



GOPS 2016
Shanghai



全球运维大会

2016

重新定义运维

上海站

会议时间： 9月23日-9月24日

会议地点： 上海·雅悦新天地大酒店

主办单位：



指导单位：



互联网+下的云安全服务实践

侯奎宇 绿盟科技



NSFOCUS 网络安全态势感知平台 | 产品白皮书 | 2019年10月

安全运营 Operation

漏洞分析和挖掘
威胁感知
安全智能
云及虚拟化安全
合规性

绿盟科技研究院



累计发布安全紧急通告**131**个（截止到2015年12月）：

14年时间
增长668.7%




www.nsfocus.com
info@nsfocus.com
www.nsfocus.com

在4个重要市场，占有率第1
ADS/NIPS/RSAS/WAF



2012-2015连续4年入选Gartner魔力象限
2009-2014连续6年
入侵防护市场份额第一
2013年22.3%，2014年21.7%
2012年23.2%，2011年19.2%
2010年17.5%，2009年16.8%

2014年入选Gartner漏洞评估市场报告
2011-2014连续4年
安全性与漏洞管理软件市场份额第一
2013年24.5%，2014年25.1%
2012年23.6%，2011年25.4%
(数据来源IDC报告)

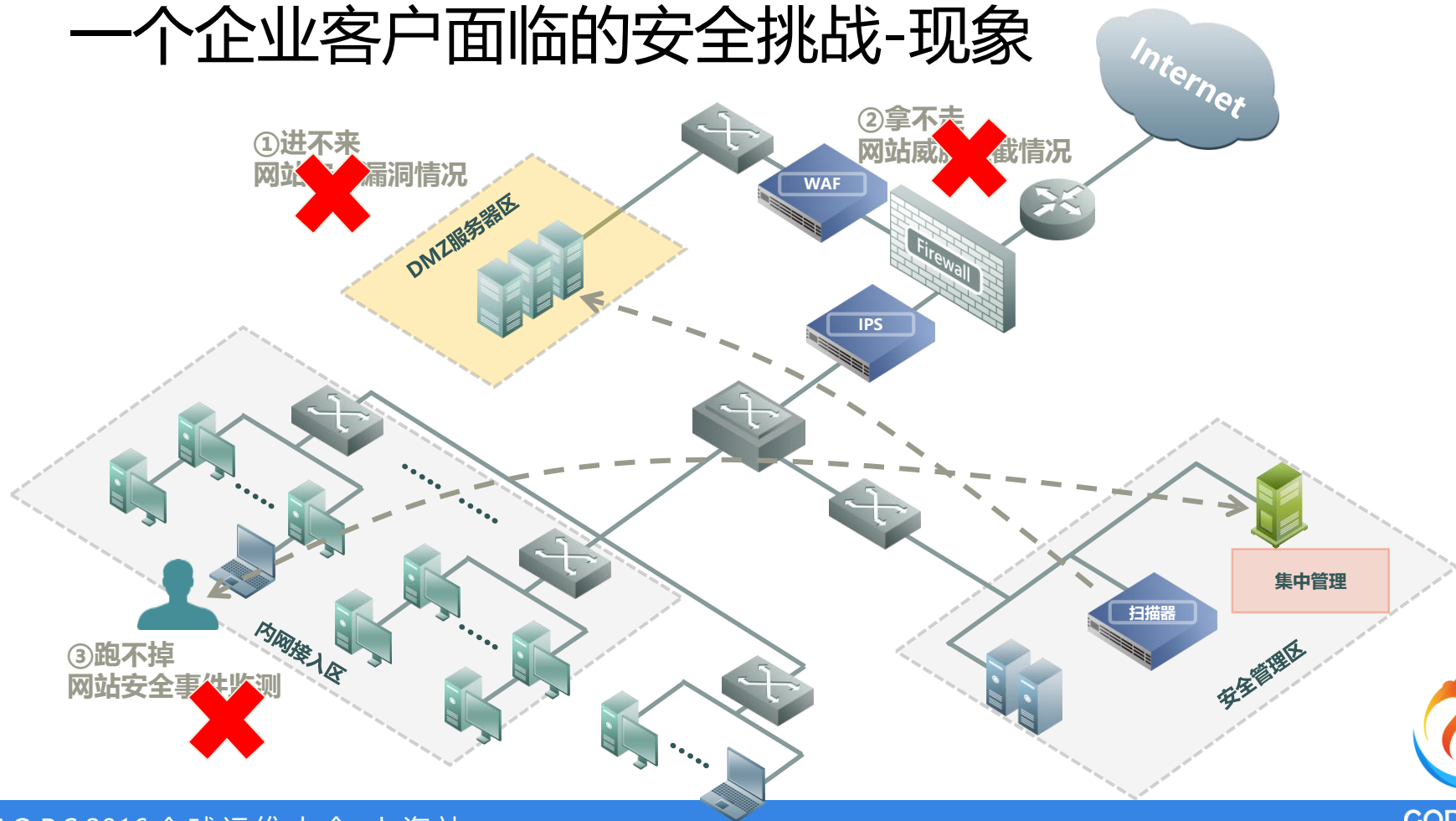
2014年入选Gartner魔力象限
2010-2014连续5年
亚太地区Web应用防火墙市场份额第一
2013年25.9%，2014年26.8%
2012年25.6%，2011年31.9%
2010年25.2%
(数据来自于Frost & Sullivan)

2014年10.1%，位居行业第一
(数据来自于Frost & Sullivan)

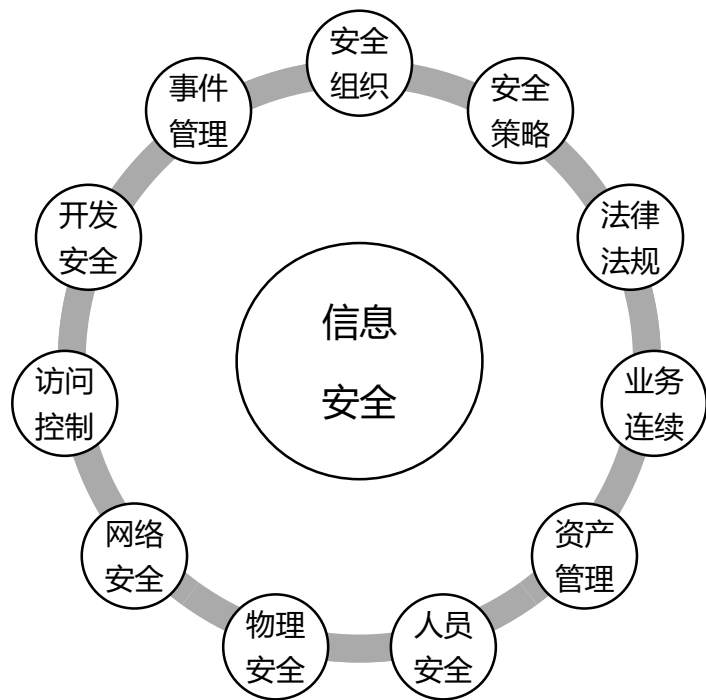
2010年约30%，位居行业第一
(数据来自于《计算机安全》)



一个企业客户面临的安全挑战-现象



一个企业客户面临的安全挑战

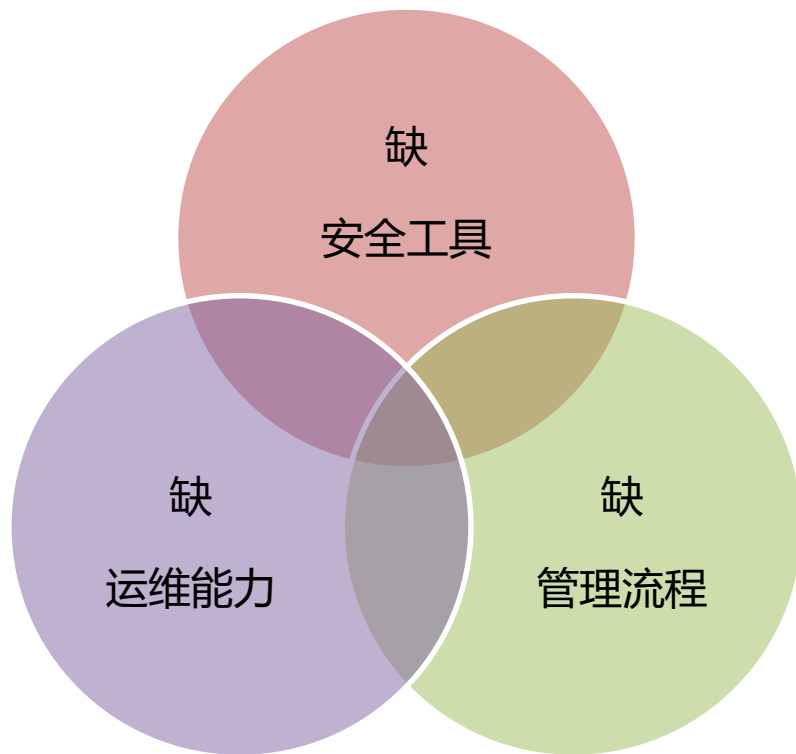


VS

- 采购过程太复杂
- 部署过程太繁琐
- 安全团队难组建
- 安全风险真假难辨
- 7×24小时难实现



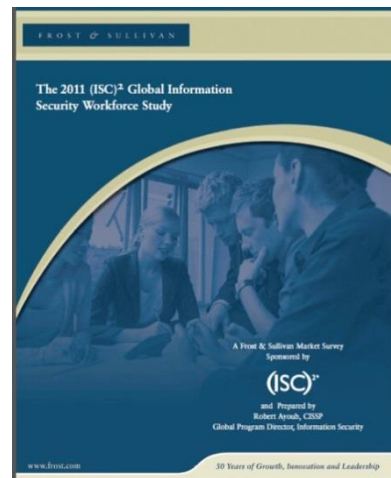
一个企业客户面临的安全挑战-原因



本质原因：安全人力资源的匮乏

- 全球性人荒 (Frost & Sullivan)

- 2010年,全球安全专业人才225万
- 到2015年,全球需要425万安全专业人才

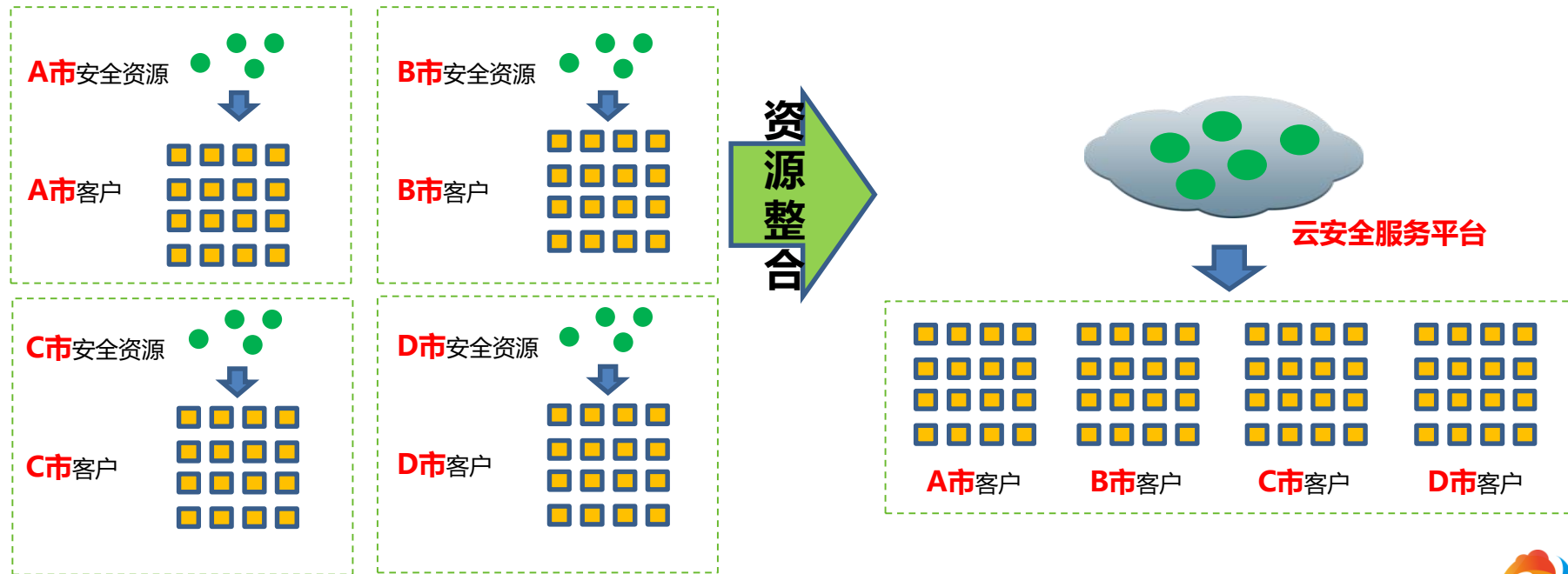


- 中国人荒更严重 (工信部中国电子信息产业发展研究院)

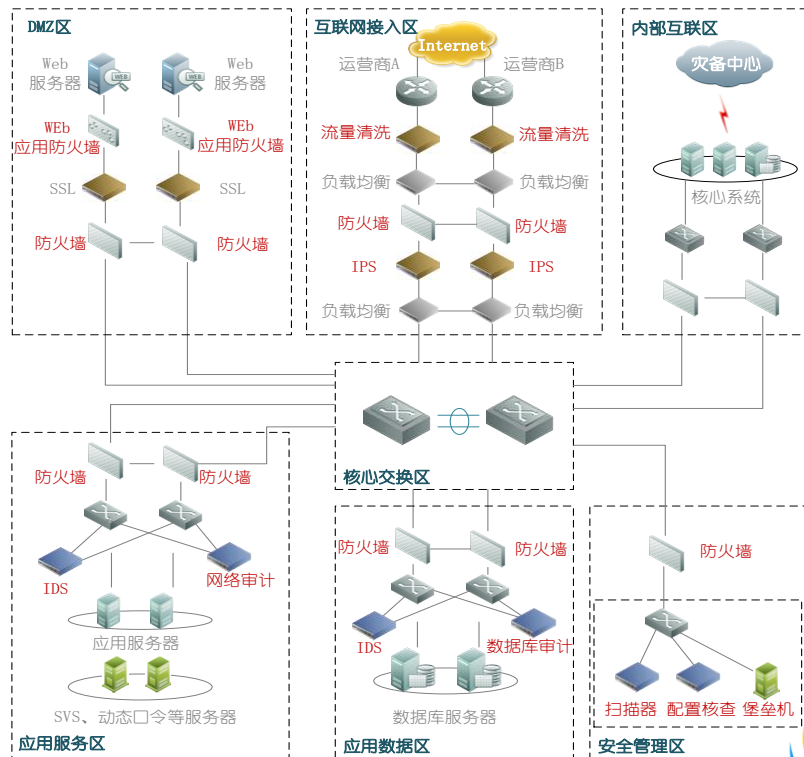
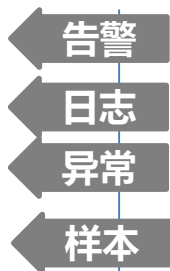
- 现有缺口50万
- 在缺口不增加的情况下需要17年补齐



到了集中解决的时候了，让云来帮助我们！



从云端发起



绿盟云 客户业务系统

怎么防止网站出事

三要素

- 事前：积极预防，防患于未然
- 事中：全天候监测，第一时间发现问题
- 事后：快速响应，迅速消除事件影响



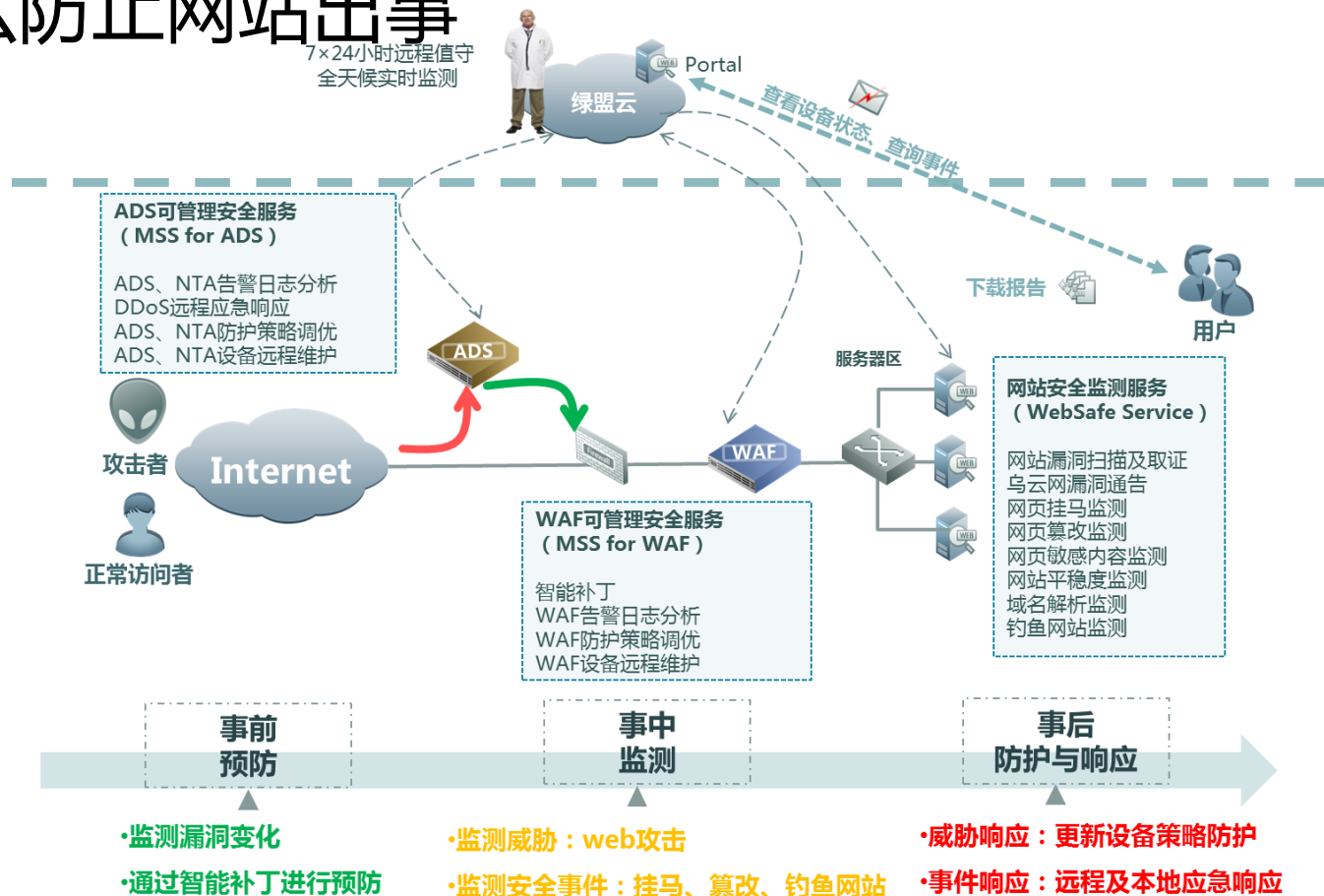
怎么防止网站出事

网站保障体系应具备的条件

- 卓越的安全设备或服务：能够及时准确发现漏洞和攻击
- 专业的安全专家团队：能够监测、处理、响应安全漏洞、安全威胁和安全事件
- 全天候监控、快速响应：能够7*24小时与攻击行为对抗
- 成熟可靠的安全运营流程制度：保障安全事件的闭环解决



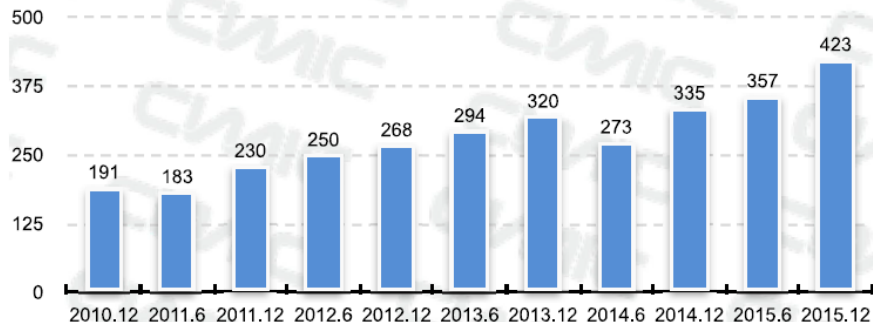
怎么防止网站出事



还有更多的客户

截至2015年12月，中国网站³数量为423万个，年增长26.3%。

中国网站数量



来源：

中国互联网络发展状况统计调查

2015.12

万个

截至2015年12月，中国网页⁴数量为2123亿个，年增长11.8%。

中国网页数及增长率



来源：

中国互联网络发展状况统计调查

2015.12

亿个

怎么为他们提供安全服务？

更低的客单价？更便捷的获取方式？



绿盟云

NSFOCUS CLOUD

cloud.nsfocus.com

基于
云计算
大数据

实现
智慧安全2.0

智能•敏捷•可运营

提供
云端安全服务

面向
企业客户



有什么解决方案

◀◀ 网站安全SaaS解决方案



谁动了我的网站？

- 黑客众多，攻击频繁，漏洞入侵，谁动了我的网站？
- 预算不足，编制不足，检测困难，谁保护我的网站？

◀◀ 移动安全SaaS解决方案



谁能帮我保护APP？

- APP研发结束，我该怎么筛查漏洞，发现后门？
- APP业务增长，我怎么确认帐号信息没泄露？怎么了解用户资金没被盗？

◀◀ 数据中心异常流量清洗解决方案



谁能帮我清洗流量？

- 业务托管在IDC，遭受异常流量攻击，谁来帮我识别DDoS？
- IP被封，业务中断，谁来告诉我该怎么办？

◀◀ 公有云安全SaaS解决方案

Coming
soon

我在云上安全么？

有什么服务

网站安全

大客户：
网站安全监测服务

中小客户：
网站安全SaaS解决方案
评估+监测+防护

安全检测

内网检测：
极光自助扫描

紧急漏洞：
紧急漏洞在线检测

移动安全

APP：
安全检测
安全加固
安全SDK
渠道监控

Server：
评估、监测、防护

威胁情报

威胁分析中心
威胁情报中心

邮件安全

反垃圾邮件服务

数据安全

亿赛通文档安全云服务

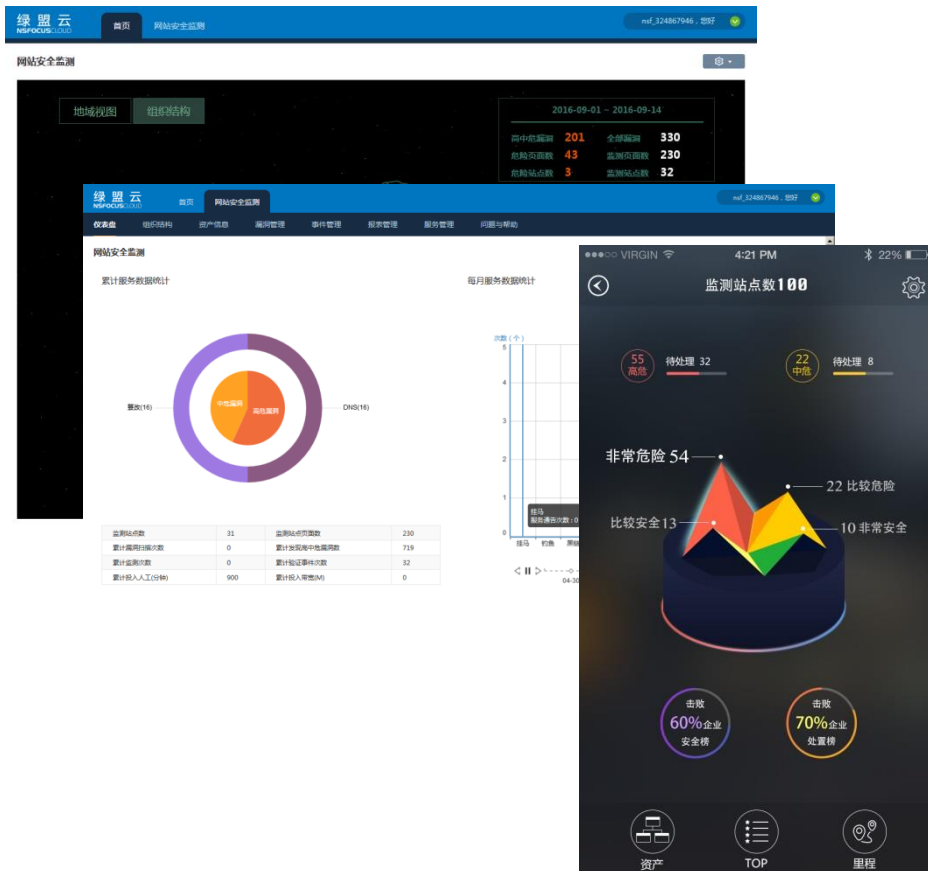
流量清洗

最终客户：
黑洞云清洗

数据中心合作运营：
综合抗D服务

众测/众修/云SRC

有什么服务—网站安全监测服务



面向**网站**，提供**7x24**小时

托管服务

- 漏洞生命周期管理
- 安全通告
- 网站平稳度监测
- 域名监测
- 网页挂马监测
- 网页篡改监测
- 敏感内容监测
- 远程钓鱼网站监测

有什么服务—极光自助扫描



轻松上手，**内网漏洞**扫描

• **无需**专业设备和软件

一次安装，随时使用

• 漏洞检查、**准确全面**

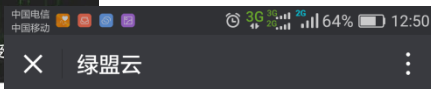
超过**15000**条漏洞库，专业团队支持，持续更新

主机、数据库、交换路由设备等安全漏洞，都能查；



有什么服务—紧急漏洞扫描

2014-07-03 DISCUZ 7系列SQL注入漏洞
2014-08-18 2014-06-06 IE VML UAF远程代码执行0day漏洞
DISCUZ EDITPOST 2014-08-12 WordPress xmlrpc.php DO
2016-07-07 文件SQL注入漏洞 2014-04-28 Apache Struts2 CVE-2014-0094修复补丁绕过漏洞
Spring Boot框架SPEL表达式注入漏洞
2016-08-23 Google Chrome V8引擎远程
2016-08-18 Zabbix高危SQL注入漏洞
2016-06-16 Apache Struts2 远程代码执行
2016-07-14 Apache Struts2 远程代码执行漏洞(S2-037) 2014-04-17 "心血"漏洞
PHP multipart/form-data 远程DOS漏洞 2015-05-16
2014-09-25 GNU Bash 环境变量远程命令执行漏洞(CVE-2014-6271)
2016-05-06 OpenSSL AES-NI CBC 中间人劫持漏洞
(CVE-2016-2107)



Google Chrome V8引擎远程代码漏洞

2016-08-23

Google Chrome V8引擎3.20至4.2版本中存在远程代码漏洞...

Zabbix SQL注入漏洞

2016-08-18

Zabbix是一个基于WEB界面的提供分布式系统监视视功能的企业级开源解决方案...

Struts2 开发模式远程代码执行

2016-07-14

Struts2 是第二代基于Model-View-Controller (MVC) 应用框架。Struts2是java...

Spring Boot 框架 SPEL 表达式漏洞

Zabbix SQL注入漏洞

发布日期 2016-08-18

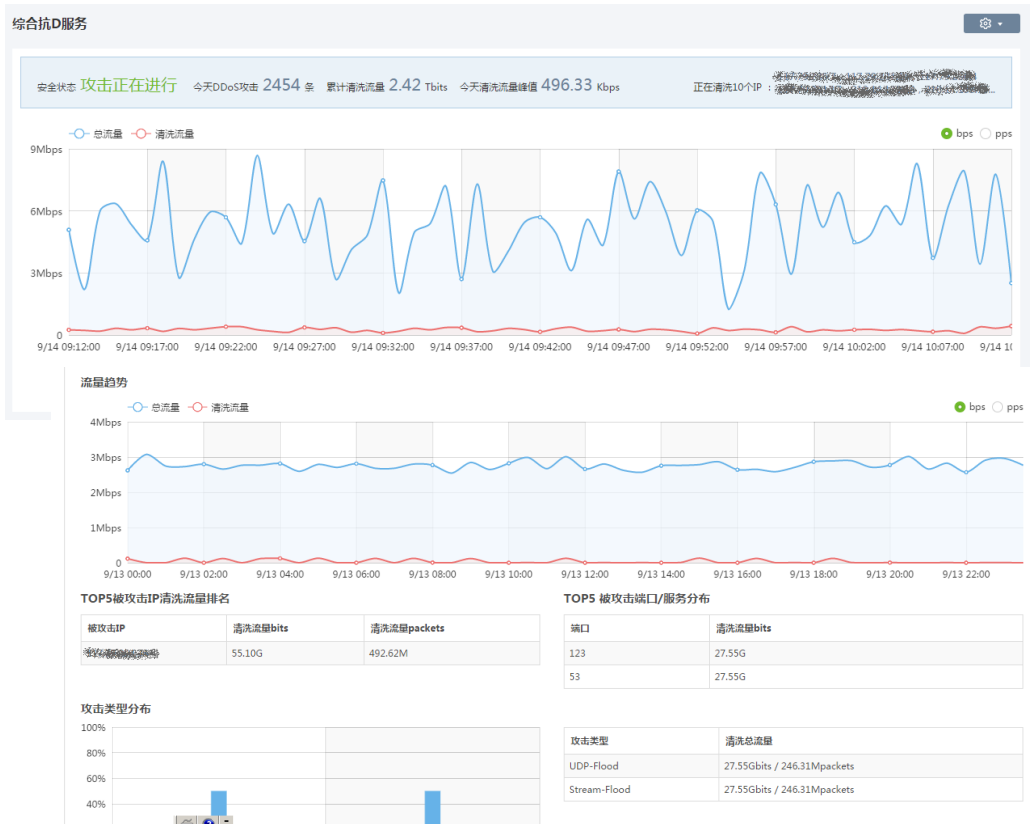
共有 528 个网站提交检测, 其中有 32 个网站存在漏洞

- 受影响的软件及系统
ZABBIX 2.2.13, 3.0.3版本
- 不受影响的软件及系统
ZABBIX 2.2.14, 3.0.4, 3.2.0版本
- 综述
2016年8月12日, 1n3通过邮件披露Zabbix软件jsrpc.php文件在处理profileIdx2参数时存在insert方式的SQL注入漏洞, 与官方通告的latest.php文件在处理toggle_ids参数时存在insert方式的SQL注入漏洞属于同一类型的漏洞, 只是攻击的位置不同。攻击者可以使用guest账户登录, 利用此漏洞直接获取服务器的操作系统权限。

输入检测目标, 如:
http://www.xxx.com/xxx?

立即检测

有什么服务—综合抗D服务



我们怎么做的？

情报



我们怎么做的？

NSFOCUS Information Technology Co. Ltd [CN] https://nti.nsfocus.com

NTI 绿盟威胁情报中心

我的探索 我的关注 我的帮助 点此登录

NTI 绿盟威胁情报中心

52.169.236.78
United States, Wilmington
2016-07-20 17:39:48
扫描

163.172.28.33
United Kingdom, Southend-on-Sea
2016-07-20 17:39:33
扫描

138.68.12.229
United States, Wilmington
2016-07-20 17:27:17
扫描

176.31.39.67
France, Roubaix
2016-07-20 16:54:39
扫描

©2015 绿盟科技 京公网安备110108002872 京ICP证

我们怎么做的？



基础数据能力

- 42全球亿资产侦测能力
- 亿级存活IP和站点指纹信息
- 地理定位系统
- 全网whois/ASN
- 全网Passive DNS数据



信誉情报

- 千万级恶意IP
- 万级C&C
- 亿级恶意域名
- 几十万恶意URL
- 百万级文件



漏洞情报

- 30万+漏洞
- IP及域名漏洞分析
- 0-day漏洞跟踪预警
- 漏洞相关poc和恶意样本跟踪



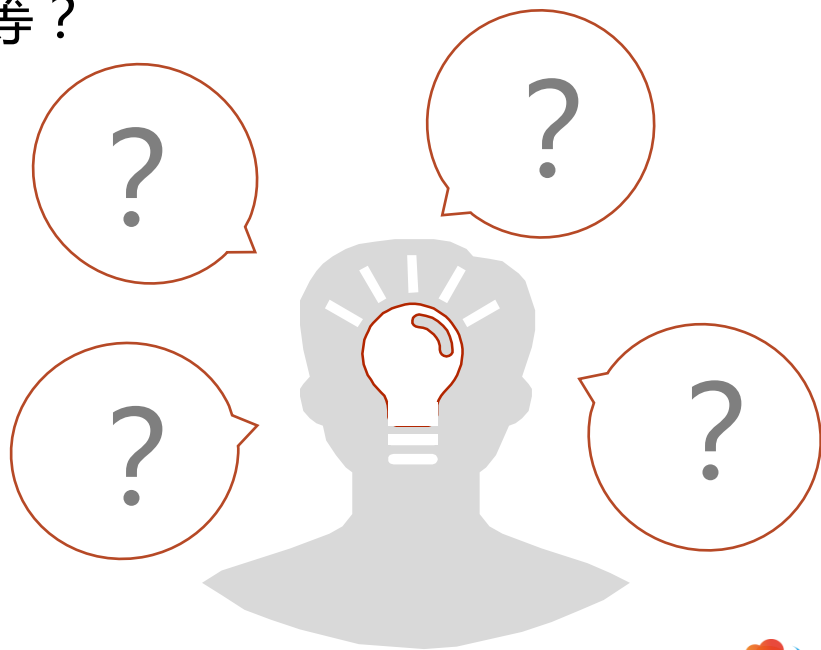
关联分析 威胁分析 建模

- 10+情报关联分析维度
- 威胁综合评分机制
- 威胁分析模型



我们怎么做的

- 我的IP是否被黑客利用，充当肉鸡等？
- 攻击我的IP关联了哪些样本？
- 恶意样本还感染过哪些IP或域名？
- 恶意历史如何？
- 哪个攻击者注册的？



我们怎么做的

人

我们怎么做的一运营



北京安全运营中心

成都安全运营中心

7×24小时，两地双中心





微信服务号：绿盟云

- 最专业的安全服务
- 最新的安全资讯
- 最热门的市场活动



Thanks

高效运维社区
开放运维联盟

荣誉出品





想第一时间看到高效运维公众号的好文章么？

请打开高效运维公众号，点击右上角小人，并如右侧所示设置即可：

