

简译版

## 保持强有力的安全度量框架

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	Keeping a Strong Security Metrics Framework Strong		
原文作者	约书亚·戈德法布 ( Joshua Goldfarb )	原文发布日期	2020 年 2 月 11 日
作者简介	约书亚·戈德法布是一位资深的信息安全专家。		
原文发布单位	Dark Reading		
原文出处	<a href="https://www.darkreading.com/threat-intelligence/keeping-a-strong-security-metrics-framework-strong-/a/d-id/1336962">https://www.darkreading.com/threat-intelligence/keeping-a-strong-security-metrics-framework-strong-/a/d-id/1336962</a>		
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 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>		

# 保持强有力的安全度量框架

约书亚·戈德法布

2020 年 2 月 11 日

安全团队需要花费大量精力来构建可靠的度量标准,以便更好地为组织机构服务并增加其价值。但是,随着时间的推移,保持这一框架的稳健也是需要战略投资的。不幸的是,这是一个经常被忽视的领域。

以下有 10 个技巧,可以帮助您维护安全度量框架的价值。

## 1. 与受众交流

制定度量标准是为了向安全组织的受众提供重要的信息,而不是为了度量标准本身。因此,确保您报告的内容能够满足受众的信息需求、关注的问题和疑虑是至关重要的。您需要定期与利益相关者沟通,征求、接受并整合他们的反馈。您的受众不会阻碍您制定度量标准,相反,度量标准是为他们而制定的。

## 2. 保持警惕和协调

不要只是报告度量指标——要分析、理解、监控并调整它们。如果您看到一个或多个指标正以一种令人不安的方式发展成趋势,那么请深入了解为什么会出现这种情况,以及它对业务的影响。当您持续监控指标时,您将能确保这些指标所衡量的风险不会上升到您无法接受的水平。如果风险水平大幅提升,您可以采取正确的措施来有效地控制该风险。

## 3. 确保数据准确性

一个框架的好坏取决于它的基础数据的好坏。您可能拥有相关度最高以及最及时的指标,但如果用于计算它们的数据不准确、不一致和(或)有缺陷,那么这个指标也会有问题。默认情况下,可靠数据充当输入,产生的指标则可靠,而不可靠数据充当输入,产生的指标则不可靠。

## 4. 尝试使用不同的建模和聚合方法

也许去年您建模框架和聚合度量指标的方式取得了很好的效果。但也许从那时起情况已经发生改变，那种方法将不再奏效。如果您已经模块化地构建了度量标准，那么可以在各种不同的模型和聚合中利用它们。从而找到一个适合您当前企业环境的方法

## 5. 保持控制措施

一个成熟的度量框架包括度量指标到控制措施的正确映射。要保持这两者间的正确映射。随着时间的推移，控制措施可能会在实质、重要性和（或）优先级上发生变化。此外，映射可能会演变为不正确的。确保控制措施和度量指标之间的精确映射，使安全团队能够不断地评估和衡量控制措施对企业整体安全态势的有效性。

## 6. 注意风险

风险不是静态的，也不是轻易能发现的。它是连续的、动态的和流动的。关注不断变化的风险环境，可以使组织机构将重点放在减轻其面临的最重要和最相关的风险上，同时减少花在不太重要和不太相关的问题上的时间和资源。这使得组织机构能够应用有限的安全资源，最大程度的减小风险。

## 7. 注意度量的精确范围

在设计和测量度量指标时，它会创建一个数据点。通常，这个数据点是一个数字或一个百分比，它本身并不能反映整体的情况，也不提供上下文环境。要为度量的风险添加重要的上下文内容，您需要设置一个可接受的范围以及该范围的可接受偏差。随着时间的推移，这些范围可能需要进行调整，以反映业务环境和威胁环境演变的变化，这些变化将影响您所测量的各种数据点的误差。注意范围，确保误差符合可接受的风险水平。

## 8. 利用情报

除了协助和告知预防与侦查能力，情报还可以为度量标准提供信息。好情报可以帮助您了解现有威胁，并识别到新威胁。反过来还可以帮助您不断地评估您的度量标准是否解决了真正威胁组织机构的威胁。

## 9. 保持联系

同行业的组织机构、行业团体和专家可以帮助组织机构了解其相对于其他具有类似规模、行业和地理位置的其他机构的相关情况。这些联系可以提供必要的信息，使您的度量标准框架保持强大。

## 10. 要有效率

如果汇总和报告度量指标的过程本身就很令人头疼，那么没有度量框架是一成不变的。为了使度量标准切实可行并持续提供价值，它们需要具备可扩展性。将度量标准所需的数据合并到尽可能少的系统中。当需要指标时，利用自动报告和仪表板来简化生成指标的过程（理想情况下自动且近乎实时）。这确保了度量指标始终都是最新的。它还减少了您在创建、设计、开发和生成新度量标准方面的投资，而这些度量标准反过来又能鼓励创新、创造力和前瞻性思维。

## 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>