
Tencent 腾讯 | 腾讯安全
CSS
互联网安全领袖峰会
Cyber Security Summit
春秋航空网络与信息安全分享
邱豪奇 春秋航空-信息技术部-副总经理

- 安全建设理念
- 业务安全维度
- 体系安全维度
- 基础架构维度

安全建设理念

VS

谁跑得更快？

良好的企业环境是安全工作持续稳定开展的基石

用对人始终是重新掌控主动的核心因素

企业安全建设理念

持续　　渐进　　平衡

工具
安全源头的“深度”与“广度”决定了安全边界，控制环节的“精度”与“时延”决定了安全工作的有效性，合适工具的使用能加速促进安全管理转型。

人
安全事务的发起者、组织者、推动者，为安全工作的最终落实负责，合适的人员才是打开安全困局的钥匙。

环境
行业背景决定最低安全标准；管理层安全意识决定安全建设高度；一线员工执行水平决定企业安全水平。

企业安全建设更像是中医调理，更关注整体而非局部

体系安全维度

信息安全组织发展进程

初创阶段
(2008~2014)

信息安全体系初建
信息安全组织、岗位设立
信息安全审计
SMS部门体系初步建设

SDLC阶段
(2015~2017)

上线前渗透测试
信息资产风险评估
软件开发生命周期安全规定
部门安全绩效体系建立

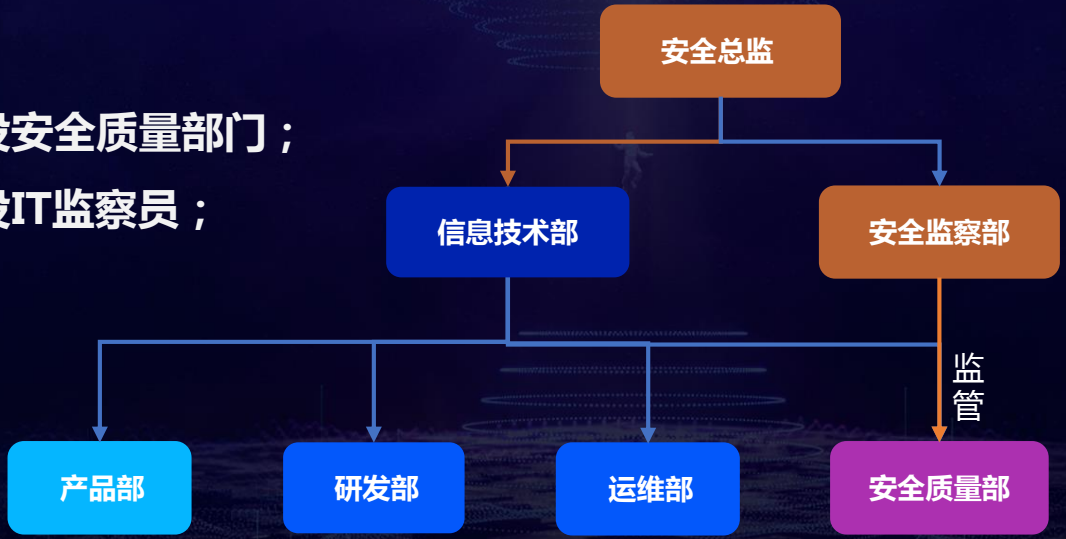
安全合规
(2017~至今)

《网络安全法》
信息系统等级保护
第三方支付数据安全标准（PCI）
通用数据保护条例（GDPR）
行业自查&法定自查

初创阶段（2008—2014）

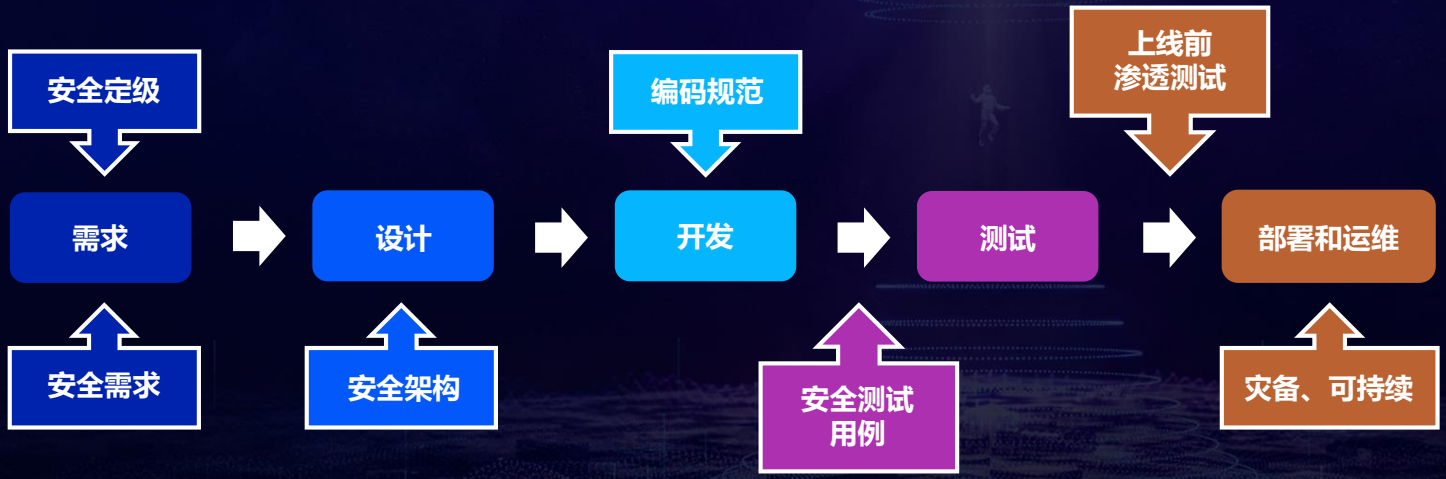
信息技术部下设安全质量部门；

安全监察部下设IT监察员；



SDLC阶段(2015~2017)

180+项目/每年



风险管理全流程渗透（持续、动态）

风险管理启动时机：

- ✓ 年度例行（2次）；
- ✓ 系统评价、管理评审中发现问题时；
- ✓ 新运行项目、项目重大变更；
- ✓ 外部环境、内部组织重大变更；
- ✓ 重大安全事件发生、重复事件发生；

安全合规阶段(2017~至今)

7个重要信息系统等级保护定级备案；

设立DPO(Data Protection Officer) ；

整合6大业务部门开展数据合规工作；

结合技术与业务合规标准。

季度应急演练深入开展

启动

演练设计人员
演练目标
演练对象
演练场景

计划

统一方案
涉众评审通过
双盲演练
（时间、场景）

执行

演练数据颗粒化
演练记录员
领导现场观摩
当天现场总结

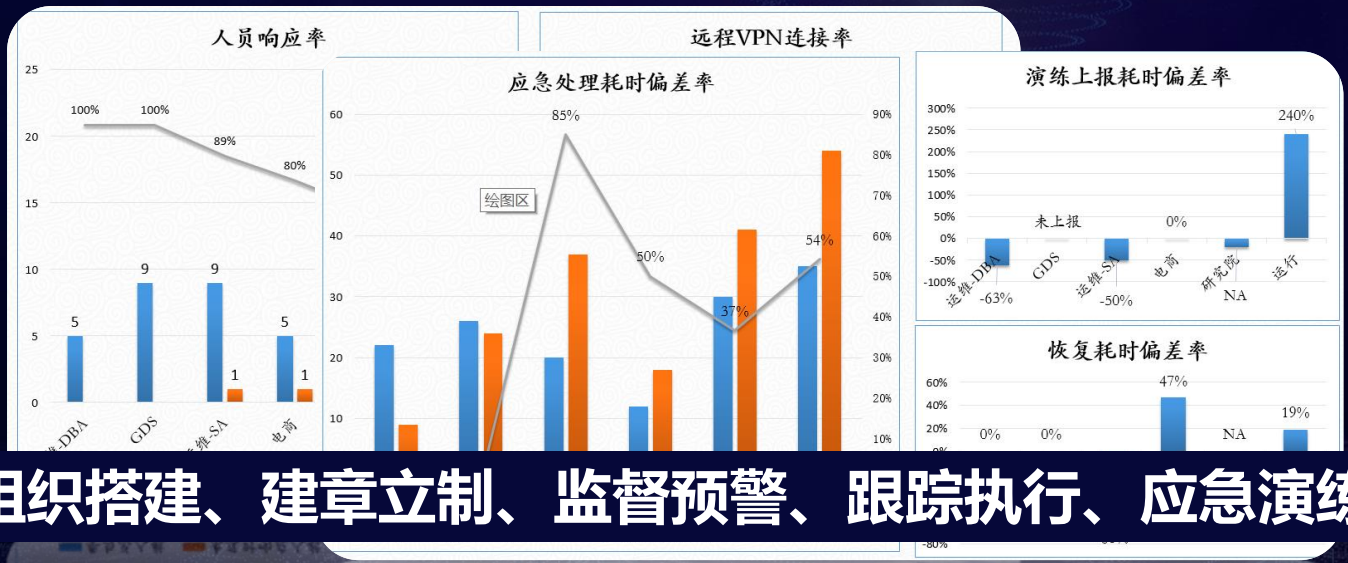
复盘

涉众复盘
多角度问题总结
数据记录追溯完整
应急预案复盘

总结

数据统计分析
优化措施落实
应急预案修订

季度应急演练深入开展



组织搭建、建章立制、监督预警、跟踪执行、应急演练

业务安全维度

终端的防护

加固混淆

防止二次打包
防止源码泄漏

黑客 → 植入病毒 → 二次打包再签名

帐号密码
支付短信
通讯录等

携带病毒的APP

交互安全

防批量注册
防短信轰炸
防登录撞库

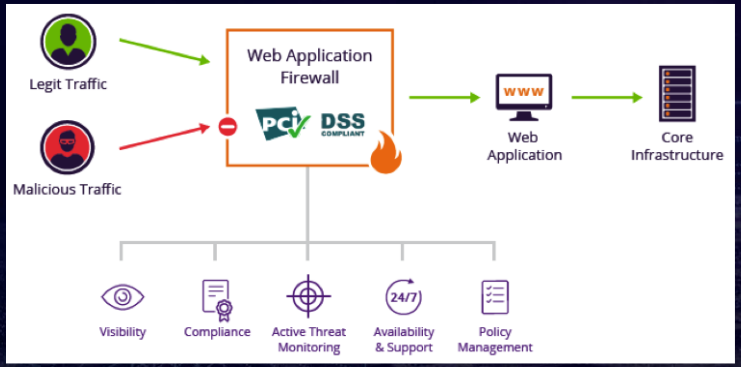
数据通讯的防护

HTTPs

全站部署HTTPs

防劫持
防篡改
.....
安全加密
使网站可信

WAF



防爬、防刷
防御CC攻击
防数据泄露
.....
防网页篡改、木马后门
0day漏洞修复

合规认证


@SEC
Attestation of Compliance for PCI QSA Assessments
No.: atsec-2019-PCI-DSS-C-01410-02062
This is to certify that:
Spring Airlines Co., Ltd.
Has been assessed and validated according to the following payment card industry standard:
Payment Card Industry (PCI) Data Security Standard (DSS)
Requirements and Security Assessment Procedures
Version 3.2.1, May 2018
Office location: F3 of HongQiao V+ Building, No.4560, Hongqiao Road, Changning District, Shanghai, and P.R.China
Data center location: B7-1# Room of B7 Building, No.180, Xiuyan Xi Road, Pudong District, Shanghai, P.R.China
Assessment Scope:
Spring Airlines provides payment authorization service for its customer, while the customers buy tickets on its mobile Application. Sensitive authentication data (including CVV2/CVC2/CAV2/CVN2) and cardholder data (including PAN and expiration date) are transmitted securely over HTTPS interface with strong cryptography. Once the internal payment processes are completed, cardholder data and sensitive data are transmitted to payment service provider over Internet with strong cryptographic HTTPS interface. The sensitive authentication data and cardholder data are held in the VRAM and purged immediately after authorization. No sensitive authentication data and cardholder data are stored in the cardholder data environment after the payment authorization process. The mobile Applications involved in the payment authorization are developed by Spring Airlines and the support platform are iOS and Android.
Date of Issue: January 8, 2019
Date of Initial Compliance: January 8, 2016
Date of Expiry: January 8, 2020
LiuYan
PCI Laboratory Director
atsec (Beijing) Information Technology Co., Ltd
Tel: +86 10 53010681
Fax: +86 10 53010678
Email: info_cn@atsec.com
www.atsec.cn
The validity of this attestation can be verified through the above website.
Refer to Report on Compliance (ROC) for the compliance and assessment details.

PCI-DSS的全称为(Payment Card Industry Data Security Standard)支付卡产业数据安全标准，是全球最严格且**级别最高的**金融**数据安全标准。**

由于操作性极强，被金融业外的各大行业奉为**通用的安全标准。**

一般的认证流程是这样的

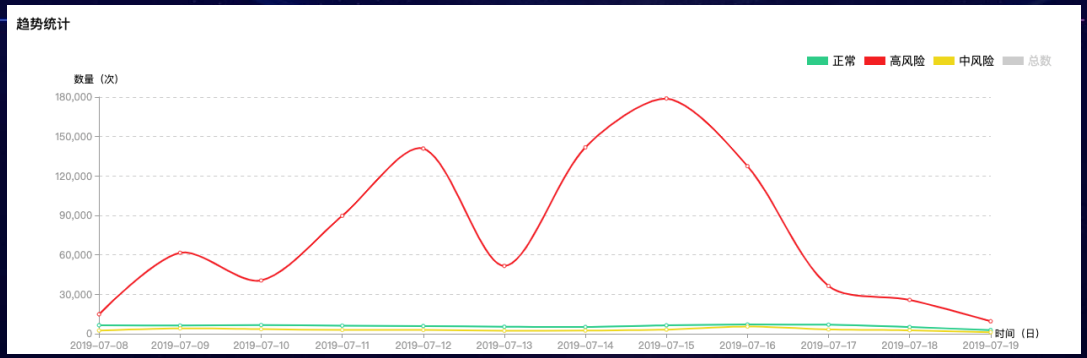
收到企业提交的PCI-DSSS认证申请后，PCI-DSS会授权独立审查公司，对申请企业进行全方位、彻底的审核。而审核内容分含6大领域、12项规范、200余向审核指标，以6大领域为例，包括：

1、 构建并维护安全的网络;
2、 保护持卡人数据;
3、维护漏洞管理程序;
4、 执行严格的访问控制措施;
5、定期监控网络和测试网络;
6、 维护信息安全政策。

审核包括自我安全检测、漏洞分析、安全调查三大阶段，考察范围涉及硬件、软件、员工和公司管理等多项指标，**并且每年至少接受一次重检。**

风控平台

- 欺诈账号识别
- 设备指纹
- 机器注册识别
  - 趋势分析
  - 历史记录
  - 排行榜
  - 名单服务
  - 服务报告
  - 数据提取



“提直降代”对春秋不是一项“ZZ”任务，是基因使然
持续打击“黑代”与“薅羊毛”行为，守护旅客利益诉求

基础架构维度

备份机制的演进

方法与工具

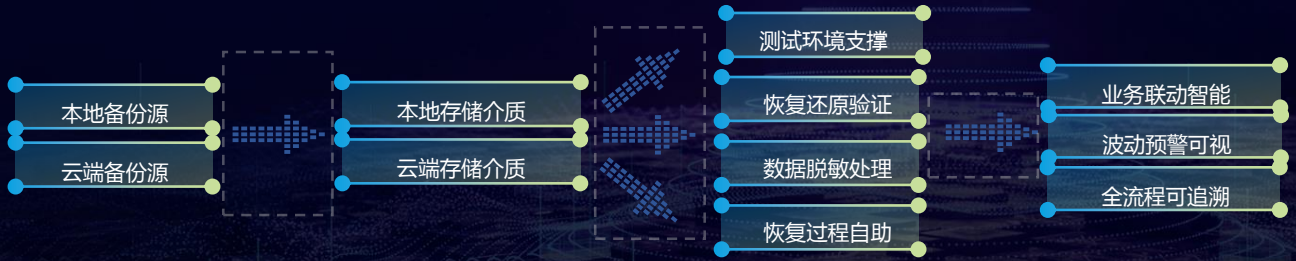
应用与恢复

第一阶段
- 通用备份软件（主）
- 少量备份脚本（辅）

第二阶段
- 自动化脚本规模化
- 通用备份软件（辅）

第三阶段
- 任务监控集中化
- 备份恢复自助化
- 备份恢复工单化

第四阶段
- 业务联动智能化
- 波动预警可视化
- RTO考核指标化



监控模式的演进

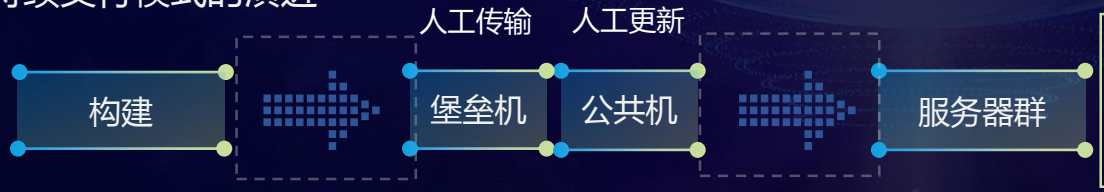
Nagios → Zabbix → Open-Falcon + 自研监控中心（时光机等） → 未来

2010年 2014年 2019年

网络层
系统层
数据库层
中间件层
应用层
业务逻辑层

1. 无需二次开发，快速兼容业务逻辑监控
2. 监控秒级批量部署
3. 告警信息集中展示
4. 自定义告警方式 
5. 自定义告警升级模式
6. 展示服务器之间的互联拓扑结构图
7. 自动抓取性能低下的代码，上报性能优化组

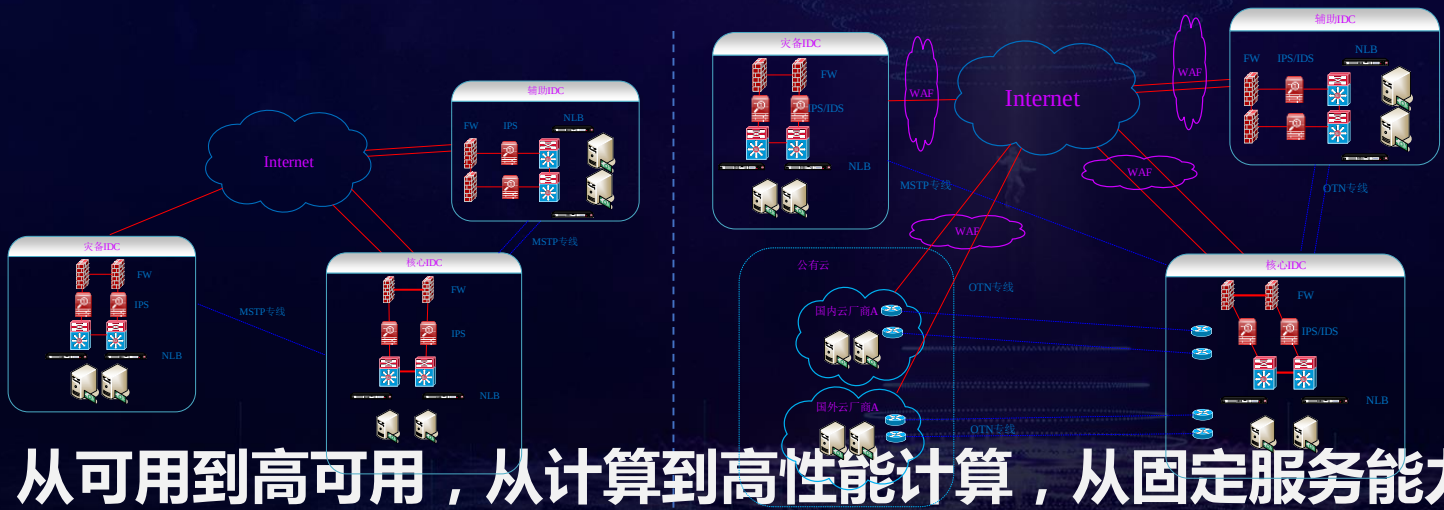
持续交付模式的演进



1. 代码有版本基线 —— 回滚时间缩短30分钟
2. 提升更新效率 —— 单次更新缩短30分钟
3. 减少误操作 ——运维全年0次
4. 所有操作都有记录 ——操作透明可追溯

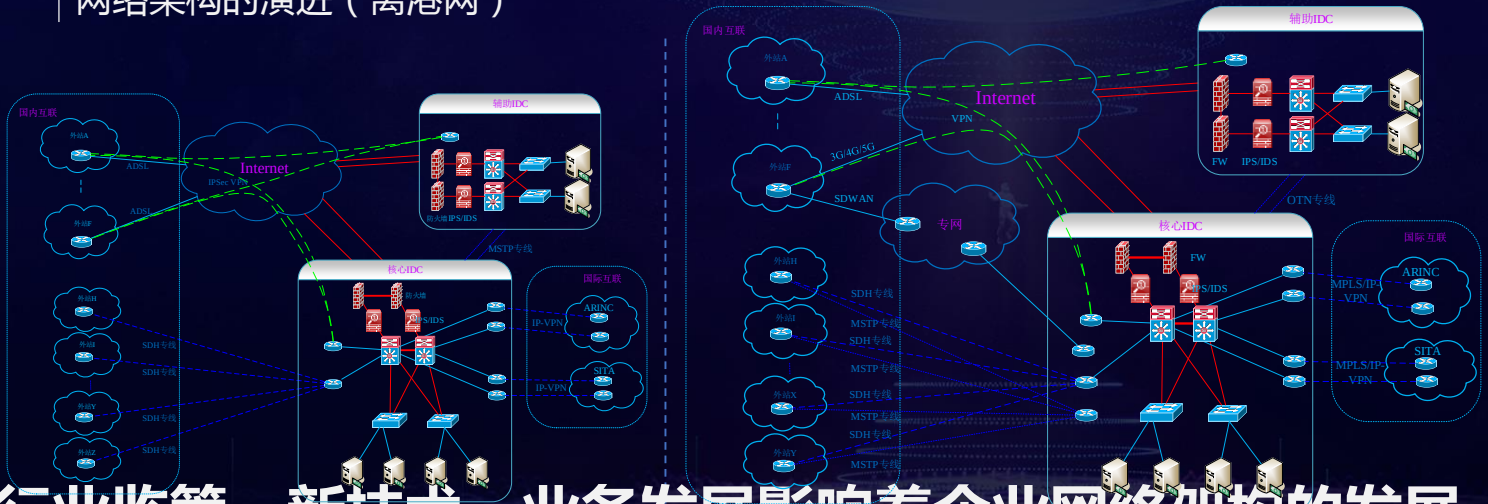
网络架构的演进

网络架构的演进（生产网）



从可用到高可用，从计算到高性能计算，从固定服务能力到弹性服务能力，业务需求与安全合规推动着架构演进。

网络架构的演进（离港网）



行业监管、新技术、业务发展影响着企业网络架构的发展，
我们持续做的是找到合适的演进时间点并完成它。

企业安全建设是一件持续开展的工作，这两年它的显性价值越来越被感知，但幕后英雄还是常态。

构建企业自身的安全体系，比完成单个安全项目更有意义，持续迭代与跟踪执行要有机制保证。

工具、环境、人员决定着安全工作螺旋式发展，作为企业管理者更应该培育后两者。


感 谢 聆 听