更新评分。至关重要的是，该模型还需要在整个推理链中提供透明度，并对个人身份信息进行屏蔽，以保护个人隐私。

有了正确的数据类型——不仅来自网络监控系统，还包括上面列出的行为指标和开源数据源——具有最高风险的内部人员将很快显现出来。

结论

任何完善的内部威胁缓解计划都需要将政策、流程和技术结合起来，还需要正确的领导，以在整个企业范围内沟通和推动计划实施。

然而，即使所有的步骤都做到位，这个计划也不应止于查找不良行为者。相反，一旦发现了高风险用户（假设他们没有做任何非法的事情），公司应积极与他们沟通，努力降低风险，让他们再次发挥自己的价值。

毕竟，他们一开始就获得内部人员权限是有原因的。

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，截止到 2019 年 9 月 30 日，安天的威胁检测引擎为全球超过六十万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”等几十个高级网络威胁行为体（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络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，“您们也是国家队，虽然您们是民营企业”。

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>