一．事件列举

事件 1:

通过对视图 3 的观察我们发现，id 为 1487 号员工的用户的 ip 地址登录错误的的次数明显高于正常范围。（图 3.1）

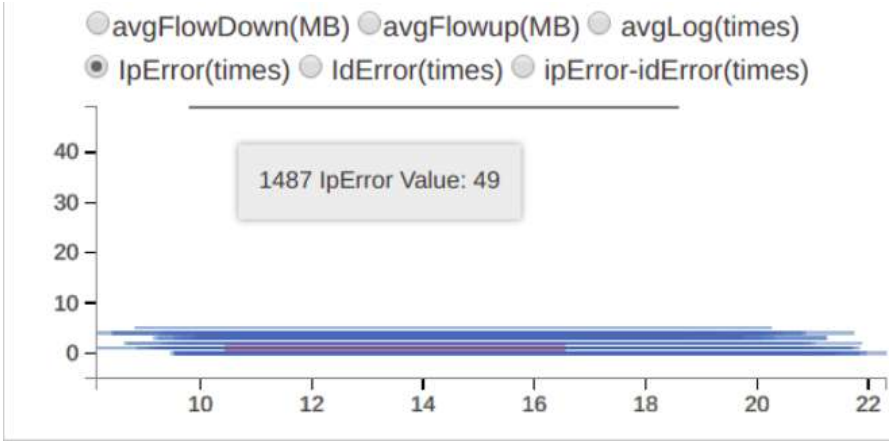

图 3.1 各 ip 地址登录错误次数统计（黑线为 1487）

而当统计 ip 地址登录错误和 id 被登录错误次数的差值是发现，1487 号员工两项统计数据的差值也明显高于正常范围。（图 3.2）

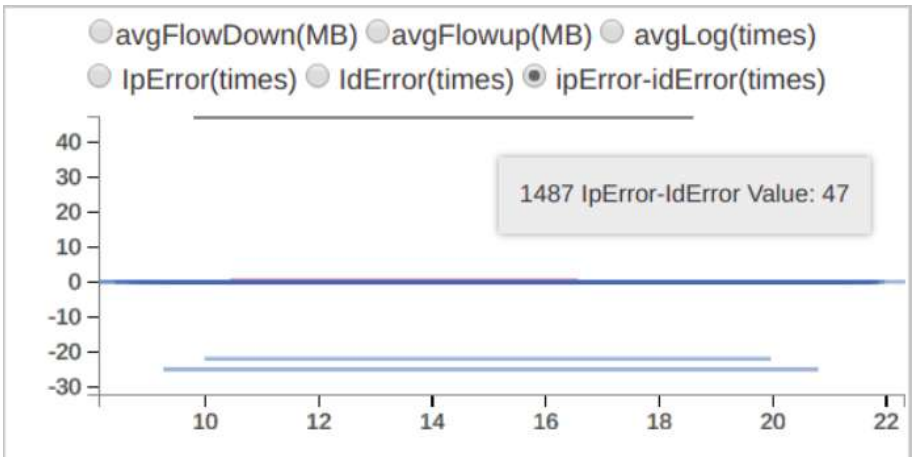

图 3.2 各 ip 地址登录错误次数与各 id 用户名被登录错误次数差值统计

通过分析，我们认为会产生上述情况的原因是，1487 号员工的 ip 地址的错误登录并非用来登录自己的用户 id，而是试图侵入其他员工的用户 id。

事件 2

通过事件 1，我们所定了 1487 号员工为怀疑对像，选中他后，观察视图 4 我们发现该员工在 11 月 4 日在没有产生别的流量协议的情况下产生了 ssh 协议流

量。通过联动，我们在视图五中展示了 1487 号员工在 11 月 4 日的各协议流量情况。（图 3.3）

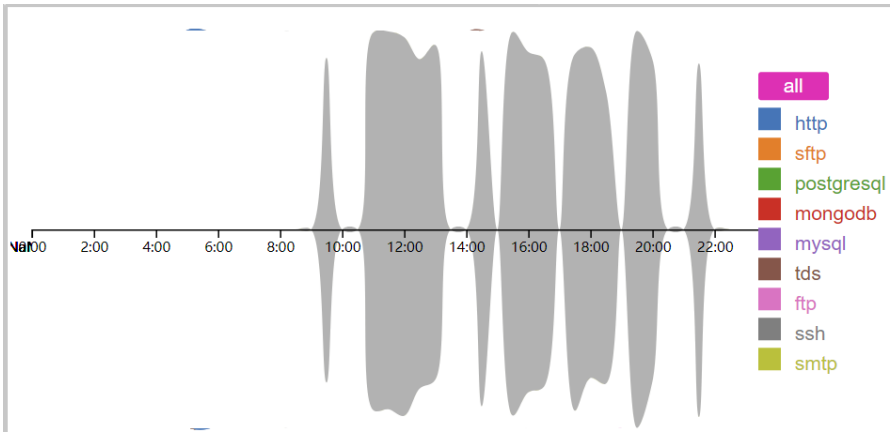

图 3.3 1487 号员工 11 月 4 日流量汇总图

从图 3.3 中我们可以看出，1487 号员工在 11 月 4 日当天没有到公司签到，也没有登录自己的用户 id。并且除了 ssh 流量外没有产生别的协议流量，这基本排除了他远程工作的可能性。因此 1487 号员工极有可能在 11 月 4 日通过自己的 ip 地址使用 ssh 建立连接试图侵入其他员工的用户 id。

事件 3

为了寻找被 1487 号员工在 11 月 4 日侵入的用户 id，我们从视图 3 的统计中，ip 地址登录错误和 id 被登录错误的差值为负数并且明显小于其他员工的员工 id。它们是 1211，1080，1228。（图 3.4）

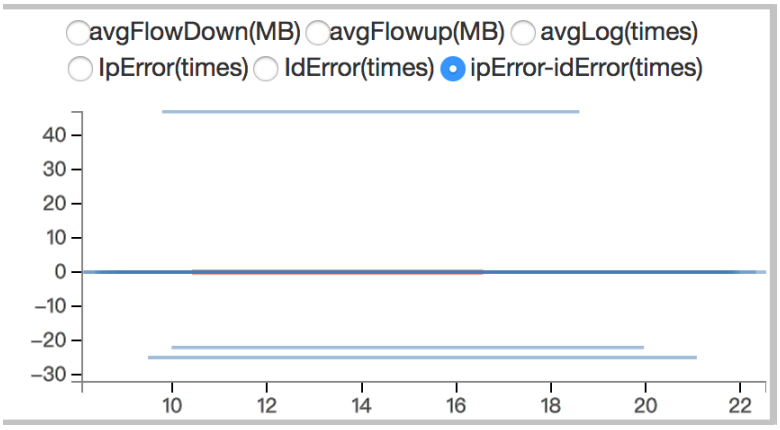

图 3.4　各 ip 地址登录错误次数与各 id 用户名被登录错误次数差值统计

通过观察三位员工在 11 月 4 日当天的流量汇总图，我们发现 1211 号员工的流量在 11 月 4 日存在明显异常。（图 3.5）

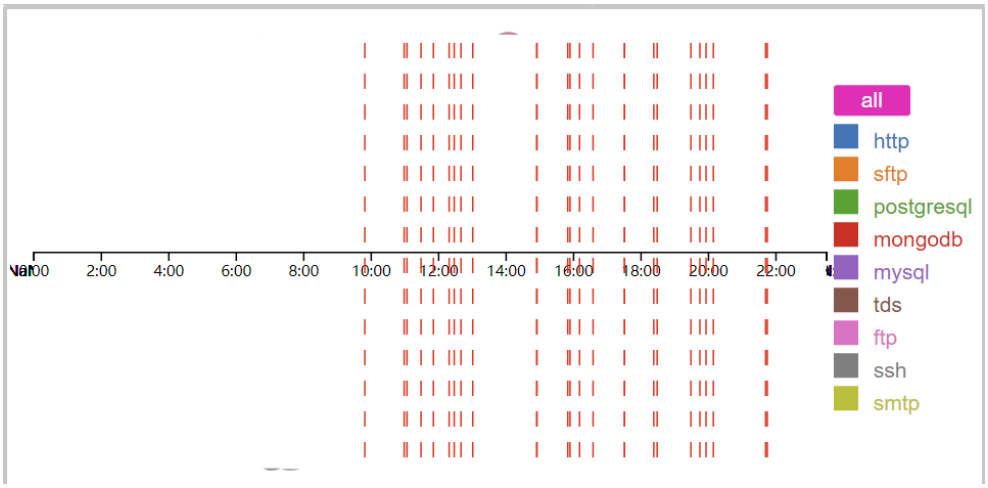

图 3.5　1211 号员工 11 月 4 日流量汇总图

从图 3.5 中我们可以看出，在 11 月 4 日的 10:00 到 22:00，1211 号员工的用户 id 被连续多次试图登录并失败，单 1211 号员工在当天未来到公司也没有产生与工作相关的协议流量。

因此我们猜测在 11 月 4 日，1487 号员工通过 ssh 建立链接，在 10:00 到 22:00 之间一直试图侵入 1211 号员工账号。

事件 4

而对于和 1211 号员工一样账号明显在 11 月中某些时间被人不断试图入侵的员工 1080。我们采用使视图 4 和视图 6 联动的方法动态观察他 11 月每一天的流量汇总情况。发现在 11 月 3 日，该员工的账号被多次入侵失败。（图 3.6）

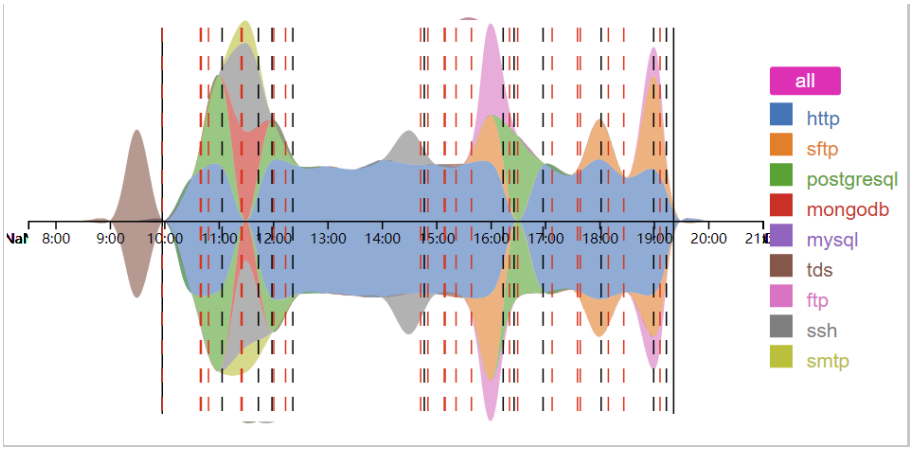

图 3.6　1080 号员工 11 月 3 日流量汇总图

事件 5

同样的对于 1228 号员工，我们在动态观察后发现，他在 11 月 6 日，也出现

了账号被多次入侵失败的异常情况。（图 3.7）

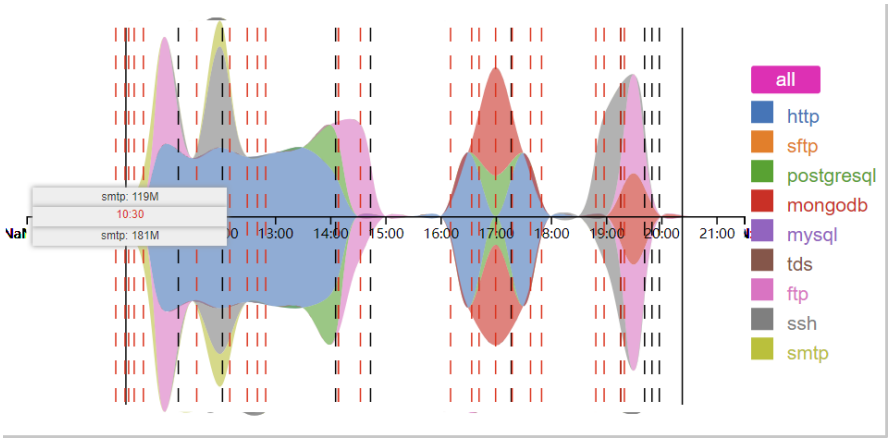

图 3.7　1228 号员工 11 月 6 流量汇总图

事件 6

联动观察后发现，ip 为 1281 的研发部门员工在他的同组成员中，访问的下行流量明显要多并且落差很大（图中红线为 1281 号员工，蓝线表示同组其他员工）（图 3.8）

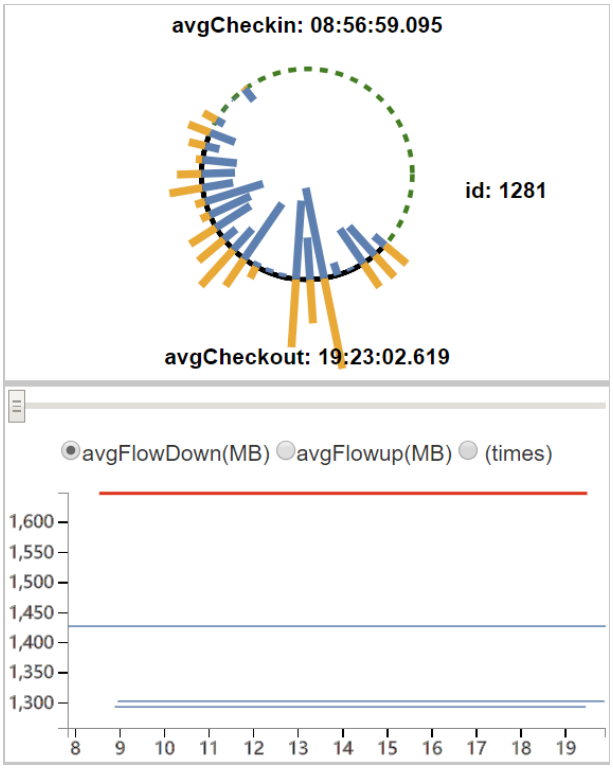

图 3.8　1281 号宇员工平均下行流量图

二．事件关联分析

人物分析:

1、事件 1，2 中的试图侵入其他员工账号的 1487 号员工，事件 3，4，5 中被侵入账号的 1211，1080，1228 号员工，和事件 6 中下行总流量异常的 1281 号员工都属于研发部门。

2、而被侵入账号的 1211，1080，1228 号员工都是隶属 id 为 1059 的研发部门领导的二级领导。

3、1487 号员工使 1228 号员工为二级领导的研发部门小组的成员。

数据库定向查询添加的信息

为了得到更多的信息，我们把有问题的员工 id 在后台 mysql 数据库中进行了定向查询。得到了以下信息。

1、试图侵入 1211、1080, 1228 号员工账号的 ip 地址为 10.64.105.4，即 1487 号员工的 id。

2、1487 号员工曾经成功访问过他的领导 1228 号员工的账号三次，时间分别为：11 月 6 日 19:42:57；11 月 16 日 20:22:04；11 月 24 日 12:43:41.

在观察 1228 号员工 16 日和 24 日的流量情况后（11 月 6 日的流量汇总图在图 3.7 中已经显示）我们发现在被 1487 号员工入侵的时间里，1228 号员工 id 产生的流量基本为 mysql、mongodb 这样的数据库协议和 ftp 即传递文件协议。（图 3.9，图 3.10）

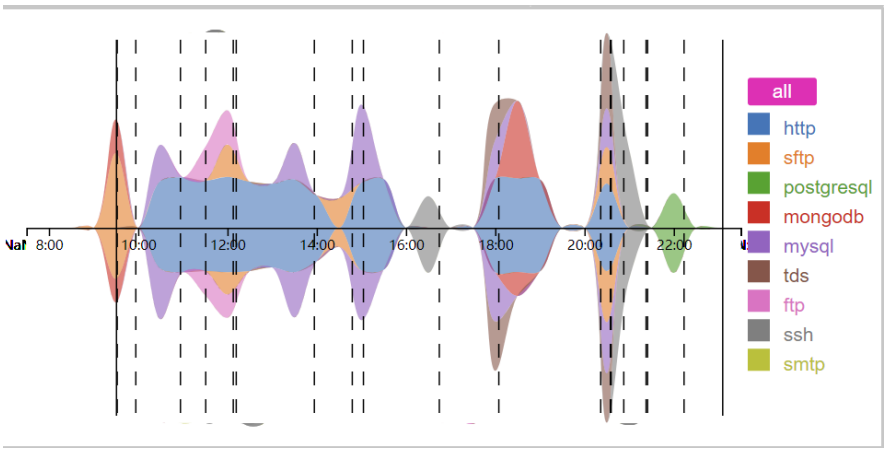

图 3.9 1228 号员工 11 月 16 日流量汇总图

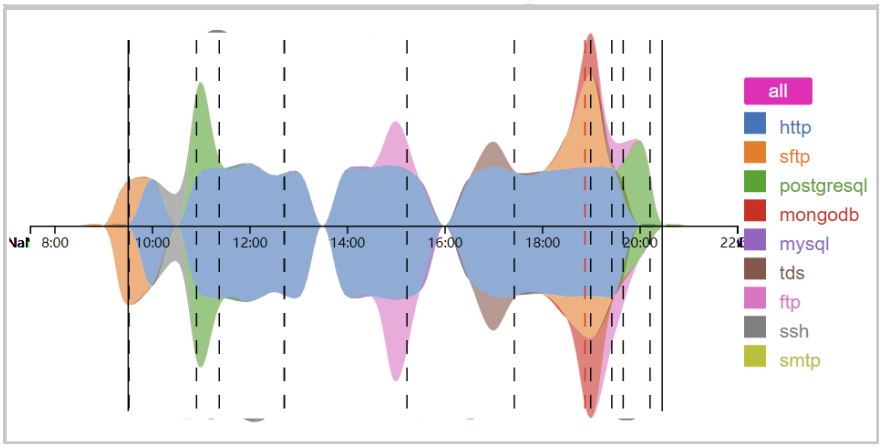

图 3.10 1228 号员工 11 月 24 日流量汇总图

3、而事件 5 中流量异常的 1281 号员工在我们从数据库中定向查询后发现，他和 1487 号员工同时在 11 月 27 日提出了辞职申请。同一天提出辞职申请。而同一天还有 1376 号员工也提出了辞职，该员工则与同样被是图侵入用户的 1211 号员工在同一小组。

分析和猜想

被 1487 试图入侵账号的三个员工都是隶属 id 为 1059 的研发部门领导的二级领导。他们的账号中很有可能有关于新产品的信息内容

因此我们揣测，很有可能是 1487 号，1281 号，1376 号员工共同试图窃取公司新产品的信息向外界传递并且在事后后辞职。