CTIC

网络安全走向云化

薛 锋

01

网络安全的几个变化

数据化

云化

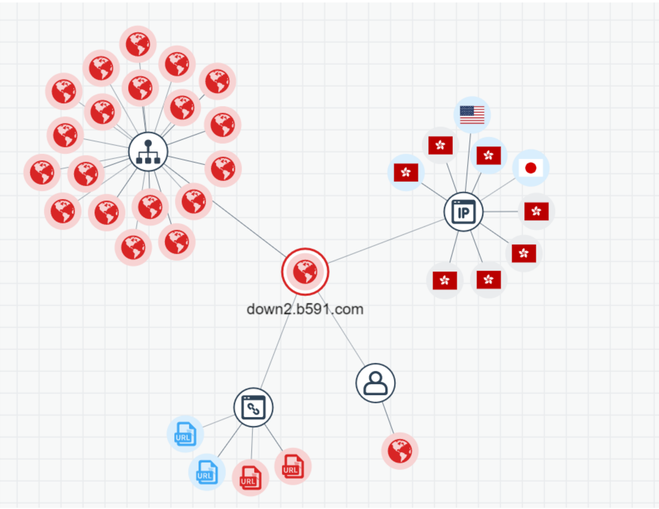
实战化

服务化

策略化、规则化

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 1024:65535 (msg:"ET
EXPLOIT Computer Associates Brightstor ARCServe Backup Mediasvr.exe
Remote Exploit"; flow:established,to_server; content:"|00 06 09 7e|";
offset:16; depth:4; content:"|00 00 00 bf 00 00 00 00 00 00 00 00|"; distance:4;
within:12; reference:url,www.milw0rm.com/exploits/3604;
reference:url,doc.abc.net/maindoc/2003518; classtype:attempted-admin;
sid:2003518; rev:5;)
```

数据化



f(garbage) = garbage


100%
EVOLUTION
78%
STATUS

Office 365 aws 阿里云 salesforce zoom


咖啡厅


酒店


高铁内


家里

…

Google

VirusTotal

Backstory

paloalto NETWORKS

PALO ALTO NETWORKS
APPLICATION FRAMEWORK
Accelerating security innovation

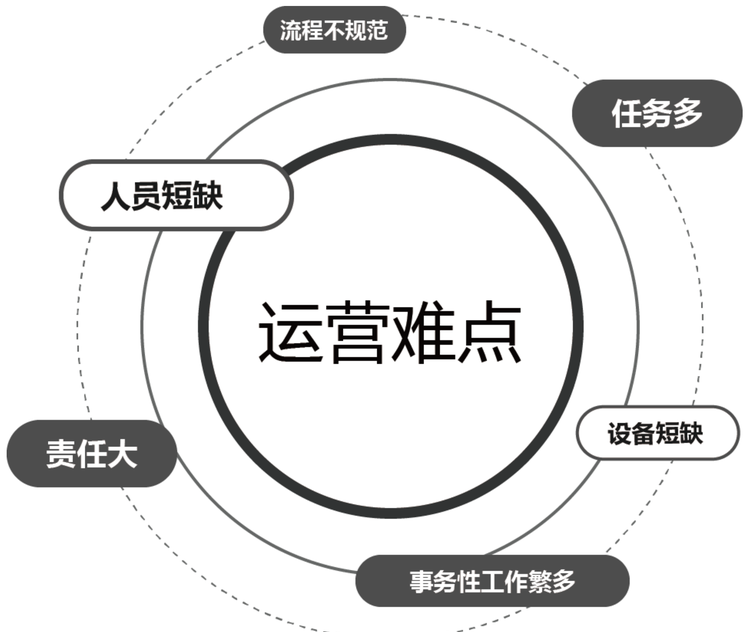
WILDFIRE

网络安全走向实战化

大型网络攻防演练

依赖于封禁IP的防守方式不可持续

勒索、挖矿、APT攻击等走向日常化



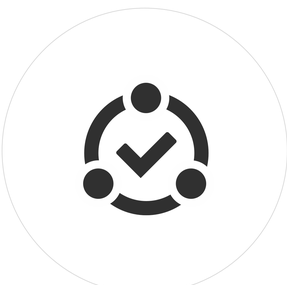
服务化

专业安全分析师

+

高级检测响应手段

+



规范服务流程

02

基础安全的薄弱环节

检测与响应能力的缺失

对DNS的忽视

对邮件安全的忽视

众包应用的局限性

IDS is Dead ?

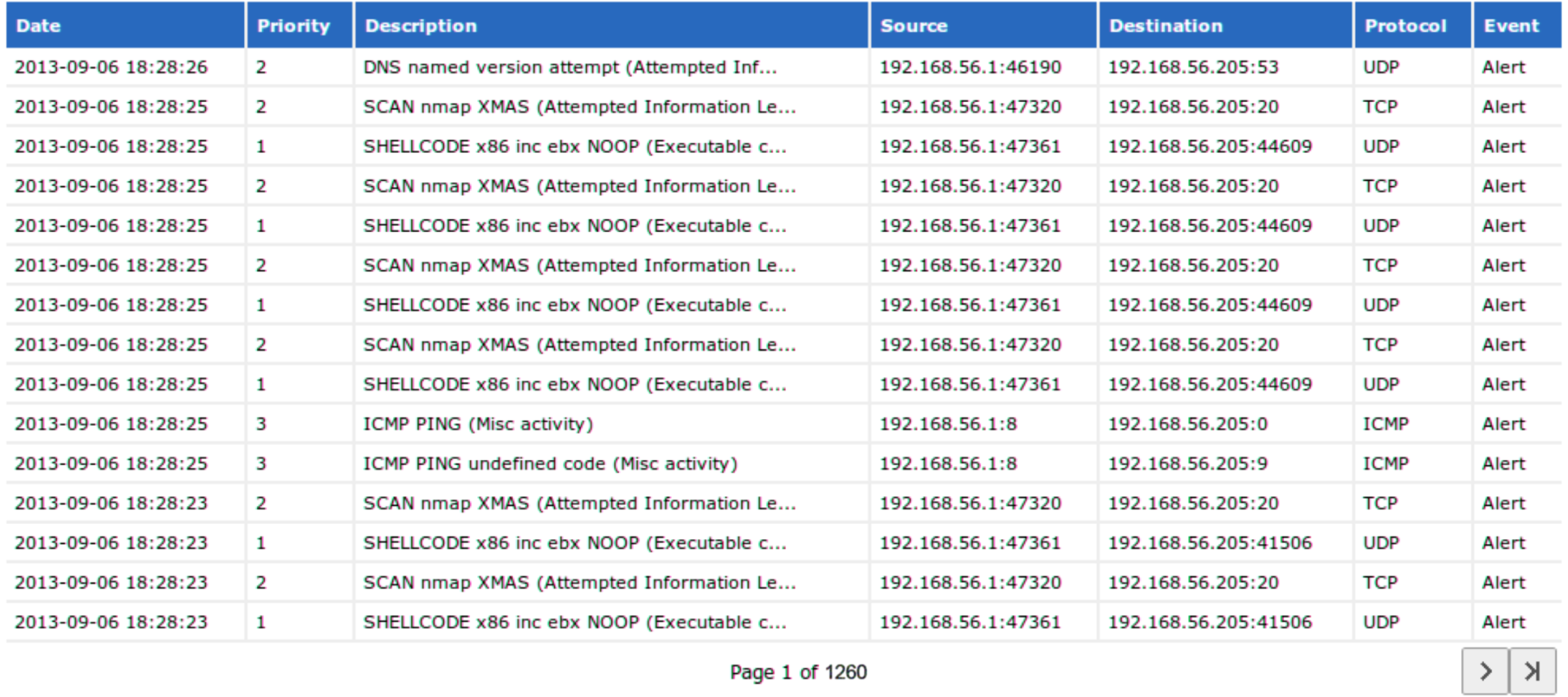
入侵检测系统已死?

Assume Breach

思路转变：失陷假定

告警事件数

100,000+



Date	Priority	Description	Source	Destination	Protocol	Event
2013-09-06 18:28:26	2	DNS named version attempt (Attempted Inf...	192.168.56.1:46190	192.168.56.205:53	UDP	Alert
2013-09-06 18:28:25	2	SCAN nmap XMAS (Attempted Information Le...	192.168.56.1:47320	192.168.56.205:20	TCP	Alert
2013-09-06 18:28:25	1	SHELLCODE x86 inc ebx NOOP (Executable c...	192.168.56.1:47361	192.168.56.205:44609	UDP	Alert
2013-09-06 18:28:25	2	SCAN nmap XMAS (Attempted Information Le...	192.168.56.1:47320	192.168.56.205:20	TCP	Alert
2013-09-06 18:28:25	1	SHELLCODE x86 inc ebx NOOP (Executable c...	192.168.56.1:47361	192.168.56.205:44609	UDP	Alert
2013-09-06 18:28:25	2	SCAN nmap XMAS (Attempted Information Le...	192.168.56.1:47320	192.168.56.205:20	TCP	Alert
2013-09-06 18:28:25	1	SHELLCODE x86 inc ebx NOOP (Executable c...	192.168.56.1:47361	192.168.56.205:44609	UDP	Alert
2013-09-06 18:28:25	2	SCAN nmap XMAS (Attempted Information Le...	192.168.56.1:47320	192.168.56.205:20	TCP	Alert
2013-09-06 18:28:25	1	SHELLCODE x86 inc ebx NOOP (Executable c...	192.168.56.1:47361	192.168.56.205:44609	UDP	Alert
2013-09-06 18:28:25	3	ICMP PING (Misc activity)	192.168.56.1:8	192.168.56.205:0	ICMP	Alert
2013-09-06 18:28:25	3	ICMP PING undefined code (Misc activity)	192.168.56.1:8	192.168.56.205:9	ICMP	Alert
2013-09-06 18:28:23	2	SCAN nmap XMAS (Attempted Information Le...	192.168.56.1:47320	192.168.56.205:20	TCP	Alert
2013-09-06 18:28:23	1	SHELLCODE x86 inc ebx NOOP (Executable c...	192.168.56.1:47361	192.168.56.205:41506	UDP	Alert
2013-09-06 18:28:23	2	SCAN nmap XMAS (Attempted Information Le...	192.168.56.1:47320	192.168.56.205:20	TCP	Alert
2013-09-06 18:28:23	1	SHELLCODE x86 inc ebx NOOP (Executable c...	192.168.56.1:47361	192.168.56.205:41506	UDP	Alert

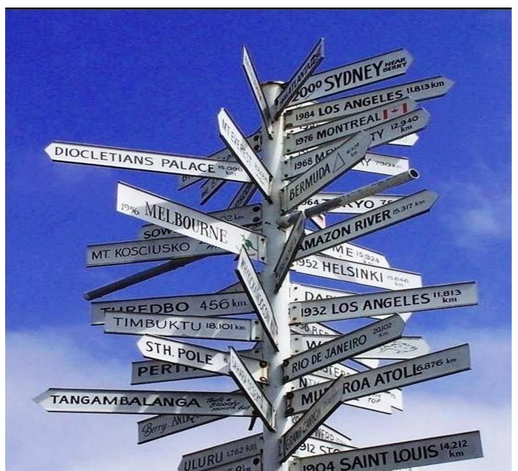
Page 1 of 1260

攻击杀伤链-Kill Chain

DNS在网络中的重要性

知道你要去哪

告诉设备该去哪

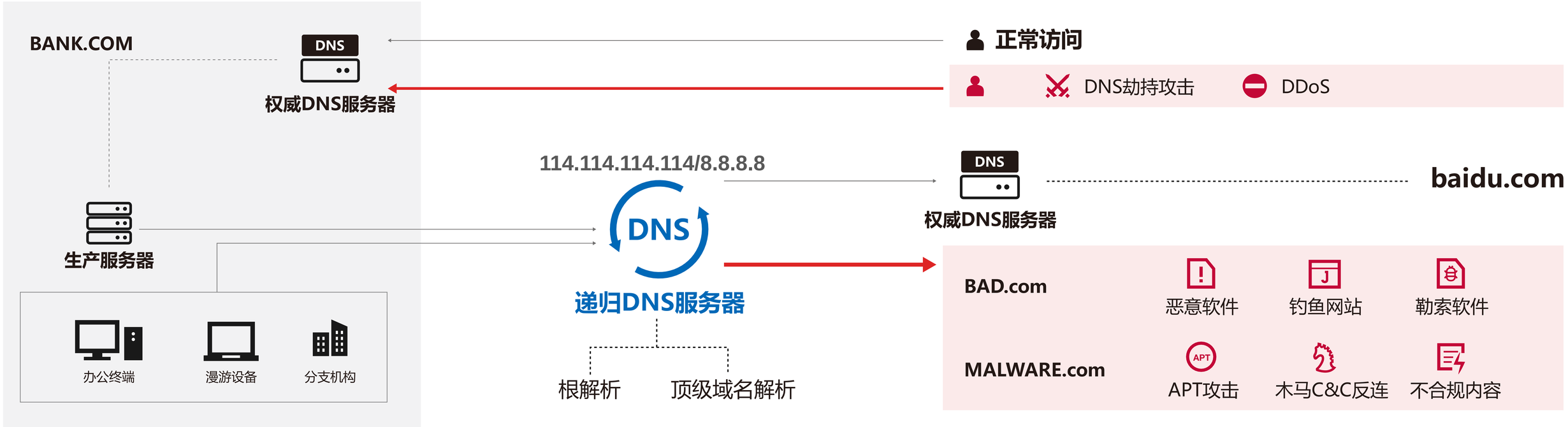


告诉别人你在哪

DNS故障 ≈ 断网

DNS劫持 ≈ 欺骗

DNS管控 ≈ 上网行为管控


BANK.COM
DNS
权威DNS服务器
正常访问
DNS劫持攻击
DDoS
114.114.114.114/8.8.8.8
DNS
权威DNS服务器
baidu.com
生产服务器
DNS
递归DNS服务器
BAD.com
恶意软件
钓鱼网站
勒索软件
MALWARE.com
APT
APT攻击
木马C&C反连
不合规内容
办公终端
漫游设备
分支机构
根解析
顶级域名解析

91.3% of malware uses DNS in attacks

*Source: Cisco 2016 Annual Security Report

94% of malware incidents were delivered via email

*Source: Verizon 2019 Data Breach Investigations Report

大型网络攻防演中/日常网络安全事件：邮件成为主要的突破点

钓鱼邮件、利用垃圾邮件大规模传播、用户凭证被窃、
BEC低成本、易于传播

工具的缺失

没有防护设备，或者仅依赖传统垃圾邮件网关
对新型攻击的检测能力缺失
在邮件安全上投入较少，重视度低

安全意识的缺乏

员工缺乏邮件安全意识
缺乏有效的邮件安全意识培训


攻击方
组织化、团伙化、众包
防守方
单兵作战、无联防
打码
猫池
暗网
众测
众测
众测

03

微步在线的探索

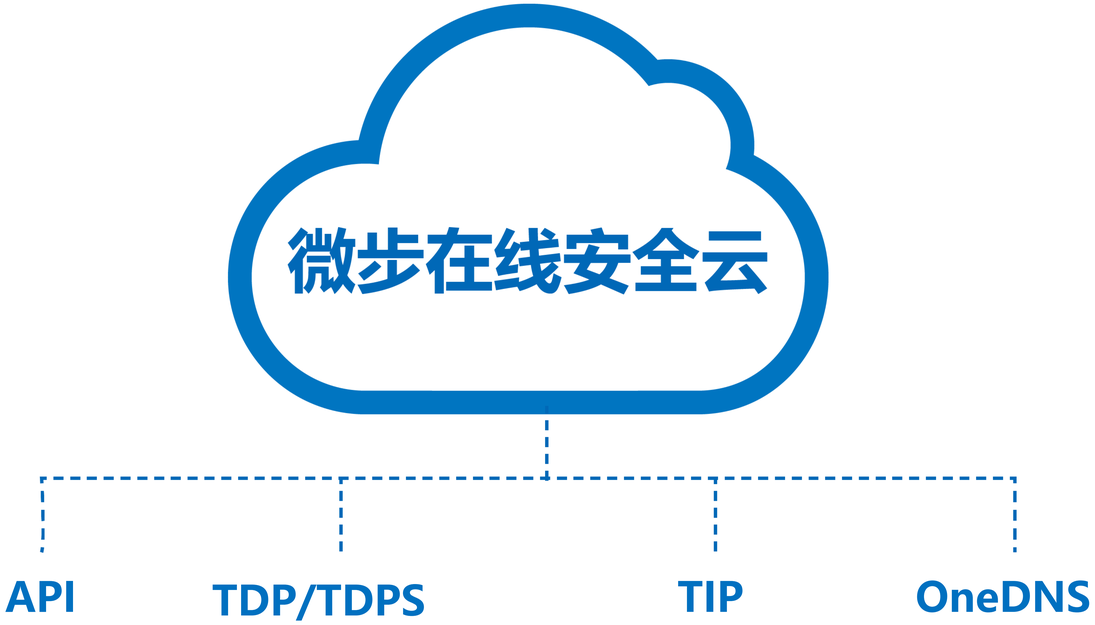
安全云

专业、稳定的DNS服务OneDNS

威胁情报管理平台TIP

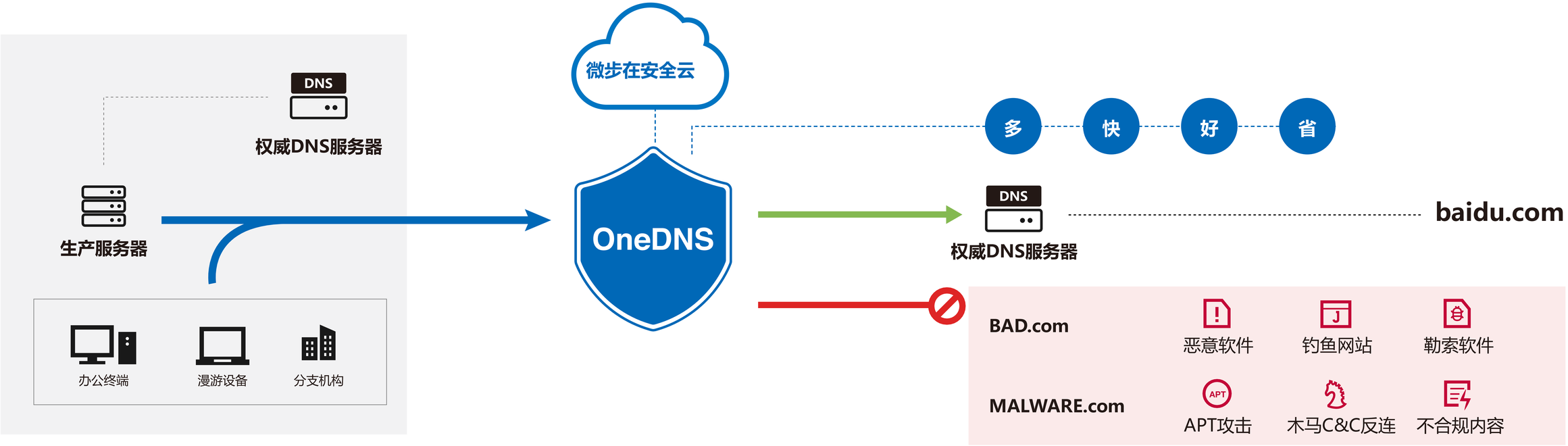
威胁检测平台TDP

威胁情报社区

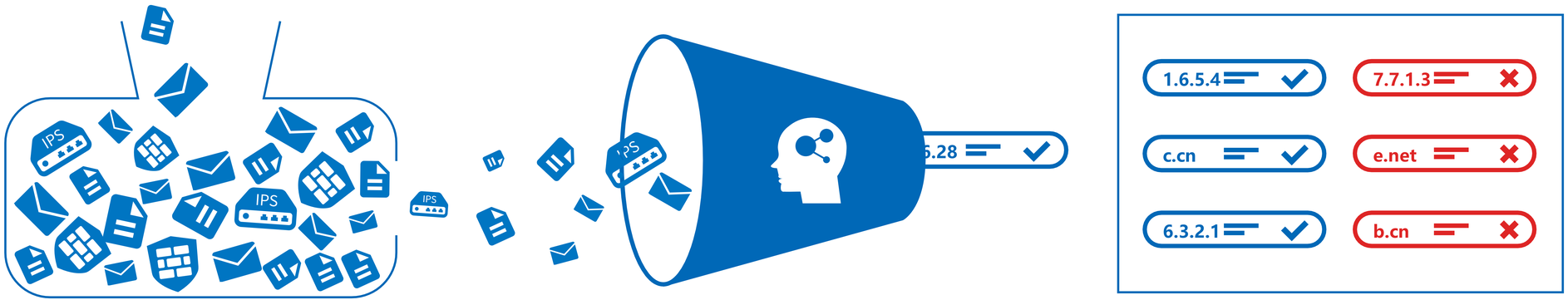


- 十大银行中的8家
- 十大证券中的6家
- 五大互联网中的4家
- 五大智能手机中的3家
- 十大能源中的5家

OneDNS – 企业安全DNS服务



威胁数据化 - 威胁情报管理平台TIP(Threat Intelligence Platform)



日志获取

IPS、WAF、邮件、应用日志

“自动化”提取

关联分析、丰富上下文、去误报

自有情报累积

攻击IP、IOC、攻击团伙画像

重新定义入侵检测

IDPS

入侵结果

•精准判定攻击结果：成功与否
•判定是否针对性攻击、是否为攻击事件

新型检测方案的重点

入侵过程

•提供攻击时序过程以供分析
•依据攻击链分析攻击手段和工具

用于分析与溯源，支撑响应

等保2.0

威胁情报检测系统

等保二、三、四级都提出对威胁情报检测系统的硬性要求

等保三级和四级要求引入威胁情报库，并需要升级到最新版本

1. 全流量的日志、文件提取与报警pcap存储
2. 威胁情报检测模块
3. 机器学习模型检测模块
4. 恶意文件检测引擎模块
5. 云沙箱检测模块
6. 内网横向移动检测模块
7. 自定义情报检测模块
8. 攻击链回溯分析模块

威胁检测平台TDP(Threat Detection Platform)

基于各攻击阶段告警发现与攻击链还原的网络流量综合检测平台，并配套专业服务团队与服务工具集的MDR服务内容

威胁监控服务

应急响应服务

专杀工具集

- 针对性攻击识别
- 终端联动
- 资产梳理
- API风险
- 敏感数据泄露
- 异常发现

攻击链还原

1. 扫描/侦查
2. 投递武器
3. 漏洞利用
4. 工具安装
5. 命令与控制
6. 内网渗透
7. 行动或数据窃取

Making Intrusion Detection Work, Whatever It's Called

管它叫什么呢

¥ 10,000,000

CTIC

谢谢！