0.设计网络流量监测功能，并且可以按照协议划分对应的流量，再根据协议划分对应的字段和数据包

1.完善主机监测功能，对于进程和文件监测更进一步，文件监测可以监测全局文件的添加变化，着重监测注册表等重要文件变化

2.封装主机监测功能和网络流量监测功能到客户端，并且可以将数据实时反馈给服务端

3.封禁策略 基于签名规则策略（根据一张规则表静态去判断流量是否为恶意攻击流量） 或者 基于行为策略（基于学习算法预测是否为攻击行为流量）

4.页面设计









5.根据第三点的策略进行web端告警通知,web页面右上角有个消息红点类似于qq的消息点