



第四届全国网络与信息安全防护峰会

安全威胁情报基础能力

薛锋

微步在线/ThreatBook

提纲

- ✧ 自我介绍
- ✧ 威胁情报
- ✧ 两个故事
- ✧ 基础能力

自我介绍

- ✦ 微步在线创始人、CEO。国内首个安全威胁情报公司
- ✦ 亚马逊中国首席安全官(CISO)
- ✦ 微软互联网安全战略总监
- ✦ 耐威实验室技术负责人
- ✦ 公安部

两个故事

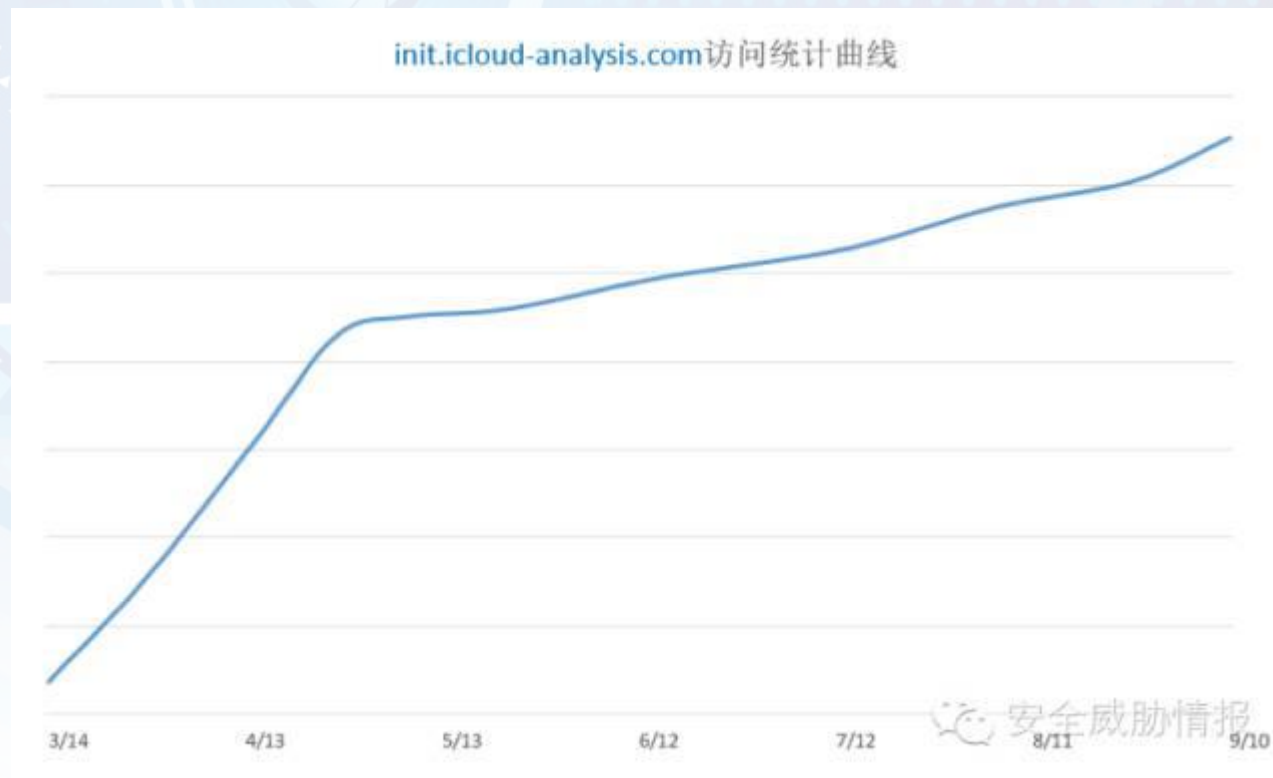
故事一：索尼



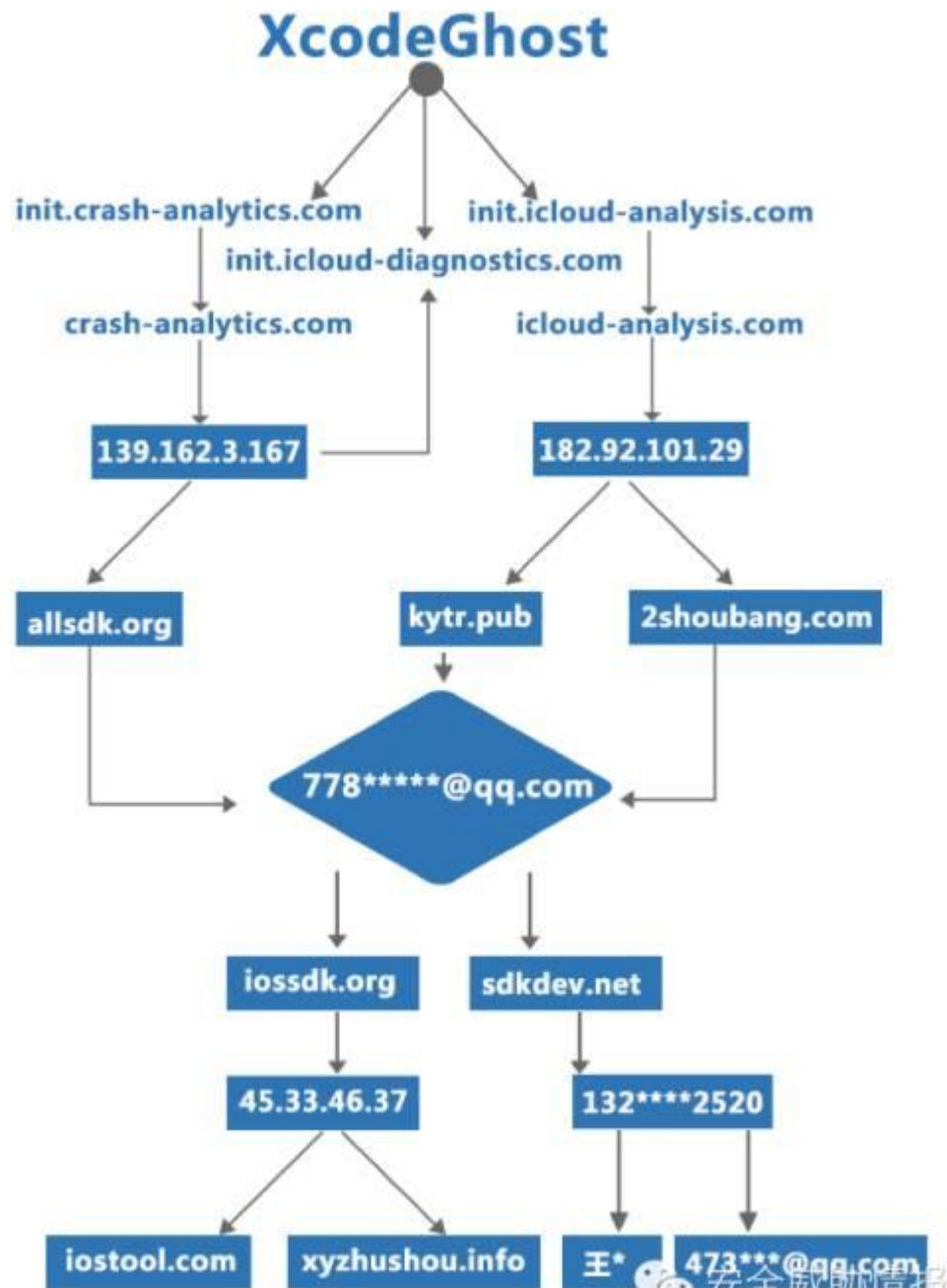
故事二：XcodeGhost



故事二：XcodeGhost



故事二：



故事二：XcodeGhost动机

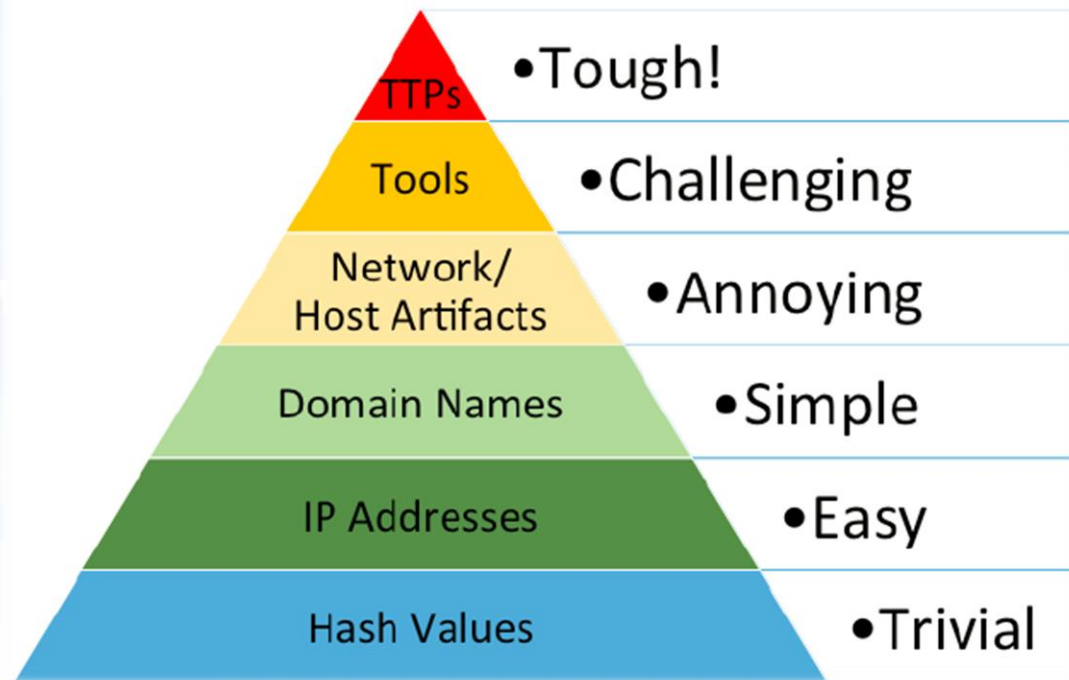
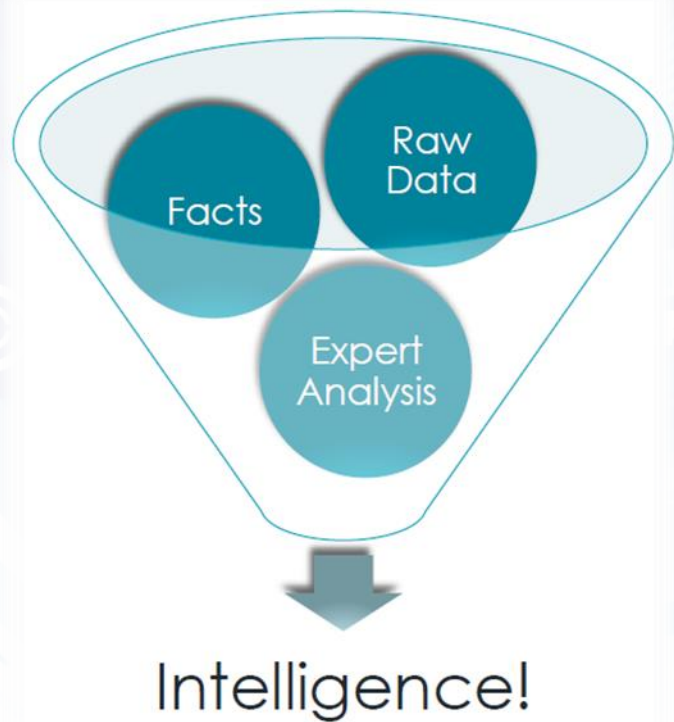
★ 疑点一：XcodeGhost 与 KeyRaider 的关系

8月，PaloAlto Networks 曾披露过代号为 KeyRaider 的恶意程序盗取了 225000 个 Apple 帐号，报告中提到 KeyRaider 曾向 icloud-analysis.com 发送信息

★ 疑点二：XcodeGhost 与流行的 PC 木马病毒 TrojanSpy 的关系

2015年3 至 9月 期间，与 XcodeGhost 相关的域名 icloud-analysis.com 和 allsdk.org 都曾指向 IP 地址 50.63.202.48，ThreatBook 通过威胁情报关联分析发现，同一时间段内超过七成的寄生于此 IP 地址的木马病毒属于 TrojanSpy 家族。

安全威胁情报



三大原则：防住、检测、保密

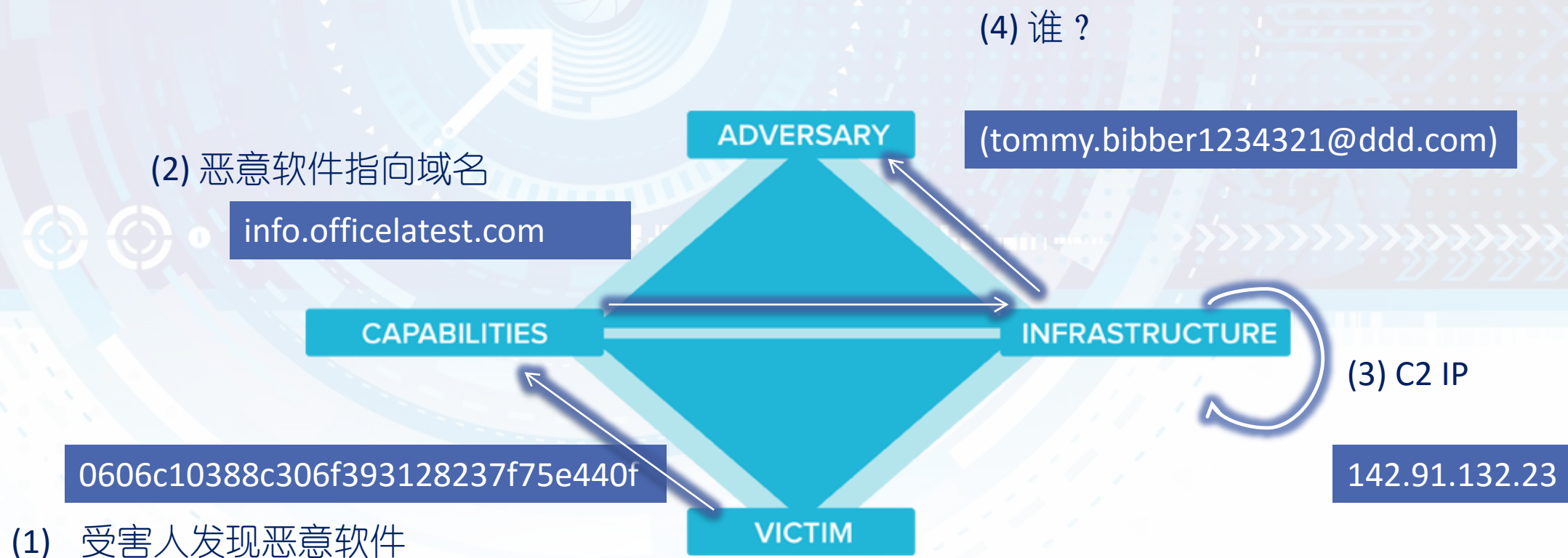
检测和响应

Detection and Response

知彼、知己



钻石模型

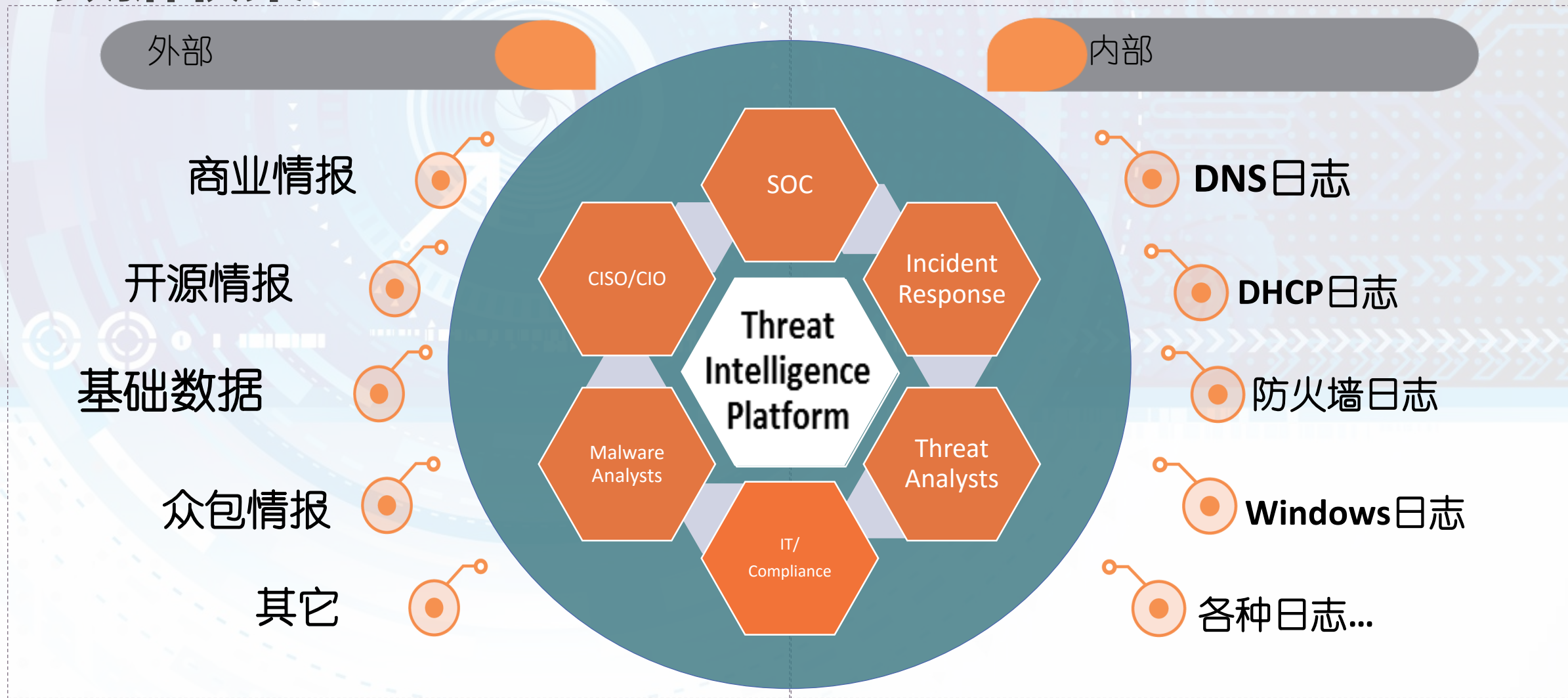


基础能力

数据

分析

数据收集



分析



安全分析云

VirusBook - 免费病毒、

+

← → ↻

🔒

virusbook.cn/view_report/scan/d4526f0710fa27504a66e61e67b74112ed0ecfa6347419d351961151cba232d5-1442149360910


📖 ☆

☰

🔗


🔔

⋮



Beta

云查杀 静态分析 动态分析



正在分析

SHA256 : d4526f0710fa27504a66e61e67b74112ed0ecfa6347419d351961151cba232d5

分析日期 : 2015-09-13 21:02:40 (6秒前)

云查杀: (还有 4 款引擎没有返回结果) (扫描队列长度: 1)

检出率: 7 / 8

反病毒软件	结果	病毒库日期
安天 (Antiy)	✓	2015-09-13
AVG	Trojan horse Generic_vb.HPF	2015-09-13
腾讯 (Tencent)	Win32.Trojan.Neurevt.Pezb	2015-09-13
百度 (Baidu)	Trojan.Win32.Neurevt.cna	2015-09-13
金山 (Kingsoft)	Win32.Troj.Neurevt.c	2015-09-13
趋势 (TrendMicro)	TROJ_NEUREVT.TUJ	2015-09-13
IKARUS	Trojan-Spy.Agent	2015-09-13
360 (Qihoo 360)	Win32/Trojan.Dropper.c04	2015-09-13

安全分析云

动态分析报告:

屏幕截图



安全分析云

网络分析

主机通信

IP地址	位置	经纬度
104.41.150.68	博伊顿	-78.3905101,36.665756
122.49.30.20	北京	116.3974589,39.9388838
8.8.8.8	GOOGLE	

DNS请求

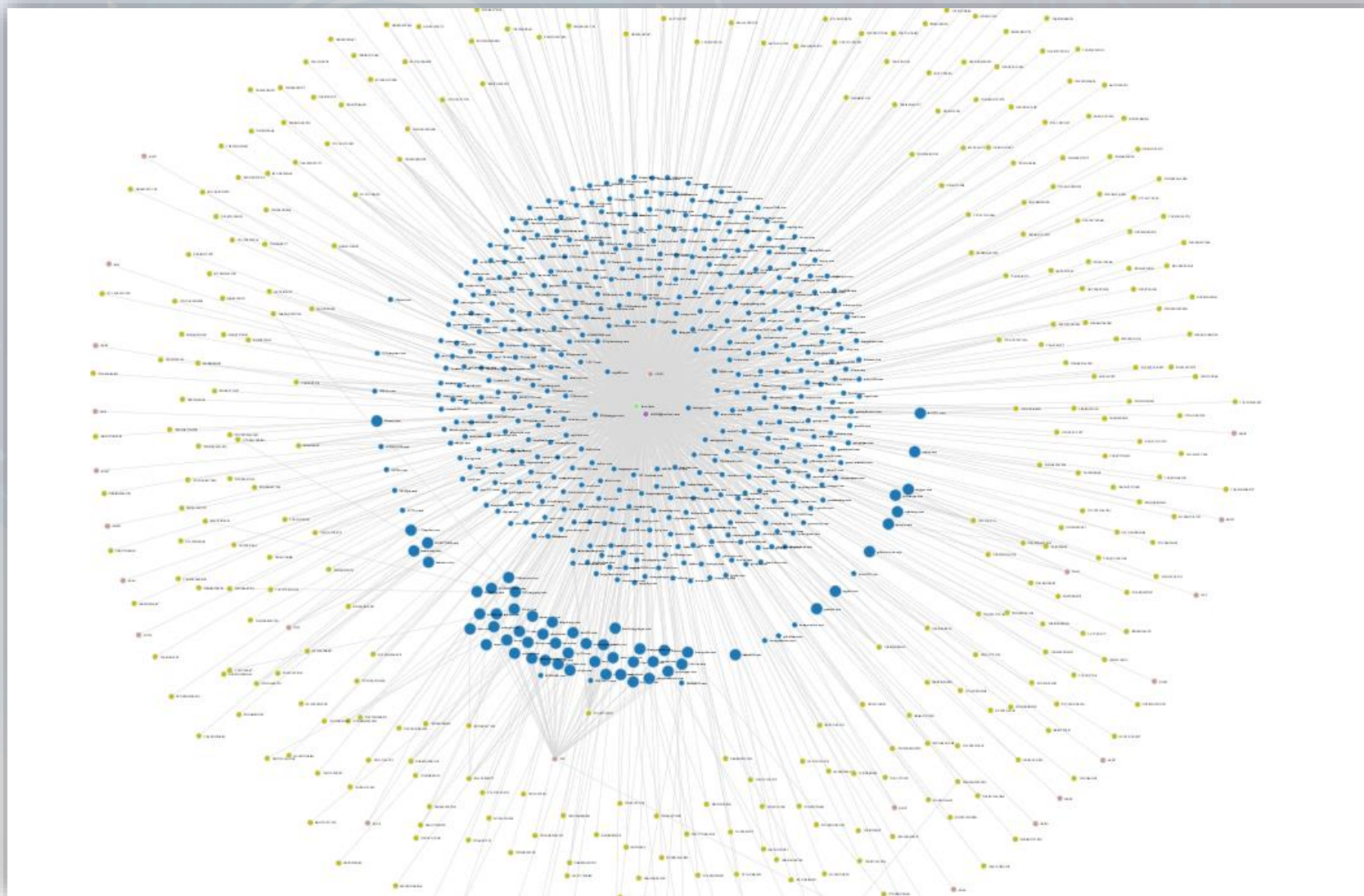
域名	IP地址	位置	经纬度
dns.msftncsi.com	131.107.255.255	美国	-89.143509,37.136162
teredo.ipv6.microsoft.com	94.245.121.251	都柏林	-6.286360,53.334129
asust.5i9u.com	122.49.30.20	北京	116.3974589,39.9388838

IP Connections
DNS

网络行为状态图



关联



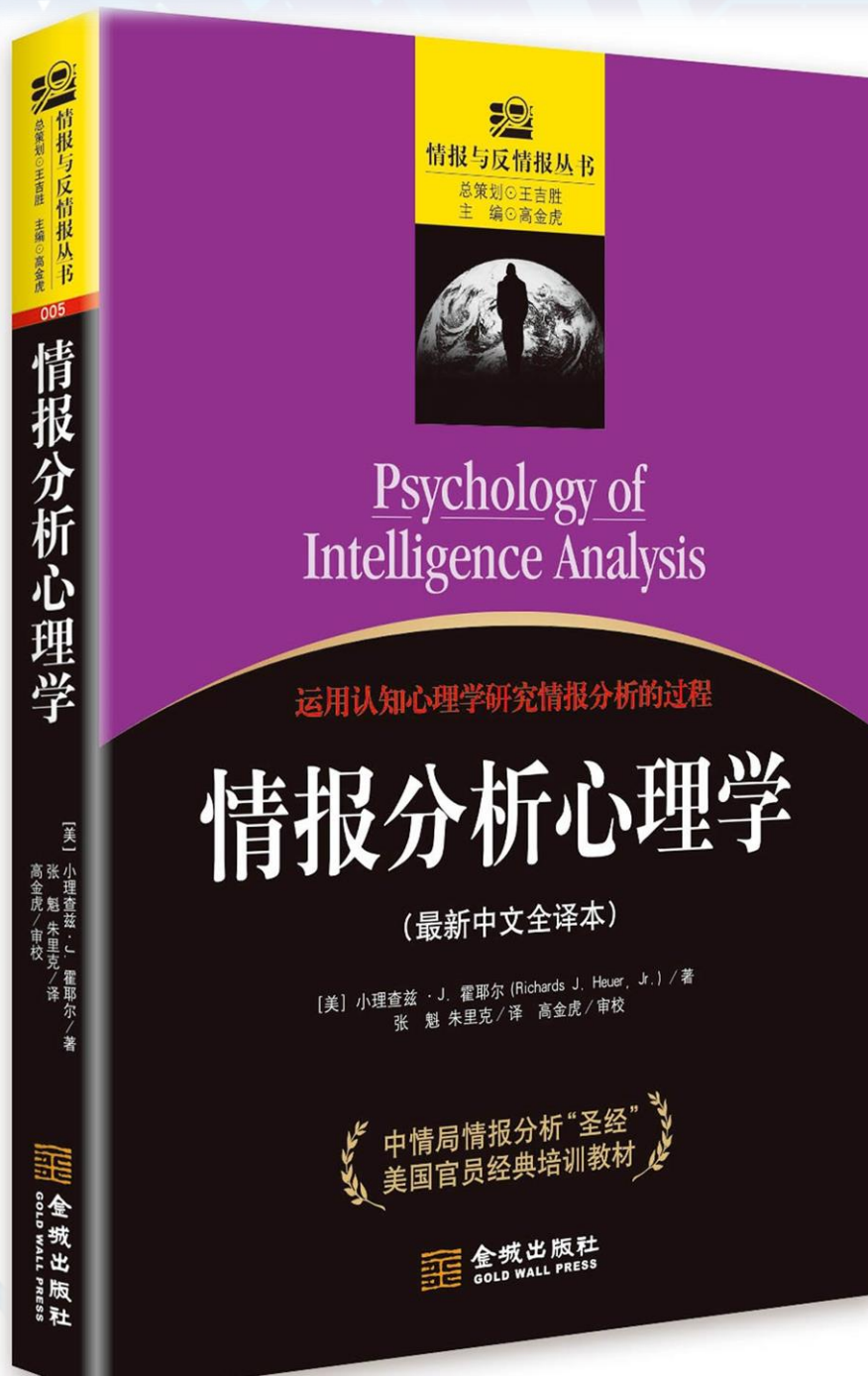
安全分析师



威胁情报分析现状

- ✦ 分析师需求增大
- ✦ 分析师人才短缺
- ✦ 缺乏高质量分析交流平台
- ✦ 缺乏优质威胁情报信息和基础资源共享
- ✦ 分析师缺乏分享动力

分析方法论-CIA





谢谢！

xuefeng@threatbook.cn

关注微博和微信公众号：**安全威胁情报**