简译版

事件响应：防止误报的五种方法

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	Incident Response: 5 Steps to Prevent False Positives		
原文作者	科恩·范因佩（Koen Van Impe）	**原文发布日期**	2020年9月4日
作者简介	科恩·范因佩是一位安全分析师。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/cyber-incident-response-false-positives/		
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。		

事件响应：防止误报的五种方法

科恩·范因佩

2020 年 9 月 4 日

威胁情报平台中的“误报”（false positive）使安全团队疲惫不堪。这就像是开车开到了错误的地址——虽然到达了某个地方，但是却浪费了本可以达到预期目的地的时间。对于安全团队来说，了解如何过滤误报可以节省时间，更有效地应对实际威胁。对现代安全运营中心（SOC）来说，如何进行威胁过滤，以及发现错误时如何处理都应纳入事件响应计划。

误报是什么？

误报是威胁情报、安全运营和事件响应中的常见问题。错误的攻击信标（IoC）或安全告警显示某处存在问题，但实际上并不存在。对于分析师而言，误报会分散其注意力，使其无法及时解决真实存在的问题，造成时间和资源的浪费。

无论安全团队旨在阻止恶意活动（例如过滤恶意活动）还是检测恶意活动（例如取证调查），误报都会将其指向错误的方向。如果安全团队使用信标进行威胁分析，则错误标记的信标会使其在评估风险或威胁时误入歧途。

除了误报，安全团队还可能会遇到“漏报”（false negative）的情况。漏报会使安全团队忽视某些网络安全事件或威胁。误报和漏报都会导致安全团队疲乏等问题。除了资源浪费和经济损失，它们还会破坏组织的声誉，使运营团队未来的协作更加困难。

除了上述两种情况，安全团队还有可能会遇到“正报”（true positive，即正确识别事件）和“正拒”（true negative，正确地拒绝事件）。

良好的事件响应计划应包括情境信息

误报通常与情境有关，对于每个企业或个人而言都是不同的。企业认为是真实告警的内容，可能会被另一家企业认为是误报——例如，运行 TeamViewer 或向谷歌公共 DNS 解析器 8.8.8.8 发起 DNS 请求。

查看威胁报告时，企业可以通过以下几种方式获取情境信息：

- 获取信标的更多描述性细节，例如用于启动流程的特定选项或参数。
- 检查该信标如何与其他信标（一系列活动、相关行动或使用的策略和技术等）建立关联。
- 了解发现信标时的详细条件和环境信息。
- 了解信标的生命周期。五年前相关且准确的信标，现在可能并不被认为是恶意行为了。

如果缺乏必要的情境信息，威胁数据的有效性就大打折扣了。这类数据可能也有用，但容易出现错误和误解。与具有情境信息的数据相比，这类数据对事件响应的价值较小。

不幸的是，没有任何一种方法能够消除所有误报。企业可以采取以下措施，降低误报的发生频率及其对事件响应计划的影响。

1. 防止威胁情报报告中出现误报

首先，企业应防止威胁数据中出现误报。企业不希望内部或公司资产等信标出现在网络威胁情报中。例如，企业不希望触发告警的是其代理服务器或 Sharepoint 站点的名称。如果企业与其他组织共享威胁信息，且在共享数据中添加了此类信息，就会带来敏感信息泄露风险。不过，这些信标可以提供情境信息。

除公司信息外，属于 RFC 1918 CIDR 块（“专用”IP 地址）、RFC 3849（IPv6 文档前缀）或 RFC 6761（专用域名列表）的信标，也不应出现在共享信息中。

2. 向分析师告知误报的可能性

其次，企业应向分析师告知误报的可能性。这通常涉及良性信标，例如前面提到的谷歌公共 DNS 解析器。在向分析师发送此类通知时，还应向其提供“平台即服务”提供商、已知端口扫描程序、热门域（例如 Alexa Top 1M）、根名称服务器、热门公共解析器和常用云服务（例如 Office 365）等网络地址空间的白名单。

在分析师处理威胁数据时，企业可以以可视化方式将此通知呈现给他们；也可以将通知附在基于这些信标编写的安全告警中，并附上置信度得分（例如，误报风险为“高”）。

如果企业对其白名单的质量很有信心，可以不把这类信标放在威胁数据中。企业需要注意，不要盲目启用或信任白名单，而是要谨慎考虑攻击者控制了哪些数据——企业当然不

希望启用的白名单中有最让其头疼的攻击者的基础架构。

企业还可以使用社区提供的白名单。一个很好的例子是，可用于恶意软件信息共享平台（译者注：Malware Information Sharing Platform，MISP 是一种开源软件解决方案，用于收集、存储、分发和共享有关网络安全事件分析和恶意软件分析的信标和威胁。共享信息有助于更快地检测到攻击并提高检测率，同时还可以减少误报）告警列表的白名单。

3. 上报发现（恶意活动和误报）

第三种方法是上报发现，无论发现的是恶意活动还是误报迹象。基于这些发现，企业可以向信标赋予分值或质量等级。这是安全运营团队和事件响应团队，到威胁情报团队的反馈循环。这为他们提供了上报活动的机会，这些活动可能是恶意活动，也可能是误报。

这一步的关键是，使信息的上报和使用尽可能简单。一个非常简单的解决方案是 SightingsDB，它甚至可以从 Docker 容器运行。

4. 向分析师告知发现

第四种方法是将这些发现告知分析师。企业可以选择定期报告，也可以在达到特定阈值时统一报告。报告数据的方法包括：威胁情报平台中的仪表板或电子邮件。

完成这一步的最佳方法是，在网络威胁情报团队中设立专门的职位。此人可以定期查看报告并进行验证。

5. 手动处理可疑信标，精简网络威胁情报。

第五种方法是手动处理和验证可疑信标，发挥“人”在预防误报中的主动作用。如果经过验证，这些信标是误报，则防止这些信标进一步发送给安全团队或事件响应团队。

企业可以将该任务赋予第四种方法中所述的“查看和验证报告”人员；也可以赋予其他人员以实现双重验证。理想情况下，这能够减少将来的误报，有助于安全团队节省时间，使其有更多的时间来应对真正的威胁。

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