

第十八届全国大学生信息安全竞赛—作品赛初赛团队名单

序号	团队名称	作品名称
1	比特守护队	ATWatch: 基于动态图神经网络的金融异常检测系统
2	主动指纹	伪装者-射频指纹识别攻防研究与实现
3	零日突破	基于深度学习的射频隐写技术探究
4	C++20 标准委员会	“獬豸”: 基于高效函数秘密分享的轻量级可扩展电子投票系统
5	another sky	基于双服务器的空间 skyline 安全查询方案的设计与实现
6	啊队	QOQDefender: 低成本高效发展的分布式恶意软件检测系统
7	今天你摆烂了对不对队	隐心智链: 基于匿名加密与大模型的心理守护平台
8	sky	链盾智检 - 基于区块链与 AI 的智能合约安全检测系统
9	什么档次和我一队	DroneSentry: 基于射频指纹的非法无人机小样本开集识别系统
10	Explorer	AICodeScanner
11	Penghu Bay	基于词素匹配的恶意域名检测
12	盘古 666	智能网络安全攻防实验场
13	羚锐狮	基于连接复用的高速网络协议模糊测试系统
14	NK-Vertex	面向向量数据库的自适应数据水印系统
15	ice	基于扩散模型的边缘-语义协同优化的鲁棒可控水印
16	云枢御险	基于深度学习的网络攻击检测系统
17	安全堡垒	链识智鉴——基于区块链与数据算法驱动的智能合约身份认证系统
18	无人机侦测队	蜂鸟电磁眼: 便携式的无人机射频智能监视系统
19	想不出名字是不对的	隐私可审计跨境微支付系统研究
20	HPU	HPU
21	卫星无线电监测与对抗仿真系统	卫星互联网无线电智能监测与对抗仿真系统
22	havaidea	面向漏洞检测模型的智适应安全防护增强方法
23	图智流光	基于可编程数据平面的加密恶意软件流量识别
24	一支笔	120
25	猛攻鼠鼠队	隐波缉影——基于电磁波衍射模型的低成本隐藏摄像头定位系统
26	BioSignature 靠脸吃饭	基于人脸的安卓模糊密码系统
27	云帆 NSN_东山	智析恶意, AI 御毒——基于大语言模型的自动化恶意软件行为解析系统
28	390 安全	基于 AI 的跨平台多模态社交网络用户隐私分析与保护系统
29	真页	智链安盾——基于链式思维与反馈闭环的代码漏洞智能修复系统
30	重生之我在武工大学密码	同态加密下的多模态安全融合分析系统
31	CO_OD	“獬豸”-自动化应急处置 AI 智能体系统
32	711	GUIAgent 安全评测平台
33	智能鹰眼	智能鹰眼——隐私有好的端侧大模型反诈助手
34	代码敲到失联	基于无害化后门的 RAG 数据库水印技术
序号	团队名称	作品名称
35	火眼金睛	镜鉴 AI: 多模态生物信号驱动的反伪系统

36	匿名恢复取证队	匿名安全和强追溯的分布式数字取证系统
37	二一队	SecureIoT-Guardian: 基于国密算法与 PUF 技术的轻量级物联网综合安全保障系统
38	随便组个队	DumpMind: 多 Agent 驱动的 Kdump 自动化分析平台
39	弗雷尔卓德队	SecAgent-基于 MCP 的网络安全智能体系统
40	Tyche's blessing	人工智能模型的数据投毒检测
41	深藏 blue 队	基于 SM4 和 OPT 的隐私保护中学生学生成绩方案的设计与实现
42	完成主义者	真盾卫士——AI 内容可信检测系统
43	抱佛脚	AndroAnalyzer: 基于图表示学习的安卓恶意软件检测系统
44	龙盘队	ProtoMind——基于大模型的智能协议解析与自动化测试系统
45	老当益壮	密链: 面向区块链数据共享的可搜索加密索引系统
46	Family Guys	智翼空链——基于深度强化学习与后量子密码的 eVTOL 空域管理系统
47	东里四小只	大语言模型驱动的移动应用密码技术安全审计系统
48	V2X	V2X-Safer: 大模型生成场景驱动下的 V2X 车路协同 ADS 安全检测系统
49	shield	智界-深度学习模型隐私风险评估与安全防御系统
50	304	JustOneLab: 更懂小白的网络安全漏洞综合实验场
51	流量哨兵巡航队	支持流式轻量测量与多维扩散异常检测平台
52	到此一游	AI 赋能的全栈式多功能 Web 应用渗透测试系统
53	格幻致知	《格幻致知——通用型 LLM 全幻觉检测系统》
54	极光实验室	"Z-lucky"网络安全运维管理平台
55	云格密码局	云格致安——基于理想格的云存储数据共享与审计方案
56	图像隐写	基于 AIGC 的构造式图像隐写算法设计与系统实现
57	好好好好运来	安安安安全
58	双鸭山分鸭	穹御——鸿蒙终端应用加固系统
59	GraphSec 研创队	基于异构图和强化学习的欺诈交易异常检测系统
60	神经防火墙	MoodLock——基于多模态特征解耦与同态加密的情绪隐私安全计算方案
61	坚实密码队	请
62	少年先疯队	鸿痕——基于深度排序哈希网络和特征哈希算法的人脸认证系统
63	安全	安全
64	FortFi 小队	帧行密护——基于 BFI 无线感知的人体行为识别与隐私保护系统
65	0Day Phantom	面向零日攻击的高鲁棒网络威胁检测平台
66	MulCryptDB	MulCryptDB: 面向语义检索的多模态加密数据系统
67	N05ec	SiFSafer: 基于说话人无关特征驱动的深度伪造攻防平台
68	重生归来全世界计算机水平倒退队	基于区块链的医疗数据安全共享平台
69	信息不安全	基于神经元剪枝的 NeRF 水印算法
70	DeepGuard	融合 DeepSeek 的安全文件传输服务
71	七么么	基于扩散模型的网络安全自动化响应系统
72	ChainWatchers	RAGFlow: 基于大模型跨模态语义增强的智能合约攻击检测系统
序号	团队名称	作品名称

73	Samepursuit1	基于集成学习与深度神经网络的 PE 恶意程序检测系统
74	天幕	隐盾 Sentinel: 多源融合驱动的城市风险检测与智能防控系统
75	无线指纹侦探	Signal Detective——基于 ESP32 的 MAC 地址随机化环境 WiFi 射频指纹识别系统
76	补包侠	PackPatcher
77	110406	基于蜜罐的智能攻击溯源系统
78	开饭手马克	基于耳道内提取心音的身份认证系统
79	智鉴网纹小队	智瞳安网——基于设备指纹的以太网终端接入识别系统
80	星零智御	星零智御—基于零信任架构与联邦学习的抗量子卫星通信安全系统
81	Deepwater	“数安天眼”-基于区块链可信技术的敏感数据全链路安全防护系统
82	NBUT	基于全同态加密的去中心化肺炎识别系统
83	R@dar202501	基于 Windows 平台的网站漏洞检测与安全保护系统
84	好像被资本做局了队	PrivScope: 小程序隐私合规检测系统
85	内生安全云资源研究小队	基于内生安全的网络云资源节点选址研究
86	SafeDrone	SafeDrone-无人机智能规划与自主导航的安全测试与防御系统
87	望尘莫及队	web 安全漏洞与敏感数据双引擎自动化检测系统
88	奶龙本龙	基于多粒度级联森林优化算法的网络入侵检测——智能家居
89	HIT-威胁情报	威胁慧眼-知识驱动的智能威胁情报构建和分析平台
90	呵呵盒	SecRAG: 可信检索增强生成系统
91	签与签寻	后量子安全的分布式数字签名系统
92	荆州勇士队	视界增强——基于对抗训练的目标检测模型鲁棒性强化系统
93	秃击队	纹藏·墨契-基于 AI 生成与模型水印的数字文创 IP 孵化与版权保护平台
94	安全大模型	基于大模型实现的日志异常检测系统
95	gdsfg	7689
96	Sevia	SemAuth: 基于语义的用户身份认证系统
97	说什么都对	ModelShield: 端云协同架构下的小模型端侧安全部署与反窃取系统
98	BASE	链信通-基于区块链的可信数据交易平台
99	摸鱼突击队	移动应用第三方信息共享隐私威胁检测系统
100	端点星队	GaiaDB-支持 SQL 查询的密文数据库系统
101	肖申克的末日	FluidGuard: 面向多场景的大模型越狱攻击检测与防护系统
102	薛定谔的信用	PriTrace: 隐私保护的溯源信贷审批系统
103	仁至义尽队	智空协同: 面向空地融合的无人机目标识别系统
104	比特护卫队	隐枢: 基于区块链的跨系统数据安全共享与隐私计算平台
105	nb666	Silenaud: 针对移动设备远程控制诱导诈骗的智能风险预警系统
106	Crystal	量锁阡玘: 车规级 PQC 算法融合与硬件加速系统
107	绿色心情	DP-Shield: 基于差分隐私的网络侧信道攻击防护系统
108	南瞳	Lattice-dateagg: 智能电网中基于格的数据聚合方案
109	廉洁自律	基于后量子密码算法的云存储文件保护系统
110	IMUST-SEC	基于 ai 研判的主机与系统安全程序
序号	团队名称	作品名称

111	提示词炼金队	智盾·双擎-基于动态裂变的无监督越狱攻击防护系统
112	拉着无人机起飞队	RL-Chain:可靠轻量的无人机区块链数据共享系统
113	Disruptor	基于路径交集减小与不变量引导的补丁定向模糊测试系统
114	故障机器人	系统安全和可信密码结合的车联网 AI 应用数据安全保障系统
115	NewsPursuer	MASPom:多智能体架构下大模型舆情监测与分析系统
116	Star	面向智慧水利的跨机构数据智能平台
117	Sp4rk1e	基于优化并发的网络安全训练与竞赛平台
118	rozer1 队	时空密网——基于多粒度时空图卷积技术的加密流量威胁检测系统
119	转移重心	FlowMind-X:基于 Tai-e 与大语言模型智能融合的 WEB 漏洞数据流分析与挖掘系统
120	PrivSeek	PrivSeek:基于秘密分享的轻量级大语言模型密态推理系统
121	CTF 从入库到删库跑路	AI 砺刃网安实训平台
122	重生之我要拿国一	流光防护——为您的信息安全保驾护航
123	AI-AntS	M-FUSE:面向多层次安全的高效数据隐私融合计算平台
124	海底小小纵队	虚实结合——WiFi 无线感知与流量分类下的人体行为画像
125	R@dar202504	基于 C/S 架构的用户上网行为管控平台
126	羊村守护队	羊村守护队
127	影码视界	隐码视界
128	何不归乡	知识库与人工智能赋能的分布式入侵检测系统
129	待机中队	医域智穹——隐私协议语义感知的医疗数据可信中枢
130	VulnXploit	PDM&Fuzz:基于扩散模型的协议漏洞自动化挖掘系统
131	TL404	数维链——区块链+AI 双轮驱动下的数据层级确权与安全流通平台
132	123666	创新发展
133	鉴伪先锋	鉴伪先锋——辨真伪狙击虚假影像
134	Velvet	融入大模型的代码安全审计工具
135	丝绒	基于 DGA 与机器学习的多模态恶意域名识别哨兵
136	5ufferNarRat0r	漏洞猎鹰 VulnFalcon——精准漏洞根因定位系统
137	压力队	天盾-智能反恐侦察车
138	FireEye	“火感天眼”-基于异构感知与 SAC 强化学习的火场预警、逃生与救援系统
139	航电智算	基于航空宽带通讯系统安全防御
140	R@dar202502	基于指纹认证的 Kerberos 认证系统
141	Thunder	溯链星眸:大语言模型驱动的 APT 供应链攻击检测与溯源系统
142	影安未来	影安未来-面向人脸安全分析的 AI 攻防靶场平台
143	TriVerse	WiFiRescue——基于 WIFI 感知的风险识别与智能救援系统
144	白捡 0day	强化学习驱动的 MQTT 动态安全护盾平台
145	密码破的都队	《面向移动车联网的匿名凭证认证系统》
146	SPX	基于 SPHINCS+的抗量子门限签名及冷钱包应用
147	南波万	基于同态加密的隐私保护数据挖掘技术
148	AAA	联邦学习本地模型贡献度评估机制
序号	团队名称	作品名称

149	粉红色的回忆	天禄：面向大语言模型的自动化安全测试系统研究
150	名加盐防止碰撞	DShareGuard-面向智慧路网的数据安全感知与共享系统
151	从容应队	NetDefender——基于深度学习的恶意流量智能检测平台
152	棱镜安全小组	历史信息驱动的 JVM 缺陷检测技术
153	恐龙抗量子小队	后量子匿名证书方案
154	yit-网络安全	云析眼
155	YMLI	基于 ResNet 和 Transformer 的人脸伪造识别系统
156	MICS LAB	WaterVeil——基于 UDH 编码驱动的屏摄鲁棒可溯源水印系统
157	AI 医疗团队	赛克科技-基于人工智能的肺功能质控及结论判读检测
158	别拿脸蒙我	VeriFace：基于多模态融合的抗 Deepfake 攻击身份认证系统
159	一八一八队	基于大模型反幻觉增强技术的代码漏洞挖掘系统
160	云想小队	源御——基于 iOS 的移动网络入侵检测系统
161	404 NOT FOUND	基于 CNN-TCN-Attention 混合神经网络的新型入侵检测系统
162	盐水鸭 Carry	CANGenius——车载 CAN 总线智能模糊测试系统
163	vivo50 就很队	MediShard-基于分片区块链的医疗保险高效异地结算方案
164	喻家山代码纹析组	CodeSleuth：基于代码风格指纹的软件供应链安全智能感知与溯源系统
165	海底大纵队	基于算术编码和双重预测的密文域可逆信息隐藏系统
166	好好学习	恶意域名检测
167	伏羲矩阵	基于动态行为建模的银行客户异常交易实时智能风控系统
168	R@dar202503	分布式网络资产探测及处理系统
169	雨中奔跑	基于云边端链协同的物联网零信任安全管控系统
170	微笑面队	瞳驭——高速公路场景下多模态感知与实时预警系统
171	超人人强和波比队	SDN 架构下 Floodlight-Mininet 的 DDoS 检测防御系统
172	InkSec	支持双重版权保护的结构化数据水印平台
173	历史队名	基于国密算法的电子邮件加密系统
174	无言以队	BlockCharge——基于群签名和零知识证明的区块链充电支付系统
175	Defvoid	声智禁拟——音频数据不可学习
176	白马程序员	大语言模型生成式安全自对齐训练评估平台
177	Robuster	LiteGuard：基于高效单帧图像与时序残差分析的轻量级深伪检测 APP
178	安全第一队	基于可分离图卷积与序列建模的加密流量检测系统
179	桂花乌龙茶	风云慧聚——气象大模型助力光伏发电预测系统
180	那一天的忧郁	“心安私语”——基于分级加密的多模态智能体隐私防护系统
181	启明枢机	基于人工智能大模型的隐私数据防护
182	灵码神盾	AegisCode——上下文感知驱动的项目级安全增强代码自动生成系统
183	UltrasoundGuard	声盾：智能音箱近超声隐身防窃听系统
184	月落青山去	基于触碰行为和生理特征融合的安全指纹认证系统
185	牛牛就是牛	「智镜·无垠」——基于知识图谱与 DeepSeek 的全维度反诈中枢
186	大锦鲤	隐士——面向隐私保护的智慧视觉系统
187	天奕·天眼追光队	面向动态威胁感知的加密通信系统设计
188	凭证卫士	小程序凭证泄露检测平台
序号	团队名称	作品名称

189	宝宝巴4队	近虹天鉴：基于红外虹膜反射的人脸活体检测系统
190	ID 防火墙	面向人脸定制化生成模型的主动防御系统
191	AIGC 水印检测	面向 AIGC 的溯源水印嵌入与检测系统
192	光锥之外	智能语音应用的窃听漏洞分析及防护系统设计
193	AIFBI	智盾卫士——多模态大模型量化部署安全管家
194	Zero_Hero	面向智能设备零权限传感器的安全防护者
195	定坤	安全之钥-轻量级密码算法的唯密文故障分析软件
196	人民当家做组	智链盾——基于机器学习的多维度智能合约漏洞检测系统
197	数网恢恢监管队	分布式可信安全的数据流转系统
198	VulRator	VulRator-基于模糊学习的函数级别漏洞挖掘和搜索模型
199	校园影卫	《钓影缉毒——高校网络威胁的智能识别与处置》
200	驾校保卫处	玄鉴-MirrorNet：区块链赋能下的网络安全事件记录分析服务系统
201	SM9 信安攻坚队	基于国密 SM9 的通用身份认证与加密通信系统
202	小纵队	鉴真-智能检测伪造人脸
203	格外有本事	基于人脸密态识别的智能远程安全控制系统
204	深藏 blue 队	D&S IoT-基于动态函数级模糊测试和静态分析的物联网漏洞发现系统
205	理工神盾局	日新钥异：长期服役物联网安全无线密钥生成系统
206	大卫说得队	支持多模态的大模型安全等级评测与加固系统
207	阿玛特拉斯	SmartPatchAnalyzer：基于大模型的二进制漏洞 Patch 对比与代码审计系统
208	极客	灵穹麒麟漏洞全息感知系统
209	时时刻刻检索队	限时可验和高效的安全数据检索系统
210	PSGvsARS	基于灰盒模糊测试技术的智能合约漏洞检测系统
211	AutoHacker	基于大模型的网络自动化渗透与安全加固系统
212	美少女队	BERT-DGA：基于 LLM 的恶意软件动态生成域名感知与检测系统
213	Poker Face	Vehicle IDSor——基于深度学习的智能网联汽车 SOME/IP 协议实时入侵检测移动平台
214	珞珈喵喵虫队	通感识面：多模态特征增强的安全人脸认证系统
215	无影无踪导航队	支持无序途径点的准确高效不经意导航
216	SunnyDay	智盾哈希——基于深度哈希技术的恶意软件检测平台
217	顶个诸葛亮	Oday 挖掘
218	没人比我们略懂网安	模型风险雷达：基于成员推理的机器学习模型数据泄露风险诊断系统
219	尝尝咸淡对不队	零鉴溯影——零信任驱动的工业互联网内部威胁溯源系统
220	xjtu 队	面向信息安全试验的网络攻击负载生成技术
221	BSXYY	基于国密算法的 CA 认证中心
222	海底超级小纵队	PassAgent：基于大语言模型的个人全能口令助手
223	水印工厂	基于水印变换的 AI 生成代码识别和溯源系统
224	无孔不入	LLM-PenGuard：大语言模型驱动的智能渗透测试系统
225	Achieve Science	智能电网中隐私保护的用户参与式细粒度电器级需求响应系统
226	啊对对队	WEB3 智能合约安全审计 AI 工具
序号	团队名称	作品名称

227	溯古弘文	诗钥密令——基于文化遗产与网络安全融合的诗词智能伴学 APP
228	ncc 第一大队	BinSentin31: 基于三体智能协同的内生安全缺陷哨兵系统
229	伏甲	伏甲: 基于大模型的工控软件漏洞挖掘平台
230	SynSec	CyberGuard——基于多模态数据可鉴伪的身份认证与安全态势分析系统
231	请来使用我们的脱敏工具吧	DataMasker: 面向多场景的个性化数字隐私保护方案
232	固界巡安	固界巡安——面向关基设备的海量固件安全分析系统
233	我们是第一队	A-Shield: 面向智能对抗攻击的自适应网络入侵检测系统
234	TalentChain	智链诚聘——长安链赋能新型网络招聘系统
235	代码写的都对	基于低成本 ESP32 的 WiFi 终端高安全性身份认证技术
236	SecureFuzz	SecureFuzz——智能合约链上漏洞模糊检测系统
237	gostgogo	基于跨模态语义交互的社交媒体虚假新闻检测系统
238	安全小分队	网络安全意识培养与培训平台
239	我没有这个天赋	电力网络空间测绘与攻防模拟系统
240	我竟无言以队	智眸勘真——面对新闻场景的伪造检测平台
241	啊对对对队	声鉴未来——电信反诈智能平台
242	钥你好看队	基于国密的隐私增强认证与密钥协商协议
243	地破稀客说能赢	MCPGAP: 基于模型上下文协议的综合安全治理与审计平台
244	百事可乐	ASCENT: 基于 DID 的供应链数据可信流通管理平台
245	江大码到成功队	SafeIDS: 基于数据增强和集成学习的网络入侵检测系统
246	JCC	基于大数据的威胁情报并行挖掘预警平台
247	TruthAgent	TruthAgent: 面向社交平台的 AIGC 谣言检测与舆情传播干预推演系统
248	拖延症不队	高熵的物理层密钥生成及安全性评估
249	ee3a	ee3a
250	一眼盯真队	深瞳——基于深度学习的伪造人脸替换检测系统
251	智行乐学队	基于 GO 语言的编码神器--goendecoder
252	量子 Q 队	基于 QSVM 算法的网络攻击行为识别系统
253	Cyber Team	Cyber Range CoGenius: 面向网络靶场的多智能体细粒度虚拟场景生成系统
254	Ave Muguizi	基于联邦安全的工业互联网 DDoS 防护系统
255	TraceRing	明真-基于国产开源多模态大语言模型的可解释图像鉴伪
256	智盾团队	智盾隐投——基于门限环签名的抗量子攻击电子投票系统
257	皇室大超骑	“护网先锋”企业安全自查任务助手
258	Spark	鸾鸟网安——智能网络攻防一体化平台
259	智测先锋	洞玄: AI Agent 驱动的智能系统安全风险评估平台
260	超级无敌大苹果	SafeGuard: 融合数据增强和对比学习的异常流量识别平台
261	兑兑队	CybeXpert-基于混合专家架构的多维度网络安全大模型
262	我爱学密码队	DataShieldX: 安全且高效的电子身份证查询统计系统
263	PPSUC	基于对抗性隐喻的语言模型越狱攻击
264	奶龙和胖猫	基于机器学习的恶意威胁检测系统
序号	团队名称	作品名称

265	醉把佳人成双队	DDoS 动态防御系统
266	新和联胜	图鉴天工——多功能遥感安全检测与应用平台
267	少年侦探团	状态转换漏洞：一种新的 Web 竞态漏洞发现与检测
268	Safe Call	智警通：基于多种机器学习模型的欺诈识别预警系统
269	洞玄	洞玄：基于 bert 模型的固件漏洞检测系统
270	星链工坊队	灵哨智御——面向不平衡数据分析的网络入侵检测系统
271	梅纹畫	“哨戒”基于 UWB 区域信息 AI 智能防护
272	我想上啊	OA 漏洞探测工具
273	AEGIS	ICS-Aegis：基于多智能代理的工业控制系统自动化漏洞验证系统
274	四个人	守护者-应急响应与缺陷管理系统
275	不想丸了	基于 CTF 的网络安全竞赛平台
276	比完开派队	FALCON：基于大模型的多智能体工控固件漏洞检测系统
277	VideoGuard	VideoAthena——基于数字水印与深度学习的视频异常篡改多维度自动检测系统
278	dfseeker	慧眼识流-基于深度学习的网络流量监控与威胁告警系统
279	200 OK	SonicGuard：基于对抗扰动的语音隐私主动防御系统
280	三抓三坚持	基于 AI 与规则对比分析的网络入侵检测系统
281	打饭不被插队	睿眸-智能恶意威胁分析系统
282	backguard	“灵哨”大模型安全检测平台
283	老谢野混沌	VoiceGuard——多模型韵律保持语音防护系统
284	AIsec	AIGCGuard：面向动作引导式不合规内容的检测与修复系统
285	北京邮电大学网安院	基于 bilstm 的恶意流量检测系统
286	为什么要演奏春日影	基于扩散模型的可恢复图像安全保护系统
287	契科夫	隔纱辨影——基于可搜索加密的精准密文检索
288	智御威胁	插件盾——动态威胁感知防御
289	清源	基于文本特征分析的过滤系统
290	我说的都队	基于 eBPF 与异构溯源图的攻击检测系统
291	用实力牵制监管者 180s	基于 LLM 的入侵检测与蜜罐诱捕系统设计
292	OsirisFreya	基于 DeepSeek 大模型增强的 ETW 动静双模态协同防御反勒索系统
293	守门人小队	基于工业物联网的轻量级开集入侵检测系统
294	队名五个字	ChamVerDB：基于变色龙哈希验证的加密外包数据库方案
295	网联智盾	面向 C-V2X 的智能网联汽车高安全不可克隆认证技术研究
296	安全无处不在	安全无处不在
297	汪汪先锋队	智途安行——车路云一体化态势感知入侵检测系统
298	少年先锋队	安全增强型一键部署式代码缺陷分析系统
299	老辈子说得队	智守书阁——基于信息安全的高校图书馆智慧管理系统
300	Dawning Future	PassMind：大模型驱动的可演进口令强度评估系统
301	EchoSentinel	EchoSentinel：面向短视频平台的数字人视频风险感知、监测与评估系统
序号	团队名称	作品名称
302	云蜜	云蜜链——对抗 APT 隐蔽渗透威胁的自适应欺骗防御系统

303	SuperIdol	绘隐鉴权—支持用户端预览的版权图像共享平台
304	干饭不想排队	LLM-HWfuzz:大语言模型赋能的硬件模糊测试平台
305	gogogo 出发咯	基于中间语言跨编译配置的智能漏洞检测平台
306	汪汪队	智能轻量化 Web 安全深度检测引擎
307	The Watchers	基于认知隐蔽性的社交媒体隐写检测系统
308	三缺一不可	FideModPUF: 基于可靠性建模的 PUF 性能测评系统
309	网盾探隅信安赛	网盾探隅_智能网络安全攻防演练靶场与威胁响应平台
310	超高校级的信安 F4	FLARE: 面向商用大模型的事实与逻辑双通道幻觉检修系统
311	小熊维尼和小猪皮杰一队	AI 安全棱镜——具身 LLM 系统的攻击链预演防御平台
312	VulTeam	VulTracer: 基于大模型提示词增强的源代码漏洞检测系统
313	叻鉴星躔	CTICopilot: 基于 AgenticRAG 的网络威胁情报分析智能体
314	safeguard	MultiGuard——基于多维特征融合的人机检测
315	Bug 别和我作队	DeepAegis:基于大模型的全自动渗透测试平台
316	弹弹弹性	面向服务与流量双重欺骗的弹性蜜罐防御系统
317	这海星吧对不队	SpecProbe: 面向处理器微架构安全的漏洞检测系统
318	骨振识息	骨振识息: 基于头部接触响应的智能用户认证系统
319	后门盾-智防先锋	后门盾-智防先锋
320	呼神护卫	CopyrightGuard: 面向 AIGC 创作者的多维度版权保护与溯源平台
321	声量科技团队	面向短视频的多模态舆情安全威胁感知系统
322	et3	et3
323	MedVax	MedVax——面向 AI 伪造的用户隐私源头防护系统
324	Test1024	X-Comp:移动应用隐私合规实时测评系统
325	NUX	智鉴工盾-基于深度学习的工控网络入侵检测系统
326	one	“棱镜守护” 动态访问控制加密·指纹盾
327	CallGuard	CallGuard: 面向实时语音通话场景的 AIGC 风险感知与主动防御系统
328	多喝热水队	医影智链——区块链赋能的医学影像安全存储与共享系统
329	机动特战队	lynx-hunter /radar
330	Deep blue dream	多协议动态化智能网联汽车异常流量检测系统
331	取经大队	破影猎手——面向数字人视讯电诈的实时监测与预警系统
332	我都行(狗头)	PASVault: 基于深度学习蜜加密技术的抗泄露口令管理器
333	智胜先锋	DeepTestX: 基于大语言模型的深度学习库智能模糊测试系统
334	IoT	IoTStateFuzzer——基于模型学习的物联网设备业务逻辑漏洞检测系统
335	派小星	智域鉴析: 域名解析链安全监测与威胁鉴定平台
336	PrivAIcy	MultiPriv: 多模态大模型用户隐私感知与保护系统
337	焊光通讯局	声盾锁界 ——自适应录音屏蔽器
338	111	ConfGuard: 基于置信度过滤与 DistilBERT 的 CAN 总线入侵检测系统
339	好想和你凑一队	LSTC: 基于半全局三角中心的网络暴力溯源与预警平台
340	洪磊全球粉丝后援会	地脉舆擎——基于复杂网络的事故舆情监控系统
341	信安强国 ncepu	基于区块链认证体系的电力交易辅助平台

序号	团队名称	作品名称
342	难搞哦	青铜链脑 FuzzOrb: 融合模糊测试与 AI 大模型分析的智能合约守护系统
343	你说的不队	零落盘动态执行远程运维引擎
344	Deepsleep 队	面向工业物联网的跨平台可信数据管理与安全预警系统
345	守护者	火柴人守护者—基于 NPU 加速的边缘隐私保护智能监控系统
346	零信任安全小组	“御镜”基于 IP 追踪的智能防破解
347	独行长路	基于大语言模型的可解释 Web 攻击检测与自适应防御系统设计
348	云海之上	基于深度学习的 RTL 级 IP 软核恶意逻辑图谱特征检测系统
349	畅言先锋	EchoShield: 基于对抗扰动的语音内容隐私保护系统
350	大佬打架不站队	基于多模态 Agent 的工业异常检测平台
351	网管小分队	迷踪匿网: 高隐蔽抗追踪的匿名通信网络系统
352	看看你的后门	深瞳-AI 模型后门威胁洞见平台
353	DB Guardians	满足差分隐私的离线多关系数据库查询技术研究
354	极光象限	智慧蓝碳-基于区块链与 AI 的感知数据可信溯源系统
355	海底小分队	Deep Shield—基于 FreqNet 的 AI 伪造图像识别系统
356	sohu	智捕钓域——基于 SBERT 模型的钓鱼域名检测系统
357	只要名字起的长就会有人读下来对不	FlowEye: 基于深度学习的多阶段网络加密恶意流量检测系统
358	青春猪头少年不会梦到明德楼	安眸: 面向社交场景的网络异常监测与舆情可视分析系统
359	深藏 blue	按图索骥、逐影溯源——视觉媒体溯源取证平台
360	WYE	基于 AI 分析的资产信息探索与漏洞调测平台
361	疯狂星期四	智核——基于强化学习的轻量级物联网 PUF 身份认证系统
362	普信队	基于 DeepSeek 智能文本合规审查系统
363	Found404	ThreatHunter: 基于 AI Agent 的自主渗透和系统安全风险评估平台
364	智医慧眼	智医慧眼 - 多模态大模型安全医疗影像精准诊断系统
365	葫芦娃救爷爷队	天穹净瑕——基于补丁定位和清除的抗图像对抗攻击航天器可信识别
366	无限进步	AI 智御星网盾-全维网络安全领航者
367	零信任小组	安全基线检测工具
368	比特守护者	基于加密指令标签的计算安全处理器设计与原型验证系统
369	在努力了队	Hetero Guard: 基于异构图卷积神经网络的 DNS 隐蔽信道检测系统
370	沧溟链盾	智藏宝——基于区块链的艺术品确权流通系统
371	心防特工队	“心防”——基于多模态生理信号与 AI 的连续自适应身份认证系统
372	我太想进步了	智能反诈问答系统
373	联智共济	联智共济
374	早八起不来队	基于 SM4 加密的后量子投票系统
375	Error 404	“频盾”——低功耗 Deauth 帧攻击频域监测系统
376	密码的周一	国密慧播——基于 SM9 的广播函数加密研究
377	萌新历练	基于 SM9 优化与 DNA 加密技术的图片加密算法研究
378	灵枢智创	穹盾-校园低空安全智能防护与应急响应平台
379	信安小分队	基于多智能体协作的 CTF 题目分析

序号	团队名称	作品名称
380	凌晨等电话队	慧眼识真伪——面向社会场景的全模态 AIGC 鉴伪系统
381	星盾	“隐流”——基于国密 SM4 的工业相机零信任安全实时传输系统
382	安全第一	截流防诈——基于 Transformer 和 GNN 的诈骗电话检测系统
383	爬虫小队	基于智能爬虫的自动化局域网资产探测与安全评估系统
384	云安诊	基于可逆信息隐藏的抗量子攻击云医疗数据安全系统
385	0day 快递员	DomainGuard: 恶意域名实时检测系统
386	一个队	求真图谱-基于多层次语义与知识图谱协同校验的 AI 幻觉识别与溯源系统
387	当代孔乙己联合会	基于深度学习与大模型协同的多模态恶意软件智能检测系统
388	paper++	智鉴医谣: 基于 AIGC 检测与 RAG 的医疗辟谣平台
389	舞龙舞狮	De jaVuzz
390	一定行	基于深度学习的钓鱼邮件检测
391	不如黄焖鸡	安云医链: 基于加密病历安全分享的就诊系统
392	ShieldCoder	CodeShielder: 基于微调大模型的专家级漏洞检测系统
393	1	1
394	EyeSec	基于大模型的智能化网络威胁检测与防御系统
395	灵枢创智	“灵枢 AI”基于多模态 Agent 的实时违规视频鉴别与防御系统
396	INFINITEINTERVAL	IntelliFuzz-NLP: 基于模糊测试的智能自然语言处理系统测试平台
397	烟熏三文鱼	基于 YOLOv12 的在线博彩网站交易账户自动化获取系统
398	404 Not Found	ImageGuard: 基于 SRE-LICM 算法的图像隐私保护系统
399	菜鸟驿站施工队	匿流: 身份与查询双重隐匿的数据流通系统
400	疯狂星期四 SEU	APISeeker: 基于 LLM 的影子 API 检测系统
401	Safety Guardian	CyberEye-多元态势感知平台
402	杭电网安	基于大语言模型的智能化漏洞检测与分析系统
403	1001011	123
404	锃斤拷烫烫烫	火眼金睛——多模态视频篡改检测与定位系统
405	网络先锋队	支持双向认证匿名支付的隐私认证系统
406	破坏性创造	基于人工智能语义识别的数据安全传输系统
407	Crypto_Navigator	VuInTester: 基于 APT 领域大模型的自动化渗透测试系统
408	车安信	CIBPU: 冲突不可见的安全分支预测单元
409	无研以队	泛在场景下的人工智能模型攻防技术与验证
410	Roar MilkDragon	MalGuard-大模型驱动的社交媒体恶意图像细粒度检测系统
411	网安三剑客	基于大模型的自动驾驶安全保障系统
412	隐算密投团队	零迹票联——基于安全多方计算的电子投票系统
413	早睡一点吧	VideoGuard: 基于大模型的短视频有害内容检测与预警系统
414	柒兑	孪生智盾·变电站数字孪生安全赋能平台
415	诺瓦骑士	基于 IVC 的零信任图像交易技术
416	NeuraGuard	频御智盾: 多任务对抗攻防验证与隐蔽扰动优化平台
417	甘法大-天启	图像视频监控中的异常检测
418	BitStorm	大模型驱动的空间可信状态估计与推理

序号	团队名称	作品名称
419	Double_H	基于 Shapley 可加性解释的恶意软件概念漂移可解释分析系统
420	洞见青蓝队	青蓝洞见：师生协同的污点模式学习与引导式智能漏洞挖掘系统
421	哈基米南北绿多队	基于移动端应用分析的蓝牙安全检测系统
422	MNGA	IPv6 网络安全态势感知与漏洞治理可视化平台
423	Oneyee	毓秀智骨平台——基于 AES 的加密通信与双向认证的 Cobb 角测试系统
424	其惟春秋	跨模态语义融合虚假新闻检测与取证系统
425	d11Times' fans	基于跨模型通用对抗水印的人脸图像保护微信小程序
426	海空之眼	“海空之眼”——基于风光互补的水空协同海洋牧场安全监测平台
427	众智协同团	ZTAgent: 基于任务调度和策略编排的零信任安全智能体平台
428	NK 拿拿龙	NTP-Defender: NTP 服务安全态势监测平台
429	渔业小队	面向水质污染溯源的多模态数据无人采集监测平台
430	数据都队	凌瞳——基于大语言模型的 IPv6 智能测绘与安全运维系统
431	中财 BOOK 思议	基于深度学习的神经区分器训练与验证系统
432	轻舟已过万重山	触迹 Guardian: 基于触摸屏行为的持续认证系统
433	联御智行	ICPOD-类别非平衡的协同式隐私保护目标检测系统
434	NeuroX	NeuroX: 精准安全的脑电隐私保护系统
435	我和评委站一队	安驰星盾: 基于自适应多模态网络入侵智能分析平台
436	数智东南队	多模型虚假新闻检测集成系统
437	电容手掌智能认证团队	基于电容屏感知的安全手掌认证系统
438	让我们一起说中文	基于 PQC 的文件安全交换系统
439	Auroral	基于大模型的多模态风险内容识别系统
440	untitled	PicGuard: 绘画图像的主动对抗防御扩散模型
441	取名好难	面向内容理解的选择性图像加密系统
442	deepsleep	基于数字水印的医疗影像安全系统
443	bug 改改改改到厌倦	潜痕——面向 AIGC 的水印版权维护平台
444	女院最后的深情	基于 python 的 web 防火墙应用
445	NKV	智鉴流控: 大模型隐私流控验证系统
446	菜鸟队	基于潜在可分离性的模型后门攻击检测系统
447	银河蛋仔防卫队	基于对抗生成网络的自动驾驶异常场景生成系统构建
448	黑产捕手队	基于多维特征的涉诈黑灰产应用收集与检测系统
449	DeepGuardians	鉴卫: 基于双路协同的网页端深度伪造检测系统
450	没有想法	深鉴真知——基于多模态对比学习的真实环境多媒体篡改检测系统
451	adbo	基于深度学习的 DDoS 攻击检测系统的设计与实现
452	flyteam 开发堂	图像隐藏平台
453	Book 思议队	T-FLOWUS: 基于 UMAP 和 OCSVM 的可信联邦学习系统
454	迷你三吹	MiniSentry——基于任务驱动的规避型恶意小程序检测系统
455	安全卫队	“狡狴”——文生图场景下的内容安全守护神兽
456	沉稳好	基于差分隐私的联邦时序集成医学分割模型
457	先天没笑容圣体	针对微调 LLM 版权保护的盲盒水印方法和研究

序号	团队名称	作品名称
458	蛋仔派队	音落留痕：基于口令猜测模型的键盘声学安全检测系统
459	星火	云盾慧眼
460	牛顿的苹果砸不到我	时空寻径者：6G 网络基于时空耦合路由跳变的隐蔽交火攻击防御系统
461	真的好累	心电密码
462	链时代小分队	Sec-Protector: 基于大模型的多智能体系统密钥泄露检测工具
463	flow	工业蜜盾—基于蜜网的工业互联网协同威胁检测系统
464	你说对不队	面向车联网的高效且安全的联邦学习系统
465	寻微	“寻微”——基于神经网络的 APT 侦测系统
466	吉农信安小分队	基于光学编码与混沌加密的高安全性数据传输系统
467	TRTPS	慧语星枢——基于提示词工程的二进制漏洞检测平台
468	TCW	极速木马猎手：轻量化远程访问木马早期检测与终止系统
469	CDLZ	基于内联重优化的二进制代码相似性分析平台
470	At	基于混沌算法的图像和文本加密
471	隐麟卫宸	基于短信验证码增强的两因子认证系统
472	数据不安全小组	面向数据要素流通的数据容毁确权系统
473	绿羽傲飞战队	新域密链:洋葱分层式天地协同安全通信指挥链
474	旺仔小分队	基于大模型的虚假新闻检测
475	文件堡垒	云境密通：支持细粒度控制和高效群分享的文件堡垒系统
476	信息制胜	智安御灾——基于多模态隐私安全联邦学习的自然灾害跨域协同预警系统
477	MidCypher	MobAgent—基于多专家协同的移动端旁路漏洞智能化“检”与“验”
478	对对对队	天巡——无人机网络安全感知平台
479	Deepfake 克星	慧眼如炬——基于对抗训练的 AI 生成图像检测技术
480	爱拼才会赢	面向无人机的“云-网-端”数据安全审计协议研究
481	云盾	支持资源受限设备检测的云端数据安全审计系统
482	BGRAG	BGRAG——基于行为图的 RAG 大模型漏洞检测系统
483	点击生成一个队名	量子云仓——基于后量子密码算法的文件加密存储系统设计与实现
484	momo	MoLLaFuzz——基于 LLaMA 生成式大语言模型的工业协议漏洞挖掘
485	铸盾卫士队	基于模糊测试的智能合约漏洞检测系统
486	热血奋斗	面向工控网络的小样本生成与入侵检测系统
487	格式对不队	盾瞳-融合加权集成学习的 DDOS 攻击预警系统
488	信安大机灵	隐域风控——基于可信执行环境的隐私保护身份认证风险评估系统
489	人类能否取代 AI 队	基于 LLM 智能体的二进制漏洞检测与分析
490	AMC	AeroTrust AI 航材智能溯源链
491	春日影	IoT 全生命周期漏洞挖掘与安全保障系统
492	TruthDecoder 识真者	鉴真——面向中文语义的跨模态新闻伪造检测平台
493	F0yt34m	智能网络安全实训云平台
494	hfut	闻声识机——开集环境下手机型号鉴别系统
495	信息安全小队	电荷智盾：电力负荷预测信息安全分析预警系统
496	Badname	AnonMeta：基于 SGX 的元数据保护匿名通信系统

序号	团队名称	作品名称
497	Cyras	CyraSafe-扶光大模型服务安全风险评估平台
498	不上早八队	《邻森卫盾——基于双模架构与异构特征融合的 APT 检测》
499	DoTA	DoTA: 基于污点分析的面向拒绝服务攻击的智能合约分析框架
500	NetOru	SwiftIrisAuth——基于 LWE 的链上虹膜认证系统
501	ncc 后花园	RAGFUZZ-基于大模型的第三方库自动化模糊测试系统
502	摆试可乐	匿查查——基于 PEPSI 的恶意文件共享检测系统
503	87622	瞒天过网: 面向大语言模型的隐蔽通信系统
504	三个臭皮匠	多模态水印辅助的智能驾驶风险警示鲁棒识别系统
505	/etc found	IoTalon: 基于多模态大模型的设备越权访问漏洞检测
506	2324	“检密”密码算法正确性与一致性验证平台
507	好想和你凑一对	鲸鱼——基于模型微调和知识蒸馏的恶意流量检测系统
508	hdu 数据安全队	数囊信舱——基于数据对象的政务可信数据空间构建
509	Amaterasu	区块隐锋-抗关联生成式区块链隐蔽通信系统
510	电科院求真	基于同态加密的位置隐私查询服务
511	游戏王	基于虚幻引擎 (UE) 5 的模拟现实类信息安全基础教育严肃游戏系统
512	智鉴千行	智鉴千行-基于指令微调与双阶段知识增强的漏洞检测系统
513	心算 DILITHIUM	量子方舟——面向 PQC 迁移的混合证书签发和验证系统
514	AWG111	ICDefender: 面向工业控制流网络 的小样本生成与检测系统
515	安声守卫	MimicLock: 基于不可学习样本的语音克隆防护系统
516	如来佛祖	基于 Librosa 技术的声音验证码双保护锁
517	Emoji 小队	万物归 E——零宽隐语颜码密域
518	果之林批发部	棱鉴——基于深度学习的 AIGC 图像鉴别和篡改识别溯源系统
519	万一中了	天盾: 基于转发式欺骗的无人机防御系统
520	King	玄壁——Linux 主机安全防护平台
521	根本写不完	隐私防护者, 基于双混沌系统的数据安全防护系统
522	不要指望我们队	CLPi-NetSurv: 基于深度学习的轻量级网络流量分析与异常报警系统
523	御网苍穹	御网苍穹-基于机器学习的无人机集群网络入侵检测
524	ERC20	RoleSem: 多智能体上下文角色感知的智能合约权限漏洞检测与利用系统
525	四上无难事	慧眼——基于深度学习的网络安全态势感知系统
526	御网天鹰	御网天鹰——全流量驱动的大模型自动化漏洞挖掘系统
527	一路向西	基于国密算法 SM2 和 SM4 的视频媒体文件高效加密系统
528	智汇司法	司法卫士: 裁判文书网大模型聚汇分析与辅助决策系统
529	跟上不要掉队	凌悟 RAG 智慧引擎——大模型幻觉缓解方案
530	桃花灼灼	基于动态交易网络的 Web3 恶意账户细粒度检测系统
531	毕者方贤	智筑云脑——AI 智慧工地监管平台
532	拉仓巴拉丹扎木苏日丹队	基于多源异构数据级联分析的黑灰产移动应用检测及其团伙挖掘
533	神的团队	“模甲”——大模型越狱防御工具
534	Kernel Panic	SecureFuzz
535	天线宝宝排排队	“明鉴”——以大小模型协同为基础的 APP 用户协议检测系统

序号	团队名称	作品名称
536	啊对对对对	“神经卫士·智盾”基于多模态深度强化学习的零日攻击自适应检测与智能响应系统
537	XORacle	基于联邦学习的隐私保护航班延误预测系统研究
538	隐私数盾小队	个性化本地差分隐私下的多维数据收集方案
539	fuzzlover	FuzzSol——基于灰盒模糊测试的智能合约漏洞检测系统
540	Code 安全卫士	ShellSight: 面向 SSH 协议的加密流量可视化系统
541	TeXIQw	Firm-BERT: 基于大语言模型的智能固件漏洞检测平台
542	NULL	基于联邦深度学习和同态加密的疾病诊断医疗系统
543	信息都队	VarColenc: 云端加密压缩键值存储的可变长度列式分包方案
544	嘿嘿	智链鹰巡: 基于可信分片区块链和强化学习的多无人机自主协同控制系统
545	宝宝巴适	EvilLens: 基于多模态的儿童邪典视频挖掘治理平台
546	旺旺队	图文溯源: 面向视觉语言模型的多模态全过程水印系统
547	二仙桥暴龙	ETGuard: 电网智能终端设备威胁狩猎系统
548	古月卓文武	轻量级跨平台动态可搜索加密数据库系统
549	斑马小镇	智鉴先锋——基于大模型智能体的音视频内容风险智能分析系统
550	NEU-Defender	IVN-Defender : 面向车内网络的分层入侵检测系统
551	鸿鹄迁云	鹄迁云: 大模型驱动的开源库国产化迁移平台
552	隼焱火炎	基于 AI 驱动的等保合规自动化测试平台
553	NKOne2Three	基于秘密共享的安全多方数据联合分析平台
554	黄油面包	AutoReMCP: 基于 MCP 的反编译代码优化与安全分析平台
555	Ouroboros	大语言模型辅助的 Java 静态分析漏洞挖掘
556	LECTF	MaskSentinel: 面向主流视频通信应用的即插即用深度伪造快速检测预警系统
557	万事顺意	面向联盟链的异构隐私计算框架不动产交易系统
558	auv 小分队	共鉴——抗恶意干扰的多无人机协作感知安全系统
559	爱用 gdb	调试至上——基于大语言模型的漏洞成因定位调试器
560	橙	数据++——基于区块链和沙箱的一站式可信数据交易处理平台
561	西风骑士团	守护天空: 基于分层闭环设计的无人机网络入侵检测系统
562	坐看云起时	CVFinder: 融合多特征驱动图神经的智能合约漏洞检测平台
563	长大网安小队	基于容错预约束的环链端到端加密监管通讯系统
564	Arcadia	AbyssSight: 暗网节点态势感知与执法攻防平台
565	摸鱼小分队	ECU-SecCom: 车载 ECU 安全通信系统
566	QL 队	基于 CodeQL 的 C/C++同源漏洞检测
567	又寸不又寸	隐私政策大语言模型多智能体系统
568	敲的都队	御安慧瞳-软件漏洞智能检测与分析平台
569	智慧树	智御盾安全卫士
570	真假易辨队	VID-GUARD: 基于大模型的视频虚假内容检测系统
571	晚安玛卡巴卡	基于 AI Agent 和 LLM 的自动化漏洞修复系统
572	乐天小队	SFGuard——基于 TensorFlow 框架的 API 滥用检测器
573	奋起上进	智能安全响应系统

序号	团队名称	作品名称
574	代码一定队	基于高维超混沌的无人机 3D 点云数据加密系统
575	无敌奶龙	VortexProtect: 基于后量子密码的 Android 应用虚拟化保护系统
576	业筑奇士队	洞猎: 控制流增强的层级化定向模糊测试框架
577	PRISTINE	PRISTINE: 基于残差声纹提取的被动语音溯源系统
578	专业团队	Falcon: 基于路径敏感稀疏分析的供应链漏洞挖掘系统
579	御空卫士-基于无人机通信安全防御	无人机巡检系统
580	RotorSpotter	RotorSpotter: 无人机检测与定位轻量级系统
581	盾势研究小组	DDoS 模拟突击 -- 网络安全漏洞暴露系统
582	Bri9htM0on	Fenrir-基于 MCP 的自动化代码审计工具
583	今晚不加班队	视频数据内容高效加密与智能感知系统
584	海底小纵队 PLUS	LipKnows: 基于唇动特征的活体检测系统
585	cmmccddb	网络流量监控
586	rust	rust
587	第一梯队	自动化运维安全管控系统
588	猛猛冲	主机安全基线检测与优化系统
589	所以爱会消失对不队	智影堪真——人脸安全智能系统
590	知曜	零界医信: 基于零知识证明的可信医疗大模型数据交付与生成验证平台
591	眼睛大了, 脾气小了, 小狗越来越好	智控卫士——基于深度学习的工控网络入侵检测平台
592	霸王龙队	智护电网: 基于隐私计算的电力大模型预测系统
593	11111	多模态谣言检测系统
594	X Chain	ArtiFlow——艺链永鉴
595	安全先锋队	驾驶行为画像安全检测可视分析
596	智械先锋	信息安全
597	菜鸟小分队	基于深度学习的智慧交通图像处理与安全监控系统
598	DNNFortress	NeuroShield——面向硬标签场景的深度学习抗提取防御系统
599	gogogo 队	免疫智盾-深度神经网络守护者
600	666 当兵马俑不叫我	面向位置服务的渐进式几何搜索隐私保护方案
601	DeepSeal	PromptGuard——基于内容级输出相似性的 Prompt 版权保护系统
602	XU17	SQLiPecker——基于 Multi-Agent 的 SQLi 漏洞检测系统
603	非常队	量铠智行——轻量子的智能车虚拟钥匙系统
604	闪亮的代码	护城卫士——基于联邦学习的城市安防智能分析平台
605	哈基米哈气	基于 ECDH 算法的无人机安全通信系统
606	星眸守护	星眸守护: 基于树莓派和 yolov11 的驾驶行为感知系统
607	智胜者	慧眼识人——多维度生物特征识别与行为感知系统
608	自动代码修复课题小组	基于大语言模型的自动代码修复工具设计与实现
609	假如不对	潜绘——基于生成式隐写的人脸信息隐藏
610	大展宏图	基于国密算法的视频和图像加密系统
611	Traffic-X-Ray	Traffic-X-Ray: 加密即时通信网络透视系统

序号	团队名称	作品名称
612	信息安全队	基于语义引导的安全文本多标签分类系统
613	春日部防卫队	基于 TCM 安全芯片的可信内容发布与防篡改系统研究
614	工业大学	安全第一
615	奶龙熬熬觉	OS Agent 环境注入评估与防御平台
616	小鸡队	碳链宝：基于联盟链与 Agent 的碳市场全流程保护与交易平台
617	来杯咖啡	并发卫士——面向操作系统内核的并发缺陷静态检测工具
618	团结进取	AudioDefender：多任务学习驱动的音频伪造检测系统
619	两个火箭队	晴天伴——基于双向互动与个体认知的青少年心理健康演化分析系统
620	屠码 OCR	屠码 OCR
621	星海护卫队	图片防篡改及水印生成检测系统
622	sudo win	支持隐私保护的联邦学习聚合软件实现
623	链盾小分队	链盾——基于联邦学习和边缘算法的智能网站检测系统
624	猛猛冲就行	VisionGuard AI——多模态图像真实性智能检测系统
625	寻路精灵	InAPSage：智能驱动的内网攻击路径推演系统
626	御林安全工作室	DeepTraceAudit 基于数据流和控制流的代码审计系统
627	破晓小分队	LLM-GUARD：面向线上大语言模型的多模态数据保护系统
628	李想大虾队	混合式入侵检测平台
629	乐迪出发队	轻量级入侵防御系统
630	拖延症晚期医疗队	保密空间分布式电磁定位系统
631	cufeinfo	区块链异常交易追踪检测
632	璇玑镖局	抗量子可扩展 SM4 国密算法的 FPGA 优化实现
633	方程组	智驾盾——基于鲁棒性安全联邦学习的云边端高效分心驾驶行为协同预警系统
634	蛋仔派对	“NeuraGuard · 星界防线”——基于 AI-SDN 的安全矩阵
635	SecureTech 先锋	基于 Intel SGX 的多层级动态可搜索加密系统
636	超混沌密网传输研究队	暗域密盾——Mindspore 赋能的四阶全互联细胞神经网络超混沌图像加密传输系统
637	天镜开发团队	天镜日志安全分析系统
638	聚合	密网绘途——基于联邦学习的地图数据隐私保护与安全共享系统
639	放学后茶会	PassSlayer——零信任全覆盖无密码认证系统
640	信安对对队	稻安信盾——水稻病害数据安全治理平台
641	信息致胜	大小模型协同的多模态数据要素安全治理与管控系统
642	我真的很想要这份文凭队	MICS-Gateway：一种基于意图识别的自适应大模型安全网关体系
643	什么都队	SecureDataFlow：基于多方加密 TEE 的跨部门数据安全 流通与计算平台
644	不秃头小队	FadeMind：面向扩散模型的多概念遗忘系统
645	鸡猫牛	基于负数据库的隐私保护脑电波识别系统
646	音控盾	基于 LightGBM 的抗翻录鲁棒水印系统
647	maercs	智盾网安——基于监督式人工智能方法的恶意网站检测系统
648	85KG 俱乐部	LLM-SecGuard: 基于多维心理学的大模型越狱安全评测平台

序号	团队名称	作品名称
649	406CCB 大师	ChatAPK-大模型与智能代理驱动的自动化应用程序取证系统
650	赛博守护-人民万岁	基于大模型的威胁情报智能抽取与分析系统
651	咋不队	群体智慧网络安全穹顶
652	西南陈冠希	灵鉴隐痕——深度学习赋能的加密流量行为鉴别系统
653	春宵苦短，前进吧	LightShield-基于压缩感知的图像加密系统
654	dky 信安	寰驭通安——基于国密周期性可否认环签名方案的车联网溯源平台
655	VigilSwift	VigilSwift-PIDS: 可真实部署的快速轻量化在线 APT 检测系统
656	对的都对	DDos 攻击检测系统
657	经纬智盾	摄界经纬——拍摄地智能识别与连续定位系统
658	FZTO	SigTrace: 基于数字签名的电子文档泄露溯源系统
659	网安全对队	面向模型攻击的容忍研究
660	BITaudit	IncreAudit: 基于增量式 LLM 的智能合约代码审计系统
661	果酱大王	基于 BERT 和 Deepseek-r1 改进的大语言模型防御器
662	AAA 批发中心	基于语义-行为建模 LLM 的反沙箱检测系统
663	PPP	PPP
664	X 特遣队	车联轻盾——基于国密和后量子双重验证的车联网签名系统
665	跃迁	AIGC 安全系统: 跨模态校验与后门管控
666	赛博烧饼	MT-TrafficNet: 适应复杂网络的多任务流量大模型
667	Nexpower	基于 SDN 的云计算环境 DDoS 动态防御系统项目书
668	无境	龙渊海鉴-基于可视化技术的海上风电场信息安全检测平台
669	DeepPot	DeepPot: 基于大语言模型的智能蜜网威胁狩猎系统
670	OCS	虚假帧率的智能检测算法
671	piano	一验万年——公开可验证的同态数据封装机制隐私计算服务平台
672	头脑特工队	基于联邦学习的隐私保护推荐系统
673	智能盾护队	《MySecureDrive Guardian》——基于智能驱动与加密技术的安全文件存储系统
674	智绘先锋团	幻彩织影——基于语义引导的双重伪装迷彩
675	张钰朋队	信息安全战略
676	安全小队	隐询智索——抗泄漏的多模态隐私查询系统
677	史迪奇大队	双模态 CoT 后门: LLM/VLM 具身智能的知识图谱增强攻防
678	七八九	茶韵华彩: 民族风韵与茶文化的交融
679	柑橘橙	慧眼奇鉴——基于商密算法和信息隐藏的远程医疗图像双认证平台
680	九章通輿	慧眼秘行: 大模型决策下的安全智能交通系统
681	银眸	联邦苍穹守卫——基于联邦学习的网络入侵检测平台
682	密盾先锋	“驭驰防线”——抗远程攻击的智能网联汽车入侵防御系统
683	L1af	基于同态加密的智能钓鱼演练系统
684	代码敲不队	控制流约束下代码复用攻击检测与风险评估系统
685	灵感菇队	面向流媒体平台的递进式恶意域名挖掘系统
686	狗头大队	车联网环境下抗量子攻击的密钥分发协议与令牌认证系统
687	It's MyGO!!!!	墨衡——大模型生成文本的多水印动态融合评估系统

序号	团队名称	作品名称
688	知道熬夜不队	基于文本水印对语言模型生成内容的版权保护和鉴别
689	flyteam	工控卫士——基于图神经网络的工控场景 APT 溯源追踪系统
690	网络 sec	基于大模型的隐私收集合规性检测平台
691	东北大学小分队	智盾图谱——基于知识图谱与大模型的软件组件安全智能管家
692	字眼侦察队	变亦可辨——面向短文本变异对抗的多模态智能检测技术研究
693	SYN 北方完美夜曲	火焰越权漏扫系统
694	AAAA	灵镜——基于 AI 智能体与样本演化机制的网络安全自动化防御系统
695	密影安防 11h	密影安防
696	sanbao	PenTestLLM——知识增强的多智能体渗透测试系统
697	叫啥名	链密舆情——基于区块链的可信舆情取证系统
698	BOI	DeepSuma: 网络空间测绘智能问答系统
699	三人棒	LLagent 基于多智能体协同的第三方库漏洞识别与修复
700	AuroraSec	“虚拟钥匙”——基于增强电路的门禁系统破解与密钥分析
701	山海签盾	基于哈希函数的后量子数字签名方案的国产化替代研究与应用
702	深藏 bbluuuee	AI 合成的虚假视频检测-DeSY
703	[temp name]	智控模测: 融合语言模型与物理感知的工业协议模糊测试框架
704	脑洞大开	基于属性基加密的无人机群组密钥管理方案
705	深藏 blue 队	音御 GANsVoice——基于对抗扰动嵌入的语音防护系统
706	三角洲猛攻大队	基于 AES 和国密算法的文件加密工具
707	奇迹再现	LomLive: 基于 Lombard 效应的实时语音通话伪造检测系统
708	起名难	基于树莓派的 ai 流量监测报警系统
709	APTbusters	ApexSentinel: 基于大语言模型的 APT 检测与溯源系统
710	阳光开朗	VeriDome——多模态深度伪造内容检测系统
711	Besti Club	玄鉴: 基于选择性状态空间模型的恶意流量分类系统
712	324	智能网联车队传感器攻击的抗干扰防御算法
713	从容应对	网络安全防护系统
714	無限進步	云驿密匣——基于鸿蒙系统的国密邮件安全传输系统
715	PhOenix Rising	智隐潜行: 基于流量规避策略的内网扫描评估系统
716	404 Have Found	混沌面纱——基于通用对抗扰动的秘密信息保护
717	乐迪队	基于小型机器狗的信息安全多维动态防护系统设计与实现
718	多进程小分队	面向深度人脸伪造的肖像保护平台
719	码上无忧	基于加密 QR 码的快递隐私分级保护系统
720	银河护卫队	AxoraFL: 基于区块链的安全高效联邦学习安全聚合系统
721	UABW	面向网络协议的智能符号执行和模糊测试工具平台
722	伪人小分队	基于 Tinyml 的深度伪造检验软件
723	长大对对队	基于 SM4 国产密码技术的文件加密防护系统
724	前途无量队	车联网协同式异常检测系统: 联邦学习架构下的高精度入侵防御与隐私保护
725	你说的都	链钥政通——数据共享与信息检索隐私保护系统
726	哈哈哈哈哈	ShamirGuard——基于秘密共享的人脸识别隐私保护系统

序号	团队名称	作品名称
727	赛博佛组	AetherCTF: 自进化智能体驱动的次世代 CTF 实训平台
728	图码乾坤	图码乾坤—基于可逆数据隐藏的大容量抗量子数据保护系统
729	成群结队	基于卷积神经网络的网络安全态势感知系统
730	老秦人攻打提瓦特	零信任赋能的主动式内网防护系统
731	智聚寻盾队	FUZZ-ZW: 基于聚类分析与禁忌搜索引导的模糊测试系统
732	Ginkgo	云鉴深析—基于大模型分级的高校敏感数据预警系统
733	西安给我一个机会	“析安”—基于大模型智能决策的渗透测试系统
734	没钱打什么比赛	LogAPT: 面向日志的 APT 检测与链路溯源系统
735	小邮专业团队	强化隐私保护的医疗联邦诊断系统
736	Crychic	面向短视频平台的 AIGC 视频检测与版权保护系统
737	dhlw	AntiAIEdit: 抗扩散模型图像恶意编辑的主动防御系统
738	琢光-crypto	基于同态加密的隐私保护深度学习共享系统
739	FaceGuardians	护颜幻盾: 面向全生命周期的智能人脸信息保护平台
740	DeepGuardian	DeepGuardian: 面向微信场景的诈骗检测平台
741	嘿嚯哈嘿	Y-Guardian 光盾——基于深度学习与多模态干扰的主动式防护系统
742	后门防卫队	ProtoShield: 针对大模型微调的少样本驱动高效后门防御系统
743	链穹卫	基于区块链的无人机认证系统
744	一次买够	JBShield: 高维概念视角下的大语言模型越狱防御系统
745	sixstars	StaticMAID: 大模型赋能的安全漏洞分析与修复一体化平台
746	名字好难组队	明鉴——基于大模型的语义驱动智能合约漏洞定位平台
747	Chain	基于区块链的去中心化物联网资源监测与调度框架
748	今晚吃毛肚	HSRB-FL: 异构场景下安全鲁棒的区块链联邦学习系统
749	海底小纵队	告效立判—基于门限全同态加密的多平台广告效果评估系统
750	御音卫士团队	御音卫士——基于组合防御的智能座舱语音对抗防御系统
751	AEGIS26	智御—大模型赋能的 APT 攻击类免疫动态安全防护系统
752	图图与 YO 爷爷	基于 YOLO 的图像敏感信息智能检测与掩盖系统
753	三点一线队	基于同态的聚合可验证联邦学习系统
754	anyvolunteer4	PrimeStrike: APT 组织基础设施前移态势感知平台
755	Aurora	“动察无遗”——行为可视化安卓动态威胁检测引擎
756	码力安全局	御模天线——面向越狱漏洞的大模型安全防护系统
757	败犬 RSA 太多了!	基于 QCNN 启发与 pyqanda2 的混合量子经典网络入侵检测系统——KDD Cup 99 验证
758	emm	SVD-GAN 驱动的区块链交易异常检测系统
759	Timekeeper	LLM-Guardian: 大语言模型安全评估系统
760	深藏 blue plus	貔貅: IPv6 网络空间资产搜索引擎
761	山顶	散钥于众, 聚信于签—基于口令防护的门限盲化钱包方案
762	大模型评估专家	基于混合专家模型的大模型评估系统
763	GraphGuardians	基于图神经网络的加密恶意流量检测
764	HIT 加油鸭	基于代码和流量融合的移动应用分析系统
765	智御之光	VoiceFort: 基于滤波+恢复技术的即插即用声纹识别对抗防御插件

序号	团队名称	作品名称
766	龙马一启冲	基于关联数据具有自主身份属性约束的选择性披露凭证
767	无名	支持跨域多方可验证的分布数字身份系统设计与应用
768	哲臻安全	声影真知—基于视听觉表示学习的零样本深度伪造检测
769	隐私审计小队	ShareScanAgent:基于大模型 Agent 的共享隐私检测系统
770	代码打得都队	DynASR——基于图表示学习的多阶段攻击行为耦合检测与动态场景重构系统
771	顶呱呱	智鉴·云盾--基于深度学习的恶意代码检测系统
772	要快乐小分队	基于谓词加密的分布式无人机群组安全通信系统
773	桃李自蹊	灵析：大模型协同的智能漏洞挖掘系统
774	剥蒜的情谊	一种无监督式的深度伪造检测系统
775	MalAgent	MalAgent：鸿蒙及跨生态恶意软件深度解构与检测系统
776	逐光未来	APP 广告全链路自动化审计与恶意检测平台
777	布吉岛	紫穹：基于 LLM 的自动化渗透测试和漏洞修复系统
778	安全大师	智谱芯界（GuardGLM）：基于国产大模型的多应用隔离防护系统
779	Vitality	智鉴--基于多模态大模型的深度伪造图像检测系统
780	格局	ChainSafeFort——灵鉴智能合约检测扩展中枢
781	勇攀高峰队	一种基于国产硬件的数字货币冷钱包
782	星城密锋	SymRecover++：基于弱源码的智能符号表重建工具
783	猛攻队	慧眼识真：面向文本、图像和视频的 AIGC 综合检测平台
784	零壹研究	基于深度学习的时间序列网络流量异常检测
785	苍穹	基于强化学习的 ELF 对抗性样本测评数据集生成系统
786	地表最强摸鱼协会之逆袭版	SMap——全球双栈资产关联测绘与安全分析平台
787	无限进步队	多模智盾：多模态多场景的人工智能模型版权保护与评估平台
788	属性锁卫	云御安途:基于 CPABE 的云边多网抗合谋多权威加密系统
789	灵迹隐者队	DP-TrajAnalyzer：差分隐私轨迹分析与可视化平台
790	云芯可信	动态可伸缩的 FPGA 可信机密计算环境
791	奋进一流爱国队	“天空慧眼”——空中目标异常行为检测系统
792	欧皇小队	智能网络靶场研究与设计
793	当 0 当 1 不当 3	面向流媒体语音的高效隐写分析系统
794	哈基米小队	AIGCTraceShield 大模型生成内容溯源平台
795	对对队	新闻之眼：面向新闻场景的高准确率多模态伪造检测平台
796	叫什么队	基于 SDN 的 Ddos 检测与防护系统
797	遇疯而彳亍	HUNTER-GNN—基于大语言模型与图神经网络的智能 APT 威胁狩猎平台
798	大模型的自动化评估平台	AI 卫士：大模型的自动化评估平台
799	超级飞侠	加密通信应用程序
800	不想列队	安卓恶意代码捕获
801	Asuri	基于强化学习的大语言模型安全对齐方法
802	智瞳	智瞳：面向串谋行为的恶意小程序检测系统
803	无敌奶龙队	PS-MDM——基于多源公共服务的黑产域名挖掘和多端防护系统

序号	团队名称	作品名称
804	图灵哨卫	天眼守卫-面向深度伪造的智能攻防检测平台
805	ncc 护发研究小组	幻影密卡——基于匿名凭证技术的身份验证系统
806	浪里白条	DMWmark: 音频分类数据集和模型知识产权保护系统
807	安网先锋	面向动态网页的 Web 漏洞扫描器的研究与实现
808	Not Found 404	鉴影: 跨平台黑灰产溯源取证智能体
809	对影成明月	基于入侵检测技术与混合 Transformer 的智能网络安全防护系统
810	伊萨卡有二头卡车	EPIC: 基于电磁侧信道的人工智能模型反演攻防系统
811	i surA	基于大模型技术的漏洞静态分析自动化工具
812	慧音执守	慧音执守-物联网语音安全领航者
813	芒果菠萝	Secure Cloud-安全存储与可靠计算云平台先行者
814	QQ 弹弹战队	隐刃: 面向智慧交通的语义通信隐式后门攻击
815	TopOne-Sec	SQLXGuard: Web 下的 SQL 哨兵
816	暗流智瞳	暗流智瞳——基于 LLM 的 Tor 暗网流量未知威胁发现系统
817	海大冲浪家	云影密链——基于区块链分级权限认证的云端图像加密存储系统
818	你说的都队	软件供应链中隐私保护和透明化的数字签名方案
819	无问锡东	基于机密计算的深度学习模型保护方案
820	以太卫士	以太哨兵-基于图大模型的区块链安全一体化检测平台
821	晨晖劲旅	微界隐踪——微博平台下基于鲁棒秘密分享的可溯源批量水印方案
822	「逆伪之锚」盯真队	鉴伪复原——基于篡改定位与身份恢复双重水印的人脸深度伪造主动取证平台
823	可爱猪猪警官扫图队	基于颜色矩和直方图特征的违规图像检测方法
824	无敌豚豚	BinMatchLLM: 网络核心设备固件补丁自动化识别与分析系统
825	极目楚天	基于注意力机制的鲁棒不可见视频水印系统及 Web 平台设计
826	智检视界队	智检视界——基于 SSP 和 YOLOv11 的图像真实性与暴力元素检测平台
827	123, 上链接	艺数链界 - 云象区块链艺术品确权流通平台
828	霍格沃兹网络安全部	基于语义分析与混合神经网络的 SQLi 检测系统
829	BOOK 思议对对队	守护之盾-视频监控多目标跟踪系统应对攻击的新型防御
830	也不是不行	AppTension: 基于意图理解的应用数据合规检测系统
831	GZU-007	融合威胁情报与多智能体的网络入侵检测系统
832	赛博神谕	擎翼盾-MA: 无人机动态通信欺诈实时拦截系统
833	我们说得对	基于 RAG 的数据智能分级系统
834	发际线与我作战	基于网络安全知识图谱分析的防御策略智能决策平台
835	费大厨队	“清风”智能新闻鉴伪平台
836	安全不打烊	M2X-Guard: 基于多引擎协同与多模态数据融合的 XSS 检测系统
837	大禹队	基于大语言模型的威胁情报感知与安全防护引擎
838	Cryptolab	支持量子安全与多功能的 FIDO2 协议设计与实现
839	Starfive	强化学习和 LLM 驱动的 5G 空口协议模糊测试系统
840	智慧火花队	基于 TEE 的安全人脸识别系统
841	求个心安	面向目标检测算法的智能安全评估系统
842	SUNNY	LLMTrace: 大模型赋能的新闻真伪判别与生成溯源一体化系统

序号	团队名称	作品名称
843	信息隐藏	多模态隐蔽通信系统
844	Minuscular	枢阵隐私-基于隐私计算的数据共享平台
845	Ghost in the car	面向自动驾驶远程劫持攻击的三级协同防御方案
846	代码 Kenan	BubbleBreaker: 基于类人行为模拟的社交平台信息茧房评估系统
847	0	CipherCore: 基于实时响应的智能数据加固系统
848	今天又摆烂了对不队	明瞳——基于移动端 GUI 智能体的 iOS 变身 APP 检测系统
849	什么都不队	误导界面弹框对抗框架
850	黑神话: Multimode	基于多模式的多核安全感知调度方法
851	602	基于大模型技术的软件漏洞全流程管理
852	寒霜火焰鸚鵡	Android 应用程序隐私合规检测系统
853	秦时明月队	车联智眼: 实时轻量化安全检测系统
854	每天进步一点	溯影: 面向泄密溯源的深度学习抗屏摄水印系统
855	圣洛夫基金会璃月分部	“码投”——基于屏-摄协同的安全气隙通信系统
856	慧辩	灵眸辩真--AIGC 人脸检测系统
857	无懈可击	基于高效数据脱敏的深度学习数据集隐私保护
858	SSNH	基于阈值与混合行为分析的僵尸网络恶意域名检测系统
859	年轻无极限	密算智行: 基于安全多方计算和低秩矩阵分解的路况预测系统
860	智感天盾	“智感天盾”——无人机多模态探测与反制系统
861	赤旗插满全球队	基于同态加密与双 CA 信任架构的车联网联邦学习安全增强方法
862	一定能赢的对不	数字箔条——基于数据分片重组的网络拓扑混淆系统
863	哈哈	面向互联网智能家居系统的用户位置隐私保护框架
864	Cyber 飞行者	支持 HarmonyOS NEXT 的密文关键词检索完整性验证
865	castor	castor
866	Achilles' Heel	GovLLMAegis: 基于对抗的政务 LLM 安全评测系统
867	海棠果	AI 换脸风险预警
868	anti-deepfake	基于语义解耦的联邦式隐私音频伪造检测系统
869	颜盾	“颜盾”——基于自学习扰动的图片隐私防护系统
870	bbbbbuapt	针对内容安全审核平台的可靠性评估系统
871	BinaryBlitz	基于 YOLO11 与 LSTM-T-AKF 融合的无人机隐私保护与抗欺骗系统
872	南理信安小分队	人工智能模型全生命周期安全风险评测系统
873	四个臭皮匠	基于鲁棒 LSTM 的轻量化车载网络入侵检测系统
874	检流净域	御流智检
875	fakebuster	“星火·智鉴”——基于大语言模型的虚假新闻智能检测系统
876	大模智安小分队	大模智安机器人
877	GAIGuardian	GAIGuardian: 面向生成式 AI 的动态演化监管系统
878	牛马小纵队	智能网联车辆动态行驶场景下密钥自主生成系统
879	对对对对队	雷巡网鉴: 面向匿名网站指纹识别的安全对抗效能评估系统
880	你输入的对不队	獬豸火眼——针对中文大模型越狱攻击的风险评测与识别治理系统
881	四只松鼠	融合多模态注意力与群体认知的网暴信息检测与取证系统

序号	团队名称	作品名称
882	永不落幕	HT-Detector: 面向硬件木马检测的集成电路硅前安全评测 EDA 工具
883	DDL Driven	Gasate: 基于数字孪生的卫星安全评估系统
884	有模法的麻瓜队	LLMMoat: 面向大模型全链路的越狱攻击检测和防护系统
885	定不负此队	VulnTriageGPT-案例知识辅助的漏洞挖掘系统
886	tara 分析小队	基于多模态大模型的智能网联汽车 TARA 分析平台
887	NoRegret	知识不对称性驱动的 RAG 系统隐私细粒度提取与动态防御框架
888	金睛紧箍	Multi-image 多模块图像综合处理系统
889	ICUworking	Holmes: KG+LLM 驱动的网络威胁情报综合推理引擎
890	保证第一队	高效隐私盾: 机器遗忘架构 ForgetSys-Pro
891	汪汪队立大功	Crypto-PowerToys: 基于大模型的跨平台密码学工具箱与信息安全综合工具集系统
892	文脉联坊	抗量子安全导向的多域标识认证与用户可追踪机制研究
893	VK	Security-Coding Agent——基于静态分析和动态模糊测试的多智能体代码安全系统
894	来都来了	时序侦探: 基于 RTL 的测信道攻击检测系统