附件1：

安全创新领域及主要内容说明

|  |  |
| --- | --- |
| **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、隐私保护 |
| 信创安全 | 围绕基础硬件（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、情报分析、安全检测、安全运营等方面 |
| 红蓝对抗 | 攻防演练常态化、免杀对抗、WebShell检测、多源威胁情报、加密流量检测、数字取证和事件响应（DFIR） |
| 云安全 | 云原生安全、容器和虚拟化安全、业务上云、多云管理、云安全审计 |
| 移动安全 | BYOD管理、移动办公、APP安全检测与防护 |
| 安全架构 | 安全域划分、安全防护体系、SASE、CASB、零信任、自适应防护体系、低时延安全架构 |
| 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 |
| 安全开发 | DEVSECOPS、安全需求库、开源治理、威胁建模、安全规划和设计、内生安全、安全验证、软件供应链安全 |
| 业务安全 | 业务安全需求建模、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）、隐私计算、API接口安全 |
| 安全运营 | 资产梳理、态感、SOAR、流量分析、特权管理、攻击面管理、安全有效性验证、供应链管理、身份鉴别与权限管理（IAM）、加解密 |
| 其他 | 其他安全相关方向 |