上海海事大学港湾校区

平台安全服务

# 项目概述

上海海事大学港湾校区信息化建设以来，网络安全事件频发，学校已经有部分安全设备部署，包括深信服安全态势感知SIP、深信服AF防火墙、深信服终端检测响应平台EDR等，需持之有效的安全运营管理服务。学校目前有服务器虚拟机50台，重要的网站和URL应用10多个，大约200台办公电脑，为有效防止信息化网络系统被非法访问和黑客攻击，亟待建立网络安全服务以提供最大限度地防范，在受到侵扰的破坏后将损失尽旦降低。通过安全服务分析报告提供恢复被破坏的数据和系统的手段，尽量降低损失；并且分析侵入者的手段。采用现有网络安全基础，通过对网络系统的风险分析及需要解决的安全问题，制定合理的安全策略及安全方案来确保网络系统的机密性、完整性、可用性、可控性与可审查性。

教育部关于印发《教育信息化2.0行动计划》的通知（五）担当责任，保障安全中提出：加强教育系统党组织对网络安全和信息化工作的领导，明确主要负责人为网络安全工作的第一负责人，建立网络安全和信息化统筹协调的领导体制，做到网络安全和信息化统一谋划、统筹推进。完善网络安全监督考核机制，将网络安全工作纳入对领导班子、干部的考核当中。以《网络安全法》等法律法规为纲，全面提高教育系统网络安全防护能力。全面落实网络安全等级保护制度，深入开展网络安全监测预警，提高网络安全态势感知水平。做好关键信息基础设施保障，重点保障数据和信息安全，强化隐私保护，建立严密保护、逐层开放、有序共享的良性机制，切实维护好广大师生的切身利益。

# 整体要求

1. 本项目服务期为一年。
2. 投标方须针对招标技术参数给出偏离表，提供相应截图和必要说明，否则该参数被视为非实质性响应，扣分处理。
3. ★所投安全服务不是投标人自己的，需提供服务厂商针对本项目的授权书和服务承诺函
4. 本项目采用一次招标三年有效，分年度签订合同，每次签约有效期一年，每年度合同有效期终止前2个月，由采购人对中标人进行年度考核和验收，如通过则可续签第二年合同，第二年合同价为第一年的原合同价，如遇特殊情况，则以当年度法定程序批准的预算执行或者甲方有权重新招标。

# 安全服务清单

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务名称 | 服务内容 | 数量/单位 |
| 1 | 平台安全服务 | 安全运营服务 | 1年 |
| 2 | 7\*24网站安全实时监测 | 1年 |

# 服务内容和要求

## 安全运营服务

|  |  |  |
| --- | --- | --- |
| **服务类** | **服务类型** | **内容及要求** |
| 服务内容 | 首次威胁分析和处置 | 安全威胁分析：安全服务平台被动发现配合安全专家主动日志分析，识别服务范围内资产发现的病毒类事件、漏洞类事件、攻击类事件，并建立安全事件的进度监控机制 |
| 对外服务威胁检查：针对对外的服务器，着重对webshell、病毒进行重点排查，主动发现服务器风险隐患 |
| 首次威胁处置：投标方输出首次威胁分析报告，提供处置方法和工具，并上门提供首次处置服务 |
| 首次威胁汇报：处置完毕后，进行本次处置汇报，并进行报告解读 |
| 威胁分析和预警 | 结合大数据分析、人工智能、安全专家提供安全事件发现服务：依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括漏洞信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，经由大数据处理平台结合人工智能和安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态,发现各类安全事件，并自动生成工单 |
| ▲实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件（提供安全事件（如暴力破解）的工单截图，需展示当前安全事件的处置状态） |
| 实时监测网络安全状态，对病毒事件自动化生成工单,及时进行分析与预警。病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发DOS型、C&C访问型、文件感染型、木马型 |
| 安全专家针对每一类威胁，进行深度分析验证，分析判断是否存在其他可疑主机，将深度关联分析的结果通过邮件、微信等方式告知用户 |
| 流行威胁通告与排查 | 结合最新威胁情报，及时对流行威胁进行评估、风险通告预警 |
| 安全专家排查是否对用户资产造成威胁，通知用户协助及时修复或调整安全策略 |
| 主动响应服务 | 策略调配：新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新 |
| 策略定期管理：安全专家每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果 |
| 策略调整：安全专家根据安全事件分析的结果以及处置方式，根据用户授权情况按需对安全组件上的安全策略进行调整工作 |
| 针对病毒类的安全事件：安全专家提供病毒处置工具，并针对服务范围内的业务资产使用病毒处置工具进行病毒查杀，对于服务范围外的业务资产，安全专家提供病毒查杀方法和工具 |
| 针对攻击类的安全事件：通过攻击日志分析，发现持续性攻击，获取用户授权后采取行动实时对抗，当用户无防御措施时，投标方需提供攻击类安全事件的处置建议 |
| 针对漏洞利用类的安全事件：安全专家验证该漏洞是否利用成功，提供工具协助处置 |
| 针对失陷类的安全事件：安全专家协助用户处置，并提供溯源服务 |
| ▲基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置的解决方案（提供在服务平台申请主动响应的实际界面截图证明） |
| 根据事件发生的根因、影响范围，针对性给出安全加固方案 |
| 安全专家通过现象深入分析安全事件的成因，发现用户网络中存在的薄弱点，通过技术手段和方法溯源攻击路径 |
| 针对勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，快速恢复业务，消除或减轻影响 |
| 通过结合主动发现、主动处置、被动响应流程，对僵尸网络、病毒、后门、黑链等各类安全事件的处置服务 |
| 服务质量监督 | ▲服务监控：投标方需为用户提供服务监控门户，在门户中用户可查看业务安全状态，处置中的失陷事件以及针对这些事件的处置进度，处置责任人、联系方式等信息，方便用户时刻了解投标方的服务效果（提供服务监控门户，需展示上述相关信息）  投标方需有可视化的措施监督安全专家的服务水平，从工单的响应、工单的审核以及工单处理等维度判断服务是否出现停滞（提供可视化的服务监督措施截图，需展示工单认领、工单响应等维度） |
| ▲服务进度督促：针对服务平台生成的工单，招标方可按需催单，服务平台采用短信方式通知安全专家，督促投标方第一时间处理（提供短信催单实际图片） |
| 服务可视 | ▲通过安全服务平台，可随时查看业务资产安全状态（提供业务资产安全状态截图证明）在线展示所有事件监测结果、防御过程和防御结果  ★本项目使用服务工具支持将学校的安全态势感知、防火墙、终端检测响应平台收集的安全日志上传到安全服务平台上，并支持在该平台上对服务工具进行管理（提供安全日志上传配置截图、联动响应截图、平台远端管理截图）  ▲为了保证安全监测的效果，需要安全服务平台具备检测规则的自定义功能，以满足日益复杂的安全趋势所带来的安全需求（提供服务平台上检测规则的自定义功能截图） |
| 服务交付物 | 交付物名称：《安全服务运营报告》  交付物名称：《首次威胁分析与处置报告》  交付物名称：《事件分析与处置报告》  交付物名称：《安全通告》  交付物名称：《综合分析报告》  交付物名称：《季度汇报PPT》  交付物名称：《年度汇报PPT》 | |

## 7\*24网站安全实时监测

|  |  |  |
| --- | --- | --- |
| **服务类别** | **服务名称** | **详细参数** |
| **服务内容** | **保护网站** | 学校官方网站、统一身份认证、云盘、VPN等对外的网站系统。 |
| **定期风险评估（云评估）** | 暴露面检测 | 支持关键资产系统域名发现，自动发现客户所填入域名相关的所有子域名； |
| 支持检测网站服务器端口开放情况，比如数据库端口、Ftp服务端口等； |
| 漏洞脆弱性检测 | 支持对Web漏洞进行扫描，覆盖通用漏洞和常规漏洞。支持SQL注入、XSS、安全配置错误、已知漏洞组件包含、敏感信息泄露等常见漏洞的检测； |
| 专家漏洞验证服务 | 对风险评估报告中的高危漏洞进行专家验证，确保高危事件的准确性，并定期给用户推送云扫描报告。 |
|  | 高危0day事件告警 | 支持高危0day实时检测，出现0Day漏洞时，主动对所监控用户业务做扫描发现，重要网络安全事件和安全漏洞快速预警通告和检测，检测结果第一时间定向推送到客户，能够支持微信端实时推送告警信息（提供截图证明）； |
| **实时异常监测（云监测）** | 敏感词监测 | 支持对目标站点提供7×24小时网页敏感词检测能力。发现网页敏感词事件第一时间通过微信通知用户，监测内容能够在报告中进行呈现； |
| 业务可用性监测 | 支持页面响应监测，通过固定的频率模拟用户请求访问被监控站点，实时获取站点的响应状态和请求详情，精准的探测出网站的各种异常3分钟检测一次，当连续3次访问失败时判断为业务不可用； |
| 支持网站存活监测，通过固定的频率探测被监控站点存活状态 |
| 篡改监测 | ▲对目标站点的关键页面进行实时篡改监测，分钟级篡改发现，第一时间通过微信进行实时告警，并提供主动电话告警（提供微信告警截图证明）； |
| ▲支持整站内容进行篡改监测，梳理并在首页展示站点结构图，显示网站各节点是否存在被篡改事件（提供界面截图证明）； |
| 黑链监测 | 支持对目标站点提供7×24小时网页黑链监测能力。发现网页黑链事件第一时间通过微信通知用户，监测内容能够在报告中进行呈现。 |
| **及时告警** | 微信告警 | 支持以微信的方式对篡改、挂马、网站不可用等安全事件进行实时告警，支持微信端内容的及时推送（提供截图证明）； |
| 邮件告警 | 支持邮件的方式推送安全事件报告、月报运营报告，便于站点安全的管理 |
| **可视化展示** | 风险管理可视 | 平台展示包括web业务系统的风险统计、风险分布、潜在风险篡改TOP5和风险等级统计；  风险列表中包括已被篡改风险、潜在篡改风险、非篡改风险；  风险状态包含未解决状态、平台自动已解决状态、人工标记已解决状态，便于快速了解风险处理进度；  支持根据单位名称展示风险；（提供截图证明） |
| 篡改监测过程可视化 | ▲支持提供可视化的篡改监测界面，首页可直观展示篡改监测过程和监测结果，如正在监测哪一个页面，历史监测页面的安全状况等，便于实时掌握业务风险情况；（提供截图证明） |
| ▲网站篡改事件应支持查看“举证图片”，管理人员可通过微信及web登录界面，直观查看被篡改内容，便于第一时间掌握被篡改的情况（提供微信及web界面截图证明）； |
| 交付报告 | 支持每月定期进行网站安全评估，并生成安全评估报告，报告应至少包含扫描站点信息、风险分布情况、漏洞的风险描述、影响范围、解决方案和具体的攻击举证进行详细的展示（提供云扫描报告）； |
| 支持每日生成安全运营日报，每月生成安全运营月报，并针对安全事件实时生成安全事件报告（提供各类报告证明）；  平台可自动生成以下报告：《安全事件报告》、《内网扫描报告》、《云扫描报告》、《每日值守报告》、《安全运营报告》、《重大活动值守报告》；支持手动按时间范围导出《值守报告》。（提供界面截图证明和报告证明） |