

AiLPHA 大数据智能安全分析平台

V3.5.3

用户手册

文档版本: 02

发布日期: 2021-03-26



www.dbappsecurity.com.cn



本文中出现的任何文字描述、文字格式、插图、照片、方法等内容·除另有特别注明·版权均属杭州安恒 信息技术股份有限公司(简称"安恒信息")所有·受到有关产权及版权法保护。任何个人、机构未经安 恒信息的书面授权许可·不得以任何方式复制或引用本文的任何片段。

经授权使用本文中内容的单位或个人, 应在授权范围内使用, 并注明"来源: 安恒信息"。违反上述声明 者,安恒信息保留追究其法律责任的权利。

除杭州安恒信息技术股份有限公司的商标外, 本手册中出现的其他商标、产品标识及商品名称, 由各自权 利人拥有。 Historie Contraction of the second se



文档说明

产品名称		AiLPHA 大数据智能安全分析平台		
适用平台	/版本		V3.5.3	
拟制人	AH1171 (AiLPI	HA-测试)	评审组	AH5888(远程技术支持-标准文档)
发布人	AH5888(远程技	支术支持-标准文档)	备注	受控文档
修订记录				

修订记录

日期	修订版本	修改记录	修改人
2021-03-05	01	初灾发布。	AH5888(远程技术支持-标准文档)
2021-03-26	02	第二次发布。 替换 2.3.4 关于截图。	AH5888(远程技术支持-标准文档)
		the solution water and the solution of the solution is a solution of the solut	





目录

1. 产品简介 1 1.1 产品概述 1 1.2 产品功能 1 1.3 产品特点 1 1.4 角色和权限说明 2 2. 首页 3 2.1 登录首页 3 2.2 首页信息展示区概要 6 2.3 用户信息区域介绍 9 2.3.1 个人中心 10 2.3.2 人门指引 10 2.3.3 小工桌 11 2.3.4 尖子 13 2.3.5 退出 13 3. 筑一门户 14 3.1 功能简介 14	前言	·	I
1.1 产品機 1 1.2 产品功能 1 1.3 产品特点 1 1.4 角色和权限说明 2 2. 首页 3 2.1 登录首页 3 2.2 首页信息展示区概要 6 2.3 用户信息区域介绍 9 2.3.1 个人中心 10 2.3.2 人门指引 10 2.3.3 小工具 11 2.3.4 尖子 13 2.3.5 週出 13 3. 依一门户 14 3.1 功能简介 14	1. 产	² 品简介	1
1.2 产品功能 1 1.3 产品特点 1 1.4 角色和权限说明 2 2. 首页 3 2.1 登录首页 3 2.2 首页信息展示区概要 6 2.3 用户信息区域介绍 9 2.3.1 个人中心 10 2.3.2 人门指引 10 2.3.3 小工具 11 2.3.4 关于 13 2.3.5 超出 13 3. 统一门户 14	1.1	1 产品概述	1
1.3 产品特点 1 1.4 角色和权限说明. 2 2. 首页. 3 2.1 登录首页. 3 2.2 首页信息展示区概要. 6 2.3 用户信息区域介绍. 9 2.3.1 个人中心. 10 2.3.2 人门指引. 10 2.3.3 小工具. 11 2.3.4 关于. 13 2.3.5 退出. 13 3. 统一门户. 14	1.2	2 产品功能	1
1.4 角色和权限说明 2 2. 首页 3 2.1 登录首页 3 2.2 首页信息展示区概要 6 2.3 用户信息区域介绍 9 2.3.1 个人中心 10 2.3.2 入门指引 10 2.3.3 小工具 11 2.3.4 关于 13 2.3.5 超出 13 3. 统一门户 14	1.3	3 产品特点	1
2. 首页	1.4	4 角色和权限说明	
2.1 登录首页 3 2.2 首页信息展示区概要 6 2.3 用户信息区域介绍 9 2.3.1 个人中心 10 2.3.2 入/7指引 10 2.3.3 小工具 11 2.3.4 关于 13 2.3.5 退出 13 3. 统一门户 14	2. 首	重页	
2.2 首页信息展示区概要 6 2.3 用户信息区域介绍 9 2.3.1 个人中心 10 2.3.2 人门指引 10 2.3.3 小工具 10 2.3.4 关于 13 2.3.5 退出 13 3. 统一门户 14	2.1	1 登录首页	
2.3 用户信息区域介绍 9 2.3.1 个人中心 10 2.3.2 入门指引 10 2.3.3 小工具 10 2.3.4 关于 13 2.3.5 退出 13 3. 统一门户 14	2.2	2 首页信息展示区概要	6
2.3.1 个人中心	2.3	3 用户信息区域介绍	9
2.3.2 入门指引	2	2.3.1 个人中心	
2.3.3 小工具	2	2.3.2 入门指引	10
2.3.4 关于	2	2.3.3 小工具	11
2.3.5 退出	2	2.3.4 关于	
 统一门户	2	2.3.5 退出	13
3.1 功能简介	3. 约	充一门户	14
	3.1	1 功能简介	



4. 态势感知 17 4.1 概述 17 4.2 外部攻击态势 17 4.2 小部攻击态势 17 4.2 小部攻击态势 17 4.2 小部攻击态势 17 4.2 次部攻击态势 17 4.2 以磁要 17 4.3 (向成防感知 20 4.3 (向成防感知 20 4.3.1 功能每介 20 4.3.2 区块磁要 21 4.4 资产失陷态势 26 4.4 资产失陷态势 26 4.1 功能每介 26 4.2 区块磁要 26 4.5 Wris 业务系统态势 30 4.5.1 功能每介 30 4.5.2 区块磁要 30 4.6 数据中心态势 33 4.61 功能每介 33 4.6.1 功能每介 33 4.6.2 区块概要 33	3.2	块概要	14
4.1 概述 17 4.2 外部攻击态势 17 4.2.1 功能简介 17 4.2.2 区块框要 17 4.3 横向威胁感知 20 4.3.1 功能简介 20 4.3.2 区块框要 20 4.3.2 区块框要 21 4.4 资产失陷态势 26 4.1 功能简介 26 4.2 区块框要 26 4.1 功能简介 26 4.2 区块框要 26 4.5 WEB 业务系统态势 30 4.5.1 功能简介 30 4.5.2 区块框要 30 4.5.2 区块框要 30 4.6 数据中心态势 33 4.6.1 功能简介 33 4.6.2 区块框要 33	4. 态势感	知	17
4.2 外部攻击态势	4.1 概述	<u>t</u>	17
4.2.1 功能简介	4.2 外部	3攻击态势	17
4.2.2 区块概要 17 4.3 横向威胁感知 20 4.3.1 功能简介 20 4.3.2 区块概要 21 4.4 资产失陷态势 26 4.4 资产失陷态势 26 4.4 资产失陷态势 26 4.4.2 区块概要 26 4.5 WEB 业务系统态势 30 4.5.1 功能简介 30 4.5.2 区块概要 30 4.6 数据中心态势 33 4.6.1 功能简介 33 4.6.1 功能简介 33 4.6.2 区块概要 33	4.2.1	功能简介	
4.3 横向威胁感知 20 4.3.1 功能简介 20 4.3.2 区块欄要 21 4.4 资产失陷态势 26 4.1 功能简介 26 4.2 区块欄要 26 4.5 WEB 业务系统态势 30 4.5.1 功能简介 30 4.5.2 区块欄要 30 4.6 数据中心态势 33 4.6.1 功能简介 33 4.6.1 功能简介 33 4.6.2 区块欄要 33	4.2.2	区块概要	17
4.3.1 功能简介	4.3 横向]威胁感知	
4.3.2 区块概要. 21 4.4 资产失陷态势. 26 4.1 功能简介. 26 4.2 区块概要. 26 4.5 WEB 业务系统态势. 30 4.5.1 功能简介. 30 4.5.2 区块概要. 30 4.6 数据中心态势. 33 4.6.1 功能简介. 33 4.6.2 区块概要. 33 4.6.2 区块概要. 33	4.3.1	功能简介	20
4.4 资产失陷态势. 26 4.1 功能简介. 26 4.2 区块概要. 26 4.5 WEB 业务系统态势. 30 4.5.1 功能简介. 30 4.5.2 区块概要. 30 4.6 数据中心态势. 33 4.6.1 功能简介. 33 4.6.2 区块概要. 33 4.6.2 区块概要. 33	4.3.2	区块概要	21
4.4.1 功能简介	4.4 资产	· 失陷态势	
4.4.2 区块概要	4.4.1	功能简介	
4.5 WEB 业务系统态势	4.4.2	区块概要	
4.5.1 功能简介	4.5 Web	业务系统态势	
4.5.1 50 4.5.2 区块概要	151	功能符合	30
4.5.2 区块概要	4.5.2		20
4.6 双据中心态势	4.5.2	<i>亾坎彻女</i>	
4.6.1 功能简介	4.6 数捷	中心态势	
4.6.2 区块概要	4.6.1	功能简介	
	4.6.2	区块概要	



4.7 AI 异	常分析	
4.7.1	功能简介	
4.7.2	区块础安	
4.0.00000		40
4.8 SHER	RLOCK 网络崔仝	40
481	功能简介	40
1.0.1		10
4.8.2	区块概要	40
4.9 资产	态势感知	43
	SV SI.	
4.9.1	功能简介	43
4.9.2	区块概要	43
4 10 TH +		4.5
4.10 攻击	山 有矩 哧 溯源	45
4 10 1	功能简介	45
4.10.2	区块概要	45
4.11 资产	^立 威胁溯源	
4.11.1	功能简介	48
4.11.2	区块概要	48
4 10 不生		50
4.12 十⊏	コルコルコルコルス	
4.12.1	功能简介	
4.12.2	区块概要	
	杭州安恒信息技术股份有限公司	



4.13 安全	全态势			54
4.13.1	功能简介			54
4.13.2	区块概要			55
4.14 重任	呆方案			56
4 15 4 37			QV .	FC
4.15 AIV	IEW			30
4.16 仪表	麦盘			56
			S	
4.17 大厦	异轮播	<u>,</u>		56
			S.	
5. 威胁感	知	<u>S</u>	<u>s</u>	59
			xA.	
5.1 安全	事件	<u> </u>	<u> </u>	59
511	功能简介	Solution of the second		59
01111	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
5.1.2	区块概要	S S		59
	12			
5.2 资产	感知	<u>ب</u> ي:		60
	S.	ON CON		
5.2.1	功能简介	<u>у</u>		60
	J. J			
5.2.2	区块概要			61
5.3 业务	全景			62
5.3.1	功能简介			62
5.3.2	区块概要			62
5.3.3	业务监控			69



5.4 Shef	RLOCK		2
5.4.1	功能简介		2
5.4.2	页面详细介绍		4
5.4.3	访问关系		7
5.4.4	行为画像		!
5.4.5	服务端口		!
5.4.6	访问端口		3
5.4.7	脆弱性		1
5.4.8	资产指纹		5
6. 安全分	析		3
6. 安全分 6.1 INV	析	88	8 3
6. 安全分 6.1 INV <i>6.1.1</i>	析 TESTIGATION 功能简介	88 	3 3
6. 安全分 6.1 INV 6.1.1 6.1.2	析 TESTIGATION 功能简介 安全告警		3 3
6. 安全分 6.1 INV 6.1.1 6.1.2 6.1.3	・析 	88 	3 3 3 3
 6. 安全分 6.1 INV 6.1.1 6.1.2 6.1.3 6.1.4 	 析 Diffation 功能简介 安全告警 原始日志 异常记录 	88 	8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8
 安全分 6.1 INV 6.1.1 6.1.2 6.1.3 6.1.4 6.2 威胁 	 析 TESTIGATION 功能简介 安全告警 原始日志 扉始日志 昇常记录 	88 	3 33 33 33 33
 安全分 6.1 INV 6.1.1 6.1.2 6.1.3 6.1.4 6.2 威肋 6.2.1 	 析 DESTIGATION 功能简介 安全告警 原始日志 扉始日志 引花录 小情报 功能简介 	88	3 33 33 33



6.2.3	情报源		113
6.3 UEB	A		114
6.3.1	功能简介	8	114
6.3.2	UEBA 用户画像		115
6.3.3	UEBA 用户管理	Š ^V	
6.4 可视	化中心	jiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	120
6.4.1	功能简介	*****	120
6.4.2	图表管理	<u>S'</u>	121
6.4.3	仪表盘管理		124
6.4.4	AiView 设计器		125
6.5 报告	管理		128
6.5.1	功能简介		128
6.5.2	报告中心	∽ ∽	128
6.5.3	报告订阅		130
6.6 SOA	R		132
6.6.1	功能简介		132
6.6.2	任务看板		133
6.6.3	剧本编排		135



6.7 安全	全模型	143
6.7.1	模型管理	143
6.7.2	指标管理	153
6.7.3	数据字典	157
6.7.4	数据清洗	159
6.7.5	白名单	163
7. 安全运	营营	171
7.1 工作	作台	171
7.1.1	功能简介	171
7.1.2	工单状态	171
7.1.3	<i>待办工单</i>	172
7.1.4	通报情况	172
7.1.5	最新动态	173
7.2 通报	很预警	173
7.2.1	功能简介	173
7.2.2	<u> 预警</u>	173
7.2.3	通报	179
7.3 工单	单管理	185
	杭州安恒信息技术股份有限公司	



7.3.1	功能简介	
7.3.2	查询工单	185
7.3.3	新增工单	185
7.3.4	处 <i>置工单</i>	188
7.3.5	删除工单	192
7.3.6	批量处置工单	192
7.4 订阅	1规则	192
7.4.1	功能简介	193
7.4.2	查询订阅规则	193
7.4.3	新增订阅规则	193
7.4.4	订阅规则其他操作	194
7.4.5	订阅记录	194
7.5 绩效	【考核	194
7.5.1	功能简介	194
7.5.2	查询绩效	195
7.5.3	导出报告	195
7.6 重大	保障	195
7.6.1	功能简介	196
	杭州安恒信息技术股份有限公司	



7.6.2	新增重保任务	
7.6.3	管理重保任务	
7.6.4	编辑重保任务	197
7.6.5	查看重保任务	198
7.6.6	删除重保任务	
7.6.7	态势感知重保大屏预览入口	
8. 资产管	r理	200
8.1 资产	≃管理	200
8.1.1	功能简介	
8.1.2	页面布局	200
8.1.3	资产新增、编辑、修改	201
8.1.4	资产导入和导出	
8.1.5	SOC 同步	
8.1.6	<i>设置</i>	204
8.1.7	<i>投屏</i>	206
8.2 WEE	3 业务系统	207
8.2.1	功能简介	207
8.2.2	<i>灾 面 布 局</i>	207



8.2.3	Web 业务系统新增、编辑	、修改	
8.2.4	Web 业务系统导入和导出	!	211
8.2.5	<i>设置</i>		211
8.2.6	<i>投屏</i>	Š	
8.3 安全	2设备	, Śł	
8.3.1	功能简介		
020	而而在月		214
0.3.2			
8.3.3	<i>安主设备新瑁、编辑、删</i>		216
8.3.4	<i>投屏</i>	l S	217
8.3.57	APT 大屏		
8.3.6	WAF 大屏		
8.3.7	数据库审计大屏		
8.4 弱点	〔管理		
8.4.1	功能简介		
8.4.2	弱点管理		
8.4.3	扫描报告的导入		227
8.5 处置	【联动		
8.5.1	功能简介		
		杭州安恒信息技术股份有限公司	



8.5.2	联动设备		231
8.5.3	<i>联动策略</i>		233
8.5.4	<i>阻断事件</i>		236
8.6 安全	≥域	<u></u> S°	
	市坐在入	. Ph	226
8.0.1	<i>▶」月6日]) </i>		230
8.6.2	页面布局		236
8.6.3	安全域新增、编辑、修改		
8.6.4	安全域导入和导出	S S	240
8.6.5	<i>其他操作</i>	S S	240
87 组织	2架构		241
	Š	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	2.1
8.7.1	功能简介	2.	
8.7.2	组织结构查询	5	241
8.7. <i>3</i>	组织架构新增		
074	4月4月加4约4户作品		241
0.7.4	组织未何痈神		
8.7.5	组织结构删除		242
9. 系统管	理		243
9.1 运维	主管理		243
9.1.1	<i>运维告警</i>		



9.1.2	<i>健康检查</i>		
9.1.3	存储管理		246
9.1.4	故障日志		247
9.2 配置	管理	<u>So</u>	
9.2.1	<i>系统配置</i>	N	248
9.2.2	数据配置		254
9.2.3	推送管理		255
9.2.4	<i>系统开关</i>		256
9.2.5	<i>集群扩容</i>		257
9.3 任务	管理		262
9.3.1	流计算任务		262
9.3.2	定时任务		267
9.4 系统	管理		268
9.4.1	升级管理		268
9.4.2	许可证		269
10. 用户权	《限管理		272
10.1 E	志审计管理员		272
10.2 权图	艮管理 员		272
		杭州安恒信息技术股份有限公司	



10.2.1 角色管理	
10.2.2 用户管理	
10.3 认证安全	
10.3.1 登录安全设置	
10.3.2 密码策略设置	
10.3.3 水印设置	
11. 术语和缩略语	
	in the second se



前言

感谢您选择安恒信息的网络安全产品。本手册对安恒信息 AiLPHA 大数据智能安全平台(以下简称"大数 据平台"、或"AiLPHA 大数据平台")进行了简单介绍·并对平台的使用方法进行了详细描述。主要包 括产品简介、首页、统一门户、态势感知、威胁感知、安全分析、安全运营、资产管理、系统管理和用户 权限管理。

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

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

预期读者

本文档主要适用于使用平台的人员, 包括系统管理员、权限管理员、操作管理员等。本文假设读者对以下 领域的知识有一定了解:

- ◆ TCP/IP、 SNMP、 Syslog、 HTTP、 FTP、 NFS、 Samba 等基础网络通讯协议
- ◆ 数据库、服务器、网络安全设备、路由器、交换机等常见设备(系统)的基本工作原理和配置
- ◆ 虚拟机、容器技术等常见的 IT 技术原理
- ◆ Syslog 协议的基本工作原理和配置》

格式约定

本手册内容格式约定如下

内容	说明
粗体字	Web 界面上的各类控件名称以及内容。例如:"在菜单栏中选择' 系统状态 '进入 系统状态 页面,选择接口状态页签"。
<>	Web 界面上的按钮。例如:"微信认证失败,点击< 我要上网 >不弹出微信认证界面"。
>	介绍 Web 界面的操作步骤时,用于隔离点击对象(菜单项、子菜单、按钮以及链接等)。 例如:"在菜单栏选择' 策略配置>认证管理>认证策略 '查看是否开启了认证策略"。



本手册图标格式约定如下:

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

获得帮助

使用过程中如遇任何问题,请致电服务热线 400-6059-110。

请访问安恒社区<u>https://bbs.dbappsecurity.com.cn</u>获取更多文档。

联系信息

- 地址: 浙江省杭州市滨江区西兴街道联慧街 188 号安恒大厦 Allo. hr. windight
- 邮编: 310052
- 电话: 0571-88380999
- 传真: 0571-28863666
- 官网: <u>http://www.dbappsecurity.com.cn</u>
- 邮箱: <u>400-doc@dbappsecurity.com.cn</u>





1.1 产品概述

AiLPHA 大数据智能安全分析平台采用大数据分析技术架构,结合专业的安全经验,依托雄厚的研发实力, 兼顾未来业务的发展,以"数据驱动安全分析,形成安全闭环,解决安全事件遗漏"为产品理念。为企业 用户提供全局安全态势感知能力和业务不间断稳定运行提供安全保障,为用户信息安全决策提供数据支撑。 广泛适用于政府、金融、运营商、公安、电力能源、税务、工商、社保、交通、卫生、教育、电子商务及 各企事业单位等。

1.2 产品功能

1. 实时预警

支持安全威胁实时分析、秒级预警、安全事件取证、

2. 亿级存查

万亿级别的超大规模数据管理和快速查询。

3. 异常检测

侦测越权行为、账户盗用等用户异常行为。

4. 智能学习

基于机器学习,为用户提供安全态势感知能力。

5. 深度关联

支持深度联动分析识别影响范围有效安全事件。

6. 追踪溯源

支持安全事件溯源, 还原攻击轨迹。

1.3 产品特点

1、 性能可靠稳定

采用多核处理技术、多线程应用系统·处理能力可达 10 万条/秒·节省用户成本; 支持分布式部署、并行 处理· 兼顾未来扩容及发展的需求。



2、超大存储查询

解决万亿级别的数据存储难题· 满足客户长时间的日志存储需求· 采用高效的压缩存储技术· 节省用户大量存储资源; 具备高效的查询能力· 能够在秒级内从数万亿条规模的结构化和非结构化大数据中查询出客户所需的数据· 提高工作效率。

3、完善的数据可视化

数据大屏直观展示丰富易用的安全数据·解决客户的整体安全态势感知需求;表报系统支持定期自动生成 丰富的行业安全报告和报表·解决客户的安全运营分析报表需求。

4、深度智能分析

采用大数据和机器学习技术· 对多维度的信息和多源数据进行整合、关联、智能分析和预测· 辅助安全人员做出精准判断和调查。

5、 模块化功能扩展及开放兼容

基于模块动态扩展技术· 能够为用户实现高度可扩展能力; 高度兼容多种主流安全设备· 采用专利技术提高协议解析的精准性·并提供丰富的第三方系统对接 API。

1.4 角色和权限说明

AiLPHA 大数据智能安全分析平台默认设置有三个账号 · 分别是权限管理员(useradmin)、日志审计管理员 (opadmin)和系统管理员(admin)。

用户角色	缺省用户名称	权限说明
权限管理员	useradmin	新增用户和角色。
日志审计管理员	opadmin	查看操作日志。
系统管理员	admin	除了新增用户角色以及查看操作日志外的所有权限。

有关角色和权限配置的更多详细信息,请参考用户权限管理。

如无特别说明,《本文仅从 admin 视角进行描述,配置内容以 admin 用户操作举例说明。



2. 首页

2.1 登录首页

设备安装上架并连接网线、电源后,用户可通过 Web 方式登录及管理 AiLPHA 大数据智能安全分析平台。 在浏览器中输入<u>https://AiLPHA 大数据智能安全分析平台 IP</u>,进入登录窗口。



在登录窗口中输入用户名、密码 · 点击<登录>进入 AiLPHA大数据智能安全分析平台。

- ▶ 目前只支持 Chrome 浏览器。
- ◆ 出厂默认管理 IP 请查看设备面板·默认用户名/密码为: admin/iS%4Rh37g3。
- ▶ 现场部署并且对接 AiCSO 系统后,支持使用 AiCSO 账号登录。

管理员及拥有所有功能模块访问权限的用户登录后进入的默认页面如下。







页面布局分为功能菜单、 用户信息和信息展示区三部分。

序号	名称	说明
1	功能菜单	以不同的角度提供各类管理功能的配置入口,方便用户根据实际需要进行切换,如下图所示。 및 参数版和 / 成数版和 / 全全级 / 名 安全运费 · 《 》"管理 · · · · · · · · · · · · · · · · · · ·
2	用户信息	显示当前登录用户 · 可在此区域进行修改用户信息 · 查看入门引导 (仅限 admin) · 查看小工具 · 查看平台版本 · 退出登录等操作 · 如下图所示 ·
3	信息展示区	该区域主要用于展示各类风险、告警信息展示,以及执行相关的功能操作。详细 操作请参考首页信息展示区概要。

租户用户(即只拥有部分权限的账号)登录后进入的默认页面如下·具体因 useradmin 所分配的权限和可用功能模块而异。



择"**退出**",可以退出Web登录。



2.2 首页信息展示区概要

区块	说明	详细
搜索框	 支持输入 IP、域名、文件 HASH、邮箱。 IP 支持 sherlock 溯源,跳转至 "威胁感知 > Sherlock"页面。 IP、域名、文件 HASH、邮箱支持威胁情报 查询,跳转至 "安全分析> 威胁情报>情报 查询"页面。 	
安全运营	 ◆ 展示平台当前开启状态的通报数据。 ◆ 点击跳转至 "安全运营>工作台"页面。 	安全运营 30 _{通报}
资产管理	 ◆展示平台当前资产个数。 ◆ 点击跳转至"资产管理>资产管理"页面。 	资产管理 933台
业务拓扑	◆ 展示平台当前业务拓扑个数。 ◆ 点击跳转至" 威胁感知>业务全景 "页面。	^{业务拓扑} 25个
日志总量	 ◆ 展示当前设备上所有接入的日志总量(数据 源为原始日志)。 ◆ 跳转至 "安全分析>Investigation>原始日 志"(跳转无带入时间·默认本日)。 	日志总量 6.1 _{亿条}

6	D	3信	息
	DAS-980	curity s	2201

区块	说明	详细
已存储时间	 ◆ 显示当前设备上所有接入数据的已存储时间,单位 周(与索引状态无关)。 ◆ 点击跳转至 "系统管理>配置管理>数据配置"界面。 	已存储时间 9周
剩余容量/总容 量	 ◆ 当前的数据磁盘使用情况。 ◆ 跳转至 "系统管理>运维管理>存储管理" 页面。 	剩余容量/总容量 36.4T/39.8T
风险资产	 显示最近7天内风险资产数: 已失陷、高风 险、低风险资产个数。 支持跳转。 	ANERP 5 Estatore Estatore
风险资产列表	 ◆ 展示 Top5 风险资产信息(资产感知页面列表前5个)。 ◆ 点击<更多> · 跳转至 "威胁感知>资产感知"页面。 	MAXAN : SAVE : MAXAN : <th< td=""></th<>
安全事件	 ◆ 显示最近 7 天内安全事件: 高危事件、中危 事件、低危事件个数。 ◆ 支持跳转。 	【 安全事件 図 31 g 0 g 4 g 1 g 1 g 1 g 1 g 1 g 1 g 1 g 1 g 1
安全事件列表	 ◆ 展示 Top5 安全事件信息(安全事件页面列 表前 5 个)。 ◆ 点击<更多> · 跳转至 "威胁感知>安全事 件"页面。 	MARKA MEMORY ME MEMORY ME V-RENDER D(V-R) (0) (0) (0) (0) (0) (0) (0) (0) (0) (0



区块	说明	详细
SOAR (任务看板)	显示最近 7 天内任务状态占比和任务趋势。 不支持跳转。	I soan demi Hayn 0 + Hayn 10 +
任务列表	展示 Top5 任务信息(任务看板页面列表前 5 个) 点击< 更多 > · 跳转至 " 安全分析>SOAR>任务 看板" 页面。	
告警	 ◆ 告警显示: 本周/本月的所有告警数(所有安全告警(包括误报))。 显示本周与上周・本月与上月对比的告警数・红色是上升・绿色是下降。 点击<带入时间条件>(本周/本月)跳转至"安全分析>Investigation>安全告警"页面。 已处理、未处理告警数量(已处理是处于处理中、处理完成、误报的告警)・点击<带入条件>跳转至"安全分析>Investigation>安全告警"页面。 	ин ал 5 л 4 холхт Сна нар ха сна нар
告警类型	告警类型Top10。	I MERE



区块	说明	详细
告警统计	 ◆ 显示查询时间范围内的告警统计。 ● 圆点图中: ● 从上至下显示: 探查、投递、利用、横向渗透、命令控制、内部侦察等告警情况。 ● 以圆点大小显示告警数趋势。 ● 当鼠标移到圆点上, 圆点具有光环。显示时间、攻击链名称、具体告警数量;若无告警显示无数据。 ● 单击圆点, 进入安全告警页面。 	
安全设备	平台安全设备日志量 Top10 排行。	RELATENCE
日志趋势	查询时间范围内日志趋势图。	

2.3 用户信息区域介绍

登录系统后· 在页面右上角的用户信息区域显示当前登录用户· 可在此区域进行修改用户信息、查看入门引导(仅限 admin)、查看小工具、 查看平台版本、退出登录等操作。





2.3.1 个人中心

用户名:	admin
手机号码:	
邮箱地址:	
登录密码;	修改座码
统一门户:	

点击页面右上角的用户名称,在弹出的下拉菜单选择"个人中心"可以查看或者编辑当前用户的个人信息。 点击登录密码处的<修改密码>,在弹出的修改密码对话框可以修改用户密码。

2.3.2 入门指引

点击页面右上角的用户名称· 在弹出的下拉菜单选择"入门指引"可以查看系统入门指引· 点击对应的蓝 色字体· 可以自动跳转到对应的功能界面进行配置。入门指引用于引导用户完成初始配置。 主要包括以下 几个方面:

- 企业信息:包括授权许可配置和组织架构配置。
- ◆ 网络环境 : 配置内网 IP、划分安全域、查看原始日志。
- ◆ 资产梳理: 导入资产和Web 业务系统、将重点监控的资产拖拽到拓扑中。
- ◆ 安全建模: 使用模型管理和黑白名单对告警精准度和误报进行调优。
- ◆ 安全监测: 监测全网安全态势并处置风险资产、查看并且处理告警、使用 Sherlock 对安全事件溯源。

VI.J	引导	×
对印度	用AILPHA大数据智能安全分析平台,请参考以下过程完善您的系统配置。	
0	企业信息	
	 请导入您所在组织的授权许可证。 请录入您的组织架构,并为每个分支机构分配安全管理员和安服人员。 	
2	网络环境	
	◎ 请配置您的企业内部使用的IP段并划分安全域。 ◎ 请确认您的流量和日志数据已接入AILPHA大数据,数据内容可以在原始日志中查看。	
3	资产梳理	
	 请导入您的资产和Web业务系统,可以使用自动发现功能发现某个安全域的在线资产。 请将需要重点监控的资产拖拽到拓扑中,依据网络结构指定您的防护预案。 	
4	安全建模	
	。 使用模型管理和黑白名单对告管精准度和误报进行调优。	
6	安全监测	
	 请持续监测全网安全态势,发现并处置风险资产,使用Sheriock对网络入侵和病毒事件追踪溯源 使用安全告誓直接查看详细的安全风险和举证信息。 	D, a

继续使用

2.3.3 小工具

支持使用小工具对指定内容生成二维码、 Base64 编解码和 URL 编解码。

点击页面右上角的用户名称·在弹出的下拉菜单选择"小工具"可以使用二维码等小工具。

ALM C. C.		x
THE THEFT IN NET		
in the second se	516-46	62-140.000
M.	9,4	

2.3.3.1 二维码

进入小工具页面后,选择**二维码**页签,左边输入框输入内容,点击<**生成二维码**>,右边展示生成二维码, 扫描二维码可获取输入内容。输入框最多支持 2950 字节生成二维码。



小工具 1. 选择二维码		3
Head 1773 HG 30 14bm Connectors Namp-Alevertarin Connect (Angle: 2013-tan-Cactae-Control insee age-Outrin-Organ Head 1773 HG 30 14bm Connector Namp-Alevertarin 1-bm -Aser Agent Mustikett 0 (Windows NT & T. WCM56) Agent Mission 253 28 (Orline) Head Control (2013) 2013 2013 Stature 251 28-bm - Cactard Type: mattpaidStorm-data Benders	<mark>● #####</mark> 3.点击	4. 生成二编码支持扫描获取输入内容

2.3.3.2 Base64 解码

进入小工具页面后,选择 Base64 解码页签。当左边输入框输入源内容,点击<Base64编码>,右边输入框中将会输出 Base64 编码内容,如图所示。

小工具 1.选择Base64解码	** &	×
	St E.	
(httk://explicit/supressing_landers)	A Read Street and	
2.输入源内容	3. 点击 () Sectore()) () Employed()	

当右边输入框输入编码后内容,点击<Base64解码>,左边输入框将会输出解码内容,如图所示。

□ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
4. 输入Base64解码内容 2. 1972年12日AND39日 1972日和日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日	
2.	кілі Евіс Віртики Кладили Ляркоми (Самір Закос Англійски Англійи) Барада Англійски Кладили (Самір Халана Англій) Барада Англійски Калана Англійски Калана Англійски Англійски Англій
	會入續码內容
3. 点击	

2.3.3.3 URL 解码

进入小工具页面后·选择 URL 解码页签;当左边输入框输入源内容·点击<URL编码>·右边输入框中将 会输出 URL 编码内容·如图所示;



ALO			. X
□ BB Dead 4585 (FLINE) 1.选择URL编码			
mp (H 72 Hi 10 RBH moudespicat (M)		Lie supermutations.	
2. 输入需要编码的内容	3. 点击	4. 输出URL编码内容	
	1.000 1000		
		Solution and the second s	
			- 4

当右边输入框输入编码后内容,点击<URL解码>,左边输入框将会输出解码内容,如图所示。

小工員 1. 洗择URL 解码	× Di
Desi Banefakti URUSHI	
4.输出URL解码内容	2. 输入URL 缘码内容
	3.燕蛮)

2.3.4 关于

点击页面右上角的用户名称· 在弹出的下拉菜单选择 "**关于**"可以查看系统版本信息· 包括软件版本和规则版本等。

A	LPHA大数据智能安全分析平台
\$	v3.5.3.2_release (2fb6e34f_222c92d)-2101280540 3.5.3.1
规则版本:	tag-v3.5.2.7
AlView版本:	v1.0.0(6f1ef819)

2.3.5 退出

点击页面右上角的用户名称·在弹出的下拉菜单选择"退出"可以注销当前用户。



3. 统一门户

3.1 功能简介

点击平台左上角的 logo A*UPHA**** · 进入统一门户页面。可以根据不同用户的喜好自定义统一门户信息 · 统一门户设置只和当前登录账号相关。

3.2 区块概要

非租户用户的统一门户菜单包含: 业务拓扑、态势感知、资产感知、威胁狩猎、威胁情报、通报预警、处置联动、 UEBA、 Ai 异常检测、运行监测,如下图所示。



租户用户的统一门户菜单包含: 态势感知(同 admin)、资产感知(同 admin)、威胁狩猎(同 admin)、威胁情报(同 admin)、通报预警(同 admin)、安全态势(新增大屏)、安全告警、资产管理,如下图所



⊼°



各模块详细说明见下表。

区块	说明	详细
菜单跳转	点击大屏上的图标可以快速跳转至相应 菜单页面。当某用户不具备某菜单权限, 菜单变灰不可点击跳转。	INTER ANTE ANTE ANTE
图标	 点击页面右下方的●・可以显示相关图标。 编辑菜单图标●:点击后,可对大屏名称和菜单进行编辑,也可对菜单进行顺序调整。 首页图标●:点击后,跳转至首页,若无首页权限,跳转至用户登录后显示的页面。 重置图标●:点击确认后,统一门户大屏恢复出厂状态(不包括大屏名称)。 确认图标●:点击后,保存编辑后的内容,大屏变成不可编辑状态。点击编辑图标后才会出现确认图标。 	



区块	说明	详细
	点击业务图标右上角编辑按钮时 · 可以进 行添加菜单操作 · 菜单总数不得超过 10 个 ·	_0_
添加菜单	 图标: 默认图标·点击可进行修改。 对应名称: 可自定义,可重复,必填。 对应菜单: 选择后不可重复选择。 对应菜单: 可许及,可定义,必值。 	
	 ▲ 内应路径: 可选择,可自定义,必填。 ◆ 主菜单栏和子菜单栏: 最多可添加两 个子菜单栏。 	
		<i>с</i> ,
Mi Mi		





4.1 概述

以缩略图的形式展示态势感知解决方案。

- ◆ 当用户为非租户时,包括:外部攻击态势、横向威胁感知、资产失陷态势、Web 业务系统态势、数据中心态势、 AI 异常分析、Sherlock 网络星空、资产态势感知、攻击者追踪溯源、资产威胁溯源、平台运行状态监测、 启用状态的重保方案、 Aiview 和仪表盘。
- ◆ 当用户为租户时,包括: 安全态势、 Sherlock 网络星空、 资产态势感知、 攻击者追踪溯源、 资产威胁 溯源。

4.2 外部攻击态势

4.2.1 功能简介

外部攻击态势大屏主要展示根据选择的时间范围内的来自互联网攻击的详情。

4.2.2 区块概要

选择"态势感知"菜单, 点击外部攻击态势页面查看外部攻击态势大屏。如下图所示。



数据源为安全告警, 数据流方向:外访问内, 整张大屏 5 分钟刷新一次。各模块详细说明见下表。



	说明	详细
时间控件/暂停	 ◆ 提供<暂停>按钮,支持轮播和暂停 暂停时,可鼠标点击切换任意模块 ◆ 时间范围: 默认显示最近 7 天。时间可 选择: 最近24 小时、最近 7 天、最近 30 天、本日、本周、本月。 	
告警数统计	 大屏左下角显示统计时间内符合条件的 (direction:外访问内)安全告警总告警 数、攻击源 IP 数(srcAddress 的种类数)、 攻击目的 IP 数(destAddress 的种类数)。 点击<总告警数据>,新打开安全告警页 面。 	ини ини ини ини ини ини ини ОБНИКО 27.755 RatSipto 171 RatSipto 122
告警地图展示	 可手动切换中国地图与世界地图,世界地图单位到国、中国地图单位到区域。 显示统计时间内所有源 IP 的地理分布,地图上进行攻击的路线模拟展示,目标点为局域网的显示系统配置区域。 	
攻击来源/攻击类型 排行	 攻击来源排行与攻击类型排行统计每 5 秒切换。 攻击来源排行: 统计时间段内攻击来源 IPTop5 · 点击 可显示 Top100 。点击某个来源 IP · 新打 开安全告警页面 · 条件带入所选时间+来 源 IP (srcAddress)信息+direction:10。 攻击类型排行: 统计时间段内攻击类型 Top5 (针对 name 的统计)·点击 可以显示 Top100。点 击某个告警类型 · 新打开安全告警页面 · 条件带入所选时间+告警类型 (name)信 息+direction:10。 	1921682219 145287 9876 54978 192168200 34390 19216810230 34390 112111 17838 8222 15123 **


区块	说明	详细
受攻击安全域排行/ 受攻击资产排行	 ◆ 每 5 秒切换。 ● 受攻击安全域排行: 统计时间段内被攻击安全域 Top5(针对 destSecurityZone 的统计)·点击 ● 可以显示 Top100。点击某个安全域名称,新打开安全告警页面,条件带入所选时间+安全域(destSecurityZone)信息+direction:10。 ● 受攻击资产排行: 统计时间段内被攻击资产 Top5(针对 destAddress 的统计,显示资产名称,无资产名称显示 IP),点击 ● 可以显示 Top100。点击某个资产名称,新打开安全告警页面,条件带入所选时间+目的资产 IP(destAddress)+direction:10。 	受攻击安全域排行 米の配 23 / 352 ・ -
攻击源国家排行/攻 击源区域排行	 每5秒切换。 攻击源国家排行: 统计时间段内攻击源国家 Top5(针对 srcGeoCountry 的统计)·点击 可以显示 Top100。点击某个攻击源国家·新打 开安全告警页面、条件带入所选时间+攻击 源 国 家 信 息 (srcGeoCountry)+direction:10。 攻击源区域排行: 统计时间段内攻击源区域 Top5(针对 srcGeoRegion 的统计)·点击 可以显示 Top100。点击某个攻击源区域·新打 开安全告警页面、条件带入所选时间+攻击 源 区域信息 (srcGeoRegion) 	東京国家排行 第二日 東京国家 34698 井田 19411 伊家斯 57 日本 5 10 5 小 34698 中国 19411 伊家斯 57 日本 5 小 5



区块	说明	详细
攻击链分布统计	 根据攻击链的统计,逆时针轮播展示,被展示阶段的区域高亮显示。中间的统计数与下面的折线图、实时告警事件根据攻击链的不同显示不同,当对应的攻击链统计数据为0时,该阶段的区域灰底,轮播直接跳过不显示。 中间统计数及统计图轮播展示并根据攻击链轮播的变化而变化,统计内容包含:境外告警数、境内告警数、影响资产数、影响网站数、攻击来源数、告警类型数。鼠标上移对应的告警数据,出现对应攻击链统计范围内的统计图。 境外告警数:显示境外攻击来源 IP Top10排行境内告警数:显示国内攻击来源IP Top10排行影响资产数:显示受影响资产(destAddress) Top10排行。 影响网站数:显示来源IP Top10排行。 攻击来源数:显示来源IP Top10排行。 攻击来源数:显示来源IP Top10排行。 车等类型数:显示未源IP Top10排行。 	

4.3 横向威胁感知

4.3.1 功能简介

关注企业网内部横向威胁态势· 分析内部安全域之间的威胁关系· 内部资产之间的攻击关系· 发现企业内部疑似被黑客控制的主机或内部员工的违规操作行为。



4.3.2 区块概要

ACCPHA	MINISTER									
172		and a second	11				00000000 1 3 909 1 2000000			10236 18 9,12 70 109,57 18 107,5 18 107,5 18
		accenting a		Jac -						
		and the second		YAN	i			WORTH A stang tom		120139
		and the second second						COMPLETE VALUE IN		13331
	1	35						VITE IS AND THE		3297
		1.00								794
		2	1		- 19 - 19 - 19 - 19 - 19 - 19 - 19 - 19			Colored To .	1.112	396
			e di l	1 1 1 2 2	and the manual Wolard			The second second		
W 880189	- Ber				AND DO BURDINGS			AND THEFT		
ANY INSTITUTE	10000		-		- STATIN		2224 2296			
AV 8011205		102.100.20.29	-	we want of some						
NAME AND ADDRESS OF AD		102 108 20.79 102 108 20.79	-	MESSI (MARK) WESSI (MARK)		and the second second	1000 0000			
05-12-000-00 05-12-000-00 05-12-000-00 05-12-000-00		No. 100.00.70 102.100.00.70 102.100.20.70 102.100.20.70	-	MERGY SCHOOL MERGY SCHOOL MERGY SCHOOL WICHNIGT SCHOOL			1114 11141 1474 1 1477 1 1477 1			
04-12 1000 40 05-12 1000 40 05-12 1000 40 05-12 1000 40 05-12 1000 40		1021 100.30.79 1021 100.30.79 1021 100.30.79 1021 100.30.79	Inter	WE NOT STATED		Market Market and Same	1000 0000 1000 0 1000 0 1000 0 1000 0 1000 0			

选择"态势感知"菜单,点击横向威胁感知页面查看横向威胁感知大屏。如下图所示。

数据源为安全告警,数据流方向:内访问内,整张大屏 5 分钟刷新一次。各模块详细说明见下表。

区块	说明	详细
时间控件/暂停	 提供<暂停>按钮,支持轮播和暂停。 暂停时,可鼠标点击切换任意模块。 时间范围:默认显示最近7天。时间可选择:最近24小时、最近7天、最近30天、本日、本周、本月。 	 ・場近7天 ・目 ・目 ・目
安全域关系网络	 无数据的时候显示暂无数据。 安全域网络图: 展示选择时间范围内不同内部安全域 之间的攻击关系(不展示同一安全域的 攻击效果)·按攻击次数排行最多显示 Top6。 攻击方向连线上显示攻击次数和正常 访问次数。 连线上鼠标点击时显示:攻击指向、异 常访问次数、正常访问次数、累计流量。 点击异常访问、新打开安全告警页面, 条件带入时间+来源安全域 	



区块	说明	详细
	(srcSecurityZone) 信息+ 目 的 安 全 域 (destSecurityZone) 信 息 +direction:00+appProtocol != dns。	
	 点击正常访问 · 新打开原始日志页面 · 条件带入时间 + 来源安全域 (srcSecurityZone)信息+目的安全域 (destSecurityZone) 信息 +direction:00+appProtocol != dns ° 	
	 鼠标点击安全域图标时显示:安全域名称、安全域描述。 	
	◆ 无数据的时候显示暂无数据。◆ 资产网络图:	4
	 支持自由布局和圆形布局切换·默认是 自由布局资产按风险评级展示不同的 颜色: 已失陷为红色·高风险为橙色、 低风险为黄色·健康为绿色·不在资产 管理的为蓝色;属于资产管理的 IP·显 示资产名称·其他显示资产 IP。 	
	 展示选择时间范围内不同资产之间的 攻击关系(不展示同一资产的攻击效 果)·按攻击次数排行最多显示Top60。 	172.31.0.50 192.168.3.79 异策访问:1次 《正常访问:0次 》, 累计法里:08
资产网络图	 连线上鼠标浮动时显示: 攻击指向、异常访问次数、正常访问次数、累计流量。 	- Micon
	点击异常访问·新打开 安全告警 页面· 条件带入所选时间+来源 IP(srcAddress)信息+目的 IP(destAddress)信息 +direction:00+appProtocol != dns。	test2 M操作集: E25頁 安全告部TOP3: 線低Unix SSH服务器架力域 解 51 次, 建築Unix FFP服务器架力域例 33 次, 建築業力域解成功 20 次 最近分常提生性的1: 2019-09-23 17:02:44 资产学 1: 1.1.2 安全編: Test2 溶合業型: 1:0米-Windows
	● 点击正常访问·新打开 原始日志 页面· 条件带入所选时间+来源	電気部務: 急却 酒任人: test themock
	IP(srcAddress) 信 息 + 目 的 IP(destAddress) 信 息 +direction:00+appProtocol != dns。 ● 点击实体圆点 · 浮动时显示:	



区块	说明	详细
	 圆点有对应资产时显示:资产名称、风险评级、安全告警 Top3(告警名称:事件数量)、最近异常发生时间、资产 IP、安全域(属于内部安全域显示所属安全域名称、不属于内部安全域但是属于内网 IP 时显示(内网)、不属于内部安全域也不属于内网 IP 时显示未分配)、资产类型、组织架构、责任人。 圆点无对应资产时显示:资产 IP、安全域(属于内部安全域显示所属安全域名称、不属于内部安全域但是属于内网 IP 时显示、分配)下不属于内部安全域也不属于内网 IP 时显示未分配)。 	192.168.198.203 资产ⅡP: 192.168.198.203 安全域:局域网 Sherlock
告警统计	 选择时间范围内内部告警数。 选择时间范围内内部支击者数(srcAddress)。 选择时间范围内内部受害者数(destAddress)。 平台安全域个数(与时间过滤无关)。 	PS部総合計算数 139891 PS部の加速数 24 PS部定法定数 20 安全地 253
被访问业务排行/ 被访问端口排行	 每个页面每 5 秒轮播 · 默认先轮播访问次数,再轮播流量;鼠标点击之后,暂停轮播,可查看完整数据。 被访问业务排行: 统计时间段内被访问业务(destAddress)的被访问次数和流量Top5、点击 显示Top100、有资产名称显示资产名称,无则显示资产IP。 点击条目,新打开原始日志页面,带入条件: 时间+数据流方向(direction)+目的IP(destAddress)+appProtocol != dns。 被访问端口排行: 	被访问业务排行 WEINBARE-177 16: 101 %4 112957 WEINBARE-175 100 %4 112957 WEINBARE-175 100 %4 112957 WEINBARE-175 100 %4 112957 WEINBARE-175 100 %4 102957 WEINBARE-175 100 %4 112997 10005 11297 10005 11297 10005 11297 10005 11297 10005 11297 10005 11297 10005 11297 10006 11297 <tr< td=""></tr<>



区块	说明	详细
	 统计时间段内被访问端口(destPort)的 访问次数和流量 Top5 · 点击 可以显示 Top100。 点击条目 · 新打开原始日志页面 · 带入 	Ŝ
	● 时间+数据流方向(direction)+目的端口 (destPort)+appProtocol != dns。	
内部攻击者排行/ 内部受害者排行	 每个页面每 5 秒轮播。 内部攻击者排行: 统计时间段内内部攻击者(srcAddress) Top5、点击 显示 Top100、有资产名称显示资产名称、无则显示资产 IP。 点击条目、新打开安全告警页面、带入条件: 时间 + 数据流方向 (direction)+来源 IP(srcAddress)+appProtocol != dns。 3)内部受害者排行: 统 计 时 间 段 内 内 部 受 害 者(destAddress)的 Top5、点击可以显示 Top100。 点击条目、新打开安全告警页面、带入条件: 时间 + 数据流方向 (direction)+目的 IP(destAddress)+appProtocol != dns。 	第回時期 100 168 35 15 1 20 170 102 168 35 15 1 20 170 102 168 35 200 1 3771 WEEBERSE rhang.com 3 273 1 1 3 20 3 HESSELARKE 284 WEEBERSE rhang.com 1 20 170 NUTRREE rhang.com 1 30 3 7117 7 94 198870 396
最新安全告警事 件	 滚动展示,选择时间范围内最近 50 条告警数据:攻击时间、内部攻击者:srcAddress。内部受害者:destAddress,威胁等级,攻击类型:name。 鼠标放上去,暂停滚动,显示所指向信息 点击条目,新打开安全告警页面,带入条件:eventId+时间范围。 	AN EXTENSION NUMBER AND ADDRESS AND ADDRESS AD



区块	说明	详细
安全域/资产威胁 方向	 安全域威胁方向: 显示源安全域>目的安全域的攻击次数和访问次数;同一安全域相互攻击的数据不过滤 默认显示 Top5 · 点击 显示 Top100 ° 鼠标放上去 · 暂停轮播 · 显示所指向信息。 点击条目 · 新打开安全告警页面 · 带入条件: 时间范围+数据流方向(direction):00+来源安全域(srcSecurityZone)+目的安全域(destSecurityZone)+目的安全域(destSecurityZone)+appProtocol != dns ° 资产威胁方向 显示源 IP>目的 IP 的攻击次数和访问次数 有资产名称显示资产名称 · 无则显示资产IP 默认显示 Top5 · 点击 显示 Top100 ° 鼠标放上去 · 暂停轮播 · 显示所指向信息。 点击条目 · 新打开安全告警页面 · 带入条件: 时间范围+数据流方向(direction):00+来源 IP(srcAddress)+ 目 的IP(destAddress)+appProtocol !=dns ° 	



	区块	说明	详细
	内部攻击类型分 布/内部攻击趋势	 内部攻击类型分布: 选择时间段内,内部安全告警分布 Top10。 点击某图例,环形图过滤掉该攻击类型 数据。 鼠标放上去右边图例,环状图联动显示 告警类型以及百分比。 内部攻击趋势: 显示选择时间段内的告警趋势。 	/// 内部攻击类型分布 ● ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●
4	1.4 资产失陷病	态势	С. ;;

4.4 资产失陷态势

4.4.1 功能简介

资产失陷风险态势: 数据流方向为内访问外的安全告警事件。即数据源为: 安全告警, 数据流方向: 内访 问外。

4.4.2 区块概要

选择"态势感知"菜单,点击资产失陷态势页面查看资产失陷态势大屏。如下图所示。



数据流方向:内访问外,整张大屏5分钟刷新一次。各模块详细说明见下表。 数据源为安全告警,



区块	说明	详细
时间控件	时间范围: 默认显示最近7天。时间可选择: 最近24 小时、 最近7天、最近30天、本日、 本周、本月。	 財師范徴: 最近7天 届近24小时 最近7天 最近7天 最近30天 本日 4日 100 198 本月
告警地图展示	 地图可以手动切换中国地图与世界地图, 世界地图单位到国、中国地图单位到区域。 统计时间内,所有攻击源 IP 的地理分布显示在地图上,并进行攻击的路线模拟展示。 	
告警数统计	 ◆ 外连主机数: 统计时间内 · 外连主机数的 种类统计 (srcAddress)。 ◆ 外连告警数: 统计时间内外连告警数的统 计。 	外连主机数 <i>163</i> 外连告常数 1636660



区块	说明	详细
外连域名排行/外 连目的 IP 排行/外 连资产排行	 每个页面每 5 秒切换轮播 · 鼠标点上去 · 暂停轮播 · 可查看完整数据 外连域名排行 : 统 计 时 间 段 内 攻 击 外 连 域 名 (requestDomin) Top5 · 点击 显示 Top100 ° 点击条目 · 新打开安全告警页面 · 带 入 条 件 : 时 间 + "direction:01 OR appProtocol:dns" + dns 请 求 域 名 (requestDomain) ° 外连目的 IP 排行 : 统计时间段内攻击外 连目的 IP (destAddress) Top5 · 点击 显示 Top100 ° 点击条目 · 新打开安全告警页面 · 带 入 条 件 : 时 间 + " direction:01 OR appProtocol:dns" + 目 的 IP(destAddress) ° 外连资产排行 : 统计时间段内攻击外 连来源 IP (srcAddress) 的 Top5 · 来源 IP 如果 是资产 · 则显示资产名称 · 点击 显示 不 Top100 ° 点击条目 · 新打开安全告警页面 · 带 入 条 件 : 时 间 + " direction:01 OR 	小臣成名牌行 Www.waqenfoodp/#gapocallipipocallipipo 5/471/402 gato cache 997998 shaftead m 16236 caseteo actes 937988 shaftead m 16236 caseteo actes 937988 shaftead m 16236 caseteo actes 13758 caseteo actes 13759 staseteo actes 13759
外连目的国家排 行/外连目的区域 排行	 ● 每个页面每 5 秒切换轮播,鼠标点上去, 暂 停轮播,可查看完整数据。 ◆ 外连目的国家排行: ● 统 计 时 间 段 内 外 连 目 的 国 家 (destGeoCountry) Top5 · 点击 □ 显示 Top100。 	小学 外连目的区域排行 ● RMM 1211403 RT 90975 13 03570 13 6505 14 1312



区块	说明	详细
	 点击条目·新打开安全告警页面·带入条件:时间+"direction:01 OR appProtocol:dns"+目的国家(destGeoCountry)。 外连目的区域排行: 统计时间段内外连目的区域(destGeoRegion)的Top5·点击可以显示Top100。 点击条目·新打开安全告警页面·带入条件:时间+"direction:01 OR appProtocol:dns"+目的区域 	小班目的國家耕行 1000000000000000000000000000000000000
最新外连事件	 (destGeoRegion)。 滚动展示选择时间范围内最近 50 条告警数据: 攻击时间、外连源 IP、远控地址(appProtocol 如果是 dns 就显示外连域名,不是则显示外连目的 IP)、威胁等级、攻击类型。 鼠标放上去,暂停滚动,显示所指向信息。 点击条目,新打开安全告警页面,带入条件: eventId+" direction:01 OR appProtocol:dns" +时间。 	
外连安全域排行/ 外连趋势	 每个页面每 5 秒切换轮播。 外连安全域威胁方向: 显示统计时间范围内 · 外连资产安全域(srcSecurityZone)Top5 · 点击 显示 Top100。 鼠标放上去 · 暂停轮播 · 显示所指向信息。 点击条目 · 新打开安全告警页面 · 带条件:时间+"direction:01 OR appProtocol:dns" + 来源安全域(srcSecurityZone)。 外连趋势:显示时间范围内外连告警数趋势。 	外连安全域名排行 #39飛 1 354356 12 29600 1 22679 9 5623 16 2050 ** **



区块	说明	详细
可疑外连 Top10/ 外 连 告 警 类 型 Top10	 每个页面 5s 切换轮播。 可疑外连 Top10: 选择时间范围内,可疑外连来源 IP 排行 Top10,目标 Top3,以关系图方式显示来 源 IP 对目的地址的连接关系。 外连告警类型分布Top10: 选择时间段内,外连安全告警分布 Top10。 点击某图例,环形图过滤掉该攻击类 型数据鼠标放上去右边图例,环状图 联动显示告警类型以及百分比。 	

4.5 Web 业务系统态势

4.5.1 功能简介

数据大屏直观展示 Web 业务系统态势,实时统计分析当天 Web 业务系统态势相关数据,包括进出流量、访问量、攻击量、网站区域访问量、访问区域、访问 IP 排行、访问/攻击路线、详细攻击信息、网站攻击趋势、被攻击网站排行、攻击 IP 排行、攻击类型排行等数据。

4.5.2 区块概要

◆ 选择"**态势感知**"菜单, 点击 Web 业务系统态势页面查看 Web 业务系统态势大屏。如下图所示。





 ◆ 点击大屏中被攻击网站排行任意一个网站 · 进入该网站实时监控 · 仅查看该网站Web 业务态势 · 如下 图所示 ·

A&LPHA www.mit	ieba.com.co	n							
ANA BERRUCH								W BEENDRUHT	
63.65 ···	100000000 1000000000000000000000000000				A.				
	erineken EM				Ŧ				
								W MAPPER	
									20
								-	28
	· Second								28
	111	B.D.DOW	BRANCE AND	0.205 F	BIRLING.	2005	No.		
		B-110-4151	912 10441 10191 140 441	NAME AND ADDRESS OF THE OWNER	fentes (webs)	9月1人市市 9月1人市市			
WW 动用PP维行	B	8-100-255	#10 100 4 4 1	www.alibaba.com.cn www.alibaba.com.cn	Andrea Tendera	MEAMS MEAMS	-	····	
	28	ANY PRISER	12.07				Contraction of the last of the	BY SEED	10004
and the second s	85			• • • •	No.				
	-29								
		Contraction of the local division of the loc	and the second s		204401004	101030-016-0	and an in the second		

以上区块概要信息说明参见下表,以下各区块均实时展示当天数据。

区块	说明	详细
进流量/出流量 访问量/攻击量	大屏左上方实时统计当天的进出流量、访问 量、攻击量。	
网站区域访问量	以不同颜色展示区域访问量数据。	/// 网站区域访问量 * 7/6628
网站区域访问量排行	实时统计各区域访问量·展示访问量最多的 10 个区域及对应访问量。	



区块	说明	详细
访问 IP 排行	实时统计访问 IP · 展示访问量最多的 5 个 IP 及对应访问量 · 点击更多显示Top50。	がの P 時行 ドロ 180 22.2 ドロ 180 22.2 ドロ 180 22.2 ドロ 180 22.2 ドロ 185 25 105 ドロ 185 25 105 ビロ 185 25 105 ビロ 185 25 105 ビロ 185 ビロ 185 185 185 185 185 185 185 185 185 185 185
访问/攻击路线	 ◆ 实时展示监控地区的访问/攻击路线,蓝 ●路线表示正常访问路线,橘色路线表示 示攻击路线;监控地区设置请查看"系 统管理>配置管理",如图,监控地区为 浙江省。 当没有告警事件发生时,无橘色路线。 	
当天详细攻击信息	 ◆ 展示当天最近 10 条详细攻击信息。 ◆ 当无告警事件发生时 · 该区块显示暂无数据。 	NUMBER OF STREET, STRE
网站攻击趋势	时序图分析网站攻击趋势 · 包含访问分析、 流量分析。	
攻击网站排行	 展示被攻击次数(告警事件发生)最多的 5个网站·点击更多展示Top50。 当无告警事件发生时·该区块显示暂无数据。 单击其中某一个攻击网站·进入该站点实时监控。 	### 板攻击网站排行 日 10日 25名 合際政 21 www.idbate.com.ct 84 82 Hays Networkstate.com.ct 82 93 (122.14.161.144) 84 14 www.idbate.com.ct 28 15 (action load?rebbates.com) 14
攻击 IP 排行	 ◆ 展示攻击次数最多的 5 个攻击 IP (告警事件) · 点击更多展示 Top50。 ◆ 当无告警事件发生时 · 该区块显示暂无数据。 	秋田 190222 182 WEI 180222 182 WEI 180441 28 WEI 189441 28 WEI 189441 28 WEI 189441 28 WEI 189441 28 WEI 199441 28 WEI 199441 28 WEI 199441 28



区块	说明	详细
攻击类型排行	 展示攻击次数最多的 5 个攻击类型(告警事件攻击类型)·点击更多展示 Top50。 当无告警事件发生时 · 该区块显示暂无数据。 	パレマカ美型排行 50000 1017 おままが 150000 1010020300 400 101100020300 400 101100020300 400

4.6 数据中心态势

4.6.1 功能简介

大屏页面使用 3D 逻辑安全域展示内部网络系统发生的安全态势·用户能进行自定义的安全域划分·并根据具体安全域的告警与漏洞信息进行统计。

4.6.2 区块概要

选择"态势感知"菜单,点击数据中心态势页面查看数据中心态势大屏。如下图所示。

A&LPHA REPOSE	;	Tel 1							(6)
	8				av abstit	12.9			
		nulo7	110 101	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		NACE OF COMPANY	1012222 1173380 10142 2014-25-12:0631221	(E) (E) (B)(E) (C)(E)	1 Mail
			10	d Heale					
		-	in in in in in	159 847) 847 5197086717341779		winaut	10 .	•	per l'
The second se		-			. nérž				
AV 158		1日本市場							
######################################	29568				-	-	STARS.	-	-
100 M	30400		1985						
2 TE S NO. Alimet		OF TRANSPORTS	1000		09-T0-0931-80	100.022	1007168.11.108	nalez	
system)		10016-10016-100-00			06-19-06-12-29	165,2,2,2	1962/100.11.108	neled	
Present	(299	IN INCOMPOSE			09-19 00-31.38 09-19 00-31.38	180,2,2,2	P02.166.11,106	nubel:	M (

以上区块概要信息说明参见下表,数据源为安全告警,大屏整体2分钟刷新一次。



区块	说明	详细
时间控件	 时间范围:默认显示最近7天。时间可选择:最近24小时、最近7天、最近30天、本日、本周、本月。 默认收起,点击 	时间范围:最近7天 最近24小时 最近7天 最近30天 本日 本周 本月
拓扑图	 默认有四个区域:核心网络区、业务核心区、 模拟监控区、终端接入区。 点击 . 弹出安全域组配置: 选中任一区域可修改区域名称,可添加 /移除平台安全域至区域。 同一安全域不可重复添加。 配置安全域组后,拓扑图上该区域显示 总资产数量、所选时间范围内告警数 量、漏洞数。 无配置安全域组时显示资产:0告警: 0漏洞:0° 	
	Contraction of the contraction o	



区块	说明	详细
攻击者基本信息/ 攻击者画像信息	 ◇ 攻击者基本信息: ● 默认显示实时场景分析中第一条记录中攻击者 IP 对应的相关信息:黑客 IP、信誉度、来源地、情报信息、攻击类型、危险等级、最近攻击时间。 ● 点击黑客 IP 旁边的● . 可添加联动策略至 "资产管理>处置联动>联动策略整。 ◇ 攻击者画像信息 ● 取击者画像信息 ● 型、放击 IP 在全时间段范围内攻击者 IP 对应的相关信息。 ● IP 反查:攻击 IP 在全时间段范围内攻击的 destAddress 个数。 ● IP 主要攻击类型:攻击 IP 在全时间段范围内的攻击类型。取事件数量最多的10个。 ● 处置建议:实时场景分析中第一条记录对应的处置建议。 ● 攻击资产显示该 IP 所有时间段的攻击网站(destAddress)Top10。 	
告警	默认显示: 安全告警Top5 点击 显示 Top100	W SIS Illightenexcy SSSS Net 90339 Visit 2993 ryset 1461 FRenked (293



区块	说明	详细
资产告警/安全域 告警	 每个页面 10s 切换轮播。 资产告警: 资产 IP、告警次数,漏洞。 默认显示: Top5 点击 显示 Top50。 安全域告警: 显示资产所属安全域、告警次数(资产为 srcAddress 或者 destAddress)、漏洞数(资产为受害主机)。 资产所属安全域告警次数排行。 	
实时场景分析	 统计时间段内按时间倒序显示 Top50: 攻击时间、攻击者、被攻击目标(destAddress)、攻击类型和危险等级。 进入数据中心态势大屏时,默认展示实时场景分析中第一条记录中事件的弹框。 选中某条事件,攻击者基本信息、攻击者画像显示该指定事件攻击者信息(srcAddress)以及事件弹框。 	AN VERSION DESCRIPTION OF A DESCRIPTION

4.7 AI 异常分析 4.7.1 功能简介

通过模型管理支持针对不同类型的数据采集与处理(全部日志 SOC 接收解析后统一放入原始日志中)·配 置对应的监控模型策略(规则模型、统计模型、关联模型、 AI 模型、其他)及告警策略(处理结果统一放 入安全事件中,当模型中标记为安全告警时, 放入安全事件中同时放入安全告警中)。在元数据统一管理 下, 用户可以根据不同的关注领域灵活操作, 包括对数据处理逻辑的新增、删除、修改、查询、启动、停 止等。

4.7.2 区块概要

选择 "态势感知"菜单, 点击 AI 异常分析页面查看 AI 异常分析大屏。如下图所示。



	例でExponentialSmoothing (19行為単	
	44xx8 34xx8 74xx7	
W. WEXNER BREDOKTAL SERVICE PARA		
патанцатосямона, а набного А инероказанская алекта маталимся, инероказана, при в:15	p4-87 54-88 54-32 54-33 56-31 56-32 64-37 64-30 05-03 <t< td=""><td></td></t<>	
	94 64 67 64 69 194 23 04 25 04 23 04 23 34 24 54 27 04 10 05 01 05 06 747 192925932345 28	

大屏 5 分钟刷新一次 · 各模块详细说明见下 :

区块	说明	详细
时间控件	时间范围: 默认收起组件,默认显示最近 30 天。 时间可选择:最近 24 小时、 最近 7 天、最近 30 天、本日、本周、本月。	时间范围: 最近30天 💼 🔹
设置	 点击右上角 · 弹出场景设置。 一共可配置四个场景: 选择模型、下拉单选模型列表中的 AI 模型、支持模糊查询。 选择算法、下拉单选对应 AI 模型中包含的算法、支持模糊查询。 场景不能重复、4 个场景中不能出现某个场景的模型和算法与其他场景完全一致;场景不足时可以空缺。 	
暂停按钮	支持页面暂停/开启轮播。	



区块	说明	详细
区域 1 场景缩略图展示	 显示配置的 4 个场景模型,大屏从上至下依 次轮播 4 个场景,用户超过 30 秒不点击时,自动进行场景轮播,每 20s 换一个场景,高 亮显示。 点击缩略图切换对应场景展示内容到"区域 2"和"区域 4"。 轮播时继续当前场景向后轮播。 5 分钟刷新数据时,轮播从第一个场景重新开始。 	网络会话数异常检测-E 44++6 34++6 14++6 14++6 14++6 14++6 14++6 14++6 14++6 14++6 14++6 14++6 14++6 14++6 14++6 14++6 12++11 12++11 12++11 12++11 12++11 12++11 12++11 12++11 12++11 12++11 12++11 12++11 12++11 12++11 12++11 12++11 12++11 12++11 13++6 15++6 14++6 15++6 14++6 14++7 14++7 14++7 14++7 14++7 14++7 12++7 14++7
区域 2 场景模型、算法 介绍	 展示每个场景的 AI 模型名称,模型描述。 该模型使用的算法名称,算法描述、相关专利 和论文。如果没有,该部分不显示。 	W
区域 3 AI 分析示意图	从左到右流动效果代表 AI 实时计算过程。 形状说明: ◆ 服务器图标:表示监控指标来源。 ◆ 算法图标: 表示算法特征。 ◆ 折线图图标:表示分析结果。	



区块	说明	 详细
区域 4 分析结果展示	 AI 分析算法结果: AI 分析算法结果.标题为"某算法分析结果"。 曲线支持滚轮时间缩放.时间序列数据过多时需要放大时间查看详情.缩放不影响红色异常点显示。 历史数据中部分为训练数据时.模型训练数据与异常检测数据用竖线隔开。 AI 算法辅助评分柱状图: AI 算法辅助评分柱状图: AI 算法辅助评分柱状图.标题为"某算法标准差偏离"等.柱状图中异常点对应柱子为红色。 鼠标浮动在辅助评分的标题上方时提示对应评价参数描述。 折线图和柱状图时间轴范围、布局保持一致。 当返回结果无数据或接口数据异常时提示"AI模型正在训练中"。 当时间序列不适合算法计算时提示"AI模型数据不适合使用当前算法进行训练"。 	
区域 5 多场景异常信息 综合分布	 泳道图展示 4 个 AI 异常分析场景的异常分 布情况 异常等级分为 3 级: 1 黄色 一般 2 橘黄 中度 3 红色 严重 0 透明 无异常 时间间隔 最近24 小时: 共45个间隔 · 10 分钟一 个间隔。 最近 7 天: 共45 个间隔 · 70 分钟一个间 隔 · 级别均值向上取整。 	



区块	说明	详细
	 最近 30 天: 共 45 个间隔 · 300 分钟一个 间隔 · 级别均值向上取整。 	
	 ■ 鼠标浮动在标题上方时提示:场景、时间、异常等级。 	°

4.8 Sherlock 网络星空

4.8.1 功能简介

夏洛克(Sherlock)帮助用户透视整个网络·追踪网络实体的连接关系·发现访问行为的蛛丝马迹。大数据标签画像分析寻找相似的受害团体和黑客组织·AI算法发现观测指标中隐藏的未知威胁·情报、弱点信息辅助安全事件的追根溯源。

4.8.2 区块概要

选择"态势感知"菜单·点击 Sherlock 网络星空页面查看 Sherlock 大屏· 支持Tab 切换· 有立体· 平面· 球面三个Tab 页· 默认展示立体效果。切换至平面·如下图所示。



数据源: 原始日志, 区块概要信息说明参见下表。



区块	说明	详细
	◆ 根据起始时间、结束时间到原始日志索引中取 destAddress+srcAddress 事件数量最多的 800 个 IP。	
	◆ 圆点有对应资产时: 根据资产风险等级显示相应的 颜色。	8
	 ■ 己失陷:红色 ■ 喜风险:橙色 	
	● 低风险:黄色	
	● 健康: 绿色	
总体	● 资产为 Web 服务器时 · 圆点标记为 W	
	 ● 资产为邮件服务器时 · 圆点标记为m ● 资产为 DNS 服务器时 · 圆点标记为 D 	
	◆ 圆点无对应资产:	
	● IP 属于内部安全域或内部 IP 时显示浅蓝色。	
	● IP 不属于内部安全域 · 也不属于内网 IP 时显 示深蓝色。	
	● IP 是情报 IOC 且类型是黑客组织、监管单位 时 · 显示情报标记 ; 其他类型显示深蓝色。	
	搜索框中输入待追踪的网络实体 IP · 点击<搜索>或者是	
输入框	回车键·跳转至"威胁感知>Sherlock"·租户只能查询	1002 Auro
	安全域过滤后的 IP。	
图示按钮	点击图示按钮 · 显示不同的图标与资产类型和情报类型的对应关系。	Mitanja Mitanja Dosavis Listavo Satavo
	◆ 点击实体圆点 · 浮动时显示:	
	圆点有对应资产时显示:资产名称、风险评级、	
实体详情	安全告警 Top3(告警名称:事件数量)、最近	192.168.54.189
	全域时显示安全域名称,不属于内部安全域但	중·全域: 地域的 Sheriock
	是属于内网 IP 时显示 (内网)·不属于内部安	
	全域也不属于内网 IP 时显示未分配)、资产类	Innan
	型、钮�����、贡仕人。当没有相关信息时, 该项内容不显示。	



区块	说明	详细
	● 圆点无对应资产且为浅蓝色时显示: IP、安全 域(属于内部安全域时显示安全域名称 · 不属 于内部安全域但是属于内网 IP 时显示(内 网))。	116.196.80.246 199.87.295 201 199.87.295 201 199.87.295 201 199.87.97 199.87.97 199.87 199.77
	● 圆点无对应资产且为深蓝色时显示: IP·安全 域: 未分配 · 地理位置: 国家-省-市 · 例如"中 国-浙江-杭州" 。	
	 圆点为情报时显示:情报类型,情报标签,置 信度,地理位置,组织名称,运营商。当没有 相关信息时,该项内容不显示。 	
	◆ 点击 Sherlock · 可跳转至 " 威胁感知>Sherlock "页 面 · 带条件: IP •	6

切换至立体, 查看 Sherlock 大屏的立体效果。图标之间的连线会不定时随机高亮, 有对应资产时, 图标下 方显示资产名称, 无对应资产, 情报则显示 IP。资产颜色同平面效果, 情报都为深蓝色。鼠标移动时, 立 体图旋转效果停止, 鼠标停止移动, 5s 后继续开始旋转,如下图所示。



切换至球面, 查看 Sherlock 大屏的球面效果。有对应资产时, 图标下方显示资产名称, 无对应资产, 情报则显示 IP。如果是情报中的黑客组织,监管单位或资产类型为 Web 服务器, 邮件服务器, DNS 服务器, 则同平面效果中图标一致。除此之外, 全部展示主机图标。鼠标点击某个卡片时, 相关联的线高亮。同样, 点击线时, 相关的卡片高亮。



如下图所示。



4.9 资产态势感知

4.9.1 功能简介

感知资产风险情况。

4.9.2 区块概要

选择"态势感知"菜单,点击资产态势感知页面查看资产态势感知大屏,如下图所示,当用户为租户时, 资产态势感知大屏只显示安全域过滤后的 IP 对应的资产。



区块概要信息说明参见下表。



区块	说明	详细
总体	 ◆ 资产管理下所有资产。 ◆ 首先以风险评级(已失陷、高风险、低风险、健康)排序,其次是资产 ID 倒序排列。 ◆ 默认显示三行, 滑动鼠标可以往下滚动。 ◆ 大屏整体 5 分钟刷新一次。 	-
标签	 ◆ 默认显示全部资产 · 点击根据标签过滤资 产。 ◆ 默认展开 · 点击 	全部 全部 有政主资产 7天 N 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
风险评级分布	 ◆ 大屏顶部条状图显示不同风险评级资产所 占百分比: 风险资产/资产管理所有资产。 ◆ 鼠标悬停此处会显示具体分布信息。 	(j.
	 ✓ 缩略图左上角显示资产名称·右上角是快速跳转链接: Sherlock·资产威胁溯源·点击图标可跳转至相应页面·带条件: IP。 ✓ 详细信息: 7 天告警: IP 作为 srcAddress 或者是destAddress 的最近 7 天状态为"未处理"的告警数据;有数据时为黄色高亮·没有数据置灰。 	パイリート パリート パリート
缩略图资产信息	 本日日志: IP 作为 srcAddress 或者是 destAddress 的本日日志数量;日志量监 控开关关闭时显示;有数据时为蓝色 高亮·没有数据时置灰。 漏洞: IP 受害主机的漏洞数;有数据时 为蓝色高亮·没有数据时置灰。 本日流量: IP 作为 srcAddress 或者是 destAddress 的本日流量;流量监控开关 	新小学校 新小学校 新小学校 新小学校 新小学校 新小学校 新学校 100.1.2.3
	 关闭时显示;有数据时为蓝色高亮・ 没有数据灰掉。 资产评分:资产管理页面打开资产评分・缩略图显示资产评分・替换掉本日 流量;有数据时为蓝色高亮・没有数据 	APTE! 7天防衛 本日白志 編列 本日法里 0 0 0 0 0 - - - - - - - - - - - - - -



区块	说明	详细
	灰掉; 资产评分详见资产管理模块(没	
	有实时更新)。	
	 ● 其他: 资产 IP、资产类型、资产重要性、 	
	安全域、责任人·同资产管理资产信息。	8

4.10 攻击者追踪溯源

4.10.1 功能简介

攻击者可视化溯源分析大屏·为安全运维人员提供包括攻击行为分析、团伙分析、攻击取证信息、攻击趋势、攻击手段·攻击影响范围等信息;以攻击 IP 为中心·对该 IP 产生的告警类型、所攻击的受害主机 IP·以及使用攻击手段类似相似 IP 等信息进行展示。支持任意攻击者信息查询·可生成详细的攻击者溯源报告,并能够一键导出报告。

4.10.2 区块概要

选择"态势感知"菜单,点击攻击者追踪溯源页面查看攻击者追踪溯源大屏,如下图所示。



以上区块概要信息说明参见下表·以下各区块均实时展示当天数据。当用户为租户时·只显示安全域过滤 后的 IP 及过滤后各区块的数据。



区块	说明	详细
攻击 IP	 ◆ 默认溯源最近一次安全告警事件中的攻击者 IP;攻击 IP列表显示安全告警数 Top10 的攻击者 IP · 点击选择 IP 即可。 ◆ 支持手动输入 IP · 点击搜索 · 查询出相应数据。 	I文击IP: 192.168.58.105 192.168.58.105 10.0.0.0 10.11.0.1 172.16.0.0 172.16.13.67 172.17.0.0
添加联动策略	 快速添加联动策略: 若没有添加联动设备或者是设备未连接,点击< 方连接状态的联动设备,点击添加,提示操作成功,添加联动策略至"资产管理 处置联动>联动策略",且●变成●, 点击●快速删除联动策略。 	() () <
时间控件	时间范围: 默认显示最近 7 天。时间可选择: 最 近24 小时、 最近 7 天、最近 30 天、本日、本周、 本月。	 財詞范囲: 最近7天 最近24小时 最近7天 最近30天 本日 本月 本月 () 新時5056×1002 () 新時5056×1022 () 新時5056×1022



区块	说明	详细
下载报告	 ◆ 点击● · 下载选择时间范围内的攻击者取证报告。 ◆ 点击● 收起、展开左侧 IP 查询框时间控件等组件。 	
拓扑图	显示选择时间范围内: ◆ 该攻击者(srcAddress)的相似 IP Top20 ◆ 告警类型(name) Top20 ◆ 攻击主机(destAddress) Top20	ALL
攻击者基本信息	 攻击者 IP 该 IP 地理信息 经纬度 运营商 情报信息 没有值则显示暂无 	
攻击对象情况	选择时间范围内攻击者攻击对象及攻击次数 的 Top20。	双击対象情况 202.101.172.35 67.1 192.168.54.189 163 193.166.255.170 11.6 192.168.198.203 52 104.239.157.210 29
攻击取证	 取得为前 2000 条数据中的聚合20 条。 显示时间、攻击链、攻击 IP、攻击对象、攻击结果(显示指定攻击 IP 对应的安全告警数据,包括开始时间、攻击链、攻击源地址、目的地址、攻击事件名称等)。 	
趋势分析	选择时间范围内攻击者访问趋势与攻击趋势。	20時分析 ● 00000 m 105500 1000 1000 1000 1000 1000 1000 10



区块	说明	
告警分布	 ◆ 选择时间范围内攻击 IP 攻击次数 Top20 的安 全告警。 ◆ 鼠标指向告警名称 · 显示 name:攻击次数。 	新設定相当社会主 新設定相当社会主 新設:photoMillional Abuse.com/comag.emax FBI Gameov FBI Gameov Anubis水(応通讯

4.11 资产威胁溯源

4.11.1 功能简介

资产威胁溯源大屏从资产的角度考虑,为安全运维人员提供包括被攻击行为分析、影响资产范围分析、攻击取证信息等;可呈现被访问趋势、被攻击趋势、被攻击手段、资产状态,资产评分等信息。帮助用户分析现有资产安全状况,了解资产被攻击详情,帮助事后取证溯源。

4.11.2 区块概要

选择 "**态势感知**"菜单,点击资产威胁溯源页面查看资产威胁溯源大屏,如下图所示。当用户为租户时,只显示安全域过滤后的 IP 及过滤后各区块的数据。



区块概要信息说明参见下表。



区块	说明	详细
资产 IP	 ◆ 默认溯源攻击次数最多的资产 IP;资产 IP列 表显示安全告警数 Top10 的资产 IP·点击选择 IP 即可。 ◆ 不支持手动输入 IP。 	 第产中: 193.166.255.170 193.166.255.170 193.166.255.170 104.239.157,210 142.0.36.234 143.215.130.33 148.81.111.111 159.253.145.242
时间控件	时间范围: 默认显示最近 7 天。时间可选择: 最 近24 小时、 最近 7 天、最近 30 天、本日、本周、 本月。	时间范围: 最近7天 (1) 最近24小时 最近7天 最近30天 本日 本周 本月
收起/展开组件	点击————————————————————————————————————	
拓扑图	 显示选择时间范围内如下信息: 该资产(destAddress)的相似 IP Top10。 告警类型(name)Top10。 攻击来源(srcAddress)Top10。 弱点 TOP10。 	Undeclared Selected BURE AVIT
攻击者基本信息	 安全域: 没有值显示暂无。 资产状态: 取风险评级, 没有值显示暂无。 资产 IP: 没有值显示暂无。 资产评分: 需要在"资产管理>资产管理>设置"中打开资产评分,此处才显示,且每天凌晨更新一次;关闭则显示暂无。 资产类型: 没有值显示暂无。 资产名称: 没有值显示暂无。 	



区块	说明	详细
攻击源排名	选择时间范围内该资产的攻击源 IP 及攻击次数 的 Top10。	1192.168.58.105 124
攻击取证	 取得为前 2000 条数据中的聚合20 条。 显示时间、攻击链、攻击 IP、攻击对象、攻击结果(显示指定攻击 IP 对应的安全告警数据:显示指定攻击 IP 对应的安全告警数据;包括开始时间、攻击链、攻击源地址、目的地址、攻击事件名称等)。 	
趋势分析	选择时间范围内攻击者访问趋势与攻击趋势。	11日 11日 11日 11日 11日 12日 12日 12日
告警分布	 ◆ 选择时间范围内资产 IP 受攻击次数 Top10 的 安全告警。 ◆ 鼠标指向告警名称 · 显示 name : 攻击次数。 	/// 告留分布 fitsec.com

4.12 平台运行状态监测

4.12.1 功能简介

AiLPHA 大数据智能安全分析平台运行状态监测 · 凸显 AiLPHA 具备来自全网安全设备的多元异构数据接入能力 · 打破数据孤岛 · 内置丰富的规则和知识库 · 利用多种计算分析引擎和安全分析工具 · 可长期保障用户全网资产安全 · 实时告警威胁情况。同时平台具备良好的数据存储和计算性能 · 支持动态扩容缩容 · 根据需求灵活配置。包含安全运营、安全监测、流量监控、 AiLPHA 引擎、日志吞吐量监控、平台性能监控、磁盘容量监控/运维告警模块。



4.12.2 区块概要

A & LPHA 大数据检验安全分析平台运行状态临界 /// 日志書吐側論控 BEAUER THEFT ALPHALSUEI 🚺 📋 S 本向訪問 **出办工**9 36.2万 **V***22 言律物育 扫集業 164 951 WEEKP 326 8 111 鬼巢监控 自能出院

选择"态势感知"菜单,点击平台运行状态监测页面查看平台运行状态监测大屏,如下图所示。

区块概要信息说明参见下表。

区块	说明	详细
安全运营	 ▼台运行天数。 本周告警:点击本周告警跳转到"安全分析 >Investigation>安全告警"页面,条件:时间本周。 待办工单:该用户待处理工单,点击跳转至 "安全运营>工作台"。 通报:开启状态的通报,点击跳转至 "安全运营>工作台"。 	W 安全返营 ALPHA已运行 0 0 2 0 天 本商告報 待力工単 通数 6 1 4 3 0 0
安全监测	 已失陷资产:不支持跳转。 风险资产:包含已失陷、高风险、低风险资产数,点击跳转到"威胁感知>资产感知"界面。 安全域:安全域的个数,点击跳转到"资产管理>安全域"界面。 Web 业务系统:Web 业务系统的个数,点击跳转到"资产管理>Web 业务系统"界面。 	※ 安全监測 C共和語 ^か C共和語 ^か C C



区块	说明	详细
	◆ 资产:资产的个数·跳转到" 资产管理≻资产 管理"界面。	
流量监控	 ◆ 展示最近 48 小时入流量+出流量监控情况。 ◆ 鼠标悬停趋势图,展示时间及流量监控值。 ◆ 展示实时流量,上升/下降箭头表示与前一分钟 实时流量对比。 	新聞協控 Calandray Cal
AiLPHA 引擎	 展示已添加到大屏的安全设备、管理引擎、可 视化引擎、情报引擎、 AI 引擎、态势感知、横 向威胁、外部态势、 sherlock、资产感知、业务 拓扑。 点击跳转到相应的页面。 	
日志吞吐量监 控	 展示最近 48 小时日志监控情况 · EPS 向上取整。 数据入库量: ES 全集群的数据写入速率。 鼠标悬停趋势图 · 展示时间及数据入库量。 展示实时数据入库量 · 上升/下降箭头表示与前一分钟数据对比。 1)展示运维告警 · 点击每条告警 · 跳转至 "系统 	
运维告警/监控 窗口	 管理>运维管理>运维告警"页面 · 查看详细告警 信息。条件:时间+事件名称;最多展示最近 1000条运维告警。 2)点击 ·展开监控窗口。 ◆采集设备:展示所有设备状态 · 灰色表示未 检测 · 红色表示离线 · 绿色表示在线;当刚 添加采集设备时 · 状态为灰色;直到下一次 	



区块	说明	详细
	运维告警产生, 状态会依据运维告警变为绿	
	色/红色; 状态根据最近一次运维告警确定:	
	最近一次运维告警周期内存在日志采集服务	S
	异常• 则该设备节点离线;若最近一次运维	
	告警周期内不存在日志采集服务异常·则设	S. S. S.
	备在线;周期默认为1h; 设备厂商为安恒·	. Pr
	资产类型为审计组件大类下的采集器、通信	
	服务器、关联引擎,或者安全类下的日志审	
	计系统的资产,在指标:探针发送数据量统计	
	中该资产 IP 对应的最后一条统计结果的时间	
	跟当前时间对比·超过 X 小时表示异常· 在	
	X 小时之内表示正常。	
	◆ 消息队列: 消息队列展示所有 kafka 节点的状	
	态·红色表示离线、绿色表示在线; 状态根	
	据最近一次运维告警确定:最近一次运维告	
	警周期内存在 kafka 节点状态异常 · 则该	
	kakfa 节点离线; 若最近一次运维告警周期内	
	不存在 kafka 节点状态异常 · 则 kafka 节点在	
	线; 远维告警周期默认1小时。	
	🔹 实时流计算引擎:展示所有关联引擎、自定	
14 - C	义引擎、规则引擎、日志 ETL 引擎、告警	
Die Vice	ETL 引擎的状态,红色表示离线、绿色表示	
	在线。	
	 ◆ 数据仓库: 展示所有 ES 节点的状态 · 红色表示离线、绿色表示在线; 状态根据最近一次运维告警确定: 最近一次运维告警周期内存 	



区块	说明	详细
	在 ES 集群健康状态异常 · 则该 ES 节点离 线;若最近一次运维告警周期内不存在 ES 集 群健康状态异常 · 则 logstash 节点在线;运维 告警周期默认 1 小时。	60.°0.'
磁盘容量监控	磁盘容量监控和平台运维告警可切换, 10秒钟切换 一次, 鼠标浮动时不切换。 展示总容量/剩余/昨日新增/日志已存储/预估 剩余可存储/宿主机系统盘,数据盘容量。 总容量取宿主机数据盘总和, 剩余取数据 盘剩余容量。 昨日新增: 取昨天原始日志/会话流量/会 话审计索引大小, 版本安装或者升级前两 天昨日新增无数据展示。 日志已存储:取原始日志索引个数。 预估剩余可存储: 剩余容量/昨日新增, 版 本安装或者升级前两天昨日新增无数据 展示。 点击每条告警, 跳转到安全告警。 	磁盘容重监控 日本語 2 31 Mail 2 32 Mathiles - 日本語で研想:日本 Webのパクロー Hal 1 54 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
安全设备设置	 ◆ 点击 弹出选择安全设备界面,可勾选安全设备展示在<ailpha引擎>模块中,最多同时勾选 7个。</ailpha引擎> ◆ 点击<确定>生效,点击<返回>退出选择安全设备界面。 	

4.13 安全态势

4.13.1 功能简介

安全态势大屏为分部安全管理员和分部安服人员提供包括攻击类型、攻击源、攻击目标等实时的攻击信息, 使用户能够实时准确的了解全球攻击轨迹。


4.13.2 区块概要

A&LPHA					en est 🛛 🖸 S
	7		Times .	No state of the st	
		1		NOT 10:00100017	
				NO.3 802 102113	4
And 白喉洋病				AV 2016/10/65/015	
	all and a			 NO11111	
100000000000000000000000000000000000000	112134		NAME OF TAXABLE PARTY.	NU2 1112	
2010-06-18 19:01 10		1113	Love of Constraining Stateme	1021113	4
2010-00-10 10223-00			tive to reprint a stress	804 1115	2
2010-00-11 10223-00	10112		Live Comprising Autom		

选择"态势感知"页面, 点击安全态势查看安全态势大屏。如下图所示。

数据源为安全告警, 数据流方向: 内访问外, 整张大屏 5 分钟刷新一次。各模块详细说明见下表。

区块	说明	详细
时间控件	时间范围: 默认显示最近7天。时间可选择: 最近 24 小时、 最近7天、最近30天、本日、本周、本 月。	 財師范顗: 肇近7天 暈近24小厨 暈近30天 承日 一次為 本月 一次為 小月
告警详情	 滚动展示 · 选择时间范围内最近 50 条告警数据: 攻击时间、攻击源 IP:srcAddress、攻击目标: destAddress、威胁等级、攻击事件类型: name。 鼠标悬停该位置 · 暂停滚动 · 显示所指向信息。 点击条目 · 新打开安全告警页面 · 带入条件:eventId+时间范围。 	TRANS TR



区块	说明	详细
	◆ 选择时间段内 · 攻击类型分布Top10。	
	◆ 点击某图例,环形图过滤掉该攻击类型数据。	/// 攻击类型分布
攻击类型分布	 ◆ 鼠标悬停右边图例 · 环状图联动显示攻击类型 以及总数 · 	
	 ◆ 鼠标移动至环形图上 · 显示攻击类型 · 总数以 及百分比 · 	
		如 攻击灌护期行
		NO.1 1952 11211 2
攻击源 IP 排行	显示统计时间段内攻击源 IP Top10。	N03 2010 112113
		NO4 892 10115 4
		川 攻击目标绑行
		803 1111 7
攻击类型排行	显示统计时间段闪攻击奕型 Top10 (针对 name 的	N021112 6 N031113 5
	统计)。	N041115 2

4.14 重保方案

以缩略图形式显示发布状态 (详见重大保障页面)的重保方案,点击图片进入重保方案大屏预览页面。

4.15 AiView

以缩略图形式显示发布状态(详见AiView设计器页面)的AiView,点击图片进入AiView大屏预览页面。

4.16 仪表盘

以缩略图形式显示发布状态(详见仪表盘管理页面)的仪表盘,点击图片进入仪表盘预览页面。

4.17 大屏轮播

使用系统管理员角色下的用户登录平台, 支持态势感知菜单下的大屏及安全设备相关大屏设置轮播。如下 图所示。



	NG - WANDON - 4-RODEN - B	SSAR - • RPER - • SMER -	inter 🖸
299.000		1. 100 AA 100 70 AA 100 70 100 44	20
87.0.7.W		大唐轮播及轮播设置协	312 · · ·
		REDUCTORING METHY AND PROVIDED, 10 ORIGIN TOPM, AND PROVIDED METHY S. 21 REVEATS AND AND A AND REDUCTORING OF PE TANKATSS SERVICE AND AND REDUCTOR METHY STRATISTICAL AND AND REDUCTOR	

轮播设置

在**态势感知**页面点击页面右上方的**轮播设置**按钮 🥯 · 展开**配置自动轮播大屏**页面 · 可自定义设置轮播时 间间隔、轮播大屏等。如下图所示。

大麻列表	210	已进中大屏 4
🔽 数据中心		○ 外部攻击态费
দল্পল্য 🔛	i ja	横向威胁感知
Sherlock	网络星空 🖉 🔽	遗产实施态势
图2-387-639		Web业务系统走势
秋志書道	REAL PROPERTY.	

- ◆ 轮播时间间隔默认为 10 秒·支持设置范围 5~1200 秒。
- ◆ 支持自定义选择轮播大屏,默认不选择。
 不选择大屏的情况下,点击轮播按钮
 支持态势感知菜单下所有大屏轮播,轮播顺序为解决方案大屏、重大保障大屏、安全设备相关大屏;
- ◆ 当自定义选择轮播大屏并保存后,点击**轮播**按钮 · 按照自定义选择的大屏及顺序轮播。





5. 威胁感知

5.1 安全事件

5.1.1 功能简介

安全事件页面展示最近 7 天安全事件汇总情况以及最近的安全事件管控趋势。安全事件根据高危事件、中 危事件、低危事件分别汇总显示;在事件列表区域逐条展示安全事件。

5.1.2 区块概要

选择"威胁感知>安全事件"菜单,进入安全事件页面,如下图所示。其区块概要如下表所示:





区块	说明	详细
筛选框	 ◆ 支持输入名称、描述、标签、攻击者或者受害者等进行查询。 ◆ 输入时有下拉提示最近 30 天安全事件名称 · 支持模糊查询。 	atter Luse între RED Hotse Rete
时间选择框	支持最近7天、最近30天、本日、本周、本月。	 (現近7天) (現近7天) (現近30天) 本日 本周 本月
安全事件	 ◆ 展示时间范围内高危事件、中危事件、低危事件数量・单位: 起。 ◆ 点击高危事件/中危事件/低危事件, 其它等级灰色显示, 系统会自动根据事件危险等级过滤。 	28 € 0 ± 0 ± 0 ± 0 ± 0 ± 0 ± 0 ± 0 ± 0 ± 0
安全事件管控 趋势	展示最近 60 天安全事件数量变化趋势。其中: Y 轴:安全事件数量。 X 轴:日期· 颜色代表等级。	
安全事件列表	 显示时间范围内安全事件卡片,按照结束时间 排序。 安全事件卡片内容:事件名称、标签、描述、 首次发生时间、最近发生时间、举证、事件等 级等。 点击卡片,跳转到"安全分析>Investigation> 安全告警"页面,带入保存查询模板的条件。 	Entry EXTRAC + south Administration Provide Transmitter Setting of any other and a setting administration and the set of the set of the administration of the set of the setting administration administration of the set of the administration of

5.2 资产感知

5.2.1 功能简介

以资产为核心视角, 直观了解自身网络环境中存在风险资产。资产感知通过攻击链形式展示, 剖析从扫描

探查阶段到资产破坏阶段资产失陷过程。感知失陷、异常资产,从海量的日志中提取有价值的资产溯源路线。平台简单易用,支持一键全方面钻取,降低运维成本,提高运维效率。

5.2.2 区块概要

选择"**威胁感知>资产感知"**菜单·进入资产感知页面·如下图所示·当用户为租户时·只显示安全域过 滤后的资产。

990 - 80A1830				N.Y		
风险资产			安全域风险资产数排行	OV.		
5 Estere	5 RANGE	0 645875	机化物数容量 有云 半分段 电信号校云		2	4
风险资产外表			\$9 ³			
58275 - I	R\$H	S	*		9,	风险资产报告
我种名称 =	资产IPiete =	安全地 :	ANDER X	MADIFIE O	和正时常说生时间。	操作
股份额 192.168.395.21	162 168 99 21	南信令项云	2012Window's RDP BluekeepE38(CE R)で用品調味が、CVE 2019-0708() 417 0.2、現在2016点から RDP BluekeepE36 (公用は2015年1月)日の1000000000000000000000000000000000000	BIER	2021-12-30 13.59-20	查察律信
的公网pc-192,168.99.40	192.166.99.46	K/8/58/92	※超資产発生1473次 確定NS17414 を加え放用用利用425次 定量内容IP 等能改成44508□ (部分件話109次) ま 25 次	BRM	2028-12-38 13-58-40	资料详细
2142 Ripo 192, 168 199 43	192.160.99.45	ALMANDA D	2010日の単位116817、2010月20日 2010445回辺(1823年4月10日の)1654 次、対応は517-014555222日第三日月1 6月1日	Esta	2020-12-30 13 50 56	自由注意

资产风险评级基于最近 7 天内未处置的安全告警中攻击链、攻击意图、威胁方向等进行多因子融合建模· 评估资产的"已失陷"、"高风险"、"低风险"状态。其中·"已失陷"说明攻击者已经攻陷该资产· 下一步可能会进行窃取敏感信息或资产破坏·需要引起高度重视。区块概要见下表。

区块	说明	详细
风险资产统计	 不同颜色展示已失陷资产数、高风险资产数、 低风险资产数。 点击对应图标 · 联动过滤风险资产列表。 	ANDER S S S S C ANALYS C ANALYS
安全域风险资 产数排行	 ◆ 展示风险资产所属安全域 Top5 排行。 ◆ 点击柱状图 · 与风险资产列表联动 · 过滤安全 域。 	安全組織編練が翻算行
风险资产列表	 ◆ 支持风险评级、安全域下拉选择过滤。 ◆ 右上角可基于资产名称或 IP 关键字进行搜索; 支持模糊查询。 ◆ 列表以最近异常发生时间倒序排列。 	NAMENAR Series and Antipartic



区块	说明	详细
	 主展示区展示资产名称、资产 IP 地址、安全域、风险概况、风险评级(已失陷、高风险、低风险状态)、最近异常发生时间、操作等共7列展示。其中部分支持进行正序倒序排行。 	08.00
	● 操作栏点击 查看详情 •钻取至" 威胁感知 ▶Sherlock"页面•带条件:资产 IP。	St.
	◆ 列表数据 10 分钟更新一次。	C.

5.3 业务全景

5.3.1 功能简介

将拓扑绘制的内容进行实时监控。 提供列表模式和缩略图两种展示界面。业务全景可以通过业务拓扑图的 方式展示当前整个业务拓扑的威胁分析。

5.3.2 区块概要

*其*单 · 默认违 默认进入业务全景缩略图模式页面·如下图所示。 选择"**威胁感知>业务全景**"菜单,





缩略图模式

(1999年1月) 金秀全部

- ◆ 出厂内置三个业务拓扑 · 分别为:企业网(3D)、企业网、通用 Web 应用 · 随机排序。
- ◆ 内置的业务拓扑不关联资产、安全设备、 Web 业务系统、安全域 · 显示业务拓扑的截图。
- ◆ 鼠标移到缩略图上时,显示缩略图的业务描述,并且右上角显示<编辑拓扑>按钮。
- ◆ 点击页面左上角"**列表模式**"图标 · 进入业务拓扑列表模式 · 如下图所示 ·

= 列於權式 = 編結器	0		新聞
0.9588	are suite	操作	
2		- 8 / 1	
2334345345		a a / a	
36	838	- B / B	
est	cess	- B Z E	
esti		- B / B	
55	1999	- · · ·	
test			

列表模式



◆ 出厂内置三个业务拓扑, 分别为:企业网(3D)、企业网、通用 Web 应用, 按名称排序。

新建业务

点击<新建业务>·打开新建业务页面。

标题:新建业务,业务名称:必填项,业务描述非必填,如下图所示:

a Poster a rate of					P.H.D.
4 5 T K	新建业务	×	1	lin.	
62	USCON INTERNET		1.80	2.3	
12334343343	TANK MARY TOWN			$\widetilde{X} = \overline{g}$	
	WHERE MICCREAME			2. 8	
eet 1	** 00		18	1.1	
	987 977 (1997) (1997) (1997)	-		× 1	
				2.9	
**				2. 2	

填写完毕后,点击<保存>,缩略图区域显示"请配置业务拓扑"。

AND A CONTRACTOR	, S.	The second second second second second
- 2°7#	Conte - an Lang - an me an ma	BERE AT AN
10001		
	Division and Dist Law The	
and the state of t		
	ETHERNE-IAL STITULASE	
#我们算艺产,比量状态艺产 全型交易的ant		
Balantie WhiteGel, loghering	Tereserie 22 min	
	新作用音器 142 2/5 144 4	
S I I I I I I I I I I I I I I I I I I I		
V MARK /		
· #20#		
· ····		
· them.		
. 2112		

点击<保存并编辑拓扑>·进入业务全景编辑页面·如下图所示:

编辑业务拓扑

点击<编辑拓扑>按钮·进入业务拓扑编辑页面·左侧是左上显示资产选择器(资产列表)、Web业务系统、 安全设备、安全域·左下显示元素选择器·中上显示工具栏·及<更多设置>、<保存>和<返回>按钮·中下



显示拓扑绘制区,右侧显示元素编辑器。如下图所示。

AILPHA	1 1840 - ABRY - & 5218 - & 5228 -	4 0100 · 0 3400 ·		
most gate entries				
- 1111			+ #### ## - #####	
100				
MUMUL and ALLER.				
			2	
more muse mass			0,2	
🖷 🖷 🖷			8	
muss			2	
			0	
-mult - scans, stars				
+ + - +				
> 258			C.	
· 2528			20	
1 00100000				
- arca		0	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
TOUT		0,3		
1.0 100 000		~~~~		
(int (in) ==>)		*	~	
14 878 9			c'	
		X	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	

业务拓扑编辑页面各模块详细信息见下表。

区块	说明	详细
资产选择器	 按资产名称显示资产,并且按资产 ID 倒序排序。 资产都用一个图标显示,每个图标下方显示资产名称。 当资产过多一屏无法显示时,会显示分页。 支持资产 IP、资产名称模糊查询。 可拖拽到拓扑绘制区,拖拽后的资产还是会显示 在资产选择器中,但是会置灰显示。 	



区块	说明	详细
元素选择器	 按组显示 · 具体分组有: 基本元素 : 包含元素种类为文字、矩形、多边形、分组、信号塔、云、用户、用户组、管理员、端口、服务器集群、数据库服务器、无线、移动终端、应用服务器、邮件服务器、云数据库、中间件服务器、AiLPHA 大数据、API 接口、FTP、服务器、终端。 网络设备元素 : 包含元素种类为路由器、交换机、负载均衡、VPN。 安全设备元素 : 包含元素种类为安全管理系统、APT、数据库审计系统、日志审计系统、抗 DDoS系统、流量监测设备、入侵防护系统(IPS)、入侵检测系统(IDS)、上网行为审计系统、统一威胁管理(UTM)、网页防篡改、下一代防火墙、运维审计系统、主机安全管理系统(EDR)、Web应用防火墙(WAF)。 3D 设备元素 : 包含元素种类为服务器、防火墙等。 	 > 基本元素 > 网络设备元素 > 安全设备元素 > 3D设备元素 > 3D设备元素 * 3D设备元素 * 3D设备元素 * 第二 * 支換机 ※ 按换机 ※ 放换机 ※ 放射机 ※ 放射机 ※ 放射机 ※ 放射机 ※ 放射机 ※ 放射机 ※ 成为机 <l< td=""></l<>
工具栏	 ◆ 默认显示<撤销>、<恢复>、<删除>、<缩放>、<网格>、<布局>、<标尺>等按钮。 ◆ 点击<更多设置>、弹框显示更多设备页面。 主题选择:浅色、深色。 导入导出:导出图片、导出拓扑数据、导入拓扑数据。 	
拓扑绘制区	 默认是 100%的比例显示 · 可点击按钮或鼠标滚动放大、缩小。 显示内容跟上一次编辑保存时的一致 · 如果是第一次编辑则显示为空。 拖拽元素至绘制区 · 利用工具栏、元素编辑器等绘制拓扑图。 	



区块	说明	详细
元素编辑器 _资产	 拓扑绘制区中选中单击元素 · 显示该元素对应的编辑页面。 打开元素编辑页面后 · 可编辑组件属性 · 是否绑定资产、资产名称、资产 IP、资产描述、资产图片、宽度、高度; 选择绑定资产 · 带出选择资产框 · 下拉选择要绑定的资产 · 元素即可绑定资产 。 点击<收回> · 关闭元素编辑器。 	
元素编辑器 _安全域、安 全 设 备 、 Web 业务系 统	安全域、安全设备、 Web 业务系统的元素编辑器一样 · 都是可设置边框粗细、边框颜色、背景颜色 · 是否缩略 图。	• RANK • RANK • RANK • RANK • RANK • RANK
2		



5.3.3 业务监控



缩略图点击图标,或列表模式中点击操作列的<**业务监控**>,打开业务监控页面,如下图所示:

点击拓扑中的元素图标,不同元素所展示信息见下表。

区块	说明	详细
未绑定资产 的元素显示	点击拓扑图的元素·显示资产元素显示资产名称。	武产祥績 X 防 愛产教務:55米域
绑定资产的 元素显示	 资产元素显示以下信息: 资产名称 风险评级(已失陷、高风险、低风险、健康、并以不同颜色标记;并且当资产为已失陷、高风险、低风险时资产元素上需要标记) 安全告警Top3(告警名称:事件数量) 最近异常发生时间 资产 IP 安全域(属于内部安全域时显示安全域名称、不属于内部安全域但是属于内网 IP 时显示内网、不属于内部安全域也不属于内网 IP 时显示未分配) 资产类型 组织架构 	WEB业务系统-api.websa



区块	说明	详细
	 ◆ 责任人 ◆ 当没有相关信息时,该项内容不显示。 提示信息下方显示<sherlock>按钮,点击跳转到</sherlock> Sherlock页面,带入条件: IP 为该资产 IP,时间范围为最近 7 天。 	8.00
Web 业务系 统_有绑定 资产	 Web 业务系统显示以下信息: 图标-系统名称 域名 网络速率 访问次数 访问成功率 7天告警 如果Web 业务系统信息所需都存在的情况下,下方显示<安全告警>、<访问日志>、<访问系统>、<投 屏演示>。 安全告警:新页面跳转到<安全告警>、条件 destAddress = 所有关联资产 IP,时间最近7天。 访问日志:新页面跳转到<原始日志>、条件 destHostName=所有域名和子域名,时间本日。 访问系统:新页面跳转业务系统的<访问地址>。 投屏演示:新页面跳转。 	spi webssa. at we
Web 业务系 统_无绑定 资产	 Web 业务系统显示以下信息: 图标 系统名称 域名 网络速率 访问次数 访问成功率 7 天告警(高:0中:0低:0) 如果Web 业务系统信息所需都存在的情况下,下方显示<访问日志>、<访问系统>、<投屏演示>。 访问日志:新页面跳转到<原始日志>,条件 destHostName=所有域名和子域名,时间本日。 访问系统:新页面跳转业务系统的<访问地址>。 投屏演示:新页面跳转。 	www.testc



区块	说明	详细
安全设备_ 有绑定资产	 安全设备显示以下信息: 图标 安全设备名称 安全设备关联资产名称 本日日志数 关联资产数量 设备状态 日志量 如果安全设备信息所需都存在的情况下,下方显示 <日志检索>,<管理界面>,<处置联动>和<投屏演示>按钮。 日志检索:新标签页跳转<原始日志>,条件: 设备 地址 deviceAddress=多个设备 IP,时间本日。 管理界面:新标签页跳转<设备管理>界面 URL,当 多个资产有管理地址时,下拉显示资产名称,用户可选。 处置联动:新标签页跳转 "资产管理>处置联动> 联动策略",带入<安全设备>的条件。 投屏演示:新标签页跳转投屏演示。 	
安全设备_ 无绑定资产	 安全设备显示以下信息: 图标-安全设备名称 本日日志数(0) 关联资产数量(0台) 设备状态(未检测) 日志量(一条 0EPS)的直线 <日志检索>・<处置联动>和<投屏演示>按钮。 日志检索: 置灰状态 处置联动:新标签页跳转 "资产管理>处置联动> 联动策略"、带入<安全设备>的条件(暂无数据) 投屏演示: 置灰状态 	
安 全域_有 绑定资产	 ◆ 安全域显示以下信息: 图标 安全域名称 网段 包含资产(资产 IP 在安全域里的资产数量) 风险资产(资产 IP 在安全域里的风险资产的数量) 	MICR MICR



区块	说明	详细
	 7 天告警(安全域包含的资产 7 天告警高、中、低的总和) <安全告警>和<资产管理>按钮: 安全告警:新页面跳转到<安全告警>·条件安全域,时间最近 7 天。 资产管理:新页面跳转到<资产管理>·条件左侧安全域选择该安全域。 	0.00 0.00 0.00
安全域_无 绑定资产	 ◆ 安全域显示以下信息: 图标 安全域名称 网段 包含资产(0台) 风险资产(0台) 7 天告警(高:0中:0低:0) < 安全告警>按钮: 安全告警:新页面跳转到<安全告警>,条件安全域, 时间最近7天。 	Material States
资产、Web 业务系统、 安全设备、 安全域已删 除	拓扑图的图标上标记已删除。	Well Service S

5.4 Sherlock

5.4.1 功能简介

Sherlock 入口展示纷繁复杂网络中网络实体之间的访问和攻击连接关系,支持选中连接关系中的某个实体 查看详情, 或在 IP 地址搜索框中输入待追踪的网络实体 IP 查看详情。

选择"威胁感知>Sherlock"菜单,查看 Sherlock 页面,如下图所示。



			•		1 0
	4946->.0-10.12		Q.	• •	
•		2		• •	
•.	算法元(sheetod) 試予行→17篇77年刊201章。特许道道整 中11人に9章马说。人類第10百萬多分的学校的以前支援 19章ご天元400,常任一副企業考試安全部的法律系列	1988. amfikazzarte. Rakiere. Affikaziotzkier I.		. .	
			S.		

◆ 点击右上角 · 显示不同的图标与资产类型和情报类型的对应关系 · 同 "**态势感知>Sherlock 网络 星空**"平面效果中的图示按钮的效果 。

此页面同"态势感知>Sherlock 网络星空"的平面效果·点击右上角·可投屏至"态势感知>Sherlock 网络星空"。

◆ 点击实体圆点^{Sherlock}或者输入 IP 点击检索后跳至 Sherlock 详情页面 · 如下图所示 · 当用户为租户时 · 只能查询安全域过滤后的 IP 。

TW-100-11-126	0, %		¢	最近7天	21.0
成果 访问关系 行为重象 服务排口 访问副					
		194			
周产苔屑: 卸件运告基-132 168 11 138 安全様: 未分配 両产実型: 点用時-卸件設め間 WED最考析的: 聖元 安全録音: 新元		2		, du	
攻击堕		9			
- Solon	内震信意	6 ·····			
	0				
	2020-1	0 2-24 00:00:00 202	0-12-26 06:00:00	2020-12-38 12:00:00	
1280 Big 0	10 (REAL O				
风险计情					
(2018/中部共務-112,165 11,110) 截近7天 通短VPN用户 cardy Iv 初始以近年	责 1种动力共11次,发起VP从用户 cendy.br	EEE认证电散。用户 Hoat	登登刘政、VPN用O	candy lo 初级以证共数 等7种	收击共计7次,最近
次次出出生在7小时间, 读是产生教祝古为 200				1991 - 19	
スは出生生た70年前、は日子当時代なか <mark>2000</mark> 。 「安全希望 - 「天史提 - 」 dilliniti - 「NAM - 」	10000 ·		- 10.		
スな出生生を7.541年、 (#20 ²⁴ 生物)代なか 2000 安全古智 - 末代現 - 創始たり - 別には - 1 実施方向 - 長智	(111) - (111) - (111)	威胁等些	64203R -	最近异常发生时间:	- MAR

- ◆ 搜索框、时间控件· 几个Tab 页通用· 切换至其他页面· 查询条件保留。
- ◆ 点击右上角 · 可选择投屏至攻击者溯源、资产威胁溯源大屏, 带条件: 搜索 IP。



5.4.2 页面详细介绍

点击 Sherlock 页面的某一个原点,可以查看该 IP 的相关信息。

点击<Sherlock>进入资产详细页面介绍:





42.1111.3	69.99						
n.e	他司关系	行为资源	(89)第□	05/439822	1019年1日		
文体(記) 57 赤 11 赤	2 + to町m 9 toifi追捕福	可添加#室湾产/行	山道道		地理校園:中國一會	a	
					8 ÷ 12 H		Series Series
			Centres .	1 11	States of the second se	O Statest	

资产信息/情报信息/实体信息

搜索框支持所有 IPv4 格式的 IP 查询 · 所以查询出的信息也有不同的情况:

- 搜索框 IP 有对应资产,查询结果为资产信息。
 显示资产名称(搜索框 IP 对应的资产名称)、资产类型、安全域、Web 业务系统、安全设备、没有值的字段显示"暂无"。
 点击,跳转到编辑资产页面,显示搜索框 IP 的资产信息,编辑后点击<保存>、跳转回 Sherlock 概况页面,刷新后显示编辑后的信息。
- 搜索框 IP 属于情报 IOC · 查询结果为情报信息。
 显示情报标签、置信度、地理位置、运营商、组织名称 · 没有值的字段显示"暂无"。
 以印章形式显示情报分类 · 优先级为行业情报>分析团队情报>安全大脑>第三方。
 点击 · 跳转至修改情报页面 · 显示搜索框 IP 的情报信息 · 编辑后点击<保存> · 跳转回 Sherlock 概况页面 · 刷新后显示编辑后的信息。
- 搜索框 IP 无对应资产,查询结果为实体信息。
 - 属于内部 IP ·显示实体名称(搜索框 IP)、地理位置、安全域(属于某一安全域显示安全域名称· 反之是(内网))。

不属于内部 IP · 但属于内部安全域 · 显示实体名称 (搜索框 IP) 、地理位置、安全域 (所属内部 安全域名称) 。

不属于内部 IP · 也不属于内部安全域 · 显示实体名称 (搜索框 IP) 、地理位置、安全域 (未分配)。 点击 · 有添加资产和添加行业情报两个选项 · 选择添加资产 · 跳转到新增资产页面 · 带入条 件:资产名称为搜索框 IP · 保存后跳转回 Sherlock 概况页面 · 刷新后 · 页面显示资产信息。 选择添加行业情报 · 跳转到添加情报页面 · 带入条件 : IOC 类型 : IP + IOC : 搜索框 IP · 保存后 页面跳转回 Sherlock 概况页面 · 刷新后 · 页面显示情报信息。

◆ 攻击链

以不同颜色展示 7 个攻击链: 侦查、投递、利用、横向渗透、内部侦查、命令控制、获利, 被搜索 ip 告警所在攻击链环节高亮, 并依照箭头高亮颜色逐渐加深, 每个攻击链上显示选定时间范围内搜索框 中 IP 的未处理状态的安全告警数量, 超过 99 显示 99+。点击图标,与风险详情列表联动,过滤攻击 链。



◆ 告警时序

搜索框中 IP 的所有状态的安全告警数量 · 鼠标移到柱子上时 · 显示该柱子对应的时间以及告警数量。 风险详情

区块概要见下表。

区块	说明	详细
风险总结	显示以下内容(无对应资产时不显示): ◆ 资产名称 ◆ 资产状态 ◆ 最近一次攻击发生时间 ◆ 遭受攻击 Top3 告警/事件名称及总数 ◆ 发起攻击 Top3 告警/事件名称及总数	THEREIN INFORMATING MILLING AND
过滤条件	 ◆ 支持安全告警、安全事件切换。 ◆ 支持处置状态(切换至安全事件,无处置状态项)、 威胁方向、攻击链、威胁等级下拉选择过滤。 	80000 8289 + 858 + 8000 + 800 + 8000 +
安全告警 列表	 ◆ 安全告警主展示区:告警、威胁方向、攻击链、攻击 方法、威胁等级、告警次数、最近异常发生时间、操 作(处置、告警详情)。 ◆ 点击处置,支持添加白名单、处理状态、禁用模型、 添加至联动策略、EDR 联动,更改告警状态,风险评 级稍后也相应更新;点击查看告警详情,跳转至安全 告警,带条件:处置状态(alarmStatus)+事件名称 (name)+模型 ID(modelName)+来源 IP(srcAddress)或 者是目的 IP(destAddress)。 	SMICH UPDER_25.5() +== detection == 0.1(); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 4155 × 415 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 101 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(200, q)); 415 × 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(100, q)); 415 × 100, eq. (0.1); 1 100, eq. (0.1); 1 100, BC/9.5()(100, eq., 0.1()(100, q)); 415 × 100, eq. (0.1); 1
异常记录 列表	异常记录主展示区: 威胁方向、异常记录、攻击链、威胁 等级、记录次数、最近异常发生时间、操作(点击查看事 件详情, 跳转至异常记录,带条件:事件名称(name)+模型 ID(modelName)+来源 IP(srcAddress)或者是目的 IP (destAddress))。	BEQ



区块	说明	详细
告警事件 详 情_非 情报模型	 点击》,展开告警、事件详情列表,包含详细信息、 原理描述、处置建议。 每条记录显示 "srcAddress 对 destAddress 发生了 X 次[name]",并根据聚合后的事件数量降序显示,只 显示 Top100。 	文文文字型 - 本社型 + ADDATA - DOB (ADDATA - DOB (ADDATA (ADDATA (ADDATA - DOB (A
告警事件 详 情 _ 情 报模型	告警、事件为情报模型时显示碰撞的情报信息 · 包括情报 分类、情报标签、地理位置、置信度、运营商、组织名称、 第三方链接 · 点击更多跳转至情报查询页面 · 查询更多情 报信息。	
详情链接	 详细信息中的 srcAddress 或 destAddress · 点击 · 显示下拉钻取列表。 情报查询:新打开情报查询页面。 带入条件: IP · 并且默认显示查询结果。 安全告警查询:新打开安全告警页面。 带入条件: IP · 时间范围,并且默认显示查询结果。 异常记录查询: 新打开异常记录页面。 带入条件: IP · 时间范围,并且默认显示查询结果。 原始日志查询: .新打开原始日志页面。 带入条件: IP · 时间范围,并且默认显示查询结果。 Sherlock:新打开 Sherlock 详情页面。 带入条件: IP · 并且默认显示查询结果。 攻击者追踪溯源:新打开攻击者追踪溯源大屏。 带入条件: IP 。 	● 展型FP 112 (B, 00, 1)(B, A23PB0D00CT104, an Astesse, network) network) network) network) network) network) network) network) network) network) network) network) network) network) network) network) network network) network

5.4.3 访问关系

切换至访问关系Tab页, 进入 Sherlock 访问关系页面, 默认展示如下图所示。





区块概要见下表所示:

区块	说明	详细
	◆ 图形模式、列表模式,默认选中图形模式。	
模式切换	 ◆ 访问方向: 所有方向、访问内网、来源内网、访问互 联网、来源互联网 · 默认选中所有方向。 	Rectoral: Blage: Amage Weights: Restor Grant Adams Granter and State
	 ◆ 访问类型: 所有类型、异常访问、正常访问 · 默认选 中异常访问 · 	1999 Mag Fann (1999
	◆默认收起。	蔺級▲
	◆ 异常访问类型: 文本输入框·默认为空。	异常访问类型 : 情绪入异常访问参注言的
	◆ 攻击链: 下拉选项有扫描探查、渗透攻击、获取权限、	双击铁 雪出田 🔻
高级		世界特徴: 憲法将 *
	◆ 应用协议: 卜拉选项为日志字典中 appProtocol 的值 · 可以多选 · 默认为空;支持模糊查询。	访问目的第口: 回知人用的第口号,用意与公开
	 ◆ 访问目的端口: 文本输入框·默认为空。 	连接TOP: 10 30 50
	◆ 连接关系 TOP:可选项有 10、30、50,默认选中 10。	義定
~	▶ 提供< 自动拓展关系网络 >按钮, 开启时支持在现有	
扩展关系	关系网络下自动拓展·关闭时维持现有关系网络。	
网络	◆ 提供< 扩展下一级关系网络 >按钮 · 随机选择现有关	H
	系网络中的一个资产每点击一次按钮扩展一次下一 级关系网络。	



区块	说明	详细
	 ◆ 访问了互联网 IP 的 X 个 IP 目标: 原始日志索引中指 定时间范围内 direction=11 或 01 · 并且 srcAddress 为 搜索框中 IP 的事件中 destAddress 的个数。 	
访问关系	 ◆ 访问了内网 IP 的 X 个 IP 目标: 原始日志索引中指定 时间范围内 direction=10 或 00 · 并且 srcAddress 为搜 索框中 IP 的事件中 destAddress 的个数。 	192.168.11.108 访问了内网的2个IP目标
统计信息	 ◆ 被来源互联网的 X 个 IP 访问: 原始日志索引中指定 时间范围内 direction=11 或 10 · 并且 destAddress 为 搜索框中 IP 的事件中 srcAddress 的个数。 	被来源内网的90个IP访问 访问了互联网的5个IP目标 被来源互联网的7个IP访问
	◆ 被来源内网的 X 个 IP 访问: 原始日志索引中指定时 间范围内 direction=01 或 00 · 并且 destAddress 为搜 索框中 IP 的事件中 srcAddress 的个数。	
历史访问	按点击时间正序显示当前页面最近点击的 5 个资产名称。	历史访问 202.181.169.98 211.4.4.2 149.4.4.1 169.4.4.1 WEB业务系统-api.websaas.c
连线和图 标	 连线颜色: 正常访问为蓝色,异常访问为红色。 图标:显示不同的图标与资产类型和情报类型的对应 关系,具体见右图。 	 内网 互联网 DNS服务器 监管单位 邮件服务器 黑客组织 WEB服务器
图形模式	 默认 Top10。 根据资产类型和情报类型显示相对应的图标,图标下方显示资产名称,并且不同的风险等级显示不同的颜色: 已失陷:红色 高风险:橙色 低风险:黄色 健康: 绿色 其他:蓝色 	LES 5.6% www.akbass com.or.192.196.11,100 201102.100.100.00 201102.100.100.00 201102.100.100.00 201102.100.100.00 201102.100.100 201102.100.100 201102.100.100 201102.100.100 201102.100.00 201100.00 201100.00 201100.00 201100.00 2000.00 2000.00



区块	说明	详细
	 ◆ 鼠标点击图标时浮出显示资产详细信息 · 内容包含: ● 有对应资产 	
资产详情	资产名称、风险评级、安全告警 Top3 (告警名称:事件数量)、最近异常发生时间、资产 IP、 安全域(属于内部安全域时显示安全域名称,不 属于内部安全域但是属于内网 IP 时显示(内 网),不属于内部安全域也不属于内网 IP 时显示 未分配)、资产类型、组织架构、责任人。	
	当没有相关信息时, 该项内容不显示。 < Sherlock >、 < 关系拓展 >按钮(搜索框 IP 对应 的图标不显示< 关系拓展 >按钮)。	
	● 无对应资产_内网	APADI ANA HIANA
	显示 IP、安全域 (所属安全域或者是 (内网))。	
	● 无对应资产_互联网	
	显示 IP、安全域:未分配、地理位置。	
	◆ 点击关系拓展 · 展示该图标对应的 IP 的访问关系;	
	点击 <sherlock> · 跳转至 "威胁感知>Sherlock"页</sherlock>	
	面·带条件: IP。	
	◆ 浮出框显示以下内容	
	 两个图标之间的访问方向,两者相互访问时显示 两条线。 	
	 访问类型(正常访问: XXX 异常访问 XXX)· 支持钻取。 	
	● 累计流量: 原始日志中 bytesIn+bytesOut 之和。	
	 最近访问时间:原始日志中满足条件的最近一条 	HERE AND ADDRESS OF THE OWNER OF THE OWNER
连线详情	日志的时间。	Martin Contraction (Contraction (Contraction))
	● 异常访问类型 Top3: 没有异常访问时不显示该 项。	Character Control of C
12	● 正常访问类型 Top3 (appProtocolTop3):没有正常访问时不显示该项。	Elitarititizada andi
	◆ 连线粗细根据访问次数变化	
	连线粗细根据当前数据自动计算,最多的固定显示最	
	粗。	

区块	说明	详细
	◆ 以列表展示访问关系。	NAME IN AN ADDRESS OF A DRESS OF
列表模式	默认显示 Top10 · 高级查询设置过滤可增加展示条 数。	
	 ◆ 列表中正常访问、异常访问支持钻取。 	
5.4.4 行さ	回像	0°0°
刃换至 行为画	像 页签,进入行为画像页面,如下图所示。	SV.

5.4.4 行为画像

A !LPHA !!!!		> anne -	4.8858 -	-		+	0.1	ŭ
ACCESS Brance							~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
02101110							- Ili	A 809 + 0.
di nin		inite()	101 area				0	
200 						***	23	
	(114-00-04) (16-000)				5118.51 5	S.		·
Landaren Lan	7.7	-7	-		S		777	

- ◆ 访问流量变化趋势(折线图显示请求流量、出流量)
- ◆ 访问次数变化趋势(折线图显示主动访问、被动访问)
- ◆ 访问来源Top10(柱状图)
- 访问目标Top10(柱状图) ٠

5.4.5 服务端口

切换至服务端口页签,进入服务端口页面,如下图所示。

A*LPHA ===	Game - star	annin- a anna		eu -			D +***
10.00 Barbald						5. Act.	+ 10
NG actives (The	a and stat	ant orac					
1 (1000) (2000, 101)	0	2 G8	1 GB	C KB	() () () () () () () () () () () () () () (Maria	0.00%
MINING PARTY							
10						4.1	6
Prevent.	10.142	10.00	6428		4/3	100	
1 🙀 101	approx.	inite .	100	14		8829	
					818	1	1.46
						0	



区块概要见下表。

区块	说明	详细
端口个数统计	◆ 统计时间段内搜索 IP 作为目的 IP 的目的 端口中。	1 D
	◆ 开放端口、不常用端口、风险端口个数。	
	◆ 统计时间段内搜索 IP 作为目的 IP 的目的 端口中。	
流量统计	 ◆ 端口响应总流量、请求总流量、风险端口 响应流量、风险端口流请求流量、风险端 □流量占比。 	
	 ◆ 支持多个端口查询 · 以英文逗号隔开 · 	
	◆ 列表显示 Top50 端口,按端口被访问次数 倒叙排列。	£
开放端口详情列表	◆ 主展示区展示:	
	开放端口: 属于风险端口时红色字体显示,非风险端口时黑色字体显示。	
	端口类型、响应流量、请求流量、被访问 次数、操作(显示流量日志)。	
	显示选择时间范围内流量变化趋势	
端口详情_流量变	◆ 鼠标移到线上时浮出显示时间、响应流 量、请求流量。	
化趋势	 ◆ 点击<流量日志> · 跳转至原始日志页面 · 带条件: 目的 IP(destAddress) · 目的端口 (destPort) ° 	3
	◆ 指定时间范围内按事件数量取Top5。	
	◆ 每个 IP 对应的记录显示以下内容:	
M.	● IP:支持跳转溯源。	
端口详情_访问来	 事件数量柱状图: 被访问 XXX 次、 请求流量 XXX (单位自动切地) 	
源 Top5	bytesIn 总和)、响应流量 XXX(单位	
	自动切换 · bytesOut 总和)、应用协	
	议(appProtocol 事件数量最多的 Top3)·应用协议支持跳转溯源。	



5.4.6 访问端口

切换至**访问端口**页签,进入访问端口页面,如下图所示。

A/LPHA	U 2000 - 00000 -	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · ·			4	-
and a second							
00.00.2.00						A 401 -	1.0
R0 0014 -014	CAUSE CAUSE IN	201 0100				3	
t state and	() 1000	() 	ma ka	0 KB	Car and	0 1.00%.	
senacores					N		
-						41.0	- 11
anima)	wins	LINDE	teni			80	
> 😥 eee	8017	1100			- V	cate .	
					Cy citta	* T * 165- 88	
					~~~		

访问端口页面同服务端口,只是搜索中 IP 是作为源 IP 的数据, 区块概要如下表。

区块	说明	详细
端口个数统计	统计时间段内搜索 IP 作为源 IP 的目的端口中 开放端口、不常用端口、风险端口个数。	
流量统计	统计时间段内搜索 IP 作为源 IP 的目的端口中 上传总流量、下载总流量、风险端口上传流量、风 险端口流下载流量、风险端口流量占比。	all neer all neer all neer all neer
访问端口详情 列表	<ul> <li>支持多个端口查询,以英文逗号隔开。</li> <li>列表显示 Top50 端口,按端口访问次数倒叙排 列。</li> <li>主展示区展示:</li> <li>访问端口:属于风险端口时红色字体显示,非 风险端口时黑色字体显示。</li> <li>端口类型、上传流量、下载流量、访问次数、 操作(显示流量日志)。</li> <li>流量日志支持跳转溯源,带条件:来源 IP(srcAddress)、目的端口(destPort)。</li> </ul>	
端 口 详 情_流 量变化趋势	<ul> <li>◆ 显示选择时间范围内流量变化趋势。</li> <li>◆ 鼠标移到线上时浮出显示时间、上传流量、下载流量。</li> <li>◆ 点击&lt;<b>流量日志</b>&gt; · 跳转至原始日志页面 · 带条件:来源 IP(srcAddress)、目的端口(destPort)。</li> </ul>	1



区块	说明	详细
端口详情_访 问目标 Top5	<ul> <li>◆ 指定时间范围内按事件数量取Top5 目标 IP。</li> <li>◆ 每个 IP 对应的记录显示以下内容:</li> <li>IP:支持跳转溯源。</li> <li>事件数量柱状图。</li> <li>被访问 XXX 次、请求流量 XXX(单位自动切换・bytesIn 总和)、响应流量 XXX(单位自动切换・bytesOut 总和)、应用协议(取appProtocol 事件数量最多的 Top3)、应用</li> </ul>	
端 口 详 情_ 访 问域名 Top5	<ul> <li>协议支持跳转溯源。</li> <li>着定时间范围内按事件数量取 Top5 域名。</li> <li>每个 IP 对应的记录显示以下内容:</li> <li>域名: 支持跳转溯源。</li> <li>事件数量柱状图。</li> <li>被访问 XXX 次、请求流量 XXX(单位自动切换、bytesIn 总和)、响应流量 XXX(单位自动切换、bytesOut 总和)、应用协议(取appProtocol 事件数量最多的 Top3)、应用协议支持跳转溯源。</li> </ul>	Andreastors Andreastors Andreas Jantas of Takitas of Takitas of my

# 5.4.7 脆弱性

切换至**脆弱性**页签·进入脆弱性页面。脆弱性包含**弱点和弱口令**两个Tab页·支持 Tab 切换。默认显示搜 索框中 IP 的弱点信息(同弱点管理页面中根据该 IP 查询的结果)·如下图。

		4.805	- B
		ertte	8.028
	HARE - TARES	BLAIK COMP.	
61218			
		818 - T - 488- N	011.0
	-	sense - ramon -	ener ener

切换至弱口令,显示搜索框中 IP 的弱口令信息,如下图。

A'LPHA	1212	e-mti -	Q-AMINI		6 B30E -	-	* 8488-	S SHEEP				D also 2
10.00	ord,											
192 104 11 120											6 4211	<li>(1) 93</li>
65 0	100.0	inde.	ARMO:	inniai1	ant 11-16							
-												
www.				100.0			ANTE:		100.1	Attentio		
								123.00H				
										1118	9	82 1 2



若资产处于防护中状态,除弱点和弱口令两个Tab页外,增加漏洞补丁、病毒木马、网站后门三个Tab页。

切换至**漏洞补丁**·显示搜索框中 IP 的漏洞补丁·数据来源于 EDR·点击右上角<EDR 扫描>·可跳转至 EDR 设备页面。

АЛЕРНАТЕТ - на о лини и авыно и селе - о селе - и ягия -	0 8458 -	
All NEW Departures		0
(The result for	(	State - o
ER INFOR EARD AND AND AND AND	2	
BAR BOYS BUNTIN BARAN BURTHO		LIFELB
ReinyTest -	HHILE I HITTO	MB =
ARTHTE CONSCIENCES AND A CONTRACTOR AND A CONTRACT AND A	0	191
PRERVERSION Annual TYPE	. V	54 E
#2.0203-00-0778-70388-1779241-678000283102442042880884	&`	
webs世界的经中行的A Statione Veb1世界。		

切换至病毒木马 ·显示搜索框中 IP 的病毒木马 ·数据来源于 EDR ·如下图所示:

A&LPHA	* \$206 - 1 1228 - 1 Brill - 0 MARK -	5 ann -
achimit Sheloch		
400 (ML 21 (M)	er e.	n #### ~ 07
DATE CARE BACK AND CHAO		
ano atten anti-tre section surface	· Lx · D	10008
	and the second s	Milesi -
Constanting and Constanting of the	augure juur area	2010-09-00 16 03:01
	2/1/2	ATR - I - NAC- RE : D

切换至网站后门,显示搜索框中 IP 的网站后门,数据来源于 EDR,如下图所示:

	on- a sain a scal- a sain-	
IIII. Instat		
National Street St		a #erk - 0
INC. CANTA MAN AND AND	States States	
RAN MUNI REPORT REPORT DESCRIPTION	11/10	12400
никалан н	A REPORT	Without (
C Viscon Contract of the Contr		001000000000000000000000000000000000000
Charles and Contract 200 Secondary - Exercise	.0P3067806326.10%	2019-00-02, 02:402,02
C Sine Constraint of Land and Bart Section Sec. Sec.	40-40(0)(Clips 10)	1775-00-00 TX XX 13
Constitution and Contract Contract of Contract on the	Providence Alex Providence Alex	2019-06-99-90-00
Charter and Charter to State Carter Cart	ANTERNA ANT	275-0-0 110.0

## 5.4.8 资产指纹

切换至资产指纹(有对应资产时,才会显示该 Tab 页),进入资产指纹页面, 默认显示搜索框中 IP 的资产 详情, 数据来源于"资产管理>资产管理>资产详情", 如下图所示:



ALPH	A	n en u néme	-			1-11- a AARE- 5 area
	Bartini -					
Cigo and Au	NA.					4, ANA - 12
10.0	-	tines and	0.041	am anal		
1000						
	1142	- weight			88713	and an example of the second sec
	104	. Aut			17484	• The set of set of the set of
BAGR.						
	877	100100-01100			A****	
	8*NE	2004031000			107805	() M
	8758				851	
-						
	1141				8710	

若资产处于防护中状态·支持Tab 切换·除资产详情外·增加监听端口、软件信息、账号信息、运行进程四个Tab页。

切换至监听端口页签,显示搜索框中 IP 的监听端口,数据来源于 EDR,如下图所示:

	C LENDE - MARKET - & O'RIN' - IS O'RIN' -	8 0/80 - 0 1000 -		0 ****
nen Deter				
HER HAR TANK		Ő		- 11.12
the scene codes	BARD MARK DARK		0.	
store and much weat	aries .	Nº C	2.	
902.1	TEMPOR -	and in the second secon	Nume -	
8	159)	Ci lini	29 Daw	
VA	285	Commil S	mind on	
386. 270	(F)	S IMMI S	75000	
1481		S I MARKED	and lost	
1993		1111 Q	140522.018	
1627		Mark .	initial wa	
1040		JOY	****	
10.0	-	Ohn	100000.000	

切换至软件信息页签,显示搜索框中 IP 的软件信息,数据来源于 EDR,如下图所示:

A&LPHA	· anno · · · · · · · · · · · · · · · · · ·	·	B
scouts) Average	11. 0		
101106/001	No or		5. AUT - 121
ER DANK (ISRN RHWI	inder man man		
1010 1010 1010 1010			
1011 Q	000	804 -	water -
HIERSEN	W09241	91.9390	1 Property Page 106300 contraine
· · · · · · · · · · · · · · · · · · ·	ADD TO THE OWNER OF	FALLOW	Laurante par mainte para
Anoster That and one Atline			
many I	Prior Composition	11.00.00	In Party of Assessing our Classe
tanuan teran tanta Conja fetar	Outpatha homes	this canada	
Interior Transferrer Conservation - 194	Netropie Station	642004	
xxtheoreman)			
The Propulsion stream (1911)			
MARK Provanie Market	init bearing	-0.02.00.000	Chipmental phononical Process Instance
PROVIDED AND DESCRIPTION OF A DESCRIPTIO	the country of	AATH	CoProgram Year collisional contribution (10.14.11.1.1.1.) allowants and Demontry Dr.

切换至账号信息页签,显示搜索框中 IP 的账号信息,数据来源于 EDR,如下图所示:



Distant.							
E-101.74.24						4 848	- 0
to other three	ANNO 10540	and arms					
ring print aven the	Anne						
Are -	10.000	Arts -	area i	NAMES OF TAXABLE PARTY.		LONGSON 1	
	8	101003000	CART	+7:30	100	94	
<i></i>		revenues.	Cart	12.00	0.995		
here :	1.0	tion 1	CREE	1758	2000	) :#S	
No. of Concession, Name	28.5	1041	049	47128	1.000	5	

### 切换至运行进程页签,显示搜索框中 IP 的运行进程,数据来源于 EDR,如下图所示:

Statuck					S.			
au ativa	Galles Read) and		-		Di			
					0			
1984 -	and an	195.08	DIVAGE		-taalgeen -		1010	
Summer die Provinsi	-	1.10	tion.		Oreanet artist	101044	84	
toine .	(m.		ican.	** *	mante and	0.000	**	
170-14	-	11.043	ion.	Salar and the second	Distance	0.000	-	
075.04	Citation and Doct of	1100	-	No research configurations are set of the se	- Climerer			
and an	C. Transmission and	2100	1.000	and a start and the second start of the	Constanting in it as	01000		
	C. Designation of the local distance in the	1.000	100	Contraction of the second	and the second second	0-0104		
	Company and the state	1.000	1122	S and S	and the second s	1 description	-	
				902 903 903				
			5.02 5.02 20 20 20 20 20 20 20 20 20 20 20 20 2	100 100 100 100 100 100 100 100 100 100				
		eo/, 10 /,	Ure. 12 00500	100 100 100 100 100 100 100 100 100 100				
			501,00,000,000,000,000,000,000,000,000,0	90-90-50- 90-50-				
		"./Cf	Source . de Son	1000 1000 1000 1000 1000 1000 1000 100				
		1.10% 10%	Source . 12 Der Source	100 100 100 100 100 100 100 100 100 100				
		1.10; 0, 10, 10, 1,	SOUL					
	is to the second s		SOUTO					
		·'/C;©() (0);?		1000 1000 1000 1000 1000 1000 1000 100				
		1,0% 10 %	Sollie	100 100 100 100 100 100 100 100 100 100				
			2011, 50, 50, 50, 50, 50, 50, 50, 50, 50, 50	100 100 100 100 100 100 100 100 100 100				
Ň								





# 6.1 Investigation

## 6.1.1 功能简介

Investigation 可以使用不同查询条件对安全告警、 异常记录和原始日志进行查询。当用户为租户时 · 只显示 根据来源安全域过滤后的数据。

◆ 安全告警、原始日志和异常记录支持弱密码敏感信息隐藏功能。
 ◆ 系统默认开启该功能。如果想查看弱密码等敏感信息,需要输入 admin 用户登录密码进行密码校验。

### 6.1.2 安全告警

### 选择 "安全分析>Investigation>安全告警"页面, 查看安全告警页面,如下图所示。

90							$\sim$	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	0 0	8년			- E - E	1886 J
						6		2		國民 331以 張峰集		<b>(3</b> 9)))	8 99 ±	没有 ~
作场群	i [	maikin (CV	ミ油(利用)((用))((用))	成於情報	这些存在vetstel运门	2298	网络咬击拳	(11850年 18/8年)	± ∰∐∳ ±	eriem (devic	etXiz	±⊴8≱78	en en	
ezd	b	6112/0 R	18 W 18	e Bitani	1 897AB	ambu	10.845	10 MATTES	術 勤業の	1				
						$\prec$	5							
800 500					36								-	
800 500 200					ji V		0							h
800 500 200 600		-		See 0			0	<b>Dall Dest</b>	Dellas					ſ
800 500 200 600 300 0			10 12 29 JUL 81						2020.13	2000 a				0.3000
800 500 200 000 800 300 0 9-12-3	29 500	0000 20	20-12/29-01-50	00 2020	12 29 13 00 00	2020 19-29	0436600	2020-12-29 060000	2020-12-	29 07:30:00 24	a20-12-29 0	00-00-00	2020-12-29.1	0.30/00
800 500 200 000 300 0 10-12-1	29 506	920P	20-12-29-01-50 R#50	00 2029 00 2029	901500 901500 901500	2020 12.23 B	04 3000	2020-12-29 060000 911WIINNEE 90	) 2020-12- M/858AW	29 07:30:00 21 28 07:30:00 21	<b>11</b> 120-12-29 (	10000 10000 10000	2020 12 29 1 Refet	0.30.00 (2.80)
800 500 200 600 00 0 100 0 100 0 100 0	29 50	9000 200 920P 118.72.62.11 3	20-12/29-01-50 R650 220-154-13 4.4	00 2020 MH 7 2020	12 29 03 00 00 941 870 14 10 E Sec 2010	e£.ef. 9505	04 30:00	2020-12-29 060090 912WINNER-20	0 2020-12 MERAR RH	29 07:50:00 21 82468946 2005-12-29 11 1	2:47	angenere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere Benere	2020-12-29-1 (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (20-32) (	0.50.00 (2.50.00 (2.50.00 (2.50.00)
800 590 200 600 300 80 90-12	29 000	92000 20 92009 20 92009 118 72 42 11 3 49 118 182 3	20-12-29-01-50 R0500 220-154-13 44 11-22-10-59	NET RE	12.29/03.0000 9/02/02 9/02/02 Microsoftacoe Apacte mod pacet Rei-Microsoft	21 21 21 21 21 21 21 21 21 21 21 21 21 2	04.3000 MENREL 60	2020-13-29 063000 91111000090	0 2020-12- MEALE 9-01 9-01	25 07:30:00 21 25 07:30:00 21 2005-12:29 11 1 2005-12:29 11 1	2.47	0-00-00 9-00-00 9-00-00 9-00-00 9-00-00 9-00-00 9-00-00	2020-12-29-1 2020-12-29-1 20日天王 (19日天王) 大市 正明(19日初	0.30.00 1099 1

可通过时间、表达式、字段(处置状态、攻击链、威胁等级等)、分析场景、聚合变量等多种变量对安全告 警筛选及查询,如下图所示。





# 点击 问 可以查看搜索语法:

153	3614	· · · · · · · · · · · · · · · · · · ·		西京	编进	2019
ANO	14	umAddress == "192.168.1.101" ANO destAddress == "192.168.1.102"		See.	小子椰子	destPart == 1024
80	15	amAddrass "192 196 1 101" OR deplAttress "192 168 1 192"	2	ayut :	存在	dest/iddress exist
NOT		NOT (ircAddress == "192.188.1.101")	.02	molecut	不得些	dayDotriven individed
	等于	amAddress "192 168.1.101"	79	10.	167	dest/4ddress in [192,168.1.1011,192.168.1.1027]
la .	不够于	wicAddwee In: 1102.588.1.101"		11001	不用于	Best/Address notin (*102.768-1.101*,*192.168.1.102*)
	大于	destPat + 1024		contant	4.8	message contains "SQL(E)/-
<	伊王	deatPort + 1624		46.280	全文检查	#6.80("主入政策")
	大于伸于	destPart >= 1024				

### 2、 聚合

安全告警支持变量聚合查询。基于不同的分析场景对应不同的聚合变量和聚合列表名。自由探索下默认聚 合维度有: 事件名称、攻击者、受害者、目的端口、告警子类型、应用协议、攻击链, 支持自定义, 最多 可添加 15 个变量, 聚合时最多可选择 4 个变量来聚合。

点击聚合变量后边的 / 按钮,可自定义聚合字段,最多可添加 15 个聚合变量。

A&LPHAIIII = nn q =man	America Commence	N SERIE - IN DOCTOR	e σ.	14117L -		0
REAL REAL						
**	字段显示 <b>#8</b>		× 1		-	
S.	有位于四 21525	E87#	10	0.92 (	8 (F) 2 (F)	· ##
STAR AND STAR AND	DEFENSION Q	200.120710	2	12 2328/31	a lass	
	2.5/till(Sublame)	Brt # formanie)				
100 E	C C C C C C C C C C C C C C C C C C C	Robell attacher:				10.000
	RORE & Ryusensensen	受得著 vicimi	<b>1</b>			-
	E247,300FieS26	EttalDiskePutt				
	El 25/NT2Epiles2NEDermit (	● ● ● 〒 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●				
2020-72-05-000000 2020-42-20-24-25000 2020	354·后方器作识版本(satisfieve)	② 自用性的(appProtocol)	2009	-12-III WIDOUII		20100
	(29) InveCence)	10.3485/sitCharts	- B	2011年1月	- 用料方案: ()	0.80
A 100 100 100 100 100 100		The Lot	I IND		10005	
A 142 200 14 144 200 Da and	- 44	-	AND	***	ARCEN.	
140,200,10 TAU,205,30 (2010)	White and vice-il	90 M		80.0	人間的基本	111

-	5	

DECHT I MAD	ipitar (\$	sun														
									0 0	東注			1	4	88	-
は算状会に	1.00	to TEAM	10384	<b>2</b> +318												
10:22:45	无	<b>田田市</b>	福司港市	內容信意	每-91空制	10月	THUR.	E E	itm.							
AEE:40日1	0.8		10													
东部北京;	市式	大学	10233													
										(RB) 3191	9 高地東 二位間	0 83	8 :	819 1	26	∧ 差許
STAR	ness	CVERRINGER)	10.65	12.400 Evolution (2017)	2276	05938	108813	825	90.100	HW MA	推翻用文件编码路	(anne)		1:10	1	参加后字书
新会交展(	011250	NAR 588	n Bria	0 19762	取用新安	攻击器	201	前中島名称	820	文件目	BREER	DHR:	<b>n</b> []	自文中大		90768-01994

然后选择要聚合的字段·点击<**搜索**>即可(可聚合条数不能超过200000条)。选中时变蓝色·再次点击取 消置灰·选择的聚合变量越多粒度越细·最多选4个字段。不选聚合变量时表示直接查询。聚合后效果如 下图所示。



### 3、保存发布

输入相关查询条件,点击<保存>,填写名称、描述、建议、分组及保存搜索时间,保存。保存后的条件可


### 点击左上角 • 按钮查看。



输入相关查询条件· 点击<发布>·选择要跳转的功能模块· 如创建统计指标· 带入查询框内表达式并写入 指标配置过滤条件以及数据源(安全告警)。





<b>SLPH</b>	A	0.88	C 4.04400	s		0 938 <b>8</b> -	* 0/08-	o sheete -
ever ) wa	65 (99)	en stone						
基本信用								
+ 9890	104.00							
+ NGR8	1041-010	(m)						
1665 <u>1</u>	(6.FA20)							
distant.	810.0 mil	at any second	and bartha					
RANGE M		_						
2100.00	9259					*5		
* mained	25 >		除人	奈井教護護, 过去等	in .	*	Ŷ.	SV
l+1	2494	😑 alamTag	- ['Mot'] -100 at	opProtocal "ftp"			e.	0
	iline Br	-					'l'	
	机计范围	court		× .			2	
	1080	19		-				
3						×		
	用氧化化	-					G.	
30/	的化计结束					2	6.	
	4276				1	2		
1	10					(s. 1	Š	

## 4、 字段显示

点击 < 按钮重置告警显示字段·可选择安全告警列表展示的字段内容。如下图所示。

其中·点击已选择字段后面的 号可以删减显示字段·点击未选择字段后的 号可以增加显示字段·然后点击<重置>·完成显示字段的重新设置。

			.02					0.4	88	11	-0.88
6,000- 6,000- 3,000- 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	2020-07-21	015200 25752	Con	200217-21 15:200	2005-01-11 IT2	<b>G m m G m m G</b> 500 20022		2000-07-211100.00	250.07-21 12.5000		InII.
P10		HISP.	DAM .	82940	284	(196940)	mento	61004	192259	101689	REVE
a#90 80	Ξ.,	HITHMETH	1992030-0021	18457	18302-01	- 00	102	196	4891	3929-07-01-1011-28	+10.77
SERVICE.	0.	Mospad (nil		46786	10.11.31.100	80	TOP.	(Vida)	mibitin	3000-87-61 W 11-78	
1.Botheter	-02	Service Station		50010	10.20.08.88	99.	108	104	1022001	2020-07-0110211-28	AUT
RMCHARANT/	20	ALL REAL REAL REAL REAL REAL REAL REAL R	(#)	35100	81.251.985.902	00)	TOP	Hu	ADRIN	000-07-01-061528	10.00
(Atricin)	2	ATTPROVEN	10	8031	101-225-08.101	400	105	30066	ALC: N	1020-07-01-01:01:26	141012
Distancia /		54EL0CODE UT7-IL IIS Crossed Station		1015	10 20 56 69	00	TOP	190	2008	0000-07-01 (0:11-26	*11.8
antyligtundroppost	0.4	ASSERTATION ( WE	1028-48-112	THEF	10 50 2 61	60°	TOP	100	marian -	2020-07-51-00-01-28	
#DG(appPreface)		ALTERNATION	1410	1000	1021013.30	10	1121	. HE	almetri -	2010-07-01 16-0-14	10.00
WACK AVENINGS	0.0	HUNT non-Diffueir a	100.26 12.06	52021	10.11.36.100	195. 195	10F.		0801	3039-07-311-0011-24	402
#Clockettines	0.	HITPENDER	11024-0.1171	ADDT.	10 852 01	20	158	1000	mean	2020-97-01 Mc11-28	*12
St.ComeStatut		ADDREET FOR 14-50 EDIA and		1414	101134120	10.	NOR:	105	00.04	1030-43-31 10:11-26	-
alertane.	0.5	ADDENTIFIC COD	1038.46.113	DHD	(630.2.9)	00	10.0	. Hes	A(691	3029-07-01-0011-28	100
- Million August Ray	9.	ASSAUDITAL ( 1942) 1988 (		34946	18.11.34.120	101	104	145	0800	3020-07-311-02.11-36	*102
Report	0.1	X560年無書成(現任 初期)		54313	10 11 11 195	10	TEP	101	内容利用	2005-07-011012-28	*12
and the second s	1.	从总标题册式(特征 和别人)		540.0	10 11.55.155	40	tor	Hali	400044	3000-07-02 46-02-28	Attem
		1008世際語(単臣)		R-HAR-F	40.00 10.0	100	Burger C	1144	man in terms	WHAT IN NORSE	-



#### 5、 导出

点击 *** 按钮· 可按照告警列表展示字段格式·导出最近 10000 条告警· 导出文件格式为 CSV。如下图

## 所示。

1	A	В	C	D	E	F	G	CH	1
1	起始时间	事件名称	威胁等级	攻击链	攻击意图	来源IP	目的IP	模型类型	处置状态
2	2019/9/16 14:32	規则引撃さ	高	其他	异常事件			高线模型	未处理
3	2019/9/16 14:32	消息队列胡	高	其他	异常事件			离线模型	未处理
4	2019/9/16 14:32	统计引擎故	高	其他	异常事件		N	高线模型	未处理
5	2019/9/16 14:32	定制规则引	高	其他	异常事件			高线模型	未处理
6	2019/9/16 14:32	CEP引擎故	高	其他	异常事件		SV	离线模型	未处理
7	2019/9/16 14:30	mfjtestut	高	其他	异常事件		123.123.	1高线模型	未处理
8	2019/9/16 14:30	其它离线3	高	其他	异常事件		111.111.	1 离线模型	未处理
9	2019/9/16 14:30	140.205.1	高	其他	异常事件	1	140.205.	1 高线模型	未处理
10	2019/9/16 14:30	Waf离线30	高	其他	异常事件	15	10.10.10	, 离线模型	未处理
11	2019/9/16 14:30	192.168.3	高	其他	异常事件	0	192.168.	s高线模型	未处理
12	2019/9/16 14:30	fishcocod	高	其他	异常事件	00	34.89.99	离线模型	未处理
13	2019/9/16 14:30	221.0.92.	高	其他	异常事件	072	221.0.92	离线模型	未处理
14	2019/9/16 14:30	欢乐豆07番	高	其他	异常事件	0	90. 2. 2. 1	1高线模型	未处理
15	2019/9/16 14:30	192.7.1.2	高	其他	异常事件		140.205.	1 高线模型	未处理
16	2019/9/16 14:30	apt-edit]	高	其他	异常事件		12.10.13	, 高线模型	未处理

### 6、 告警详情查看

告警列表单击某一条事件,展开该条告警详细信息,如来源 IP、目的 IP、端口、地理位置、攻击方法、模型类型等信息。如下图所示。



在**数据血缘**区域 · 可以查看该安全告警信息的数据来源、原始日志/异常记录和模型类型等 · 方便用户掌握 数据的来龙去脉。如下图所示。



AILPHA	THE G NO.	Q AMES	- ALEVERIA -	4 8806 -	8.8	kiett -	• 907°1018 -	0 8	4111 -				🛛 admin
• =								0 0	#11				88
	accessive.	9052	480	the	NUME	HENO	entio	distant.	alasense.	110100	THE PARTY	-	-
10.0	2021-05-12 00:42-54	WILLIGAD WING WY	100 (100 (100 ) 50	40.966.00.01		811.0	yerotrastery 74ametet	20)	1126.14630	948	88. C	make .	11.78
-													к
4	"Anta") "	20100104								0			1
( man										2			-
		8150×17		Wells.			ADMD.			C annu			
		WHITEN 10.20 THE RD		NUMPOT OF STREET			B.C.B.T.MPRIME	100		REINER	Q#70		
1000	w(						18A18			1			_
5.00 2.00 - 0.00 - 0.00	() 長行ちの形式会形に、2 () ただ長行時は日参加で、2 () ただ長行時に日の一てあたい () () 長二 長二 かごかごかの) () () 長二 長二 かごかごかの)	- ARRIGHTSSER He and Shows I form () Mark () State () And () He () State () And () State () () State () And () State	DANEBUNIT. NU BOTABORLINEN NOXFRE. NOV,	44/6/15.5.0 <b>0</b>	£*.					-	81241	2 ANALY	
8.975	8					E (MN)		X					
	pi territaria		and the interview	111.4114.000				5					
т	京大専用工業のたちはかい	2	# # 10 (H (H))				20	3					

**已阻断**标记: 在告警详情中如果告警相关 IP 已经添加到阻断策略中时, 告警详情页面会显示"已阻断"标记。如下所示。

	estatellari - adametra -	4 500 DHF -	a soliti • • •	35 ⁴ 第19~ 0 3	BERT -		🗍 admin
• 15 NicAddiway "192 MM 1 1" (10 dat	194889995		N	00	P =#	(a []*	-
Rena limati niena int	r KRAZIN MHIG R	nice made and	Par and	Burnow UAR	e esto ester e	An	
NR.000 VIE.000 400,000 NR.000 NR.000 NR.000		3019	3000				823
2021 01-01-020205 2021 05-1			(-55-1555 B1000	nin teater	02-30-00:50:00 -2571	00 (0.000) (0.000) (0.000) (0.000)	1.03.12.000001
- 20/0/10113031 EB	anomin'	A THE MARKING	**************************************	700490517 2514823 I	16223.2 BIL	FIFTHER DODE	68
192 195 13			間間的 seconacy 日本化学	_152   M	64.256.16.12 -	anta) ( anta) (	5218
The state of the s	S.	^r S	114		8.946 FTP2 8.068 (62.)	4回来46 80分钟,这三次98	

## 7、 告警详情联动

查看告警详情后, 点击某字段前的^{QQ}按钮, 可将该字段内容快速联动到查询框; 点击^{QQ}可链接到相关 页面, 如情报查询、追踪溯源、模型详情等页面。如下图所示。





事件处理。选择一条告警,查看告警详情,点击<**事件处理**>,可将该事件标记为**未处理/处理中/处理完成/ 误报状态**;点击告警列表上方的<**事件处理**>可批量标记事件;点击<**上下文**>可以查看前后 10 分钟的原始 日志,点击<**添加白名单**>可以把该告警 IP 添加到系统白名单;点击<**联动防火墙**>可以通过防火墙联动处 理该条告警信息;点击<**发布预警**>可以发布告警预警信息;点击<**生成工单**>可以对该告警进行派单处理。 如下图所示。



### 8、 告警详情沙箱报告

当告警满足 sandboxReportId exist 条件时, 普通查询/聚合查询列表中, 选择一条告警, 点击展开详情, 支持查看沙箱报告、下载恶意文件和下载沙箱报告操作,如下图所示。







## 选择"安全分析>Investigation>原始日志"页面,查看原始日志页面,如下图所示。

	10							0 0 =	8.			<b>D A B</b>	RI
1	nt 💀	ৰস্থিত							R\$ 6	4199 余徳間	<b>□</b> 733 §	a (879 ± 3	の「く思
	90850 900	945-558	REP	889	Banako	(110)	自用协议	28X0	设备的	日的地球 ###52	Binten	日的图家	ons请用的 名
1	2020-12-3 10.41-07	用户事の登録以近来放ら数 行動設		68 65 65 66	22		ssh :	FTF短日表	emilian iz	Elenista Rifitxon of m	Sattanie	90.91	
2	2009-12-3 10:40:57	但用成本会成功重成计	140.205.38 29	140.205.50 22	25	YOF	inte	क्षाक्रकान इ.स.	doFinewald	上市門面示 泉(古田高坡 取田島田和 泉	EM4	中国	
i	2020-12-34 10:40 57		140.205.38 29	140 295 38 22	27	TOP		診癌素量(+ 風病	duf kawale	上海时撤出) 动物研造物 动物通常用 同	上海	中國	
09	2020-12-3 10:40 57	ERRADINGE	140.205.39 29	140 205 39 22	65	TGP.		RISE WIT BIT	daFtrewal	上海同間至2 地包状语傳 动体语非常	上海	0.00	
5	2020-12-36 10-40-57		140.205.39 29	140 205 39	147	1CP		ROMERICA AN	daFirminal	上海印度云) 电信取通45 印秋语46音	Ŀя	中面	

#### 1、 查询

可通过时间、表达式、标签、日志类型、字段对原始日志进行筛选及查询、如下图所示。

-	acidimi -	110 19031 117 Hang Products Man" #######	01			
THE R.	EMI 1			- 6		** 221
84	88		M ()	=67	ani	
1965	10.	pro-ballances on 1922 (48-5 1971 and departments on 1922 (48,1-1921		Gant	0407421+1528	
-		and an international or the second state of th	.0	C ME	and all a set	
107		WIT an Advance "Advance on the	and the	344	senative visual	
	47	production on VEC 108 LTET	0	81	annihilitation/wattyles 100.0 cmm//100.0 000/g	
	147	And American An India and A. State	10 1A	787	sectors on the sector sector	
	**	shafter = 524	Ci (mm	5.8	tweep conv 32.21	
	++	400794+103	- Ante	8728	8-4732-8811	
	1747	and to the	2 S			

点击 按钮弹出表达式框, 可添加表达式条件以及组,选择后自动写入表达式搜索框内, 如下图所示。

····	S.				
1015.74010 10月15日	Same-Second 1	每干()	- #1995	- 1	
11toriya	and and a surrouting	187(m)	- 1111		

时间筛选器下方可设置聚合页面自动刷新 · 默认关闭 · 开启后支持刷新频率 : 15 秒 · 30 秒 · 1 分钟 · 5 分



钟、 10 分钟、 15 分钟。如下图所示。

P	HA	U ARRE / KRM	N- + ##11#1-	1 2507 -	<ul> <li>itrail</li> </ul>	0 katlif -		6 =
1	Band							
u							0.0 ==	
-	2.061						198	on manager i
	******	PAGE	107	1000	100003	1000	18 at 19 at 19	A.C. A.C. A.S. A.S.
	25-67 111-9	1995)* (1994)* (1984)=1	1111	in warz			403	1.2
÷	2010/07/1023-04	and and any contraction	102103-0110	102.00100-0			Agent is party	
1		interpretation in Market State	9115	44.4.4				
	200000000000	indexection of the last to the	100 100 71 140	++++				
1	2020-05-25 10:20:20	-014000	100.001.00.00	172.00101.121	101	100		
۰.	and if way in	-718404	100.554.55.22	172-10-101-120	2008	10		
	10000000000000	-formerset	ter da la la	101.00.001100	100	100		100 100 00 21

输入相关查询条件· 点击<发布>· 选择要跳转的功能模块· 如创建统计指标· 带入查询框内表达式并写入 指标配置过滤条件以及数据源(原始日志)。如下图所示。

AILPH	IA	Q AMME	S and store -	L Settini -		s n+sz -	o saltra -	02			() estet -
-	aline mella							97			
* 0	1032240 - 11877						×	$\mathcal{C}$	0:0 =B		C
F. ==	12 700								2	(9) montained in g	4.4 = 10 10 1 5 1 = 10 k
	***	antes	620	1000		PERSONAL PROPERTY IN CONTRACT OF CONTRACT.	WUGARRED	67942	kares	(LEG 214	a (manute)
	anti-re-re-sector	10098000	1929	(40.13			o'V	2 =	*1.02	10.001	" =3+0411
W.	uqudid tissuis	HTTERE	4479	381.07			12.	0	410	10,4470	4 Average 1
(4))	0028-00-01-02-10	111/2008	8434	(64)-1				U.,	1.100	12127	AcomPagementages
112	1000 0010 (101218	ALL BRIDE	84.74	-90.0		9. 0	1.	X-m.	214	10407	1001
11/2	3020 85-27 11:5210	14/81	10.164	18.000				Ches.	141	- 10	HERE
313	100-0-24 (102-0)	1111-101-014	1,040,000	(40.92				「漢	108	19491	140491
115	2020-06-21 1232-12	111-8405	49.79	34112		1	S	194	#18.	441	Heles
¥0[5	mm+45-51 11:02:10	Tool and the	8418	18111				100	4.10	4(10)	HERM
Canadada	THE TOTAL	COMPANY.	10000	0400	5	÷0:		101	100	Bath	10.044
ALPH			2.50000	1 \$205 Y	0.620 <b>0</b> -	• 3/#*/E •	C 5488-				D are
820H - 83	and the sec	88			3		0				
					0		2				
4.0000	( mail lance )				3						
				0	X	S.					
+ 90428	and solution.			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		2					
ALC COL				N.		. ~					
				Ox		2					
19982	and show the second										
				0	1						
RSIST	201	1	X		0						
2.61.8	2600		- il		5						
+ 11996	74.		X								
10154276											
30	[insertion of the second secon	the state of the s	C+								
	spanie in weak	ana i 1674					0				
	2010 021	1					(A)				
	WH208 (mm)										
	1000C 10	SU.									
1.0		5									
	and the	2									
754	and the second s										
=0	CONTRACT OF										
-											
- 817	383										

## 2、 保存发布

输入相关查询条件, 点击<保存>,填写名称、 分组及保存内容(默认为搜索, 可多勾选保存为可视化)并 保存, 已存搜索条件创建完成。保存后的条件可点击左上角"按钮查看。如下图所示。



### 保存查询条件

	100 M	- Selet Millianingsoni	anite .		-	
	- MAAA - warning	- Sec the addition	entre .			1 20 H 10 1 10 10
1000 1000 1000						
				1000	( and a	Sugara .
					C.J.	
	A DEC OF TRACE			-		
	110 0 0000	10.0		-	00	
	3010.01		*)	100 Tes		
	Contraction of the					
	ante dive la	100				
		181.88	dian, someon	-0-		
				V		
				=		
			10.			
				il in the second s		
				. C.		
	-	NAME CONTRACTOR	NAME CONT OF			

### 查询已存搜索

N . Intelligible 1	BMILLE		1, 3× -0, .	
■ LdE®®C	**************************************		. aughteased to house ?	0 0 #8
	π	88	statutors Jacob	× 1
er	Π.	94 B B		07984
2.选择分维	Π.	用 <b>用量</b> 型行为		Cirita
	<b>E</b> .	23.946	Wether + thankt, J	
	π.	WEEKSIE	NgTide	
	π	010(20)	Aug Tig par and the Aug and the and the aug to the aug tig the	
	<b>E</b> ,	F1Pdb/2807	Wine C	
	π.	1112468		
	E .:	10%B1	h hat i han i h	
		NERE		

输入相关查询条件 · 点击、发布> · 选择要跳转的功能模块 · 如创建统计指标 · 带入查询框内表达式并写入 指标配置过滤条件以及数据源(原始日志)。 如下图所示。

ANLP	НА	niti (Di annes	S at the	L Sellin - n eren -	-	o salatite -				] anns -
0 E =-	0 12 20s	S. I.I.						<b>0</b> 0 =8	19	0 00 00 00 1 XX - PA
	+uminesi		624	100*	PERSONNER	INGENEED	67949	ABRES	ANG CH	a (manufacture)
	sale room	imitatel	1929				-	+180	840	H =======
<i>k</i> 1	00046-0110.02.18	HTTRACE	.4479	Sales?	8		100	410	10,457	4 eventeta
		111123433	8434	16131	+		100	1.100	12162	Accelementation
	3004001-04218	erre-Relation	1434	10.00	.0		100	408	19497	1001
	3039 05-27 (1.5214)	14/88	12144	14.40	4.		140	41	-	Hartz
10	10040710314	0110-020-020	1,600	2.4033			195	105	9.00	140/67
11	22210/21123248	1117-WARK	6579	DALLER			the .	*18	4441	Helen
(i)	10046521110219	HIT/BACK	8414	16121	- H		161	4.100	6101	Histor
	WHICH OR IS	COLUMN A	3434	0000			100	200	BACK	1004



LPHA IIII	Q 2000	AND A REAL	* R*93 - C R083 -		4
e oraz anaz bais					
*##					
1990 00-011-					
aneg (dilimit					
	-				
888 8604					
1042 10		+			
14238					
states in soldiers	- 9419		.0		
math and				ć.	
REAL OWN					
6108C 10				N V	
				ò	
Mand 14	+				
Allowances (T)					
				_0/2	
1 M 1					

### 3、 可视化数据

点击<**可视化**>·以图表模式展示原始日志分布情况。可手动对图表进行配置, 支持的图表类型有柱状图、 折线图、面积图、表格、饼图、 单值图等。如下图所示。

AALPHATTE	8.9108- 8.8109-1-	#3448##			0 0
and second data	No.	S			
			0 0	H	
E SE 2 HER LADORA		2		10	10 5 10 - 22
BE BE BE AND A DESCRIPTION	2º				
No. And Address of Add				1488*	#E
terior 1		5			
The DEPARTMENT OF STREET, SERVICE OF	0.0				-
10.00 - 14 -					
A CARACTER AND A CARA					
		144 Ata	* 70 B		

- ◆ Y 轴支持统计方法: event count,count,avg,sum,max,min,distinct count(默认 event count)。
- ◆ X 轴配置: 默认按照采集器接收时间(collectorReceiptTime) · 根据 Y 轴统计方法可筛选不要的字段: event count、distinct count:所有字段; avg、sum、max、min: 数值类型字段。
- ◆ 维度配置: 默认没有维度字段 · 可点击<添加>按钮添加聚合维度字段 · 最多添加一个; 鼠标移动到字 段筛选框 · 显示删除图标 ·

### 可视化样式

在**可视化**页签点击<**样式**> · 可对图表样式进行设置 · 手动输入 X · Y 轴单位 · 基线值设置 · 所有内容非必 填。设置好的图表样式可在数据可视化处展示。如下图所示。



		- B - 6 - 85	
R 49 2 100 Lague		Hit follow and	2 30 10 H 40 X 30
	•		1 and 1
E-m			
80 /	-172		
B res	1		
#0 (H)			
and the second se			
. THE R	the second se		A CONTRACT OF
The second secon	•		
In the second se		 $\sim$	
Energy and and an and an		e S	
Sun		80	
STATE AND ADDRESS OF A			
1010		000 000 000 000	
TARSONNAL ATTR		200 21 21	

### 4、 时序图查看

点击<时序图>· 查看原始日志时序分布情况, 支持手动选择时间粒度。如下图所示。



### 5、 字段显示

点击 按钮 · 可设置原始日志列表展示的字段内容。如下图所示。

其中·点击已选择字段后面的 号可以删减显示字段·点击未选择字段后的 号可以增加显示字段·然后点击<**重置**>·完成显示字段的重新设置。

1170 A		NERRENCE	0.511		1080m	#88048	<b>中和33年日</b> 年	699.05
CUMPTO DO	un	Constar nijest	化学校学会の計量用計	181,011148,328	123.14.140.89		WHOM:	#050#
Signal and the second second	C	Notest JT 197937	10070574884	10121-045128	175.00.001.00		PULL N	<b>ADIERH</b>
sigman (		2000-07-21 19:39:37	0.969.0.0520.0	012136.00	(0,00.00.0)		#2103W	(BADDAR)
ARE DO LONG		2008-01-07-10-50-51	这种种中的现在都有计	10121145128	172.10.100.00		Riticle	A DOM N
Inter the second defenses		5105-67-17 1838-57	EXMANDER AND	standard radio state	172.10.100.00		61128	0.5954
Call Call Call Call Call Call Call Call	10	30347-17131011	0.002964066644	renzes sala nere	100 100 100 100		+++32m	6.00044
	+	2020/07-37-10-90/97	100000-0000-000	10121145.105	(72.10.10) #4		W(+129)	Actor
OB STADAO COMPANY		2006-07-07 19390-07	STATE AND A STREET	19121545-00	012 10 100.00		Ref URK	RELATION
Server Sector (1975)	14	2020-07-07-12-50-07	CONSIGNATION .	101211545-028	172 HL 181 14		81125	(\$554 d)
*889%		2000-07-07 18-18-87	CONTRACT/RAIL	10121148-488	172.16.140.46		6411036	annipa.
(and (and and	1	5300-83-17 T9 WITT	158870431884i+	INTERNAL DARLEY	6427.311.6		and state	BOETH.
RP90-Hpress		2006-07-02 19:09:97	254929-00129-0012	10123-040,028	COLORD PT		Worker .	(Anticola)
ROUGH BOOM AND	1	TROPPET TO SURVEY	Anna antipair	0010145-00	ALMOND IN		go+ink	annan .

with distance in the local distance in the l	****	ADV.	1000P (	85010	91108110	100.000	1.081
20.000.000	Decision of the local	102.00108.244	142-148-1402200		Reactor	100,108,00,00	1
	becomposed.	101.001.000.000	100.000.000.000		station	10,000,007	TRANSPORTE
	100203210	101 101 100 JUL	102100-000100		filment (	100,000,000	
101000-001000	BROWNER.	10.0010.00	100.000.0014		100.01	10.100.017	
	Courses.	10.01.01.0	100 100 10 10		Since .		
3444.00A	NUMBER OF STREET	10.06.00	100.000.000		1000	10.000	
	111100-000	10000	And the result			No. best	
prime in the late	*****	100.444	(1) in m(-)		10.000	Name -	Attention and an order to the
1000	1000002059	10,000,000,000	10.100.00.00		date:	NUMBER C	
( 100 m ( 100 m ( 100 m (	Internet Concer	2404441	10000		1000	20.0753,45	- An page Attraction used 15

6、 日志导出

点击 ^{国 导出}按钮 · 可按照列表展示字段格式 · 导出最近 10000 条日志 · 导出文件格式为 CSV · 如下

图所示。

1	A	#	C D	E	÷.	G	н	20	1	ж	1	M	N
1.	采集器接收时间 專(	件名称 来测	top Elfur	来递用户:	在事件设备分	设备名称	UR1	207					
23	2019/9/16 14:02 508	B远程准192	168.1192.168.	198.203	网络IDS	192,168.	30.57	4					
3	2019/9/16 14:01 SM	B远程准192	.108.1192.168.	198,203	网络IDS	192, 168.	30, 57						
4	2019/9/16 14:00 SM	B远程潜192	.108, 1192, 168,	198,203	网络105	192, 168,	30, 57		$\sim$				
5	2019/9/16 13:59 思j	<b>意</b> 文件F192	.168.1192.168.	30,15	网络IDS	192, 168,	30, 57		2				
0.	2019/9/16 13:59 图)	重文件FI192	. 168, 1192, 168,	30.15	同語IDS	192.168.	30.57		0				
7	2019/9/16 13:59 ¥21	B行为分192	.168.5192.168.	33, 211	短度面计设	192.168.	30.57		N.				
8	2019/9/16 13:59 BT	TP请求让112	. 1, 1, 1172, 16,	100.2	审计设备	ftp-test			Coursel.				
9	2019/9/16 13:59 80	TP请求让112	1, 1, 1172.16,	100.2	南计设备	ftp-test	/ls5/forv	m. exe, jse	esionid=6	P9D40B211	0D3F64D04	895525290	C875
10.	2019/9/16 13:59 SM	B远程道192	,168,1192,168	198.203	网络1DS	192, 168,	30, 57	6					
11	2019/9/16 13:59 願う	务器遇到11.	11, 11, 2, 2, 2, 5		应用程序	500清产国	<pre>//to_pages</pre>	. do?aetho	d=select /	from su	bstring		
12	2019/9/16 13:59					<b>町市殿008</b>	)生-APT	1					
13	2019/9/16 13:59 请3	求的文件者。	参数名和参数目	<b>自含HTTP</b> 响尼	2分割攻击1-	<b>司代授202</b>	世-APT	. Call					
34.	2019/9/16 13:59 BT	护请家们1.	11.11.192.168.	11, 9	审计设备	SOC语产用	1/1s5/fort	#?Cmeta="	user'				
15	2019/9/16 13:59 II:	S短文件名准	實漏洞 1602600	20	C	500资产同	15-APT	and the second					
16	2019/9/16 13:59 易	统命令注入口	文击12040050		in the second	SOC资产国	TAPT .						
17.1	2019/9/16 13:59 BT	TP请求111.	11.11.192.168.	11.6	面计设备	SDC语产同	/images7b	oost. înî					
18	2019/9/10 13:59					SOC 资产国	HE-APT						
19	2019/9/16 13:59 net	tetat毒令等	(行時 12040065	il.		SDC資产同	HE-APT						
20	2019/9/16 13:59 潤	获请求的文作	1名、参数名和1	·動包含SSI	年入 12070	SOC语产店	APT -						-

7、 日志详情查看

日志列表单击某一条日志, 展开该条日志详细信息, 如来源IP、目的IP、端口、地理位置、报文、原始日

志等等信息。如下图所示。

The second a setting for the former	Rect 10 MAR
AND AND A REAL PROPERTY AN	
ARTING BENINGS	Restaurantes and the later of the
adaCiniti Agree	REPORTED AND A
americanoise sales	Reservation a province
employeeshine against	Straphoreney, e.c. and
ematum 🔪 🧐 dent	Interfect, Baltingh
morphy and a second description	
another all	
antikogravske sjonen annen annen	
arranderer a can arrangementer an essential	
A REAL PROPERTY A REAL PROPERTY AND ADDRESS OF REAL PROPERTY.	
antibugetor between a grand all and all an	
BARRING ALCO-CLARMANCE	
WHENHARD AND AND AND AND AND AND AND AND AND AN	
advertise-story and to ball of	

8、 日志详情联动

查看日志详情后,点击某字段前的 @ @ 按钮, 可将该字段内容快速联动到查询框。如下图所示。



I see the second second second	in the second			1			
II (3000000)	- 100,000,000	1.04					
Z BORNER	- 1010.0	Later -					
10.00	· · ·						
	X						
	V					1.0000000000000000000000000000000000000	 9423
* B B STATUS	****	101	inter-	88511	PROBA10	008209	
1000 (000 00 00 00 00 00 00 00 00 00 00 0	(second states)	Contraction (second C.).	100.0007482007		10000	C 100 100 0010	
	1						
-	manna						
SME	NALESSE		and the second second				
	Rathing of the		. 105 - 10 - 10 - 10 - 10 - 10 - 10 - 10				
5463 	Ratha		n Mala wa wa katalon wa k	10		2	
M 1000	Rating	nersettele nood	n dan ing ing ing panan (	an Birtanatan	6.5	C	
M Shines		ini ( 18 si si si si si si menarikan si sase	n Maria ang ang ang ang ang ang ang ang ang an	ni Birtanan Billiorei	6.5	0	
504000 00000 00000 000000 000000000 000000		rini ; et al a nine menoritaria const	n, 1805, val en les strannes, . Intern	M Mitanian BMCarri Marchari	10, 20, 700, 700, 700, 700, 7 10, 20, 740 20, 20, 70, 700 (11)	.0°	
M 5000000000000000000000000000000000000			n dan sejan berganan.	ni Bittanoini Bittanoini Bittanoini Bittanoini	10, 2, 10, 10, 10, 10, 11, 1 10, 2, 14, 14, 14, 14, 14, 14, 14, 14, 14, 14	80.00	
MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA MARCA			n dan ini ini ini ini ini ini ini ini ini i	ta Biologiania Biologiania Statute Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologiania Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia Biologia B	6, 2, 10, 10, 10, 10, 1 6, 2, 10 6, 5, 10, 10, 10, 10 6, 5, 10, 10, 10, 10 8, 10, 10, 10, 10 8, 10, 10, 10, 10 8, 10, 10, 10, 10, 10 8, 10, 10, 10, 10, 10 10, 10, 10, 10, 10 10, 10, 10, 10, 10, 10 10, 10, 10, 10, 10, 10 10, 10, 10, 10, 10, 10, 10, 10 10, 10, 10, 10, 10, 10, 10, 10, 10, 10,		
At 1000000000000000000000000000000000000		ani, es acamper	n, lato, vel vel vel starven, . Neko	te Officiality Statistics Materiality Material Material Material	9,5 00 00 00 00 0 9,5 00 00 00 0 9,5 00 00 00 805 600	1.00.0	
All Million And All An		tani en scenarian Senariantinon chon	n dan serien de landen,	an Bitternetter Bitternetter Bitternettersters Bitternetterstersters Bitternetterstersters Bitternettersterstersters	9, 5	.0°.	

#### 9、 日志详情二维码

在日志详情的**原始日志**区域,可以查看原始日志内容,点击二维码图标可生成二维码。扫描二维码可获取 该条原始日志,点击<**X>**按钮可关闭二维码。当原始日志超过 2950 字节长度,二维码扫描内容自动截断。 如下图所示。

		NUMBER NO. 1			-		Install.	and and
		· · · · · · · · · · · · · · · · · · ·						
	Barden and Street of Stree	4.4 HD TLASSARTING	at the second se	THE REAL PROPERTY AND INC.	and "			
	status status	ALL SECONDERING IN THE OWNER		C. C. Participation	A stand and a stand			
	Marriel & Low Street, or other	to so Total etc.	A44 949			-min		
	WEIGHT MILLION	A RAY	語	E MARCENE (				
	California antonio	All ort-mate in figurations, of get	20	A CONTRACTOR				
	abdimenter	No other two	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~					
	and succession of a	AU STREET A CALENDARY AND ADDREET		区的新闻的				
r	Bich# /		C.	ACCOUNT OF THE OWNER				
		The Real Property in Low real Property in Lines, or other	dia Continue	and the state of the		about in such		and and a second second
	and the start of the start of the	tion of \$1 bit \$2489 bit and age assessed of	and the second	100 Month in contraction of	a a st. a. Compose			- P
	30 -		V V	0				/

## 10、 更多查询

点击<**更多**>,可过滤日志类型(流量/日志)、切换数据来源(原始日志/异常记录)。如下图所示。

	- 10000	4 BESE -	 	0 NAUE -		0 +***
100 8404	J.					
					0 0 ==	0.000 88
1005-029-028	3					
NDAR BUCH CHEER						
R HE R HAL					fit 3+4	B 20 8 877 9 10 - 80

切换至**异常记录**,页面重新加载。

## 6.1.4 异常记录

选择 "**安全分析>Investigation>原始日志**"页面·点击<**更多**>·在弹出的页面**数据来源**选择 "**异常记录**" · 可以查看异常记录页面 · 如下图所示。



AL	PHA	12 H MI	Q EMME									a	-
ARCE.	-	98115											
										0 0 at			**
	81 4 88 69 88 89	-	4 40	0178 N		*							
		094										4 00 g mm	- 15
													4
	00.001 80.001 80.001 80.001 61.697	-		a and any a									
	man on pro-		Day of the summer	and in diam	200-01	16.000 E	0-0.0 mone	2010.2 0.000	with we in France	STOCK TO A SHOE	"Curlings	and the first second	
	CO.M.		991121R	10000	** ***		1189	1.81	1880	4171	- mape	44722	
1.1	200.00	T STATUS	1710ETHE					2111	-11-0.41	0163		attendant.	
	300-02	10.0010	and the second s					102-008-11-020	712-00-002-1	20052	5	and service	
		T MAKING C	100000 EB					102-00211-020	10.001			(manager	
	300.02		NUMBER OF STREET					veral i	24.0000	max	-	(ALDIANCS	
	10.02		INSERT					1444		(tem)		Atelan	
	10.00	hes	NUMB ONCOME INCOMENTS LANGER					111.00.00.00.00	10.000 m			(and the second	
	20100	t science -	Transfer D.B.					100,000 11 100		() Apriliti		(anjoint)	
		T 10-00-00	100408		8			194.404.71.548		.#ite5		Anysinis	
	20100	CILLER OF			- 4			NUMBER OF		AUNT		(anjoine)	
	-	T TO BE AD						10.047150	-IFNI	all all a		And all the lot of the	
	-	risal in	- indiana	4				and started into	CINED	101003		And and	
	-	- the state	ani-keeps						25	10402		Angelante	

## 1、查询异常记录

可通过时间、表达式、字段对异常记录进行筛选及查询,如下图所示

EX NO.					
	6 0.00		No 65	-	
ani (0	ALCOHOM 17 102 104 1 107 1022 INVESTIGATION - 102 102	- 6	- Net -	autor of the	
A 8	ALADING - THE RELEWOOD DURING STREET, NO. 101	-	HAR	Ministration of Concession, Name	and the second s
er 8.	ACT (0.000 - 102 W1 011	- O'	1000 1000 1	sectors along	HE BLANK
- #E	E 0100000 or 762 000 7 001	S.	201	and a second sec	10,000,000
1.14	40 Administration (1993) 100 - 100		1 18 (m)	and states and the rest for the second	
27	F and the intervence of the second seco		Oran an r	Paraga Lengers Taxibut	
07	- and the P A (A)		C	erertal-dari	
+++	All and and a second se	0.			

## 2、保存发布

输入相关查询条件, 点击<保存>, 填写名称、分组及保存内容(默认为搜索, 可多勾选保存为可视化)并



保存, 已存搜索条件创建完成。保存后的条件可点击左上角 _ 按钮查看当前已经保存的搜索条件。

	-		875263		1. Bital	-
-	2. 2	to David David		_		
tes mains	diver.					
NY 2.700			12201 april - the Activation		and the spectrum and	- 3
				and the second sec	Sametar	
1110						
And in case of	And some state.	and state over 1988 in				
-			and the	- Frite	nesse agrice	
	-		and the line line	<u>A</u>		
		4.0 (4				
	nents Rents	C 2000 - AT	nu - <b>- \$2311 -</b> € \$2501 -	• mmm		
	nenz Renz Renz	Constra - Ann	m - ⊢s±nfi- cotim -	*. III'III - 0 NATIE -	0,0,==	
		© 22600 → 4700	na + Stalf + C Stalf +		0 0 == / 1	
LPHA	HEDE HEDE HEDE HEDE HEDE HEDE HEDE HEDE	erati a contro ~ tota	na + Settin + ⊂ Settin + saftasis - Noar lafaa + Sot		0,0 == / 1	
LPHA	n an ment Pote - Sine A A A	<ul> <li>□ 228800 → 8288</li> <li>##</li> <li>##</li> <li>##</li> <li>##</li> <li>##</li> <li>##</li> <li>##</li> </ul>	m = 4.52311 + 2.5232 + auf=ust = larar laftar = lar splar = lar	AUTPULTER HISTORIA	0,0 ==	4: 
	11 日本 10日本 10日本 10日本 日、 日、 日、 日、 日、 日、 日、 日、 日本 10日本 11日本 11日本 11日本 11日本 11日本 11日本 1	<ul> <li>□ 2.55800 → 4000</li> <li>■ 4000</li> <li>■ 4000</li> <li>■ 4000</li> <li>■ 4000</li> </ul>	eartheast - Second - C Second - eartheast - Second - lagture - Second - lagture - Second - lagture - Second - lagture - Second -		0,0,== / 1	L:
LPHA	12 日、11日 1940年 11日日 日、 日、 日、 日、 日、 日、 日、 日、 日、 日、 日本 (1) 日 日 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) 日 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	<ul> <li>■ 22880 &gt; 4288</li> <li>■ 42</li></ul>	estass - Need estass - Need Igter - Set Igter - Set I	* ##### *###### ****** ################	0 0 == / 1	1. 
LPHA	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	★ 225500 > 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4258 ★ 4			0,0 == / 1	1
LPHA			A SCONT - C SCOUT		0.0 ==	
LPHA			A Second a constant A Second		0 0 == / 1	
LPHA			A SCOTA A COMMANDE CONTRACTOR A SCOTA A CON		5+ 0 0	
LPHA		■ 2000年年日 単本 単十四型 第一型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型行為 二型型 二型型 二型型 二型型 二型型 二型型 二型型 二型				L :

输入相关查询条件, 点击<发布>按钮, 选择要跳转的功能模块, 如创建统计指标, 带入查询框内表达式并 写入指标配置过滤条件以及数据源(原始日志)。如下图所示。

AILP	HA:::: ==	-	-		• • # RTBE •	- 1001				ŭ ====
Adopt -	BANA		2	5						
			C.					0 0 =1		
<b>月</b> ==	2.064		25						-	R == H == 1 = H = = R =
	*******		100	100	*******	*******	6816		Distant.	
	200-0527105210	Castarina	1411	20110			1.78	1.00	840	and the second
1			BATE.	841.1.1				418	848	A mitemati
10		भाग्यतमा	6430	4000	1		10	100	847	A
1		industrie	1410	ALCO.	- A-		-100	100	840	+401
	and the second	Onerga	11144	33344			100	-		0.000
	mington	orrestored.	8479	miiii	*		10	10.00	040	1001
1	monitrusta.	arreduced	6439	1000.00			14	100	200	and the second s
			1470	10111			- 14	110	8.85	warden .
-	And an other states of		64.10.1				-	4.08	Page 1	a a second



AALPHA		a arres - a sorta -		1-
Real				
- 900 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100				
-9549				
1002				
NR ADDRESS				
RINK R				
868 9428				
-1672 all				
Aprile 22			01	
and a set of the set of the set of				
0	_			
Rest over -				
- 10 Decision				
A810 98				
Eferei-ar (C)				
azva 💽)			Dis and the second s	
1.1				
- en			()	

#### 3、数据可视化

点击**可视化**页签·以图表模式展示原始日志分布情况·可手动对图表进行配置·支持的图表类型有柱状图、 折线图、面积图、表格、饼图、单值图。如下图所示:

A/LPHATEE = == U ==== - = == - + + + + + + + + + + + + +				0 -	-
1010 Industry BELL	S				
( + ( = )		G	0 0 +1	1	
E MR. 21 MAN LADORAL	15	S.	#20 1010171 ALIMP	B R	- 25
And					4
	Co			LARGHAIL	e
and the second s		X ·			**
I'm DARHERMAN, HERMANNAS	0 10	<u> </u>			-
	$\mathcal{O}$				
ter in the second se	S S				
A DESCRIPTION OF A DESC				-	_
1 Miles					
	<b>0</b> .*				
	0	And Ada to		795	

- ◆ Y轴配置: 从下拉框选择,主要有 event count、 count、 avg、 sum、 max、 min 等(默认 event count)。
- ◆ X 轴配置: 从下拉框选择, 默认按照采集器接收时间(collectorReceiptTime), 根据 Y 轴统计方法可筛选 不要的字段: event count、distinct count:所有字段; avg、sum、max、min:数值类型字段。
- ◆ 维度配置: 默认没有维度字段 · 可点击<添加>按钮添加聚合维度字段 · 最多添加一个; 鼠标停留到字 段筛选框 · 会显示删除图标 · 点击删除图标可以删除该字段 ·

### 样式设置

点击<**样式**>,可对图表样式进行设置,手动输入X、Y轴单位,基线值设置,所有内容非必填。设置好的



图表样式可在数据可视化处展示。如下所示。

A*LPHA IIII	0 mmi - mmi -	+ *****		-		ALC: NOT
and a second second						
					8 5 11	0 100 00
E 44 0 100	LADIE.				BRITCHIER B	an Ban Tan - we
1 10	11. P 11.0					and the second
1						
#5 in						102
1		1				100
#1.14		-			2	- 10
1000 2101110-0	-				0	
1						a.
8415 44					0	
and inter-					V S	
					00	
LANDARD DIE					. V	
and a second second					N°	Sec. 1
		44.8	ant		A	
		Marile (12 pieces) Maril	(1) bright Bridge 17 (States	Branchaman Balan	Allower Branchitzshein Bracheltzst	inin 📕 😽 🛛 8.22 🖡
				3		

#### 4、 时序图查看

点击**时序图**,查看原始日志时序分布情况,支持手动选择时间粒度。如下图所示:

ANLPHATTE + ++ ++ +++++		a m-mm	
and managine BBDE			
(e) =			0 0 at t 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1002 4 * 4 1003 02 04 10 1004 0612 \$20(3		S S	
E ** 2 1944		A S	
190 (100- 270 (100-			1000,00.50 Pi
40.200. 40.200. 40.200.			
201-01-01-0200 200-01-01-02000	and the second second second second		AND THE REAL PLANE AND
KX000 96.17	811728888 HIN	- RBT 1007 BEFE	POLE 00770 40000 4-0
A REALFACT AND ADDRESS OF ADDRESS	· Q	Carter presented miner	A100 41

## 5、 字段显示

点击 按钮, 可选择异常记录列表展示的字段内容。如下图所示:

CPNA:	5 MG		Comments of	* STOR -	B. STORES		R 9/468-					
	*											
- ( m)									ø	0.46		- 63
1000 - 10 1000 - 10 1001 - 10	-	52	teres the		-							
	2	0								18 cm		100.81
		1000	*****	PLANET .		0108	821	140	4010	10040	011722	100
NE REAL		200-012-4281. T	HINES Hand	-			0.000		1145		men.	
*1450-124	- 1	2010/07/11/17	AUTE intend				10010111	10000	1146		1000	
Alfail		post or 1	10128 (1000)				9090101	live and the	1100		-	100
and a second second second		100-002 (0,01) (1)	HIDOR - Street		*		11000	and a	1145			+14
	1		0-457972 attention				100.000.00	11 754 46 22	1040		THE OWNER	-
			Hing front		+		01200202010	0.001	1146		and a	100
10110-101-101-	14		Horen - Donald		- K			102 223 6 106	max		(1000)	1414
	1	2000-00111-0011-0	717-835-0-898 215	(4)			0.0210	1002023144	1044		(1000)	100
			MINER-Disease									

6	安恒信息
1	DAS-SECURITY SECON

LPHA	0.005	Q STAR					- 0 Auto	8-					0
ant (manyor) And	ME.												
										0.0 ==			1.85
1001 - 1 100 - 10 1012 - 2012	- 12		+128		pre -								
E ez . (2.196)	= [	anterio di	88.20	********	204	-	101	1064	4515	1010	10.0000 044	* 12 10 - 10 1	- 120 -
	•	100-0-0-11	Annual An	2			394,963	111-10-10-0	0140		1004	+1.8	1=
Ratadionica -		200-0-11-0.1 117	ADDE COM		4			301030	4140		(	- anni	condition to
ABRING		300-017-01 14)	ADDE Lines Jef BERNEN MERI	*	1		308301	000000	0.95			-ie	
	14	201-00/11-001 1117	第四号第二日中日 三三一前月7日子 新市区第三日本書		*		(*******		11-05		R	++#	attiku
		10	100-105-97 101-105-97 840/0010101		÷		19.18.9	manierz	*****		Terret	+14	\$5.02
	1.0	andersi. tit	111-455-945 6307055-648		8		10.042341.46	30,000	1140	2	(HERE)	.928	4534
CONTRACTOR OF	1.0	200-0-7-92 117	ADDER (1044) ADD BRAND		A			001010-00	1000	S.	(PERK)	01K	**
	12	to state	107824-0-8 8000 60048-00-0	8			N HERE	NUMBER OF	10.00		(mont)	.416	-
		200-0-27-0-1 117	10027-01-8 1078-01201		3		$ 0\rangle(0 1)$		-		()000	110	10181
		10.00	NUMB 1044 CS-804-97 RADIO-109		÷		minute	- risten	gen		(Heat)	***	stitu
		10-0-0-01	80.08 10/m (0.081/8				******		man		(1424)		- 10

### 6、导出

点击 🗖 📲 按钮, 可按照列表展示字段格式, 导出最近 10000 条日志, 导出文件格式为 CSV。如图所示:

1. 新始社会 運用方式	******	1744 0498	where many manual stream	************	
(2) 2000/5/22 29:27 税100年 (BAssa, 045) 単色(Mata)税22 20	1	F	35.4 107.0 218.107.26.42 2148.6	<b>其待於證 + () 新</b> 版	Rama lang Streen Witchidty
#1 2020/5/27 34 27 成形合著 (Bhone Out) - 教育教师各独一表研究		12	1021681162042424288888888	医隐状管 网络四 他们	The Lass are from 05403543
# 2020/5/27 5927 仮記告盤 DBone-043敏麗教師書書新書2		10	58:540-228347 60:01 (01014810)	黑性幼稚 朱白彩 約約5	THE Lana inco String (0267Ptres)
集 2000/5/27 1927 提到各型 108mme-039 按用户接手系经在测进行合型	4		211.136 192003620407048204	其他校理 半分配 接续	150 Elimitationo Strato Gill 1934Ee4
第一2001/6/27 39 27 按照希警: Discare-039 按用户接关系结权指注行传管	.0		103324836235444(1920)#20	<b>当场边境 长行影 扬红</b>	Eta Elisasiano Strang (36d20eE36
7 2020/3/77 1927 指则告誓 DBins-039信用户接关系体权错误行告誓	4	1	10.328.52338.17.78.3 投影機会	网络红鹭 末分配 碎粒	to Lauring String Official
# 2020/3/27 39 27 投影合筆 208ane-025 - 現式determ的時間第	14	(E)	111.2712日122222301度目標業	非线结婚 未什起 胡蜂	Laws land Timing (\$175 date)
9 2020/5/27 1927 177市段会会 前除主持	道	- Ŧ	0116785(1420204-9201mm	网络拉提 未分配 别除	Stavaland Shing Bild HeST
10 2000/5/27 2827 板刷合著 DBone-OCOL-201教感教徒対象的编程的间开头	i#	÷.	426403 3833843 f071488	清洁放理 未分配 热行	FR Lanalwig String OTTE4223:
11 2000/5/27 2927 起目音響 - 88one-039 油雨户接予紧接权用进行音響	#	E C	20217301611348479281488	其他故障 未分配 _ 程权)	steel's' Bansiens Strep B's Needs
12 2020/5/27 2927 规则告誓: Disone-035 创建用户配质文件	1	2	1142128(15001 - 成別編集)	其他校徽 未升配 创建	Lavatarg 3tring (\$6536)(no.
3.8 2000/5/27 33:37 规则专擎: 080++-025		± 1	108.12 68.158.248.342 保助構成	其他幼稚 未办包 律欲;	12 Lievalong String: 9476ac1b
34 2000/6/27 35 27 操作成功	(情 )	I ON	182168.11160.168.84 夜到機型	其他典型原用规则 舟桥	biz ILliwalang Shing (952d51b6k)
[48] 2020/0/27 39.27 信用或功	(t)	it. O	192166.11192.168.84宽利模型	网络美型系规规网 身份	122 Suevalang String, (\$6945291
16 2000/1/27 1927 规则省署 10kome-025曹表3elete创新规理	P .	t.	202305242132445(規約機型	黄蜂花塘 米分配 一般政	Lawa long String (\$7563855
12 2020/3/27 38:37 规则含蓄 DB:208-023 報感相談多素統會2	(E)	1. A. Y.	361712016118745 经担理型	黄蜂草覆 未分配 一筋行	1.00111033/rg.2111011
38 2000/5/27 10 37 10 (FR) 使用李超过渐度门前	). E	ž )	218.11.385.103.32.88;规则模型	美術装護 未分配 主相!	行行: jueralang String @De25b8ca
19 2020/5/27.29.27.规则查看:U8cres-020给用户接干系统包造行信誉	4	ž .	21011.74461.120.0.3 投影機動	再佳软牌 未分配 一種织	Tana lang Strep (077502-8)
20 2020/5/27 2127 规则背景: DBone-030 - 箱用户接于系统初度进行音響	*		39171242172310出版目標個	其他故障 未分配 一根包)	11 Lanalang String (34554ce55
[21] 2020/5/27 29:27 板形香蕈、080min 021、「町礫松長行為」	1		103126843651684 板町種園	其他故障 未分配 一部建	Land lang String (potenties
201 2000/5/27 33-37 MYOQL 進稅兼件:Yeesp中共效	<u> </u>		117.60.02161.285.22.1肥則機型	再他故障 未力配 助行)	教授 Laivalang3ting-91e3estc2
23 2000/5/27 39:27 规则告誓: 08099-040 西欧用户知道行力	1	X	1267年1月21929043股利機業	其他标准 未力配 极权	Em Thereau automatic and a state of a sta
24: 2000/0/17 33:07 854度多種正常用引	a .	- T.	1921(811)192388.84 限利機劃	RUBLIC RUEN	212 Juleasiana 37740,09982967
25 2000/9/27 39:27 世紀音響: 04cme-040皇素(####國際取得	1 ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	5	192366-0113832437 能利權金	天物花霞 見探州 前時	Elavalang String (dT1bf5a7a
20 2000/5/27 39 37 NHI音響 DB089-000		5	222.2380430.535.29 规则搜索	网络草覆 未放配 一剂罐	5.4ma1ert3.5met(\$1107.5817
27 2020/1/27 29 27 M/SQL @R/#IT / myscie.Mit	1 ~~~	5	272.184.0.(210.5.130.190.0.000	高橋装置 素力配 前行	NR Slauslerg Strig @10051de
28. 2020/5/27 28.27 加利省量。Ubote-201001 天范重新演算用Deved 行法	<u>+</u>	X	3911129232576441988	网络双腹 水开起 引行	the pressed strep (pc) #1.24
27 JUNIOS CONTRACT ALL ALL ALL ALL ALL ALL ALL ALL ALL AL	The second secon		121 00 192 192 192 192 3 192 8 19 19	内内に度 大力配 単位	se Lanuarg strep geokdin
10 2002-211 2011年間 DB200-044 - 新聞都羅羅美一次支付	1		111 00 0 11 10 10 0 1 10 0 10 0 10 0 1	ADDA ADD 101	THE PROPERTY OF A CONTRACT OF
相口:200/50/2021和局責業:0500-00m-1集成相位任務。		ST6	11.766万万22237237231回时建国	A位机械 未分配 推迟	EX. 1.8H0 0PG 377023940109041

### 7、异常记录详情查看

异常记录列表单击某一条日志·展开该条记录详细信息·如攻击者、受害者、来源 IP、目的 IP、端口、地理位置、攻击链、模型等信息。选择一条异常记录·查看记录详情·点击<**上下文**>可以查看前后 10 分钟的原始日志·点击<**添加白名单**>可以把该异常记录 IP 添加到系统白名单;点击<**联动防火墙**>可以通过防



#### 火墙联动处理该条异常信息。 如下图所示。



**已阻断**标记:在异常记录详情中如果异常记录相关 IP 已经添加到阻断策略中时,详情页面会显示"已阻断"标记。如下所示。



### 8、 异常记录详情联动

查看日志详情后 · 点击某字段前的^{QQ}按钮 · 可将该字段内容快速联动到查询框 · 点击 · 可链接到相关 页面 · 如情报查询、追踪溯源、模型详情等页面。如下图所示:



BU AND A CONTRACT OF BUILDING				02032	12.00	
· · · · · · · · · · · · · · · · · · ·				.0+0	1	- 1
nen e le le nen ente ente	1 1920 - 1940 -					
and more even	- Churcher					
SR STRA				(18)790		19 C -
DEH HAN 92 ALL SADE	1887 BBF 8	EAS NONE	WEFEE REAL	9010305K 348	NAME TRANSM	2346.54
- DOD HILLY BANK THE HAR	-1079-10 - 0.2.4. N	NAME .	annual Real	with Aut	1001	Aug.
and the second s					0	
CO ROAT SERVICE AND ADDRESS AN						
2000-00-00 (10-00-0)				0		
8255				~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
and a second sec						
ALCON ALCON		17 mil		N'		
all and the second second second		EXCharacterial	al ministry (			
AdaCierter ing set		BUDININ				
ARTIGUESING NO. NO.		Resident autom	100,040			
##25210-100000 ( 162100000)		noonist	(Appendix)			
AREESCHWARDER AND BER						
401818 80-11			12.			
			X/~			
Activities of the Activities o			2			
and a second second			C'			
Internet and internetion		<u></u>	2.			
100 B (000 00 0 0 0 0 0 0 0 0 0 0 0 0 0 0						
REAL AND AN AND AN						
MERICAN AN ANNA		an C				
All and an and an and an and an and an and an an and an		AT ADDRESS	ng udal.			
WERENING OF THE OWNER		AT ADDRESS	main.			
AZENCES AL COLOR AZENCES AL COLOR AZENCESCO AL COLO		AT EDWartson	an tar			
Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attendence Attend	2	AT MILLION MILLION HILLION HILLION HILLION	aginan agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agina agin a a a a a a a a a a a a a a a a a a a			
ABCONTANT A CONTANT ABCONTANT A CONTANT ABCONTANT A CONTANT ABCONTANT A CONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANT ABCONTANTANTANTANTANTANTANTANTANTANTANTANTAN	150	M ADDRESS OF A	ang randri ang tant Restant			
ABUSE AND A A A A A A A A A A A A A A A A A A	22	AT ADDRESS OF A	ng vord.			
VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSIO	37	en Ensemmen Inscientes Bissettementer	ng total.			
4220-000 40 CONSTRAINT 4220-000 40 CONST 4220-000 40 CONST 4220-000 40 CONST 4220-0000 40 CONST 4220-00000 40 CONST 4220-00000 40 CONST 4200-0000 40 CONST 420	13/120		ag voral ag sai ag sai ag sai			
VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSIO	27 180 181	ATT	adi nanj			
VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSIO	30,91	ATT STATES	ad istal			
423-000 AL LENGUE	22 CON 16	AT A CONTRACT OF	an ingan an ingan an ingan			
4230-000 AL COLOR 4230-000 AL COLOR 4230-000 AL COLOR 4230-000 AL COLOR 4230-000 AL COLOR 4230-000 AL COLOR 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 4230-000 42300-000 4230-000 4230-000 4230-000 4230-000 4	2000 - 20 - 20 - 20 - 20 - 20 - 20 - 20	AT A CONTRACT OF	an is sur-			
BERGENER      BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER     BERGENER	10200 2010 2010 2010 2010 2010 2010 201	er Energies	ang vorwi- kat 22 Ng than Rati Ann			
922-000 00 00000000000000000000000000000	2000 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 -	ett Linnanum Instrumenter Begetenseneret	ag vora ag an ag an ag an ag an ag			
	10° 00131 (50		an visus an ten an ten an ten			
9230-000         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.0         0.	2020 100 100 100 100 100 100 100 100 100		ag usa Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran Maran			
1000000000000000000000000000000000000		ATT	ng to rat.			

## 9、异常记录详情沙箱报告

当异常记录满足 sandboxReportId exist 条件时,查询列表中,选择一条异常记录,点击展开详情, 支持查 看沙箱报告、下载恶意文件和下载沙箱报告操作,如下图所示。



A204 13004	NUFAT	80.00	63601423	SCOREMENTE	10104	4290394	Reive	625.00
10.11.41.100 702.10	LT174 (#18)	<b>田田田和1114年</b>	1000			1021-01.11110-03.00		20.000
10 11 A1 199 70 10 10	(21.179 (@YR)	1682.00M	-			3021-01-13-00-00-en		103814
	1540  150-155.21 175(後来の東子中では からにに知ら来来る。 中国の第三 49	odrika za dostatnobani, Bilo Roskevijiana	tan ar ar ar a	ENELIERNAN, B	TANKA BA	文持宣書沙	1757 (***********************************	a Batta 文件
52.11.41.100	#1210	1401	100083	0.000		165	488.21.170 -	
SER DURBARI REGE DE DEDAG	nongio - en jamporturo	-44	1000 1000				Parks: 314-000 B 100 Regne: Allina.commit Regne: Regne: Regne Regne: 100, 101, 21, 17, 0	(81,211,171) (81,891) (800)
enit.								
基本信息						0		
Rday 011141.159	SRA: 192.168.21.176	2600-1724/117/10096	Alexa Press	<ul> <li>Administration</li> </ul>	458.	11111 - 11111- 11111	102907456	
398 <b>1</b> 85		同时支持领证负面查看沙路报告				V	ALM P	
(5	9) ×###	牢级:中危			the second			

### 10、更多查询

点击<更多>,可根据威胁等级、攻击链快速查询,

切换数据来源(原始日志/异常记录)。如下图所示:

AILPHAIII = #1 = # #	- ADARCY - & REDRY - IN NEEDE - A MYSRIP - CA ADARCY	Q 🖛 -
an . N (states - parts		0.0.11
1044 6 7 5. 555 02 59 50 5541 2554 \$1422		
E at 2 cm		MACHINE BAR ART AND - BP
威胁情报		
1 功能简介		

## 6.2 威胁情报

## 6.2.1 功能简介

威胁情报通过标签化录入方式, 支持登记恶意 IOC、黑客组织、监管机构。情报信息将作为威胁、whois 知 识库· 识别互联网中的网络实体· 情报知识将赋能到 Sherlock 概况和告警详情部分。情报库的不断更新与 丰富,为用户提供更准确的告警信息,以便用户及时做出应对措施。

# 6.2.2 情报查询

选择 "安全分析>威胁情报>情报查询"页面, 输入 IP、域名、文件 HASH(MD5/SHA1/SHA256)、邮箱进 行情报查询, 展示查相关情报类型、情报源、情报标签、地理位置、置信度、运营商及组织名称信息。如



### 下图所示。

		AILPHA威胁情	报
	181.160.96		9
.18	1.169.98 () ·····		
10:001	200 857A	<b>期技术</b> 燕南市法	S S
ind	na Na	唱织名称 验元	EMALPHASHE
第三方有	18 official and its	Whon Vinsilinu	
		AILPHA威胁情报	
	Ryel-canne care		C) a
fget-	career.com		
10	and an		
	AND NO.		
82	NUM COMMAN MILLION	New Westhall	E BALPALEH
			2.5
Iget-	career.com		
	and rents cents crots		
	自然時 知无	HINAR INA	

第三方链接。情报查询结果支持跳转第三方链接: 安恒数据大脑、微步在线、 Whios、 VirusTotal, 补充相 关情报信息。如下图所示。

🖻 安全戰級大脑						
		皇素结果			RE	
	- 181.1 - 1	69.98	T drasgenera	8 8 0	. «N#	
	AGR/MEHL			10.020.00	and independent of	
	藏粉情服集團		x = 415 (201			
	and		Reality in the second		Nex3	



# 6.2.3 情报源

选择 "安全分析> 威胁情报> 情报源"页面, 查看情报源, 包括安恒安全数据大脑、安恒 AiLPHA 分析团队、行业情报三种情报源。安恒安全数据大脑、安恒 AiLPHA 分析团队情报源为内置情报源, 定期会更新情报源; 行业情报为用户自定义维护情报源, 用户可在行业情报中添加相关情报信息。如下图所示。

0.0100 - 30000 - <b>30</b>	4.8			2	~	
۲	**************************************	$\bigcirc$	(1) 日本市場の第一次 (1) 日本市場の第一次 (1) 日本市場の第二次 (1) 日本市場の第二次(1) 日本市場の第二次(1) 日本市場の第二次(1) 日本市場の (1) 日本市場の(1) 日本市場の(1) 日本市場の(1) 日本市場の(1) 日本市場の(1) 日本市場の(1) 日本市場の(1) 日本市場の(1) 日本市場の(1) 日本市場(1) 日本市(1) 1) 日本市(1) 1) 日本市(1) 1) 1) 1) 1) 1) 1) 1)		※127時日2日: 1 小口前日10月1日日: 1 日日日の10月1日日: 1 日日の10月1日日: 1 日日の11月1日日: 1 日日、1 日日、1 日日、1 日日、1 日日、1 日日、1 日日、1 日日	
	0100400110		DEFALTING THE DE	P.	(Eurod	

1、 情报源管理

选择一个情报源 · 点击 按钮 · 进入情报源管理界面 ; 输入需要修改的情报信息 · 点击修改或者删除。 安恒安全数据大脑、安恒 AiLPHA 分析团队管理界面可以对情报信息修改、删除 ; 行业情报管理界面可以 对情报信息进行添加、修改、删除。如下图所示。

TRADITION -		
st-career.com D		122
WENE COLER CACHER CACHER		1200
HENDER MER.	Buik CER	
REAR PRESE		OTO SHEAR
HINE / MER / GAME   MR	<u>~</u> ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
	RANE AREA MARINE MIREA MARINE	E Servite
e O		
唐报源设置		
AJK////VE		

◆ 安恒安全数据大脑支持在线更新、离线更新, 离线更新需要上传相关离线更新包, 更新成功后会有相

应更新时间及更新状态提示,如下图所示。



core and der constants an		
A18.00 M		
RATER (		
MR-MIT-PERFERENCE MITERFMITER, METERFORMER, METERFORMER,		
(ARRA)		
ALTH		
28% principal and a second		
MEATING_INUNGANDERED. BERTREMALMENTON-LEPONEDPONEDPONED		
Man Metric Al 2015 (1) 14 (14 (14 Metric All 14		
Robert, Anitheostering,		
14465		
nexten		
用某些某些目的主要有有意义的不过是不同的意思的意义。如果正是主体的自己的意思,如此		
Million .		
	-0	

◆ 安恒 AiLPHA 分析团队仅支持离线更新 · 离线更新需要上传相关离线更新包 · 更新成功后会有相应更 新时间及更新状态提示 · 如下图所示 ·

AND AND NOT TOURS IN .	<u></u>
Aug 21	0,
Res. and down	
analys, introduced strangers, which are consists + over the unit of a	× ×
REFERENCE HIN A V SHOW	
and contraction of	
	iv si
ADDITION AND A DESCRIPTION OF A DESCRIPR	
(Viewer)	
	O`

◆ 行业情报支持离线更新 · 同时支持情报导出 · 如下图所示。

安全分析 / 成制	的情报。「情报源」「行业情报」「设置」
高线更新 更新包	
情报库3	29新包上停后将在后台更新情报信息。情报库更新后相关的情报模型中会同步最新的情报库信息。 9更新包 或时间: 五
生成的	
情報库3	》》 更新后相关的機报模型每天凌晨会同步最新的情报信息。如需立即生效通点击"模型同步"按钮。 1915

# **6.3 UEBA**

# 6.3.1 功能简介

UEBA 提供画像及基于各种分析方法的异常检测 · 通常是基本分析方法来评估用户和其他实体(主机 · 应用 程序 · 网络 · 数据库等) · 来发现与用户或实体标准画像或行为相异常的活动所相关的潜在事件 · 这些活动

包括内部或第三方人员对系统的异常访问(用户异常),或者外部攻击者绕过防御性安全控制的入侵(异常用户)。通过对用户日常行为的聚类以及 AiLPHA 大数据智能安全分析平台安全域信息,将不同类别的使用者(User)区分出来。当这些用户实体有非职责内操作时,平台会将该用户标记较高异常评分(Anomaly Score)。

## 6.3.2 UEBA 用户画像

### 1、 UEBA 用户画像

选择"安全分析>UEBA>UEBA 用户画像"菜单, 打开 UEBA 用户画像界面。如下图所示。

	4 cade-	0 Rabite	2 Length	0 Exera	
SUB-THP		1	Rame		=
weix mang Bertrebern	2013-09-11 19:05:35	3 190	年度第一日 王臣 曹凯代人	2	0
					0

## UEBA 用户画像页面布局见下表。

序号	名称	说明
1	查询	支持用户信息、账号、邮箱模糊查询。
2	风险用户	显示风险评分不为 0 的用户,根据风险评分倒序排列。
3	重点关注用户	显示重点关注用户。
4	用户管理	点击跳转至 UEBA 用户管理界面。

2、 UBEA 用户画像详情



## 行为时间轴:记录该用户 vpn 账户登录期间行为, 包括访问、遭受攻击情况等,如下图所示。

REDWIT DERA / GERARMEN DEBARONNES

	novace) 🔽 🕴	446 - 19	arlin:	2 2 3 190
utilm cFix	6 8862			00
	. 12m	A	10 10 5	) )
2019-09-11 19-25-20	🕞 as as as as (590 172 16 (01 132	N R. HERT Jodes		
2010-00-11 16:25:06	<ul> <li></li></ul>		and	2 2 5
2019-00-11 10 13:22	0 46.66.06.568(BadowssScatter)	72 16 101 138057 <b>6</b> 5 <b>6 1</b> 6 101 138057 <b>6</b> 5 <b>6</b> 101 138057 <b>6</b> 5	TEP BARBINGS	
2019-06-11 18:13:21	0 06.06.06.0606/ExponeseScar.721	72.16.101.138/行了最力能解成22. 103		
2019-06-1119-13:35	0 44.96.48.554(/ExtorestScar2)1	72.16.101.15869.7 <b>6</b> .19244.022.	夏朝十日	
2018-00-11 18 11 18	66.66.66.654(#biteressScan211	72.16.101.1385/57集力研解的法。	単位 単純五 	

参数说明如下所示:

序号	名称	说明
1	编辑	点击跳转至该用户编辑页面。
2	时间控件	支持最近 24 小时、最近 7 天、最近 30 天、本日、本周、本月时间查询。
3	风险评分	根据用户登录期间攻击及遭受攻击情况来进行评分,分数越高风险越大。
4	行为时间轴	展示用户 VPN 登录期间行为,点击时间可跳转至安全分析页面。
5	用户风险评分	展示用户最近7天风险评分。
6	用户活跃时间段	展示最近7天用户在线时间段。
	This file is restilled	



## 访问关系

SHORT DOAL DOATHING DOBATION



•	// ЦО //
٠	互联网

	٠	内网
图形模式	٠	图标下方显示资产名称·并且不同的风险等级显
		示不同的颜色:
		已失陷:红色
		高风险:橙色
		低风险:黄色

健康: 绿色

其他: 蓝色

用户 客户端 分配身份 互联网 内网 图标下方显示资产名称,并且不同的风险等级显

异常访问

客户端

内网

互联网

192.168.22.13

vide share

分配身份



项目	说明	详细
	鼠标点击图标时浮出显示资产详细信息· 内容包含: ◆ 有对应资产	
图标详情	资产名称、风险评级、安全告警 Top3(告警名称:事件数量)、最近异常发生时间、资产 IP、 安全域(属于内部安全域时显示安全域名称 · 不 属于内部安全域但属于内网 IP 时显示(内网) · 不 属于内部安全域和内网 IP 时显示互联网)、资产 类型、组织架构、责任人。 无对应资产 内网	172.16.101.13 加助計算: 但如此 法全告责TOP1: 通监服力或新成功 121.2 能力能常发生时间: 2019-09-11 185358 现在程: 172.16.101.13 安全域: 同知时 现在关键: 局加时 同时法法
	<ul> <li>九內应负/ _內兩</li> <li>显示 IP、安全域(所属安全域或者是(内网))。</li> <li>无对应资产_互联网</li> <li>显示 IP、安全域:未分配、地理位置。</li> </ul>	172.16.101.13
	<ul> <li>◆ 两个图标之间的访问方向,两者相互访问时显示</li> <li>两条线。</li> </ul>	S:U
	◆ 访问类型(正常访问: XXX 异常访问 XXX)。 支持钻取。	172.16.101.13
	◆ 累计流量: 原始日志中 bytesIn+bytesOut。	
<u></u>	<ul> <li>◆ 最近访问时间:原始日志中满足条件的最近一日</li> <li>志的时间。</li> </ul>	87113238: 1.34M8 8271069849: 2019-09-11 19:1507 549256349970093- 9213948(820-77)
	<ul> <li>◆ 异常访问类型 Top3 · 没有异常访问时不显示该 项。</li> </ul>	ENGERETOPS: http://doi
	◆ 正常访问类型 Top3 (appProtocolTop3)·没有正常访问时不显示该项。	

登录地区: 展示该用户登录地区分布热力图, 如下图所示。



W2597 LESA / GEBARPING UEBARPINGTO

parteration and some			-8278, ···
💿 *** mini *		alaan urse: vicey zhong	190 Jacobs
TARAN USERS BONS			
N發梁地区热力图		学版	9 10 M
			8
	States.	N	
		S	
.3 UEBA 用户管	19世 - 11日 -	<u>~</u>	

### 1、 UEBA 用户新增

点击<添加用户>,打开 UEBA 用户添加页面,输入相关信息点击<保存>,如下图所示。



## 2、 UEBA 用户编辑

点击<编辑>,打开 UEBA 用户编辑页面,修改相关信息,点击<保存>,如下图所示。



A LPHA	THE PART OF SHARE	a commente a seriero	a and a state - a summ-	
	CONTRACTOR CONTRACTOR			
8100				
1.00	*			
	a .	*		
1044	**	72	a jestime -	
1988				
8195	**		**	
- 18	(001)		200 20 -	
-	-	+3		0
8199				
**	1000 mpane			
	1000			2
	89			$O_{\mathcal{D}_{\mathbf{x}}}$

3、 UEBA 用户删除

点击操作列<**删除**>,即可删除该用户。

## 4、 UEBA 用户批量导入

点击<**批量导入**>·弹出导入文件弹框·下载模板填写导入即可·如下图所示。

		S		
文件上传;	未选择任何文件	S	远择文件	<u>模版下载</u>
	0	R		
	send the second s	g细、油在保存的	时选择 "CSV U"	TF-8(逗号分
CSV文件采	用UTF-8编码,如果使用Excell	Carden Harrennin .		1.0.0

## 5、 UEBA 用户画像

点击操作列的<UEBA>,跳转至该用户 UEBA 用户画像界面。

### 6、 查询

UEBA 用户管理支持状态查询及全局搜索。

# 6.4 可视化中心

# 6.4.1 功能简介

平台数据经过分析聚合, 各类图表将数据可视化, 为用户更直观的展示数据分布、数据排行情况。

◆ 支持用户自定义添加报表。



- ◆ 支持用户导出报表。
- ◆ 支持用户引用图表自定义仪表盘。
- ◆ 支持用户创建"数据可视化大屏", 满足用户报表、仪表盘、 Aiview 大屏定制需求。

## 6.4.2 图表管理

选择 "安全分析>可视化中心>图表管理" 菜单, 查看图表管理界面, 默认存在内置的报表。

如下图所示。

estan devoiro 📾	8.1715						
ER NEIDIE	2	88 05/59	1	je.		23	88
8:::::::::::::::::::::::::::::::::::::				jeji -			8-12 10-14
<b>SARD</b> :	报表关键 :	1248-0455	10-21	Citaterio :	<b>銀行</b>	95	出现有
10 100	二律分布国-讲讨图	8.005 Total	121	2000-12-30 10 27 23		PDF	WORD
top ag€top	一使日本思考表	编天 <u>世</u> 像709	RARHERINEL X	2020-12-18 10:28-24	a + / +	PDF	WORD
Magaeli	-469458.8(W	Nationary	41-2140+12 State+	2020 12-12 18 22 18	8 4 7 8	PDF	WEDRO
C RPARH	一個分布間。在於間	HP Mar	Nº.	2023-12-13 18 21 48	0.0.0	PDF	WORD
HKQ193517	一個台布里住法則	802015/90H	6	2029-12-13 16:21 16	a • > •	PDF	CIRCOW
配置を使う	一些分布透电识别	B/ID+R/DISEL+	S i	2020-12-13 16:20:41		₽DF	WORD
anieter	一進分有國社民間	MARCH	2 S	2020-12-13 19:20:01	B 6 2 8	PDF	09099

#### 1、 报表查询

输入标签或者名称,可查询到相关报表;点击<重置>,清空所有查询条件。如下图所示。

65	11247-5-2	2		0					<b>2</b> 14	88
4) ±1	EN - BIA									***
	8888	SER. MILLER	1948-045	62	000004 -		8	ini i	101	199
	tent	二地日和西洋和北西	Just test	123	2020-12-30 10:27-23		٠	1	PDF	WORD
	₩天TOP		<b>BRADIO</b>	安全都许高的统计	2620-12-18 10:48:34			1	PDF	WORD
	Repair C	()-minman	Nilestor.	安全部住民和政计	2020-12-13 10.22 16	n		1	PDF	WORD
	minit . S	-#19484100	87°%01		2620-12-13 10:21.48	10		1	PDF	WORD
	REELES. HIME REELES	一進行有對一種社園	802015345VT		2020-12-13 16 21 16		٠	1	PDF	WORD
	<b>自然与期</b> 间		影影标言共计		2020-12-13 10:20 41	n		1	PDF	WORD
	MRRAIT.	-4565-008	Altherit		2620-12-13 16 20.01			1	PDF	WORD

### 2、 报表类型

支持生成一维时序折线图、一维时序面积、一维时序柱状图、一维分布饼状图、一维分布环状图、一维分布柱状图、一维分布横向柱状图、一维分布列表、一维分布文字云、二维时序折线图、二维时序面积、二



维时序柱状图、二维分布饼状图、二维分布环状图、二维分布柱状图、二维分布横向柱状图、二维分布列 表和大字报 18 种报表。生成一维时序图、大字报需要引用没有 groupby 的统计指标;一维分布图、二维时 序图需要引用有 1 个 groupby 的统计指标;二维分布图需要引用 2 个 groupby 的统计指标。部分报表预览 效果,如下图所示。



3、 报表新增

点击 新達 按钮 · 进入报表新增界面 · 输入相关信息 · 选择报表类型 · 统计指标 · 点击<保存 > · 报表新增成功 ·



如下图所示。

基本信息			
· 8955	赤银色型(A)的		
+ 陳紹介紹	不可希望地整理的现实化		
服表标签			
报费场查	内阳安全成物	-	一可自定义添加标签,报表可绑定多个标签
國表配置			2
• 经费关证	1403854B	- +	选择报表类型,不同报表类型对应不同类型指标
+ RETIRE	內阿吉爾奧登訪是(reservedTypeCourt)	• #B331i	
统计对象	事件名称(nama)		2
推序	inter .	- 90	可选择指标groupby的字具
	SIG GIF Kin	5 10 20	→ 按照降序/升序TOPN生成打 表
		30	Sr St

## 4、 报表其他操作

报表列表支持编辑、预览、编辑和删除操作,选择某一个报表,点击操作栏相关按钮,可进行相关操作。 如下图所示。

RAID -		sind S	10	MARK .		10161
**********	CHINEMAN	(server an in the server and the server and	not an a set	0000000000	· · · · · · · · · · · · · · · · · · ·	
		Belingeningen /	-vhasen	(0.00-0.01-0.01-0.01-0.01-0.01-0.01-0.01		10.00
-		mennenderin	1000448	(10/10/17) 22 10:00	100000	10.000
whice design	mennet	anter anter anter anter	-Team	10100-0112120-00	#1404040	10 100
10050100.00	- manange	THE REAL PROPERTY AND INCOME.	-record	president and the set		er ein
****	and preside	Torrada companyor and	-datast	10/10/07 11:10 10:10	a a 2 a	10.000
verser .	(mall the	THE BORD DOCTOR	All and	provide an address of	(#140274)	101 1000
******	Contraction	750100-MERGERED.001				100.000
+005/4	Calve ere :	T00002118	A16340	00000410100100	101012010	NOT: 16240

#### 5、 报表导出

报表支持单个/多个导出, 导出格式为 PDF、 WORD · 点击<报表导出> · 即可获得相应格式报表。



如下图所示。

R1000 - PP					*reells	1.5
- +1+++tm	4448	04/6	48	denormi i		-
and cross	cantal risk.	extractive and the second	1010.040	and an inclusion		inc.mm
017000/1088	CHEVENNE	or press to construct on the	100000	C INTERCOLOGICAL DE LA COLONIA		-
Dational	(2010)100	Damp (1) (Starting all	-010.040	0000 Arr 10 00100 Ar		-
	Carlot Barriell	+ Burg of Court #	-	100-010-0100	A 417-1	nr ios
designation and the second second	and second	her beingen anderen anderen bei beingen anderen and	ningati	1044-01-01-02-02-02	3	-
10454Bhcr4	CHICKE BARLINE	The sector of the sector of the sector of the sector secto		1000 - 07 100 100 100 100 IN	Que.	
restor	CARGONAR	********	trisian.	10000000000 C	(B)(B)(A(A))	101.000
version.		Travits/s-Methiasescont	1004440			107 100
199511		101040-10	1010485	C INTERNET		110 0000

## 6.4.3 仪表盘管理

选择"**安全分析>可视化中心>仪表盘管理**"页面,用户可按实际情况定制仪表盘、管理仪表盘,将重点 关注的数据可视化展示在仪表盘中。

## 1、 新增仪表盘

点击 *** ·进入仪表盘新建页面。

- ◆ 填写仪表盘名称、仪表盘描述。
- ◆ 选择仪表盘布局,布局可选择一行四个/三个/两个/一个报表, 也可以选择不同宽度。
- ◆ 选择报表· 报表即 "**安全分析> 可视化中心> 图表管理**"中的报表· 点击<**添加到选中布局**>。
- ◆ 最后点击<**保存**>,仪表盘新增成功。如下图所示。

NAME .			
** ## 自定义	请辞布局、选中有闸机会高罢		
##############		* n#+280	
Extensional	C C DETHERE	× 0071000000000	
-			
nas suspeed . G	國權者,点古派加封進中布萬		
ana ''	<ul> <li>releasestell</li> </ul>		
8868 C		Acres .	
Ballion Nellie		-m-st +45	
S.Q.			
E Casegera		_m=+0.6 ( A.D.	
a an		2003/08.01428	
Continuoune		- area 118	
V and the second second			
ARE DESCRIPTION OF THE OWNER OF T		-8158.08	

#### 2、 仪表盘其他操作

仪表盘支持禁用/启用操作;支持预览、编辑、删除操作; 支持排序操作。



如下图所示。

41118	COLUMN NAME				-	
		In an and the strategies		TRACATOR	+2	-
	stan -	Statistic -	-	1.00		-
1.04	WHERE	divising advances through in a pressure of	3898-8135-93363*	•	-0	P(4)

3、 仪表盘预览

在 "安全分析>可视化中心>仪表盘管理"页面·选中某个仪表盘·点击<预览>·预览页面支持放大报表、编辑报表·如下图所示。



4、 态势感知仪表盘预览入口

**态势感知**页面支持仪表盘预览,如下图所示。

Н	Afina
	THE .
	Constant like op: Reserver. Notes Constant like op: Reserver.
Ľ	

# 6.4.4 AiView 设计器

选择 "**安全分析>可视化中心>Aiview 设计器**"菜单·新打开一个 Aiview 大屏管理页面·显示已发布/未 发布大屏数量以及大屏的名称和分辨率·并支持用户登录·用户管理· 授权管理·大屏管理·大屏编辑·



大屏发布, 创建演示预案等操作。如下图所示。

Affen Constant Classes & states	ANEN	• • D ators
100/	* • C / terrate	
	AFiew	
i fankakred ber	anacimite	

- 1、 创建 AiView 大屏
- ◆ 点击 从覆蔽避 新增 Aiview 大屏 · 在现有的模板中进行选择并在其基础上进行编辑 · 可点击<**预览**>随 时查看大屏最终结果 · 如下图所示 •

ATTeve							mit.W		25				• • •	admin *
		<b>10</b>	10			100	10.11	- 10	a e	10 10				
all rende														
	1.1						THE ADDRESS OF			and the second se				
	100						TRAKE	n Avian		1000				
	100												P2080	
and a second sec		* Comments		e Tardinda	199					APORTAN)	240.0	1884/5		
inner.													BARDON BARDING	
Contract of Contra								- 201					Million State	
TRANS.														
Comp.						1.1								
TRANS.		* newspaper	in - )	County	Southern .				10.00		+ Lower	and a lot of the lot o		
Base .	•••	Contraction of the local division of the loc		1.1.1.1		1				central and		the second second		
INSIGN T														
-		1000												
CORRECT OF								1						
COLUMN 1														
COLUMN .		A CONTRACTOR			· Services		+ waters		<ul> <li>Here</li> </ul>	and the second se	Concerned in the second	there is a second s		
10000		and the second second	-	100						a na anta				
-		Re mailent	Care Colored	Const.	1					- F - F - I		Sec. 1		
and the second second		exclassion and a	68 141 14		12		単					1990		
******		nerostics.	CO STATUTA		-	-		Test and test			A beamers			
******		403108	THE REAL PROPERTY.		PROPERTY	84111	PROM	<b>Beauting</b>		THE R. LEW.		194		
W21046	***	R.T.L	110 4000 40	- 44	H				**		1 Dates in			
-		8.2%	I THE OWNER WAT								and the second	PROFILE OF TAXABLE		
-		10	And I have been seen as	10.00	10				<b>A</b> .		100	COP CONTRACTOR		
Barrow .		8176	THE PARTY NAME		and see the	the set lies					1	- 10 H		
					_						CALL OF			
8000														


◆ 点击 新学 Aiview 大屏 · 在空白的编辑页面上进行编辑 · 可点击<**预览**>随时查看大屏最终结 果 · 如下图所示 •



#### 2、 AiView 大屏其他操作

用户登录大屏管理页面后· 可发布/取消发布某大屏· 查看已发大屏的链接地址· 也可进行编辑、预览、复制、删除操作· 如下图所示。



3、 AiView 大屏预览

在大屏管理界面选中一个 Aiview 大屏·点击<预览>·即可预览该大屏·如下图所示。

688 - 0 1011 0 1076	D- 1057		城市数据好营家		241000	P 1790.31	basen	
		00000	A TOTAL OF A			1167773 5479906 55155 54743 54743		a right of a life
A all a second	BURATO	8.,	a new new	All Distances				21111



#### 4、 态势感知 AiView 大屏预览入口

态势感知页面也支持 Aiview 大屏预览,如下图所示。

A/Inv	20
	inder and the
Affactor	

# 6.5 报告管理

# 6.5.1 功能简介

报告管理支持用户引用报表(选择"**安全分析>可视化中心>图表管理**"菜单中的报表)定制报告·同时 为用户提供深度威胁分析报告及报告订阅服务。

# 6.5.2 报告中心

选择"**安全分析>报告中心>报告管理**"页面,页面列表展示所有报告,包含内置的深度威胁报告。用户 可按照实际情况定制报告。

- 1、 自定义报告
- ♦ 新增



点击<新增>,进入报告新增界面。填写基本信息、标签、选择报表、勾选报告输出项,点击<保存>, 报告新增成功。如下图所示。

10-4-14-8				
• 提出氧物	空秋日本		▲—— 擅宝相关其大	信白
• 程告描述	1968 B		A THE R	
经承销资	第18時提發	支持自定义标签	,可绑定多个标签。	
服告配置			P	
• 3483	#58 <b>8</b>	7 BISR		3
	ALMALIN, MAR, WARPING PORM	Q. BAR	Canal galageration	Q.
	3.2.1(一線85年面形型)		空東北引水(一連日市井沢町)	
	前型类型未增地社会系(二串会有標料性(計算))		<b>医动脉的</b> 等 (一個时間所说里)	
	查查查查查查查查查查查查查查查查查查查查查查查查查查查查查查查查查查查查		(国际中部社会中)二组合有社区国	
	[] 国连首号地址分布路势(二進时序所或置)	×	选择报表	
	自使表音频的 (二億可序形成置)	Š.	2.	
	18% 目标地址分布路价 (二條町平所成置)		6	
	#156.0419-0222.418236 (	4	,0	
	<ul> <li>□ ==#######</li> <li>□ ==########</li> <li>GEF ● TRUE</li> </ul>	援表描述信息	是否仅展示有数据报表	
◆ 显示	描述信息: 勾选该项·则导出	出报告中 · 会展	 示报表的描述信息。	
<ul> <li>● 显示</li> </ul>	有数据报表: 勾选该项, 则导	出报告中 · 仅	会展示有数据的报表	• 暂无数据的推
_				
不。				

				and a local division of the local division o
man ()	anas -	110	AND A CONTRACT OF	-
Desilitore 1	CONTRACTORY AND	17403 12346a	NALE OF \$1, DO NOTE	2121
S marrie	A PA ST ATMENDIAL CONTRACTOR	and the second se	mencan	4.14
XC.				818 - 1 - wad- 82 1

◆ 导出



报告导出支持 PDF、WORD、HTML 等格式导出,点击<导出报告>即可。如下图所示。

				HIMOGRAM	#
	MARK -	48	- MARKAN C -	** 1	
B481-F101	HEADTING APPROXIMATE APPREND		2017-12-12 12 00:00	101101	
Person	Alcohards Anevateurs torbinancia 8 No. 27 Eleasteringuisade		2010/07/07 2010	1.1	-
				18 - 1 - 987-	<b>NB</b> 1

#### 2、 深度威胁分析报告

报告列表内置深度威胁分析报告, 报告从总体威胁态势感知、资产分析、外部攻击者行为分析和分析取证 四个方面进行分析, 并且结合分析为用户提供分析说明和处置建议。深度威胁报告不支持编辑与删除, 仅 支持 WORD 格式导出报告。深度威胁报告如下图所示。



# 6.5.3 报告订阅

选择 "**安全分析>报告中心>报告订阅**"页面,页面列表展示所有报告订阅服务,用户可对报告设置报告 订阅,报告会按照设置周期定时发送至用户邮箱。

1、 订阅条目查询



支持报告名称/邮箱关键字、发送周期、启用状态查询订阅条目,如下图所示。

安全分析 》报告中心 / 报告订阅

大韓子: 前加入加加名称, 即相	ч			
茨逐周期:不禄 日报 周报 月报				
逝日居用:小服 是 含				
启用 禁用 删除		S.		
报告名称 =	发送周期 👙	生成时间。	时间范围。	收件人
		in the second se	8	智无数据

#### 2、 订阅新增

点击<新增>,进入报告订阅新增界面。

- ◆ 选择发送周期, 发送周期可选每天/每月/每年。
- ◆ 选择生成时间, 某天某个整点, 报告统计时间为上一天/上一周/上一个月。
- ◆ 选择是否开启自动发送, 即启用/禁用报告订阅。
- ◆ 选择需要订阅发送的报告。
- 选择发送格式。
- ◆ 填写收件人邮箱。

提交完成后点击<保存>即可。如下图所示。

发送明期:	●天 → 司法採号夫/総局(巻月) 即生成旧線/周線/月線
生成时间:	電天 v 1g v 生成报告、报告统计时间
自动发送:	▲ 用自即自用把書订稿服务
• 服装西缀:	
发进模式:	
• 信件人創稿:	Alphasdminigdbapa.com.on
	注: 2008年1878、後年1958 (2008年2018年20日時、 希望 (正成支援) - (001100580500) 配数の1100580



#### 3、 订阅其他操作

订阅条目列表支持启用/禁用订阅条目;支持查看报告订阅发送历史记录;支持订阅条目编辑、删除。 如下图所示。

P88	<u>6</u>				查看/	编辑/删除报告订阅	初历	史记录
100 10 14 96 AS		5	0					
Ant	$\mathcal{O}_{\mathcal{S}}$							
					启用/禁用	订阅条目		
2000	.05	1000	5.000		604.488 ·		82.	
Stationsk.		87	10×10	4-7	Approximation and a set of	1010-00-01 TO 80.01	•	5 503
ARE ARE	S.	47	140.14	1-8	sengini sen	1010-00-12 15 26 10	0	
	2					a.a	In A.T.	400.00

# 6.6 SOAR

# 6.6.1 功能简介

SOAR 通过剧本编排将平台上现有的模型、指标和设备联动组件整合到一起, 使现有模型高度复用, 并为用户提供了丰富的告警事件响应能力。任务看板中的任务依据剧本自动化、半自动化手动执行, 既节省了时间, 人力和成本, 也可避免人在处理大量数据的过程中带来的误差或失误。



# 6.6.2 任务看板

	4,309		Gérana.			11077-1-1-0	20	
	On Ge De	102- Br 48-	(		rand 3.4 Area 7 These 8			/
anuw 1						Ś.		
9340 ·-		- Rec				in Com	steres r	
-	14							
	0.040	amaitmi	10040	8110	HISHERINI (	-	Transis :	
	1000		040	-		panalit water	10000M	
10	ANDER CONTRACTOR		and the state of the	100070078784, \$1200	a maa mag kandar m	. 6.		

选择 "**安全分析>SOAR>任务看板**"页面,查看任务看板页面。任务看板页面主要包括**任务概览**和任务详 情两部分内容,如下图所示。

# 6.6.2.1 任务概览

**任务概览**显示在当前时间窗口下,任务的概览情况,包括任务总数、任务平均处理时间、节约时间、任务 状态占比(进行中、已完成、已取消的任务比例)、任务趋势(总任务数的时间趋势)和时间控件(默认最 近 7 天)。如下图所示:



6.6.2.2 任务详情

**任务详情**区域默认支持剧本名称、剧本 ID、任务进度、开始时间等查询;点击 · 可支持任务名称查询; 点击<**重置**> · 可清空所有查询条件。



任务列表默认根据任务开始时间倒序排序,默认展开第一条,每 10 秒左右刷新一次,如下图所示。

576								
ER	4 840.00				Plant 18 1021-16 11 (01/01/18	Later in reaction		-
1.84								
10.00	extendente -	118.018	BAUE .	entrani -	100000000	mani -	80	
C 4 C Hiess	++1244		10	3000 (F (1.0)-0				
TORN BARRY						00		
4						20		
		-				, 9°		
	-							
					ġ.;			
Reas		p.Zeran			i. loi	1		
Read		atera	2	2014/17120-0				

#### 任务详情功能详情

- ◆ 任务甘特图:已完成的节点为蓝色, 未进行的节点为灰色, 有输出的节点可查看输出结果。
- ◆ 模型: 最终模型的甘特图时间为触发告警的时间; 非最终模型的甘特图时间根据最终模型追溯模型触发异常记录的时间。
- ◆ 防火墙:

防火墙甘特图的时间为 WAF 阻断核查的时间,若告警信息里有来源 IP 且联动设备连接成功,点击< 查看>跳转到"资产管理>处置联动>联动策略"页面,携带条件为资产 IP 和阻断 IP。反之,则不跳转。

- ◆ 通报: 通报甘特图的时间为短信、邮件、工单第一个触发的事件, 点击<**查看**>,弹出框显示通报记录。
- ◆ 预警:预警甘特图的时间为预警生成的时间 · 点击<查看> · 跳转到 "安全运营>通报预警>预警" 页面 · 携带的查询条件为该条预警的预警编号。
- ◆ EDR 联动: EDR 联动甘特图的时间为 EDR 联动核查的时间。如果有目的 IP 且是 EDR 防护资产 · 点击<查看>跳转到 "威胁感知>Sherlock>脆弱性" · 携带的查询条件为目的 IP。反之 · 则不跳转。
- ◆ 人工查验: 人工查验甘特图的时间为人工查验处理时间。进行时右边为<操作>图标, 点击后弹出人工 查验框,展示告警内容, 点击<查看详情>,跳转到"安全分析>检索中心>安全告警"页面,携带的 条件为 "eventId", 时间范围为告警 startTime 的本日时间(00:00:00-23:59:00)。

点击<**处理**>可对告警进行处理·处理后右边变成<查看>图标· 且告警的处置状态变成"处理完成"。 操作栏:

取消操作

可单个取消任务·也可批量取消。任务取消后·状态更新为"已取消"·任务结束时间为取消时间。在人工查验前取消·人工查验的<操作>按钮不显示·未执行的节点不显示<查看>按钮。在人工查验后取消·已完成的节点不变·未进行的节点不显示<查看>按钮。

删除操作



可单个删除任务 · 也可批量删除 · 选择当前页任务详情全部任务时 · 操作左上角显示<删除查询结果所有>按钮 ·

查看操作

点击<**剧本查看**>·跳转到该任务对应剧本的剧本查看界面。若剧本已删除点击按钮提示"该剧本已删除"。

#### 6.6.3 剧本编排

选择 "安全分析>SOAR>剧本编排" 页面,默认进入剧本编排缩略图模式页面,如下图所示。

1010 8448		Contraction of the second seco	
NE NEARING NE	and the second	· mit sil stage	81 8
		2	140
			in ( <mark>tan</mark> )En is
CLEADERCHEIG TRANSMISSIONERS AND STREET IN DESCRIPTION CONTINUES AND	92/2000 Robinstein (seriesten) seserer 980 Dours-Gets (begründen)	PRESERVICE	WAFAUNA改击的中 Windows States - Augustation PDD - Patrick States
en Etillenne La Indenationale over 18. Boerne	EXEMPLE REAL	<i>1</i> 02	

#### 缩略图模式

- ◆ 页面右侧上方有<**创建剧本**>按钮。
- ◆ 缩略图展示剧本名称和剧本描述;鼠标悬浮在剧本编排的缩略图上,缩略图显示<编辑>、<查看>、<</li>
   安全告警>、<异常记录>、<刪除>和<剧本状态>等按钮,若该剧本有任务进行中,则左下角显示<任务</li>
   中+num(任务中的事件数量)>按钮。
- ◆ 系统出厂内置六个剧本 · 分别为 : SQL 注入攻击成功阻断、安全产品联动、内部横向移动防护、 WAF 绕过残余攻击防护、挖矿主机处置响应、勒索病毒处置响应 · 默认状态为未启用。
- ◆ 点击页面左上角<**列表模式**>按钮,进入剧本编排列表模式,如下图所示。



e+-01	d Marvanana	W& BUILD	a. (*)	PE SUIPE	- #140 MBD			-	* #
-	* 88 MR	858							100
	BERID 4	8428 :	62	Wa	甲件状态		80		
	eecontyLinkape	STRATE			8	20 81	RESIDEN I	****	854
	tawww.saTaw	内部拥有相关的		•	9	11 H	<b>O</b> BHER	使变抑郁	8774
	bypesa_Wat	WARREN HIS STREET		0	91	23	R PRIOR	安全合规	2019
	Miningainus	他们主切社要考虑		0	(18年)	23, AI	1 1122	学生计型	225
	Rascomware	REPART				- 10 A	s water	*****	89
	watyuanta	WAF電信事件E相交信AI NTA完整分析				<b>20</b> m	95.84A	**=#	201
	wahuang	回》-起\$SOAR		•	1584 18313	<b>n</b> 2 ===	1 9922	****	201

#### 列表模式

- ◆ 页面左侧上方**<启用>、<禁用>、<刪除>**三个按钮,页面右侧上方有<**创建剧本**>按钮。
- ◆ 列表显示剧本 ID、剧本名称、标签、状态、事件状态、操作等。事件状态中只有有任务在进行中的剧本才显示<任务中+num(任务中的事件数量)>按钮 · 操作列中有<查看>、<剧本查看>、<编辑>、<安全事件>、<安全告警>、<删除>等按钮。
- ◆ 出厂内置六个剧本 · 分别为 : SQL 注入攻击成功阻断、安全产品联动、内部横向移动防护、 WAF 绕 过残余攻击防护、挖矿主机处置响应、勒索病毒处置响应 · 默认状态为未启用。

### 6.6.3.1 新增剧本

点击<创建剧本>·若存在历史进度·在弹出的对话框中可选择<继续上次>·进入历史创建剧本界面既编辑器页面;也可选择<新创建>·进入创建剧本界面既剧本详情页面。

编辑器页面界面左侧显示数据源、分析组件、处置响应。页面上方两侧显示<编辑详情>、 <返回>按钮, 中



间显示剧本名称和威胁程度(与剧本详情一致),页面下方右侧展示<**下一步**>按钮,如下图所示。

tion sold 804807 sola	
hest /	5
nse#	
d) mene	
OI meta	
19404	
E mean	
an annan	
2 HEAD	N.
g west	$\mathcal{O}$
23 ands	
eñas	
E lake	
3- 100	0,3
Q ##	<u>^</u> 0

进入界面的同时弹出**剧本详情**弹窗·包括基本信息和剧本分类·点击<确定>可保存剧本详情·点击<取消>则不保存·点击<编辑详情>展开具体内容。

start and 2240 and		
- Contraction (Contraction)		18 ( K)
100		
C. Arts		
(5 W/3	vitte seguite	
6 MW	1 X TOBRE 1	
Area .	HALL MANNERS	
(C + M		
27.9788		
(p. 1944)		
25 Marc		
The second secon		
THE CONTRACT OF THE OWNER OWNER OF THE OWNER OWN		
(grant )		
3		
63 HH		
1 m fm		and the second second
Las views		
1 X		

编辑器页面各模块详细信息见下表所示。

区块	说明	详细
200	<ul> <li>◆ 数据源: 安全日志、异常记录、安全 告警。</li> </ul>	
数据源	◆ 将数据源拖拽至编辑页面时,显示图标、描述信息和<编辑>、<删除>按钮。 点击<删除>或键盘上 <backspace>、</backspace>	



区块	说明	详细
	<ul> <li>数据源中数据类型默认: 全部,点击</li> <li>&lt;编辑&gt;可编辑数据类型。</li> <li>安全日志和安全事件能连线到统计指标,情报模型,规则模型。安全告警只能连线到统计指标。分析组件和处置响应不可连线到数据源。</li> </ul>	资油日本3 时期限款提去型 资油日本是从安全设备改集的全部原油日本。 可进一步分析提终出异常记录。 数据关型 全部
分析组件	<ul> <li>分析组件:统计指标、统计模型、关联模型、情报模型、规则模型。</li> <li>将分析组件拖拽至编辑页面时,显示图标、<b>《编辑</b>》和《<b>删除</b>》按钮,需连线后才能对组件进行编辑,点击《<b>删</b>除》或键盘上《Backspace》、《Delete》即可删除组件。</li> <li>最后一个分析组件的告警默认输出,如果没有连接处置响应组件,界面提示"缺少处置响应模块无法保存".无法进行下一步操作。</li> <li>同一个节点不能同时连接分析模型(指标)和响应组件。</li> <li>统计指标:处置响应元素和统计模型自身不可连线,其他都可连线。</li> <li>规则模型:除安全告警、统计指标、处置响应元素不可连线,其他都可连线。</li> <li>情报模型:除安全告警、统计指、AI模型、处置响应元素和情报模型自身不可连线,其他都可连线。</li> <li>全联模型:仅统计模型、规则模型、情报模型和关联模型自身可连线。</li> </ul>	分析组件 手二 统计版型 通一 余時度型 通一 解胶模型 通一 解胶模型 通一 解胶模型 通一 解胶模型



区块	说明	详细
	◆ 处置响应: 防火墙、 EDR、通报、预 警、人工查验。	
处置响应	<ul> <li>将分析组件拖拽至编辑页面时,右上方显示&lt;编辑&gt;、&lt;删除&gt;按钮,需连线后才能对组件进行编辑,点击&lt;删除&gt;按钮或键盘上<backspace>、</backspace></li> <li>2000/2000/2000/2000/2000/2000/2000/200</li></ul>	处置确应 器 動火増 → EDR 通服 ● 预磨 多 人工置验
	<ul> <li></li></ul>	
按钮	<ul> <li>点击&lt;返回&gt;、返回到剧本编排页面。</li> <li>点击&lt;编辑详情&gt;、弹出剧本详情弹窗,可进行编辑。</li> <li>点击&lt;下一步&gt;、跳转到新页面,显示 剧本详情的内容(置灰不可编辑)和组成元素,点击&lt;上一步&gt;、返回编辑页面,点击&lt;完成&gt;,平台新增剧本中的指标和模型,并跳转到剧本编排页面,页面显示新增剧本。</li> </ul>	201 - 1 101 101 
组件删除	<ul> <li>任何组件的输入组件或连线删除后, 该组件配置内容清空并标红出错,连 线后重新添加配置保存校验。</li> <li>关联模型之前的任一模型删除,关联 模型的配置标红报错。</li> <li>统计模型有两个指标输入时,删除任 一指标,统计模型自动更新不报错。</li> </ul>	



区块	说明	详细
	◆ 指标修改后默认新生成一个指标 指	
	标的后一个组件统计模型阈值不变,	
	如果修改了时间窗口自动修改后面	
	统计模型的时间窗口。其他任何组件	8
	的配置修改不影响后面组件的配置。	× ×
		S.

# 6.6.3.2 处置响应详情

#### 1、防火墙

拖拽图标到页面中间,图标详情显示**<编辑**>和<**删除**>按钮,如下图所示。

顫 防火墙3	Å 🤇
联动设备	192.168.31.102
阻断IP	来源印
篇1次阻断	10分钟
第2次阻断	30分钟
第3次阻断	6/Jat

点击<编辑>·弹出防火墙编辑页面·页面内容主要分为告警来源、处置联动-联动设备、处置联动-处置 策略三个部分·如下图所示。

States a		(0.1.08)	2					
100								
C Marco		0.00.00.00						
10 (PA)4	2	-			3			
	S S	wante.						
	Co l	10000 0	10.0					
	2				1			
Ene . Q	3							
press ()	O ANALS	112000					10.7599A	
		4-124	1000					
1 mm 2	THE CHARTER TO A	80100	ion -	1.1	3	 -	SPRINT-SPILL TREE	and a
at most		9-24		- 00				
	(88							
Added -				1000	-			
10 Acres		-		_				
Q.M.								
8.14								
								1 mar - 1

▶ 告警来源: 显示告警来源的字段"模型 ID",不可编辑。



- ◆ 处置联动-联动设备: 联动设备为状态是已连接的安全设备的资产 IP。阻断 IP 默认为"来源 IP" · 不可编辑不可选。
- ◆ 处置联动-处置策略: 默认 3 次阻断且阻断时间分别为 10 分钟 · 30 分钟 · 6 小时 · 除了第一个阻断 · 其他每个阻断后都有一个删除图标 · 可删除阻断策略; 最后一个阻断后有新增图标 · 可新增阻断 · 最 多 6 次阻断 。

#### $2 \cdot EDR$

拖拽图标到页面中间,图标详情显示<删除>按钮,如下图所示。

EDR5	
联动EDR管理平台对告警 行漏洞扫描及修复	中的目的IP进

#### 3、通报

拖拽图标到页面中间,图标详情显示详情, <编辑>和<删除>按钮, 如下图所示。



◆ 点击<**编辑**>,弹出通报编辑页面,页面内容主要分为告警来源、结果通知两个部分,如下图所示。

Barren P				and the second s
a wife		1210	ana.	100
The second se	Stor. 1			197.
1 China	Party and the state	VERSE (Section 1)		and the second
7.00	1000) 10	ian ye		C. Hartoot
2-		(1995) ANDREAD C		
2.44		3 M (1		[4]mm - 2+]
1001 8.00		A PROPERTY AND A DESCRIPTION		1000 1000
9.2				
0.4788				



- ◆ 告警来源: 显示告警来源的字段"模型 ID",不可编辑。
- ◆ 结果通知: 通过工单、邮件或短信的方式通知所选组织下的通知人。

#### 4、 预警

拖拽图标到页面中间,图标详情显示详情和<删除>按钮,如下图所示。



#### 5、 人工查验

拖拽图标到页面中间,图标详情显示详情和**<删除**>按钮,如下图所示.



#### 6.6.3.3 其他操作

#### 1、查看

点击<查看>·跳转到查看页面·上方显示<返回>按钮和剧本名称以及威胁程度·点击<返回>可返回到剧本编排界面。下方显示剧本内容·如下图所示。

	ille in the second seco								
	ST. GREET V		25 10.2X89 / P						
Ň	0		USERIA characticoloftume contains "soft						
	」目前已由最小用社区市中情報到前期记录。至 这一份公共描述出来出来。	$\rightarrow$			COMPACIAL E	18	RE BAR		10
	****			1	mpan aviato		-	-	
	**			2	BILL	#H62	NAME OF TAXABLE	100,100.2 5	
					INVESTIGATION OF A	werth usy	W1122W	1044	
					1.492.010		Manage	30246	
	(2 materi / 4		23.00 2.00	1/	#100000 CODDO/W		RITER	6040	
	Macconder. Eg-Junger. Read Deam	۴	ERROR and that contains "which from observ" OR perfored contains: SEUCT count? OR polytical contains: Seud tathor? OR perfored contains. "Waiting" OR performance to particle CRI perford contains: "Weiting" CRI performance "touch the "	/					



#### 2、剧本查看

	<b>Х.</b> Париј на	ACKERALES		SOLIANSIO TURM STAAS	~	11 R0/187	2.1 2.1
and the second s			. /	WHA WHIA SCA WHIA SCA WHIA SCA	#HD sverifi (rgA, ) everifi (rgA, ) everifi (rgA, )	Biston Bisto Bistoppe Bistoppe Bistoppe	102-101-2 12 유명의 103년 33년년 6년9년
MALIARIA CICARO BUYON TRI JOR BRUMULIA. MERSI Diversi	NELLS.	peyload contains "when from whene" peyload contains "SELECT court" OR peyload contains "SELECT" (OII) pey contains " if view? OII avoidad contains INSERT" (IR payload contains "Into, o OR payload contains "Into, o	OR- doad Na 1 Na 1				

点击<**剧本查看**>·新打开一个页面显示剧本内容·如下图所示·

#### 3、编辑

点击<编辑>,跳转到剧本编辑页面,可对剧本详情和剧本内容进行编辑,具体操作步骤同剧本新增。

#### 4、异常记录/安全告警

点击<**异常记录**>或<**安全告警**>·新打开异常记录页面或安全告警页面·带条件:时间(最近7天)+最终 模型的 modelName。

#### 5、删除

缩略图模式下仅可进行单个剧本删除,列表模式下可进行单个剧本删除,也可进行批量删除。删除剧本时, 可选择该剧本的模型和指标是否一并删除。

#### 6、启用/禁用

缩略图模式下仅可对单个剧本进行启用/禁用。列表模式下可对单个剧本进行启用/禁用.也可进行批量启用/禁用。 当剧本禁用时对应的模型都禁用.有被其他剧本引用的自建指标或引用的是内置指标则不禁用. 只禁用在该剧本内自建的指标。剧本在禁用时不生成新任务。

#### 7、任务中

点击**<任务中**> · 可跳转到任务看板页面 · 显示该剧本下所有进行中的任务 ·

# 6.7 安全模型

#### 6.7.1 模型管理

用户选择 "安全分析>安全模型>模型管理" 菜单,进入模型管理界面。模型管理支持对系统中所有的模



型进行编辑、删除、启用、禁用、查询等操作。

#### 1、 模型查询

安全計算 安全规算 模型装置 **光現于**(前的)1、目的11.0 Q.) 推型标题: 1811.0 **新新 开展 开展 光道** 月末日長 石田 田忠 天田 机型关型: 不同 机形板型 光动机型 统计模型 小模型 情经模型 有线模型 21 B BA (2000) THEY AREA REC2 00 10.00 15 XHBA (111) : 模型名称: 62 使空大空: 算术记录 ne: dominin2021 domain2021 统计操作 5 0 0 统计模型 统计模型 0 longimeting 3 0 #BREAK! 9494875 堆 guardiantroxing 0 **地质形存在影响** Multiple INVent 情报规划 F正在访问内部系 3 2 8 statemaiSystem 统 市同PI袋蟹访问4 newsnoptiv 统计模型 5 1118 C 45(8) 技育-截载SOAR-1460.00 经利用型 ٩ 8 8 8 2 1 40398512

- ◆ 查询条件默认有关键字搜索栏、 模型标签、 告警状态、异常记录、 模型类型、 定制模型 · 所有条件默
   认都为不限。
- ◆ 模型标签有:从下拉框选择。
- ◆ 告警状态有:不限、开启、关闭。
- ◆ 异常记录有:不限、开启、关闭。
- ◆ 模型类型有:不限、规则模型、关联模型、统计模型、 AI 模型、情报模型、离线模型。
- ◆ 定制模型有:不限、是、否。
- ◆ 所有条件都为单选, 被选择的条件字体变色区分。并且模型管理列表信息自动进行过滤。
- ◆ 关键字搜索栏可以通过关键字查询模型 ID 及模型名称 · 只能输入字母或者文字 · 不能输入特殊字符。

#### 2、 模型列表

- ◆ 列表中显示列: 模型 ID、模型名称、标签、模型类型、定制、异常记录、 告警、状态和操作。操作包含查看详情、复制、编辑、安全事件、安全告警、删除。
- 列表默认显示出厂后出厂模型及自定义模型的所有模型。
- ◆ 用户定制模型通过创建时间降序放入列表中。点击列表中的列名称可以进行升序降序显示 · 每个列名 都支持排序。
- ◆ 可以对模型进行启用、禁用操作, 启用后模型才会生效。
- ◆ 可以对模型进行编辑、删除操作。
- ◆ 可以对模型进行复制。

#### 扩展流程

- ◆ 出厂模型只能在列表中显示、启用禁用、是否告警操作, 不能进行编辑、删除操作。
- ◆ 可以进行对模型进行批量启用、批量禁用、批量删除操作。出厂模型不能进行删除。

#### 规格及限制

列表中每页显示 50条记录,超过 50条时分页显示。

所有出厂的模型不能进行删除、编辑、复制。

#### 3、 模型创建

在模型管理页面, 点击<添加模型>, 进入创建模型页面, 如下图所示。

ANLPHATEL See Comment	and then along	er marmel (manuel /	10	1
NAME IN THE REAL PROPERTY OF		LETI NUS FROM	WHERE	AHER
	,c			

- ◆ 规则模型: 根据安全分析的应用场景 · 从日志数据中筛选出安全事件 · 触发告警或进行后续高级安全 分析。
- ◆ 关联模型: 跨越多个设备来源及数据种类, 从多个安全事件中检测行为模式, 发现隐藏的高级威胁及
   安全风险, 触发严重安全告警。
- ◆ 统计模型: 从安全事件中 · 发现重要的统计型特征 · 通过阀值过滤 · 找出异常指标 · 可以发现如频繁 暴力破解尝试等恶意行为 。
- ◆ 情报模型:利用威胁情报增强网络安全威胁检测和应急处置能力,支持通过已知线索筛选原始日志, 进行恶意 IP、恶意域名、恶意文件识别等威胁分析。
- ◆ AI 模型:根据历史数据 · AI 引擎持续构建并更新基线信息 · 自适应的发现异常和偏离 · 发现不曾想 象过的攻击来源及方式 ∘

#### 4、 创建规则模型

在创建模型页面, 点击规则模型, 显示新增规则模型页面, 如下图所示。



	A HERE A	No C Seen	~ B2461 ~	- same -	a read -	a model -	a second s
547 · 22	45 45	en cars and	8				
8448							
* 1833 D	00214						
. 1852.0							
#268							
1019-2	10053						
防御知道							
1000	<b>R</b> ide						
0.623	- 99						
0.623	28-						
DERE RIER	26 -						
8593- 9399	25-						
8583. 9358 10.	28-						
8533) 8598 11 1 1	28 -						
0.533. 0.558 1. 1. 1.	98 - 9834	#ca					
0593) 0593 01 1 1	- 3824	<b>神</b> 七道					
0553) 0553 1	- street	Noi Roli		8			
0525 0158 1 1	15 - 1 - 3885 - 3985 - 4046	Noil Roll		* *			
0593. 9358 11	100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 -	Noil Roll Roll Noil		9 9 9			
0523. 6198 11. 1	125 - 122 1000 - 1000 - 1000	勝七道 第七道 「 「 勝七道 」 同時日第 (Netting		9 9 9 9		* 202	
6583. 6198 10	25 - 10 - 1037 - 1095 - 1095 - 1095	Noil Roll Roll Noil Roll Roll		9 9 9 9		,*** 60°	
8535 9318 10 1	25 - 1 - 5537 - 5545 - 5545 - 5545	Noil Roll Roll Noil Noil Roll Roll Roll		8 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9		560 ***	

新增规则模型页面包含以下字段:

- ◆ 基本信息: 模型 ID、模型名称、 模型标签、 模型描述等
- ◆ 数据配置: 数据源、数据类型等。
- ◆ 模型配置: 配置规则模型的条件语句。 包括告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议、是否触发安全告警、是否输出异常记录等。

配置模型时, if ()判断条件筛选过滤条件, {}输出模型字段配置, 如下图所示:

	esexyrationes	
	5	
5         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -           60000         -		
		WE
All State     1	. · ·	
Image: Constraint of the second of	Brackber 1	
ARREY 40	of the second seco	
ARREN BELEVANA CONTRACTOR AND	81	
Admin gs		
- 258804 - 29880 - 29990		
1222 #5		
7,91983 ·		
simulate (1)		





- ◆ 默认表达式为空,根据语法树/字段搜索生成表达式。
- ◆ 字段选择内容来自于数据字典 · 选择的数据源不同 · 可选字段也不同 ·
- ◆ 字段信息包括字段名称及字段 ID 显示 · 如: 目标地址 (destAddress)。
- 支持字段模糊检索。可以通过中文名称或者英文字母过滤。
- ◆ 关系运算符根据字段数据字典的类型不同,内容不同。
- 匹配字段内容根据数据类型及关系运算符不同选择而不同。
- ◆ 点击 ·展开语法树 · 点击<添加条件>或<添加组>选择字段添加 · 在表达式框内生成一条表达式 · 每
   一个条件后面都有删除按钮 · 可以对条件进行删除。
- ◆ 多条件输入自动组合传入后端。
   相同字段带入以()组合都为 or 组合 · 不同字段之间以 and 组合 · 如 : a=1 · b=2 · c=3 · a=2 · b=4 · 带入后端的条件自动组合为(a=1 or a=2) and (b=2 or b=4) and c=3 °
- ◆ {}大括号内是模型输出字段 · 默认有告警名称、威胁等级、告警类型、攻击链告警描述、处置建议字段,也可自定义添加字段:如受害者、攻击者、标签等告警字典中字段。
- ◆ 字段值输出支持字段映射、静态值、模板、表达式。
   当选择静态值时,下方显示输入框,可输入文字。



当选择字段映射时· 下方下拉显示可选字段。 当选择模板时· 下方显示输入框·可输入模板。 当选择表达式时·下方显示 if 判断语句。

◆ 可开启/关闭是否输出异常记录/触发告警。

#### 5、 创建关联模型

在创建模型页面,点击关联模型,显示新增关联模型页面,如下图所示。

PHA	1988 - BO D 2MMID - ASMAD OPAN - IL C+AM	
10 - 9-91	an ansiet control stocke	
20000		
- 102 6.00	WEAKH	
mania.		
macris.		
#292	The second second	
1953	~°5`	
115.00	and *	
makela		
esen.		
法政府规定	244W,00 ARE##44, 825E##46	
0156		
(1) (1)		
et.		
	###	
	anti dissomento	
8		
0.1		
	ogan Beil	
2	ALASS BLA	

新增关联模型页面包含以下字段:

- ◆ 基本信息 : 模型 ID、模型名称、模型标签、模型描述等。
- ◆ 数据配置: 数据源、数据类型等。[∞]
- ◆ 模型配置: 配置规则模型的条件语句。包括关联方式、 if 过滤条件(事件 A、事件 B, 告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议、是否触发安全告警、是否输出异常记录)等。



16				→
	<b>B</b> HA	事件印		→ <b>关联条件</b>
東北人信日	Eluc(eventAluC) -	● ●HSE 指EDoC(wentElloC) ~ ●		
미데봅니	1 39			
希望名称	静态描	14		N
<b>北注写</b> 目	释主题	14 C		Ň
	6	14		S.
2963	#ol8	1 m		
	REALINE (WARNING			
8.8.8	Hell	18		5
	(0)))	· • .	NO.	
可适亨用			×	2
3998.5	標版	(*)		
	1378942		6 V	
い意識な	·信乐	14	N	
	大助开带关盘	(4) (4)	Les 15	~
all services			$\sim$ $\sim$	<i></i>

配置关联模型时,筛选条件有字段筛选和表达式筛选,默认为字段筛选,如下图所示:

- ◆ 默认关联方式: follow_by: 先发生事件 A · 后发生事件 B 。 下拉可选择其他方式:
  - and: 事件 A 和事件 B 同时发生。
  - not_follow_by: 先发生事件 A · 但没有发生事件 B 。
  - repeat_until: 事件 A 发生 n 次或以上,再发生事件 B。
- ◆ 事件 A、 B 通过表达式过滤。
- 支持字段模糊检索,可以通过中文名称或者英文字母过滤。
- 匹配字段内容根据数据类型及关系运算符不同选择而不同。
- ◆ 点击 · 展开语法树 · 点击添加条件或添加组选择字段添加 · 在表达式框内生成一条表达式 · 每一个 条件后面都有删除按钮 · 可以对条件进行删除。
- ◆ 多条件输入自动组合传入后端。
   相同字段带入以()组合都为 or 组合 · 不同字段之间以 and 组合 · 如 : a=1 · b=2 · c=3 · a=2 · b=4 · 带入后端的条件自动组合为(a=1 or a=2) and (b=2 or b=4) and c=3 °
- ◆ if 条件过滤事件 A 和事件 B 之间的关联关系。
   关系符当前版本仅为 "="号,其他暂不用支持。
- ◆ 每一个条件后面都有删除按钮, 可以对关联条件进行删除。



- 字段值输出支持字段映射、静态值、模板、表达式等多种形态。
  - 当选择静态值时,下方显示输入框,可输入文字。
  - 当选择字段映射时,下方下拉显示可选字段。
  - 当选择模板时,下方显示输入框,可输入模板。
  - 当选择表达式时,下方显示 if 判断语句。
- 可开启/关闭是否输出异常记录/触发告警。

  - ◆ 筛选条件约定同筛选条件一。
  - ◆ 筛选条件二与筛选条件一不能相同。
  - ◆ 同一个关联模型中, 关联条件不能相同。

6、 创建统计模型

在创建模型页面,点击统计模型,显示新增统计模型页面,如下图所示:



新增统计模型页面包含以下字段:

◆ 基本信息 : 模型 ID、模型名称、模型标签、模型描述等。



8	es n	MS市田市の市(AmiricanCount)	- er	
esti		en en angeneralita Ne on angeneralita		Areite
0	ages	Pc8		
	-	916		N.S.
		ŧ.		
-	+++2	ALS.	+	
		Altern I water		
8	144	816	+	S.
		10.	+	D.
	1349	128ulatei	· · · · · · · · · · · · · · · · · · ·	
			All and the second	
		FRENCH	-	
			0.00	
			PCR .	
			- 84	
		COLUMN STATE		S &
÷	want	81	Ŧ	C'
		194923	+	
0	-	en:	-	$O' : \mathcal{A}$
		NINERS	+	
		AWAGAD		

▶ 模型配置: 配置规则模型的条件语句。包括 if 过滤条件、统计指标、时间窗口,模型输出等。

- ◆ 默认显示一条统计指标选择框, 阀值输入框。
- ◆ 统计指标为下拉框选择, 内容来自统计指标管理中,可以进行模糊查询统计指标项。
- ◆ 点击 · 在已有条件下新增一行统计指标。
- ◆ 每个条件后面有个删除按钮 · 点击删除可以对指标进行删除操作 。
- {}大括号内是模型输出字段, 默认有告警名称、威胁等级、告警类型、攻击链告警描述、处置建议字段, 也可自定义添加字段:如受害者、攻击者、标签等告警字典中字段。
- 字段值输出支持字段映射、静态值、模板、表达式。
  - 当选择静态值时,下方显示输入框,可输入文字。
  - 当选择字段映射时,下方下拉显示可选字段。
  - 当选择模板时,下方显示输入框,可输入模板。
  - 当选择表达式时,下方显示 if 判断语句。
- ◆ 可开启/关闭是否输出异常记录/触发告警· 默认开启触发告警。
- ◆ 当符合条件的事件阀值满足阀值设置数, 产生告警。



时间窗口默认显示多个统计指标时间窗口的公倍数。并且动态提示时间窗口应该输入统计指标的公倍数信息。如:请输入 5、10、15、20 等 5 的倍数值。



#### 7、 创建情报模型

在创建模型页面,点击情报模型,显示新增情报模型页面,如下图所示。

PALSE         PALSE <td< th=""><th></th></td<>	
• H200         TERM           • H201         TERM	
- MERO 2005 - MERO 2005 MERO 20	
- MEAT MAN	
HEAT MEET	
HERE	
RUNZ	
BREAL MADE	
A MERICO MINIMA IOCEMA INVENTE ANNO CONTRACTOR AND A MERICA AND A MERICA CONTRACTOR AND A MERICA CONTR	
CO - RAM - RAM - ARM - ARM	
A 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	
* ` `	
A DEAL AND A DEAL	

新增情报模型页面包含字段:模型基本信息(模型 ID、模型名称、模型描述、处置建议)·数据配置(数据源、数据类型)·模型配置(if 过滤条件: 表达式筛选、碰撞字段、情报 IOC·模型输出)。

情报模型筛选原始日志或安全事件数据与威胁情报库进行碰撞·碰撞时需要选择指定字段与指定威胁情报 库进行碰撞·碰撞上产生安全事件· 亦可产生安全告警。

#### 8、创建 AI 模型

在创建模型页面,点击 AI 模型,显示新增 AI 模型页面。如下图所示。

A/LPHA	a nu o enem		+ #895-	- 1111	* HP20 -	- Strate -		
seam semu	HERE HERE WER	0	0					
数-开始的	ny and		~)					
+ (8510 /								
+82871+ =	NAMESTIN C							
agent in	C							
-	alertane.	COLUMN A						
and the second sec	Q							
				L				
1988								
Agentan	0.4			•				
tinget: W	1044							
10000	C. Beeck, C. Doctober							
BAR.								
G	HEREN PRETARE, 2921	10000000000	it EAT ARMS	NAME:				
~~	10492							
	Conversion Department International Conversion of Automatical Vision of Conversion of	A-MAGNETS	はない思想	anni ann				
-	100000000000000000000000000000000000000							
S.	CALCULA CONTRACTOR		副調約港 和	minima Segma				
	and the second s							
	PEPT ALLOST							

新增 AI 模型页面包含字段: 模型基本信息(模型 ID、模型名称、模型标签、模型描述)·模型配置(统计指标、检测周期·处置建议)。

配置统计指标: 统计指标为下拉框中过滤出已保存统计结果并且未配置 group by 的统计指标。

检测周期: 检测周期为 10 的倍数。



被 AI 模型依赖的统计指标不能被删除。

9、 离线模型

选择 "安全分析>安全模型>模型管理"菜单·进入模型管理页面,可以看到模型类型还有离线模型。

**离线模型**仅支持查看,不能新增、修改、删除。

10、 模型重置

选择"安全分析>安全模型>模型管理"菜单·进入模型管理页面。点击 按钮·然后在弹出的"确 定重置系统内置模型状态"对话框点击<确定>·内置模型的告警和状态恢复出厂设置。

#### 11、 模型导入导出

模型管理界面·按下"ctrl+?"组合键弹出隐藏 按钮·勾选定制模型·点击<导出>·导出定制模型规则包。

选择"系统管理>系统管理>升级管理"页面·点击<点击上传升级包>可以上传已导出定制模型规则包· 可导入定制模型·若环境中已存在相同名称定制模型·无法导入该规则包。如下图所示。

1000	anna - C - wa		100	peace	10			10	
mailer.	watter and a second	9092	e .	•	0			-	
1.与选定制权	M	m1+402		•	38	- •	٠		
10.02		611998		0	•			-	
-		100.025		- 31	0			-	
		10403	8	300	- 38		٠	٠	
++		101002	π.	3	38			-	
		10.00	*		0			-	
	Aug 11	and any second		•	0				
	**	101-102		•	(3)				
10	2	stres	*		•	- •		-	
		0.007		1.00	<b>*</b>	1.00			

# 6.7.2 指标管理

指标管理主要是将安全数据以某些条件过滤后进行统计, 生成的指标信息可以作为统计模型及 AI 模型的



模型指标项。选择"安全分析>安全模型>指标管理"菜单进行编辑功能。

#### 1、 指标检索

REST REPUBLIC NO.

法	(建字:		166) 1663	φ			Q.										
766	(新年)	0.579					17.1										
3	調測	जेला .	<b>3</b> %	83 <b>A</b> %88	安全市等												
100	方法:	<b>齐相</b>	COU	NT AVO S	WAX	MIN D	ISTINCT_COUNT										
-979 -979	DEC.	不容	豊	酒													
12A	她计	市際	蕉	an i							1						
	読書	不得	用度	美田							V						
										$\mathcal{O}$							
agi i	375									રું						15	31
	-	88	É	1.00		2008		经计	- Call	665 1770	1	-	100				
	0 =	191	1	and a		1	Broad ay	方法	att 1	-	Actes	100	and a				
	dom	dor	6			5.90	事件名称 美洲产 日的产	cour	10.95		-	-	1121	a.			
	an	940				CR		O M				-					
	ang	195	63			33/92	来商户 目的户方带协议	COUT	19	Q.		0			-	-	ĥ
	rbum ii					记费		4 M		3	1.000	~					
	ArGE	AIG	ė.			原始	BOSE SEPAL	10001	1383	-	- 16	-					i.
	NI.	NI	_			118	N.	) in	<i>O</i> .			-					
		100	8					Local Anna	S .								
	itwes	963	5			原始	目的吧 末潮門	rout	181	8	摄	0	-				
		120	2			11.52		mar .									

查询指标参数如下所示:

参数名称	参数含义	参数取值
关键字	设置查询指标的关键字。	手工输入,可以有统计指标 ID、统计指标名称。
指标标签	可根据内置或自定义指标标签检索。	下拉框选择。
数据源	设置查询指标的数据来源。	不限、原始日志、安全事件、安全告警等。
统计方法	设置查询指标的统计方法。	COUNT · AVG · SUM · MAX · MIN ·
		DISTINCT_COUNT °
保存结果	设置查询指标是否保存结果。	不限、是、否。
定制统计	设置查询指标是否为定制统计。	不限、是、否。
状态	设置查询指标的状态。	不限、开启、关闭。

#### 2、 指标新增

чгп	A	0 801 U 2990 - 10890 -	+ <del>\$2</del> 09i -	s said -	■ po*包括 *	0 朱桃曾理 ↓
eeen vie	\$400 I	但15世间 · 高级期间				
基本信息						
く温心し	NUMPORTS					
1768	and i have	1.0.0				
- Q.						
1866E	\$5.0 ALTON	お前毎				
网络结合	10445.000	SEX BANKARASENDON				
				i		N
数据起度						A.
お採用	课输日志			5.42		
* 215g	出版:			-		· · ·
CHARGE COLOR						
140						
	过度影件	10				0
3	Group By	alitita			6	
	精计方法	count +			$\sum_{i=1}^{n}$	
	0.080	19 *			×	2
8						
1 3	CRAT	46				.C.
	iem///s					
870	PROFILE.	(T)				

需要输入指标基本信息(指标 ID、指标名称、指标标签、指标描述)·数据配置(数据源、数据类型)·指标配置(if 过滤条件、指标输出配置)。

新增指标参数如下所示:

参数名称	参数含义	参数取值
基本信息		
指标 ID	设置指标的 ID 标识。	手动输入。统计指标 ID 在整个数据字典中必须为唯
	S.	•
指标名称	设置指标名称。	手动输入。统计指标名称在整个数据字典中必须为唯
		- •
指标标签	设置指标的标签类型。	点击输入框选择,可以多选。在弹出的指标标签对话 框,点击< <b>添加标签</b> >新增自定义标签信息。
数据配置		
数据源	设置指标的数据来源。	原始日志、异常记录和安全告警。内容对应相应数据字 典的数据表·默认显示原始日志;数据源只能单选。

参数名称	参数含义	参数取值
数据类型	设置指标的数据类型。	默认全部 · 取消全部后可选择其他数据类型 · 支持多选 。
指标配置		
过滤条件	设置指标的过滤条件。	非必选项。
	筛选条件内容包含:字段选择、 关系运算符、匹配字段内容。 字段和匹配字段内容都是来自 数据字典。	点击 · 展开语法树 · 点击添加条件或添加组选择字 段添加 · 在表达式框内生成一条表达式 · 每一个条件后 面都有删除按钮 · 可以对条件进行删除 •
Group By	设置指标的分类条件。 字段显示内容来自于数据字 典。	可以下拉框进行选择,可以对字段进行快速查询,字段 信息包含中文(英文)显示;可以自定义顺序选择多个 group by 字段信息。 每个条件后面有个 <b>删除</b> 按钮,点击删除可以对条件进 行删除操作。
统计方法	默认显示一组统计指标,内容 包含:统计方法函数选择、字 段选择、统计指标 ID、统计指 标名、详细描述等。	函数为下拉框选择,内容包含:COUNT、AVG、SUM、 MAX、MIN、DISTINCT COUNT,只能进行单选。
时间窗口	设置指标保留的时间窗口。	时间窗口下拉可选, 默认 1min,还可选 5min、10min。
保留方式	设置指标保留的方式。	保留方式可下拉选择·默认全部·可选 TOP X。
是否保存统 计结果	设置添加指标的统计结果是否 保存。	开关按钮选择。如果选择不保存则缓存24 小时。
是否开启	设置指标添加后的状态是否开 启。	开关按钮选择。

字段筛选截图如下所示

 2			0		
105-5-5	27014710-0	(effice - (deat)			
	REACHING .	78710 - 10		94	- Am
ANE -	0.000	(10000 100		<ol> <li>(EWE)</li> </ol>	control to black
				10	derednes with
				700	0007449-00010
				87	(Hardware N 1942 Hit 1 187 1942 Hit 2
				182	dama and a rest of the rest of
				51.	construction (2012).
				2308	141 Million ( - 102)
				法治学过期	41.42344-1222
				ANYLES NOVES	1010/00/00000-101001-101001-001
-			1.211	101112	
-111				A.11811	WINDOWSKI ADMA W2.841

杭州安恒信息技术股份有限公司

🗸 安恒信息



#### 表达式筛选截图如下所示

表达式是直接写在 siddhiSQL 语法里,以下是常见语法。

80. 80 101 0	-	104	-	
40.0			-	18
	straighter - 201401131.000 Sterrows - 201401.005		1747	arv-0
(A) R.	an Aphran or "All 160 ( 127 (10 Indexemples - "All 160 ) 122"		111	mutthins and in the second sec
1427	NUT181-Malence 102 108 1 1011	1000	792	
- #7	40.50 Here - 10.10 - 111		87	Ameridade and the second secon
10 Tal	anotativate (***102.100.1.)		187	and hitsey min ( 101 100 1 101 100 100 100
	anamerica estat	171210	2.4	constitution with the second second
× 37	0007701115229	-	2008	minute all
+ 27	The amplication state		25718	An Andrews - Will
the safest meaning and	New York New York New York (N. 27, 1999)	100,000 (00,000 (00,000)	ALC: N	Reserved on the second se

#### Group By 筛选截图如下所示

		×
12189/4	8	* 00
Onud By	ERITECTOR Protocol · BRIPCONDAGRAM · BRIBCLANDPORT	2 6
纳计方法	<b>地用字段</b>	
10480	ALTERNING Protection	
	H89Posstwament	
	BRIEF-Eloest-ostvare)	
保護方式	Electric constraint	
NY One Lot	Ets:Ri+&/out.terNate)	
TOWNSDAM	Caracteria and Caract	

#### 3、 指标查看、复制、统计结果、删除

- ◆ 点击[™]按钮, 可查看指标详情。
- ◆ 点击 按钮, 打开复制页面,可复制指标。
- ◆ 点击●按钮, 可查看统计结果。
- ◆ 点击 按钮, 可删除指标,内置指标不可删除。

#### 4、 指标启用、禁用

点击 🍧 按钮 🕖 可以启用或禁用指标;指标支持批量启用或禁用。

# 6.7.3 数据字典

选择"安全分析>安全模型>数据字典"菜单进入数据字典页面。

数据字典统一管理平台上的字段信息包括: 数据来源、数据的标准化字段格式说明、目标存储平台等基础 信息以及攻击链、告警字典等数据。

通过数据字典可以查询接入的数据对应的字段信息· 包含表名· 表字段信息。支持数据字典中数据信息的 维护· 包括数据信息的录入、修改、删除。



#### 1、 数据字典检索

A'LPHA	N 87 Q 288	e senar	- A RADO - IL BALLE - A DURA - D ANDE -		0 emer
1007 10050	物种干燥				-
KRE: Milli	NO((KEPHINE)				
THE	NOT WHERE AND THE	AR 10 100 10	ng tractory and		
Trint it 21	the parts store				
표주에서 2월 표	ά .				
Record N	2				
522200 E					
MICCOM!					
R 153 R	÷			0	
				0	**
9980	1998 C	9988	418 ·	TARE	RA .
Resident	Butter la	Roal			
ada	And Test	and .		CORD	+ 2.4
35414	DEMAN	101	gen wurdennen werdensterenten (DK	CEND GEED COUD	820
alerithine	11404	-	clive.	CEND CEED CEED	±0000
mai	00040	104	wish	din can can	+ (2)(4)
odate -	1017-03	110	16543		4.8.9
DE20940340	(P109283)	0.06	Indianal	0000 0000 0000	10 Pt 10
**	ISRNC	1746	gliencrationers Resalaccularies all sector	CELEV CARD CELEV	- (c)(t)
the state	1055 B	end.	where whereas a fer ner freeder action	000000000000000000000000000000000000000	(4 G2(4)
1000	379.3	110	inductive of the second s	0000 0000 0000	<ul> <li>(2)(1)</li> </ul>
access/spery	\$1*39.04/06/Y	100	\$78*Yex -1528*\$283882 #*\$7518425#25	× CON 6550 (CON)	(A) (F) (A)

- 查询条件关键字搜索栏可以通过关键字查询任何关键字的信息,包括字段 ID、字段名、描述关键字。
- 字段类型: 不限、 boolean、 double、 enum、 float、 int、 ip、 long、 string、 timestamp、 array。
- 字典类型: 不限、原始记录、异常记录、安全告警。
- 是否常用: 不限、是、否。
- 是否内置: 不限、是、否。 •
- 是否常用: 不限、是、否。
- 否支持查询: 不限、是、否。
- 是否支持聚合: 不限、是、否
- 2、数据字典新增

点击 🧯 按钮 · 打开新增字典页面 · 如下图所示:

AOLPHA	NET O MIC	Q 200000	~ #EAN#REL ~	4 安安9 <b>6</b> ~	8 全部活業	* 80°83 -	o siedių -
820H   82M3	259A NETR						
+ 360	and a state						
+ 988 :	061725						
7693	string						
· 7888	🛛 Pails 🔽 Pails	2 F228					
· 唐谷常用: (						00	
基直支种新闻:	•					S.	
ADDREN (	0					V.	
9828Z -	1061-21022					)	
	97 N				8		

- ◆ 字段 ID 字段名必填。
- ◆ 字段类型列表下拉选择, 默认为 string。
- ◆ 内置的字段类型有: boolean、double、enum、float、int、long、string、timestamp、ip。
- ◆ 字典类型分为原始日志、异常记录、安全告警,默认全选。

#### 3、 数据字典查看、修改、删除

- ◆ 点击操作列 按钮 · 可查看字典详情 •
- ◆ 点击操作列 按钮,可编辑字典。内置字典不可编辑。
- ◆ 点击操作列 按钮,可删除字典,内置字典不可删除。字典被模型或指标引用后不可删除。

#### 6.7.4 数据清洗

#### 功能简介

选择"安全分析>安全模型>数据清洗"菜单进入数据清洗页面,可配置系统的过滤项、检测项。数据源 为原始日志,数据(日志、流量)先通过检测项,后通过过滤项。检测项不配置时,所有数据通过过滤项。

数据清洗和白名单的作用分别是前置过滤和后置过滤, 确认要分析的数据和不分析的数据。首先要配置数据清洗,确认要分析哪些数据, 然后在数据清洗的基础上,配置白名单,确认不分析哪些数据。

数据清洗的作用是从海量的原始日志数据源中筛选出需要分析的数据· 只有通过数据清洗后原始日志数据 才会进行进一步的分析。如果系统不配置数据清洗, 那么所有的原始日志数据都会直接进入下一步的白名 单过滤。



# 6.7.4.1 检测项

检测项仅分析(统计、模型)检测项配置匹配的数据。 不同策略条目的关系: 逻辑或。数据满足其中一条 检测项策略,支持存储、查询, 同时支持分析(统计、模型)。

#### 1、查询

界面输入策略名称, 点击查询 🤐 按钮。支持策略名称模糊查询。如下图所示。

包括

各条件关系:相同字段逻辑或,不同字段逻辑与

取消

选择学议。

确定

ATTAL TOTAL PRIAM				C BATTER -	$\dot{\mathcal{O}}_{\mathbf{V}}$	٥
10900 (Cont 1000 (000) 1 12000 7000 (000) (000) (	Device Texa of the second			Ċ,	• •	
				2	-	
at hit		12.1888	-	1 Har interes	$\rightarrow$	19 MT
CORE SING				0		
and the		* 支持规则件》		*		
autori i						1011
			NORM O	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
International Part 1	the set with the set of the	ernow and will	2		Alte 1	sing- ag i
			X	6		
Au 7-1-				N.N.		
刘建						
刘建			S	S.		
<b>刘建</b> < <b>创建</b> >・打开	新增检测项策略	§页面, 如下图	所示。			
<b>刘建</b> < <b>创建</b> >・打开	新增检测项策略	ふしん うちょう うちょう うちょう うちょう うちょう あんしょう うちょう あんしょう うちょう うちょう しんしょう しんしょう しんしょう しんしょう しんしょう あんしょう しんしょう しんしょう しんしょう しんしょう しんしょう しんしょう しんしょう しんしょう ひょうしん しんしょう しんしょう しんしょう しんしょう しんしょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひ	所示・			
<b>刘建</b> < <b>创建</b> >・打开 新増检测□	新增检测项策略	5页面・ 如下图	所示。			
<b>刘建</b> < <b>创建</b> >・打开 新増检测项	新增检测项策略	3页面 · 如下图	所示・			
<b>刘建</b> < <b>创建</b> >・打开 新増检測項	新增检测项策略 新略	3页面 · 如下图	所示。			
<b>刘建</b> < <b>创建</b> >・打开 新増检測項 ・名称	新增检测项策略 前带略	うううう ううしょう ううしょう ううしょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひ	所示。			
<b>刘建</b> < <b>创建</b> >・打开 新増检測項 ・名称	新增检测项策略 5 <b>前略</b> 10入188568	うううう ううう ううう ううう ううう ううう ううう ううう ううう う	I所示。			
<b>3)建</b> < <b>创建</b> >・打开 新増检測功 ・名称	新增检测项策略	うううう ううう ううう ううう ううう ううう ううう ううう ううう う	所示。			

参数说明如下表所示。

参数	参数说明	备注
名称	输入检测项策略名称。	必填项。
添加条件	点击< <b>添加条件</b> >添加筛选条件,条件内容:字段名称、运	条件之间的关系:相同字段逻辑

输入值多值以"分割

复制



参数	参数说明	备注
	算符、字段取值、复制按钮、删除按钮。	或·不同字段逻辑与。
	运算符支持包括和通配符:	
	<ul> <li>◆ 包括: 支持输入一个或多个值 · 多个值以英文逗号分 隔;</li> </ul>	60
	◆ 通配符:支持输入通配符·如: "192.168.111*"。	1.00

#### 3、编辑

点击操作栏 按钮·弹出修改检测项策略弹框· 输入相关信息· 点击<确定>保存。如下图所示。

影改检测	项策略		***	** 6		
* 名称	112.10.10.1		2	. S.		
	添加条件		30 30 00			
	来源P(srcAddre ~	通配符 ~	112 10.10.1		复制	Ū
	各条件关系: 相同字段	逻辑或,不同字	段逻辑与			
	确定 取消		S			

- 4、刪除
- ◆ 点击检测项策略可选框 · 点击<删除> · 支持删除指定检测项策略;
- ◆ 点击全选框·勾选当前页面所有检测项策略· 点击<删除>·支持删除指定检测项策略;
- ◆ 点击操作栏 按钮 · 删除该条检测项策略。

# 6.7.4.2 过滤项

过滤项不分析(统计、模型)过滤项配置匹配的数据。不同策略条目的关系: 逻辑或。数据满足其中一条 过滤项策略,支持存储、查询, 不做分析(统计、模型)。出厂内置两条过滤项。

#### 1、查询

界面输入策略名称, 点击查询 9 按钮。支持策略名称模糊查询,如下图错误:未找到引用源。所示。



	8/98- a 6098-	0 ***
une, Garilet, Vertrage, somearilet		
	A.2900	<b>6</b> .90
•		
支持模糊資油		5
countries in	max	80
1100 Sec. 10		2.1
	Alberton A Debition A Debition A	→ NARAHAL → LA DADAR → W NYFRE → E AREEN → UNIF, NATIONE, UNIF FARM, HARRANTIME → <u>Rotation</u> → <u>Rotation</u> → <u>Contaction</u> → <u>Rotation</u> → <u>Contaction</u> →

## 2、创建

点击<创建>,打开新增过滤项策略页面,如下图所示。

• 名称		
	添加条件 · · · · · · · · · · · · · · · · · · ·	
	「御経学録 ~ 包括 の 輸入値 教育ない 分割	复制 🛙
	各条件关系:相同字段逻辑或 不同字段逻辑号 确定 取消	

# 参数说明如下表所示。

参数	参数说明	备注
名称	输入检测项策略名称。	必填项。
添加条件	点击< <b>添加条件</b> >添加筛选条件 · 条件内容 : 字段名称、运 算符、字段取值、复制按钮、删除按钮。 运算符支持包括和通配符 : ◆ 包括 : 支持输入一个或多个值 · 多个值以英文逗号分 隔;	条件之间的关系:相同字段逻辑 或,不同字段逻辑与。
参数	参数说明	备注
----	-----------------------------------------------------	----
	<ul><li>◆ 通配符:支持输入通配符·如: "192.168.111*" 。</li></ul>	

#### 3、编辑

点击操作栏 按钮, 弹出修改过滤项策略弹框, 输入相关信息, 点击<确定>保存。如下图所示。

			0.1	
<b>‡</b>				
estAddi 🌒 包括	× 127.0	.0.1	5	(RE) 0
	estAddi @ 包括	r estAddi ● 包括 ~ 127.0	estAddi ● 包括 ~ 127.0.0.1	estAddi ● 包括 ~ 127.0.0.1 家

#### 4、删除

- ◆ 点击过滤项策略可选框 · 点击<删除> · 支持删除指定过滤项策略;
- ◆ 点击全选框·勾选当前页面所有过滤项策略· 点击 ◆ 按钮 · 支持删除指定过滤项策略;
- ◆ 点击操作栏 按钮,删除该条过滤项策略。

# 6.7.5 白名单

选择"安全分析>安全模型>白名单"菜单、可配置系统的白名单。

与数据清洗模块功能不同·数据清洗模块属于前置过滤·对数据进行全局过滤·但无法进行细粒度添加策略·无法针对指定模型进行添加过滤策略;而白名单主要针对数据源为异常记录/安全告警的数据进行过滤· 当发现异常记录/安全告警存在某一类误报较多时·可以添加相关白名单,后续满足白名单过滤条件的异常记录/安全告警将不再入库·快速排除掉该类误报。

## 6.7.5.1 白名单相关操作

#### 1、查询

- 支持对白名单名称/条件进行模糊查询;
- 支持对白名单启用状态进行查询;
- 支持对白名单是否生效进行查询。



#### 如下图所示。

and Inc. Const. Altern The Yes will Altern The Yes will Altern The Yes of	支持对自名单名称条件进行模糊和	e de			
C					
	54	Ameri	100007	(mn	an .
states prevent to pell	gender - Trill Ministreet, schief Mehand, in participation (14) 20 20 20	*=#	0021-01-021 92-00-00		-
one terrisol	metros	8.00 M	antistation .	10	-
and an international state	Sector - 19 10 Sector ( Cigr. Sector) - and - (N. W. 192)	548	MARKEN COM		ME 514
NAME TO REPORT OF THE PARTY	mantana - Sari 🔤 atamay - 2019k1039 🔤 antana - Mattalaw	7948	. Interest in the second	0	
state creater interior	Security - the states - the test state of the security in the security of the	TAUL.	mercran comm.	(C)	100 100

#### 2、创建

点击<创建>,打开添加白名单页面。如下图所示。

添加白名单页面条件、策略名称必填·策略名称选填·生效时间支持长期生效和定时生效· 支持将最近 7 天历史告警标记成误报。

	MALERAN X	
ates to a s		~
	- man S S	
(10094700 C	Head American and American American	
one permand		E) An NY
( AND A DECEMPENT OF A DECEMPENTA DECEMPENTA DECEMPENT OF A DECEMPENTA D		Et an an
6458.09CNJ = 01	And	(1) 201.000.
Canal Distancies and	and a second	E
Constantine Constantine	XXXX Californian ()	and the second
		- past auto-

#### 3、编辑

在白名单列表中选择一条白名单,点击操作栏下的<编辑>,打开修改白名单页面,如下图所示。 支持修改白名单条件、策略名称、策略描述、生效时间、勾选将最近7天历史告警标记为误报。



A88	<b>学员白白来</b>	
Allow of A a	- BE BUILDER - THE AND REAL POST OF A CONTRACT OF DESCRIPTION	
	terminate particular	
and to make	NEAR INFIDENCIAL STREET	S P
one mercedati	Allere and and another the transmission	
() from a subscience of		

## 4、 启用/禁用

支持单条白名单启用/禁用· 也支持批量启用/禁用白名单。当启用白名单后· 白名单过滤立即生效; 禁用白 名单后· 白名单失效· 不再对异常记录/安全告警进行过滤。

◆ 单条白名单启用/禁用

白名单列表中选择一条白名单,点击状态栏下的启用/禁用按钮,白名单启用/禁用生效,如下图所示。

AILP	HAtta - na	C EMME - MANNET	+ weiler - u untile	sres- skitt-			0 ****
41m / 1	1000 Jane		<u></u>	S			
		. 0					
***	10 10 10 ml		S				
	11. 10		8 0				
	(vieta)	84	2 5	N-ROOM	name1		-1017
	new becaused	10000 - 17 - August	Colline and the Colling of the Day of	anty Pinta	2011/11/11/10:00:00	(	
	new inservice	interest of the state		a risa	ARTITUT NAME	•	
	new province of	man - He water		rina (inter	manual distance		
	OCK DISACCOMPT			How Final	manage and a		
	DOM INTRACIONAL	Mar and and and	and the second s	No.	maintaint	•	
		Oj.	S		***		an. as i. a

## ◆ 批量启用/禁用白名单

白名单列表栏中多选白名单·点击列表左上方<**后用>**或者<**禁用>**按钮·可**后用/禁用**选择的白名单;当全选 白名单列表·点击列表左上方<**后用>**或者<**禁用>**按钮·可选择对当前页面的白名单生效或者对所有满足查 询条件的白名单生效·如下图所示。



AND TR TR AT	Q.				
BSONE		Adda64	1000	82	81
Chastlenewsk her	and a state of the	0.9	and or all residen.	•	-
	a page the second as provided a provide the second se	10.0	2021-01-011-0000-05		
1 AND 2 ALC: N & A	and a state of the second s	ites.	2021-24-07-0228-46	()	-
CONTRACTOR NO.	naintan - <b>30 -</b> adama - 70 001227 - addma 770 002	r Aug	autorational (		-
and transformed	making - Brief at states - 118 mileter - 118 mileter	er. 388	marene marie	50	-
			Ain	111 .	
			- Ann	CALCE 1	

#### 5、删除

支持单条白名单删除, 也支持批量删除白名单。当删除白名单后, 该条白名单失效, 不再对异常记录/安全 告警进行过滤。

◆ 单条白名单启用/禁用

白名单列表中选择一条白名单,点击操作栏下的<删除>,如下图所示。

ALF	PHA::::: - ==	Carrier - martin	+ 2216 - N TRUE -	• 2792				G
8110	ALC: NO.			Q.	2			
	10 million ( 100	(8)						
**	ne te la sil		B					
-				R				
	NORRA I		0	2	1.000	CREAK!	410	80
62	the property of	press - W - mod	and the second s		224	and to at some		
62	100 (100 million)	preside - The most	Color and all	No MINAN	284	2011-01-01-02-02-02		
-	trans formation of the	man	Comment of		2mm	per si al transiti		
	ten (restater)				Tes .	particular shares		
	tes (restance)	and from			TAB	plan an an epision		
		U.S.	S					088- 85 · 3

批量删除白名单

白名单列表栏中多选白名单·点击列表左上方<删除>·可删除选择的白名单;当全选白名单列表·点击列表左上方<删除>·可选择对当前页面的白名单生效或者对所有满足查询条件的白名单生效·如下图所示。



100 0000 000 0				
HER DECEMBER 1				
NTAL IN HE AL				
80 80 m				100
D DAWA BRUCA	1000	10000	. 65	
	104	autorup scalas		
The provide the second	100	approval to and		
and the second state of th	124	anner seine		
(a) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	100	month and a		
🖬 – none (1962), weinder: - 1967 - 176 - 176 (1823) - 176 (1823) - 176 (1823)	1100	anna san	•	
		Arres .	1111	
		- OV		

#### 6、 白名单失效

白名单列表中, 可以查看到有一栏为失效时间。失效时间与创建/编辑白名单时的生效时间/类型有关。

◆ 当创建/编辑白名单的生效时间/类型为"长期生效"时 · 则白名单列表中失效时间为不失效 · 如下图所示。

and the second second			
and Income	ИТЕНИ		
And 10 10 10	0. 0		
ADDA (10) N (1)	+ 800 = 1 (atention - "W. HE: treationing - [79/97] maker [1] (1) (atention of [1] (1))		
			_
	- manual page this and	_	
	MARKE CREATING AND INVESTIGATION OF COMPANY		10
VALUE (DATUM OF ALL)			-
100 m 2112 10 10 10			44.25
and the second second	LINE CONTRACTOR DATES	-	
	and and all a super and the		
CONTRACTOR CONTRACTOR		- C	
ALLA EMPLANANT	and the second	80	
		END A	lines at 1
		10 Marca	

当创建/编辑白名单的生效时间/类型为"定时生效"时,需要指定一个失效时间,则白名单列表中失效
 时间即为指定的失效时间,当时间到失效时间时,该条白名单失效,不再对异常记录/安全告警进行过滤,如下图所示。



AILPHATEL	men canno wanto a parte a prete a ante-	E alter -
and manual	ditibe#	×
1000 10 10 10	- Box 🔠 Stration - 107 And Investige (1949) (Manuel J (1920) (	
(art art (art))	-men and provid	1000
served :	MARK MARTINE, THE MENUE	44
press (resources)	选择定时生效。可推定失效时间、自名导到失效时间后将不再过透	C 44 10
inter presented		
and includes the	Aller SHAR	
The second secon		C 201 10 10
And Distances and	Bang mantenanciada O	(C) 0.00
		The second second
	Ś.	

## 7、 将最近 7 天历史告警标记为误报

在创建/编辑白名单时·在**历史告警**选项中可勾选"将最近7天告警标记为误报"。此选项勾选单次生效· 即当勾选后·满足该条白名单过滤条件下的最近7天安全告警处置状态会置为"误报"·当再次编辑该白 名单时·该选项置为未勾选·可再次勾选对相关安全告警进行标记误报·如下图所示。

And manager	HOTELE	× .	
AREA IN AN AN			
AASA TH. A. S	1 889 😨 (double 110 🚾 freedowing - D-aff) (Maxar) ((1) (analyze) (10 (20 10 20 1)		
	- meter man t-scornigh		ECC
(onene)	HEAM MULTING HEAM STATE	40.7	2019
One DHIMMING	C. C.	<b>(</b> )	44.107
0.000,000,000,000			25.00
10-10-10-01	A REAL PROPERTY AND A REAL PROPERTY	(0)	100.000
GR# 20140404080	Contraction of the second seco	<b>6</b> 50	44.39
Ante manarieriant	entre and the second second	(C)	10.00
		ERICI I	9.82 AZ 17
		1 6 M	

## 6.7.5.2 创建白名单其他方法

除了选择"安全分析>安全模型>白名单"菜单进入白名单页面创建白名单外·其他页面也有创建白名单入口·如下所示:

## ◆ 入口一: 异常记录创建白名单

选择 "**安全分析> Investigation> 原始日志**" 页面选择数据来源: 异常记录· 任意展开一条异常记录详 情·支持添加白名单·如下图所示。



£.200 - 2
0.0012

## 入口二:安全告警创建白名单

选择 "**安全分析> Investigation> 安全告警**" 菜单 · 在该页面普通查询/聚合查询下 · 选择一条告警点击 列表操作栏下<**处理**> · 支持添加白名单 · 如下图所示 ·

AUP	PHA		0.0000 - 00		- N. SEGE- # 0788	- 's suttaine - )			0	-
-						10 ² 3				
-						* 00	415			
						X	Concercia militari		an ¥ m.	- 3
1000		Overside the	International Constant and the	an menandan la	Internetari Department I aprese (	PE-montran etermination of	inania ini	-		14
		8100 Dos	Ne Real Per		when month of	Y .C.				
-										
		4.87	1984	WEP-MR	anton	inell Standard	ALC: N	allegene .	AREA 1	-
- e -		10.1011.01	111-10.100.000	(643)4	WWWWWWWWWWWWWW		84	200303-011028-02	110	12.
				T DESIGNATION OF T						-
		16 98 13	112 15 00 1	and the second se	and an a state of the state of		810	3021-11-07 10:02 02:	ALL AND	
		12.2.1	112 20 00 1	(*****			esc.	200-0-0-10000	100	100
		96 98233 9224 94 988 11 200	112 H. 100 H	(man) (main)			84	annendrichten annendrichten annendrichten	11	101
		NE 9223 1221 NG 9841238 NE 9223	112 56 66 1	(march) (SH2) (march)			81 81 81			
		NE NE 13 1221 NG NE 15.00 NE NE 13 2121	112 52 001 112 52 100 00 112 55 00 7 112 00 00	(martin (hearing) (martin) (martin)			81 81 81			

◆ 入口三:安全告警-查询下创建白名单

选择"安全分析>Investigation>安全告警"页面, 普通查询/聚合查询下, 选择一条告警展开详情, 支持添加白名单, 如下图所示。

	- 49400 - A 21208	· notifi · notifie ·	0 KAT21# -		C entre
till bergins \$250	0				
₩2.₩1	NO C	<u> </u>	0	9 •8	
	~ ~	, ,		sistemation and	na Mana Kana - m
Invite Contraction and	highing sminkvess #	salastic instant and the	And Alexandra and Ale	a notación Roan Sudra	400110
WARE MADE THE OWN DOWN	102VHD GR00 3.50	3:040 H100*C /			
All Aller . Cliffer	83749	Britan	timest scotte	House average adverses	ettera an
- 162.000 (102.000) (102.000)	8m2#	man/manetalaw) (crister		the advances	1011 AND 00
CONSTRUCTION OF THE OWNER OWNE	I E DELETION IN NUMBER INCLUSION DELETION B LIPPI	tosicso & HEIN) Anterician, a Reiz, Nichtrosik, Reizhour		Annue (Brith - ) (Ballour B I	1. 1499 11. 142W 1
102100-11,200 - (10.00) KAND		#12FURD#F04507219214 45050		172.18.100.30 -	(#)
和金融 ANG 1240	10	<b>汉</b> 州上帝		2.210 million	# 36070 10Ph
		1.000		mace = ====	

◆ 入口四:安全告警-聚合查询下创建白名单

选择"安全分析>Investigation>安全告警"页面, 聚合查询告警详情中, 选择一条会话详情, 支持添加白名单, 如下图所示。



	mail 1	*2014	*#	的银子来来	mesen	3284	timits)	10000-046	sie niewentes	R018133660 1	MACRONIAL I	num i	10
-	100108-01-01	##	-	TIN LIN	HUNDREDUK (2.45)	(B) (D) (11) (A)	10-01 m	Daily .		mationation H	and the second s	-	
12.465	e entre	-		*###	Teac. of the agenum	89742 -	an contractor	BICEN -	2000		. Date		
	PE			450		2414	BASONDER	DARATEMEN	2 max eres area	orden Versional energy into praction spinorecellation energy	n Kress Sala even approxim sight controls 6 100 50 6000	now Mith Set c	
								292848		*	2 46 00 00 00 00 00 00 00 00 00 00 00 00 00	43-5 811-17 60	
distry and a	A RE	water - Dater -		8 m	at at			( INNEATE	- 272 RA		(Busten) C.a		15.0
0.0	nininini.	18.74 (1.1) (3.5		基本信息 请·文神主帝源					15	SV			
	11.47 1941 11	100 Mill 10 11 1 12	iz pa nen en	195.168.11.11 evel-10.0(241, 10.046.120.10	152887 + 172.16.100.90 2/57 8.11.11	8.89				V			

### ▶ 操作入口五: Sherlock 创建白名单

选择"**威胁感知→Sherlock**"页面· 对指定 IP 进行查询· 点击列表操作栏<**处置**>按钮· 支持添加白名 单·如下图所示。





7. 安全运营

# 7.1 工作台

# 7.1.1 功能简介

选择"安全运营>工作台"页面,工作台概括了工单、通报情报,从工单状态、待办工单、通报情况、最新动态为用户展示安全运营全局情况。如下图所示:

	C STURM	- 1000-000-	A SERVICE	8 9311 <b>=</b> -	= जगक्तवे ∽	-		antes 🛛
essa Ina						K		
Tans					I III TEMNI	05		
606	9	5	EA.	6+	12	2	15-	208
301¢				tii-			3	
I#28	¥6	454. IN	) Ref	10 th	195V	Lo.	SIGNI (2000 WAISPOOL	148 esteri Dura-Grand SV (317000)
LIBRATH HTV/RODECT	NEW P	10 20	0.00.09 21 47 52	15	PUDBUG CB	Argana #1 1	sal of booked by subscreet	The linear (www.eeess) or (
tender som son same	-	200	0.08-06 11.47-48	100	Constant of			
TRACT WEIRHOUSE	(Incol)		0.07.28 15.46.25	114			NONI LEARNIN WALLFRONTH	143: 0-0281 [PH:50Course+33] (87: 12815
TERMI NO	-0444	-	14.22.17 15.20.0	Ju ,	rubsuo ca	Argans RJ 1	Weller (worke) [L.S.B.LOOD) Necletic] 202 [Bollel] [Net	VALUE COMPARENT (VALUE - VALUE) (VALUE COMPARENT (VALUE) (VALUE) (VALUE) (VALUE) (VALUE) (VALUE) (VALUE) (VALUE)
TORS OF A CONTRACT OF A DESCRIPTION OF A	-	a. 20	6-07-34 (3.34 %)	( da	15	1 17.00		
I III 81 Adapty Terms	-	-si	0 07 21 70 48 24	6	On1	the fact	5月286)【武田王代-66-191,148,997 1998】【三田王代-60-191 (40:00 model)	nostie] 100 17 (ecologi (Embol vectorent) 12
THEM! NO.	1009		. 800000	S IN S	00	- Invit	e caramatica ( a caramatica) ( a caramatica ( a car	tooverwates to be said the sur-
TRATI NUMBER (FOR THE ADDRESS )	-	a	11.75 00 10 10 10 10 10 10 10 10 10 10 10 10	5 🙀 🤇	5			122
1.00.01.00	(Inca)	5 20	0410121020	. 6	22	20 (PG	ALTER CEASES WEDFALLER TO	BORNE CHERNOLOGIA COLORES
Line Str. or	<b>EXERCISE</b>	116 N (200	a we and a set of the	Q.	0	D ANT	MORENT OF THEOREM TO CONTRACT	al or inseril have been in
				S.				

# 7.1.2 工单状态

工单状态展示未处理、处理中、已解决和已关闭的工单数量;点击某个状态可跳转到"安全运营>工单管理"界面,并带上状态条件。如下图所示:

工单状态	- M	点出市	LUNAL (	911年1月1日日	并带上该状态条件	ŧ.				
	来处理			处理中		8	解决		已关闭	
	22			0		0	). ₁ .		0	
2028 1928										
12 - 10		148 1898			- 197		- 100	( Jane )		
0.000	Albert .	INSU .	-	RN6	Wittensi -	HEAL .	284.1	1981.1	HERE .	
1400100000000	817	(uneth) (man) ei	16.0	1060	1000	00108	12/10	40822	(0.0+ c+ c) (0.00 m)	12.00.00
C	#10	10405281 (10000-01) 1040222-201				0000	854	843002	(mode): 0.259	12.46.70



# 7.1.3 待办工单

待办工单按照工单创建时间列表展示未关闭的工单·点击<处置>·跳转到该工单详情页面。

点击 按钮 · 可以跳转到 "安全运营>工单管理" 界面 · 如下图所示:

97上年			"到疆工单"按钮,后击可期转到的	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
			"肥多"铁镜,自击到	時到工學管理界進
工单主题 ※	秋志	优先级		展代
【通处理】【获取股票】【哈哈哈-规则编型2】0 次	未放理	-	2019-09-11 18 49 16	91 B
【書任理】【詳報授用】【訓除新-規則機型2】4 次	未推理	10	2019-09-11 17:27:14	22.W
【请处理】【积积权限】【始始始·规则搜型2】2 次	未处理	覆	2010-09-11 17 77 34	013
【通过理】【获取权用】【始始始-规则模型2】11 武	未处理	*	2015-29-11 47:07:14	91-2
【書任理】【祭取役用】【始始始-规则相型2】43 次	1355	R	2019-09-11 16:57.14 (###WT#	
【書任理】【原取授用】【始始始-相別構型2】17 次	未放理		2019-09-11 16 47 14	419
【佛处理】【原职权限】【端始始-规则模型2】6 次	未改理	*	2010-09-11 48:37:14	œ.a
【清论理】【资产采标】【应用程序会运流量统 计】3次	未处理		2010-20-11 15 57 14	113
【書社理】【音产破坏】【应用程序会话流量的 计】6次	AND NO.	S	2019-09-11 15:47:14	4 <u>1</u> 2
【请忙理】Unix SSH服务器最力装解	100 A	-	2019-09-11 15:06:00	SER
	S	100	# 22 5 ( 1 2 3 3	- 新至 1

# 7.1.4 通报情况

展示未关闭的通报紧急、警告、一般级别的通报数量; 点击跳转到 "安全运营>通报预警>通报"页面, 并 带上优先级状态。如下图所示。

通报情况	C data	國際總面調	<b>后,</b> 并带上(	优先级状态			
	28 ×			警告		-192	
	<b>2</b> ↑			2		1 个	
2211							
8688 10-10-1	and the			- 98	- 10 88		
10.011.00							
	mann i	**		10.1	main in	manual -	80.
3 300 ( ) ( man	patients) (possis introduct an		-		autom	224.6.08.12.54.10.00	
international c	proventy providents or	-			avent	2010/06/12 14:00:04	A12 100 100 100



## 7.1.5 最新动态

展示最近通报的 4 条通报信息 · 点击可跳转到该通报详情页面 ; 点击 按钮 · 跳转到 "安全运营>通报 预警>通报"页面。如下图所示。

最新动态	"自建市场器",后击司其转到的建分器开展页面 —— 🔶 🕂 🚽
affe	【获取权限】【SMB运程溢出攻击】2次 【获取权限】[SMB运程溢出攻击]2次【获取权限】【思察文件攻击】2次【获取权限】【应用程序会适流量统计】6次
2	10分钟結 Unix SSH服务器種力破解 ▲ 点面親結對通报手續界面。 [描述] 暴力破解的原理是咬击者利用用中名和液弱字典。一个一个类較率、要試量百能等登更、攻击者尝试使用暴力破解 乾燥服务器的后程登越用中名和液弱,会造成用中SSH登录用户名和流码扩量。可以直流name字段。要是否有大量sh稳重 失败的操作。[違议] 验证FTP服务器是否存在第口令、短时间可以通上原中的访问,提端登录家码的服杂量。同时购买 10分钟相

## 7.2 通报预警

## 7.2.1 功能简介

选择 "安全运营>通报预警"页面, 页面展列表预警和通报。用户对平台产生的安全告警进行新增预警, 提示平台用户该告警可能存在一定风险隐患, 需要注意或确认; 当确认该告警的确存在风险隐患, 用户可 即刻将该预警通报, 平台下所有用户可以看到该通报信息,及时采取安全防护措施。

## 7.2.2 预警

选择 "安全运营>通报预警>预警" 页面,页面列表按照创建时间倒序排列展示所有预警。

#### 1、 查询预警

默认支持预警名称、创建人、标签、级别查询;点击<**高级查询**>,可支持编号、预警时间查询;点击<**重** 置>,可清空所有查询条件。如下图所示。



#### 2、 新增预警



点击<新增>,进入到新增预警页面,输入名称、标签、级别、对象、详情, 再添加举证信息,举证信息支持输入攻击者 IP、资产 IP、安全告警 ID、域名/URL,最后点击<保存>, 预警新增成功。如下图所示。

	恶魔文件攻击	$\sim$
标签:	<b>当</b> 進行为	梁則: 室● ~ ~
対象に	36 23 57 138 168 3 30 8	- CV
洋播:	H B TI F I U & Ø I Ø	= = = = = <u>-</u>
	[冊述]	
	检测到回意文件下载或上传行力,下载或上传的文件中包含一 资源消耗率危害。	整不安全的内部、如台会等每大马,会造成主机被控制。
	【建設】	*
	利用杀毒软件对资产中的文件及相关密动项进行核查。一目通 骨,如文件沙销等。	以对唐章文体进行删除。同时,可采取相关的防病者设
	B BOR ( ) HARRIS & TENTING AND A TEN	Br S
	◎ PETFLET# (●PTYN914大小小中) 截过2000. 至期中日4大小小中日和	· ·
举证:	源如樂這信息	
举证:	凝如単迂信意	
举证:	凝如鄉近信息 攻击者IP → 36.23.57.136	
₩位:	版加举证信息 攻击者IP ~ 36.23.57.136	
举证:	様加単迂信思 攻击費iP → 36.23.57.136 数产iP → 166.3.30.8(180.130.8)	
# <u>@</u> :	版加寧迂信息	
₩Ğ:	坂古単迂信思     攻击者IP ~ 36.23.57.136     坂市IP ~ 166.3.30.8(180-3.30.8)     安全告部IO ~ 51224438045146725	
₩Œ:	添加単逆信息 攻击費iP → 36.23.57.136 波产iP → 166.3.30.8(166.3.30.8) 安全告寄iD → 51224438045146725	

## 3、 安全告警入口预警新增

选择 "安全分析> Investigation>安全告警" · 选择一条告警 · 展开查看详情 · 点击<发布预警> · 进入新增 预警界面; 安全告警名称会自动填入预警名称; 安全告警威胁等级会自动填入预警级别; 安全预警来源 IP 和目的 IP 会自动填入预警对象; 安全告警模型描述及模型建议会自动填入到预警详情; 安全告警来源 IP 、 资产 IP、事件 ID、目的主机名/URL 会自动填入到举证信息攻击者 IP、资产 IP、安全告警 ID、域名/URL · 点击保存 · 预警新增成功。详情可参考上图所示。

#### 4、 预警查看

选择一条预警, 点击操作栏中的<查看>,进入预警详情界面。

#### 5、 预警详情



1) 页面元素: 展示预警标签、级别、创建人、预警时间、详情、举证信息等; 支持通报、

编辑、删除、返回、查看上一条预警、下一条预警; 支持举证信息跳转; 支持添加备注信息; 支持查看历史记录。如下图所示。

or passes arguests		(0) 48 (0) (1)
149. EXTENDE MAIL: ANYTH: 158. ALTONIA TALENA	and an and a second sec	S #11-8/1-018
HE INF) UNEXTYPELING, TELINETYPEI OFENNE PERMIT PERMIT PERMIT UNEXTYPELING, TELINETYPEI OFENNE PERMIT UNEXTYPE STORE INFORMATION STORE INFOR		02,00
		2
Bar Server	****	\$

2) 举证信息跳转: 点击举证信息下拉按钮, 支持跳转到不同页面。详细请查看下表。

举证信息	跳转页面	详情
攻击者 IP	<ul> <li>◆ 支持跳转:情报查询/安全告警查询/安全事件查询/原始日志查询/Sherlock/攻击者追踪溯源/资产威胁溯源。</li> <li>◆ 安全告警查询/安全事件查询/原始日志查询带条件: srcAddress:攻击者 IP+时间条件: 最近 30天。</li> </ul>	<ul> <li>学証</li> <li>攻击者(P)</li> <li>192.168.95.22 -</li> <li>安全音響音詞 (2) 算法已受意词 (2)</li> <li>第始日本意词 (2)</li> <li>第始日本意词 (2)</li> <li>第始日本意词 (2)</li> <li>第始日本意词 (2)</li> <li>第始日の第四</li> <li>(1)</li> <li>(2)</li> <li>(3)</li> <li>(4)</li> <li>(4)</li> <li>(5)</li> <li>(5)</li> <li>(6)</li> <li>(7)</li> </ul>
资产 IP	<ul> <li>◆ 支持跳转:情报查询/安全告警查询/安全事件查询/原始日志查询/Sherlock/攻击者追踪溯源/资产威胁溯源。</li> <li>◆ 安全告警查询/安全事件查询/原始日志查询带条件: srcAddress:资产 IP OR destAddress:资产 IP+时间条件: 最近 30 天。</li> </ul>	第一冊         WEB並動系統 20.19.17.443-11.25.17.01(11.25           放击者IP         情報音波 GD           安全古智印         音楽記書音波 GD           地名FURL         開始日古音波 GD           Sheftort GD         Sheftort GD           福注         王戸鉱制潟園 GD
安全告警 ID	<ul> <li>◆ 支持跳转到安全告警页面:查询条件:指定安 全告警事件 ID。跳转方式:新增页面。</li> <li>◆ 携带时间条件: 最近一年。</li> </ul>	挙证 资产中 166-3-30.8(166-3-30.8) - 攻击者中 35-23.57 136 - 安全等答印 51224438045146725 69 総名(URL www.alipha.com +

举证信息	跳转页面	详情
域名/URL	支持跳转: 情报查询/打开链接。	<ul> <li>学研下 165 5 30 8(166 5 30.0) ・</li> <li>Roman 36 23 87 136 ・</li> <li>学会栄育の 51224438045146725 69</li> <li>焼気URL www.alkpha.com ・</li> <li>焼気URL NWW.alkpha.com ・</li> </ul>

3) 备注: 在备注框中填入相关信息,备注框支持贴图、插入链接、文字编辑等等操作。

支持附件上传·单个附件大小不可超过 20M·全部附件大小不可超过 50M·点击<提交>。历史记录会保存备注信息。如下图所示。



4) 历史记录:预警编辑、备注提交都会保留相应的历史记录·历史记录可查看预警所有的变化及动



态,也支持下载备注提交的附件,如下图所示。



- ◆ 通报: 点击<**通报**>, 该条预警被通报,通报完成后当前页面自动切换到下一条预警详情页面。
- ◆ 编辑: 点击<编辑>・进入到预警编辑页面・ 编辑页面可编辑名称、标签、级别、对象、详情、举证信
   息等・ 点击<保存>即编辑成功・ 编辑操作会记录在预警详情页面历史记录中。
- ◆ 返回: 点击<返回>,可返回到"安全运营>通报预警>预警"页面,并会保留之前的查询条件。
- ◆ 删除: 点击<删除>,删除当前预警,页面会自动切换到下一条预警详情页面。
- ◆ 上一条/下一条预警: 点击<**上一条/下一条预警**>,可切换上一条/下一条预警详情页面。
- 6、 预警编辑
- 选择 "安全运营>通报预警>预警"页面,预警列表中选择某一条预警点击<编辑>,进入到预警编辑页面。



编辑页面可编辑名称、标签、级别、对象、详情、举证信息等· 点击<**保存**>即编辑成功· 编辑操作会记录在预警详情页面历史记录中。如下图所示。

(R. 1	NUCL MENT		
- 88	0810103.01011		
-	and 1	m m -	
-+			
	play Mechanical and Alexandronical Mechanics	anaurre 20,04843, 180270785	
	ideal characteristic contraction of the	areatarian in fatoretaga	
	I BREAM THE AND	1000	
*4	101104		
	and - origination	•	
	same - same		Č.
	anne - lipiopearp		
	#215 ·		
	47 84		
			<u> </u>

### 7、 预警删除

选择"安全运营>通报预警>预警"页面·预警列表中选择某一条预警点击<删除>按钮·可删除该条预警; 点击预警列表上方<删除>按钮支持批量删除预警。如下图所示。

124 8044			SC	2		
10 AU			U O			
Name and Address	10.		Den S	<ul> <li>(6) -</li> </ul>		
	-					14
81.	70.10 ·	· · · · ·		100.1	March -	*******
	100001 (000000001111		2		2010/07/14/14	
	2010/02/2010		Canarinimensurina	LANGE C	2010/01/11/14 41:10	
	10010110-010020110		20	MARKS .	1000-00-10-14-07-00	
100000000	Intelligence and the state			and the second s	223410.00	
14.0	110040) 1100444280pr142	-		avent.	2010/06/11 (027.0)	
	Transit Samerenger	······································		Acres.	104401010	0 C 447 44 21
				Ave.	20021120	
	in transferrent in the second	. 0		Andrew .	2010/00 11 13 al 14	22 44000 20
(an owned)	Interest Standard and			+1410	and in the second	
	Toplay Supersonant o	-		1000		
	S				DUCK - T P	1421 RE 1

#### 8、 预警通报

选择"安全运营>通报预警>预警"页面·预警列表中选择某一条预警点击<通报>·该条预警被通报; 点击预警列表上方<通报>支持批量通报预警。



预警被通报后不再展示在预警列表中,可至 "安全运营>通报预警>通报"页面查看。如下图所示。

- 24						
<ul> <li>********</li> </ul>	4961 (1014		<ul> <li>(66) altr.</li> </ul>		88	
100 THE R. W. C. W						atreate
81.	Anna -	**	14.1	441.1	PROFE -	
	1000000 2-1-0000011-0	-		avent.	(and all of the first of the fi	
	DECKER, Index	-	2012/01/01/01/01/01/01/01/01	6925	( more in the second	** *****
	1880001 2+4+80/8011-F				anna a star	
	transfit here aparts to	-		server.	- Cor	
	interest content and in-	-		01001	managerature	
-	The state of the second	-		44883	Seat arri	*****
	(source presentation) to			averet.	generative.	1212
	(and the state of the state of the	-		24930	C anna and w	
	tranker printmanagement			sores.	. V seesara	
and second	Desided strategical statements			second.	D' anne inte	

## 7.2.3 通报

选择 "**安全运营>通报预警>通报**"页面,页面列表按照通报时间倒序排列展示所有通报,通报均由预警转化而来。

#### 1、 通报查询

默认支持通报名称、状态、标签、级别查询; 点击<高级查询>,可支持编号、发布人、通报时间查询; 点击<重置>,可清空所有查询条件。如下图所示。

Ru Ad		高级	查询		_
4020 Juli 100	ite/ inte	C	- 88 ann	22	10°C 223 -

2、 通报查看

选择一条通报,点击操作栏中的<查看>,进入通报详情界面。

3、 通报详情



1) 页面元素。

展示通报标签、级别、创建人、发布人、预警时间、发布时间、详情、举证信息等; 支持关闭、派 发工单、编辑、删除、返回、查看上一条通报、下一条通报; 支持举证信息跳转; 支持添加备注信 息;支持查看历史记录。如下图所示。

solt alle Bulk		
100 ( 100000 ) ##10 00, 10000 ( )		11 (11 m m m
NB         NC           NBA         \$4.4993           NBA         \$4.9993           NBA         \$2.9993           NBA         \$2.9993	THE PARTY AND A PA	So ration
-18 100 molecularitaritati valimiterati al'azardi razdati azarrian Alambia 1911 shiarenetricitoteziati gi -la martella, be lakkainaia zuriaz		Sr I
NU TETRY MACHINESTING TETRY MACHINESTING TETRY MACHINESTING MILLING MACHINESTING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING MILLING	illi	2
	60	
• • • • • • • • • • • • • • • • • • •	*	1
A DECEMBER AND A DECEMBER OF A		0
M.		
secs.	2 C	
A 12 TO A 14 T	, N	

2)举证信息跳转: 点击举证信息下拉按钮,支持跳转到不同页面。详细请查看下表。

举证信息	跳转页面	详情
	1200 S	<b>挙证</b> 资产IP 166.3.30.8(166.3.30.8) -
	◆ 支持跳转:情报查询/安全告警查询/安全事件查	攻击者IP 36.23.57.136 -
攻圭孝 ID	询/原始日志查询/Sherlock/攻击者追踪溯源/资产 威胁溯源。	安全告部D / / / / / / / / / / / / / / / / / / /
攻山扫 Ir		波名/URL 安全事件遵阅 69
	◆ 安全告警查询/安全事件查询/原始日志查询带条件: srcAddress:攻击者 IP+时间条件: 最近 30 天。	安全日志登词 co Sherlock co 攻击雷迴院勝源 co 资产威胁测波 co
		举证
. (	◆ 支持跳转:情报查询/安全告警查询/安全事件查	题miP 166.3.30.8(166.3.30.6) -
	询/原始日志查询/Sherlock/攻击者追踪溯源/资产	攻击者IP 情报直阅 @
资产 IP	<i>15</i> 0,197,7991,71示 。	安全音響的 (5 GD) 安全事件查询 (5 GD)
	<ul><li>◆ 安全告警查询/安全事件查询/原始日志查询带条</li></ul>	线名/URL 安全日志黄词 GD
	件: srcAddress:资产 IP OR destAddress:资产 IP+时间条件: 最近 30 天。	Shitrlock GD 攻击者道段崩漠 GD 资产威胁强厚 GD

举证信息	跳转页面	详情
安全告警 ID	<ul> <li>◆ 支持跳转到安全告警页面: 查询条件: 指定安全 告警事件 ID。跳转方式:新增页面。</li> <li>◆ 携带时间条件: 最近一年。</li> </ul>	<ul> <li>学研P</li> <li>166.3.30.8(166.3.30.8) +</li> <li>攻击者IP</li> <li>36.23.57.136 +</li> <li>安全吉答印</li> <li>51224438045146725 G9</li> <li>域名/URL</li> <li>WWW allipha.com +</li> </ul>
域名/URL	支持跳转: 情报查询/打开链接。	<ul> <li>第1日</li> <li>155 5 30 円156 3 30.8) -</li> <li>200 円157 20 20 20 20 20 20 20 20 20 20 20 20 20</li></ul>

3) 备注: 在备注框中填入相关信息, 备注框支持贴图、插入链接、文字编辑等操作; 支持附件上传, 单个 附件大小不可超过 20M, 全部附件大小不可超过 50M, 点击<提交>。历史记录会保存备注信息。如下图所 示。



4)历史记录: 通报编辑、备注提交都会保留相应的历史记录 · 历史记录可查看通报所有的变化及动态 · 也



支持下载备注提交的附件。如下图所示。

历史记录	
所纳管理员	5 102, 153, 74 106 2019-09-12:14 45:46 进行了30下操作
<ul> <li>由京都</li> </ul>	
600530	98
SMT 12	4. 11/2 568.74 188. 2019-09-12 15:04-47 出行了部 予願作
+1508	
200	
	事理会
201 1 = 1	8-06-12 T0.130.00 2019-06-12 T.200.00 2019-06-12 T.1.00.00 3019-09-12 T540.00
机防管理器	§ 192 568 74 185 2019-05-12 15 10 29 进行了此于瞬作
• 80.55	N. ### 父亲为 ###
•=#	# 基础文件标准 101 W0017 · · · · · · · · · · · · · · · · · · ·
• 17.00	M. 3623.57 136, 1663.30.8 20.51 306, 166.3.30.6, 121 10 10 1
•65	N IIIII AR A A A A A A A A A A A A A A A
いた変換が	5. 1122.558.74.1055 2019-59-12 15 11 09 2EFT.781/FWPF
·#22	

5) 关闭/开启: 点击<**关闭/开启**>,可以关闭/开启该通报。通报详情页面状态实时修改,如下图所示。

ALLY ALLY ANY	S. S.	
10 61		
AND ACCESS		
3a a	20 - D	
**		
STREET STREET, TREEWISTING STREET, STR	(adjy size. a state and a state of the state	
(\$1) and a contraction of a contraction of the second seco	minimative hitsing	

4、 派发工单

在通报详情页面点击<派发工单>,进入新增工单界面。

- 通报名称会自动输入到工单主题。
- 通报标签自动输入到工单标签中。
- ◆ 通报紧急/警告/一般级别会对应工单优先级高/中/低; 通报对象会自动输入到工单对象中。
- 通报详情会自动输入到工单详情。
- 通报举证信息也自动输入到工单举证信息。



最后需要手动选择工单受理人, 点击<**保存**>, 派发工单成功。如下图所示。

- ◆ 编辑: 点击<编辑>・进入到通报编辑页面 · 编辑页面可编辑名称、标签、级别、对象、详情、举证信息等 · 点击<保存>即编辑成功 · 编辑操作会记录在通报详情页面历史记录中。
- ◆ 返回: 点击<返回>、可返回到"安全运营>通报预警>通报"页面,并会保留之前的查询条件。
- ◆ 删除: 点击<**删除**> · 删除当前通报 · 页面会自动切换到下一条通报详情页面 ·
- ◆ 上一条/下一条通报: 点击<**上一条/下一条通报**>,可切换上一条/下一条通报详情页面。
- 5、 通报编辑

选择"安全运营>通报预警>通报"页面,预警列表中选择某一条通报点击<编辑>,进入到通报编辑页面。 编辑页面可编辑名称、标签、级别、对象、详情、举证信息等,点击<保存>即编辑成功。



<b>z</b> (†)	88,21432,2110	112			
tite:	diment.		Ab wa		
en.	362337.138.98333	0.0.121.10.10.1			
195	NOR N R	1.0.0.2.2.2			8
	(%d) (%d) (%s) (%s)	Rimin, Terlimontes	-BTRIME NUMBER		36
	\$ 100111148W.				
	B NIN TH IMIAN	(七):不利益(2364、金虹明符大):不可	18:21010	$\dot{\alpha}$	
=1	Maswant				
	8(*)P ~	168.5.30.0(100.3.35/0)			
	10089 -	<b>36.11.17</b> .197			
	2000 -	11224438045146725			
	1864URL -	www.alipha.com		* ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	

#### 6、 通报删除

选择"安全运营>通报预警>通报"页面,通报列表中选择某一条通报点击<删除>按钮,可删除该条通报; 点击通报列表上方<删除>。支持批量删除通报。如下图所示。

TAST	16.53世			0				
88	393			Q	S.			
20101	041-05170	1.5 ===	24		and and	* <b>8</b> 8 (000		88 88
TR.	**	支持批量删除记录	0	N.				
	80.	#\$80 -	965		-FB (	<b>86</b> 人:	anne 单条册	除记录 🖬
	2012/00009585	TRADA) (Windows AD) D united the state of th	TR	C		RATE ST	1025-12-0 14:25:00	22 40 40 10
	2012030316-0001	tions ted and	176	3		a kezeri kezi	2020-12-08-00-53(0)	22 million 2.0
	20120308363437	TAMA CONTRA	THE			6443305	2026-92-02 (0.3522)	
	30702480632328	APREPORT 1 TH MARKED TO APREN (C IMARKED 1) APREN 201. E		-		A6381812	3625-0-34 23 28 03	and second set
	001030002030	LARTESI (Webbin RDP Br Landau/2007年月期日前 10 年月20日-000日 11日	Hat	-4		<b>私地推进</b> 现	1000-15-04 23 00-38	24 45259 22
	2010124400002127	Salaka HTTP Solver (B) PERSK		80	18.501.188	NAMES OF	2020-11-24-23 https://	-
	Distances and	TRACARD INVALVATION ADD BI	-	-11		NATER	2520 0-24 10:30 29	
	201123000023462	INFORMATION INVASION REPORT INVASION INVASION REPORT VELISION INVASION INVASION		-8		0.6832	2620-11-21-11-14-88	

7、 通报开启/关闭

选择"安全运营>通报预警>通报"页面,通报列表中点击某一条通报点击<开启/关闭>按钮,可开启/关闭 该条通报。



点击通报列表上方<开启/关闭>,支持批量开启/关闭通报。如下图所示。

100 000							
BREE	10.000			400 mile	31.0	(40) (40) (40)	41 88
TH - 15 80	Ter Product						
81.	8649	90		241	851.1	allow -	**
and parents	@#1004_3110011		**	SEALTH 196 (44) (10.0 TO 10.0 (	-	1010-00-0210.0010	
	Design Designation	-	-		second.	1000000 10 10 10 10 10 10 10 10 10 10 10	
		8.03	**	-49+100338	server.	manufactor at an an an	
	100001 (1000004040-1)	-	**		same!	and them	88 mil 200
	Internet Investments in		**		arrent.	and a starting and	
	\$2003000 10-000 000000(11-0		14		00000	Approved to the set	

## 7.3 工单管理

## 7.3.1 功能简介

选择"安全运营>工单管理"页面, 页面列表按照创建时间倒序排列展示所有工单。

用户可以通过工单管理界面新增工单、通报详情页面新增工单、安全告警页面新增工单·并将工单指派给相应的处理人·经过各个环节的处理·工单记录状态为**未处理/处理中/已解决/已关闭**·便于监督工单是否及时处理以及闭环。

## 7.3.2 查询工单

默认支持工单主题、状态、标签、优先级查询; 点击<高级查询>,支持编号、创建人、受理人、创建方式和创建时间查询;点击<重置>,清空所有查询条件。如下图所示。

100	1.00		T 14	100.00
	1.691	75	1.9	12:21

-											WORK AND
IWER	SHATES.		## 4.C		0	6 <b>5</b> ans		☆先段 ■ 音詞框	54	•	29 22 .
公園 -	899		25								818
	19 E	928976 2 C	E#EM +	88	例大概	WORKE :	包建方式:	東連人 ※	包建人生	6929993	操作
	2012200000 302	***	181日) [sr 1 snatBitlitt 当1 8次	#15.0	e	0.049	Ribit	新纳普理员	5.55世纪5	2020-12-28 1 7:41:41	12.01 (444) 254
	20122806000 301	inter and the second se	(ASR) [M (Stocpesaw distancesaw distancesaw	NOT		101246	n conti	<b>新建物型</b> 型	多的普通气	2929-12-28 1 7:31:41	en su no
	201122858608 305	#128	(4040年時1) (15月45日第1) (5月455月(1) (初日945月1) (初日945月1) (初日945月1)	-	8	101948	相当世間	新闻教育员	影響管理	2820-12-28 1 7:31:41	ton and me
	20122806000 299	812	(FI用) [# nd tr 逻辑HI #FSGLI(人句	4117	W.	101294	#:058	11月1日日日	83511进行	2020-12-28-1 7-31-41	

## 7.3.3 新增工单

手动新增工单有三种方式· 分别是工单管理界面新增工单、通报详情页面新增工单、安全告警页面新增工单,详细操作步骤如下:



#### 1、 工单管理界面新增工单

选择"安全运营>工单管理"页面,点击<新建>,进入新增工单界面。

输入主题、标签、优先级、受理人、对象、详情, 再添加举证信息, 举证信息支持输入攻击者 IP、资产 IP、 安全告警 ID、域名/URL,最后点击<保存>, 工单新增成功。若受理人有绑定邮箱,则工单生成时发送邮 件给受理人,一个工单发送一封邮件。如下图所示。

* 主题:	WMALL NEW		
6班	and the set	优先级: 低	Ċ, Č
<ul> <li>HEREFERENCE</li> </ul>	II. MERORIA		'lli
• 受理人:	10.57		2
<ul> <li>2)置約11-</li> </ul>	(25.4		3
102	SEATESTICS N. P. 263	. BELER. HA DE	E.
;甲销;	$H = \Theta = \mathcal{R} = \mathcal{R} = \mathcal{R} = \mathcal{R} = \mathcal{R}$		
		S C	
	■ 附件上件(単个物件大小不可提出20%4、全)	BHEMAXA-A-TUMICESDM()	
举证:	語加学正信意		

#### 2、 安全告警入口新增工单

安全告警入口预警新增。

选择 "**安全分析> Investigation> 安全告警**" · 选择一条告警 · 展开查看详情 · 点击<**生成工单**> · 进入新增 工单界面 ·

安全告警名称会自动填入工单主题; 安全告警威胁等级会自动填入工单优先级;安全告警来源 IP 和目的 IP 会自动填入工单对象;安全告警模型描述及模型建议会自动填入到工单详情;安全告警来源 IP、资产 IP、 事件 ID、目的主机名/URL 会自动填入到举证信息攻击者 IP、资产 IP、安全告警 ID、域名/URL;最后需 要手动选择组织架构、工单受理人、处置动作,点击<**保存**, 工单新增成功。



若受理人有绑定邮箱,则工单生成时发送邮件给受理人,一个工单发送一封邮件。详情可参考下图所 示。

* ±#:	Apecha root_sepret年最佳的计量可能	*
68	(and the second	2003 K V
CHORES.	and and a second se	
・ 宏雄人:	0.110	
化置均均	8.5.9	
77.8-	210.04 123 101,11 22 10.50	
	12 8 12 7 2 4 8 [開枝] 電車加線用や高Appoin機器開始です。 向AP機能、自動的時時間での許容。 を用きく開発的な影響用しないがすれたが [開枝] 両面「第日が思想プチド谷木丁小林教会 同面」での「数字のプチド谷木丁小林教会 同面」での「数字のですいないか」 を開きため、「数字】を見まっていた。	арайняша Гиннора я 2312 жа Гаван 2. аран 24. арин - кан ни та ла Балан Салан Салан 2. аран 2
#Z:	単加単正信号 15日巻戸 - 218 H4 (23-18)	
	安全秘密的 - 555738741007	risesme
	365549L ~ 11.22.18.59	0 01

#### 3、 通报详情派发工单

选择"安全运营>通报预警>通报"页面·选择一条通报·点击<查看>·进入通报详情页面;点击<派发工 单>·进入新增工单界面。

通报名称会自动输入到工单主题;通报标签自动输入到工单标签中;通报紧急/警告/一般级别会对应工单优先级高/中/低;通报对象会自动输入到工单对象中;通报详情会自动输入到工单详情;通报举证信息也自动输入到工单举证信息; 最后需要手动选择组织结构、工单受理人、处置动作, 点击<**保存**>, 派发工单成功。如下图所示。

- 252	982/066_010012			
10	11100	ietul +		
Wealth.	4,000,000	I lea		
1884	303	· ANGAIND BR	中山的 性情的 100 年 10	
nellion.	411 -	1		
18	94,2537 FOR 988 X 30 R 121 10 10 1			
-	11 0 T F I N 0 P	/ / E E H H E -		
	19675			
	ubligate Tablingh, Tabliers Hildrand	остьй-в7ейсти скімвій (	aniaforma	
	1380<2			
	1039401201*9223009065666 8.82575984	a -decregoraties, by the		
	I HILL MINISTERION, AND	try-2000 team	S.	
*0	Atoniati			

# 7.3.4 处置工单

## 1、 页面元素

选择"安全运营>工单管理"页面,选择一条工单,点击<处置>,进入到工单详情界面,如下图所示。

No. of Concession, Name		40.000			1	3	- 1948	1000	+ L	84. 88
R-11.00				8		8				
411	1001	THER -	10	-	ARTIN C	mana, -	881	981-	WHERE I	
	418	Acceleration and a second seco		0	him	and a	drife	64997		
	1010	Indial Image	-	0	2000	tion it.	204	source.	(1000)000000000000000000000000000000000	12040
		HIGH-REP FILMERED MERINE	-	1	(H)II	1008		04855	0000-00-10-10-10-00	
-	***	10000001 (1000-000) 000001 (00			Our .	anist	and .			
	-	HINNEY DOLLARS	-		1100	nose .		44887		130.000.00
	ait	Industry Indep	-			Artest	47.0	44881		1,2048.00
	418	TORNEY TORNEY		1		and a		44997	100000-10100-10	1.0.4870
	412	APPEND I Daniel		d'	108	nest	100			
and in case of	418	Contest live an	-	3	1.0	next	214	64535	and the second second	
	418	Tingent to.			21100		ane.	44997		12 44 24

工单详情界面展示工单标签、优先级、创建人、受理人、创建时间、更新时间、对象、详情、举证信息、 备注、历史记录等; 支持工单处置、指派、退回、关闭、编辑、删除、返回、查看上一条工单、下一条工 单。点击<**关闭**>、操作显示已完成。

关闭状态下的工单· 点击<**处置中**>·操作显示请处理; 支持举证信息跳转; 支持添加备注信息; 支持查看历史记录。如下图所示。



1118 (FER (FER			
		221 24 24 25 25 46 8	4 48 1 1
NE ST. NE ANTON S. ANTON SECOND	and a second state of the	Indian	
85  Not  United to the state of			Į
92 2019, 144 00000000- 0000, 0000000- 00000, 00000000- 00000, 00000000- 00000, 00000000-			
		0	
(0.4.5.7.7.4.4.7.7.5.8.4.8.0.1.		N.C.	
		S.	
imperior in the second second second		Sr.	
		Ň	
1010		0,	

2	、举	证信息跳轴	ŧ	
Ķ	5.击举	证信息下拉	边按钮· 支持跳转到不同页面。 详细请查看下表。	5
			S. S.	
	举证	E信息	跳转页面	
	攻击	话者 IP	<ul> <li>支持跳转:情报查询/安全告警查询/安全事件查询/原始日志查询/Sherlock/攻击者追踪溯源/资产威胁溯源。</li> <li>安全告警查询/安全事件查询/原始日志查询带条件: srcAddress:攻击者 IP+时间条件: 最近 30 天。</li> </ul>	<ul> <li>学研P</li> <li>秋田小学 WEB小学 医振行 20,19,4,3,443-11,25,17,661</li> <li>秋田都市</li> <li>192,168,11,139 -</li> <li>安全田部の</li> <li>特別近隣 60</li> <li>安全田部立員 60</li> <li>特別記景重調 60</li> <li>労助日市西面 60</li> <li>Sheltock 60</li> <li>秋田海道野潮遊 60</li> <li>香注</li> <li>商戸或納満課 60</li> </ul>
	资产	≖ IP	<ul> <li>支持跳转:情报查询/安全告警查询/安全事件查询/原始日志查询/Sherlock/攻击者追踪溯源/资产威胁溯源。</li> <li>安全告警查询/安全事件查询/原始日志查询带条件: srcAddress:资产 IP OR destAddress:资产 IP+时间条件: 最近 30 天。</li> </ul>	<ul> <li></li></ul>

安全告警 ID	<ul> <li>◆ 支持跳转到安全告警页面:</li> <li>◆ 查询条件: 指定安全告警事件 ID。跳转方式:新增页面。</li> <li>◆ 携带时间条件: 最近一年。</li> </ul>	
域名/URL	支持跳转: 情报查询/打开链接。	

#### 3、 备注

在备注框中填入相关信息,备注框支持贴图、插入链接、文字编辑等等操作。

支持附件上传·单个附件大小不可超过 20M·全部附件大小不可超过 50M·点击<提交>。

历史记录会保存备注信息。如下图所示。



## 4、 历史记录



工单编辑、备注提交都会保留相应的历史记录·历史记录可查看工单所有的变化及动态·也支持下载备注 提交的附件·默认正序。如下图所示。

NICE III	图 152 168 74 106 3018-00 42 14 45 48 进行了782 FI图/9
· (10)	12
00044	
n.exte	8 102 168 FZ 100 2019-00-12 19:04 47 3017 790 FWH
and	
h	
30	4-06-12 10.0000 720TH-06-12 120000 2015-06-12 120000 2015-06-12 1500000
6.22	
6 20 6(1)	A 102 106 74 100 3010-00 12 16 10 28 #F778FF88
+ 555	A 102 106.7 x 100 3019-00-12 10 1028 単行790F期内 M. 希望 R田白 教明
+ 110 + 111 + 111 + 111	A 100 106.74 100 3015-00-12 10 1028 #FF780FB89 N. #PP 0.B51 #FF N. #PP.244028 0.B13 #FF N. #PP.244028 0.B13 #FF780FB89
4 日7 8(日田12) • 日日1 • 王初 • 王初	A 100 106.74 100 3015-00-12 10 1028 #H778EFBBM M. #PP (2011) #PH M. #PP (2011) #PH M. #PP(2010) #EP(2010) #H778EFBBM M. #PP(2010) #PH 3008 \$EP(1) #2107 130 (003 300 (121 10 10 1))
<ul> <li>4 20</li> <li>6 20</li> <li>6 20</li> <li>7 20</li> <li>7 20</li> <li>6 55</li> </ul>	100 100 7 x 100 30 10 00 0 x 10 10 20 世日 790 F 100 10     10 7 x 100 30 10 10 10 20 世日 790 F 100 10     10 30 20 20 7 20 10 20 10 20 10 20 10 10 10 1     10 30 20 20 7 20 10 20 10 20 10 20 10 10 10 1     10 30 20 20 7 20 10 20 10 20 10 20 10 10 10 1     10 30 20 20 7 20 10 20 10 20 10 20 10 10 10 1     10 30 20 20 7 20 10 20 10 20 10 20 10 10 10 1
+ 100 + 0.00 + 2.00 + 2.00 + 5.00 + 555 K (0.000)	102 106.7 x 102 2019-00-12 10:1028 世行796 FBB19     16 通数2447.2 (2019) 2019-00-12 10:1028 世行796 FBB19     16 通数2447.2 (2019) 2019-2018 (2019) 2019 (2019) 10:10 (     16 2017) 2019 (2019) 2019 (2019) 2019 (2019) 10:10 (     16 2017) 2019 (2019) 2019 (2019) 2019 (2019) 10:10 (     16 2017) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019) 2019 (2019

## 5、 工单处置

点击<处理中/已解决/关闭>·可以改变工单状态为处理中/已解决/关闭。工单详情页面状态实时修改。如下图所示。

Contraction of the second seco	
en en energe. Alt levens Stat senta Stat senta	

## 6、 工单指派

点击<**指派**>·弹出指派工单框·可选择工单状态、组织架构、受理人、处置动作、填写备注·点击<**提交**>· 工单指派成功· 该工单受理人将会更新为最新指派的受理人。

如下图所示。

1 192 2 parties innie 2003	100 00 00 00 00 00 00 00 0
Mile	1996 1999 Jones Hann Alff. Bern anneysan



- ◆ 编辑: 点击<编辑>,进入到工单编辑页面,编辑页面可编辑主题、标签、优先级、受理人、对象、详情,再添加举证信息,举证信息支持输入攻击者 IP、资产 IP、安全告警 ID、域名/URL 等,点击<保存>即编辑成功,编辑操作会记录在工单详情页面历史记录中。
- ◆ 返回: 点击<返回>·可返回到"安全运营>工单管理"页面, 并会保留之前的查询条件。
- ◆ 删除: 点击<**删除**> · 删除当前工单 · 页面会自动切换到下一条工单详情页面 ·
- ◆ 上一条/下一条工单: 点击<**上一条/下一条工单**>,可切换上一条/下一条工单详情页面。

## 7.3.5 删除工单

选择"安全运营>工单管理"页面,工单列表中选择某一条工单点击<删除>,可删除该条工单。

点击工单列表上方<删除>支持批量删除工单。

如下图所示。

ACCN 2MER						X				
2848		20.000			1.00.000		- 100	2		
						S	.2.			
408	indian-	1410	48	414	MANY .	and i	1988	2004.1	-	
ARC HOUSE	014	REPORT, MILL	distant.		-		Cargent	ALCONT.	and of here is	1.0 militia
Del minis	818	TRANSIT (September 199	-	*	100	A298	STATE.	dealers .	0.000	10000
-		Distant Inc. and		*		and a	Jula	average 1	0000000	1.0 market
	81.8	Distance in the second					ate	10000		10,000
· ····	414	traine: (no-ime	1000		(C)	Arrest	3858	And Person	printed of the local	100400
	418	Distant line and	100		S.		ale.	10000		
	818	THERE IN A PARTY OF	1000		1	244)	218	ALC: NO.	1000 AUG 10 10 10	
a more thanks	817	Income Line and	1000	. (	- int	and a	818	autom:		1.04484
a recorded	41.5	1004482 Simeline	Contract of Contract		1.00	aleren .	818	10000	100000 40 10 10 10 10	1.0
-	818	TRADES Discovers	-	. 0	1.100	C nine (	mim.	44887	Accession in Advances	
weiter offer Stars	Desta	11.0		S		0.		- WITH - {	Section 18	186 9 18

# 7.3.6 批量处置工单

选择"安全运营>工单管理"页面, 勾选待处置的工单, 点击工单列表上方<处置>, 选择处置状态为未处 理/处理中/已解决/已关闭, 支持批量处置工单。

如下图所示。

	2.									
	0	199.5								
- 0										
L	4994	1428	48	474	MEAN -	mand 1	THEA .	888A.1	-	
	010	REPORT AND A	Contract of		1000	1.248	areas.	Average 1	and of here is	1.5 mg hts
mon	ect	Distance) ( Depending of the local distance)	-		1204	A298	00,027	And and a	0.000	10000
	818	11000001 [1000-00108 -	-		1148	and a	214	autom:	00000000	10000
	818	Distance in the second			1114		214	10000	000010717	
	414	trainet the sum	1000		1.00	Anna	214	august.	animative increase	10000
	418	Distance in the state	100		110		21e	ALC: NO.		100000
	#18	THEFT IN THE R. P. LEWIS CO., Name of Street, or other	1000		1.04		214	KOWEN .	100401000	
and a local data	818	180101 (04.00.0			1.00	1100	218	autom:	month of table in	1.2 44.04
the same set	415	TOWARD Downline			1.040		218	10002	10000 AD 10 10 AD 10	10000
_		(WETH) Dischold	-		100		mie.	44885	And in case of the local division of	

# 7.4 订阅规则



## 7.4.1 功能简介

选择"安全运营>订阅规则"页面,列表展示所有订阅规则条目。

订阅规则数据源为: 安全告警· 支持添加工单/预警/邮件/短信相关规则·当安全告警满足订阅规则时· 平 台对订阅规则通知人自动生成预警/工单、发送邮件/短信· 让用户可以实时关注到平台告警情况· 以便及时 作出防护措施。

## 7.4.2 查询订阅规则

订阅规则支持通知人、发送方式查询;点击重置清空所有查询条件。如下图所示。

ESEX UNH							
dame dament				0	BANCHER IN	an 102	
(a) (b)		#0) em-		- mail De			10 10
-			BALADHTAN				
3865.1	A854-1	REAL I	1.8911				-
10.00	0.0	1958, 2412, 1993, 4119, 574 5, 25	10	**	300000000	-	1.1
ACC MR	1.85	1958 2411 2515 4104 174 1, 91		J		1000	10.0
1.000		1978 8554 2023 8-29, 879 5, 80	- 10		399424775	-	1.10
And Dist.	38	10052, 2010, 2010, 2108, 179 5, 20	100004		constant of the second	-	1.1
				6			88.1

## 7.4.3 新增订阅规则

点击<新增>,弹出订阅规则新增窗口。

选择发送方式预警/工单/邮件/短信/钉钉; 选择通知人· 当发送方式为预警时· 无需选择通知人· 其他三种 方式均需要填写通知人。

配置过滤条件,点击<确定>,新增订阅规则成功。

如下图所示。

	- 9.812	5 <b>#</b>		_		** 48
	-	-	100-0			F
ANC -	191	APRIL 1	1000 C		anar	
and a state	- 1969	State (set) and set of the set		1.000		
				84 84		-



- ◆ 订阅规则发送方式为邮件或者短信时,订阅规则生效需至 "系统管理>推送管理>邮件服
   务器配置/短信服务器配置/钉钉服务器配置" 配置相关邮件服务器、短信服务器、钉钉服
   务器。
  - 订阅规则发送方式为工单或者预警时,无需配置服务器。
  - ▶ 订阅规则发送周期默认为 10 分钟, 如需调整订阅周期,请联系平台技术支持人员。

## 7.4.4 订阅规则其他操作

订阅规则支持编辑、删除操作; 点击操作栏<编辑>、<删除>等按钮即可。当订阅规则通知人用户没有配置 手机号、邮箱或者用户被平台删除时, 该情况下, 通知人无法正常接收订阅信息, 订阅规则条目会有异常 提示。如下图所示。

LOW DIMON				3			
classe limite				000			
ACRES IN COLUMN		(#91) 214		- Andre			** #
				×	2		
MAL.		-	4841	- 100° -	and and i	anar	
-	**	1988, 8810 2010, 0100 PTR 4, 85	10	a VIII S			14.14
an death		12008 April 2020 Augos 278 4.80		D' m C		-	(619
Longest	10	10008 3010 UNIO PIOS 274 4.80	+*	6 0	000000000000000000000000000000000000000	-	(#/#
Arrent	10	10808, 8210, 3930, Post, 878 0, 20	millio.	0, 47.	present in reserve		20.
					A48.1	(1)   HAR	OWN

# 7.4.5 订阅记录

选择"**安全运营>订阅规则>订阅记录**"页面,页面记录所有订阅信息发送情况,可以通过通知人、发送 方式、告警内容、时间范围查询订阅记录;也可以对订阅记录进行安全告警溯源。

如下图所示。

Contra 1	14.78	×0 0	(REAL PROPERTY OF A		
aniti,		Canal and	- (AARE)	- Dented Income	40 00
	865   88%	Hana -		28 - 96 - 1484 -	-
	118 11. 	Distance: Compare representation losses and Distances. Compare representation losses and Distances. Compare representations Distances. Compare rep		a ne avante avant	

## 7.5 绩效考核

## 7.5.1 功能简介

选择"安全运营>绩效考核"页面。通过工单处理情况、总资产数、风险资产数、风险概率等信息,对总



部及分部的工作行为及取得的工作业绩进行评估· 并运用评估结果对总部及分部的工作行为和业绩产生正面的引导。

## 7.5.2 查询绩效

可通过组织架构· 截止时间进行筛选和查询· 默认组织过滤框为空· 截止时间框为上周· 点击重置清空所 有查询条件·如下图所示。

A'LPHA							1
000F 8848		27.025					all and the second
lares		(a)+(a)		100			80 88
	BRANCE BUNT			MINISTRIA, 15. WARLS		. V	Butters Statute
00100	0024	Manual A		987529 (	1070.1		A686 -
00000		- H	3		1 25		
60.14	F	1.1	14 - C	14.			
22)+	C	002	18 - C	14 C	T'S	+	
					<u>~</u> ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		1 · · · · · · · · · ·

## 7.5.3 导出报告

◆ 点击 导出查写编集 按钮 · 导出历史截止时间的数据 · 导出文件格式为Excel · 如下图所示 ·

A.	1	Attack to the C	0	CP CP	+	- 6	H
	1		组织绩效考	複			
-			计道数位				
截止时间	2020-09-15 21:59:59			~			
			资料性单			- 77	10
用积余存	转办工师	酒苗24小时工单	蒙驁3日工单	委留7日工单	总资产数	风险资产数	月間数3
制运转研查	1	1		5		0	-
现小学	5			D.	100	0	1.0
<b>史艺小学</b>	a .	1	111	0	232	111	3%

◆ 点击 按钮 · 弹出弹框 · 可选择组织架构及截止时间 · 点击<**导出**> · 导出至截止时间过滤后 的组织架构的数据 · 导出文件格式为Excel · 如下图所示 ·

AILPHAIN		8- x <del>- x</del>				1
	and in nexus		-			1.44.1.44
		80.0				
man min		10.00 m to 10 m	-	-	5	
	1.0.7		Long Street			
ania C	- (AL 2		88 81			
						1001 883 140
	¢	p	Ē		G	
1 草藏运的提紧把构	有常义的截止时间	组织绩效率	橫			
2 3 <b>B J B J J D D D D D D D D D D</b>	27.00	过渡生存				
I DILLEIM  IOISCOLULE	17.10	医神经带				
5 和我私称 林み王( 6 あさ小学 5	第 委留24小时工事 3	掌管:日工单	索盤7日工単 3	总资产数	风能洪产数 0	风险数率

# 7.6 重大保障



## 7.6.1 功能简介

选择"安全运营>重大保障"页面,保障团队以"事前重在预案,事中在于保障,事后在于复盘"的思想, 在备战、临战、实战、战后复盘、结束各个阶段为活动的地区、应用和拓扑提供高质量的保障服务,确保 活动顺利进行。

## 7.6.2 新增重保任务

点击<新增>,进入到新增页面,输入基本信息、活动时间、保障团队、保障范围,点击<保存>,重保任务新增成功。

如下图所示。



## 7.6.3 管理重保任务

1、 统计信息

显示**已保障活动**(结束状态下的活动个数)、 **正在保障活动**(实战状态及复盘状态下的活动个数)、即将保 障活动(临战状态下的活动个数)·如下图所示。



#### 2、 查询过滤



支持任务名称, 保障阶段选择过滤, 点击<重置>, 清空查询条件, 如下图所示。

COST MARK			
· 1982 - 1 1982 - 1 1983			
lands and bland	500 K	- 200 cm-1	

#### 3、 列表内容

列表内容包括: 任务名称、活动时间、任务阶段、待办工单数、已处理工单数、保障组长、创建时间、发 布大屏、操作栏。

各任务阶段的操作不尽相同, 备战: 上传预案; 临战: AI 异常, 保障拓扑, 安全告警, 下载预案, 创建预警, 创建工单; 实战:同临战; 战后复盘:保障拓扑,下载预案, 上传保障报告; 结束:同战后复盘。 详情见下图。



## 7.6.4 编辑重保任务

任务列表中选择某一条重保任务点击<编辑>,进入到编辑页面,编辑页面可基本信息、活动时间、保障团队、保障范围,点击<保存>即编辑成功,如下图所示。





# 7.6.5 查看重保任务

任务列表中选择某一条重保任务点击<查看>,跳转到该任务的重保大屏如下图所示。



# 7.6.6 删除重保任务

任务列表中选择某一条重保任务点击<删除>,可删除该条任务,如下图所示。

Design of Des								
		200.0	(C)		1812			
				o`				
100.00		S game		0083368.1	2000 L	Common C	- 14	-
	000000000000000000000000000000000000000	- 1		1	11		•	
49,40,70		()	-Q1°			20.010.000	•	
		1 miles	0,		10	1000 Aug - 17 (4) 47 (4)	100	-
AND REAL PROPERTY.	annersen i	A.	Y	1.4	36		100	
100.002		9= /	0	1.87		100000000000000000000000000000000000000	- 12	-
10,000	Revenue	-	<b>?</b> ,	(+)		and the second s		
ani, mi ini	manute				-10	printer of shift of	12	-
40.00	- Andrew .	-	à.		34	(10) - 10 - 10 - 10 - 10	128	-
***.240.25	and a state of the		14	5.65	10	1000-0011-0010		
Concern	* Sedenman					1000 (0.07 (0.07 M)	0	-


# 7.6.7 态势感知重保大屏预览入口

**态势感知**页面也支持重保大屏预览,如下图所示。







# 8.1 资产管理

# 8.1.1 功能简介

选择"资产管理>资产管理"界面,展示接入的资产类型和数量,对资产进行统一运维、监控、管理、联动。角色类型为分部安全管理员及分部安服人员的用户仅支持查看其所属组织架构下安全域的资产,不支持操作。

# 8.1.2 页面布局

资产管理页面布局如下图所示, 在资产列表区有两种展示模式: 列表模式和缩略图模式。

#### 列表模式

N. MARKE					1. 3								
**** 1	-	R*85		1	520	ATHE	824			2 [		-	123
DIS*0 SWSTIR				2	Si in		~	100	170	98. (	-	0	0
解离选*(0) 指数*(1)		RPER -	Report.	NER	нея	4010		(998)			==		
No. of Concession, Name				2				8.11	10.1				
Updament.		162 768 84 10	HAD THE AND TO	theft	(CRAMBER (1) (C))	# 31		His .	0.001	+ 4	1.	•	Ŧ.
244								8.18	46.4				
					C.			8.1	4. 1				
W120		1 MP1	10000 AJ 54	421	- HE -	13.79		푸님 :===	( e. )	-14		- 1	4.
PR-91					S			£-1	. 41.1				
		Contraction and						RII.	(a - 1				
++++		二、共活和第1111	A REAL	.418.	RATEHINE	+		m	2.53	+ 1	(#	•	11
					2 2			8.8					
185825		1.11	Constant Constant	1.000	3			R. 44					
4日有社に第17471日		evitia.	(4194)	- HIE CA	WHERE RECEIPTING COMPL			PUT	0.001	X		•	10
SACSING BON, LICENCE, CO.								8.4	10.1				
100-0A/h		10000						St 44	1.80.8				
NUL CONTRACTOR		- wartzo	O'ann.	1941	WARDER AND CONTRACTOR			#113	1.001			•	н.
			7	25				6.4	1.8.8.1				
2108		197257						We want	1911				
OCCUPANT.		- marter -	THEFT	Car	Annal Part of Court			#1.4 E	411				н.
								B() 0					
27281								W 1 44	1411-1				
			1234	1.1	MANTERSON (must )			41.10	0.2281			-	83
		0.3							1.8.9				
NOT NOT		202		4102	China Sector (1997)			8.1	1.50				
	1.0	114	000.000.041111		Territoria (11)				1.22	2.0	•	51	10
400 - 16(840)		1. Co						8.1	120				
190 THE GODE H				833					1.0		6337		
- mentioned		antity	140.144.2.5	10.01	And the part of the second sec	M018		91) W.S.	1.79.7	2.1		•	AU .

缩略图模式



Contraction of the second s						
8798. A	MT44	100 A	2	8788 erer	<ol> <li>(a)</li> </ol>	88.1-
			1		888* 30 St.	0 G
ARTIN ARTIN	C 402.000.00 (0		Care,		- A	
ALBOM YOU	ALLAN ALLAN	88 10.08	1048 8028	AU 1004	NO SILLE OF	1000
+++	0			8 8 (	0 0	
800 80%	879 0 8782 25 87881 0 87881 0		5"7 2222 8"52 0" 8"591 23 808 565	3		
and the second s	BILL.		1972 A	<b>9</b>	JO HEA	
ESTERATION (1000,100)	and the		- ertii	arter 100		
(1)	way while	44. 1019		## #INH	ny mility an	+10.00
4448			0 0 0			
042888	849. (1		-	. V	100 LUIN 100	
1/101	Bridd on	(1787) 1 (B   (off))	ATES AVERTIC	#(set) () ·	RPER (moldRead) and (	
141	87891. 43		aren an		8/18/21 - 2.0	
Maximum .	BILA.		8414		BHA.	

资产管理页面布局序号说明参见下表。

序号	名称	· 说明
1	快速查询菜单	以不同的角度提供了资产管理快速查询功能, 方便用户根据实际需要进行查询。分为资产状态、安全域、资产类型、安全设备、资产重要性、网段分类等。
2	查询区	显示查询条件及< <b>查询</b> >、 < <b>重置</b> >按钮。 查询条件:资产名称、资产 IP、资产标签。
		高级查询 · 资产类型、资产来源、 EDR 防护状态。
		该区域主要用于资产信息展示以及相关功能的操作。
3	资产列表	功能操作: 删除、新增资产、导入、导出、资产同步、设置、投屏。
		资产信息展示: 列表模式、缩略图模式。

# 8.1.3 资产新增、编辑、修改

1、 资产新增

点击 新增产 按钮,打开新增资产页面。新增资产页面包括基本信息、更多信息、操作系统信息、设备管理、流量监控。

基本信息



资产 IP 与资产名称为必填项 · 资产类型下拉选择 · 资产重要性有普通 · 重要 · 资产标签和资产类型按需填 写 · 如下图所示 ·

* 潮产IP」	SHEAR STOR		• 遗产名称:	是最大进产出作		
资产类型:	NE/NE	×100	依严继要性:	音道		2
					0	
			1200			
资产标图:	10101011011/001		責任人主	司官人主任人		

#### 更多信息

更多信息包括资产编号、资产状态、使用人、 C-机密性、 I-完整性、 A-可用性、是否是等保资产、地理 位置、描述等。如下图所示。

统产编号;	IBNEX.ND/HAREE		· 出产状态;	他用中	Ŷ
使用人:	Marxiella.			+	÷
1-克整性:	+		ATTRE	₩ 	
皇帝皇峰保密#1	e	. 50	田田行屋	864	-
<b>第</b> 西:	indo.terme	B	S		

### 操作系统信息

操作系统信息包括操作系统、 OS 版本、 MAC 地址,如下图所示。

桑作系统信息	No.	0		
当作系统:	and the second	$\sim$	08版本: 明治人(	1068
MAC地址: 《	Sala NAGIMU			
. 6				

#### ◆ 设备管理 🛛

设备管理包括设备厂商、设备型号、设备版本、设备存放地址、管理地址、日志量监控、在线状态检测、 处置联动(见处置联动模块)。如下图所示。

1822					CONTRACTOR CONTRACTOR CONTRACTOR
10.0	100	5	0401	40.000	2. 新聞東古語大術人口工。 (1.1)東京的陶醉作品。 (1.1)東西市特別 1. 学家会会家庭、日本東美的陶醉方白
1991			-	And an other states of the second states of the sec	
1201	0.0				
Comp.	10				
	•	ADA (10 + ) (1000			

◆ 流量管控



流量管控包括流量监控、开放端口监控、主动外连行为监控。如下图所示。

AAMAN [		Ð					1、 (1917-1947年), 《聖堂太行(1949年)) 2、 (1944年), 「1979年), 《建築社会(1948年)) 3、 (1949年), 不是世行任任、王建立(1948年)(1931	
	- 0	Ð.,	*****		APRIL 1			
111-07	-	D	*****	-				

#### 2、 资产编辑

点击 按钮, 打开编辑资产页面, 显示资产来源、更新时间、安全域、安全设备、 Web 业务系统。编辑相关信息, 最后保存。如下图所示。

11148.	10.0141		print to the second sec		2.	
11110	Aug.	1110	at some of		XII.	
****	and the second s					
1.219		1.0798	100 pt 8 k av 1 march 1 1 7 (1) a		2	
1792	10.00	073051	18 · ·			
1112	Access of	401	441411	*		
12.0						
1140	10.01	0.00	aller v			
-	(The second s	1489	· 2.	St	in the second se	
- 100		- 1780		Nº (		
118801-		-	(en	6. 5		
89.	100 ( T 100)			o ji	)	
-			. 5			

#### 3、 资产删除

点击 按钮 · 即可删除该资产 · 关联安全设备和Web 业务系统的资产不能被删除 ·

资产可以批量删除; 列表模式勾选全选框,可删除查询结果所有。

# 8.1.4 资产导入和导出

1、 资产导入

点击 数 按钮, 弹出导入资产弹框。如下图所示。资产导入分为资产增量导入和资产替换导入:

- ◆ 资产增量导入:当出现资产重名后 IP 相同时,不能保存。
- ◆ 资产替换导入:当出现资产重名后 IP 相同时,保留最新导入的资产。



导入资产			$\times$
* 文件上传:	未选择任何文件	选择文件	螺旋下载
	● 资产増量导入 ○ 资产替担	续导入	
● CSV文件采 隔)" 格式。	用UTF-8编码,如果使用Excet编辑	重,请在保存时选择 "CSV L	JTF-8(道萼分
		取消	
			L.
共资产批量	导出功能。		5
<del>,</del>			
		*** C	
可对探针	- 的所有资产信息即网络	各内部的资产信息讲	持同步。 Se

## 2、 资产导出

点击⁹¹¹按钮, 提供资产批量导出功能。

# 8.1.5 SOC 同步

点击 按钮 · 可对探针上的所有资产信息即网络内部的资产信息进行同步 · SOC 同步需要在设置中 50 mining 开启 SOC 资产同步按钮。

# 8.1.6 设置

点击 * 按钮· 弹出资产设置页面。如下图所示。

质产设置	2 S. *
常用设置	
are a	
	A 🖸 NARE 🚰 # 3.58 77.58 36.68 # 85.5 77.89
	(1) 图书书: 图 图 CD 和
SOCHET BE	
EDRIE!" RI	き (周田) 足さをの内法アッド 10 50 2,50
二月 二	
	E: RIE
* 11200	1 🖸 RG8 🖸 45M
2RE	机: 安全城 - 安全域距离
* 安全	Not · DELR · REA · DAVE · FIPSREES ·
	电信频表示 》 我们就通讯员 《 华力员 》 读就员 * "
<b>按照</b> 在 • 安全:	<ul> <li>第二 安全城 - 安全地図</li> <li>第二 安全城 - 安全地図</li> <li>第41 1961 × 卫生局 × 服務務 × DM27区 × FTP文件設務務 × 电信号地方 × 計工取造元方 × お力方 × 流発方 × 例用物理分方 × 副子 第三氏 × 阿雷云 ×</li> </ul>
	桃豆 和前



1、常用设置

◆ 资产评分

资产评分开启, 对资产进行评分计算。

字段显示

字段显示最多只能勾选 5 个 · 资产评分勾选框置灰 · 不可以勾选。开启 EDR 资产同步且 EDR 设备连接成 功时 EDR 防护状态可勾选。

♦ SOC 资产同步

SOC 资产同步启用·系统定时进行资产同步·也可以手动同步; SOC 资产同步禁用·资产不会同步。

◆ EDR 资产同步

EDR 资产同步启用 · 系统 5 分钟进行资产自动同步 · 未添加联动 EDR 资产时 · 提示 "系统未配置联动 EDR 资产 · EDR 资产同步不生效" ·

EDR 资产可在资产管理界面添加·资产类型选择 "安全类/主机安全管理系统(EDR)"·设备厂商选择 "安恒(DBAPPSecurity)"· 管理地址填写·勾选是否联动 EDR。

如下图所示。

设备厂商;	空間(DBAPPSecunty)	0 .	2 (2#19)	BRARRE (P	
设制版本:	UNKASSEHIT	20°	设备存在地址;	INA REPUBLI	
智理地址;	🚛 🐨 🚛	92 169 64 10		■最高額動EOR	
	ter X	37 -			新記

2、 流量自动发现资产

◆ 自动发现

自用自动发现 满足发现类型与发现区域的资产会被发现。 关闭自动发现 资产发现立即关闭。

### 发现类型

发现类型包括服务器和终端。

## ◆ 发现区域

发现区域分为安全域、内网、网段。



如下图所示。

发现区域:	安全域 💌 安全域配置	
* 安全域:	诸远峰	Sol
	局城网	al i
	3.2.1	.~

● 内网:点击 按钮·跳转至"系统管理>配置管理"界面· 可根据需求配置内部 IP。

如下图所示。

	St St
发现区域:	内网 • 内网配置
	确定 取消

• 网段: 点击 #### 按钮,可根据需求配置 IP 区间。如下图所示。

发现区域:	网般	and the second			
* IP区间:	添加网的				
.5	确定	取消			

8.1.7 投屏

- ◆ 点击 🖵 按钮投屏至 "**态势感知>资产态势感知**"大屏。
- ◆ 点击 🕐 按钮, 跳转至"**威胁感知>Sherlock**"页面。
- ◆ 点击 💌 按钮 · 跳转至"**态势感知>资产威胁溯源**"大屏。



# 8.2 Web 业务系统

# 8.2.1 功能简介

选择 "资产管理>Web 业务系统"界面, 对Web 业务系统进行统一运维、监控、管理、联动。角色类型为分部安全管理员及分部安服人员的用户仅支持查看其所属组织架构的Web 业务系统,不支持操作。

# 8.2.2 页面布局

Web 业务系统页面布局如下图所示。

其中系统列表区域有两种展示模式, 一种是列表模式, 一种是缩略图模式

THE WEDGERSON				2			
系统出行	10.0	955 mb/6	**	BRATE ADDRESS		87 5	23
B/H - =			Ž	C. REALERER	RA 80	0	4
原換名称 :	1883 1		*##31*	6)	原作		
RM	www.tail.com	Ő	í.	5	/ 1 +	9. (P)	
94.009	3333	S	J.			а: <i>#</i> .	
			S	#26 ( )	10 张/元 - 1	8¥ 1	
Biangow III		S a	8				
sean.	164		*	artista anti-		85 83	
		2 5		Reproduction and	0.0	0	Ģ
向 网站	- 21	a oa.com					
www.ca.com		Ceda					
			··· 1-				
1元前型: 第:1	HIN AND TH	19 1 1 1 1 1 1 1	≝: ¢				
9 ##88 / 16	8806 - 4983	o Mada / / Jotas / a	5(\$1)				
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~						
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~			#28 ( ) ( )	10.0/2 - 2		
					17 HUR 3-11 H	10.00	

Web 业务系统页面布局序号说明参见下表。

序号	名称	说明
1	本沟区	显示查询条件及< <b>查询</b> >、 < <b>重置</b> >按钮。
1	查明区	查询条件: 系统名称、域名、标签、组织架构。



序号	名称	说明
2	操作	模式切换 • • • (列表模式、缩略图模式)、 <b>《新增 Web 业务系统</b> 》、 <b>《导入》、 《导</b> 出》、 <b>《设置</b> 》、 <b>《投屏</b> 》。
3	Web 业务	该区域主要用于 Web 业务系统信息展示以及相关功能的操作。
	系统列表	资产信息展示: 列表模式、缩略图模式。
3.2.3 <b>V</b>	Veb 业务	系统新增、编辑、修改
· Web ⊻	业务系统新增	
点击 ^{新增W}	eb业务系统 按银	田· 打开新增 Web 业务系统页面。
如下图所词	ج	A ST LOS

# 8.2.3 Web 业务系统新增、编辑、修改

#### 1、 Web 业务系统新增

如下图所示。

Bitter:	NLABES:		Andrew Segretaria	
系统装载: 10		0 2	7	
	and the state of t	五份服務性	普通	. w.
系统S茎: 2		Ditt	1966.), #15.),	
itilitette 👩	D http://www.sas	è.		
规构	6			
道桥: 11				编辑组织常校
梁梅				
开发圈: 💷		<b>系统版本</b> :	446.) \$058.5	
RANG:	Reservation of the second s	服务组件版本:	用他人服用组织描述	
G	Anweighter	Web臨腸版本:	and A Web Web 2013	

## 基本信息

域名、系统名称为必填项,系统类型默认 Web 业务系统;系统重要性下拉普通、重要;系统标签、责任人 非必填。访问地址默认开启支持 http 与https,默认将域名赋值给访问地址,也可以填写其它。



## 组织架构

组织架构为用户自定义组织,可在"资产管理>组织架构"配置。

#### 系统架构

系统架构包括开发商、系统版本、技术架构、服务组件版本、 Web 容器名称、 Web 容器版本。

#### 更多信息

更多信息包括系统编号、系统状态、使用人、 C-机密性、 I-完整性、 A-可用性、是否是等保系统、地理位置、描述等。如下图所示。

更多信息				
重统编号:	制成人名法格芬		系统状态: 使用中	×.
使用人:	制成入标用人		C-机器性	(w)
1-地震的 1	Φ.	~	A留用性: 中 5	×
商资基等 <b>存</b> 系统:	<del>.</del>	. •		(M)
描述:	IDNE A JURI S			
		5		

## 关联信息

关联信息包括子域名、关联资产。关联资产分为前置机、负载均衡、数据库、 CDN、其他。资产下拉显示 当前系统最新的 100 个资产。如下图所示。



流量监控包括流量监控和访问成功率监控。流量监控强制开启,不可关闭。如下图所示。

逸聞曾控				
远最监控:				
动尚成功重编榜:	πO	成功率資值:	80	

2、 Web 业务系统编辑



列表模式点击操作列,按钮,缩略图鼠标上移点击,按钮,打开编辑 Web 业务系统页面,显示系统来源、更新时间。如下图所示。

派兵中道: [本仙皇	人工業人		更新时期;	2020-12-28 10:39:08		
• #8:	FIRE DE CERT		系统名称:	网站		
sisan.			16 E B 14		6	
					d	
系统招告	805959		傳任人:	主席	A.	
101551	FC 140 - 1	60.000		(	Q.	
把架构				Ś	V	
1019:	LDAP			Nj.	. w.	\$5000
<b>I统架构</b>				8		
开发用:	dad./#3194480		系统版本:	and a second		
10.000	inst, c.m.+ statution@iff.st	810	·但何能本:	A THINGTHE		
1				V.C.		
110409-07:	Electronic and a second	9740	HARDE	Day ( marting B		
多信息			Ô.			
<b>新改编句</b> :	BE-XHAY		C States		<u>₹</u>	
表用人:	EMA-DEA		2.机速性:	ŧ		
1.85%	¢.	- S.	A-17/Hitts	)#.		
CARGES IN	т. Т.	S	BUNER	367638	(a)	
		000	0			
用语:						
	0,	ŝ.				
現估慮		J.				
子城寨。	EU .C					
天教资产。						
建氰酸烃	No.					
言葉協力						
A LEGISTIC MARKED A	成功主義通:					
D-J-MODELET-						

## 3、 Web 业务系统删除

列表模式点击操作列 [•] 按钮,缩略图模式鼠标上移点击右上角 [•] 按钮,即可删除该 Web 业务系统。资 产可以批量删除;列表模式勾选全选框,可删除查询结果所有。



# 8.2.4 Web 业务系统导入和导出

### 1、 Web 业务系统导入

点击 争入 按钮 · 弹出导入 Web 业务系统页面 · 如下图所示。

Web 业务系统导入分为 Web 业务系统增量导入和 Web 业务系统替换导入:

- ◆ Web 业务系统增量导入: 当出现资产 IP 相同时,不能保存。
- ◆ Web 业务系统替换导入: 当出现资产 IP 相同时,保留最新导入的资产

导入Web业务	系统	in the second seco	<b>5</b>
* 文件上传:	<b></b>	读择文件	提版下载
● CSV文件采 稿)" 格式。	● Web业务系统增量导入 用UTF-8编码,如果使用Excel编辑	Web业务系统替接导入 5. 储在保存时选择 "CSV	UTF-8(這号分
	Ő		

## 2、 Web 业务系统导出

点击 ⁹世 按钮 · 提供 Web 业务系统批量导出功能

# 8.2.5 设置

点击 * 按钮 · 打开 Web 业务系统设置页面。如下图所示。

Web业务系统设置		
自动发现:	(ĦC)	
发现区域:	安全域 * 安全域配置	
* 发现美型:	2 访问城省 🗌 访问师和通口	
• 安全域:	请远端	÷
确定	取洞	

## 自动发现

自动发现出厂默认禁用 · 启用后自动发现满足发现区域和发现类型的 Web 业务系统。关闭自动发现 · 那么 Web 业务系统自动发现功能立即关闭。

◆ 发现区域

发现区域分为安全域和内网。

Web业务系统设置	SV.
自动发现:	· · · · · · · · · · · · · · · · · · ·
发现区域:	安全城 🔻 安全城配置
* 发现关型:	
* 安全域:	
确定	局域网 32.1

内网: 点击 按钮 · 跳转至 "系统管理→配置管理"界面 · 可根据需求配置内部 IP · 如下图所

₹ °

自动设有			
III WLOCH	2000		
发现区域		内岡配書	
Ĩ,		3 T 2 PROLES	
、安安現実型	: 🔽 访问域名 🗌 访问(	P\$D#C	
C			

发现类型

发现类型包括访问域名和访问 IP 和端口。

# 8.2.6 投屏

◆ 点击 🔍 按钮投屏至 "**态势感知>Web 业务系统态势**"大屏。



点击 按钮 · 跳转至对应的 Web 业务系统的"态势感知>资产威胁溯源"大屏。

STOTE Webrits State



投屏说明见下表。

序号	名称	说明
1	投屏	投屏至 " <b>态势感知&gt;Web 业务系统态势</b> "大屏。
2	投屏演示	投屏至该系统 " <b>态势感知≻Web 业务系统态势</b> "大屏。



3	安全告警	该系统关联资产,显示安全告警按钮,点击跳转到"安全分析>Investigation>安全告警"页面。 该系统不关联资产,不显示<安全告警>按钮。
4	原始日志	点击跳转至" <b>安全分析&gt;Investigation&gt;原始日志</b> "页面。
5	访问系统	该系统开启访问地址,显示< <b>访问系统</b> >按钮,点击新打开配置地址。 该系统关闭访问地址,不显示< <b>访问系统</b> >按钮。
6	资产管理	该系统关联资产·显示 <b>&lt;资产管理&gt;</b> 按钮·点击跳转到 <b>资产管理</b> 界面。 该系统不关联资产·不显示 <b>&lt;资产管理&gt;</b> 按钮。

# 8.3 安全设备

# 8.3.1 功能简介

# 8.3.2 页面布局

安全设备页面布局如下图所示。

择"	资产管理	▶安全设	<b>备</b> "界面	面, 对安全设备	备进行统一运	维、监控、管理。		
.3.2					456 05	CUTI IIII		
王反首	È火山巾 ≌≹®≋	同知下含		640		5		
0.850	and some of			ingenti ana	20	BBLM REVINGE	- 25 3	
-	H Bib			Q	Si		NEGS LEVA	4
	2987 :	REFA	设备关型	ARRY	6		#在	
10	0159386 1999	945(DEAH) Security(	200000	O O			<ul> <li>(ii)</li> </ul>	
100	来@128月31	Security)	823633 W1536	GIRLING			2	
q.	wataxe	≅tBOBAPP Seculty)	安全制以4日 11月8月入第 1964月	. S			$\left( \mathbf{S}_{i}\left( \mathbf{s}\right) \left( \mathbf{s}\right) \left( \mathbf{s}\right) \left( \mathbf{s}\right) \left( \mathbf{s}\right) \left( \mathbf{s}\right) \right)$	-
0	深信核上网行 为管理	RISRISAN GFOR	STER-LR CONSIDER				2 B (0)	
111	1800234	Ratili Topes	destairti-					
10	Redrict	PERMANAGERARY ACT	安全国/下— 中国大城				× • 11	
1	品结菌药的火 相	all would be	安全的下一 1930.0周				2 1 0	
50	sellinos - C	Stilliosanin Becurb/i	安全的(主所 유소학변화)동 (EOR)	(111)			2.4.4.4	
G	DY: ACM	#18(DEAP# Tecurity)	安全国/下一 代初大編					
-01	母亲日衣淑计 平台	9년(DBAPP Security)	安全時日志 東行製紙				2 0 16	





安全设备页面布局序号说明参见下表。

序号	名称	说明
1	查询区	显示查询条件及< <b>查询</b> >、 < <b>重置</b> >按钮。查询条件: 设备名称、设备类型、设备 厂商。
2	操作	模式切换 • • • (列表模式、缩略图模式)、< <b>新增设备</b> >、< <b>处置联动</b> >、< <b>投屏</b> >。
	19	该区域主要用于安全设备信息展示以及相关功能的操作。
		资产信息展示: 列表模式、缩略图模式。
3	安全设备列表	列表模式:显示设备名称、设备厂商、设备类型、关联资产、操作。
		缩略图模式:显示设备名称、本日日志数、关联资产、设备状态(根据资产管理 界面在线状态检测获取设备状态·未关联资产显示未检测)、日志量。



# 8.3.3 安全设备新增、编辑、删除

## 1、 安全设备新增

点击 ^{新国设备} 按钮, 打开新增页面,如下图。

<ul> <li>Ball Sheen</li> </ul>	用 · · · · · · · · · · · · · · · · · · ·	
anwasan b	<	
8 👔		ġ.
a anti-matrix		
0500 W500		, ŚŚ

设备名称、设备类型、设备厂商为必填项。满足设备类型和设备厂商的资产才能被关联,一个安全设备可 以关联多个资产,同一个资产只能被一个安全设备关联。

### 2、 安全设备编辑

列表模式点击操作列 / 按钮,缩略图鼠标上移点击 / 按钮,打开修改页面。

如下图所示。

基本值担		<u> </u>		
+ (0&&5);	*TellBanni	Záreji Zann v mace Bolles	14	
* 2992	安全時()問題在附设會	+12#/ # #15,084PPSecuth)		
2935				
絕世	STREAMARNAN AND AND AND AND AND AND AND AND AND	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	全市重要全分析。 但沈晨常常道的是	
他就说严	Will State			
80				

3、 安全设备删除

列表模式点击操作列 [•] 按钮 · 缩略图模式鼠标上移点击右上角 [•] 按钮 · 即可删除该安全设备。安全设备 可以批量删除。



# 8.3.4 投屏

安全设备可以通过投屏功能在大屏展示安全设备的安全态势。



## 投屏说明见下表。

序号	名称	说明
1	日志检索	跳转至该系统"安全分析>Investigation>日志检索"页面。
2	管理界面	<ul> <li>◆ 该安全设备关联资产的("设备管理&gt;管理地址")开启 ·显示按钮 ·点击新打开配置地址。</li> <li>◆ 该安全设备不关联资产或资产的("设备管理&gt;管理地址")关闭 ·不显示按钮。</li> </ul>
3	处置联动	跳转至"资产管理>处置联动"页面·带入该安全设备。
4	投屏演示	<ul> <li>◆ 安全设备资产类型为安全类/Web 应用防火墙 · 点击跳转至 WAF 监控安全态势。</li> <li>◆ 安全设备资产类型为安全类/APT · 点击跳转至 APT 监控安全态势。</li> <li>◆ 安全设备资产类型为安全类/数据库审计系统 · 点击跳转至数据库安全分析智能 平台。</li> </ul>
5	资产管理	◆ 该安全设备关联资产,显示资产管理按钮,点击跳转到 <b>资产管理</b> 界面。

序号	名称	说明
		◆ 该安全设备不关联资产,不显示< <b>资产管理</b> >按钮。
6	处置联动	点击跳转至" <b>资产管理&gt;处置联动"</b> 页面。
7	投屏	投屏至 " <b>态势感知&gt;平台运行状态检测"</b> 大屏。

# 8.3.5 APT 大屏

APT 监控安全态势大屏实时统计分析当天 APT 设备, 包括攻击源 IP 排行、攻击来源区域分布、攻击目标 排名、被攻击目标数、累计攻击者、攻击路线、详细攻击信息、告警统计、告警趋势、告警类型分布等数 据。 APT 大屏如下图所示:

A&LPHA APIG	探察全部教			1					3
ANY RECEIPTORY DET 2. Name TREMAINTS 2. Name TREMAINTS 3. Name TREMAINTS 3. Name TREMAINTS 3. Name TREMAINTS 3. Name TREMAINTS	50%2 34236 3141 1205 50%	545 541	1		7		ANY BITHINIT (1965 ANN ANN ANN		500 8800 800
								19694 10794 2020-0	
NO.2312110744           INV.NA.11.211           INV.NA.11.211	1810 1810 1810 1810 1810 1810 1801	2005-09-04 34555.00 2005-09-04 34555.00 2005-09-04 345550.00 2005-09-04 3455400 2005-09-04 3455400 2005-09-04 3455400	 197, 546, 198, 244 197, 546, 198, 244	PRI 144.3 YE 245 TRI 144.3 YE 245 TRI 144.1 271 TRI 144.1 271 TRI 144.2 TRI 145 TRI 144.2 TRI 145 TRI 144.2 TRI 155	Annual annous Annual annous Annual annous Annual annous Barton Bart	1.00 1.00 1.00 1.00 1.00 1.00 1.00 1.00			Mary ( ) and Parket St. Strategy ( ) States of ( ) States of ( ) ( ) St +

以下各区块均实时展示当天数据。

区块	说明	详细
攻击源 IP 排行	默认展示时间范围内攻击次数最多的 5 个 IP 及对应攻击量 · 点击更多显示 Top100;点击跳 转至攻击者追踪溯源界面。	



区块	说明	详细
攻击来源区域分布	默认展示时间范围内攻击来源区域Top10。	
攻击目标排名	默认展示时间范围内攻击目标排名 Top5 及对 应被攻击量·点击更多显示 Top100。	
被攻击者目标数/累 计攻击者	显示该设备被攻击者目标数/累计攻击者。	被攻击者目标数 <b>545</b> 累计攻击者 <b>541</b>
攻击路线	实时展示攻击路线· 根据经纬度显示最近 20 条。	
当天详细攻击信息	<ul> <li>◆ 展示当天最近 50 条详细攻击信息。</li> <li>◆ 当没有告警事件发生时 · 该区块不展示内容。</li> </ul>	



区块	说明	详细
告警统计	<ul> <li>共发现告警数。</li> <li>恶意文件数:点击可下载报告。</li> <li>高危: 威胁等级[7 to 10]。</li> <li>中危: 威胁等级[4 to 6]。</li> <li>低危: 威胁等级[0 to 3]。</li> </ul>	
告警趋势	<ul> <li>关联1个资产,显示统计时间范围内告警 趋势。</li> <li>关联多个资产时,轮播显示统计时间范围 内告警趋势。</li> </ul>	
告警类型分布	南丁格尔玫瑰图显示时间范围内告警类型的 Top10。	<ul> <li>         ・ 新会報告報告報告報告報告報告報告報告報告報告報告報告報告報告報告報告報告報告報告</li></ul>
APT 资产	APT 资产可选多个 · 也可选单个 ·	APT资产: 10.16.10.38, 192 168 3 3 APT 10.16.10.38 192.168.30.57



区块	说明	详细
时间范围	时间范围可选: 最近 24 小时、最近 7 天、最近 30 天、本日、本周、本月。	时间范围:最近7天 最近24小时 最近7天 最近30天 本日 本周 本月

# 8.3.6 WAF 大屏

WAF 监控安全态势大屏实时统计分析当天 WAF 设备 · 包括攻击源 IP 排行、攻击来源区域分布、被攻击站 点排行、被攻击站点数、累计攻击者、攻击路线、详细攻击信息、告警统计、告警趋势、告警类型分布等 数据。如下图所示。

	空交全市外							Ø
10/00000000000     10/000000     10/000000     10/00000     10/00000     10/0000     10/0000     10/0000     10/0000     10/0000     10/0000     10/0000     10/0000	232 58 1 1 6	1854 1854 1861		1				AW 告報(6)) ・1055 Mill 2770 あたまた。 4055 Mill 2770 単約5年 年高 2770 単約5年 年高 2770 単約5年 年高 2770 単約5年 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の55 単の5 単の
	ra + 44 + 144							1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1         1
1111400	290							## 告告典型分布
TELECAR DALBALLI ZZZIMALLI DILJENS	10 8 8 1	2009-09-04 18.29-04 2009-09-04 18.29-04 2009-09-04 18.29-04 2009-09-04 18.29-04 2009-09-04 18.29-04 2009-09-04 18.29-04	11111	9875 94295346138 9875 9875 9875 9875	10.1940/03 10.1940/03 10.1940/05 10.1940/05 10.1940/05 10.1940/05	ADALAN ADALAN ADALAN ADALAN ADALAN	****	2 2000 2 10120 2 10224 bit a 10121 2014 10 1 1012

以下各区块均实时展示当天数据。

区块	说明	详细
攻击源 IP 排行	默认展示时间范围内攻击次数最多的 5 个 IP 及对应攻击量 · 点击更多显示 Top100;点击跳 转至攻击者追踪溯源界面。	



区块	说明	详细
攻击来源区域分布	默认展示时间范围内攻击来源区域Top10。	
被攻击站点排行	默认展示时间范围内被攻击站点 Top5 及对应 被攻击量 · 点击更多显示 Top100;点击跳转至 该站点的 WAF 监控安全态势大屏。	建築主動連邦行     290       10.190.093     290       153.0436     10       153.0436     10       153.0431     8       101.76.05     7
被攻击站点数/累计 攻击者	显示该设备被攻击站点数/累计攻击者。	被攻击站点数 <b>1854</b> 累计攻击者 <b>1851</b>
攻击路线	实时展示攻击路线·根据经纬度显示最近 20 条。	
当天详细攻击信息	<ul> <li>展示当天最近 50 条详细攻击信息。</li> <li>当没有告警事件发生时,该区块不展示内容。</li> </ul>	
告警统计	<ul> <li>◆ 总告警数</li> <li>◆ 阻断告警数:</li> <li>◆ 高危: 威胁等级[7to 10]</li> <li>◆ 中危: 威胁等级[4 to 6]</li> <li>◆ 低危: 威胁等级[0 to 3]</li> </ul>	



区块	说明	详细
告警趋势	<ul> <li>         关联1个资产,显示统计时间范围内告警         趋势。     </li> <li>         关联多个资产时,轮播显示统计时间范围         内告警趋势。     </li> </ul>	************************************
告警类型分布	南丁格尔玫瑰图显示时间范围内告警类型的 Top10。	### 告警类型分布
WAF 资产	WAF 资产可选多个 · 也可选单个 ·	WAF资产: 172.16.100.202 安恒WAF 1.1.1.8 172.16.100.202 192.168.30.57
时间范围	时间范围可选: 最近 24 小时、最近 7 天、最近 30 天、本日、本周、本月。	时间范围: 最近7天 最近24小时 最近7天 最近30天 本日 本周 本月

# 8.3.7 数据库审计大屏

数据库安全分析智能平台大屏实时统计分析当天数据库审计系统设备 · 包括告警类型分布、告警账号分布 趋势、告警账号排行、数据库告警量趋势、实时列表、总告警数、本日新增告警数、本日告警来源 IP 数、 本日告警账号数、告警工具使用排行、告警来源 IP 排行/告警目标 IP 排行等数据。



## 数据库审计大屏如下图所示:

	<b>酒補</b> 運台						
/// 省里类型分布	AW 数据库货税单	1946					
						265	
						0	
	001000					0	
Allen alter	000110					+ D D B B B B B	
						0	
w 告禁账号公司趋势						## 告世工具使用综行	
2						(1) Martin	5040
						Start 1	990
						· Bib Dreepe	300
						(Miles)	015
	the second second		THE R. LANS.	1000 BEE	tant them to the	anatalia /	015
w 告望能句用行	-		-		and the second se	## 告梦庭后户供行	
	2019-09-25-00-45-32	HACTORN R.	-	585834016	51.341.68 126	10,012,0134	29
	2019-09-25 (8) 45 12	STARTING.		42 120 102 97	207 54 175 176	104,240,022,256	.4
	2010-09-25 01 45 22	04-6-2222-8		122 06 42 42	11217243.944	A sincipal gree	
100 100	2019-06-25 (81-45-32	THE OWNER		36.34.55.90	29 101 111 110	111110	3
	2019 09 25 00 45 37	Stoff-Tipting		117 196 36 56	112 96 24 121	101.04.140.110	3
- Man - Courteen	PERIOD STATISTICS	A MARKAN MARKE		and some of	A NORMALINEST		
					2		
Ւ各区块均实时展示当	白大数据。				67		

以下各区块均实时展示当天数据。

区块	说明	详细
告警类型分布	默认展示时间范围内告警类型分布 Top9+其 他。	<ul> <li>生活性学生の分布</li> <li>・ またしまやりやれたさき</li> <li>・ またしまやりやりやりやり</li> <li>・ またしまやりやりやりやりやり</li> <li>・ またしまやりやりやりやりやりやりやりやりやりやりやりやりやりやりやりやりやりやりやり</li></ul>
告警账号分布趋势	默认展示时间范围内告警账号分布趋势 (distinct userName)。	世 世 世 世 世 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田
告警账号排行	默认展示时间范围内告警账号的分布 Top10。	## 告啓紙号排行     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000     15,000



区块	说明	详细
数据库告警量趋势	展示本日告警数据量及上周同时段告警数。	
实时列表	<ul> <li>◆ 滚屏显示 deviceAddress: xxx 的最新 50 条 数据 · 包括时间、名称、风险等级、来源 IP、目的 IP。</li> <li>◆ 点击溯源至原始日志 · 带入条件: 时间 +eventId。</li> </ul>	Name         Name         Name         Name           Strate         Strate         Strate         Strate         Strate           Strate         Strate         Strate         Strate         Strate         Strate           Strate         Strate         Strate         Strate         Strate         Strate         Strate           Strate         Strate         Strate         Strate         Strate         Strate         Strate           Strate         Strate         Strate         Strate         Strate         Strate         Strate           Strate         Strate         Strate         Strate         Strate         Strate         Strate           Strate         Strate         Strate         Strate         Strate         Strate         Strate           Strate         Strate         Strate         Strate         Strate         Strate         Strate
总告警数	展示时间范围内安全设备总告警数。	скох 9.6 Л
本日新增告警数	展示本日安全设备告警数。	2 0
本日告警来源 IP 数	展示本日告警来源 IP 数。	*==###### Ø
本日告警账号数	展示本日告警账号数。	≈⊡nen0x O
告警工具使用排行	1.展示时间范围内告警工具使用 Top5 · 点击更 多显示 Top10。 2.点击溯源至原始日志页面。	第二月使用排行         python3       19824         xssel       1298         SGL Developer       1180         missa       1062         @PHLTHES       1062
告警来源IP排行/告 警目标 IP 排行	<ul> <li>◆ 展示时间范围内告警来源 IPTop5 · 点击更 多显示 Top10 ; 点击溯源至原始日志页面。</li> <li>◆ 展示时间范围内告警目标 IPTop5 · 点击更 多显示 Top10 ; 点击溯源至原始日志页面。</li> </ul>	10.222.295/98       118         168.291.707       7         168.291.707       7         168.291.707       7         168.291.707       7         168.291.707       7         168.291.707       7         168.291.707       7         168.291.707       6         171.81.91.247       6         171.7156.63.164       5         177       188         177       188         177       188         177       188         177       188         177       188         177       188         177       188         178       164         178       164         178       178         178       178         178       178         178       178         178       178         178       178         178       178         178       178         178       178         178       178         178       178         178       178         178       178



区块	说明	详细
时间范围	时间范围可选: 最近 24 小时、最近 7 天、最近 30 天、本日、本周、本月。	时间范目:最近7天 最近24小时 最近24小时 最近30天 本日 本月

# 8.4 弱点管理

# 8.4.1 功能简介

选择"资产管理>弱点管理"界面, 支持安恒信息Web应用弱点扫描器、绿盟扫描器和天镜脆弱性扫描与管理系统扫描报告导入、查看。

# 8.4.2 弱点管理

## 1、 查询

弱点管理支持弱点名称、威胁等级、受影响主机名、 CVE 编号和扫描器类型等查询。如下图所示。

業必要用	X	MENNE MARK	-	REFERENCE	
CVERT	Qx_	HERRY OF	*		
24 22	20 S	- Children			
		S			

## 2、 重置

弱点管理支持查询条件重置,如下图所示。

HAR	KENK 2001 -	REALTANCE
CVEIRM	196 <b>8</b> 4 <u>1</u> ±0 -	
84 88		

#### 3、 详情



列表展示弱点名称、威胁等级、扫描器名称、受影响主机、 CVE 编号及操作列。如下图所示。

關約將條 :	NEGRO DE S	100080 :	经影响主机 :	84148	CVESS :		i\$IS	
HTTP Server局型/DEF本母	(E8	\$65882*8	192,168,30,190	19002			8	-
Oracle MySQL Server的社会全角用	中推	安信迟程安全评估	192 103 30 195	13308	CVE-2918-2761	à	8	-
Olaciw MySQL Server设计学 全限网		安徽总理安全评估	792 168 35 196	13306	CVE-2018-2640		8	(#)
Oracle MySQL Serveri的中央全部同	0.05	要優估場安全律告	192 168 30 196	13306	GVE-3818-2562		8	-
Oracle MySQL Server包括安全情况	中態	安徽远和安全评估	192 108 30 196	13308	Q-64/E-3218-3058		8	
多数Diacka ^m 是安全规则	中雪	安德远程安全评估	162 165 35 196	13306	CVE-2015-3152		8	-
Oracle MySOL Server回注册金属词	1078	安徽访耀安会评话	192,168,30,199	113305	GVE 2918 3133		8	+(
Oarde MySQL Server监持安全推闭	中省	安徽远程安全评估	152 103 30 190	13398	CVE-3018-3251		8	(m)
Oracle MySQL Server원라와 순제에	中間	支偿迟程安全评慎	192 108 30 108	13506	CVE-2018-3174			

## 点击操作列的 学 按钮, 可查看弱点详情。弱点详情包括弱点名称、威胁等级、扫描器名称、受影响主机

名、弱点描述和解决建议。如下图所示。

710 7518	 NECT # 15

第四名印	Onick MySQL Server提供要金融商	#2 ¹ (2005)
	如料金板板面帶電	Remarking was not used and a set of the set
袋的描述	Gracial Hyspill 编图中备立(Gracial)公司的一套开源的关系数据希望错录	ater den BRARRANELER, MARE, MARELARDER, Manz server BRANN-1-BRENNT, Dreise Manz-PRIVAL Server1943.5.5
NURBER	自用厂员已没有行动计T以投算器具。计T误和财物: http://www.oracle	n. com/technetuare.retur 11y-acvissory.eputer.1018.3136638.ntm3
通用		33

# 8.4.3 扫描报告的导入

本平台支持的扫描工具有安恒信息Web 应用弱点扫描器、绿盟扫描器和天镜脆弱性扫描与管理系统。 点击<**扫描报告导入>**,弹出扫描报告导入页面,如下图所示。

224		自接很皆夸人		3	CROCE LAND				
1000		10:10/j.Wintbil)	- 69996 -	國際對自己這些世界系統					
			已制成文:4: 9 (西风文)	•			a T		
	Envan	in .		R34 - 182	99	CMINE -		104	
	HERE Danne MILLER = 16	(12);	##1500mail?#	(0003663006))	03002		2.	(a	
	Oracle MyGGL Tenner@HS-2-868	195	*#BW####	1102-005-00.004	13306	CVERD1P-2791			
	Charles MySTEL Server (219 1) (197	25	*****	No. of Co. yes	-	CV8.2018.2949			
	Owner Myntal Samuellin and Samuellin	-942	white the	7400/488.00.494	11500	OVE-ONE-2982		- 11	

导入的信息都可以在扫描列表中显示,每个域名每个漏洞为一条。同一个系统保留最后一份漏洞信息。

## 1、 安恒信息 Web 应用弱点扫描器



安恒信息 Web 应用弱点扫描器支持的扫描报告格式为 xml。扫描报告导入页面选择安恒信息 Web 应用弱 点扫描器· 选择需要导入的扫描报告导入。如下图所示。

扫描报告导入			×
安恒值息web应用题点扫描器	線塑扫描器	天鏡龍銅性扫描与智	理系统
已选择文件	∲ ◎ 选择:	x#	00
		取消	提交
		取消	提交

## 2、 绿盟远程安全评估

1) 支持绿盟Web 应用漏洞扫描器在线导入, 要求必须购买接口模块。

扫描报告导入页面选择绿盟扫描器下绿盟Web 应用漏洞扫描器,点击<新增>,打开新增扫描器弹框。 输入扫描器名称、扫描器地址、用户名、密码,其中扫描器名称及扫描器地址唯一,点击<保存>。如

输入扫描器名称、扫描器地址、用户名、密码,具甲扫描器名称及扫描器地址唯一,点击<**保存**>。如下图所示。

新塘扫描器	5			>
· 日田開名称:	15 T	32		
	S.			
THE SHARE				
			关闭	保持

选择自己新增的扫描器, 对扫描器接口进行连接测试。或者点击连接测试按钮, 对扫描器接口进行连接测



试。选择需要导入报告任务 ID,提交。如下图所示。

恒信意web应用额点	時間線	樂望扫描器	天镜能	副性扫描布管理)	影響
适择白檀器:	線證WE	6成用编词扫描器		Ý	
扫描器名称:	网络树	1971	新聞	连接测试	
任务(D)					

支持绿盟远程安全评估 5.0 离线导入。扫描报告导入页面选择绿盟扫描器下绿盟远程安全评估 5.0 · 选择需要导入的扫描报告导入。如下图所示。

<b>I</b> 描报告导入		**	
安恒信息web应用器点	白梅語	大統絶弱性目振気	管理系统
选择扫描器;	線路辺程安全評估の		2
	LUSHXH DS		
	6	取満	振交

3) 支持绿盟远程安全评估 6.0 在线导入,要求必须购买接口模块。扫描报告导入页面选择绿盟扫描器下 绿盟远程安全评估 6.0,点击<新增>,打开新增扫描器弹框。输入扫描器名称、扫描器地址、用户名、 密码,其中扫描器名称及扫描器地址唯一,点击<保存>。如下图所示。

新增扫描器		5
* 扫画聯名称	「「「「「」」」	
	输入扫描器物理	
* 用户名	輸入用中省	
* <b>室</b> 码	编入密码	

选择自己新增的扫描器 · 对扫描器接口进行连接测试; 或者点击<连接测试>按钮 · 对扫描器接口进行连接测试。



选择需要导入报告任务 ID,显示任务名称,提交。如下图所示。

安恆信息web应用關点	扫描器	縁盟扫描離	天镜脆	勞性扫描与管理	系统
选择扫描器:	建塑造板	验全评估6.0		*	
扫描器名称:	潮田博	~	新増	连接测试	
任勢(D):				v.	S.
任务名称:					2

## 3、 天镜脆弱性扫描与管理系统

支持天镜脆弱性扫描与管理系统在线导入,要求必须购买接口模块。

扫描报告导入页面选择天镜脆弱性扫描与管理系统,点击<新增>,打开新增扫描器弹框。

输入扫描器名称、扫描器地址、用户名、密码· 其中扫描器名称及扫描器地址唯一· 点击<**保存**>。如下图 所示。

* 2	白描羅名称:	「「「「「「「」」」、「「」」、「「」」、「」、「」、「」、「」、「」、「」、「	
• 1	日振行		
		(Brau)	
S.S.	•用户名:	鑑入用中書	
·S	· 密码:	输入密码	

选择自己新增的扫描器,对扫描器接口进行连接测试。或者点击<连接测试>,对扫描器接口进行连接测试。



选择需要导入报告任务 ID,显示任务名称,提交。如下图所示。

服告导入				×
r恒信意web应用期点	白褐磷 绿豆白褐素	天眼的	關性扫描与管理系统	-
扫描器名称:	请选择	~ 新增	连接测试	
任务ID:			~	
任务名称:				
			e de la companya de l	
			取消 影	×.

8.5 处置联动

# 8.5.1 功能简介

选择"资产管理>处置联动"界面, 支持 WAF 联动,

处理联动包含三个部分: 1.联动设备添加; 2.联动策略设置; 3.完成阻断事件。

## 8.5.2 联动设备

## 1、 新增联动设备

在资产管理页面点击<新增资产>,在基本信息区域,资产类型选择安全类/Web应用防火墙(WAF),厂商为安恒(DBAPPSecurity)或者是 Imperva;资产类型选择安全类/下一代防火墙,厂商为山石防火墙(5.5R5)或华为(Huawei)或华三(H3C)或网御星云(leadsec)或天融信(Topsec);资产类型选择网络类/防火墙,厂商为深信服(SANGFOR),并开启联动设备。如下图所示。

0.0010		5	
18.8	attraining (	1000	100-0221
2442		(area)	-
where-	C Com		
2108415			
SALESS-	and when attaine .	10088 Inte +	
1.00	(II) = w	ALL BARREN	

联动设备页面新增一条记录,列表显示设备详细信息:安全设备、资产名称、资产 IP、设备类型、端口、 状态、操作(编辑、连接测试)。



如下图所示。

Biologi Distant	围起都持					
5-2-28 Entitions	a • Emp	3022-011				12 29
安全印象 :	80°86 :	Bipip :	设备支型 :	第0 1	88	提作
	绿阳镜火罐	30.0.0.200	学会进行一代的大相	80	17 M	(*) (*)
防火炬	APT .	10.2.5 144	全全国-下一代的大概	443	Catar.	× +

若安全设备关联该资产, 联动设备界面显示该安全设备。

#### 2、 编辑联动设备

联动设备页面点击操作列的编辑 按钮 · 进入资产编辑页面 · 保存后返回联动设备页面 · 并更新列表相关

信息。

### 3、 删除联动设备

资产管理页面编辑 WAF 设备 · 关闭 < 处置联动 > · 保存 · 联动设备界面不再显示该设备 · 如下图所示 ·

设备管理	
设备广观。	安街IDBAPPSecurity) * 设装型号: Intel College
设策板本	alina A. Lithines an
管理地址。	Contraction to an an an
日本豊富技士	
在成状态检测:	(元) 12月1731: 周辺市人田市 - 12月1月日 30日14 -
处置联动	

## 4、 测试连接

联动设备页面点击操作列连接测试 按钮 · 重新检测该 IP 对应 WAF 设备的连接状态 · 并更新 "状态" 列;当状态异常时 · 提示连接失败 · 正常时 · 提示连接成功 ·

#### 5、 查询与重置

联动设备支持安全设备与资产 IP 查询,支持查询条件重置。



如下图所示。

2222 212500X	a - 874	ISBN 0°				22 23
安全设备 =	90×8502 ÷	жар :	88X8 :	第11 =	秋志	操作
	乌为额头情	30.0.0.200	安全线于一代数火槽	.440	1677	× [4]
助火總	APT	1020344	非大规划一干 柯金克	3441		× ×

# 8.5.3 联动策略

选择"资产管理>处置联动>联动策略"界面,显示被触发的联动策略信息。列表展示策略更新时间、阻断 IP、阻断时间、安全设备、资产名称、资产 IP、策略来源、本月事件次数、状态、策略阶段、操作(删除)。如下图所示。

出产管理 使置联动 RECEIPT CONTRACT - 3PP 00.00 BRIE COLLEG 安全道像、東方の外の加えら sates." 前天: 20 #129444 MNAN ITTELLE 加速更新时间 REF P 用新社術 安全运输 8/F88 : 限产10 202635 538936 本目明件次因 88 接触的的 開始 3800-12-17 1 102.168.26.1 安徽WAE :50 88 田志市 192,168,172 决定 安留いた 0 . £ TT-58 2020-12-15 1 102 168 26 1 192.186.1.1 82. 実際がみ **HALEPS** 13 口径 已佳志 2 0.55.47 2(20-12-13.) 10:14:101 192 108 20 1 6.51 安信いルド THE OWNER 210 2118 Bate Ŧ 445.45 2020-12-13 1 210(82335-7 192 160 26 1 63. # QUINE BREAKE nit 112 10400 . 2.07.45 2029-12-11 1 7 03:58 102,168,251 HAN . 4444 6.5 \$ BUNK **CENAL** 100 前線 8

联动策略来源有两种:一是自建;二是剧本编排。

用户自建联动策略优先级高于剧本编排创建。用户自建联动策略阻断时间为永久, 状态为已生效, 策略阶段;剧本编排创建策略阻断时间(10min、30min、6h、24h、72h、永久)可调整、可删除、可添加。



新煤飯路

按钮,

1、 联动策略增加

A. 点击

弹出新增页面,填写阻断 IP、资产 IP (资产 IP 多选), 保存。如下图所示。

6	安恒	信息
	DAS-SECU	rity छङ्डव

* 255 doint 1 1 2 3 4	
-omiti Desenvez	
* 遼严印: [192,168.30.82 ×]	*
192.168.30.82	8
	87°.44 36678

B. 选择"**态势感知>数据中心态势**"大屏 · 点击**攻击者基本信息**模块黑客 IP 右侧 ● 。联动策略页面显示该阻断信息。如下图所示。

A&LPHA								
14 ¹			NAME OF T	AV 33.844		nt bes for an Maria Tangkash Adalar 013-05-24 36.441.07	an a	
				A STATE	R+ months and manufactures.	1012 III - 101		
AV 197				W RETENS	167			
Editificances 2 States State 1 States State 2 System 1 Mildes States 1	999600 99978 2788 2788 2788 2788 2788	1913/02/03/04 1943/03/02/04 1922/03/04 1922/03/04 1944/03/02/04	2000 715 715 715	10.24 (0.44)	102.004/54.005 102.004/54.005 102.004/54.005		CONTRACTOR CONTRACTOR FILE Connection Contractor (Contractor) File State (Contractor)	0.500

C. 选择"态势感知>攻击者追踪溯源"大屏·点击攻击 IP 左侧 ● 。联动策略页面显示该阻断信息。如下图所示。

	(*) And in the second s	
Non-special special biological states	w Ratilitat	
	المحكمة المحكمة المحكمة المحكمة المحكمة المحكمة المحكمة	
	and the second se	
	aw pastaka	
Including and Tables	202.101.172.35 ( 819)	
INCOMPANY AND ACCOUNTS ACCOUNTS	193, 196, 255, 170 2555	0
	102.148.198.203 / 1/24	
REALISTING OF THE REAL PROPERTY AND A DESCRIPTION OF	104.239.167.210 7 / 5	£
and the second s	142.0.38.234 7/1	
** REALE	autoral www. to the own	
	and and a second s	
2014/01/2 Multi 10	Fitsec/kt/i#iil.	
ann an	HE TRINSPAN	
attendek went to 🔹 🥌 💷 👘 till find fin Voldstatik of första attigkan kok overeter attende	n man man hitse	


#### 2、 联动策略删除

- A. 点击操作列 2 按钮·删除该条策略信息。
- B. 选择"态势感知>内网安全态势"大屏·点击攻击者基本信息模块黑客 IP 右侧 联动策略页面不

再显示该阻断信息。

如下图所示。

A&LPHA 内间安全态势							
		*****	3 AF REAL	41.00 • 10 • 10 • 10 • 10	er blatten Rom Di Watermond Roman de art teket tot	anna a Maria a Maria a	54 R:
			X001648th With reserved, a Elimical Miner Notifica, wa Association and Science and Science and Science and Science and Science and Science and Science and Science and Science and Science and Science and Science and Science and Science and Science and Science	Le Bather, Valla A.D. WORTVer R.D. A.F. (1994) Bather School (1994) Bather School (1994)	AN JOHR AMINATY, JI STATE MA IN JANUA		<b>1</b> 011-08
AV 58	金属市業		AN XATLEBO				
contine (MUS (111)+)			N-DAME		in the second second	NAME	ANNIE .
Ethenned	econesi		195307 1442100		121 HE MAY HAR	APTRACTOR	
BB1E, realition for the	americ.		05-0716-42:00	1948310	1253.45102.100.100.	ARLIN Prints	
Ry-Jolinia Lipes	HERE A		15-107 14:47:00		12.141.102.161	EB1073-Marriel	100
102712	Hand		95-07 144750	94556	218,246,46,228	repositing	

C. 选择 "态势感知>攻击者追踪溯源"大屏 · 点击攻击 IP 左侧 ● 。联动策略页面不再显示该阻断信息。 如下图所示。

A&LPHA water and a second seco	The fact that 🗖 second
mailan mailan	Arr 20.8283-659
	37 99004, 40 772894 10 A.
PRESERVE WILLIAMS BREADWARD BREADWARD	1.2.3.41.162.108.11.108 494. 202.101.109.00 2
And the optimized and the opti	295.246.40.228 2
	APTHEOLOGICA

3、 查询与重置

联动策略支持安全设备、资产 IP、阻断 IP 查询。支持查询条件重置。如下图所示。



2298 NO.		1.4	menp use		ENP	and in the		ARAS INCLUS	200	-	22	84
										L		
101 E.e.M.	0.01.01	1.0										1222
MBRHEIG	089	Ratein	9988 :	#FEB :	30 ² 0 -	相称为此	R842 :	*79422	465 :	station (s)		m
2020-12-17 1 6:11:58	192.166.1.2	62.	#12map	\$\$	102.155.25.1 96	nit	12	0	785	5	1	ř.
2020-12-15 1	192.168.1.1	65	#HEWAF	#18mAF	192 188 28.1	12	mitt	0	Can C	-	1.17	1

### 8.5.4 阻断事件

选择"资产管理>处置联动>阻断事件"页面,显示WAF发送过来的阻断事件信息,包括阻断时间、阻断 IP、目的IP、域名、触发策略、资产IP、操作。支持安全设备、资产IP、阻断IP和时间查询。支持查询 条件重置。如下图所示。

100 000 00 00 00 00 00 00 00 00 00 00 00				2		
Pites Pits	ITH BIT		*	0		
9229 examinate	- 3544	million .	Barre station of		2020-12-28-00-00-00-1	8291238183843
			S	6		88 84
EBING :	ERSP :	109P ±	HA		30mm	酸性
2020-12-26 10.29 32	110.327.187.149	189,108,89,107	100 YOM 600 VA7	numi.	0.26.11.0	
2829-12-28 16:27 32	88.19.2.158	211 100 3 43	S211 198345	10.002 <i>0</i>	8.24 15.0	
2020-12-26 16:24:32	110.101.101.00	140.204.89.5	140.200.00.5	11117方法相关	8.24.15.0	(*)
2020-12-28 10:23 23	172.58.84.210	104(166),212(2)	134 102 1274	90(主),积高	824101	
2929-12-26 16:21 22	112.10.132.101	113.120.212	ATRA 120.217.0	1944.006	9.24.15.0	
2020-12-20 10 19-22	87.198.146.162	TRUCH CIT	5 TI2 64 217.6T	nusil.	9.26.10.0	

# 8.6 安全域

### 8.6.1 功能简介

选择"资产管理>安全域"页面,有缩略图和列表两种模式,默认显示缩略图模式。

将收集到的客户在用 IP 段 · 细化成各个安全域 · 然后配置到安全域中 · 以便在数据分析或数据展示中能够 直观查看到对应 IP 所属部门或者使用用途 ·

安全域分为内部安全域和未分配,非内部安全域的 IP 自动归为未分配。出厂情况下,默认内置一个名为 "局域网"的内部安全域。包括内置的安全域在内,用户可进行安全域新增,编辑,删除,导入导出等操作。

### 8.6.2 页面布局

安全域页面布局如下图所示。



× =				単入 単世 新選会会
作为云       NB     127.80.1       172.158.80-172.34 295.255       加油井市     149       水油井市     0       7天西慶     第19       ● 女金朱田田     ● 共平宮道		U加用FF 0 0	(10.00 (10.10 (10.10 (10.10 (10.10 (10.10 (10.10 (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10.10) (10	小市政务云 (日本政务云 (日本)1411(日)1951(日 (日本)1411(日)1951(日 (日本)1411(日)1951(日 (日本)1411(日)141 (日本)1411(日)141 (日本)1411(日)141 (日本)141(日)141(日)141 (日本)141(日)141(日)141(日)141(日)141(日)141(日)141(日) (日本)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)141(日)14(日)14
281-2-2157-0	6 <b>3</b>	- 201984	and y	10 H H
26 20. J.	6 <u>8</u> mu	- 2013/42 8	e.	第月 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二
216 210-0-0-0-0 04 921650 :	55 ann Heileri	- Internet	N. N.	第月 3 日本 年齢(1) 第日 第日
188 200-3-2005.00 時	65 aug	- 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111990 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 111900 - 110000-0000 - 1110000 - 110000 - 110000 - 1100	231.255	1 922 1000 1000 1000 1000 1000
28 28-3-2000 時 - = 完全域名称: 単九正 深期日	55 and Holeso	- 1010940 =	8.	1 前面 1 前面 1 前面 1 前面 1 前面 1 前 1 前 1 前 1 前 1 前 1 前 1 前 1 前 1 前 1 前
<ul> <li>2001 201010</li> <li>2011 2</li></ul>	6年 第11日 単約第5日 単約第5日 単の単元の「「「「「「「「「」」」」」」」」」」」」」」」」」」」」」」」」」」	- 8115940 - 127 3 0 1, 172 39 2 102 588 59 7 102 588 59 7 102 588 59 7	293.255 192.785 90,41-192.1	1 988 100 10 10 100 10 10 100 10 10 10 10 10 10 10 10 10 10 10 10 10 1
<ul> <li>(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)</li></ul>	新日本 新日本 新日本 新日本 新日本 新日本 新日本 新日本	- 40170440 - 1 127.0.0.1,172,19,00,172,33,2 102,1980,00,171,102,1980,00,14 102,1980,00,171,102,1980,00,14 102,1980,00,171,102,1980,00,14 102,1980,00,22,192,100,00,28 102,198,00,20,21,100,00,28 102,198,00,21,100,00,28 102,198,00,00,00,00,00,00,00,00,00,00,00,00,00	95.256 192.168.90,41-192.1 192.160.99.31-192.5	1 1000 1000 1000 1000 1000 1000 1000 10
<ul> <li>(第二) (1000)</li> <li>(第二) (1000)</li> <li>(第二) (1000)</li> <li>(第二) (1000)</li> <li>(第二) (1000)</li> <li>(第二) (1000)</li> </ul>		- 1021709802 - 1021709802 - 1021709802 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 10221902 - 102	95.256 192.168.90,41-192.1 192.160.99.31-192.5	1 1000 1000 1000 1000 1000 1000 1000 10

17711 QAM

序号	名称	说明
1	查询区	显示查询条件及< <b>查询</b> >、 < <b>重置</b> >按钮。查询条件:安全域名称、标签、组织架构。
2	操作	模式切换 · · · · · · · · · · · · · · · · · · ·
3	安全域列表	该区域主要用于安全域信息展示以及相关功能的操作。 安全域信息展示:列表模式、缩略图模式。
4	快速跳转	点击页面底部<快速跳转: 内部 IP 配置>·页面跳转至配置管理页面。

# 8.6.3 安全域新增、编辑、修改

#### 1、 安全域新增

点击

新增安全域 ·打开安全域配置页面·如下图所示·填写相关信息·点击<保存>。



PTT ( 02)	11 安全國配置	
* 210	and a minimum	
	and the present	
描述	1010人中生4001月	
	6235	*
• 101m		
安全域脉道		
6年	annie	N. N.
组织架构		joh .
相识	WITHHING	
安全域同段		
	lőtor-	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
	注:內部安全城之间的阿翰不克持交集,配置的安全城网股确保 中	不在與它大靈安全地
		**
	保存 通回	× ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

#### 基本信息

名称为必填项且唯一;描述为非必填项; 图标为必选项, 默认选择一个图标,点击图标可进行修改。

#### 安全域标签

标签为非必填项,默认云和边界两个标签,用户可自定义添加标签。

#### 组织架构

组织架构为非必选项· 支持多选· 选择时默认不带上下级· 点击后面的全部· 带上下级所有。当前用户若拥有组织架构权限· 显示<编辑组织架构>按钮·点击可新打开一个组织架构界面。

#### 安全域网段

安全域网段必填,必须配置一个及以上 IP 条目。安全域网段支持三种类型: IP 地址、 IP 区间、子网掩码。

内部安全域之间的网段不支持交集· 配置的安全域网段确保不在其它内部安全域中。

#### 2、 安全域编辑

列表模式点击操作栏的 / 按钮 · 缩略图鼠标上移点击 / 按钮 · 打开安全域配置页面 · 显示安全域的相关信

息·包括基本信息·安全域标签·组织架构·安全域网段·可查看和修改安全域配置·修改后点击<保存>· 安全域信息更新·并返回到列表模式或缩略图模式的当前页。



#### 如下图所示:

· · · · · · · · · · · · · · · · · · ·	4 ALGAR		
• 条称	\$3为资		
iez.	<u>会社</u> 局地図。未配置協定下、助AU 1 Diaes A 127.0.0.1 2 Class B 10 0.0.0-10 255 255 2	下区間中20間線開中 55. 取以子院種研255000	
* 劉核.			80
安全辅助器			N.
杨笙	面別時度推		
細胞業務			
(BIR	10200000	#描述的##	
安全域间段			
- (955)	iPI告社 · 127.0月.1		3
<ul> <li></li> <li><!--</td--><td>P图用 - 172.16.0.0</td><td>· 172 31 255 395</td><td>3</td></li></ul>	P图用 - 172.16.0.0	· 172 31 255 395	3
	5 IDP	S di	
	注:内部安全地之间的网段不支持 中	AR DENTERMARKEMENSER	
	847 26	S III	

#### 3、 安全域删除

 列表模式下可点击操作栏的 按钮删除该安全域。也可选择单个安全域前的多选框或多个安全域前 的多选框,再点击<删除>进行单个安全域删除或安全域批量删除。

当选择全选框后 · 可删除当前页的安全域 · 也可选择删除查询结果所有 (<删除查询结果所有>按钮需要全选安全域才会出现) ·

若所选删除的安全域被 Web 业务系统发现或资产发现,则该安全域删除失败。如下图所示。

AILPHATER	ADDL		0
FTER ( #### )	E		
*** ·	(98) and	<ul> <li>(a) (a) (a) (a) (a) (a) (a) (a) (a) (a)</li></ul>	
			81. WO
	60000		#1
· · · · ·		107 3 4 1 10 4 4 9 10 30 20 20 20 20 20 20 20 20 20 20 20 20 20	(e) (e) (e) (e)
- Cl		10.11	Service in the
		1004	8.4.9
80		910	A. A. A.
		( ava ( ) )	Contract and Contra
A DESCRIPTION OF THE OWNER OWNER OF THE OWNER OWNER OF THE OWNER OWNE			

2) 缩略图模式上移点击右上角 [●] 按钮即可删除该安全域。



# 8.6.4 安全域导入和导出

#### 1、 安全域导入

点击 按钮· 弹出导入安全域页面· 如下图所示。可点击<模板下载>下载模板文件进行填写· 若文件 中有一条安全域的字段填写错误·则整个文件导入失败。

PTT #28		
(428 100 mmm)	导入安全地	× 2 ** **
	· \$455	
新 We 华为云 Int No. 10 (10.000.000.000.000.000.000.000.000.000.	COULTRANT MER REMARKING BEARINESS CONTRACT	杭州市政务云
1227" 10 Sign" 1 2228 10		name a Diane a Mare di Diane anno di Diane
1.0010 0.0100	A BEER A BEER X	Canno v man

#### 2、 安全域导出

点击 按钮, 导出平台中所有的安全域,导出的内容如下图所示。



### 8.6.5 其他操作

#### 1、 安全告警

列表模式下点击操作栏的 按钮 · 缩略图模式下点击 按钮 · 新打开一个安全告警界面 · 带入条件:时间(最近 7 天) +目的安全域(destSecurityZone)为该安全域名称。

#### 2、 资产管理

当安全域下有资产时,列表模式下显示 按钮,缩略图模式下显示 ******* 按钮,没有资产则不显示。 点击按钮,先打开一个资产管理页面,带入条件: 左侧安全域选择该安全域。



### 8.7 组织架构

### 8.7.1 功能简介

选择"资产管理>组织架构"页面·默认显示一级和二级节点。出厂情况下·会内置一个名为"总部"的 根节点·不可删除。各节点下会显示对应的用户信息和关联业务。

### 8.7.2 组织结构查询

组织架构支持关键字搜索·输入关键字自动匹配包含关键字的组织架构(模糊搜索)·搜索结果需要显示上级组织·可点击展开查看对应的下级数据。查询数据为空·显示暂无数据。如下图所示。

### 8.7.3 组织架构新增

选中根节点· 点击<添加子节点>· 填写组织架构的基本信息· 包括组织名称、组织编号、组织简称、单位 地址、地区·然后点击<保存>· 组织架构新增成功· 如下图所示•

17785 Q 82758 805		
N INAL	· · · · · · · · · · · · · · · · · · ·	
i information information in the second s	· IBIRAR ( THIN	(如於樂事: 321)
± /1998885	S S	
1 · · · · · · · · · · · · · · · · · · ·	1200000 TZI	第4回形地 123
31318 E		
3 M	SE STRURNERITE	

# 8.7.4 组织架构编辑

选中节点 · 右侧显示该节点的基本信息以及该节点对应的用户信息和关联业务 · 若无用户信息或关联业务 · 则显示暂无数据。可对基本信息进行编辑 · 点击关联业务中的安全域或 Web 业务系统 · 新打开一个安全域 /Web 业务系统页面 · 带入条件 : 安全域名称/Web 业务系统名称。



antes o astra				(42)
11 10月1日	基本信用			
<ul> <li>(c) (c) (c) (c) (c) (c) (c) (c) (c) (c)</li></ul>	+ (BRS1)	(1121)	组织病导	321
11	0.020	123	#052	123
* この かい時PCE 目前式気	ŧЯΞ	812#149/mile18		
D eff	用户结束			80
	用户内 :	<b>#8</b> =	### =	इंस्.सः :
	cardy -	发纺装理具	17304074/236.00	n)
	berr .	248797	her/Tasilishaponer	with com th

# 8.7.5 组织结构删除

删除节点时需要先解除所有绑定关系,没有解除绑定时不能删除。如下图所示。

	and a providence and and and another the	14
<ul> <li>- 2 MM</li> <li>- 2 MMM</li> </ul>		
	AP42	
	Day max man	

◆ 组织架构有子节点时,不支持删除父节点,需要先删除子节点才支持删除父节点。



# 9. 系统管理

可对平台进行运维管理、配置管理、任务管理、系统管理等操作。

### 9.1 运维管理

运维管理包括运维告警、健康检查、存储管理、故障日志等功能, 便于用户实时且直观的了解平台的使用 情况及其健康状况。

### 9.1.1 运维告警

选择"系统管理>运维管理>运维告警"进入运维告警页面。该页面汇总了平台中运维告警的信息并加以 展示, 使用户更方便了解系统运维的健康状况。

	1040 - MBHRI - + 92	98- usser- son	de a sinter-		0
Date - Gente - Kanan			ò	6.	
MENE OF INCOME.	5626 (111)	5 · · · · · · · · · · · · · · · · · · ·		· Reality acres of the strategy of	20-60 m 10 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
i nane			Ő.	×A.	Territor -
1				Contraction of the second	
	In the second state of the				
	C 200.0000 (214)	1.71000 00009-3711.000 CM	Constant and the second	(21-6 (4-500) (200-5-11 (100)	e source is loose as an in many
1		0	e de		
A MODE					
19458	intenter -	WEAR .	DER .	#H218	PORTER STATE
212	3020468-11 H0:00109	口水市和市井东	20	2167-036	STATISTICS AND A STATISTICS
	2020-09-11 10:00:52	SZEMMERT		0.0243.0	\$535 ( 4.1.0, 10, 10, 10, 10, 10, 10, 10, 10, 10, 1
0-1	2020/08/11 11:00 58	DESCRIPTION	S	201059	Min. Manifest Matter
	3000-848-11 13:00 (4	NIFRASARE V	$\gamma$ .	2154850	SERVICE TO THE THE PARTY.
REARANS	3000-02-11 1x100-17	CANAGE OF C		2433855	能化理论能改进分配
	2000.00 H 14.00 HT	O ARRENADO		R.RMAR	808110.10.10.10.2087
	930048 TT 1948.37	Basiminate		NAME AND	Bolighter
	TO THE MART TO ARE ADDREED	Insertigener)		2167493	Section in in install
	1000-04-01-12 4/E4	CARAGES		0.51855	LANSING STREET
Di setenter		2			The second s
	2020-388-1118-27502M	the second se		and the second sec	AND A THE THE THE THE PARTY OF

#### 查询

可通过告警详情、告警名称、告警级别、时间范围、模块分类(点击**高级查询**图标出现)字段对运维告警进行筛选及查询,如下图所示。其中告警详情支持模糊查询,告警名称支持多选,告警级别仅支持单选。

 WEAK
 <th

#### 告警趋势

告警趋势以柱状图的形式展现, 如下图所示。时间范围默认与查询条件中的时间范围保持一致, 也可重新



选择时间粒度,如1小时,1天,一个月,一年,告警趋势图随着时间粒度的切换而变换。



#### 告警详情

- ◆ 告警详情由告警总数、告警名称占比、告警列表三部分组成, 如下图所示。
- ◆ 告警总数显示总数和高、中、低每个级别的数量, 高、中、低分别用红、橙、黄 3 个颜色显示。
- ◆ 告警名称占比以环状图的形式展示。
- ◆ 告警列表包含告警时间、告警名称、告警级别、模块分类、告警详情, 列表默认按照触发时间倒序显示, 点击表头**触发时间**支持排序。

也豐详情			S.V	<i>C</i> .	
幸福世教	to the second se	西蒙名称	THE .	S Blanc	ntariti
152	2020-12-28 09:00 59	日志采真服的异常	3: 10	(長期無干無限)	服务安借工中用归平台背景
• T 152	2029-12-28 00:01:02	Barresar		設備主義局務	服務委伍丁時週刊平台算業
• + •	2020-12-28-07-01-03	BEXRENA		215-5-16-15	HaeqIescifts
	2020-12-28-00-01-04	BANKER		設備重量程序	服务在但正应用已平台异常
	2525-12-28.09-01-64	日本马南是当开东	80.	数据工業服务	经济会信工业集中平台集中
	2029-12-28-04-01-02	HERRENAR	)*	数据采集服务	服务会培工控制同学会具有
	2020-12-28 03 01 03	E###RESIM		飲損業構設到	服务安德工业第65平台异常
	2005-12-01 02:01:62	日志采集致资料常		飲損半無限例	服务安借工控用约平台异常
- Barassow	2029-12-28 01,010	日本学家成为异常		数据平量服务	服务安位工作算时平台异常

### 9.1.2 健康检查

健康检查对平台使用情况、组件节点状态、集群状态、接口开放状态等进行巡检, 巡检结果以不同的图标 进行展示, 并加以结果描述及处置建议, 使用户可精确定位系统故障并对其进行修复。

#### 巡检结果

- ◆ 若没有历史巡检结果,巡检结果显示:未巡检,且无"**查看历史巡检结果**"字样。
- ◆ 若有历史巡检结果 · 巡检结果显示: 最近一次巡检时间yyyy-mm-sshh:mm:ss (指巡检的开始时间)·
   且有 "查看历史巡检结果"字样 · 点击后出现巡检结果弹窗 · 可根据巡检结果 · 巡检方式以及时间范围对其进行查询筛选 · 巡检记录可查看 · 如下图所示。



点击右上方<一键巡检>可对运维检测项进行巡检。

点击右上方<导出 PDF>可导出健康检查报告。

巡检結果					
11115X02020115-51: 2020-12-	11.42.2.2			04	
数据健康检查	50114259			00	
	10199月第二十世纪	- 当晚方式 全部	← 时间常匮 2020-32	22 00.00 00 - 2020 12 28 09 24 82 0	
0	10100160 ·	的给我来	副自方式	NAHF.	
0	2020-12-27 02:00:00	50 XB	(B2)		
0	2020-12-24 11-47 53	10112	带动	THE C	
0			0.22		
			· · · · · · · · · · · · · · · · · · ·	二 (二) (二) (二) (二) (二) (二) (二) (二) (二) (二	

#### 运维检测项

NAME DIVISION MONOR

运维检测项包括数据健康检查、探针健康检查、大数据集群健康检查、 Elasticsearch 健康检查、实时流计算 引擎健康检查、管理服务健康检查、节点宿主机 IP 健康检查等 · 检测结果以列表的形式展示在每个运维检 测项的下方 · 如下图所示。

其中监测结果若正常·以《展示; 若异常· 则以《展示·并给出相应的处置建议。

#### 探针健康检查

	Wester Or		
近期结果	総直内帯		此眉建安
•	安住工程用日午台和美安人的专	() () () () () () () () () () () () () (	導位費得时去借工控導相平和状态
大數据集群健康检查			
监测结果	総要内容	<b>接近</b>	St-Ballion
0	ania .	节:病間: 1	
•	Hadoogi	1. servert 14:5 • 1. datamode 14:5 • 1. datamode 14:5 • 1. datamode 34:05 • 1. imémende 15:5 •	
0	Zaateseper	1.2006eeper3标志● 1.2006eeper2研志●	

宿主机节点健康检查的结果处置建议为"查看主机监控",如下图所示:



节点 192.168.30.194 健康检查

<b>王明</b> 成果	检查内容	编述	<b>绘图</b> 理说
0	<b>基</b> 年很差	CPU: 32 年, 四序; 251.82GE, 硬盘; 39.76TE	[兼育主机会班]
0	CPURIRIE	22.49%	(會習完明成符)
0	超直利用率	8.39%	[唐卷王所成将]
0	玉统合数	£.53	[童尊主听皇培]
0	网络香叶属	入25届: 90.544804, 出活動151.514800	[#2=131=]
0	磁盘+O使用定	2.38%	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
0	系统进程数	10	DINETHIER
0	內存使用案	66 82%	【章章王印度云]

点击处置列的"查看主机监控"可跳转至Ambari界面,如下图所示:

Articul Inghia 📷 🚥		Indicate Colorest and	in the H Amer	
# 1.053 # Data				
formal camp mang mana		Ó		
Companyood .	+100	Hune Martine	int the +	
· Scherer / elimenter	10111 .	THE R	9.190	
· · · · · · · · · · · · · · · · · · ·	fam +		A STATE OF STATES	
		The second second	ania O	
humany		000/1420 B	Children B	
Headstratement 1 (102) 189-Additionary 102 (102) 2 (20)		NOUL		
Radit: Atribute (e), a* Off. present (e), (e)		alfulder .	3	
Dest. 1144 4020-00071 0008 12 9% and Manuals 200 0720		and the	Second Contraction of	
Lined Rogs 9.10 Weatheast with from a House days			Manual Linux E.	
Contrast, Marcolan Contrasted ACE 1 Terror				
		H		
		MULLIN		
		Andrew B	And a second sec	

# 9.1.3 存储管理

选择 "系统管理>运维管理>存储管理"页面,可查看磁盘使用情况和磁盘使用趋势。

#### 磁盘使用情况

展示当前磁盘使用情况。具体将磁盘使用量分为三个等级·分别是普通(0-60%)、警告(60-90%)和危险 (90-100%)。如下图所示。

総盘使用情况			
	言義已使用意回発(の-10%)	著者已使用意艺说(1076—5976)	<b>加坡日使用最</b> 互換 (97%-100%)
0-152 168 30 154 #1/140716 39GFJ	2.4% #1.37298.85G		

#### 磁盘使用趋势

展示选择时间范围内磁盘使用趋势。如下图所示。



			12.00	121-0010-0010-0010-0110-0	8
	<ul> <li>Or manual</li> </ul>	40. 60. 201		2004-00 	
#00 200		Reft Rest Rest Rest		1         4         1         5         9         9           20         11         11         14         16         14           41         14         16         16         16         16         16           41         16         16         16         16         16         16         16           41         16         17         16         27         16         28         26	1111
-		Rational			

### 9.1.4 故障日志

选择"系统管理>运维管理>故障日志,进入故障日志页面。,可下载容器、宿主机等组件的日志信息,相 关人员可通过日志中的报错记录快速且准确地定位问题所在,如下图所示。

- ◆ 点击<**下载**> · 下载文件为 zip 包 · 解压后包含对应组件的日志文件 ·
- ◆ 点击<**全部下载>**,下载文件为 zip 包, 解压后包含页面所有组件日志。

	10	22
1014	HARM	揚作
Elasticsearch	ger the section as	Fitt
ALPHA Base管理指数	Takitan)	EE.
Halloop	Cinitation and S	下版
Zoolweper		下秋
Kalka	tatiang O	199
ALPHA智能安全平台用户常常	tabilit us	Fal
\$75A	EQUIPMENTER DI	100

#### User Onboard 日志

在故障日志页面按下"Ctrl+?"组合键,可以弹出User Onboard 日志信息界面。点击操作列<下载>可以下载User Onboard 日志,采集用户使用信息用于提升产品易用性、有效性。





del viconicte	Наля	
User Onboard Flic.		A.
8154	system: hig	
ALPABRE主手自用い物商	optita itu	
Talla	stafkji-log	
Justinger	and-reporting	1942
Hadrop	hadrop top	194
ALT-IN ROOM TERMS	Tealer Fog.	170
Dark start	effective to long	140
-	1288	50 12

### 9.2 配置管理

配置管理包括系统配置、数据配置、推送管理、系统开关等功能, 将系统配置界面化, 使用户操作更加便捷。

### 9.2.1 系统配置

选择"系统管理>配置管理>系统配置"菜单进入系统配置页面,系统配置包括系统配置、更多配置、网络代理和界面美化等,系统配置与更多配置将配置参数界面化,使用户易于操作,界面美化支持用户自定义,可满足用户的定制需求。

#### 9.2.1.1 系统配置

选择"系统管理>配置管理>系统配置"进入系统配置页面,点击系统配置页签。系统配置分为通用配置和内部 IP 配置两个部分。

#### 通用配置

建制成的		e la companya de	Real
	* gent		1
	* 7.82E	安全想理干标	
	socati	763 168 31 75	
	BOCGALL	443	
	SOC APIKey	IEdg2r2ve	
	AVVIEWESSE:	1/fbs//192.766.30.1946.8009	

1) 监控地区与大屏名称,配置监控地区与大屏名称。



配置监控地区与大屏名称,如下图所示,即对"**态势感知>Web 业务系统态势**"名称及监控地区、"**态势感知>资产失陷态势**"、"**态势感知>外部攻击态势**"等监控地区生效,如下图所示。 Web 业务系统态势



资产失陷态势



外部攻击态势





- SOC 地址、 SOC 端口、 SOC APIKey · 配置 SOC 地址、 SOC 端口号与 SOC APIKey · 配置完成后进入"资产管理>资产管理"页面 · 点击<SOC同步>进行测试。
  - ◆ 若 SOC 同步成功,则配置参数正确且生效。
  - ◆ 若 SOC 同步失败,则配置参数错误,需重新配置。
- AiView 地址・配置AiView 地址。
   配置完成后 · 选择 "安全分析>可视化中心>AiView 设计器" · 查看刚刚配置的 AiView 大屏
   是否可以正常显示。找到对应的大屏 · 点击 查看大屏。
  - ◆ 若可成功跳转,则配置参数正确且生效。
  - ◆ 若跳转失败,则配置参数错误,需重新配置。

#### 内部 IP 配置

收集客户现场在用 IP 段· 将其配置为内部 IP· 以便数据接入后可立即自发现资产和判断是否为内部 IP。

内部 IP 配置同步至 SOC、 APT、 AiNTA · 且在所有安全事件的分析结果中均有体现。

内部 IP 配置默认以下私网IP 地址区间 IP 为内部 IP:

- Class A 127.0.0.1
- ◆ Class B 10.0.0.0-10.255.255.255 · 默认子网掩码:255.0.0.0
- ◆ Class C 172.16.0.0-172.31.255.255, 默认子网掩码:255.240.0.0
- ◆ Class D 192.168.0.0-192.168.255.255 · 默认子网掩码:255.255.0.0
- Class E 169.254.0.0/16

外部 IP: 非内部 IP(IP 不为空)。

点击<添加 IP 配置> ·可以新增内部 IP 地址。内部 IP 配置支持IP 地址、 IP 区间、子网掩码 · 添加完成后



#### 点击<保存 IP 配置>,如下图所示。

内部中型直							633PEH	研护距离
• 伊型	iPtStE	×	127.0.0 1					
+ (85)	FER		10.0.0		10.255.255.255			
* 951	128	÷.	192:168:30.0		102 100 295 295			
+ (85)	PTSIE	3	0.00.0.00					
+ 8(2)	PIBE		192.108.7.7					
	atornea	1	an e na			2		
	REALUTE 1. Casa A 2. Casa B 3. Casa D 3. Casa D 5. Casa E 9.80P1 4	02/00/0 10:0:0 10:0:0 172:18 192:18 199:25 199:25	1959時間中: 1 1 0 10 355 255 255 第14 子何間 0 0 172 31 255 255 第14 7 8 0 0 192 168 255 255 第14 8 0 0 192 168 255 255 第14 4 0 0 16 第14 子校明時 255 2 1 19平均第2	1955 215 0 0 0 Rangil 255 28 F Yu Nulli 255 55 0 0	800 255 b.0			

### 9.2.1.2 更多配置

更多配置主要涉及**常用参数和更多参数**两个部分,参数保存时,若需重启,需重启后方可生效,若不重启,则不生效。

全用作数		-
做任い	10 20 00 14 127 0.0 1 tocomboot 192 168 31 20 10 14 1 33,40 14,0 36 10 14 0.6 10 14 22 1 10 14 0.01	(nuc)
大于其實證書		
展応導入の調査権		
<b>副范围</b> 存		
* HORXIE	[ALPHAGEMER]	
推送的式货币汇量	[ALPHAZEMERIKE]	
推送跑款背管内育		
interna.	Mbc.rtsuarest 8111	
展点管理平和地址	101.085.11.36	
资点当理于64代*	) attin	
RATERFERE	1110	
mestgator 日布拉著至于爆伤器	12	
* mesogaten ta联合安置可能	500	
* mesogation 2面配合数量符制	50.50	
* mestgator JdR 68:87881	50,50,20	
* investigation 4進股合数臺灣地	50.50.20	
要由日本意味时高量大效素(于)	39.	



#### 常用参数

配置项	说明
信任 IP	可配置多个,以英文逗号分隔, 配置生效后, 可免登录访问所有接口。
允许页面嵌套	开启时,平台上的页面可相互嵌套,若关闭,则不可相互嵌套。
是否导入内置情报	开启时 · 导入威胁情报包 · 威胁情报导入成功后 · 按钮自动转换成关闭状态 · 若关 闭 · 则不导入威胁情报包 。
首页缓存	开启时·首页进行缓存· 若关闭·则首页取消缓存。
告警推送主题/推送 测试告警主题/推送 测试告警内容	告警推送主题与推送测试告警内容对邮件和钉钉生效, 推送测试告警主题仅对邮件生效。
运维巡检地址	若可成功跳转则配置参数正确且生效; 若跳转失败, 则配置参数错误, 需重新配置。
弱点管理平台地址	弱点管理平台的 IP 地址。若可成功跳转则配置参数正确且生效;若跳转失败,则 配置参数错误, 需重新配置。
弱点管理平台用户/ 密码	弱点管理平台登录用户名/密码
Investigation 分析场 景显示模板数	Investigation 分析场景显示模板数量。取值范围: 1~20。
Investigation 1/2/3/4 维聚合数量限制	设置 Investigation 的 1/2/3/4 维聚合数量。
原始日志查询时间 最大范围	设置原始日志查询时间最大范围。取值范围: 30~365。

### 更多参数

点击<添加参数>,可以选择已存在的配置参数,也可以创建新的配置参数。

点击对应参数行的删除图标 🍍 , 可以删除参数。



e e
*
# (RR-141) #
, S'
N. Contraction of the second s
S. I.
.V
<u>v</u> .

- ◆ 选择已存在的配置参数。可选择后台文件中已存在的配置参数添加至界面对其进行修改。
- ◆ 创建新的配置参数。可添加自定义参数, 参数名称不可重复, 参数不可为空。

更多参数中参数的添加与删除操作无需进行保存,且上述操作仅对参数是否显示在前台页 面有效,后台文件中参数并未被删除。

### 9.2.1.3 网络代理

用户启用网络代理后·"威胁情报>情报源>安恒安全数据大脑"设置中的在线更新功能通过代理服务器 请求安恒安全数据大脑情报库更新。网络代理默认关闭。可设置开启/关闭使用网络代理、设置代理服务器 地址端口、开启/关闭代理服务器认证。点击<保存代理配置>即可保存已更改配置。如下图所示。

AND DOLL	RAER RACE PERIC		
(CHACTE			ditertation.
• 地址:		• 205 (0.01) (0.01) (0.01)	
• 用作品:			
• 南南:	No.		
	- ALCONECTION		

### 9.2.1.4 界面美化

界面美化支持对大屏名称、 Logo 以及主题色的修改,其中大屏名称及 logo 的修改需输入许可码,如下图 所示。



律政产品名称	aga		
个性化换肤			
话得最佳:	$ \mathbf{x} $ $\mathbf{x}$	然類5	北下和色
	88	1222	取論

参数配置保存成功后,如下图所示, 产品所涉及到上述参数的页面也将相应修改。

A*LPHA	222 h mil - Q miles		+ 9218 -	 		0	Ç +**
AART AND	8453					- OV	
1000	FFER PRe-						
-instance and						Ċ.	
17830	10/10/2009/05/2019/10		1 (D)				
+ Miner		A					
Other	Rection ( Rector )				~		
10488	N + 1 +427784						
	10 10 E				*		

### 9.2.2 数据配置

选择 "系统管理>配置管理>数据配置"进入数据配置页面。进行数据集管理。

#### 数据集管理

索引是集群用来存放数据的地方,数据集管理的作用就是对这些索引进行管理。

索引需写入磁盘中·数量随时间增长·磁盘空间占用过多会导致其性能下降·因此数据集配置设定磁盘利用上限·点击<数据集配置>·如下图所示·设置安全日志时间、流量日志时间以及磁盘利用率上限参数·若达到上限阈值·即对数据进行清理操作。

操作界面如下图所示:

intit 7	ANNA STATE					
_		對國生命原則			×	2020km-81.00100.00-2800-12-28 12-45-24
(##)	- S	8550				2.5493.2
	India and	+安全形式:	1	15		 ster -
10	ahita samatang dan 2010/127	* 西藤田市)	30	×		
10	alpha canadylog flav 2020/228	数据调制				
100	alpha camatylog fina 2020/225	• 把盘利用修上用	70%			
	alpha carwrfylog ffrai 2500/224					
10	adurta-consert prog Provi 2020/0223				<i>师</i> 券 迂原	

索引以列表的形式展现,如下图所示,包括数据集名称, 启用状态,数据集状态,操作栏。索引可进行开



2012/01/2012	<b>出用状态</b> :	20月後が20 - 日本
alpha-security/op-fox-20201227	开展	ant 🖌
aliptie security tog-frau-20201226	<b>778</b>	932
alipha-eesaritying-fran-20201225	开窗	88
alpha-cacardylog-floo-20291224	开启	
alpha-securtatog-flow-20291223	开启	
adata securta lag-flow-20201222	ffe	
ulpha securty/op-flow-20201221	开启	
alpha security top flow-20201220	評局	
alpha-securitylog-flow-20251219	并可	
elpha-security/op-flow-20251218	ΗR	

### 9.2.3 推送管理

选择"**系统管理>配置管理>推送管理**"进入推送管理页面,包括邮件服务器配置、短信服务器配置和钉 钉服务器配置三个部分,点击对用的页签分别进行相关配置。

影得聖肖觀亞麗	地位很多相处地	\$7\$TELERABELIE	S	
958A 🥶	D	S	22	
####8 <b>#</b> : mt		S c		
BBILIDAR: 🚺		. 6		
• (MIC) 456	9%	in the second se		
3(198032): Ja	difficial com	0		
· · · · · · · · · · · · · · · · · · ·				
	# 23.800	isi#		

邮件服务器配置

- ◆ 邮件服务器配置。进入邮件服务器配置页面 · 点击 **后用** · 填写邮件服务器(此处填写用户使用的邮件 系统的发件服务器名称)、端口、发件箱地址和密码 · 点击<保存>。如下图所示:
- ◆ 点击<**发送测试邮件**> ·输入一个收件邮箱 ·点击<**发送**> ·



NURGHER	经增加并非通过 化化加度分配图	
85.65		
- 即件服用器。	The summaries as an	
991,997		
• 80)	458	
· MARKER	rdəniğlur.com	
• E31		N.

#### 短信服务器配置

- ◆ 进入短信服务器配置页面,点击**启用**,填写短信 URL,点击<保存>,如下图所示:
- ◆ 点击<**发送测试短信**> ·输入一个手机号码 · 点击<**发送**> 。

\$1465.853	RIGERBEN ENTERNMEN
基本品吧:	
+ EBRL:	High Rep retire
	URLINN Mar fau setween mennerentertaken anner Tegykkey vitt Mittel an Zuck Landener Mittel Landener er und 1.755401 Zuck bergesen et 2.3017023
	(RP) MERINDER

#### 钉钉服务器配置

- ◆ 进入钉钉服务器配置页面 · 点击**启用** · 填写Webhook · 点击<保存> · 如下图所示 :
- ◆ 点击<**发送测试消息**>,选择提醒所有人或提醒指定人员,并输入其联系电话,点击<**发送**>。

BESHE CONTRACTOR
I WERDANI

# 9.2.4 系统开关

选择 "系统管理>配置管理>系统开关"进入系统开关页面, 包括 SSH Service 配置和服务器时间设置两



部分。

SSH service 默认处于开启状态,后台 SSH 可登录。若关闭,则不可登录。

服务器时间与客户端时间一致或相差小于等于 10 分钟则正常显示。

若大于 10 分钟,则工具栏中字体显示橙色,系统开关界面上显示红色, 鼠标浮动时出现异常提示。



### 9.2.5 集群扩容

页面支持集群扩容, 支持添加宿主机,支持修改宿主机组件节点数配置。

#### 操作入口

以系统管理员用户登录大数据智能安全分析平台·选择"系统管理>配置管理>系统开关"·进入系统开 关页面·在键盘按下"Ctrl+?"组合键·页面弹出集群扩容相关功能按钮·如下图所示。

	> mananı - athiani-				a sintist -	0
same same water			(	2	S	
SSH service Reproduction-see			30%		Biydantau an ar ciwat	
ante at		2		Ser la		
		.0	0			

#### 集群扩容注意事项

- 新增加的服务器设备跟原宿主机的操作系统版本必须一致。
- ◆ 集群扩容前,服务器/home/init/conf/目录下 hostinfo.json 文件不支持修改容器 IP。
- ◆ 集群扩容过程中 ・ 如果出现扩容失败等异常 ・ 可点击<下载日志> ・ 将日志发送至相关技术人员进行后 续处理。



BATHER'N			
8,000	•	Haddirs	
Exection and a	•	vert en	
eAres	•		
	•		
44		St	

#### 集群扩容步骤

步骤1. 准备好集群扩容的服务器。

注意需要保证扩容服务器的操作系统版本跟宿主机服务器操作系统版本一致。

- 步骤2. 以系统管理员用户登录大数据智能安全分析平台·选择 "系统管理>配置管理>系统开关"·进入系统开关页面,在键盘按下 "Ctrl+?" 组合键·页面弹出集群扩容相关功能按钮。
- 步骤3. 点击<**集群扩容**>按钮,进入集群环境扩容页面,如下图所示。显示已有宿主机 IP 地址和已有宿 主机的内存大小和 CPU(逻辑)核数。

如何招聘: 《	CORE CARLON CONTRACT	Q	
I marts	THE STREET	102	
	No X	集新信息 中KEDER FRENVERNDIR	
		#150P	
	TANNET PLANES THREE	a (42.1183.30.40	(20.966, dourn)
	S		T-2
	AND I IN COMPANY		
S.	HINY HILLS		
.5			
. C			
	378		
S.			
	20E		
	in the second second		

#### 步骤4. 添加宿主机或修改集群配置。

- 1) 点击<**下一步**>·展开已有宿主机集群配置。
- 2) 点击<编辑>可修改集群配置。



已有宿主机 IP 下的集群配置仅支持在最大配置范围内增加·不支持减少(新添加但尚 未执行扩容的宿主机·支持在最大配置范围内增加和减少;

执行扩容后的宿主机,视为已有宿主机)。

其中Kafka 节点最大配置范围是 3; ES 节点最大配置范围是 4; Datanode 节点最大配置是 4。如下图所示。



3) 点击<添加宿主机>·展开宿主机 IP 及密码输入框·输入正确的 IP 及 root 密码·点击<保存>·如果 IP 及密码错误·保存后会弹出相关提示;可以添加单台或者多台宿主机·如下图所示。



IN TRUE WINA	1
MAY15-025' 30	
8.04.0	ADDG 1 40-2922 BERNA DEFECTION AND A STATE OF THE ADDRESS OF THE ADDRES
	attitution and a second and a
STORAL STATEMENT	Inter Hiel Social     Caller Modeller, Resconwy
and y ministra	
U.M.	

步骤5. 确认扩容配置。

添加宿主机后·如果 IP 及密码正常·展开集群配置·可修改宿主机配置·点击<保存>·可进入下 一步操作·如下图所示。

II. Loris	0	章加格主机或總改的 ADDR主机成總改的	0 <b>日7月23日</b> 1、時間市に第主作可由	8	
	00	W主机P		Path Robert Attenned	
		kata 3	46.4	mturode: 4	85
		- 192 188 38.41	l e la	(258.3038, 48:(vm))	
- AMIAA # SEALCHE	ા	34454 (142.)	1		000 404
		-Roman's		1-9	
1.4	0				



步骤6. 扩容配置。

点击<**扩容**>·进入集群扩容流程·弹出扩容进度条及扩容日志信息·等待扩容结束。如下图所示· 扩容期间·相关集群组件和服务会被停用(扩容成功后会自动启动)。



步骤7. 完成扩容。

当前进度条达到 100% · 扩容完成 · 可进入其他页面进行正常操作 · 如下图所示 ·



HALF ADD. ADD.	
antriag'at	
A.Prod	REIV 2000     Account of the count of t
And I Conception	
aur and	Description         Description <thdescription< th=""> <thdescription< th=""></thdescription<></thdescription<>
	•
	• Barris

步骤8. 检查流计算任务。

扩容完成后,流计算任务下各引擎会自动重启,以管理员用户登录大数据平台管理界面,选择 "系 统管理>任务管理>流计算任务"进入流计算任务页面,检查各引擎是否重启成功,如下图所示, 引擎状态为Running 表示重启成功。

(前	19						ô.							
		88	HEE.	退交Yam 时间	18QFREE BIST	HIERAN	282M	HO	是否很荣 制语	提示的动 校路			18/15	
	83	相称了厚	运行规则 驾宽、储 运行规则 以23期 至上 天秋 增型、资 件用约员 实计编的 引擎	2021-02 24 09 15 03	20021-02- 246 09 11 15		100 a	Runne	ā.	3	8.0	(F.C.	25	
	ŝ	d\$\$	短取日 三、田 坂、郡仲 及古物的 引駆	2021-02 02 15-13 23	2021-02- 02*05-11 36	3101h40	) M	Ranny			Bi	92	VFIR	
	(i) (i	estrop	运行商计 留近 统 计概题的	2021-32- 25 (0-1± 24	2021-03 24 09:14: 38	adhaan	172	Barries			28	62	1245	

# 9.3 任务管理

任务管理包括流计算任务和定时任务两大功能、使用户能够实时了解引擎以及定时任务的执行动态。

# 9.3.1 流计算任务

选择"系统管理>任务管理>流计算任务"进入流计算任务页面。

流计算任务以列表的形式展现,如下图所示。列表显示名称、描述、提交Yam时间、提交Flink时间、持续时间、安全模型、状态、是否需要部署、是否自动拉起、操作(重启、停止、详情)等信息。列表中有三条记录, 分别为**规则引擎、etl引擎、统计引擎**。



増加	88										
		88	Wd	世空Yern 时间	영오FilmA 명원	1769253	9282	958	最高级要 邮寄	即古白山 拉邦	j@ft
	20	#0191#	运行规则 模型。镜 粉模型。 叫用器 包、并获 模型。信 产育动致 实功能的 石型	2021-80- 06 14:19: 20	2021-03- 09 14:19 31	10023n55 m	323	Running	a		NET 1942 1278
	e.	लगे क	(1)取日 志、福 仮、事件 及等部的 引導	2021-02- 02-15-13 23	2021-02- 02 15:13 36	elezant m	3	Rannetz		•	Sillen rite irm
	<b>a</b> 2	统计印第	运行统计 指版:统 计输制的	2021-02- 24 09:14: 24	2021-02- 24-02-14 36	24d5h	175	Running			<b>登</b> 日 将止 神情

### 9.3.1.1 历史状态

点击流计算任务名称前的 按钮 · 可查看相关引擎的历史状态 · 如下图所示 · 点击操作列中的<下载>·即 可下载引擎的日志信息。

()	Ħ								C					
		2.0	858	健QYar 间	僅Q7inn 时间	Restrict	1929	## C	RUDAN M	展高時線度 展		(Qr)	i.	
i e	-	मधनःख	运行共取機 型、統計損 係、統計機 型的引電	2020-13-21 12:40:30	2025-03-21 02-0254	Buttern 1		and the second	ē		82 4	2 29	10	
	10			1	न्द्रशह	S	8	NERROW				1812		
	100	ication_10054th	5441704_0099	ŝ	1000-12-21 12-86	24	S					予照		
	100	ication_1015455	5441704_0000	3	1020 12 27 12:01	25	0.	2020-12-21 12-4	0.26			YR		
	1410	kalor_102545	1441714_0008	-	1970-15 IN DA 20	ы "С	5	2025-12-21 12-0	ê ni			790		
	160	lication_1005451	9441704_0086	2	1420-12-14 12-15	SI CO		2025-12-19-00-2	6.23			78		
	100	sation_102545	5841704_0004	Q.	1000-12-14 09 42	M M		2020-12-14 13.1	15.26			78		

# 9.3.1.2 相关操作

1) 启动/重启

点击操作列中的<**启动/重启>**,也可勾选一条或多条,点击列表左上角的<**启动/重启**>,进行此操作时,列 表中引擎的状态变为 **Restarting**,是否需要部署为否,且操作列中启动处于**加载中**状态,不可操作,详情 处于置灰状态,不可点击,如下图所示:

A*LPHA:	Unner - en		-					10	
soors - Doory - Janasia									
140 BM									
	8.0	821-010	deressi.	-	1100	45	471895	. 81	
11.1.1.1000	STREET	200303-014030-01-07		and the	-	No. of Concession, Name		82 11 10	
DOM: NOTE: CONTRACT	STREAMER OF STREAM					and the second sec		1.144.010	
	Dividing2, 9982, PTO-DECAVOR,				.17	-		1.141.141	

#### 2)停止

点击操作列中的<**停止**> · 进行此操作时 · 列表中引擎的状态变为 **Stop** · 是否需要部署保持不变 · 且操作列 中停止和详情处于置灰状态 · 不可点击 · 如下图所示 :

A*LPHA:::: ==	U sees - and						0		1
1100 - 1000 - <b>BIBIR</b>							. V		
40.00							3		1990
		STreeds.	REVIEW	-	10.000	2. #	100405		
1	0111041_0141. N/92014	10000-0000-0		and down	10	1 sec		84.44	
CONTRACTOR .	Different of	0000000	10403407	199		2		. 81 . 10	-
1.000	U-4098 AD41. P*DIAD141.09				11 0	05		-	10

#### 3)详情

点击操作列中的详情·新打开一个页面显示 job 详情·如下图所示。

de Annes Park Contemport	3	· bi: '0	Nation 111 Constitution (2010)	
2	Available Tank First	automa S		
0 forestation	O testamine if testimoger if	Same interes	Strips #	
C Lai Manan	Renerg Sal Lat	22		
	And Rease		. Toda	(Lawrence)
	forepired told life	S.		
	annaa sairan	Deater I inches	1 fam	344 1
	100 m	6.00		

#### 4) 实时消费

电脑键盘按键"ctrl+?"··弹出<实时消费>按钮。当模型出现触发延迟或者数据出现入库延迟时·点击相关引擎<实时消费>·再点击右上方<部署>·各引擎将实时消费数据·如下图所示。

AILP	HA	S NO. O AMMO	- 100100-	+ 1215 -	9.9948	- <b>*</b> 878	81 8.88	dtie -		1000		0
n=24 / 1	(10) ave	un .								2	/	
80. B											194	
	-	-	2114481	direction in the second	Manif	10.002	88	010048	Attractat.	-		
		La malingat, 4 1985, 446 11, A0485, W PrinterChaile 198	2020 (0.0) (0.21) 10	an-o-state H	2		-	5		81		****
10.1	- 12	UNDA ME	200-0.00 21 25. 27	ution for its att att ext	1829-710		-			84	41 14 2	100
1.0		Linearent, et	1001 01 07 00 00. 01	1007103-01-98,00 44	10	198	-			81	42. PR 2	



#### 5) 是否自动拉起

- ◆ "是否自动拉起"如果是开启状态 · job10 分钟自动拉起;
- ◆ "是否自动拉起"如果是关闭状态 · job 不会自动拉起。

#### 6)部署

- ◆ 任一记录是否需要部署若为是·则<部署>按钮高亮。
- ◆ 配置变更时, <**部署**>按钮高亮, 鼠标浮动显示 "**请点击部署,配置变更在分析引擎中生效**"。
- ◆ 部署过程中,按钮不可重复点击,鼠标浮动提示: "**部署中**"。
- ◆ 部署完成后·部署按钮置灰·鼠标浮动显示"**已保持最新状态**"

### 9.3.1.3 Flink 监控

#### 1) Flink 监控

电脑键盘按键 "ctrl+?", 弹出<Flink 监控>按钮。如下图所示。

		initation in					, r	2	0		1		
am (8	-						à		1.			*	794685
		200	101	Berwaller	COTINADE.	Henney .	NAME		RADBAR .	RITINUM		3	in i
	ð	Note:	NYRDRE N NEE WE 2. READ, M PSUDREME 18	2001-11-47 (000) M	3335-05-02 9824 () 10	-	Sa	S	M		81	*1	on ann
	•	1111	TRACES AND WHICH SECURE	2020 ALC ALC 2020	unitale special and all of the second	Antering	- a	5	.8	()	81	82	on along
	-	41108	CONTRACTOR -	2021-01-01-01-00	and show table	THE	117	2m			81	40	MALES IN

点击<**Flink 监控**>进入 Flink监控页面,展示各流计算任务流向框图、流计算任务运行配置、流计算任务资源分配等信息。如下图所示。

LPHA	JURNER Resalt			)				9
aurean 1	A012		S					
	Nort III	Canhan	Angel	and the second s		vites	entrainforme (CSI)	erething and the
	M111#	5		110-11-11-11-11-11-11-11-11-11-11-11-11-	method advan	Titti	endorsetteleden Politi	
	-	unter the	unitation Angle	interio interi		Name of State	nginosadan 1993	
	in the second se	energy to any the angle of the second	analos da as Angl	analysiskaite Attis	analysis and affili	another fragmention article	Annalescha salades Annal	
			and inclusion of the Association		restFlucture section Table	and the second	mail find on particular	and and

5		5201
	pwa-secontry	SIL

option: 1000000 concerning options property	3mm_0gHLA_1010000710340	•
por instant wheeler respective and the rest.	(advert)	Entroity: some, environment
Supram, Berninger & Stationer	lanar	
opus Roomer Visioners presso	*	
spine IEEE/INVATION/AND		
one succession and the second	8	
place and an endpoint of parameters		
ngon allinasi di sedali montati ne	false -	
option BERARD CORPORATION	8	
heften: MELLINE FOR a parenter)	e	
ingrease and and and a second		
lafor: #9608/0811000.compromety.		
per without the transformation		
计算机名词源负配		C.O
apather generation is dependent	1000 VD 10040 +	* **
with Broth 1 milli	waar wa terest a	
APTOR BEATERS IN APTOR	und 2 MD 10000 is	
	Contract of the second s	OV S

#### 2) Flink 监控-流计算任务

点击<Flink 监控>进入 Flink 监控页面, 流计算任务可以下拉选择规则引擎, etl 引擎,统计引擎等。

流计算任务选择不同引擎时· 展示不同流计算任务流向框图、流计算任务运行配置· 点击框图· 展示流计 算任务指标监控。如下图所示。

rect mine	5		20					
400 M	-		3 ***		- Harrison	-		
#1141\$P	120 122	artik	Contraction of the local division of the loc	NUT:	-	(Vourse)		
1	E -			-	alline .			
	5		Contrast of	-	-			
下边选择引举			-		X			
S.			anterna -	- and the second		-		
i S				And Service of Service	10		自進中枢開展並進行責任多證程	
								-

#### 3) Flink 监控-流计算任务运行配置

点击<**Flink 监控**>进入 **Flink 监控**页面 · 流计算任务选择不同引擎时 · 展示不同流计算任务运行配置 · 支持 手动修改各运行配置 · 部分配置支持查看消费详情 ·



流计算任务运行配置修改后,需要点击页面最下方<保存>,再点击页面右上方<部署>,部署完成后,配置 生效。如下图所示。

httpRuin: 田田市田市市市市市市市市市市市市市市市市市市市市市市市市市市市市市市市市市	baas togRule 1610008715943	0
		点击可查看消费组消费详
ngRun:日世報問題 kaha為時代的)ogSource auto offset reset);	latest	目前正特: tetrot. earliest方式
ingPlate: 第二十年期間は 是己族的日期 (Stackwhiter SPHHCostTime);	taha	e so
logRole: IRCHING #2800act/Whenperakeling:	6	
logRule: 和是#法利的服务并发展(lube parakelow)	0	I SV
kgilue: 31+100000000 #33000000440/Frd.paralelerer.	0	A & A + + + + + + + + + + + + + + + + +
ngdae) gtmatalij/jgjp #380388664545m prakeen:	8	
xgRole: 新聞用MARA 推进MicriBARATAre in PartCostTime;	hise	6
Kopfum: \$198760A80H Hitselfither paralessing	6	Ap.
ogslavi: WHS(28000 F720000 paratemer):	4	

#### 4) Flink 监控-流计算任务资源分配

点击<Flink 监控>进入 Flink 监控页面 · 流计算任务资源分配展示各引擎最大并发数、内存分配、引擎槽位 等信息。

支持对内存分配、引擎槽位手动修改, 支持重置流计算任务资源分配。流计算任务资源分配修改后, 需要 点击页面最下方<**保存**>, 再点击页面右上方<**部署**>, 部署完成后, 配置生效。如下图所示。

R
/

### 9.3.2 定时任务

选择"系统管理>任务管理>定时任务"进入定时任务页面。

定时任务以列表的形式展现 · 如下图所示 · 列名包括任务名称 · 任务状态 · 触发类型 · cron 表达式 · 间隔时间等 ·



E新名称:	任务联邦	植的学校 -	crostate :	SERVICE)	HERE(N) =	任务编述	Forecomme =	傳教封甸	1011
174051	40	ADDITA		10	0	运时课程(Lalia中 的古物信息, 非能 分在内押中	2029-12-24 11 0 9-30	2020-11-04 09-2 0:01	
建铁四年4月上 数据	1847) 1	cron带油式	0.0.0.1 · MON		0	均建造改考核上 测数据	200395-12-248-0010 0100	2020-11-04 08-2 5-01	
建油放电炉上 四提	1819	cturi#ii±st	0.011-2		0	构建地动物统上 月前据	2028-12-01 01 0 D D0	3020-11-04 09-2 6:01	
mita	20	cron#Ltst	0.20 ***>		a	編算贵戶相同后 安全員際以及贵 戸倉尚勤協行書 产的細胞指数 行命會得該	2028-12-28.012 0.00	9190-11-04.09.2 9-01-	
Prates	86	REPORT		600	L.	会自然意志不开 (現以八天)的時 等数据,以均均 置数据之约的时 可就产进行停 音、统计相关严 音等数、双和音 产量的发展的可可	and a second	2020-12-17 13.4 7.47	
1.000 A (1.000 A (1.0	1847 (	CHOREEZ	100**2		0	国村田和市計算 信誉業業長、大	2029-12-28 00.0	2000-11-04 09 2 5 01	

#### 编辑

选择一条可编辑的定时任务·点击<编辑>·进入编辑定时任务页面·如下图所示·任务名称置灰不可编辑·可对初始延迟时间、触发类型、时间间隔、任务描述进行编辑。

任务名称:	NUMERICAL NUMERICAL 1
829 <u>5</u> :	
任务新述。	增度获取最近n天(原以7天)的告偿数据、采用内量预定义的规则对估产进行评规,统计各估产告偿数,获取估产最后告偿时间

#### 启用/停止

- ◆ 选择一条停止的定时任务 · 点击<**启用**> · 该定时任务会根据设置的 cron 表达式/时间间隔和最初延迟 时间去调用对应的任务接口 · 调用任务接口后 · 最后运行时间更新 •
- ◆ 选择一条启用的定时任务,点击<**停止**>,该定时任务不会调用对应的任务接口。

# 9.4 系统管理

系统管理包括升级管理和许可证两大功能,可对系统进行版本及使用期限更新等操作。

### 9.4.1 升级管理

选择"系统管理>系统管理>升级管理",可查看版本信息、在线升级和查看升级历史。

#### 版本信息



-		
	85948.0. v14 8. /vianus (COAst-140_08c-200210100 x0.7.25-pert Research v14.0. v2.1.25 (art.) vp.3.4.25-c0.1.25-pert	

#### 版本升级

#### 升级历史

显示升级历史, 内容包括升级包名称、操作人、 IP、更新时间、更新结果和备注等信息。如下图所示。

iste				G	
ranae -	995			April	
Support and a Common server, Concert of a	1000	100 (444-25) (454	and the second second	and and a second	developing and the second seco
Contrational and a lot of the paper, download the balance	100	internal facility	and show and	C Summer	00144-0-1-0 (
NAMES AND ADDRESS OF TAXABLE ADD	-	100100-10.001	Apprendiate (an and an	Committee .	الوا بيورادي (10 مريزي مسمور) و 1 ليارينيون الوا بيورادي (10 مريزي مسمور) و 1 ليارينيون
Appropriet and a press of the p	100	100,000,000	Carrierie . X	and a state of the	00-sc1210_4115_4.812
Instantia di Angliana di Anglia	1000	101.700-71.000	mention (	and a state of the	THAT COULD
Improvided (see ) 4.25 x2 5.25 and (see ) 4.25. x2 5.25 and (see ) 990000000000	-	and and the part	CO measul inary	0-89.03	(indep.L.) (40.1017); (1.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (2.1017); (
higher with all 1.00 per other metabolish per	1000	100,044,04,000	Interaction (	-44-886-815	PERMIT COMPACT CONTRACTOR
Appropriate of a \$1,000,000 million of \$1,000,000,000 million of \$1,000,000,000 million of \$1,000,000,000,000,000,000,000,000,000,0	100		Comments C	10-037-01	101011111_0000000000000000000000000000
			S		+ ## - 1 - 1 + + + + + + + + + + + + + + + +

### 9.4.2 许可证

功能简介

选择"系统管理>系统管理>许可证",进入许可证页面。

可查看系统许可证相关信息、导出许可证申请文件、导入许可证等。

目前支持 AiLPHA 大数据智能安全分析平台及 Aiview 数据可视化中心。

#### 许可证导出

展开许可延期,点击 与进,可导出许可证申请文件。如下图所示。



#### 许可证导入

点击 与入,选择许可证文件,导入许可证。如下图所示。



#### 许可证书

导入许可后,页面可查看许可证信息。如下图所示。




#### 点击**授权模块**,可展开并查看授权模块列表。如下图所示。

austi auto and

ALPHA 大教室智能在全分析平台 梁明版本: v3.6.3.1_velemee	最优限中: 使用关型: 内部制成 通俗期間: 36个月		
Duid: 26069041_5c0015 设施251 DA5_AUL 52100 自己200月间: 2023-12-15	升级他归相: 2020年12月15日 至 2023年12月15日 建設業集 - 許可範疇 -		ST#日期: 2020年12日1
<b>探</b> 珠		- Ant	後日
ALPHA Bass 安全大政策		N 12.5	-
Woden SIEM 委会遵護中心		v2.5	
Investigation 衛都冠音中心	2.	¥3:5	120
資产与风秋客運中心	ill'	W3.3	2
世界部成中心		v3-4	Se
Shenack, #08/179180-00	**	V 43.5	
SOAR 编矩跟应中心	×	¥35	-



# 10. 用户权限管理

## 10.1 日志审计管理员

账户名/密码为: opadmin/略, 登录成功后的界面, 页面只提供一个操作日志查询功能菜单, 查询条件包括:操作用户名、操作者 IP、操作模块、操作类型、时间范围。同时界面提供操作日志的详细列表以及退出窗口。日志内容包括 AiLPHA 安全分析应用日志和 AiLPHA BaaS 安全大数据平台日志两部分。

操作界面如下图所示。		
------------	--	--

AILPHAIIII . BI				23	C		0
37308					<u>)</u>		
80.0-0		1817#17		Ć,	WORK CONT		+3
sties		· ///18		000 JH			
81 88							
AUTHORIDA	1744 GasG@-8+2187715			*	2		
aniana -	MARK -	and a	annia -	Anua .		annani -	
suspective.	40.31 (41.21	No.	82	(and)		2003-49-12 11-15-24	
interne la constante de la con	0.31(41)	H1287D	(##)		82	2005-06-1211-1530	
1000	0.14.1.140	#840	HE C	(87020 )	2.5	2005-88-17 11 19-44	
-	10.94.8.8	010 TEptC: same prescripted? 000000000000000000000000000000000000		( agina	.83	2020-00-12 10-00-21	
48740 C	30.34.1.139	Referit)	THE CONTRACT	Merets.	8.4	2005-00-1271300-10	
inter l	10.14.0.0	11178403; raes percention (000000000000000000000000000000000000	****	andt		2005-09-12 11:09:00	
antes 177	10 mili	North Roll Barly, and a Spirit Will Broads/2010 Hands and Roll Barl Role and Develop Hands and Roll Barl State and State and State and State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A State and A Sta	walling of	Rinate	84	3000-00-02 17 00 07	
<u>1112</u>	6 H I I	Re-11 Section 2016 A sector 3 page 12 Bioscience 12 (1996) Re-2017 B - Bioscience 12 (1996) Re-2017 B - Bioscience 12 (1997) Re-2017 B - in Bioscience 12 (1997) Re-2017 B - Bioscience 12 (1997) Re-2017 B - 2017 B - 2		anizh		2020-00-12 Tr 00100	

通过操作用户名、操作者 IP、操作模块、操作类型、时间范围进行条件检索, 方便审计日志。

## 10.2 权限管理员

账户名/密码为: useradmin/略·登录成功后的界面· 选择用户管理可以新增和删除用户;通过角色管理· 可以新增和删除角色。

权限管理员具有角色管理和用户管理的权限。



## 10.2.1 角色管理

LPHA		s east	-0		
and an and a second					
ante.			30.0		ŝ
					•
Anon -	****	****		-	
alerst .	-				
	observed.			1	
	0000.0	FORM AND AND AND ADDRESS TO ADDRESS AND ADDRESS AND ADDRESS AND ADDRESS ADDR EXTENSION ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDR			
	COLUMN A	HARLING AND		-	
(Well-A	100000.00	NUME CONTRACTOR OF TAXABLE AND ADDRESS OF TAXABLE AND ADDRESS OF TAXABLE ADDRESS			
14997			13	1.9	
arare .	81415	935 martine		1	
n-sist		u-exceedables.des		1	
			82.		į

#### 选择"**权限管理>角色管理**"菜单进入角色管理界面,如下图所示。

系统内置 7 个角色· 分别为: 系统管理员、总部安全管理员、总部安服人员、分部安全管理员、分部安服 人员、操作审计员和用户管理员。 不同的角色拥有不同的菜单权限。

系统内置的角色不可用修改或者删除。

#### 1、 角色新增

点击 *** 按钮 · 打开新增页面 · 如下图所示。



- 新增角色名称。
- ◆ 角色类型选择 · 不同的角色类型拥有不同的数据权限 ·
- ◆ 菜单权限选择, 根据角色类型的不同,可选择的菜单权限也有所不同。
- 2、 角色编辑

点击操作列 Z 按钮 · 支持角色编辑 · 内置角色不可编辑 ·



#### 3、 角色删除

点击操作列 ¹ 按钮,支持角色删除。内置角色不可删除。

## 10.2.2 用户管理

选择"权限管理>用户管理"菜单进入用户管理界面,如下图所示。

AILPHAIIII .	elen Upon						1
and street		PERS INCOME		Salata (	- interior	S.	41
						2	
MARK 1	AZNE -	BITSHI	10.02	381	min .	Distance >	
-	dermont.	198			annes	SHIDE PERMIT	E-1008
	1.000	18			singer	pagert margin	P. R. (R. 19)
	ALC: NO.				(Jangers)	grade in technik	an in order
					2	ник (I)	4AC- 82 -

#### 1、 用户新增

点击 按钮 · 打开新增页面 · 如下图所示。

WARD AND ADDRESS OF A DRESS OF A			
ANUPHA	e 1484		E
1000 1000 40			
Arce		SG	
altern and the	- Barris and and	5 E	
1000 (A			
-			
-40. 10			
	S		
150 81499			
Desc.		5	
atores (3D			
		2	

- ◆ 基本信息包括: 用户名、真实姓名、手机号码和邮箱地址。其中用户名、真实姓名必填。
- 组织架构: 下拉可选择用户自定义的组织。
- 角色信息:不同的组织架构可选择的角色也不同。
  - 组织架构为总部时,只能选择角色类型为系统管理员、总部安全管理员、总部安服人员的角色。
  - 组织架构为分部时,只能选择角色类型为分部安全管理员、分部安服人员的角色。
  - 用户角色选择使用户拥有角色赋予的菜单功能。
- ◆ 登录绑定 : 默认关闭,可开启。类型 : IP 地址、 IP 区间、子网掩码。
- ◆ 完成账户创建 · 自动发送邮件 · 默认密码为 do*JKfn7PK · 未配置了邮件服务器或未配置了用户邮箱地 址 · 不发送邮件 ·
- 2、 用户编辑



点击操作列²²按钮,支持用户编辑。内置用户不可编辑。

#### 3、 用户删除

点击操作列 · 按钮 · 支持用户删除 · 内置用户不可删除 ·

#### 4、 重置密码

点击操作列。按钮·支持用户密码重置。

#### 5、 解锁

点击操作列》按钮·支持用户解锁

## 10.3 认证安全

in the second se 以权限管理员 useradmin 用户登录系统,可以进行认证安全设置。

### 10.3.1 登录安全设置

登录安全设置如下图所示。

```
教师学生问题
在 1989 - 26、油菜型菜生用 101
                            - that the
Reward one - particular
Horida di alla mentali all'anna -
```

### 10.3.2 密码策略设置

密码策略设置支持密码最小长度、密码最大长度、密码有效期、密码修改提醒时间、密码复杂度及密码预 期处理方式(首次登录是否强制修改密码)。如下图所示。





## 10.3.3 水印设置

水印设置模式有 IP、用户名、系统名称。如下图所示。



杭州安恒信息技术股份有限公司



# 11. 术语和缩略语

术语	解释
AI	人工智能(Artificial Intelligence)·英文缩写为AI。它是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。
Ambari	Apache Ambari是一种基于 Web 的工具 · 支持 Apache Hadoop 集群的供应、管理和监控。 Ambari 已支持大多数 Hadoop 组件 · 包括HDFS、MapReduce、Hive、Pig、Hbase、Zookeeper、 Sqoop 和 Hcatalog 等。 APT (Advanced Persistent Threat)攻击 · 即高级可持续威胁攻击,也称为定向威胁攻击 ·
APT	指某组织对特定对象展开的持续有效的攻击活动。
DDoS	分布式拒绝服务攻击(Distributed Denial of Service Attack · 简称 DDoS)是指处于不同位置的的多个攻击者同时向一个或数个目标发动攻击 · 或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。由于攻击的发出点是分布在不同地方的 · 这类攻击称为分布式拒绝服务攻击 · 其中的攻击者可以有多个 ·
EPS	每秒可以采集或者处理的事件数量 (Event per Second) · 用来表示设备数据采集和处理性能的一个指标。
ES	Elasticsearch 是一个基于Lucene 的搜索服务器。它提供了一个分布式多用户能力的全文 搜索引擎 · 基于RESTful web 接口 · Elasticsearch 是用 Java 语言开发的 · 并作为Apache 许可条款下的开放源码发布 · 是一种流行的企业级搜索引擎。
Kibana	Kibana 是为 Elasticsearch 设计的开源分析和可视化平台。你可以使用 Kibana 来搜索,查看存储在 Elasticsearch 索引中的数据并与之交互。你可以很容易实现高级的数据分析和可视化,以图表的形式展现出来。
SSL	SSL(Secure Sockets Layer · 安全套接字协议)及其继任者传输层安全(Transport Layer Security · TLS)是为网络通信提供安全及数据完整性的一种安全协议。TLS与SSL在传输层与应用层之间对网络连接进行加密。
UEBA	UEBA(User Entity Behavior Analysis · 用户及实体行为分析)·是由 UBA(用户行为分析) · 概念演进而来。UBA 最初的提出 · 是为了应对日益增长的内部(人员)威胁。但是 · 更多的 IT 资产和设备 · 即实体(Entity)的概念被渐渐引入。通过 UEBA · 异常行为分析不仅可以发现内部失陷主机 · 还能对外部网络攻击以及渗透成功后的内部横向移动有更强的洞察力。
VirusTotal	VirusTotal·是一个提供免费的可疑文件分析服务的网站。



术语	解释
WAF	Web 应用防护系统(Web Application Firewall、简称:WAF)、也称网站应用级入侵防御系统、Web 应用防火墙。WAF 是通过执行一系列针对HTTP/HTTPS的安全策略来专门为Web 应用提供保护的一款产品。
容器技术	容器技术可以有效的将单个操作系统的资源划分到孤立的组中,以便更好的在孤立的组之间平衡有冲突的资源使用需求,这种技术就是容器技术。
虚拟机	虚拟机(Virtual Machine)指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。在实体计算机中能够完成的工作在虚拟机中都能够实现。在计算机中创建虚拟机时·需要将实体机的部分硬盘和内存容量作为虚拟机的硬盘和内存容量。每个虚拟机都有独立的CMOS、硬盘和操作系统·可以像使用实体机一样对虚拟机进行操作。
	the state of the solution of t

杭州安恒信息技术股份有限公司