简译版

通过数据安全分析减少数据泄露的危害

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	Reduce the Harm of a Data Breach With Data Security Analytics		
原文作者	辛西娅·卢（Cynthia Luu）	**原文发布日期**	2021 年 8 月 31 日
作者简介	辛西娅·卢是 IBM 数据保护解决方案 Security Guardium 的产品营销经理。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/posts/reduce-data-breach-data-security-analytics/		
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	安全自动化是指，在检测和遏制攻击和入侵企图方面能够减少或替代人工工作的工具。安全自动化包括依赖于人工智能（AI）、机器学习、安全分析和自动化安全编排的解决方案。调查发现，具备成熟安全分析解决方案的受访企业，其数据泄露的成本比安全分析解决方案不太成熟的企业低 32.9%。安全 AI 和自动化还可以显著减少检测和响应数据泄露的平均时间，这反过来又会降低平均成本。		
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。		

通过数据安全分析减少数据泄露的危害

辛西娅·卢

2021 年 8 月 31 日

在过去的一年里，数据泄露的平均总成本增加了近 10%，达到 424 万美元。这是 IBM Security 年度数据泄露成本报告历史上的最高值。这是由多种因素造成的，包括新冠疫情造成的远程办公激增和数字化转型等。关键行业正在努力改善其网络安全计划，以适应不断变化的数据环境和 IT 基础架构。如今，自动化已经成为对抗数据泄露的一种重要手段，企业需要考虑适应性强、智能且互联的安全工具。

安全自动化是什么？

安全自动化是指，在检测和遏制攻击和入侵企图方面能够减少或替代人工工作的工具。安全自动化包括依赖于人工智能（AI）、机器学习、安全分析和自动化安全编排的解决方案。

调查发现，具备成熟安全分析解决方案的受访企业，其数据泄露的成本比安全分析解决方案不太成熟的企业低 32.9%。安全 AI 和自动化还可以显著减少检测和响应数据泄露的平均时间，这反过来又会降低平均成本。

数据安全分析能够发现潜在威胁和风险用户

关键数据安全解决方案可以帮助安全团队发现本地和云中的敏感数据，并对其进行分类。这些解决方案还可以监控违反安全策略的数据活动，检测异常的用户数据访问。此外，通过内置的智能和互联功能，这些解决方案的效果可以更上一层楼。这些内置功能有助于发现最严重的风险和异常行为。此外，它们可以无缝地为安全运营中心（SOC）创建票证，有助于 SOC 查找和修复威胁。

无论企业是否面临活跃的数据泄露风险，安全团队都要处理大量的噪音和告警。因此，他们需要实时、快速地识别和关注最严重的威胁。为此，他们需要一目了然的风险视图，以便清晰地看到高风险区域——分析师可以浏览、阅读这些区域，并深入查看更多信息。此外，高级分析（包括基于序列的分析、异常检测分析、风险识别算法和威胁检测分析）也可以帮助安全团队进行自动化的威胁猎杀和优先级排序。这种内置的威胁情报有助于精简检测

和调查。这样一来，安全团队就可以将时间和精力花在最重要的任务上了。

通过安全分析防止数据泄露或内部人员威胁

防止内部人员威胁是一个关键用例，尤其是对于远程办公的员工而言。数据分析可以帮助安全团队对风险用户进行评分，以便进一步查看。查看之后，数据库管理员可以制定策略，根据需要从视图中编辑数据。或者，他们可以立即采取行动，阻止用户访问数据。此外，安全团队可以通过数据隐私规则和零信任策略，扩展这些保护措施。

无论企业面临数据泄露还是其他问题，都应该打破孤岛并加快响应流程，这样可以降低风险。因此，安全团队应寻找具有预置集成和开放应用程序编程接口（API）的解决方案。通过这些解决方案，跨团队和工具的交流会更加容易，有助于精简开票流程，减少事件处理时间。此外，安全团队还应精简分享见解的流程，以便及时为 SIEM 和 SOC 提供信息。自动化、流程标准化和集成都可以加快事件响应速度，有助于降低数据泄露的总成本。

数据安全策略是零信任策略的一部分

侧重数据丢失预防和访问控制的安全策略，也能够为其他方面提供帮助。举例来说，数据安全策略是零信任模型的一部分。零信任方法假设用户 ID 和网络流量已经受到攻击，并依靠人工智能和分析技术不断验证用户、数据和资源之间的连接，而非盲目信任它们。如今，许多工作场所正在转向远程办公，且其之间的连接越来越少。零信任策略可以帮助企业保护其数据和资源，实现在正确的环境中受限访问，以防止和最大限度地减少数据泄露或其他网络攻击。反之，强大的数据安全计划也能够为零信任策略和控制提供支持。

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