教育部教育考试院
2026年网络攻击检测技术服务

第三章 技术需求书

教育部教育考试院

2026年6月

目 录

1. 项目概述

1.1 项目背景

教育部教育考试院（以下简称考试院）为了持续抵御日益复杂多变的高级网络攻击，保护考生隐私及考试数据安全，保护信息系统的正常稳定运行，考试院引入第三方专业的安全检测技术服务团队，依托考试院已部署的各类安全设备，通过全天候网络攻击检测，快速应急响应等防御措施，构建覆盖“风险预警－攻击防御－事件处置”的全生命周期安全能力，保障考试业务安全。

1.2 服务期限

本项目服务期为 1 年，自合同签订之日起执行。

1.3 服务地点

服务地点：考试院指定地点。

2. 服务范围

本项目主要是对采购人所涉及的中国教育考试网、海外考试报名信息系统、通用网上报名系统、中小学教师资格考试信息系统、国家教育考试管理与服务平台、综合办公平台等 30 余个业务系统、100 余个子系统，包括非信创数据中心业务和信创私有云业务流量。

3. 服务方式

本项目服务方式包括驻场服务、定期现场服务、远程服务等方式。

（1） 驻场服务：服务商按照采购人要求，在指定地点每日提供现场技术服务。

（2） 定期现场服务：服务商在采购人要求的时间内，周期性提供技术服务。

（3） 远程服务：服务商通过远程（电话、微信等）手段提供技术服务，必要时到现场服务。

4. 服务内容

本项目服务内容包括检测服务、分析研判服务和重点时段网络安全保障服务。

4.1 检测服务

检测服务内容包括网络攻击检测服务、隐蔽性威胁检测服务和安全检测分析与指导服务。

4.1.1网络攻击检测服务

（1） 服务商利用采购人的态势感知平台、天眼威胁监测与分析系统等安全设备实时检测网络攻击，对网络攻击信息进行识别与分析，确定网络攻击的影响范围，及时记录并上报，同时协助采购人进行处置与加固，实现每日安全告警清零。

（2） 服务期内，服务商提供 1 名安全检测工程师进行 5*8 小时驻场服务。

（3） 编制《风险记录闭环表》，提交月度《安全分析报告》；服务期满后，提交《网络攻击检测服务总结报告》。

4.1.2隐蔽性威胁检测服务

（1） 服务商利用采购人防病毒设备、终端安全管理系统、态势感知平台等安全设备，识别网络中潜藏的恶意程序以及持续性攻击。给出处置建议，并协助采购人进行处置。

（2） 服务期内，服务商至少安排 1 名网络安全工程师到现场服务。每月不少于 5 天，全年预计 60 天。

（3） 编制《隐蔽性威胁检测报告》。

4.1.3安全检测分析与指导服务

（1） 分析采购人网络安全检测能力的不足，给出优化建议，持续提升网络安全整体防护水平。

（2） 服务期内，服务商至少安排 1 名高级安全工程师到现场服务。每季度不少 3 天，全年预计 12 天。

（3） 编制《安全检测分析建议》。

4.2 分析研判服务

分析研判服务内容包括异常告警与事件分析研判服务和反编译分析服务。

4.2.1异常告警与事件分析研判服务

异常告警与事件分析研判服务主要服务内容包括分析研判服务、远程技术支持服务和安全自查服务。

4.2.1.1分析研判服务

（1） 针对检测服务中发现的高风险、高威胁告警分析研判、验证和溯源，评估风险等级，制定应对策略并协助处置，实现安全风险闭环管控。

（2） 服务期内，服务商安排 1 名渗透测试工程师到现场服务。每周不少于 1 天，全年预计 120 天。

（3） 编制《异常告警处置表》和《异常告警与事件分析研判报告》。

4.2.1.2远程技术支持服务

（1） 服务商提供 7*24 小时远程技术支持服务。

（2） 服务商根据采购人要求，及时提供技术支持服务。重大及以上网络安全事件服务团队在 30 分钟内到达现场。一般网络安全事件服务团队在 1 小时内到达现场。

（3） 根据实际情况，编制《安全事件响应报告》。

4.2.1.3安全自查服务

（1） 在采购人上级单位或监管部门开展安全检查前，依据检查内容，协助采购人开展安全自查，内容包含但不限于：策略有效性验证、脆弱性检测、密码策略审查等内容，提升整体网络安全防护能力。

（2） 编制《安全自查报告》。

4.2.2反编译分析服务

（1） 针对检测服务中发现的木马病毒、间谍程序等恶意代码样本，服务商提供反编译分析服务，包括但不限于动态分析、静态分析、代码逆向等。

（2） 服务期内，服务商至少安排 1 名高级安全工程师到现场服务。每月不少于 2 天，全年预计 24 天。

（3） 编制《恶意样本分析报告》。

4.3 重点时段网络安全保障服务

（1） 服务商在采购人承办的各项考试及国家重大活动期间，提供 7*24 小时现场值守服务。

（2） 服务期内，服务商至少安排 1 名网络安全工程师现场服务，全年预计 60 天。

（3） 编制《重保工作总结报告》。

5. 服务要求

5.1 人员要求

服务商项目服务团队包括但不限于项目经理、技术负责人、安全检测工程师、网络安全工程师、渗透测试工程师、高级安全工程师，所有项目成员均由采购人考核通过，不得随意更换；如要更换，服务商提前 10 个工作日向采购人提交盖章有效的书面申请，在经采购人同意后可进行调整。

服务商提供全部服务团队人员的简历、资质证明、社保证明，并加盖服务商公章，否则相应项不予认可。

服务团队人员要求如下：

（1） 项目经理（1 人）

项目经理负责本项目统筹规划、协调推进。应具备 5 年以上项目管理经验，具有信息系统项目管理师（高级）、CISSP、CISP、CISP-DSG 等资质证书。

（2） 技术负责人（1 人）

技术负责人负责协助项目经理进行项目管理，规划采购人总体安全检测防护体系，把控项目关键节点与质量交付标准、监控进度与风险。具有 CISP、CCSK 资质证

书。

（3） 安全检测工程师（驻场，1 人）

安全检测工程师负责日常安全检测、分析并协助处置。具备 CISP 资质证书。

（4） 网络安全工程师（至少 3 人）

网络安全工程师负责隐蔽性威胁检测与重点时段网络安全保障服务。全部具备 CISP 资质证书。

（5） 渗透测试工程师（至少 1 人）

渗透测试工程师负责开展异常告警与事件分析研判服务，具备 CISP-PTE 证书。

（6） 高级安全工程师（至少 1 人）

高级安全工程师负责安全检测分析与指导与反编译分析服务，具备 CISP、CCSS 资质证书证明。

5.2 服务可用性要求

（1） 服务商确保项目服务团队人员能力配置合理，安全检测工程师的岗位保证专人专岗并设置人员备份；

（2） 服务商提供的安全检测工程师配备笔记本电脑，并进行定期专业培训，以提高服务可用性。

5.3 规范性要求

服务商按照 ITIL 服务管理流程、服务活动指导文件及实施规则，以保证服务过程规范，主要包括：

（1） 遵循服务管理质量体系和流程文件，以保证服务过程实施规范性；

（2） 建立有效的交付管理制度流程，包括计划、实施、检查和改进等关键环节；

（3） 在服务过程中进行的任何活动，服务商建立服务档案，保留完整的服务记录；

（4） 建立规范的安全服务文档管理体系，安全服务文档的数量、内容及编写质量满足采购人网络攻击检测的工作要求；

（5） 服务商接受采购人或采购人委托的第三方对服务质量和绩效进行评价，并根据评价结果持续改进服务质量；

（6） 服务商接受采购人委托的信息化监理机构的管理。

6. 服务验收

（1） 服务商按照合同及附件中约定的相关条款、内容，按时、保质、保量地完成服务内容；若合同及附件中未约定的相关服务，服务商按照相关规范标准及时响应采购人的请求。

（2） 服务商在每项工作完成后，做好真实、详细地记录，采购人有标准规范格式要求的，按照采购人要求的格式及内容进行记录。服务商按照本项目要求提交相应成果物，所提交的成果物应齐全、完整、有效。成果物是否合格将作为验收付款的条件之一。

7. 知识产权

本项目涉及的全部及/或任何部分的相关知识产权、相关权益，包括本项目相关的且为实施本项目而新形成的商业秘密信息、技术资料和技术诀窍等，均归采购人所有。

采购人将拥有其在本项目所从事的所有工作（包括各类纸质文档，电子文档及其他可交付物）中所包含的或与之相关的全部版权、专利权、商业秘密、商标权和其他知识产权以及所有权和其他权益。

服务商当保证其提交的可交付物及有关参与本项目服务的任何活动包括履行本项目服务实施的任何行为，以及本项目合同终止后的任何涉及本项目的任何行为，均不会侵犯任何第三方的知识产权。

服务商提供的工具产品系其拥有所有权或知识产权的产品，如因产品侵权所发生的纠纷由服务商负责，与采购人无关。

8. 保密

（1） 服务商承诺以最严格的保密方式保存和维护从建设方或建设方代表获得的保密信息，未经建设方事先书面同意，不得向任何第三方披露。保密信息包括但不限于本项目合同、规格、计划、设计、软件及开发资料、数据、图纸、式样、样本或建设方为上述内容向服务商提供的任何其它资料。

（2） 服务商应保证其雇员只有在为了本项目的目的而必须知道保密信息的情况下，才允许获取从建设方或建设方代表获得的任何保密信息。

（3） 必须了解本项目合同规定的保密要求并与服务商签订保密协议。

（4） 未经建设方书面许可，服务商透露或使用了保密信息，应当在不损害建

设方其它利益的情况下，尽一切努力协助建设方收回保密信息，防止使用、传播、出售或以其它任何方式处置该保密信息。

（5） 本项目合同终止后 3 个工作日内，服务商应向建设方交还其获得的保密信息，不得以任何方式进行复制留存。

（6） 本项目合同有效期间及其后的 5 年内，本条款以及附件的规定仍对服务商发生效力，不因本项目合同的终止而失效。