如何建立全方位的威胁监控

微步在线 - 薛锋

2018 ThreatBook 安全分析与情报大会

有多少黑客试图攻击你的企业？

扫描 IP 中是针对性攻击？还是人工、僵木蠕？

有多少服务器已经被拿下？挖矿还是DDoS?

还有多少Wannacry？外传数据？被勒索？

内网有多少黑客在渗透，移动，试图扩大权限？

收到的邮件多少附件带木马?

多少是诈骗、勒索?

有多少人打开了附件或者链接?

隔离的网络安全吗？

如果这些问题，你都不关心……

如果这些问题，你都不能回答……

威胁监控目标：基于攻击链的全面威胁监控

攻击杀伤链-Kill Chain

生产网Weblogic漏洞攻击

办公网攻击

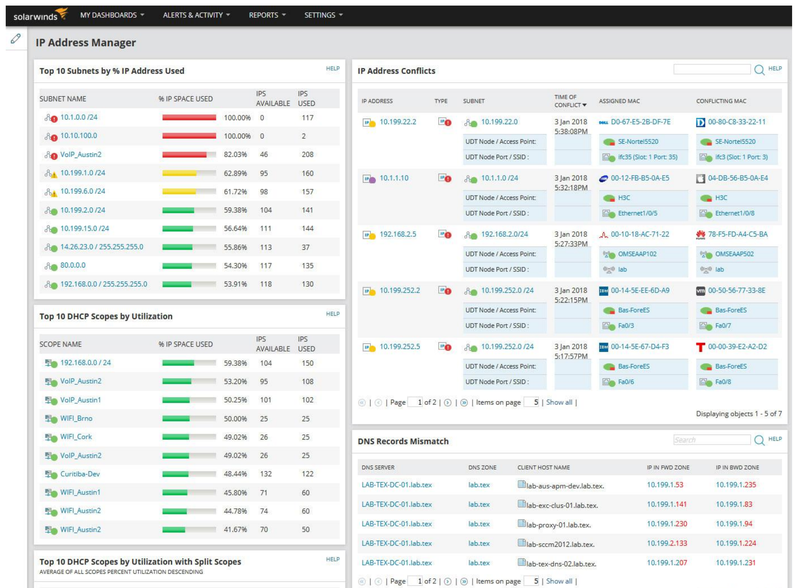

1
扫描/侦查
2
投递武器
3
漏洞利用
4
安装持久化
5
命令与控制
6
内网渗透
7
行动或数据窃取
搜集邮箱
鱼叉式Email
发送邮件
Office漏洞
PowerShell
C&C:
***.windowsupd
ate.top
Windows漏洞
Over Pass the
hash
窃取资料

实现威胁监控途径：工具+技术+运营

工具

技术

运营



传统工具：

IPS

WAF

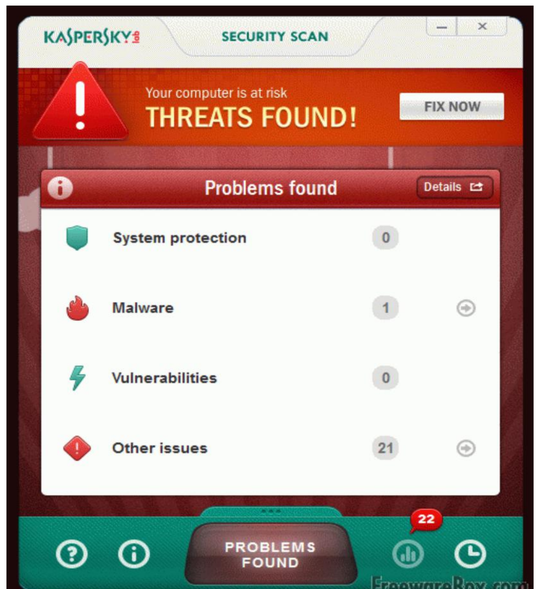
Firewall

SIEM

AV

海量报警、无上下文、已知威胁

内网威胁？无文件攻击？



监控探针/Sensor

南北向流量（网络边界）

DMZ区域、办公网、生产网、隔离内网

东西向流量（内网流量）

办公网内部流量、办公网向生产网流量、DMZ向生产网流量等

关键节点流量

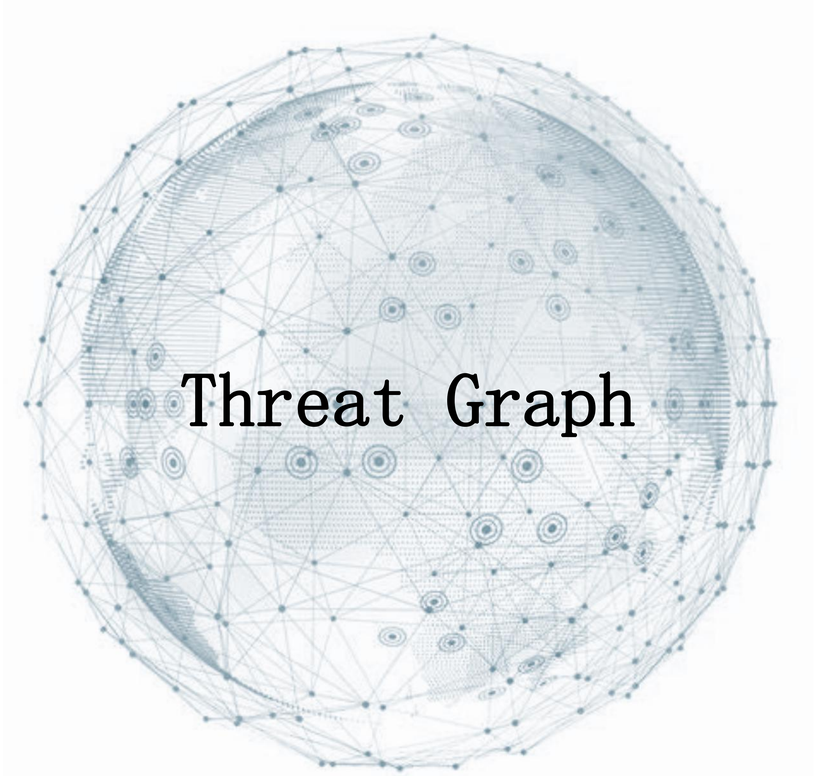
邮件网关流量、域控流量

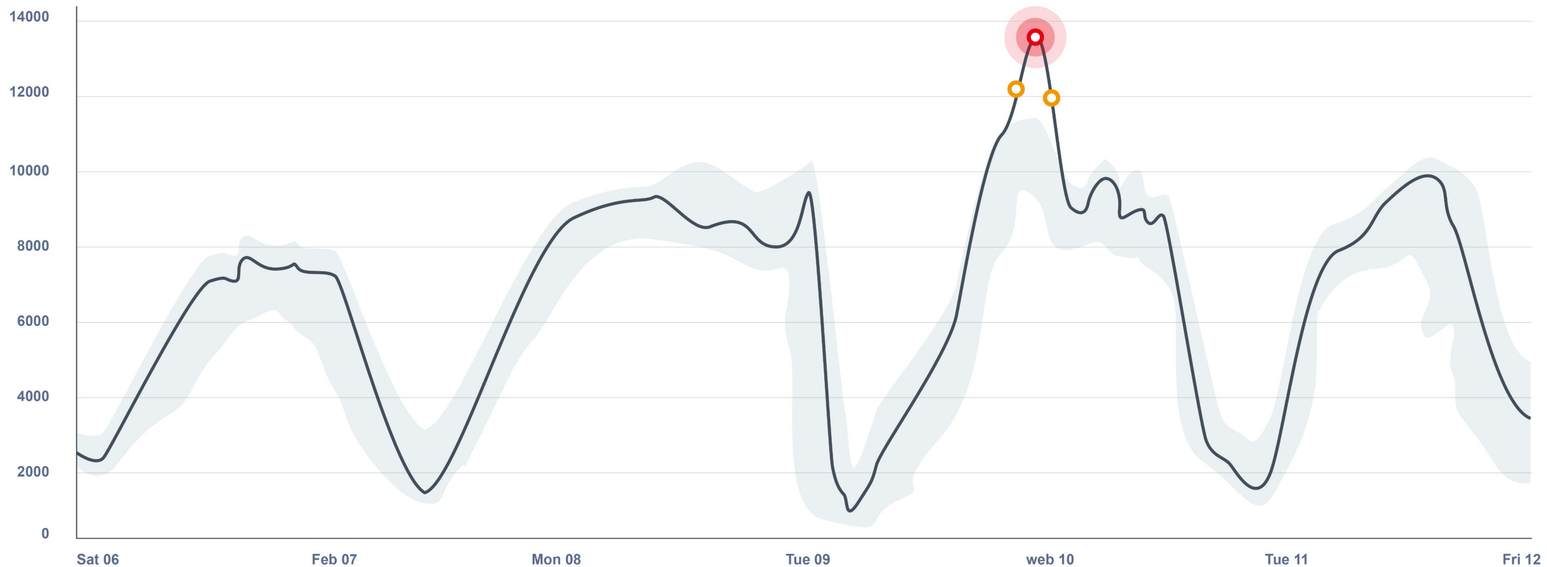
终端-恶意文件

终端-进程、网络、注册表、驱动等行为

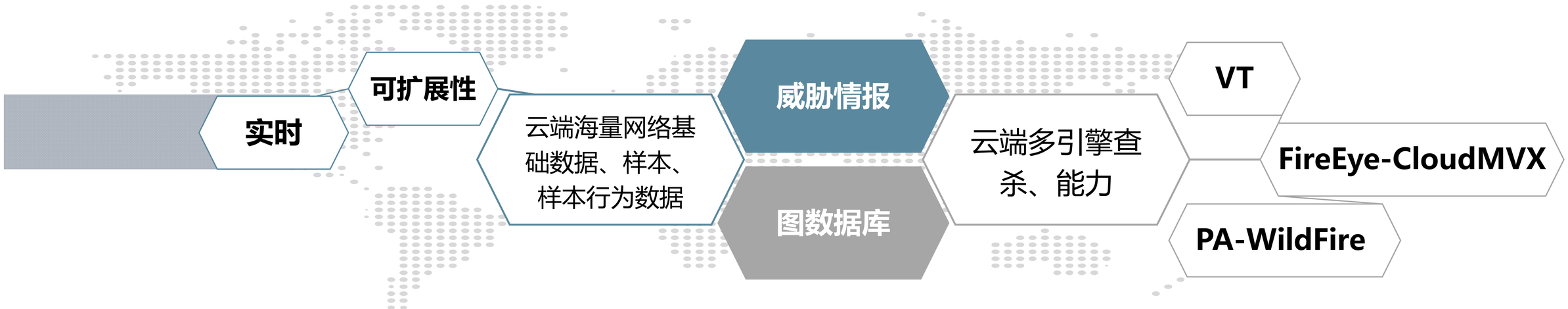
基于签名的传统技术


大数据
人工智能
云计算
新技术


Threat Graph


14000
12000
10000
8000
6000
4000
2000
0
Sat 06
Feb 07
Mon 08
Tue 09
web 10
Tue 11
Fri 12

应用云计算提升本地设备能力



全面的探针应用

可指导行为的上下文

自动化的响应能力

paloalto NETWORKS

BLUECAT NETWORKS

SANGFOR 深信服科技

IMPERVA

Symantec

Check Point SOFTWARE TECHNOLOGIES LTD.

McAfee

Microsoft

360 企业安全

天融信 TOPSEC

paloalto NETWORKS

SANGFOR 深信服科技

BLUECAT NETWORKS

Symantec

IMPERVA

Check Point SOFTWARE TECHNOLOGIES LTD.

McAfee

360 企业安全

天融信 TOPSEC

工具

开源： ELK、Windows-Sysmon、Linux-Osquery、Suricata、Bro

微步在线： TDP、TDP-Agent、TDPS、EDP

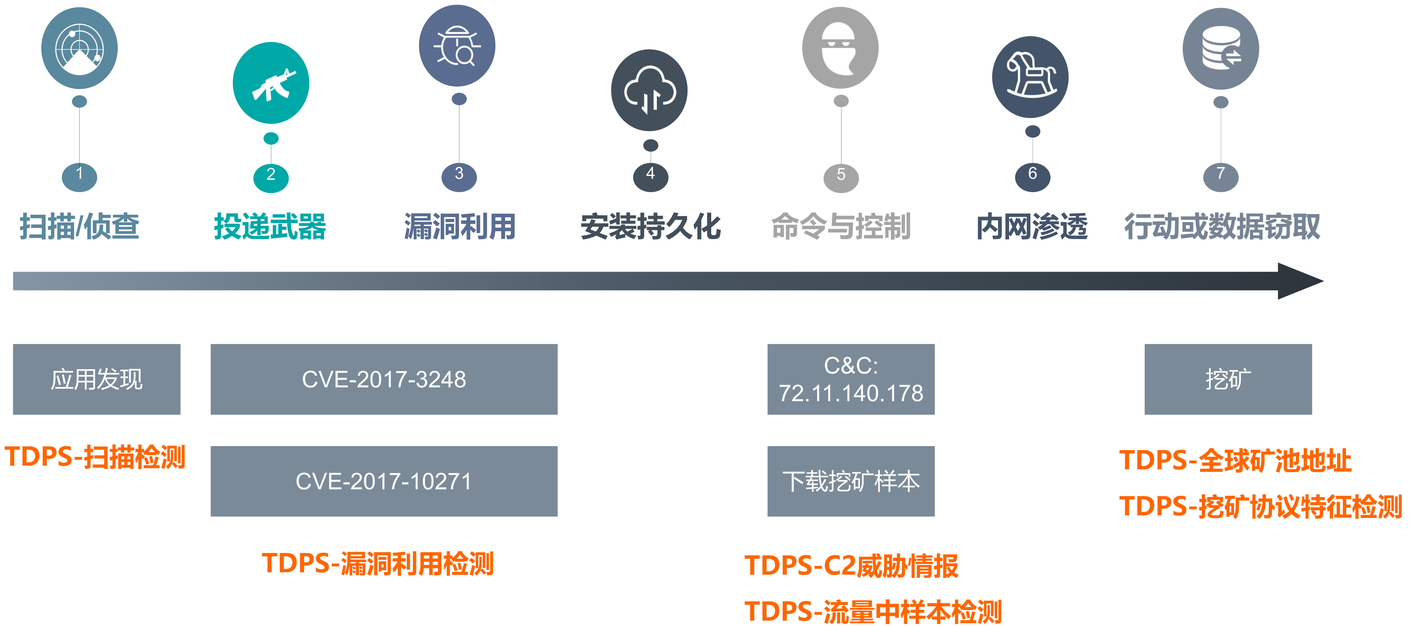
技术

开源： ELK-Xpack、VT、开源情报

微步在线： TDP、TDPS、EDP、TIP、API

运营

微步在线： MDR、TIP-自动化响应


1
扫描/侦查
2
投递武器
3
漏洞利用
4
安装持久化
5
命令与控制
6
内网渗透
7
行动或数据窃取
应用发现
TDPS-扫描检测
CVE-2017-3248
CVE-2017-10271
TDPS-漏洞利用检测
C&C:
72.11.140.178
下载挖矿样本
TDPS-C2威胁情报
TDPS-流量中样本检测
挖矿
TDPS-全球矿池地址
TDPS-挖矿协议特征检测


1
2
3
4
5
6
7
扫描/侦查
投递武器
漏洞利用
安装持久化
命令与控制
内网渗透
行动或数据窃取
搜集邮箱
发送邮件
Office漏洞
PowerShell
C&C:
***.windowsupda
te.top
Windows漏洞
窃取资料
鱼叉式Email
恶意软件下载
TDP-邮件点击检测
TDP-C2威胁情报
TDP-全球矿池地址
Over Pass the
hash
TDP-数据泄露检测
EDP-钓鱼邮件检测
TDP-流量中样本检测
TDP-内网漏洞利用检测
TDP-OPtH检测


预警
防御
响应
发现
持续全方位
威胁监控
大数据
AI
云
威胁情报

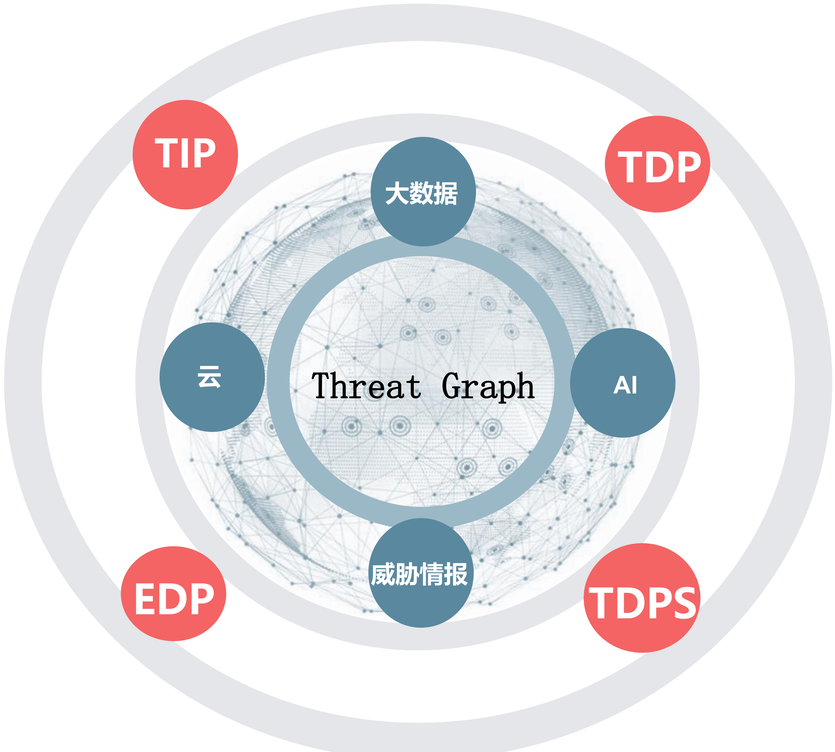
微步在线进展

金融行业

互联网

能源

国际化集团


TIP
大数据
TDP
云
Threat Graph
AI
威胁情报
EDP
TDPS


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

微步在线 www.threabook.cn

x.threatbook.cn