采购需求清单

项目编号：GZSSNG-WSXJ-JYJYB-2021-005

广州市少年宫2021年信息安全保障服务项目采购需求清单：

1. 安全扫描  
   1.服务范围：综合管理应用系统、门户网站、学员系统

2.服务内容

定期对应用系统漏洞扫描，及时发现高危风险漏洞，发出安全预警和制定加固防御方案。   
 服务主要包括：

* 系统漏洞扫描

利用漏洞扫描软件对网络设备、操作系统的各类安全问题测试，测试内容包括共享目录、账户信息、账户口令、系统漏洞等系统基本信息进行扫描。

* 数据库扫描

利用漏洞扫描软件对服务器运行的数据库系统进行安全测试，测试内容包括数据库帐户安全、漏洞测试等。

* 应用安全扫描

利用漏洞扫描软件针对服务器运行的应用系统进行安全测试，测试内容包括帐户安全、应用脚本安全测试。   
通过漏洞扫描服务及时发现信息系统存在的各种安全隐患（网络结构、网络设备、服务器主机、操作系统、数据库和用户账号、口令等安全对象）和应用系统的漏洞。   
 3.服务频率：每月一次   
 4.服务成果：《安全扫描报告》

1. 渗透测试

1.服务范围：门户网站、学员系统

2.服务内容   
 以手工测试为主，工具测试为辅，在授权和监督下对指定系统进行非破坏性质的攻击性测试，并对结果进行单独验证和交叉验证。测试对象以B/S架构为主，兼顾网络和操作系统。渗透测试实施前编写详细的实施方案和实施计划，用于指导和规范渗透测试工作，渗透测试完成后必须提交渗透测试报告，除了描述发现深层次的安全漏洞外，还需要详细描述入侵过程，获取渗透对象的重要数据等步骤。   
渗透测试工作程序：

* 信息收集

使用NMAP、whois、Trace、PING等工具和搜索方式对测试目标的存活情况、网络注册信息、域名等基础情况进行信息收集，为下一步渗透测试提供基础资料。

* 端口扫描

采用NMAP等扫描工具对测试目标的TCP/UDP端口进行扫描，以测试目标对外提供的应用服务。   
通过获知的应用服务，测试人员将会根据已知服务初步判断可能存在、利用的安全弱点，为下一步渗透提供依据。

* 口令猜解

主要采用暴力破解工具：根据定义好的字典，对目标系统进行口令猜测。   
口令猜解包括2个方面猜解：用户名猜解、密码猜解。

* 认证测试

根据手头帐户信息及默认认证信息，手工登录尝试。认证测试主要为了验证受测系统是否存在管理、设计等方面的问题。

* 溢出测试

测试人员利用溢出工具对测试目标进行溢出测试的目的是，测试计算机程序的可更正性缺陷。   
溢出测试包括远程溢出和本地溢出。

* 远程溢出

测试人员在外网通过溢出工具对测试系统边界设备或者系统内部服务器进行的溢出操作，通过远程溢出测试发现和验证目标系统是否存在严重的安全漏洞。   
远程溢出测试主要根据目标系统软件版本存在的安全漏洞。

* 本地溢出

本地溢出测试指的是在测试人员获取了某个测试系统的一般账户之后，通过特殊的代码或者软件将一般账户的权限提升，以此获取更多的操作权。   
本地溢出能够实现的关键是一般账户的获取，因此本地溢出测试可以发现目标系统在账户安全策略的安全弱点。

* WEB注入测试

脚本注入测试主要针对WEB网站服务器和后台数据库，利用SQL注入、脚本代码、cookie等方式获取WEB目录的访问或者对后台数据库进行操作，以此来发现WEB网站在网站安全配置、数据库安全配置、网页代码等方面是否存在安全弱点。一般来说，脚本注入测试主要测试以下内容：测试网站验证模块是否能够让非法用户绕过认证；测试数据库接口模块是否存在非法用户通过数据库提供的某些接口进行系统操作；测试网站脚本代码是否存在通过提交自定义的URL（自定义的RUL往往含有特殊字符）来修改后他数据库；其他网站安全弱点。   
 3.服务频率：每年一次   
 4.服务成果：《渗透测试方案》、《渗透测试报告》

1. 网站监控

1.服务范围：网站

2.服务内容

* 监控网站的可用性，确保网站的可用性程度（监控频率：5分钟）
* 监控网站的响应时间（监控频率：5分钟）
* 监控网站的下载速度（监控频率：5分钟）
* 监控网站的HTML加载时间（监控频率：5分钟）
* 监控网站的服务器端口连通性（监控频率：5分钟）
* 监控网站的DNS劫持（监控频率：5分钟）
* 监控网站的首页敏感字和关键内容（监控频率：1小时）
* 监控网站的首页挂马（监控频率：1小时）
* 7x24小时远程人工值守验证服务
* 网站安全漏洞扫描、挂马扫描、疑似被篡改扫描

1. 服务频率：服务期内7×24小时全程监测。   
   4.服务成果：《网站监控日报》、《网站监控月报》

四、应急演练   
1.服务范围：综合  
2.服务内容

通过测试与演练工作，提高应急响应人员的应对信息安全突发事件的能力，及时发现各部门应急预案中可能存在的不足和缺失，并依此对预案及其管理系统进行持续的改进。应急演练内容如下：

* 制定应急演练计划；
* 应急演练流程、规范培训；
* 审核现有关键应用系统应急预案；
* 设计应急演练场景；
* 编制应急演练脚本；
* 应急演练执行
* 应急演练评价
* 应急演练总结

3.服务频率：一年一次，一次桌面演练，一次实战演练

4.服务成果 ：《信息系统应急演练方案》、《信息系统应急演练总结报告》

五、应急预案编制和应急响应服务  
 1.服务范围：综合   
 2.服务内容   
 立足于单位自身的安全管理及系统监测预警、应急处置能力的现状，协助客户建立、健全网络安全事件应急预案体系。通过分析应急响应需求、预案规划、编制、评审成果文档，确保应急预案体系的合规、完善以及可落地执行性。

为保障业务安全稳定运行，确保在出现安全事件时有完善、有效的应急响应支持服务，提供的应急响应服务能对安全事件作出合理分析，及时处理安全事件。   
 安全事件是指信息系统中的计算机或网络设备系统的硬件、数据因非法攻击或病毒入侵等安全原因而遭到破坏、更改、泄漏造成系统不能正常运行，或已经发现的有可能造成上述现象的安全隐患，如非授权访问、信息泄密、系统性能严重下降、蠕虫或大面积爆发病毒等。   
较大安全事件包括：

* 业务中断
* 大规模病毒爆发
* 网络瘫痪
* 主机或网络异常事件
* 数据丢失
* 涉密信息泄密

应急响应服务主要包括以下内容：

* 排查故障，隔离关键数据；
* 攻击手段分析，提供应急方案或工具软件；
* 定位攻击来源，提出安全建议；
* 数据及网络业务恢复。

3.服务频率：一年一次   
4.服务成果：《应急响应事件处置报告》

六、安全培训服务  
1.服务范围：广州市少年宫全体工作人员   
2.服务内容：   
1、通过对用户的人员进行技术培训，使其具备对信息安全防范意识的理解、掌握信息安全基础知识、了解信息安全的原则等；

2、通过信息安全培训，使用户能在较短的时间内，掌握信息安全基础知识、安全攻防基础知识、安全事件应急预案等，掌握基本的信息安全事件的应急处置，协助用户在不同状况的应急预案处理，以保证信息系统的正常、安全地运行。

3.服务频率：一年一次   
4.服务成果：《安全培训材料》

七、服务工具提供

服务商为达到本项目的信息安全目标，应提供使用：网站监控工具、渗透测试工具、应急响应取证分析工具、安全运维公共服务管理工具、安全检测与加固软件和安全配置管控软件各 1 套外，其费用包含在项目总价里。

所有服务工具产生数据需电子化，可通过数据接口、数据导入等方式与中心网管监控运维平台系统进行数据集成，如涉及的数据电子化和数据接口开发、数据导入费用由投标人承担。   
服务期过后，服务工具中的数据需保留给广州市少年宫，数据清除后服务工具返还服务商，确保数据的完整性和机密性。   
为避免产权和使用权纠纷,投标人必须承诺在签订合同时,提供服务期内使用的软件产品和工具的知识产权证明或原厂商针对本项目的租赁(或购买)的相关证明文件原件送采购人审查核对,如不能提供原件或资料与投标文件不符,所产生的后果由中标人负责。   
 各工具具体参数要求如下：

1.网站监控工具

网站监控工具具有报警功能，实现网站可用性监控、及时准确的发现被 篡改的页面。通过架设网站监控平台，对网站的可用性、网页的完整性 进行远程监控，一旦发现网站某个网页被恶意篡改，能立即准确定位， 获得被篡改前后的内容对比，并可以及时发出警报，在第一时间通知相 关技术人员进行应急处理。

**主要功能列表**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能项** | **要求** |
| 1 | 网站状态的监控 | 能通过曲线图跟饼形图形象的反映网站的可用性情况 |
| 2 | 网站响应时间监控 | 提供网站响应时间监控，当响应时间超过阀值时，及时产生报警。 |
| 3 | 网站 HTML 加载时间监控 | 提供网站 HTML 加载时间监控，当网站 HTML 加载时间超过阀值时，及时产生报警。 |
| 4 | 网站下载速度监控 | 提供网站下载速度监控，当网站 HTML 加载时间超过阀值时，及时产生报警。 |
| 5 | 服务器端口连通性监控 | 系统通过曲线图跟饼形图形象的反映服务器端口的可用性情况 |
| 6 | 网站 DNS 劫持监控 | 提供灵活的 DNS 劫持监控，当 DNS 解析出现故障时及时报警，减少损失，降低影响。 |
| 7 | 页面敏感字监控 | 提供页面敏感字监控服务，及时发现网页中的敏感字予以报警，降低影响。 |
| 8 | 页面关键内容监控 | 提供页面关键内容监控服务，及时发现网页中缺失的关键内容并予以报警，降低影响。 |
| 9 | 疑似篡改监控 | 提供两种级别的网站篡改监控服务，第一种为首页疑似篡改监控服务，第二种为全站疑似篡改监控服务，当响应时间超过阀值时，及时产生报警。 |
| 10 | 网站挂马监控 | 1、网站挂马监控状态：能显示网站监控各项功能的监控状态汇总，包括“无报警”，“有报警”“异常但未报警”。  2、网站挂马监控详细情况：能查看木马扫描结果的汇总列表，包括挂马数量，涉及到的CVE 等信息 |
| 11 | 网站漏洞扫描 | 根据用户选择，安排调度漏洞扫描任务，将任务通过技术接口传送给漏洞扫描系统；漏洞扫描系统在接到任务后对目标网站进行漏洞扫描，并将最终结果通过接口交付给监控工具 |
| 12 | 基于业务的自动监 控 | 业务监控 业务监控状态各节点状态监控  各节点报警 |
| 13 | 产品资质证书 | 提供计算机软件著作权登记证书复印件 |

2.安全检测与加固软件

提供基于Web应用的自动化安全漏洞扫描配套工具，能扫描和检测所有常见的Web应用安全漏洞 ，例如 SQL  注入（SQL-injection）、跨站点脚本攻击（cross-site  scripting ）、缓冲区溢出（buffer overflow）及最新的 Flash/Flex 应用及 Web  2.0 应用曝露等方面安全漏洞的扫描。

主要功能列表

|  |  |  |
| --- | --- | --- |
| **序号** | **功能项** | **要求** |
| 1 | 知识库 | 内置漏洞知识库漏洞信息47000条，提供详细的漏洞描述和对应的解决方案描述。 |
| 2 | 智能扫描 | 可以智能发现非默认端口启动的服务，并调用相应扫描插件进行扫描。 |
| 3 | 仪表盘 | 从多种数据源获取实时数据，以丰富的、可交互的可视化界面为数据提供更好的使用体验。 |
| 4 | 报告生成 | 提供对漏洞扫描结果进行综合分析、综合评分，并输出包含漏洞扫描内容的综合报表。 |
| 5 | 登录扫描 | 提供对目标系统进行登录扫描。 |
| 6 | 定时计划任务 | 提供对多个扫描任务并发执行，提供多任务自动调度。提供定期扫描与周期扫描（周期扫描可细化到隔天、隔周、隔月）。 |
| 7 | 图形化界面 | 界面友好，并有技术文档；所有的图形界面均具备中文。 |
| 8 | 终端 | 支持同时运行4个以上虚拟机，可移动热拔插，响应时间不高于5秒。 |
| 9 | 产品资质证书 | 提供计算机软件著作权登记证书复印件。 |

3.安全运维公共服务管理工具

通过集中采集信息系统中的系统安全事件、用户访问记录、系统运行日志、系统运行状态等各类信息，经过规范化、过滤 、归并和告警分析等处理后，以统一格式的日志形式进行集中存储和管理，结合丰富的日志统计汇总及关联分析功能，实现对信息系统日志的全面审计，能够随时了解整个系统的运行情况，及时发现系统异常事件；同时当特殊安全事件和系统故障发生时，通过安全管理平台能够进行快速定位，并提供客观依据进行追查和恢复。

**主要功能列表**

|  |  |  |
| --- | --- | --- |
| 序号 | 功能项 | 要求 |
| 1 | 产品要求 | 自行开发，具备计算机软件著作权登记证书。 |
| 采用SaaS服务模式为所有用户提供安全服务，租户之间的数据采用逻辑隔离的方式，从而保护租户数据隐私。 |
| 系统自身自动保存登录日志与操作日志供审计。 |
| 2 | 运行环境 | 基于B/S架构（监视及管理），中文界面，风格友好，操作简便。 |
| 采用JAVA架构开发，支持在Linux系统上运行。 |
| 产品要求集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护。 |
| 3 | 使用界面 | 采用基于浏览器的用户界面，至少支持IE与Firefox。 |
| 4 | 管理范围 | 涵盖主机、数据库、中间件以及提供相关接口的应用系统 |
| 5 | 综合展示 | 系统要求提供友好、直观、易懂的图形呈现，提供强大的信息交互与管理能力，能够根据设定自动生成各类动态图表及报表。 |
| 6 | 部署方式 | 采用SaaS服务模式为所有用户提供安全服务，替用户统一解决了安全服务工具的缺失，并使所有租户能够享受到规模经济所带来的专业能力。 |
| 覆盖主机从创建到运行的各个环节，将各类安全服务工具与数据集中处理，为用户提供一站式的服务体验。 |
| 采用非侵入式自动化执行引擎，在减少对主机的影响的同时，为用户带来了更高效的服务手段。 |
| 将复杂、专业的安全服务操作封装在自助式的页面操作中，降低了用户自行进行安全服务的技术门槛，提高了安全服务质量的水平与一致性。 |
| 7 | 性能要求 | 10,000用户并发环境下操作性能不高于3秒；  10,000用户并发环境下检索性能不高于30秒；  基于海量数据存储架构，支持PB级数据存储； |
| 8 | 接口管理 | 平台应据有良好的集成接口，留有二次开发接口，能够根据实际需求进行深度开发。 |
| 9 | 安全日志审计 | 用户可按主机，或按业务特性，如数据库服务器、中间件服务器、应用服务器等，进行安全日志审计 |
| 平台至少提供系统行为审计、拒绝访问审计、系统登录审计、账号变更审计、软件审计、操作审计服务。 |
| 10 | 自助审计 | 用户可以方便的增加日志信息过滤条件，从而自行进行日志分析，用户可以添加、编辑、固定、删除任意过滤规则。 |
| 支持自定义查询，至少支持lucene请求语法、Regex正则表达式精准查询、topN多项对比搜索功能。 |
| 平台还应提供日志数据统计、数据类型统计、数据采集情况统计，以及被结构化解析的日志原始数据，便于高级用户自行开展审计工作。 |
| 11 | 安全日志存储 | 平台数据结构应支持PB级的海量日志数据存储，并且在PB级的存储条件下，用户查询操作性能应不高于30秒。 |
| 12 | 安全态势告警 | 系统提供安全态势告警，当安全审计发现异常时，除了通过短信、邮件、系统消息进行告警外，还提供了用户统一的查看视图，把安全主机信息、安全配置信息、安全基线信息、安全漏洞信息、安全审计信息、安全响应信息都汇总在统一的安全仪表盘中，使用户可以方便、快速的了解主机的整体安全态势。 |
| 13 | 安全审计报告 | 提供安全审计报告，可以方便的查看历史安全审计报告，报告内容可方便地导出到Word等多种格式文件。 |
| 14 | 产品资质证书 | 提供计算机软件著作权登记证书复印件。 |