服务内容

## 基础安全

通过合规检查、漏洞扫描、基线核查、系统弱口令核查等手段，评估基础IT设备的脆弱性以及由此引起的风险，从而为制定相应的应对措施与解决方案提供实际的依据。评估范围包括但不限于：主机、数据库、中间件、网络设备、安全设备等。同时乙方需要按照甲方要求，协助甲方解决发现的安全问题，并协助完成信息安全优化整改。

基础安全评估服务需要进行现场服务。

**（1）合规检查**

根据安全法律法规、安全标准、专项整治及其他特定安全要求，进行合规性检查，检查内容包括：物理安全、账号口令管理、终端安全管理、系统开发运维管理、合伙伙伴管理、资产管理、网络与安全域管理、安全审计、移动存储介质管理、等保、sox审计等方面制度的安全风险，最后并提供整改建议。

**（2）基线检查**

通过评估工具以自动化扫描的方式对评估范围内的基础IT设备进行基线扫描，并通过人工辅助确认两种方式结合完成安全检查工作。基线核查项要求满足教育部以及教育厅的设备安全配置规范, 对于不满足项提供整改建议。

**（3）漏洞扫描**

通过评估工具以自动化扫描的方式对评估范围内的基础IT设备进行安全扫描，发现目标存在的安全风险、漏洞和威胁。扫描工具应采用两款主流安全扫描工具，扫描工具应使用最新版本版本，更新漏洞库，对发现的安全隐患进行分析，同时提供具有专业性、针对性的安全加固、整改建议，形成安全加固报告，并对修复的漏洞进行回归性测试。

**（4）弱口令检查**

通过在线扫描及离线破解相结合的方式进行系统弱口令核查，乙方应提供符合工信部和集团公司定义的弱口令字典，弱口令字典应包含常规弱口令、易猜解口令、高重复率口令等。

**（5）资产调查**

对所有系统、设备、服务器、终端进行调查和统计，并按统一标准绘制网络拓扑图。所有资产应该注明所属应用系统、资产类型、资产负责人、IP地址。明确标注闲置资产，或上线未登记资产。

**（6）日常安全运维**

对安全系统及设备进行管理，包括安全设备日常管理及告警处理，定期升级特征库、定期更新安全防护策略、定期导出日志信息进行分析、响应并处理设备告警信息、对于设备出现的故障进行紧急响应等；

## 应用安全

**（1）应用安全评估**

对应用系统开展应用安全评估，梳理应用系统以及支撑应用系统的系统软件的版本、补丁等信息；检查应用系统的网络安全域划分情况、互联网开放情况、开放端口和服务、业务接口开放情况，发现存在应用安全风险隐患；开展以及支撑应用系统的系统软件的应用漏洞扫描、应用系统弱口令扫描、应用系统安全基线配置核查等，充分评估应用系统安全基础环境的安全情况，提供安全评估和加固建议等。

**（2）移动APP检测评估**

应覆盖APP程序本身检测和APP涉及接口的检测，并针对Android和IOS平台上的APP终端进行安全风险分析，发现软件自身的安全隐患。程序自身检测主要包括客户端保护、身份鉴别、数据存储安全、安全审计等。APP接口检测主要包括内容安全、计费安全、能力开放接口安全、客户信息安全、业务逻辑安全、传播安全和营销安全的测试。

**（3）应用（含APP）渗透测试**

对应用系统（含APP）开展渗透测试，采用模拟常见黑客所使用的攻击手段对目标系统进行模拟入侵，发现系统中存在可被利用的弱点，并验证存在弱点可能对业务造成影响，验证弱点被利用可能造成的危害。渗透测试采用内部测试和外部测试相结合的方式，对系统实现全面的测试。渗透测试的对象包括并不限于：以ASP、PHP、JSP、.NET、Perl、Python、Shell等语言编写的WEB程序，以及应用系统使用的Oracle、MySQL、MSSQL、Sybase、DB2、Informix等主流数据库，Apache、IIS、Tomcat、Weblogic等主流WEB服务器，FTP、DNS等主流应用服务器等；渗透场景至少包括检测以下种类：

SQL注入

跨站脚本

绕过类漏洞

权限控制（提权、越权、平权）

任意文件上传下载

账号密码明文传输

信息泄露

业务逻辑漏洞

远程命令执行

未授权访问

弱口令

入侵痕迹（可疑文件、配置修改、日志分析、网站篡改、挂马、挂暗链、挂盗链）

APP（IOS 安卓）测试

中间件漏洞

## 代码审计

对应用系统（含移动APP,以下简称系统）开展源代码审计服务，挖掘系统代码中存在的安全缺陷，评估验证代码中安全缺陷可能导致的危害，以及评估可能造成风险。代码审计对象包括不限于：使用ASP、ASP.NET（VB/C#）、JSP（JAVA）、PHP等主流语言开发的B/S应用系统、使用C++、JAVA、C#、VB等主流语言开发的C/S应用系统，以及使用XML语言编写的文件、SQL语言和数据库存储过程等。

**系统代码审计**

（1）协助编制和优化应用编码安全规范

协助甲方编制和优化应用编码安全规范，定期提供专业修订建议，协助对规范的落地实施进行检查。

（2）扫描环境部署和维护

部署和维护代码审计环境，包括安装配置审计环境、代码扫描工具及同步工具等，并根据需要进行升级更新；每天检查审计服务器运行情况，包括检查系统的CPU、内存、磁盘使用情况，以及审计工具软件的可用性。

（3） 代码同步

核对被审计系统的版本号及对应的代码，检查审计服务器上的代码版本信息，按需通过SVN或FTP获取和同步系统代码。

（4） 代码扫描

根据业务需求，周期性或按需地对应用源代码进行工具扫描。根据定义好的代码扫描策略配置代码扫描工具，工具包括但不限于fortify等源代码扫描工具；执行代码扫描任务，采用自动静态分析技术扫描某个应用程序的源代码，找出源代码当中存在的一些语义缺陷、安全漏洞。

（5） 代码人工分析

根据代码扫描报告进行分析，重点对代码安全缺陷和代码质量缺陷等方面的隐患进行分类归纳和分析；通过分析数据流、控制流、配置文件等发现系统漏洞，按需输出高质量的代码安全分析报告和修复估计建议；针对每次代码扫描出现的误报、漏报进行归纳和总结，调整扫描工具进行扫描的准确度，降低误报、漏报率。

（6） 漏洞人工验证

根据代码分析报告发现的安全漏洞在测试环境对漏洞进行利用测试，以确认漏洞真实存在。

## 安全保障

安全保障服务是针对每年的重大、重要事件，以及全网突发的重大安全事件提供专项保障服务，具体包括安全应急支持、全网安全值守、全网安全异常监测、安全保障加固、安全事件深度分析、内容安全监测等内容。

**（1）安全应急支持服务**

安全应急支持服务针对每年国内重大、重要事件，以及全网突发的重大安全事件提供应急支持服务。主要工作内容包含但不限于：制定安全应急方案、工作要求及相关制度；在事前为应急响应做好预备性的工作；在安全事件发生后，按照甲方要求及时对异常的系统、网络进行分析，确定了安全事件的各项技术细节，保留相关证据并制定进一步的响应策略；及时采取行动限制安全事件扩散和影响的范围，限制潜在的损失与破坏，保障系统正常运行；事后要通过对有关安全事件或异常行为的分析结果，找出根源，明确相应的补救措施并协助完成彻底清除；协助恢复安全事件所涉及的系统，并还原到正常状态，使业务能够正常运行。

在提供安全应急支持服务中，乙方应第一时间确定安全事件的类型和攻击源，及时隔离攻击源，制止事态影响进一步恶化；对于对外提供不可中断服务的环境，应该配合甲方人员尽快恢复系统的正常运行，或是最小限度的正常的运行。配合乙方进行事件的追溯和取证，包括但不限于攻击日志、截图、入侵工具分析、漏洞分析及攻击者定位等。配合乙方尽快修补相关漏洞，杜绝该类信息安全事件再次发生。

安全应急支持工作期间，乙方需要每周提交安全应急响应周报，当发生具体安全事件时需要出具详细的安全事件报告：内容包括事件分析、应急响应与处置、安全问题整改建议、安全问题跟踪等。

安全应急支持的响应时限要求如下：

1．一般需求响应，响应时限为2小时；

2．一般安全事件响应，响应时限为1小时；

3．重大安全事件响应，响应时限为0.5小时，需要到现场解决的必须保证1小时内到达现场。

**（2）安全值守服务**

根据每年国内重大、重要事件对安全保障的要求，乙方应提供保障期间7\*24小时的安全值守服务。主要内容包括但不限于：监控系统的运行情况，接收安全事件告警，及时发现安全事态的异常变化，并提供预防性的处置措施，跟踪后续同类安全事件的发展与变化。

乙方应根据甲方需求对相关互联网网站提供非侵入式的防篡改、防挂马检测服务，有效检测异常发现时间为半小时内，1小时完成异常问题报告，并协助进行异常处理，处理完毕后，需出具异常报告和问题处理报告；每月出具一份月度总结报告。具体内容至少包括：

1．网络钓鱼检测

能提供网络钓鱼检测支持，同时支持三种搜索引擎的钓鱼检测算法，对钓鱼链接或者网页能保留证据。

2．网页木马检测

支持对网页的木马检测，提供静态匹配和动态沙箱技术、提供木马现场证据信息。

3．漏洞监控

检测网站对外开放的端口，检测网站对外提供服务的弱口令，检测网站的中间件、程序代码是否存在漏洞。

4．告警服务

网站监控平台相关的安全事件告警，发布网站遭受篡改的及时信息，以便应急响应，发布最新的安全漏洞以及相关新闻。

5．可用性监测

检测目标站点的网络ping时延，检测目标站点的DNS解析时延，检测目标站点的首页访问时延，能计量服务器掉线等安全事件发生的频率、时间段，同时提供报警操作。

除此外，乙方还应提供乙方需为甲方提供一系列的技术手段进行现场安全监控服务，具体内容如下：

1．集中化日志数据分析

能对甲方提供的集中化或临时抽取的主机、网络设备、应用及安全设备日志进行快速查询检索、深度分析判断。

2．流量流向分析

能提供基于流量的网络连接关系采集及分析，以图形化的方式展现不同系统或设备之间的互联情况，并分析并通信协议及数据包内容。

3．可用性监测分析

提供可视化的系统可用性监测工具，主要是检测目标站点的网络ping时延，检测目标站点的DNS解析时延，检测目标站点的首页访问时延，能计量服务器掉线等安全事件发生的频率、时间段，同时提供报警操作。

4．木马分析检测

提供能够自动探测网络流量中可能涉及潜在入侵、攻击和滥用的分析检测工具，对网络流量提供了数据表和图形分析，便于安全人员自行对网络运行情况做监控。具体包括木马和黑名单分析、分析模型、协议还原、匹配规则等相关功能.

保障期间乙方应根据甲方要求按周定期提交《安全值守报告》，对发现的问题进行安全解决建议。

**（3）安全保障加固服务**

安全保障加固内容包括网络设备、安全设备、操作系统、WEB应用、数据库、邮件服务、FTP服务等，目的是为了提高网络安全性，增强甲方抵御各类网络攻击的能力。

具体服务内容：

1．全年安全保障

根据每年重大、重要事件的保障计划，完成全年的安全保障。

2．基础网络设备的安全保障加固

基础网络设施的安全保障加固包括但不限于下列设备：交换机、路由器、无线网络设备、防火墙等。提供的服务包括：进行不必要网络服务、修改不安全的配置、使用最小特权原则对设备进行访问控制、对系统进行软件升级。提出可行性加固方案等。

3．操作系统的安全保障加固

操作系统的安全保障加固服务包括：检查系统补丁、关闭不必要端口、停止不必要服务、修改不合适的权限和安全策略、检查账户口令安全。对于Windows NT/2000/2003/2008等Windows操作系统、UNIX、Linux操作系统，依据甲方的实际情况，制定相应的安全保障加固计划，并进行最终实施。

4．网站应用的安全保障加固

（1） 网站应用开源框架和中间件

乙方安排专业人员对已使用的网站应用中间件和开源框架进行安全检查，并对存在的安全风险进行升级和补丁加固。

（2） 网站防篡改

针对网站防篡改，制定网站目录权限控制，单点IP修改站点以及根据用户需求对网站进行防篡改的加固需求。

（3） 网站应用漏洞

对常见Web应用攻击输入进行过滤，修复已发现的安全漏洞，定点清除Webshell等对Web应用进行安全保障加固。

（4） 其他高级网站应用安全保障加固策略

5．数据库系统的安全保障加固

针对数据库的安全保障加固主要包括对数据库操作权限进行加固，对数据库的密码、帐号策略进行审核，对恶意构造的SQL语句进行过滤等。

针对数据库的系统加固内容主要包括：数据库系统补丁、数据库用户权限管理、数据库用户口令强度和有效期检查、存储过程、远程登录和远程服务、操作审核跟踪、备份过程、后门木马等。

6．其他应用的安全保障加固

根据甲方网络中存在的其他应用，如邮件服务、FTP服务、SSH和远程登录服务、Samba服务、NFS服务、DNS服务等，提供包括应用漏洞补丁修复、用户口令检查、管理员登录IP限制等定制化的安全保障加固服务。

**（4）安全事件深度分析服务**

安全事件深度分析服务主要指通过收集各类数据信息，深度分析数据并发现网络数据流中存在的威胁、网络操作系统中存在的漏洞、发现数据中隐藏的攻击行为或趋势,监测威胁情报，快速响应重大安全事件并提出解决方案。尤其对高级可持续性威胁（APT）和高危安全事件响应工作由乙方专家团队去发现、跟踪和处置。乙方需要在专业的安服人员对情报信息的采集、整理、研判后，进行关联分析和溯源分析。

服务要求：

1．快速响应机制

通过对安全事件的聚合、存储，从原始安全信息中发掘高质量的安全知识，能生成高层安全事件报告。

2．完善的事件发现机制

能够对 IDS、防火墙、路由器、网关等多种网络安全设备产生的丰富的日志和告警信息集中分析，提高发掘安全知识的效果，发现传统安全工具难以发现的安全事件。

3．定制化的恶意代码专杀工具

能够提供恶意代码专杀工具定制化服务，在事件深度分析基础之上，根据深度分析结果，结合乙方实际情况需求，由乙方专业工程师编写针对于特定种族的恶意代码专杀工具。

**（5）内容安全监测服务**

内容安全监测是对在各Web站点检测并监控的内容违规敏感词，存在淫秽色情、涉恐涉暴、通讯信息诈骗等违法有害信息传播风险，损害用户个人权益或危及国家安全和公共利益的情况。

乙方每次服务前须向甲方提交内容安全监测方案，经甲方确认后方可实施。

服务完成后，提交内容安全监测报告，对内容安全监测过程中发现的问题进行分析，并提出安全建议，配合制定相关合理处置流程。

内容安全监测的过程不能影响各项业务的正常进行，所进行的监测必须避开业务高峰期，并且内容安全监测的全过程必须由甲方人员在现场进行全面监督和管理。乙方需给出全面评估过程中的风险规避方案。

内容安全监测过程中所需要的软硬件等工具或设备均由乙方免费提供，并且乙方要保证所使用的检查工具不存在任何版权问题，请在实施方案中对所使用的工具的做功能方面的详细说明。

**（6）考核支撑服务**

配合甲方并按照甲方要求做好方案制定、考核指标材料输出等工作。

## 新技术新业务安全评估

**（1）风险评估服务要求**

内网部分：进行资产分析、脆弱性分析、威胁分析。资产分析应包括设备硬件、设备软件、数据信息、服务、人员、系统拓扑、环境/设施分析；同时对当前设备的漏洞情况、数据库安全配置、主机安全配置、网络设备安全配置、中间件安全配置、安全设备安全配置、web应用安全配置等方面进行技术脆弱性分析，识别在账户口令、日志审计、认证授权、协议安全等方面的脆弱性。

外网部分：核实目标网络单元暴露在互联网上的资产，对暴露在互联网上资产进行管理和技术脆弱性识别，确认相关的安全管理制度、安全管理机构和人员、安全管理要求等管理方面是否存在脆弱性；识别资产在互联网开放的端口服务、软硬件版本、中间件版本、数据库版本等内容，针对发现的漏洞、版本等信息，分析目标网络单元存在的风险。

乙方应根据甲方风险评估计划，对甲方要求范围内的网络和系统完成一次风险评估服务，及时发现网络和系统中存在的安全风险，评估结束后，乙方应根据评估结果提供安全加固方案。

服务内容包含资产调查、脆弱性评估、机房环境评估、安全措施评估、管理脆弱性评估。其中脆弱性评估包含漏洞扫描、配置核查、渗透测试、网络架构分析。

**（2）渗透测试服务要求**

在实际网络环境下，借鉴黑客攻击的手法和技巧，通过漏洞扫描、人工验证、尝试攻击等方式对实际网络系统中数据库、操作系统、网络设备、应用系统及WEB中间件等进行人工渗透，发现系统存在的所有可能的漏洞及潜在的风险，对存在的风险进行判定，给出加固指导意见并验证加固效果。

远程公网系统渗透测试：在远程对外网目标系统进行技术测试和威胁情报分析，从攻击者的角度来对应用系统的安全程度进行安全评估。渗透测试重点关注Web应用层安全，内容包括Web认证机制、权限管理、会话管理、数据库注入漏洞、等测试，评估潜在安全风险，并给出安全加固建议。

渗透测试服务主要通过人工渗透测试为主，WEB扫描为辅的方式进行应用层面的安全评估。

渗透测试前应给出详细的过程说明文档，包括渗透方法，一种或几种存在的攻击路径等，经过授权方可开始渗透测试。

渗透中使用的工具应该是安全无毒的。

渗透结果必须保密，不得向互联网扩散，不得向漏洞平台提交。

渗透测试至少要包括但不限于：SQL注入、XSS跨站脚本、绕过、权限控制、任意文件上传下载、账号密码明文传输、信息泄露、业务逻辑、远程命令执行、未授权访问、应用弱口令等系统安全性渗透测试。

WEB扫描：作为渗透人员的辅助方式，因存在随机插入数据等风险，建议只在测试系统中进行扫描。如有必要在生产环境中采用WEB扫描，需要获得授权，并要求不得影响甲方生产系统数据以及正常运行。

**（3）风险整改技术指导与支持服务要求**

乙方需结合符合性测评、风险评估、渗透测试、评估结论，对目标网络单元存在的安全问题和隐患给出合理的整改建议，提供必要的整改技术支持。在完成服务后6个月内对隐患和问题整改提供技术咨询。

对于甲方目标网络单元存在的安全问题和隐患，乙方应遵循保密原则。

乙方应统一提交对应系统的检测报告的报告格式，对每个漏洞描述测试过程及截图和提出较为详细的加固建议，并保持漏洞描述准确，加固建议相对统一。

**（4）安全防护和管理改进建议服务要求**

根据甲方的安全防护和安全管理情况，结合上级单位要求给出改进建议，并协助编制适用于甲方的相关安全管理文件。

乙方应协助甲方对现有的安全管理体系进行审核，了解现有管理体系文档与安全保护相关等级以及行业标准的符合情况，提出改善建议。