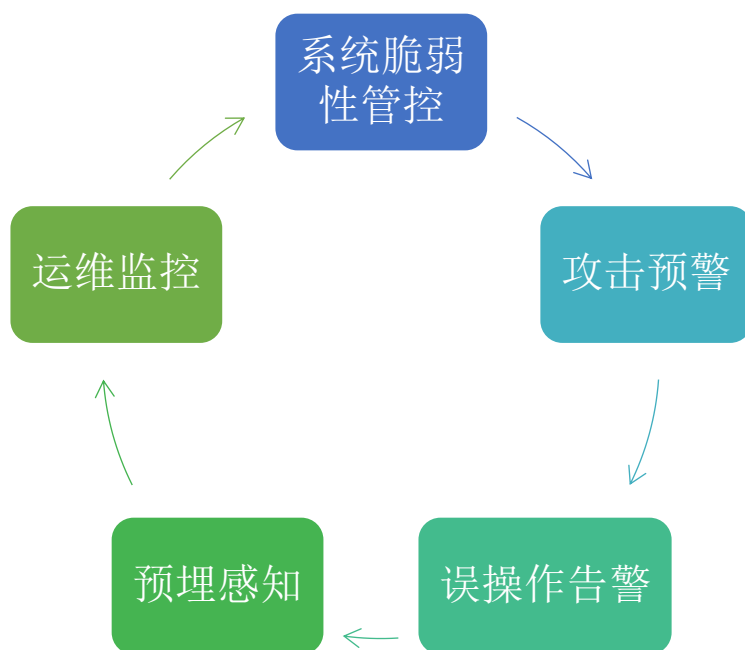


绿盟工业网络安全监测预警平台

(NSFOCUS-INSP)

产品概述

INSP 以大数据框架为基础，通过攻防场景模型的大数据分析及可视化展示等手段建立和完善工业网络安全态势全面监控、安全威胁实时预警、安全事故紧急响应的能力。通过独有的自适应的体系架构，高效地结合情境上下文分析，协助安全专家快速发现和分析安全问题，并能通过实际的运维手段实现安全闭环管理，同时弱化工业信息孤岛导致不能关联分析的问题。利用情报和智能分析成果，对企业发布早期预警信息，评估工业企业内部可能受影响的设备或资产，避免核心业务系统遭受的攻击和预防潜在的安全隐患。



客户价值



- 基于大数据架构和能力，帮助企业对海量日志进行采集，存储和分析
- 上至业务层网络，下达生产现场，全局把控
- 通过大数据分析和可视化技术，帮助客户感知网络安全态势
- 本地分析结果通过情报进行验证，并进一步关联分析，形成预警
- 通过对企业合法资产的监控和对比，提升企业对资产变化的感知，暴露可疑资产风险
- 通过持续的漏洞监控和管理，帮助企业将风险管理落地，实现闭环管理
- 安全合规

产品优势

全面的日志管理和综合审计

平台可以对工业网络安全数据进行采集，包括目前主流的网络设备日志，安全设备日志、工业主机系统日志、工业数据库系统日志、工业组态应用系统日志等。

工控安全管理

平台设备管理功能模块支持工业安全网关、工控安全审计系统、工控漏洞扫描系统等设备接入。统一监控绿盟工控安全设备，实现安全设备管理和状态监控，实现设备配置基线管理。

全方位监测预警

自动收集情报和智能分析成果，对企业发布早期预警信息，评估企业内部可能受影

响的设备或资产，避免核心业务系统遭受的攻击和预防潜在的安全隐患，提高预警的准确性。

一站式信息综合管理

平台提供一站式的信息综合管理功能。一站式综合管理包括对安全设备上传的事件类日志信息、业务系统上传的操作等日志信息、采集的安全设备配置策略信息进行统一的分析和呈现。平台可以从多种维度对海量数据进行安全分析和统计，并通过趋势图，占比图等清晰展示全网安全态势。

脆弱性全生命周期管理

平台支持通过对企业资产进行7*24小时持续监控，验证和预警全生命周期的管理，实现最终的企业风险管理闭环的目标。

典型应用场景

