SINOREGAL

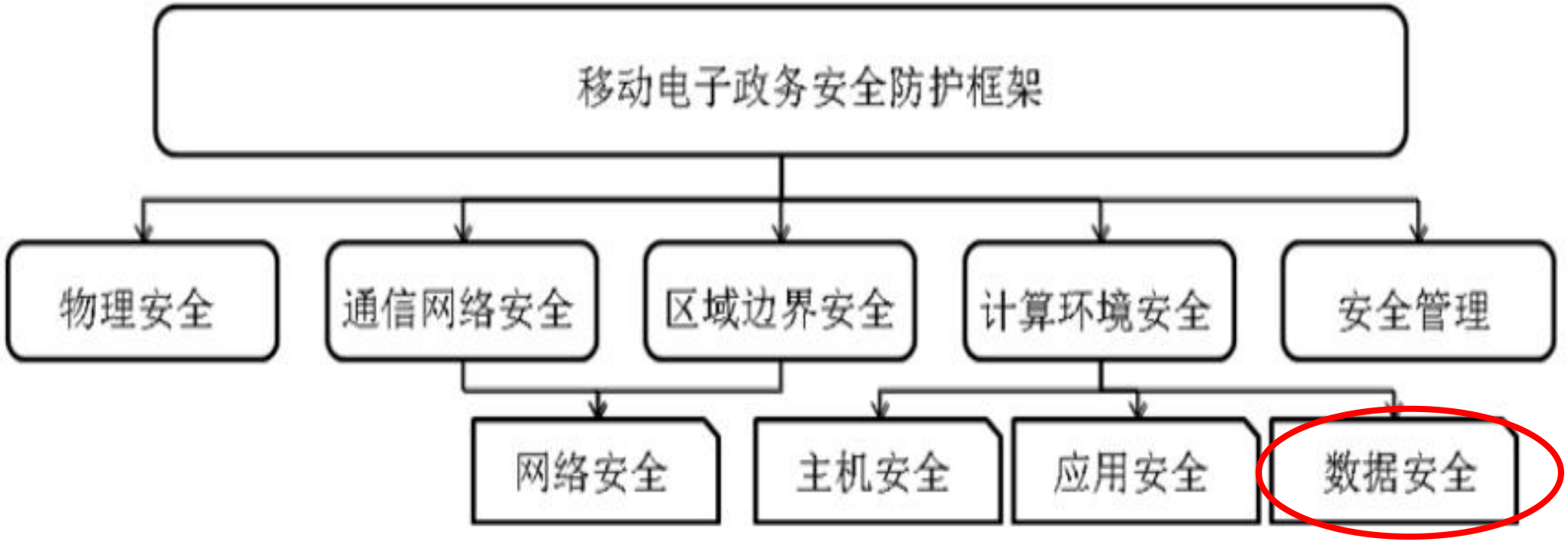
移动政务数据库安全解决方案

星瑞格软件

国有控股企业　安全自主可控

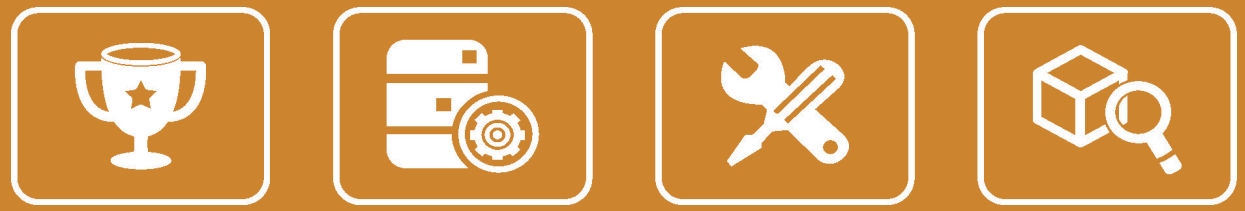
www.sinoregal.cn

2 移动政务安全保护框架



3 Agenda

- 数据安全背景
- 政策法规
- 需求及典型场景分析
- 数据库安全解决方案



SINOREGAL

数据安全背景

5 2016十大数据泄露事件--数据安全不容忽视

SINOREGAL

某电商大量数据泄露事件	大量手持身份证照片泄露事件
个人信息售卖平台化	济南20w孩童信息被出售事件
大麦网600w用户账号信息泄露	MongoDB商业用户信息泄露
某直辖市政府考试系统考题泄露	Jeep1.5w名车主信息泄露事件
某银行200多w公民信息被转卖	OpenSSL“水牢漏洞”

没有数据安全，就没有客户的持续信任，就没有企业生存空间

500多万条公民信息被泄露引诈骗与催债

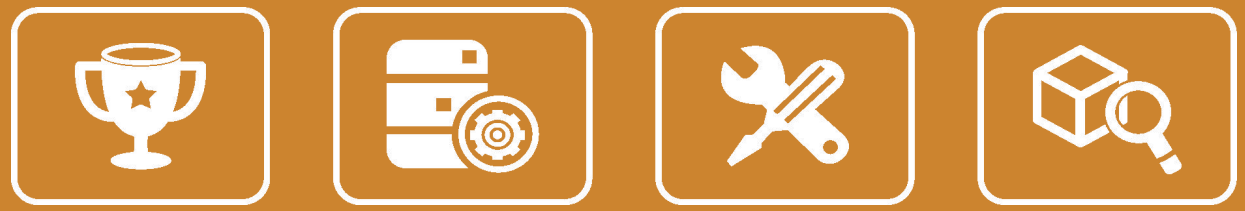
——梅州大埔警方率先打响“安网11号”侵犯公民个人信息案集群战

发布日期：2017-08-24 浏览次数： 来源：梅州市公安局

文章摘要： 近日，梅州大埔警方在广东省公安厅网警总队和广州市公安局相关部门的大力支持下，正式打响了大埔县公安局开展严打整治网络犯罪专项行动的首场跨区域集群战役，成功打掉侵犯公民个人信息团伙1个，抓获利用公民个人信息进行催债、电信诈骗的违法犯罪嫌疑人31名，依法清查手机72部，扣押作案手机、电脑、银行卡一批，查获涉案公民个人信息500多万条。

公司“内鬼”出卖信息

在第一波出击成功收网后，侦办民警马不停蹄，连夜将犯罪嫌疑人安全带回梅州，并部署对各嫌疑人的审讯工作。经审讯，犯罪嫌疑人章某澜（男，27岁，某联通公司员工）、贾某峰（男，33岁，某电信公司员工）、钟某超（男，29岁，某电信公司员工）对利用工作上的便利，将相关个人信息有偿提供给催债公司用来催收欠款，以及转卖给茂名化州何某苏、王某雄电信诈骗团伙使用的事实供认不讳。目前，涉案10名犯罪嫌疑人已被大埔警方依法刑拘，其他涉案违法人员待处理。

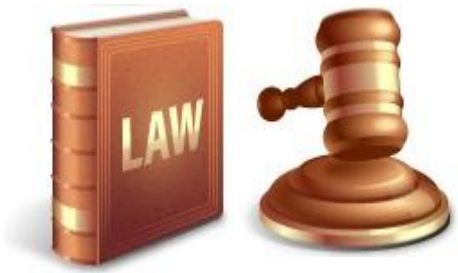


SINOREGAL

政策法规

8 信息安全日趋重要

- 随着网络安全形势的日益严峻，信息安全已提升至国家的战略高度，越来越受到关注。敏感信息在政府、企业内部处处可见，除了要阻挡外来的黑客窃取敏感数据外，内部偷盗也是一个重要数据泄露的管道。两高院更于前些日子明确了，非法出售公民个人信息获利5000元以上即可定罪，最高可判7年有期徒刑。
- 依据『信息安全等级保护管理办法』、《网络信息安全法》要求，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害者，都必需加强信息安全保护措施。
- 今年6月1日颁布并实施的《网络安全法》第三章,第二十一条明确要求：采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；



9 信息系统安全等级保护：五级


公　　安　　部
国　家　保　密　局
国家密码管理局　　文件
国务院信息化工作办公室
公通字[2007]43 号

第七条 信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。
第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。
第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。
第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。
第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

第一级：用户自主保护级；
第二级：系统审计保护级；
第三级：安全标记保护级；
第四级：结构化保护级；
第五级：访问验证保护级。

等级	对象	侵害客体	侵害程度	监管强度
第一级	一般系统	合法权益	损害	自主保护
第二级		合法权益	严重损害	指导
		社会秩序和公共利益	损害	
第三级	重要系统	社会秩序和公共利益	严重损害	监督检查
		国家安全	损害	
第四级		社会秩序和公共利益	特别严重损害	强制监督检查
		国家安全	严重损害	
第五级	极端重要系统	国家安全	特别严重损害	专门监督检查

10 信息系统等级保护安全设计技术要求

等级	第一级	第二级	第三级	第四级	第五级
手段	自主访问控制 身份鉴别 数据完整性	自主访问控制+ 身份鉴别+ 客体重用 审计 数据完整性	自主访问控制 强制访问控制 标记 身份鉴别+ 客体重用 审计+ 数据完整性+	自主访问控制 强制访问控制+ 标记+ 身份鉴别 客体重用 审计+ 数据完整性 隐蔽信道分析 可信路径	自主访问控制+ 强制访问控制 标记 身份鉴别 客体重用 审计+ 数据完整性 隐蔽信道分析 可信路径+ 可信恢复

按上表中，可以非常直观的看出：第二级以上即具备审计要求

每一个级别的安全保护措施都比上一级别有所加强，手段有所增加，而且这种增加还不仅仅是手段种类的增加。

对于相同的手段，在不同级别中还有不同的定义，表中每个手段后面的“+”就表示相同手段有增加的要求。

法规要求-基本法

SINOREGAL

《中华人民共和国网络安全法》**2017年6月1日正式实施**

- 第一部网络安全“基本法”
- 提出了个人信息保护的基本原则和要求
- 重点保护关键信息基础设施
- 将原来分散在法规、规章中的规定上升到人大法律层面，并且加大惩处力度
- 监测预警制度化、法制化

第十七条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：
（三）采取记录、跟踪网络运行状态，监测、记录网络安全事件的技术措施，并按照规定留存网络日志；
（四）采取数据分类、重要数据备份和加密等措施；

第三十六条 网络运营者对其收集的公民个人信息必须严格保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。网络运营者应当采取技术措施和其他必要措施，确保公民个人信息安全，防止其收集的公民个人信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施，告知可能受到影响的用户，并按照规定向有关主管部门报告。

第四十五条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

法规要求-”十三五”国家信息化规划

《国家信息化发展战略纲要》 《“十三五”国家信息化规划》

•是对《国家信息化发展战略纲要》的细化落实

•强调信息安全与发展并重

• “信息安全等级保护制度” 得到全面落实

•党政机关信息系统安全防护。

•互联网企业数据监管、数据安全为主攻方向
加强数据安全保护，实施大数据安全保障工程，建立跨境数据流动安全监管制度

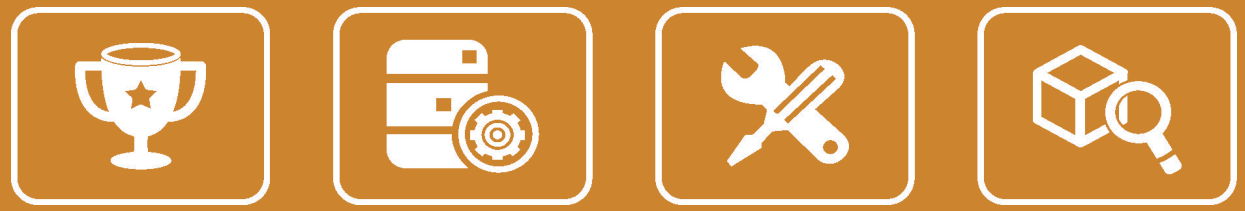
•建立关键信息基础设施安全防护平台，强化安全监管、综合防护
组织实施信息安全专项，建立关键信息基础设施安全防护平台，支持关键基础设施和重要信息系统，整体提升安全防御能力

13 严厉的法律制裁

最高院和最高检：非法出售公民个人信息获利5000元以上即可定罪，最高可判7年有期徒刑

2017年5月9日上午，“两高”发布《最高人民法院 最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（以下简称《解释》），自2017年6月1日起施行。《解释》一共13条，明确了“公民个人信息”的范围、非法“提供公民个人信息”的认定标准，以及侵犯公民个人信息罪的定罪量刑标准，等等。

其中比较醒目的是，违法获取、出售公民个人信息获利5000元以上即被认为情节严重，可判3年以下有期徒刑或拘役；造成被害人死亡、重伤、精神失常或者被绑架等严重后果的，造成重大经济损失或者恶劣社会影响的，即被认为情节特别严重，可判3-7年有期徒刑，并处以罚金等。



SINOREGAL

需求及典型场景分析

需求分析

当前电子政务信息系统中的涉密数据在数据库集中存储，保存了大量公民个人敏感信息、政府机关，企事业单位机密信息，传统的信息安全解决方案不能对数据安全提供全面的保护，主要体现在缺乏有效追踪手段，不能发现泄密源头，不能厘清责任：

- **传统防护薄弱**
- **安全配置缺陷**
- **外部黑客攻击**
- **内部违规操作**
- **安全取证困难**

政策性要求

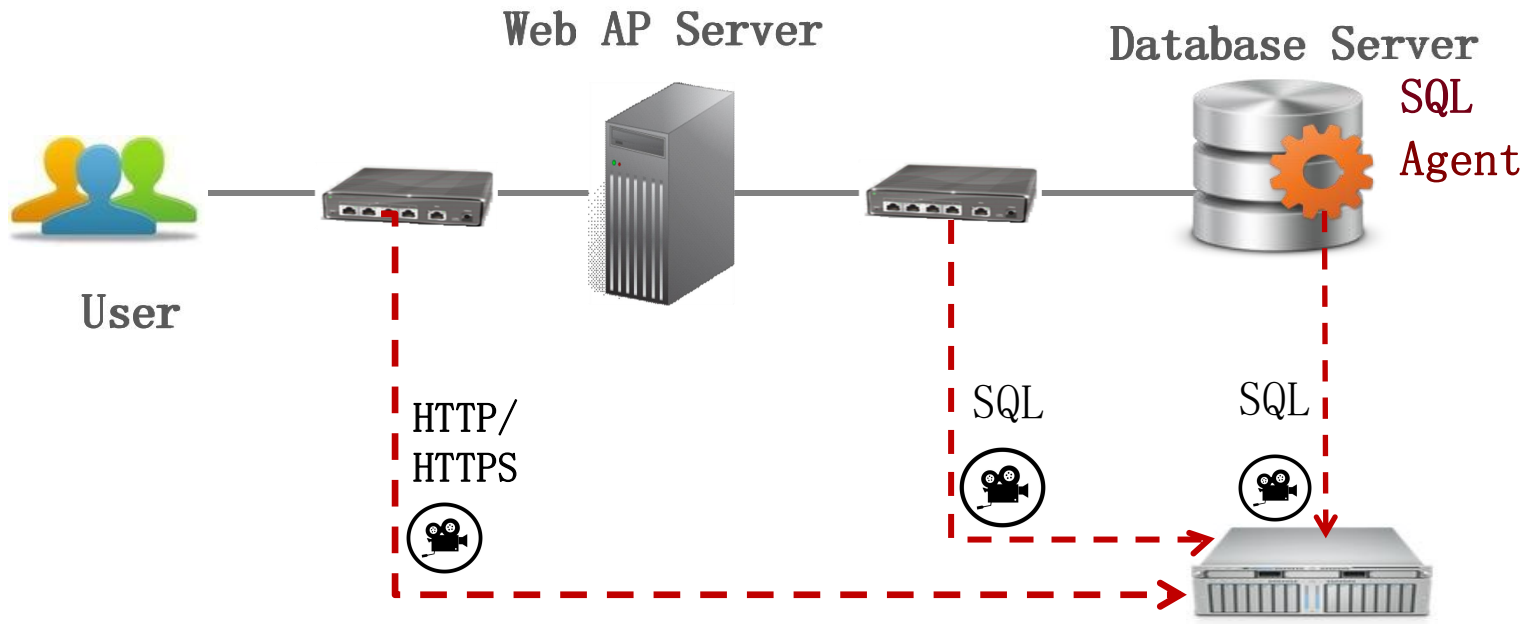
- 电子政务需要符合国家颁布的相关等级保护要求，其中对数据库系统的访问行为监控、审计、安全事件报警等方面提出了明确的安全防护要求。

数据库安全审计的基本概念

金库 —— 数据库

运钞 —— 应用访问数据库

数据库安全审计系统架构



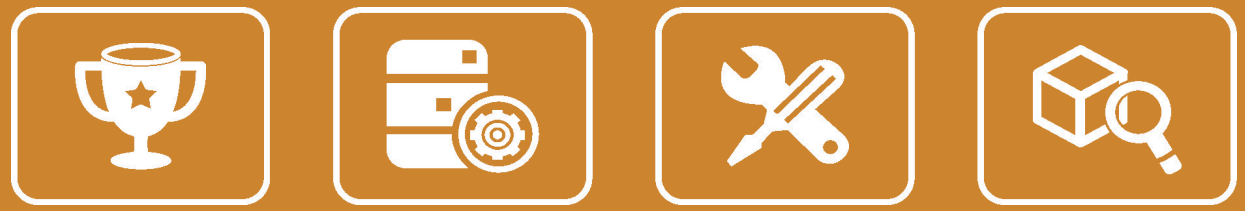
场景和解决手段举例分析

SINOREGAL

- 场景一，能否知道谁查询过个人的敏感信息（领导的信息、重点管控人员...）？
  - 需求：要求定位出是谁通过业务系统查询了个人的敏感信息。因为查询的人通过应用系统来做查询，以往只能审计数据库操作，通过应用做的操作无法区分应用端的用户是谁，因此无法定位真是的操作者是谁。
  - 关联应用和数据库访问流量的参数并进行智能匹配，将应用层和数据层访问打通，还原完整路径。

- 场景二，利用网页漏洞，反复高频操作；批量导出大量的用户信息，提供给不法分子
  - 需求：要求能按用户区分访问操作次数，按查询返回查询笔数（达到限定值）筛选数据或进行报警。
  - 识别用户重复操作的次数和记录数，如果达到阀值将报警

- 场景三，绕过实名制认证流程，违规进行操作。
  - 需求：对于绕开正常路径访问数据库，应用服务的行为能进行捕获和报警。
  - 通过设定数据库、应用服务的合法访问路径。一旦有非常规路径进入的服务调用，数据库（到表、语句、参数等）访问即可报警。



SINOREGAL

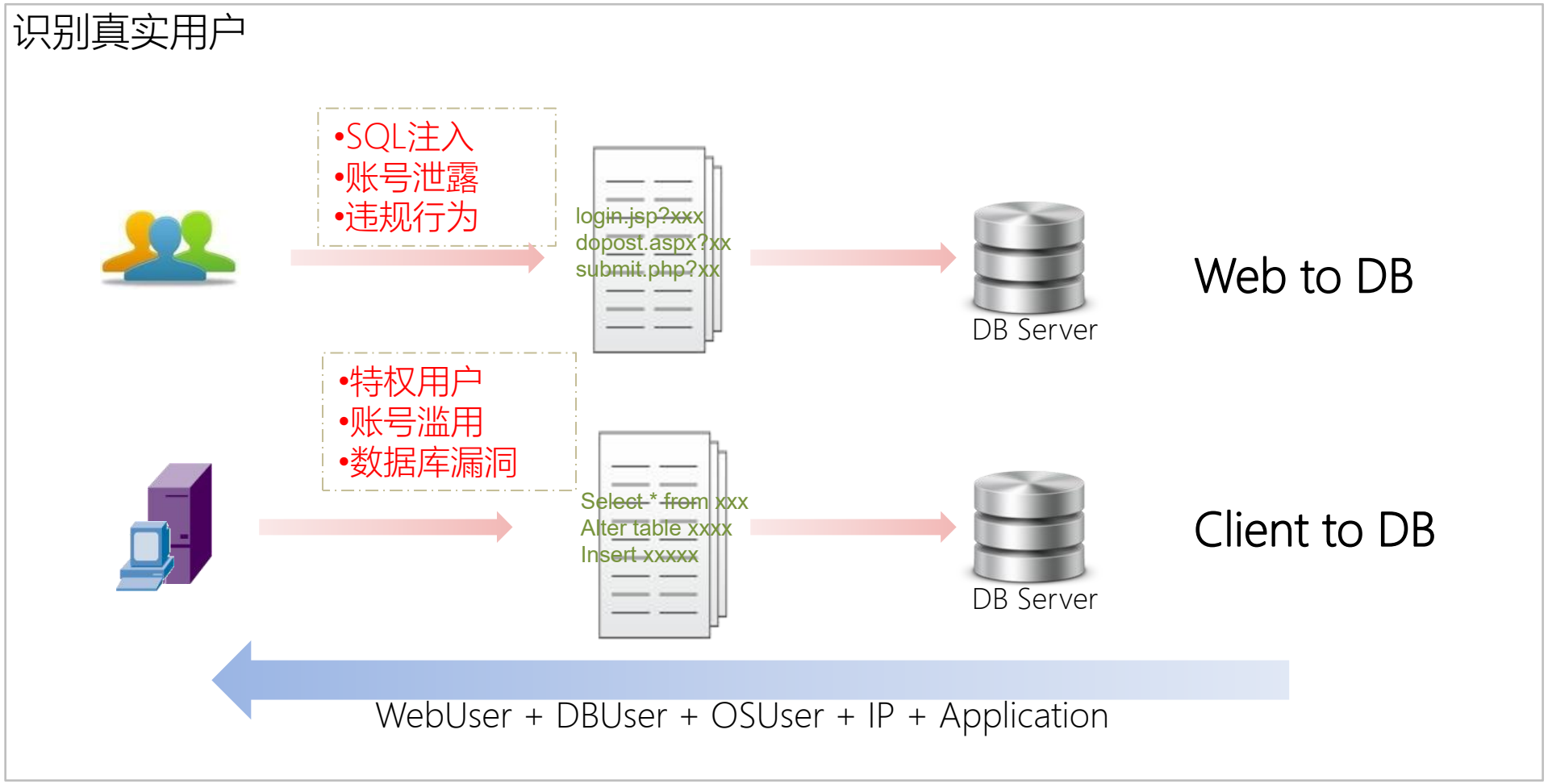
数据库安全解决方案

事前/事中/事后的全程数据安全防护

- 数据库全程监测与审计系统 — 对数据全程审计，提供预警和预测功能（事中/事后审计和警告）
- 服务器访问控制及权限管理系统 — 从操作系统层管控敏感数据的访问权限管理和命令执行权限管理（事前/事中阻断）

对数据的保护可以从两方面着手，一个是从数据库审计的角度，监控与记录数据库的访问，另一个是从操作系统层管控敏感数据的访问权限，对敏感数据做到审计加上保护，不仅可以防堵黑客窃取敏感信息，也可以阻止内部人员盗卖信息。

21 端到端全程审计



全程审计记录，精准定位风险源头，精准识别操作对象，精准关联风险线索

22 多层审计,Web User Matching

http://xx.com.cn/abc.asp?use=**fred@pqa.com**

Web/Application Server

Select * from …
Insert …
Update …
Delete …

Database Server

dbAudit

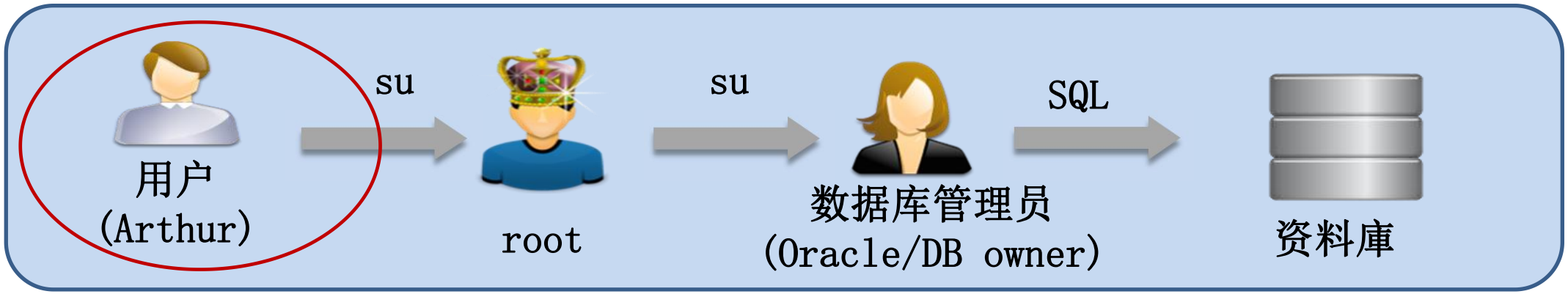
Web Matching Technology -SQL-Web Pattern Relationship Discovery

SQL运行时间	应用端用户	SQL语句
2014-01-03	fred	Select * from …
2014-01-03	fred	Insert …

特权用户追踪审计

SINOREGAL

- 用户隐藏身分时，执行记录应可分辨真实原始用户



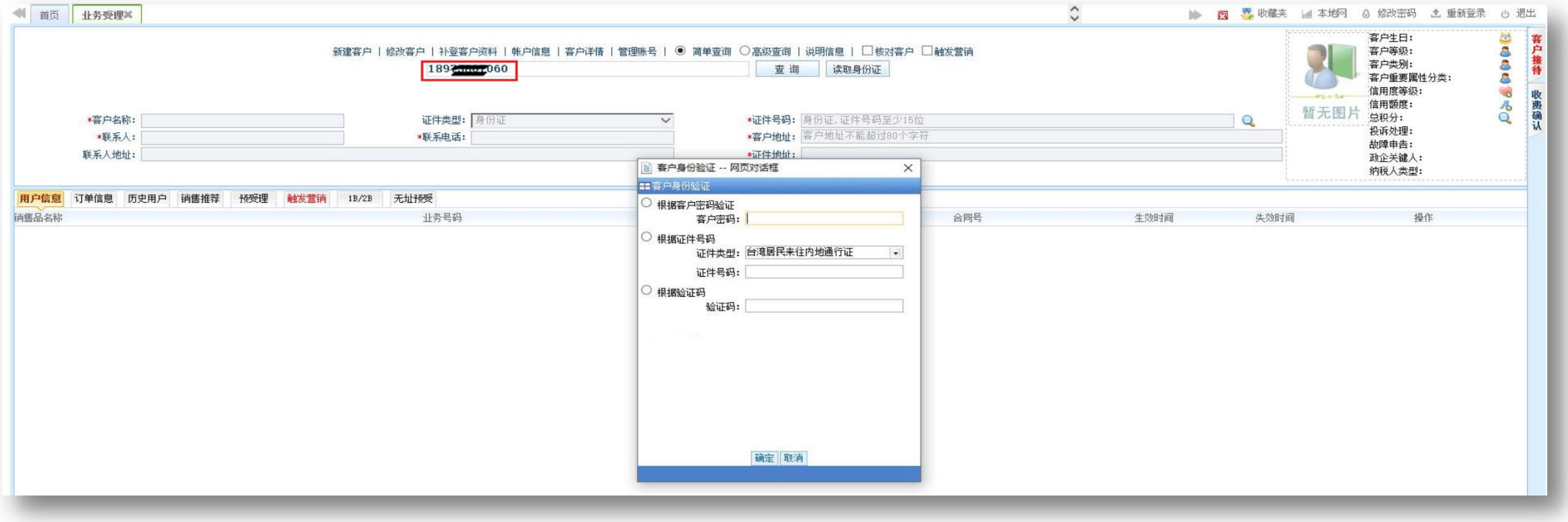
- 执行记录应可分辨是否为自动程序(cron job)或是人为执行

- 执行命令信息应完整记录(程序名称与OS指令)

24 场景一 敏感数据：谁查了我的个人信息

场景描述：

应用系统含有客户重要隐私，在办理业务的时候可能泄露身份证号码，从而被一定权限的业务员用来查询其隐私数据。用户***，身份证：430102******05148在办理业务过程中，身份证号泄露，营业员746L******可以利用其身份证号码查询该用户账户信息，而系统不会记录谁查询了这些信息，简单日志也无法作为有效依据



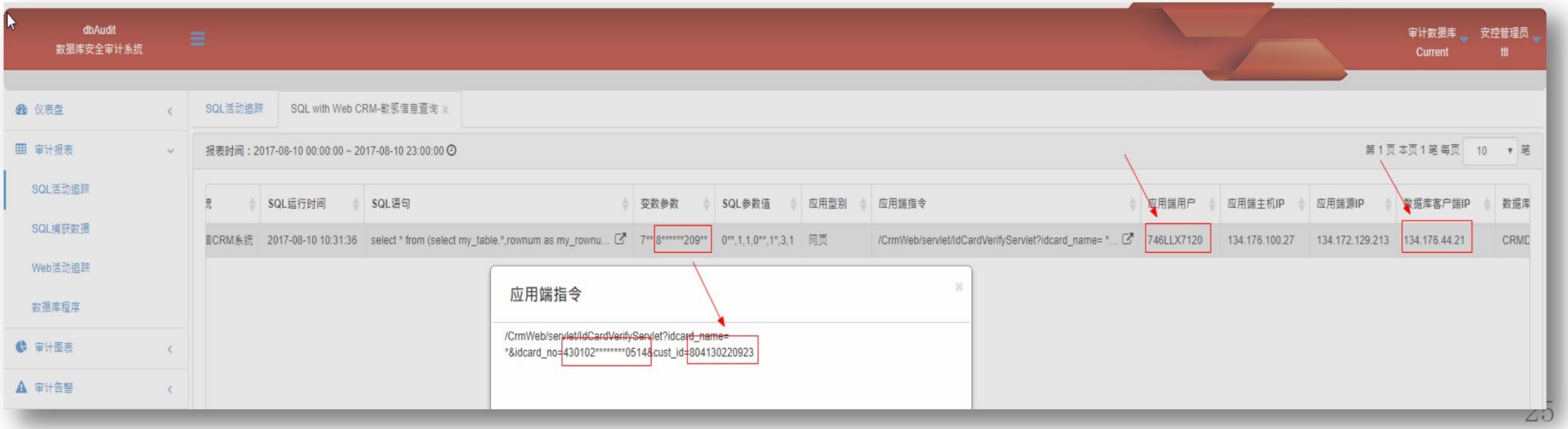
25 场景一 敏感数据：谁查了我的个人信息

■ 审计设置：

本场景中查询敏感数据的SQL语句，以‘物’ 的分类条件设置监控报表，可查询出谁,什么时间，什么地点（IP）查询了谁的敏感信息。

■ 审计结果：

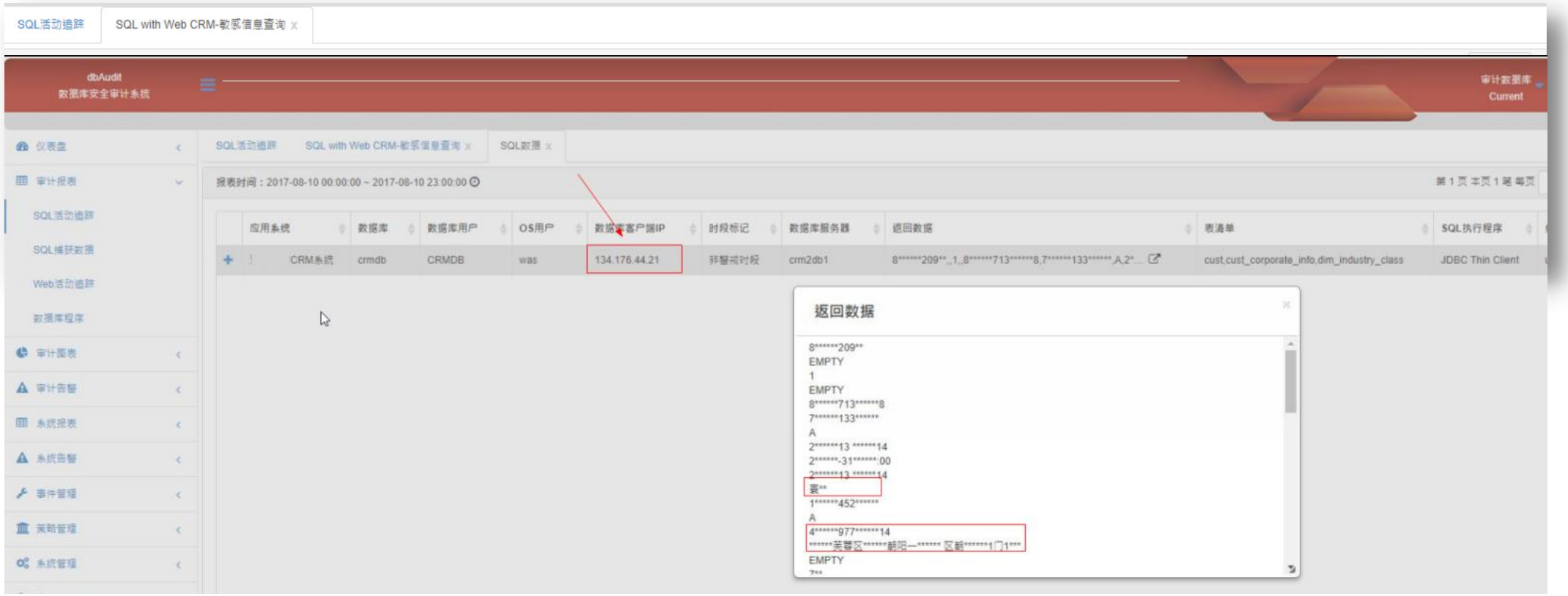
在按以上条件定制好报表后，定向查询某营业员工号，报表可以列出指定时间段其查询敏感信息的人事时地物信息



26 场景一 敏感数据：谁查了我的个人信息

审计结果：

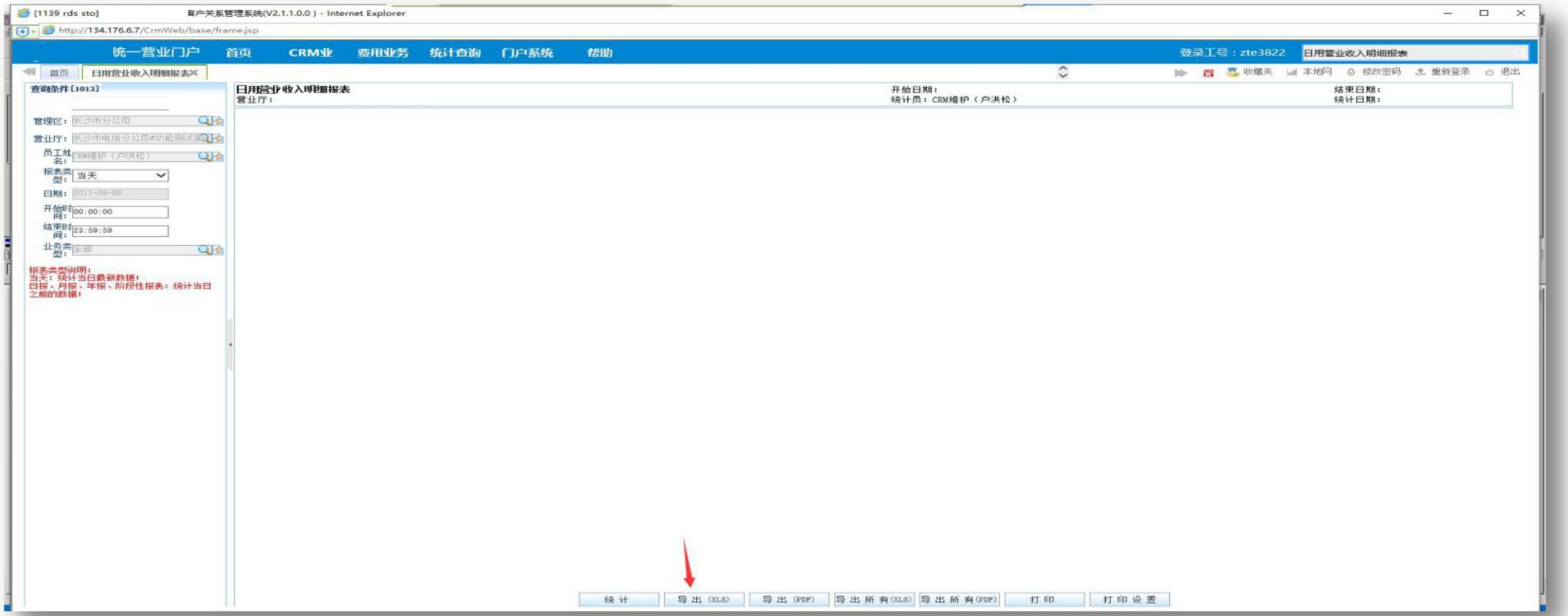
同时对于其查询了哪些客户信息，审计系统还能通过双向审计的数据捕获报表查出



场景二 高频与数据导出：谁在做高频操作或导出了大量数据

场景描述：

应用系统包含导出功能，该能力能够导出大量关键信息，比如客户信息、机密信息等。由于该功能的重要性，对终端营业员使用它导出大量数据，频繁导出数据，非营业时段导出数据需要格外关注。



场景二 高频与数据导出：谁在做高频操作或导出了大量数据

审计设置：

本场景通过以‘物’分类条件筛选应用导出功能SQL，设置SQL返回笔数较多的条件，同时设置统计重复执行次数的报表，即可审计导出量大（返回笔数多），执行频度高的活动。

审计结果：

根据设置条件和报表内容可以看到该报表含义是用户733Z****32在同一分钟里面连续执行了四次大笔数的报表查询导出动作，其中各有两笔是重复操作。可以设置阈值条件来告警，当某账户警戒时段反复查询导出数据时告警。

29 场景三 定向：谁在做异常流程操作

场景描述：

应用系统访问数据库的正常流程是终端用户通过网页发送请求到应用服务器，再由应用服务器通过连接池把相应数据库访问请求通过固定数据库账号来访问数据库。应用系统会对用户访问修改数据的流程做出符合规定的控制。

但是难免有系统维护操作，打补丁等操作，会向厂商或者合作方开放一些数据库账号，相关人员可通过plsql等开发工具直接登录修改数据。

这里的人工操作存在有意或者无意的不符合规定的数据库访问修改流程。比如有可能直接修改数据库的客户信息等敏感信息，而不必通过实名身份认证的流程。

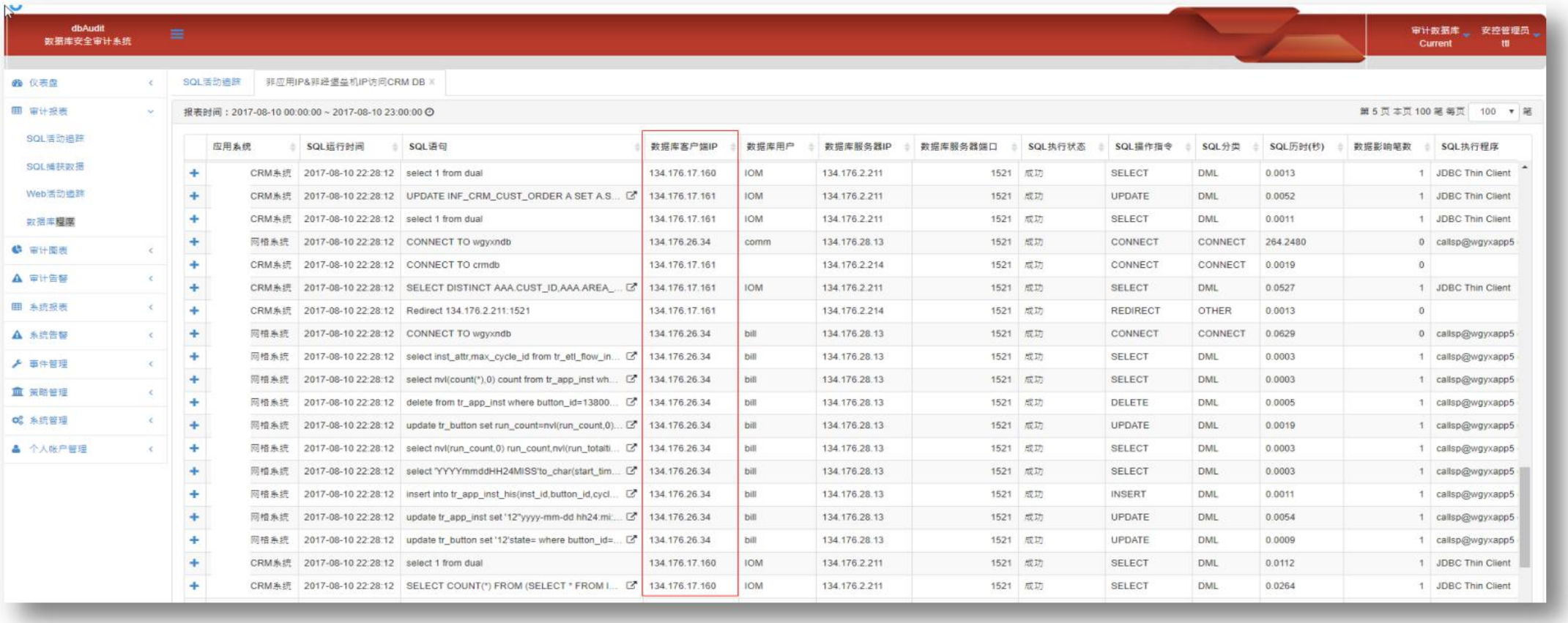
审计设置

针对这个场景，审计系统可利用分组功能，按照‘人’的分类新建所有应用访问数据库用户组，按照‘地’的分类设置所有应用服务器IP组和设置所有堡垒机防护IP组，并通过以上自定义条件分组，灵活组合设置多张报表并告警，全面监控审计这些特殊流程的操作

30 场景三 定向：谁在做异常流程操作

■ 审计结果：

报表1：列出所有不是从应用服务器和所有堡垒机地址访问数据库的活动。
根据当前的调查反馈，红色框中IP既不属于应用端IP，也不属于堡垒机防护IP。



31 场景三 定向：谁在做异常流程操作

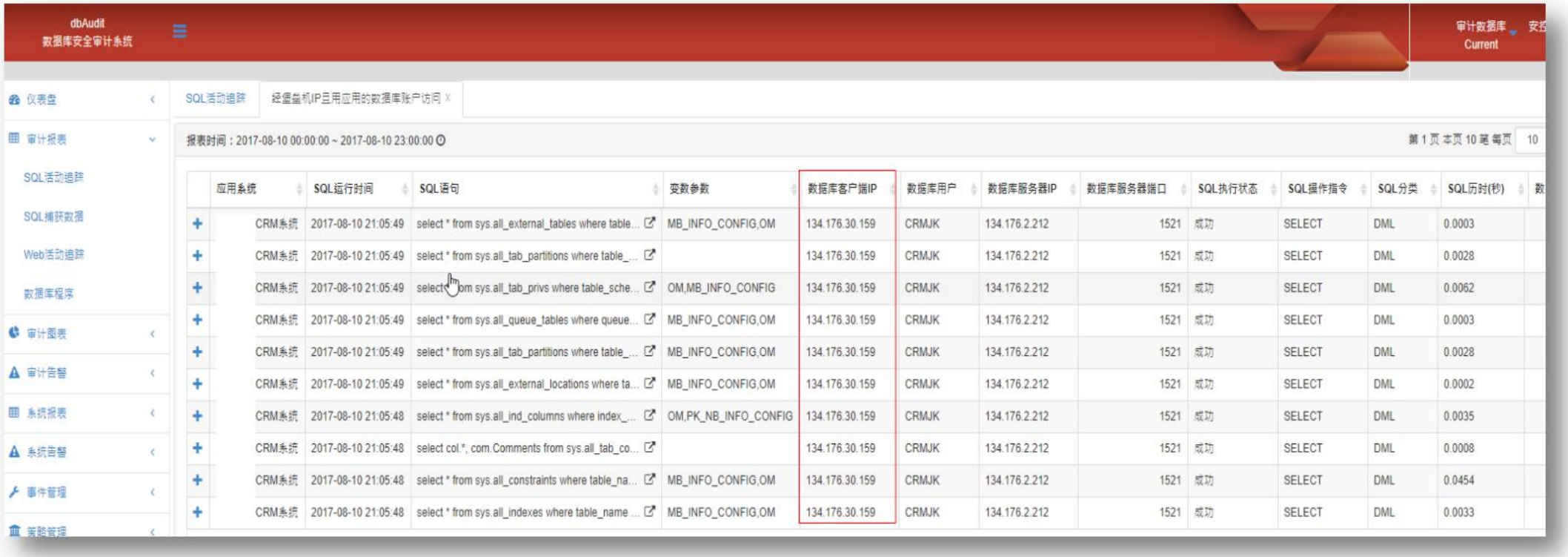
SINOREGAL

- **审计结果：**

  报表2：列出所有以应用服务器账户却不是从应用服务器IP发起访问数据库的活动。

  根据目前提供的信息。134.176.30.159不属于应用服务器的IP，却使用应用用户访问生产数据库

。



应用系统	SQL运行时间	SQL语句	变数参数	数据库客户端IP	数据库用户	数据库服务器IP	数据库服务器端口	SQL执行状态	SQL操作指令	SQL分类	SQL历时(秒)
CRM系统	2017-08-10 21:05:49	select * from sys.all_external_tables where table...	MB_INFO_CONFIG,OM	134.176.30.159	CRMJK	134.176.2.212	1521	成功	SELECT	DML	0.0003
CRM系统	2017-08-10 21:05:49	select * from sys.all_tab_partitions where table_...		134.176.30.159	CRMJK	134.176.2.212	1521	成功	SELECT	DML	0.0028
CRM系统	2017-08-10 21:05:49	select * from sys.all_tab_privs where table_sche...	OM,MB_INFO_CONFIG	134.176.30.159	CRMJK	134.176.2.212	1521	成功	SELECT	DML	0.0062
CRM系统	2017-08-10 21:05:49	select * from sys.all_queue_tables where queue...	MB_INFO_CONFIG,OM	134.176.30.159	CRMJK	134.176.2.212	1521	成功	SELECT	DML	0.0003
CRM系统	2017-08-10 21:05:49	select * from sys.all_tab_partitions where table_...	MB_INFO_CONFIG,OM	134.176.30.159	CRMJK	134.176.2.212	1521	成功	SELECT	DML	0.0028
CRM系统	2017-08-10 21:05:49	select * from sys.all_external_locations where ta...	MB_INFO_CONFIG,OM	134.176.30.159	CRMJK	134.176.2.212	1521	成功	SELECT	DML	0.0002
CRM系统	2017-08-10 21:05:48	select * from sys.all_ind_columns where index_...	OM,PK_NB_INFO_CONFIG	134.176.30.159	CRMJK	134.176.2.212	1521	成功	SELECT	DML	0.0035
CRM系统	2017-08-10 21:05:48	select col.*, com.Comments from sys.all_tab_co...		134.176.30.159	CRMJK	134.176.2.212	1521	成功	SELECT	DML	0.0008
CRM系统	2017-08-10 21:05:48	select * from sys.all_constraints where table_na...	MB_INFO_CONFIG,OM	134.176.30.159	CRMJK	134.176.2.212	1521	成功	SELECT	DML	0.0454
CRM系统	2017-08-10 21:05:48	select * from sys.all_indexes where table_name ...	MB_INFO_CONFIG,OM	134.176.30.159	CRMJK	134.176.2.212	1521	成功	SELECT	DML	0.0033

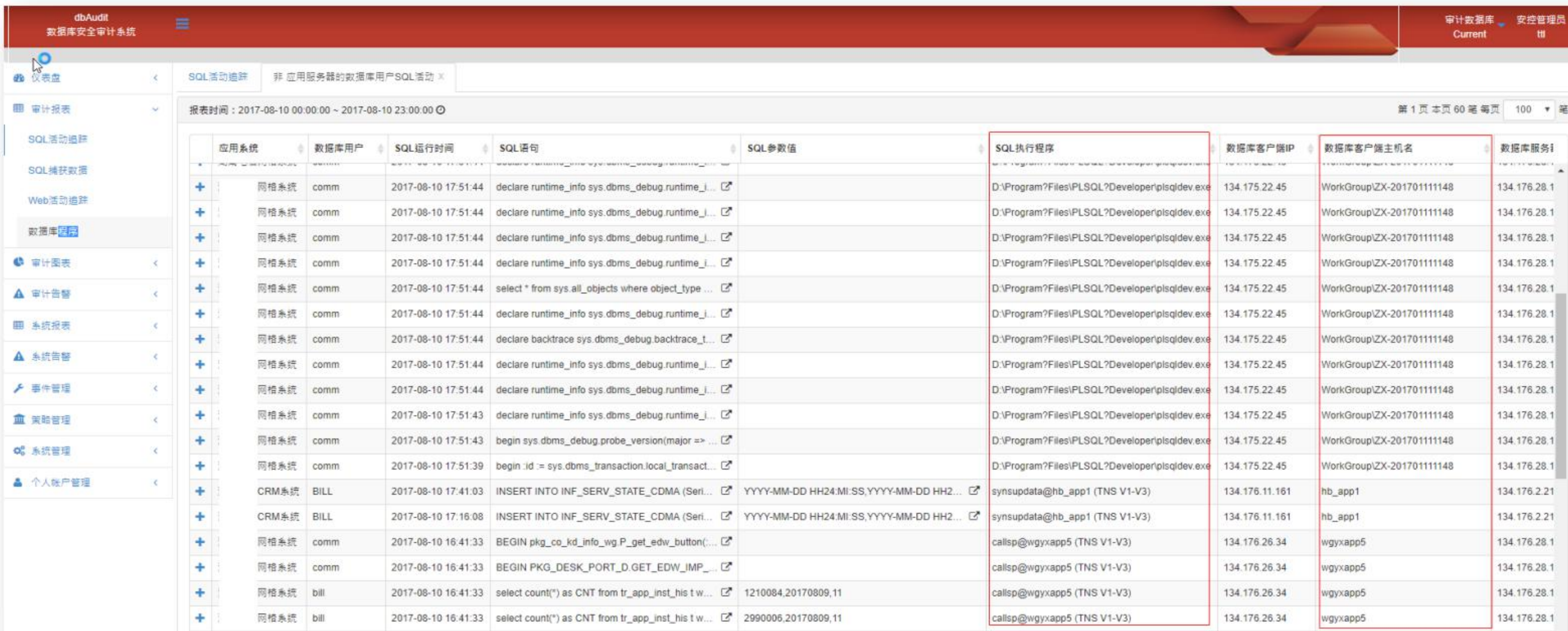
32 场景三 定向：谁在做异常流程操作

SINOREGAL

■ 审计结果：

报表3：列出所有非应用服务器账户访问数据库的活动。

报表中列出通过SQL开发工具人工访问访问数据库的活动，包括执行的SQL和结果。



数据库安全审计生命周期

SINOREGAL

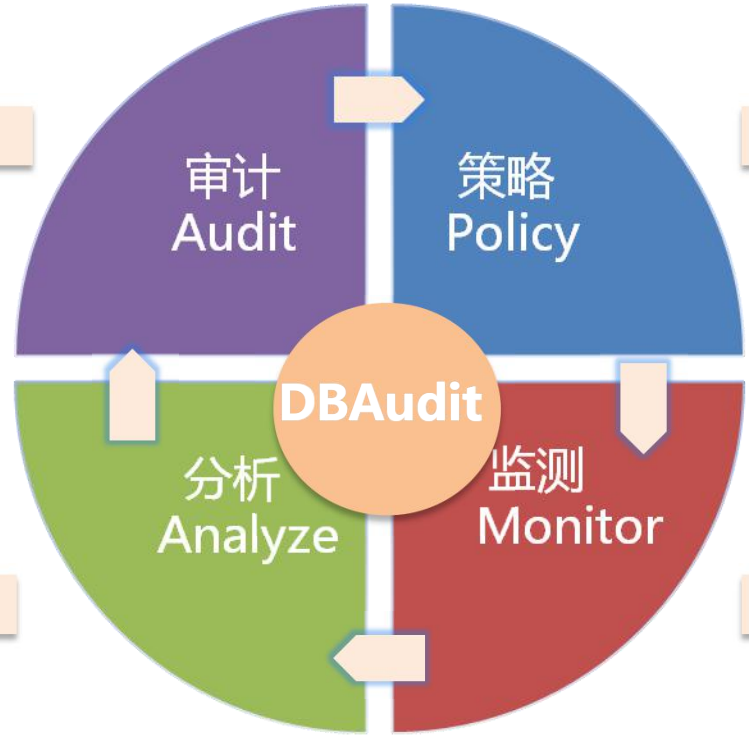
端到端全程审计

多层审计支持

Web user matching技术

智能学习策略，精准溯源

弹性架构，部署灵活



双向审计，屏蔽敏感参数

预置丰富审计策略

数字签名加密，数据不可破坏

操作简单、友好中文化支持

违规行为自动预警

SINOREGAL

谢 谢！

THANKS FOR YOUR WATCHING!

Sinoregal

福建星瑞格软件有限公司

网站：www.sinoregal.cn
邮箱：sinoregal@sinoregal.cn

福州总公司
地址：福州市鼓楼区洪山园路68号
节能大厦1号楼3层
总机：0591-86321188

广州办事处
地址：广州市天河区珠江新城兴民路
222号天盈广场西塔810室
电话：020-38063899

上海办事处
地址：上海市黄浦区福州路318号
浦汇大厦1605室
电话：021-63120198

北京办事处
地址：北京市海淀区首体南路22号
国兴大厦6层6B
电话：010-68005260