226周分享
第二期

由安全审计扩展出的思维感悟

1. 4A平台详解
2. 审计策略与漏洞标准
3. 常用一些审计技巧
4. 一些牛逼案例

本周分享者：

shiyan

01

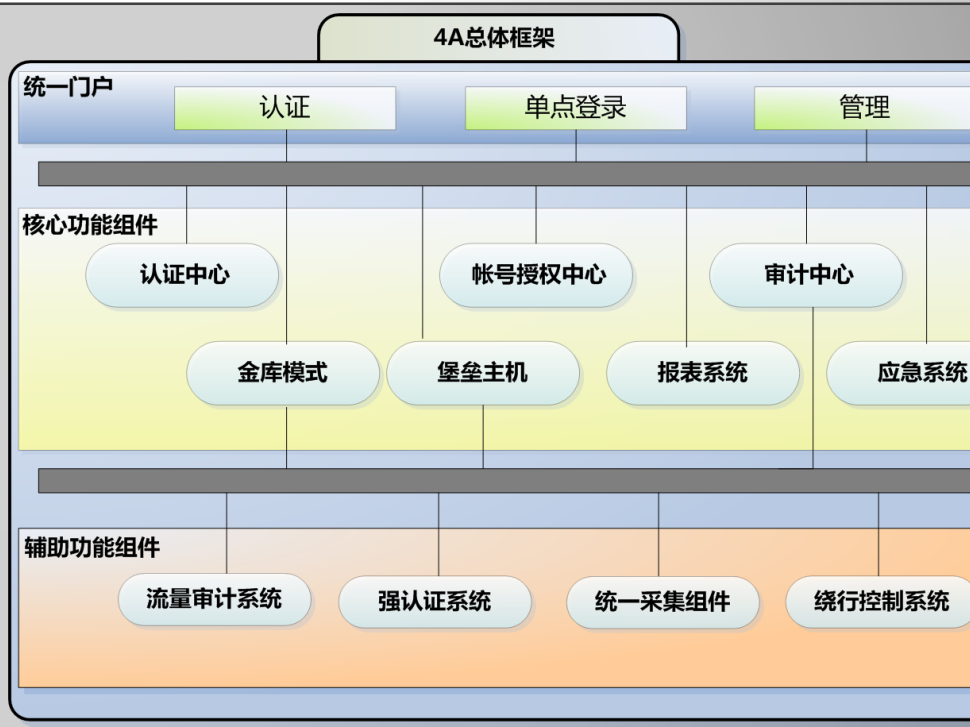
4A平台详解

- 什么是4A平台?
- 它解决了什么问题?

什么是4A平台？ (统一安全管理平台解决方案)

4A概述

4A 即帐号（Account）、认证（Authentication）、授权(Authorization)和审计(Audit),4A能为企业提供统一框架，整合企业应用系统、网络设备、主机系统。确保合法用户安全、方便使用特定资源。这样既有效地保障了合法用户的权益，又能有效地保障IT系统安全可靠地运行。4A系统使得系统和安全管理人员可以对IT系统的用户和各种资源进行集中管理、集中权限分配、集中审计，从技术上保证IT系统安全策略的实施。



它解决了什么问题?

1.
登录账号管理混乱，系统账号的作用只是区分工作角色，运维人员的流动影响系统账号。

2.
多个用户使用一个账号或者一个用户使用多个账号

3.
运维权限划分不明，越权操作频频发生

4.
认证方式过于简单，无双因子认证账号容易丢失被盗

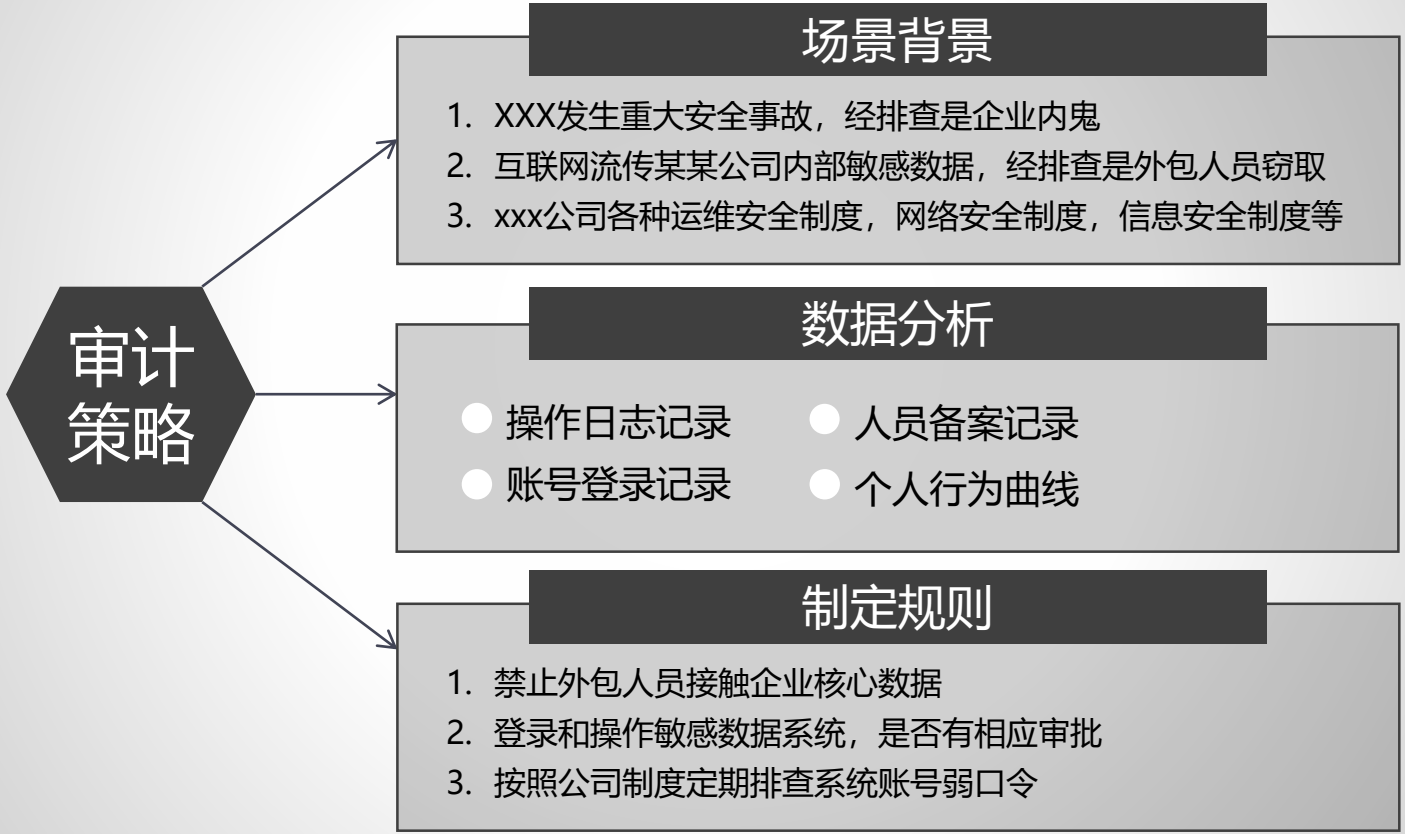
5.
对运维过程没有监控措施，出现网络安全故障难以排查原因和准确追责

02

审计策略与漏洞标准

- 什么是审计策略
- 什么是漏洞标准
- 两者之间的区别

什么是审计策略


审计策略
场景背景
1. XXX发生重大安全事故，经排查是企业内鬼
2. 互联网流传某某公司内部敏感数据，经排查是外包人员窃取
3. xxx公司各种运维安全制度，网络安全制度，信息安全制度等
数据分析
操作日志记录
人员备案记录
账号登录记录
个人行为曲线
制定规则
1. 禁止外包人员接触企业核心数据
2. 登录和操作敏感数据系统，是否有相应审批
3. 按照公司制度定期排查系统账号弱口令

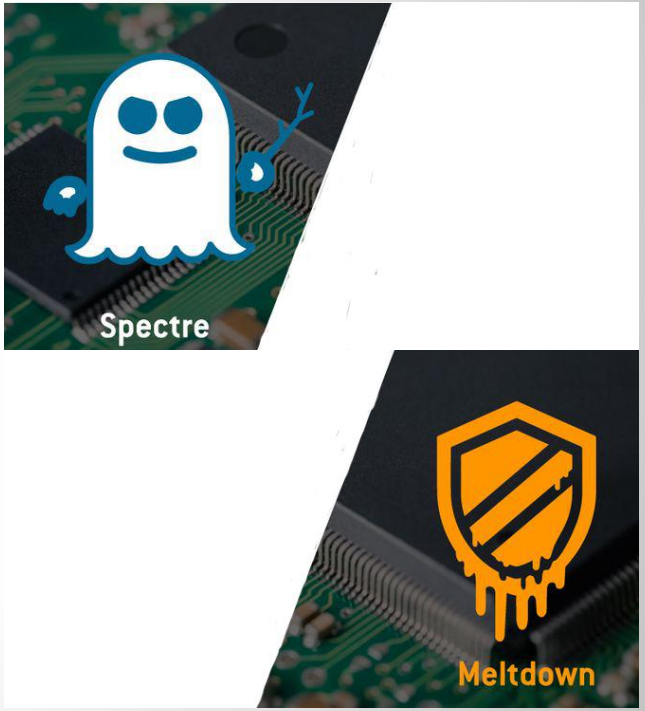
什么是漏洞标准

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

1. 漏洞是谁首发的?

XSS

3. 漏洞利用是否标准化?



2. 它有什么危害?

两者之间的区别

规则制定

1、审计策略是由审计人员根据现场情况，业务情况，人员情况，规章制度情况，等等制定的判断规则。
2、漏洞标准是由漏洞首发人员制定的，后续人员都是利用前者的标准进行挖掘漏洞。

系统与人员

1、审计策略主要是针对人员。
2、漏洞标准主要是针对系统和代码层面上的。

事故后处理

1、审计策略除了提前发现问题，整改问题，更多的还可以发生事故后，定责。
2、漏洞标准更多的是发现漏洞，修补漏洞，发生事故后还原漏洞的整个过程。

整改的深度

1、相对而言，审计策略是可以杜绝该类问题的发生的。
2、漏洞标准只是针对目前的情况进行修复，可能会存在整改不彻底等等情况。

03

常用的一些审计技巧

- Excel 篇
- Python 篇
- SQL 篇

Excel 篇（常用公式）

=VLOOKUP(对比字段,对比区域,2,FALSE)

=IF(COUNTIF(Sheet2!A$1:A$59,E2)=0,"不包含","包含")

=IF(B3=G3,“不正常","正常")

=TEXT(E3,"yyyy年m月d日")

=REPLACE(E2,4,4,"****") 正则匹配，替换其中数据为星号

=INT((N3-M3)*86400)+1

参考地址：http://www.ffcell.com/School/Formula/index.aspx

Python 篇（三方库介绍）

Pandas

```python
# coding:utf-8
'''
Effect：xxxxxxxxx
Creation_Time：2019/07/30
Remarks：以后新增代码语句，请增加修改时间和修改原因
'''
import pandas as pd

jk_xlsx = 'xxxxxxx.xlsx'
JK_List = ['xx1','xx2','xx3','xx4','xx5','xx6']

def Jk_Division(jk_xlsx):
    data = pd.read_excel(jk_xlsx)
    data_wudou = data[-data[JK_List[1]].str.contains(',')] # 没有逗号的数据
    data_dou=data[data[JK_List[1]].str.contains(',')] # 有逗号的数据
    data_new=data_dou.drop(JK_List[1], axis=1).join(data_dou[JK_List[1]].str.split(
        ',', expand=True).stack().reset_index(level=1, drop=True).rename(JK_List[1]))
         # 多个人的切分成一个人
    data01=pd.concat([data_wudou,data_new],sort=True) #
    合并无逗号数据和分割后无逗号数据
    data02 = data01[JK_List] # 该行为定义最终报表的字段顺序
    data02.to_excel('分割结果--'+jk_xlsx,index=0) # 输出最终结果

def main():
    # 执行脚本
    Jk_Division(jk_xlsx)

if __name__ == '__main__':
    main()
```

相关介绍

Pandas是一个开源的，BSD许可的库，为Python编程语言提供高性能，易于使用的数据结构和数据分析工具。

安装方法：

python3 -m pip install --upgrade Pandas

Or

pip install Pandas

中文网站

https://www.pypandas.cn/

SQL 篇（简述一些语法）

```
SELECT * FROM SHIYAN t WHERE t.time >= '2260-00-00 00:00:00' AND t.id IS NULL;

update
(select * from SHIYAN t WHERE  EXISTS (SELECT * FROM ZZL tt WHERE t.name = tt.name ))f
set name_type ='名称一致',name_have ='包含';
```

参考链接：https://www.runoob.com/sql/sql-tutorial.html

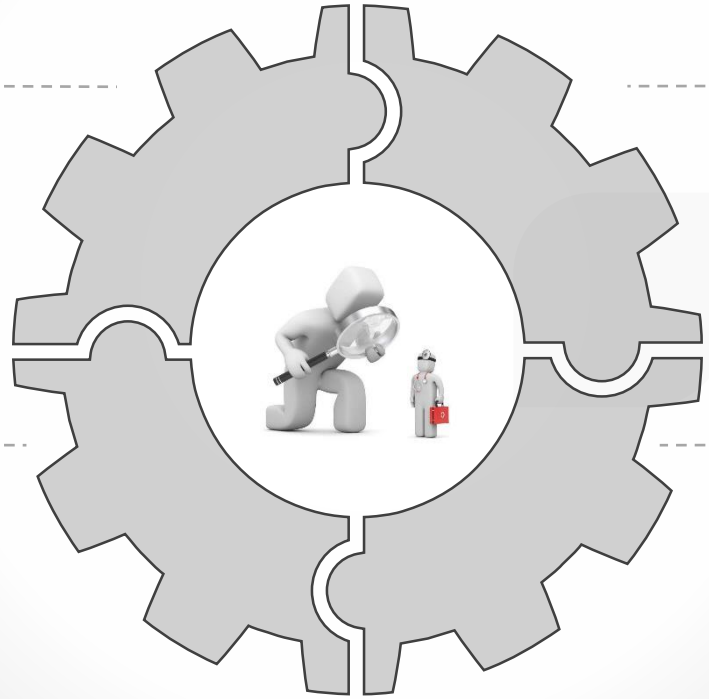
04

一些牛逼案例

一些牛逼案例

离职人员

合作伙伴



历史遗留

意识薄弱

END

谢谢观看

THANK YOU