

序号	作品名称	团队名称
1	隐士——面向隐私保护的智慧视觉系统	大锦鲤
2	破影猎手——面向数字人视讯电诈的实时监测与预警系统	取经大队
3	GAIGuardian: 面向生成式 AI 的动态演化监管系统	GAIGuardian
4	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	无限进步队
5	LLM-SecGuard: 基于多维心理学的大模型越狱安全评测平台	85KG 俱乐部
6	基于扩散模型的可恢复图像安全保护系统	为什么要演奏春日影
7	面向 AIGC 的溯源水印嵌入与检测系统	AIGC 水印检测
8	基于大模型的网络自动化渗透与安全加固系统	AutoHacker
9	面向信息安全试验的网络攻击负载生成技术	xjtu 队
10	多模态谣言检测系统	11111
11	GUIAgent 安全评测平台	711
12	SecureDataFlow: 基于多方加密 TEE 的跨部门数据安全 流通与计算平台	什么都队
13	DP-Shield: 基于差分隐私的网络侧信道攻击防护系统	绿色心情
14	SpecProbe: 面向处理器微架构安全的漏洞检测系统	这海星吧对不队
15	PASVault: 基于深度学习蜜加密技术的抗泄露口令管理器	我都行(狗头)
16	基于跨模态语义交互的社交媒体虚假新闻检测系统	gostgogo
17	状态转换漏洞: 一种新的 Web 竞态漏洞发现与检测	少年侦探团
18	PassMind: 大模型驱动的可演进口令强度评估系统	Dawning Future
19	PromptGuard——基于内容级输出相似性的 Prompt 版权保护系统	DeepSeal
20	PrivSeek: 基于秘密分享的轻量级大语言模型密态推理系统	PrivSeek
21	CallGuard: 面向实时语音通话场景的 AIGC 风险感知与主动防御系统	CallGuard
22	IPv6 网络安全态势感知与漏洞治理可视化平台	MNGA
23	LLMMoat: 面向大模型全链路的越狱攻击检测和防护系统	有模法的麻瓜队
24	基于联邦安全的工业互联网 DDoS 防护系统	Ave Muguizi
25	PrivScope: 小程序隐私合规检测系统	好像被资本做局了队
26	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	TL404
27	FALCON: 基于大模型的多智能体工控固件漏洞检测系统	比完开派队
28	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	AEGIS
29	鸪迁云: 大模型驱动的开源库国产化迁移平台	鸿鸪迁云
30	安眸: 面向社交场景的网络异常监测与舆情可视分析系统	青春猪头少年不会梦到明德楼
31	SymRecover++: 基于弱源码的智能符号表重建工具	星城密锋
32	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	斑马小镇
33	限时可验和高效的安全数据检索系统	时时刻刻检索队
34	暗流智瞳——基于 LLM 的 Tor 暗网流量未知威胁发现系统	暗流智瞳
35	Oday 挖掘	顶个诸葛亮
36	M-FUSE: 面向多层级安全的高效数据隐私融合计算平台	AI-AntS
37	SwiftIrisAuth——基于 LWE 的链上虹膜认证系统	NetOru
38	IVN-Defender : 面向车内网络的分层入侵检测系统	NEU-Defender
39	“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	C++20 标准委员会

40	共鉴——抗恶意干扰的多无人机协作感知安全系统	auv 小分队
41	“棱镜守护” 动态访问控制加密·指纹盾	one
42	跨模态语义融合的虚假新闻检测与取证系统	其惟春秋
43	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	Family Guys
44	DroneSentry: 基于射频指纹的非法无人机小样本开集识别系统	什么档次和我一队
45	鉴卫: 基于双路协同的网页端深度伪造检测系统	DeepGuardians
46	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	超混沌密网传输研究队
47	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	V2X
48	NetDefender——基于深度学习的恶意流量智能检测平台	从容应队
49	MASpom: 多智能体架构下大模型舆情监测与分析系统	NewsPursuer
50	明鉴——基于大模型的语义驱动智能合约漏洞定位平台	名字好难起队
51	X-Comp: 移动应用隐私合规实时测评系统	Test1024
52	ShareScanAgent: 基于大模型 Agent 的共享隐私检测系统	隐私审计小队
53	SonicGuard: 基于对抗扰动的语音隐私主动防御系统	200 OK
54	慧眼识真伪—面向社会场景的全模态 AIGC 鉴伪系统	凌晨等电话队
55	SQLiPecker——基于 Multi-Agent 的 SQLi 漏洞检测系统	XU17
56	伪装者-射频指纹识别攻防研究与实现	主动指纹
57	大语言模型生成式安全自对齐训练评估平台	白马程序员
58	MimicLock: 基于不可学习样本的语音克隆防护系统	安声守卫
59	声盾锁界 ——自适应录音屏蔽器	焊光通讯局
60	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	比特守卫者
61	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	信息制胜
62	“狻猊”一文生图场景下的内容安全守护神兽	安全卫队
63	智界-深度学习模型隐私风险评估与安全防御系统	shield
64	《面向移动车联网的匿名凭证认证系统》	密码破的都队
65	“海空之眼”一基于风光互补的水空协同海洋牧场安全监测平 台	海空之眼
66	洞玄: AI Agent 驱动的系统化安全风险评估平台	智测先锋
67	AndroAnalyzer: 基于图表示学习的安卓恶意软件检测系统	抱佛脚
68	智鉴—基于多模态大模型的深度伪造图像检测系统	Vitality
69	医域智穹——隐私协议语义感知的医疗数据可信中枢	待机中队
70	云御安途: 基于 CPABE 的云边多网抗合谋多权威加密系统	属性锁卫
71	零落盘动态执行远程运维引擎	你说的不队
72	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	四只松鼠
73	御安慧瞳-软件漏洞智能检测与分析平台	敲的都队
74	骨振识息: 基于头部接触响应的智能用户认证系统	骨振识息
75	图文溯源: 面向视觉语言模型的多模态全过程水印系统	旺旺队
76	RotorSpotter: 无人机检测与定位轻量级系统	RotorSpotter
77	RAGFUZZ-基于大模型的第三方库自动化模糊测试系统	ncc 后花园
78	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	喻家山代码纹析组

79	“灵哨”大模型安全检测平台	backguard
80	「智镜·无垠」——基于知识图谱与 DeepSeek 的全维度反诈中枢	牛牛就是牛
81	基于 YOLO11 与 LSTM-T-AKF 融合的无人机隐私保护与抗欺骗系统	BinaryBlitz
82	数囊信舱——基于数据对象的政务可信数据空间构建	hdu 数据安全队
83	按图索骥、逐影溯源——视觉媒体溯源取证平台	深藏 blue
84	强化学习和 LLM 驱动的 5G 空口协议模糊测试系统	Starfive
85	抗量子安全导向的多域标识认证与用户可追踪机制研究	文脉联坊
86	HT-Detector: 面向硬件木马检测的集成电路硅前安全评测 EDA 工具	永不落幕
87	MalAgent: 鸿蒙及跨生态恶意软件深度解构与检测系统	MalAgent
88	CyraSafe-扶光大模型服务安全风险评估平台	Cyras
89	基于强化学习的大语言模型安全对齐方法	Asuri
90	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	聚合
91	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	前途无量队
92	轻量级入侵防御系统	乐迪出发队
93	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	嘿嘿
94	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	[temp name]
95	声鉴未来——电信反诈智能平台	啊对对对队
96	面向无人机的“云-网-端”数据安全审计协议研究	爱拼才会赢
97	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	山海签盾
98	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	方程组
99	“心安私语”——基于分级加密的多模态智能体隐私防护系统	那一天的忧郁
100	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	LECTF
101	DeepPot: 基于大语言模型的智能蜜网威胁狩猎系统	DeepPot
102	面向向量数据库的自适应数据水印系统	NK-Vertex
103	IoTStateFuzzer——基于模型学习的物联网设备业务逻辑漏洞检测系统	IoT
104	音落留痕: 基于口令猜测模型的键盘声学安全检测系统	蛋仔派队
105	图鉴天工——多功能遥感安全检测与应用平台	新和联胜
106	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	真页
107	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	智鉴千行
108	ICDefender: 面向工业控制流网络的小样本生成与检测系统	AWG111
109	VeriFace: 基于多模态融合的抗 Deepfake 攻击身份认证系统	别拿脸蒙我
110	EchoShield: 基于对抗扰动的语音内容隐私保护系统	畅言先锋
111	视界增强——基于对抗训练的目标检测模型鲁棒性强化系统	荆州勇士队
112	匿查查——基于 PEPSI 的恶意文件共享检测系统	摆试可乐
113	智谱芯界 (GuardGLM): 基于国产大模型的多应用隔离防护系统	安全大师
114	基于大语言模型的威胁情报感知与安全防护引擎	大禹队

115	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	难搞哦
116	基于潜在可分离性的模型后门攻击检测系统	菜鸟队
117	基于 YOLO 的图像敏感信息智能检测与掩盖系统	图图与 YO 爷爷
118	ConfGuard: 基于置信度过滤与 DistilBERT 的 CAN 总线入侵检测系统	111
119	RAGFlow: 基于大模型跨模态语义增强的智能合约攻击检测系统	ChainWatchers
120	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	洞见青蓝队
121	VarColenc: 云端加密压缩键值存储的可变长度列式分包方案	信息都队
122	“智感天盾”——无人机多模态探测与反制系统	智感天盾
123	面向车联网的高效且安全的联邦学习系统	你说对不队
124	SmartPatchAnalyzer: 基于大模型的二进制漏洞 Patch 对比与代码审计系统	阿玛特拉斯
125	NeuroShield——面向硬标签场景的深度神经网络抗提取防御系统	DNNFortress
126	InAPSage: 智能驱动的内网攻击路径推演系统	寻路精灵
127	基于大模型反幻觉增强技术的代码漏洞挖掘系统	一八一八队
128	洞玄: 基于 bert 模型的固件漏洞检测系统	洞玄
129	LogAPT: 面向日志的 APT 检测与链路溯源系统	没钱打什么比赛
130	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	赤旗插满全球队
131	MalGuard-大模型驱动的社交媒体恶意图像细粒度检测系统	Roar MilkDragon
132	玄鉴: 基于选择性状态空间模型的恶意流量分类系统	Besti Club
133	LLM-GUARD: 面向线上大语言模型的多模态数据保护系统	破晓小分队
134	新域密链: 洋葱分层式天地协同安全通信指挥链	绿羽傲飞战队
135	DejaVuzz	舞龙舞狮
136	OS Agent 环境注入评估与防御平台	奶龙熬熬觉
137	紫穹: 基于 LLM 的自动化渗透测试和漏洞修复系统	布吉岛
138	基于 AI Agent 和 LLM 的自动化漏洞修复系统	晚安玛卡巴卡
139	基于全同态加密的去中心化肺炎识别系统	NBUT
140	VideoGuard: 基于大模型的短视频有害内容检测与预警系统	早睡一点吧
141	AudioDefender: 多任务学习驱动的音频伪造检测系统	团结进取
142	漏洞猎鹰 VulnFalcon——精准漏洞根因定位系统	5ufferNarRat0r
143	DeepTestX: 基于大语言模型的深度学习库智能模糊测试系统	智胜先锋
144	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	VK
145	针对内容安全审核平台的可靠性评估系统	bbbbbbupt
146	AxoraFL: 基于区块链的安全高效联邦学习安全聚合系统	银河护卫队
147	“检密”密码算法正确性与一致性验证平台	2324
148	PDM&Fuzz: 基于扩散模型的协议漏洞自动化挖掘系统	VulnXploit
149	同态加密下的多模态安全融合分析系统	重生之我在武工大学密码
150	面向自动驾驶远程劫持攻击的三级协同防御方案	Ghost in the car
151	明瞳——基于移动端 GUI 智能体的 iOS 变身 APP 检测系统	今天又摆烂了对不队
152	瞳驭——高速公路场景下多模态感知与实时预警系统	微笑面队
153	火焰越权漏扫系统	SYN 北方完美夜曲

154	面向深度人脸伪造的肖像保护平台	多进程小分队
155	AI 卫士：大模型的自动化评估平台	大模型的自动化评估平台
156	基于 SM4 加密的后量子投票系统	早八起不来队
157	绘隐鉴权—支持用户端预览的版权图像共享平台	SuperIdol
158	幻彩织影——基于语义引导的双重伪装迷彩	智绘先锋团
159	基于深度学习的网络攻击检测系统	云枢御险
160	VeriDome——多模态深度伪造内容检测系统	阳光开朗
161	ATWatch：基于动态图神经网络的金融异常检测系统	比特守护队
162	智护电网：基于隐私计算的电力大模型预测系统	霸王龙队
163	..	哲臻安全
164	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	游戏王
165	SigTrace：基于数字签名的电子文档泄露溯源系统	FZTO
166	基于混合专家模型的大模型评估系统	大模型评估专家
167	蜂鸟电磁眼：便携式的无人机射频智能监视系统	无人机侦测队
168	碳链宝：基于联盟链与 Agent 的碳市场全流程保护与交易平台	小鸡队
169	面向流媒体语音的高效隐写分析系统	当 0 当 1 不当 3
170	QQQDefender：低成本高效发展的分布式恶意软件检测系统	啊队
171	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	点击生成一个队名
172	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	dky 信安
173	高效隐私盾：机器遗忘架构 ForgetSys-Pro	保证第一队
174	基于谓词加密的分布式无人机群组安全通信系统	要快乐小分队
175	护颜幻盾：面向全生命周期的智能人脸信息保护平台	FaceGuardians
176	ChainSafeFort——灵鉴智能合约检测扩展中枢	格局
177	智能网联车辆动态行驶场景下密钥自主生成系统	牛马小纵队
178	AeroTrust AI 航材智能溯源链	AMC
179	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	Oneyee
180	基于容错预约束的环链端到端加密监管通讯系统	长大网安小队
181	面向工业物联网的跨平台可信数据管理与安全预警系统	Deepsleep 队
182	隐询智索——抗泄漏的多模态隐私查询系统	安全小队
183	隐私防护者，基于双混沌系统的数据安全防护系统	根本写不完
184	云驿密匣——基于鸿蒙系统的国密邮件安全传输系统	無限進步
185	轻量级跨平台动态可搜索加密数据库系统	古月卓文武
186	面向动态网页的 Web 漏洞扫描器的研究与实现	安网先锋
187	基于大模型技术的漏洞静态分析自动化工具	isurA
188	SafeGuard：融合数据增强和对比学习的异常流量识别平台	超级无敌大苹果
189	潜痕——面向 AIGC 的水印版权维护平台	bug 改改改改到厌倦
190	极速木马猎手：轻量化远程访问木马早期检测与终止系统	TCW
191	基于差分隐私的联邦时序集成医学分割模型	沉稳好
192	灵析：大模型协同的智能漏洞挖掘系统	桃李自蹊

193	智瞳：面向串谋行为的恶意小程序检测系统	智瞳
194	鉴影：跨平台黑灰产溯源取证智能体	Not Found 404
195	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	FortFi 小队
196	高熵的物理层密钥生成及安全性评估	拖延症不队
197	基于 Intel SGX 的多层级动态可搜索加密系统	SecureTech 先锋
198	云盾慧眼	星火
199	基于 BERT 和 Deepseek-r1 改进的大语言模型防御器	果酱大王
200	基于语义解耦的联邦式隐私音频伪造检测系统	anti-deepfake
201	隐私政策大语言模型多智能体系统	又寸不又寸
202	“清风”智能新闻鉴伪平台	费大厨队
203	面向工控网络的小样本生成与入侵检测系统	热血沸腾
204	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	星零智御
205	“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	FireEye
206	智盾隐投—基于门限环签名的抗量子攻击电子投票系统	智盾团队
207	LSTC：基于半全局三角中心的网络暴力溯源与预警平台	好想和你凑一队
208	M2X-Guard:基于多引擎协同与多模态数据融合的 XSS 检测系统	安全不打烊
209	面向短视频平台的 AIGC 视频检测与版权保护系统	Crychic
210	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	DoTA
211	散钥于众，聚信于签—基于口令防护的门限盲化钱包方案	山顶
212	一种无监督式的深度伪造检测系统	剥蒜的情谊
213	鲸鱼—基于模型微调和知识蒸馏的恶意流量检测系统	好想和你凑一对
214	Android 应用程序隐私合规检测系统	寒霜火焰鹦鹉
215	SafeIDS：基于数据增强和集成学习的网络入侵检测系统	江大码到成功队
216	CANGenius——车载 CAN 总线智能模糊测试系统	盐水鸭 Carry
217	面向流媒体平台的递进式恶意域名挖掘系统	灵感菇队
218	MiniSentry——基于任务驱动的规避型恶意小程序检测系统	迷你三吹
219	CIBPU:冲突不可见的安全分支预测单元	车安信
220	ECU-SecCom：车载 ECU 安全通信系统	摸鱼小分队
221	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	东北大学小分队
222	玄鉴-MirrorNet：区块链赋能下的网络安全事件记录分析服务系统	驾校保卫处
223	一种基于国产硬件的数字货币冷钱包	勇攀高峰队
224	HSRB-FL：异构场景下安全鲁棒的区块链联邦学习系统	今晚吃毛肚
225	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	代码打得都队
226	多模态水印辅助的智能驾驶风险警示鲁棒识别系统	三个臭皮匠
227	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	Robuster
228	枢阵隐私-基于隐私计算的数据共享平台	Minuscular
229	基于 C/S 架构的用户上网行为管控平台	R@dar202504
230	医影智链——区块链赋能的医学影像安全存储与共享系统	多喝热水队
231	凌瞳——基于大语言模型的 IPv6 智能测绘与安全运维系统	数据都队

232	基于加密 QR 码的快递隐私分级保护系统	码上无忧
233	基于 AIGC 的构造式图像隐写算法设计与系统实现	图像隐写
234	et3	et3
235	VulRator-基于模糊学习的函数级别漏洞挖掘和搜索模型	VulRator
236	面向短视频的多模态舆情安全威胁感知系统	声量科技团队
237	基于大语言模型的自动代码修复工具设计与实现	自动代码修复课题小组
238	IntelliFuzz-NLP:基于模糊测试的智能自然语言处理系统测试平台	INFINITEINTERVAL
239	控制流约束下代码复用攻击检测与风险评估系统	代码敲不队
240	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	piano
241	基于国密 SM9 的通用身份认证与加密通信系统	SM9 信安攻坚队
242	基于 CNN-TCN-Attention 混合神经网络的新型入侵检测系统	404 NOT FOUND
243	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	拉仓巴拉丹扎木苏日丹队
244	AIGCTraceShield 大模型生成内容溯源平台	哈基米小队
245	安全之钥-轻量级密码算法的唯密文故障分析软件	定坤
246	面向内容理解的选择性图像加密系统	取名好难
247	MoLLaFuzz——基于 LLaMA 生成式大语言模型的工业协议漏洞挖掘	momo
248	隐心智链：基于匿名加密与大模型的心理守护平台	今天你摆烂了对不队
249	基于跨模型通用对抗水印的人脸图像保护微信小程序	d11Times' fans
250	PicGuard：绘画图像的主动对抗防御扩散模型	untitled
251	司法卫士：裁判文书网大模型聚汇分析与辅助决策系统	智汇司法
252	基于对抗性隐喻的语言模型越狱攻击	PPSUC
253	基于阈值与混合行为分析的僵尸网络恶意域名检测系统	SSNH
254	Secure Cloud—安全存储与可靠计算云平台先行者	芒果菠萝
255	ImageGuard：基于 SRE-LICM 算法的图像隐私保护系统	404 Not Found
256	御网天鹰——全流量驱动的大模型自动化漏洞挖掘系统	御网天鹰
257	Deep Shield—基于 FreqNet 的 AI 伪造图像识别系统	海底小分队
258	SQLXGuard：Web 下的 SQL 哨兵	TopOne-Sec
259	基于 CodeQL 的 C/C++同源漏洞检测	QL 队
260	VoiceGuard——多模型韵律保持语音防护系统	老谢野混沌
261	抗量子可扩展 SM4 国密算法的 FPGA 优化实现	璇玑镖局
262	支持 HarmonyOS NEXT 的密文关键词检索完整性验证	Cyber 飞行者
263	基于联邦深度学习和同态加密的疾病诊断医疗系统	NULL
264	地脉舆擎—基于复杂网络的事敌舆情监控系统	洪磊全球粉丝后援会
265	御音卫士——基于组合防御的智能座舱语音对抗防御系统	御音卫士团队
266	双模态 CoT 后门：LLM/VLM 具身智能的知识图谱增强攻防	史迪奇大队
267	知识库与人工智能赋能的分布式入侵检测系统	何不归乡
268	基于 LightGBM 的抗翻录鲁棒水印系统	音控盾
269	基于大模型技术的软件漏洞全流程管理	602
270	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	深藏 blue 队
271	威胁慧眼-知识驱动的智能威胁情报构建和分析平台	HIT-威胁情报
272	融合威胁情报与多智能体的网络入侵检测系统	GZU-007

273	ProtoMind——基于大模型的智能协议解析与自动化测试系统	龙盘队
274	智瞳安网——基于设备指纹的以太网终端接入识别系统	智鉴网纹小队
275	睿眸-智能恶意威胁分析系统	打饭不被插队
276	基于耳道内提取心音的身份认证系统	开饭手马克
277	DeepTraceAudit 基于数据流和控制流的代码审计系统	御林安全工作室
278	日新钥异：长期服役物联网安全无线密钥生成系统	理工神盾局
279	量子方舟——面向 PQC 迁移的混合证书签发和验证系统	心算 DILITHIUM
280	支持多模态的大模型安全等级评测与加固系统	大卫说得队
281	擎翼盾-MA：无人机动态通信欺诈实时拦截系统	赛博神谕
282	基于无害化后门的 RAG 数据库水印技术	代码敲到失联
283	多协议动态化智能网联汽车异常流量检测系统	Deep blue dream
284	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	猛攻鼠鼠队
285	FLARE：面向商用大模型的事实与逻辑双通道幻觉检修系统	超高校级的信安 F4
286	PassSlayer——零信任全覆盖无密码认证系统	放学后茶会
287	区块隐锋-抗关联生成式区块链隐蔽通信系统	Amaterasu
288	御网苍穹-基于机器学习的无人机集群网络入侵检测	御网苍穹
289	基于 ECDH 算法的无人机安全通信系统	哈基米哈气
290	护城卫士--基于联邦学习的城市安防智能分析平台	闪亮的代码
291	FuzzSol——基于灰盒模糊测试的智能合约漏洞检测系统	fuzzlover
292	安驰星盾：基于自适应多模态网络入侵智能分析平台	我和评委站一队
293	基于语义分析与混合神经网络的 SQLi 检测系统	霍格沃兹网络安全部
294	WaterVeil——基于 UDH 编码驱动的屏摄鲁棒可溯源水印系统	MICS LAB
295	大语言模型驱动的移动应用密码技术安全审计系统	东里四小只
296	智核——基于强化学习的轻量级物联网 PUF 身份认证系统	疯狂星期四
297	鉴真——面向中文语义的跨模态新闻伪造检测平台	TruthDecoder 识真者
298	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	Achieve Science
299	基于大语言模型的智能化漏洞检测与分析系统	杭电网安
300	AI 换脸风险预警	海棠果
301	慧语星枢——基于提示词工程的二进制漏洞检测平台	TRTPS
302	基于动态交易网络的 Web3 恶意账户细粒度检测系统	桃花灼灼
303	VisionGuard AI——多模态图像真实性智能检测系统	猛猛冲就行
304	基于国密算法的 CA 认证中心	BSXY
305	基于关联数据具有自主身份属性约束的选择性披露凭证	龙马一启冲
306	基于模糊测试的智能合约漏洞检测系统	铸盾卫士队
307	图片防篡改及水印生成检测系统	星海护卫队
308	源御——基于 iOS 的移动网络入侵检测系统	云想小队
309	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	没有想法
310	AegisCode——上下文感知驱动的项目级安全增强代码自动生成系统	灵码神盾
311	面向人脸定制化生成模型的主动防御系统	ID 防火墙
312	心电密码	真的好累
313	基于光学编码与混沌加密的高安全性数据传输系统	吉农信安小分队

314	VulTracer: 基于大模型提示词增强的源代码漏洞检测系统	VulTeam
315	Fenrir-基于 MCP 的自动化代码审计工具	Bri9htM0on
316	闻声识机——开集环境下手机型号鉴别系统	hfut
317	支持双重版权保护的结构化数据水印平台	InkSec
318	基于多模态 Agent 的工业异常检测平台	大佬打架不站队
319	ThreatHunter: 基于 AI Agent 的自主渗透和系统安全风险评估平台	Found404
320	鸾鸟网安——智能网络攻防一体化平台	Spark
321	火眼金睛——多模态视频篡改检测与定位系统	锃斤拷烫烫烫
322	FadeMind: 面向扩散模型的多概念遗忘系统	不秃头小队
323	ETGuard: 电网智能终端设备威胁狩猎系统	二仙桥暴龙
324	基于入侵检测技术与混合 Transformer 的智能网络安全防护系统	对影成明月
325	动态可伸缩的 FPGA 可信机密计算环境	云芯可信
326	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	伏羲矩阵
327	面向服务与流量双重欺骗的弹性蜜罐防御系统	弹弹弹性
328	基于 TCM 安全芯片的可信内容发布与防篡改系统研究	春日部防卫队
329	Falcon: 基于路径敏感稀疏分析的供应链漏洞挖掘系统	专业团队
330	智盾哈希——基于深度哈希技术的恶意软件检测平台	SunnyDay
331	智能网络安全实训云平台	F0yt34m
332	基于负数据库的隐私保护脑电波识别系统	鸡猫牛
333	天盾-智能反恐侦察车	压力队
334	LLM-Guardian: 大语言模型安全评估系统	Timekeeper
335	基于语义-行为建模 LLM 的反沙箱检测系统	AAA 批发中心
336	智鉴·云盾——基于深度学习的恶意代码检测系统	顶呱呱
337	棱鉴——基于深度学习的 AIGC 图像鉴别和篡改识别溯源系统	果之林批发部
338	摄界经纬——拍摄地智能识别与连续定位系统	经纬智盾
339	SVD-GAN 驱动的区块链交易异常检测系统	emm
340	玄壁——Linux 主机安全防护平台	King
341	支持流式轻量测量与多维扩散异常检测平台	流量哨兵巡航队
342	“颜盾”——基于自学习扰动的图片隐私防护系统	颜盾
343	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	乐迪队
344	AetherCTF: 自进化智能体驱动的次世代 CTF 实训平台	赛博佛组
345	Sec-Protector: 基于大模型的多智能体系统密钥泄露检测工具	链时代小分队
346	凌悟 RAG 智慧引擎——大模型幻觉缓解方案	跟上不要掉队
347	支持跨域多方可验证的分布数字身份系统设计与应用	无名
348	“星火·智鉴”——基于大语言模型的虚假新闻智能检测系统	fakebuster
349	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	年轻无极限
350	加密通信应用程序	超级飞侠
351	DomainGuard: 恶意域名实时检测系统	0day 快递员