
# 数据安全分析在应用层攻防的应用浅谈

OWASP 中国

The Open Web Application Security Project

OWASP 中国
The Open Web Application Security Project

# • About Me

Alibaba（Taobao）Security Team

Qunar Security Team

Anquanbao

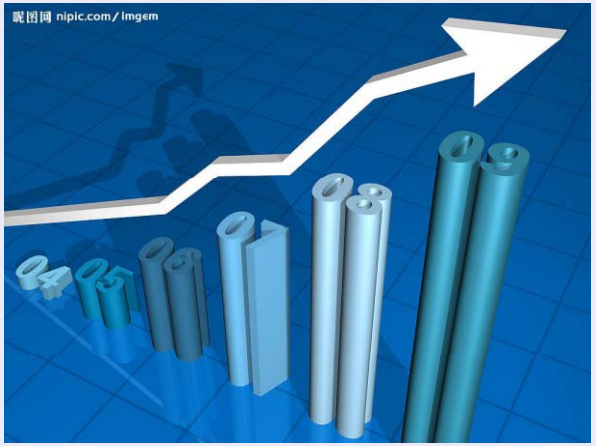
安全宝
Anquanbao.com

# 应用层攻击正在兴起

OWASP 中国
The Open Web Application Security Project

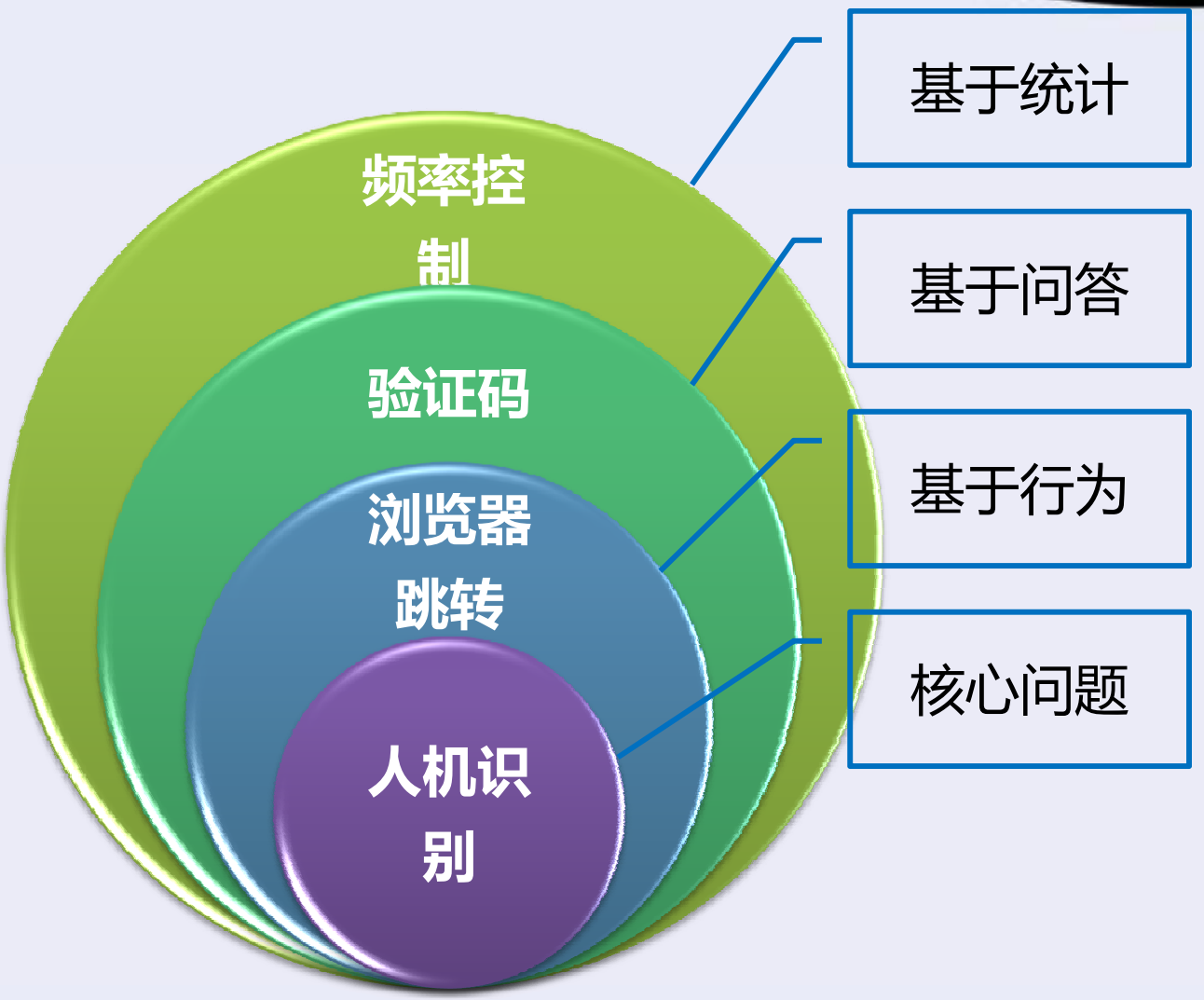
- 绿盟2012年上半年安全威胁报告中指出
  - SYN flood 攻击约占所有DDOS攻击的26.17%
  - Http GET DDOS攻击约占所有DDOS攻击的24.30%

难于防范的
http GET DDOS攻击
呈逐年上升趋势



# 传统做法&一些共识





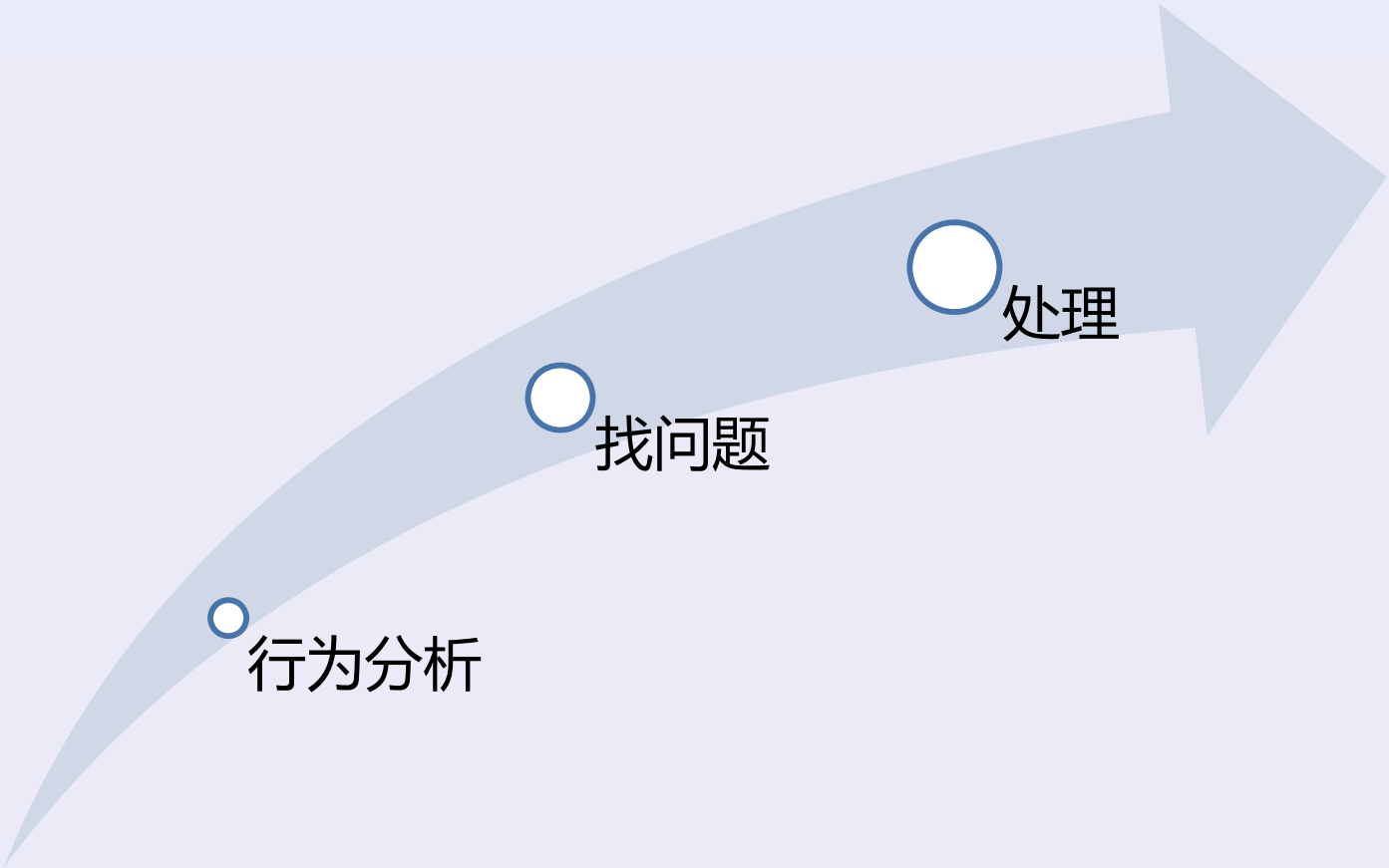
# 问题

OWASP 中国
The Open Web Application Security Project

- 阈值凭经验设定导致效果不理想。
  - 到底是1秒30次？还是1秒20次？这是个问题。

- 防御手段都被攻击者熟知。
  - 限制IP访问速率？多弄点IP。
  - 特定页面的保护？随机页面。

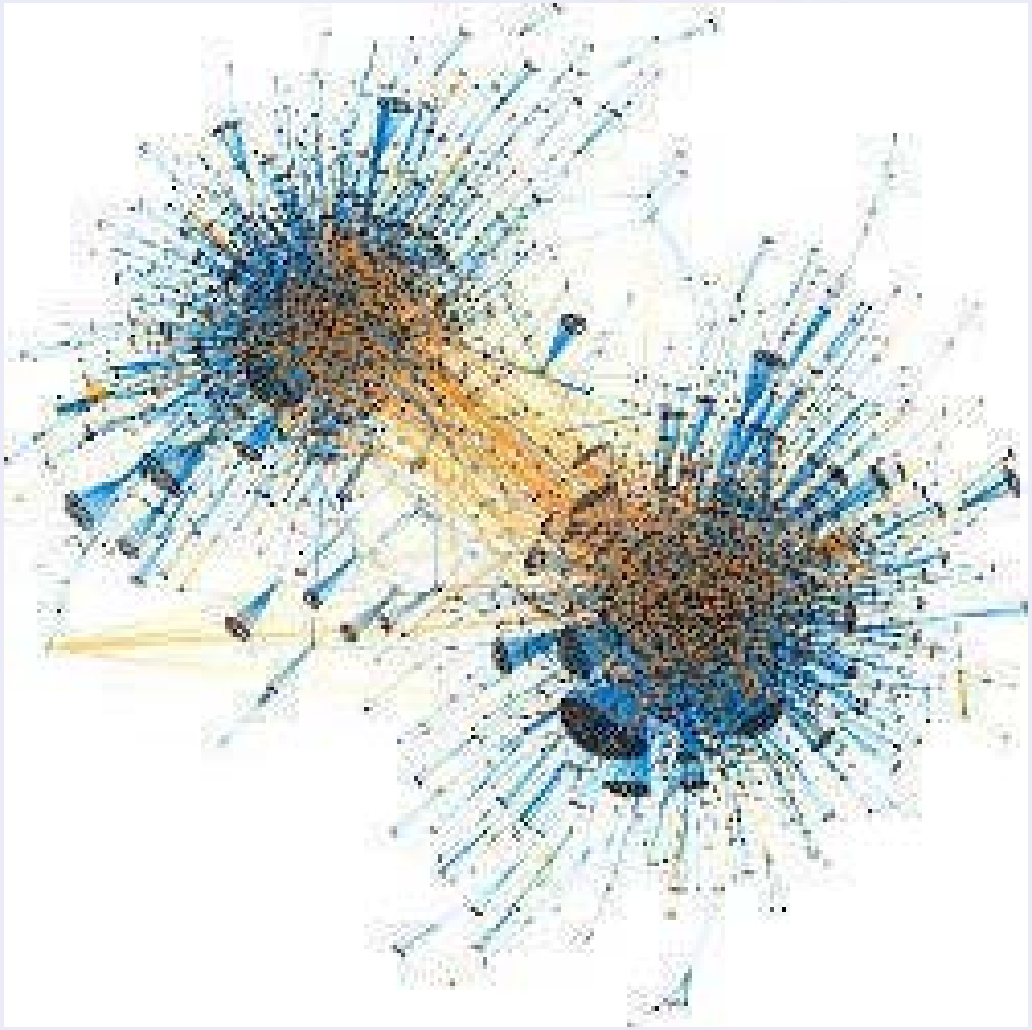
# 安全，行为分析

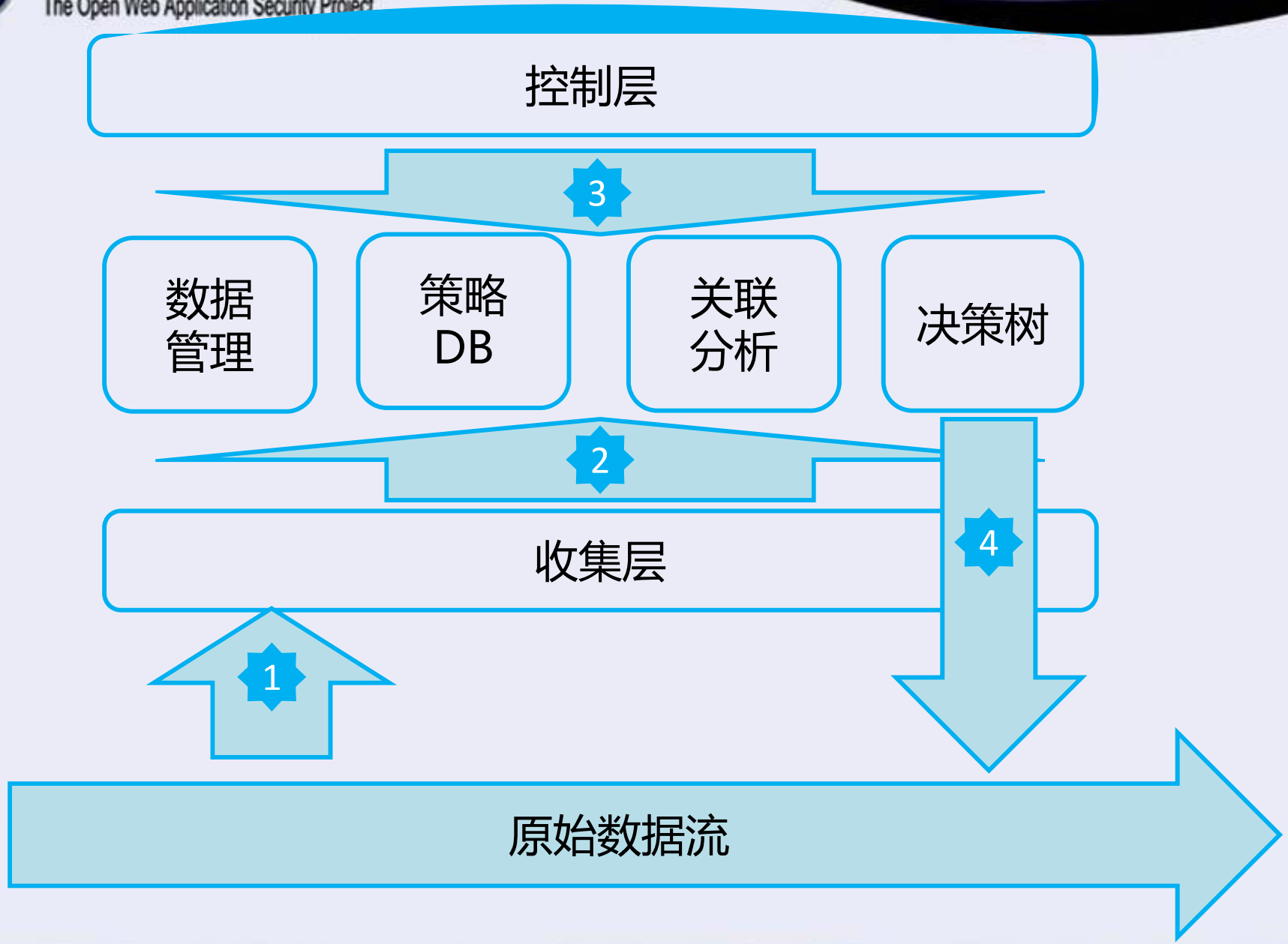


# 分析什么？怎么分析？

OWASP 中国
The Open Web Application Security Project

- 找异常的思想：
  - 统计
  - 关联
- 个体的异常：
  - 重复行为
  - 周期频率
  - 个体特征
- 全局的异常：
  - 变化趋势
- 抽象一般化模型




控制层
3
数据
管理
策略
DB
关联
分析
决策树
2
收集层
4
1
原始数据流

# Why?



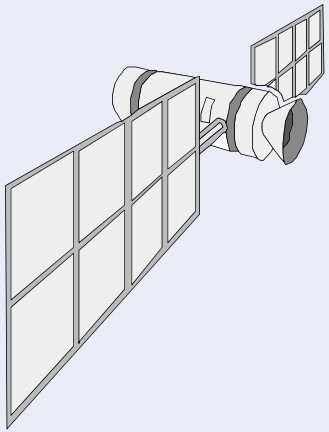
- 实时数据分析
  - 有限的数据
  - 简单的计算
  - 逻辑的耦合
  - 实时性高
- 离线数据分析
  - 实时性不高
  - 更复杂的计算
  - 更大的数据量
  - 逻辑的隔离

- 准实时数据分析
  - 折中的方案

# 感知



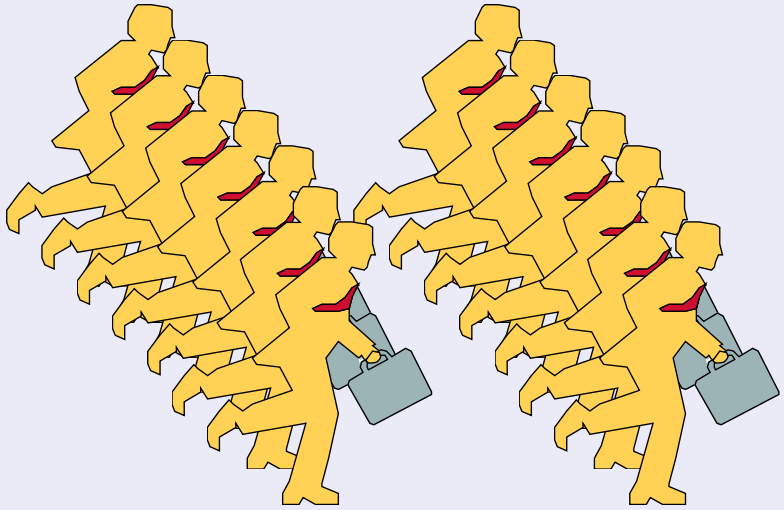
- 信息的采集
  - 流量，变化。
  - 负载，变化。
  - 异常，变化。



# 关联分析


独立的信息

- IP
- Cookie
- URL
- 访问时间
- 状态返回
- etc



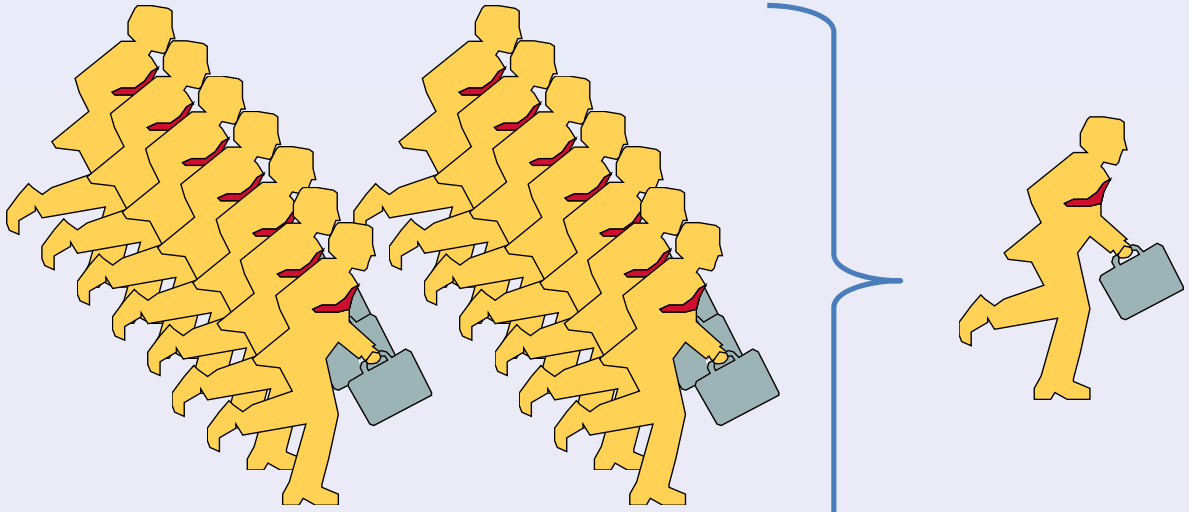
关联的信息

- 请求间隔
- 用户访问路径
- 停留时间
- etc

# 关联分析



- 提取一般访问模型



- 提取恶意特征模型

# 找不同

OWASP 中国
The Open Web Application Security Project


匹配相似程度

Question：

异常 = 疑似 = 攻击？

异常 = 疑似 ≠ 攻击!

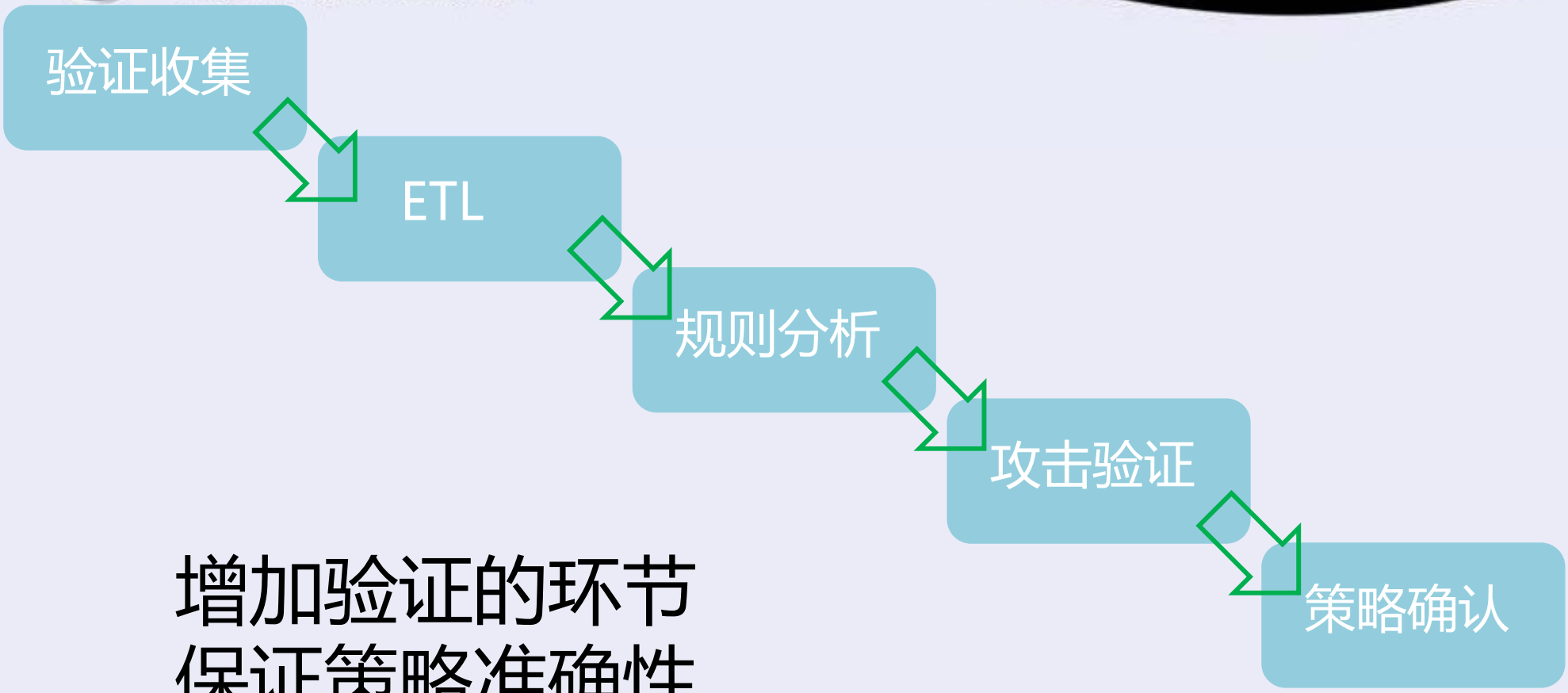
# 风险评估

OWASP 中国
The Open Web Application Security Project

- 可用性评估
  - 引起资源的持续恶化
- 恶意评估
  - 具备攻击性
  - 具备已确认的攻击特征

# 验证

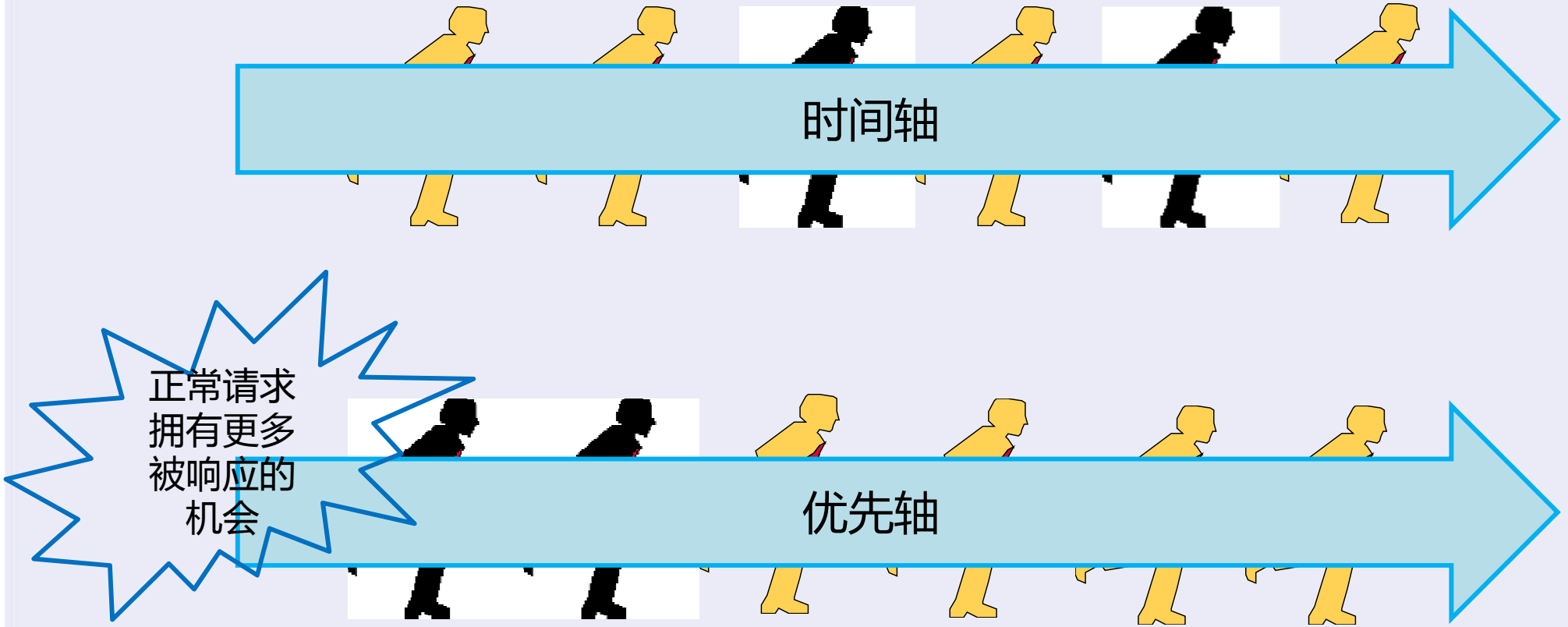
OWASP 中国
The Open Web Application Security Project




增加验证的环节
保证策略准确性

# 排列组合





OWASP 中国
The Open Web Application Security Project

# 做聪明的应用层安全防护体系

OWASP 中国
The Open Web Application Security Project

# Thanks!