

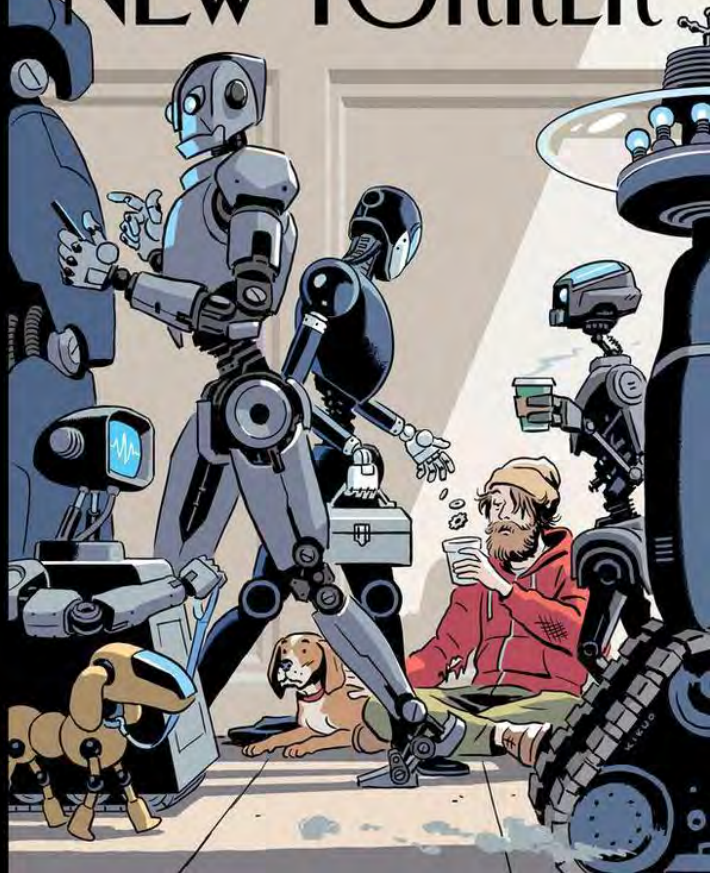


浅析安全威胁发展与情报态势感知技术 推进实时防御和超前防御理念

杜建峰

大中国区安全咨询

Nov 29, 2017, Beijing

THE
NEW YORKER

Cyber Time's

.....

第一章：安全威胁的快速发展和挑战

第二章：新一代智能威胁态势感知技术

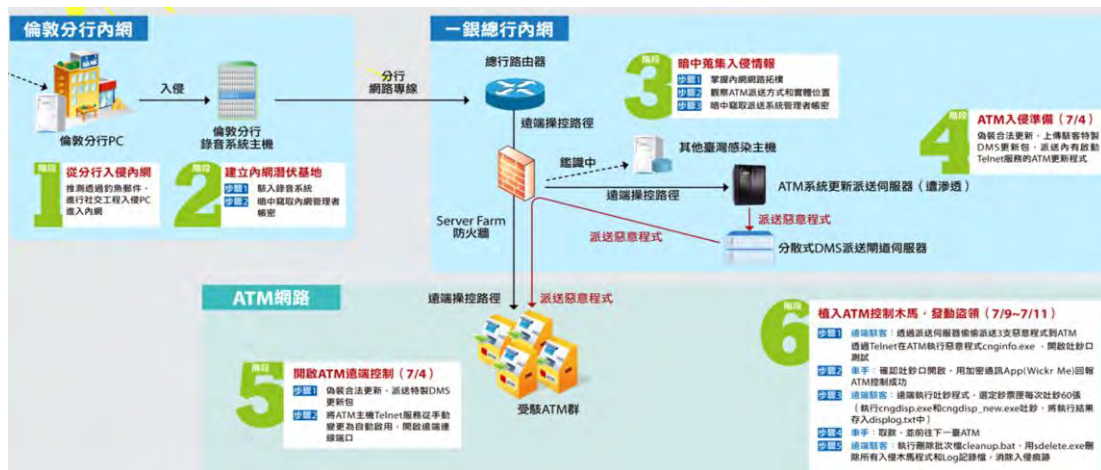
第三章：推进实时和超前防御技术理念

2016全年及2017年上半年全球安全大事件

- 2月，SWIFT黑客事件爆发 多家银行损失巨款 / 零日漏洞和恶意木马软件
- 4月，德国核电站检测出恶意程序被迫关闭 / SCADA/ICS 工业自动化恶意软件攻击
- 6月，全球银行业使用的恐怖嫌疑人数据库被泄露 / 数据泄漏
- 8月，美国国家安全局陷入斯诺登之后最大泄密风波 / 数据泄漏 + “源代码” 零日
- 9月，雅虎曝史上最大规模信息泄露 5亿用户资料被窃 / 数据泄漏
- 10月，希拉里邮件门事件发酵 / 数据泄漏
- 10月，美国遭史上最大规模DDoS攻击、东海岸网站集体瘫痪 / DDOS拒绝服务攻击 + IoT
- 11月，旧金山地铁被勒索软件攻击 乘客免费乘坐地铁 / 勒索软件
- 11月，德国90万家庭断网 遭黑客蓄意入侵 / 互联网攻击
- 12月，俄罗斯中央银行约3100万美元被盗等事件 / 凭证窃取 + 第三方
-
- 3月，维基解密公布揭秘了中情局CIA关于黑客入侵技术的最高机密 / IoT和移动端攻击
- 4月，影子经纪人公开NSA（美国国家安全局）黑客武器库 / 十款零日攻击工具
- 5月，“WannaCry” 敲诈勒索病毒5月12日在全球爆发. / 勒索病毒+零日
- 6月，新一轮勒索病毒“Petya” 来袭 / 勒索病毒 + 零日
-

➤ 台灣第一銀行ATM入侵盜領案

2016年7月9日至10日期間（週末），來自於包括俄羅斯的十多名領錢的車手們，分別於第一銀行台中和台北等22間分行、41台ATM自動提款機，總共從ATM盜領8,327萬元。



釣魚郵件先由外網引誘倫敦分行內部員工感染惡意程式->黑客入侵倫敦分行內網->滲透入侵台灣一銀總行內網->潛伏收集情資->掌握ATM程序更新機制DMS，並竊取系統管理者帳號及密碼->偽裝合法更新程序包，派送至各台ATM自動開啟遠端控制->作案期間待車手通知執行惡意程序開啟吐鈔（每次60張）->完成後執行sdelete程序刪除所有入侵木馬程序及Log日誌記錄檔

➤ 2017-5-12 WannaCrypt攻击及感染过程

STEP 1-2: 初始投放



STEP 1
通过钓鱼邮件发送给
受害者具有恶性性质
的URL/PDF/HTA



STEP 2
欺骗用户点击URL链接
或打开附件，完成

两个关键点：

1. 利用漏洞来实施攻击
2. 成功利用漏洞后，通过漏洞分发恶意软件

STEP3-5: 蠕虫大规模传播

STEP 3
WannyCrypt在本地被运行，
开始执行后续攻击过程



STEP 5-1
扫描本地局域网中的IP地址，通
过“永恒之蓝”攻击SMB漏洞



STEP 5-2
生成随机互联网IP地址，通过
“永恒之蓝”攻击SMB漏洞

STEP 4
执行本地
用户文件的加密勒索攻击

网络攻击正在进化

■ 攻击者正在改变

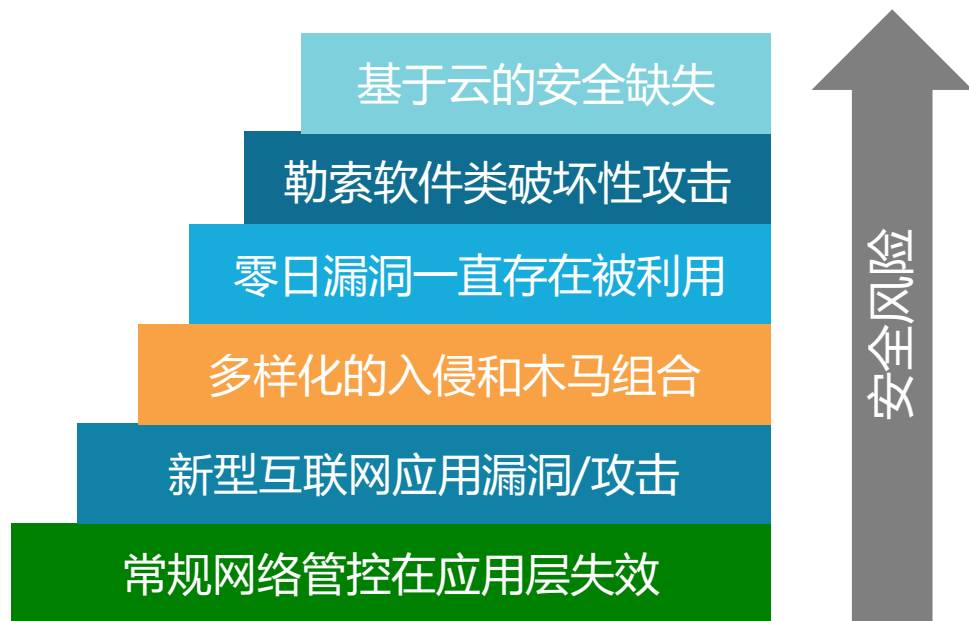
- 有组织的犯罪机构
- 有经济 / 政治目的的犯罪
- 大规模破坏性攻击

■ 攻击策略正在演进

- 更有耐心, 层层推进
- 从不起眼的用户入手
- 针对性的目标

■ 攻击技术愈发先进

- 利用新的应用逃避检测
- 使用零日类攻击躲避传统的签名类检测
- 隐藏和C2服务器的通讯

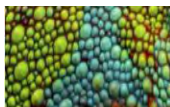




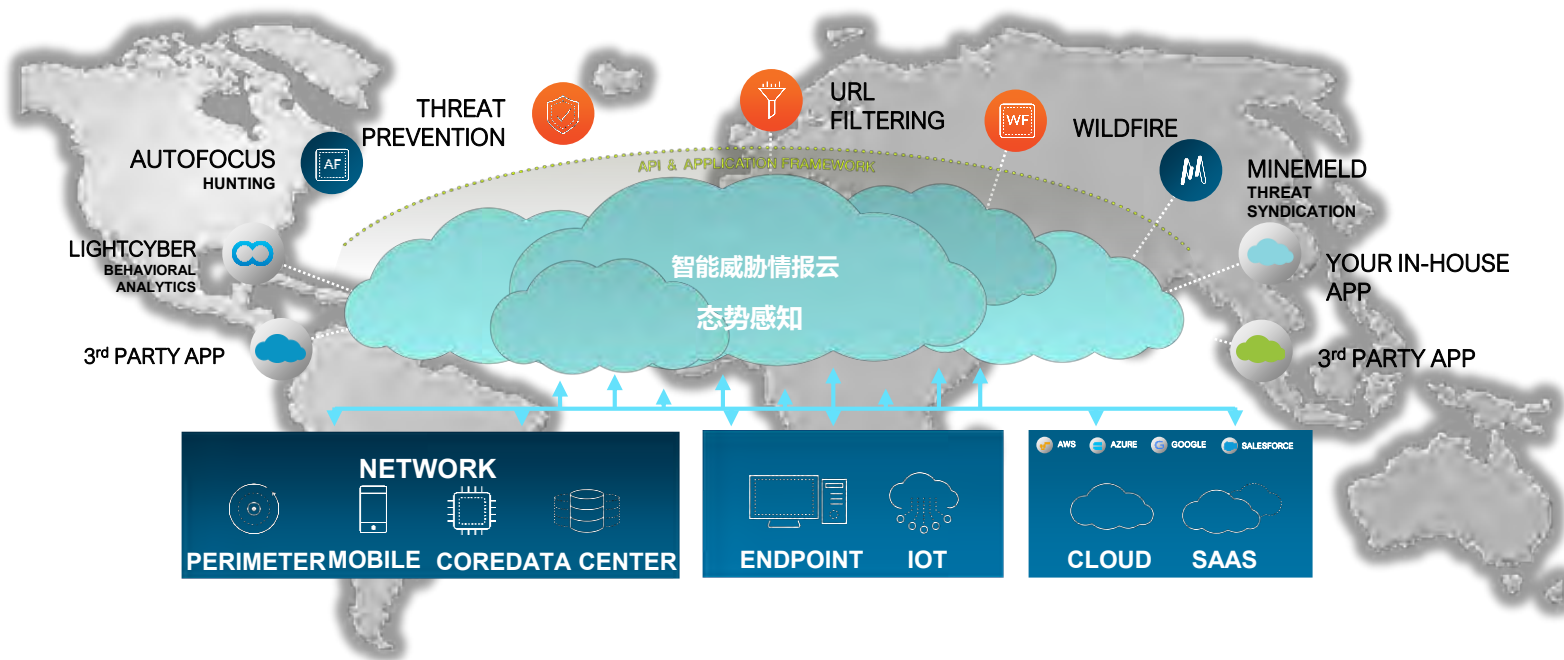
新一代智能威胁态势感知技术和利用



我们的方法: 首先要可见、关联性和洞察全局



构建全球化的安全威胁情报态势感知智能云

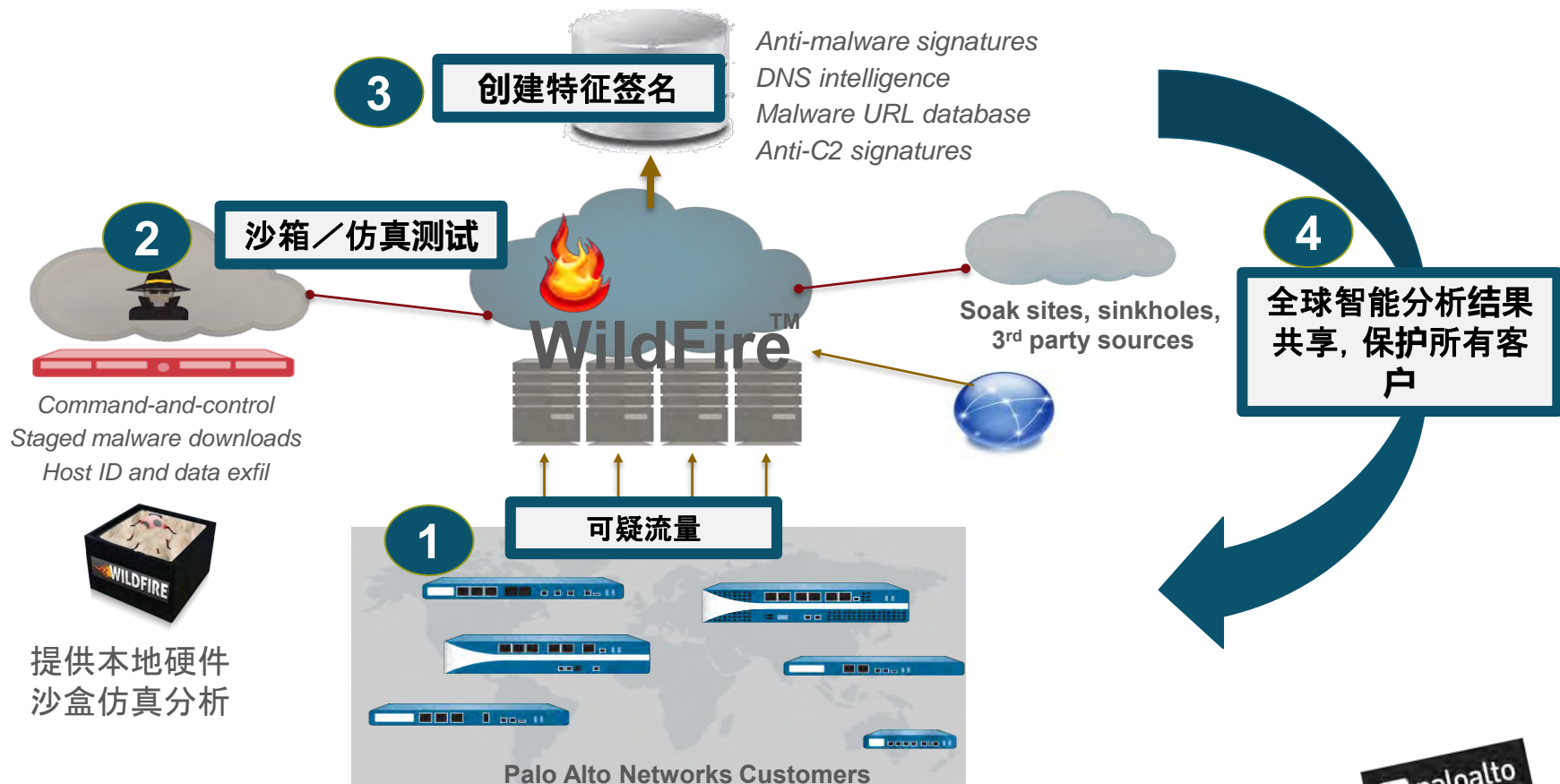


全球布局覆盖采样

智能分析和实时交互

开放给第三方交互

具体实现 - 发现并阻止0-day和未知威胁



安全大数据的挖掘与利用

态势感知，可操作的威胁情报



unit42

AUTOFOCUS™

识别



独特的，有针对
性的攻击

上下文



攻击，
活动，技术

分析



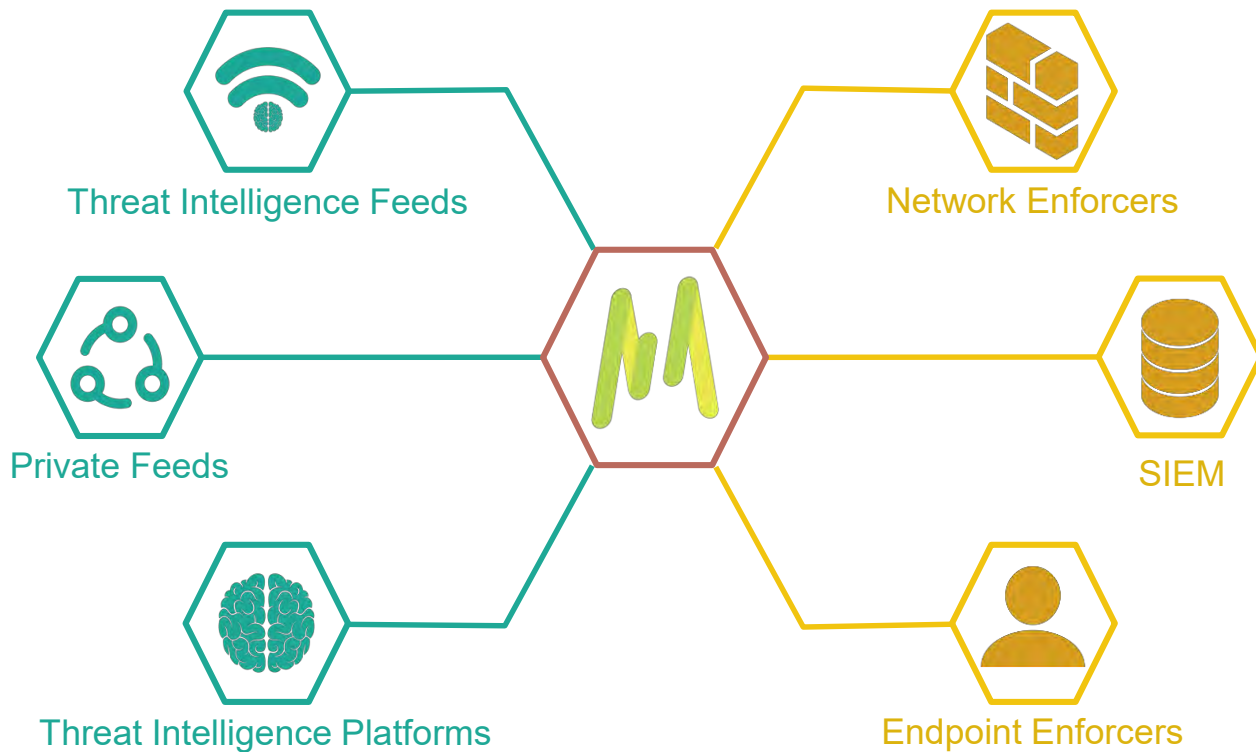
关联全球和本地
威胁情报

保护

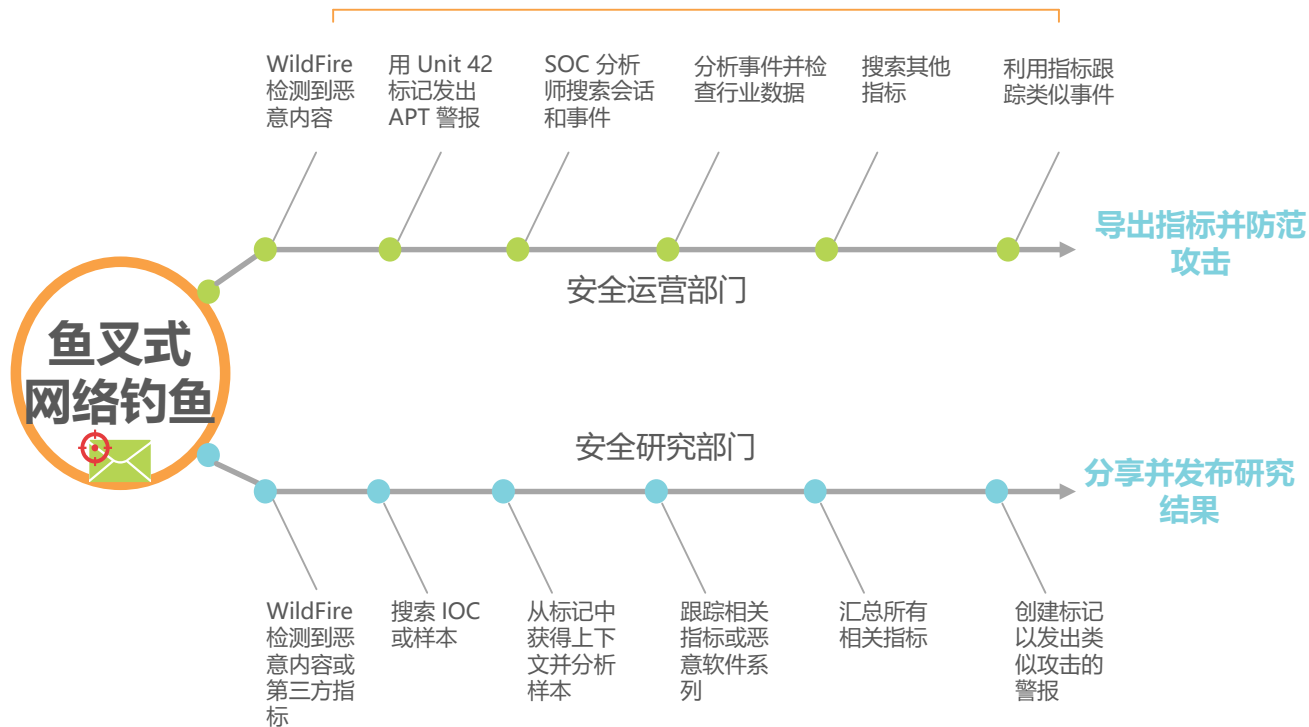


主动防范攻击

引入更多的第三方资源，和提供更多的资源给第三方



威胁情报态势感知的分步用例流程举例



某大型互联网用户



外部情报源

- ✓ 15K+ sample 查询
- ✓ 每半小时拉取数据



内部情报源

- ✓ 70K+ sample/IOC查询



SOC

- ✓ 黑客攻击的第一梯队目标
- ✓ 情报数据主要来自于国内
- ✓ 缺乏安全数据共享及合作
- ✓ 安全问题事件化, 人工二次筛查

终端安全产品 边界安全产品

- ✓ 未知流量全部上传
- ✓ 每半小时推送安全策略





推进实时和超前防御技术理念



在攻击生命周期的各个阶段预防威胁



收集情报

漏洞利用

执行
恶意软件

控制通道
C2

窃取数据

计划攻击

隐性渗透感染

恶意文件执行

恶意软件
与攻击者通信

数据盗窃, 破坏, 销毁

利用智能威胁云的情报，实现实时防御

1

减少攻击面

- 应用白名单或阻断高风险应用
- 阻断已知病毒，网络攻击
- 阻断常见的攻击工具文件类型

2

检测未知威胁

- 分析所有网络应用流量
- SSL 解密
- WildFire 沙箱云端检测

3

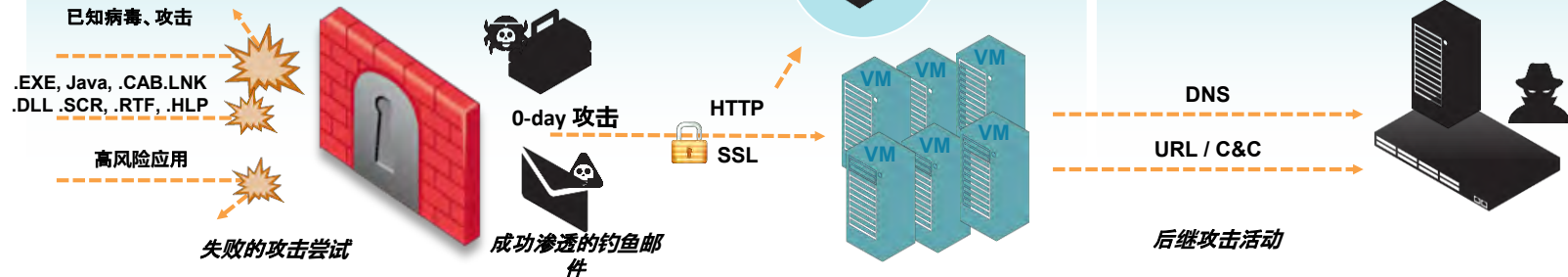
实时安全防护

检测、阻断 C&C 操作:

- DNS 查询流量中的“坏”URL
- URLs 过滤 (PAN-DB)
- C&C 特征 (anti-spyware)

WildFire™

网络威胁在东西向的渗透



举例：超前防御说明（5/12爆发前已进行之工作）

2017/02/10

安全情报云 (Autofocus)

该ransomware的1.0版由
Malwarebytes研究员SIRi
发现

**掌握第一只样本并累积、
关联各项数据供关联分析
使用！**

2017/03/25

安全情报云 (Autofocus)

由GData安全研究员
Karsten Hahn发现在相关的
活动.

2017/04/19

网关威胁防御 (PA Firewall)

**自动提供给全球客户的签
名预防**

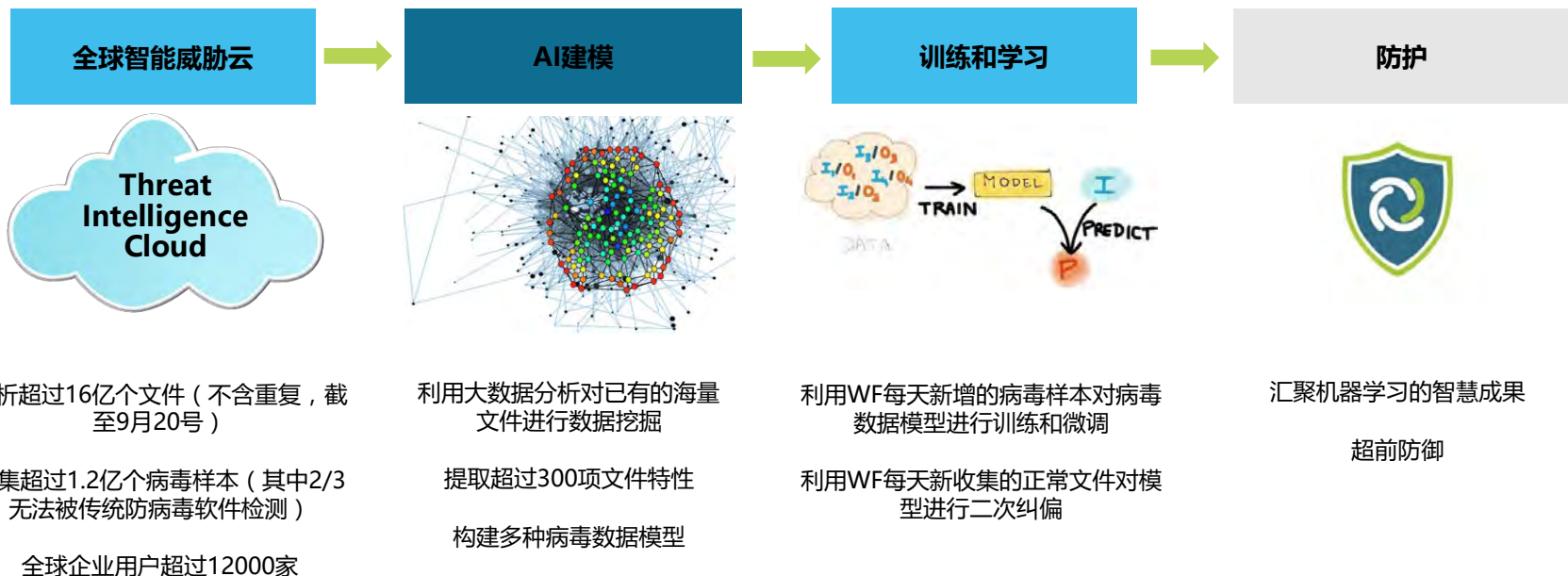
2017/04/26

终端威胁防御 (TRAPS)

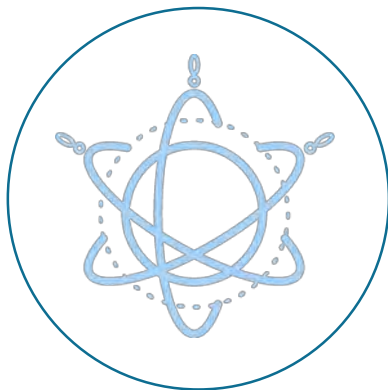
本地分析（机器学习）

核心技术原理：

通过态势感知、将Machine Learning技术应用于安全防御
智能提前阻止未知恶意软件



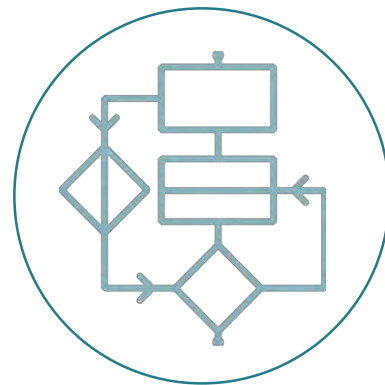
安全威胁情报态势感知，在互联网+时代的意义：



全球化采样和协作



智能化分析、追踪和标示



高度互联和及时响应



谢谢

