黑盾综合日志审计分析系统 HD-LAS V4.0

用户手册

福建省海峡信息技术有限公司

2023年11月

目录

目	录	2
1	概述	4
	1.1 初次使用说明	4
	1.2 系统简介	4
	1.3 系统概述	4
	1.4 管理概述	4
	1.4.1 客户端分类	4
	1.4.2 系统授权	5
2	功能使用	7
	2.1 登陆	7
	2.2 总览	8
	2.2.1 总览	8
	2.2.2 大屏可视	8
	2.3 资产管理	9
	2.3.1 资产管理	9
	2.3.2 资产发现	. 11
	2.4 事件分析	.14
	2.4.1 告警监控	. 14
	2.4.2 日志检索	. 21
	2.4.3 审计事件	. 23
	2.4.4 关联事件	. 25
	2.5 报表管理	.26
	2.5.1 安全报告	. 26
	2.5.2 统计报表	. 28
	2.6 策略管理	. 33
	2.6.1 关联分析规则	. 33
	2.6.2 统计分析规则	. 34
	2.6.3 审计分析规则	. 35
	2.6.4 基线分析规则	. 36
	2.6.5 预处理规则	. 37
	2.6.6 规则字典	. 39
	2.6.7 归并规则	. 40
	2.6.8 <i>过滤规则</i>	. 41
	2.6.9 分类规则	. 42
	2.7 系统管理	.43
	2.7.1 基础配置	. 43
	2.7.2 系统用户	. 48
	2.7.3 系统角色	. 48
	2.7.4 组织结构	. 49
	2.7.5 系统日志	. 49

2.7.6	引擎监控5	50
2.7.7	设备管理5	50

1 概述

1.1 初次使用说明

本文档帮助用户了解黑盾综合日志审计分析系统的主要功能和操作步骤。在 进行操作之前,请确认已经获得操作权限的账号。

1.2 系统简介

黑盾综合日志审计分析系统是基于 B/S (Browser/Server)架构。客户端是 Web 浏览器,用于浏览管理界面。服务器运行着系统的主要功能,并与客户端通 信,显示各项安全事件信息。

1.3 系统概述

黑盾综合日志审计分析系统的服务器分为后端服务器和前端服务器两大部 分。

后端服务器负责对各项网元设备的安全事件进行捕获、归类和分析,并将分 析结果存储到数据库中。

前端服务器的设计目的是将后端服务器分析结果数据展现给用户,并提供丰富的报表供用户使用。系统可以进行各种形式的服务器和客户端操作的配置,以及数据存储模式的配置,Web服务器管理等。配置工作通过修改配置文件进行。

1.4 管理概述

1.4.1 客户端分类

黑盾综合日志审计分析系统 Web 客户端可以查看各项安全事件、安全预警等 各项分析结果;并产生各种分析结果报告。登陆界面如图 1-1。

4



1.4.1.1Web 客户端

Web 客户端完全使用浏览器,不需要安装额外的软件或者 Java 插件。管理员可以在任何地方访问 Web 客户端,并且不受代理和防火墙的限制。

1.4.1.2客户端启动

在启动客户端之前先确定设备已经启动。

启动过程如下:

- (1) 打开浏览器,在地址栏中输入 https://服务器 IP 地址。
- (2) 输入用户名、密码及验证码。
- (3) 点击"登录"按钮,客户端随即启动。

1.4.2 系统授权

黑盾综合日志审计分析系统授权入口共两处,登录页面-系统授权和设备管 理-许可管理;授权类型分为两种,本地授权和网络授权。

系统授权	×
	修正系统时间
当前系统时间:	2022-01-01 14:19:17
修正系统时间:	2022-01-01 14:19:20
	修正时间

	产品授权
提示:若选择文件报	钗,授权文件大小不超过16M!
授权方式:(🔵 文件授权 🛛 🔘 网络授权
授权服务器IPV4地址:	10.5.17.29
本地管理口IPV4地址:	10.9.14.163
本地管理口子网掩码:	255.255.0.0
网关:	10.9.14.254
	保存并授权

总范 设备	黃管理 ×															
系统管理>设	皆管理									● R)#F						
系统信息	网络管理	日期时间管理	运行管理 诊	新工具 许可管理 访问	許可管理 访问控制策略 级联设置 日志备份与恢复											
▼ 关于ざ	■ 关于产品															
				11110-117												
授权类型	2	授权客户		喪权时间	授权有效期	服务有双期	灾港数	凝洗版本	设备型号							
正式		海峡		2021-01-26 08:22:14	2021/12/30	2021/12/30	5	HD-LAS V4.0	HD-LAS V4							
📕 机醋砂	ц.															
			授权类	型: 💿 文件授权 🗌 网络	授权											
			产品激活方	式: 厂商LICENSES	Timucenses											
			本机注册	码: 39829DF578E9586EE5C1EA	CCFA8B7377											
			・上传LICENSES文	件: 选择文件 *单个文件大小	不超过16M											
						授权										

1.4.2.1本地授权

本地授权过程如下:

(1) 授权类型: 文件授权;

(2)选择并上传授权文件,点击授权,并确认授权,待授权成功后,授权信息更新。

1.4.2.2网络授权

网络授权过程如下:

(1) 授权类型: 网络授权;

(2)输入网络配置信息,点击授权,并确认授权,待授权成功后,授权信息更新。

2 功能使用

2.1 登陆

要使用该平台需先登录到平台的服务端,输入管理员的账号和密码,点击登录,登录到平台主界面如下图所示:



2.2 总览

2.2.1 总览

路径:总览->总览。可查看总览信息。

日志审计 / 总克					◎帮助 ◎刷新						
今日日志数 0 日志忠数 32203W		今日关联事件数 23847 关联事件总数 251523		今日南计事件数 0 南计事件参数 1852W							
▲ 日志分类排名	(48 ∨ 14)	资产日志排名	◆日 ∨	📕 设备类型日志数排名	(今日 ∨)						
0											
0 0											
		智无数据		輪无数据							
0 0											
■ 事件排名					今日 ~						
		─────────────────────────────────────									
1,500											
1,200											
600											
300											
0 00:00 01:00 02:00 03	3:00 04:00	05:00 06:00 07:00 08:00 09:00	10:00 11:0	0 12:00 13:00 14:00 15:00							

2.2.2 大屏可视

路径: 总览->大屏可视。可查看大屏信息。

大屏可视	
以击态势	
1000	
[Line] [tim]	
ar search as a second s	
Constant and a second sec	
开启大屏投放	

2.3 资产管理

2.3.1 资产管理

路径:资产管理->资产管理。

资产管理>资产管理									●周朝
快速筛选	业务视角 组织架构	资产名称:		IP:	域名:	URL :	资产类型: 全部	~	查約 里田
资产类型						×			
299 IP IP资产	5 ● 应用资产	◎ ⑦新端 6	2 沈星编辑 📄 沈星制	除 🛛 Excel导入 🗌 🕞 导出Exc	cel 固产发现任务			🕏 应用资产 IP	IP资产 🛞 域名资产
4		序号	资产名称	↓ [IP][抽名][URL]	⇒ 所展业务	分组	第口(服务)	设备类型	操作
♥ 漱石賞/*		1	IP 220.181.124.47	[220.181.124.47]				启明星辰IPS	R 🗹 🗰
设备类型		2	IP 220.181.124.35	[220.181.124.35]				启明星辰IPS	R 🗹 🛍
3 ■ 主机服务器	2 ● 网络设备	3	IP 220.181.124.36	[220.181.124.36]				启明星辰IPS	R 🖉 🗊
299 • 安全设备	1 ■ 应用软件	4	IP 220.181.124.37	[220.181.124.37]				启明星辰IPS	R 🗷 🗰
1 日 办公外设	2 參 物联网设备	5	IP 220.181.124.38	[220.181.124.38]				启明星辰IPS	R 🗹 🗊
28:m:(2):0		6	IP 220.181.124.39	[220.181.124.39]				启明星辰IPS	R 🗹 🗰
1 / / / MB		7	IP 220.181.124.40	[220.181.124.40]				启明星辰IPS	R 🗹 🗊
③ 普通服务器	③ 关键服务器	8	IP 220.181.124.41	[220.181.124.41]				启明星辰IPS	R 🗷 🗊
0 ⑦ 终端	0 (*) 默认分组	9	IP 220.181.124.42	[220.181.124.42]				启明星辰IPS	R 🗷 🗰
资产网段		10	IP 220.181.124.43	[220.181.124.43]				启明星辰IPS	R 🗹 🗰
2 # 10.9.14.0/24	1 # 10.500.111	11	IP 220.181.124.44	[220.181.124.44]				启明星辰IPS	R 🗷 💼
1		12	IP 220.181.124.45	[220.181.124.45]				启明星辰IPS	R 🗷 🗰
₼ 10.50.0.112		13	IP 220.181.124.46	[220.181.124.46]				启明星辰IPS	R 🗷 💼
		14	IP 220.181.124.53	[220.181.124.53]				启明星辰IPS	R 🗷 💼
		15	IP 220.181.124.58	[220.181.124.58]				启明星辰IPS	R 🗷 🗰
					ŧ	ŧ308条 上一页 1 2	3 4 5 16	下一页 20 条/页~	到第 1 页 确定

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】, 查询条件内容清空。

点击【新增】,跳至新增页面。

总览 资产管理 ×							
新增资产							×
📕 基本信息							
	*资产类别:	○应用资产					
	*资产名称:	最多输入60个字符		城名:	最多输入200个字符		
	IP地址:			URL :	最多输入200个字符		
	所属单位:	请选择单位		监控URL:	最多输入200个字符		
	*所属网络:	政务外网互联网接入区		*所属业务:			
	部署位置:	最多输入100个字符		所属区域:	请远禅区城	 	
	0.85/0	· 通用: 20 (20)	~	*:148 米刊 ·			
		201427-1-10-10		(A.F.)	DOT-WAR IN 1		
	"台广"为祖:	第四十分地	~	() () () () () () () () () () () () () (1 第1299页录入		
	等保定级:	清洁择等保定级	~	机密性:	请选择机密性	~	
	完整性:	请选择完整性	~	可用性:	请选择可用性	~	
	系统用途:	最多输入100个字符					
	备注:	最多输入200个字符					
📕 特殊属性							
		+ 端口 服务		协议	标签	应用信息	
				提交 关闭			

点击【提交】,页面跳转至资产管理页面。 左边勾选框勾选多项,点击【批量编辑】,可以批量编辑资产。 左边勾选框勾选多项,点击【批量删除】,可以批量删除资产。 点击【excel导入】,页面跳至 excel导入页面。

Excel导入									×
日 导入模板下载 1 "导入文件:	更新已存在资产	自动创建业务系统	8 🔽 全量更新,删除	余导入清单中不存在资产					
验证告警 共 0 条	■ 导入列表								
	序号 "资产名称	*资产类型	资产分组	所属业务	所属网络	URL	IP地址	域名	*设备类型
					毎入 実利				

点击【导入模板下载】,打开模板。

E	ಕ -ೇ ಕ				资产导入提板 (1).xls	[兼容權式] - Excel(产品激活失敗)					- 0	×
文	件 开始 插入	页面布局 公式 数据 审	网 規图 ♀ 告诉我您想要做什么								聖荣	乌 .共享
1000	★ 照切 完全 照初 ~ 本 後式副 B I	• 11 • Å* Å* <u>U</u> • ⊡ • <u>∆</u> • <u>A</u> • <u>*</u>	■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	^{第現 ・} ♀ • % * [*] 8 *8	● ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	差 好 检查单元格 <i>解释性文本</i>	适中 超链接 警告文本 链接单元相		★ ∑ 自动求和 、 A 」 」 道底、 Z 」 通底、 排序 、 ・	▼ ♀ 间端选 查找和选择		
	9995版 G	字体 6	对开方式	13 数字 13		1430		单元船	946			^
G2	• • • • •	√ fe										v
	В	С	D	E	F	G	Н	I	J	K	L	X A
1			_		资产	导入模板						
2	*资产名称	+资产类型	所属业务系统	资产分组	所属网络区域	IP地址	设备类型 (操作系统)	VCPU数量	内存容量	硬盘容量	域名	UR
3 4 5	安全态势感知应用服 安全态势感知域名服 安全态势感知web服务	5器 IP资产 5 5器 域名资产 应用资产	 		矩阵实验室网络 矩阵实验室网络 矩阵实验室网络	192, 168, 85, 6 192, 168, 85, 7 192, 168, 85, 8	服务器 服务器 web服务器	0		0 硬盘1容量 0 0 0 0	csa.si.ne csa.si.ne	<u>shttp:</u> etl.cr http:
5 7 8 9												
10 11 12												

表格内填写相关信息后保存,选择导入文件,验证告警为0时点击【提交】, 页面跳至资产管理页面。

点击【导出 excel】,可将列表资产导出,导出内容如下所示

🖬 5-								资产制	寻出清单2020	0103 (1).xls 月	東容視式] - Exc	el(产品激活失敗)									
文件 7	开始 插入 页面布局	公式 数据	(审阅	100 R	告诉我您想要做什么																
● ● 第 私站 ・ ● 第 第 前 前 前 前 前 前 一 前 一 一 一 一 一 一 一 一 一 一 一 一 一	切 制 * 記刷 rs 学	- 10 - A - <u>0</u> - <u>A</u> - '		=	自动换行 自动换行 自动换行 自动换行	常現	• 400,000 500,000	● 長件格式 ・ 考	要用 要用 野格格式 -	鸞规 ≙查单元格	差 】 <i>解释性文</i>	好 法 警告文本 样式	适中 性接单3	计 元格 新	算 出	▲ ● ● ● ● 二 ●	権式	∑ 自动 ↓ 填充	課和 - ;・ 」 ;・	▲ 之下 1序和筛选 编辑	重扰和进
A1	* : 🗙 🗸 fr	序号																			
A 1 序号 2 1 3 2 4 3 5 4 6	B 资产名称 10.50.0.200q 10.50.0.221 10.50.0.204 10.50.0.252	10.5 10.5 10.5 10.5	1 50.0.200 50.0.221 50.0.204 50.0.252	C IP/域名		D URL	11 11 12 14 14	E 资产类型 >资产 >资产 >资产 >资产	F 设备类 Linux/Unix3 Windows 7 Windows 7 Linux/Unix3	型 所 系统 系统	G 應单位 調 調 調	H 所属网络 女务外网公用区 女务外网互联网接 女务信息网 女务信息网	1 业务系统 福州市交通综合行 福州市交通综合行 福州市交通综合行	J 风险等级 訂正常 訂正常 訂正常 訂正常	2020-01-03 2020-01-02 2020-01-03 2020-01-03	K 创建时间 09:36:20.0 14:30:32.0 09:31:19.0 09:35:23.0		L	М	N	(
7 8 9 10																					

点击【资产发现任务】,页面跳至资产发现页面。 点击操作中的【查看】,跳至产看资产页面,可查看资产信息。 点击操作中的【编辑】,跳至编辑资产页面,可编辑资产信息。 点击【删除】,可删除资产。

2.3.2 资产发现

路径:资产管理->资产发现。 资产发现模块有'发现资产'和'发现任务'2个标签页。

1、前者是发现结果,可对发现资产进行审核

发现资产					▼ 发现	现任务状态分	布				
1	.41 ⇒ ^{愛現}	75 通过/不通过	⇒	66 转正		2 ^{未开始}	38 单次进行中	2 单次已完成	334 任务结束	17 日中)	2 上 异常
现资产	发现任务										
产类型:全	部 审核状态:		IP地址:		城名:		URL :	任务名称:			> 直询 1
全部选择(1 批量删除 🛛 🚨 批量审核通过	🗹 批量编辑									
序号	[IP][越名][URL]		端口(服务)			资产分组	所周业务	任务名称	发现时间	审核状态 审核	时间 操作
1	[10.9.14.33]		22(ssh),3306(MySQL)				ZCSM-20210119-4065	2021-01-19 18:42:47	来审核	윤 💼
2	[10.50.0.250]		443(HTTPS),8	000(jdwp),9000(http),9010	l(http)			ZCSM-20210119-3777	2021-01-19 18:31:41	未审核	۵ 🕯
3	[10.50.0.240]		22(ssh)					ZCSM-20210119-3777	2021-01-19 18:31:41	未审核	۵ 🛎
4	[10.9.14.3][http://10.9.14.3:9003]		22(ssh),80(HT	TP),443(HTTPS),3306(MyS	QL),5100(http),	65446546		ZCSM-20210119-8621	2021-01-04 15:34:26	未审核	۵ 🕯
5	[10.9.14.3][http://10.9.14.3:9002]		22(ssh),80(HT	TP),443(HTTPS),3306(MyS	QL),5100(http),	65446546		ZCSM-20210119-8621	2021-01-04 15:34:26	未审核	۵ 🕯
6	[10.9.14.3][http://10.9.14.3:8080]		22(ssh),80(HT	TP),443(HTTPS),3306(MyS	QL),5100(http),	65446546		ZCSM-20210119-8621	2021-01-04 15:34:26	未审核	2 💼
7	[10.9.14.3][http://10.9.14.3:9001]		22(ssh),80(HT	TP),443(HTTPS),3306(MyS	QL),5100(http),	65446546		ZCSM-20210119-8621	2021-01-04 15:34:25	未审核	۵ 🛎
8	[10.9.14.3][http://10.9.14.3:9400]		22(ssh),80(HT	TP),443(HTTPS),3306(MyS	QL),5100(http),	65446546		ZCSM-20210119-8621	2021-01-04 15:34:25	未审核	윤 💼
9	[10.9.14.22][http://10.9.14.22:9010]		22(ssh),443(H	ITTPS),8000(jdwp),8009(ajp	o13),8080(http	65446546		ZCSM-20210104-3858	2021-01-04 15:34:25	未审核	۵ 🕯
10	[10.50.0.33]		80(HTTP),443	(ssl),3306(MySQL),8680(tc	pwrapped)			ZCSM-20210119-3777	2021-01-19 18:31:43	未审核	۵ 🕯
11	[10.50.0.252]		23(telnet),80(HTTP)				ZCSM-20210119-3777	2021-01-19 18:31:42	未审核	۵ 🕯
							共1	41条 上—页 1 2	3 4 5	8 下一页 2	9. (表/页~到第11页 🦛

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】, 查询条件内容清空。

点击【全部选择】,可以选中列表中的所有数据,再次点击,选中效果取消。 左边勾选框勾选单个或多个资产,点击【批量删除】,可以删除选中内容。 左边勾选框勾选单个或多个资产,点击【批量审核通过】,可以批量审核通 过未审核资产。

左边勾选框勾选单个或多个资产,点击【批量编辑】,可以编辑选中内容。 点击【查看】,进入已审核资产查看页面。

总览 资产发现 ×									
查看信息									×
📕 基本信息									
	资产类别:	1b.)%page							
	资产名称:	10.50.0.252					域名:		
	URL :						监控URL:		
	IP地址:	10.50.0.252					所属单位:		
	所属网络:	政务信息网					所屬业务:	福州市交通综合行政执法支队办公目助化系统开发项目	
	部署位置:						所屬区域:		
	告誓祖:						设备类型:	Linux/Unix系统	
	资产分组:	关键报务器					负责人:		
	董保完级:						机密件:		
	空酸性・						可用性。		
	70211 ·						Pointie -		
	.5690-Hilliz -								
	晉汪:								
■ 特殊属性									
		第日	服务	协议	标签	banner			
		80	HTTP	tcp					
							关闭		

点击【审核】,进入未审核资产审核页面。

《信息									
	*资产类别:	四周月							
	"资产名称:	10.50.0.252			域名:	最多输入200个学符			
	IP地址:	10.50.0.252			URL :	最多植入200个字符			
	所属单位:				监控URL:	量多输入200个字符			
	所属网络:	政务外网公用区			所属业务:				
	部署位置:	最多输入100个字符			所属区域:	请选择区域		~	
	告誓组:		0		设备类型:	Linux/Unix系统 ×			
	资产分组:	请选择分组	v		负责人				
	等保定级:	请远择等保定级	~		机密性:	请选择机密性		U I	
	完整性:	请远挥完整性			可用性:	请选择可用性		~	
	系统用途:	最多输入100个字符							
	备注:	最多输入200个字符							
属性									
		新語 MC	服务	协议		标签	应用信息		
		100 23	teinet	tcp		诸镇入协议名称	诸幅入应用调息		

点击【删除】,可删除资产。

2、后者是资产发现任务,可进行资产发现任务操作。

(3650)							× 2361139-00	di. C.20				
	141 发现	₽	75 通过/不通过	⇒	66 转正		2 未开始	38 单次进行中	2 单次已完成	334 任务结束	17 已中止	2 异常
資产	发现任务											
名称:		任务对象:		任务类型:	全部	~ 任务状态	5:	创建时间:				直闭
	批量停止 🕕 批量計	189:	***	344 alfa			114105	Trease C	Bacherowerka	波力W/+ 中4 603-34	Assault 1	100.20-
20	119646	4	央型	HR.		100%	119408	2020.12.16.11.22.21	2020.12.16.11.22.26	页件数/未申核 包建香 0/0	2020.12.16.11.22.21	1917
20	70011 20201210 02	-		_		1005	15.00 (4.00	2020 12 10 122551	2020 12 16 11 21 20	0/0		
30	2CSM-20201210-82		墨沃			100%	12990EW	2020-12-16 11/21/19	2020-12-16 11:21:30	0/0	2020-12-16 11/21/19	
31	ZCSM-20201216-75	3	単次			100%	任勞嬉來	2020-12-16 11:20:45	2020-12-16 11:20:50	0/0	2020-12-16 11:20:45	18 Ш
32	ZCSM-20201216-34	4	单次	-		100%	任勞结束	2020-12-16 11:18:28	2020-12-16 11:18:40	0/0	2020-12-16 11:18:28	6
33	ZCSM-20201216-70	13	单次	C		100%	任务结束	2020-12-16 11:04:21	2020-12-16 11:04:41	1/0	2020-12-16 11:04:21	1
34	ZCSM-20201215-84	14	单次	C		100%	任务结束	2020-12-15 11:57:58	2020-12-15 18:27:13	1/0	2020-12-15 11:57:58	S 🖬
35	ZCSM-20201215-77	8	单次	C		100%	任务结束	2020-12-15 11:53:33	2020-12-15 11:53:39	0/0	2020-12-15 11:53:33	13 th
36	ZCSM-20201215-11-	0	单次	C		100%	任务结束	2020-12-15 11:45:32	2020-12-15 11:52:19	0/0	2020-12-15 11:45:32	1
37	ZCSM-20201215-85	.7	单次	G		100%	任务结束	2020-12-15 10:56:26	2020-12-15 10:56:29	0/0	2020-12-15 10:56:26	1
38	ZCSM-20201215-90	5	单次	C		100%	任务结束	2020-12-15 10:55:52	2020-12-15 10:55:59	0/0	2020-12-15 10:55:52	6 🗊
39	ZCSM-20201215-13	2	单次	C		100%	任务结束	2020-12-15 10:54:38	2020-12-15 18:26:57	1/1	2020-12-15 10:54:38	1
40	7C5M-20201215-00	4	461/2			100%	1536449	2020-12-15 10-21-50	2020-12-15 10:41:25	0/0	2020-12-15 10-21-50	F9 #

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】, 查询条件内容清空。

点击【新增】,进入新增页面

	■ 发现资产	■ 发现任务状态分布	
	0 ⇒ (发现 通过/	0 参 0 0 0 0 不通过 非开始 和汉田行中 州汉田田成 新王 未开始 和汉田行中 州汉田成成	0 0 0 任亲结束 已中止 异常
	发现资产 发现任务	◎/HE27 ■ 基本信息	^
WRR 0 ALLEMAN WRRR 1 0 ALLEMAN WRRR 1 0 ALLEMAN WRR 1 0 ALLEMAN BATH 0 MRR 1 0 ALLEMAN MRR 1 0 ALLEMAN MRR 1 0 ALLEMAN MRR 1 0 ALLEMAN BATH	任务名称: 任务对象:	*任务名称: ZCSM-20210127-2480 任务类型: 0 实时 周期	查询 里蓝
	④ 新増 │ ● 批量停止 │ 圓 批量删除	发现策略: 💿 快速機式 🦳 标准模式 📄 进阶模式 🦳 深度模式	
	序号 任务名称 类型	□ □ 扫描对象	台建者 包建时间 操作
		Fig XBRE XBR/A Fig V Fig Fig V Fig Fig XE	

填写相关内容,点击【提交】,进行资产发现任务。 左边勾选框勾选多项,点击【批量停止】,可以批量停止资产发现任务。 左边勾选框勾选多项,点击【批量删除】,可以批量删除资产发现任务。 点击操作中的【查看】,进入查看页面。

总流 资产发现 -	
任务结果	×
任务结果 任务信息与历史记录	
IP:	2 9 #2
任务状态: 金飯(0) 网络选严(0) 应用发产(0)	
	共0条 上一页 下一页 20条/页 到篇 1 页 論定

点击操作中的【编辑】,进入任务编辑页面。 点击操作中的【中止】,可以中止资产发现任务。 点击操作中的【跳过本轮】,资产发现任务会跳过本轮。 点击操作中的【再次执行】,任务再次执行。 点击【删除】,删除资产发现任务。

2.4 事件分析

2.4.1 告警监控

路径:事件分析->告警监控。

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。

1、待确认告警页面

事件分析>告審监控					●R18
时间: 近1天 ~					
	📕 告警类型分布 🔘		■ 告警触发规则	排名TOP5 ●	
非応言 35992 全 日応重 2 金 関告及以上 35993 会 中市 0	35,993 关联分析音 国政	■ 勤武商毒(35993) ■ 其他(0)	[MEBJ2019-00	3]勒波病毒:35993	
(法确认告款 (35991) 法处理告款 (1) 已派弟告款 (1) 日东路告款	(1) 日关闭告款(0)	人政能			
日知られ: () () () () () () () () () (等级:全部	∨ 触觉规则:	源IP:		查询 里靈
⊖ 批量論认 │ ◎ 批量回略 │ ⊖ 导出Excel │ ⊘ 全部确认 │ ◎ 全部回略					
序号 告誓名称 来源	告誓美别 触发	规则	告誓数量 🗧 时	司范围≑	發版≑
1 检测到数素病毒遗信 关联分析音管	和素術書 (R0)	2019-003]勒紫病毒	35991 200 201	21-05-18 14:24:32 21-05-19 14:24:30	7°E
序号 告誓名称/内容	告警题	生成时间	濟IP	目的IP	操作
1 1 1 Locky 副素統導通信 1 Locky 副素統件	10.50.2.164	2021-05-19 14:24:30	10.50.2.164 【攻击者】	137.74.46.46【被攻击者】	国 ② ③ 話
2 ¹ 起気到勤策病毒通信 Locky勤策软件	10.50.2.164	2021-05-19 14:24:28	10.50.2.164 【攻击者】	91.234.32.19【被攻击書】	<u>民</u> ② ② 番 出

点击一条告警事件, 左边勾选框勾选多项, 点击【批量确认】, 可以批量确认告警。

点击一条告警事件, 左边勾选框勾选多项, 点击【批量忽略】, 可以批量忽略告警。

点击【导出 excel】,导出页面如下

▲ 約 ● ※約 ● ※約 ● ※約 ● ※約	Arial Arial BIU+	- 10 - A /	· = =	- 82 + 1	計算算法 ■ 自动接行 □ 合并創業中・	***** ********************************	条件格式 - 新格式	業現 差 检查单元格 解释性文本	好 警告文本	适中 计算 链接单元格 輸出			∑自动求和 ↓ 填充・	AZT MIRHORIZE	WEEKOUESE		
剪贴板	9	*体	n	对齐方	e a	2014 G			龙桥			种元的		98			
1	• E × 🗸	fe 序号															
A	в	С	D	E	F	G	н	1	J	К	L	M	N C	P	Q	R	
序号	告警名称	美型	告醫樂別	告警等级	告警課	譚IP	目的IP	告誓内容	处置状	志发生时间							
	USIP) - Ckeditors and the	天联分析省智	Weblyth	中厄	220.160.52.163	10.50.2.185	220.160.52.16.	友現10.502.185署武坊内日	\$\$220.16Cnull	2020-01-07 11:06:45							
	い」「PJFCKeditors用約解解型	大地方引着智	WebXtt	44/3	220.100.02.103	10.50.2.105	220.100.52.10.	2010/10/2012/10/2010/19日	5x220.10Cmull	2020-01-07 11:06:42							
	35/DEckeditorises and	学校ので言葉	Webthill	中/法	220 160 52 163	10.50.2.105	220 160 52 16	200010-50-2-105番號(2)時日	\$7220.16C null	2020-01-07 10:54 10							
	1月1日Fckeditori無疑認知	关联分析曲察	Wahtfrills	中心	220 160 52 163	10.50 2 185	220 160 52 163	2010-10-50-2 105-2010110日	\$7220.16Cmull	2020-01-07 10:53:55							
	访问Fckeditor编辑器编	关联分析集整	WebItra	山角	220 160 52 163	10.50 2 185	220 160 52 163	労役10.50.2.185書試方回日	\$7220 16C mull	2020-01-07 10:52:45							
	访问Fckeditor编辑器	关联分析告察	WebIt	中国	220 160 52 163	10.50.2.185	220 160 52 163	发现10.50.2.185要试方面目	\$7,220,16C null	2020-01-07 10:52 31							
	访问Fckeditor编辑器组	关联分析告察	WebI安击	中段	220, 160, 52, 163	10.50.2.185	220,160,52,163	发现10.50.2.185要试访问目	\$%220.16C null	2020-01-07 10:52:20							
	访问Fckeditor编辑器组	关联分析告题	Web珍击	中茂	61.154.11.191	10 50 2 185	61.154.11.191	发现10.502.185尝试访问目	8561.154. null	2020-01-07 10:49:24							
	访问Fckeditor编辑器组	关联分析告题	WebI文击	中危	61.154.11.191	10.50.2.185	61.154.11.191	发现10.502.185尝试访问目	初61.154, null	2020-01-07 10:49 13							
	HTTP SYS远程执行代	关联分析告警	Web攻击	中危	218.5.241.22	10.50 2.194	218.5.241.22	检测到针对HTTP SYS远程	丸行代码 遷 null	2020-01-06 13:25:46							
	HTTP.SYS远程执行代	关联分析告誓	Web玟也	中危	218.5.241.22	10.50.2.194	218.5.241.22	检测到针对HTTP.SYS远程	丸行代码漏 null	2020-01-06 13:21:15							
	HTTP.SYS远程执行代	关联分析告誓	Web攻击	中危	218.5.241.22	10.50.2.194	218.5.241.22	检测到针对HTTP.SYS远程	丸行代码 mull	2020-01-06 12:48:47							
	HTTP.SYS远程执行代	关联分析告答	Web攻击	中危	218.5.241.22	10.50.2.194	218.5.241.22	检测到针对HTTP.SYS远程	丸行代码源 null	2020-01-06 12:48:43							
	HTTP.SYS远程执行代	6 关联分析告答	Web攻击	中危	218.5.241.22	10.50.2.194	218.5.241.22	检测到针对HTTP_SYS远程	丸行代码還 null	2020-01-06 12:48:36							
	HTTP.SYS近程执行代	关联分析告警	Web攻击	中危	218.5.241.22	10.50.2.194	218.5.241.22	检测到针对HTTP.SYS远程	丸行代码 濃 null	2020-01-06 12:47:57							
	访问Tomcat控制给	关联分析告警	Web攻击	中危	218.5.241.22	10.50.2.194	218.5.241.22	10.50.2.194访问218.5.241	228)Tomc: null	2020-01-06 12:47:49							
	访问Fckeditor编辑器组	关联分析告誓	Web攻击	中危	220.160.52.165	10.50.2.90	220, 160, 52, 165	发现10.50 2.90尝试访问目标	5220 160 null	2020-01-06 09:55:43							
	访问Fckeditor编辑器组	关联分析告警	Web攻击	中意	220.160.52.165	10.50.2.90	220.160.52.168	发现10.50.2.90尝试访问日和	#220.160 null	2020-01-06 09:54:41							
	访问Tomcat控制台	关联分析告誓	Webitte	中應	220.160.52.165	10.50.2.90	220.160.52.168	10.50.2.90050220.160.52	16589Tominull	2020-01-06 09:45:21							
	访问Tomcat控制台	关联分析告答	Webi交击	中范	220.160.52.224	10.50.2.90	220.160.52.224	10.50.2.9005(0)220.160.52	224B9Tom(null	2020-01-06 09:24:22							
	访问Tomcat控制台	关联分析告答	Webi交击	中地	61.154.11.191	10.50.2.90	61.154.11.191	10.50.2.9005(0)61.154.11.1	1831 omc. null	2020-01-06 09:17:54							
	切问Tomcat控制台	关联分析告誓	Weblyth	中間	220.160.52.165	10.50.2.90	220.160.52.165	10.50.2.9005(0)220.160.52	165E9Tom(null	2020-01-06 09:11:38							
	ThinkPHP v5运程fCthi	天联分析省智	Weblyth	中度	112.111.2.122	10.50.2.71	112.111.2.122	R220304TXj112.111.2.1228	ThinkPHF null	2020-01-03 16:09:04							
	ThinkPHP v5四程1098	天联分析音響	WebAct	中度	112 111 2 122	10.50.2.71	112.111.2.122	R22R300TX9112.111.2.1228	ThinkPHF null	2020-01-03 16 08 44							
	ThinkPHP VSILKETUNE	大地方切古智	websydd	中/四	112.111.2.122	10.50.2.71	112.111.2.122	N27835557X3112.111.2.1228	I ninkPTIF null	2020-01-03 16:08:34							
	ThinkPHP VSILLETUNE	大联分析音響	vveo xtti	14/3	220.160.52.224	10.50.2.71	220.160.52.224	1020033057X3220.160.52.2240	C) I NINKPH NUII	2020-01-03 16:08:15							
	TUNKE AN ACCESS	大限方所首會	vve0xxtt	478	212.04.117.102	10.50.2.71	212.04.117.104	*22/33/99TX9212.04.117.1021	SThinkPri null	2020-01-03 15:31:49							

点击一条告警事件,点击操作中的【查看】

用户指南

总范	告警监控>										
查看											>
× a	藝術信息										
(*	<mark>中危)</mark> XXE实	体注入攻击									
	告誓内容:	发现10.9.2.46对	120.35.5.146实施	EXXE实体注入攻击	行为			原理	现在越来越多主要的web制	星序被发现和报告存在XXE(XML External Entity	y attack)漏洞,比如说facebook、
	告誓类别:	注入攻击							paypal等等。举个例子, 经存在了很多年,但是它是	我们扫一眼这些网站最近奖励的漏洞,充分证 A.来没有获得它应得的关注度,很多XMI 的鳗	实了前面的说法。尽管XXE漏洞已 析器默认是会有XXE漏洞的,这章
	告撃源 :	120.35.5.146							味着开发人员有责任确保。	这些程序不受此漏洞的影响。	
	源IP:	10.9.2.46						dan salar	化原源电影教师 因为化源	·····································	白根赤間にも根のたけの
	目的IP:	120.35.5.146							DOM:09-1-46/09-2, E4/32-046	10/12/22/2010/2011 40/2003013/236 / 10/0111	J80779871272800734X44.
형	收击者城名:							安全建议	配置XML处理器去使用本地	他静态的DTD , 不允许XML中含有任何自己声明	明的DTD.
8	政击者端口:										
	生成时间:	2020-12-25 14:	02:39								
	告暫追溯:										
			0	0	0	0	@				
扫	描探则	遭受攻击	已被入侵	C&C通信	内网渗透	盗职数据	黒产牟利 (抱矿、勤素、晴穂)				更多详情》
							^				
×	(朕事件列表	ŧ									
	时间: 清志	肇事件发生时间	~								✓ 査询 定員
<mark>志</mark> 封	imite 🔍 hi	1入黑名单									
	皮号 孝	件名称	中	件类型 等级	时间		资产名称/IP地址	设备	类型 遼IP	目的IP	协议 操作
										共1条 🔄 🚺 下一页	10条/页> 到第 1 页 确定

点击一条告警事件,点击操作中的【确认】,可以确认告警。 点击一条告警事件,点击操作中的【忽略】,可以忽略告警。 点击一条告警事件,点击操作中的【一键断网】,可以对 IP 进行封堵。 点击一条告警事件,点击操作中的【恢复断网】,可以对 IP 进行解封。 2、待处理告警页面

事件分析>告警监控				◎周新
时间:近天				
■ 告警统计	▼ 告警类型分布 ◎		其 告警触发规则排名TOP5 ◎	
未た第 35983 ● 日代第 2 ● 常数同じ上 35984 ● 中集 0	35,984 _{关联分析} 四等取	■ 記意病毒(3594) ■ 其他(0)	[规则2019-003] 取法病毒 :35984	
待确认告誓(35982) 待处理告誓(1) 已派单告誓(1) 已忽略告誓	(1) 已关闭告誓(0)	へ收起		
告誓名称: 告誓発別: 全部 ッ 戦发規則:	舌管源:	等级:全部 >		童狗 里豆
- 寻出Excel │ 🙏 批量派单 │ 📍 加入黑盔单				
像号 告警名称/内容 来源	告誓源 告誓类别	触发规则 生成时间	遼IP 目的IP	等级 操作
1 は刈到金家病毒通信 メビジン よび よび	f蓉 10.50.2.164 動素病毒	[规则2019-003]勒素病毒 2021-05-19 11:23:12	10.50.2.164 [攻击者] 195.123.209.123 [者]	^{被攻击} 🕂 🗮 🔃 🖥 🗮 🖚 🔛

点击【导出 excel】,导出页面如下

							20200107號主導件自當地	Full)日中(1)-XIS (第44個工人) - EXG	000 102002000							
文件	开始 插入 页面布	局 公式 数据	审阅 視	ାଆ ଢ଼ି≊	告诉我您想要做什么…											
「「「」」の「」」の「「」」の「」」の「「」」の「「」」の「」」の「」」の「」	第切 長制 - 作式刷 B <i>I</i> <u>U</u> -	• 10 • A ∧	. ≡ ≡ =	- ≫ 	◎ 自动换行 □ 合并后層中 ·	^{常規} ・ ♀・%・ % ぷ	● 正 条件格式 奏用 ・ 表格格式・	差 主单元格 <i>解释性文本</i>	好 警告文本	适中 计算 链接单元格 输出	*	插入	影響権式	∑ 自动求! ▼ 填充 × < 満除 ×	口 × A Z 排序	▼ 和筛选 查
鲍马祜	R G	字体	G	对齐方,	đ, ra	数字 54			样式			1	单元格		编辑	ŧ.
A1	• : × 🗸	fe 序号														
_4 A	В	C	D	E	F	G	н	- I	J	К		L	M	N	0	P
1 序	号 告警名称	类型	告警类別	告警等级	告警源	源IP	目的IP	告警内容	处置状态	: 发生时间						
2 1	检测到敏感信息泄漏	关联分析告警	信息泄露	高危	47.103.217.163	47.103.217.163	10.50.5.230	检测到47.103.217.163存在	E敏感信息池 null	2020-01-03 10:08:46						
3 2	跨站脚本攻击	关联分析告警	跨站脚本	中危	10.5.12.55	114.242.143.169	10.5.12.55	发现访客114.242.143.169	对目标10.5 null	2020-01-02 20:10:11						
4 3	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	121.51.23.159	发现访客10.50.2.71多次尝	t试访问目标 null	2020-01-02 17:29:47						
5 4	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	121.51.23.159	发现访客10.50.2.71多次尝	\$试访问目标 null	2020-01-02 17:29:36						
6 5	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	183.232.95.149	发现访客10.50.2.71多次尝	\$试访问目标 null	2020-01-02 17:29:34						
7 6	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	119.29.29.29	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:28:12						
8 7	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	119.29.29.29	发现访客10.50.2.71多次尝	1试访问目标 null	2020-01-02 17:27:59						
9 8	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	120.241.186.171	发现访睿10.50.2.71多次尝	s试访问目标 null	2020-01-02 17:27:56						
10 9	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	111.47.223.195	发现访客10.50.2.71多次尝	s试访问目标 null	2020-01-02 17:24:24						
11 10	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	112.47.4.157	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:19:46						
12 11	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	121.51.131.56	发现访客10.50.2.71多次尝	\$试访问目标 null	2020-01-02 17:18:50						
13 12	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	112.60.0.199	发现访客10.50.2.71多次尝	\$试访问目标 null	2020-01-02 17:18:47						
14																
15																
16																
17																
18																
19																
20																
21																
22																
23																
23																

左边勾选框勾选多项,点击【批量派单】,可以批量派单告警。

左边勾选框勾选多项,点击【加入黑名单】,可以批量对告警中的源 IP 或目的 IP 加入黑名单。

■ 告警统计	■ 告警类型分布 ●	X #	吉警触发规则排名TOP5 @
★ *** ★ ★			×
▲ 南龙及以上 ▲ 中	加入35歳1P: 🗿 源1P:		10 (33333
▼ 35993 ▼ 0	10.50.2.164(黑谷单)	195.123.209.123	
- - 時以告誓(35991) - 侍处理告答(1) - 已派单日			
警名称: 舌醫樂別: 全部	黑名单有效期:	(#j	
导出Excel A 批型派单 A 加入黑名单	标签:	快速迅振	~
序号 告留名称/内容	备注: 检测到勒索病毒通信		目的IP 等级 操作
1 Locky勤業软件			195.123.209.123 [城校曲 严重 民 🌢 🔍 🐽 🖽
		投 交	

点击操作中的【查看】

总范告報	警监控 ×														
查看															×
															÷.
▲ 叁/4×12	52														-1
(中危))XXE实(本注入攻击													
告	1000日 100000000	发现10.9.2.46对	120.35.5.146实施	XXE实体注入攻击	行为			原理	现在越来越多主要的web	程序被发现和报告存	在XXE(XML External	Entity attack)漏洞	, 比如说fa	cebook,	
告	1110美別:	注入攻击							paypal等等。举个例子	,我们扫一眼这些网站	s最近奖励的漏洞,3	的证实了前面的)	いた。 尽管の	(XE)屬同已	
	告誓源 :	120.35.5.146							经停住了很多年,但是E 味着开发人员有责任确例	5.从米没有铁得已应得 R这些程序不受此漏洞	的失注度。很多XMI 的影响。	山的科グロネルス定さ	(何XXE)應用	的,这意	
	源IP:	10.9.2.46											-		
	目的IP:	120.35.5.146						芯吉	此屬河非常危险,因为此	扁洞会适成服务器上制	奴感教馆的泄露,和	着在的服务器拒绝	服务攻击。		
被攻击	诸城名:							安全建议	配置XML处理器去使用本	≤地静态的DTD,不允	许XML中含有任何自	1己声明的DTD。			
被攻击	清端口:														
生	咸时间:	2020-12-25 14:0	02:39												
告	:答追溯:														
6-			0	8	6	0	&								
扫描探测	RI	遭受攻击	已被入侵	C&C通信	内阿渗透	盗取政援	黒产牟利 (投矿、勒索、磷链)							更多详情》	
📕 关联赛	事件列表														1
时间	: 请选择	事件发生时间	~										× ±≊≊	王王	ч
➡ 封埔IP	🔍 🙇 ta	(黒名単													
. 5	\$ 号 事(\$名称	中	半类型 等级	时间		资产名称/IP地址	设备	类型 源IP		目的IP		协议	操作	
										共1条	1-7	下一页 10 条/页~	別第 1	页确定	

点击操作中的【派单】,可对告警进行派单处理

总览 告誓监控 ×				
派单				×
"标题: 现象描述:	意查业务使口API模拟异常调用 发现10.50.0.2407;220.160.52.51存在业务接口api商纸异常等	樂型:	攻击音響	
原因分析:				
处理意见:				
相关资产: "最长接受时间;	·····································	*最长处理时间:	18/L	
* 人 甲F-10*	语证据律论方			
通知方式:	■ 邮件 🗹 短信	*影响程度:	· 请选择 · · · · · · · · · · · · · · · · · · ·	
时件:	上传期件 "单个附件大小不超过16M			
		152 900		

点击操作中的【加入黑名单】,可以对告警中的源 IP 或目的 IP 加入黑名单。 点击操作中的【一键断网】,可以对 IP 进行封堵。 点击操作中的【恢复断网】,可以对 IP 进行解封。

3、已派单告警页面

事件分析>告要监控		Ø用来
时间:近天		
╡ 告警统计	✓ 告警类型分布 ◎	其 告警触发规则排名TOP5 ◎
本位置 本位置 35992 全 電磁区以上 全 第6座区以上 今	35,993 关新分析告留数 単型原毒(3993) 単発(10)	[HEIR12019-003]#0:#triffe## ; 35993
待确认告答(35991) 待处理告答(1) 已感触告答(1) 已感略告答	へ収起 (1) 已纯闭音磬(0)	
告容挑別:全部 、 等級:全部 、 工单状态:全部 、	8 · · · · · · · · · · · · · · · · · · ·	告罄名称: 查询 主日
⊖ 尋出Excel . 九八黑名单		
床号 告留这称/内容 来源 告留源 1	生成时间 雜极 逐	IP 目的IP 派单时间 工单状态 操作
1 检测到激素病毒通信 关联分析告留 10.50.2.164 計 Locky型素软件	的業務署 (規則:2019-003)勤業務署 2021-05-19 11:23:28 严重 10	1502.164 [改由者] 91.234.32.19 [補改曲 2021-05-19 11:23-51 侍援壬 🕄 🐥 🚓 🕮

点击【导出 excel】,导出页面如下

. . .							20200107安全事件告答	3出清单 (1).xls [兼容模式] - Exc	iel(产品激活失败)						
文件	开始 插入 页面布	调 公式 数据	审阅 衫	189 Q	告诉我您想要做什么										
間	(前切) 気利 → が格式刷 B I U →	- 10 - A			自动换行 合并后居中 ·	^{常規} ・ ♀・% ・ % *%	● 素格格式 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	是 查单元格 <i>解释性文本</i>	好 警告文本	适中 计算 链接单元格 输出	× +	₩ Ⅲ 插入	診験権	∑ 自动求耗 ↓ 填充、	」 ▲ 2 ▼ 排序和筛选
鲍贴	lig in a	字体	G	对齐方	जी ह	数字 5			样式				单元格		编辑
A1	* : × ~	た 序号													
	в	с	D	E	F	G	н	1	J	к		L	м	N	0 P
1 序	号 告警名称	米型	告警关別	告警等级	2 告警源	源P	BINP	告警内容	か 置状态	发生时间					
2 1	检测到敏感信息泄漏	关联分析告警	信息泄露	高危	47.103.217.163	47.103.217.163	10.50.5.230	检测到47.103.217.163存在	敏感信息池 null	2020-01-03 10:08:46					
3 2	跨站脚本攻击	关联分析告警	跨站脚本	中危	10.5.12.55	114.242.143.169	10.5.12.55	发现访客114.242.143.169	对目标10.5 null	2020-01-02 20:10:11					
4 3	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	121.51.23.159	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:29:47					
5 4	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	121.51.23.159	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:29:36					
6 5	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	183.232.95.149	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:29:34					
7 6	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	119.29.29.29	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:28:12					
8 7	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	119.29.29.29	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:27:59					
9 8	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	120.241.186.171	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:27:56					
10 9	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	111.47.223.195	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:24:24					
11 10	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	112.47.4.157	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:19:46					
12 11	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	121.51.131.56	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:18:50					
13 12	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	112.60.0.199	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:18:47					
14															
15															
16															
17															
18															
19															
20															
21															
22															
23															

左边勾选框勾选多项,点击【加入黑名单】,可以批量对告警中的源 IP 或目的

IP 加入黑名单。 点击操作中的【查看】

总范	告警监控	~										
查看												×
	基本信息											Т
												1
	中危)XXE实	体注入攻击										1
	告誓内容	: 发现10.9.2.46对	120.35.5.146实施	EXXE实体注入攻击	行为			原理	现在越来越多主要的web程	序被发现和报告存在XXE(XML External Enti	ty attack)漏洞,比如说facebook、	1
	告醫类别	: 注入攻击							paypal等等。 辛个例子, 非 经存在了很多年,但是它从	\$11扫一眼逗些网站最近奖励的漏洞,充分。 .来没有获得它应得的关注度。很多XML的影	止实了前面的说法。尽管XXE漏洞已 异析器默认是含有XXE漏洞的,这意	1
	告警察	: 120.35.5.146							味着开发人员有责任确保这	些程序不受此漏洞的影响。		1
	源IP	: 10.9.2.46						危害	此屬洞非常危险,因为此屬)	同会造成服务器上敏感数据的泄露 , 和潜在	的服务器拒绝服务攻击。	1
	EB3IP	: 120.35.5.146										-I
	度攻击者或名 成功主奏地口							安全建议	配置XML处理器去使用本地	瓣态的DTD,不允许XML中含有任何自己声	W明白DTD.	-I
	生成时间	· · 2020-12-25 14	02:39									I.
	告藝追溯	:										1
	_											1
	8	-5	•••	••••	0	0	*					1
3	3攝探測	遭受攻击	已被入侵	C&C通信	内阿渗透	盗取数据	黒产牟利 (投矿、勤業、晴链)				更多详情》	1
							^					1
												÷
× ;	关联事件列表	Ę										-1
	时间: 清志	绎事件发生时间	~								✓ 査询 東景	1
<u>a</u> ;	BİTİRLIP 📃 🙇 🖄	山入黒名単										ł
	序号 寻	叫什名称	#	件类型 等级	2 时间		资产名称/IP地址	设备	类型 渡IP	目的IP	协议 操作	
										共1条 上一页 1 下一	□ 10条/页> 到第 1 页 确定	

点击操作中的【加入黑名单】,可以对告警中的源 IP 或目的 IP 加入黑名单。 点击操作中的【一键断网】,可以对 IP 进行封堵。 点击操作中的【恢复断网】,可以对 IP 进行解封。

4、已忽略告警

事件分析>告警监控					④ 刷新
时间: 近1天 ~					
舅 告警统计	■ 告警类型分布		■ 告警触发规则排名TOP5 ●		
株式 株式 日本 35992 ● 2 ● 高度型以上 ● 中度 0 0	35,993 关联分析曲管数	■ 記意傳毒(35993) ■ 其他(0)	[10]即12019-003]取)求(明确):35993		
待确认告誓(35991) 待处理告誓(1) 已派单告誓(1) 已感睹告誓(1) 已关闭告誓(0)	へ改起			
告誓关別: 全部	告替源:	告誓名称:		查询	**
G 尋出Excel					
序号 告慰名称/内容 来遭	告誓源 告誓美别	触发规则 生成时间	等级 遼IP	目的IP 撞	fi -
1 1	10.50.2.164 勤業病毒	(規則2019-003)勘索病毒 2021-05-	-19 11:23:48 严重 10.50.2.164 【攻击者】	195.123.209.123【被攻击 客】	ත්ර 🛗

点击【导出 excel】,导出页面如下

							202001073624014118-0	actualities (1) you a fast and find a cou	1000 maabon 2000							
文件	开始 插入 页面布	调 公式 数据	医 审阅 初	2011 Q 1	告诉我您想要做什么											
■ 3 1 10 1 10 1 10 1 10 1 10 1 10 1 10 1	9初 同初 - Arial 日 J U - 日 名式刷	- 10 - A - A - A - A		- 8⁄2 +-	自动换行	常規 ♀ % * % * % * **	★件格式 表格格式 ●	9. <mark>差</mark> 查单元格 <i>解释性文本</i>	好 警告文本	适中 计算 链接单元格 输出	× * *	通行		∑ 自动求和 ↓ 填充、	・ A Z 排序和) 第选查
鲍贴板	G	字体	5	对齐方	ವೆ ಇ	数字 5			样式			4	元格		编辑	
A1	• : × 🗸	fx 序号														
A	В	С	D	E	F	G	н	1	J	К		L	M	N	0	P
1 序号	告警名称	类型	告警关别	告警等级	告警源	源IP	目的IP	告警内容	处置状态	发生时间						
2 1	检测到敏感信息泄漏	关联分析告警	信息泄露	高危	47.103.217.163	47.103.217.163	10.50.5.230	检测到47.103.217.163存在	較懸信息泄null	2020-01-03 10:08:46						
3 2	跨站脚本攻击	关联分析告警	跨站脚本	中危	10.5.12.55	114.242.143.169	10.5.12.55	发现访客114.242.143.169	对目标10.5 null	2020-01-02 20:10:11						
4 3	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	121.51.23.159	发现访客10.50.2.71多次尝	试访问目标 null	2020-01-02 17:29:47						
5 4	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	121.51.23.159	发现访客10.50.2.71多次尝	:试访问目标 null	2020-01-02 17:29:36						
6 5	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	183.232.95.149	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:29:34						
7 6	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	119.29.29.29	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:28:12						
8 7	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	119.29.29.29	发现访客10.50.2.71多次尝	试访问目标 null	2020-01-02 17:27:59						
9 8	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	120.241.186.171	发现访客10.50.2.71多次尝	试访问目标 null	2020-01-02 17:27:56						
10 9	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	111.47.223.195	发现访客10.50.2.71多次尝	试访问目标 null	2020-01-02 17:24:24						
11 10	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	112.47.4.157	发现访客10.50.2.71多次尝	试访问目标null	2020-01-02 17:19:46						
12 11	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	121.51.131.56	发现访客10.50.2.71多次尝	:试访问目标 null	2020-01-02 17:18:50						
13 12	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	112.60.0.199	发现访客10.50.2.71多次尝	:试访问目标 null	2020-01-02 17:18:47						
14																
15																
16																
17																
18																
19																
20																
21																
22																
23																

点击操作中的【查看】

用户指南

总范 告警监控 ×									
查看									×
📕 基本信息									
(中危)XXE实体注	入攻击								
告誓内容:发现:	0.9.2.463120.35.5.1463	E施XXE实体注入攻击	行为			原理	现在越来越多主要的web程/	李被发现和报告存在XXE(XML External Entity	attack)漏洞,比如说facebook、
告替类别:注入3	て击						paypal等等。举个例子,我	们扫一眼这些网站最近奖励的漏洞,充分证: 来设有获得立中得的关注度,得多VMI的解释	实了前面的说法。尽管XXE漏洞已 6葉對以具合有VVE浸湿的 注意
告替源:120.3	5.5.146						味着开发人员有责任确保这	些程序不受此漏洞的影响。	
源IP:10.9.3	.46								
目的IP:120.3	5.5.146					范吉	此屬洞非常危险。因为此屬源	N会造成服务器上軟感数据的泄露,和潜在的	服务器拒绝服务攻击。
被攻击者城名:						安全建议	配置XML处理器去使用本地	静态的DTD,不允许XML中含有任何自己声明	月的DTD.
被攻击者端口:									
生成时间:2020	12-25 14:02:39								
告誓追溯:									
8		0	6	0	&				
扫描探測 遭受	y击 已被入侵	C&C還信	内网渗透	盗取数据	黒戸牟利 (投矿、勤素、晴徳)				更多详情》
					^				
📕 关联事件列表									
时间: 请选择事件多	生时间 ~								✓ 査询 本員
🕹 封埔IP 📃 📍 加入黑名	£								
序号 事件名称		事件类型 等级	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		资产名称/IP地址	设备	类型 遼IP	目的P	协议 操作
								共1条 上一页 1 下一页	10 条/页 > 到第 1 页 确 定

点击操作中的【一键断网】,可以对 IP 进行封堵。 点击操作中的【恢复断网】,可以对 IP 进行解封。

5、已关闭告警

事件分析>告審监控		O R#*
时间: 近15分钟 ~		
其 告警统计	■ 告警类型分布 ◎	■ 告警触发规则排名TOP5 [®]
株位置 日位置 367 0 電気以上 中間 367 0	367 ■ 私家病毒(357) 关联分析音图数 ■ 其色(0)	[1988;2019-003]取波病毒:367
待确认告誓(367) 待处理告誓(0) 已派单告誓(0) 已忽略告誓((へ改起 0) 已关闭告誓(0)	
音智英則:全部 ~ 等級:全部 ~ 工単状态:全	# ◇ 散发规则: 告替源: 告	響名称: 査询 _ 王玉
□ 导出Excel ▲ 加入無名单		
序号 告罄名称/内容 来遊 告醫遊	告察关别 触发规则 生成时间 等级 滚口	目的IP 关闭时间 工单状态 操作
	暫无数据	

点击【导出 excel】,导出页面如下

										2020010)/安主事件	F告留号	出清單 (1).xis	[兼容模式] -	Excel(miniations)	夫奴()									
文件	开始	插入 页面布	局 公式	数据	审阅 衫	UEI 🖓	告诉我您想要做什么																		
精點	6 剪切 ● 复制 → ● 复制 →	Arial B I U -	• 10 E • 🖄 • 🔺	A A		- ≫- • •	自动换行 合并后居中 ·	常規 擎 - % ,	•.0.0.00	また。 条件格式 マ	要用 表格格式、	常規	单元格	差 <i>解释性文</i> :	好 ☆ 警告文	本	适中 链接单元格	计算 输出	× • •	■■	影	₩ 橋式 v	∑ 自动求 ■ 填充・	印、加加、加加、加加、加加、加加、加加、加加、加加、加加、加加、加加、加加、加加	A Z▼ ≶和陈选 查
鲍则	板店		字体	r	5	对齐方	st s	数字	5						样式						单元格			编	緝
A1	Ŧ	: × ~	fx 序号																						
4	A	в	С		D	E	F		G		н			1		J		к		L	N	1	N	0	Р
1 店	号	告警名称	类型		告警类别	告警等级	告警源		源IP		目的IP)		告警内容		处置状态		发生时间							
2 1	检测	则到敏感信息泄漏	关联分析告警		信息泄露	高危	47.103.217.163	47.103.3	217.163	10.50	0.5.230		检测到47.	103.217.1637	7在敏感信息池	null	2020-01-03	10:08:46							
3 2	跨如	山脚本攻击	关联分析告警		跨站脚本	中危	10.5.12.55	114.242	.143.169	10.5.	12.55		发现访睿1	14.242.143.1	69 对目标10.5	null	2020-01-02	20:10:11							
4 3	数数	較件扫描	关联分析告警		扫描行为	低危	10.50.2.71	10.50.2	71	121.6	51.23.159		发现访客1	0.50.2.71多次	《尝试访问目标	null	2020-01-02	17:29:47							
5 4	数	纹件扫描	关联分析告警		扫描行为	低危	10.50.2.71	10.50.2	71	121.6	51.23.159		发现访客1	0.50.2.71多次	《尝试访问目标	null	2020-01-02	17:29:36							
6 5	敬い	纹件扫描	关联分析告警		扫描行为	低危	10.50.2.71	10.50.2	71	183.2	232.95.14	9	发现访客1	0.50.2.71多次	《尝试访问目标	null	2020-01-02	17:29:34							
7 6	敬頼	120件扫描	关联分析告警		扫描行为	低危	10.50.2.71	10.50.2	71	119.2	29.29.29		发现访客1	0.50.2.71多岁	《尝试访问目标	null	2020-01-02	17:28:12							
8 7		120件扫描	关联分析告警		扫描行为	低危	10.50.2.71	10.50.2	71	119.2	29.29.29		发现访客1	0.50.2.71多岁	《尝试访问目标	null	2020-01-02	17:27:59							
9 8		120件扫描	关联分析告警		扫描行为	低危	10.50.2.71	10.50.2	71	120.2	241.186.1	71	发现访客1	0.50.2.71多次	《尝试访问目标	null	2020-01-02	17:27:56							
10 9		11文件扫描	关联分析告警		扫描行为	低危	10.50.2.71	10.50.2	71	111.4	47.223.19	5	发现访客1	0.50.2.71多次	《尝试访问目标	null	2020-01-02	17:24:24							
11 10		11文件扫描	关联分析告警		扫描行为	低危	10.50.2.71	10.50.2	71	112.4	47.4.157		发现访客1	0.50.2.71多次	《尝试访问目标	null	2020-01-02	17:19:46							
12 11		較件扫描	关联分析告警		扫描行为	低危	10.50.2.71	10.50.2	71	121.6	51.131.56		发现访客1	0.50.2.71多次	R尝试访问目标	null	2020-01-02	17:18:50							
13 12		較件扫描	关联分析告警		扫描行为	低危	10.50.2.71	10.50.2	71	112.6	60.0.199		发现访客1	0.50.2.71多次	R尝试访问目标	null	2020-01-02	17:18:47							
14																									
15																									
16																									
17																									
18																									
19																									
20																									
21																									
22																									
23																									

左边勾选框勾选多项,点击【加入黑名单】,可以批量对告警中的源 IP 或目的 IP 加入黑名单。

点击操作中的【查看】

总流 告警监控 ×	
查看	x
ਡ 基本信息	
(中危)XXE实体注入攻击	
雪智内音: 光現10.9.2.46対10.35.5.146実施XXE実体注入攻击行为 音智原则: 注入攻击 音智原言: 12.03.5.146 原則: 10.9.2.46 目的P: 12.03.5.146 核び击者執行	 取在越来越多主要的web環境能況現和提告存在XXEXMLEterralEntity attacki展向,比如現场ocebook, psypai每%,都个每子,我们已一般这些限论最优度效的选展问,充分企实了有面的创起。尽管XXE展现已 经存在了很多年。但是比水规定有可定立理的过程。我有关的比如都折蹦就认是含有XXE展现的,这里 除着开发人员有责任确保证当程序不受此意间的参加。 此果得非常能加、因为此展明合油或服务器上数据数据的泄漏,和指在的部务器把包服导攻击。 設置 配置XML处理器去使用年短静态的DTD,不允许XML中含有任何自己再明的DTD。
生成时间:2020-12-25 14:02:39	
舌部追溯:	
● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	更多详情》
★联事件列表	
时间: 情选择事件发生时间 >	✓ 査察 定用
る.封海12 🔍 加入黒石単	
□ 序号 李件名称 李件类型 等级 时间	设备类型 遵护 目的印 协议 操作
	共1条 上→河 Ⅰ 下→河 10条/页> 到版 1 页 (発定

点击操作中的【加入黑名单】,可以对告警中的源 IP 或目的 IP 加入黑名单。 点击操作中的【一键断网】,可以对 IP 进行封堵。 点击操作中的【恢复断网】,可以对 IP 进行解封。

2.4.2 日志检索

路径:事件分析->日志检索。

#142701*D/0/02/R																		0/2	191
近15分钟 ~ 2021-5	-19 11:11:53		2021-5-19 1	1:26:53										收藏	己录	~	★ 流量	日志检索	
5 #																	展开其它	豪件 ~	
源IP:				目的	SIP :		源端口:			Eß	端口 :			源地理	位置:				
目的地理位置:				采集			事件等级:			事件	分类:			原始	旧志:				L
"注:"+"表示"或",要	要输入多个的	影件可输入"a	+b" , 代表"aś	条件或b条件"			22 <u>4</u>	iii)	添加到收藏										
展开统计图 ~																			I.
按源IP活跃度	分	类排行		事件列表	ŧ														
源IP活跃度搜索		Q	0	▲ 找量	加入黑名单	🕞 黄份导出 📋 抗量制除													
潤IP	分类数	事件数		序号	原始事件名称	事件名称	事件分类	等级令	发生时间 ≑	采集时间	日志遼	设备类型	遭IP	遼端口	目的IP	目的端口	协议	操作	
10.50.2.164	4	1521		1		恶意程序	恶意程序	严重	2021-04-14	2021-05-19	10.9.17.1	启明星辰IPS	10.50.2.164[保留]	18332	45.58.135.1 06[荷兰]	80	tcp	鳥 ⊛	
				2		恶意程序	恶意程序	≓ ≡	2021-04-14	2021-05-19	10.9.17.1	启明星辰IPS	10.50.2.164[保留]	18332	45.58.135.1 06[荷兰]	80	tcp	≜ ⊙	
				3		恶意程序	恶意程序	严重	2021-04-14	2021-05-19	10.9.17.1	启明星覆IPS	10.50.2.164[保留]	18332	45.58.135.1 06[荷兰]	80	tcp	鳥 ⊙	
				4		恶意程序	恶意程序	≓ ≡	2021-04-14	2021-05-19	10.9.17.1	启明星夜IPS	10.50.2.164[保留]	18332	45.58.135.1 06[荷兰]	80	tcp	鳥 ⊙	

点击源 Ip, 跳至 Ip 画像

(INELASSP Q) 10.50.1.159 ByliR : [£15946 √] 2020-1-141654	局加网 <mark>古田地</mark> k39 🛗 2020-1-14 17;	A 加入第名単 民 P低目が終 1139 〒 含 約			
数无数据 数 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	10 <mark>5011</mark> 59				
(1) 2017 (1) 20	01-14 (双 書 藝			
			人收起		
▼ 分类	📕 事件列表				
(关键字搜索 Q	0				
所有分类	数量 亊	件名称	事件分类	时间范围	
	智无数据				

点击【ip 信息详情】,进入 ip 信息详情页面

<u>83</u>	き 事件格	索 × 10.50.1	.159 ×								
IF	信息详情										×
	情报信息	资产信息									
	10.50.1.1	59 未封堵									
		IP别名:								(State	
		地理位置:	局域网	经度0.000000	纬度0.000000					AL MAN	
		标签:								(is a second se	
	威胁情报(0)	相关样本(0)	域名(0)	开放調口(0)							
	中国				**		(in c. 1978)		***		
	*42				权规则问		1410/19882		<u>22</u>		
										共0张信恩	

点击"分类排行",可勾选分类检索筛选安全事件

事件分析>日志检索																ORM
近15分钟 ~ 2021-5-19 11:11	.53 🗐 2021	-5-19 11:2	6:53									收藏	记录	×	+ 法国	目志检索
与罪															展开其	它条件~
Imip :			目的IP:		源靖口:			目的	湖口:			源地知	1位置:			
目的地理位置:			采集器:		事件等级:			事件	:分类:			原如	8日志:			
*注:"+"表示"成",需要输入多	个条件可输入"a+b",	代表"a条件	F成b条件"		25 C	19 (流加到收藏									
幕开统计划 >																
按源IP活跃度	分类排行	X 3	4件列表													
事件分类搜索	Q	0	🤱 就量加入黑名单 🗌 🕞	11日日 11日 11日日 11日日 11日日 11日日 11日日 11日日												
◇ □ 所有分类	1521		序号 医始事件名称	事件名称	事件分类	等级章	发生时间章	采集时间	日志遊	设备类型	源IP	逐渐口	EMP	目的第口	协议	操作
 □ 发现抱旷程序 □ 发现勘测软件 □ 商意程序 	652 362 362		1	志意程序	恶意程序	72	2021-04-14	2021-05-19	10.9.17.1	启明星微IPS	10.50.2.164[保留]	18332	45.58.135.1 06[荷兰]	80	tcp	_ ▲ ⊙
□□ 发现木马恶意程序	145		2	恶意程序	恶意程序	≓ ∎	2021-04-14	2021-05-19	10.9.17.1	启明星辰IPS	10.50.2.164[保田]	18332	45.58.135.1 06[確当]	80	tcp	. 0
			3	恶意程序	恶变程序	72	2021-04-14	2021-05-19	10.9.17.1	启明星表IPS	10.50.2.164[保賀]	18332	45.58.135.1 06[荷兰]	80	tcp	. 0
			4	恶意程序	恶意程序	7 2	2021-04-14	2021-05-19	10.9.17.1	启明星 微IPS	10.50.2.164[保留]	18332	45.58.135.1 06[荷兰]	80	tcp	. ⊛
	_		5	而意程序	而會經常		7071-04-14	2021-05-19	10.9.17.1	户印度展示(PS	10.50.2.164[18332	45.58.135.1	80	ten	۹. (۱)
										共 1521	条 上一回	1	2 3 4	5 F	-页 2	10 条/页~

左边勾选框勾选多项,点击【批量加入黑名单】,可将一个或多个源 ip 或目的 ip 加入黑名单。

左边勾选框勾选多项,点击【备份导出】,导出页面如下

A A	B C D	E	F G	H	1 1	K	L.	M	N O	P	Q R	S T	UV	I V	N X	Y
1 序号	事件名称 事件分类 等级	发生时间(occuretime)	호텦(device 源IF	P 源调口	目的IP 目的潮口]) iii (proto	cci规则D(rul	原始规则名称(rulename)	内容 (log content)							
2 1	4458#314 8#24322.8 仮危	2021-01-27 10:55 10	8#40657;8172.20	0.11.55269	84.161.22(445	tcp	6227121	主机被8	\$#2 {"eventType&quo	t: 1064,&qu	ot;eventName"	"6227121&quo	t;,"protocol&	quot;; &qu	uot;tcp"J	& quot; srclp&quc
3 2	445ĺ 异 8 低地	2021-01-27 10:54:10	黑8172.20	0.11.64676	152 205 87445	tcp	6227121	主机被8	\$#2 ["eventType&quo	t: 1064.&qu	ot,eventName"	: & quot: 6227121& quo	t; " protocol&	quot;: &q	uot;tcp"	"_srclp&quc
4 3	8#26292;88#26292;8中危	2021-01-27 10:53:40	黑,810.9.1	4.33 3306	10.9.14.16 48959	tcp	2010494	MySQL登录&#	f262 ["eventType&quo	t:: 1004.&qu	ot;eventName"	":2010494&quo	t;,"protocol&	quot;: &qu	uot;tcp".i	"srclp&quc
5 4	暴.8 暴.8 中危	2021-01-27 10:53:40	8#40657;810.9.1	4.33 3306	10.9.14.16 48959	tcp	2010494	MySQL登录&#</td><td>262 [& quot; eventType& quo</td><td>t:: 1004,&qu</td><td>ot, eventName"</td><td>& quot:2010494& quo</td><td>t; " protocol&</td><td>quot;: &q</td><td>uot;tcp"_i</td><td>"srclp&quc</td></tr><tr><td>6 5</td><td>8#26292;88#26292;8中范</td><td>2021-01-27 10:53:40</td><td>8#40657;810.9.1</td><td>4.33 3306</td><td>10.9.14.16.48960</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>1262 [& quot; eventType& quo</td><td>t: 1004,8.qu</td><td>ot;eventName"</td><td>: & quot:2010494& quo</td><td>t; ," protocol&</td><td>quot;: &q</td><td>pot;tcp"_l</td><td>"_srclp&quc</td></tr><tr><td>7 6</td><td>暴.8 暴.8 中危</td><td>2021-01-27 10.53.40</td><td>黑810.9.1-</td><td>4.33'3306</td><td>10.9.14.16 48960</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>1262 (" eventType&quo</td><td>t: 1004,&qu</td><td>ot,eventName"</td><td>"2010494&quo</td><td>t; " protocol&</td><td>quot;: &q</td><td>uot;tcp"i</td><td>"_srclp&quc</td></tr><tr><td>8 7</td><td>8#26292;88#26292;8中危</td><td>2021-01-27 10:53:39</td><td>8#40657;810.9.14</td><td>4.33 3306</td><td>10.9.14.16 48949</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>262 (& quot; eventType& quo</td><td>t: 1004,8 qu</td><td>ot;eventName"</td><td>8 quot: 20104948 quo</td><td>t;,"protocol&</td><td>quot;: &qu</td><td>uot;tcp"J</td><td>& quot;srclp&quc</td></tr><tr><td>9 8</td><td>暴.8 暴.8 中危</td><td>2021-01-27 10:53:39</td><td>黑.8 10.9.1</td><td>4.33 3306</td><td>10.9.14.16 48946</td><td>tcp</td><td>2010494</td><td>MySQL登,录,&#</td><td>262 ["eventType&quo</td><td>t: 1004,&qu</td><td>ot, eventName"</td><td>":2010494&quo</td><td>t;,"protocol&</td><td>quot;: &q</td><td>pot top" .i</td><td>& quot_srclp&quc</td></tr><tr><td>10 9</td><td>8#26292,88#26292,8中危</td><td>2021-01-27 10:53:39</td><td>8#40657.8 10.9.1</td><td>4.33 3306</td><td>10.9.14.16 48947</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>262{"eventType&quo</td><td>t:: 1004.&qu</td><td>ot;eventName"</td><td>: & quot;2010494& quo</td><td>t;,"protocol&</td><td>quot;: &q</td><td>uot;tcp" l</td><td>& quot_srclp& quot</td></tr><tr><td>11 10</td><td>暴.8 暴.8 中危</td><td>2021-01-27 10:53:39</td><td>黑.810.9.1</td><td>4.33 3306</td><td>10.9.14.16 48947</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>1262 [& quot; eventType& quo</td><td>t: 1004,&qu</td><td>ot, eventName"</td><td>"2010494&quo</td><td>t; " protocol&</td><td>quot;: &q</td><td>uot;tcp"_i</td><td>& quot; srclp& quc</td></tr><tr><td>12 11</td><td>8#26292;88#26292;8中危</td><td>2021-01-27 10 53:39</td><td>黑810.9.14</td><td>4.33 3306</td><td>10.9.14.16 48949</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>1262 [& quot; eventType& quo</td><td>t: 1004.8.qu</td><td>ot;eventName"</td><td>& quot;2010494& quo</td><td>t;;"protocol&</td><td>quot;: &q</td><td>pot;tcp"_l</td><td>& quot_srclp& quc</td></tr><tr><td>13 12</td><td>暴,8暴,8中危</td><td>2021-01-27 10:53:39</td><td>8#40657,810.9.1</td><td>4.33 3306</td><td>10.9.14.16 48948</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>1262 [& quot, eventType& quo</td><td>t.: 1004,&qu</td><td>ot,eventName",</td><td>",2010494&quo</td><td>t;,"protocol&</td><td>quot;: &q</td><td>uot top"</td><td>"_srclp&quc</td></tr><tr><td>14 13</td><td>8#26292,88#26292,8中危</td><td>2021-01-27 10:53:39</td><td>8#40657:8 10.9 14</td><td>4.33 3306</td><td>10.9.14.16.48950</td><td>tcp</td><td>2010494</td><td>MySQL登录.&#</td><td>262 (& quot; eventType& quo</td><td>t: 1004.&qu</td><td>ot;eventName"</td><td>& quot:2010494& quo</td><td>t;,"protocol&</td><td>quot; &q</td><td>pot;tcp"i</td><td>& quot_srclp&quc</td></tr><tr><td>15 14</td><td>暴.8 暴.8 中危</td><td>2021-01-27 10:53:39</td><td>黑,810.9.1</td><td>4.33'3306</td><td>10.9.14.16 48952</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>R262 (& quot; eventType& quo</td><td>t: 1004.&qu</td><td>ot,eventName"</td><td>& quot, 2010494& quo</td><td>t,,"protocol&</td><td>quơt,: & qi</td><td>eqt(tcp"_i</td><td>"_srclp&quc</td></tr><tr><td>16 15</td><td>8#26292;88#26292;8中炮</td><td>2021-01-27 10:53:39</td><td>8#40657;810.9.1-</td><td>4.33'3306</td><td>10.9.14.16.48955</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>262 ("eventType&quo</td><td>t: 1004.8.qu</td><td>ot, eventName",</td><td>"2010494&quo</td><td>t;;"protocol&</td><td>quot;: &q</td><td>pot;tcp"l</td><td>"_srclp&quc</td></tr><tr><td>17 16</td><td>8#26292.88#26292.8中危</td><td>2021-01-27 10:53:39</td><td>8#40657;810.9.1</td><td>4.33'3306</td><td>10.9.14.16 48950</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>262 [& quot, eventType& quo</td><td>t: 1004.&qu</td><td>ot;eventName"</td><td>"2010494&quo</td><td>t;,"protocol&</td><td>quot;: &q</td><td>eot;tcp".i</td><td>"_srclp&quc</td></tr><tr><td>18 17</td><td>暴8 暴8 中危</td><td>2021-01-27 10:53:39</td><td>黑810.9.14</td><td>4.33'3306</td><td>10.9.14.16.48958</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>262 (& quot; eventType& quo</td><td>t:: 1004.&qu</td><td>ot;eventName"</td><td>":2010494&quo</td><td>t;,"protocol&</td><td>dnot: g dr</td><td>pot;tcp" l</td><td>"_srclp&quc</td></tr><tr><td>19 18</td><td>8#26292,88#26292,8中危</td><td>2021-01-27 10:53:39</td><td>8#40657;810.9.1</td><td>4.33'3306</td><td>10.9.14.16 48957</td><td>tcp</td><td>2010494</td><td>MySQL登.录.&#</td><td>f262 {"eventType&quo</td><td>t: 1004,&qu</td><td>ot;eventName"</td><td>"2010494&quo</td><td>t;,"protocol&</td><td>quot;: &q</td><td>uot;tcp"_l</td><td>",srclp&quc</td></tr><tr><td>20 19</td><td>8#26292.88#26292.8中危</td><td>2021-01-27 10:53:39</td><td>8#40657.810.9.1</td><td>4.33'3306</td><td>10.9.14.16.48946</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>262 (& quot; eventType& quo</td><td>t: 1004.8.qu</td><td>ot.eventName".</td><td>"2010494&quo</td><td>t; " protocol&</td><td>quot;: &q</td><td>aot;tcp"</td><td>& quot_srclp& quc</td></tr><tr><td>21 20</td><td>暴,8 暴,8 中危</td><td>2021-01-27 10:53:39</td><td>8#40657;810.9.1</td><td>4.33'3306</td><td>10.9.14.16.48948</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>P262 (& quot; eventType& quo</td><td>t: 1004.8.qu</td><td>ot;eventName"</td><td>"2010494&quo</td><td>it;,"protocol&</td><td>quot;: &q</td><td>aot top8 quot</td><td>& quot, srclp& quc</td></tr><tr><td>22 21</td><td>暴.8 暴.8 中危</td><td>2021-01-27 10:53:39</td><td>8#40657,810.9.1</td><td>4.33'3306</td><td>10.9.14.16.48951</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>262 (& quot, eventType& quo</td><td>t: 1004.&qu</td><td>ot, eventName"</td><td>"2010494&quo</td><td>t; ," protocol&</td><td>dnot): gd</td><td>pot;tcp",i</td><td>"_srclp&quc</td></tr><tr><td>23 22</td><td>暴.8 暴.8 中危</td><td>2021-01-27 10:53:39</td><td>8#40657.810.9.1</td><td>4.33'3306</td><td>10.9.14.16 48955</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>262 [& quot; eventType& quo</td><td>t: 1004.8.qu</td><td>ot,eventName"</td><td>: & quot:2010494& quo</td><td>t;,"protocol&</td><td>quot;: & q</td><td>aot;tcp8quot;.l</td><td>& quot; srclp& quc</td></tr><tr><td>24 23</td><td>暴.8 暴.8 中危</td><td>2021-01-27 10:53 39</td><td>黑.810.9.1-</td><td>4.33'3306</td><td>10.9.14.16'48953</td><td>tcp</td><td>2010494</td><td>MySQL登,录,&#</td><td>262 (" eventType&quo</td><td>t: 1004,&qu</td><td>ot, eventName",</td><td>".2010494&quo</td><td>t".protocol&</td><td>quot; &q</td><td>eot.tcp".i</td><td>"_srclp&quc</td></tr><tr><td>25 24</td><td>暴88#26292;8中危</td><td>2021-01-27 10:53:39</td><td>8#40657;810.9.1</td><td>4.33 3306</td><td>10.9.14.16 48956</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>262 (& quot; event l ype& quo</td><td>t: 1004,8 qu</td><td>ot, eventName"</td><td>8 quot:20104948 quo</td><td>t;,"protocol&</td><td>anot:: ga</td><td>Jot top"</td><td>& quot srclp& quo</td></tr><tr><td>26 25</td><td>暴8 暴8 中党</td><td>2021-01-27 10:53:39</td><td>8.#40657.810.9.1</td><td>4.333306</td><td>10.9.14.16 48958</td><td>tcp</td><td>2010494</td><td>MySQL登,录,&#</td><td>1262 (& quot; eventType& quo</td><td>t: 1004.8.qu</td><td>ot.eventName",</td><td>& quot, 2010494& quo</td><td>t;,"protocol&</td><td>quot; & q</td><td>aot, tcp".</td><td>"_srclp&quc</td></tr><tr><td>27 26</td><td>8#26292;88#26292;8中危</td><td>2021-01-27 10:53:39</td><td>8#40657;810.9.1</td><td>4.333306</td><td>10.9.14.16 48951</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>262 (& quot; eventType& quo</td><td>t: 1004.8.qu</td><td>ot, eventName"</td><td>",2010494&quo</td><td>t; " protocol&</td><td>dnot:: g dr</td><td>Jot top8 quot</td><td>& quot, srclp& quo</td></tr><tr><td>28 27</td><td>暴.8暴.8中危</td><td>2021-01-27 10:53:39</td><td>黑,810.9.1</td><td>4.33'3306</td><td>10.9.14.16 48952</td><td>tcp</td><td>2010494</td><td>MySQL登,录.&#</td><td>262 (" eventType&quo</td><td>t: 1004,&qu</td><td>ot,eventName",</td><td>",2010494&quo</td><td>t,,",protocol&</td><td>quot;: &q</td><td>vot, tcp"</td><td>"_srclp&quc</td></tr><tr><td>29 28</td><td>8#26292.88#26292.8中危</td><td>2021-01-27 10 53 39</td><td>8#40657;810.9.1</td><td>4.33'3306</td><td>10.9.14.16.48954</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>262 (& quot; eventType& quo</td><td>t: 1004.8.qu</td><td>ot;eventName"</td><td>& quot 2010494& quo</td><td>t.,"protocol&</td><td>dnot: gd</td><td>pot;tcp" l</td><td>"_srclp&quc</td></tr><tr><td>30 29</td><td>暴.8暴.8中危</td><td>2021-01-27 10:53 39</td><td>8#40657.810.9.1</td><td>4.33'3306</td><td>10.9.14.16 48954</td><td>tcp</td><td>2010494</td><td>MySQL登录&#</td><td>1262 ["eventType&quo</td><td>t: 1004,&qu</td><td>ot, eventName"</td><td>" 2010494&quo</td><td>t.,".protocol&</td><td>quot;; &q.</td><td>uot.tcp"./</td><td>"srclp&quc</td></tr></tbody></table>								

左边勾选框勾选多项,点击【批量删除】,可以批量删除选中内容。 点击操作中的【加入黑名单】,可将源 ip 或目的 ip 加入黑名单。 点击操作中的【pcap 下载】,可下载 pcap。

点击查询结果中单个安全事件,下方下拉安全事件详情,点击更多详情,跳转至 事件详情页面

总宽	事件检索 ×				
事件详	恃				×
基本	属性				
		事件名称:	系统漏洞攻击	事件等级:	中間
		事件分类:	尝试利用属词的攻击行为	设备类型:	海峡黑蝠APT防御系统
		发生时间:	2020-01-14 10:30:01	采集时间:	2020-01-14 10:31:49
		日志源IP:	10.52.0.67	日志源资产:	黑箔APT
		采集器:	Collector_10.9.1.150_15	攻击锚阶段:	遭受攻击
		原始事件类型:		原始规则名称:	GPL NETBIOS SMB IPC\$ unicode共豪访问
		操作及响应动作:	1	操作结果:	
		准确度:	2		
网络	萬性				
		源IP:	10.50.1.159	源端口:	53921
		目的IP:	10.50.1.201	目的端口:	139
		源ip地理信息:	(country=尾城网, province=, city=, longitude=0.000000, latitude=0.000000)	目的ip地理信息:	{country=尾域网, province=, city=, longitude=0.000000, latitude=0.000000}
		源主机名:		目的主机名:	NULL
		渡IP标签:	0	目的IP标签:	0
		发送字节数:	0	接受字节数:	0
		协议:	tcp	用户:	NULL
		文件名称:			
			-		
				关闭	

2.4.3 审计事件

路径:事件分析->审计事件。

事件分析>育	计事件							0 8
事件名称	t:	事件来源:	对象IP:	触发规则名称:				28 EE
序号	事件名称		对象IP	事件等级	事件来源	触发规则名称	生成时间	⇒ 提作
1	恶意程序		10.50.0.111	严重	基线分析规则	源)清口-接收流量	2021-05-14 14:59:34	R
2	恶意程序		10.50.0.111	严重	基线分析规则	源端口-接收流量	2021-05-14 14:59:34	R
з	恶意程序		10.50.0.111	严重	基线分析规则	源講口-接收流量	2021-05-14 14:59:34	R
4	恶意程序		10.50.0.111	严重	墓线分析规则	源號口-接收流量	2021-05-14 14:59:34	R
5	恶意程序		10.50.0.111	严重	基线分析规则	源端口-接收流量	2021-05-14 14:59:34	R
6	恶意程序		10.50.0.111	严重	基线分析规则	漂拂口-接收流量	2021-05-14 14:59:34	R
7	恶意程序		10.50.0.111	FE	基线分析规则	源講□-接收流量	2021-05-14 14:59:34	R
8	高意程序		10.50.0.111	严重	基线分析规则	源);曰-接收流量	2021-05-14 14:59:34	R
9	恶意程序		10.50.0.111	严重	基线分析规则	源端口-接收流量	2021-05-14 14:59:34	R
10	恶意程序		10.50.0.111	严重	基线分析规则	源端口-接收流量	2021-05-14 14:59:34	R
11	恶意程序		10.50.0.111	严重	基线分析规则	源靖口-接收流量	2021-05-14 14:59:34	R
12	恶意程序		10.50.0.111	产里	基线分析规则	源)出口-接收流量	2021-05-14 14:59:34	R
13	恶意程序		10.50.0.111	严重	醫线分析规则	源靖口-接收流量	2021-05-14 14:59:34	R
14	恶意程序		10.50.0.111	≓ ≢	基线分析规则	源靖口-接收流量	2021-05-14 14:59:34	R
15	恶意程序		10.50.0.111	严重	基线分析规则	源)月-接收流量	2021-05-14 14:59:34	R
			10 50 0 111		Sec. 12. 71. 107 (1277)	200 mar (***) - ante (au) an (***	2021 05 1111 0 0 11	•
							共18622630条 上一页 1 2 3 4 5	下一页 20 条/页~

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】, 查询条件内容清空。

点击【查看】,跳至审计事件详情页面。

查看										
📕 基本信息										
	事件名称:	恶意程序				对象IP:	10.50.0.111			
	事件等级:	严重				事件来源:	基线分析规则			
	触发事件名称:	源端口-接收流量				关联日志数:	1			
	生成时间:	2021-05-14 14:59:34								
📕 关联日志										
序号	事件名称	事件分类	事件等级	发生时间	遼IP	ž	夏靖口	目的IP	目的端口	操作
1	恶意程序	恶意程序	严重	2021-05-14 14:59:34	10.50.2.164	2	865	163.172.205.136	80	R

点击【查看】,跳至日志详情页面。

2 4			
日志详情			
基本属性			
事件名称:	形意程序	事件等级:	严重
事件分类:	冠章程序	设备类型:	做步在线或胎检测平台
发生时间:	2021-05-14 14:59:34	采集时间:	2021-05-14 15:00:12
日志源(设备IP):	10.50.0.111	日志源(设备名称):	10.50.0.111
采集器:	Collector_127.0.0.1_1	攻击链阶段:	遭受攻击
原始事件类型:		原始规则名称:	ÍÚ¿ó
操作及响应动作:		操作结果:	
准确度:	5		
网络属性			
源IP:	10.50.2.164	源端口:	2865
目的IP:	163.172.205.136	目的端口:	80
源ip地理信息:	(country=保留, province=, city=, longitude=0.000000, latitude=0.000000)	目的ip地理信息:	(country=法国, province=, city=巴黎, longitude=2.213749, latitude=46.227638)
源主机名:		目的主机名:	
源IP标签:		目的IP标签:	
发送字节数:	823	接受字节数:	448
协议:	tcp	用户:	

2.4.4 关联事件

路径:事件分析->关联事件。

时午名和	: 1	攻击者:	被攻击者:	触发规则名称:					E N
序号	爭件名称	事件分类	攻击者		极攻击者	事件等级	触发现则名称	生成时间	⇒ 操作
1	勤素软件	发现到麦软件	10.50.2.164		137.74.46.46	72	检测到勘索病毒通信	2021-05-19 14:00:30	R
2	勘索软件	发现勤要软件	10.50.2.164		91.234.32.19	严重	检测到勘查病毒通信	2021-05-19 14:00:28	Fa
3	勤宪软件	发现勘察软件	10.50.2.164		195.123.209.123	严重	检测到勘察病毒通信	2021-05-19 14:00:24	EA
4	勘索软件	发现额套软件	10.50.2.164		137.74.46.46	FE	检测到勤实病毒通信	2021-05-19 14:00:23	R
5	勘赏软件	发现副素软件	10.50.2.164		91.234.32.19	严重	检到到勤業病毒通信	2021-05-19 14:00:21	R
6	题发软件	发现额素软件	10.50.2.164		137.74.46.46	严重	检测到勘赏病毒通信	2021-05-19 14:00:18	E
7	勤素软件	没现到要软件	10.50.2.164		91.234.32.19	戸室	检测到勘索病毒通信	2021-05-19 14:00:16	PA
8	勤策软件	发现数要软件	10.50.2.164		195.123.209.123	严重	检测到勤繁病毒通信	2021-05-19 14:00:12	Fa
9	勘实软件	发现教室软件	10.50.2.164		137.74.46.46	78	检测到勤实病毒通信	2021-05-19 14:00:11	Pa
10	勘索软件	发现职责软件	10.50.2.164		91.234.32.19	严重	检测到职实病毒通信	2021-05-19 14:00:09	R
11	勘索软件	发现勤赏软件	10.50.2.164		137.74.46.46	严重	检测到勘赏病毒通信	2021-05-19 14:00:06	R
12	勤策软件	发现到素软件	10.50.2.164		91.234.32.19	戸室	检测到勘索病面通信	2021-05-19 14:00:04	R
13	勤繁软件	发现勘察软件	10.50.2.164		195.123.209.123	₽ ∎	检测到数素病毒通信	2021-05-19 14:00:00	R
14	勘案软件	发现额素软件	10.50.2.164		137.74.46.46	严重	检测到数素病毒通信	2021-05-19 13:59:59	EA.
15	勘察软件	发现勤奏软件	10.50.2.164		91.234.32.19	严重	检测到副实病毒通信	2021-05-19 13:59:57	R
÷.	We also not the	LECTRON AND PARTY.	*******				en. The Trade and address 198 Adv		

共284682条 上一页 1 2 3 4 5 下一页 20条/页~

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】, 查询条件内容清空。

点击【查看】,跳至关联事件详情页面。



点击【查看】,跳至日志详情页面。

查看			
日志详情			
基本属性			
事件名称:	恶意程序	事件等级:	严重
事件分类:	恶意怪序	设备类型:	微步在线或影检测平台
发生时间:	2021-05-14 14:59:34	采集时间:	2021-05-14 15:00:12
日志源(设备IP):	1050.0.111	日志源(设备名称):	10.500.111
采集器:	Collector_127.0.0.1_1	攻击锚阶段:	遭受攻击
原始事件类型:		原始规则名称:	ĺÚ _č 6
操作及响应动作:		操作结果:	
准确度:	5		
网络属性			
源IP:	10.50.2.164	滂ゥロ:	2865
目的IP:	163.172.205.136	目的講口:	80
凄ip地理信息:	(country=保留, province=, city=, longitude=0.000000, latitude=0.000000)	目的ip地理信息:	(country=法国, province=, city=巴黎, longitude=2.213749, latitude=46.227638)
源主机名:		目的主机名:	
遭 即标签:		目的IP标签:	
发送字节数:	823	接受字节数:	448
协议:	tcp	用户:	
		关闭	

2.5 报表管理

2.5.1 安全报告

路径:报表管理->安全报告。

威胁分析报告	综合日报	综合周报	综合月报
分析内部微产遭受到的外部威胁痛况,以及助种状态。	每日安全状况摘要报告,展示资产状况、攻击事件以及 处置情况等内容。	每周安全代况携要驳告,展示遗产状况、攻击事件以及 处置情况等内容。	每月安全状况講要报告,展示道产状况、攻击事件以及 处置情况等内容。
更多报告 敬请期待			

选择威胁分析报告

		威胁	份析报告	
	() YHER			
				章词 里:
攻击者排名: O TOP10		TOP100		
攻击地区排名: O TOP10	O TOP50	TOP100		
攻击手段列表: 0 TOP10	О ТОР50	TOP100		
				导出报告 历史
一、攻击防护总览				
在报告期间 , 共有来自于	-1个地区的1个攻击;	者,对您的网络发起过10573次攻击。		
		20573次 攻击总数	び 日外置	
		11	11	
대-디ノ		2 攻击者	女 走源地区	
合日报		****	■ ¹ ^{(x ± # # ± ± # ± ± ± ± # ± ± ± ± ± ± ± ±}	
合日报	951 David	- 次由者	●● ^{攻击勝地区}	
合日报 ^{时间面面: ●} 今天 (^{失胸車机} : ● 17210	昨天 回道 17050 Trap	■ 次击者 次击者	●■ ^{攻击勝地区}	6 1
合日报 ^{时间范面} : ● 今天 失知主机: ● TOP10 今日新藻画同: ● TOP10	#天 自始 TOP50 TOP TOP50 TOP	■ 次击者 次击者 2次 100 100	■ ¹ (x ± i 𝑘 = 𝔅 ≤	86 85
合日报 时间范重: • 今天 失知主机: • TOP10 ◆日新煤風网: • TOP10 ◆日新煤風网: • TOP10	許天 目症 TOP50 TOP TOP50 TOP TOP50 TOP	■ 132曲音 (注: 120 100 100	■ x=###	OB III
合日报 时间范围: ● 今天 失阻主机: ● TOP10 今日新環風詞: ● TOP10 今日新環風詞: ● TOP10	#天 回航 TOP50 TOP TOP50 TOP TOP50 TOP TOP50 TOP	■ 132曲音 122 120 100 100	●■ ^{攻击勝地区}	8 H 2
合日报 时间范围: • 今天 失租主机: • TOP10 ◆日新灌溉间: • TOP10 ◆日新灌溉前: • TOP10	昨天 自动 TOP50 TOP TOP50 TOP TOP50 TOP	■ 132曲音 (余) 122 120 100 100	全日报	8日 第三 [92576] (202376)
合日报 时间范围: • • • 天 失時主机: • • тор10 • 日新灌風詞: • • тор10 • 日新灌風詞: • • тор10 • 日新灌風動: • • тор10 • 日新灌風動: • • тор10	昨天 回頭 TOP50 TOP TOP50 TOP TOP50 TOP	■ Xt (100 100 100	今日报	8 (8) 9 (8) 9 (8) 1 (1
合日报 时间范围: ● 今天 失期主机: ● TOP10 ◆日新灌馬開: ● TOP10 ◆日新灌馬筋: ● TOP10 一、今日安全概览 今日您的网络整体安全评明	昨天 回成 TOP50 TOP TOP50 TOP TOP50 TOP TOP50 TOP 3000000000000000000000000000000000000		▲ 1 次击勝地区 合日报 8±机9个,中他主机19个。	9 時 第 第 9 年 日 9 年 日 7 日 7 日 7 日 7 日 7 日 7 日 7 日 7 日 7 日 7

选择综合周报

其中,各业务系统的失陷主机概况如下: 业务系统

失陷主机

			综合周报		
时间范围: 🤇	本周 □上周	□自定义			查询 里亞
本周新増備洞: 🤇	тор10 Отор50	O TOP100			
本周新増威胁: 🤇	тор10 Отор50	O TOP100			
					导出报告 历史下载
一、本周安全相	既的				
本周始的网	洛整体安全评级为 <mark>良</mark> 。:	主要存在以下不安全条目	:已失隘主机1个,高危主机9个,中危主机19个。 良 83分		
其中,各业	务系统的失陷主机概况如	1下 :			
			牛路士机	W/L MW	
	业务系统		VHTM	₩1+芯叙	

事件总数

选择综合月报

综合月报

비미/만료	: 💽 本月	() 上月		查询
本月新増漏洞	O TOP10	O TOP50	O TOP100	
本月新増威胁	• TOP10	O TOP50	O TOP100	
				导出报告 历
一、本月安	全概览			
本月您的	的网络整体安全	全评级为 <mark>差</mark> 。:	主要存在以下不安全条目:已失陷主机0个,高危主机2个,中危主机0个。	
			A MANUAL AND A	

2.5.2 统计报表

路径:报表管理->统计报表。 通过填写相关查询条件,点击【查询】,出现相关查询结果。

选择资产分布统计报表

■ 统计报表类型	时间范围: 近7天 🗸					
✓ ▷ 资产报表 ※ 適产分布統計	□ 导出Word ④ 下数历史					
> > ●	■ 设备类型Top10的资产统计		新田田	•		
○ 単计争件产生趋势统计 >> 关联事件分布统计	📕 资产列表					
)() 关联事件产生趋势统计	序号 资产名称	[IP][遽名][URL]	设备类型	所属业务	入库时间	
			智无数据			

选择告警分布统计报表

■ 统计报表类型	时间范围	1: 近7天 ~						
※ <>>> 法产服表) ※ 第产分布统计	⊖ 导出W	ord ③ 下载历史						
◇ D) 告答报表 (***>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	▲ 告警	类型Top10的告警统计						
2、音響产生趨勢	7W							
 ※ 告答Top10排行 D 日本会社収率 	ew							
2 日本市政統计报表	5W							
201 日志英型统计报表	4W							
○、口念改善未認続け投表 ○、日志等级统计报表	3W							
2) 日志发生总数统计报表	2W							
 二、ロ志友生知識病计被表 > 一 事件統计报表 	0						_	
2、审计事件分布统计		動変病毒			隐蔽地道	1	非法上传	
□< 軍计事件严生趋弱统计 >< 关联事件分布统计	▲ 告警:	列表						
2、关联事件产生趋势统计	序号	告留名称	告留关别	触发规则	遼IP	EMIP	发生时间	
	1	检测到勘察病毒通信	動家病毒	[规则2019-003]勘案/病毒	10.50.2.164 【攻击者】	91.234.32.19【被攻击者】	2021-05-19 11:52:16	
	2	检测到勘察病毒通信	副索病毒	[规则2019-003]勘案病毒	10.50.2.164 【攻击書】	195.123.209.123 【被攻击者】	2021-05-19 11:52:12	
	3	检测到勘察病毒通信	副家病毒	[规则2019-003]勘案病毒	10.50.2.164 【攻击書】	137.74.46.45 【被攻击者】	2021-05-19 11:52:11	
	4	检测到副家病毒通信	副索病毒	[规则2019-003]勘案病毒	10.50.2.164 【攻击者】	91.234.32.19【被攻击者】	2021-05-19 11:52:09	
	5	检测到勘索病毒通信	副素病毒	[规则2019-003]勘索病毒	10.50.2.164 【攻击者】	137.74.46.45【被攻击者】	2021-05-19 11:52:06	
	6	检测到勒索病毒通信	面素病毒	[规则2019-003]勘素病毒	10.50.2.164【攻击者】	91.234.32.19【被攻击者】	2021-05-19 11:52:04	
	7	检测到勘索病毒通信	面素病毒	[规则2019-003]勘素病毒	10.50.2.164【攻击者】	195.123.209.123【被攻击者】	2021-05-19 11:52:00	
						共70417条 上一页 1 2	3 4 5 下一页 10 条/页~	

选择告警产生趋势报表



选择告警 TOP10 排行报表



选择日志协议统计报表

📕 统计报表类型	时间范围	■: 近7天 ~			
◇ ➢ 资产报表 》(资产分布统计)	日母生	lord 0 下戰历史			
✓ ▷ 告告授表 √ 告告公本法社	📕 协议	Top10的统计			
2. 音響产生趨勢	3000				
※ 告審Top10排行	2500				
○ □ ○ □ ○ □ ○ □ ○ □ ○ □ ○ □ ○ □ ○ □ ○ □	2000				
2、日志英型统计报表	1500				
(□□□波羅東源院计报表) (2) 日志等级统计报表	1000				
2 日志发生总数统计报表	500				
> 日志友生和賞焼计授表 → ○ 事件続け招表	0				
☆ 审计事件分布统计				tcp	
○(軍计學件严生趋势统计 ○(关联要件分布统计)	📕 日志	列表			
10、关联事件产生编号统计	序号	日志名称	协议		发生时间
	1	恶意程序	tcp		2021-05-14 14:59:34
	2	恶意程序	tcp		2021-05-14 14:59:34
	3	恶意程序	tcp		2021-05-14 14:59:34
	4	恶意程序	tcp		2021-05-14 14:59:34
	5	恶意程序	tcp		2021-05-14 14:59:34
	6	恶意程序	tcp		2021-05-14 14:59:34
	7	恶意程序	tcp		2021-05-14 14:59:34
				Д	2505条 上一页 1 2 3 4 5 下一页 10象页~

选择日志类型统计报表



选择日志设备来源统计报表



选择日志等级统计报表

📕 統计报表类型	时间范围	副: 近7天 ~				
> 逆 逆序接表 ○(资产分布统计)	⊖ 导出W	ford O 下载历史				
> 告 告 告 任 使 表	📕 事件	等级统计				
○ 告望产生趋势	3000					
 一 日本統计报表 	2500					
 () 日志协议施计报表 () 日志樊型施计报表 	2000					
☆ 日志设备未源统计报表	1500					
 (人) 日本没生き数统计报表 (人) 日本发生き数统计报表 	500					
 二、「日志发生類度統计报表 > 一 事件統计报表 	0					
○ 审计事件分布统计 ○ 常计事件充在统计				严重		
20、第11年(F) 王編時代11 20、关联事件分布统计	📕 日志	列表				
)() 关联事件产生趋势统计	序号	日志名称	设备类型	日志等级	日志分类	发生时间
	1	恶意程序	微步在线威胁检测平台	严重	恶意程序	2021-05-14 14:59:34
	2	恶意程序	微步在线威胁检测平台	戸室	恶意程序	2021-05-14 14:59:34
	3	恶意程序	微步在线威胁检测平台	戸重	恶意程序	2021-05-14 14:59:34
	4	恶意程序	微步在线威胁检测平台	戸里	恶意程序	2021-05-14 14:59:34
	5	恶意程序	微步在线威胁检测平台	戸里	恶意程序	2021-05-14 14:59:34
	6	恶意程序	微步在线威胁检测平台	≂≘	恶意程序	2021-05-14 14:59:34
	7	恶意程序	微步在线威胁检测平台	≓≘	恶意程序	2021-05-14 14:59:34
					共 2505 魚 上一页 1	2 3 4 5 下一页 10条/页~

选择日志发生总数统计报表



选择日志发生频度统计报表

	비민오페	; 近7天 ~					
Ri+	G 导出Wa	rd 🕑 下载历史					
=;+	📕 日志義	收量趋势					
9.99	1件/杉						
D排印行 1	0.8時/杉						
先计报表 允计报表	0.6件/杉						
N.源统计报表 会计探查	0.4件/杉						
自数统计报表	0.2件/杉						
國際計畫表							
	이야/杉	2021-05-12	2021-05-14	2021-05-15	2021-05-16	2021-05-17	2021-05-19 2021-05-19
;)布统计 生趋势统计	0件/杉	2021-05-13	2021-05-14	2021-05-15	2021-05-16	2021-05-17	2021-05-18 2021-05-19
0-布统计 =生趋势统计 0-布统计	0件/8	2021-05-13 列表	2021-05-14	2021-05-15	2021-05-16	2021-05-17	2021-05-18 2021-05-19
3) 市坑计 ■生越期统计 3) 市坑计 ■生越期统计	0件/8 日志3 度号	2021-05-13 刘表 日志名称	2021-05-14 设备类型	2021-05-15 日志等级	2021-05-16 日志分満	2021-05-17 1948	2021-05-18 2021-05-19 秋生时间
→ 方統计 → 生雄男统计 → 方統计 = 生雄男统计 = 生雄男统计	0件/8 目志3 爆号	2021-05-13 刘表 日志名称 示意继承	2021-05-14 设备类型 微步在线或款检测平台	2021-05-15 日志等级 严重	2021-05-16 日志分英 恶意提序	2021-05-17 194X tcp	2021-05-18 2021-05-19
→方统计 **生植期统计 分布统计 **生植期统计	0時/6 日志3 修号 1 2	2021-05-13 日志名作 示意程序 	2021-05-14 设备类型 限步在线或款检测平台 限步在线或款检测平台	2021-05-15 日志等级 戸重 戸重	2021-05-16 日都分異 思察程序 思察程序	2021-05-17 1940 tcp tcp	2021-05-18 2021-05-19 ※生動詞 2021-05-14 1459-34 2021-05-14 1459-34
→布统计 ==生编码统计 →布统计 ==生编码统计	014/6 日志3 度号 1 2 3	2021-05-13 利表 日本名称 市家程序 市家程序 市家程序	2021-05-14 设备类型 物炉在线或物检测平台 物炉在线或物检测平台 物炉在线或物检测平台	2021-05-15 日志等级 戸室 戸室 戸室	2021-05-16 日本分支 思想後本 思想後本 思想後来	2021-05-17 10% tcp tcp tcp	2021-05-18 2021-05-19 X12800 2021-05-14145924 2021-05-14145924 2021-05-14145924 2021-05-14145924
內病決计 ≝生越影响计 } 今年成計 ≝生越影响计	0時/6 日志3 度号 1 2 3 4	2021-05-13 山表 日本名称 市泰理学 市泰理学 市泰理学 市泰理学	2021-05-14 (26集実型 (初步在成成制地制平台 (初步在成成制地制平台 (初步在成成制地制平台 (初步在成成制地制平台	2021-05-15 H&#@ FE FE FE FE</td><td>2021-05-16 日都分員 思想短年 回意短年 思想短年 思想短年</td><td>2021-05-17 1052 top top top top</td><td>2021-05-18 2021-05-19 X2150 2021-05-14145934 2021-05-14145934 2021-05-14145934 2021-05-14145934</td></tr><tr><td>(內病)计 "生越暴除计) 今流计 "生越弱统计</td><td>0時#6 日志3 修9 1 2 3 4 5</td><td>2021-05-13 山表 日本名称 市泰理学 市泰理学 市泰理学 市泰理学 市泰理学 市泰理学</td><td>2021-05-14 収集工程 取歩石減低加快加平台 取歩石減低加快加平台 取歩石減低加快加平台 取歩石減低加快加平台 取歩石減低加快加平台 取歩石減低加快加平台</td><td>2021-05-15 E&#@ FE FE FE FE</td><td>2021-05-16 日本分支 初生の生年 初生の生年 初生の生年 初生の生年 初生の生年 初生の生年 の生ま の生ま の生ま の生ま の生ま の生ま の生ま の生ま</td><td>2021-05-17 18942 top top top top</td><td>2021-05-18 2021-05-19 X2150 2021-05-14145934 2021-05-14145934 2021-05-14145934 2021-05-14145934 2021-05-14145934</td></tr><tr><td>3市總计 "生越聚統计 3市統计 "生趣弱统计</td><td>0時/€ ■ 日志3 18号 1 2 3 4 5 6</td><td>2021-05-13 利表 日本名称 古聖理年 古聖理年 古聖理年 古聖理年 古聖理年 古聖理年 古聖理年 古聖理年</td><td>2021-05-14 取参互援 取参互援援助社会平台 取参互援援助社会平台 取参互援援助社会平台 取参互援援助社会平台 取参互援援助社会平台 取参互援援助社会平台 取参互援援助社会平台</td><td>2021-05-15 E4&#e8 7%2 7%2 7%2 7%2 7%2 7%2 7%2 7%2</td><td>2021-05-16 日本分支 初始後年 初始後年 初始後年 初始後年 初始後年 初始後年 初後後年</td><td>2021-05-17 18942 top top top top top</td><td>2021-05-18 205 205 205 205 205 205 205 205 205 205</td></tr><tr><td>3年就倒开 雪生越最快计 一雪生越最快计 "生越最好统计</td><td>0年/6 ■ 日志3 月 月 日志3 月 日 志 3 1 2 3 4 5 6 7</td><td>2021-05-13 学校 日本本作 学校培祥 学校培祥 学校培祥 学校培祥 学校培祥 学校培祥 学校培祥 学校培祥 学校培祥 学校培祥 学校培祥 学校培祥 学校培祥 学校 学校 学校 学校 学校 学校 学校 学校 学校 学校</td><td>2021-05-14 记載美型 他步行线域的性质平台 他步行线域的性质平台 他步行线域的性质平台 他步行线域的性质平台 他步行线域的性质平台 他步行线域的性质平台 他步行线域的性质平台 他步行线域的性质平台</td><td>2021-05-15 H&#@ 77章 77章 77章 77章 77章 77章</td><td>2021-05-16 日本分支 三部協定 三部協定 三部協定 三部協定 三部協定 三部協定 三部協定 三部協定</td><td>2021-05-17 8092 top top top top top</td><td>2021-05-18 2021-05-18</td></tr></tbody></table>			

选择审计事件分布统计报表



选择审计事件产生趋势统计报表



选择关联事件分布统计报表

■ 统计报表类型	时间范围	图: 近7天	~					
◇ ▷ 资产报表 >> 资产分布统计	⊖ 导出W	ord 🛛 💿 下動历史						
◇ ▶ 告誓报表 >> 告誓分布统计	📕 事件	分类Top10的关助	等件统计					
☆ 音響产生趋势	7W							
○ 音響Top10期行 > □ 日志統计报表	6W							
2、日志协议统计报表	5W							
以1日志英型统计报表 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	4W							
>< 日志等级统计报表	2W							
(1) 日志发生总数统计报表 (2) 日志发生频度统计报表	1W							
◇ 🖻 事件统计报表	0				44-20 Minutes	ensi n		
○(単计事件分布统计)>(审计事件产生趋势统计					2008090	3/1+		
14、关联事件分布统计	📕 事件	列表						
[2] 天获學件严生趋务统计	序号	事件名称	事件分类	触发规则名称	等级	源IP	目的IP	发生时间
	1	勤素软件	发现勤素软件	检测到勘索病毒通信	严重	10.50.2.164	91.234.32.19	2021-05-19 11:57:04
	2	勤素软件	发现勤素软件	检测到勘索病毒通信	严重	10.50.2.164	195.123.209.123	2021-05-19 11:57:00
	3	勘索软件	发现勘察软件	检测到勘索病毒通信	严重	10.50.2.164	137.74.46.46	2021-05-19 11:56:59
	4	勘索软件	发现勘索软件	检测到勘索病毒通信	严重	10.50.2.164	91.234.32.19	2021-05-19 11:56:57
	5	勘索软件	发现勘索软件	检测到勘索病毒通信	严重	10.50.2.164	137.74.46.46	2021-05-19 11:56:54
	6	勘索软件	发现勘索软件	检测到勘索病毒通信	严重	10.50.2.164	91.234.32.19	2021-05-19 11:56:52
	7	勘索软件	发现勘察软件	检测到勘察病毒通信	严重	10.50.2.164	195.123.209.123	2021-05-19 11:56:48
							共65017条 上一页 1 2	3 4 5 下一页 10 祭/页~

选择关联事件产生趋势统计报表

長 类型	时间范围	園: 近7天 ~						
	□ 尋出₩	Vord ④ 下载历史						
表	▼ 关联	事件趋势						
2) (音響学会場合) 2) 音響学会場例 2) 音響での2018行 日志続计报表 2) 日本的次期计报表 2) 日本党単連続计报表 2) 日本党単来源地计报表	4W 3W 2W							\frown
8年10月1日表表 吉发生总数统计报表 吉发生须度统计报表	1W							
● 事件统计报表								
1计报表 计事件分布统计	0	2021-05-13	2021-05-14	2021-05-15	2021-0	5-16	2021-05-17	2021-05-18 2021-05-19
は1投表 計事件分布統計 計事件产生趋野统计 誤事件分布统计	◎	2021-05-13 列表	2021-05-14	2021-05-15	2021-0	5-16	2021-05-17	2021-05-18 2021-05-19
57股票 计事件分布统计 计事件产生趋弱统计 联事件分布统计 联事件产生趋势统计	0 一 第件 康号	2021-05-13 列表 爭件名称	2021-05-14	2021-05-15 触双规则名称	2021-0: 等级	5-16 渡1P	2021-05-17 E@9IP	2021-05-18 2021-05-19 双生时间
121按赛 计事件分布统计 计事件产生趋势统计 联事件产生趋势统计	0 第一集日 月 1	2021-05-13 列表 事件名称 敬赏软件	2021-05-14 學件分类 发现勘索软件	2021-05-15 触发规划名称 检测到勒索病毒通信	2021-0: 等级 严重	5-16 源IP 10.50.2.164	2021-05-17 E891P 195.123.201	2021-05-18 2021-05-19 現生時间 9.123 2021-05-19 13:44:48
131按聚 计事件分布统计 计事件分布统计 教事件分布统计 数事件分布统计 影事件分布统计	□ ■ 事件 度号 1 2	2021-05-13 列表 學件名称 副素软件 副素软件	2021-05-14 學件分異 发玩勘索软件 发玩勘索软件	2021-05-15 純炭規則名称 检測形取素病毒運業 检測形取素病毒運業	2021-0: 等级 严重 严重	5-16 JØIP 10.50.2.164 10.50.2.164	2021-05-17 Ild01P 195.123.201 137.74.46.4	2021-05-18 2021-05-19 天生時 8.123 2021-05-19 13.44.48 6 2021-05-19 13.44.47
1911股票 科學為分布統计 计學與不生態發統计 製墨作分布統计 製墨作产生態節统计	0 第一年 1 2 3	2021-05-13 列表 争件名称 取素软件 和素软件 和素软件	2021-05-14 學特分異 发現勘索软件 发現勘索软件 发現勘索软件	2021-05-15 触发规则和作 检刑列取素病毒通信 检刑列取素病毒通信 检刑列取素病毒通信	2021-0: *** *** *** ***	5-16 JBUP 10.50.2.164 10.50.2.164 10.50.2.164	2021-05-17 EM91P 195123.20 137.74.46.4 91.234.32.1	2021-05-18 2021-05-19 ಸ±ಕಾಗಿ
1911股票 科學為方面與十 计學與不主意的统计 製墨作分布開始 設圖作产生態的统计	○ ■ 事件 度号 1 2 3 4	2021-05-13 列表 学件名称 私素软件 私素软件 私素软件 和素软件	2021-05-14 學村分页 型玩取素似件 型玩取素似件 型玩取素似件 型玩取素似件 型玩取素似件	2021-05-15 触发现到私你 检测到和素肉毒通信 检测到和素肉毒通信 检测到和素肉毒通信 检测到和素肉毒通信	2021-0 940 75 75 75 75	5-16 3831P 10.50.2.164 10.50.2.164 10.50.2.164 10.50.2.164	2021-05-17 III01P 195.123.20 137.74.64 91.234.32.1 137.74.64	2021-05-18 2021-05-19 ж±ня
17世族第 计学校第一世纪的社会	○ ■ 事件 序号 1 2 3 4 5	2021-05-13 列表 学件名称 和素软件 和素软件 和素软件 和素软件 和素软件 和素软件 和素软件	2021-05-14 學村分異 发現影素软件 发現影素软件 发現影素软件 发現影素软件 发現影素软件 发現影素软件 发現影素软件	2021-05-15 熱双短別名印 也向乐政策病毒運復 也向乐政策病毒運復 也向乐政策病毒運復 也向乐政策病毒運復 也向乐政策病毒運復	2021-0 等校 产室 产室 产室 产室 产室 产 室	10502.164 10502.164 10502.164 10502.164 10502.164	2021-05-17 H80JP 195.123.20 137.74.64 9.1234.32.1 137.74.64 9.1234.32.1	2021-05-18 2021-05-19 ж±ны
17世族第 17世紀年 11世紀年 11世紀年 11世紀年 11世紀年 11世紀 11世紀 11	0 第一事件 月 2 3 4 5 6	2021-05-13 列表 学校名称 影素软件 影素软件 影素软件 影素软件 影素软件 影素软件 影素软件 影素软件	2021-05-14 學性分支 型玩動素助件 型玩動素助件 型玩動素助件 型玩動素助件 型玩動素助件 型玩動素助件 型玩動素助件	2021-05-15 熱双短刻名印 社の形況素病毒運業 社の形況素病毒運業	2021-01 %00 72 72 72 72 72 72 72 72 72	75:16 78:19 10:50.2.164 10:50.2.164 10:50.2.164 10:50.2.164 10:50.2.164 10:50.2.164 10:50.2.164 10:50.2.164 10:50.2.164	2021-05-17 HóiP 195.123.20 137.74.64 9.1234.321 137.74.64 9.1234.321 137.74.64 137.74	2021-05-18 2021-05-19 ೫1230 2021-05-19 13:444 6 2021-05-19 13:444 9 2021-05-19 13:444 9 2021-05-19 13:444 9 2021-05-19 13:444 9 2021-05-19 13:444 9 2021-05-19 13:444 9 2021-05-19 13:444

点击【导出 excel】,可导出列表内容。 点击【下载历史】,进入历史下载页面。

2.6 策略管理

2.6.1 关联分析规则

路径:策略管理->关联分析规则。

规则编号: 规则名称: 告容关别:	:		告警等级:			查询 主臣
 ● 新増 ◎ 抗風制除 ▲ 抗風回用 ○ ま 	山島開用 G 批量导出 G 全部导出 9 批量导入 0 子柳刻					规则类型: ★ 内置
序号 规则编号	规则名称	告誓等级	风险阶段	状态	创建时间	操作
1 * HD-SOC-COR-00096	SQL报楷慎意泄漏	陶仓	存在漏洞	启用	2021-03-31 11:05:10	R 🛛 🗰 🛇
2 * HD-SOC-COR-00095	teamviewer	信息	被收集信息	启用	2021-03-31 11:05:10	R 🛛 🗰 🛇
3 * HD-SOC-COR-00094	[规则2019-070]输出敏感信息	中危	被收集信息	启用	2021-03-12 17:11:30	R 🛛 🗰 🛇
4 * HD-SOC-COR-00093	[規則]2019-069]vpn傳展問題選	严重	被入侵 (失陷)	启用	2021-03-12 17:11:30	R 🛛 🗰 🛇
5 * HD-SOC-COR-00092	[规则2019-035]存在JBoss反序列化漏间,JBossMQ但件成功访问	严重	存在局洞	启用	2021-03-12 17:11:30	R 🛛 🗰 🛇
6 * HD-SOC-COR-00091	(規則2019-034)經僅炸導攻击·經僅接口溢用	中危	被攻击 (不确定)	启用	2021-03-12 17:11:30	R 🛛 🗰 🛇
7 * HD-SOC-COR-00090	[规则2019-068]Web编编器流示布上传媒作	高危	被攻击 (不确定)	启用	2021-03-12 17:11:30	R 🛛 🗰 🛇
8 * HD-SOC-COR-00089	(規则2019-033]PHPCMS2008代码注入漏商攻击(CVE-2018-19127)	中危	被攻击 (不确定)	启用	2021-03-12 17:11:30	R 🛛 🗰 🛇
9 * HD-SOC-COR-00088	(规则2019-032]Apache Spark RPC协议Java反序列化雇用攻击(CVE-2018-17190)	中危	被攻击 (不确定)	启用	2021-03-12 17:11:30	R 🛛 🗰 🛇
10 * HD-SOC-COR-00087	[規則2019-067]並弱接口ap:電缆開筆调用	中急	被攻击(成功)	启用	2021-03-12 17:11:30	R 🛛 🗰 🛇
		共143	\$ <u>1</u> 2 3	4 5	15下一页10 銀河	t∨ 918 1 7 8 2

点击【新增】,进入新增规则页面



填写相关信息,点击提交,新增规则完成。 左边勾选框勾选多项,点击【批量删除】,可以批量删除选中规则。 左边勾选框勾选多项,点击【批量启用】,可以批量启用选中规则。 左边勾选框勾选多项,点击【批量禁用】,可以批量禁用选中规则。 左边勾选框勾选多项,点击【批量导出】,可以批量导出选中规则。 点击【全部导出】,可以导出全部规则。 点击【批量导入】,可导入规则。 点击"子规则",进入子规则页面

子规则名称:	创建时间:			查询 里蓋					
①新增 前 批量制除) 新藩 🔋 記彙部分								
座号 子规则名称	7	使用次数	创建时间	操作					
1 SMB ipcont	fig命令执行响应	3	2021-03-12 16:41:26	民 🖉 💼					
2 wmic运程设	約回	3	2021-03-12 16:41:26	🗟 🗹 🏛					
3 尝试读取pa	asswd文件	3	2021-03-12 16:41:26	1997年1997年1997年1997年1997年1997年1997年1997					
4 Apache Dru	uid远程代码执行攻击	3	2021-03-12 16:41:26	8 2 章					
5 GitLab任意	这件读 取	3	2021-03-12 16:41:26	8 2 1					
6 Apache sky	walking這程代码执行攻击	3	2021-03-12 16:41:26	8 2 1					
7 VMware vC	Center Server远程代码执行篇词攻击	3	2021-03-12 16:41:26	民 🖉 🏛					
8 Laravel远将	紀码执行攻击	3	2021-03-12 16:41:26	R 🛙 🛍					
9 JIRA服务器	機板注入漏洞攻击	3	2021-03-12 16:41:26	R 🗷 🛍					
10 Confluence	任意文件读取	3	2021-03-12 16:41:26	民 🖉 🛍					

点击操作中的【查看】,可查看规则。 点击操作中的【编辑】,可进行编辑。 点击操作中的【删除】,可删除规则。 点击操作中的【禁用】,禁用规则。 点击操作中的【启用】,启用规则。

2.6.2 统计分析规则

路径:策略管理->统计分析规则。

用户指南

规则名称:	规则分类: 全部	◇ 等級: 全部 ◇	规则状态: 全部 🗸			查询 重量			
⊕新選 0 批	© ## 0 R###								
序号	规则名称	规则分类	等级	监控频率	规则状态	操作			
1	多个目标系统遭受暴力破解攻击	字段统计	中危	5分	已启用	🔒 🖪 🖬 🖬			
2	实验区FW没有数据产生	日志统计	信息	5分	已禁用	🙃 🖪 🖉 🗰			
3	疑似病毒感染主机较多	字段统计	高危	5分	已启用	🔒 🖪 🖬 🗰			
4	高危事件数量异常大	日志统计	高危	10分	已启用	🔁 🖪 🖉 🛍			

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。

点击【新增】,进入添加规则页面

⑦ 新増 0 批量制除					
序号 规则名称	規则分类	等级	蓋控頻率	规则状态	操作
	添加规则			×	
	*规则名称:				
	*等级: 严重		~		
	*监控频率:		v		
	*已存搜索: 激试天下		v		
	搜索内容: 与关键	2:应用检测 或 敏感 🛛 与 事件等级:严重 或 高危 或 中危			
	*规则分类:日志统计		~		
	*条件:	分 ∨ 之内计数 = ∨ 数字			
		提交 关闭			

填写相关信息,点击【提交】,添加统计分析规则完成。 左边勾选框勾选多项,点击【批量删除】,可以批量删除规则。 点击操作中的【查看】,进入查看规则页面。 点击操作中的【编辑】,进入编辑页面。 点击操作中的【禁用】,禁用规则。 点击操作中的【启用】,启用规则。 点击操作中的【删除】,删除规则。

2.6.3 审计分析规则

路径:策略管理->审计分析规则。

规则名称: 处理顺序	:: 处理方式: 全部 状态: 全部	 创建时间: 				~	29 X2	
④新増 1 1 批量粉除 1 量 批量応用 1 〇	新達 ◎ 批量物料 ▲ 批量用用 ◎ 批量時月 ◎ 批量時日 ◎ 推量時日 ◎ 推動時日 ◎ 推動							
序号 规则编号	规则名称	处理顺序 ⇔	处理方式	状态	创建时间	更新时间	2 操作	
41 SJFXGZ-20210413-30422	审计有效时间段的告答-不属于	41	继续处理其它规则	兼用	2021-04-13 15:32:26	2021-04-13 15:45:52	R 🛛 🗰 🔒	
* 42 SJFXGZ-20210413-10083	审计有效时间段的告望,属于每日	42	继续处理其它规则	業用	2021-04-13 15:38:53	2021-04-13 16:52:46	R 🗹 🗊 🔒	
* 43 SJFXGZ-20210413-04238	审计有效时间段的告誓-不雇于每日	43	继续处理其它规则	熱用	2021-04-13 15:39:58	2021-04-13 17:06:12	R 🗹 🗊 🔒	
* 44 SJFXGZ-20210413-59566	审计有效时间段的告告-属于每星期	44	继续处理其它规则	新用	2021-04-13 15:41:06	2021-04-13 17:10:07	R 🗹 🏛 🔒	
▲ 45 SJFXGZ-20210413-16579	审计有效时间段的告望-不懂于每星期	45	继续处理其它规则	蘇用	2021-04-13 15:41:46	2021-04-13 17:10:50	R 🗹 💼 🔒	

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。

点击【新增】,进入新增规则页面

规则编号: SJF	XGZ-20210519-11038	"规则名称:	
*过滤内容: 🔒	<mark>育计目标</mark> 审计行为 审计行为执行者 审计行为来源	审计有效时间段 其它条件	
	● 属于 ○ 不属于		
	新增 审计目标类型	*审计目标值	
	謝除 请选择审计目标类型	v [
合并条件: 1~{	86400 秒内发生 1 次		
响应方式: 🗸	产生告惑		
*	*告警标题:		
	*告警等级:	✓ *告警关別: 请选择告警类型	~
	风险阶段:无	✓ 告答源: 源 P	~
	告警显示: 插入标签		
	原理:		

した 現交 美術 大術

填写相关信息,点击提交,新增规则完成。 左边勾选框勾选多项,点击【批量删除】,可以批量删除选中规则。 左边勾选框勾选多项,点击【批量启用】,可以批量启用选中规则。 左边勾选框勾选多项,点击【批量禁用】,可以批量禁用选中规则。 左边勾选框勾选多项,点击【批量导出】,可以批量导出选中规则。 点击【批量导入】,可导入规则。 点击【调整规则处理顺序】,进入调整规则处理顺序页面

┏ 上移至顶	20184 ◆ 2018年 ◆ 2018年 ◆ 2018年 ◆ 2018年 ◆ 2018年 ◆ 2018年 ◆ 2018年 ◆							
17	SJFXGZ-20210331-83076	设备关型不属于	17					
18	SJFXGZ-20210331-36075	审计行为的告誓-不履于	18					
19	SJFXGZ-20210331-22742	ip地址的告答·属于	19					
20	SJFXGZ-20210331-60379	审计行为执行者的告誓-不属于	20					

点击操作中的【查看】,可查看规则。 点击操作中的【编辑】,可进行编辑。 点击操作中的【删除】,可删除规则。 点击操作中的【禁用】,禁用规则。 点击操作中的【启用】,启用规则。

2.6.4 基线分析规则

路径:策略管理->基线分析规则。

用户指南

规则名	称:	规则描述:	状态: 全部 ジ 創建时	(#]:	更新时间:				查询 重查
⊕ 新増	0 #5	副除 🔒 批量向用 🚫 批	金禁用 📔						规则类型: ★ 内置
	序号	规则编号	规则名称	规则描述		状态	创建时间	更新时间	操作
	11	JXFXGZ-20210414-58705	发送流量(自定义)			启用	2021-04-14 17:47:38	2021-04-14 17:47:38	R 🗹 🗊 🛇
	12	JXFXGZ-20210414-74813	发送流量(周)			启用	2021-04-14 17:46:33	2021-04-14 17:46:33	R 🗹 🗊 🛇
	13	JXFXGZ-20210414-26035	发送流量(禁用)			禁用	2021-04-14 17:45:48	2021-04-14 17:45:48	R 🗹 💼 🔒
	* 14	JXFXGZ-20210414-76000	发送汽量			启用	2021-04-14 17:44:17	2021-04-28 11:28:54	R 🗹 🛍 🛇
	* 15	JXFXGZ-20210414-24708	漆拂口-接收流量	规则描述1		启用	2021-04-14 17:41:35	2021-05-14 14:58:57	R 🗹 💼 🛇
	* 16	JXFXGZ-20210414-42657	目的端口-总流量	描述1		启用	2021-04-14 17:39:03	2021-04-28 11:28:54	R 🗹 💼 🛇
	17	JXFXGZ-20210413-56571	基纯分析规则-自定义			启用	2021-04-13 17:49:30	2021-04-13 17:49:30	R 🗹 🗰 🛇
	* 18	JXFXGZ-20210413-56731	基线分析规则-总流量(禁用)			新用	2021-04-13 17:47:41	2021-04-28 11:28:54	R 🗹 💼 🔒

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。

点击【新增】,进入新增规则页面

规则编号: JXFXGZ-20210519-	-86607		规则名称:		
*过滤内容: 新造 删除 &	逻辑关系 & ✓ 谓选择条件	*条件	*运算符 ~	"条件值	
*基线分析方式: "统计方式: (●移动平均 ●移动方差	"复线关	型:●日 ○周		
*统计字段:	4		+: 1~99		~ ~
*等级: 严重		~			
响应方式: 🔽 产生告警					
*告警标题:					
*告警等级:	严重	*告愁迷!	The second second second second		
			10. 诸达综合管架型		~
风脸阶段: 告馨显示:	无		版: 通P		~
风险阶段:	え	日 「	99 - 199129年1日第二日 第: 1991日		~
风险阶段: 告誓显示:	无		가 · (1982년)(中古왕英亚) (1997년 - 1998년) (1997년 - 1998년 br>(1998년 - 1998년 br>(1998년 - 1998년 br>(1998년 - 1998년 -		~

填写相关信息,点击提交,新增规则完成。 左边勾选框勾选多项,点击【批量删除】,可以批量删除选中规则。 左边勾选框勾选多项,点击【批量启用】,可以批量启用选中规则。 左边勾选框勾选多项,点击【批量禁用】,可以批量禁用选中规则。 左边勾选框勾选多项,点击【批量导出】,可以批量导出选中规则。 点击【批量导入】,可导入规则。 点击操作中的【查看】,可查看规则。 点击操作中的【编辑】,可进行编辑。 点击操作中的【删除】,可删除规则。 点击操作中的【禁用】,禁用规则。 点击操作中的【启用】,启用规则。

2.6.5 预处理规则

路径:策略管理->预处理规则。

见则名	称:	规则状态:全部 ~				<u>0</u> .0 = = =
新潮	0	北星影响 🛛 🕞 导出 🚽 🙃 沈星导入				
	序号	规则名称	设备类型	规则内容	规则状态	操作
	1	http-2xx-危险的请求方法	任意设备	秋态码_在Http状态码2xx	BER	
	2	无效的JSP请求	任意设备	http站站_规则表达式\(jspijspx)action(do)\b	日月月	
	3	无效的PHP请求	任意设备	目的IP: 读口的tage,规则表达式:^((?lphp).)+\$	已启用	<u>⊗ R Z â</u>
	4	可信任城名的事件	任意设备	目的主机名_在可信任域名	巴思明	<u>⊗</u> R 2 0
	5	无效的ASP请求	任意设备	目的IP:读口的tiags,规则表达式^((?!asp).)+\$	BRR	<u>⊚ R. Ø â</u>
	6	php話感收到无效请求	任意设备	谭主机名_在php网站主机名	BAR	⊗ R. Ø m
	7	java站原收到无效请求	任意设备	目的主机名_在java同站主机名	Ball	<u> </u>
	8	aspinet站点权到无效请求	任意设备	目的主机名_在isp.net网站主机名	BER	
	9	容易决报SQLI主入的web静态文件访问	屋盾入侵险到系统	「http站站上规则表达式^((?\\/).)-_(js]cssjjpg]gif]png bmp ico)\$	已無用	© <u>8</u> ₫ 1
	10	容易浸报的Webshell响应-加密型	黑盾入侵检测系统	规则名称_包含webshell请求返回	已启用	8 B 3 8
	11	周城网发起的拒绝服务攻击	任意设备	事件分娩。等于拒绝服务攻击、网络层拒绝服务攻击、网络层拒绝服务攻击	Ban	<u>0 R 2 a</u>
	12	容易洪报的阿盘文件传输	任意设备	秋志硕_等于206 http头_包含:User-Agent: netdisk	BER	<u>⊗ R</u> ⊠ ≜
	13	容易进程的规则文件传输	任意设备	源IP_在·尾域网IP段	Ban	© R. 23 ∰

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。

点击【新增】,进入新增页面

策略管理>预处	遭规则		•
规则名称:	规则状态:全部		28 SE
⊕ #ræ 1	1 批量制除 〇 専出 〇 社量导入		
 	9 1991247	新增	× 操作
1	http-2ox-危险的清灾方法	*规则名称:	
2	无效的JSP请求	设备类型:	○ ○ ○ 前
3	无效的PHP请求	*规则内容: 必须有一个	<u> </u>
4	可信任城名的事件	新彊 我则学段 操作符 "内客 ◎	
5	无效的ASP要求	*規則結果: 法部金确定 → 等于 組入1-10回放	
6	php站点也到无效遵求	*优先级别: 0 載雨 物法	0 R 🗈 🛍
7	java站原收到无效需求		0 R 12 8
8	aspinetia总收到无效请求		
9	容易课报SQU注入的web静态文件访问		©≅⊠ a
10	容易进程的Webshell同应-如密型		
🗌 11	局域则发起的拒绝服务攻击		
12	容易浸服的同盘文件传输	長 次 美田	
13	容易误报的规则文件传输	任意设备 源印_正月城间印段	Ce# 0 & 0

填写相关信息,点击【提交】,添加预处理规则完成。 左边勾选框勾选多项,点击【批量删除】,可以批量删除规则。 点击【批量导入】,进入批量导入页面

总范 预处	上理规则 ×				
事件感知>预	处理规则				● ≈#
规则名称	规则状态: 全部				**
④ 新端	◎ 批量粉除 □ 寻出 - 3 批量导入				
	序号 规则名称	批星导入		×	201
	1 興試1217/1	*导入文件:			0 🛛 🗰
	2 http-500				o R 🗷 🛍
	3 test_in				⊗ &⊠ ≣
	4 test_ip===				0 2 3
	5 test_预处理优先级1				⊘ ि 🖉 🏛
	6 test预处理优先级——正则表达式				
	7 test1				⊘ ि 🖉 🛍
	8 预处理优先测试3				0 8 0
	9 预处理优先级测试2				⊘ ि⊠ ∎
	10 预处理优先级测试1				0 2 2
	11 准确的APT事件-066				0 🖪 🗹 🏛
	12 非php网站收到php相关请求				0 🖪 🗹 🛍
	13 Webshell的问得到正常响应	主机服务器	●件名称_等于webshell后门木马	状态码_在:Http状态码4xx 已启用	⊗ 🗟 🖉 👼
				共13条	

点击【导出】,可以导出规则。 点击操作中的【查看】,进入查看规则页面。 点击操作中的【编辑】进入编辑页面。 点击操作中的【禁用】,禁用规则。 点击操作中的【启用】,启用规则。 点击操作中的【剧除】,删除规则。

2.6.6 规则字典

路径:策略管理->规则字典。

・ 協 定 Q	字曲名称:	
所有字典(54)	规则类型:	
Webshell尝试访问-字典	条注 ·	
HTTP代理隧道请求-字典	m/± .	
Webshell访问成功-字典		
xstream反序列化攻击-字典		
Ripple20-Treck-TCP-IP漏洞攻		
F5设备漏洞攻击-NIDS		
Apache Dubbo Provider RCE	规则值:	
docker未授权访问-字典		
asp.net网站主机名		
java网站主机名		
php网站主机名		
一网络多播地址段		
一可信任城名		
设备类型字典-Windows		
工作时间段		
一访问控制-可信源IP		
访问控制-保护目标IP		
一僵尸网络通信-字典		
一抱矿程序外联-字典		
—Java反序列化攻击-字典		
永恒之蓝(MS17-010)攻击字典		
规则2019-043字典-WebShell		
sql注入攻击-2019002		
— Apache Struts2 RCE漏洞利用		
SQL注入明应-字典		
teamviewer		
一隐蔽隧道		
Http状态码3xx		
Http状态码2xx		
常规HTTP请求方法		
危险的HTTP请求方法		

鼠标移至"所有字典",出现【新增】,点击【新增】进入新增字典页面

策略管理>规则字典		Θ
■ 字典列表	J 字典评情	
(字典服素 Q) ◇ 所有字典[54]	影増字典	
	*字典名称:	
	872 75042 809	
· (2音樂)(東非, Windows - 工作时间段 - (3) 问注制, 可慎潔)(P - (3) 问注制, 保申問知) - 信利何違意意, 字典 - 把好程序列数, 字典	(我時:和川國力活動推动,所一種力活動,如1-200,且為一G的意大子和一位的	
tearnviewer 時期建選 Http:状态時3xx	82 300	

填写相关信息,点击【提交】,添加字典完成。 点击【编辑】,进入编辑页面。 点击字典名称,右边显示字典信息。 点击【删除】,删除字典。

2.6.7 归并规则

路径:策略管理->归并规则。

策略管理>归并规则								❷刷新
規则各称:	级:全部	~					29 I	R
 新增 10 我最新除 								
序号 规则名称 归井时	间(秒)	归并字段	归并处理	4 4	件设置	规则状态 非	RHF	
1 (BistHORM) 60		事件名称	保留	第	-8		0 🗹 🗊	
通过持定担关本海夕供	上十	【本海】	山垣相子。	本海星		土『舌』	翌日	太

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。 点去【新始】 进入新始页页

点击【新增】,进入新增页面

体信息	"规则名称:						
日并条件							
	字段条件:	新増 字段名 ●		操作符		*内容 🕘	
	*字段选择:	至少选择一个					
			待选择归并字段	全选		已选择(0)	全选
		事件名称					
		资产IP					
		设备类型					
		源IP			→		
		目标IP			+		
		源海口					
		目示詞し					
		190961910					
		支持特征运动进行系统					
其他信息							
				<u>程</u> 交	关闭		
- 1	ム合百		। रेर भ		न जन 🗁 मे		
「与相っ	大信息,	息 击 【 损	〔父】,将	》加归开为	则元脉	0	
NI. L N	キャー	上夕西上		し町正7厶 ┓	- 미 - 비	,旦而四人,回回	

- 点击操作中的【禁用】,禁用规则。 点击操作中的【启用】,启用规则。
- 点击操作中的【删除】,删除规则。

2.6.8 过滤规则

路径:策略管理->过滤规则。

策略管理>过滹岘则					☑別新
规则名称:				查询	意识
 新増 10 批量影除 					
度号 规则名称	过滤条件		规则状态	操作	
1 大量误极的拒绝服务攻击	目的IP_每于:10.9.17.150		已启用	0 🗹 🗰	
圣计库宫护关本为女体		山田坦子本为仕田		壬四∎	*
迪 坦 填 与 相 大	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	出现相大宜闻结果;	息击【	里直】	,笡
询条件内容清空。					

点击【新增】,进入新增页面

用户指南

总览 归并规则 ×	过滤规则×				
新增过滤规则					×
📕 基本信息	*规则名称:				
📕 过滤条件	*文印各件 ·	至小进程——个			
	TRUCKIT .	±2/20# 1	10 a-se		
		+ 1 <u>9</u> 26∓ix ⊎	587147	NA U	
			提交关闭]	
그는 도구 그 ㅋ	ントウ	⊢⊥ ∎и∹		1 जन के	
項与相	大信总	,点击【提父	こ】,浴加过滤洌	则元成。	
左边勾	选框勾	洗多项, 点击	-【批量删除】.	可以批量删除	宛则 。
				4 2 . 4. C	/

点击操作中的【编辑】,进入编辑页面。 点击操作中的【禁用】,禁用规则。 点击操作中的【启用】,启用规则。 点击操作中的【删除】,删除规则。

2.6.9 分类规则

路径:策略管理->分类规则。

無略管理>分美规则							
■ 事件分类	📕 分类规则						
事件分类拨素	④ 新增				天皇	字換素	
◇ ▷ 所有分类	规则名称	所属分类	设备类型	规则表达式	优先级别	备注	操作
ヘ- ○ 网络安全事件 ヘ- ○ 数据安全事件	test_rulename应用检测_TeamViewer	Teamviewer外联票	黑腦入侵检測系统	-SC:(["rulename": "应用检测_TeamViewer))	5		R 🖸 🗴
	test-SC:((ORACLE数据库登结成功))	oracle数据库登录	黑腦入侵检測系统	-SC:((ORACLE数据库登结成))	4		R 🖉 🛛
	网页被理挖矿木马	挂马事件	黑盾入侵检测系统	[-N:41,-SC:((网页挖矿木马))]	3		R 🗷 🖬
ヘービー 可用性安全事件 ヘービー 昇常网络访问安全事件	oracle数据库登录成功	oracle数据库登录	黑盾入侵检测系统	-SC:((ORACLE数据库登陆成功))	3		R 🗷 🛛
 ヘービン 合規性事件 ヘービン 系統运行事件 	mysql数据库登录成功	mysql数据库登录	黑盾入侵检测系统	-SC:((MYSQL数据库登陆成功))	3		RØO
	FTP暴力破解	FTP账号暴力破解	黑腦入侵检測系统	(-N:10,-SC:((FTP Brute-Force)))	3		R 🗹 🛛
	sqimap注入	警试sqi注入	黑盾入侵防御系统	-SC:([: sqlmap.Scanner))	2		R 🖉 🛛
	AWVS扫描	web罵闹扫描	黑盾入侵防御系统	-SC:[[tools: Acunetix:Web:Vulnerability:Scanner]]	2		RØO
	任意文件上传	任意文件上侍	黑腦入侵防御系统	-SC:((Arbitrary.File.Upload))	2		RØO
	struts2远程代码执行	\$2远程代码执行	黑盾入侵防御系统	[-SC:((Apache:Struts)),-SC:((Code:Execution)))]	2		RØO
	访问控矿网页	潜在的危险遭讯	黑腦入侵检測系统	[-Ni41,-SCi[(coinhive.com))]	2	访问控矿网页,浏	R 🗹 🛛
	发现黑客工具	发现已知恶意文件	黑雪入侵检测系统	[-N:1066,-SC:(("300304")))] -SC:((-mimikatz))	2		R 🗹 🛛
	mssql数据库登录成功	mssql数据库登录	黑盾入侵检测系统	-RE:([SQL Server[\s\d]+?整违成功))	2		RØO
	黑产生利-增强	黑链/喷链	黑腦入侵检測系统	-SC:(("rulename": "讀報-)))	2	APT规则名称标识	R 2 0
	黑严牟利-抱矿	发现挖矿程序	黑腦入侵检測系统	-SC:[("rulename": "招致"-)))	2		R 🖸 🖬

鼠标移至菜单栏,出现【新增】、【编辑】、【删除】按钮,点击【新增】,跳 出事件分类添加弹框

焦略管理>分操规则								
■ 事件分类	■ 分类规则							
	• ##							
V D SEGS	规则名称		所謂分类	设备类型	规则表达式	伏先取到	61 <u>1</u>	1911
へ-〇 网络安全事件	test_rulename应用检测_Tex	amViewer	Teamviewer外訳事	黑眉入侵拉克系统	-SC(("rulename") "应用检测_TeamViewer)))	5		
へ 已 北海安全事件	test-SC:((ORACLE款編库登)	RE(SR35))	oracle数据库登录	黑盾入侵拉则系统	-SC:((ORACLE数据库登陆统))	4		RES
へ・10 内容安全争件 へ・10 主机安全事件	同页被挂挖矿木马		推动要件	菜酒入侵性肉系统	(I-NAL-SC-((同页把扩末马)))	3		RBO
ヘービラ 可用性安全事件 ヘービラ 昇常网络访问安全事件	oracle数据库整要成功		oracle数据库登录…	黑腦入侵检測系统	-SCi((ORACLE数据库登陆成功))	3		RBC
 ヘー(2) 合規性事件 ヘー(2) 系統运行事件 	mysol数提库登录成功		mysql数重车登录	黑盾入侵结奥系统	-SCI(MYSQL数据库登纸成功))	3		RDs
	FTP暴力破解		FTP账号最力破解	黑插入侵检测系统	[-N:10-SCI(FTP.Brute-Force))]	3		RDo
	sgimap注入	件分类				2		REO
	AWVS担捕	· Chan de Chi -			ty Scanner()	2		REO
	任意文件上传	力完合称:				2		REO
	struts2运程代码执行	* 等级: 信息			cution())	2		RCO
	访问把矿网页	• 攻击链: 无			×	2	访问控扩展页,例…	RØS
	发现里香工具		提交	¥.¶	(mikatz))	z		Reo
	mstor数据率整要成功	_	mssqi数据库登录。	黑猫入侵给商系统	-REI(ISQL Server[Is]d]+?登廷成功))	2		REC
	黑产牟利·诸路		黑结/细结	黑腦入侵检測系统	-SC (("rulename"; "論語-))	2	APT规则名称标识_	REO
	黑严牟利·拉斯		发现抱矿程序	黑皙入侵检刺系统	-SC:(("rulename": "#88"-))	2		REIO
	教学建造印度		101238-0410HE	黑暗入侵铃游系统	(-N-1031-SC-0回要相關)))	1		

点击【编辑】,跳出事件分类编辑弹框。 点击【删除】,可删除菜单中事件分类。 点击分类规则中的【新增】,进入新增规则页面

科分类	■ 分类规则			
分类搜索	第斤:總规定引	×	关键字搜索	
新教設施 (2) 同語会委等任 2) 国家会委等任 2) 国家会委等件 2) 里利会会等件 2) 王利会会等件 2) 王利会会等件 2) 王利会会等件 2) 王利会会等件 2) 王利会会等件 2) 王利会会等件 2) 名利信誉件 3) 名利信誉件 3) 系統出行著件	所憲分換: 阿特会会等年 		820 6 12	
	新注: 		讷问我们啊页,问	R 2 0 R 2 0 R 2 0
			被防火填阻斯的遷信	
	能 交 天前			

填写相关内容,点击【提交】,新增规则完成。 点击操作中的【查看】,进入查看页面。 点击操作中的【编辑】,进入编辑页面。 点击操作中的【删除】,删除分类规则。

2.7 系统管理

2.7.1 基础配置

路径:系统管理->基础配置。 基础配置中可对相关内容进行配置,点击'区域管理',进入区域管理页面。



通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。可进行增删查改操作。

点击'IP网段管理',进入 ip 网段管理页面。

明言地	I IPP	网段管理 系统参数	业务管理 资产分组	黑白名单 索引管理	通用配置 邮箱配置	邮件文案模板					
名称	t : [IP/IP段:	所属	网络:	所属业务:	所屬分组:		是否局域网: 全部	~	± i	9 E E
稲増	 11.2 	戦略 🕣 批量导入 日 !	批量导出 🛛 批量编辑	🗊 网络管理							
	序号	名称	IP/IPfQ	所属同绪	所需业务	所開分組	是否局域网	地理信息	备注	创建时间	操作
	1	10.9.14.0/24	10.9.14.0/24	测试1			5	中国福建福州		2021-03-19 16:09:20	1
	2	10.50.0.112	10.50.0.112	测试1			Ξ.	中国福建福州		2021-03-19 15:59:46	1
	3	10.50.0.111	10.50.0.111	奥hit1		关键服务器,终端	믔	阿富汗赫拉特		2021-03-19 15:57:30	1

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。可进行增删查改等操作。 点击'系统参数',进入系统参数页面。

用户指南

总范 基础配置 -				
系统管理>基础配置				ØRIN
区域管理 IP网段管理 系统参数	业务管理 资产分组 黑白名单	索引管理 通用配置 邮箱配置 邮件	文室模板	
📕 密码设置				
·最短來码长度	8	辛符 (8-64)	初始帶码:	
"密始强度	高(至少包含数字、小写字母、大写字目)	1、特殊符号中任意三种)		
	● 甲(至少包含数字、小写字母、大写字母			
	○ 吨(主>包含数子、小号子电、入号子	2. 1978/015-4112/2- AP)		
📕 登录设置				
"连续登录失败次数	5	次(1~5)	"自动解锁时长: 30	分钟(30~1440)
(香港)) 正照时	20	分前(1~20)		
TENK N N N N N N N N N N N N N N N N N N		JAH (1-10)		
密码过期强制重置	· 香			
		<u>₽</u> ≈		
可修改系统参 点击'业务管	数,点击提3 理',进入」	を,保存信息。 と务管理页面。		
系统管理>基础配置 区域管理 IP网段管理 系统参数	业务管理 资产分组 黑白名单	索引管理 通用配置 邮箱配置 邮件	文案模板	❷周新

系统搜索	Q IP/IP#	R :	所属自	自位:	创建时间:					-	10 Ei
f	◎ 批量計	90 0 3] 找量导入								
海峡(1)户网站 态势够知平台		序号	业务系统名称	等保定级	所属单位	资产范围	业务责任人	童务责任人电话	业务责任人邮箱	创建时间	操作
		1	志势感知平台							2021-04-13 14:31:59	R 🛛 🗰
		2	海峡门户网站	二级(描导保护)	福建會海峡信息技术		张王			2021-04-13 14:28:22	R 🛛 🕇

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。可进行增删查改等操作。 点击'资产分组',进入资产分组页面。

系统管理>基础配置 区域管理 IP网段管	意理 系统参数 业务管理 <u>资产分</u>	3月 一月 一月 一月 一月 一月 一月 二月	5 部結配置 邮件文案模板			ØRIST
分组名称:	IP/IPER:	操作时间:			查询	里西
④新增 目 党量影除						
序号 分類	184	IP/IP鏡	备注	创建时间	更新时间	操作
1 关键	主 股务器	10.50.0.111	关键服务器分组		2021-05-19 16:18:35	2
2 #3	服务器		普遷服务器分组		2019-12-13 15:23:42	
3 /线研	•	10.50.0.111	终端分组		2019-12-13 15:22:44	2
4 260	い分組		未分类分组			2
				共4条	上一页 1 下一页 10条/页~ 到第 1	页 确定

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。可进行增删查改操作。 点击'黑白名单',进入黑白名单页面。

理>基础配置	1908 Ticesto vi		800 m #2	1001201 1001	D.8249 65	25.51 m el	1/4 文宗福振					
		295篇建 20广力组	ADD# AD		theorem of the	1886 <u>8</u> 8	71十人 黑信权					
此/IP段:	别	8 :	标签:		操作的	时间:						黄田 1
增 ◎ 批量勿日	6 🔺 就量处置 🗌 🕞 批	重移出 🔍 加入白名单										
IP地址/IP段	别名	标签		IP来源	潘/目的IP	处置状态	黑名单有效期	操作者	操作时间	藝注		提作
59.222.20.161	[中国]			香蘭目的IP	目的IP	未封堵		超级管理员	2021-05-27 17:48:49	标题10527-1		🗷 🔺 🔕 🕞 💐
220.181.125.6	7[中国]			音響源の	191P	未封堵		超級管理员	2021-05-27 17:48:11	标题10527		🗹 🔺 🔕 G 🙏
10.50.2.164[8				舌歐洲中	潤IP	未對堵		超级管理员	2021-05-20 11:51:11	标题1		🛛 🛦 🔕 G 🙏
163.172.205.1	36[(表面)			告答目的IP	目的IP	未封填		超级管理员	2021-05-20 11:50:54	标题1		🖾 🛦 📀 🕞 🚨
										共4条 上一页	1 下一門 20 9	1 页 1 页

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。可对列表中的 IP/IP 段进行忽略、处置、编辑等操作。 点击'索引管理',进入索引管理页面。

区域管理 12网段管理 系统参数 业务管理	资产分组 黑白名单 索引管理 通	用配置 邮稿配置 邮件文案模板		9 03
索引名称:				空 羽 王章
🔒 我皇启用 📔 💿 批量关闭 📗 🍈 设置				存储总数:173.4GB 索引总数:250
素引名称	记录数量	存储大小	状态	操作
netflow-20210406	0	5768	开启	Q
netflow-20210506	0	5768	开启	Q
event-20210517	51,781	39.6MB	开启	Q
netflow-20210419	0	5768	开启	Ċ
netflow-20210531	21,941,336	4.7GB	开启	Ċ
netflow-20210410	0	5768	开启	Ċ
netflow-20210515	0	5768	开启	Ċ
event-20210529	0	5738	开启	Ċ
netflow-20210501	0	5768	开启	Ċ
netflow-20210522	0	5738	开启	Ċ
netflow-20210605	15,172,118	3.1GB	开启	Ċ
netflow-20210320	0	5768	开启	Ċ
event-20210622	338,300	141.8MB	开启	Ċ
event-20210718	0	4868	开启	Ċ
event-20210718	0	4868	开启	Q

共250条 上一页 1 2 3 4 5 - 13 下一页 20 余页 到篇 1 页 碘变

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。可进行启用、关闭及设置操作。 点击'通用配置',进入通用配置页面。

系统管理>基础配置						●用新
区域管理 IP网段管理 系统参数	业务管理 资产分组 黑白名牌	主 索引管理 通用配	置邮箱配置	邮件文案模板		
▎ 系統参数						
小司名称。	福建会演员使用自由于有限公司			10507/mm	2010-20215 June Strait Information Connection All Pickits Personnel	
2000	THE REPORT HOLD THE PLANE			NOX168	2019-2012Pojan suan anormatori Corporatori. Ali rigitis reserves.	
*系统名称:	黑盾综合日志审计分析系统			登陆logo:	①上份图片 /static/h-ui.admin/images/logo_big.png	
系统logo:	①上传图片 /upload/logo.png				*单个文件大小不超过16M	
	*单个文件大小不超过16M					
Child D True TOP						
SNMP Trap端口:	162			SNMP版本:	V2C	
◎ 资产风险配置						
THE PLAN AND A MARKED AND AND				No. 10 Ed. Manufacture / Loter -		
产重风控资产指为值:	50			间闪控资产扣为"量;	30	
中风险资产扣分值:	13			低风险资产扣分值:	11	
21数和量						
· 기구요르						
	关联分析引擎未知IP自动加入资产					
📕 操作日志记录配置						
			_	10.4		
				<u>49</u>		

可修改通用配置,点击提交,保存信息。 点击'邮箱配置',进入邮箱配置页面。

系统管理·基础配置	◎陶新
区域管理 计网段管理 系统参数 业务管理 资产分组 黑白名单 索引管理 通用配置 邮箱配置 邮件文案模板	
*觉件稿: xiegp@heidun.net	
1846 Generatives	
- vegovneour.ve.	
·密码:	
*发送即户部务器(SMTP): pmp.exmail.qq.com	
ISATEMIC / AS	
-2MITHMET : 485	_
游试邮稿收件稿 : 1-128个中年	366at
戦争	
可进行时常可思想作	

可进行邮箱配置操作。 点击'邮件文案模板',进入邮件文案模板页面。

系统管理>基础 区域管理	E当 IP网段管理	系统参数	业务管理	资产分组	黑白名单	索引管理	通用配置	邮箱配置	邮件文案模板							❷制新
模板名称:														- 1	查询	東西
④ 新増	◎ 批量删除															
B	号 模板名称	1	邮件文案内容									创建时间	设置默认	機板	操作	
1	1		1									2021-02-18 17:31:07	数 6人		R 🛛 🕯	D
											共1	島 上—页 1	ब _न ∎	20条/页~到	H 1 页	确定

可进行邮件文案模板的增删查改。

2.7.2 系统用户

路径:系统管理->系统用户。

总龙 系统用户 ×								
系统管理 / 系统用户								⊖刷新
📕 标题	用户账号:	用户名称:	手机号:		45种 :			查询 並且
关键字搜索	④新増 │ ⑩ 批量制除 │ ④ 模	板下戴 🔰 导入						
按部门直着按角色重要	序号 用户账号	用户名称 用户角色	手机	66788	绑定微信		秋念	操作
◇ 所有 (4)	1 account	account 账户管理员	18590000004	8940855277@qq.com			正常	R 🛛 🗊 🗛 🗇 🛇
默认部门(0)	2 auditman	auditman 审计员	18590000003	894085511@qq.com			正常	20410
	3 sysman	sysman 系统管理员	1859000002	89401111@qq.com			正常	R 🛛 🗊 🗛 🖯 🛇
	4 secman	secman 安全管理员	18590000001	89400000@qq.com	唐唐		正常	00 🖞 🖞 🖬 🖸 🔊
						#4 ∯ [±≅] 1 (∓≅	20 剱/页~	संस्था 1 ज्ञ (क) इत्य

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。可在此进行系统用户的增删查改、分配权限等操作。

2.7.3 系统角色

路径:系统管理->系统角色。

統管理>系统角色							Θ
▲ 角色分类 光線支援素	安全管理员 (500,000) 数据权限等级:全部 描述:安全管理员						
< 所有(7) ————————————————————————————————————	📕 包含部门						
	2 编辑						
一审计员 一账户管理员	序号 部门名称		上级部门		部门角	e	
一進护方				智无数描			
一安服工程师					共04	E 1-7 7-8	20 条/页~ 到第 1 页 确定
	角色成员						
	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)						
	席号 用户账号	用户名称	用户角色	手机号	AFRO	哪定微信	是否锁定
	1 secman	secman	安全管理员	1859000001	89400000@qq.com		I.R

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。可在此进行增删查改,权限维护操作。

2.7.4 组织结构

路径:系统管理->组织结构。

息范 组织结构 ×									
系统管理>组织结构									❷制新
 ▲ 组织结构 ×量字提示 Q 	福建省高等 福建省高等学校 所属角色:維持	学校师资培训中心 ^{药师资培训中心}							
	■ 部门人员	调整部门 号 用户账号	用户名称	NV D	用户角色	手机	451Q	穩定微信	是否锁定
 一人學部 一网络与逆续款育字號 一福達原范大学附届小学 		1 130765939611	yc123	福建省高	系统管理员	13075939617	1046305326@qq.com		<u>م</u>
一心理学院 一 旅游学院 一 社科处		2 18558787282 3 353074448@qq.com	用戶名者者	福建省高	·维护方, <u>业</u>	18558787283	siss@heidun.net 353074448@qq.com		m 否
- 校关工委 - 基理处 - 品克思主义学院		4 shizy	shizy	福建省高		18606019606	493277063@qq.com		8
- 宣传部 - 此時保卫处 - 4 李55		5 IISI1 6 admin1111	≄m admin1111	福建省商…		13599625327	493277063@qq.com		音
- 地理科学院 - 学生工作处		7 wufeng	wufeng	福建省高		18450098336	493277063@qq.com		否
10日本総合 10日本総合 10日本総合 10日本総合 10日本 10日本 10日本 10日本 10日本 10日本 10日本 10日本		o aorinia.	8.4.4				₩9327700099940011 ₩9327700099940011		a 页 例 定

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。可在此进行增删查改等组织结构。

2.7.5 系统日志

路径:系统管理->系统日志。

								-
类型:	全部日志 > 账户名	称: 通作	時容: 操作	状态:全部 🍚 諸	H作田寸间):	t		<u>8</u> 8
量對除	2 日志清空 き 日志優份							
序号	账户名称	客户满IP	操作时间	操作内容	响应时间	操作状态	日志类型	操作
1	superadmin	10.50.0.111	2021-01-27 12:48:48	系统管理-系统日志	6(ms)	请求成功	操作日志	R 🗊
2	superadmin	10.50.0.111	2021-01-27 12:48:48	引擎监控	7(ms)	请求成功	操作日志	B. 🗊
3	superadmin	10.50.0.111	2021-01-27 12:48:46	意道	1(ms)	请求成功	摄作日志	R 🖬
4	superadmin	10.50.0.111	2021-01-27 12:48:45	登陆系统	7(ms)	请求成功	登码日志	R 🗊
5	superadmin	10.50.0.111	2021-01-27 12:06:16	组织机构	6(ms)	请求成功	操作日志	R. 🖬
6	superadmin	10.50.0.111	2021-01-27 12:03:59	系统角色	2(ms)	请求成功	摄作日志	B 💼
7	superadmin	10.50.0.111	2021-01-27 12:03:44	系统角色	7(ms)	请求成功	操作日志	R 🖬
8	superadmin	10.50.0.111	2021-01-27 12:02:54	系统用户	8(ms)	请求成功	操作日志	B 🗊
9	superadmin	10.50.0.111	2021-01-27 11:48:22	基础配置	ll(ms)	请求成功	摄作日志	R 🖬
10	superadmin	10.50.0.158	2021-01-27 11:48:16	设备管理	7(ms)	请求成功	操作日志	R 1
11	superadmin	10.50.0.158	2021-01-27 11:48:16	级职管理	13(ms)	请求失效	操作日志	R 🗊
12	superadmin	10.50.0.158	2021-01-27 11:48:16	设备管理·设备信息	89(ms)	操作成功	操作日志	R 🖬
13	superadmin	10.50.0.111	2021-01-27 11:47:46	安全报告·周期报告	1(ms)	请求成功	操作日志	B 🖬
14	superadmin	10.50.0.111	2021-01-27 11:47:31	安全报告·周期报告	1(ms)	请求成功	操作日志	2

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。可在此进行查看、删除及备份等操作。

2.7.6 引擎监控

路径:系统管理->引擎监控。

总范 引撃	监控 =								
系统管理>引用	副旋接								◎刷新
采集监控	分析监控								
服务器名制	R: [] [] [] [] [] [] [] [] [] [] [] [] []	运行状态: 全部		-					10 10
序号	服务器名称	IP地址	运行状态	服务融分类	编制行规则	已处理日志数(每分钟)	出错日志数(每分钟)	采集资产数	操作
1	Collector_10.9.1.150_150	10.9.1.150	# #	副集-collector	389	0	0	29	•
2	Parser_10.9.1.150_82	10.9.1.150	# #	采集 -parser	389	0	0		R 🗊
3	Collector_10.9.1.151_150	10.9.1.151	正常	采集-collector	389	0	0	0	
- 4	Parser_10.9.1.151_82	10.9.1.151	ER	采集-parser	389	0	0		Eg
5	NetFlow_10.9.2.231_83	10.9.2.231	正常	采集-netflow	389	0	0	1	
6	Collector_10.9.1.150_40	10.9.1.150	ER	采集-collector	389	0	0	19	•
						五6歲 上	5 1 7-5	20 条/页 > 到望	1 页 确定

通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。可在此进行添加、查看及删除操作。

2.7.7 设备管理

路径:系统管理->设备管理。 可进行多项设备管理,点击'系统信息',进入系统信息页面,可查看系统信息。

系统管理>设备管理		OR]AF
系统信息 网络管理 日期时间管理 运行管理 诊断工具 许可管理	访问控制策略 日志备份与恢复	
1 10-10-00 H		
▲ 基本信息		
设备型号: HD-NGSOC	系统版本: HD-LAS V4.0	机器码: 39829DF578E9586EE5C1EACCFA8B7377
授权类型: 试用	授权客户:海峡	最新升级时间: 2021-02-22 14:30:00 KMC开级
▶ 規则库信息		
关联分析规则库	采集规则库	预处理规则库
当前版本: v202151	当前版本: v2021S1	当前版本: v2021S1
更新时间:	更新时间:	更新时间:
规则库更新: 更新	规则库更新: 更新	规则库更新: 更新
_		_
▲ 硬件信息		
STITUS AND		ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL
<u>∃</u> 98.60% <u>∃</u>		<u>∃</u> 74.48% <u>∃</u>
二 CPU使用率 二		二 内存使用率 二
E 3		
	存储策略	

点击'网络管理',进入网络管理页面,可继续网络配置和查看路由信息。

6管理>设备管理							
信息 网络管理 日期	即时间管理 运行	行管理 诊断工	具 许可管理	访问控制策略 日志备份与恢复			
其大司要							
主机名: HD-LAS				DNS: 114.114.114.114		*Kafka对外监听地址: 10.50.0.240	
PT 447 PT 300							
网络配置							
司卡名称	秋志	地址分配方式	t IPv4地址	塊码(IPv4)	IPv6地址	子同前缀长度	同关
enp1s0(默认管理口)	启用	~ 静态	× 10.50.0.240	255.255.255.0			10.50.0.1
enp2s0	禁用	~ 动态	~				
enp3s0	禁用	~ 动态	~				
enp+su							
enp5s0	禁用		~				
enp6s0	禁用	~ 动态	~				
静态路由							
目标网络			子同推码	-ज	跳	局卡名称	状态
10.0.0			0.0.0.0	10.5	0.0.1	enp1s0	正常
10.50.0.0			255.255.255.0	0.0.0	0.0	enp1s0	正常
					继攻		

点击'日期时间管理',进入日期时间管理页面,填写内容,点击【提交】,日 期时间设置完成。

系统管理>设备管理	●別新
系統信息 网络管理 日期时间管理 运行管理 诊断工具 许可管理 访问控制策略 日志备份与你复	
与NTP服务器同步	
油前日期 : 2021-07-20	
無利可何 : 175027	
当前时医:上海	
較	

点击'运行管理',进入运行管理页面,可查看服务信息,并进行重启服务、重 启设备及恢复出厂设置等操作。

系统管理-12条管理										
系統信息 网络管理 日期时间管理 运行管理 诊断工具 许可管理 访问控制策略 日志备份与恢复										
◎ 批量量用服务 ◎ 天明设备 ○ 和賞出「設置										
序号 服务名称	秋恋	操作								
1 数据采集股务	已启动	*								
2 数据预计理报务	已启动	*								
3 任务周期股务	已启动	*								
4 分析級時	已启动	*								
5 使严辩测服务	已启动	*								
6 满意中间件服务	已启动	*								
7 数据检测服务	已启动	*								
8 分布式协调服务	已启动	*								

点击'诊断工具',进入诊断工具页面。

系统管理>诊	會管理												❷周新
系统信息	网络管理	日期时间管理	运行管理	诊断工具	许可管理	访问控制策略	日志备份与恢复						
				输入目标	地址				ping	traceroute	telnet		
				***	_								
				外们结果	停止								

点击'许可管理',进入许可管理页面,可查看产品相关内容,并进行本地授权 或网络授权。

系统管理>设备	管理								❷制新			
系统信息	网络管理 日期时间管理 运行	行管理 诊断工具	许可管理访问	回控制策略 日志备份与恢复								
	5											
授权类型	授权客户		要权时间	接权有效期	服务有效期	资源数	系统版本	设备型号				
试用	784A	2	2021-07-09 08:01:35	2021/12/31	2021/12/31	5	HD-LAS V4.0	HD-NGSOC				
📕 机器码												
		授权类型: 🔇		告援权								
		产品邀活方式:「	"简LICENSES									
		本机注册码:	3982901978695666E5C1EACCFA887377									
	• ±f	专LICENSES文件:	通师文件 * 他个文件大小不超过16M									
					授权							

点击'访问控制策略',进入访问控制策略页面,可对主机和账号进行管理。

系统管理>	设备管理										回制新
系统信息	网络管理	日期时间管理	运行管理	诊断工具	许可管理	访问控制策略	日志备份与恢复				
其 管理	主机								•	1、内容牛的主机,允许访问本平台。 2、默认为定,表示任何的编述问念平台。 3 4 3 年代14回,2 4 4 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
										IP+4: 1) 标准情形: \$21192.168.1.1; 2) 周旋接近: \$21192.168.1; 4) 第21192.168.1; 2) 周旋接近: \$21192.168.1; 4) 第21192.168.1; 2) 周旋接近: \$21192.168.1; 4) 第21192.168.1; 4) 第21192.158.1; 4) 第21192.1; 4) 第21192.158.1; 4) 第21192.1; 5)	
▼ 账号	管理									4) 网段格式:标准格式/掩码,缩写格式/掩码,混合格式/掩码,其中掩码范围是1-128。	
									•	1、内容中的用户服号,不允许访问本平台。 2、就认为空,表示任意报号都能访问本平台。 3、输入能式说明:多个输入场号之间崩积绝之分号分隔。 例:zhangsanlisiwangwu	
								歡			

点击'日志备份与恢复',进入日志备份与恢复页面。 通过填写相关查询条件,点击【查询】,出现相关查询结果;点击【重置】,查 询条件内容清空。可在此进行配置、备份及恢复等操作。

用户指南

