# 前沿研究方向规划

目录

[前沿研究方向规划 1](#_Toc509910834)

[AI与文件检测引擎 1](#_Toc509910835)

[背景 1](#_Toc509910836)

[1、PE恶意文件检测引擎 1](#_Toc509910837)

[2、深度神经网络 1](#_Toc509910838)

[3、移动安全 1](#_Toc509910839)

[4、社会工程学 1](#_Toc509910840)

[蓝盾数据中心 1](#_Toc509910841)

AI与文件检测引擎

## 背景

目前网络安全已经进入了一个崭新的时代，面向各种新战场，需要新的架构、新的方法、新的编程语言来支撑我们应对越来越艰巨的战斗。新战场以黑产对抗、反勒索软件、反Insider-basedAPT、物联网/车联网这些新方向为代表。

一方面是新的攻击不断涌现，另一方面防守方却显得捉襟见肘了。安全的核心是对抗，而对抗是多维度的、持续的。为了进行有威慑力的对抗，最大的挑战还是缺少高素质安全专业人才。在这种情况下，**我们需要靠人工智能来填补人才空缺。**

下一代安全必然是基于数据驱动的，是基于人工智能的。人工智能AI的前沿技术可以为[网络安全](http://product.yesky.com/netsecurity/)防护提供新的思路，**为企业和组织在网络攻击中占据先机**。如今，越来越多的网络安全公司开始利用深度学习、自动化处理、人工智能等技术手段对数据进行深度分析，改善现有的安全防御体系，实现对威胁的快速及时响应和控制，在深度和广度上与攻击者抗衡。目前，用人工智能预测网络攻击的 Cylance 公司估值已达到 10 亿美元以上。

## 1、PE恶意文件检测引擎

Windows是目前最常见的操作系统，也是遭受网络攻击最频繁的系统。TrustPath开发部署于蓝盾第三代FW的AI引擎，在测试环境下可以达到99%的识别率，体现出AI技术的适用性。我们从AI引擎的本地化及自主研发的角度，结合当前PE恶意文件检测的新技术、大数据技术、以及安全对抗的的新形势，致力于实现一个可对标TrustPath的PE恶意文件检测引擎，为公司提供技术积累，也为公司产品提供更多的功能。

## 2、深度神经网络

深度学习是目前人工智能热点和趋势，已在图片和文字识别等领域取得了非凡的成绩，也使得越来越多的安全公司意识到这一领域带来的巨大机遇。我们根据公司现有的大量恶意样本库，考虑到病毒文件的特殊性，结合新技术的发展，致力于利用深度框架实现恶意文件的分析与检测。为公司的云安全产品，态势感知产品等提供更多的安全检测功能。

另一个方面，深度学习的发展也是一把双刃剑，利用深度学习来对抗安全检测也让安全态势变得越来越复杂。我们通过对对抗网络深入研究，致力于研发更加健壮的安全解决方案。

## 3、移动安全

移动互联网环境下，终端的发展对安全提出了巨大挑战。终端的智能化，内存和芯片处理能力的增强，带来了非法篡改信息、非法访问、病毒和恶意代码新的安全威胁。随着移动通信技术和应用的演进，移动终端也逐渐由通信工具向个人的信息处理中心转变，终端中存载着很多个人信息，一旦丢失或被窃取会造成很大的损失。因此，前沿对移动安全的规划包括恶意软件的检测和用户行为及隐私的保护。

**AI与Android恶意软件检测**

2018年移动安全线将整合AI引擎到产品中，虽然蓝盾已经拥有了自己的Android恶意软件检测AI引擎，而且准确度能够达到98%以上，但是该引擎属于初级阶段的产品，目前只能检测文件是恶意还是非恶意，对于恶意文件的更多其他信息，如家族信息、恶意行为等等暂时没办法输出，所以接下来需要继续深入研究，迭代AI引擎，以至于能够输出更多有用的信息。

**隐藏的敏感操作（HSO）**

用户对个人隐私越来越重视，如何能够准确检测出存在盗取用户信息行为的Android应用程序将是未来的一大难题。目前前沿组对这一块也是有规划，通过对Android应用程序进行细粒度的行为检测来达到检测信息泄露的行为。目前还有一个难题，Android应用程序加固的比例将会越来越高，所以单纯的静态分析可能不再合适，如何进行脱壳分析或者动态分析也是未来的发展方向。

## 4、社会工程学

如今在AI大数据迅速发展更新的大时代，如何获得更有价值的信息? 如和保护个人隐私? 如何预防机密信息泄露? 这些问题变得越来越重要，社会工程学已是企业安全最大的威胁之一。社会工程学是一种通过人际交流的方式获得信息的非技术渗透手段。网络攻击者正在转向基于文件的恶意软件，因为越来越多的攻击者使用邮件附件和网络链接，可是现在产品主要对可执行文件检测的比较多，而静态文件的审查检测要少的很多，这样就给企业安全带来一个很大破口， 为此，前沿将静态文件的检测加入到人工智能检测引擎中，为了更有效的保障企业安全与信息数据的保密。

**AI与文档检测引擎**

随着时间的推移，网络攻击者正在转向基于文件的恶意软件，PDF规格已经改变。增加的脚本功能可以使文档以与可执行文件几乎相同的方式工作，包括连接到Internet的能力，运行进程以及与其他文件/程序进行交互。内容复杂性的增长为攻击者提供了更多的武器来发动强大的攻击，并且更灵活地隐藏恶意有效载荷（例如，加密，隐藏为图像，字体或Flash内容）并逃避检测。现在主要针对静态特征的提取，与机器学习对恶意文档进行分类预测，目前均有一个非常良好的预测效果，下一步正对分类器的鲁棒性与抗逃逸做深入研究，使其有更加全面的分析预测能力可以输出到产品中。

另一个方面使用沙箱动态行为分析，主要针对于两个方面的研究，沙箱的对抗分析与动态行为分析。使用开源的cuckoo做开发基础，对文档的动态行为进行二次分析。

**安全沙箱**

**背景**

1. **沙箱对抗分析**
2. 动态行为分析

蓝盾数据中心