OWASP

Open Web Application Security Project

业务上线前后的漏洞管理实践

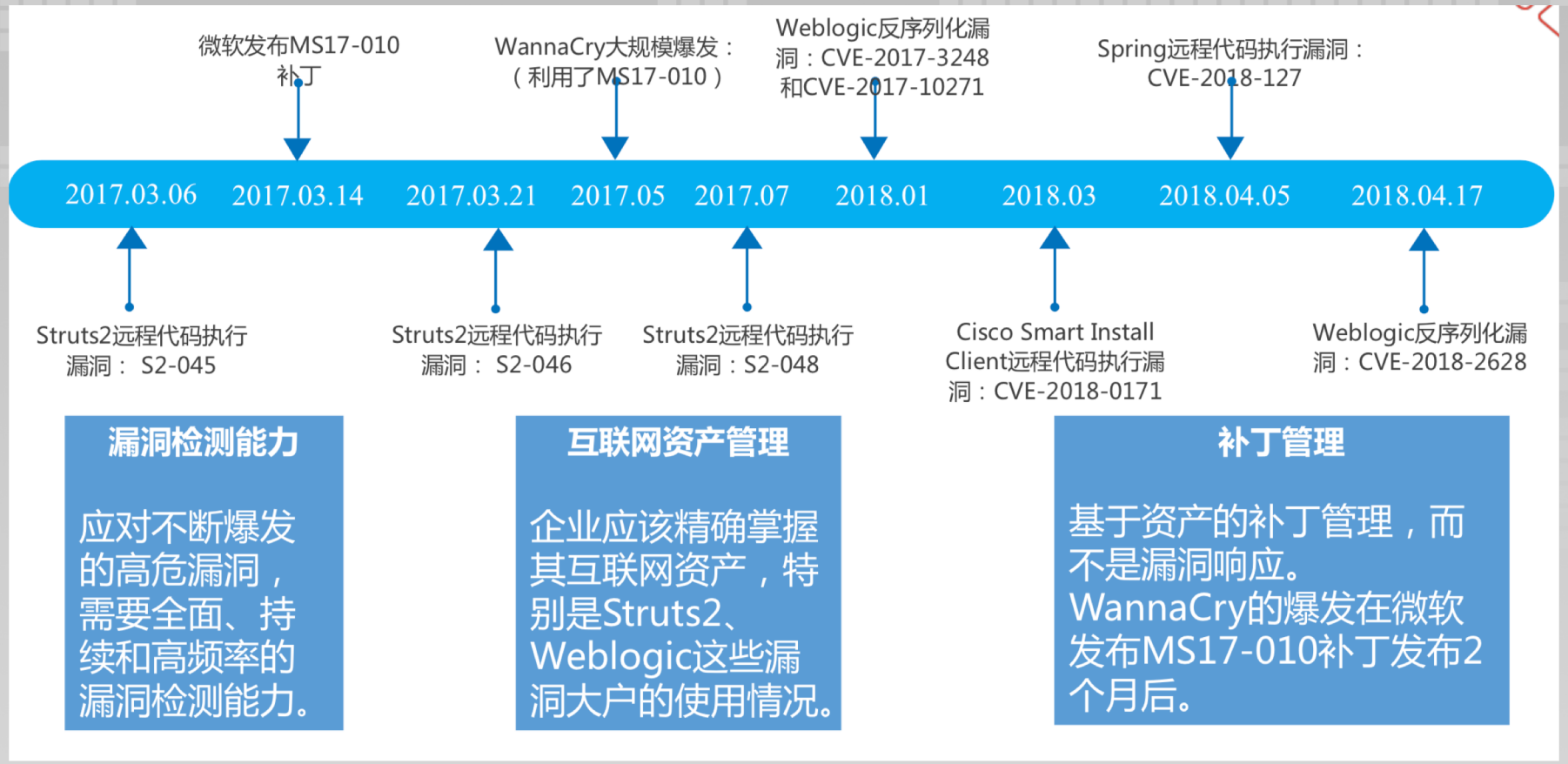
李俊 魔方安全

目录

2 业界实践—互联网公司业界实践

- 小米
  https://sec.xiaomi.com/article?id=5 （安全扫描自动化检测平台建设）
- 携程
  http://mp.weixin.qq.com/s/OtqJ-14vEPEcLmf4Ctk7vQ （携程安全自动化测试之路）
- 腾讯
  https://security.tencent.com/index.php/blog/msg/100 （自研之路：腾讯漏洞扫描系统的十年历程）

某大型券商漏洞管理实践



某大型券商漏洞管理实践

漏洞运营过程中的痛点

我们的实践

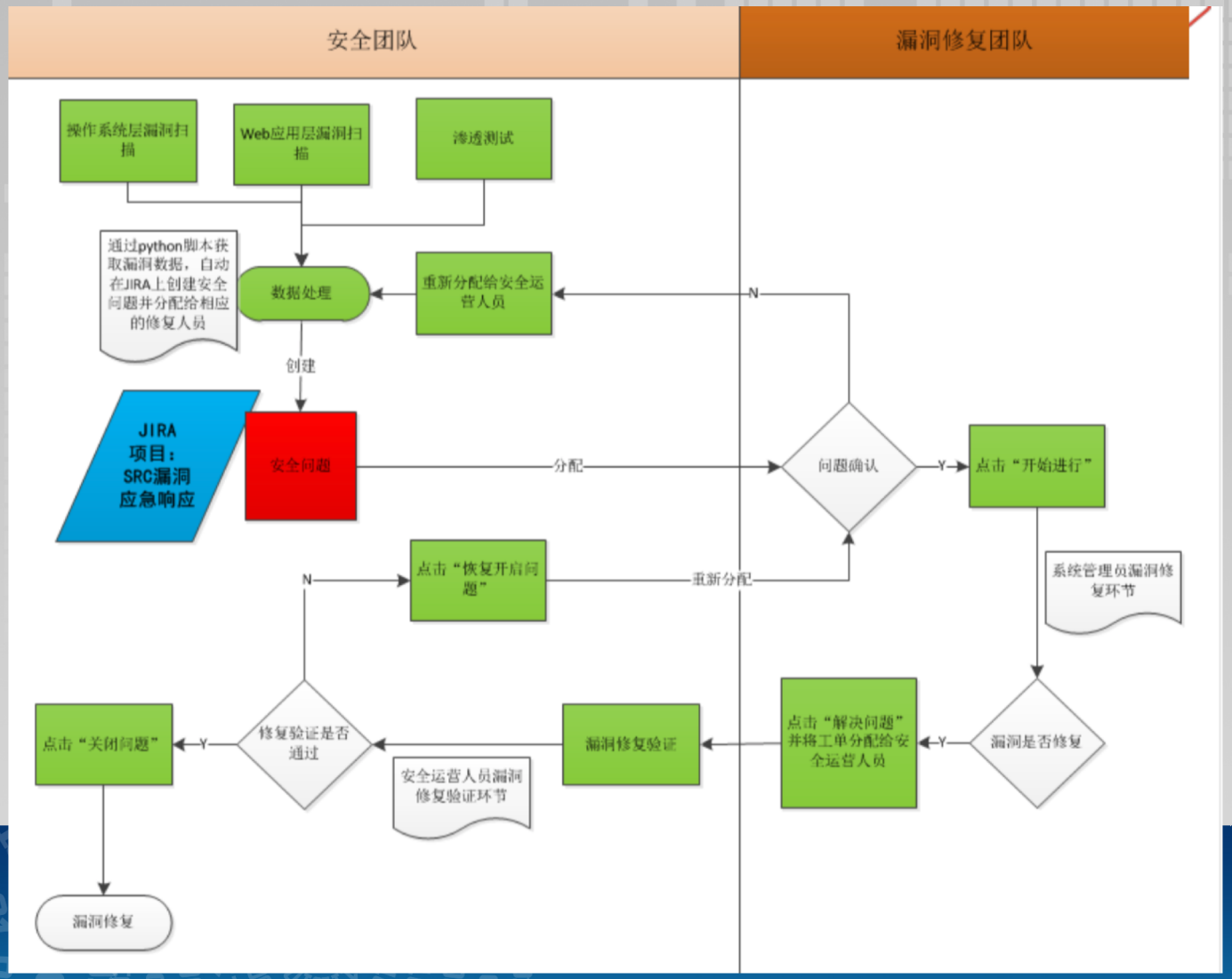
某大型券商漏洞管理实践

漏洞检测手段	检测方式	检测频率	扫描目标
互联网侧主机层漏洞扫描	网络扫描	每周三次	全网互联网IP地址
互联网web应用层漏洞扫描	网络扫描	每周一次	全网互联网web应用URL
内网侧主机层漏洞扫描	网络扫描 +Agent扫描	每周一次	核心网所有IP地址
外部渗透测试	人工	每两个月一次	公司所有互联网应用，含APP应用

某大型券商漏洞管理实践

漏洞类型	举例	修复优先级
已被exploited的RCE（远程命令执行）漏洞	Struts2 S-045、S-046、S-048、Oracle WebLogic Server Java Deserialization Remote Code Execution、MS17-010等等，常用于直接拿下互联网边界的一台服务器，再做进一步渗透或横向移动。	极高
其他已被exploited的远程利用漏洞	Struts2 S2-049等一些可导致拒绝服务攻击，服务器信息泄漏类型的漏洞。	高
已被exploited的本地利用漏洞	多用于提权，如Nginx的本地提权漏洞CVE-2016-1247	中高
其它漏洞	SSL自签证书、SSL版本低，SSL证书不被信任等	中低

某大型券商漏洞管理实践



某大型银行漏洞管理实践

- **互联网资产庞大：**子域名、高危端口与组件、可扫描站点众多，难以覆盖全面，频度要求一天一扫描
- **风险监控：**无法有效对互联网业务进行持续的风险监测和0day漏洞预警
- **源码监控：**无法有效国内外开源社区进行监控
- **内网扫描全面性与频度：**nessus、awvs、appscan，无法统一管理，也无法横向对比，扫描频度要求每周一次
- **漏洞管理：**缺乏工具进行漏洞精细化跟踪和度量

③某大型银行漏洞管理实践

目录

1 业务上线前后面临的挑战

- **挑战来自于三个方面：**

1、外部威胁：安全漏洞的爆发频率、范围，使得突发性的漏洞应急工作越来越普遍；

2、IT格局变化：企业的IT规模可以快速扩张，边界开始模糊；

3、自身业务发展：企业的互联网化带来业务和开发的快速迭代，使得安全问题更为普遍；

- **漏洞发现与管理的主要演变：**

1、从单一的针对漏洞发现，扩展到资产识别、资产异动变化；

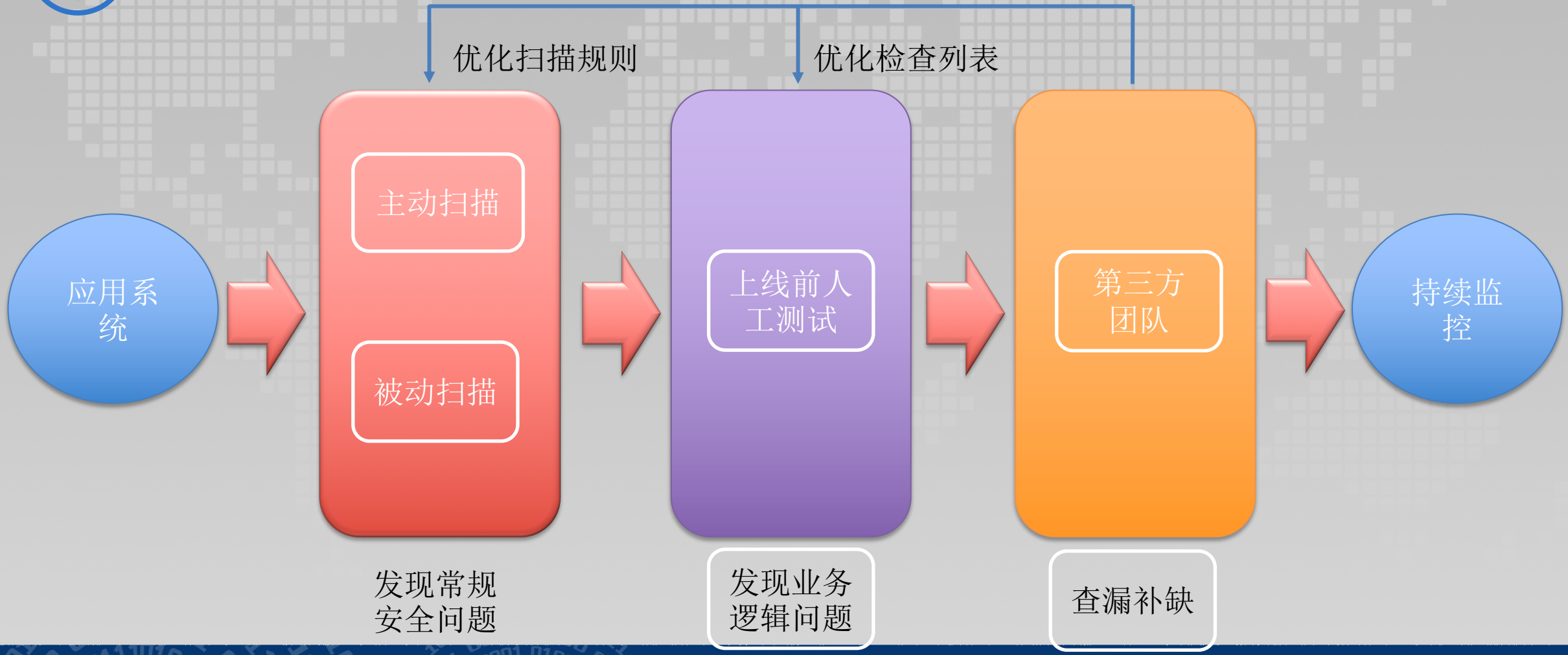
2、从单一节点的扫描方式，扩展到分布式可扩展；

3、从安全主动发起到如何与业务、流程结合；

4、漏洞有效跟踪和管理、沉淀；

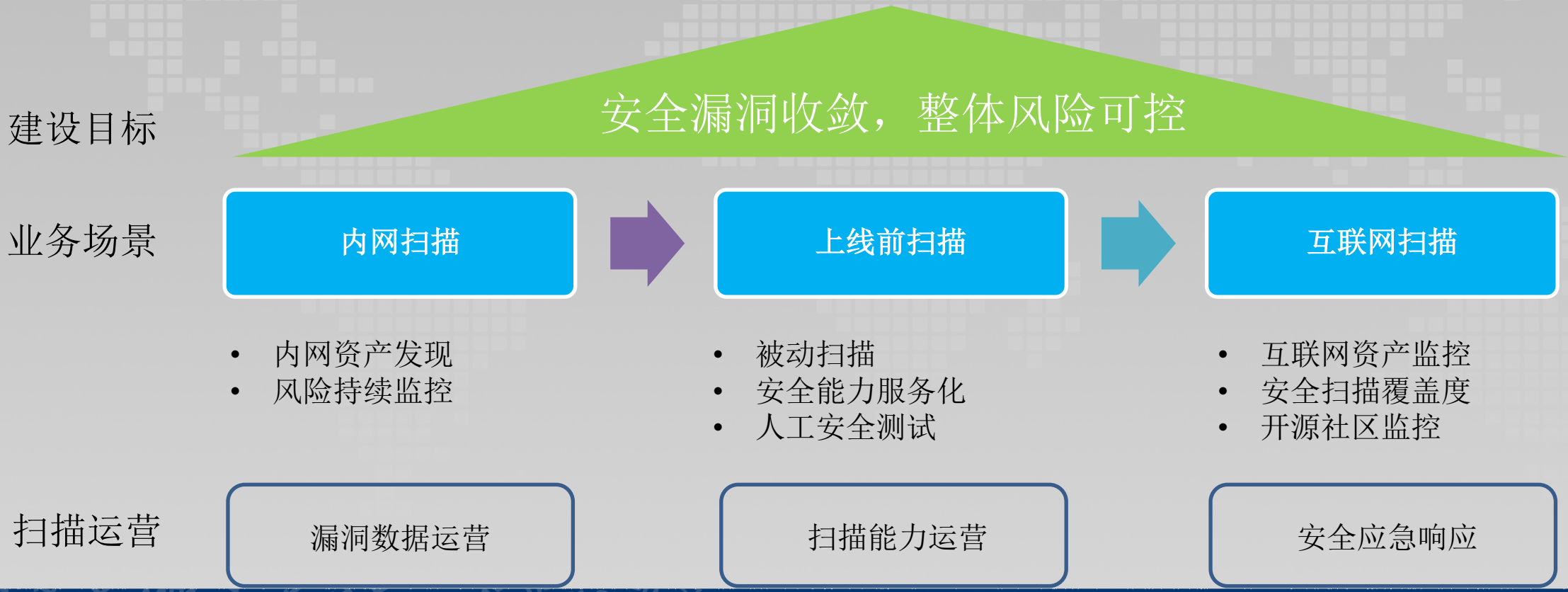
目录

2 应用安全实践方法论

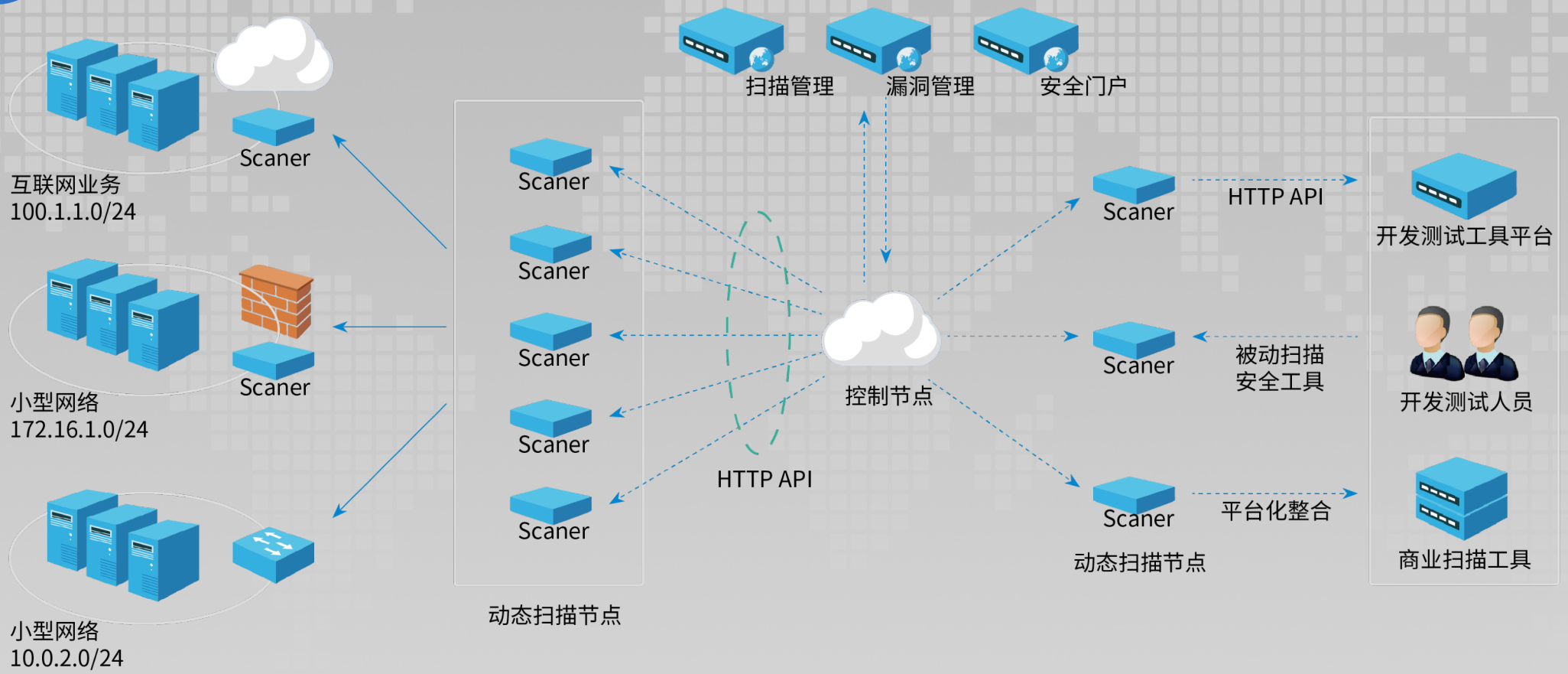

优化扫描规则
优化检查列表
应用系统
主动扫描
被动扫描
上线前人工测试
第三方团队
持续监控
发现常规安全问题
发现业务逻辑问题
查漏补缺

2 新一代安全扫描实践

在企业的规模与业务快速增长的需求下，安全团队通过建设云扫描平台，提高风险发现能力与安全工作效率



2 全网安全扫描与漏洞管理平台



资产发现、漏洞监控

上线前扫描

1、适应快速变化的环境，可弹性扩展；
2、可与内部流程、系统快速整合；
3、扫描可运营；

2 安全扫描运营流程

互联网监控

资产输送

内网扫描平台

各类扫描工具联动

Nessus vulnerability scanner

acunetix WEB APPLICATION SECURITY

HP WebInspect

漏洞自动化归集

漏洞管理平台

内部的ITIL系统

对接开发测试

Jenkins

运维管理系统

资产数据关联

网络准入

2 内网扫描

特点：环境复杂覆盖难度大

要求：全面覆盖，出现紧急事件时可快速响应

资产发现与持续监控

- 全网资产发现
- 风险持续监控

扫描策略制定

- 全量扫描
- 应急扫描
- 红线扫描
- 上线前扫描

扫描工具集中管理

- 扫描工具集中管理
- 结果统一回收

2 主要业务场景介绍—全网资产发现与持续监控

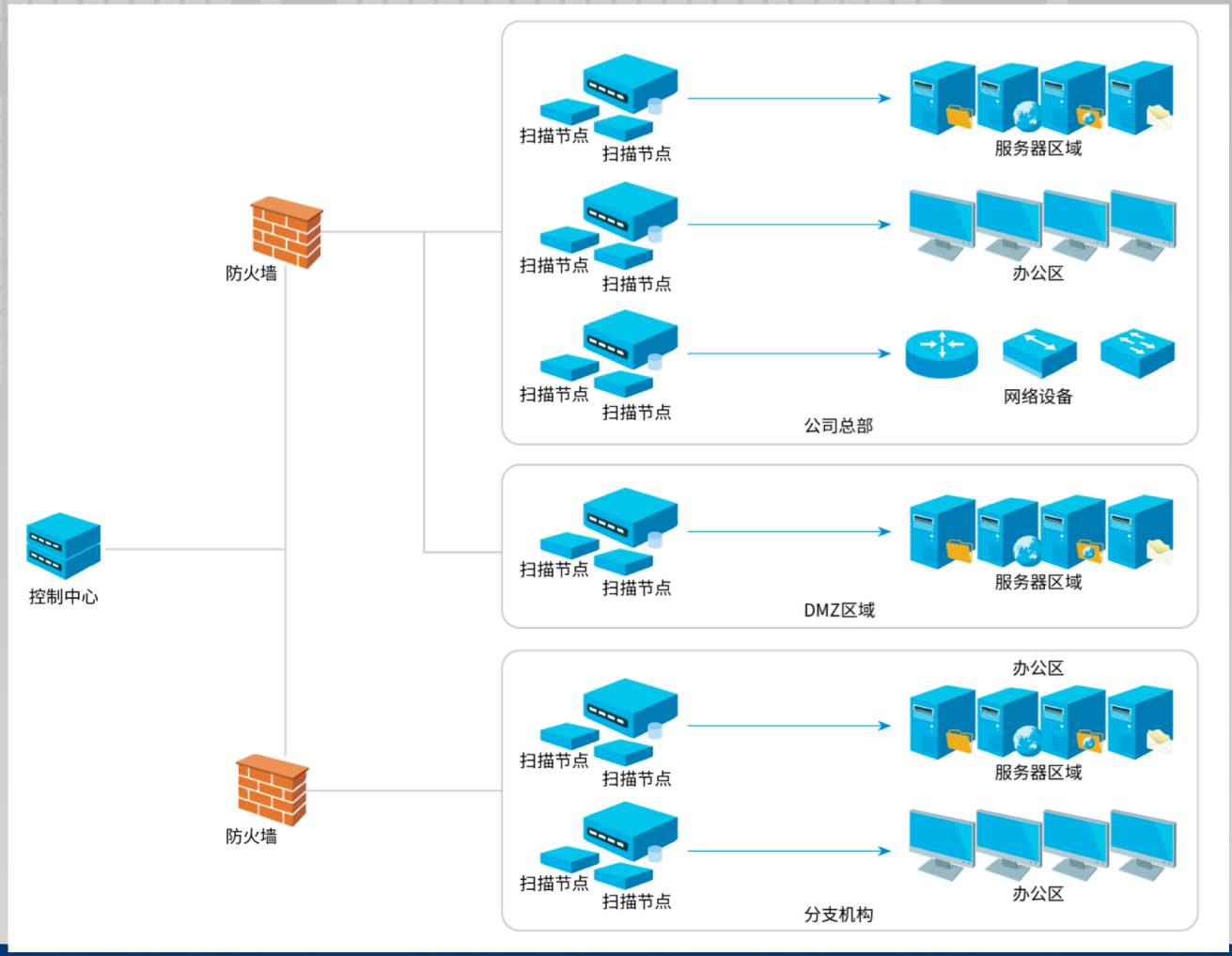
➢ 主要业务场景：

1.应急扫描：紧急任务，0day漏洞，安全事件，安全制度

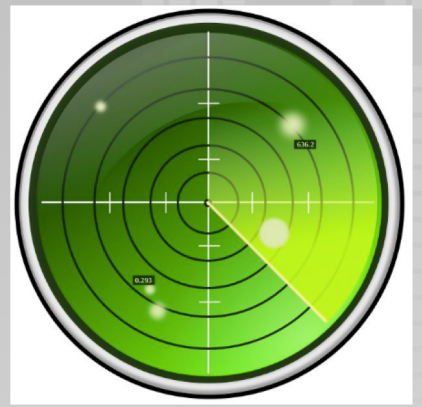
2.全量扫描：周期性的对全网安全资产进行全插件扫描

3.上线前扫描：对新上线的Web/服务器和存在服务变更的资产进行扫描

4.红线扫描：特定高危漏洞、默认口令的合集，全网持续性扫描



2 业务场景--扫描能力集成



内网扫描平台

各类扫描工具联动

1、统一管理
2、单一目标多个分发
3、结果统一回收

acunetix WEB APPLICATION SECURITY

Nessus® vulnerability scanner

NSFOCUS

AppScan IBM. Rational.

HP WebInspect™

BURPSUITE PROFESSIONAL

2 互联网扫描

特点：最大的风险暴露面

要求：快速感知互联网的变化，并发现自身的风险

互联网资产监控

- 未知资产发现
- 高危端口发现
- 管理后台发现
- 应用站点梳理

安全扫描覆盖度

- 持续周期性扫描
- 高危漏洞快速预警

敏感信息监控

- Github开源社区

2 业务场景--互联网资产发现与梳理

从黑盒与白盒两个角度发现企业外部资产并进行梳理

- 新增域名、IP业务
- 高危端口与管理后台发现
- 可扫描站点（200）、无法扫描站点（404、500等）

主域名

如test.com

子域名 a.test.com

IP 1.1.1.1

C网段 1.1.1.0/24

第三方组件 开发语言

数据库 Web应用

端口/服务

操作系统

2 上线前扫描

特点：业务快速迭代，守门式的安全测试效率低下

要求：在上线前仅可能的发现更多问题

被动扫描	安全能力服务化	人工安全测试
基于流量镜像	内部系统集成	业务逻辑
基于流量代理	安全工具集合	
基于Web日志		

2 主要业务场景介绍—被动扫描

➢ **被动扫描**，结合用户访问流量，获取会话并进行扫描。相比主动扫描：

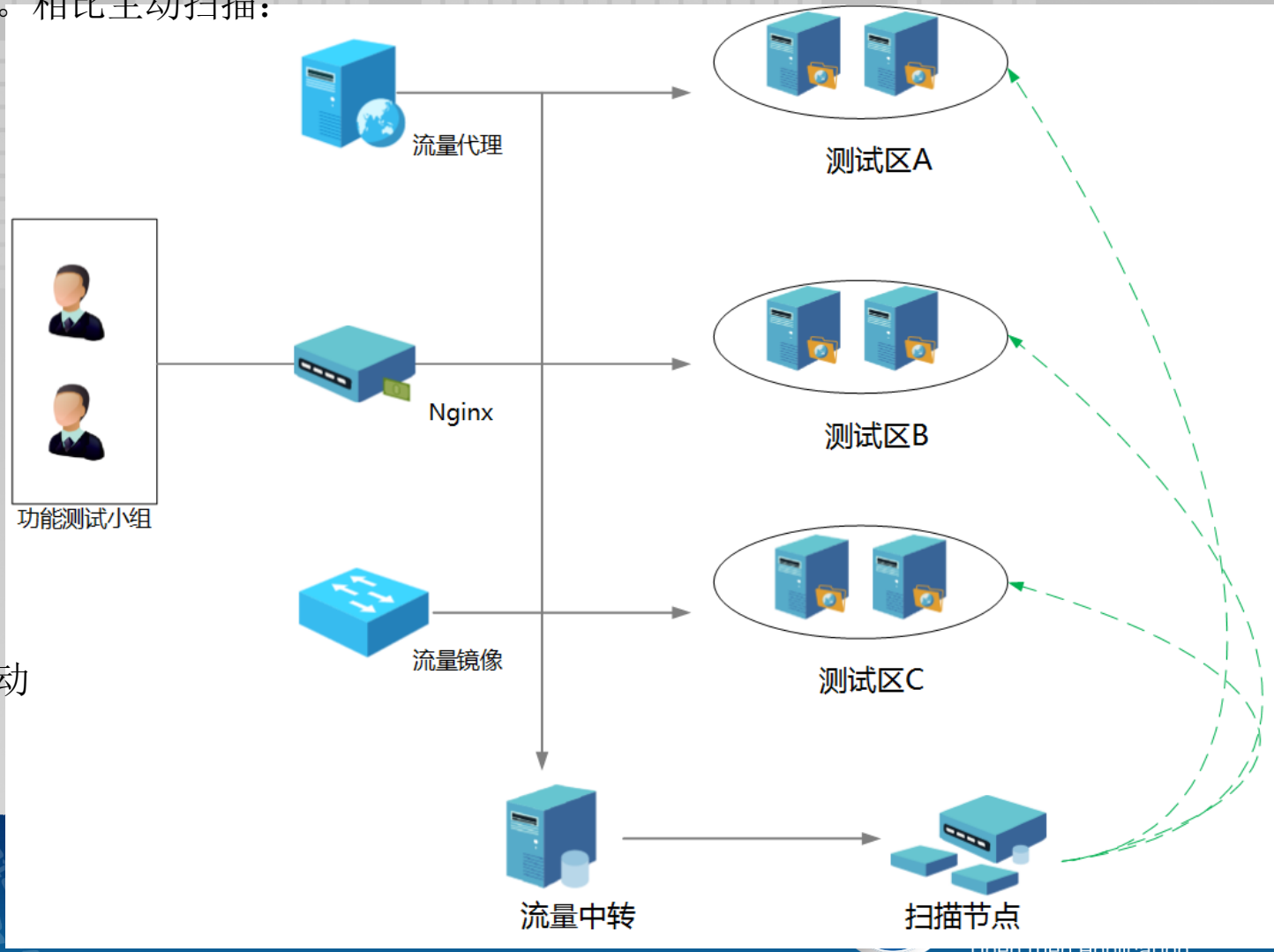
1、自动化程度高
2、可对具有交互行为的链接进行扫描
3、快速检查常规安全漏洞，覆盖度高

适合在开发测试环境中部署。

流量采集
- 流量镜像
- 流量代理
- nginx镜像

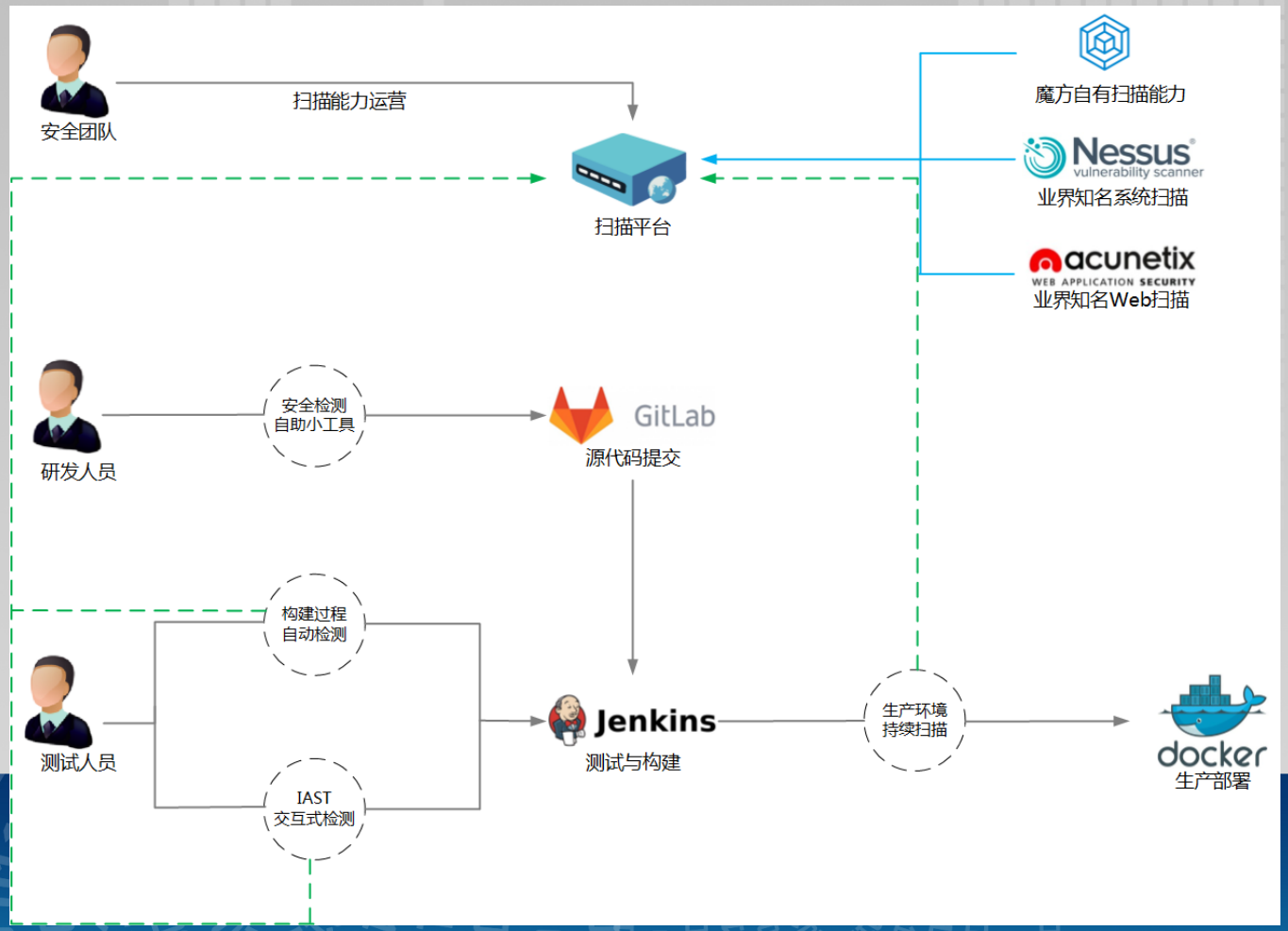
策略制定
- cookie替换
- 定时重放
- 第三方扫描工具联动

流量回放



2 业务场景—安全能力服务化

安全能力服务化，将安全检测能力通过对接内部系统或简易的工具集成到开发测试流程中，提高安全工作效率。



- 扫描能力集成至CMDB、研发管理平台等
- 简易的安全门户与扫描API，研发人员可简易使用
- 各类插件、流量代理等收集流量，执行被动扫描

2 数据运营

漏洞数据运营

- 漏洞管理
- 漏洞归档
- 安全工作量化

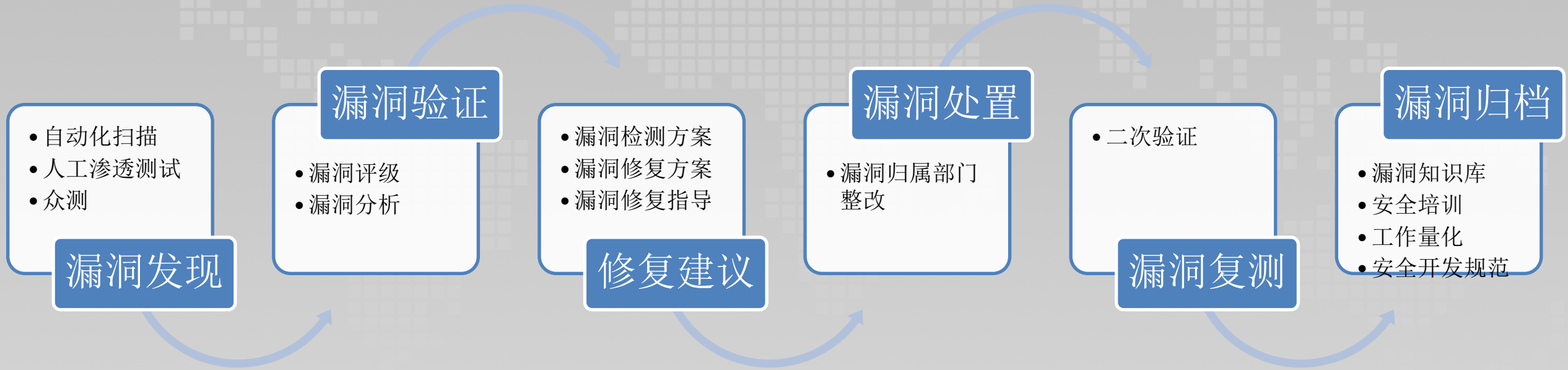
扫描能力运营

- 扫描能力优化
- 扫描规则自定义

应急响应

- 0day爆发全网预警

2 业务场景—漏洞跟踪与管理

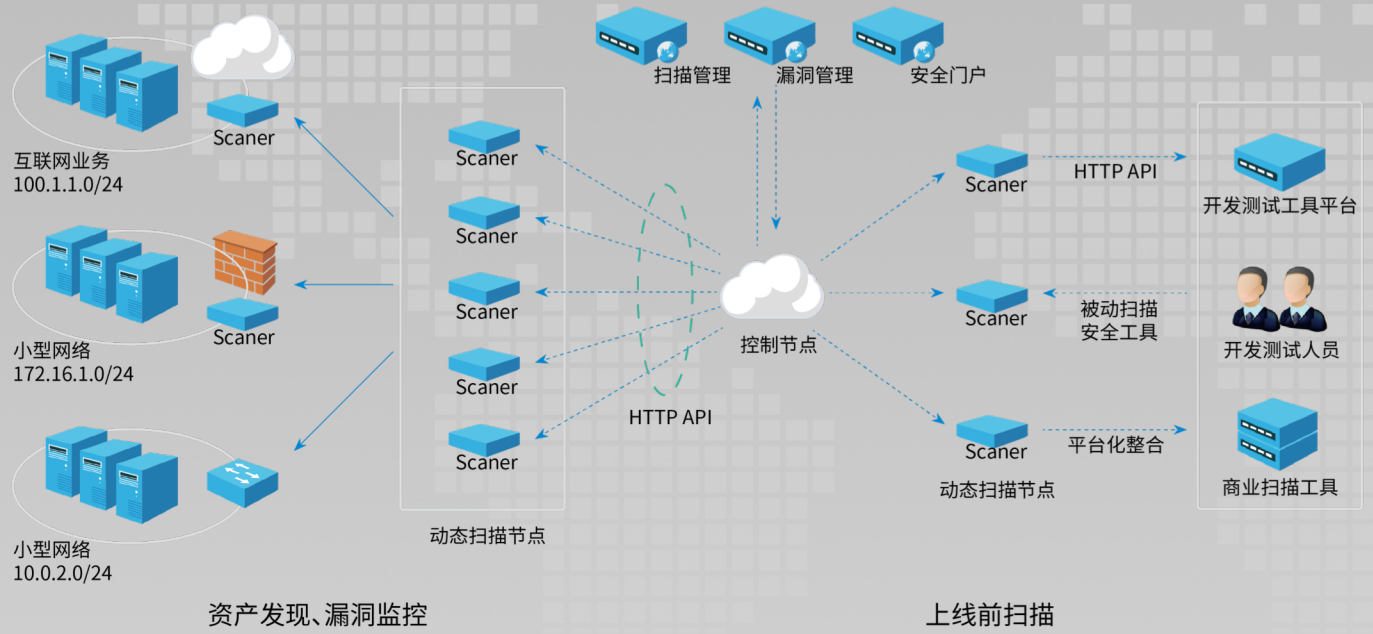


将漏洞作为企业一种有价值的“资产”来做管理

2 业务场景—扫描能力运营与应急响应

目录

3 某大型企业漏洞威胁感知云平台



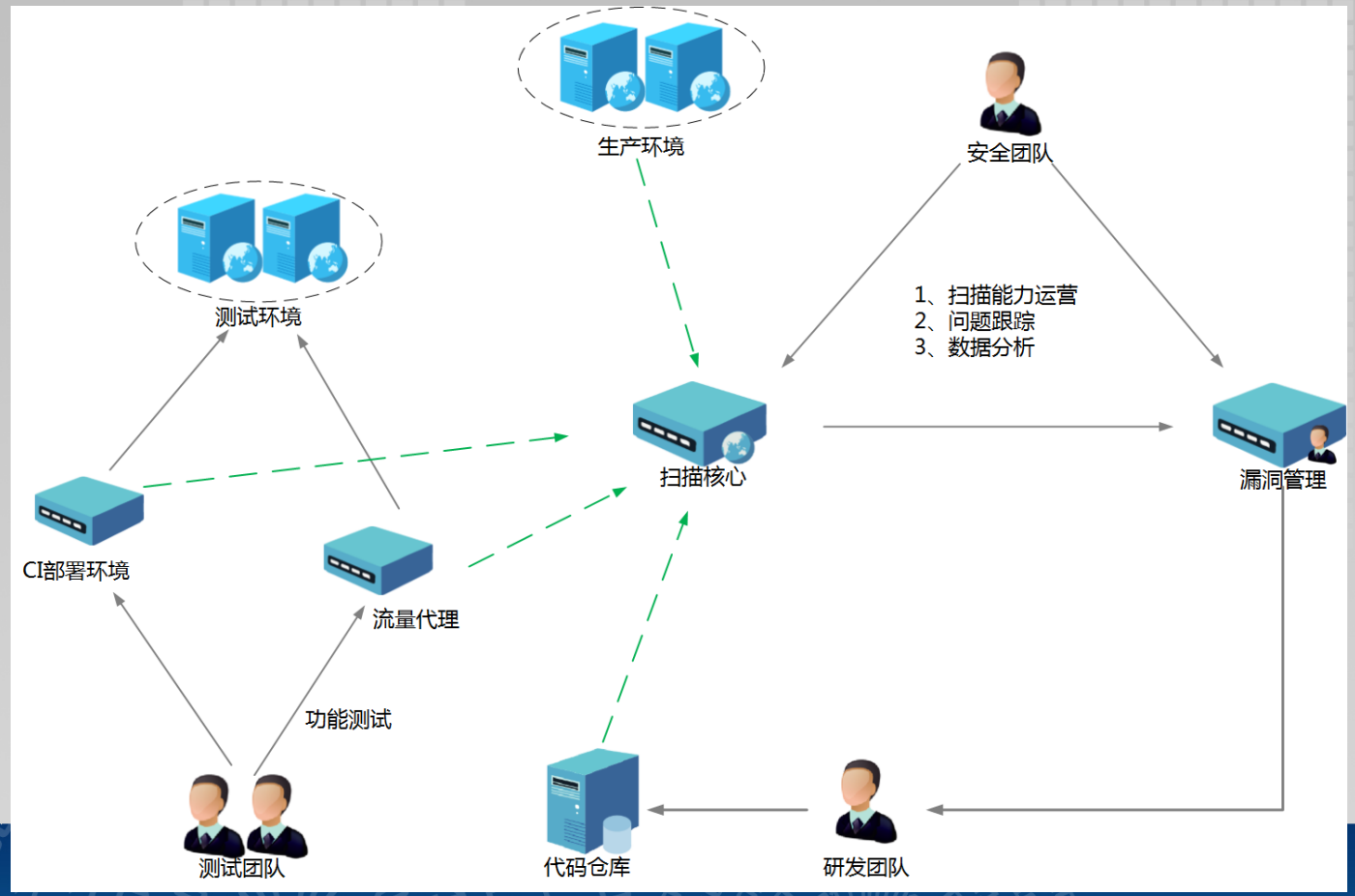
IT安全基础架构部搭建扫描云平台服务于内部云与内部安全建设

- **能力输出：**作为内部HIC云平台的安全产品。
- **自动化上线评估：**安全扫描嵌入开发测试环节
- **全网资产梳理：**摸底内网资产与特定应用
- **全网漏洞稽查：**持续风险监测与高危漏洞预警。

✓ IP总扫描量 230万IP，
✓ 日扫描IP量峰值可达百万级别
✓ HIC云客户上百个

3 某企业漏洞管理建设项目介绍

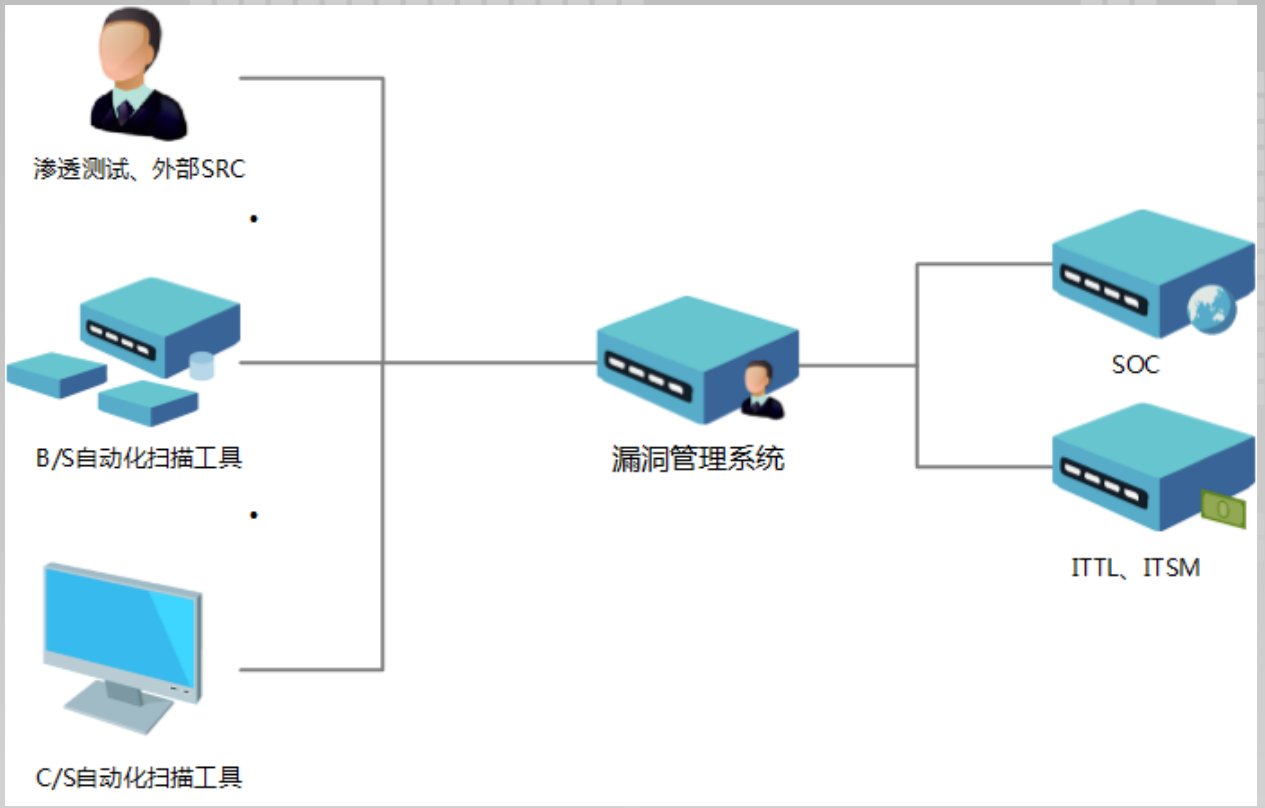
某企业开发业务迭代频繁而安全工作滞后，内部考虑将安全扫描融入至开发测试环节



魔方采用产品+服务方式实现协助其SDL落地

- 将安全扫描与开发测试流程相结合
- 定期对业务逻辑安排人工检测
- 结合漏洞数据提供针对性的改善方案

3 某证券漏洞管理项目



某证券安全组通过魔方的漏洞管理系统，实现以下场景的漏洞管理工作：

1. 通过自动采集和人工填入，整合漏洞结果，满足稽核部门的要求。
2. 结合系统自带的跟踪机制，落实到负责人。
3. 基于漏洞数据优化安全策略，并制定下一步的安全工作措施。

谢谢关注 • THANKS

OWASP
Open Web Application
Security Project