攻击者群组画像

### 1、设计原理

通过攻击者的攻击特征，包括攻击时间、攻击地点、攻击类型、将相似攻击行为的攻击主机进行分组，进行攻击者分组画像，发现攻击者的攻击行为的特征，对攻击行为进行有效防范。

### 2、数据源

数据源来自威胁情报，字段如下:

|  |  |
| --- | --- |
| 字段解释 | 字段名 |
| 源ip | SRCIP |
| 目的ip | DSTIP |
| 记录时间 | RECORDTIME |
| 应用层协议 | PROTOCOL |
| 上行字节数 | UPBYTESIZE |
| 源端口 | SRCPORT |
| 目的端口 | DSTPORT |
| 数据流方向 | FLAGIP |
| 目的ip经度 |  |
| 目的ip纬度 |  |

### 群组画像分类

针对确定的攻击地点和攻击目标，将单位时间内的数据流量，根据确定的攻击地点和攻击目标（dstip，dstport，同个经纬度），根据攻击目标特征分组。

1. 以（dstip\_dstport\_经纬度）作为分组类别，统计在单位时间内，针对该攻击目标的攻击手法进行整合；
2. 对组内的攻击时间计算时间间隔，统计时间频率；
3. 对组内攻击者的地理位置进行整合，形成身份画像

被攻击资产群组画像

### 1、设计原理

通过被攻击者的被攻击特征，包括被攻击时间、被攻击地点、被攻击类型、被攻击频率，将相似攻击行为的被攻击主机进行分组，进行被攻击者分组画像，发现被攻击者的特征，对攻击行为进行有效防范。

### 2、数据源

数据源来自威胁情报，字段如下:

|  |  |
| --- | --- |
| 字段解释 | 字段名 |
| 源ip | SRCIP |
| 目的ip | DSTIP |
| 记录时间 | RECORDTIME |
| 应用层协议 | PROTOCOL |
| 上行字节数 | UPBYTESIZE |
| 源端口 | SRCPORT |
| 目的端口 | DSTPORT |
| 数据流方向 | FLAGIP |
| 源ip经度 |  |
| 源ip纬度 |  |

### 3、群组画像分类

针对确定的攻击地点和攻击目标，将单位时间内的数据流量，根据确定的被攻击地点和攻击目标（srcip，srcport，同个经纬度），根据攻击目标特征分组。

1. 以（srcip\_srcport\_经纬度）作为分组类别，统计在单位时间内，针对该攻击目标的攻击手法进行整合；
2. 对组内的被攻击时间计算时间间隔，统计时间频率；
3. 对组内攻击者的地理位置进行整合，形成身份画像