



CSAP安全事件规格匹配

日志采集器

杨雅伦

2021-11-23 发表

组网及说明

不涉及

问题描述

在态势感知处置中心中看到如下的信息，咱们设备是如何判定为挖矿通信的？源日志为字符串，字符串是什么意思？字符串怎么匹配

The screenshot displays a security event analysis interface. The top section shows a summary of event counts for various categories. Below this, a table lists individual events with columns for event type, status, time, source IP, destination IP, and other details. A specific event is highlighted, and a modal window titled '日志详情' (Log Details) is open, showing the raw log data for that event.

日志类型	日志子类型	日志产生时间	源IP	源端口	目标IP	目标端口	产生日志设备IP	产生日志设备名称	详情
告警类	告警	2021-11-22 14:44:08	10.157.252.155	48800	43.227.140.113	8080	10.156.4.15	Xiangji_NTA	
告警类	告警	2021-11-22 14:43:40	10.157.252.155	48794	43.227.140.113	8080	10.156.4.15	Xiangji_NTA	
告警类	告警	2021-11-22 14:43:28	10.157.252.155	48794	43.227.140.113	8080	10.156.4.15	Xiangji_NTA	
告警类	告警	2021-11-22 14:43:20	10.157.252.155	48794	43.227.140.113	8080	10.156.4.15	Xiangji_NTA	
告警类	告警	2021-11-22 14:43:12	10.157.252.155	48794	43.227.140.113	8080	10.156.4.15	Xiangji_NTA	
告警类	告警	2021-11-22 14:43:04	10.157.252.155	48794	43.227.140.113	8080	10.156.4.15	Xiangji_NTA	
告警类	告警	2021-11-22 14:42:56	10.157.252.155	48794	43.227.140.113	8080	10.156.4.15	Xiangji_NTA	
告警类	告警	2021-11-22 14:42:48	10.157.252.155	48794	43.227.140.113	8080	10.156.4.15	Xiangji_NTA	
告警类	告警	2021-11-22 14:42:40	10.157.252.155	48794	43.227.140.113	8080	10.156.4.15	Xiangji_NTA	
告警类	告警	2021-11-22 14:42:32	10.157.252.155	48794	43.227.140.113	8080	10.156.4.15	Xiangji_NTA	

日志详情

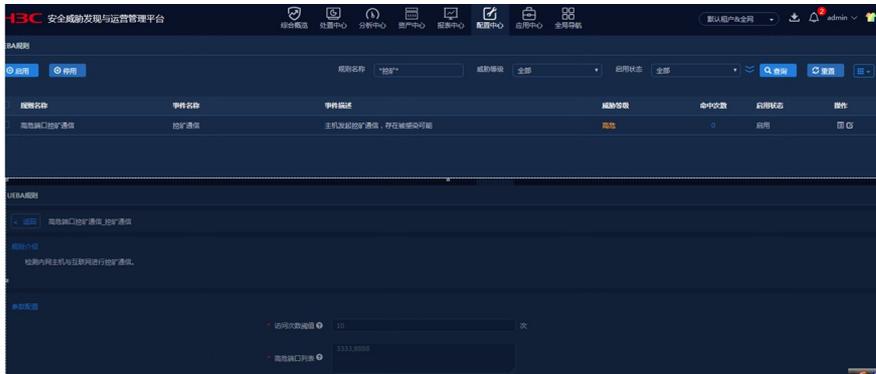
```
HTTP/1.1 200 OK (text/html)
Content-Type: text/html; charset=utf-8
Content-Length: 144
Server: Apache/2.4.18 (Ubuntu)
Date: Wed, 22 Nov 2021 14:44:08 GMT
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Expires: 0
Pragma: no-cache
```

过程分析

1、根据规则名称在平台上查看规则明细，会有基本的匹配规则，匹配了如下规则：

这个规则是根据访问3333、8888高危端口的次数达到阈值触发。

2、日志详情是服务器上的原始日志，可能是unix格式，所以以字符串形式展现，我们设备会分析提取出关键字段和日志类型，也就是日志处可以看到的源目ip、端口等信息。关注提取出的信息即可，原字符串涉及到不同格式解码。



解决方法

- 1、根据事件详情中检测引擎，该事件检测引擎为UEBA规则
- 2、在UEBA规则中找到该规则及其对应的触发机制。注意“规则名称”搜索时如果要模糊搜索需要加*

