第二月工作月度总结

转眼之间，入职第二个月也过去了，在第二个月的工作期间中，利用自身所学以及不断对我司产品常见问题的解决方案的学习，承担起了日常漏洞扫描和安全应急响应的工作，并在工作之余也主动去补充安全相关知识的学习，希望在以后可以承担起更多的职责。

本月在工作成果方面，主要分为三块：

1、前端爬虫项目开发：前端部门需要对HiKVision官网海内五千余款及海外两千余款产品的产品信息、详细参数和产品结构图进行收集，通过手工方式费时费力，于是开发了Hikang官网爬虫框架，使用Html结构化和正则表达实现精准页面元素抽取，并对官网反爬机制做了绕过和控制访问频率，并对每个功能做了模块化封装，方便以后的调用和二次开发维护。

在Hikang官网进行维护期间和严格GCD云盾反爬机制下，手工访问产品页面都无法查看到具体产品参数信息，使用爬虫依旧保持在抓取成功率98%以上，及时为前端部门提供了最新的友商竞品信息。

2、开源组件跟踪：针对目前多数漏扫软件对于各部门所引用的开源组件漏洞检测存在漏报的情况，在本月推动和跟踪各个部门所有产品对于开源组件的引用详细信息，并整理汇总成表格；每周跟踪各个开源组件版本存在的安全漏洞和新爆出来的危险漏洞进行预警和分析，提问题单，跟催研发修复漏洞，保证产品的安全性。

3、漏洞扫描及漏洞分析和应急响应：本月完成齐鲁石化、荆门石化、北京市交通委、认证环境等项目的安全应急响应和解决方案，为产品和项目的顺利交付提供安全方面支持；同时与部门研发一起研究寻找vsftpd、TS8500 Trace关闭、Tomcat等高危漏洞的解决方案，并保证漏洞修复成功的同时，对系统无任何影响后发给项目上。

本月在工作过程之余，也会在工作的基础上去扩展自己的知识和技术范围，通过不断反思和改进工作内容，来提高自己的知识储备和技术能力。比如在开发爬虫的过程中，经常性的遇到反爬虫机制，通过网上的搜索和个人思考，采用了控制访问频率、设置身份验证cookie、正则结构化抽取反爬页面并重放请求等方法来绕过反爬机制，针对越来越多的站点，去搜寻常见识别算法和通用抽取算法等。同时针对自己的岗位也制定了每日的学习计划，包含Metaspoit、Kali渗透测试以及安全开发规范设计等方面知识。

在这一个月中分析自己的工作情况，总结反思自己：偶尔在工作过程中容易分心，对于技术方面总是冒出一些奇怪的想法，然后去论证和尝试这些思路 ，导致工作进度有些耽误，后续要保证工作完成的前提下再去扩展研究，。

下月工作计划：根据本月的工作情况，对进行中的工作继续完成，同时希望能够承担一些更有挑战性的工作和任务，不断地提高自己，锻炼自身，不断进步。