附件3：安全保障服务

| **序号** | **分类** | **服务** | **描述** |
| --- | --- | --- | --- |
| 1 | **安全检测与监控** | 系统上云检测 | 业务系统在生产环境上线前，依据系统重要性，提供安全基线检查、渗透测试、代码审计等全面的安全检测服务，提供检测报告与整改建议，并提供复测服务 |
| 2 | 系统漏洞扫描 | 为业务系统提供定期的操作系统、中间件、数据库等系统漏洞扫描服务，提供扫描报告与整改建议，并提供复测服务 |
| 3 | Web漏洞扫描 | 为业务系统提供定期的Web应用漏洞扫描服务，提供扫描报告与整改建议，并提供复测服务 |
| 4 | 安全威胁监控 | 为业务系统提供实时的安全威胁监控服务，提供安全事件通报单与整改建议，并提供复测服务 |
| 5 | **网络防护** | 边界访问控制 | 针对云各网络边界，依据业务系统的访问规则，提供白名单方式的南北向网络访问控制服务 |
| 6 | 云内访问控制 | 依据业务系统在云内的访问、交互规则，提供白名单方式的东西向网络访问控制服务 |
| 7 | 入侵防御 | 提供识别业务系统异常网络访问并对其进行阻断服务 |
| 8 | 抗DDoS | 为互联网发布的业务系统提供高可靠的抗DDoS防护服务 |
| 9 | **主机防护** | 安全登录 | 通过堡垒主机为虚拟服务器提供专网内的安全登录服务 |
| 10 | 操作审计 | 通过堡垒主机为虚拟服务器提供操作审计等服务 |
| 11 | 防病毒 | 为虚拟服务器提供实时防病毒监控服务，并提供病毒查杀服务。 |
| 12 | **应用防护** | 网页防篡改 | 为互联网发布的业务系统提供网页防篡改服务，避免源站被恶意攻击和入侵，防止源站地址被篡改 |
| 13 | Web应用防护 | 依据互联网发布的业务系统的访问规则，提供网页挂马监测、黑词暗链监测、可用性监测、未知资产监测等的应用层前端防护服务，对各类请求进行内容检测和验证，并对非法的请求予以实时阻断 |
| 14 | 数据防爬虫 | 通过DNS流量清洗，为互联网发布的业务系统提供页面数据的防爬虫服务 |
| 15 | **数据备份与审计** | 自动备份 | 提供针对虚拟服务器的可自助设置时间点的自动备份服务 |
| 16 | 手动备份 | 提供针对虚拟服务器的可自助设置时间点的手动备份服务 |
| 17 | 专用设备备份 | 提供专门的备份设备，可进行文件、数据库、虚拟服务器等备份功能，需信息中心协助配置 |
| 18 | 数据库审计 | 通过配置数据库信息、分析抓取数据库访问流量，提供数据库访问、操作等行为审计服务 |
| 19 | **配合支持** | 补丁更新支持 | 为业务系统管理单位开展虚拟服务器补丁更新提供技术支持服务 |
| 20 | 应急处置支持 | 为业务系统管理单位开展安全事件处置提供技术支持服务 |
| 21 | 等保测评配合 | 配合业务系统管理单位完成系统的等级保护测评 |