DPtech IMA3000 工控监测审计系统

杭州迪普科技股份有限公司

产品概述

“两化融合”进程的不断深入使得工控系统不再是安全孤岛，漏洞攻击、病毒泛滥、指令篡改、非法操作等安全问题严重影响工控系统的安全性，而传统安全设备无法识别工业环境下的协议及攻击行为，无法进行有效安全监测及防护。迪普科技推出 DPtech IMA3000 系列工控监测审计系统，是专用于工业控制网络中的安全监测与审计设备，可基于 OPC、Modbus、IEC104、IEC61850/MMS、DNP3、S7 等主流工业协议深度报文解析，实时检测告警针对工业协议的网络攻击、非法操作、非法设备接入以及漏洞攻击、病毒传播等异常行为，同时指令级信息记录为事件调查提供坚实基础。

产品特点

- **工业协议深度检测**
  DPtech IMA3000 系列产品内置专业工业协议检测引擎，通过对工业协议攻击特点深入分析，可以有效检测工业畸形报文、参数值篡改、控制域异常、非法操作等攻击行为。
- **工控漏洞攻击检测**
  DPtech IMA3000 系列产品内置专业工控漏洞攻击特征库，可有效检测针对西门子、施耐德、GE 等工控设备以及 WellinTech、WINCC 等上位机系统、软件的漏洞利用、恶意代码等攻击行为。
- **基线行为建模检测**
  DPtech IMA3000 系列产品支持工控网络流量学习建模，结合算法形成安全检测基线，可对偏离基线的行为进行实时检测告警，可有效识别流量突变异常、超过阈值、长周期无流量、非授权设备接入、操作点位偏离等异常行为。
- **指令级安全监测审计**
  DPtech IMA3000 系列产品可针对工控环境中重点/敏感操控指令等关键事件进行监测审计记录，比如组态变更、协议负载变更等事件，可记录详细的操作地址和值，为事件回溯提供基础。
- **强大的本地化分析能力**
  DPtech IMA3000 系列产品支持本地化安全日志存储，可对包含攻击事件、流量异常事件、病毒事件等工控安全事件进行全面分析，可进行工控网络全流量监控、协议深度分析等。
- **IPv6 全面支持**
  DPtech IMA3000 系列产品全面支持 IPv6 相关功能，支持双栈检测，全面适应下一代网络。

产品系列

IMA3000 高端

IMA3000 中端

IMA3000 低端

IMA3000 导轨

功能价值

技术优势	功能价值
数据灵活采集	支持工控采集策略，可基于源 IP、目的 IP、协议、时间等条件进行流量灵活采集，同时支持全流量采集策略。
工业协议深度解析	支持 OPC、Modbus、IEC104、IEC61850/MMS、DNP3、S7 等在内的多种工业协议深度解析，可有效识别协议内容负载，同时支持协议自定义，满足工业网络大量私有协议场景下用户自行扩展要求。
工控流量分析	支持梳理工控网络流量访问关系，从流量趋势、协议、资产等维度进行流量统计分析，有利于用户掌握工控网络流量情况。
安全事件分析	支持攻击事件分析、流量异常分析、指令异常分析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。
工控指令监测	支持 Modbus、S7、IEC104 等主流工控协议指令监测记录，对用户操作行为审计，满足合规性要求的同时，发现潜在安全威胁。
实时告警	支持工业协议深度检测、工控漏洞攻击检测、行为基线建模检测等多种检测引擎，有效检测告警工控网络中的入侵行为。

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