明御®主机安全及管理系统

用户操作手册

杭州安恒信息技术股份有限公司

二〇二二年五月

目 录

1 产品简介

明御主机安全及管理系统是一款集成了丰富的系统防护与加固、网络防护与加固等功能的主机安全产品。明御主机安全及管理系统通过自主研发的文件诱饵引擎，有着业界领先的勒索专防专杀能力；通过内核级东西向流量隔离技术，实现网络隔离与防护；拥有补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力。目前产品广泛应用在服务器、桌面 PC、虚拟机、工控系统、国产操作系统、容器安全等各个场景。

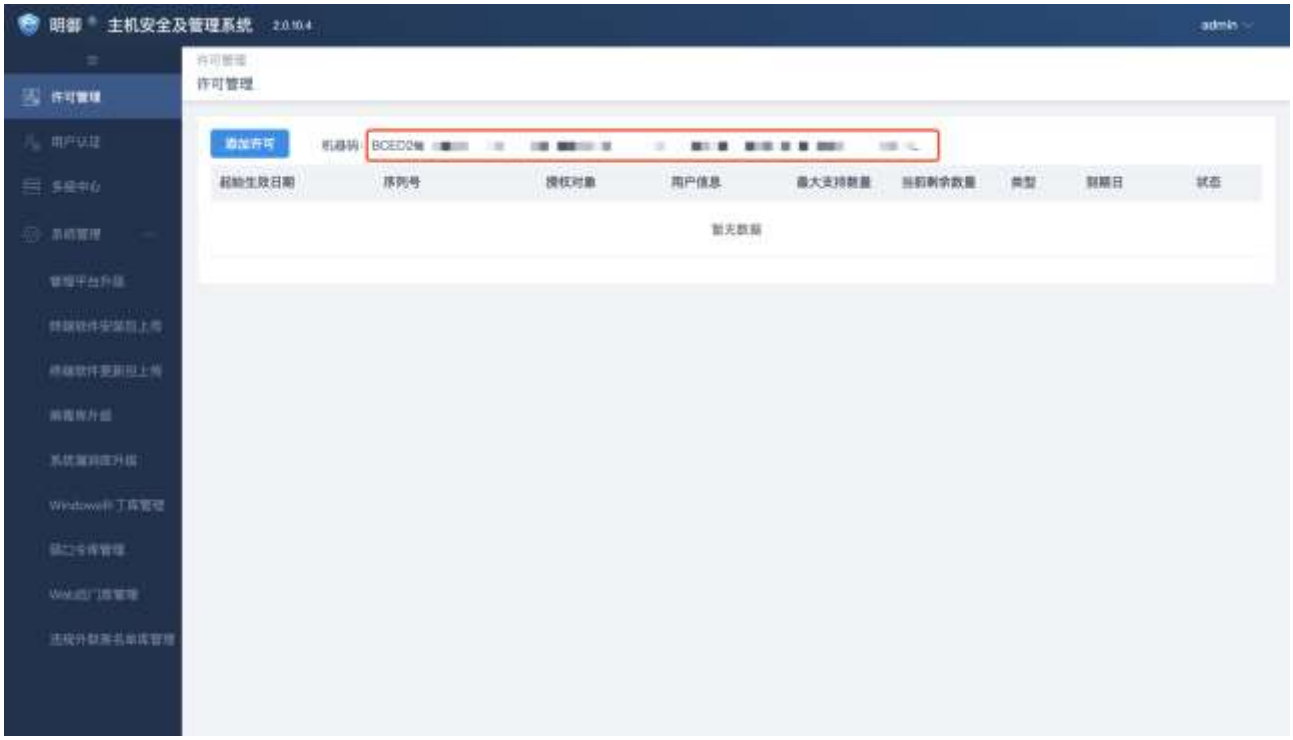
说明：以下**中心**指部署了 EDR 管理中心的 Linux 主机（物理机或虚拟机），**平台**指 EDR 管理中心的 Web 页面，**端**指部署了 EDR 客户端的主机。

2 登录及添加许可

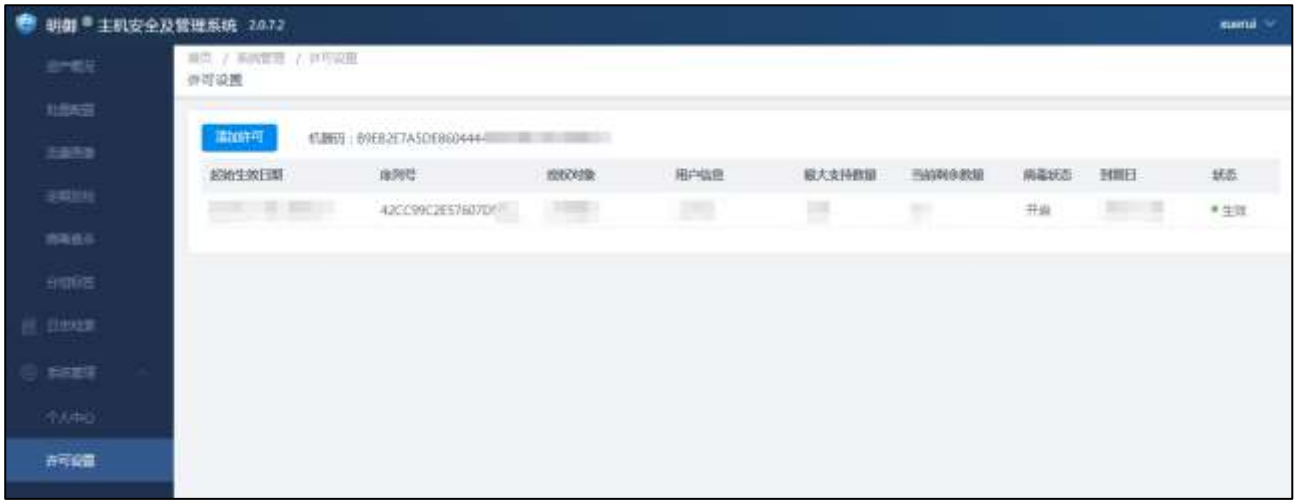
通过在浏览器中输入 https://中心 IP，登录平台，管理客户端主机。

1、 使用 admin 账号登录

2、admin 登录后点击左侧“许可管理”，通过机器码申请许可授权（许可申请：https://61.164.47.206:65526/downloads/EDRxksq.xlsx）



3、得到许可授权后点击“添加许可”输入获得的许可即可开始使用。



2.1 用户认证

如何添加租户？

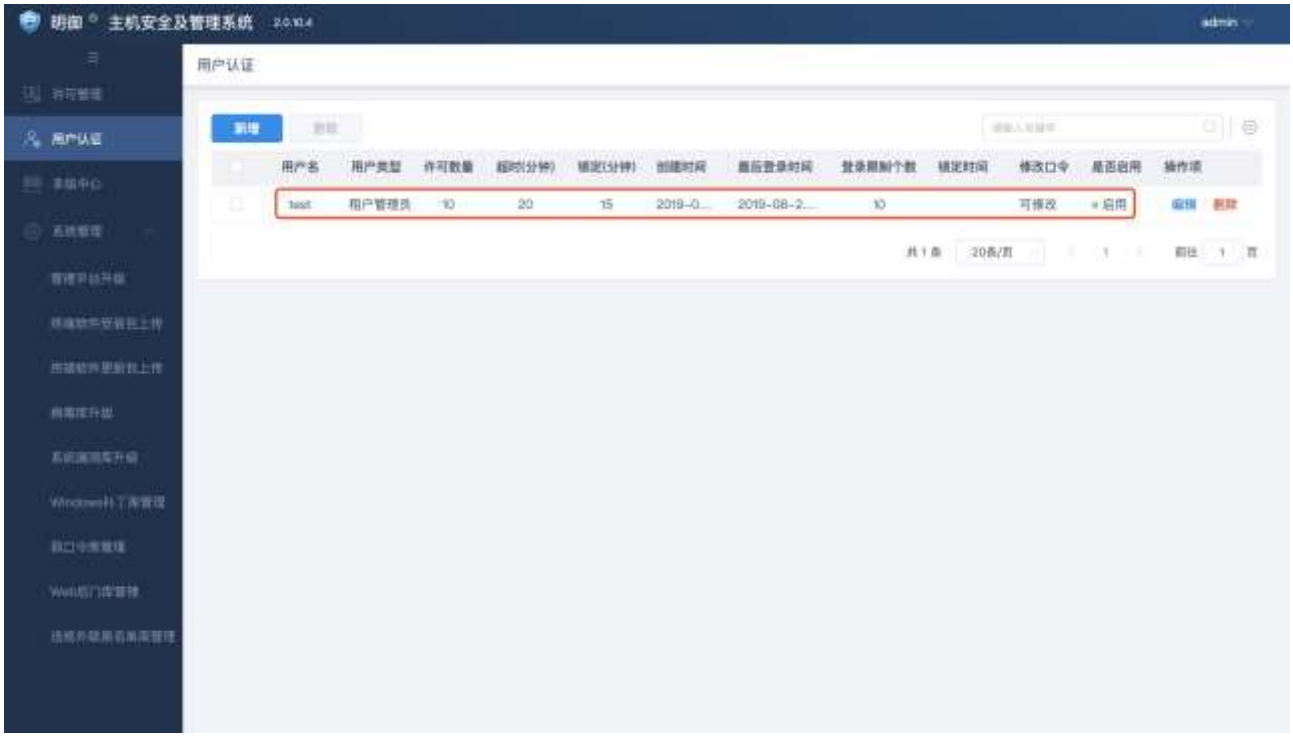
步骤1. 使用 admin 账号登陆管理平台；

步骤2. 进入用户认证，初次进入，需要修改密码；

步骤3. 点击新增；

步骤4. 输入用户名、密码、确认密码以及许可数量(根据实际情况输入许可数量)；

步骤5. 确定后即可新增租户；



步骤6. 后续再使用租户用户名登录管理平台。

3 首页

3.1 信息展示

在首页可查看如下内容：

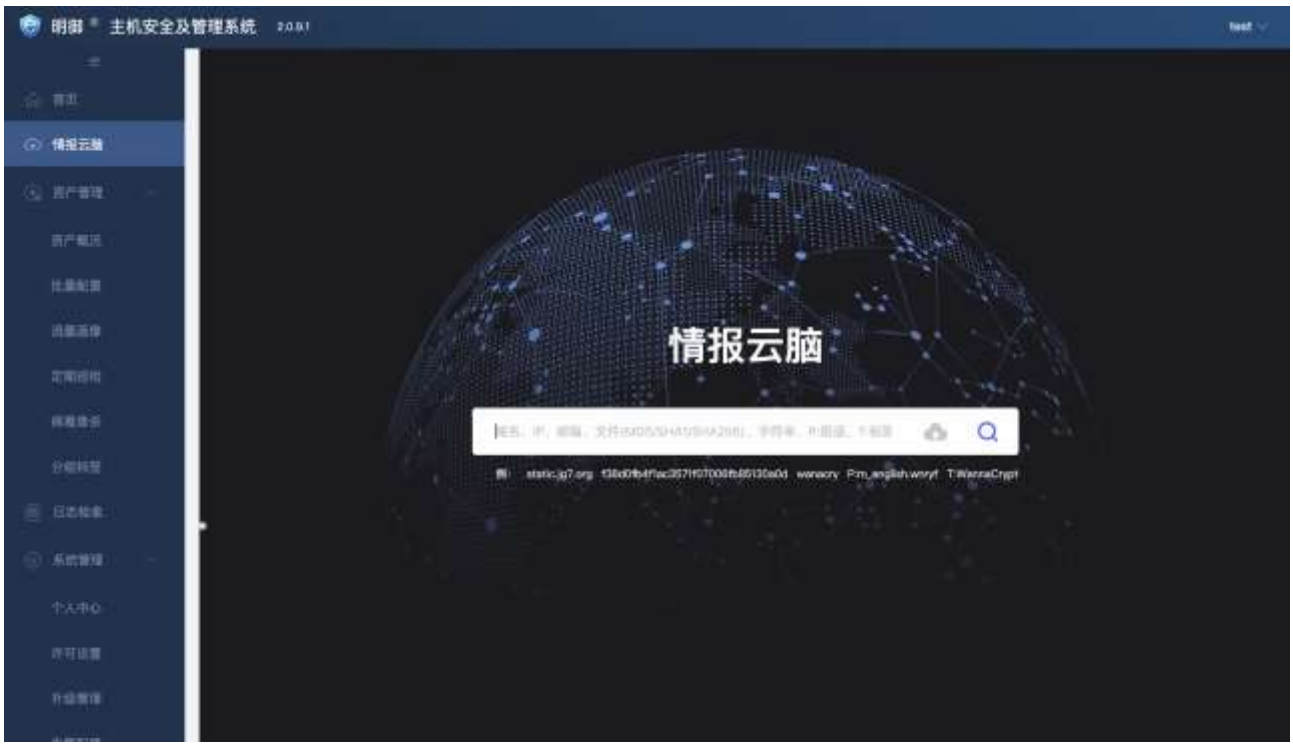
- 待处理漏洞数量、恶意程序数量、异常登录、Web 防护请求数量；
- 资产状态包括在线和离线的资产数量统计；
- 风险资产 TOP5 排行；
- 按系统安全和网络安全来查看攻击类型所占比；
- 管理平台性能监控包括 CPU、内存、系统盘；
- 攻击来源区域 TOP5、攻击来源 IP TOP5；
- 管理平台安全动态。

3.2 用户信息

点击右上角“账户名”，在关于中可以查看系统版本、授权等信息；点击“修改密码”可以进行修改密码操作。

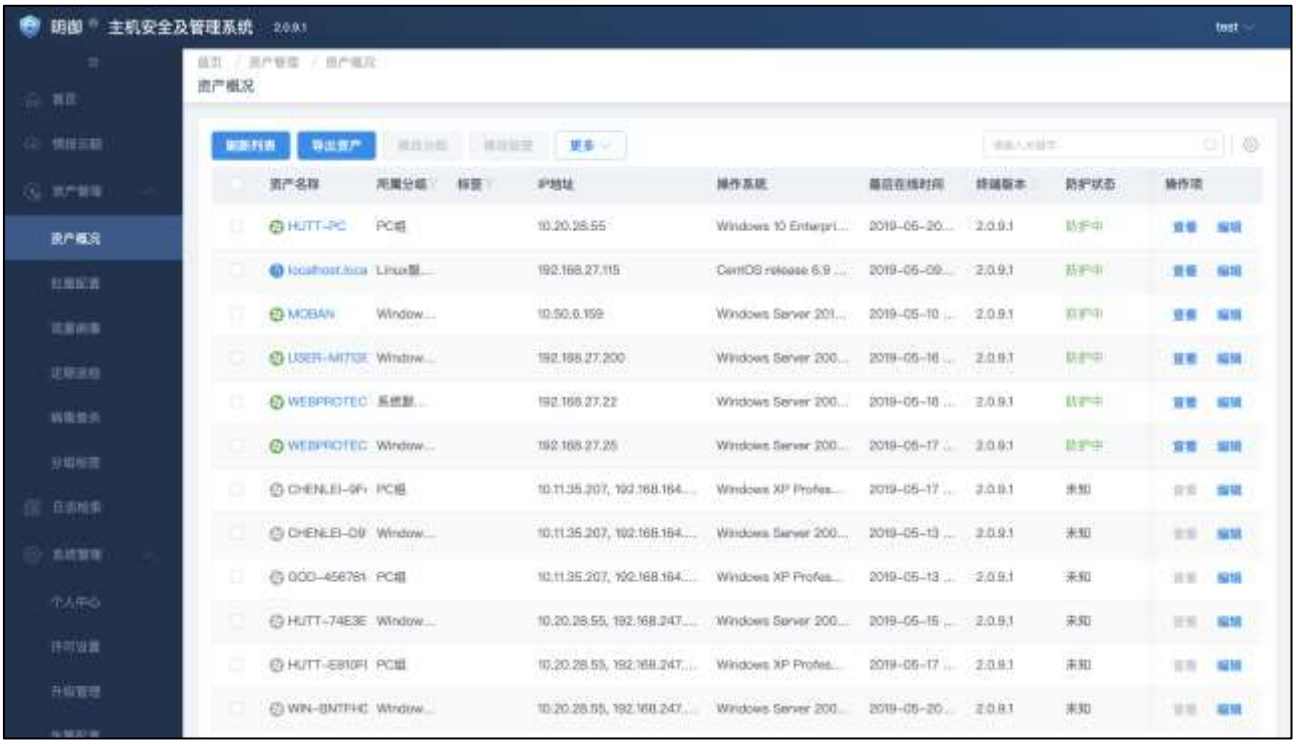
4 情报云脑

点击输入 IP、域名、文件（MD5/SHA1/SHA256）、邮箱等信息，进行查询；
也可点击上传文件进行文件的自动化动静态分析



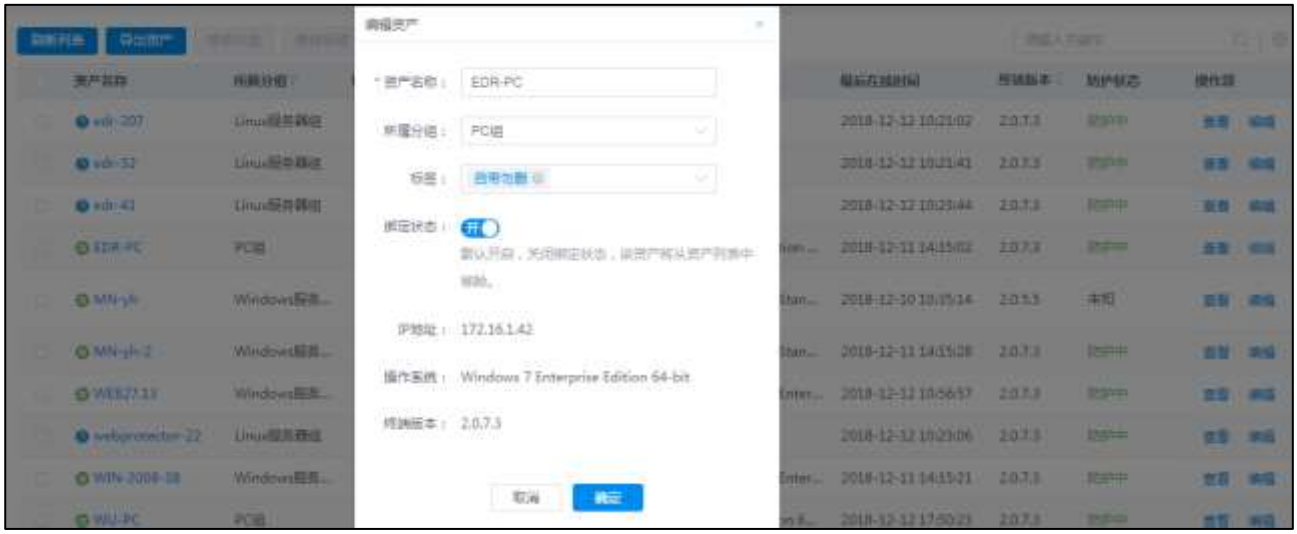
5 资产概况

在资产概况中可以查看所有绑定该中心的主机信息 。包括名称、分组、标签、IP、操作系统、终端版本等。



- 点击“导出资产”可将所选资产的概况信息导出。
- 点击“修改分组/标签”可修改所选资产的分组/标签（**每个资产必须且只能在一个分组内，可以有多个“标签”**）
- 点击“更多-设置卸载密码/卸载监控端/解除绑定”可对端执行相应操作。
- 点击“更多-停止防护”可关闭所选资产当前所有防护，点击“更多-启动防护”可恢复所选资产关闭防护前的状态。

- 点击操作项下的“编辑”可编辑资产相关信息，其中绑定状态调整为关，将解绑定该资产，被解绑的资产会从资产列表中“删除”



在“查看”或者点击“资产名称”中可看到资产指纹、系统防护、网络防护、Web 应用防护、工具箱五大功能。

6 资产指纹

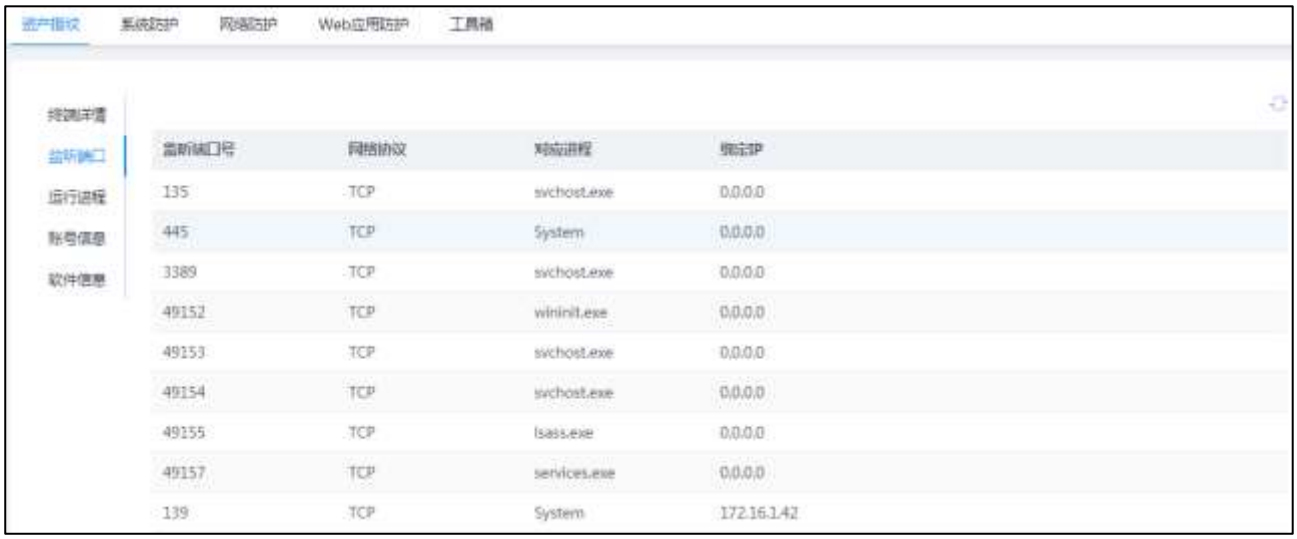
点击“资产概况”对应资产行的“查看”，可看到该资产的功能模块。

6.1 终端详情

在“资产指纹-终端详情”中可以查看到终端的网络信息、环境信息、以及其他信息等；也可以对资产进行远程重启主机。

6.2 监听端口

在“监听端口”中可以查看到系统占用的端口号、网络协议、对应进程和绑定的 IP 信息。



6.3 运行进程

在“运行进程”中可以查看到系统上运行的进程、进程路径、内存占用、CPU 使用率、启动参数、启动时间、运行用户及父进程等信息；也支持远程结束相关进程（系统相关进程无法结束）。

6.4 账号信息

在“账号信息”中可以查看到当前系统的账号包括隐藏账号的相关信息。

6.5 软件信息

可以查看该终端上运行的软件、以及软件厂商、版本号以及软件的安装目录。

7 系统防护

点击“资产概况”对应资产行的“查看”，可看到该资产的功能模块。

7.1 主动防御

7.1.1 主动防御

在主动防御功能中，监控系入侵关键点，及时的阻断恶意程序的入侵行为，抵御部分未知风险。

7.1.2 文件实时监控

实时监控文件的状态，在文件执行或者进入主机时进行扫描。

扫描时机：文件执行时进行扫描（默认）。

排除设置：如果不希望扫描指定程序，可以在此设置忽略，模糊匹配。

7.1.3 系统防御

保护指定项目不被篡改或执行；因特殊情况需要关闭 EDR 自身保护的，可以选择在此关闭“启用自身防护”。

7.1.4 执行防御

勾选指定防护项目，防止指定命令被恶意利用。

7.1.5 病毒免疫

可针对顽固流行病毒进行智能拦截。

7.2 病毒查杀

可对终端进行病毒木马扫描，扫描后将结果隔离、删除或加入信任区不再查杀。支持快速扫描、全盘扫描和指定目录扫描三种扫描模式，指定目录扫描需在“扫描路径”处添加需要扫描的路径。扫描结果可通过点击“查看扫描结果”来查看。

对于扫描结果，可单选、多选、全选进行隔离处理。病毒文件处于被占用的状态无法通过普通的隔离处理可使用“强力隔离”处理。

在隔离区，可“恢复”或“删除”已隔离的文件；在信任区，可将进程“添加”进来，信任区的进程启动不会被阻断。

7.3 漏洞管理

在漏洞管理中可对客户端主机进行扫描，默认进入管理界面时会触发一次扫描。标志绿色盾牌的漏洞补丁描述行表示管理中心已下载该补丁，可直接修复。白色盾牌表示管理中心尚未下载该补丁。

根据中心和端主机是否可访问互联网的不同情况，漏洞补丁的获取有以下几种情况：

7.3.1 只有中心可访问互联网

通过 admin 账户登录，中心下载补丁后推送给端主机修复。

步骤1. 使用 admin 账号登录，依次点击“Windows 补丁库管理”，“在线更新补丁”，“收集补丁”。

步骤2. 选择相应资产进行补丁收集（即检测需要下载的补丁）。

步骤3. 收集完成后点击“下载补丁”即可将已收集但未下载的补丁下载。下载完成后租户登录再对相应的主机进行漏洞修复。

7.3.2 只有端可访问互联网

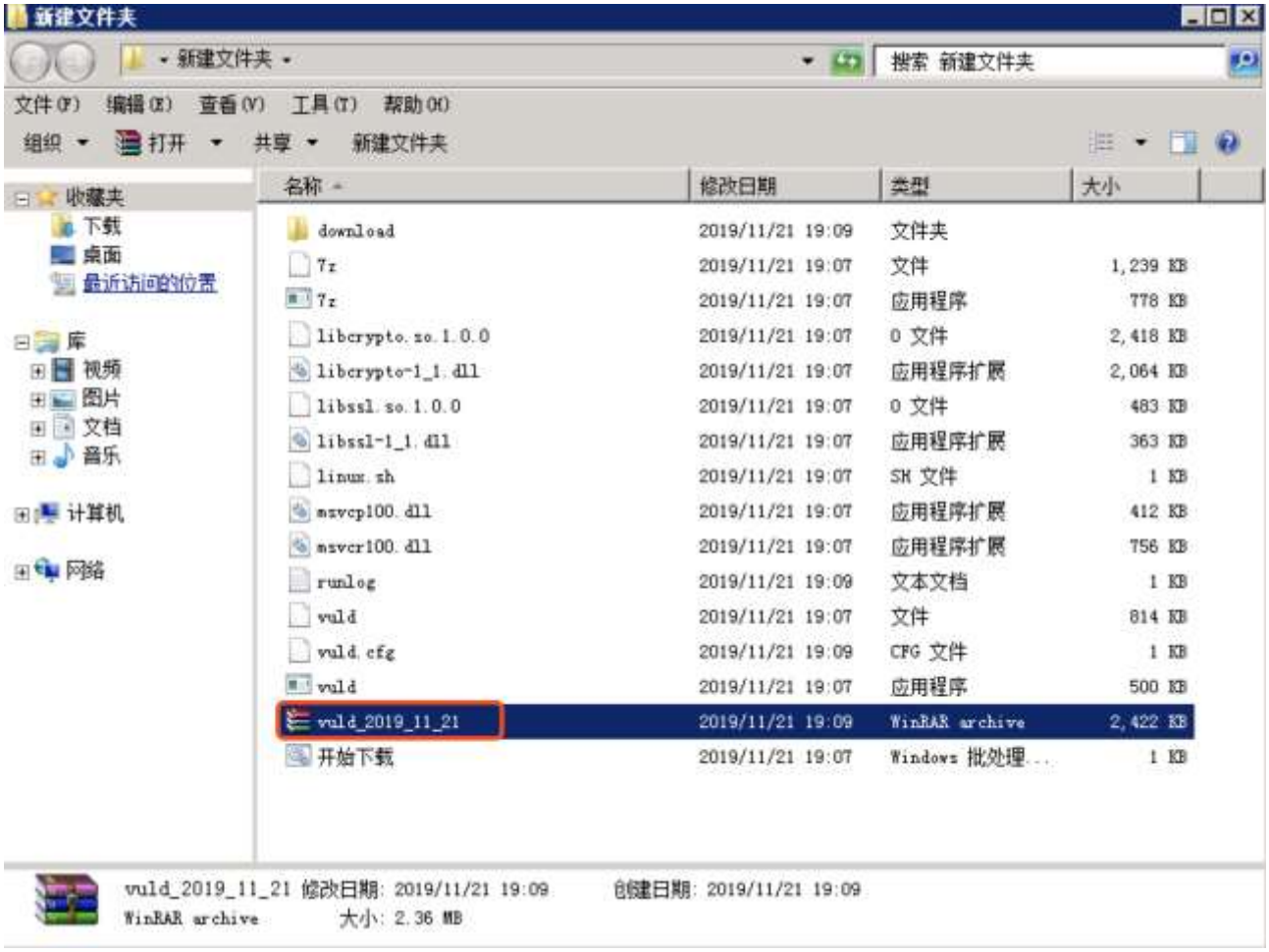
中心已下载过的补丁仍由中心推送给端主机修复，中心未下载过的由端主机下载进行修复。检测出漏洞后直接点击修复即可。

7.3.3 中心和端都不可访问互联网

通过 admin 账户登录，离线上传补丁后，中心推送给端主机修复。

步骤1. 使用 admin 账号登录，依次点击“Windows 补丁库管理”，“离线更新补丁”，“收集补丁”，并选择相应资产，收集完成后点击“下载”得到离线下载器 EDR_lxxzq.zip。

步骤2. 在可以访问互联网的主机上解压离线下载器 EDR_lxxzq.zip，在解压文件的路径下执行开始下载.bat 开始下载离线补丁。下载完成后得到一个 vuld_xxxx_xx_xx.zip 压缩包。



步骤3. 将下载得到的一个 zip 压缩包在步骤 1 中的上传文件处上传。

步骤4. 通过租户账户登录，到对应资产的漏洞管理功能下，可进行漏洞修复。

7.3.4 中心和端都可访问互联网

中心已下载过的补丁由中心推送给端主机修复，中心未下载过的由端主机下载进行修复

注意

补丁修复存在一定风险，需测试后再进行修复，以免对正常业务造成影响

7.4 系统登录防护

在系统登录防护功能中，可配置策略对远程登录做限制。

可配置防暴力破解策略（针对 Windows 操作系统的 RDP 协议、Linux 操作系统的 SSH 协议）。

默认的联动效果：当有远程 IP 触发策略，微隔离模块会自动添加一条规则阻断远程 IP 对本机 3389 端口或 22 端口的访问，时间为 60 分钟。

可配置弱口令检测策略，在系统账号大于 30 个的情况（例如域控服务器），默认不进行检测。

7.5 进程防护

7.5.1 进程黑名单

启用进程黑名单后，若设置仅记录，所有在黑名单内的程序运行都将被记录；若设置阻断并记录，所有在黑名单内的程序运行将被阻止并记录。

7.5.2 进程白名单

启用进程白名单后，若设置仅记录，所有不在白名单内的程序运行都将被记录；若设置阻断并记录，所有不在白名单内的程序运行将被阻止并记录。

选择“自动评估”，再选择一个路径开始扫描，扫描结果将自动添加到进程白名单。

7.6 文件访问控制

监控目标文件或目录的改写操作。

8 网络防护

8.1 微隔离

对不同业务之间进行流量隔离并精确阻断非法流量。可针对单条或者选择多条规则进行停用/开启，选择停用后的规则不生效。

通过“快捷操作-关闭本地端口”、“快捷操作-屏蔽恶意 IP”输入需要关闭的端口或需要屏蔽的地址，可一键生成对应的规则。

新增规则中，各参数意义如下：

- 规则类型：选择入站规则，则规则仅针对入站连接，即访问本机的请求；选择出站规则，则规则仅针对出站连接，即本机向外发送的请求；选择双向规则，则包括以上两种连接。
- 本地 IP：通常是*，多网卡配置不同规则的情况填入具体地址。
- 本地端口：要限制本机访问其他主机填*，限制其他主机访问本机则填入被访问的相应端口或*（代表全部端口）。
- 远程 IP：远程主机的 IP 地址或地址段。
- 远程端口：要限制本机去访问远程主机的端口则填入相应端口或*（代表全部端口），限制远程主机对本机发起访问则填*。
- 协议类型：通常默认所有。
- 处理方式：放行或阻止，放行的优先级高于阻止，可用于屏蔽整段 IP 的访问再开放个别 IP 允许访问。
- 有效时间：超过有效时间该条规则会失效。

应用举例：

需求：为当前主机配置禁止 192.168.1 网段除 192.168.1.10-192.168.1.20 以外的主机访问本机 445 端口。

配置内容：

规则一		规则二	
规则类型	双向规则	规则类型	双向规则
本地 IP	*	本地 IP	*
本地端口	445	本地端口	445
远程 IP	192.168.1.0-192.168.1.255	远程 IP	192.168.1.10-192.168.1.20
远程端口	*	远程端口	*
协议类型	所有	协议类型	所有
处理方式	阻止	处理方式	放行

8.2 防端口扫描

实时检查入站连接并阻断对本机端口的恶意探测，防止敏感信息泄露。可设置单个 IP 请求时间范围、最大扫描端口数量、IP 锁定时间，可查看已临时锁定 IP，并解除锁定。

8.3 违规外联防护

违规外联分为黑白名单两种模式，只能选择一种模式应用，可随时切换另一种模式。

8.3.1 白名单模式

配置白名单后，仅允许连接白名单中的 IP 地址，连接其他 IP 地址将被禁止。开启白名单模式但未添加任何白名单 IP 时，白名单不生效。

新增白名单：输入需要加入白名单的 IP 地址或 IP 地址段。

批量导入：可下载格式为.csv 的模板，填好模板后上传。

断开/允许互联网：选择“断开互联网”后，将一键添加规定的三类私有地址 10.0.0.0-10.255.255.255、172.16.0.0-172.31.255.255、192.168.0.0--192.168.255.255。选择“连接互联网”后，将删除已添加的三类私有地址。

8.3.2 黑名单模式

配置黑名单后，连接黑名单外的 IP 地址不受影响。自带不少于 10 万条威胁情报。

9 网站防护

9.1 网站漏洞防护

网站漏洞防护，可对网站常见的 SQL 注入攻击、XSS 跨站、Web 容器及应用漏洞进行实时防护。每条规则都有单独的开关，开启网站漏洞防护后，除“自动屏蔽扫描器”外，其他规则默认全部开启。

9.2 CC攻击防护

智能检测并防御 CC 攻击，保证网站正常服务能力。可调节高、中、低三个防护等级，可自定义拦截提示，三个等级区别如下：

- 低：最简单验证策略，当单个 IP 规定的时间周期内访问次数达到设置阈值时，自动锁定一段时间。低级别兼容性最好。

  浏览器行为验证说明：当达到规定的访问次数时，如果开启了此选项并且用户是通过浏览器来访问的网站，则说明是正常用户，不会将此 IP 拉黑。这个选项是为了将正常用户和攻击工具、爬虫类程序进行区分。

- 中：对于低级别无法防御的情况（可以自动执行脚本的攻击工具和浏览器无异），可以尝试开启此安全级别，该级别可以智能判断访客的真实性，并且无需访客参与验证，使用了 Cookie、JS 脚本混合验证方式。

- 高：对于长期处于被攻击状态的网站，建议开启高级别模式，高级别模式安全性最高，会在访客首次访问时通过输入一个随机的验证码来确认（图片方式验证码，具有对抗图片识别工具的干扰色），通过验证后浏览无需再次输入验证码。

9.3 网站访问控制

网站访问控制可以对一些特定的请求在网站漏洞防护之前直接进行阻断或拦截。

9.4 网站后门查杀

设置扫描路径后，检测路径下的网站后门，检测结果可放入隔离区并删除或放入信任区。隔离区和信任区可在“扫描设置”中查看，隔离区的文件可删除或恢复到原路径下，可将任意指定文件或文件夹添加到信任区下。

10 工具箱

10.1 勒索防御

10.1.1 风险评估

点击“开始评估”，系统会针对弱口令、系统漏洞、恶意进程、高危端口四项依次检测，检测完成后会根据检测结果给出受到勒索软件攻击可能性的评估。

步骤1. 若其中一项或几项不安全，点击查看可以查看检测结果详情。

10.1.2 实时防御

开启勒索软件启动防护引擎，可以防御已知勒索病毒，在进程试图启动时进行阻断；
开启勒索软件加密防护引擎，可以防御未知勒索病毒，在勒索进程试图加密时进行实时阻断。

白名单设置：如果有对诱饵文件执行写入、重命名、删除的操作程序，但是是被信任的程序，可以在此设置白名单，进行放行。支持模糊匹配。

10.2 挖矿防御

10.2.1 风险评估

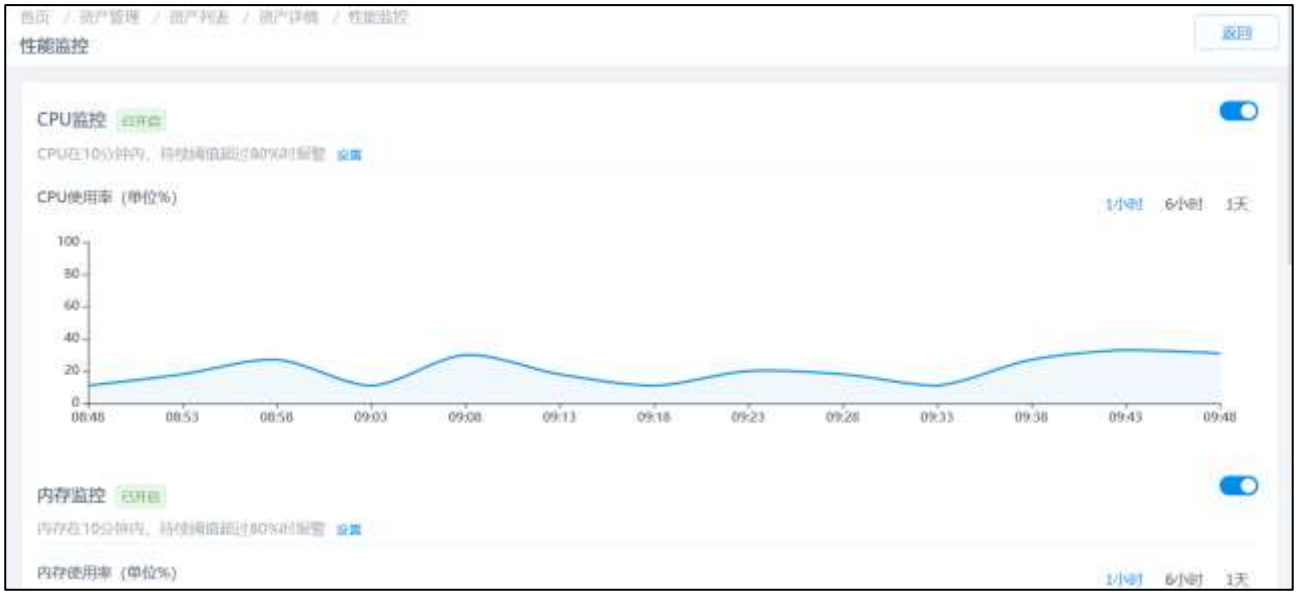
点击开始评估，系统会针对弱口令、系统漏洞、资源占用、恶意进程、DNS 历史查询、异常外联六项依次检测。检测完成后会根据检测结果给出受到挖矿软件攻击可能性的评估。若其中一项或几项不安全，点击查看可以查看检测结果详情。

10.2.2 实时防御

开启挖矿软件启动阻止，每当进程启动时触发一次检测，实时防御挖矿软件。

10.3 性能监控

在性能监控中可对 CPU、内存、网络、磁盘的使用率进行监控。当超过设置的阈值时产生告警。CPU、内存、网络、每个磁盘都存在单独的开关。



10.4 外设管理

10.4.1 无线网卡

可选择是否开启外设监控、使用审计、外设权限。

权限说明：

Ø 禁用：无线网卡插入主机将不被识别。

Ø 放行：默认选项，不进行任何限制。

10.5 文件推送

当需要下发文件、安装应用程序到资产上或者远程执行命令时，可以使用文件推送工具。

Ø 上传的文件：在此选择上传的文件或脚本，文件应该小于 20M；

Ø 下发后立即执行：如果需要立即执行文件，将开关打开；

Ø 执行参数：脚本需要执行时携带的参数；

Ø 备注：关于此次文件推送的备注信息。

10.6 屏幕水印

当租户需要对通过屏幕拍照泄密数据的行为进行溯源，可以使用屏幕水印。

步骤1. 选择一个资产，进入到屏幕水印功能，打开屏幕水印开关；
步骤2. 选择需要展示的水印内容，修改其他默认配置项
步骤3. 点击保存后屏幕水印立即生效。

屏幕水印功能界面：

11 病毒查杀

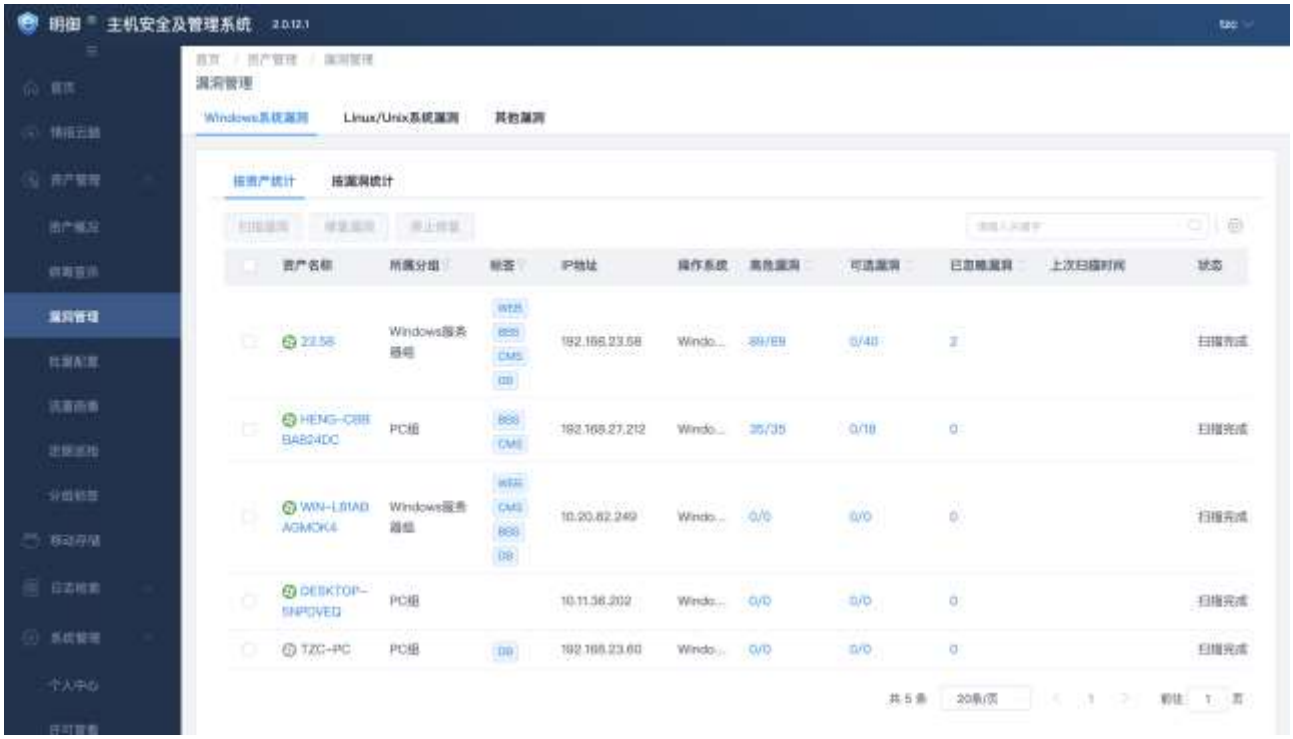
查看全部在线资产的病毒查杀情况。

“快速扫描”可对关键目录进行扫描，“全盘扫描”可对全部磁盘进行扫描，“立即隔离”可隔离资产被扫描到的所有病毒。具体的扫描结果需点击资产名，跳转到相应资产的病毒查杀界面查看、处理。

12 漏洞管理

查看全部资产的漏洞扫描情况。

可在 Windows 系统漏洞、Linux/Unix 系统漏洞、其他漏洞模块中通过“扫描漏洞”进行漏洞的发现。也可以安装漏洞统计查看目前网络内所有资产的漏洞情况。Windows 系统漏洞模块可以批量修复漏洞，也可以点击资产名称进入到相应漏洞扫描界面进行处理。



13 批量配置

可选择一个资产作为样例录制模板，录制好的内容可应用给大量资产。默认内置 10 个模板。

录制步骤如下：

步骤1. 选择一个资产开始录制。

步骤2. 进入录制页面，点击“开始录制”，选择需要批量应用的配置。

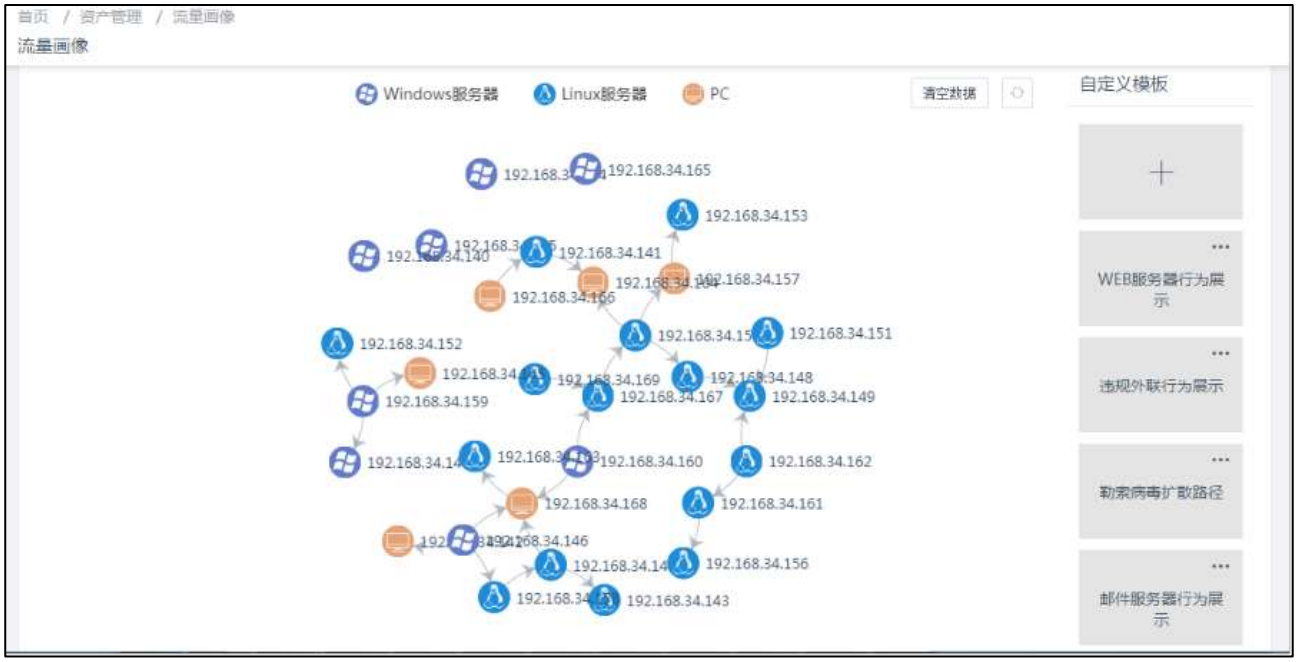
步骤3. 选择可配置的操作后点击“停止录制”，填写模板名和备注保存。在列表里可以看到录制好的模板，可对模板进行应用、查看、编辑、删除四项操作。

14 流量画像

流量画像通过绘制内网全景流量图展示内网主机间的通信关系和内网主机对外通信情况。发现威胁后可对主机间通信进行一键阻断。

流量画像功能首页展示全景流量图，可按 Windows 服务器、Linux 服务器、PC 机三类进行过滤查看，还可按端口、时间过滤查看。

通过自定义模板，资产分组、资产标签、资产名称、资产 IP 过滤查看。



单击某个资产可查看该资产的流量画像详情。通信关系图展示该资产的通信关系：

通信关系列表，列出该资产的通信详情。点击“阻断”可对相应的通信进行一键阻断。

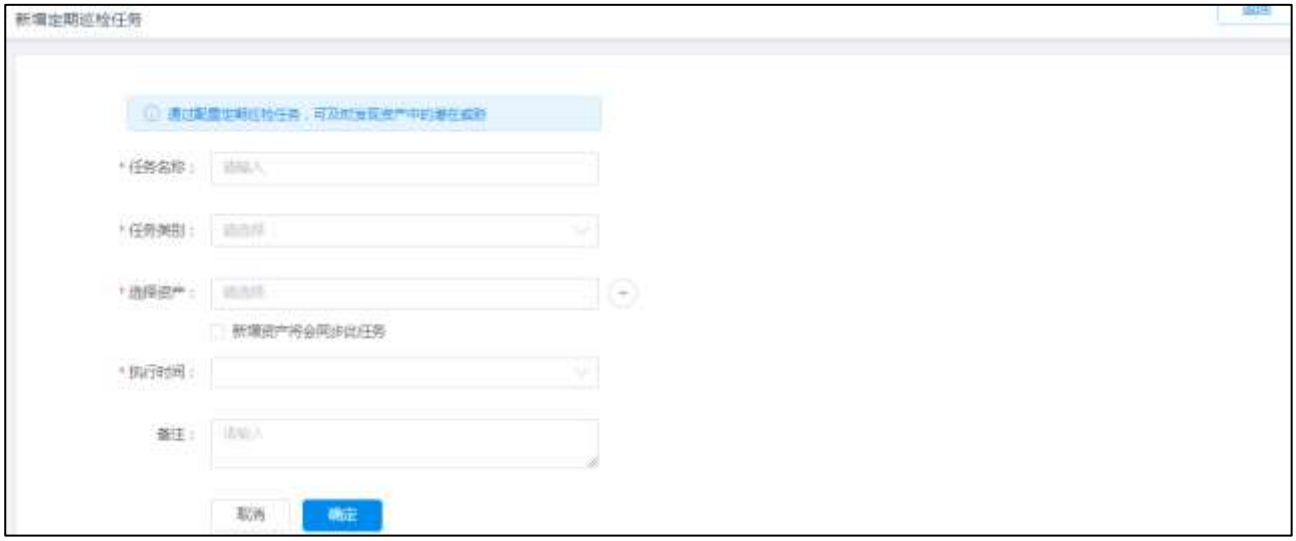
方向	本地IP	本地端口	远程IP	远程端口	协议	开始时间	上次通信时间	通信次数	操作项
入站	172.16.1.255	138	172.16.1.48	138	TCP	2018-12-20 18:27:44	2018-12-20 22:27:46	21	阻断
入站	172.16.1.255	137	172.16.1.48	137	TCP	2018-12-20 18:18:20	2018-12-20 22:23:42	150	阻断
入站	172.16.1.255	138	172.16.1.47	138	TCP	2018-12-20 18:00:37	2018-12-20 22:24:30	23	阻断
入站	172.16.1.255	137	172.16.1.47	137	TCP	2018-12-20 17:53:06	2018-12-20 21:53:07	51	阻断
入站	172.16.1.255	138	172.16.1.39	138	TCP	2018-12-20 01:01:08	2018-12-20 22:16:43	111	阻断

点击两个资产间的箭头，可查看箭头两端的两个资产的通信详情。

15 定期巡检

定期巡检可通过配置定期巡检任务完成定期检测。

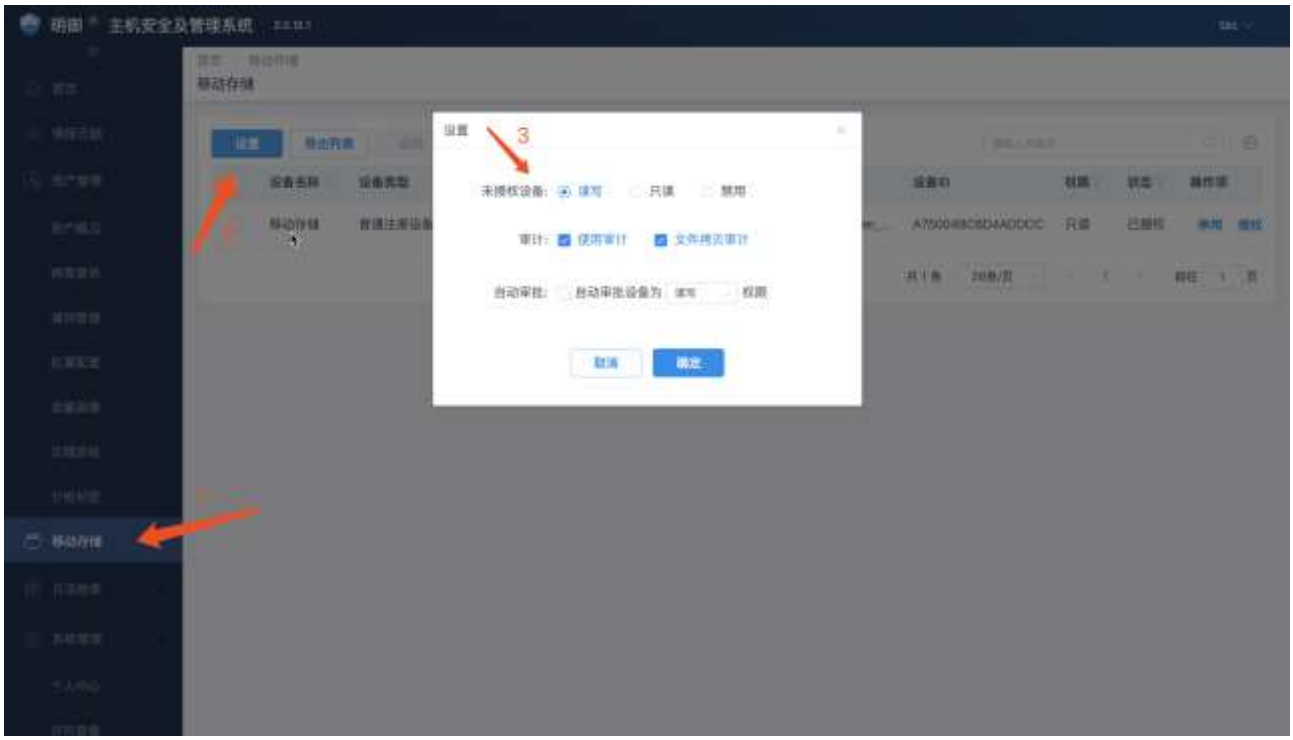
点击“新增”可新增定期巡检任务。填写任务名称、任务类别（病毒查杀、网站后门查杀、弱口令检测、漏洞扫描）、巡检资产、设置是否将新增资产同步此任务、执行检测的时间、备注。点击“确定”保存任务。



16 移动存储

16.1 全网禁用

明御主机安全及管理系统默认是对移动存储不进行控制（即默认读写权限），如果需要对移动存储进行控制，首先需要在“移动存储”模块的“设置”中进行未授权设备的权限控制；



16.2 设备注册

如果需要对特定的移动存储设备开放使用权限，需要进行设备注册。

步骤1. 打开主机卫士界面，找到菜单栏中的设备注册；

步骤2. 插入移动存储设备（如图中的新加卷 D：），提交注册申请；

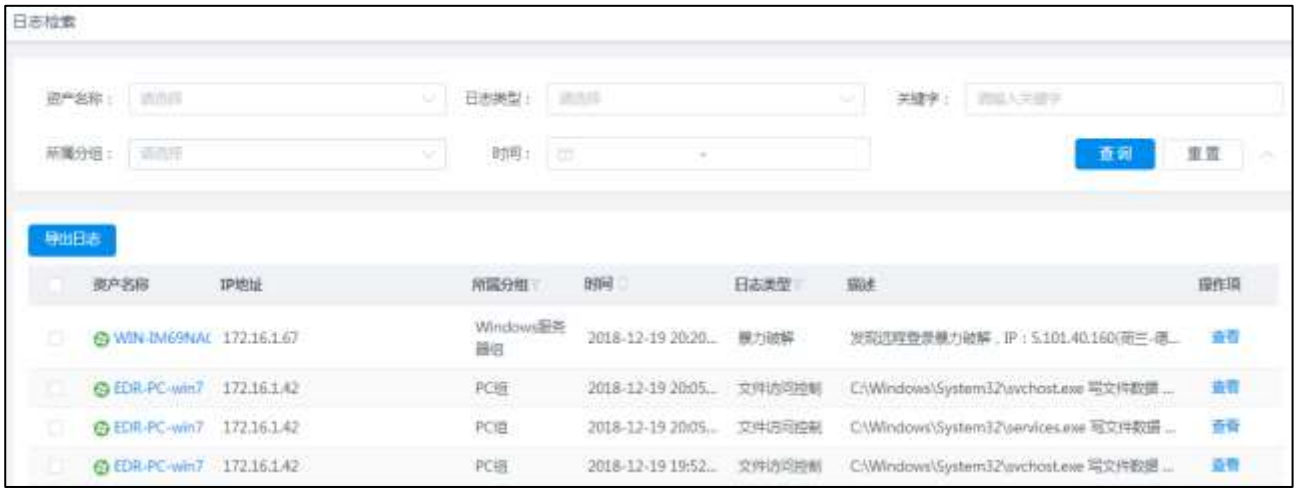
步骤3. 租户登录管理中心，找到对应的申请注册的设备，点击审核。设置设备的使用权限；

步骤4. 点击确定即可完成注册。注册后该设备即可对所有资产享有使用权限。

备注：如果审批设置为未通过或者停用设备，则该设备的权限和未授权设备权限一致。

17 日志检索

日志检索中记录了网站防护、登录防护、异常文件、性能监控、系统防护的日志。可以根据关键字、日志类型等信息来查询。点击“导出日志”可导出格式为 csv 的日志，支持最多导出 10 万条，当前总数超过 10 万条则导出最新的 10 万条。点击资产名，可跳转到相应的配置页面查看详情或更改配置。



18 系统管理

18.1 个人中心

可修改用户密码、修改用户真实姓名、修改头像。

18.2 升级管理

通过 admin 用户登录，上传管理平台、终端软件、病毒库、系统漏洞库、Windows 补丁库、弱口令库、Web 后门库、违规外联黑名单库的离线包。

再通过租户账号，在“系统设置-升级管理”界面，可升级客户端和病毒库。点击资产名称可跳转到相应资产的配置页面。

18.3 添加资产

在添加资产页面中，可以查看目前软件所支持的操作系统版本。以及可以在该页面下载客户端安装包。并且可以查看连接管理中心时所需要的管理员识别码（UUID）。

19 多级中心

下级中心如何连接上级中心？

步骤1. 使用 admin 账号登陆管理平台；

步骤2. 进入多级中心，点击配置上级；

步骤3. 输入上级中心的地址（提前获取上级中心 IP 在此填入）以及端口（默认 443）；

步骤4. 点击连接上级成功后即可在上级连接状态查看连接状态和上级 IP。