数据安全与信息安全提升项目需求

一、项目背景

在当前网络安全形势日趋严峻和网络攻防实战常态化的背景下，新型攻击手法、攻击技术层出不穷，隐秘高效的自动化攻击也越来越多，以安全合规建设为目标的静态、被动网络防御体系往往力不从心。美术学院当前的防护体系缺乏针对未知攻击、隐蔽攻击的高级威胁检测能力，不能对流量进行深度解析，不能发现潜伏在其中的各种安全威胁，一旦发生网络安全事件甚至没有审计数据以供回溯。对学校网络安全的智能感知能力不能预判相关的威胁，不能进行有效数据取证与责任判定。

美术学院有必要对本单位进行全局安全运营方案建设，探索学校安全运营的新思路、找到安全建设的新内涵、实践安全治理的新方法，通过布局协调指挥综合管理，形成安全体系化能力基座，实现监控预警、处处响应、分工处置、责任到人、安全闭环的全流程管理，提高整个校园安全防护体系的安全态势感知预警能力和安全合规水平，最大程度防范以及降低外部攻击所引起的组织声誉、重大的经济损失和政治影响。

二、需求内容

序号	名称	规格型号、技术参数	数量
1	API 安全检测与访问控制系统	API 安全监测与访问控制系统（API-SMAC）是为了解决应用 API 接口访问场景下的安全问题推出的一款 Web 应用侧数据安全产品。	1

		该平台基于 API 资产治理、身份治理、流量管控、访问鉴权、机器学习等多种核心技术，帮助用户梳理庞杂的应用及接口，绘制接口画像和接口访问轨迹，监测敏感数据流动风险，识别接口调用的异常用户行为，为应用系统的业务数据合规正常使用和流转提供数据安全保障。 产品参数： 1.默认流量：200M； 2.基础功能（业务应用、API 接口资产管理，身份管理、风险监测以及统计分析等模块）； 3.支持国产化环境。维保年限：原厂 3 年。	
2	数据库权限管控系统	数据库防水坝是一个数据安全内控管理安全设备，提供全面的资产防护能力，包括：敏感数据发现管理；运维操作数据即时动态脱敏；防范敏感数据危险操作；限制特权账户随意访问敏感数据；利用身份管理、授权等机制对运维人员进行合规管理；协助运维人员实现工单管理和免密登陆；提供全面风险分析报告等功能。 产品参数： 1.默认数据库实例：16 个； 2.基础功能（数据库准入、访问控制、运维审计等）； 3.支持国产化环境；	1

		4.账号托管； 5.支持 HA 主备模式；	

		6.在线会话数：4000； 7.运维 SQL 吞吐量 4000 条/秒； 8.含防假冒套件：10 套。 功能拓展包：标准版运维脱敏功能，维保年限：原厂 3 年。	
3	数据库安全审计系统	数据库审计系统，以数据资产安全访问合规为出发点，以精确审计、全面审计为基础，提供围绕数据库的日常化运营、可疑分析和安全报告，全面管理整个数据库安全事件的生命周期。 产品参数： 1.默认流量：200Mbps； 2.基础功能：双向审计，报表等； 3.支持国产化环境； 4.数据库实例：512； 5.峰值 SQL 吞吐 20000 条语句/秒。 维保年限：原厂 3 年。	1
4	融合安全数据底座分析中台	工作台支持自定义个性化配置，支持以拖拽组件的方式进行画布页面设置，页面可选组件包括“CVE 漏洞利用、SOAR、WEB 安全、内网病毒、原始告警、告警监控、安全事件、安全日志、安全设备、工单、平台概览、快速搜索、持续攻击、文件分析、资产管理、风险资产”等，可选组件不少于 65 个。	1

		每个组件均支持点击“收藏组件”按钮进行自定义收藏；质保期原厂 36 个月软硬件服务。	
5	运维堡垒机维保服务	12 个月原厂软硬件维保。	1
6	WEB **应用防火墙维保服务**	12 个月原厂软硬件维保。	1
7	日志审计维保服务	12 个月原厂软硬件维保。	1
8	网站监测平台维保服务	12 个月原厂软硬件维保。	1
9	资源发布平台续保	12 个月原厂软硬件维保。	1
10	IPV6 反向代理扩容	12 个月原厂软硬件维保。	1
11	认证计费系统续保及功能完善	12 个月原厂软硬件维保。	1
12	IPV6 防火墙续保服务	奇安信 5000：3 年威胁情报等全功能模块升级+硬件三年原厂质保。	1
13	校区防火墙续保	奇安信 7000：3 年威胁情报等全功能模块升级+硬件三年原厂质保。	1
14			1

	校区业务防火墙续保	奇安信 5000：3 年威胁情报等全功能模块升级+硬件三年原厂质保。	

三、技术指标

1、API 安全检测与访问控制系统

指标项	详细功能要求
规格	至少支持 200M 流量。
国产环境	适配银河麒麟 V10-鲲鹏 920ARM、银河麒麟 V10-飞腾 F2500ARM、龙蜥 V7.9/V8.2/V8.4-鲲鹏 920ARM 等。
插件部署	支持串联部署，通过串连方式分析流量并进行安全防护。
旁路部署	支持旁路部署，通过镜像流量进行分析和安全防护。
加密流量	支持 TLS1.2 及 TLS1.3 的加密流量解析。
态势感知	提供数据流转安全态势大屏，统计展示数据访问量、业务流转、应用访问热度、API 台账、应用涉敏接口、流动防护等。
资产识别	支持通过镜像流量或探针代理自动识别请求和返回中的 API 资产及应用资产，包括但不限于 API 的接口信息、参数信息、请求方法等。 支持通过 API 资产的发现时间、活跃时间、访问次数、请求方法进行关联分析，识别已知 API、未知 API 等。
一类数据采集组件	包含 30 种以上的深度检测模块，可支持 shiro 反序列化、蚁剑、哥斯拉、冰蝎 3.0、冰蝎 4.0 等检测能力，且能识别如 shootback、TunnaProxy、dnscat2、reGeorg、reDuh、CobaltStrike 等隧道通信工具。
二类数据采集组件	支持对 Agent 进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。

集中数据库审计风险控制组件	支持自定义报表，自定义报表支持告警名称、告警等级、操作类型、操作系统用户名、数据库名/实例名、主机名、数据库账号、客户端 IP、客户端工具、数据库类型、客户端端口 11 种统计维度，支持来自审计日志、告警日志、会话日志的 29 种统计指标，根据以上条件进行灵活选择后生成报表。
资产画像	支持通过 IP、端口、API 接口统计、API 流量统计等维度进行应用资产画像。 支持树状化展示应用资产中的 API 个数以及 API 资产的详细信息，包括但不限于请求方法、状态、访问次数等。 支持单个 API 资产通过访问次数、请求方法、状态、发现时间、活跃时间、近 7 天访问曲线图展示 API 资产画像。
资产管理	添加管理业务应用以及 API 接口。 支持利用文件进行 API 资产的自定义导入，字段必须包含 web 主机、请求方法、URL。 统计展示 API 接口资产信息访问情况信息，如访问数据量、访问次数、敏感次数等。 支持对 API 资产进行自定义状态标签。
数据标签管理	至少包含 180+种业务类型，可根据不同业务类型对数据进行自动分类，业务类型包括个人通信信息、个人位置信息、个人身份信息、网络身份标示信息、组织机构信息、企业信息、行业相关信息、基础信息、天气信息、个人设备信息等。
身份治理	以“人、应用、终端、账号”四个维度进行身份定义，联动安全设备全局进行身份治理。
身份	AI 赋能安全，通过梳理身份标签、访问关系拓扑、上下文访问链路等建

画像	立身份画像，通过身份基线比对，实现风险身份的自动化智能监测。

风险监测	支持自动识别流量中 SQL 注入、XSS 跨站攻击、命令注入的异常行为； 支持自动识别 API 接口中的异常机器行为，包括爬虫、跨域访问等； 支持自动识别 API 流量中的弱口令，防止暴力破解行为； 支持对 API 流量中的敏感数据进行识别，包括但不限于身份证号、手机号、银行卡号等； 支持对单 IP、单 URL 单位时间内的高频访问敏感数据进行检测； 支持 API 滥用防护，防止刷单、薅羊毛、漏洞攻击等 API 接口的异常行为； 支持针对 API 接口的盗用防护，防止接口盗用导致的 API 数据泄露； 支持 API 鉴权防护，通过提取用户鉴权与认证数据，针对鉴权及认证失败信息进行检测分析； 支持 AI 算法检测，通过实时检测进行建模训练，形成风险检测模型，识别异常行为。
访问策略	支持根据不同身份及身份因子，针对 API 接口访问频次、单日请求次数、单日获取敏感数据次数等维度设置对 API 接口的访问进行控制。 支持 API 访问策略关联设置到具体的 API 接口资产。 支持通过预设敏感词类型、敏感词以及自定义敏感词，根据配置对报文进行检测，对检测到配置中的敏感词执行脱敏处理动作。 支持根据不同身份及身份因子，对 API 接口中进行水印设置，提供 API 接口的溯源能力。
事件溯源	支持将采集的安全事件信息进行展示，提供事后安全审计追溯能力。并对安全事件进行合并去重、富化。