



OWASP

Open Web Application
Security Project

金融业攻防人才能力建设

分享人：杨明 2021年12月

目录

CONTENT

1

金融人才战略

2

金融应用场景

3

攻防能力保障

4

人才梯队建设



OWASP
Open Web Application
Security Project

一、金融人才战略



金融人才战略

本质

人才是战略资源

核心

培养人、吸引人
使用人、发掘人

目标

推动企业长远发展



» 同业金融人才战略

- 工商银行：“人才兴行、人才强行”；科技**3.54万人**、投入**238.19**亿元；
- 招商银行：“人才立行”；科技**8882**人、投入**120**亿元；
- 上海农商：“一体两翼三化四位协同”；科技**374**人、投入**7.22**亿元。
 - “一体”：以人才发展为主体
 - “两翼”：绩效管理、资源配置
 - “三化”：市场化、专业化、信息化
 - “四位协同”：各级领导、人力资源条线、各业务条线、员工

金融科技人才战略导向

战略导向



关键人才

提供安全稳定的金融服务

安全人才的战略地位

金融业攻防人才紧缺!



OWASP
Open Web Application
Security Project

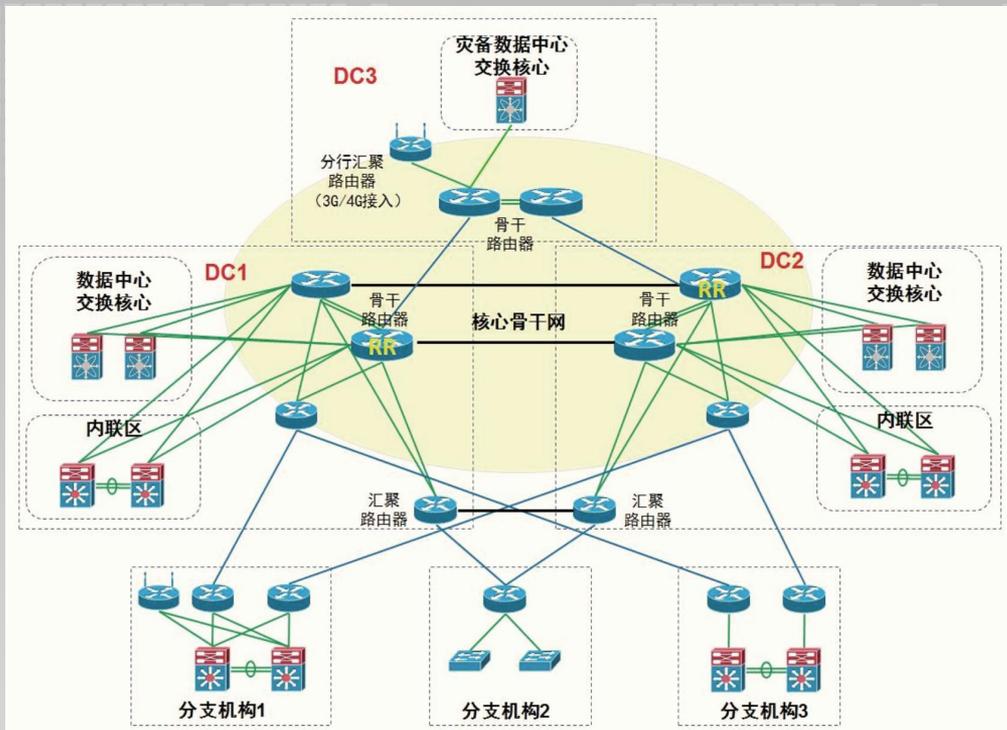
二、金融应用场景



总体概况

- 全省83家农商银行，营业网点3000多个，在岗员工3万多人；
- 服务三农、服务县域、服务小微、服务社区；
- 支持乡村振兴、服务实体经济、践行普惠金融；
- 服务的全省小微企业户数占比50%、农户数占比85%以上。

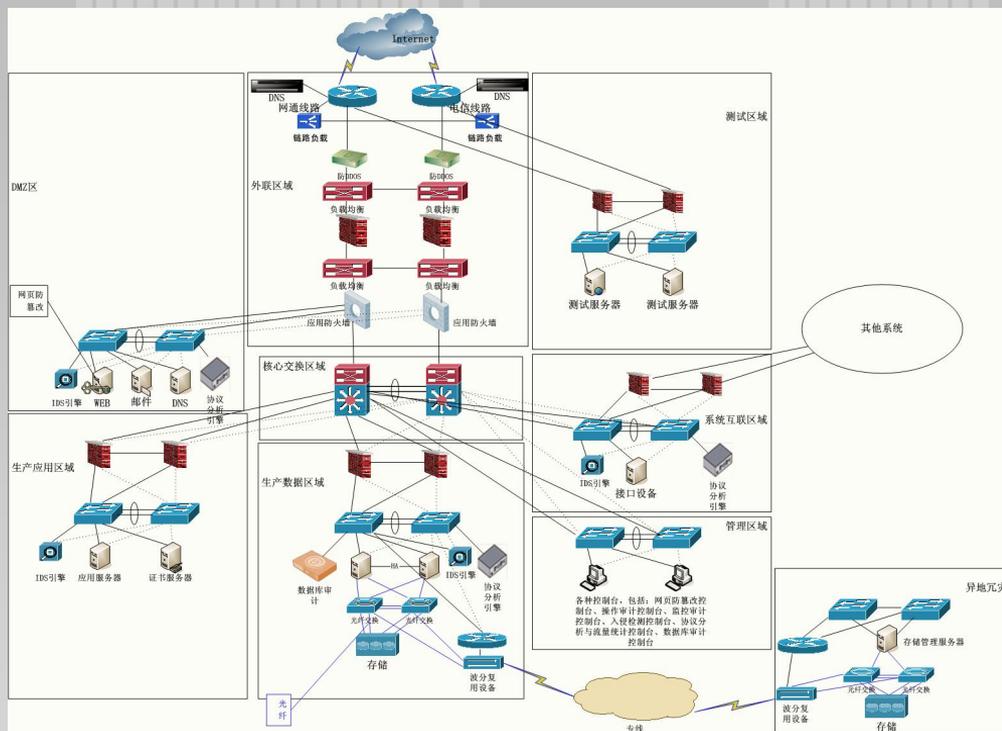
整体网络架构



- 两地三中心
- 同城双活

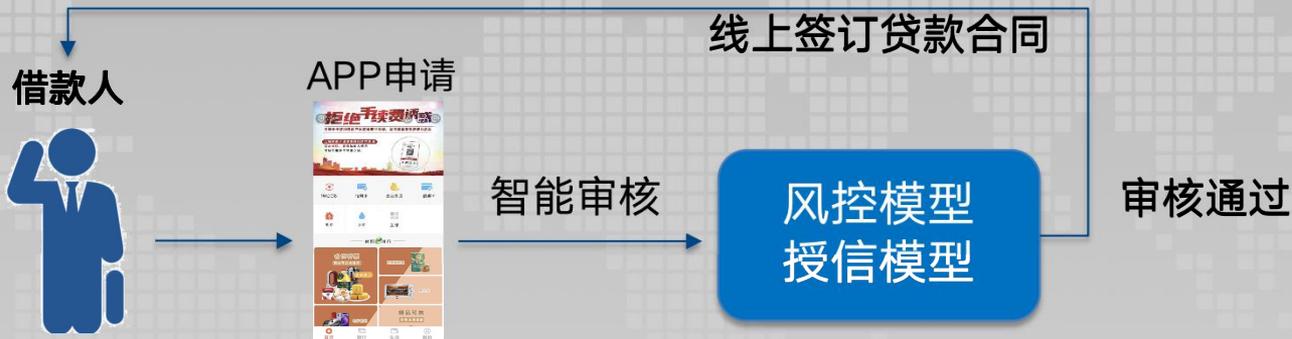


互联网区网络架构



- JR/T 0068-2020 《网上银行系统信息安全通用规范》
- 2012年5月8日发布初版
- 2020年2月5日发布更新版

线上贷款平台



数据整合

申请人, 申请人父母、
配偶、子女, 担保人,
关联企业等。

深入分析

水电气缴费、社保、公
积金、不动产、征信、
银行流水、纳税等。

全流程

贷款申请、资格审查、
审批、签约授信、放款、
还款、注销合同。



移动营销平台

移动营销业务平台

移动终端

- ① 产品展示
- ② 信息采集
- ③ 商户管理
- ④ 其他非现金业务

运营商VPDN

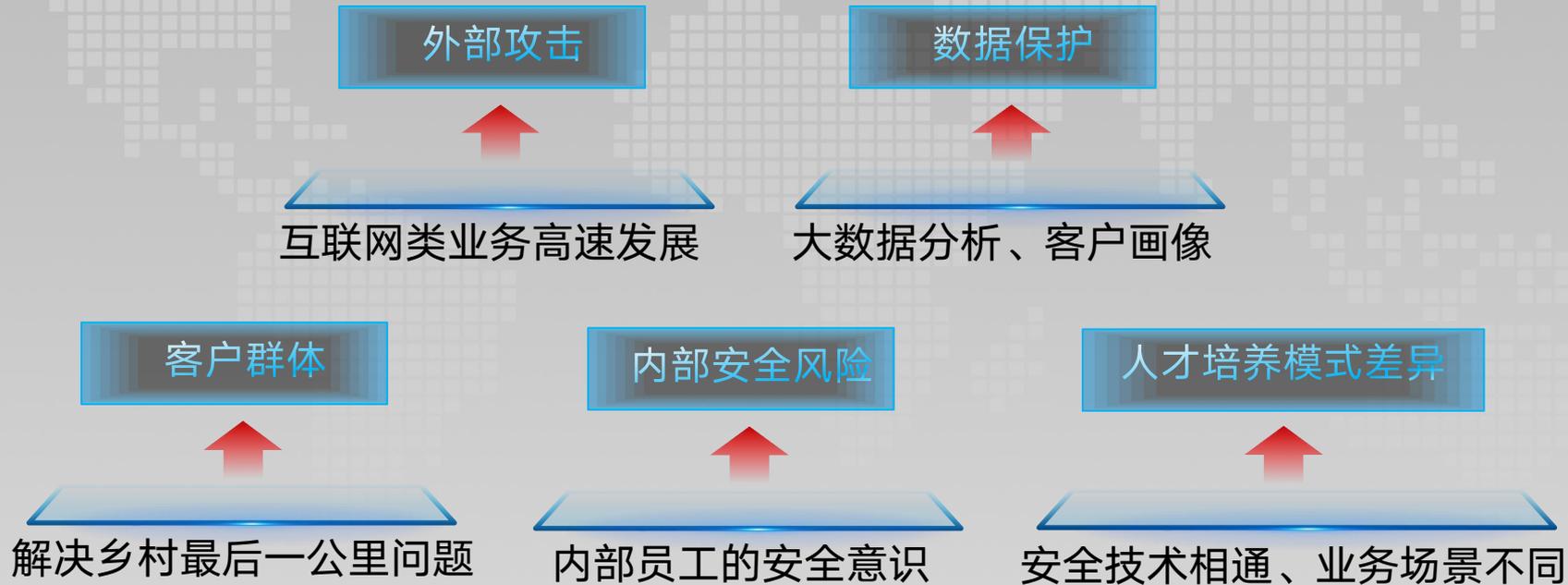
数据中心

- ① 4G/5G接入
- ② 移动业务平台
- ③ 统一认证平台

移动营销安全平台



金融应用场景

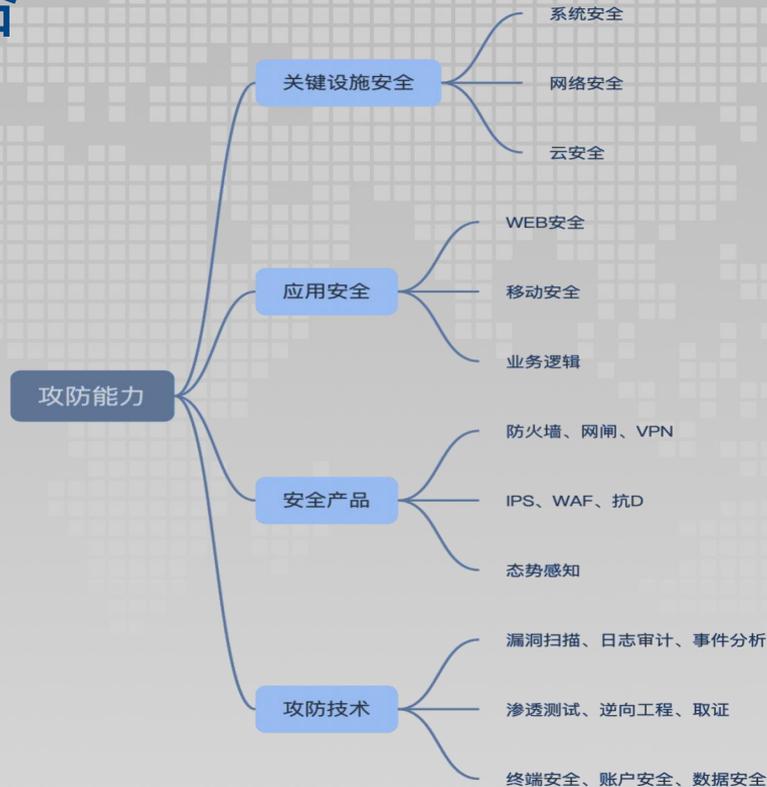


三、攻防能力保障



攻防能力保障思路

- 跟踪最新技术的敏锐性
- 攻击场景快速复现能力
- 防御技巧的灵活运用
- 贴合业务的解决方案



攻防能力保障措施

体系建设

安全培训

CTF

红蓝对抗

- 安全专业岗位人员将更多精力用来挖掘更深层次的漏洞和未知威胁；
- 培养安全技术岗位人才的金融素养，让他们更了解金融业务。



CTF团队能力建设

CTF团队能力建设

加密解密

古典密码（单表代换、多表代换），流密码（伪随机数、线性同余、反馈移位），块加密（AES、DES、分组模式），非对称加密（RSA），哈希函数（MD5），编码（BaseURL、ASCII、Unicode、二维码、条形码）

信息隐藏

图片隐写（元数据、文件头、LSB），音频隐写（MP3波形、频谱、LSB音频），压缩包分析（明文攻击、CRC32、伪加密）

取证分析

磁盘取证，VMDK取证，内存取证，流量包分析（HTTP、DNS、WIFI、USB、数据提取）

WEB安全

信息收集及扫描、SQL注入漏洞、XXE漏洞、命令注入漏洞、SSRF漏洞、反序列化漏洞、文件上传漏洞、文件包含漏洞

逆向分析

汇编基础，代码分析（静态、动态、Fuzzing），PE，加壳与脱壳，逆向破解

二进制

PWN基础、栈溢出漏洞、格式化字符串漏洞、堆溢出漏洞



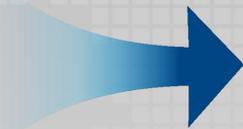
四、人才梯队建设



新形式下的金融安全团队

传统

- 安全开发团队
- 安全测试团队
- 安全运维团队
- 安全研究团队
- 安全管理团队



金融

- 安全开发团队 (含测试)
- 安全管理团队
- 安全运维团队
- 业务安全团队

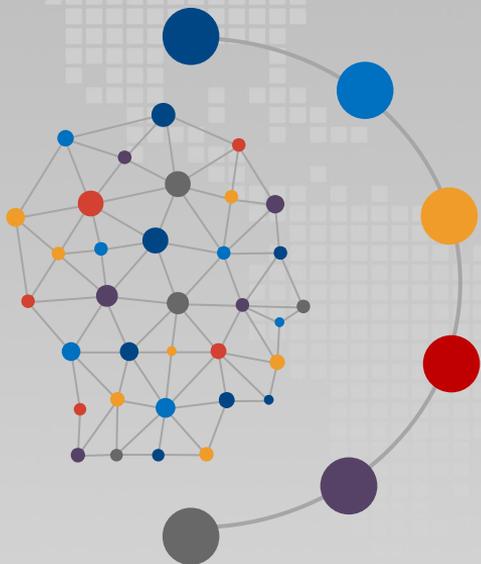


业务安全团队理解

- 知金融业务、懂金融安全；
- 思维发散、熟悉业务逻辑；
- 深入研究业务产品设计和用户体验。



安全人才梯队建设面临的问题



■ 攻防人才缺口从哪里补充？

- ① 外部招聘？文化融入问题！
- ② 内部培养？个人主观能动性问题！
- ③ 有钱？招不到想要的人！！
- ④ 稳定？安全大佬看不上！！

■ 体制决定了体质！

■ 安全需求紧迫、缺安全人才孵化的土壤！



稳健的安全人才梯队建设思考

01

未雨绸缪做好人才**储备**

02

避免人才**断层**

03

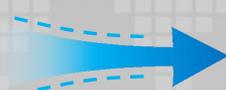
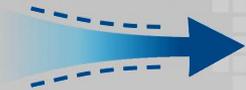
留住头部人才、允许普通人才的流动

04

轮岗、集中培训



个人能力与组织能力匹配、相互促进



对“木桶理论”说NO!!

攻防人才，个人优先发挥长板，团队不能有短板。

发展关键人才，实现个人与团队能力的融合



» 攻防能力复制

可复制的攻防能力：

- **内部讲师**--传递知识
- **师徒制**--传递经验



➤ 稳健的安全人才梯队建设模型

岗位
供给

机会
希望

培养
评价

发现
保留

激励
发展



» 愿景

- 实现**安全文化**层面的提升!
- 人人具备安全意识 → 成为真正的大众文化!

