

洞智安全众测平台

产品介绍

2025年11月



目录

MULU

1

背景

2

产品功能

3

产品优势

4

典型案例

01 背景

```
if (a) {
  for (; o > 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 (; o > 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), 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)), e
},
isArray: function(e, t, a) {
```

当前背景

当前背景

在数字化时代，网络安全的重要性日益凸显，成为国家安全的重要组成部分。我国政府高度重视网络安全，确立了网络安全的法律框架和责任要求，相关政策法规不仅为网络安全管理提供了明确的指导，并强调了实战攻防、安全防护验证、数据安全保护、安全实战评估和人才培养的重要性，为网络安全工作的规范化和系统化奠定了坚实基础。

背景分析

- 响应国家法律法规：**《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规，明确了网络安全管理的法律框架和责任要求
- 加强关键基础设施的网络安全防护：**关键信息基础设施是国家网络安全的中中之重，其安全直接关系到国家安全和社会稳定
- 应对全球和国家网络安全形势：**全球网络安全形势日益严峻，网络攻击手段不断升级



专家谈《网络安全法》草案：是重大历史进步

2015年07月17日 20:43 来源：中国网信网

【打印】

千呼万唤始出来，《网络安全法》草案（以下简称草案）终于同公众见面了。回顾2003年，中办23号文《国家信息化领导小组关于加强信息安全保障工作的意见》便已提出“抓紧研究起草《信息安全法》”的要求，迄今已十二年整，恰如日珣过隙。古称十二年为一纪，《国语晋语四》曰“蓄力一纪，可以远矣”，但功归一载，利在千秋。

专家谈《网络安全法》草案：是重大历史进步

此次草案公开征求意见，表明这项工作进入了实质性立法程序，这是一个重大历史进步。欢欣鼓舞之所在，不是因为草案具体内容，而源于征求意见本身的象征意义。时至今日，我们对网络安全立法不是搞清楚、看明白了，而是问题更多、更复杂了，很多观点分歧可能更大了，网络安全立法难度不降反升，但突破恰恰在此时。中央网络安全和信息化领导小组成立后，中央领导同志英明决策，切实将网络安全提升到了国家安全和发展的战略高度，不但作出“网络强国”的全局战略部署，更扎实推进各项工作取得积极进展。网络安全宣传周、网络空间安全一级学科等，无一不历经多年论证而蹒跚，今朝方开花结果。

专家称《网络安全法》草案兼具综合法与专门法特点

作为第一部网络安全法（《电子签名法》不应计算在内），草案首先要体现综合性，其侧重点应该在以下四个方面：

一是要明确部门、企业、社会组织和个人的权利、义务和责任。二是规定国家网络安全工作的基本原则和理念。三是将成熟的政策规定和措施上升为法律，为政府部门的工作提供法律依据，体现依法治国要求。这首先是政府部门的工作需要（如对境外违法信息予以阻断，实施网络通信管制等）；其次，这些规定和措施往往经过了实践检验，部门间争议较小，有利于提高立法效率。四是建立国家网络安全的一系列基本制度、形成制度框架，这些基本制度带有全局性、基础性，是推动基础性工作、夯实基础能力所必需。

《网络安全法》草案解读：关键信息基础设施保护工作进入正轨

草案规定了关键信息基础设施运营者的安全保护义务，解决了其保护责任模糊不明的问题。他们有必要从国家安全角度承担防护责任，但这个责任毕竟是有界限的。大家希望知道做到什么程度就无责了，也关心自身的权利如何保障。对很多重点行业的信息技术或网络安全部门来说，这不仅仅是免责的需要，也是推动工作的需要，因为这些内设机构如果没有强制性依据，很难得到业务部门的配合。

《网络安全法》

当前痛点

网络安全形式日益严峻



随着互联网的高速发展，一边催生着更多的新经济、新应用，一边也让更多系统漏洞频频爆发。导致企业财产收到严重损失，造成了一定的社会不良影响。

网络安全人才严重短缺



***据新华社报道，我国当前网络安全人才需求预计将超过140万，而每年网络安全相关专业的本科高校毕业生规模仅2万余人**
企业对网络安全人才的需求呈爆发式增长。但是因为市场上安全人才紧缺，所以导致安全人才供应远远满足不了企业的需求

当前
痛点



传统安全服务满足不了现状

传统安全服务费用较高，企业测试范围过多时，需要加大资金投入让安全公司增添人手，承担过高的成本，并且**人才水平层次不齐**，导致无法很好的提供优质的安全服务。**安全服务周期长**，发现安全服务问题，处理不及时，导致效率低下



缺乏标准化管理

目前网络安全众测服务在服务流程、人员管理、平台安全保障等方面缺乏统一的标准，这可能导致信息泄露、测试人员行为不可控、漏洞黑产交易等安全风险。
同时国家相关部门已经发布了《网络安全技术 网络安全众测服务要求》（GB/T 43741-2024），该标准将于2024年11月1日正式实施，旨在规范网络安全众测服务所涉及角色的安全职责、服务流程和要求

产品架构

平台以“洞见全局，智测未来-发挥社区力量，群策群力保障安全”的理念，专注于打造提升安全防御能力的虚拟训练环境，为用户提供高效实用的安全培训和模拟实战演练。

平台从项目管理的启动阶段，通过合规评估确保活动遵循法律法规，利用专项检测和专家管理深化专业服务，到漏洞管理确保漏洞追踪，再到用户管理与人才培养，为企业认证提供信誉支撑。数据后台的强大数据支持与运营管理的高效有序，配合商城管理与信息调度，以及基础设施的稳健技术支撑，共同构成了一个促进用户、企业和平台之间互动与成长的生态系统。通过这一系列紧密相连的服务和功能，洞智平台不仅提升了众测的专业性和效率，也强化了网络安全防御的整体能力。



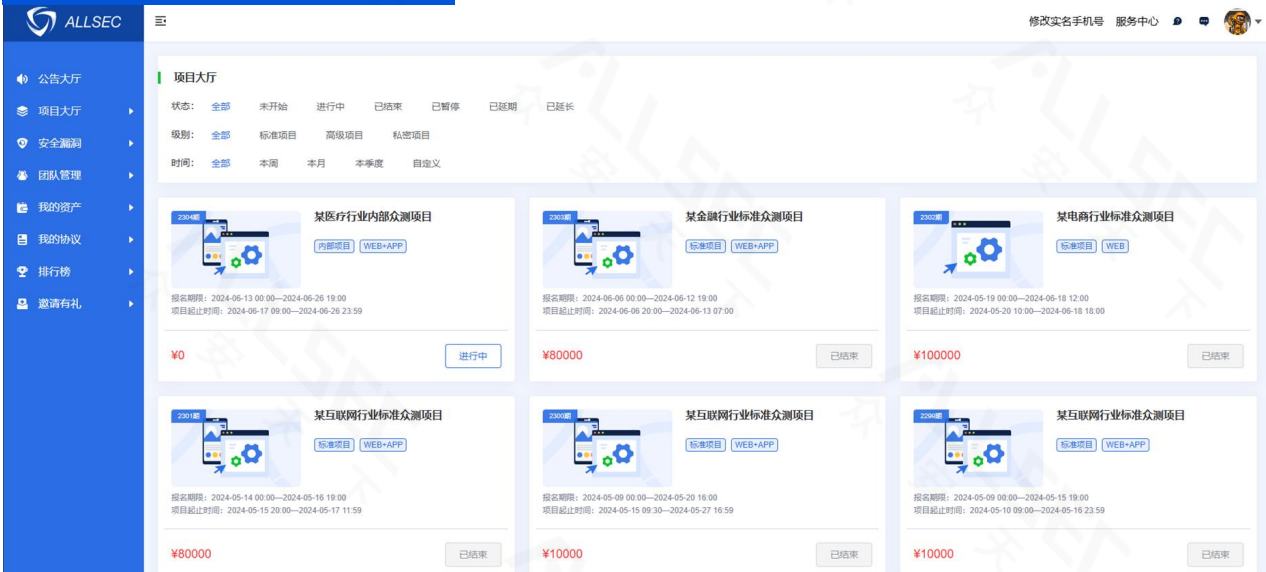
02

产品功能

```
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("\uffu00a0") ? 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)), e
},
isArray: function(e, t, a) {
```

洞智安全众测平台

平台项目大厅界面



功能模块

公告大厅

项目大厅

安全信息

团队管理

资产管理

协议管理

排行信息

成果管理

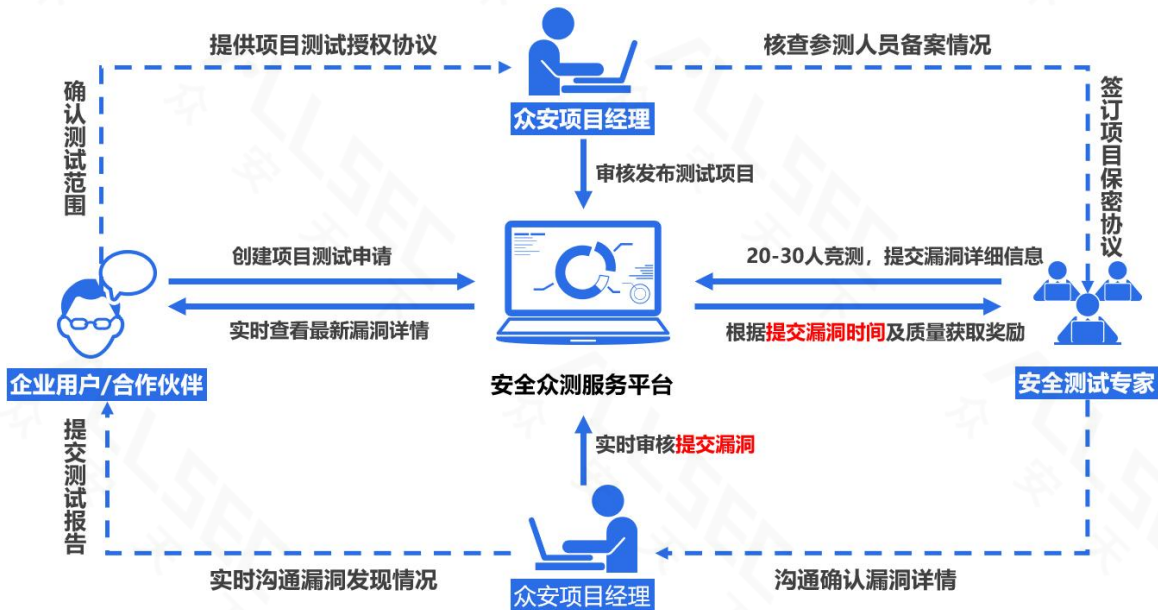
应用场景

企业风险摸底

指定范围测试

专项检查测试

众测服务流程



- 测试成果及发现过程可实时审核 实时提交
- 参与测试项目的测试人员积分排名实时更新展示
- 测试项目的当前状态及当前进度可实时进行查看
- 测试进行中支持流量审计 保证测试过程可回溯

平台角色



系统管理员

ALLSEC平台系统管理员，负责平台日常运行维护。具有高级管理权限，负责对项目工单进行审核、分配安全专家的权限



项目经理

合同指定项目经理，负责整体项目把控。具有与用户或渠道沟通项目情况，对安全专家提交的漏洞进行审核并提供详细修复建议的权限。



安全专家

已经在平台上通过身份认证和考核，完成注册的安全测试人员。具有对已发布项目进行安全测试，提交测试漏洞及漏洞详情的权限。



企业用户

项目所属甲方。具有对项目进度、参与人数、漏洞查看的权限。

主要功能

01 项目管理

通过对项目的创建、发布等实现整个项目管理流程，项目结束后由项目经理点击生成整个项目统计分析报告，反馈给厂商；支持对项目进行创建、审核发布、编辑项目、生成报告、下载报告等功能操作

03 企业管理

系统支持企业用户在厂商端进行企业信息的认证以及更新和维护功能，工作人员可在后台管理系统对企业认证进行审核，并为其分配账号、查询相关企业厂商信息以及对企业信息进行更新与维护，可实现编辑与删除功能

05 运营管理

后台管理系统支持工作人员对平台主要数据进行查询，支持后台管理人员通过信息管理对资源位图片、文章内容、季度榜单、QA内容进行新建、编辑和删除功能。安全专家可对自己的资产进行提现、查看等功能，后台可对提现审核进行处理等功能。同时也支持安全专家对平台进行反馈，对相关的运营规则可查看具体明细等



02 漏洞管理

系统支持安全专家在众测平台系统在线提交所发现的漏洞，项目经理在后台管理系统对漏洞进行审核，企业用户在厂商端对安全专家所提交的漏洞进行导出

04 专家管理

系统要求安全专家获取邀请码后才可登录注册平台，并且实名认证后才可成功注册。登录成功后填写自己的相关技能信息，并且可查看自己签署的协议。平台支持对所有安全专家RANK值进行统计排名并公示

06 调度通信管理

平台支持通过短信、邮件、单点沟通的方式对用户机进行通知、警告与沟通等流程

服务场景

渗透测试服务通过专业的安全团队使用先进的工具和技术，对客户的IT基础设施进行深入的安全检查。

平台通过组织众测活动，邀请外部安全专家参与到客户的安全测试中来。

渗透测试服务

安全众测服务

红蓝对抗服务

服务场景

漏洞排查验证服务

攻防演练服务

暴露面威胁排查服务

通过众测平台组织红队模拟黑客攻击，蓝队负责防御和应对这种对抗演练，帮助客户提高安全团队的应急响应能力和防御策略的有效性。

通过众测创建接近真实的攻防环境，让参与者在控制的风险下学习和实践各种攻防技术。

通过全面的资产发现和漏洞评估，帮助客户了解其攻击面的现状，并提供减少攻击面的建议和解决方案。

专家团队会对客户的系统进行细致的漏洞扫描，确保所有已知的安全漏洞都得到识别和记录。

03

产品优势

```
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)), e
},
isArray: function(e, t, a) {
```

构建多团队协作安全生态，保障数字智能安全发展

云端安全专家团队

6000+已签约白帽专家

金融

政务

工业制造

能源

云计算

互联网

运营商

医疗

交通

高科技

物联网

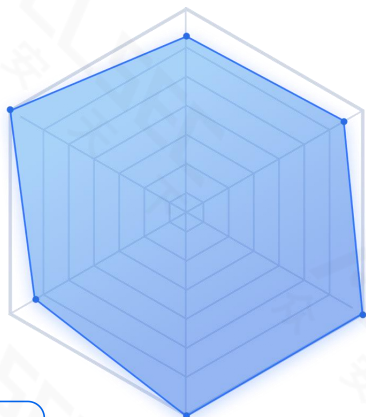
...

行业领域

行业经验

10+平均攻防经验年数

白帽人数



挖掘能力

签约攻防战队 **15+**

攻防战队

移动安全

Web安全

IOT安全

渗透测试

代码审计

逆向分析

暗网监测

数据安全

威胁情报

安全开发

红蓝对抗

...

技术领域

累计发现漏洞 **200000+**

众测智库：30人+（10年+实战经验）

- 汇聚跨行业领域、一线实战型顶尖安全专家与优秀团队领袖
- 持续深耕网络安全众测行业，提供核心技术能力支撑
- 持续探索创新，面向行业用户提供创新服务与核心产品能力

核心安全实验室：20人+（8年+攻防经验）

- 能力标准化研发
- 核心场景需求分析
- 一线专家安全运营，二线专家远程支持

10年+

支持项目实施过程可视化数据大屏展示

平台当前在线人数

当日提交漏洞数量

漏洞数量统计

- 汇总整个项目周期内的所有提交漏洞，以及其中经过研判为有效的漏洞数

漏洞趋势统计

- 通过每日漏洞数量的折线图，呈现漏洞发现的趋势和变化

漏洞数量统计

- 根据漏洞类型进行分类统计，列出数量最多的前五种漏洞类型，为安全策略调整提供方向



漏洞系统Top5排名

- 将发现漏洞最多的前五个系统列出，有助于针对性地加强这些系统的安全防护

安全专家地域统计

- 以地图形式展示参与本次项目的安全专家分布地域，增强团队间的协同感

安全专家Top5排名

- 根据每位安全专家提交的有效漏洞数量和成果贡献，列出前五名，激励团队士气与工作热情

漏洞提交实时动态

- 实时滚动展示安全专家提交的最新漏洞简要信息，便于企业客户实时查看并修复中高风险

核心亮点：调配人才资源



调配专家团队

凭借其调配攻防人才资源的能力，拥有一支经验丰富、技术背景深厚的专家团队

提供定制化解决方案

能够迅速响应客户需求，快速组织专项团队，针对不同的安全场景和挑战，提供定制化的解决方案

增强客户网络安全防护能力

核心亮点：支持常态化安全评估

● 定期安全检查

支持通过定期的安全检查和漏洞扫描，持续监控和评估系统的安全状况

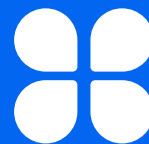
● 常态化安全评估

常态化的安全评估有助于企业建立起一套动态的安全防护机制，能够在安全威胁出现时迅速响应，减少风险暴露时间，确保业务连续性和数据安全

安全检查

漏洞扫描

安全防护机制



优势亮点：发挥众测社群社区力量



● 通过开放式的协作模式，充分发挥众测社区的力量，组织众测活动，激发社区成员的积极参与

● 利用社区的集体智慧和广泛技术专长，加速了漏洞的发现和处理速度

● 鼓励社区成员贡献自己的知识和技能，能够更全面地识别和修复安全问题

● 提高了安全测试的效率，促进了知识的共享和技术的创新

优势亮点：支持护网重保专项

制定响应计划

通过深入分析客户的网络安全状况，制定针对性的应急响应计划，确保在面临安全威胁时能够迅速有效地应对



加强安全措施

服务还包括加强安全防护措施，如加固系统漏洞、提升访问控制和加强监控，以构建更为坚固的网络安全防线

确保关键信息基础设施在高风险期间的安全稳定运行

应用场景-智慧城市安全监测系统部署



众测平台为智慧城市的建设提供全面的网络安全监测服务。通过部署先进的安全设备和系统，实时监控城市关键基础设施，如交通控制系统、公共安全摄像头和智能电网，确保城市运行的安全性和稳定性。平台利用红蓝对抗演练，模拟各种网络攻击情景，提高城市应急响应和危机管理能力，保障居民生活安全。

全面监控 应急响应 红蓝对抗

应用场景-医疗信息系统安全加固与维护



全国标准信息公共服务平台
National public service platform for standards information

标准信息一网打尽

首页 国家标准 行业标准 地方标准 团体标准 企业标准 国际标准 国外标准 示范试点 技术委员会

网络安全技术 网络安全众测服务要求
Cybersecurity technology—Requirements for crowdsourcing security test services
国家标准 推荐性 即将实施

国家标准《网络安全技术 网络安全众测服务要求》由TC260（全国网络安全标准化技术委员会）归口，主管部门为国家标准化管理委员会。

主要起草单位 国家计算机网络应急技术处理协调中心、中国电子技术标准化研究院、国家信息技术安全研究中心、阿里云技术有限公司、奇安信网神信息技术（北京）股份有限公司、中国移动通信集团有限公司、中国科学院软件研究所、上海斗象信息科技有限公司、北京天融信网络安全技术有限公司、中通服咨询设计研究院有限公司、上海文鲸信息科技有限公司、蚂蚁科技集团股份有限公司、杭州安恒信息技术股份有限公司、北京市政务安全保障中心（北京信息安全测评中心）、北京东方网信科技有限公司、北京众安天下科技有限公司、北京奇虎科技有限公司、中国工业互联网研究院、启明星辰信息技术集团股份有限公司、北京数字观星科技有限公司、中国电子科技网络信息安全有限公司。

发布于 2024-04-25 实施于 2024-11-01

当前标准

GB/T 43741-2024 即将实施

网络安全技术 网络安全众测服务要求

针对医疗行业信息系统的敏感性和重要性，提供专业的安全众测服务。通过模拟黑客攻击，发现并修复潜在的安全漏洞。同时，平台支持常态化的安全评估，帮助医疗机构建立起一套完善的信息安全管理体系，防范医疗数据泄露和网络攻击，保障医疗服务的连续性和安全性。

漏洞修复 信息管理 数据保护

应用场景- 教育网络环境安全优化方案



利用众测平台进行教育类应用或服务的测试。包括对在线教育平台、教育软件、学习管理系统等进行测试，以确保它们在不同的网络环境下都能稳定运行，满足教育学员的需求。众测平台通过招募和组织大量的志愿者或专业测试人员，对教育应用进行实际使用和测试，从而发现并报告可能存在的问题，提高教育网络环境安全

04

典型案例

```
if (a) {
  for (; o > 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 (; o > 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("\uff\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)), n
},
isArray: function(e, t, a) {
```

建设国家级众测平台

案例标签

行业安全能力 安全人才 安全生态



项目背景

工业互联网整体还处在发展初期，安全管理水平和安全防护水平相对较差，随着新一代信息技术与制造业的加速融合，传统网络安全威胁持续向工业领域渗透和蔓延，工业信息安全漏洞频发，工业信息安全形势日趋严峻，对于维护国家安全、社会稳定、企业安全生产带来更大挑战。



客户痛点

- 互联网安全涉及工业控制、互联网、信息安全三个交叉领域，面临传统网络安全和工业控制安全双重挑战。自从震网病毒被发现至今，针对工业控制系统进行破坏活动的网络攻击就一直没有停止。
- 工控系统在互联网上的暴露问题是工业互联网安全的一个基本问题。所谓暴露，是指我们可以通过互联网直接对某些与工控系统相关的工业组件，如工控设备、协议、软件、系统等，进行远程访问或查询。同时工业互联网系统普遍存在安全漏洞，特别是底层的控制主机和工业控制系统操作站的安全漏洞数量在逐年上升。
- 虽然很多工业企业虽然有IT组织负责IT网络安全，但其在安全意识和培训计划中，往往会忽视IT和OT之间的差异；IT安全人员因为自身对工业系统安全知识的缺乏，很少会对OT人员进行安全培训，OT人员的信息安全培训普遍缺失。

建设国家级众测平台

案例标签

行业安全能力 安全人才 安全生态



技术及平台建设

安全技术支撑

利用攻防能力优势，支撑各项安全检查工作，协助工联院落地行业内重要的安全工作。

- 运营商远程检查
- 其他专项支撑
- 合规与现场检查
- 攻防演练支撑

行业级平台建设

建设完成首个国家级工业互联网安全渗透测试与众测服务平台。并协助统筹6大子系统的验收对接工作，**圆满完成平台建设及交付验收任务。**

- 承担平台核心系统建设
- 平台安全运维
- 助力大平台交付验收
- 重大活动保障支持



工联众测平台运营

利用运营优势，支撑各大众测项目活动及平台生态运营，提升平台在业内的知名度。

- 安全众测项目运营支撑
- 企业厂商生态运营
- 白帽专家生态运营
- 工联大讲堂运营支撑



安全赛事及市场活动运营技术支撑

利用在攻防赛事活动的经验优势，支撑各大安全赛事活动及市场活动，助力多项活动**圆满收官。**

- 2022-2023年车联网安全赛事
- 特聘专家邀请活动
- 众测平台专项活动：公益行
- 市场活动运营

建设国家级众测平台

案例标签

行业安全能力 安全人才 安全生态



效果收益



白帽专家生态运营

工作内容：负责构建和维护一个健康活跃的白帽专家生态系统，包括专家招募、社区管理和激励机制的设立。

工作成果：成功邀请1000+用户和众多安全战队的加入，为平台提供了强大的技术支持和资源。



企业厂商生态运营

工作内容：设计合作方案、邀请企业参与以及用户对接，以促进企业与平台之间的有效合作。

工作成果：成功构建了一个多元化的企业合作网络，为平台带来了广泛的行业支持和资源。



安全众测项目运营支撑

工作内容：为各项众测项目提供了全面的漏洞审核和项目技术支持。

工作成果：确保项目的顺利进行和高效率的漏洞发现，成功地识别了大量关键漏洞，促进了安全社区的积极参与。



工联大讲堂运营支撑

工作内容：负责大讲堂的运营策划和专家邀请工作，确保内容的高质量和吸引力。

工作成果：成功举办了多场行业内具有影响力的讲座和研讨会，提升了平台的品牌影响力。



谢谢大家