安世加

"Face the challenge, Embrace the best practice"

EISS-2020
企业信息安全峰会
之上海站

2020年11月27日

浅谈大中型软件企业信息安全建设

科大讯飞安全架构师 钱君生

2020年11月27日

安世加

议题概要

在业界，谈论互联网、金融或运营商安全建设的比较多，谈论大中型软件企业安全建设比较少。实际上，大中型软件企业在当下的IT企业中占有很大的比重，就大中型软件企业的信息安全建设来说，与互联网企业、金融企业存在着很大的差异性。本次分享将结合大中型软件企业安全建设的过程，讨论相关实践细节。

关于我

OWASP中国安徽区域负责人，现就职科大讯飞集团公司，任安全架构师，是开源图书《BurpSuite实战指南》、《API安全技术与实战》（机械工业出版社）编写者。

安世加

议题大纲

Contents

01 **大中型软件企业业务特点**

业务形态以2B交付为主、产品交付与项目交付并存……

02 **业务对安全建设的挑战**

安全职责、预算、投入均不对等、安全环境复杂……

03 **安全建设实践思路**

多模型融合的安全体系、关键安全策略……

04 **未来展望**

未来想做的事……

安世加

大中型软件企业业务特点

大中型软件企业业务特点

● 业务形态以2B交付为主

- ✓ 客户对象主要是企事业单位
- ✓ 业务开展以项目制形式
- ✓ 通常需要开展招投标和采购活动
- ✓ 系统集成和软件产品集成
- ✓ 业界有甲方爸爸一说，客户在业务中占主导地位

● 产品交付与项目交付并存

- ✓ 企业的业务开展围绕收益展开
- ✓ 在不断的项目交付过程中，积累自己的基础平台或产品；
- ✓ 典型的产品如ERP、HRM、CRM、OA等
- ✓ 围绕项目建设内容，采用产品交付+定制来完成项目交付

安世加

业务对安全建设的挑战

1 安全职责、预算、投入均不对等

- ✓ 安全事件板子打在客户方，肉疼在厂商
- ✓ 甲方爸爸关心安全，但往往没银子
- ✓ 安全工作必须要做
- ✓ 利润或收益减少，投入可能无收益

2 安全环境复杂难以标准化

- ✓ 不同的项目，环境不一样
- ✓ 不同的客户，要求不一样
- ✓ 不同的行业，标准不一样
- ✓ 不同的预算，内容不一样

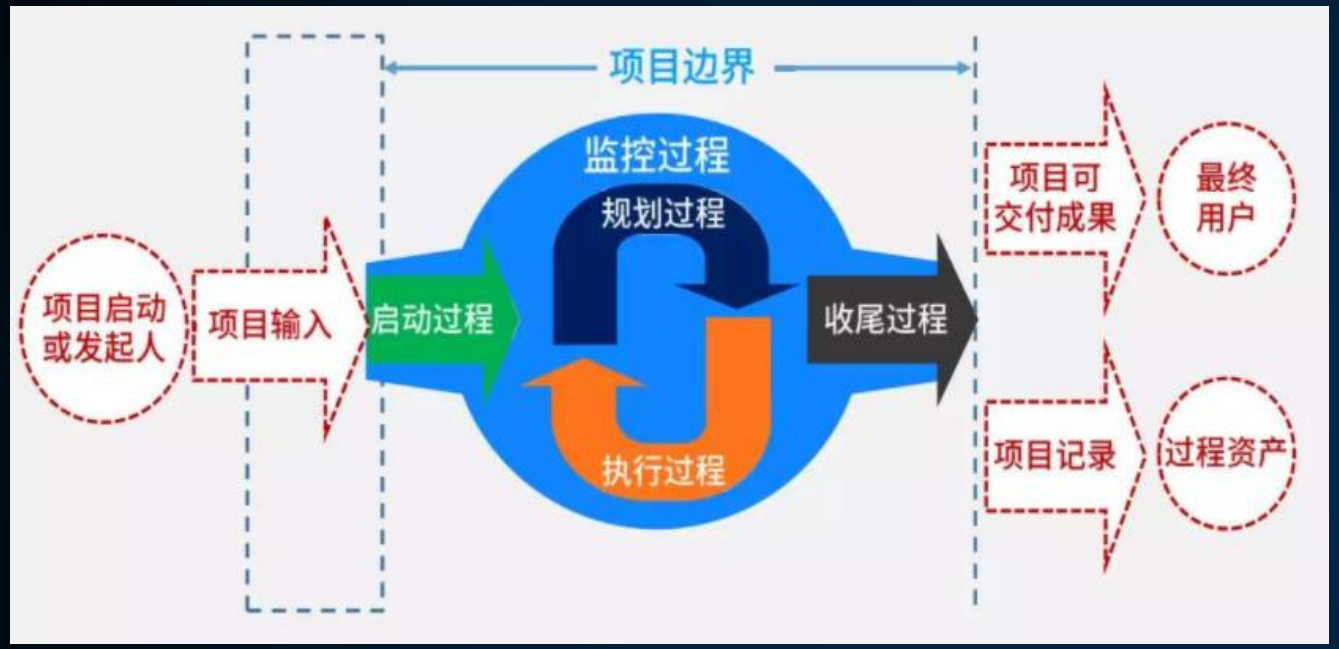
3 业界最佳实践参照样本缺乏

- ✓ 业界谈论金融、互联网企业多，谈论软件企业的少
- ✓ 业界最佳实践参照样本少，有头部企业做得好，但很少公开说
- ✓ 更多的是落后同时代的其他IT企业，在摸着石头过河

安世加

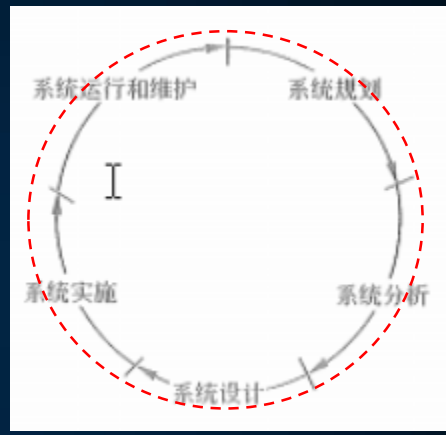
多模型融合安全建设思路

- **安全建设思路围绕业务的生命周期开展**



【图片来源/网络】

业务对象：信息系统



- ✓ 等保
- ✓ ISSE

- ✓ SAMM
- ✓ SDL

安世加

落地实施关键安全策略

01

分级分类策略

02

底线管控策略

03

公共组件策略

DevSecOps管道化策略

04

数字化平台运营策略

05

安世加

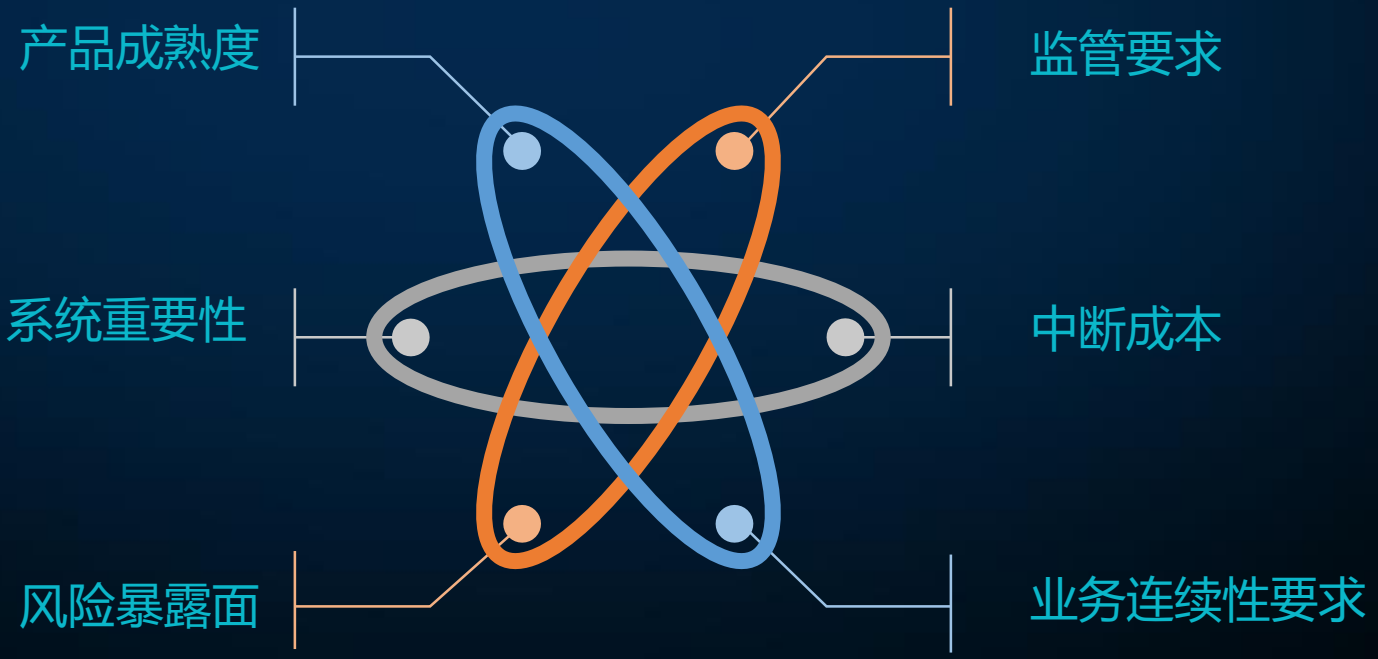
分级分类策略

- **为什么要分级分类**
  - ✓ 内外部安全要求不一样
  - ✓ 产品成熟度不一样
  - ✓ 安全投入不一样

- **如何分级分类**
  - ✓ 从定性和定量两个方面制定分类标准
  - ✓ 挑选对安全影响至为关键的指标

- **常用指标项**

$\sum$ 指标项评分*指标权重

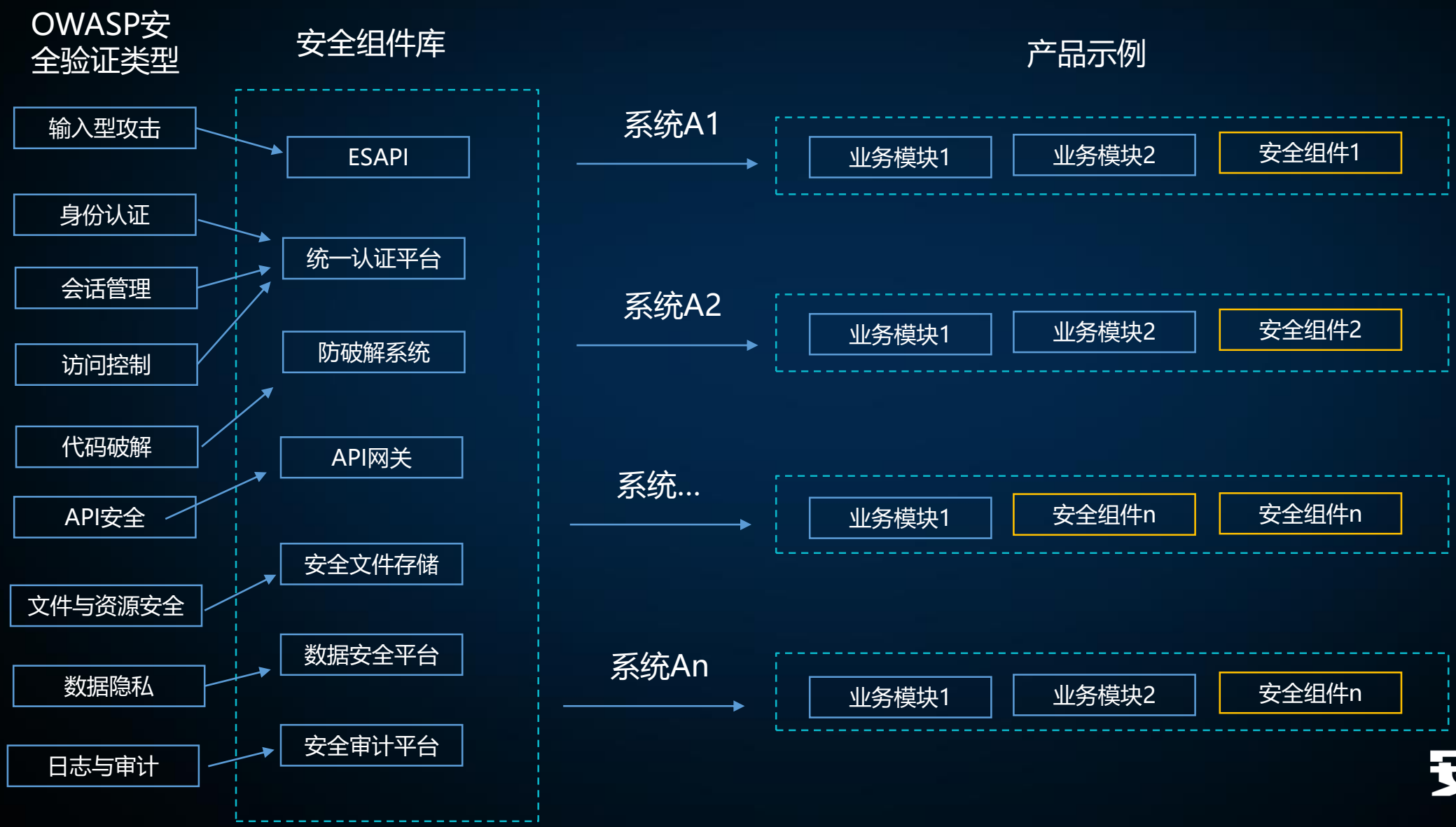


安世加

底线管控策略

- **为什么要底线管控**
  - ✓ 明确最低安全要求
  - ✓ 防止安全投入不足
- **如何底线管控**
  - ✓ 发布底线要求（精简、明确、利于执行、周期调整）
  - ✓ 制定底线管理办法
  - ✓ 建立审查和惩奖机制
- **常用底线管控样例**
  - ✓ 合规性管控底线，比如：APP应用必须参考《APP违法违规收集使用个人信息行为认定方法》进行上线前合规检测
  - ✓ 技术路线选型管控底线，比如：禁止使用GPL协议产品或代码；禁止使用fastjson
  - ✓ 运维部署管控底线，比如：禁止存在高危漏洞的应用系统上线发布；禁止高危端口对互联网开放；

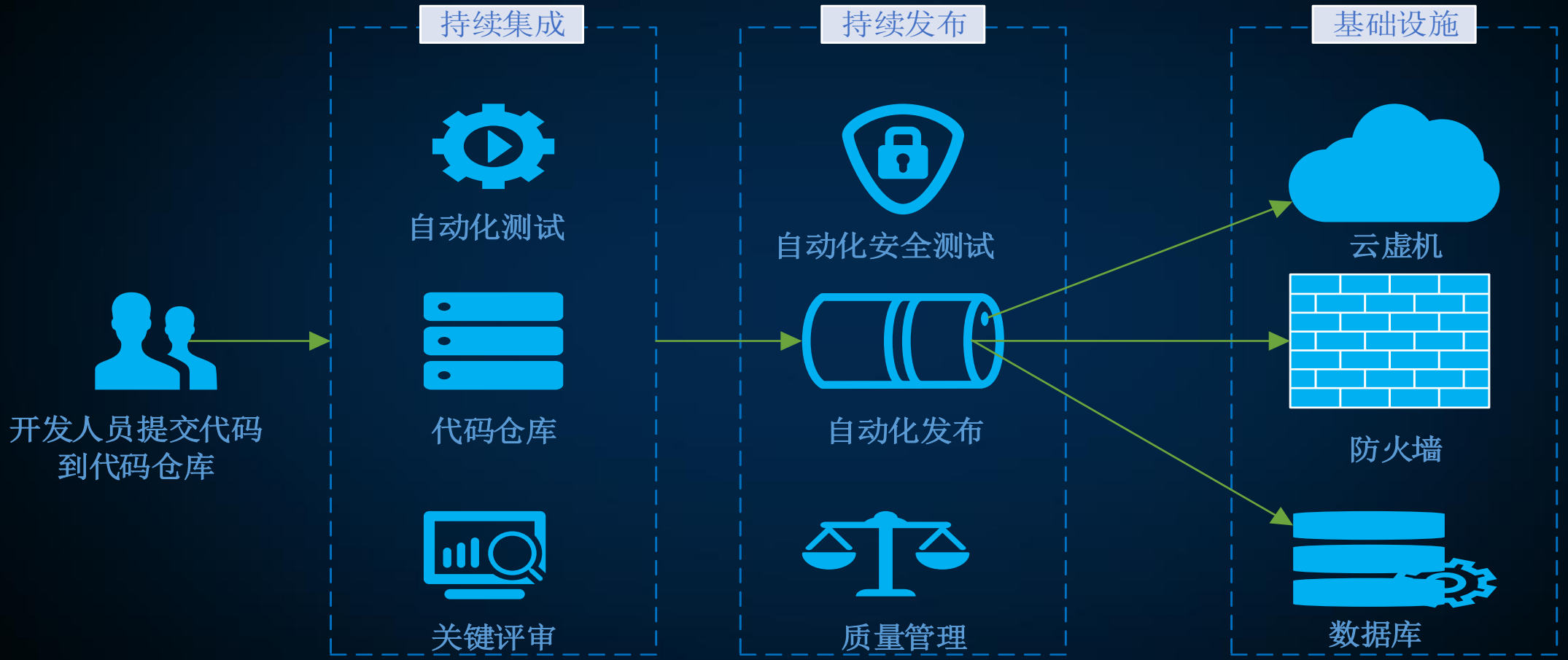
公共组件策略



- ✓ 专业的人做专业的事
- ✓ 通过安全组件的复用，降低软件架构的安全风险

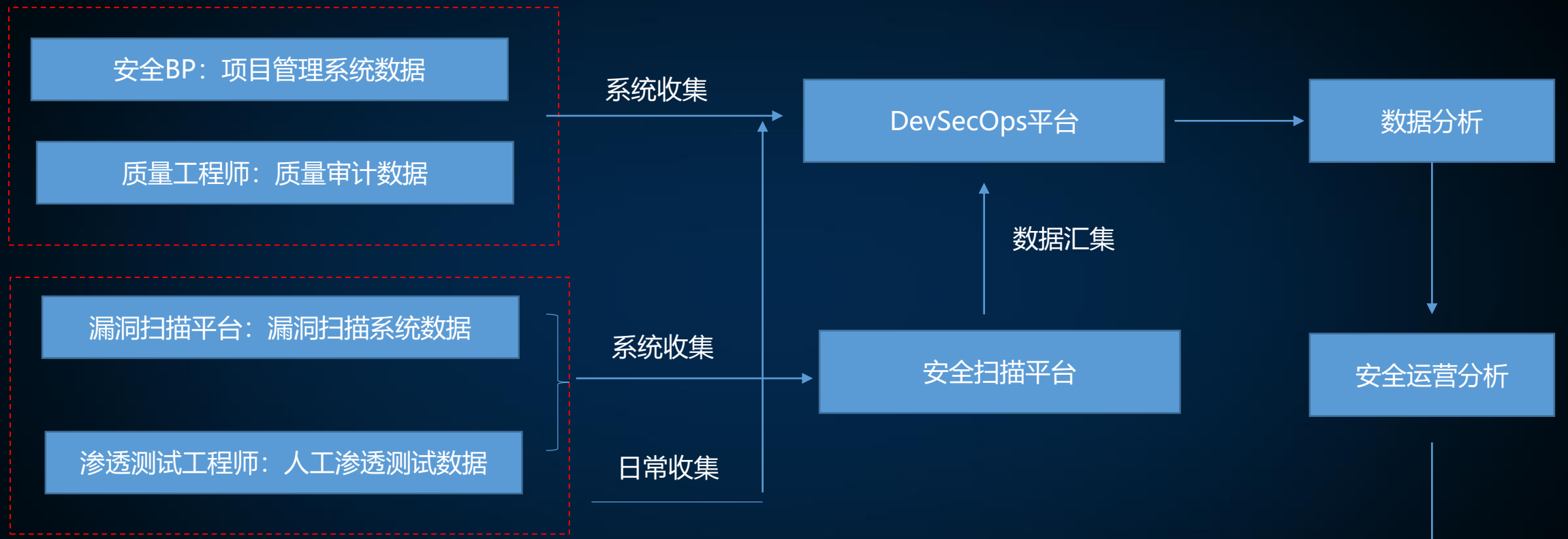
安世加

DevSecOps管道化策略



安世加

数字化运营策略



安全事件

- 安全事件数、安全事件危害等级

质量管理

- 线上发现问题数、底线管控符合度、研发过程漏洞总数、漏洞修复率

公共组件

- 复用数、缺陷数、需求响应度、客户满意度

安世加

未来展望

安世加

安世加 专注于安全行业，通过互联网平台、线下沙龙、培训、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站：http://anquanjia.net.cn/

微信公众号：asjeiss

安世加