附件：服务内容

**1**安全服务方案设计

**1.1**服务范围

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **系统名称** | **服务器数量** | **所在网络** | **物理位置** | **等保备案** |
| 1 | 福建省森林资源管理系统 | 4 | 政务信息网 | 省政务云 | 二级 |
| 2 | 福建省林业网上行政审批系统 | 4 | 政务信息网 | 省政务云 | 二级 |
| 3 | 福建省营造林信息管理系统 | 4 | 政务信息网 | 省政务云 | 二级 |
| 4 | 福建省林业信息共享服务平台项目 | 4 | 政务信息网 | 省政务云 | 二级 |
| 5 | 福建省林木种质资源普查信息系统 | 2 | 互联网 | 省政务云 | 二级 |
| 6 | 档案管理系统 | 1 | 政务信息网 | 省政务云 | 二级 |
| 7 | 国有林场财务管理网络应用系统 | 1 | 政务信息网 | 省政务云 | 二级 |
| 8 | 福建省林业局平时考核系统 | 2 | 互联网 | 省政务云 | 二级 |
| 9 | 福建省林业巡护指挥调度云平台 | 6 | 互联网 | 省政务云 | 二级 |
| 10 | 智慧林业视频监控联网调度系统 | 7 | 互联网 | 省政务云（托管） | 二级 |
| 11 | 福建省食用林产品安全信息追溯管理平台 | 4 | 政务外网 （互联网） | 省政务云 | 二级 |
| 12 | 福建省古树名木管理信息系统 | 1 | 互联网 | 省政务云 | 二级 |
| 13 | 福建省自然保护区视频监控体系建设项目 | 2 | 互联网 | 省政务云（托管） | 二级 |
| 14 | 林场国有资产管理系统 | 1 | 互联网 | 省政务云 | 二级 |
| 15 | 全国森林资源保护管理监测平台 | 3 | 互联网 | 省政务云 | 二级 |
| 16 | 福建省森林和草原火灾风险普查软件项目 | 8 | 政务外网  （互联网） | 省政务云 | 三级 |
| 17 | 福建省林业局网站 | X | 互联网 | 省政务云 | 三级 |
| 18 | 福建省林业局直属单位网站群系统 及8个直属单位子站 | 2 | 互联网 | 省政务云 | 二级 |
| 19 | 福建“互联网+全民义务植树”网站系统 |  | 互联网 |  |  |
| 20 | 全国林木采伐管理系统（省级） |  | 互联网 |  |  |

**1.2服务期限**

服务期限为自合同签订生效之日起三年。

**1.3服务概述**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务大类** | **服务类别** | **服务内容** | **服务频率** | **交付成果** |
| 1 | 资产梳理与巡检服务 | 资产梳理服务 | （1）资产识别分析服务 | 1次/季度 | 《资产清单》 |
| （2）资产信息梳理服务 |
| 巡检服务 | （1）云上服务器巡检服务 | 1次/月 | 《云上服务器巡检报告》 |
| 2 | 主机系统安全检测服务 | 主机系统安全检测服务 | （1）主机系统漏洞扫描服务 | 1次/季度 | 《主机系统安全检测报告》 |
| （2）主机系统安全配置核查服务 |
| （3）主机系统后门检查服务 |
| （4）网络攻击威胁实时监测服务 |
| （5）主机入侵行为实时监测服务 |
| （6）横向渗透攻击行为实时监测服务 |
| （7）主机系统安全加固辅导服务 |
| （8）中间件安全评估与配置加固建议服务 |
| （9）数据库安全评估与配置加固建议服务 |
| 3 | 应用安全检测服务 | 互联网网站安全监测服务 | （1）可用性监测服务 | 全年 | 《互联网网站安全监测报告》 |
| （2）合规性监测服务 |
| （3）安全性检测服务 | 1次/季度 |
| 应用系统安全检测服务 | （1）应用安全漏洞扫描服务 | 1次/季度 | 《应用安全检测报告》 |
| （2）应用安全漏洞验证服务 |
| （3）应用安全漏洞加固辅导服务 |
| 安全渗透测试服务 | （1）网站安全渗透测试服务 | 1次/半年 | 《安全渗透测试报告》 |
| （2）应用安全渗透测试服务 |
| （3）安全加固建议及辅导服务 |
| 4 | 综合安全保障服务 | 安全应急演练服务 | （1）应用应急预案设计服务 | 1次/年 | 《安全应急预案》、《安全应急演练报告》 |
| （2）应用应急演练服务 |
| 安全应急响应服务 | （1）安全应急响应服务 | 全年 | 发生安全事件应急响应后提交《安全应急响应报告》 |
| （2）安全应急处置服务 |
| （3）远程安全咨询服务 |
| （4）网络安全设备应急服务 | 全年 |
| 安全检查专题服务 | （1）安全检查专题服务 | 全年 | 安全检查相关材料 |
| 重要时期保障服务 | （1）重要时期远程保障服务 | 国庆、两会等重要时期 | 《重要时期远程值守日报》 |
| 安全通告服务 | （1）安全通告服务 | 全年 | 《安全通告》全年不少于6期 |
| 5 | 安全培训服务 | 普及性安全培训 | （1）安全意识培训 | 1次/年 | 安全培训材料 |
| 6 | 安全措施有效性验证服务 | 安全措施有效性验证服务 | （1）网络边界管控有效性及策略核查服务 | 1次/季度 | 《安全措施有效性验证报告》 |
| （2）硬件设施有效性及策略核查服务 |
| （3）安全软件措施有效性及策略核查服务 |

**2**安全服务要求

**2.1**资产梳理与巡检服务

**2.1.1**资产梳理服务

**2.1.1.1**资产识别分析服务

通过资产识别工具，自动化探测和采集资产属性，发现正在使用的IT资产，包括网络设备、web服务器、数据库服务器、应用系统等。

**2.1.1.2**资产信息梳理服务

结合已有IT资产清单和资产识别分析服务发现在用IT资产，通过人工服务完成资产清单的梳理，帮助用户发现无主资产、无用资产、新增资产等资产信息。

**2.1.1.3**服务价值与交付成果

定期每季度通过资产梳理服务，明晰当前的IT资产，以及发现资产的变更。

**交付成果：《资产清单》**

**2.1.2**巡检服务

**2.1.2.1**云上服务器巡检服务

每月定期对云上虚拟机服务器的CPU、内存、硬盘、网卡进出IO等情况进行查看分析，及时发现服务器的异常，保障云上虚拟机服务器的正常运行，进而为云上业务的可持续运行提供支撑。

**2.1.2.2**服务价值与交付成果

通过定期的虚拟机巡检，保证虚拟机的正常运行。

**交付成果：《云上服务器巡检报告》**

**2.2**主机系统安全检测服务

**2.2.1**主机系统漏洞扫描服务

定期每季度1次指派专业的安全服务工程师到客户现场，针对主机系统进行漏洞扫描、端口扫描、弱口令扫描等，覆盖系统的补丁、服务的开放性及安全研究机构发现的系统问题等，发现系统本身存在的安全问题。

**2.2.2**主机系统安全配置核查服务

定期每季度1次指派专业的安全服务工程师到客户现场，参照等级保护2.0合规性标准，对主机系统进行配置核查，发现主机系统配置存在不合理和不安全的情况，提升客户对主机系统配置的安全意识。结合发现的问题进行及时调整，加强主机系统安全。

**2.2.3**主机系统后门检查服务

定期每季度1次指派专业的安全服务工程师到客户现场，针对主机系统后门进行检查，检查内容包括：

**1）主机系统后门检查**

主机系统被入侵潜伏后，通常存在隐藏比较深的系统后门（Rootkit），重点发现绕过杀毒软件的系统后门。

**2)主机系统入侵痕迹检查**

针对主机账号、启动项、进程、网络连接等进行检查。

**3)主机系统日志分析服务**

根据系统层日志、安全日志、应用层日志以及其他特征发现主机系统的入侵痕迹，避免黑客使用隐藏账户等躲避检查的安全隐患。

**2.2.4**网络攻击威胁实时监测服务

针对福建省林业局云上主机的网络流量进行安全实时监测，及时有效地发现云上业务存在的网络安全攻击威胁与安全风险，如SQL注入、反序列化、漏洞利用、反向外联、未授权访问等行为，一旦发现网络流量安全告警，并成功匹配到安全攻击行为特征，则及时进行预警通告，为进一步安全处置工作提供可靠保障。

**2.2.5**主机入侵行为实时监测服务

实时监测福建省林业局云上业务系统云主机安全状态，对主机入侵、可疑后门、恶意程序、违规操作、主机漏洞等进行实时监测、检测，实时地感知网络安全攻击威胁行为，能够准确定位主机系统存在的安全薄弱点与安全漏洞风险，并进行预警，提升主机入侵事件发现和应急响应能力。

**2.2.6**横向渗透攻击行为实时监测服务

对福建省林业局云主机内网横向渗透攻击行为进行监测，如横向移动、内网探测、恶意扫描等行为，一旦发现横向渗透行为，能够及时发出预警，结合应急处置措施，有效阻断黑客攻击途径，防止黑客通过内网对其它业务主机发起安全攻击。

**2.2.7**主机系统安全加固辅导服务

定期每季度1次指派专业的安全服务工程师到客户现场，通过分析主机系统漏洞扫描、安全配置核查、后门检查的结果，明确主机系统当前存在的安全问题，对在检测中发现的主机系统安全问题提供安全加固建议及辅导，协助系统管理员完成主机系统后门清理、漏洞加固和配置加固，提高系统的整体安全性，最大限度消除服务器高风险漏洞，使其符合等级保护的基本要求。

**2.2.8**中间件安全评估与配置加固建议服务

定期每季度1次指派专业的安全服务工程师到客户现场，针对中间件进行安全合规评估，并提供配置加固建议。

结合工具检测和人工安全审查方式来挖掘Apache/IIS/Tomcat/Weblogic/WebSphere等Web应用服务器（中间件）的脆弱性和安全性问题，主要评估账号、日志、配置等不正确的问题带来的安全威胁，帮助用户及早发现中间件存在的风险，避免造成敏感信息泄漏的后果。

针对Apache/IIS/Tomcat/Weblogic/WebSphere等Web应用服务器（中间件）提供加固建议，包括配置加固与优化建议，最大程度降低中间件本身的漏洞风险、纠正中间件使用中构成安全威胁的错误策略、加强中间件账号、日志、配置等带有安全风险的配置，从整体上提升中间件的安全性。

**2.2.9**数据库安全评估与配置加固建议服务

定期每季度1次指派专业的安全服务工程师到客户现场，针对数据库进行安全合规评估，并提供配置加固建议。

结合工具检测和人工安全审查方式来挖掘数据库系统的脆弱性和安全性问题，主要评估数据库系统安全漏洞、安全配置不正确带来的安全威胁以及由于数据库系统账号、权限等配置不严谨而产生的安全风险。帮助用户及早发现数据库系统存在的风险，避免造成敏感信息泄漏的后果。

提供数据库安全加固建议，包括最大程度降低数据库系统（SQL Server，Oracle等）本身的漏洞风险、纠正数据库系统使用中构成安全威胁的错误策略、加强数据库系统账号、密钥、权限等带有安全风险的配置，从整体上提升数据库系统的安全性。

**2.2.10**服务价值与交付成果

通过主机安全检测与加固辅导服务，全面深入地发现主机服务器可能存在的安全风险，及时协助修复主机系统层安全中发现的安全漏洞与隐患，最大限度地防止黑客入侵。保证信息系统稳定、安全地运行。

**交付成果：《主机系统安全检测报告》**

**2.3**应用安全检测服务

**2.3.1**互联网网站安全监测服务

针对服务范围内的互联网网站进行全年的安全监测，并每季度进行1次安全性检测。

**2.3.1.1**可用性监测服务

针对互联网网站应用提供全年可用性监测服务，可用性监测主要涉及以下指标：网站可用性、网站访问的速度情况、网站响应时间，从而判断互联网网站是否能达到最优、最安全的服务质量。通过的可用性检测服务，从互联网线路远程实时监测目标网站站点在多种网络协议下的响应速度、首页加载时间等反映网站性能状况的内容，一旦发现网站无法访问，第一时间通知用户。

**2.3.1.2**合规性监测服务

**2.3.1.2.1**远程网页变更监测服务

针对互联网网站应用提供全年远程网页变更监测服务，远程网页变更监测服务在远程对比的基本原理上，增加了两大核心技术，来解决业界恶意变更监控普遍误报率较高的问题。一是内容网页前后模糊匹配技术通过预设值敏感度，作为前后匹配误差的判断标准；二是内容匹配算法，不仅对比网页的变化，而是识别内容，并进行非法库的匹配。例如，扫描发现网页修改中出现了“共产党”，其他部分又出现不和谐词语，系统会计算出一个差值，来进行匹配判断是否为恶意变更行为。这样一方面提升扫描效率，一方面极大降低误报率。一旦发现网站网页异常变更，第一时间通知用户。

**2.3.1.2.2**网页敏感信息监测服务

针对互联网网站应用提供全年网页敏感信息监测服务，对网站存在的敏感信息进行检测，并且可以检测多种类型的敏感信息，同时，还能够支持自定义导入敏感信息，在自身的敏感词库的基础上，不断丰富敏感词汇。监测工具同时利用百度、谷歌等搜索引擎的强大搜索能力，通过搜索引擎接口提交搜索参数，使页面敏感词检测覆盖面更深更广，从而实现远程实时监测目标站点页面状况，一旦发现页面出现敏感关键词，第一时间通知用户并提供安全参考建议，方便用户及时删除敏感内容，避免事件影响扩散，给自身带来声誉和法律风险。

**2.3.1.2.3**网页恶意链接监控服务

针对互联网网站应用提供全年恶意链接检测服务，检测网站暗链、桥页等恶意链接以及网页新增链接等。通过监测工具内置的暗链特征库，将远程网页信息抓取到本地，进行暗链特征匹配，通过排除信任域名库、IP地址域名、常见隐藏手段等的干扰，并结合暗链关键词库的匹配技术，将目前挂暗链主要目的的搜索引擎关键词，准确匹配出来，从而在有效检测暗链的同时，将误报降到最低限度。一旦发现页面出现网页恶意链接，第一时间通知用户。

**2.3.1.3**安全性检测服务

**2.3.1.3.1**网站漏洞扫描检测服务

针对互联网网站应用提供全年网站漏洞扫描检测服务，提供OWASP定义的Web威胁相关的漏洞扫描检测，通过远程的网站漏洞扫描检测，同时有效识别Web2.0以及Flash，保障网站漏洞扫描的全面性。

网站漏洞扫描服务提供广度和深度两种扫描方式，广度优先策略是按照网页内容目录层次深浅来爬行页面，处于较浅目录层次的页面首先被爬行。当同一层次中的页面爬行完毕后，爬虫再深入下一层继续爬行，能有效控制页面的爬行深度，避免遇到一个无穷深层分支时无法结束爬行的问题。

**2.3.1.3.2**网站钓鱼检测服务

针对互联网网站应用提供全年网站钓鱼检测服务，服务工具通过借助搜索引擎的搜索能力以及网页的模糊匹配技术，通过借助网页关键词，判断搜索关键词而来的网站中，是否出现与本域名不匹配，且相似度高的网站，来判断该网站是否为钓鱼网站，一旦发现将第一时间通知用户。

**2.3.1.3.3**网页木马检测服务

针对互联网网站应用提供全年网页木马检测服务，检测工具采用业内领先的一体化挂马检测技术，高效、准确地识别网站页面中的恶意代码，从而使网站管理员能够第一时间感知网站的安全状态，及时清除网页木马，避免给用户带来安全威胁，继而影响网站信誉。检测工具采用基于沙箱检测和静态特征库匹配相结合的木马检测技术作为网马检测引擎，提高引擎检测准确性，降低误报率。

**2.3.1.3.4**弱口令检查服务

针对互联网网站应用提供全年弱口令检查服务，检测工具基于调度任务对网站进行远程自动扫描，获得所述网站主机诸如：SSH、FTP、ORACLE等服务的弱口令信息，包括：用户名、密码。检测工具通过内置的用户名字典和密码字典以及组合字典，可以进行标准模式破解以及组合模式破解两种扫描方式进行弱口令扫描，扫描一方面同弱口令字典中的弱口令进行匹配，另一方面使用获取到的口令进行模拟登陆验证，从而实现弱口令检查功能，从而有效提高弱口令检测效率。

**2.3.1.4**服务价值与交付成果

定期每季度采用安全监测服务平台等检测服务工具对单位的互联网网站提供远程安全监测，用户无须安装任何软件或调整网络架构，由于无需购买和部署设备，因此用户可以在几个小时内将监测服务投入运行，并可以在第一时间获得监测到的网站安全问题，并获得专业的技术指导协助。

**交付成果：《互联网网站安全监测报告》**

**2.3.2**应用安全检测服务

**2.3.2.1**应用安全漏洞扫描服务

定期每季度1次指派专业的安全服务工程师到客户现场，为目标应用提供全方位的安全漏洞及安全隐患检查，从攻击者视角审查目标应用系统的脆弱性状况，包括应用漏洞、应用配置。

**2.3.2.2**应用安全漏洞验证服务

定期每季度1次指派专业的安全服务工程师到客户现场，对已经发现的安全问题进行人工验证，以判断应用当前的漏洞是否真实有利用，剔除误报干扰。并提供专业的安全加固措施指导建议，帮助客户解决当前应用存在的安全问题。

**2.3.2.3**应用安全漏洞加固辅导服务

定期每季度1次指派专业的安全服务工程师到客户现场，提供专业的应用安全漏洞加固措施指导建议，协助应用开发商及时采取可行的应用安全加固措施进行安全加固。首次安全加固后，将进行漏洞复查和对比，以形成加固前后对比。协助客户解决当前应用存在的安全问题。

**2.3.2.4**服务价值与交付成果

通过应用安全检测服务，全面深入地挖掘可能存在的被黑客利用的网站应用层安全漏洞和数据库的安全隐患，同时实现对单位作为业主或其负责运维的信息系统在发现漏洞时的有序管理，实现安全事件可追踪、可追溯，保障漏洞得到及时、有效地修复，确保各信息系统的安全运行。

**交付成果：《应用安全检测报告》**

**2.3.3**安全渗透测试服务

**2.3.3.1**网站安全渗透测试服务

定期每半年安排渗透测试团队采用人工黑盒的方式对用户的应用系统进行模拟攻击测试。主要测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、Web脚本渗透、B/S或C/S应用程序测试等，渗透结果进行人工分析，并对漏洞提交源代码加固建议报告。

**2.3.3.2**应用安全渗透测试服务

定期每半年针对应用系统进行专家级人工的渗透测试服务，全面检测Web应用程序的安全性，深度挖掘程序中存在的各种漏洞和所面临的威胁，漏洞测试覆盖OWASP十大漏洞，如XSS跨站脚本攻击漏洞、SQL注入漏洞、恶意代码上传漏洞、Cookie注入漏洞及其它各种敏感信息的检查等。

**2.3.3.3**安全加固建议及辅导服务

根据渗透测试结果，提供详细的应用安全加固建议，并协助应用开发公司完成应用加固，并提供复查以确保漏洞得到修复。

**2.3.3.4**服务价值与交付成果

（1）深度挖掘应用系统中的安全漏洞，并判断漏洞可能造成的最大限度的损失；

（2）以最权威的客户数据，让客户感受应用系统安全漏洞将带来的影响和损失，以便做好安全损失与保护的评估。

**交付成果：《安全渗透测试报告》**

**2.4**综合应急安全保障服务

**2.4.1**安全应急演练服务

**2.4.1.1**应用应急预案设计服务

针对单位自身的网络实际情况，并结合网络安全应急处置相关的政策要求，每年设计出1份符合单位要求的安全应急预案，预案中包括5个场景。

制定应急预案管理的责任部门，建立统一的应急预案框架，框架应包括事件分级方法、各级事件启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；在应急预案框架制定不同事件的应急预案，应急预案要指名适用的系统、设备等，要结合系统实际状况。比如针对门户网站的网页篡改、针对业务系统的入侵等。组织信息网络应急保障队伍，开展应急演练，做好应急演练相关文档记录。

**2.4.1.2**应用应急演练服务

为保障网络与信息系统安全，预防和遏制网站及应用系统突发安全事件的发生，减轻和消除突发事件造成的危害和影响，每年组织技术力量共同完成1次应急演练，包含安全应急预案中3个场景，演练完成后提交《应急演练报告》及相关应急演练记录，确保能够应对各类安全事件的发生。

**2.4.1.3**服务价值与交付成果

通过开展安全应急演练，提高单位对安全突发事件的组织指挥能力和应急处置能力。

**交付成果：《安全应急预案》、《安全应急演练报告》**

**2.4.2**安全应急响应服务

**2.4.2.1**安全应急响应服务

当单位网络和信息系统遇到黑客攻击或网页篡改等恶性事件，迅速对事件作出相应的判断，确认事件给信息系统带来的影响和损害程度，区分一般事件和应急响应事件等，如果确认事件为应急响应事件且远程支持无法解决时，1小时内安排工程师到达现场处置，实施最有效的紧急救援及恢复补救方案。

**2.4.2.2**安全应急处置服务

根据突发事件信息，初步判定突发事件的程度。能够自行解决，要及时加以解决；如果不能自行解决故障，由单位领导现场指挥，协调各部门力量，按照分工负责的原则，组织相关技术人员立即启动应急预案，进入应急预案的处置程序，及时控制安全事件的蔓延，采取有效的措施以防止事件进一步扩大，尽可能地减少负面影响。

**2.4.2.3**远程安全咨询服务

当单位网络和信息系统故障或出现安全事件时能立即通过电话咨询或远程维护等方式提供7×24小时远程安全咨询服务支持。

**2.4.2.4**网络安全设备应急服务

出现安全设备故障问题，存在设备厂商无法提供及时、有效的售后服务风险，临时提供借用设备进行支撑，保证故障期间业务的正常运行。

同时，安全设备过保但无法及时采购相应设备或维保服务等情况需要网络安全设备的情况时，提供网络安全设备的借用作为应急使用。

可借用网络安全设备主要包括防火墙、入侵防御、上网行为管理、日志审计、数据库审计、堡垒机等多类型设备，具体借用设备类型、借用时间等事项另行协商。

**2.4.2.5**服务价值与交付成果

通过应急响应为遇到黑客攻击或网页篡改等恶性事件，实施最有效的紧急救援及恢复补救工作。

**交付成果：发生安全事件应急响应后提交《安全应急响应报告》**

**2.4.3**安全检查专题服务

**2.4.3.1**安全检查专题服务

在上级监管部门对单位进行安全检查期间，协助单位按照上级监管部门要求，进行专门的全面安全检查协助服务和保障协助，包括协助单位梳理出单位现有的信息安全管理制度相关材料等。

**2.4.3.2**服务价值与交付成果

通过安全检查专题服务，保障了在上级监管部门安全检查期间能够进行高效地协助工作。

**交付成果：安全检查相关材料**

**2.4.4**重要时期保障服务

**2.4.4.1**重要时期远程保障服务

在国庆、两会等重要时期，针对信息系统资产包括主机、网络、应用等系统进行远程保障，包括加强安全监测与处置力度，保障重要时期的安全。

**2.4.4.2**服务价值与交付成果

在重要时期，通过加强安全支撑，为重要时期的业务稳定运行赋能。

**交付成果：《重要时期远程值守日报》**

**2.4.5**安全通告服务

**2.4.5.1**安全通告服务

提供最新的安全动态、技术和安全信息，包括实时安全漏洞通知、定期安全通告汇总和安全知识库更新等。通告内容包括但不限于以下内容：

国内外最新重大漏洞、病毒安全通告；

国家安全政策及法律法规；

同行业安全威胁事件通告；

国内外重大安全事件，新技术发展动态通告；

重大安全漏洞爆发时需结合资产情况，提出相应修复建议。

**2.4.5.2**服务价值与交付成果

可以根据通告信息，轻松掌握最新的安全漏洞状态并能够安排及时修补IT资产漏洞，提高单位安全脆弱性管理能力。

**交付成果：《安全通告》全年6期**

**2.5**安全培训服务

**2.5.1**安全意识培训服务

每年提供1次安全意识培训服务，必要时根据本单位要求，邀请相关网络安全专家进行专业培训。培训内容可包含但不限于：信息安全意识、信息安全发展方向、安全标准、政策法规解读、单位的周期性安全服务报告解读。

**2.5.2**服务价值与交付成果

通过安全培训服务以满足单位客户获取安全知识和经验的需求，从而使客户最终达到强化安全意识，理解安全理论，掌握安全技术，获得安全实践经验，通过安全认证，能够融会贯通并应用于所在单位的信息化安全建设当中。

**交付成果：安全培训材料**

**2.6**安全措施有效性验证服务

**2.6.1**网络边界管控有效性及策略核查服务

针对托管机房，定期每季度1次指派专业的安全服务工程师到客户现场，对网络边界、外联线路等安全情况进行分析，发现其可能存在的安全隐患。

**2.6.2**安全设备措施有效性及策略核查服务

针对托管机房，定期每季度1次指派专业的安全服务工程师到客户现场，对单位安全设备措施有效性及策略进行核查。

针对防火墙、入侵检测、防病毒网关等安全设备提供以下服务：

**1)安全策略优化：**根据业务变化情况，检查访问控制策略，调整和优化安全规则达到一致性。

**2)运行状态巡检**：检查设备运行状态，性能处理能力是否存在瓶颈或运行异常。

**3)自身安全性检查：**从设备账号管理、远程管理、权限管理等方面开展设备自身安全性检查。

**4)日志巡检：**定期检查相关安全设备日志进行分析，查看是否存在安全隐患。

**2.6.3**安全软件措施有效性及策略核查服务

针对服务范围内的业务系统，定期每季度1次指派专业的安全服务工程师到客户现场，对相关安全软件措施有效性及策略进行核查。

针对网页防篡改、终端防病毒、终端安全管理等现有安全软件提供以下服务：

**1)安全策略优化：**根据业务变化情况，检查访问控制策略，调整和优化安全规则达到一致性。

**2)运行状态巡检：**检查软件运行状态，性能处理能力是否存在瓶颈或运行异常。

**3)自身安全性检查：**从软件账号管理、远程管理、权限管理等方面开展设备自身安全性检查。

**4)日志巡检：**定期检查相关安全软件日志进行分析，查看是否存在安全隐患。

**2.6.4**服务价值与交付成果

根据业务环境变化情况，定期评估安全设备、安全软件的防护有效性，对已采取的安全措施的有效性进行确认，对有效的安全措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施。对于不适当的安全措施进行优化配置，并定期分析设备告警情况，及时发现安全隐患。

**交付成果：《安全措施有效性验证报告》**