基于大数据的WEB攻击溯源

下一代安全防御体系

OWASP 中国

The Open Web Application Security Project

About Me

OWASP 中国
The Open Web Application Security Project

- ID:sm0nk
- 猎户实验室安全研究员
- 特长：WEB攻防、攻击建模
- 爱好：金庸武侠、关联分析

- *http://weibo.com/shellr00t*

TASS®
江南天安

目录结构

OWASP 中国
The Open Web Application Security Project

- Web Intrusion Tracking System WEB入侵追踪系统（以大数据为基础，联动为主线，实现攻击溯源的下一代智能安全防御系统）
  - 大环境（棱镜、第五空间、哨兵）
  - WEB攻击定位：WEB攻击切入点、APT敲门砖
  - 面临的挑战与机遇

传统安全防御体系

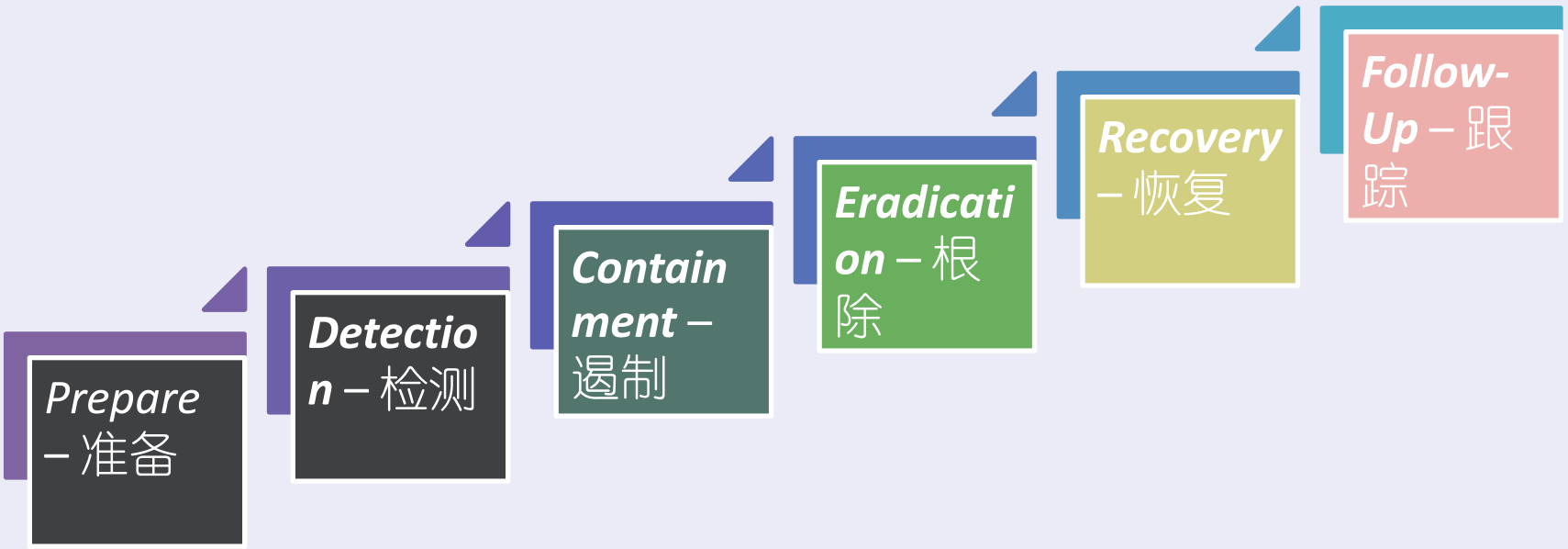
OWASP 中国
The Open Web Application Security Project

如果发生安全事件怎么办？

业务安全漏洞能否检测？

应急响应模型-密切关联

OWASP 中国
The Open Web Application Security Project



目录结构

OWASP 中国
The Open Web Application Security Project

大数据

OWASP 中国
The Open Web Application Security Project

1. 什么是大数据？ 2、大数据到底有多大？ 3、大数据时代怎么理解？

大数据

大数据 特点:

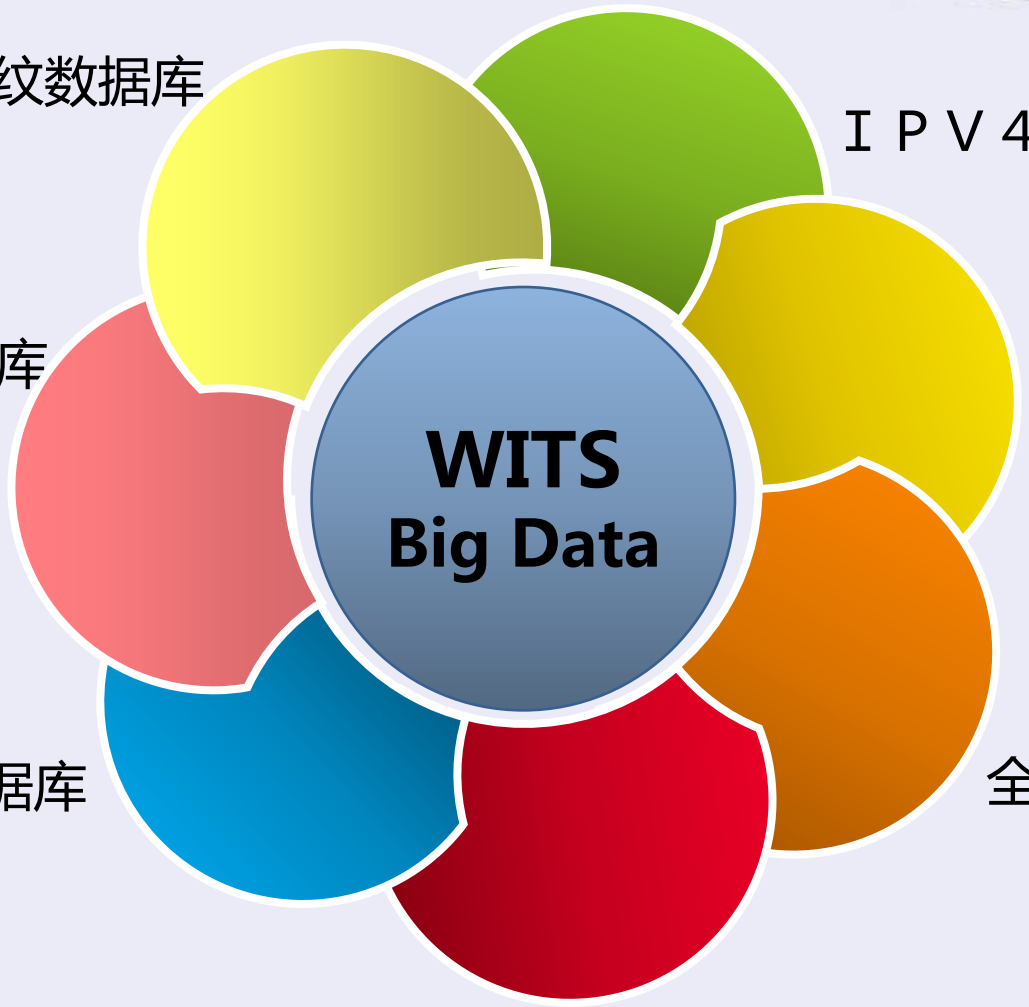
数据量大、数据种类多、 要求实时性强、数据所蕴藏的价值大。在各行各业均存在大数据，但是众多的信息和咨询是纷繁复杂的，我们需要搜索、处理、分析、归纳、总结其深层次的规律。

IBM出版了一本书叫做《无所不包的数据》在对大数据进行描述时，常见的GB或者TB的数据存储单位已经不再使用，而是以PB（1024TB）、EB（1024PB）甚至ZB（1024EB）。

由于大数据对所有网络用户的数据进行汇集存储，在一定程度上，为用户的个人数据的隐私保护埋下了安全隐患。

大数据之溯源应用

OWASP 中国
The Open Web Application Security Project



黑客工具指纹数据库

ＩＰＶ４信息知识数据库

黑客ＩＰ日志数据库

ＩＤＣ信息数据库

黑客信息数据库

全球域名信息数据库

黑客指纹数据库

大数据处理过程

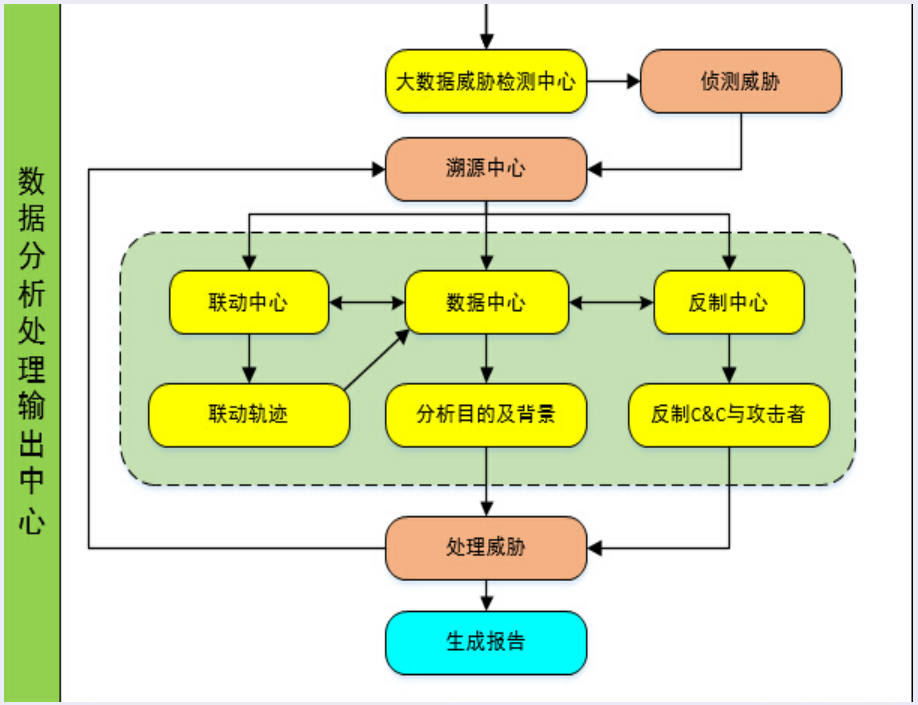
OWASP 中国
The Open Web Application Security Project

BIG DATA

利用大数据对确切的攻击行为进行分析

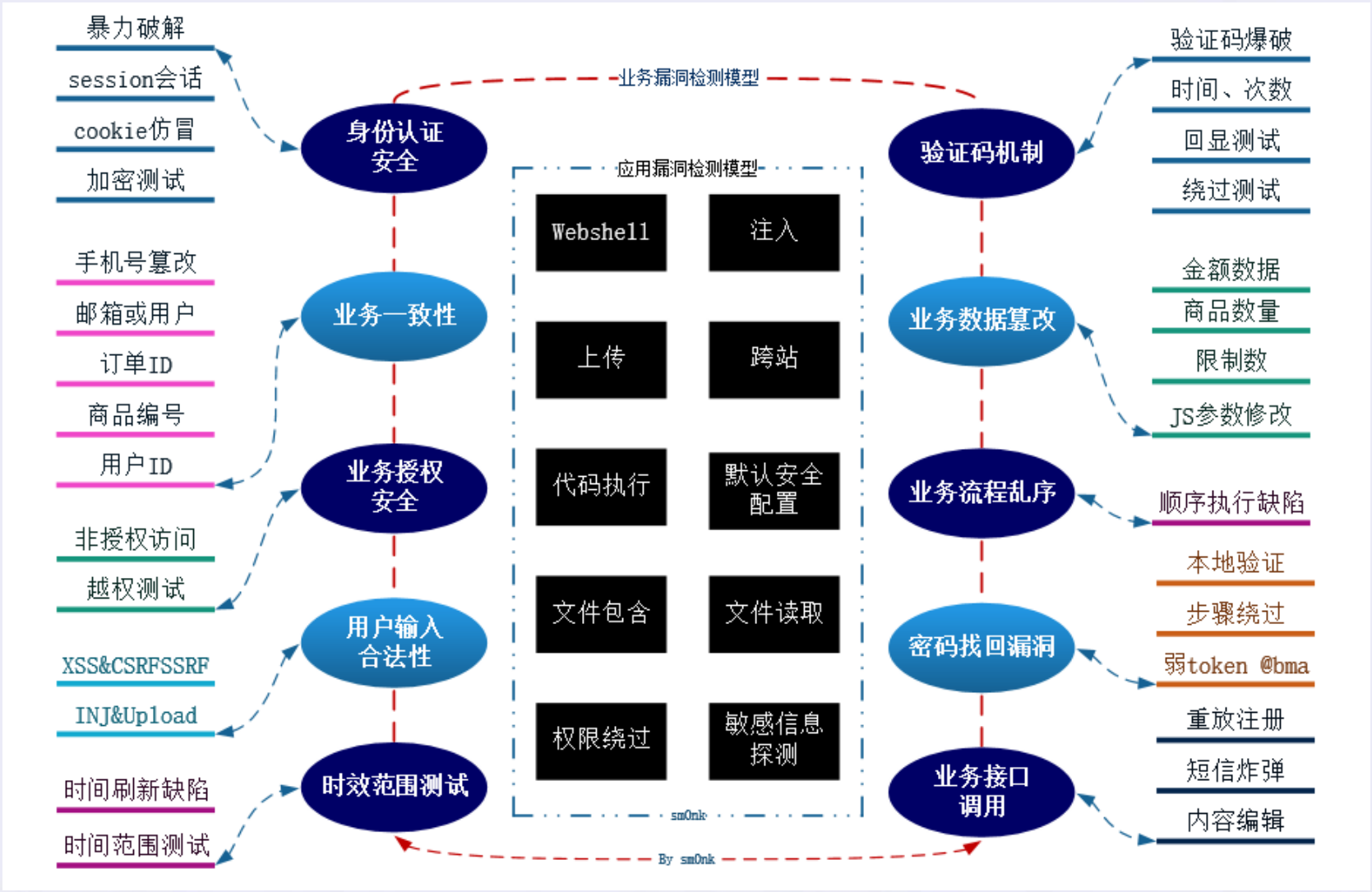
- ✓分析攻击者的来源
- ✓攻击路线
- ✓身份背景
- ✓目的
- ✓攻击者是谁
- ✓从哪来
- ✓来干什么
- ✓拿到了什么？

入侵事件的处理模型



攻击检测模型

OWASP 中国
The Open Web Application Security Project



目录结构

OWASP 中国
The Open Web Application Security Project

溯源威胁模型

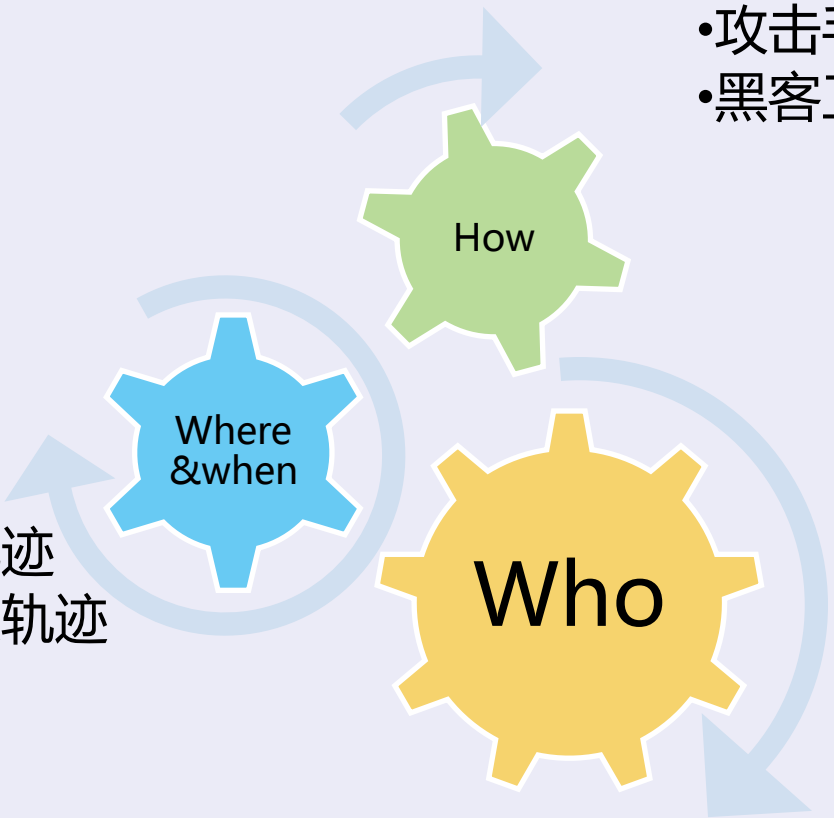
OWASP 中国
The Open Web Application Security Project

- 杀毒软件原理？
- 威胁模型
  - 标准？应用 top10、业务逻辑top10
  - 需要哪些技术？
    - 漏洞原理及触发规则
    - 攻击样本
    - 对未知方法及木马的“主动学习”模式（蜜罐）
    - 攻防技术及研究人员的储备
  - 结果导向：正则匹配、双向数据包比对

溯源取证扮演的角色

OWASP 中国
The Open Web Application Security Project

•攻击手段分析取证
•黑客工具分析取证



•本次安全事件轨迹
•绘制攻击者历史轨迹

•攻击者身份、个人信息、
•攻击者网络指纹

溯源取证解决的问题

OWASP 中国
The Open Web Application Security Project

分析检测过程

OWASP 中国
The Open Web Application Security Project

双向检测

请求包、返回包
双因子检测模式

动态建模

建立策略，对比正常的访问行为基线；如明显偏离正常行为模式则可产生告警

大数据支撑

1.海量基础数据支撑
2.海量攻击数据
3.互联网资安分析
4.机器学习

事件还原

OWASP 中国
The Open Web Application Security Project

- 对整个事件的串联分析及展现

事件追溯

OWASP 中国
The Open Web Application Security Project

- 对特征、手法、行为、时间段、目的进行智能分析

攻击者IP：	218.30.1[redacted]
攻击时间：	2015-05-16 01:44:05 到 2015-05-16 02:17:58
攻击者人数：	2人
国家、时区：	中国
攻击者浏览器：	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; .NET CLR 1.1.4322)
黑客IP来源：	中国

356 68.36.236.[redacted] 61.183.[redacted] 高危文件 未收录 成功 98次 高危 2015-04-08 16:00 北京时间下午 日志：未知 探针：未知 云端：已收录 否 攻击溯源

基本信息

IP地址：	68.36.[redacted]
IP所属组织：	CMCS - Comcast Cable Communications, Inc.,US
经纬度：	-74.1001,40.7923
IP来源：	United States,New Jersey
HOSTNAME：	c-68-36-236-16.hsd1.mi.comcast.net
PREFIX：	68.36.0.0/15
ASN：	AS33668
REGION：	New Jersey

通过IP信息可以初步判断该IP来自虚拟空间提供商，非正常用户访问

处理引擎

攻击分析引擎：	发生了98次攻击行为
态势感知引擎：	可疑
云端恶意IP分析引擎：	否
规则分析引擎：	PHPINFO
攻击者数量分析引擎：	2
APT分析引擎：	是
域名分析引擎：	

通过攻击分析引擎判断检测到了5次攻击行为。
态势感知引擎判断为可疑，其依据是云端大数据模型。
该IP被识别为恶意IP，证明之前被有过攻击行为。
该攻击手法被识别为“PHPINFO”方式攻击。
攻击者数量被判定为2人。
被识别为APT攻击，其依据主要是此IP之前有过APT攻击行为，而现在又进行了同样手法的攻击。

云端信息

端口：	80,1723
反向域名：	未检查到域名
注册国家：	未收录
IP所属国家：	美国
服务器信息：	centos 6.5
虚拟空间判断：	是

通过云端的历史记录，该IP曾经开放了80,1723端口也可以断定为跳板机器，非正常用户访问

沙箱信息

脚本沙箱：	发现后门
程序沙箱：	未发现可执行文件

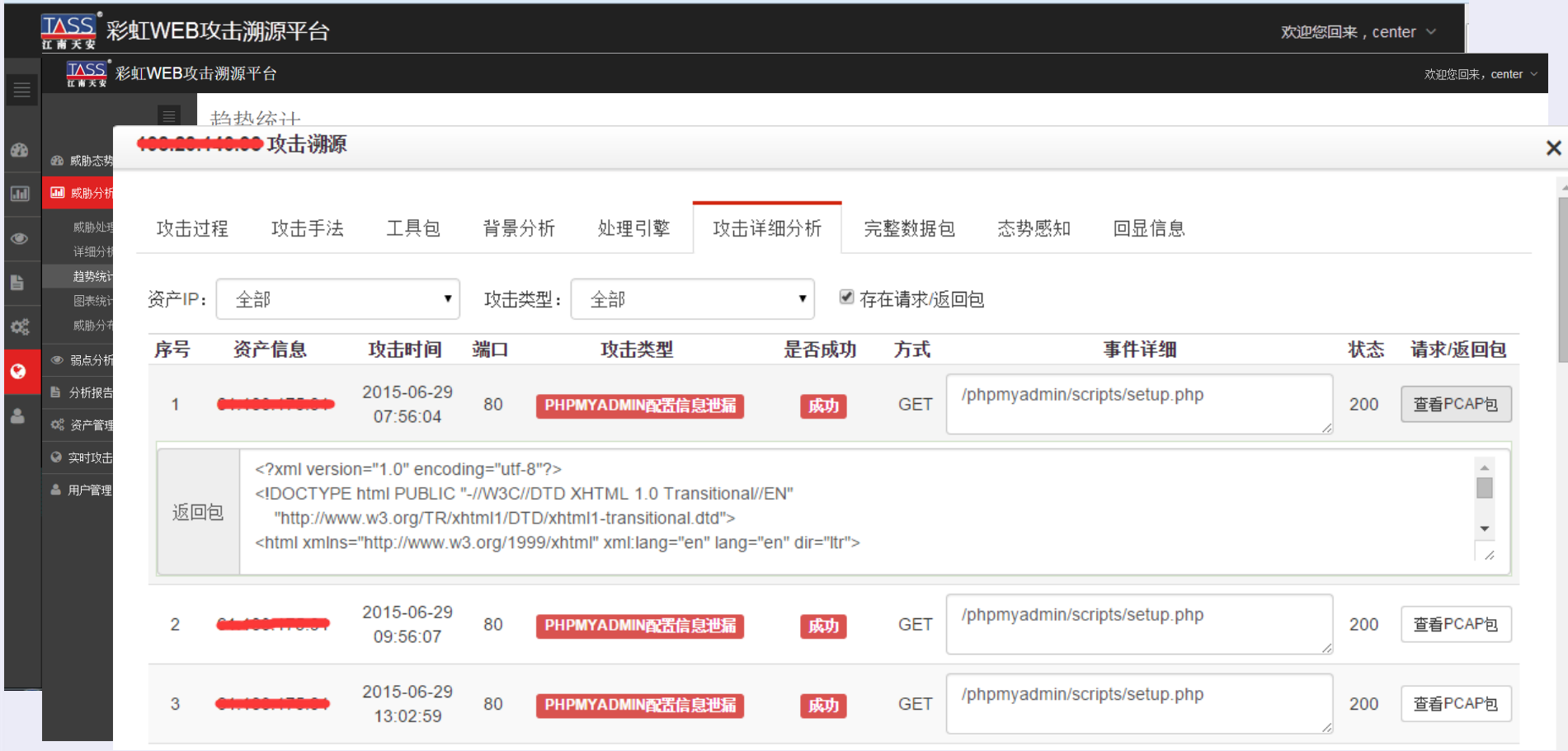
通过脚本沙箱，识别出来有后门程序

目录结构

OWASP 中国
The Open Web Application Security Project

溯源DEMO

OWASP 中国
The Open Web Application Security Project



溯源案例

OWASP 中国
The Open Web Application Security Project

CE-736	119.97.193.[redacted]	www.[redacted].gov.cn	后门分析引擎 目录扫描引擎	中国	
CE-738	202.103.25.[redacted]	www.[redacted].gov.cn	后门分析引擎	中国	
CE-741	101.226.66.[redacted]	www.[redacted].gov.cn	后门分析引擎	中国	
CE-742	101.226.66.[redacted]				

[redacted] 攻击溯源

攻击过程 | 攻击手法 | 工具包 | 背景分析 | 处理引擎 | 态势感知 | 攻击详细分析 | 完整数据包

2015

发现来自 美国 攻击者，USERAGENT是：

2015-03-16 21:17:45 攻击者第一次访问了 [redacted] 的 /fckeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx 页面

2015-03-16 21:18:21 对 [redacted] 服务器的 /cgi-bin/php4 文件进行了 敏感信息扫描 攻击，该攻击状态是 未知 的

2015-03-16 21:31:45 对 [redacted] 服务器的 /fckeditor/editor/filemanager/connectors/php/upload.php 文件进行了 敏感信息扫描 攻击，该攻击状态是 成功 的

2015-03-16 22:01:45 对 [redacted] 服务器的 /includes/fckeditor/editor/filemanager/connectors/aspx/connector.aspx 文件进行了 敏感信息扫描 攻击，该攻击状态是 未知 的

2015-03-16 23:45:05 对 [redacted] 服务器的 /publish/webscan_test.txt 文件进行了 WEBDAV 攻击，该攻击状态是 未知 的

[redacted] 攻击溯源

攻击过程 | 攻击手法 | 工具包 | 背景分析 | 处理引擎 | 态势感知 | 攻击详细分析 | 完整数据包

攻击者IP：	[redacted]
攻击时间：	
攻击者人数：	2人
国家、时区：	USA、西六区
攻击者浏览器：	chorme Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0
黑客IP来源：	云端引擎库记录
黑客工具分析：	Tornado
黑客云鉴定：	该黑客的攻击手法（扫描指纹，注入指纹）曾经攻击过多个中国政府网站。点击查看详情

通过黑客工具分析，该工具“Tornado”是集sql注入，漏洞扫描，密码拆解为一体的非公开工具，经分析该工具为某一组织自有软件，该工具曾多次攻击过中国政府网站。

通过时区判断，该次攻击事件连续多次进行工具，攻击时间集中在美国时间周一到周五9点到17点左右，初步判断该攻击行为可能是有上班规律的某特定组织。

根据云端记录，该攻击手法曾攻击过多个中国政府。

攻击者多维度信息

OWASP 中国
The Open Web Application Security Project

356	68.36.[redacted]	61.183.[redacted]	高危文件	未收录	成功	98次	高危	2015-04-08 16:00 北京时间下午	日志：未知 探针：未知 云端：已收录	否	攻击溯源

基本信息

IP地址：	68.36.[redacted]
IP所属组织：	CMCS - Comcast Cable Communications, Inc.,US
经纬度：	-74.1001,40.7923
IP来源：	United States,New Jersey
HOSTNAME：	c-68-36-236-16.hsd1.mi.comcast.net
PREFIX：	68.36.0.0/15
ASN：	AS33668
REGION：	New Jersey

通过IP信息可以初步判断该IP来自虚拟空间提供商，非正常用户访问

处理引擎

攻击分析引擎：	发生了98次攻击行为
态势感知引擎：	可疑
云端恶意IP分析引擎：	否
规则分析引擎：	PHPINFO
攻击者数量分析引擎：	2
APT分析引擎：	是
域名分析引擎：	

通过攻击分析引擎判断检测到了5次攻击行为。
态势感知引擎判断为可疑，其依据是云端大数据模型。
该IP被识别为恶意IP，证明之前被有过攻击行为。
该攻击手法被识别为“PHPINFO”方式攻击。
攻击者数量被判定为2人。
被识别为APT攻击，其依据主要是此IP之前有过APT攻击行为，而现在又进行了同样手法的攻击。

云端信息

端口：	80,1723
反向域名：	未检查到域名
注册国家：	未收录
IP所属国家：	美国
服务器信息：	centos 6.5
虚拟空间判断：	是

通过云端的历史记录，该IP曾经开放了80,1723端口也可以断定为跳板机器，非正常用户访问

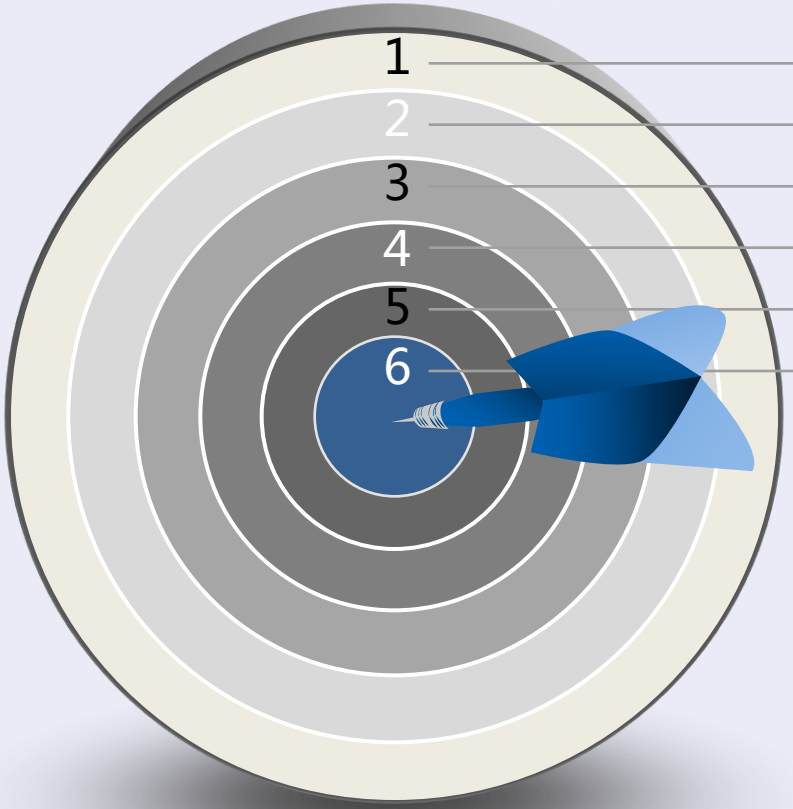
沙箱信息

脚本沙箱：	发现后门
程序沙箱：	未发现可执行文件

通过脚本沙箱，识别出来有后门程序

整体威胁分析

OWASP 中国
The Open Web Application Security Project



已侦测到 **21012123** 条访问记录
共遭受到 **228363** 人次黑客攻击
共有 **12** 台服务器，被 **550** 人次黑客攻击
分析统计后定性为黑客攻击事件 **88** 起
其中有 **2** 台服务器，被黑客**攻击成功**
截获 WebShell 后门 **2** 个

黑客IP来源：

中国：461	**美国：46**
法国：14	德国：5
中国香港：4	俄罗斯：3
加拿大：3	乌克兰：2
哥伦比亚：2	朝鲜：2
中国台湾：1	荷兰：1
阿塞拜疆：1	越南：1
罗马尼亚：1	马其顿：1
意大利：1	菲律宾：1

应急响应模型对比分析

OWASP 中国
The Open Web Application Security Project

Prepare – 准备（双向监控流量）

Detection – 检测（态势感知、预警、自动化精确规则匹配）

Containment – 遏制（推送规则给WAF、FW）

Eradication – 根除（自动化定位原因，联动阻断，防御二次）

Recovery – 恢复（漏洞加固方案）

Follow-Up – 跟踪（实时监控、持续跟踪）

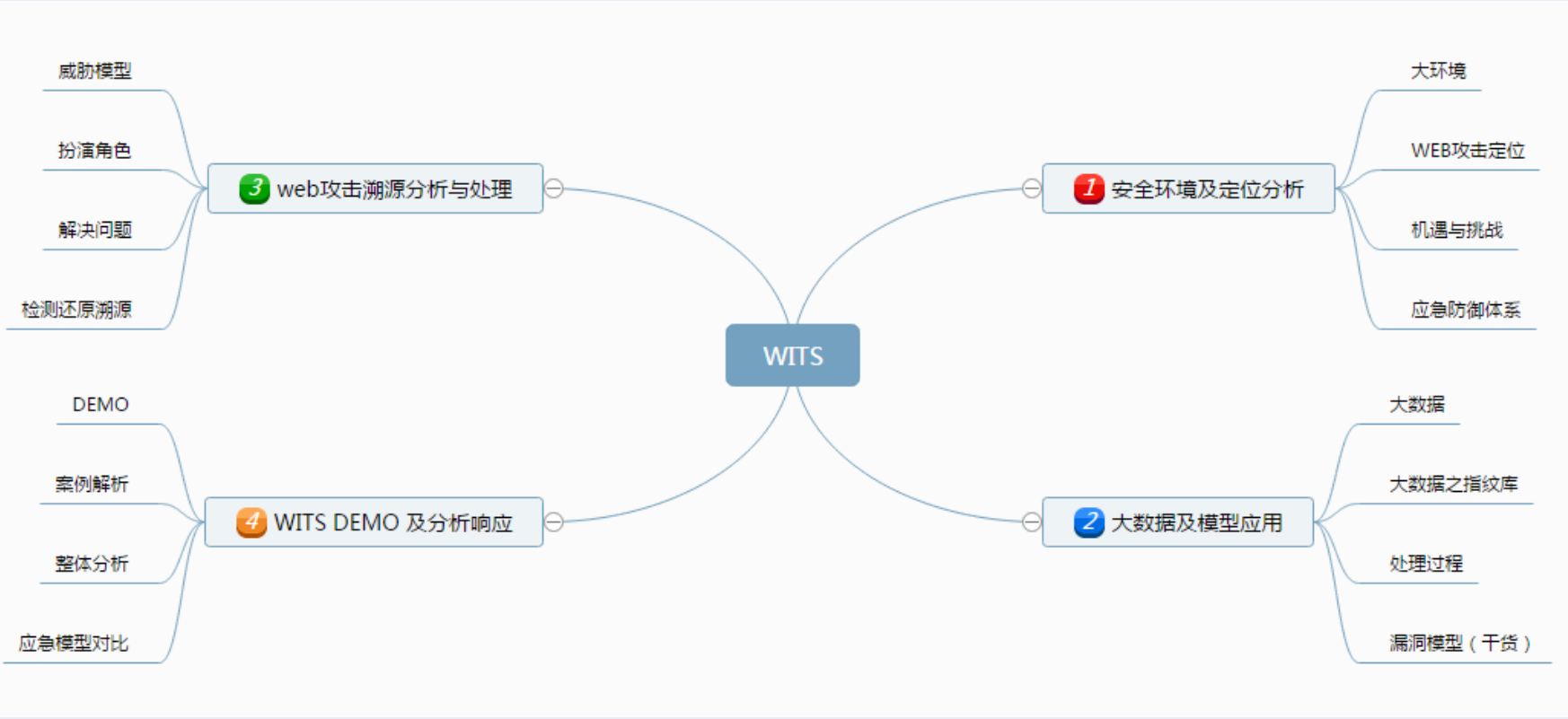
安全功能展望

OWASP 中国
The Open Web Application Security Project

- 联动处理
  - 目前已经实现联动分析，联动接口已开放
  - WAF、FW联动
- 引擎融入
  - 沙箱脚本
  - 杀毒引擎
- 瓶颈分析
  - 各家安全产品联动处理接口多而杂
  - 业务逻辑漏洞

总结

OWASP 中国
The Open Web Application Security Project



OWASP 中国
The Open Web Application Security Project

Thx,Q&A