# 前沿研究方向规划

目录

[前沿研究方向规划 1](#_Toc509929789)

[SDN（软件定义网络）&NFV（网络功能虚拟化） 2](#_Toc509929790)

[背景 2](#_Toc509929791)

[1、P4专题 2](#_Toc509929792)

[2、SDN控制器专题 2](#_Toc509929793)

[3、安全云专题 3](#_Toc509929794)

[区块链 3](#_Toc509929795)

[背景 3](#_Toc509929796)

[1、区块链应用 4](#_Toc509929797)

[人工智能，大数据与网络安全 4](#_Toc509929798)

[目标 O 4](#_Toc509929799)

[时间范围 4](#_Toc509929800)

[关键成果KR 4](#_Toc509929801)

[AI与文件检测引擎 5](#_Toc509929802)

[背景 5](#_Toc509929803)

[1、Windows恶意文件检测引擎 6](#_Toc509929804)

[2、深度神经网络 6](#_Toc509929805)

[3、移动安全 6](#_Toc509929806)

[4、社会工程学 7](#_Toc509929807)

软件脆弱性智能分析技术 [8](#_Toc509929808)

[背景 8](#_Toc509929809)

[1、基于深度学习的 9](#_Toc509929810)

SDN（软件定义网络）&NFV（网络功能虚拟化）

## 目标 O

* 将SDN技术落地到公司产品中

## 时间范围

* 2018

## 关键成果KR

* SDN方向1位研究员，完成以下目标：
  + 完成4项SDN和NFV方面的专利；
  + 攻坚公司云计算产品中控制器和交换机方面所碰到的技术难题；
  + 参与公司云计算产品的开发工作，并向其他开发人员提供相关培训。

## 背景

SDN全称是Software Defined Network,即软件定义网络，是一种网络设计理念，或者一种推倒重来的设计思想。只要网络硬件可以集中式软件管理，可编程化，控制转发层面分开，则可以认为这个网络是一个SDN网络。NFV全称是Network Function Virtualization，即网络功能虚拟化，关注网络转发功能的虚拟化和通用化，将网络功能从专用设备(硬件架构不一定是X86)迁移到通用X86服务器上运行的虚拟机或者容器中。

NFV和SDN如果相互结合，又可以是互补的存在。借助SDN，不仅传统的NF连接方式都能支持，SDN还能提供更高效的NFV实现方式。毕竟SDN提供的管理层和转发层的分离，使得网络变得极其灵活。反过来，NFV也能够提供SDN的运行环境，帮助SDN的实现。

## 1、P4专题

P4是一门编写协议无关的包处理器的高级语言，是一种声明式编程语言，主要用于编程程序以下达指令给数据转发平面的设备(如交换机、网卡、防火墙、过滤器等)如何处理数据包。通过P4我们可实现：定制数据解析流程、可执行并行和串行的匹配+动作操作、支持协议无关的转发。通过这些特性，我们可以更好的控制数据流向，并在高性能的保障下为公司的业务提供更强的功能。

## 2、SDN控制器专题

当前SDN控制器种类繁多，主流的控制器有14种。其中最为出名的是由服务商共同参与的开源OpenDaylight（ODL）项目及运营商主要关注的ONOS项目。我们将基于现有项目的接口或开源的代码，快速实现公司的产品功能。由于控制器的更新较快，我们将持续关注新功能的推出，以求更好的利用到产品中来，同时降低开发成本。

## 3、安全云专题

安全云专题主要包括安全虚拟器件和容器级别的虚拟化安全服务两种。通过这两种方式，可提供安全云服务。

安全虚拟器件是NFV（网络功能虚拟化）的一种。通过这种技术，我们将公司的传统产品以软件的形式向客服提供服务。安全虚拟器件本质上是一个虚拟设备，可以很方便的部署在云端，有很好的扩展性。同时可考虑实现容器级别的虚拟化安全服务。

区块链

## 目标 O

* 将区块链与公司产品结合，提出市场可行的方案

## 时间范围

* 2018

## 关键成果KR

* 区块链方向1位研究员，完成以下目标：
  + 完成2项区块链方面的专利；
  + 完成至少2项可行的区块链方案；
  + 参与并指导公司区块链产品的开发工作。

## 背景

区块链是对过往技术的重新组合，是现阶段信息科技创新的高潮。作为分布式账本的一种，区块链兼具去中心化和环环相扣的特点。因为区块链的特性，很多企业或者说机构都看到了区块链在未来发展中的效用。而且从近期国家频频出现的动作来看，并不是只有银行及支付行业被区块链科技影响到，很多领域都在慢慢涉及。

区块链本质上是一个去中心化的分布式账本数据库。其本身是一串使用密码学相关联所产生的数据块，每一个数据块中包含了多次比特币网络交易有效确认的信息。

## 1、区块链应用

区块链已经成为了当前的热点所在。如何寻找到该技术和行业的密切结合点，推出先进的产品，在市场上产生巨大的影响力。

人工智能，大数据与网络安全

## 目标 O

* 让AI赋能蓝盾

## 时间范围

* 2018 Q2 – Q4

## 关键成果KR

* 蓝盾人工智能实验室**5位**安全研究员继续合作，并参与到以下**4个问题和方向**的讨论中。计划是在2018年Q2结束前，整个实验室有**2篇**文章被录取。
  + PE文件检测与大数据分析
  + APK文件检测与移动安全分析
  + PDF文件检测与社交工程分析
  + 大数据框架与数据服务（业务系统支撑）
* 作为蓝盾咨询的角色，继续与蓝盾**4产品组继续**合作，并参与到制定这4个产品的技术规划中。计划是在2018年Q2结束前，4类产品均已经成功被AI赋能，并达到能交付到客户的稳定度，计划写作技术规划**文章（answered by request）**
  + 边界安全产品组-防火墙
  + 移动安全产品-EMM
  + 全局态势安全产品-态势感知产品
  + AI for everybody-蓝盾云
* 与**2外部团队**保持合作，引入其核心技术到蓝盾产品中，已成功引入**2项**（具体见下），计划是在2018年Q2会多引入**4项**：
  + Trustpath团队的Machine Learning based Malware Detection Engine
  + Panda团队的 深度学习与动静结合 引擎
* 作为泛AI化战略的一部分，我们将会在2018年Q2-Q4对以下**6个领域**进行市场调研与案例分析等
  + AI安全芯片
  + 物联网安全
  + 雷达
  + 语音识别
  + 人脸识别智慧软件等

AI与文件检测引擎

## 1、Windows恶意文件检测引擎

### 目标 O

* 自研PE恶意文件检测引擎，可赋能于公司的云安全产品等

### 时间范围

* 2018

### 关键成果KR

* PE恶意文件检测方向1位研究员，完成以下目标：
  + 完成1篇恶意文件检测方面的论文；
  + 性能可对标与TP的AI引擎，可部署与公司云安全产品；

### 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。

### 简述

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Windows恶意文件检测的新技术、大数据技术、以及安全对抗的新形势，致力于实现一个可对标TrustPath的恶意文件检测引擎，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

### 目标 O

* 将深度学习与公司安全产品结合，提出可行的解决方案

### 时间范围

* 2018

### 关键成果KR

* 深度学习方向1位研究员，完成以下目标：
  + 完成至少1篇基于深度学习的恶意文件检测相关的论文或专利；
  + 完成至少2项基于深度学习的恶意文件检测的技术方案设计与实现；

### 简述

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，态势感知等产品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

### 目标 O

* 改善 apk 恶意软件的AI检测引擎，并增加引擎支持更多分类类型的功能，并且部署到移动安全线的产品

### 时间范围

* 2018

### 关键成果 KR

* 移动安全方向1位研究员，完成以下目标：
  + 支持移动安全线产品中部分功能的研发需求
  + 增加 恶意软件家族 分类模型 1 个,识别率 到达 95%
  + 增加 HSO 模型 1 个,识别率 到达 98%
  + 完成 英文论文一篇 并 提交 到 信息安全 顶级会议中
  + 阅读并收集 至少 50份 顶会论文，形成自己独有的研究方向2个，由此产生技术壁垒

### 简述：

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

### 目标 O

* 改进基于恶意文件的检测和分类引擎，针对恶意文件逃逸Model ，建立新的抗逃逸model ,并且部署到对应的检测引擎中

### 时间范围

* 2018

### 关键成果 KR

* 社会工程方向1位研究员，完成以下目标：
  + 新计算特征 10 个，添加到抗逃逸的检测Model 中，
  + 迭代检测Model 3 次 以上，以加强其鲁棒性
  + 增加 自动逃逸 模型 1 个，参考Automatically Evading Classifiers
  + 完成 英文论文一篇 并 提交 到 信息安全 顶级会议中
  + 阅读并收集 至少 10份 顶会论文，形成自己独有的研究方向2个，由此产生技术壁垒

### 简述：

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，使其有更加全面稳健的分析预测能力可以输出到产品中。

软件脆弱性智能分析技术

## 1、基于深度学习的漏洞检测系统

### 目标 O

* 构建基于深度学习的漏洞检测系统

### 时间范围

* 2018

### 关键成果 KR

* 深度学习方向1位研究员，完成以下目标：
  + 基于深度学习的智能漏洞检测系统原型
  + 实施5种技术比较（Checkmarx, Flawfinder, RATS, VUDDY and VulPecker）
  + 完成每周一篇论文以及一篇阅读笔记

### 简述

软件脆弱性智能分析技术是目前重要研究课题。但是，目前解决方案主要是依靠人工自定义软件脆弱性特征，导致经常遗留下大量软件漏洞（例如出现高误报率）。

大量网络攻击来源于软件漏洞，尽管在安全编程技术方面做了努力，但是软件漏洞仍然遗留，并将继续成为一个标志性的问题。这可以通过以下事实来证明：2010年通用漏洞披露（CVE）中登记的漏洞数量约为4,600个，2016年增长至约6,500个。有一种替代的方法是在软件程序中（或简称程序）智能检测漏洞。目前已经存在有大量的静态检测漏洞的系统以及学术研究，范围是从开源工具到商业工具，再到学术研究的项目。然而，目前漏洞检测的解决方案有两大缺点：消耗人工劳动，以及出现高漏报率。

所以我们需要将AI与漏洞检测结合，用基于深度学习的漏洞检测来减轻人工繁杂的自定义特征的工作。