财富 100 强金融机构通过基于风险的警报来提高检测和调查能力

主要挑战

这家主要金融机构生成的大量警报要求分析师花费大部分时间对警报进行分类，消耗了该组织几乎所有的分析师资源。

主要成果

在 Splunk 的帮助下，这家金融服务组织显著降低了警报数量，同时提高了真实正利率并运营 MITRE ATT&CK。

行业： 金融服务

解决方案： 安全和欺诈，企业安全

这家财富 100 强金融服务机构是美国最大的银行机构之一，对负责任地管理风险略知一二。

多年来，他们一直是颠覆性想法的早期采纳者，从互联网首次成为主流时推出在线交易，到免除客户的帐户费用。

这家跨国机构的安全团队负责保护公司的安全态势免受不必要的入侵，他们一直在关注变革性的技术和流程，以加强他们的防御。在 .conf18 上，他们遇到了一个给人留下深刻印象的话题：基于风险的警报 (RBA)。

当团队回国后，他们将实施 RBA 作为首要任务。RBA 增强了该组织现有的 Splunk Enterprise Security 解决方案，以展示一个不同的故事：基于属性的故事。观念和流程中发生的这些看似微妙的变化，为团队提供了一种更好的方法来收集相关的安全背景，并加速威胁搜寻。

这里越来越吵闹

从历史上看，安全运营中心 (SOC) 一直是一个嘈杂的地方。追求“完美”的相关性搜索以查明违规会产生太多的误报，并且不是检测活动的有效方法。

“在一天的 200 个警报中，只有一小部分需要进一步调查，大多数都与违反政策有关。”该组织的一名安全工程师说。问题是，无论何时大量警报到达 SOC，安全分析师都必须筛选所有警报，并尝试拼凑出正在发生的情况。SOC 通常缺乏相关机制来通过数据有效了解正在发生的情况。该团队将 RBA 视为一个机会，可以改进 SOC 内广泛接受的最佳实践，同时改进其检测、调查和复杂的威胁搜寻能力。

数据驱动的成果

65%
减少警报数量

~2x
改进警报精确度

改善
复杂的威胁检测

每个人都喜欢美好的结局

安全和业务之间的关系可以更加紧密，从历史上看，语言在这种脱节中扮演着重要角色。这位安全工程师说，RBA 给该团队带来的早期好处之一是“基于风险的警报让业务和安全部门可以说同一种语言”。

安全从业者在发言时，往往技术性非常强，这使得 SOC之外的大多数人难以理解其中的含义。风险属性是 RBA 的核心组成部分，它提供了使 SOC 和业务达成共识所需的通用语言。“以前，我们在一堆不同的地方之间转换，所以丢失了细节，而且过于技术化。”这位安全工程师说。“RBA 为特定用户/对象集中了所有风险属性。我们现在可以向 SOC 之外的团队展示，与用户/对象相关联的各种危险行为是如何交织到安全情境中的。”

使用框架作为指南

大量的警报会导致疲劳，安全分析师不成比例地承受了这种疲劳带来的冲击。这迫使许多分析师采取一种安全警报心态，这种心态特别关注与分类相关的活动。RBA 中驱动显著事件的属性为安全分析师提供了了解整个安全情境所需的背景。值得调查的属性可以映射到领先的网络安全框架，例如 MITRE ATT&CK，分析师现在可以花更多的时间对真正的威胁进行安全调查。借助 Splunk 平台，这家顶级机构的团队减少了误报，同时提高了整体检测覆盖率。

> 许多产品会出于业务或合规性目的而有所选择，但并不真正影响安全运营。配备了 Splunk Enterprise Security 后，基于风险的警报提供了真正的安全改进，同时清楚地展示了安全对企业的价值。”
>
> 金融机构 安全工程师

希望了解 RBA 如何帮助增强贵组织的安全运营？观看此演示。

21-18016-Splunk-Tier2-Fortune100-FinServices-A4-CS-102