Cargills Bank Ltd.

在斯里兰卡率先采用认知安全技术

网络犯罪分子双眼紧盯金融机构。Cargills Bank 采用积极主动的方法，借助认知安全解决方案 IBM® QRadar® Advisor with Watson™ 来更好地保护客户交易安全。分析人员可以轻松查看各种威胁数据，获得切实可行的洞察，迅速做出决策。

业务挑战

Cargills Bank 希望增强现有的防御网络安全能力，改进监控，并实施更强有力的预防协议，以便防范复杂的威胁。

转型

该银行使用行业领先的安全情报平台 IBM QRadar SIEM 以及 QRadar Advisor with Watson 认知功能，及早检测网络威胁并对其进行分类。

成果

防范
复杂的威胁事件，实施更强大的预防协议

加快
检测和准确识别网络威胁和警报的过程

转变
将数百万份安全文档转变为与特定威胁相关的切实可行的情报

业务挑战

应对瞬息万变的威胁形势

Cargills Bank 是一家位于斯里兰卡的新银行，以其无障碍、便利和包容的非传统业务模式而闻名。该银行以 Cargills 品牌 174 年的悠久历史和丰厚底蕴为基础，分支机构数量不断增加，并且在斯里兰卡全国各 Cargills Food City 购物中心设有 340 多个访问点。

“作为斯里兰卡最年轻的银行，我们没有设立传统的实体银行，是一家真正的数字银行，同时能够通过 Cargills Food City 购物中心的零售足迹来发展超市银行业务，”Cargills Bank 首席运营官 Rohan Muttiah 说道。“Cargills 拥有全国最大的价值链，这为我们的银行服务提供了独特的业务生态系统。”

由于复杂的网络攻击和不断变化的威胁格局持续困扰全球金融机构，解决安全问题一直是 Cargills Bank 的首要任务。Cargills Bank 希望增强现有的防御能力，改进监控，并实施更强有力的预防协议，以便防范复杂的威胁。

该银行还希望找到一种解决方案，帮助安全分析人员及时掌握海量安全数据，包括来自内部系统以及威胁情报、安全研究论文、安全博客、网站和分析威胁所需的其他外部信息来源的数据。

“我们致力于提升客户的数字银行业务体验，同时时刻留意新出现的安全威胁。随着网络犯罪变得更加有组织且愈加复杂，必须以成熟的技术为基础，部署具有高度适应性的预防、检测和响应功能，”Rohan Muttiah 补充道。

“ IBM 一流的认知安全服务产品组合将帮助我们防范威胁并缓解风险，支持和巩固我们领先数字银行的地位。”

— Rohan Muttiah，Cargills Bank 首席运营官

转型故事

利用人工智能技术来保障安全

Cargills Bank 实施了全面的流程来识别和评估潜在的解决方案。该银行选择 IBM QRadar Security Information and Event Management (SIEM) 解决方案进行全面的安全监控、威胁检测并获取实际洞察，同时采用 QRadar Advisor with Watson，这是首款利用 IBM Watson® AI 功能的安全解决方案，可帮助快速对潜在安全事件进行调查和分类。

“我们一直很清楚，传统的网络安全方法难再奏效。银行业整体倾向于依赖事后诊断和响应方法，”Rohan Muttiah 说道。他还指出，银行在维持 24x7 全天候响应能力方面面临困难，缺乏经验丰富的合格人员，并且潜在事件的数量超出了人力能够应付的范围。

IBM QRadar Advisor with Watson 是 IBM QRadar Security Intelligence Platform 的一部分，提供强大的认知功能，可以帮助安全析人员进行调查和采取响应措施。该解决方案结合来自 Qradar 的威胁情报和安全事件数据，通过利用 Watson 对安全博客、网站、研究论文和其他来源进行自然语言处理的能力，帮助分析人员调查潜在威胁，帮助将网络安全调查从几周或几天缩短到几分钟或几小时。

“越来越频繁的网络攻击也带来了大量相关数据，我们几乎无法迅速理解这些数据，”IBM 斯里兰卡和马尔代夫软件销售主管 Manori Unambuwe 说道。“Watson 已经接受过网络安全语言方面的训练，‘阅读’了超过 200 万份网络安全文件，让先前无法访问的研究报告信息可用于现代安全工具。”

IBM QRadar SIEM 可以检测异常，发现高级威胁并排除误报。它可以整合来自分布在整个网络中的数千个设备、端点和应用的日志事件和网络流数据，然后使用高级安全分析引擎对这些数据进行规范化处理和关联，从而发现需要调查的安全违规行为。

“Cargills Bank 通过使用 IBM QRadar SIEM 和 QRadar Advisor with Watson 来接收划分过优先级的实时警报，跨越了这些限制。“IBM 一流的认知安全服务产品组合将帮助我们防范威胁并缓解风险，支持和巩固我们领先数字银行的地位，”Rohan Muttiah 补充道。

“Cargills Bank 通过使用 IBM QRadar SIEM 和 QRadar Advisor with Watson 来接收划分过优先级的实时警报，缩短了调查时间，跨越了这些限制。”

— Rohan Muttiah，Cargills Bank 首席运营官

成果丰硕

遵守基于风险的信息安全方法

IBM 解决方案在当地的实施得益于两家 IBM 业务合作伙伴：技术合作伙伴 - 斯里兰卡的 Blue Chip Engineering Co. 以及实施合作伙伴 - 印度的 Secbounty Services Private Limited。

“在银行提供的即时可用环境中，我们在一周时间内实施了 IBM QRadar SIEM，并在不到一天的时间内启动和运行了 QRadar Advisor with Watson 组件，”Secbounty Services 创始人兼董事 Ramprasath R 说道。他补充说，Cargills Bank 的分析人员使用这款解决方案，在很短的时间内识别并隔离了安全威胁。

“有了 Watson，只需一个数据包，分析人员即可在几分钟内接收到调查所需的所有信息，”Ramprasath R 说道，这些信息包括人员姓名、涉及的恶意软件，以及攻击者的 IP 地址、URL 地址和域名。“手动获取所有这些信息需要花费数小时，还要搜索多个论坛，将 IP 地址与攻击者的身份和恶意软件类型关联起来。”

此外，该解决方案还帮助 Cargills Bank 遵守其基于风险的信息安全方法，该方法应用的治理结构包括董事会级别的风险小组委员会、基于 ISO 27001:2013 的信息安全委员会以及技术指导委员会。

“IBM Watson 支持我们遵守和实施与风险、信息安全和技术相关的关键政策和流程。认知型 SOC 支持我们与现有数据中心员工协同工作，同时通过开展与人工智能相关的培训和学习活动，助力他们实现职业发展，”Muttiah 说道。

CargillsBank
Banking on the Human Spirit

关于 Cargills Bank Ltd.

Cargills Bank Ltd. 是斯里兰卡的一家牌照商业银行。174 年来，Cargills 品牌一直忠实地服务于斯里兰卡人，始终坚守自己的价值观和商业道德规范。Cargills Bank 秉承这一传统以及“人文银行”理念，本着包容和无障碍原则，通过提供各种产品，如 Cargills Cash Savings Account（覆盖超过 340 家 Cargills Food City 购物中心）和 Cargills Bank 借记卡，为大众提供银行服务。

解决方案组件

QRADAR | QRadar Advisor | QRadar SIEM

采取下一步行动

了解有关 IBM Security 企业安全与合规安全解决方案的更多信息，请访问：
https://www.ibm.com/cn-zh/security

如需进一步咨询，IBM 随时为您提供帮助

电话咨询 (工作日9:00-17:00)：

手机：400-810-1818 转 2395

座机：800-810-1818 转 2395

请 IBM 专家与我联系

扫码关注微信公共账号"IBM 安全"
汇集全面、详实的 IBM 安全资料
第一时间为您提供安全解决方案

IBM Security

75 Binney Street

Cambridge MA 02142

美国出品

2018 年 5 月

用户负责评估和验证与 IBM 产品和程序一起运行的其他任何产品或程序。

本文档内的信息“按现状”提供，不附有任何种类的（无论是明示的还是默示的）保证，包括不附有关于适销性、适用于某种特定用途的任何保证以及非侵权的任何保证或条件。IBM　产品根据其提供时所依据的协议和条款获得保证。

客户应遵守适用的法律和法规。IBM　不提供法律建议，也不表示或保证其服务或产品将确保客户遵从任何法律或法规。

良好安全实践声明：IT　系统安全性涉及通过防御、检测和响应来自企业内部和外部的不正当访问来保护系统和信息。不当访问可能导致信息被篡改、销毁或盗用，也可能导致系统被损坏或误用，包括攻击他人。任何 IT 系统或产品都不应被认为是完全安全的，并且没有任何单一产品或安全措施能够完全有效地防止任何不当访问。IBM　系统和产品旨在成为全面的安全方法的一部分，这样的方法一定会包含其他运营规程，并且可能需要其他系统、产品或服务配合才能获得最好的效果。IBM　不保证任何系统和产品可以完全抵御来自任何一方的恶意或非法行为。