**营运路段网络安全运维方案**

**2023年2月**

目 录

[1 项目概述 5](#_Toc27117)

[1.1 参考标准 5](#_Toc26962)

[1.2 遵循原则 6](#_Toc11115)

[2 服务内容 6](#_Toc6132)

[3 安全运维服务内容 9](#_Toc7885)

[3.1 安全风险评估服务 9](#_Toc13850)

[3.1.1 服务描述 9](#_Toc31001)

[3.1.2 输出成果 10](#_Toc12311)

[3.1.3 服务收益 10](#_Toc31514)

[3.2 等保建设咨询服务 10](#_Toc14919)

[3.2.1 等保差距分析 10](#_Toc2962)

[3.2.2 等保差距整改 11](#_Toc23789)

[3.3 安全巡检服务 12](#_Toc1044)

[3.3.1 系统漏洞检测 12](#_Toc15405)

[3.3.2 系统基线核查 14](#_Toc19880)

[3.3.3 安全日志审计 15](#_Toc25747)

[3.3.4 输出成果 15](#_Toc5037)

[3.4 安全加固服务 16](#_Toc26882)

[3.4.1 加固方法 16](#_Toc18058)

[3.4.2 加固指导内容 17](#_Toc17675)

[3.4.3 交付成果 19](#_Toc13617)

[3.5 应急响应服务 19](#_Toc20208)

[3.5.1 安全事件应急响应 20](#_Toc31626)

[3.5.2 输出成果 21](#_Toc7915)

[3.6 安全应急演练 21](#_Toc13612)

[3.7 安全通告服务 21](#_Toc15721)

[3.7.1 服务描述 21](#_Toc7971)

[3.7.2 输出成果 22](#_Toc14422)

[3.7.3 服务收益 22](#_Toc26761)

[3.8 重大活动安全保障 22](#_Toc32699)

[3.8.1 现场值守 22](#_Toc12602)

[3.8.2 预案制定 23](#_Toc11308)

[3.8.3 应急处理 24](#_Toc28407)

[3.8.4 输出成果 25](#_Toc9700)

[3.9 安全意识培训 25](#_Toc29860)

[3.10 其它 25](#_Toc6526)

[4 保密承诺 25](#_Toc29841)

[4.1 保密协议 26](#_Toc20391)

[4.1.1 保密协议的必要性 26](#_Toc24041)

[4.1.2 保密条款 26](#_Toc26437)

[4.2 项目实施人员专项保密承诺 27](#_Toc14013)

[4.2.1 保密承诺的必要性 27](#_Toc11743)

[4.2.2 保密内容和范围 27](#_Toc24391)

[4.2.3 保密责任 27](#_Toc28755)

# 项目概述

## 参考标准

1. **信息安全标准**

* GB/T 20984-2007信息安全风险评估规范
* GB/T 31509-2015信息安全风险评估实施指南
* GB/T 22239-2019 信息系统安全等级保护基本要求
* GB/T 25058-2019 信息系统安全等级保护实施指南
* GB/T 25070-2019 信息安全技术信息系统等级保护安全设计技术
* ISO/IEC 27001:2013信息安全管理体系要求
* IATF信息安全保障体系框架
* 《信息技术安全性评估准则GB/T 18336-2008》
* 《Open-Source Security Testing Methodology Manual v3》OSSTMM-2010
* 《Information Systems Security Assessment Framework》ISSAF-2008
* 《Web Security Threat Classification》WASC-2010
* 《OWASP Testing Guide v3》OWASP-2008

1. **国家法律法规**

* 中华人民共和国网络安全法
* 中华人民共和国计算机信息系统安全保护条例 （国务院147号令）
* 信息安全等级保护管理办法（公通字[2007]43号）

## 遵循原则

* **保密原则**

安全服务是一个长期的过程，对营运路段信息的保密尤为重要，除了保密协议的约束外，安全服务提供方须充分认识到安全服务工程同时是一项重大而光荣的任务，严格挑选安全服务人员，保障服务人员的可信度。

* **标准性原则**

安全服务方案的设计与实施依据国内或国际的相关标准进行；

* **规范性原则**

安全服务过程和文档设计遵循了多种安全标准，具有很好的规范性，可以便于项目的跟踪和控制；服务团队人员需具备为营运路段网络系统提供规范安全服务的能力。

* **可控性原则**

安全服务所使用的工具、方法和过程都事先与营运路段沟通确认，经双方认可方可实施，服务进度遵守进度表的安排，保证对服务工作的可控性；

* **最小影响原则**

提供所有安全服务的前提是要保障营运路段网络系统的业务连续性：任何服务项目都尽量不中断业务服务；同时对于占用网络或系统资源较大的服务项目，尽量避开业务高峰实施。

# 服务内容

为实现本次安全运维服务项目的目标，安全运维服务方要为营运路段提供以下安全服务内容。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务**  **项目** | **服务描述** | **服务方式** | **服务**  **说明** | **服务输出**  **文档** |
| 1 | 安全风险评估服务 | 安全风险评估，是从风险管理角度，运用科学的方法和技术手段，分析网络与信息系统所面临的安全威胁及存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，并提出针对性的安全防护建议和整改措施。  安全风险评估是对网络中已知或潜在的安全漏洞、安全风险、安全隐患，进行探测、识别、控制、消除的全过程，它是信息安全服务工作的必要组成部分，是信息安全工作中非常重要的一个环节。  安全风险评估的参考标准主要是GB/T 20984、GB/T 31509、公安部等级保护，风险评估方法包括但不限于资料收集、调查问卷、人员访谈、现场查勘、漏洞扫描、基线核查、风险分析。 | 现场 | 一年按需执行 | 输出包括但不限于 《安全风险评估报告》、《资产分析报告》、《脆弱性评估报告》、《威胁评估报告》 |
| 2 | 等保建设咨询服务 | 等保差距分析，是依据公安部等级保护基本要求，从物理、网络、主机、应用、数据、制度、机构、人员、建设、运维共十个方面，分析信息系统安全防护能力与对应等级要求之间的差距，明确不满足项并提出整改建议。  不同等级的要求存在差异，所以不同等级应用系统的等保差距分析，其工作量也存在差异。目前，应用系统大多定为二级或三级，等级越高，工作量越大。  等保差距整改，是双前期的等保差距分析报告为依据，为客户设计满足等级保护要求、可落地执行的安全整改建设方案并执行，确保信息系统满足等级保护要求，并顺利通过等级保护测评。  我们的等保差距整改，将以纵深防御为主要设计思路，为用户提供“三重防护、一个中心”的安全整改建设方案。 | 现场 | 一年按需执行 | 输出包括但不限于 《XX系统等级保护差距分析报告》（含安全整改建议）、《XX系统等保差距整改建设方案》 |
| 3 | 安全巡检服务 | 安全巡检服务，对高速公路路段中心、收费站和ETC门架的网络设备、安全设备、重要业务系统、重要终端等进行的安全检测，检测完成后提供全面的巡检报告，报告中给出存在的安全风险并提供对应的修复建议。  安全巡检服务内容，包括安全漏洞检测、基线配置核查、安全日志审计。 | 现场 | 每季度一次，一年共4次； | 输出包括但不限于 《XX安全巡检服务报告》《XX安全漏洞检测报告》、《XX基线配置核查报告》、《XX安全日志审计报告》 |
| 4 | 安全加固服务 | 安全加固服务，是协助对目标系统的安全漏洞进行修复、配置隐患进行优化的过程。  安全加固是保证设备和系统安全运行的关键防护措施，通常情况下，操作系统、数据库、中间件、网络设备、安全设备，都需要进行安全加固。 | 现场 | 一年按需执行 | 输出包括但不限于《XX安全加固报告》（含加固前后漏洞对比）、《XX加固前漏洞扫描报告》、《XX加固后漏洞扫描报告》、《XX安全加固应急及回退方案》 |
| 5 | 安全应急响应 | 应急响应服务，是在业务系统或服务器遭受黑客入侵攻击时，第一时间对入侵事件进行分析、检测、抑制、处理，查找入侵来源并恢复系统正常运行。  我们的应急响应服务，在完成应急事件事处理后，还将提供详细的应急响应报告，报告中将还原入侵过程，同时给出对应的解决方案。 | 现场 | 一年按需执行 | 输出包括但不限于 《XX系统安全应急响应报告》、《XX系统安全事件应急预案》 |
| 6 | 安全应急演练 | 根据应急预案和演练方案，协助用户完成各类安全事件的应急处置演练工作，确保安全应急工作的标准化和流程化，以及安全应急的效率和质量。  针对特定演练场景（网页被篡改攻击、网站遭受DDOS攻击、内网ARP攻击等)，制定演练预案、准备演练工具、参与演练软环境准备、协助演练硬件环境调测验证、进行正式应急演练、汇报总结。 | 现场 | 一年1次 | 输出包括但不限于《XX安全应急演练报告》 |
| 7 | 安全通告服务 | 安全通告服务，是每月为用户提供信息安全研究月报，月报内容包括本月的信息安全整体态势、新增漏洞数量、漏洞分布情况、高危漏洞分析、本月主要安全事件，以及针对新漏洞的更新和防护方案。  同时，在出现重大安全漏洞和突发事件时，将第一时间进行深度分析，并将对应的分析报告提供给用户。 | 远程 | 每月1次，一年共12次 | 输出包括但不限于《xx信息安全研究月报》、《xx重大事件分析报告》 |
| 8 | 重大活动安全保障 | 在重大会议或重大节假日期间，为用户提供全程的网络安全保障工作，确保用户业务系统的安全稳定运行。  1、内外网暴露面与风险清理：对保障单位内外网进行资产初步梳理，发现发布应用、以及各类业务系统，发现网络内开放的端口情况，摸清资产情况，下线无主资产、关闭风险端口，同时探测相关资产存在的漏洞隐患，形成整改清单。  2、人员驻守服务：提供30人天以上的安全值守服务，对发现的安全风险及时处置，组织和协调全体保障人员，共同分析研判和封堵网络攻击行为。  3、防护能力提升服务：针对发现的问题及防护短板，提出安全策略优化与加固建议，提供满足防护要求的安全设备解决方案，并安排专业的技术人员随时监测攻击事件并及时处置。 | 现场 | 1年按需执行 | 输出包括但不限于《xx现场值守日报》、《xx现场值守工作总结》、《xx网站安全应急响应预案》、《xx安全事件应急响应报告》 |
| 9 | 安全意识培训 | 为用户提供安全意识培训，内容包括信息安全普及知识、法律法规、安全趋势、安全管理、移动安全、大数据安全以及常见办公安全等。 | 现场 | 一年1次 | 输出包括但不限于《XX单位安全意识培训记录》 |
| 10 | 其它 | 根据业主需要，提供多种排名领先品牌的专业漏扫工具、基线核查工具、U盘接入检测工具、违规外联/内联检测工具等。 | 远程 | 1年按需执行 | 输出包括但不限于《XX单位安全检查报告》 |

# 安全运维服务内容

## 安全风险评估服务

### 服务描述

安全风险评估，是从风险管理角度，运用科学的方法和技术手段，分析网络与信息系统所面临的安全威胁及存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，并提出针对性的安全防护建议和整改措施。

安全风险评估是对网络中已知或潜在的安全漏洞、安全风险、安全隐患，进行探测、识别、控制、消除的全过程，它是信息安全服务工作的必要组成部分，是信息安全工作中非常重要的一个环节。

安全风险评估的参考标准主要是GB/T 20984、GB/T 31509、公安部等级保护，风险评估方法包括但不限于资料收集、调查问卷、人员访谈、现场查勘、漏洞扫描、基线核查、风险分析。

### 输出成果

安全风险评估的主要输出成果如下：

 《安全风险评估报告》

 《资产分析报告》、《脆弱性评估报告》、《威胁评估报告》

### 服务收益

我们的安全风险评估，可为客户带来以下收益：

 了解网络和信息系统的安全现状，明确采取何种安全措施，可以有效降低威胁事件发生的可能性及造成的影响，从而将风险降低到可接受的水平。

 明晰组织的网络安全需求，提出合理的安全规划建议，为制定或调整组织信息系统安全策略提供参考，为组织的网络安全规划提供依据。

## 等保建设咨询服务

### 等保差距分析

* + - 1. **服务描述**

等保差距分析，是依据公安部等级保护基本要求，从物理、网络、主机、应用、数据、制度、机构、人员、建设、运维共十个方面，分析信息系统安全防护能力与对应等级要求之间的差距，明确不满足项并提出整改建议。

不同等级的要求存在差异，所以不同等级应用系统的等保差距分析，其工作量也存在差异。目前，应用系统大多定为二级或三级，等级越高，工作量越大。

* + - 1. **输出成果**

等保差距分析的主要输出成果如下：

 《XX系统等级保护差距分析报告》（含安全整改建议）

* + - 1. **服务收益**

我们的等保差距分析，可为客户带来以下收益：

 准确评估信息系统与保护等级之间的差距，明确不符合要求的安全项。

 提供安全整改建议，为等保差距整改提供依据，为通过安全等级保护测评打下基础。

### 等保差距整改

* + - 1. **服务描述**

等保差距整改，是双前期的等保差距分析报告为依据，为客户设计满足等级保护要求、可落地执行的安全整改建设方案并执行，确保信息系统满足等级保护要求，并顺利通过等级保护测评。

我们的等保差距整改，将以纵深防御为主要设计思路，为用户提供“三重防护、一个中心”的安全整改建设方案。

* + - 1. **输出成果**

等保差距整改的主要输出成果如下：

 《XX系统等保差距整改建设方案》

* + - 1. **服务收益**

我们的等保差距整改，可为客户带来以下收益：

 落实国家信息安全的基本政策。

 确保信息安全建设的有的放矢，既符合等级保护要求，又使得投资决策更加科学有效。

## 安全巡检服务

信息安全是动态的，随着时间的变化会不断暴露出新的安全漏洞、恶意软件、攻击手段，新些将打打破现有信息安全的平衡。安全风险管理是一个持续性的过程，安全巡检服务是安全风险管理过程中的重要组成部分。

安全巡检服务，是指定期对营运路段的网络设备、安全设备、重要业务系统、重要终端等进行的安全检测，检测完成后提供全面的巡检服务报告，给出存在的安全风险并提供对应的修复建议。

通过安全巡检服务，可以有效发现设备和系统中存在的安全漏洞、安全配置隐患、安全风险，为安全加固提供事实依据。并通过周期性检查，促进ISMS信息安全管理体系和PDCA在实际工作中的执行，确保设备和系统的持续、安全、稳定运行。

安全服务提供方的安全巡检服务，包括系统漏洞检测、基线配置核查、安全日志审计。

### 系统漏洞检测

* + - 1. **检测方法**

漏洞检测指利用带有安全漏洞知识库的扫描工具，对业务系统进行基于网络的安全扫描，检测信息系统所存在的安全隐患和漏洞。

漏洞检测是进行安全风险评估的必要手段，可以识别主机开放的服务端口、用户账号、系统漏洞等信息，能较真实地反映业务系统的操作系统、数据库、中间件、网络设备、安全设备所存在的网络安全问题和面临的网络安全威胁。

1. **工具选择**

系统漏洞检测，需采用国产厂商自主研发的专业漏洞扫描设备，产品具有CNNVD国家漏洞库兼容性认证和国际CVE漏洞库兼容性认证。

1. **策略选择**

漏洞检测应遵循如下原则：

* **选取适当的扫描策略**

进行漏洞检测时，会依据不同类型的扫描对象、不同的应用情况，选择不同的扫描策略。除了利用扫描工具自身所集成的扫描策略外，对承载较复杂应用的评估对象，评估团队会按照不同的安全需求，编辑或生成适合于被评估对象的专用策略，应用量身定制的策略进行扫描，提高系统扫描效率，并达到更好的扫描效果。

* **选取适当的扫描时间**

为减轻漏洞检测对网络和主机的影响，漏洞检测时间尽量安排在业务量不大的时段或晚上。

* **单点试扫，主备分开**

对于重要的设备，先小范围进行扫描，确认系统不受较大影响后再进行大规模扫描。对双机热备的设备在一次扫描会话中只选取其中一台进行扫描。

* + - 1. **检测内容**

系统漏洞检测的内容，包括操作系统漏洞检测、数据库漏洞检测、中间件漏洞检测、网络设备漏洞检测、安全设备漏洞检测，并给出漏洞修复建议。

* **操作系统漏洞检测**

对业务系统的所有操作操作系统进行安全漏洞检测，查找操作系统中的安全隐患和安全隐患，并给出对应的漏洞修复建议。

* **数据库漏洞检测**

对业务系统的所有数据库进行安全漏洞检测，查找数据库中的安全隐患和安全隐患，并给出对应的漏洞修复建议。

* **中间件漏洞检测**

对业务系统的所有中间件进行安全漏洞检测，查找中间件的安全隐患和安全隐患，并给出对应的漏洞修复建议。

* **网络设备漏洞检测**

对业务系统的所有网络设备进行安全漏洞检测，查找网络设备中的安全隐患和安全隐患，并给出对应的漏洞修复建议。

* **操作系统漏洞检测**

对业务系统的所有安全设备进行安全漏洞检测，查找安全设备中的安全隐患和安全隐患，并给出对应的漏洞修复建议。

### 系统基线核查

* + - 1. **检测方法**

系统基线核查是指通过安全技术专家的经验，根据安全配置基线手册，对本次指定的目标主机的操作系统进行安全检查，发现其潜在的安全隐患，是作为漏洞检测发现弱点方式的补充。

通过基线检测和渗透测试发现应用服务在配置、补丁和日常维护和管理上存在的安全问题。

3. 3. 2. 1. **核查内容**

基线检测的内容主要包括安全配置检测、安全漏洞检测。

* **安全配置检测**

安全配置不合理通常都是由于人为的疏忽造成，主要包括了账号、口令、授权、日志、IP通信等方面内容，反映了系统自身的安全脆弱性。安全配置方面与系统的相关性非常大，同一个配置项在不同业务环境中的安全配置要求是不一样的，如在WEB系统边界防火墙中需要开启HTTP通信，但一个WAP网关边界就没有这样的需求，因此在设计业务系统安全基线的时候，安全配置是一个关注的重点。

* **安全漏洞检测**

通常是系统自身的问题引起的安全风险，一般包括了登录漏洞、拒绝服务漏洞、缓冲区溢出、信息泄漏、蠕虫后门、意外情况处置错误等，这些漏洞可通过系统配置进行行检查，从而反映出系统自身的安全脆弱性。

### 安全日志审计

* + - 1. **审计内容**

对防火墙、IPS、WAF等产生的安全日志进行收集，综合对这些日志进行关联分析，从多个维度对目标的运行状态进行分析，得出一段时间内目标系统及相关设备的安全运行状态。

* + - 1. **审计方法**

安全日志审计，采用工具和人工结合的审计方法综合进行。

### 输出成果

安全巡检服务的主要输出成果如下：

* 《营运路段巡检服务报告》

## 安全加固服务

为了有效保障网络的安全运行，在对操作系统、数据库、中间件、网络设备、安全设备进行安全检测后，需要对发现的安全风险进行修复。

由安全服务人员，根据安全加固列表，逐一对系统的安全漏洞、安全设置进行检测、修复、配置的全过程。安全加固是保证设备和系统安全运行的关键防护措施，通常情况下，操作系统、数据库、中间件、网络设备、安全设备，都需要进行安全加固。

通过安全加固，可最大程度消除或降低系统的安全风险，提升系统的安全防护能力，确保系统的持续、安全、稳定运行。

### 加固方法

安全加固，是指根据安全加固列表，采用人工手动加固方法，对目标系统的安全漏洞进行修复、基线配置进行优化的过程，是一项纯技术服务。

安全加固是一项对系统等进行的安全保护措施，通过安全加固一方面能够修补系统中的安全漏洞，同时也优化配置，加强对象的安全性。这对于安全保护来说，是非常必要的。

安全加固是为了解决在安全评估中发现的技术性安全问题，所有的被加固对象应不再存在高风险漏洞和中风险漏洞（根据CVE标准定义）。同时，在此过程中注意避免影响修补加固对象原有的功能和性能（若可能存在，必须事先指出，并进行周密的计划和布置规避相应的风险）。

安全加固首先要让加固对象满足安全基线要求，这是安全加固的基本目标。并采用优化配置、调整安全策略、安装补丁、安装安全软件等方式进行，在尽量不影响修补加固对象原有功能和性能的基础上，解决在安全评估中发现的安全问题，修补其中存在的漏洞。

安全加固也不仅仅局限于单独的加固对象，对象所处的环境，包括其他安全设备的安全防护（比如入侵检测系统、防火墙等）、网络结构等，都属于需要考虑的范围。在加固实施中，安全运维服务方也应对这些部分对加固对象的保护中提出积极的建议。

安全加固也是组织所制定的安全策略的实施实践，从实践的角度来检验安全策略的有效性。因此，安全加固的最终目的如下。

1. 确保对象满足安全基线要求；
2. 优化配置，安装适用的安全软件等加强对象的安全性能；
3. 从实践角度检验安全策略的有效性。

### 加固指导内容

* + - 1. **操作系统加固**

可进行安全加固的操作系统包括Windows、Linux、AIX、HP-Unix、Solaris。操作系统的加固内容如下表所示。

|  |  |  |
| --- | --- | --- |
| **序号** | **加固大项** | **加固小项** |
| 1 | 账号管理和认证授权 | 账号、口令、授权、关机设置 |
| 2 | 协议安全配置 | IP协议安全、防火墙、SYN攻击防护 |
| 3 | 服务和共享配置 | 系统服务、默认共享、共享权限 |
| 4 | 日志安全配置 | 日志审核策略、日志文件设置 |
| 5 | 其它安全配置 | 空闲超时设置、自动播放、启动项、数据执行保护 |

* + - 1. **数据库加固指导**

进行安全加固的数据库系统包括Oracle、SQL Server、DB2。数据库的加固内容如下表所示。

|  |  |  |
| --- | --- | --- |
| **序号** | **加固大项** | **加固小项** |
| 1 | 账号管理和认证授权 | 账号、口令 |
| 2 | 通信协议安全 | 网络数据传输安全、信任IP设置 |
| 3 | 日志安全配置 | 数据库审核策略、数据库日志文件设置 |
| 4 | 其它安全配置 | 连接超时设置、监听器密码 |

* + - 1. **中间件加固指导**

进行安全加固的中间件系统包括Tomcat、Apache、WebLogic、WebSphere。中间件系统的加固内容如下表所示。

|  |  |  |
| --- | --- | --- |
| **序号** | **加固大项** | **加固小项** |
| 1 | 账号管理和认证授权 | 账号、口令 |
| 2 | 通信协议安全 | 启用https传输、更改tomcat默认端口 |
| 3 | 日志安全配置 | 日志记录设置 |
| 4 | 其它安全配置 | 登录超时、错误重定向、禁止显示文件 |

* + - 1. **网络设备加固指导**

进行安全加固的网络设备包括主流厂商的路由器、交换机。网络设备的加固内容如下表所示。

|  |  |  |
| --- | --- | --- |
| **序号** | **加固大项** | **加固小项** |
| 1 | 账号管理和认证授权 | 账号管理、登录安全要求、认证授权 |
| 2 | 通信协议安全 | SNMP协议安全、路由协议安全、IP协议安全 |
| 3 | 日志安全配置 | 日志记录设置 |
| 4 | 其它安全配置 | 关闭不必要的服务、端口 |

* + - 1. **安全设备加固指导**

可进行安全加固的安全设备是主流厂商的防火墙，如迪普科技、天融信、绿盟等安全设备。安全设备的加固内容如下表所示。

|  |  |  |
| --- | --- | --- |
| **序号** | **加固大项** | **加固小项** |
| 1 | 账号管理和认证授权 | 账号、口令、授权 |
| 2 | 访问控制安全 | 安全策略、远程管理 |
| 3 | 日志安全配置 | 启用本地日志、启用远程日志 |
| 4 | 增强安全要求 | 限定管理IP、更改默认Banner、设备自身安全设置 |

### 交付成果

安全加固服务的主要交付成果如下：

* 《营运路段安全加固汇总报告》

## 应急响应服务

应急响应服务是为满足营运路段发生安全事件，需要紧急解决问题的情况而提供的一项安全服务。当营运路段发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，安全服务提供方的安全专家要在第一时间对安全事件进行应急响应处理，使营运路段网络应用系统在最短时间内恢复正常运行，帮助营运路段查找入侵来源，挽回或减少经济损失。

对安全事件进行应急响应处理后，安全服务提供方要提供详细的应急响应报告，报告中要还原入侵过程，同时给出对应的解决方案。

### 安全事件应急响应

服务期限内，安全运维服务方需提供7×24小时的远程安全应急响应，接到营运路段安全事件通知后，立即对安全事件进行分析、抑制、溯源。最大程度降低安全事件对营运路段带来的损失。

安全应急响应，包括以下服务内容。

* **判定安全事件类型**

从网络流量、系统和IDS日志记录、桌面日志中判断安全事件类型。查明安全事件原因，确定安全事件的威胁和破坏的严重程度。查明安全事件原因，确定安全事件的威胁和破坏的严重程度。

* **抑制事态发展**

抑制事态发展是为了将事故的损害降低到最小化。在这一步中，通常会将受影响系统和服务隔离。这一点对保持系统的可用性是非常重要的。

* **排除系统故障**

针对发现的安全事件来源，排除潜在的隐患，消除安全威胁，彻底解决安全问题。

* **恢复信息系统正常操作**

在根除问题后，将已经被攻击设备或由于事故造成的系统损坏做恢复性工作，使网络系统能在尽可能短的时间内恢复正常的网络服务。

* **用户信息系统安全加固**

对系统中发现的漏洞进行安全加固，消除安全隐患。

* **重新评估用户信息系统的安全性能**

重新评价用户系统的安全特性，确保在一定的时间范围内，不发生同类的安全事件。

* **安全态势监控**

定期跟踪国内外的安全漏洞发布平台（如CNCERT、CNVD、乌云），及时发现新近出现的安全漏洞，通过电话、邮箱等方式，及时向营运路段通告最新的针对业务的（或具有重大影响的）安全漏洞、安全病毒、安全攻击、安全技术等安全态势信息，并提供有参考意义的安全防护建议，保证营运路段信息安全工作的前瞻性和预判性。

### 输出成果

应急响应服务的输出成果如下：

* 《营运路段安全事件应急预案》

## 安全应急演练

根据应急预案和演练方案，协助用户完成各类安全事件的应急处置演练工作，确保安全应急工作的标准化和流程化，以及安全应急的效率和质量。

针对特定演练场景（网页被篡改攻击、网站遭受DDOS攻击、内网ARP攻击等)，制定演练预案、准备演练工具、参与演练软环境准备、协助演练硬件环境调测验证、进行正式应急演练、汇报总结。

## 安全通告服务

### 服务描述

安全通告服务，是每月为用户提供信息安全研究月报，月报内容包括本月的信息安全整体态势、新增漏洞数量、漏洞分布情况、高危漏洞分析、本月主要安全事件，以及针对新漏洞的更新和防护方案。

同时，在出现重大安全漏洞和突发事件时，将第一时间进行深度分析，并将对应的分析报告提供给用户。

### 输出成果

应急响应服务的主要输出成果如下：

 《xx信息安全研究月报》

 《xx重大事件分析报告》

### 服务收益

我们的安全通告服务，可为客户带来以下收益：

 让用户及时掌握最新的安全漏洞态势、前沿安全技术，以及最新的重大安全事件，第一时间进行安全预警和策略优化。

 提升用户安全人员的技术能力，提升用户信息化管理水平。

## 重大活动安全保障

重大活动安全保障，是指在重大会议、节假日等特殊时期内，我司派出安全攻防经验丰富的安全专家，进驻用户现场，协助用户对目标系统进行现场安全值守和保障，对网站的安全状况进行实时监控和日志分析。

在现场保障期间，当目标遭受黑客入侵攻击时，现场值守人员立即对入侵事件进行分析、检测、抑制、处理，查找入侵来源并恢复系统正常运行，完成后给出应急响应报告，报告中将还原入侵过程，同时给出对应的解决建议。

### 现场值守

现场值守的内容，主要包括以下三类：

* + - 1. **网站连通性监控**

通过系统自带的Ping工具或第三方监控工具，对目标网站的连通性进行实时监控，一旦网站的连通性出现异常，将第一时间得知，从而对其进行快速处理。

* + - 1. **网站运行状态监控**

通过流量分析系统之类的工具，对目标网站的出入流量进行实时监测，分析网站的流量 、并发、会话、全链接、半链接等关键数据，并同时对网站、数据库、中间件的日志进行分析并形成日志审计记录，从而有效评估网站的运行状态是否正常，确保网站的正常运行。

* + - 1. **网站安全状态监控**

通过防火墙、WAF、网站防篡改、IDS、DDOS流量清洗等设备，对目标网站的安全状态进行实时监控，实时了解网站的安全状况。

同时，通过高频率地对网站源代码进行递归备份，并使用文件对比工具，高频率地对网站源代码进行比对，可有效发现源代码更改情况，从而防止攻击者绕过安全设备对非法篡改网站页面。

### 预案制定

我司安全值守人员，将根据用户目标网站的安全现状，结合业界主流的网站攻击手法，分析网站可能遭受的攻击行为及其影响范围、严重程度，并和用户一起，提前制定对应的网站安全应急响应预案。

通过制定应急响应预案，可以在入侵攻击事件发生前防患于未然，当攻击事件发生时，可根据预案进行快速响应，从而在最短的时间恢复系统的正常运行。

### 应急处理

在目标网站遭受黑客入侵攻击时，现场值守人员立即对入侵事件进行分析，并结合应急响应预案，对入侵事件进行检测、抑制、处理，查找入侵来源并恢复系统正常运行。

入侵攻击事件的应急处理，包括但不限于以下内容。

 判定安全事件类型

从网络流量、系统和IDS日志记录、桌面日志中判断安全事件类型。查明安全事件原因，确定安全事件的威胁和破坏的严重程度。查明安全事件原因，确定安全事件的威胁和破坏的严重程度。

 抑制事态发展

抑制事态发展是为了将事故的损害降低到最小化。在这一步中，通常会将受影响系统和服务隔离。这一点对保持系统的可用性是非常重要的。

 排除系统故障

针对发现的安全事件来源，排除潜在的隐患，消除安全威胁，彻底解决安全问题。

 恢复信息系统正常操作

在根除问题后，将已经被攻击设备或由于事故造成的系统损坏做恢复性工作，使网络系统能在尽可能短的时间内恢复正常的网络服务。

 客户信息系统安全加固

对系统中发现的漏洞进行安全加固，消除安全隐患。

 重新评估客户信息系统的安全性能

重新评价客户系统的安全特性，确保在一定的时间范围内，不发生同类的安全事件。

### 输出成果

现场值守任务的输出成果如下：

 《xx现场值守日报》

 《xx现场值守工作总结》

 《xx网站安全应急响应预案》

 《xx安全事件应急响应报告》

## 安全意识培训

为用户提供安全意识培训，内容包括信息安全普及知识、法律法规、安全趋势、安全管理、移动安全、大数据安全以及常见办公安全等。

## 其它

根据业主需要，提供多种排名领先品牌的专业漏扫工具、基线核查工具、U盘接入检测工具、违规外联/内联检测工具等。

# 保密承诺

本次营运路段安全运维服务工作中，可能要涉及很多关键的设备数据和技术参数，同时安全服务提供方也可能会采用自己的独有技术进行深层次的风险检测，因此保密承诺的重要性在于，项目实施人员对营运路段网络与信息数据等相关信息的对外保密责任。

本项目的保密承诺分为以下两部分：

* 保密协议
* 项目人员项目专项保密承诺

## 保密协议

### 保密协议的必要性

保密协议可以确保在本项目中，双方对项目涉及的系统数据、技术参数等整体系统安全相关资料的保密。

双方以《中华人民共和国保守国家秘密法》为根本依据，并根据中华人民共和国国家科学技术委员会颁布的《科学技术保密规定》、《计算机软件保护条例》以及《商用密码管理条例》等相关法律、法规签订保密协议。

### 保密条款

承认接受的秘密资料。本协议中秘密资料包括通过口头、书面、电子或其他方式提供的关于技术和系统安全及其他方面的一切数据、报告、信息、翻译资料、预测和记录。

同意维护商业秘密资料的保密性，不向任何第三方披露有关信息，除非由于法律需要在必要的程度上向国家有关管理部门透露。同意在披露有关信息前，正式书面知会对方并得到对方书面许可。同意秘密资料只作为本项目的用途。

上所涉及的相关秘密资料包括以下内容：

* 整体系统安全策略相关技术
* 整体系统安全总体解决方案相关技术
* 所有整体系统安全服务的技术内容以及相关细节
* 所有检测报告、分析技术以及内容
* 所有的整体系统安全咨询技术内容
* 所有的整体系统安全培训技术内容
* 所有与该项目相关的技术文档
* 与此项目相关的商务信息

## 项目实施人员专项保密承诺

### 保密承诺的必要性

项目实施人员专项保密承诺可以确保在本项目工作中，人员本身对项目涉及的系统数据、技术参数等整体系统安全相关资料的保密。

双方应根据《中华人民共和国反不正当竞争法》、《中华人民共和国计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》、《商用密码管理条例》和国家、地方有关法律规范，为保障国家、营运路段及甲方的财产不受损害，就企业管理和技术秘密保护签订保密承诺。

### 保密内容和范围

所有项目参与人在项目中涉及到的相关技术资料。包括：机构设置和运行机置；计算机及其它辅助产品、安全产品的型号、数量、配置、运行状态等资料；应用系统名称、功能、业务类型、交易量、交易特征等信息；现有网络拓扑结构及其相关资料；业务流程、逻辑流程等资料；计算机系统的漏洞信息；现有安全机制及规划目标；项目文档、工程文档；与其它公司的合作信息、合同；其他需要保密的信息资料。对分析的过程数据和结果数据严格保密。

### 保密责任

所有人员必须按要求从事项目的实施工作，并将工程实施相关资料交保存。分析人员必须遵守国家的有关制度及的保密协议，在职或离职后均不得泄漏秘密内容（包括上述所列所有保密款项）给任何其他单位和个人，不得利用此数据进行非法操作（如侵害网络的行为）。