明御[®]主机安全及管理系统

用户操作手册



杭州安恒信息技术股份有限公司

二〇二二年五月



口米
口水

1,	产品简介1
2	登录及添加许可1
	2.1 用户认证2
3 ·	首页4
	3.1 信息展示4
	3.2 用户信息4
4 '	情报云脑5
5	资产概况5
6	资产指纹7
	6.1 终端详情
	6.2 监听端口8
	6.3 运行进程8
	6.4 账号信息8
	6.5 软件信息9
7	系统防护9
	7.1 主动防御10
	7.1.1 主动防御
	7.1.2 文件实时监控 10
	7.1.3 系统防御10
	7.1.4 执行防御11
	7.1.5 病毒免疫11
	7.2 病毒查杀12
	7.3 漏洞管理12
	7.3.1 只有中心可访问互联网13
	7.3.2 只有端可访问互联网 14
	7.3.3 中心和端都不可访问互联网 15
	7.3.4 中心和端都可访问互联网 17
	7.4 系统登录防护17
	7.5 进程防护18
	7.5.1 进程黑名单
	7.5.2 进程白名单
	7.6 文件访问控制



8 网络防护
8.1 微隔离19
8.2 防端口扫描21
8.3 违规外联防护21
8.3.1 白名单模式
8.3.2 黑名单模式
9 网站防护
9.1 网站漏洞防护22
9.2 CC 攻击防护23
9.3 网站访问控制23
9.4 网站后门查杀24
10 工具箱
10.1 勒索防御
10.1.1 风险评估24
10.1.2 实时防御24
10.2 挖矿防御
10.2.1 风险评估25
10.2.2 实时防御25
10.3 性能监控
10.4 外设管理
10.4.1 无线网卡
10.5 文件推送
10.6 屏幕水印
11 病毒查杀
12 漏洞管理
13 批量配置 29
14 流量画像
15 定期巡检
16 移动存储
16.1 全网禁用
16.2 设备注册
17 日志检索
18 系统管理
18.1 个人中心
18.2 升级管理



18.3	忝加资产	
19 多级中间	ம்	



1 产品简介

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

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

2 登录及添加许可

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

1、使用 admin 账号登录

────────────────────────────────────	全及管理系统
用户服录	●射射 [®] 主机安全及管理系统
2. WeiARP-5	將梅查杀 龍師管理
在 IIIS	強嚴國像 网络防御
2. WeiARP-5	外设管控 安全运输
在 IIIS	重承*极简*理念,
2. WeiARP-5	构建一站式容测安全解决方案,

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



	明御 主机安全及	2 新理系统 2010	1							admin ~
		的可能增								
3	(FUMU	AA HI REAR								
Ц	minoriti	的放开可	HANN BCEDON -							
-	5是书位	相助生政日期	席两号	教任対象	用户信息	最大支持教皇	当初利会数量	#51	制制日	就在
Ð					猶夫数縣					
- 0	WETANE									
- 1	0100001920001.0									
	MARTINE									
1	WRW/ II									
3	MANAGER									
	Westowell于库管理									
	BILLOWWER.									
3	WALL TREE									
	REPARTMENT									

3、得到许可授权后点击"添加许可"输入获得的许可即可开始使用。

🤤 朝朝 🖱 主机安全	及管理系统 2.0.7.2								sunui 🐃
2002	単位 / 新秋世班 / 20万年 (中可設置	Ξ.							
118458	at lars	ROER WITH COERCOARD							
	影响生效日期	1000011940000777-1000777	1067438	用户信息	能大支持数据	TANHORNE	用毒纸石	BHIEL	165
-24203	And the Party of Street, or other	4200990265760707					##	10000	* 生斑
1950.5									
entre									
H. Dissis									
0 REEF									
-17.440									
# 768									

2.1 用户认证

如何添加租户?

- 步骤1. 使用 admin 账号登陆管理平台;
- 步骤2. 进入用户认证,初次进入,需要修改密码;
- 步骤3. 点击新增;



😌 明樹 🖱 主机安全及	管理系统 2010.3		i administra i a
⇒ ○) 洋石製理	所用整理 / 用户以近 / 展 新増用户	微用/P.	atte
A. MIRINU			
E 8690	用户典型:	输产管理员	
🕀 ARRA 🕓	* 用户名:	9667	
WEFERS	- 19195;	4-000.987.200774.00761060100	
mannamatic	* miAmia:	2003	
MARCHARD IN	* 符可数量	0	
008.0716			
用建筑和市外的	* 顧射(分钟))	20	
Wedower的工作管理	* (838: (5)-94)	18	
0029株田和	* 豐豪間制个数:	10.	
UNITED AND A DESCRIPTION OF A DESCRIPTIO	展西田田	④ 約用 〇 不包用	
	可否修改口令:	④ 可继续 手可修改	
		東京 4 法	

步骤4. 输入用户名、密码、确认密码以及许可数量(根据实际情况输入许可数量); 步骤5. 确定后即可新增租户;

	明御 * 主机安全及	管理系统	20104												elemin
		用户认证													
速															
.8	用户认证	310									11111111-0.411	D.M.			
	####D		878	相产类型	许可数量	超时(分钟)	MIR(5)1991	创建时间	重任登录时间	业录用制个数	MUERIA	修改口中	最否应用	操作项	
		0	test	相户管理员	10	20	15	20190	2019-68-2	(10		可推改	* 启用	6251	把算
										л	1.0 208/3	1 1	(X = U)	有任	π.
	NAME WHEN !!														
	INTERNAL PROPERTY OF														
	BOLLEN BE														
	WWW.STIRVEN.														
	出现外联系有利率管理														

步骤6. 后续再使用租户用户名登录管理平台。



3 _{首页}

3.1 信息展示

在首页可查看如下内容:

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



3.2 用户信息

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



第四						
G *****	6	1018G		- 10		over Manager
		* 当时能弱;	(RL).2/015			0
# * ##	18	•新信用的	1002-01005		事件编型法官	48 88 88 -
		())()()()()()()()()()()()()()()()()()(001100.00000	1837	RMGE RREE	
			R(6)	1476		0 2525 0 2527
The second se				854		H TRUCK

4 情报云脑

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

	明御『主机安全及	2管理系统 2001	last 🖂
3	е на		
G	0 442 0		
-0	an a		
	117°403		
	11.8418		
	1850	情报云脑	
	मामालंग		
	#889	Ies. P. BB. Standsharmann, PRA. PER. TAB	
	9989638	Ni statis-ju? org. 13800964194-3571670008565030404 www.ovy Pro.anglish.word TilleoraiCright	
	Bake.	그는 그는 말씀을 많이 가지? 친구는 물속 그가 가지?	
-6	Anna -		
	1240		
	终于E46 期		
	TT SE TRA		
	A MARKAN AND A MARKAN		

5 资产概况

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



	明御 " 主机安全及	28理系统 2001								test ~
10		単立 / HP95 / HP90 南戸戦況	¥[]							
12	*****	828758 ¥21.97*	Antes Sector	夏季 ~			00.000	É.		0
-3	10°88	37*8B	和東分類	PHU	操作系统	着信在线时间	经建筑市	新新城市	输传项	
	ROMA		PCE	10.20.98.55	Windows 10 Entrepri	2019-05-20	2.0.9.1	₩₽单		80
	1.11.CM	🖂 🔇 Kössthost Asca	Linus	192.168.27.115	CentOS release 5.9	2019-05-09	2.0.9,1	新新市		6218
	12.804	@ MOBAN	Window	10.50.6.159	Windows Server 201	2019-05-10	2.0.9.1	新新 中	-	-
		O OUSER-MITTOL	Window	192,188,27,200	Wildows Server 200	2019-05-16	2.0.9.1	0.010		8258
	WERE		Kenn.	192.166.27.22	Windows Server 200	2018-06-18	2.0.9.1	W###	-	1611
		webeautec	Window	192 188 27.25	Windows Server 200	2019-06-17	2,0.93	MP9	- 22	501R (
-		O CHENLEI-OF	PCIE	10.11.95.207, 102.168.164	Windows XP Profes	2019-06-17	2.0.0.1	#90	88	and the
	22222	© OHENER-DU	Window	10.11.35.207, 102.166.164	Windows Sarver 200	2019-05-13	2.0.9.1	*10	10	1010
- 10		0 000-456781	PC#I	10,11,35,207, 102,168,164,	Windows XP Profes	2019-05-13	2,0.9.1	未知	100	1918
	ተላቸዋ	HUTT-74E3E	Window	10.20.28.55, 192.968.247	Windows Server 200	2019-05-15	2.0.9,1	¥50		1818.3
		O @ HUTT-EBIOR	PCHL	10.20.28.55, 192.168.247	Windows XP Profes	2019-06-17	2.0.9.1	未知	10	1210
		C WIN-BATTHO	Window_	10:20:28:55, 192:168:247	Windows Server 200	2019-05-20	2.0.8.1	#30	- 10	ARM .

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

HOW BLA										
2185	P38 9667	Mat 94	5 88-	1			mail	1387		
0 =	W.DEIER 13 18 .	#15\$01\$ 20	设置和数据符					-	医神顶 网络	
	第户名称	新闻分组了	阿察血控制	Piblé	操作系统	和后在城时间	的现在不	防护电影器	使性症	
	@ ed= 207	Linux服务器组	AND HIS COLUMN	172.16.1.37	CentOS release 6.5 (Final)	2018-12-12 10:21:02	2.0,7.3	Bisheter.		1418
	@ ede-32	Linux保持關鍵	棲止燃炉 回动转炉	172.10.1.32	CentOS release 6.3 (Final)	2018-12-12 10:21:41	2.0.7.3	Billion		62:11
	🔞 edr-41	Linux提料翻接	日常公司	177.16.1.41	CentOS release 6.5 (Final)	2018-12-12 10:23:44	2.0.7.3	11994	50	(RIS
	@ EDR-PC	PCH		172.16.1.42	Windows 7 Enterprise Edition	2018-12-11 14:15:02	2.0.7.3	(Date:	88	-

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



219	He Rame		网络克严				(max)	INTE.	3	1
	3/-2n	HALOH	· 8*80 :	EDR-PC		415-71203164	SM64	MMG	10112E	
1	• -di-207	Constitution (Sec.)	新疆分词:	PCig		2018-12-12 10:21:02	20.7.2		-	-
112	@ vdv32			BONR O		3010-15-12 10/10/41	2.0.7.5			-
	© x0::41	Linux最具制度	· · · ·	Double of		2018-12-37 10:25:44	20,7,8		- 10000 (-
	O STR PC	708	新运送空 ·	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		2018-12-11 14:15/12	2073			-
IR:	O MILON	WindowsBell		W26.	Lhan_	2018-12-30 10-15/34	2033	未知		-
125	O'MN-96-2	Wedsetlill	伊姑迎 (177.16.1.42	itan	0010-12-11 14(15)08	2.0718			-
. 16	ØW887238	Windows Hill	操作系统。	Windows 7 Enterprise Edition 64-bit	Conter-	2010-12-12 10:56:57	2033		22	-
	• sebproteiter-22	Linus Barrier	/€14HE © (2.0.7.3		2014-12-12 1023:06	207.5		1.0	-
	O WIN-2008-18	Windows ###			Enter	2014/12/11 14:15:21	107.8		2.22.00 C	1893
1.3	G WULPC	PCB		ACTR CON	-8.00	2018-32-32 17:50 23	207.5		-	-

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

6 资产指纹

点击"资产概况"对应资产行的"查看",可看到该资产的功能模块。

6.1 终端详情

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

意见 / 此产管理 / 资产概况 / HUTT-PC		扳回
HUTT-PC		
所屬分组: PC组	操作系统: Windows 10 Enterprise Edition 64-bit	
IP地址: 10.20.28.55	终端版本: 2.0.9.1	
资产指达 系统助护 网络助护	Web应用助护 工具箱	
#编讲辑 — · · · ·	HUTT-PC (#38, POH)	
金听湖口 · · · · · · · · · · · · · · · · · · ·	● 网络信息	
运行进程	IP抽址: 10.20.26.55,192.168.153.1,192.168.247.1	
11	MAC地址: EC-F4-BB-78-67-02,00-50-56-C0-00-07,00-50-56-C0-00-08	
10100 LEEL	〕环境信息	
THE S.	操作系统: Windows 10 Enterprise Edition 64-bit	
	处理器:intel(R) Core(TM) /7-4700MQ CPU @ 2.40GHz	
	主版: Alienware	
	内存: 7.9368	
	硬盘: Samsung SSD 840 EVO 120GB	
	显卡: NVIDIA GeForce GTX 765M	



6.2 监听端口

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

医产制 取	1.002751P	网络古护	Webizmasse	工机和			
终端羊茸							0
台切出口	當時	和日号	同語协议		NEWSHIEL	initp	
运行进程	135		TCP		sychostaxe	0,0,0,0	
账号值息	445		TCP		System	0.0.0.0	
软件信息	3389		TCP		sychostexe	0,0,0,0	
	4915	2	TCP		wininit,exe	0.0.0.0	
	4915	3	TCP		sychost.exe	0,0.0,0	
	4915	4	TOP		sychostlexe	0.0.0.0	
	4915	5	TCP		lsass.exe	0,0.0,0	
	4915	7	1CP		services.exe	0.0.0.0	
	139		TCP		System	172.16.1.42	

6.3 运行进程

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

月产指纹 苏	統防护 网络防护	炉 Web应用防护 工具	相					
纯错详情								e
监听编口	进程名	进程路径	内存占用	CPU使用率	启动争取	自动的	垂作项	
调行进程	System Idle	N/A	0.08	0.00%	N/A	2019,	結束詳報	
账号信息	System	N/A	0.0B	0.50%	N/A	2019.	给用进程	
软件信息	Registry	N/A	0.0B	0.50%	N/A	2019,	結束過程	
	smss.exe	N/A	0.08	0.00%	N/A	2019,	结束进程	
	C5F96.6Ke	N/A	0.0B	0.00%	N/A	2019,	结束进程	
	wininit.exe	N/A	0.08	0.00%	N/A	2019,	他來进程	
	C\$F\$15,6100	N/A	0.0B	0.00%	N/A	2019,	暗束进程	
	services.exe	N/A	0.0B	0.00%	N/A	2019	結束进程	
	lsass.exe	C:\WNDOWS\system32	19.16MB	0.50%	C:\WINDOWS\syst	2019,	结束进程	
	winlogen.exe	C:\WINDOWS\system32	9.10MB	0.00%	winlogon.exe	2019,	结束进程	

6.4 账号信息

在"账号信息"中可以查看到当前系统的账号包括隐藏账号的相关信息。



er-alix a	usisin Misisin	Web应用防	P ING			
10(31)212						
BARMO	用户省	root权限	用户组	用户状态	空間開始间	上次控制
运行进程	Administrator	m	Administrators	•已禁用	下次登录时青更改忽码	时间:N/A 朱愿:N/A
10日日日 10日日 10日日 10日日 10日日 10日日 10日日 10日	edr	m	Administrators	* EBR	亦不过時	附间:2018-12-11 15:08:05 床間:172.16.2.15(局期风)
	Guest	西	Guests	• 已禁用	永不过期	时间:N/A 來源:N/A

6.5 软件信息

可以查看该终端上运行的软件、以及软件厂商、版本号以及软件的安装目录。

語合語論	系统防护 网络防护	Web应用结护	工具線			
终端洋情						0
追防第□	软件名			ГŘ	版本号	安装目微
运行进程	明御主机安全及管理系	庑		杭州安恒国意技术股份有限公司	2.0	C:\Program Files (x86)\D8AppSecurity\EDR
际带信度						
软件图题						

7 系统防护

点击"资产概况"对应资产行的"查看",可看到该资产的功能模块。

资产指纹	系统防护	网络防护 Web应用防护 工具箱		
)	主动防御 主动把戴恩意程序运行,防止对主机造成质置。	病毒查杀 针对网络中遗行的病毒。本马进行全面宣杀。	
	:::	漏洞管理 案时高调官方发布漏洞补丁并一键伊复,对绵作系统进行全面 加度和调试。	系统登录防护 支持P屬白名单、计算机白名单等多种登录历护机制。并这 进行關口令检测。	EWH
10	0111	进程防护 配置进程的黑/白名章。 阻止恶意程序的运行。	文件访问控制 直控目标文件/目录的改写操作。	



7.1 主动防御

7.1.1 主动防御

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

7.1.2 文件实时监控

实时监控文件的状态,在文件执行或者进入主机时进行扫描。

扫描时机: 文件执行时进行扫描(默认)。

排除设置:如果不希望扫描指定程序,可以在此设置忽略,模糊匹配。

文件实时监控 系统防御	文件实时监控 实时监控文件的状态,在文件执行或者进入主机时进行扫描。	
执行防御	扫描时机: 🗹 有文件执行时进行扫描, 不影响性能	
病毒免疫	有新文件产生时扫描新文件,占用少量系统资源存储介质(U盘,移动硬盘)连接时自动扫描	
	排除设置: 28略指定程序的动作 例如: C:\test.exe	
	发现病毒时: ④ 仅记录日志	
	○ 直接删除	

7.1.3 系统防御

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



文件实时监控 系统防御	系統即	5部 桥指定文件不被愿意篡改成执行,确保系统安全	脂质并记录	
执行防御		防护项目	防护说明	
病毒免疫		禁止创建Autorun配置文件	保护碾盘不被自动运行的昂意程序感染	
		禁止在系统巨豪下创建未知二进制文件	可關止部分思慮程序创建	
		禁止通过命令行下载可执行文件	防止通过系统命令下继未知可执行文件	
		禁止修改Host文件.	保护本地域名解析不被恶意重定向	
	8	启用自身防护	保护目身的文件及进程	

7.1.4 执行防御

勾选指定防护项目,防止指定命令被恶意利用。

文件实时监控 系统防御	执行数	御 定命令嶺岳潭利用,対主机造成誘물。	阻断并记录
执行防御		防护项目	防护说明
病毒免疫		禁止在临时目录执行程序	可阻止卸分基度程序执行
		禁止通过命令行滚加用户账号	防止恶意程序调用命令激加张号
		禁止通过命令行修改整号激活状态	防止思覺程序調用命令酒停改服号激活状态
		禁止通过命令行启动FTP	防止调用FTP命令下截其他基置代码
	8	禁止PowerShell隐藏执行脚本	可聞止大部分无文件把矿窖毒
		禁止运行远程脚本	阻止重接通过UPU,地址运行脚本
		禁止运行HTA脚本	阻止危险的HTML应用程序执行

7.1.5 病毒免疫

可针对顽固流行病毒进行智能拦截。

文件实时监控	病毒免疫
系统防御	针对顽固流行病毒进行智能拦截,使系统免疫这些病毒。
执行防御	病毒免疫:
病毒免疫	



7.2 病毒查杀

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



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

均毒查	₽.	
3	共扫描1302个文件,发现27个病毒木马文件 Hallenting 2018-12-10 11:28:18	2回唱席 送力隔离 进入路里区 重新白细
	文件器径	病毒名称
10	将毫木马文件0/27	
- 20	D:\SHELL\all.asp	高總統件(Script.ASP.RootKit.10.e)
11	D:\SHELL\aspx.jpg	后门(Backdoor ASP,Ace.ar)
	D:/SHELL\bin.asp;.gif	前门(Backdoor:Akspy)8.1443)
	DNSHELL\conn-aspx	語[3(Backdoor,Akspy(8.1443)

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

7.3 漏洞管理

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



画気 / 田州 漏洞管理	*管理 / 另外概况 / EUR-PC / 展明管理			100
	发现6个高危漏洞,需要立即修复。 最同時期間目的18月8日,开始時期日期开始5月7日中期時期日期 已來考(23) 已錄用(4)		-9995	<u>URIN</u>
	展開种丁描述	发布日期	转丁大小	状态
	最次 到300/6			
	⁽¹⁾ 针形CVE-2018-1038的Windows内核更新(KB4100480)	2018-04-10	22.10M8	特修复
	Microsoft 管理控制起文件指式中的属目可能允许拒绝服务(KB3051768)	2015-05-12	969.54KB	神经复
	◎ 這是奠重的以中的黨章可能允许把總服用(x83036491)	2015-03-11	1.52MB	待信度
	◎ Windowsi內核權式組动機與可能允许這種的以升代码(XB2876284)	2013-10-08	780.34KB	计师变
	0 "大店" 商專利用未经授权的数学证书进行取簿(KB2718704)	2012-06-03	257.59KB	侍使度
	♥ WT2±20数2字记2+307ml(元:(平期5編(K82641690))	2011-11-9	226.56KB	计计学规

根据中心和端主机是否可访问互联网的不同情况,漏洞补丁的获取有以下几种情况:

7.3.1 只有中心可访问互联网

通过 admin 账户登录,中心下载补丁后推送给端主机修复。 步骤1. 使用 admin 账号登录,依次点击"Windows 补丁库管理","在线更新补丁","收集补丁"。



步骤2. 选择相应资产进行补丁收集(即检测需要下载的补丁)。



ペールは / Antitit / Westmann TREE Windows社工業管理				
-	血用到新产			2.
	全部资产 (2014)日 (2014)日 EDR (2017)日 (2017)日 (2017)日 (2017)日 (2017)日 (2017)日 (2017)日 (2017)日 (2017)日 (2014)日 (201	1/1 	田志福宏洋 ○ 現井名・IP ○ EDR-FC・172.16.1.42	9/1
		Rin 🚺	3 Acie	

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

Windows补丁库	管理			
已下数补丁	在线里新补丁	南线更新补丁		
EDR管理中	心可联互联网时,	建议在线更新补丁库		
1 82.54	Г			
5月4日日	ware I comm. The	ddine T		
收编	4bT=			
	18 (5/27/22 Beller	Tony . WEER TERROR.		
2 F83+N	Г			
TH	Televent	FFT THE		

7.3.2 只有端可访问互联网

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



単页 / 当时 潮汐繁理	教師 / 田小板足 / EDR-PC / 編制数価			
	发现6个高危漏洞,需要立即修复。 加速和规定时间2000年,开始的加速用此加速于64-88838.088 Exem (200) Example(4)		-19452	<u>Taim</u>
	漏洞种丁描述	发布日期	补丁大小	状态
Sec.0.	Weithors			
D	日本計算ICVE-2018-103885WindowsPitE更新(KB4100480)	2018-04-10	22.10648	(6(E3E
-67	◎ Microsoft 實理控制由文件相對中的編詞可能的由戶目格服务(KB3051768)	2015-05-12	969.5468	侍你是
301	◎ 近程桌面协议中的期间可能七环接收服务(KB3036493)	2015-05-11	1.52MB	待修复
12	Windows的相關在我認知識面別結果的問題指行代码(KB2876284)	2013-10-08	780.3483	体控制
- 30	◎ "火焰",與專利用未经授权的數字证书进行取集(KB2718704)	2012-06-03	257.59KB	待使复
:0	0 期15的数字还当利和5c;并积3g)(82641690)	2011-11-9	226.5688	待律规

7.3.3 中心和端都不可访问互联网

通过 admin 账户登录,离线上传补丁后,中心推送给端主机修复。

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



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



(件() 编辑() 音看(V) 丁具(17) 悲助(00)			
组织 • 🤃 打开 •	共享 • 新建文件夹) 🗉 • 🔟 (
😧 收藏夹	名称 -	修改日期	类型	大小
🐞 下载	beolawob 🏭	2019/11/21 19:09	文件夹	
■ 東面	7z	2019/11/21 19:07	文件	1,239 KB
运 截开访问目的方面	1 7 z	2019/11/21 19:07	应用程序	778 KB
二 库	liberypto. so. 1. 0. 0	2019/11/21 19:07	0 文件	2,418 KB
🗉 🔄 视频	🐴 libcrypto-1_1 dll	2019/11/21 19:07	应用程序扩展	2,064 KB
田 🎫 閏片	libssl. so. 1.0.0	2019/11/21 19:07	0 文件	483 KB
	S libss1-1_1 dll	2019/11/21 19:07	应用程序扩展	363 KB
ゴ 🚽 📋 四小	linum sh	2019/11/21 19:07	SH 文件	1 KB
🌉 计算机	🚳 muvcp100. dll	2019/11/21 19:07	应用程序扩展	412 KB
	🚳 msvcr100. dll	2019/11/21 19:07	应用程序扩展	756 KB
🗣 网络	runlog	2019/11/21 19:09	文本文档	1 KB
	🗋 vul đ	2019/11/21 19:07	文件	814 KB
	vuld. cfg	2019/11/21 19:09	CFG 文件	1 KB
	vald	2019/11/21 19:07	应用程序	500 KB
	🚝 vald_2019_11_21	2019/11/21 19:09	WinRAR archive	2,422 KB
	🔄 开始下载	2019/11/21 19:07	Windows 批处理	1 KB

步骤3. 将下载得到的一个 zip 压缩包在步骤 1 中的上传文件处上传。

	用的认证 / 医前营港 / Windowsh门店管理
R. HPWE	Windowsky J m and
0 skete >	日下數补丁 在成更新补丁 网络更新补丁 2
常用于 成开始。	EDR管理中心无法联互联网时,输以着组更新补丁库
HERROR EVENLE //	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
的細胞性患病包上用	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
前和年時時	2011-12-121012-10150:000-1-013-000-0-0-013-000-0100-0100-01
SIGERAR.	(2) FREESTRE Teles: - FREETREETREFEETE
Windows H T IF TE T	1 78
104 510	3) 上行南线补丁也
WebSTATE	Lexile-Telemeno.
REPUBLICAN	上W完UU 100%

步骤4. 通过租户账户登录,到对应资产的漏洞管理功能下,可进行漏洞修复。



13	"管理:/ 田戸範兒 / LDR.PC / 漏科管理				
	发现6个高危漏洞,需要立即修复。 副時期日期時間14月月,开始的10月月前前本会中期時期1月日 日前期(128) 日期8(4)			-10153	antes 🛛
	麗丽林丁羅述		发布日期	静丁大小	状态
	LE1312010/6				
-					
	● 計EULVE-2018-1038的Mindows円的图例(0684100480)	#2 54 P	2018-04-10	22.10MB	经济发
	 計划CVE-2018-1038的Windows内线更新0584100480) Microsoft 管理控制由文件相応中的编码可能允许拒绝股份(K83051768) 	#E 24 1	2018-04-10	22.10MB 969.54KB	倍体加 份权加
0 0 101	 ● 計划CVE-2018-1038EDWindows内核型数(K84100480) ● Microsoft 管理投影台文件提出中部環境可能分片拒绝最赘(K83051768) ● 近妊娠期份以中的配向可能分(所包透影的(K83056493) 	#2 54 5	2018-04-10 2015-05-12 2015-03-11	22.10MB 969.54KB 1.52MB	(中位)里 (中位)里 (中位)里
	 	#2 54 S	2018-04-10 2015-05-12 2015-03-11 2013-10-08	22.10MB 969.54KB 1.52MB 780.34KB	
	 計切てVE-2018-10588日Windows内核運動(X84100480) Microsoft 管理指統自文件相比中的編録可能が正常直接服务(X83051768) 近妊娠期後以中的編録可能が正常直接緊約(X83036493) Windows内核構成変換循環可能が正常提供方式(K82876284) "大治・病毒利用未受感吸的影響(正有进行预測(X82718704)) 	#2 54 5	2018-04-10 2015-05-12 2015-03-11 2013-10-08 2012-06-03	2210MB 969.54KB 1.52MB 780.34KB 257.59KB	(合修复 (合修复 (合修复 (合修复 (合修复))

7.3.4 中心和端都可访问互联网

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

⚠ 注意

补丁修复存在一定风险, 需测试后再进行修复, 以免对正常业务造成影响

7.4 系统登录防护

在系统登录防护功能中,可配置策略对远程登录做限制。

#184031	
· 2019 -	(85% ×
市産電車時的	
登录莱用地。	補助時
	 即/PP3團 域名
(P/IP范围:	
计算机名:	
时初始略;	(C) Hainelin Z Contraction
" 党理方式)	(満足所有策略)元件登録、
*秋街:	 回用 ○不屈用
	Recitus alle alle alle alle alle alle alle all

可配置防暴力破解策略(针对 Windows 操作系统的 RDP 协议、Linux 操作系统的 SSH 协议)。 默认的联动效果:当有远程 IP 触发策略,微隔离模块会自动添加一条规则阻断远程 IP 对本机 3389 端口或 22 端口的访问,时间为 60 分钟。



18月 / 四十世道 / 四十四日 / 10月中日 / 1 新統整要助計	101225P			15		-
RANF CHA	防暴力破解範圍		×			•
	• 单个印度求时间应置:	120	积内			
DUNU U/I+ZMA	* 登录失败为数:	10	22		#2	IV/TIL
	< iPhilippini	3000	Бi			
		R/A #32		ł.		

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

100 / 100-100 / 100-102 / 100-10 / 1 系统登集功许		
	第日今世別に	•
Dist. Kelshing	* (REDACTORNE) : 36000	WE INCH
	KTIN MALE	

7.5 进程防护

7.5.1 进程黑名单

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

进程防护 已关闭 所有不在黑名单规则内的程序都会	被放行。 黑岩华模式 🖓	关闭		
周期登録作録示 沿所近有高名) 建设:开启"但记录"废整一起910	单后,若设置红斑斯并记录,所有能多问者。 4、避免地止正常的程序,确认无问题后,7	时的程序运行推动被用之。 F启。		
新维斯谷单 批量导入	制新列表 更多 ~		898.5.5.971	d l Ø
图 规则内容	美型	番注	启用规则 操作	a.
		誓无数据		

7.5.2 进程白名单

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

选择"自动评估",再选择一个路径开始扫描,扫描结果将自动添加到进程白名单。



进程防护 已天闲 所有不在白名单规则内的程序都会被	粗止, 白老单模式 ~		关闭	Ψ.
高度性操作提示:高用进程自名中 建议:开启"议记录"或 包 一段时间。	后,教设置成新新并记录,所有不在规则 避免期止正常的程序,确认无问题后,J	的表示的程序运行都有知道定。 7回。		
新設白名单 批量基人	単数列表 更多 ~		建制入土地学	0 6
1 規則内容	展型	香注	启用规则	操作项
		智无数据		

7.6 文件访问控制

监控目标文件或目录的改写操作。

文件访问	(2来)				164
文件访	同控制 巴开南				•
-	RAARDA REESTROFFER	网络 作一所有访问自己河在日本检察中 副 别			
100					
1.028	文件指经	業型	御注	编件:10	
12	C/Program Files (x86)\	日素		5018	80**
131	C/\Lisers\	日間		98	899
0	C/\Windows\	当後		940 B	889
10	DSProgram Files (x86)s	百葉		0010	(101) (101)
130	Drivoviti	百要		编辑	1999 -

8 网络防护

8.1 微隔离

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

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

and an				
	光闭本地翻口		×.	
16万间业务之间进行资源采用并指确则的常志3	WAR A THE HUBBER	1998日号,多个可用出号;分围		
Instead Income	445.135.138	2		
	L			
RESIDENCE AND AND ADDRESS		1254 452 3		
HE CONTRACTORNEY NO				
TELEVISION ANALY				



	规则类型	本地EP	本地城口	远程IP	远程端口	协议类型	处理方式	剩余有效时间	順進	启用规则	操作
13	🙁), taken	×	445	×	- i C	所有	粮止	.水赤	关闭本二		编表
	🙁 人比和时		135	•	1	新闻	藉止	ф.2,	关闭本。		1923
		*	139	*		斯有	題注	8A.	判闭本		101

新增规则中,各参数意义如下:

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

应用举例:

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

规则一		规则二	
规则类型	双向规则	规则类型	双向规则
本地 IP	*	本地 IP	*
本地端口	445	本地端口	445
远程IP	192.168.1.0-192.168.1.25 5	远程 IP	192.168.1.10-192.168.1.2 0
远程端口	*	远程端口	*
协议类型	所有	协议类型	所有
处理方式	阻止	处理方式	放行



(11-11日) (11-11日) (11-11日)	使产档记 / EDR-PC	win7 / 他包裹	() #028099		
107,940		16500F 💿 3	R) AUHERT		19982-07, 80-1-5-290220-1021201 (
・本地的	2003.0003.0	PERIO -			
*本地論口	的明明: 建硫入0+6	6352000007	¢.		MEXH5. MCIENT 0-65535
+ TEASTA	wind I wake, i	PTEM"			** (Carinal)
* 边程跳口	10100 . WEAD-9	6352(PROB CE)	έr.		
协议美型	新有				
处理方式	 ● 総行 ○ 単止 				
启用规则					生物理解
有效的词间	天	91	\$	E!	天教最大治999、小时最大治24。分、 砂織大治60、不能入表所永久。

8.2 防端口扫描

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

訪謝口归描	12					-
matting (1979)	Elephinasisp			-		
AP710年入2年3月1日日の11月1日日の1日日の1日日の1日日の1日日の1日日の1日日の1日日の	IP地址	剩余放空时间	操作项			8
* # \$ 0*\$(#100)358 : 120		能无数提				
* #LX515428C.02# - 10						
* PEERSH 500		1000c X8				
18.9						

8.3 违规外联防护

违规外联分为黑白名单两种模式,只能选择一种模式应用,可随时切换另一种模式。

8.3.1 白名单模式

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

新增白名单:输入需要加入白名单的 IP 地址或 IP 地址段。

批量导入:可下载格式为.csv的模板,填好模板后上传。



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

海伐外联	防护				Satist
追和外 自航支	联防护 <mark>12000</mark> 外接白名草防御權式。 百名草根式 ~			仪元兼	
		RATIN DE .	the later		
100	PRU	關注	启用规则	操作项	
	192.158.0.0-192.168.255.255	就止运动互联网被略	•	-	
	172.16.0.0-172.31.255.255	禁止访问目际网络略			
	10.0.0.10.255.255.255	某止动向互联网兼赋			
			共3.册 20条/面 -	6 i 5 i	1 I I

8.3.2 黑名单模式

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

违规外联防护				Rec.MI
违规外联防护 (000章) 当前支持护行名单防制模式。 量名单据式			(928)	
10::::\$r=::::::::::::::::::::::::::::::::	Di Chiristen (Kreznich, Skillinger (S.			
机电量合作 杜拉马入 和而为	東 一 臣弟 い	信证人天何争		
IP地址	間注	ELHINEN	INHEIR	
D MURSon	已知念113452条相同(
		共1 美 10 船 类		#在 1 R



9.1 网站漏洞防护

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



的 出版 同時 時 同時 同時 同時	户 田井倉 SQU主入攻击。	XSS跨站、Web容额。	及应用漏洞进行	实时物种。 日定义	三戰退示	
SQUEX	XSSREE	应用程序编词	自亲义规则			2 文件名解析職務助护
RENID	类型	状态		关键字	描述	■ 禁止浏览畸形文件
100	SQU主入			post url	探测数字型SQU注入防护	
101	SQLIEA.			post url	探测学符串型SQL注入防护	
102	SQU主入			cookieļuri	屏藏MYSQL操作中施险的存储过程	目初時間は短期
103	SQUEA			cookie{post[url	对数据库进行数据意间操作防护	
104	SQLIEA			uri	禁止基于时间的注入判断	
105	SQLIE 入			cookie post url	防止对数据库进行创建、删除、备	

9.2 CC攻击防护

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

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

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

- ▶中:对于低级别无法防御的情况(可以自动执行脚本的攻击工具和浏览器无异),可以尝试开启此安 全级别,该级别可以智能判断访客的真实性,并且无需访客参与验证,使用了 Cookie、JS 脚本混 合验证方式。
- ▶高:对于长期处于被攻击状态的网站,建议开启高级别模式,高级别模式安全性最高,会在访客首次 访问时通过输入一个随机的验证码来确认(图片方式验证码,具有对抗图片识别工具的干扰色), 通过验证后浏览无需再次输入验证码。

9.3 网站访问控制

网站访问控制可以对一些特定的请求在网站漏洞防护之前直接进行阻断或拦截。

【結访 肖控制					88
网站访问控制 日开幕 史志新董印度广东新经,可对新生的	的市會成页面进行政行成元载。 自住义元载	開示			-
WRINAWERで、: PFIEWを見た他へいの場合である。 PWG人を引き、D2 1192.168.1.**	1 192166,1.101° 100∰ 1192.168.1.101-193 , 30⊕ 1933.5° (COBHENDE	2.168.1.201"			
IPEB	均衡器	描述	建度方式	100	接作 组
192.168.10.*	www.3000000.com/a	dmin	允许		1001日 日初本



9.4 网站后门查杀

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

atani04				
1658	20			
E 3	文件路径	病毒类型	编成时间	操作项
	$D\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	PHP执行命令术马(n.994)	2018-12-20 14:07:38	12
11	D:\1shentou\dictionary\fuzzdb\attack\sqll\sql-injection\exploit\ms-sql_backup_writefile	一句请未马(fuzzy)(n.fuzzy)	2018-12-20 14:07:38	100
<u>61</u> 34	D\1shentou\ulictionary\fuzzdb\web-backdoors\asp\cmd-asp-5.1.asp	ASP50行命令本马(n.891)	2018-12-20 14:07:38	(CM

10 工具箱

10.1 勒索防御

10.1.1 风险评估

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

動素防禦					
网络评结	风岭评估				开始评估
买时防御		•	0		
	第日令	系统藏词	思想进程	两元04日	

步骤1. 若其中一项或几项不安全,点击查看可以查看检测结果详情。

10.1.2 实时防御

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



风险评估	实时防御			
实时防御	動素软件启动防护引擎:	法配置影响进程启动的护全局配置		
	勒索软件加密防护引擎:	通过行为分析对未知物素软件的加速行为进行实时和断	白名单设置	

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

10.2 挖矿防御

10.2.1 风险评估

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

挖底" (55-80)							
7025710 2011080	风险许信 <mark>使制制</mark> 但矿肉毒会大量得	n Mart Robert Males R. R. Gelder 7 (2019) 11	R it Andri Miblicfi	11月11日 11月1日 11月11日 11月11111111	La Lienalogora	545	FIMEIFER
	0	•		0			
	1004 (1007)	利用用用	前原出州 (安全	新想出程 1919	DNS防止重定	野瀬外和	

10.2.2 实时防御

开启挖矿软件启动阻止,每当进程启动时触发一次检测,实时防御挖矿软件。

挖矿防御		New.
网络汗性	之时防御	
并时仍 到	1997年の時期の1日止: 〇〇 は東京町町田谷の2017年主日英国	

10.3 性能监控

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





10.4 外设管理

10.4.1 无线网卡

Г

可选择是否开启外设监控、使用审计、外设权限。 权限说明: Ø禁用:无线网卡插入主机将不被识别。 Ø放行:默认选项,不进行任何限制。

存储介质 无线网卡	无线网卡 对无线网卡进行访问控制,有效解决内部数据泄漏问题。
	使用审计: 开关打开后,设备连接或断开时会产生日志
	权限控制: 禁用 放行

10.5 文件推送

当需要下发文件、安装应用程序到资产上或者远程执行命令时,可以使用文件推送工具。 Ø上传的文件:在此选择上传的文件或脚本,文件应该小于20M; Ø下发后立即执行:如果需要立即执行文件,将开关打开; Ø执行参数:脚本需要执行时携带的参数; Ø备注:关于此次文件推送的备注信息。



文件推送 可以用于下发文件、安装应F	用程序、远程执行命令,			
文件上传	二 上传文件	0.0B	清空上传文件	
	文件应该小于20M			
下发后立即执行				
执行参数	脚本或程序的执行者	9 <u>81</u>		
备注:	请输入备注信息不正	01±50个字符		
	推送			

10.6 屏幕水印

当租户需要对通过屏幕拍照泄密数据的行为进行溯源,可以使用屏幕水印。

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

屏幕水印功能界面:

水印内容	🖸 资产名称 📋 🦻 📄 MAC 📄 登录用户 🔮 系统时间	
自定义内容	期極入由定民内留	
内容颜色	#2727D3	
字俳大小	50	
文字倾斜角度	30	
行何期	80	
拔爾爾	10	



11 病毒查杀

查看全部在线资产的病毒查杀情况。

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

病毒查杀									
- AND	ALLENSING STREET	全盘扫描	立即編集	2118					C
0 #	前页已选择1项,未进	M#1項 1	12					全选局页	反進電页
	资产名称	和属分组了	ip地址	操作系统	病毒数	上3月1月月月月月	扫描状态	操作项	
	M9EZO6HBUU4	系统默认道	124.160.26.187	Windows 7 Uttl	52	2018-09-25 16:27:16	未扫描	快運扫描	御上的新
	@ WU-PC	系统默认图	124,160,26,187	Windows 7 Ulti	0	2018-09-25 14:24:12	未扫描	快速扫描	19127-000
						共2条 20条/页		1 > 8	HE I F

12 漏洞管理

查看全部资产的漏洞扫描情况。

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



۲	明御『ヨ	机安全及	管理系统	2.0.12.1									tae 🖂
ŵ			RA / RA RAME	tere / acritere			-						
Ð			Windows R	(CB) Linux	Unix系统識別	其他加加							
- (3)	8798		接用/*		11†								
	80.835		(lensis	42.53	8.182						0011/08	τ	000
				资产名称	MRSB	● 日本	P教徒	用作系统	RREA	可透識用	EBRRR	上次日盛时候	状态
	RNAL			@ 22.58	Windows服务	197225 (2020)	192.185.23.68	Windo	89/E9	6/48	ż		LINE WORL
					04	CMS (m)							
	10.000			CHENG-CRH BABOADC	PCHE	BBB	192.165.27.212	Windo	35/35	0,/18	0		EHEREN
				@ WN-LDIAD	Windows展着	extrail CALC	10.20.82 249	Windo	0/0	0/0			扫描完成
0				AGMORGE	20.02	888							
-				O DEBKTOP- SNPQVED	PCHB		10.11.58.202	Windo	0/0	b/b	ů;		白梅究成
-00	派式整理			@ TZC+PC	POB	(00)	192 106 23 60	Windo	ovo.	0/0	o		目前死术
										共五曲	20県/雨	la a rei	101E T 2

13 批量配置

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

步骤1. 选择一个资产开始录制。

nt main m				
(BYT TRANSPORT			
all and the provide state		87°	3描检查 17 / 1981	关闭网站漏肩筋护 2018-11-00125500
and the second sec	100.			
1	master1 27,44			
Milesiog L	MN-yh-2012	1.00	and the second s	Mark of the set of
MALING INVERS	WEB27.13	2	CPR-MI	XHI// QX/+#11
	WIN-9PSQMF6NQ3P			
The second s	DESKTOP-25UVO8Q		the state of the local division of the local	
	Tocalihost.localidomain		_	
II 白服礼 墨 田林 6	edr-207-centos6.5		1991+	非应该用意动作的
(12008-11 NO 175560)	3		17.590)	0.3010-11-30 27-58-03

步骤2. 进入录制页面,点击"开始录制",选择需要批量应用的配置。



集页 / 通行管理 / 图示概记 / Mith-yh-2012	0	开始教制
MN-yh-2012 Emwember	1) 新配置如下改编,有元券记录在毕止条州的和34年8
形理分组:Windows服务器但	操作系统:Windows Server 2012 14: Sti	的毒童派
iPitat : 17.	修施后本:20.7.4	同站每门置杀
	/	性配直控
部門論成 系统防护 网络防护 Web应用防护 工具補		做隔离
受知牛或進転过程中 不支持副新而重		网站访护
操作,奇妙特导致学制模板过程停止		整景防护
		网络防护
(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		进程防护
STER HACKING MACHINE DO AS		外设管理
N-Digg 100-00-1		勒索防御
○ 环境信息		文件访問控制

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

14 流量画像

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

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

通过自定义模板,资产分组、资产标签、资产名称、资产 IP 过滤查看。

画像 ()Windows服务器	🔕 Linux服务器 🥮	PC	清空数据	自定义模板
0	103 160 200 192.168.34.165			-
0	192.108.3	192.168.34.153		
192 3492,168	3 192.168.34.141			•••
6	192.168.34.166	2.168.34.157		WEB服务器行为展示
192.168.34.152	192.168	1,34.15 192.168.34.151		
() 192.168.3 192.168.34.159	4 192 168 34,169 4 192 168 34,169 192.168,34,16	192.169-34.148 57 192.168.34.149		违规外联行为展示
192 158 34 1 1	92.168.3	192,168,34,162		
	192.168.34.168	192.168.34.161		勒索病毒扩散路径
.192 (P) 193	192.168.34.14	192.168.34.156		
Č.	192.168.34 192.168.34.1	43		邮件服务器行为展 示

单击某个资产可查看该资产的流量画像详情。通信关系图展示该资产的通信关系:



() WIN-J 192.16	URA191RR35 8.23.215		
通信关系图	通信关系列表		
		0	
		192.168.27.200 192.168.27.32	
		() 1921682828219 () 49216610.54	
		192.168.23.232	

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

方向	本地护	本地端口	远程即	话程端口	物议	开始回问	上次通信时间	通信次数	操作项
🚯 A38	172.16.1.255	138	172.16.1.48	138	TCP	2018-12-20 18:27:44	2018-12-20 22:27:46	21.	IR MAY
St 🚷	172.16.1.255	137	172.16.1.48	137	TCP	2018-12-20 18:18:20	2018-12-20 22:23:42	150	0 (364)
人益	172.16.1.255	138	172.16.1.47	138	TCP	2018-12-20 18:00:37	2018-12-20 22:24:30	23	188W
(合入站	172.16.1.255	137	172.16.1.47	137	TCP	2018-12-20 17:53:06	2018-12-20 21:53:07	51	ABH
人站	172.16.1.255	138	172.16.1.39	138	TCP	2018-12-20 01:01:08	2018-12-20 22:16:43	111	REMY

点击两个资产间的箭头,可查看箭头两端的两个资产的通信详情。

15 定期巡检

定期巡检可通过配置定期巡检任务完成定期检测。

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

和短期检								
ma	1 and 1			新新人民教育				
	28	600809164	推注	操作项				
	周围京动行道	2018-08-07 20:19:02		编辑	are.			
	的梅午市重乐	2018-08-07 20:18:18	半改变状	1818	801			
				共 2 条 20条/页	1	1	Æ 1	A



908

201400		10/2T /TT
BC 188	Tel: 1234 7903.	ALC: NOT THE REPORT OF
		and the second se

0 404	建定制化物生命,可以用发展发展中中的基础成为		
• 任务名称:	1842.5		
* 任所與制:	10.04		
* 謝辱良神 :	10.51	Ð.	
	新编员产将会同步自任务		
ः विद्वालिको ।			
19日:	(Bal)		
	10% Max		

16 移动存储

16.1 全网禁用

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

🥶 明国 * 主協会	全反管理系统					
5 m	第二日 - 1913年1月 					
- 98110	THE MERS 144	um 3				
15 ares		未接收设备: ④ 球对 只读 第四	_	1880		ans
87483	5000 WRENDA	审计: 👩 使用审计 👩 文件把负审计	-	A7500HBC8D4A0DCC	R# 2#	10 (10 (10 (10 (10 (10 (10 (10 (10 (10 (
N2211		adan adangah an un		ALL M 208/2		#E 1
100.010			_			
C.N.D.C.E.		ECH HOE	_			
2000			_			
110.010						
0.000						
S 154716 🔏						
iff anna -						
- X400						
2,599						



16.2 设备注册

如果需要对特定的移动存储设备开放使用权限,需要进行设备注册。 步骤1. 打开主机卫士界面,找到菜单栏中的设备注册;



步骤2. 插入移动存储设备(如图中的新加卷 D:),提交注册申请;



受 安恒主机卫士			≂ _ X
设备注册		×	
盘符:	新加卷 (D:)		
设备名称:	新加卷		
容量:	28.90GB		
厂商:	kingston		
产品型号:	datatraveler_3.0		
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		
程度時本、20121 佐吉定時本、25 00 15 75			

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

使用授权			
D 使宝 (京徳 ○ 藤田		
	o ne co and		
硬件信息			
设备供应商:	kingston	容量:	28.85GB
产品类型:	datatraveler_3.0	设备ID:	A75004BC8D4ADDCC
注册信息			
设备类型:	普通注册设备	注册来源:	DESKTOP-5NPDVEQ
设备名称:	移动存储	责任人:	
联系电话:			
申请原因:			
		C same	

步骤4. 点击确定即可完成注册。注册后该设备即可对所有资产享有使用权限。

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



17 日志检索

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

日志检索							
<u>@</u> **	sik : 1000		日志満型: 川			- 207 : 00.0207	
#185	H8: (1001		明明: []]	(重利	R R
But	18						
	资产 名 俗	TPIENE	MESHIT	1999 C	日志美型	霸建	服作項
	⊕ WIN-IM69NAC	172.16.1.67	Windows服务 副何	2018-12-19 20:20	腺力破解	发彩边理查录最力破解,IP:5.101.40.160(而三-德	20
	GEDR-PC-win7	172.16.1.42	PCHE	2018-12-19 20:05	文件协调控制	C/;Windows\System32\avchost.exe 型文件数据	放 有
	GEDR-PC-win7	172.16.1.42	PCIE	2018-12-19 20/05,	文件因司控制	C\Windows\System32\services.exe 冠文件数量	重要
	G EDR-PC-win7	172.16.1.42	PC语	2018-12-19 19:52	文件的均控制	C//Windows/System32/avchost.exe 端众件数据	20

18 系统管理

18.1 个人中心

可修改用户密码、修改用户真实姓名、修改头像。

个人中心	
	1a,at
	和中國政治
自己相关	
24, 31, 11 L	TO ANY
	傳道

18.2 升级管理

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





· 明御 " 主机安全)	及管理系统 20114	admin -
#	許可審理 / 系統面接 / 整理平均升起 建設工业14.6	
(5) 新可能理		
Re Hering	Dentition 1 1	
⊞ жино	高线升级 通过上传集线安装包进行开纸	
- BINE -	国南版本 1/2 0-10-4 西球市均匀	
管理 平台开版	12.0.10.4 上次更新时间	
MARKETELLA MARKETELA MARKETEL MARKETELA MARKETELA MARKETELA MARKETELA MARKETELA MARKETELA	注意事项 • 外级过程中位在苏邦平就正架进行,微确保升级过程中没有重要的任务进行。 • 升级过程师,诸功姆斯测定器,跟先姆斯导致开级失踪。 • 升级对话后,而前岸自动重点。 • 黑格升楼不能则能本升级,加速撑板近指本的黑楼安装包,仅支持 lar.ge情式。	

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

升级管理	3								
1000	a Person	TRANK					100.A.3	82	
	资产名称	州第分也	标签	1PH21d	操作系统	王程序版本	病毒疾病本	操作项	
	@ 27.44	Windows選 各發信		115,238,89,34, 192,168,27	Windows Serve	2.0.7.4	25.00.10.61	开展主题体	REFER
	O DESKTOP-250	PCIE	a mwolest	172.16.1.48	Windows 10 Pr	2.0.7.4	25.00.11.06	计位主题中	REMARK
	O DESKTOP-782	PCIE		60,190,226,180, 192,168.1	Windows 10 64	2.0.7.4	25.00.11.06	7142.27(27)	Hamas
	O DESKTOP-MPS	PCIE		180.165.57.225, 169.254.1	Windows 10 64	2.0.7.4	25.00.11.06	101110	HUNGS
	edr-207-cento	Linua銀月器 包	自用范围	172.16.1.37	CentOS release	2.0.7.4	25.00.11.06	HOLDO	Asses

18.3 添加资产

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





19 _{多级中心}

下级中心如何连接上级中心?

步骤1. 使用 admin 账号登陆管理平台;

步骤2. 进入多级中心,点击配置上级;

配置上级		×					
* 上级控制中心地址	[項						
* 下级控制中心端口	请输入 请输入下级中心地址						
	取消连接 连接上级						

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



步骤4. 点击连接上级成功后即可在上级连接状态查看连接状态和上级 IP。

多级中心									详情
本中心名称:	localhost.localdomain	版本号:	2.0,10,1	4	0	114	112	0	0
上姐连接状态:	已连接(192.168.27.203)	@抽题:	192.168.27.32	在螺簧严	寓线资产	病毒文件	高危漠河	异常复杂	web请求防护