DPtech 工控安全监管与分析平台

杭州迪普科技股份有限公司

产品概述

工业化和信息化相辅相成，二者结合已经成为明确的趋势，工控系统与信息系统数据交互成为必然，然而这也带来了安全风险的扩散。面对这种情况，如何从全局掌握工控安全风险，充分发挥工控防火墙、工控监测审计、工控漏洞检测等工控安全产品的能力，实现对安全威胁的发现识别、理解分析、响应处置能力，已经成为工控安全建设的重中之重。

迪普科技推出的工控安全监管与分析平台，具备丰富的安全知识库（资产、协议、 漏洞、威胁、事件、情报）以及设备管理、配置管理等安全管理功能。可有效收集各类工控安全产品以及工业互联网安全探针数据，包括资产数据、漏洞数据、异常行为数据、流量数据、指令数据、攻击数据等，通过对采集的数据进行分类、去重、聚合、建模、关联、标准化、深度学习等处理，实现工控安全事件深入分析，并形成多维度安全可视化展示。

产品特点

- **工控安全集中管控**

  支持工控安全设备集中管理，可接入工控防火墙、工控监测审计、工控入侵检测、工控漏洞检测等数十种迪普安全设备以及第三方设备。实时监测设备资源状态，并对工控安全设备进行集中版本升级、特征库升级策略下发等。管理能力包含计划任务、基线检查等。

- **工控安全威胁分析**

  支持访问控制事件、病毒事件、攻击事件、流量异常事件等安全事件分析功能，从事件趋势、事件分布、类型分布、事件源等多个角度统计分析安全事件。支持流量监控、工业指令分析等功能，从流量占比、协议分布、功能码、类型标识等统计分析；支持关联分析引擎，能制定关联分析规则以及事件发生次数或频率，有利于安全事件分析溯源。

- **工控安全态势监控**

  支持包含资产、漏洞、威胁、流量、指令、网络拓扑、健康指数、安全报告等多维度的态势可视化呈现，提供全网所发现的安全漏洞、各类安全威胁及攻击行为事件、工控操作指令等信息，对漏洞隐患信息、安全事件、指令按严重等级、类型分类，通过饼图、柱图、趋势图等形式辅助数据的直观展示。

- **自动生成资产拓扑**

  支持资产拓扑管理功能，依托工控漏洞检测或工控监测审计产品进行资产发现，自动生成基础拓扑结构，并基于模板调优，根据实际需求批量导入导出资产信息，提升用户对资产、脆弱性、安全威胁的感知能力。

- **实时告警提示能力**

  当产品检测到当前环境产生威胁事件时，为快速追溯定位提供直观的告警方式，资产拓扑展示中故障节点实时闪烁告警，提醒 运维人员以尽快处理。支持自定义报警规则，对网络中发现的威胁和故障，向区域负责人进行发送邮件等 方式提醒。

功能价值

技术优势	功能价值
设备管理	支持工控安全设备集中统一管理，可接入工控防火墙，工控审计、工控 IDS、工控漏洞检测等设备，实时监测设备运行状态，可对工控安全设备进行版本更新、策略修改、设备日志收集等。
态势监控	支持采集工控资产情况数据、工控资产漏洞数据、工控行为异常数据、工控攻击事件数据、工控流量情况数据、工控主机安全数据，对访控事件、攻击事件、流量事件、病毒事件、关键事件、主机事件等进行智能分析，进行可视化态势监控。
事件分析	支持攻击事件、流量事件、病毒事件、关键事件等多种安全事件分析，从事件趋势、事件分布、类型分布、事件源等多个角度统计分析安全事件，有利于用户对安全事件分析溯源。
资产管理	支持自定义分区域资产管理和详细资产列表，包含资产 IP、MAC、操作系统、厂商、型号、资产状态等信息。
拓扑管理	支持梳理工控网络流量访问关系，基于流量方向，资产信息生成基础拓扑，提供符合工控场景的模板对拓扑进行优化。
报表展示	使用大屏集中展示，提供面向多种维度的报表模板，包含实时展示和历史统计展示。
实时告警	为快速追溯定位提供直观的告警方式，资产拓扑展示中故障节点实时闪烁告警，提醒运维人员以尽快处理。支持自定义报警规则，对网络中发现的威胁和故障，向区域负责人进行发送邮件等方式提醒。

杭州迪普科技股份有限公司

地址：浙江省杭州市滨江区通和路 68 号中财大厦 6 楼

邮编：310051

官方网站：www.dptech.com

服务热线：400-6100-598