附件五：服务内容和要求

**（一）服务内容**

1、7\*24小时网络威胁监测服务

服务拟使用硬件的品牌型号：360边缘安全大脑1台+探针1台。

边缘安全大脑是本次安全运营保障服务的服务工具，服务商需提供全新的服务器和探针设备，部署在信息中心机房，为学院提供实时网络威胁监测、预警与分析服务。包括对学院内网告警进行有效性验证，过滤无效错误告警；对安全告警监测分析并同步学院；通过工单流程处置和闭环有效告警；进行安全策略优化和SOAR自动化响应等。

3、其他运营处置服务

提供周期性运营复盘服务，定期复盘学院安全事件与风险情况，提供季报、半年报、年度报告并存档，报告内容涵盖阶段性安全运营统计分析及重要安全事件，如告警和事件统计、变化曲线等，助学院掌握整体安全运营状况与规划建设。

每年提供一次网络应急演练服务，安全专家依学院信息系统实际调研制订安全攻防演练方案，通过红蓝方真实对抗演习，从多维度发现学校安全防御问题，完善安全体系建设，提升对抗新兴威胁能力，演练后交付报告。

每年提供一次安全培训服务，依学院需求提供网络安全意识培训，内容含近两年网络安全事件、发展形势与意识提升。

1. **服务要求**

1、运营平台能力要求

平台的整体能力需包含安全动态、服务态势、服务概览、服务报告、人工智能AI机器人等等。托管服务通过统一运营平台进行整体运营，运营过程遵循可观、可管、可控、可溯的原则，能够保障在整个运营过程中,告警、分析和事件处置措施是连续和完整的，同时所有的告警分析研判过程完全可被回溯。运营过程需融入ChatGPT等先进技术进行数据处理和分析,以更好地保障学院网络安全和运营效果。

2、运营平台界面要求

运营界面要能展示整体的安全态势情况，用户可以查看不同的威胁信息,如资产监测情况和风险情况的概览、不同类别资产应用的TOP排名、近7天的风险感知情况、近7天的热门攻击播报、近7天的漏洞发现情况以及近7天的威胁识别情况等等。通过这些指标,使用户快速了解整体安全态势,以便及时采取措施来保护业务和安全。此外，在界面上用户可以随时与运营人员进行互动交流,从而更好地了解整个运营过程的情况。

3、安全运营人员要求

服务商的安全运营团队必须是经验丰富的安全专家组成，提供包括远程运营和安全分析等方面的工作，为学院的业务和安全保驾护航。运营团队成员的职责：运营经理对项目整体情况负责，监督项目进度，及时发现风险，保障运营效果；运营工程师负责日常的告警分析、事件的处理等;运营专家要专注于运营能力的研究和运营效果的不断提升。

4、探针能力要求

①数据采集：

数据解析规则支持规则嵌套和逻辑组合方式，能够对一组事件进行多层规则解析处理，添加、删除、重命名、合并、拆分与裁剪现有字段，对范式化后字段再解析处理。支持多种数据解析，包含精准匹配、包含再解析、正则匹配后从数据头、尾进行二次解析等处理。

②数据分析：

支持内置500+规则模型，并支持模型的启用与停止配置。支持查看模型对应的典型攻击场景，理解典型的攻击过程，辅助告警分析研判。支持关联规则根据数据标准进行规则编写的自动化推荐，系统根据事件类型自动推荐其所属的对象。支持关联规则在配置时评估该策略运行所使用的资源情况，在线显示该规则的性能指标，分为优、良、差多个级别。告警事件支持 ATT&CK 攻击技术识别与详细说明展示，包括攻击技术的说明，攻击技术的数据源等信息辅助分析。

③资产识别：

支持网站子URL的爬取，并形成网站地图。支持标记来源，来源至少包括爬虫、被动流量、情报等。支持限制爬取的目录层数（不低于5级）、单个路径下文件数量（不少于50个文件）、爬取URL总数（不少于3000）、能够过滤特定类型的URL（如图片、样式表、字体等），支持对网站地图中爬取到的特殊URL进行自动化标记，至少包括API和管理后台标记。

支持国产化设备的指纹特征识别，支持3000+种国产化指纹，其中包括：a.达梦、人大金仓等国产数据库的指纹≥10种。b.东方通等中间件的指纹≥10种。c.华为、海康威视等国产监控设备≥200种。d.金蝶OA、致远OA等国产业务系统指纹≥500种。5.天融信防火墙、启明IDS等国产安全设备指纹≥500种。

支持设置用户可以管理的资产范围，能够限制用户只能管理资产范围内的资产和这些资产对应的威胁。支持设置用户可以管理的资产范围，能够限制用户只能管理资产范围内的资产和这些资产对应的威胁。

④脆弱性检测

平台需支持后期扩展漏扫服务。POC插件需至少支持国产信创应用漏洞检测，国产信创应用漏洞≥500个。支持在1day漏洞爆发的24小时内进行漏洞情报实时推送（联网），且能针对新披露的高危1day漏洞自动匹配预估受影响资产数据，明确受影响范围。

⑤终端兼容性

产品支持对第三方提供数据接口，支持获取的数据包括客户端安装数量、客户端版本统计、操作系统统计、病毒库版本统计、补丁库版本统计、违规外联统计、终端安全检查结果等；支持获取分组列表、终端列表信息；支持查询终端软件、硬件、资产登记信息。支持向终端下发程序升级、病毒库升级、漏洞库升级以及杀毒扫描命令。

⑥基础管理

支持对管理员账户登录或高危操作进行多因子认证，包括动态口令二次认证且可通过微信小程序查看动态口令，支持多因子认证的高危操作包括账号添加修改、重置密码、重置二维码、文件分发等。

支持终端用户提交故障信息并可上传相关附件，管理员收到信息后可查阅并处理。支持终端用户提交意见反馈信息，管理员收到信息后可查阅并处理。

支持配置管理员账户登录白名单，即管理员只能在指定IP范围内的终端上才能登录管控中心。

⑦漏洞与补丁管理

产品支持蓝屏修复功能，当安装补丁出现蓝屏时可恢复系统。

支持查看服务端下载的补丁文件信息，并可通过服务端页面提供的下载链接下载相关补丁文件。支持管理员配置补丁包含列表、补丁排除列表。终端用户可查看已安装的补丁、已忽略的补丁，可按照KB号卸载指定补丁，支持清理补丁安装包，减少对磁盘空间的占用。

⑧安全与合规检查

支持对Windows终端进行安全基线检查，管理员可根据业务需要，配置每个检查项的扣分标准、修复方式以及是否为否决项，支持设置周期检查、开机检查、定时检查等。安全检查项包括身份鉴别检查、访问控制检查、入侵威胁检查、系统状态检查以及系统运行检查。

安全审计检查：审核登录事件、审核帐号管理、审核目录服务访问、审核对象访问、审核策略更改、审核特权使用、审核进程跟踪、审核系统事件、审核账户登录事件、管理审核和安全日志、系统过期日志检查。