基于大数据分析的专网异常检测

OWASP 中国

The Open Web Application Security Project

提纲

OWASP 中国
The Open Web Application Security Project

- 基于预警监控的防御思路探讨
- 内网安全需求探讨
- 大数据分析下的内网安全检测

WebRAY

信息安全管控背景

OWASP 中国
The Open Web Application Security Project

- 国家安全委员会
- 中央网络安全和信息化领导小组 习近平组长，李克强 刘云山副组长
- 国家网络与信息安全协调小组 李克强组长

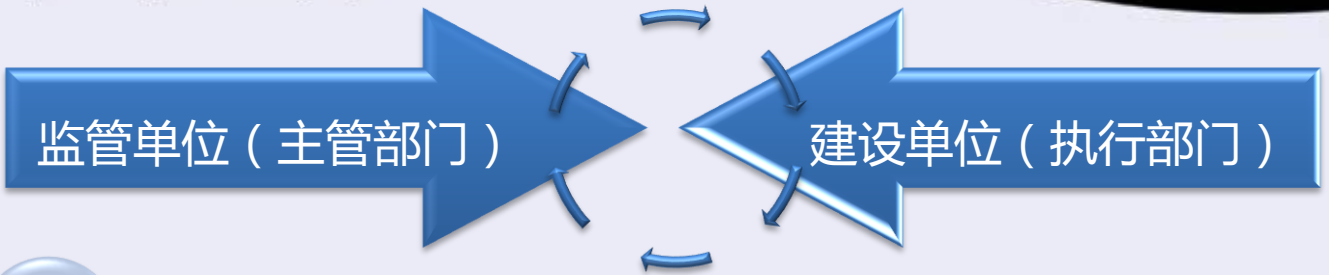
- 工信：网络与信息安全协调小组办公室；联合检查、风险评估等工作推动
- 公安：等保工作推动
- 国办、国安、保密、密码等监管部门

- 银监会：信息科技风险管理指引
- 证监会：证券期货业信息系统安全等级保护
- 电监会：
- 运营商：

- 省/市网络与信息安全协调小组
- 省/市网络与信息安全协调小组办公室
- 省/市公安、国安、保密、密码等主管部门

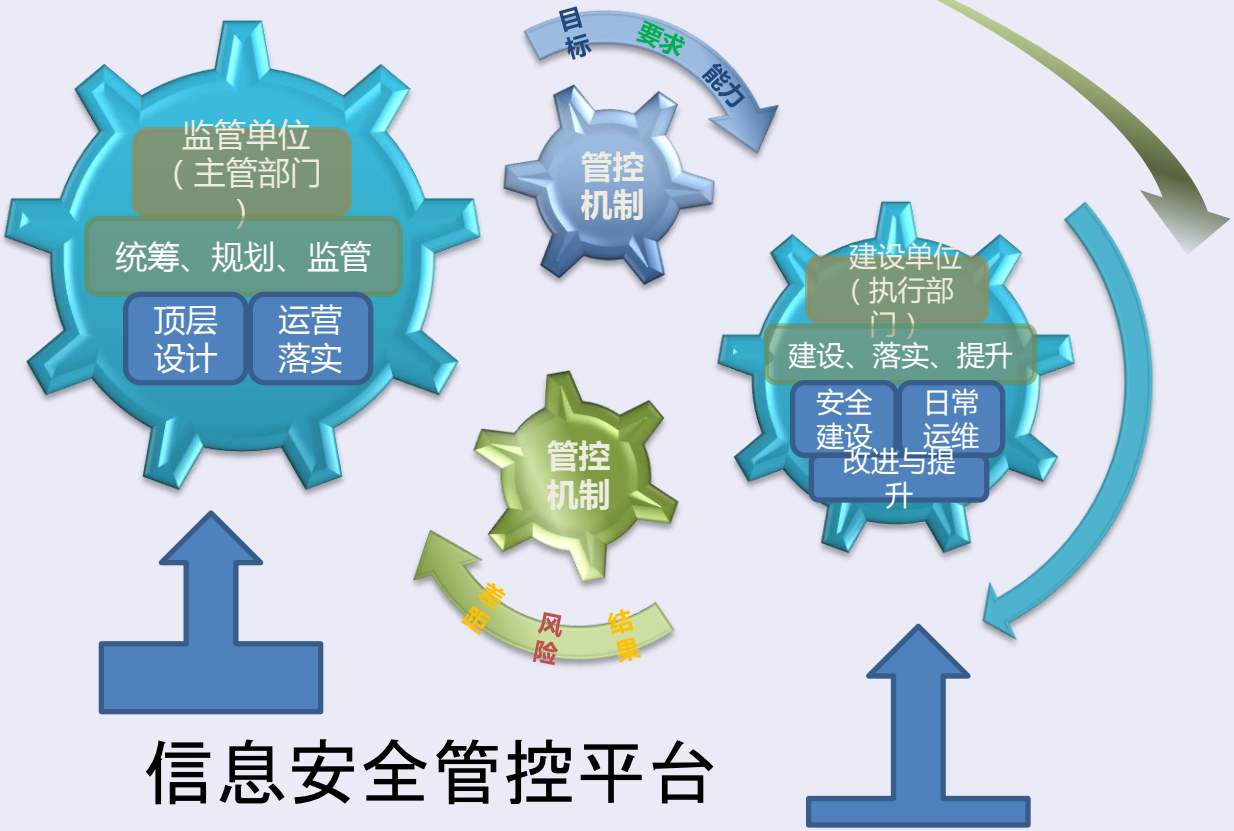
问题与挑战

OWASP 中国
The Open Web Application Security Project



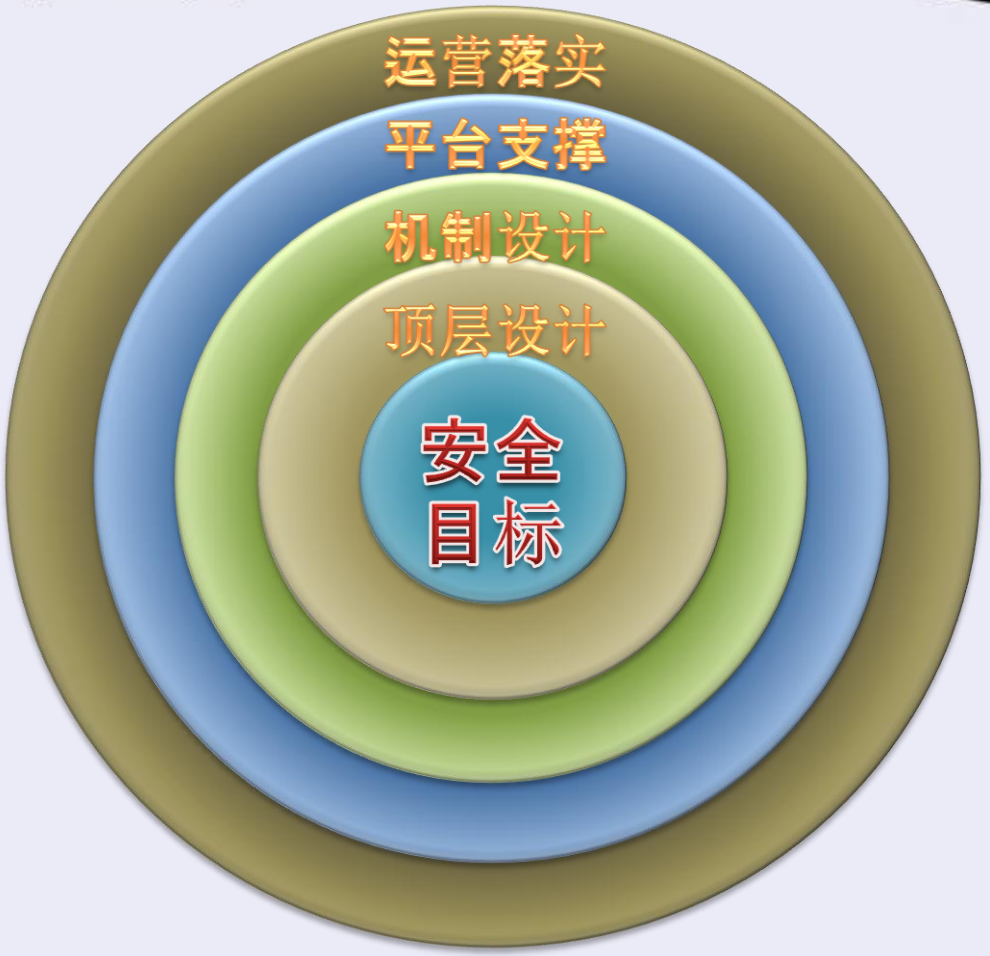
统筹协	责任不明确，协同效果不佳	多头管理，有些无所适从
工作协	协调方式单一，互动不充分	缺少指导和支持，工作效率低
资源共	资源不清且分散，难以充分共享	资源不够，工作推动慢
应急协	协调机制单一，效率不高	能力不足，工作做不到位
绩效评价	缺少客观数据支撑，权威性不够	缺少内在驱动力，领导重视不够

信息安全管控理念


监管单位
（主管部门）
统筹、规划、监管
顶层设计
运营落实
目标
要求
能力
管控机制
建设单位
（执行部门）
建设、落实、提升
安全建设
日常运维
改进与提升
管控机制
结果
风险
信息安全管控平台

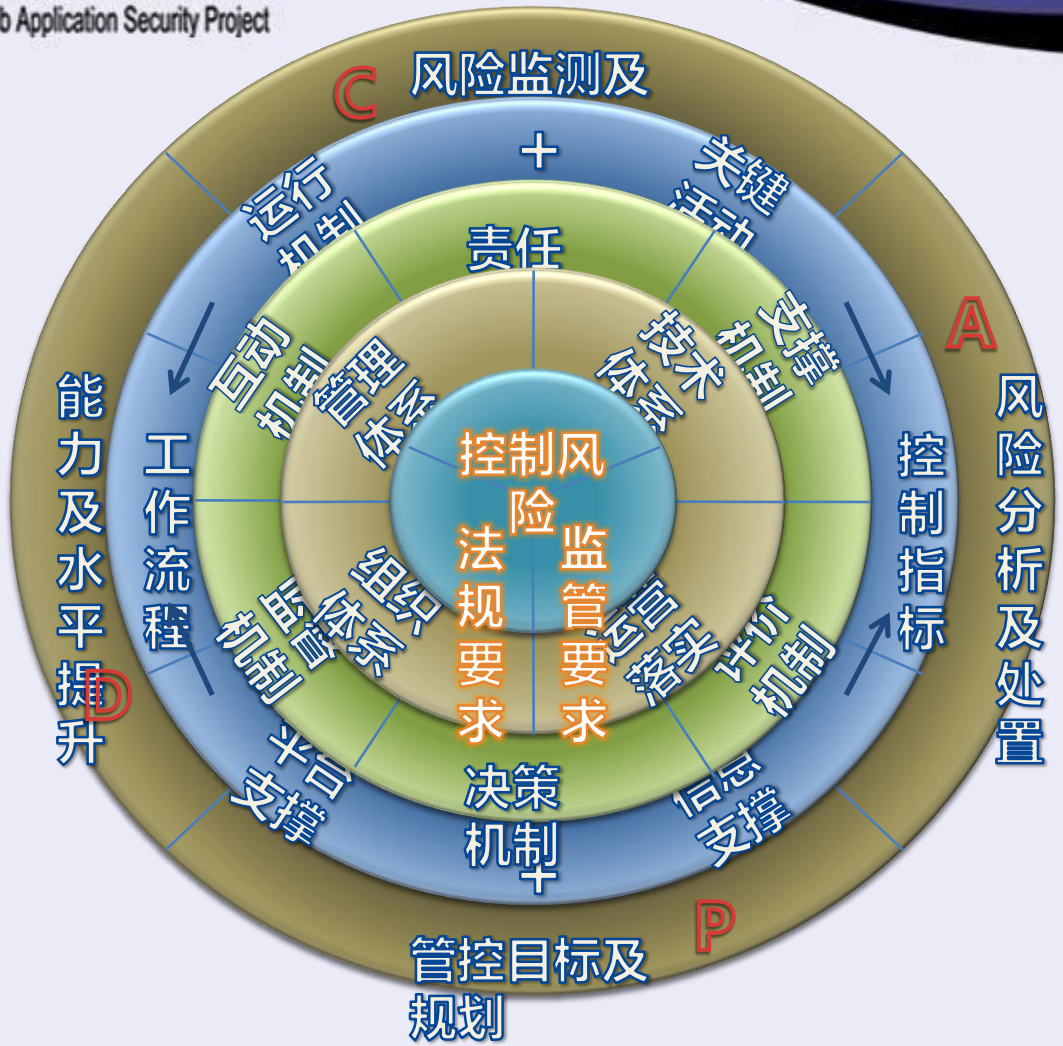
信息安全管控目标

OWASP 中国
The Open Web Application Security Project



信息安全管控目标

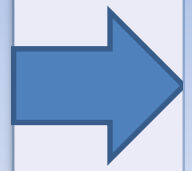
OWASP 中国
The Open Web Application Security Project



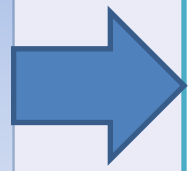
真正的内网安全需求？

OWASP 中国
The Open Web Application Security Project

- 互联网的安全攻击？
- 对终端安全的防范？
- 对病毒的防范？
- 对服务器的保护？
- 网络隔离的需求？
- 身份认证需求？
- 安全审计需求？
- ．．．．



- 真正的需求？



- 看清网络

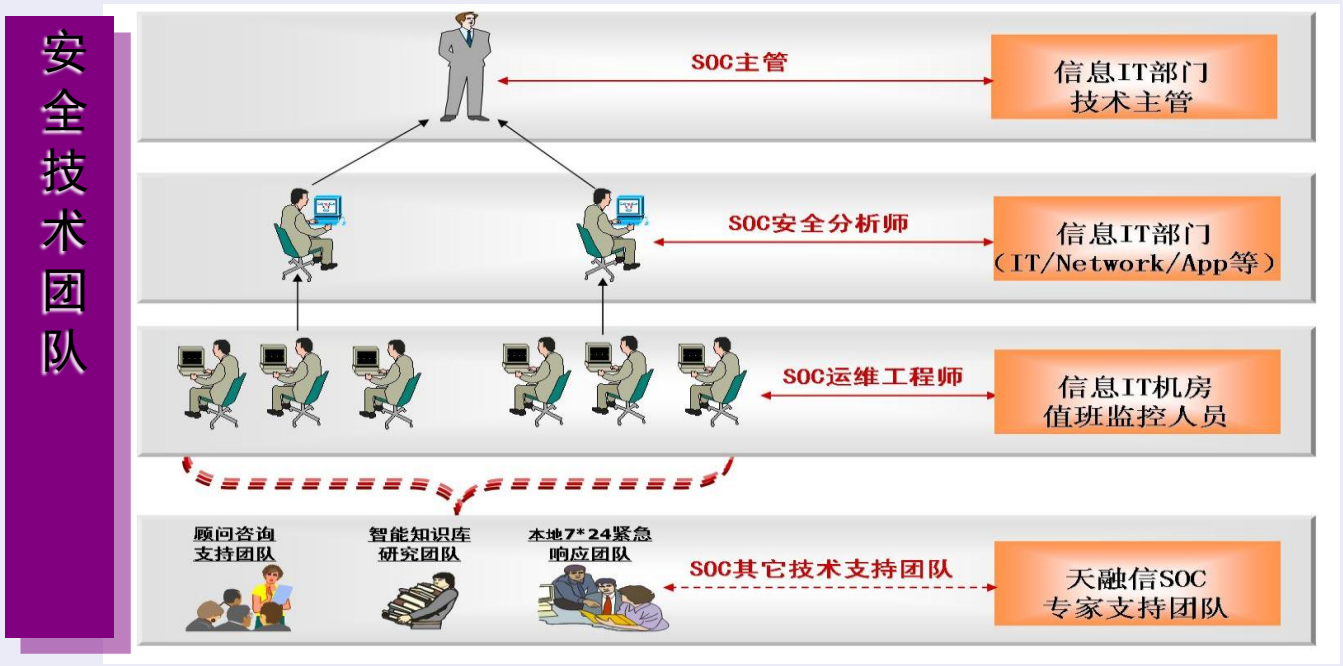
传统解决思路

OWASP 中国
The Open Web Application Security Project

- SOC
- 监控中心
- 服务器日志扩展
- …

传统解决思路

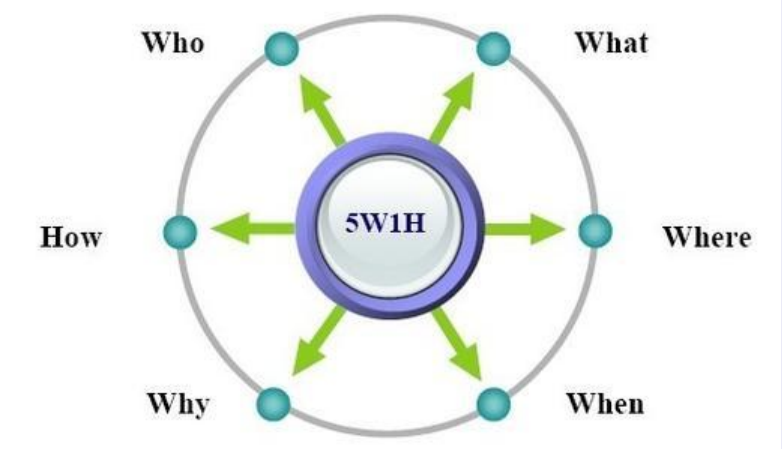
OWASP 中国
The Open Web Application Security Project



核心问题-责任认定的方法论

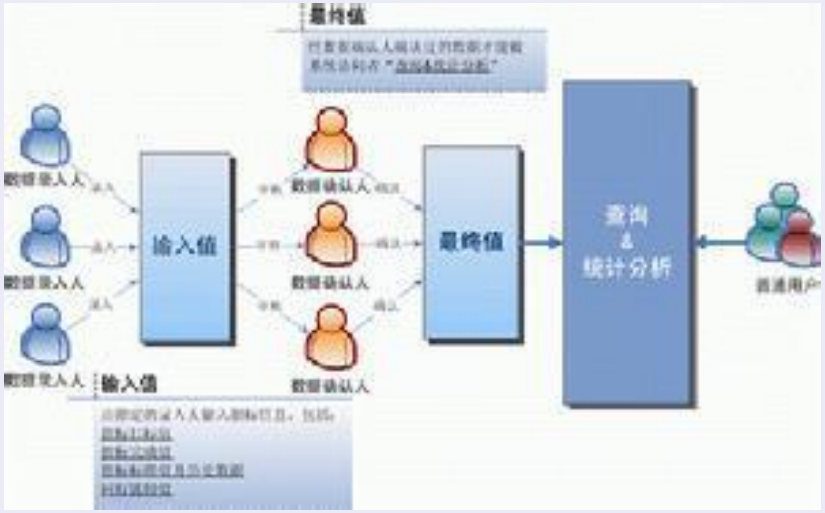
OWASP 中国
The Open Web Application Security Project

- 责任认定系统清晰定义以下几个因素
  - Who
  - When
  - Where
  - What
  - Why
  - How

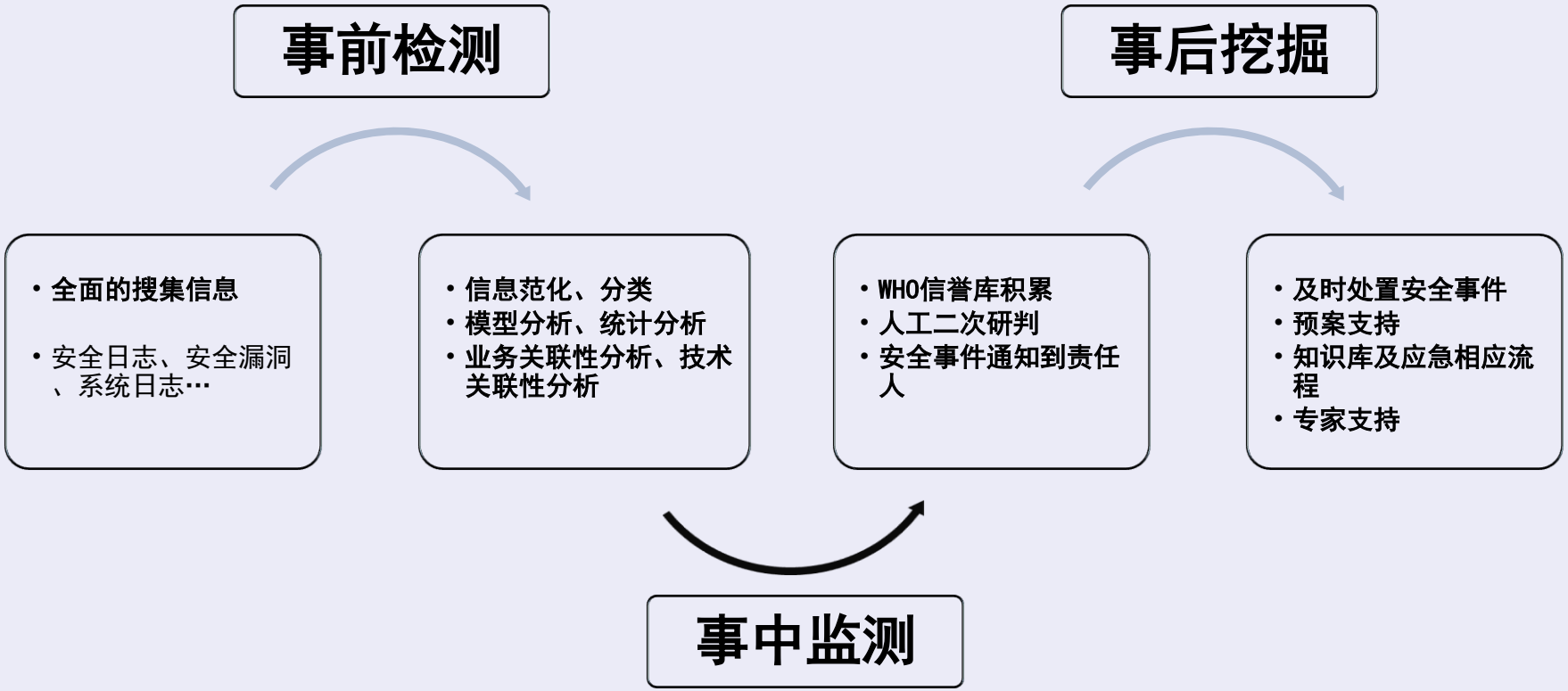


采用5W1H分析方法为主线进行责任认定，采用迭代等方法

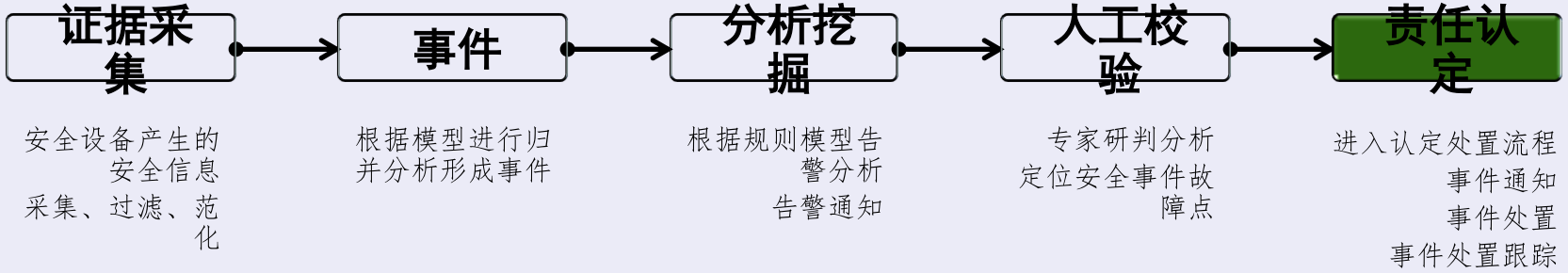
- 解决证据的准确性问题
- 解决证据的完整性问题
- 解决证据存储的问题
  - 证据合并
  - 证据改变
  - 证据简化
  - 证据取消



责任稳定-业务层面分析


事前检测
事后挖掘
• 全面的搜集信息
• 安全日志、安全漏洞、系统日志…
• 信息范化、分类
• 模型分析、统计分析
• 业务关联性分析、技术关联性分析
• WHO信誉库积累
• 人工二次研判
• 安全事件通知到责任人
• 及时处置安全事件
• 预案支持
• 知识库及应急相应流程
• 专家支持
事中监测

事件处理流程


证据采集
事件
分析挖掘
人工校验
责任认定
安全设备产生的安全信息采集、过滤、范化
根据模型进行归并分析形成事件
根据规则模型告警分析告警通知
专家研判分析定位安全事件故障点
进入认定处置流程
事件通知
事件处置
事件处置跟踪

系统结构图


展示中心
实时监控
事件态势
应急处置
信誉库监控
报表管理
数据中心
业务关联
告警模型
预案管理
工单管理
技术关联
统计分析
资产管理
任务调度
数据库
知识库
事件处置
专家研判
采集中心
降噪处理
范化 / 归并
数据识别采集
设备安全信息
日志采集
日志分析
服务器信息
私有协议

处理流程

1 采集

安全事件
性能参数
日志

2 处理

日志范化
分类、定级
日志存储

3 分析

告警模型分析
规则关联
业务关联性分析
技术关联性分析

4 计算

型分析
规则关联
业务关联性分析
技术关联性分析
事件预警

5 展示

实时告警
工单流程展示

5 处置

人工研判分析
安全事件通报
事件处置跟踪

5 报告

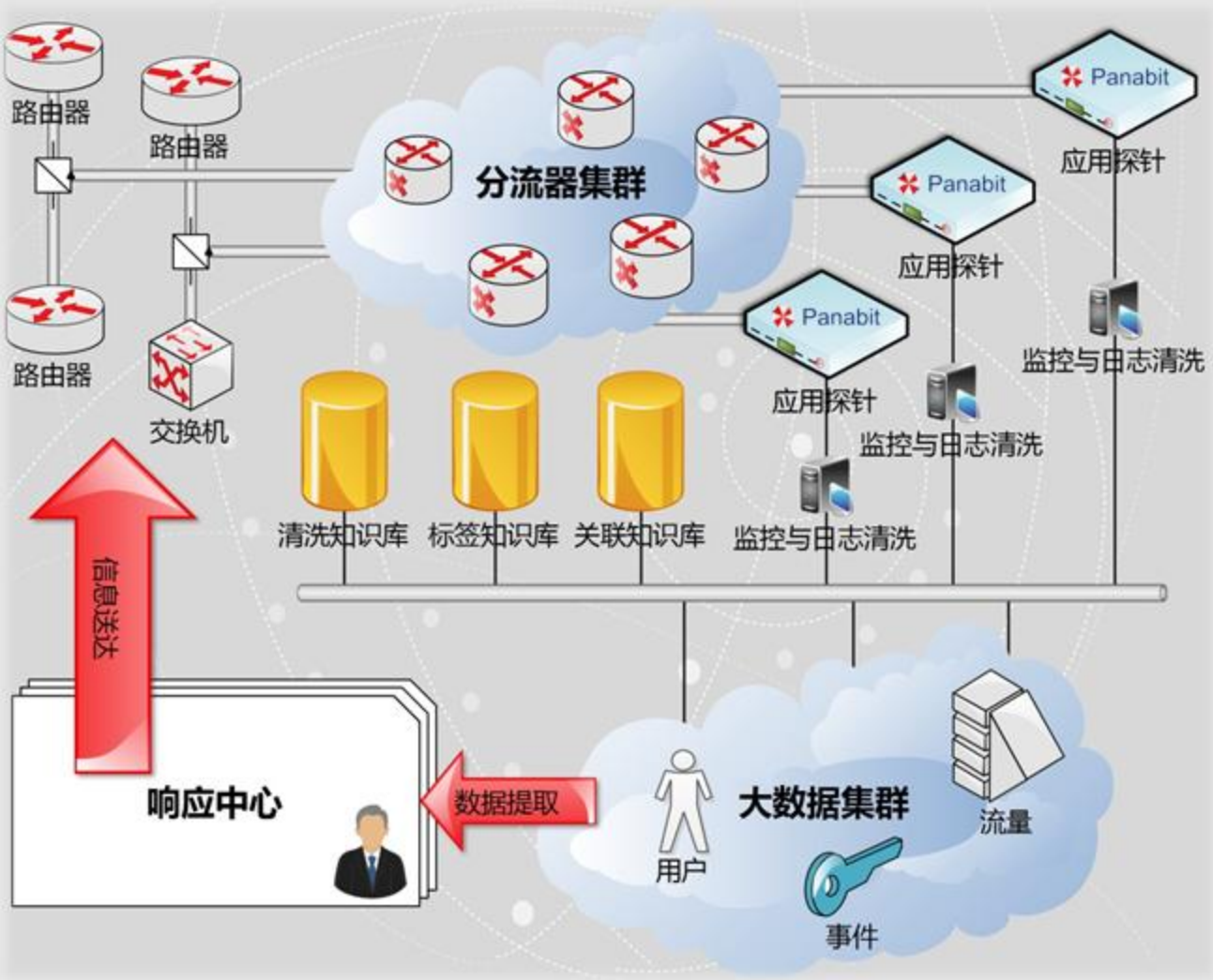
安全事件报告
安全状态报告
周报、月报等

证据采集-监控、识别获取证据

OWASP 中国
The Open Web Application Security Project

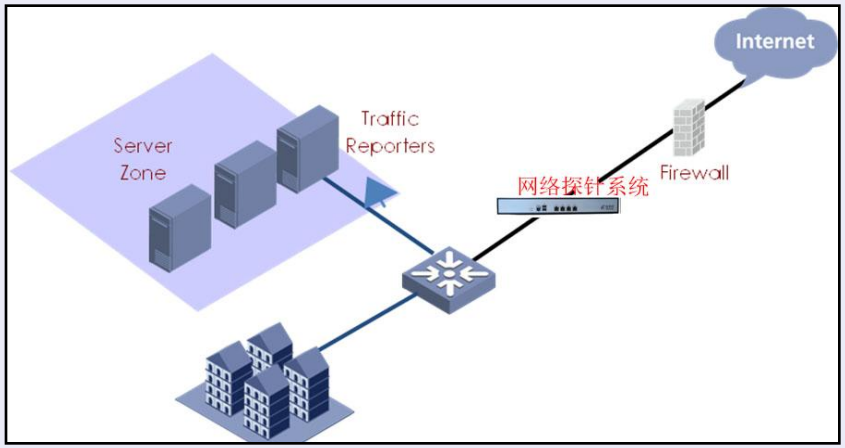
说明:

1) 核心节点交换机上部署探针；
2) 探针识别网络流量，通过管控中心配置策略，从指定流量中获取信息，一方面杜绝流量异常、一方面感知未知流量，同时替代提取需要的信息；
3) 将网络设备、网络安全设备相关信息收集，进行数据挖掘和分析；
4) 将服务器、客户端数据收集、汇总，进行数据挖掘和分析；

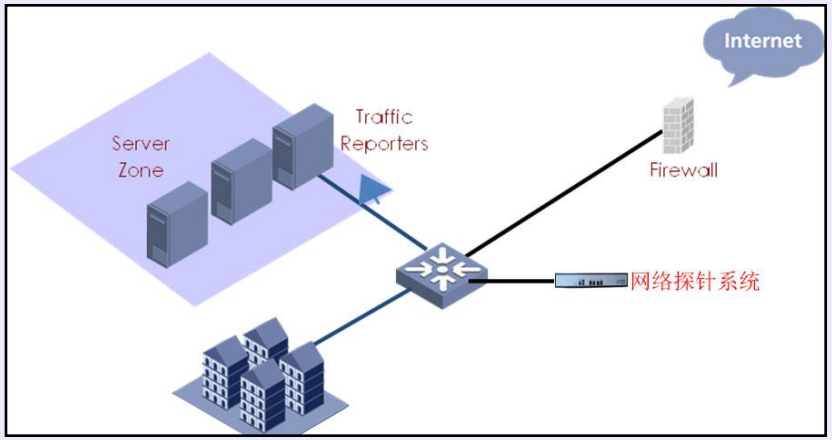


证据采集–部署模式

OWASP 中国
The Open Web Application Security Project

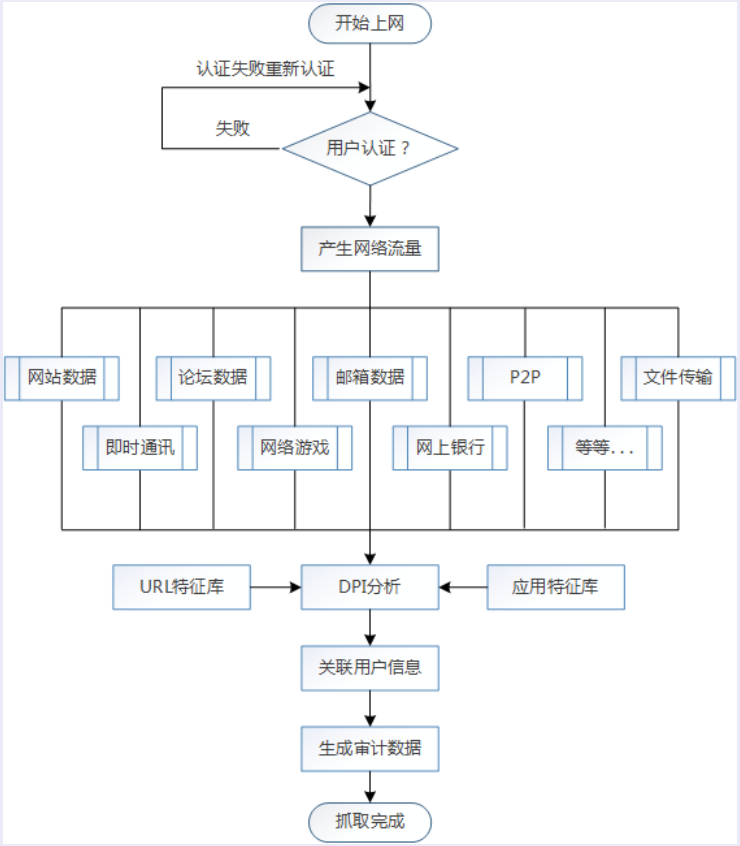


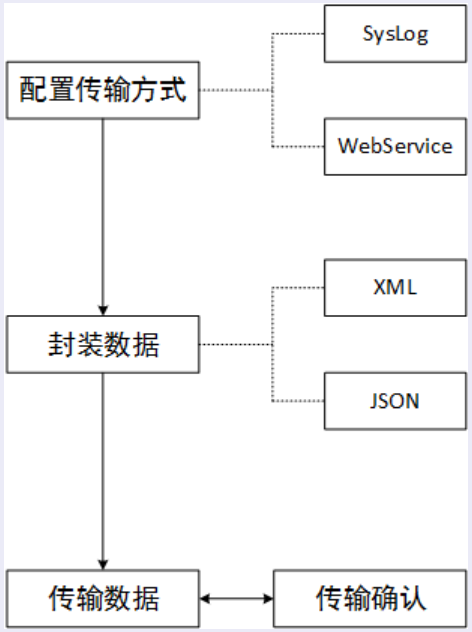
串联监听



旁路监听

证据采集–流程接口


开始上网
认证失败重新认证
失败
用户认证？
产生网络流量
网站数据
论坛数据
邮箱数据
P2P
文件传输
即时通讯
网络游戏
网上银行
等等...
URL特征库
DPI分析
应用特征库
关联用户信息
生成审计数据
抓取完成


配置传输方式
SysLog
WebService
封装数据
XML
JSON
传输数据
传输确认

阶段1: 证据采集-主动扫描、探测网络威胁

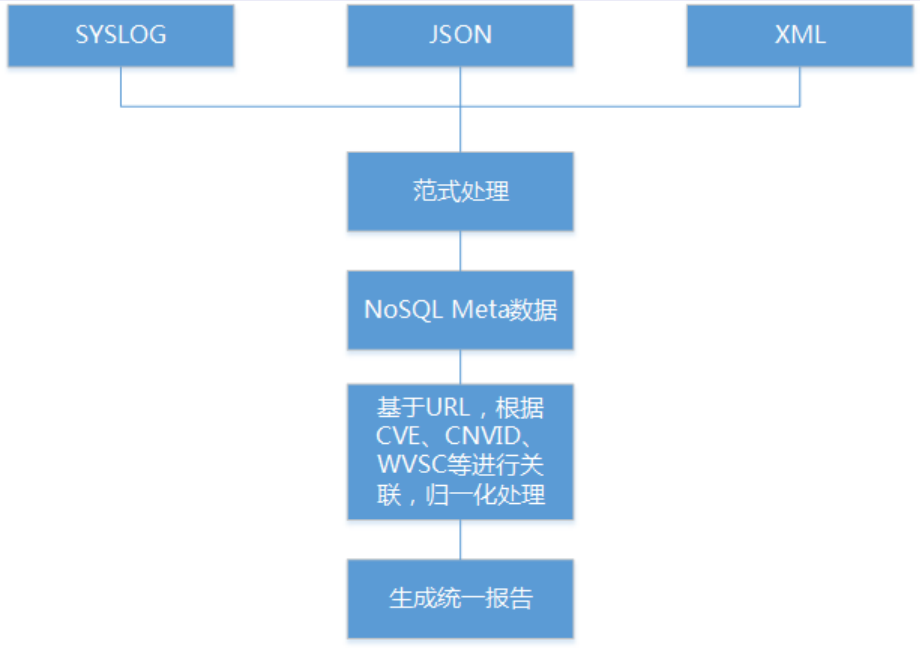
1）集成漏洞扫描、Web扫描、数据库扫描 、无线扫描进行漏洞、威胁分析

2）主动探测目的是为了更好的对可疑目标进行识别和风险积累

阶段2: 数据关联、分析、归一化

1）数据关联分析、归并；

2）形成Key-Value形态的范式，NOSQL存储，便于检索

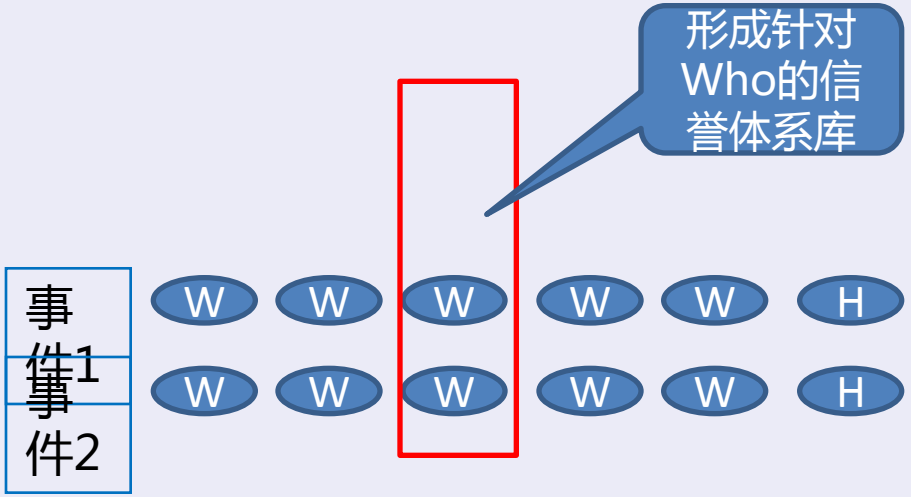


阶段3: 分析

1）形成完整的回溯流程，能完整的对单个事件进行事件回溯，确定单独事件的5W1H元素；

2）形成混合模式的5W1H链条；

3）形成Who链条的信誉体系库；



OWASP 中国
The Open Web Application Security Project

阶段4: 计算与专家库介入

1） 通过数据挖掘与阶段3分析，形成完整事件过程；

2）专家介入，校对事件追溯过程；

3）通过内置的事件分析模版，进行责任匹配；匹配失败进行专家知识库积累；

4）再次训练专家库；

阶段5: 责任认定

1）根据学习结果，形成初步认定结果；

2）展示相关问题及其证据链；

3）更新WHO信誉库；

OWASP 中国

The Open Web Application Security Project

欢迎指正，谢谢！