**网路安全服务清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务**  **项目** | **服务描述** | **服务方式** | **服务**  **说明** | **服务输出**  **文档** |
| 1 | 安全风险评估服务 | 安全风险评估，是从风险管理角度，运用科学的方法和技术手段，分析网络与信息系统所面临的安全威胁及存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，并提出针对性的安全防护建议和整改措施。  安全风险评估是对网络中已知或潜在的安全漏洞、安全风险、安全隐患，进行探测、识别、控制、消除的全过程，它是信息安全服务工作的必要组成部分，是信息安全工作中非常重要的一个环节。  安全风险评估的参考标准主要是GB/T 20984、GB/T 31509、公安部等级保护，风险评估方法包括但不限于资料收集、调查问卷、人员访谈、现场查勘、漏洞扫描、基线核查、风险分析。 | 现场 | 合同期间按需执行 | 输出包括但不限于 《安全风险评估报告》、《资产分析报告》、《脆弱性评估报告》、《威胁评估报告》 |
| 2 | 等保建设咨询服务 | 等保差距分析，是依据公安部等级保护基本要求，从物理、网络、主机、应用、数据、制度、机构、人员、建设、运维共十个方面，分析信息系统安全防护能力与对应等级要求之间的差距，明确不满足项并提出整改建议。  不同等级的要求存在差异，所以不同等级应用系统的等保差距分析，其工作量也存在差异。目前，应用系统大多定为二级或三级，等级越高，工作量越大。  等保差距整改，是双前期的等保差距分析报告为依据，为客户设计满足等级保护要求、可落地执行的安全整改建设方案并执行，确保信息系统满足等级保护要求，并顺利通过等级保护测评。  我们的等保差距整改，将以纵深防御为主要设计思路，为用户提供“三重防护、一个中心”的安全整改建设方案。 | 现场 | 合同期间按需执行 | 输出包括但不限于 《XX系统等级保护差距分析报告》（含安全整改建议）、《XX系统等保差距整改建设方案》 |
| 3 | 安全巡检服务 | 安全巡检服务，对高速公路路段中心、收费站和ETC门架的网络设备、安全设备、重要业务系统、重要终端等进行的安全检测，检测完成后提供全面的巡检报告，报告中给出存在的安全风险并提供对应的修复建议。  安全巡检服务内容，包括安全漏洞检测、基线配置核查、安全日志审计。 | 现场 | 每季度一次，合同期内共4次； | 输出包括但不限于 《XX安全巡检服务报告》《XX安全漏洞检测报告》、《XX基线配置核查报告》、《XX安全日志审计报告》 |
| 4 | 安全加固服务 | 安全加固服务，是协助对目标系统的安全漏洞进行修复、配置隐患进行优化的过程。  安全加固是保证设备和系统安全运行的关键防护措施，通常情况下，操作系统、数据库、中间件、网络设备、安全设备，都需要进行安全加固。 | 现场 | 合同期间按需执行 | 输出包括但不限于《XX安全加固报告》（含加固前后漏洞对比）、《XX加固前漏洞扫描报告》、《XX加固后漏洞扫描报告》、《XX安全加固应急及回退方案》 |
| 5 | 安全应急响应 | 应急响应服务，是在业务系统或服务器遭受黑客入侵攻击时，第一时间对入侵事件进行分析、检测、抑制、处理，查找入侵来源并恢复系统正常运行。  我们的应急响应服务，在完成应急事件事处理后，还将提供详细的应急响应报告，报告中将还原入侵过程，同时给出对应的解决方案。 | 现场 | 合同期间按需执行 | 输出包括但不限于 《XX系统安全应急响应报告》、《XX系统安全事件应急预案》 |
| 6 | 安全应急演练 | 根据应急预案和演练方案，协助用户完成各类安全事件的应急处置演练工作，确保安全应急工作的标准化和流程化，以及安全应急的效率和质量。  针对特定演练场景（网页被篡改攻击、网站遭受DDOS攻击、内网ARP攻击等)，制定演练预案、准备演练工具、参与演练软环境准备、协助演练硬件环境调测验证、进行正式应急演练、汇报总结。 | 现场 | 1次 | 输出包括但不限于《XX安全应急演练报告》 |
| 7 | 安全通告服务 | 安全通告服务，是每月为用户提供信息安全研究月报，月报内容包括本月的信息安全整体态势、新增漏洞数量、漏洞分布情况、高危漏洞分析、本月主要安全事件，以及针对新漏洞的更新和防护方案。  同时，在出现重大安全漏洞和突发事件时，将第一时间进行深度分析，并将对应的分析报告提供给用户。 | 远程 | 每月1次，合同期共12次 | 输出包括但不限于《xx信息安全研究月报》、《xx重大事件分析报告》 |
| 8 | 重大活动安全保障 | 在重大会议或重大节假日期间，为用户提供全程的网络安全保障工作，确保用户业务系统的安全稳定运行。  1、内外网暴露面与风险清理：对保障单位内外网进行资产初步梳理，发现发布应用、以及各类业务系统，发现网络内开放的端口情况，摸清资产情况，下线无主资产、关闭风险端口，同时探测相关资产存在的漏洞隐患，形成整改清单。  2、人员驻守服务：提供10人天以上的安全值守服务，对发现的安全风险及时处置，组织和协调全体保障人员，共同分析研判和封堵网络攻击行为。  3、防护能力提升服务：针对发现的问题及防护短板，提出安全策略优化与加固建议，提供满足防护要求的安全设备解决方案，并安排专业的技术人员随时监测攻击事件并及时处置。 | 现场 | 合同期间按需执行 | 输出包括但不限于《xx现场值守日报》、《xx现场值守工作总结》、《xx网站安全应急响应预案》、《xx安全事件应急响应报告》 |
| 9 | 安全意识培训 | 为用户提供安全意识培训，内容包括信息安全普及知识、法律法规、安全趋势、安全管理、移动安全、大数据安全以及常见办公安全等。 | 现场 | 1次 | 输出包括但不限于《XX单位安全意识培训记录》 |
| 10 | 其它 | 根据业主需要，提供多种排名领先品牌的专业漏扫工具、基线核查工具、U盘接入检测工具、违规外联/内联检测工具等。 | 远程 | 合同期间按需执行 | 输出包括但不限于《XX单位安全检查报告》 |