#### 一、项目概述

学校各业务部门已建成覆盖教学、学生管理、科研支持、资产运维、财务报账、图书资源管理、一网通办流程办事等平台系统，所包含的的数据越来越多地被搜集、存储、汇聚，并用于行业科研合作、数据交换和共享，成为支撑业务运营发展的重要资产。学校现有的安全防护措施包括日志审计、网络防火墙、网络态势感知、终端准入等手段，数据平台在数据采集、传输、存储、处理、交换等生命周期中数据安全防护建设中存在如下问题：

1.有网络安全，但缺少数据安全

安全防护设备无法解析数据库协议，无法实现对数据库操作的安全管控，黑客一旦突破了边界进入内网之中，再非法入侵学校数据库系统，就轻而易举地进行删除、拷贝数据等破坏行为，需要建立面向数据资产的数据安全防护措施，与网络安全形成互补。

2.缺少发现数据的手段和工具

业务平台上汇集了大量的数据资源，随着业务扩增和数据增长，数据库也在不断增加，经过长期积累，很难理清有哪些敏感数据，敏感数据在哪里，为哪些人开放了权限，数据的使用频率如何等。缺少专业的手段和工具发现和梳理数据，快速形成完整的数据资产目录，从全局掌握数据资产分布和权限分布情况。

3.第三方合作伙伴账户及权限缺少管控

学校各业务系统的供应商作为第三方合作伙伴，在建设系统过程中（如：搭建开发/测试环境），需要对其开放数据，目前很多单位因为在规划阶段没有提前考虑数据安全规划，在业务平台建设阶段对第三方合作伙伴开放了很多核心数据库，重要数据直接暴露在第三方开发/测试人员面前，存在安全风险，并且当第三方在项目交付后，数据库账号没有及时收回，仍能随时访问重要数据，这也是安全风险之一。

基于以上现状，为强化西安美术学院数据安全保障，根据《数据安全法》《网络数据安全管理条例》《关于加快推进教育数字化的意见》等文件要求，加强学校数据收集、汇聚、存储、流通、应用等全生命周期的安全管理，计划通过引入数据安全数据安全管理平台，建设一套数据安全防护保障体系，从数据全生命周期视角形成闭环的数据安全建设流程，包括制度管理建设、数据采集、存储、传输、处理、交换、销毁几个关键阶段，为学校业务平台的数据共享交换和上层业务应用提供数据安全保障。

#### 二、建设目标与内容

（一）建设目标

建设一套数据安全防护保障体系，将数据安全防护、数据安全管理、数据安全运营统一纳管，具备统一资产管理、统一身份治理、统一风险监测、统一数据安全态势感知能力，能够快速有效发现敏感资产，根据数据安全统一规划对全域数据进行分类分级，并通过相应的数据安全软件，保护数据资产安全，实时进行风险监测和风险告警，全面风险分析研判，安全事件应急响应，异常事件告警，安全合规检查，为学校数字化转型数据提供安全保障。

（二）建设内容

学校数据安全防护建设规划为数据安全风险可见、数据流转可视、数据访问过程可查，进行数据安全基础能力建设，完善数据安全防护能了场景，包括数据安全管理制度、敏感数据保护以及数据安全一体化平台。

具体建设清单如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **建设内容** | **数量** | **业务描述** |
| 1 | 数据安全管理规范制定服务 | 1项 | 建立健全数据安全制度规范体系，制定包括数据分类分级、访问权限、共享开放、数据安全运维、应急预案与演练、监测预警、应急处置灾难恢复、应急处置等各种安全管理活动中的流程和管理制度、操作规程等，以指导数据安全技术体系的实现和合理使用，促进组织数据安全管理工作标准化、流程化、规范化，使各项数据安全管理工作有规可依。  交付2个数据安全管理制度。 |
| 2 | 数据安全一体化平台 | 1套 | 全场景安全风险事件的集中收集、清洗、分析与预警，实现全量数据资产的识别和集中呈现，达成数据安全智能管控的“可视化”、“可量化”、“可感知”和“可追溯”的数据安全态势感知综合分析平台。  可支持不少于：1G数据库流量（10G网络流量)，1,500个资产授权（关系数据库资产按实例数核算）。 |
| 3 | 敏感数据安全防护软件 | 1套 | 通过账号托管、数据库准入、访问控制、运维脱敏、误操作恢复等防护措施，对内部人员进行数据安全合规管理。  提供数据库实例不少于10个。 |

#### 三、技术要求

**1.数据安全管理规范制定服务**

根据国家标准、教育部标准、行业标准和西安美术学院实际业务情况，兼顾各个标准之间的兼容性、一致性以及标准的可扩展性，并结合学校的数据特点进行归纳整理，梳理学校重要的业务数据状况，设计并建立西安美术学院数据安全制度规范体系，制定包括数据分类分级、访问权限、共享开放、数据安全运维、应急预案与演练、监测预警、应急处置灾难恢复、应急处置等各种安全管理活动中的流程和管理制度、操作规程等，相关制度规范能够在学校可落地，可有效指导学校各业务数据通过安全技术体系合理使用和有效防护，促进组织数据安全管理工作标准化、流程化、规范化，使各项数据安全管理工作有规可依。

本次需交付2个数据安全管理制度。

**2.数据安全一体化平台**

|  |  |  |
| --- | --- | --- |
| 产品功能 | 系统架构 | 支持前后端分离和微服务体系，使用跨平台的技术，实现应用与硬件平台无关联； |
| 采用B/S架构，全中文操作界面，支持主流浏览器，支持https/SSL等加密传输协议； |
| 支持创建多个租户，并为不同租户按需分配数据安全能力。 |
| 产品性能 | 提供大于等于1G数据库流量(10G网络流量)，大于等于1,500个资产授权。 |
| 产品部署 | 支持CentOS、Redhat、Ubuntu等操作系统；支持银河麒麟、龙蜥、统信、OpenEuler等国产操作系统，及海光、鲲鹏等国产CPU芯片部署环境。 |
| 安全性 | 平台具有安全审计员、安全保密员、系统管理员三种角色，实现三权分立； |
| 支持对访问身份进行强验证，包括生物特征-指纹、软硬证书、OTP码等； |
| 支持对平台用户的密码复杂度（数据、大小写字母、特殊字符、密码长度等）、有效期、复杂度、密码错误锁定策略等进行限制，有效期过后提供登录重置密码或禁止登陆需联系管理员处理2种处理方式，以确保平台自身账户的安全；支持通过根据密码有限期进行密码前置更新或自动更新配置，以确保平台自身账户的安全。 |
| 产品功能 | 资产管理 | 支持按数据库、数据库账号、数据资产、SQL语句等类型区分管理资产； |
| 支持MySQL、Oracle、PostgreSQL、SQL Server、DB2、Informix、MariaDB、Sybase、Greenplum、QianBase、Elasticsearch、MongoDB、Hive、ODPS、HBase、Redis、Impala、RDS\_Mysql、RDS\_Postgresql、RDS\_ SQLServer、武汉达梦、南大通用、人大金仓、神舟通用、瀚高等类型的数据源进行统一管理；实时展示数据库运行指标，至少包括实时请求数、实时会话数、访问量、流入量、流出量；支持根据组织架构或权限组，进行数据库分组； |
| 支持为同一数据库配置多IP地址，可通过多个隔离网络访问此数据库，满足云上网络架构部署需求； |
| 至少包含两种数据库账号自动发现能力，包括：通过数据库用户表扫描数据库账号、基于数据库访问流量发现数据库账号；支持数据库账号权限检测，以列表形式展示权限信息； |
| 支持通过手工自定义SQL语句和SQL风险等级，形成可统一管理的高危SQL列表；提供从原始审计日志中一键提取高危SQL的功能；一条高危SQL语句可关联同个类型下的多个数据源；支持一键启动、停用高危SQL语句防护。 |
| 身份管理 | ▲支持以“人、终端、应用、账号”四个维度精确定义唯一的资产访问身份；支持通过终端设备IP、MAC地址、应用名称、动态指纹、数字证书、数据库账号、业务账号名称等因素的组合，构建多维的身份鉴别策略；**（提供功能截图并加盖供应商公章）** |
| 支持身份的分组管理；支持设置身份的审计级别、有效时间、信任度、关联可访问的敏感数据等级；支持身份的黑名单管理； |
| 支持基于数据库访问日志，一键发现资产的访问身份；可通过设置、完善身份信息，将未知身份转化为已知身份； |
| ▲支持基于数据库协议，自动检测应用连接数据库的SQL语句上下文，形成应用动态指纹；支持通过应用的名称、HASH值、动态指纹，为身份绑定唯一的、可信的应用，防止应用被仿冒。**（提供功能截图并加盖供应商公章）** |
| 法规解读 | 支持上传doc、docx、pdf等格式的法规政策文件进行统一管理，并支持一键下载至本地； |
| 支持不少于50份数据安全法律法规的条文解读，至少包括《数据安全法》、《个人信息保护法》、《数据出境安全评估办法》等；总结、展示合规文件中所有的数据安全核查项，并提供简单易读的安全指导标签，辅助快速理解落地。 |
| 风险策略 | 支持围绕资产、身份、操作行为、执行结果、特定账号等访问全链路，自定义风险规则列表和信任规则列表；可在特定时间点根据信任规则列表或风险规则列表，自动过滤第三方数据安全设备的日志，当访问事件与信任规则匹配时，不再进行风险检测、告警、以及风险拦截，实现海量风险事件的过滤、降噪；当访问事件与风险规则匹配时，及时进行风险检测、告警。 |
| 审计日志 | 所有审计日志统一在平台集中存储、展示、检索；支持展示审计事件包含的相关主体、相关客体、相关行为、相关执行结果、返回结果等信息，至少包含客户端IP、资产IP、原始SQL、执行结果、执行时长、安全响应行为、风险等级等45个以上的审计要素，以便精准审计到人； |
| 支持灵活组合审计日志发生时间、访问主体、操作类型、设备类型、关键字等要素，进行审计日志检索； |
| 支持根据特定规则进行事件过滤，过滤后的事件日志不在标准化日志展示中心呈现，以减少海量日志内容带来的运营压力；过滤后的事件仍可在事件回溯模块中展示，以保证回溯环节中的日志完整性； |
| ▲支持将审计日志查询条件通过且或逻辑组合对日志进行精确查询；支持等于、不等于、包含、不包含、为空、不为空等运算条件；**（提供功能截图并加盖供应商公章）** |
| 支持对返回内容进行遮蔽，内置不低于10条常见遮蔽规则；支持通过字符串或正则表达式自定义遮蔽规则；遮蔽内容经过身份验证后支持查看。 |
| 审计告警 | 支持对日志进行聚合分析，当同一主机/同一数据库账号/同一客户端IP/同一设备/陌生业务账号累计触发同一规则达到一定次数时，才会进行告警，以降低告警次数； |
| 支持对告警信息进行详细的订阅设置，包括告警接受的对象、接收方式、资产范围、告警范围、风险类型、告警发送时间、告警频次等信息；支持通过短信、邮件、专有钉、钉钉、企业微信等多种告警方式发送风险提示。 |
| 风险处置 | 支持对数据安全事件进行集中去重展示，并统计展示对应事件的历史告警次数和处置状态； |
| 支持以最近发生的时间、风险策略名、风险等级、资产地址、处置状态等条件进行精确检索，提升风险处置效率；支持设置不同检索条件模版和默认检索条件，可一键调用检索，以提升事件检索效率； |
| 支持对特定风险类型自定义危害情况和处置预案，提升运营效率； |
| ▲支持从安全事件中提取关键因子，形成信任规则，当访问事件触发信任规则时，不再列入安全事件列表**（提供功能截图并加盖供应商公章）**。 |
| 画像分析 | 内置资产画像模块，通过梳理资产标签、访问关系等内容，实时计算资产的安全评分和风险等级；统计分析、展示资产被访问的情况，包括常访问的数据库账号、客户端IP、操作类型等，供资产的安全运营提供参考数据； |
| 内置身份画像模块，实时计算身份对应的安全评分和风险等级；统计分析、展示来访者的访问习惯和潜在的风险，包括常访问的时间、常使用的终端、常使用的工具、涉及的操作的风险类型、高频操作类型、操作轨迹、影响的资产范围等信息，为安全策略的制定和优化提供数据支持；针对风险身份，提供针对性防护建议。 |
| 态势大屏 | 提供安全态势大屏，直观展现数据安全总体态势，包括敏感资产访问热度、活跃身份、访问时间热度、资产脆弱性统计、风险资产Top5、风险身份TOP5、风险类型Top5、安全防护效果、告警趋势、实时高危事件等模块，呈现整体系统的安全总体态势。 |
| ▲提供资产分布态势大屏，直观展现用户整体系统的风险情况，包括数据库/敏感表/敏感列的数量统计、数据访问趋势、数据库类型占比、SQL执行时长分布、数据敏感列分布、敏感表数据分布、数据库登录情况TOP10等内容；支持个性化换肤；**（提供功能截图并加盖供应商公章）** |
| 提供运行监控大屏，直观展现安全设备整体运行情况。主要展示运行天数、安全设备数、事件总数、告警总数、设备运行情况、日志采集趋势等模块。 |
| 工作台 | ▲运营处置工作台提供高频配置流程入口，包括用户创建、数据库资产、防护策略部署；展示防护能力的使用情况及资产变更数据；通过风险处置列表、待办列表、督办列表将日常运营工作提供集中化处理。**（提供功能截图并加盖供应商公章）** |
| 安全报表 | 内置合规报表、专项报表、综合报表、自定义报表四种类型。合规报表：提供萨班斯报表、等保报表、PCI报表、数据安全法报表模板，帮助用户满足日常合规需求，便于各类监管场景下的合规审查；专项报表：面向巡检等各类业务需要，面向运维、脱敏等业务场景提供数据安全专项报表；综合报表：面向数据库从敏感资产分布、SQL语句执行、风险事件角度对数据源进行综合分析，综合判断安全；支持按需选择资产范围和时间范围即时生成在线报表。 |
| 设备管理 | 支持对接第三方数据安全设备，实现数据收集、数据外发、任务联动；支持监控数据安全子设备运行状态，可直观呈现子设备的CPU、内存、磁盘使用率、网络接发情况及其趋势； |
| 可通过产品界面，采集并展示第三方设备的审计数据、告警数据、设备运行数据； |
| 工单管理 | 支持通过根据实际业务流自定义配置工作流程；支持工单节点处置带外通知，包括短信、邮件。 |

**3.敏感数据安全防护软件**

|  |  |  |
| --- | --- | --- |
| 功能模块 | 部署方式 | 1.支持反向代理部署；  2.支持分布式部署，通过管理中心对分布式部署的各网关节点进行集中配置管理、分析、统计等。 |
| 产品性能 | 数据库实例大于等于10个。 |
| 高可用 | 支持集群，可随业务随时平滑扩展； |
| 支持主备HA部署。 |
| 权限模版 | 针对不同敏感等级的敏感资产，支持通过内置的权限模版，实现身份的初始化授权，1级敏感资产默认授权只读且可查询明文，其余敏感等级资产默认授权数据只读且脱敏权限，确保资产数据安全，实现基于资产的零信任防护；内置的权限模版无法编辑、删除； |
| 支持设置数据操作、数据库对象操作两种类型的权限模版；支持通过数据操作模版，自定义对敏感资产的DQL、DML操作权限；支持通过数据库对象操作模版，自定义表、视图、存储过程、函数等各种实体的DDL、DCL操作权限； |
| ▲支持通过权限模版，为特定身份授予数据操作、数据库对象操作权限；支持限制授权有效期，可将授权有效期约束在指定时间段、指定时间周期、指定时间域；当需要变更某身份所使用的授权模版时，应当在变更前，进行授权前后的权限对比，明确标注操作变更项，防止因平台误操作造成不合理授权；**（提供功能截图并加盖供应商公章）** |
| 支持为不同等级的敏感资产，自定义设置不同的权限模版。 |
| 准入控制 | 支持数据库登录授权，通过身份的多因素认证，至少应支持应用名称、应用签名、主机名、证书、数据库用户、操作系统用户、用户名、IP地址、MAC地址等因素的任意组合，系统根据多维身份管理策略，自动判别登录主体的合法性，如不符合设定的身份管理策略，登录失败； |
| 支持通过不删除账户的方式，在系统中回收资产授权权限。 |
| 防绕过 | ▲可通过在数据库服务器安装探针，实现直连阻断、本地操作管控，防止非法身份绕过安全系统，违规对数据库进行访问；**（提供功能截图并加盖供应商公章）** |
| 具备应用防假冒功能，至少支持通过安装安全客户端进行MD5值和应用程序名校验、及提取数据库的动态访问内容作为动态指纹两种方式实现应用防假冒；针对假冒应用，可进行行为阻断或告警。 |
| 数据库账号安全 | 具备免密登录功能，通过安装安全客户端，将数据库账号与运维终端的数字证书进行绑定，实现在运维终端无需输入数据库用户名密码就可登录数据库，减少因数据库帐密公开造成的泄露问题；免密登录至少支持Toad、PL/SQL DEV两种运维工具； |
| 支持产品OTP登录二次身份认证； |
| ▲具备账号托管功能，支持将真实数据库账号映射至自定义的托管账号，并通过OTP、或系统动态生成的动态码作为配套密码，实现运维人员通过托管账号及动态码校验即可访问数据库，防止因数据库帐密公开造成的泄露问题；动态码应当脱敏显示，查看动态码时应当输入平台密码进行二次校验，动态码支持在线手动更新、自定义；**（提供功能截图并加盖供应商公章）** |
| 支持安全客户端的短信二次认证功能，当登录安全客户端时，使用短信验证码验证成功才会登陆放行。 |
| 权限管控 | 针对敏感数据集合的访问，任何账户（包括DBA\SYSDBA\Schema User\any权限等用户）都需要通过授权才可以访问，对不具备访问权限的操作，明确阻断拒绝，实现用户权限分离管理； |
| ▲支持通过标准SQL、原始SQL、正则SQL等方式自定义高危SQL，用以精细化控制针对指定对象的ALTER、DROP、CREATE 、TRUNCATE等高危操作行为；支持将访问日志中的原始SQL进行标准化，形成标准SQL，方便运维人员从访问日志中直接拷贝标准SQL用以自定义高危SQL；**（提供功能截图并加盖供应商公章）** |
| 支持DB2数据库联邦表管控； |
| 支持无需进行SQL语句自定义，即可在系统页面直接设置针对数据库角色、数据库对象、数据库系统等进行数据库授权相关操作的管控授权；数据库角色授权中，应当包含对DBA、SYSDBA、SYSADMIN、服务器管理员、安装管理员、ADMIN、DBADMIN、USERADMIN、SECURITYADMIN等数据库角色的授权；数据库对象授权中，应当包含对访问敏感对象、访问业务用户对象、访问系统对象的授权；数据库系统授权中，应当包含对任意对象及任意数据的删除、创建、修改等； |
| 支持无需进行SQL语句自定义，即可在系统页面直接设置针对数据库用户代码的操作管控授权，包括存储过程、函数、包、触发器、视图、索引等代码进行创建、删除、修改； |
| 支持无需进行SQL语句自定义，即可在系统页面直接设置针对数据库账号的操作管控授权，包括对用户、角色的创建、删除和修改，以及对密码的更改； |
| ▲支持无需进行SQL语句自定义，即可在系统页面直接设置针对数据表对象的操作管控授权，包括对数据库、SCHEMA、敏感数据表、业务用户表格、系统表格、以及表空间的删除、清空、修改、创建；**（提供功能截图并加盖供应商公章）** |
| 支持数据访问频次控制，当请求超过自定义的阈值时，阻断请求；支持查询行数控制，当查询行数超过自定义的阈值时，超过的行数进行脱敏显示，防止返回过多明文导致批量数据泄漏； |
| 支持删除行数控制，当删除行数超过自定义的阈值时，可实现在不阻断删除操作的前提下，不删除任何数据；支持更新行数控制，当更新行数超过自定义的阈值时，可实现在不阻断更新操作的前提下，不更新任何数据； |
| 支持运维连接数控制、以及对单次请求关联的表个数进行管控，以降低大量恶意连接、复杂SQL等因素对数据库性能的影响； |
| 支持对通过DBeaver等三方运维工具进行数据导出的行为进行管控，未授权身份无法实现数据导出。 |
| SQL窗口 | ▲支持直接通过SQL窗口进行数据库操作，提供可审计、可管控的数据访问方式；**（提供功能截图并加盖供应商公章）** |
| 支持通过SQL窗口访问阻断时，可直接发起工单进行权限申请； |
| 支持SQL输入时数据库对象与关键字智能提示、SQL美化； |
| 支持SQL查询结果集可视化查看、修改、添加、删除，并通过访问身份进行权限控制； |
| 支持对通过SQL窗口导出查询结果集的行为进行管控，并支持通过工单申请数据导出权限；结果集导出格式至少包含XLSX、CSV、TXT、SQL等； |
| 支持查看及生成指定数据库表的DDL语句； |
| 安全防御 | 支持僵尸账号检测，对僵尸账号进行永久锁定，防止僵尸账号造成数据泄露； |
| 支持数据库口令暴力破解防御，对口令攻击行为进行防御，防御数据库爆破行为； |
| 支持数据库防扫描，防止黑客或恶意用户对数据库进行扫描、侦查和探测，以发现潜在的安全漏洞和攻击目标； |
| 支持超时登出，当登录数据库后一定时间不操作时，自动断连。 |
| 敏感数据脱敏 | ▲支持数据脱敏，可通过自定义脱敏策略，实现通过运维工具进行数据访问时，部分字段可返回脱敏后的结果；应当支持对敏感类型进行自定义分段处理；脱敏算法至少支持空值、随机映射、遮盖、加密等。**（提供功能截图并加盖供应商公章）** |
| 误操作恢复 | 支持误操作恢复，可在永久时间段或指定时间段内记录误操作的时间、数据库名称、SCHEMA、对象名称、SQL语句、恢复状态等信息；支持设置误操作前的数据保留时间；支持对DROP、Truncate类型的操作进行一键恢复。 |
| 工单管理 | ▲提供工单申请功能，可通过工单针对数据库登录、访问授权、自定义SQL执行、高危SQL执行等操作进行在线申请；工单采用逐级审批机制；实时展示待办工单审批状态。**（提供功能截图并加盖供应商公章）** |
| 申请人员提交工单申请后，支持通过预先设定好的审批流程，根据工单申请涉及的不同数据库，流向不同的审批人员。 |
| **备注** | **“▲”项为重要技术参数要求，具体见“评审方法及标准”；无标识项为其他技术参数要求，具体见“评审方法及标准”。** | |