**上海海事大学数据库行为记录服务技术要求**

**一、功能要求**

数据库一般储存着各种重要信息。在日常生产和运维过程中，面临大量查询、修改等访问和操作，也面临着外部网络针对数据库漏洞的攻击行为，敏感数据存在通过生产环境泄露的风险。

主要的风险概述：

 管理风险：人员的职责、流程有待完善，操作不规范；

 技术风险：系统安全漏洞、补丁的更新慢；

 事后追溯：数据库违规事件出现却无法有效追溯和行为记录。

为了有效监管数据库行为记录，现提出以下功能要求：

**1、业务系统行为记录**

应实现对多个业务系统的运行及访问进行行为记录，包括访问系统的用户、IP、访问数据、操作内容能够、访问时间分布、IP地址的网段分布等，相关内容支持可视化输出。

**2、数据库操作行为记录**

应能够对所有数据库操作进行详细行为记录，记录操作者、操作时间、操作对象以及操作命令等内容，为安全事件的处置提供依据，主要包括：

1. 建立、修改、删除数据库（包括数据表、视图、过程、索引、函数, 数据库链接）
2. 对数据库进行数据的插入
3. 对数据库进行数据的删除
4. 对数据库进行数据的修改
5. 对数据库进行数据的查询
6. 数据库环境参数设置
7. 数据库及用户权限修改
8. 用户登录行为

**3、统计分析**

支持对过往的行为记录数据进行统计分析，并支持可视化报表输出。

**二、技术指标**

|  |  |  |
| --- | --- | --- |
| 数据库类型 | 支持的数据库类型 | 支持oracle、SQLserver、MySql、postgreSQL、MariaDB等数据库行为记录。 |
| 业务系统兼容 | 支持java web环境下的业务系统，可以将业务系统三层关联行为记录。 |
| 行为记录能力 | 行为记录要素 | 执行人who：行为记录到前端的应用用户、数据库用户名、主机名称、操作系统用户等。 |
| 执行内容what：具体的操作，访问的数据库、表、列、字段、包、存储过程、函数、视图。 |
| 执行时间when：每个操作发生的具体时间，操作时间、登录时间等。 |
| 执行地点where：操作的来源和目的，包括IP地址、用户名、数据库类型。 |
| 执行方式how：通过哪些客户端应用程序或第三方工具执行的操作，如：DDL、DML。 |
| 影响范围（影响行数）Range：该操作执行的影响范围，如查询、修改或删除的记录行数。 |
| 执行结果ResultSet：执行成功与否的结果以及返回结果集，如查询操作的返回内容。 |
| 复杂SQL语句支持 | 准确行为记录长SQL语句。 |
| 有效分割、准确行为记录多SQL语句。 |
| 准确行为记录绑定变量的SQL语句。 |
| 告警能力 | 告警策略 | 支持敏感语句告警策略。 |
| 自定义添加敏感语句和信任语句。 |
| 根据风险操作、语句管理等模块定义告警规则。 |
| 支持高、中、低风险告警。 |
| 支持系统资源监控与告警。 |
| 响应方式 | 根据不同的安全级别采用不同的响应方式，包括记录、告警。 |
| 告警方式包括：系统界面告警、邮件、SYSLOG。 |
| 行为记录结果展现与查询 | 行为记录信息显示 | 三个纬度的导航：会话维度、风险纬度、sql分布。 |
| 操作记录的信息：行为记录结果中包括：告警级别、事件发生时间、客户端IP、目标数据库IP、操作类型、客户端MAC地址、客户端端口号、返回状态、结果信息、客户端执行命令等详细信息内容。 |
| 报表统计分析 | 统计信息 | 所有数据库访问行为，触发报警策略的报警信息并根据风险等级进行报警信息展示。 |
| 所有对数据库的操作行为按客户端访问、账号访问、账号使用、客户端工具使用进行分析。 |
| 支持所有对数据库的DML操作、DDL操作进行统计分析。 |
| 支持全部报表信息导出,报表导出PDF格式。 |

**服务保证期内要求**

供应商在服务质保期内应当为采购人提供以下技术支持服务：

电话咨询：成交供应商应当为用户提供技术援助电话，解答用户在使用中遇到的问题，及时为用户提出解决问题的建议。

现场响应：用户遇到使用及技术问题，电话咨询不能解决的，成交供应商在2小时内采取相应响应措施；无法再2小时内解决的，应在8小时内派出专业人员进行技术支持。

**三、资质要求**

报价单位需通过公安部信息安全产品检测中心的检验检测报告。

**四、服务要求**

提供一年内不少于6次的现场服务。

**五、培训要求**

提供一次免费培训，确保学校相关运维人员掌握应用软件进行数据库行为记录作业。