

逐鹰攻防演练平台

产品介绍

2025年11月

目录

MULU

1

背景

2

产品方案

3

典型案例

```

    if (a) {
      for (i = 0; i < l; i++)
        if (r = t.apply(e[i], a), r === !1) break
    } else
      for (i in e)
        if (r = t.apply(e[i], a), r === !1) break
    } else if (a) {
      for (i = 0; i < l; i++)
        if (r = t.call(e[i], i, e[i]), r === !1) break
    } else
      for (i in e)
        if (r = t.call(e[i], i, e[i]), r === !1) break
    return e
  },
  trim: b && !b.call("\uffff\u00a0") ? function(e) {
    return null == e ? "" : b.call(e)
  } : function(e) {
    return null == e ? "" : (e + "").replace(C, "")
  },
  isArray: function(e, t) {
    var n = t || [];
    return null != e && (N(Object(e)) ? x.merge(n, "string" == typeof e ? [e] : e) : b.call(n, e))
  },
  isArray: function(e, t, a) {

```

01

需求背景

网络空间安全已经渗透到国家、经济、社会各个方面

国家安全



- 我国遭受APT攻击，涉及政府机构、教育、科研、国防军工和交通运输等14个重点行业领域，APT组织窃取敏感数据，实施战略性破坏，服务攻击者背后势力的政治、军事或经济等目的，直接危害我国数据安全、网络安全和核心利益安全。（2024年）
- 我国西北工业大学遭境外网络攻击,境外黑客组织利用木马程序窃取我国重要数据，严重威胁我国国家安全。（2022年）

网络攻击直接威胁国家安全

经济安全



- 全球勒索软件攻击事件激增，我国制造业成为受害重灾区，勒索攻击导致企业生产停滞、数据丢失，造成巨大经济损失。（2024）。
- 中国工商银行在美国全资子公司——工银金融（ICBCFS）遭遇了勒索软件攻击，导致部分系统中断（2023）

网络攻击造成严重经济后果

社会安全



- 国家安全局近期批斗“台独”网军通过自动化漏洞扫描和密码爆破工具，攻击控制大陆计算机网络。开展窃密、破坏、反宣活动。伺机散布虚假消息、操纵舆情走向，误导大陆和台湾民众认知，监控打压岛内异见人士。（2025年）
- 二维码网络钓鱼攻击流行网络犯罪分子利用用户对二维码的信任，嵌入恶意链接，导致用户信息泄露和财产损失。

网络威胁已无处不在

网络安全政策法规与实践

1

《网络安全法》中的应急演练要求

《网络安全法》明确要求“定期组织网络安全应急演练”。该法律从国家层面强调网络安全应急演练的重要性，要求关键信息基础设施运营者等定期开展演练，以提升应对网络安全事件的能力，保障国家网络安全。



有关部门和各级政府职责

- 第八条 网络安全监管职责划分
- 第十六条 各级政府应加大网络安全技术投入和扶持
- 第十九条 各级政府及有关部门开展网络安全宣传教育
- 第三十条 规范网信和有关部门的监管执法权力

- 第三十九条 网信协调有关部门履行信息基础设施安全监管职责（抽查、演练、信息共享、应急协助等）
- 第五十条 国家网信和有关部门履行信息内容安全监管职责
- 第五十一条 网信部门统筹落实监测预警和信息通报工作
- 第五十二、五十三、五十四、五十五、五十六、五十七、五十八条 政府各部门的监测预警与应急处置职责

2

等保与关基条例下的细化要求

等保2.0标准和关基条例进一步细化网络安全要求，明确攻防演练作为重要手段，要求相关单位定期开展，以确保网络安全防护体系的有效性和可靠性，推动网络安全等级保护制度的深入实施。

维护国家网络空间主权、国家安全和社会公共利益

第二章 关键信息基础设施认定			
8 保护工作部的定义	9 制定认定规则	10 认定、通知、上报	11 重认定
第三章 运营者责任义务		第四章 保障和促进	
12 三同步	17 检测评估	26-30 检测标准	34 安全标准、规范、指南
13 安全防护制度和责任制	18 事件报告	30 网络安全	35 人才保障
14 安全管理机构及职责	19 采购网络产品和服务	31-32 风险评估	36 技术支持与攻关
15/16 安全防护工作具体职责	20 明确义务和责任	33 网络安全	37 网络安全审查
		38 网络安全	38 网络安全
第五章 法律责任 (39~49)			
警告、责令改正	处罚、处分	拘留	刑事责任
第六章 附则			

公共通信	基础电信业务	增值电信业务
信息服务	广播电视	重点发电企业
能源	骨干型电网	石油石化企业
交通	公路	水路
水利	管理运营	水利枢纽
金融	全国性银行	头部证券
公共服务	邮政	大型保险
电子政务	应急管理	支付机构
国防科技	军工集团	金融职能机构
		社会保障
		卫生健康

3

攻防演习的常态化与发展

自2016年起持续开展，覆盖范围从央企扩展至重点行业。国家攻防演习已成为我国网络安全领域的重要实践，通过定期开展攻防演练，检验和提升各行业网络安全防护水平，促进网络安全技术和人才发展，保障国家关键信息基础设施安全。

国家级

行业级

省市级

	2017年	2018年	2019年	2020年	2021年	2023年-2024年
典型攻击模式	1. 互联网突破； 2. 旁站攻击； 3. 传统攻击行为； 4. 物理设备攻击； 5. 利用大型内网做跨区域攻击； 6. 集权类设备攻击； 7. Oday； 8.	6. 集权类设备攻击； 7. 供应链攻击； 8. 邮箱系统攻击（获取信息）； 9. 供应链攻击（获取信息）； 10. 钓鱼、水坑、利用“人”的弱点； 11.	8. 供应链攻击； 9. 邮箱系统攻击（获取信息）； 10. 钓鱼、水坑、利用“人”的弱点； 11. 钓鱼、水坑、利用“人”的弱点； 12. 目标单位周边WiFi攻击； 13. 业务外连单位攻击； 14.	11. 钓鱼、水坑、利用“人”的弱点； 12. 目标单位周边WiFi攻击； 13. 业务外连单位攻击； 14. 安全产品漏洞； 15. 交换机、路由器、iot等漏洞； 16.	14. 安全产品漏洞； 15. 交换机、路由器、iot等漏洞； 16. Oday漏洞单独加分； 17. chrome等浏览器漏洞； 18. 供应链问题日益严重； 19. 二级单位薄弱点被逐步放大； 20.	20. 企业级即时通讯系统漏洞； 21. 办公软件漏洞； 22. 应用系统Oday漏洞； 23. 供应链软件漏洞； 24. 规则调整二级单位刷分严重； 25.
标志	重保必要条件，攻击行为“组织化”状态明显，防守不够严密、监测能力不足是较大短板。	防守方认知逐渐清晰，部分参与过的单位能力大幅提升，攻击难度加大，开始尝试“更隐蔽”的攻击方式。	行业现象明显，能力强弱两级分化，钓鱼、水坑、供应链等攻击普遍；有一些防守“应试性”现象明显。（停业务、断网等）“大目标”概念出现；	互联网企业攻击队重兵投入；社工方式应用普遍，Oday普遍，利用安全产品漏洞攻击现象增多；增加了沙盘推演环节；与目标系统同等重要的系统也参照目标系统扣分；	漏洞储备竞赛与赛前踩点现象（自动化）严重；刷分导致很多二级单位被打；	依然漏洞储备竞赛，攻击手段仍以供应链软件漏洞利用为主，聚焦集权系统、存储敏感信息环境系统；刷分导致很多二级单位被打；

面向关基的政策指导要求

法律与标准依据

- 《网络安全法》：要求关键信息基础设施运营者定期开展网络安全事件应急演练。
- 《关基安全保护要求》（GB/T 39204-2022）：需围绕关键业务的可持续运行设定场景，定期组织攻防演练。演练应覆盖关键信息基础设施的核心供应链、上下游产业链等业务相关单位。

01

关键要求

- **年度演练频次**
 - 每年至少1次，重大变更后需重新评估
- **跨组织联动**
 - 纳入供应链上下游及核心业务场景，强化联防联控
- **成果应用**
 - 将演练结果转化为安全策略优化与人员培训计划

红蓝对抗机制



攻击方

由高级攻防专家组成，采用多样化手段（**情报、社工、高级渗透、供应链**）验证防御能力



防守方

聚焦**监测、处置、修复**全流程，提升主动防御与协同能力

演练流程

1

准备阶段

制定防守方案、召开启动会、梳理资产与应急预案

2

安全自查整改

漏洞扫描、基线检查、日志审计及加固

3

预演练阶段

模拟攻击（如Web渗透、社会工程学攻击），检验整改效果并备案

4

正式防护阶段

实时监测、攻击阻断、应急响应与溯源

5

总结阶段

形成报告、整改脆弱点、优化防护体系

重点行业监管持续加码



金融行业：行业监管要求定期开展实战化攻防演练

金融行业因涉及大量资金和敏感信息，对网络安全要求极高。行业监管规定金融机构每年至少开展一次实战化攻防演练，以检验和提升网络安全防护能力，防范金融风险，保障金融稳定。

- 《金融数据中心容灾建设指引》（JR/T 0264—2024）
- 《金融数据中心能力建设指引》（JR/T 0265—2023）
- 《银行保险机构数据安全管理办法》（2025年）
- 《银行保险机构应对突发事件金融服务管理办法》
- 《银行业重要信息系统突发事件应急管理规范（试行）》



能源行业：国家能源局印发《2025年能源监管工作要点》

能源行业是国家重要基础设施领域，电力系统的安全稳定运行至关重要。组织开展电力行业网络安全演习，推动网络安全靶场、漏洞库等基础设施建设。



政务领域：数字政府建设评估将攻防演练纳入考核指标

政务领域信息化程度不断提高，网络安全是保障政务工作正常开展的关键。将攻防演练纳入数字政府建设评估考核指标，促使政府部门重视网络安全，定期开展演练，提升政务网络安全防护能力，保障政务信息安全。

- 《互联网政务应用安全管理规定》（2024年）
- 《信息安全技术 政务网站系统安全指南》GB/T 31506-2022
- 《信息安全技术 网络安全事件应急演练指南》GB/T 38645-2020

组织安全防护有效性验证和人才培养需求

攻防能力差距显著

大部分企业在首次参加红蓝对抗中普遍存在**攻防能力不平衡**的问题，大部分企业暴露出的**安全漏洞和短板**，反映出企业网络安全防护体系存在薄弱环节，需要**加强攻防能力建设**。

主流通信工具
漏洞利用攻击

安全设备0DAY
依然成为主流的
攻击渠道

利用常规漏洞打
穿整个网络

利用供应链
0DAY/Nday漏
洞攻击

社工钓鱼手段成为
重要突破渠道

利用开发测试网
漏洞攻击

集权类系统仍是
攻击热点

多级纵深网络成
为攻击跳板

虚拟化和云端漏
洞攻击成为趋势

安全防御体系验证刚需

随着攻击手段的复杂化和体系化，传统渗透测试已无法满足组织**安全防御体系验证需求**，组织需要通过**攻防演练**，**模拟真实攻击场景**，全面**检验安全防御体系的有效性**，及时发现和修复潜在风险隐患。

红蓝对抗机制



演练流程



人才能力培养诉求

防守团队平均需要**3次实战演练**达到基本对抗能力。**网络安全人才短缺**是企业面临的普遍问题，防守团队通过**多次实战演练**，**积累实战经验**，提升应对网络攻击的能力。



```

    if (a) {
      for (i = 0; i; i++)
        if (r = t.apply(e[i], a), r === !1) break
    } else
      for (i in e)
        if (r = t.apply(e[i], a), r === !1) break
    } else if (a) {
      for (i = 0; i; i++)
        if (r = t.call(e[i], i, e[i]), r === !1) break
    } else
      for (i in e)
        if (r = t.call(e[i], i, e[i]), r === !1) break
    return e
  },
  trim: b && !b.call("\uffff\u00a0") ? function(e) {
    return null == e ? "" : b.call(e)
  } : function(e) {
    return null == e ? "" : (e + "").replace(C, "")
  },
  isArray: function(e, t) {
    var n = t || !1;
    return null != e && (N(Object(e)) ? x.merge(n, "string" == typeof e ? [e] : e) : b.call(n, e))
  },
  isArray: function(e, t, n) {

```

02 产品方案

演练平台产品方案



为用户提供攻防演练和赛事活动**全流程**的技术支撑，**涵盖演练前准备工作创建、演练中攻防态势呈现与演练后数据统计汇总**。旨在确保演练全程安全可控，赛事规则灵活配置，保障比赛公平高效，提升攻防对抗协同能力，培养专业网络安全人才。



演练赛事活动平台技术需求

容纳攻击、防守、裁判和指挥运营各方人员接入，实现演练规则制定、活动任务管理、用户权限控制，攻击行为审计、网络安全隔离、数据分析汇总，攻防态势可视化呈现等全方位支撑。

攻击流量审计与防御功能

具备实时监测网络流量、检测攻击行为的能力，并能及时拦截破坏性攻击行为和高危操作。

用户管理与权限控制功能：

具备完善的用户管理体系，支持对不同角色用户（如指挥中心、攻击方、防守方、裁判等）进行精细化的权限分配和管理，保障活动有序进行。

赛事管理与评分功能

支持创建多样化的赛事规则，同时具备自动化的评分系统，能根据攻击和防御表现进行客观、准确评分，确保比赛的公平性和透明度。

数据分析与复盘功能：

对演练和赛事过程中的各类成果数据进行全面收集和深度分析，可提供详细的复盘报告和可视化图表，帮助参与者总结经验教训，提升攻防能力。

攻防态势可视化功能：

提供实时监控画面，直观展示演练和赛事情况，包括攻击漏洞成果、失陷资产情况等，让主办方和参与者能够清晰地了解活动的整体态势和关键信息。

资源管理与扩展功能：

能够根据活动规模和资源需求灵活分配计算资源、存储资源、网络资源等；支持资源的弹性扩展，以应对大规模参赛队伍和高并发流量情况，确保平台的高效运行。



攻防演练平台-提供实战攻击训练环境，提升团作战能力

攻击方

- 发现系统存在的高、中、低漏洞
- 突破防守方的网络边界
- 获取防守方的系统或其他数据
- 获得防守方的目标系统权限

提交成果



提交成果

防守方

- 发现攻击方的攻击类型
- 分析研判攻击方的攻击痕迹、攻击样本
- 事件分类分级处置和响应、阻断攻击方的攻击
- 追踪溯源，还原攻击链条

裁判方

成果审核
对攻击方和防守方提交的成果进行审核

分数分配
对攻击方和防守方提交的成果打分

数据留存
记录学员强项与薄弱点优化课程

站内互动
负责攻击方和防守方进行互动沟通

裁判大屏
裁判专属实时大屏

核心功能



逐鹰攻防演练平台共计5个系统：赛事官网、指挥中心、攻击系统、防守系统、研判系统：

赛事官网



逐鹰攻防演练平台指挥中心



逐鹰攻防演练平台攻击系统



逐鹰攻防演练平台研判系统

排名	用户昵称	成果得分	成果数量	通过率	特大大成果	特大大成果	特大大成果	特大大成果
4	网络安全攻防演练	888	60	65%	20	10	10	20
5	网络安全攻防演练	888	60	65%	20	10	10	20
6	网络安全攻防演练	888	60	65%	20	10	10	20
7	网络安全攻防演练	888	60	65%	20	10	10	20
8	网络安全攻防演练	888	60	65%	20	10	10	20
9	网络安全攻防演练	888	60	65%	20	10	10	20
10	网络安全攻防演练	888	60	65%	20	10	10	20

逐鹰攻防演练平台防守系统



核心功能——赛事官网

功能一：赛事通报

赛事相关的赛事简介、参赛对象、时间安排、等级规则、奖项设置等关键信息。

功能二：线上报名

支持学生输入联系方式、姓名等关键信息进行线上报名，同时可查看报名进度及报名结果。

功能三：报名审批

指挥中心获取赛事官网线上报名的选手信息，进行审核驳回操作，同时将审核结果反馈给选手。



核心功能——演练平台指挥中心

为用户提供赛事全流程服务，涵盖赛前准备工作创建、赛中数据配置以及赛后数据统计。



演练平台指挥中心

赛事开始前

赛事创建

目标单位管理

选手与团队创建

防守方账号创建

裁判账号配置

大屏配置

赛事进行中

报名审核

生成VPN

分发VPN

目标单位分配

成果分配

大屏配置

赛事结束后

赛事详情

赛事统计

资产概览

排名中心

成果列表

系统管理

核心功能——演练平台攻击系统

ALLSEC
众安天下

提升选手实战与协作能力，保障赛事公平高效开展

关键词：实时排名、规则指引、成果提交、审核互动、数据分析、赛事动态通知

演练平台攻击系统

个人中心

当前排名

成果提交分析

能力统计

赛事详情

赛事规则

赛事简介

演练目标

成果报告

提交成果

成果审核查看

互动评论

公告消息

平台公告

审核结果通知

互动通知

赛事大屏

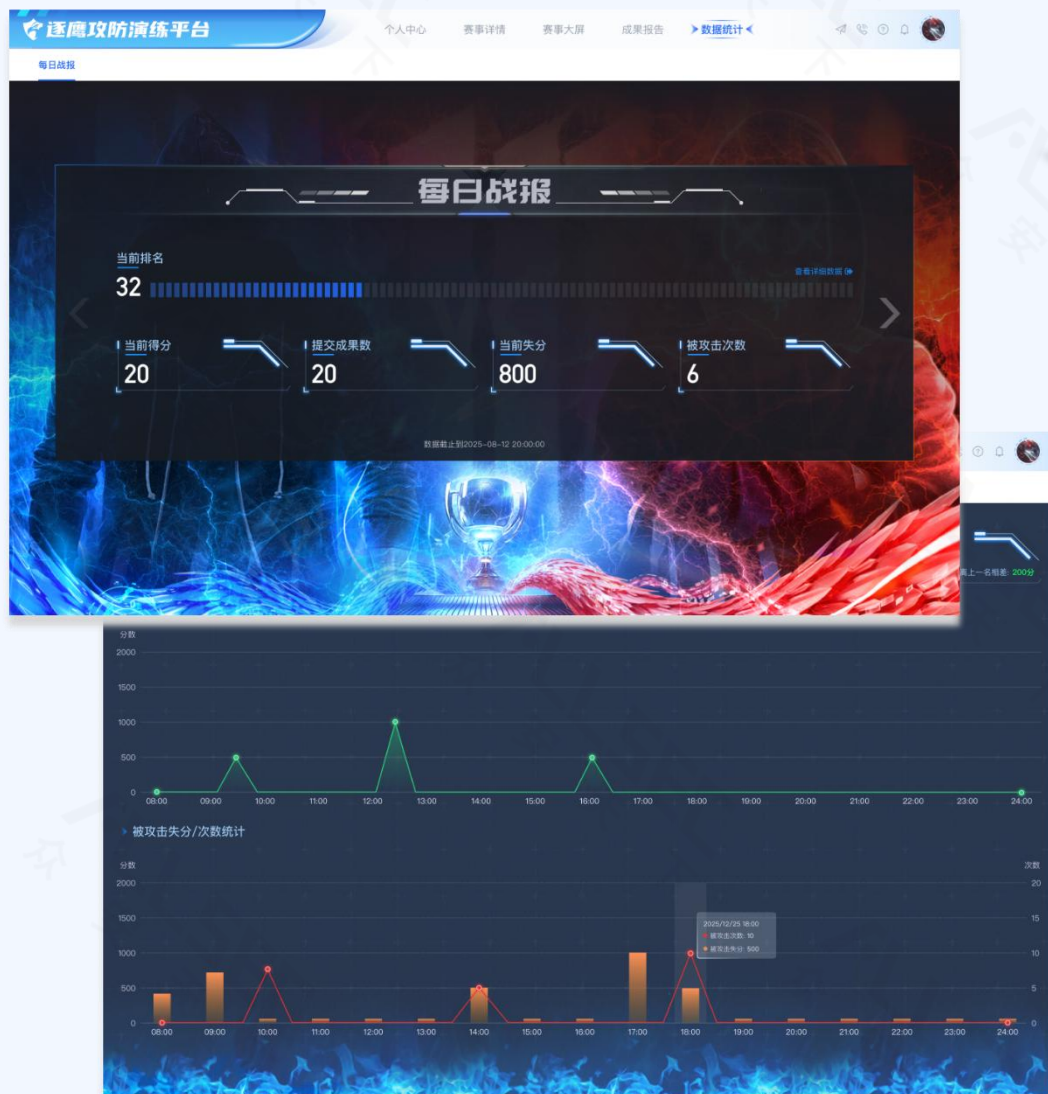
攻击方排名

积分统计

成果等级分析



核心功能——演练平台防守系统



实时掌握演练对抗态势、提升选手防守对抗能力与赛事公平性

关键词：赛事规则指引、成果提交、审核与互动、赛事动态通知

演练平台防守系统

个人中心

当前排名

积分统计

溯源成果分析

赛事详情

赛事规则

赛事简介

奖项设置

成果报告

提交溯源成果

成果审核查看

互动评论

公告消息

平台公告

审核结果通知

互动通知

赛事大屏

防守方排名

积分统计

防守方溯源成果

核心功能——演练平台研判系统



全面掌握赛事数据，公平审核成果，实时反馈，保障赛事公正

关键词：赛事说明、赛事大屏、成果列表、排名中心、公告消息。

演练平台研判系统

赛事说明

赛事简介

赛事规则

奖项设置

赛事大屏

成果类型统计

排名分析

审核成果分析

公告消息

系统公告

审核通知

分享通知

成果列表

审核成果

查看成果

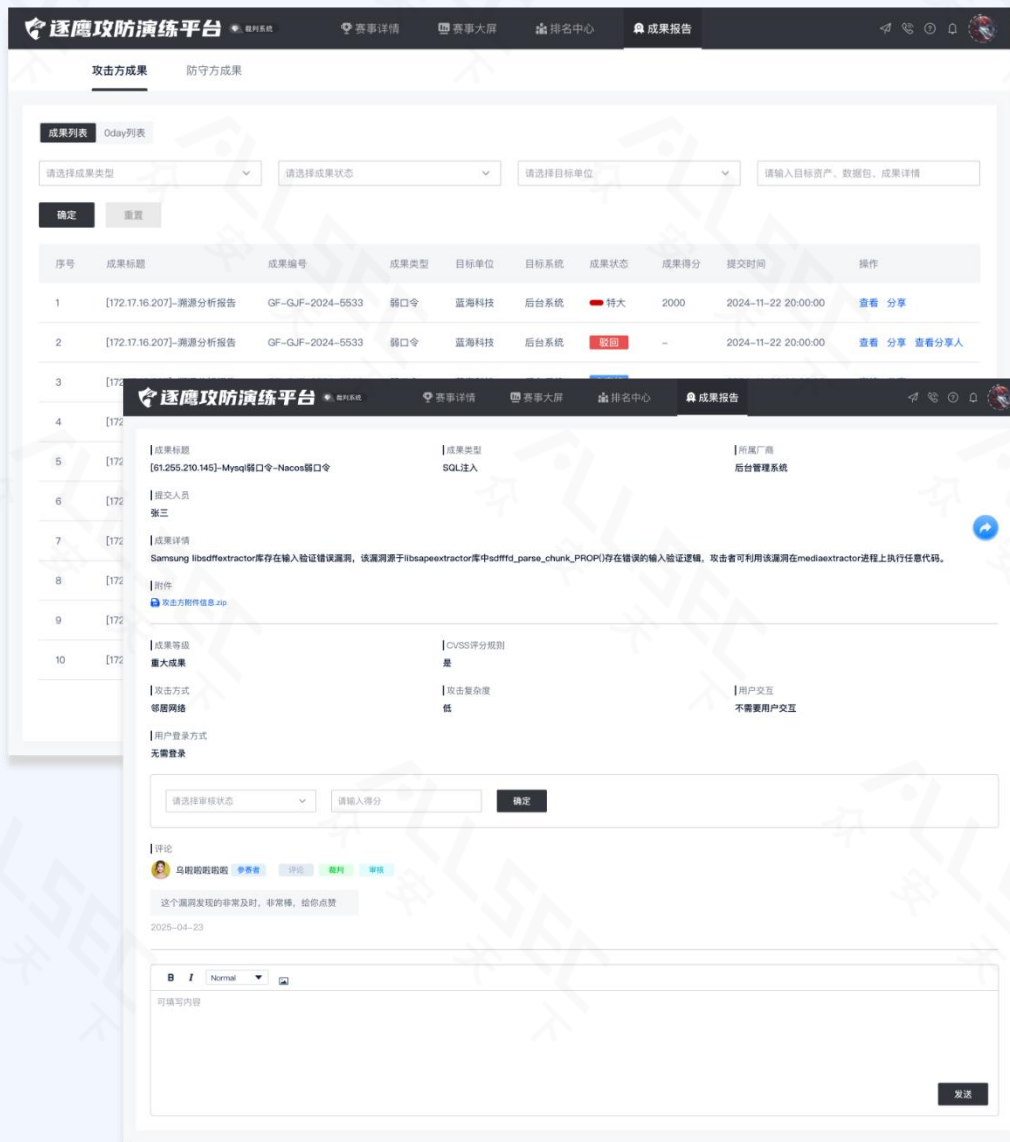
互动评论

排名中心

攻击方排名

防守方排名

互动评论



核心优势：沉浸式攻防大屏多维度数据看板



攻击态势大屏，从攻击方角色进行多维度数据分析，整个赛事过程中实时更新攻击方排名，精准分析成果等级分布及各类成果占比，同时，为保障选手参与度，从不同维度设置多种第一名奖项，包括成果通过率第一、提交成果数量第一、得分第一等，激励选手在不同方面发挥优势，提升整体参与热情和赛事竞技水平。

防守态势大屏，从防守方角色进行多维度数据分析，整个赛事过程中实时更新防守方失分排名、得分排名、积分排名，激励防守方参与到整个攻防赛事当中，积极做好追踪防御溯源工作，提升防御能力。



核心优势：沉浸式攻防大屏多维度数据看板



裁判研判数据大屏，在赛事过程中，我们将从裁判审核结果排名、成果占比分析以及审核通过率排名三个维度，实时更新并分析每位裁判的审核成果数据。多维度数据分析确保全程监控裁判工作，及时纠正偏差，保障赛事审核的公平公正。

平台演练数据大屏，从管理员角色考虑，需要实时查看整个赛事攻击方/防守方/裁判方三个角色进行多维度数据分析，攻击方排名、防守方排名、攻击队伍、防守队伍、成果占比分析、攻击频率等数据。能够全面了解赛事进展，及时发现问题并进行调整，保障赛事顺利进行。



核心优势：沉浸式攻防大屏多维度数据看板



流量审计大屏，在赛事过程中，平台支持全程实时监控赛事流量动态，提供源IP、累计请求次数、累计请求目标、累计请求流量、累计攻击数据包等数据分析，为赛事的稳定运行提供全方位、精细化的数据分析支持，助力快速应对各类突发状况，保障赛事顺畅进行

流量攻击大屏，在赛事过程中，平台全程追踪流量动态变化，包括威胁事件数、威胁事件分类数、数据包统计、数据包实时监测等数据分析，为赛事的网络安全保障提供全面、精准、实时的数据支持，确保赛事平台在复杂的网络环境中稳定运行。



核心优势：激发防守方参与意识

攻防演练平台-防守方系统从设计层面给客户视觉冲击，赛事开始前，显示当前总积分，赛事进行中以及结束后可实时查看当前排名、积分以及溯源成果状态，使得防守方积极参与到该场赛事当中，做好防御工作。

当前排名 溯源成果数 有效成果数 成果通过率 累计得分 累计失分

溯源成果趋势分析

实时统计该防守方提交溯源成果数据分析

溯源成果类型TOP5

实时统计该防守方溯源成果类型TOP5

排名/积分趋势

实时记录该防守方当前排名趋势以及当前积分趋势图

提交溯源成果实时动态

实时记录该防守方提交溯源成果动态



溯源成果等级分析

实时记录该防守方成果等级分析

核心优势：支撑不同赛事级别和自定义需求

攻防演练平台设计**五级赛事**规则，从**基础**到**国赛**，逐级提升难度，**满足不同赛事级别**需求，助力技术提升，为赛事提供科学规则支撑。

难度系数	面向目标	赛事内容	赛事目的
基础级	初级工程师	基础网络安全概念、基础漏洞和基础攻防	了解网络安全基础知识、掌握基本攻防技能
进阶级	中级工程师	高危漏洞的发现分析和利用	提升对网络威胁和漏洞的认识和处理能力
专业级	高级工程师	获取系统权限等高级攻防技术	锻炼攻防技术和提高实操应急能力
资深级	资深工程师	获取关键系统权限和深入系统安全分析	挑战参与者极限提升攻击研究能力
国赛级	顶级工程师	模拟国家级赛事规则和环境的高难度挑战	提供高水平实战平台、预演国家级演练

支持不同等级的任务评定规则，适应比赛难度系数，适应相应难度规则和场景

核心优势：支撑不同等级赛事级别

逐鹰攻防演练平台

系统管理 | 规则配置

序号	角色类型	规则级别	创建时间
1	攻击方	基础级	2024-12-02 09:00
2	攻击方	进阶级	2024-12-02 09:00
3	攻击方	专业级	2024-12-02 09:00
4	攻击方	资深级	2024-12-02 09:00
5	攻击方	国赛级	2024-12-02 09:00
6	防守方	-	2024-12-02 09:00

展开/收起

不同赛事级别规则列表

逐鹰攻防演练平台

赛事统计 | 规则配置

规则信息

*角色类型: 攻击方

*规则级别: 基础级

*规则描述

1.攻击目标和手段：攻击方以获取指定目标系统（靶标系统）的管理权限为目标，不限制攻击路径和攻击手段，可以采用社会工程学、0day漏洞等攻击手段。攻击方需要在确保参演单位业务系统稳定运行的前提下进行攻击，攻击行为应是可控、可管、可审计的。

2.攻击行为监控：对于攻击行为的监控较为严格，组织方会对违规行为进行评定，并予以警告和扣分处理。攻击目标主体单位的下属子公司、下属企业及控股企业等需要证明其网络上与主体单位的连通性，才能进行计分。

3.角色分配：攻击队伍中每人按照技术能力扮演不同角色，多个队伍可以通过情报共享进行联合作战。

4.攻击阶段：攻击队的工作可分为信息收集、建立据点和横向移动三个阶段。在信息收集阶段，攻击方需要进行详尽的情报搜集工作。

5.木马使用要求：使用的木马应不具有自动删除目标系统文件、损坏引导扇区、主动扩散、感染文件、造成服务器宕机等破坏性功能。禁止使用具有破坏性和感染性的病毒、蠕虫。

6.非法攻击阻断及通报：演练指挥部应组织技术支撑单位对攻击全流量进行记录、分析，在发现违规攻击行为时阻断非法攻击行为，并转由人工处置，对攻击队进行通报。

7.演练规则：演练前明确制定攻击规则、防守规则和评分规则，保障攻防过程有理有据，避免攻击过程对业务运行造成不必要的影响。

取消 保存

创建不同赛事级别页面

支持不同等级的任务评定规则，适应比赛难度系数，适应相应难度规则和场景

核心优势：指挥中心平台灵活配置

攻击方/防守方排名配置 CONFIGURATION

允许管理员根据不同场景、不同需求，可对攻击方/防守方选手排名隐藏或者匿名展示。

动态打分机制 MECHANISM

根据某些场景可配置倍数审核打分的需求，确保了赛事的灵活性和透明性。

裁判权限灵活配置 CONFIGURATION

裁判权限灵活配置，裁判黑白名单设置、裁判是否可以查看排名中心、允许裁判查看成果详情中的选手信息满足不同用户对平台的特定需求。

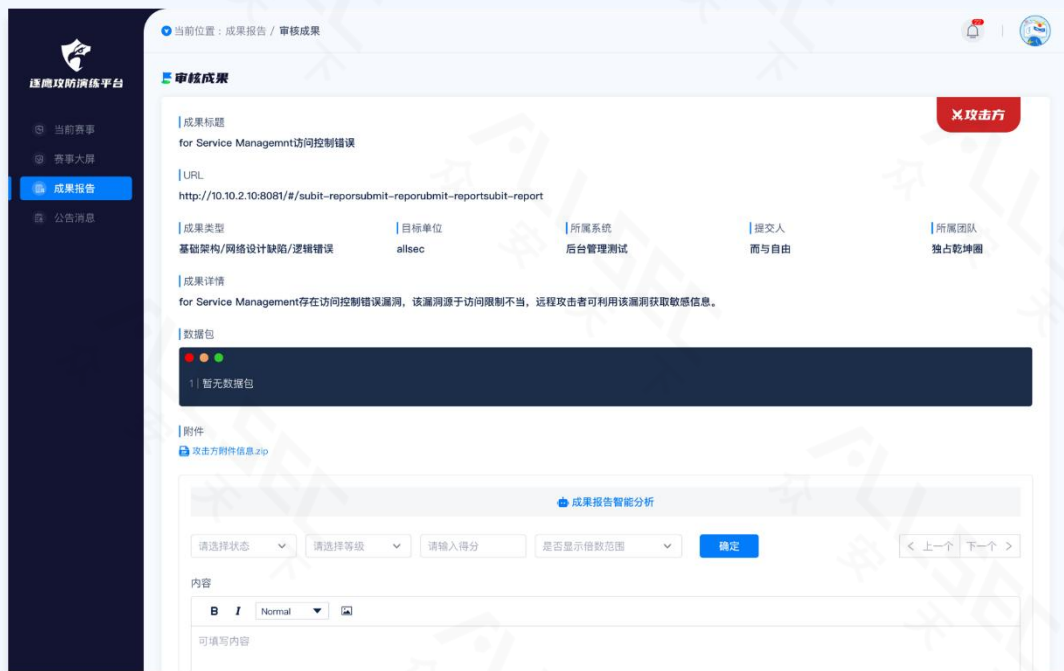
目标资产灵活分配 ASSIGNMENT

平台允许目标单位/目标系统/目标资产按照公共资产/定向资产均匀分配/全部分配的同时，也支持手动分配特定资产给特定选手



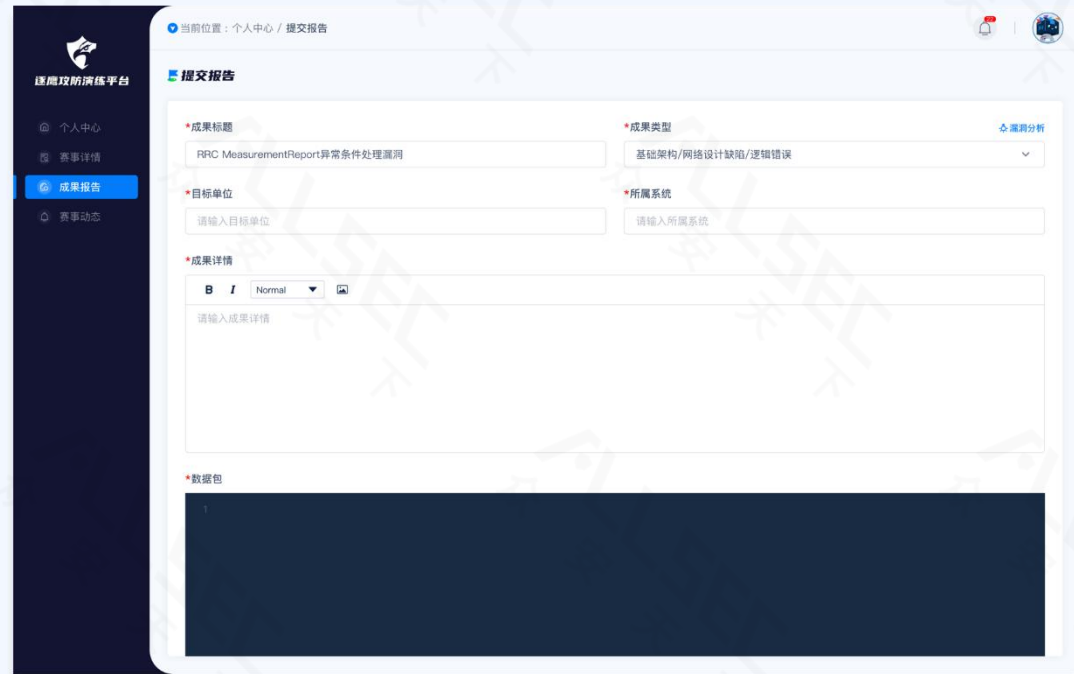
致力于满足不同客户不同需求，保障赛事公平化、灵活化、人性化

核心优势：AI机器人互动



AI智能评分

AI智能评审选手提交的成果报告，裁判审核成果报告可根据AI评分直接引用或修改



AI智能报告生成

AI智能生成报告，帮助选手提交规范化的成果报告，减少选手提交成果报告信息和提升用户体验

攻防演练平台应用场景



监管侧专项检查攻防演练

监管部门利用攻防演练平台对关键信息基础设施、重要信息系统等进行专项检查。通过模拟真实网络攻击场景，对被检查单位的网络安全防护能力、应急响应能力、漏洞修复能力等进行全方位评估；



公开赛事实战比武

攻防演练平台广泛应用于CTF夺旗赛和AWD攻防赛等多种赛制。通过实战对抗、赛事比武等操作，提升网络安全行业人才实战能力。平台还具备多个维度可视化数据大屏，能够实时反映比赛情况，了解选手赛事比武情况；



高校攻防实战培训

高校利用攻防演练平台开展网络安全教学与实践，通过红蓝对抗、攻防实战、教学实训等多种形式，为学生提供沉浸式学习体验。帮助学生应对复杂网络环境；为网络安全领域输送了高素质专业人才，助力筑牢网络空间安全防线。



集团公司内部实战攻防

平台支持企业能够定期执行攻防演练，有助于评估现有的网络安全防护能力，精准发现潜在的安全漏洞和弱点。企业可以利用这些信息测试并验证安全策略的实际效果，进而根据演练的反馈结果，针对性地调整和优化安全措施，确保网络安全防护体系的持续强化和改进。



平台应用场景与价值

ALLSEC
众安天下

实战演练

攻防竞技

比武练兵

人才磨砺



支撑演练赛事活动

可常态化承办各类行业或区域的实战攻防演练和攻防竞技赛事活动，为开展攻防演练、竞技赛事、成果汇总提供技术支撑和工作抓手。



攻击态势大屏



防守态势大屏



裁判研判与数据提交大屏



平台演练数据运营大屏



平台每日演练数据运营大屏



流量攻击大屏



检验提升网络安全防御能力

全面检验并掌握网络安全状况、数据安全防护能力，及时防范化解网络安全威胁风险，积累网络攻防作战经验，全面检验网络安全防护建设水平和应急处置能力，提高人员协同联动水平。



培养攻防实战精英

推动网络攻防实战人才培养，建立网络安全人才队伍，选拔高端人才，构筑一个供高等院校展示自身教学实力的高效平台，营造良好的网络安全技术教育氛围，强化教育、科技、人才一体良性循环



汇集攻防数据，呈现攻防态势

通过对攻防演练、竞技赛事的成果和数据汇总、统计、分析和计算。可视化呈现攻、防视角下的多种维度下的竞技态势，为演练和赛事的得分排名、统计分析和活动总结提供数据支撑。

客户案例



中华人民共和国公安部
Ministry of Public Security of the People's Republic of China



福州市人民政府
www.fuzhou.gov.cn



铜川市人民政府
www.tongchuan.gov.cn



湖南省工业和信息化厅
Industry and Information Technology Department of Hunan Province
湖南省国防科技工业局

```

    if (a) {
      for (i = 0; i; i++)
        if (r = t.apply(e[i], a), r === !1) break
    } else
      for (i in e)
        if (r = t.apply(e[i], a), r === !1) break
    } else if (a) {
      for (i = 0; i; i++)
        if (r = t.call(e[i], i, e[i]), r === !1) break
    } else
      for (i in e)
        if (r = t.call(e[i], i, e[i]), r === !1) break
    return e
  },
  trim: b && !b.call("\uffff\u00a0") ? function(e) {
    return null == e ? "" : b.call(e)
  } : function(e) {
    return null == e ? "" : (e + "").replace(C, "")
  },
  isArray: function(e, t) {
    var n = t || [];
    return null != e && (N(Object(e)) ? x.merge(n, "string" == typeof e ? [e] : e) : b.call(n, e))
  },
  isArray: function(e, t, a) {

```

03

典型案例

典型案例：为国家级攻防演练赛事提供技术支撑

- ◆ **主办单位：**河南省人民政府、河南工信厅、中国工业互联网研究院等
- ◆ **协办单位：**北京众安天下科技有限公司
- ◆ **赛事成果：**以赛代练，挖掘出网联汽车众多漏洞风险问题



1' 2023年车联网（智能网联汽车）安全挑战赛



1' 2023年国家铁路行业网络攻防演练

- ◆ **主办单位：**某部委某局
- ◆ **协办单位：**某大学、北京众安天下科技有限公司
- ◆ **赛事成果：**通过实网攻防，拉练行业内30+支实战人才队伍，排查出重大风险

- ◆ **主办单位：**湖南省工信厅
- ◆ **技术支撑单位：**北京众安天下科技有限公司
- ◆ **赛事成果：**通过实战攻防演练，锻炼来自15所高校、48支人才队伍的实战能力



1' 湖南省“网安湘军杯”网络安全技术实战赛



1' 2023年福建省第五届网络安全职业技能竞赛

- ◆ **主办单位：**福建省通信管理局、福建省工信厅等
- ◆ **协办单位：**北京众安天下科技有限公司
- ◆ **赛事价值：**网络安全人才队伍建设培养

众安天下支撑多场国家级大型攻防赛事，在平台支撑、技术支撑、运营支撑等方面有丰富的实战经验。

典型案例：湖南湘军杯网络安全技术实战赛

项目背景

在数字化转型的浪潮中，湖南省紧跟国家网络安全战略，通过举办“网安湘军杯”网络安全技术实战赛，提升省内网络安全防护水平，培养网络安全人才，加强网络安全意识。该赛事由湖南省工业和信息化厅、湖南省高等教育学会计算机专业委员会指导，国家新一代自主安全计算系统产业集群国链安全可靠计算机产业促进中心主办，是一场覆盖全省数十所高校的重要赛事。



赛事规模

28所高校

66支队伍

197名选手

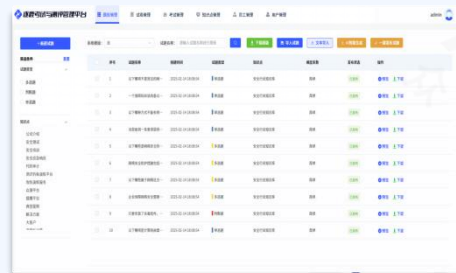


赛事模式

理论+实践

线上+线下

靶场+实网



典型案例：湖南湘军杯网络安全技术实战赛



活动主办方、承办方

- 赛前筹备：**联合指导单位制定赛事规则，成立组委会监督方案、落实场地租赁、设备调试及人员分工。
- 比赛执行：**监督比赛进程，协调突发问题，管理参赛队伍签到，维护现场秩序与安全。
- 赛事总结：**审核成绩，组织颁奖典礼，提交《比赛总结报告》。



众安天下

- 搭建比赛平台：**根据比赛形式与规则，搭建稳定、高效、安全的比赛平台
- 准备技术方案：**制定详细的技术方案，包括比赛环境搭建、漏洞预置
- 提供技术指导：**在比赛过程中，为参赛队伍提供必要的技术指导与解答
- 处理技术问题：**及时处理比赛中出现的技术问题
- 复盘总结与反馈：**收集比赛过程中的各类数据，总结赛事中的技术应用情况

攻防演练竞技赛事平台方案

网络安全攻防平台

-指挥中心-		-攻击平台-		-防守平台-		-研判平台-	
赛事管理	成果管理	个人中心		个人中心		赛事详情	
账号管理	公告管理	成果提交		成果提交		成果审核	
目标单位管理	日志管理	成果管理		成果管理		成果管理	

网络安全竞赛平台

-竞赛管理-		-竞赛中心-	
赛事管理	赛事运维	赛事中心	练习中心
赛队管理	赛题管理	赛事信息	我的成绩
用户管理			

网络安全众测平台

-任务大厅-	
项目管理	成果管理
学生管理	数据展示
运营管理	社区互动

应用 场景

攻防赛事比武	高校行业攻防赛事	高校安全意识培养	高校人才选拔
实战能力验证	高校实训演练	职业技能大赛	常态化赛事演练

典型案例：湖南湘军杯网络安全技术实战赛



客户收益

- 推动**产、学、研、用**深度融合，搭建**校、政、企**三方高效联动桥梁，营造良好网络安全技术教育氛围；
- 强化**教育、科技、人才**一体良性循环，打造网络安全技术人才品牌，促进**教育链、人才链与产业链、创新链**的有机衔接，为全省网络安全行业发展凝聚了新的共识、注入了新的活力。
- 不仅为参赛选手搭建了展示技能的舞台，更为高校与企业之间架起了人才输送的桥梁，有力地促进了**产教融合**与**校企合作**的深入发展。



典型案例：2023年全国铁路行业技术检测比武

ALLSEC
众安天下

活动背景

为了全面检验并掌握**铁路关键信息基础设施**安全状况、**数据安全**防护能力，及时防范化解网络安全威胁风险，提升铁路公安机关网络安全防护**实战能力**，铁路公安局组织网安部门专门力量对铁路信息系统开展远程网络安全技术检测工作。**以攻击者视角，对铁路信息系统进行安全检测。**

检测范围与目标

国铁集团、所属各企业以及国铁集团控股公司的各类网络和信息系统：

- 铁路外服网侧漏洞风险摸排、隔离验证
- 铁路内网跨网跨域防护有效性验证

技术支撑

- ✓ 演练现场支撑（3人）：技术保障+会务保障
- ✓ 演练平台支撑（3人）：技术支撑+平台保障
- ✓ 攻防服务支撑（6人+）：一线攻击+远程保障



关键词：暑期安全保障、数据安全保障

参演单位

18个铁路局公安队伍

中国人民公安大学

4家技术支撑单位



典型案例：2023年全国铁路行业技术检测比武

项目成果与价值



- ✓ 提升了铁路关键信息基础设施的安全防护能力；
- ✓ 促进了铁路行业网络安全人才的培养和技术创新；
- ✓ 为铁路行业的网络安全工作提供了重要的技术支撑和经验积累。



- ✓ 在技术检测中取得多个重大成果，积累成果积分排名第一；
- ✓ 得到部局领导高度认可，正式成为公安部铁路局技术支撑单位；
- ✓ 在此次活动中获得公安部铁路局颁发的感谢信。



中华人民共和国公安部

感谢信

北京众安天下科技有限公司：

为深入贯彻落实习近平总书记关于网络强国的重要思想，进一步提升铁路信息系统和关键基础设施整体安全防护水平，我局于近期组织开展了相关专项工作。

在此次工作中，贵公司作为技术支撑单位，高度重视、精心组织，选派业务能力突出的技术人员参加此次工作，并取得了重要成果，充分展现出贵公司兢兢业业的工作态度和高超的专业技术水平。

在此，对贵公司的大力支持表示衷心感谢！



典型案例：2024年全国铁路行业技术检测比武

活动背景

在数字化时代，网络安全的重要性不断增强，特别是在关键基础设施领域。为了贯彻落实国家网络安全战略、提升网络安全防护水平的重要举措，通过**实战演练检验**和**提升铁路系统的信息安全防护能力**。2024年，**公安部铁路局**联合**郑州警察学院**举办了全国铁路行业实战攻防演练活动，旨在提升铁路行业信息系统的安全防护能力，确保铁路运输的安全与稳定。

18个铁路公安局队伍



4所高校队伍



3支专业安全厂商队伍



公司作为**唯一技术支撑单位**，圆满成功支撑公安部铁路局-2024全国铁路网络攻防演练专项任务，得到公安部局领导高度认可，并荣获**公安部最佳技术支撑奖**、公司**6名骨干**荣获**公安部突出贡献奖**，同时圆满完成了2024年度公安部铁路局常态化攻防演练技术检测专项工作，得到领导高度认可。

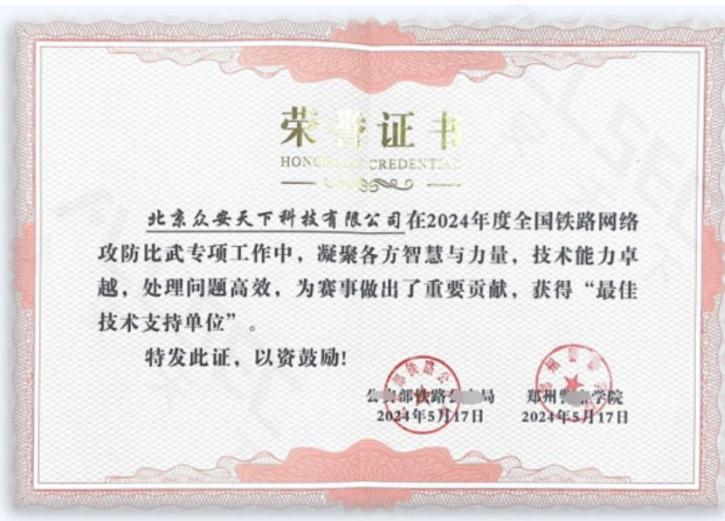
典型案例：2024年全国铁路行业技术检测比武



- ✓ 检验和提升了铁路关键信息基础设施的安全防护能力；
- ✓ 各参演单位在实战中锻炼了队伍，检验网络攻防实战能力；
- ✓ 为铁路行业的网络安全工作提供了重要的技术支撑和经验积累。

价值与认可

- ✓ 为本次技术检测提供了全流程的技术支撑和真实演练环境；
- ✓ 确保演练全程安全可控，保障活动公平高效和顺利开展，得到部局领导高度认可；
- ✓ 在此次活动中获得公安部铁路局颁发的感谢信。



典型案例：2025年铁路信息系统网络安全技术实网检测



为深入贯彻落实习近平总书记关于网络强国的重要思想，勇担网络强国使命，检验中国国家铁路集团有限公司相关部门的网络安全实战能力，进一步提升铁路公安网安队伍的实战能力和铁路关键信息基础设施整体安全防护水平，确保“两会”期间铁路重要信息系统、网络平稳可控，部局首次联合国铁集团共同开展“2025年铁路信息系统网络安全技术实网检测”活动。



检测范围（53家）

北京铁路局、国铁集团本级在京单位：53家单位、148个系统

- 铁路外服网侧漏洞风险摸排、隔离验证
- 铁路内网跨网跨域防护有效性验证

检测目的

- 发现防守单位存在的风险隐患和不足之处，进一步提升网络安全防护能力。
- 以战代训，通过实战检测发现防护薄弱点，提升各防守单位人员网络安全意识，应急响应、溯源处置、调查取证能力。
- 锻炼队伍，提升基层铁路公安网安的网络攻防实战能力和调查取证能力。



参演队伍（8支）

铁路公安局（5支）：北京局、沈阳局、上海局、广州局、南昌局

国铁队伍（3支）：国铁集团信息中心、铁科院、北京局

典型案例：2025年铁路信息系统网络安全技术实网检测



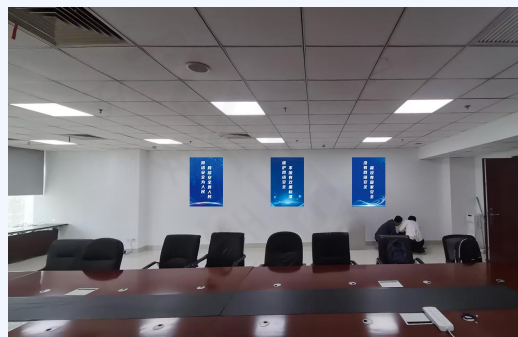
组织筹办

需求调研

方案设计

场地布置

环境搭建



重大成果确认：

同步验证



同步研判



同步处置

实网检测

攻防对抗

溯源取证

研判处置



项目启动



现场比武



领导观摩



成果汇报

公安部铁路局、国铁集团信息中心相关领导现场观摩，听取指挥部做专项汇报工作，对赛事支撑与保障给予高度评价。

ALLSEC

众安天下 · 天下众安



公司公众号

公司官网: www.allsec.cn 电话: (010) 86395035 邮箱: BD@allsec.cn