1. **模型因子与log中对应关系：**

**异常数据传输场景**

外发文件次数异常 - hit\_normal\_file 注意发送时间段

外发文件大小异常 - 留空

非工作时间外发数据次数异常 - hit\_normal\_file 注意发送时间段

触发ITM内置策略 - hit\_inside\_itm

触发ITM：未知文件类型策略 - hit\_unkown\_type

触发ITM：证书私钥策略 - hit\_cert\_key

触发ITM：SAM或passwd文件策略 - hit\_passwd

触发ITM：客户DLP策略（员工通信录，客户通信录） hit\_cust\_info

**员工离职场景**

外发简历 - hit\_resume

访问招聘网站 - recruit （swg-\* log中可以看到）

外发文件次数异常 - hit\_normal\_file

外发文件大小异常 -留空

触发ITM：外发加密文件策略 -hit\_encrypt

触发ITM：客户DLP策略（员工通信录，客户通信录） - hit\_cust\_info

**研发数据泄露场景**

外发文件次数异常 - hit\_normal\_file 注意发送时间段

外发文件大小异常 - 留空

非工作时间外发数据次数异常 - hit\_normal\_file 注意发送时间段

向GitHub或SVN传输文件 - 参考日志中：



触发ITM：研发代码策略 - hit\_src\_code

**感染木马场景**

下载恶件 - type: virus, count: #

访问不安全网站 - type: unsafe, count:#

触发ITM内置策略 - hit\_inside\_itm

非工作时间外发数据次数异常 - hit\_normal\_file 注意发送时间段

非工作时间外发数据大小异常 - 留空

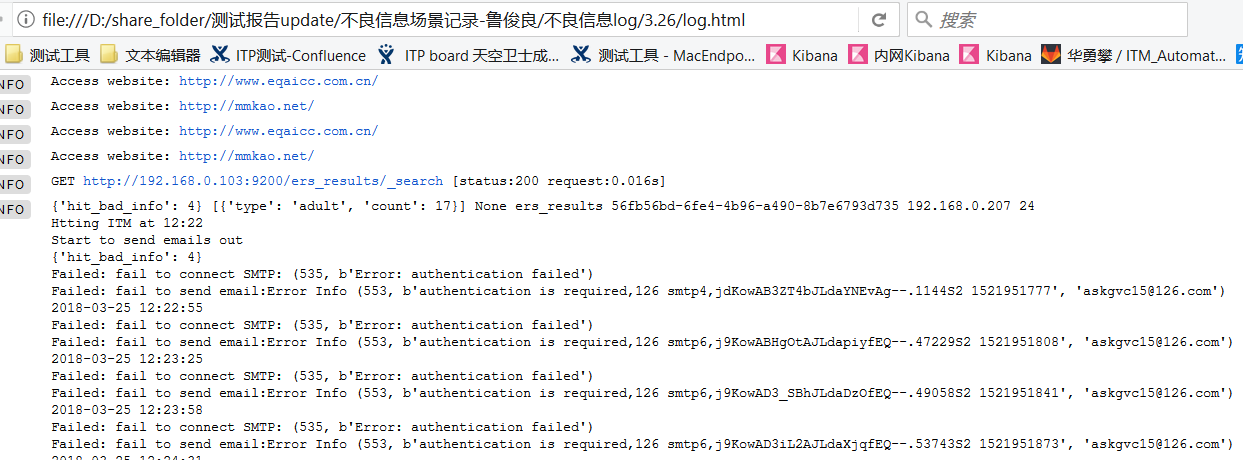
触发ITM：SAM或passwd文件策略 -hit\_passwd

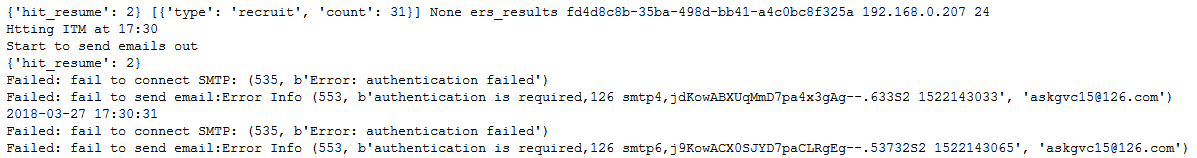
触发ITM：客户DLP策略 - hit\_cust\_info

1. **测试案例分配建议：**

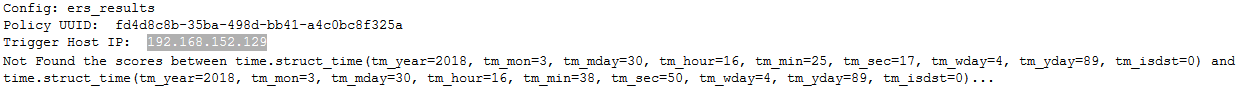
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 机器1 | 机器2 | 机器3 | 机器4 | 机器5 | 机器6 | 机器7 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 异常数据传输场景 | | | | | | | |
| 顺序 | Abnormal\_Data\_Transport\_Test\_Case\_05 | Abnormal\_Data\_Transport\_Test\_Case\_06 | Abnormal\_Data\_Transport\_Test\_Case\_07 | Abnormal\_Data\_Transport\_Test\_Case\_08 | Abnormal\_Data\_Transport\_Test\_Case\_09 | Abnormal\_Data\_Transport\_Test\_Case\_10 | Abnormal\_Data\_Transport\_Test\_Case\_11 |
|  | Abnormal\_Data\_Transport\_Test\_Case\_02 | Abnormal\_Data\_Transport\_Test\_Case\_04 |  | Abnormal\_Data\_Transport\_Test\_Case\_03 | Abnormal\_Data\_Transport\_Test\_Case\_01 |  |  |
| 下午6点以后 | Abnormal\_Data\_Transport\_Test\_Case\_11\_02 | Abnormal\_Data\_Transport\_Test\_Case\_11\_02 | Abnormal\_Data\_Transport\_Test\_Case\_11\_02 | Abnormal\_Data\_Transport\_Test\_Case\_11\_02 | Abnormal\_Data\_Transport\_Test\_Case\_11\_02 | Abnormal\_Data\_Transport\_Test\_Case\_11\_02 | Abnormal\_Data\_Transport\_Test\_Case\_11\_02 |
|  | Abnormal\_Data\_Transport\_Test\_Case\_05 | Abnormal\_Data\_Transport\_Test\_Case\_06 | Abnormal\_Data\_Transport\_Test\_Case\_07 | Abnormal\_Data\_Transport\_Test\_Case\_08 | Abnormal\_Data\_Transport\_Test\_Case\_09 | Abnormal\_Data\_Transport\_Test\_Case\_10 | Abnormal\_Data\_Transport\_Test\_Case\_11 |
|  | Abnormal\_Data\_Transport\_Test\_Case\_02 | Abnormal\_Data\_Transport\_Test\_Case\_04 |  | Abnormal\_Data\_Transport\_Test\_Case\_03 | Abnormal\_Data\_Transport\_Test\_Case\_01 |  |  |
| 不良信息场景 | | | | | | | |
|  |  |  | Bad\_Info\_Test\_Case\_01 |  |  | Bad\_Info\_Test\_Case\_02 | Bad\_Info\_Test\_Case\_03 |
|  | | | | | | | |
|  |  |  |  |  |  |  |  |

1. **问题汇总：**
2. **邮箱认证失败**





1. **确认IP是否正确**



虚拟机网卡设置方式：桥接

1. **ES 连接不稳定，只能却Kibana上面查询**

**异常**：

1522828128(1)

1522828135(1)

**正常**：



1. **Recruit对应访问招聘网站**

hit\_normal\_file 对应外发文件

1522828401(1)

1. **注意git环境配置**

