IBM

即刻申请企业安全免疫力检测
零死角“透视”您的企业安全盲区

尽管已经进入“后疫情”时代，我们的工作模式和生活方式还是悄然发生了变化。远程协作模式和远程访问的数量相较以前明显增加，这不仅导致网络负载的激增，伴随而来的网络信息泄漏和潜在威胁也会变得更加频繁和隐蔽。

另一方面，企业正面临着日益严苛的监管环境，《网络安全法》、GDPR、等保 2.0等国内外法规的出台和生效，一次次考验着企业的安全建设、加固、管理的能力。安全人才紧缺和安全知识匮乏，很容易让企业在安全攻防战中处于被动地位。当务之急，是要发现自身的安全威胁，了解自身的安全建设等级，才能有的放矢地提升整体安全运维水平。

IBM 作为全球最大的企业网络安全提供商，12个市场细分领域的领导者，一直致力于为企业构筑健全的网络安全免疫系统。针对企业所面临的安全困境，IBM 特别推出免费的企业安全免疫力检测，运用连续 11年位列 Gartner 安全信息和事件管理（SIEM）魔力象限领导者位置的 IBM QRadar，通过简单、快速、易实施的方式，帮助企业发现安全风险和威胁，为企业安全提供“疫苗式”的决策指引。

“企业安全免疫力”评估能为您做什么？

- 智能化整合分析安全信息，内外部高级威胁无处遁形，CISO 决策有依
- 内置专业分析模型，不受安全人员分析水平限制，潜在未知威胁立现
- 提供业内最完整的 SIEM 平台所需能力，助力提升安全运维能力
- 提供丰富的功能和报告模板，一站式满足您所需的合规需求

申请评估的技术条件

- 镜像网内流量，特别是内部与互联网间的流量
- 将标准化的，系统可自动识别的网络设备和安全设备日志送至 QRadar
- 提供 PC 服务器，品牌不限
- 24 core CPU 64GB 以上内存 1T 磁盘空间
- 千兆网卡，万兆网卡型号需进行确认（明确支持 Napatech, Intel 10Gb）
- 部署 QRadar，并启用 Qflow
- QRadar 环境可以与互联网连接

实施评估的内容

- 了解客户环境的网络流量带宽
- 根据带宽，申请 QRadar PoC 测试 license
- 安装 QRadar
- 配置 Qflow
- 接入典型的安全设备日志，如 WAF, 防火墙、杀病毒、VPN 等
- 定义基本的网络结构和资产信息
- 启用 X-Force，并确认威胁情报成功同步
- 启用内置的关联规则
- 安装 QRadar apps，如：Wannacry, Petya, BadRabbit 等，丰富关联规则
- 仅需两周，就观察发现的 offense 并进行分析，出具《企业免疫力评估报告》

预期可发现的威胁

- 恶意软件：如勒索软件 — WannaCry, Petya, BadRabbit 等；蠕虫，或连接僵尸网络服务器
- 应用程序：明文传输，如：邮件、ftp、重要业务信息（银行账号）
- 侦察：针对重要资产的扫描
- 渗透：各类漏洞利用，通过 QFlow 可以确认漏洞利用是否成功
- 访问：普通用户或者管理员用户认证失败类问题
- 借助人工智能将发现问题的可视化
- 帮助客户发现未知的威胁

根据 IBM 的安全免疫力检查经验，超过 95%以上的企业都存在着各种各样的安全隐患和问题。在这个没有网络安全就没有国家安全的特殊时期，及早采取措施，才能扼杀威胁于萌芽，把损失减少到最低。

欢迎咨询更多方案、获得免费试用或产品演示

致电 IBM 安全销售顾问 400-810-1818 转 2395

扫描二维码，
即刻评估“企业安全免疫力”

IBM Security