奇安信网神工业日志收集与分析系统ILAS

聚焦工业审计合规，链接安全信息孤岛

奇安信网神工业日志收集与分析系统，采用大数据技术和智能分析方法，集日志采集与存储、日志归一化、交互式分析、关联分析、仪表板、报表统计、告警管理等功能于一身，实现工业网络中安全设备、网络设备、操作系统、数据库、中间件及应用系统等的日志、报警信息的全面采集、存储、分析和展示，全面满足工业行业及组织对工业日志的安全合规管理要求和审计分析需求，已在数千家各类工业企业落地实践。

用户价值 CUSTOMER VALUE

满足工业安全合规要求

奇安信网神工业日志收集与分析系统可满足国家及各工业行业、工业安全法规政策中安全审计方面的要求。

提高工控安全运维人员工作效率

通过奇安信网神工业日志收集与分析系统可更加快速准确识别工业网络中安全告警信息，发现工业网络中违规行为后进行应急响应。

全局掌握企业的工控安全总体状况

利用奇安信网神工业日志收集与分析系统，为工业企业管理层进行工业安全建设决策提供依据，整体提升了企业工业安全防护水平。

产品功能 PRODUCT FUNCTIONS

资产管理

对IT/OT资产进行分组管理，对资产信息进行增删改查，具备丰富的属性管理功能，为日志分析提供丰富的上下文信息。

日志采集

全面采集各类日志，支持Syslog、SNMP Trap、JDBC、SFTP/FTP、SMB、API、Kafka、文件读取、日志代理方式采集。

数据治理

系统提供强大的数据治理功能，主要包括动态数据建模和数据质量管理，保证日志分析的准确有效性。

事件分析

用户可以通过界面实时查看来自网络中各种IT/OT资源的日志情况。系统内置了大量的分析场景，用户无需学习，即可开展审计操作，也允许用户自定义场景，并对场景进行树型结构的分类和归档。

仪表板

系统提供了灵活自定义的仪表板，同时内置丰富的仪表板主题，通过仪表板，不同角色和不同用户可快速获取到各自所关注的安全信息，满足各自管理需求。

关联分析

系统内置大量关联分析场景，如认证登录、授权行为、违规行为、系统变更、攻击入侵、敏感操作和设备故障等，通过启用这些内置场景，可实时发现网络攻击和违规行为。通过关联分析引擎，用户可以灵活定制关联规则。

告警管理

系统对于发现的安全事件可以进行自动告警，并提供多种响应方式。可对告警进行统计查询和归并抑制。

报表管理

系统提供丰富的报表管理功能，预定义了多种设备事件趋势以及总体报表，满足等保等其他合规性要求。系统提供自定义报表，用户可根据自身需要进行定制。

日志备份与恢复

系统支持按照日志存储周期进行定期备份，并支持在线恢复。外部存储空间备份为日志数据提供高可靠保障。

奇安信 新一代网络安全领军者

产品优势 PRODUCT ADVANTAGES

大数据，秒级完成10TB级的日志数据的搜索

系统基于大数据技术，和高效的算法，使搜索尽可能在内存中完成，秒级完成10TB级的日志数据的搜索，使人工的日志搜索、调查和取证变为可行。

可视化，快速而美观地展现日志处理的结果

系统采用了多种可视化技术，实时展现日志处理结果，将安全管理和运维人员从繁重的事件查看工作中解脱出来，从而发现安全威胁。

分布式，打破单节点计算资源限制

系统独创性的提供了分布式关联分析的能力，将海量日志的处理分散到集群的计算节点中，并且过弹性扩展计算节点数量来增加关联分析的能力。系统提供了分布式的采集器，实现了集群部署和资源调度的自动化、智能化。

高弹性，满足弹性部署和资源扩展要求

系统具备灵活的高弹性部署能力，避免了采用开源大数据技术的重量级资源需求。系统既可以部署在物理服务器中，也可以部署在虚拟机和Docker容器中；既支持传统x86架构平台部署，也支持国产化平台部署。

智能化，日志综合审计更准确、更高效

系统对数据进行智能化处理，保证了高质量的输入数据，为后续分析打下良好的基础。系统采用了机器学习对海量日志进行分析，基于关联分析引擎并结合威胁情报，实时发现网络中的安全风险。实现了实时、历史、交互式、自动化的日志分析，综合审计更准确、更高效。

部署场景 DEPLOYMENT SCENARIO

支持单点部署、级联部署、分布式部署、分布式集群部署等。