安全智能 情报驱动

微步在线

技高一筹 HIGH-TECH FOR TECH HIGH

以人工智能 护数据资产

微步在线-国内首家威胁情报公司

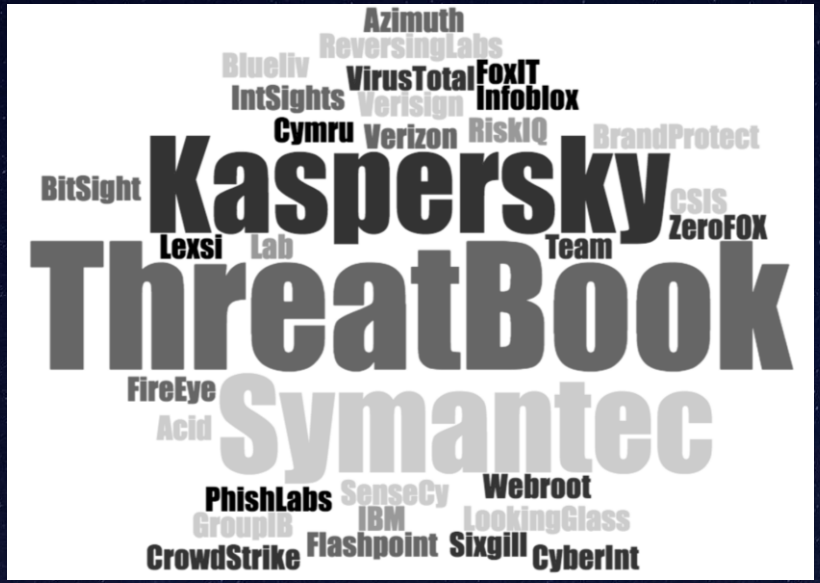
CEO —— 薛 锋

- 前亚马逊中国首席安全官(CISO)
- 前微软中国互联网安全战略总监
- 国际顶级黑帽子(Blackhat)欧洲安全大会和微软Bluehat安全大会上首位来自中国的演讲者
- 曾任职于公安部第三研究所

- 成立于2015年7月，致力于提供以威胁情报为核心的安全服务
- 当前公司总计员工70人，主要成员来自于亚马逊、微软、BAT、美团等公司
- 累计融资1.65亿人民币，投资机构包括：北极光、如山创投、高瓴资本等
- 2017中国唯一入选Gratner威胁情报市场指南
- 入选全球网络安全500强(CyberSecurity 500)

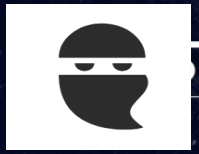
唯一入选Gartner全球威胁情报市场指南的中国公司

Gartner是**全球最具权威**的IT研究与顾问咨询公司，其魔力象限和市场指南一直是企业采购的重要参考依据。
微步在线成为**唯一**入选Gartner全球威胁情报市场指南的**中国公司**。



Gartner预测，三年内应用威胁情报的大型企业将从现在的1%增长到 15%

技高一筹 HIGH-TECH FOR TECH HIGH
以人工智能 护数据资产



人力有限、经验有限	人	专业团队、团伙作战
有限的时间做迅速的响应	时间	充裕的攻击准备和移动时间
依赖有限的组织内外支持	资源	成熟的工具、服务支持
手工操作与分析	自动化	自动化的工具和流程
资产不可见、攻击不可见	可见性	更了解组织的网络结构

评估检测与响应：MTTD、MTTR

MTTD均值：172天

- 以上是亚太地区的均值，北美地区为99天
- Source：FireEye Mandiant M-Trends 2017

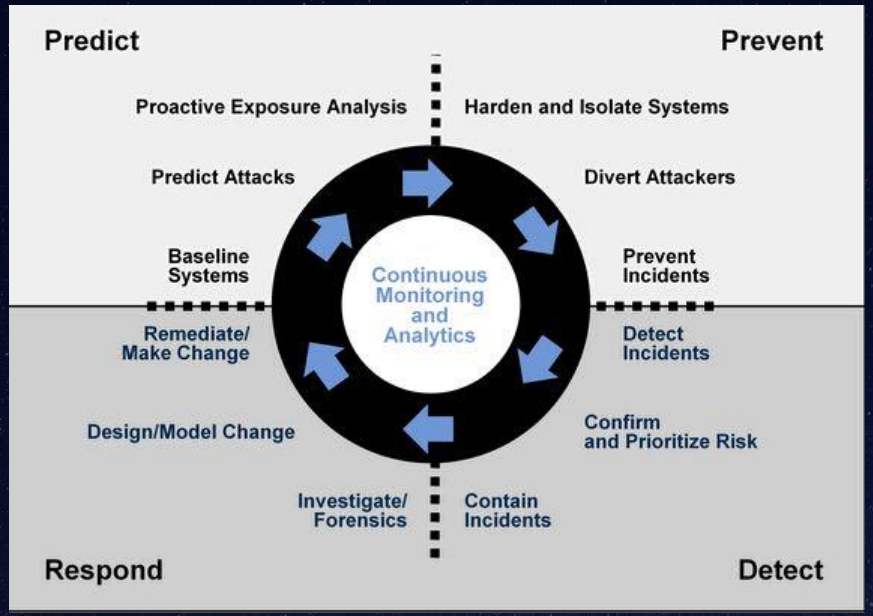
MTTD – Mean Time To Detection/平均发现时间

MTTR – Mean Time To Response/平均响应时间

衡量企业安全水平的国际“标准”

企业/组织	国家	行业	事件	数据泄漏量	被攻击时间	发现/公布时间	MTTD
艾可飞（Equifax）	美国/全球	金融服务业	数据泄漏	1.45亿	2017年5月	2017年9月	**120**
雅虎(Yahoo)	美国/全球	互联网	数据泄漏	30亿	2013年8月	2016年12月	**超过一年**
德勤 (Deloitte)	英国/全球	专业服务	数据泄漏	500万	2017年3月	2017年5月	**120**

安全建设思路转变：从传统的“防防防！”到检测与响应



60%的信息安全预算将会投入到检测和响应…

- Gartner

“企业将处于持续被攻陷的状态…”

- Neil MacDonald, Gartner

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.ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com**”,
“related_samples”:[“**22ccdf145e5792a22ad6349aba37d960db77af7e0b6cae826d228b8246705092**”],
“patches”:[“CVE-2017-0144”]}

全面监控与检测

用户应用开关域名（IOC）进行全面的失陷检测

快速响应

应用配置DNS解析的方式保护主机达数百万台

自动联动修复

应用情报中的CVE标识自动联动终端管理进行补丁修复

情报驱动的威胁检测与响应

谢谢