**附件一：黑猫电子招标采购交易平台安全服务**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **服务名称** | **服务简介** | **服务频率** | **服务配置** |  |
| 脆弱性检测 | 脆弱性检测识别信息系统各个层面中可能使资产受损的薄弱环节，针对景德镇黑猫咨询有限责任公司网络结构主要有以下层面进行检测：1、弱口令检查：对所有系统进行一轮关于账号安全策略的检查；2、安全基线核查：使用软件自动及手工的方式对网络设备、安全设备、主机、数据库配置标准，并输出报告； | 每季度一次 | 现场调查过程：拟指派初级工程师、中级工程师/项目经理（CISP/PMP）；后台整理/分析：拟指派高级工程师（CISP/CISSP）； |  |
|
|
|
| 全网漏洞探测及验证 | 通过漏洞扫描工具向网络目标系统发送测试代码，从目标系统的反馈结果，以得到目标系统有敏感信息或探测是否存在安全漏洞的过程。并对确认后的加固内容进行实施，并对加固效果进行验证和核查。 | 每季度一次 | 现场调查过程：拟指派初级工程师、中级工程师/项目经理（CISP/PMP）；后台整理/分析：拟指派高级工程师（CISP/CISSP）； |  |
| 渗透测试 | 从攻击者的角度来对信息系统的安全程度进行安全评估。对现系统不造成任何损害的前提下，模拟入侵者对指定系统进行攻击测试。确定用户系统所存在的安全威胁，及时使安全管理员发现系统维护和管理中的不足，以降低安全风险，对应单位重要信息业务安全建设尤为重要。 | 一年两次 | 拟指派中级渗透测试工程师、高级渗透工程师。 |  |
|
|
|
| 应急响应 | 主要针对重大安全时期以及安全事件发生时建立起安全响应机制，把损失和破坏降低到最低限度、弥补那些被利用缺陷、恢复计算服务。7\*24小时应急技术支持服务，以最快速度恢复网络、系统的可用性，阻止和减小安全事件所带来的负面影响，并对以下范围安全事件进行威胁清除、溯源分析并协助加固业务系统安全，输出《应急响应分析及处置报告》至少包含安全事件分析，处置结果分析，残留风险分析，安全加固和改进建议。 | 按需 | 拟指派中级渗透测试工程师、高级工程师、项目经理； |  |
| 安全威胁专项分析 | 通过分析业务系统基础信息，以现网业务执行者视角为基础，分析操作轨迹全生命周期中产生的日志信息，确定具备审计价值的关键要素，形成黑白名单相结合的行为场景，并根据现网实际情况评估操作轨迹中存在的风险点与监控盲点。 | 一周一次 | 每周输出威胁分析详细报告 |  |
| 安全通告与预警服务 | 信息安全是动态发展的。面对日益演变的安全攻击手段和系统安全漏洞的不断发现和利用，信息系统所面临的风险也在不断变化。每月提供实时安全动态及最新的安全技术和安全理念。 | 每月一次 | 总部电子邮件预警服务 |  |
| 合计 |  |  |  |  |