力控科技 FORCECON | HUACON 力控华康

工业网络安全审计系统 HC-ISD

北京力控华康科技有限公司

www.sunwayland.com

目 录

产品概述

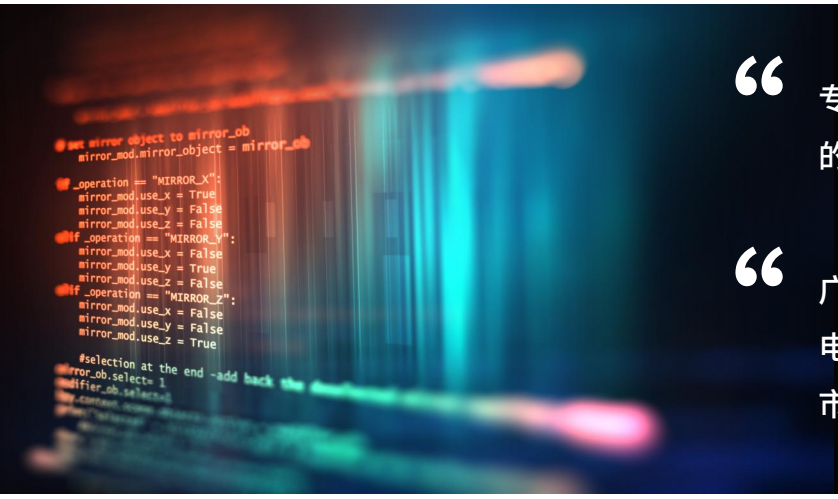
从“震网”病毒到“HAVEX”，从“BlackEnergy”到“勒索”病毒，针对工业控制网络，特别是对关键基础设施的直接攻击、信息窃取和勒索事件等工控网络安全事件层出不穷。随着“两化融合”和“中国制造2025”战略的不断推进，工业控制系统的信息化程度会迅速逐步提高，针对工业控制网络的攻击将成为一种常态，工业控制系统的信息安全将会得到前所未有的高度关注。

传统的网络安全产品无法适用于工业控制网络，原因有很多，诸如：工控网络首先要保证可用性，牺牲可用性的安全手段是不提倡的；工控网络无法接受“漏报”和“误报”；传统安全产品无法识别工控协议，特别是众多的私有协议；工控网络内的所有产品升级的频次可能很低，需要频繁升级的安全产品可能不适用……

IT 领域的入侵检测和审计产品也无法满足工控网络安全的需要，但是，入侵检测和安全审计是非常必要的安全技术手段，《中华人民共和国网络安全法》中明确要求“采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月”。

工控安全审计系统正是**专门为工业控制网络量身打造的工控网络安全产品**。它能实时监测工控网络的状态，检测工控网络中入侵行为，也能根据用户定义的审计策略，追踪工控网络安全事件，它能对工控网络的数据进行留存。

工控安全审计系统适用于SCADA、DCS、PCS、PLC等工业控制系统，可以被广泛的应用到**石油石化、天然气、电力、智能制造、水利、铁路、城市轨道交通、城市市政**以及其他与国计民生紧密相关领域的工业控制系统。

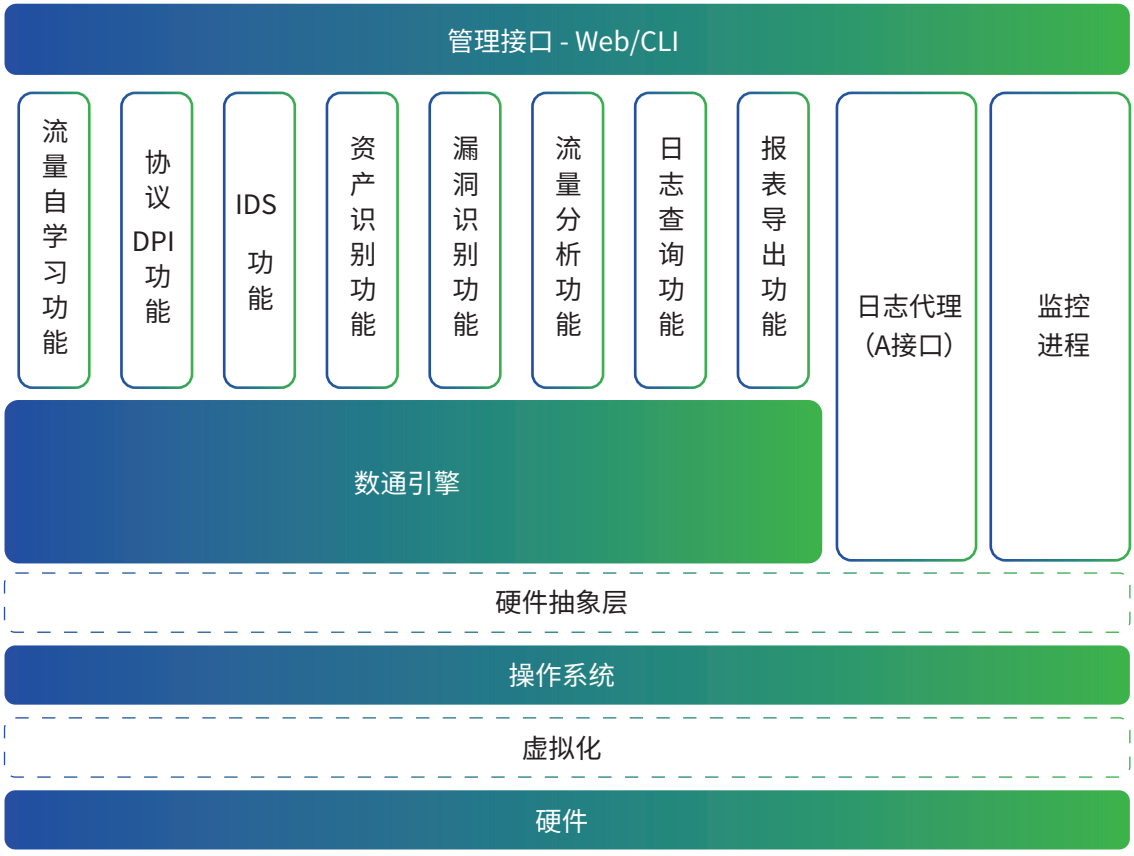


“专门为工业控制网络量身打造的工控网络安全产品”

“广泛应用到石油石化、天然气、电力、智能制造、水利、铁路、城市轨道交通、城市市政”

产品架构

主要由硬件、操作系统、核心功能、用户接口层共四个部分组成，可以在各种不同场景的工业网络环境中进行灵活的部署和管理。



工业网络安全审计系统架构图

①硬件层

使用专用的硬件平台，提供可靠稳定的硬件环境，辅助以系统运行的必须软件，组成基础平台层，支持传统IT网络协议，支持工业网络协议。

②操作系统层

处理器完成运算和控制的设备，存放程序和数据，何处存放哪个程序，何处存放哪个数据. 操作系统的设备管理功能采用统一管理模式，自动处理内存和设备间的数据传递，从而减轻用户为这些设备设计输入输出程序的负担。作业是指独立的、要求计算机完成的一个任务。操作系统的作业管理功能包括两点，一是在多道程序运行时，使得备用户合理地共享计算机系统资源，二是提供给操作人员一套控制命令用来控制程序的运行。

③核心业务层

在该层实现系统的应用功能。包括基于工业网络协议识别、解析，基于白名单、黑白名单的异常行为告警，资产识别、漏洞识别、日志采集与分析等应用功能。

④用户接口层

在该层实现和最终用户的人机界面，通过WEB接口进入管理界面进行系统配置管理。

产品特点

实时工控网络监测

默认通过旁路的方式(也可以串接)对工控网络进行实时监测,对协议、流量等元素进行统计分析,实时显示网络的状态。

独有的异常流量检测方法。

实时入侵检测

实时检测工控网络中的攻击行为,利用内置的工控威胁库,根据已知的威胁特征建立检测规则,实时对网络中的入侵进行告警。

工控行为和协议规则自学习

通过深度解析工控协议、分析工控过程行为,自动学习基于工控协议的操作行为和规则,建立安全检测模型。

不合规行为监测

通过自定义规则或白名单规则,检测业务流量中不合规的工控网络行为,对不合规行为进行实时的告警和响应,留存网络数据。

工控协议深度检测

支持OPC协议的深度包检测、OPC 动态端口开放;报文格式和完整性检查。

支持Ethernet/IP、Modbus/TCP,IEC104,DNP3,Profinet,MMS,S7,GOOSE,SV等工控协议的深度检测,例如报文格式检查、功能码控制、寄存器控制,连接状态控制等的检测。

支持自定义格式的工控协议检测。

工控网络数据留存

根据用户自定义设置,留存所有网络的原始数据,可配置为留存六个月及以上时间。

系统自身安全性

基于 SSL 的远程管理:通过网络可以直接对工控安全审计系统进行管理和配置。通讯采用了SSL加密技术,所有配置管理信息在网络上全部以密文传输,可以防止恶意攻击者使用网络监听工具窃取信息。

系统具备网络层恶意攻击检测及过滤控制能力(如抗 SYN Flood、UDP Flood、ICMP Flood、抗 Ping of Death、Smurf、Land attack 攻击等)。

基于角色的分权分级管理,有利于减少对系统的滥用。

安全审计及响应

对安全事件进行审计,及时追溯安全事件的轨迹。

对用户的操作行为进行细粒度审计,方便还原操作的真相。

独立的告警响应机制,可定义对不同安全级别的安全事件的响应方式。

严苛的工业级硬件设计

产品硬件采用了适应工业环境的硬件设计。

◉防护等级 IP40，满足工控网络应用环境要求。

◉通过多项国际安全认证、可靠性和稳定性满足要求。

◉通过工业级宽温测试，工作温度、湿度满足工业现场要求。

◉低功耗、无风扇、全封闭设计。

支持多重检测机制

采用以下手段对于应对日益严重的APT（高级可持续性威胁）攻击提供了全面的防护：

◉支持对已知攻击行为的检测和防护，内置了庞大可升级的工控威胁库；

◉支持自学习工控协议规则和行为，建立安全检测模型；

◉可通过白名单防护阻止一切不明的威胁。

工控协议支持及深度检测

工控安全审计系统支持多种工控协议的识别与检测，对其中的Ethernet/IP、Modbus/TCP，OPC，IEC104，DNP3，MMS，S7，GOOSE 等协议都能实现深度解析。

工控协议的自定义接口

工控安全审计系统提供了开放的协议接口，可以对未知协议和私有协议进行自定义。系统提供私有协议开发接口，方便用户扩展支持私有协议和定制化开发。

灵活的部署方式

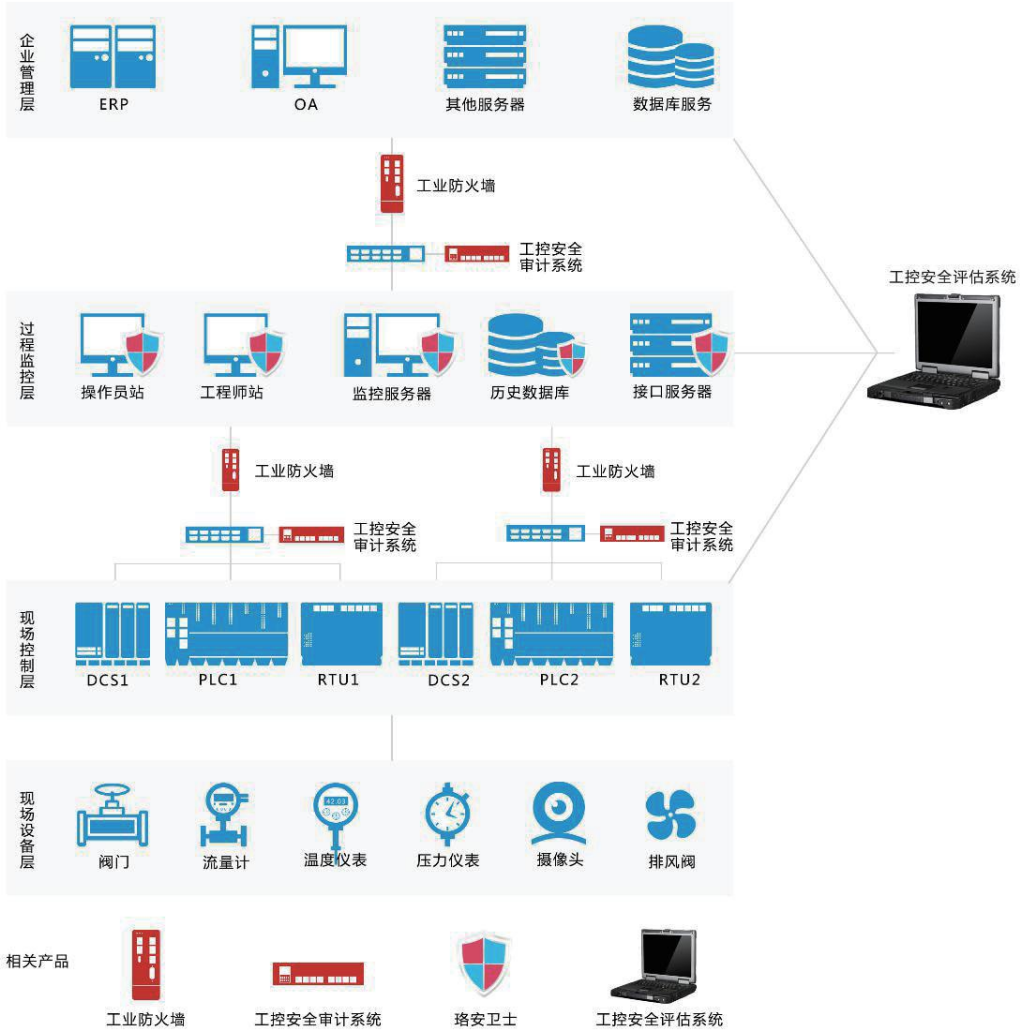
工控安全审计系统默认采用旁路接入的部署方式，对工控网络无影响。针对特殊需求的用户，也支持透明桥接的部署方式，低延时和设备故障 Bypass 可满足工控网络部署要求。

典型应用

由于工业控制系统所覆盖的行业重要性，比如油化、电力、核电厂、水利、交通、市政、军事、高端制造业等，其安全性问题也越发的重要，并且牵涉到国计民生。对于这些关键信息基础设施，如何进行安全监测及预警，如何及时有效的进行事前的防范，事中的监测以及事后的追溯，正成为工控安全领域亟待解决的问题。

工业网络审计系统能够像“黑匣子”一样精准记录工业控制系统内部的网络通信行为，为可能出现的安全隐患提供详实的记录。可以对工业网络出现的网络异常行为、针对工业协议进行的不合规攻击以及工业控制流程出现的关键操作进行实时的检测与告警。

典型应用



实时网络监测，让攻击无处遁形

工控安全审计系统实时对工控网络进行监测，通过内置的工控威胁库，能最大限度的识别已知的攻击行为；通过自定义或白名单策略，能及时发现不合规的行为，对发现潜在的未知威胁提供了有效的技术手段。实时的告警和响应使得恶意的攻击意图无处遁形。

网络数据留存，依法合规

工控安全审计系统支持用户自定义留存工控网络的网络日志数据，符合《中华人民共和国网络安全法》的规定。

安全数据审计，还原“安全事故”真相

对工控网络数据审计和分析，可追溯安全事件的轨迹，为还原事故真相提供了有效的技术手段。

行业安全数据积累，凸显安全数据价值

工控安全审计系统监测、审计工控网络最接近设备层的“管道数据”，安全数据真实可靠，具有较高的价值。通过大数据分析可获取行业安全态势，逐步提升安全防护能力。

力控科技 FORCECON

北京力控华康科技有限公司

地址：北京市海淀区天秀路10号中国农大国际创业园1号楼
总机：010-62839678
全国统一服务热线：400 650 1353
www.huacon.com.cn

关注公众号　关注小程序