InSecOps 星哨

新能源厂站无人安全值守方案

01 新能源安全现状

企业防御视角 | 安全能力视角 | 网络攻击视角 | 发展历程视角

新能源安全现状 - 厂站现状

地理位置偏远

新能源厂站一般都在偏远的山头、沙漠等地带，到现场进行故障处置、响应，路上需耗费大量时间，导致故障响应和处理时间极长

厂站地域分散

集管新能源厂站所在地域分散，再加上位置偏远，要完成一轮风险评估、安全巡检等日常安全运营作业，耗时以月计，难以及时发现安全风险

装机容量较小

新能源电站相对传统水电，大多装机容量较小，主要集中在50-150MW区间，大量新能源电站还处于投入期，导致网络安全投入不足，升压站无IT、网络安全相关专业运营人员，难以应对网络安全威胁。

集管厂站较多

集管新能源厂站从数量上说，数倍于传统水电站数量，并且随着新能源建设的加速，数量只会越来越多，传统人工运营的方式，让集控中心对于新能源电站的安全越来越难以应对。

新能源安全现状 - 安全运营现状

攻击趋势上升，增加安全生产风险

攻击者持续利用利用APT、0Day漏洞、钓鱼攻击、勒索病毒等手段，对新能源系统进行攻击，可能导致关键设备损坏、生产中断，导致巨大的经济损失

- 根据标普全球普氏的“原油安全哨兵”研究项目，自2017年以来，全球针对能源领域的网络攻击数量激增.
- 2023年，美国Colonial输油管道系统遭袭，导致美国东海岸多州加油站关停，政府向黑客支付了230万美元赎金。
- 沙特阿美在2021年7月确认，公司部分数据遭到泄露，并遭遇网络勒索，涉及金额高达5000万美元。

止步安全合规，难以确保网络安全

目前大部分新能源厂站仅满足于达到法律法规的最低要求，而没有从业务连续性和风险管理的角度出发，进行更为深入和全面的安全防护和持续的安全运营。

缺失安全专员，无法响应安全要求

目前大部分新能源厂站只有负责生产运维的班组，缺失具有安全技能的专员，导致无法针对安全事件快速做出响应，无法根据集控的要求执行网络安全作业。

受限地理因素，阻碍网络安全运营

新能源厂站“远小散多”的特性，决定了集控的安全专员或外协人员无法快速到达现场，造成安全事件、风险等无法及时响应，阻碍了网络安全运营工作的开展。

02

无人安全值守方案

介绍 | 对比 | 设计理念 | 整体架构 | 各模块介绍

安全挑战

攻击趋势上升，增加安全生产风险
攻击者持续利用利用APT、0Day漏洞、钓鱼攻击、勒索病毒等手段，对新能源系统进行攻击，导致关键设备损坏、生产中断，导致巨大的经济损失。

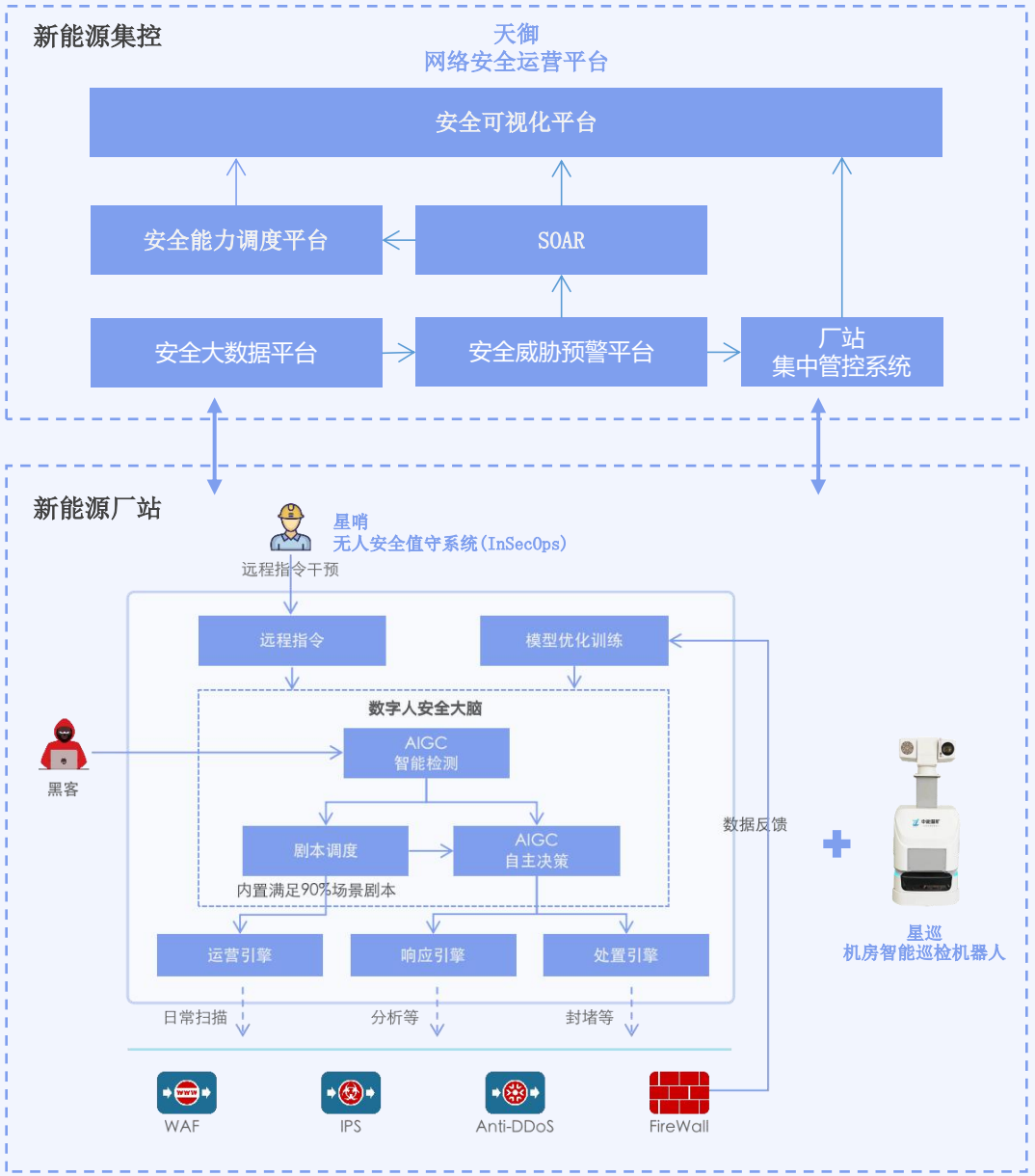
止步安全合规，难以确保网络安全。
大部分新能源厂站仅满足于达到法律法规的最低要求，而没有从业务连续性和风险管理的角度出发，进行更为深入和全面的安全防护和安全运营。

缺失安全专员，无法响应安全要求。
大部分新能源厂站只有负责生产运维班组，缺失具有安全技能的专员，导致无法针对安全事件快速做出响应，无法根据集控要求执行网络安全作业。

受限地理因素，阻碍网络安全运营。
新能源厂站“远小散多”的特性，决定了集控的安全专员无法快速到达现场，造成安全事件、风险等无法及时响应，阻碍了网络安全运营工作的开展。

方案介绍

无人安全值守一体化防护方案 —— 提供一体化安全服务能力建设，通过对所有厂站整体风险呈现、统一登录、集中策略下发、无人值守任务编排、人工干预等代替安全人员，负责新能源厂站无人安全值守，进行自动监测、自动巡检、自主分析、自动处置、主动报告等安全运营业务，对新能源厂站物理环境进行运营管理。包括设备状态监测、环境参数监测、资产判断、网咯安全物理环境检查等。为业务/用户提供按需定义的安全服务能力，实现弹性扩展、安全统一运营、无人值守的一站式云安全解决方案。



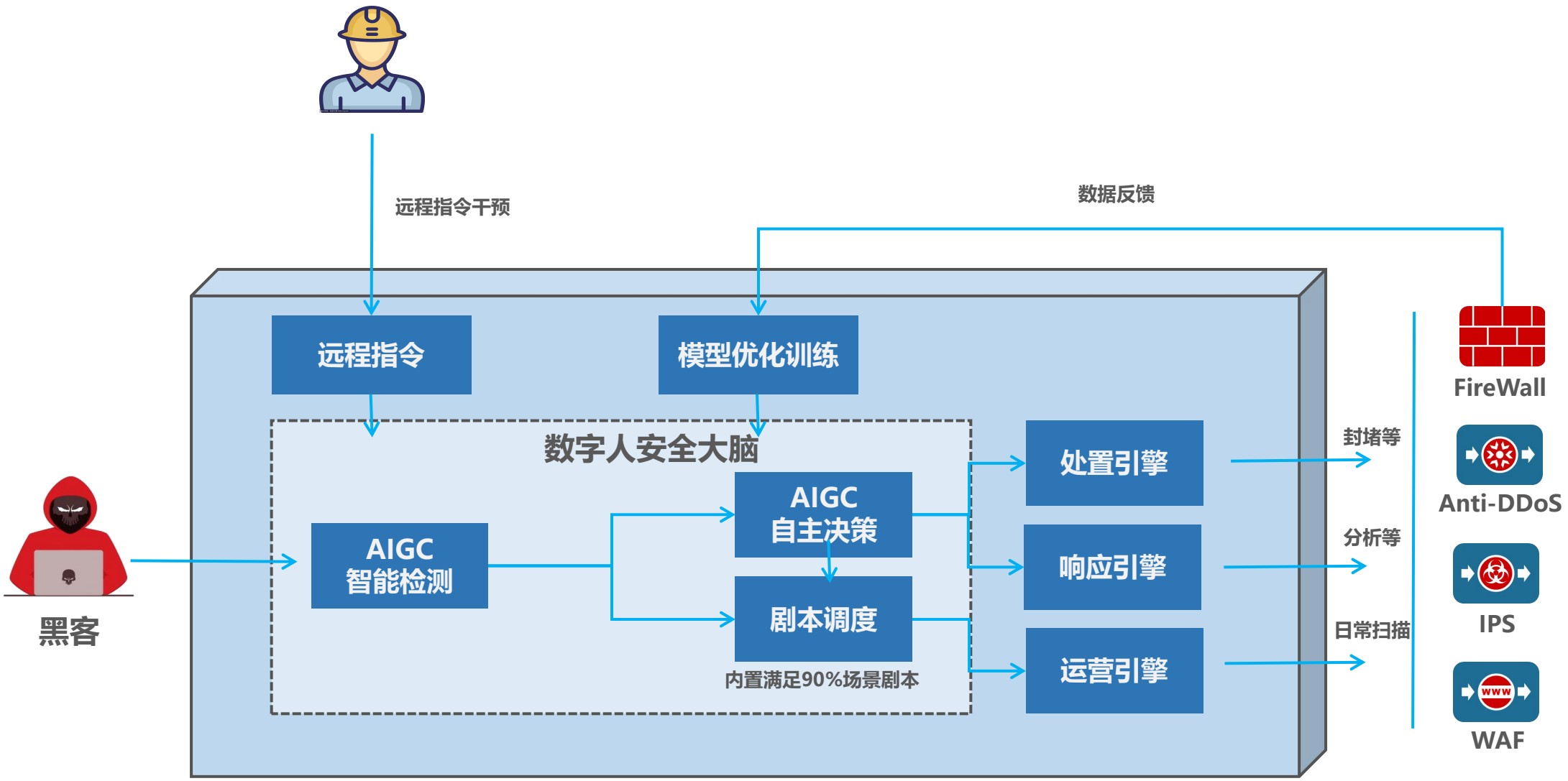
产品介绍 - 星哨-无人安全值守系统(InSecOps)

通过自动化技术、设备管控技术、AIGC技术实现对网络安全的定期巡检、自动监测、自主分析、自动处置，减少对人工的依赖，达到新能源厂站现场网络安全少人化、无人化运营，大大降低企业在安全上的投入、提升厂站安全防御能力。

核心功能

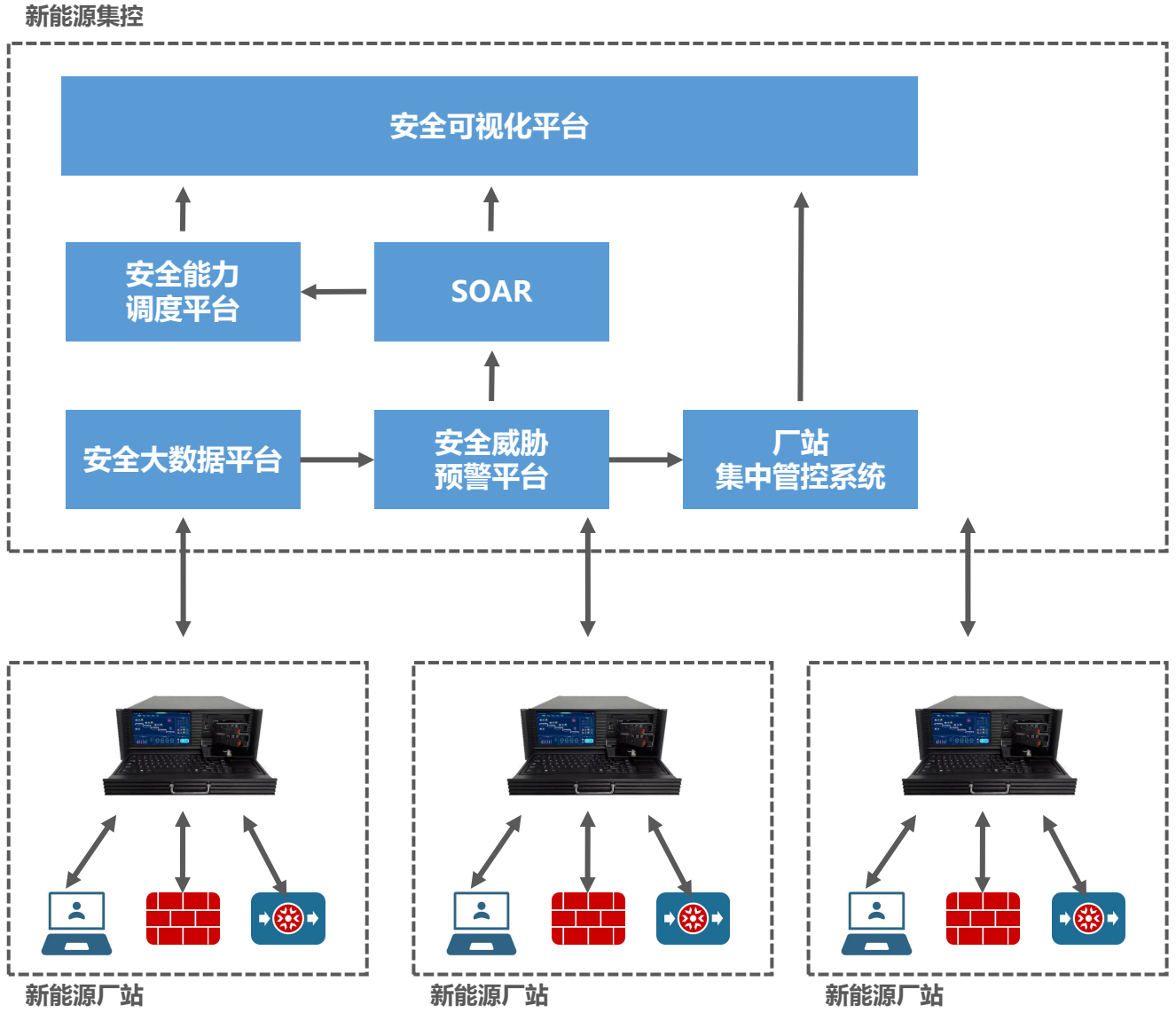
1. 资产管理（发现、注册、退运）
2. 漏洞管理（资产漏洞、30W+漏洞库、漏扫报告）
3. 自动监测（状态监测、日志监测、流量监测）
4. 自主分析（故障分析、日志分析、流量分析、情报分析、综合分析）
5. 自动处置（封堵、加固、升级、上报）
6. 定期任务（定期巡检、定期漏扫、定期基线检查）
7. 自动报告（暴露面报告、威胁报告、资产报告、巡检报告、日报、周报、月报、年报）
8. 主动通知（电话、短信、系统消息）
9. 远程受控（接收集控登录、策略下发、配置等指令）

产品介绍 - 星哨-无人安全值守系统(InSecOps)



产品介绍 - 天御-网络安全运营平台

通过对新能厂站无人值守系统数据的统一采集、分析、可视化展示，呈现整体安全风险。并可透过无人值守系统执行运营工作计划、远程指令下发、远程配置下发、远程系统登录等集中管控能力，以从全局掌控、分析、处置网络安全风险。



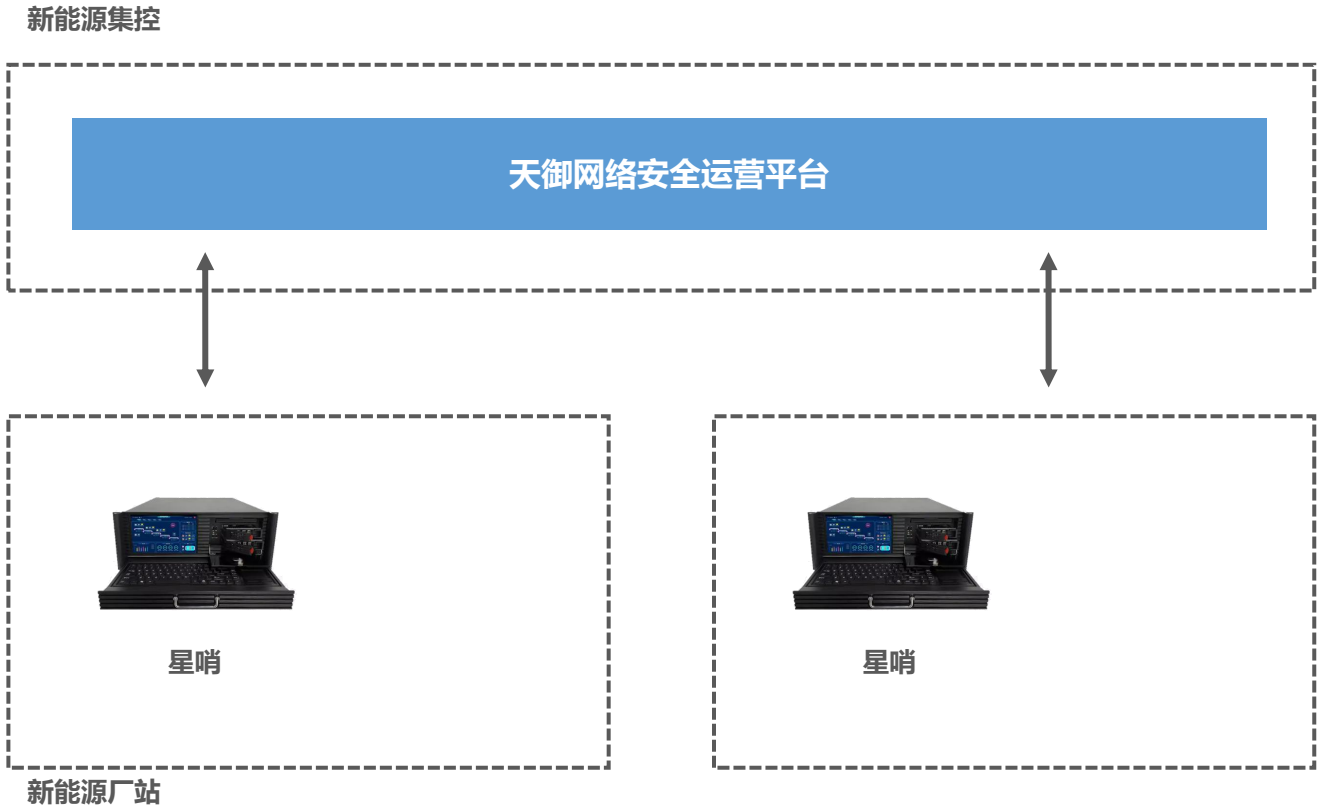
整体方案

天御

负责所有厂站整体风险呈现、统一登录、集中策略下发、无人值守任务编排、人工干预等业务。

星哨

代替安全人员，负责新能源厂站无人安全值守，进行自动监测、自动巡检、自主分析、自动处置、主动报告等安全运营业务。



03 无人安全值守应用

介绍 | 对比 | 设计理念 | 整体架构 | 各模块介绍

应用 - 日常巡检

代替人工，定期进行网络安全巡检，并输出报告，上报集控中心

设备巡检

检查主机、服务器、防火墙等设备是否正常运行、有无高IO、高CPU占用等情况。

系统及软件巡检

检查所有系统和应用软件是否为最新版本，确认安全补丁和更新是否已经安装。

安全设施巡检

检查防火墙、入侵检测等设备规则库是否最新，版本是否最新等

策略巡检

审查网络安全政策和程序

漏洞扫描

定期执行扫描任务并上报扫描结果

基线检查

定期检查安全基线，并提供整改建议

机房巡检

通过星巡机器人定期对机房物理环境进行检查。

网络巡检

检查网络通断，并上报故障

应用 - 风险监测

通过采集、接收两种方式汇聚新能源厂站安全设备、安全系统的日志数据，并能通过可视化编排的形式对日志数据进行范化、清洗、入库，实时检测各类安全设备的告警。

日志监测

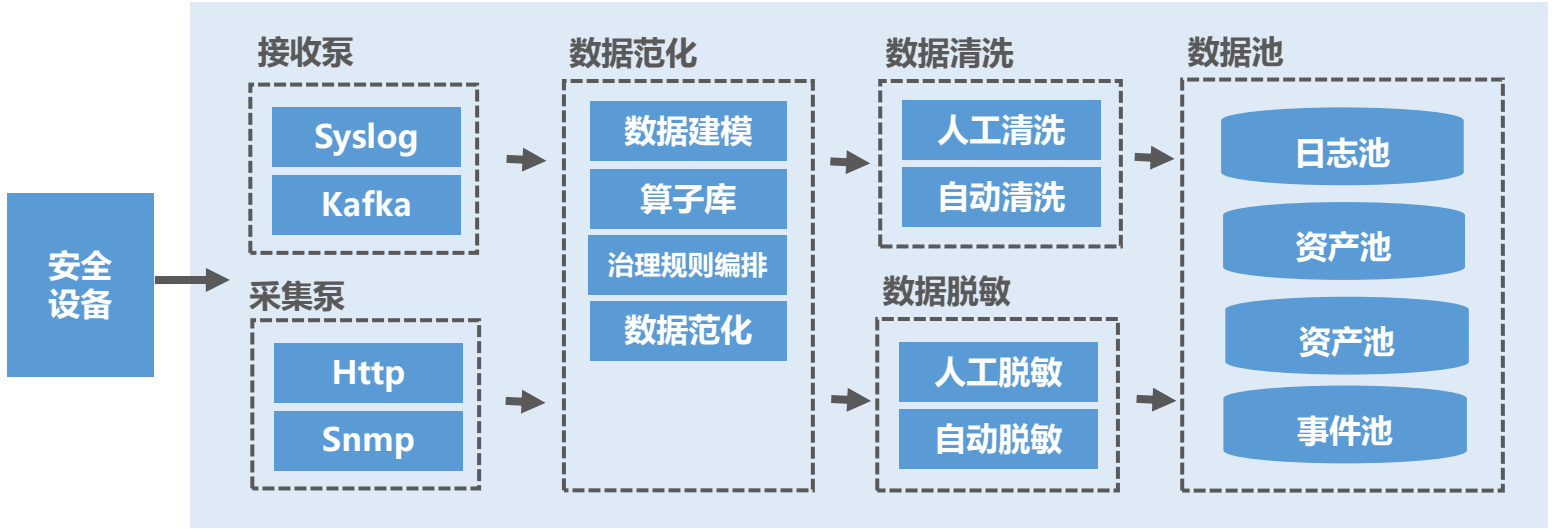
监测安全设备、系统发现的告警。

流量监测

监测流量中发现的异常流量中断等场景。

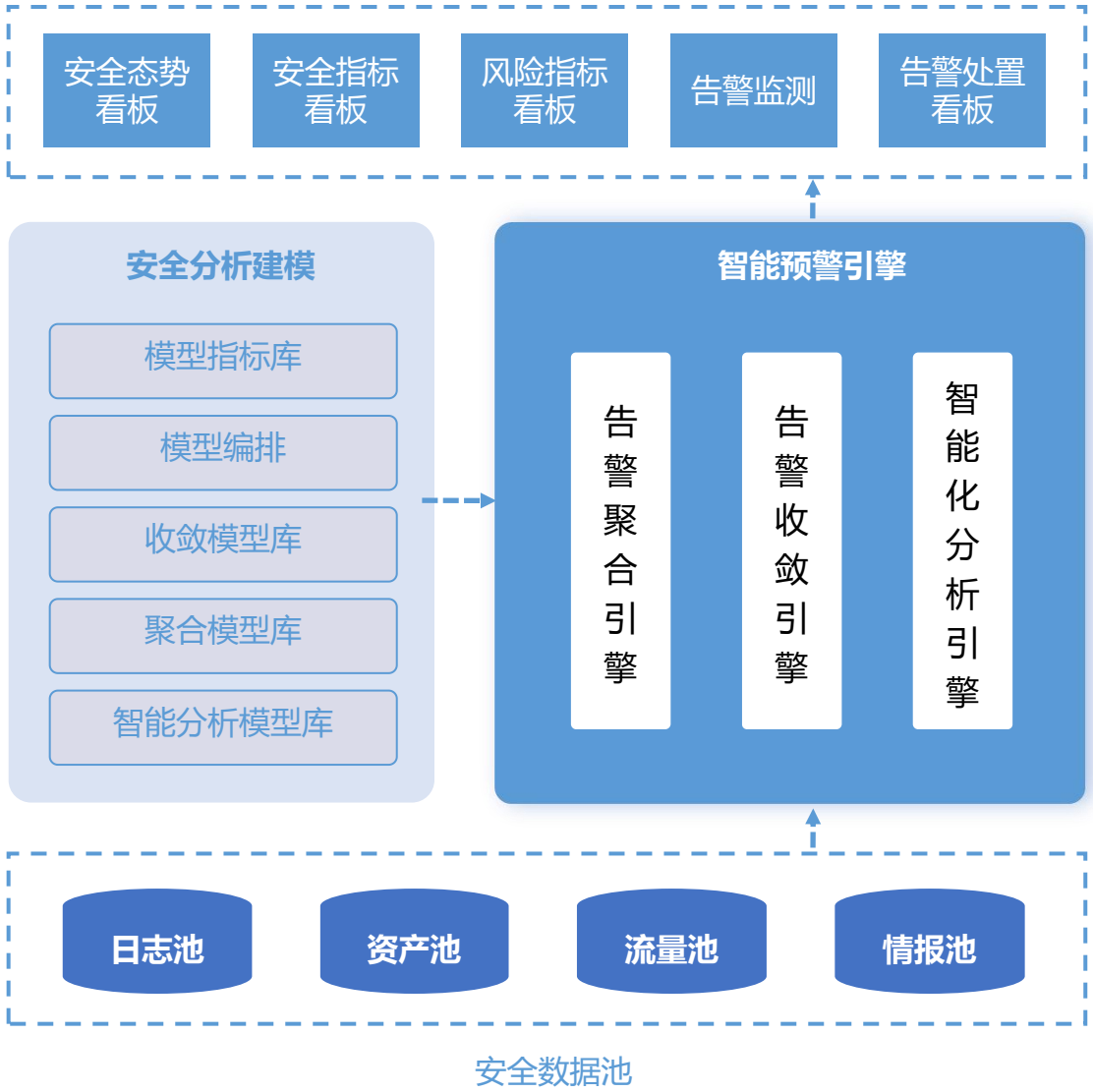
蜜罐检测

自带蜜罐，监测异常的扫描、恶意访问等信息。



应用 - 自主分析

对新能源厂站的流量数据、日志数据进行综合分析，发现故障、收敛告警数量

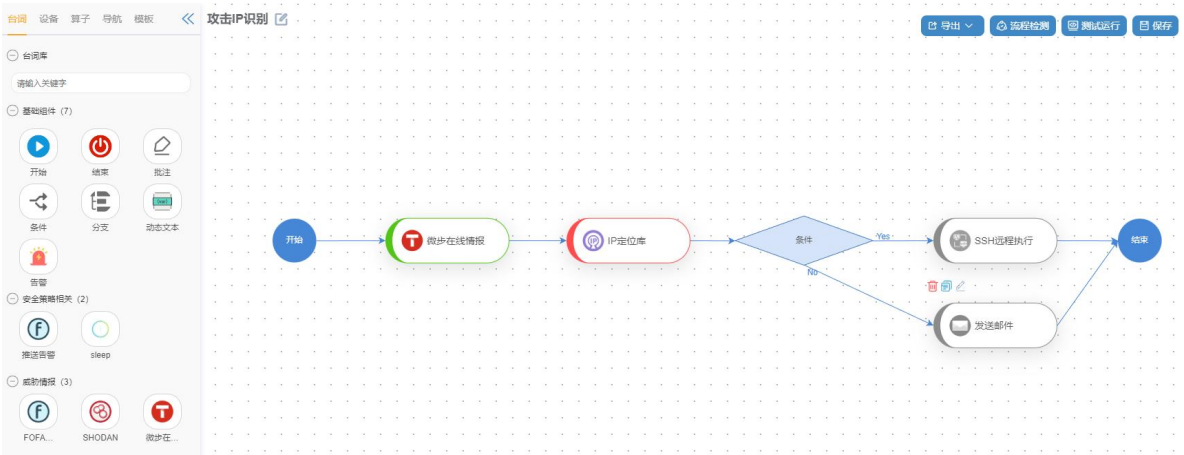


- **故障分析：**通过机器学习算法对厂站流量进行基线学习，发现异常流量，分析故障点；
- **告警收敛：**通过统计分析模型，对低危、垃圾告警进行过滤，解决告警泛滥的问题；
- **情报分析：**结合定期更新的情报数据，判断新能源厂站安全风险。
- **智能分析：**使用AI等智能分析技术，综合流量、日志、情报数据，发现未知威胁、内部威胁

应用 - 自动处置

- **告警处置：**针对不同告警定义针对性的安全剧本实现安全告警的封堵、延迟响应、引流等操作；
- **封堵：**针对安全风险，实现IP访问的自动封堵；
- **加固：**针对安全风险，实现主机的主动加固。
- **更新：**针对病毒、密码登告警，自动升级病毒库、提醒升级软件版本等。

系统内置满足日常安全运维80%场景的处置剧本，对安全告警、安全加固、软件升级等业务进行自动处置。



应用 - 自主报告

综合无人安全值守系统运行的数据，自动生成各类报告，并定期报送。

应用 - 集控中心集中管控

通过天御网络安全运营平台，对所有无人值守系统及厂站安全设备进行集中管控

安全设备统一登录

安全策略统一下发

自动任务下发

远程设备配置

远程处置人工干预

整体风险可视化

04 方案价值

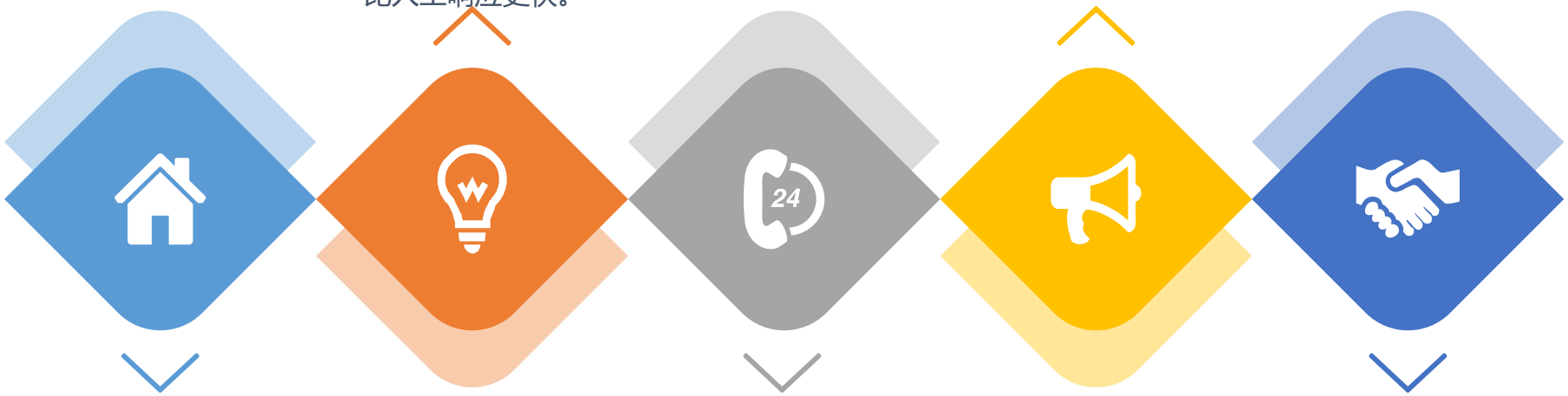
价值

减少人为错误

无人安全值守系统可以7×24小时不间断地监控网络安全，一旦检测到异常或攻击，能够立即响应，比人工响应更快。

实现远程运维

厂站出现特殊情况需要人员干预，可远程操作，避免长途劳碌奔波。



提升响应速度

自动化减少了人为操作的环节，从而降低了因操作失误导致安全事件的风险。

节省人工成本

厂站现场无人人员驻守，大部分问题由系统解决，降低了昂贵的人工成本。

掌控安全全局

通过无人值守对电站进行整体安全运营，再通过天御平台对集控厂站进行安全风险整体管控，达到掌控安全全局的目的。

感谢聆听！

同时请各位领导及专家就以下问题发表意见：

- 贵单位目前的网络安全防御现状如何？
- 贵单位是否已有平台进行安全设备集管及安全事件自动化响应处置？
- 其他问题