iSOC统一安全管控解决方案

方案概述

信息安全事件随时发生，及时发现和定位问题，并采取相应的响应措施，以保证业务的正常运营是信息安全管理的基本目标。

华为iSOC统一安全管控中心（以下简称iSOC）提供全方位的安全管控解决方案。它从安全监控、安全审计、安全决策三个维度，通过对安全对象的日志采集、分类存储、关联分析，帮助客户在海量安全事件中洞察安全风险，准确定位安全问题，支持快速查询检索和工作流以提升安全运维效率，同时帮助客户审视IT建设是否满足相关法律法规的要求。

方案特点

专业安全 统一管控

- iSOC缺省支持160多类设备的日志采集和识别，包括主流的主机系统、数据库、网络设备、安全设备和存储设备等；对于非主流设备的日志提供快速定制接入，实现日志集中管理。

日志防篡改 安全可靠

- iSOC平台对日志采用专用的日志加密技术进行加密存储，通过内部时间戳防篡改标志，确保数据一旦写入，即不可篡改，满足企业业务合规性审计要求。

领先的事件采集性能，实现海量数据的采集和分析

- 采用领先的并行处理技术对日志进行同步采集和分析；在相同运行环境下，性能优于同类产品，实现海量数据的即时高效采集和分析。

强大的关联分析引擎，帮助客户快速定位IT安全事件

- 强大的关联分析引擎，通过跨物理、虚拟和云环境同步数据，将所有孤立的 IT 数据捆绑到单一智能仪表板，从而将安全事件数据实时转换成有用信息，在复杂的网络环境中，帮助客户快速定位安全异常。
- 预置100多条关联规则模板，帮助客户精确洞察IT漏洞。提供现场定制客户化的关联规则，满足客户特定业务场景的安全需求。

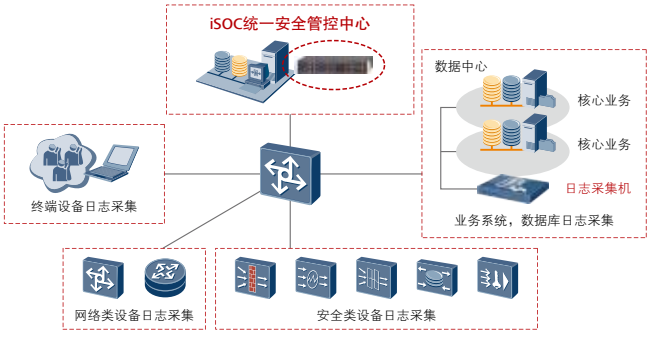
友好直观的安全可视化门户，让客户对整体风险一目了然

- 通过易用直观的呈现界面，实时展现关键资产和业务的安全状况，帮助客户有效的安全决策。

简单易用 灵活部署

- 通过灵活的数据采集部署方式，不改变客户现有的网络结构，支持集中部署、级联部署和远程协助方式，使性能获得无限拓展，满足客户多样性网络需求。

典型部署



HUAWEI

方案规格

维度	功能模块	特性
安全监控	日志识别	支持160多类主流设备的日志采集和识别，对于非主流设备的日志提供快速定制接入。 操作系统类日志包括windows、Linux、Unix等；DB类日志包括Oracle、Sql server、DB2等；web server类支持包括IIS、Apache等；网络设备日志包括但不限于华为产品以及其他厂商产品；文件日志采集支持NFS、CIFS、SCP方式采集远程日志。
	采集协议	支持的日志采集方式： 明文Syslog、加密Syslog、SNMP V1/V2/V3、ODBC或JDBC、WMI、OPSEC、 SDEE、Logfiles（安装Agent）
	Richer处理	支持各类日志格式标准化处理
	关联规则管理	支持（关联规则定义、修改、删除、部署等） 支持逻辑关联、扩展关联、风险关联、动态基线统计等
	标签管理	支持（标签建立、删除、修改、标签与事件关联）
	事件过滤	支持所有日志全部实时分析，并入库。 支持基于设备IP、设备类型、日志字段等多种组合过滤策略，选择日志是否入库，是否实时分析。
	安全仪表板	支持实时的，以不同颜色、或图标、或关键字直观地显示事件源安全状况
安全审计	告警管理	支持（告警设置、趋势分析、攻击路径分析、排行分析、告警响应配置、策略管理等） 支持短信告警、E-Mail告警、与第三方网管系统对接
	风险管理	支持（风险定义、风险计算、风险分析、威胁识别、脆弱性识别、预警管理等）
	资产管理	支持（资产关键属性定义、资产发现、资产维护、导入等）
	脆弱性管理	支持（脆弱性分类管理、批量导入、漏洞管理、扫描报告管理等）
	威胁管理	支持（威胁分类管理、导入等）
	安全知识库管理	支持（知识统计、导入、关键字检索等）
	工作流管理	支持（流程定义、流程监控、工单管理等）
安全决策	合规报表	支持（输出为PDF格式） 缺省提供如下4类合规类报表（用户可新增自定义合规报表）：ISO27002；Sarbanes-Oxley (SOX)；BASEL II；PCI-DSS
	资产报表	支持（输出为Excel、html、PDF格式）
	风险报表	支持（输出为Excel、html、PDF格式）
	告警报表	支持（输出为Excel、html、PDF格式）
	自定义报表	支持（曲线图、柱状图和饼状图）
	定时报表	支持（定时在后台生产报表）
	GIS	支持（安全态势展示、跨区域攻击线路展示）
	TOPO管理	支持（拓扑管理等）
系统管理	高可用性	支持active-standby热备部署 支持冗余电源模块
	用户管理	支持（用户新增、删除、修改；用户授权）
	数据权限管理	支持（按区域给用户授予数据权限）
	系统运行监控	支持（监控CPU、内存、磁盘使用情况）
	license管理	支持
	存储管理	支持（数据备份与恢复、原始数据管理、网络存储设置、运行状况查看等）