中安星云
Interstellar Security

中安星云
数据库审计系统

DATABASE AUDIT SYSTEM

产品介绍

中安星云数据库审计系统具备性能高、数据库支持种类多、协议解析精确等优势，集多核多线程并行处理、精准协议解析、海量日志存储和检索等技术于一身，旁路部署在网络中，提供三层关联审计、数据库漏洞检测、数据库发现等功能并生成合规报告，便于事故追根溯源，提高数据资产安全。

产品价值

安全事件追溯、事后回放定责

提供基于语句、客户端、IP、数据库用户、关联用户、时间、影响行数、操作对象等多种维度的数据库操作记录和事后分析能力，为用户提供稳定可靠的事后追溯的依据和来源，帮助用户有效定位到业务工作人员，从而为安全事件定责。

监控访问行为、违规及时告警

提供数据库风险告警能力，对于 SQL 注入、数据库漏洞攻击、批量数据下载、高危 SQL 语句等风险行为，提供实时告警功能。

提供短信、邮件、SNMP、Syslog 等多种告警方式。

可视化状态监控、协助调优

提供直观的展现数据库运行状态、数据库连接情况、SQL 语句分布、TOP10 语句等信息，协助用户针对性的进行调整优化、提高数据库可用性。

满足合规要求、输出合规报表

提供满足《网络安全法》、《网络安全等级保护基本要求》、《涉及国家秘密的信息系统分级保护技术要求》、《企业内部控制基本规范》等法律法规的相关要求的安全审计报表，协助用户快速通过相关测评。

产品优势

全面审计、防止漏审

通过可配置的主机探针技术实现了访问数据库行为的流量捕获，从而实现了对数据库访问流量的全方位捕获。

精准识别、准确解析

基于精确 SQL 语句协议识别、解析和三层关联技术，提供更准确的数据库审计记录，为可信审计溯源提供了坚实的基础。

高效存储、快速分析

创新的采用非结构化的存储方式，1T 硬盘可以存储 20 亿到 30 亿条日志；同时配合海量日志存储分析检索技术，实现了数据亿级数据秒级检索和分析。

日志脱敏、简单易用

提供业务翻译能力，有利于非专业人员查看，可以用其它内容或符号代替日志中存在的敏感信息，防止敏感数据的泄露，旁路镜像部署无需修改网络环境。

主要功能

01 数据库兼容性

支持 oracle、mysql、DB2、Sybase、达梦、南大通用、人大金仓、浪潮 KDB 等数据库的安全防护。

02 三层关联审计

三层关联审计，能够实现完整的业务审计。可以完成从真实用户访问应用程序、应用程序访问数据库之间的行为进行关联。能够将真实用户计算机 IP 地址、登陆的用户名、数据库 IP 地址、SQL 语句、访问发生的时间等信息记入审计日志，从而定位到网络中具体的人，实现全方位的立体审计。

03 本地审计

系统针对数据库与应用在同一服务器、直接在数据库本地进行的操作也给出了解决方案。

04 超长语句审计

支持跨包的 SQL 语句拼接功能，能够完整解析与审计超长 SQL 语句（超过 65535 字节），屏蔽逃逸审计通道。

05 入侵检测

可以对网络中存在的 SQL 注入、缓冲区溢出、权限提升等漏洞攻击行为进行审计和告警。

06 日志模糊化

用其它内容或符号代替日志中存在的敏感信息（如身份信息、联系方式），在日志存储和检索过程中显示的模糊化后的内容。

07 日志报表

具备强大的报表模板以及可定制的客户化报表，满足不同层次用户的需要。可提供 DPA、SOX、等保、医疗防统方等行业性报表模板。

08 三权分立

采取三权分立的账户管理模式，实现安全管理员，系统管理员与安全审计员权限分离，满足相关法案法规要求。

应用部署

采用旁路镜像的方式接入用户的网络环境中，具有对网络零改造、适应性高、部署方便等特点。