2022北京网络安全大会

2022 BEIJING CYBER SECURITY CONFERENCE

全球网络安全 倾听北京声音

工业互联网安全实验室

木链科技 崔旭中

木链 BOLEAN

浙江木链物联网科技有限公司专注于工业互联网安全领域，主营业务为工控安全产品开发和技术研究，并为客户提供专业的网络安全服务

核心产品：设立专注安全研究的星期五安全研究实验室，并拥有具备自主知识产权的“5+2”产品线，涵盖工业互联网安全运营平台、工业互联网安全实验室两大平台，以及防护类、监测类、管理类、检测类和攻防类5大纵深防御产品

业务范围：等级保护合规建设、安全服务、安全实验室、产学研合作

客户群体：军工、电力能源、钢铁冶金、轨道交通、市政水务、石油石化、智能制造、烟草等多个行业









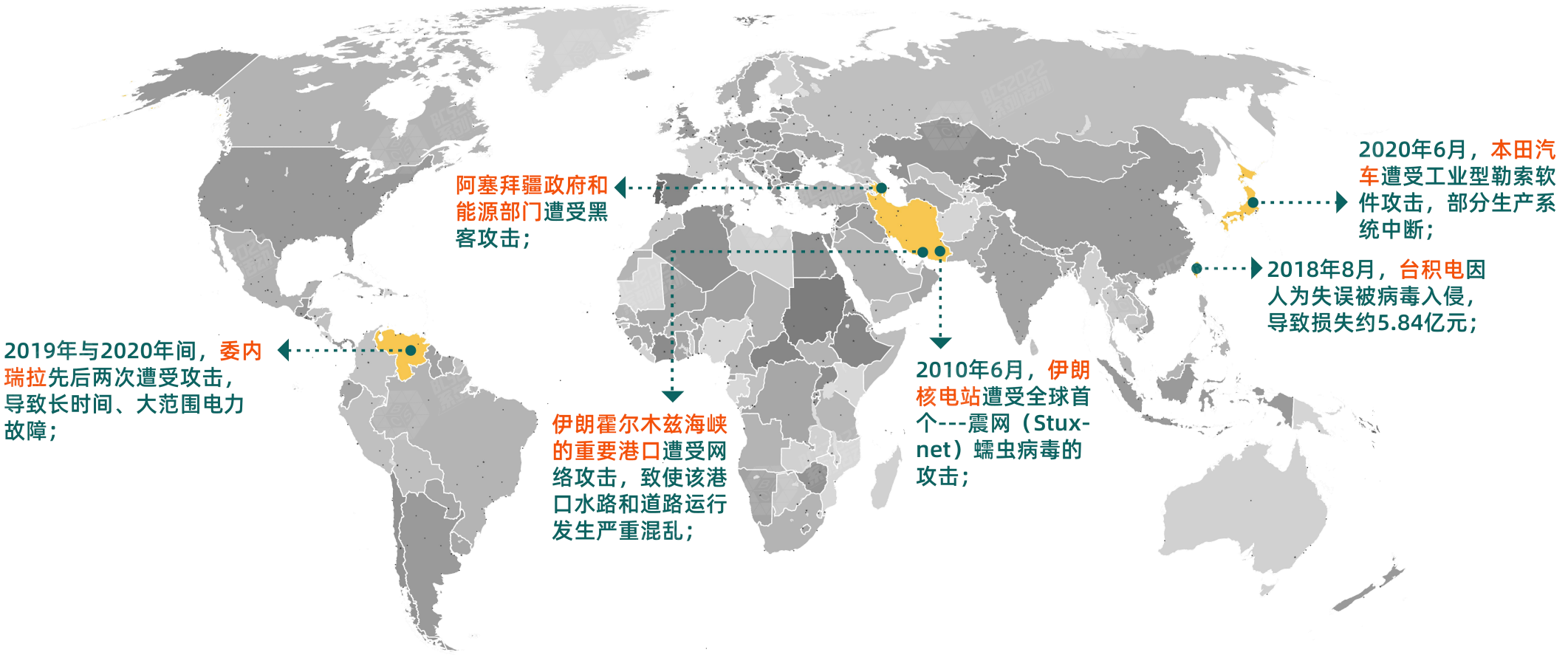



CONTENT

目录

安全事件

近年国际上工控网络安全事件频发，网络空间安全斗争日趋尖锐和复杂，关键基础设施、重要数据和个人隐私都面临着严重的威胁和风险。**网络空间安全问题，涉及公共秩序的构建和产业健康发展。**



政策驱动，人才缺口

国家战略、法律法规等级保护、护网行动

驱动因素：政策法规、防范未知的安全问题

- 网络安全的本质在对抗，对抗的本质在攻防两端能力的较量。要以技术对技术，以技术管技术，做到魔高一尺、道高一丈 ----节选自4·19讲话
- 从**攻击者视角**分析问题，以防御者视角解决问题，用**实战演练检验效果**

建设需求：人才团队、技术积累、安全体系

- 网络安全人才的需求增长到140万，高校培养的网络安全专业人才仅3万余人
- 立足业界需求，“**理论体系-学术成果-工具产品-事件案例-攻防实践**”知识链条牵引下，立足业界需求，依托科研项目，聚焦核心需求

《关键信息基础设施安全保护条例》

第二章 支持与保障 第十四条

能源、电信、交通等行业应当为关键信息基础设施网络安全事件应急处置与网络功能恢复提供电力供应、网络通信、交通运输等方面的重点保障和支持

第四章 运营者安全保护 第二十四条

（二）定期对从业人员进行网络安全教育、技术培训和技能考核

（四）制定网络安全事件应急预案并定期进行演练

第四章 运营者安全保护 第二十七条

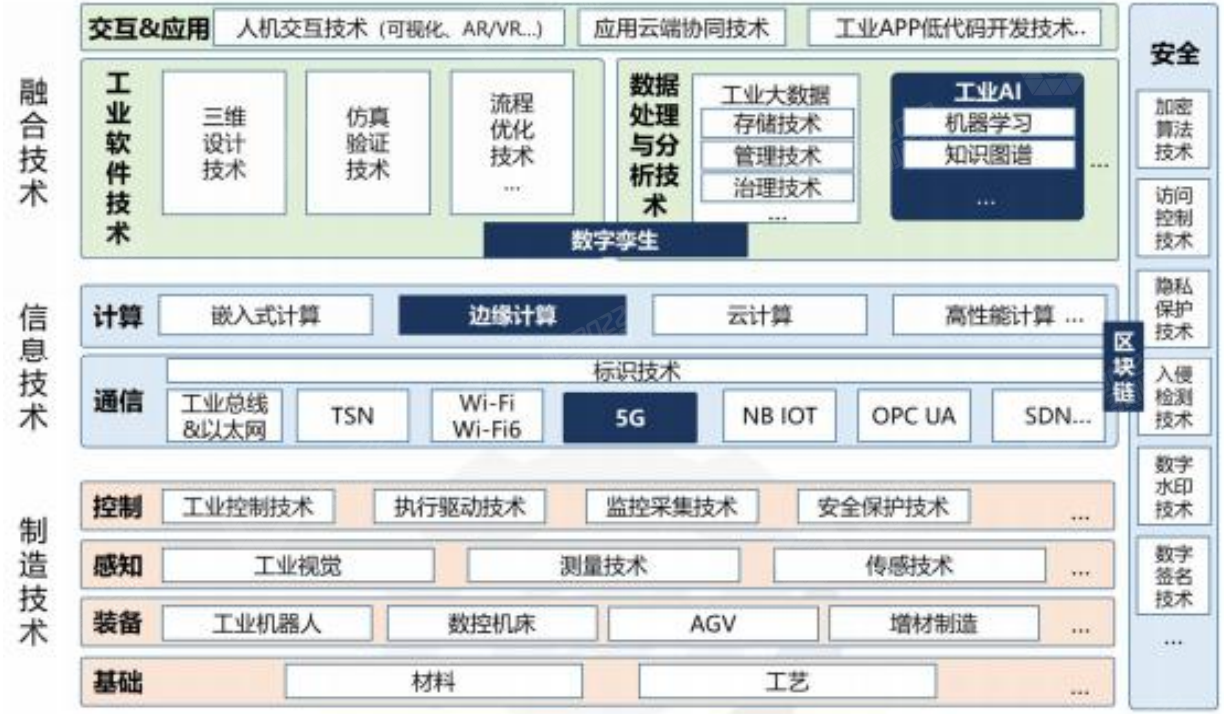
运营者应当组织从业人员网络安全教育培训，每人每年教育培训时长不得少于1个工作日，关键岗位专业技术人员每人每年教育培训时长不得少于3个工作日

产业发展进程

- 制造技术支撑构建了工业互联网的物理系统
- 信息技术勾勒了工业互联网的数字空间
- 融合技术驱动了工业互联网物理系统与数字空间的全面互联与深度协同

工业化——信息化——数字化

数字化，是用数据科学整合**制造科学**和**管理科学**的过程。



安全技术，是产业进程**健康发展**的必要保障。

用户关注

工业企业：缺乏信息安全管理经验

安全策略防护原理、防护效果如何不可知，是否会对生产环境产品影响无法有效验证

- 安全知识
- 对生产影响

高等院校：理论与实践匹配度低

安全教育侧重于理论，网络安全实验的场景太少，不能建立起完整的实践课程

- 课程体系
- 工控安全实验

科研单位：技术创新缺乏验证平台

内部考核局限于书面方式，缺乏实战场景，技术研究创新缺乏测试、验证平台

- 攻防演练
- 安全竞赛
- 测试验证

安全实验室解决方案

致力成为提高工业生产与信息系统安全性，稳定性的综合实验平台。
同时也是支撑网络空间安全技术验证、网络武器试验、攻防对抗演练和网络风险评估的重要研究平台。

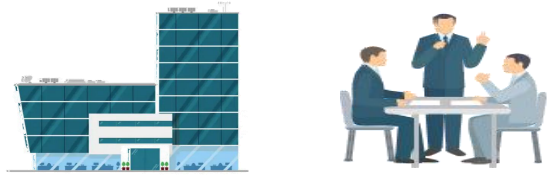
安全能力

- 场景仿真
- 教学培训
- 攻防演练
- 安全竞赛
- 漏洞检测
- 产品测试
- 态势分析
- 产学研合作
- ……

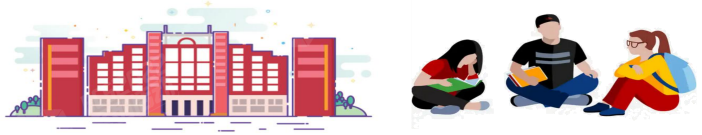
工控安全实验室

- 仿真靶场
- 实训平台
- 研究载体

企业安全部门

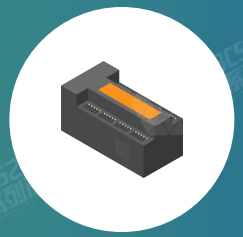


高校师生



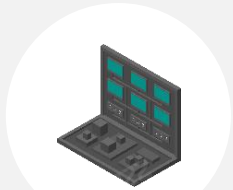
科研单位研究员

安全实验室组成



生产仿真系统

采用与行业相关的工控设备及组态软件，模拟各行业工业环境及工艺流程



工控网络安全靶场平台

通过虚拟化、虚实结合组网等技术，低成本、高效率的仿真出接近真实的工控网络环境，为企业安全建设赋能

攻击防御系统

配套自动化攻击平台及工控环境中涉及的各类防护套件，真实还原工控环境攻防场景

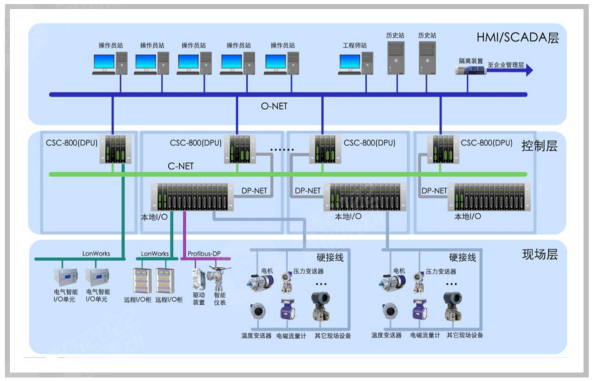
效果展示系统

以物理仿真沙盘、数字沙盘、数据驾驶舱等多种方式展示工控安全实验室中的各类数据

高级安全系统

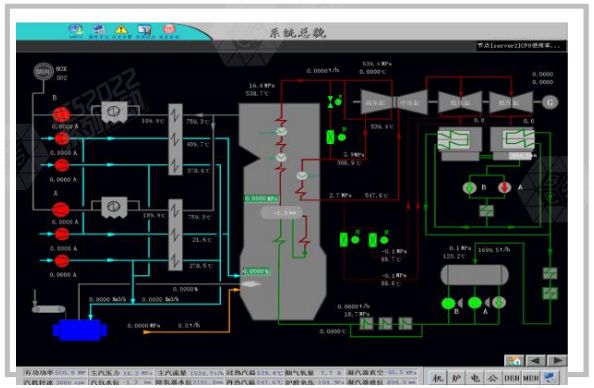
蜜罐、漏洞挖掘、数据安全互联网关等高级工具，帮助用户进行深入的网络安全研究

生产仿真系统



控制系统仿真

选用行业主流的控制、仿真设备模拟用户真实业务结构



生产工艺仿真

采用行业相关的组态软件模拟相关生产工艺

构建原则

- **主流设备选型**：选用行业中的主流控制设备和品牌。
- **最简化原则**：针对已经选型的控制系统，应构建其最简化的结构，包括基本的输入输出模块、基本的上位机组态及数据服务器。
- **模拟应用最真实原则**：对于实际的配置内容与客户工业控制系统现场应用要尽可能保持一致。

模拟仿真光伏发电工艺流程

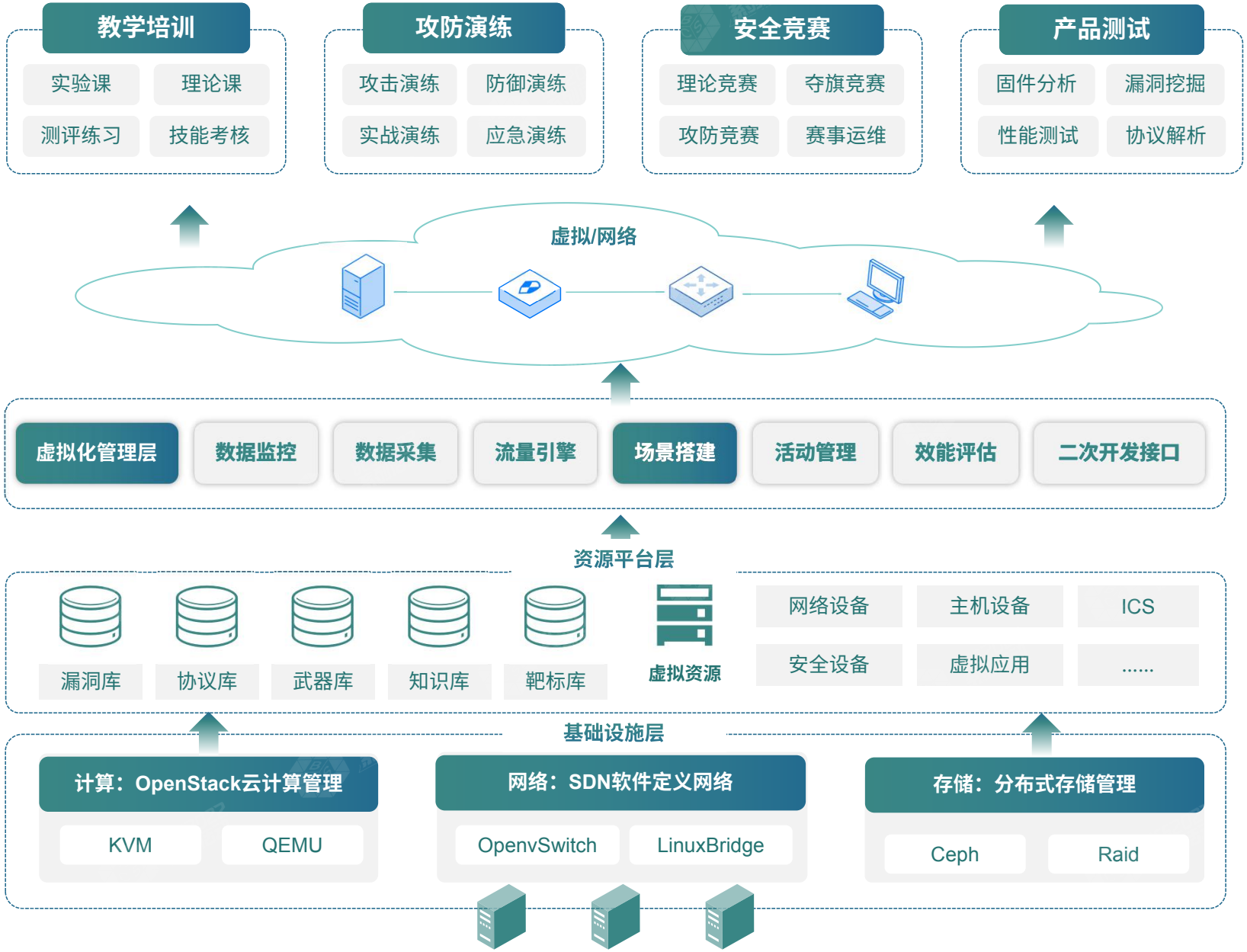
仿真自动控制系统壁挂板效果图

靶场平台架构说明

靶场物理节点

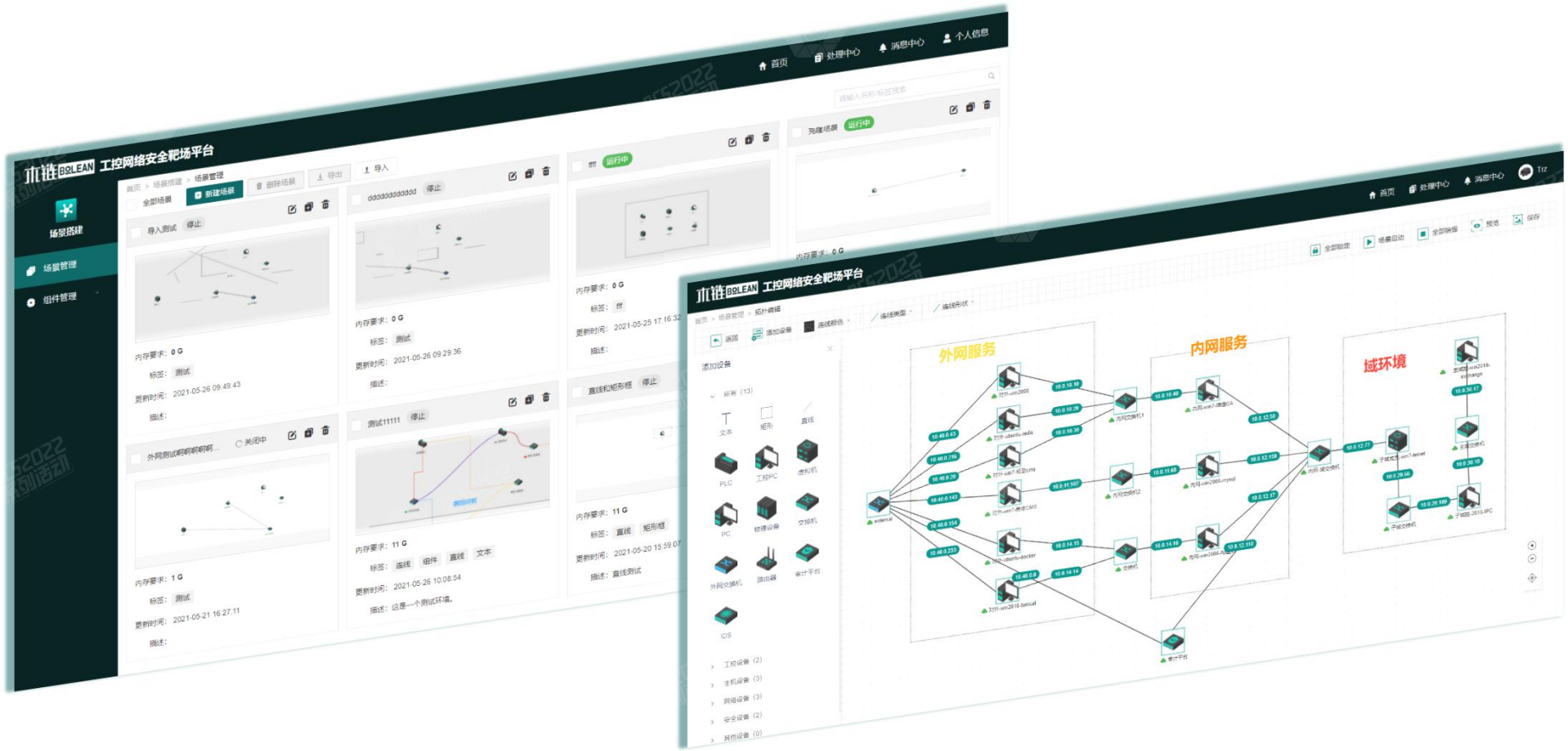
承载靶场应用平台及各类虚拟化软件

CPU	2*12核
内存	256G
硬盘	4*2T
承载能力	模拟60个虚拟资源
数量	3台



场景管理

场景的搭建和管理是靶场平台的核心功能，是实验室提供工业互联网安全应用服务的基础。



场景管理　教学培训　攻防演练　安全竞赛　产品测试

教学培训

教学培训模块依托于工控网络安全靶场提供的虚拟资源池，针对高校工控安全人才培养和企业用户的工控安全培训教育需求，构建教育培训系统

学员/受训人员　　教师/团队管理人员　　平台管理员

理论课程

- 信息安全基础
- 工控基础知识
- 工控网络基础
- 法规政策解读
- 工控安全基础
- 行业解决方案
- 安全产品原理
- 工控攻防技术
- 工控漏洞解析
- 安全管理体系
- 网络安全意识
- 支持课程定制

实验课程（实战）

- 内网渗透实验
  - 永恒之蓝勒索病毒攻击
  - 钓鱼攻击
  - 水坑攻击
- 漏洞复现实验
  - 永恒之蓝漏洞利用
  - Docker API未授权
  - CVE-2019-0708远程桌面代码执行
  - ……
- 支持场景定制

练习考试

- 测评练习
- 在线考试
- 教学统计

教学管理：学员管理 | 班级管理 | 课程管理 | 试卷管理 | 考题管理 | 系统设置

靶场镜像：Windows xp/7/8/10/11 | Linux Redhat/Centos/Ubuntu | Windows Server 2000/2003/2008/2012/2016 | 工业设备 PLC/SCADA/DCS | 自定义镜像

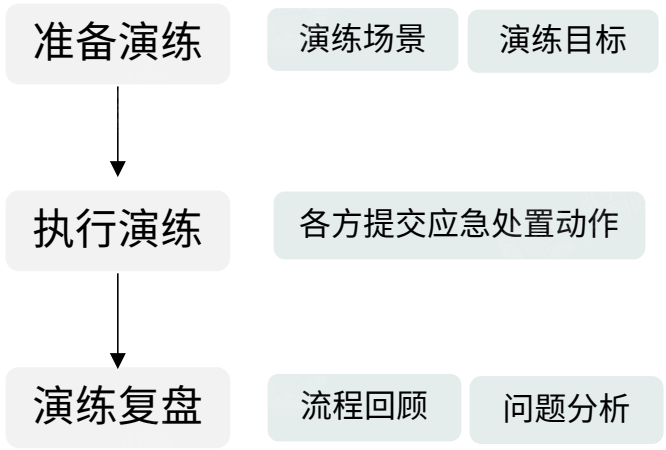
攻防演练

借助靶场平台提供的场景构建模块，可迅速搭建起高仿真的靶场环境，开展攻防技术的演练，通过逼真的环境演练，使受训人员认识网络安全技术的深层次问题，并通过实战演习追踪前沿网络安全技术，不断开阔思路和眼界，提升专业技能水平

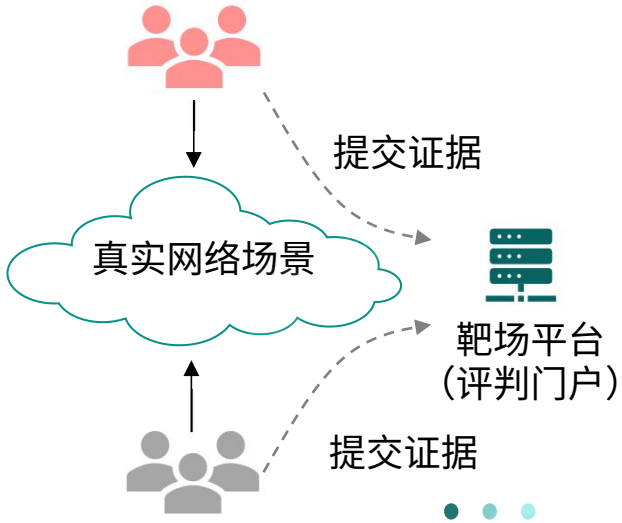
常规演练

- 网络攻击演练
- 网络防御演练
- 红蓝对抗演练
- 网络混战演练
- 技能鉴定

应急演练



HVV演练



安全竞赛

夺旗竞赛　攻防竞赛　理论竞赛

攻防工具　可视化展示　赛事定制

理论竞赛

支持选择题、填空题、判断题、简答题（需人工参与判定）夺旗题与实操题等6种不同形式的题目，方便开展各类考核活动

夺旗竞赛

在一系列的靶标中预留旗标（FLAG）参赛人员通过网络安全相关知识获取到旗标后得分

攻防竞赛

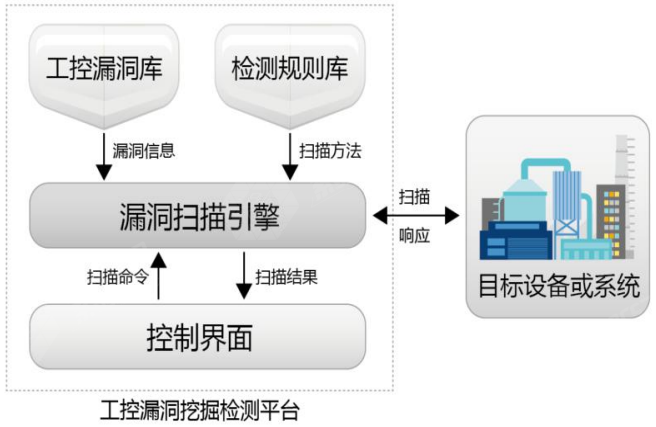
每个参赛队伍具备相同的网络环境和服务通过保护自己的服务（防守），以及攻击其他队伍的服务（进攻）得分

产品测试

服务器　　工控设备　　安全设备　　PC终端　　物联网设备

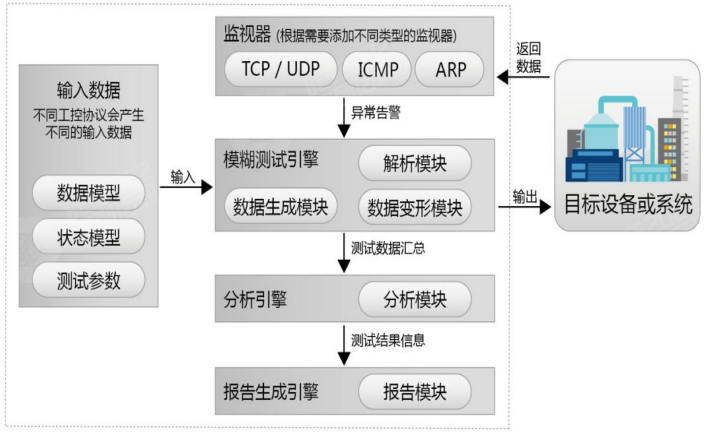
安全检测内容

固件代码安全性检测
基于工控漏洞库的已知漏洞检测
风暴压力测试
针对通用漏洞进行针对性攻击测试
基于工控协议的语法模糊测试
基于工控协议的智能模糊测试
用户自定义测试



工控漏洞挖掘检测平台

基于工控安全漏洞库的已知漏洞检测



工控漏洞挖掘检测平台

基于工业控制协议的模糊测试挖掘未知漏洞

漏洞扫描

工控漏洞扫描系统基于网络的漏洞分析、评估和综合管理系统，**融合了已有的漏洞扫描产品**和**工业控制系统漏洞研究成果**。目标是为SCADA、DCS等工业控制系统提供完善的全方位的漏洞检测，发现潜在的漏洞和缺陷

■ 离线扫描

- 工控产品提供商和集成商的测试环境、实验环境
- 工控系统的模拟环境、演示环境

■ 现场扫描

- 上线前或试运行阶段的工控系统
- 上线后生产间歇期的工控系统

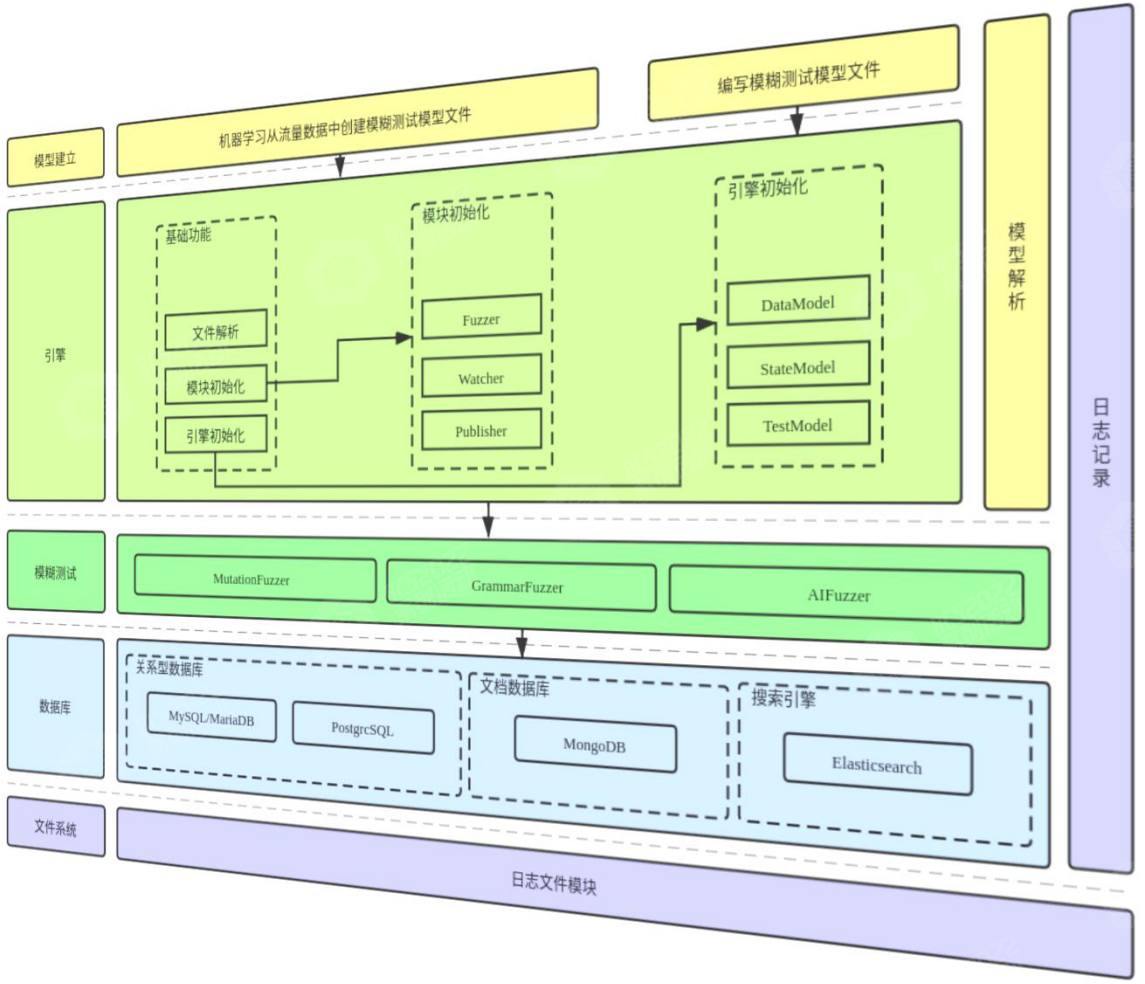
漏洞扫描任务
弱口令扫描任务
网站扫描任务
无线扫描任务
工控扫描任务
立即评估任务
定时评估任务
周期评估任务

主机存活扫描
端口扫描
性能参数
口令猜测
授权扫描
数据库参数

漏洞挖掘

木链科技漏洞挖掘系统，针对工控网络自身脆弱性和通信协议的安全性，主要围绕工控网络中可能存在的各类工控系统、设备、协议等方面的未知安全漏洞，开展有效的分析和研究，对如何防御这些安全威胁提供指导作用。

- 自启发式变异算法，高效发现工控漏洞
- 一键模糊测试全程自动化处理
- 可扩展更多工业协议
- 自学习能力，不断丰富算法库和异常数据特征库

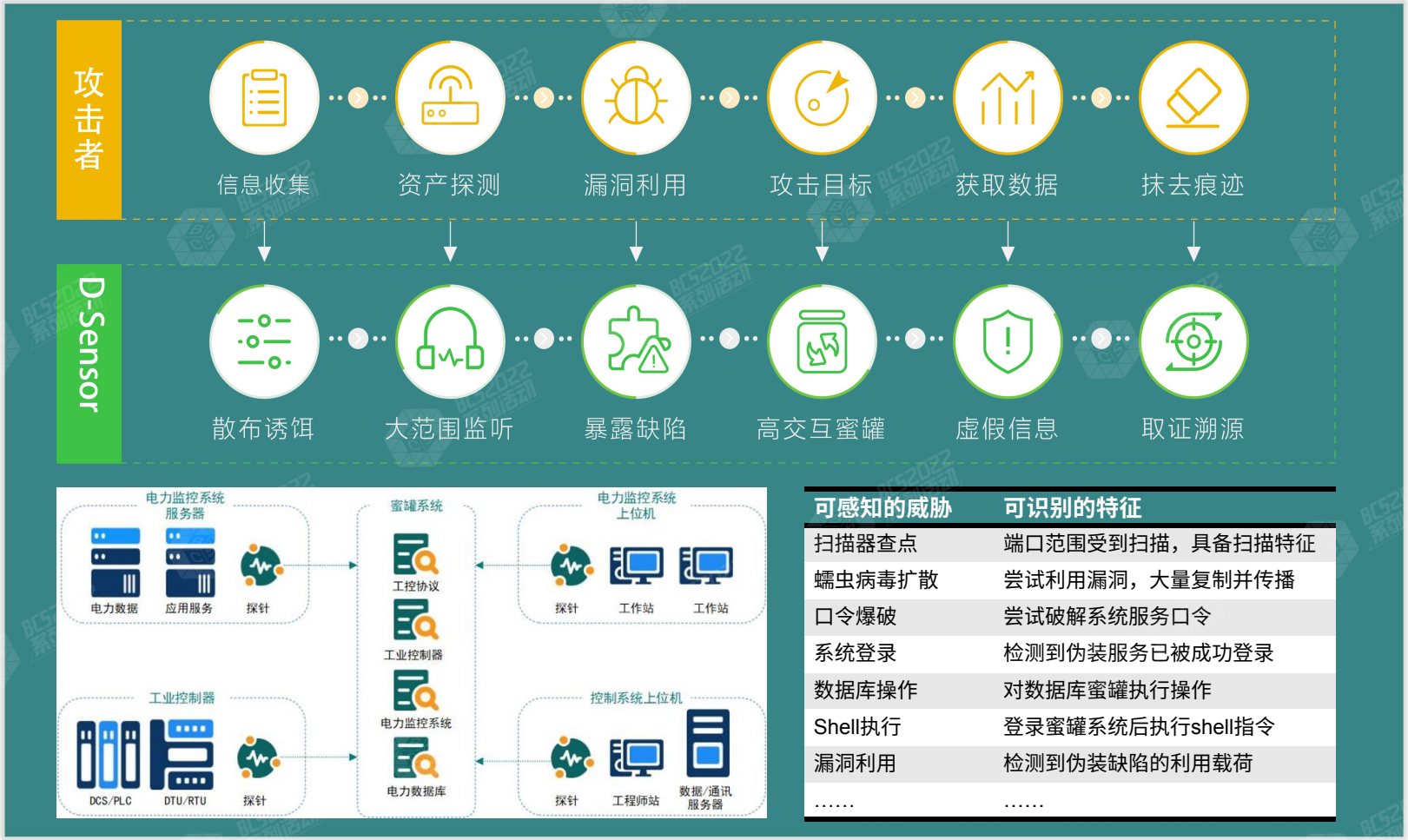


工控网络攻击诱捕

工控蜜罐系统

工控蜜罐系统是一种情报收集系统

- 通过搭建一套虚拟或物理工控系统，连接到工控系统网络，通过主动暴露缺陷或漏洞的方式，引诱黑客前来攻击。
- 蜜罐系统能够有效帮助攻击研究和漏洞研究、加固安全防御体系，减小真实工业系统的安全风险。

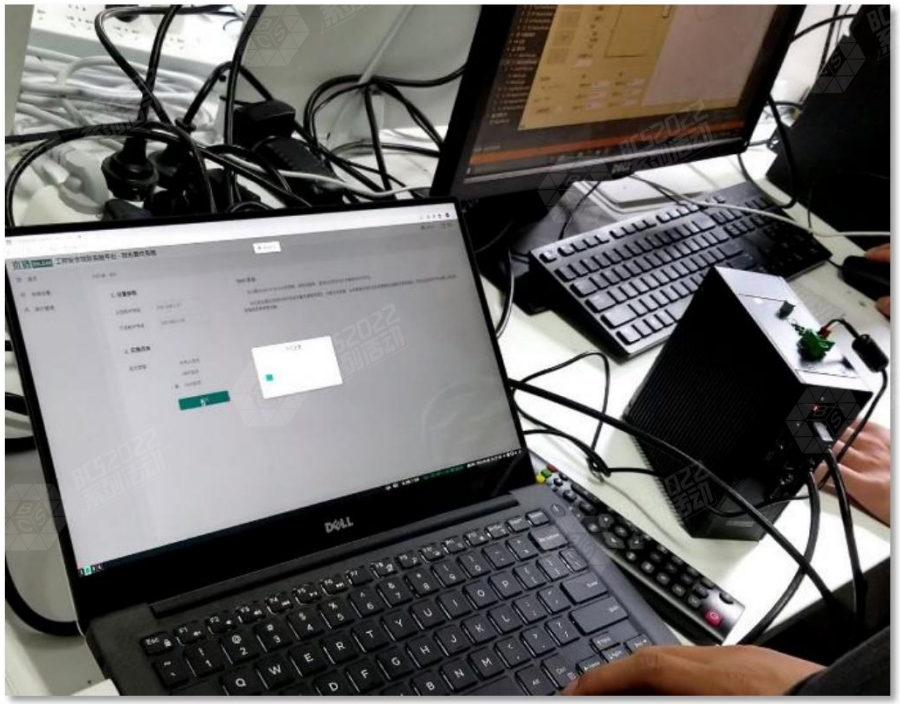


可感知的威胁	可识别的特征
扫描器查点	端口范围受到扫描，具备扫描特征
蠕虫病毒扩散	尝试利用漏洞，大量复制并传播
口令爆破	尝试破解系统服务口令
系统登录	检测到伪装服务已被成功登录
数据库操作	对数据库蜜罐执行操作
Shell执行	登录蜜罐系统后执行shell指令
漏洞利用	检测到伪装缺陷的利用载荷
……	……

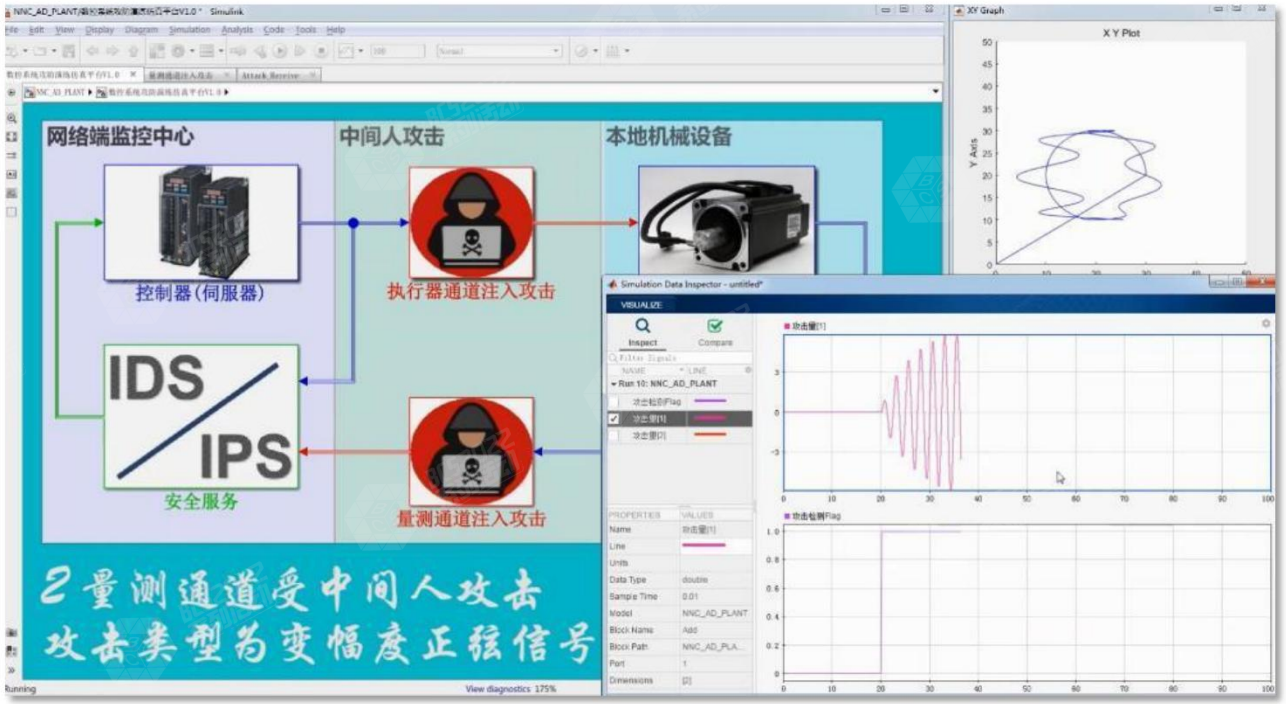
自动化攻击套件

内置多种自动化攻击手段，包括网络扫描，口令爆破，中间人攻击、恶意代码、泛洪攻击、DoS攻击、ARP攻击等等，支持攻击方式的定制化，支持在各类攻击方式基础上进行攻击参数自定义。

意义：通过自动化攻击，验证安全防护方案和成果，以提升效率。



客户现场进行工控安全攻防演练，操作攻击套件界面



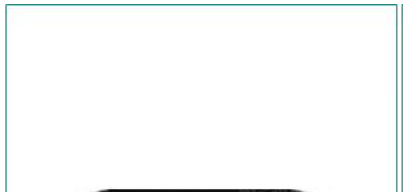
定制化攻击套件能够实现针对客户平台的攻击，干扰系统正常工作

安全防护套件

安全防护套件包括工控网络中必需的各类软硬件工控安全设备。

其中安全防御系统是指能够主动防御攻击行为、异常行为的设备集合，如工控安全防火墙、主机卫士、网闸设备等。

安全监测系统以安全审计、监测、管理为主，如工控审计平台、综合管理平台，用于监测当前工控仿真系统的安全情况。



工控审计平台

全局统筹
异常告警
事后溯源

主机卫士

纯软件产品
工控主机一键加固
保护工业环境主机安全

工控防火墙

边界防护
区域隔离
重点设备保护

工业网闸

边界隔离
“2+1”双主机代理
物理摆渡

效果展示系统

工控安全防护监测

实时监测安全实验室相应安全产品的运行状态，包括捕获到的攻击信息，防御情况等

靶场效能评估

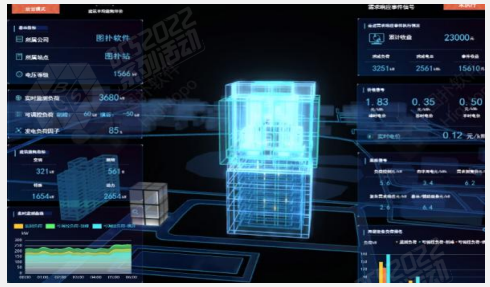
集中展示靶场平台平台自身性能情况，涉及设备运行状态、演练任务、用户情况、场景状态等

业务场景监测

监测靶场虚拟场景中各组件状态，实时同步各组件受攻击的情况及对威胁情报的标识解析

- 攻击信息
- 控制器IO信息
- 运行状态
- 演练计划排期
- 防护信息
- 威胁情报信息
- 系统事件
- 网络流量信息

物理沙盘



电子沙盘

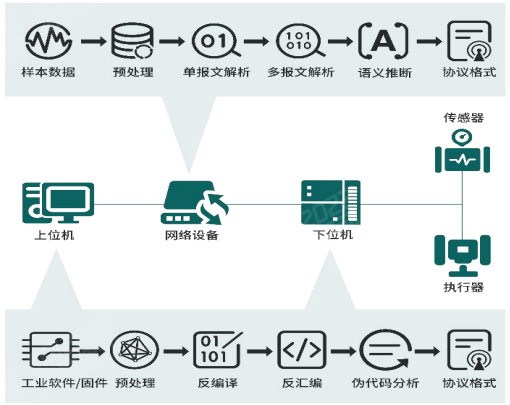
工业教仪

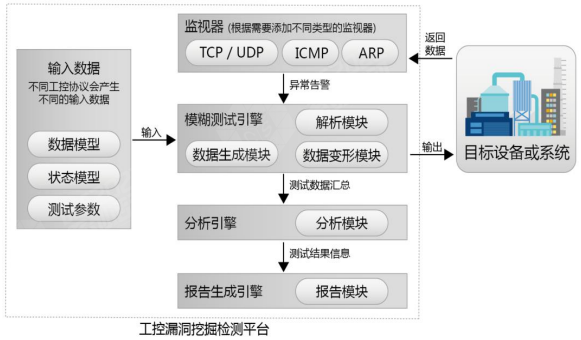
安全生态

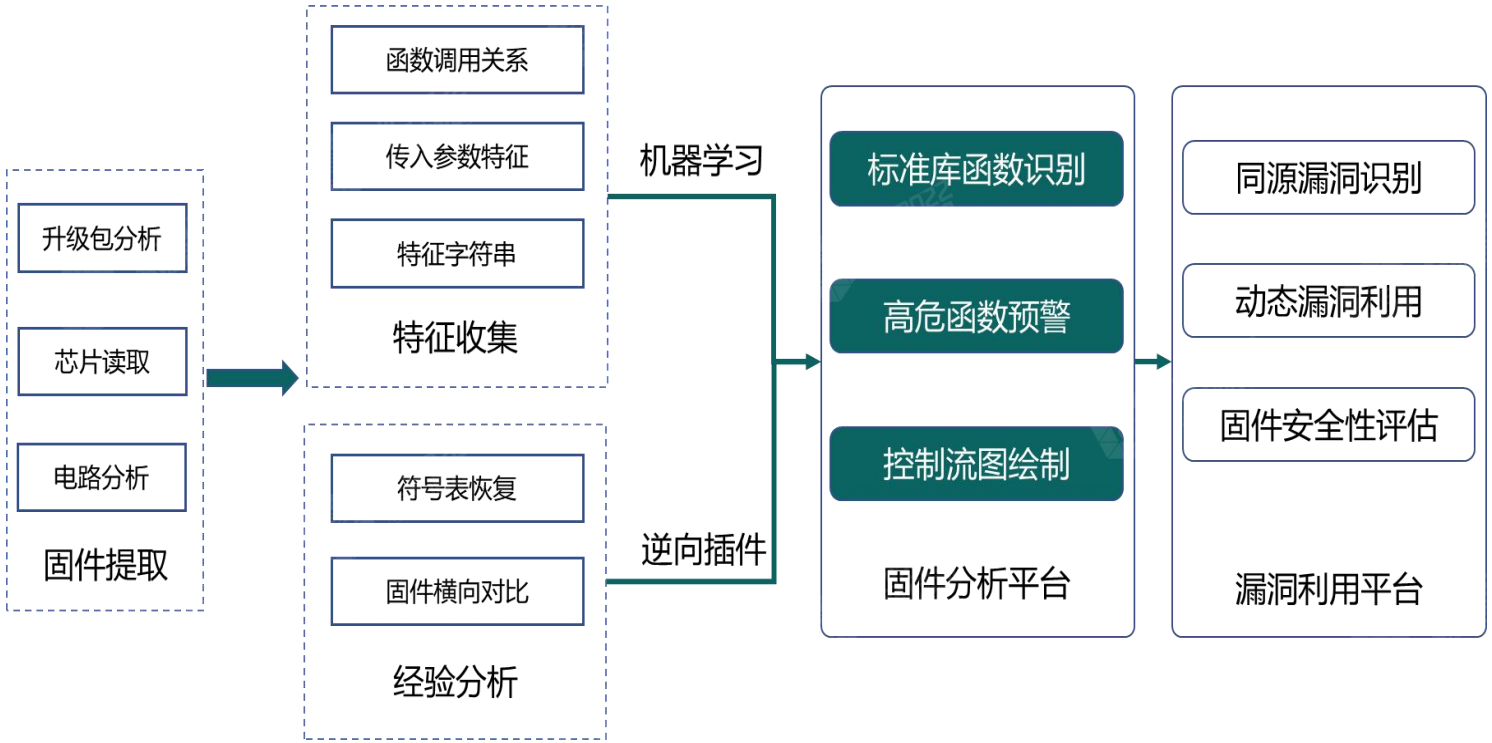
结合BoleanGuard®系列丰富的产品线，打造木链工控网络安全生态，为工业互联网安全实验室持续赋能

优势

深入的技术研究手段







木链工业互联网安全实验室一方面为企业的创新研究提供了专业的实验田和验证平台，另一方面也融入了木链的固件分析、协议解析能力以及漏洞挖掘、测试体系，能够帮助用户对工控系统进行更深度的研究分析

优势

科研合作

坚持“技术驱动，数据赋能”的产品理念与“协同创新”的产学研合作机制，与某省电力科学研究院、浙江大学、上海交通大学等众多科研院所、高等院校达成深度合作。

2018年12月，获得中国工程院院士、浙江大学教授——陈纯院士技术指导。

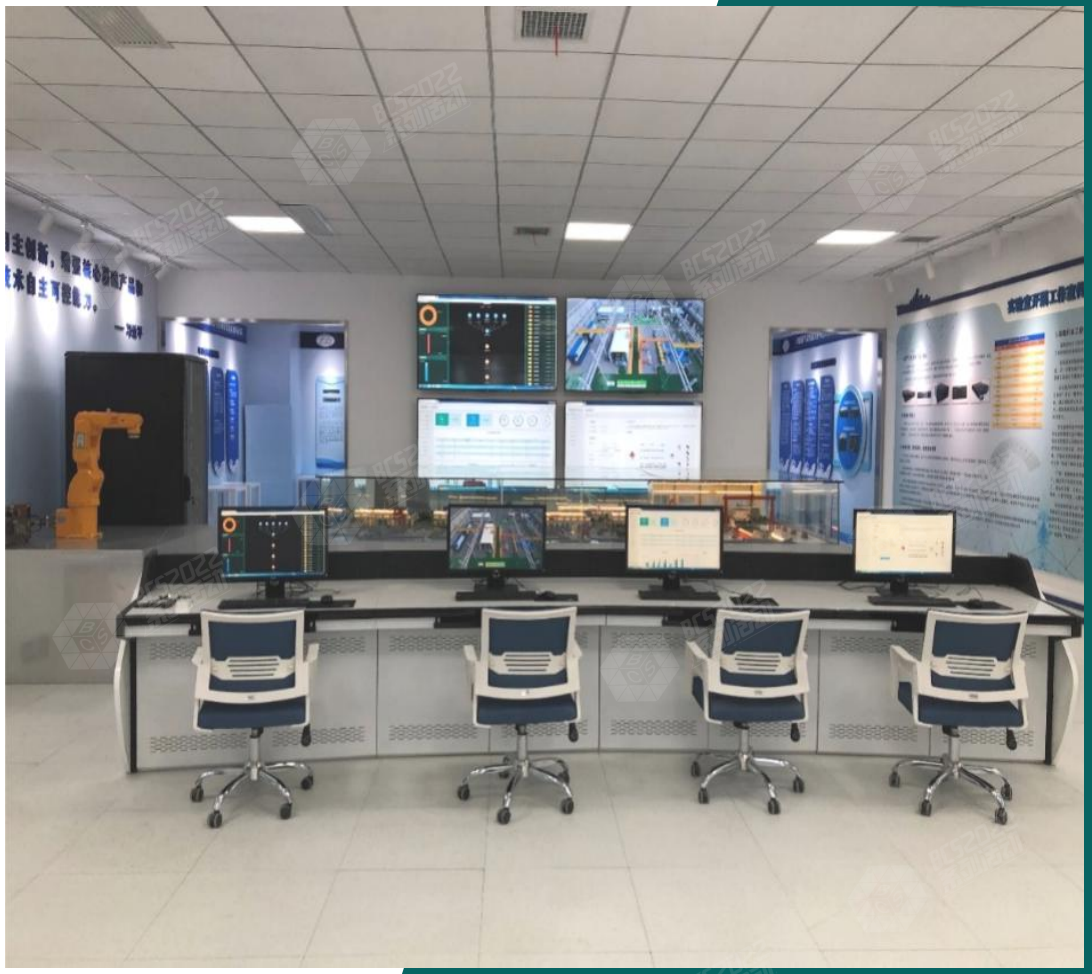
2019年1月，木链与某省电科院签订联合开发协议，联合开发电力行业站控层工控安全审计平台。

2019年1月，木链承接上海交通大学搭建工控系统攻防演示平台项目，并开展攻防演练培训，成功验收，双方后续将共同探索工控安全人才培养体系。

船舶制造实验室

客户需求

- 工业现场的仿真：需要将各类可动部件与静态模型相结合，利用PLC设备和微型模拟焊机、切割机、打磨机、喷涂机、温度传感器、湿度传感器、灯带、小车等部件进行联动
- 组态定制化：需要基于造船系统真实的架构，定制3D效果，与各类传感器、执行器等设备的数据进行联动，能够实时展示现场的状态。在现场出现异常情况（如温度过高）时，组态软件将能够通过组件的颜色变化展示现场情况



解决方案

- 通过建造仿真造船行业真实情况的模型，将各类可动部件、小车、灯带等其他效果部件，统一部署在模型上，这样能够直观地展示造船真实场景，同时能够有效展示工业控制系统正常运行的情况，以及受到攻击后的异常运行情况
- 参考造船厂3D架构图设计并制作组态软件界面，将各类传感器数据合理地对接到图片中不同的位置，提升实时展示效果

电力科研实验室

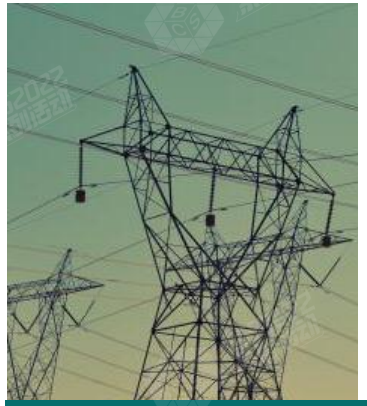
客户需求

- 建设一套集人才培养、技术研究和安全体系建设于一体的平台，用于企业内部人才技能提升、安全攻防演练及相应验证测试，提升整个企业的安全建设能力

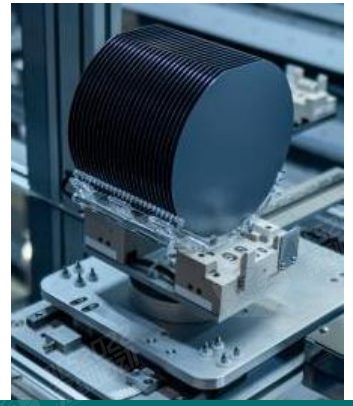
解决方案

- 教学培训：平台内置大量课程，形成了完整的课程体系，满足课堂教学和课外自学的需求，课程配备有实操环境，学习的同时动手操作，最大的保证学习效果
- 攻防演练：通过虚拟场景化的方式以及虚实结合技术架构，建立一个高度仿真的网络安全攻防实战演练环境，实现内部信息安全人才培养、攻防演练技术研究和漏洞研究测试等不同方向的工控安全建设
- 产品测试：靶场测试验证系统对电力行业设备的网络性能测试与安全性测试。通过专业的测试与验证系统，排除设备潜在的系统隐患，从而在根源上提升工控系统的安全性

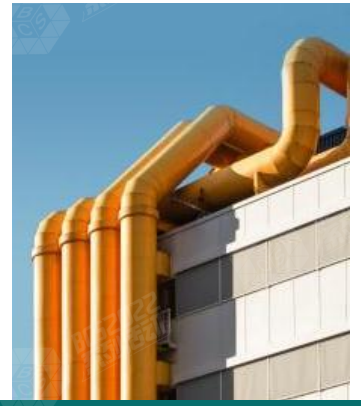
精选项目案例


电力


烟草


先进制造

轨道交通


天然气


钢铁


水务

国家电网 STATE GRID

电科院工控安全实验室建设项目

中能融合 ZHONGNENG INTEGRATED

能源工业互联网态势感知安全设备定制化项目

CSSC

某所安全攻防研究及威胁情报中心建设项目

中华人民共和国工业和信息化部

化工行业工控风险监测设备开发项目

ZENITH 中天钢铁

工控安全生态运营平台建设项目

积累大量工业互联网安全建设项目案例，具有丰富的安全实施经验

THANKS