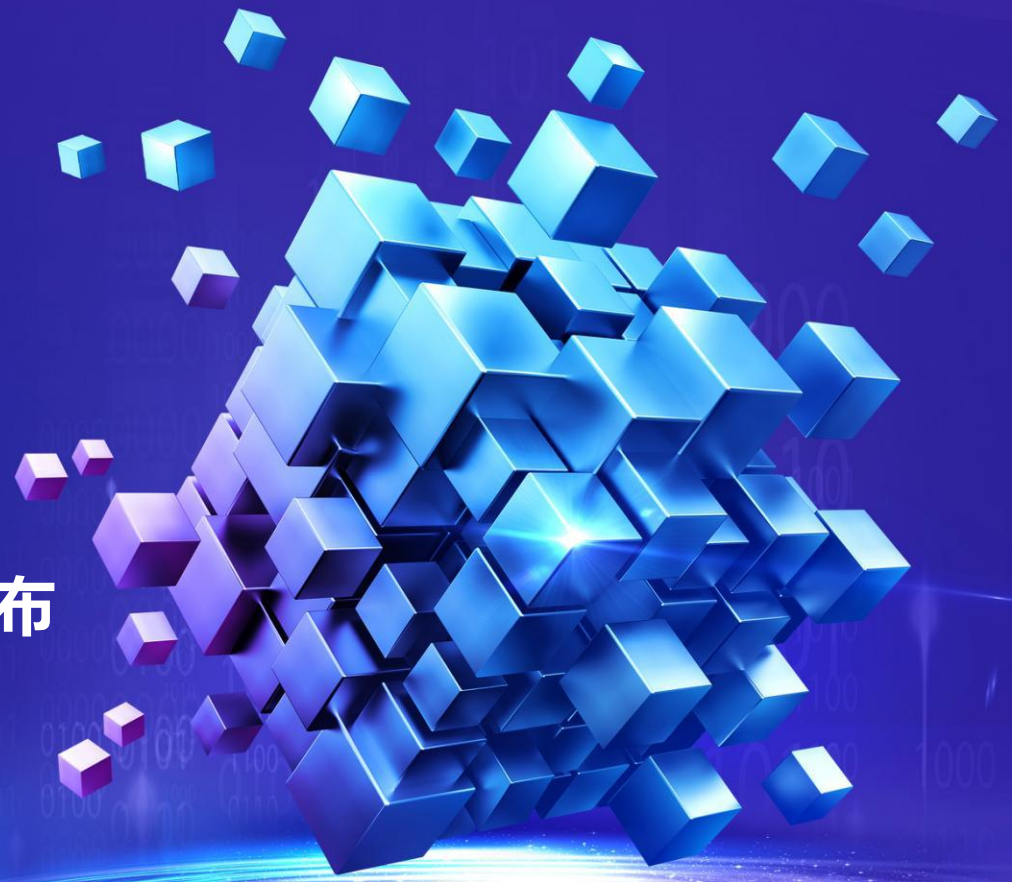
2021 WEST LAKE CYBERSECURITY CONFERENCE
西湖论剑·网络安全大会

2021 CYBERSECURITY : THE FOUNDATION OF DIGITAL REFORM

安联纵横·智维感知

——暨工业互联网安全态势感知技术与发布



演讲人：井柯
安恒信息工业互联网安全事业部副总经理

工业互联网助力实体经济和数字经济协同发展

1. 帮助工业企业互联网化转型

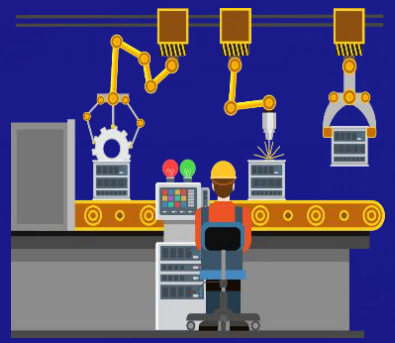
2. 为创新企业提供资源和市场

3. 助力城市

产业数字化 数字产业化

面向行业的
大供应链企业

工业化



信息化

面向领域的
新型互联网企业

新模式
新业态

其他增值服务

备品备件后服务创新

远程运维 | 故障预测 | 精益管理

系统互联 | 设备互联 | 产品互联 | 能力互联

工业互联网平台

工业知识和机理

MES | WMS | CPS | SCADA

工业现场 | 工业设备 | 设备工程师

大数据算法及模型

Openstack | Kubernetes | Hadoop

软件工程师 | 云设备 | 云中心

数字化理念引领企业战略、组织、流程、业务与交付模式的全面转型，**数字化转型**已成为企业生存发展之刚需。

新冠疫情让制造企业对数字化转型有了更加深刻的感受和更加迫切的需求。

工业互联网依赖设备网络化和软件智能化

工业智能化五大特征

互联 **数据** **集成** **创新** **转型**

- 工业软件
- 网络接口
- 网络化已成定势
- 复杂程度高

在工业智能化背景下，**网络安全**已经成为**功能安全**和**数据安全**的核心元素。

工业互联网建设需具备“安全基因”

超过 **80%** 涉及国计民生的关键基础设施依靠工业控制系统来实现自动化作业。

工业控制系统已是国家安全战略的重要组成部分，与生产安全息息相关。

从“事后诸葛”到“防患未然”

当我们面临着许多已知和未知的安全威胁，攻击途径日益多样，花样翻新的速度也越来越快，**高级持续性攻击**总是指向我们毫无准备的漏洞。

传统安全模式

特征库更新

恶意代码报告

特征分析

样本捕获

工业互联网安全模式

全面掌握
网络行为

追踪高风险
及异常流量

主动调整
安全策略

掌握网络
攻击特征

工业互联网态势感知解决方案

城市级/行业级安全监管

网络安全协调指挥体系
- 资产管理
- 信息通报
- 安全监测
- 态势感知
- 工作台
- 移动端
- 管理评价
- 检查督查
- 行业监督
- 应急指挥

网络安全协同防御体系
- 情报中心
- 信息共享
- 安全热点
- 专项行动
- 教育培训
- 应急演练

综合防控体系
- 关基保护
- 等级保护
- 态势感知
- 重大安保
- 情报侦查
- 攻防演练
- 安全监测
- 通报预警
- 侦察调查
- 行政执法
- 指挥调度

新业态专项监管体系
- 工业云安全
- 工业数据安全
- 工业平台安全
- 标识解析安全
- 工业APP安全
- 工控安全

全息档案体系
- 单位全息
- 资产全息
- 人员全息
- 攻击武器全息

资产普查体系
- 移动端填报
- 机器学习核验
- 抽查审查
- 考核评估

关保业务扩展
- 监管对象
- 挂图作战
- 空间图谱
- 追踪溯源

企业安全运营

管人
- 值班排班
- 日常TODO
- 交班日志
- 考核评价

管事
- 通知 预警
- 工单 通报
- 应急预案
- 处置闭环

管资产
- 资产准入
- 资产评估
- 资产档案
- 资产报表

管设备
- 运维监控
- 策略下发
- 配置管理
- 在线升级

资产与风险
- 资产管理
- 漏洞管理
- 基线管理
- 事件管理

安全分析
- 模型管理
- 指标管理
- 威胁管理
- 关联分析

态势感知
- 总体态势
- 运营态势
- 业务安全态势
- 资产风险态势

安全运营
- 应急响急
- 合规管理
- 知识库
- 安全评价

安全数据中台
- Modern SIEM
- 威胁情报
- 用户实体行为分析（UEBA）

安全业务中台
- 自动化办公引擎
- 绩效管理引擎
- workflow引擎
- 值班排班资源调度引擎

安全能力中台
- 安全编排自动化响应（SOAR）
- 识别能力
- 检测能力
- 防护能力
- 响应能力

工业网络空间测绘引擎
- 全网扫描
- 指纹识别
- 专项扫描
- 状态识别

工业威胁检测识别引擎
- 流量威胁检测
- 站点威胁检测
- 恶意文件检测
- 工业漏洞检测

工业云端安全监测引擎
- 漏洞云监测
- 事件云监测
- 0day预警
- 云端资产梳理

工业网络安全防御引擎
- 网络防御
- 数据防御
- 主机安全防御
- 业务应用防御

工业威胁情报管理引擎
- APT组织
- 恶意软件
- 僵尸网络
- 远控地址

工业网络攻击诱捕引擎
- 攻击检测
- 攻击隔离
- 攻击取证
- 攻击溯源

工业网站安全监测引擎
- 篡改
- 暗链 后门
- 可用性
- 敏感词

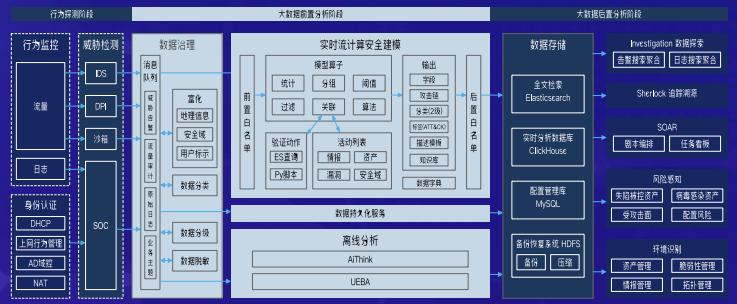
工业安全合规检查引擎
- 等保检查工具箱
- 应急处置工具箱
- IDC检查工具箱
- 工控检查工具箱

三大安全中台

从现场海量数据中实时识别有价值的信息，并将获得的信息通过**以平台为中心的协同决策**来挖掘潜在知识，指导安全决策与生产过程优化。

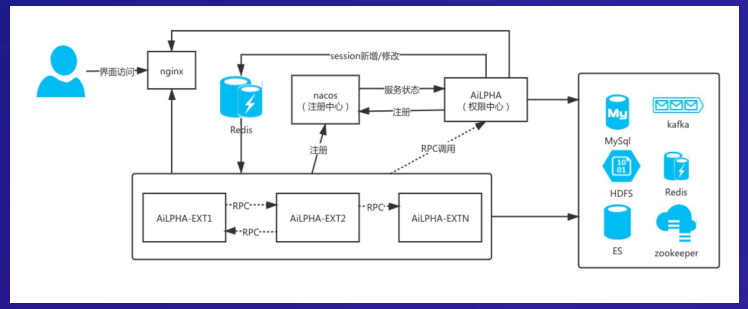
1. 安全数据中台

- 基于工业用户场景的模型管理
- 代码级模型粒度定义，方法多元化，参数模板化
- 专业而又易于理解的安全事件解释，集成攻击链、告警标签、处置建议、知识库



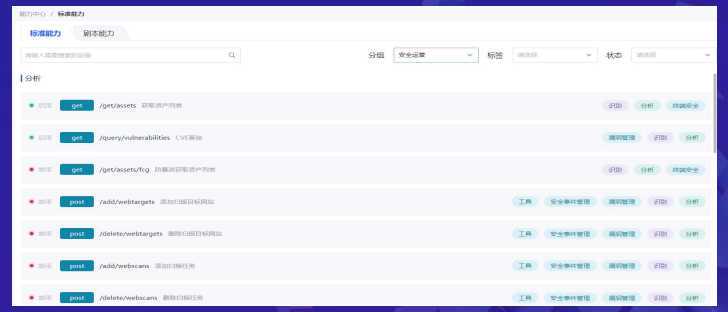
2. 安全业务中台

- 安全业务应用剥离解耦，快速定制、灵活开发
- 融合工业安全业务场景需求，突出安全重点
- 安全业务绩效管理定制
- 安全基线模版化



3. 安全能力中台

- 安全能力 API 化接入（标准接口），形成安全能力编排调度
- 跨厂商、多设备标准能力接入
- 提供统一的安全能力目录管理



五大核心安全分析模型

规则模型

根据安全分析的应用场景，从日志数据中筛选出安全事件，触发告警或进行后续高级安全分析。

1200+条规则

统计模型

从安全事件中，发现重要的统计型特征，通过阈值过滤，找出异常指标，可以发现如频繁暴力破解尝试等恶意行为。

50+统计场景

AI模型

根据历史数据，AI引擎持续构建并更新基线信息，自适应的发现异常和偏离，发现你不曾想象过的攻击来源及方式。

10个业务场景

关联模型

跨越多个设备来源及数据种类，从多个安全事件中检测行为模式，发现隐藏的高级威胁及安全风险，触发严重安全告警。

50+关联场景

情报模型

利用威胁情报增强网络安全威胁检测和应急处置能力，支持通过已知线索筛选安全日志，进行恶意IP、恶意域名、恶意文件识别等威胁分析。

3个情报库碰撞

另有电力、石化、生产制造、市政、交通等行业 **100+工控业务模型**

十大业务应用

实时监测
多源异构数据采集
及时识别安全威胁

态势感知
多维感知安全态势
威胁风险直观展示

信息通报
及时通报风险隐患
督促加强安全防护

安全处置
在线传达业务指令
及时同步处置情况

安全基线
采集设施资产信息
精准评估隐患范围

威胁情报
威胁情报集中管理
威胁情报关联分析

追踪溯源
安全事件溯源取证
黑客画像行为分析

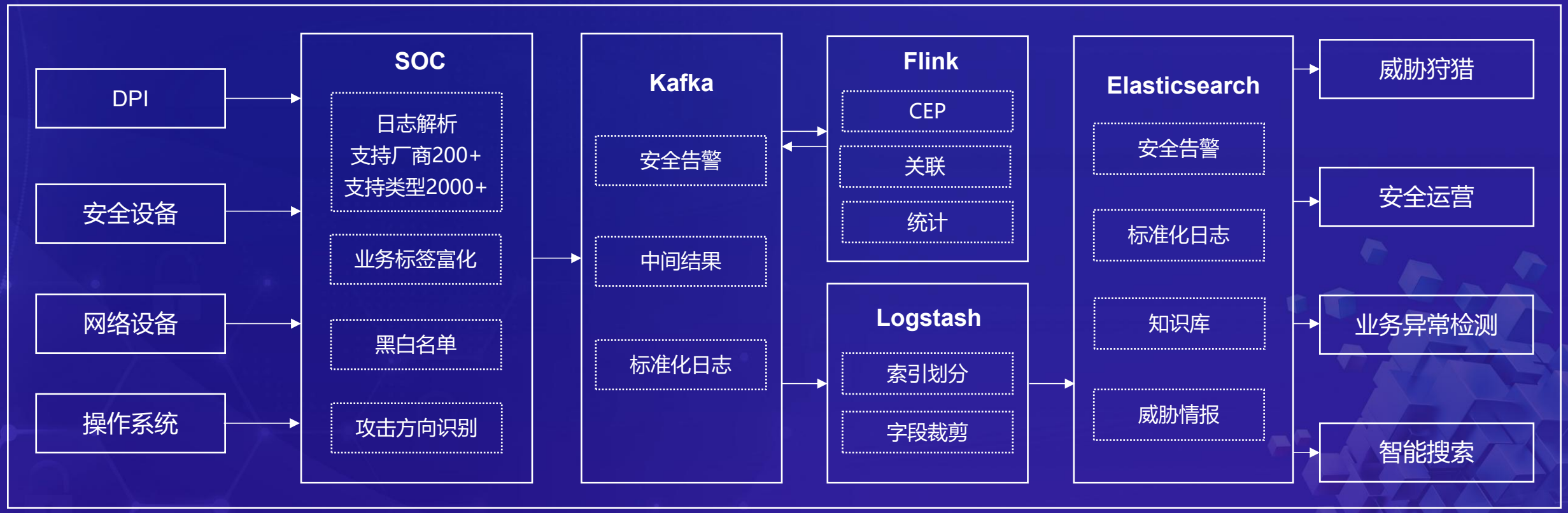
检查监督
汇总分析检查结果
形成历史检查数据

绩效管理
建立安全指标体系
科学评估工作成效

知识库
事件处置知识库
产品应用知识库

大数据技术架构

- 大数据实时流式分析计算引擎
- 高吞吐、低延迟、高容错
- 增强 Flink 流式 SQL 解析能力，支持 SQL 定义过滤器、时间窗口和 CEP 复杂事件模型



技术亮点一：全维度多场景数据采集

工业企业生产网

流量解析：支持 **40** 余种工控协议解析、超过 100 种 IT 协议解析还原

日志采集：支持 200+ 厂商，**3000+** 类型的日志解析

工业互联网平台

SaaS安全能力：支持云WAF、WEB漏扫、云EDR、云数据库审计等 **10** 余种SaaS安全能力数据接入

公网主动探测：探测互联网中暴露的工业控制系统及其安全漏洞，每秒 **60W** 并发，2小时可完成全球IPv4空间探测

公共互联网测绘

国家级平台：**支持**国家级工业互联网态势感知平台对接

第三方平台：支持威胁情报及第三方平台数据对接

系统对接

技术亮点二：工业控制场景用户行为分析 (ICS-UEBA)

针对工业控制系统行为，进行定性、定量研究，分析行为偏好与典型特征，从而判断**网络安全 (Security)** 与**业务安全 (Safety)** 异常。

实体识别
- 工控设备
- 工控系统
- 用户

分析研判
- 基线学习
- AI 分析

风险识别
- 安全事件识别
- 业务异常识别

数据源
- 关键过程参数
- 控制指令偏好
- 工控通信关系
- 网络通信行为
- 资产活动
- IT 流量解析
- 安全设备日志
- 应用日志
- ……

分析算法
- 深度学习：LSTM, RNN, CNN
- 异常检测：HMM, IsolationForest
- 关联分析：Apriori, FP-Growth
- 特征降维：PCA, t-SNE
- 聚类：K-Means, DB-Scan
- 分类：SVM, RandomForest, XGBoost
- UP/DOWN
- Weekly 周期性异常
- 潜伏性异常
- .....

异常识别
- 生产业务异常（关键参数异常变化）
- 控制器非正常时间重启
- 疑似工控设备嗅探
- 异常数据读取
- 异常数据写入
- 工控流量突变
- 工控设备下线
- 频繁密码尝试
- ……

技术亮点三：安全编排与自动化响应 (SOAR)

SOAR 使响应时间从小时甚至天降低到**分钟级别**，并将分析人员从耗时且重复的分析工作中解放出来，流程化完成事件管理，减少对人工的依赖，提高协作沟通效率。

核心能力

安全编排

- 多种数据源
- 五大分析模型
- 内置 API

安全自动化

- 构建自定义剧本
- AI 和机器学习分析
- 自动化响应

安全响应

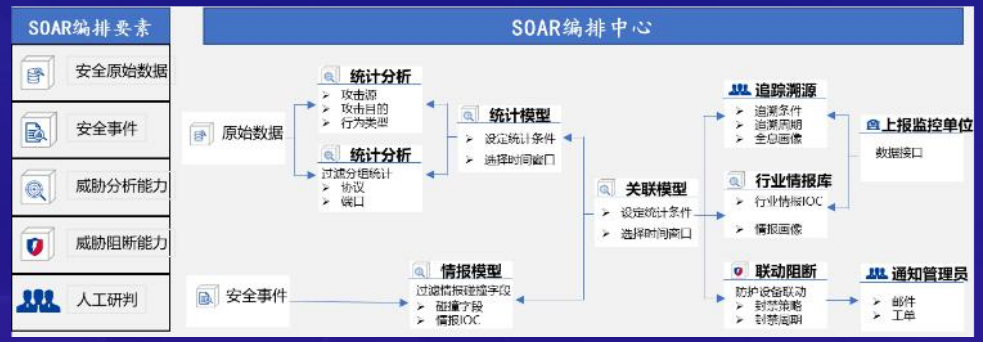
- 多种处置方式
- 单一视图管理

技术优势

- 图形拖拽式编排
- 数 10 种 APP 对接
- 近 200 种已对接动作
- 支持第三方设备/系统联动

客户收益

- 实时响应，最大程度降低损失
- 自定义安全响应流程
- 积累安全能力，总结安全成果
- 联通第三方系统，无限扩展可能



数据源

- 工控流量解析数据
- IT 流量解析数据
- 安全设备日志数据
- 应用日志数据
- 安全告警
- ……

分析组件

- 统计指标
- 统计模型
- 关联模型
- 情报模型
- 规则模型
- ……

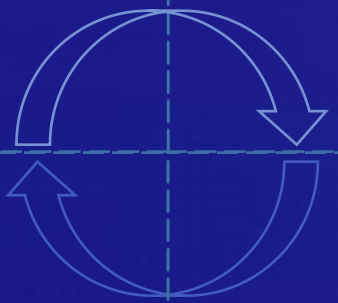
处置响应

- 防火墙阻断
- EDR 查杀
- 通报预警工单
- 人工核查
- ……

技术亮点四：智能化工控安全运营体系

以全面的工业安全引擎为基础，采用**闭环安全**模型体系，实现对资产、设备、人员、事件的**智能工业安全运营。**

PMPE 闭环安全模型



- 安全监控：实时监控、集中管理、数据分析
- 安全预警：安全评估、漏洞检测、态势分析
- 应急处置：人工处置、自动处置、通报预警
- 安全防护：区域隔离、行为审计、数据防护

智能安全运营管理

工业安全运营

- 管资产：资产准入、资产评估、资产档案、资产报表
- 管设备：运维监控、策略下发、配置管理、在线升级
- 管人：值班排班、日常TODO、交班日志、考核评价
- 管事：通知 预警、工单 通报、应急预案、处置闭环

多种工业安全监测防护引擎

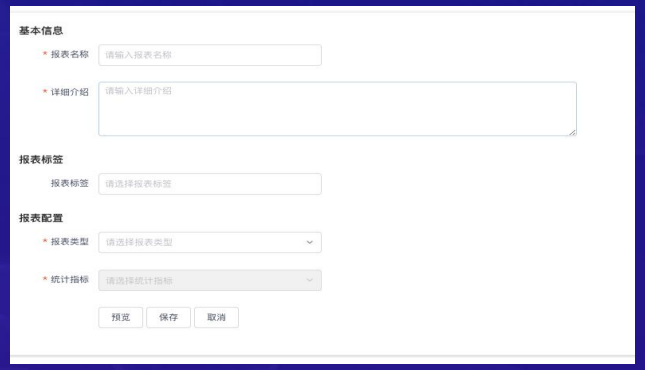
- 工业网络空间测绘引擎
- 工业威胁检测识别引擎
- 工业云端安全监测引擎
- 工业网络安全防御引擎
- 工业威胁情报管理引擎
- 工业网络攻击诱捕引擎
- 工业网站安全监测引擎
- 工业网络空间测绘引擎

技术亮点五：开放性的工业网络安全态势展现

平台预制全面态势感知能力，同时提供**个性化**态势感知视角；
支持指标、图表、拓扑、大屏等**多维度自定义可视化能力**，构建**开放性工控**态势感知能力；
可满足**不同行业、不同规模、不同形态**的工业应用场景。

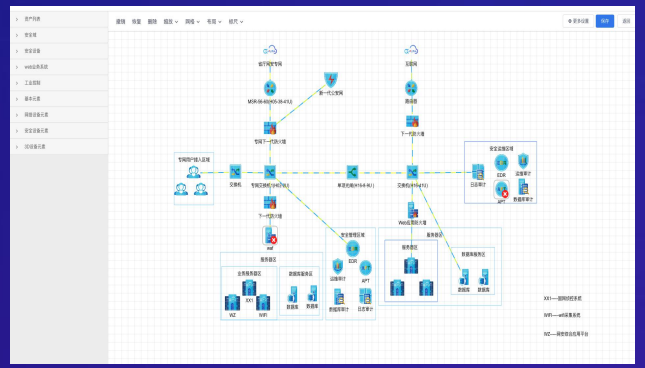
自定义图表管理

- 预制多种统计指标
- 采用简易语句添加自定义指标
- 支持各类统计图表样式
- 构建个性化仪表盘



业务全景

- 内置全面工控资产组件
- 内置各类IT资产组件
- 关联真实资产状态
- 支持分级分域拓扑构建



可视化自编排

- 预制多种可视化模版
- 拖拽式自编辑大屏
- 关联后台数据指标
- 支持组件扩展

安全共建，一站式、立体化安全才是破局之道

解决方案与安全服务	行业解决方案	安全服务	工业安全数据中心	一体化动态防御
高可用工业安全产品	工业网络安全风险评估平台 安全漏洞扫描平台	工业防火墙 工控主机卫士	工业安全监测审计平台	工业安全态势感知 工业安全管理平台	结构安全 本体安全 行为安全
安全的基础平台支撑	安全OS/安全芯片	工业化硬件	安全数据库	基因安全

- 推出“增强级”工业防火墙，适用于复杂应用场景
- 推出全新工控漏洞扫描平台

集中管控工控安全产品能力的工业安全管控平台

- 推出高度适配工控主机的主机防护软件
- 工业互联网安全态势感知平台

工业控制系统安全产品，已完成各行业突破，**覆盖关键领域**：

- **入围中国化工集团框采，成功牵手头部自动化厂商**

综合工控安全态势

工业资产安全运维

工业资产脆弱性态势

工业网络内部横向威胁

攻击者追踪溯源

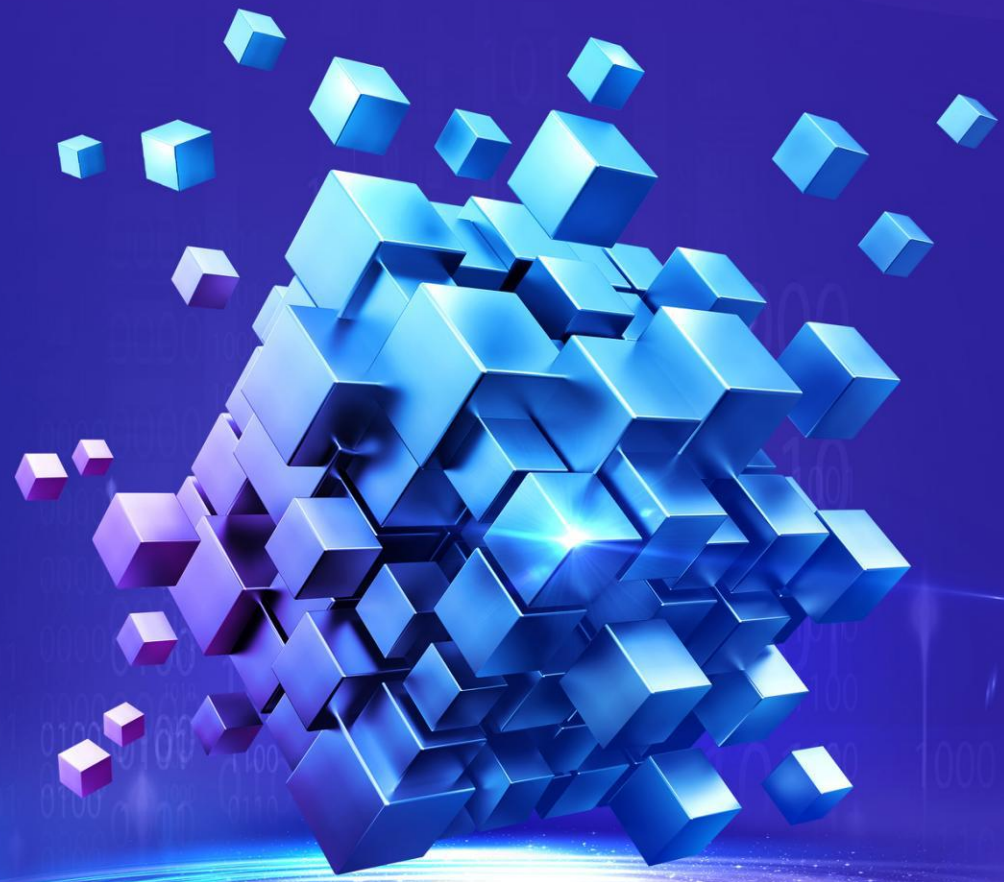
工控业务安全态势

2021 WEST LAKE CYBERSECURITY CONFERENCE
西湖论剑·网络安全大会

2021 CYBERSECURITY : THE FOUNDATION OF DIGITAL REFORM

谢谢您的观看指导!

西湖论剑·网络安全大会



扫码了解更多西湖论剑资讯

关注服务号获取最新西湖论剑动态