三中科技工控入侵检测系统

产品名称	三中科技工控入侵检测系统
公司名称	郑州三中网安科技有限公司
价格	.00/个
规格参数	
公司地址	郑州高新技术开发区长椿路11号
联系电话	0371-55519655

产品详情

产品概述

[illegible]

[illegible]

应用价值

工控网络入侵检测

[illegible]

工控内网安全监视

[illegible]

工控协议合规性检测

对协议通讯内容进行鉴别与合规性检查，及时发现协议违规使用、命令越权操作等各种行为并进行报警展示。

工控网络全流量审计

l 提供实时分析与长时间全流量数据保存及审计追溯能力

l 关键取证数据的数据包和统计信息永久保存

l 高效多角度的数据挖掘快速检索能力

功能特点

网络流量监控

[illegible]

基于特征的深度协议识别与解码

系统提供近百种网络通讯协议的准确识别、解码与分析。其中包括以下专有工控协议，[illegible]

基于协议合规性检查的入侵检测

基于协议数据解码以及对会话端口通信等异常业务发现工业控制网络内的危险指令、高风险指令、数据库操作以及工控协议的使用等异常业务数据。

丢失的网络协议规性审计等异常行为及时发现工业控制网络内的入侵行为，系统检测到这些入侵行为，会实时给用户提供警报展示。

基于业务行为基线的入侵检测

系统支持多视角、多层次对工控网络内各工控协议的业务指令进行统计建模，建模的维度为通信关系、协议类型、业务指令、通信频率、响应周期等，通过一段时间的自动学习建立业务模型，这个业务模型就是工控网络的业务基线。

通过业务基线，系统可以识别以下异常行为：

- 业务基线没有业务交互的两个控制节点产生了业务交互；
- 控制节点间发生了之前没有发生的业务指令；
- 键业务产生的时间与基线有较大的差异；
- 业务指令的响应周期比基线值有较大幅度的增加；
- 控制节点间的业务指令交互频率较大幅度的高于或者低于基线值；

这些异常行为意味着工控网络很可能正在被入侵，基于业务行为基线能够对新型和未知的攻击进行识别。

智能警报

系统能够对产生警报的通讯数据进行深入的智能分析，从而能够更准确的发现异常的网络行为。用户可以根据网络状况灵活调整警报参数，并提供相应的数据依据。

- 工控网络协议合规性检查警报
- KPI参数警报（用户自定义关键流量阈值，诊断条件等）
- 警报设置：警报属性定义，触发条件，解除警报条件等，触发的警报信息可以通过E-mail发送给指定人员，或者是发送到指定的SYSLOG服务器。

智能报表

提供丰富的内置报表，异常流量分析报表、异常行为分析报表、流量报表、入侵警报报表、协议应用统计报表，并支持用户自定义新报表，包括TOP排行报表。

网络流量单向采集

提供严格的数据单向采集方式，确保单向无反馈传输。所配单向接收网卡（适配器）只接收数据，无法向外部网络发送任何数据。

系统部署

在生产控制区（安全区I）内部署多个前端探针作为数据监测点，对来自计算机监控系统中心交换机的数据流进行实时旁路监测、解析和检测分析。管理员通过控制台连接至分析中心，实现对网络安全的集中监视管理。

分布式部署多个网络监测探针采集监测点的网络流量数据，实时分析网络状态和检测异常，并负责将告警信息上报给分析中心。分析中心负责汇总各探针上报的数据和日志，进行存储、关联分析和统一呈现。

分析中心负责收集所有探针获取的数据包进行长期保存，并且可以在必要时刻进行回溯，对关键数据进行深度解析，为安全事件追溯提供数据依据，同时提供日志挖掘分析，除了展现数据流向外，还能