1. Q1季度

**网络安全审计**：

1. 开发前端检测器负责各个模块业务上逻辑处理，界面优化，代码优化，测试部bug修复
2. 检测器日志后台v1.2版本内测以及性能优化
3. 开发检测器日志后台v1.3简易版本，功能需求上改进，测试部提交bug处理，ie8兼容性问题以及界面显示问题处理，数据表迁移，并处理对应sql语句优化等
4. 远程协助客户修复检测器，客户需求开发处理

**前沿组**：

大数据基础架构（Hadoop+Spark）

1.集群维护

2.搭建数据中心自动化数据采集，数据同步平台（构建大量脚步，以增加大数据体系的自动化程度如爬虫：周期性从各种数据源收集数据如病毒样本，病毒分析报告以及程序源代码等，蓝盾数据中心目前已达到400多万样本。）

3.提供开源沙箱cuckoo 动态文件行为分析服务

4.为合作方软件基因 每周提供病毒样本（提供对方指定MD5值的病毒样本以进行深度学习模型实验）

未来规划方向：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。