IBM Security

关于 SIEM 的五大误解

您最近是否研究过 SIEM 解决方案？因为一切都已改变。

有传言说 SIEM 解决方案笨拙又复杂，因此只适用于大型企业。的确，有些 SIEM 只适用于大型企业，但是这种误解忽略了为各种规模的企业量身设计的更先进的 SIEM 解决方案。

网络安全行业面临严重的技能短缺已不是什么秘密。安全解决方案（SIEM 或其他产品）必须支持您在资源（可能）有限的情况下高效地开展工作。

我们将化解关于 SIEM 的五大误解，并探讨如今 SIEM 解决方案能为您带来哪些收益。

IBM Security

误解 #1

SIEM 只能检测已知威胁；

无法检测未知威胁。

SIEM 解决方案只利用规则检测威胁，要编写有效的规则，您首先需要知道要检测什么。

真相

有效的 SIEM 结合利用规则、异常检测、机器学习和行为分析技术，发现已知和未知的威胁。

它们还使用先进的关联技术，连接点并了解相关的威胁活动。如果您的 SIEM 中有预置的高级分析和规则，您就可以立即利用这些技术处理网络、资产、用户和应用活动，这样您不仅能检测已知的威胁，还可以识别可能象征未知威胁的异常活动。

IBM Security

误解 #2

SIEM 仅适用于拥有先进安全团队的大型企业。

传统观点认为，因为市场上最好的 SIEM 解决方案可以扩展到支持最大的企业，所以它们仅适用于大型企业。

真相

最好的 SIEM 解决方案适用于各种各样的企业，无论它们是刚刚开始使用安全监控的成长型企业，还是需要高级用例的《财富》20 强跨国企业。

事实是，尽管许多先进的安全团队更喜欢利用额外的功能来支持高级用例和专业用例，但是一款好的 SIEM 解决方案并不需要额外的功能来交付价值。一款理想的解决方案可以帮助您从标准用例（如威胁检测、云监控和合规性报告）入手，也就是即装即用。随着实践日益成熟，业务不断增长，SIEM 应该扩展到支持更多的环境、多个地理区域和高级用例，例如深度数据包检查、DNS 分析和紧密集成的事件响应编排。

IBM Security

误解 #3

SIEM 需要大量的数据，而且收集这些数据的成本非常高。

因为市场上某些供应商的产品以很快变得非常昂贵而闻名，导致一些安全团队认为所有的 SIEM 都这么贵。

真相

如果您考虑的供应商是根据存储的数据量收费，那么这会非常快速地让成本变得很高。但是不同的供应商会有不同的解决方案定价模式。

在您做任何事情之前，想想您要解决的问题：您是不是一家需要保护支付卡数据的零售商？您的业务是否正在迁移到 Amazon Web Services，您是否需要了解新环境？为安全目的而收集的数据应该帮助您处理独特的用例。如果您不需要面面俱到的分析，那么就不要这么做。也就是说，如果您还有数据保留需求，以便满足法规或企业政策要求，您的 SIEM 供应商应该能提供仅用于存储、搜索和报告的平价解决方案。如果能只分析对贵企业来说重要的内容，并将其余日志和事件数据发送到低成本存储中，您就可以在不消耗整个预算的情况下实施 SIEM 项目。

IBM Security

误解 #4

您需要一支全职的数据科学家团队，才能有效使用 SIEM。

他们经常说，要有效使用 SIEM，您需要一名全职数据科学家（或一支数据科学家团队）从零开始构建所有的规则和分析功能。

真相

如果您不能（或不想）找到并聘请一支恰好了解安全性的数据科学家团队，那么就找一个能够提供现成预打包内容的供应商吧。

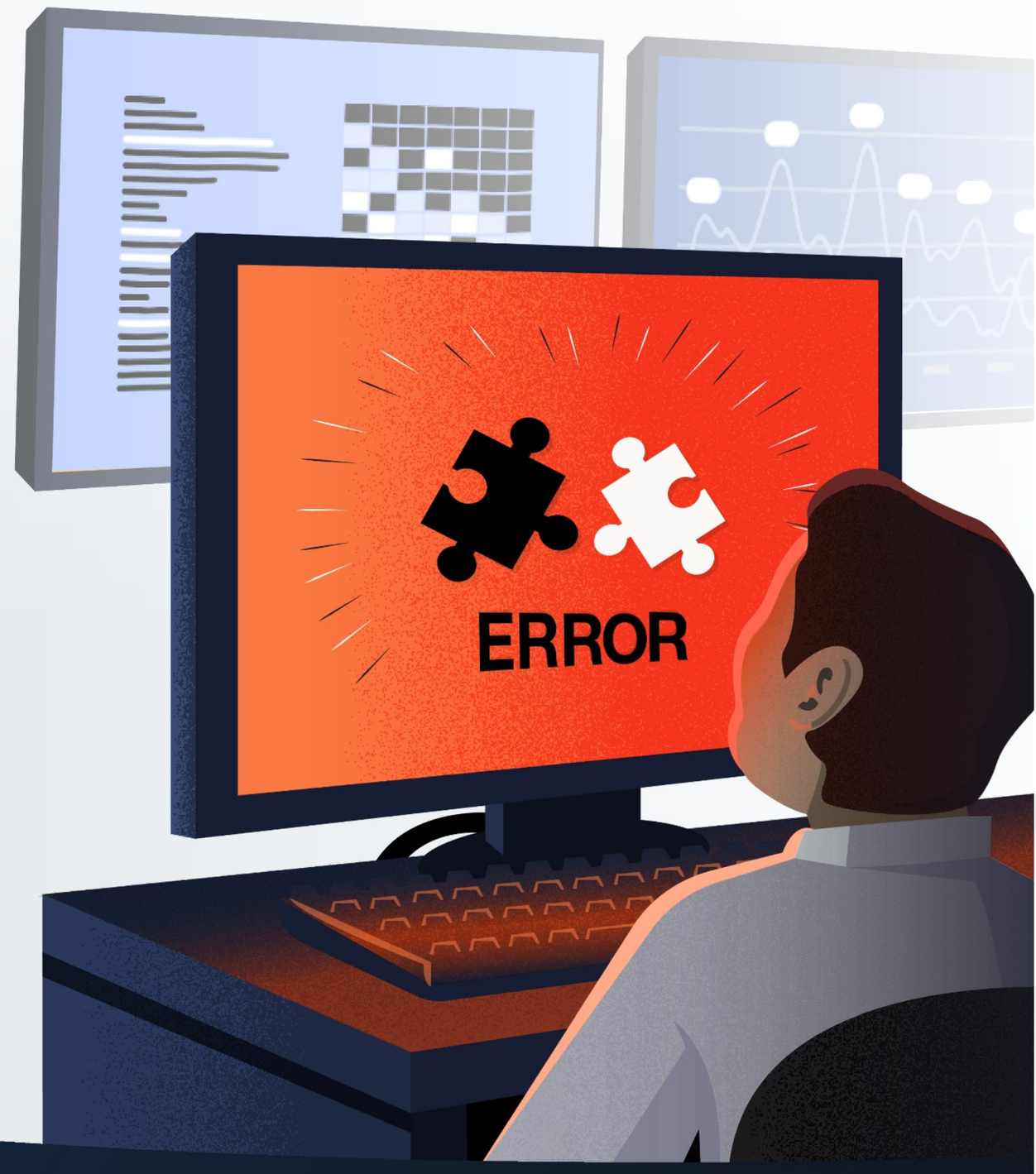
有些供应商采取的方法是，既然解决方案无论如何都可能要定制，那为什么不从头开始构建解决方案呢？事实上，如今的安全团队根本没有资源来承担这样一个需要如此专业技能的大型项目。不论使用哪款 SIEM 解决方案，您都需要向它提供有关您的网络的信息，但是在这之后，您应该能够利用预先编写的规则、分析和相关策略，立即检测威胁。您不应该从头开始一切工作。如果您仍然担心，那么您需要了解的是许多 SIEM 供应商都会与托管安全服务提供商 (MSSP) 合作，让您可以获得先进 SIEM 的所有收益，同时得到安全运营专家的帮助。

IBM Security

误解 #5

SIEM 很难与环境中的其他解决方案相集成。

关于 SIEM 一种普遍的说法是：尽管 SIEM 依赖其他解决方案的数据来提供价值，但它们很难与其他解决方案相集成。



真相

领先的 SIEM 解决方案必须易于集成。幸运的是，很多 SIEM 都具有这一特点。

十年前问世的早期 SIEM 未能随着不断变化的需求和不断进步的技术而发展，因此很难与其他解决方案相集成。然而，这类产品要么已经退出了历史舞台，要么正在苦苦挣扎。如今，领先的解决方案提供了数百种与商用 IT 和 OT 技术的现成集成，同时还提供了简单的连接器，与自定义应用相集成并解析应用日志。如果您想知道有哪些供应商全面支持的现成集成，那就去看看不同供应商的客户支持网站或者浏览他们的应用交换。

IBM Security

如今人们对 SIEM 的刻板印象往往是过时的技术造成的。如果您在十年前（甚至五年前）评估一款 SIEM 解决方案，那么很多重要的误解都不是误解。但是，在技术和威胁环境不断进化的同时，SIEM 也在进化。

如果您很难检测威胁或理解日志管理器中的日志，那么您可能需要立马重新审视 SIEM 解决方案，自己研究它们发生了多大的变化。

IBM Security

关于 IBM QRadar

IBM QRadar Security Intelligence Platform 是一款灵活的解决方案，它帮助您集中洞悉企业范围内的安全数据，并从最高优先级的威胁中挖掘可执行的洞察力。

该解决方案基于 QRadar SIEM，其中包括数百条预配置的规则和分析，以及来自 IBM X-Force 的威胁情报。借助 500 多个现成的集成功能和 160 多个应用，客户可以快速上线运行，并轻松添加新的安全和合规用例。此外，客户还可以通过一个单独的界面添加并管理多个完全集成组件，用于日志存储、用户行为分析、网络数据包检测、漏洞管理以及基于 AI 的威胁调查。这样，客户就可以选择从小规模或大规模入手，根据需求的变化轻松扩展或缩小规模。

有关更多信息，敬请访问：

www.ibm.com/qradar。