问题3：

异常员工及其事件：

我们用多方法预检测并交叉比对的方式查找公司内部可能存在的异常事件，基本思路是独立地使用不同的方法发现疑似异常事件/人员，然后将不同方法的结果汇总。若一个员工同时出现在两种及以上异常检测的名单中，则该员工可能确实存在异常动机和行为；出现次数越多，则可能性越大。通过数据可视化，我们为公司管理者提供了四种异常预检测方法：（1）排查异常时间登录公司服务器的现象；（2）排查大量tcp流量；（3）排查对公司服务器过于频繁的页面访问；（4）排查异常的上下班时间。另外，也可以关注员工对敏感内容网站的访问，比如对个别黑客技术网站的访问：hackdig, web2hack。

基于如上方法，我们发现了如下异常员工：

1173号：11月1号较晚时间（22:10）在50.47公司服务器上登录，当日下载量排名第10名；然而从weblog记录来看，该员工本月并未访问过该服务器的页面；该员工平时的网页访问量主要集中在研发组所有人都常用的几个服务器和50.44，并非50.47。总之，该员工在大多数人下班后登录并不常用的服务器并大量下载文件，我们认为这可能存在潜在的安全隐患：该员工可能利用系统漏洞私自拷贝不相关的资料，或者是电脑被安装病毒/木马程序之后自行下载资料。如图3-1。

1265号：该员工有访问黑客技术网站的记录。11月14号，该员工比自己通常的下班时间（7-8点）晚了近两小时下班；当日，该员工下载总量在所有员工中排名第10，大部分流量来自服务器50.40；同时，该员工当日对50.40服务器的页面访问次数排名也很靠前。如图3-2。这几项异常让我们不得不对其动机产生怀疑，有进一步深入调查的必要。