EventLog Analyzer

SIEM 解决方案

可视化管理，轻松审计日志!

VISUAL MANAGEMENT, EASY AUDIT LOG!

日志管理 | 日志分析 | 用户监控 | 合规管理

ANY HUMAN-READABLE JOURNAL

任何人类可读的日志

都可以上传进行审计分析

6亿多个恶意IP库

700多种日志源内置报表

发现异常立即实时告警

高效的日志审计管理

卓豪（中国）技术有限公司

Zoho (China) Technology CO., LTD.

EventLog Analyzer

产品简介

EventLog Analyzer 可以对来自企业和组织中的所有IT资源（包括网络、系统和应用）产生的安全信息（包括日志、告警等）进行统一的实时监控、历史分析。

对来自外部的入侵和内部的违规、误操作行为进行监控、审计分析、调查取证、出具各种报表报告，实现IT资源合规性管理的目标，同时提升企业和组织

日志管理

可对不同日志源所产生的日志进行收集，实现日志的集中管理和存储。

它支持：Windows、Linux、Unix、网络设备、应用程序、VCenter、Checkpoint、漏洞、PaloAlto、风险预测、Meraki、Syslog设备等。

日志监视

它提供文件完整性监视（FIM）功能，确保组织的敏感数据只被合法访问，而不被非法访问。
可以收集并分析特权用户所做的活动所产生的所有事件，获取特权用户活动的精确信息，如：执行了什么活动、活动的结果、影响的服务器、从哪里进行访问等。

实时告警

它可针对事件日志产生告警、关联事件告警、根据主机告警及合规性告警，并可以自定义告警配置、预置告警配置等。

告警通知方式支持：E-mail通知、SMS通知、发送Trap到其它管理平台。

合规管理

默认提供PCI DSS,FISMA,ISO27001,HIPPA,SOX,GLBA,GPG13

GDPR等合规性报表.