上海南洋万邦 Azure 云安全分析解决方案（结合 Grafana ）

根据微软官方规划，**Microsoft Sentinel 功能将于 2026 年 8 月 18 日在中国地区 Azure（世纪互联运营）环境中正式停用**。这意味着企业将无法继续依赖 Sentinel 作为云原生 SIEM 平台为**日在中国地区 Azure（世纪互联运营）环境**开展安全事件集中分析与可视化管理。在云资源规模持续扩大、安全审计和风险管控要求不断提高的背景下，企业亟需构建**不依赖 Sentinel、可持续演进的云安全分析与可视化能力**。

针对上述变化，上海南洋万邦软件技术有限公司基于世纪互联 Azure 的服务现状与企业实际安全需求，提出本 Azure 云安全分析解决方案。方案以 **Azure Log Analytics** 作为统一的安全日志采集与分析底座，结合 **Grafana 开源可视化平台**，构建集中、透明、可扩展的云安全监测与分析体系，在不引入重型商业 SIEM 的前提下，持续保障云环境安全可视性。

在日志与数据层面，将分散在虚拟机、Web 应用、第三方 WAF、VPN Gateway、Load Balancer、Azure Bastion、Azure SQL 数据库、Redis 及容器等资源中的日志统一接入 Log Analytics。通过集中存储与标准化数据结构，解决日志来源多、格式杂、难以统一分析的问题，为安全分析和审计提供稳定可靠的数据基础。

在安全分析与展示层面，方案采用 **Grafana 开源方案**作为核心可视化与分析门户。通过定制化安全仪表盘，将身份与登录安全、主机安全、Web 与边界安全、数据库安全等关

键安全事件以趋势、统计和 Top N 形式直观呈现。例如，登录失败来源分析、异常会话趋势、WAF 拦截情况、网络连接异常以及数据库高风险操作行为，均可在统一界面中快速查看和对比分析，显著提升安全事件的可理解性和响应效率。

采用 Grafana 开源方案的同时，也为企业带来更高的灵活性与可控性。企业无需受限于单一厂商安全产品的生命周期和功能边界，可根据自身需求持续扩展仪表盘内容、分析维度和数据来源，避免因产品下线或策略变化导致的能力中断，确保安全分析平台的长期可用性和可演进性。

从整体价值来看，该方案并非简单替代 Microsoft Sentinel，而是在其停用的既定前提下，帮助企业构建一套**贴合世纪互联 Azure 实际能力、基于开源技术、成本可控且可持续运营的云安全分析与可视化平台**。在不引入 SOC 代运营和复杂第三方 SIEM 的情况下，企业依然能够保持对云安全态势的持续感知和，为后续安全治理和体系升级奠定坚实基础。

Independently Controlled

Based on open-source solutions, avoid single vendor product end-of-life risks

Cost Managed

No costly SOC managed services, or complex third-party licensing

Continuously Evolving

Support continuously expanding analysis dimensions & data sources in sync with business growth