

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、僵尸蠕？

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？

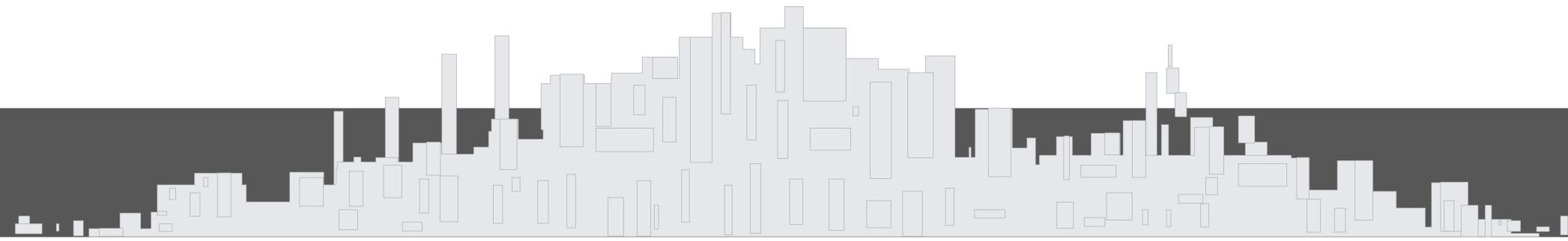
有多少人打开了附件或者链接？

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……

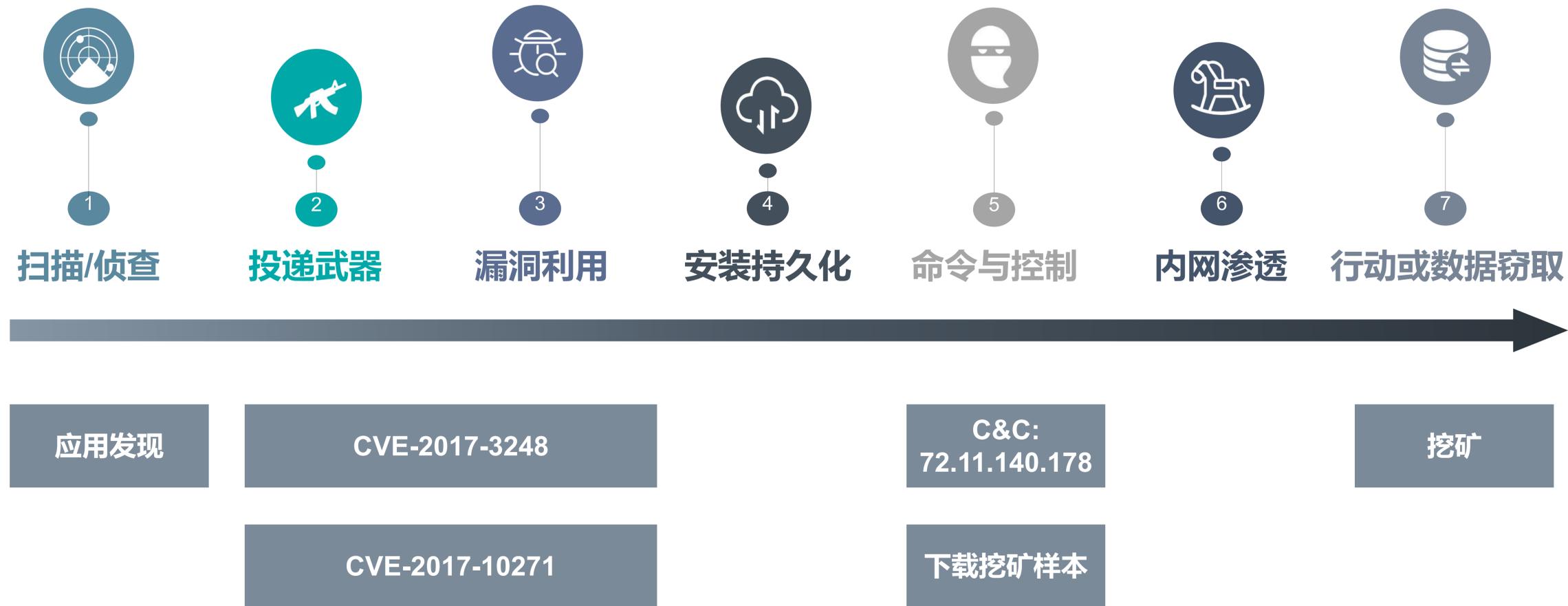
威胁监控目标：基于攻击链的全面威胁监控





攻击杀伤链-Kill Chain

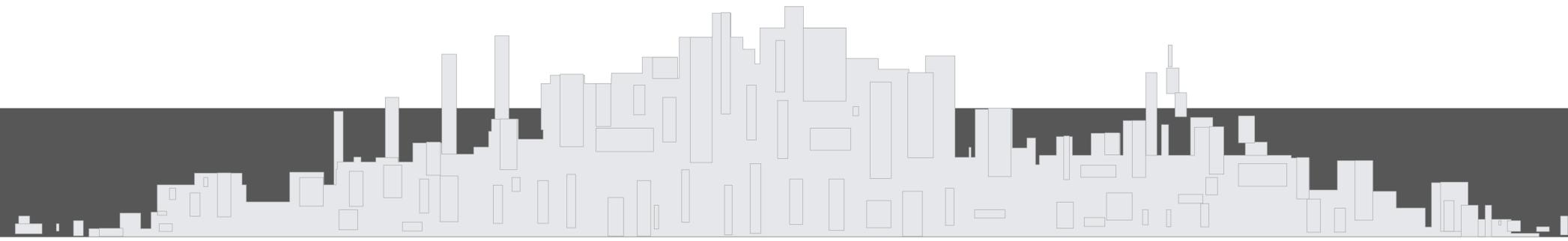
生产网Weblogic漏洞攻击

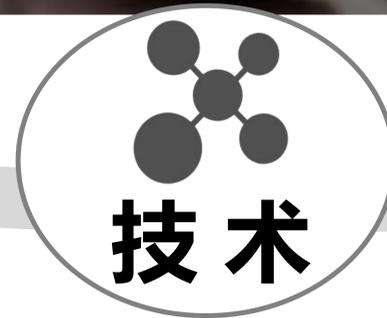


办公网攻击



实现威胁监控途径：工具+技术+运营





solarwinds MY DASHBOARDS ALERTS & ACTIVITY REPORTS SETTINGS

IP Address Manager

Top 10 Subnets by % IP Address Used

SUBNET NAME	% IP SPACE USED	IPS AVAILABLE	IPS USED
10.1.0.0 /24	100.00%	0	117
10.10.100.0	100.00%	0	2
VolIP_Austin2	82.03%	46	208
10.199.1.0 /24	62.89%	95	160
10.199.6.0 /24	61.72%	98	157
10.199.2.0 /24	59.38%	104	141
10.199.15.0 /24	56.64%	111	144
14.26.23.0 / 255.255.255.0	55.86%	113	37
80.0.0.0	54.30%	117	135
192.168.0.0 / 255.255.255.0	53.91%	118	130

Top 10 DHCP Scopes by Utilization

SCOPE NAME	% IP SPACE USED	IPS AVAILABLE	IPS USED
192.168.0.0 / 24	59.38%	104	150
VolIP_Austin2	53.20%	95	108
VolIP_Austin1	50.25%	101	102
WIFI_Brno	50.00%	25	25
WIFI_Cork	49.02%	26	25
VolIP_Austin2	49.02%	26	25
Curitiba-Dev	48.44%	132	122
WIFI_Austin1	45.80%	71	60
WIFI_Austin2	44.78%	74	60
WIFI_Austin2	41.67%	70	50

Top 10 DHCP Scopes by Utilization with Split Scopes

IP Address Conflicts

IP ADDRESS	TYPE	SUBNET	TIME OF CONFLICT	ASSIGNED MAC	CONFLICTING MAC
10.199.22.2	IP	10.199.22.0	3 Jan 2018 5:38:08PM	D0-67-E5-2B-DF-7E	00-80-C8-33-22-11
10.1.1.10	IP	10.1.1.0 /24	3 Jan 2018 5:32:18PM	00-12-FB-B5-0A-E5	04-DB-56-B5-0A-E4
192.168.2.5	IP	192.168.2.0/24	3 Jan 2018 5:27:33PM	00-10-18-AC-71-22	78-F5-FD-A4-C5-BA
10.199.252.2	IP	10.199.252.0 /24	3 Jan 2018 5:22:15PM	00-14-5E-EE-6D-A9	00-50-56-77-33-8E
10.199.252.5	IP	10.199.252.0 /24	3 Jan 2018 5:17:57PM	00-14-5E-67-D4-F3	00-00-39-E2-A2-D2

DNS Records Mismatch

DNS SERVER	DNS ZONE	CLIENT HOST NAME	IP IN FWD ZONE	IP IN BWD ZONE
LAB-TEX-DC-01.lab.tex	lab.tex	lab-aus-apm-dev.lab.tex.	10.199.1.53	10.199.1.235
LAB-TEX-DC-01.lab.tex	lab.tex	lab-exc-clus-01.lab.tex.	10.199.1.141	10.199.1.83
LAB-TEX-DC-01.lab.tex	lab.tex	lab-proxy-01.lab.tex.	10.199.1.230	10.199.1.94
LAB-TEX-DC-01.lab.tex	lab.tex	lab-sccm2012.lab.tex.	10.199.2.133	10.199.1.224
LAB-TEX-DC-01.lab.tex	lab.tex	lab-tex-dns-02.lab.tex.	10.199.1.207	10.199.1.231

传统工具：
 IPS
 WAF
 Firewall
 SIEM
 AV

Nagios XI Operations Center

Last Update: Fri Jan 27 2012 11:32:18 GMT-0600 (Central Standard Time)

Up D UR Pe UH Pr All
 Hosts: 3 2 0 0 2 5 Services: 45 1 8 15 0 24 69

Host Name	Duration	Status Information	
192.168.5.32	22d 17h 1m 53s	check_icmp: Failed to resolve 192.168.5.999	
Host Name	Service	Duration	Status Information
www.amazon.com	DNS IP Match	25m 40s	DNS CRITICAL - expected '72.21.194.1*' but got '72.21.211.176'
DUMMYBPI	BPI Process:Test Group	11d 1h 26m 30s	Unknown BPI Group Index
BPI2	BPI Process:DNS Resolution	11d 1h 26m 30s	Unknown BPI Group Index
BPI Test	BPI: Test Group	11d 1h 26m 30s	Unknown BPI Group Index
BPI Process 1	BPI Process: Test Group 2	11d 1h 26m 35s	Unknown BPI Group Index
DUMMYBPI	BPI Process:dfsadfsadfsadf	11d 1h 28m 12s	Unknown BPI Group Index
BPI2	BPI Process:Websites Services	11d 1h 28m 14s	Unknown BPI Group Index
BPI2	BPI Process:Content	11d 1h 28m 14s	Unknown BPI Group Index
DUMMYBPI	BPI Process:akooankooanslo	11d 1h 29m 33s	Unknown BPI Group Index
BPI2	BPI Process:Website-Sites	11d 1h 29m 34s	Unknown BPI Group Index
BPI Test	BPI: akooankooanslo	11d 1h 29m 34s	Unknown BPI Group Index
1.9Test	BPI - akooankooanslo	11d 1h 29m 48s	Unknown BPI Group Index
DUMMYBPI	BPI Process:Test Group 2	11d 1h 30m 50s	Unknown BPI Group Index
BPI2	BPI Process:DNS_IP	11d 1h 30m 56s	Unknown BPI Group Index
BPI Test	BPI: Test Group 2	11d 1h 30m 59s	Unknown BPI Group Index
192.168.5.7	HTTP	22d 16h 59m 32s	HTTP WARNING: HTTP/1.1 403 Forbidden
192.168.5.7	Nagios XI Daemons	91d 2h 30m 5s	Error: Could not parse XML from http://192.168.5.7/nagiosxi ()
192.168.5.7	I/O Wait	91d 2h 33m 30s	Error: Could not parse XML from http://192.168.5.7/nagiosxi ()
192.168.5.7	Load	91d 2h 34m 8s	Error: Could not parse XML from http://192.168.5.7/nagiosxi ()
192.168.5.7	Nagios XI Jobs	91d 15h 58m 31s	Error: Could not parse XML from http://192.168.5.7/nagiosxi ()
thefrugallambe.com	Web Page Content	170d 5h 20m 45s	HTTP CRITICAL - string not found
thefrugallambe.com	DNS IP Match	197d 19h 38m 26s	DNS CRITICAL - expected '99.198.111.18' but got '65.60.39.10'
192.168.5.32	Ping	218d 19h 31m 14s	check_icmp: Failed to resolve 192.168.5.999
www.cnn.com	DNS IP Match	218d 20h 24m 13s	DNS CRITICAL - expected '157.166.226.25' but got '157.166.226.25,157.166.226.26,157.166.255.18,157.166.255.19'

海量报警、无上下文、已知威胁
 内网威胁？无文件攻击？

KASPERSKY SECURITY SCAN

Your computer is at risk
THREATS FOUND! **FIX NOW**

Problems found

- System protection: 0
- Malware: 1
- Vulnerabilities: 0
- Other issues: 21

PROBLEMS FOUND

FreewareBox.com





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

大量的人力投入

响应周期慢

容易绕过

误报高





大数据



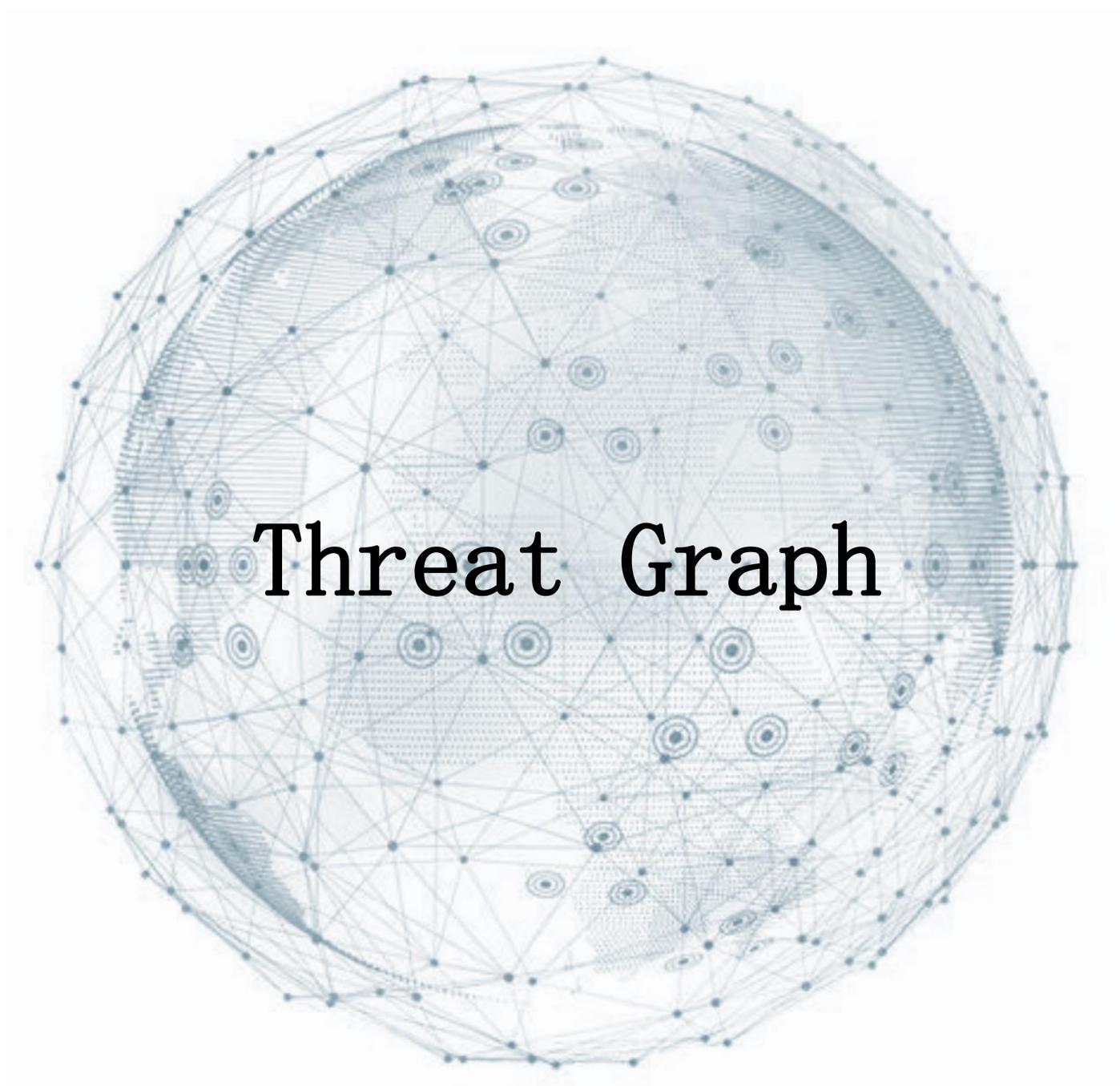
人工智能



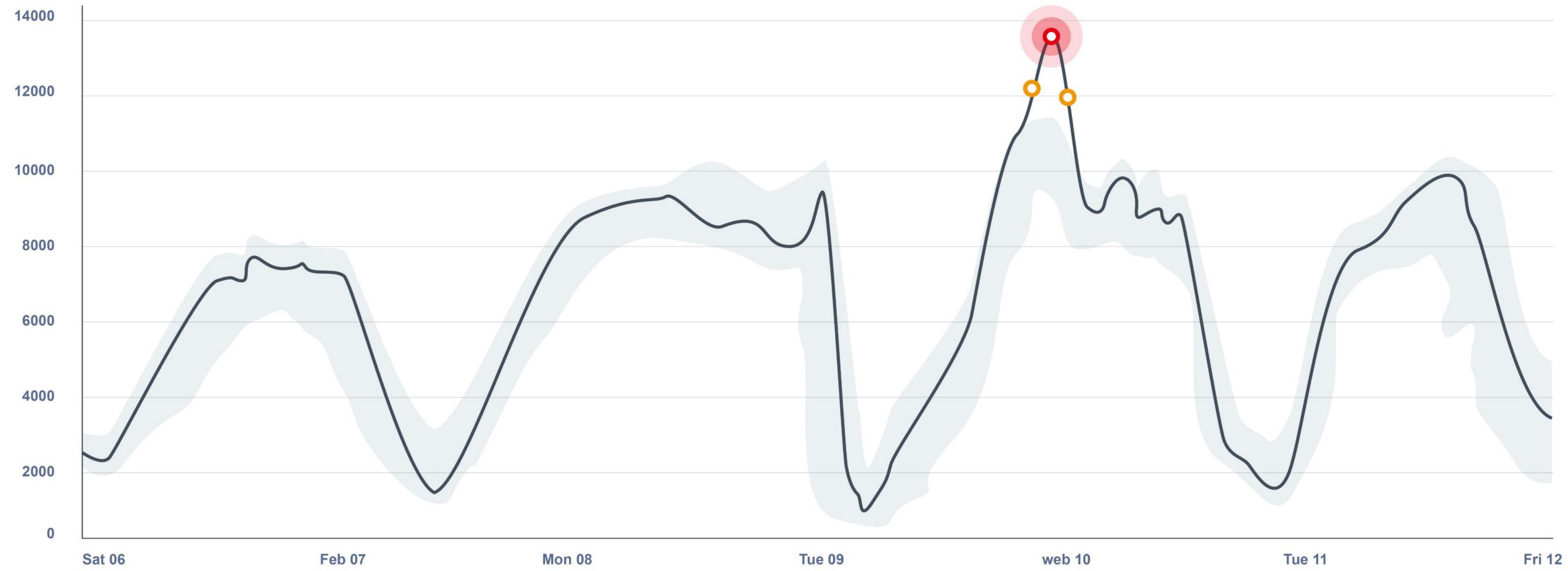
云计算

新技术

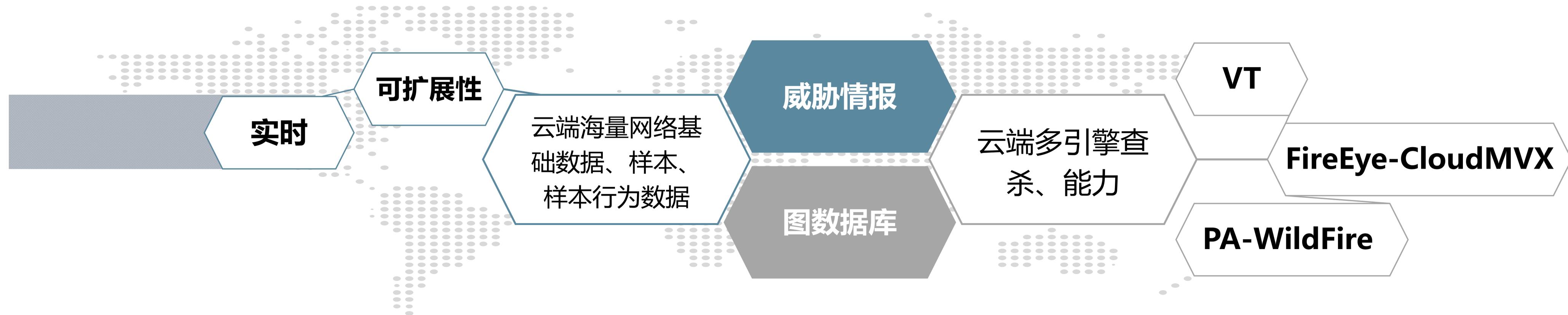




Threat Graph



应用云计算提升本地设备能力



实时

可扩展性

云端海量网络基础数据、样本、样本行为数据

威胁情报

图数据库

云端多引擎查杀、能力

VT

FireEye-CloudMVX

PA-WildFire

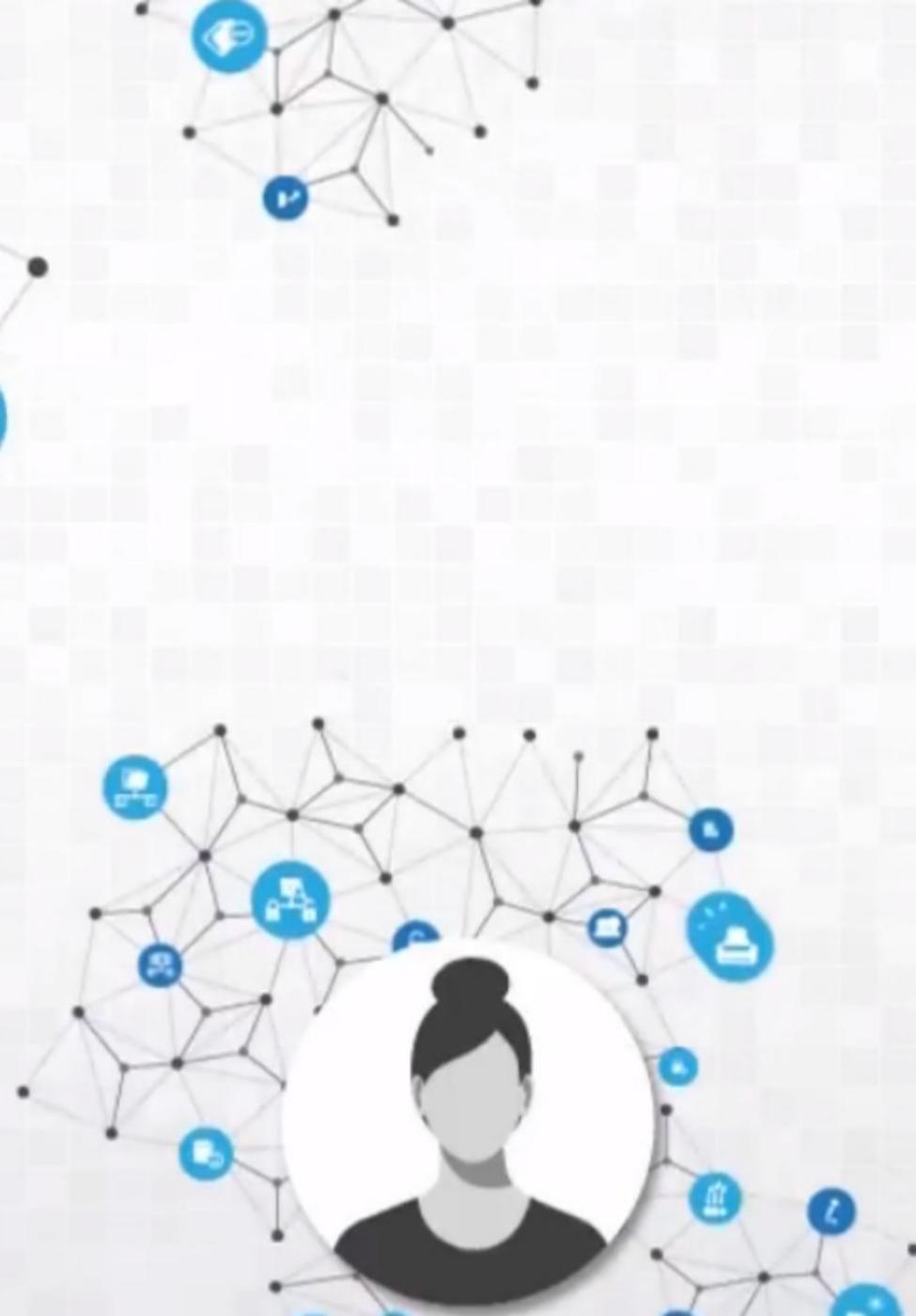
自动化的响应能力

全面的探针应用

安全运营人员

可指导行为的上下文









开源： ELK、Windows-Sysmon、Linux-Osquery、Suricata、Bro
微步在线： TDP、TDP-Agent、TDPS、EDP



开源： ELK-Xpack、VT、开源情报
微步在线： TDP、TDPS、EDP、TIP、API



微步在线： MDR、TIP-自动化响应



应用发现

CVE-2017-3248

C&C:
72.11.140.178

挖矿

TDPS-扫描检测

CVE-2017-10271

TDPS-漏洞利用检测

下载挖矿样本

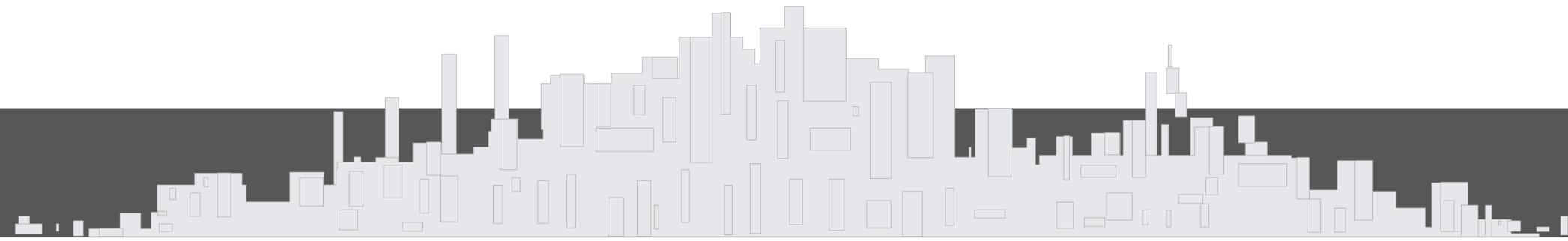
TDPS-C2威胁情报
TDPS-流量中样本检测

TDPS-全球矿池地址
TDPS-挖矿协议特征检测





微步在线进展



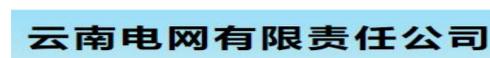
金融行业



互联网

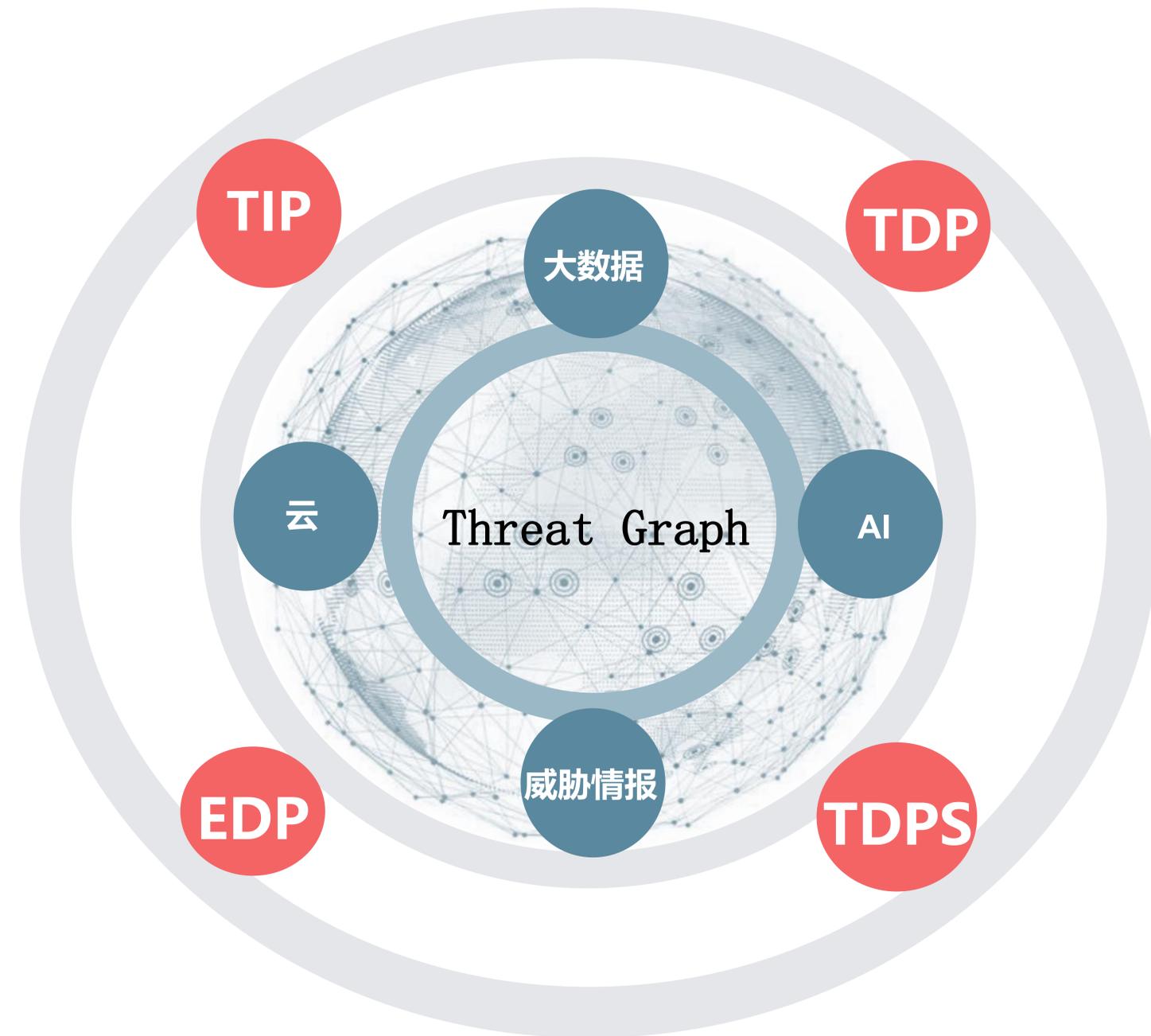


能源



国际化集团





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
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
x.threatbook.cn