魔方安全科技
CUBESEC TECHONOLOGY


以攻为守的情报分析

Attack As Defense

CubeSec产品团队
吴昊　ID：短信炸弹
袁帅　ID：Sampro

CubeSec Product Develop Team
Written By Hao Wu 、 Shuai Yuan

魔方安全团队介绍

CUBESEC团队由前绿盟科技NSTRT成员121创立，团队成员在代码审计，代码安全开发生命周期（SDL）、APT渗透、无线安全、家庭智能终端逆向分析、手机系统逆向分析、手机应用安全测试等方面有很强的技术实力。

目录

01

PART ONE

何为情报分析

情报分析的概念

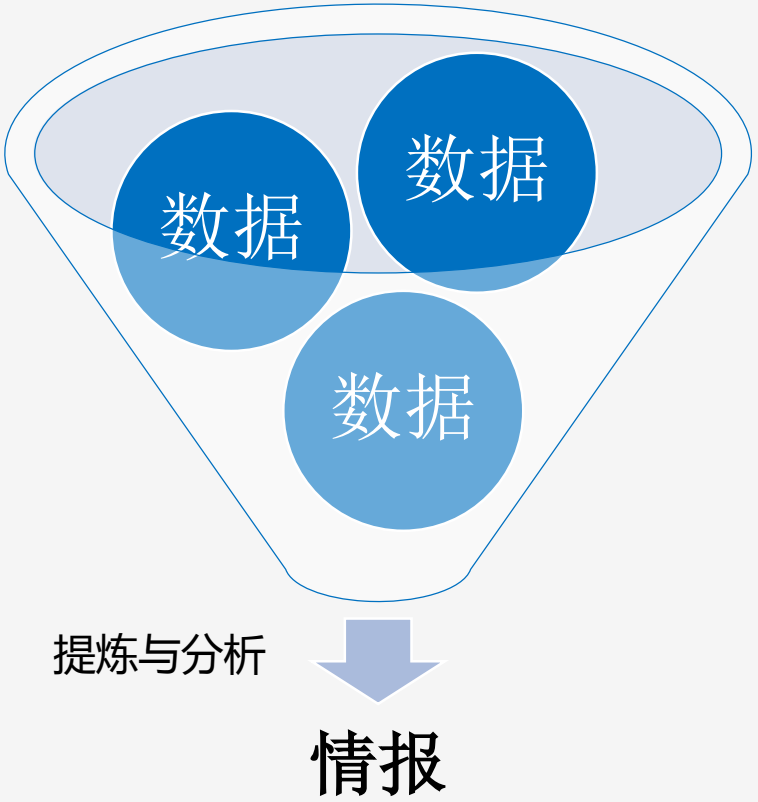
美国《国防部军事与相关术语字典》认为：情报分析是通过**对全源数据进行综合、评估、分析和解读，将处理过的信息转化为情报以满足已知或预期用户需求的过程。**

- **各种各样的情报：**

战争相关：敌情收集、报文窃听等

商业相关：竞争对手分析、市场分析等

生活相关：天气预报、生活资讯等



信息安全相关的情报

资料引用：http://www.sec-un.org/2015-4-30-isc2-hangzhou-conference-of-the-cyber-security-threat-intelligence-systems-and-biosphere-ppt.html

02

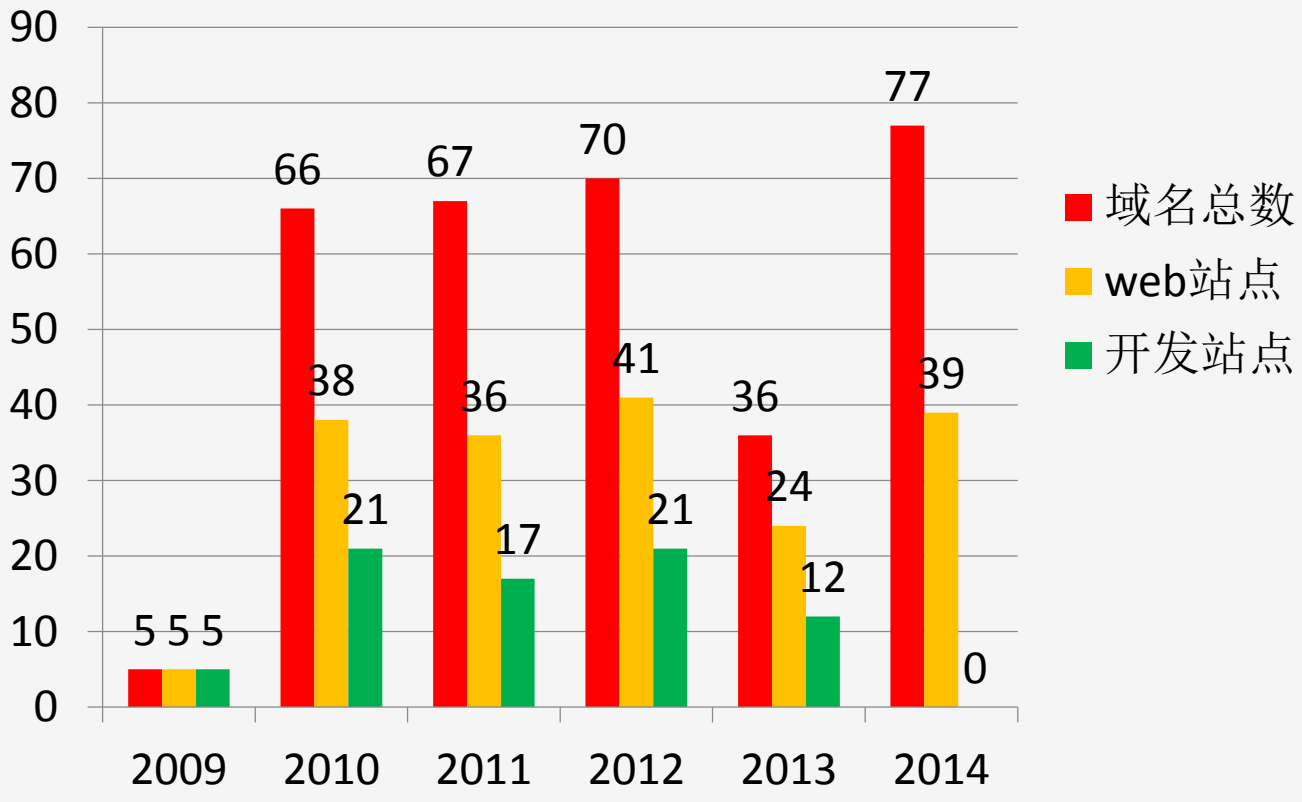
PART TWO

互联网+时代下的安全风险

互联网+时代下企业特点

在互联网+的时代下，除了互联网企业外，越来越多的传统行业的线上业务也在逐步增加。

- 某传统行业客户的互联网资产统计图



互联网安全应该怎么做？？

互联网+时代下的安全问题（一）--边缘资产之殇

随着互联网资产数量的增加，**边缘资产**往往成为黑客的首要目标。

- 互联网公司

提交日期	漏洞名称
2015-09-20	[redacted]房屋运营平台存在爆破风险(可修改房价/经纪人信息泄漏等等)
2015-09-09	[redacted]分站Mysql显错SQL注入漏洞
2015-09-01	[redacted]产存在SQL宽字节注入漏洞
2015-08-28	[redacted]产主站存在SQL注入
2015-08-27	[redacted]站点第三方应用存在SQL注入（Xpath报错注射）
2015-08-24	[redacted]how某栏目SQL注入
2015-08-24	[redacted]博审核不严导致人人都可以成为大V（流程审核不当非技术漏洞）
2015-08-23	[redacted]告某站SQL注入
2015-08-21	[redacted]尔夫频道宽字节SQL注入
2015-08-20	[redacted]站点SQL注射（DBA权限/147个库/千万级数据）
2015-08-20	[redacted]业务站点管理后台弱口令
2015-08-19	[redacted]车ROOT权限SQL注入（19库）
2015-08-07	[redacted]发请求导致未实名账号创建云应用数量限制被突破

- 电子商务

2015-01-23	[redacted]某系统后台源码泄露
2014-11-16	[redacted]任意密码爆破(可大规模扫号)
2014-10-11	[redacted]某后台管理系统弱口令
2014-10-09	[redacted]某服务弱口令可能导致重要信息泄露
2014-08-16	[redacted]存储XSS
2014-07-11	[redacted]某后台弱口令
2014-06-22	[redacted]DNS域传送漏洞
2014-06-15	[redacted]某站点存在SQL注入
2014-06-01	[redacted]APP存在命令执行漏洞
2014-05-21	[redacted]某些开发人员意识不足泄漏敏感信息（github）

互联网+时代下的安全问题（二）--非常规入侵手法

互联网上的信息增多，**敏感信息泄露**成为了辅助渗透的重要手段。

漏洞概要

缺陷编号：[redacted]

漏洞标题：

相关厂商：

漏洞作者： solstice

提交时间： 2015-04-10 16:31

公开时间： 2015-05-28 08:38

漏洞类型： 内部绝密信息泄漏

危害等级： 高

自评Rank： 20

一个员工的密码提交到github，导致全公司Wiki，Jira和代码泄漏。

互联网+时代下的安全问题（三）--重大漏洞的挑战

随着互联网资产的增多，重大漏洞成为安全运维的重大挑战。

重大安全漏洞爆发

如2014年的心脏滴血、Shellsock，2013年的Structs2的S2-016等

安全漏洞修补

针对重要的系统进行优先修补

利用漏洞修补前的时间进行入侵

安全漏洞检测

运维人员和安全人员对内部系统进行检测

查漏补缺

继续对部分边缘系统进行排查与修补

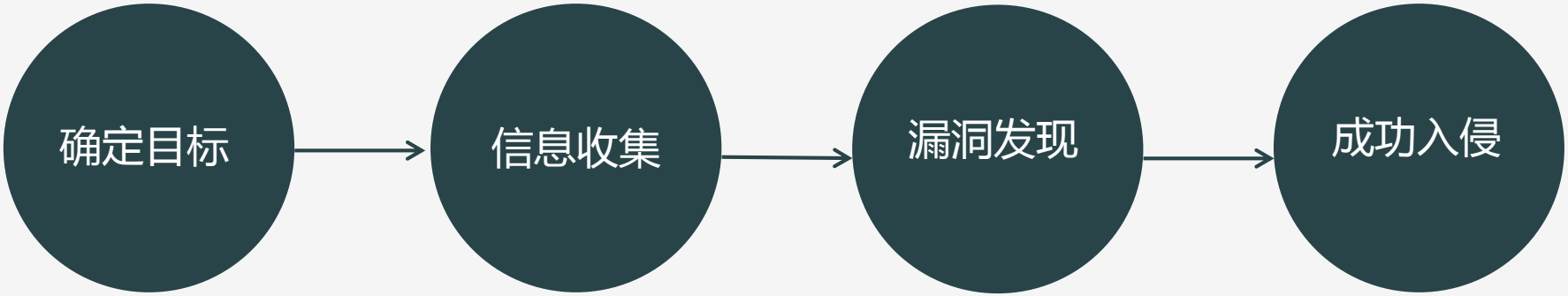
03

PART THREE

以攻为守的安全情报分析

以攻为守的安全情报分析原型

以攻为守的安全情报分析来源于渗透测试，在进行入侵时往往先锁定目标，然后进行大规模的**信息收集**，再发现一个**脆弱点**时进行利用，并持续扩大，最后成功入侵。



渗透测试的过程

以攻为守的安全情报分析技术架构

以外网资产作为持续监控对象，模拟APT攻击过程中的**资产发现、信息收集、漏洞挖掘**，定位企业外网脆弱点，先于恶意攻击者发现问题所在。

以攻击者的角度挖掘企业的脆弱点

以攻为守的安全情报分析技术—自动资产发现

定位资产是情报分析中的关键环节，在互联网+的企业中，外网资产变更速度较快，难以规范整理，必须是“自主挖掘”。

自动资产发现—子域名发现

子域名的收集是资产发现的重要模块分为：

搜索引擎抓取 通过搜索引擎挖掘子域名

全球DNS A记录查询 通过全球DNS数据库查找

常见子域名爆破 前缀数据库暴力猜测

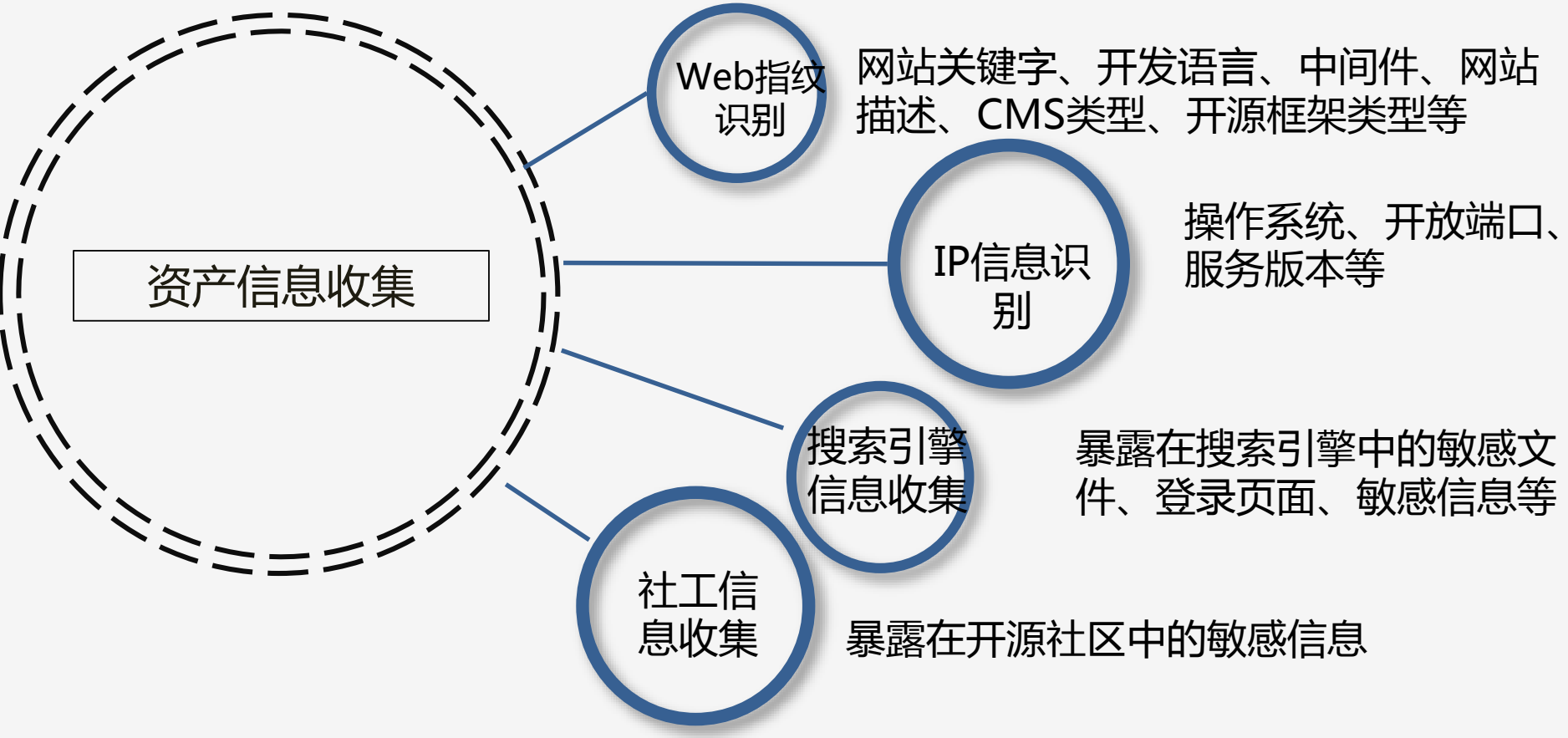
→ **外网域名资产库**

- 发现未知的外网子域名
- 发现外网资产变更，如临时部署在外网的测试服务器
- 发现已遗弃的未知域名

收集边缘子域名

以攻为守的安全情报分析技术—资产信息收集

通过确定的资产信息，对资产进行大范围的信息收集，包括**Web指纹、IP信息识别、搜索引擎信息、社工信息**。



资产信息收集—外网资产信息库

通过**IP信息识别与Web指纹识别，**结合资产发现功能，形成一个庞大的资产数据库，纵观外网。

- **IP信息库**

IP地址	操作系统/服务	端口	版本	Banner
10.1.1.1	Linux	NA	2.62	NA
10.1.1.1	SSH	9000	OpenSSH4.3	Welcome

- **Web指纹信息库**

域名	服务器类型	端口	版本	开发语言	标题
a.test.com	Apache	80	2.20	PHP	XXX门户
b.test.com	Apache Tomcat	8080	5.0	JSP	后台管理

资产信息收集—外网资产信息库

➢ 网段内敏感端口监控

ip	type	port	name	product	version	extrainfo	ostype	banner	domain
114.80.11.254	2	2002	telnet	Cisco router telnetd			不允许	不允许	[redacted].com
114.80.11.254	2	4002	telnet	Cisco router telnetd			不允许	不允许	[redacted]com
58.68.234.33	2	23	telnet	HP H3C SR8808 SecBlade f...			不允许	不允许	[redacted].com
58.68.234.34	2	23	telnet				不允许	不允许	[redacted]com
58.68.234.161	2	23	telnet	HP H3C SR8808 SecBlade f...			不允许	不允许	[redacted].com
58.68.234.162	2	23	telnet	HP H3C SR8808 SecBlade f...			不允许	不允许	[redacted].com
58.68.234.177	2	23	telnet	HP H3C SR8808 SecBlade f...			不允许	不允许	[redacted].com

➢ 资产中隐藏后台的发现

搜索关键字： Tomcat x

Tomcat

ip	type	port	name	product	version	extrainfo	ostype	banner	domain
203.130.47.61	2	80	http	Apache Tomcat/Coyote JS...	1.1				[redacted].com
203.130.47.61	2	80	http	Apache Tomcat/Coyote JS...	1.1				[redacted].com
203.130.47.65	2	8081	http	Apache Tomcat/Coyote JS...	1.1				[redacted]com
203.130.47.66	2	8080	http	Apache Tomcat/Coyote JS...	1.1				[redacted].com
211.151.66.68	2	8080	http	Apache Tomcat/Coyote JS...	1.1				[redacted].com

资产信息收集—搜索引擎信息收集

搜索引擎信息收集是应对非常规入侵的一种新的手段，通过Google、Bing、Baidu等各大搜索引擎，结合搜索引擎语法对敏感信息进行收集，包括**登录入口、泄露邮箱、敏感文件**等。

- **登录入口**

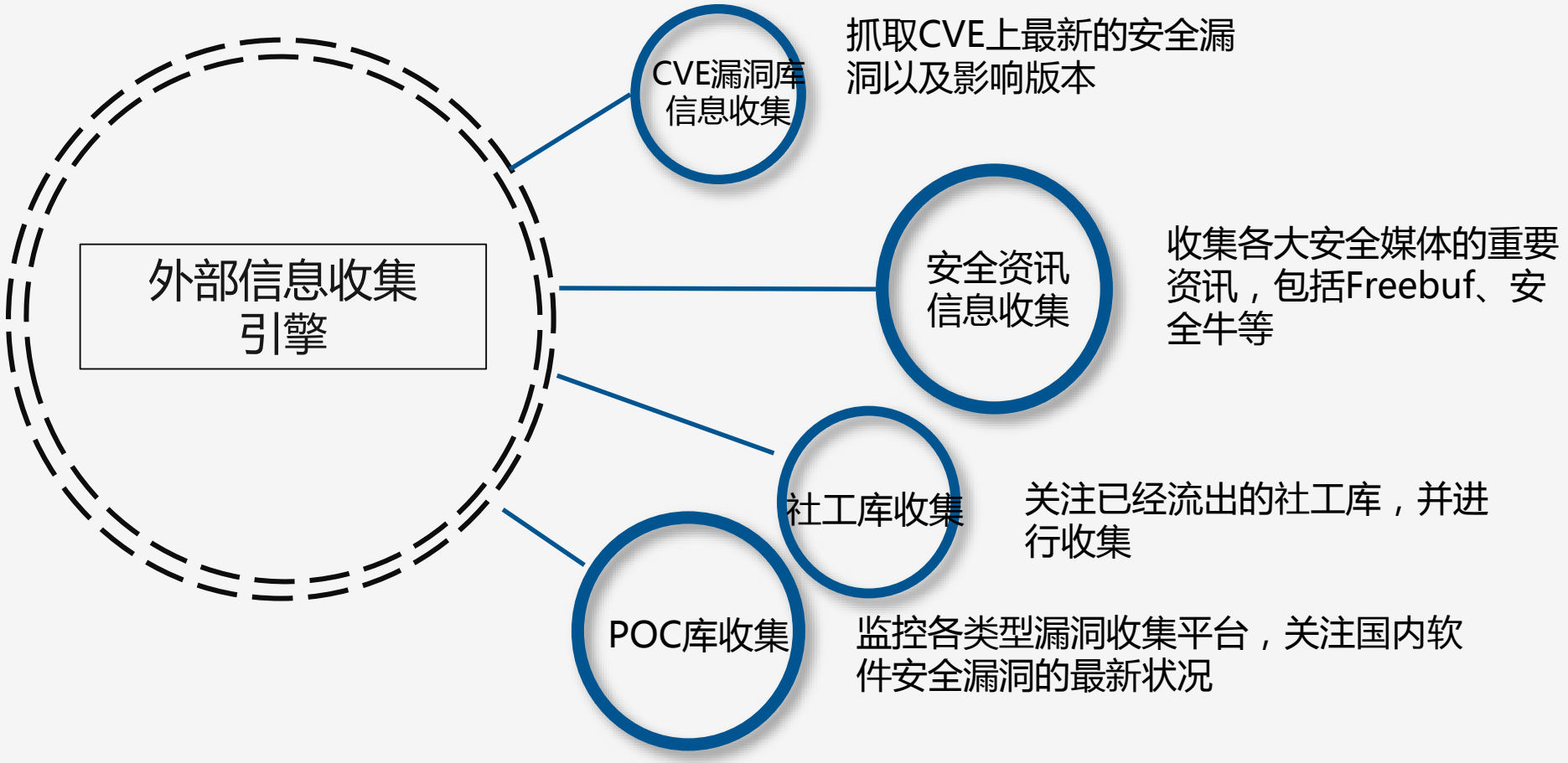
[redacted]com	敏感路径泄露	http://yungouboss.[redacted]com/page/login.html
[redacted]com	敏感路径泄露	http://id.[redacted].com/?ref=http%3A%2F%2F10.13.34.73
[redacted]com	敏感路径泄露	http://id.[redacted].com/
[redacted].com	敏感路径泄露	http://auth.[redacted].com/
[redacted].com	敏感路径泄露	http://id.[redacted].com/?ref=http%3A%2F%2Fcode.auton

- **泄露邮箱**

[redacted].com	email	llpan@[redacted]
[redacted].com	email	y.feng@[redacted]
[redacted].com	email	@[redacted]
[redacted]com	email	service@[redacted]
[redacted]com	email	h_rsv@[redacted]
[redacted].com	email	a_rsv@[redacted]

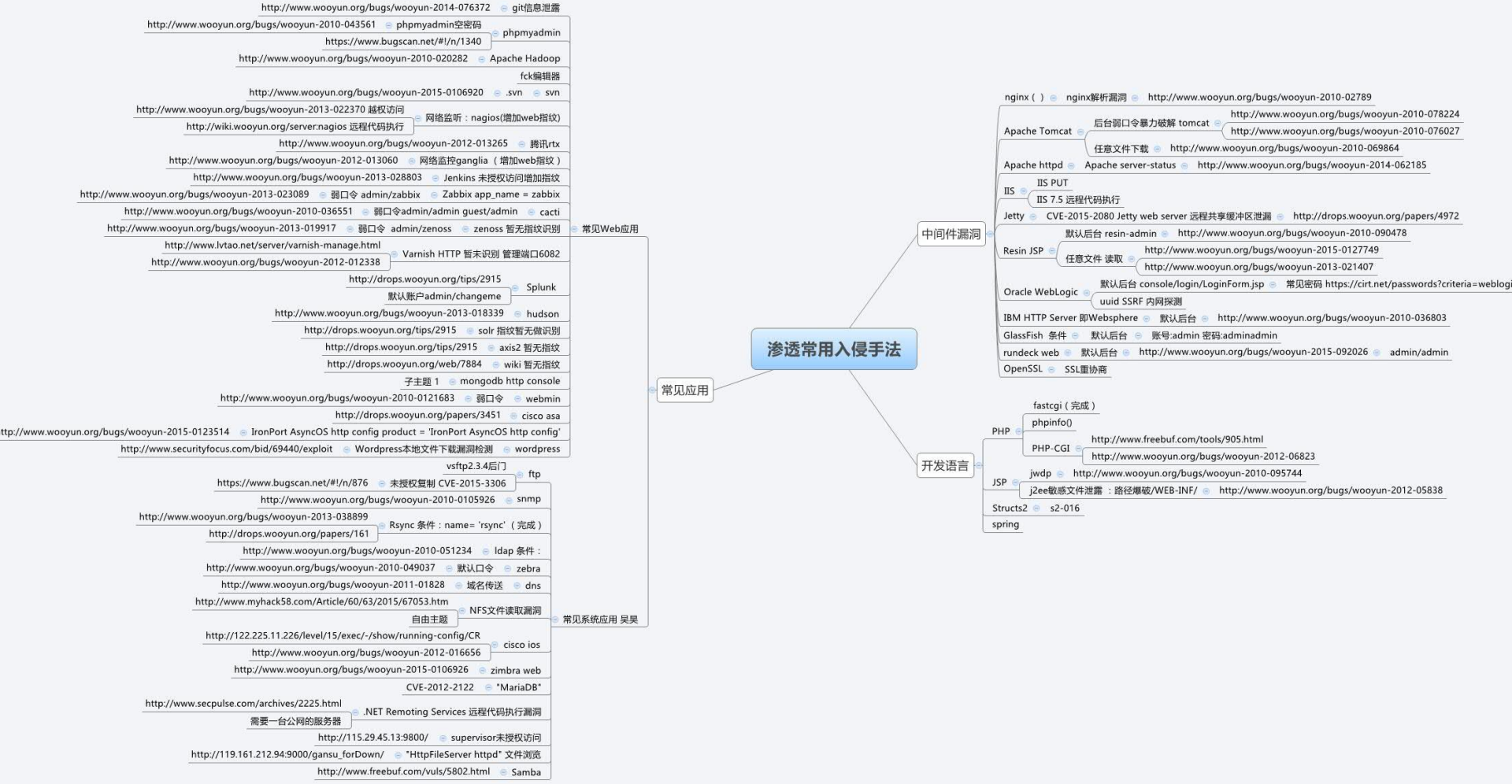
以攻为守的安全情报分析技术—外部信息收集

外部信息收集主要用于收集互联网上的情报，包括**重大的安全漏洞所影响的范围**、**最新的POC**、**社工库信息**等。



POC库收集—POC扫描

将渗透中常用的入侵手法转化成测试脚本，重点关注可入侵型的安全漏洞以及运维失当问题。



以攻为守的安全情报分析技术—情报分析

情报分析是根据海量信息进行筛选，通过可视化的方式展示，同时也可以根据企业自身需要提供所需要的情报。

脆弱性情报

- 高危端口泄露
- 弱口令端口
- 系统安全漏洞
- 开源组件信息
- 漏洞挖掘情报
- 漏洞预警情报

资产状况情报

- 资产变更
- 可用性探测

敏感信息情报

- 敏感文件泄露
- 可撞库登录URL
- 开源社区监控
- 外泄邮箱监控
- 社工库情报

安全资讯情报

- 最新CVE漏洞资讯
- 最新EXP漏洞资讯
- 恶意病毒资讯

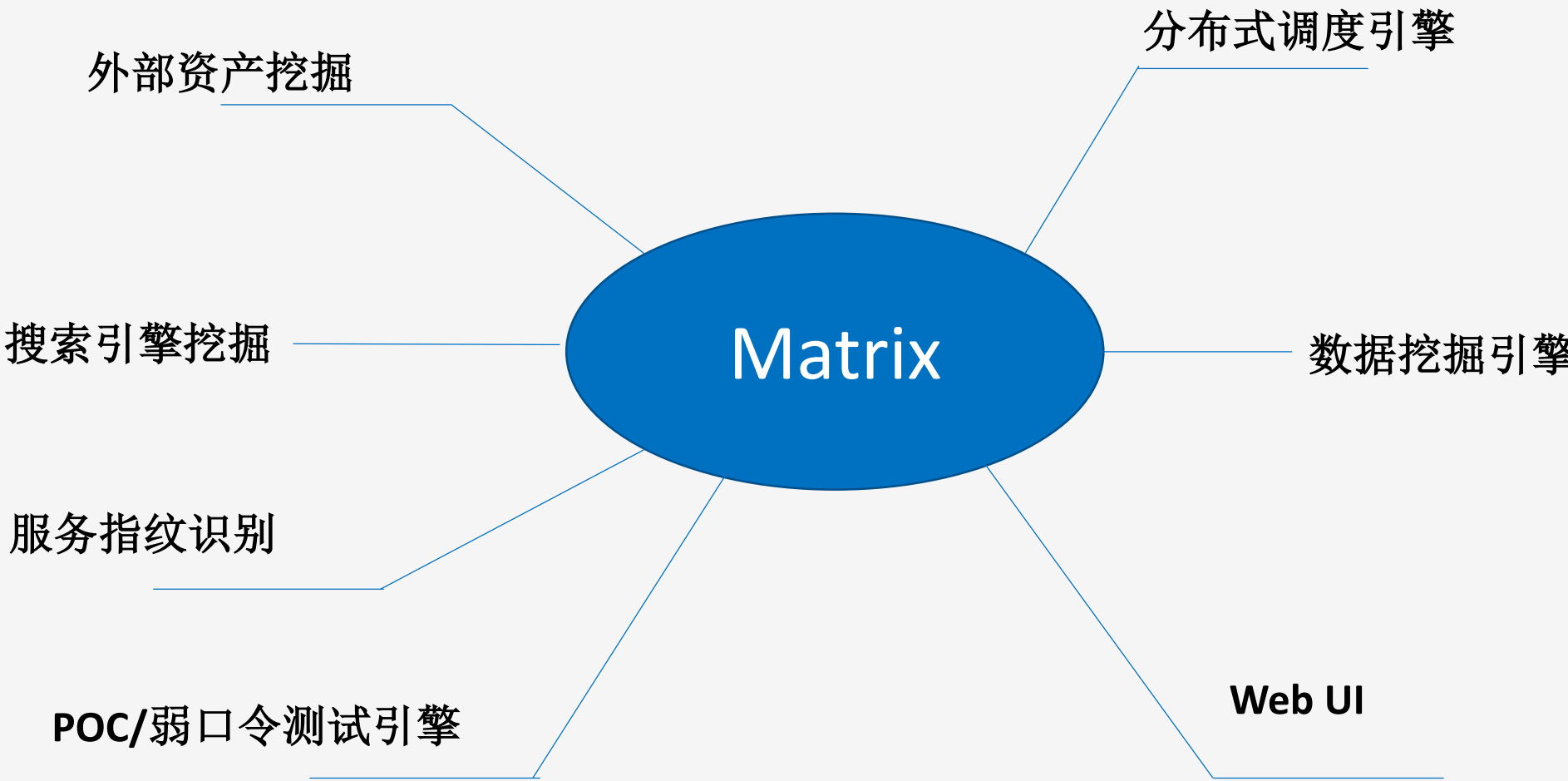
04

PART FOUR

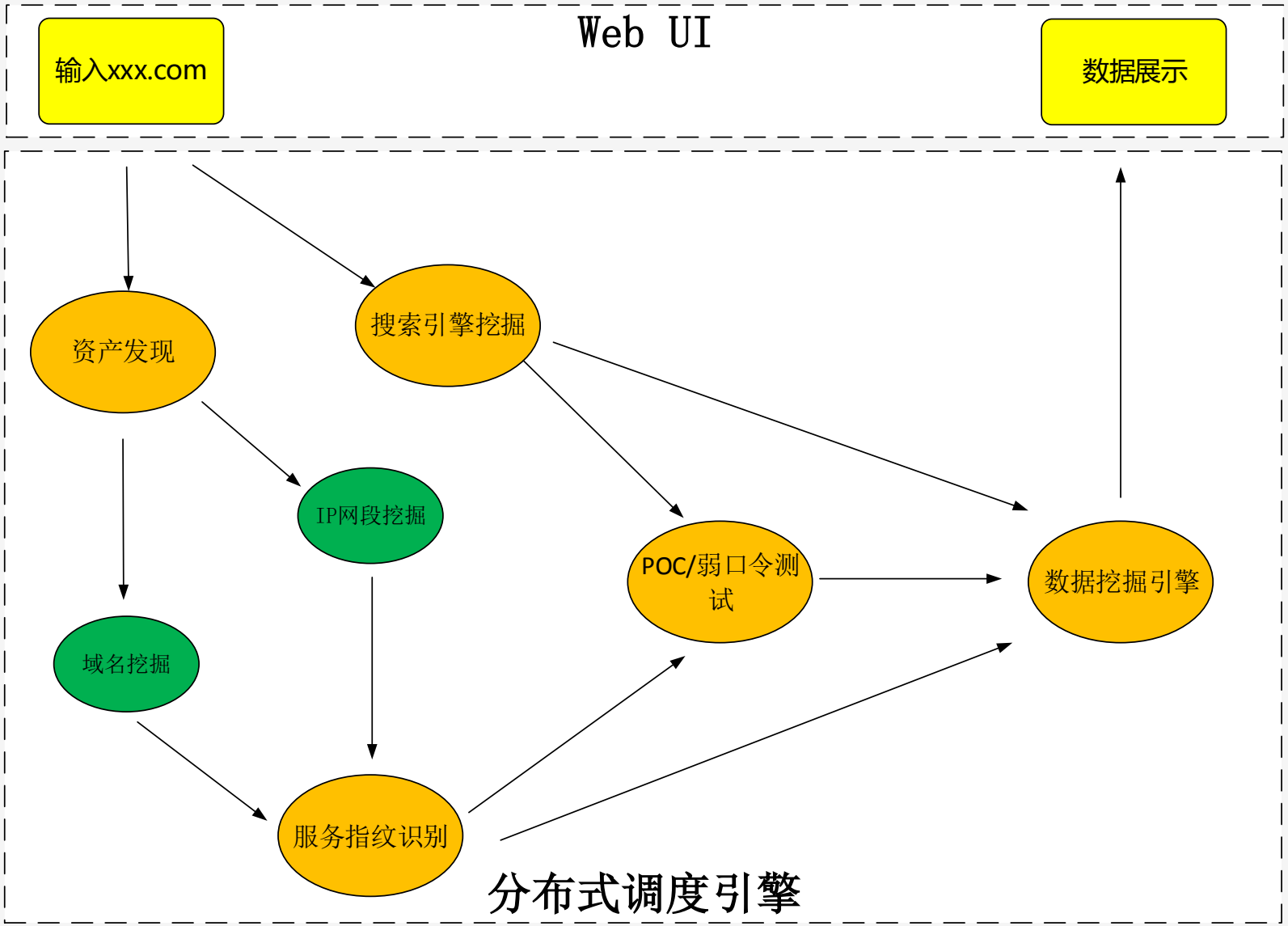
Matrix系统架构

Matrix系统架构—功能架构

目前Matrix系统分为**七大模块：**



Matrix系统架构—系统工作流程



Matrix系统架构—自动资产识别

提高外网资产发现的准确率，建立资产权重算法：

Asset权值计算

IP权值计算

web指纹计算

计算网段权值

单IP权值

算法向量包括：
1、Web指纹，如title、keyword
2 、域名解析与IP反查
3、IP信息，如Banner、

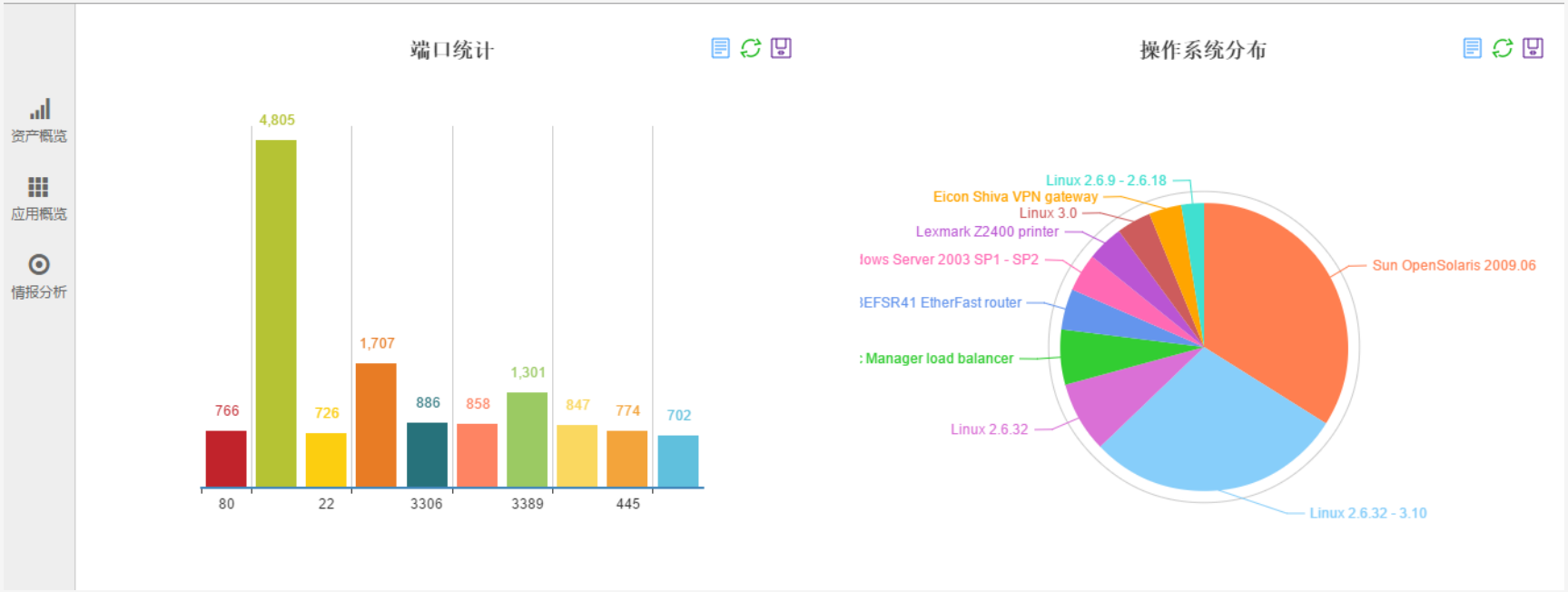
搜索关键字：

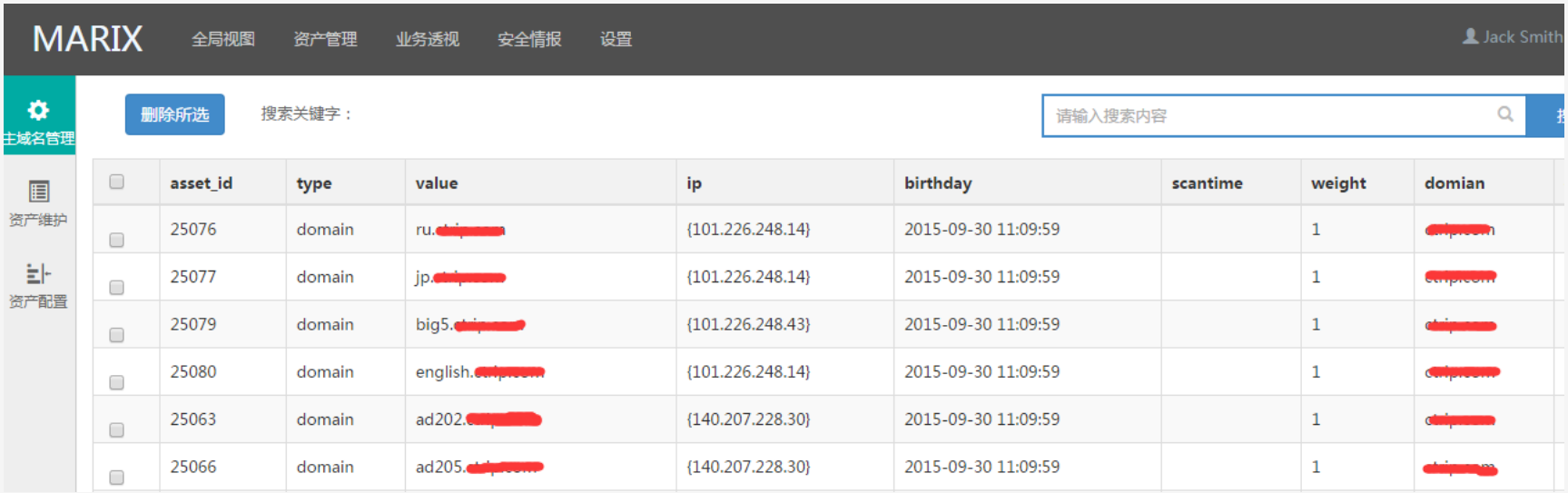
请输入搜索内容

搜索

IP	类型	端口	服务	应用	版本	关联域	权重	扫描时间	操作
113.31.[redacted].78	服务识别	3306	mysql	MySQL	5.5.27	[redacted]	100	2015-10-26 22:58:05	✖
113.31.[redacted].100	服务识别	22	ssh	Huawei VRP sshd		[redacted]	80	2015-10-26 22:58:05	✖
113.31.[redacted].105	服务识别	55	ssh	WeOnlyDo sshd	2.1.3	[redacted]	80	2015-10-26 22:58:05	✖
113.31.[redacted].119	服务识别	3389	ms-wbt-server	Microsoft Terminal Service		[redacted]	80	2015-10-26 22:58:05	✖
113.31.[redacted].120	服务识别	55	ssh	WeOnlyDo sshd	2.1.3	[redacted]	80	2015-10-26 22:58:05	✖
113.31.[redacted].122	服务识别	22	ssh	OpenSSH	5.3	[redacted]	80	2015-10-26 22:58:05	✖
113.31.[redacted].131	服务识别	22	ssh	OpenSSH	4.7	[redacted]	80	2015-10-26 22:58:05	✖
113.31.[redacted].132	服务识别	1688	ms-wbt-server	Microsoft Terminal Service		[redacted]	80	2015-10-26 22:58:05	✖
113.31.[redacted].133	服务识别	3307	mysql	MySQL		[redacted]	80	2015-10-26 22:58:05	✖
113.31.[redacted].133	服务识别	3316	mysql	MySQL	5.6.12-log	[redacted]	80	2015-10-26 22:58:05	✖

Matrix系统架构—Web UI





内容总结

化被动转换为主动，将主动权放在自己手上

安全+运维自动化

感谢各位聆听

Thanks for Listening