**安全智慧升级**

**----蓝盾全线产品AI化**

AI时代群雄逐鹿，网络安全的企业充分认识到人工智能的重要意义。因为机器学习在一定程度上的确可以帮助企业更好地分析网络威胁、响应攻击和安全事件，同时还能够完成技术价值较低的自动化工作。未来，应用于网络安全领域的机器学习必然呈现快速发展的趋势。据ABI 研究机构的分析师估计，到2021年，网络安全领域的机器学习将会促进大数据、人工智能和安全分析方面的支出增长，可达960亿美元。

目前，全球各大技术巨头已经表明将利用人工智能技术更好地保护他们客户的安全。例如，谷歌正在利用机器学习技术来分析在安卓系统上运行的移动终端威胁，以及在受感染手机系统上识别和移除恶意软件。云基础设施巨头亚马逊则收购了初创公司 Harvest.AI，并发布了Macie这个结合机器学习的服务，对S3 云储存服务中的数据进行整理分类。

除了各大巨头纷纷与人工智能联手之外，网络安全厂商也已经开始将机器学习整合入其全线产品中，希望进一步提高安全能力。目前，大部分的主要安全厂商已经不再单纯依靠基于签名的方式，而是转向了机器学习的方式以提高效率和能力。

人工智能在网络安全领域的发展还处于初期阶段，大部分应用案例都是用于终端、网络、SIEM等场景，未来还有非常广阔的发展空间。而蓝盾，将在2018年实现全线产品的人工智能化（即“AI-enabled”），借力AI，乘风而起。

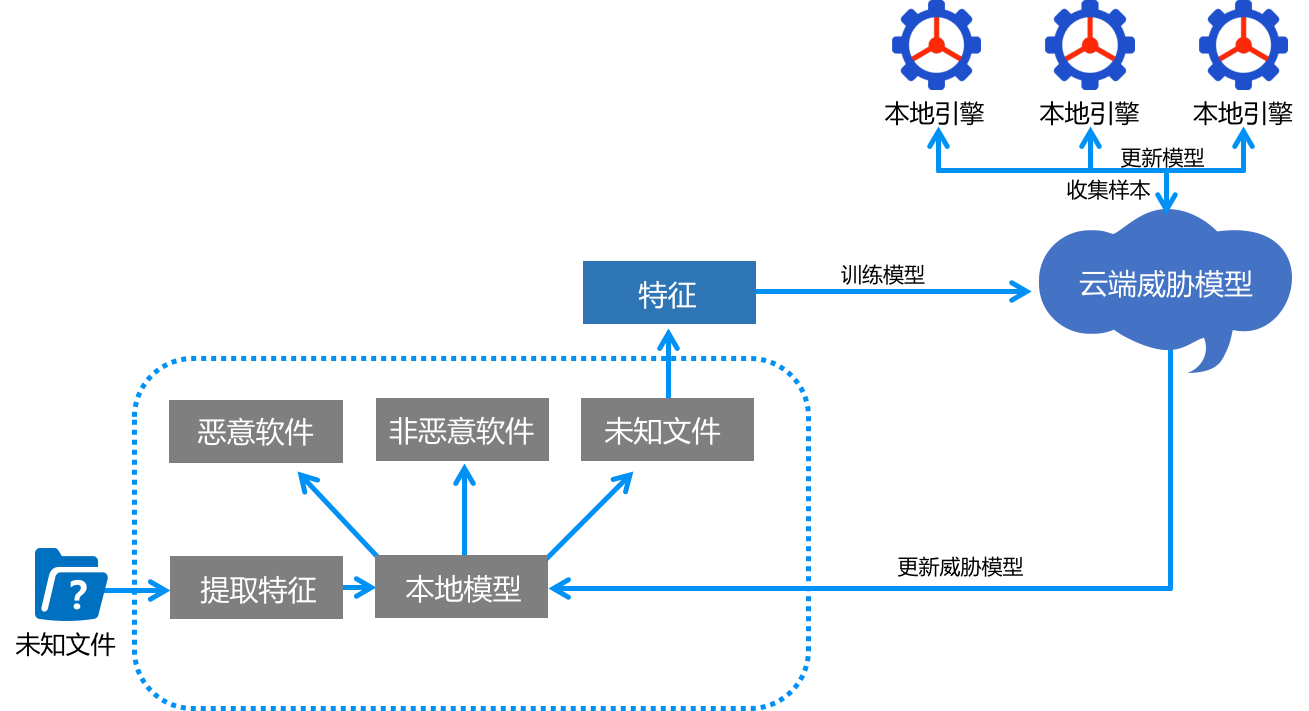
**蓝盾认为，让人工智能充分融合到行业解决方案中，才能发挥其作用。遵循这样的原则，我们把2018年的AI布局分成以下4方面。**

## **1. 使用机器学习去自动化重复的安全任务 - 蓝盾防火墙**

人工智能真正的红利在于能够进行自动重复性劳动，使得人类更专注于重要的工作。人工智能的终极目标应该是：“使人类无需再做重复性、低价值的决策与行为”。让机器去处理重复工作和应对勒索软件，人类从而可以腾出时间去实现更多策略上的排兵布局。我们有理由相信，**人工智能的平台化和云化将会是全球发展的主流。**

蓝盾在人工智能与网络安全的早期，就已经非常注意对“效率”和“自动化”的极致追求，在内部成功建立了·

* 人工智能流水线
* 大数据处理流水线
* 基于蓝盾云和边界防御产品（防火墙）的模型自动触发并更新机制等

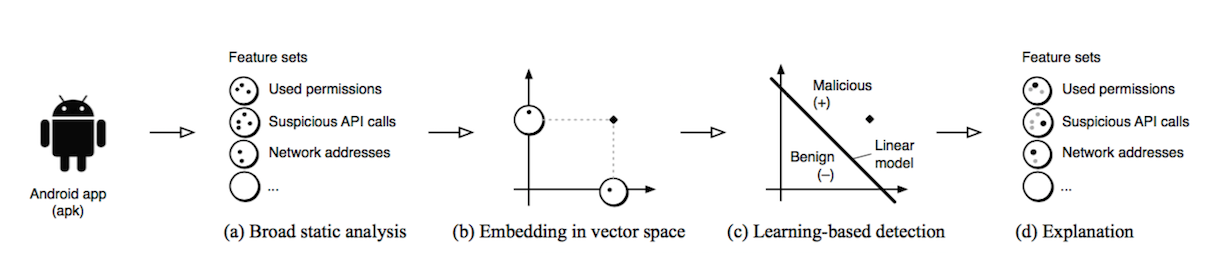


(蓝盾防火墙)

## **2. 使用机器学习去分析移动终端 - 蓝盾移动安全**

机器学习已经在移动设备上广泛运用，但大多数案例的目的是改善基于声音的体验，如Google Now，Apple‘s Siri等。但其实，基于人工智能的安全在移动安全领域也拥有非常广泛的发展前景。蓝盾在此领域使用机器学习

* 分析针对移动终端的威胁（如恶意软件APK的检测）；
* 分析哪些APP侵犯用户个人隐私的行为，即HSO检测；
* 识别伪基站；



(Source：*Drebin Effective And Explainable Detection Of Android Malware In Your Pocket*，NDSS2014，Daniel et. al.)



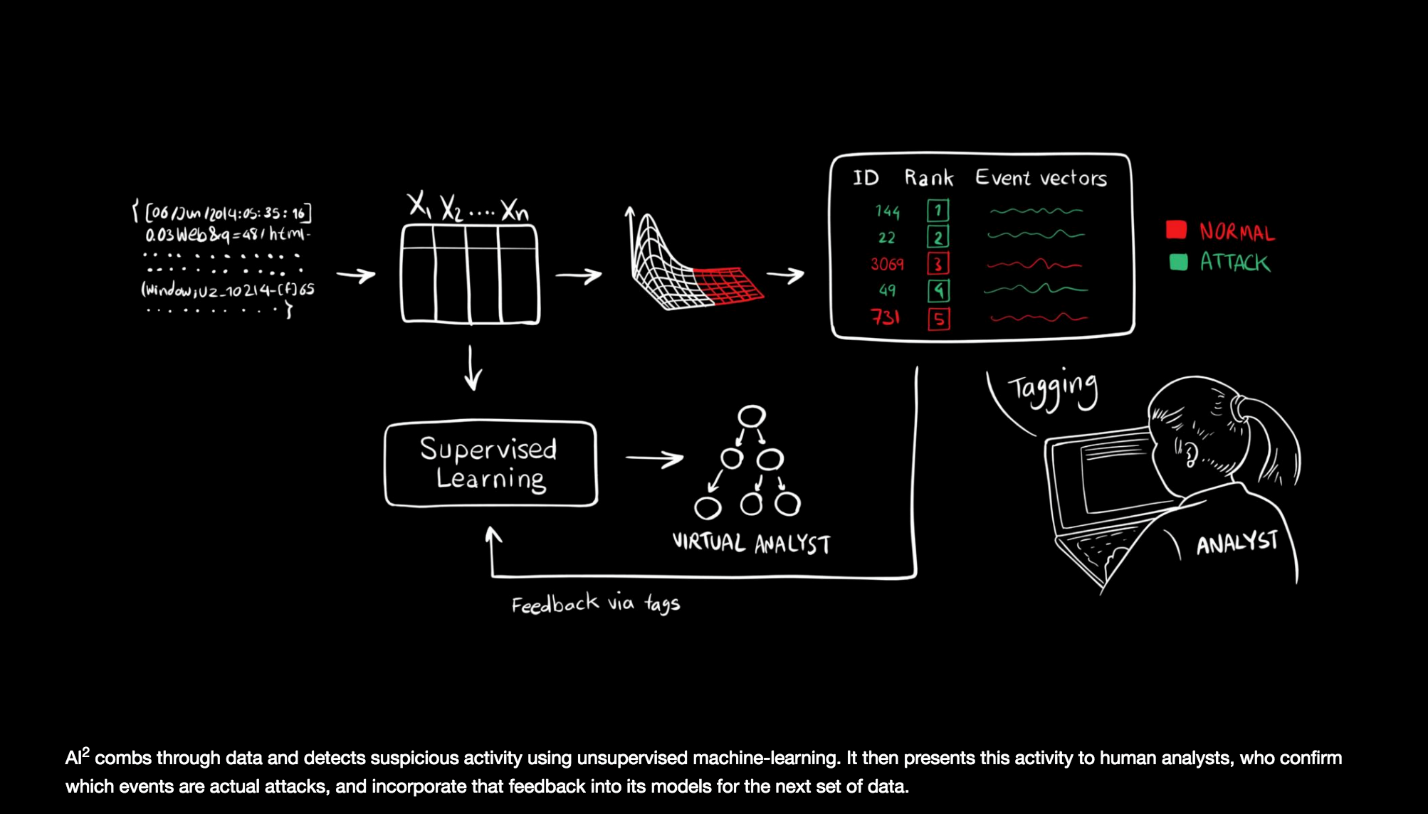
（蓝盾安全卫士）

**3. 使用人工智能以增强人工分析 - 蓝盾态势感知平台**

网络安全领域应用人工智能的一个核心理念是希望人工智能能在所有方面为人类分析师提供帮助，其中包括恶意攻击检测、网络状态分析、终端保护和漏洞评估。

例如，在2016年，MIT计算机科学与人工智能实验室开发了一个系统叫AI2，这是一个自适应机器学习安全平台。此平台的目标在于帮助分析师“大海捞针”。系统能够每天审阅数以百万的登入信息，过滤数据并且将预处理后的数据传送给人类分析师，从而将告警数量降低至每天100个。该实验室进行的实验表明其攻击的检测率高达85%，误报率亦可大幅降低。

蓝盾态势感知平台与以上MIT的系统有异曲同工之妙。她利用大数据技术进行海量数据的融合，利用人工智能识别各种安全攻击，支持追踪溯源和调查取证，实时评估整体网络的安全态势，预测其发展趋势，再配上可靠、有执行力的安全运维流程，多方协作，解决各种安全问题建立一个完整的安全保障体系，从而支撑业务应用的连续性，保护敏感信息的安全。这是场景驱动 & 数据驱动的典型应用。



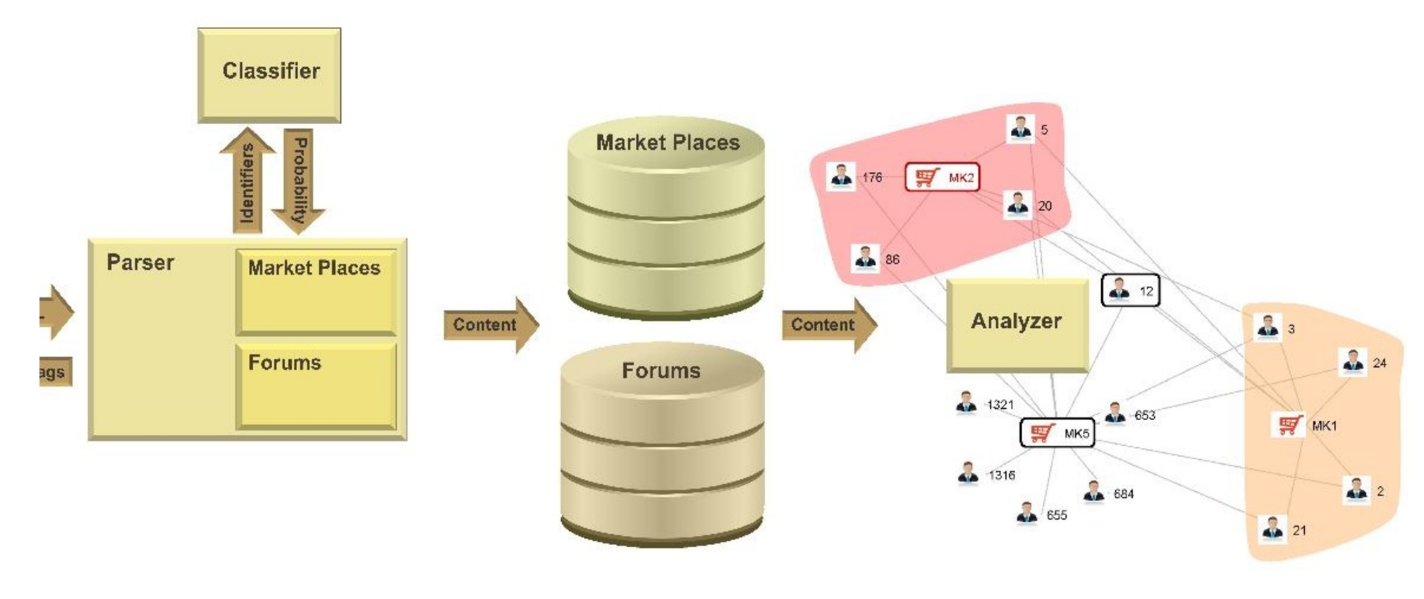
（Source：*AI^2: Training a Big Data Machine to Defend*, Kalyan et. al. ,2016 IEEE 2nd International Conference on Big Data Security on Cloud）



（蓝盾态势感知平台）

**4. 使用机器学习以检测零日漏洞 - 漏洞扫描与挖掘平台**

一些安全人士相信机器学习能够解决零日漏洞问题，特别是零日威胁和其他针对缺乏防御的IoT设备的攻击。针对此问题，安全领域已经具有相当多的研究工作。据福布斯引述，一批ASU的研究人员使用机器学习去检测在暗网中的流量并由此辨识出和零日漏洞相关联的数据。通过这种方式，组织机构将可能为漏洞打上补丁，并将远程非法操控拒之门外，预防数据泄露。



（Source：***MIT Technology Review***，“*Machine-Learning Algorithm Combs the Darknet for Zero Day Exploits, and Finds Them”*）

而集三大功能于一体（主机扫描、Web扫描和弱密码扫描）的蓝盾安全扫描系统，基于系统庞大、精良的漏洞库，采用先进的深度扫描、智能登录扫描等技术，全方位发掘网络中各类主机、设备、应用及系统的深层次脆弱点，立体地分析和呈现网络安全风险，让用户更准确地了解安全态势，快速精准修补漏洞，在网络攻击和威胁发生前做好坚实的防护。系统创新性地应用了智能任务调度算法，实现强大的安全漏洞扫描SAAS平台。

**5. 使用机器学习以提供智能分析服务—蓝盾安全云**

蓝盾将打造一个智能、专业的威胁分析平台，以云的方式提供基于人工智能的可疑文件、高危应用检测分析服务，适用客户群体可扩展到需要病毒深度分析能力的企业或个人，这将进一步推广和加深蓝盾智慧安全的品牌形象。



（蓝盾安全云）

**结语：**

2018年的网络安全是基于人工智能的网络安全。人工智能的高地是**兵家必争之地**。业界对于人工智能发展的共识是：场景、数据、计算能力和人才发展AI技术的四大要素。蓝盾希望在2018年能遵循此共识，继往开来，抱着雄心壮志在人工智能风起时，破浪前行**。**