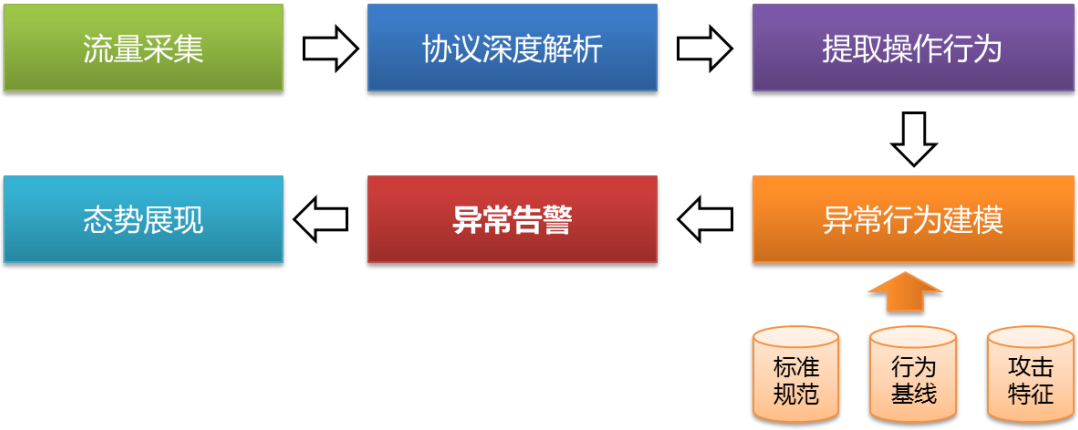
绿盟工控安全审计系统产品彩页

一. 产品概述

绿盟科技工控安全审计系统基于对不同业务系统工控环境的理解和对协议规约的深度解码，通过预制的行业经验模型，结合工控系统中操作过程中相关的规程要求，来感知系统中潜在的异常操作行为。深度分析从上位机指令下达过程从上位机控制端到下位机操控指令进行有效的合规性定义。



工控安全审计系统能够分析工控现场中的操作是否符合定义的操作要求，如发现其中有任何的违规操作及时进行报警。系统主要通过旁路部署的方式对工业生产过程进行零风险的监测与记录，基于对工业控制协议（如 IEC 60870-5-101、102 和 104 协议、IEC 61850、IEC 61970、ICCP、MODBUS TCP、PROFINET 等）的通信报文进行深度解析，能够实时检测针对工业协议的网络攻击、用户误操作、用户违规操作、非法设备接入以及蠕虫、病毒等恶意软件的传播并实时报警，同时详实记录一切网络通信行为，包括指令级的工业控制协议通信记录，为工业控制系统的安全事故调查提供坚实的基础。

二. 客户价值

绿盟工业安全异常行为审计产品可以：

- 及时发现生产系统中潜在的异常操作行为；

- 为安全事故的调查取证提供详细的数据记录；
- 通过可视化的友好用户界面提高工控系统安全审计管理效率；
- 满足相关的合规性要求；
- 模板化的免配置模板，减少了运维过程人员的投入

三. 产品优势

绿盟工业安全异常行为审计系统的优势集中体现在以下几个方面：

- 工业通信协议的深度过滤

绿盟工业安全异常行为审计系统可以针对工业协议进行深度解析，可以针对工业网络协议的内容和数据进行细致的合规性检查，对于操作指令中包含的针对点表、寄存器的异常操作进行报警，最大限度地保护控制系统的安全。

支持的通讯协议包括IEC 60870-5-101、102和104协议、IEC 61850、IEC 61970、ICCP、Modbus Tcp、Profinet、OPC、S7等工控系统常用协议类型。通讯协议可根据用户需求进行现场分析和定制化处理，灵活应对不同系统类型的工控环境。

- 适用于工业现场的免配置模型

绿盟工业安全异常行为审计系统预置了基于不同行业业务运行特点的模板，免去了用户配置的复杂操作，用户可以基于行业和多种特性的组合，来定义相关的应用场景。

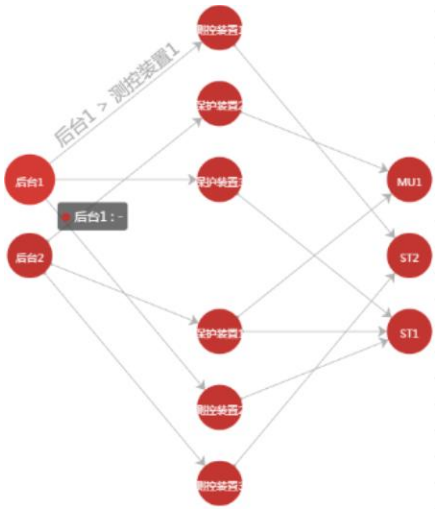
- 符合工业用户使用习惯的配置方式

工业中广泛应用的组态软件将专业的工艺流程、复杂的数据反馈封装成简单的图形化界面，直观的反映工业现场的生产情况。组态软件以其图形化、直观性和易用性深受广大工业用户的喜爱，也成为工业用户习惯的使用方式。绿盟工业安全异常行为审计系统也做到了简单、直观、易用。

四. 关键功能

4.1 基于机器自学习的业务行为基线

工业网络中设备众多、网络通信复杂，用户很难全面的掌握网络中所必须的业务通信需求，这会给安全设备的规则配置带来很大的困难。为了方便用户进行异常行为检测规则的配置，提高规则配置的准确性，减少规则配置的工作量，绿盟工控安全审计系统检测开发了基于机器自学习的业务行为基线功能。该功能采用被动检测的方式从网络中采集数据包，并进行数据包的解析，智能的与系统内置的协议特征、设备对象等进行匹配，生成可供参考的网络交互信息列表，通过对协议分布和流量信息的匹配，形成“工控场景行为基线”，帮助用户以最捷的方式了解和掌握网络中的业务通信状态，发现网络潜在的安全。智能化的流量自学习规则，还可以辅助系统自动生成相关的异常检测规则，对现有的规则进行调优等。



4.2 工控协议深度解析

绿盟科技基于对工控环境的理解，针对工控环境使用的规约进行了相关的分析和研究，对于协议的内容进行了完全的解码，可以深入到指令级别的分析，对于从上位机控制端到下位机操控指令进行有效的合规性定义。通过镜像方式对流量进行深入解码，分析其中的操作是否符合定义的操作要求，如发现其中有任何的违规操作，及时进行报警，有管理员来进行相关的处理。

4.3 工控网络异常行为监测告警

绿盟科技针对不同客户在审计工控中的需求，对于基于 IEC 60870-5-101、102 和 104 协议、IEC 61850、MODBUSRTU 和 PROFINET 等工控协议的操作指令进行有效的识别，定义了其中存在的高危操作，能够及时进行报警。如对于变电站侧的 SV 报文，能够发现其中存在的采样值的变化情况，如发现采样操作超过了预定义的 3000HZ 的频率，会发出相关的告警。用户也可以根据实际的工程经验，在系统界面中进行配置。

异常行为告警包括：任何外接设备入场告警；模型内设备间不符合模型访问时间、频率告警；模型内设备间不符合基线原行为操作告警；模型内设备间不符合基线原行为路径操作告警等。

五. 典型应用

5.1 电力行业

通过预制的审计要求，可以对从调度中心到厂站和厂站到调度中心之间的传输的信息进行有效审计。发现其中操作指令是否符合预制的审计规则，如果发现其中存在恶意的操作行为或者一些误操作的指令进行下发，审计设备可以进行及时的告警。并且在存在操作异常的时候追诉中，审计设备可以实现对恶意事件和行为事后追查稽核、重建事件和系统条件，生成问题报告。为事后的分析提供有效的依据。如下图所示：