WIZEYE

# 破解企业攻防实战人才缺失的困境

**张兆心**

哈尔滨工业大学（威海）
网络与信息安全技术研究中心(NIST)

求真 奋进 务实 创新

# 行业的客观需求

WIZEYE

| 需求 | 困境 | 解决方案 |
| --- | --- | --- |
| • 可快速上手了解业务系统的人才<br>• 保障企业安全的人才 | • 供需不匹配 漏洞挖掘人员or攻防实战人才<br>• 培养代价非常大 | • 寻找具有漏洞挖掘能力的人<br>• 试图培养真正的需求点 |

**人才能力培养很重要**

**能力如何转为生产力更需要进行大量探索**

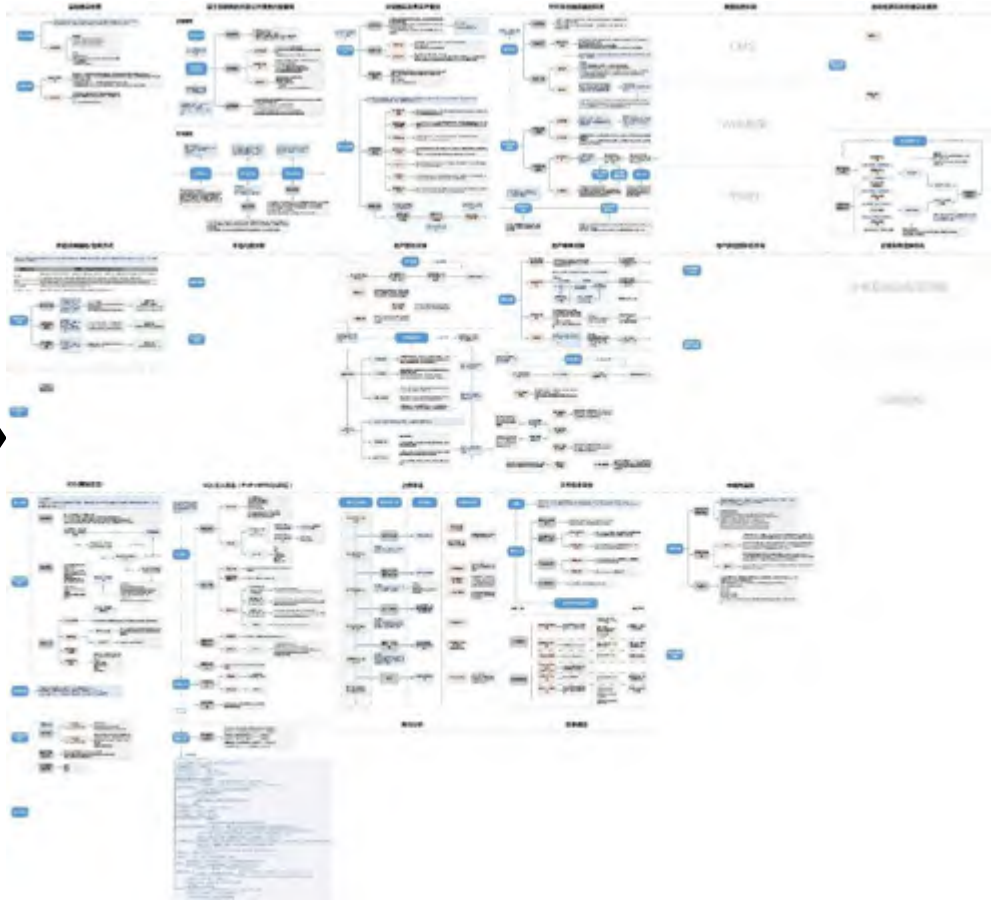
# 攻防实战型人才定位

WIZEYE

实战出发、攻防兼备

完整的知识体系

漏洞成因的深入理解



# 学生攻防技术培训实践

WIZEYE



**课程效果反馈**

- 兴趣极高
- 非常关注后续进展
- 钻研性强

**学生客观特点**

- 无业务概念，基础差
- 无体系支持
- 专注
- 可塑性强

# 针对问题做出的尝试

WIZEYE

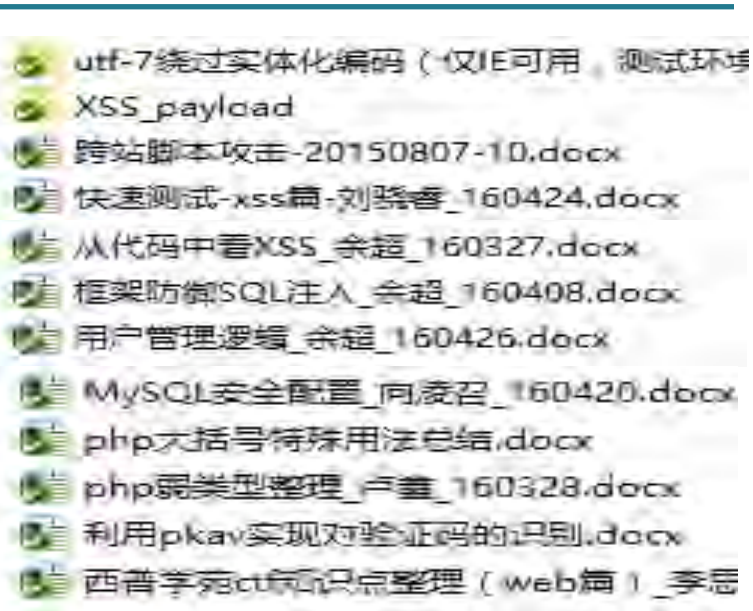
**培训方法：**
- 根据漏洞原理及防护方案建立攻防技术体系
- 建设实验平台以实现实践环境

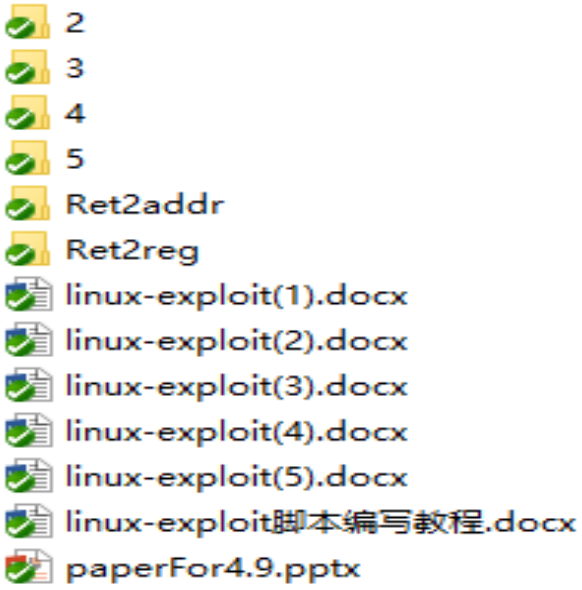
**培训方式：**
- 建立大一“直培”体系
- 寒暑假封闭集训

**培训环境：**
- 配套教材
- 具备实际经验的讲师

# 有效培训手段汇总

WIZEYE





## CVE-2016-1494 (python – rsa)漏洞详解

uncleheart 2016-04-12 共155865人围观，发现7个不明物体 系统安全 终端安全

原创作者：uncleheart

## 0×01 概述

CVE-2016-1494漏洞讲的是Python-rsa的签名伪造。在某些特定情况下，可以伪造python rsa库生成的签名信息。但是前提需要RSA的公钥指数e值很小，以下皆以e=3讨论。

# 培训后效果

WIZEYE

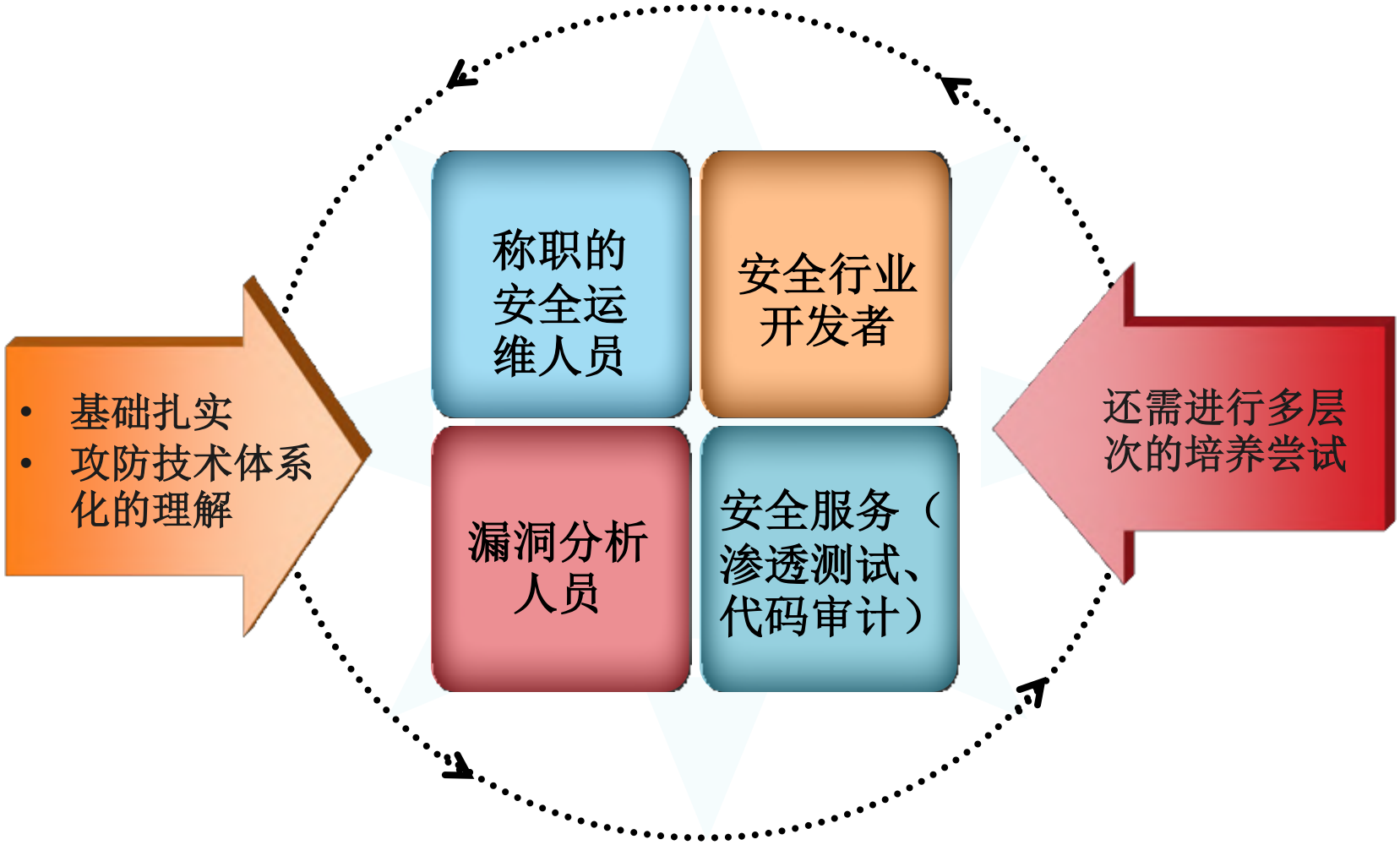
人员基本能力

- 可直接利用的攻防知识体系
- 漏洞的综合分析能力
- 代码审计能力

攻防实战经验

- Web漏洞挖掘
- 逆向技术
- 内网渗透
- 病毒分析
- 。 。 。

# 人才适用性总结


基础扎实
攻防技术体系化的理解
称职的安全运维人员
安全行业开发者
漏洞分析人员
安全服务（渗透测试、代码审计）
还需进行多层次的培养尝试


Thanks!