攻防演练平台（ADP）

ATTACK-DEFENSE PLATFORM

为工业 4.0 保驾护航，助您赢在工控安全

电 话：4000-680-620　　**传 真**：010-62971782

邮 箱：support@winicssec.com　　**邮 编**：100085

微 博：http://weibo.com/winicssec

微信公众号：**威努特工控安全**

地 址：北京市海淀区上地三街 9 号嘉华大厦 F 座 907 室

北京威努特技术有限公司

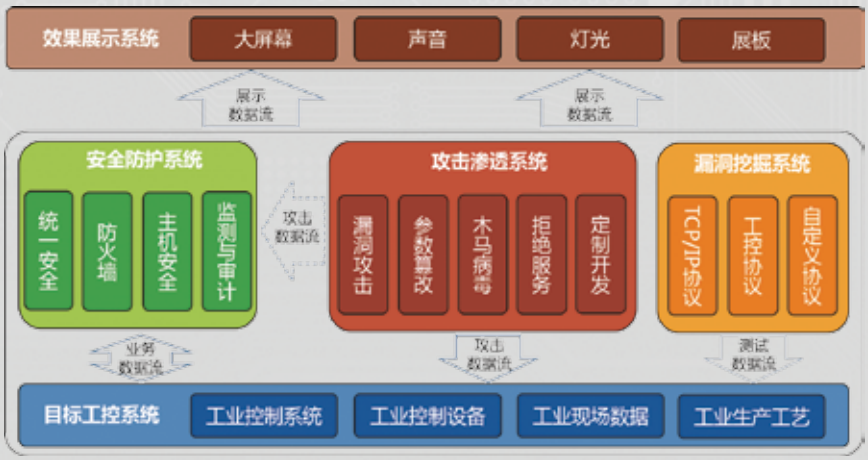
www.winicssec.com

平台概述 / Product Overview

威努特攻防演练平台（ADP）是威努特基于深厚的工控安全研究和技术积累而开发的一套综合性研究平台，该平台在仿真工业控制网络及系统、工业生产工艺流程的基础上，具有攻防演练、攻防技术验证、安全检测和风险评估等诸多功能。

通过搭建由目标工控系统、漏洞挖掘系统、攻击渗透系统、安全防护系统、效果展示系统等五个子系统组成的攻防演练平台，可以充分展示恶意软件的攻击影响及防护方案的策略部署和防护效果，充分验证新的攻击和防护技术，实施针对工控系统的风险评估和漏洞挖掘，实现攻防研究、人才培养、检测认证等目的。

方案组成 / Solution Composition



模拟某一工业行业典型的控制系统，是攻防演练的目标。该子系统包含组成工控系统的软、硬件资源，如系统结构组态软件、控制策略组态软件、人机交互组态软件、DCS、PLC、RTU 等。在工控系统的基础上，也可以根据实际需求做延伸，将一些与工控系统联系紧密的生产控制、信息管理等系统也予以仿真，如 MES 系统、MIS 系统等。

用于展示攻防效果的子系统，包括攻击的路径、防护的手段、攻击给工业生产带来的危害和损失等。根据行业的不同和实际客户需求，该子系统一般包含沙盘模型（仿真生产过程中的全部或关键工艺流程，并展示部分攻击效果）、展示挂板（部署目标工控系统的硬件设备和操作终端）、操作台（用于安放操作主机）、大屏幕显示终端（用于展现一些攻击路径、攻击效果）、声光电展示终端等。

用于对目标工控系统的关键控制设备进行未知漏洞挖掘，该子系统主要包含威努特工控漏洞挖掘产品及其他辅助技术和设备，通过该子系统，可以对工控系统的关键控制设备进行健壮性测试，并出具相关的测评报告等。

用于对目标工控系统进行渗透及攻击的子系统，该子系统主要包含用于渗透、攻击的软件、硬件和攻击方案，通过该子系统，可以还原一些真实工控安全事件的全过程并发现工控系统中的安全隐患和薄弱环节。

用于监测、防护目标工控系统的子系统。该子系统主要包含威努特工控可信网关、可信卫士、工控安全监测与审计、统一安全管理中心等产品和系统，通过该子系统，可以实时发现攻击并对目标工控系统做防护，从而验证安全产品和方案在真实工控环境中的应用效果。

典型应用场景 / Typical Application Scenario

工控系统风险评估

在对各个行业（如电力、石油、化工等）仿真的基础上，进行工控系统的风险评估，不用去工业现场即可全面了解工控系统面临的风险。

工控设备漏洞检测

对工控系统中的PLC、DCS等设备进行全面的漏洞挖掘，掌握攻防主动权。

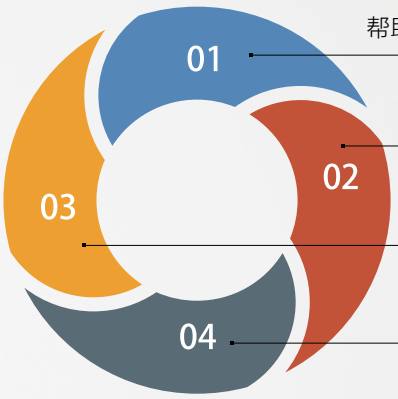
验证安全方案

通过加载各类行业知名的病毒、恶意软件来模拟攻击，可以充分验证新的防护方案和产品的有效性。

企业、高校的工控安全人才培养

基于该平台进行实战攻防演练，帮助企业技术人员或高校工控安全实验室学生更快、更直观的掌握工控安全的攻防知识和操作技能。

客户价值 / Customer Values



01 帮助行业企业正确评估当前的工控系统风险

02 帮助行业企业提升工控设备自身安全性

03 提升行业的安全技术方案水平

04 提升技术人员的安全意识和安全技能

典型客户案例一 / Typical Customer Case 1

• 大学过程控制实验室工控安全攻防演示实验平台

案例解析

该平台是在大学过程控制实验室的基础上，根据教学研究的需要而建设的综合性实验平台。

目标工控系统	西门子 S7-300 PLC 控制系统 +WinCC 组态软件
安全防护系统	威努特可信网关 2 台 + 威努特统一安全管理中心 1 台 + 威努特工控主机卫士 5 个点
攻击渗透系统	在多个攻击源上部署威努特攻击套件，从不同网络层面、不同网络路径对目标工控系统发起渗透和攻击，攻击的手段包括有：远程渗透、木马植入、PLC 漏洞攻击、控制设备参数篡改等。
漏洞挖掘系统	威努特工控漏洞挖掘系统 1 台
效果展示系统	装备制造生产线沙盘模型 + 网络分层效果展板 + 网络拓扑 / 攻击路径效果指示灯带

平台亮点

- 模块化设计，扩展升级方便灵活
- 全方位教学场景设计
- 多层次仿真实验接口
- 丰富的效果展示手段
- 工控安全“白环境”整体解决方案
- 前瞻性的工控漏洞挖掘研究

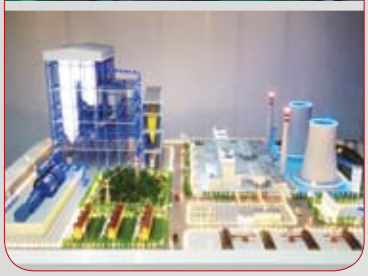
平台功能

典型客户案例二 / Typical Customer Case 2

• 火力发电厂工控安全攻防演练平台

案例解析

该平台是根据客户业务发展的需要，结合现场实际而建设的，集攻防演练、设备测评、对外展示于一体的多功能平台，在保障安全产生的同时，还被赋予了企业对外展示的职能。



目标工控系统	主控艾默生 Ovation DCS 控制系统 + 辅控西门子 S7-300 PLC 控制系统
安全防护系统	威努特可信网关 2 台 + 威努特统一安全管理中心 1 台 + 威努特工控主机卫士 10 个点
攻击渗透系统	在多个攻击源上部署威努特攻击套件，从不同网络层面、不同网络路径对目标工控系统发起渗透和攻击，攻击的手段包括有：远程渗透、木马植入、控制系统漏洞攻击、控制设备参数篡改等
漏洞挖掘系统	威努特工控漏洞挖掘系统 1 台
效果展示系统	火力发电生产工艺全流程沙盘模型 + 网络分层效果展板 + 报警指示灯 + 报警蜂鸣器

平台亮点

- 模块化设计，灵活扩展与升级
- 生产工艺全流程仿真
- 第三方接口预留
- 丰富的效果展示手段
- 工控安全“白环境”整体解决方案
- 高效工控漏洞挖掘，建立设备入网标准

平台功能