WOTA

51CTO

World Of Tech 2017

# 全球架构与运维技术峰会

2017年4月14日-15日　北京富力万丽酒店

ARCHITECTURE

WOTA

51CTO

出品人及主持人：

于　雪　51CTO WOT大会主编

# 主动安全防御体系构建

WOTA

51CTO

# 可知 可感 可查 可控

## 打造新一代Web安全治理体系

WOTA

51CTO

# 李春鹏

盛邦安全
技术顾问

分享主题：

可知、可感、可查、可控
——打造新一代Web安全治理体系

# 目录
content

# 背景介绍|安全管理者的梦想与现实

## 梦想：

- 我的地盘我做主
- 什么系统上线我说了算
- 系统在哪里我都知道
- 系统干了什么我都了解
- 系统有什么弱点我都清楚
- 出了任何问题立刻定位
- 找得到人，断得了网


## 现实：

- 都说是我的地盘，可我做不了主
- 线上有哪些系统真是不知道
- 系统在哪里，归谁管我也不清楚
- 这系统有什么漏洞，都干了什么我更不清楚
- 出了事了，都来找我，可我该找谁？
- 断网？连系统在哪都不知道，怎么断网？

# 背景介绍|四部委联合发文加强网站治理

公　　安　　部
中　央　网　信　办
中央机构编制委员会办公室
工　业　和　信　息　化　部

公信安〔2015〕2562号

关于印发《党政机关、事业单位和国有企业互联网网站安全专项整治行动方案》的通知

各省、自治区、直辖市、新疆生产建设兵团公安厅、局，网信办，机构编制委员会办公室，通信管理局：

为提高党政机关、事业单位和国有企业互联网网站安全防护水平，防范和打击境内外不法分子攻击篡改，破坏网站安全的违法犯罪活动，维护党政机关、事业单位和国有企业互联网网站安全稳定运行，保障网络安全和国家安全，公安部、中央网信办、中央机构编制委员会办公室、工业和信息化部决定，自2015年9月底至2016年6月底，在全国范围内开展党政机关、事业单位和国有企业互联网网站安全专项整治行动。现将《党政机关、事业

公安部网站大检查
2013.9

结论：5.2万gov.cn网站，76%以上网站存在安全隐患，40%网站可以被拿到控制权

中央网信办 <1号文> 2014.5.9

2014.10.18：香港占中事件， 匿名组织对国内攻击
监测报告：55%左右政府网站存在安全隐患！过半高校网站存在安全漏洞,更有20%的高校官网已经被黑客入侵篡改

中央网信办、中编办
<69号文件>
2014.11.24

2015.9.3 国家“9.3”阅兵，30%左右重要政府网站在阅兵当天关闭，包括大量央企、省级门户网站

第一次全国政府网站普查
2015.3.24

公安部（执法）、中央网信办（起草）、中编办、工信部
<2562号文件>
俗称**四部委文件** 2015.9.30

# 背景介绍|网络安全年

“一带一路”会议、金砖会议、香港回归20周年、中国人民解放军建军90周年、“十九大”

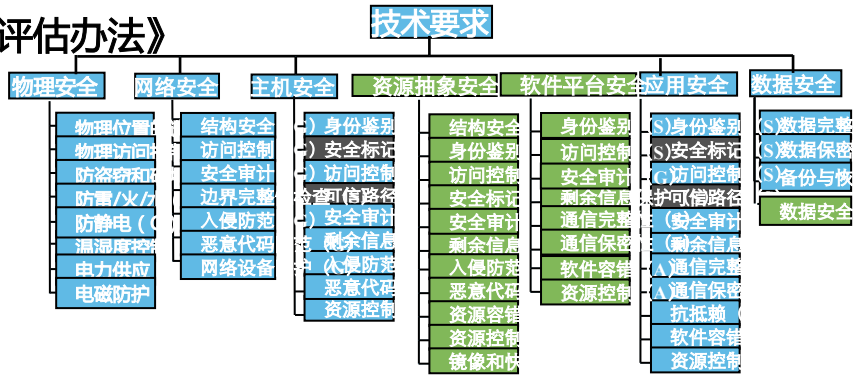
《中华人民共和国网络安全法》

第二条 网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。因业务需要，确需向境外提供的，应当按照本办法进行安全评估

关键信息系统检查

“云等保”

《个人信息和重要数据出境安全评估办法》




**关键信息基础设施包括**

**网站类**

如党政机关网站、企事业单位网站、新闻网站等；

**平台类**

如即时通信、网上购物、网上支付、搜索引擎、电子邮件、论坛、地图、音视频等网络服务平台

**生产业务类**

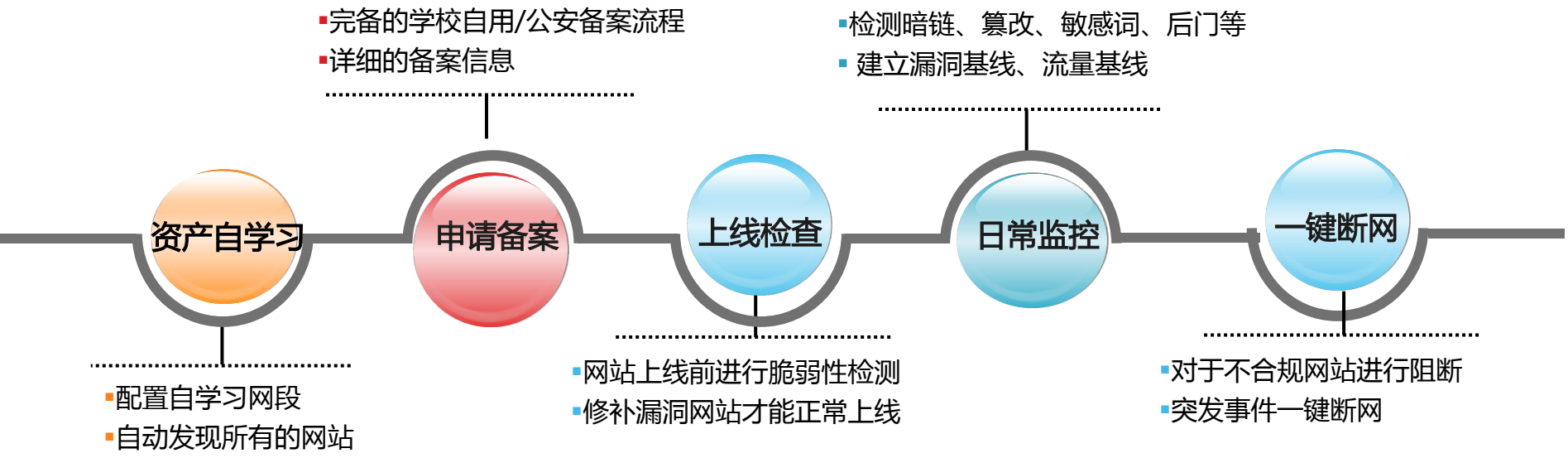
如办公和业务系统、工业控制系统、大型数据中心、云计算平台、电视转播系统等。

# 目录
content

“当我派一个人出去买马时，我并不希望这个人告诉我这匹马的尾巴有多少根毛。我只希望知道它有什么样的特点。”

——林肯

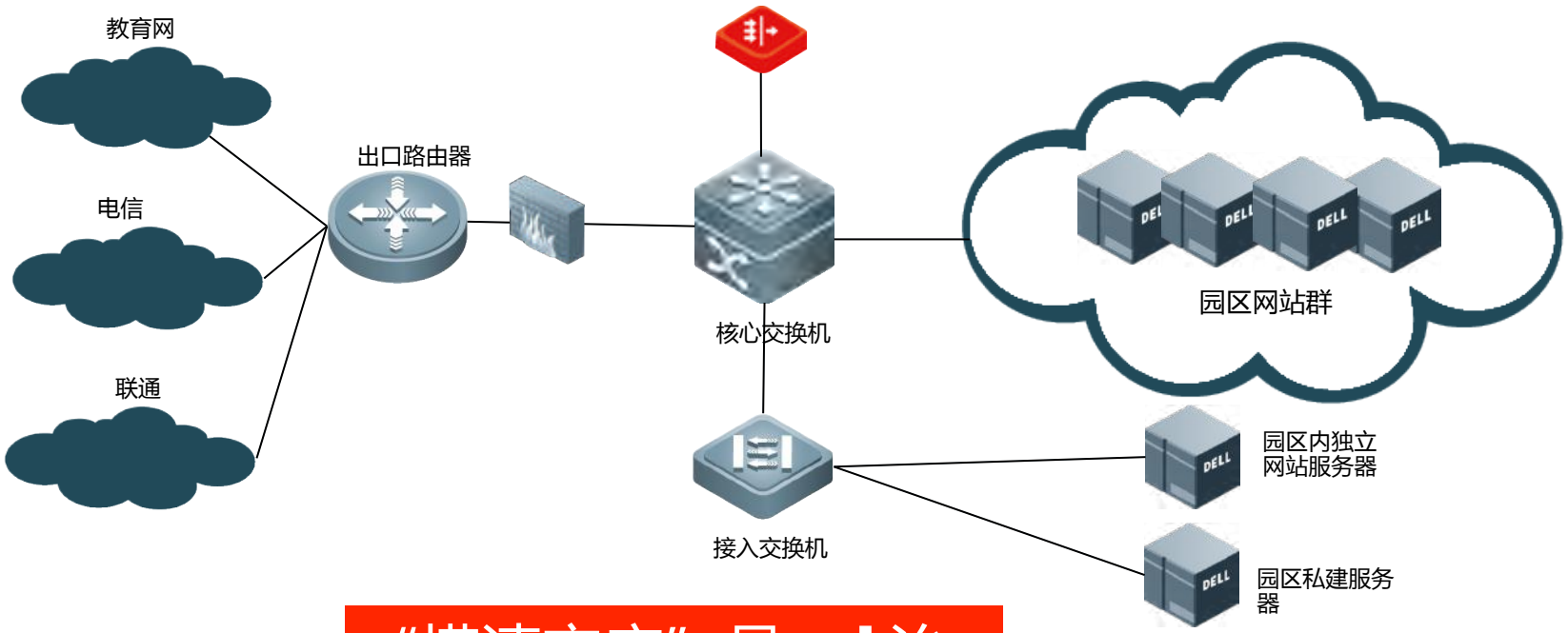
# 治理思路|Web系统全生命周期管理




可选与安全探针联动进行安全防护

网站安全不仅仅是WAF、防篡改！

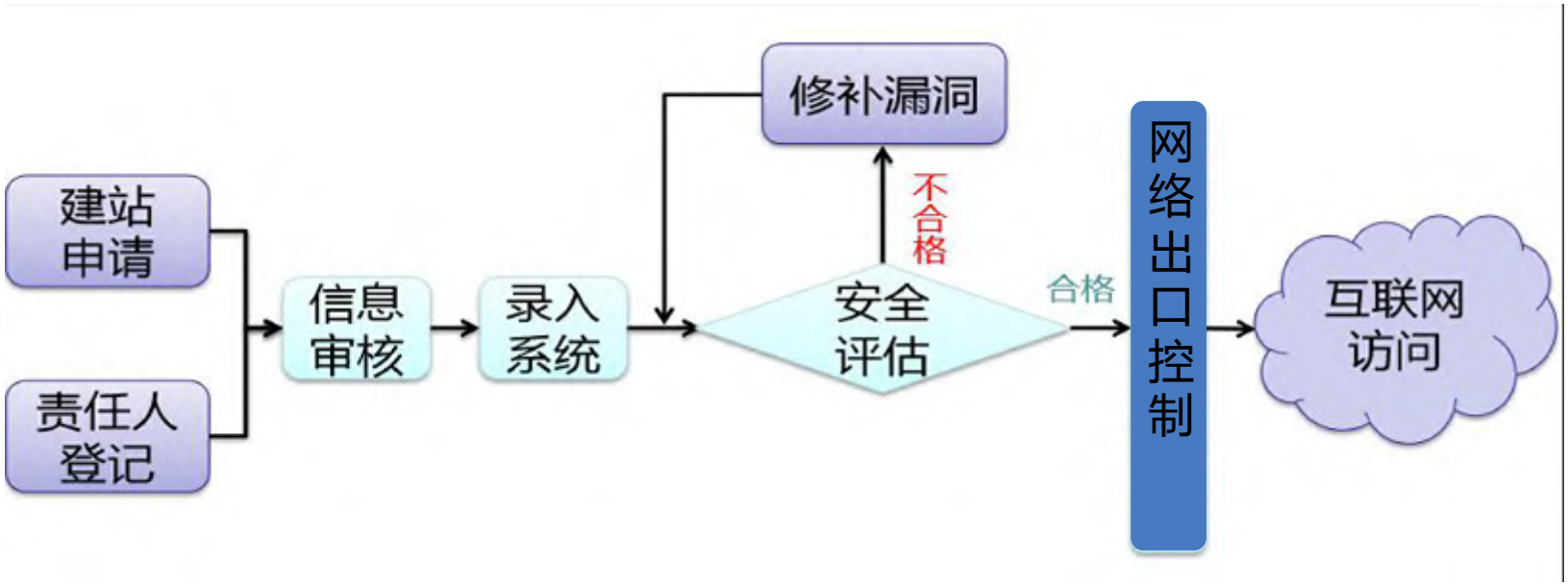
# 治理思路|自动学习所有在运站点




**“摸清家底”是web治理的第一步！**

通过技术手段分析镜像流量：
核心交换：学习所有内部和外部的**Web**资产（包含高端口）
出口交换机：学习所有由内到外提供服务的**HTTP**的域名以及网站名称（包含高端口）

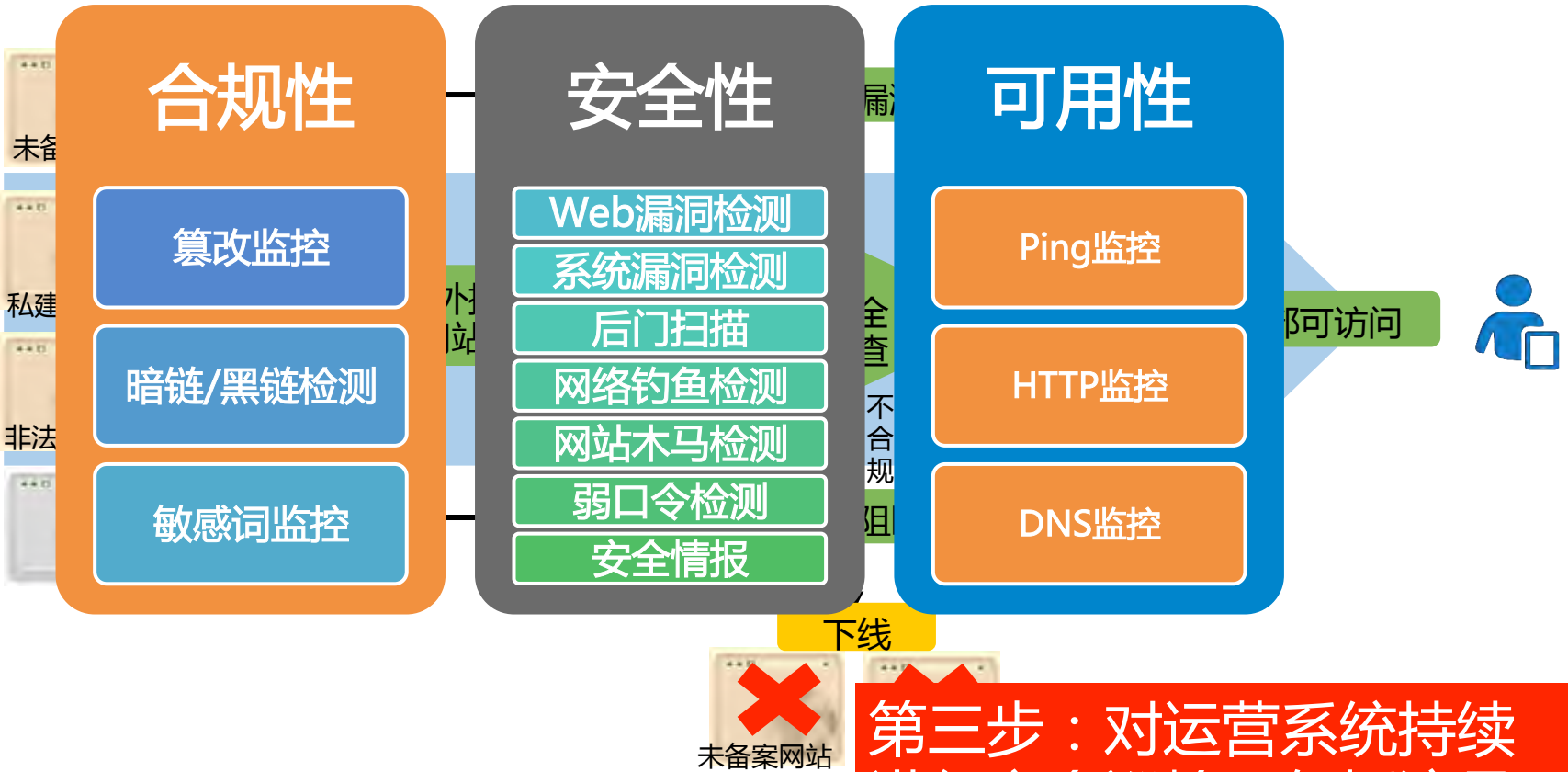
# 治理思路|网站安全准入机制-备案、评估




所有权确认 备案管理 安全检查

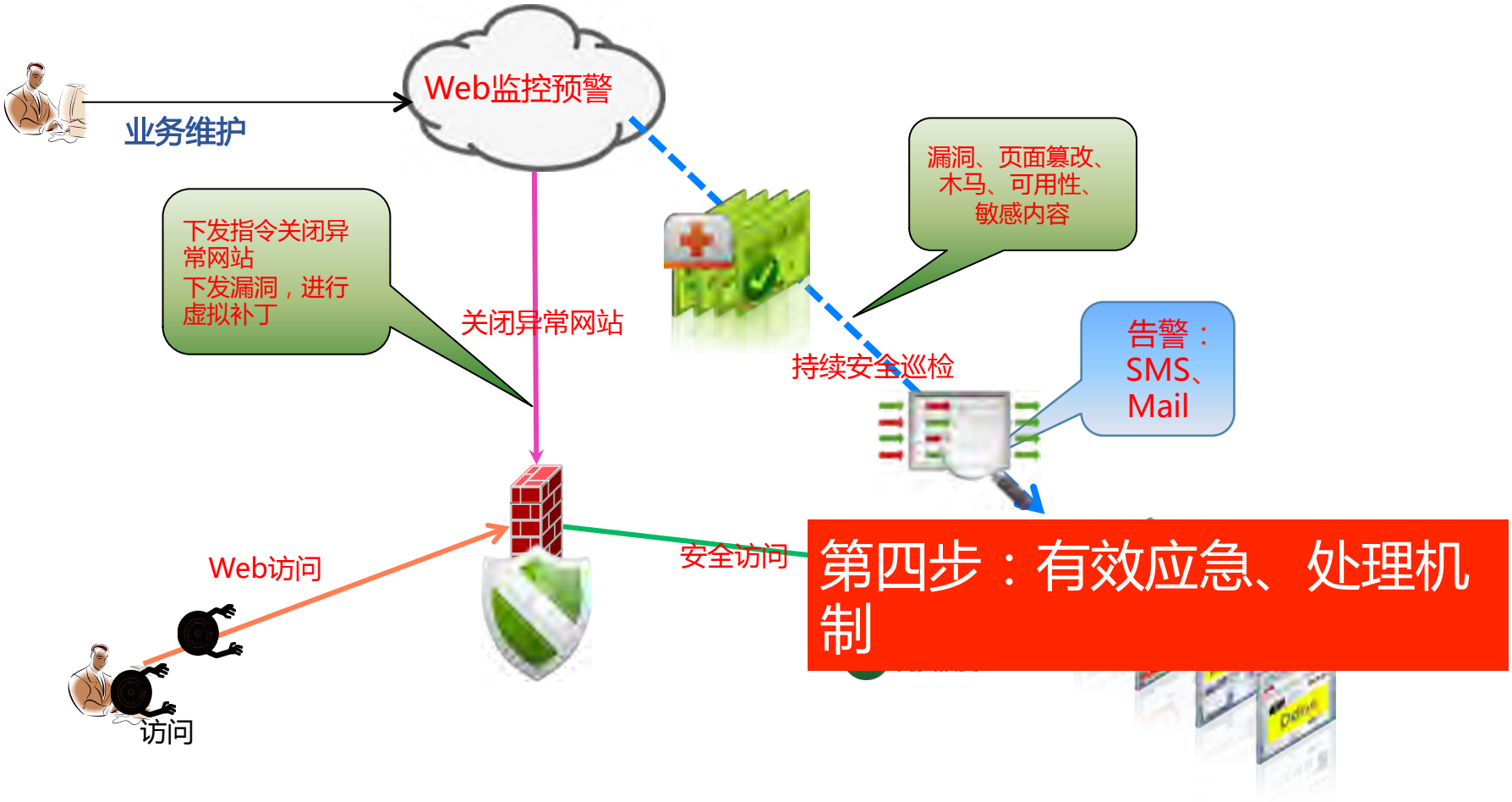
第二步：所有Web系统备案、评估后再允许对外服务

# 治理思路|网站运营监控机制

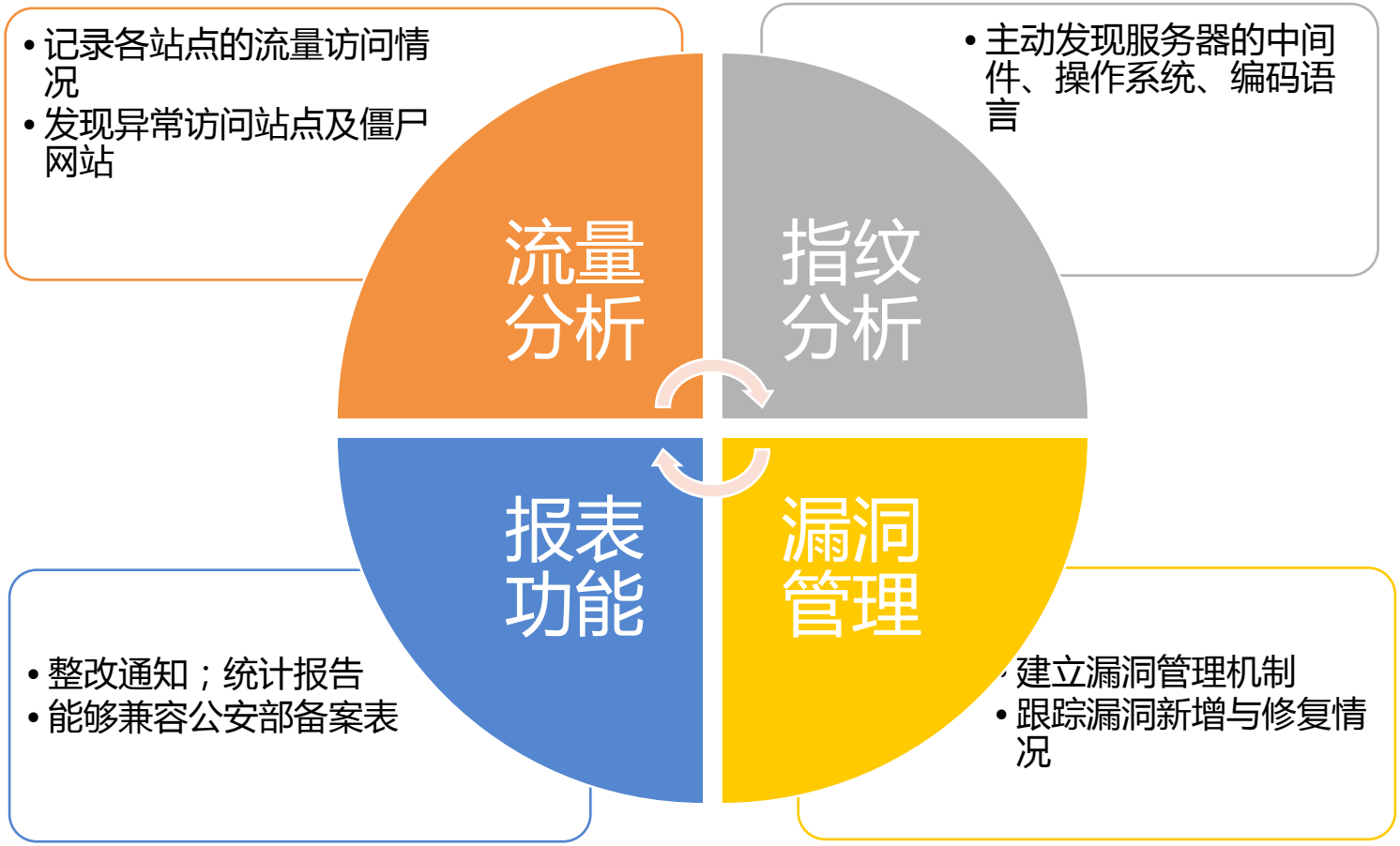



第三步：对运营系统持续进行安全巡检，包括流量被动发现

# 治理思路|一键断网+安全设备联动



# 治理思路|其他能力


• 记录各站点的流量访问情况
• 发现异常访问站点及僵尸网站
流量分析
• 主动发现服务器的中间件、操作系统、编码语言
指纹分析
报表功能
• 整改通知；统计报告
• 能够兼容公安部备案表
漏洞管理
• 建立漏洞管理机制
• 跟踪漏洞新增与修复情况

# 目录
content

# 方案效果|可知


资产总数
4898
漏洞总数
23814
访问流量
23461363
WebRAY
1315
流量统计
近一周
近一个月
流量排名：
资产漏洞TOP10
服务类型
风险信息
近一周事件统计
Web站点总体态势
漏洞
事件
访问量

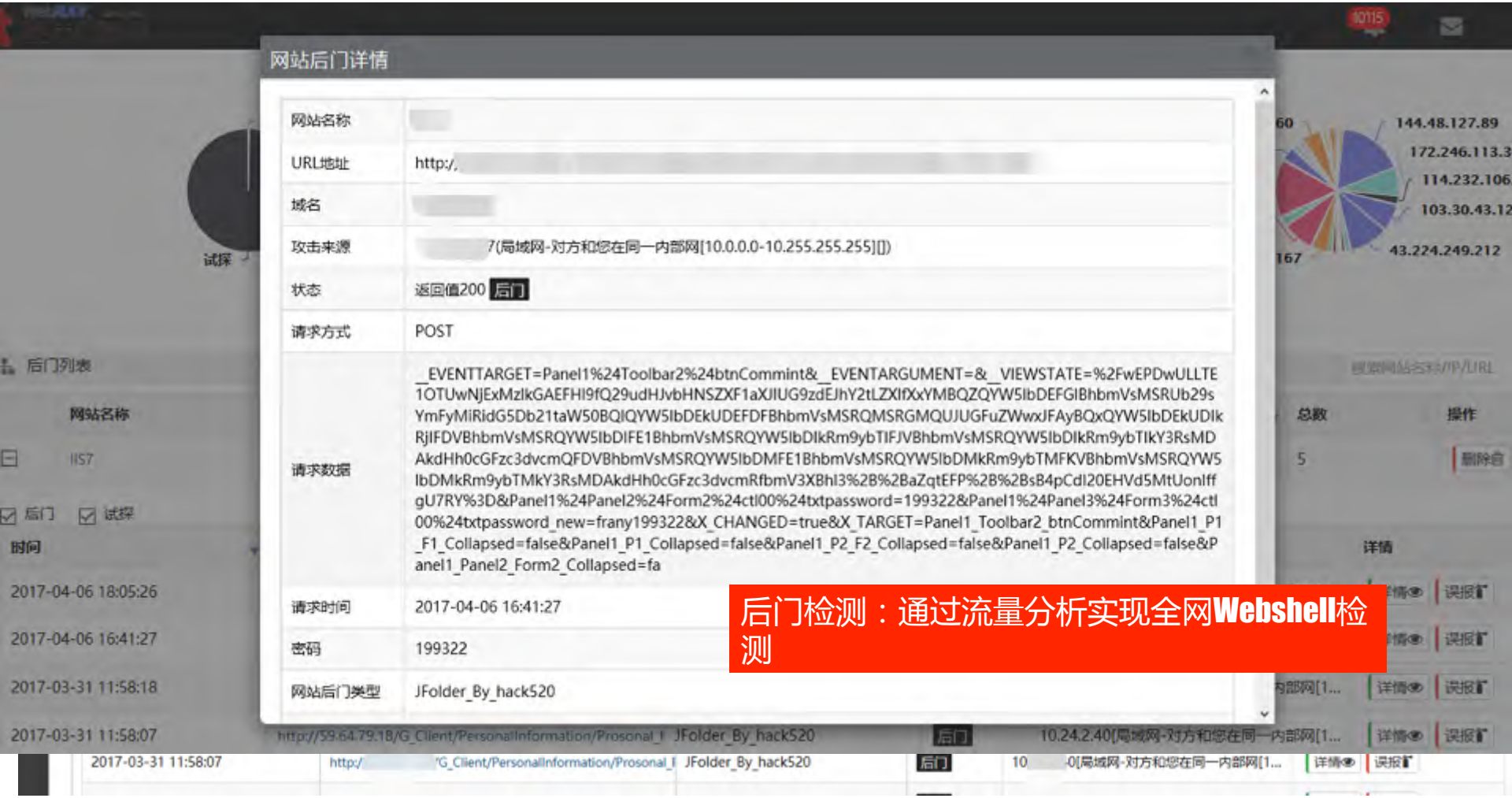
# 方案效果|可知


网站指纹
导出列表
中间件分布
nginx/1.4.1: 3 %
Microsoft-IIS/7.5: 3 %
App-webs/: 3 %
nginx/1.8.0: 4 %
Start HTTP-Server/1.0: 5 %
Apache-Coyote/1.1: 19.8 %
Switch: 17.8 %
Microsoft-IIS/8.0: 8.9 %
nginx/1.10.2: 6.9 %
中间件Top10
20
10
0
操作系统分布
Server 2012 Standard: 14.3 %
2 R2 Datacenter: 14.3 %
vs Server 2008 R2: 14.3 %
Microsoft Windows Serv
Linux Kernel 3.10 Linux Kernel 3.
操作系统Top10
3
2
1
0
网站名称
URL
IP
中间件
操作系统
语言
编码
物理地址
ZK Web Server
WWW Server/1.1
ASP.NET
WMI V5
Switch
gb2312
UTF-8
指纹分析：主动发现服务器的中间件、操作系统、编码语言

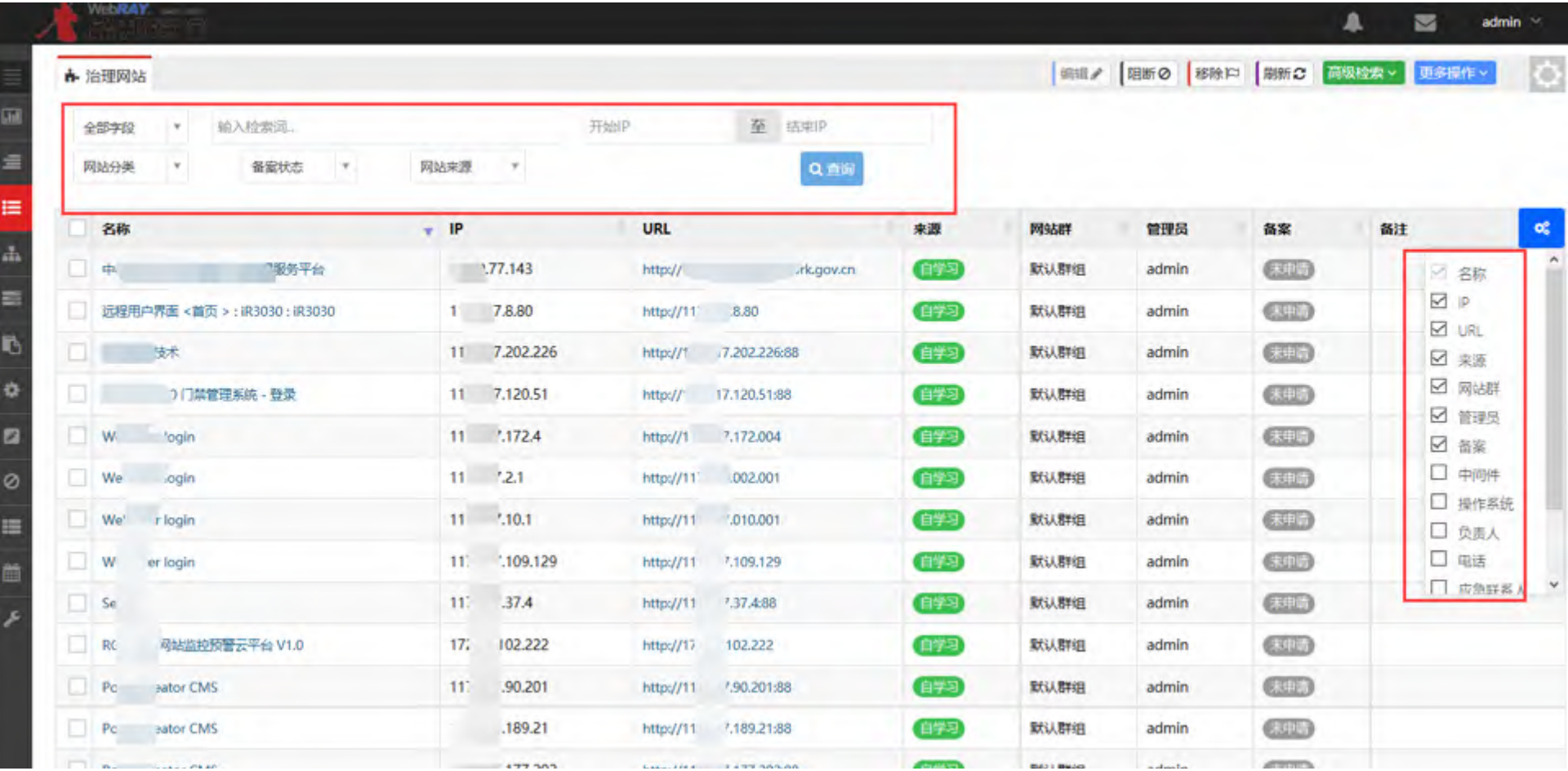
# 方案效果|可感


流量分析
流量统计
今天
昨天
近一周
近一月
开始时间
至
结束时间
网站名称
所属组织
URL
访问流量
操作
默认群组
测试网站
网站详情
26110
25199
3409
2825
1850
596
362
176
169
流量走势图
日统计
周统计
月统计
总访问流量
访问流量日统计
3M
2M
1M
0M
12-30
01-01
01-03
01-05
01-07
01-09
01-11
昨天
60981
0
6880246
近一月
7759034
流量分析：记录网站访问情况，发现异常流量及僵尸网站

# 方案效果|可感


网站后门详情
网站名称
URL地址
http:/
域名
攻击来源
7(局域网-对方和您在同一内部网[10.0.0.0-10.255.255.255][])
状态
返回值200 后门
请求方式
POST
请求数据
_EVENTTARGET=Panel1%24Toolbar2%24btnCommint&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTE1OTUwNjExMzIkGAEFHI9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXIfXxYMBQZQYW5lbDEFGIBhbmVsMSRUb29sYmFyMiRidG5Db21taW50BQlQYW5lbDEkUDEFDFBhbmVsMSRQMSRGMQUJUGFuZWwxJFAyBQxQYW5lbDEkUDIkRjIFDVBhbmVsMSRQYW5lbDIFE1BhbmVsMSRQYW5lbDIkRm9ybTIFJVBhbmVsMSRQYW5lbDIkRm9ybTIkY3RsMDAkdHh0cGFzc3dvcmQFDVBhbmVsMSRQYW5lbDMFE1BhbmVsMSRQYW5lbDMkRm9ybTMFKVBhbmVsMSRQYW5lbDMkRm9ybTMkY3RsMDAkdHh0cGFzc3dvcmRfbmV3XBhI3%2B%2BaZqtEFP%2B%2BsB4pCdI20EHVd5MtUonIffgU7RY%3D&Panel1%24Panel2%24Form2%24ctl00%24txtpassword=199322&Panel1%24Panel3%24Form3%24ctl00%24txtpassword_new=frany199322&X_CHANGED=true&X_TARGET=Panel1_Toolbar2_btnCommint&Panel1_P1_F1_Collapsed=false&Panel1_P1_Collapsed=false&Panel1_P2_F2_Collapsed=false&Panel1_P2_Collapsed=false&Panel1_Panel2_Form2_Collapsed=fa
请求时间
2017-04-06 16:41:27
密码
199322
网站后门类型
JFolder_By_hack520
后门检测：通过流量分析实现全网Webshell检测
后门列表
网站名称
时间
2017-04-06 18:05:26
2017-04-06 16:41:27
2017-03-31 11:58:18
2017-03-31 11:58:07
JFolder_By_hack520
144.48.127.89
172.246.113.3
114.232.106
103.30.43.12
43.224.249.212

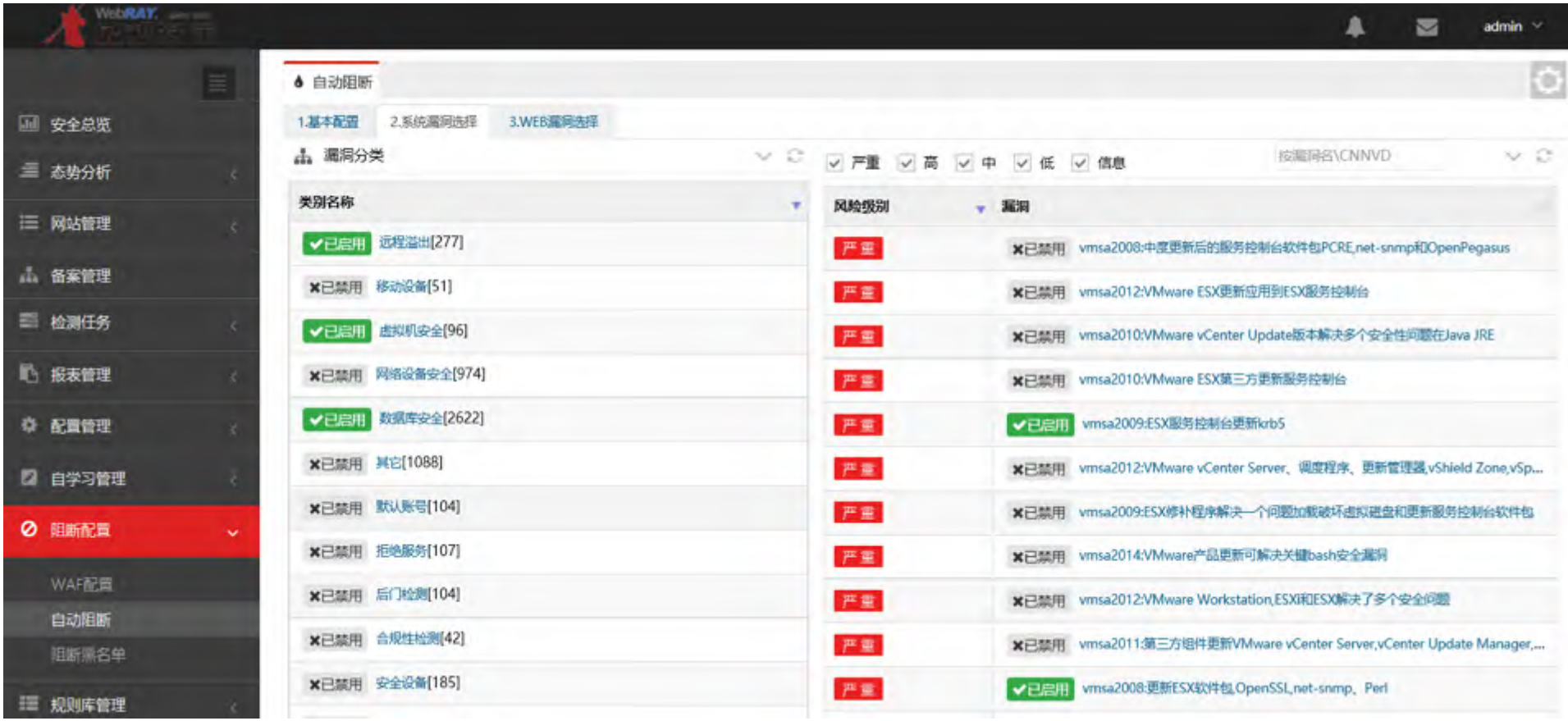
# 方案效果|可查


admin
治理网站
编辑
阻断
移除
刷新
高级检索
更多操作
全部字段
输入检索词...
开始IP
至
结束IP
网站分类
备案状态
网站来源
查询
名称
IP
URL
来源
网站群
管理员
备案
备注
名称
IP
URL
来源
网站群
管理员
备案
中间件
操作系统
负责人
电话
自学习
默认群组
admin
未申请

# 方案效果|可查


安全态势
风险总览
网站群分析
指纹分析
漏洞分析
事件分析
流量分析
配置管理
备案管理
报表管理
日志分析
库管理
漏洞分析
对比分析
严重
高
中
低
信息
刷新
风险级别
漏洞名称
漏洞分类
漏洞类型
出现总数
操作
严重 SNMP代理默认社区名称 SNMP安全 系统漏洞 4 漏洞详情
严重 OpenSSL<0.9e/0.9B3多个远程安全漏洞 远程溢出 系统漏洞 9 漏洞详情
严重 Microsoft Windows DCOM RPC接口长主机名远程缓冲区溢出漏 Windows安全 系统漏洞 1 漏洞详情
严重 MS03-039:微软RPC接口缓冲区溢出(824146)（未受信任的检查） Windows安全 系统漏洞 1 漏洞详情
严重 MS04-007:ASN.1漏洞可能允许执行代码(828028)（不受信任的 Windows安全 系统漏洞 1 漏洞详情
严重 Windows Local Security Authority Service远程缓冲区溢出漏洞 Windows安全 系统漏洞 1 漏洞详情
高风险 Struts2远程代码执行S2-045 Struts2远程代码执行S2-045 WEB漏洞 23 漏洞详情
高风险 Struts2远程代码执行S2-032 Struts2远程代码执行S2-032 WEB漏洞 5 漏洞详情
高风险 MySQL Null Root Password Weak默认配置漏洞 数据库安全 系统漏洞 6 漏洞详情
高风险 Microsoft SQL服务器sa帐户默认密码为空
漏洞管理：定期自动检测，及时发现高危漏洞

# 方案效果|可控


admin
安全总览
态势分析
网站管理
备案管理
检测任务
报表管理
配置管理
自学习管理
阻断配置
WAF配置
自动阻断
阻断黑名单
规则库管理
自动阻断
1.基本配置
2.系统漏洞选择
3.WEB漏洞选择
漏洞分类
严重
高
中
低
信息
类别名称
风险级别
漏洞
已启用 远程溢出[277]
已禁用 移动设备[51]
已启用 虚拟机安全[96]
已禁用 网络设备安全[974]
已启用 数据库安全[2622]
已禁用 其它[1088]
已禁用 默认账号[104]
已禁用 拒绝服务[107]
已禁用 后门检测[104]
已禁用 合规性检测[42]
已禁用 安全设备[185]
严重 已禁用 vmsa2008:中度更新后的服务控制台软件包PCRE,net-snmp和OpenPegasus
严重 已禁用 vmsa2012:VMware ESX更新应用到ESX服务控制台
严重 已禁用 vmsa2010:VMware vCenter Update版本解决多个安全性问题在Java JRE
严重 已禁用 vmsa2010:VMware ESX第三方更新服务控制台
严重 已启用 vmsa2009:ESX服务控制台更新krb5
严重 已禁用 vmsa2012:VMware vCenter Server、调度程序、更新管理器,vShield Zone,vSp...
严重 已禁用 vmsa2009:ESX修补程序解决一个问题加载破坏虚拟磁盘和更新服务控制台软件包
严重 已禁用 vmsa2014:VMware产品更新可解决关键bash安全漏洞
严重 已禁用 vmsa2012:VMware Workstation,ESXI和ESX解决了多个安全问题
严重 已禁用 vmsa2011:第三方组件更新VMware vCenter Server,vCenter Update Manager,...
严重 已启用 vmsa2008:更新ESX软件包,OpenSSL,net-snmp、Perl

# 目录
content


WebRAY 「股票代码：836731」
盛邦安全
网站安全治理平台 V3.4
帐号
密码
验证码
YQXK
Login


WOTA
51CTO
Thank you !