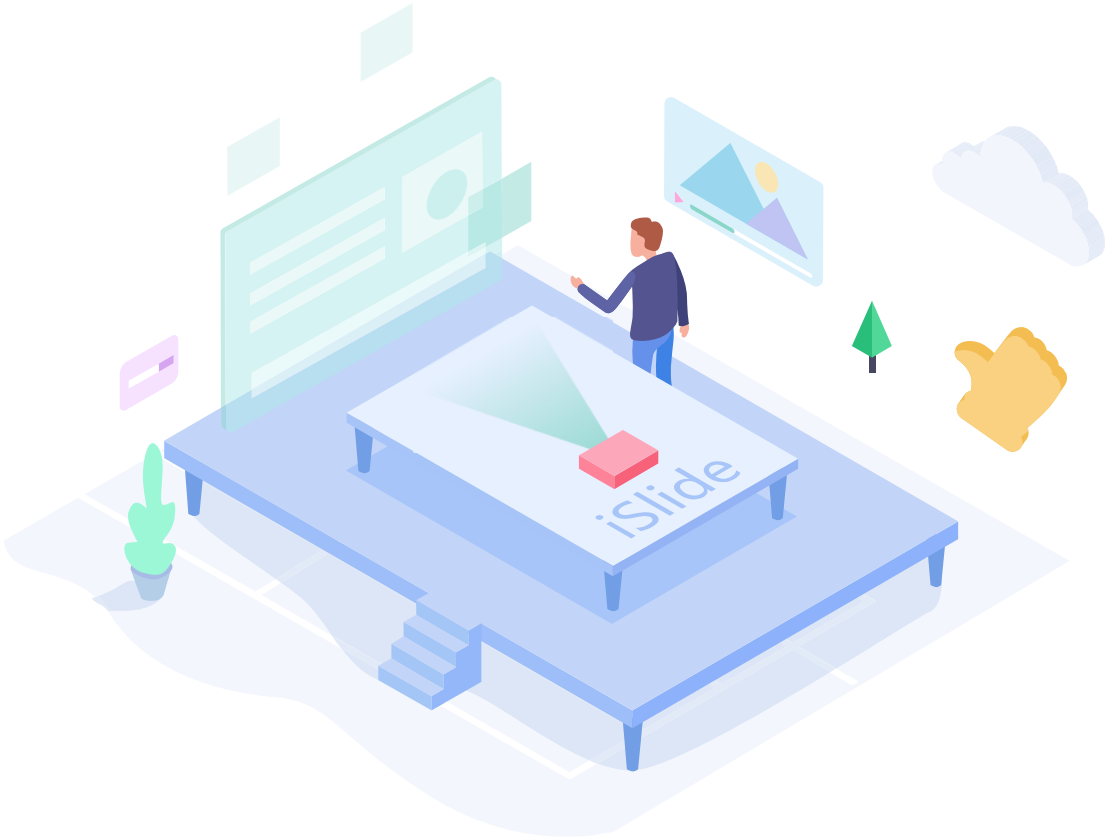
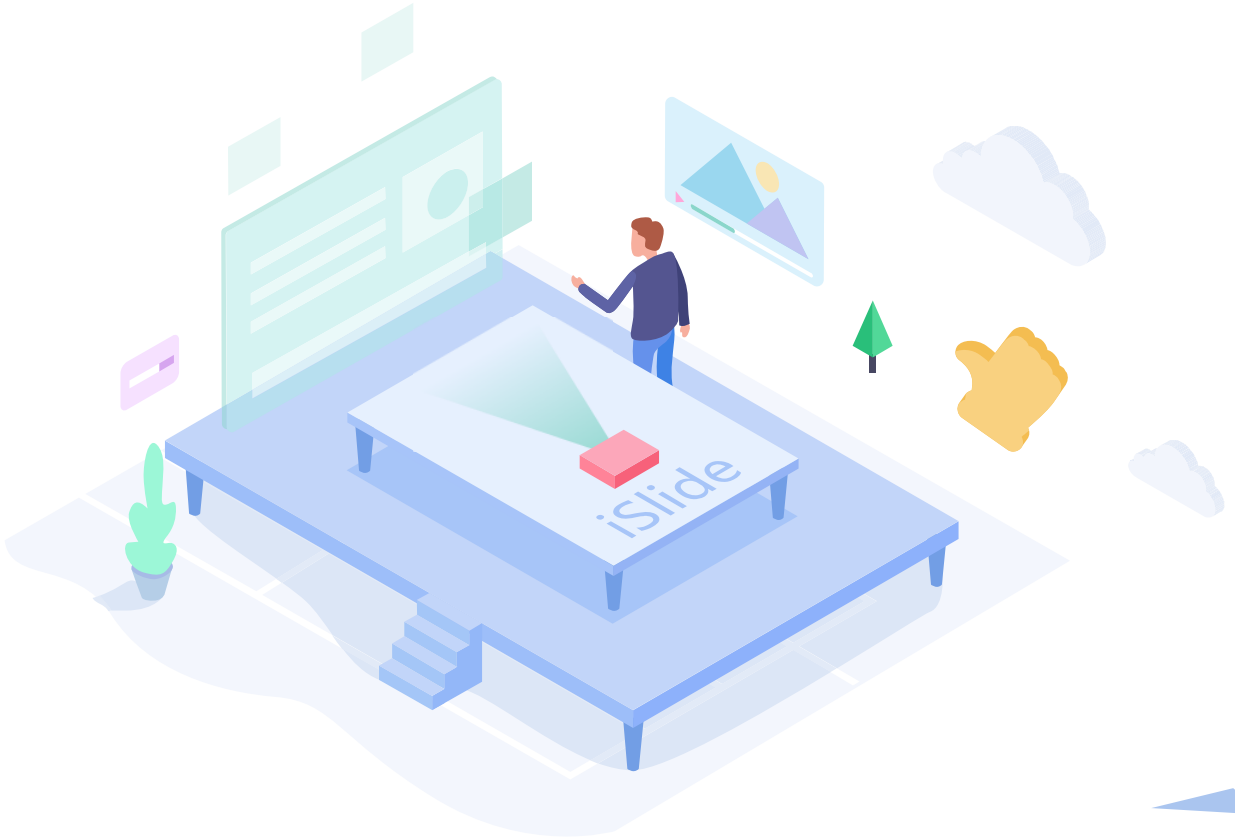


什么是安全审计

226周分享 shiyan

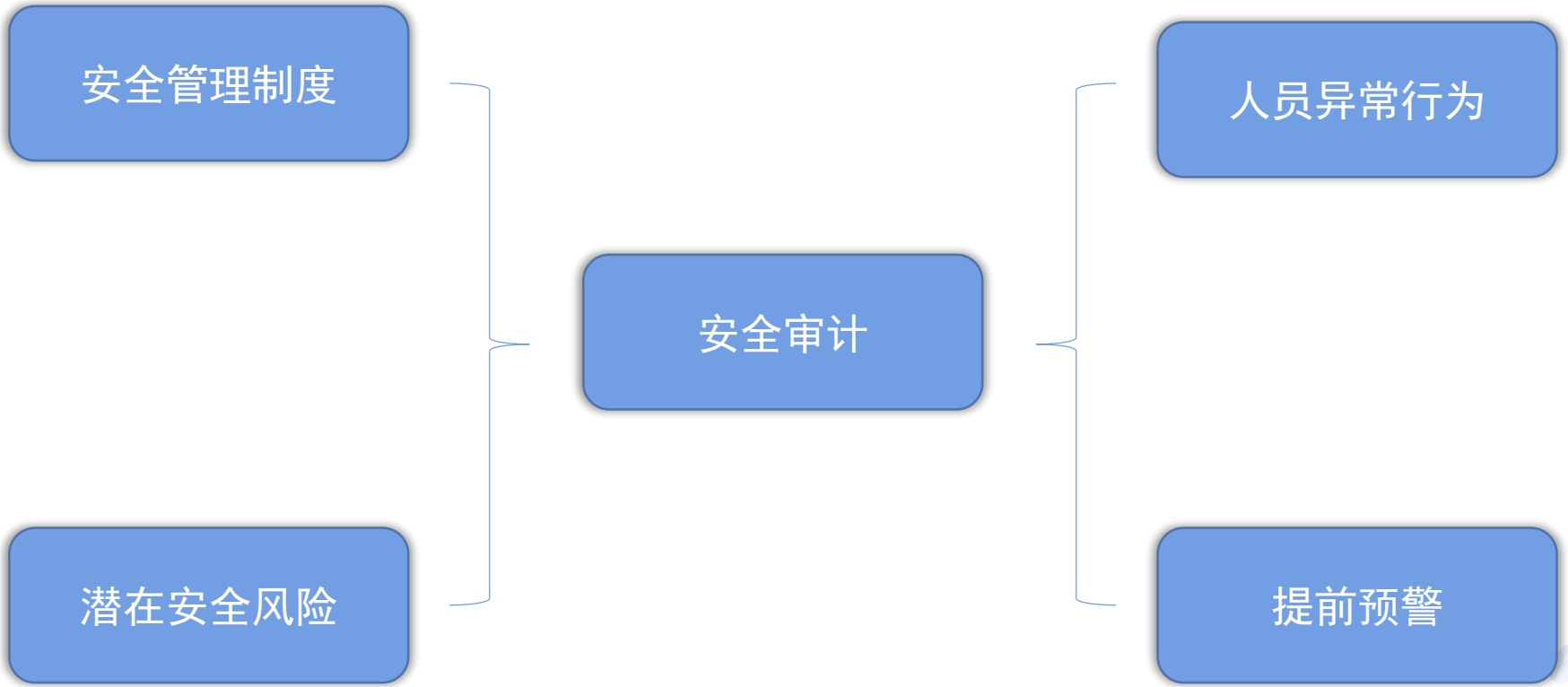
目录

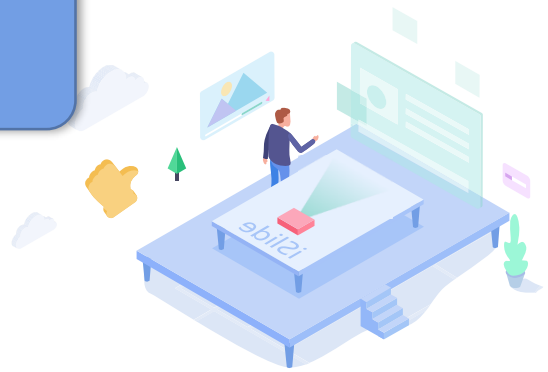
1. 前言
2. 概述
3. 审计点
4. 审计范围
5. 审计工作开展流程
6. 审计团队模型
7. 常用工具
8. 审计展望



前言

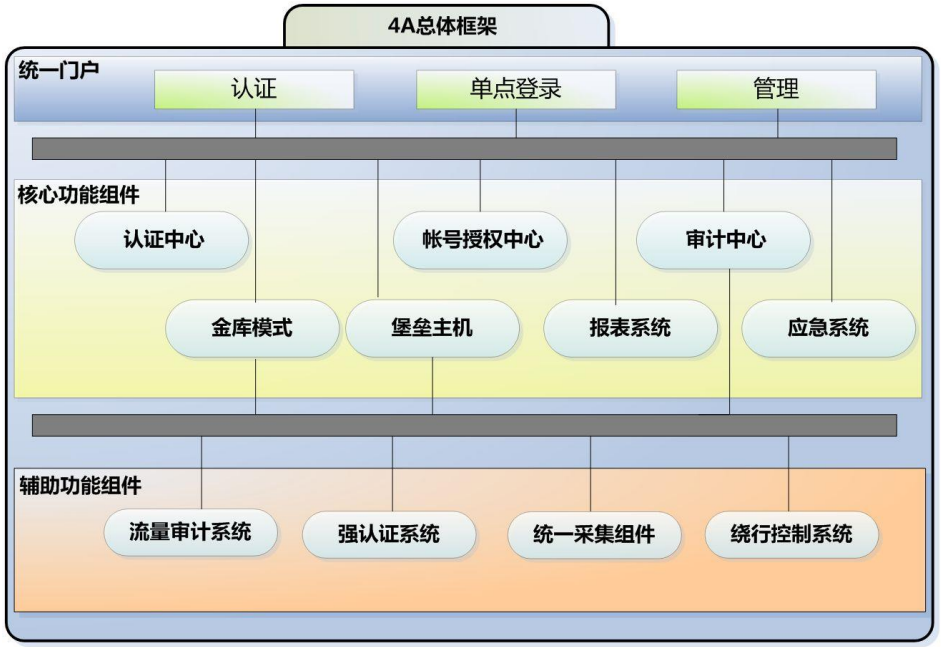
- 安全审计可能对于一个渗透测试人员是陌生的，第一反应可能会认为是代码审计？检查代码中的存在的漏洞？其实不是的，安全审计是一个体系化的建设，更多的是数据上的安全分析。

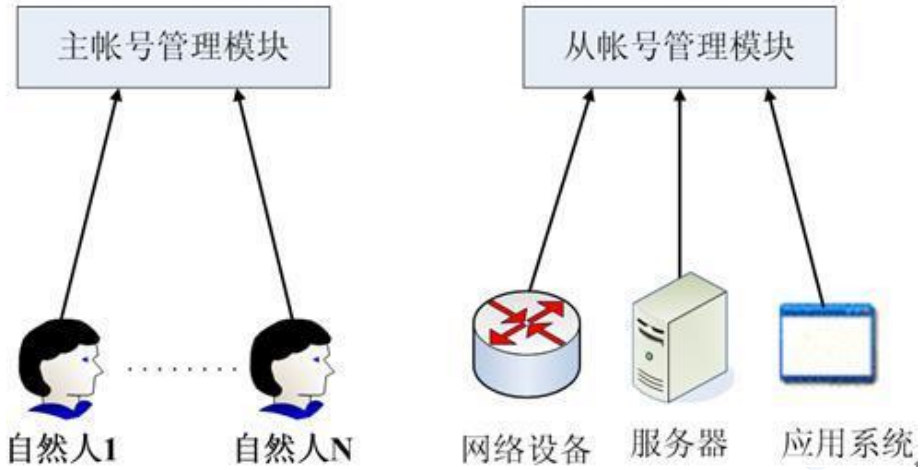




概述

- 安全审计首先需要根据现有公司业务体制，安全制度等等信息数据，建立一个功能完善的信息安全审计体系，通过与业务操作结合，人员可通过安全管理控制平台进行业务操作，授权，查询等，而相应的产生的记录，都是留存保留，实时监控，用于审计。
- 运用国内外先进的信息安全技术和审计手段，挖掘潜在的安全风险和威胁，实现对违规行为、恶意行为、异常行为等存在安全风险的行为进行核查并整改，最大限度的降低风险问题，避免风险，建设一个安全的生产环境。





审计点

- 主要以用户的操作，访问等行为为重点分析点，如果当前用户的操作与自身的权限不符或违反了相应的信息安全规章制度。
- 发现当前业务操作中，产生安全事故时，无法追责的情况，明确具体的人员职责。

- 通过分析用户的个人行为曲线，和相应的操作权限，发现是否存在异常情况，定位异常行为和核查问题。
- 建立完善的安全规章制度或挖掘现有的安全规章制度中目前可实现的审计点，进行审计，发现问题。
- 等等。。。

异常案例

J24

	A	B	C	D	E	F	G	H	I
1	业务系统	主帐号ID	从帐号	操作命令	源地址	目的地址	开始时间		
2	xxxxx	lizhonghua	shiyan	login	10.11.22.123	10.11.21.181	2019-03-30 23:25:13:437		
3	xxxxx	lizhonghua	shiyan	su -	10.11.22.123	10.11.21.181	2019-03-30 23:25:13:438		
4	xxxxx	lizhonghua	shiyan	kill 20075	10.11.22.123	10.11.21.181	2019-03-30 23:25:13:439		
5	xxxxx	lizhonghua	shiyan	pwd	10.11.22.123	10.11.21.181	2019-03-30 23:25:13:440		
6	xxxxx	lizhonghua	shiyan	ls	10.11.22.123	10.11.21.181	2019-03-30 23:25:13:441		
7	xxxxx	lizhonghua	shiyan	cat /etc/shodown	10.11.22.124	10.11.21.181	2019-03-30 23:25:13:442		
8									
9									

审计范围

- 人员安全（人员管理为主）
- 数据安全（敏感信息为主）
- 网络安全（网络秩序为主）
- 系统安全（合规行为为主）
- 应用安全（业务逻辑为主）
- 用户安全（账户管理为主）
- 终端安全（终端管控为主）

数据在手，一切皆有，盘他！！！

审计工作开展流程

- 审计目标 -> 现状调研 -> 现状分析 -> 审计分析 -> 数据建模 -> 审计结果

1、制定的具体的审计点和审计目标

2、梳理现有业务体系，流程机制

3、分析现有业务现状，规划审计项

4、数据分析，挖掘安全风险

5、现有审计场景进行数据建模，自动化，流程化

6、输出审计结果

审计团队模型

标准团队：5人

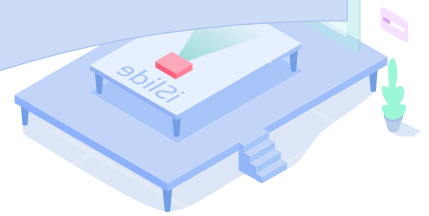
项目经理（1）
审计分析师（1）
数据分析师（1）
调研员（2）

实际情况的话

全栈团队：9人

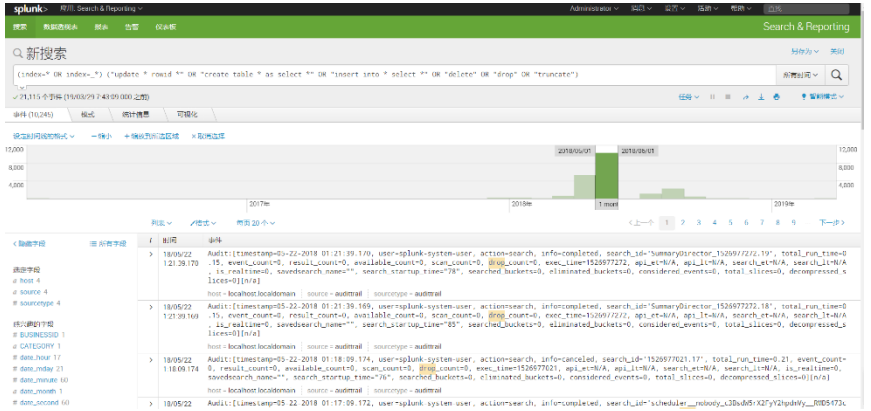
项目经理（1）
审计分析师（2）
数据分析师（3）
研发人员（1）
调研员（2）

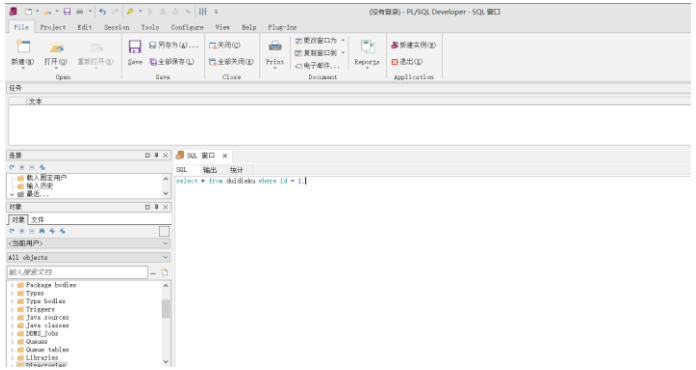
- 项目经理统领全局（决策，梳理，调研，规划，分析，研发，等等）
- 团队成员（会调研，会写分析工具，会优化审计方法和流程，会word、PPT、Excel，会数据分析，会建模，沟通能力强，问题梳理能力强，会把书本上的公式套用到实际运用中，挖掘安全问题并制定相应审计方法，思考问题闭环的方法和意识，问题本质的思考和扩展，等等）

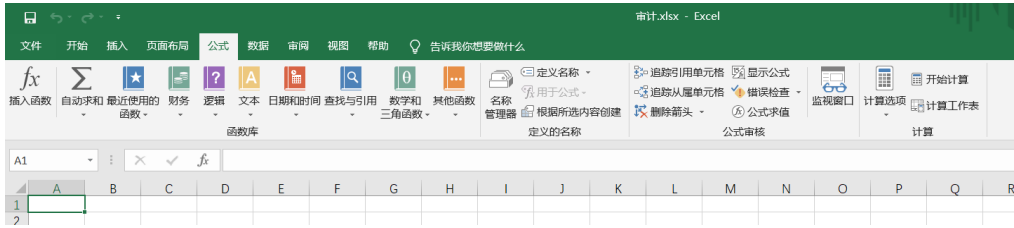


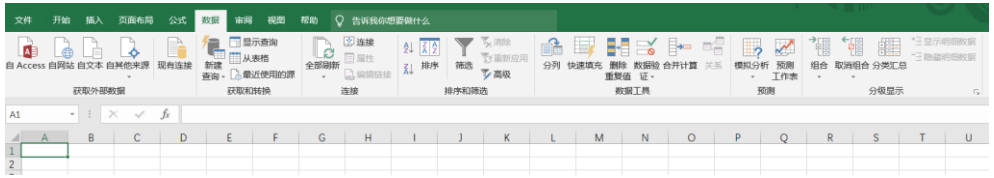
常用工具

- Splunk（重量级数据分析工具）
- 历史审计库（日常数据储存）
- Excel（小中量数据分析）
- 审计平台（自动化审计）
- Jupyter Notebook
- 等等

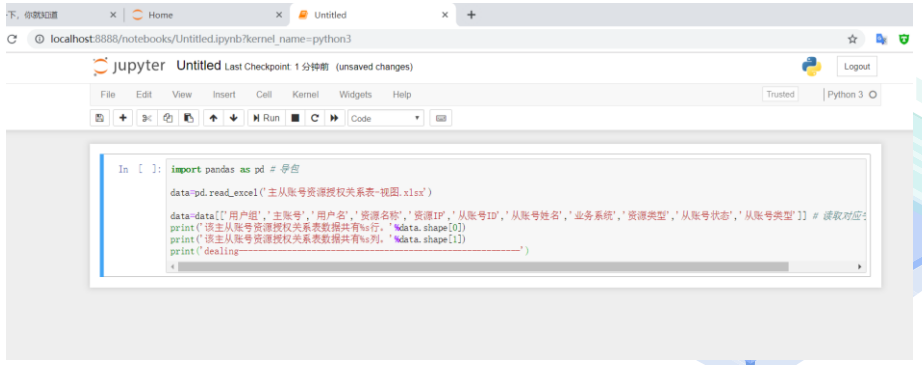




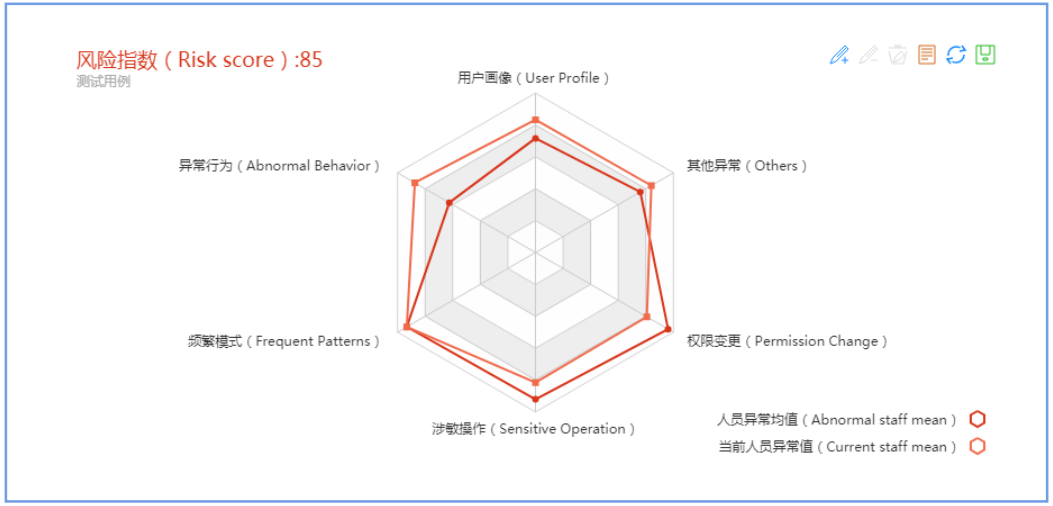




```
select distinct tt.group_name as 主账号归属组织,tt.master_account_id as 主账号ID,tt.master_account
.resource_type as 资源类型,tt.resource_ip as 资源IP,tt.slave_account_id as 从账号ID,dd.account_type
from                    _RELATION tt, (select distinct              _id,master_account_name,account_
where account_type2 ='第三方' or account_type2 ='     ' or account_type2 ='不确定')dd
where tt.master_account_id=dd.master_account_id
and ( tt.slave_account_id like 'root'
or tt.slave_account_id like 'oracle'
or tt.slave_account_id like 'sys'
or tt.slave_account_id like 'system'
or tt.slave_account_id like 'db2inst1'
or tt.slave_account_id like 'admin'
or tt.slave_account_id like 'administrator'
or tt.slave_account_id like 'dba')
```



审计展望



1、词频(term frequency, TF)

$$TF_{i,j} = \frac{n_{i,j}}{\sum_k n_{k,j}}$$

人员异常检测检测

2、逆向文件频率(inverse document frequency，IDF)

$$IDF(x) = log\frac{N+1}{N(x)+1} + 1$$

```
and 5.446700507614214
awk 0.3553299492385787
bin 6.715736040609137
by  0.2131979695431472
bye 7.390862944162437
cat 46.776649746192895
cd  265.6446700507614
chmod 3.2893401015228427
```

3、TF-IDF

$$TF - IDF = TF * IDF$$

审计展望

1.自动审计
2. 自动派单
3. 自动生成审计报表
4. 人员异常行为告警
5. 模型化自动学习

完

THE END