日志审计分析平台

杭州迪普科技股份有限公司

产品概述

迪普日志审计分析平台（DPtech LSP）是一款智能的全网日志分析产品。平台以大数据技术为核心，快速全面的收集各类网络设备、安全设备、主机服务器、中间件、数据库以及业务系统的日志信息，实时进行安全事件的分析，协助用户进行安全分析及合规审计，及时有效的发现异常行为和安全事件。

产品功能

■ **日志采集**

平台可通过 Syslog、SNMP、WMI、FTP 等协议采集各类不同厂商的安全设备、网络设备、主机操作系统，以及各种应用系统产生的日志。用户仅需安装部署审计中心,无需另装采集器,即可实现对日志的采集工作。

■ **日志统计与分析**

平台提供了统计视图 ,审计员可以依据内置或者自定义的统计策略,从日志的多个维度实时进行安全事件统计分析，并以柱状图曲线图等形式进行可视化的展示，审计员可以查看不同设备审计事件数量统计图。挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系 ,平台提供了 GUI 方式的关联规则设置功能 ,异常统计模型的检查分析功能 ,如：暴力破解、用户账号权限异常等。

■ **采集策略管理**

平台能够对所有的采集策略进行统一管理,并决定是否接收某一资产的日志信息

■ **日志处理**

支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，并根据实际业务需求减少采集对象发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间的占用。

平台具有归并技术，日志审计分析平台会在一段时间内比较收到的安全事件，如果安全事件相同，则只记录一条安全事件，该安全事件包括安全事件详情及该安全事件发生的次数，这样可以减少安全事件存储量。

■ **日志查询**

平台提供日志查询功能,便于从海量数据中获取有用的日志信息，用户可自定义查询策略,基于日志名称、主机类型、源 IP 地址、验证级别、原始日志等各种条件进行组合查询,并可导出查询结果。

■ **安全总览**

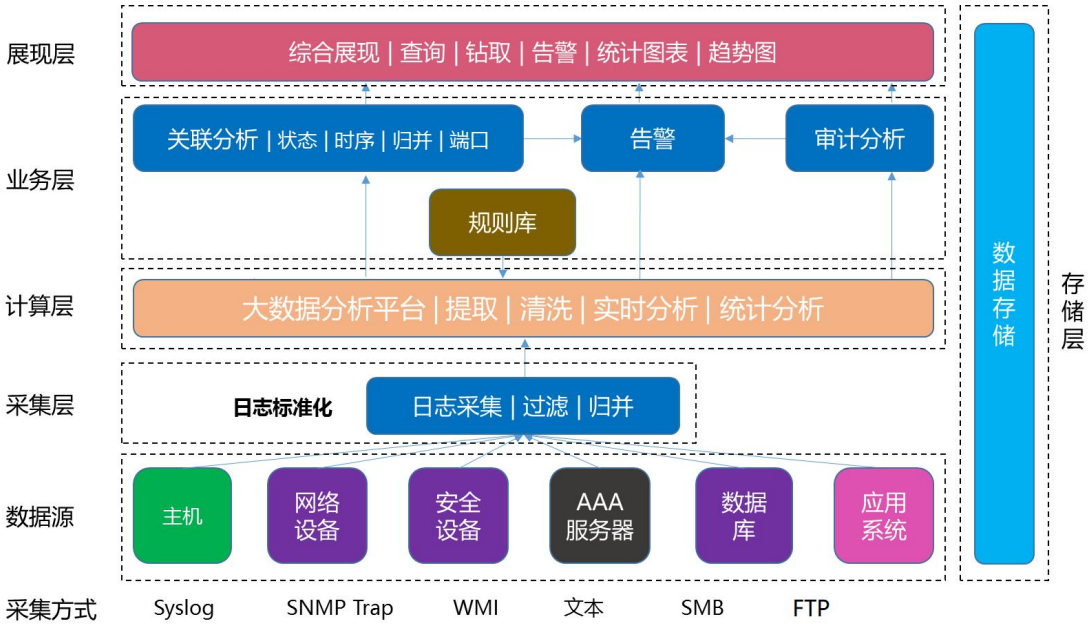
用户登录即可进入安全总览。在首页，能够快速地导航到各个功能，能够在一个屏幕中看到接收日志量、关联事件量、审计事件量、告警日志量,日志数量 Top10,最近 24 小时内接收日志数量、关联事件、审计事件、告警日志时间分布趋势图，以及当前设备使用情况。

■ **安全报告**

平台内置丰富的报表模板，包括综合报表、概览报表等，用户可以依据需求自定义生成报表，并发送至相应的接收人。不仅如此，平台还提供将用户对日志信息的查询，导出为报表的操作。

产品架构

迪普日志审计分析平台的主要功能包括如下模块：



- 采集层：采集各种设备的事件日志，标准化为统一的格式，然后进行过滤、归并、关联和审计，通过会话解析从海量日志中分析潜在的安全问题，同时进行相关数据的存储和管理；
- 分析层：平台通过分析引擎，对日志进行关联分析、审计分析并对异常事件告警策略进行管理；
- 展示层：展示安全总览，将整个平台收集、分析、管理的安全事件、告警概况等信息多维度的展现在用户面前。

产品优势

■ 全面采集

支持 Syslog、SNMP Trap、文件上传、WMI、FTP、SMB、Kafka 等方式采集。内置 414 种解析策略，主流设备包括：网络设备、安全设备、操作系统、数据库、应用系统、虚拟化等。

■ 实时分析

支持基于规则的分析模型。内置丰富的安全监控场景模板，例如跳板机登陆事件、同源异常登录尝试、远程密码猜测等。系统采用流式分析模式，实时分析接入的海量日志，实时挖掘潜在威胁。

■ **精准检索**

亿级（TB）原始日志查询耗时低于 1 秒，支持简单易用的日志查询普通模式，根据系统预置的查询条件，根据用户需求查询对应的日志，并且支持查询条件的保存，供后续快捷使用；支持更加精确的专家模式查询，根据页面的指导提示，通过组合查询表达式完成精确查询。

杭州迪普科技股份有限公司
地址：浙江省杭州市滨江区月明路 595 号迪普科技
邮编：310051
官方网站：http://www.dptech.com/
服务热线：400-6100-598