**XX单位**

**安全服务项目方案**

目 录

[1 项目概述 4](#_Toc177750760)

[1.1 项目介绍 4](#_Toc177750761)

[1.2 项目目标 5](#_Toc177750762)

[1.3 项目对象 5](#_Toc177750763)

[1.4 项目内容 6](#_Toc177750764)

[1.5 服务原则 7](#_Toc177750765)

[2 安全服务方案 9](#_Toc177750766)

[2.1 漏洞扫描服务 9](#_Toc177750767)

[（1） 服务简介 9](#_Toc177750768)

[（2） 服务内容 9](#_Toc177750769)

[（3） 交付成果 10](#_Toc177750770)

[2.2 安全基线检查服务 11](#_Toc177750771)

[（1） 服务简介 11](#_Toc177750772)

[（2） 服务内容 11](#_Toc177750773)

[（3） 交付成果 12](#_Toc177750774)

[2.3 安全日志分析服务 13](#_Toc177750775)

[（1） 服务简介 13](#_Toc177750776)

[（2） 服务内容 13](#_Toc177750777)

[（3） 交付成果 13](#_Toc177750778)

[2.4 渗透测试服务 14](#_Toc177750779)

[（1） 服务简介 14](#_Toc177750780)

[（2） 服务方法 14](#_Toc177750781)

[（3） 服务流程 16](#_Toc177750782)

[（4） 交付成果 17](#_Toc177750783)

[2.5 漏洞复测服务 17](#_Toc177750784)

[（1） 服务简介 17](#_Toc177750785)

[（2） 服务内容 18](#_Toc177750786)

[（3） 交付成果 18](#_Toc177750787)

[3 组织实施方案 19](#_Toc177750788)

[3.1 组织管理 19](#_Toc177750789)

[3.2 过程控制 19](#_Toc177750790)

[3.3 项目配合 20](#_Toc177750791)

[3.4 相关资料 20](#_Toc177750792)

[3.5 人员配合 21](#_Toc177750793)

[3.6 场地环境 21](#_Toc177750794)

[3.7 设备测试方案 21](#_Toc177750795)

[3.8 试运行方案 22](#_Toc177750796)

[3.9 用户交接 23](#_Toc177750797)

[3.10 附录文档 23](#_Toc177750798)

# 项目概述

## 项目介绍

2020年，全球突发新冠肺炎疫情，抗击疫情成为各国紧迫任务，APT组织利用社会热点、供应链攻击等方式持续对我国重要行业实施攻击。安全漏洞、数据泄露、网络诈骗、勒索病毒等网络安全威胁日益凸显，有组织、有目的的网络攻击形势愈加明显，为网络安全防护工作带来更多挑战。

《2020年我国互联网网络安全态势综述》报告中提到全年新增收录通用软硬件漏洞数量创历史新高，达20,704个，同比增长27.9%，近五年来新增收录漏洞数量呈显著增长态势，年均增长率为17.6%。其中，高危漏洞数量为7,420个（占35.8%），同比增长52.1%；“零日”漏洞数量为 8,902 个（占%），同比增长 56.0%，从各类数据来看网络安全形势依旧严峻，新发现的漏洞、新的攻击方式、安全意识匮乏等问题都成为企业网络安全事件高发的原因。

为了贯彻国家对信息系统安全保障工作的要求以及等级保护2.0坚持“积极防御、综合防范”的方针，全面提高企业信息安全防护能力。XXXX需要通过持续性的安全服务保障措施，全面提高信息安全防护能力，创建安全健康的网络环境，保护国家利益，促进信息化的深入发展。

**国家发布的法律及信息安全通用标准：**

《中华人民共和国网络安全法》 中华人民共和国主席令 第三十五号

《中华人民共和国密码法》

《中华人民共和国数据安全法》

《信息安全等级保护管理办法》

《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

《信息安全技术 网络安全等级保护实施指南》（GB/T 28448-2019）

《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

## 项目目标

本项目的目标是：确保XXXX整体信息系统的信息安全水平，建立完善的信息安全纵深防护体系，并通过提供专业化技术服务支持，确保信息系统安全，在系统受到攻击时能迅速响应，最大程度减少损失并追踪责任人。

## 项目对象

经过详细沟通，本项目涉及的信息系统如下表所示：

| **实施范围** | **范围类型** | **详细资产** |
| --- | --- | --- |
| 安全服务范围 | 运维系统 | 操作系统类型及数量 |
| 业务系统 | XX系统 |
| XX系统 |
| XX系统 |
| 数据库系统 | 数据库类型及数量 |
| 中间件 | 中间件类型及数量 |
| 服务器 | 计算节点（操作系统类型及数量） |
| 存储节点（操作系统类型及数量） |
| 管理节点（操作系统类型及数量） |
| 安全节点（操作系统类型及数量） |
| 安全设备 | 防火墙（数量） |
| IPS（数量） |
| WAF（数量） |
| 其他安全设备（数量） |
| 网络设备 | 业务交换机（数量） |
| 存储交换机（数量） |
| 管理交换机（数量） |
| 互联网接入路由器（数量） |

## 项目内容

| **序号** | **服务内容** | **服务描述** | **服务方式** | **服务频次** |
| --- | --- | --- | --- | --- |
| 1 | 漏洞扫描服务 | 安全服务工程师对网站进行漏洞扫描，发现扫描对象存在的web应用漏洞、主机操作系统漏洞、数据库漏洞、逻辑缺陷、弱口令、信息泄露等脆弱性问题。 | 远程/现场 | 每年X次 |
| 2 | 安全基线检查服务 | 通过人工检查的方式对评估目标范围内的主机系统安全、中间件安全、数据库安全等进行系统的安全规则配置进行检查。 | 远程/现场 | 每年X次 |
| 3 | 安全日志分析服务 | 通过登录被评估目标设备，提取日志数据进行人工安全分析，对客户系统遭受到的攻击方式、频率、防御有效性等方面进行数据分析总结，找出内网真实存在的安全威胁，记录并交付日志分析报告。 | 远程/现场 | 每年X次 |
| 4 | 渗透测试服务 | 通过模拟黑客攻击的方式对系统进行渗透，挖掘系统存在的安全漏洞，了解应用系统可能存在的潜在漏洞以及发生漏洞利用时可能造成的危害，渗透结束后生成相关报告并提供修复建议。 | 远程/现场 | 每年X次 |
| 5 | 漏洞复测服务 | 针对漏洞扫描、安全基线检查、安全日志分析、渗透测试中发现的安全漏洞和配置缺陷，根据提交的安全评估报告，安全服务工程师将针对提供的报告上存在的问题进行漏洞复测，以确保漏洞已经修复，提供漏洞复测报告。 | 远程/现场 | 每年X次 |

## 服务原则

本次提供的安全服务，全程遵循以下原则。

* 先进性原则

安全服务和形成的规划方案，在路线上应与业界的主流发展趋势相一致，保证依据此方案进行安全服务的对象具备先进性。

* 标准性原则

安全服务和工具的选择，按照国家安全管理、安全控制、安全规程为参考依据。

* 实用性原则

具备多层次、多角度、全方位、立体化的安全保护功能，各种安全技术措施尽显其长，相互补充。当某一种或某一层保护失效时，其它仍可起到保护作用。

* 可控性原则

安全服务和安全规划的技术和解决方案，涉及的工程实施应具有可控性。

* 系统性、均衡性、综合性研究原则

安全服务从全系统出发，综合分析各种安全风险，采取相应的安全措施，并根据风险的大小，采取不同强度的安全措施，提供具有最优的性能价格比的安全解决方案。

* 可行性、可靠性原则

技术和解决方案，应在保证网络和业务系统正常运转的前提下，提供最优安全保障。

* 可扩展性原则

良好的可扩展性，能适应安全技术的快速发展和更新，能随着安全需求的变化而变化，充分保证投资的效益。

# 安全服务方案

## 漏洞扫描服务

### 服务简介

漏洞扫描是一类重要的网络安全技术，它和防火墙、入侵检测系统互相配合，能够有效提高网络的安全性。通过对网络的扫描，管理员能了解网络的安全设置和应用服务的安全状态，及时发现安全漏洞，客观评估网络安全风险等级。管理员能根据扫描的结果更正网络安全漏洞和系统中的错误配置，在黑客攻击前进行防范。如果说防火墙和网络监控系统是被动的防御手段，那么漏洞扫描就是一种主动的防范措施，能有效避免黑客攻击行为，做到防患于未然。

漏洞扫描服务主要采用安全评估系统进行网络漏洞扫描，通过在互联网上或者企业网络内部对客户信息资产（主机操作系统、数据库系统、应用系统、网络设备及其他形式的设备）进行自动化的漏洞扫描。扫描结束后人工分析和去除误报并生成《漏洞扫描报告》。报告对各种扫描过程中发现的系统脆弱性做出详细的说明，以及从脆弱性可能引发的安全隐患或者安全事件，并提供基本的修补建议。

安全服务工程师在服务完成后将提供扫描报告和解决方案，报告包含检查的各项内容，在多次扫描情况下提供扫描的对比报告和安全趋势报告。同时，扫描报告包括IP和漏洞对应表，以便管理员使用。

### 服务内容

在漏洞扫描服务的过程中，安全服务工程师将通过以下风险规避措施，避免在扫描过程中对客户网络或业务系统造成不必要的影响。

* 派遣具有丰富安全扫描经验的安全服务工程师进行安全扫描操作；
* 采用的扫描工具是通过国家权威测评机构认可的商用扫描工具；
* 会根据客户实际情况在保证扫描效果的前提下，配置科学、高效的扫描策略，同时根据客户业务的实际情况在非业务高峰期实施。

漏洞扫描服务具体实施流程如下：

* 根据客户实际情况及要求，确定漏洞扫描的实施范围；
* 根据扫描的对象选择合适的漏洞扫描策略；
* 制定详细的漏扫方案，方案主要内容包括：
* 扫描范围；
* 扫描时间；
* 服务专家；
* 扫描工具部署位置；
* 扫描策略；
* 风险规避措施。
* 根据方案进行漏洞扫描；
* 根据扫描结果，编写《漏洞扫描报告》。

### 交付成果

* 在3-7个工作日内，安全服务工程师将根据扫描结果，输出《漏洞扫描报告》。

## 安全基线检查服务

### 服务简介

安全基线指的是系统最低的安全配置要求，常见的安全基线配置标准有ISO270001、等级保护2.0等，某些行业也会有自己的行业标准。安全基线检查通常涉及操作系统、中间件、数据库等基础设施，基线检查能够及时发现这些基础设施因配置不充分导致的安全隐患，向管理员充分展示所面临的安全问题，并提供有效的解决方案，确保安全设施的安全性和完整性。

安全基线检查服务主要通过安全评估系统及人工核查的方式进行。通过多年在信息安全领域的积累，总结归纳了一套有具有行业领先性的安全配置检查标准。同时，将派出有丰富经验的安全服务工程师，对检查对象进行人工基线核查。

人工基线核查对安全服务工程师的安全知识、安全技术和安全经验要求很高，因为他们必须了解最新的安全漏洞、掌握多种先进的安全技术和积累丰富的评估经验，这样才能对本地安全评估中的所有安全对象目标进行最有效和最完整的安全评估，并提供最合理和最及时的安全建议。

安全服务工程师在服务完成后将提供基线检查报告和解决方案，报告包含检查的各项内容，以便管理员使用。

### 服务内容

安全服务工程师将根据安全配置检查标准，采用人工检查用表（checklist）及安全评估系统对评估目标范围内的主机操作系统安全、中间件安全、数据库安全等进行系统的安全规则配置、安全策略配置、日志报警信息以及系统和软件升级、更新情况，是否存在后门等项目进行检查。

检查对象包括以下操作系统、中间件及数据库：

* 操作系统包括：Windows（32位Windows XP/7 8/10/ Server、64位Windows XP/7/8/10/ Server）、Linux（Centos、Debian、Fedora、Redhat、Suse、Ubuntu等）、Unix（Aix、HP-UX、Solaris等）、国产操作系统（中标麒麟、红旗、深度、凝思等）等。
* 中间件包括：IIS、Apache、Tomcat、Weblogic、Websphere、Nginx、Jboss、Resin等。
* 数据库包括：Oracle、Mysql、DB2、Informix、Mssql、Sybase、达梦等。

针对不同的检查对象，具备差异化的安全配置检查内容，具体如下：

* 操作系统安全基线核查包括：操作系统基本信息、硬件基本信息、应用软件、进程、活动端口开放情况、开机自启动项、客户列表、主机日志信息、补丁信息、安全审计信息和安全策略配置情况，能够采集浏览器上网记录、USB使用记录等。
* 数据库安全检查包括：账号、角色和口令设置、权限设置、数据库日志信息、通信协议、存储过程、版本信息、补丁信息等。
* 中间件安全检查包括：账号、角色和口令设置、权限设置、中间件日志信息、通信协议、存储过程、版本信息、补丁信息、默认端口、登录时常、错误重定向等。

### 交付成果

* 在3-7个工作日内，安全服务工程师将根据检查结果，输出《安全基线检查报告》。

## 安全日志分析服务

### 服务简介

随着企业IT资产的不断增多，每天安全设备都记录了大量的安全日志，除了数据包、日志、资产数据，还包括威胁信息、攻击信息、身份与访问信息、客户行为信息、应用信息、业务信息、外部情报信息等。而越来越多的恶意软件也开始使用隐蔽技术，悄无声息地藏匿在海量的安全日志中。如果不具备丰富的安全经验，是很难进行关联分析和威胁溯源的。

日志分析服务的主要目的是帮助管理员对现网使用的防火墙、IDS、IPS、WAF等安全设备的威胁日志进行专业化人工分析，查找潜在的攻击痕迹，分析日志当中真实存在威胁以及病毒或木马攻击痕迹，找出确定有效的攻击，并交付日志分析报告，为管理员进行下一步操作提供有力的支撑。

### 服务内容

日志分析服务将由经验丰富的安全服务专家实施，通过登录评估目标设备，提取日志数据进行人工安全分析，对客户系统遭受到的攻击方式、频率、防御有效性等方面进行数据分析总结，如内网有多台安全设备的，安全服务专家还将针对多台设备的安全日志进行关联分析，找出内网真实存在的安全威胁，记录并交付日志分析报告。

### 交付成果

* 在3-7个工作日内，安全服务专家将根据日志分析结果，输出《日志分析报告》。

## 渗透测试服务

### 服务简介

渗透测试服务是指高级安全服务专家在得到授权的前提下，通过智能工具扫描与人工测试、分析的手段，以模拟真实黑客入侵的方式对关键应用系统或者主机的安全漏洞、安全隐患进行全面检测，识别服务对象存在的安全风险，是工具扫描和人工评估的重要补充。

渗透测试的目的在于发现应用及系统中可能存在的攻击路径和薄弱环节，验证恶意的攻击者能够通过哪些信息系统的脆弱点获取测试对象的不同程度的信息数据，甚至证明攻击者能够达到直接破坏或中断测试对象业务的能力，深层次发现测试对象存在的风险和漏洞以及黑客攻击路径，提出专业安全建议和解决方案。

在执行渗透测试时，安全服务专家会针对整个渗透过程进行记录，并编写《渗透测试报告》。报告记录漏洞的挖掘与利用过程，方便漏洞复现；同时提供清晰可落地的修复建议，帮助快速修复隐患，总结抵御攻击的最佳实践。此外，报告还涵盖尽量详细的项目信息与测试细节，为管理员提供可查找、可核对的实施记录，也可作为参考案例用于后续测试与培训。

### 服务方法

渗透测试主要采用以下测试方法:

* 工具测试

在渗透测试过程中，为避免对客户网络或业务系统造成不必要的影响，所使用的工具将根据系统实际情况以及最小影响的原则进行选择。

在渗透测试时，高级安全服务专家通常会使用以下工具进行：

* 信息收集工具：Hping、搜索引擎、nmap、nslookup、dnsenum；
* WEB手工分析工具：burp suite、OWASP ZAP；
* 数据库注入测试工具：Havij、sqlmap、pangolin；
* 应用软件：Ftp、远程桌面连接工具等；
* 浏览器：IE、Firefox；
* WEB漏洞扫描器：IBM appscan最新版、HP webinspect最新版、WVS最新版、Netsparker；
* 综合扫描器：Nessus（可扫数据库、服务器、中间件等）；
* 漏洞利用平台：Metasploit；
* 人工测试

人工测试的主要工作是对扫描发现的弱点以及信息进行分析验证，找到真实存在的漏洞并加以利用或者发掘出新的弱点，人工测试也是渗透测试工作最主要的部分。

高级安全服务专家将通过多样化的技术手段对测试对象进行全方位的渗透测试，具体内容包括：

* 端口扫描：通过对目标地址的tcp/udp端口扫描，确定其所开放的服务的数量和类型，为进行深层次的渗透提供依据；
* 远程溢出：对端口扫描发现的漏洞加以利用，检验是否可以使用工具等手段实现远程溢出攻击；
* 口令猜测：对指定应用系统的认证模块进行口令猜测，使用多种手段猜测口令；
* 本地溢出：在拥有了一个普通客户的账号之后，使用一些特殊的技术手段，检验是否能够获得管理员权限或提高普通客户权限；
* 脚本测试：利用SQL语句进行一些特殊操作，绕过应用系统自身的限制，检查出应用系统代码的漏洞环节。包括以下环节：
* 检查应用系统架构：检验客户是否能够绕过系统直接修改数据库；
* 检查身份认证模块：检验非法客户是否能够绕过身份认证；
* 检查数据库接口模块：检验客户是否能够获取系统权限；
* 检查文件接口模块：检验客户是否能够获取系统文件；
* 检查其他安全威胁；
* 敏感信息测试：利用工具获取应用系统的源代码、应用软件版本系统等敏感信息。

### 服务流程

在渗透测试过程中，采用业界领先的漏洞检测技术、攻击技术、攻击工具和安全团队编写的脚本。过程分为四步：计划与准备、信息收集、实施渗透、输出报告。

* 计划与准备阶段

主要是针对渗透测试项目举行研讨会，讨论渗透测试操作思路，说明渗透测试的实施范围和测试对象，然后根据研讨内容制定相应得实施方案与计划。由领导审核批准实施方案与计划，项目组根据实际情况的需要，会对实施方案与计划进行一定的调整。

* 信息收集阶段

信息收集阶段是所有入侵攻击的前奏和基础，通过信息收集分析，高级安全服务专家可以有针对性地制定入侵攻击的方法策略，提高入侵的成功率、减小暴露或被发现的机率。信息收集分析几乎是所有入侵攻击的前提/前奏/基础。通过信息收集分析，高级安全服务专家可以相应地、有针对性地制定入侵攻击的计划，提高入侵的成功率、减小暴露或被发现的几率。

信息收集的方法包括端口扫描、操作类型识别、应用识别、账号扫描、配置识别等。信息收集后，高级安全服务专家将对其进行分析，并制定渗透测试方案。

* 在实施渗透阶段

在实施渗透阶段，高级安全服务专家根据前期收集到的信息，对存在的漏洞进行人工验证和渗透测试，并根据实际情况进行记录。通过收集信息和分析，存在两种可能性，其一是目标系统存在重大弱点：测试者可以直接控制目标系统，这时测试者可以直接调查目标系统中的弱点分布、原因，形成最终的测试报告；其二是目标系统没有远程的重大弱点，但是可以获得远程普通权限，这时测试者可以通过该普通权限进一步收集目标系统信息。接下来，高级安全服务专家将尽最大努力获取本地权限，收集本地的资料信息，寻求本地权限升级的机会。这些不停的信息收集分析、权限升级的结果构成了整个渗透测试过程的输出。

* 输出报告阶段

为了能让客户更好的理解渗透测试过程，高级安全服务专家将根据渗透测试得出的结果，进行汇总分析，并输出《渗透测试报告》。

### 交付成果

* 在3-7个工作日内，安全服务专家将根据渗透测试结果，输出《渗透测试报告》。

## 漏洞复测服务

### 服务简介

针对漏洞扫描、基线检查、渗透测试、日志分析中发现的安全漏洞和配置缺陷，安全服务专家都会提供对应的修复建议与方案，并指导管理员完成漏洞和配置修复。为了评估修复的效果，安全服务专家会针对报告上存在的问题进行漏洞复测，以确保漏洞已经修复。

### 服务内容

安全服务专家在接到漏洞复测任务时，将根据报告情况与管理员沟通，并制定复测计划。在评估期内，安全服务专家将使用相同的测试工具，对评估对象进行漏洞复测。

在漏洞复测服务的过程中，会派遣有丰富安全经验的安全服务专家，根据客户实际情况，在保证复测效果的前提下，配置科学、高效的复测策略，同时根据客户业务的实际情况在非业务高峰期实施，以避免在复测过程中对客户网络或业务系统造成不必要的影响。

在完成漏洞复测后，安全服务专家将与之前的报告进行比对，并输出《漏洞复测报告》，确认修复动作的有效性。如评估期内依然无法修复漏洞的，安全服务专家也会在《漏洞复测报告》中指明现在依然存在的问题，并指导管理员继续进行漏洞和配置修复动作。

### 交付成果

* 如果一次漏洞复测未能对现存问题进行修复的，安全服务专家将提供《未修复漏洞告知书》，对未修复漏洞进行书面告知，提出修复建议。
* 在复测期内，如所有已知漏洞均复测通过，3-7个工作日内，安全服务专家将根据漏洞复测结果，输出《漏洞复测报告》。
* 如复测期内依然存在部分复测未通过漏洞，3-7个工作日内，安全服务专家将根据漏洞复测结果，输出《漏洞复测报告》，并明确指出复测未通过漏洞，提出修复建议。

# 组织实施方案

## 组织管理

项目管理是整个项目实施的核心，项目管理的方法是基于稳定的组织、完整的计划和丰富的文档。项目管理的目的就是要运用完善的管理方法和经验，提高项目实施的可操作性和可控制度，保证项目按照设计预期高质量地完成。

一个项目的成功实施需要良好的实施方案，同时还需要一个负责任的组织去执行。因此，在项目建设工作开展之前，制订有效的项目实施计划是必不可少的。通过本计划对项目实施过程进行管理与控制，协调各方面的力量，预见可能发生的问题，并预先准备好的解决方法，从而保证系统建设工作得以有效、按部就班地开展。

我公司将按照通过ISO9001的质量体系认证，所有工程及服务的流程均按照ISO9001的质量体系标准执行。

## 过程控制

过程控制的要点是，制定并执行文件化的过程控制程序，对系统质量形成过程的4M1E五个基本要素实施全面控制与管理，一旦发生偏离能够立即发现和纠正，确保过程输出质量符合规定要求。4M1E五个要素是指：人（man）、机（machine）、物（matter）、料（material）、环境（environment）。

项目参与方在项目进行过程中随时对相关问题进行沟通。所有重要的、有主题的日常沟通活动都应留下记录或形成备忘录。通常这些记录或备忘录需要双方的签字以作为备案。项目经理有责任将项目中出现重大变更、重要事件、进展、以及其它与项目密切相关的内容进行记录，从项目启动到项目终验，最终形成完整的项目日志。

## 项目配合

我方在安全服务实施过程中，采购人需要提供相关技术资料和场地环境，并且相关管理人员和技术人员也将进行必要的工作配合。

## 相关资料

（1）技术资料

每个系统业务的设计文档；

系统各种业务应用网络拓扑（电子版）；

每个相关系统的业务流程，例如系统故障处理流程，业务服务提供方式等；

安全产品配备情况，当前已使用的安全产品及使用情况，配置情况；

特别的安全策略、应用系统特殊运行的环境、必须开放的端口、服务等；

采购人的其它有必要提醒和说明的技术资料。

（2）管理资料

现有的信息系统安全体系框架；

信息系统安全管理制度；

遵循的行业法规或规范；

系统维护手册或制度等；

人员、密码、资料等管理方法；

安全管理策略文档。

（3）日常维护资料

网络负载、利用率、网络质量等网络维护统计资料；

安全事件发生成功或未成功统计数据文档；

安全信息资料，包括签名备份、日志安全审计、安全产品日志备份等。

## 人员配合

相关项目负责人配合实施管理性工作，如确定评估范围、对系统相关人员分发调查问卷、提供系统网络管理员名单、各业务系统相应管理员名单等；

需要采购人相关技术人员全程配合或协调工作；

扫描过程中需要扫描目标网络中管理员的配合；

相关人员协助评估，回答有关调查问卷和问题，参加确认协调会，对每一阶段评估结果书面确认；

采购人负责信息安全管理的领导和信息技术部门以及包括系统开发、建设、运行维护和终端等各种角色，均将配合进行安全顾问访谈。

需要运维单位、相关厂商、系统集成商提供必要的支持和一些确认工作。

## 场地环境

项目工程实施人员办公间、独立的文件柜（加锁）；

提供必要的电源接入及被评估网段的网络接入方式；

提供被评估网段的空闲IP地址、网络掩码、网关等配置信息；

相关管理员提供本地脆弱性评估系统的访问权限；

相关管理员提供适当的网络环境和权限供远程评估；

提供互联网接入端口，以方便下载临时补丁、查询相关资料等。

## 设备测试方案

在试运行阶段我公司工程实施人员会在客户处不断的对整个系统进行调优。将用户的系统优化到最佳状态，调优项目包括如下（也可根据实际情况判断）：

安全设备的性能分析

1、设备配置参数分析

2、运行状态监控与分析

3、设备日志情况分析

4、网络连接检查

5、高峰时的性能、流量分析

服务器系统的性能分析

1、配置参数分析

2、运行状态监控与分析

3、日志情况分析

4、联动效果分析

## 试运行方案

经过测试后系统进入试运行阶段，进入试运行期。在试运行期间项目经理和厂商工程师随时待命如出现问题，则我方会立即派人予以现场解决，直到无故障时为止。

在试运行期间，本公司所提供的软、硬件设备出现问题或故障时，本公司会协调我公司资深技术人员及厂商相关技术人员进行问题解决或维修更换。

在整个系统实施完毕和整体联调结束后，由项目管理组批准后将正式投入试运行。

本部分工作完成后，形成的提交件有：

《系统试运行报告》

《重大问题处理报告》

## 用户交接

在工程实施之前，我方将向用户单位提交《工程联系单》，以便实施工作的开展；

在货物设备到达用户现场后，我方将向用户提交《交接设备清单》，并签署《货物签收单》；

在系统实施过程中，我方希望能与用户一起共同参与系统的整体规划和实施，并在实施过程向用户讲解实施的过程和内容；

在实施完后，向用户提交系统所涉及相关《设备集成报告》，《设备测试报告》以及设备相关手册等资料。

## 附录文档

文档的提交应覆盖以下内容，电子文档是成果不可分割的部分。要求如下文档：

1、项目实施前：需求分析报告；设计方案、设计说明书；项目实施计划；

2、项目实施期间：项目实施工作单、故障诊断及排除记录、项目实施过程中衍生的其它相关资料；

3、项目实施后：系统试运行和自测报告、故障诊断与排除手册、工作总结报告；

4、培训期间：培训计划、用户使用手册、管理员使用手册；

5、其他需要提交的材料