

主机安全

用户使用指南



前言

概述

天翼云主机安全系统(简称"主机安全系统"或者"系统")是在深入分析与研究常见黑客入侵技术的基础上,总结归纳大量的安全漏洞信息和攻击方式后,研制开发的新一代终端安全防护产品。

本手册描述天翼云主机安全系统的配置方法,主要包括快速入门、Web 配置页面简介、许可管理、角 色权限、用户认证、首页、终端监控大屏、终端管理、发布端管理、高级威胁、策略管理、响应处置、 屏幕溯源、风险评估、安全策略、日志检索、终端全览、多级中心、升级管理、系统管理、运维平台 等。

手册所提供的内容仅具备一般性的指导意义,并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因,手册中所提供的内容与用户使用的实际设备界面可能不一致,请以用户设备界面的实际信息为准,手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要,手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容 均为示意,不指代任何实际意义。

预期读者

本文档主要适用于使用天翼云主机安全系统的读者,包括服务工程师、系统管理员、网络管理员等。 本文假设读者对以下领域的知识有一定了解:

- ◆ TCP/IP、SNMP 等基础网络通讯协议。
- ◆ 终端防护类产品基本原理。
- ◆ 网络安全相关知识,包括 DDoS、SQL 注入、目录遍历、暴力破解等常见攻击原理及防护手段。
- ◆ 安全防护策略的基本工作原理和配置。

格式约定

本手册内容格式约定如下。

内容	说明
粗体字	Web 界面上的各类控件名称以及内容。例如:"在菜单栏选择'系统状态'进入系统状态。
<>	Web 界面上的按钮。例如: "微信认证失败,点击<我要上网>不弹出微信认证界面"。

内容	说明
>	介绍 Web 界面的操作步骤时,用于隔离点击对象(菜单项、子菜单、按钮以及链接等)。 例如:"在菜单栏选择' 策略配置>认证管理>认证策略 '查看是否开启了认证策略"。
斜体字	可变参数,必须使用实际值进行替代。例如:"在浏览器地址栏输入'http:// <i>管理 IP'</i> ,回车后进入系统 Web 管理平台登录页面"。

本手册图标格式约定如下。

图标	说明
	提示,操作小窍门,方便用户解决问题。
	说明,对正文内容的补充和说明。
	注意,提醒操作中的注意事项,不当的操作可能会导致设备损坏或者数据丢失。
À	警告,该图标后的内容需引起格外重视,否则可能导致人身伤害。

修订记录

日期	修订版本	修改记录
2025-01-20	02	优化文档结构和部分描述。
2023-06-30	01	初次发布。





1	快速入门	 1 1
	1.2 产品功能	1
	1.3 登录系统	2
	1.4 角色与权限说明	2
2	Web 配置页面简介	3
3	操作日志	4
	3.1 Admin 账户操作日志	4
	3.1.1 查询操作日志	4
	3.1.2 导出操作日志	4
4	联动管理	5
	4.1 数据外发	5
	4.1.1 日志外发	5
	4.1.2 API 接口	6
5	首页	7
6	态势大屏	9
	6.1 设置大屏模式	9
	6.1.1 图表模式	9
	6.1.2 列表模式	9
	6.2 安全概况大屏	10
	6.3 终端管控大屏	11
7	终端管理	.12
	7.1 管理终端	12
	7.1.1 查看终端详情	12
	7.1.2 编辑终端	13
	7.1.3 查看策略	14
	7.1.4 终端登记	14



7.1.5	远程协助17
7.1.6	其他操作18
7.2 移动	力存储20
7.2.1	注册设备20
7.2.2	设置自动授权22
7.2.3	其他操作22
7.3 管理	里分组标签22
7.3.1	新增分组23
7.3.2	新增标签23
7.3.3	其他操作24
7.4 主标	几发现24
7.4.1	新建主机发现任务
7.4.2	执行主机发现任务25
7.4.3	查看主机发现扫描结果
7.4.4	其他操作
7.5 容器	暑安全
7.5.1	查看容器详情
7.5.2	启动容器防篡改防护
7.5.3	暂停容器防篡改防护
7.5.4	停止容器防篡改防护
7.6 敏愿	感词检索
7.6.1	新增任务和相关操作项
7.6.2	其他操作项
7.7 网立	占备份
7.7.1	新增任务和相关操作项
7.7.2	其他操作项



	7.8 网站恢复	33
	7.8.1 新增任务	33
8	资产盘点	34
	8.1 资产盘点	34
	8.1.1 进行资产盘点	34
9	风险评估	36
	9.1 查杀病毒	36
	9.1.1 终端视角	36
	9.1.2 病毒视角	44
	9.2 网马查杀	46
	9.2.1 扫描终端的网马	47
	9.2.2 查看扫描结果	49
	9.2.3 处理网马	49
	9.2.4 导出报告	50
	9.2.5 设置查杀模式	50
	9.2.6 相关操作	51
	9.3 漏洞管理	53
	9.3.1 Windows 系统漏洞	53
	9.3.2 Linux 系统漏洞	58
	9.3.3 Windows 应用漏洞	60
	9.3.4 Linux 应用漏洞	62
	9.4 终端体检	64
	9.4.1 终端评估	64
	9.4.2 勒索评估	65
	9.4.3 挖矿评估	65
	9.4.4 弱口令评估	66
	9.4.5 查看评估结果	66



9.5 基线	检查67
9.5.1	新增任务67
9.5.2	执行任务67
9.5.3	相关操作68
9.6 定期	巡检任务68
9.6.1	新增定期巡检任务68
9.6.2	编辑定期巡检任务69
9.6.3	删除定期巡检任务70
9.7 弱口	令检测70
9.7.1	应用弱口令70
9.7.2	新增定期巡检任务71
9.7.3	新增定期巡检任务71
10 入侵检 10.1 攻音	测73 击矩阵
10.1.1	攻击热力图73
10.1.2	受攻击主机热力图73
10.1.3	受攻击工作组热力图74
10.2 入住	灵告警74
10.2.1	入侵告警信息75
10.2.2	入侵告警处理
10.3 检测	则规则
10.3.1	检测规则
10.3.2	信任列表82
10.3.3	处置方式
10.4 模型	Ð83
10.4.1	新增信任模型
10.4.2	查看信任模型



11 威胁情报	87
11.1 智能鉴定	
11.2 沙箱分析	
12 发布端管理	
12.1 管理发布端	
12.1.1 新增发布端	
12.1.2 修改发布端信息	
12.1.3 其他操作	
12.2 配置发布信息	
12.2.1 新增发布目录	
12.2.2 配置发布端策略	
12.2.3 其他操作	
13 高级威胁	94
13.1 设置勒索防御	94
13.2 设置挖矿防御	94
13.3 设置渗透追踪	95
13.4 查看情报云脑	
14 策略管理	98
14.1 终端策略	
14.1.1 新增策略	
14.1.2 编辑策略	
14.1.3 绑定终端	
14.1.4 其他操作	
14.2 容器策略	
15 响应处置	149
15.1 微隔离	
15.1.1 混合模式	
15.1.2 白名单模式	



15.1.3 黑名单模式	156
15.2 流量画像	159
15.2.1 查看通信关系	159
15.2.2 自定义模板	162
15.3 文件推送	163
15.4 事件调查	164
15.4.1 搜索事件数据	164
15.4.2 配置数据采集	164
16 日志检索	167
16.1 防护日志	167
16.1.1 查看防护日志	167
16.1.2 导出防护日志	167
16.1.3 统计分析	168
16.2 操作日志	168
16.2.1 查询操作日志	169
16.2.2 导出操作日志	169
16.3 运维日志	169
16.3.1 查询运维日志	169
16.3.2 导出运维日志	169
16.4 篡改分析	170
16.5 日志报表	171
16.5.1 导出报表	171
16.5.2 订阅报表	171
17 终端全览	173
17.1 查看终端详情	173
17.2 前往租户	173
17.3 导出	173

C 天翼云 State Cloud

18 多级中心	175
18.1 查看中心详情	
18.2 配置上级中心	
18.3 其他操作	176
19 系统管理	
19.1 Admin 账户系统管理	
19.1.1 客户端及库升级	177
19.1.2 管理平台升级	
19.1.3 Windows 补丁库	
19.1.4 密码及访问策略	185
19.1.5 部署管理	
19.1.6 个性化	
19.2 租户账户系统管理	189
19.2.1 部署管理	189
19.2.2 许可分配	196
19.2.3 告警配置	196
19.2.4 个人中心	198
20 运维平台	199
20.1 查看运维诊断结果	
20.2 清理磁盘	200
20.3 重置密码	201
20.4 恢复数据	201
20.4.1 恢复 MySQL 数据	
20.4.2 检测 ES 状态	
21 FAQ	
21.1 如何区分 Docker 版本与非 Docker 版本?	
22 术语&缩略语	205



1快速入门

1.1 产品简介

天翼云主机安全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。 主机安全系统有着业界领先的文件诱饵勒索专防专杀能力;能通过内核级东西向流量隔离技术,实现 云主机隔离与防护;并拥有补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力。

主机安全系统由管理控制中心和客户端组成。

- ◆ 管理控制中心部署在独立云主机上,主要功能是把所有客户端信息和管理集中于一体,便于 集中监管和配置安全策略,聚合客户端情报信息进行后续的响应以及处置。管理控制中心采用 B/S 架构,安装完成后,用户可以在任意与管理控制中心网络可达的计算机上访问管理控制中心 的 Web 页面,对终端进行管控。
- ◆ 客户端软件是一个独立的本地可执行程序,安装在需要被管控的主机上,并完成管理员通过 管理控制中心下发的任务和策略。

1.2 产品功能

主机安全系统具有以下功能模块:

1. 防御已知和未知类型勒索病毒

主机安全系统不仅可以阻止已知勒索病毒的执行,而且面对传统杀毒软件束手无策的未知类型勒 索病毒时,主机安全系统采用诱饵引擎,在未知类型勒索病毒试图加密时发现并阻断加密行为, 有效守护主机安全。

2. 防御高级威胁全流程攻击

主机安全系统根据 ATT&CK 理论,对攻防对抗的各个阶段进行防护,包括单机扩展、隧道搭建、 内网探测、远控持久化、痕迹清除。不仅可以做到威胁攻击审计,而且还可以防止黑客进行渗透 攻击,实现攻防对抗 360 度防御。

3. 管控全局终端安全态势

服务器、PC 和虚拟机等终端安装了客户端软件后,上传终端指纹、病毒木马、高危漏洞、违规 外联、安全配置等威胁信息到管理控制中心。用户在管理控制中心可以看到所有安装了客户端软 件的主机及安全态势,并进行统一任务下发,策略配置。

4. 全方位的主机防护体系



主机安全系统不仅包含传统杀毒软件的病毒查杀、漏洞管理、性能监控功能,在系统防护方面还可做到主动防御、系统登录防护、系统进程防护、文件监控,还支持网络防护、Web应用防护、 勒索挖矿防御、外设管理等多个功能点。

5. 流量可视化,安全可见

主机安全系统通过流量画像的流量全景图,展示内网所有流量和主机间通信关系,梳理通信逻辑, 以全局视角对策略进行规划,便于用户第一时间发现威胁,一键清除威胁。

6. 简单配置,离线升级,补丁管理

主机安全系统支持用户自主进行安全配置,能够明确、有效的进行主机防护。主程序、病毒库、 漏洞库、补丁库、Web 后门库、违规外联黑名单库全部支持离线导入升级包、一键自动升级,可 在专网使用。

1.3 登录系统

产品仅支持从天翼云平台页面单点登录主机安全的 web 管理页面。

1.4 角色与权限说明

主机安全系统中,管理员角色与租户角色拥有不同的操作权限。

角色	权限
	◆ 用户认证:新增用户、编辑用户信息、删除用户、登录用户、用户权限。
	◆ 联动管理:产品联动配置、数据外发配置。
	◆ 终端全览: 查看终端列表及终端详情。
	◆ 操作日志: 查看用户登录、编辑、删除等操作
	◆ 多级中心: 配置上级、查看多级中心详情、编辑下级中心信息、删除下级
官理贝	中心。
(admin)	◆ 升级管理:管理平台升级、终端软件安装包上传、终端软件更新包上传、
	病毒库升级、系统漏洞库升级。
	◆ 系统管理: Windows 补丁库管理、弱口令库管理、Linux 驱动包上传、密
	码及访问策略。
	◆ 运维平台:查看运维诊断结果、清理磁盘、重置密码、恢复数据。
	◆ 首页: 查看系统信息概览。
	◆ 终端管理:终端概况、病毒查杀、网马查杀、漏洞管理、微隔离、移动存
	储、分组标签。
却占	◆ 发布端管理:管理发布端、配置发布信息。
俎尸	◆ 高级威胁:勒索防御、挖矿防御、渗透追踪、情报云脑。
	◆ 策略管理:基础信息、系统防护、网络防护、渗透追踪、网页防篡改、Web
	应用防护、信任名单、桌面管控、终端体检。
	◆ 响应处置:信息搜索、文件推送、定期巡检、流量画像。



角色	权限
	◆ 屏幕溯源:对通过屏幕拍照、屏幕截图泄密数据进行溯源,确定泄密的终
	端信息。
	♦ 风险评估:终端体检、基线检查。
	◆ 安全策略: 容器篡改防护。
	◆ 日志检索:防护日志、操作日志、运维日志、日志报表。
	◆ 系统管理:添加终端、推广部署、升级管理、许可分配、告警配置、个人
	中心。
	◆ 运维平台: 查看运维诊断结果、清理磁盘、重置密码、恢复数据。

2 Web 配置页面简介

系统提供简便的 Web 配置页面,主要包括四部分:1.产品信息;2.用户个人中心;3.导航栏;4.操作 区。下图以租户管理员的 Web 配置页面举例说明。

主机安全		安全首页					
首页 安全首页 态势大屏	•	aa⊡⇔ 0	Ľ	待处理病毒 0	<u></u>	得处摄潮洞 0	2
终端管理	•	安全威胁防护					今日 本周 本月
风险评估 入侵检测 或防情报	•		9	病毒实时防护	系統型の	1953Pa	Web请求約3年 0
策略管理	•	终端状态 ⊙ 在线状态 防护状态	异常状态	风险终端 TOP5 ③	今日 本周 本月	事件类型占比 ◎	系统安全 网络安全 …
调应处量 日志检索 系统管理	· ·	SR の 正将 の で の で の で の で の で の で の で の の の の の の の の	% % %		新无政策		● 注紙件経 ● ● 詳細活動計 ● ● 診園上の新 ● ● 放動上の新 ● ● 次大坊の回正 ● ● 改動上の新 ● ● 改動上の新 ● ● 改動上の新 ● ● 改動上の新 ● ● 改動素ホラ ●
		威胁区域		威胁IP		重点关注	
		帽无数编			帽无政语		新无政绩

各区域的详细说明请参见下表。

序号	名称	说明
1	产品信息	产品名称及版本信息,点击此区域可返回 Web 管理平台主页。
2	用户个人中心	用户可在此区域进行以下操作:查看系统版本和授权信息、反馈意见、 登录运维平台、修改密码、退出系统、身份验证器。
3	导航栏	提供了各类管理功能的配置入口,方便用户根据实际需要进行切换。
4	操作区	该区域主要用于信息展示以及相关功能的配置。



3 操作日志

租户用户可在此页面查看租户用户的操作审计记录。

3.1 Admin 账户操作日志

Admin 可在操作日志页面查看用户、操作 IP、日志类型、描述、时间、状态等日志信息。

3.1.1 查询操作日志

步骤 1. 以 Admin 角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"操作日志",设置查询条件(如关键字、日期等),点击<查询>,即可 查询符合该条件的操作日志。

	关键字	■: 请输入关键字(掛	操作IP, 日志类型, 描述)	选择日期: ③ 开始日期	结束日期	2 重置 导出日志	ま 🗙 展开 🗸
<u>2</u>	用户≎	操作IP ≎	日志类型	描述		● 时间 ◇	状态
用户认证	admin	10.11.	日志操作	读取了admin-总	操作日志数据记录	2022-11-28 10:19:55	成功
	admin	10.11.	用户登录	admin登录成功		2022-11-28 10:19:53	成功
	admin	10.11.	日志操作	读取了admin-总	操作日志数据记录	2022-11-28 10:17:54	成功
多级中心	admin	10.11.	日志操作	读取了admin-总	操作日志数据记录	2022-11-28 10:09:52	成功
	admin	10.11.	日志操作	读取了admin-总	操作日志数据记录	2022-11-28 10:09:44	成功
-ecolese	admin	10.11.	用户登录	admin登录成功		2022-11-28 10:09:41	成功
► 操作日志	1 admin	10.11.	日志操作	读取了admin-总	操作日志数据记录	2022-11-28 10:00:04	成功
	admin	10.11.3	用户登录	admin登录成功		2022-11-28 09:59:19	成功
赤外自庄	admin	10.24.	用户登录	admin登录失败		2022-11-27 14:51:20	失败
	admin	10.11.	用户登录	admin登录成功		2022-11-25 19:26:50	成功
					共 73 条	≤ 1 2 3 4 > 20条/页 ∨	前往 1 页

3.1.2 导出操作日志

点击<导出日志>,选择文件格式(CSV或 Excel),可将所查询的操作日志导出至本地。

关键字:	请输入关键字 (操	作IP,日志类型,描述) 选择	日期: ③ 开始日期	结束日期	查询 重置	导出日志 🗸] 展开 ✔
用户 ≎	操作IP ≎	日志类型	描述		时间 🗘	CSV	状态
admin	10.1	日志操作	读取了admin-总操作	日志数据记录	2022-11-28 10:19:55	EXCEL	成功
			支持导出 CSV	格式和 Excel	格式。		
	•	支持最多导出1	0万条,当前总数	数超过 10 万条	则导出最新的10万	条。	



4 联动管理

用户可在该功能快速配置与 Ailpha、APT、-Gatway、堡垒机、蜜罐产品联动。

4.1 数据外发

用户可在该功能快速配置 syslog、kafka 日志外发及 OpenAPI 调用。

4.1.1 日志外发

步骤 1. 以 Admin 角色登录主机安全系统管理平台,在导航栏选择"联动管理>数据外发>日志外发" 进入页面点击 ^{●●}按钮后,开启此功能;再点击<新建>按钮。

日志外发 API接口	日志外发 支持syslog、kafka两种日志外发方式。				
	新建				
	IP地址及其端口号	日志类型	外发方式	topic	操作项

步骤 2. 在弹窗中**外发方式、IP 及端口号、日志类型**后,点击<确定>按钮即可。





4.1.2 API 接口

步骤 1. 以 Admin 角色登录主机安全系统管理平台,在导航栏选择"联动管理>数据外发>API 接口" 进入页面点击 ^{●●}按钮开启此功能即可。

日志外发	OpenAPI调用
API接口	产品支持第三方平台OpenAPI调用,关闭可增强产品安全性。产品联动关联使用OpenAPI,如关闭则联动同步关闭。
	◆ 只要有任意一个如上产品联动必须开启此 api 接口按钮。



仅租户角色具有查看首页权限。

以租户账号登录主机安全系统管理平台,默认进入"安全首页"显示主机终端总体安全概览。

△ 混合云管理平台			Team-1000002052_1000002052 ~
主机安全	安全首页		
首页 ▲ 安全篇页 态防大屏	0 +CH	екцана 0 Феверан	@cl速期号 0
终端管理 🔻	安全威胁防护		今日 本周 本月
风险评估 マ 入侵位则 マ 成防情报 マ		sinetrator 0 Sinetrator	ia Mepilikata
策略管理 🔻	终端状态 (6) 在线状态 (5)户状态 异常状态	风险终端 TOP5 ① 今日 本周 本月	事件类型占比 ① 系统安全 网络安全 …
○ 中心公園 ▼ 日市地表 ▼ 系統管理 ▼	・ (歴史 0 0 載 0% 0 ご 酸 0% 0 日期 0%	NT/LINUE	 ● 法現外経 ● 法現外経 ● 非知道 ● 和知道 ● 和知道 ● 和知道 ● 和利司
	威胁区地	a成後)IP	重点关注
	N/E.ROH	制天政国	制元的组

具体展示信息说明如下。

信息	说明
弱口令	点击弱口令数字,用户可查看终端的弱口令评估结果。详情可参考 <u>弱口令评估。</u>
待处理病毒	点击待处理病毒数字,用户可查看病毒查杀详情。详情可参考病毒查杀。
待处理漏洞	点击待处理漏洞数字,用户可查看详细漏洞信息。详情可参考 <mark>漏洞管理</mark> 。
安全威胁防护	包括渗透追踪防护、勒索深度防护、病毒实时防护、系统登录防护、Web 请求防护,点击防护数字可查看详细防护日志。详情可参考 <u>防护日志</u> 。
终端状态	展示终端总数以及终端状态的占比,包括防护中、停止防护、熔断、隔离中、 驱动未安装、授权过期等。 <u>客端状态</u> [•] <u>在线状态</u> [·]
威胁区域	展示本周攻击次数前五的区域。
事件类型占比	展示本周攻击事件的数据。点击右上角 *** 图标和 "系统安全"、"网络安全" 可查看事件详情。



信息		说明			
	事件类型占比 ⑦	系统安	全网络安全 …		
		○ 违规外联	0		
		○ 异常登录	0		
		○ 勒索深度防护	1		
		○ 防暴力破解	1		
		○ 文件访问监控	0		
		○ 防端口扫描	197		
		O 病毒木马	1		
风险终端 TOP5	默认展示本周被攻击次数前	五的终端。可调	围整统计时间为	"今日"或	"本月"。
威胁 IP	展示本周被攻击次数前五的结	终端 IP 及被攻击	击次数 。		
重点关注	展示日志里的重点关注事件。	2			



仅租户角色具有终端监控大屏操作权限。

态势大屏以可视化的方式展示资产的状态以及安全概况,方便租户快速掌控资产的安全态势。

6.1 设置大屏模式

6.1.1 图表模式

步骤1.在首页页面上方点击<态势大屏>。

明御终端安全及防病毒系统 3.0.3	安全首页	态势大屏

步骤 1. 进入大屏界面后,点击器图标进入图表模式,点击< 图标或 图标可切换要展示的大屏。



步骤 2. 点击 图标,点击开关,开启或关闭轮播功能。开启轮播功能,系统会自动切换大屏。



6.1.2 列表模式

点击 图标进入列表模式,点击对应图片即可展示对应大屏。





6.2 安全概况大屏

安全概况大屏展示终端的总体的安全态势。



详细信息请参见下表。

编号	名称	说明
1	终端分布图	以立体图片的形式展示终端分布情况,可切换展示"全部节点"和"风险 节点"。
2	防护概况	展示风险总数、今日新增风险数量以及风险等级分布图。
3	入侵检测	展示安全防护类型及事件数量统计。
4	防护风险趋势	展示最近一周安全防护事件变化趋势。
5	最近发现的风 险终端	展示最近发现的 5 个风险终端,包括终端名称、IP 地址、风险类型、风险等级和发现时间。
6	检测概况	统计弱口令数量、待处理病毒数量、待处理网马数量和待修复漏洞数量。
7	威胁 IP	展示被攻击次数最多的终端 TOP5,包括 IP 地址和被攻击次数。
8	安全动态	展示所有终端最新的病毒防护等安全事件。



6.3 终端管控大屏

进入终端管控可视化大屏,滚动展示终端部署、防护、资源、告警等信息。



详细信息参见下表。

编号	名称	说明
1	终端状态	终端近期在线、离线状态统计。
2	终端分组统计	终端分组的终端数量统计(包括 Linux 服务器组、系统默认组和 Windows 组和其他自定义分组)。
3	设备系统分类	终端设备按操作系统分布图,包括设备数量及占比。
4	终端安全态势 图	包括总装机量、防护率,并滚动展示各分组的设备类型、安装量和防护率。
5	最新安装主 机、最新发现 主机	展示最新安装的主机和最新发现的主机信息,包括终端名称、IP、操作系统 等信息。
6	版本统计	统计 Windows 版本信息及 Linux 版本信息。
7	标签统计	统计终端标签信息。
8	客户端告警	展示客户端告警信息,主要包括客户端各类防护告警信息。



7 终端管理

仅租户角色具有终端管理权限。

7.1 管理终端

租户角色可在**终端概况**页签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,并可进行查看终端详情、编辑终端、查看策略等操作。

7.1.1 查看终端详情

步骤 1. 以租户角色登录主机安全系统管理平台, 在导航栏选择 "终端管理>终端概况"进入终端概况页面, 选择需要查看的主机终端(须确保终端为在线状态), 点击终端名称或者点击操作项列中的"查 €" 图标

看"图标。

	终端名称 〇	所属分组 🖓	标签 🛛	IP地址 ≎ ♡	MAC地址 ⑦	操作系统 🗘	终端版本 〇	在线状态 🖓	防护状态 🖤	绑定策略	最近一次离线时间 🔅	SSS	操作项			
~	BESKTOP	PC组	DB	10.23.	FC-34-97-B	Windows 10 Enterp	3.0.7.104	 在线 	 防护中 	ttt	2023-10-11 14:46:35	2233333	查看	编辑	策略	远程协助

步骤 2. 进入**终端详情**页面,即可查看该主机终端的详细信息,并可进行远程重启主机、关闭主机及修改远 程端口操作。

i i i i i i i i i i i i i i i i i i i	终端详情	监听端口	运行程序 账	号信息 性能监控	临时封锁IP	Web框架	Web服务	数据库	Web应用	运行应用	安装软件	JAR包	计划任务	环境变量	内核模块	注册表启动项	Windows证书	在线统计
I I I I I I I I I I I I I I I I I I I			计算机信息	1							激活信息	l.						
If BRUER: SUS System Product Name MERSE: Windows 10 Enterprise Edition 64-bit MdfB. MERSE: 0.10904 Image: Bit Im		ww	计算机名称:	DESKTOP-FSHBS	E6						产品ID:	00329-	-00000-00003	-				
操作系統 Windows 10 Enterprise Edition 64-bit 网络信息 ウ吉波 ウゴ ウゴ ウゴ ウゴ ウゴ クゴ	= =		计算机型号:	ASUS System Pro	duct Name													
内核版本: 0.0.0904 ① 0.0904 ①			操作系统:	Windows 10 Enter	rprise Edition 64-	bit					网络信息	1						
・ 企 の ・ 使件信 ・ 使件信 ・ 192.168.0°	-	-	内核版本:	10.0.19045							eth0:	FC	-34-97-🃭 🖬	A 10.23	: 100			
重配 認定 外部 硬件信息 配合(R) Core(TM) 15-10400 CPU © 2.90 GH2 支援語 Materian 528 GH2 528 GH2 支援: Materian 528 GH2	0 🖻	C									eth1:	00	-50-56	192.168	.8) I MAN i::a4d	cc:23de:d		
处理語: Intel(R) Core(TM) I5-10400 CPU © 2.90 GHz 辺智士 主転: ASUSTEK COMPUTER INC. 辺智士 量卡: Intel(R) UHD Graphics 630 辺福 世工 内存信	重启锁知	こ 关机	硬件信息								eth2	00	-50-50-00 🔅	192.168		e40:1cbd:		
主転 ASUSTEK COMPUTER INC. 远程管理 量率 Intel(R) UHD Graphics 630 远程管理端口: 3389 内存信息: A-DATA Technology 2666MHZ 17179869184			处理器:	Intel(R) Core(TM)	i5-10400 CPU @	2.90GHz												
量率: Intel(R) UHD Graphics 630 远程管理端口: 3389 内存信息: A-DATA Technology 2666/HZ 17179869184			主板:	ASUSTeK COMPU	TER INC.						远程管理	₽						
内存信息: A-DATA Technology 2666MHz 17179869184 内存: 15.79GB 客戶端信息 硬盘: HP SSD EX900 250GB 终调版本: 3.07.104 硬盘:NB: - 病毒車更新时间: 2023-10-11 14:04:00 网卡: 其Kn(R) Elsernet Connection (14) 1219-V 网马库更新时间: 2023-10-11 107:58:36			显卡:	Intel(R) UHD Grap	phics 630						远程管理	端口:	3389					
内存: 15.79GB 客户端信息 硬盘: HP SSD EX900 250GB 终强版本:: 3.07.104 硬盘SN码: - 病毒库更新时间: 2023-10-11 14:04:00 网卡: Intel(R) Ethernet Connection (14) /219-V 网马库更新时间: 2023-10-11 107:58:36 声卡: 英特尔(R) 显示音音频			内存信息:	A-DATA Technolog	gy 2666MHZ 1717	79869184												
硬盘: HP SSD EX900 250GB 终端版本: 3.0.7.104 硬盘SN码:			内存:	15.79GB							客户端信	言息						
硬盘SN码: 病毒库更新时间: 2023-10-11 14-04-00 阿卡: Intel(R) Ethernet Connection (14) 1219-V 网马库更新时间: 2023-10-11 07:58:36 声卡: 英特尔(R) 显示器音频			硬盘:	HP SSD EX900 25	OGB						终端版本		3.0.7.104					
网卡: Intel(R) Ethernet Connection (14) /219-V 网马库更新时间: 2023-10-11 07:58:36 声卡: 英特尔(R) 显示器音频			硬盘SN码:								病毒库更	新时间:	2023-10-11	14:04:00				
声卡: 英特尔(R)显示器音频			网卡:	Intel(R) Ethernet (Connection (14)	219-V					网马库更	新时间:	2023-10-11	07:58:36				
			声卡:	英特尔(R) 显示器看	音频													
显示器: AOC2250			显示器:	AOC2250														

终端概况说明如下。

终端信息	说明
终端详情	 ◆ 对终端进行详细信息展示:包括网络信息、环境信息、其他信息等; 并支持远程关闭主机、重启主机、IP/MAC 绑定(适用于 Windows 主机)等操作。 ◆ 点击网络信息的 [•] 图标,可对终端进行 IP/MAC 绑定操作。设置好需要进行绑定的 IP 以及对应的 MAC。绑定后如果 IP 被修改,将会自动退回至绑定的 IP,并在运维日志进行告警。目前只支持对 Windows 系统主机进行 IP/MAC 绑定。 ◆ 点击远程管理端口的 [•] 图标,可修改终端远程管理端口。修改完毕后,



终端信息	说明
	需要重启远程管理服务才能生效,重启过程中将会断开已连接会话。
监听端口	对终端上端口情况进行实时监控。
运行程序	对终端上进程运行情况进行实时监控,并支持远程结束相关进程。
账号信息	对终端上所有账号信息进行统计。
运行应用	对终端上运行的软件应用信息进行统计。
性能监控	对终端上的内存、CPU、磁盘、网络 IO 进行监控统计。
临时封锁 IP	对终端上因为防暴力破解和防端口扫描而引发的临时封锁 IP 进行管理。
注册表启动项	对终端上所有的注册表启动项进行统计和管理。
Web 框架	对终端上运行的 Web 框架进行统计。
Web 服务	对终端上运行的 Web 服务进行统计。
数据库	对终端上运行的数据库进行统计。
Web 应用	对终端上运行的 Web 应用进行统计。
在线统计	对终端的在线时间进行统计。
安装软件	对终端安装包名、版本号、类型、发布者、安装时间等进行统计。
Jar 包	对终端安装所关联的 jar 包进行统计。
计划任务	对终端被制定了哪些计划任务进行统计。
环境变量	对终端的环境变量进行统计。
内核模块	对终端内核模块名称、版本号、模块路径和大小、模块依赖等进行统计。
Windows 证书	对终端的各种证书进行统计。

7.1.2 编辑终端

步骤 1. 以租户角色登录主机安全系统管理平台, 在导航栏选择"终端管理>终端概况"进入终端概况页面, 选择需要编辑的终端, 点击右侧操作项列中的"编辑"图标。

 ● 终端名称 ○
 所履分組 ▽
 标签 ▽
 IP地址 ○ ▽
 MAC地址 ▽
 操作系统 ○
 在线状态 ▽
 防护状态 ▽
 绑定策略
 最近一次集线时间 ○
 sss
 操作项

 図
 ④ DESKTOP-...
 PC组
 DB
 10.23.●
 FC-34-97-B...
 Windows 10 Enterp....
 3.07.104
 • 在线
 • 防护中
 ttt
 2023-10-1114/46/35
 223333
 査員 (編集) 策略) 近程协助

步骤 2. 在弹出的对话框中编辑终端信息,点击<确定>,即可修改终端信息。

编辑终端信息时,若绑定状态开关的状态调整为关闭,将解绑该终端,被解绑的终端会从终端列表中删除。



编辑终端		×
基本信息	ā. ————	
*终端名称:	linux-HJY	
* 所属分组:	test 🗸	
标签:	请选择 ✓	
绑定状态:	并 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	
IP地址:	192.1	
操作系统:	CentOS Linux 7 (Core)	
终端版本:	3.0.2.104	
登记信息		
	取消	

7.1.3 查看策略

步骤 1. 以租户角色登录主机安全系统管理平台, 在导航栏选择"终端管理>终端概况"进入终端概况页面。 步骤 2. 选择需要查看的终端, 点击右侧操作项的"策略"图标, 即可对该终端的策略信息进行查看和编辑 操作, 详情请参考<u>策略管理</u>。

 ● 终端名称 ○ 所圖分組 ☑ 标签 ☑ IP地址 ○ ☑ MAC地址 ☑ 操作系统 ○ 终端版本 ○ 在线状态 ☑ 防护状态 ☑ 绑定策略 最近一次离线时间 ○ sss 操作项

 ◎ DESKTOP-... PC组 DB 10.23.211.2 FC-34-97-B... Windows 10 Enterp... 30.7.104 • 在线 • 防护中 tt 2023-10-11 14:46:35 223333 查看 编辑 策略 远程协助

 7.1.4 终端登记

7.1.4 兴圳豆

终端登记功能仅适用于 Windows 系统终端。

租户管理员可向客户端下发登记指令,客户端用户提交登记信息后,租户管理员可在"终端管理>终端概况"页面的列表中查看登记信息,方便租户管理员了解终端的信息。

步骤 1. 租户管理员下发终端登记指令。

以租户角色登录主机安全系统管理平台,在导航栏选择"终端管理>终端概况"进入终端概况页面,点击<登记管理>。

	DESKTOP	рс±11		10.23. 211	FC-34-97-B	Windows 10 Enterp	3.0.7.104 ませ 戸二方と	• ^{在线} 1 工 		ᄤ	2023-10-11 14:46:3	5 2233335 60 -	查香 绨	<u>編</u> 策	唐 远稍	创办助
	终端名称 🗘	所属分组 🏹	标签 7	IP地址 0 ⑦	MAC地址 习	操作系统 ۞	终端版本 🗘	在线状态 🖓	防护状态 🖓	绑定策略	最近一次离线时间	SSS	操作项			
0 当	前页已选择 1 项,未进	选择 4 项 全选当页	反选当页													重置
导出线	端 登记管理	修改分组修改	际签 更多	§ ∨								请输入关键字			C B	©



5 登记管理					是否启用登记终端:
新增登记设	置删除			请输入关键字	
2 登记信息 ≎	输入类型	<u>1</u>	是否必填	是否启用	操作项
终端负责人	输入框		必填项	启用	编辑删除
3)	在弹出的 新增登记信 。 新增登记信息	息对话框中编辑	谓相关信息,点击< 0	角定>。	×
	*登记信息:	终端负责人	L		
	*是否启用:				
	*是否必填:	◉ 必填项	○ 非必填项		
	* 输入类型:	◉ 输入框	○ 下拉框		
			取消	确定	

详细配置请参见下表。

配置项	说明
登记信息	不超过 15 字符。
是否启用	必须将 是否启用 后的开关置于开启状态,才能使登记信息生效。
是否必填	设置是否为必填项。
输入类型	 ◆ 输入框。 ◆ 下拉框:需要添加数据,以供选择。
4) 点击<	
ら 登记管理	是否启用登记终端: 💶
新增 登记设置 删除	请输入关键字 Q Ö 腊 🕥

5) 在弹出的**登记设置**对话框中选择提醒方式(对于未完成登记信息的终端,会在终端的操作系统界面弹出登记信息弹窗,提醒用户完成终端登记操作),点击<确定>。



登记设置		×
针对未完整登记信息的终端	ł	
○ 不提醒		
● 每次开机提醒		
○ 每隔 2 小时提醒—2	欠	
○ 开机堂驻提醒		

步骤 2. 终端用户提交登记信息。

1) 终端用户在系统托盘右键点击主机安全系统客户端图标 2,选择"资产登记"(以 Windows 10 系统举例说明)。



2) 在弹出的对话框中编辑登记信息,点击<提交>。

搞您根据管理员要求进行	资产登记	_ ×
*所属部门:	财务部	
*终端负责人:	张三	
	提交信息	

3) 在弹出的对话框中点击<确定>。





步骤 3. 租户管理员查看终端登记信息。

以租户角色登录主机安全系统管理平台,在导航栏选择**"终端管理>终端概况**"进入**终端概况**页面,可查看终端登记信息。

导出终端	登记管理	修改分组	修改标签更	\$ V			10.20.11.16	
所属分组▼	标签工	IP地址 0 T	MAC地址T	操作系统 💲	终端版本 🗘	终端状态	所属部门	终端负责人
系统默认组		10.20.11.16	3C-52-82-47	Windows 10 64-bit	3.0.2.104	防护中	财务部	张三

7.1.5 远程协助

租户管理员可向客户端下发远程协助指令,客户端接收到远程协助命令后,租户可以对其进行远程协助。 步骤 1. 租户管理员下发远程协助指令。

 以租户角色登录主机安全系统管理平台,在导航栏选择"终端管理>终端概况"进入终端概况页 面,点击<远程协助>。

DESKTOP	PC组	192.168.27.1	43 00-0C-29-10	Windows 10 64-bit	3.0.3.107	防护中	hjy	查看编辑	1 策略	远程协助
2)	弹出是很	否确定远程协助	页面, 点击	< 确认 >即可进	抗远程协	吔助。				
		提示					×			
		○	制作存在安全风险	法诺信提/作						
			RIFITLX INDU	时连闻床下。						
					取消	Ξ́	确定			
3)	在浏览	器新页签等待连	接建立。							

远程连接中.

远程协助该功能默认被控终端强制服从远程连接指令;

勾选<admin 账户-系统管理-密码及访问策略-高危操作二次验证>后建立连接需要输入身份验证器的验证码;

<策略管理-终端管理-远程协助-应答方式>可以设置:自动应答和用户响应。



7.1.6 其他操作

◆ 以租户角色登录主机安全系统管理平台,在导航栏选择"终端管理>终端概况"进入终端概况页面。租户可在此页面修改终端分组、修改终端标签、导出终端、登记管理操作。

ţ	出终端 登记管	理修改分组	修改标签	更多 🗸					请输入关键字	(2 0 間	0
0	当前页已选择 1 项,	未选择 19 项 全	先当页 反选当	颃							重置	
	终端名称 ≎	所属分组下	标签了	IP地址 ≎ ▼	MAC地址了	操作系统 ≎	终端版本 🗘	终端状态	终端负责人	操作项		
	localhost	系统默认组		10.56.3	00-0C- 2.	CentOS Linux 7 (Core)	3.0.3.104	防护中	-	查看 编辑 策	格 远程协助	6

勾选终端,点击<更多>,在弹出的下拉框中选择不同的菜单项,可对终端进行卸载客户端、删除 终端、停止防护、启动防护、关闭主机、重启主机、重启客户端、迁移终端、修改远程管理端口、导 出终端调试日志、消息推送、一键隔离、取消隔离等操作。

导出线	端 登记管理	修改分组	修改标签 更多 >	2							Ĭ	输入关键字) C	81 0
● 当	前页已选择 1 项,未选择	19 项 全选单	♪ 升级													重置
	终端名称 0	所属分组	⑦ 重启客户端	± ≎ V	MAC地址 🎖	操作系统 ○	终端版本 💲	在线状态	防护状态 🖓	绑定策略	最近一次离线时间 0	11111	操作项			
	(a) CentOS7	Linux服务	⊗ 删除终端	1.34.194, 1	00-0C-29-15	CentOS Linux 7 (Core)	3.0.7.102	 在线 	 防护中 	zyh	2023-09-12 10:31:46		查看	编辑	策略	
	DESKTOP-PBQ	PC组	🖪 导出终端调试日志	3.72.109, 1	00-0C-29-D2	Windows 10 64-bit	3.0.7.102 •	• 在线	• 防护中	通用模板	2023-09-08 17:40:14		查看	编辑	策略	远程协助
	HUTT_MATEBO	PC组	⑧ 停止防护	1.33.12	E0-D4-E8-EA	Windows 11 Professi	3.0.7.103	 在线 	• 防护中	hutt	2023-09-12 10:00:23	TEST	查看	编辑	策略	远程协助
	(a) localhost.locald	Linux服务	◎ 启动防护	1.45.97, 19	00-0C-29-FF	CentOS Linux 7 (Core)	3.0.7.102	• 在线	• 防护中	lennon	2023-09-11 20:20:58		查看	编辑	策略	
	(a) localhost.locald	Linux服务	00 —键隔离	3.16.71	00-0C-29-2B	CentOS Linux 7 (Core)	3.0.7.102	• 在线	 防护中 	jxq	1.55	-	查看	编辑	策略	
	10-20-178-2	Linux服务	000 取消隔离).178.224	FA-1B-5F-A4	CentOS Linux 7 (Core)	3.0.7.102	• 在线	• 防护中	通用模板			查看	编辑	策略	
	(a) 10-20-84-50	Linux服务	☆ 关闭主机).84.50	FA-0B-68-22	CentOS Linux 7 (Core)	3.0.7.102	。 已卸载		通用模板	2023-09-07 10:03:49	自定义	查看	编辑	策略	
	(ii) 111111111111111	PC组	➡ 重 ± 1 ☐ 锁定主机	3.72.135	00-0C-29-D2	Windows 10 64-bit	3.0.7.102	• 已卸载		通用模板	2023-09-01 17:33:36		查看	编辑	策略	远程协助
	(I) DESKTOP-5DBR	PC组	● 消息推送	3.72.165	FC-34-97-C3	Windows 10 Enterpri	3.0.7.102	• 已卸载		通用模板	2023-09-01 16:51:10		查看	编辑	策略	远程协助
	(1) DESKTOP-O4L3	PC组	🕒 迁移终端	1.35.62, 19	00-0C-29-27	Windows 10 64-bit	3.0.7.102	• 已卸载		通用模板	2023-09-04 15:37:16		查看	编辑	策略	远程协助
) jxq-862-176	Linux服务	❷修改远程管理端□	168.27.176	00-0C-29-F9	CentOS Linux 7 (Core)	3.0.7.102	• 已卸载		通用模板	2023-08-24 14:20:05		查看	编辑	策略	
	(B) LAPTOP-POC9R	PC组	18 重新登记信息	3 1.34.194	6C-94-66-B8	Windows 11 64-bit	3.0.7.113	。 已卸载		通用模板	2023-09-08 17:53:00		查看	编辑	策略	远程协助

具体操作说明如下。

操作	说明
导出终端	可将终端信息以 CSV 格式导出至本地。
修改分组/修改标签	修改所选终端的分组/标签,每个终端必须且只能在一个分组内,可以有多个标签。
登记管理	设置终端登记信息,详情请参见 <u>终端登记</u> 。
卸载客户端	卸载终端上的主机安全系统客户端软件。
删除终端	删除终端后,主机安全系统不能对终端进行管控,许可也将释放。终端信息 以及相关日志将会删除,但部分防护依然有效。
停止防护	关闭所选终端当前所有防护。
启动防护	启动对终端的防护。
关闭主机/重启主机	对所选终端进行关机或重启。
重启客户端	对客户端进行重启。



操作	说明
锁定主机	锁定目标客户端。
迁移终端	填写新中心 IP 和 UUID,点击< 确定 >,可对租户内终端进行同中心跨租户迁 移以及不同中心间迁移。
修改远程管理端口	填写需要修改的远程管理端口,勾选 立即重启 ,点击<保存>即可修改远程管理端口。
导出终端调试日志	将所选终端的客户端运行日志,异常转储日志,操作系统日志信息导出。
升级	对客户端主程序进行升级操作。
消息推送	对客户端所在终端进行消息推送(仅适用于 Windows 主机)。 消息推送 × ③ 对Windows主机进行满息弹窗提醒 *消息内容: 请输入消息内容 提示时间: 持续提示 - 0 + 秒 取消 确定
重新登记信息	对客户端重新登记资产信息。



操作	说明
一键隔离	对选定客户端进行一键断网。
取消隔离	对选定客户端取消一键断网策略。

7.2 移动存储

主机安全系统默认对移动存储不进行控制(即默认读写权限),若要对移动存储进行控制,需要对未授权的设备进行审批。

- ◆ 支持管理员对入网的移动存储介质进行注册,并且对已注册的移动介质进行管理。可以有效防止 数据外泄以及移动存储携带病毒入网的问题。
- ◆ 支持的移动存储介质格式包括但不限于 FAT32、exFAT、NTFS 等。

7.2.1 注册设备

当在移动存储管控中(详情请参考<u>配置移动存储管理</u>)设置了禁用移动存储设备,需要在客户端注册移动 存储设备,用户才能在终端上使用移动存储设备。

步骤1.登录终端设备,运行主机卫士客户端。主机卫士客户端的安装方式请参考添加终端。



步骤 2. 点击页面右上方的 [>] 图标,在弹出的下拉框选择"**设备注册**"。

步骤 3. 插入移动存储设备,编辑责任人、联系电话和申请原因,点击<申请注册>提交注册申请。



设备注册			×
盘符:	移动存储 (F:)	~	
设备名称:	移动存储		
容量:	14.66GB		
厂商:	multiple		
产品型号:	card_reader		
责任人:	设备保管责任人		
联系电话:	设备保管人联系电话		
申请原因:	请向管理员注明申请原因		
	申请注册		

步骤 4. 以租户角色登录主机安全系统管理平台,在左侧导航栏选择"终端管理>移动存储",可在设备列 表中查看到该设备即表示注册成功。

步骤 5. 点击设备右侧操作项的"授权"图标。

j	受置 导出列表								请输入关键字		Q () 🗄 🔘
	设备名称 ≎	注册来源	设备类型	责任人 ≎	联系电话≎	容量 ≎	设备供应商	产品类型	设备ID	状态『	操作项
	移动存储		普通注册设备	成都技术	-	57.73GB	kingston	datatraveler_3.0	1B3A912EJ. 🔳 🔍 💪	已授权	删除 授权

步骤 6. 在弹出的**授权**对话框中选择设备权限,点击<确定>,即可完成设备权限设置。

>
终端名称:
容量: 57.73GB
设备ID: 1B3A912EB567DDCC
注册来源:
责任人: 成都技术





当在移动存储管控中(详情请参考<u>配置移动存储管理</u>)设置了禁用移动存储设备,需要开启自动审批功能, 才能在终端上使用移动存储设备。设置自动审批的操作方法如下:

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"终端管理>移动存储"进入移动存储页面,点击<设置>。

设置 导出列表	删除							请输入关键字		Q Ů 🗄 🎯
设备名称 ≎	注册来源	设备类型	责任人 ≎	联系电话 ≎	容量 ≎	设备供应商	产品类型	设备ID	状态了	操作项
移动存储		普通注册设备	成都技术		57.73GB	kingston	datatraveler_3.0	1B3A912EB!	已授权	删除 授权

步骤 3. 在弹出的对话框中设置是否开启自动审批,并设置设备权限、时间策略等,点击<确定>。

自动授权			
时间策略:	● 永久生效 ○ 有效期截3	ā 请选择日期	ė
权限:	○ 只读 ○ 禁用 Ο 词	写	
应用到:	全部终端		

7.2.3 其他操作

步骤1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择 "终端管理>移动存储",可进行以下操作。

- ●选择需要删除的设备,点击右侧**操作项**的"**删除**"图标,在弹出的对话框中点击<确定>,即可 将该移动存储设备删除。
- 勾选多个设备,点击上方的**<删除>**,在弹出的对话框中点击**<确定>**,可批量删除移动存储设备。
- 勾选需要导出的移动存储设备(可勾选多个),点击**<导出列表>**,即可将所选择的设备列表进 行导出。

Ì	受置 导出列表	删除							请输入关键字	C	0	
()	当前页已选择1项, 🕫	未选择 0 项 全选	当页 反选当页									重置
	设备名称 ♡	注册来源	设备类型	责任人 ≎	联系电话 ≎	容量 🗘	设备供应商	产品类型	设备ID	状态『	操作	项
	移动存储		普通注册设备	成都技术		57.73GB	kingston	datatraveler_3.0	1B3A912EB	已授权	删除	₹ 授权

7.3 管理分组标签



对终端设置分组、标签,方便对终端进行分类管理以及对终端进行批量操作。

租户可对分组及标签进行管理,包括新增、编辑和删除等操作。同时可为终端选择分组及添加标签,详情 请参考<u>编辑终端</u>。

- ◆ Windows 7、Windows 8、Windows 10、Windows 11 等操作系统终端默认划分为 PC 组。
- ◆ Windows Server 2003、Windows Server 2008 等操作系统终端默认划分为 Windows 服务器组。
- ◆ Linux 操作系统终端默认划分为 Linux 服务器组。
- ◆ 其他的为系统默认组。

7.3.1 新增分组

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"终端管理>分组标签",选择分组页签。

步骤 3. 点击<新增>。

分組	新聞 副除余	Q 0 55 0
标签	分组名称 ◇	操作项
	Linux 銀号器组	编辑一册除
	□ PCifl	编辑 删除
	Windows腿务器组	编辑 删除
	赛统歌认组	
	test	编辑 删除

步骤 4. 在弹出的对话框中输入组名称,点击<确定>,即可新增分组。

*组名称:	test	

7.3.2 新增标签

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择 "终端管理>分组标签>标签",选择标签页签。

步骤 3. 点击<新增>。

分组	新增	游输入关键字	Q	0	III ()		
标签	标签名称	创建时间	颜色		操作项		
	CMS	2021-12-28 10:55:50	•		编组	删除	
	BBS	2021-12-28 10:55:50			编辑	删除	
	DB	2021-12-28 10:55:50	•		编辑	田邸余	
	WEB	2021-12-28 10:55:50	•		编祖	删除	
	□ xty	2022-04-25 14:31:59	•		编组	删除	

步骤 4. 在弹出的对话框中输入标签名称,选择颜色,点击<确定>,即可新增标签。





7.3.3 其他操作

步骤1.以租户角色登录主机安全系统管理平台。

- 步骤 2. 在左侧导航栏选择 "终端管理>分组标签",选择分组页签,租户可在此页面对分组进行编辑及删除操作。
 - 点击操作项列中的<编辑>,在弹出的对话框中修改组名称,即可编辑分组。
 - 点击操作项列中的<删除>,在弹出的对话框中点击<确定>,即可删除分组。
 - 勾选分组(可勾选多个),点击列表上方的**<删除>**,在弹出的对话框中点击**<确定>**,即可批量 删除分组。

分组	新地 删除 请输入关键字	0 0 00 00
标签	◄ 当前页已选择 1 项,未选择 3 项 重置	全选当页 反选当页
	■ 分組名称 ()	操作项
	Z PC组	编辑 删除
	□ Windows服务器组	编辑 删除
	□ 系统默认组	
	□ Linux服务器组	编辑删除

- 步骤 3. 在左侧导航栏选择 "终端管理>分组标签",选择标签页签,租户可在此页面对标签进行编辑和删除操作。
 - 点击**操作项**列中的<**编辑>,**在弹出的对话框中修改标签名称和颜色,点击<**确定>**,即可编辑标 签。
 - 点击操作项列中的<删除>,在弹出的对话框中点击<确定>,即可删除标签。
 - 勾选需要删除标签(可勾选多个),点击列表上方的**<删除>**,在弹出的对话框中点击**<确定>**, 即可批量删除标签。

分组	新增删除			请输入关键字	Q Ü 🏭 🎯
标签	标签名称	创建时间	颜色		操作项
	CMS	2021-12-28 10:55:50	•		编辑 删除
	BBS	2021-12-28 10:55:50			编辑 删除

7.4 主机发现

租户可对网段内的终端进行扫描,扫描后可查看主机名、IP、MAC、设备类型、操作系统、安装版本、发



现时间。

7.4.1 新建主机发现任务

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"终端管理>主机发现"。

步骤 3. 点击<新建任务>。

新建任务					请输入关键字	Q Ú 🗄 💿
任务名称	发起主机	扫描网段	创建时间	上次扫描时间	状态	操作项
xty	管理中心	192.168.27.100-192.168.27.200	2022-04-25 14:08:44	2022-04-26 11:18:21	扫描结束	执行编辑查看删除

步骤 4. 在弹出的对话框中编辑任务名称、发起主机、扫描网段,点击<确定>即可新建主机发现任务。

创建扫描的	1 务	×
*任务名称	请输入任务名称	
发起主机	请选择终端名称(ip), 不填则默认为管理平台	~
*扫描网段	请输入扫描网段,如192.168.0.50-192.168.0.80	
	取消 确	定

7.4.2 执行主机发现任务

支持单个执行和批量执行主机发现任务两种方式。

♦ 单个执行:

在主机发现任务列表点击操作项列中的<执行>,在弹出的对话框中点击<确定>。

新建任务 拼	衍删除				请输入关键字	Q C 88 (0)
任务名称	发起主机	扫描网段	创建时间	上次扫描时间	状态	操作项
xty	管理中心	192.168.27.100-192.168.27.200	2022-04-25 14:08:44	2022-04-26 11:18:21	扫描结束	执行编辑查看删除
				共	1条 20条/页 >	1 》前往 1 页

◆ 批量执行:

勾选需要执行的任务(可勾选多个),点击列表上方的<执行>,在弹出的对话框中点击<确定>。

新建任务	执行删除				请输入关键字	Q 🖒 🏭 🎯
◀ 当前页已选择 2	1项,未选择0项	重置				全选当页 反选当页
☑ 任务名称	发起主机	扫描网段	创建时间	上次扫描时间	状态	操作项
🗹 xty	管理中心	192.168.27.100-192.168.27.200	2022-04-25 14:08:44	2022-04-26 11:18:21	扫描结束	执行编辑查看删除
✓ test	管理中心	192.168.22.1-192.168.22.100	2022-08-12 10:51:46		-	执行编辑删除
1				н	€2条 20条/页 ∨	< 1 > 前往 1 页



7.4.3 查看主机发现扫描结果

步骤 1. 在主机发现任务列表中点击操作项列中的<查看>。

新建任务	いっ 副除				请输入关键字	Q C 🎛 🎯
任务名称	发起主机	扫描网段	创建时间	上次扫描时间	状态	操作项
xty	管理中心	192.168.27.100-192.168.27.200	2022-04-25 14:08:44	2022-04-26 11:18:21	扫描结束	执行编辑查看删除
test	管理中心	192.168.22.1-192.168.22.100	2022-08-12 10:51:46		-	执行编辑删除
				# 2	条 20条/面 > (1) 前往 1 页

步骤 2. 即可查看主机发现扫描结果,包括主机名、IP、MAC 等信息。

✿ 扫描结果						
主机名	IP	MAC	设备类型	操作系统	安装版本	发现时间
	192.168. = '4'	00:0C:29:26 • • •	general purpose	Linux 3.2 - 4.9	未安装	2022-04-26 11:18:53
	192.168	00:0C:29:4E	general purpose	Linux 3.2 - 4.9	未安装	2022-04-26 11:18:53
DESKTOP-8()	192.168 . .	00:0C:29:1	general purpose	Windows 10.0.1	3.0.2.104	2022-04-26 11:18:53
	192.168. 💻	00:0C:29:	general purpose	Linux 3.2 - 4.9	未安装	2022-04-26 11:18:53

7.4.4 其他操作

- ◆ 点击操作项列中的<编辑>,在弹出的对话框中修改相关信息,点击<确定>,即可编辑主机发现任务。

新建任务	城宁 删除				请输入关键字	Q Ú 🎬 🎯
任务名称	发起主机	扫描网段	创建时间	上次扫描时间	状态	操作项
xty	管理中心	192.168.27.100-192.168.27.200	2022-04-25 14:08:44	2022-04-26 11:18:21	扫描结束	执行编辑查看删除
test	管理中心	192.168.22.1-192.168.22.100	2022-08-12 10:51:46		-	执行编辑删除
				ж	2 条 20条/页 ∨	< 1 > 前往 1 页

7.5 容器安全

主机安全系统可对云工作负载保护平台下的容器提供全生命周期安全管控及防护。

7.5.1 查看容器详情

步骤 1. 在左侧导航栏选择 **"终端管理>容器安全"**,进入容器安全页面,查看容器名称、镜像、容器 ID、 容器所在终端、容器创建时间、运行状态、篡改防护状态等信息。点击**操作项**列中的 **"查看"** 图 标。


刷新	例表						请输入关键字	Q Ú 🎛 🎯
	容器名称	镜像	容器ID	终端名称	创建时间	状态	篡改防护	操作项
	mysql-test	mysql	5a59002	ubuntu	2022-10-19 07:40:08	停止	未防护	查看启动 暂停 停止
	gracious_robinson	mysql	b5a08 🚪 📑		2022-10-19 07:39:47	停止	未防护	查看 启动 暂停 停止

步骤 2. 可查看容器详情信息。

容器详情	
容器名称:	cocky_galileo
资产名称:	jxq-862-176
所属分组:	系统默认组
标签:	
容器ID:	810296c4c322
镜像:	nginx
启动参数:	"/bin/bash"
创建时间:	2020–07–13 13:18:45
状态:	运行
端口:	80/tcp
开始时间:	2020–11–10 19:23:17
结束时间:	2020-11-10 19:18:55
	关闭

7.5.2 启动容器防篡改防护

点击操作项列中的<启动>,可启动对容器的防篡改防护功能。

刷新列表	刷新列表 消输入关键字										
① 当前页已选	择 1 项, 未选择 1 项 全选当页	页 反选当页					重置				
■ 容器名称	镜像	容器ID	终端名称	创建时间	状态	篡改防护	操作项				
mysql-te	st mysql	5a596c209c2a	ubuntu	2022-10-19 07:40:08	停止	未防护	查看 启动 暂停 停止				
7.5.3 暂停容器防篡改防护 点击操作项列中的<暂停>,可暂停容器防篡改防护功能。											
刷新列表						请输入关键字	Q Ů 🖽 🎯				
① 当前页已选择	1项,未选择1项全选当页	反选当页					重置				
■ 容器名称	镜像	容器ID	终端名称	创建时间	状态	篡改防护	操作项				
mysql-test	mysql	5a596c209c2a		2022-10-19 07:40:08	停止	未防护	查看 启动 暂停 停止				



7.5.4 停止容器防篡改防护

点击操作项列中的<停止>,可停止容器防篡改防护功能。

局	新列表						请输入关键字	Q Ú 🗄 🎯
C)当前页已选择1项,未选择	1项全选当页 反	选当页					重置
	容器名称	镜像	容器ID	终端名称	创建时间	状态	篡改防护	操作项
\checkmark	mysql-test	mysql	5a596c209c2a	ubuntu	2022-10-19 07:40:08	停止	未防护	查看 启动 暂停 停止

7.6 敏感词检索

主机安全系统可对资产目录下敏感词汇进行检索和统计。

7.6.1 新增任务和相关操作项

步骤 1. 在左侧导航栏选择 "终端管理>敏感词检索",进入检索页面,点击"新增任务"按钮,填写名称、 敏感词、查询范围、执行时间、备注等相关信息后点击确定。

新增任务	查看所有结果	执行一次	删除			Q () 🏭 Θ
□ 名称 ≎	1	敏感词◎	新增任务	×	1	操作项
1		hello	² * 名称	123	ž,	扁植 查看 立即检索 删除
			* 敏感词	333		
			* 查询范围	分组列表 目录		
				DESKTOP-V2UU4H2(11 v /opt		
				+ 添加一行		
			* 执行时间	×		
			备注	频率 💿 每天 🛛 每周 🔿 每月		
				时间 ① 14:08:38 3 Xfrct		
				取消 确定	共1条 < 1 >	20条/页 ~ 前往 1 页

步骤 2. 可查看配置的任务详情信息。

新增任务	查看所有结果	执行一次 删除				青输入关键字	Q Ů = ()
□ 名称 ≎	1	敦感词 ♡	执行时间 ⇒	状态『	完成时间 🗘	操作项	l
1	h	nello	每天 13:54:19	未开始		编辑	查看 立即检索 删除

步骤 3. 点击操作项的"编辑"按钮,编辑需要修改的相关信息后点击确定。



删除					请输入关键字		Q 0 🖽 0	٢
编辑任务				×		操作项		
* 名称	1			2		编辑查	看一立即检索一删除	
* 敏感词	hello				1	je se		
* 查询范围	分组列表	目录						
	localhost.localdomain(10.50.3	/opt						
		+ 添加一行						
* 执行时间	每天 13:54:19			~				
备注								
			3 取消	确定				

步骤 4. 点击操作项的"立即检索"按钮,即可对其配置任务进行敏感词检索操作。

彩	谱 任务 查看所有结果	执行一次删除				请输入关键字	Q Ů 🎛 🎯
C) 共 1 项, 已选择 1 项 全选	当页 反选当页					重置
	名称 ≎	敏感词≎	执行时间 ↓	状态『	完成时间 🗘	操作项	
	1	hello	每天 13:54:19	未开始		编辑 查	看 立即检索 删除

步骤 5. 点击操作项的"查看"按钮,即可对计划执行完毕后结果进行查阅。

新增任务 查看所有	有结果 执行一次 删除				请输入关键字 Q C 腊 ③
① 共 1 项, 已选择 1	项 全选当页 反选当页				重置
☑ 名称 ≎	敏感词 ◊	执行时间 🗘	状态▼	完成时间 ↓	操作项
☑ 1	hello	每天 13:54:19	未开始		编辑 查看 立即检索 删除



り、敏感词任务详情				
敏感问:	服务器: [请选择服务器 ^		查询 重置
		DESKTOP-V2UU4H2 (10.11.38.215)		
命中信息♀	服务器 🗘	localhost.localdomain (10.50.38.101)	文件路径	
		localhost.localdomain (10.11.40.191)		
		容器1 (192.168.33.205)		
		(10.24.8.118)		
		ADMIN-PC (10.11.43.253)		
		BOB-OFFICEPC (10.24.9.237)		
		centos5.0-x64-2.6.18-8 (10.50.38.26)		
			共0条 《	1 > 20条/页 > 前往 1 页

步骤 6. 点击操作项的"删除"按钮,即可对该计划进行删除操作。

	名称 ≎	敏感词 ≎	执行时间 🗘	状态『	完成时间 🗘	操作项
~	1	hello	每天 13:54:19	未开始	100	编辑 查看 立即检索 删除

7.6.2 其他操作项

步骤 1. 点击列表上方<查看所有结果>按钮,可对所有计划执行完毕后结果进行查阅。

新增任务查看所有结果	执行一次 删除				请输入关键字	Q Ů 🗄 🍥
名称 ≎	敏感词♀	执行时间 ♡	状态『	完成时间≎	操作项	
1	hello	每天 13:54:19	未开始		编辑 查	看 立即检索 删除

步骤 2. 点击列表上方<执行一次>按钮,可启动勾选计划并执行一次操作。

新	增任务查看所有结果	执行一次删除				请输入关键字	QC	0 == (0)
0) 共 1 项, 已选择 1 项 全选	当页 反选当页						重置
	名称 ≎	敏感词 ↓	执行时间♀	状态『	完成时间 🗘	操作项		
	1	hello	每天 13:54:19	未开始		编辑 查看	立即检索	删除

步骤 3. 点击列表上方<删除>按钮,可对勾选计划执行删除操作。

新增任务查看所	有结果 执行一次 删除			谱	的入关键字 Q C 腊 ③
① 共 1 项, 已选择 1	1项 全选当页 反选当页				重置
✓ 名称 0	敏感词 ↓	执行时间 ↓	状态下	完成时间 🗘	操作项
1	hello	每天 13:54:19	未开始		编辑 查看 立即检索 删除

7.7 网站备份

主机安全系统可对资产提供相关目录备份服务。



7.7.1 新增任务和相关操作项

步骤 1. 在左侧导航栏选择 "终端管理>网站备份",进入备份页面,点击"新增任务"按钮,填写名称、 资产、备份方式、网站路径、例外路径等相关信息后点击确定。

明御终端安全及防病毒系统 ^{3.03} 终端概况 资	新增任务	\times	索 网站备份	网站恢复	Í.	💮 te	est 🗸
新增任务	2 * 名称					Q Č BE	۲
□ 名称 ◇ 资产 备份方式 网站路径	*资产 请选择 🗸		备注	保留时间	是否启用 操作	页	
12 localho 异地备 /opt	*备份方式本地备份 ~			30	编辑	立即备份	删除
	* 网站路径						
	例外路径						
	* 备份路径						
	*执行时间 每天 00:00:00	~					
	备注						
	*保留最近 - 30 + 天的备份						
	*是否启用						
	3 取消 确定		, ,	1条 < 🚺	20条/页	~ 前往 1	页

步骤 2. 可查看配置的任务详情信息。

亲	增任务	删除	①修改和删除备	备份任务会导致相	关备份文件删除							请输入关键字		Q () 🗄 🎯
	名称 ≎	资产	备份方式	网站路径	备份服务器	例外路径	备份路径	执行时间	更新时间	状态『	备注	保留时间	是否启用	操作项
	12	localho	异地备	/opt	DESKTOP-C		/opt	每天 00:	2022-11	未开始		30		编辑 立即备份 删除

步骤 3. 点击操作项的"编辑"按钮,编辑需要修改的相关信息后点击确定。



* 名称	12
*资产	localhost.localdomain 🗸
* 备份方式	异地备份 🗸
备份服务器	DESKTOP-CMUVBV4
* 网站路径	/opt
例外路径	
*备份路径	/opt
*执行时间	每天 00:00:00 ~
备注	
*保留最近	- 30 + 天的备份
* 是否启用	

步骤 4. 点击操作项的"立即备份"按钮,即可进行备份操作。

新	餁务	删除	〕修改和删除备	份任务会导致相关	备份文件删除							请输入关键字		QŮ	≣ ⊚
	名称 ≎	资产	备份方式	网站路径	备份服务器	例外路径	备份路径	执行时间	更新时间	状态▼	备注	保留时间	是否启用	操作项	
	12	localho	异地备	/opt	DESKTOP-C		/opt	每天 00:	2022-11	未开始		30		编辑 立即备份	删除
步骤	§ 5. 点	击操作	□项的	"删除"	' 按钮,	即可对	该任务	进行删	除操作	0					
步骤	≹ 5. 点 ^{名称 ≎}	击操作 ^{资产}	三项的	"删除" ^{网站路径}	,按钮,	即可对	该任务	进行删	除操作	o 状态T	备注	保留时间	是否启用	操作项	

7.7.2 其他操作项

步骤1. 勾选任务后点击列表上方<删除>按钮,可对勾选任务执行删除操作。

新增	単任务	删除	〕修改和删除备	i份任务会导致相;	关备份文件删除							请输入关键字		Q	0 🗄	0
0	当前页已选择	1 项, 未选	¥ 0 项 全选	当页 反选当	页										重	
	名称 ≎	资产	备份方式	网站路径	备份服务器	例外路径	备份路径	执行时间	更新时间	状态▼	备注	保留时间	是否启用	操作项		
	12	localho	异地备	/opt	DESKTOP-C	0550	/opt	每天 00:	2022-11	未开始	a#	30		编辑 立即會	备份 册	删除

主机安全系统可对云工作负载保护平台下的容器提供全生命周期安全管控及防护。



7.8 网站恢复

主机安全系统可对资产提供相关目录备份后恢复服务。

7.8.1 新增任务

步骤 1. 在左侧导航栏选择 "终端管理>网站恢复",进入恢复页面,点击"新增任务"按钮,填写名称、 目标主机、备份主机、恢复到、恢复例外等相关信息后点击确定;点击右方操作项相关按钮,执 行同上网站备份通理相关操作。

新增任务 删除				Q () ## ()
	新增任务	×	attention	192.0元1万
	* 名称	× =	[10,000,000]	1941 F-94
	*目标主机 请选择 ~			
	*备份文件 请选择 🗸			
	*恢复到			
	恢复例外			
	[取消 確定		



8 资产盘点

仅租户角色具有资产盘点权限。

8.1 资产盘点

租户可以通过**资产盘点**功能对资产详细情况进行盘点,包括WEB、数据库、软件、注册表、端口、进程、 账户、安装包、jar、计划任务、环境变量、内核、证书等。

8.1.1 进行资产盘点

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"资产盘点"进入资产盘点页面,点击右上角"**立即扫描**"按钮即可对资产进行扫描任务下发。

资产盘》	Ā	Ξ								
\$	14830 当前发现的资	产总数	Web服务是一种网络资源说 Apache、Nginx、Tomcat、	i问服务,一般部署网站 WebLogic、Websphere	服务器上,以便为用户提供 、Jboss、WildFly、Jetty、	网站访问服务。具体而言,Wet IHS、Tengine、BESAppServer得	Web服务	共的软件产品,运行后在计算	最近更新时机操作系统层面表现为一个"服务"进程。	间: 2023-09-06 13:39:44 立即扫描 常见的web服务包括:
æ	Web服务	6	6 Web服务总数	1 Web服务种类数	1 、5% 存在Web服务的主机	⑦ 1 政 Apache	0 其他		0	Apache 6 其他 0
4	Web框架 Web应用	2							请输入关键字	Q I TE I O E
9	数据库	0	web服务名称 0	版本号	启动用户 0	协议 tcn680	服务进程路径 0	关联进程数 ○	服务所在的主机 ○	IP地址 0
	软件应用	187	Apache	2.4.6	S apache	tcp6 :::80	/usr/sbin/httpd	1	localhost.localdomain	10.23.16.71
٢	注册表启动项	4004	Apache	2.4.6	S apache	tcp6 :::80	/usr/sbin/httpd	1	(a) localhost.localdomain	10.23.16.71
	端口	106	Apache	2.4.6	S apache	tcp6 :::80	/usr/sbin/httpd	1	(a) localhost.localdomain	10.23.16.71
	进程	1675	Apache	2.4.6	S apache	tcp6 :::80	/usr/sbin/httpd	1	(a) localhost.localdomain	10.23.16.71
	系统账户	27	Apache	2.4.6	R root	tcp6 :::80	/usr/sbin/httpd	6	(a) localhost.localdomain	10.23.16.71
¥	系统安装包	1391								
JAR	JAR包	6802								
2	计划任务	67							共6条 〈 1 〉	20条/页 > 前往 1 页

步骤 2. 进入**资产盘点**页面,即可查看所有主机的相关 WEB 、数据库、软件、注册表、端口、进程、账户、 安装包、jar 、计划任务、环境变量、内核、证书等信息。



资产盘归		1										
\$	14830 当前发现的资	铲总数	软件应用是为满足用户不	同领域、不同问题的	应用需求而提供的软件	牛, 应用软件可以招	5宽计算机系统的应用领域,放力	软件应用 t硬件功能。软件应用t	3有不同的用途,如办公室软件、多	媒体软件、互联网软件等。	最近更新时间: 2023-09	1-06 13:40:27 立即扫描
e	Web服务	6	210 软件应用总数	36 软件应用种类数	13 - 存在软件	57%	③ SSH — system — pickup — dudied —	6 r 6 c	syslog 5 chrony 4 Redis 4		② system SFTP 其他	7 7 84
Π	Web框架	2					Addita	J Vivivale	All the All th	调输入关键	建字 C	λ 7; © Ε
۵	Web应用	3	软件应用名称 ○	版本号 🗘	应用类別 ≎	启动用户 🗘	可执行文件路径 🗘	关联进程数 0	软件应用所在的主机 ○	IP地址 〇	CPE 0	「商≎
9	数据库	0	SSH	9.2	系统应用	🚯 root	/usr/sbin/sshd	12	(a) debian	10.23.137.42	cpe:/a::SSH:9.2	-
	软件应用	187	SSH	9.2	系统应用	🔞 root	/usr/sbin/sshd	3	Ø debian	10.23.137.42	cpe:/a::SSH:9.2	
0	注册表启动师	4004	SSH	9.2	系统应用	🚯 root	/usr/sbin/sshd	3	(a) debian	10.23.137.42	cpe:/a::SSH:9.2	
			SSH	9.2	系统应用	🚯 root	/usr/sbin/sshd	3	(a) debian	10.23.137.42	cpe:/a::SSH:9.2	-
	端口	106	SSH	9.2	系统应用	🚯 root	/usr/sbin/sshd	2	(a) debian	10.23.137.42	cpe:/a::SSH:9.2	
	进程	1675	system	252	系统应用	🚯 root	/lib/systemd/systemd	2	 debian 	10.23.137.42	cpe:/a::system:	-
	系统账户	27	system	252	系统应用	🔞 root	/sbin/init	31	 debian 	10.23.137.42	cpe:/a::system:	
	系统安装包	1391	SFTP	-	运维工具	🚯 root	/usr/lib/openssh/sftp-se	1	 debian 	10.23.137.42	cpe:/a::SFTP:	
·	TRUXALE	1551	SFTP		运维工具	🚯 root	/usr/lib/openssh/sftp-se	1	 debian 	10.23.137.42	cpe:/a::SFTP:	-
JAR	JAR包	6802	SFTP		运维工具	R root	/usr/lib/openssh/sftp-se	1	debian	10.23.137.42	cpe:/a::SFTP:	
	计划任务	67						共	210条 < 1 2 3 4	4 5 6 11	> 20祭/页	· 前往 1 页

资产盘点说明如下。

终端信息	说明
端口	对终端上端口情况进行实时监控。
进程	对终端上进程运行情况进行实时监控,并支持远程结束相关进程。
系统账户	对终端上所有账号信息进行统计。
软件应用	对终端上运行的软件应用信息进行统计。
注册表启动项	对终端上所有的注册表启动项进行统计和管理。
Web 框架	对终端上运行的 Web 框架进行统计。
Web 服务	对终端上运行的 Web 服务进行统计。
数据库	对终端上运行的数据库进行统计。
Web 应用	对终端上运行的 Web 应用进行统计。
系统安装包	对终端安装包名、版本号、类型、安装包路径、安装时间等进行统计。
Jar 包	对终端安装所关联的 jar 包进行统计。
计划任务	对终端被制定了哪些计划任务进行统计。
环境变量	对终端的环境变量进行统计。
内核模块	对终端内核模块名称、版本号、模块路径和大小、模块依赖等进行统计。
Windows 证书	对 Win 终端的证书进行统计。



9 风险评估

仅租户角色具有终端管理权限。

9.1 查杀病毒

用户可在病毒查杀页面查看所有终端的病毒查杀情况,并支持以终端视角和病毒视角对病毒进行查杀。

- ◆ 支持对所有终端批量进行病毒扫描(快速扫描/全盘扫描/自定义扫描)、停止扫描、处理病毒。
- ◆ 支持设置单个终端信任区和模板化设置信任名单,并可查看单个终端的病毒查杀详情。
- ◆ 支持查杀设置,包括查杀模式(极速模式、低资源占用模式)、多引擎设置(默认引擎、深度扫描引擎)、压缩包扫描设置及处理方式等。
- ◆ 支持扫描后导出病毒查杀的结果报告。

9.1.1 终端视角

9.1.1.1 扫描终端

扫描终端支持快速扫描、全盘扫描、自定义扫描及停止扫描等操作。

9.1.1.1.1 快速扫描

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"风险评估>病毒查杀",选择终端视角页 签。

步骤 2. 勾选需要扫描的终端(可勾选多个),点击<快速扫描>。

终端视角										
处理病毒 快速扫描	全盘扫描	自定义扫描	更多 ∨	查杀设置				请输入关键字	Q	८ ⊞ ⊚
① 共 37 项, 已选择 1 项	2 全选当页 反选	当页								重置
■ 终端名称 \$	所属分组♡	标签了		IP地址 ≎	待处置病毒数 🗘	上次扫描时间 🗘	病毒库版本	状态	操作项	
I localhost.locald	系统默认组			10.11.40.191,1	/	2022-11-17 11:47:35	22.11.21.19	扫描完成	查看 信任区 解	蘭区

步骤 3. 在弹出的对话框中点击<确定>,即可对终端进行快速扫描。

提示		×
是否快速扫描选中终端?		
	取消	确定

9.1.1.1.2 全盘扫描

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"风险评估>病毒查杀",选择终端视角页 签。

步骤 2. 勾选需要扫描的终端(可勾选多个),点击<全盘扫描>。



处理病毒快速扫描	全盘扫描 自	定义扫描更多、	• 查杀设置			词	输入关键字	Q () = ()
① 共 37 项, 已选择 1 项	2 全选当页 反选当页	ĺ.						重置
■ 终端名称 \$	所属分组了	标签了	IP地址 ≎	待处置病毒数 🗘	上次扫描时间 ♡	病毒库版本	状态	操作项
all localhost.locald	系统默认组		10.11.40.191,1	/	2022-11-17 11:47:35	22.11.21.19	扫描完成	查看 信任区 隔离区

步骤 3. 在弹出的对话框中点击<确定>,即可对终端进行全盘扫描。

提示	×
是否全盘扫描选中终端?	
	取消 确定

9.1.1.1.3 自定义扫描

- 步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"风险评估>病毒查杀",选择终端视角页 签。
- 步骤 2. 勾选需要扫描的终端(可勾选多个),点击<自定义扫描>。

处理病毒	快速扫描	全盘扫描	自定义扫描	更多 ×	查杀设置				请输入关键字	QŮ	
①共371	页,已选择1项	全选当页 反选	当页								重置
■ 终端名	;称 ≎	所属分组♡	标签下		IP地址 ≎	待处置病毒数 🗘	上次扫描时间 ≎	病毒库版本	状态	操作项	
1 0 0	alhost.locald	系统默认组			10.11.40.191,1	/	2022-11-17 11:47:35	22.11.21.19	扫描完成	查看 信任区 隔离区	

Х

步骤 3. 在弹出的对话框中点击<添加一行>,新增扫描路径。

自定义扫描路径

/home/Hotfix-dev-3.0.3-v1.0.0-18.zip删除/home/zyh删除/home/zyh/222删除
/home/zyh 删除 /home/zyh/222 删除
/home/zyh/222 删除
/home/zyh/333 删除

步骤 4. 选择终端,再选择需要扫描的路径,点击<确定>,即可新增自定义扫描路径。



自定义路径



步骤 5. 点击<扫描>,即可进行自定义扫描。



9.1.1.1.4 停止扫描

×

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"风险评估>病毒查杀",选择终端视角页 签。



步骤 2. 勾选正在扫描的终端(可勾选多个),将光标移至更多,在弹出的下拉框选择"停止扫描"。

处理病毒	快速扫描	全盘扫描	自定义扫描	更多 >	查杀设置				请输入关键字		Q (5 88	٢
①共37	7项,已选择1项;	全选当页 反遗	当页	停止扫描								重要	ł
● 终端	岩名称 ♡	所属分组	r	导出报告	IP地址 ≎	待处置病毒数 🗘	上次扫描时间 ♡	病毒库版本	状态	操作项			
2 (0)	localhost.localdom	系统默认约	B	升级病毒库	10.50.38.101	/	2022-11-22 00:00:11	22.11.21.19	扫描完成	查看 信任区 [隔离区		

步骤 3. 在弹出的对话框中点击<确定>,即可停止终端病毒扫描。

提示		×
扫描正在进行中,你确定要停止吗?		
	取消	确定

9.1.1.2 查看扫描结果

租户可查看单个终端扫描结果,并可对扫描结果进行添加信任、处理病毒或重新扫描操作。

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"风险评估>病毒查杀",选择终端视角页 签。

步骤 2. 选择需要查看的终端,点击右侧操作项的"查看"图标。

~	(a) localhost.localdom	系统默认组	10.50.38.101	/	2022-11-22 16:07:05	22.11.21.19	正在扫描(27	查看	信任区	隔离区

步骤 3. 进入病毒查杀页面,点击<查看扫描结果>。

租户也可在此页面进行终端扫描、查看隔离区、查看信任区操作。

DESKTOP-NCTPGB4-10.50.24.193



步骤 4. 进入扫描结果页面,可在此页面查看详细病毒木马文件,支持以下操作。

- ◆ 勾选多个病毒木马文件后点击<**信任**>或<**处理**>,可对文件进行批量添加信任区或批量处理操作。
- ◆ 点击<**处理所有**>,可一键处理所有病毒木马文件。
- ◆ 点击<**立即处理**>,可对病毒文件进行处理。
- ◆ 点击<**重新扫描**>,在弹出的对话框中设置扫描路径,点击<确定>可重新对终端进行病毒扫描。

隔离区 信任区



a1111111111110.50.38.26	
共扫描 54206个文件, 发现 938个病毒木马文件 扫描时间: 2022-06-16 09:45:49	立即处理重新扫描
文件路径	病毒名称
n 病毒木马文件2/938	
/root/aspx/nishang/Utility/Add-Persistence.ps1	HackTool/PS.Nishang
/root/aspx/nishang/Utility/Invoke-Encode.ps1	Backdoor/Meterpreter.q
/root/aspx/nishang/Utility/Base64ToString.ps1	HackTool/PS.Nishang
/root/aspx/nishang/Utility/Download.ps1	HackTool/PS.Nishang

9.1.1.3 处理病毒

租户可对已扫描出的病毒文件进行处理,处理后的文件会被放至隔离区。

- 步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"风险评估>病毒查杀",选择终端视角页 签。
- 步骤 2. 勾选需要处理病毒的终端(可勾选多个),点击<处理病毒>。

处理病	海快速扫描 2	全盘扫描	自定义扫描	更多 Y	查杀设置				请输入关键字		Q () 🎬	٢
① 共	◎ 共 37 项,已选择 2 项 全选当页 反选当页										重置	
■ 约	終端名称 ◇	所属分组	T t	示签了	IP地址 ♡	待处置病毒数 🗘	上次扫描时间 🗘	病毒库版本	状态	操作项		
10	Diocalhost.localdom	系统默认约	闺		10.11.40.191,192	/	2022-11-17 11:47:35	22.11.21.19	扫描完成	查看信任区	隔崗区	

步骤 3. 在弹出的对话框中点击<确定>,即可对该终端病毒进行处理。处理完成后,租户可对隔离区文件进 行恢复及删除操作。

处理完的病毒可在隔离区找回	征小	
	处理完的病毒可在隔离区找回	

9.1.1.4 导出报告

租户可导出病毒扫描结果报告。

- 步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"风险评估>病毒查杀",选择终端视角页 签。
- 步骤 2. 将光标移至**更多**, 在弹出的下拉框选择"**导出报告**", 即可将所有终端的病毒扫描报告导出至本地。

勾选终端(可勾选多个),点击<**导出报告**>,可将所勾选的终端病毒扫描报告导出至本地。

处	理病毒 快速扫描	全盘扫描 自定	22扫描	更多 🗸	查杀设置				请输入关键字	Q	0 🗄	٢
0	共 37 项, 已选择1项	全选当页 反选当页		停止扫描							重	置
	终端名称 ≎	所属分组了	标签1	导出报告	IP地址 0	待处置病毒数 🗘	上次扫描时间 ♡	病毒库版本	状态	操作项		
~	DESKTOP-V2U	系统默认组		升级病毒库	10.11.38.215,1	/		22.7.16.8 •	55.	查看 信任区 隔	漓区	



9.1.1.5 升级病毒库

可升级终端上的病毒库,方便租户查杀最新的病毒。操作方法如下:

- 步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"风险管理>病毒查杀",选择终端视角页 签。
- 步骤 2. 勾选需要升级病毒库的终端(可勾选多个),将光标移至更多,在弹出的菜单栏中选择"升级病毒 **库**",即可升级所勾选终端上的病毒库。

处理病毒 快速扫描	全盘扫描	自定义扫描	更多 🗸	查杀设置				青输入关键字		
① 共 37 项, 已选择 1 项	〔 全选当页 反选当	页	停止扫描							重置
终端名称 🗘	所属分组♡	标签1	导出报告	IP地址 🗘	待处置病毒数 🗘	上次扫描时间 ◊	病毒库版本	状态	操作项	
DESKTOP-V2U	系统默认组		升级病毒库	10.11.38.215,1	/		22.7.16.8 •		查看 信任区	隔离区

列表中"病毒库版本"支持排序,支持模糊匹配搜索。

9.1.1.6 设置查杀模式

租户可进行自定义病毒查杀模式,包括扫描模式、多引擎设置、压缩包查杀设置及处理方式等。

- 步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"风险管理>病毒查杀",选择终端视角页 签。
- 步骤 2. 点击<查杀设置>对所有终端设置查杀模式。

选择多个终端后点击<**查杀设置**>,可对终端病毒查杀模式进行批量设置。

攵	地 一	全盘扫描	自定义扫描	更多 🖌	查杀设置			1	青输入关键字	C	\ ୯ ☷ ⊚
0)共 37 项,已选择1项	全选当页 反逆	选当页								重置
	终端名称 ♡	所属分组下	标签『		IP地址 0	待处置病毒数 🗘	上次扫描时间 🗘	病毒库版本	状态	操作项	
~	DESKTOP-V2U	系统默认组			10.11.38.215,1	/		22.7.16.8 •		查看 信任区	隔离区
	(a) localhost.locald	系统默认组			10.50.38.101	/	2022-11-22 16:07:05	22.11.21.19	正在扫描(查看 信任区	隔离区

步骤 3. 在弹出的对话框中设置查杀模式,点击<确定>即可设置成功。

查杀设置	×
扫描模式:	 极速扫描 根据系统硬件配置,自适应扫描速度,对低配主机性能有一定影响 ● 低资源占用,CPU使用率低于 - 100 + % CPU使用率限制设置仅支持Linux系统,Windows通过 智能检测优化各项系统资源占用
多引擎设置:	
压缩包扫描设置:	打描压缩包, 扫描深度 - 99 + 层, 自动跳过 - 100001 + M以上的压缩包文件
处理方式:	 自动处理(优先进行文件修复,修复失败后隔离) • 由用户自行选择 · 删除
	取消



详细配置请参见下表。

配置项	说明
扫描模式	 ◆ 极速扫描:根据系统硬件配置,自适应扫描速度,对低配主机性能有一定影响。 ◆ 低资源占用:限制扫描时 CPU 使用率低于设置值,仅适用于 Linux 系统主机。
多引擎设置	 ◆ 默认引擎:高性能跨平台通用病毒扫描引擎,建议开启。 ◆ 深度扫描引擎:开启后将占用 200MB 磁盘空间,深度扫描引擎占用内存 更多,但扫描速度更快(进行压缩包扫描时需要选择"深度扫描引擎")。
压缩包扫描设 置	设置压缩包的扫描深度,对大于设置值的压缩包不扫描。
处理方式	 对病毒文件的处理方式: ● 自动处理:优先修复并恢复文件,如修复失败则隔离病毒文件。 ● 由用户自行选择:由用户自行选择病毒文件的处理方式。 ● 删除:删除病毒文件。

9.1.1.7 其他操作

租户可查看病毒查杀的病毒详情,并支持对隔离区和信任区进行添加及删除操作。

9.1.1.7.1 查看病毒详情

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"风险评估>病毒查杀",选择终端视角页 签。

步骤 2. 点击待处理病毒数。

Iocalhos	t.locald 系统默认组	10.50.38.246	1308/1308	2022-11-17 15:52:22	22.11.16.19	处理完成	查看	信任区	隔离区
----------	----------------	--------------	-----------	---------------------	-------------	------	----	-----	-----

步骤 3. 在弹出的对话框中查看病毒的名称、MD5 值及文件路径。



病毒数				×
提取样	本			
	病毒名称 1308/1308	MD5	文件路径	
	Backdoor/PHP.WebShell	27b1130fa	/home/zyh/333/webshell-master/php/2020.08.20.13.php	
~	Backdoor/ASP.WebShell.a	d3584159	/home/zyh/333/webshell-master/asp/con2.asp	
×	Backdoor/PHP.WebShell.au	889bfc9fb	/home/zyh/333/webshell-master/web-malware-collection-13-06-2012	
	Backdoor/JSP.WebShell.b	f60be869c	/home/zyh/333/webshell-master/jsp/date.jsp.txt	
×	Backdoor/PHP.WebShell.au	5037ab00	/home/zyh/333/webshell-master/php/PHPshell/c99shell/c99shell.php	1
	Backdoor/ASP.WebShell	9ea82afb8	/home/zyh/333/webshell-master/xakep-shells/ASP/indexer.asp.txt	
\checkmark	Backdoor/JSP.WebShell.d	df46c0a60	/home/zyh/333/webshell-master/jsp/x.jsp	
~	Backdoor/PHP.WebShell.ae	527cf81f9	/home/zyh/333/webshell-master/web-malware-collection-13-06-2012	
V	HackTool/PHP.DirSniffer.a	13f5c7a03	/home/zyh/333/webshell-master/xakep-shells/PHP/Private-i3lue.php.txt	
-	其 1308 条	20条/页 ~	< 1 2 3 4 5 6 … 66 → 前往 1 〕 取消 确认	页

步骤 4. 勾选病毒文件(可勾选多个),点击<**提取样本**>,即可下载病毒文件至本地。

病毒数			×
提取林	¥本2		
	病毒名称 1308/1308	MD5	文件路径
	Backdoor/PHP.WebShell	27b1130fa	/home/zyh/333/webshell-master/php/2020.08.20.13.php
	Backdoor/ASP.WebShell.a	d3584159	/home/zyh/333/webshell-master/asp/con2.asp
	Backdoor/PHP.WebShell.au	889bfc9fb	/home/zyh/333/webshell-master/web-malware-collection-13-06-2012
	Backdoor/JSP.WebShell.b	f60be869c	/home/zyh/333/webshell-master/jsp/date.jsp.txt
	Backdoor/PHP.WebShell.au	5037ab00	/home/zyh/333/webshell-master/php/PHPshell/c99shell/c99shell.php
	Backdoor/ASP.WebShell	9ea82afb8	/home/zyh/333/webshell-master/xakep-shells/ASP/indexer.asp.txt
	Backdoor/JSP.WebShell.d	df46c0a60	/home/zyh/333/webshell-master/jsp/x.jsp
	Backdoor/PHP.WebShell.ae	527cf81f9	/home/zyh/333/webshell-master/web-malware-collection-13-06-2012
	HackTool/PHP.DirSniffer.a	13f5c7a03	/home/zyh/333/webshell-master/xakep-shells/PHP/Private-i3lue.php.txt
-	a 1.1 milairi 11		
	1 共 1308 条	20条/页 >	《 1 2 3 4 5 6 ··· 66 》前往 1 页
			取消 确认

9.1.1.7.2 处理隔离区中的文件

步骤 2. 点击操作项列中的<隔离区>。

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"风险评估≻病毒查杀",选择终端视角页 签。



☑ ③ DESKTOP-V2UU4H2 系统默认组

步骤 3. 进入隔离区页面,可对隔离区的文件进行恢复或删除操作。

● 勾选需要处理的文件(可勾选多个),点击**<恢复>**,在弹出的对话框中点击**<确定>**,可恢复文件至隔离前的路径。

22.7.16.8 •

查看 信任区 隔离区

- 勾选需要处理的文件(可勾选多个),点击**<删除>**,在弹出的对话框中点击**<确定>**,可删除文件。
- 点击<恢复全部>,在弹出的对话框中点击<确定>,可恢复所有的文件至隔离前的路径。
- 点击<删除全部>,在弹出的对话框中点击<确定>,可删除隔离区中的所有文件。

10.11.38.215,192.... --/--

●点击<提取文件>,在弹出的对话框中点击<确定>,可提取隔离区中的所选择文件。

Ð	國南区(centos5.0-x64-2.6.18-8-10.50.38.26)			
15	加全部 副除金部 (活動 副)(18 <u>1</u>)(17(2))(注			0 12 0
œ,	文件路径	病毒名称	摄离时间	操作项
	/root/xakep-shells/ASP/EFSO_2.asp.txt	Backdoor/ASP.WebShell	2022-11-18 12:50:12	(5. 32 110)
	/root/php/PHPshell/c99shell/c99shell.php	Backdoor/PHP.WebShell.au	2022-11-18 12:50:12	恢复一般除
	/root/jsp/Chropper for jsp/夼U跟jsp胸艿 < 蝶母宁能 jsp	Backdoor//SP.WebShell.d	2022-11-18 12:50:12	(55.50 ±009
	/root/net-friend/asp/猫號アasp協程級/dabao.asp	Backdoor/ASP.WebShell	2022-11-18 12:50:12	你复一副時
	/root/asp/RadHat-webshell-del-backdoor/的環境語.asp	Backdoor/Agent.kc	2022-11-18 12:50:12	恢复一删除
	/root/asp/grasp.asp	Trojan//Seneric:7FF797EFEC87F877	2022-11-18 12:50:12	(5. 2 1988
	/home/zyh/webshell-master/asp/ajs/shell_decoded.asp	Worm/VBS.Agent.e	2022-11-17 19:33:07	恢复一副除
	/home/zyh/webshell-master/asp/ASPXspy2.aspx	Trojan/ASP.Agent.a	2022-11-17 19:33:07	(5. 50 809
	/home/zyh/webshell-master/asp/Inderxer.asp	Backdoor/ASP.WebShell	2022-11-17 19:33:07	恢复一副時
	/home/zyh/webshell-master/asp/404.asp	Backdoor/ASP.Webshell	2022-11-17 19:33:07	恢复一批除
	the network of the tradicities of the second states of the second states $\Delta = 100000000000000000000000000000000000$	Bandrahan et ACD Michaelor II	エレート 1 2 3 4 ▶ 200	

9.1.1.7.3 设置信任区

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>病毒查杀",选择终端视角页签。

步骤 3. 点击操作项列中的<信任区>。

☑ ④ DESKTOP-V2UU4H2 系統默认组 10.11.38.215,192.... -/-- - 22.7.16.8 ● -- 直看 信任区 隔离区

步骤 4. 进入信任区页面,租户可添加和删除信任区。

● 点击<添加>,在弹出的对话框中选择路径,点击<确定>,即可将该路径添加至信任区。

● 勾选信任项目,点击<删除>,在弹出的对话框中点击<确定>,即可删除勾选的信任项目。

う信任区		
25570 MMOS		Ú ∰ ()
信任项目	项目类型	操作项
C\Windows\INF\	目录	册印余

9.1.2 病毒视角

9.1.2.1 处理病毒

◆ 方式一:单个处理



步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>病毒查杀",选择病毒视角页签。

步骤 3. 选择需要处理的病毒,点击右侧操作项的"立即处理"图标,即可对该病毒进行处理。

终端视角病毒视角				
处理病毒 删除记录			请输入关键字	۵ 🛱 ک
_ MDS值i: ≎	病毒名称 ↓	已影响终端数 🗘 首次发现	时间 首次发现终端	操作项
_	Backdoor/Meterpreter.q	3 2022-06	-16 1 centos5.0-x64-2	立即处理 查看 删除记录
0061d800aee63ccaf41d2d62ec15985d	Backdoor/ASP.Ace.b	2 2022-06	-16 1 centos5.0-x64-2	立即处理 查看 删除记录
00898cbc3a95544865c6ef3f6dba7506	Backdoor/PHP.WebShell.h	2 2022-06	-16 1 centos5.0-x64-2	立即处理 查看 删除记录
01227ed2792dae420c158fc5c3d8cb0a	HEUR:Backdoor/ASP.WebShell.a	2 2022-11	-16 1 CentOS7	立即处理 查看 删除记录
0152de452f92423829e041af2d783e3f	Backdoor/ASPX.Webshell	2 2022-11	-16 1 CentOS7	立即处理 查看 删除记录
0176c418103fe6acff9b0845429abb52	Backdoor/PHP.WebShell.h	2 2022-06	-16 1 centos5.0-x64-2	立即处理 查看 删除记录
02e8597a4ddade7b69f6fa546ebfe170	Backdoor/Agent.jz	2 2022-06	-16 1 centos5.0-x64-2	立即处理 查看 删除记录
0396bb6a40b74c40fb260aa80525c86f	Backdoor/PHP.WebShell.aj	2 2022-11	-16 1 CentOS7	立即处理 查看 删除记录
03b06b4183cb9947ccda2c3d636406d4	Trojan/Generic!D2D6A5257B9210DD	2 2022-06	-16 1 centos5.0-x64-2	立即处理 查看 删除记录
0421445303cfd0ec6bc20b3846e30ff0	Backdoor/PHP.B374k.b	2 2022-06	-16 1 centos5.0-x64-2	立即处理 查看 删除记录
0477aac059f4f125816e25b207ae50c4	Trojan/Generic129B1D80C24C5E222	2 2022-11 共2286条 < 1 2 3 4	-16 1 CentOS7	立即处理 查看 删除记录 20条页 ∨ 前往 1 页

◆ 方式二:批量处理

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>病毒查杀",选择病毒视角页签。

步骤 3. 选中需要处理的病毒,点击病毒列表上方的<处理病毒>,即可对所选病毒进行处理。

终端	视角 病毒视角							
<u>y</u>	2255市 2256 2 ² □ □ 25 2 ³ □ □ 25 2 ³ □ □ 25 2 ³ □ 10 2 ³ 2 ³ □ 10 2 ³ 2 ³ □ 10 2 ³ 2 ³ 0			[谢给入关键字		٥٥	
	MD5值 ≎	病毒名称 ♡	已影响终端数 ↓	首次发现时间	首次发现终端		操作项	
		Backdoor/Meterpreter.q	3	2022-06-16 1	centos5.0-x64-2	立即处理	查看	删除记录
	0061d800aee63ccaf41d2d62ec15985d	Backdoor/ASP.Ace.b	2	2022-06-16 1	centos5.0-x64-2	立即处理	查看	删除记录
	00898cbc3a95544865c6ef3f6dba7506	Backdoor/PHP.WebShell.h	2	2022-06-16 1	centos5.0-x64-2	立即处理	查看	删除记录
	01227ed2792dae420c158fc5c3d8cb0a	HEUR:Backdoor/ASP.WebShell.a	2	2022-11-16 1	CentOS7	立即处理	查看	删除记录
	0152de452f92423829e041af2d783e3f	Backdoor/ASPX.Webshell	2	2022-11-16 1	CentOS7	立即处理	查看	删除记录
	0176c418103fe6acff9b0845429abb52	Backdoor/PHP.WebShell.h	2	2022-06-16 1	centos5.0-x64-2	立即处理	查看	删除记录
	02e8597a4ddade7b69f6fa546ebfe170	Backdoor/Agent.jz	2	2022-06-16 1	centos5.0-x64-2	立即处理	查看	删除记录
	0396bb6a40b74c40fb260aa80525c86f	Backdoor/PHP.WebShell.aj	2	2022-11-16 1	CentOS7	立即处理	查看	删除记录
	03b06b4183cb9947ccda2c3d636406d4	Trojan/Generic!D2D6A5257B9210DD	2	2022-06-16 1	centos5.0-x64-2	立即处理	查看	删除记录

9.1.2.2 查看病毒详情

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>病毒查杀",选择病毒视角页签。

步骤 3. 选择需要查看的病毒,点击右侧操作项的"查看"图标。

终端	视角 病毒视角							
处	理病毒 删除记录				清输入关键字		۹ 0	
C	共 2286 项,已选择 20 项 全选当页 反选当页							重置
	MD5值 ≎	病毒名称 ≎	已影响终端数 ♀	首次发现时间	首次发现终端		操作项	
<u>~</u>		Backdoor/Meterpreter.q	3	2022-06-16 1	centos5.0-x64-2	立即处理	查看	删除记录
<u>~</u>	0061d800aee63ccaf41d2d62ec15985d	Backdoor/ASP.Ace.b	2	2022-06-16 1	centos5.0-x64-2	立即处理	查看	删除记录
×	00898cbc3a95544865c6ef3f6dba7506	Backdoor/PHP.WebShell.h	2	2022-06-16 1	centos5.0-x64-2	立即处理	查看	删除记录



步骤 4. 即可查看该病毒的详细信息。包括终端名称、病毒路径、发现时间、发现方式及处理结果。

4v					
				请输入关键字	Q () III ()
终端名称	病毒路径	发现时间	发现方式	处理结果	
centos5.0-x64-2.6.18-8	/root/aspx/nishang/Utility/Invoke-Encode.ps1	2022-06-16 10:12:36	主动扫描	已删除	
centos5.0-x64-2.6.18-8	/root/aspx/nishang/Utility/Add-Persistence.ps1	2022-06-16 10:12:36	主动扫描	已删除	
ADMIN-PC	[HKLM\System\CurrentControlSet\Services(5)]	2022-09-22 16:36:54	主动扫描	未处理	
WIN-80NSPKIA48J	[HKLM\System\CurrentControlSet\Services(5)]	2022-09-23 09:49:18	主动扫描	未处理	
容器1	[HKLM\System\CurrentControlSet\Services(5)]	2022-10-12 14:20:15	主动归描	未处理	
容器1	[HKLM\System\CurrentControlSet\Services(5)]	2022-10-27 00:34:46	主动扫描	未处理	
容器1	c\windows\mssecsvr.exe	2022-10-27 00:34:46	主动扫描	已删除	
容器1	c:\windows\mssecsvc.exe	2022-10-27 00:34:46	主动扫描	已删除	
容器1	[HKLM\System\CurrentControlSet\Services(5)]	2022-10-27 00:34:46	主动扫描	未处理	

9.1.2.3 删除记录

◆ 方式一: 单个删除

Backdoor/Meteroreter all

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>病毒查杀",选择病毒视角页签。

步骤 3. 选择需要删除记录的病毒,点击右侧操作项的"删除记录"图标。

步骤 4. 在弹出的对话框中点击<确定>,即可删除该条病毒记录。

■ -- Backdoor/Meterpreter.q

◆ 方式二:批量删除

. _

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>病毒查杀",选择病毒视角页签。

步骤 3. 勾选需要处理的病毒,点击病毒列表上方的<删除记录>。

处理病毒	〕				请输入关键字		Q ()	
①共2	286 项,已选择 20 项 全选当页 反选当页							重置
MD)5值 ↓	病毒名称 ≎	已影响终端数 ↓	首次发现时间	首次发现终端		操作项	
I 1 − 1		Backdoor/Meterpreter.q	3	2022-06-16 1	centos5.0-x64-2	立即处理	查看	删除记录
006	51d800aee63ccaf41d2d62ec15985d	Backdoor/ASP.Ace.b	2	2022-06-16 1	centos5.0-x64-2	立即处理	查看	删除记录
800	398cbc3a95544865c6ef3f6dba7506	Backdoor/PHP.WebShell.h	2	2022-06-16 1	centos5.0-x64-2	立即处理	查看	删除记录

步骤 4. 在弹出的对话框中点击<确定>,即可删除所勾选的病毒文件记录。

0	提示	×	
你确定要删除	余所选记录吗?		
取消	確定		

3

2022-06-16 1... centos5.0-x64-2.... 立即处理 查看 删除记录

9.2 网马查杀



租户可在网马查杀页面查看所有终端的网马查杀情况。

- ◆ 支持对所有终端批量进行网马扫描、停止扫描、处理网马。
- ◆ 支持设置单个终端信任区和模板化管理信任名单,并可查看单个终端的网马查杀页面。
- ◆ 支持查杀设置,可进行扫描完成后自动处理。
- ◆ 支持通过路径配置对 Web 应用目录进行深入检测,并对扫描出的风险文件进行立即隔离、添加信 任区或删除操作。
- ◆ 支持扫描后导出网马查杀的结果报告。

9.2.1 扫描终端的网马

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在导航栏选择"风险管理>网马查杀",勾选需要扫描的终端(可勾选多个),点击<开始扫描>。

开始扫描 处理网马 停止扫描 导出报告	查杀设置					请输入关键字	(Q C 📰 🎯
① 共 37 项, 已选择 1 项 全选当页 反选当页								重置
■ 终端名称 ◇ 所属分组 ▼	标签▼	IP地址 0	网马数 ≎	隔离区 🗘	信任区 🗘	上次扫描时间 ♡	状态	操作项
図 ⑧ 容器1 中心节点		192.168.33.205	12/12	-		2022-11-08 14:47:34	扫描完成	查看
步骤 3. 在弹出的对话框中	自定义扫描路径。	2						
点击< 添加一行 >,	新增自定义扫描	苗路径 。						
i	添加自定义扫描路径					×		
					1			
	扫描路径				操作	贞		
		-						
		④ 添加	一行					
		<u>.</u>	1	-				
				关闭		扫描		

步骤 4. 选择终端,选择路径,点击<确定>,即可新增自定义路径。



Events ● DExtOP-60(43)(192-16827.44) ● DExtOP-60(43)(192-1687.44) ● DExtOP-60(4	自定义路径	×
www.interventionality interventionality interv	E:\xshell\	
v weise v v v v v v v v v v v v v v v v v v v	全部终端 1	► □C:
● CEXPTOP-BOK43Q(192-168.27.41) ● DESKTOP-BOK43Q(192-168.27.41) ● DESKTOP-BOK43Q(192-168.27.	请选择 > 请选择 >	·▼ □E:
● DESKTOP-BOK43Q(192:168.27.43) ● DSSKTOP-BOK43Q(192:168.27.43) ● DSSKTOM-BOK43Q(192:168.27.43) ● DSSKTOM-BOK43Q(192:168.27.43)	清输入内容 Q	▶ □!AppDatasbak
t Lysten vounde information ↓ Diskell ↓	(1) DESKTOP-80K43JQ(192.168.27.143)	□\$RECYCLE.BIN
► trappDatastak ► trappDatastak ★ T ★ T ★ T ★ T ★ T ★ T	1	Lisystem volume information
実 変 歩 骤 5. 勾选需要扫描的自定义路径,点击< 扫描 >,即可对该路径进行扫描。 添加自定义扫描路径 ×		▶ □zAppDatasbak 2
▲ 1 → ★現 @@@ 步骤 5. 勾选需要扫描的自定义路径,点击< 扫描 >,即可对该路径进行扫描。 添加自定义扫描路径 × □ 扫描路径 * 1		
✓ 1 》 按照 5. 勾选需要扫描的自定义路径,点击< 打描 >,即可对该路径进行扫描。 添加自定义扫描路径 × I描路径 操作项 操作项 Exchell、 删除		
▶ 送知 ● 「● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●		
▼ 3) 步骤 5. 勾选需要扫描的自定义路径, 点击< 扫描 >, 即可对该路径进行扫描。 添加自定义扫描路径 ×		
▼ ★ ● 骤 5. 勾选需要扫描的自定义路径,点击 (月描) 「 第加自定义扫描路径 ★ ● ● 打描路径 ● ● 「 ● ● 「 ● ●		
步骤 5. 勾选需要扫描的自定义路径,点击< 扫描 >,即可对该路径进行扫描。 添加自定义扫描路径 × ✓ 打描路径 操作项 Exshell、 账		
步骤 5. 勾选需要扫描的自定义路径,点击< 扫描 >,即可对该路径进行扫描。 添加自定义扫描路径 × <u>清描路径</u> <u>操作项</u> E\xshell\ <u></u>		
步骤 5. 勾选需要扫描的自定义路径,点击<扫描>,即可对该路径进行扫描。 添加自定义扫描路径 ×		关闭
添加自定义扫描路径 ¥ 「 」 日描路径 操作项 E\vshell\ 删除 1	步骤 5. 勾选需要扫描的自定义路径,点击< 扫描 >,	即可对该路径进行扫描。
 ☑ 扫描路径 操作项 ☑ E\xshell\ 删除 	添加自定义扫描路径	×
Image: Patrice patrix操作项E\xshell\<		
Image: ParticipationImage: Participati	· · · · · · · · · · · · · · · · · · ·	
E:\xshell\ 删除	☑ 扫描路径	操作项
	Elyscholly	anire
1		אנאנונע
	1	
④ 添加一行 2	\odot)	忝/川──行 2
关闭		关闭 扫描

步骤 6. 勾选正在扫描的终端(勾选多个),点击<**停止扫描**>,在弹出的对话框中点击<**确定**>,即可停止 终端网马扫描操作。

	开始扫描 处理网马	停止扫描 导出报告	查杀设置					请输入关键字	Q	0 = 0
	① 共 1 项, 已选择 1 项 全选	当页 反选当页								重置
~	终端名称 ≎	所属分组『	标签了	IP地址 🗘	网马数 ≎	隔离区 ≎	信任区 🗘	上次扫描时间 ♡	状态	操作项
	DESKTOP-80K43JQ	PC组		192.168.27.143	62/62	-	-	2022-11-11 16:18:41		查看



9.2.2 查看扫描结果

租户可查看单个终端的网马查杀结果,并可将网马文件加入信任区或进行隔离。

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>网马查杀",选择需要查看的终端,点击右侧操作项的"查看"图标。

×	终端名称 ♡	所属分组『	标签了	IP地址≎	网马数≎	隔离区 🗘	信任区 ≎	上次扫描时间 ♡	状态	操作项
~	DESKTOP-80K43JQ	PC组		192.168.27.143	62/62	-	-	2022-11-11 16:18:41		查看

步骤 3. 进网马扫描结果页面,可在此页面查看详细网站后门文件,并对木马文件进行处理。

- ◆ 勾选多个木马文件,点击<**信任**>,可将文件添加为信任文件且后续跳过该文件扫描。
- ◆ 勾选多个木马文件,点击<**隔离**>,可将木马文件移动至隔离区。
- ◆ 点击<**隔离所有**>或<**立即隔离**>,可将所有木马文件移动至隔离区。

共扫描604084个文件,发现62个网站后门文件 扫描时间: 2022-11-11 16:18:41	<u> 文明時</u> 篇 書 返回
文件路径	后门类型
网站后门文件0/62	
C\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\\$R9GGOYE\Angler\6ae123e38de013fecce073745136ade394e1a4b278e252ad2848 a2f9b6304d5 <mark>清 信任 陽高</mark>	Trojan/VBS.Obfuscated.aa
C\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\\$R9GGOYE\Angler\9c39e004e3fbd7b8da875528f73d70abec523205abdc1cf86e3e9 b0307de3b51	Trojan/JS.Iframe.u
C\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\\$R9GGOYE\Angler\ca494aef2ba1e8273936765b8e8af17ef4ebe18cc134356c9b0b8 fd417395d39	Trojan/JS.Iframe.u

9.2.3 处理网马

租户可对已扫描出的网马进行查杀操作。

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"风险评估>网马查杀",勾选需要处理网 马的终端(可勾选多个),点击<处理网马>。

开始扫描处理网马	停止扫描 导出报告 2	查杀设置					调输入关键字	Q	0 🗄 💿
① 共 1 项,已选择 1 项 全)	先当页 反选当页								重置
✓ 终端名称 🗘	所属分组『	标签『	IP地址 ≎	网马数≎	隔离区 🗘	信任区 ≎	上次扫描时间 ♡	状态	操作项
1 DESKTOP-80K43JQ	PC组		192.168.27.143	62/62		071	2022-11-11 16:18:41	20	查看

步骤 2. 在弹出的对话框中点击<确定>,即可对终端网马进行处理(将文件移动至隔离区)。



		提示	×
		是否确定处理选中网马?	
			取消 确定
9.2.4	导出报告		

租户可导出网马扫描结果报告。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在导航栏选择 "风险评估>网马查杀",选择终端后点击<导出报告>,可将所选中的终端网马扫描 报告导出至本地。

点击<**导出报告**>,导出所有终端的网马扫描报告。

	开始扫描	处理网马	停止扫描	导出报告	查杀设置					请输入关键字	(Q C		٢
(D 共 1 项,	已选择1项全	选当页 反选	当页									重置	
×	终端名和	弥 ≎	所属分组	T	标签下	IP地址≎	网马数 ≎	隔离区 🗘	信任区 ≎	上次扫描时间 🗘	状态		損	鮮印页
~	DES	KTOP-80K43JQ	PC组			192.168.27.143	62/62	-	-	2022-11-11 16:18:41			Ĩ	看

9.2.5 设置查杀模式

租户可进行自定义病毒查杀模式,包括扫描模式、多引擎设置、网马引擎及处理方式等。

步骤 1. 以租户角色登录主机安全系统管理平台, 在导航栏选择"风险评估>网马查杀", 点击<查杀设置>。

	开始扫描	处理网马	停止扫描	导出报告	查杀设置						请输入关键字		Q Ú III 💿
	① 共 1 项	, 已选择 1 项 🕯	全选当页 反选	当页									重置
~	终端名	称 ≎	所属分组"	r	标签了		P地址 ≎	网马数 ≎	隔离区 🗘	信任区 ≎	上次扫描时间 🗘	状态	操作项
~	I DES	SKTOP-80K43JQ	PC组			la	192.168.27.143	62/62	272		2022-11-11 16:18:41		查看

步骤 2. 在弹出的对话框中编辑相关信息,点击<确定>即可对所有终端设置网马查杀模式。

勾选终端后点击<查杀设置>,可对被勾选终端设置网马查杀模式。



查杀设置		\times
扫描模式:	 极速扫描 根据系统硬件配置,自适应扫描速度,对低配主机性能有一定影响 ● 低资源占用,CPU使用率低于 - 50 + % CPU使用率限制设置仅支持Linux系统,Windows通过智能检测优化各项系统资源占用 	
多引擎设置:	 ・ ・ ・	
网马引擎:	网马专用引擎,根据网马特征扫描	
处理方式:	 自动处理(网马文件隔离到隔离区) 由用户自行选择 删除 	
	取消	椗

9.2.6 相关操作

租户可查看网马查杀详情,并支持对隔离区和信任区进行添加及删除操作。

9.2.6.1 查看网马详情

步骤 1. 以租户角色登录主机安全系统管理平台,在左侧导航栏选择"风险评估>网马查杀"进入网马查杀 页面。

步骤 2. 点击网马数。

~	终端名称 🗘	所属分组『	标签▼	IP地址♀	网马数 ≎	隔离区 🗘	信任区 ≎	上次扫描时间 🗘	状态	操作项
\checkmark	DESKTOP-80K43JQ	PC组		192.168.27.143	62/62			2022-11-11 16:18:41		查看

步骤 3. 在弹出的对话框中查看网马详情,包括网马名称及文件路径。



网马描	述		×					
提取	双样本							
	网马名称 62/62	文件路径						
Z	Worm/Xbash.a	C:\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\\$R9 GGOYE\Xbash\31155bf8c85c6c6193842b8d09bda88990d710db9f70efe8 5c421f1484f0ee78						
V	HVM:Trojan/Swrort.gen!A	C:\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\\$R9 GGOYE\VegaLocker\8370b5aaf5d21fdfe7052c90b1e6b8fd3e0fa0bc2600 7badd416b1d4a99bc3cd						
	Ransom/LockFile.fe	C:\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\\$R9 GGOYE\CryptoMix\cadb8633e114f4b91b9b394878231c780bb305939f2 b2a84b0e0f7b3b464f164						
	SVM:TrojanDownloader/JS.Nen ucod.x	C:\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\\$R9 GGOYE\Locky\2504b1f2bdd2839c9c68a29cfd9ca9d831234da473a4b4e1 05471523b4981b6a						
		共62条 20条/页 ∨ 《 1 2 3 4 ≯ 前往 1 〕	ភ					

9.2.6.2 管理隔离区中的网马文件

步骤 1. 以租户角色登录主机安全系统管理平台,在左侧导航栏选择"风险评估>网马查杀",点击隔离区 列中的数字。

म	始扫描	处理网马	停止扫描	导出报告	查杀设置					谢输入关键字		Q 🖒 🏭 🎯
0	共 1 项, 已	选择1项 🕯	全选当页 反逆	适当页								重置
	终端名称(>	所	属分组了	标签了	IP地址 🗘	网马数 ≎	隔离区 🗘	信任区 ≎	上次扫描时间 🗘	状态	操作项
~	DESKTO	DP-80K43JQ	PC	组		192.168.27.143	61/61	1	-	2022-11-11 16:18:41	处理完成	查看

步骤 2. 进入隔离区页面,可对隔离区中的网马文件进行处理。

- 点击**操作项**列中的"恢复"图标,在弹出的对话框中点击<确定>,可将此网马文件从隔离区恢 复至原始路径。
- 点击操作项列中的"删除"图标,在弹出的对话中点击<确定>,可删除此网马文件。
- 勾选需要恢复的网马文件(可勾选多个),点击<**恢复**>,在弹出的对话中点击<**确定**>,可将网 马文件从隔离区恢复至原始路径。
- 勾选需要删除网马文件(可勾选多个),点击<**删除>**,在弹出的对话框中点击<**确定>**,可删除 选择的网马文件。
- 点击<恢复全部>,在弹出的对话框中点击<确定>,可将所有网马文件从隔离区恢复至原始路径。
- 点击<删除全部>,在弹出的对话框中点击<确定>,可删除所有网马文件。
- 勾选需要提取样本的网马文件(可勾选多个),点击<提取样本>,即下载网马文件至本地。



俠	反全部 删除全部 恢复 删除 提取样本			0 🗄 🔘
	文件路径	网马名称	隔离时间	操作项
	C:\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\\$R	Trojan/VBS.Obfuscated.aa	2022-11-23 13:37:36	恢复 删除

9.2.6.3 配置信任区

步骤 1. 以租户角色登录主机安全系统管理平台,在左侧导航栏选择"风险评估>网马查杀",点击信任区 列中的数字。

C	井 1 项, 已选择 1 项 全选当页 反选当页									重置
	终端名称 ↓	所属分组下	标签了	IP地址 🗘	网马数 ≎	隔离区 🗘	信任区 ≎	上次扫描时间 🗘	状态	操作项
~	DESKTOP-80K43JQ	PC组		192.168.27.143	60/60	1	1	2022-11-11 16:18:41	处理完成	查看

步骤 2. 进入信任区页面,租户可对信任项目进行添加及删除操作。

- 点击<添加>,在弹出的对话框中选择路径,点击<确定>,即可将该路径添加至信任区。
- 勾选信任项目,点击**<删除>**,在弹出的对话框中点击**<确定>**,即可删除勾选的信任项目。

ř	出版金 加加 1 1 1 1 1 1 1 1 1 1 1 1 1		0 = 0
	信任项目	项目类型	操作项
	C\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\\$R9GGOYE\Angler\9c39e004e3fbd7b8d	文件	删除

9.3 漏洞管理

租户可在**漏洞管理**页面查看所有终端的漏洞扫描情况,支持的漏洞类型包括但不限于操作系统漏洞 (Windows、Linux 等)、数据库漏洞(MySQL 等)、Web 容器漏洞(Tomcat、Apache、Nginx 等)、其他 组件漏洞。在查看漏洞扫描情况时,默认进入管理界面时会触发一次扫描。

终端视角 漏洞视角								
扫描漏洞 修复漏洞 停止	修复 导出						请输入关键字	Q O # @
终端名称 ≎	操作系统 ≎	IP地址 ↓	高危漏洞 ≎	可选漏洞≎	上次扫描时间 🗘	上次修复时间	状态	操作
DESKTOP-80K43JQ	Windows 10 64-bit	192.168.27.143	0/0	0/0	2022-11-23 13:41:17		扫描完成	查看

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。

9.3.1 Windows 系统漏洞

租户可对 Windows 系统漏洞进行扫描、修复、停止修复、查看扫描结果、导出扫描结果及重启终端操作。



9.3.1.1 终端视角

9.3.1.1.1 扫描终端漏洞

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Windows 系统漏洞",选择终端视角页签。

步骤 3. 勾选需要扫描的终端(可勾选多个),点击<扫描漏洞>。

Windows系统漏洞 Linux系统漏	洞 Windows应用漏洞 Lir	nux应用漏洞							
终端视角 漏洞视角	终端视角 漏洞视角								
扫描漏洞 修复漏洞 停止	修复导出					游转	俞入关键字	Q () III ()	
① 共 1 项, 已选择 1 项 全选当页	反选当页							重置	
✓ 终端名称 ◇	操作系统 ↓	IP地址 🗘	高危漏洞 ◊	可选漏洞 ♡	上次扫描时间 🗘	上次修复时间 🗘	状态	操作项	
1 BESKTOP-80K43JQ	Windows 10 64-bit	192.168.27.143	0/0	0/0	2022-11-23 13:48:40		扫描完成	查看	

步骤 4. 在弹出的对话框中点击<确定>,即可对勾选的终端进行漏洞扫描。

提示		×	
0 确定要开始扫描吗?			
	取消	确定	

9.3.1.1.2 查看扫描结果

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Windows 系统漏洞",选择终端视角页签。

步骤 3. 选择需要查看的终端, 点击右侧操作项的"查看"图标。

~	终端名称 ↓	操作系统 ◊	IP地址 ♀	高危漏洞 ♀	可选漏洞♀	上次扫描时间 🗘	上次修复时间 🗘	状态	操作	巨项
~	DESKTOP-80K43JQ	Windows 10 64-bit	192.168.27.143	0/0	0/0	2022-11-23 13:48:40		扫描完成	查看	音

- 步骤 4. 系统进行终端自动扫描,扫描结束后进入漏洞扫描结果页面。租户可在此页面查看详细漏洞扫描信息,并对终端漏洞进行修复、重新扫描、忽略漏洞及查看漏洞详情操作。
 - ●勾选多个漏洞,点击<一键修复>,可对漏洞进行批量修复。
 - ●将光标悬停至漏洞,点击<**修复**>,可修复该漏洞。
 - ●将光标悬停至漏洞,点击<**忽略**>,可忽略该漏洞。
 - ●将光标悬停至漏洞,点击<**详情**>,可查看漏洞补丁详情。



WIN-2DMMMKTNP67-123.133.72.6, 10.20.30.200		
发现4个高危漏洞,需要立即修复。 已自动开启蓝屏修复功能,保证资产安全 已安装 已氯嗪 (1)		一號修复重新扫描
漏洞补丁描述	发布日期	补丁大小 状态
◇ □ 高危漏洞0/4		
2019-适用于 Windows 7 和 Windows Server 2008 R2 的 05 仅安全性质量更新(CVE-2019-0708) 修复 忽略	详情 2019-05-11	100.50MB 待修复
◎ 2019-适用于 Windows 7 和 Windows Server 2008 R2 的 09 安全更新(SHA256代码签名支持V3),	2019-09-23	53.27MB 待修复

9.3.1.1.3 修复终端漏洞

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Windows 系统漏洞",选择终端视角页签。

步骤 3. 勾选需要修复漏洞的终端(可勾选多个),点击<修复漏洞>。

扫	描漏詞 修复漏洞 停止修结	■ 与出						请输入关键字	Q 🖒 🏪 🔘
0	共 1 项,已选择 1 项 全选当页	反选当页							重置
	终端名称 ↓	操作系统 ♡	IP地址 0	高危漏洞 ≎	可选漏洞 ↓	上次扫描时间 🗘	上次修复时间(状态	操作项
	DESKTOP-80K43JQ	Windows 10 64-bit	192.168.27.143	0/0	0/0	2022-11-23 13:51:33		扫描完成	查看

步骤 4. 在弹出的对话框中点击<确定>,即可修复所勾选终端的漏洞。

提示			>
0	确定要修复漏洞吗?		
		取消	确定

对于正在修复漏洞的终端,用户可进行停止修复操作。

1) 勾选正在修复漏洞的终端(可勾选多个),点击<**停止修复**>。

扫描漏洞 修复漏洞 停	上修复导出					游	输入关键字	Q () III ()
① 共 1 项, 已选择 1 项 全选当	2 页 反选当页							重置
✓ 终端名称 ◊	操作系统 ↓	іРіші⊥ ≎	高危漏洞 ↓	可选漏洞 ♡	上次扫描时间 🗘	上次修复时间 🗘	状态	操作项
DESKTOP-80K43JQ	Windows 10 64-bit	192.168.27.143	0/0	0/0	2022-11-23 13:51:33		扫描完成	查看
2) 在弹	自出的对话框中。	点击< 确定 >,	即可停止的	多复漏洞	٦.			
	提示	7				×		
		确定要停止修	复漏洞吗?					
					取消 確認	È		

9.3.1.1.4 导出报告

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Windows 系统漏洞",选择终端视角页签。



步骤 3. 点击<导出>,即可将所有终端的漏洞报告导出至本地。

勾选终端(可勾选多个)点击<**导出**>,可将所选中的终端的漏洞扫描报告导出至本地。

终端视角 漏洞视角								
扫描漏洞 修复漏洞 停止	上修复 导出					请知	俞入关罐字	Q () III ()
① 共 1 项, 已选择 1 项 全选当页	页 反选当页							重置
✓ 终端名称 🗘	操作系统 ♡	IP地址 0	高危漏洞 ◊	可选漏洞 ♡	上次扫描时间 🗘	上次修复时间 ↓	状态	操作项
DESKTOP-80K43JQ	Windows 10 64-bit	192.168.27.1 <mark>4</mark> 3	0/0	0/0	2022-11-23 13:51:33		扫描完成	查看

9.3.1.1.5 重启终端

对于已进行漏洞修复的终端,需进行重启操作才能使漏洞修复生效。操作方法如下:

步骤 1. 以租户角色登录主机安全系统管理平台。

- 步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Windows 系统漏洞",选择终端视角页签。
- 步骤 3. 选择需要重启的终端,点击右侧**操作项**的"重启"图标,在弹出的对话框中点击<确定>,即可重启 该终端。

lows系	統漏洞 Linux系统漏洞 Wind	dows应用漏洞 Linux应用漏洞							
终端视	角漏洞视角								
	描漏洞 修复漏洞 停止修复	导出					请输入关键字		Q () III ()
	终端名称 🗘	操作系统 🗘	IP地址 🗘	高危漏洞 🗘	可选漏洞♀	上次扫描时间 🗘	上次修复时间 🗘	状态	操作项
	LAPTOP-杨	Windows 10 64-bit	10.11.37.142	2/2	0/0	2022-08-11 13:35:01		扫描完成	0
	C ZIONLAB-PC	Windows 7 Professional 64-bit	10.50.24.190	6/6	0/0	2022-06-21 16:26:40		扫描完成	
	🚱 ZIONLAB-PC	Windows 7 Professional 64-bit	10.50.24.190	5/5	0/0	2022-07-24 00:00:20		扫描完成	
	G WIN-4U90DL0SLL3	Windows Server 2016 Datace	10.20.176.1	2/2	0/0	2022-06-24 13:34:53		扫描完成	
	WIN-DE6R47QT6FD	Windows Server 2016 64-bit	10.103.8.98	1/1	0/0	2022-07-20 16:40:14	2022-07-20 16:09:59		
	❸ 苦苦	Windows 10 Enterprise Editio	10.20.28.207	1/1	0/0	2022-08-05 09:15:17		需要重启	0
	DESKTOP-QV9C0KN	Windows 10 64-bit	10.11.32.44	0/0	0/0				

9.3.1.2 漏洞视角

9.3.1.2.1 修复终端漏洞

◆ 方式一: 单个修复

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Windows 系统漏洞",选择漏洞视角页签。 步骤 3. 进入漏洞列表页面,选择需要修复的漏洞,点击右侧操作项的"修复"图标。

终端视角	漏洞视角							
修复	导出				请输入关键字		Q 0	≣ ⊚
补丁	编号≎	漏洞名称 ◇	补丁大小	漏洞级别工	影响终端数 🗘	发布日期 💲	状态	操作项
•	KB5013945	2022-适用于 Windows 10 Version 1909 的 05 累积更新,适合基于 x64 的系统	563.35MB	高危	1/1	2022-05-10	未修复	Ø



步骤4.在弹出的对话框中点击<确定>,即可对漏洞进行修复。

	损			×	
		确定要修复漏洞吗?			
			取消	确定	
♦	方式二:批量修复				

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Windows 系统漏洞",选择漏洞视角页签。 步骤 3. 勾选需要修复的漏洞,点击列表上方的<修复>。

终端视角源	嗣洞视角							
修复	2 导出				请输入关键字		Q C	
◀共11项,	已选择1项	重置					全选当页	反选当页
■ 补丁编	号 ≎	漏洞名称 ♡	补丁大小	漏洞级别工	影响终端数 🗘	发布日期 🗘	状态	操作项
1 • KB5	5013945	2022-适用于 Windows 10 Version 1909 的 05 累积更新,适合基于 x64 的系统	563.35MB	高危	1/1	2022-05-10	未修复	Ø

步骤 4. 在弹出的对话框中点击<确定>,即可对漏洞进行批量修复。

提示	×
确定要修复漏洞吗?	
	取消 确定

9.3.1.2.2 导出报告

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Windows 系统漏洞",选择漏洞视角页签。

步骤 3. 点击<导出>,即可将所有 Windows 系统终端的漏洞报告导出至本地。

勾选终端(可勾选多个),点击<**导出**>,可将所勾选的终端的漏洞扫描报告导出至本地。

终端视角	角 漏洞视角							
修	复导出]			请输入关键字		Q 0	≣ ⊚
◀共1	11项,已选择1项	- 					全选当页	反选当页
	补丁编号 ♡	漏洞名称 🗘	补丁大小	漏洞级别下	影响终端数 🗘	发布日期 🖇	状态	操作项
~	KB5013945	2022-适用于 Windows 10 Version 1909 的 05 累积更新,适合基于 x64 的系统	563.35MB	高危	1/1	2022-05-10	未修复	Ø
	KB5003174	2021-适用于 Windows 10 Version 1803 的 05 累积更新,适合基于 x64 的系统	1.28GB	高危	1/1	2021-05-11	未修复	Ø
	• KB4474419	2019-适用于 Windows 7 和 Windows Server 2008 R2 的 09 安全更新(SHA256代码	53.27MB	高危	2/2	2019-09-23	未修复	Ø
	KB4012212	2017-适用于 Windows 7 和 Windows Server 2008 R2 的 03 仅安全质量更新(永恒之	33.18MB	高危	1/1	2017-03-28	未修复	Ø



9.3.2 Linux 系统漏洞

租户可对 Linux 系统漏洞进行扫描及查看漏洞详情操作。

◆ linux 系统漏洞、应用漏洞扫描结果基于 CVE 编号聚合。

9.3.2.1 终端视角

9.3.2.1.1 扫描终端漏洞

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Linux 系统漏洞",选择终端视角页签。

步骤 3. 勾选需要扫描的终端(可勾选多个),点击<开始扫描>。

Windows系统漏洞 Linux系	统漏洞 Windows应用漏洞	Linux应用漏洞						
终端视角 漏洞视角								
开始扫描 导出 2							请输入关键字	0 0 11 0
① 共 1 项, 已选择 1 项 全选	当页 反选当页							重置
✓ 终端名称 🗘	操作系统 ♡	IP地址 0	致命漏洞 ≎	高危漏洞 ↓	中危漏洞 ♀	低危漏洞 🗘	上次扫描时间 🗘	状态
I localhost.localdom	CentOS Linux 7 (Core)	192.168.27.141	15	276	357	18	2022-11-23 14:43:04	扫描完成

步骤 4. 在弹出的对话框中点击<确定>,即可对终端进行漏洞扫描。

提示				×
0	确定要开始扫	描吗?		

9.3.2.1.2 导出报告

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险管理>漏洞管理>Linux 系统漏洞",选择终端视角页签。

步骤 3. 点击<导出>,即可将所有 Linux 系统终端的漏洞报告导出至本地。

勾选终端(可勾选多个),点击<**导出**>,可将所选中的终端漏洞报告导出至本地。

0	共1项,已选择1项全线	当页 反选当页							1
/	终端名称 ↓	操作系统 ♀	IP地址 ♡	致命漏洞♀	高危漏洞≎	中危漏洞 🗘	低危漏洞 ↓	上次扫描时间 ♡	状态
/	(a) localhost.localdom	CentOS Linux 7 (Core)	192.168.27.141	15	276	357	18	2022-11-23 14:43:04	扫描病



9.3.2.1.3 查看漏洞详情

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择 "风险评估>漏洞管理>Linux 系统漏洞",选择终端视角页签。选择需要查看的漏洞类型,点击漏洞数字。

	终端名称 ↓	操作系统 ≎	IP地址 ≎	致命漏洞 ≎	高危漏洞 ↓	中危漏洞 ≎	低危漏洞 ♡	上次扫描时间 🗘	状态
~	(a) localhost.localdom	CentOS Linux 7 (Core)	192.168.27.141	15	276	357	18	2022-11-23 14:43:04	扫描完成

步骤 3. 在弹出的对话框中查看漏洞详情(可切换漏洞等级),包括 CVE 编号、漏洞名称以及处理建议。

漏洞描述			×
	致命漏洞	高危漏洞 中危漏洞 低危漏洞	
CVE	漏洞名称	处理建议	产品
CVE-2019-14901	Linux kernel Marvell WiFi chip driver 缓中区错误漏洞(centos)(CVE-2019-14 901)	目前厂商已发布升级补丁以修复漏洞	
CVE-2019-16746	Linux kernel 缓冲区错误漏洞(centos) (CVE-2019-16746)	目前厂商已发布升级补丁以修复漏洞	
CVE-2019-17133	Linux kernel 缓冲区错误漏洞(centos) (CVE-2019-17133)	目前厂商暂未发布修复措施解决此安	
CVE-2019-14895	Linux kernel Marvell WiFi chip driver 缓冲区错误漏洞(centos)(CVE-2019-14 895)	目前厂商暂未发布修复措施解决此安	

关闭

9.3.2.2 漏洞视角

9.3.2.2.1 查看漏洞详情

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Linux 系统漏洞",选择漏洞视角页签。

步骤 3. 选择需要查看的漏洞,点击右侧操作项的<查看>。

V	Vindows系统漏洞 Lin	nux系统漏洞 Windows应用漏洞 Li	nux应用漏洞								
ŝ	终端视角 漏洞视角										
	导出						请输入关键字	Q ८ ⊞ ⊚			
	CVE 🗘	漏洞名称 ↓	影响终端数 🗘	漏洞级别工	应用名称	应用版本	操作系统版本	操作项			
	CVE-2019-10126	Linux kernel 缓冲区错误漏洞(CVE-20	1	致命	kernel	3.10.0-862.el7	centos-7	直看			
	CVE-2019-10126	Linux kernel 缓冲区错误漏洞(CVE-20	1	致命	kernel-tools	3.10.0-862.el7	centos-7	查看			
	CVE-2019-10126	Linux kernel 缓冲区错误漏洞(CVE-20	1	致命	kernel-tools-libs	3.10.0-862.el7	centos-7	查看			
	CVE-2019-14895	Linux kernel Marvell WiFi chip driver	1	致命	kernel	3.10.0-862.el7	centos-7	查看			



步骤 4. 在弹出的对话框中可查看漏洞详情,包括应用名称、应用版本、操作系统版本、CVE 编号、描述 及建议等。

详情	×
应用名称:	kernel
应用版本:	3.10.0-862.el7
操作系统版本:	centos-7
CVE:	CVE-2019-10126
描述:	Linux kernel是美国Linux基金会发布的开源操作系统Linux所使用的内核。Linux kernel中的drivers/net/wireless/marvell/mwifiex/ie.c文件 的'mwifiex_uap_parse_tail_ies'函数存在基于堆的缓冲区溢出漏洞。攻击 者可利用该漏洞造成内存损坏或其他危害。
建议:	目前厂商暂未发布修复措施解决此安全问题,建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法:https://www.kernel.org/

确定

9.3.2.2.2 导出漏洞报告

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Linux 系统漏洞",选择漏洞视角页签。

步骤 3. 点击<导出>,即可将所有 Linux 系统终端的漏洞报告导出至本地。

勾选终端(可勾选多个),点击<导出>,可将所选择的漏洞报告导出至本地。

Wi	ndows系统漏洞 Lir	nux系统漏洞 Windows应用漏洞	Linux应用漏洞						
终	端视角 漏洞视角								
Ę	≩出						请输入关键字	QO	
0	共 666 项, 已选择 11	顷 全选当页 反选当页							重置
	CVE \$	漏洞名称 🗘	影响终端数 🗘	漏洞级别工	应用名称	应用版本	操作系统版本		操作项
~	CVE-2019-10126	Linux kernel 缓冲区错误漏洞(1	致命	kernel	3.10.0-862.el7	centos-7		查看

9.3.3 Windows 应用漏洞

租户可对 Windows 应用系统漏洞进行扫描、查看扫描结果、导出扫描结果操作。

9.3.3.1 终端视角

9.3.3.1.1 扫描漏洞

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Windows 应用漏洞",选择终端视角页签。



步骤 3. 勾选需要扫描的终端(可勾选多个),点击<开始扫描>。

终端视	角 漏洞视角									
开始	2 約扫描 早出						请输入关键		QÓ	≣ ⊚
▲共	2项,已选择1项	重置							全选当页	反选当页
	终端名称 🗘	操作系统 🗘	IP地址 0	致命漏洞 🗘	高危漏洞 🗘	中危漏洞 🗘	低危漏洞 🗘	上次扫描时间 🗘	状	迏
	DESKTOP-80K	Windows 10 64-bit	192.168.27.143	0	0	0	0		未	扫描
	WIN-3QFTRUC	Windows 7 Ultimate Edition 6	10.11.32.44, 19	0	0	0	0		未	扫描
							# 2 条 20 条	而 < - 1	〉前往	1 页

步骤 4. 在弹出的对话框框中点击<确定>,即可对终端进行漏洞扫描。

×

9.3.3.1.2 导出漏洞报告

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>其他漏洞",选择终端视角页签。

步骤 3. 点击<导出>,即可将所有其他类型漏洞报告导出至本地。

勾选终端(可勾选多个),点击<**导出**>,可将所选择终端的漏洞报告导出至本地。

终端视角 漏洞视	角							
开始扫描	⊋出					请输入关键	\$	Q C III ()
◀共2项,已选择	1项 重置							全选当页 反选当页
■ 终端名称 💲	操作系统 💲	IP地址 \$	致命漏洞≎	高危漏洞 🗘	中危漏洞 🗘	低危漏洞 🗘	上次扫描时间 🗘	状态
DESKTO	P-80K Windows 10 64-bit	192.168.27.143	0	0	0	0		未扫描
🕒 WIN-3Q	FTRUC Windows 7 Ultimate Edition	6 10.11.32.44, 19	0	0	0	0		未扫描
						共2条 20条	顶 ~ 1	》 前往 1 页

9.3.3.2 漏洞视角

9.3.3.2.1 查看漏洞详情

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Windows应用漏洞",选择漏洞视角页签。

步骤 3. 选择需要查看的漏洞,点击右侧操作项中的<查看>。



经重	制制角	漏洞视角					
	导出				请输入关键字	Q	0 🗄 🎯
	CVE		漏洞名称	影响终端数 💲	漏洞级别了	漏洞类型了	操作项
	CVE-	2016-6662	Oracle MySQL 远程代码执行漏洞/提权漏洞(centos)(CVE-2016	1	致命	数据库漏洞	查看

步骤 4. 在弹出的对话框中查看漏洞详细信息,包括 CVE 编号、描述及建议。

详情	×
CVE:	CVE-2016-6662
描述:	Oracle MySQL是美国甲骨文(Oracle)公司的一套开源的关系数据库管理系
	统。该数据库系统具有性能高、成本低、可靠性好等特点。Oracle MySQL中的
	配置文件 (my.cnf) 存在远程代码执行漏洞。攻击者 (本地或远程) 可通过授权
	访问MySQL数据库(网络连接或类似phpMyAdmin的Web接口)或SQL注入方
	式,利用该漏洞向配置文件中注入恶意的数据库配置,导致以root权限执行任意
	代码,完全控制受影响的服务器。以下版本受到影响:Oracle MySQL 5.5.52及之
	前的版本, 5.6.x至5.6.33版本, 5.7.x至5.7.15版本; MariaDB 5.5.51之前的版
	本, 10.0.27之前的10.0.x版本, 10.1.17之前的10.1.x版本; Percona Server
	5.5.51-38.1之前的版本, 5.6.32-78.0之前的5.6.x版本, 5.7.14-7之前的5.7.x版
	本。
建议:	目前厂商已经发布了升级补丁以修复此安全问题,补丁获取链接:
	http://www.mysql.com/products/https://jira.mariadb.org/browse/MDEV-
	10465https://www.percona.com/blog/2016/09/12/percona-server-critical
	update-cve-2016-6662/

确定

9.3.3.2.2 导出漏洞报告

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Windows 应用漏洞",选择漏洞视角页签。

步骤 3. 点击<导出>,即可将所有其他类型漏洞报告导出至本地。

勾选终端(可勾选多个),点击<**导出**>,可将所选择终端的漏洞报告导出至本地。

资产视角 漏洞视角					
导出			请输入关键字		Q Č 🗄 🎯
CVE	漏洞名称	影响资产数 ≎	漏洞级别了	漏洞类型了	操作项
CVE-2015-0235	GNU glibc 基于堆的缓冲区溢出漏洞	2	致命	其他漏洞	查看
CVE-2016-2842	OpenSSL 安全漏洞 (CVE-2016-2842)	1	致命	其他漏洞	查看

9.3.4 Linux 应用漏洞

租户可对 Linux 应用系统漏洞进行扫描、查看扫描结果、导出扫描结果操作。


9.3.4.1 终端视角

9.3.4.1.1 扫描漏洞

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理>Linux 应用漏洞",选择终端视角页签。

步骤 3. 勾选需要扫描的终端(可勾选多个),点击<开始扫描>。

终端视角 漏洞视角								
2 开始扫描 导出						请输入关键:		Q () 🏭 🎯
▲共23项,已选择1项	重置						全	选当页 反选当页
■ 终端名称 \$	操作系统 🗘	IP地址 0	致命漏洞 ◊	高危漏洞 🗘	中危漏洞 🗘	低危漏洞 🗘	上次扫描时间 🗘	状态
Iocalhost.local	CentOS Linux 7 (Core)	10.50.24.182	0	2	0	0	2022-07-20 13:22:01	扫描完成

步骤 4. 在弹出的对话框框中点击<确定>,即可对终端进行漏洞扫描。

	×
取消	确定
	取消

9.3.4.1.2 导出漏洞报告

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理> Linux 应用漏洞",选择终端视角页签。

步骤 3. 点击<导出>,即可将所有其他类型漏洞报告导出至本地。

勾选终端(可勾选多个),点击<**导出**>,可将所选择终端的漏洞报告导出至本地。

终端视角 漏洞视角									
开始扫描 导出						请输入关键	97 7	QU	
◀共23项,已选择1项	重置							全选当页 历	反选当页
■ 终端名称 💲	操作系统 ◊	IP地址 0	致命漏洞♀	高危漏洞 🗘	中危漏洞 🗘	低危漏洞 🗘	上次扫描时间 🗘	状	态
ocalhost.local	CentOS Linux 7 (Core)	10.50.24.182	0	2	0	0	2022-07-20 13:22:01	扫	描完成

9.3.4.2 漏洞视角

9.3.4.2.1 查看漏洞详情

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>漏洞管理> Linux 应用漏洞",选择漏洞视角页签。

步骤 3. 选择需要查看的漏洞,点击右侧操作项中的<查看>。



终	端视角 漏洞视角									
Ę	学出						请输入关键	÷ C	20	
	CVE	漏洞名称	影响终端数 ≎	漏洞级别『	漏洞类型『	应用名称	应用版本	操作系统版本		操作项
	CVE-2015-9262	libXcursor 安全漏	1	致命	Unix/Linux漏洞	libdrm	2.4.83-2.el7	centos-7		查看

步骤 4. 在弹出的对话框中查看漏洞详细信息,包括应用名称、应用版本、操作系统版本、CVE 编号、描述及建议等。

详情		×
应用名称:	libdrm	
应用版本:	2.4.83-2.el7	
操作系统版本:	centos-7	
CVE:	CVE-2015-9262	
描述:	libXcursor是X.Org基金会运作的一个X窗口系统光标管理库。 1.1.15之前版本中的library.c文件的_XcursorThemeInherits存在 洞。远程攻击者可利用该漏洞造成拒绝服务或执行代码。	libXcursor 玍安全漏
建议:	目前厂商已发布升级补丁以修复漏洞,补丁获取链接: https://bugs.freedesktop.org/show_bug.cgi?id=90857	
		确定

9.3.4.2.2 导出漏洞报告

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择 "风险评估>漏洞管理> Linux 应用漏洞",选择漏洞视角页签。 步骤 3. 点击<导出>,即可将所有其他类型漏洞报告导出至本地。

勾选终端(可勾选多个),点击<**导出**>,可将所选择终端的漏洞报告导出至本地。

W	indows系统漏洞 Lir	ux系统漏洞 Window	vs应用漏洞 Linux应用	用漏洞						
终	端视角 漏洞视角									
1	≩ 出						请输入关键	字	QŮ	≣ ⊚
	CVE	漏洞名称	影响终端数 ◊	漏洞级别工	漏洞类型▼	应用名称	应用版本	操作系统版本		操作项
	CVE-2015-9262	libXcursor 安全漏	1	致命	Unix/Linux漏洞	libdrm	2.4.83-2.el7	centos-7		查看
	CVE-2018-1126	procps-ng 安全漏	1	致命	Unix/Linux漏洞	procps-ng	3.3.10-17.el7	centos-7		查看

9.4 终端体检

租户可通过对对应终端进行终端评估、勒索评估、挖矿评估或弱口令评估来及时发现终端中的潜在威胁。 同时可对各个分配的评估任务的执行结果进行相关的查看操作。

9.4.1 终端评估

步骤 1. 以租户角色登录主机安全系统管理平台。



步骤 2. 在左侧导航栏选择"风险评估>终端体检",勾选需要评估的终端(可勾选多个),点击<终端评估>。

刷	新列表终端评估	勒索评估 2	挖矿评估	弱口令评估				请输入关键字	C	0		
0	共 3 项, 已选择 1 项	全选当页 反选当	颌								重置	
	终端名称 🕽	所属分组『	标签了	IP地址♀	终端得分 🗘	勒索风险 ≎	挖矿风险 🗘	弱口令数量 ♡	上次扫描时间 ♡	目	1描状态	
	DESKTOP-80K	PC组		192.168.27.143	970				2022-11-23 15:09:58	扫)描结束	

步骤 3. 在弹出的对话框中点击<确定>,即可对终端进行终端评估。

提示		×
1 确定进行经	冬端评估?	
	取消	确定

9.4.2 勒索评估

- 步骤1.以租户角色登录主机安全系统管理平台。
- 步骤 2. 在左侧导航栏选择 "风险评估>终端体检",勾选需要评估的终端(可勾选多个),点击<**勒索评** 估>。

刷新列	岐 终端评估	勒索评估	挖矿评估 2	弱口令评估				请输入关键字		Q () ≣ ⊚
0 共	3 项,已选择1项:	全选当页 反选制	当页								重置
.	冬端名称 ↓	所属分组了	标签了	IP地址 ≎	终端得分 🗘	勒索风险 ≎	挖矿风险 🗘	弱□令数量≎	上次扫描时间 🗘		扫描状态
1 0	DESKTOP-80K	PC组		192.168.27.143	970				2022-11-23 15:09:58		扫描结束

步骤 3. 在弹出框中点击<确定>,即可对该终端进行勒索评估。



9.4.3 挖矿评估

- 步骤1.以租户角色登录主机安全系统管理平台。
- 步骤 2. 在左侧导航栏选择"风险评估>终端体检",勾选需要评估的终端(可勾选多个),点击<挖矿评估>。

刷新列表 终端评估	勒索评估	挖矿评估	弱口令评估 2				请输入关键字	. (Q (٢
① 共 3 项, 已选择 1 项	全选当页 反选当	顷								重	置
■ 终端名称 🗘	所属分组『	标签『	IP地址 ≎	终端得分 ◊	勒索风险 ≎	挖矿风险 🗘	弱口令数量 ≎	上次扫描时间 🗘		扫描	伏态
1 CESKTOP-80K	PC组		192.168.27.143	970				2022-11-23 15:09:58		扫描	結束



步骤 3. 在弹出的对话框中点击<确定>,即可对该终端进行挖矿评估。

提示			×
0	确定进行挖矿评估?		
		取消	确定

9.4.4 弱口令评估

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>终端体检",勾选需要评估的终端(可勾选多个),点击<弱口令 评估>。

刷新列表 终端评估	勒索评估	挖矿评估	喝口令评估 2					È O	(℃ ≣ ⊚
① 共 3 项, 已选择 1 项	全选当页 反选制	顷							重置
■ 终端名称 ◇	所属分组下	标签了	IP地址 0	终端得分 ≎	勒索风险 🗘	挖矿风险 🗘	弱口令数量 ≎	上次扫描时间 🗘	扫描状态
DESKTOP-80K	PC组		192.168.27.143	970				2022-11-23 15:09:58	扫描结束
步骤 3. 在弹出框	中点击<	<确定>,	即可对终靖		1令评估。				
		提示	7				×		
		0	确定进行弱	口令评估?					

9.4.5 查看评估结果

步骤1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>终端体检",选择已进行评估的终端,点击终端得分、弱口令下的 数字或者勒索风险、挖矿风险下的评估等级,即可查看终端相关风险的详细评估报告。

取消

确定

刷新列表 终端评估	勒索评估 挖矿评					请输入关键字	Q	८ ≣ ⊚
终端名称 ≎	所属分组『标	签 IP地址 ≎	终端得分≎	勒索风险 ♡	挖矿风险 🗘	弱口令数量 🗘	上次扫描时间 🗘	扫描状态
DESKTOP-80K	PC组	192.168.27.143	970	低	低	0	2022-11-23 15:16:04	扫描结束
		弱口令				×		
	弱口令 账号: admin, 弱口令: 123456, 帐号状态: 正常,账号类型:本地账号							
▲ 弱口令扫描结果不展示 windows 类 guest 的空口令;								



◆ 标识本地账户和域账户。

9.5 基线检查

基线检查是指对终端操作系统、数据库、软件的配置进行安全检测,并提供检测结果说明和加固建议。系统支持对操作系统、中间件、网络设备、虚拟化设备和数据库五类终端进行基线核查。

租户可通过新增任务,批量执行等操作来对指定终端进行基于基线策略执行时间的基线检查。同时可对各 个基线检查任务进行结果查看、执行、编辑和删除操作。

9.5.1 新增任务

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>基线检查",点击<新增任务>。

新增任务批量执行	删除				请输入关键字	0, 0 = 0
任务名称 🗘	终端数	检查项	开始时间 ◊	结束时间 🗘	进度	操作项
信通院测试	1	37	2022-06-29 13:59:00	2022-06-29 14:04:16	扫描完成) 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
				共一	Ⅰ条 20条/页 ~ 《	1 》 前往 1 页

步骤 3. 在弹出的对话框中输入任务名称(不超过 30 字符)、选择检查终端、基线策略及执行时间,点击< 确定>即可生成基线检查任务。

*任务名称:	test	
*检查终端:	选择终端	
*基线策略:	等保二级 S2A1G2 / Linux	Ŷ
执行时间:	每月 1、31号 00:00:00	~

9.5.2 执行任务

◆ 方式一: 单个执行

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>基线检查"。



步骤 3. 选择需要执行的任务,点击右侧**操作**项的^论图标,在弹出的对话框中点击<确定>,即可执行该基 线检查任务。

新增任务批量执行删	除				请输入关键字	Q Ů 🖽 🎯
任务名称 ↓	终端数	检查项	开始时间 ↓	结束时间 ♡	进度	操作项
□ 1	1	44			未扫描	执行查看编辑删除

◆ 方式二:批量执行

步骤1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"风险评估>基线检查"。

步骤 3. 勾选需要执行的任务(可勾选多个),点击任务列表上方的<**批量执行**>,在弹出的对话框中点击< **确定**>,即可批量执行基线检查任务。

新增任务 批量执行	删除 2				请输入关键字	Q Ů 88 ()
① 共 1 项, 已选择 1 项 全	选当页 反选当页					軍置
☑ 任务名称 ≎	终端数	检查项	开始时间≎	结束时间≎	进度	操作项
1 1	1	44			未扫描	执行 查看 编辑 删除

9.5.3 相关操作

以租户角色登录主机安全系统管理平台,在左侧导航栏选择"风险评估>基线检查",可对基线检查任务进行以下操作:

- ◆ 点击操作项列中的"查看"图标,可查看基线检查任务的详情。
- ◆ 点击操作项列中的"编辑"图标,在弹出的对话框中编辑相关信息,可编辑基线检查任务。
- ◆ 勾选需要删除的基线检查任务(可勾选多个),点击列表上方的<删除>,在弹出的对话框中点击<
 确定>,可批量删除基线检查任务。

亲	增任务 批量执行 删除					请输入关键字	Q () H ()
0) 共 1 项, 已选择 1 项 全选当页	反选当页					重置
	任务名称 🗘	终端数	检查项	开始时间 ◊	结束时间♀	进度	操作项
~	1	1	44			未扫描	执行 查看 编辑 删除

9.6 定期巡检任务

租户可通过配置定期巡检任务完成定期检测,及时发现终端中的潜在威胁。同时可对需要定期批量执行的 检测任务进行新增、编辑和删除操作。

9.6.1 新增定期巡检任务

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"响应处置>定期巡检",点击<新增>。



新増				请输入关键字 Q C E ③
□ 名称 ⁽¹⁾	创建时间 🗘	上次巡检时间 🗇	备注 ♡	操作项
		暂无数据		
			共 0	条 20条/页 ~ 《 1 》 前往 1 页

步骤 3. 在新增定期巡检任务页面编辑相关信息,点击<确定>后即成功新增定期巡检任务。

\$

新增定期巡检任务		
通过 通过	記置定期巡检任务,可及时发现终端中的潜在威胁 定期巡检执行时间以管理中心时间为准	
*任务名称:	test	
*任务类别:	快速查杀 ×	~
* 选择终端:	DESKTOP-80K43JQ 新曾终端将会同步此任务	+
*执行时间:	每月 31号 00:00:00	~
备注:	诸输入	li
	取消 确定	

详细配置方法请参见下表。

参数	说明
任务名称	最长长度为 30 字符。
任务类别	 选择任务类别: ◆ 快速查杀:快速扫描终端的默认扫描路径,并依照配置的病毒扫描策略对病毒进行相关处理。 ◆ 全盘查杀:扫描终端所有文件,并依照配置的病毒扫描策略对病毒进行相关处理。 ◆ 网站后门查杀:查杀终端是否有网站的后门程序,并依照配置的网马扫描策略对其进行相关处理。 ◆ 弱口令检测:检测终端的弱口令并展示对应弱口令详情。 ◆ 漏洞扫描:扫描终端的系统漏洞并展示对应漏洞详情。
选择终端	点击一图标,选择要执行定期巡检任务的终端。
执行时间	定期巡检任务的执行时间,周期可为日、每周、每月,并需要设置具体的时间点。

9.6.2 编辑定期巡检任务

- 步骤 1. 以租户角色登录主机安全系统管理平台。
- 步骤 2. 在左侧导航栏选择 "响应处置>定期巡检",选择需要编辑的巡检任务,点击右侧操作项的"编辑" 图标。



新增删除				请输入关键字 Q U 器 ③
名称 🗘	创建时间 🗘	上次巡检时间 🗘	备注 ♡	操作项
test	2022-08-15 10:38:59			
			共 1	条 20条/页 ∨ く 1 > 前往 1 页

步骤 3. 在编辑定期巡检任务页面修改需要更改的任务信息,修改完成后点击<确定>即可更改成功。

通过 提示	配置定期巡检任务,可及时发现终端中的潜在威胁 :定期巡检执行时间以管理中心时间为准	
*任务名称:	test	
*任务类别:	快速查杀 ×	~
*选择终端:	DESKTOP-80K43JQ 新增终端将会同步此任务	
*执行时间:	每月 31号 00:00:00	~
备注:	请输入	4

9.6.3 删除定期巡检任务

◆ 对于已存在的定期巡检任务,点击右侧操作项的"删除"图标,在弹出的对话框中点击<确定>, 即可删除该巡检任务。

新增删除			请输入关键字	
				确定删除该条数据?
名称 ♡	创建时间 🗘	上次巡检时间 ≎	备注 ↓	取消 确定
1	2022-11-23 16:56:06			编辑删除
▲ 「二世夕人仁	夕 占土利丰卜士的。	山陵 、 大通山的社	送掘山占土 ~冲ウ 、	可対測於作々进行

◆ 勾选多个任务,点击列表上方的<**删除**>,在弹出的对话框中点击<**确定**>,可对巡检任务进行批量 删除操作。

新増 删除 2			请输入关键字	Q Ů 🎛 🎯
◎ 当前页已选择 1 项, 未选择 0 项	全选当页 反选当页			重置
✓ 名称 ↓	创建时间 🗘	上次巡检时间 ♀	备注 ♀	操作项
1	2022-11-23 16:56:06		-	编辑删除

9.7 弱口令检测

租户可通过配置对终端进行应用弱口令检测、主机弱口令检测、配置管理等操作,发现终端中的弱口令信息,同时可对应用弱口令、主机弱口令、配置管理等进行查看和编辑操作。

9.7.1 应用弱口令

步骤 1. 以租户角色登录主机安全系统管理平台。



步骤 2. 在左侧导航栏选择"响应处置>弱口令检测>应用弱口令",点击<立即检测>,即可对终端进行对应应用的弱口令进行检测和查看,包括 tomcat、weblogic、onvif、SIP 等应用。

应用弱口令	主机弱口令	配置管理	
₫	1 当前发现的弱口	令总数	tomcat
web服务应用			Tomcat最Apache软件基金会(Apache Software Foundation)的Jakarta项目中的一个核心项目,由Apache、Sun和其他一些公司及个人共同开发而成,运行时使用的端口为 "8080"。Tomcat是一个免费的开放源代码的Web应用服务器,属于轻量级应用服务器。如使用圆口令密码测会造成在Tomcat中所运行的服务都有篡改网页信息、网页数据泄漏等
Amender TCP 8080		0 💣	安住风殿。
weblogio	c	0 প	
多媒体应用			
onvif TCP 8000		0 ď	
SIP UDP/SSL 50	060/5061	0 🚭	立即检测
数据库应用			
BM db2 TCP/SSL 50	000/50000	0 🕈	
TCP/SSL 14	43/1443	0 🕈	
			最近检测时间: 2022-11-23 17:01:05,本应用并未发现酮口令, 您也可以再次检测

9.7.2 新增定期巡检任务

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"响应处置>弱口令检测>主机弱口令",选择对应主机,点击<立即检测>。即 可对选中主机进行主机弱口令检测,最终查看左方检测出的弱口令数量。

应用弱口令	主机弱口令	配置管理
た	1 受弱口令影响的主持	nto Q
Windows 192.168.27.1	10 64-bit	0 o *
Windows 10.24.8.192	10 Enterprise E	0 °
CentOS L 192.168.27.1	inux 7 (Core)	0 ď
Windows 10.24.10.136	11 64-bit	0 🖋
没有	与更多的数据啦~	

9.7.3 新增定期巡检任务

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"响应处置>弱口令检测>配置管理",点击<更新规则>,上传对应需要更新的 弱口令文件即可更新弱口令规则库。



应用弱口令 主机弱口令 配置管理

更新规则	弱口令规则总数 7438		內置規则总数 7438		自定义規则总数 0 済物人关键字 Q O 語 (の)
弱账号 ≎	弱口令 🗘	规则类型 ◊	针对应用 ≎	应用类别 ≎	最后更新时间↓↓
db2inst1	db2inst1	□ 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1	123	□ 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1	123123	□ 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1	123456	□ 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1	12345678	□ 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1		□ 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1	test	□ 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1	Admin123	□ 系统内置	db2	数据库应用	2022-08-10 09:27:15
			共 7438 条 < 👖	2 3 4 5	6 … 372 > 20条/页 > 前往 1 页



10入侵检测

业内首创提出"Attack Movie"概念,可对攻击过程像"放电影"一样进行回放,提供"叠加分析模式"和 "演变分析模式",令攻击过程及演变历史一目了然。

10.1 攻击矩阵

租户角色可在攻击矩阵页签查看所有攻击手段、攻击演示过程、攻击趋势及攻击总数等信息。

10.1.1 攻击热力图

步骤 1. 以租户角色登录主机安全系统管理平台, 在导航栏选择"入侵检测>攻击矩阵"进入攻击矩阵页面, 点击右方的"攻击热力图"按钮查看攻击热力图。

攻击总数						近3天 🗸 🕻	■ Q 搜索	
攻击趋势			The MITRE A	TT&CK® Matrix		1 1	x击热力图	
	初始访问⑦	执行⑦	持久化⑦	权限提升②	防御规避⑦	凭据访问②	发现⑦	横向和
	^{0/9} 2	0/12 0	0/19 0	0 0/13 0	0/40 0	0/15 0	0/29	0 0/9
	有效帐号	Windows管理规范	系统启动/登录初始化脚 本	系统启动/登录初始化脚 本	直接存取卷	操作系统凭掘转储	系统服务发现	
	通过可移动媒体复制	计划任务/作业	计划任务/作业	计划任务/作业	Rootkit	网络嗅探	应用程序窗口发现	
	外部远程服务	命令和脚本解释器	有效帐号	进程注入	混淆的文件或信息	输入捕捉	查询注册表	
	水坑攻击	软件部署工具	账户操纵	利用特权升级	伪装	爆破	系统网络配置发现	i
	利用面向公众的应用程序	原生API	外部远程服务	有效帐号	进程注入	多因子认证拦截	远程系统发现	
	供应链攻击	共享模块	创建账户	访问令牌操纵	Indicator Removal on Host	强制认证	系统所有者/用户发现	t
	Trusted Relationship	客户端命令执行漏洞利 用	Office应用程序启动	城策略修改	有效帐号	利用漏洞获取凭据	网络噢探	使用 据
	硬件附加	用户执行	浏览器扩展	创建或修改系统进程	修改注册表	窃取应用Access Token	网络服务扫描	

10.1.2 受攻击主机热力图

步骤 1. 以租户角色登录主机安全系统管理平台, 在导航栏选择"入侵检测>攻击矩阵"进入攻击矩阵页面, 点击右方的"受攻击主机热力图"按钮查看受攻击主机热力图。



	攻击总数	0	•										近3天 🗸 🕻	Q	搜索		
势							The MITRE /	AT	T&CK® Matrix					受攻:	由主机热力图	Ξ	TN
		初始证	间⑦	执行②			持久化②	-	权限提升②	防	御规避②	凭据	方间②	发现	0	-	横向
		0/9	2	0 0/12		0	0/19	0	0/13 0	0	0/40 0	0/15	0	0/29		0	0/9
			有效帐号	v	Vindows管理规范		系统启动/登录初始化脚本		系统启动/登录初始化脚 本		直接存取卷		操作系统凭据转储		系统服务发现		
		通	过可移动媒体复制		计划任务/作业		计划任务/作业		计划任务/作业		Rootkit		网络嗅探		应用程序窗口发现		
			外部远程服务	1	命令和脚本解释器		有效帐号		进程注入		混淆的文件或信息		输入捕捉		查询注册表		
			水坑攻击		软件部署工具		账户操纵		利用特权升级		伪装		爆破	b .	系统网络配置发现		ì
		利用配 序	面向公众的应用程		原生API		外部远程服务		有效帐号		进程注入		多因子认证拦截		远程系统发现		
			供应链攻击		共享模块		创建账户		访问令牌操纵	li H	Indicator Removal on Host		强制认证	系	统所有者/用户发现		ţ
		Tr	rusted Relationship	客户端 用	命令执行漏洞利		Office应用程序启动		城策骼修改		有效帐号		利用漏洞获取凭据		网络嗅探		使用 据
			硬件附加		用户执行		浏览器扩展		创建或修改系统进程		修改注册表	窃	取应用Access Token		网络服务扫描		•

10.1.3 受攻击工作组热力图

步骤 1. 以租户角色登录主机安全系统管理平台, 在导航栏选择 **"入侵检测>攻击矩阵**" 进入**攻击矩阵**页面, 点击右方的 **"受攻击工作组热力图**" 按钮查看受攻击工作组热力图。

\bigcirc	攻击总数	0 0					近3天 🗸	· ■ Q 搜索	~
文击趋势				The MITRE A	ATT&CK® Matrix			受攻击工作组热力 @ 🛛 🖉 🔒	
		初始访问⑦	执行②	持久化⑦	权限提升②	防御规避②	凭据访问 ②	发现⑦	構向
		0/9	0 0/12	0 0/19	0 0/13	0 0/40	0 0/15	0 0/29	0 0/9
		有效帐号	Windows管理规范	系统启动/登录初始化脚 本	系统启动/登录初始化脚 本	直接存取卷	操作系统凭据转储	系统服务发现	远程
		通过可移动媒体复制	计划任务/作业	计划任务/作业	计划任务/作业	Rootkit	网络嗅探	应用程序窗口发现	软件
		外部远程服务	命令和脚本解释器	有效帐号	进程注入	混淆的文件或信息	输入捕捉	查询注册表	污染
		水坑攻击	软件部署工具	账户操纵	利用特权升级	伪装	爆破	系统网络配置发现	通过
		利用面向公众的应用程序	原生API	外部远程服务	有效帐号	进程注入	多因子认证拦截	远程系统发现	利用
		供应链攻击	共享模块	创建账户	访问令牌操纵	Indicator Removal on Host	强制认证	系统所有者/用户发现	内网
		Trusted Relationship	客户端命令执行漏洞利 用	Office应用程序启动	域策略修改	有效帐号	利用漏洞获取凭据	网络噢探	使用据
		硬件附加	用户执行	浏览器扩展	创建或修改系统进程	修改注册表	窃取应用Access Token	网络服务扫描	远程

上述三个按钮右方的"仅显示命中计数"和"中/英文版矩阵"可以根据用户需求按需调整。

10.2 入侵告警

租户角色可在入侵告警页签查看所有告警趋势、告警总数等告警信息。



10.2.1 入侵告警信息

步骤 1. 在左侧导航栏选择 "入侵检测>入侵告警",进入入侵告警页面。可以看到每条告警信息都会显示 当日发生几次原始事件。

160)	近1周 ~ 薗 〇 搜索 ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
	数	添加用户 当日发生 2 次
		可疑进程: C:\Windows\System32\net.exe
		受攻击主体: uwin7-SL Uvin7-SL
~		攻击描述: 在【2023-09-08 16:02:16】(1小时前),可疑进程【C\Windows\System32\net.exe】采取【持久化】攻击战术,利用【创 建账户.本地账户】攻击技术,对隶属于【SL】工作组的【WIN7-SL】发起了一次【添加用户】攻击
攻击技术 10) ~	
间用远程服务	112	
刘建账户	28	检测模型: 内置模型/SY000302添加用户
则建或修改系统进程	13	攻击技术:
ndicator Removal on	3	
查询注册表	1	
攻击战术 6	5 ~	TA0001 TA0002 TA0003 TA0004 TA0005 TA0006 TA0007 TA0008 TA0009 TA0010 TA0011 TA0040
黄向移动	113	T1136 001
寺久化	42	
2限提升	14	
方御规避	4	

步骤 2. 点击 3 按钮可以看到具体原始事件的相关信息。

A	160	近1周 v 菌 Q 搜索	
告警趋势	告警总数	TA0001 TA0002 TA0003 TA0004 TA0005 TA0006 TA0007 TA0008 TA0009 TA0010 TA0011 TA0040	
~		T1136 001	
攻击技术	10 ^		
利用远程服务	112	原始事件	
创建账户	28	O 2023-09-08 08:02:11 发生1次进程启动事件 ▶ ④ 客户端名称 EDR	
创建或修改系统进程	暒 13	O 2023-09-08 07:33:26 发生1次进程启动事件 Ba02803fcc7071cafcb3b209262874b41486d17e bdb395156f3ef31509935dfd	
Indicator Remova	Il on 3	④ 文件公司名称 Microsoft Corporation	
查询注册表	1	le 父进程路径 C:\Windows\System32\cmd.exe	
7/7	C	lib 进程文件描述 Net Command	
以面成小	112	· 巴 登录全局标识 7	
19月1日19240	115	④ 启动账户 Administrator	
持久化	42	© 原始文件名 net.exe	
权限提升	14	G 完整性级別 High	
防御规避	4	1-1-1. 2006.03.972 (111.6-5-1-)+ [7] 1	

步骤 3. 选择告警信息下方的 🛇 按钮,即可选择如何处理该告警信息。



			9				
A	127		2		今天 🗸 菌	Q 搜索	
告警趋势	告警总数	检测模型: 攻击技术:	内置模型/SY000582:使用ms17010				
攻击技术 利用远程服务	8 ^ 115	TA0001 TA0002	TA0003 TA0004 TA0005 TA0006	TA0007 TA0008 TA000	9 TA0010	TA0011 TA0040	
创建账户	6						
创建或修改系统进程	ł 3						
查询注册表	1	⊕ <u>&</u>					
远程服务	1	3					
攻击战术 横向移动	5 ^ 116	22分钟前 确认该告警 信任该告警 信日	1D 发现高危告警 (已确认)				
持久化	9	下下 你为未处理	CWE daw (Cotor 20)				
■ 权限提升	3	可照 信任该模型	WIN-VF1K08RC2GK				
发现	1	文于:自足义信任模型 攻击; _{周辺} 。	4在【2023-09-08 15:12:10】(22分钟前),	可疑进程【C:\Windows\System32\	wuauclt.exe】采耳	双【横向移动】攻击战2	长, 利

10.2.2 入侵告警处理

若执行本操作,代表您认为本条告警不具备风险性,本条告警将被标记为"己确认"状态,未来发生相同告警仍会通知。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"入侵检测>入侵告警",进入入侵告警页面

步骤 3. 选择告警信息下方的 ^会 按钮,选择**确认该告警**,跳出"操作成功,告警状态已变更!"则确认该 告警成功。

			2
	A	127	今天 ★ 箇 Q 搜索 ∨
	告警趋势	告警总数	检测模型: 内置模型/SY000582:使用ms17010 攻击技术:
			TA0001 TA0002 TA0003 TA0004 TA0005 TA0006 TA0007 TA0008 TA0009 TA0010 TA0011 TA0040
	攻击技术	8 ^	
	利用远程服务	115	- T1210
	创建账户	6	
	创建或修改系统进	程 3	
1	查询注册表	1	
1	远程服务	1	3
	攻击战术	5 ~	22分钟间 确认该告警 若执行本操作,代表您认为 本条告警不具备风险性,本
	横向移动 116 持久化 9		□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
			一 你为木处理 会通知。 可疑 信任该模型 xe
	权限提升	3	受攻。自党以信任横刑
	发现	1	ロシスロビルエ 攻击 _{地型に}



10.2.2.1 信任该告警

若执行本操作,代表您认为本条告警不具备风险性,本条告警及未来发生相同告警均标记为"已信任"状态。

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"入侵检测>入侵告警",进入入侵告警页面

步骤 3. 选择告警信息下方的 G 按钮,选择**信任该告警**,跳出"操作成功,告警状态已变更!"则信任该告警成功。





1	127	5 今天 * 箇 Q 搜索 >
告警趋势	与警总数	检测模型: 内置模型/SY000582:使用ms17010 攻击技术:
攻击技术	8 ^	
利用远程服务 创建账户 创建或修改系统进程…	6	
查询注册表 远程服务	1	θ <u>Α</u>
攻击战术	5 ^	22分钟前 2023-09-08 15:12:10 发现高危告警 (已确认)
横向移动	116	使用ms17010 当日发生 3 次
持久化	9	可疑进程: C:\Windows\System32\wuauclt.exe
权限提升	3	受攻击主体: 📲 WIN-VF1K08RC2GK
发现	1	攻击描述: 在【2023-09-08 15:12:10】(22分钟前),可疑进程【C\\Windows\System32\wuauclt.exe】采取【横向移动】攻击战术,利

10.2.2.2 标为未处理

若执行本操作,代表您暂时无法确定本告警的风险性,本条告警将被标记为"未处理"状态。 步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"入侵检测>入侵告警",进入入侵告警页面

步骤 3. 选择告警信息下方的 ^会 按钮,选择**标为未处理**,跳出"操作成功,告警状态已变更!"则标为未 处理成功。





Â	127	5	今天 🗸 📾 🔍 搜索 🗸 🗸
告警趋势	告警忌数	检测模型: 内置模型/SY000582:使用ms17010 攻击技术:	I
	/	TA0001 TA0002 TA0003 TA0004 TA0005 TA0006 TA0007 TA0008 TA0009	9 TA0010 TA0011 TA0040
攻击技术	8 ^		
利用远程服务	115	- 11210	
创建账户	6		
创建或修改系统进程	3		
查询注册表	1	⊕ &	
远程服务	1	Ψ	
攻击战术	5 ^	● 22分钟前 2023-09-08 15:12:10 发现高危告警 (已确认)	
横向移动	116	使用ms17010 当日发生 3 次	
持久化 ■	9	可疑进程: C:\Windows\System32\wuauclt.exe	
权限提升	3	受攻击主体: 📲 WIN-VF1K08RC2GK	
发现	1	攻击描述: 在【2023-09-08 15:12:10】(22分钟前), 可疑进程【C:\Windows\System32\v	wuauclt.exe】采取【横向移动】攻击战术,利

10.2.2.3 信任该模型

若执行本操作,代表您信任该检测规则,该规则将添加至信任列表,该规则相关告警均标记为"已信 任"状态。如需重新启用可前往【检测规则】页面处理。

步骤1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择 "入侵检测>入侵告警",进入入侵告警页面

步骤 3. 选择告警信息下方的 G 按钮,选择**信任该模型**,跳出"操作成功,告警状态已变更!"则信任该模型成功。

		2
A	127	今天 ~ 閭 Q 搜索 ~ ~
上数构执	告警总数	ms17010】攻击
古喜起穷		检测模型: 内置模型/FY000243:使用ms17010 攻击技术:
攻击技术	8 ^	
利用远程服务	115	TA000 确认该告警 ⑦ 若执行本操作,代表您信任 TA0006 TA0007 TA0008 TA0009 TA0010 TA0011 TA0040
创建账户	6	该检测规则,该规则将添加 信任该告警 至信任列表,该规则相关告
创建或修改系统进程	呈 3	标为未处理 警均标记为"已信任"状态。 11210
查询注册表	1	信任该模型 规则】页面处理。
远程服务	1	自定义信任模型4
攻击战术	5 ^	
横向移动	116	3
持久化	9	● 22分钟前 2023-09-08 15:12:10 发现高危告警 (未处理)
权限提升	3	
发现	1	【使用ms1/010 当日发生 3 次



127				5	今天 🗸 ඕ	Q 搜索	
告警总数	检测模型 攻击技术:	: 内置模型/SY0005	82:使用ms17010]
/	TA0001	TA0002 TA0003 TA0004	TA0005 TA0006 TA00	007 TA0008 TA0009	TA0010	TA0011 TA0040	
攻击技术 8							
利用远程服务 1	5			T1210			
创建账户	6						
创建或修改系统进程	3						
查询注册表	1						
远程服务	1						
攻击战术 5	● 22分钟前 202	23-09-08 15:12:10 发现高危告警(已确认)				
横向移动 1	⁶ 使用ms	17010 当日发生 3 次					
持久化	9 可疑进程	C:\Windows\Syste	em32\wuauclt.exe				
权限提升	3 受攻击主	本: 載 WIN-VF1K08 R	C2GK				
▶ 发现	1 攻击描述	在【2023-09-08 1	15:12:10】(22分钟前),可疑进程	≣【C:\Windows\System32\wu	iaucit.exe】采取	【横向移动】攻击战术,利	

10.2.2.4 自定义信任模型

若执行本操作,则自动跳转到【模型】页面设置自定义信任模型。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择 "入侵检测>入侵告警",进入入侵告警页面。

步骤 3. 选择告警信息下方的 G 按钮,选择自定义信任模型,即自动跳转到【模型】页面设置自定义信任模型。

			2	
<u> </u>) 6 尚 教			今天 ∨ 箇 Q 搜索 ∨
告警趋势		检测模型: 攻击技术:	内置模型/SY000582-使用ms17010	
		TA0001 TA0002	TA0003 TA0004 TA0005 TA0006	TA0007 TA0008 TA0009 TA0010 TA0011 TA0040
攻击技术	8 ^			
利用远程服务	76			T1210
创建账户	8			
创建或修改系统进程	3			
查询注册表	1			
1 1远程服务	1	3		
		● 55分钟 商认该告警	⑦若执行本操作,则自动跳转	
攻击战术	5 ^	信任该告警	到【	
横冋移动	77	使用标为未处理		
持久化	11	可疑信任该模型	xe	
权限提升	3	受攻自定义信任構型		
发现	1	攻击海北,	4 エ (2023-05-00 13.12.10, 13.75),前),前	可疑进程【C:\Windows\System32\wuauclt.exe】采取【横向移动】攻击战术,利



步骤 4. 选择**主机类型**和命中的**事件类型**及相关条件参数(可配置多条件),具体**事件类型和参数**可以在入 侵检测页面查看,如下为例:

言任模型 / 新增信任模型	
/言仁措刑_2022_00_08	16:24:04
哈性候坐-2023-09-0 6	10.54.04
虽然 主机上发生的事件命中	P了 特定检测模型 >> SY000582 但该事件满足以下条件
Windows ~ 主材	1上发生的事件命中了 进程创建 ── 事件,且该事件 • 满足以下任何一个条件 ○ 满足以下所有条件
命令行参数	◇ 等于 · C:\Windows\NetworkDistribution\\svchost.exe ④ ○
那么我信任该事件	
最后	
是否开启策略:	
本模型适用主机:	全部主机
	取消 促在
	נו איי ביו איי
05 告警总数	今天 > 箇 0 搜索 > >
告警趋势	
\land	
/ \	
攻击技术 10 へ	Exel-co-co-co-co-co-co-co-co-co-co-co-co-co-
利用远程服务 76	○ 2023-09-07 05:32:33 发生1次进程启动事件 Ⅰ □●事件美型 进程启动
创建账户 8	O 2023-09-07 05:30:25 发生1次进程启动事件 10 相思夹型 T_HOST_PROCESS_CREATE_MSG 回版本 23.5.7.1
Indicator Removal on 3	O 2023-09-07 05:27:16 发生1次进程启动事件
创建或修改系统进程 3	回启动参数 C:\Windows\NetworkDistribution\\svchost.exe
却持我们流 2	O 2023-09-07 05:25:09 发生1次进程启动事件 日本市内市政政 日本市内市政政 日本市内市政政 G 进程PID 3180
攻击战术 6 へ	O 2023-09-07 05:22:16 发生1次进程启动事件 G 父进程全局唯一标识 1381104
個问杨切 77	
占ク 収 12	
持久化 13	● 1小时前 2023-09-08 15:12:10 发现高危告警 (已确认)
 持久化 13 防御规避 5 权限提升 5 	● 1小时前 2023-09-08 15:12:10 发现高危告警 (已确认)

步骤 5. 选择是否开启策略、本模型适用主机、策略名称、策略描述后,保存即可完成自定义信任模型配置。



模型 / 新地	曾信任模型	
⇒/〒+古田	1 2022 00 00 1	16.24.04
1百1土作吴尘	-2023-09-08 I	10:54:04
	叩マ1」参奴	
那么我们	言任该事件	
最后		
[是否开启策略:	
	本模型适用主机:	全部主机
	策略名称:	信任模型-2023-09-08 16:34:04
	策略描述:	请输入
l		
		取消 保存

10.3 检测规则

租户角色可在检测规则页签查看检测规则详情、信任列表、处置方式等信息。

10.3.1 检测规则

步骤 1. 以租户角色登录主机安全系统管理平台, 在导航栏选择"入侵检测>检测规则"进入检测规则页面, 查看对应检测规则详情, 如:初始访问、执行、权限维持、权限提升等。

检测规则 根据ATT&CK理i	2,对攻防对抗的各个阶段进行防护,实现攻防对抗360度防御	同信任列表	默认处置方式	~
0	初始访问 检测攻击者试题进入内部网络的行为。 初始访问技术包括鱼叉式网络钓鱼、利用面向公众的服务弱点、利用有效账户等。			
\$	执行 检测攻击者运行恶意代码的行为。 执行包含攻击者在本地或远程系统上运行恶意代码的技术,该技术通常与所有其他攻击阶段的技术相结合,以实现更广泛的目标,例如权限维持、探索网络、窃取数据等。			
0	权限维持 检测攻击者维持系统持久访问权限的行为。 权限维持包括攻击者在临时访问的基础上新增保持对系统持久访问的技术,避免因为系统重启、凭证变更、瀛洞修复等原因导致系统访问权限被中断。			
٥	权限提升 检测攻击者试图获得更高级别权限的行为。 权限提升包括攻击者用来在系统或网络上获得更高级别权限的技术。攻击者通常可以进入并探索具有非特权访问权限的网络,但需要更高的权限才能实现其目标。常见的方法是利用系统弱点、错	误配置和漏洞。		
\$	防御规度 检测攻击者试图避免被发现的行为。 防御规道包括攻击者在整个入侵过程中用来避免被发现的技术。用于防御规避的技术包括卸载/禁用安全软件或器满/加密数据和脚本等。攻击者还利用和滥用受信任的进程来隐藏和伪装他们的恶	意软件。		

10.3.2 信任列表

步骤 1. 以租户角色登录主机安全系统管理平台, 在导航栏选择"入侵检测>检测规则"进入检测规则页面,



点击"**信任列表**"按钮,即可查看对应添加信任列表的规则。注:信任列表需要通过"入侵检测>入侵告 警"对相关告警实施对应阻断等操作后才会显示需要操作的信任列表。

<mark>检测规则</mark> 根据ATT&CK理	2,对攻防对抗的各个阶段进行防护,实	信任列表	2		×	◎ 信任列表	默认处置方式	~
0	初始访问 检测攻击者试测进入内部网络的行为。 初始访问技术包括鱼叉式网络钓鱼、4	规则ID	规则名称	操作项		1		
s	执行 检测攻击者运行恶意代码的行为。 执行包含攻击者在本地或远程系统上							
0	权限维持 检测攻击者维持系统持久访问权限的并权限维持包括攻击者在临时访问的基础		共0条	< 1 > 20条页 > 前往	E 1 页			
9	权限提升 检测攻击者试图获得更高级别权限的行权限提升包括攻击者用来在系统或网络	ī为。 3上获得更高级别相	Q限的技术,攻击者通常可以进入并序梁具有非特	权访问权限的网络,但需要更高的权限才能实现	其目标。常见的方法是利用系统弱	l点、错误 配置和漏洞。		
\$	防御规避 检测攻击者试图避免被发现的行为。 防御规避包括攻击者在整个入侵过程中	中用来避免被发现。	的技术。用于防御规题的技术包括印刷/禁用安全和	2件或混淆/加密数最和關本等。攻击者还利用4	這用受信任的进程来隐藏和伪装他			

10.3.3 处置方式

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"入侵检测>检测规则"进入页面,点击"默 认处置方式"按钮,即可设置对应的处理方式,如:默认处置方式、仅记录、关闭等方式。

<mark>检测规则</mark> 根据ATT&CK理论	2,对攻防对抗的各个阶段进行防护,实现攻防对抗360度防御	☞ 信任列表	默认处置方式	^
0	初始访问 检测攻击者试题进入内部网络的行为。 初始访问技术包括鱼叉式网络钓鱼、利用面向公众的服务弱点、利用有效账户等。		默认处置方式 仅记录 关闭	
\$	执行 检测攻击者运行恶意代码的行为。 执行包含攻击者在不地或远程系统上运行恶意代码的技术,读技术通常与所有其他攻击阶段的技术相结合,以实现更广泛的目标,例如权限维持、探索网络、窃取数据等。			
8	权限维持 检测攻击者维持系统持久访问权限的行为。 权限维持包括攻击者在临时访问的基础上新增保持对系统持久访问的技术,避免因为系统重启、凭证变更、漏洞修复等原因导致系统访问权限被中断。			
Ø	权限提升 检测攻击者试图获得更高级别权限的行为。 权限提升包括攻击者用来在系统或网络上获得更高级别权限的技术。攻击者通常可以进入并探索具有非特权访问权限的网络,但需要更高的权限才能实现其目标。常见的方法是利用系统弱点、错误	吴配置和漏洞。		
÷	防御规避 检测攻击者试图谱免被发现的行为。 防御规避包括攻击者在整个入侵过程中用来避免被发现的技术,用于防御规避的技术包括卸载/禁用安全软件或混渐/加密数照和脚本等,攻击者还利用和滥用受信任的进程来隐藏和伪装他们的恶意	款件。		

10.4 模型

信任模型简单来看可以认为是与"检测模型"起相反的作用。即对某些符合条件的事件,将其定义为 是信任的,对这些事件并不生成告警。具体来说信任模型一般在以下场景使用,**场景1**:某个内置检测模 型有误报,可以只针对这个内置检测模型添加一条信任模型,以便排除这个内置检测模型的误报。场景2: 希望将符合某条件的事件始终定义为是可信的事件而在告警,在这种场景下,信任模型针对的不是某一个 检测模型,而是所有检测模型(包含自定义检测模型)。



自定义信任模型:是"信任模型"的一种,指的是在产品使用期间,由用户自定义添加的那些信任模型,模型的内容由用户自定义确定。

10.4.1 新增信任模型

步骤1. 以租户角色登录主机安全系统管理平台。

步骤 2. 选择【入侵检测】-【模型】-【新增信任模型】,选择任意任意检测规则或特定检测模型(特定检测模型需要填写对应事件 ID,事件 ID 可至入侵告警的 rule ID 查看)。

	4	
133 信警总数	10分钟前 2023-08-25 13:37:33 发现简称音音 (未处理)	近3天 🗸 🛅 🔍 漁業 🗸 🗸
告響趋势	可疑的PowerShell条数子串混送	
	 可菜類19⁻⁰ (· 交击技术
攻击技术 9 へ 利用远程服务 17 资源助培 6	取【执行】攻击战术、利用【PoweShell命令和固本解释器】攻击技术、 对隶属于【PC编】工作编的【MUAUTO-PC】发起了一次【可减的 PoweShell争数子弗思测】攻击	140001 740002 140003 140004 TA0005 140005 140007 140008 140009 TA0010 140011 140040
■ 命令和脚本解釋器 3	检测模型: 內置模型/SE000134可程的PowerShell参数子串混淆	
• 运程服务 2		
Windows管理规范 2	<u> </u>	
	原始事件	
攻击战术 3 へ 福向移动 19	O 2023-08-25 05:37:24 发生1次进程启动事件 ◎ HostName	MXIAUTO-PC
2/IB 6	@ AppIP	10.50.38.213
10 M	@ eventStr	进程启动
执行 2	₽ _b MsgType	T_HOST_PROCESS_CREATE_MSG
Diam'n 2	ତ version	23.5.7.1
高度 25	® rule_id	SE000134 2
	CommandLine	powershell -ep bypass .WinPwn.ps1
<u>新御</u> 0	@ Hashes	MD5=852d67a27e454bd389fa7f02a8cbe23f
中危 2	Processid	13540
可解世纪/约// 10	B ParentProcessGuid	27
CiWindows) Sustem 32) 10		
Callificational Contemp 201 6	● 37分钟前 2023-08-25 13:10:45 发现高音告答 (床外理)	
c:\vvindows\system32\ 0		
C:\Windows\System32\ 6	使用ms17010	
C:\Windows\System32\ 3		

步骤 3. 选择**主机类型**和命中的**事件类型**及相关条件参数(可配置多条件),具体**事件类型和参数**可以在入 侵检测页面查看,如下为例:

模型 / 新增值任模型					
f任模型-2023-08-25 14:00:28					
虽然 主机上发生的事件命中了 任章检测规则 ✓					
Windows > 主机上发生的事件命中了 逻辑创建 > 事件,且读事件 • 满足以下任何一个条件 · 满足以下所有条件					
参令行参数 ✓ 等于 ✓ powershell -ep bypass .WinPwn.ps1 ④ ④					
最后					
是否开启策略: 〇〇					
本模型透用主机: 全部主机					
策略各称: 個任權型-2023-08-25 14:00.28					
策略描述: 谢翰入					
取 164 亿 花子					



Û.	33 音響总数	24分钟前 2023-08-25 13:37:33 发现高信告管 (未处理)	近天・自 🤉 演奏 🗸
告告趋势 攻击技术 利用远程服务 波原功持 命令和脚本解释器 远程服务	9 ^ 17 6 8 3 2	可聞的PowerShell参数子非混済 可問題等: C.WindowiSystem32WindowsPowerShellv1.0/powershell.exe 変改進主法: 単 (MXAUT0-7c) 2023-06-25 1337-333 (24分時期)、可能进程 [C.WindowiSystem122WindowsPowerShellv1.0] powershell ace 取 (形示) 致能法年、利用 (PowerShell参和学術開) 没指 対策量子 (PCIa) 工作細胞 (MXAUT0-PC) 送起了一次 (可能研 PowerShell参数子中思考) 改造 1111-1111-11111-11111-11111-11111-11111-1111	双曲技术: 2] 美 技术。 140001 140002 140003 140004 140005 140006 140007 140008 140009 140010 140010 140011 140040 1009 01
Windows管理総 攻击战术 構向等动 影响 执行 内陸等级 高浩 平危 可疑进程/软件	3 ~ 19 6 2 3 ~ 25 6 2 10 ~	2 原始事件 ② 2023-06-25 05:37:24 架生1次进程回动事件 ④ ApplP ④ exemtStr ④ MgSTpe ④ resentStr ④ MgSTpe ④ resentStr ④ MgSTpe ④ resentStr ④ Notice ④ Procesidi ④ Procesidi ④ Procesidi	MXLAUTO-PC 10:5038:213 世短短期 T_HOST_PROCESS_CREATE_MSG 23:57.1 SE00114 powerhell ep bipass_IWInPin.ps1 M05=85266727e454bd386fe/T0286cbe23f 11340 57

步骤 4. 选择是否开启策略、本模型适用主机、策略名称、策略描述后吗,保存即可完成信任模型配置。

信任模型 / 新增信任模型	宮任模型 / 新闻信任模型										
信任模型-2023-08-	25 14:02:57										
IB											
虽然 主机上发生的事件	命中了 任意检测规则>> 但该事件满足以下条件										
Windows 🗸	Windows ∨ 主机上发生的事件命中了 and p 再件,且该事件 ● 满足以下任何一个条件) 满足以下所有条件										
请选择字段	◆ 等于 > 満続人要匹配的内容										
TR (composition)											
那么 我信任该事件 最后											
定日开启策略											
本模型适用主	1: 全部主机										
策略名称:	偕任模型-2023-08-25 14:02:57										
策略描述:	诗论入										
	戰法 做存										

10.4.2 查看信任模型

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 选择【入侵检测】-【模型】可查看、编辑、删除已经配置的信任模型;模型列表中,展示模型名称、模型内容、应用范围、最后修改时间、修改人、操作项。



+ 新增信任模型 〇 禁用模型 / 启用模	2 - 869-0272			请输入关键字	Q	0 📰 💿
模型名称 ↓	模型内容	应用范围	最后修改时间	修改人	操作项	
hsc	虽然主机上发生的事件命中了检测模型(任意规则)但该事件却满足条件[]那么信任该事件	centos5.6-x64-2.6.18-238	2023-08-24 16:05:48	autotest	(二) 直看	编辑 删除
zhj	虽然主机上发生的事件命中了检测模型[SE001095]但该事件却满足条件[]那么 信任该事件	LAPTOP-FP3DRB7A等1台终	2023-08-24 15:03:34	autotest		编辑删除
信任模型-2023-08-25 10:39:49	虽然主机上发生的事件命中了检测模型[:信任模型-2023-08-25 10]但该事件却满足条件[]那么 信任该	localhost.localdomain等25	2023-08-25 10:40:09	autotest	查看	编辑删除
celue	虽然主机上发生的事件命中了检测模型[任意规则]但该事件却满足条件[]那么 信任该事件	localhost.localdomain等1台	2023-08-25 10:56:41	autotest		编辑删除
xin1	虽然主机上发生的事件命中了检测模型(任意规则)但该事件却满足条件[]那么信任该事件	localhost.localdomain等26	2023-08-25 13:36:08	autotest	● 直督	编辑 删除

步骤 3. 打开关闭开关或者勾选模型来控制的信任模型的启用或者禁用。

	L					
+新增信任機型 〇 菜用模型 / 启用模型	2 - 服除模型			请输入关键字	QO	
模型名称 ↓	模型内容	应用范围	最后修改时间	修改人	操作项	
hsc	虽然主机上发生的事件命中了检测模型(任意规则)但该事件却满足条件()那么信任该事件	centos5.6-x64-2.6.18-238等	2023-08-24 16:05:48	autotest	① 查看	编辑删除
zhj	虽然主机上发生的事件命中了检测模型[SE001095]但该事件却满足条件[]那么 信任该事件	LAPTOP-FP3DRB7A等1台终	2023-08-24 15:03:34	autotest	(二) 直看	编辑删除
信任模型-2023-08-25 10:39:49	最然主机上发生的事件命中了检测模型[: 信任模型-2023-08-25 10]但该事件却满足条件[]那么 信任该	localhost.localdomain等25	2023-08-25 10:40:09	autotest	查看	编辑删除
celue	虽然主机上发生的事件命中了检测模型(任意规则)但该事件却满足条件()那么 信任该事件	localhost.localdomain等1台	2023-08-25 10:56:41	autotest	① 查看	编辑删除
xin1	虽然主机上发生的事件命中了检测模型【任意规则】但该事件却满足条件[I那么信任该事件	localhost.localdomain等26	2023-08-25 13:36:08	autotest	① 查看	编辑删除

+ 新増信任模型 🛇 禁用模型 🗸 启用模	型 — 例9中4頁型			请输入关键字	Q C B# 0
● 共 5 頃,已选择 1 项 全选当页 反选当页	Ā				重要
■ 模型名称 0	模型内容	应用范围	最后修改时间	修改人	操作项
hsc	虽然主机上发生的事件命中了检测模型(任意规则)但该事件却满足条件[]那么 信任该事件	centos5.6-x64-2.6.18-238等	2023-08-24 16:05:48	autotest	○ 查看编辑 删除
zhj	虽然主机上发生的事件命中了检测模型[SE001095]但该事件却满足条件[]那么 信任该事件	LAPTOP-FP3DRB7A等1台终	2023-08-24 15:03:34	autotest	○ 查看 编辑 删除



11 威胁情报

11.1 智能鉴定

租户角色可在**智能鉴定**页签通过 IP、域名、文件 Hash、漏洞编号在线搜索相关威胁信息;支持对 APT、木马、病毒、蠕虫、后门、勒索、挖矿、僵尸网络、漏洞利用等 10 余种不同类型的威胁进行离线鉴定。。

智能鉴定			城名、IP、文件Hash、漏洞编号 Q 在线线	家	今日 本周 本月
支持对APT、木马、柄毒、蠕虫、后()、勤要、挖矿、(■尸闷斑、漏洞利用等10余种不同类型的威胁进行高线鉴定。Q				_
			IP Manage Andrea	经满 点形 点形 一	-
129 0	30827 0		22086 0	0	
				请施入关键字	Q () 11 ()
终端名称	IP地址 🗘	鉴定内容	威胁类型了 告警信息	威胁等级	〒 时间 ℃
				共0条 < 🚺	> 20条质 > 前往 1 页

11.2 沙箱分析

管理平台联网时,支持对文件进行在线沙箱、多引擎、情报分析,可在线预览分析结果并支持报告下载。

沙箱分管理平	7m2701 理平白鲜刚时,支持对文件进行在此分离、参引集、情报分析,可在线预洗分析结果并支持报告下载。											
上作	5文件 删除记录						清榆入关键字			Q (2)		
	文件名称	文件类型	MD5	威胁等级『	处理状态™	文件上传时间♀	检测完成时间 🗘	操作项				
	CW.eXe	eXe	60ca507ef4ba7dbbb7ef6e	· 商商 •	检测完成	2023-06-21 14:04:12	2023-06-21 14:06:00	在线预览	下载	删除		
	loginx789.jsp	jsp	930cd4dd1052d073eedfb	● 安全	检测完成	2023-06-21 12:34:46	2023-06-21 12:37:00	在线预览	下载	删除		
	license.lic	lic	a996cc13aadd90ef559751	● 安全	检测完成	2023-06-13 17:00:58	2023-06-13 17:02:01	在线预览	下载	删除		
	1KEY_HD.rar	rar	9396f300094d4ec5304d9e	• 高危	检测完成	2023-05-15 00:13:04	2023-05-15 00:15:04	在线预览	下载	删除		
	文件头.png	png	6455271ad6cf31e625a8d0	●未知	检测异常	2023-05-06 11:14:28	2023-05-06 11:30:00	在线预览	下载	删除		
	2.php	php	587cd9d885339814126cae	●安全	检测完成	2023-05-06 11:04:27	2023-05-06 11:06:00	在线预览	下载	删除		
	1.php	php	97b611ece9ae822bee8a04	• 未知	检测异常	2023-05-06 10:44:24	2023-05-06 11:00:00	在线预览	下载	删除		

共7条 < 1 > 20祭/页 > 前往 1 页



12 发布端管理

租户可通过配置发布策略,将发布目录下的文件同步到网站目录。

豪 发布端管理为附加功能,需要单独购买许可(模块型号 WPT-EE-ALL)才能使用此功能。

仅租户角色具有发布端管理权限。

12.1 管理发布端

租户可在此页面进行发布端新增、升级、卸载、编辑、查看、启用、修改标签、解除绑定等操作。

12.1.1 新增发布端

12.1.1.1 新增 Windows 系统发布端

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"**发布端管理**",进入**发布端管理**页面。点 击<**新增**>。

亲	f增 刷新列表	卸載	修改标签解除绑定					0 = 0
	发布端名称	标签了	IP地址	操作系统	最后在线时间	发布服务状态	版本号	操作项
	OESKTOP-8JKE	DB	10.106.15.120	Windows 10 Profes sional 64-bit	2022-06-10 10:34:3 1	开启	2.0.17.10	
	CUNCUN		10.20.18.40	Windows 10 64-bit	2022-03-04 17:36:3	-	2.0.17.7	

步骤 2. 在弹出的对话框的 Windows 系统区域进行 Windows 系统发布端的离线安装。

- ◆ 方式一:点击离线安装的<下载>,下载客户端安装包,以管理员权限将安装包拷贝到终端服务器
 上,双击安装程序,执行安装。
- ◆ 方式二:点击离线安装的<复制>,复制客户端安装包下载链接。以管理员权限登录终端服务器, 在浏览器地址栏中粘贴客户端安装包下载链接,即可下载安装包。下载完成后双击安装程序,执行安装。

新增发布端



Windows系统

Windows XP SP3 / Windows Vista / Windows 7 / Windows 8、8.1 / Windows 10 Windows Server 2003 SP2 / Windows Server 2008、2008R2 / Windows Server 2012、2012R2 / Windows Server 2016 / Windows Server 2019

 离线安装:下载安装包,拷贝到主机上进行安装。

 https://10.20.178.151/service/file/download2?name=edr_do

 wnload/windows/test/push/10.20.178.151_10571/1/push_ins

 taller_10.20.178.151_LU661a78.exe

×



-Q-

客户端主机安装 Windows 系统发布端步骤与主机安全系统客户端安装步骤一致,详情可参考《主机安全及管理系统 V3.0R23C11 软件安装指南》。

12.1.1.2 新增 Linux 系统发布端

- 步骤 1. 以租户角色登录主机安全系统管理平台。在导航栏选择**"发布端管理"**,进入发布端列表页面,点 击<**新增**>。
- 步骤 2. 进行 Linux 系统发布端的离线安装或在线安装。
 - 离线安装

选择 CPU 架构以及操作系统位数,点击离线安装的<下载>,下载安装包,点击<复制>复制脚本命令。将软件包拷贝到服务器上进行解压,执行脚本命令进行安装即可。

A	离线安装	:选择CPU架构以及操作	系统位数下载安装包,拷!	贝到服务器上解压		
N		后扒打脚半进行安表。			1	2
	1	x86架构	~			9
.11		64位操作系统	~	2	下载	复制

● 在线安装

点击在线安装的<复制>,复制下载链接,在客户端上以管理员权限执行该命令进行安装。

D	离线安装:	选择CPU架构以及操作题 后执行脚本进行安装。	系统位数下载安装	麦包,拷贝到服务器上解	压	
		x86架构	~			
		64位操作系统	~		下载	复制
		tarno-same-permis nt_setup_3.0.1.4.x64.ta install_edr.sh	sionsno-sam ar.gz && chmo	e-owner -zxvf linux_ag d +x install_edr.sh &&	ge ./	
			「下命へ進行中」	±.		

12.1.2 修改发布端信息

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"发布端管理",进入发布端管理页面。



步骤 2. 选择需要修改的发布端,点击右侧**操作项**中的¹²图标。

新	增 刷新列	表卸電	R.	修改标签	解除绑定					0 = 0
	发布端名称	标签	7	IP地址		操作系统	最后在线时间	发布服务状态	版本号	操作项
				102.10	0.24.70	Windows 8.1 Enter	2022-06-21 14:57:1	× (7)	2014	
	algentwine			192.16	8.21.78	prise Edition 64-bit	1	天闭	3.0.1.4	Y O U

步骤 3. 在弹出的对话框中编辑发布端信息,点击<确定>即可成功修改发布端信息。

发布端名称:	aigentwin8
标签:	请选择
绑定状态:	■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
MINE VOUN	MARCHINEL STORAGE FAR 1 MARCHINELEN (Science and Librare
IP地址:	192.168.21.78
IP地址: 操作系统:	192.168.21.78 Windows 8.1 Enterprise Edition 64-bit

12.1.3 其他操作

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"发布端管理",进入发布端管理页面。 步骤 2. 租户可在此页面对发布端进行**刷新列表、卸载、修改标签、解除绑定、升级**等操作。

勾选多个发布端后,可对发布端进行批量卸载、修改标签及解除绑定操作。

亲	I	卸载	修改标签解除绑定					0 ⊞ ⊚
	发布端名称	标签了	IP地址	操作系统	最后在线时间	发布服务状态	版本号	操作项
	eigentwin8		192.168.21.78	Windows 8.1 Enterprise Edition 64-bit	2022-06-21 14:57:11	关闭	3.0.1.4	

12.2 配置发布信息

12.2.1 新增发布目录

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"发布端管理",进入发布端管理页面。



步骤 2. 点击右侧操作项中的 ◎ 图标,进入发布目录列表页面。

新增 刷新列表	卸载修改林	透 解除绑定					0 = 0
发布端名称	标签了	IP地址	操作系统	最后在线时间	发布服务状态	版本号	操作项
aigentwin8		192.168.21.78	Windows 8.1 Enterprise Edition 64-bit	2022-06-21 14:57:11	关闭	3.0.1.4	£
步骤 3. 点击 发	布服务器周	后的开关置	于开启状态,开展	自发布服务器	功能。		
☆ 发布端详情							
发布服务器 开启前请确认已安装刚发	布服务程序, 开启后	配置发布目录即可为	网站提供发布服务,发布地址:	192.168.21.78:10572	设 <u></u> 置		
新增							
名称		发布目录	发布	例外	是否启用		操作项
test		C:\Windows					
步骤 4. 点击<	新增 >。						
发布服务器 开启前请确认已安装刚发	布服务程序,开启后	配置发布目录即可为	网站提供发布服务,发布地址:	192.168.21.78:10572	设置		
新増							
2 名称		发布目录	发布	例外	是否启用		操作项
test		C:\Windows					

步骤 5. 在弹出的对话框中输入发布端需要发布的目录,并设置发布例外(发布例外下的目录文件不会被同步至网站目录),将**是否启用**开关置于开启状态,点击<确定>,即可成功新增发布目录。

*名称:	发布目录			
*发布目录:	C:\!AiGent			〕选择
发布例外:	C:\!AiGent\document.docx 发布例外的内容不会根据发布	配置发布到网站服务器	⑦ 送	择
是否启用:				



12.2.2 配置发布端策略

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"策略管理",进入策略管理页面。 步骤 2. 选择需要配置的模板,选择发布配置页签,将发布配置后的开关置于开启状态,点击<新增>。

時略管理	Θ	基础信息	系统防护	网络防护	渗透追踪	网页防篡改	女 Web应用院	防护 终端体检	2 发布配置	信任名单	桌面管控	事件响应
请输入策略名称	Q XX 2/2	发布配置 通过配置发行	已 开启 行策略,可	将发布目录了	下的文件同步	到网站目录。						8
田市安徽 已绑定 16 个终端	···1	④ 新增	>						请输入关键字			Q @
已绑定 0 个终端	…	日名	称	网站目录	发布端地 址	发布目录	同步删除	同步软链接	同步时机	策略状态	操作	项
11:991突0x 已绑定 0 个终端							暂无数	居				

步骤 3. 在弹出的对话框中输入发布规则后点击<确定>,即可完成发布策略配置。

新增规则		×
* 策略名称:	发布策略0730	
*发布目录:	C:	
同步删除:	是 ⑧ 否 选择是,发布时将删除网站目录下与发布目录不同的文件	
同步软链接:	○ 是 ● 否 选择是,发布时将同步文件原有的软链接	
同步时机:	 ✓ 事件同步 发布目录的内容变更会立即同步到网站服务器 ✓ 定时同步 600 秒 可输入范围10~3600秒 	
*网站目录:	/root	
同步例外:	多个例外文件以分号";"结尾。例如:同步目录例外为/网站目录/abc,则配置为abc	0
开启同步:		
	取消 确定	٦

规则参数说明如下表所示。

参数	说明
发布目录	选择发布服务器下相应发布目录。
同步删除	选择是否在发布时删除网站目录下与发布目录不同的文件。
同步软链接	选择是否在发布时同步文件原有的软链接。
同步时机	◆ 事件同步:发布目录下的文件只要发生改变,将立即同步更改过的文件 内容。



参数	说明
	◆ 定时同步:定时同步发布目录下的文件。
网站目录	选择需要同步的网站服务器下的目录,需写真实目录。

12.2.3 其他操作

进入发布端详情页面,租户可对发布端的 IP 及端口进行设置;选择需要操作的发布目录,可对发布目录进行编辑及删除操作。

支持批量发布目录及单条发布目录删除操作。

会 发布端详情				
发布服务器 开启前请确认已安装刚发布服务程	序,开启后配置发布目录即可为网站提供发	布服务,发布地址:192.168.21.78:1(572 设置	
新増				
名称	发布目录	发布例外	是否启用	操作项
test	C:\Windows			



13 高级威胁

仅租户角色具有查看高级威胁操作权限。

主机安全系统具备高级威胁防护功能,主要包括勒索防御、挖矿防御、渗透追踪和情报云脑。

13.1 设置勒索防御

内核级多维度防御引擎,及时发现并阻断勒索病毒,准确高效地实时保护用户关键数据。同时可通过 常见问题,了解有关勒索病毒的小知识。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"高级威胁>勒索防御"进入勒索防御页面。

步骤 3. 选择需要设置的引擎类型,点击引擎右侧区域的<去设置>,即可对该引擎进行设置。

详细配置方式可参考配置勤素防御。

勒索防御 内核级多维度防御引擎,及时发现并阻断勒索病毒,准确高效的实时保护用户关键数据。 常见问题 勒索诱饵防护引擎 去设置 1. 常见勒索软件的类型 针对勒索病毒遍历文件实施加密的特点,在终端关键目录下放置诱饵文件,当有勒索病毒尝试加密诱饵文件时及时中止进程,阻止勒索病毒的进一步加密和扩散 2 如何在事前防御勤索软件 3. 正常软件被勤素防御误报了, 怎么加白名单 勒索行为防护引擎 去设置 4. 什么情况下可以解密勒索软件加密的文件 通过分析常见的勒索软件样本,总结了样本具有的共性特征形成了引擎行为库,系统API级别分析,有效抵御未知勒索病毒, 文件保险柜 去设置 添加访问控制策略,对重要文件或目录进行访问权限控制,仅允许配置的例外进程操作,避免被勒索病毒破坏,

13.2 设置挖矿防御

通过进程启动防护机制,保护系统不被挖矿类恶意程序非法侵占资源。同时可通过常见问题,了解有 关挖矿病毒的小知识。

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"高级威胁>挖矿防御",进入挖矿防御页面。

步骤 3. 点击反挖矿引擎右侧区域的<去设置>,即可对该引擎进行设置。

详细配置方式可参考配置挖矿防御。



 技能が約

 通过进程启动防护机制,保护系统不被挖矿类恶意程序非法侵占资源。

 反挖矿引擎
 五设置

 通过分析程序行为及其它指标实时发现恶意挖矿程序,无特征,能实时发现未知恶意挖矿程序。

 上次

 工学软件被挖矿防御误报了,怎么加自名单?

 4.发现挖矿病毒的常规处理流程?

13.3 设置渗透追踪

根据 ATT&CK 理论,对攻防对抗的各个阶段进行防护,实现攻防对抗 360 度防御。同时可通过常见问题,了解渗透追踪的小知识。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"高级威胁>渗透追踪",进入渗透追踪页面。

步骤 3. 选择需要设置的引擎,点击引擎右侧区域的<**去设置**>,即可对该引擎进行设置。

详细配置方式可参考事件响应

- ◆ 功能:检测到终端触发对应规则后,终端会执行相应动作,防止对终端产生危害。
- ♦ 使用场景:适用于需要自定义修改配置策略模板事件响应场景。
- ◆ 使用限制:暂无。

操作步骤

步骤 1. 选择事件响应页签。

步骤 2. 将事件响应后的 🤍 图标置于开启状态,开启事件响应功能。

	已开启]]建满足指定条件,执行终端响应动作			
	新増			
	条件	动作	是否告警	操作项
步骤	3. 点击<新增>。 E 76 创建满足指定条件,执行终端响应动作			
	新增			
	条件	动作	是否告警	操作项

步骤 4. 在弹出的对话框中选择触发条件和执行动作,点击<确定>。



		×
新建		
	关闭	确定
	新建	新建

详细配置请参见下表。

参数	说明				
触发条件	包括文件变更、进程变更、网络连接、账号变更。				
执行动作	触发规则后终端执行的动作,包括结束进程、删除文件等。				

渗透追踪

根据ATT&CK理论,对攻防对抗的各个阶段进行防护,实现攻防对抗360度防御。

	单机扩展 针对本机的扩展行为进行监测,防止操权行为和信息泄露。	去设置	 常见问题 1. 了解单机扩展 2. 了解隧道搭建 3. 了解远程持久化
F	陳運作發建 识别渗透过程中的隧道代理,可阻断隧道代理搭建行为。 远控持久化	去设置	4. 了解内网探测 5. 正常软件被渗透追踪误报了,怎么加白名单?
•	对失跑后主机运控持久化行为进行检测,可阻断运控。 内网探测 对内网的恶意攻击行为进行识别,可阻断恶意探测行为。	去设置	
	痕迹清除 可对渗透的收尾阶段的数据清除行为进行识别和阻断。	去设置	

13.4 查看情报云脑

情报云脑支持对外联 IP、DNS 解析、可疑文件上传至云端进行鉴定,协助分析其是否存在威胁。

同时提供智能鉴定功能,在用户同意云端鉴定的前提下,上传可疑的外联 IP、DNS 解析、可疑文件至 云端进行鉴定,并可快速查看鉴定结果。

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"高级威胁>情报云脑"进入情报云脑页面。



步骤 3. 租户可对可疑域名、可疑外联 IP 或可疑文件进行鉴定。

在输入框中输入需要鉴定的域名、IP、邮箱、文件 Hash 或字符串,点击 Q 图标,即可对该 对象进行鉴定。

点击 夺图标,将文件上传至云端,即可对文件进行鉴定。

	情报云脑						
			青输入域名、IP、	邮箱、文件Hash、字符串			
			最近搜索:				
智能鉴定	已为您鉴定	123 项可疑事件,	其中 <mark>0</mark> 项严重,	0 项高危, 10 项中危, 2 项低危,	0 项可疑, 84 项安全		Ţ
时间 🗘		资产名称	IP地址	鉴定内容	关联路径		评级 ≎
2021-06-0	3 16:11:09	LAPTOP-杨	10.11.39.25	180.101.49.11	D:\Users\LENOVO\AppData\Local\Kingso	oft\WPS Office\11.1.0.10116\office6\wp	低危
2021-06-0	3 16:11:08	LAPTOP-杨	10.11.39.25	59.82.41.131			安全
2021-06-0	3 16:11:06	LAPTOP-杨	10.11.39.25	220.181.38.150			安全
2021-05-17	02:57:	localhost.loca	192.168.27.12	101.101.101.101			安全
2021-05-17	02:56:12	localhost.loca	192.168.27.12	101.102.103.104			安全
2021-05-16	3 22:32:	localhost.loca	192.168.27.12	104.244.78.231			未知
2021-05-10	6 18:30:21	localhost.loca	192.168.27.12	46.239.223.80			安全

步骤 4. 鉴定完毕后,租户可查看详细鉴定结果。

a8edf	12ee16b9173537ede3b0fbf5f11e6fc5e1ef0717dd833cf196b529d987f 🔤	0 问题反馈
安恒情排	安全	AND THE REPORT OF THE REPORT O
用户标签	· 新标志	
文件类型	exe 首次发现 2018-05-08 17:21:42	安全人
文件大小	112640字节 最近发现 2021-11-05 15:51:33	
VT检测	0/73	憲信府: ★ ★ ★ ★ ◇
分析时间	2021-11-30 10:08:37	
文件图标		
威胁情报	静态分析 动态分析 文件内容 同源样本 可视化分析	
- 100 100		
威胁情	授	
情报来	医 首次发现 导行发现 情况行奖	日不许旺 器信表



14 策略管理

策略是主机安全系统设备的基本功能,一般分为两部分:匹配条件和执行操作。主机安全系统会对根据匹配条件对流量进行检查,并对匹配的流量执行指定的操作。

仅租户具有策略管理操作权限。

租户可在**终端策略**页签以模板形式配置主机策略,包括基础信息、桌面管理、系统防护、终端体检、 主机审计、入侵防御、网页防篡改、网站管理、响应处置。

租户可在容器策略页签以保护容器镜像内的目录。

内置策略模板有通用模板、业务模板和审计模板,内置策略模板不可进行修改、删除。租户可自定义 默认模板,新安装的客户端将自动绑定到默认模板。

租户可对模板进行新增、编辑、查看已绑定终端、绑定新终端操作。同时可通过导出模板的方式对模 板进行备份,通过导入备份的模板恢复备份。

14.1 终端策略

14.1.1 新增策略

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择 "策略模板≻终端策略",将光标移至左上角 ④图标,在下拉框中选择"新 增"。



步骤 3. 在弹出的对话框中填写策略信息,点击<确定>,即可新增策略。


新增策略		×
* 策略继承	业务模板	~
* 策略名称	test	
备注		li
		取消 确定

14.1.2 编辑策略

操作步骤

步骤 1. 以租户角色登录主机安全系统管理平台。

- 步骤 2. 在左侧导航栏选择 "策略模板>终端策略",选择需要编辑的策略,点击该策略,进入编辑策 略页面。
- 步骤 3. 编辑需要修改的策略信息,点击<保存>即可成功修改该策略。

策略的详细配置方法请参见下文。

基础信息 系统	防护 网络防护	渗透追踪 网页防篡改 Web应用防护 终端体检 信任名单 桌面管控 事件响应
病毒防护勒索防御	病毒防护 针对网络中流行	的病毒、木马进行全面直杀。
挖矿防御 漏洞管理	扫描时机:	☑ 文件执行时 ☑ 文件修改时 ☑ 存储介质连接时 (Windows)
系统登录防护	多引擎设置:	この 默认引擎 高性能跨平台通用引擎
防暴力破解		
进程防护		开启后将占用200MB磁盘空间
文件访问监控	病毒免疫:	☑ 开启病毒免疫 (Windows)
	实时扫描:	● 自动处理(优先进行文件修复,修复失败后再隔离) 由用户自行选择 删除 针对实时发现病毒(文件执行、文件修改、存储介质连接时)的病毒处理方式
	智能鉴定:	☑ 开启智能鉴定 采集特征到中心进行二次鉴定,鉴定结果到高级威胁-情报云脑查看。

系统默认策略模板(内置模板)无法编辑,仅支持编辑自定义策略。

14.1.2.1 配置基础信息

- ♦ 功能:修改策略模板名称和相关备注信息。
- ♦ 使用场景:适用于需要修改策略模板名称和备注信息的场景。
- ◆ 使用限制:无。



操作步骤

步骤 1. 选择**基础信息**页签。

步骤 2. 配置策略名称和备注信息,点击<保存>。

*策略名称	测试			
备注	请输入备注			

详细配置请参见下表。

参数	说明
策略名称	策略名称为对应的配置模板。请输入 1~200 位字符(支持中文、数字、英 文、下横线、横线、"."、英文括号)。
备注	策略名称对应该的配置模板的备注介绍。不得超过 200 位字符。

14.1.2.2 配置终端管理

选择**终端管理**页签,可对终端设置管控。

基础信息	终端管理 系统网	5护 终端体格	佥 主机审计	十 入侵防	御 网页防器	[改 网站管理	响应处置			
客户端管理	针对客户端设置卸	针对客户端设置卸载密码、桌面快捷方式、升级方式及内容、下载限速								
运程协助 外设管控 移动存储管控 屏幕水印 系统性能监控	卸载密码 🔵 密码:	请输入	*							
	桌面快捷方式 Windows:	Linux:								
	升级设置 升级方式: 执行时间:	✓ 定时升级 每天 10:30:0	0 ~							
	升级内容: 错峰时间:	□ 软件版本✓ 随机延迟	✓ 病毒库 10	☑ 网马库	☑ 漏洞库	✓ 威胁情报库	☑ 弱口令库			
	下载设置 下载限速:	20	48	KB/S						

各配置项和说明如下表。

配置项	说明
客户端管理	针对客户端设置卸载密码、桌面快捷方式、升级方式及内容、下载限速。



配置项	说明
远程协助	针对不同的远程协助场景选择不同的策略,提升远程协助的安全性。
外设管理	按照设备类型以及接口类型对外接设备进行管控,重启系统后方可生效。
移动存储管理	移动存储设备的默认读写权限及使用审计设置,要对具体设备进行个性化设置 需要在 <u>查看终端详情</u> 中操作。
屏幕水印	在终端上设置屏幕水印,可以对通过屏幕拍照泄密数据进行溯源,锁定泄密者, 挽回损失。
隐形水印	通过安装溯源泄密服务,对通过屏幕拍照、屏幕截图泄密数据进行溯源,锁定 泄密者。
系统性能监控	实现监控网络流量、CPU、内存及磁盘的使用状况。

14.1.2.2.1 配置客户端管理

14.1.2.2.1.1 配置卸载密码

- ◆ 功能:设置客户端卸载密码,防止客户端意外卸载。
- ◆ 使用场景:适用于需要自定义修改配置策略模板卸载密码场景。
- ◆ 使用限制:暂无。

操作步骤

步骤 1. 选择客户端管理页签。

步骤 2. 点击卸载密码后的 💭 图标置于开启状态,开启卸载密码功能。

步骤 3. 输入密码。

十对客户端设置卸	印载密码、桌面快捷2	5式、升级方式)	及内容、	下载限速					
卸载密码 🔵 密码:	请输入	* *							
桌面快捷方式 Windows:	Linux:	0							
升级设置									
升级方式:	☑ 定时升级								
执行时间:	每天 10:30:00	~							
升级内容:	软件版本 🗸	病毒库 🔽	网马库	✓ 漏	同库 🔽	威胁情报库	~	弱口令库	
错峰时间:	✓ 随机延迟	10		分钟					
下载设置									
下载限速:	2048	KB/S	6						



14.1.2.2.1.2 配置桌面快捷方式

- ◆ 功能: 启用后将显示客户端的桌面图标并设置客户端随系统自启动。
- ♦ 使用场景:适用于需要自定义修改配置策略模板客户端管理场景。
- ◆ 使用限制:无。

步骤 1. 选择客户端管理页签。

步骤 2. 点击选择操作系统后的 图标置于开启/关闭状态。

针对客户端设置的	印载密码、桌面的	快捷方式、升级	方式及内容、	下载阳	速					
卸载密码 🔵	请输入	*								
桌面快捷方式 Windows:	Linux	:								
升级设置										
升级方式:	✓ 定时升级									
执行时间:	每天 10:30:0	00 ~								
升级内容:	□ 软件版本	✓ 病毒库	🗹 网马库	~	漏洞库	~	威胁情报库	~	弱口令库	
错峰时间:	✓ 随机延迟	1	0	分钟						
下载设置										
下载限速:	20	148	KB/S							

详细配置请参见下表。

参数	说明
Windows 桌面快捷方式	启用后将显示客户端的桌面图标并设置客户端随系统自启动,仅针对Windows终端生效。
Linux 桌面快捷方式	启用后将在应用程序中显示并设置客户端随系统自启动,仅针对 Linux 终端生效。

14.1.2.2.1.3 配置升级设置

- ◆ 功能:设置客户端定期升级,使客户端及规则库保持最新。
- ♦ 使用场景:适用于需要自定义修改升级场景。
- ◆ 使用限制:暂无。

步骤 1. 选择客户端管理页签。

步骤 2. 勾选定时升级。

步骤 3. 设置执行时间,选择升级内容,错峰时间。



针对客户端设置卸	印载密码、桌面快捷方	式、升级方式及	及内容、下载	限速			
卸载密码 👥 密码:	请输入	` ***					
桌面快捷方式 Windows:	Linux:	D					
升级设置							
升级方式:	✓ 定时升级						
执行时间:	每天 10:30:00	~					
升级内容:	软件版本 🔽	病毒库 🔽	网马库 🔽	漏洞库	✓ 威胁情报库	✓ 弱口令库	
错峰时间:	✓ 随机延迟	10	分钟				
下载设置							
下载限速:	2048	KB/S					

详细配置请参见下表。

配置项	说明
执行时间	可配置自动升级时间,支持按每日、每月、每周,并设置具体时间点。
升级内容	支持软件版本、病毒库、网马库、情报库、漏洞库和弱口令库。
	避免批量升级客户端引发升级风暴。将在设置的时间内给绑定的终端随机
	一个时间升级。

14.1.2.2.1.4 配置下载设置

- ◆ 功能:设置下载限速,保证客户网络环境运行稳定。
- ♦ 使用场景:适用于需要自定义修改升级场景。
- ◆ 使用限制:暂无。

步骤 1. 选择客户端管理页签。

步骤 2. 设置下载限速(单位 KB/S)。



针对客户端设置卸	叩载密码、桌面快捷方式、升级	方式及内容、	下载限速			
卸载密码 🔵						
密码:	请输入 😽					
桌面快捷方式						
Windows:	Linux:					
升级设置						
升级方式:	✓ 定时升级					
执行时间:	每天 10:30:00 ~					
升级内容:	软件版本 🔽 病毒库	🖌 网马库	✓ 漏洞店	₣ 🔽 威胁情报	3年 🔽 弱口令)	车
错峰时间:	✓ 随机延迟 10)	分钟			
下载设置						
下载限速:	2048	KB/S				

14.1.2.2.2 配置远程协助

- ◆ 功能:管理员可通过远程协助,处理终端及系统使用问题,提升管理员的工作效率。
- ♦ 使用场景:适用于需要自定义修改配置策略模板远程协助场景。
- ◆ 使用限制:无。

操作步骤

步骤1. 选择远程协助页签。

步骤 2. 配置用户响应。

针对不同的远程协助场景选择不同的策略,提升远程协助的安全性。

应答方式: 🔘 自动应答 💿 用户响应

◆ 自动答应:无需用户选择响应方式,用户无感知,管理员强制远程。

◆ 用户响应: 需用户选择响应方式, 用户允许后管理员接管远程。

14.1.2.2.3 配置外设管理

- ◆ 功能:按照设备类型以及接口类型对外接设备进行管控,重启终端操作系统后才能生效。
- ◆ 使用场景:适用于需要自定义修改配置策略模板外设管理场景。
- ◆ 使用限制:无。

操作步骤

步骤1. 选择外设管理页签。

步骤 2. 点击外设管控后的 🤍 图标置于开启状态,即可开启外设管控功能。



步骤 3. 选择目标设备,在权限控制列选择权限(禁用或放行)。

外设管控 📰 (已关闭) 按照设备类型以及接口类型对外接设备进	行管控,重启系统后方可生效。		C
按设备		按接口	
设备类型	权限控制	接口类型	权限控制
无线网卡	○ 禁用 ○ 放行	USB接口	○ 禁用 ● 放行
光驱	○ 禁用 ○ 放行	串口/并口	○ 禁用 ● 放行
软驱	○ 禁用 ○ 放行	1394控制器	○ 禁用 ● 放行
打印机	○ 禁用 ○ 放行	PCMCIA	○ 禁用 ● 放行
调制解调器	○ 禁用 ○ 放行		
红外设备	○ 禁用 ○ 放行		
蓝牙设备	○ 禁用 ○ 放行		
摄像头	○ 禁用 ○ 放行		
手机/数码设备	○ 禁用 ● 放行		

14.1.2.2.4 配置移动存储管理

- ◆ 功能:移动存储设备的默认读写权限及使用审计设置,利于对移动存储设备进行统一管控。
- ◆ 使用场景:适用于需要自定义修改配置策略模板移动存储设备场景。
- ◆ 使用限制:无。

选择移动存储管控页签,设置设备读写权限和设备使用审计。

移动存储设备的默认读写权限及使用审计设置,要对具体设备进行个性化设置需要在"终端管理->移动存储"中操作 设备读写权限:

读写
只读
禁用
设备使用审计:
使用审计
文件拷贝审计

详细配置请参见下表。

参数	说明
	◆ 读写: 赋予移动存储设备既可以写入也可以读取权限。
设备读写权限	◆ 只读: 赋予移动存储设备既仅可读取权限。
	◆ 禁用: 赋予移动存储设备不可以使用权限。
	◆ 使用审计:移动存储设备使用时对操作进行审计记录。
设备读写权限	◆ 文件拷贝审计: 移动存储设备执行文件拷贝对操作进行审计记
	录。

14.1.2.2.5 配置屏幕水印

◆ 功能:可以对通过屏幕拍照泄密数据进行溯源,锁定泄密者,挽回损失。

♦ 使用场景:适用于需要自定义修改配置策略模板屏幕水印场景。



◆ 使用限制:无。

操作步骤

步骤 1. 选择**屏幕水印**页签。

步骤 2. 点击屏幕水印后的 图标置于开启状态,即可开启屏幕水印功能。

步骤 3. 设置水印内容、自定义内容等信息,可配置水印信息。

幕水印 EF	自用油油管	数据进行溯源,	锁定泄	密者,挽	回损失。	
水印类型	全屏水印]		國水印		
	CE ZMAR ZMAR	a in the second				
水印内容	□ 终端	名称 🗌 IP		MAC 🔽	登录月	户
自定义内容	请输入	、自定义内容				
内容颜色	#00	OOFF				
字体大小	-	50	+			
倾斜度		30	+			
行间距mm	-	80	+			
块间距mm	-	10	+			

详细配置请参见下表。

配置项	说明
水印类型	终端支持九宫格展示局部区域水印或者全屏水印。
	终端显示如下水印内容:
	◆ 终端名称
	◆ IP
水印内容	◆ MAC
	◆ 登录用户
	◆ 系统时间
自定义内容	不超过 20 个字符。
内容颜色	终端显示水印内容的字体颜色。
字体大小	终端显示水印内容的字体大小。
倾斜度	终端显示水印内容的字体倾斜角度。
行间距 mm	终端显示水印内容每行之间的距离,单位是 mm。
块间距 mm	终端显示水印内容每块之间的距离,单位是 mm。



14.1.2.2.6 配置隐形水印

- ◆ 功能:设置屏幕隐形水印,增强屏幕的溯源效果和溯源能力。
- ◆ 使用场景:适用于需要自定义修改配置策略模板隐形水印功能的场景。
- ◆ 使用限制: 该功能需要单独购买屏幕溯源服务许可。

操作步骤

- 步骤 1. 选择隐形水印页签。
- 步骤 2. 将**隐形水印**后的开关置于开启状态,设置水印强度(取值范围 1~10,数字越大,屏幕水印强 度越高),设置是否启用**部分屏增强**功能。

隐形水印 设置屏幕隐刑	已开启 形水印,	,增强屏	幕的溯源效果	和溯源能力。		•	0
水印强度	-	1	+				
调节终端桌	面屏幕;	水印强度					
✓ 部分屏	增强						
勿选开户业	Thase	依洪屏营	\$\$\$*******	- 天影响屋首柳岩动里	左須士程度と提高部公屈取江市市家		

14.1.2.2.7 配置系统性能监控

- ◆ 功能:实现监控网络流量、CPU、内存及磁盘的使用状况。
- ◆ 使用场景:适用于需要自定义修改配置策略模板系统性能监控场景。
- ◆ 使用限制:无。

14.1.2.2.7.1 配置系统性能监控

用于监控系统性能监控

操作步骤

步骤1. 选择系统性能监控页签。

步骤 2. 点击系统性能监控后的 2 图标置于开启状态,即可开启系统性能监控。

已开启 实现监控网络流量	、CPU、内存及磁盘的使用状况。	
系统性能监控	Agent性能监控	

步骤 3. 选择系统性能监控 Tab。



已开启 实现监控网络流量	、CPU、内存及磁盘的使用状况。
系统性能监控	Agent性能监控
CPU监控:	
✓ 开启报警	CPU在 - 10 + 分钟内,持续阈值超过 - 80 + %时报警
开启熔断	CPU在 - 10 + 分钟内, 持续阈值超过 - 90 + %时客户端自动熔断
开启恢复	CPU在 - 10 + 分钟内,持续阈值低于 - 50 + %时客户端自动恢复
内存监控:	
☑ 开启报警	内存在 - 10 + 分钟内,持续阈值超过 - 80 + %时报警
开启熔断	内存在 - 10 + 分钟内,持续阈值超过 - 90 + %时客户端自动熔断
开启恢复	内存在 - 10 + 分钟内,持续阈值低于 - 50 + %时客户端自动恢复
网络IO监控:	
✓ 开启报警	网络IO监控在 - 10 + 分钟内,出网流量持续超过 - 4096 + KB/S时报警
✓ 开启报警	网络IO监控在 - 10 + 分钟内,入网流量持续超过 - 4096 + KB/S时报警
磁盘使用监控:	
☑ 开启报警	单个磁盘使用 - 90 + %时报警

- 步骤 4. 配置具体监控项(CPU 监控、内存监控、网络 IO 监控和磁盘使用监控,本文以 CPU 监控举例说明)。
 - 1) 勾选开启报警,设置告警阈值。
 - 2) 勾选开启熔断,设置熔断阈值。
 - 3) 勾选开启恢复,设置恢复阈值。

详细配置请参见下表。

参数	说明
开启报警	监控项匹配达到规则阈值进行日志记录。
开启熔断	监控项匹配达到规则阈值进行自动熔断,客户端不提供处理能力。
开启恢复	达到熔断条件后匹配达到预设规则将自动恢复客户端能力。

14.1.2.2.7.2 配置 Agent 性能监控

用于监控 Agent 性能监控

操作步骤

步骤1.选择系统性能监控页签。

步骤 2. 点击系统性能监控后的 图标置于开启状态,即可开启系统性能监控。



内存监控:

已开启 实现监控网络流量、CPU、内存及磁盘的使用状况。	
系统性能监控 Agent性能监控	
步骤 3. 选择 Agent 监控 Tab。	
已开启 实现监控网络流量、CPU、内存及磁盘的使用状况。	
系统性能监控 Agent性能监控	
CPU监控: 开启报警 CPU在 - 10 + 分钟内, 持续阈值超过 - 80 + %时报警	

步骤 4. 配置具体监控项(CPU 监控、内存监控,本文以 CPU 监控举例说明)。

 开启熔断 内存在 10
 + 分钟内,持续阈值超过 90
 + %时客户端自动熔断

 开启恢复 内存在 10
 + 分钟内,持续阈值低于 20
 + %时客户端自动熔断

 开启熔断
 CPU在 10
 +
 分钟内,持续阈值超过 90
 +
 %时客户端自动熔断

 开启恢复
 CPU在 10
 +
 分钟内,持续阈值低于 20
 +
 %时客户端自动熔断

开启报警 内存在 - 10 + 分钟内,持续阈值超过 - 80 + %时报警

- 1) 勾选开启报警,设置告警阈值。
- 2) 勾选开启熔断,设置熔断阈值。
- 3) 勾选开启恢复,设置恢复阈值。

详细配置请参见下表。

参数	说明
开启报警	监控项匹配达到规则阈值进行日志记录。
开启熔断	监控项匹配达到规则阈值进行自动熔断,客户端不提供处理能力。
开启恢复	达到熔断条件后匹配达到预设规则将自动恢复客户端能力。

14.1.2.3 配置系统防护

选择系统防护页签,可对终端设置防护。



基础信息	终端管理	系统防护 终端体检 主机审计 入侵防御 网页防篡改 网站管理 响应处置							
病毒防护 勒索防御 挖矿防御	针对网络中流行的病毒、木马进行全面宣杀。								
	扫描时机:	☑ 文件执行时 ☑ 文件修改时 ☑ 存储介质连接时 (Windows)							
漏洞管理	多引擎设置:	默认引擎							
		高性能跨平台通用引擎							
		(1) 深度扫描引擎							
		开启后将占用200MB磁盘空间							
	病毒免疫:	✓ 开启病毒免疫 (Windows)							
	实时扫描:	 自动处理(优先进行文件修复,修复失败后再隔离) 由用户自行选择 删除 							
		针对实时发现病毒(文件执行、文件修改、存储介质连接时)的病毒处理方式							
	智能鉴定:	✔ 开启智能鉴定							
		采集特征到中心进行二次鉴定,鉴定结果到威胁情报-智能鉴定查看。							

各配置项和说明如下表。

参数	说明
病毒防护	针对网络中流行的病毒、木马进行全面查杀。
勒索防御	内核级防御引擎,第一时间发现并阻断勒索病毒的加密行为,实时保护用户关键数据。
挖矿防御	通过进程启动防护机制,保护系统不被挖矿类恶意程序非法侵占资源。
漏洞管理	扫描并且修复系统漏洞,对操作系统进行加固。

14.1.2.3.1 配置病毒防护

- ◆ 功能:对网络中流行的病毒、木马进行全面查杀。
- ◆ 使用场景:适用于需要自定义修改配置策略模板病毒防护场景。
- ◆ 使用限制:无。

步骤 1. 选择病毒防护页签。

步骤 2. 配置扫描时机、多引擎设置、病毒免疫、实时扫描、智能鉴定参数。



详细配置请参见下表



参数	说明
扫描时机	默认全部勾选,用户可根据实际场景进行勾选。
	◆ 当文件被执行时,将会触发病毒防护功能。
	◆ 当文件被修改时,将会触发病毒防护功能。
	◆ 当存储介质被连接时(Windows),将会触发病毒防护功能。
	病毒防护时的引擎选项:
	◆ 默认引擎(高性能跨平台通用引擎,建议开启)。
多引擎设置	◆ 深度扫描引擎 (开启后将占用 200MB 磁盘空间,深度扫描引擎占用内存更多,但
	扫描速度更快(进行压缩包扫描时需要选择"深度扫描引擎")。
病毒免疫	用于检测非文件类病毒,仅适用于 Windosw 系统终端。
	发现病毒(文件执行、文件修改、存储介质连接时)后的处理方式:
实时扫描	◆ 自动处理(优先进行文件修复,修复失败后再隔离)。
	◆ 由用户自行选择。
	◆ 删除(删除病毒文件)。
智能鉴定	采集特征到威胁情报中心进行二次鉴定,鉴定结果请在查看情报云脑查看。

14.1.2.3.2 配置勒索防御

- ◆ 功能:内核级防御引擎,第一时间发现并阻断勒索病毒的加密行为,实时保护用户关键数据。
- ◆ 使用场景:适用于需要自定义修改配置策略模板勒索防护场景。
- ◆ 使用限制:无。

步骤 1. 选择勒索防御页签。

步骤 2. 配置生效方式。

勒索防御 === (用 <mark>原并记录</mark>) 内核级防御引擎,第一时间发现并阻断勘察病毒的加密行为,实时保护用户关键数据。	阻断并记录 ^
勤素诱饵防护引擎 针对勤業病毒適历文件实施加密的特点,在终端关键目录下放置诱饵文件,当有勒索病毒尝试加密诱饵文件时及时中止进程,阻止勤素病毒的进一步加密和扩散。	阻断并记录 仅记录
勤素行为防护引擎 通过分析常见的物素软件样本,总结了样本具有的共性特征形成了引擎行为库,系统API级别分析,有效抵御未知物素病毒。	
文件保险柜 添加访问控制策略,对重要文件进行访问权限控制,仅允许配置的例外进程操作,避免被勘索病毒破坏。	正在保护中 0 个 设置

步骤 3. 点击引擎后 图标将开关置于开启状态。



動素诱组防护引擎 针对物素病毒遍历文件实施加密的特点,在终端关键目录下放置诱饵文件,当有勒素病毒尝试加密诱饵文件时及时中止进程,阻止物素病毒的进一步加密和扩散。	
動棄行为防护引擎 通过分析常见的助素软件样本,总结了样本具有的共性特征形成了引擎行为库,系统API级别分析,有效抵御未知勘察病毒。	
文件保验柜 添加访问控制策略,对重要文件进行访问权限控制,仅允许配置的例外进程操作,避免被勘察病毒破坏。	正在保护中 0 个 设置

详细配置请参见下表。

参数	说明				
勒索诱饵防护引擎	针对勒索病毒遍历文件实施加密的特点,在终端关键目录下放置诱饵文件,当 有勒索病毒尝试加密诱饵文件时及时中止进程,阻止勒索病毒的进一步加密和 扩散。				
勒索行为防护引擎	通过分析常见的勒索软件样本,总结了样本具有的共性特征形成了引擎行为 库,系统 API 级别分析,有效抵御未知勒索病毒。				
文件保险柜	添加访问控制策略,对重要文件进行访问权限控制,仅允许配置的例外进程操 作,避免被勒索病毒破坏。				

添加文件保险柜的操作方法如下:

步骤 4. 点击<**设置**>。

動素诱组防护引擎 针对動素病毒遍历文件实施加密的特点,在终端关键目录下放置诱饵文件,当有動素病毒尝试加密诱饵文件时及时中止进程,阻止勘察病毒的进一步加密和扩散。	
勤素行为防护引擎 通过分析常见的物素软件样本、总结了样本具有的共性特征形成了引擎行为库,系统API级别分析,有效抵御未知物素病毒。	
文件保险柜 添加访问控制策略,对重要文件进行访问权限控制,仅允许配置的例外进程操作,避免被勘索病毒破坏。	正在保护中 0 个 设置

步骤 5. 弹出**文件保险柜**对话框,点击<**添加一行**>,输入保护项、例外程序后点击**<保存>**,再点击< 确定>,即可添加文件保险柜。

动态	何办程序	揭作而
K1/~4W	ידעברו ענק	
bin	cc.bin	保存 1



详细配置请参见下表。

参数	说明
保护项	支持模糊匹配,例如输入"bin",则只要文件名中包含"bin",该文件就会被加入文件保护柜。
例外程序	文件保险柜保护项中不需要保护的程序,且多个程序用";"间隔,例如输入 "agent.exe",则该程序就会被加入文件保护柜例外程序。

14.1.2.3.3 配置挖矿防御

- ◆ 功能:通过进程启动防护机制,保护系统不被挖矿类恶意程序非法侵占资源。
- ♦ 使用场景:适用于需要自定义修改配置策略模板挖矿防护场景。
- ◆ 使用限制:无。

操作步骤

步骤1. 选择挖矿防御页签。

步骤 2. 点击 🤍 图标将开关置于开启状态,即可开启反挖矿引擎。

通过进程启动防护机制,保护系统不被挖矿类恶意程序非法侵占资源。

反控矿引擎 通过分析程序行为及其它指标实时发现恶意挖矿程序,无特征,能实时发现未知恶意挖矿程序。



开启后可以通过分析程序行为及其它指标实时发现恶意挖矿程序,无特征,能实时发现未 知恶意挖矿程序。

14.1.2.3.4 配置漏洞管理

- ◆ 功能:扫描并且修复系统漏洞,对操作系统进行加固。
- ♦ 使用场景:适用于需要自定义修改配置策略模板漏洞管理场景。
- ◆ 使用限制:无。

操作步骤

步骤 1. 选择漏洞管理页签。

步骤 2. 根据实际情况勾选扫描后自动修复高危漏洞(Windows)或者修复完成后删除补丁文件 (Windows)。

扫描并且修复系统漏洞,对操作系统进行加固。

扫描后自动修复高危漏洞 (Windows)

◎ 修复完成后删除补丁文件(Windows)



14.1.2.3.5 配置弹窗拦截

- ◆ 功能:自动识别并拦截终端上的广告弹窗。
- ♦ 使用场景:适用于对终端有弹窗拦截需求的场景。
- ◆ 使用限制:无。

步骤 1. 选择弹窗拦截页签。

步骤 2. 配置恶意弹窗防护引擎按钮。

病毒防护 勒索防御	弹窗拦截 III 通过开启一键拦截,实现自动	的识别并拦截终端上的广告弹窗						
挖矿防御 漏洞管理 弹窗拦截	恶意弹窗防护引擎 自动识别并拦截终端上的广告弹	章窗,覆盖输入法、压缩类、杀毒软	件、视频播放、浏览器、游戏助手、	模拟器、装机下载、桌面管理、办	公学习、聊天通讯、图片编辑、网络	¥工具等 15 大类软件、100+ 款软件	,500+ 种广告弹窗。	
系统登录防护	● 輸入法	[<mark>↓</mark>] 压缩类	(十) 杀毒软件	▶ 视频播放	② 浏览器	游戏助手	@ 模拟器	
39 더 주 60 17	★ 装机下载	「」 桌面管理	曲 办公学习	🕐 聊天通讯	图片编辑	④ 网络工具		

详细配置请参见下表

参数	说明
	默认勾选,用户可根据自身需求进行勾选。
恶意弹窗防 护引擎	◆ 自动识别并拦截终端上的广告弹窗,覆盖输入法、压缩类、杀毒软件、视频播放、
	浏览器、游戏助手、模拟器、装机下载、桌面管理、办公学习、聊天通讯、图
	片编辑、网络工具等 15 大类软件、100+ 款软件,500+ 种广告弹窗。

14.1.2.3.6 配置系统登录防护

- ◆ 功能:对系统账户登录进行细粒度的精准访问控制。
- ♦ 使用场景:适用于需要自定义修改配置策略模板系统登录防护场景。
- ◆ 使用限制:无。

操作步骤

步骤 1. 选择系统登录防护页签。

步骤 2. 点击系统登录防护后的 🤍 图标置于开启状态,即可开启系统登录防护。

已开启 对系统账户登录进行细粒度的精准访问控制。					
新增					
登录账号 访问来源策略	时间策略	处理方式	状态	操作项	

步骤 3. 点击<新增>。



已开启 对系统账户登录进行细粒度的精准访问控制。				
新埔				
登录账号 访问来源策略	时间策略	处理方式	状态	操作项

步骤 4. 弹出**新增规则**对话框,编辑相关信息后,点击<确定>。

新增规则		×
*登录账号:	支持输入****,表示所有用户	
访问来源	意策略	
	● IP/IP范围 ○ 域名	
IP/IP范围:	例如: * 192. 168. 1. 1 192. 168. 2. 1/24 192. 168. 3. 1-192. 168. 3. 255	11
计算机名:	例如: localhost	
时间策略:	⑦ 开始时间 至 结束时间	
处理方式:	(满足所有策略) 允许登录	~
状态:	● 启用 ○ 不启用	
	关闭	确定

详细配置请参见下表。

参数	说明	
登录账号	支持输入"*",表示所有账号都记录。	
	访问来源 IP 或者 IP 段。	
	支持的格式如下:	
	◆ *	
IP/IP 范围	◆ 192.168.1.1	
	◆ 192.168.2.1/24	
	192.168.3.1-192.168.3.255	
域名	访问来源域名例: baidu.com。	
计算机名	访问来源计算机名例: localhost。	
时间策略	略 访问来源开始时间至结束时间节点。	



参数	说明						
从理主书	◆ (满足所有策略)允许登录:满足所有配置策略时,允许登录。						
处理力式	◆ (满足任意策略)禁止登录:满足任意一条策略时,禁止登录。						
状态	策略启用状态: 启用/不启用。						

14.1.2.4 终端体检

选择终端体检页签,可对终端设置风险项进行分析统计得分。

基础信息	冬端管理 系统防	护	终端体检	Ξ	E机审计	入侵防御	网页防篡改	网站管理	响应处置				
终端感知设置	自定义终端环境愿	感知频率	率及评分上	限									
病毒风险感知	感知频率设置												
쪠狗风险感知	每天 00:00:00)				~							
应用合规感知 终端健康感知	扣分权重设置												
	病毒风险感知:	-	20	+	(建议区)	间20~50)			漏洞风险感知:	-	20	+	(建议区间20~50)
	应用合规感知:	-	20	+	(建议区)	间20~50)			网络风险感知:	-	20	+	(建议区间20~50)
	终端健康感知:	-	20	+	(建议区)	间20~50)							

各配置项和说明如下表。

配置项	说明
终端感知设置	终端感知设置: 自定义终端体检频率及评分上限。
病毒风险感知	针对病毒程序文件风险、系统恶意代码感染风险进行感知。
漏洞风险感知	针对系统漏洞风险、中间件漏洞风险进行感知。
网络风险感知	针对网络变化风险进行感知。
应用合规感知	针对终端上运行的应用、服务、注册表进行感知。
终端健康感知	针对终端整体的健康状态进行感知。

14.1.2.4.1 终端感知设置

步骤 1. 选择终端体检页签。

步骤 2. 选择**终端感知设置**页签。

步骤 3. 选择感知频率(每天、每周或每月)。

步骤 4. 选择扣分权重设置。



自定义终端环境感	知频率	及评分上	限						
感知频率设置									
每天 00:00:00				~					
口分权重设置									
病毒风险感知:	-	20	+	(建议区间20~50)	漏洞风险感知:	-	20	+	(建议区间20~50)
应用合规感知:	-	20	+	(建议区间20~50)	网络风险感知:	-	20	+	(建议区间20~50)

14.1.2.4.2 病毒风险感知

步骤 1. 选择终端体检页签。

步骤 2. 选择病毒风险感知页签。

步骤 3. 点击病毒风险感知后的开关置于开启状态,开启病毒风险感知功能。

步骤 4. 选择扣分标准。

已开启 针对病毒程序文件	件风险、	系约	先恶意代码	玛感染	风险进	行感知	0				•	2
扣分标准: 每	華检出	-	20	+	个病毒	,扣	-	10	+	分		

14.1.2.4.3 漏洞风险感知

步骤1. 选择终端体检页签。

步骤 2. 选择**漏洞风险感知**页签。

步骤 3. 点击漏洞风险感知后的开关置于开启状态,开启漏洞风险感知功能。

步骤 4. 开启需要评估的漏洞等级(如高危漏洞),选择扣分标准和风险等级。

已开启 针对系统漏洞风险、	、中间件漏洞风险进行感知	
高危漏洞	扣分标准: - 40 + 风险等级: 严重风险 ~	
● 中危漏洞	扣分标准: - 30 + 风险等级: 一般风险 ~	
()低危漏洞	扣分标准: - 20 + 风险等级: 潜在风险 ~	
〇〇 可选漏洞	扣分标准: - 10 + 风险等级: 潜在风险 ~	

14.1.2.4.4 网络风险感知

步骤 1. 选择终端体检页签。

步骤 2. 选择网络风险感知页签。

步骤 3. 点击网络风险感知后的开关置于开启状态,开启网络风险感知功能。



步骤 4. 开启需要评估的变化参数(例如 IP 地址变化),选择扣分标准和风险等级。

巴开启 针对网络变化风险进行感知	
● IP地址变化 扣分标准: - 30 + 风险等级:	潜在风险 ~
DNS地址变化 扣分标准: - 30 + 风险等级:	: 潜在风险
	潜在风险
	一般风险
	严重风险

14.1.2.4.5 应用合规感知

步骤 1. 选择终端体检页签。

- 步骤 2. 选择应用合规设置页签。
- 步骤 3. 点击应用感知后的开关置于开启状态,开启应用合规检查项感知功能。
- 步骤 4. 点击对应子功能(包括软件合规风险、服务合规风险、注册表合规风险)后的开关置于开启 状态,开启对应子功能。
- 步骤 5. 设置检测方式(选择**按黑名单检测**或**按白名单检测**,并设置是否开启**按红名单检测**),并设置对应的名单。

步骤 6. 选择扣分标准和风险等级。

●开启) 针对终端上运行的应用、服务、注册表进行感知	
小 软件合规风险	扣分标准: - 20 + 风险等级: 一般风险 ~
● 按黑名单检测 设置黑名单	
○ 按白名单检测 设置白名单	
按红名单检测 设置红名单	
● 服务合规风险	扣分标准: - 20 + 风险等级: 一般风险 ~
 按黑名单检测 设置黑名单 	
○ 按白名单检测 设置白名单	
按红名单检测 设置红名单	
● 注册表合规风险	扣分标准: - 20 + 风险等级: 一般风险 >
 按黑名单检测 设置黑名单 	
按红名单检测 设置红名单	

名单类型的详细信息请参见下表。

名单类型 说明



黑名单	针对终端上运行的应用、服务、注册表设置对应黑名单,检测到终端有符合黑名单的 应用、服务、注册表时,根据扣分标准进行终端体检扣分。
白名单	针对终端上运行的应用、服务设置对应白名单,检测到终端有白名单之外的应用、服 务时,根据扣分标准进行终端体检扣分。
	针对终端上运行的应用、服务、注册表设置对应红名单,需配合黑名单或白名单功能 使用。相当于一个例外项。
红名单	◆ 与白名单功能配合使用时,当检测到终端有符合红名单的应用、服务时,不会扣分。
	◆ 与黑名单功能配合使用时,当检测到终端有符合红名单的应用、服务、注册表时,
	根据扣分标准进行扣分。

14.1.2.4.6 终端健康感知

步骤 1. 选择终端体检页签。

步骤 2. 选择终端健康感知页签。

步骤 3. 点击终端健康感知后的开关置于开启状态,开启终端健康感知功能。

步骤 4. 开启子功能(例如"登录账号是否存在弱口令"),设置扣分标准,选择风险等级。

已开启 针对系统整体的健康状态进行感知
● 登录账号是否存在弱口令 扣分标准: - 40 + 风险等级: 严重风险 >
● 登录日志审核是否开启 扣分标准: - 20 + 风险等级: 一般风险 >
● 远程注册表服务是否已关闭 扣分标准: - 40 + 风险等级: 严重风险 >
● 隐藏的盘符共享是否已关闭 扣分标准: - 40 + 风险等级: 严重风险 >
▲DMIN\$管理共享是否已关闭 扣分标准: - 40 + 风险等级: 严重风险 >
● 用户账户控制(UAC)是否开启 扣分标准: - 10 + 风险等级: 潜在风险 ~
● 共享目录是否已去除写入权限 扣分标准: - 40 + 风险等级: 严重风险 >
● TELNET远程连接服务是否已关闭 扣分标准: - 20 + 风险等级: 一般风险 ~
● 有风险的用户账户是否已关闭 扣分标准: - 20 + 风险等级: 一般风险 >
● WINDOWS空密码远程登录限制是否 扣分标准: - 40 + 风险等级: 严重风险 >
● WINDOWS账户锁定策略是否已开启 扣分标准: - 40 + 风险等级: 产重风险 >



14.1.2.5 主机审计

选择主机审计页签,可对终端设置桌面监控。

基础信息	终端管理	系统防护	终端体检	主机审计	入侵防御	网页防篡改	网站管理	响应处置			
开关机审计 系统登录防护 文件访问监控	已开启 审计用户) P的开关机行为,	,管理员可配置	置审计时间段							
	审计时	寸机: 🔽 开机	审计 🗹 关	机审计							
	审计周	周期: 💿 全时	段审计	指定时间段审	计 〇指次	定时间段不审计					

各配置项和说明如下表。

配置项	说明
开关机审计	审计用户的开关机行为,管理员可配置审计时间段。
系统登录防护	对系统账户登录进行细粒度的精准访问控制。
文件访问监控	监控目标文件、目录的改写操作。

14.1.2.5.1 开关机审计

- ◆ 功能: 审计用户的开机、关机行为, 管理员可配置审计时间段。
- ♦ 使用场景:适用于需要自定义开关机审计功能的场景。
- ◆ 使用限制:暂无。

操作步骤

步骤 1. 选择开关机审计页签。

步骤 2. 点击开关机审计后的 🔍 图标,设置审计时机和审计周期。

已开启 审计用户的开关机行为,管理员可配置审计时间段	
审计时机: 🗹 开机审计 🗹 关机审计	
审计周期: • 全时段审计 / 指定时间段审计 / 指定时间段不审计	

详细配置请参见下表。

处置方式	说明
字 开叶和	◆ 开机审计: 审计终端开机事件。
甲订时机	◆ 关机审计: 审计终端关机事件。
审计国期	◆ 全时段审计: 审计所有时间段的开机、关机事件。
平 l1 /미 /刘 	◆ 指定时间段审计: 审计指定时间段的开机、关机事件, 需要设置



处置方式	说明
	时间段(以周为周期)。
	◆ 指定时间段不审计:不审计指定时间段的开机、关机时间,需要
	设置时间段(以周为周期)。

14.1.2.5.2 配置系统登录审计

- ◆ 功能:对系统账户登录情况进行统计,并针对异常登录场景分析。
- ◆ 使用场景:适用于需要自定义审计登录结果相关场景。
- ◆ 使用限制:无。

操作步骤

步骤1.选择系统登录审计页签。

步骤 2. 勾选登录审计成功或者是失败按钮图标后,即可开启系统登录审计的相关策略。

基础信息	终端管理	里 系统防护	主机审计	入侵防御	网页防篡改	网站管理	响应处置	
开关机审计 系统登录审计	- <u>系</u> 4 对别	<mark>充登录审计</mark> 系统账户登录情况:	进行统计,并针	h 对异常登录场	词景分析。			
文件访问监控	22	登录审计: 🔽	审计登录成功	力 🔽 审计	登录失败			

详细配置请参见下表。

参数	说明
登录审计	◆ 审计登录成功:记录登录成功的终端日志。◆ 审计登录失败:记录登录失败的终端日志。

14.1.2.5.3 配置文件访问监控

- ◆ 功能:监控目标文件、目录的改写操作。
- ◆ 使用场景:适用于需要自定义修改配置策略模板文件访问监控场景。
- ◆ 使用限制:无。

操作步骤

步骤 1. 选择**文件访问监控**页签。

步骤 2. 点击文件访问监控后的 图标置于开启状态,开启文件访问控制。



新增 删除		
文件路径	备注	操作项
3. 点击<新增>。		

步骤 4. 弹出新增文件访问监控对话框,输入文件路径、备注,点击<确定>即可添加文件访问监控。

备注

操作项

新增文件访问监控		×
* 文件路径:		
备注:		1.
	关闭	确定

14.1.2.6 入侵防御

文件路径

选择入侵防御页签,可对终端设置暴力行为检测。

防暴力破解防端口扫描	(E开启) 对系统登录行为进行一定的	限制,防止账	号被熵	顺破。					
	判定规则								
	● 单个IP请求时间:	86400	* *	秒内 登录失败	5	^ ~	次则	阻断并记录	~
	多个IP请求时间:	120	*	秒内 登录失败	10	* *	次则	仅记录	~
	阻断设置								
	IP临时锁定时间: 3	600	秒						

各配置项和说明如下表。

配置项	说明
防暴力破解	对系统登录行为进行一定的限制,防止账号被爆破。



配置项	说明	
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。	

14.1.2.6.1 配置防暴力破解

- ◆ 功能:对系统登录行为进行一定的限制,防止账号被暴力破解。
- ◆ 使用场景:适用于需要自定义修改配置策略模板防暴力破解场景。
- ◆ 使用限制:无。

操作步骤

步骤 1. 选择**防暴力破解**页签。

步骤 2. 点击防暴力破解后的 3 图标置于开启状态,即可开启防暴力破解。

定规则											
● 单个IP请求时间:	86400	~	秒内 登录失败	5	^	次则	阻断并记录	~			
○ 多个IP请求时间:	120	^	秒内 登录失败	10	^	次则	仅记录	~			
新设置											

详细配置请参见下表。

参数	说明
单个 IP 请求时间	相同 IP 请求登录,统计登录失败次数的时间区间,取值范围 1~2147483647,进行阻断或者记录日志。
多个 IP 请求时间	不同 IP 请求登录,统计登录失败次数的时间区间,取值范围 1~2147483647,进行阻断或者记录日志。
IP 临时锁定时间	IP 被锁定 IP 的时间,取值范围 1~2147483647。

14.1.2.6.2 配置防端口扫描

- ◆ 功能:实时检查入站连接并阻断对主机端口的恶意探测,防止敏感信息泄露。
- ♦ 使用场景:适用于需要自定义修改配置策略模板防端口扫描场景。
- ◆ 使用限制:无。

操作步骤

步骤 1. 选择**防端口扫描**页签。

步骤 2. 点击防端口扫描后的服务状态,选择对应的状态。



关闭 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。	关闭 ^
单个IP请求时间范围: - 30 + 秒内	关闭
最大扫描端口数量: - 10 + 次	阻断开记录 仅记录
IP临时锁定时间: - 3600 + 秒	

详细配置请参见下表。

参数	说明
单个 IP 请求时间范围	同个 IP 进行端口扫描请求的统计时间区间,取值范围 10~2147483647。
最大扫描端口数量	最大扫描端口个数,取值范围 2~65535。
D吃时端完时间	当 IP 进行端口扫描触发防端口扫描规则,该 IP 被锁定的时间。取值范围
「「咖啡奴だ时间	10~2147483647。

14.1.2.7 网页防篡改

- ◆ 功能:保护文件不被篡改,默认保护所有子目录,通过新增白名单可实现对目录的排除。
- ◆ 使用场景:适用于需要修改策略模板网页防篡改场景。
- ◆ 使用限制:无。

操作步骤

步骤 1. 开启网页防篡改

- 1) 选择网页防篡改页签。
- 2) 点击网页防篡改后的 图标置于开启状态,即可开启网页防篡改。

已开启 保护文件不被篡改	牧,默认保护所有 ⁻	子目录,通过新增的	白名单可实现对子目录的	排除。					
新増规则									
	规则名称	保护对象	允许改写的IP	允许改写的进程	允许改写的用户	处理方式	是否启用	操作项	

步骤 2. 新增网页防篡改规则。

1)	选择 网页防篡改 页签,点击< 新增规则 >。	
保护	宿) 文件不被篡改,默认保护所有子目录,通过新增白名单可实现对子目录的排除。	
1	新编规则	
	规则名称 保护对象 允许改写的IP 允许改写的进程 允许改写的用户 处理方式 是否启用 操作项	
\mathbf{a}	递山 延横坝则 对泛振,检入坝则农药,但拉日县,进民队理士士,目不宜田	上十 / 74

 2) 弹出新增规则对话框,输入规则名称、保护目录,选择处理方式、是否启用,点击<确定> 即可新增规则。



新增规则				×
* 规则名称:				
*保护目录:				
处理方式:	阻断并记录	~		
是否启用:				
			关闭	确定

详细配置请参见下表。

参数	说明					
规则名称	网页防篡改自定义规则名称,不超过 30 字符。					
保护目录	网页防篡改自定义规则需要保护的文件目录,必须以"/"或"/"结尾。 例如: /etc/					
	触发防篡改自定义规则的处理方式:					
处理方式	◆ 阻断并记录: 对触发防篡改规则的行为进行阻断并记录日志。					
	◆ 仅记录: 对触发防篡改规则的行为不做处理仅记录日志。					
是否启用	网页防篡改自定义规则启用状态。					

网页防篡改为附加功能,需要单独购买许可(模块型号主机安全系统-MODULE-SERVER-WEB)才能使用此功能。

14.1.2.8 网站管理

选择网站管理页签,可对服务器设备上的网站站点攻击行为防护进行配置

基础信息 终	端管理 系统防护	终端体检 主机管	计 入侵防御	网页防篡改	网站管理 响应处置					
发布配置	已 开启 通过配置发布策略	可将发布目录下的文件	司步到网站日录							
网站漏洞防护	ACALIBULE AN (PARCE)	51020000	-20-231-344 14 20-8							
CC攻击防护	新増	>					请输入关键	字	Q	٢
网站访问控制										
网站IP黑白名单	名称	网站目录	发布端地址	发布目录	同步删除	同步软链接	同步时机	策略状态	操作项	

各配置项和说明如下表。



配置项	说明								
发布管理	通过配置发布策略,可将发布目录下的文件同步到网站目录。								
网站漏洞防护	针对网站常见的 SQL 注入攻击、XSS 跨站、Web 容器及应用漏洞进行实时防护。								
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。								
网站访问控制	灵活配置 IP 或页面路径,可对特定的访问者或页面进行放行或拦截。								
	◆ 黑名单模式:禁止特定终端用户访问黑名单中的网站页面。								
网站 IP 黑白名单	◆ 白名单模式: 仅允许特定终端用户访问白名单中的网站页面。								

14.1.2.8.1 发布配置

- ◆ 功能:通过配置发布策略,可将发布目录下的文件同步到网站目录。
- ♦ 使用场景:适用于需要修改策略模板网页发布场景。
- ◆ 使用限制:无。

操作步骤

步骤 1. 选择发布配置页签。

步骤 2. 点击发布配置后的 图标置于开启状态,即可开启发布配置。

已开启 通过配置发布	策略,可将2	发布目录下的文件同	步到网站目录。							
新增	>						谓输入关键	8	Q	0
名	称	网站目录	发布端地址	发布目录	同步删除	同步软链接	同步时机	策略状态	操作项	

步骤 3. 点击<新增>。

已开启 通过配置发布策略,可:	将发布目录下的文件际	同步到网站目录。						
新増 >]					请输入关键	字	Q
名称	网站目录	发布端地址	发布目录	同步删除	同步软链接	同步时机	策略状态	操作项

步骤4. 在弹出的对话框中输入发布规则后点击<确定>,即可完成发布策略配置。



新增规则		×
* 策略名称:		
*发布目录:		
同步删除:	○ 是 ● 否 选择是,发布时将删除网站目录下与发布目录不同的文件	
同步软链接:	是 ④ 否 选择是,发布时将同步文件原有的软链接	
同步时机:	☑ 事件同步 发布目录的内容变更会立即同步到网站服务器	
	✓ 定时同步 600 秒 可输入范围10~3600秒	
*网站目录:		
同步例外:	多个例外文件以分号*;"结尾。例如:同步目录例外为/网站目录/abc,则配置为abc	0
开启同步:		
篡改恢复:		
	取消 确	Ē

规则参数说明如下表所示。

参数	说明
发布目录	选择发布服务器下相应发布目录。
同步删除	选择是否在发布时删除网站目录下与发布目录不同的文件。
同步软链接	选择是否在发布时同步文件原有的软链接。
	◆ 事件同步:发布目录下的文件只要发生改变,将立即同步更改过的文件
同步时机	内容。
	◆ 定时同步:定时同步发布目录下的文件。
网站目录	选择需要同步的网站服务器下的目录,需写真实目录。
同步例外	排除不同步的目录。
开启同步	发布服务的内容会同步到网站服务器。
篡改恢复	用于数据被篡改后将原有数据覆盖篡改内容。

14.1.2.8.2 配置网站漏洞防护

- ◆ 功能:针对网站常见的 SQL 注入攻击、XSS 跨站、Web 容器及应用漏洞进行实时防护。
- ◆ 使用场景:适用于需要自定义修改配置策略模板网站漏洞防护场景。
- ◆ 使用限制:无。



14.1.2.8.2.1 开启网站漏洞防护

步骤 1. 选择网站漏洞防护页签。

步骤 2. 点击网站漏洞防护后的 网际置于开启状态,即可开启网站漏洞防护功能。

iQL注入	XSS攻击 应用	程序漏洞 自定义规则				✓ 文件名解析漏洞防护
见贝川D	类型	状态	关键字	描述	自定义告警级别	✓ 禁止浏览畸形文件✓ 敏感信息防泄漏
46	sql注入		url	数据库注释注	警告信息	> 自动屏蔽扫描器
47	sql注入		url	防止对数据库	警告信息	◇ 资源防盗链
48	sql注入		url	单引号注入探测	警告信息	> 网站文件上传防护 → 网站访问检测
00	sql注入		url	防止非法访问i	警告信息	×

14.1.2.8.2.2 更改拦截提示内容

步骤 1. 点击<自定义拦截提示>。

已 开启 针对网站常见	的 SQL注入攻击、XSS题	营站、Web容器及应用漏浴	同进行实时防护	。自定义拦截提示			C
SQL注入	XSS攻击 应用程序	齐漏洞 自定义规则					☑ 文件名解析漏洞防护
规则ID	类型	状态	关键字	描述	自定义告警级别		✓ 禁止浏览畸形文件✓ 敏感信息防泄漏
146	sql注入		url	数据库注释注	警告信息	~	自动屏蔽扫描器
147	sql注入		url	防止对数据库	警告信息	~	资源防盗链
148	sql注入		url	单引号注入探测	警告信息	~	网站访问检测

步骤 2. 在弹出的对话框中输入拦截提醒内容,点击<确定>即可更改拦截提示。



14.1.2.8.2.3 选择防护类型

步骤1. 勾选右侧的防护类型,即可开启相应防护。



SQL注入	XSS攻击	应用程序漏洞	自定义规则					✓ 文件名解析漏洞防护
规则ID	类型	状	态	关键字	描述	自定义告警级别		 ✓ 禁止浏览畸形文件 ✓ 敏感信息防泄漏
146	sql	έλ (0	url	数据库注释注	警告信息	~	自动屏蔽扫描器
147	sql	ŧл C	0	url	防止对数据库	警告信息	~	资源防盗链
148	sql注	ŧλ C		url	单引号注入探测	警告信息	~	网站访问检测
100	sql	έλ 🔵	0	url	防止非法访问i	警告信息	~	

防护类型的说明如下表所示。

防护类型	说明
文件名解析漏洞防护	存在漏洞的 Web 中间件在解析文件名时,由于内置逻辑问题,可能将非脚本类型的文件(扩展名绕过)当做脚本文件执行引发漏洞。
禁止浏览畸形文件	由部分系统保留的特殊字符串创建的文件,普通方法无法直接访问,但是可以被 Web 中间件解析,从而引发漏洞。
敏感信息防泄露	管理员无意中存放在网站目录下的敏感文件,例如日志文件、压缩包、数 据库文件等,可能被攻击者通过猜测的方式获取下载地址,引起信息泄露。
自动屏蔽扫描器	可检测各种主流扫描器行为,根据设置屏蔽对本站的扫描。
资源防盗链	采用引用方式防盗链,防止网站内部资源被其他网站引用,造成带宽浪费 并消耗系统性能。
网站文件上传防护	部分业务系统存在文件上传功能,对用户上传的文件进行检测,对恶意文件(如网马文件)进行拦截。
网站访问检测	访问网站中的网马文件,例如: <u>http://192.168.1.1/1.php</u> ,访问时会被拦截。

14.1.2.8.2.4 修改规则的启用状态

步骤 1. 选择攻击类型(如 SQL 注入),选择目标修改规则 ID,点击状态列表下的 图标,即可修 改规则的启用状态。



iQL注入	XSS攻击 应	拉用程序漏洞	自定义规则					✓ 文件名解析漏洞防护
规则ID	类型	状	态	关键字	描述	自定义告警级别		 ✓ 禁止浏览畸形文件 ✓ 敏感信息防泄漏
146	sql注入		D	url	数据库注释注	警告信息	~	自动屏蔽扫描器
147	sql注入		D	url	防止对数据库	警告信息	~	资源防盗链
148	sql注入	C		url	单引号注入探测	警告信息	~	网站访问检测
100	sql注入		D	url	防止非法访问i	警告信息	~	

14.1.2.8.2.5 系统默认规则

步骤 1. 点击<SQL 注入>或<XSS 攻击>或<应用程序漏洞>,可查看系统默认的规则。

已开启 针对网站常见的	l SQL注入攻击、XSS器	跨站、Web容器及应用》	漏洞进行实时防护。	自定义拦截提示			
SQL注入	XSS攻击 应用程	序漏洞 自定义规则	1				✓ 文件名解析漏洞防护
规则ID	类型	状态	关键字	描述	自定义告警级别		 ✓ 禁止浏览畸形文件 ✓ 敏感信息防泄漏
146	sql注入		url	数据库注释注	警告信息	~	自动屏蔽扫描器
147	sql注入		url	防止对数据库	警告信息	~	资源防盗链
148	sql注入		url	单引号注入探测	警告信息	~	网站文件上传防护

14.1.2.8.2.6 自定义规则

步骤 1. 点击<自定义规则>。

L注入	XSS攻击	应用程序漏洞	自定义规则					✓ 文件名解析漏洞防护
								☑ 禁止浏览畸形文件
新增								✓ 敏感信息防泄漏
∭ID	类型	状态	关键字	规则	描述	自定义告警级别	操作项	自动屏蔽扫描器
								资源防盗链
								网站文件上传防护
								网站文件上传防护

步骤 2. 点击<新增>。



L注入	XSS攻击	应用程序漏洞	自定义规则					✓ 文件名解析漏洞防护
	_							✓ 禁止浏览畸形文件
新増								✓ 敏感信息防泄漏
则ID	类型	状态	关键字	规则	描述	自定义告警级别	操作项	自动屏蔽扫描器
								资源防盗链

步骤 3. 在弹出的对话框中输入规则、描述,选择关键字、状态,点击<确定>即可新增网站漏洞防护规则。

自定义规则	×
* 规则:	
* 关键字:	url cookie post host method range user-agent x-forwarded-for content-type content-length referer
* 描述:	
状态:	○ 启用 ● 未启用 关闭 确定

14.1.2.8.3 配置 CC 攻击防护

- ◆ 功能:智能检测并防御 CC 攻击,保证网站正常服务能力。
- ◆ 使用场景:适用于需要自定义修改配置策略模板 CC 攻击防护场景。
- ◆ 使用限制:无。

14.1.2.8.3.1 开启 CC 攻击防护

步骤 1. 选择 CC 攻击防护页签。

步骤 2. 点击 CC 攻击防护后的 🔍 图标置于开启状态,即可开启 CC 攻击防护。

包智	开启 能检测并	防御CC攻击,保证网站正常服务能力。 自定义拦截提示			
C	高	防护策略: 低设置 自定义告警级别:	警告信息	~	
		智能验证模式,当请求数达到触发条件时,自动识别该IP是否 分CC攻击问题。	5为真实访客浏览行为,	解决大部	
0	中				
	低				



14.1.2.8.3.2 自定义拦截提示

步骤 1. 点击<自定义拦截提示>。

17			
防护策略:1比设置	自定义告警级别:	警告信息	\sim
智能验证模式,当请求数达到触; 分CC攻击问题。	发条件时,自动识别该IP是否	为真实访客浏览行为	为,解决大部

步骤 2. 弹出自定义拦截提示对话框,编辑提示内容后点击<确定>。

自定义拦截提示		×
请不要频繁访问		<i>li</i>
	取消	确定

14.1.2.8.3.3 设置防护策略

步骤1.选择防护策略(低、中、高)。

已开启 智能检测并防御(CC攻击,保证网站正常服务能力。 自定	义拦截提示			
○ 高 ○ 中	防护策略: 低 设置 智能验证模式,当请求数达到触发 分CC攻击问题。	自定义告警级别: 条件时,自动识别该IP是召	警告信息 5为真实访客浏览行为	~ 9,解决大部	
1 ££					

防护策略的详细信息请参见下表。

参数	说明
	◆ 高: 对每个 IP 的首次访问,需要手动验证,用于识别是否为真实访客
	浏览行为,适用于网站处于长期性被攻击情况下。
	◆ 中: 对每个 IP 的首次访问,自动识别该请求是否为真实访客浏览行为,
防护策略 	无需访客参与验证,适用于网站处于间断性被攻击情况下。
	◆ 低:智能验证模式,当请求数达到触发条件时,自动识别该 IP 是否为
	真实访客浏览行为,解决大部分 CC 攻击问题。可 <u>自定义防护配置</u> 。



14.1.2.8.3.4 自定义防护配置

步骤 1. 选择防护策略为"低",点击<设置>。

5	防护策略: 低 设置	自定义告警级别:	警告信息	×	
	恕能哈证模式 当请求数达到触	发条件时 自动识别该IP是3	5为直实访家浏览行为 角	冲大部	
	日形巡巡法议,当府小私公扣局	及示[于时],日40100月以下在日	1/5英大切古网见11/5,周		
	分CC攻击问题。				

步骤 2. 弹出 CC 攻击防护设置对话框,设置"单个 IP 每 X (1~36000)秒,请求次数超过 Y (1~999) 次, IP 锁定时间 Z (1~36000)秒",设置是否启用浏览器行为验证,点击<确定>。

CC攻击防护设置	×
单个IP每 60 🛟 秒,请求次数超过 200 🛟 次,IP锁定时间	1800 🔹 秒
☑ 启用浏览器行为验证	

浏览器行为验证: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。此选项是为了将正常用户和攻击工具、 爬虫类程序进行区分。

14.1.2.8.4 配置网站访问控制

- ◆ 功能:灵活配置网站访问控制规则,可对特定的访问者或页面进行放行或拦截。
- ◆ 使用场景:适用于需要自定义修改配置策略模板网站访问控制场景。
- ◆ 使用限制:新增规则前请确认客户端已安装 Web 应用防护插件。

14.1.2.8.4.1 开启网站访问控制

步骤1.选择网络访问控制页签。

步骤 2. 点击网站访问控制后的 2 图标置于开启状态,即可开启网站访问控制。



灵活配置IP或页面路径,	可对特定的访问者或贝面进行放行或拦截。 自	E义拦截提示			
 新增规则前请确认E IP范围字段可为单个 页面路径为网页路径 	己安装Web应用防护插件。 \PP或IP段,如"192.168.1*"或"192.168.1.10–192.168 圣,格式形如"192.168.1.100/admin"。	.1.20"。通过换行来分隔的多个IP或IP段。			
新增					
IP范围	页面路径	描述	处理方式	状态 操作项	

14.1.2.8.4.2 自定义拦截提示

步骤 1. 点击<自定义拦截提示>。

已开启 灵活配置IP或页面路径,可	可对特定的访问者或页面进行放行或拦截。	E义拦截提示			
 新增规则前请确认已: IP范围字段可为单个! 页面路径为网页路径; 	安装Web应用防护插件。 P或IP段,如"192.168.1.*"或"192.168.1.10-192.168 ,格式形如"192.168.1.100/admin"。	1.20"。通过换行来分隔的多个IP或IP段。			
新増					
IP訪闻	而而路径	描述	 	状态	操作顶

步骤 2. 弹出自定义拦截提示对话框,编写提示内容后点击<确定>。

您的访问权限	 		
			1.

14.1.2.8.4.3 新增规则

步骤 1. 点击<新增>。

已开启 灵活配置IP或页面路径	ē, 可对特定的访问者或页面进行放行或拦截.	, 自定义拦截提示							
 新增规则前请确认 IP范围字段可为单 页面路径为网页路 	 新增规则前请确认已安装Web应用防护插件。 IP范围字段可为单个IP或IP段,如*192.168.1.**或*192.168.1.10-192.168.1.20*。通过换行来分隔的多个IP或IP段。 页面路径为网页路径,格式形如*192.168.1.100/admin*。 								
新増									
IP范围	页面路径	描述	处理方式	状态	操作项				

步骤 2. 在弹出的对话框中输入 IP 范围、页面路径、描述,选择处理方式、状态,点击<确定>即可生成访问控制规则。


新增规则				×
IP泡围:				
	*	1.1		
	192.100.	2 1/24		
	192, 168.	3. 1-192. 168. 3.		
				li
页面路径:				
				h
描述:				
				1.
*处理方式:	⊙ 允许	○ 拒绝		
* 牛太・				
1/23.				
			关闭	确定

详细配置请参见下表。

参数	说明
IP 范围	 终端的 IP 范围,支持以下格式: <
页面路径	页面路径为网页路径,例如"192.168.1.100/admin"。
处理方式	 ◆ 允许: 允许 IP 范围内终端访问指定页面。 ◆ 拒绝: 禁止 IP 范围内终端访问指定页面。
状态	是否启用规则。

14.1.2.8.5 网站 IP 黑白名单

- ◆ 功能: 黑名单模式下禁止特定终端用户访问黑名单内的网站页面; 白名单模式下仅允许特定 终端用户访问白名单内的网站页面。
- ◆ 使用场景:适用于需要自定义修改配置策略模板网站 IP 黑白名单的场景。
- ◆ 使用限制:新增规则前请确认客户端已安装 Web 应用防护插件。

14.1.2.8.5.1 黑名单模式

步骤 1. 选择网站 IP 黑白名单页签。

步骤 2. 将网站 IP 黑白名单后的开关置于开启状态,选择黑名单模式。



步骤 3. 点击<新增黑名单>。

网站IP黑白名单(已开启 不在黑名单规则内的程序者	B会被放行。 黒名単模式 > 2		
 新增规则前清确认已要 IP范围字段可为单个IP 页面路径为网页路径, 新增黑名单 3 	·装Web应用防护插件。 或IP段,如 192.168.1.* "或 "192.168.1.10-192.16 格式形如 "192.168.1.100/admin" 。	58.1.20",通过换行来分隔的	的多个IP或IP段。
IP范围	页面路径	状态	操作项



步骤 4. 在弹出的新增规则对话框中编辑相关信息,点击<确定>。

新增规则		×
IP范围:	192.168.0.1	
页面路径:	192.168.0.1/login	
描述:		
*状态:	 高用 未启用 	
		关闭 确定

参数	说明
	终端的 IP 范围,支持以下格式: ◆ "*"表示所有 IP。
IP 范围	 ◆ 单个 IP,例如 192.168.0.1。 ◆ IP 网段,例如 192.168.2.0/24。 ◆ 地址范围,例如 192.168.1.1-192.168.1.100。



参数	说明
页面路径	页面路径为网页路径,例如"192.168.1.100/admin"。
状态	是否启用规则。

14.1.2.8.5.2 白名单模式

- 步骤 1. 选择网站 IP 黑白名单页签。
- 步骤 2. 将网站 IP 黑白名单后的开关置于开启状态选择白名单模式。
- 步骤 3. 点击<新增白名单>。

列站IP黑白名单(已开启 在白名单规则内的程序都	会被阻止。 白名単模式 ~ 2		
 新增规则前请确认已安 IP范围字段可为单个IP 页面路径为网页路径, 新增白名单 3 	袭Web应用防护插件。 或IP段,如"192.168.1.* "或"192.168.1.10-192 格式形如"192.168.1.100/admin"。	.168.1.20 ",通过换行来分隔的	的多个IP或IP段。
IP范围	页面路径	状态	操作项

暂无数据

步骤 4. 在弹出的新增规则对话框中编辑相关信息,点击<确定>。

新增规则				×
IP范围:	192.168.	0.1		
页面路径:	192.168.	0.1/login		
描述:				
*状态:	● 启用	○ 未启用	关闭	确定



14.1.2.9 响应处置

选择响应处置页签,可对威胁事件配置放行等操作。

基础信息	终端管理 系统防护	终端体检	主机审计	入侵防御	网页防篡改	网站管	理 响应处置	t				
信任名单 进程防护 违规外联	已开启 信任名单添加文件路径 新增信任名单	或MD5值,可有 删除	针对护网高级威	胁、病毒防护	、病毒扫描、网	刚马扫描、	助索防护放行;	信任名单添加IP,	可针对防暴力破解	、防端口扫描、	Web应用防护放行。	
流量画像事件响应	信任项				*	型	备注	E			操作项	

各配置项和说明如下表。

配置项	说明
信任名单	信任名单添加文件路径或 MD5 值,可针对护网高级威胁、病毒防护、病毒扫描、网马扫描、勒索防护放行;信任名单添加 IP,可针对防暴力破解、防端口扫描、Web 应用防护放行。
进程防护	匹配黑白名单里的系统进程执行放行与阻止操作。
违规外联	通过探查方式检测主机直接连通互联网或通过其他设备访问互联网。
网络分域隔离	据业务需求,可创建多个网络域供终端操作者选择,同时只能启用一个网络域。
流量发现	采集资产流量,绘制全景流量图展示主机之间的通讯关系。
事件响应	创建满足指定条件,执行终端响应动作。

14.1.2.9.1 配置信任名单

- ◆ 功能:信任名单添加文件路径或 MD5 值,可针对护网高级威胁、病毒防护、病毒扫描、网 马扫描、勒索防护放行;信任名单添加 IP,可针对防暴力破解、防端口扫描、Web 应用防护放行。
- ◆ 使用场景:适用于需要修改策略模板信任名单场景。
- ◆ 使用限制:无。

操作步骤

步骤 1. 选择信任名单页签。

步骤 2. 点击信任名单后的 图标开关置于开启状态,开启信任名单功能。

已开启 信任名单添加文件路径或MD5值,	可针对护网高级威胁、	病毒防护、病毒排]描、网马扫描.	、勒索防护放行;	信任名单添加IP,	可针对防暴力破解、	防端口扫描、	Web应用防护放行。	
新增信任名单 删除									
信任项			类型	备	注			操作项	



步骤 3. 点击<新增信任名单>。

已开启 信任名单添加文件路径或MD5值,	可针对护网高级威胁、	病毒防护、病毒扫描、	网马扫描、	勒索防护放行;	信任名单添加IP,	可针对防暴力破解、	防端口扫描、	Web应用防护放行。	
新增信任名单									
信任项			类型	备	注			操作项	

步骤 4. 弹出新增信任名单对话框,选择类型,输入信任项、备注,点击<确定>即可生成信任名单。

新增信任	名单	×
类型:	● 文件路径 ○ MD5 ○ IP	
* 信任项:	请输入文件路径或者文件名,可针对网马扫描	萌放行 "
备注:		
	关闭	确定

类型的说明如下表。

类型	说明
文件路径	对文件路径或者文件名匹配,可针对护网高级威胁、病毒防护、病毒扫描、网马扫描、 勒索防护放行。例如:/etc、init.c。
MD5	对文件 MD5 值进行匹配,可针对护网高级威胁、病毒防护、病毒扫描、网马扫描、勒 索防护放行。
IP	对 IP 进行匹配,可针对防暴力破解、防端口扫描、Web 防护放行。例如: 192.168.1.1、 192.168.2.0/24、192.168.3.1-192.168.3.100。

14.1.2.9.2 配置进程防护

- ◆ 功能:匹配黑白名单里的系统进程执行放行与阻止操作。
- ◆ 使用场景:适用于需要自定义修改配置策略模板进程防护场景。
- ◆ 使用限制:暂无。
- ◆ 建议:开启"仅记录"观察一段时间,避免阻止正常的程序,确认无问题后,开启。

操作步骤(以白名单模式为例)

步骤 1. 选择进程防护页签。

步骤 2. 开启进程防护(设置为"阻断并记录"或者"仅记录")。



E黑名单规则内的程序都会	被放行。 黑名单模式 ~				阻断并记录	^
•风险性操作提示:启用进	程黑名单后,若设置成阻断并记录,规则 	列表中的程序运行都将被阻止。			关闭 阻断并记录	
- 建议, 开后 议记家 观察	一段时间,避光阻止正吊时怪序,娴以无	则题后,丌危。		Common and an and	仅记录	
新增黑名单				请输入关键字		
ា ±៣៣៧	举刑	备注	启用规则		操作项	

步骤 3. 设置为白名单模式。

阻断并记录 不在黑名单规则内的程序都会被放行。	黑名单模式 ~				阻断并记录	~
 风险性操作提示:启用进程黑名单后 建议:开启"仅记录"观察一段时间, 	黑名单模式 白名单模式	己录,规则列表中的程序运行都将被阻止。 9,确认无问题后,开启。				
新増黒名単				请输入关键字	Q	0
规则	类型	备注	启用规则		操作项	

详细配置请参见下表。

配置项	说明	
黑名单模式	不在黑名单规则内的程序都会被放行。	
白名单模式	不在白名单规则内的程序都会被阻止。	

步骤 4. 点击<新增白名单>。

在白名单规则内的程序都会	会被阻止。 白名单模式 ~		阻害	所并记录	`
 风险性操作提示:启用进 建议:开启"仅记录"观察 	挂程白名单后,若设置成阻断并记录,不在 【一段时间,避免阻止正常的程序,确认无	规则列表中的程序运行都将被阻止。 问题后,开启。			
新增白名单 >			请输入关键字	Q	0

步骤 5. 在弹出的对话框中中输入类型、进程参数、备注、启用规则,点击<确定>即可添加白名单。

新增白名单		×
* 类型:	请选择	~
进程参数:	请输入进程参数	
备注:	请输入	
启用规则:		
		关闭 确定



详细配置请参见下表。

参数	说明		
类型	支持文件路径和 MD5。		
进程参数	对应进程相关参数。		
路径匹配模式	 当类型选择"文件路径"时,需要设置路径匹配模式: ◆ 全字匹配:文件路径与设置的路径一致时才匹配规则。 ◆ 模糊匹配:文件路径包含设置路径的部分值时匹配规则。 		
备注	该策略的备注详情。		
启用规则	是否启用规则。		

14.1.2.9.3 配置违规外联

- ◆ 功能:通过探查方式检测终端直接连通互联网或通过其他设备访问互联网的行为,对非法外 联行为进行处置,预防终端访问其他恶意链接造成的相关影响。
- ◆ 使用场景:适用于需要自定义修改配置策略模板违规外联场景。
- ◆ 使用限制:无。

操作步骤

步骤 1. 选择**违规外联**页签。

步骤 2. 点击违规外联后的 🤍 图标置于开启状态,即可开启违规外联功能。

(已开启) 通过探查方式检测主机直接连通互联网或通过其他设备访问互联网	
探测地址 发现选规外联终端: ● 不处理 ● 弹窗提醒用户并关机 ● 弹窗提醒用户并断网 (重启主机恢复网络) 设置探测地址,系统自动检测是否外联探测地址。	已设置探测地址 0 个

步骤 3. 点击"已设置探测地址 X个"中的蓝色数字,其中"X"表示具体数字。

已开启 通过探查方式检测主机直接连通互联网或通过其他设备访问互联网	
探测地址 发现违规外联终端: • 不处理 弹窗提醒用户并关机 弹窗提醒用户并断网 (重启主机恢复网络) 设置探测地址,系统自动检测是否外联探测地址。	已设置探测地址

步骤 4. 在弹出的对话框中点击<添加一行>。输入域名或 IP 后点击<保存>,再点击<确定>,即可保存 探测地址。



	探测地址		×
	域名/IP		3 操作项
	请输入域名/IP	0	保存
		 ● 添加一行 	9
			取消 确定
步骤 5. 设置处	建方式。		
尼开启 通过探查方式检测主	机直接连通互联网或通过其他设备访问互联网		
探测地址		89月7月日二十年6月(第二十月46月日46)	已设置探测地址 0 个
及现过观가联终端: 设置探测地址,系统	 ・	國媒唯用厂升町网(里后土机隊夏网络)	

发现违规外联终端的处置方式请参见下表。

处置方式	说明		
不处理	发现违规外联终端不做任何处理。		
弹窗提醒用户并关机	发现违规外联终端,客户端会弹出弹窗进行警告使用者,并进行关机处理。		
弹窗提醒用户并断网 (重启主机恢复网络)	发现违规外联终端,客户端会弹出弹窗进行警告使用者,并进行对终端 断网处理,需重启终端后方可恢复网络,如发现防护日志出现终端因为 违规外联导致断网,需要给该终端重启操作后方可恢复。		

14.1.2.9.4 网络分域隔离

- ◆ 功能:根据业务需求,可创建多个网络域供终端操作者选择,同时只能启用一个网络域。
- ◆ 使用场景:适用于需要自定义修改配置策略模板网络分域隔离场景。
- ◆ 使用限制:终端切换到此网络域后,将无法访问其他所有自定义网络域地址。

操作步骤

步骤 1. 选择网络分域隔离页签。

步骤 2. 选择触发网络分域隔离规则时,系统的处理方式(需要选择"阻断并记录"或"仅记录")。



根据业务需求,可创建多个网络域供终端操作者选择,同时只能启用一个网络域

自城	阻断并记录
全 7 人 15岁	关闭
an w road	阻断并记录
注: 终端切换到此网络域后,将无法访问其他	仅记录
所有自定义网络域地址	
编辑	

步骤 3. 点击<新增域>。

新坊地	阻断并记录
1) 默认域	
备注: 终端切换到此网络域后,将无法访问其他 所有自定义网络域地址	
编辑	

步骤 4. 弹出新增网络域对话框,输入网络域、地址段、备注,点击<确定>即可添加网络域。

新增网络域			×
* 网络域:			
*地址段:			4
备注:	请输入备注信息		1.
		关闭	确定

详细配置请参见下表。

参数	说明
网络域	字符长度最大为 10 位。
地址段	地址段格式可以为: 0.0.0.0/24、192.168.1.10-192.168.1.100、192.168.1.1。
备注	网络域的备注信息。

14.1.2.9.5 流量画像

- ◆ 功能:采集终端流量,绘制全景流量图展示主机之间的通讯关系。
- ◆ 使用场景:适用于需要自定义修改配置策略模板流量画像场景。
- ◆ 使用限制:暂无。



操作步骤

步骤 1. 选择**流量画像**页签。

步骤 2. 点击流量画像后的 团 图标置于开启状态,即可开启流量画像功能。

● 日开启 采集资产流量,绘制全景流量图展示主机之间的通讯关系

14.1.2.9.6 事件响应

- ◆ 功能:检测到终端触发对应规则后,终端会执行相应动作,防止对终端产生危害。
- ♦ 使用场景:适用于需要自定义修改配置策略模板事件响应场景。
- ◆ 使用限制:暂无。

操作步骤

步骤 1. 选择事件响应页签。

步骤 2. 将事件响应后的 🤍 图标置于开启状态,开启事件响应功能。

	已开启 创建满足指定条件,执行终端响应动作			
	新増			
	条件	动作	是否告警	操作项
步骤	3. 点击<新增>。 C开E 创建满足指定条件,执行终端确应动作			
	新油			
	条件	动作	是否告警	操作项
步骤	4. 在弹出的对话框中选择触发条件和	和执行动作,点击< 确定 >。		

新增			×
触发条件			
类型:	文件变更 ~		
文	件 请输入文件路径	新建	
执行动作			
	告警 是否产生告警日志		
	删除文件 删除此文件		
		关闭 确定	È



详细配置请参见下表。

参数	说明
触发条件	包括文件变更、进程变更、网络连接、账号变更。
执行动作	触发规则后终端执行的动作,包括结束进程、删除文件等。

14.1.3 绑定终端

绑定终端是指将策略应用到特定的终端上。创建策略后,必须将策略绑定到终端才会生效。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"策略模板>终端策略",进入终端策略页面。

步骤 3. 选择需要绑定终端的策略,点击策略右侧的 *** 图标,选择 "绑定终端"。

策略管理	e
请输入策略名称	Q
通用模板 已绑定 39 个终端	
审计模板 绑定终于 已绑定 0 1 设为默认	満 2 以模板

步骤 4. 在弹出的对话框中选择需要绑定的终端(将**终端列表**中的终端移动至**已选择端列表**),单击< 确定>,即可将终端绑定至本策略。



选择终端

终端列表 3/5		已选择终端列表	3/3
请选择分组	~	请选择分组	~
选择标签	~	选择标签	~
终端名称VIP	Q	终端名称VIP	Q
■ 终端名称		☑ 终端名称	
☑ ⑧ linux-HJY(192.168. ■ ■.)		2 OESKTOP-80K43JQ(192.16	
💿 🔕 localhost.localdomain(10.11 🖕 🖕 192.16 🛛 👘 🕒		∑ 🙆 linux-HJY(192.168. 严 🔍)	
Ø WIN-3QFTRUC04HH(10.11.♣ ▲* 192.168 ♣		🗹 🔕 localhost.localdomain(i 🖥 📕 🍋	
🖉 🔕 localhost.localdomain(10.11 💼 🖕 192.168 🖕 👘			
☑			
		T	光 西 亡

14.1.4 其他操作

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在导航栏选择"策略模板>终端策略",进入终端策略页面。

步骤 3. 点击相关按钮,可对策略进行导入、导出、查看、设为默认模板及删除操作。



×





14.2 容器策略

仅租户角色具有安全策略操作权限。

可在**安全策略**页面对容器目录及子目录内的文件进行篡改防护,支持设置"允许改写的进程"、"放行子

目录"。将容器镜像内的目录保护后,任何以该镜像创建的容器内的目录都将被保护,目录下的内容 (包括子目录和文件)都将无法被修改。

違: 建议将日志目录、缓存目录、数据库目录及网站服务需要写入文件的目录做放行处理。

新增容器篡改防护规则的操作方法如下:

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"策略模板>容器策略",进入容器篡改防护页面。

步骤 3. 将容器篡改防护后的开关置于开启状态,开启容器防篡改功能。

容器篡改防护 已开启 将容器镜像内目录保护后,任何以 数据库目录及网站程序需要写入的	该镜像创建的容器内的目录都 1目录做放行配置。	将被保护。目录下的所有目	录、文件(包括子目录和文件)都将无法修改。建议将	将日志目录、缓存目	录、	
新增删除						请输入关键字	Q () III ()
规则名称	保护镜像名	保护容器目录	允许改写进程	处理方式	是否启用	备注	操作项
			暂无数据				
步骤 4. 点击<新 容器篡改防护 C开启 将容器镜像内目录保护后,任何以 数据库目录及网站程序需要写入的	「増>。	将被保护。目录下的所有目	录、文件(包括子目录和文件)都将无法修改。建议将	将日志目录、缓存目	ज़ .	
新増删除						请输入关键字	0 🗄 🕥
	保护镜像名	保护容器目录	允许改写进程	处理方式	是否启用	备注	操作项
			暂无数据				

步骤 5. 进入新增规则页面,填写规则详细信息后点击<确定>,即可成功新增容器篡改防护规则。



♠ 新增规则		
* 规则名称	rule123	
保护镜像名	ops	只支持"*"号结尾的模糊匹配
*保护容器目录	/bin	只允许配置一个保护目录,配置多个目录需创建多个规则
允许改写进程	/bin/md	请输入允许修改保护容器目录的进程,多个用逗号分隔, 不允许配置*号
处理方式	阻断并记录 🗸	
是否启用		
放行子目录	/bin/md/e	允许某些进程修改某些子目录(目录必须以/结尾)或文件, 路径和进程用逗号分隔,换行分隔多条配置。例如: /var/www/logs/,* /var/www/cache/,/bin/java
备注		
	取消 确定	

参数	说明
规则名称	最大长度 20 字符。
保护镜像名	被保护的镜像名称, 仅支持以 "*"结尾的模糊匹配, 且仅支持英文, 最大长度 1024 字符, 例如 ops*。
保护容器目录	仅允许设置一个保护目录,例如/bin。
允许改写进程	允许修改保护容器目录的进程,可输入多个,用英文逗号分隔。例如/bin/md。
处理方式	 触发规则时系统的处理方式: ◆ 仅记录:仅生成防护日志。 ◆ 阻断并记录:阻断改写请求,并生成防护日志。
是否启用	是否启用该规则。
放行子目录	允许修改的子目录,目录必须以"/"结尾,也可以是具体文件,进程和路径用英 文逗号分隔,多个配置项用回车分隔。



15 响应处置

仅租户角色具有响应处置权限。

响应处置是指对所有终端进行信息采集,对采集的信息进行分析处理后得到流量画像,对采集到的信息提供检索功能。并支持对终端执行文件推送等操作。

15.1 微隔离

微隔离可对不同业务之间进行流量隔离并精确阻断非法流量。租户可启用或停用微隔离规则,停用后的规则不生效。同时租户通过一键封锁 IP、一键关闭端口输入需要屏蔽的地址或者关闭的端口,可一键生成对应规则。

◆ 确保关闭本地端口或屏蔽 IP 不会对业务造成影响后进行相应操作。

◆ 微隔离规则放行的优先级高于阻止, 在配置时可以先阻止所有端口后, 再放行必要的端口。

◆ 针对 Linux 终端配置的微隔离规则与本地防火墙规则冲突时,以微隔离配置的规则为准。

◆ 微隔离暂不支持 ipv6

15.1.1 混合模式

支持终端规则和标签规则两种配置方式。关于标签的更多信息,请参考新增标签。

15.1.1.1 终端规则

15.1.1.1.1 新增终端微隔离规则

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"响应处置>微隔离",选择终端规则页签。

步骤 3. 选择**混合模式**,点击<新增规则>。

对不同业务之间进行流量隔离并精确阻断非法流量				(2	◎ 混合模式	~ Ø
终端规则 标签规则						
规则名称: 请输入规则名称 ①	方向: 请选择方向	~			查询	重置
新加速规则 — ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	本地端口 ↓ 远程IP ↓	過日降 远程端口 ◇ 协议	义 ◇ 处理方式 ◇	启用状态 ◇ 应用终端	添加时间	操作项
11 入站 192.168.27.57	135 *	* 所有	有 阻止	HIRAM-PC(1	2022-10-2	编辑 删除

步骤 4. 进入新增微隔离页面,编辑相关信息,点击<确定>即可新增微隔离规则。



en manan	请输入规则名称	• 最多输入30个字符,可用于说明规则的用途
《类型	必填项,请选择协议类型	\sim
类型	○ 双向 ● 入站规则 ○ 出站规则	 入站(默认)表示远程主机访问本地主机,出站表示 本地主机访问远程主机
本地IP	IP支持IPv4, 输入形式例如: 192.168.1.1 192.168.2.1/24 192.168.3.1-192.168.3.255	 IP支持IPv4, 输入形式例如: 192.168.1.1 192.168.1.1/24 192.168.1.1-192.168.1.255 "/"表示子网掩码、"-"表示IP段,多个IP需换行输入
地端口	例1如: 445	* 例如: 445 "*"表示所有端口、多个端口换行输入
远程IP	IP支持IPv4, 输入形式例如: 192.168.1.1 192.168.2.1/24 192.168.3.1-192.168.3.255	 IP支持IPv4, 输入形式例如: 192.168.1.1 192.168.1.1/24 192.168.1.1-192.168.1.255 "*表示子网摊码、"-"表示IP段、多个IP需换行输入
民端口	例如: 445	● 例如: 445 ***表示所有端口、多个端口换行输入

参数	说明
规则名称	可用于说明规则的用途,最多输入 30 个字符
规则类型	 ◆ 入站:规则仅应用于入站连接,即访问本机的请求。 ◆ 出站:规则仅应用于出站连接,即本机向外发送的请求。 ◆ 双向:规则应用于入站及出站两种连接。
本地 IP	通常设置为"*",表示所有本地 IP。多网卡配置不同规则的情况请填写具体 IP。
本地端口	本地主机的端口,例如 455,输入多个请用回车间隔,"*"表示所有端口。
远程 IP	远程主机的 IP 地址或地址段。
远程端口	远程主机的端口,例如 455,输入多个请用回车间隔,"*"表示所有端口。
协议类型	支持所有、TCP、UDP 和 ICMP。
处理方式	放行或阻止,放行的优先级高于阻止,可用于阻止整段 IP 的访问再放行个别 IP 允许访问。



参数	说明
状态	开启后规则生效,关闭后规则不生效。
应用终端	点击 <选择终端> ,设置本条规则应用的终端。

15.1.1.1.2 一键封锁 IP

当需要禁止终端访问目标主机时或禁止目标主机访问终端时,可设置一键封锁 IP。操作方法如下:步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在导航栏选择"响应处置>微隔离",选择混合模式。

步骤 3. 选择终端规则页签,点击<一键封锁 IP>。

微隔离 对不同业务之间进行流量降	扇萬并精确阻	断非法流量							۲	混合模式	~ 0
终端规则标签规则											
规则名称: 请输入规	则名称		方向: 请选择,							查询	重置 >
新増规则 一键	i锁IP	一键关闭端口	シン 合出		禁用	删除					0 = 0
规则名称 ◊	方向 🗘	本地IP♀	本地端口 0	远程IP ≎	远程端口 ◊	协议 ♡	处理方式 ♡	启用状态 ♡	应用终端	添加时间	操作项
test27.143	双向	192.168.27	3389	*	*	ТСР	放行		DESKTOP-8	2022-04-25	编辑删除
Ubuntu18-tcp	双向	×	*	*	*	TCP	MELL			2022-01-05	编辑删除

步骤 4. 进入一键封锁 IP 页面,编辑相关信息,点击<确定>。

规则名称	封锁IP
*封锁IP	192.168.1.0/24 • 例如: 192.168.1.1 192.168.1.1/24 192.168.1.1-192.168.1.255 "/"表示子网掩码、"-"表示IP段、多个IP需把 输入
应用终端	已选择终端(2) x

参数	说明
规则名称	长度为 1~30 位,支持中文、英文、数字、"_"、"-"、"·"。
封锁 IP	设置终端禁止访问的 IP (被封锁的 IP 也无法访问终端)。可设置多个,用回车 分隔,例如: 192.168.1.1、192.168.1.0/24、192.168.1.1-192.168.1.254。



参数	说明
应用终端	封锁规则应用的终端。点击 <选择终端>, 设置规则应用的终端。

15.1.1.1.3 一键关闭端口

当需要禁止使用终端的指定端口,可设置一键关闭端口。操作方法如下:

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"响应处置>微隔离",选择混合模式。

步骤 3. 选择终端规则页签,点击<一键关闭端口>。

微隔离 对不同业务之	如隔离 14不同业务之间进行流量隔离并精确阻断非法流量											~	0
终端规则	标签规则												
规则名称:	请输入规则	则名称		方向: 请选择		~					查询	重置	~
新増规则	一键封	锁IP	一键关闭端口	导入 导出		禁用	删除					0 8	0
规	名称 ♀	方向 🗘	本地IP ≎	本地端口 🗘	远程IP ≎	远程端口 🗘	协议 ♡	处理方式 ♀	启用状态♡	应用终端	添加时间	操作项	
test	27.143	双向	192.168.27	. 3389	*	*	TCP	放行		DESKTOP-8	2022-04-25	编辑 删除	ŧ
Ubu	untu18-tcp	双向	*	*	*	*	TCP	阻止			2022-01-05	编辑删除	15

步骤 4. 进入一键关闭端口页面,编辑相关信息,点击<确定>即可关闭该终端的端口。

则名称	关闭端口	
讨锁端口	443 22	•例如: 445 多个端口换行输入
立用终端	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	

参数	说明
规则名称	长度为 1~30 字符,支持中文、英文、数字、"_"、"-"、"."。
封锁端口	例如 445,输入多个端口请用回车分隔。
应用终端	选择规则应用的终端。点击 <选择终端> ,设置规则应用的终端。



15.1.1.2 标签规则

标签规则是指对某一标签下的终端设置微隔离规则,包括微隔离规则、一键封锁 IP 以及一键关闭端口。 步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"响应处置>微隔离",选择**混合模式**, 选择**标签规则**页签。

步骤 2. 可执行以下操作。

- ●选择标签(如 Linux),点击<新增规则>,可对标签下的终端新增微隔离规则。
- ●选择标签(如 Linux),点击<一键封锁 IP>,可对标签下的终端设置一键封锁 IP。

●选择标签(如 Linux),点击<一键关闭端口>,可关闭标签下的终端的相应端口。

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						۲	混合模式	~ (2)
终端规则标签规则									
Linux 日设置 4 个規則 日关联 0 个终端 (回看)	新增规则	鍵封锁IP 一個	建关闭端口	导入有	出 启用	禁用	副除		Q () # 0
PC 已设置 0 个规则	规则名称 💲	方向 🗘	本地端口 ◊	远程地址 🕽	远程端口 🗘	协议 🗘	启用状态 🗘	添加时间	操作项
已关联 15 个终端 [查看]	z	入站	445	*	*	所有		2022-06-2	
数据库服务器 已设置 0 个规则 已关联 1 个终端 (壹看)	555666	入站	33445	*	*	所有		2022-06-0	
BBS	33333	双向	*	BBS CMS	*	所有		2022-06-0	
已设置 0 个规则 已关联 0 个终端 [查看]	123	入站	445	CMS	22222	所有		2022-06-0	

15.1.1.3 其他操作

以租户角色登录主机安全系统管理平台,在导航栏选择"终端管理>微隔离",选择混合模式,可执 行以下操作:

- ◆ 点击<**导出**>,可导出微隔离规则。
- ◆ 点击<**导入**>,选择微隔离规则文件(已导出的微隔离规则文件),即可导入微隔离规则。
- ◆ 勾选规则(可勾选多个),点击<**启用**>,在弹出的对话框中点击<**确定**>,可批量启用微隔离规则。
- ◆ 勾选规则(可勾选多个),点击<**禁用**>,在弹出的对话框中点击<**确定**>,可批量禁用微隔离规则。
- ◆ 勾选规则(可勾选多个),点击<**删除**>,在弹出的对话框中点击<**确定**>,可批量删除微隔离规则。



<mark>做隔离</mark> 时不同业务	5之间进行流量	國高并精	确阻断非法流量							0	混合模式	~ 0
终端规则	标签规则	IJ										
规则名	称: 请输入	规则名称		方向:	请选择方向		~				查询	重置 >
新增耕	见则 ——1	建封锁IP	一键关闭端口	导入	导出	启用	禁用	删除				0 🗄 🍥
▲共36	5 项,已选择	2项	重置									全选当页 反选当页
	规则名称 🗘	方向 🗘	本地IP ≎	本地端口 ≎	远程IP ≎	远程端口	协议 🗘	处理方式 \$	启用状态 ◊	应用终端	添加时间	操作项
X	—键封锁1	双向	*	*	10.20.28	*	所有	阻止		MYPC-ji	2022-08	编辑 删除
	192.168.2	双向	192.168	*	*	*	所有	阻止		MYPC-ji	2022-08	编辑 删除
	192.168.2	双向	192.168	*	*	*	所有	阻止		localhos	2022-08	编辑 删除

15.1.2 白名单模式

可以在白名单模式下配置标签规则,白名单内的规则默认放行,白名单外的规则默认阻止。

15.1.2.1 新增标签规则白名单

对某一标签下的终端设置微隔离规则白名单,操作方法如下:

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择 "终端管理>微隔离",选择白名单模 式,选择标签(如 PC),点击<新增规则>。

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						©	白名单模式	- <mark>1</mark>
PC 已设置1 个规则	2 3 新增规则 导	入 导出	启用	禁用	删除		请输入关键字		Q () 🗄 💿
已关联 15 个终端 [查看]	□ 规则名称 🗘	方向 0	本地端口 🗘	远程地址 🗘	远程端口 🗘	协议 🗘	启用状态 0	添加时间	操作项
数据库服务器 已设置 0 个规则 已关联 1 个终端 [查看]	test	入站	445	BBS 192.16	58 445	所有		2022-08- <mark>1</mark>	
BBS						共1条	€ 20条/页 ∨	۲ ا	》 前往 1 页

步骤 2. 在弹出的新增微隔离对话框中编辑相关信息,点击<确定>。



名称	请输入规则名称	• 最多输入30个字符,可用于说明规则的用途
V MC TH		
议类型	必填项,请选择协议类型 >	
见则类型	○ 双向 ● 入站规则 ○ 出站规则	• 入站(默认)表示远程主机访问本地主机,出站表示 本地主机访问远程主机
本地IP	IP支持IPv4, 输入形式例如: 192.168.1.1 192.168.2.1/24 192.168.3.1-192.168.3.255	 IP支持IPv4, 输入形式例如: 192.168.1.1 192.168.1.1/24 192.168.1.1-192.168.1.255 "水表示子网掩码、"-"表示IP段,多个IP需换行输入
5地端口	例如: 445	● 例如: 445 "*"表示所有端口、多个端口换行输入
* 远程IP	IP支持IPv4, 输入形式例如: 192.168.1.1 192.168.2.1/24 192.168.3.1-192.168.3.255	 IP支持IPv4, 输入形式例如: 192.168.1.1 192.168.1.1/24 192.168.1.1-192.168.1.255 "/"表示子网掩码、"-"表示IP段,多个IP需换行输入
远程端口	例如: 445	 例如: 445 *****志示斫有端口 多个端口 為介端 入

配置项	说明
规则名称	不超过 30 字符。
	◆ 入站:规则仅应用于入站连接,即访问本机的请求。
策略类型	◆ 出站:规则仅应用于出站连接,即本机向外发送的请求。
	◆ 双向:规则应用于入站及出站两种连接。
本地端口	本地主机的端口,例如 455,输入多个请用回车间隔,"*"表示所有端口。
	远程主机的 IP 地址,标签与 IP 必填一项,两者都填则两者均生效。
远程地址	◆ 选择标签:选择终端标签。
	◆ 填写 IP: 远程主机的 IP 地址、地址段、子网。
远程端口	远程主机的端口,例如 455,输入多个请用回车间隔,"*"表示所有端口。
协议类型	支持所有 TCP、UDP 和 ICMP。
状态	开启后规则白名单生效,关闭后规则白名单不生效。



15.1.2.2 其他操作

以租户角色登录主机安全系统管理平台,在导航栏选择"终端管理>微隔离",选择白名单模式,可 执行以下操作:

- ◆ 点击<**导出**>,可导出微隔离规则。
- ◆ 点击<导入>,选择微隔离规则文件(已导出的微隔离规则文件),即可导入微隔离规则。
- ◆ 勾选规则(可勾选多个),点击<**启用**>,在弹出的对话框中点击<**确定**>,可批量启用微隔离规则。
- ◆ 勾选规则(可勾选多个),点击<**禁用**>,在弹出的对话框中点击<**确定**>,可批量禁用微隔离规则。
- ◆ 勾选规则(可勾选多个),点击<**删除**>,在弹出的对话框中点击<**确定**>,可批量删除微隔离规则。

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						۲	白名单模式	~ 0
PC 已设置 2 个规则	新增规则	入导出	启用	禁用	删除		请输入关键字		Q ○ ☷ ⊚
· 已关联 15 个终端 [查看]	◀共2项,已选择2	项重置							全选当页 反选当页
数据库服务器 已设置0个规则	✓ 规则名称 🗘	方向 🗘 👘	本地端口 🗘	远程地址 🗘	远程端口 🗘	协议 0	启用状态 🗘	添加时间	操作项
日天联「介矮嫣」宣看」	☑ 白名单1	出站	443	BBS	443	所有		2022-08-2	
BBS 已设置 0 个规则 已关联 0 个终端 [查看]	🔽 test	入站	445	BBS 192.168	445	所有		2022-08-1	

15.1.3 黑名单模式

可以在黑名单模式下配置标签规则,对黑名单内的规则进行阻止。

15.1.3.1 新增标签规则黑名单

对某一标签下的终端设置微隔离规则黑名单,操作方法如下:

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"终端管理>微隔离",选择黑名单模式,选择标签(如 PC),点击<新增规则>。

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					0	黑名单模式		- 1 ©
2 PC 已设置 0 个规则)	启用	禁用	删除		请输入关键字		QOE	≣
已关联 15 个终端 [查看]	规则名称 ♀ 方向 ♀	本地端口 0	远程地址 🗘	远程端口 🗘	协议 🗘	启用状态 🗘	添加时间	操作项	
数据库服务器 已设置 0 个规则 已关联 1 个终端 [宣看]				暂无数据					
BBS 已设置 0 个规则 已关联 0 个终端 [查書]					共0条	20条/页 >	< 1	> 前往 1	I 页

步骤 2. 在弹出的新增微隔离对话框中,编辑相关信息(配置方法与微隔离配置相同),点击<确定>。



	请输入规则名称	• 最多输入30个字符,可用于说明规则的用途
义类型	必填项, 请选择协议类型	~
则类型	○ 双向 ● 入站规则 ○ 出站规则	 入站(默认)表示远程主机访问本地主机,出站表示本地主机访问远程主机
本地IP	IP支持IPv4, 输入形式例如: 192.168.1.1 192.168.2.1/24 192.168.3.1-192.168.3.255	 IP支持IPv4, 输入形式例如: 192.168.1.1 192.168.1.1/24 192.168.1.1-192.168.1.255 7/"表示子网炮码、"-"表示IP段,多个IP需换行输入
本地端口	例如: 445	• 例如: 445 **"表示所有端口、多个端口换行输入
远程IP	IP支持IPv4, 输入形式例如: 192.168.1.1 192.168.2.1/24 192.168.3.1-192.168.3.255	 IP支持IPv4, 输入形式例如: 192.168.1.1 192.168.1.1/24 192.168.1.1-192.168.1.255 "/"表示子网掩码、"-"表示IP段,多个IP需换行输入
程端口	例如: 445	 例如: 445 **"表示所有端口、多个端口换行输入

15.1.3.2 其他操作

以租户角色登录主机安全系统管理平台,在导航栏选择"终端管理>微隔离",选择**黑名单模式**页签,可执行以下操作:

- ◆ 点击<**导出**>,可导出微隔离规则。
- ◆ 点击<**导入**>,选择微隔离规则文件(已导出的微隔离规则文件),即可导入微隔离规则。
- ◆ 勾选规则(可勾选多个),点击<**启用**>,在弹出的对话框中点击<**确定**>,可批量启用微隔离规则。
- ◆ 勾选规则(可勾选多个),点击<**禁用**>,在弹出的对话框中点击<**确定**>,可批量禁用微隔离规则。
- ◆ 勾选规则(可勾选多个),点击<删除>,在弹出的对话框中点击<确定>,可批量删除微隔离规则。



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				◎ 黑名单模式	~ (2)
PC 已设置1 个规则	新增规则	入导出信	用禁用删除	请输入关键字		Q 0 🎛 🎯
已关联 15 个终端 [宣君]	▲ 共 1 项, 已选择 1	项 重置				全选当页 反选当页
数据库服务器 已设置 0 个规则	✓ 规则名称 🗘	方向 ♀ 本地端□	◎ 远程地址 ◎ 远程端口 ◎	协议 🗘 信用状态	50 添加时间	操作项
日大味「小珍嬌(宣言)	PC	入站 445	PC 192.168. 445	所有	2022-08-2	. 🗹 🔟
BBS 已设置 0 个规则 已关联 0 个终端 (音音)				共1条 20条质	[~ < 1	》 前往 1 页



15.2 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,并可在发现威胁后对主机间通信进行一键阻断。

租户可通过流量画像功能查看全景流量图,并支持通过以下方式进行流量筛选:

◆ 通过 Windows 服务器、Linux 服务器、PC 机三类主机和端口、时间进行过滤查看。

◆ 通过自定义模板,可按终端分组、终端标签、终端名称、终端 IP(且/或)过滤查看。

15.2.1 查看通信关系

租户可在此页面查看终端通信详情,包括终端通信关系图、终端间通信详情及终端全部通信详情。

15.2.1.1 查看终端通信关系图

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"响应处置>流量画像",进入终端展示页面。



步骤 3. 点击需要查看的终端的分组,可在此页面查看对应分组该终端的相关信息,和各个组之间的 通信信息。





步骤 4. 点击页面右上角的<**老版**>,即可切换为老版本流量画像的相关功能页面。





15.2.1.2 查看终端通信关系详情

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"响应处置>流量画像",点击右上角<老版>,进入终端展示页面。



步骤 3. 点击需要查看的终端,并选择**通信关系列表**页签,进入**通信关系列表**详情页面。租户可在此 页面查看该终端的所有通信详情,并可根据筛选条件进行通信查询。

通信关系图	通信关系列表								
本地IP:	请输入		远程IP:	请输入			本地端口:	请输入	
远程端口:	请输入		开始时间:	日 开始	台日期 -	结束日期		查询	RR
									۲
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
😫 出站	192.	64889	120.:7.3	80	TCP	2020-10-19	12:20:44	2020-10-19 12:20:44	1
and the second s									



15.2.2 自定义模板

通过自定义模板可查看对应分组或者标签的终端之间的通信关系。创建自定义模板的操作方法如下: 步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"响应处置≻流量画像",点击右上角<老版>,进入终端展示页面,点击右 侧自定义模板列表中的 十 图标。

自定义模板	
+	

步骤 3. 在弹出的对话框中输入自定义模板信息后点击<确定>,即可新增自定义模板。

自定义模板		×
	并且或者	
所属分组:	请选择	~
标签:	请选择	~
终端名称:	请输入终端名称,用;分隔,最多10个	1
IP:	请输入IP,用:分隔,最多10个	1
*策略名称:	请输入策略名称	
	取消	确定

步骤 4. 点击模板右上角的 ••• 图标, 租户可对自定义模板进行编辑和删除操作。

自定义模板	
+	
审计策略	编辑删除



15.3 文件推送

当租户需要下发文件、安装应用程序到终端上或者远程执行命令时,可以使用文件推送工具。 步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"响应处置>文件推送",进入文件推送页面。

- 1) 点击<**上传文件**>,选择文件(文件需要小于 20MB),即可上传文件。
- 2) 选择执行方式、执行权限及执行参数。
- 3) 点击<选择终端>,选择被推送的终端。

步骤 3. 点击<推送>即可成功推送该文件。

文件推送	
文件上传	▲ 上传文件 清空上传文件
	文件应该小于20M
下发后立即执行	
执行权限	● 最高权限 ○ 当前账号
执行参数	脚本或程序的执行参数
备注:	请输入备注信息不超过50个字符
推送给:	选择终端(0)
	推送

主叱远痒工传的又忤或脚平,又忤应小于 ZUMB。
如果需要立即执行文件,则开启立即执行。
状认最高权限,部分程序和脚本无法用 system 权限执行,则选用当前账号。
 却本需要执行时携带的参数。该功能必须在开启下发后立即执行选项后才可配置。 原可执行程序默认执行无需参数时则执行参数选项留空。 原可执行程序执行需要配置参数则执行参数选项填写实际参数。如原可执行程序运行命令为 push.sh filename 主机安全系统,则填写 filename 主机安全系统。



参数	说明
备注	关于此次文件推送的备注信息。
推送终端	点击 <选择终端>, 选择所需推送的终端。

♦ Windows 终端文件推送默认位置:

C:\Program Files \(x86\)\AppSecurity\主机安全系统\config\upload

◆ Linux 终端文件推送默认位置: /usr/local/appsecurity/主机安全系统 /config/upload

15.4 事件调查

能够对终端上的**文件、进程、网络连接、DNS 查询、端口监听、账户、启动项、计划任务**进行检索, 实现相关安全事件的调查。

15.4.1 搜索事件数据

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择 "响应处置>事件调查",输入关键字,点击<搜索>,即可搜索符合条件的事件信息。



15.4.2 配置数据采集

步骤 1. 点击页面右上方的<配置数据采集>。



请输入搜索内容	容							搜索
□ 全选 □ 文	文件	进程	网络连接	DNS查询	端口监听	□ 账户	启动项	🗌 计划



步骤 2. 点击状态列的开关可启用或关闭对应项目的数据采集功能。

☆ 配置数据采集			
类型	搜索结果	状态	操作项
文件	当文件创建,修改,删除时记录文件事件		设置
进程	当进程创建时记录进程事件		设置
网络连接	当连接外部IP端口时记录事件		设置
DNS查询	当查询外部DNS时记录事件		设置
端口监听	当进程创建监听端口时记录事件		设置
账户	当账户创建,提权时记录事件		设置
启动项	当启动项创建,删除时记录事件		设置
计划任务	当计划任务创建,删除时记录事件		设置

步骤 3. 点击对应项(例如文件)的<**设置**>。

步骤 4. 在弹出的对话框中编辑相关信息,点击<确定>,即可设置数据采集策略。



文件设置		×
采集文件:	lic:conf	
		·// 采集全部清填*号,多个对象用分号(:)分隔
Linux忽略文件:		
Linux忽略路径:	/root	
Linux忽略扩展名:		

取消

确定



16日志检索

报表:对事件趋势、病毒以及风险终端进行图表展示,支持导出各种类型报表。方便用户及时了解终端的防护信息。

日志检索是对记录系统以及终端的事件信息,包括防护日志、操作日志、运维日志等日志类型。支持 按照分类及关键字进行搜索。

日质检索不同角色拥有不同的操作权限。

◆ admin 用户和租户都具有查看各自操作日志的权限。

◆ 仅租户角色具有防护日志、运维日志、日志报表等权限。

16.1 防护日志

租户可在防护日志页面查看系统防护日志、网络防护日志、Web 应用防护日志及自动响应日志。

16.1.1 查看防护日志

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"日志检索>防护日志",设置查询条件(如时间、终端、分组、日志类型、 风险评级、概况等),点击<查询>,即可查询符合该条件的操作日志。

日志详情	统计分析								l.				
时间:	2023-10-12 00:00:00 - 2023-10-12 23:59:59	•	终端:	调输入终端名称 (IP)	~	分组:	请选择所属分组	~	日志类型:	请选择日志类型			~
风险评级:	请选择	~	概况:	请输入关键字 (操作IP, 日志类型, 描述)							查询	重置	母田 四

步骤 3. 点击》图标,可查看防护日志详情。

	终端名称	IP地址	日志类型	风险概况	风险评级	时间 🗘
>	(iii) HIRAMWONG8A70	1.0.00	违规外联防护	已检测到主机存在违规外连行为,探测地址:www.baldu.com,未处理	高风险	2022-11-04 10:18:49
>	(I) HIRAMWONG8A70	$\mathbf{h}_{ij} = (\mathbf{h}_{ij})^{(i)} (\mathbf{h}_{ij})^{(j)} (\mathbf{h}_{ij})^{(j)}$	违规外联防护	已检测到主机存在违规外连行为,探测地址: www.baldu.com,未处理	高风险	2022-11-03 16:58:17

步骤 4. 点击终端名称链接,可跳转至**策略管理**页面,详情请参考<u>策略管理</u>。

终端:	容器1()	~	概况: 请输入关键字 (操作IP, 日志类型, 描述) 查询	重置	导出日志 > 展开 >
终端名称	IP地址	日志类型	风险概况	风险评级	时间 ≎
) (1) 容器1	the families	病毒防护	发现恶意程序 C:\Users\admin\AppData\Roaming\快压\X86\vip.exe(TR/Crypt.Agent.gyhdn),未处理	高风险	2022-11-10 00:31:51

16.1.2 导出防护日志

点击<导出日志>,选择文件格式(支持 CSV 和 Excel),可将所查询的防护日志导出至本地。



时间:	2023-10-12 00:00:00	2023-10-12 23:59:59		终端:	请输入终端名称 (IP) ~	分组:	请选择所属分组 ~	日志类型:	请选择日志类型		
. 脸评级 :	请选择		~	概况:	请输入关键字 (操作IP, 日志类型, 描述)					査询 重置	1 - 导出
终	尚名称	IP地址	日志类型	X	险概况				风脸评级	时间 0 ₂	CSV
> (1)	MXJAUTO-PC	10.50	防端口扫描	1(0.50 🂵 🎦 发生端口扫描行为,已放行被扫描端口: 445,570	084			低风险	2023-10-12	EXCEL

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。

16.1.3 统计分析

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"日志检索>防护日志>统计分析",选择时间、终端、分组后,点击<重 新生成>按钮,即可查询符合该条件的防护日志统计分析结果。

间: 今日	~	终端: 请输入终于	幽名称 (IP)		~ 分	1组: 词选择所	佩分组		×				重新生质	起
风险数		风脸终端数				事件等级分布				风险终端TOP:	3 [5]			
95		1			٩	<u>E</u> ,			2	1 MXJAU	TO-PC(10.50.	38.213)		
同比 1 🔻		同比 2 💌			~	低风脸 95		高风脸 0	已失陷 0					
系统防护														
	 ○ 系統登示防护 ○ 暴力破解防护 ○ 暴力破解防护 ○ 进程黑名単 ○ 文件の時間提換 		○ 勤素深度防护 ○ 进程白名単 ○ 挖矿防御 ○ 弹震拦截	0 0 0	1 0.8 0.6 0.4 0.2									
\sim	• 193 408 HO ST.				0 00:0	00 02:00	04:00	06:00 (10:00 10:00	12:00 14:00	16:00	18:00	20:00	22:00
eb应用防护														
\frown	○ 防CC攻击 0				1 0.8									
息数	 网站漏洞防护 网站漏洞防护 网站法院把制 				0.6									
0	 网页防篡改 0 				0.4									

步骤 3. 在左侧导航栏选择"日志检索>防护日志>统计分析",点击<重置>按钮,即可重置该结果为 默认时间统计结果。

 前限 ④日 (月日 <li(月日< li=""> <li(月日< li=""> (月日 (月日</li(月日<></li(月日<>	日志详情 统计分析									
Nake Platikat Rultikat F#f980/f Example Example Rultikatory (C Modulation (C) Modulation (C) <th>时间: 今日</th> <th>0</th> <th>终端: 请输入终端各称 (IP)</th> <th>×</th> <th>分组:</th> <th>请选择所属分</th> <th>相</th> <th>~</th> <th></th> <th>重新生成 重置</th>	时间: 今日	0	终端: 请输入终端各称 (IP)	×	分组:	请选择所属分	相	~		重新生成 重置
A統防护 0 系統原導励計 0 0 0 系統原導励計 0 0 0 0 ● 東力電解防 0 0 0 0 ● 東力電解防 0 0 0 0 ● 建築自宅集 0 0 0 0 ● 建築自宅集 0 0 0 0 ● 東田電 0 0 0 0 ● 東田電 0 0 0	风能数 95 同比 1 ▼	()	风胞纬编数 1 同比 2 ▼	٢	事件	等级分布 低风脸 95	王 高风脸 0	記 失陥 0	风始終終TOP3 民 愈 MXJAUTO-PC(10:50:38:213)	95
	系统防护 (一) 0	 系統登录防护 の 系統登录防护 の 新力磁解防护 近極風名拳 0 文件協同监控 0 	 私未完成部件 注照自名单 26755章 7零世紀 	1 0 0.8 0 0.6 0 0.4 0 0.2						

16.2 操作日志

租户可在**操作日志**页面查看用户登录日志、修改密码日志、策略管理日志、分组标签日志、移动存储 日志、告警配置日志、终端解绑日志、启停防护日志及短信发送日志。



16.2.1 查询操作日志

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"日志检索>操作日志",设置查询条件(如时间、状态、日志类型、概况 等),点击<**查询**>,即可查询符合该条件的操作日志。

时间: 2023-10	0-12 00:00:00 2023-10-12 23:59:59	 状态: 请选择状态 	✓ 日志美型: 请选择日志类型	✓ 概况: 请输入关键字 (操作ⅠP, 日志类型, 描述)	
		1		重询	重置导出区
用户 0	操作IP ≎	日志类型	描述	Bylia) 🗘	状态
autotest	10.23.72.115	日志操作	读取了防护日志数据记录	2023-10-12 14:26:21	成功
autotest	10.23.72.115	日志操作	读取了防护日志数据记录	2023-10-12 13:59:21	成功
autotest	10.23.72.115	日志操作	读取了防护日志数据记录	2023-10-12 10:20:46	成功
autotest	10.23.72.115	日志操作	读取了防护日志数据记录	2023-10-12 09:45:45	成功
autotest	10.23.72.115	日志操作	读取了防护日志数据记录	2023-10-12 09:23:16	成功
autotest	10.23.72.115	日志操作	读取了防护日志数据记录	2023-10-12 09:16:41	成功

16.2.2 导出操作日志

点击<导出日志>,选择文件格式(CSV或 Excel),可将所查询的操作日志导出至本地。

时间:	2023-10-	12 00:00:00 - 20	23-10-12 23:59:59	③状	(态: 请选择状态		/ 日志类型:	请选择日志类型	概况:	请输入关键字(操作IP,日志类型	1, 描述)	
											<u>金狗 重き</u>	E 1 寻出 R
用户		操作IP 0			日志类型	描述				时间 0		CSV
auto	otest	10.23.72.115			日志操作	读取了防	户日志数据记录			2023-10-12 14:26:21	2	EXCEL
i.					•	支持导b	H CSV	「格式和 Excel 格式。				
	ľ		•	支持	寺最多导	出 10 万条,当	前总额	数超过 10 万条则导	出最	新的 10 万条	0	

16.3 运维日志

租户可在运维日志页面查看终端日志、性能监控日志、外设管控日志及运维日志。

16.3.1 查询运维日志

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"日志检索>运维日志",设置查询条件(如终端、分组、时间、日志类型、 概况等),点击<查询>,即可查询符合该条件的运维日志。

时间:	2023-10-12 00:00:00 - 2	2023-10-12 23:59:59	④ 终端:	请输入终端名称 (IP)	~	分组:	请选择所属分组	~	日志类型:	请选择日志类型		~
概况:	请输入搜索关键字(类型、科	取況)									查询	1日 号出区
	终端名称	IP地址	日志类型	概況				1			<mark>2</mark> 时间 0	
>	DESKTOP-FSHBSE6	10.23.72.160	终端升级	版本升级,升级前的版本 3.0.7.104							2023-10-	12 14:10:01
>	DESKTOP-FSHBSE6	10.23.72.160	弱口令扫描	系统中有账号存在弱口令: admin							2023-10-	2 10:48:48

16.3.2 导出运维日志

点击<导出日志>,租户可将所查询的运维日志导出至本地。



时间:	2023-10-12 00:00:00	2023-10-12 23:59:59	⑤ 终端:	请输入终端名称 (IP)	~	分组:	请选择所属分组	~	日志类型:	请选择日志类型		~
概况:	请输入搜索关键字(类型、	概況)									查询	重置 导出 5
	终端名称	IP地址	日志类型	概况							时间 🗘	CSV
>	DESKTOP-FSHBSE6	10.23.72.160	终端升级	版本升级,升级前的版本 3.0.7.104							2023-10	-12 EXCEL
F	- 1			◆ 支持	序导出	CS	V格式和Ex	cel 格式。				
	1		士性	旦夕巳山 10 百夕) 14	<u> </u>	5 米か キアンナ 10 -	てタ 回 巳 山	山里文	にわれ 10 五	.夕	

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。

篡改分析 16.4

需要管理员为租户启用防篡改许可后才具备篡改分析功能。

租户可对数据篡改事件,篡改结果和篡改目标源进行分析,展示攻击防护次数和高危风险终端 TOP10。 操作方法如下:

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"日志检索>篡改分析",进入篡改分析页面,选择时间,点击<生成报表>, 可生成篡改分析报表。

篡改分析报表内容包括防篡改数据、网站篡改分析、篡改源分析、攻击防护次数统计、高风 险终端 TOP10、总体情况。

选择时间	2022-07-15	J.S.	2022-08-15	0	生成报表	导出 ∨						
防篡改数据												
1												
0.8 -												
0.6 -												
0.4 -												
0.2 -												
0.0	5 2022-07	-18	2022-07-21	2	022-07-24	2022-07-27	2022-07-30	2022-08-02	2022-08-05	2022-08-08	2022-08-11	2022-08-14

网站篡改分析

步骤 3. 点击<导出>,选择文件格式(支持 PDF、HTML 和 DOC),可将篡改分析报告导出至本地。


前 🗐 2022-07-15 -	2022-08-15	生成报表	导出~			
篡改数据			PDF HTML DOC			
0.8						
0.6 -						
0.4						

16.5 日志报表

租户可在日志报表页面进行报表导出,或者报表订阅操作获取对应报表信息。

16.5.1 导出报表

- 步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择"**日志检索≻日志报表**",选择**报表导** 出页签。
- 步骤 2. 编辑报表标题(不超过 30 字符),选择**导出文件**类型(支持 PDF、HTML 和 Word),选择 时间,点击<**立即导出**>,即可将所选时间段的日志报表导出至本地。

报表导出	报表订阅	
* 报表标题:		
选择时间:	2022-07-16 - 2022-08-15	
导出文件:	PDF HTML Word	
	立即导出	

16.5.2 订阅报表

为方便租户及时了解终端防护状态信息,主机安全系统支持订阅报表功能。开启订阅报表功能后,系统会定期发送终端风险报表至配置的收件人邮箱。

设置报表订阅的操作方法如下:

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"日志检索>日志报表",选择报表订阅页签。

步骤 3. 开启**订阅开关**,配置报表标题、导出类型、执行时间及收件人邮箱,点击<保存>。



发供答害前	注 个人由心 修改	
汉门相同的		
订阅开关:		
报表标题:	xty	
导出类型:	○ 日报 ● 周报 ○ 月报	
*执行时间:	每天 14:51:11	×
收件人邮箱:	请输入收件人邮箱	



17 终端全览

admin 用户在终端全览页面可查看终端的详细信息,并可以登录租户账号对终端进行管理。

仅 admin 用户角色具有终端全览权限。

17.1 查看终端详情

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"终端全览"进入终端列表页面。

步骤 3. 可查看所有终端的详细信息,包括租户名、终端名称、IP 地址、MAC 地址、操作系统、终端 版本、防护状态及操作项等。

导出				谓输	入关键字	Q	0 ⊞ ⊚
租户名 ◊	终端名称 ⇔	IP地址 ≎	MAC地址	操作系统 ≎	终端版本 🗘	终端状态下	操作项
test	(1) localhost.localdomain	15mi Sintali	Q*******	CentOS Linux 7 (Core)	3.0.3.104	防护中	前往租户
test	(1) 容器1	Version Com-	Q	Windows 7 Ultimate Edition 32-bit	3.0.3.107	防护中	前往租户
test	٢	1	0 -00000D	SUSE Linux Enterprise Server 11 (x86_64)	3.0.2.104	离线	前往租户
test	(ii) ADMIN-PC	1	9 20	Windows 7 Ultimate Edition 64-bit	3.0.2.106	离线	前往租户
test	BOB-OFFICEPC	1) (m. 4)	0 82	Windows 10 Professional 64-bit	3.0.2.108	离线	前往租户
test	(i) centos5.0-x64-2.6.18-8	1-jin'n-jer	06E	CentOS release 5 (Final)	3.0.3.104	已卸载	前往租户
test	(i) CentOS7	19	o to	CentOS Linux 7 (Core)	3.0.3.104	离线	前往租户
test	DESKTOP-55U53T2	1	0 AA	Windows 10 64-bit	3.0.2.106	离线	前往租户
test	DESKTOP-64NLTVC	1 ⁴	$\mathbf{C} = \{ \mathbf{F} \mid \{ \mathbf{F} \mid \mathbf{e}_{\mathbf{F}} \mid \mathbf{e}_{\mathbf{F}} \} \mid \mathbf{C} \}$	Windows 10 64-bit	3.0.2.106	离线	前往租户

17.2 前往租户

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"终端全览"进入终端列表页面。

步骤 3. 选择需要登录的终端,点击右侧**操作项**的前往租户,即可使用该租户账号登录主机安全系统 管理平台对终端进行管理。

导出					请输入关键字	Q	0 = 0
租户名 ≎	终端名称 🗘	IP地址 ≎	MAC地址	操作系统 ⇒	终端版本 🗘	终端状态『	操作项
test	(a) localhost.localdomain	10	Quality and the second second	CentOS Linux 7 (Core)	3.0.3.104	防护中	前往租户
test	(#) 容器1	19,	(=====================================	Windows 7 Ultimate Edition 32-bit	3.0.3.107	防护中	前往租户
test	۵	10 - 34.19	() →	SUSE Linux Enterprise Server 11 (x86_	54) 3.0.2.104	离线	前往租户
test	(iii) ADMIN-PC	10	s	Windows 7 Ultimate Edition 64-bit	3.0.2.106	离线	前往租户

17.3 导出

步骤 1. 以 admin 用户登录主机安全系统管理平台。



步骤 2. 在左侧导航栏选择"终端全览"进入终端列表页面。

步骤 3. 选择需要导出的资产,点击<**导出**>,即可完成信息导出。

	导出 ②				调节	输入关键字	C	ຊ ປ 8≣ ⊚
C)当前页已选择3项,未选择17	'项 全选当页 反选当页						重置
	租户名 ◊	终端名称 🗘	IP地址 ♡	MAC地址	操作系统 🗘	终端版本 🗘	终端状态『	操作项
	test	(1) localhost.localdomain	16 Malaylia	d = (0,1) + (d + 2)	CentOS Linux 7 (Core)	3.0.3.104	防护中	前往租户
	Test	⑧ 容器1	tylid projecti	Too and 10 p (6	Windows 7 Ultimate Edition 32-bit	3.0.3.107	防护中	前往租户
	test	۵	$\gamma_{\rm c} \gamma_{\rm c} = 0, 100$, the sphere $m_{\rm c}$	araya asiste (s. do	SUSE Linux Enterprise Server 11 (x86_64)	3.0.2.104	离线	前往租户

	◆ 导出格式为 csv
•	不选择资产则默认导出全部内容



18 多级中心

多级中心用于下级中心连接上级中心,上级中心可以查看所有下级中心的部署情况以及风险数据。设置多级中心可减少主服务器的压力,减轻带宽占用,降低管理的成本;并解决分支机构、异地联动、多部门协同的难题。

仅 admin 用户具有多级中心操作权限。

18.1 查看中心详情

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"多级中心"进入多级中心总览页面,点击右上角<详情>。

多级中心					详情
本中心名称: 10-20-178-151	版本号: 3.0.3.103	3 39	2675	35	0 0
上级连接状态: 未连接	IP地址: 10.20.178.151	在线终端 离线终端	病毒文件	高危漏洞	异常登录 web请求防护
配置上級 關除				请输入关键字	Q () III ()
下級中心名称	离线终端 病毒文件 高危漏洞	异常登录 web请求	防护 版本号	最后通讯时间	操作项

步骤 3. 进入**多级中心详情**页面,可查看该中心数据信息、病毒趋势、终端-病毒排行、终端-漏洞排行、 威胁 IP-TOP5 及事件类型占比等数据。





18.2 配置上级中心

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"多级中心"进入多级中心总览页面,点击<配置上级>。

多级中心					详情
本中心名称: 10-20-178-151	版本号: 3.0.3.103	3	39 2675	35 0	0
上级连接状态: 未连接	IP地址: 10.20.178.151	在线终端	离线终端 病毒文件	高危漏洞 异常登录	web请求防护
配置上级 删除				请输入关键字	Q () 🏭 💿
□ 下级中心名称 ۞ 在线IP 在线终端	离线终端 病毒文件 高危漏	洞 异常登录	web请求防护 版本	号 最后通讯时间	操作项

步骤 3. 在弹出的对话框中输入上级控制中心地址和端口,点击<连接上级>,即可配置上级中心。

配置上级			×
* 上级控制中心地址	192.168.27.142		
* 上级控制中心端口	443		
		取消连接	连接上级

18.3 其他操作

- 步骤 1. 以 admin 用户登录主机安全系统管理平台。
- 步骤 2. 在左侧导航栏选择"**多级中心**",进入**多级中心**总览页面,可对下级中心进行编辑、查看及 删除操作。

勾选多个下级中心后点击列表上方的**<删除**>,可进行批量删除操作。

配置	让级 删除								请输入关键字	C	0 ≣ ⊚
《 当前	前页已选择1项,未	选择0项 重	置							全进	当页 反选当页
 Image: A start of the start of	下级中心名称 🗘	在线IP	在线终端	离线终端	病毒文件	高危漏洞	异常登录	web请求防护	版本号	最后通讯时间	操作项
~	linux142	192.168.27.142	0	2	0	0	0	0	3.0.1.4	2022-08-15 16: 35:36	
								共1	条 20条/页 ~	< 1 >	前往 1 页



19 系统管理

系统管理是指对系统的维护以及对系统资源进行管理,使系统更好地适配实际使用场景。

在系统管理页面,不同角色拥有不同的操作权限。

- ◆ 仅 admin 用户具有控制端系统管理权限。
- ◆ 仅租户角色具有客户端系统管理权限。

19.1 Admin 账户系统管理

admin 用户可在**系统管理**页面进行客户端及库升级、管理平台升级、Windows 补丁库、平台管理、个性化等操作。

19.1.1 客户端及库升级

admin 用户可在此页面查看客户端及特征库当前版本信息,并可上传离线包进行离线升级或者在线升级特征库。

19.1.1.1 在线升级

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>客户端及库升级",进入客户端及库升级页面。

步骤 3. 点击<在线升级>,选择需要升级的库,点击开始升级即可完成库的在线升级。

and the state of the						±.	高浅升级 の 在线升付
备广场 似文符易现开版		在线升级		×	and the second se		3
() Windows客户端	(A) Linux_X86架构64位客户如	为您检测到以下可升	级版本		(A) Linux_ARM架构客户端		
版本: 3.0.7.104 最近升级: 2023-10-12.09:19:23	版本: 3.0.7.104 最近升级: 2023-10-12.09-19:49	● 已选择 2 项	全选当页 反选当页	重素	版本: 3.0.7.104 最近升级: 2023-10-12.09:19-26		
	_	☑ 库名称	当前版本	最新版本			
(1) Linux_MIPS架构客户端		☑ 病毒库	23.8.2.20	23.10.11.20			
版本: 3.0.7.104 最近升级: 2023-10-12.09:19:37		☑ 威胁情报	库 23.9.11.20	23.10.11.19			
征库 每天 03:45:00自动升级 设置				5 取消 开始升级			
③ 病毒库	阿开版 6 系统漏洞库	•	入侵检测库	•	▲ 威胁情报库	可升级	
版本: 23.8.2.20 最近开版 - 2023_10_12.09:20:14	版本: 23.9.18.17 最近升级: 2023-10-12.09:22:57		版本: 23.10.7.17 前近开版: 2023-10-12.09:23		版本: 23.9.11.20 普近开版: 2023-10-12.09:50:15		

步骤 4. 通过每个特征库或者客户端方框历史记录,可以查看升级成功或者失败的对应记录。



客户端 仅支持高线升级							
 Windows客户端 题本: 3.0.7.104 最近升级: 2023-10-12 09:19:23 	 (▲) Lin 版本: 3 最近升级 	nux_X86架构64位客/ 0.7.104 E: 2023-10-12 09:19:49	□端	(入) Linux_X86架 版本: 3.0.7.104 最近升级: 2023-10-1;	构32位客户端 2 09:19:53	 Linux_ARM架构客户端 版本: 30.7.104 最近升级: 2023-10-12 09:19:26 	
 Linux_MIPS架构客户端 基本: 3.0.7.104 最近升级: 2023-10-12.09:19:37 							
Linux_X86架构64位客户	端			×			
历史升级记录							
升级时间	升级前版本	当前版本	方式	是否成功			
2023-10-12 09:19:51	3.0.7.104	3.0.7.104	离线升级	● 升级成功			
2023-10-11 13:56:05		3.0.7.104	离线升级	● 升级成功			
2023-10-11 13:44:16		1.771	离线升级	❷ 升级失败			
	共3条 <	1 > 2	0条/页 ~	前往 1 页			

关闭

19.1.1.2 离线升级

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>客户端及库升级",进入客户端及库升级页面。

步骤 3. 点击<离线升级>, 上传文件, 即可完成客户端及库的离线升级。

客户跳 仅支持离线升级	离线升线	ž	×	the Carlos and Carlos
(4) Windows客户端	(① Linux_X86架构64位客户氧		(1) Linux_ARM架构客户端	
版本: 30.7.104 最近升级: 2023-10-12 09:19:23	徽本: 307.104 最近升级: 2023-10-12 09:19:49	1	版本 3.0.7.104 顺近升级: 2023-10-12.09:19-26	
(①) Linux_MIPS架构客户端		将升级包拖拽至此处,或点击上传		
該本: 3.0.7.104 最近升级: 2023-10-12 09:19:37		取消	开始升级	
特征库 每天 03:45-00自动升级 设置				
③ 病毒库	□HU ③ 系统漏洞库	• 入侵检测库	▲ 威胁情报库	可升级
版本: 23.8.2.20 最近升级: 2023-10-12.09:20:14	顺本: 23,9.18.17 截近升级: 2023-10-12.09-22:57	版本: 23.10.7.17 最近开模: 2023-10-12.09:23:51	版本: 23.9.11.20 最近升级: 2023-10-12.09:50-15	



品>网络安全基础产品>安全防护产品>天翼云主机安全系统(主机安全系统)",点

击"版本软件",选择对应中心架构后下载安装升级一体包。

19.1.1.3 自动升级

步骤 1. 以 admin 用户登录主机安全系统管理平台。

- 步骤 2. 在左侧导航栏选择"系统管理>客户端及库升级",进入客户端及库升级页面。
- 步骤 3. 点击<自动升级设置>,可以设置是否在线升级、执行时间、升级代理,点击确定按钮即完成 了自动升级设置。

全部 可升级 🕖							1	
客户端 仪支持直线升级		自动升级设置		×		企 南 田	升级 ④ 在线升级 🔘 🛛	自动升级设置
 Windows客户端 ※本. 30.7.104 	▲ Linux_X86架构64位客户端 ^{業本:} 307.104	● 当前平台可以正常	常访问升级服务器	到武网络 2	(A) Linux_ARM架构客户端			
最近升载: 2023-10-12 09:19:23	最近升级: 2023-10-12.09:19:49	在线升级: 💽 硫	確平台或代理服务器支持访问升级服务器	Ţ	臺近升級: 2023-10-12 09:19:26			
Linux_MIPS架构客户端 邮本: 307104		执行时间: 每天 03 升级代理: ()	3:45:00	2				
最近升级: 2023-10-12 09-19-37		IP地址:	1.1.1.1					
特征库 每天 03:45:00自动升级 设置		端口号:	11					
() 病毒库	③ 系统漏洞库	用户账号:	: 請輸入用户账号		△ 威胁情报库	3774		
版本: 23.8.2.20 截近升级: 2023-10-12.09:20:14	版本: 23.9.18.17 最近升级: 2023-10-12.09:22:57	密码:	請输入問問		原本: 23.9.11.20 最近升级: 2023-10-12.09.50:15			
			取消	确定	3			
送 网马库	of 弱口令库	(<u>)</u>	Linux驱动库					
版本: 23.9.1.19 最近升级: 2023-10-12.09-20:15	版本: 22.11.24.15 最近升级: 2023-10-12.09-20:25	题。	本: 23.10.7.10 近升级: 2023-10-12.09:23:48					

步骤 4. 点击<测试网络>,可以测试当前平台是否可以正常访问升级服务器。

	A		
当前 ³	2台可以正常访问升级服务器		测试网络
在线升级:	确保平台或代理服务器支持访	问升级服务器	
执行时间:	每天 03:45:00		~
升级代理:			
			To manager

19.1.1.4 可升级

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>客户端及库升级",进入客户端及库升级页面。

步骤 3. 选择"可升级",即能看到可升级的客户端及库。



			-14 P=25.43	中在线开级
③ 病毒库	◎丹級	向升级		
版本: 23.8.2.20 最近升级: 2023-10-12 09:20:14	版本: 23.9.11.20 最近升级: 2023-10-12.09:50:15			

步骤 4. 右上角有可升级标识的说明此库可以进行升级。

全部	可升级 2		
特征库	每天 03:45:00自动升级 设置		
3	病毒库	▲ 威胁情报库	可升级
版本: 最近升	23.8.2.20 针级:2023-10-12 09:20:14	版本: 23.9.11.20 最近升级: 2023-10-12 09:50:15	

19.1.2 管理平台升级

admin 用户可在此页面查看平台当前版本信息,并可上传离线包对平台进行离线升级。

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择 "系统管理>管理平台升级"进入管理平台升级页面。点击<选择离线包>, 系统将进行自动清理缓存。



注意事项

- 升级过程平台任务将不能正常进行,请确保升级过程中没有重要的任务进行。
- 升级过程中,请勿刷新浏览器,避免刷新导致升级失败。
- 升级完成后,系统将自动重启。
- 离线升级安装包仅支持.tar.gz格式。



步骤 3. 缓存清理完毕后,在弹出的对话框中点击<点击上传>,上传离线包后即可进行平台离线升级。

离线升级	×
 升级操作前,建议您提前备份数据库或者备份的 升级大概需要 10 分钟左右,升级过程中请勿重 	服务器镜像文件。 這复操作。
② 操作成功	
取消 点击上传	

19.1.3 Windows 补丁库



用户可在 Windows 补丁库管理页面查看补丁详情,并进行在线更新补丁及离线更新补丁操作。

19.1.3.1 查看已下载补丁

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>Windows补丁库管理",选择已下载补丁页签。

- 步骤 3. 进入已下载补丁页面,用户可查看已下载的漏洞补丁列表。同时可在此页面查看漏洞分类及 漏洞补丁详情,并对漏洞补丁进行查询、忽略、删除及取消忽略操作。
 - 点击操作项列中的</>
 ②图标,在弹出的对话框中点击<确定>,可忽略漏洞补丁。
 - 点击**操作项**列中的^会图标,在弹出的对话框中点击<确定>,可取消忽略漏洞补丁。
 - 点击操作项列中的^Ⅲ图标,在弹出的对话框中点击<确定>,可删除漏洞补丁。
 - 勾选多个补丁后点击列表上方的<**忽略**>、<**取消忽略**>或<**删除**>,可进行批量忽略、批量取 消忽略及批量删除操作。



已下载补丁	在线更新补丁 离线更新补丁					
发布日期:	百 开始日期 - 结束日期 下载日期:	崮 开始日期	- 结束日期	关键字: 清	俞入关键字	
忽略状态:	请选择				查询	重置へ
高危漏洞	可选漏洞 忽略 取消忽略 删除					已下载补丁: 80个
漏洞补	丁描述	发布日期	补丁大小	适用系统	下载日期	操作项
2022-j	适用于 Windows 10 Version 1507 的 05 服务堆栈更新,适合基于 x6	2022-05-10	11.60MB	win10	2022-05-20	0
2022-j	适用于 Windows 10 Version 1909 的 05 累积更新,适合基于 x64 的	2022-05-10	563.35MB	win10	2022-05-20	0 1
2021-j	适用于 Windows 10 Version 2004 的 12 累积更新,适合基于 x64 的	2021-12-14	602.96MB	win10	2022-01-21	
2021-j	适用于 Windows 10 Version 1607 和 Windows Server 2016 的 09	2021-09-13	11.50MB	win2k16	2022-01-21	0 1
2021-j	适用于 Windows 10 Version 1809 和 Windows Server 2019 的 08	2021-08-09	13.60MB	win2k19	2022-01-21	
2021-j	适用于 Windows 10 Version 2004 和 Windows 10 Version 20H2 和	2021-08-09	14.50MB	win10	2022-01-21	0 🔟
2021-j	适用于 Windows 10 Version 1909 的 08 服务堆栈更新,适合基于 x6	2021-08-09	14.40MB	win10	2022-01-21	0 1
2021-j	适用于 Windows 10 Version 1803 的 05 服务堆栈更新,适合基于 x6	2021-05-11	13.20MB	win10	2022-01-21	

19.1.3.2 在线更新补丁

主机安全系统管理中心可连接互联网时,可以在线更新补丁。操作方法如下:

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>Windows补丁库管理",选择在线更新补丁页签。 步骤 3. 进入在线更新补丁页面,点击<下载补丁>。

已下载补丁	在线更新补丁	离线更新补丁
EDR管理中	心可联互联网时	,建议在线更新补丁库
1 下载补	Ţ	
在线下载	一小坊	
下载	补丁	
已下载补	丁80个,可在已下载	补丁 查看。

步骤 4. 在弹出的对话框中选择操作系统类型及漏洞级别,点击<确定>。

下载补丁		×
*操作系统类型:	■ 全选	
	Windows XP Windows 7 Vindows 8	
	Windows 10 Windows Server 2003	
	Windows Server 2008 Vindows Server 2012	
	Windows Server 2016 Windows Server 2019	
	○ 仅32位 ○ 仅64位 ● 32位和64位	
*漏洞级别:	☑ 高危	
	取消 确定	



19.1.3.3 离线更新补丁

主机安全系统管理中心无法连接互联网时,可离线更新补丁库。操作方法如下:

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>Windows补丁库管理",选择离线更新补丁页签。 步骤 3. 进入离线更新补丁页面,点击<下载>,下载离线下载器。

已下载补丁	在线更新补丁	离线更新补丁	
EDR管理中	心无法联互联网	1时. 建议离线更新补下网	车
1 下载离线	线下载器		
下载后,	可通过下载器离线下	载补丁包	
下雪	武		
2 上传离线	线补丁包		
上传离线	詠丁包到管理中心		
上传达	文件		

步骤 4. 下载器下载成功后,可通过下载器离线下载补丁包。

- 1) 解压下载后的压缩包。
- 2) 在解压后的文件中双击 "vuld.exe" 文件运行下载器程序。

名称	修改日期	类型	大小
d	2022/6/20 16:01	文件夹	
1 7z	2022/6/20 16:00	应用程序	785 KB
libcrypto-1_1.dll	2022/6/20 16:00	应用程序扩展	2,064 KB
libssl-1_1.dll	2022/6/20 16:00	应用程序扩展	363 KB
litexml.dll	2022/6/20 16:00	应用程序扩展	1,330 KB
Mfc100.dll	2022/6/20 16:00	应用程序扩展	4,295 KB
msvcp100.dll	2022/6/20 16:00	应用程序扩展	412 KB
Msvcr100.dll	2022/6/20 16:00	应用程序扩展	756 KB
runlog	2022/6/20 16:01	文本文档	1 KB
🗑 system	2022/6/20 16:00	dat 媒体文件	88 KB
📆 system64	2022/6/20 16:00	dat 媒体文件	78 KB
🦁 vuld	2022/6/20 16:00	应用程序	673 KB

3) 在下载器界面中勾选操作系统类型,选择 32 位或 64 位系统补丁,选择漏洞级别,点击<开 始下载>,即可离线下载漏洞补丁。



Windows XP	Window	s 7 🗌 Windows 8	Windows 10	
Windows Ser	ver 2003	Windows Server 2008	Windows Server 2012	
Windows Ser	ver 2016 [Windows Server 2019	全选	
〇 仅下载32位	系统补丁 ()仅下载64位系统补丁	32 and 64	
选择漏洞级别				
☑高危	□□□选			

4) 下载的漏洞补丁文件将会保存在解压文件夹目录下。

名称	修改日期	类型	大小
d	2022/6/20 16:01	文件夹	
1 7z	2022/6/20 16:00	应用程序	785 KB
libcrypto-1_1.dll	2022/6/20 16:00	应用程序扩展	2,064 KB
libssl-1_1.dll	2022/6/20 16:00	应用程序扩展	363 KB
🚳 litexml.dll	2022/6/20 16:00	应用程序扩展	1,330 KB
🚳 mfc100.dll	2022/6/20 16:00	应用程序扩展	4,295 KB
msvcp100.dll	2022/6/20 16:00	应用程序扩展	412 KB
msvcr100.dll	2022/6/20 16:00	应用程序扩展	756 KB
runlog	2022/6/20 16:13	文本文档	1 KB
🗒 system	2022/6/20 16:00	dat 媒体文件	88 KB
📆 system64	2022/6/20 16:00	dat 媒体文件	78 KB
🧿 vuld	2022/6/20 16:00	应用程序	673 KB

步骤 5. 点击<上传文件>,可将离线补丁包上传至管理中心,进行补丁离线更新。

上传完成后,租户角色登录主机安全系统管理平台即可对相应终端进行漏洞修复。



已下载补丁	在线更新补丁	离线更新补丁
EDR管理中	心无法联互联网	时,建议离线更新补丁库
1 下载离	线下载器	
下载后,	可通过下载器离线下	载补丁包
下	戝	
2 上传离	线补丁包	
上传离线	补丁包到管理中心	
上传过	文件	

根据中心和端主机是否可访问互联网的情况,可通过以下方式获取漏洞补丁。

联网情况	获取方式
日右山心可访问五曜网	admin 用户登录主机安全系统管理平台,在左侧菜单栏选择"系统
八有千心可切问五状网	管理≻Windows 补丁库管理" ,下载补丁后推送给端主机修复。
	◆ 中心已下载过的补丁仍由中心推送给端主机修复。
只有端可访问互联网	◆ 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。
由心和禮教不可法词互联网	admin 用户登录主机安全系统管理平台,离线上传补丁后,中心推
中心和缅甸个可切问互联网 	送补丁至端主机进行漏洞修复。
	◆ 中心已下载过的补丁由中心推送给端主机进行漏洞修复。
中心和端都可访问互联网 	◆ 中心未下载过的补丁由端主机下载后进行漏洞修复。

19.1.4 密码及访问策略

用户可在密码及访问策略页面配置密码及访问策略。

19.1.4.1 密码策略

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>密码及访问策略"进入密码及访问策略页面。

步骤 3. 配置密码策略信息,点击<提交>,即可配置密码策略。



密码策略		
口令最小长度:	10	
至少包括以下几种策略:	2 密码策略仅包含以下策略组合、密码中不允许包含空格	
策略类型:	☑ 大写字母 ☑ 小写字母 ☑ 数字 ☑ 特殊字符	
密码有效期:	0	F
	建议设置90天有效期,过期后用户密码需强制更改 支持设置0~360天。0表示永不过期	

详细配置请参见下表。

参数	说明	
口令最小长度	取值范围 8~50。	
至少包括以下几 种策略	设置密码需要包含的字符类型种类,取值范围 2~4。	
策略类型	密码策略类型	
密码有效期	建议设置 90 天有效期,过期后用户密码需强制更改 支持设置 0-360 天,0 表示永不过期	
 ◆ 新升级到 V3.0.3 版本默认 0 天,此功能不生效,需要重新设置; ◆ 新安装 V3.0.3 版本默认 90 天。 		

19.1.4.2 访问策略

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>密码及访问策略"进入密码及访问策略页面。

步骤 3. 配置访问策略信息,点击<提交>,即可配置访问策略。

访问策略		
登录限制IP:	请输入登录限制IP	2
	192.168.1.1; 192.168.1.1-192.168.1.255 不填表示不限制IP, "*"表示所有IP、"-"表示IP段,多个IP需换行输入	
验证码开关:		
身份验证器作用范围:	登录时 高危操作二次认证	
	提交	重置

详细配置请参见下表。

参数	说明
----	----



参数	说明
登录限制 IP	不填表示不限制 IP, "*"表示所有 IP、"-"表示 IP 段,多个 IP 需换行输入,例如: 192.168.1.1;192.168.1.1-192.168.1.255
验证码开关	开启时,用户登录系统 Web 管理平台需要输入验证码。
身份验证器	用户可选择在登录时或者高危操作时使用双因子认证。

身份验证器中高危操作包括文件推送、远程协助、重启终端、关机等操作。

19.1.4.3 租户策略模板

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>密码及访问策略"进入密码及访问策略页面。

步骤 3. 配置租户策略模板信息,点击<提交>,即可配置租户策略模板策略。

阻户策略模板							
* 修改策略模板:	① 允许	租户修改 🔘 不	允许修改				
	0	开始时间	至	结束时间			
	們: 這择00:00:00-23:59:59表示任意时间段用户均可修改策略模板 這择06:00:00-23:59:59表示波时间段内相一可修改策略模板,其余时间段不允许 這择"不允许修改"表示任意时间段均常止修改策略模板						
					提交	重置	

详细配置请参见下表。

参数	说明					
修改策略模板	设置是否允许租户修改策略模板,同时允许租户修改下支持配置时间段。					
	例:选择 00:00:00~23:59:59 表示任意时间段租户均可修改策略模板					
	选择 08:00:00~23:59:59 表示该时间段内租户可修改策略模板,其余时间段不允					
	许					
	选择"不允许修改"表示任意时间段均禁止修改策略模板					

19.1.5 部署管理

用户可在部署管理页面对日志保留天数进行设置。超过日志保留天数后,将清理最早日期的日志。

以 admin 用户登录主机安全系统管理平台,在导航栏选择"系统管理>部署管理",进入部署管理页面。设置日志保留天数,点击<应用配置>。



日志保留:	-	180	+	天
	日志默认	、保留180天, ፣	可以在	此定义日志保留时长,如您的日志占用磁盘已超过80%,建议调整日志保留的时间
	应用香	置		

19.1.6 个性化

用户可在**个性化**页面对 Logo、登录背景、厂商公司名称、厂商英文缩写、客户端名称进行设置,以满 足个性化需求或者 oem 需求。

19.1.6.1 个性化

以 admin 用户登录主机安全系统管理平台,在导航栏选择"系统管理>个性化",进入个性化页面。 填写个性化内容,点击<保存>。

产品名称:	1-30个字符,支持中英文及数字
	替换平台产品名称
客户端名称:	1-20个字符,支持中英文及数字
	替换客户端注册信息、桌面快捷方式、客户端显示名称等。例如:XXX主机卫士
LOGO:	6
	点击替换图片,像素256*256,格式为".png",上传后将更换平台及客户端LOGO图标
登录背景:	
	点击替换图片,像素1920*1080,格式为".png",上传后将更换WEB管理平台登录肯易
一商公司名称:	1-30个字符,支持中英文及数字
	替换厂商名称相关标识、注册信息厂商等。例如:XXX有限责任公司
厂商英文缩写:	1-20个英文字母

恢复默认保存

详细配置请参见下表。

参数	说明
LOGO	像素 256*256,格式为".png",上传后将更换平台及客户端 LOGO 图标
产品名称	替换平台产品名称
登录背景	像素 1920*1080,格式为".png",上传后将更换 WEB 管理平台登录背景



参数	说明
厂商公司名称	替换厂商名称相关标识、注册信息厂商等。例如: XXX 有限责任公司
厂商英文缩写	替换客户端部署目录等信息。例如: XXXSecurity
客户端名称	替换客户端注册信息、桌面快捷方式、客户端显示名称等。例如: XXX 主机卫士

◆ 个性化参数生效于管理中心平台和新装的客户端的终端,个性化参数配置后终端需重装在线/离线部署新生成客户端才能调整为个性化界面和相关名称显示。

◆ 支持 openapi 配置个性化相关参数。

19.1.6.2 恢复默认

以 admin 用户登录主机安全系统管理平台,在导航栏选择"系统管理>个性化",进入个性化页面。 点击<恢复默认>以此恢复出厂信息。

保存

恢复默认

19.2 租户账户系统管理

租户可在此页面进行部署管理、许可分配、告警配置及个人中心等操作。

19.2.1 部署管理

19.2.1.1 添加终端

租户可在**添加终端**页面查看连接管理中心时所需要的管理员识别码(UUID),并进行系统终端添加。 终端添加前可为终端选择分组,不选择的情况下系统会进行自动选择分组(PC组、Windows 服务器 组、Linux 服务器组)。

19.2.1.1.1 配置终端

租户在可对新增终端配置并复制联动所需的 APIKEY,并设置离线定期删除、客户端绑定地址、绑定分组。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>部署管理",选择添加终端页签。

步骤 3. 点击<**设置**>。



添加终端 推广部署 AD推送

别码: VR002ae6 回	① 确保安装客户端的主机可正常访问到管控中心的10571端口,如需修改IP地址则	则前往设置	设置
	Windows系统 Windows XP SP3 / Windows Vista / Windows 7 / Windows 8、8.1 / Windows 10/ Windows 11 Windows Server 2003 SP2 / Windows Server 2008、2008R2 / Windows Server 2012、2012R2 / Windows Server 2016 / Windows Server 2019/ Windows Server 2022		
	离线安装: 下载安装包, 拷贝到主机上进行安装。 https://wwwwwwisterfile/download2?name=edr_download/windows/cesh//wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww	下载	复制
	在线安装: Win7及以上系统,以管理员权限运行CMD程序,复制以下命令进行安装。 powershell -executionpolicy bypass - c *\$client = new-object System.Net.WebClient; \$client.Headers['User-Agent'] = 'edr_agent/2.0(http request using rpc prot cool): \$client DownloadGill/thtp://	复制	
	occu); scient.Lowiniaadriet (http:// "i.io5/ ydowiniaadywindows/win_installer.exe , st.xecution.Context.Sessionstate.Path.GetUntest/vebreovebrevitePath FromPSPath(:\win_installer.exe'))*; "\$proc = Start-Process _/win_installer.exe -ArgumentList @('uuid VR002ae6center = 1 = "51:10571ui 0') -Verb ru nas -PassThru; \$proc.WaitForcit() *	近印	

步骤 4. 在弹窗中配置相关内容,点击<确定>保存配置。

终端设置		×
APIKEY值:	0YmAspPYshWjU3HrWBOkdA==	复制
自动删除:	超过 - 30 + 天末	天上线自动删除离线终端
* 绑定地址:	10.20.178.151:10571 🗸 安装	专客户端,默认绑定至IP ①
自动分组:	自动选择 🗸 安装	专客户端,默认绑定至分组
		关闭 确定

详细配置请参见下表。

参数	说明
自动删除	设置是否开启自动删除策略,开启后,当终端未上线时间达到设置值时会 删除离线终端。当总终端数量较多且有部分终端长时间离线时建议开启此 功能。
绑定地址	安装客户端需要绑定管理中心,默认不用修改此配置。
自动分组	安装客户端后,客户端所在终端将绑定至指定分组。默认为自动选择,请 根据实际进行设置。

19.2.1.1.2 添加 Windows 系统终端

以租户角色登录主机安全系统管理平台,在左侧导航栏选择"系统管理>部署管理",选择添加终端 页签,租户可在 Windows 系统区域进行 Windows 系统终端的离线安装及在线安装。

- ◆ 离线安装
 - ●方式一:点击离线安装的<下载>,下载客户端安装包,以管理员权限将安装包拷贝到 终端服务器上,双击安装程序,执行安装。
 - ●方式二:点击离线安装的<复制>,复制客户端安装包下载链接。以管理员权限登录终端服务器,在浏览器地址栏中粘贴下载链接并回车,进行客户端安装包本地下载。 下载完成后双击安装程序,执行安装。



添加终端

推广部署

AD推送

别码: VR002ae6 回	③ 确保安装客户端的主机可正常访问到管控中心的10571端口,如需修改IP地址则	则前往设置
	Windows系统 Windows XP SP3 / Windows Vista / Windows 7 / Windows 8、8.1 / Windows 10/ Windows 11	
	Windows Server 2003 SP2 / Windows Server 2008, 2008R2 / Windows Server 2012, 2012R2 / Windows Server 2016 / Windows Server 2019/ Windows Server 2022	
	离线安装: 下载安装包, 拷贝到主机上进行安装。 https://1/service/file/download2?name=edr_download/windows/ceshi/110571/1/win_installer_11_VR002ae6.exe	下载
	在线安装:Win7及以上系统,以管理员权限运行CMD程序,复制以下命令进行安装。	
	powershell -executionpolicy bypass -c *\$client = new-object System.Net.WebClient; \$client.Headers['User-Agent'] = 'edr_agent/2.0(http request using rpc prot ocol) '; \$client.DownloadFile('http://101:10571/download/windows/win_installer.exe', \$ExecutionContext.SessionState.Path.GetUnresolvedProviderPath	复制
	FromPSPath('\win_installer.exe'))''; "\$proc = Start-Process ./win_installer.exe -ArgumentList @('uuid VR002ae6center 1	

◆ 在线安装

点击在线安装的<复制>,复制安装链接,在客户端上使用 cmd 执行该命令进行一键安装。



19.2.1.1.3 添加 Linux 系统终端

以租户角色登录主机安全系统管理平台,在左侧导航栏选择"系统管理>添加终端",选择添加终端 页签。租户可在 Linux 系统区域进行 Linux 系统终端的离线安装及在线安装。

◆ 离线安装

选择 CPU 架构以及操作系统位数,点击离线安装的<下载>,下载安装包,并复制脚本命令。将软件包拷贝到服务器上进行解压,执行脚本命令进行安装即可。

A	Linux系统 支持Centos5.0+、Redhat5.0+、Suse11+、Ubuntu 国产系统:统信UOS、银河麒麟、中标麒麟、中科方	14+、debian等主流发行版本操作系统 7德、欧拉、龙蜥、深度、凝思、磐石、	: 110000.	
	离线安装: 选择CPU架构以及操作系统位数下载安	R装包,拷贝到服务器上解压后执行脚本	地行安装。	2 3
	x86架构 🗸	64位操作系统 🔹	1	下载复制
	tar no-same-permissions no-s	32位操作系统		
	在线安装:下载以管理员权限执行以下命令进行 wgetno-check-certificate http://	64位操作系统 64位操作系统(统信签名deb包) 64位操作系统(额额签名deb包)	notest/10.50.121.11_10571/1/agent_setup.sh -O agent_setup.sh && chmod +x agent_setup.sh && Jagent_setup.sh	复制
	批量安装: 通过SSH远程方式, 批量安装Agent。	填写服务器IP等信息,并上传文件。安	装前需保证管理中心已安装expect插件。	

◆ 在线安装

点击在线安装的<复制>,复制下载链接,在客户端上以管理员权限执行该命令进行安装。



A	Linux系统 支持Centos5.0+、Redhat5.0+、Suse11+、Ubuntu 14+、debian等主流妄行版本操作系统; 因产系统: 统值UOS、银河商额条 中标题题,中科方语、放龙、龙振、深度、凝思、银石、虹旗等。	
		下载 复制
	在线安装: 下载以管理员权原执行以下命令进行安装。 wget — no-check-certificate http://10.50.121.11:10571/download/linux/autotest/10.50.121.11_10571/1/agent_setup.sh -O agent_setup.sh && chmod +x agent_setup.sh && /agent_setup.sh	复制
	批量安装: 通过SSH近程方式,批量安装Agent。	

◆ 批量安装

点击**批量安装**的**<下载>**,获取批量安装模板。按照模板要求填写服务器 IP 等信息,填写完成后点击**< 上传文件>**,上传编辑好的模板文件,进行客户端批量安装。

Linux系统 支持Centos5.0+, Redhat5.0+, Suse11+, Ubuntu 14+, debian等主流发行版本操作系统; 国产系统: 统值UOS, 银河翻赢, 中标酒蘸, 中标方德, 吸拉, 龙蜥, 深度、凝思, 磐石, 虹顶等。		
 离线安装:选择CPU架构以及操作系统位数下载安装包,拷贝到服务器上解压后执行脚本进行安装。		
x86架构 🗸 64位操作系统 🗸	下载	复制
tarno-same-permissionsno-same-owner -zxvf linux_agent_setup_3.0.7.104.x64.tar.gz && chmod +x install_edr.sh && ./install_edr.sh		
在线安装: 下载以管理员权限执行以下命令进行安装。 wgetno-check-certificate http://10.50.121.11:10571/download/linux/autotest/10.50.121.11_10571/1/agent_setup.sh -O agent_setup.sh && chmod +x agent_setup.sh && ./agent_setup.sh	复制	
批量安装:通过SSH选程方式,批量安装Agent。		

上传文件前需保证管理中心已安装 expect 插件。查看安装 expect 插件的操作步骤如下。

步骤 1. 以 root 用户登录管理端服务器的操作系统 CLI 界面,执行 except 命令,查看是否有返回结果。 若有返回结果,则说明管理中心已安装 except 插件。若没有返回结果,则执行下一步进行插 件安装。

[root@localhost	yum.repos.d]# expect
expect1.1>	
expect1.1>	
expect1.1>	
expect1.1>	

步骤 2. 使用 rpm 包安装方式安装 except 插件,执行 rpm -ivh rpm 包文件名进行安装。

支持添加的终端操作系统版本如下表所示。

系统	版本	
Windows 系统	支持 Windows XP、Windows 7、Windows 8、Windows 10、Windows 11、Windows Server 2003、Windows Server 2008、Windows Server 2008R2、Windows Server 2012、Windows Server 2016、Windows Server 2019、Windows Server 2022 等版本 操作系统。	
Linux 系统	支持 Centos5.0+、Redhat5.0+、Suse11+、Ubuntu 14+、debian 等主流发行版本操 作系统; 国产系统:统信 UOS、银河麒麟、中标麒麟、中科方德、欧拉、龙蜥、深度、	



系统	版本
	凝思、磐石、红旗等。等。

19.2.1.2 推广部署

用户可在推广部署页面发布部署通知。

管理员发布部署通知的 Web 页面,填写推广信息后生成推广链接,将推广链接下发后,终端用户可 自行部署客户端。推广文案可自定义,修改后需要点击**<重新生成>**更新到推广页面中。

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>管理部署",选择推广部署页签。

步骤 3. 输入推广标题及推广文案,点击<重新生成>,生成最新推广链接。

步骤 4. 点击<复制>,复制推广链接进行推广(通过邮件、即时通讯工具进行推广)。

添加终端 推广部	署 AD推送	
管理员发布部署通知的web	页面,填写推广信息后生成掩厂链接,将推广链接下发后,终端用户可自行部署客户端。推广文案可自定义,修改后需要点击重新生成按钮后/	应用到推广页面中。
推广标题:	终端安全软件部署通知	
推广文案:	各位同事: 为了更好地维护终端安全,单位决定从即日起全面部署终端防护软件。请您根据您的终端操作系统选择对应文 件下载并安装,安装后无需任何设置即可使用。感谢您的支持与合作!	1
推广链接:	复制推广链接,通过邮件、OA、通讯工具发送链接,终端用户自行部署客户端。 重新生成	2
	https://10.20.178.151/#/promotion-deploy-notice?lessUser=ceshi 复制	3

终端用户打开推广链接,在链接页面上执行相关操作即可部署客户端。

终端安全软件部署通知	
各位同事: 为了更好地维护终端安全,单位决定从即日 起全面部署终端防护软件。请您根据您的终端操作系统选 择对应文件下载并安委 安装后无需任何设置即可使用。	EDR 安全防护
I Windows系统 Windows XP SP3 / Windows Vista / Windows 7 / Windows 8, 8,1 / Windows 10 Windows Samer 2003 SP2 / Windows Samer 2008 - 2008-20 / Windows Samer	I Linux系統 支持Centos5.0+、Redhat5.0+、Suse11+、Ubuntu 14+等主流发行版本操作系统; 同声系统: 由局問題 短辺問題 (統在)US
I Windows系统 Windows XP SP3 / Windows Vista / Windows 7 / Windows 8, 8,1 / Windows 10 Windows Server 2003 SP2 / Windows Server 2008, 2008R2 / Windows Server 2012, 2012R2 / Windows Server 2019 ● 高线安装: 下载安装包, 拷贝到主机上进行安装。 下载	┃ Linux系統 支持Centos5.0+、Rednat5.0+、Suse11+、Ubuntu 14+等主流发行版本操作系统; 国产系统:中标麒麟,银河麒麟,统信UOS 64位操作系统
I Windows系统 Windows XP SP3 / Windows Vista / Windows 7 / Windows 8, 8.1 / Windows 10 Windows Server 2003 SP2 / Windows Server 2008, 2008R2 / Windows Server 2012, 2012R2 / Windows Server 2016 / Windows Server 2019 • 高线安装: 下载安装包, 拷贝到主机上进行安装, 下载 • 在线安装: 在客户端上使用以下链接下载后进行安装	↓ Linux系統 支持Centos5.0+、Redhat5.0+、Suse11+、Ubuntu 14+等主流发行版本操作系统; 国产系统:中标麒麟,银河麒麟,统信UOS x86架构 ● 64位操作系统 ● 高线安装: 选择CPU架构以及操作系统位数下载安装包,拷贝到服务器上解压后执行脚本 进行安装。
I Windows系統 Windows XP SP3 / Windows Vista / Windows 7 / Windows 8, 8.1 / Windows 10 Windows Server 2003 SP2 / Windows Server 2008, 2008R2 / Windows Server 2012, 2012R2 / Windows Server 2016 / Windows Server 2019 ■高线安装: 下载安装包, 拷贝到圭机上进行安装, 下载 ■在线安装: 在客户端上使用以下链接下载后进行安装 powershell -executionpolicy bypa	I Linux系統 支持Cantos5.0+、Radhat5.0+、Suso11+、Ubuntu 14+等主流发行版本操作系统: 国产系统: 中标翻瞬,银河翻瞬,航信UOS x86架构 64位操作系统 • 高线安装: 选择CPU架构以及操作系统位数下载安装包,拷贝到服务器上解压后执行脚本 进行安装。 tarno-same-permissionsno-s 下載 重制
I Windows系统 Windows XP SP3 / Windows Vista / Windows 7 / Windows 8, 8, 8, 1 / Windows 10 Windows Server 2003 SP2 / Windows Server 2008, 22008R2 / Windows Server 2012, 2012R2 / Windows Server 2019 ● 高线安装: 下载安装包, 拷贝到主机上进行安装。 下载 ● 在线安装: 在客户端上使用以下链接下载后进行安装 powershell -executionpolicy bypa	Linux系統 支持Centos5.0+、Rednat5.0+、Suse11+、Ubuntu 14+等主流发行版本操作系统: 国产系统: 中标觀顯, 银河麒麟, 抗信UOS x86架构 ・ 64位操作系统 ・高线安装: 法择CPU架构以及操作系统位数下载安装包, 拷贝到服务器上解压后执行脚本 进行安装。 tarno-same-permissionsno-s 下載) 管理员权限执行以下命令进行安装。



19.2.1.3 AD 推送

windows 用户通过 ad 推送工具给账户登录时设置自动化脚本以此达到批量安装效果。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>管理部署",选择 AD 推送页签。

步骤 3. 点击<下载域推送工具>下载工具。

端推广部署 4D推送					
下载域推送工具	 将域推送工具放到域控服 务器上,双击执行	 选择部署或者删除客户端 的操作	选择需要执行操作的域控 用户账户	设置安装参数,包括管理 平台IP及安装目录	安装完成后,可在【终 端管理】-【终端概况】 查看终端上线情况

步骤 4. 在域控服务器上打开 ADTOOL.exe 工具。

a) 填写管理中心地址和租户标识(租户识别码),点击<测试连通性>

 DAS域控批量音 共发现 11 个域用 管理中心地址: ① 租户标识: 	8署工具 v1.0 3户,其中 0 个用户已 10.20.178.151:105 VR002ae6	设置域安装脚本。 571	连通性 ②		刷新数据
6	未设置域安装脚本		💋 已设置域安装脚本	? 已设置其他启动脚本	
I號用户名 admin Administrator cccc ceshi3 ceshi6 chu.bob Guest hiram.wong krbtgt test zhichao.tong		域用户描述 管理计算机供 供来宾访问计 密钥发行中心	j 10.20.178.151:10571连接成功! ③ 确定		
全选	全不选	反选		[设置域安装脚本

b)选择未设置域安装脚本页签,选择域用户,点击<设置安装脚本>设置需要安装的域用户



里中心地址:	10.20.178.151:10	571	测试连通性			刷新数据
租户标识:	VR002ae6					
6	未设置域安装脚本		🚺 已设置域安装脚本	?	已设置其他启动脚本	
用户名		域用户描述		当前域登录启	动脚本	
admin Administrator cccc ceshi3 ceshi6 chu.bob		管理计算机(域的内置帐户			
Guest		供来宾访问i	计算机或访问域的内置帐户			
hiram.wong krbtgt test zhichao.tong		密钥发行中,	心服务帐户			
						0

c)选择已设置域安装脚本页签,选择域用户,点击<删除安装脚本>调整需要安装的域用户

理中心地址: 租户标识:	10.20.178.151:10571 VR002ae6	测试连通性		刷新数据
G	未设置域安装脚本	● 已设置域安装脚本	? 已设置其他启动脚本	
拥户名	域用	户描述	当前域登录启动脚本	
Administrator	管理	计算机(域)的内置帐户	EDRInstall.bat	
2222			EDRInstall.bat	
ceshi3 🕕			EDRInstall.bat	
Cesillo			EDICINISTALI, DAL	
				2

步骤 5. 点击<【终端管理】-【终端概况】>查看是否安装成功

终端 推厂部者 AD推送					
下载域推送工具	将城推送工具放到城控服 务器上,双击执行	选择部署或者删除客户端 的操作	选择需要执行操作的域控用户账户	设置安装参数,包括管理 平台IP及安装目录	安装完成后,可在【终 端管理】-【终端概况】 查看终端上线情况



选择终端

◆ 已经登录域账户的终端需要重新退出登录才可以触发安装过程

- ◆ AD 推送工具可通过"全选" "全不部" "反选" 快速选择域用户
 - ◆ 刷新数据为刷新域控服务器下的域用户

19.2.2 许可分配

租户可在许可分配页签对终端进行许可分配。

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>许可分配",进入许可分配页面。

步骤 3. 选择终端授权对象,点击右侧操作项的 🕫 图标。

生效日期	授权对象	最大支持数量	当前剩余数量	模块类型	到期日	状态	操作项
2022-08-10	ceshi	1	0	EDR-SST-CLIETN	2023-08-31	●生效	69
2022-08-10	ceshi	20	18	EDR-MODULE-PC	2023-08-31	●生效	63
2022-08-10	ceshi	20	19	WPT-EE-ALL	2023-08-31	●生效	¢
2022-08-10	ceshi	500	497	EDR-MODULE-SERVER	2023-08-31	●生效	¢\$

步骤 4. 在弹出的对话框中选择终端(在**终端列表**中勾选终端,点击 >>> 图标,将终端移动至**已选择终** 端列表),点击<确定>,即可完成终端许可分配。

终端列表	2/2		已选择	释终端列表	0/2
请选择分组	~		请选择	泽分组	~
选择标签	~		选择	示签	~
终端名称/IP	Q		终端	名称/IP	Q
✓ 终端名称	'n			终端名称	
☑		\sim		WIN-3QFTRUC04HH(10.11	 , 192.16
☑				DESKTOP-80K43JQ(192.16 ⁸)	1 7 - 1

取消 确定

19.2.3 告警配置

租户可在告警配置页面进行邮件告警配置、Syslog 配置。

×



19.2.3.1 配置邮件告警

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>告警配置",选择邮件告警页签。

步骤 3. 进入**邮件告警**页面,输入邮件配置信息后点击<应用配置>,即可成功配置邮件告警。

另可对邮件告警配置进行重置邮件操作,重置后将返回上一次配置的结果。

邮件告警 Sysl	log
告警类型	2 🗹 系统防护 🗹 网络防护 🗹 Web应用防护
告警级别	□ 已失陷 □ 高风险 □ 低风险
	发件辅默认使用edr@dbappsecurity.com.cn,如需使用个人邮箱请前往 个人中心 修改
收件人邮箱	test1@163.com +
发送时间间隔	10 分钟
是否启用	○ 是 ● 否
	应用配置重置

19.2.3.2 配置 Syslog

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>告警配置",选择 Syslog 页签。

步骤 3. 进入 Syslog 页面,输入 Syslog 配置信息后点击<应用配置>,即可成功配置 Syslog。

另可对 Syslog 配置进行重置操作,重置后将返回上一次配置的结果。

邮件告警 Sys	
告警类	型 🗹 系统防护 🗹 网络防护 🔽 Web应用防护
Syslog服务器地	址 192.
Syslog服务器端	D 515
是否启	用 〇 是 💿 否

应用配置	重置
------	----



19.2.4 个人中心

租户可在个人中心页面中查看个人信息、配置联系电话及邮箱。

19.2.4.1 查看个人信息

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"**系统管理>个人中心**",进入**个人中心**页面。

步骤 3. 点击用户头像,选择头像文件,即可自定义头像,上传文件建议不超过 2MB。

I 个人信息 ceshi 租户管理员		
	載音 保存	

19.2.4.2 配置手机号码

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>个人中心",进入个人中心页面。 步骤 3. 输入联系电话,选择是否启用,点击<保存>。

联系电话:	
	请填写紧急联系人电话号码,用于弱口令,勤索病毒,致命漏洞的风险告知和文件加密,系统性能消耗 过高的紧急通知!
是否启用:	

手机号码设置为"启用"的手机号码可收取系统紧急通知。

19.2.4.3 配置邮箱

步骤1.以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择"系统管理>个人中心",进入个人中心页面。

步骤 3. 输入是否使用默认邮箱、发件箱地址、SMTP 密码、SMTP 服务器地址、SMTP 服务器端口及 是否支持 SSL 等信息后点击<应用配置>,即可成功完成邮箱配置。



使用默认发件箱	○ 是 ● 否 默认发件箱为edr@dbappsecurity.com.cn,要求EDR服务器可与该地址通信,测试语句: telnet
	smtp.dbappsecurity.com.cn 25
*发件箱地址	test@163.com
* SMTP密码	请输入SMTP密码
MTP服务器地址	smtp.163.com
MTP服务器端口	23
是否支持SSL	○ 是 ● 否

20运维平台

admin 用户或者租户都可在运维平台对主机安全系统进行运维诊断、磁盘清理及重置密码操作,方便 排查系统故障。

20.1 查看运维诊断结果

步骤1.登录主机安全系统运维平台。

 \square

 ◆ 方式一: 登录主机安全系统管理平台,将光标移至右上角用户名上,在下拉框中选择"运 维平台",页面将跳转至运维平台。

	test 🔨
关于	
用户反馈	
运维平台	
修改密码	
注销	

◆ 方式二: 或在浏览器地址栏输入 <u>https://IP 地址:10579</u>,以 admin 用户访问运维平台。输入 账号和密码,点击<**登录**>。

其中 IP 地址是主机安全系统管理平台的 IP 地址。

 ◆ 运维平台独立于主机安全系统平台,仅可使用运维平台 admin 账号进行登录, 且该 admin 账号密码每日会进行更新。获取最新运维平台账号密码,请致电信息技 术支持热线 400-6059-110。

主机安全系统出厂默认关闭且每天 00:00 定时关闭运维平台,用户需在使用前以



root 用户角色登录中心端服务器,执行 docker start 主机安全系统-ops 命令进行开

启。

步骤 2. 进入运维平台,在导航栏选择"运维诊断",进入运维诊断页面,用户可查看运维诊断详细 结果。

选择需要重启的服务,点击右侧**操作项**的**<重启>**,在弹出的对话框中点击**<确定>**,可对服务 进行重启操作。

选择多个服务后点击<一键重启>,在弹出的对话框中点击<确定>,可批量重启多个服务。

一键目	信 导出日志						
	检查项	结果	端口	PID	CPU	内存	操作项
	edrcenter	正常	9081	98893	0.0	8.5	重启 导出日志
	rpc-server	正常	10571	65993	0.0	0.1	重启导出日志
	es	正常	9200	105176	0.0	16.0	重启 导出日志
	mysql	正常	3306	65290	0.0	5.6	重启 导出日志
	redis	正常	6379	65917	0.0	0.1	重启 导出日志

2021-11-09 15:59:40

勾选多个服务后点击列表上方的<**导出日志**>,在弹出的对话框中点击<确定>,可批量导出多个服务的日志信息。

—键]	E 启 导出日志						
	检查项	结果	端口	PID	CPU	内存	操作项
~	edrcenter	正常	9081	98893	0.0	8.5	重启导出日志
	rpc-server	正常	10571	65993	0.0	0.1	重启 导出日志
	es	正常	9200	105176	0.0	16.0	重启 导出日志
	mysql	正常	3306	65290	0.0	5.6	重启 导出日志
	redis	正常	6379	65917	0.0	0.1	重启 导出日志

2021-11-09 15:59:40

20.2 清理磁盘

清理补丁文件将导致所有补丁文件被清空,请谨慎操作。

步骤 1. 登录主机安全系统管理平台,将光标移至右上角用户名上,在下拉框中选择"运维平台"。

步骤 2. 进入运维平台页面,在导航栏选择"磁盘清理"进入磁盘清理页面,用户可查看磁盘详情列 表。

步骤 3. 选择需要清理的文件,点击右侧操作项的<清理>,可对磁盘进行清理操作。

选择多个文件后点击<一键清理>,可进行多个文件批量清理。

步骤 3. 选择需要导出日志的服务,点击右侧**操作项**的<**导出日志**>,在弹出的对话框中点击<确定>, 可导出该服务的日志信息。



一键	清理 2 录总磁盘50G,已用16G			
	清理项	占用磁盘	详情	操作项
	1.时日志	3.5G	EDR中心目录下的临时文件	清理
	压缩包	1.3GB	/opt和/root下的压缩包	清理
	服务日志	226.88MB	EDR中心服务运行日志	清理
	补丁文件	2.16GB	清理补丁文件,谨慎选择此步骤,将导致所有补丁文件清空	清理

20.3 重置密码

步骤 1. 登录主机安全系统管理平台,将光标移至右上角用户名上,在下拉框中选择"运维平台"。

步骤 2. 进入运维平台页面,在导航栏选择"忘记密码",进入忘记密码页面,输入密码并确认密码, 点击<确定>,可对主机安全系统管理平台 admin 用户的账户密码进行重置。

密码强度需要符合设置要求,关于密码强度的详细信息,请参考<u>密码及访问策略</u>。

* 输入密码	•••••	
* 确认密码:	••••••	
		提交

20.4 恢复数据

20.4.1 恢复 MySQL 数据

步骤 1. 登录主机安全系统管理平台,将光标移至右上角用户名上,在下拉框中选择"运维平台"。

步骤 2. 进入运维平台页面,在导航栏选择"数据恢复"进入数据恢复页面,选择 MySQL 数据库页 签。

步骤 3. 选择备份文件后对系统数据进行恢复。

- ◆ 选择历史备份
 - 1) 选择历史备份文件。
 - 2) 点击<确定>,进行数据恢复。



SQL数据库 ES防护日志	
J通过选择历史的备份数据或者上传备份数据文件,进行数据恢复。该操作将恢复所有资产、配置信息,i	青谨慎操作。
选择历史备份:	上传本地备份:
	上传文件
<u>确定</u> 2	制定

- ◆ 上传本地备份
 - 1) 点击<上传文件>,上传本地备份文件。
 - 2) 点击<确定>,进行数据恢复。

*、配置信息,请谨慎操作。
上传本地备份:
上传文件
御定 2

20.4.2 检测 ES 状态

步骤 1. 登录主机安全系统管理平台,将光标移至右上角用户名上,在下拉框中选择"运维平台"。 步骤 2. 进入运维平台页面,在导航栏选择"数据恢复"进入数据恢复页面,选择 ES 防护日志页签。 步骤 3. 点击<检测>,可对系统 ES 服务状态进行检测。

MySQL数据库 ES防护日志				
ES故障恢复,该操作仅恢复为7天内的防护日志/	操作日志/运维日志,请谨慎操作。			×
检测 批量删除 一键恢复				©
检查项	说明	占用空间	状态	操作项
cloudbrainv2-wyh	租户wyh的	281b	yellow	
performance-liuz	租户liuz的性能数据	297b	yellow	

对于检测状态为 red 的检查项,勾选检查项后点击<**批量删除**>,可对检查项进行批量删除操 作。



MySQL数据库 ES防护日志				
ES故障恢复,该操作仅恢复为7天内的防护日志/	操作日志/运维日志,请谨慎操作。			×
检测 批量删除 一键恢复				0
检查项	说明	占用空间	状态	操作项
cloudbrainv2-wyh	租户wyh的	281b	yellow	
performance-liuz	租户liuz的性能数据	297b	yellow	
ops-test	租户test的运维日志	253.9kb	yellow	

勾选检查项后点击<一键恢复>,可恢复该检查项7天内的防护日志/操作日志/运维日志。

MySQL数据库 ES防护日志				
ES故障恢复,该操作仅恢复为7天内的防护日志/操	作日志/运维日志,请谨慎操作。			×
检测 批量删除 一键恢复				0
当前页已选择 1 项,未选择 11 项				全选当页 反选当页
✓ 检查项	说明	占用空间	状态	操作项
Cloudbrainv2-wyh	租户wyh的	281b	yellow	



21.1 如何区分 Docker 版本与非 Docker 版本?

主机安全系统 V3.0.3 版本仅支持 Docker 版本,支持 V2.0.17.x 的 Docker 版本直接升级至 V3.0.3 版本, 如若为 V2.0.17.x 及以前的非 Docker 版本,请参考《主机安全及管理平台 V2.0.17.9 维护指南》进行迁移数据库到同版本新中心后(新中心操作系统为 Centos7.x)使用 Docker 包部署后升级至 V3.0.3 版本。

Docker 安装包安装升级通用,且适用于 CentOS 7.x 操作系统。

区分方法如下:

使用 root 用户登录主机安全系统中心的后台,执行 docker ps 命令,若能查看主机安全系统中心所有 服务的容器,则说明为 Docker 版;若不能执行该命令,则说明为非 Docker 版。



22 术语&缩略语

术语	解释
DDoS	分布式拒绝服务攻击(Distributed Denial of Service Attack,简称 DDoS)是指处于不同位置的多个攻击者同时向一个或数个目标发动攻击,或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。由于攻击的发出点是分布在不同地方的,这类攻击称为分布式拒绝服务攻击,其中的攻击者可以有多个。
认证	是一种信用保证形式。按照国际标准化组织(ISO)和国际电工委员会(IEC)的定义, 是指由国家认可的认证机构证明一个组织的产品、服务、管理体系符合相关标准、 技术规范(TS)或其强制性要求的合格评定活动。
网马	网马就是在网页中植入木马,用户打开网页就运行了木马程序,从而危害用户的终端。网页木马实际上是一个 HTML 网页,与其它网页不同的是该网页是黑客精心制作的,用户一旦访问了该网页就会中木马。
虚拟机	虚拟机(Virtual Machine)指通过软件模拟的具有完整硬件系统功能的、运行在一个 完全隔离环境中的完整计算机系统。在实体计算机中能够完成的工作在虚拟机中都 能够实现。在计算机中创建虚拟机时,需要将实体机的部分硬盘和内存容量作为虚 拟机的硬盘和内存容量。每个虚拟机都有独立的 CMOS、硬盘和操作系统,可以像 使用实体机一样对虚拟机进行操作。