58同城

2021

58同城 第2届 安全技术沙龙

业务风控建设 & 应用安全实践

58安全应急响应中心 Security Response Center | 58安全 58 CYBERSECURITY

DATE - 2021.12.17 线上直播

廖新喜

快手Web安全负责人

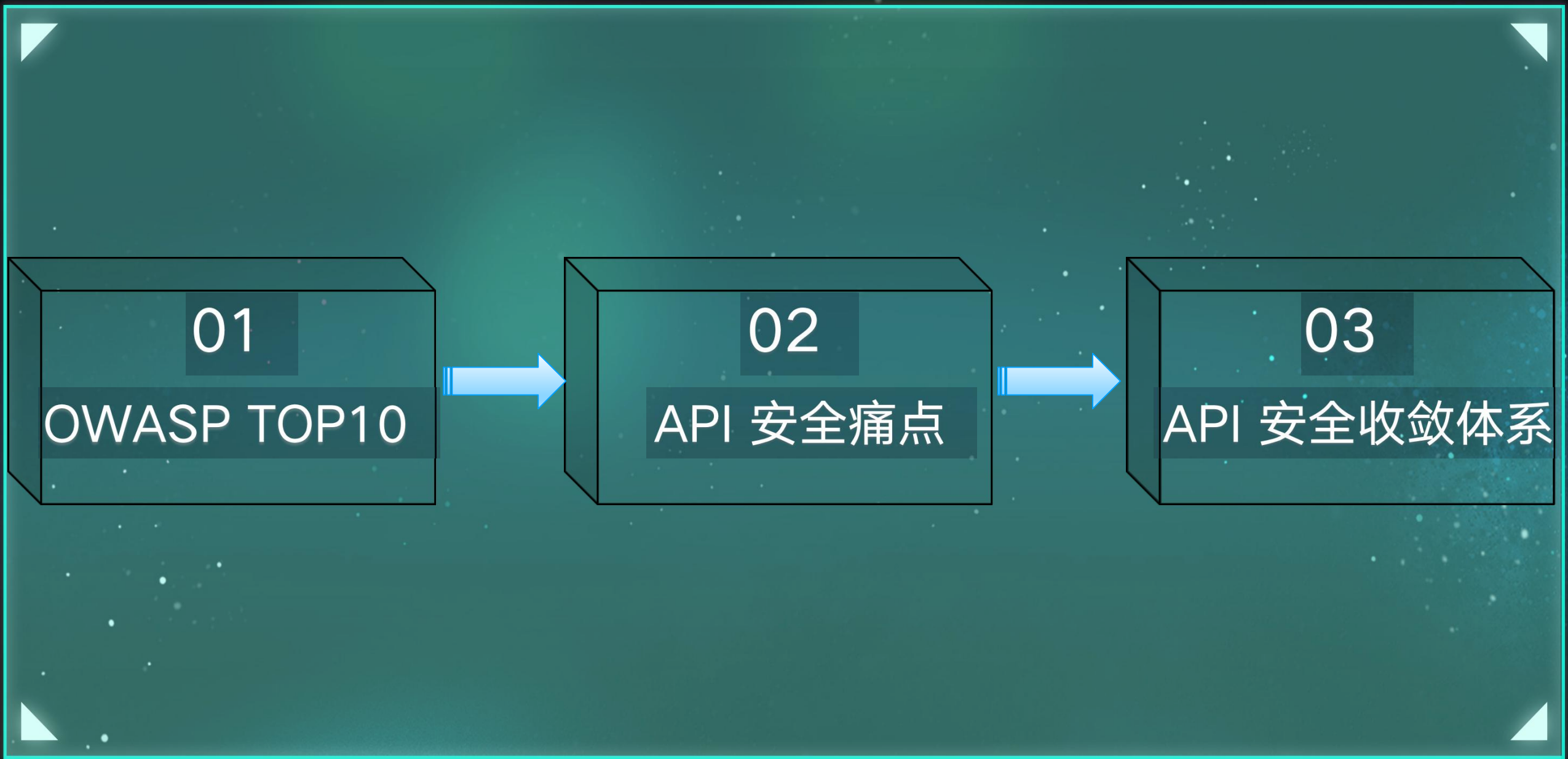
分享主题

API 安全

议题介绍

本议题主要介绍API 安全的发展现状、快手API 安全的痛点难点及对应的解决方案。个人觉得2021年OWASP TOP 10更加符合甲方现状，像前五大风险：越权、加密失败、注入、不安全设计和不安全配置。那这些痛点应该如何解决呢？传统的应用安全三板斧还有效吗？还需要引入其他应用安全能力吗？本议题将详细一一解析

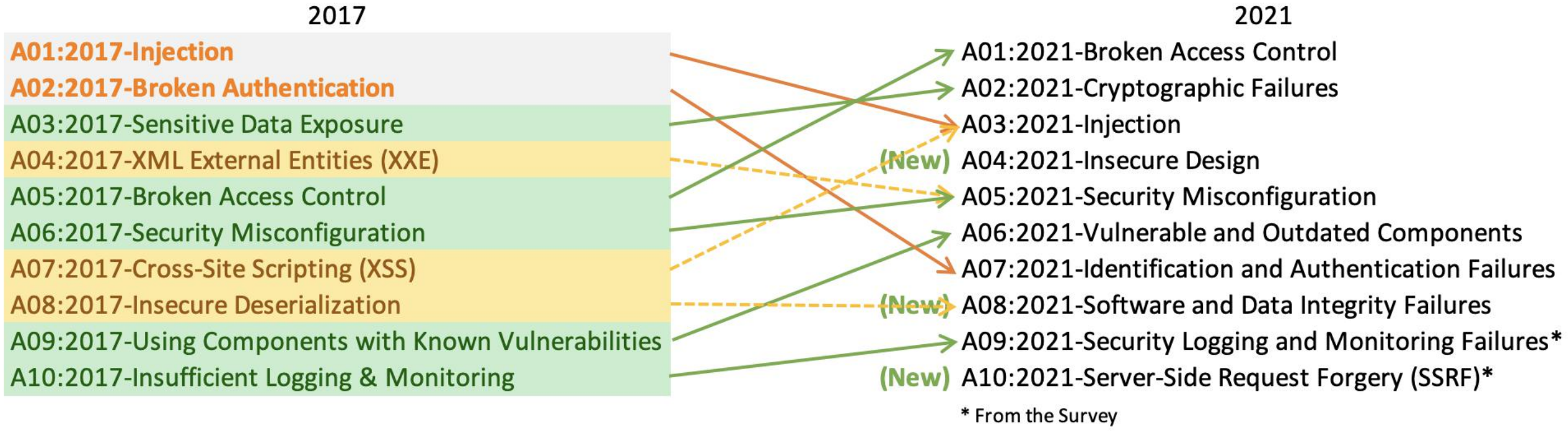
目 录



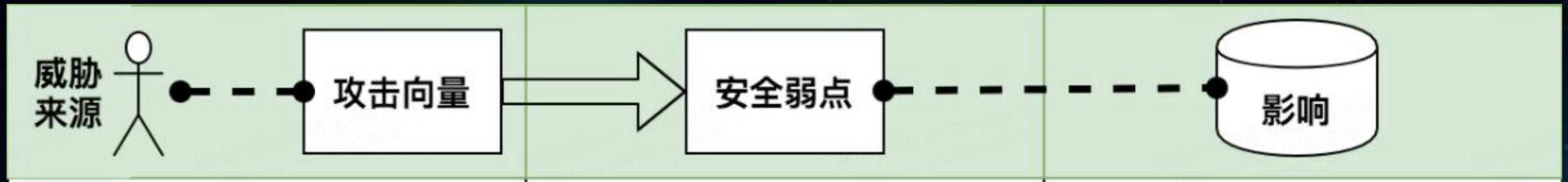
01

OWASP TOP 10

OWASP Top10

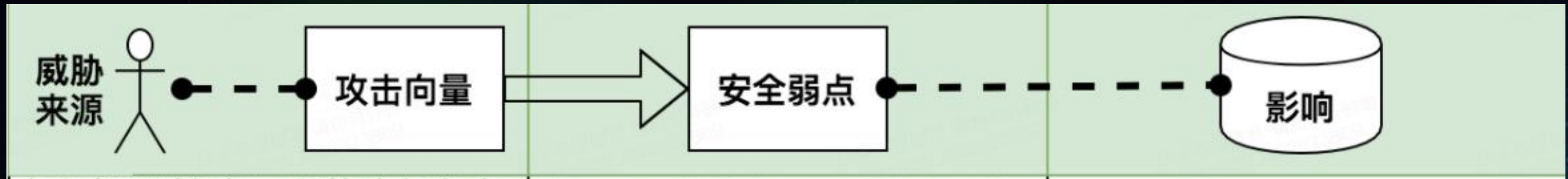

2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

A01:2021-失效的访问控制



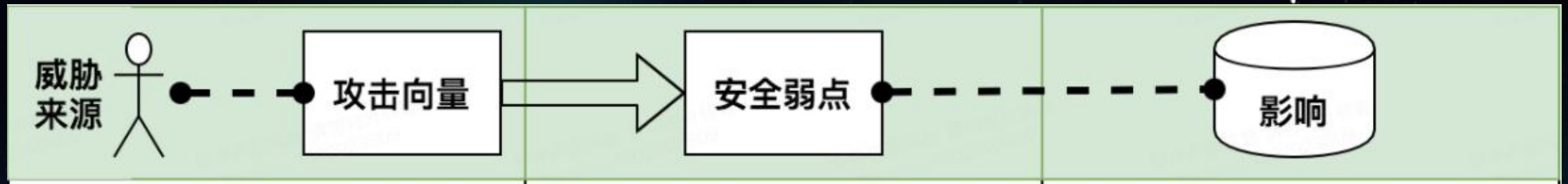
攻击者可以在发送的请求中改变对象 的ID来攻击存在“水平越权”漏洞的API。这将导致敏感数据的未授权访问。该问题在基于API的应用中非 常普遍，因为服务器通常不会完整地 跟踪用户的状态，而是依赖用户请求参数中的对象ID来决定访问哪些目标对象。	这已经成为最普遍、且影响广泛的API攻击。 授权和访问控制机制在现代应用中已经非常 复杂并广泛使用。即使应用已经实现了适当 的鉴权设施，开发者在访问敏感对象时仍可 能忘记使用这些鉴权设施。通常在静态或动 态测试中并不检查访问控制机制。	未授权访问将导致数据向未授权的组织披露、数据丢失或数据篡改。未授权的对象访问也能导致整个账户被控制。

A03：2021-注入



攻击者通过任何可用的注入方法(如， 直接输入、参数、集成服务等)向API 提供恶意数据，并期望这些恶意数据 被发送至解释器执行。	注入漏洞非常常见，通常出现在SQL、LDAP或者NoSQL查询、OS命令、XML解释器和ORM中。 攻击者可以使用扫描器或者模糊测试工具发现。	注入会导致信息泄漏和数据丢失。还可能导致DoS，或者主机被接管。

A05:2021-配置错误



攻击者通常会试图查找未修补的缺陷、 公共端点或未受保护的文件和目录， 以获取对系统未经授权的访问或了解。	从网络层到应用层，在API的任何层级都可能发生安全配置错误。自动化工具可用于检测和利用不必要的服务或遗留选项等错误配置。	安全配置错误不仅会暴露敏感用户数据，还包括系统细节，而这些细节可能导致服务器完全被控制。

02

API 安全痛点

甲方漏洞现状

编号	漏洞标题	定义
1	水平越权	对象级别的越权，通过某个遍历参数可以访问到其他对象资源
2	过度数据暴露	依赖通用方法，开发人员倾向于公开所有对象属性而不考虑其各自的敏感度，依赖客户端在向用户显示数据前执行数据筛选，返回的数据也缺失脱敏操作
3	注入	当不受信任的数据作为命令或查询的一部分发送给解释器 时，就会出现注入缺陷，如SQL、NoSQL、命令注入等。 攻击者的恶意数据可诱使解释器在未经恰当授权的情况下执行非预期的命令或访问数据
4	业务安全缺陷	业务逻辑上的缺陷，主要是过分信任用户的输入，这些漏洞跟业务强相关
5	安全配置错误	安全错误配置通常是由于不安全的默认配置、不完整或临 时配置、开放云存储、开发swagger，配置错误的HTTP 头、不必要的 HTTP 方法、允许跨域资源共享(CORS)和包含敏感信 息的详细错误消息造成的
6	高并发缺陷	攻击者通过并发http/tcp请求而达到次获奖、多次收获、多次获赠等非正常逻辑所能触发的效果，一般都是系统幂等性设计缺失或者错误导致的额

痛点

=LE多

发版快

敏感多数据

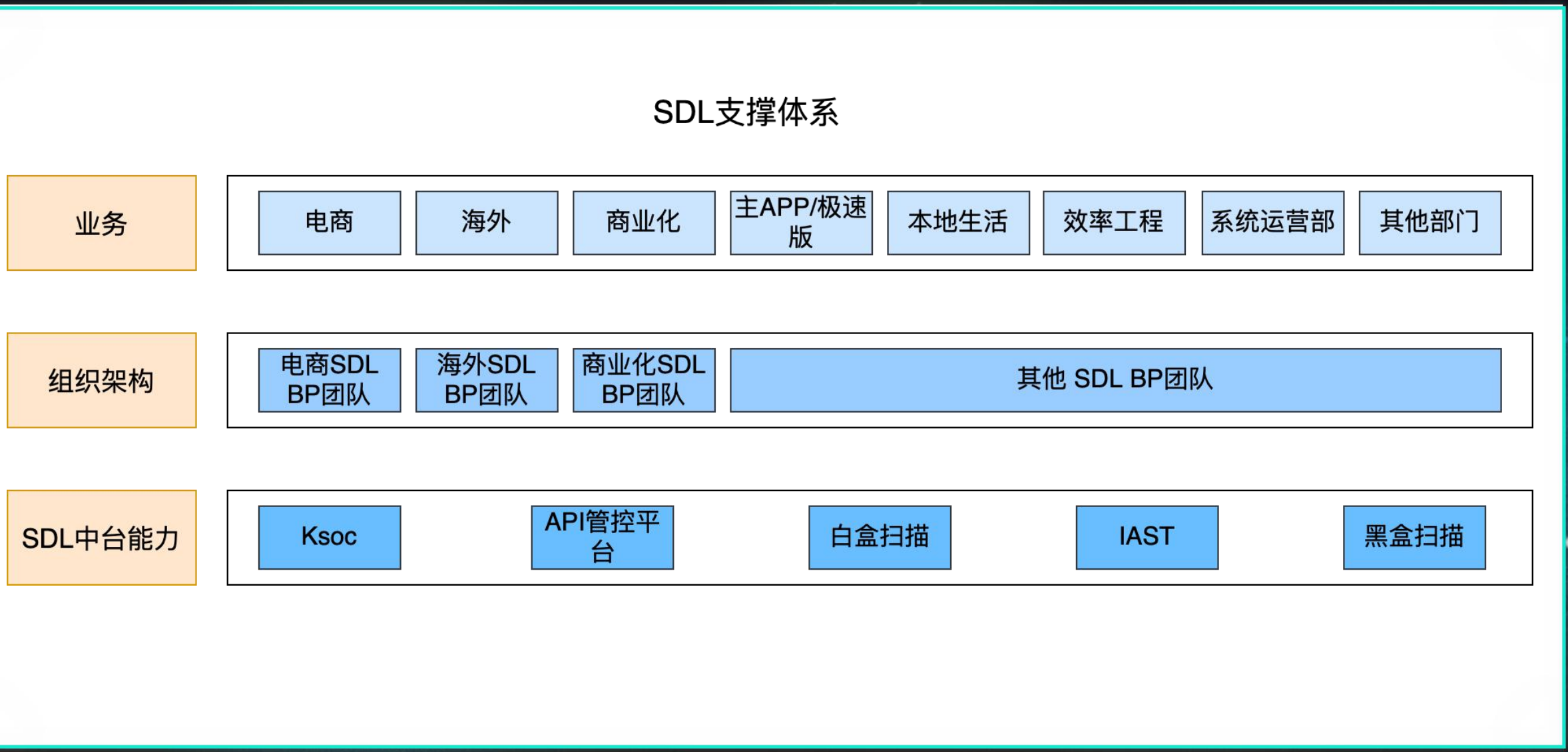
越权占比高

人力支撑困难

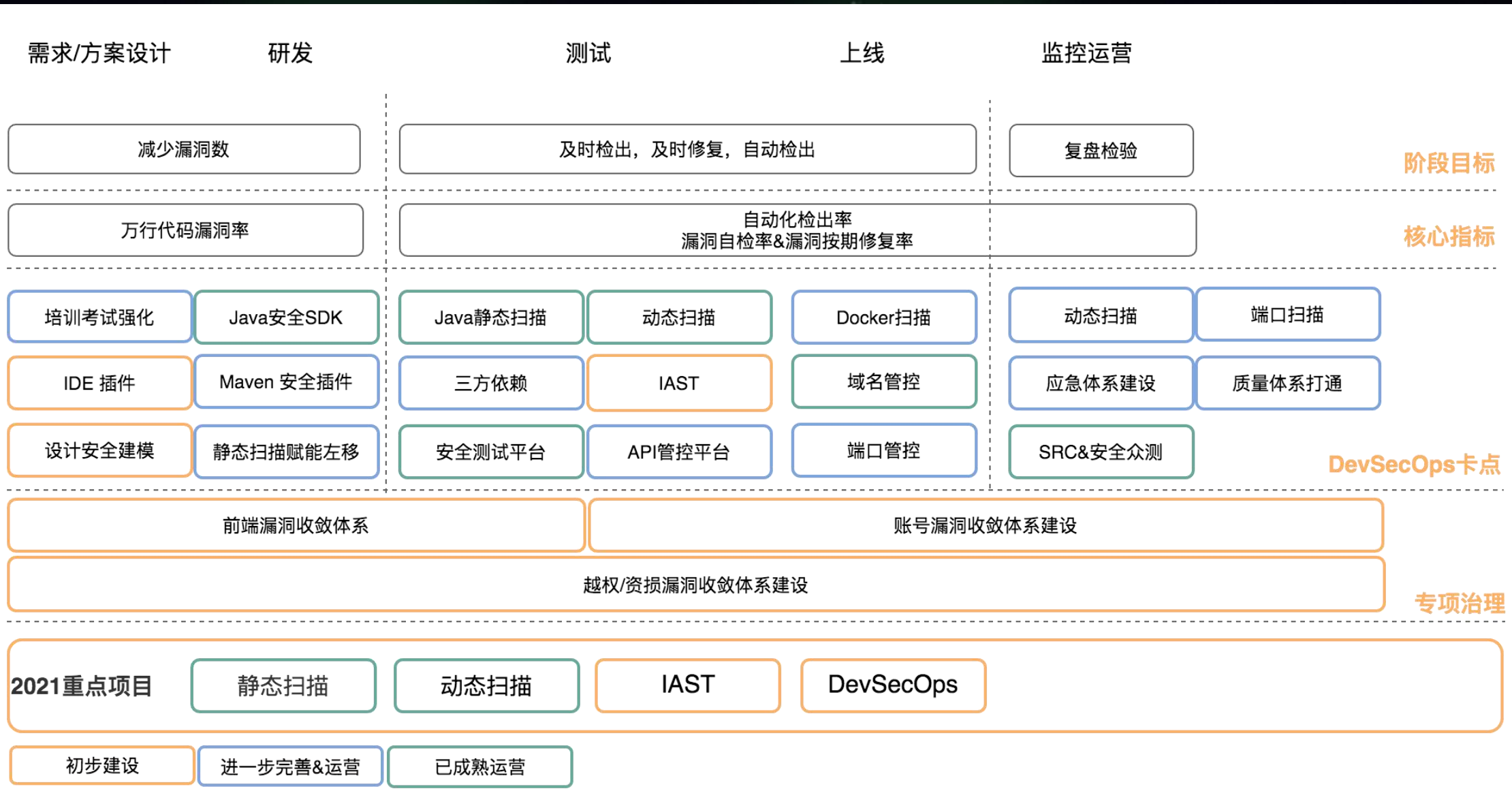
03

API 安全收敛体系

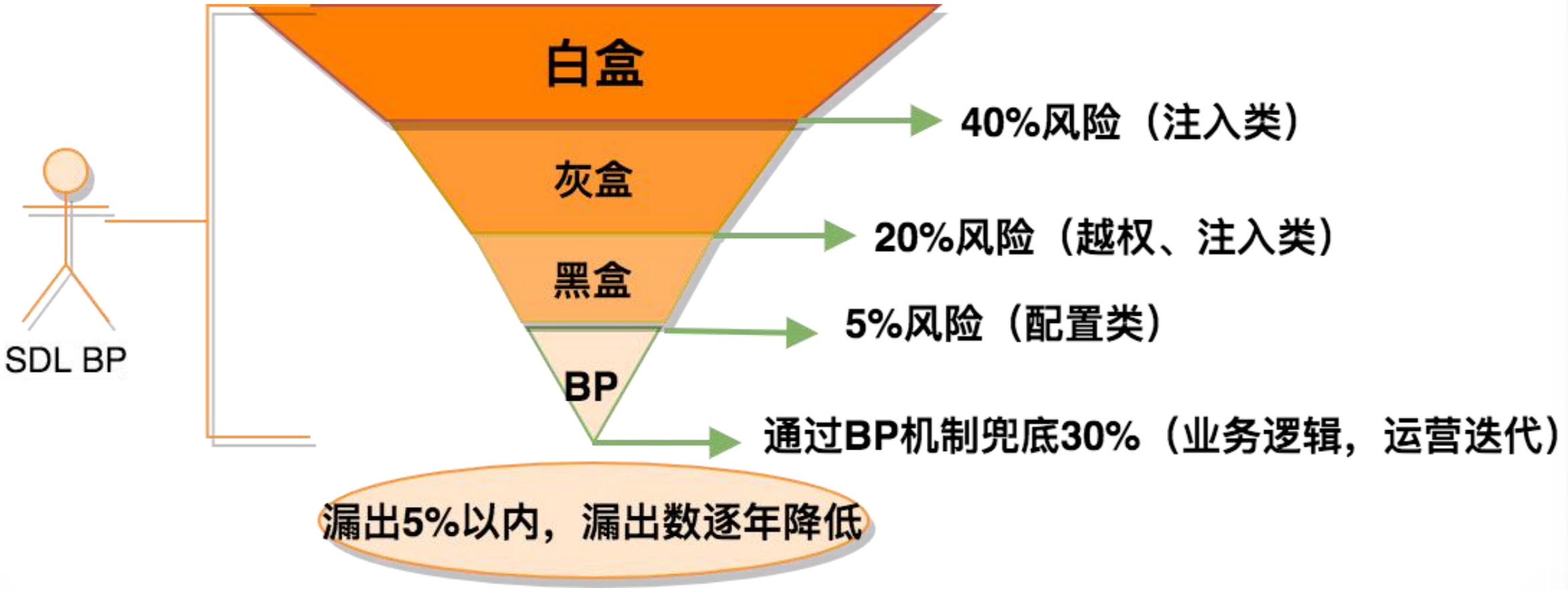
SDL BP架构


SDL支撑体系
业务
电商
海外
商业化
主APP/极速版
本地生活
效率工程
系统运营部
其他部门
组织架构
电商SDL BP团队
海外SDL BP团队
商业化SDL BP团队
其他 SDL BP团队
SDL中台能力
Ksoc
API管控平台
白盒扫描
IAST
黑盒扫描

漏洞收敛体系

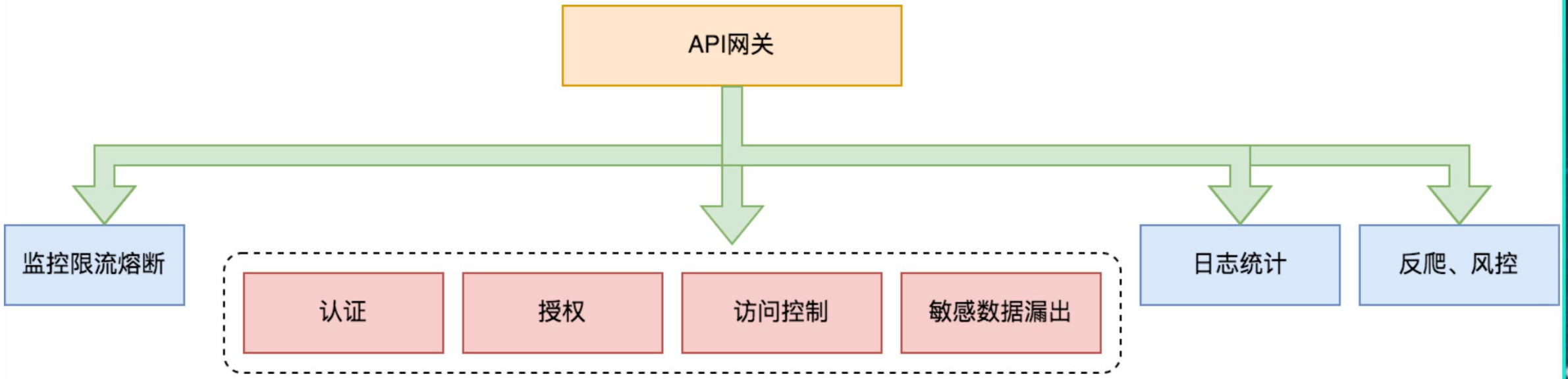

需求/方案设计
研发
测试
上线
监控运营
减少漏洞数
及时检出，及时修复，自动检出
复盘检验
阶段目标
万行代码漏洞率
自动化检出率
漏洞自检率&漏洞按期修复率
核心指标
培训考试强化
Java安全SDK
Java静态扫描
动态扫描
Docker扫描
动态扫描
端口扫描
IDE 插件
Maven 安全插件
三方依赖
IAST
域名管控
应急体系建设
质量体系打通
设计安全建模
静态扫描赋能左移
安全测试平台
API管控平台
端口管控
SRC&安全众测
DevSecOps卡点
前端漏洞收敛体系
账号漏洞收敛体系建设
越权/资损漏洞收敛体系建设
专项治理
2021重点项目
静态扫描
动态扫描
IAST
DevSecOps
初步建设
进一步完善&运营
已成熟运营

应用安全三板斧

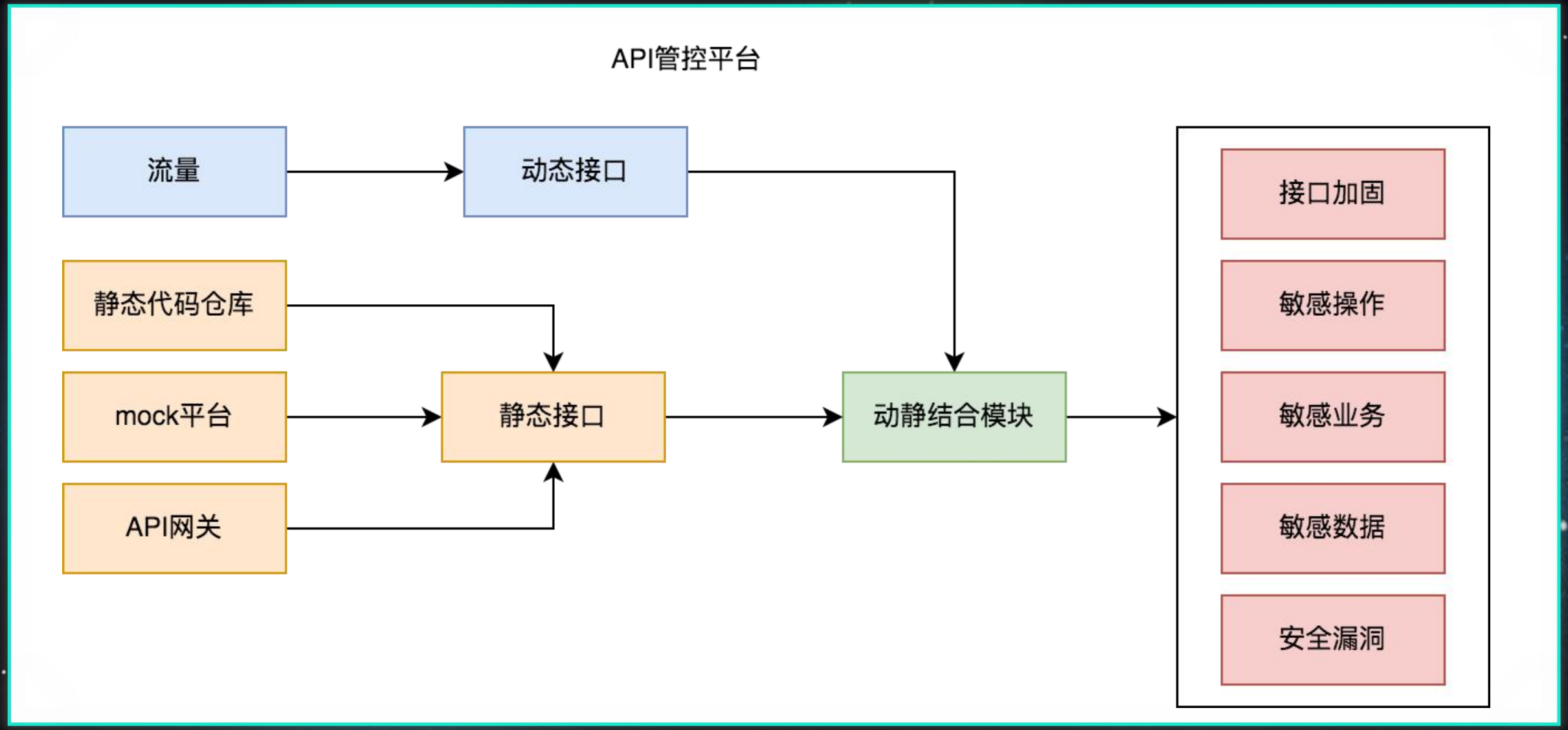

白盒
灰盒
黑盒
BP
SDL BP
40%风险（注入类）
20%风险（越权、注入类）
5%风险（配置类）
通过BP机制兜底30%（业务逻辑，运营迭代）
漏出5%以内，漏出数逐年降低

应用安全三板斧之IAST

API 网关



API 管控平台


API管控平台
流量
动态接口
静态代码仓库
mock平台
API网关
静态接口
动静结合模块
接口加固
敏感操作
敏感业务
敏感数据
安全漏洞

提问环节