

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



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

可知 可感 可查 可控

打造新一代Web安全治理体系



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

治理思路

方案效果

关于我们

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

中央网信办 <1号文
> 2014.5.9

中央网信办、中编办
<69号文件>
2014.11.24

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

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

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

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

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》

技术要求

关键信息基础设施包括

网站类

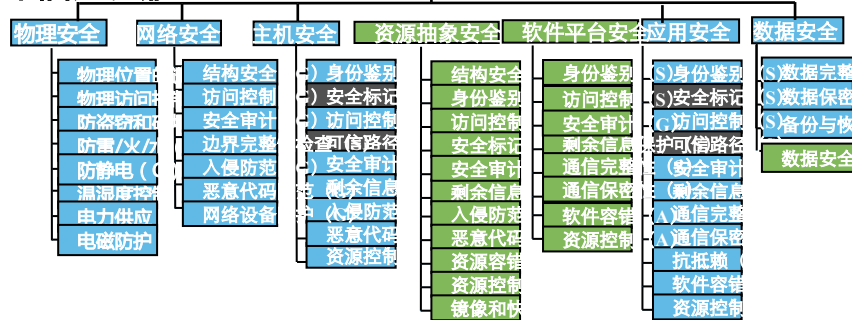
如党政机关网站、企事业单位网站、新闻网站等；

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

背景介绍

治理思路

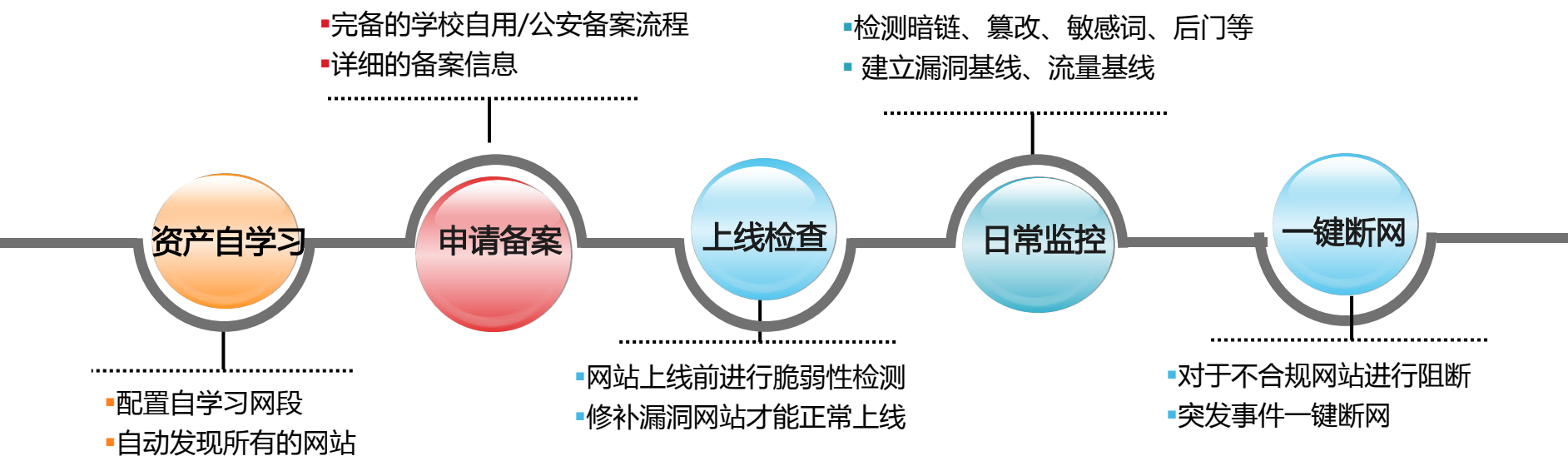
方案效果

关于我们

“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

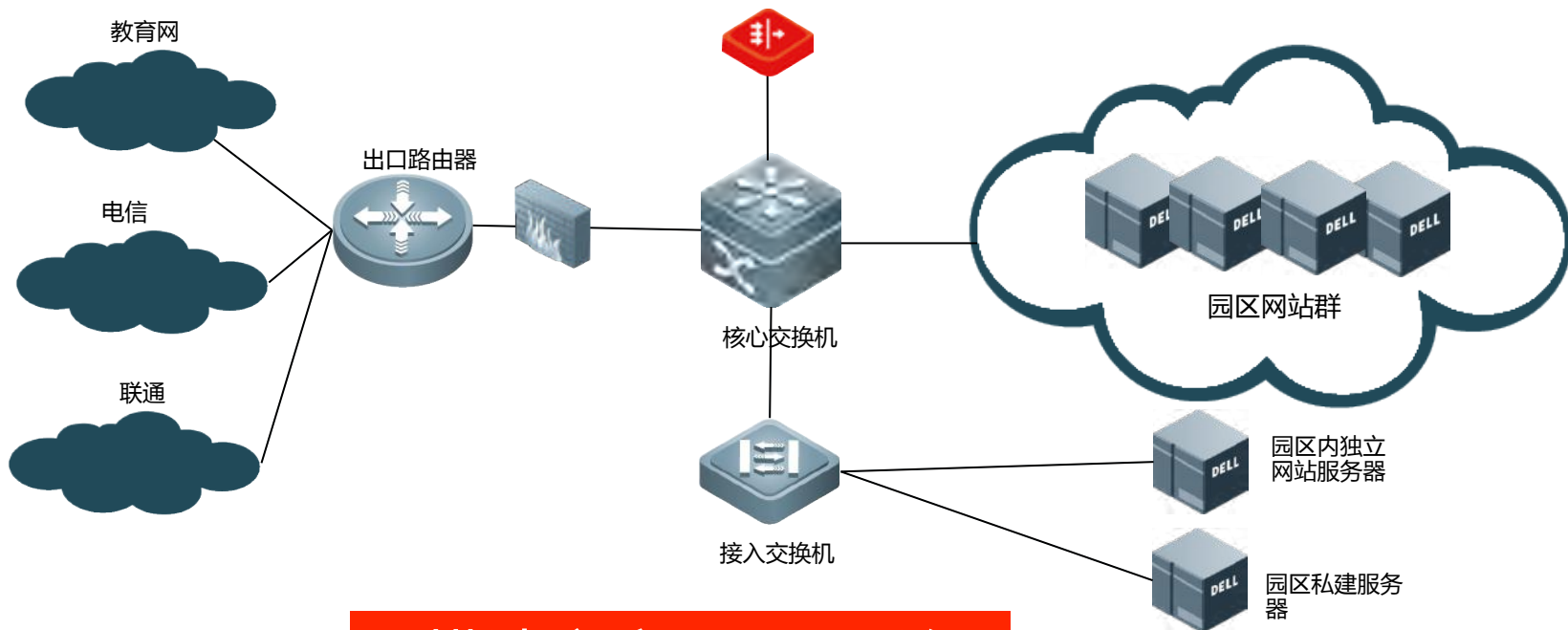
治理思路|Web系统全生命周期管理



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



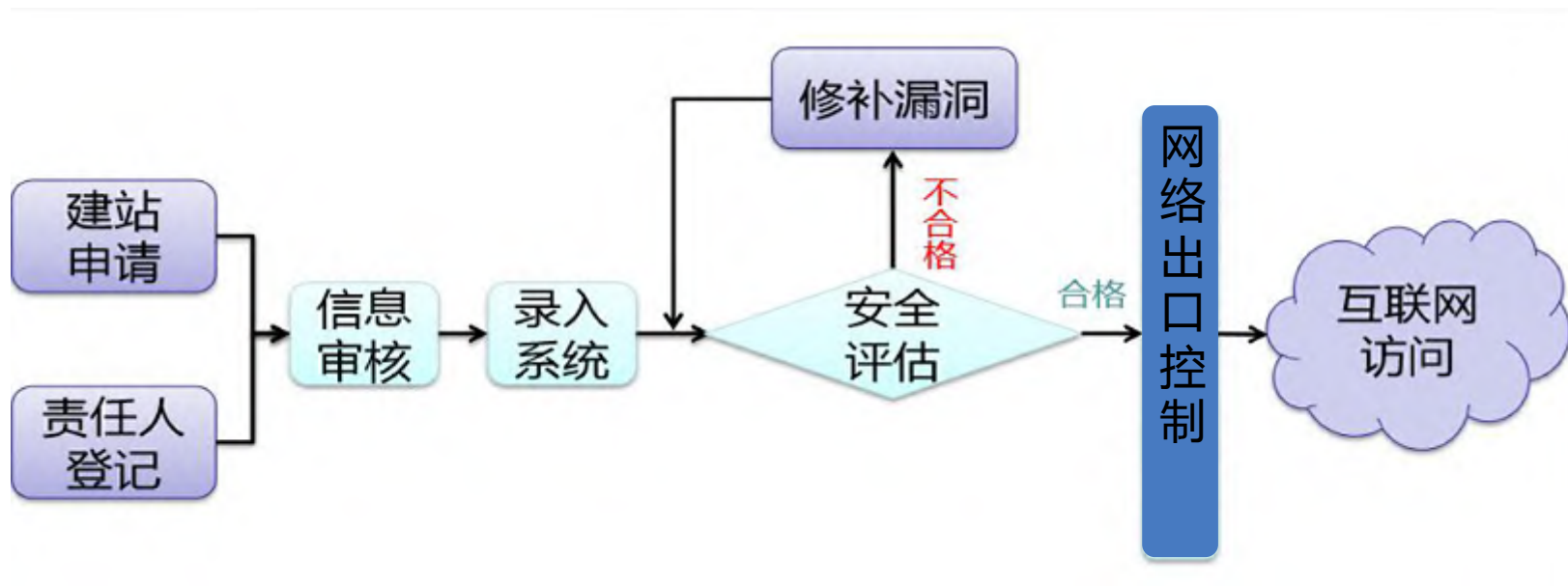
“摸清家底” 是web治理的第一步！

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



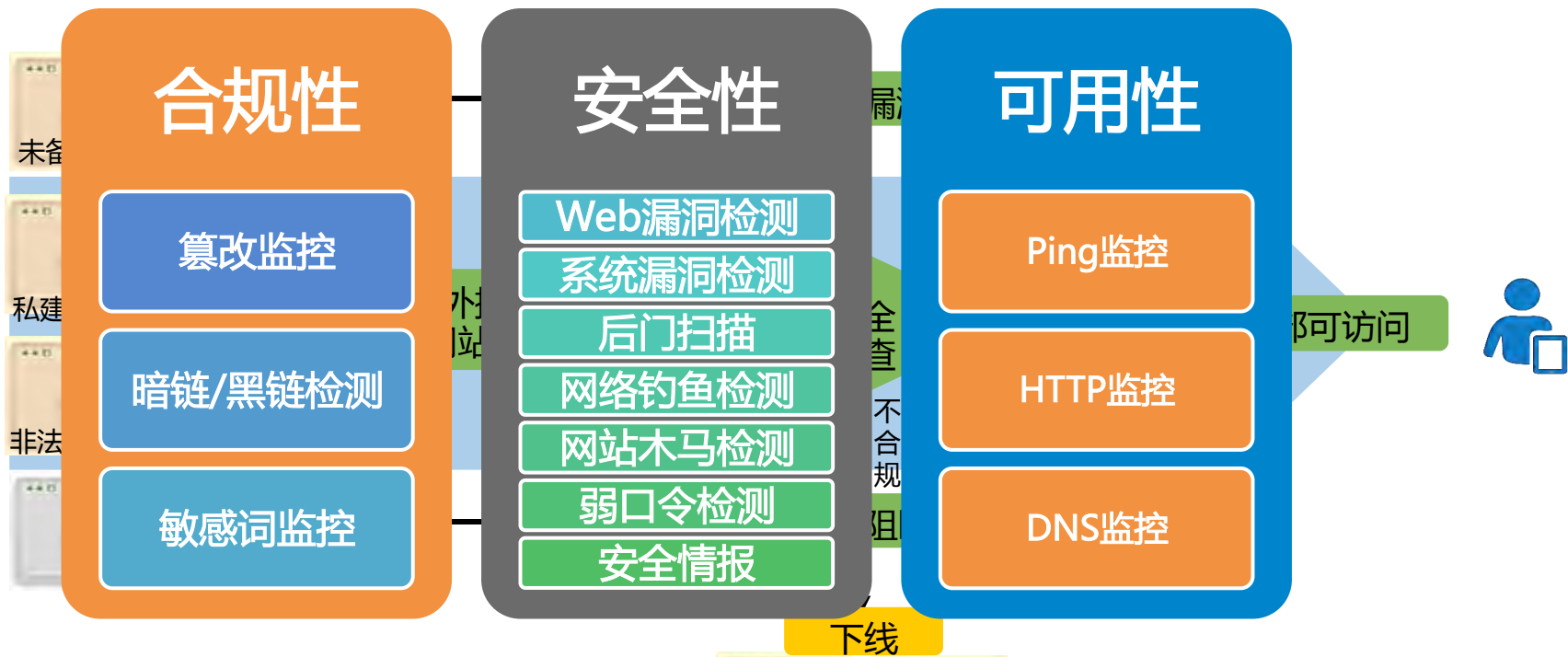
所有权确认

备案管理

安全检查

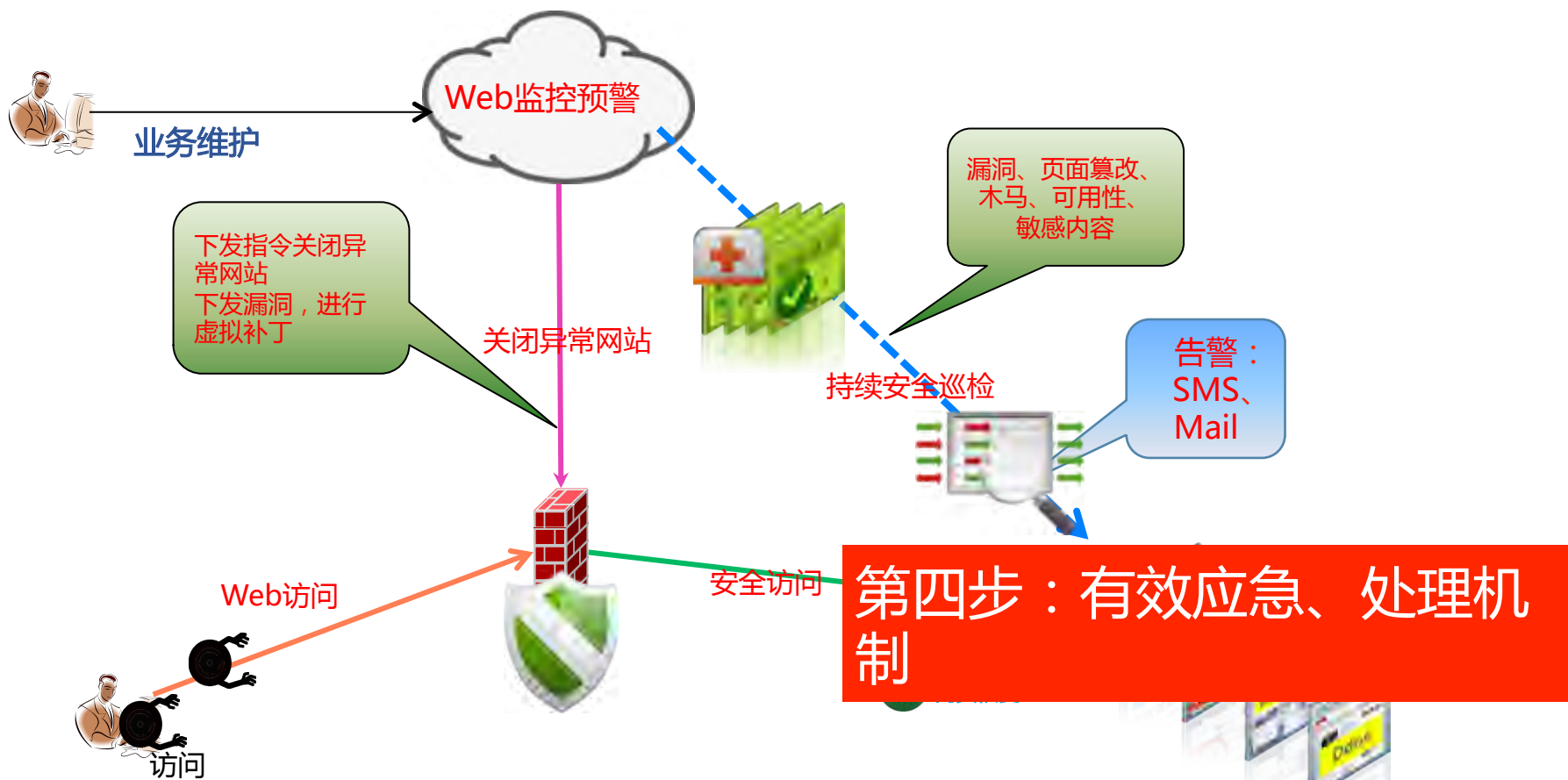
第二步：所有Web系统备案、评估后再允许对外服务

治理思路|网站运营监控机制

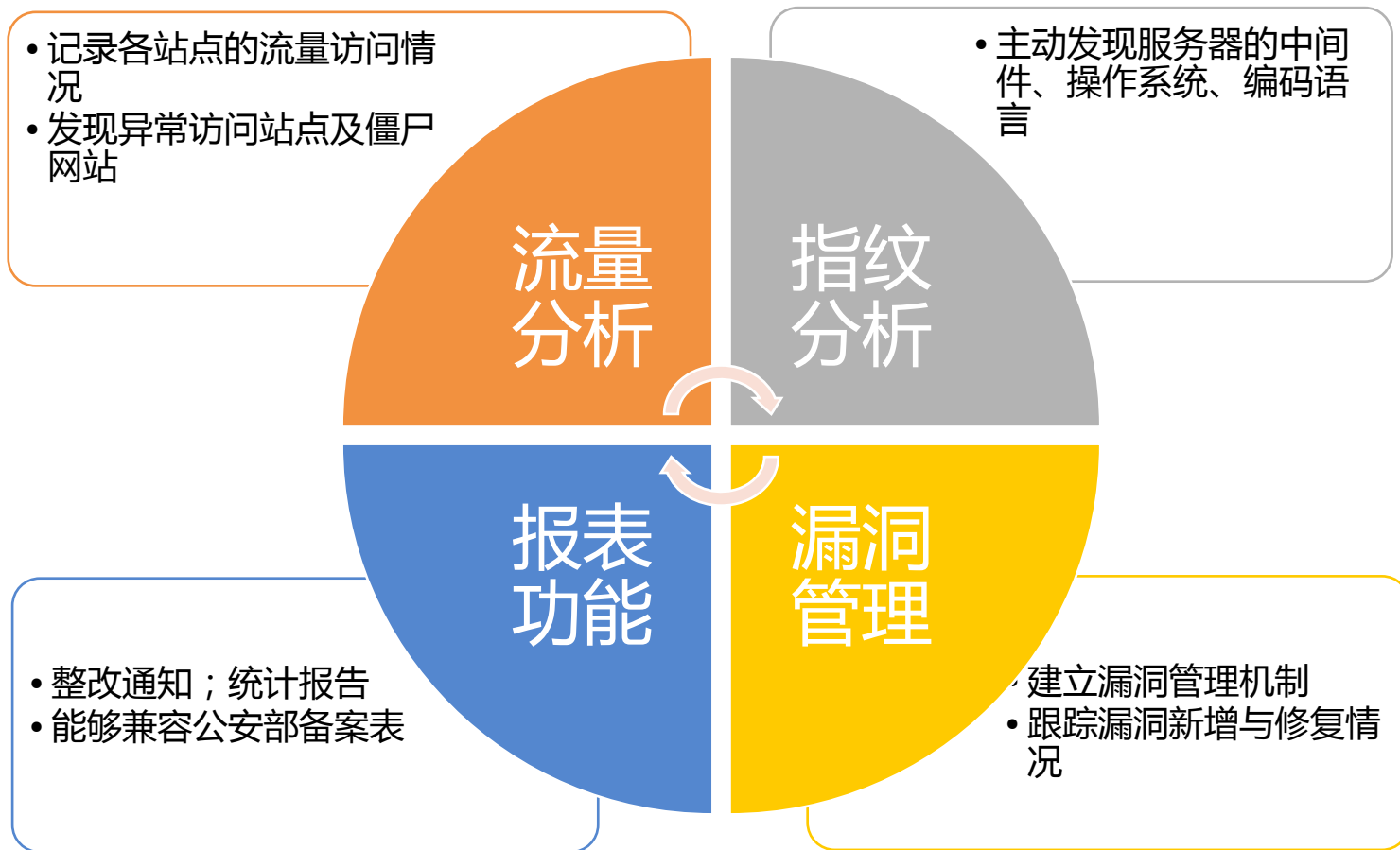


第三步：对运营系统持续进行安全巡检，包括流量被动发现

治理思路|一键断网+安全设备联动



治理思路|其他能力



目录

content

背景介绍

治理思路

方案效果

关于我们

方案效果|可知



方案效果|可知



方案效果|可感



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	返回码200 后门
请求方式	POST
请求数据	__EVENTTARGET=Panel1%24Toolbar2%24btnCommint&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTE1OTUwNjExMzlkGAEFH19fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2lLZXlfdXxYMBQZQYW5lbDEFGIbHbmVsMSRUB29sYmFyMIRidG5Db21taW50BQIQYW5ibDEkUDEFDFBhbmVsMSRQMSRGMQUJUGFuZWwxJFAyBQxQYW5ibDEkUDIkRjIFDVBhbmVsMSRQYW5ibDIFE1BhbmVsMSRQYW5ibDikRm9ybTIFJVBhbmVsMSRQYW5ibDikRm9ybTlKY3RsMDAkdHh0cGFzc3dvcmQFDVBhbmVsMSRQYW5ibDMFE1BhbmVsMSRQYW5ibDMkRm9ybTMFKVBhbmVsMSRQYW5lbDMkRm9ybTMkY3RsMDAkdHh0cGFzc3dvcmRfbmV3Xh3%2B%2BaZqtEFP%2B%2BsB4pCdi20EHVd5MtUonlffgU7RY%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

方案效果|可查

The screenshot displays a web management interface with a search bar and a table of website information. A red box highlights the search filters, and another red box highlights the column selection menu.

Search Filters:

- 全部字段 (All Fields)
- 网站分类 (Website Category)
- 输入检索词 (Enter search term)
- 开始IP (Start IP) 至 (To) 结束IP (End IP)
- 网站备案状态 (Website Registration Status)
- 网站来源 (Website Source)
- 查询 (Search)

Table Columns:

- 名称 (Name)
- IP
- URL
- 来源 (Source)
- 网站群 (Website Group)
- 管理员 (Administrator)
- 备案 (Registration)
- 备注 (Remarks)

Table Data:

名称	IP	URL	来源	网站群	管理员	备案	备注
中...服务平台	177.143	http://...rk.gov.cn	自学习	默认群组	admin	未申请	
远程用户界面 <首页> : iR3030 : iR3030	17.8.80	http://11...8.80	自学习	默认群组	admin	未申请	
...技术	117.202.226	http://1...7.202.226:88	自学习	默认群组	admin	未申请	
...门禁管理系统 - 登录	117.120.51	http://...17.120.51:88	自学习	默认群组	admin	未申请	
W...login	117.172.4	http://1...7.172.004	自学习	默认群组	admin	未申请	
We...login	117.2.1	http://11...002.001	自学习	默认群组	admin	未申请	
We'...r login	117.10.1	http://11...010.001	自学习	默认群组	admin	未申请	
W...er login	117.109.129	http://11...7.109.129	自学习	默认群组	admin	未申请	
Se...	117.37.4	http://11...7.37.4:88	自学习	默认群组	admin	未申请	
RC...网站监控预警云平台 V1.0	17102.222	http://17...102.222	自学习	默认群组	admin	未申请	
Pc...ator CMS	117.90.201	http://11...7.90.201:88	自学习	默认群组	admin	未申请	
Pc...ator CMS	117.189.21	http://11...7.189.21:88	自学习	默认群组	admin	未申请	

Column Selection Menu:

- 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
- 应急联系人

方案效果|可查

The screenshot displays the WOTA security dashboard interface. On the left, a navigation menu includes options like '安全态势', '风险总览', '网站群分析', '指纹分析', '漏洞分析' (highlighted), '事件分析', '流量分析', '配置管理', '备案管理', '报表管理', '日志分析', and '库管理'. The main content area shows a table of vulnerabilities under the '漏洞分析' tab. The table columns are '风险级别', '漏洞名称', '漏洞分类', '漏洞类型', '出现总数', and '操作'. A red box highlights the entry for 'Struts2远程代码执行S2-045', which is classified as '高风险' (High Risk) and has 23 occurrences. A red banner at the bottom right contains the text: '漏洞管理：定期自动检测，及时发现高危漏洞'.

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/0.9.8.3 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洞	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) (不受信任的检查)	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) (不受信任的检	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

The screenshot displays the WebRAY security management interface. On the left is a navigation sidebar with options like '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', and '规则库管理'. The '阻断配置' (Block Configuration) section is highlighted in red.

The main content area is titled '自动阻断' (Automatic Blocking) and includes three tabs: '1.基本配置' (Basic Configuration), '2.系统漏洞选择' (System Vulnerability Selection), and '3.WEB漏洞选择' (WEB Vulnerability Selection). The '3.WEB漏洞选择' tab is active.

Below the tabs, there are filters for '漏洞分类' (Vulnerability Classification) and '风险级别' (Risk Level). The '风险级别' filter is set to '严重' (Severe), '高' (High), '中' (Medium), and '低' (Low), with '信息' (Information) also checked. The search criteria is set to '按漏洞名\CNNVD'.

The main table displays a list of vulnerabilities with columns for '类别名称' (Category Name), '风险级别' (Risk Level), and '漏洞' (Vulnerability). The '类别名称' column shows various categories like '远程溢出[277]', '移动设备[51]', '虚拟机安全[96]', '网络设备安全[974]', '数据库安全[2622]', '其它[1088]', '默认账号[104]', '拒绝服务[107]', '后门检测[104]', '合规性检测[42]', and '安全设备[185]'. The '风险级别' column shows '严重' (Severe) for most entries. The '漏洞' column shows the specific vulnerability details, including the CVE ID and the affected software.

类别名称	风险级别	漏洞
<input checked="" type="checkbox"/> 已启用 远程溢出[277]	严重	<input checked="" type="checkbox"/> 已禁用 vmsa2008:中意更新后的服务控制台软件包PCRE_net-snmp和OpenPegasus
<input checked="" type="checkbox"/> 已禁用 移动设备[51]	严重	<input checked="" type="checkbox"/> 已禁用 vmsa2012:VMware ESX更新应用到ESX服务控制台
<input checked="" type="checkbox"/> 已启用 虚拟机安全[96]	严重	<input checked="" type="checkbox"/> 已禁用 vmsa2010:VMware vCenter Update版本解决多个安全性问题在Java JRE
<input checked="" type="checkbox"/> 已禁用 网络设备安全[974]	严重	<input checked="" type="checkbox"/> 已禁用 vmsa2010:VMware ESX第三方更新服务控制台
<input checked="" type="checkbox"/> 已启用 数据库安全[2622]	严重	<input checked="" type="checkbox"/> 已禁用 vmsa2009:ESX服务控制台更新krb5
<input checked="" type="checkbox"/> 已禁用 其它[1088]	严重	<input checked="" type="checkbox"/> 已禁用 vmsa2012:VMware vCenter Server, 调度程序, 更新管理器,vShield Zone,vSp...
<input checked="" type="checkbox"/> 已禁用 默认账号[104]	严重	<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> 已禁用 拒绝服务[107]	严重	<input checked="" type="checkbox"/> 已禁用 vmsa2014:VMware产品更新可解决关键bash安全漏洞
<input checked="" type="checkbox"/> 已禁用 后门检测[104]	严重	<input checked="" type="checkbox"/> 已禁用 vmsa2012:VMware Workstation,ESXi和ESX解决了多个安全问题
<input checked="" type="checkbox"/> 已禁用 合规性检测[42]	严重	<input checked="" type="checkbox"/> 已禁用 vmsa2011:第三方组件更新VMware vCenter Server,vCenter Update Manager,...
<input checked="" type="checkbox"/> 已禁用 安全设备[185]	严重	<input checked="" type="checkbox"/> 已启用 vmsa2008:更新ESX软件包,OpenSSL_net-snmp, Perl

目录

content

背景介绍

治理思路

方案效果

关于我们



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 YOXX

Login

Thank you !