

青藤蜂巢操作注意事项

研判的思路还是联系客户确认进程是否是业务进程同时根据其他的告警进行分析。蜂巢进行应急响应的方法有两种，**一是处置，二是标记**

标记意味着不存在危害或是危害不算太大，例如网络连接受限的容器中发现webshell的危害性显然不算太高，标记可以表示危害已解除或是小到足以忽略，但是与白名单不同的是，下次遇到同类型的事件仍会告警

处置意味着需要对问题进行处理，一般是以容器为维度：

隔离容器：对容器进行双向封禁，不能访问外部（推荐）

杀容器：将容器销毁

暂停容器：将容器保持当前状态暂停，取消暂停后还可以拉起

1.反弹检测

根据行为特征进行告警，研判思路有四个：

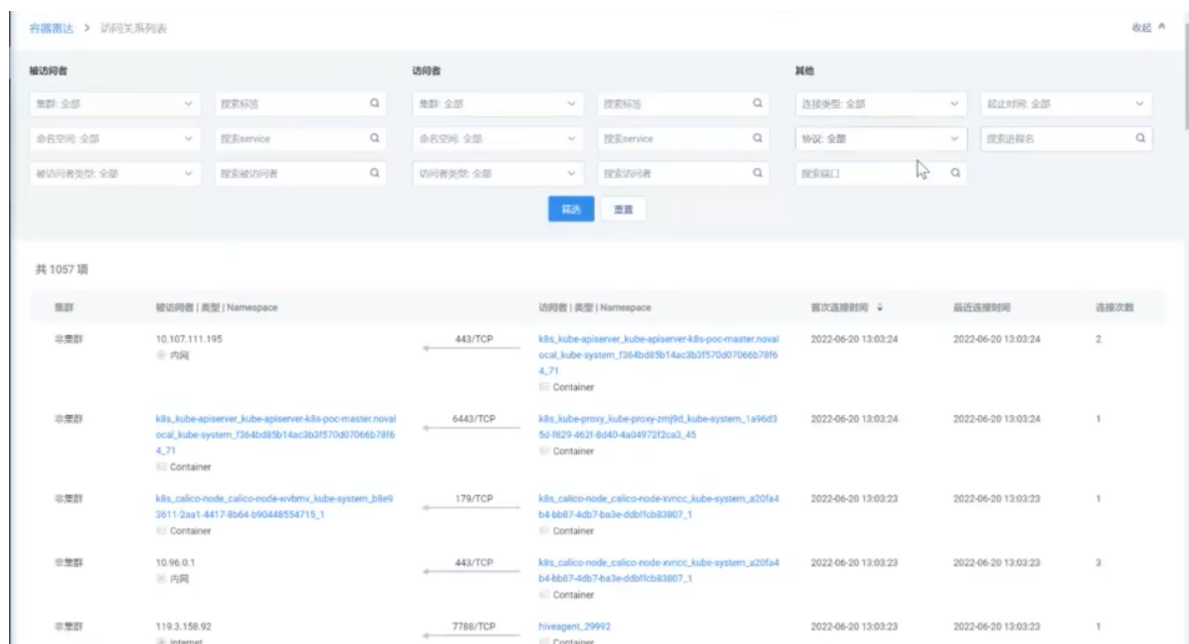
（1）反弹目标的ip

ip为主机的情况下

首先判断是**内网ip**还是**外网ip**。

如果是**外网ip**，我们可以去**微步**、**小红伞**等威胁情报社区，查询该ip是否是涉及黑产的恶意ip，同时随着hw的进行，红队的ip池也会进一步的暴露，我们可以将**反弹的ip与已知的红队ip进行比对**，判断是否可能是恶意ip。

如果是内网，则先判断目标ip。**如果安装agent**，那么可以使用主机上的青藤万相来清点资产内容，找到可疑的进程，判断是否是恶意进程，还是正常的业务进程。**如果没有安装agent**，那么可以通过全局网络事件（查日志）来判断是否为恶意进程，**特别是此ip频繁连接、探测其他的ip**。也可以通过蜂巢的**容器雷达**来查询容器之间的通信状况



容器雷达 > 访问关系列表

筛选: 全部 搜索: 搜索服务 其他: 连接类型: 全部 截止时间: 全部 命名空间: 全部 搜索: 搜索service 命名空间: 全部 搜索: 搜索service 协议: 全部 搜索: 搜索进程名 被访问者类型: 全部 搜索: 搜索被访问者 访问者类型: 全部 搜索: 搜索访问者 搜索端口

筛选 重置

共 1057 项

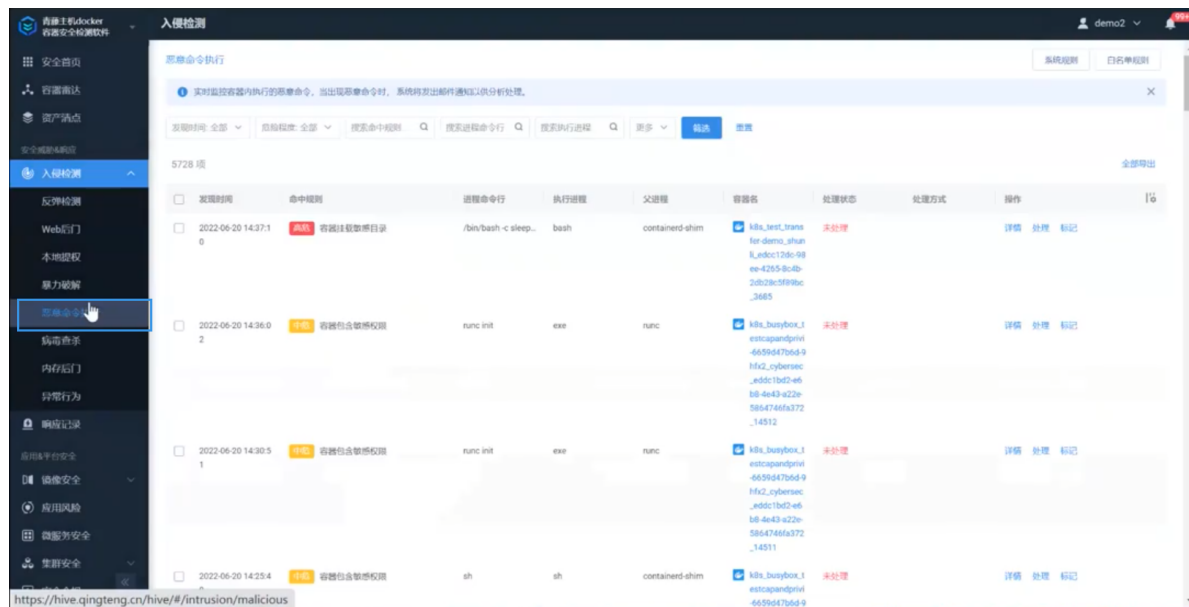
源	被访问者 类型 Namespace	访问者 类型 Namespace	首次连接时间	最近连接时间	连接次数
容器组	10.107.111.195 内网	443/TCP k8s_kube-apiserver_kube-apiserver-k8s-poc-master.novalocal_kube-system_f364bd95b14ac3b3f570d07066b78f64_71 Container	2022-06-20 13:03:24	2022-06-20 13:03:24	2
容器组	k8s_kube-apiserver_kube-apiserver-k8s-poc-master.novalocal_kube-system_f364bd95b14ac3b3f570d07066b78f64_71 Container	6443/TCP k8s_kube-proxy-kube-proxy-zm9d_kube-system_1a96d35d1829-462f-6d40-4a04972f2ca2_45 Container	2022-06-20 13:03:24	2022-06-20 13:03:24	1
容器组	k8s_calico-node_calico-node-ivtmv_kube-system_b8e93611-2aa1-4417-8b64-b90448554715_1 Container	179/TCP k8s_calico-node_calico-node-ivmcc_kube-system_a20fa4b4-bb67-4db7-ba3e-ddbfcb83807_1 Container	2022-06-20 13:03:23	2022-06-20 13:03:23	1
容器组	10.96.0.1 内网	443/TCP k8s_calico-node_calico-node-ivmcc_kube-system_a20fa4b4-bb67-4db7-ba3e-ddbfcb83807_1 Container	2022-06-20 13:03:23	2022-06-20 13:03:23	3
容器组	119.3.158.92 Internet	7788/TCP hiveagent_29992 Container	2022-06-20 13:03:23	2022-06-20 13:03:23	1

ip为容器的情况下

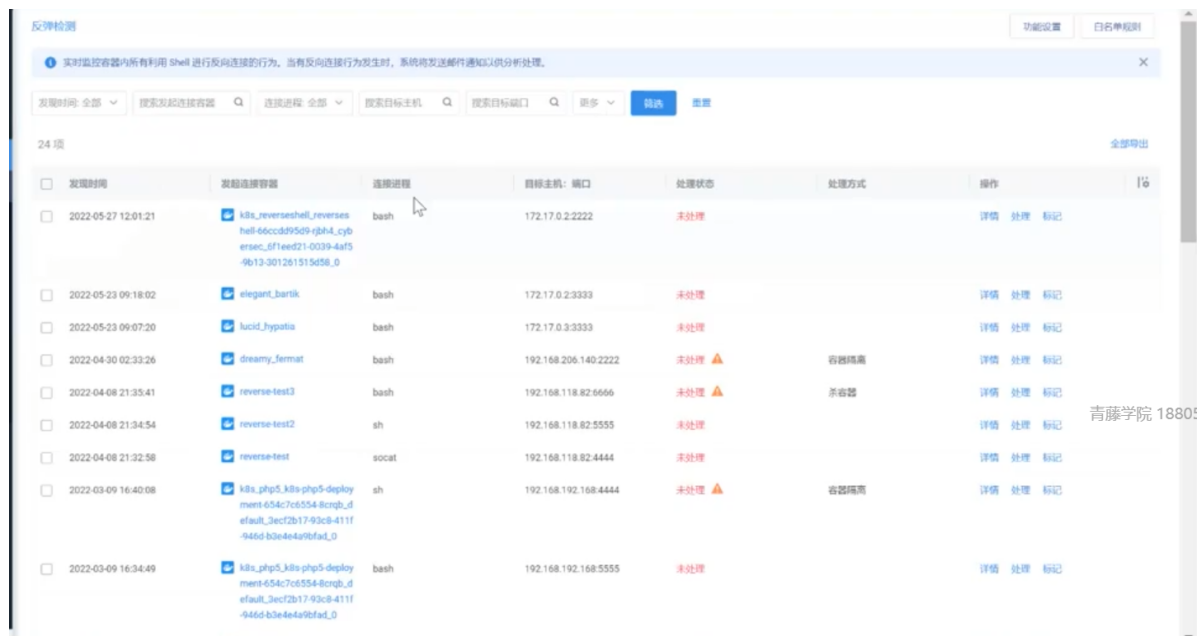
首先查看宿主机上**是否安装了青藤万相的agent**，若安装了则可以通过资产清点来查询该容器的端口监听是否进行正常业务。若未安装则与上文一样，通过全局网络事件来判断（**依靠日志，容器雷达等工具**）

(2) 反弹行为

我们可以查看反弹的同一时间段有没有触发其他的告警，例如产品中的恶意命令执行的告警：



因为反弹的行为是恶意渗透行为之后的步骤，当攻击队渗透进容器后，才会尝试反弹，以此当反弹告警伴随着其他命令执行的告警时，就很有可能是攻击队的行为。



(3) 反弹事件前后行为

正常的进程执行了反弹脚本的操作，我们在逻辑上是可以判断出来的。**在反弹前**，可能会**先下载反弹脚本**。**在反弹后**，可能会**获取主机的密码信息，查看list文件**，这样我们就可以根据这些行为进行辅助判断，通过**日志查询**判断

(4) 容器是否横向渗透

当攻击者拿下容器后，很可能会进行横向渗透，由此我们也可以判断是否被反弹，通过网络日志判断。例如，此容器存在反弹shell的告警，我们可以关联的查询它的一些其他网络连接的关联信息

反弹检测

实时监控容器内所有利用 shell 进行反向连接的行为。当有反向连接行为发生时，系统将发送邮件通知以供分析处理。

发现时间: 全部 | 搜索发起连接容器 | 连接进程: 全部 | 搜索目标主机 | 搜索目标端口 | 更多 | 筛选 | 重置

24 项 | 全部导出

<input type="checkbox"/>	发现时间	发起连接容器	连接进程	目标主机: 端口	处理状态	处理方式	操作	16
<input type="checkbox"/>	2022-05-27 12:01:21	k8s_reverseshell_revershell-66cc0d95d9-jbh4_cybersec_bf1eed21-0039-4af5-9b13-301261515d58_0	bash	172.17.0.2:2222	未处理		详情 处理 标记	
<input type="checkbox"/>	2022-05-23 09:18:02	elegant_barik	bash	172.17.0.2:3333	未处理		详情 处理 标记	
<input type="checkbox"/>	2022-05-23 09:07:20	lucid_hypatia	bash	172.17.0.3:3333	未处理		详情 处理 标记	
<input type="checkbox"/>	2022-04-30 02:33:26	dreamy_ferret	bash	192.168.206.140:2222	未处理	容器隔离	详情 处理 标记	
<input type="checkbox"/>	2022-04-08 21:35:41	reverse-test3	bash	192.168.118.82:6666	未处理	杀容器	详情 处理 标记	
<input type="checkbox"/>	2022-04-08 21:34:54	reverse-test2	sh	192.168.118.82:5555	未处理		详情 处理 标记	
<input type="checkbox"/>	2022-04-08 21:32:58	reverse-test	socat	192.168.118.82:4444	未处理		详情 处理 标记	
<input type="checkbox"/>	2022-03-09 16:40:08	k8s_php5_k8s_php5-deploy-ment-654c7c6554-8crgb_d-efault_3ecf2b17-93c8-411f-946d-b3e4e49bfad_0	sh	192.168.192.168:4444	未处理	容器隔离	详情 处理 标记	
<input type="checkbox"/>	2022-03-09 16:34:49	k8s_php5_k8s_php5-deploy-ment-654c7c6554-8crgb_d-efault_3ecf2b17-93c8-411f-946d-b3e4e49bfad_0	bash	192.168.192.168:5555	未处理		详情 处理 标记	

接下来通过容器雷达，查看该容器被反弹后的时间有无大规模的尝试连、探测其他容器

容器雷达 > 访问关系列表

收起

输入容器: 集群: 全部 | 搜索标签: | 命名空间: 全部 | 搜索service: | 被访问表类型: 全部 | 搜索被访问者: | 访问者类型: 全部 | 搜索访问者: | 筛选 | 重置

其他: 连接类型: 全部 | 起止时间: 全部 | 协议: 全部 | 搜索进程名: | 搜索端口: |

共 1057 项

集群	访问容器 类型 Namespace	访问者 类型 Namespace	首次连接时间	最近连接时间	连接次数
非集群	k8s_kube-apiserver_kube-apiserver-k8s-poc-master.novalocal_kube-system_f364bd95b14ac3b3f570d07066b78f64_71 Container	6443/TCP k8s_kube-proxy_kube-proxy-zm9jd_kube-system_1a96d35d-f829-462f-8640-4a04972f2ca3_45 Container	2022-06-20 13:03:24	2022-06-20 13:03:24	1
非集群	10.107.111.195 内网	443/TCP k8s_kube-apiserver_kube-apiserver-k8s-poc-master.novalocal_kube-system_f364bd95b14ac3b3f570d07066b78f64_71 Container	2022-06-20 13:03:24	2022-06-20 13:03:24	2
非集群	172.16.17.129 内网	179/TCP k8s_calico-node_calico-node-vmcc_kube-system_a20fa4b4-bb87-4db7-ba3e-dbfcb83807_1 Container	2022-06-20 13:03:23	2022-06-20 13:03:23	1
非集群	k8s_calico-node_calico-node-vmcc_kube-system_b8e93611-2aa1-4417-8b64-b90448554715_1 Container	179/TCP k8s_calico-node_calico-node-vmcc_kube-system_a20fa4b4-bb87-4db7-ba3e-dbfcb83807_1 Container	2022-06-20 13:03:23	2022-06-20 13:03:23	1
非集群	10.96.0.1 内网	443/TCP k8s_calico-node_calico-node-vmcc_kube-system_a20fa4b4-bb87-4db7-ba3e-dbfcb83807_1	2022-06-20 13:03:23	2022-06-20 13:03:23	3

2.对反弹事件的加白

在告警中可能会存在误报，因此我们需要对其中的一些正常的业务进程进行加白处理，加白的逻辑如下：

新建白名单规则

×

若同时符合下列条件，则将其加入白名单

条件列表:

☐ 连接进程: 请选择连接进程

☐ 进程树: 请填写进程树，各进程以英文逗号隔开，例如: init,watchdog.sh

☐ 目标主机: 请填写目标主机IP，可添加多个

目标端口:

请输入端口或端口段，多个以换行分隔，例如:
1223
1200-1204

描述:

请输入规则描述信息

连接进程

进程树

目标主机

目标端口

存在两种加白的逻辑：

(1) 我们已知一个外部的ip地址，其业务行为就是对不同容器发起反弹，获取shell，这里我们一般通过目标主机和目标端口来进行加白

(2) 反弹指向的ip不确定，但是反弹都是由某一特定进程的行为组成，这里我们一般用进程树描述其业务行为

3.web后门的研判

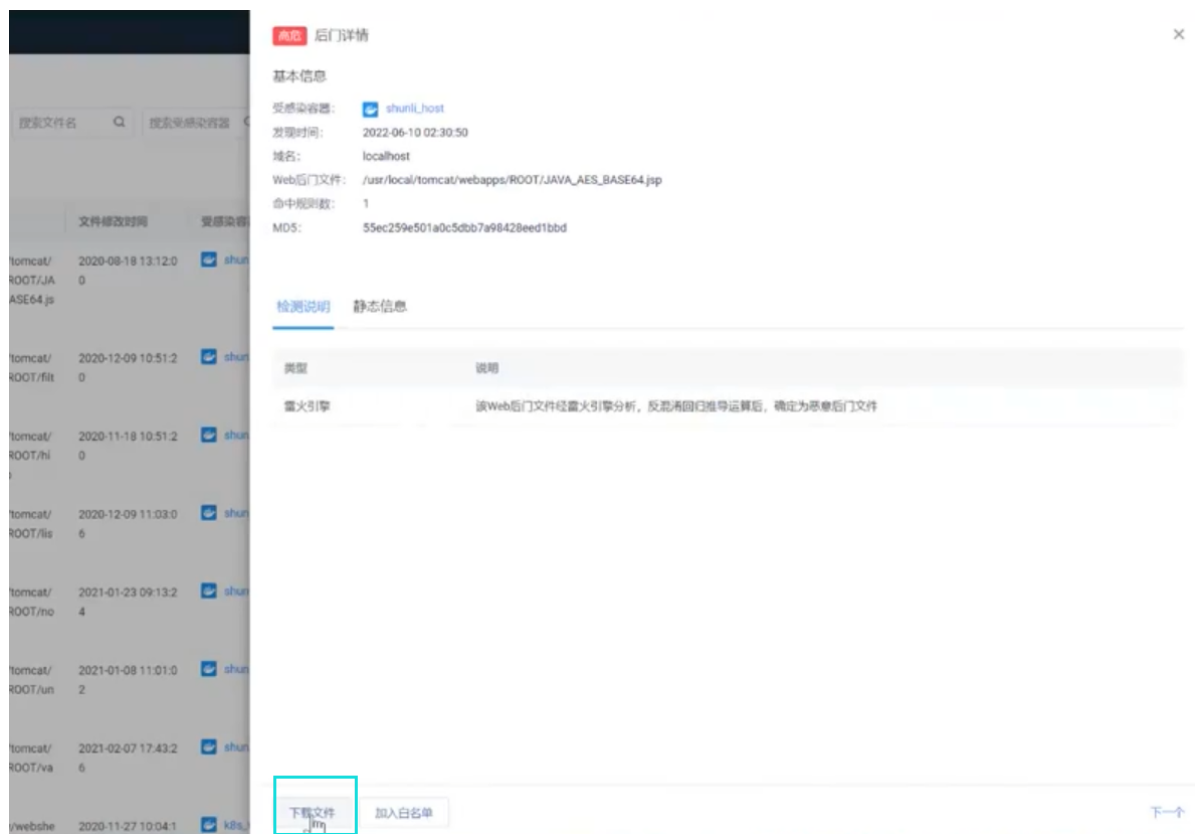
对于web后门的研判，一般有三种类型：

(1) 已知恶意样本

若上传的web后门与样本库中的恶意样本一致，那么几乎可以直接断定为恶意攻击。

(2) 雷火引擎

可以直接使用雷火引擎，对疑似恶意后门的文件进行分析。但雷火引擎也可能存在误报的场景，此时就需要我们进行恶意代码分析。在web后门详情里，选择下载文件：



对于文件的内容进行分析与审计，可以在网上寻找后门文件常见的形式、特征、变种

(3) 系统执行、已知后门

对于有些写死在代码里命令执行，比如sql之类的，就可能存在误报。还有根本就不可能上传web文件的地方出现文件上传的地方告警，多半是存在误报的情况。

(4) 白名单

对于web后门文件的白名单处理，一般有两种方法：

新建白名单规则

×

如果符合下列全部条件：

条件列表：

☒ 文件MD5：

请输入文件MD5，只能输入一个

☐ 自定义文件：

☐ 文件目录：

请输入目录规则，多个以英文逗号隔开

☐ 文件名：

请输入文件名正则表达式，英文逗号分割多个正则，如：.*filename.*

则将Web后门加入白名单。

描述：

请输入规则描述信息

青藤学院 18805143201 王曹宇轩

一个是文件的MD5，另一个是文件的目录与名称，尽量使用MD5，因为在hw前期就已经处理了大部分业务上的误报文件，hw过程中遇到误报，使用MD5能够更小范围的选择加白的文件。

4.本地提权

说白了就是某个容器的进程所属的用户组、suid、运行运行用户和权限发生变化，就可能是本地提权，如图，就是运行用户发生变化导致的提权，

- (1) 向客户确认此进程发生的变更与操作是否是业务需要的
- (2) 查看权限提升后的进程的操作，一般来说一个攻击队成员在提权成功后的第一件事都是确认当前的权限，因此他很有可能进行whoami命令或访问系统文件（例如尝试访问etc/passwd），这些问题反应在监控日志上，我们根据进程的pid去查看后续的行为。

6. 恶意命令执行

分为两类问题：

第一类是容器存在逃逸风险（以特权模式启动、容器启动时附加权限、容器启动时挂载了容器的根目录、root目录）

第二类是shellcode里包含一个RCE的操作

研判时与客户沟通，查看容器中的进程是否是正常的业务进程，同时需要查看容器关联的资产，追溯到控制器的角度，和客户再确认

而研判RCE更多时候要依靠经验，例如通过进程树，发现容器执行了一个nc反弹的命令，那基本可以断定是恶意命令执行

加白也是按照判断容器逃逸风险和判断存在RCE来执行的。

(1) 当容器拥有敏感权限时，我们最好通过镜像名来进行加白的操作



新建白名单规则

若同时符合下列不为空的条件，则将其加入白名单

白名单类型：☐ 恶意进程 ☒ 逃逸风险

风险类型：☐ 特权容器 ☒ 敏感权限 ☐ 敏感目录

条件列表：

容器名： 请输入需要加白的容器名，以模糊方式进行匹配；支持输入多个，用英文“,”隔开

镜像名： 请输入镜像名，以精确方式进行匹配；支持输入多个，用英文“,”隔开

描述： 用户'demo2'于2022-06-20添加该白名单

取消 创建

(2) 当容器挂载在敏感目录时，我们加白时还需要加上敏感目录的名称

新建白名单规则

×

若同时符合下列不为空的条件，则将其加入白名单

白名单类型：

☐ 恶意进程

☒ 逃逸风险

风险类型：

☐ 特权容器

☐ 敏感权限

☒ 敏感目录

条件列表：

敏感目录：

请输入需要加白的目录，以模糊方式进行匹配；支持输入多个，用英文“；”隔开

容器名：

请输入需要加白的容器名，以模糊方式进行匹配；支持输入多个，用英文“；”隔开

镜像名：

请输入镜像名，以精确方式进行匹配；支持输入多个，用英文“；”隔开

描述：

用户"demo2"于2022-06-20添加该白名单

S 英 , 😊 🗣️ 📄 🔄 🗑️ 🏠

取消

创建

(3) 当处理RCE的时候我，可以通过**父进程**（**推荐，反映了真实的业务执行链路**），如果不方便，还可以选择**执行进程与进程命令行**来实现加白

新建白名单规则

×

若同时符合下列条件，则将其加入白名单

白名单类型：☒ 恶意进程 ☐ 逃逸风险

条件列表：

父进程：

请输入父进程名，以严格匹配方式进行匹配；支持输入多个，用英文逗号“,”隔开

执行进程：

请输入执行进程名，以严格匹配方式进行匹配；支持输入多个，用英文逗号“,”隔开

进程命令行：

请输入进程命令行，以正则表达式进行匹配（选填）

描述：

用户"demo2"于2022-06-20添加该白名单

7.病毒查杀

容器内自带的病毒查杀功能，容器里的文件会经过四种病毒引擎的扫描：

/usr/bin/kuboard-agent-server

🚫 经检测该文件为恶意文件

受感染容器: k8s_kuboard_kuboard-v3-59ccddb94c-fgsbc_kuboard_270742fb-a687-43f4-b275-79d605403f94_1

主机IP: 172.16.17.54

文件名: /usr/bin/kuboard-agent-server

文件MD5: 741c9f02e1621534eac08e8a726aec85

文件SHA256: -

检测结果 1/4

检测库	检测结果	说明	修复方法	检测库更新时间
小红伞病毒引擎	✔️ 非恶意		删除文件	2020-03-19 17:11:00
ClamAV病毒引擎	✔️ 非恶意		删除文件	2021-10-21 19:42:27
自研病毒引擎	❗️ 恶意	Hacktool.Linux.Netagen tftp.a	网络代理穿透工具frp 未知来源程序建议删除	2022-05-06 11:00:30
T-Sec-反病毒引擎	✔️ 非恶意		删除文件	2020-08-31 18:14:01

关联进程 其他信息

进程名: kuboard-agent-s

进程路径: /usr/bin/kuboard-agent-server

父进程: entrypoint.sh

父进程路径: /bin/dash

启动时间: 2022-06-20 04:00:12

进程启动用户: root

用户所属组: root

容器PID: 27

主机PID: 21398

[下载文件](#) [加入白名单](#)

其中包含了四种引擎的告警信息和处理的方法，**小红伞和青藤自研引擎的准确率较高**，一般可以直接判断为病毒。其他两者误报率可能会高一点，可以将文件下载下来，**上传到情报威胁社区进行二次确认**。同时可以根据蜂巢中显示的病毒的信息，查看病毒的一些特征，与用户确认是否是正常业务。

关于**病毒文件加白**，一般是**根据文件的md5或是sha256进行加白**，推荐使用**sha256**避免出现**哈希碰撞**

新建白名单规则

如果符合下列任一条件则将病毒文件加入白名单

条件列表:

☐ 文件MD5: 请输入文件MD5, 只能输一个

☐ 文件SHA256: 请输入文件SHA256, 只能输一个

描述: 用户"demo2"于2022-06-20添加该白名单

8.内存后门

内存后门的检测库有三种：恶意类规则、内存webshell库、雷火引擎。

(1) 恶意类规则

可以将webshell文件下载下来查看代码，如果其中的关键字与规则中的关键字信息类似，就可以确定是内存后门。如果不能确定的话，还可以将运行报告发送给研判组。

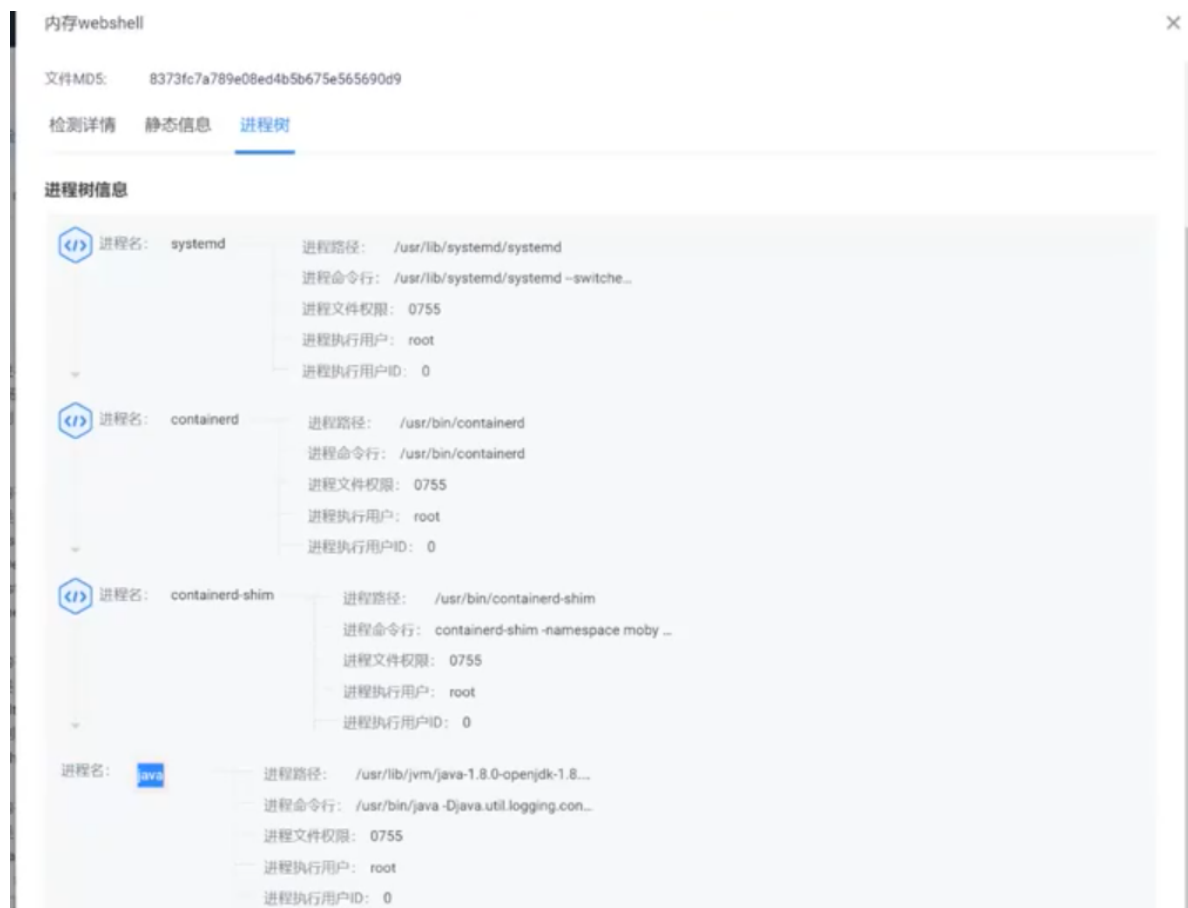
(2) 内存webshell库

通过代码审计，判断是否存在内存后门的可能性

(3) 雷火引擎

基于代码反编译和词法语法的分析

对于内存webshell，我们可以根据显示的进程树，通过进程对于端口的监听，进一步查看站点信息：



内存webshell

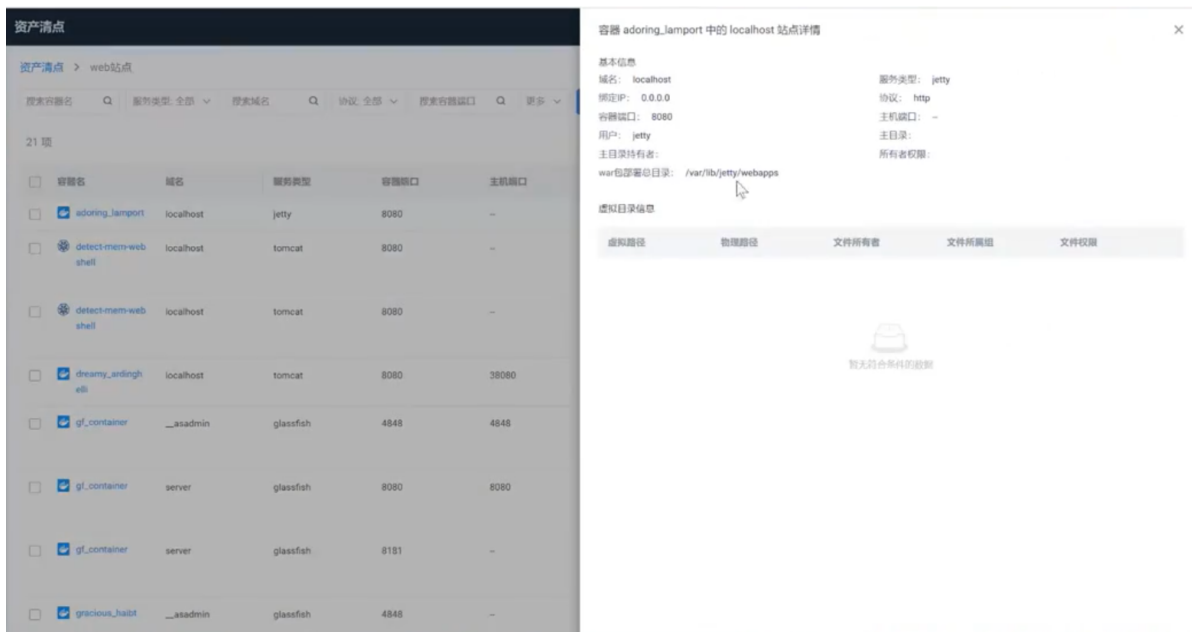
文件MD5: 8373fc7a789e08ed4b5b675e565690d9

检测详情 静态信息 进程树

进程树信息

进程名	进程路径	进程命令行	进程文件权限	进程执行用户	进程执行用户ID
systemd	/usr/lib/systemd/systemd	/usr/lib/systemd/systemd --switche...	0755	root	0
containerd	/usr/bin/containerd	/usr/bin/containerd	0755	root	0
containerd-shim	/usr/bin/containerd-shim	containerd-shim -namespace moby ...	0755	root	0
java	/usr/lib/jvm/java-1.8.0-openjdk-1.8...	/usr/bin/java -Djava.util.logging.con...	0755	root	0

根据站点信息定位到对应的web服务



9.基于容器行为的建模告警

由于容器的行为模式较为固定，因此我们可以对容器的行为进行建模，若容器在运行中出现与模型不符的内容，则会告警