



万象智维网络安全超自动化平台

syslog采集设备:

设备参数初始化完成

1. **111**

syslog日志收集: -> 收集字段信息:【attack\_type,host\_state,ioc,host,type,rule\_desc】

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **attack\_type** | **host\_state** | **ioc** | **host** | **type** | **rule\_desc** |
| **远控木马** | **失陷** | **119.23.253.248:88** |  | **远控木马** | **Gh0st RAT远控木马活动事件** |
| **远控木马** | **失陷** | **182.40.146.166:49156** |  | **远控木马** | **DarkKomet远控木马活动事件** |
| **远控木马** | **失陷** | **122.10.27.109:7800** |  | **远控木马** | **普通远控木马活动事件** |
| **远控木马** | **失陷** | **39.164.228.8:49156** |  | **远控木马** | **DarkKomet远控木马活动事件** |
| **远控木马** | **失陷** | **su.sgwvrs.com** | **su.sgwvrs.com** | **远控木马** | **Flystudio U盘病毒活动事件** |
| **远控木马** | **失陷** | **\*unixtimes.org** | **out.unixtimes.org** | **远控木马** | **普通远控木马活动事件** |
| **远控木马** | **失陷** | **\*unixtimes.org** | **onow.unixtimes.org** | **远控木马** | **普通远控木马活动事件** |
| **远控木马** | **失陷** | **183.205.180.245:49156** |  | **远控木马** | **DarkKomet远控木马活动事件** |
| **远控木马** | **失陷** | **ott.office123456.com** | **ott.office123456.com** | **远控木马** | **普通远控木马活动事件** |