解决方案：IBM Security　　行业：中央政府/联邦政府

一家加拿大政府机构

采用认知方法，检测威胁

该机构采用了 IBM 的自动化安全智能和分析解决方案，摒弃了手动事件关联流程。这样，他们的安保人员就能快速识别需要调查的安全事件，并获取更多相关背景信息，更快速地检测出威胁，发现需要解决的漏洞。

联系 IBM

分享

业务挑战

一家加拿大政府机构需要一款先进的安全信息和事件管理（SIEM）解决方案来帮助他们快速检测和应对潜在的安全威胁，但是同时他们的可用资源也相当有限。

转型

该机构采用了 IBM 的自动化安全智能和分析解决方案，摒弃了手动事件关联流程。这样，他们就能快速检测出安全威胁，并发现漏洞。

成效

100,000 个问题/警报	7 天	10,000 个漏洞
从 100,000 个问题/警报减少至每天只有 10 到 20 次攻击，并且还对这些攻击进行了动态地排序	7 天完成解决方案的部署，并开始实现价值和投资回报	扫描 10,000 个漏洞，发现安全缺口，划分主动响应措施的优先级

案例之业务挑战篇

一个“大海捞针”的故事

如何分析并解读数以百万计的事件，以发现对其机构的攻击，这是全球安全团队面临的共同挑战。一家加拿大政府机构发现，随着网络日志、服务器日志和防火墙日志的与日俱增，由一个小型的安全专家团队来处理事件关联流程已经完全不现实。

“与其提供的功能集相比，QRadar 提供了一个卓越的价值主张。”

— 一家加拿大政府机构的架构和安全总监

该机构安保人员的当务之急是，部署一款安全信息和事件管理解决方案，来自动分析数百万事件、提供上下文，并划分潜在安全威胁的优先级。

该机构的架构和安全总监表示，“我们没有一个简单的方式来审查和关联我们收到的所有安全警报和日志。我们从不同的设备中获取许多种不同的日志，这些日志都需要审查。这种情况下，我们几乎不可能读取完所有的日志以检测出异常情况，就更不用说作出快速的响应了。其中的难度就好比大海捞针。”

面对有限的资源和事件，该机构必须简化部署，这一点至关重要。

“我们评估了许多不同的解决方案，希望从中找到满足以下条件的解决方案：能快速上线运行；能与不同设备兼容；并且很灵活，”该架构和安全总监说道。“我们没有足够的人力和时间来组建一支大型团队部署解决方案。”

“QRadar 帮助我们提高了工作效率。我们不用再筛选日志，而是能专注于关键问题。”

— 一家加拿大政府机构的架构和安全总监

案例之转型篇

借助高级分析应用，网络犯罪提前知

IBM® QRadar® Security Intelligence Platform 能够感知给该机构带来最大风险的威胁，并划分这些威胁的优先级，从而帮助该机构提前洞悉网络威胁。

现在，他们的安全团队每天都能收到一个安全优先事项表，从而在出现任何风吹草动时能快速作出响应，将威胁扼杀在摇篮。事实上，QRadar 已将该团队的近 10,0000 个潜在的日常问题减少至 10 到 20 个日常优先事项。

比如，在以下任何一种情况下，安全分析师都能快速收到警报，立即采取响应措施：创建和修改账户；大量数据流出企业；与命令和控制服务器通信；与匿名器（掩盖连接行为的主机）通信；出现可疑的网络行为模式；与已知的垃圾邮件发送者、钓鱼攻击网站和鱼叉式钓鱼网站通信。

为了提供这些情报，QRadar 平台中内置的高级分析工具每天会关联和解读机构架构中的近 2.16 亿事件和 1.44 亿工作流。这些数据会与 IBM X-Force® 源源不断提供的威胁反馈结合起来，将看似单独的事件放在一个上下文中，让员工能分辨机构是否存在风险。

“QRadar 帮助我们提高了工作效率，为我们提供了前所未有的可视性，”其架构和安全总监说道。“我们不用再筛选日志，而是能专注于关键问题。这等于是让我们的重心重回正轨。”

借助 IBM Security QRadar Vulnerability Manager，安全团队能主动发现安全缺口，支持补救和缓解措施的优先级划分。

该总监指出，“现在，我们能安排并执行外部漏洞扫描，对照包含 10,000 多个漏洞的 PCI 标准，扫描外部主机。“在初步扫描了总部的所有设备后，我们发现 Windows 7 团队在安全配置上做得相当出色，但我们也发现了一些非安全的工作站。电子邮件、钓鱼攻击、鱼叉式钓鱼攻击和水坑式威胁向量会给操作区域带来最大的风险。但是我们发现我们的操作区域仍然处于相当良好的状态。”

快速实现价值

快速部署是该机构的一个目标。借助 QRadar 应用，再加上 IBM Managed Security Services 提供的配置支持，该机构能够在短短 7 个工作日内就获得投资回报。

架构和安全总监认为：“与其提供的功能集相比，QRadar 提供了一个卓越的价值主张。设备是在一个周五上线的。下一个周二，在 IBM 的支持下我们启动了配置，然后在周四就开始获得有用的情报。凭借丰富的知识和专业技能，IBM 的团队帮助我们根据我们的环境快速调整好了解决方案。”

对于员工来说，以后的系统调整工作也很简单，只需要安排一名员工每天花几个小时就能完成。收集了新的情报后，通过调整阈值和筛选条件，安全团队能进一步减少他们必须处理的警报和误报数量。

案例之成效篇

更快地终止针对性攻击

QRadar 平台拥有先进的认知分析和感知功能，能帮助该机构的安全团队以前所未有的速度识别和响应安全威胁。事实上，部署到位后，QRadar 平台就捕捉到了一个来自 McAfee ePolicy Orchestrator 服务器的“有病毒的”日志访问，并将其与防火墙日志关联，结果我们发现了一个与外部 IP 地址的通信记录。

架构和安全总监表示：“过去，我们只能等待最终用户报告异常行为，而且前提还是最终用户要能发现异常。QRadar 基于汇总数据创建了一次“攻击”，并根据相关性、严重性和可信度进行了排序。这样，我们就能更快地检测和应对事故，确保受保护的数据都留在企业内。”

此外，该机构还利用 QRadar 平台提供的洞察力，采取了其他安全措施来降低漏洞带来的风险。“我们针对过去未发现的某些漏洞，推出了更多策略和程序，”该总监补充道。

得益于这项工作，安全团队在整个企业的声誉也有所提升。

“自部署 QRadar 以来，我们在企业内的价值无疑得到了更多的肯定，”该总监表示。“我们提高了警惕，并且能更有效地监控和保护我们的网络，这让机构领导更有信心。”

关于该加拿大政府机构

该加拿大政府机构有一支小型的安全团队负责保护机构运营和市民服务免受网络罪犯的攻击。

解决方案组件

- IBM® Managed Security Services
- IBM QRadar® Security Intelligence Platform
- IBM Security QRadar Vulnerability Manager

下一步

如欲进一步了解 IBM Security QRadar 解决方案和 IBM Managed Security Services，请联系您的 IBM 代表或访问以下网站：ibm.com/software/products/en/category/security-intelligence 或 ibm.com/security/services/managed-security-services

查看更多客户案例或了解更多有关 IBM Security 的信息

联系 IBM

打印