

# 基于威胁情报的安全智能化

微步在线CEO - 薛锋

2017 | ThreatBook  
安全分析与情报大会

# 当前安全的挑战

## Challenges to Cybersecurity





**VS**





VS





VS

















人力有限、经验有限

有限的时间做迅速的响应

依赖有限的组织内外支持

手工操作与分析

资产不可见、攻击不可见

人

时间

资源

自动化

可见性



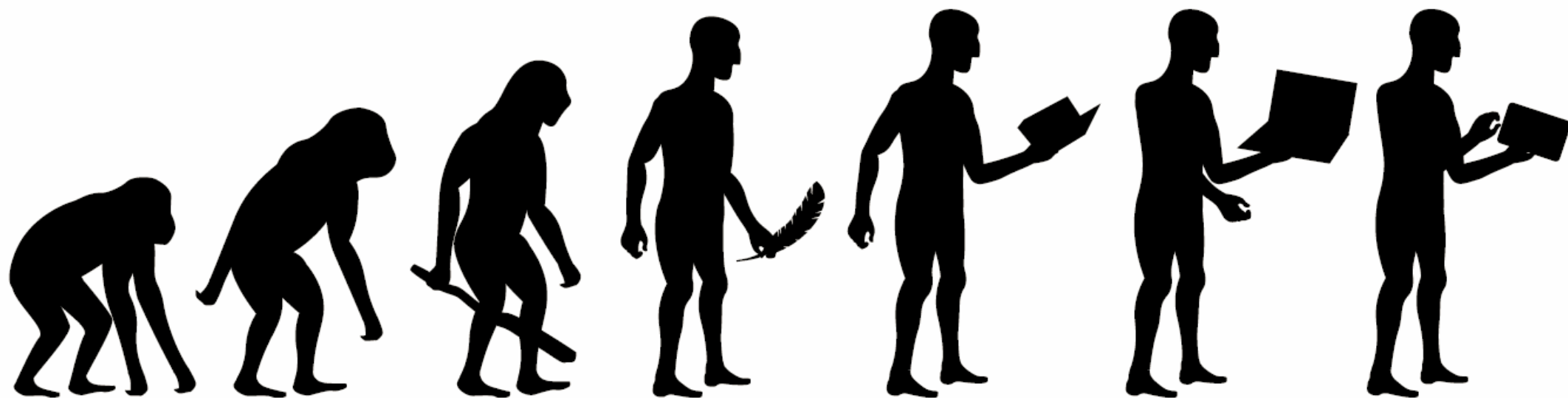
专业团队、团伙作战

充裕的攻击准备和移动时间

成熟的工具、服务支持

自动化的工具和流程

更了解组织的网络结构



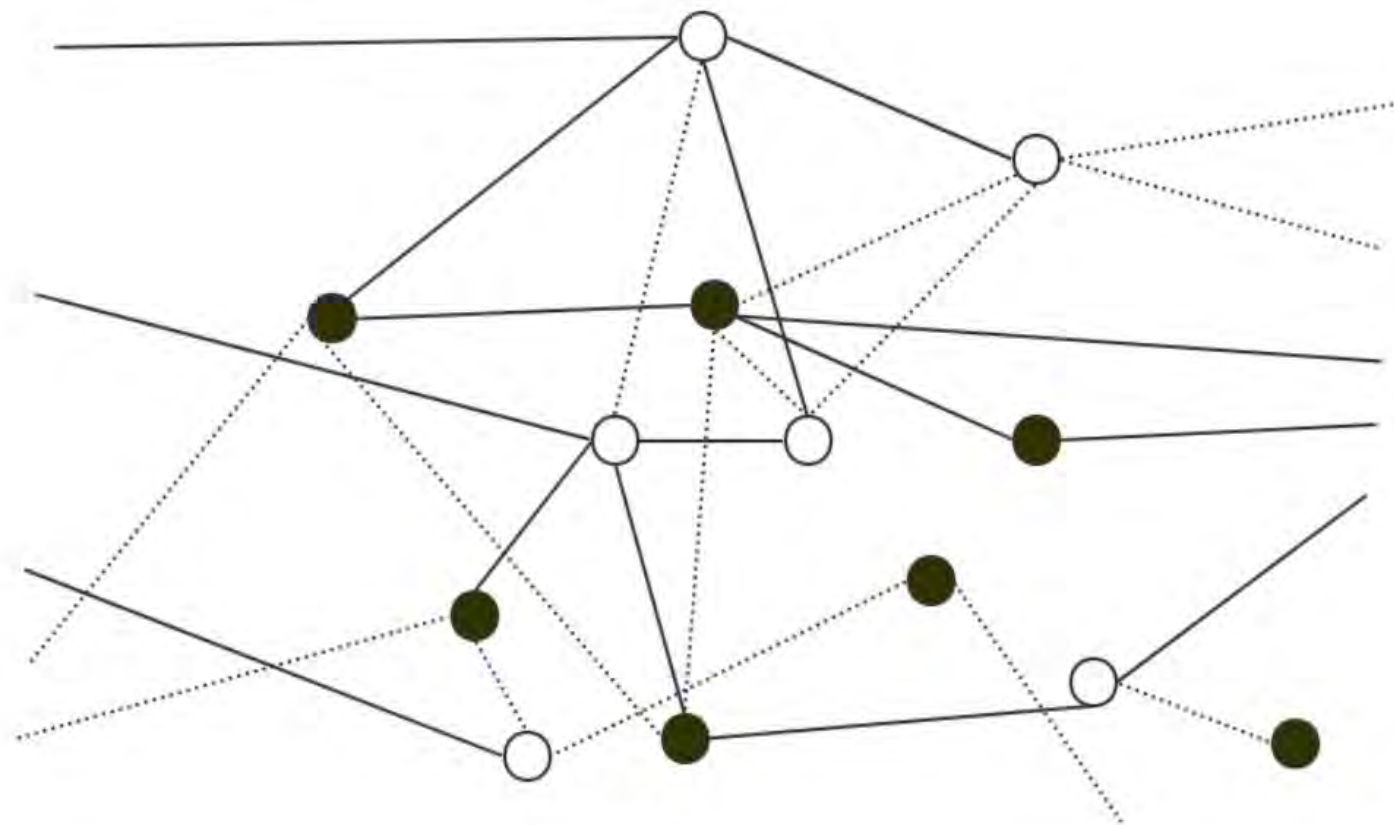
**威胁情报：从概念、落地到未来**  
Threat Intelligence: Zero to One





# 安全问题是数据问题 – 非对称

---



# 2015-2016，我们开始做威胁情报

反病毒软件	结果	病毒库日期
火绒 (Huorong)	HEUR:VirTool/Obfuscator.genB	2017-10-04
Avast	Win32:Evo-gen	2017-10-04
瑞星 (Rising)	Trojan.GenKryptik!8.AA55	2017-10-04
Baidu	Win32.Trojan.WisdomEyes.151026.9950.9984	2017-10-04
IKARUS	✓	2017-10-04
腾讯 (Tencent)	✓	2017-10-04
小红伞 (Avira)	✓	2017-10-04
Sophos	✓	2017-10-04
Kaiwei	✓	2017-10-04
百度国际版 (Baidu-International)	✓	2017-10-04
K7	✓	2017-10-04
熊猫 (Panda)	✓	2017-10-04
NANO	✓	2017-10-04
大蜘蛛 (Dr.Web)	✓	2017-10-04

## 把概念落地为数据


1. 对威胁事件的关注，对黑客团伙，攻击者工具、手段、资产的分析；
2. 对威胁分析需要的大量基础数据的收集、整理与清洗。  
形成了我们最开始做威胁情报的初始动力。


# 2016-2017：企业威胁情报落地

 **iSOC**  
(Intelligence-Driven Security Operation Center)

  
**威胁情报云**  
-----  
**威胁情报管理平台**  


**TIP-威胁检测与响应平台**

 **NTA**  
(Network Traffic Analysis)

 **EDR**  
(Endpoint Detection and Response)

 **各类安全设备**  
( WAF\IPS\NGFW )

 **应急响应服务**



# 未来：情报驱动安全智能化

威胁情报数据 → 检测&响应场景中落地 → 驱动安全智能化



# 情报驱动的安全智能化路径

The Way to Security Intelligence driven by TI







# 威胁情报：安全智能化中的Echo

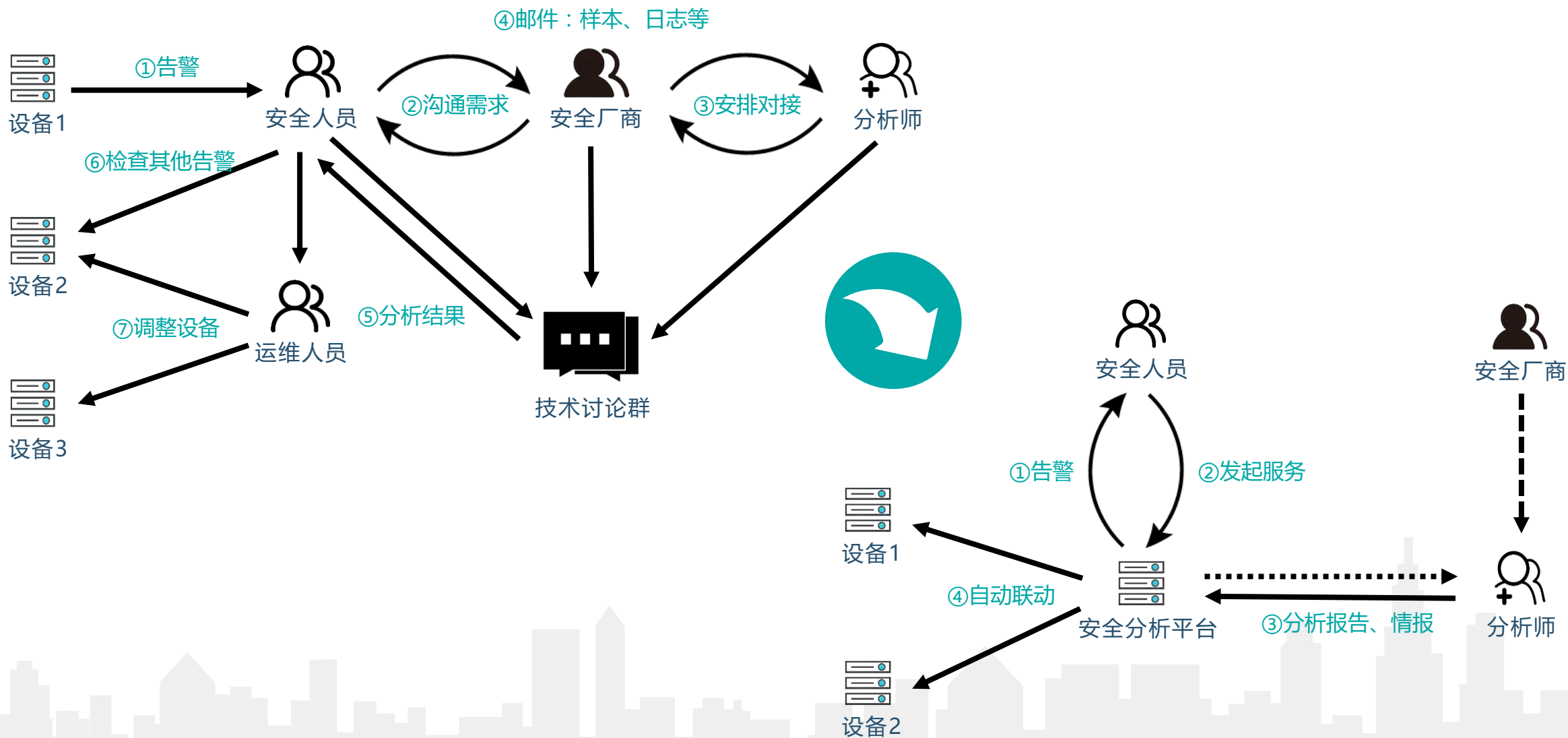


Amazon Echo



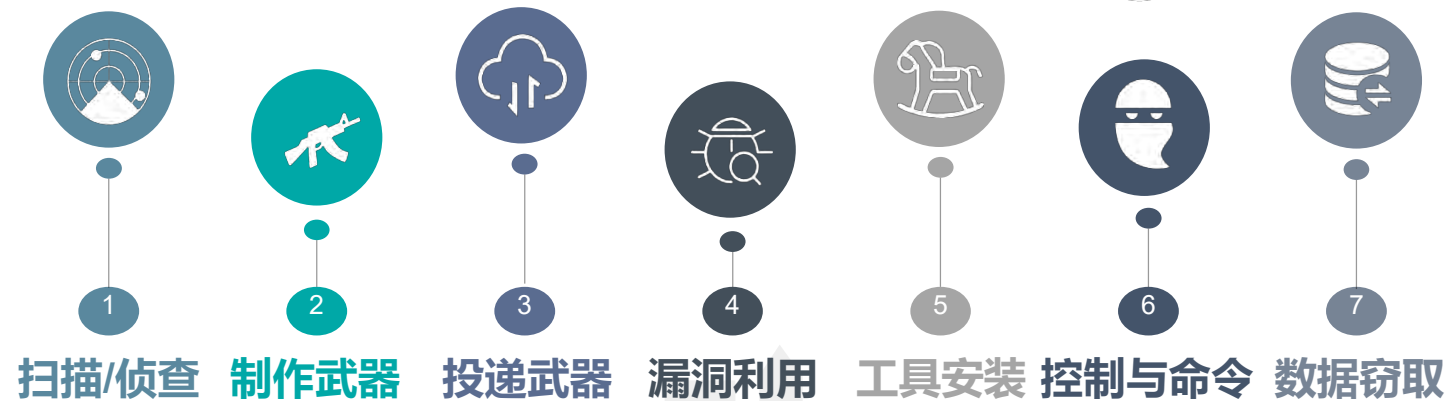
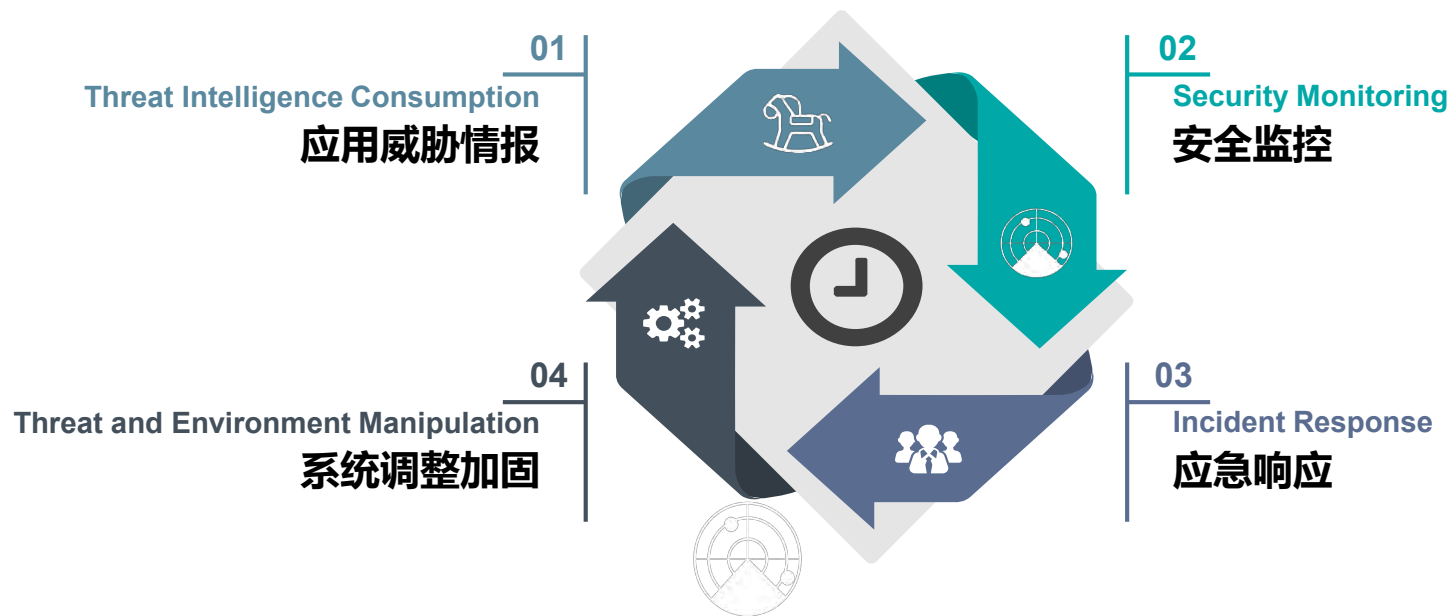
Threat Intelligence

# 自动化流程与设备联动：提升效率与现有设备ROI



# 使用和积累情报

主动防御模型



攻击杀伤链



# 主动防御(Active Defense Cycle)

**01**  
Threat Intelligence Consumption  
应用威胁情报

**02**  
Security Monitoring  
安全监控

**03**  
Incident Response  
应急响应

**04**  
Threat and Environment Manipulation  
系统调整加固



# 主动防御模型案例：WannaCry

微步在线：国内首家发布WannaCry秘密开关的威胁情报报告

```
{“ioc”：“www.aaylmaotjhsstasdfasdfasdfasdfasdf.com”,  
“related_samples”:[“22ccdf145e5792a22ad6349aba37d960db77af7e0b6cae826d228b8246705092”],  
“patches”:[“CVE-2017-0144”]}
```

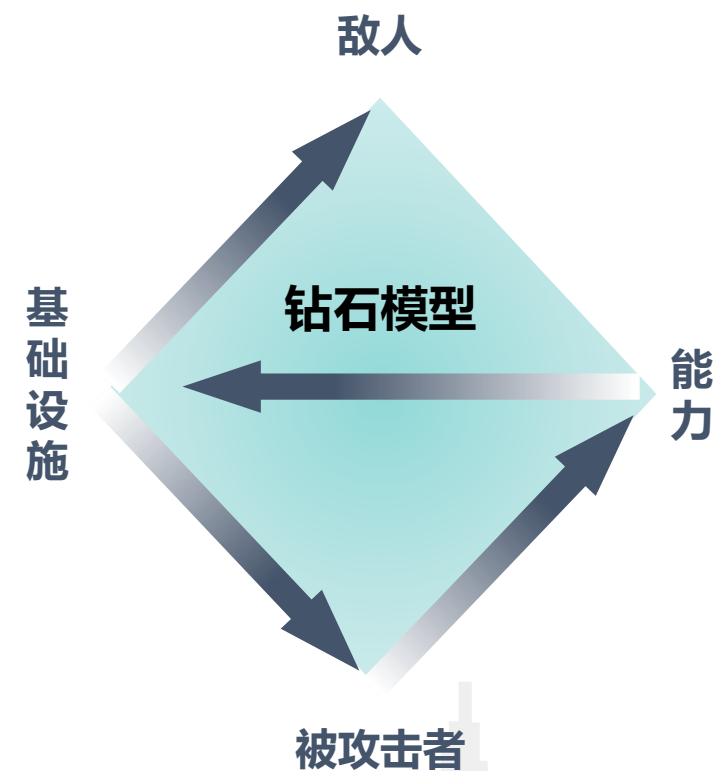
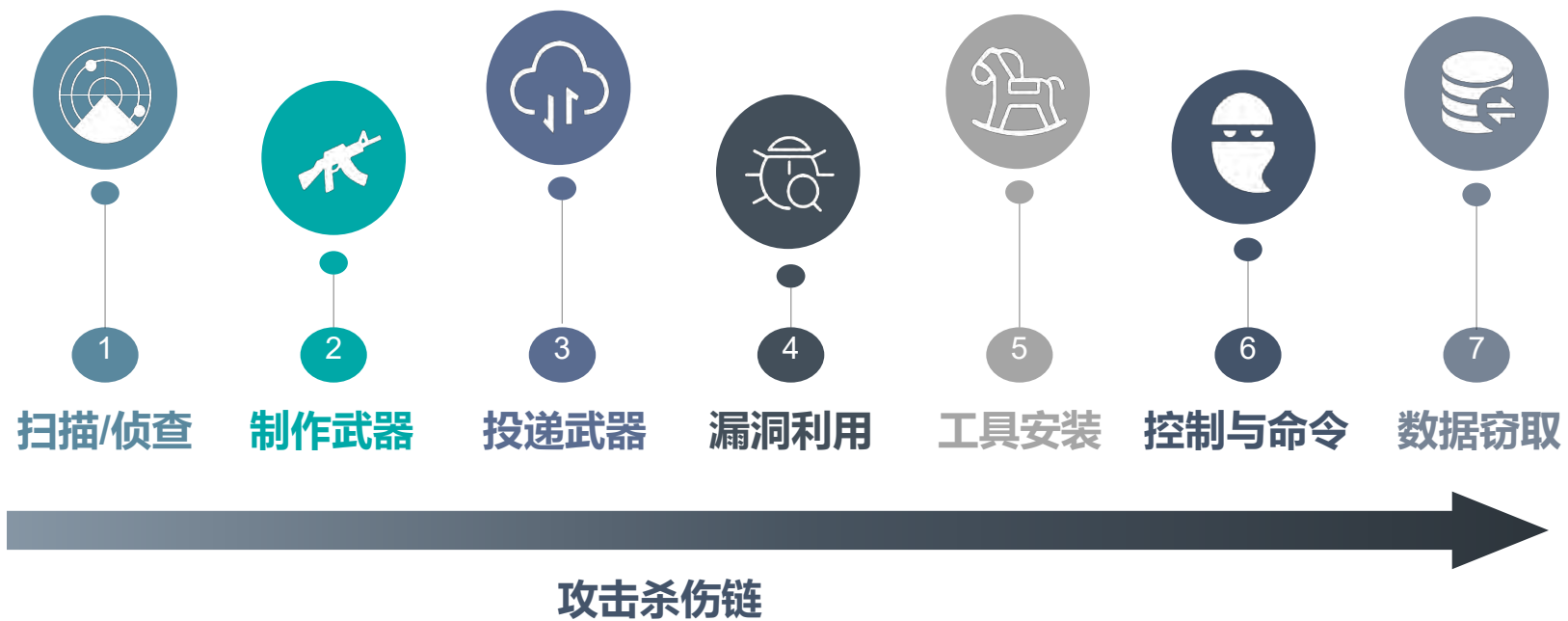


The infographic features a dark red background with a large, semi-transparent 'WannaCry Ransomware Attack' title. On the right side, there is a circular graphic composed of many small white dollar signs (\$). Below the title, there are three vertical panels, each with an icon and a title. The first panel has a server rack icon, the second has a database icon, and the third has a computer monitor icon. The text in each panel describes a specific active defense capability.

全面监控与检测	快速响应	自动联动修复
用户应用开关域名 (IOC) 进行全面的失陷检测	应用配置DNS解析的方式保护主机达数百万台	应用情报中的CVE标识自动联动终端管理进行补丁修复

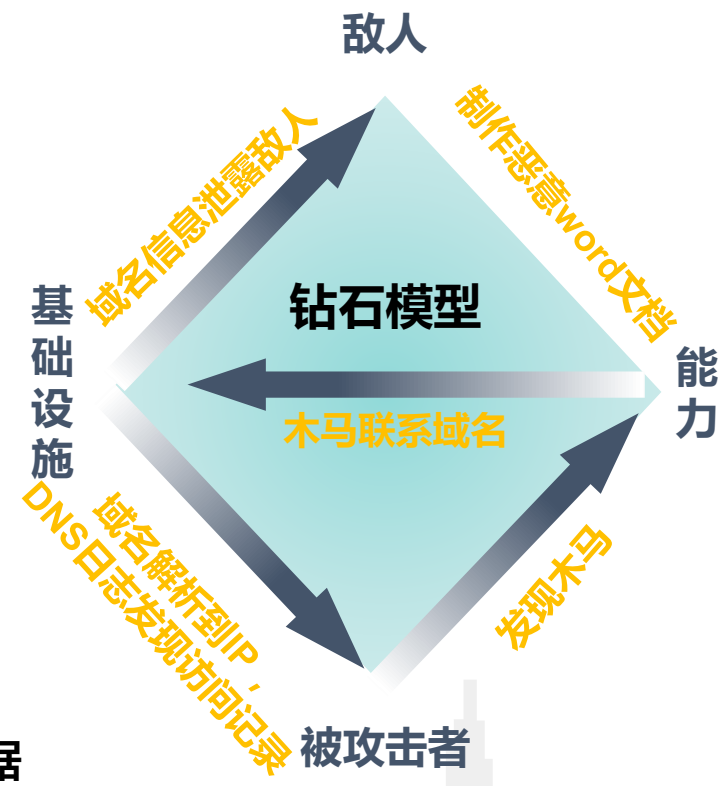
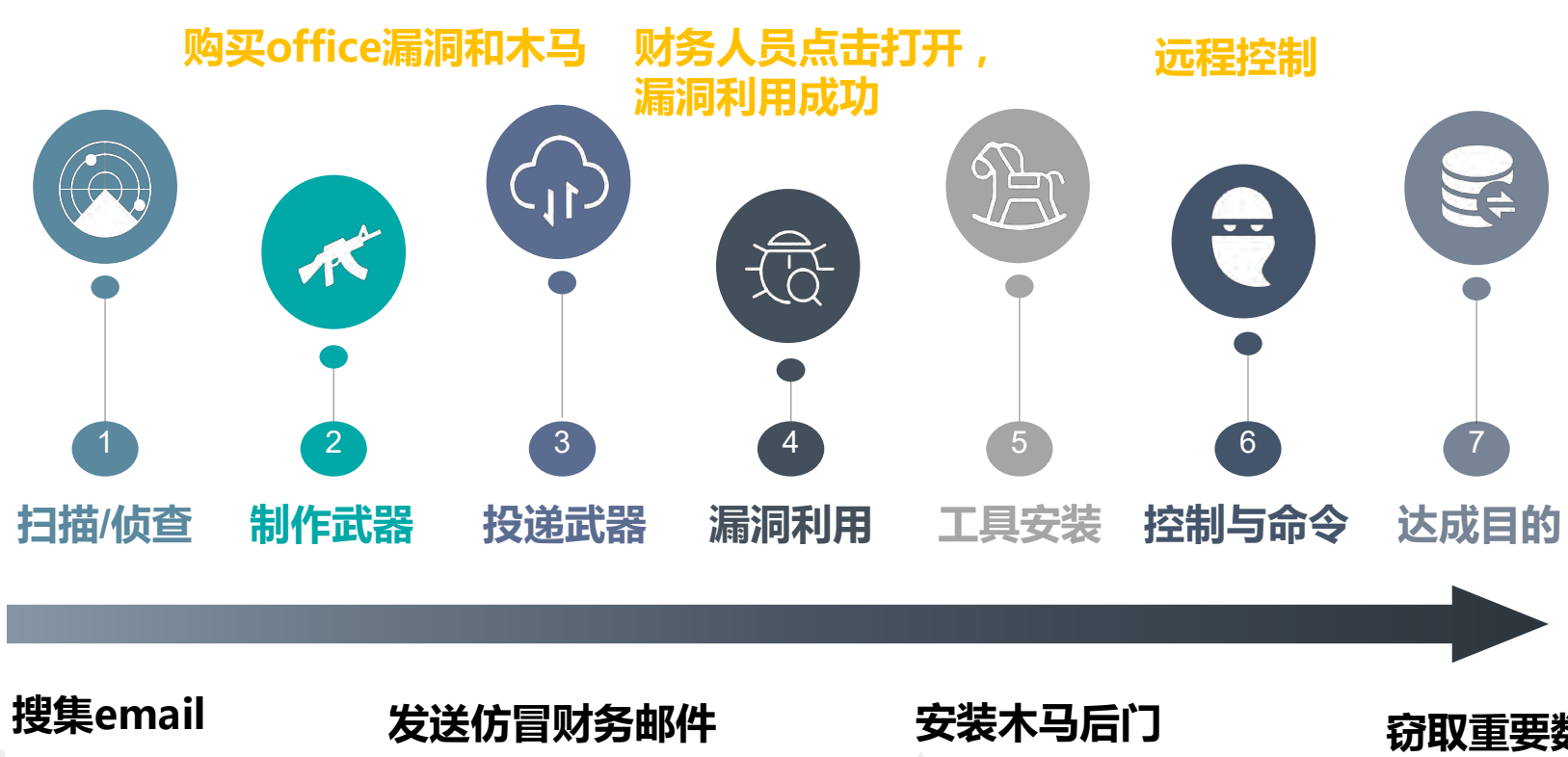


# 情报积累



# 情报积累样例

挑战：如何管理，如何长期、自动跟踪？



# 微步在线进展

ThreatBook



## 微步在线两年半以来...

1.65亿



2017年完成B轮融资

北极光、如山创投、  
高瓴资本等

70人



专注于威胁情报的=数据与产品

亚马逊、微软、百度、美  
团、阿里巴巴等

第1位

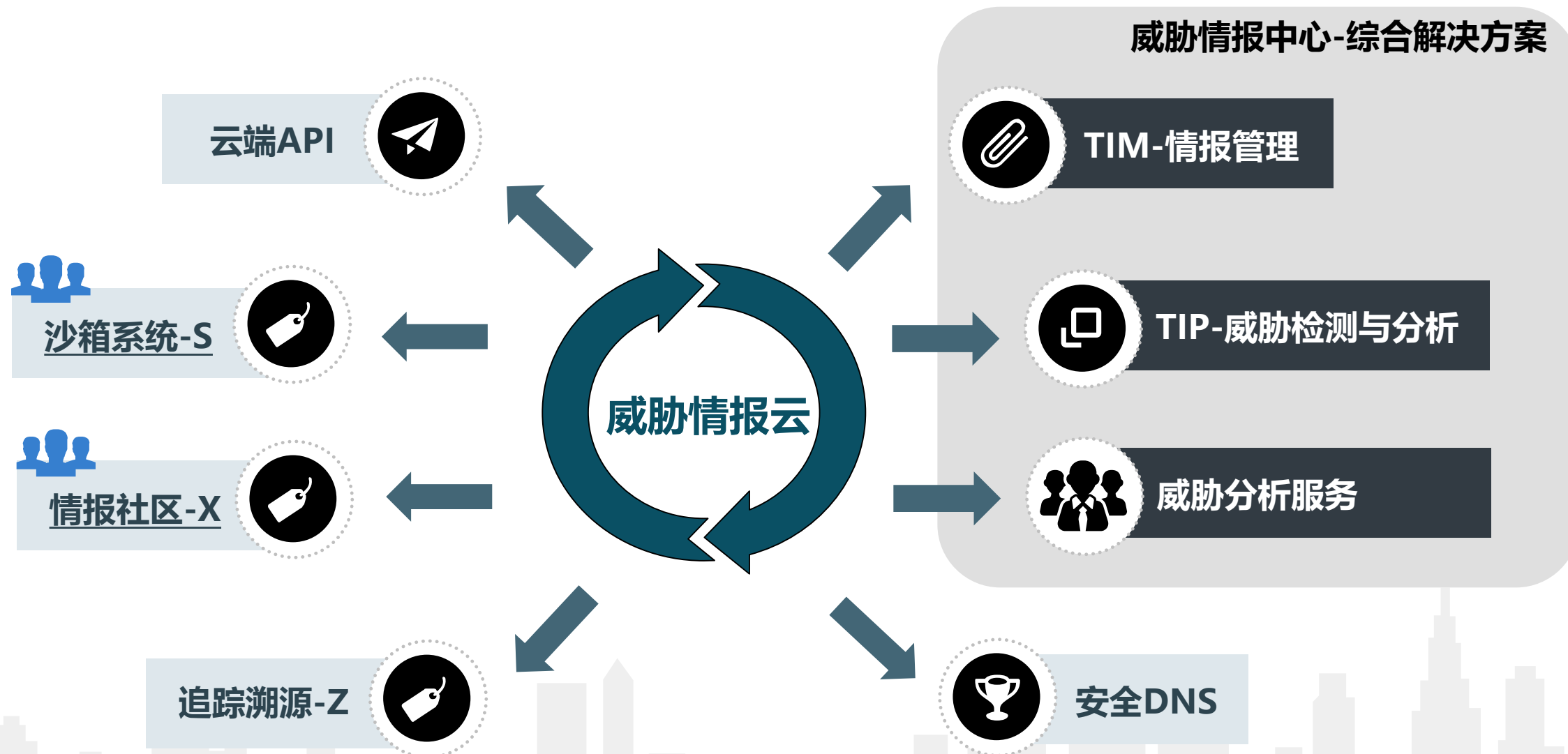


唯一入选Gartner威胁情报市场指南

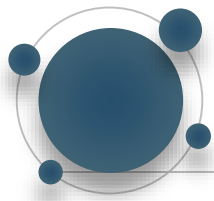
服务国内超过200家企业，金  
融、能源、互联网、政府

入选全球网络安全500强的9家中国公司之一

# 微步在线产品和服务







# 威胁情报云

## 威胁情报IOC

- **30万** 高可信IOC
- **42亿** 全球IP信誉与标签
- **分钟级** 数据更新

## 网络基础数据

- **7年** Passive DNS数据
- **16年** 域名Whois信息
- **数百万** 每日新增域名

## 黑客画像

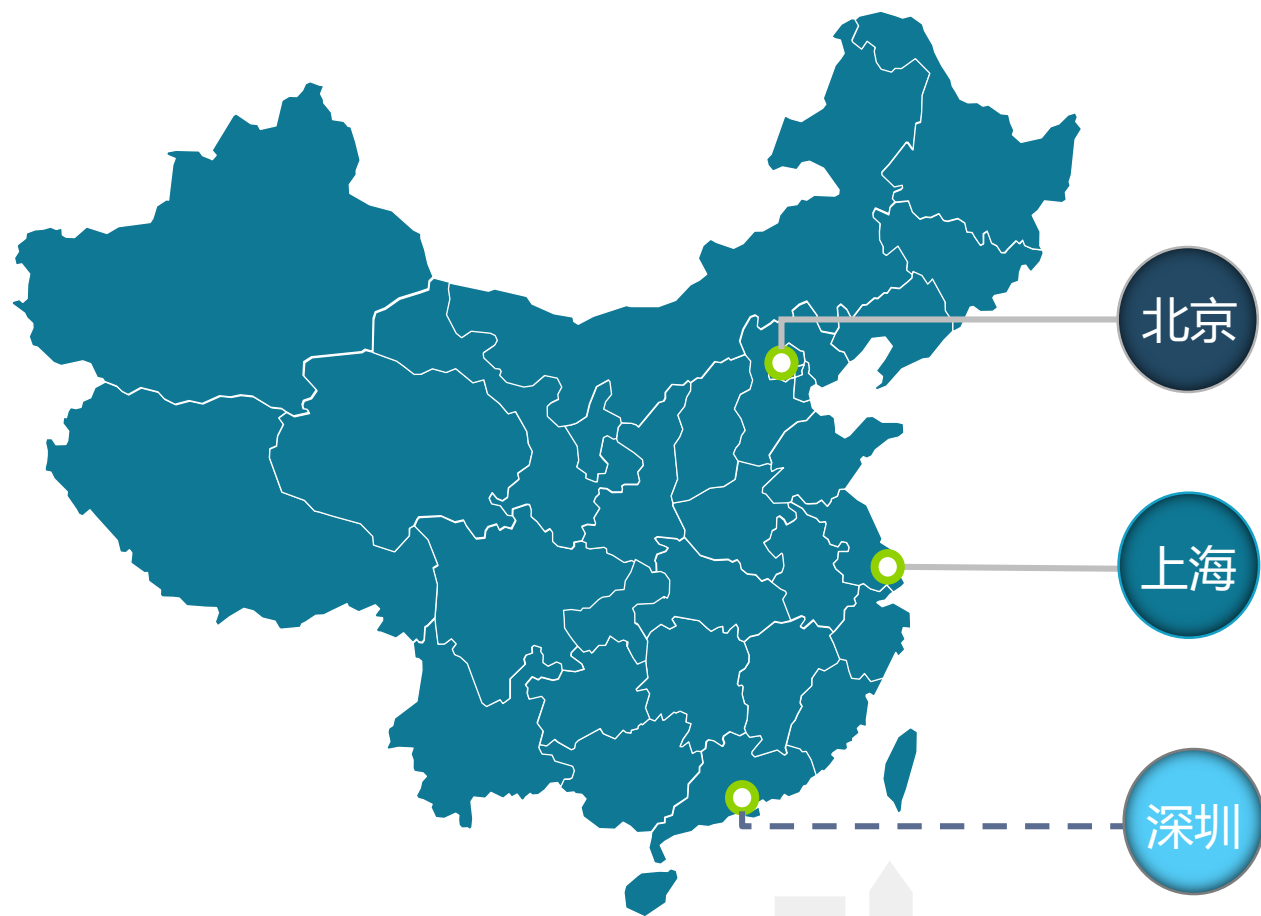
- **上百个** 全球黑客组织
- **小时级** 全球事件跟进
- **数万条** 关联IOC

## 动态沙箱与多引擎

- **百万级** 每日新增样本
- **30+** 知名防病毒引擎
- **千核** 云端沙箱(Windows、Linux)

威胁情报云

# 微步在线欢迎优秀的人才加盟



*Now this is not the end.*

*It is not even the beginning of the end.*

*But it is perhaps the end of the beginning.*

这不是结束，甚至不是结束的  
开始，而仅仅是开始的结束。

-丘吉尔



# 谢谢

安全智能 情报驱动

微步在线

[www.threabook.cn](http://www.threabook.cn)

[x.threatbook.cn](http://x.threatbook.cn)