# 白云机场信息安全态势感知通报预警平台建设项目

# 综合评审采购文件

采购人：广州白云国际机场股份有限公司

二〇一九年十二月

# 总 目 录

# 第一部分

# 采 购 邀 请 函

# 第一部分 邀请函

广州白云国际机场股份有限公司（以下简称“采购人”）就股份公司白云机场信息安全态势感知通报预警平台建设项目进行国内公开采购，现邀请合格的供应商（以下简称“报价人”）提交密封报价文件。

**1、 项目概况：**

1）项目名称：白云机场信息安全态势感知通报预警平台建设项目

2）项目地点：广州。

3）项目内容：白云机场信息安全态势感知通报预警平台建设。

4）资金来源：企业自筹资金。

采购内容：

采购内容及限价

| 序号 | 服务内容 | 数量 | 采购最高限价 |
|---|---|---|---|
| 1 | 白云机场信息安全态势感知通报预警平台建设项目 | 1 项 | 人民币：217.77 万元 |
| 合计 | | | 人民币：217.77 万元 |

项目配置清单：

| NO | 平台配置清单 | 单位 | 数量 |
|---|---|---|---|
| 1 | 日志采集与分析引擎(含软件) | 套 | 1 |
| 2 | 未知威胁分析引擎(含软件) | 套 | 1 |
| 3 | 全流量分析引擎(含软件) | 套 | 2 |
| 4 | 态势感知通报预警平台(含软件) | 套 | 2 |

注：供应商必须对全部配置清单进行报价，各项费用为固定总价包干，在项目范围不变的情况下，该费用在合同执行期间不作调整。

**2、 合格供应商资格条件：**

1） 报价人必须为具备本项目履约能力的在中华人民共和国境内注册的独立的企业法人，同时持有登记机关颁发的营业执照，并提供加盖公章的营业执照的复印件。

2） 报价人具有增值税一般纳税人资格（需提供相应证明文件并加盖公章）。

3） 报价人需在广东省机场管理集团有限公司采购、招商管理网络平台(wz.gdairport.com)

主页中“合作商注册”模块，按规定格式填写正确的供应商登记信息，登记为合格的候选供应商（已注册的除外）。并提供应商登陆系统打印的合作商登记表并加盖公章。

4） 2016 年 1 月 1 日至今，报价人没有因腐败或欺诈行为而被政府或业主宣布取消报价资格；同时，2016 年 1 月 1 日年至今报价人（包括其关联公司）与采购人无发生各种诉讼、仲裁和不良投诉。（须就此项内容提供承诺函并加盖报价人公章）。

5） 报价人不得被列为“黑名单”，以“信用中国”网站（www.creditchina.gov.cn）查询为准，报价人需在采购公告发布后按采购文件给定的格式要求从“信用中国”网站截图并加盖公章（未按格式要求截图或截图信息不清晰将作废标处理），同时下载信用评估报告、打印并加盖公章后附在报价文件中。（截图格式见附录 9）

6） 报价人不得被列为严重违法失信企业名单（黑名单），以“国家企业信用信息公示系统”网站（www.gsxt.gov.cn）查询为准，报价人需在采购公告发布后从“国家企业信用信息公示系统”网站截图并加盖公章。（截图格式见附录 8）

7） 报价人法定代表人为同一人的两个及两个以上法人；母公司、全资子公司及其控股公司，都不得在该项目中同时报价。

8） 报价人必须具有有效的 ISO90001 质量保证体系认证，并提供证书的复印件并加盖公章。

9） 报价人必须具有中国信息安全认证中心颁发的信息安全服务资质（信息系统安全集成三级及以上）或中国信息安全测评中心颁发的信息安全服务资质（安全工程类一级及以上），并提供证书的复印件加盖公章。

10）报价人如非产品制造商，必须取得原制造厂商的唯一授权。

11）本项目不接受联合体报价。

**3、 获取采购文件**

1） 本次采购文件同时在集团公司采购招商管理网络平台 wz.gdairport.com 上发布。

2） 在规定的报名期间，报名的供应商不足 3 名时，采购人有权：

① 发布公告延长接受报名时间。在延期报名时间内，已报名供应商的资料仍有效并可自行补充资料，未报名的申请单位可根据公告的约定参与报名。

② 重新采购。

**4、 报价文件的提交形式、地址和截止时间**

1） 报价人须现场递交方式递交项目报价文件。

2） 报价文件现场递交地址为：广州市白云区人和镇新白云机场东南工作区广州白云国际

机场股份有限公司办公楼 425 办公室，收件人：张利

3） 报价文件递交截止时间：2020 年 1 月 6 日。报价文件按指定时间、地点送达，逾期递交的报价文件恕不接受。

4） 采购人不接受以邮件、电话、传真等形式的报价。

**5、 本项目不设未成交供应商经济补偿，准备报价文件和递交报价文件所发生的任何成本或费用由供应商自理。**

**6、 有关此次采购之事宜，可按下列地址向采购人查询：**

采购人：广州白云国际机场股份有限公司

地　址：广州市白云区人和镇新白云机场东南工作区广州白云国际机场股份有限公司办公楼 425 办公室

联系人：张利

联系电话：13824401857

投诉监督

供应商可以对本次采购采购活动中的任何违法及不公平内容向广州白云国际机场股份有限公司纪检监察室实名投诉。

联系电话：020-36067072

# 第二部分

# 供 应 商 须 知

# 第二部分 供应商须知

## 目　录

# 一、说　明

## 1　项目说明

**1.1**　广州白云国际机场股份有限公司拟就白云机场信息安全态势感知通报预警平台建设项目进行国内采购，本项目采用采购形式确定成交供应商，广州白云国际机场股份有限公司组织采购工作。

1.2　采购范围

1）采购内容及限价：

| 序号 | 服务内容 | 数量 | 采购最高限价 |
|---|---|---|---|
| 1 | 白云机场信息安全态势感知通报预警平台建设项目 | 1 项 | 人民币：217.77 万元 |
| 合计 | | | 人民币：217.77 万元 |

2）服务内容：

| NO | 平台配置清单 | 单位 | 数量 |
|---|---|---|---|
| 1 | 日志采集与分析引擎(含软件) | 套 | 1 |
| 2 | 未知威胁分析引擎(含软件) | 套 | 1 |
| 3 | 全流量分析引擎(含软件) | 套 | 2 |
| 4 | 态势感知通报预警平台(含软件) | 套 | 2 |

注：：供应商必须对全部配置清单进行报价，各项费用为固定总价包干，在项目范围不变的情况下，该费用在合同执行期间不作调整。

1.3　采购要求

1.3.1　本项目技术服务进度要求：

明确工作时间要求：项目完成时间 2020 年 3 月 30 日前

如果进度延误，每逾期一天，成交供应商需向采购人支付最终合同价格的 0.03%作为逾期损害赔偿；逾期损害赔偿费的最高限额为最终合同价格的 3%。

1.3.2　供应商的项目报价应将相关配置报价。

1.3.3 供应商所提供的工作方案必须详细、完整、可靠、可行性强。

1.3.4 供应商报价中的费用应是供应商为完成本项目的总费用。

1.3.5 供应商必须提交对采购文件实质性响应的项目报价文件。

1.4 现场考察

1.4.1 工程现场考察由供应商自行前往，采购人不统一安排。供应商若需相关数据，须自行测量。

## 2 定义

2.1 本文件中下列术语定义为：

服务： 指供应商提供白云机场信息安全态势感知通报预警平台建设。

供应商： 指与第 3 条规定的要求一致的、响应采购邀请函、参加报价的独立法人。

采购人： 广州白云国际机场股份有限公司。

合同： 指由采购所产生的合同或合约文件。合同由广州白云国际机场股份有限公司与成交供应商签订。

## 3 合格的供应商

3.1 合格的供应商要求见采购邀请函中的第 2 点。

## 4 合格的服务

4.1 合同中提供的所有服务，均应来自中华人民共和国或与之有正常贸易关系的国家和地区，本合同的支付仅限于对这些服务。

## 5 报价费用

供应商应承担所有编写项目报价文件和参加报价的所有费用，不论采购的结果如何，采购人在任何情况下均无义务和责任承担这些费用。

# 二、采购文件

## 6 采购文件构成

6.1 要求提供的服务、采购过程和合同条件在采购文件中均有说明。采购文件包括：

第一部分 采购邀请函
第二部分 供应商须知
第三部分 合同条款
第四部分 项目报价文件格式
第五部分 用户需求书

6.2 供应商应认真阅读采购文件中所有的事项、格式、条款和规范等要求。供应商没有按照采购文件要求提交全部资料，或者项目报价文件没有对采购文件各方面都做出实质性响应的供应商的项目报价文件将被拒绝。

## 7 采购文件的澄清

7.1 任何要求对采购文件进行澄清的供应商，均应以书面形式通知采购人。

7.2 采购人将通过广东省机场管理集团有限公司采购、招商管理网络平台(wz.gdairport.com)以补充 公告的形式对采购文件进行澄清。

## 8 采购文件的修改

8.1 在规定的递交报价文件截止日期前的任何时候，无论出于何种原因，采购人可主动或在解答供应商提出的需澄清问题时以修改书对采购文件进行修改。

8.2 修改书是采购文件的组成部分，对所有参与供应商均有约束力。供应商在收到采购文件的修改书应书面通知采购人。

8.3 为使供应商编写报价文件时，有充分时间对采购文件的修改部分进行研究，采购人可自行决定，酌情延长报价文件递交截止日期。

## 9 采购语言及计量单位

9.1 采购方发出的采购文件采用中文。

9.2 采购文件中使用的计量单位都是公制系统。

# 三、项目报价文件的编制

## 10 项目报价文件

10.1 报价文件由商务文件和技术文件两部分组成。

10.2 报价文件的签署要求：报价文件所有需盖章或签字的部分均需报价人法定代表人或法定代表人授权委托代表签字并加盖公章，否则将被视为无效报价文件。

10.3 报价文件包括纸质文件一式 5 份，计算机文件一式 1 份。纸质版正本 1 份，封面标注“正本”字样，副本 4 份，封面标注“副本”字样。正本与副本不符的内容，以正本为准。

10.4 报价文件应做到清晰、完整，文本、图纸规格应当尽量统一。除非另有规定，否则报价文件的计量单位宜采用国际标准计量单位，尺寸齐全、准确，所有文字说明和文字标注以中文为准，报价均为人民币，时间均为北京时间。

## 11 报价文件编制要求

11.1 报价文件由下列资料组成：

1） 封面：写明项目名称、供应商名称及年月日；加盖供应商公章。
2） 目录。
3） 填妥并盖章的报价函（格式见附录 1）。
4） 报价明细表（格式见附录 2）
5） 诚信承诺函及企业声明（格式见附录 3）
6） 法定代表人证明书及法定代表人授权书（格式见附录 4）
7） 企业营业执照复印件（盖公章）。
8） 增值税一般纳税人证明文件（盖公章）。
9） 广东省机场管理集团有限公司采购、招商管理网络平台合作商登记表（盖公章）。
10）报价人没有因腐败或欺诈行为，与采购人无发生各种诉讼、仲裁和不良投诉的承诺函（盖公章）。
11）“信用中国”网站（www.creditchina.gov.cn）下载的信用评估报告（盖公章）。
12）“国家企业信用信息公示系统”网站（www.gsxt.gov.cn）查询截图（盖公章）。
13）有效的 ISO90001 质量保证体系认证，并提供证书的复印件（盖公章）。
14）中国信息安全认证中心颁发的信息安全服务资质（信息系统安全集成三级及以上）或中国信息安全测评中心颁发的信息安全服务资质（安全工程类一级及以上），并提供证书的复印件（盖公章）
15）报价人如非产品制造商，必须提供原制造厂商的唯一授权。
16) 提供由国家信息中心网络安全部提供的硬盘数据恢复服务，并提供授权书及售后服务承诺函。
17）为本项目拟投入的技术力量。主要包括项目负责人及项目经理的资格、服务经历及业务能力，项目组服务人员的资格、经历及业务能力，参加本项目人员配置情况等，对资格、获奖及经历等内容必须附上有关的证明材料，并能保证材料的真实性；（格式见

附录 5）。

18）企业类似业绩证明材料复印件（格式见附录 6）。

19）企业获奖业绩表及证明材料复印件（格式见附录 7）

20）本项目的服务方案，完工本项目工作的具体举措，服务计划表，拟投入人员情况等。

21）报价人认为有必要提供的其他资料。

11.2 报价文件密封袋（箱）应用封条在开口处密封，填写密封日期，封条上加盖供应商单位公章。

## 12 知识产权和专利权

12.1 供应商应保证，采购人在中华人民共和国使用供应商在服务期间提供的成果的任何一部分时，免受第三方提出侵犯其专利权、商标或工业设计权的起诉。

12.2 报价已包括所有应支付的，对专利权和版权、设计或其他知识产权而需要向其他方支付的版税。

## 13 保密

13.1 如采购人向供应商提供图纸、详细资料、样品、模型、模件和所有其他资料，这些均被视为保密资料，仅被用于它所规定的用途，除非得到采购人的同意，不能向任何第三方透露。

## 14 报价文件有效期

14.1 ★项目报价文件应在采购邀请函规定的报价日后的 90 天有效期内保持有效。报价文件有效期比规定短的将被视为非响应报价而予以拒绝。

14.2 特殊情况下在原有报价文件有效期截止之前，采购人可征求供应商同意延长报价文件有效期。这种要求与答复均应以书面形式提交。供应商可以拒绝采购人的这种要求。

## 15 不允许偏离的条款

15.1 采购文件中的重要条款（带“★”号条款）不允许偏离，如项目报价文件中对重要条款有偏离，则是供应商的风险。

15.2 对供应商须知 15.1 条中任何条款的偏离将导致报价文件无效。

15.3 下述条款不应视作不可偏离：

1) 未加注“★”号的条款；
2) 用户需求书中已明确的供应商可提供其他优选报价文件部分。

15.4 项目报价文件中优于用户需求书要求部分不视作偏离，将不被拒绝，供应商对这种优于基础资料和设计任务书要求的情况必须单独说明。

# 四、项目报价文件的递交

## 16 项目报价文件的密封和标记

16.1 供应商应将项目报价文件应第三部分 11.2 要求密封和标记。

16.2 如果报价人递交的报价文件未按要求密封，采购人将拒绝接受其报价文件。

16.3 如果因密封不严，标记不清而造成报价文件过早启封、失密等情况，采购人概不负责。

## 17 递交报价文件截止时间

17.1 供应商应将正本和所有副本，由供应商代表按采购邀请函第 5 条要求于项目递交报价文件截止时间前送达报价地点。

17.2 采购人可以通过修改采购文件自行决定酌情延长截止期。在此情况下，采购人和供应商受截止期制约的所有权利和义务均应延长至新的截止日期。

## 18 迟交的项目报价文件

18.1 采购人将拒绝在截止时间后递交的任何项目报价文件。

# 五、采购过程

## 19 报价文件的递交

19.1 采购人在采购文件中规定的日期、时间和地点在有供应商代表在场的场合组织接收报价文件，参加报价的供应商代表应签到以证明其出席。

## 20 评审小组

20.1 本项目的评审工作由采购人内部组成评审小组完成。评审小组共 5 名成员。

## 21 项目报价文件的评审

21.1 评审小组将审查项目报价文件是否完整、供应商是否符合合格条件、报价有无计算上的错误、文件签署是否合格、项目报价文件的总体编排是否有序。

21.2 算术错误将按以下方法更正：

1) 如果总价与数量乘单价的积而得到的总价不一致，则以单价为准计算总价。
2) 如果用大写数值与用数字表示的数值不一致，以大写数值为准。

21.3 在详细评审之前，评审小组会要审查每份项目报价文件是否实质上响应了采购文件的要求。实质上响应的报价文件应该是与采购文件要求的全部主要条款（加“★”号）、条件和规格相符，没有重大偏离的报价文件。

21.4 如果项目报价文件实质上没有响应采购文件的要求，其报价文件将可能被拒绝。不满足下列情况之一的，其报价文件将可能被拒绝：

1) 完全符合采购邀请函中第 3 点“合格的供应商”要求；
2) 报价有效期符合采购文件规定；
3) 供应商递交一种报价方案和报价；
4) 报价没有超过最高限价；
5) 报价函必须有法定代表人或授权代表签字且加盖公章；
6) 报价文件须有法定代表人或授权代表签字且加盖公章；
7) 法定代表人授权书必须有法定代表人和被授权人的签字或盖章；

## 22 报价文件的详细评审

22.1 评审小组对通过初步评审的报价文件中的商务服务、技术方案等方面采用百分制综合评分，其构成及权重为：价格部分得分占 30%，商务技术部分得分占 70%，详细评分标准如下：

1）商务技术评分表

| 序号 | 项目 | 评审内容 | 评分 |
|---|---|---|---|
| 1 | 报价人资质 | 1、报价人获得 CMMI5 证书，在报价文件中需提交资质证书扫描件并加盖报价人公章。<br>2、报价人获得由国家认证认可监督管理委员会批准、经国家登记主管机关依法登记册的第三方认证机构所颁发的《知识产权管理体系认证证书》（知识产权管理体系符合标准：GB/T 29490-2013）<br>3、报价人获得中国网络安全审查技术与认证中心颁发的《信息安全服务资质认证证书》（信息安全风险评估一级）<br>4、报价人获得中国网络安全审查技术与认证中心颁发的《信息安全服务资质认证证书》（信息安全应急处理一级）<br>5、报价人获得国家互联网应急中心的《应急服务支撑单位》国家级<br>6、报价人产品同时具备公安部颁发的销售许可证和 IPV6 READY LOGO 认证。<br>满分 10 分，有一项不满足扣 2 分，直至扣完为止。 | 10 |
| 2 | 报价人技术团队实力 | 报价人技术团队实力评估（需提供人员社保证明）：<br>**1、2 名项目经理，满分 10 分，具体要求：**<br>其中一人：获得 PMP、CISP、获得 ITIL FOUNDATION、获得 ISO 27001 LA 等证书，<br>全部证书具备得 5 分，部分证书具备不得分<br>另一人：获得信息系统项目管理师、国际注册内部控制师（CICS）、信息安全等级保护测评师、注册信息安全专业人员认证（CISP）、主任审核员（ISO27001 LA）、CCSK 认证资质，<br>全部证书具备得 5 分，部分证书具备不得分<br>**2、至少 5 名实施人员，满分 5 分，具体要求：**<br>成员需具备 CISP 大数据安全分析师（CISP-BDSA）或 CISP 云安全工程师（CISP-CSE）证书，一人具备证书得 1 分，满分得 5 分。 | 15 |
| 3 | 报价人业绩情况 | 报价人类似项目合同金额超过 400 万以上的项目达到 5 个或以上的，得 5 分；少于 5 个大于等于 3 个得 2 分；少于 3 个得 0 分；<br>其中类似项目是指项目名称、供货产品清单或服务内容名称含态势感知、安全态势、安全大数据中心、大数据智能、安全威胁分析、安全数据分析、安全监测预警、云审计大数据、安全监控、安全综合分析、关键信息基础设施安全防护管理平台或网络安全预警安全字样，或项目建设内容可体现以上字样需求的。 | 5 |
| 4 | 技术方案评估 | 1、对甲方业务现状分析是否到位，平台建设（集成、衔接，及实施计划安排等问题）是否符合甲方现状进行落地，是否符合甲方项目定位、目的；<br>2、对甲方的 IT 环境、业务组成熟悉度，提供技术方案的全面性和优劣性；<br>3、对平台分期建设规划建议与甲方需求迫切度吻合程度是否合理；<br>4、提供的质量保障手段是否完善，是否充分考虑各种风险；<br>5、安全运营能力是否匹配甲方现行及未来的业务发展； | 15 |

| | | | |
|---|---|---|---|
| | | 专家根据技术方案进行综合评判，满分为 15 分；<br>其中：优良为 15-11 分；好为 10-6 分；一般为 5-0 分； | |
| 5 | 核心产品重点技术指标评估 | 报价人对综合评审采购文件中的“技术指标功能要求表”内容进行评估，提交对应的“技术指标功能要求响应表”，并按要求提供相关资料；其中“▲”为重点技术要求项，每一个“▲”不满足项扣 2 分，其他一般项每一个不满足项扣 0.5 分 ，直至扣至 0 分。 | 15 |
| 6 | 数据恢复服务及保密 | 报价人提供由国家信息中心网络安全部提供硬盘数据恢复服务，并提供授权书及售后服务承诺函得 10 分。<br>不能提供由国家信息中心网络安全部开具的授权书及售后服务承诺函不得分。 | 10 |

2）价格评审细则：价格分满分 30 分，各供应商的价格得分按如下标准计算：

（1）基准价：取所有通过初步评审的供应商报价的算术平均值作为基准价，

（2）当报价等于基准价时，价格得分为 30 分；

（3）当报价高于基准价时，按每高 1%的在 30 分基础上扣 1 分，不足 1%的按插值法计算，直至扣至 0 分；

（4）当报价低于基准价时，按每低 1%的 在 30 分基础上扣 1 分，不足 1%的按插值法计算，直至扣至 0 分；

（5）基准价为所有进入价格评审的响应人的评标价中去掉一个最高价和一个最低价后的算术平均值（若进入价格评审的响应人小于 5 家时，则计算时不去掉最高价和最低价）。基准价和价格得分的计算结果均保留两位小数，第三位四舍五入。

## 23 综合得分计算

23.1 综合得分＝商务技术得分+价格得分。

## 24 成交供应商的确定

24.1 评审小组按综合得分从高到低排序，推荐综合得分最高的报价人为第一成交候选人，综合得分次高者为第二成交候选人，依次类推，评审小组将推荐总得分前 3 名的报价人为成交候选人。如出现总得分相同，评审价低者排名靠前，若评审价仍相同，则由评审小组投票，按少数服从多数原则确定供应商排名先后。

24.2 采购人根据评审小组的推荐，就本项目确定成交供应商，并由采购人将结果通知所有参加报价的未成交的供应商。

## 25 与采购人的接触

25.1 除供应商须知的相关规定外，从报价文件截至之日起至授予合同期间，未经采购人书面要求，供应商不得就与其项目报价文件有关的事项与采购人联系。

25.2 供应商试图对评审小组的评比或采购人授予合同的决定进行影响，都可能导致其报价文

件被拒绝。

# 六、授予合同

## 26 资格后审

26.1 采购决定将考虑供应商的财务、服务能力等，其基础是审查供应商提交的资格证明文件和其它采购人认为必要的、合适的资料。

26.2 如果审查通过，则将合同授予符合第 31.1 条规定的供应商；如果审查没有通过，则取消其成交资格。在此情况下，评审小组将对技术和商务上充分满足采购文件要求的供应商中，综合得分次高的供应商能否满意地履行合同义务作类似的审查，或重新组织采购。

## 27 合同授予标准

27.1 除第 36 条的规定之外，采购人将把合同授予被确定为实质上响应采购文件的要求并具有履行合同能力的符合采购需求、综合得分最高的供应商。

## 28 授予合同时更改采购服务数量的权力

28.1 采购人在授予合同时有权在一定的幅度内对报价表中规定的服务数量予以增加或减少，但不得对单价或其它的条款和条件做任何实质改变。

## 29 接受和拒绝任何或所有报价文件的权力

29.1 采购人保留在签署合同之前任何时候根据评审小组的决定拒绝所有或任何报价文件，以及宣布所有或任何项目报价文件无效的权力，对受影响的供应商不承担任何责任，也无义务向受影响的供应商解释采取这一行动的理由。

## 30 成交通知书

30.1 在项目有效期期满之前，采购人将经过采购人确认的成交通知书以书面形式通知成交供应商。

30.2 成交通知书将是合同的一个组成部分。

## 31 签订合同

31.1 成交供应商在收到成交通知书后，应派遣其授权在合同上签字的代表与广州白云国际机场股份有限公司签署合同。

31.2 合同的组成基于本采购文件的以下部分以及项目报价文件的相应的部分：

（1） 第三部分 合同条款

（2） 最后报价承诺澄清文件

（3） 第四部分 附件－报价文件格式

（4） 第五部分 用户需求书

31.3 如果成交供应商没有按照上述第31.1条规定执行，采购人将有充分理由取消该成交决定。在此情况下，采购人可将合同授予其他满足采购要求的供应商，或重新组织采购。

## 32 成交结果通知

32.1 采购人会在广东省机场管理集团有限公司采购、招商管理网络平台(wz.gdairport.com)发布采购结果，并于公示完毕后 7 个工作日内将已盖公章的成交通知书发给候选成交报价人，原件及扫描件均有效。

# 第三部分

# 合 同 条 款

合同编号：

# 服务采购合同

**项目名称：**白云机场信息安全态势感知通报预警平台建设项目

**委托方（甲方）：**广州白云国际机场股份有限公司

**受托方（乙方）：**_____

**签订时间：**　年　月

**签订地点：**广州市

本合同甲方委托乙方就白云机场信息安全态势感知通报预警平台建设项目进行项目建设，并支付项目建设报酬。双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国合同法》的规定，达成如下协议，并由双方共同恪守。

**第一条** 乙方进行项目建设的内容、要求和方式：

1、项目内容：

甲方委托乙方对股份公司提供信息安全态势感知通报预警平台建设，具体的内容如下：

| NO | 平台配置清单 | 单位 | 数量 | 金额 |
|---|---|---|---|---|
| 1 | 日志采集与分析引擎(含软件) | 套 | 1 | |
| 2 | 未知威胁分析引擎(含软件) | 套 | 1 | |
| 3 | 全流量分析引擎(含软件) | 套 | 2 | |
| 4 | 态势感知通报预警平台(含软件) | 套 | 2 | |
| 5 | 安全文明施工费 | 项 | 1 | |
| 6 | 规费 | 项 | 1 | |
| 7 | 税费（1—6 项累计×9%） | | | |

备注：以上总金额包含乙方所供软件出厂价、安装调试费、杂费、保险费、服务费、税费等。除此以外，甲方无须再向乙方支付其他费用。

2、项目建设要求和方式：

（1）乙方负责提供相应项目建设报告初稿供甲方审阅，并按甲方意见进行核对修改；

（2）乙方完成相应项目建设报告正式文本的修改，向甲方提交《项目建设方案》正式文本纸质版一式三份。

（3）在项目建设过程中，乙方应遵守国家法律法规及地方法规的有关规定。

（4）乙方对甲方为完成实施项目建设而提供的任何技术资料、数据或其他工

作成果负有保密义务，应妥善保管，不得泄露，并不得以任何形式提供给任何第三方或用于本合同以外的其它目的。

**第二条** 项目建设报酬及支付方式为：

1、项目建设报酬总额为：_____；

2、项目建设报酬由甲方分 两期 支付给乙方。

具体支付方式和时间如下：

（1）合同签订后，甲方收到乙方提供的合格发票后 15 个工作日内，向乙方支付合同总金额的 50%，即人民币　　万元整（小写：　　元）。

（2）乙方完成全部项目建设内容，并按甲方要求办理完结算手续，甲方收到乙方提供的合格发票后 15 个工作日内，向乙方支付合同总金额的 50%，即人民币　万元整（小写：　　元）。

（3）乙方提供的发票必须为增值税专用发票。开具发票等相关的税费均由乙方承担，除合同约定的费用，甲方不再额外支付乙方其他费用。

开户银行：_____

账　　户：_____

账　　号：_____

**第三条** 包装、质量标准、售后、技术服务和保修

1、乙方向甲方所提供的产品，均为原产品生产厂商在中国大陆合法销售、使用的产品，并满足国家有关标准，保证甲方的合法使用权。

2、乙方向甲方提供产品的配置参数、质量标准、技术指标必须满足合同的约定，以及乙方在报价文件中的承诺和产品生产厂家的标准。

3、乙方向甲方提供的产品，必须是产品生产厂家原厂的标准原包装，包括随机资料等且为未使用之全新产品。

4、自甲方货物验收合格之日起，保修及售后服务按原厂家规定的标准执行，如甲乙双方在合同条款里有另行约定时必须按合同保修条款执行：乙方向甲方提供产品的原厂免费保修期为　　年，乙方免费技术响应电话：　　，响应时间：　　。

5、技术服务

（1）乙方根据合同派往现场参加开箱检验的人员 应能够全权处理开箱检验中出现的 问题：参加指导安装调试的人员应经验丰富，有较高技术水平 ，能够协调或解决安装调试过程中的全部问题，参加试运行的人员应能够全权处理合同货物试运行中的所有问题 。

（2）当甲方要求乙方提供现场服务时，乙方技术人员应在接到甲方通知后 24 小时内给予答复并在 48 小时内到达现场。技术协议或专用条款另有约定的除外 。

（3）乙方技术人员、物流人员及车辆在现场提供到货、安装、调试等服务时应严格遵守施工现 场的各项安全规章制度，自觉做好安全保护措施（如进入施工现场需佩戴安全帽等〕，接受现场的监督管理：在施工现场未经许可，不得拆卸、涂抹、损坏任何货物：对合同货物的调试要在现场监理的监督下进行操作，必要时须经过现场监理或项目部负责人的同意。若乙方技术人员违反现 场安全规章制度 ，甲方有权提出更换违反上述规章制度或不符合要求的乙方现场服务人员 ，乙方应根据现场需要，重新选派甲方认可的服务人员。因上述原因引起的一切后果，由乙方承担。

（4）乙方应在合同生效后 15 日内以传真方式向甲方提交执行技术协议约定的技术服务工作的组织计划一份，双方据此确定技术联络会的次数、时间和地点。

(5)双方协商确定的安装、调试和运行技术服务方案（如有），乙方如有修改，须以书面形式 通知甲方，经甲方确认后方可实施。为适应现场条件的要求，甲方有权提出变更或修改意见，并书面通知乙方，乙方应给予充分考虑，尽量满足甲方要求。其他规定见专用条款 。

(6)甲方发生合同货物故障时，需乙方提供技术支持的，乙方应全力配合甲方恢复合同货物运行并查明故障原因。由于乙方原因导致故障的，乙方应在 30 天内向甲方提供详细书面报告 。

(7)乙方负责为甲方提供有关合同货物安装、调试、使用、维护技术的培训，指派熟练称职的技术人员对甲方指定的技术人员进行技术培训。培训范围应包含但不限于设备安装使用说明书和检修维护手册 。

(8)乙方指派的培训人员的资质要求：具有 5 年以上相关专业工作经验和类似项目培训经验，熟练掌握设备结构性能、系统功能 、操作程序 、维修方法等技术 。

(9)乙方应在培训开始前一个月向甲方提供培训计划，双方将根据合同规定和甲方实际需要，在培训开始前一个月内确定具体培训内容和计划。

(10)乙方提供所有必要且具有可行性的培训资料和工具，如教材、使用手册 （ 明确日常维护周期、维修周期等事项）、合同货物图纸、专用工具和仪器等 。培训教材归甲方所有。培训资料如有更新，乙方应及时免费向甲方提供最新版本 。

(11)培训地点在乙方工厂或合同规定的其他地点。培训须用中文普通话完成。乙方必须按照使用手册里的日常维护周期、项目，AB 修周期、项目、方法进行演示，保证其可行性 。

**第四条** 验收标准与方式

1、 验收标准

（1）货物部分：货物的型号、规格、数量、配置、包装满足合同规定的条款，以及产品原厂商的产品标准。

（2）软件及功能部分按照综合评审采购文件技术要求进行验收。（可带附件）

2、 验收方式

（1）交货日期：_____日前送货。

（2）收货公司： _____ 。

（3）收货地点： 广州白云国际机场运控大楼 。

（4）收 货 人： _____ 。

（5）联系电话： _____ 。

（6）交货方式：由乙方负责将全部货物一次性交到甲方指定地点，并承担由此产生的一切费用（如包装费、运输费等）。

（7）货物签收：甲方必须由合同签订人或合同指定收货人签收。

（8）货物签收前的一切风险由乙方承担。

**第五条** 项目联系人

双方确定，在本合同有效期内，甲方指定 _____为甲方项目联系人，乙方指定本项目负责人_____为乙方项目联系人。项目联系人承担以下责任：

1、督促工作进度；

2、传递有关信息、资料；

3、合同双方一切未尽事宜的协调。

一方变更项目联系人的，应当及时以书面形式通知另一方。未及时通知并影响本合同履行或造成损失的，应承担相应的责任。

**第六条** 违约责任

双方约定，当出现发生不可抗力的情形，致使本合同的履行成为不必要或

不可能的，可以解除本合同。

若非不可抗力原因，违反本合同约定，违约方应当按照《中华人民共和国合同法》有关条款的规定承担违约责任：

1、违反本合同第三条约定，甲方应承担以下违约责任：甲方除继续履行合同外，还应支付违约金，违约金额上限为合同总额的 10%；

2、违反本合同第一条约定，乙方应承担以下违约责任：乙方除继续履行合同外，还应支付违约金，违约金额上限为合同总费用金额的 10%；

**乙方需按照项目建设标准完成工作，标准详见附件 1**

3、违反本合同其它条款，违约方应支付合理数额的违约金，违约金不超过合同规定的总金额；

4、如果进度延误，每逾期一天，乙方需向甲方支付合同总额的 0.05%作为逾期损害赔偿；逾期 30 天的，甲方有权单方面解除合同，并由乙方承担相应损失。

**第七条** 双方因履行本合同而发生的争议，应协商、调解解决。协商、调解不成的，任何一方可向广州市白云区人民法院提起诉讼。

**第八条** 本合同一式 捌 份，甲方执 伍 份，乙方执 叁 份，具有同等法律效力。

**第九条** 本合同经双方签字并盖章后生效。

（本页为盖章页，无正文）

甲方：广州白云国际机场股份有限公司（盖章）

法定或委托代理人：_____（签名或盖章）

年　　月　　日

乙方：_____（盖章）

法定或委托代理人：_____（签名或盖章）

年　　月　　日

# 第四部分

# 项目报价文件格式

**附录 1**

附录 1-1

# 报 价 函

项目名称：白云机场信息安全态势感知通报预警平台建设项目

致: 广州白云国际机场股份有限公司

根据贵方为白云机场信息安全态势感知通报预警平台建设项目采购采购的采购邀请函，作为经供应商正式授权代表供应商_____(供应商名称和地址)的报价文件书签名方代表_____ _____(签名人全名, 职务), 在此提交项目报价文件, 正本一份, 副本四份。

签字人代表以此函申明并同意:

1) 对随附报价表所规定的服务内容的总价为含税价人民币_____元（大写：_____元）。
2) 供应商将承担按照采购文件的所有条款履行合同的责任和义务。
3) 供应商已详尽研究了所有采购文件包括修正文(如果有), 所有已提供的参考资料以及有关附件并完全明白, 供应商必须放弃在此方面提出含糊意见或误解的一切权力。
4) 供应商之报价文件有效期为自报价之日起90个日历日。
5) 供应商同意按照采购人可能提出的要求提供与其所递交报价文件有关的任何其它数据或信息。
6) 我方理解贵方不一定接受最低报价或任何贵方可能收到的报价文件。

本报价文件连同贵方成交通知书应构成对双方均有约束力的合同, 直至正式合同编制完毕并生效。

供应商名称：（公章） _____

供应商地址： _____

授权代表姓名、职务（印刷体）：_____

法定代表人或授权代表签名：_____

公章：_____

日期：_____

附录2

附录2-1

# 报价明细表

| 序号 | 平台配置清单 | 总价(含税价) | 税率（%） | 备注 |
|---|---|---|---|---|
| 1 | 日志采集与分析引擎(含软件) | | | |
| 2 | 未知威胁分析引擎(含软件) | | | |
| 3 | 全流量分析引擎(含软件) | | | |
| 4 | 态势感知通报预警平台(含软件) | | | |
| 5 | 安全文明施工费 | | | |
| 6 | 规费 | | | |
| 7 | 税费（1—6 项累计×9%） | | | |
| 合计 | | | | |

供应商名称：（公章） _____

授权代表姓名、职务（印刷体）：_____

法定代表人或授权代表签名：_____

公章：_____

日期：_____

## 附录 3 诚信承诺函及企业声明

附录3-1

# 诚信承诺函

致：广州白云国际机场股份有限公司（采购单位名称或采购代理机构）

我司承诺我司（包括独立法人及关联公司和自然人）不存在白云机场信息安全态势感知通报预警平台建设项目合格供应商资格条件第 4、5、6 条所述情形，如有造假行为，我公司愿意无条件接受采购人的以下处理：

1.取消本项目报价、成交资格，并在相关网站公示；

2.由采购人没收合同履约保证金；

3.三年至六年内停止或禁止参加广州白云国际机场股份有限公司及其下属单位的所有非招标采购项目采购活动；

4.对不良行为予以纪录，并进行公告；

5.报广东省机场管理集团有限公司备案；

6.其他行政处理决定。

供应商名称：（公章） _____

授权代表姓名、职务（印刷体）：_____

法定代表人或授权代表签名：_____

公章：_____

日期：_____

附录3-2

# 企业声明

致：广州白云国际机场股份有限公司

我公司就参加白云机场信息安全态势感知通报预警平台建设项目，作出郑重声明：

在项目采购、实施、运行过程中严格遵守白云机场相关管理规定。承诺如违反，将自愿接受：通报批评，记录不良行为，列入黑名单，停止广州白云国际机场股份有限公司及其下属单位的所有非招标采购项目采购活动。

特此声明！

供应商名称：（公章） _____

授权代表姓名、职务（印刷体）：_____

法定代表人或授权代表签名：_____

公章：_____

日期：_____

**附录 4**

附录4-1

# 法定代表人证明书

_____现任我单位_____职务，为法定代表人，特此证明。

有效期限：_____签发日期：_____

附：法定代表人性别：_____年龄：_____身份证号码：

注册号码：_____ 企业类型：_____

经营范围：

_____

_____

_____

_____

_____

单位：（盖公章）_____

日期:　　年　　月　　日

附录4-2

# 法人授权书

致：广州白云国际机场股份有限公司

本授权书宣告：（报价人名称）　（职务）　（法定代表人姓名）是本单位的法定代表人，授权（职务）　（姓名）为我单位代理人，该代理人有权在白云机场信息安全态势感知通报预警平台建设项目的报价活动中，以我单位的名义签署报价文件，与采购人协商、签订合同协议书以及执行一切与此有关的事项。

报价人：（盖公章）_____

法定代表人：（签字）_____

被授权人（代理人）：（签字）_____

日期：　年　月　日

## 附录 5

附录5-1

# 项目组人员

报价人应列出拟在本项目中任职的主要管理人员和专业人员的安排，应包括项目负责人，实施人员、投入本项目的其他人员等，详见如下表格（各表格可按报价人的情况扩展与扩充）：

**本项目主要管理与技术人员安排（表一）**

| 序号 | 职务 | 姓名 | 年龄 | 性别 | 职称 | 专业 | 主要资历简述 |
|---|---|---|---|---|---|---|---|
| 1 | 项目负责人 | | | | | | |
| 2 | ……项目实施人员 | | | | | | |
| 3 | 其它主要人员（*）<br>…… | | | | | | |
| | | | | | | | |

*指除表中提到的人员外，报价人认为有必要加入的其他方面的本项目主要管理与技术人员。

**主要人员简历与经验（表二）**

（至少列写 4 人）

| 姓名 | | 性别 | | 年龄 | | 职务职称 | |
|---|---|---|---|---|---|---|---|
| 时 间 | 简历与经验简述 | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**注：项目负责人及专业负责人业绩须提供证明材料。**

附录 6

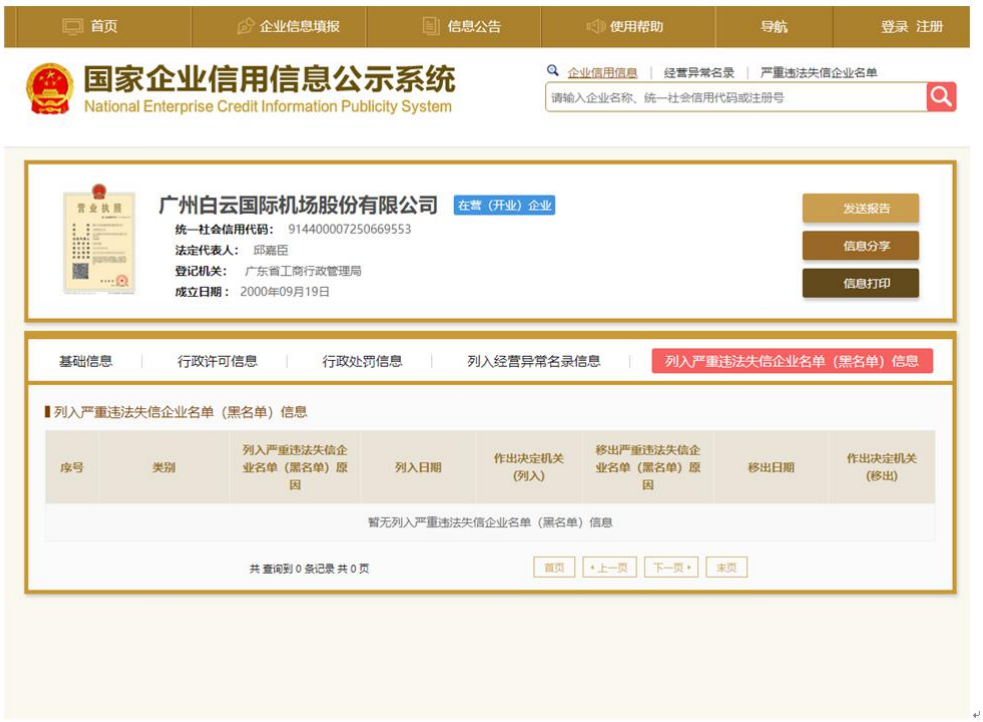
# 报价人的类似业绩

| 项目 | 服务内容 | 完工时间 | 合同价 | 备注 |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

注：1.近 3 年内是指： 2016 年 1 月 1 日至今（以合同签订日期为准）。

附录 8

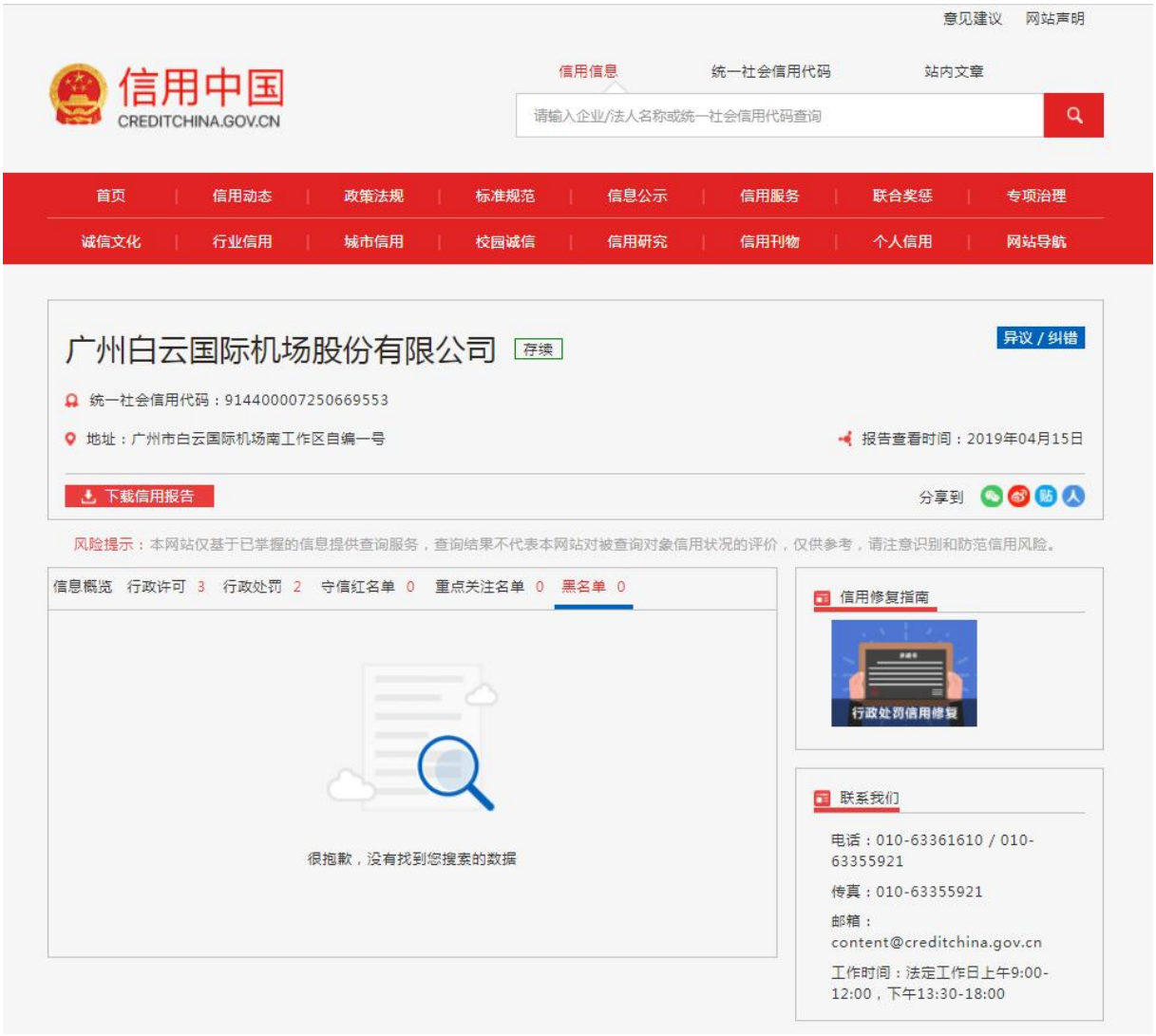
# 国家企业信用信息公式系统网站（www.gsxt.gov.cn）截图格式要求




注：报价人须按上述格式要求截图并加盖公章，截图清晰显示报价人单位名称及列入严重违法失信企业名单（黑名单）信息，否则将被认定为无效报价文件。

附录 9

# “信用中国”网站（www.creditchina.gov.cn）截图格式要求




注：报价人须按上述格式要求截图并加盖公章，截图清晰显示报价人单位名称及列入黑名单信息，否则将被认定为无效报价文件。

附录 10

# 资格审查和报价文件有效性审查表

项目名称：

| 序号 | 报价人名称<br>审查项目 | | | |
|---|---|---|---|---|
| 1 | 报价人必须为具备本项目履约能力的在中华人民共和国境内注册的独立的企业法人，同时持有登记机关颁发的营业执照，并提供加盖公章的营业执照的复印件。 | | | |
| 2 | 报价人具有增值税一般纳税人资格（需提供相应证明文件并加盖公章） | | | |
| 3 | 广东省机场管理集团有限公司采购、招商管理网络平台合作商登记表并加盖公章 | | | |
| 4 | 2016 年 1 月 1 日至今，报价人没有因腐败或欺诈行为而被政府或业主宣布取消报价资格；同时，2016 年 1 月 1 日年至今报价人（包括其关联公司）与采购人无发生各种诉讼、仲裁和不良投诉。（须就此项内容提供承诺函并加盖报价人公章）。 | | | |
| 5 | 报价人不得被列为“黑名单”，以“信用中国”网站（www.creditchina.gov.cn）查询为准，报价人需在采购公告发布后从“信用中国”网站下载信用评估报告并加盖公章。 | | | |
| 6 | 报价人不得被列为严重违法失信企业名单（黑名单），以“国家企业信用信息公示系统”网站（ww.gsxt.gov.cn）查询为准，报价人需在采购公告发布后从“国家企业信用信息公示系统”网站截图并加盖公章。 | | | |
| 7 | 报价人须提供由国家信息中心网络安全部提供的硬盘数据恢复服务，并提供授权书及售后服务承诺函。 | | | |
| 8 | 报价人需提供 ISO9001 质量管理体系认证证书，并提供证书的复印件加盖公章 | | | |
| 9 | 报价人需提供中国信息安全认证中心颁发的信息安全服务资质（信息系统安全集成三级及以上）或中国信息安全测评中心颁发的信息安全服务资质（安全工程类一级及以上），并提供证书的复印件加盖公章 | | | |
| 10 | 法定代表人证明书及法人授权书 | | | |
| 11 | 报价函有法定代表人或授权代表签字且加盖公章； | | | |
| 12 | 报价表有法定代表人或授权代表签字且加盖公章； | | | |

| | | | | |
|---|---|---|---|---|
| 13 | 报价有效期符合采购文件规定（90 个日历日）； | | | |
| 14 | 报价没有超过最高限价； | | | |
| 结论 | 是否通过并进入下一阶段评审 | | | |

注：1.每一项目符合的打“〇”，不符合的打“×”，并在备注中说明理由。出现一个“×”的结论为“不通过”。

2.表中全部条件满足为“符合”的结论为“通过”，同意进入下一阶段评审。

3.若专家意见不一致时，则按少数服从多数的原则决定该报价人是否通过资格及有效性审查，进入下一阶段评审。

4.结论一栏应写“通过”“不通过”。

# 第五部分

# 用户需求书

一、项目概况

广州白云国际机场股份有限公司（以下简称“股份公司”）网络分为三张大网（包括生产网、园区网、WIFI 网），各张网络在安全技术、安全管理方面采用了一定的措施，基本实现了网络信息安全的安全运行。但随着互联网、物联网、移动互联网技术的不断发展，以及等保即将进入 2.0 时代，股份公司目前的网络安全的形势也不容乐观。

网络层面：三张网络安全域分布广、网络复杂，系统数量庞大，各资产（网络安全设备和业务系统）游离于统一安全监管之外。各类安全设备也相互独立各自为战，缺乏综合分析和立体防护能力，进而形成一座座信息安全数据孤岛，难以实现统一分析发现高隐蔽性威胁。

防护层面：各张网络仅在边界做基础防护，各个安全域内部缺乏完善的安全防护体系，存在内部安全监测和安全审计等盲区。

监控与运维层面：各类资产使用情况难以智能检测资源使用状况，资源监控目前依赖 IT 运维服务公司——信息公司建设的 zabbix 网管系统，往往需事先设定的阈值才能告警，不能智能识别资源不足带来的潜在性风险。

态势分析层面：缺乏相关的态势分析手段对股份公司及下属各单位的安全态势进行感知，错失一些前期防范的机会。对于新型攻击、复杂隐藏攻击，以及非普遍性的资源使用问题更是难以发现：每次发现安全事件后，只能通过各独立的设备或系统单独分析，运维人员较难快速准确输出相关解决方案。

因此，为提升股份公司及下属各单位的信息安全态势分析能力，实现编制信息安全的“晴雨表”来分析目前和预测未来的安全状况，同时通过态势感知通报预警平台进行股份公司运行管理制度的落地，有必要对股份公司的安全和运维体系进行升级改造。

二、项目建设目标

按照一体化、标准化、智能化、可视化的要求建设态势感知通报预警平台，完善股份公司及下属各单位网络安全信息采集及分析基础设施，实现：

- 信息安全方面：实现股份公司把目前分散的安全防护体系进行集中统一，预测网络安全态势，对发现问题实现通报预警闭环。其中包括：
  - 大屏直观展示威胁相关的影响范围、攻击路径、目的、手段，对网络安全的态势感知跟踪分析，全面掌握安全态势、威胁、风险和隐患；

➢ 形成股份公司及下属各单位协调联动的网络安全监测预警处置工作机制，构建以网络安全综合防控体系，推动网络社会综合治理向深层次发展，整体提升股份公司及下属各单位网络安全防护水平。

➢ 有效的业务指导以及技术支撑，提供快速有效的应急防护体系，准确发现网络安全事件线索，及时通报预警重大网络安全威胁，并在紧急情况下实施高效应急防护；

➢ 将依托拟将建设的情报体系，从而为股份公司及下属各单位后续针对信息安全事件的调查工作提供有力的技术支撑，从而提升股份公司及下属各单位网络安全的监控能力、威胁管理和应急响应能力。

● 运行管理方面：实现股份公司资产运行维护状态态势预测与管理制度落地。

➢ 第一时间发现问题。无论是资源使用异常还是其他各种可能导致故障的情况，做到提前预警，最大限度地防止故障情况的发生；

➢ 第一时间通知人员。平台通过短信、邮件、工单等方式，将实时通知运维人员将故障时间进行快速处理，并提供相应的应急处理解决方案；

第一时间处理问题。平台提供各种监测数据，提供资产管理和自动巡检，协助服务运维方快速诊断故障根源，对运维结果进行评价。

三、项目建设内容：

本次项目设备采购及系统集成包括广州白云国际机场股份公司态势感知通报预警平台采购项目所需硬件设备和系统软件。态势感知通报预警平台，将围绕开展以下内容：

● 信息安全方面：对股份公司及下属各单位分散的业务系统进行实时流量和日志监测，填补安全监测盲区，及时发现网络安全隐患，并对网络攻击进行溯源。需推送网络安全隐患和网络安全预警信息，从事件发现与核查、信息通报、事件溯源及通报处置等形成闭环流程。需补充第三方的安全情报信息，对本地发现的安全事件进行碰撞，提高事件发现的精准度。

**信息安全工作开展将围绕网络核心流量监测和重要资产日志分析。**

● 运行管理：对股份公司的资产资源使用状况进行智能监测，并通过平台辅助服务运维方做到故障预警通知、应急事件处置、资产管理存档、运行维护情况分析评估。并需通过平台实现科学详细的电子化考核，提升服务运维方的服务质量。

**运行管理工作开展将围绕重要资产日志分析和单位管理制度进行分析。**

以下，将从生产网（含 T1 生产网和 T2 生产网）、园区网和 WIFI 网（T1 WIFI 网和 T2 WIFI 网）等区域从网络流量、资产日志进行分析本次项目的工作量。

# 采购清单

| 序号 | 设备名称 | 硬件要求 | 功能要求 | 单位 | 数量 |
|---|---|---|---|---|---|
| 1 | 态势感知通报预警平台 | **基础硬件要求：**<br>2U 机架式，不少于 2 物理 CPU，内存≥256GB，硬盘≥4TB*12，≥4 个千兆电口<br>性能情况要求：<br>支持≥800 个日志源资产<br>支持≥5Gbps 的镜像流量 | 提供白云机场生产网（含 T1 生产网和 T2 生产网）、园区网和 WIFI 网（T1 WIFI 网和 T2 WIFI 网）网络安全态势监控界面和运行管理手段：<br>1） 能够提供大规模数据存储、高压缩比及快速检索能力、追溯取证能力以满足企业合规要求。智能分析与防护设备形成安全联动能力。对深度机器学习技术提高数据挖掘能力，为股份公司安全提供决策依据、提高信息安全的纵深防御能力。<br>2） 能结合股份公司现有管理制度进行落地。 | 台 | 2 |
| 2 | 日志采集与分析引擎 | **基础硬件要求：**<br>≥4 个电口，1 个 console 口，内存≥128GB，磁盘≥4T*8 raid5，EPS≥10000/秒，<br>授权要求：<br>支持不少于 800 个日志源 | 实现白云机场生产网（含 T1 生产网和 T2 生产网）、园区网和 WIFI 网（T1 WIFI 网和 T2 WIFI 网）信息资产（含网络安全设备、重要业务系统）的日志采集分析，并通过预置的解析规则实现日志的解析、过滤及聚合，同时可将收集的日志数据上传到态势感知通报预警平台进行二次挖掘分析，为安全威胁和运行管理态势感知、分析与关联、运行管理决策支撑提供更多数据源。 | 台 | 1 |
| 4 | 未知威胁分析引擎 | **基础硬件要求：**<br>吞吐率：网络层：10Gbps<br>应用层：4Gbps<br>千兆管理口*2<br>千兆业务口 RJ45 网口*4，千兆业务 SFP 光口*20，万兆 SFP 光口*2 | 可将白云机场生产网（含 T1 生产网和 T2 生产网）、园区网和 WIFI 网（T1 WIFI 网和 T2 WIFI 网）收集的异常流量数据（含文件、邮件、网页等）进行镜像收集，分析未知威胁，并上传到态势感知通报预警平台进行二次挖掘分析，为安全威胁和运行管理态势感知、分析与关联、运行管理决策支撑提供更多数据源。 | 台 | 1 |

| | | | | | |
|---|---|---|---|---|---|
| 5 | 全流量分析引擎 | **基础硬件要求：**<br>≥千兆 RJ45 网口*2(管理口*2)，≥千兆RJ45网口*4，≥千兆 SFP 网口*12，万兆 SFP 光口*2<br>冗余电源，吞吐量：5Gbps，新建连接数≥8 万/秒，并发连接数 ≥280 万 | 以流量分光或流量镜像方式收集白云机场生产网（含 T1 生产网和 T2 生产网）、园区网和 WIFI 网（T1 WIFI 网和 T2 WIFI 网）流量，做到全流量审计、威胁深度识别、协议解析、应用识别、数据分析、行为还原以及流量趋势分析，可将收集的异常流量数据上传到态势感知通报预警平台进行二次挖掘分析 | 台 | 2 |
| 6 | 安装调试服务 | 安装流量和日志探针，并收集白云机场生产网（含 T1 生产网和 T2 生产网）、园区网和 WIFI 网（T1 WIFI 网和 T2 WIFI 网）流量和日志结果对接 | | 项 | 1 |

# 详细产品参数

## 1. 态势感知平台技术指标

| 指标项 | 指标要求 |
|---|---|
| 产品形态 | 平台支持软硬件一体机，也支持软件形态部署，软件形态支持部署在物理机/虚拟机/云环境； |
| 配置与性能 | 共两台服务器，单台服务器配置：<br>1.内存≥256GB，配置企业级存储磁盘总容量≥48TB；<br>2.支持服务器横向平滑扩展，可以通过增加硬件服务器数量的方式增加平台集群的计算处理性能。 |
| 配置与性能 | 最大支持 800 个日志源收集授权，5Gbps 流量分析 |
| 数据类型 | 1. 支持通过多种类型的安全、泛安全类数据接入采集，应包括但不限于设备日志数据、流量数据、弱点漏洞数据、系统性能数据、威胁情报数据、资产人员数据；<br>2. 支持通过流量采集设备采集接入全流量数据，包含流量中的请求包和返回包等信息，并可在数据检索中体现包信息；<br>3. 支持接入文本格式、CVS 等格式的文件数据，可通过模板文件的填写导入实现资产数据的导入和管理；<br>4. 支持通过云端对接、本地导入或手动编辑的方式，接入威胁情 |

| | |
|---|---|
| | 报数据。 |
| 分析模型与指标管理 | 1. ▲平台应内置包括规则模型、关联模型、统计模型、情报模型、AI 模型等在内的≥5 大类安全分析模型，并支持用户方根据自身需要添加个性化模型规则（要求提供截图并加盖厂商公章）<br>2. ▲支持业务编排功能，能够支持数据源（含日志、事件和告警）、5 大类安全分析模型、处置响应（含联动阻断、通报、预警和人工查验），实现，实现安全编排和自动化响应（要求提供截图并加盖厂商公章） |
| AI 高级分析 | 1. ▲平台内置不少于 8 种机器学习分析场景模型，可检测发现勒索挖矿告警数异常、安全设备日志数异常、网络会话数异常、域名请求数异常等特定场景条件下的安全态势异常；（提供截图并加盖公章）<br>2. 支持时间序列、UEBA、Bayes、随机森林等长周期高级机器学习算法；<br>3. 支持自定义部署 AI 机器学习模型，允许用户选用的高级机器学习算法不少于 4 种，通过输入任意指标类数据进行模型训练，发现异常行为并生成安全事件与告警，辅助用户发现潜在的安全风险。 |
| 网络实体分析画像 | 1. ▲实现实体间网络互访关系的多级钻取，支持多重流量关联关系分析，支持通过端口、协议、异常访问类型过滤关联关系。（要求提供截图并加盖厂商公章） |
| 安全态势可视化 | 1. ▲以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测等多个维度进行可视化展示，提供不少于 11 块大屏展示界面，内容包括但不限于外部攻击态势、横向威胁感知、资产失陷态势、web 业务系统态势、数据中心态势、AI 异常分析、资产态势感知、攻击者追踪溯源、资产追踪溯源和平台运行状态监测等（要求提供截图并加盖厂商公章）。<br>2. 可视化视角覆盖云管端、边界、应用、安全设备等监测维度≥6 种；<br>3. 支持外部对内部攻击、内部跨安全域横向攻击、内部外连攻击 3 种威胁方向监测 |
| 智能检索 | 1. 支持对原始日志数据、安全告警数据进行分类检索，从检索结果可关联威胁情报和资产信息并一键跳转；<br>2. 支持检索结果导出（不少于 10000 条），导出内容字段可自定义选择，支持 excel 或 CSV 格式 |
| 威胁情报 | 1. ▲支持通过离线导入或手动编辑添加的方式，形成本地威胁情报，允许用户自建行业情报库，并实现情报库的增删改查、导入、导出功能（要求提供截图并加盖厂商公章）；<br>2. 支持统计情报源碰撞命中情报数量，针对任意单条无效情报可实现禁用；<br>3. 提供攻击主机、僵尸网络、病毒木马、恶意软件、APT 情报、恶意邮件等情报的活跃时间、可信度、家族分类，可应用于本产品的实时分析；<br>4. 设备支持在线查询与溯源：云端提供对 IoC 威胁类型、多源情报、WHOIS、开放端口、SSL 证书等多维度的溯源分析；<br>5. 云端服务：支持订阅高级威胁分析情报，云端提供最新 APT 入侵、0day 漏洞预警、病毒变种情况等分析报告订阅。 |
| 数据字典管理 | 1. ▲支持管理系统中原始日志、安全事件、安全告警的所有字段和取值，每个字段均有清晰的说明；（要求提供截图并加盖厂商公章） |

| | |
|---|---|
| | 2. 支持数据标准管理，用户可以根据实际需求，对字典进行编辑，支持手动修改、增加或删除相应的字段。 |
| 资产管理 | 1. ▲支持通过流量无侵入式自动发现资产，支持发现终端、Web 服务器、DNS 服务器、邮件服务器、FTP 文件服务器等类型≥5 种（要求提供截图并加盖厂商公章）；<br>2. 支持资产信息的全量导入导出，支持从资产管理平台同步资产；<br>3. ▲支持在资产管理页面提供资产威胁溯源大屏的跳转按钮，方便快速展示所关注的资产安全态势。（要求提供截图并加盖厂商公章）； |
| 业务拓扑监控 | 1. 支持拓扑图的增加、修改、删除、导入、导出，支持创建>50 个业务或网络拓扑，支持建立平面拓扑和 3D 拓扑。<br>2. ▲安全拓扑图支持监控安全域、Web 业务系统、服务器、终端、安全设备等至少 5 种网络实体类型（提供截图并加盖公章）；<br>3. 支持通过拓扑中各个节点的安全态势状况进行计算，对拓扑所对应的业务系统进行整体健康程度的详细量化评判。 |
| 工作台 | 1. 支持统一的安全运营工作台，在工作台可以集中查看当前用户的待办工单、最新通报预警状态<br>2. ▲支持工单举证信息一键溯源，工单处置人员可以直接定位到工单关联的原始信息进行查看（要求提供截图并加盖厂商公章）；<br>3. 支持通过安全告警自动派发工单到对应的安全管理员，支持自定义编辑预警信息内容；<br>4. 支持将预警信息直接转为内部通报，支持将通报内容作为工单定向指派。 |
| 分析报告 | 1. ▲支持用户自定义编辑报告模板，根据实际的业务需求自定义统计分析的指标对象，生成有针对性的分析报告，安全分析中的所有字段内容，都可以作为报告的统计对象，并自定义时间范围实现报告导出（要求提供截图并加盖厂商公章） |
| 黑白名单 | 1. 支持通过黑白名单功能对分析对象进行过滤筛选；<br>2. 支持通过任意字段进行组合，配置筛选条件并生成黑白名单过滤规则，支持规则数≥100 条 |
| 运维监控 | 1. 支持大数据平台本身的计算、存储资源利用率监控；<br>2. 支持数据集与数据索引健康度监控；<br>3. 支持对平台各组件运行健康状态的集中监控 |
| 产品资质 | 1. 产品具有公安部网络安全保卫局颁发的销售许可证；<br>2. 产品具有 IPv6 Ready Logo 认证 |

## 2.日志采集探针技术指标

| 指标项 | 指标要求 |
|---|---|
| 工作模式 | 独立完成审计日志采集，不依赖于设备或系统自身的日志系统；<br>审计工作不影响被审计对象的性能、稳定性或日常管理流程；<br>审计结果存储于独立存储空间；<br>自身用户管理与设备或主机的管理、使用、权限无关联；<br>提供全中文 WEB 管理界面，无需安装任意客户端软件或插件 |
| 硬件规格 | 不少于 4 个电口，1 个 console 口，内存≥128GB，磁盘≥4T*8 raid5，EPS |

| | |
|---|---|
| | ≥10000/秒（峰值：14000/秒），双电源 |
| 处理性能 | 支持审计 800 个日志源； |
| 集成 CF 卡 | ▲产品硬件集成 CF 卡，产品操作系统安装在 CF 卡中，软件安装在硬盘中，提供国家权威检测机构（公安部或国家保密科技测评中心）检测报告证明并加盖原厂公章 |
| 功能扩展 | 采用解决方案包上传对产品进行功能扩展，无需要代码开发。 |
| 日志收集 | 支持 Syslog、SNMP Trap、OPSec、FTP 协议日志收集<br>支持使用代理(Agent)方式提取日志并收集；<br>支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等；<br>▲支持至少 90 种品牌 1300 种不同型号的资产日志收集，需列出支持的资产品牌和对应型号详细清单。<br>▲支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等，提供产品功能截图并加盖原厂公章 |
| 日志分析 | 可以以日志等级进行过滤；<br>应该可以通过自定义配置将用户不关心的日志过滤掉；<br>支持对收集到的重复的日志进行自动的聚合归并，减少日志量；<br>支持可由用户定义和修改的日志的聚合归并逻辑规则；<br>支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备；<br>支持对收集到的日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展。<br>可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息（公网情况）<br>▲具备安全评估模型，评估模型基于设备故障、认证登陆、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件，提供产品功能截图并加盖原厂公章<br>▲内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针对等 5 大类 50 子类的安全分析场景，提供产品功能截图并加盖原厂公章<br>支持基于内存的实时关联分析，跨设备的多事件关联分析；<br>支持自定义条件的事件进行聚合；<br>进行关联分析的规则可定制；<br>▲支持三维关联分析，包括支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件，提供产品功能截图，加盖原厂公章原件，并提供国家权威检测机构（公安部或国家保密科技测评中心）检测报告证明 |
| 日志备份 | ▲支持日志备份、清理、归档、恢复、下载等操作，确保日志的可靠存储和系统的稳定运行，提供产品功能截图并加盖原厂公章 |
| 日志查询 | 支持 B/S 模式管理，支持 SSL 加密模式访问；<br>支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、 |

| | |
|---|---|
| | 攻击类型、地理城市等参数进行过滤查询；<br>支持用任意关键字对所有事件进行高性能全文检索<br>支持可指定多个查询条件进行组合查询<br>支持将查询的条件存储为查询模版，方便再次使用<br>极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。 |
| 应用性能监控（APM） | 支持如下应用的性能监控（Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris）、数据库（mysql、oracle）、应用服务器（weblogic、tomcat）、web 服务器（apache）。<br>支持应用性能历史详情回溯查看<br>支持如下性能监控参数<br>▪ 支持监控 Windows 操作系统如下参数：cpu 使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数；<br>▪ 支持监控 Linux 操作系统如下参数：一分钟系统负载、5 分钟系统负载、15 分钟系统负载、cpu 使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数<br>▪ 支持监控 Mysql 如下参数：查询缓存命中率、键缓存命中率、立即获得锁数、连接数、线程数、每秒 SQL 查询数、每秒发送字节、每秒接收字节；<br>▪ 支持监控 Oracle 如下参数：库缓存命中率、内存排序比率、词典缓存命中率、SGA 数据缓存命中率、重做日志缓存命中率；<br>▪ 支持监控 Apache 如下参数：总访问数、写日志次数、每秒发送字节数、长连接数、关闭连接数、空闲活动数、查询 DNS 数、正在发送数、请求完成数、负载、等待连接数、总数据量、读操作数、工作线程数、空闲线程数、CPU 占用率<br>▪ 支持监控应用服务器（tomcat、weblogic）如下参数：活动线程数、堆内存（已用）、守护线程数； |
| 脆弱性管理 | 支持从 IBM Rational AppScan 导入资产弱点漏洞信息<br>支持从 Web 应用监测工具导入网站弱点漏洞信息<br>支持从数据库弱点扫描器导入数据库弱点漏洞信息<br>支持从 NetSparker Web 应用扫描器导入网站弱点漏洞信息<br>支持从 Nessus 网络扫描器导入网络弱点漏洞信息<br>支持从 OpenVAS 扫描器导入弱点漏洞信息<br>内置 73000+条 CVE 漏洞数据知识库<br>内置数十项符合 OWASP 的 Web 漏洞数据知识库 |
| 地理安全系统 | 内置 GeoSec 地理安全子系统，内置世界以及中国安全 GIS 地图<br>支持用地理地图展示来源威胁的趋势<br>支持用地理地图展示目的威胁的趋势<br>支持在地理地图上标注威胁事件的发生分布<br>内置 IP 地址到经纬度的转换库<br>支持以地理信息类进行统计的数据报表<br>支持切换 Google 地图 |
| 告警功能 | 可预设置安全告警策略； |

| | |
|---|---|
| | 支持数据阀值设置，超过阀值将产生告警;<br>可以通过邮件、短信和屏幕显示进行告警;<br>支持自动防止报警信息在短时间内大量发送(告警抑制);<br>具备报警合并和在一个时间段内抑制报警次数的能力。 |
| 综合查询及报表管理 | 内置合规性报表 1000+种;<br>内置 SOX、ISO27001、WEB 安全等解决方案包<br>内置完善的等级保护合规报表<br>内置综合性自动化审计报告<br>支持用户自定义报表;<br>自定义的报表支持多个统计维度的数据集合。<br>支持报表导出为 PDF 和 Word 格式文件。 |
| 用户管理 | 根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容;日志员只负责完成对系统本身的用户操作日志管理。<br>系统自带自身管理日志<br>▲注册用户资产时，提供自动发现识别能力，提供产品功能截图并加盖原厂公章。<br>▲提供一键式故障排除功能，提供产品功能截图并加盖原厂公章。<br>提供自助式的升级接口，支持对产品升级、规则升级。 |
| 产品资质（需提供相关证明材料并加盖原厂公章） | 产品获得公安部颁发的《计算机信息系统安全专用产品 销售许可证》 |
| | 产品获得公安部出具检验检测报告，须符合“信息安全技术 日志分析产品安全技术要求 GA/T 911-2010（第三级）”; |
| | 产品获得国家保密科技测评中心颁发的《涉密信息系统产品检测证书》，需符合国家保密标准 BMB15-2011; |
| | 产品获得中国信息安全认证中心颁发的《IT 产品信息安全认证证书》，需符合 ISCCC-TR-056-2016《日志采集与分析产品安全技术要求》 |
| | 产品获得 IPv6 Ready Logo 认证 |
| | ▲产品获得 IDC 或 CCID 赛迪顾问 2018 年“中国日志审计产品市场”排名位居中国日志审计产品市场前三名 |

## 3.未知威胁检测探针技术指标

| 指标项 | 指标要求 |
|---|---|
| 硬件外形 | 软硬一体化 2U 标准机架式设备; |
| 电源 | 冗余电源; |
| 硬盘容量 | 2T*2，带 RAID1 |
| 接口数量 | 管理口：Consle*1,USB*2,千兆 RJ45 网口*2<br>业务口：千兆 RJ45 网口*4 千兆 SFP 光口*20 万兆 SFP 光口*2 |
| 部署方式 | 旁路镜像模式部署，不影响服务器处理性能和网络架构; |

| | |
|---|---|
| 分布式部署 | ▲支持旁路部署和分布式部署，对探测器可以添加、删除，显示探测器版本、状态和 IP，管理中心可实现告警统一管理；可自定义管理中心和探测器之间的数据传输速率、时间、发送目录等参数，提供产品功能截图并加盖原厂公章 |
| 吞吐率 | 吞吐量：不低于 10Gbps |
| WEB 检测 | 20 万/秒 |
| 邮件检测 | 300 万封/24 小时 |
| 文件检测 | 10 万/24 小时 |
| 全流量检测 | 支持全流量检测，可根据需求打开或关闭全流量检测功能 |
| 审计协议 | ▲加密协议解析需要导入服务器私钥证书，并提供审计协议类型的端口号配置，可根据需要变更端口号；支持 LDAP 登录行为识别；支持 VXLAN 镜像流量解析检测，提供产品功能截图并加盖原厂公章 |
| 检测风险类别 | 支持检测 WEB 攻击、异常访问、恶意文件攻击、远程控制、WEB 后门访问、发件人欺骗、邮件头欺骗、邮件钓鱼、邮件恶意链接、DGA 域名请求、SMB 远程溢出攻击、WEB 行为分析、隐蔽信道通信、暴力破解（包括 SSH、TELNET、RDP、FTP 暴力破解）、挖矿等风险 |
| 告警黑白名单过滤 | ▲支持对文件白名单、发件人邮箱白名单、发件人域名白名单、黑域名白名单、黑 IP 白名单、域名白名单、客户端 IP 白名单、服务端 IP 白名单、WEB 风险特征白名单进行设置，提供产品功能截图并加盖原厂公章 |
| 私网 IP 地理位置定义 | ▲支持对私网地址 IP 地理位置信息添加，在产生告警时，定义 IP 可正常显示所属地理位置信息，提供产品功能截图并加盖原厂公章 |
| 弱口令风险检测 | ▲支持对 FTP、POP3、SMTP、IMAP 等协议进行弱口令检测，提供产品功能截图并加盖原厂公章 |
| 告警详细展现 | 可支持详细展现告警级别、时间、威胁名称、状态、客户端 IP、客户端 IP 所在地理位置、服务端 IP、服务端 IP 所在地理位置、报文、操作等信息，包含请求 URL、请求类型、请求内容、请求头、Host、User-Agent、Accept、Accept-Language、Accept-Encoding、Accept-Charset、Keep-Alive、Connection、Cookie、请求参数、响应码、返回长度等信息 |
| 主机威胁分析 | 可自动对内网主机进行威胁指数分析，详细展示具体的威胁指数、威胁活动、历史威胁指数、遭受的攻击类型、攻击次数、攻击状态等 |
| | 可根据不同威胁指数的主机实现攻击溯源和攻击过程的可视化分析 |
| | 可通过攻击源、攻击目的对攻击路线进行统计，包括攻击的行为、告警，并以直观的图形化形式展示 |
| 木马回连分析 | 可自动学习网络流量中包含的各种可疑 C&C IP/URL，包含各种可能对内网存在影响的 IP 和域名 |
| | 快速识别网络中存在的恶意回连行为，包含回连主机 IP、服务器 IP、时间、行为等 |
| | 对基于木马回连的非法数据传输等行为进行取证分析，包括回连主机 IP、服务器 IP、传输数据大小、协议类型等 |
| 攻击地图展示 | 可通过攻击源和目的的地理位置信息，以世界地图和中国地图的形式展示，并实现世界地图和中国地图自动切换直观展示攻击路径 |

| | |
|---|---|
| 协议解析 | 支持 HTTP、HTTPS（需要导入服务器私钥证书）协议解析，检测 WEB 攻击 |
| 双向审计 | 支持双向审计，对请求和响应都进行审计 |
| 攻击检测 | 支持 SQL 注入、命令注入、跨站脚本、代码注入、协议错误攻击检测 |
| WEBSHELL 检测 | 支持 WEBSHELL 检测,可检测访问 webshell 的行为,包含具体对应的 URL、返回码、返回数据包内容等，可显示一句话类 webshell 后门是否植入成功 |
| 动态分析 | 自动关联行为分析的详细展现，包含 SQL 注入取数据、表单破解、XSS 测试、目录穿越读取文件、多人访问 Webshell、APT 攻击等 |
| 场景化分析 | 支持场景化的分析能力，对发现的告警进行二次关联，支持对勒索病毒、网站后门、邮件 APT 攻击等事件进行预警。 |
| DNS 协议分析 | 具备 DNS 协议分析能力，发现受感染主机、危害程度、被感染病毒类型、回连 C&C 域名、DNS 返回详情、恶意主机明细等行为。 |
| 与 WAF 联动 | 支持将分析到的 WEBSHELL 攻击、木马回连和恶意攻击行为同步到 WAF，实现 APT 深度威胁分析与 WAF 联动阻断 |
| 解析协议 | 支持解析 webmail、SMTP、POP3、IMAP、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）类型报文 |
| Webmail 攻击检测 | 支持基于 webmail 攻击类型检测，包括 sql 注入、跨站、命令注入等攻击检测 |
| 社工类攻击检测 | 对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接 |
| 恶意附件检测 | 支持邮件恶意附件行为检测 |
| 解析协议 | 支持 HTTP、FTP、SMB、SMTP、POP3、IMAP、HTTPS、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）等协议传输文件检测 |
| 文件类型 | 支持 doc，xls，ppt，swf，pdf，java，rar，zip，rar，exe，vbs，scr，html，js 等多种文件解析 |
| 自定义文件类型 | 可添加或删除指定分离的文件类型，并可选择适用的协议类型（HTTP 可进一步按 GET、POST 来配置） |
| 特征检测 | 对文件进行特征匹配，利用已知的特征库发现恶意可以执行代码<br>对文件进行特征匹配，利用已知的特征库发现恶意的非可执行文件 |
| Shellcode 检测 | 通过分析文件中的二进制代码,找到文件溢出攻击的代码,并能找到 APT 攻击中的 0day 攻击 |
| 动态沙箱检测 | 对存在问题的文件输出完整的二进制动态分析报告<br>动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，分析其安全风险<br>对文件关键行为进行截图<br>可展示文件中版本信息、段信息、资源信息、导入表、字符串信息、删除文件信息等内容<br>可展示 ROP 行为检测<br>可展示具体文件的行为，包括所有的注册表行为、进程行为、互斥量等信息<br>可显示文件运行过程中企图访问的 IP、域名，以及域名及对应的 IP |

| | |
|---|---|
| 子文件扫描 | 对文件内部嵌入的子文件可进行二次扫描，分析安全性 |
| 攻击样本提取 | 可以提取出攻击的完整样本文件，并提供对该文件下载的能力 |
| 文件威胁指数 | 可展示威胁程度最高的文件样本 MD5、威胁指数、传播次数，病毒检测、静态检测和动态检测结果等内容 |
| | 根据文件传播情况分析受感染主机、接受云端威胁情报、关键威胁行为可视化、回连主机 host 和完整沙箱分析报告 |
| | 根据云端威胁情报展示云端是否确认、传播协议类型、传播次数、云端确认结果等 |
| 远程控制检测 | 支持根据威胁情报、DGA 域名请求、IDS 规则、用户配置数据，发现被远程控制的内部主机 |
| DGA 域名请求检测 | 具备 DNS 协议解析功能，发现发起 DGA 域名请求的失陷主机 |
| 挖矿行为检测 | 可发现利用失陷主机挖矿的行为 |
| 本地威胁情报 | 设备集成离线的高可用威胁情报库 ，支持离线环境下，根据威胁情报进行检测，增量威胁情报随策略升级包升级 |
| 云端威胁情报 | 支持自动从 APT 云端获取最新威胁情报 |
| 协同防御 | 支持将本地恶意文件攻击的病毒类型等信息上传到 APT 云端，提升协同防御能力 |
| 策略自动更新 | 支持自动从 APT 云端更新策略 |
| 紧急事件上传 | 支持紧急事件上传云端，帮助客户关注紧急事件 |
| 风险处理 | 支持根据需要对风险状态进行选择处理中、处理完成、延迟处理、拒绝处理等 |
| 一键登录排错 | ▲支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、H 表分区检查、表检测、同步验证、信息收集等功能，提供产品功能截图并加盖原厂公章 |
| 设备状态监控 | 支持对设备的 CPU、内存等状态进行监控，并在设备界面中进行展示 |
| 知识库 | 根据不同的风险信息，提供风险分析和处置建议知识库； |
| 告警与报表 | 告警可详细展示风险级别、发生时间、告警名称、客户端 IP、服务器 IP、报文内容（URL、请求头、请求参数、请求内容） |
| | 可根据需要针对单个告警添加白名单 |
| | 支持 kafka、短信、邮件、syslog、snmp、ftp 等告警方式 |
| | 支持对 kafka、syslog 发送的风险信息进行 AES 加密传输 |
| | 支持同时发送多人、单条发送、发送统计等高级告警功能，支持报表自动、批量发送 |
| | 报表能够支持 WORD、PDF 等格式导出； |

| | |
|---|---|
| 日志数据管理 | ▲审计数据保留策略应至少满足天数和百分比两个控制参数，支持 web 界面可配置，且恢复数据不影响正常的审计功能。对审计日志可自动备份并加密，必须导入设备才能进行恢复查看，并可自动释放磁盘空间，提供产品功能截图并加盖原厂公章 |
| 产品资质（需提供相关证明材料并加盖原厂公章） | 获得公安部颁发的《计算机信息系统安全专用产品销售许可证》（必须是“APT 安全监测产品”） |
| | 获得中国信息安全认证中心颁发的《中国国家信息安全产品认证证书（增强级）》，需符合 GB/T 20945-2013 要求 |
| | ▲提供证明具备国际领先水平的第三方权威机构检测报告（误报率低于 3%，无背景流量情况下检出率不低于 98%，有背景流量情况下检出率不低于 97%） |
| | 获得 IPv6 Ready Logo 认证 |

# 4.全流量采集探针技术指标

| 技术指标 | 技术要求 |
|---|---|
| 硬件规格 | 硬件外形：软硬一体化 2U 标准机架式设备<br>硬盘容量：2T,raid 1<br>接口数量：标配不少于千兆管理口*2，千兆业务口 RJ45 网口*4,千兆 SFP 网口*12，万兆 SFP 光口*2<br>吞吐量：不低于 5Gbps |
| 高可用性 | 部署方式：旁路镜像模式部署，不影响服务器处理性能和网络架构<br>分布式部署：支持分布式部署，管理中心可实现告警统一管理，添加和删除探测器<br>▲自定义配置：支持根据添加探测器情况，自定义探测器名称、发送时间、发送目录等信息，并可显示不同探测器的 IP、版本、状态和最近 24 小时的风险信息，提供产品功能截图并加盖原厂公章 |
| 审计功能 | 支持全流量审计，包含网络第 2-7 层数据流量<br>可选择特定协议或 IP 地址自定义检测，自定义 IP 地址访问监测，并详细记录所有的审计数据包，可展现审计数据包的时间、客户端 IP、服务端 IP、应用层协议、报文、返回码、详细信息等 |
| 协议解析能力 | 支持解析应用层协议不低于 100 多种，如 HTTP、SSL、FTP、SMTP、POP3、TFTP、TCP、UDP、NFS、SNMP、ICMP、RTMP、DNS、IRC、SMB 等<br>支持对应用层协议 HTTP/DNS/FTP/IMAP/POP3/SMTP/SMB/DNP3 等可做深层解析还原，并进行全审计<br>▲支持对 Modbus、IEC-104、DNP3、Ethernet/IP、S7 等工控协议流量的解析还原，提供产品功能截图并加盖原厂公章<br>支持对传输层 TCP/UDP、对应用层流量均可做统计分析 |
| 功能参数 | 文件审计：支持对指定时间周期内 HTTP、FTP、SMTP、IMAP、POP3 等协议传输的文件进行分离并审计，并可对文件进行本地化存储或者发送至其他文件分析平台<br>▲敏感信息识别：实现对关键字、数据来源等的自定义，通过内容深度匹配流量中的敏感信息，并对敏感信息快速定位，实现对敏感信息访问行为的有效监测，提供产品功能截图并加盖原厂公章<br>登录信息识别：识别网络中 WEB、QQ 等各种应用的登录行为，提取登录 IP、登录账户、登录网站域名等登录信息，提供产品功能截图并加盖原厂公章<br>弱口令检测：支持对 WEB 密码的弱密码校验，发现网站中存在弱密码风险， |

| | |
|---|---|
| | 避免信息泄露<br>加密流量解析：支持对 HTTPS 流量的解析还原<br>资产识别：支持对流量中资产进行识别，并进行统计分析，快速发现未登记资产<br>▲流量代理分析：处理和分析第三方接入流量，满足用户对其他平台流量无法分析溯源需求，提供产品功能截图并加盖原厂公章<br>威胁检测：支持流量异常行为检测，如网络蠕虫、木马、后门、僵尸、间谍软件、网络漏洞、网页漏洞、跨网站攻击、钓鱼邮件、暴力攻击、数据库注入攻击、ARP 欺骗、DoS 攻击等<br>支持基于智能语义分析的攻击检测模型，深度发现网络流量攻击行为<br>支持详细展现发现的威胁内容，包含时间、攻击源 IP、攻击目的 IP、网络层协议、应用层协议、规则描述、风险相关参照等信息<br>风险告警可详细展示风险级别、发生时间、告警名称、客户端 IP、服务器 IP、报文内容（URL、请求头、请求参数、请求内容）<br>本地离线情报：内置离线高可信威胁情报库，应用远控类型的情报指标（IOC，Indicator of Compromise）对僵尸主机和僵尸网络进行精准检测。高可信威胁情报库还可以通过云端实时更新，始终保持最新状态，准确发现并定位失陷主机 |
| 流量分析能力 | ▲IP 流量统计：支持对 IP 流量统计分析，可展现某 IP 在指定时间范围内的总流量、上下行流量大小及该 IP 下所有应用的总流量、上下行流量大小；应用会话流量统计分析，可展现某应用在指定时间范围内的总流量、上下行流量大小及该应用下所有 IP 的总流量、上下行流量大小，提供国家权威检测机构（公安部或国家保密科技测评中心）检测报告证明并加盖原厂公章 |
| | ▲应用层流量统计，统计各种的应用程序访问服务器的行为的流量，以折线图的形式展现，更清晰直观地展示出所选时间段内的流量趋势，每 5 分钟自动刷新；传输层流量统计，包括 tcp 流量、udp 流量、icmp 流量、其他 ip 流量、总流量的统计，采用折线图的形式展现，展现出所选时间段内的流量趋势，每 5 分钟，提供国家权威检测机构（公安部或国家保密科技测评中心）检测报告证明并加盖原厂公章 |
| 报表管理 | 支持 SYSLOG、FTP、KAFKA 等接口进行审计、风险等各种信息外送<br>报表能够支持 WORD、PDF、EXCEL 等格式导出 |
| 日志数据管理 | ▲审计数据保留策略应至少满足天数和百分比两个控制参数，且支持 web 界面可配置，且恢复数据不影响正常的审计功能，提供产品功能截图并加盖原厂公章<br>当磁盘空间达到一定的阀值，支持自动清理最早的数据释放空间 |
| 产品资质（需提供相关证明材料并加盖原厂公章） | 产品获得公安部颁发的《计算机信息系统安全专用产品 销售许可证》 |
| | 产品获得中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》 |

三、项目方案设计要求

技术方案书要求包括但不限于以下内容：

1.总述

对本项目的理解分析，以及背景、现状、设计目标和内容及需求（功能和性能）的理解等。

2.工作方案

1）项目总体工作思路

说明报价人展开本项目工作的思路，包括提出工作计划和项目管理方案（包括进度控制、质量保证、范围控制、配置管理、风险控制等），以安排保证进度、质量，并采取的相应措施及应对设计变更工作方式、方法等内容进行阐述。

2）整体工作计划

对项目整体工作进度安排、工作关键点、里程碑等进行阐述。工作计划须明确每位项目成员在项目实施每个阶段承担的具体工作。报价人必须承诺完全按照工作计划所列的技术服务人员配置和时间安排开展项目实施工作。

3）主要工作内容

对本项目中各项工作如何开展进行详细阐述。要求工作方式可行，能够切实落地。

4）风险与质量控制

对项目风险控制措施和质量保障措施进行阐述。

四、项目工期

项目总工期为三个月。

除去非驻场的文档编制工作，要求报价人技术服务人员驻白云机场现场工作服务时间不得少于 5 人/日。

五、服务团队要求

报价人必须保证从事本项目工作的相关人员具备完成合同规定的工作所需的资历和技能，并向甲方如实提供相关人员专业经验和水平的证明材料，以及其他的报价人认为有必要提供的资料。

六、安全保密要求

服务提供方须与招标人签署相关保密协议，同时要求提供服务方与其服务人员就本次服务签署的保密协议。

针对本服项目，要求服务人员的变动率不得超过 20%，确需变更应提前通知招标人并获得批准后方可进行。服务过程中所有原始资料和数据均须妥善保管，仅限在项目组内为本服务项目所用，不得以任何方式外泄或用于其它用途，服务人员须及时删除存储在电脑中或纸质的数据和文件材料。

七、服务能力要求

1.响应供应商所提供的合同所规定之设备应是全新的、未使用过的，其技术性能指标应符合设备制造商所规定之技术规格，所安装的软件应是正版软件。

2.响应供应商免费负责设备的安装调试；采购人负责提供设备安装调试的场地及条件。

3.响应供应商设立技术支持热线电话，提供每天 24 小时的电话技术支持服务。

4.提供承诺函，承诺设备安装调试完毕并经验收合格及交付采购人使用之日起计，提供设备免费保质保修期不少于原厂三年服务及三年免费软件版本升级服务，以满足质保期内产品版本和特征库保持最新的需求。设备质量保证期内，设备在正常使用情况下发生故障时，响应供应商应提供免费的维修服务或免费更换同型号设备，维修期间免费提供同型号备机保障正常应用。

5.设备发生故障需要更换部件时，在完成部件的更换且设备可正常运行时起计，所更换部件的质量保证期为三年。在部件质量保证期内，如所更换的部件发生故障，响应供应商应提供免费的维修服务，所产生的费用由响应供应商承担。

6.设备质量保证期内，设备发生故障时，在收到采购人的书面通知、电子邮件或电话通知时，响应供应商应在 4 小时内到达设备使用现场排除设备故障。响应供应商不能按时排除设备故障时，应提供备用设备给采购人以维持播出系统的正常运行。

7.设备质量保证期内的故障报修，如响应供应商未能做到上述的服务承诺时，采购人可采取必要的补救措施，但其风险和所产生的费用由响应供应商承担；采购人根据合同规定对响应供应商行使的其它权力不受影响。由于响应供应商的保证服务不到位，设备质量保证期到期时将顺延。

8.设备质量保证期内因采购人使用、管理不当所造成的设备故障，其损失由采购人承担，响应供应商有义务提供有偿服务。