态势感知集群版上安全事件少/安全事件中看不到网络取证报文

IPS防攻击 **薛佳宇** 2023-07-12 发表

组网及说明

安全威胁发现与运营管理平台增强版

问题描述

1、态势感知上产生的安全事件数量很少，但是威胁日志很多

2、已经产生的安全事件中看不到网络取证报文

过程分析

问题1：态势感知上产生的安全事件数量很少，但是威胁日志很多

1、检查态势感知上的的威胁日志存在乱码，这种现场通常与日志源配置的字符集有关，修改字符集为GBK后正常。当威胁日志内容正常显示后，安全事件数量也明显增加。

修改前：

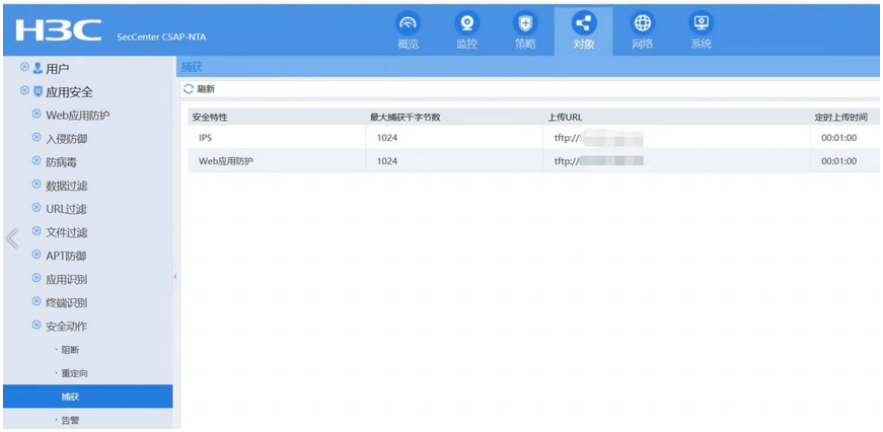
日志产生时间	攻击类型	攻击子类型	产生日志设备名称	产生日志设备IP	源IP	源端口	目的IP	目的端口	攻击名称	协议
2023-07-05 17:42:42	其他	其他				59872		53	◆◆◆◆◆◆◆_D...	UDP
2023-07-05 17:42:42	其他	其他				38311		161	CVE-2012-4964_...	UDP
2023-07-05 17:42:41	其他	其他				64501		53	◆◆◆◆◆◆◆_D...	UDP
2023-07-05 17:42:41	其他	其他				9683		161	SNMP 必◆◆◆...	UDP
2023-07-05 17:42:40	其他	其他				53967		53	◆▲◆◆◆◆Wan...	UDP

修改后：

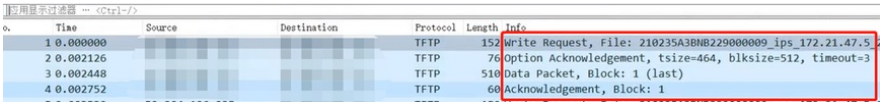
日志产生时间	攻击类型	攻击子类型	产生日志设备名称	产生日志设备IP	源IP	源端口	目的IP	目的端口	攻击名称	协议
2023-07-06 10:30:33	漏洞利用	SQL注入				40818		5432	可疑的对内连接到...	TCP
2023-07-06 10:30:06	漏洞利用	SQL注入				40256		5432	可疑的对内连接到...	TCP
2023-07-06 10:30:04	漏洞利用	SQL注入				40256		5432	可疑的对内连接到...	TCP
2023-07-06 10:29:47	威胁情报	恶意域名				57131		53	矿池域名_DNS查询	UDP
2023-07-06 10:29:47	威胁情报	恶意域名				58435		53	矿池域名_DNS查询	UDP

问题2：已经产生的安全事件中看不到网络取证报文

1、检查探针配置，IPS配置文件已开启了抓包，同时也配置了捕获报文tftp方式上传，并且探针跟tftp指定的地址之间可达。



2、在探针上抓包，可以看到与指定的服务器地址有tftp正常交互的报文



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000			TFTP	152	Write Request, File: 210235A3BNB229000009_ips_172.21.47.5
2	0.002126			TFTP	76	Option Acknowledgement, tsize=464, blksize=512, timeout=3
3	0.002448			TFTP	510	Data Packet, Block: 1 (last)
4	0.002752			TFTP	60	Acknowledgement, Block: 1

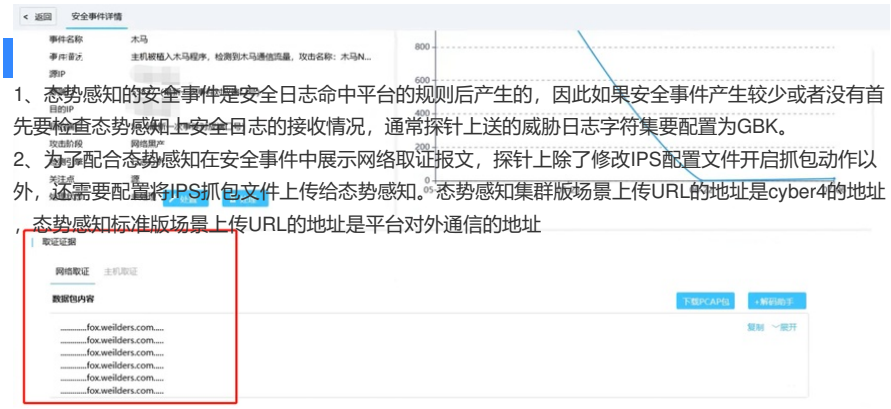
3、查看产品配置手册，有如下描述：

https://www.h3c.com/cn/d_202204/1580391_30005_0.htm

¡ 配置上传URL：

- 如果上报到CSAP平台集群版，URL配置为：tftp://Cyber4的对外通信地址。（Cyber4为集群版第四台设备）
- 如果上报到CSAP平台标准版，URL配置为：tftp://平台的对外通信地址。

4、再次检查探针上指定的TFTP服务器地址，发现用户配置的是态势感知日志采集器的地址，这个地址对应的是cyber5(登陆web的地址对应cyber3)，随后与用户沟通后确认到了正确的cyber4的地址，并修改了探针上上传URL的配置后，态势感知上可以正常看到网络取证报文。



1、态势感知的安全事件是安全日志命中平台的规则后产生的，因此如果安全事件产生较少或者没有首先要检查态势感知上安全日志的接收情况，通常探针上送的威胁日志字符集要配置为GBK。

2、为了配合态势感知在安全事件中展示网络取证报文，探针上除了修改IPS配置文件开启抓包动作以外，还需要配置将IPS抓包文件上传给态势感知。态势感知集群版场景上传URL的地址是cyber4的地址，态势感知标准版场景上传URL的地址是平台对外通信的地址