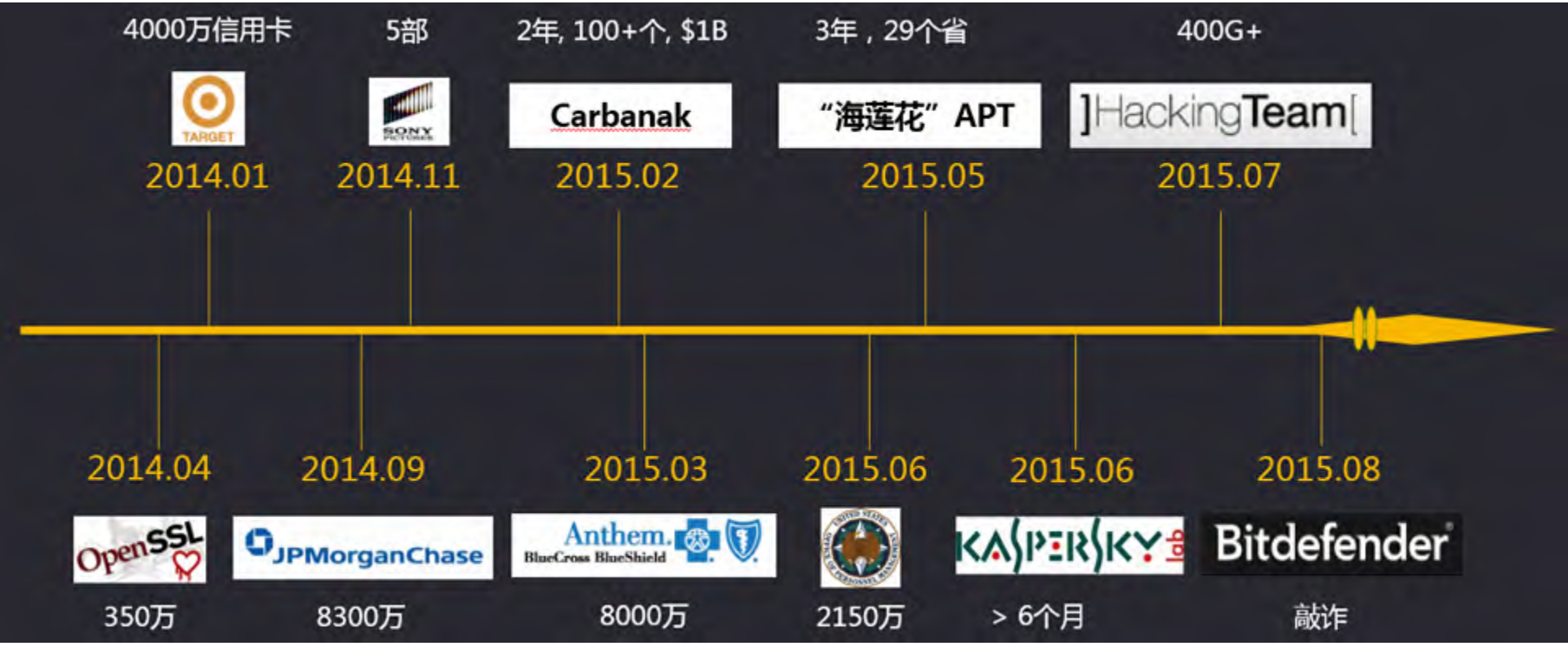
SACC 2015中国系统架构师大会
SYSTEM ARCHITECT CONFERENCE CHINA 2015
互联网+ 重塑IT架构

应用筑基 “慧眼”识魔

——下一代边界防御实践

网络空间的多事之秋


4000万信用卡
5部
2年, 100+个, $1B
3年，29个省
400G+
TARGET
SONY PICTURES
Carbanak
“海莲花”APT
]HackingTeam[
2014.01
2014.11
2015.02
2015.05
2015.07
2014.04
2014.09
2015.03
2015.06
2015.06
2015.08
OpenSSL
JPMorganChase
Anthem.
BlueCross BlueShield
KASPERSKY lab
Bitdefender
350万
8300万
8000万
2150万
> 6个月
敲诈

缺资金？少技术？没意识？

悄悄的我走了，
正如我悄悄的来；
我挥一挥衣袖，
带走你全部钱财。

重新审视传统安全方法论

静态的、被动的、防御性的战略思维

假设前提

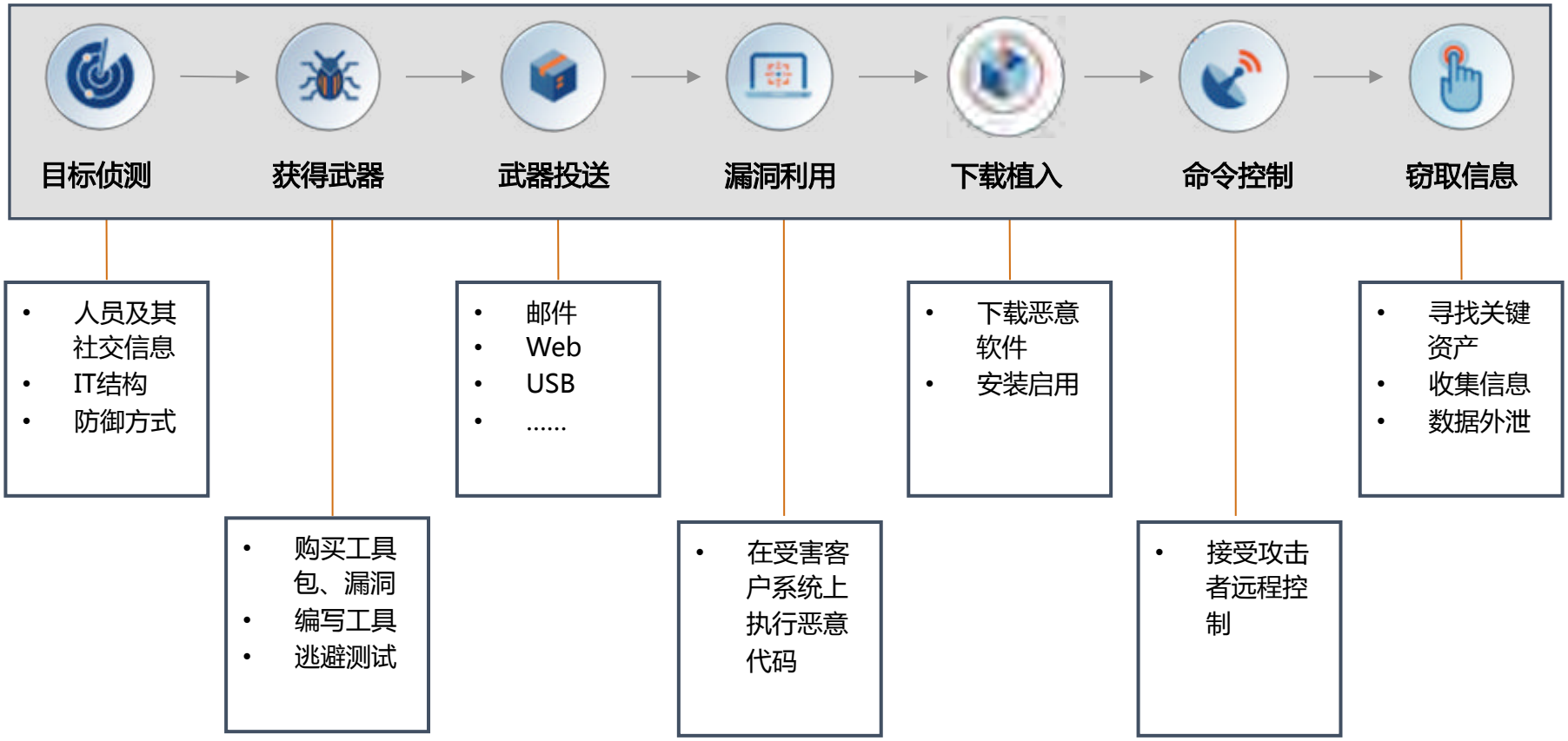
1. 信息系统蕴含的弱点可以被充分的评估和认识
2. 防护措施能够识别并阻断所有可能发生的攻击

告诉你一个真实的威胁环境

APT活动	境内感染量	首次发现时间	最近发现时间	影响省份数	影响行业	感染方式
Desert_Falcon	3	2014/4/30	2015/3/3	3	教育	鱼叉邮件、水坑
GDATA_TooHash	4	2014/6/1	2014/8/31	3	科研	鱼叉邮件
Darkhotel	334	2014/6/1	2015/3/19	29	教育、能源、电信	鱼叉邮件、网络层劫持
DarkSeoul	4	2014/6/5	2015/1/5	3	电信	鱼叉邮件
Epic Turla	14	2014/6/12	2015/3/21	6	科研、教育	鱼叉邮件
NGO_Attack	6	2014/6/18	2015/3/13	6	非政府组织	鱼叉邮件
Dragonfly	2	2014/7/15	2014/8/19	1	能源	鱼叉邮件、水坑
APT7#	1	2014/8/7	2014/8/7	1	航空	鱼叉邮件
Anunak	383	2014/9/28	2015/3/26	26	金融、电信、政府、科研	鱼叉邮件
CARETO	1	2014/10/28	2014/10/28	1	政府	鱼叉邮件
XSLCmd_OSX	1	2014/10/30	2014/10/30	1	金融	鱼叉邮件
Waterbug	1	2014/12/31	2014/12/31	1	政府	鱼叉邮件、水坑
Snake	1	2015/2/15	2015/2/15	1	金融	U盘
Equation	1	2015/4/16	2015/4/16	1	军工	U盘

定制木马、社交攻击、鱼叉钓鱼、水坑攻击……

Cyber Kill Chain

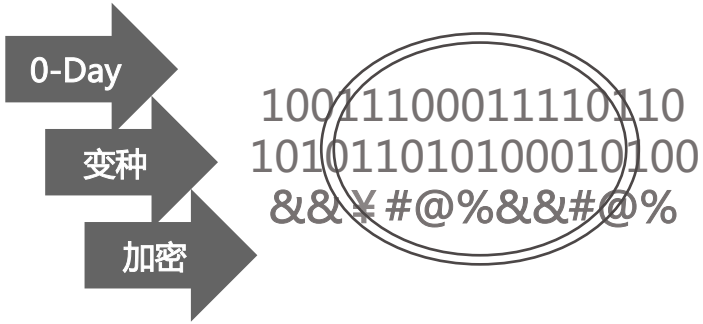


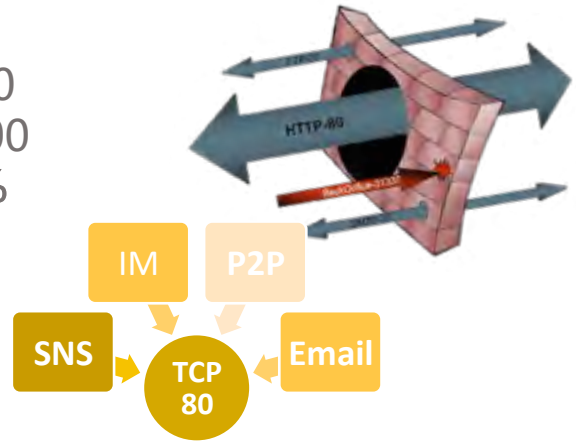
被反复洞穿的边界防线

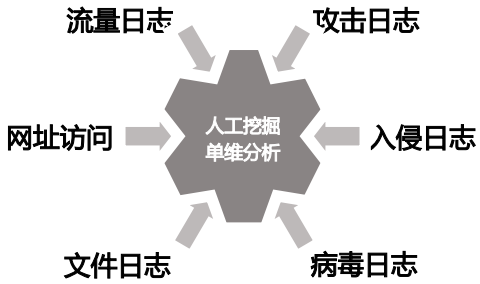
由外到内的防线
- 核心目标
  - 进入目标网络
- 主要手段
  - 钓鱼、恶意网址
  - 病毒、木马植入
  - 漏洞扫描和利用

由内到内的防线
- 核心目标
  - 获取更高权限
- 主要手段
  - 身份冒用、口令破解
  - 病毒、木马植入
  - 漏洞扫描和利用

由内到外的防线
- 核心目标
  - 核心资产暴露
- 主要手段
  - 建立C&C连接
  - 应用混淆逃逸
  - 机密数据上传







下一代安全方法论模型-PDFP

动态的、主动的、对抗性的战略思维

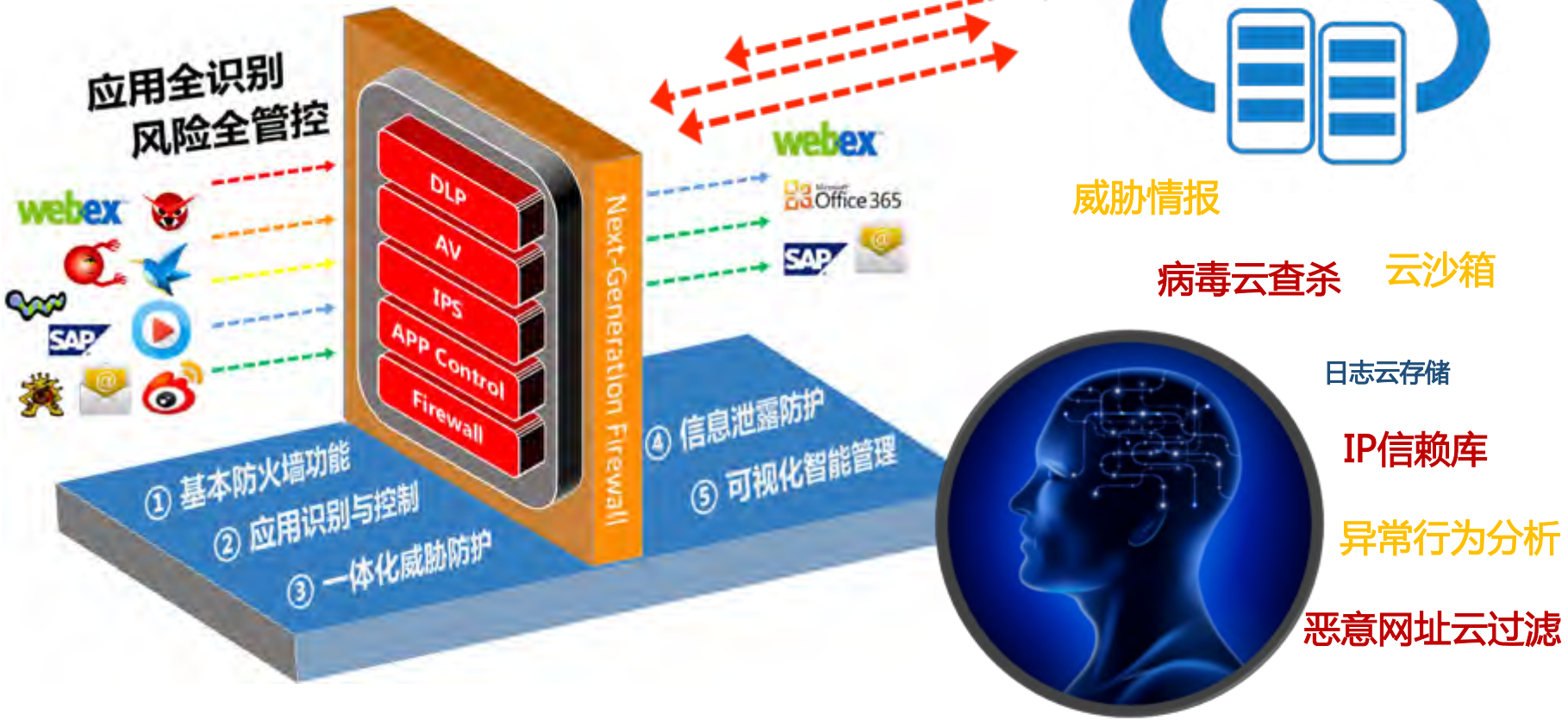
1. 未知威胁永远存在，系统已失陷
2. 借助威胁情报和大数据分析技术构建预测能力
3. 安全的起点从检测开始，通过安全情境和异常行为分析发现失陷点
4. 通过取证手段溯源攻击过程
5. 确定对抗措施，提升防御能力

防护模式的变化和能力要求

- 从以“网络或系统”为中心的策略，转变为“**以信息或数据为中心**”的策略
- 从以“控制”为中心的安全演进至以“**人**”为核心的安全
- 安全能力从“防范”为主转向“**快速检测和响应能力**”的构建
- 安全防护从“个体或单个组织”的防护，转变为“**安全情报驱动**”的信息共享、集体协作方式

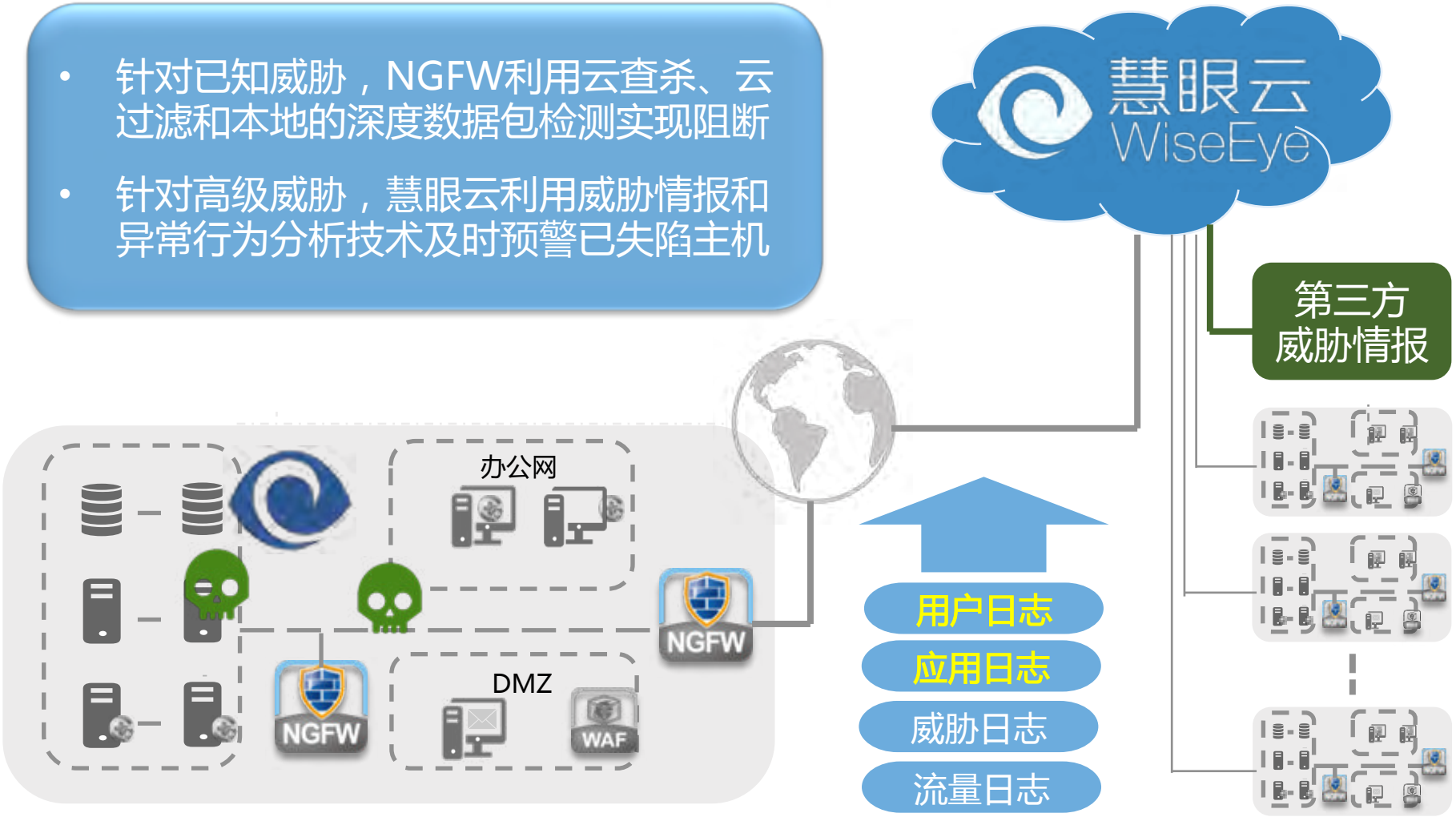
摘自：Gartner 《Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence》

“云管协同”的边界防御


网康云
威胁情报
病毒云查杀
云沙箱
日志云存储
IP信赖库
异常行为分析
恶意网址云过滤
应用全识别
风险全管控
webex
SAP
Office 365
DLP
AV
IPS
APP Control
Firewall
Next-Generation Firewall
① 基本防火墙功能
② 应用识别与控制
③ 一体化威胁防护
④ 信息泄露防护
⑤ 可视化智能管理

网康下一代边界防御解决方案

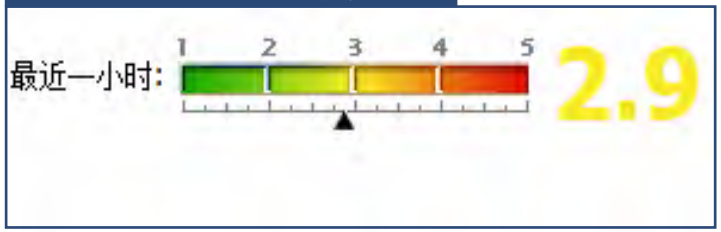
- 针对已知威胁，NGFW利用云查杀、云过滤和本地的深度数据包检测实现阻断
- 针对高级威胁，慧眼云利用威胁情报和异常行为分析技术及时预警已失陷主机



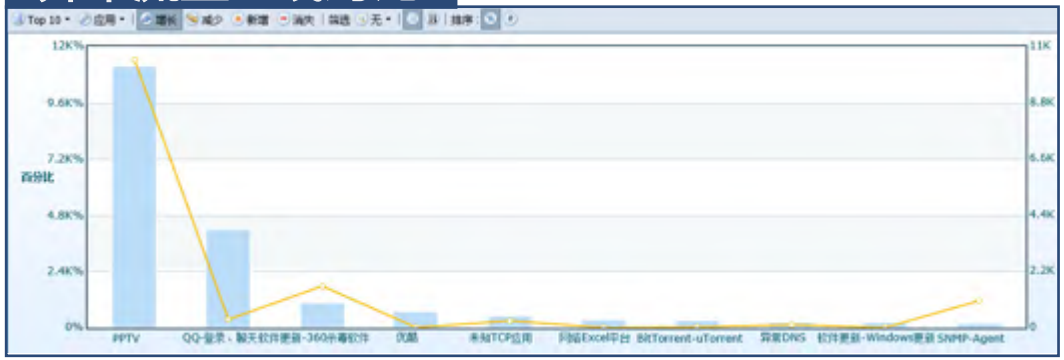
Prediction
基于威胁情报的态势感知

Detection
以风险为视角发现问题

全网风险系数

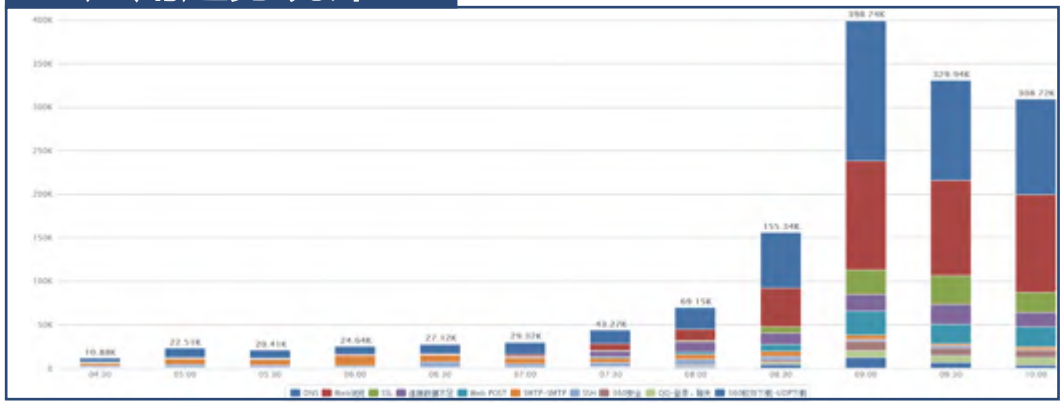


异常流量基线对比

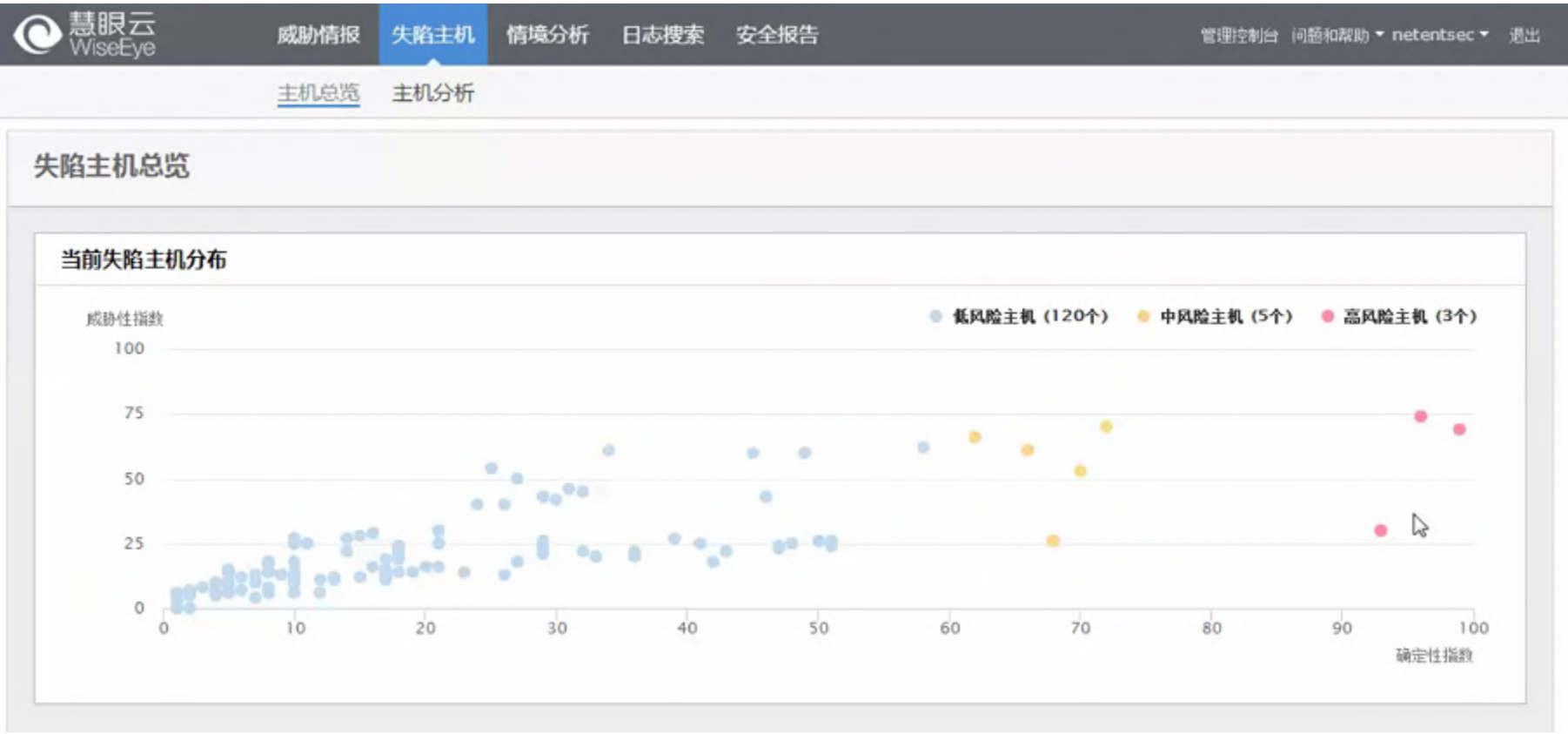


高危应用统计

应用趋势统计



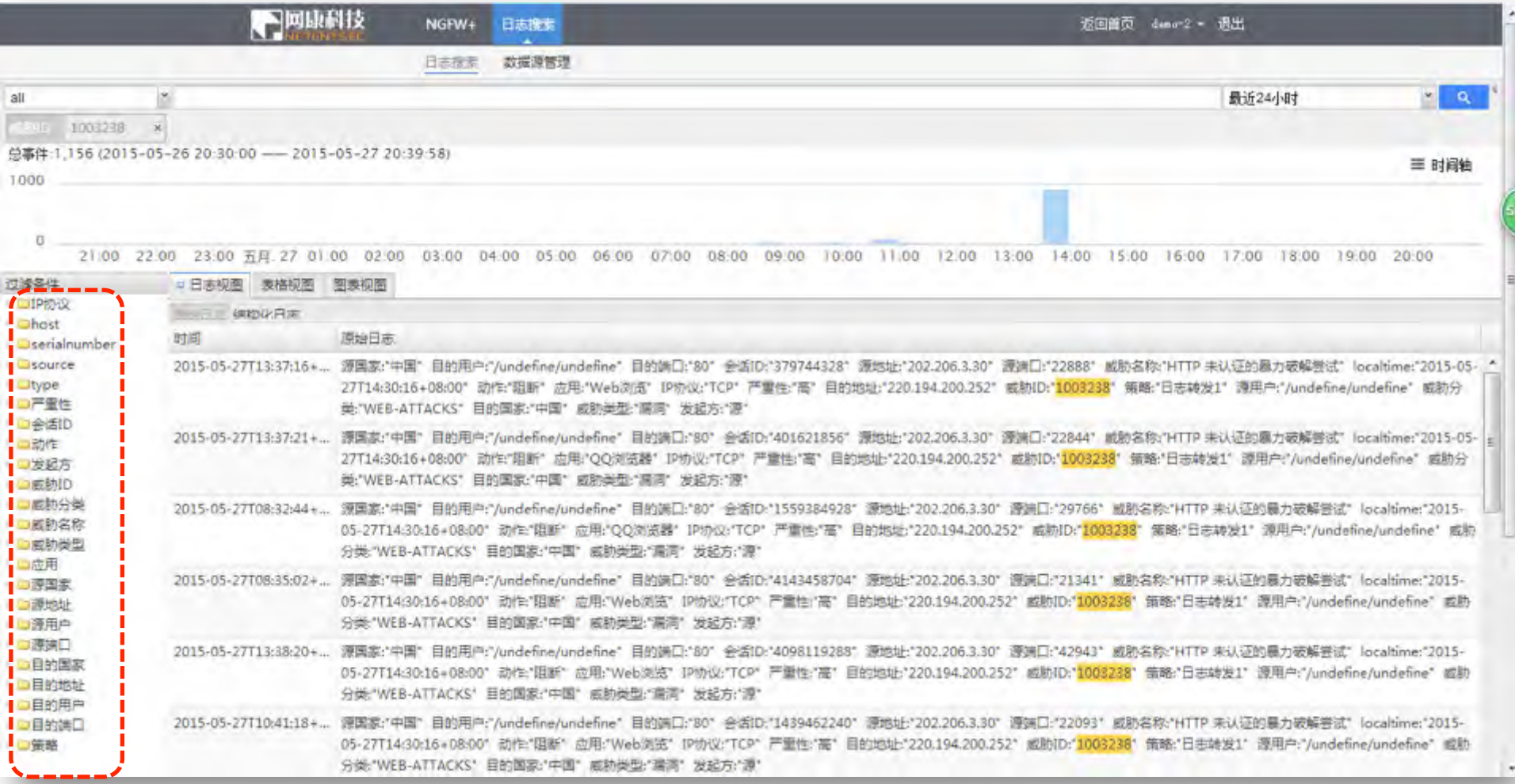
Detection
基于异常行为分析检测失陷主机



Forensic
以应用为视角关联分析问题

发生了什么？有什么异常？是什么关系？

Forensic
基于云存储的长周期溯源



Prevention 精细化应用控制

中国最大的应用识别库

全球最大的中文网页库

10余年应用层研究积累

安全提升

- 由数据流控制转向业务流控制
- 由黑名单控制转向白名单控制
- 由流量控制深入至内容级过滤

Prevention 融合的入侵防御

Certificate Of CVE Compatibility

MAPP Partners

海量特征库

ACTIVEX	IMAP	SQL-INJECTION
BACKDOOR	JAVA	TELNET
BAD-FILES	LDAP	VIRUS
DB-ATTACKS	MEDIA	VOIP
DDOS	NETBIOS	WEAKPASSWORD
DNS	OTHER	WEB-ATTACKS
DOS	POP	WEB-CLIENT
EXPLOIT	RPC	WEB-SCAN
FTP	SCADA-ATTACKS	WINDOWS
ICMP	SMTP	XSS

30类，6300余种漏洞防护

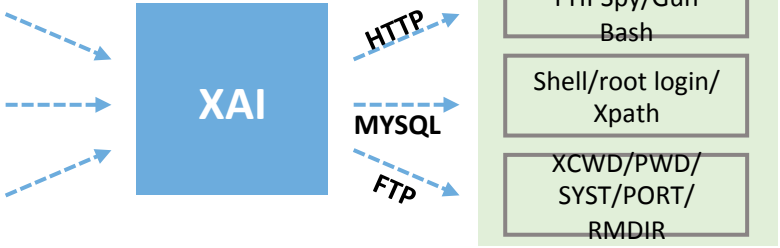
8类，8600余种间谍软件防护

防逃逸机制

防逃逸机制	逃逸方法
分片重组	将攻击流量分散到多个协议分片中
单包多次解析	将分包传递的信息压缩在单包中
目录混淆防护	使用“..”或“.”等使路径复杂化
大小写互转	大小写字符混杂
特殊编码解码	使用UTF/Base64/gzip等编码伪装
特殊字符处理	使用无意义的字符填充流量

应用预识别

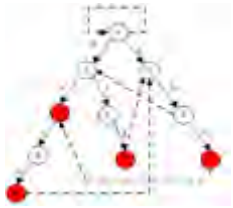
- 避免端口混淆导致的逃逸
- 有针对性检测降低误报率



高性能多模匹配算法

ACBM

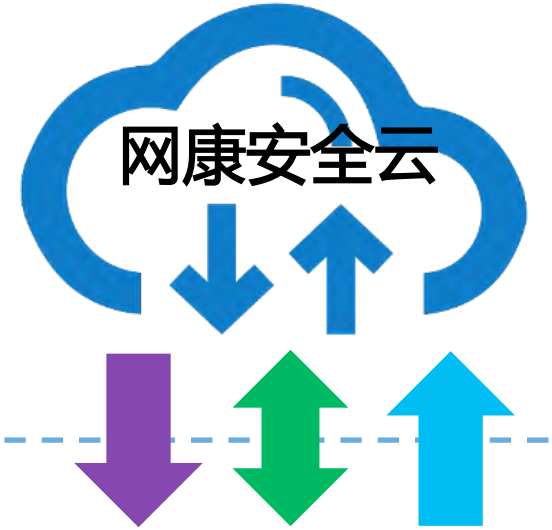
基于状态机的带跳转的多模匹配算法



WMRSR

基于前后缀过滤快速跳转和字典树的接力跳转的多模匹配算法

Prevention
病毒云查杀 恶意网址云过滤



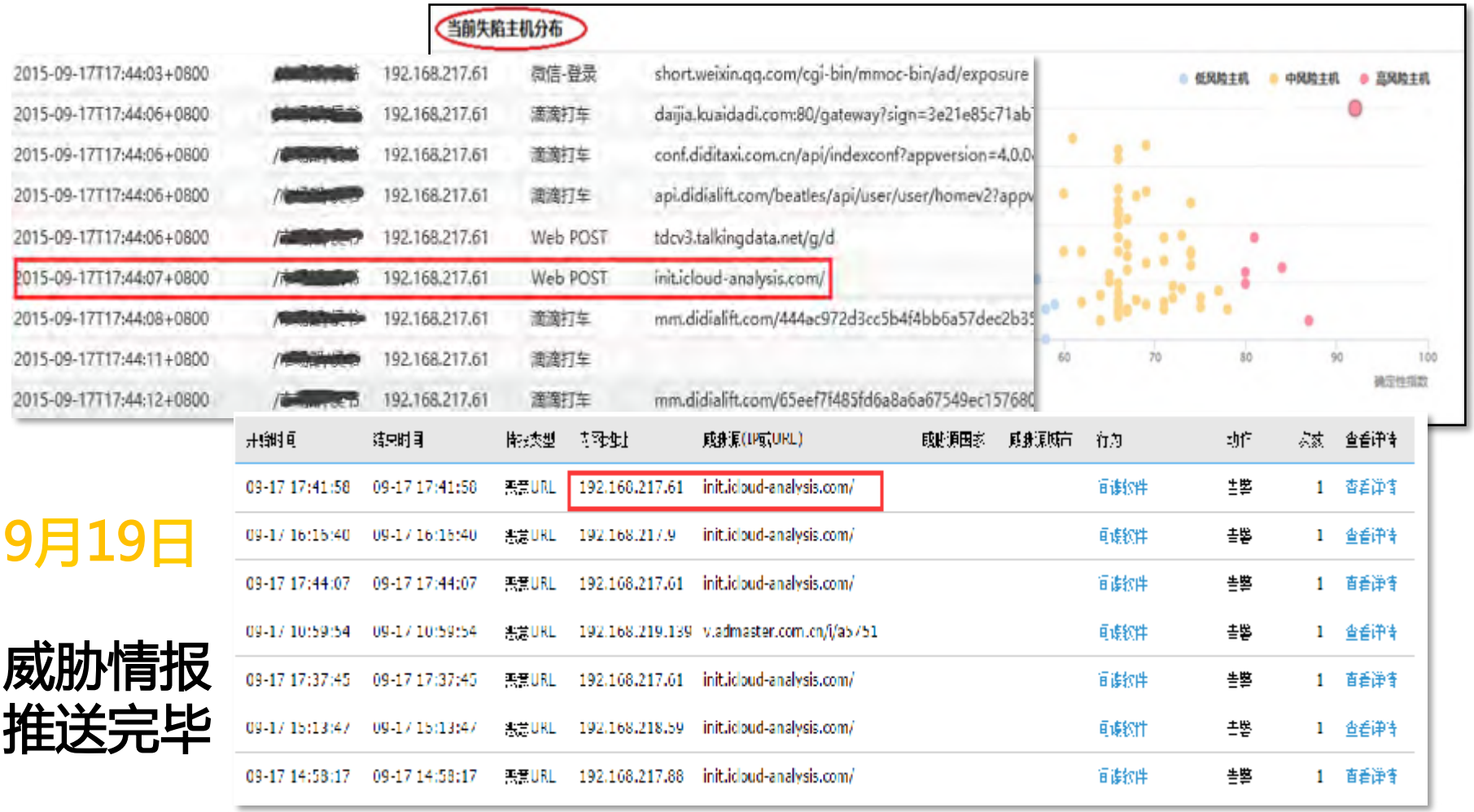
80亿 病毒文件样本 *1亿* 恶意网址

新威胁响应时间缩短至*15*分钟

在网络边界终止高级威胁

应用控制	阻断高危应用			拦截携带控制信令的未知应用	阻断业务需求外的应用访问
内容过滤	阻断恶意网址		拦截非法下载	拦截恶意网址和非法动态域名访问	
用户认证					访问行为实名审计
攻击防护		阻断攻击与渗透	拦截恶意文件	阻断间谍软件和信令传输	阻断跨域的渗透及恶意软件植入
全网可视					发现异常访问行为
外部智能	低信誉IP拦截		检测未知文件	阻断IP信赖库黑名单	主机威胁分析

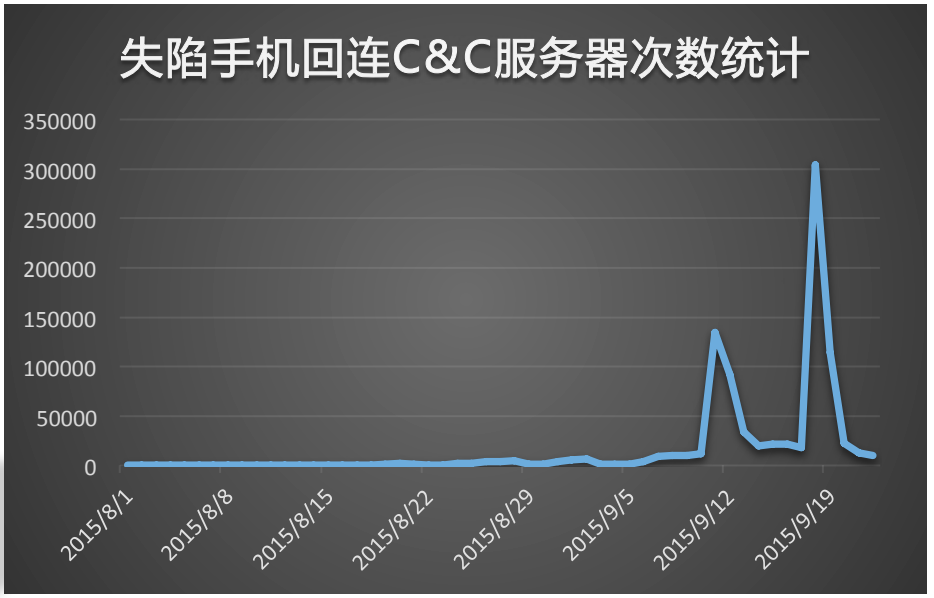
案例：XcodeGhost拦截及失陷手机检测

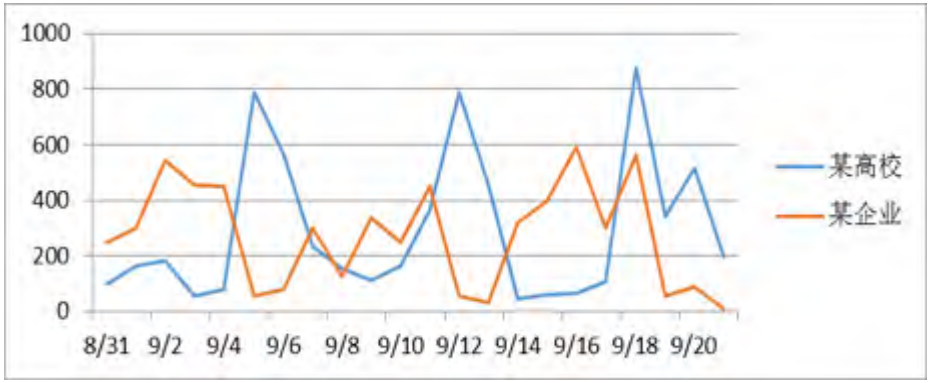


9月19日

威胁情报推送完毕

XcodeGhost 风波仍未平息





网康慧眼云，
仍然可以监测到，
大量的XcodeGhost回连C&C成功，
直到今天。。。。。。

IP地址已加入网康威胁情报库

总结：方案的价值提升

- 边界安全性大幅提升
- 全局可见性大幅提升
- 投资回报率大幅提升

THANKS

SequeMedia 盛拓传媒 | ITPUB