GOPS2016
Shanghai

GOPS

2016 全球运维大会

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： 开放运维联盟 OOPSA Open OPS Alliance　高效运维社区 GreatOPS Community

指导单位： 数据中心联盟 Data Center Alliance

互联网+下的云安全服务实践

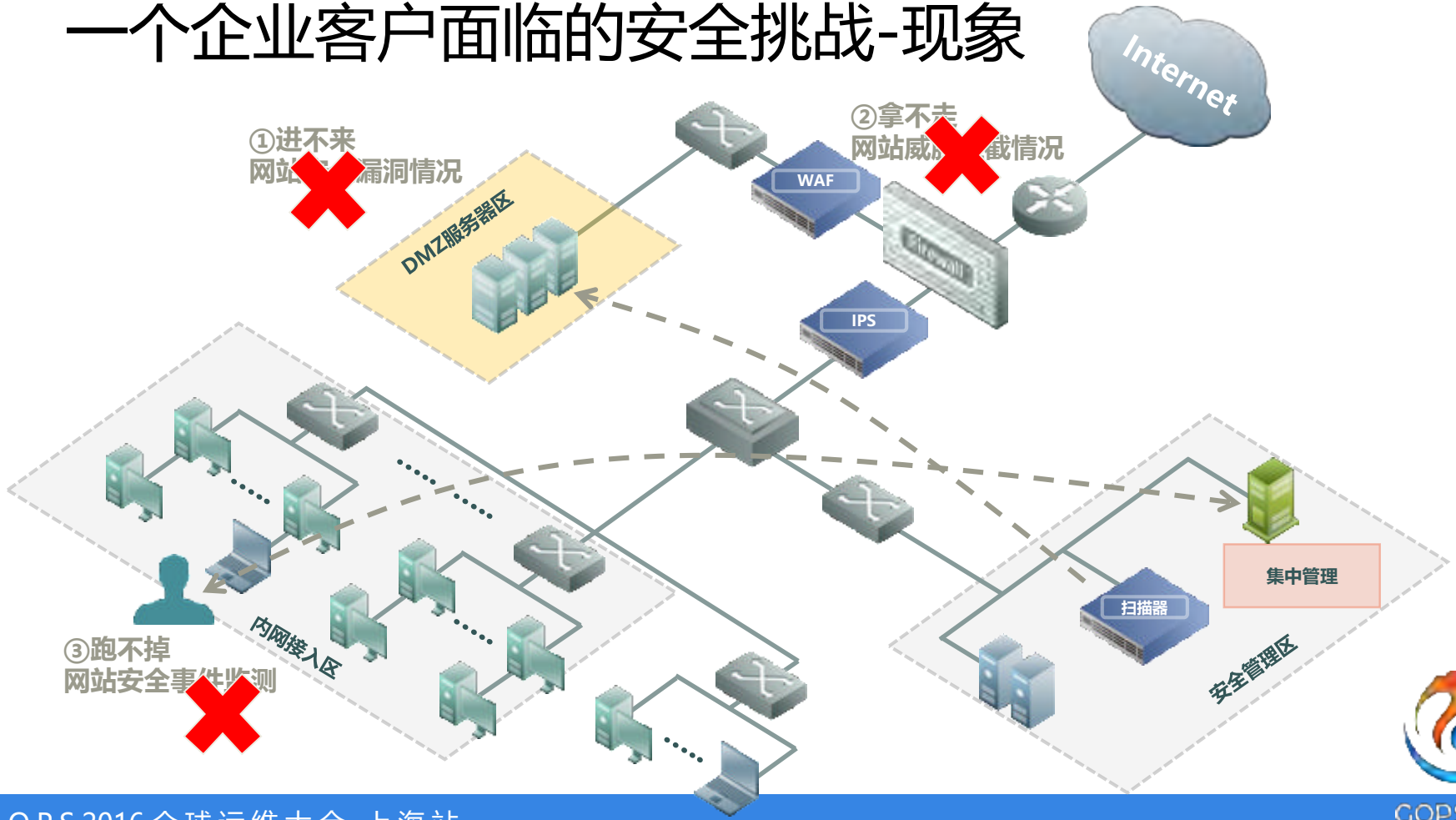
侯奎宇 绿盟科技

关于绿盟科技

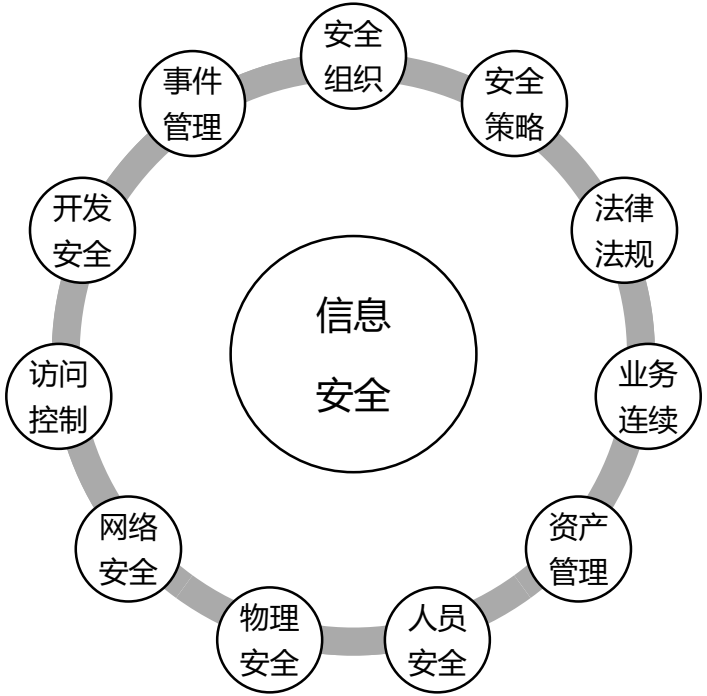

NSFOCUS
安全研究
安全产品
安全服务
安全运营
维护着国内最大的
商业漏洞库
漏洞分析和挖掘
威胁感知
安全智能
云及虚拟化安全
合规性
绿盟科技研究院
漏洞库总量快速增长
14年时间
增长668.7%
31946
76
131


NSFOCUS
NO.1
在4个重要市场，占有率第1
ADS/NIPS/RSAS/WAF
NIPS
RSAS
WAF
ADS

一个企业客户面临的安全挑战-现象



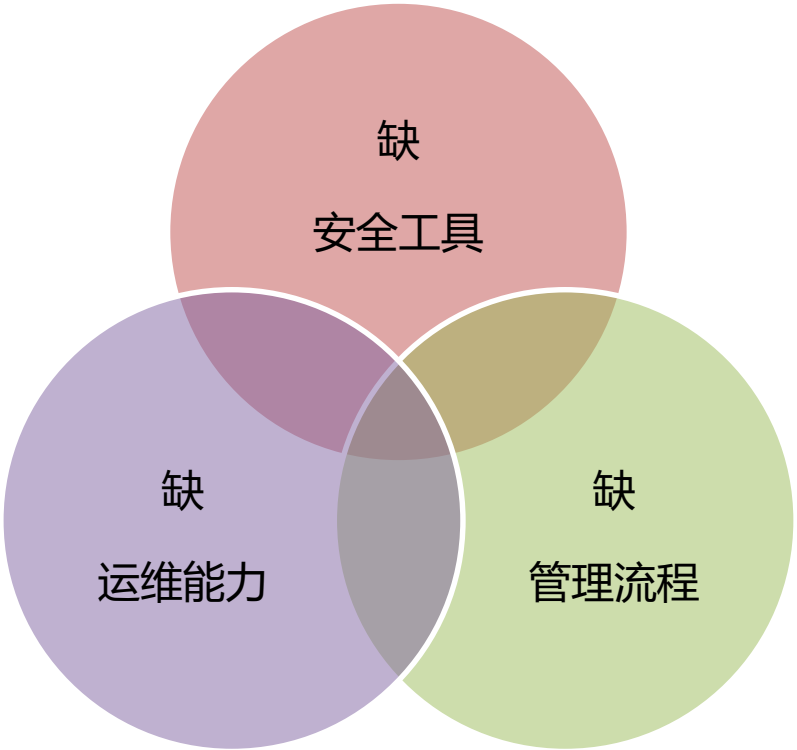
一个企业客户面临的安全挑战



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

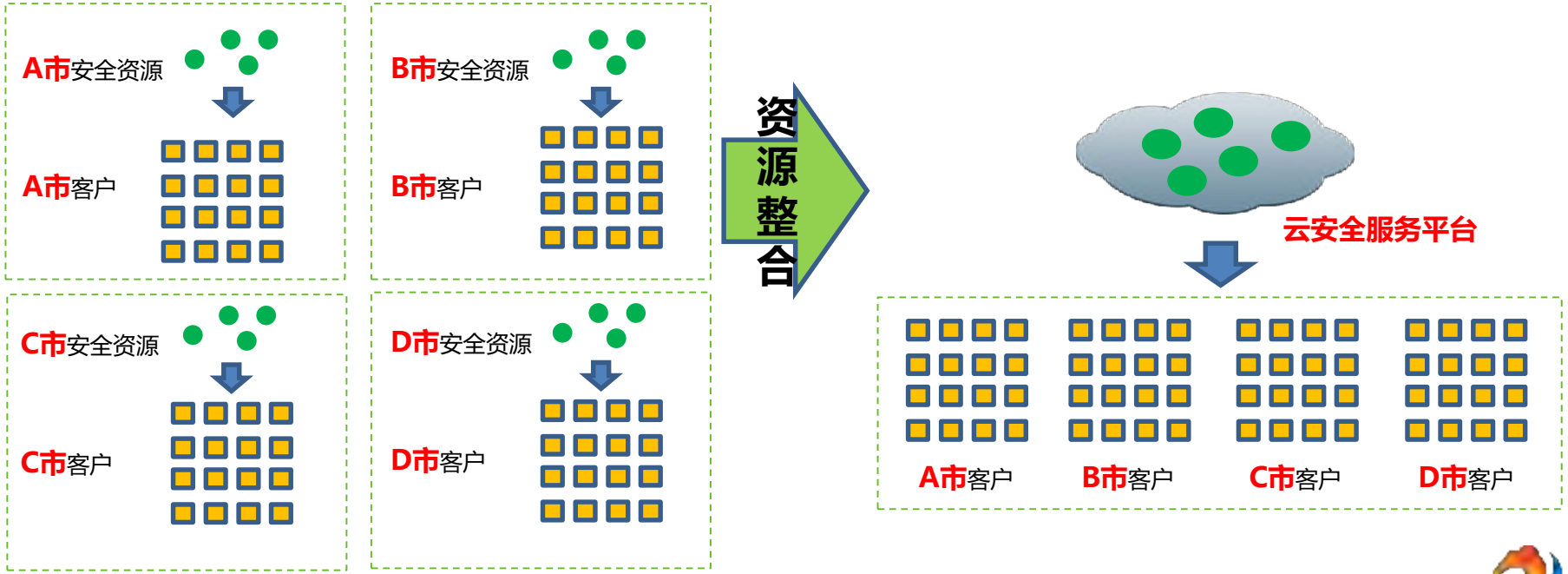


本质原因：安全人力资源的匮乏

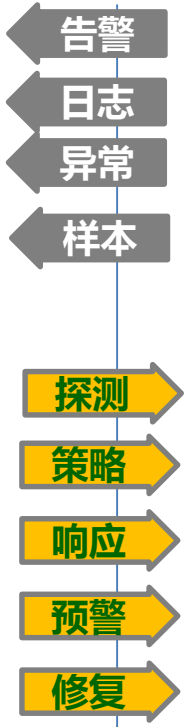
- 全球性人荒（Frost & Sullivan）
  - 2010年,全球安全专业人才225万
  - 到2015年,全球需要425万安全专业人才

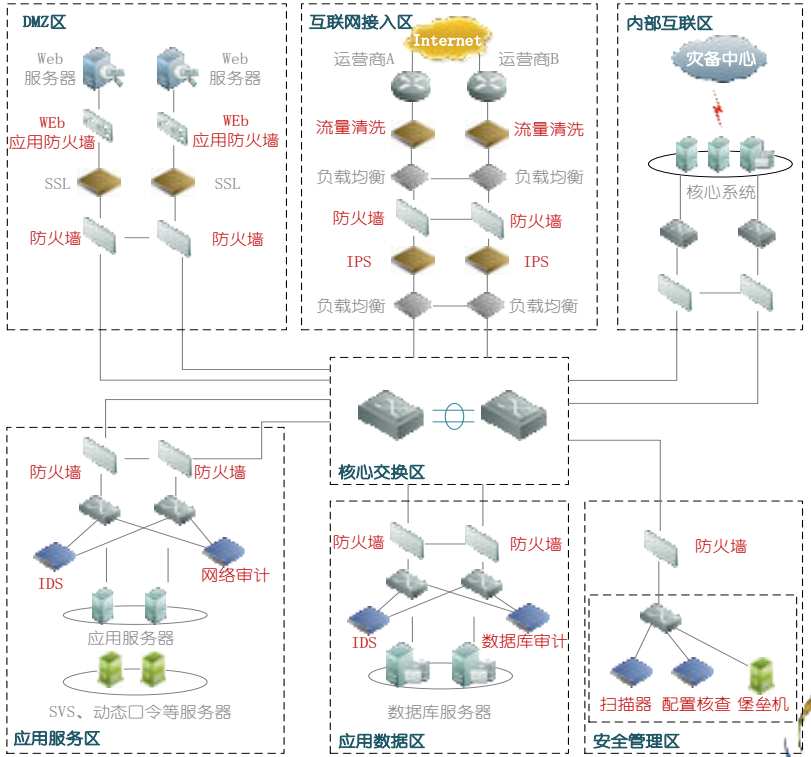
- 中国人荒更严重（工信部中国电子信息产业发展研究院）
  - 现有缺口50万
  - 在缺口不增加的情况下需要17年补齐

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

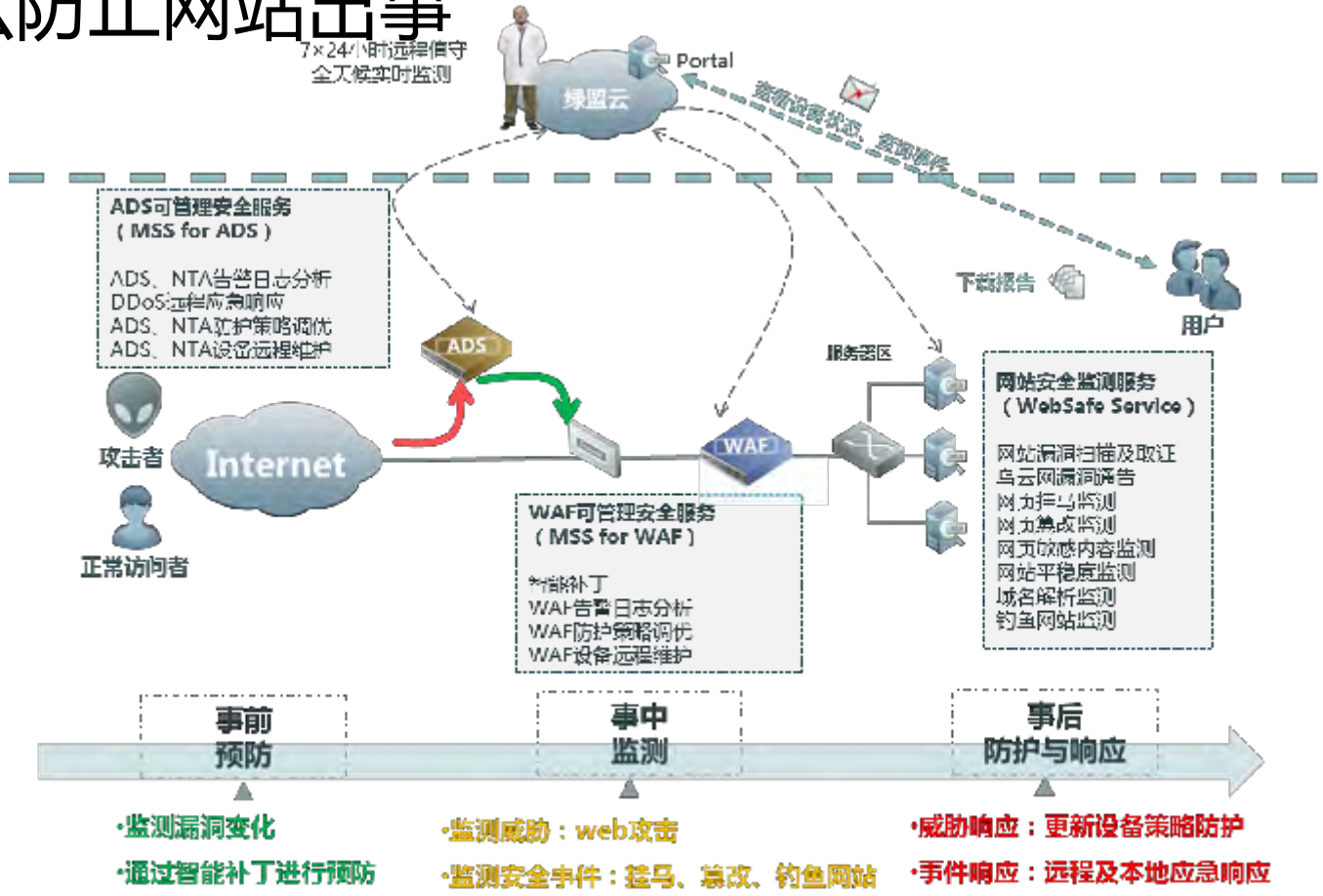
- 事前：积极预防，防患于未然
- 事中：全天候监测，第一时间发现问题
- 事后：快速响应，迅速消除事件影响

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


7×24小时远程值守
全天候实时监测
Portal
绿盟云
ADS可管理安全服务
（MSS for ADS）
ADS、NTA告警日志分析
DDoS远程应急响应
ADS、NTA防护策略调优
ADS、NTA设备远程维护
ADS
攻击者
Internet
正常访问者
WAF
服务器区
WAF可管理安全服务
（MSS for WAF）
智能补丁
WAF告警日志分析
WAF防护策略调优
WAF设备远程维护
下载报告
用户
网站安全监测服务
（WebSafe Service）
网站漏洞扫描及取证
乌云网漏洞预告
网力挂马监测
网力篡改监测
网页敏感内容监测
网站平稳度监测
域名解析监测
钓鱼网站监测
事前
预防
事中
监测
事后
防护与响应
·监测漏洞变化
·通过智能补丁进行预防
·监测威胁：web攻击
·监测安全事件：挂马、篡改、钓鱼网站
·威胁响应：更新设备策略防护
·事件响应：远程及本地应急响应

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%。

截至2015年12月，中国网页[4]数量为2123亿个，年增长11.8%。

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
NSFOCUSCLOUD

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？

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，谁来帮我辨识DDoS？
- IP被封，业务中断，谁来告诉我该怎么办？

移动安全SaaS解决方案

谁能帮我保护APP？

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

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

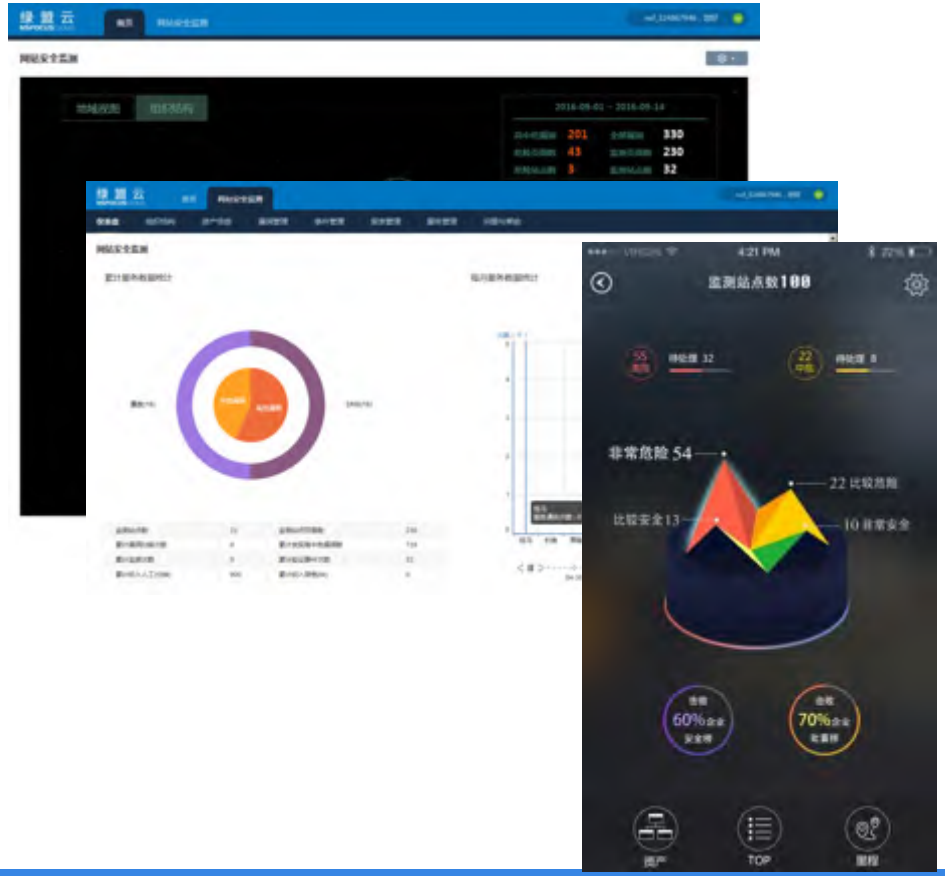
流量清洗

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

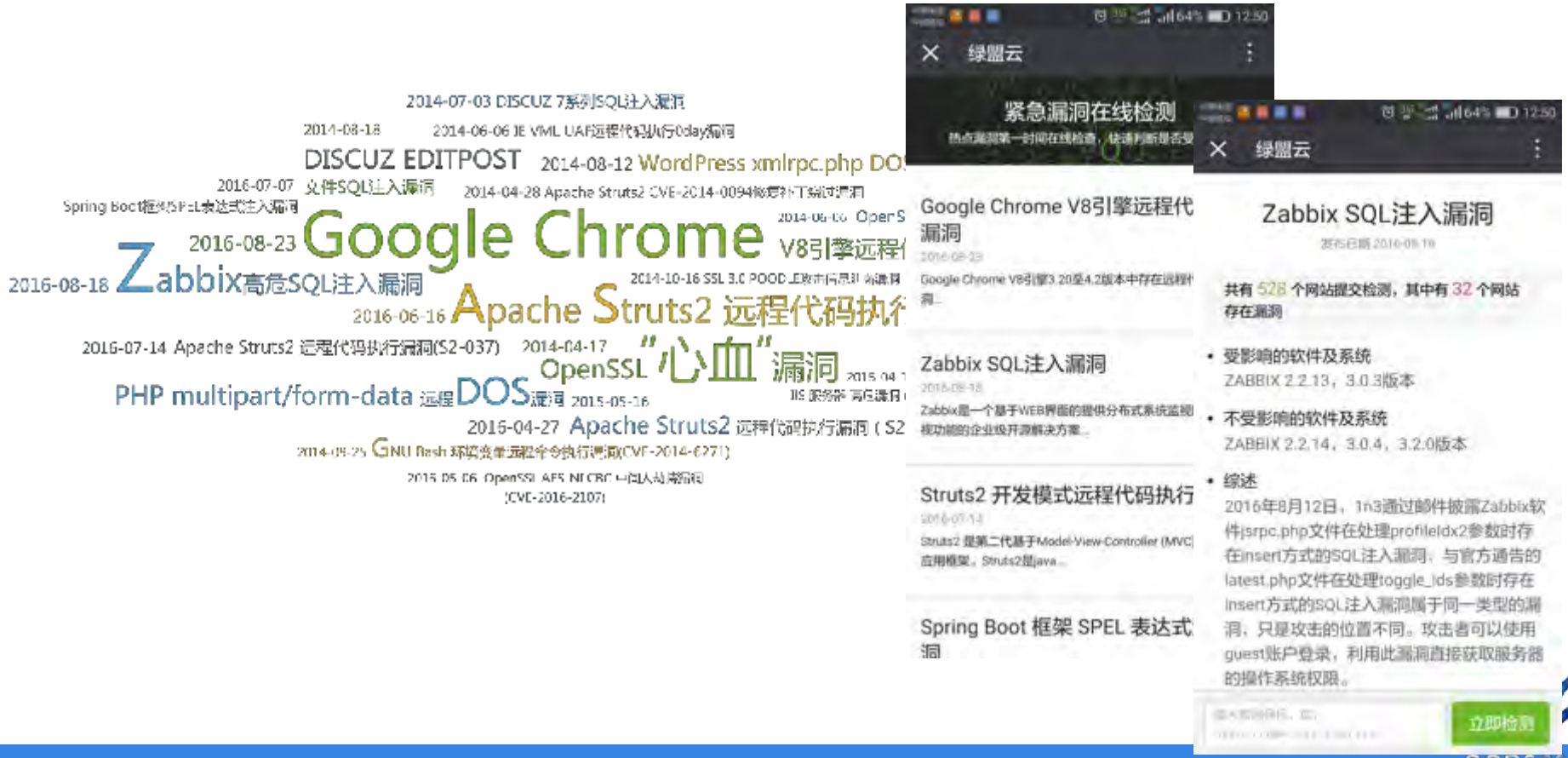
一次安装，随时使用

- 漏洞检查、**准确全面**

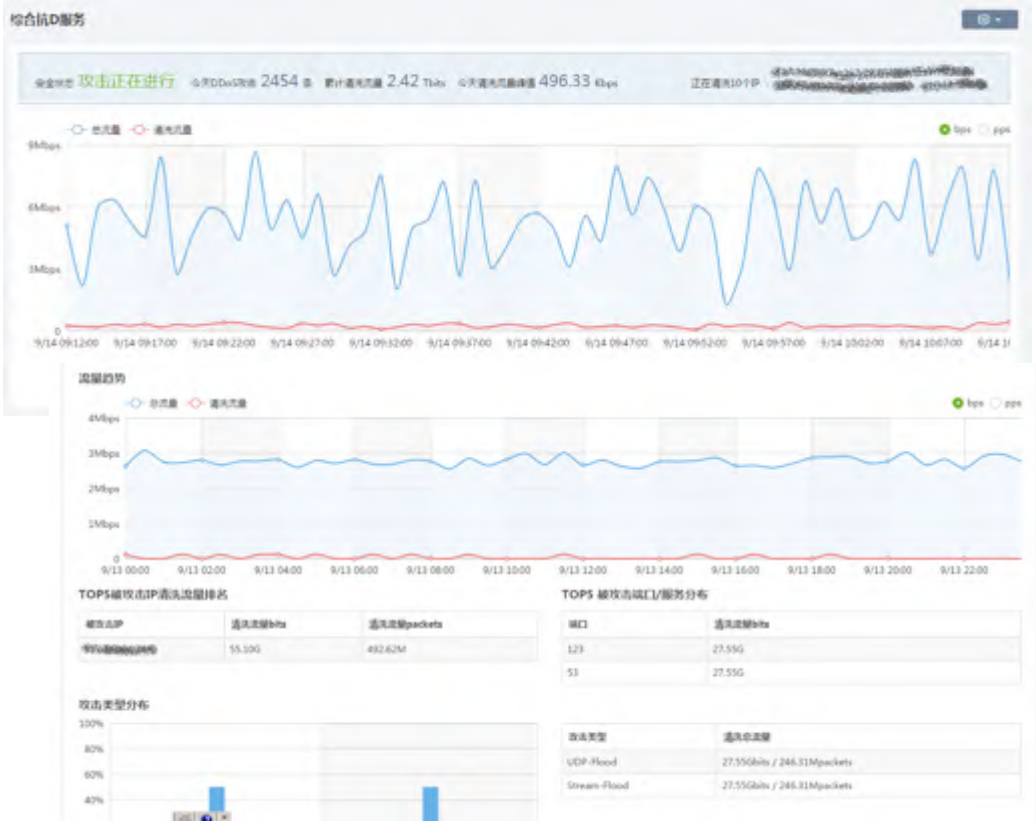
超过**15000**条漏洞库，专业团队支持，持续更新

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



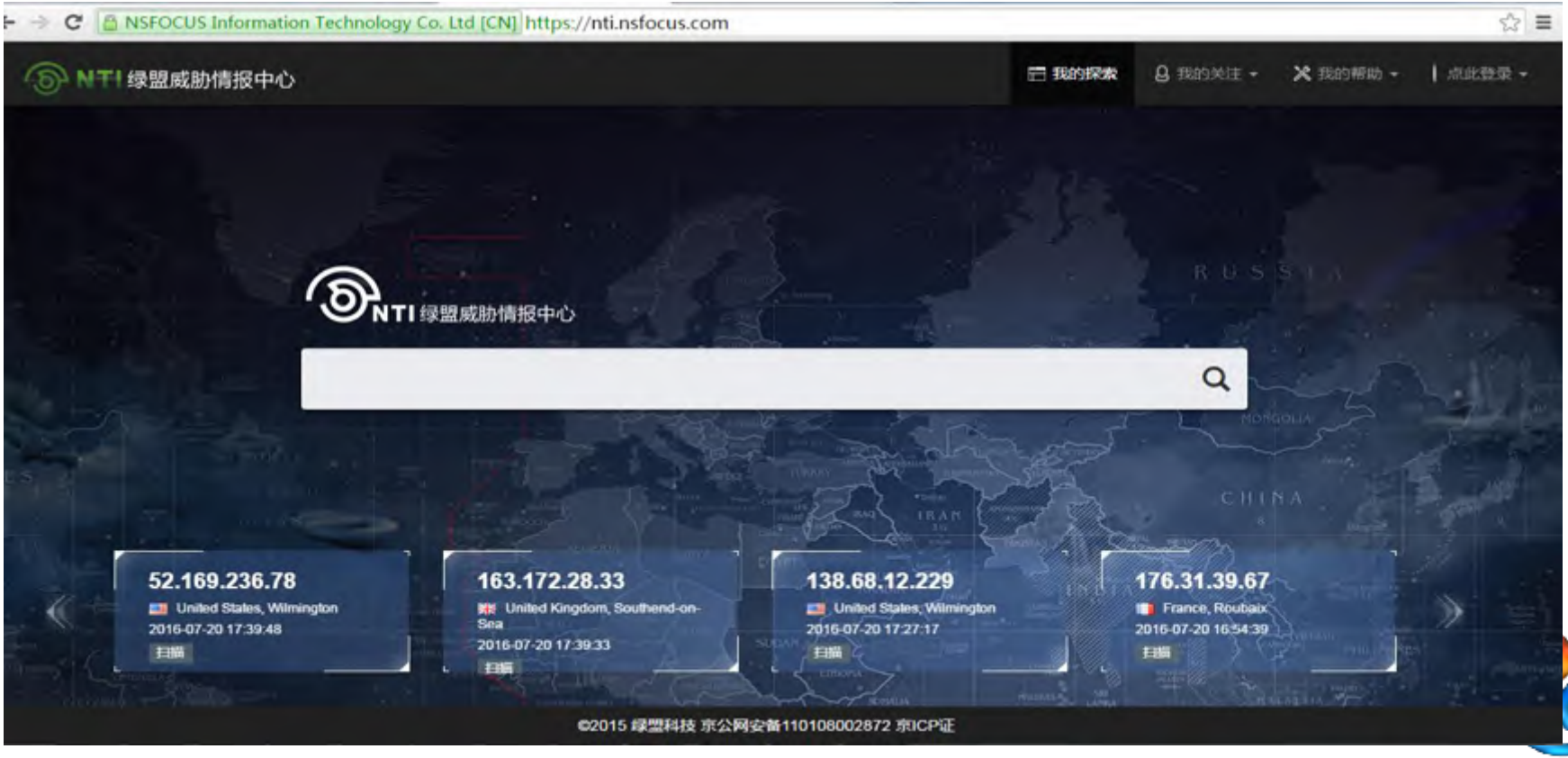
有什么服务—综合抗D服务



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
RUSSIA
MONGOLIA
CHINA
IRAN
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？

- 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

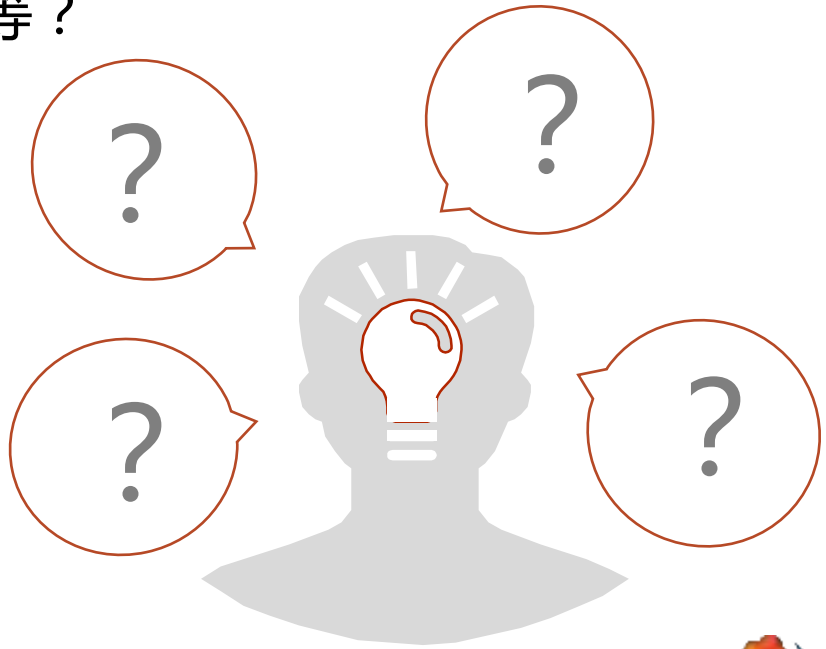
- 千万级恶意IP
- 万级C&C
- 亿级恶意域名
- 几十万恶意URL
- 百万级文件

- 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

- 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—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：