Alibaba Group 阿里巴巴集团 × 蚂蚁金服 ANT FINANCIAL

智能时代风险的安全治理思路探讨

--摸清家底实践

· 权小文@WebRAY

背景介绍

“要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。要建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。”

-习近平在网信工作座谈会上的讲话。（2016年4月19日）

背景介绍 | 从校园网看安全现状

1、利用学校资源搭建商业网站

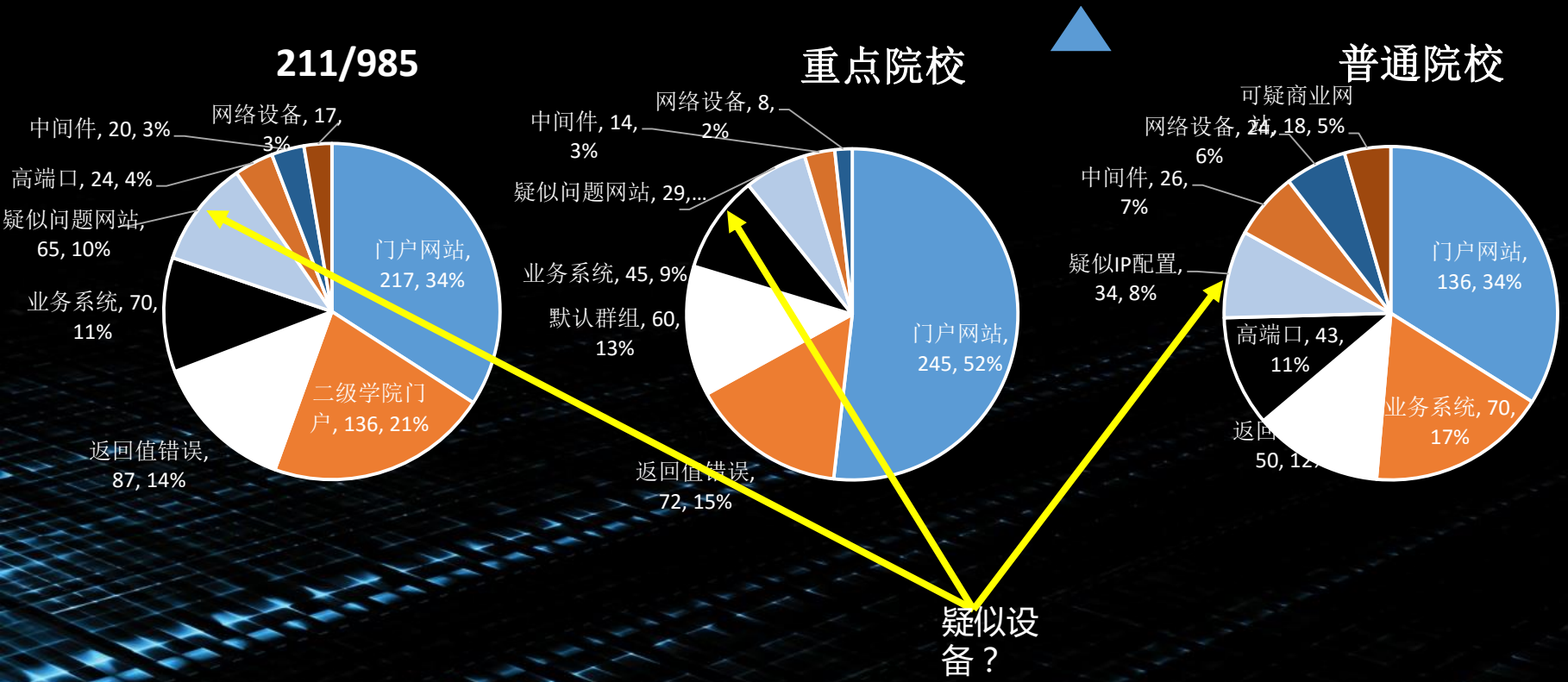
2、废弃网站未能及时退运

3、未知站点访问量异常

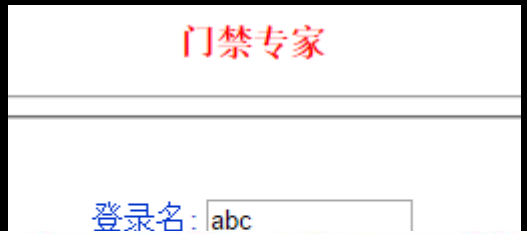
4、视频监控配置公网IP，且存在弱口令

5、打印机、网络设备配置公网IP，且存在弱口令

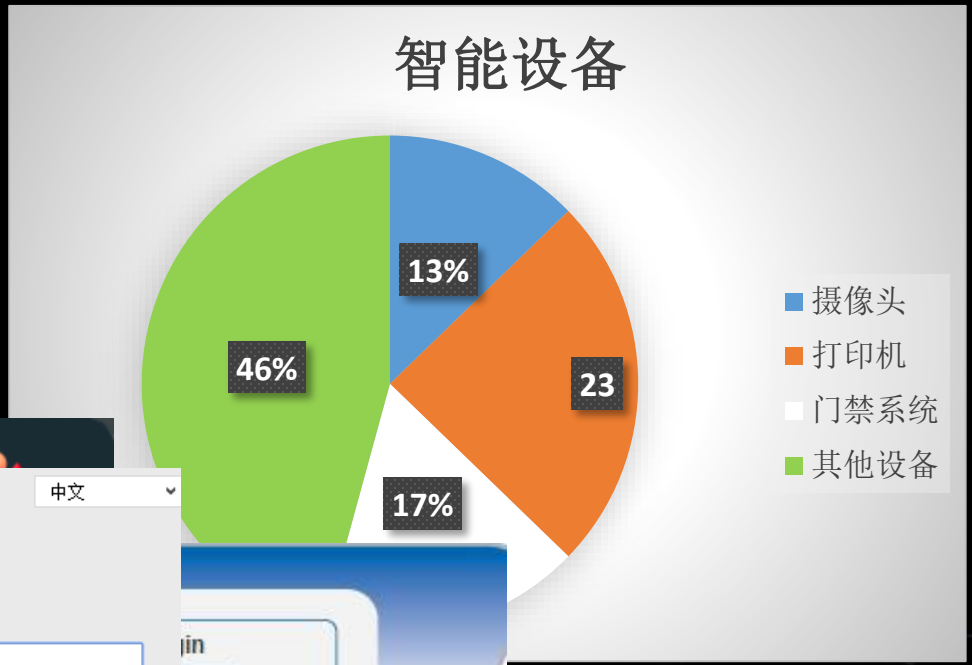
背景介绍 | 教育行业Web应用分布情况

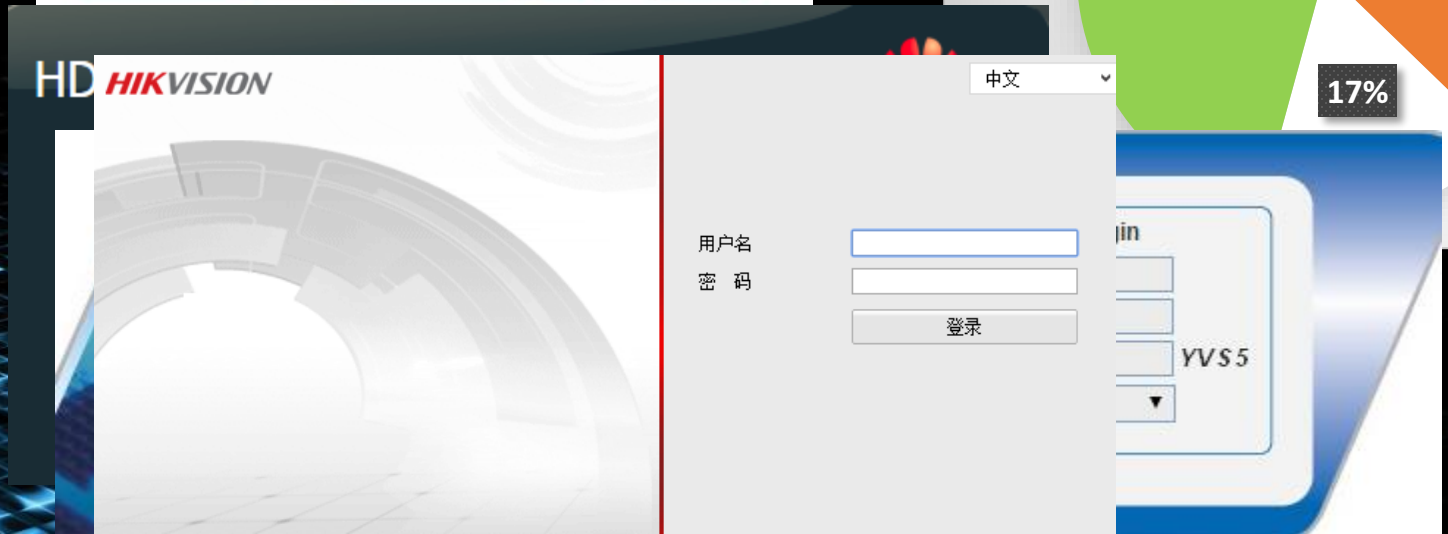


背景介绍 | 智能设备普查


门禁专家
登录名：abc


DCN

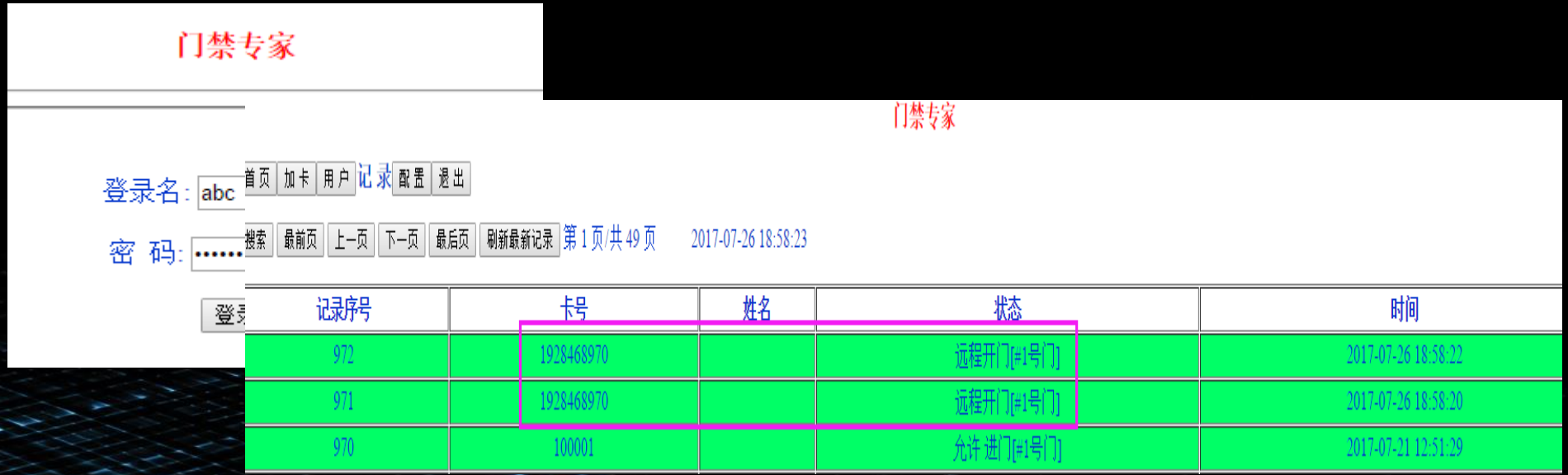

智能设备
13%
23
17%
46%
摄像头
打印机
门禁系统
其他设备


HIKVISION
中文
用户名
密 码
登录
YVS5

背景介绍 | 结论1：有人建，没人管。有人用，没人防

- 数量多，使用权、管理权分散
- 系统私搭乱建现象严重，常规手段无法监测网站数量
- 责、权、利不好界定，“网络中心”“信息中心”成为业务部门替罪羊
- 专业人员配置不足
- 退运的系统，无人监督管理，成为孤岛

背景介绍 | 结论2： 智能设备大多弱口令或者无口令



实践方案

“摸家底“系统

网络空间威胁发现系统

第一阶段

网络空间资产发现

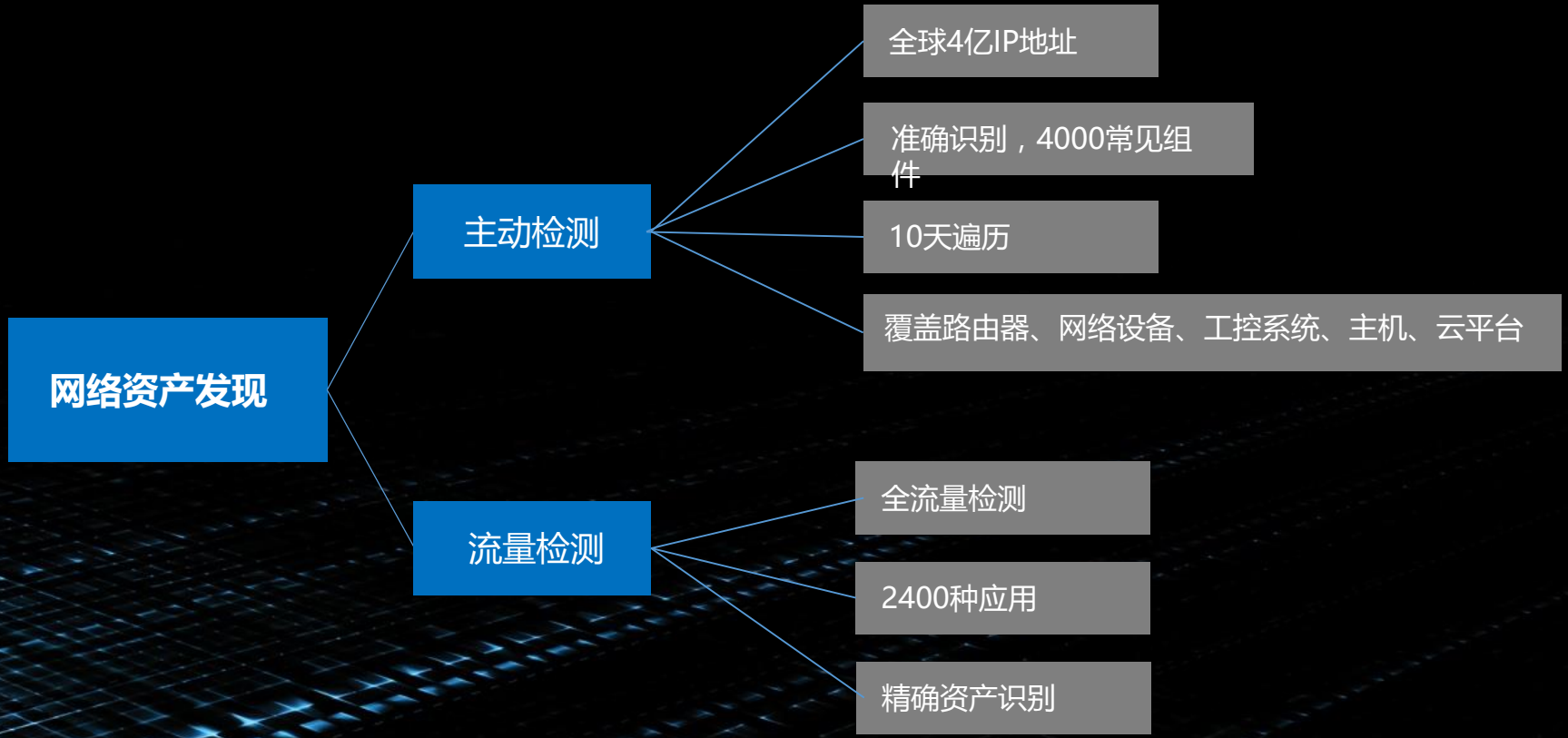
第二阶段

网络空间漏洞检测

第三阶段

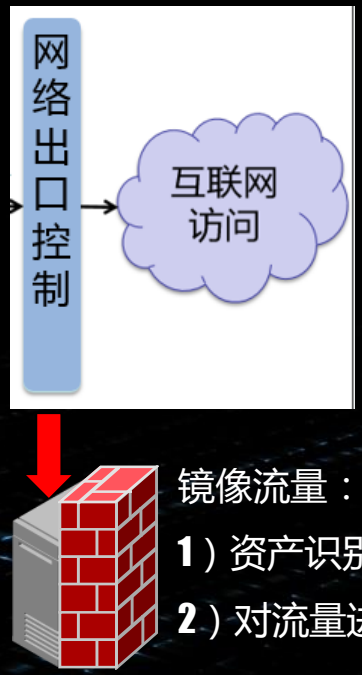
安全事件通报/处置

阶段1：网络空间资产发现



阶段1：网络空间资产发现

名称	数量
路由器	37+
打印机	10+
各种应用程序	3900+
工控设备	360+
操作系统	20+
网络安全设备	45+

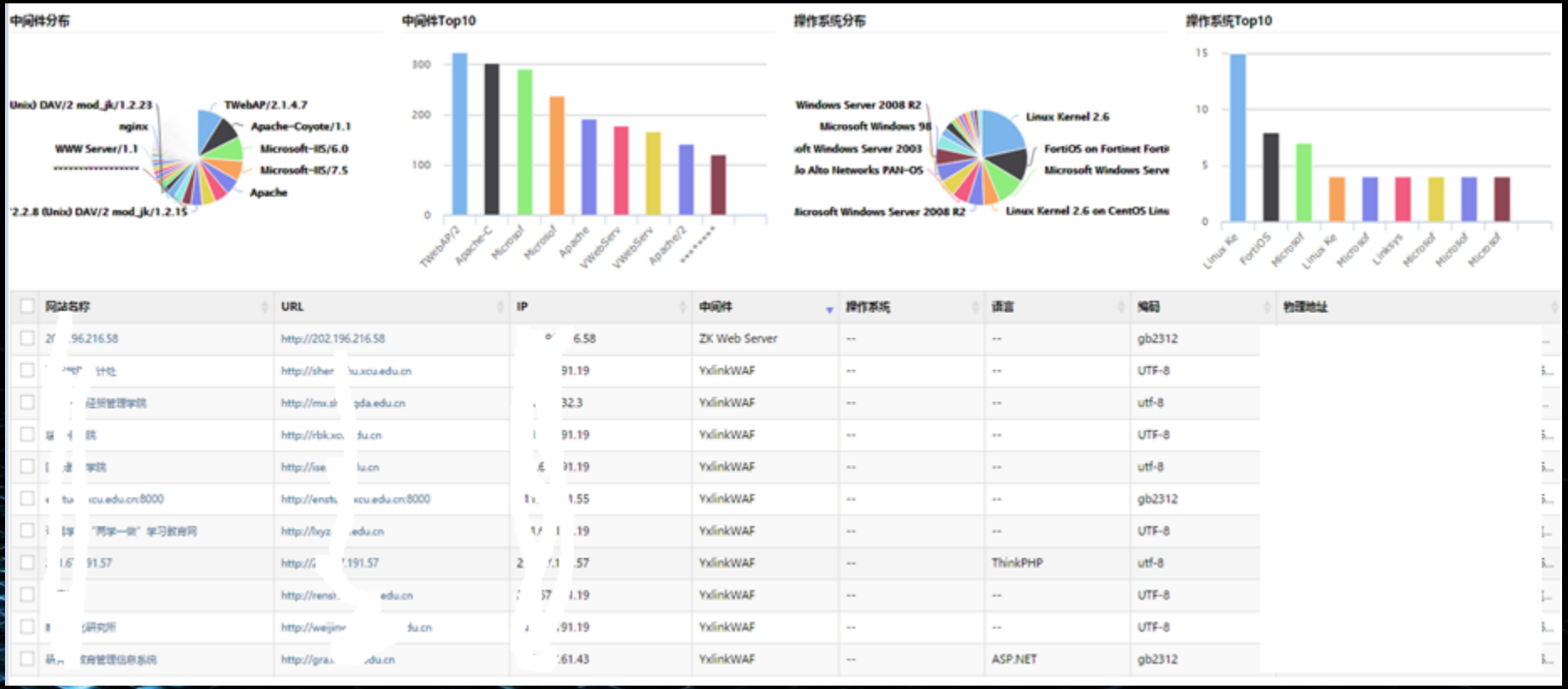


镜像流量：

1）资产识别（DPI+AI）；

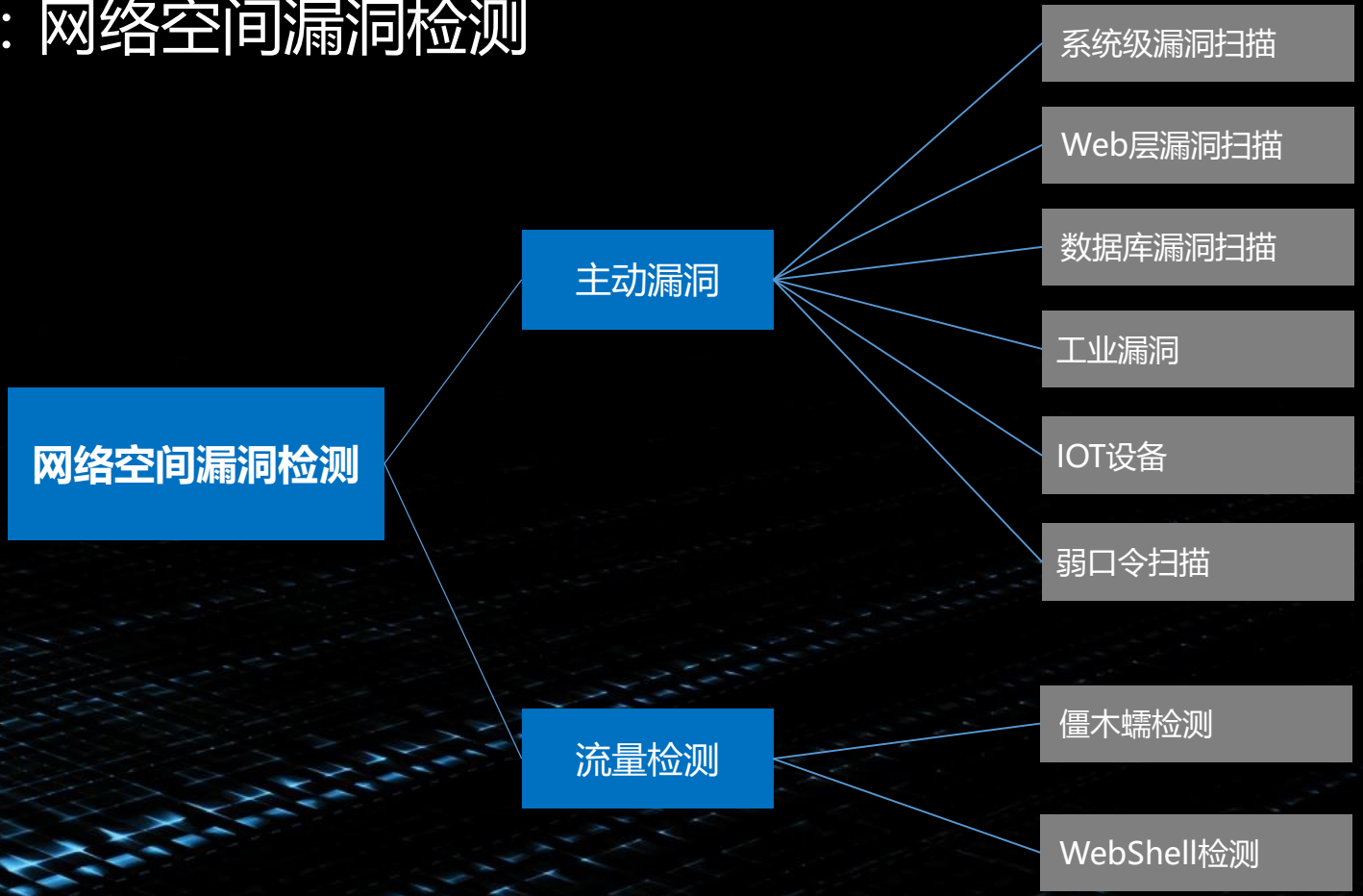
2）对流量进行webshell被动学习；

阶段1：网络空间资产发现



网站名称	URL	IP	中间件	操作系统	语言	编码	物理地址
2 .96.216.58	http://202.196.216.58	6.58	ZK Web Server	--	--	gb2312	
计处	http://sher u.xcu.edu.cn	91.19	YxlinkWAF	--	--	UTF-8	
经管理学院	http://mx.sl gda.edu.cn	32.3	YxlinkWAF	--	--	utf-8	
院	http://rbk.xc du.cn	91.19	YxlinkWAF	--	--	UTF-8	
学院	http://ise lu.cn	91.19	YxlinkWAF	--	--	utf-8	
xcu.edu.cn:8000	http://ensts xcu.edu.cn:8000	1.55	YxlinkWAF	--	--	gb2312	
"两学一做"学习教育网	http://lxyz .edu.cn	.19	YxlinkWAF	--	--	UTF-8	
91.57	http:// 191.57	.57	YxlinkWAF	--	ThinkPHP	utf-8	
	http://rensh edu.cn	4.19	YxlinkWAF	--	--	UTF-8	
研究所	http://weijinv du.cn	.91.19	YxlinkWAF	--	--	UTF-8	
教育管理信息系统	http://gra edu.cn	61.43	YxlinkWAF	--	ASP.NET	gb2312	

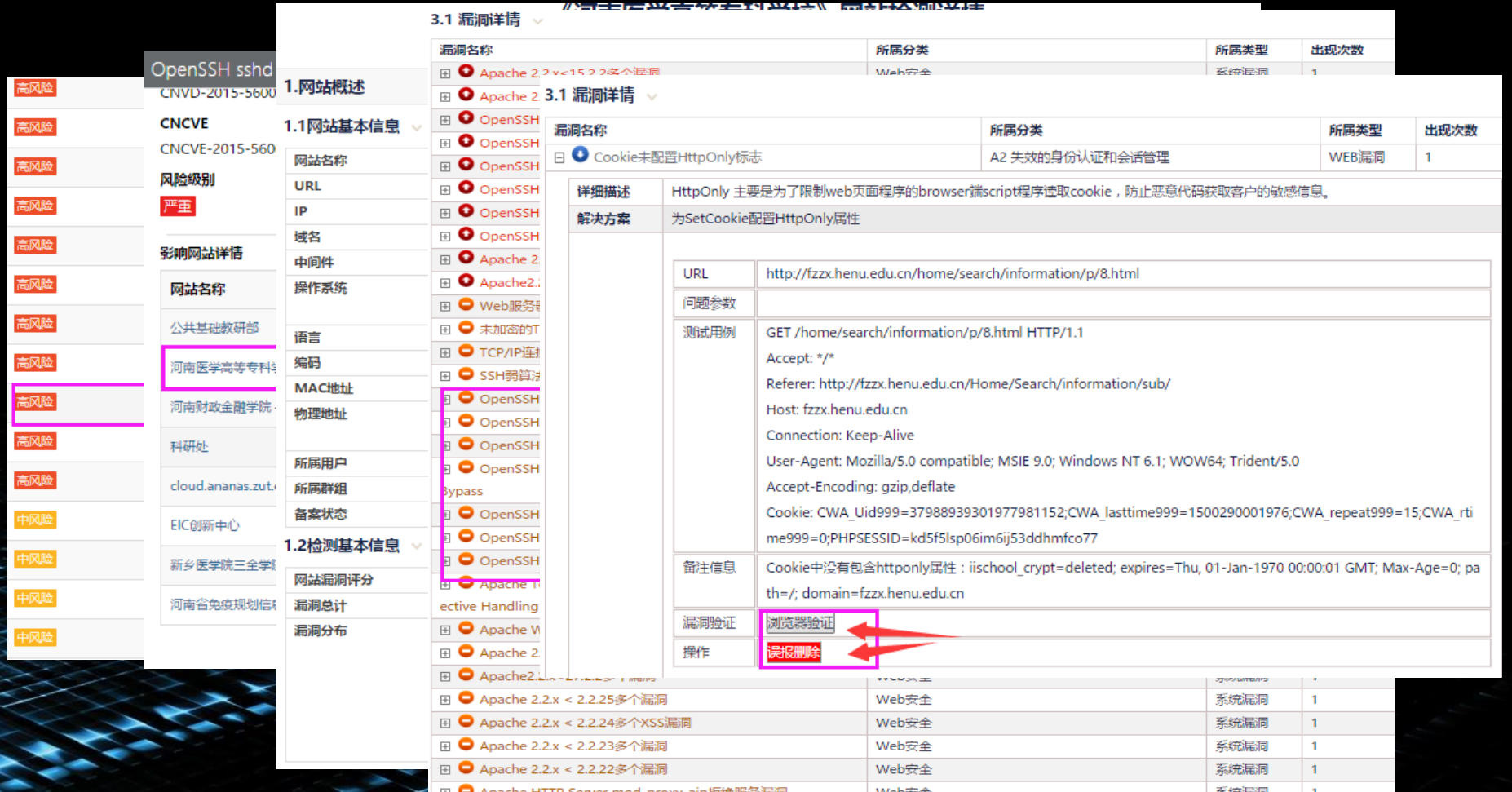
阶段2：网络空间漏洞检测



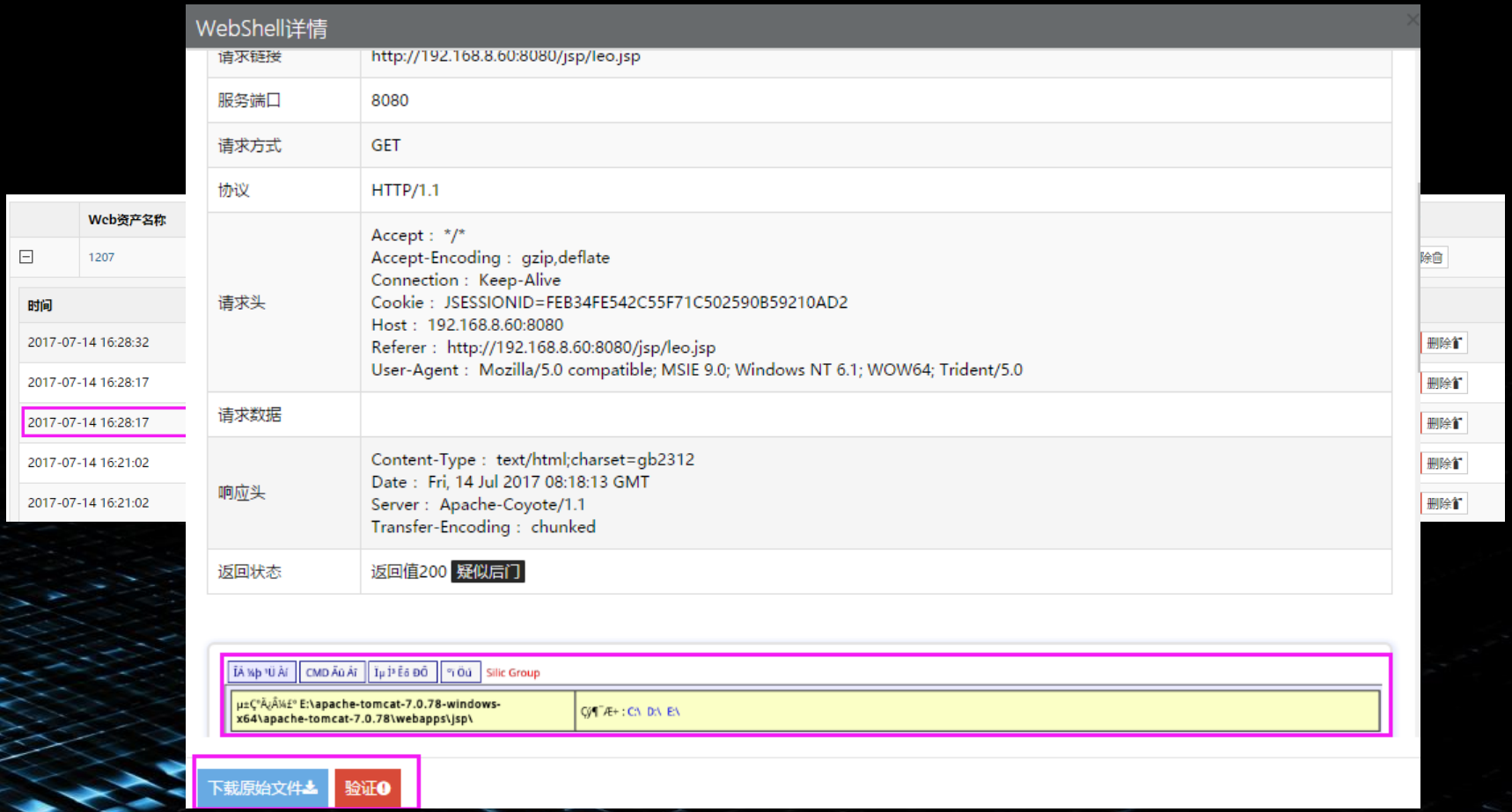
阶段2：网络空间漏洞检测

名称	数量
Web漏洞	900+
系统漏洞	70000+
数据库漏洞	2900+
工控漏洞	460+
敏感词库	20000+
暗链词库	300+
后台词典库/webshell	4000+（部分来自守望者实验室）
弱密码库	80万条

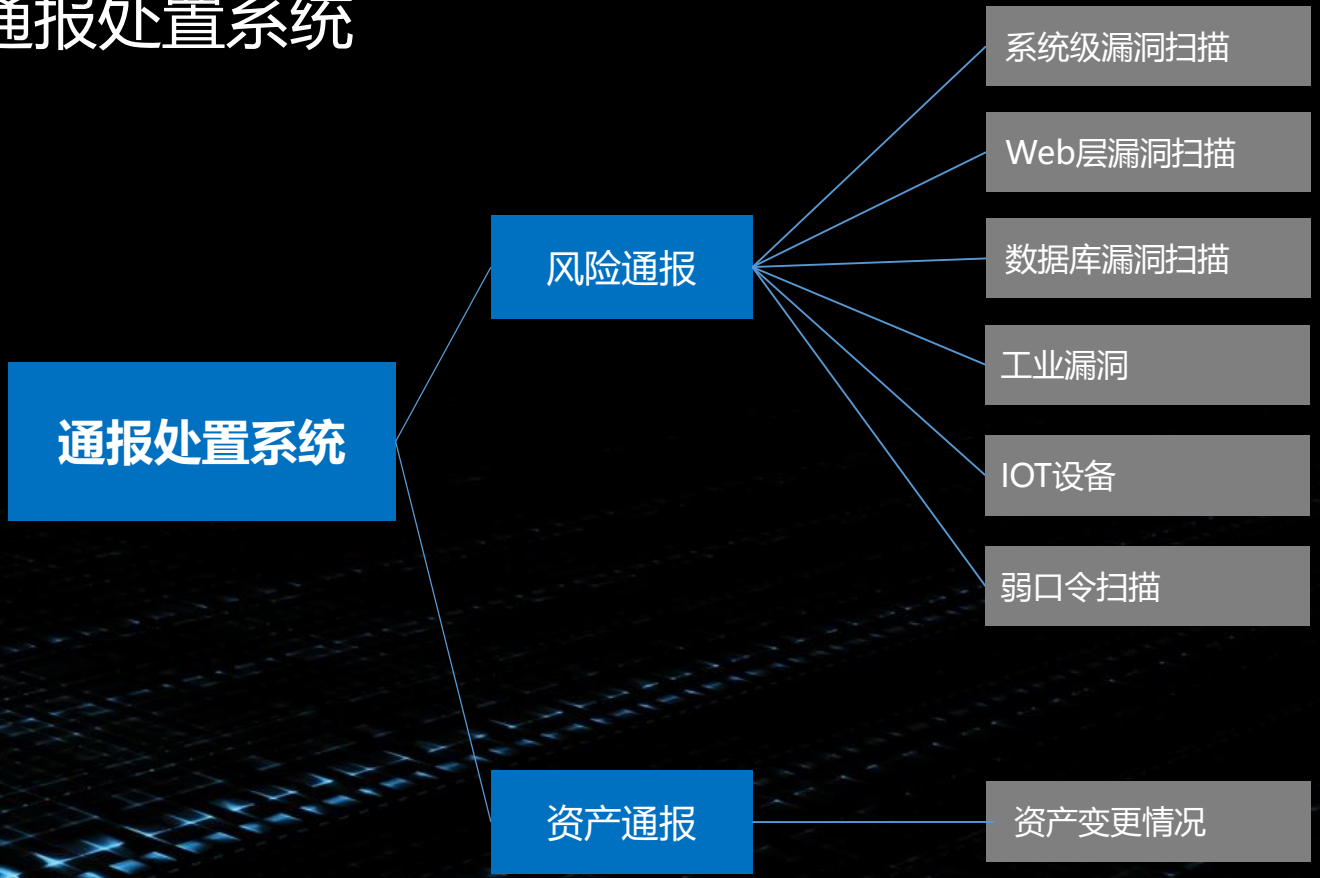
阶段2：网络空间漏洞检测



阶段2：网络空间漏洞检测



阶段3：通报处置系统


通报处置系统
风险通报
资产通报
系统级漏洞扫描
Web层漏洞扫描
数据库漏洞扫描
工业漏洞
IOT设备
弱口令扫描
资产变更情况

阶段3：风险资产事件通报处理

序号	单位名称	网站名称	行业类别	单位地址	网站域名（选择接口提供数据）	IP地址	区县	行政区划代码	创建日期
1	品药品监督管理局 分局	药品监督管理局 分局	公安		http://www. ov.cn				2017-04-09 14:41:49
2	区环境保护局	区环境保护局	公安		http://www. gov.cn		区	330402	2017-04-09 14:41:31
3	区公共资源交易中心	区公共资源交易中心	公安		http://www. .com		区	330402	2017-04-09 14:41:13
4	城乡建设委员会	城乡建设委员会	公安		http://www. v.cn			330402	2017-04-09 14:40:59
5	区人民代表大会常务委员会	区人民代表大会常务委员会	公安		http://www. gov.cn		区	330402	2017-04-09 14:40:00
6	商务局	区商务局	公安		http://www. z.gov.cn		区	330402	2017-04-09 14:39:39
7	区交通委员会	区交通委员会	公安		http://www. com		区	330402	2017-04-09 14:39:15
8	就业服务管理局2	就业服务管理局2	公安		http://www. r.cn		区	330402	2017-04-09 14:36:38
9	就业服务管理局1	就业服务管理局1	公安		http://www. .com		区	330402	2017-04-09 14:36:16
10	经济和信息化委员会	区经济和信息化委员会	公安		http://www. w.com		区	330402	2017-04-09 14:35:48

阶段3：风险资产事件通报处理

阶段3：风险资产事件通报处理

欢迎指正，谢谢