DT时代的安全建设实践分享

盒子科技

盒子科技-Odin

iBOXCHAIN
盒 子 科 技

About Company

- 盒子支付成立于2011年，—>盒子科技 ，新零售商户服务的领导者;
- 线上、线下业务，现持牌服务于全国百万级商户；
- 与银联、微信、支付宝、20家商业银行战略合作，对接饿了么、美团平台；
- 竭诚服务：收单、收款 ……需求；
- 抱歉：移动支付的快速发展意味着大家出门再也捡不到钱了……

About Me

- 安全老兵，10年+的安全建设经验
- 乙方 —>甲方
- 某云核心白帽子（曾经）
- 深圳第一批等保参与实践者
- 甲方安全建设从0 到1实践者

CONTENTS

CONTENTS

一、是什么在驱动安全行业发展？

互联网本来是安全的，自从有了研究安全的人后，就变得不安全了。

一、是什么在驱动安全行业发展？

网络攻击

系统漏洞

互联网

病毒/木马

暴力破解

金钱

白帽子

数据泄露

黑产

合规

网络安全法

一、是什么在驱动安全行业发展？

CONTENTS

二、关于安全团队建设-背景

安全事件驱动

- 网络攻击
- 数据泄露
- 被敲诈勒索

业务驱动

- 数据保护
- 安全运营
- 品牌名誉

监管要求

- 网络安全法
- 等保
- 金融行业合规

二、关于安全团队建设-目标：

为业务安全发展保驾护航

提高产品核心竞争力

二、关于安全团队建设-规模：

按需定制：

① 公司规模

② 业务系统

③ 安全定位及重视程度

阶梯式：

① 高、中、低

② 导师制

③ 不同阶段选择不同的人才

二、关于安全团队-规模：

第一梯队：HBAT,数千人，占总人数的5%-7%左右；

第二梯队：JMP，数百人，占总人数的3%-5%左右；

根据工作需求和公司要求，分阶段配置相应的人员。

二、关于安全团队-趋势

朝阳产业：>300人规模，都会有独立的安全团队；

组织架构：独立运维 or 研发，成为二级部门或更高；

未来，安全是网络空间维稳的基石，没有绝对的安全，也没有攻不破的系统，信息科技越发达，安全越得到重视。

二、关于安全团队-价值体现

二、关于安全团队-使命与担当

不忘初心　　砥砺前行

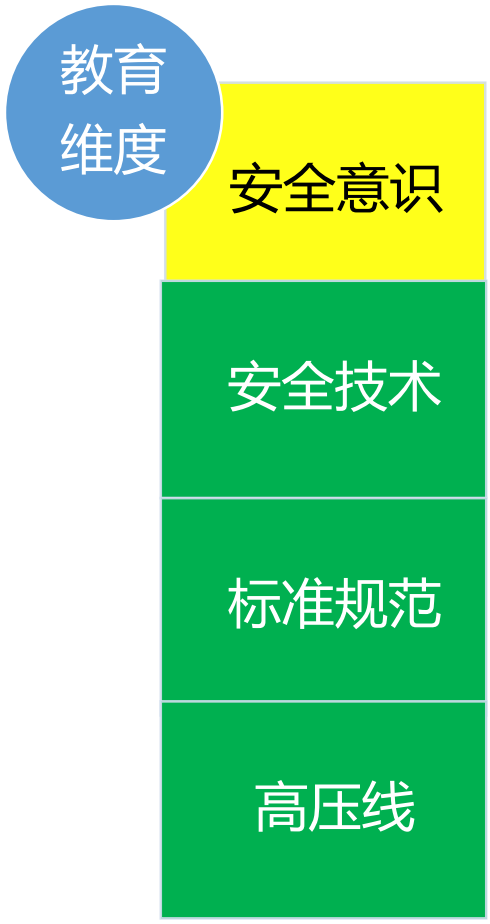
秉承匠心　　方能致远

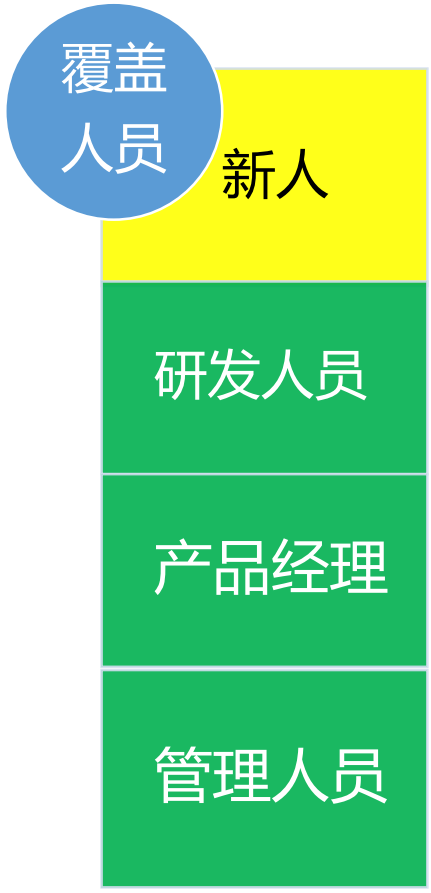
CONTENTS

三、关于安全运营要Get的点

1. 企业安全文化建设
2. 安全制度/规范
3. 安全SDL建设
4. 安全即未来

三、关于安全运营-安全文化建设





三、关于安全运营-安全制度/规范

标准规范：

- 开发语言安全规范
- 系统/中间件安全规范
- ……

奖惩制度：

- 信息安全管理制度
- 安全高压线
- ……

先培训，其次订标准/规范供其学习，最后再讲原则！安全是有底线的！

三、关于安全运营-SDL（安全开发生命周期）

为什么要引进SDL？

- 不甘于救火
- 安全工作滞后
- 上兵伐谋，其次伐交，其次伐兵，其下攻城；

在什么阶段下适合引进SDL？

- 安全团队初具规模,及时发现风险能力；
- 高风险漏洞修复过慢；
- 安全与产品、研发资源冲突；

三、关于安全运营-SDL（安全开发生命周期）

MSDL:

Training	Requirements	Design	Implementation	Verification	Release	Response
• 安全技术培训	• 安全需求	• 安全设计	• 提供安全工具	• 代码审计	• 应急方案	• 应急执行
• 安全意识培训	• 风险识别	• 攻击分面析	• 安全开发规范	• 渗透测试	• 上线前安全检查	• 漏洞扫描
• 安全规范		• 威胁建模	• 安全API		• 安全运维规范	• 情报系统

三、关于安全运营-SDL（安全开发生命周期）

1、SDL安全活动过程分别**嵌入至**“产品、架构、研发、测试、运维”业务流程中；

2、原则上“无上述安全报告”，“高危漏洞未修复”，禁止上线【当然也要视情况而定，灵活处理】；

3、“产品部门”与“开发部门”，各预留5%的资源解决安全隐患；

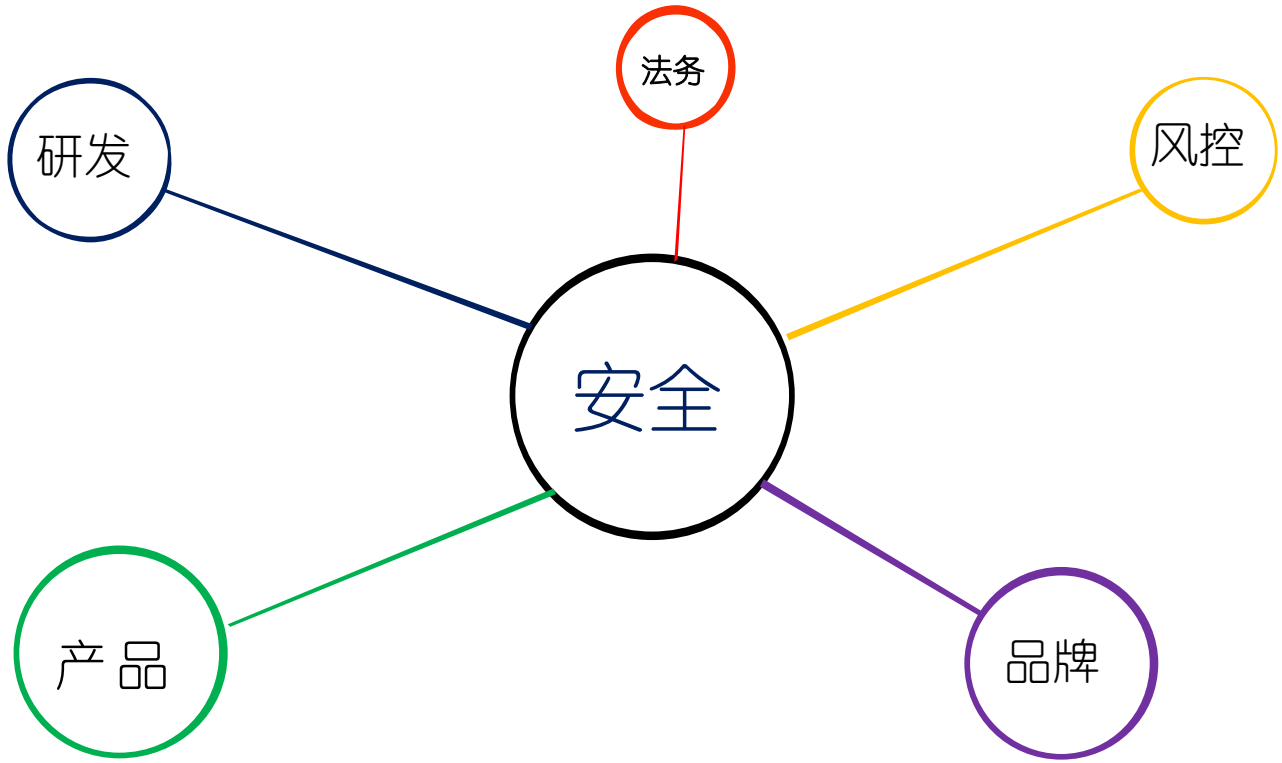
三、关于安全运营-SDL（安全开发生命周期）

不同的阶段，不同的资源，开展不同的工作！

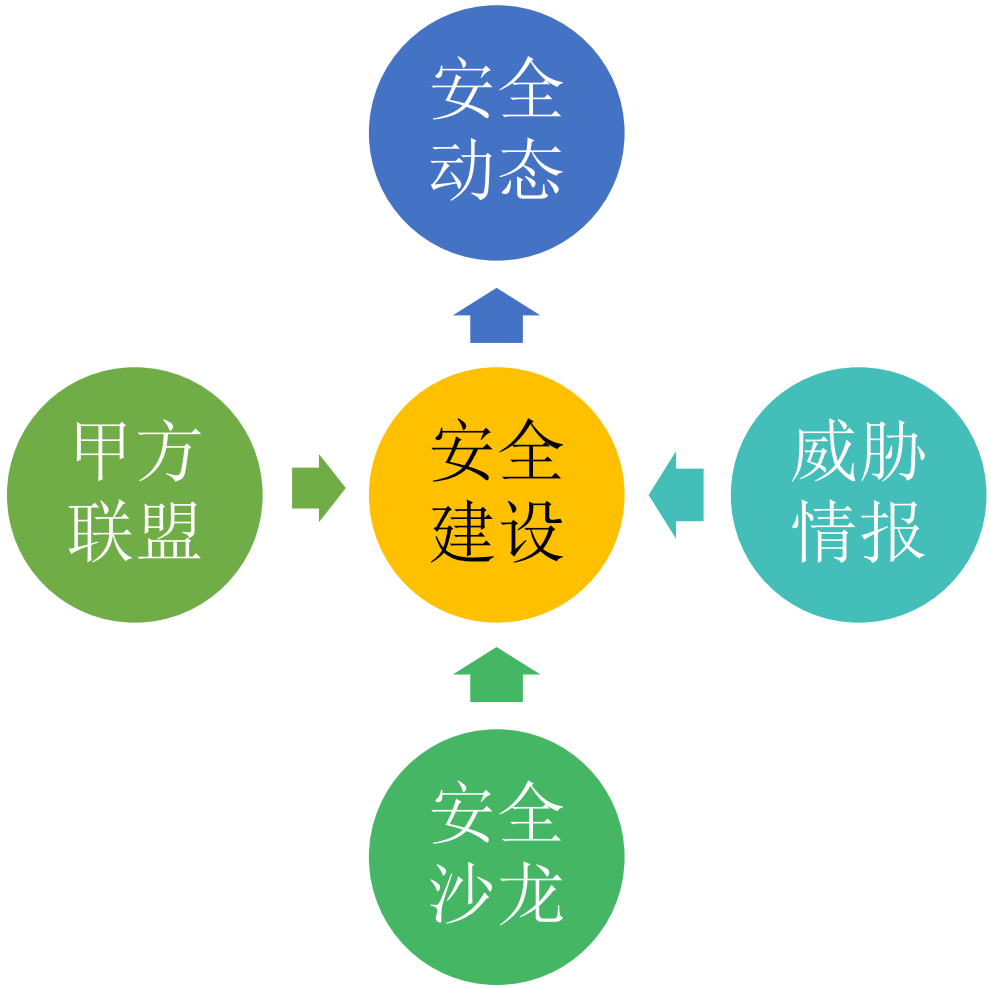
三、关于安全运营-安全即未来

安全是一个动态的行业，即要从内向外看，也要从外向内看！

三、关于安全运营-安全即未来



三、关于安全运营-安全即未来



作个总结：

- 安全是为业务服务的，要理解业务，不能脱离业务。
- 安全团队按需建设，分阶段/阶梯式建设，导师制培养。
- 安全工作可视化，量化更能体现价值，同时做好向上管理。
- 先培训，后教育，最后再讲原则，安全是有底线的。
- 根据资源，选择合适的阶段开展SDL，要量力而行。
- 安全是动态的，不断发展的，要与时俱进。

四、安全即未来

做安全就是做未来，做安全的更要重视安全，关注安全和了解安全。未来的安全是什么？它是以什么形式存在？它所具备的威胁是什么？发现问题和解决问题，这是安全的目标，也是我们的责任！

— XCon和XPwn创始人王英键

Q&A


中国电信
中国移动
531 K/s
79%
22:37
二维码名片
Odin
澳大利亚 奥古斯塔
扫一扫上面的二维码图案，加我微信

THANKS

深圳盒子信息
科技有限公司

全国服务热线
1010 9888

深圳 · 南山区软件产业基5栋C座503室
北京 · 朝阳区呼家楼京广中心一号楼37层11-12
上海 · 浦东新区张衡路1000弄润和国际总部园50号
徐州 · 江苏省徐州市经济技术开发区软件园C3栋