LanSecS 安全管理平台系统

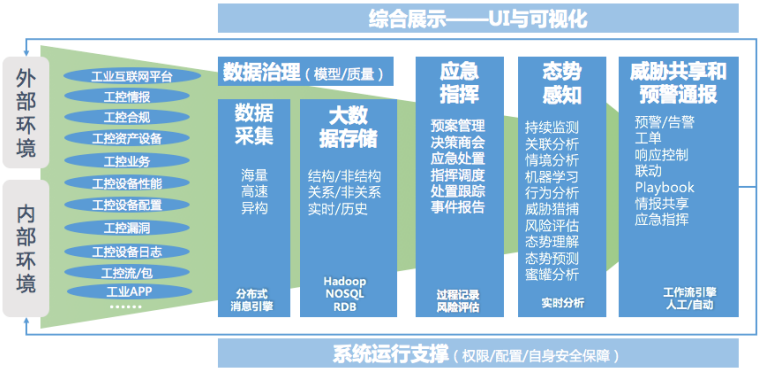
——领先的工控网络安全态势感知

LanSecS 安全管理平台系统（LanSecS SMP V2.0）是圣博润公司融合工控网络安全技术开发的新一代工控网络安全管理平台类产品。它集中收集并存储客户 IT 环境的资产、运行状态、漏洞、安全配置、日志、流量等安全相关的数据，内置大数据存储和多种智能分析引擎，融合多种情境数据和外部安全情报，有效发现网络内部的违规资产、行为、策略和威胁，网络外部的攻击和威胁，及时预警，提供包括工单在内的多种响应方式，使安全管理工作规范化流程化进行，通过丰富的仪表板将网络安全态势呈现给客户，最终生成多种合规报告。平台具备威胁信息共享、预警通报和应急指挥模块，结合态势感知数据，为客户构建网络动态深度防御体系。

LanSecS 安全管理平台采用组件化技术，是专注于安全管理和安全分析的应用套件开发平台，集成了安全事件和网络流量的采集，标准化，存储，告警，查询，分析和报表等全流程，内置大数据存储和智能分析引擎，提供功能界面定制和模块开发接口，用户可以快速部署，配置和开发一系列的安全管理相关应用。

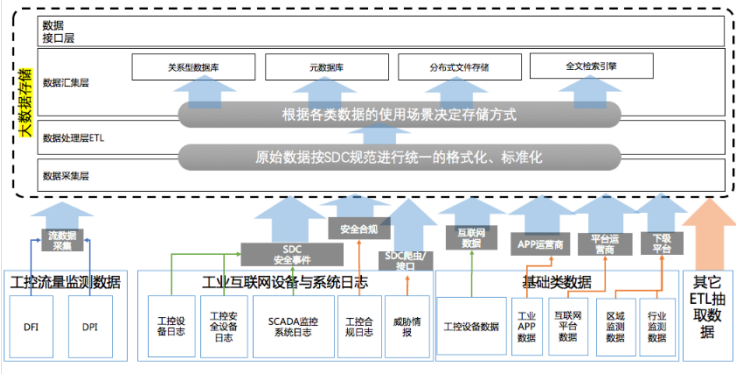
产品价值

- 助力《网安法》和《等级保护》合规管理
- 日常安全运维和等保管理工作的有力工具
- 全方位全天候动态网络内外安全态势感知
- 威胁情报的采集、利用和共享
- 多维度安全事件分析与响应
- 快速的网络安全通报和预警
- 灵活开放的开发平台，功能扩展方便、快速交付安全应用



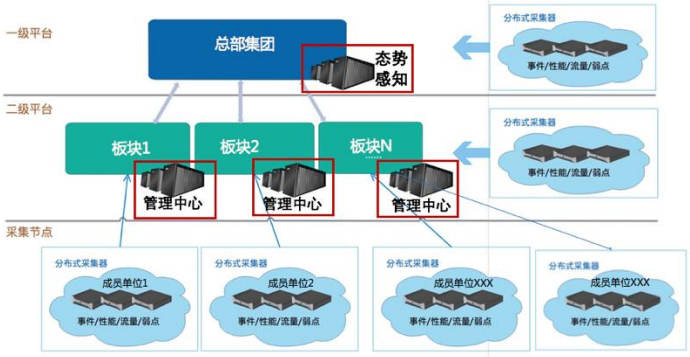
平台大数据架构

平台采用大数据基础架构作为后台数据存储分析，支持数据存储集群部署，同一数据在不同存储服务器中进行保存，实现数据冗余存储，保证数据高可靠和高可用。



部署架构

平台部署灵活简单，一键式安装部署，省去诸多配置麻烦。支持单级/多级部署架构，集中/分布式部署，采集分布式/数据存储分布式部署等方式。



获取更多详情，请访问 http://www.sbr-info.com/

性能优势

项目	性能
日志入库	日志数据的入库能力可达到 50000EPS；
流量数据	流量数据的入库能力吞吐可达到 8Gbps；
事件入库	事件入库的性能可达到 20000EPS
实时关联分析	实时关联分析的性能可达到 20000EPS
事件查询	事件查询性能：对 TB 级日志数据搜索时间＜10s
数据加载速度	在万兆网络的环境下，单台客户端支持的数据加载速度高于 200MB/s，可以线性扩展
数据接收速度	支持分布式文件系统、数据仓库和索引存储集群中单节点的数据接收速度高于 20MB/s，典型日志类数据的压缩率高于 60%
用户数	支持用户数大于 500
并发数	支持权限查询的并发数高于 200

主要功能列表

态势感知模块		
模块名称	**子功能名称**	**功能描述**
大数据存储与分析模块	数据汇集接入系统	1、支持各类结构化数据的加载，支持灵活通用的数据格式描述，包括数据包含的字段、各字段的分隔符、字段类型等； 2、数据总线支持数据订阅和发布功能。数据由数据加载客户端提供，或者由业务系统直接写入；
	数据存储系统	1、数据存储部分由分布式文件系统、数据仓库和索引存储等三个部分组成。针对数据接入汇集系统接收的网络安全威胁信息，包括流量日志、设备日志、系统日志等日志类数据、告警类数据、元数据类数据等，存储至相应的非结构化数据、半结构化、结构化存储系统中； 2、支持各类非结构化数据的加载，以文件的形式存储； 3、支持 SQL 接口下数据仓库与全文检索数据关联查询； 4、支持 Full_text 全文索引查询函数； 5、支持 SQL 接口，可以将全文检索作为 SQL 的一种过滤条件； 6、支持常见的中英文分词器，支持分词器的扩展；
	数据分析系统	1、平台可根据用户关键信息基础设施安全监测要求预置相应的数据分析模型，包括关联分析模型、溯源分析模型、威胁预警分析模型、信息系统场景化分析模型、工控系统场景化分析模型等； 2、平台预置的信息系统场景化分析模型数量大于 10 种，且可根据后续业务需要进行增加； 3、平台预置的工控系统场景化分析模型数量大于 5 种，且可根据后续业务需要进行增加；
	平台运维管理	1、平台管理主要包括操作管理、运维管理和可靠性管理三部分功能，通过这三部分功能，实现对大数据存储与分析平台的日常运营管理，确保平台可安全、稳定、可靠的运行； 2、支持故障告警，实现告警根源定位； 3、系统可保证 7×24 小时连续稳定工作，月故障率低于 2 次；
态势感知平台	风险监测预警	1、利用大数据存储与分析平台采集的数据，以及平台内置的各类数据分析模型，支持在漏洞分析、漏洞预警两个方面对用户关键信息基础设施的安全风险进行全面监测、及时准确的预警各类安全风险。 2、可使用日志关联分析技术对采集到的各种日志进行关联分析，在一定时间窗口内可对日志进行统计、序列关系、逻辑关系等分析，实时的给出相关告警； 3、支持对来自流量传感器中的各种深度解析后的流量日志进行关联分析，可针对 HTTP 头部、DNS 解析行为、邮件相关行为、文件传输行为进行关联分析，以发现潜藏在流量中的内外部威胁； 4、支持根据丰富的安全场景，以数据分析的方法，可视化呈现场景细节，帮助用户分析特定场景的安全问题，无需复杂规则配置，图表直观呈现主机外连场景信息、HTTP 代理场景信息、SOCKS 代理场景信息、异地账号登录场景信息、暴力破解场景信息、VPN 安全场景信息、账号安全及邮件安全场景信息等关注的场景； 5、威胁情报分析得到的告警可通过内置的告警推送接口向终端管理系统进行推送；
	威胁情报采集	1、云端推送的威胁情报信息，将以可机读威胁情报的形式（可机读 IOC）直接同步至网络安全态势感知平台，用于提升态势感知平台的检测能力。 2、具备公有云情报库，并可向本地威胁情报采集系统开放查询界面，内容覆盖 APT 攻击事件、勒索软件、蠕虫木马、黑客工具、僵尸网

态势感知模块		
模块名称	**子功能名称**	**功能描述**
		络、后门软件等关键威胁； 3、支持根据 IP 地址、域名、邮箱、文件、证书指纹等信誉情况进行查询，发现并标注最近时间、威胁类型、地址位置、IP 资产性质、最近报告等威胁情报内容查询； 4、支持配置自定义威胁情报进行告警匹配，IOC 类型至少包括：地址、域名、MD5、域名+端口+URI、域名：端口、地址：端口 等常用型； 5、支持 stix、openioc、json 和 xml 格式等第三方威胁情报的导入；
	状态监测展示	1、支持以可视化技术展示信息系统的整体运行状态，支持网络设备、系统主机、服务器、中间件、数据库等运行状态监测； 2、支持以可视化技术展示工控系统的整体运行状态，支持南瑞、西门子、施耐德、通用电气等系列工控系统运行状态监测，以图形化方式实时监测工控系统流量，包括 OPC、Modbus、Simens S7、IEC 104、Ethernet/IP、profienet 等协议；
	态势展示	1、支持外部威胁态势的可视化呈现，地图呈现外部威胁定位，统计展现外部威胁趋势、威胁类型 TOP5、威胁来源国家 TOP5、内网资产/IP 威胁 TOP5、威胁来源 IP TOP5，并支持调整统计时间范围，查看威胁态势变化。 2、可通过外部威胁态势查看最近告警内容，快速感知最新威胁。 3、支持资产风险态势可视化呈现，监控内网资产风险分布，量化各资产组的风险，轮播展现各资产组的风险情况、威胁分布和告警趋势； 4、支持仪表板功能，可提供预置仪表板，内置多种统计分析视图。预置仪表板包括以下维度的统计告警、资产、日志、系统维护、漏洞、web 攻击和工单分析； 5、支持周期报表可以选择生成以周、月、季度、年为跨度的报表，支持自定义报表内容，并能自动通过邮件或消息中心发送给指定责任人；
	资产管理	1、可以管理网络中的主机设备、网络设备、安全设备、应用系统、工控设备（具体包括：交换机、路由器、防火墙、服务器、SQL Server、Oracle、MySQL 数据库系统、webshpere/ weblogic 中间件、工作站、南瑞 PLC、西门子 PLC、施耐德 PLC、罗克韦尔 PLC 等）,支持批量导入资产记录，也支持手工添加资产； 2、支持自动发现网络拓扑并自动创建网络拓扑图。支持拓扑图的整体拖拽和缩放操作，支持对单个节点施放操作，支持拓扑图保存。支持拓扑图节点属性信息的显示与隐藏。支持查看节点的详细信息； 3、支持导入主流漏洞扫描器的扫描结果；支持自定义漏洞结果解析模版以增添识别其他品牌扫描器的管理；
	平台管理	支持用户角色管理，可以为不同角色赋予不同系统功能模块的读写权限，未赋予此模块读写权限的用户，将无此功能模块的显示或配置的权限，所有系统大功能模块和日志查询子功能模块都要能支持角色管理；
信息共享模块	数据存储	提供基础的数据源管理、维护数据加载、校核数据处理、交换数据处理、交换数据分发功能，平台日志数据最低保存时间半年；
网络安全预警通报模块	事件调查分析	1、调查分析模块提供根据网络安全隐患及网络安全事件的性质确定具体处置的业务场景（支持日常通报和快速处置）；
	预警通报管理	支持多种通报模式： 1、日常通报： （一）基于数据处置规则模块将符合通报预警业务的数据自动推送到通报预警子系统，并从业务分析角度以单位维度进行数据分析，统计分析各类安全隐患的数量； （二）支持用户通过分析后的单位安全隐患情况展开网络安全隐患及事件通报的业务流程，支持对于通报反馈情况、整改情况及处罚情况的跟踪和记录； 2、综合预警通报： （一）能够根据用户设置的各类通报模板，按照指定的周期完成对于指定单位的网络安全综合数据分析，并形成通报文件； （二）支持通过移动端应用提醒被通报单位的相关责任人及时查看通报文件；
	系统配置管理	系统配置管理主要具备以下功能：通报模板管理、模板关键字管理、模板周期管理
网络安全应急指挥模块	接口管理	平台支持与安全管理平台系统内涉及的各相关平台进行数据接口对接，无缝兼容。
	预案管理系统	1、提供预案管理、预案评估、预案应用功能
	决策会商系统	通过对安全事件发展态势的地图标绘和动态推演，动态、直观地反映突发安全事件的态势及领导的各种指挥调度示意
	应急处置系统	应急处置系统是包括安全事件汇总和应急指挥功能
综合展示模块	综合展示平台	1、具有网络安全态势感知平台态势展示的所有功能，包括信息系统网络安全态势展示和工控系统网络安全态势展示； 2、可提供标准接口接收第三方网络安全态势感知系统数据，集成展示到综合展示系统中； 3、可以按区域、流域、单位等不同维度对网络安全态势感知情况做总体展示；
系统集成	硬件集成	兼容主流的工控和信息系统流量采集器，工控系统流量采集器 2 种以上，信息系统流量采集器 3 种以上；
	数据集成	1、通过集成转换成统一数据格式并利用相应的大数据计算组件和模型进行相应的安全分析； 2、支持数据总线方式进行数据集成；
	平台自身安全集	从物理安全、网络安全、数据安全、应用安全、冗余备份、终端安全等方面合理规划，统筹部署，切实保障网络安全态势感知系统自身安

态势感知模块		
模块名称	**子功能名称**	**功能描述**
	成	全。

采集探针		
模块名称	**子功能名称**	**功能描述**
工控网络流量采集探针	工控网络流量采集	能够实时采集工控网络流量；可识别工控通信协议；基于工业控制系统的工控协议流量解析，进行流量大小、异常分析，直观展示，根据流量的大小、异常发现问题；
	指令采集	支持常见 PLC 芯片工控指令采集，可采集 PLC 组态下装、PLC 启停等操作指令。
	通信还原分析	能够抓取工业现场设备与上位机之间的通信并进行还原分析，支持对常见扫描以及远控木马的检测，能够通过双向流量检测的方式发现可被利用的 SQL 注入、跨站、命令执行等 web 漏洞，并记录已经发生过的攻击事件和相关报文。
工控主机行为采集探针	工控主机信息采集	能够采集包括主机基础信息采集、样本投递采集、内存行为采集、系统操作行为等在内的四类行为记录数据。
	通信还原模块	能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。
工控安全设备日志采集探针	安全信息采集	可识别工控设备包含：工控设备资产识别、上位机操作系统识别、数据库资产识别； 能够通过 SNMP、SSH、等方式采集安全设备、主机等的运行状态信息，如：端口状态，CPU、内存利用率等； 支持对漏扫引擎进行集中调度管理，下发扫描任务，采集的扫描结果可以自动参与到漏洞脆弱性分析； 资产探测可达到 30 个/秒以上；
	日志采集	支持通过 Syslog 方式采集工业防火墙、工业审计系统、工业安全管理平台、工业主机防护设备等的日志；
工控网络采集数据传输	数据传输模式	平台自带数据跨域传输功能，支持将采集到的工控安全数据从隔离装置内的非实时控制区传输到管理信息区。
信息系统流量采集探针	深度流量分析	深度流量采集基于 Flow 技术，对网络中的流量数据进行采集，提供多种主流格式的 Flow 数据采集，并支持将 SPAN 数据转化成 Flow 格式进行分析，检测判断流量数据中是否存在异常流量，对异常流量成分、来源等进行分析。
	协议解析模块	支持协议解析对网络流量进行报文和会话级的重组还原，实现针对 TCP、UDP、HTTP、DNS、SMTP、POP3、IMAP、SMB、TELNET、RDP、FTP 等协议的解析，并将网络会话中的 3 至 7 层协议包头及相应的 payload 信息进行还原，并通过下述技术手段实现安全检测。
	深度包监测	深度包检测提供动态的、深度的、主动的安全检测，为应对新型攻击带来的威胁，从智能识别、环境感知、行为分析三方面加强了对应用协议、异常行为、恶意文件的检测能力。
信息系统日志采集探针	日志采集器	1、日志采集器可通过 Syslog、SNMP Trap（被接收方式）及 WMI、JDBC、Log File、FTP、WebService（通过代理采集并转发）等不同方式，实现对安全设备日志、系统日志等数据的采集。所采集的数据将送至态势感知模块分析。 2、针对常用协议解析的数据形成标准化日志，包括 TCP 流量日志、UDP 流量日志、Web 访问日志、域名解析日志、文件传输日志、FTP 控制通道日志、LDAP 行为日志、登录动作日志、邮件行为日志、数据库操作日志、SSL 加密协商日志、Telnet 行为日志等； 3、事件解析直接支持主流主机设备、网络设备、安全设备、应用系统。具体包括：交换机、路由器、防火墙、服务器、SQL Server、Oracle、MySQL 数据库系统、webshpere/ weblogic 中间件、Mail/Web/FTP/DNS/DHCP/WINS 等，对于新设备类型不需编码，只需编写相应的解析文件并加载即可实现支持；
信息系统资产采集探针	资产发现	1、采用 SNMP 扫描方式可获取资产名称、厂家、型号、IP 地址、网络掩码、物理地址等信息。采用 IP/端口扫描方式可获取网络资产中的 IP 地址、端口号、所开服务类别、采用协议、服务版本及操作系统类型等信息。