附件1：

|  |  |
| --- | --- |
| **领域** | **主要内容** |
| 合规治理 | 关键基础设施安全建设、安全审计、合规落地、等保、IPV6、密评、个人信息保护 |
| 区块链 | 区块链密码学、区块链协议、区块链安全与隐私、应用层安全、客户端安全、合约层安全、共识层安全、WEB3.0 |
| 基础安全 | 围绕国产基础硬件（芯片、服务器等）、基础软件（操作系统、数据库、中间件等）、应用软件（OA、ERP、办公软件等）、信息安全（边界安全产品、终端安全产品等开展行业应用研究 |
| 人工智能 | 人工智能在安全领域应用,包括但不限于在代码审计、漏洞挖掘、攻击模拟、威胁检测与响应、情报和安全策略分析、安全运营赋能、自动化威胁狩猎应用等方面 |
| 红蓝对抗 | 攻防演练常态化、钓鱼防护、免杀对抗、检测和降噪、多源威胁情报、加密流量检测、白利用、数字取证和事件响应（DFIR）、终端和主机防护 |
| 云安全 | 云原生安全、容器和K8S安全、业务上云、多云管理、云安全审计 |
| 移动安全 | BYOD管理、移动办公、小程序和APP安全检测与防护、SDK安全、隐私保护 |
| 安全架构 | 安全规划和设计、安全韧性、安全防护体系、SASE、零信任、自适应防护体系、低时延安全架构、IPV6部署和防护、边缘计算 |
| 安全管理 | 安全制度、流程闭环管理、风险管理、价值体现、职责划分、团队建设、人才培养、安全可视化、安全意识建设、MSS托管探索 |
| 安全开发 | AI开发赋能、DEVSECOPS、安全需求库、开源治理、威胁建模、内存安全、内生安全、切面安全、软件供应链安全 |
| 业务安全 | 业务安全需求建模、AI生成内容（AIGC）的检测、风险识别、典型业务安全场景监控和防护、机器流量识别与对抗（AntiBot）、API接口安全 |
| 安全运营 | 资产梳理和攻击面管理、态感、挂图作战、SOAR、流量分析、密码托管、特权管理、安全验证、供应链管理、身份鉴别与权限管理（IAM）、闭环管理、风险治理、安全指标体系 |
| 数据保护 | 勒索病毒防护、数据分级分类、数据合并整合、隐私增强、防泄漏、数据数据出境 |
| 其他 | 其他安全相关方向 |

安全创新领域及主要内容说明