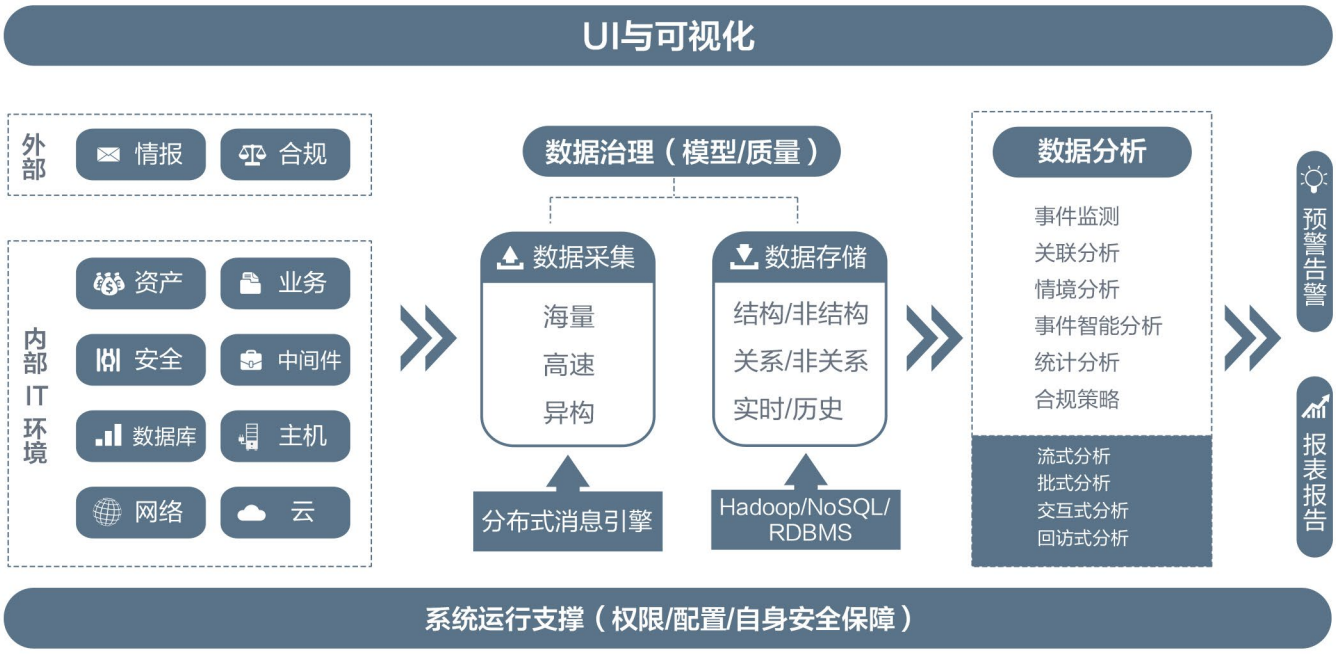
圣博润
SBR-info

LAS

LanSecS日志审计系统

LanSecS日志审计系统（简称LAS）是一款融合大数据和机器学习技术开发的，满足各行各业用户安全合规审计和安全分析需求的产品，它集中收集并存储IT基础设施和应用系统所产生的安全事件、用户访问记录、系统运行日志、系统运行状态、网络存取日志等，通过多种智能分析手段，发现网络中的违规和安全问题，及时预警，并通过仪表板和合规报告呈现给用户。

产品架构



● 数据采集

系统采用分布式消息引擎对海量、高速、异构日志信息进行采集、存储，能采集包括网络设备、安全设备、主机操作系统、虚拟化及云、数据库、中间件和应用系统等。

● 数据存储

系统内置分布式非关系型数据库，可将海量日志集中保存，满足网络安全法要求，同时支持水平弹性扩展。系统通过接口可支持将日志保存于Hadoop、NoSQL或RDBMS中。

● 数据分析

系统支持流式分析（进行实时分析）、批式分析（进行历史分析）、交互式分析（人工分析）、回放式分析（历史数据关联分析）等分析技术，对采集到的日志进行事件监测、关联分析，情境分析、智能分析，同时还提供近实时统计分析、事件即席查询、合规策略分析等功能。

● 告警管理

提供告警管理功能，支持告警查询、统计分析等功能，告警信息可以通过邮件、短信、微信等多种方式进行通知和展示，也可通过API与第三方运维系统集成。

● 系统运行支持

包括权限管理、配置管理和自身安全性等功能。

产品功能

数据采集

支持多种设备
支持多种采集协议
支持海量日志
支持分散的日志源
日志范式化、分类
日志过滤、归并
日志存储转发

数据存储

海量日志存储
全文索引
长时间存储
保证CIA
日志压缩

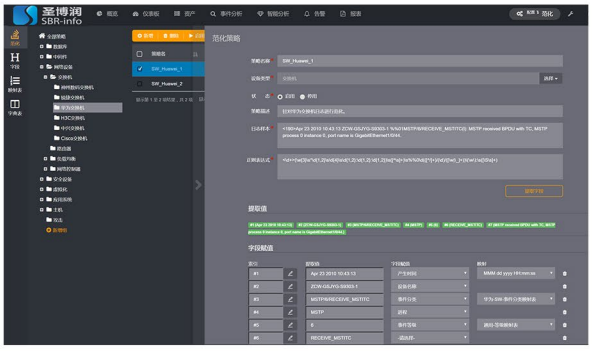
数据分析

内存实时分析
历史分析
关联分析
合规审计
可视化分析

特色功能

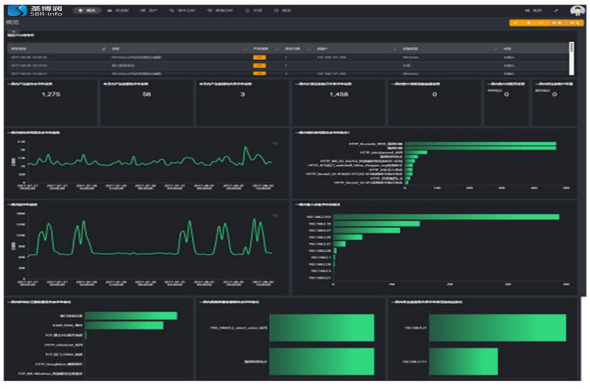
◎ 可视化日志范式化编辑

系统提供可视化日志范式化编辑功能，结果可自动转化为系统范式化策略。同时范式化字段可在分析过程中根据审计和分析的需要灵活扩展。



◎ 灵活的仪表板

系统支持仪表框架任意创建，根据需要在框架内添加不同的仪表板组件，组件位置可摆放，组件大小可拖拽。



◎ 日志聚类分析

系统采用机器学习对日志进行聚类分析，能够对日志模式进行自动识别，使审计人员清晰了解采集的日志构成。

产品特点

产品优势

- 采用业界最新的大数据和机器学习技术，来支撑海量日志处理。
- 可视化日志范式化，更灵活、更便捷。
- 基于机器学习的日志模式识别，更清晰、更高效。

产品规格

版本	型号	规格参数
软件版	LAS-SV50	系统自带50个日志源的License授权
硬件版（不限License授权）	LAS-P500	最大日志分析能力大于3000条/秒，每秒1000条日志入库
	LAS-P1000	最大日志分析能力大于6000条/秒，每秒1000条日志入库
	LAS-P2000	最大日志分析能力大于9000条/秒，每秒2000条日志入库
	LAS-P4000	最大日志分析能力大于12000条/秒，每秒4000条日志入库

咨询热线：800-810-2332　电话：8610-82138088　传真：8610-82137982
Email：Support@sbr-info.com　WWW.SBR-INFO.COM