



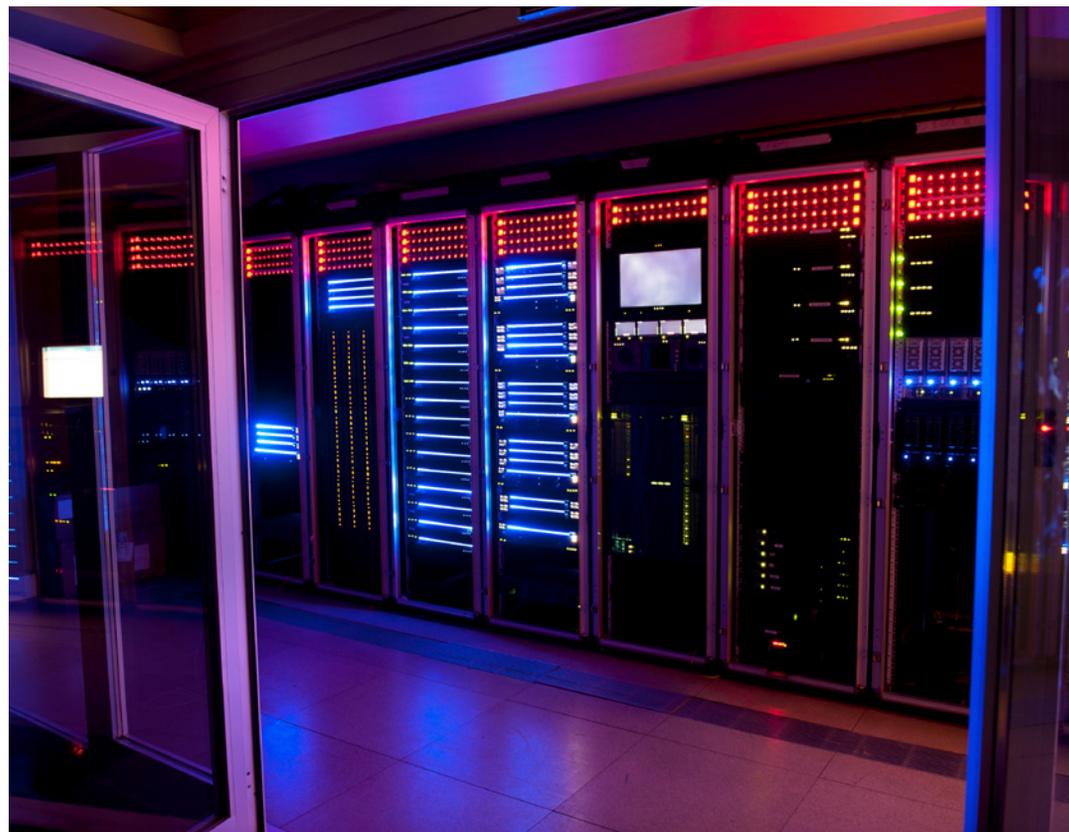
更安全、更简单、 基于服务的安全更加出色

IBM 业务合作伙伴 Atos SE 推出新的安全运营中心 (SOC) 服务，由 IBM QRadar 提供支持。

作者：Josh Young

阅读时长 5 分钟

网络犯罪无时无刻，无所不在，因此企业 IT 安全人员需时刻准备着检测和抵御攻击。但是，要想配备一个时刻值守的安全管理团队，对许多企业来说并不现实，或者财务上不可行。



Atos 中国大数据与安全部门负责人 Cheng Cai He 说：“过去二十年里，我觉得大家都看到了安全和数据泄露的威胁与日俱增。攻击的类型，即病毒的类型，在大中华区的发展非常迅速。”

因此，Atos 的许多客户已开始投入巨资引进新的安全设备和产品。但这些产品往往集成性不佳，成为其保护能力的瓶颈。

“效率不是很高，” Cheng Cai 补充道。
“许多企业，比如制造业的企业，开始频繁与我们探讨如何真正确保所有产品能够协同工作。于是我们产生一个想法：创建基于云的安全运营中心 (SOC) 服务。”

如今，安全运营中心在中国市场已遍地开花。通过安全运营中心服务，Atos 可更好地集中其客户的安全数据，提供整体网络健康状况和稳定性的 360 度视图。

“我们了解到，之前所有安全运营中心均由企业自主创建，” Cheng Cai 说。
“而且数量不多，因为其耗资巨大。企业必须购买齐全各种安全设备，如果要实现每周 7 天、每天 24 小时的保护，还必须成立一支专门的支持团队。”

安全运营中心服务
价格约为

< 1.5 FTEs

而配备内部团队则需 7 - 8 FTEs

为中小型客户提供

24x7

安全监控和保护

与此相反的是，如果中小型企业没有足够资金投入如此大型的 IT 项目，则可选择基于服务的方法（如 Atos 公司的服务），以利用安全运营中心的优势。为了让这项服务易于交付到多个最终用户环境，Atos 还需依靠基于云的交付模型。

“过去五年里，云行业在中国已相当成熟，” Cheng Cai 补充道。“我们的许多客户正在将其 IT 资产从本地迁移到云端。但这种转型有点复杂，企业需要遵守数据保护法，该系列法案禁止关键信息和客户个人数据向国外转移。因此，我们新服务的云解决方案需要托管在中国境内。”

“我们看到安全和数据泄露的威胁与日俱增。攻击的类型，即病毒的类型，在大中华区的发展非常迅速。”

Cheng Cai He，IBM 业务合作伙伴 Atos 公司中国大数据与安全部门负责人

新技术、新交付、新功能

Atos 开始考虑如何提供安全运营中心服务时进行了大量营销分析，评估客户对产品的要求和期望。同时也开始考虑可用来构建新型安全运营中心的安全产品和工具。

作为 IBM 的业务合作伙伴，Atos 果断选择 IBM 技术，特别是 [IBM Security® QRadar® XDR](#) 套件。在该平台成功进行概念验证 (POC) 后，Atos 选择了 [IBM Security QRadar SIEM](#) 解决方案来监视新型安全运营中心服务的安全信息和事件管理 (SIEM) 的需求。同时，AWS 在中国提供了所需的云环境。



QRadar 技术为 Atos 提供客户网络的整体视图，并与人工智能支持的威胁检测和日志分析共同监控此视图。“这让我们一览无遗，” Cheng Cai 补充道。“我们了解客户的实时情况。明确了优先事项和无关事项。这非常有用。”

为了简化客户部署 QRadar 的流程，Atos 签署了 [IBM® 植入解决方案协议 \(ESA\)](#)。
“我们四月份签署了植入解决方案

协议，” Cheng Cai 回忆道。“我们要把 QRadar 产品植入我们的产品，签署协议让许可授权更简单。而且此举夯实了我们与 IBM 紧密的合作关系。

新服务于 2022 年 8 月交付，初期将与 Atos 现有的三个客户进行试点合作。一个月后，Atos 安全运营中心服务正式面向公众推出。

“我们还在北京 IBM 创新中心举办了两次研讨会，演示安全运营中心服务。” Cheng Cai 说。基于充分的研讨，我们正进一步构建产品目录，以提供更多产品。”

“[QRadar] 让一切尽收眼底。我们了解客户的实时情况。明确了优先事项和无关事项。这非常有用。”

Cheng Cai He, IBM 业务合作伙伴 Atos 公司中国大数据与安全部门负责人

为什么选择 IBM?

“我们觉得 QRadar 是我们为 SIEM 做出的正确选择，” Cheng Cai 解释说，“因为其符合中国政府的许多政策和监管要求，这些要求必须遵守。我们为客户部署安全运营中心平台之日，即客户可以投入使用之时。”

他继续说：“我们还看到，过去十年里 QRadar 和 IBM Security 连续入选 Gartner 魔力象限。我们要为客户提供一流的服务，就需要一流的安全产品。”



作为跨国企业 IBM 的业务合作伙伴，Atos 非常重视继往与 IBM 建立的合作关系。“Atos 与 IBM 的合作由来已久，” Cheng Cai 解释道。“但这只是我们与 IBM 在中国合作的第二个项目。我们知道，要通过外部支持来推动新的解决方案，那么与外部企业的合作关系和信任程度将是整个运营取得成功的关键。符合这一点的外部企业，非 IBM 莫属。”

对于这种信任的重要性，Cheng Cai 解释道：“我们是以 IT 服务为基础的企业，而 IBM 中国公司拥有一支安全服务团队。在某些情况下，我们其实与 IBM 处于竞争地位。但从我们与 IBM 的现有关系以及就此项目的直接经验来看，我们相信 IBM 是个可以完全信赖的合作伙伴。”

便捷交付， 强大保护

凭借新的安全运营中心服务，Atos 能以合理的价格为中国的中小型企业提供全面的、强大的安全监控和管理。

Cheng Cai 解释道：“我们的定价让企业对安全运营中心服务的投入相当于约 1 - 1.5 个全职人力工时 (FTE)。但是，如果企业要自建内部安全运营中心服务，则需专门组建一支 7 到 8 人的团队。因此，仅从提供 24x7 全天候服务这一点而言，我们就具备明显的竞争优势，更何况购置全部安全产品还需大量经费。”

“威胁和安全技术正在迅猛发展，”他继续说。“因此，政策和技术需要不断更新。安全运营中心可满足企业与时俱进的安全所需。我们提供业内首创的服务践行承诺。”

QRadar 平台内置 AI 和自动化功能，助力快速识别和解决事件。“遭受攻击时，速度就是一切，” Cheng Cai 指出。“越早识别异常行为、实施隔离，越能减轻入侵造成的潜在损害。”



关于 Atos SE

IBM 业务合作伙伴 [Atos](#)（链接位于 [ibm.com](#) 之外）是 IT 咨询服务、数字安全解决方案和脱碳产品的全球提供商。该公司总部位于法国巴黎，在 71 个国家/地区设有办事处和站点，在全球拥有超过 112,000 名员工。

解决方案组件

- IBM 植入解决方案协议
- IBM Security® QRadar XDR
- IBM Security QRadar® SIEM®

© Copyright IBM Corporation 2022 国际商业机器（中国）有限公司有关详情，欢迎访问我们的官网：<https://www.ibm.com/cn-zh>

美国出品，2022 年 10 月

IBM、IBM 徽标、[ibm.com](#)、IBM Security 和 QRadar 是 International Business Machines Corp. 在世界各地司法辖区的注册商标。其他产品和服务可能是 IBM 或其他公司的商标。Web 站点上的“Copyright and trademark information”部分中包含了 IBM 商标的最新列表：<http://www.ibm.com/legal/copytrade>

Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 在美国和/或其他国家/地区的商标。

本文档为自最初公布日期起的最新版本，IBM 可随时对其进行修改。IBM 并不一定在开展业务的所有国家或地区提供所有产品或服务。

文中引用的性能数据和客户实例仅作参考之用。实际性能结果可能因具体配置和操作条件而异。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条款和条件获得保证。

客户负责确保遵守适用的法律和法规。IBM 不提供任何法律咨询，也不声明或保证其服务或产品将确保客户遵循任何法律或法规。

良好安全实践声明：IT 系统安全涉及通过预防和检测来自企业内部和外部的不正当访问并做出相应反应来保护系统和信息。不正当访问可导致信息被更改、破坏、盗用或滥用，也可能导致系统被损坏或滥用（包括用于攻击他人）。任何 IT 系统或产品都不应被视为完全安全，任何一个产品、服务或安全措施都不能完全有效防止不正当使用或访问。IBM 系统、产品和服务旨在成为合法、全面的安全措施的一部分，这必然涉及其他操作程序，且可能需要借助其他系统、产品或服务才能发挥最大作用。IBM 不保证任何系统、产品或服务免受任何一方的恶意或非行为侵扰，或帮助您的企业免受任意一方恶意或非行为的攻击。