

云安全中心

用户使用指南

天翼云科技有限公司



修订记录

文档版本	发布日期	修改说明
06	2025/01/15	 第六次正式发布。 新增"告警通知相关"常见问题,补充钉钉机器人和微信机器人相 关配置参数获取方式。
05	2024/12/06	第五次正式发布。 ● 更新"威胁运营 > 通知管理",新增钉钉、企微通知方式。
04	2024/11/08	 第四次正式发布。 更新"安全态势 > 安全成果展示"和"安全态势 > 威胁攻击态势", 新增"设置定时刷新时间"。 更新"分析中心 > 专题分析",新增"删除图表库"。 新增"设置 > 规则标签设置"。
03	2024/10/17	 第三次正式发布。 新增"威胁运营 > 通知管理"。 新增"分析中心 > 告警查询"。 优化文档部分描述。
02	2024/08/16	 第二次正式发布。 新增"威胁运营 > 告警管理"。 更新"产品规格"。 删除"工单管理"。 删除"威胁运营 > 威胁检测 > 白名单管理"。 删除"集成管理"。 优化文档部分描述。
01	2024/07/10	第一次正式发布。

目 录

1. 产品简介1
1.1. 产品定义
1.2. 产品优势
1.3. 功能特性
1.4. 应用场景
1.5. 产品规格6
2. 计费说明
2.1. 计费模式
2.2. 升级扩容
2.3. 续订
2.4. 退订
2.5. 查看账单15
3. 快速入门19
3.1. 使用流程19
3.2. 注册天翼云账号
3.3. 购买云安全中心实例
3.4. 接入日志、告警
3.5. 查看安全概览
4. 用户指南
4.1. 安全态势
4.1.1. 安全概览
4.1.2. 安全成果展示
4.1.3. 威胁攻击态势
4.2. 资产中心

	4.2.1. 资产概览	
	4.2.2. 资产管理	40
4.3	. 风险管理	45
	4.3.1. 漏洞管理	45
	4.3.2. 弱口令管理	48
4.4	. 威胁运营	51
	4.4.1. 告警概览	51
	4.4.2. 告警列表	52
	4.4.3. 告警管理	60
	4.4.4. 通知管理	62
	4.4.5. 威胁检测	69
4.5	. 分析中心	72
	4.5.1. 日志查询	72
	4.5.2. 原始告警查询	75
	4.5.3. 告警查询	77
	4.5.4. 专题分析	78
4.6	. 编排响应	81
	4.6.1. 剧本管理	81
	4.6.2. 插件管理	
	4.6.3. 规则配置	90
4.7	. 报表中心	91
	4.7.1. 报表任务	91
	4.7.2. 报表模板	93
4.8	. 设置	95
	4.8.1. 集成配置	95
	4.8.2. 数据源监控	96
	4.8.3. 规则标签配置	97

5. 最佳实践	
5.1. 如何进行剧本管理	102
5.2. 如何进行漏洞管理	107
5.3. 如何对资产进行查看管理	
5.4. 如何进行威胁建模	114
5.5. 等级保护测评解读	117
5.6. 如何接入产品日志、告警	
6. 常见问题	
6.1. 产品咨询类	
6.2. 计费购买类	
6.3. 配置类	125
6.3.1. 数据接入相关	
6.3.2. 告警通知相关	



1. 产品简介

1.1. 产品定义

云安全中心(CT-CSC, Cloud Security Center,简称云 CSC)作为用户侧的安全中心,通过对各个主机资 产、安全设备告警日志等数据的采集对数据进行应用,通过安全数据的统一汇聚进行安全数据的统一融合化处 理,通过平台整体整合形成数据汇聚、威胁检测、告警响应的业务能力,对业务进行应急处置和统计分析,满 足态势感知、响应处置拦截、威胁预警和攻击行为溯源等目标,最终实现统一的前台展示,帮助用户实现威胁 检测、溯源、响应的自动化安全运营闭环。



云安全中心系统主要包含应用中心、安全分析中心、安全数据汇聚以及安全响应中心四大模块。

- 应用中心:提供各类安全数据的展示、资产以及风险管理,对各类安全指标进行统计分析,出具安全运营报告,实现安全系统数据的统一管理、统一运营。
- 安全分析中心:实现安全分析和数据分析,构建各类威胁模型,深度检测安全威胁,智能分析辅助安全决策,感知整体安全态势。
- **安全数据汇聚**:实现各类数据源的数据收集,实现数据服务、数据存储、数据处理以及数据采集等。

安全响应中心:实现工单、剧本以及插件工具的管理,安全编排与自动化响应处置,提升安全威胁检测能力和处置效率。

1.2. 产品优势

云安全中心作为用户侧的安全中心,产品优势如下:

安全数据全面采集

进行内部(资产、脆弱性)、外部(流量、日志)以及云端威胁情报接入等相关安全数据的全面采集,汇 聚、分析。

安全威胁深度检测

对多源安全告警进行关联分析、规则分析、情报分析等,发现潜伏的高级持续性威胁,提升告警检出率和 准确率。

安全态势集中监测

从多告警、攻击方向、攻击趋势、影响范围等多维度多视角进行态势呈现。

● 安全告警快速处置

对接联动安全防护设备,在安全告警发生时自动下发阻断策略,并在必要时下发通知预警,及时完成安全闭环。

1.3. 功能特性

云安全中心系统主要包含安全态势、资产中心、风险管理、威胁管理、分析中心、告警管理、编排响应、报表 中心、集成配置以及数据源监控等功能:

- **安全态势**:依托接入云安全中心的数据,提供统一可视化界面展示网页业务的整体安全状态。
- 资产中心: 各类资产集中展示, 全面汇集资产情况。
- 风险管理:资产风险信息清晰明确,定期更新资产漏洞、弱口令等信息。
- **威胁管理**: 对威胁全方位管理, 提供告警概览、告警管理以及威胁检测功能, 可实现各类告警灵活定制。
- 分析中心:提供日志以及原始告警灵活查询,提供多种分析专题,为用户多角度呈现数据态势。
- **告警管理**:提供云安全中心全局告警管理能力,是各类告警进行处置的入口。

- 编排响应:是企业内部定制或者沉淀的知识经验,也是安全应急响应通用告警处理的"模板"。不论是自动化的编排,还是人工的编排,都可以通过"安全剧本"来进行表述。
- **报表中心**:通过周期性的报表任务和可定制的报表模板承载各类个性化报表的展示和生成。
- **集成配置**:数据集成一键配置,实现所配即所得。
- 数据源监控:为用户提供各类数据源的展示和基本信息统计。

1.4. 应用场景

场景一:安全运营场景

为中小企业提供专业的安全运营团队,为用户提供专业的安全运营支撑。为用户提高各类威胁检测率,降低误报率。在一定程度上降低用户在安全运营上的成本,提升了安全运营的灵活性。

方案优势

- 减少无效告警:通过不同安全产品之间的数据关联,减少孤立的数据点,降低无效告警信息的产生。
- 提升告警精准度:提高告警信息的精准度,使得安全团队能够专注于真正重要的安全告警,从而提升整体 运维效率。
- 高效统一的安全运营工具:用户云上的安全工具互相独立,每种工具只能有限防范几种常见攻击。云安全
 中心提供统一的安全运营平台,帮助用户高效统一地进行安全运营。

场景示意图



、王 尤官服务	赵清	灵响应服务	里妥时期	文王保障服务	C)
1			/.		
安全中心	工单管理	知识库	剧本库		
行为分析	自动生成	威胁情报	安全场景管理 🔶		
智能预警 威胁场最分析	自动下发 快速预警	案例库	安全编排与 自动化处置		
					次立网络教训
					反广 科拉自建
-			系统分析	Ŧ	态势感知
安服解析	全数据汇聚	2 -	系统分析	Ť	态势感知 攻击行为溯源
数 振解析 数 振清洗	全数据汇聚		系统分析 响应处量	Ť	あ労感知 次去行为溯源 成肋检测预警
数 照解析 数 服清洗 数 照标签	全数据汇聚 数据提 数据提		系统分析 响应处量	Ť	质广 从设置呈 态势感知 攻击行为溯源 威胁检测预警 响应处置
数据解析 数据清洗 数据清洗	全数据汇聚 数据规 数据规 数据机		系统分析 响应处量		质广 A 按 首 呈 态势感知 攻击行为溯源 威胁检测预警 响应处置
安 敗退解析 数顯清洗 敗題标签	全数据汇聚 数据规 数据规 数据税	w 数据采集	系统分析 响应处置	Ť	50 7 4 1 2 至 态势感知 攻击行为溯源 威胁检测预警 响应处置 ↓ 设备联动
◎ 型板 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	全数据汇聚 数据规 数据规	数据采集	系统分析 响应处量	T WAF	及广体报 直至 态势感知 攻击行为溯源 威胁检测预警 响应处置 设备联动

场景二:安全合规场景

满足国家行业监管要求,帮助企业业务安全合规。帮助企业明确安全目标,系统化构建信息系统安全,降低安全隐患和攻击风险,向客户及利益相关方展示安全承诺,增强客户、合作伙伴及利益相关方的信心。

方案优势

- 全局数据整合:将不同安全能力产生的数据进行整合和分析,使企业能够全面掌握安全态势。
- 全局统一视角:整合各安全措施后,企业能够从全局视角监控和管理安全状况,提高对整体安全态势的把握。
- 全局协同效应: 各安全能力之间实现有效协同, 形成统一的防护体系, 增强整体防御能力。
- 云安全中心依托安全服务订阅模式,为企业提供个性化服务套餐订阅,事前预防,事发检测分析,事中快速响应,事后溯源。遵从合规性要求,监控预防,实时知悉系统健康情况,"御敌于城门之外"

场景示意图



场景三: 攻防实战场景

随着逐步接受和了解公有云的安全性,企业用户的重点转向了公有云'内部'的安全。根据常见的责任分担模型,云运营商主要负责云基础设施的安全,而客户则负责云中数据和应用的安全,针对云中数据和应用的攻防 实战就显得尤为重要了。

方案优势

- 提升数据关联性:通过关联和整合海量数据日志,企业可以提升运维效率,实现更加精准的监控和管理。
- 实时分析:利用先进的安全算力,实时关联和分析海量信息,有效提高运维的响应速度和决策能力。
- 高级威胁的有效发现:借助全局数据的支持,企业可以更有效地检测和应对复杂的高级威胁,提升威胁发 现能力。

 实战效果好:当前网络威胁的数量、复杂性,网络安全工作负载的增加以及攻击面的增长,专业人员经常 抱怨依赖手动流程和大量的点工具来进行威胁检测和响应。云安全中心具备全局视野,多年安全维护经验, 帮助用户实现各类威胁的检测和响应,能满足用户的实战诉求。

场景示意图



1.5. 产品规格

云安全中心为所有用户带来的主功能是一致的,产品实例主资源目前有标准版一个版本。版本详细规格描述见 "主资源规格说明"。

另外,标准版主资源支持选择购买扩展资源,用户可以通过购买额外的扩展资源,以满足更多日志分析量以及 安全态势大屏等服务的需求。扩展资源详细规格说明见"扩展资源规格说明"。



主资源规格说明

主资源目前支持标准版,版本规格说明见下表:

版本	即时通知服务	日志分析量
标准版	10000条/月	50G/月

说明:

- 标准版包含的即时通知服务为每月 10000 条,月初余量进行重置,上月未用完的不进行转结。
- 标准版包含的日志分析量为每月 50G, 月初余量进行重置, 上月未用完的不进行转结。

扩展资源规格说明

扩展资源与主资源绑定,到期时间与主资源一致。

● 云安全中心日志分析量:日志分析量的起购单位为 50G,即每次购买的日志分析量为 50G 的整数倍。

说明:

用户日志分析量可以转结(上月余下的扩展资源部分的分析量可以累加到下个月),购买后,失效日期和 主产品保持一致。

云安全中心态势大屏:提供态势大屏直观展示用户当前的告警态势以及安全成果态势,态势大屏只需购买
 一次。



2. 计费说明

2.1. 计费模式

云安全中心支持包年包月付费模式。

标准资费

云安全中心根据开通实例时选购的主资源版本、扩展资源数量、购买时长生成预付费账单。

	计费项	标准价格
主资	§源(标准版)	1600 元/月
	日志分析量	0.45 元/GB/月
」	态势大屏	4500 元/月

说明:

一个账号仅可购买一个主资源版本和态势大屏,日志分析量可以重复购买。

扩展资源规格说明

- 云安全中心日志分析量:日志分析量的起购单位为 50G,即每次购买的日志分析量为 50G 的整数倍。
- 云安全中心态势大屏:购买后,失效日期和主产品保持一致。

说明:

- 扩展资源不支持独立购买,必须在购买主资源的基础上进行叠加购买。
- 扩展资源购买后与主资源绑定,资源到期时间与主资源一致,不支持单独退订或单独续订。
- 日志分析量转结上月未使用的余量, 套餐初始赠送日志分析量每月刷新(该部分不转结)。
- 日志分析量优先使用初始赠送部分。

2.2. 升级扩容

开通了云安全中心实例后,可根据实际使用需求购买日志分析量扩展资源和态势大屏扩展资源。



前提条件

已购买云安全中心实例。

规格限制

- 态势大屏扩展资源只可购买一次。
- 日志分析量扩展资源的购买资源最小单位为 50G,即扩展资源需要购买 50G 的整数倍。

约束条件

- 同一账号在同一个区域只能开通一个云安全中心实例,对应一个服务版本。
- 云安全中心实例生效期间,支持升级购买的服务版本以及扩增扩展资源数量,但不支持降级。
- 扩展资源与主资源绑定,到期时间与主资源一致,不支持单独续订、退订。

系统影响

购买扩展资源时,原已启用的服务不会暂停,对业务无任何影响。

购买扩展资源

若当前实例还未购买某类扩展资源,则需单独购买。

- 1. 登录天翼云控制中心。
- 2. 在控制台列表页,选择"安全 > 云安全中心",进入产品服务页面。
- 3. 在左侧导航栏,选择"已购资源"。

云安全中心		产品信息
安全态势 资产中心	•	云安全中心(标准版)<
风险管理 威胁运营 分析中心	*	态势大屏
编排响应 报表中心	•	未购买 已使用(GB) 剩余量(GB) 购买日本分析量 0 100
已购资源	×	100%

4. 选择需要购买的扩展资源, "日志分析量"扩展资源、"态势大屏"扩展资源。

* 态势大屏 - 1 + 个	购买态势大屏		
	* 态势大屏	- 1 +	



购买日志分析量		
* 日志分析量	- 50 -	+ GB
说明:		

- "日志分析量扩展资源"可以设置购买数量,固定为 50G 的整数倍。
- "态势大屏扩展资源"为固定1个。
- 5. 设置扩展资源数量。
- 在页面下方确认配置费用,阅读《云安全中心服务协议》并勾选"我已阅读,理解并接受《云安全中心服 务协议》",单击"立即购买"。
- 7. 在订单页完成订单确认并支付,付费成功后,购买扩展资源规格生效。

2.3. 续订

为避免云安全中心实例到期后,服务自动停止,需要在实例到期前进行手动续费,或设置到期自动续费。

到期说明

服务到期后,如果没有按时续费,平台会冻结服务,但用户配置信息会提供15天的保留期。

- 保留期内,平台会冻结云安全中心的服务,用户配置的各类数据会继续生效,但用户无法访问云安全中心。
- 保留期满,用户若仍未续费,平台会清除实例资源,用户原有的配置信息将会被删除,同时云安全中心将
 不再获取第三方日志、用户云上资产等信息。

续订说明

- 在购买云安全中心时,支持勾选并同意"自动续订",则在服务到期前,系统会自动按照默认的续费周期
 生成续费订单并进行续费,无须用户手动续费。
- 若购买云安全中心时勾选了"自动续订",系统将会默认设置续费周期:按月购买,自动续费周期默认为 3个月;按年购买,自动续费周期默认为1年。如需要修改自动续费周期,可进入天翼云"费用中心", 进入"订单管理>续订管理"页面,在资源页面找到待修改自动续订的资源,单击操作列的"修改自动 续订",拖动"续订周期"可修改自动续订周期。



手动续订

- 1. 登录天翼云控制中心。
- 2. 在控制台列表页,选择"安全>云安全中心"。
- 3. 在左侧导航栏,选择"已购资源"。

云安全中心		产品信息	
安全态势 资产中心	•	云安全中心 (标准版) 包刷期 付表方式 到期时间: 2024-09-06 00 35-48 (距离到期还有22天)	株订 C
风险管理	Ŧ		
威胁运营	•		
分析中心	•	头的、可他化吧盐拉和分析网络女主命务,提供王国的女主殿的后息和频管,取刀用户快速响应和处置古管。	云文至甲心現费为起能供每月 50G 的口态分析制度,如果想需要制价的制度,博力外势失。
编排响应	*	土的矿	已使用(GB) 剩余量(GB)
报表中心	- '		0 100 购买日志分析量
已购资源			100%
设置	-		

- 4. 在当前实例信息展示界面,点击"续订"。
- 5. 在"续订管理"操作界面,可以根据需要进行"手动续订"或者"开通自动续订"。

费用中心	续订管理 通常规定价 查看補助 常见问题 资源被预注
总选 订单管理 · 我的订单	 1、支持目前換訂的产品吃面洋Q
特支10日半 検丁管理 退订管理 资金管理 ・	3回時1何 全裁約1例 7天内毀滅 16天内毀滅 30天内毀滅 未30回 已毀滅 自定义 云安全中心 (新仙人武器)の成法和台湾部の (新仙人武器) (新仙人武器)
撤单管理 账单管理	手动续订 (1) 自动续订 到期转按需
产品视图	社量练订 开通自动练订
发票管理 成本管理	产品名称 资源D / 订单号 资源池 资源状态 资源名称 企业项目 倒计时 续订周期 订购方式 时间 操作
合同管理	> □ 云安全中心 - 在用 - default 30 天 - 個周期 ○ 创建 2024-06-27 1002 手动気丁 ○ 到期 2024-07-27 1002 并通信均衡丁
卡芬管理 ▼	已過程: 0/1 共1条 10%页 ~ く 1 > 前往 1 页

- 6. 点击"手动续订",进入手动续订页面。
- 7. 选择续订时长,确认续订金额后,单击"确定提交"提交续订订单。



Ш	费用中心		續這	「管理/手动續订											0 π	意度评价 资源	≸被锁定 ●
€0 ()	总逐 订单管理)1、从资源编订到续订完。	tipit—tertinin	隋,16月后到期	时间以续订完成打开	eta,									
G	我的订单			产品名称	窦	₫ID			资源池	资源状态	倒计时	续订周期	时间		操作后线	订周期、到期	时间
	 待支付订单 (約订管理) 通订管理 			◇ 云安全中心			76c13		-	在用	27天	*)	(9) 创建时间:20: (9) 当前到期时间	24-06-13 17:26:09 (): 2024-07-13 17:26:04	3个月 ① 续订后 2024-10-1	到期时间: 13 17:26:04	
8	资金管理 撤单管理	•		云安全中心 —													
(III)	账单管理																
	产品视题	•	-	續订周期:	00.0	0		F 6 1		74.0			100.0			-	
2 2 0	成本管理	•		1779	277A	51'Ħ	41/H	2719月	0个月	广作用	2个月	¥个月	亚个月	1975月 續订金額:	144	¥	
0	卡芳管理														確定提	交 : 最终要用以计	軍(月 费出账为准

8. 在订单页完成订单确认并支付,付费成功后,续订生效。

自动续订

1. 云安全中心支持在购买实例时,同步开通"自动续订"。

订购 * 购买时长	1 个月	2个月	3 个用	4 个月	5个月	6个月	7个月	8 个用	9 个用	10 个月	11 个月	1年	2 #	1 个月 3 年	
自动续订	● 开启 按月购买	一 关闭 自动续订周期	为3个月:按年购	买:自动读订周期	8为1年										
🗌 我已周婆,還解	祥接受(云安全 中心	银券协议)													
	意い設美力准。7 月 5	表洋傳												1 214	立即购买

2. 若开通实例时未开启自动续订,用户也可在开通后,通过天翼云"费用中心 > 订单管理 > 续订管理",

实现自动续订启用。

- a. 进入天翼云"费用中心 > 订单管理 > 续订管理"页面。
- b. 设置查询条件,可综合利用到期时间、产品类型、是否开通自动续订查询资源。



0	续	丁管理													0	满意变评价 重香帮助 \$	如何题 资源被制
! 单 订单		 1. 支持目助 2. 如果在自 3. 对于7天时 4. 对于设置 5. 非成者订 6. 若资源到 	续订的产品档 助续订前已完 9月期的资源, 了自助换订,1 购但具有纲也 期后续费,读	国祥见 <mark>帮助文</mark> 或人工续订, 或已到期的资 且10天内到期 或建载关系的 義周期自定派	2 11同一周朝内不台 1度,不支持设置 20度原,如果用 20原,需要分别开 動丁解东开始,1	計用目动续订。 /修改自动续订。 >若该修改自动续 T通自动续订,例 +算新的服务有效	(丁周期、美術) 如(又对云硬重) 期。	自动流行、 非 2重自动流行	(波嘉计曼,可 「, 该硬盘所挂	1868日当期自动 1869日主机多期	急订已完成寻找 别名后,可能导	当前变更未生交 致整体服务不可	始)意元。 (用。				
理 理 ! ~		e Filming	28991间 云安全中心	7天内到朝	16天内致潮 ~ 第指	30天内到期 入资源D或控制的	未500 自资源D	已到期 演输入3	自定义		滚东						
		手动续订(1) 自:	动续订	到期转按需												
÷		11.11.15J	开递自己	an a													
			产品名	5称	9	e渡iD / 订单号			资源池	资源状态	资源名称	企业项目	倒计时	续订周期	订购方式	时间	操作
		· 🗆	云安全	ΦÛ	0	-	2	,		在用	-	default	26天	171	包周期	③ 创建:2024-06-13 17:26 ④ 到期:2024-07-13 17:26	手动的了 开道自动的丁

c. 定位到云安全中心资源订单后,点击操作列的"开通自动续订",设置"自动续订周期",仔细阅读《天翼云自动续订服务协议》,如果同意全部约定,则勾选"我已阅读并同意遵守《天翼云自动续订服务协议》的约定",单击"确定提交"。

										自动	加東订	关闭	1 开通
续订周期 〇 1个月	2个月	3个月	4个月	5个月	6个月	7个月	8个月	9个月	10个月	11个月	1年	2年	3年
										缬	丁金额		¥
										□ 我已闻	读并同意道守 🤇	天翼云自动续	丁酸务协议)
											讷	金橋交	\$ 39
											1.3	这 只: 要 你要用。	以计费出账为准

3. 修改自定义续订周期。

- a. 进入天翼云"费用中心 > 订单管理 > 续订管理"页面。
- b. 设置查询条件,可综合利用到期时间、产品类型、是否开通自动续订查询资源。
- c. 定位到云安全中心资源订单后,点击操作列的"修改自动续订",拖动"续订周期"可修改自动续 订周期。

										自动	加東订	关闭	1 开通
續订周期 ○ 1个月	2个月	3个月	4个月	5余月	6个月	7个月	8个月	9个月	10个月	11个月	1年	2年	3年
										绩	丁金额		¥
										□ 我已闻	读并同意道守 🔇	天翼云自动倾	订服务协议)
											3	宝藤交 [\$6 9
												道示:要终于用	以计赛出艇为准

4. 修改自定义续订开关。

- a. 进入天翼云"费用中心 > 订单管理 > 续订管理"页面。
- b. 设置查询条件,可综合利用到期时间、产品类型、是否开通自动续订查询资源。

c. 定位到云安全中心资源订单后,点击操作列的"修改自动续订",点击"自动续订"后方的关闭/开 通按钮,单击"确定提交"。

										自治	动典订	关闭	1 开通
续订周期 ○ 1个月	2个月	3个月	4个月	5个月	6个月	7个月	8个月	9个月	10个月	11个月	1年	2年	3年
										缅	丁金额		¥
										□ 我已頃	减并同意道守 🤇	天翼云自动剑	刀服务协议)
											讷		10H
											1.3	4 示: ● 修要用:	以计赛出账为准

2.4. 退订

云安全中心支持退订,可通过云安全中心控制台界面、天翼云管理中心发起并完成退订操作。

退订说明

- 云安全中心退订后,主资源及扩展资源将一同退订;扩展资源不支持单独退订。
- 成功发起退订后,实例资源将转入冻结状态,冻结期15天。冻结期间,用户配置数据会保留15天,用
 户配置的各类数据会继续生效,但用户无法访问云安全中心,15天后资源被释放,释放后无法恢复。

操作步骤

1. 进入天翼云"费用中心 > 订单管理 > 退订管理"页面,找到相应订单,点击退订。

费用中心	退订	管理									送 满意度评价 查看帮助	常见问题	资源被锁定◎
总览 订单管理	[云安全中心	~	请输入订单号	搜索								
我的订单			产品名称		资源ID / 订单号	资源池	资源状态	资源名称	企业项目	倒计时	时间	搷	IF
续订管理		>	云安全中心			-	在用		default	30天	⑤ 创建:2024-06-27 10:05: ⑤ 到期:2024-07-27 10:05:	57 54	άJ
资金管理 撤单管理		已选择: 0/1							共1条	¥ 10余/页	I ~ < 1 >	前往	1_页

 进入退订申请页面,确认退订信息,选择退订原因,信息确认无误后勾选"我已确认本次退订金额和相关 费用",点击"退订。



退订管理/ 退订申请						🙁 满意度评价	资源被锁定
 退订成功后置原不可恢复; 通订成功后置原不可恢复; 确定退订前提以完成数据 除持续均定(云电线,后指 退订可能会导致其他存在到 退订规则请查看:退订规则纳 	4份或者数据迁移;)减速尊某使两款产品,退订后资源立即释敛)以外,退订)关联业务产生影响。 9]	后的资源将被以东西形式保留15天后释战;					
产品名称	资源ID	资源池	资源状态	时间	产品金额	可退订金额	
> 云安全中心			在用	 ① 创建:2024-06-27 10:05:57 ③ 到期:2024-07-27 10:05:54 	元	元	
*请选择退订原因:						产品金额: ¥	元
● 购买云服务时选错参数()	配置、时长、台数等)					退订金额: ¥	元
 ○ 云服务功能不完善,不満, ○ 其他一服务查的性心比面; 	足业务需求						
						🛛 我已确认本次退订全领到	n相关费田
○ 云服务故障无法修复							PIELASA
○ 其他						退订	取消

3. 系统提示退订申请提交成功,可前往订单详情查看退订进度。

战的订单/ 订单详情						😑 满意度评价
订单号:	订单类型:退订 创	建时间: 2024-06-26 11:02:56 更新时间: 202	24-06-26 11:03:45			
退订完成 查看廊11单		⊘ 发起退订) 完成
产品1 退订完成						
产品	配置	订购数量	所属资源池	周期	金额 (元)	
云安全中心	-	1	-	30天	元	
						订单金额: 元 合计退订金额: 元

4. 当状态变为退订完成时,订单完成退订。

我的订单								😁 满意度评价 查看帮助 常见问题
云订单 网订单								历史订单▶
全部项目	~ 捜索订单号	Q [2023-12-30	- 2024-1	06-27 搜索			批星支付 批星取消
订单号	产品	项目	类型 7	计费方式	创建时间	状态 🛛	金额(¥)	操作
	云安全中心	default	订购	包周期	2024-06-27 10:05:17	已完成		详情

2.5. 查看账单

客户可以在费用中心按月查看在天翼云的消费概况。

账单说明



云安全中心产品为包年包月计费产品,包年包月产品采用预付费模式,即先付费再使用,一般为包年包月的购 买形式,支付成功后,云资源将被系统分配给用户使用,直到超过保留期后被系统回收。

说明:

- 当月最终账单将在次月3日生成,在次月4日10点后可查看和导出。
- 云安全中心属于按月结算的产品,当月消费可在次月3日查看账单。

操作步骤

- 1. 登录天翼云控制中心。
- 2. 在页面右上角用户名称处,选择"费用中心"。



3. 在左侧菜单栏选择"账单管理",进入"账单概览页面",可按产品类型汇总查看产品账单。

费用中心		账单概览
总览		 ③ 您可能想了解:对账指引、按需产品周期结算说明。 1、当月最终账单将在次月3日生成,在次月4日10点后可查看和导出。
订单管理	•	 CDN、VPC等按月结算的产品,当月消费可在次月3日查看账单。 、月账单概览汇总数据由多个拆分数据组成,查询结果仅作参考,不作为对账依据,实际费用以导出明细账单为准。
资金管理	•	
撤单管理		账期
账单管理		
账单概览		
流水账单		近6个月消费汇总(¥)
账单详情		金额 (¥)
导出记录		5,000
产品视图	•	3,000
发票管理		1,000
合同管理		

4. 在左侧菜单栏选择"账单详情"页面,统计维度选择"产品",统计周期选择"按账期",计费模式选

择"包周期",账期选择需要查看的账单时间,即可查看到产品的账单详情。

总览 订单管理		 您可能想了解: 1、当月最终账 2、CDN、VPC 3、月账单概览》 	对账指引、按需产品周期结算道 4 转在次月3日生成,在次月4日 等按月结算的产品,当月消费可 二总数据由多个拆分数据组成,i	^紀 明。 10点后可直看和导出。 在次月3日直看账单。 直询结果仅作参考,不作为对	账依据,实际费用以导出明细账;	单为准。		
资金管理	•							
撤单管理		统计维度 使用	量 资源 产品	统计周期 按账期	按天 明细	计费模式 包周期	按需	
账单管理								
账单概览		账期 🗎 202	23-11					123
流水账单		账期	产品名称 🍸	账单类型	官网价(¥)	优惠金额(¥)	应付金额(¥)	实付金额
账单详情		202311	弹性云主机	退款-退订	0.00	0.00	56.00	0
导出记录		202311	云硬盘	退款-退订	0.00	0.00	5.20	0
产品视图	-	202311	云硬盘	退款-退订	0.00	0.00	3.20	0
发票管理		202311	SSL VPN	退款-退订	0.00	0.00	20.00	0
合同管理		202311	弹性云 主机	很款-很订	0.00	0.00	182.00	0



费用中心		总计	4,982.46	0.00		0.00	4,982.46	
总览								
订单管理	-	汇总图表和表格						收起へ
资金管理	-	按产品类型汇总	按企业项目汇总	按计费模式汇总				
撤单管理								
账单管理	- 4							
账单概览					 云下一代防火場 弾性云主机 	¥60.00		
流水账单		¥ 4,982.46)		SSL VPN	¥80.00		
账单详情					─ 云硬盘	¥10.00		
导出记录								
产品视图	-							
发票管理								导出



3. 快速入门

3.1. 使用流程

为全面帮助您进行安全运营,您需要购买云安全中心实例并接入安全产品日志。云安全中心获取到各类日志后,能通过日志的内容进行威胁建模,完成各类安全告警的生成,辅助您进行安全处置,实现安全运营。



19



3.2. 注册天翼云账号

在购买和使用云安全中心之前,您需要先注册天翼云门户的账号。本节将介绍如何进行账号注册,如果您拥有 天翼云的账号,请跳转至使用云安全中心。

1. 登录天翼云门户 http://www.ctyun.cn, 点击注册。

G	天興石 最新活动 デ品 ダネカ家 ・ 应用高城 ・ 合作伙伴 ・ 开发者 ・ 支持与服务 ・ 了解天真云 ・	Q 中国は一 文档 控制中心 品面中心 留理中心 留景	94,095310
			\geq
	加入天翼云合作伙伴计划 巡佩高、响应快、培训全、持续为客户与伙伴创造价值		
2.	在注册页面,请填写"邮箱地址"、"登录密码"、"手机号	品",并点击同意协议并提交,如	日1分钟

内手机未收到验证码,请再次点击免费获取短信验证码。

邮箱地址	
密码	
确认密码	
+86 手机等码	
验证码	获取验证码
邀请码(选项)	
) 教已间读(中国电信天英) 云隐私政策)	日用户协议》和《中国电信天鹅

欢迎注册天留云

3. 注册成功后,可到邮箱激活您的账号或立即体验天翼云服务。

3.3. 购买云安全中心实例

云安全中心支持包年/包月计费方式,目前提供基础版的主资源,两种扩展资源:日志分析量、态势大屏。您可以根据业务规模选择云安全中心规格。



前提条件

已经注册天翼云账号并完成实名认证。

规格限制

- 态势大屏只可购买一次。
- 日志分析量扩展资源的购买资源最小单位为 50G, 即购买时只能选择 50G 的整数倍。

约束条件

- 同一账号在同一个区域只能开通一个云安全中心实例,对应一个服务版本。
- 开通云安全中心实例,必须购买主资源,可以在主资源基础上叠加购买扩展资源,扩展资源与主资源绑定,
 到期时间与主资源一致,不支持单独续订、退订。

说明:

原则上,在任何一个区域购买的云安全中心实例支持接入所在区域的日志信息,建议在购买云安全中 心实例时,根据业务所在区域选择购买云安全中心实例。

适用场景

用户购买了天翼云上的安全服务"Web 应用防火墙(原生版)、服务器安全卫士(原生版)、云等保专区等" 并部署在天翼云上。

操作步骤

- 1. 登录天翼云控制中心。
- 2. 在控制台列表页,选择"安全>云安全中心",进入云安全中心控制台。

云安全中心			
欢迎使用云安全中心 云安全中心是天翼云一站式安全管理与运营平台,它具 控制,降低用户的安全风险,提升用户安全运营效率。	·备实时监测、多维关联分析与快速响应安全威胁的能力,通过	1一体化的安全运营解决方案,助力用户实现云安全的全面管理	要和
		₹7	4
聚焦安全威胁	高效运维运营	实现降本提效	威胁快速处置
具备强大的检测能力、响应处置能力、减轻企业 安全运营负担, 聚焦实质性安全成制,	提供多元化的检测能力,体系化的响应处置能力 以及各类环境的广泛适配,相较于传统安全产 品,云安全中心提供更加完整的告誓能力,更加 高效的安全成别拼音速度。	大幅减少企业安全人员低价值的重复工作,自动 将日志转为原始告营并汇集成有效告誓,使得安 全人员可以聚集到真正具备威胁的风险上,	对接联动安全防护设备,在告警发生时自动下发 阻断策酷,并在必要时下发通知预管,及时完成 安全闭环。

3. 单击"立即购买",进入购买页面。

基础信息	
*版本选择	初曲版
* 计费模式	包年他月
扩展配置	
* 购买态势大屏	现在购买 暂不购买
* 购买日志分析量	现在购买 暂不购买
	- 50 + GB 云安全中心免费为您提供50G的日志分析额度,如果您需要额外的额度,请另外购买。
订购	
* 购买时长	① 1个月 1个月 2个日 3个日 4个月 5个日 6个日 7个月 8个日 9个日 10个日 11个日 1年 2年 3年
* 自动续订	 ● 开启 ○ 关闭 ⑤ 月月 ○ 美用 ⑤ 月月 ○ 美用 ⑤ 月月 ○ 美用 ⑤ 月月 ○ 美用

4. 选择版本信息、扩展资源、选择"购买时长"。

参数		说明					
基本信	版本选择	支持"标准版"。规格详情请参见"产品规格"。					
息	计费模式	支持"包年包月"。					
扩展配	购买态势大	默认为"现在购买",也可以选择"暂不购买"。					

参数		说明
置	屏	说明: 态势大屏只可购买一次。
	购买日志分 析量	默认为"现在购买",也可以选择"暂不购买"。 说明: 云安全中心标准版免费提供 50G 的日志分析额度,如果您需要额外的额度, 请另外购买。 日志分析量扩展资源的购买资源最小单位为 50G,即购买时只能选择 50G 的整数倍。
	购买时长	拖动时间轴设置购买时长,可以选择1个月~3年的时长。
订购	自动续订	 开启"自动续订"后,当服务到期前,系统会自动按照默认的续费周期生成续费订 单并进行续费,无须用户手动续费。 按月购买,自动续费周期默认为3个月。 按年购买,自动续费周期默认为1年。 如需要修改自动续费周期,可进入天翼云"费用中心 > 订单管理 > 续订管理"页 面,找到对应的资源进行修改。

 确认配置参数和配置费用,阅读《云安全中心服务协议》并勾选"我已阅读,理解并接受《云安全中心服 务协议》",单击"立即购买"。

6. 进入"付款"页面,完成付款。

3.4. 接入日志、告警

开通云安全中心实例后,系统默认会接入部分日志数据并对用户进行初始化配置。您可以根据自己的业务特性 修改初始化配置。

在云安全中心的集成配置页面,选择需要接入的日志类型。部分日志支持直接转告警,可以直接打开转告警开 关,云安全中心会根据内置转告警规则进行转告警配置。





操作步骤

- 1. 登录云安全中心控制台。
- 2. 在左侧导航栏,选择"设置 > 数据源监控",打开数据源监控页面。
- 3. 在操作列点击"启用",确保数据源监控处于启用状态。

数据源监控						
数3氯溴P: 请能入政策图P	1000 <u>200</u>					
Kaika日志 Syslog日志						
数据题中 资产告存		设施厂和	设备关型	80	秋章	收到最近一条日志时间 操作
10.4.1.6 Web应用防火墙(原生版)		天興云	验火爆	9092	成用中	00
				#1#	10条/页	√ < 1 → 嗣性 1 3

- 4. 在左侧导航栏,选择"设置>集成配置",打开数据集成配置页面。
- 5. 选择需要接入的日志,并打开日志接入开关。

5	日志美型	状态 日	き接入 自动時告告
	K.	已線入	
	100	已接入	
	2 m	已線入	
	3	已接入	
	100	已接入	
		已線入	
		已接入	
		未披入	

6. 选择需要转告警的日志,并打开自动转告警的开关。

E			
顺务	日志美型	状态 日志	8入 自动转告警
		己提入	
	м	日線入	
	and the second		
		日振入	
	1.003	已接入	
	£ \$	已經入	
		已經入	
	part i	未振入	

说明:

- 系统默认会接入部分日志,用户如有需要,可以自行关闭。
- 需要先在数据源监控页面启用开关后,才可以在集成配置页面中开启日志和告警配置。
- 选择需要接入的日志时,只能针对您已经购买的云产品。
- 选择需要转告警的日志,只能针对已经选择接入的日志进行。

3.5. 查看安全概览

安全概览会通过大屏的方式展示安全评分、资产总数、告警总数、告警 TOP5、日志分布 TOP5、风险资产 TOP5、告警处置概览、近七天趋势图。

前提条件

安全概览的数据来源于接入系统的数据量,需要确保已完成数据接入。具体操作请参见接入日志、告警。

操作步骤

- 1. 登录云安全中心控制台。
- 2. 在左侧导航栏,选择"安全态势 > 安全概览",进入安全概览页面,查看安全评分和风险数据统计。

说明:

- 日志、告警等维度数据展示均支持下钻点击,通过详情进行展示。
- 概览数据只展示当前情况,最新实时数据需要手动刷新页面获取。



0 00	当前整体风险处于他风险	秋志。	^{我产品数} 157			8	4雪8数 21			
80	RENCENSE, SK	OTHER.					иссении 3		松園歌舞 3	
TOP5	B S	日志分布TOP5		更多	风险资产TOP5			告替处置概范	医外毒 一 外毒虫 一 外毒虫球 一 型線	
10.192.1.315遭受DDOS攻击 2024-08-28 16:59:50	处置充成				857FDP	6705.02		- 1		
10.192.8.415i體受DDOS攻击 2024-08-28 16:50:50	处置内成		 - 改造入環 63.01% - 初南代詞 17.81% - 全局映型(内重) 10.96% - 伍思朝課 4.11% 		10.8.77.51	1	2	LURB		
10.192.1.539遭雙DDOS攻击 2024-08-28 17:22:45	处置完成			8	10.101.3.136	· · ·	-1			
10.192.1.115遭受DDOS攻击 2024-08-28 17:04:40	处重完成		■ 以证服权 4.11%	■ 认证规权 4.11%	10,192,1,115		- 1			
10.192.1.215濃妥DDOS攻击 2024-08-28 17:01:45	处置向应				10.192.1.215		- 1			
								近七日数据 ●秋重		
天趋势图							更多	2 09-04		1
2						6		3 09-03		0
1								4 09-02		0
						近七日半	均值:0	6 08-31		0



4. 用户指南

4.1. 安全态势

云安全中心安全态势页面向您展示当前云安全中心实例中已接入数据的统计信息,为了便于用户对平台数据进 行整理分析,安全态势提供安全概览、安全成果展示、威胁攻击态势三个大屏进行可视化展示。

4.1.1. 安全概览

安全概览大屏:展现安全评分、资产总数、告警总数、告警 TOP5、日志分布 TOP5、风险资产 TOP5、告警处置概览、近七天趋势图。其中告警总数、告警 TOP5、日志分布 TOP5、告警处置概览、近七天趋势图支持下钻查看详细信息。

安全概范									
SC21717 0 	三根是44.5月20日子 40.5月2 为45月9月2月1日日日,新的50	ाळ. द्वाराव्यस्ट.	^{更产品数} 157				атак 21 истана 3	новка З	٢
1 METOOS 2004 00:03 1/01:06 4 mm 14:00:13/000000000000000000000000000000000	RF CRAS CRAS CRAS CRAS CRAS	Вазилоря	 75초시문 6101% 로운타디유 1731% 오랫테니지(1) 154% 요양태대 4.11% 나고관전 4.11% 	25			t = 8 = 2 = 1 = 1 = 1	約222年4月21 - 約2日 - 化型中 - 化型用 - - 化型用 - 化型用 - - 化型用 - 	2.0
1 RETAINING	08/31	09/01	- 10 - 3000 - 10 09/02	09/03	09	远七日平 3 /04	東多 均値: 0 09/05	Utter 0+55 1 0+55 2 0+61 3 0+62 4 0+62 5 0+61 6 0+31 7 0-52	2 1 0 0 0 0 0 0 0 0 0

安全评分

评分系统根据弱口令、漏洞和告警扣分,各占40%、30%、30%。

扣分规则:【弱口令】10分/项;【漏洞】高危5分/项,中危2分/项;【告警】致命5分/项,严重3分/项, 警告1分/项。

风险等级实时更新,低风险(80-100分)、中风险(60-80分)、高风险(0-60分)。

说明:

安全评分是依据用户的弱口令、漏洞、告警进行综合计算,不同项目其分数配额相互独立。

安全概范									
安全時行 ① 	当前整体风险处于 低风险 地成将处理预管机,系统5	秋志。 此始将降低。	^{®∧≪6®} 157			8	告意品数 21 近七日新篇 3	недана 3	0
告替TOPS	更多	日志分布TOP5		更多	风险资产TOP5			告望处器概范	B S
3 10.192.1.215遭受DDOS取曲 2004-08-28 17:01:45	处置完成			357**1P	35. ⁰⁰ 19	被攻击 次第		■ 得处器 ■ 处置中 ■ 处置完成 ■	546
4 10.192.1.315遭受DDOS攻击 2024-08-2816-59-50	经置约成		■ 攻击入委 63.01%		10.198.5.243	_	8		
5 取余 10.192.8.415遭受DDOS攻击 2024-08-28 16-58-50	处置完成		 ● 原葉(石) 17,81% ● 全局关型(内面) 10,96% ● 信息期保 4,11% ● 以正規权 4,11% 		10.8.77.51	-	-2	近七天东部	
1 10.192.1.589遭党0DOS攻击 2024-08-2817222-45	处置完成				10.107.3.136		-1		
2 設施 2014-06-28 17:04:40	化医完成				10.192.1.215				
								近七日数据 🥬	
近七天趋势图							H.S	1 09-05	0
2			- 37 - 7 059 - 33					2 09-04	0
2								4 09-02	0
1						近十日平	均值: 0	5 09-01	0
0						-		6 08-31	0
08/30	08/31	09/01	09/02	09/03	3 09/0)4	09/05	7 09-30	0

资产总数

统计已经接入云安全中心的资产总数。

安全 祥分 ①	百前整体风险处于 低风险	秋志.	^{资产总数} 157		El -		^{後數函数} 21			۲
80	References and	ornan:					近七日新聞 3		导动画的画 3	
告替TOP5	黄序	目志分布TOP5		B S	风脸资产TOP5			告誓处置概范		B S
4 2024-08-28 16:59:50	处置完成				聞/**IP	被攻击次	8		■ 特比置 — 处置中 ■ 处置充成 ■ 原幣	
5 10.192.8.415通受DDOS校击 2024-08-28 16:50:50	经置流应				10.198.5.243		8			
1 10.192.1.589讓愛DDOS咬击 2024-08-28 17:22:45	处置电域		 ■ 攻击入侵 63.01% ■ 悲劇代詞 17.81% ● 宗陽術問(内面) 10.96% 		10.8.77.51	-	2			
2 10.192.1.115遵受DDOS攻击 2024-08-28 17:04:40	经置用成		● 信息制展 4.11% ■ 以证规权 4.11%		10.101.3.136		- 1		近七天告偿	
3 10.192.1.215遺受DDOS攻击 2022-08-28 17:01:45	经重先成				10.192.1.115		- 1			
a 〒10.192.1.315違受DDDS攻击	ti-Watt				10.192.1.215	2	- 1			
								北七日数据 09-05	第 中	
近七天趋势图							更多	2 09-04		
1								3 09-03		0
								4 09-02		0
								5 09-01		0
0						近七日平	均值: 0	6 08-31		
08/30	08/31	09/01	09/02	09/03	09/	'04	09/05	7 08-30		0

告警总数

统计您当前产生的所有有效告警数量,同时展示最近七日的新增数量以及待处置的有效告警数量。

0 the	制約整体风险处于 任风险 完成将处理内管成,系统5	数/ 1: Ra. UBMPHE.	57				告留总数 21 近七日新聞 3		#处理的最 3	¢
Image Image TCP5 Image Imag	83 2682 2683 2683 2683 2683 2682	Вазеточ	 数点入程 6101% 医母代数 7231% 条件数度内面) 1096% 金属制度 484 金属制度 431% 	2\$	I RANSHAPTOPS BUTTP 10.1985.242 10.197.51 10.197.3136 10.192.115	#24.54	8 2 1	1 9/19/19/19/10	21.5 = 22° = 2.5.4 = 34	3
10.192.1.115遭受DDOS攻击	经置先成				10.192.1.215		1	近七日数据 处置中		
2 1		- 22	- 7450 - 85				ĒS	1 09-05		0 0 0
0						近七日平均	始值: 0	5 09-01 6 08-31		0
Sec. Sec. 1					0.01	0.4	00/05			

近7日新增,支持下钻至告警管理页面。

全概览										
安全研7 ① 	inskalkaf 68k rafeitete. 1447	968. 2014/1946.	^{第488} 157				信管品数 21 近七日新塘 3		点击	٢
<u>육왕</u> TOP5	更多	日志分布TOP5		更多	风险资产TOP5		-	告替处置概范		更多
3 10.192.1.215遭受0DOS攻击 2014.09.29.17.01.45	处置完成				Blaub	被攻击大数				
4 []]章 10.192.1.315遭受DDOS攻击	经普先成		■ 攻击入侵 63.01%		10.198.5.243	_	8			
	公開丸広		■ 思想代码 17.81% ■ 全局所型(内型) 10.96%		10.8.77.51		2		近十天在堂	
10.192.1.589遭受DDOS校由	行要求成		 ● 信息利尿 4.11% ■ 认证授权 4.11% 		10.101.2.136		1		2. 17 M B	
2024-08-28 17:22:45 10.192.1.115遭受000S攻击	ひ間 由成				10.192.1.115		.1			
2024-08-28 17:04:40					10.192.1.215	51		近七日数据 58		
近七天趋势图							2.5	1 09-05 -		0
			**					2 09-04 =		0
2								3 09-03 -		0
1								4 09-02 -		°
						近七日平均	9值:0	6 08-31 -		0
08/30	08/31	09/01	09/02	09/03	09/	04	09/05			

告警 TOP5

提供有效告警 TOP5 的滚动展示。

F# 0	当他整体风险处于 低风趣 地动行过过雪雪后,系统	秋志。	^{资产总数} 157				^{告智总数} 21			
80							近七日紀第 3		保险重数量 3	
TOP5	更多	日志分布TOP5		更多	风险资产TOP5			告醫处醫職意		
10.192.1.589遺愛DDOS攻击 2024.08.28.17-22-85	計圖完成				资产IP	被攻击次委		保处型 处型电成 初期		
10.192.1.115遭受0005攻击	处置完成		■ 校主入侵 63.01%		10.198.5.243					
10.192.1.215遭受0DOS攻击	an Marcel		 ■ 窓原代码 17.81% ■ 金局共型(内面) 10.96% 		10.8.77.51	-	2			
2024-08-20 17:91:45	XIIITAK		 ● 信息利益 4.11% ■ 以证报权 4.11% 		10.101.3.136		-1		近七天南晉	
2024-08-28 16:59:50	处置完成				10.192.1.115	1.	-1			
10.192.8.415遭受DDOS攻击 2024-08-28 16:50:50	经营充成				10.192.1.215		- 1			
								近七日数据 📰	8	
天趋势图							更多	1 09-05		0
			二 古田 💻 唐始音雲 📖 日志					2 09-04		0
2								3 09-03		0
1								4 09-02 6 09-01		
					/	近七日平	均值:0	6 08-31		0
0	a harri	and the second sec								

点击更多,支持下钻至告警管理页面。

全概范						
安全研分 〇 	当新餐杯和加出于 经采 收 改 用成件处理的管部,系统内加	87488 157 8. NRBE.		8	作業基本 21 近七日新期 3	невва 3
1 Stations Alle Well at 15/2016 2 Biol 10/2011 10/00000588 2014-00 21 17/2016 3 Biol 10/2011 10/00000588 2014-00 21 17/2016 4 Biol 10/2011 10/00000588 2014-00 21 17/2016 5 Biol 10/2014 10/201000588 2014-00 21 17/2016 1 Biol 10/2014 10/201000588 2014-00 21 17/2016 1 Biol 10/2014 10/201000588 2014-00 21 17/2016	度 点击 20日本 20日本 20日本 20日本 20日本 20日本 20日本 20日本	9 88.76 9 98.76 9 99.76 9 9	Diff I page Diffs 16.396.4 Alths 19.877.7 Diffs 10.397.1 Diffs 10.397.1 Diffs 10.397.1 Diffs 10.397.1 Diffs 10.397.1 Diffs 10.392.1	BR/PTOPS BR0.00 5240	8 	1322月12日 - 912日 - 12日 - 12月3日 - 378 - 912日 - 378 - 912 - 912
1 xtXxxxm 1 0 08/30	08/31	 NE = BenE = Ed 09/01 09/02 	09/03		更多 3 33(前: 0 09/05	1 045 0 2 044 0 3 043 0 4 042 0 5 041 0 6 031 0 7 0530 0

点击告警消息,支持下钻至告警消息详情页面。

80	当新教体内起位于 低风貌 克成得处理告望新 系统	秋志。 风险闲降任。	157				告誓总数 21 近七日新潮 3		你忙里走着 3	
rops 点击	更多	目志分布TOPS		更多	风险资产TOP5			告禁处置概范		
10.192.1.589連受DDOS攻击 2024-08-28 17:32-45	处置完成				资/*IP	被攻击众数			特处量 — 处置中 — 处置完成 — 印略	
10.192.1.115課授DDOS政由 2024-06-28 17:94:40	处置完成		■ 攻击入侵 63.01%		10.8.77.51	_	2			
10.192.1.215遭受DDOS攻击 2024-08-28 17:01:45	处置充动		 一部館(6語 17.81%) 金陽鉄型(内面) 10.96% 信息制振 4.11% 		10.101.3.136		1		近七天祭御	
10.192.1.315遭受DDOS攻击 2024-08-28 16:59:50	处置完成		■ 以证册权 4.11%		10.192.1.115		-1			
10.192.8.415建妥DOOS攻击 2024-08-28.16:50:50	处置完成				10.192.1.215		1			
]						近七日数据 💷		
天趋势图							更多	1 09-05 -		0
								2 09-04		0
2								3 09-03		0
								4 09-02		0
						近七日平	均值: 0	5 09-01		0
0								6 08-31 -		
00/20 00/2	4	09/01	09/02	00/02	09	/0.4	09/05			

日志分布 TOP5

提供日志分布 TOP5 的展示。

安全概范										
安全研分 ① 	当前整体风起处于 低风险 网络神经潜音管站、系统风	ХБ. 224946.	³⁷⁴⁸⁸ 157				倍豐品版 21 近七日新聞 3	例北面数	13	٢
告語TOP5 4 辺原2024-08-28 16:39:50	更多	日志分布TOP5		更多	风始资产TOP5	植攻击次		告醫处實概范	- 佐齋中 仕齋充成 京略	更多
5 設計 10.192.8.415遭受DDOS攻击 2024-09-28 16:50:50	经整地成				10.198.5.243		- 8			
1 2000 10.192.1.589遺版DDOS攻击 2024-88-28 17:22:45	处置电域		 ○ 攻击入侵 63.01% ■ 思熱代码 17.81% 		10.8.77.51	-	2			
2 設施 2024-08-28 17:04:40	经重先成		 全局単型(内置) 10.96% 信息報味 4.11% 以正授权 4.11% 		10.101.3.136	24	-1		近七天告誓	
3 記論 10.192.1.215遗变DDOS攻击 2024-08-28 17:01:45	处置传统				10.192.1.115		- 1			
4 [設命] 10.192.1.315遭毁DDOS攻击	处置完成				10.192.1.215	10	-1	ift-Date and		
近七天趋势图							更多	1 09-05		2
			- 10					2 09-04		1
2								3 09-03		0
1								4 09-02 5 09-01		0
0		_				近七日平	均值: 0	6 08-31		0
08/30	08/31	09/01	09/02	09/0	3 09/	04	09/05	7 08-30		0

点击更多,支持下钻至日志查询页面


₩₩ 0 0	当新整体风险壮于 级风险 完成特化遗告等后,系统	秋志。 隐斜阵任。	^{资产总数} 157				告告总数 21			1
80 Internet	現多	日志分布TOP5		2 8	风险资产TOPS		近七日新聞 3	告望分面概念	特化型发出 3	
10.192.1.115遭受DDOS攻击 2024-08-28 17:04:40	处置完成			2	mlb.	极攻击次数			- 時社里 - 社里中 - 社里完成 - 初考	
10.192.1.215遭受DDOS攻击 2024-08-28 17:01:45	社園完成		■ 攻击入侵 63.01% ■ 原育代码 17.81%	10	8.77.51		2			
10.192.1.315遭受DDOS攻击 2024-08-28 16:59:50	社靈和成		 全局規型(内重) 10.96% 信息利禄 4.11% 	10	101.3.136		a l		近七天音響	
10.192.8.415適受DDOS改会 2024-08-28 16-50-50	处置完成		Wildebe 4.11%	10	192.1.115	•	1			
10.192.1.589遭受DDOS攻击 2024-08-28 17:22:45	处置完成			10	192.1.215		4.			
七天趋势图							B S	近七日数据 19903 =		2
			- BT - Beat					2 09-04 =		1
1								3 09-03 -		0
								4 09-02 = 5 09-01 =		0
0						近十日平	(信: 0	6 08-31 -		0
00/20	08/21	09/01	09/02	09/02	09/04	Institutes I de	09/05			

风险资产 TOP5

展示您当前系统中风险最多的 5 个资产信息

安全概范										
安全桥分 ① 	二级图45月20日十一级风险 4 我应用处理百里云,其此见	*志。 轮号神经。	**** 157				告留总数 21 近七日新酒 3		Relation 3	0
BRETOPS Ban 0142.445@c000cbba José 402.450/000bba José 402.450/000bba José 402.450/000bba José 402.470/44 Ban 0142.124@c0000bba José 402.470/44 Ban 0142.124@c0000bba José 40.2470/44 Ban 0142.124@c0000bba José 40.2470/44 José 40.2470/44 José 40.2470/44 José 40.2470/44 José 40.2470/44 José 40.2470/44	23 1200 2305 2305 2005 2005 2005	I BLINGTOPS	TREAR 6301% REPORT 1721% REPORT 1721% REPORT 471% GEORGE 411% GEORGE 411%	₹\$	I RUBERFORS BIMP 10.116.5243 10.175.51 10.192.1.115 10.192.1.215	1983.00 	x 	I OTHER	保仁王 - 杜王中 - 杜王和成 - 308 - 第17 - 近七天有学	ΠS
1 N1-740900	08/31	09/01	00 = 5600 - B# 09/02	09/03		<u>近七日平</u> 09/04	理⊅ 均值:0 09/05	Life Life <thlife< th=""> Life Life <thl< td=""><td></td><td>2 1 0 0 0 0</td></thl<></thlife<>		2 1 0 0 0 0

告警处置概览

展示近七天的告警处置情况。



译分 ①		* 1	^{产总数} 57				告曾总数 21			۲
80	当前整体风险处于 低风险 向成终处理皆器后,系统(秋志。 我应该四任。					近七日新潮 3		9000 J	
ETOPS	R S	日志分布TOPS		Q.S	风险资产TOP5			告替处置概范	みや雪 - や香中 - や香本点 - 気勝	R
10.192.1.115遭受DDOS改由 2024-08-28 17:04:40	位置完成				10.198.5.243	State of a	-1			
10.192.1.215遭受DDOS攻击 2024-06-28 17:01:45	分量完成		 取击入侵 63.01% 悪意代码 17.81% 		10.8.77.51	-	- 2			
10.192.1.315遭受DDOS攻击 2024-08-28 16:59:50	处置完成		 金局映型(内置) 10.96% 信息制程 4.11% 		10,101.3.136		-1		近七天音響	
10.192.8.415遭受DDOS攻击 2024-08-28 16:50:50	分量完成		■ 认证授权 4.11%		10.192.1.115		-1			
10.192.1.589遭受DDOS攻击 2024-08-28 17:22:45	处置完成				10.192.1.215		-1			
								近七日数据 🥬		
七天趋势图							更多	2 09-04		0
1		100 D 10						3 09-03		0
								4 09-02		0
								5 09-01		0
0						近七日平	均值: 0 🔜	6 08-31		0

点击更多,支持下钻至告警管理页面

安全概范								
安全時79 ① 	当前推注7月18日于 任7月8 为此6月七里内留前,五月47	秋志。 趙州即任	8798 157			8	告報日報 21 近七日新書 3	есала 3
2 DD 16.19.2.1158.800007826 2 DD 16.19.2.1368.800007826 3 DD 16.19.2.1368.800007826 4 DD 16.19.2.1368.800007826 5 DD 16.19.2.1318.800007826 6 DD 16.19.2.1318.800007826 1 DD 16.19.2.1318.800007826 2 DD 16.19.2.1318.800007826 2 DD 16.19.2.139.800007826 3 DD 16.19.2.139.800007826 4 DD 20.2.49.218.158.00	85 0860 0860 0860 0860 0860	Вазанторя	\$24.42 64016 #Bertis 17419 #Bertis 17419 #Gersin 4.119 #Gersin 4.119 #U2062 4.119	25	L SUBMATORS INTER 10:16:5243 10:27:51 10:10:13:36 10:102.1115 10:102.125	1975a.i.da - - -	4 14 14	1 会社会議会 日 日 日 日 日 日 日
1 HET.REDWN	08/31	09/01	10	09/03	09/0	<mark>ui te 4</mark> 3	题参 <u> 守値: 0</u> 09/05	1 0905 0 2 0904 0 3 0907 0 4 0902 0 5 0901 0 6 0831 0 7 0932 0

点击饼图,下钻至告警管理并查询对应条件的数据



	当前整体风险处于 征风险 充成特处理告答点,系统	状态。 3股间降低。	^{资产总数} 157				告留总数 21		
an a							ACCENE 2	C monartices	
2024-08-28 16-50-50	更多 startox	日志分布TOP5		更多	风殿资产TOP5	被攻击穴	1	告誓处置截范 — 侍北梁 — 北斎	中 💻 处置完成 🚃 忽略
10.192.1.589濃重ODOS攻击 2024-08-28 17:22:45	处置完成				10.198.5.243	_	-1		
10.192.1.115遭受DDOS攻击 2024-08-28 17:04:40	处置完成		 東主入便 63.01% 三章代码 17.81% 		10.8.77.51	-	2		
10.192.1.215遭受0D05咬击 2024-08-28 17:01:45	处置完成		 金局供型(内置) 10.96% 信息利採 4.11% 以口油(F 4.11%) 		10.101.3.136		- 1	254	七天雪響
2024-08-28 16:59:50	处置充成		- 1042300 TOTA		10.192.1.115		-1		
10.192.8.415違使DDOS校告 2013 05 16 16 CF 10	处置未成				10.192.1.215		1		点击
								近七日数据(绘画中	
七天趋势圈							更多	2 09-04	- 0
2						Administrator 2024-09-03 15	155 創始:	3 09-03	0
1								4 09-02	
						近七日平	均值: 0	6 08-31	0
08/30	00/21	00/01	09/03	00/02		00/04	00/05		

点击7日数据中的其中一天,下钻至告警管理,并查询当天的数据

e Maga									
82997 0 80	当前整体功能让于 包内的 用成体化理测程品、系统5	秋志。 近19月9年任。	**** 157				6日日間 21 近七日時間 3	неллия 3	0
告替TOP5	更多	目态分布TOP5		更多	风险资产TOP5			告誓於寶毗范	ž
股份 10.192.1.115 遵受DDOS 改造 2024-06-28 17:04:40	处置完成				30.750 E 343	被攻击灾政			
10.192.1.215濃度DDOS攻击 2024-06-28 17:01:45	处置未成		政法入侵 63.01%		10.8.77.51		2		
10.192.1.315遭受0DOS政击 2024-08-28 16:59:50	处置完成		● 全局映型(内型) 10.96% ● 信息射展 4.11%		10.101.3.136		1	近七天告告	
10.192.8.415遭受DDOS攻击 2024-08-28 16:50:50	处置完成		■ 以证理权 4.11%		10.192.1.115	100	1		
10.192.1.589遭受DDOS攻击 2024-08-28 17:22:45	处置先成				10.192.1.215		1	点击	
15 L T IMMO								近七日数据 (##2.2)	2
H C X 2 S PD							113×	2 09-04	1
2							-	3 09-03	0
								4 09-02	0
1						16+03/4	100 D	5 09-01	0
0			•			2005493	ant. U	6 08-31	0
08/30	08/31	09/01	09/02	09/03	09	/04	09/05	7 08-30	0

近七天趋势图

展示最近七天告警、原始告警以及日志的发生数量以及趋势,进行轮播。

○ 天翼云

全所分 ①	当年整体风险处于低风险	Rota,	^{⊛∧⊗®} 157			8	5988 21			C
80	estatescalewees. Setty	Jan Marian II.					近七日新增 3		供给圈款量 3	
た壁TOP5 2024-06-28 17-01-45	更多	日志分布TOP5		更多	风险资产TOP5			告替处置概3		3
10.192.1.315諸安(DDOS攻击 2024-08-28 16:59-50	处置完成				用 ^{mp} 10.198.5.243	800±03	8			
2024-08-28 16:50:50	经置有成		■ 攻击入優 63.01% ■ 原意代码 17.81%		10.8.77.51	-	2			
10.192.1.58%遭受ODOS攻击 2024-06-28 17:22:45	处置完成		 ● 全局映型(内置) 10.9 ● 信息利尿 4.11% 	5%	10.101.3.136		-1		近七天告誓	
10.192.1.115@@ODOSR# 2024-06-28 17:04:40	经重大成		■ Q2880 4.11%		10.192.1.115	1000	-1			
10.192.1.215遭受0DOS攻击 2024-06-28 17:01:45	处置完成				10.192.1.215	•	- 1			
								近七日数据	使置中	
化天趋势图							東多	1 0	39.05	0
			- 25 - 25:29 - 25					2 0	19-04 -	0
2								3 0	39-03	0
								4 0	99-02	0
3						NAME	物准: 0	5 0	09-01	0
0	0	•				20 01517	250IL. U	6 0	18-31	0
08/30	19/21	00/01	00/02	00/03		/0.4	00/05			

点击更多,下钻至对应的告警管理、告警查询、日志查询页面

±9634									
安全研分 ① 	当前整51风险公子 低风险 (为此前他处理的意思,其他风	秋志。 通州即任	***** 157				#11 21 近日所有 3	нения 3	0
Stations 10192.1.54%2500058/m 1000 10192.1.11/25500058/m 2000 10192.1.11/25500058/m 300.400.217/20140 300.400.217/20140 300.400.217/20140 300.400.217/20140	R# CENC CENC CENC	日志分布TOP5	 取进入使 63.01% 要用代码 17.81% 型用电弧内面 10.65% 电型电缆内面 10.65% 	更多	RUB)肥产TOPS 淡市炉 10.1985243 10.877.51 10.1013.136	1873/ab/03	x	① 免疫処理(1) (免疫型 = 2(2)* = 2(2)* = 2(2)*(2) (2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2	更多 • 5%
	公置形成 公置形成		ULERR 4.11%		10.192.1.115	•	-1 -1 	Etabas	0
2	*		89 m (542 m 135			点击 近七日平	均值: 0	2 0904 3 0902 4 0902 5 0901 6 0031	0 0 0 0 0
08/30 0	B/31	09/01	09/02	09/03	09/04	l.	09/05	7 08-30	0

4.1.2. 安全成果展示

用户从日志接收解析到最终形成告警过程全流程的过程重要的数据统计。

前提条件

安全成果展示需要购买态势大屏扩展资源,具体操作请参见升级扩容。

查看安全成果展示大屏

- 1. 登录天翼云控制中心。
- 2. 在控制台列表页,选择"安全 > 云安全中心",进入产品服务页面。

← 天翼云

- 3. 在左侧导航栏,选择"安全态势 > 安全成果展示",进入安全成果展示大屏页面。
 - 在右上角支持选择时间范围,也可以设置定时刷新时间。
 - 单击右上角的 图标,进入全屏模式。
 - 单击左上角的 图标,返回"安全概览"页面。



设置定时刷新时间

安全成果展示大屏支持定时刷新大屏数据, 定时刷新时间最小为 5 分钟刷新一次, 最大为 720 分钟刷新一次,

进入大屏默认为 30 分钟刷新一次。

您可以执行以下步骤修改定时刷新时间:

- 1. 在威胁攻击态势大屏页面,单击右上角时间范围。
- 2. 单击"停止",间隔时间变为可配置。配置完时间后,再单击"开始",即可完成修改。





4.1.3. 威胁攻击态势

用户可以查看不同级别的告警的数量统计、异常资产、高危待处理等态势。

前提条件

威胁攻击态势需要购买态势大屏扩展资源,具体操作请参见升级扩容。

查看威胁攻击态势大屏

- 1. 登录天翼云控制中心。
- 2. 在控制台列表页,选择"安全 > 云安全中心",进入产品服务页面。
- 3. 在左侧导航栏,选择"安全态势 > 威胁攻击态势",进入威胁攻击态势大屏页面。
 - 在右上角支持选择时间范围,也可以设置定时刷新时间。
 - 单击右上角的 图标,进入全屏模式。
 - 单击左上角的 图标,返回"安全概览"页面。

○ 天翼云

	威胁攻击态势	10月9日 星期三11:04:23 最近180天 关
5 (日田内) (日田内) (日田内) (日田内)	● DANUXE##20 ● DANUXE##20	日 已输认攻击告誓
KLR3937-ATOP10 File Semi-6400 1937/CC55/CC0A3L 10.37/5/1 C034-96-27 11 C04474-VD257-0 10.1013.131 C03449-27 10 24/1447-4/055-0 10.1013.131 C03449-27 10 24/1447-4/055-7 10.1013.13 C03449-27 10 24/1447-4/055-7 10.1013.13 C03449-27 10 24/1447-4/055-7 10.1013.13 C03449-27 10 24/1447-4/055-7 10.1013.13 C03449-27 10 20149-27 10	 第 告密 第 68 第 692003 第世纪0038日 第 202133 第世の058日 第 692033 第世の058日 第 69233 第世の058日 第 69233 第世の058日 第 12533 第世の058日 第 12535 第世紀 1058日 第 12535 第世紀 1058日 第 12535 第世紀 1058日 	
	日空分実統計 TOPS ● ■ ■ ● 43 ● 43 ● ■ ■ ● 43 ● 43 ● ■ ■ ● 43 ● 43 ● ■ ■ ● 43 ● 43 ■ ■ ■ ■ ● 43 ● 43 ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	告集時长記券 25 26 15 0 9 9/10 09/14 09/18 09/22 09/26 09/30 10/04 10/08

- 4. 单击右上角的 图标,进入全屏模式。
- 5. 单击左上角的 图标,返回"安全概览"页面。

设置定时刷新时间

威胁攻击态势大屏支持定时刷新大屏数据,定时刷新时间最小为5分钟刷新一次,最大为720分钟刷新一次,

进入大屏默认为 30 分钟刷新一次。

您可以执行以下步骤修改定时刷新时间:

- 1. 在威胁攻击态势大屏页面,单击右上角时间范围。
- 2. 单击"停止",间隔时间变为可配置。配置完时间后,再单击"开始",即可完成修改。



	威胁攻击态势		11月08日星期五09:10 最近24小时 🔀
■ 风始资产 □ □ □ ② ■(④) (注册(⑤) ■ ●	● P納以攻击成功 ● P納以攻击成功 ② 数命 ● 0条 ③ 数命 ● 0条 ③ 数命 ● 0条 ③ 数命 ● 0条 ③ 33 ● 0条 ○ 第 ● 0 ○ 第 ● 0 ○ 第 ● 0	D条 D条 D条 C C C C C C C C C C C C C C C C	学用時間 現在書書 今天 :: 最近24小时 最近30天 最近180天
风险资产 TOP10 	 音響 ● 15.05… 192.168.0.66发 15.09… 192.168.0.66发 15.09… 192.168.0.66发 15.09… 192.168.0.66发 15.09… 192.168.0.65% 15.05… 192.168.0.57% 15.06… 192.168.0.57% 15.06… 192.168.0.9% 	原始告警 3日 11.10.00 云号秋上10候 11.10.35 云等禄上10侯 14.01 云等禄上10侯 14.04云等禄上10侯 14.05.云等禄上10侯 14.05.云等禄主10侯 14.65.云等禄专区 We. 14.53.云等禄专区 We. 11.22.36 云等禄专区 下	日本100 500 100 100 100 100 100 100 100 100
告尝类型 防端口 注描 建他WE 的改击	告醫分类統计 TOPS	● 新禮 ● 研 ● 熟	告罄增长趋势 35 20 20 10 10/10 10/15 10/20 10/25 10/30 11/04

4.2. 资产中心

为了便于租户对平台资产数据进行整理分析与管理,资产中心提供资产概览、资产管理两个便于管理资产的功能。

前提条件

- 已开通云安全中心实例。
- 具有云上资产数据。

4.2.1. 资产概览

资产概览显示资产总数、风险资产数、服务器离线数量、Agent 安装率和安装数量,安装软件 TOP 排行 (支持倒序和正序),操作系统分布,开放端口号 TOP 排行(支持倒序和正序)。



云安全中心	资产概览					
安全概范 🔹	资产总数	风险资	^{午数} 服务器离线数	Ch. ag	gent安装率	安装数量
资产中心	82 *	ν Ο 🛉	I2 ↑	9	90 %	73
资产管理	操作系统分布		安装软件TOP5	正序 创序	开放端口TOP5	正序 倒序
风险管理			软件名称	数量	端口号	数量
威胁运营			ncurses-base	38	22	49
分析中心 👻			hostname	23	111	40
工单管理	•	centos 40 40.00	% libxml2	22	135	17
编排响应 👻		windows 30 30.00 ⁴ linux 20 20.00 ⁴	% kpartx	21	5678	30
报表中心 👻		ubuntu 10 10.00	% os-prober	21	5679	30
已购资源						
设置 -						

4.2.2. 资产管理

为租户提供资产及资产属性的查询功能。

云安全中心		资产管理								
安全恋劳 (治产中心) (洗戸概念)	•	 ● 添加条件 								TH IR
资产管理 风险管理 成款运算		 ご 更新治产 数件状态 	最高安装安全卫士	主机名称	云突厥时间	云资源领理时间	發Pitp	词用区	握作系统	要作
分析中心		运行中	已安號	eom-loglog2	2025-02-19 18:23:29	2024-08-19 18:23:16		on-xinan1-1A	centos	22
编移电应	-	运行中	已安装	csc+est-0826-2	2025-02-26 15:41:10	2024-08-26 15:40:54	f	on-xinan1-3A	linux	12
报表中心		运行中	已安装	P-96b7-HbNI	2123-12-09 11:22:13	2024-01-02 11:21:54	6	crivinan1-2A	centos	20
已购资源		遗行中	已安装	ecm-d409	2024-10-20 19:53:33	2024-08-20 19:53:18	1	azž	linux	20
12.00		日刻期	已安装	P-9667-1LTF	2024-01-28 09:54:53	2023-12-28-09:54:33	A	cn-xinan1-2A	centos	20
		(日别期	已安装	P-96b7-igs8	2024-02-06 17:35:14	2024-01-06 17:33:47	4	cn-xinan1-2A	centos	20
		日知期	已安装	P-96b7-aHfn	2024-02-24 18:24:08	2024-01-24 18:23:55	£ %22	cr-xinan1-1A	centos	22
		84135	已安徽	P-9667-6K2Q	2024-05-31 09:15:32	2024-01-31 09:14:26	DCES.	on-xinan1-2A	centos	22
		日知時	已安朝	P-96b7-bupg	2024-03-02 17:52:29	2024-02-02 17:51:18	CFLUE	crissinan1-2A	centos	2 8
		日列期	已安装	P-9667-LagA	2024-02-24 18:24:12	2024-01-24 18:23:58	D3curar/varia	cn-xinan1-1A	centos	20
		已别期	已安装	P-9667-wAu1	2024-03-23 15:35:34	2024-02-23 15:35:19	Linearest assource and reaction (60)	cn-xinan1-1A	centos	20
		日到期	已安装	P-96b7-ChdH	2024-03-04 18:01:49	2024-02-04 18:00:42	C4 57D	cn-xinan1-3A	centos	20
		日至188	已安装	P-96b7-bVre	2024-03-04 18:25:00	2024-02-04 18:24:03	BF21 Provide State	ch-xinan1-2A	linux	22
		编行中	已安緒	ecs-c-adapter	-	2024-03-08 10:19:57	FC	cr-xinan1-1A	centos	112
		运行中	已安装	P-96b7-Umus	~	2024-03-19 14:58:54	390000	cn-xinan1-1A	centos	2.0
		遗行中	已安装	P-96b7-Fgrr	-	2024-03-14 09:08:13		cn-xinan1-1A	centos	28
		运行中	已安装	ecm-proxy	-	2024-03-15 20:25:37	295	on-xinan1-1A	centos	亚雅
		這行中	已安装	P-96b7-RCQA	-	2024-03-19 14:58:54	Concerns and a surrow A39.	cr-xinan1-1A	centos	2 0
		日共机	已安顿	c-plat-heying-lb-ecs-vpc-tfcetzp3pr-1711076353	2025-03-22 16:02:24	2024-03-22 16:02:09	3	cr-xinan1-1A	centos	22
		包用精已退订	已安緒	edr-nct-ah-15	2025-03-21 15:40:21	2024-03-21 15:40:02	2E	cr-xinan1-1A	centos	18

與157張 < 1 2 3 4 5 6 8 > 20版/页 →

选择常用搜索项查询。



llife - v "ecm-loglos" ×							×	169
総原項: 本状态		安全卫士agent是否在线 虚拟私有云名称		操作系统版本 安全		 1.点击搜索框 2.点击搜索选 3.输入搜索条 	 щ	
30 20 4.5 M	BROKOATL	+#01	2.0038364936463	2.80866804G	WITTO	4.查询搜索过	滤展示	
90~400 2050	Pris	±86044	2025-02-19 18-23-29	2022408-19 18-23-16	36/10	PEHSIA.	Series Incol	58D

查询条件组:保存查询条件,方便用户快速查询。

资产管理							1 查询已促在条件		
							2.新增已保存查询条件		50 98
۲	④ 源加条件						已保存查询条件组		
							想可以新增查资务件组、以便	TARBER	
0 更新	班/**							8122	
	资产状态	是再安装安全卫士	主机名称	云安原到期时间	云表還包建的詞	資产ID	可用区	操作系统	操作
	遂行中	已安装	ecm-loglog2	2025-02-19 18:23:29	2024-08-19 18:23:16	E	cn-xinan1-1A	centos	22
								共1条 < 1	> 20傑/页 ~



资产管理							
主机名称 = ~ *e	rm-logioj ^{a s}					×	
 ③ 添加条件 		保存查询条件组	x		已保存查询条件指		
o Hann					✓ ■REEReem-logicg		
n o kenso no kenso	最高安装安全卫士	· 會須集件進名称。		東产10	清空	另符为 保存	Re
還行中	已安装	B. C.		6-11-11-11-11-11-11-11-11-11-11-11-11-11	crysinan1-1A	centos	28
		9623					
		BZ/Pressule					
		是否保存意向时间。					
			Ring Bitter				

添加条件查询。



○ 天翼云

资产管理									
	资产状态 = 包周期已退订 ×	① 添加条件	+处理按钮,实现条件的启用、禁用以	及删除					
288A									
全部懸用 全部删除									
	资产状态	是否安装安全卫士	主机名称	云资源到限时间	云资源创建时间	资产ID	可用区	操作系统	操作
	包周期已還订	已安装	edr-nct-ah-15	2025-03-21 15:40:21	2024-03-21 15:40:02	20000000 0000 0000 0000	cn-xinan1-1A	centos	2 2
	包周期已退订	已安装	c-plat-heying-lb-ecs-vpc-i1011tfpyy-1711006195	2025-03-21 15:40:24	2024-03-21 15:40:07	91	cn-xinan1-1A	centos	22
	包周期已退订	已安装	csc-test-0826	2024-08-26 15:37:38	2024-08-26 15:27:31	21 - com anar cono anasnerað	cn-xinan1-1A	linux	放 符
								共3条 〈 1 〉	20銀/梵 ~

字段筛选:对查询结果栏进行字段的选择和移除

安全中心	<	资产管理							
3产中心	^								
资产概况		 ④ (④) 添hn各件 							
资产管理									
脸管理	^								
還洞管理		こ 更新资产							J.
弱口令管理		云资源创建时间	云资源到期时间	是否安装安全卫士	资产状态	主机名称	资产重要性	操作	已选字段
防运营	^	2024-10-21 14:43:27	2025-01-21 14:43:41	已安装	已关机	AQZQ-AF-vpo-o-plat-1442	普通资产	童若	云资源创建时间
	2	2024-10-21 14:43:26	2025-01-21 14:43:42	已安装	已关机	AQZQ-CSSP-vpo-o-plat-1442	普通资产	查看	云资源到期时间
口言 ^{言 注} 告誓列表		2024-11-28 13:57:16		已安築	已关机	ctosz-testdb	普通资产	重著	是否安装安全卫士
通知管理	~	2024-11-28 15:34:31	=	已安装	运行中	ctcsz-testdb	普通资产	查看	资产状态
或肪检测	~	2024-12-02 10:48:31	-	已安装	已关机	ctcsz-testdb	普通资产	查看	主机名称
7ŧ¢Ú	~	2024-11-29 10:21:20	<u>41</u>	已安装	已关机	ctosz-testdb	普通资产	查看	资产重要性
的应	~	2024-11-29 09:42:22	-	已安装	已关机	ctosz-testdb	普通资产	查看	待选字段
剧本管理		2024-12-02 14:42:18	2	已安装	120	ctosz-testdb	普通资产	主管	〇遺輸入搜索侍选字段
香件管理		2024-10-08 16:28:06	2025-02-08 16:27:13	未安装	运行中	dba-test1081	普通资产	童香	安全卫士agent是否在线
规则配置		2024-06-25 13:52:18	2024-12-25 13:53:29	未安装	运行中	dba-顶航资产机勿删	普遍资产	主旨	资产更新时间
中心	~	2024-11-12 20:03:46	-	未安装	已关机	clean-ctosz-agent	普通资产	直着	虚拟私有云名称

更新资产信息。

资产管理								
								查得 重要
③ 资产状态 - 包房期已通订 ×	③ 添加条件							
	能获取最新资产状态							
资产状态	最否安装安全卫士	主机名称	云资源到期时间	云资源创建时间	资产ID	可用区	操作系统	操作
包周期已进行	日安装	edr-nct-ah-15	2025-03-21 15:40:21	2024-03-21 15:40:02		cn-xinan1-1A	centos	王帝
包周期已进行	已安装	c-plat-heying-lb-ecs-vpc-i1011tfpyy-1711006195	2025-03-21 15:40:24	2024-03-21 15:40:07	\$	cn-xinan1-1A	centos	推 着
包周期已退订	已安装	csc-test-0826	2024-08-26 15:37:38	2024-08-26 15:27:31		cn-xinan1-1A	linux	素容

查看资产详情,资产详情包括资产信息和脆弱性信息组成。



管理									
							9	重約	-
④ 主机名称 - ecm-d409 ×	④ 添加条件								
こ 更新资产							点击查看,展示资	医产详情	
東产秋志	是否安装安全卫士	主机名称	云安置领期时间	云灾遭创建的词	奥PID	可用区	提作系统	1	ante 1949
运行中	Eexe	ecm-d409	2024-10-20 19:53:33	2024-08-20 19:53:18		az2	linux		<u>88</u>

资产信息展示如下图:

8产详情				
资产信息 胞羽的	性信息			
基础信息	■ 基本信息			
基本信息	主机名称: ecm-6409	主约D: 14	资产状态: 运行中	
管理圈性	Hirfs#38: linux	摄作系统版本:	唐原私用云名称: vpcb	
开放调口	法资源创建时间: 2024-08-20 19:53:18	云原题形明时间: 2024-10-20 19:53:33	1936: -	
同中信息	可用区: ar2			
8户信息	委会通: Default-Security-Group [sg-tm7rti8ve5]			
安装软件				
	(言) 管理尾性			
	是否实地安全卫士: 日 安装	安全卫士agent是否在境: 在线	旅产重要性: 普通资产	
	● 开台端口(3)			
	96D	19302	型可1P	遊覧D
	22	scp6	8	1515
	111	tcp	0.0.0.0	603
	25	tcp	127.0.0.1	1139
				< 1 > 共3 依 載述 1 5
	(B) 网卡信息(1)			
			272	22
	同卡名符	macibit	IPv4	IPv6

资产信息展示基础信息的丰富程度和购买的安全产品相关(购买了服务器安全卫士(原生版)或者云等保专区

的主机安全产品后其基础信息会更加丰富)。

脆弱性信息如下图:

15		遍到白藤结果		凝结检测结果		账号检测结果	
● 告誓(致命)数/已处置数	0/0	1 減雨急数	1477	 检察不合现数/已处置数 	0/0	奇 弱密码数/已於置数	0,
告答(严重)数/已处置数	0/0	☆高危潮洞/已处置数	521 / 0	◎ 检测合规数	0	④ 最新发现时间	00-00-00 00:00:1
)告罄(告罄)数/已处置数	2/0	中危漏洞/已处置数	810 / 0	 重新发现时间 	00-00-00 00:00:00		
) 開始告答(過醒)数/已处置数	0/0	▲ 低危識洞/已处置数	146 / 0				
		 · ·	2024-09-05 11:19:55				

○ 天翼云

4.3. 风险管理

云安全中心风险管理提供给用户漏洞管理和弱口令管理的能力。

前提条件

- 已开通云安全中心实例。
- 具有云上资产数据。

4.3.1. 漏洞管理

为租户提供漏洞查询及处置功能。

云安全中心		漏洞管理								
安全概览 资产中心	•	漏洞名称	请输入		澱洞等级 请选择		CVE編号 请输入			音响 重置
风险管理 漏洞管理	•	忽略	修复中 已修复	ema						
弱口令管理			漏洞名称	CVE编号	漏洞等级	处置状态	服务器	最后发现时间	更新时间	操作
威胁运营	*		and a	100,000.1	高危	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
分析中心	•		1000	C	高危	•已修复	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 直看
工单管理		•	-	100.001	高度	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-05 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
编排响应				(111 MIL 3	中危	• 待修复	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 直看
报表中心	•		100		低段	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已加固 直看
已购资源			and the		高危	• 待修复	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 直看
设置	*		March 1	100,000	商起	• 忽略	ecm-ceshif825d35f-17fe-3162-0e68	2024-02-20 11:15:27	2024-03-11 11:15:17	修复中 已修复 已加固 查看
			1000	1000.000.0	高危	• 待修复	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 直着
			100) ·	distant of	低危	• 修复中	ecm-ceshif825d35f-17fe-3162-0e68	2024-01-09 11:15:27	2024-03-11 11:15:17	忽略 已修复 已加固 直看
			10,1	atten	中度	• 待修复	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-01 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 查看

条件查询

支持条件查询,用户输入或选择相关条件内容。



云安全中心		漏洞管理				/	输入或选	点击			
安全概览 资产中心 风险管理	•	漏洞名称 服务器	请输入		漏洞等级 ? 处置状态]	南范 清选择	~	CVE编号 最后发现时间	请输入 箇 开始日期 - 线束日期		điğ 11 12
混河管理 弱口令管理 威胁运营	•	215	修复中 已修复 凝洞名称	已加回 CVE编号	混涡等级	处置状态		服务器	最后发现时间	更新时间	损作
分析中心 工单管理	·		10.1	-	高危	• 已加固	ecm-ceshif82	5d35f-17fe-3162-0	2024-03-11 11:15:27	2024-06-21 15:22:49	忽略 修复中 已修复 直看
编排响应 报表中心	•		18.1	C = 2	商危	• 已加固	主机名称_568	25d35f-17fe-3162-	2024-03-11 11:15:27	2024-06-21 14:53:48	忽略 修复中 已修复 直看
已购资源 设置			10.1	Chinese.	高度	 忽略 已加固 	ecm-ceshif82 ecm-ceshif82	5d35f-17fe-3162-0 5d35f-17fe-3162-0	2024-03-11 11:15:27 268 2024-03-11 11:15:27	2024-03-15 10:43:47 2024-03-15 10:43:35	修复中 已修复 已加固 查看 忽略 修复中 已修复 查看
			100	reaction in the second se	高危	 已加固 已修复 	ecm-ceshif82 ecm-ceshif82	5d35f-17fe-3162-0 5d35f-17fe-3162-0	2024-03-11 11:15:27 208 2024-03-11 11:15:27	2024-03-15 10:43:35 2024-03-12 18:25:45	忽略 修复中 已修复 查看 忽略 修复中 已加固 查看
				-	高危	 已修复 已修复 	ecm-ceshif82	5d35f-17fe-3162-0	2024-03-05 11:15:27	2024-03-12 18:25:45 2024-03-12 18:25:45	忽略 修复中 已加固 查看 忽略 修复中 已加固 查看
			100.0	100,000.0	高危	 待修复 	ecm-ceshif82	5d35f-17fe-3162-0	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 查看

处置漏洞

提供处置能力,可直接或批量修改漏洞处置状态。状态枚举值:修复中、已修复、忽略、已加固等(此处修改 漏洞状态仅用于云安全中心展示使用)。

云安全中心		漏洞管理	!									
安全概览	•	漏洞名称	R 请输入		漏洞等级	高危	×	CVE编号	请输	λ	\odot	查询 重置
风险管理		服务者	8 请输入		处置状态	请选择	÷	最后发现时间		开始日期 - 结束日期		
漏洞管理			批量如	上置								
弱口令管理		約略	修复中 已修复	etala								单个处置
2011년官	Ť		漏洞名称	CVE编号	漏洞	等级 处置状	ð	服务器		最后发现时间	更新时间	10/6- 27(17
单管理			100.2	(高	8. • Em	ecm-ceshif8	25d35f-17fe-3162-0)e68	2024-03-11 11:15:27	2024-06-21 15:22:49	忽略 修复中 已修复 直看
耕助成		1	10.1		765	tit • 忽日	主机名称_5	825d35f-17fe-3162	-0e68	2024-03-11 11:15:27	2024-06-21 14:58:03	修製中 已修复 已加固 適香
表中心		0	100.0	The self it.	商	1. etc	面 主机名称_5	825d35f-17fe-3162-	-0e68	2024-03-11 11:15:27	2024-06-21 14:53:48	忽略 修复中 已修复 直著
购资源			100.0	10.0014	商	这 • 忽日	ecm-ceshif8	25d35f-17fe-3162-0)e68	2024-03-11 11:15:27	2024-03-15 10:43:47	修复中 已修复 已加固 遺香
m	•		100.1	UR. State.	高	8 • Ebb	面 ecm-ceshif8	25d35f-17fe-3162-0	0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
			100.0	Cortes	商	• Eta	固 ecm-ceshif8	25d35f-17fe-3162-0)e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 直著
			100.0	till inner	7857	• 已修	ecm-ceshif8	25d35f-17fe-3162-0)e68	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查考
			100,0	10,000	高	8.	更 ecm-ceshif8	25d35f-17fe-3162-0)e68	2024-03-05 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 直著
			10.1	100,000,0	高	· 已修	复 ecm-ceshif8	25d35f-17fe-3162-0)e68	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
			100.0	-	高	8 • 待修	雙 ecm-ceshif8	25d35f-17fe-3162-0	0e68	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 查看

修改处置状态可填写处置说明,便于后续查看状态变更原因。



云安全中心		漏洞管理								
安全概览	-		口为修复中						~	前面
资产中心		TON:	口//1%复中						^	
风险管理	*	•	确认要把该遗洞标记	3为修复中吗?						
漏洞管理		2	淵源	名称	cv	E编号	影	响服务器		
剪口令管理		6		601	5.00 j	(ma)	ecm-ceshif825d35f-17fe-3	3162-0e68-d10676d09b781.1.1	.5	操作
威胁运营	×	8		成个空的					49	忽略 條复中 已修复 直香
分析中心	•		aing million (Langer State) (Langer	1.11.12					03	修复中 已修复 已加固 查看
工单管理		4 0							48	忽略 修复中 已修复 查看
编程响应	*	1 6							33	忽略 修复中 已修复 直看
报表中心	*	C				取消	保存		20	忽略 修复中 已修复 已加固 查看
已购资源			名称_5	CVE_2024_5	商餘	• 約略	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:47	修复中 已修复 已加固 直看
设置	*		名称_4	CVE_2024_4	453	•修复中	ecm-ceshif825d36f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:43	忽略 已修复 已加固 直著
			名称_5	CVE_2024_5	商意	• 已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 直着
			名称_5	CVE_2024_5	低数	• 已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
			名称_5	CVE_2024_5	商設	• 已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 直看

查看漏洞详情

在漏洞详情中,可以查看所有历史状态变更记录的信息,包括:处置人、处置状态、处置说明、处置时间等。

云安全中心		漏洞管理								
安全概范	•	漏洞名称	请输入		漏洞等级 高危		 VE编号 请输入 		\odot	查询 重要
资产中心	•									
风险管理 漏洞管理	*	208	修复中 已修复	Elhola						击点
弱口令管理			漏洞名称	CVE编号	漏洞等级	处置状态	服务器	最后发现时间	更新时间	操作
威胁运营	*		名称_5	CVE_2024_5	高危	• 已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-06-21 15:22:49	忽略 修复中 已修复 查看
分析中心	•		名称_5	CVE_2024_5	商危	• 忽略	主机名称_5f825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-06-21 14:58:03	修复中 已修复 已加固 查看
工单管理		•	名称_5	CVE_2024_5	商盘	• 已加固	主机名称_5f825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-06-21 14:53:48	忽略 修复中 已修复 查看
编排响应	•		名称_5	CVE_2024_5	商危	• 忽略	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:47	修复中已修复已加西 查看
报表中心	•		名称_5	CVE_2024_5	高危	• 已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
已购资源			名称_5	CVE_2024_5	高危	• 已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
设置	•		名称_5	CVE_2024_5	高危	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
			名称_5	CVE_2024_5	高危	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-05 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
			名称_2	CVE_2024_1	高危	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 直看
			名称_5	CVE_2024_5	高危	•待修复	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 查看
漏洞详情							×	¢		
漏洞名称: 名	5称 2									
CVE编号: C	VE_2024_1		漏洞级别	商范						
服务器:名称	K_2f825d35f-17	7fe-3162-0e68-d	10676d09b781.1.1.2							
处置历史:										
	处置人		处置状态	处置	说明		处置时间			
	超级管理员		 已修复 	22	222		2024-03-12 18:25:45			
	超级管理员		•修复中	11	111		2024-03-12 18:25:36			
	超级管理员		 已修复 	批量测试	式修复中		2024-03-12 17:29:17			
	超级管理员		 已修复 	批量测	式修复中		2024-03-12 17:28:07			
	超级管理员		 修复中 	批量处	置修复中		2024-03-12 17:27:42			
	超级管理员		• 忽略				2024-03-12 17:26:25			

查看漏洞关联资产

每条漏洞能够关联资产信息,可快速查看关联的资产详情。



云安全中心		漏洞管	理								
安全概范 资产中心	•	漏洞名	5称 请输入			漏洞等级 高危		✓ CVE编号	请输入	\odot	查询 重置
风险管理 漏洞管理	•	20	略修复中	已修复	2加雨				点击		
弱口令管理			漏	洞名称	CVE编号	漏洞等级	处置状态	服务器	最后发现时间	更新时间	操作
威胁运营	*			1. A	10,000	商品	• 已加固	ecm-ceshif825d35f-17fe-3162-Det	68 2024-03-11 11:15:27	2024-06-21 15:22:49	忽略 修复中 已修复 查看
分析中心	*			1.1	10,000	高段	* 忽略	主机名称_51825d35f-17fe-3162-06	e68 2024-03-11 11:15:27	2024-06-21 14:58:03	修复中 已修复 已加固 查看
工单管理		4			100.000.0	高盘	• 已加固	主机名称_5f825d35f-17fe-3162-0	e68 2024-03-11 11:15:27	2024-06-21 14:53:48	忽略 修复中 已修复 直着
编排响应	•				10.000	商范	• 忽略	ecm-ceshif825d35f-17fe-3162-0et	68 2024-03-11 11:15:27	2024-03-15 10:43:47	修复中 已修复 已加固 查看
报表中心				5.0	10.00	高危	• 已加固	ecm-ceshif825d35f-17fe-3162-0e6	68 2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
已购资源			1H	6.1	C 4. (19.)	高危	• 已加固	ecm-ceshif825d35f-17fe-3162-0et	68 2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
设置	*			1.1	1E 7 F	高哉	 已修复 	ecm-ceshif825d35f-17fe-3162-0e6	68 2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
				1.1		高危	 已修复 	ecm-ceshif825d35f-17fe-3162-0et	68 2024-03-05 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 直著
				1. I.	10.001	商店	 已修复 	ecm-ceshil825d35f-17fe-3162-0e	68 2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
				1. I	10.00	商品	•待修复	ecm-ceshif825d35f-17fe-3162-0ef	68 2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 造着



4.3.2. 弱口令管理

为租户提供弱口令查询及处置功能。

 =0	云安全中心		弱口令管理	里								
0	安全概览 资产中心	-	应用名称	请输入		服务器 请输入		ģ	と置状态 待修复	×	~ ©	童術 重型
	风险管理 溯河管理		加略	修复中 已修复	已加固							
	弱口令管理			服务器	用户名	口令类型	密码值	应用名称	处置状态	最后发現时间	更新时间	操作
G	威胁运营			and the second sec		系统明口令	123456	应用名称_1	• 待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 直看
0	分析中心	•				系统明口令	123456	应用名称_1	•待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看
	工单管理		•			系统明口令	123456	应用名称_1	•待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看
[囲]	繃排响应	-				系统砌口令	123456	应用名称_1	 待修复 	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看
	报表中心	*										
	已购资源											
20	设置	*										





云安全中心	弱口令管理			~	输入或选	译相关条件内容		「「「」「」「」「」「」「」「」「」「」「」」「」「」」「」」「」」「」」「」
安全概览 * 资产中心 *	应用名称 铸输入	服务器 请输入		ŝ	せ置状态 待修复	×	~ ©	査询 重置
风险管理	最后发现时间 🛅 开始日期 - 结束日期							
明日令管理	総略 修算中 已修算 已加固							
分析中心	服务器 用户名	口令类型	密码值	应用名称	处置状态	最后发现时间	更新时间	操作
工单管理	ecm-ceshif825d35f-17fe-316	系统则口令	123456	应用名称_1	• 待修复	2024-03-11 11:15:27	2024-01-09 11:15	:17 忽略 修复中 已修复 已加固 查看
编排响应	ecm-ceshif825d35f-17fe-316	系统弱口令	123456	应用名称_1	•待修复	2024-03-11 11:15:27	2024-01-09 11:15	:17 忽略 修复中 已修复 已加固 查看
报表中心	ecm-ceshif825d35f-17fe-316	系统弱口令	123456	应用名称_1	 待修复 	2024-03-11 11:15:27	2024-01-09 11:15	(17 忽略 修复中 已修复 已加固 查看
已购资源	ecm-ceshif825d35f-17fe-316	系统弱口令	123456	应用名称_1	 待修复 	2024-03-11 11:15:27	2024-01-09 11:15	:17 忽略 修复中 已修复 已加固 查看
设置 ~								

处置弱口令

提供处置能力,可直接或批量修改弱口令处置状态。状态枚举值:修复中、已修复、忽略、已加固等(此处修 改弱口令状态仅用于云安全中心展示使用)。

云安全中心	弱口令管	理									
安全概览	成田名称	a 1886 S		BSR story			林雪状木 法终期	×.		古 询 ■3	
资产中心	111713 11797	n misur/		WC22 04 19(10)//			AC486 0.00. 10 10 10 10				
风脸管理	最后发现	时间 芭 开始日期 • 《	古東日期								
漏洞管理		批量处置									
弱口令管理	忽略	修复中 已修复	已加固								
威胁运营										单个外置	
分析中心	•	服务器	用户名	口令类型	密码值	应用名称	处置状态	最后发现时间	更新时间	操作	
工单管理		ecm-ceshif825d35f-17fe-316		系统铜口令	123456	应用名称_1	• 待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固	f看
编排响应	1	ecm-ceshif825d35f-17fe-316		系统册口令	123456	应用名称_1	• 待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 昏	雨
报表中心		ecm-ceshif825d35f-17fe-316		系统弱口令	123456	应用名称_1	• 待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固	缅
已购资源		ecm-ceshif825d35f-17fe-316		系统明口令	123456	应用名称_1	 待修复 	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 自	T香
设置											

修改处置状态可填写状态变更原因。

标记为修复	更中					×
确认县	要把该弱口令标记为修复中吗?	?				
	用户名	口令类型	密码值	应用名称	影响服务器	
		系统弱口令	*******88*****	Redis	null6AEFBFA3-7ED3-A524-5B50-1085EB28C	
处置说明	最多可输入255个字符					
			取消保存			

查看弱口令详情



在弱口令详情中,可以查看所有历史状态变更记录的信息,包括:处置人、处置状态、处置说明、处置时间等。

云安全中心		弱口的	令管理	1								
安全概览	•	क्रम	日夕称	12540.5		服务架 (注意)		bi	書任大 法法经		0	查询 更置
资产中心		inter-	01.010	MI RELA		DOLYD BAR			MAANA MISSI			
风险管理												
漏洞管理			忽略	修复中已修复	已加固							击点
朝口令管理				服务器	用户名	口令类型	密码值	应用名称	处置状态	最后发现时间	更新时间	操作
威胁运营	*			Bi		系统弱口令	123456	应用名称_1	• 已加固	2024-03-11 11:15:27	2024-06-21 16:12:01	忽略 修复中 已修复 查看
分析中心	•			······································		系统弱口令	123456	应用名称_1	• 已加固	2024-03-11 11:15:27	2024-06-21 16:11:51	忽略 修复中 已修算 查看
工单管理		4		Julie		系统弱口令		Redis	•修复中	2023-12-01 17:29:59	2024-06-21 16:04:55	忽略 已修复 已加固 查看
编排响应				a subscription of the		系統弱口令		Redis	• 已修复	2023-12-01 17:29:59	2024-06-21 16:03:39	忽略 修复中 已加固 查看
报表中心	*					系统弱口令	123456	应用名称_wesdf	• 已加固	2024-03-11 11:15:27	2024-06-21 16:03:31	忽略 修复中 已修复 查看
已购资源						系统弱口令		Redis		2023-12-01 17:29:59	2024-03-13 14:57:43	忽略 修复中 已修复 已加固 查看
设置	*			-		应用弱口令	123456	应用名称_1	 忽略 	2024-03-11 11:15:27	2024-03-13 09:51:11	修复中 已修复 已加固 查看
				and the second second		应用器口令	123456	应用名称_3333	•修复中	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 已修复 已加固 查看
						应用弱口令	123456	应用名称_2222	•修复中	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 已修复 已加固 查着
			0.1			系统明口令	123456	应用名称_1	•修复中	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 已修复 已加固 直看
弱口令详情									×			
口令类型: 系統弱[口令											
用户名:				密码值: 123	456		应用名称:应用	名称_1				
服务器: 名称_5f82	25d35f-17	7fe-3162	-0e68-c	d10676d09b781.1.1.5								
处置历史:												
\$	沙置人			处置状态		处置说明		处置时	间			
ctyunsectest3	@chinatele	ecom.cn		 已加固 		test		2024-06-21	16:12:01			

查看弱口令关联资产

每条弱密码能够关联资产信息,可快速查看关联的资产详情。

	ŝ	口令管	理								
•		应用名称	请输入	BE	务器 请输入			处置状态 请选择		~ ©	黄润 重置
*											
		忽略	修复中 已修复 日	曲國 点击							
			服务器	用户名	口令类型	密码值	应用名称	处置状态	最后发现时间	更新时间	操作
•			ecm-ceshif825d35f-17fe-316		系统弱口令	123456	应用名称_1	• 已加固	2024-03-11 11:15:27	2024-06-21 16:12:01	忽略 修复中 已修复 直看
•			ecm-ceshif825d35f-17fe-316		系统弱口令	123456	应用名称_1	• 已加固	2024-03-11 11:15:27	2024-06-21 16:11:51	忽略 修复中 已修复 直著
	4		null6b069d22-29dc-2ac6-e8		系统第口令		Redis	•修复中	2023-12-01 17:29:59	2024-06-21 16:04:55	忽略 已修复 已加固 查看
•	4		ecm-ceshi6AEFBFA3-7ED3		系统明口令		Redis	 已修复 	2023-12-01 17:29:59	2024-06-21 16:03:39	忽略 修复中 已加固 直看
*			ecm-ceshif825d35f-17fe-316		系统明口令	123456	应用名称_wesdf	• 已加固	2024-03-11 11:15:27	2024-06-21 16:03:31	忽略 修复中 已修复 直着
					系统弱口令		Redis		2023-12-01 17:29:59	2024-03-13 14:57:43	忽略 修复中 已修复 已加固 查看
			ecm-ceshif825d35f-17fe-316		应用弱口令	123456	应用名称_1	• 忽略	2024-03-11 11:15:27	2024-03-13 09:51:11	修复中 已修复 已加固 直看
			ecm-ceshif825d35f-17fe-316		应用弱口令	123456	应用名称_3333	•修复中	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 已修复 已加固 直着
			ecm-ceshif825d35f-17fe-316		应用弱口令	123456	应用名称_2222	•修复中	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 已修复 已加固 查看
			ecm-ceshif825d35f-17fe-316		系统羽口令	123456	应用名称_1	•修复中	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 已修复 已加固 直着
	• • • • •			新口令管理 新口令管理 新田へ会計/相254356-17(6-316) ecm-cesh/相254356-17(6-316) ecm-cesh/相254356-17(6-316) ecm-cesh/相254356-17(6-316) ecm-cesh/相254356-17(6-316) ecm-cesh/相254356-17(6-316) ecm-cesh/相254356-17(6-316) ecm-cesh/相254356-17(6-316) ecm-cesh/相254356-17(6-316) ecm-cesh/相254356-17(6-316) ecm-cesh/相254356-17(6-316)	日本の一にのまた時間を立ちまた。17%-316	Gran-CeshW825cd36-17%-316 Form-CeshW825cd36-17%-316 Corm-CeshW825cd36-17%-316 Corm-CeshW825cd36-17%-316	RimeSite 1982年 RimeSite 1982年 日日日 日本 RimeSite 1982年 日本 Rime	Reds ののの-cesh/025c356-17ie-316 ecm-cesh/025c356-17ie-316 flipting- t123456 flipting- t1234	Reds ののののののののののののののののののののののののののののののののの	日本日本 日本	Receive 2005-05-1716-316 Receive 2005-05-1716-316 Receive 2005-05-1716-316 Receive 2005-05-1716-316 Receive 2005-05-1716-316 Receive 2005-05-05-1716-316 Receive 2005-05-05-1716-316 Receive 2005-05-05-05-05-05-05-05-05-05-05-05-05-



云安全中心		资产详情			
安全概览		资产信息 脆弱性信	息		
资产中心	•	基础信息	■ 基本信息		
威胁运营	-	基本信息	主机名称: ecm-ceshi	主机D: ab9fbafe-76d2-4eeb-b021-b753aadedfe6	资产状态:运行中
分析中心	-		操作系统: linux	操作系统版本:	虚拟私有云名称:vpc-osm-ceshi
工单管理			云资源创建时间: 2024-06-18 01:04:30	云资源受到明时间: 2024-07-18 01:05:37	地域:
编排响应	-		可用区: default		
报表中心	•	4			
已购资源					
设置	•				

4.4. 威胁运营

为了便于用户对平台告警数据进行整理分析与管理,威胁运营提供告警概览、告警管理、告警列表、通知管理和威胁检测等功能。

前提条件

已开通云安全中心实例。

4.4.1. 告警概览

告警概览由告警数量、已处置告警数量、待处置告警数量、攻击源数量、受影响资产数量、告警严重程度分布 、攻击源 TOP5、受威胁资产 TOP5、告警类别 TPO5 以及告警处置率等指标展现。



告警概览				曲 本周	~ 査询
告警数量 ⑦ 73 条 73 条		待处置告警数量 72 条	ଙ	攻击源数量 31 _条	受影响资产数量 0 _余
告警严重程度分布	攻击源TOP5 国家/地区	IP地址	攻击次数	受威胁资产TOP5 业务系统	IP地址 数量
	广东	183.56.201.236 154.89.104.162	 323 27 		
● 警告 73 100.00%	荷兰	220.203.28.115 194.50.16.221	• 17 • 9		
	江苏	117.89.222.68	6		
告警关別TOP5		告警	处置率		
				40 50 60	70
					90
				 1% 告警处置率 	

4.4.2. 告警列表

为用户提供查询、解决建议、处置威胁等功能

云安全中心	告警管理							9	P 🥑 🤊 🖽 🗞	TP
	TQL							7天		主印 第 第 •
	-									
的运营	· 数据/	문문 48								
吉警視地	12 9 6		•					•		
-警管理	å	2024-05-20	2024-05-21	2024-05-22	2024-0	5-23 2024	-05-24	2024-05-25	2024-	05-27
- 前检测 -										
中心 ·	- 严重等级 ≑	有效告誓名称 💠	jæip ≑	目的IP 💠	告誓阶段 💠	关联分析规则名称 💠	责任人 💠	处置状态 ≑	告誓次数	操作
管理	致命	111.7.124.33对172.17.1.2触发	111.7.124.33	172.17.1.2	侦查	XDR_WAF赛I+		待处置	1	0
响应	Ris	111.7.124.32对172.17.1.2触发	111.7.124.32	172.17.1.2	侦查	XDR_WAF事件		待处置	1	Θ
(中心)	•							(11.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1		
	致命	111.7.124.31对172.17.1.2触发	111.7.124.31	1/2.1/.1.2	「収金」	XUR_WAF		100		•

TQL 条件查询

○ 天翼云

a. 0	Ĭ					□ ~		查询 🛛 🙈 🖂 🗠
_	(B)P	src_address	一选择查询	字段				
E	目的IP	dst_address						
	威防关型	threat_category						
1	源海口	src_port				-		
	有效告警名称	alarm_name				(24-05-25	2024-	05-27
Į	攻击甲数	attack_ip_num						
	公有云租户ID	account_id				● 新水本 ▲	告醫次數	接作
	安全服务编号	service_code					1	
I	攻击次数	attack_times				1430	3	
Ran	111.0.132.30次172.17.1.2度反…	111.6.132.30	1/2.1/.1.2		\UR_WAF₩1+	待处置	2	0
致命	112.81.132.35对172.17.1.2触	112.81.132.35	172.17.1.2	侦查	XDR_WAF事件	待处量	2	0
致命	112.81.132.45对172.17.1.2触	112.81.132.45	172.17.1.2	侦查	XDR_WAF事(#	待处置	2	0
散命	111.7.124.32对172.17.1.2触发	111.7.124.32	172.17.1.2	使臺	XDR_WAF事件	待处置	1	0
散命	111.7.124.31对172.17.1.2触发	111.7.124.31	172.17.1.2	侦查	XDR_WAF事件	待处置	1	0
致命	111.7.122.34对172.17.1.2触发	111.7.122.34	172.17.1.2	侦查	XDR_WAF事件	待处量	1	0
致命	112.81.132.35对172.17.1.2触	112.81.132.35	172.17.1.2	侦查	XDR_WAF事件	待处量	1	0
	111 7 122 3533172 17 1 2년4월	111 7 100 95	170 17 1 0			(44) =		0

)頂IP					0		查询 高级
	like	横湖匹配	- 洗择查询	家件				
	not like	排除機糊匹配						
	=	等于						•
1	!=	不等于				-0		
	>	大于				124-05-25	2024	4-05-27
	<	小于						
严重等	>=	大于等于				冨状态 ▲	告誓次数	语作
	¢#	小于等于				(56) #		
	in	包含						0
E E	not in	不包含				192	2	
致	exist	存在				待处置	2	0
致	not exist	不存在				待处置	2	0
致命	111.7.124.32对172.17.1.2触发	111.7.124.32	172.17.1.2	侦查	XDR_WAF事件	待处置	1	ø
文章	111.7.124.31对172.17.1.2触发	111.7.124.31	172.17.1.2	侦查	XDR_WAF事件	待处置	1	0
戰	會 111.7.122.34对172.17.1.2触发	111.7.122.34	172.17.1.2	侦查	XDR_WAF事件	待处置	4	۲
戰	112.81.132.35对172.17.1.2触	112.81.132.35	172.17.1.2	侦查	XDR_WAF事件	特处量	1	0
37	111 7 122 353世172 17 1 2輪岩	111 7 122 35	172 17 1 2	(84)		(由6)-雪	1	0



****									-
1	c	•		•		0-		0	
0	2024-05-21	2024-0	5-22	2024-0	5-23	2024-05-25		2024-05-27	
严重等级 💠	有效告誓名称 💠)源IP 令	目的IP 💠	告誓阶段 💠	关联分析规则名称 💠	责任人 ⇔	处置状态 ≑	告誓次数	iæf
戰命	111.7.132.35对172.17.1.2触发	111.7.132.35	172.17.1.2	侦查	XDR_WAF事件		待处量	3	0
致命	111.7.132.35对172.17.1.2触发	111.7.132.35	172.17.1.2	侦查	XDR_WAF事件		待处置	3	0
致命	111.7.132.35对172.17.1.2触发	111.7.132.35	172.17.1.2	使查	XDR_WAF事(#		待处置	1	0
提醒	111.7.132.35对172.17.1.2触发	111.7.132.35	172.17.1.2	侦查	XDR_WAF事件		待处量	1	0
活躍	111.7.132.35对172.17.1.2触发	111.7.132.35	172.17.1.2	100	XDR_WAF事件		待处置	1	0

LO IRIP	like 111.7.124.33				20	24-05-01 00:00:00~202	4-08-18 00:00:00		查询 常
数据 1	ë ≣ .4	2024-05-22 ● 数量: 1	9		•				
0	2024-05-21		2024-05-22		2024-05-	25		2024-05-27	
重等级 ⇔	有效告誓名称 💠	jíjiP ≑	目的IP \$	告誓阶段 🗢	关联分析规则名称 💠	责任人 🗢	处置状态 ⇔	告暫次数	操作
致命	111.7.124.33对172.17.1.2触发	111.7.124.33	172.17.1.2	(侦查	XDR_WAF事件		待处置	1	•
致命	111.7.124.33对172.17.1.2触发	111.7.124.33	172.17.1.2	侦查	XDR_WAF事(+		待处置	1	0
提醒	111.7.124.33对172.17.1.2触发	111.7.124.33	172.17.1.2	位臺	XDR_WAF事(牛		待处置	1	0
提醒	111.7.124.33对172.17.1.2触发	111.7.124.33	172.17.1.2	(6 11)	XDR_WAF事件		处置中	1	0
						共4条	20条/页 ~	< 1 >	前往 1

选择常用时间查询



1.5							£7天		查询 看
数据	送 量 .5					常用时	点击 泉山天	●近30天 ≦	è#3
1	B	•				ж	 G 开始日期 	至 结束日期	8
0	2024-05-21	2024-0	5-22	2024-0	5-23	2024-05-25		2024-05-27	
■重等級 ⇔	有效告誓名称 💠	源IP ≑	目的IP 💠	告賢阶段◆	关联分析规则名称 💠	责任人 🗢	处置状态 ≑	告警次数	操作
致命	111.7.132.35对172.17.1.2触发	111.7.132.35	172.17.1.2	侦查	XDR_WAF事件		待处置	3	0
致命	111.7.132.35对172.17.1.2触发	111.7.132.35	172.17.1.2	侦查	XDR_WAF事件		待处置	3	0
	111 7 132 353寸172 17 1 2钟发	111.7.132.35	172.17.1.2	(皮壷)	XDR_WAF事件		待处置	1	0
致命									
致命	111.7.132.35对172.17.1.2触发	111.7.132.35	172.17.1.2	侦查	XDR_WAF事件		待处置	1	0

选择时间范围 (最大查询时间窗口为 30 天)







查询条件组

保存查询条件, 方便用户查询 (保存的查询条件最多为 10 个)

NEE 2: 2014/0-21 2014/0-21 2014/0-21 FEB 0 NOTE FEB 0 NP 0	9 8 8
0 202465-21 202465-21 PERMI 0 A0739500 0 BP 0 DDP 0 DEMO 0	
0 20445-21 20445-21 PERSE 0 REP 0	
PERSO MXX284001 0 MP 0 DEMO 0	
Image:	操作
INT. 124.333/172.17.1282E. INT. 124.33 IT2.17.12 IEE XDR_UMF## All## I # 12 fr 2028.7 I IT	0
# 2 & 2000 2 0	0
2014 05-21 2024 05-22 P 建築地 6 和2018 05 00 0 2024 05-21 2024 05-22	前注 1 2 末 部
0 2024-05-21 2024-05-22 P電歌線 ● 和改告署名称 ● 原P ● 日的P ● 台版阶段 ● 米玩分析所限的名称 ● 東丘人 ● 公園秋石 ● 台画次数 ● 白面の P ● 台版阶段 ● 水石小和手供 ● 砂道 ● 1 1 202 1117.124-3320172.17.1.2월28 1117.124-33 172.17.1.2 10000 XDR_WAF等件 ● 砂道 ● 1 1 1 202 1117.124-3320172.17.1.2월28 1117.124-33 172.17.1.2 10000 XDR_WAF等件 ● 砂道 ● 1 1 </td <td></td>	
PT型物 の 和效論型名称 の JBP の 自動P の 資理的液 の 其代 小 分量数次 分量数次 通言 111.7.124.3330172.17.1.2检波 111.7.124.33 172.17.12 通言 111.7.124.3301772.17.1.2检波 111.7.124.33 172.17.12 通言 XDR_WAF事件 代量 が当年 1 が当年 1 1 がに パロー がに パロー がに パロー パロー パロー	
(注意 111.7.124.333g172.17.1.2检验 111.7.124.33 172.17.12 (図図 XDR_VMAF等)(+ 快速重 1 (注意 111.7.124.333g172.17.1.2检验 111.7.124.33 172.17.12 (図図 XDR_VMAF等)(+ 火重中 1 1 (注意 111.7.124.333g172.17.1.2检验 111.7.124.33 172.17.12 (図図 XDR_VMAF等)(+ 火重中 1 1 (注意 XDR_VMAF等)(+ 火重中 1 1 1 1 (注意 XDR_VMAF等)(+ 火重中 1 1 1 1 (注意 111.7.124.333g172.17.1.2 (図 N F F)(+ 火重中 1 1 1 1 1 1 1 1 1 (注意)(注意)(注意)(注意)(注意)(注意)(注意)(注意)(注意)(注意)	操作
III.7.124.333172.17.1.2截法 III.7.124.33 172.17.12 (SE XDR_WAF每4年 处量中 1 共2 条 20杂页 ✓ 《 1 》 前柱 存查询条件组 ×	0
	•
存查词条件组 × 和条件语名称: est	91 T
時無件組合称: est Es ES保存重成条件:	
est	



数据总量 1						A second s				
						√ test]*			
1						清空		另存为保。	Ŧ	
0				2024-05-2	27 10:00					
王 等级 ≑ 有	效告警名称 ⇔	源IP ≑	目的IP 💠	告醫阶段 💠	关联分析规则	名称 ≑	责任人 💠	处 置状态 ≑	告暫次数	操作
<u></u> 北命 11	11.7.124.33对172.17.1.2触发	111.7.124.33	172.17.1.2	侦查	XDR_WAF	H #		待处量	1	0

查看与选择历史查询记录

历史记录最多保存 50条

21.0 处重状态 = 忽略			0 2	024-05-27 00:00:00~2024-05-27 23:59:59	₩ 8000 ± 100 × 10
数据符量 0					
平重等级 ⇔ 有效告督名称 ⇔	j@iP ≑	目的iP 🛊	告 暂 阶段 中 关联 分析 规则名称 中	责任人 ≑ 处置状态 ≑	告誓次致 操作
			无数据	共0 条 20 条页 ◇ 《	〈 1 〉 前住 1
L① 处置状态 = (588)			无数语	共0条 20条页 ∨ <	 (1)前注(1) (1) (1)<
L. Ø 21≣0705 = 1586			无数强	共0条 20条页 v 《 224-05-27 00:00:00-2024-05-27 23:59:59	 (1) 離 1 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
L ① 处置状态 = 59% 数据注量 0			元放張 ① ② ② 2 查岐条件 处量状态 = 仮容 二	共0条 20条页 v 4 024-06-27 00:00:00-2024-06-27 23:68:59 查询时间 2024-06-27 15:51:59	(1) 離 1 回 O ® 画 案 点击
L ① 处量状态 = 标路 影振音量 0			元数据 元数据 直均条件 处重状态 = 忽略 調P like 111.712433 事件输入状态 = "欢击未成功" and 严重等级 = "警告" and 炎山 略	共0条 20条页 v 4 224-05-27 00:00:00-2024-05-27 23:59:59	(1) 離 1 回 0 @ • • • • • • • • • • • • • • • • • •
▲● 灶量状态 = 您略 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●			天放焼 天放焼 重約条件 处量状态 = 原格 調P Hke 111.7.124.33 事件換入状态 = 「次击未成功" and 严重等级 = "警告" and 炎丘 略 調P Hke 111.7.132.35	共0条 20条页 ∨ 224-05-27 00:00:00-2024-05-27 23:59:59 查询时间 2024-05-27 15:51:57 2024-05-27 15:51:54 2024-05-27 15:51:54 2024-05-27 15:51:54	
1.● 处重状态 = 你略 数据总量 0	j@₽ \$	ĘŔ	无数据 一	共0条 20条页 v 4 224-05-27 00:00:00-2024-05-27 23:69:59	
21.● 灶量状态= 55% 影振谷量 0 严重等级 ◆ 有效告誓名称 ◆	j@rP ∳		无数据 一 直始条件 处量状态 = 你務 調P like 1117.124.33 事件确认状态 = 「双击未成功」 and 严重等级 = 「警告」 and 处望 客 調P like 1117.124.33 調P like 1117.124.33 建築状态 != 「物路」 and 専件确认状态 != "畏限"	共0条 20条页 v 224-05-27 00:00:00-2024-05-27 23:59:59 室向時间 2024-05-27 15:51:59 2024-05-27 15:51:54 2024-05-27 15:51:54 2024-05-27 15:22:35 2024-05-27 15:19:47 2024-05-23 17:42:32	(1) 前:1 回 ③ ③
21.● 处量状态 = 忽容 数据总量 0	jiii P ≑	Eff.		共0条 20条页 × 4 224-05-27 00:00:00-2024-05-27 23:58:59 宣助时间 2024-05-27 15:51:57 2024-05-27 15:51:54 2024-05-27 15:22:35 2024-05-27 15:22:35 2024-05-27 15:22:35 2024-05-27 15:22:35 2024-05-28 17:42:32 勤藝* 2024-05-08 1015:31	

快速查询条件



使用模糊查询时需要带*

								× ×	
0						□ 今天		60	主 狗 (1)
目的	P "进行模糊匹配	威胁关型	"进行模糊匹配		有效告警名称	E	公有云租户ID	"进行模糊匹配	
数据: 15	ģ ≣ 13								
12 9 6 3				•					
0				2024-05-2	27 10:00				
重等級 ≑	有效告警名称 👙	源IP ≑	目的IP ≑	告誓阶段 💠	关联分析规则名称 🗢	责任人 🜩	处置状 态 ≑	告誓次数	操作
致命	111.7.124.33对172.17.1.2触发	111.7.124.33	172.17.1.2	侦查	XDR_WAF事件		待处置	1	0
致命	111.7.132.35对172.17.1.2触发	111.7.132.35	172.17.1.2	侦查	XDR_WAF事件		待处置	3	0
致命	111.8.132.35对172.17.1.2触发	111.8.132.35	172.17.1.2	侦查	XDR_WAF事件		待处置	2	0
致命	112.81.132.35对172.17.1.2触	112.81.132.35	172.17.1.2	侦查	XDR_WAF事件		待处置	2	0
						□ 今天		B © Ø	主 词 7
目的IF	"进行模糊匹配	威胁类型	进行模糊匹配			🛛 威助关型	1	5	
目的呼	○进行模糊匹配	威討关型 安全服务编号	进行模糊匹配		 目的IP 有效告替名称 	 ✓ 威胁关型 ✓ 攻击叩数]	8	
目的に公有云租户に	"进行镇赖匹配 "进行镇赖匹配	威胁关型 · 安全服务编号 ;	进行模糊匹配		 目的IP 有效告報名称 公有云相户ID 	 威助关型 双击印数 女全服务编号]	B	
日的 F 公有云租户 ID 数据总	*进行機构匹配 *进行機构匹配	威討英型 · · · · · · · · · · · · · · · · · · ·	进行模糊匹配 意选择		2 目的IP 2 有效告誓名称 2 公有云相户ID	 xitikation xitikation xitikation xitikation]	R	
目的F 公有云租户ID 数据总 15 12 9	 ・注行機能匹配 ・注行機能匹配 ・注行機能匹配 	成計关型 · · · · · · · · · · · · · · · · · · ·	进行模糊匹配		2 目的IP 2 有效告替名称 2 公有云祖户ID	 <u>京助共型</u> <u>汉古印教</u> <u>文全取発編号</u> 		R.	
目的F 公有云租户ID 数据总 15 12 9 6 3 0	 ・法行標期匹配 ・法行標期匹配 13 	威討共型	进行模糊匹配	2024-05-2	 目的IP 有效告替名称 公有云祖户ID 7 1000 	 2 成前关型 2 攻击呼激 2 安全服务编号]	8	
目的F 公有云租户口 数据总 15 12 6 3 0	 *进行標期匹配 *进行標期匹配 13 	威討共型	进行模糊匹配	2024-05-2	 目的IP 有效告替名称 公有云租户ID 7 10:00 	 2 成前关型 2 攻击呼激 2 安全服务编号]	8	
日的F 公有云祖户ロ 数据总 15 12 9 9 3 0 	 *进行機构正配 *进行機构正配 * 13 有效音響名称 ◆ 	成計英型 安全派先編号 選P 令	进行練輸匹配 意志萍 目的IP \$	○ 2024-05-2	 目的P 有效告替名称 公有云相户D 7 10:00 关联分析规则名称 \$ 	 2 成前关型 2 双击印数 2 安全预务编号 表在长 \$) 处重状态	日本	
目的F 公有云祖户口 数据总 5 5 6 3 0 5 8 6 3 0 5 6 3 0 5 6 3 0 5 5 6 3 0 5 5 5 6 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	 *进行標期匹配 *进行標期匹配 13 有效告替名称 ◆ 111.7.124.333;172.17.1.2社気… 	威勝美型 安全統務編号	进行模糊匹配 意选择 目的IP 中 172.17.1.2	○ 2024-05-2 古智新段 ◆	 目的IP 有效告替名称 公有云租户ID 2 公有云租户ID 7 10:00 关联分析规则名称 ◆ XDR_WAF事件 	 2 成時失型 2 双击呼吸 2 安全服务编号 表任人 令 	したまれる キ 何次重	E 告顧次政 1	

查看告警详情



21. ① 源1	P like 111.7.124.33						67天		查询 高级
E	的IP ,进行模糊匹配	威勃美型	"进行模糊匹配		有效告警名称 法行模糊匹配		公有云租户ID	"进行模糊匹配	
数3 15 12	履总 量 45							0	
9 6 3 0	2024-05-21	2024-05-22	2024	-05-23	c 2024-05-24	20	24-05-25	2024-05	-27
							14		
■ 王 等级 ‡	有效告醫名称 🜲	ííiP ≑	目的IP ‡	告誓阶段 💲	关联分析规则名称 👙	责任人 ≑	处重状态 ≑	告誓次数	操作
■重等级 \$ 取命	有效告誓名称 ≑ 111.7.124.33对172.17.1.2触发	源IP ✿ 111.7.124.33	目的IP \$	告誓阶段 💠	关联分析规则名称 ◆ XDR_WAF事件	责任人 ⇔	处重状态 💠 待处量	告誓次数 1	· 操作
■重等級 ◆ ③命	有效告警名称 ◆ 111.7.124.33对172.17.1.2触发 111.7.132.35对172.17.1.2触发	源IP ≑ 111.7.124.33 111.7.132.35	目的IP \$ 172.17.1.2 172.17.1.2	告賢阶段 \$ (()) (()) (()) ())	关联分析规则名称 ◆ XDR_WAF事件 XDR_WAF事件	表任人 💠	处重状态 \$ 待处量 待处量	告誓次数 1 3	· 操作
■ 重等級 \$ 取命 取命 取命	有效告誓名称 ◆ 111.7.124.33对172.17.1.2舱发 111.7.132.36对172.17.1.2舱发 111.8.132.36对172.17.1.2舱发	源IP 💠 111.7.124.33 111.7.132.35 111.8.132.35	目的P ◆ 172.17.1.2 172.17.1.2 172.17.1.2		文联分析規則名称 ≑ XDR_WAF事件 XDR_WAF事件 XDR_WAF事件	责任人 ≑	处重状态 	告輩次数 1 3 2	@ 0

有效告營详情

and in intrans. m		Contraction of the second s	
	~ 25	秋春: 杨处置 处置中 处置完成 忽略	处直认念
1 15/CCR			
	111.7.124.33 中国/河南/波阳 (115.07446/35.77736) (移动)		
IP	172.17.1.2		
阶段	位置	告留口	784af392-c5a8-467c-84ba-7ea60f22acd9
吸则	致命	公布太祖户旧	27618268ad774c5e8ca87f34df86030a
al	3	关联分析规则名称	XDR_WAR#(ft
/ 原始告警: 111.7	7.124.33对172.17.1.2触发告警,攻击类型为XSS攻击	生告警的详细内容	1
2007 (dev.)			
COP 12-12	(111.7.124.33 (PD))((910)(110.07440/36.77736)((910))		
目的P地址	172.17.1.2		
告誓级别	我命	告知阶段	後直
告譬创建时间	2024-05-25-04:36:20	告誓开始时间	2024-05-21 16:50:34
古曾结束时间	2024-05-21 16:50:34	告册关联日志ID	2405w6Utb,2405w6UsR,2435w6UtyY,2405w6Utb,2405w6UuA,2405w6Uoz,2405w6Ut7,2405w6Utr 2405w6Ug,2405w6Utu,2405w6Uts
WUISR	XDR_WAF#IT	威胁类型	ATTACK
סורוא	з	公布云租户ID	27618268ad774c5e8ca87f34df86030a

✓ 原始日志: WAF告書	書件-ATTACK ■ 原始日志的内容	F	€ 1 2 3 4 11 > ⊞
基本信息 成初详情	原始信息		归并的原始日志
攻击类型	XSSIL	动作	HER .
事件类型名称	全局失型(内面)	日志来源	自研WAF
日志发生时间	2024-05-21 16:50:34	安全服务编号	waf
公有云租户ID	27618268ad774c5e8ca87f34df86030a	סניאא	3
威胁类型	ATTACK		
五元組			
201P地址	111.7.124.33 中国河南/俄阳 (115.07446/35.77736) (移动)		
	172.17.1.2		
日的地口	443		

○ 天翼云

4.4.3. 告警管理

告警管理是为了便于对告警的统一管理、处置与后续分析。告警管理用于告警的统一管理,进行告警的处置。 告警管理界面可以很详细地看到告警的基本属性,以及告警的处置情况,告警管理界面可以以告警编号、告警 名称、告警分类、告警级别、告警工单状态、告警来源及时间段查询指定的告警工单。

前提条件

已开通云安全中心实例。

查看告警详情

在告警管理中, 点击告警名。

云安全中心		告警管理							
资产中心 资产概选	^	Q遺輸入告	警告或资产P			∨ 最近7天		重调	
资产管理									
の合管理	^	1993	处室中 处直元或	自动处室					U.
濁洞管理 弱口今管理		误报	EE SS						
2019运营 告警概选	^		●告 ≑	告賢名 💠	告誓分类 ≑	銀別 令	剧本 💠	发生时间 💠	操作
告誓管理				202,103,95,207对192,168,24,80 最发音管,双击关型为PHP 反序 列化,质却通道强则达为Web应用 防火增(原生版)	Web应用防火墙(原生版)告警	(\$2)		2024-12-05 14:22:41	F
通知管理	Ŷ			202.103.96.2075;192.188.24.80 触发音響,攻击美型为ASP 代码 执行,風討連集調問为Web应用 防火增(原生版)	Web应用防火增(原生版)告警	(20)		2024-12-05 14:22:41	F
威約检測 析中心	~			202.103.95.207对192.168.24.80 触发言誓,攻击关型为Java 反序 列化,反前建模型则为Web应用 防火槽(原生版)	Web应用防火墙(原生版)告警	(22)		2024-12-05 14:22:41	F
相叫应 剧本管理	^			202.103.95.2075;192.168.24.80 触发言意,现于关型为Java 代码 执行,反前建建现则为Web应用 切火理(原生版)	Web应用防火墙(原生版)告警			2024-12-05 14:22:20	F
插件管理				202,103,96,20775192,188,24,80 触波音響,双击关型力3團用代码 执行,成前建模规则为Web应用 防火增(原生版)	Web应用防火墙(原生版)告警	(98)		2024-12-05 14:22:31	F
腰中心	\sim			202.103.95.207对192.168.24.80 触发告誓,双手提型为SOL主 入,副操建提购为Web应用的 火增(原生版)	Web应用防火墙(原生版)告警	(22)		2024-12-05 14:21:28	P
				000 100 06 0070#100 180 04 00					

进入告警处置页面,可以看到告警相关详细信息。

192.168.0.4对106.40.5	51.168触发告警 【08-15 15:37:40~08-15 15:37:45】	警告	处置 误报 重复 忽略
源IP	192.168.0.4		
目的IP	106.40.51.168 中国/内蒙古/ (118.719421/45.383339) (电信)		
告警阶段	侦查	告警ID	00a92fd1-4506-4c96-b3b9-fcd2e63371c4
告警规则类型名称	其他	告警级别	警告
关联分析规则名称	服务器安全卫士 (原生版) _漏洞扫描		

ヘ 原始告警: 192.168.0.4对106.40.51.168触发告警

处置告警

告警 关联告警



在告警详情界面,点击"处置"。

92.168.0.4对106.4	0.51.168触发告警【08-15 15:37:40~08-15 15:37:	45】 警告	处置 误报 重复 忽略
源IP	192.168.0.4		
目的IP	106.40.51.168 中国/内蒙古/ (118.719421/45.383339) (电信)		
告警阶段	侦查	告譬ID	00a92fd1-4506-4c96-b3b9-fcd2e63371c4
告警规则类型名称	其他	告警级别	警告
关联分析规则名称	服务器安全卫士 (原生版) _漏洞扫描		

进入处置界面,可以选择处置剧本、处置时限。

38 [5	ここ。		
innik: [et m]	<u>发生</u> 时间: 2024-09-05 12:04:08	外最近的的口户:	影响资产:
247AR :	处:翻译(2):		
• 处置数本选择			
81555 (00)cp 815	8 83/5 V 97		
and all all and all all all all all all all all all al			
副本名称	議員教程		
	日带运营		
0 1000	日常运营		
O manual and	日來這會		
0 200	日來运营		
a reading and a strategy and		÷	

配置完成后,点击"启动"。

在处置界面,查看处置记录,并可进行相关的处置。

				责任人修改
ì殿:【侦查】	发生时间:2024-05-30 09:06:01	外部威胁IP:	影响资产:	2
旗長: 2024-05-31 21:12:43	处量建议:			
单处置				
用户节点			C	当前剩余: 1天0小时0分钟)
始后见				
test				4/255

进入作战室,可以快速调用插件进行自动化处置,左侧是插件名称与介绍,右侧是按执行时间排序的已执行插 件的输入、输出和 Log 日志信息。



工单处置		
告警 处置 作战室 实战剧本 关联	¥件 小塔	
清治 人 久 衣	发送短信-公有云Soan垣信遇知睡件发送短信	2024-05-31 09:32:57
India V. Z. Int.	输入 输出 Log	0
系统插件 系统工具	accountid: 27618268ad774c5e8ca87134df86030a phoneNumber: 183803991210	
公有云Soan版估通知邮件 v1.0.0 支送在信 nun	message: 詞感與異1111111111111111111111 gype: 知道國通知 userid:	

告警处置完成之后,用户可以编辑小结,同时可以上传相关文件,方便后续的回顾分析。

	XDH	i .	作战室	实战剧社	关联事件	- 小組														
耐牛小	结																			
в.	IL	i e	77 (/> H1 H;	⊨≡	\mathbf{x}_2 \mathbf{x}^2	ΞE	•¶ Nor	nal 🗘	Normal	÷ _A	A	Sans Seri	f	≞	<u>T</u> _N	% 🖬 E	1		
調能	小结	内容。	大小不能	<u>₩1</u> ±2M																

4.4.4. 通知管理

4.4.4.1. 通知规则

创建通知规则

- 1. 登录云安全中心控制台。
- 2. 在左侧导航栏选择"威胁运营 > 通知管理 > 通知规则",进入通知规则页面。
- 3. 点击"新建"按钮,弹出创建通知规则窗口。



り建通知	规则	×
规则定义	ζ	
風知类型	请选琛通知类型	~
副知对象	请远择通知对象	~
助方式	🗌 短信 🔽 邮箱 🗌 钉钉机器人 🗌 微信机器人	
E效周期		l,
知时段	① 开始前 至 结束前间	
复通知	不重复	~
见则信息	.	
* 名称	清输入通知名称	
描述	清输入通知描述	

4. 配置通知规则信息。

说明:

只有在生效周期和通知时段产生的告警会进行通知。

参数	说明
通知类型	选择需要通知的告警类型,数据来源于威胁建模中的类型(可多选)。
通知对象	选择通知联系人,数据来源于在通知联系人页面创建的通知联系组(可多选)。
通知方式	选择告警通知的方式,支持短信、邮箱、钉钉机器人、微信机器人(可多选)。 说明: 如果需要向钉钉或微信发送告警的消息,需要先在通知联系组中配置钉钉 机器人或微信机器人。
生效周期	选择需要通知的星期(可多选)。

取消

确定



通知时段	选择需要通知的时间段。
重复通知	配置对于已通知但未及时处置的告警是否采用重复策略进行通知。
规则信息	用于标识特定规则的信息。

云安全中心	通知规则	创建通知规则
安全态势	新建 創用 特用	规则定义
安全成果展示	- 89	
资产中心 因治 生 理		- 通知方式 ten200411100 目の 通知通知 共1条 100余页 / く 1 > 前注 1 页
威胁运营		- 2001898 testsell2
	3	622 *室東義和 本主英
西省が本		 ・教育 ・ ・ ・
通知联系人		推动 · 通信/ 通信 · 通信 · 通信 · 通信 · 通信 · 通信 · 通信
威斯拉测 分析中心	x. x.	
日志臺洵		1014 862
原始告誓查询		取得

5. 配置完成后,单击"确定",回到通知规则页面,可以看到已创建的通知规则,状态默认为"启用"。

管理通知规则

创建通知规则后,支持对通知规则进行管理,包括启用、停用、编辑、删除操作。

通知规则

新建	启用 停用 删除	0			请输入规则名称			搜索
	名称	通知类别	通知对象	状态	最近通知时间	操作		
	test4	Web应用防火墙 (原生版) 告警	test-cw1	停用	2024-09-27 13:48:03	启用	编辑	删除
	test-cw1	常见攻击	test-cw1	停用	2024-09-10 01:46:09	启用	编辑	删除
	通知组	(安全卫士) 网络暴力破解		停用	2024-10-12 11:22:13	启用	编辑	删除
	lij	关联分析类型	test3	启用		停用	编辑	删除

4.4.4.2. 通知联系人

通知联系人由联系人和联系组组成,其中通知联系人需要填写名称、手机号以及邮箱。



通知联系人

新建联系人

- 1. 点击"新建",创建联系人。
- 2. 填写姓名、手机号以及邮箱等信息。

创建联系人		
* 姓名	请输入姓名	
* 手机号码	请输入手机号码	
* 邮箱	请输入邮箱	
		取消 确定

3. 单击"确定",完成创建。

编辑联系人

点击编辑按钮实现联系人信息的变更。

删除联系人

单个删除:选择需要删除的联系人,点击删除按钮。

新建 微加至通知联系组	9H83:		请输入姓名/手机号码/邮箱	搜索
名称	手机号码	邮箱	所属通知联系组	操作
云等保1	1333333333			编辑删除

多个删除:多选联系人,点击删除按钮。



D联系人 通知联	系人 通知联系组				
新建	添加至通知联系组 删除			请输入姓名/手机号码/邮箱	搜索
	名称	手机号码	載箱	所属通知联系组	操作
	ź	1:			编辑删除
	ī.	13:			编辑图除
		1			编辑曲除
				共3条 10条/页 >	< 1 → 前往 1 页
			警告 ×		
		此操作同步删除用 删除吗?	計组和通知规则内的通知人信息,确定		
			取消 确定		

注意:

删除联系人会同步删除用户组和通知规则内的通知人信息。

通知联系组

新建联系组

- 1. 点击新建按钮, 创建联系组。
- 2. 输入联系组组名和备注信息。
- 3. 根据需要开启钉钉机器人或微信机器人。

说明:

钉钉机器人的 token 与 secret 获取方式与微信机器人获取 key 的方式见 "常见问题 > 配置类 > 告警

通知相关"。



创建联系统	8		>
* 组名	清输入组名		
訂訂机器人			
* token	濟输 入钉钉机器人token		
* secret	请输入钉钉机器人secret		
救信机器人 			
* key	请输入;微信机器人key		
备注	清输入备注		
选择联系人			
	待选联系人 0/1	已进联系人 0/0	
	□ 请输入联系人姓名	□ 遺輸入联系人姓名	
	test1	无数据	

4. 勾选需要添加到组的联系人,点击向右按钮将待选联系人移动到已选联系人中。



5. 点击确定,完成联系人组的新建。

快捷添加入联系人组

- 1. 在联系人页面多选联系人。
- 2. 点击添加至通知联系组。


通知联	系人 通知联系组				
新建	漆加至通知联系组			请输入姓名/手机号码/邮箱	
	名称	手机号码	邮箱	所属通知联系组	操作
	· 43	1			编辑删除
		1			编辑删除
	1	1			编辑 删除

- 3. 选择需要添加的通知联系组。
- 4. 点击确定, 实现快捷添加。

删除联系组

注意:

删除联系组不会删除联系人。

单个删除:选择需要删除的联系组,点击删除按钮。

新建		MR9	请输入组名称/姓名/手机号码/邮箱
		組名称	操作
	>	组1	编辑曲诗
	>	组2	編辑 删除

多个删除:多选需要删除的联系组,点击删除按钮。在弹出的提示框中,单击"确定"。

新建 翻版	请输入组名称/姓名/手机号码/邮箱 检索
☑ 组名称	操作
☑ → 组1	编辑 删除
☑ > 組2	編辑 删除



4.4.5. 威胁检测

4.4.5.1. 威胁建模

通过威胁建模规则,匹配威胁源是否满足告警条件。

可以通过关键字、快捷方式、规则类型和标签查询威胁建模规则。

用户初次订购时会复制所有的威胁建模模板,并开启对应的威胁建模规则(如:租户订购了 Web 应用防火墙 原生版,集成配置开启开关,则会开启对应的威胁建模规则)。

新建规则

- 1. 登录云安全中心控制台。
- 2. 在左侧导航栏选择"威胁运营 > 威胁检测 > 威胁建模"。
- 3. 单击"新建"。

A CARL CO. LOND IN COMPANY

●启动 ●停止 <mark>十新建</mark>	自删除	〇自检规则				
规则名称	规则类型	相关事件	创建时间 ≑	开始时间	持续时间	操作
						无数据

4. 基本信息填写,带有*的为必填项。

* 规则名称	请输入					0/64
规则描述	请输入					0/500
* 规则类型	请选择					
* 规则模板	请选择类型	\sim				
	规则模板描述:					
标签	请选择类型	~	标签编辑			

5. 选择规则类型和规则模板后,还需要配置原始告警源、时间窗口、告警配置等。其中时间窗口需要在2小

时以内。

医松牛带花					
原始告警源					
原始告警	~ 请选择告警名称	~	过滤条件	无 🗾 1	Ŵ
原始告警	~ 请选择告警名称	\sim	过滤条件	无	Ū
添加告警					
时间窗口					
*窗口大小	请输入	分钟	~	×	
分组条件	请选择类型			v	
7.00010.000.0000.000.000					
告警配置 * 归并模式	 不归并 後自然日(0点-24点)归并 	按会适归并	会话间隔	0 分钟 ~	
告警配置 * 归井模式 分组条件	 不归并 按自然日 (0点-24点) 归并 请选择类型 	○ 按会话归井 🗧	会话间隔	0 分钟 ~	
告警配置 * 归并模式 分组条件 其它输出字段	 不归并 後自然日 (0点-24点) 归并 请选择类型 请选择类型 	○ 按会话归井 🗧	会话间隔	0 分钟 V V	
告警配置 * 归并模式 分组条件 其它输出字段	 不归并 按自然日 (0点-24点) 归并 请选择类型 请选择类型 侦选择类型 	按会适归并	会活间隔	0 分钟 V V V	
告警配置 * 归并模式 分组条件 其它输出字段 原始告誓阶段 原始告誓级别	 不归并 按自然日 (0点-24点) 归并 请选择类型 请选择类型 侦查 援醒 	按会适归并	会话间隔	0 分钟 ✓ ✓ ✓	
告警配置 • 归开模式 分组条件 其它输出字段 原始告警阶段 原始告警级别 原始告警内容 ●	 不归并 後自然日 (0点-24点) 归并 请选择类型 请选择类型 侦查 握羅 请输入 	○ 按会适归并	会活间隔	0 分钟 ~	
告警配置 * 归开模式 分组条件 其它输出字段 * 原始告警阶段 * 原始告警阶段	 不归并 ● 按自然日 (0点-24点) 归并 博选择类型 博选择类型 (侦查 提醒 请输入 	○ 按会适归并 :	会话间隔		0/1
告警配置 *归开模式 分组条件 其它输出字段 *原始告誓阶段 *原始告誓阶段 *原始告誓内容 •	 不归并 按自然日 (0点-24点) 归并 请选择类型 请选择类型 依查 援聲 请输入 请输入 	 按会适归并 	会活间隔		0/1

6. 配置完成后, 单击"保存"。列表中可以看到新建的规则。

	^							
周洞管理		065 07£ +###	回删除 C自检规则					
弱口令管理		我即找回	规则类型相关告誓					创建时间
威胁运营	~	◇ 系统异常规则组	系统异常					2024-12-02 12:31:12
告警察法								
告警管理	<	10014230	和利米型 相关告释	创建时间,一	开始时间	*#######	財用第二	15/5
告誓列表		AND LAW		CARENJES &	212443152	10.2011/1	R.J. Santa	Juni P
通知管理	~	云等保专区_下一代防火墙_ 威胁日志_1.0境板	系统异常	2024-12-02 12:31:12			5分钟	•

复制规则

- 1. 选择模板规则或者已经创建好的规则。
- 2. 点击复制按钮复制规则。



云安全中心		关联分析										
资产中心	~											
资产概选		〇規則	ID/规则	名称/告警名称								\odot
资产管理		标签:										
风险管理	~											
漏洞管理		Oest		OP11: 十新建								
弱口令管理					抑则类型	相关告誓					创建时间	
成的运营	~		~		REE						2024 12 02 12:5	8.42
告警概览				ALCONT OF ALCONT	77021044-115							
告警管理		<	10	Naka	初则米型 相	大学委	创建时间,	####R###	4条经济时间	時间第二	元山	
告誓列表			~		10.000 TO	~=	ENERGIA +	VINING	10200103		JACI P	
通知管理	~		Z	等保专区_下一代防火墙_	系统异常		2024-12-02 12:31:12			5分钟	• i	
威胁检测	~	_		COLLING LOOPERC								
威胁建模				(安全卫士) 漏洞利用攻击	(安全卫士)	-						
对象管理			>	规则相	漏同利用攻击	周 间利用以击.					2024-12-02 12:3	1:12
分析中心	~		>	URL过滤日志规则组	URL过滤日志						2024-12-02 12:3	11:12
编即响应	~		5	可秘通信(下一代防火墙)规	可秘通信(下一	可疑用信					2024-12-02 12:3	1:12
报表中心	~			贝姐姐	代防火墙)							
已购资源			>	网络暴力破解规则组	网络暴力破解	网络暴力破解					2024-12-02 12:3	1:12
:c=			>	单包攻击规则组	单包攻击						2024-12-02 12:3	1:12

3. 编辑规则信息。

4. 保存规则(规则名称不能相同)。

启动规则

新建规则默认为停止状态,在规则操作列单击启动图标,或勾选规则后,单击列表上方的"启动",即可启动 规则。

停止规则

在规则操作列单击停止图标,或勾选规则后,单击列表上方的"停止",即可停止规则。

删除规则

注意:

启动状态的规则,不允许删除,删除规则前,请先停止规则。

在规则操作列单击删除图标,或勾选规则后,单击列表上方的"删除",即可删除规则。

自检规则

进入规则页面时,系统会自动检测规则的可用性,也可以单击列表上方的"自检规则",手动检测规则的可用性。

注意:

如果日志在集成配置中关闭了自动转告警,则会使对应的规则不生效,不产生告警。

4.4.5.2. 对象管理

展示有价值的内部信息,在关联分析时,对于 IP 类型、数字类型或字符类型的字段,可以添加过滤条件属于 信息,便于进行分析。通过导入内容包,系统已内置一些信息。

对象管理						
Q 遺输入名称	十新建 副除			请输入信息内容		查询
▼ 内部信息管理	信息内容	创建时间	更新时间	有效期	信息	操作
▼ IP类信息 内网IP		2024-08-15 14:15:42	2024-08-15 14:15:42	一直有效	内网	∠ ±
DNS服务器IP						
邮件服务器地址						
日志服务器地址						
重要网络设备资产IP						
数据库服务器IP						
保留IP地址列表						
▶ 数字类信息						
▶ 字符类信息			共1条 30条	页 ~ <	1 >	前往 1 页
▶ 时间类信息						

4.5. 分析中心

分析中心可分别针对日志详情、告警信息和资产信息进行列表或图形化展示。以时间为横轴、发生告警的数量 为纵轴,展示符合查询关键字和查询时间窗的告警趋势图。

前提条件

已开通云安全中心实例。

4.5.1. 日志查询

查询条件

头部为自定义查询条件,方便管理人员通过关键字段信息或者时间段获取更精确的数据。具体操作参考"告警 管理"。

↔ 天翼云

日志查询 TQL **園** 最近7天 🗹 去自 🛅 🕒 🕸 查询 高级~ 共计 4253 条日志 💿 致命: 3 条 🖸 严重: 1 条 🤷 警告: 0 条 🚺 提醒: 0 条 \odot 数据总量: 4253 威胁类型 TOP12 1,800 1,500 BACKDOOR VULNERABIL... 1,200 900 600 BRUTE SSH -REVERSE_SH... 300 0 ATTACK 2024-08-11 2024 500 1,000 1,500 2,000 日志查询 图表分析 TOP分析 源IP地址 💲 目的端口 💲 源端口 ≎ 日志来源 💲 目的IP地址 💲 日志发生时间 🌲 192.168.1.37 7788 16489 服务器安全卫士 (原生版) 101.89.117.168 2024-08-16 00:10:07 10.101.2.141 2024-08-15 19:50:22 服务器安全卫士 (原生版) 172.16.0.179 10.115.0.23 服务器安全卫士 (原生版) 172.16.0.179 2024-08-15 19:50:22

线性图

中间的线性图,展现在某个时间的日志数据量。

日志查询					
TQL				圖 最近7天	🛃 去白 🗋 🕑 🕸 🏾 🎒 高級 🗸
共计 4253 条日志 🛛 致命: 3 条	🖸 严重: 1条 🛛 警告: 0条	▲ 提醒: 0条			0
成助党型 TOP12 BACKDOOR VULNERABIL. BRUTE SSH REVERSE_SH ATTACK 0 500 1,000	1,500 2,000	(2024-08-11 2024-08-12 2024	-08-13 2024-08-14 2024-08-15 2024-08-16
日志查询 图表分析 TOF	2分析				
源IP地址 令	目的端口 🌩	源端口 🗢	日志来源 💠	目的IP地址 💠	日志发生时间 🜲
192.168.1.37	7788	16489	服务器安全卫士 (原生版)	101.89.117.168	2024-08-16 00:10:07
10.101.2.141			服务器安全卫士 (原生版)	172.16.0.179	2024-08-15 19:50:22
10.115.0.23			服务器安全卫士 (原生版)	172.16.0.179	2024-08-15 19:50:22

日志查询

最下面表格是展示查询的数据,表格中展示的字段可以自己定义,每条数据下拉能够看到详细数据。

①控制日志查询列表表头字段

② 日志查询列表数据展示



日志查询图表分析	TOP	分析							
已选字段	1	«	2	源IP地址 🜲	目的端口 💠	源端口 🗢	日志来源 🜲	目的IP地址 💠	日志发生时间 🍦
源IP地址					7788	16489	服务器安全卫士 (原生版)		2024-08-16 00:10:07
目的端口							服务器安全卫士 (原生版)		2024-08-15 19:50:22
源端口							服务器安全卫士 (原生版)		2024-08-15 19:50:22
日志来源							服务器安全卫士 (原生版)		2024-08-15 18:02:26
目的IP地址							服务器安全卫士 (原生版)		2024-08-15 18:01:25
日志发生时间							服务器安全卫士 (原生版)		2024-08-15 18:01:25
待选字段							服务器安全卫士 (原生版)		2024-08-15 18:01:24
Q请输入搜索待选字段							服务器安全卫士 (原生版)		2024-08-15 18:01:24
规则标签							服务器安全卫士 (原生版)		2024-08-15 18:01:24
所屬系统名称							服务器安全卫士 (原生版)		2024-08-15 18:01:18
攻击结果						# 4252 & 1		4 5 6	426) 前往 1 页
日志级别						× 1202 ж	2 3	- 5 0	

日志查询结果栏字段筛选:

目的IP地址 ≑	开始时间 ≑	目的端口 ≑	源IP地址 ≑	日志級別 💠	攻击类型 ≑	日志发生时间 💠	已选字段
192.168.24.80		80	202.103.95.207	致命	本地文件包含	2024-12-05 14:22:51	目的P地址
192.168.24.80		443	202.103.95.207	致命	文件上传	2024-12-05 14:22:51	开始时间
192.168.24.80		443	202.103.95.207	致命	PHP反序列化	2024-12-05 14:22:41	目的端口
192.168.24.80		80	202.103.95.207	政命	Java 反序列化	2024-12-05 14:22:41	源P地址
192.168.24.80		443	202.103.95.207	政命	ASP 代码执行	2024-12-05 14:22:41	日志級別
192.168.24.80		80	202.103.95.207	致命	Java 代码执行	2024-12-05 14:22:31	攻击樂型
192.168.24.80		443	202.103.95.207	致命	通用代码执行	2024-12-05 14:22:31	日志发生时间
192.168.24.80		443	202.103.95.207	致命	Java 代码执行	2024-12-05 14:22:30	待选字段
192.168.24.80		80	202.103.95.207	致命	Java 代码执行	2024-12-05 14:22:20	○適給入授業待选字段
192.168.24.80		443	202.103.95.207	政命	Java 代码执行	2024-12-05 14:22:20	日志来源
192.168.24.80		80	202.103.95.207	政命	本地文件包含	2024-12-05 14:22:10	规则标签
192.168.24.80		80	202.103.95.207	政命	SOL注入	2024-12-05 14:21:28	所属系统名称
192.168.24.80		80	202.103.95.207	致命	×SS政击	2024-12-05 14:21:28	攻击结果

图表分析

图表分析可以选择不同的图表类型与样式,并可以自定义发布到专题分析图表库。





单击"发布到专题分析图表库",弹出如下对话框,选择分类后,单击"确定",将图表发布到专题分析图表 库。



原始告警查询具体操作请参考"日志查询"。

原始告警查询



原始告警查询结果栏字段筛选:

原始告警查询	图表分析									¥.
告答阶段 💲	告答内容 ÷	告告产品 👙	灏iP地址 💲	目的端口 👙	源端口 ≑	日志来遊 💲	告誓威胁类型 🔅	机器ID ‡	已选字段	
攻击	发起系统状态日志,请注意关注!								告誓阶段	
利用	发起网络通信保护,请注意及时关注!								告警内容	
攻击	发起系统状态日志,请注意关注!								告響产品	
利用	发起网络通信保护,请注意及时关注!								運呼地址	
双击	发起系统状态日志,请注意关注!								目的講口	
利用	发起网络通信保护,请注意及时关注!								決済し	
利用	192.168.0.4发起会话日志,请注意处		192.168.0.4	50514	59549				白豆水理	
双击	发起系统状态日志,请注意关注!								相關的	
利用	发起网络通信保护,请注意及时关注1								告要名称	
利用	发起网络通信保护,请注意及时关注!								告誓创建时间	
双击	发起系统状态日志,请注意关注!									
利用	发起网络通信保护, 请注意及时关注!								待选学段	
利用	发起网络通信保护,请注意及时关注!								口调细人理至待地子段	
利用	发起网络通信保护,请注意及时关注!								目的IP地址	
双击	发起系统状态日志,请注意关注!								规则标签	
利用	发起网络通信保护,请注意及时关注!								週P系统省标 落:5:4 章	
攻击	发起系统状态日志,请注意关注!								2011日本市	
利用	发起网络通信保护,请注意及时关注!								日本人取口の心	
双击	发起系统状态日志,谓注意关注!								加別名称	
利用	发起网络通信保护,请注意及时关注!								告警戒助信息	
				共 1363 条 20条/	م × <	2 3 4 5	6 69 >	前往 1 页	告警用户账号	

图表分析





4.5.3. 告警查询

告警查询具体操作请参考"日志查询"。

告警查询

ш	云安全中心		告整查询			
	安全态势 资产中心		Tal		 意応天 〇 ③ 	三 約
	风险管理		共計1条告誓 🔹 歌会:0条 💶 芦童:0条 💶 警告:1条 🚨 講醒:0条			0
	分析中心		数编记量 1 1	0		
	原始告誓查询		0	2024-10-08		
	告誓章词 专题分析					
	编即响应 报表中心		□ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	目的端口 🗢	威動米型 🗢	
	已购资源 设置	÷	10.124.23.23		BRUTE	
					共1条 2096页 ~ く 1 >	前往 1 页

告警查询结果栏字段筛选



王人 ≑	告誓规则类型名称 💠	源端口 令 目的IP 令	已选字段
	Web应用防火墙(原生版)告警	192.168.24.80	责任人
	Web应用防火墙(原生版)告警	192.168.24.80	告警视则类型名称
			源海口
		共2条 20象页 ∨ < 1 > 前往 1	页目的IP
			待选字段
			○清給入搜索特选字段
			词 P
			描述
			关联分析规则名称
			告醫阶段
			告警D
			宣孙二载之帝

图表分析

Ⅱ 云安全中心		告警查询		
安全态势 资产中心	*	TOL	□ 素が天	11 O (\$ 🗾 🗮 ×
风险管理	•	共计1条告誓 🛛 政命:0条 🛄 严重:0条	□ 警告:1余 □ 提醒:0余	0
分析中心 日志查询	×	影振告量 1	。 ◎ 2024-10-08 ● 数量:1	
原始告誓查询		0	2024-10-08	
专题分析		告誓查询 图表分析		
报表中心 已购资源	æ	X抽 create_Eme ~	告警查询折线图 🖉	▷发布到考惑分析图表率
62		- 10 + Y抽 数量 ~		
		分組 満志得失型 ~		_
		株式		

4.5.4. 专题分析

专题分析可以提供多个内部页签的大盘展示页,用户可以新增、编辑、删除专题。

创建专题

- 1. 登录云安全中心控制台。
- 2. 在左侧导航栏选择"分析中心 > 专题分析"。
- 3. 单击"专题 > 创建专题"。



专题分析		
歯 近30天	<tr ✓ ① +创建专题 ②	
	请创建一个新专题或打开已创建的专题	

4. 在弹出的创建专题对话框中,填写专题名称,单击"确定",完成创建。

创建专题		×
* 专题名称	test	
	取消	确定

配置专题

1. 从图表库中拖拽所需图表至左侧空白处。



2. 如果需要编辑图表,单击图表框右上角的编辑按钮,会跳转至对应图表分析页面。如下图点击后会跳转至

"告警查询"的图表分析页面。编辑完图表后, 需要重新将图表发布到专题分析图表库。



3. 图表库增加删除按钮,删除后报表模板中的图表分析也会进行对应删除。

三 CO 天愛云 State Close	控制	1台 Q 搜索 義用	工单 备案 支持 合作 🗘 ⑦ s*********m
云安全中心		专题分析	
安全态势	~	商 今天 ✓ ◆簡 ✓	图表库 →
资产中心	~		请选择分类 ~ 请输入图表名称 <u>查询</u>
威胁运营	×		
分析中心	~	提示	
日志查询		当前操作会影响这图表在报表中的展示, 请确认是否删除?	35 30 25
原始舌答查询 告答查询	<	ROM	
专题分析		请创建一个新专题或打开已创建的专题	病毒防护 流量日志 访问异常
编排响应	~		
报表中心	~		系统异常行为
已购资源			35
设置	~		30 25 20 15

= Co 天翼	石 控制台		Q. 攙索 费用 工	单 备案 支持 合作 🧕 🕜 s*********
安全中心				
全态势	~	* 名称	test	常用 自定义指标 自定义图表
≃中心	~			法会)同主な名
≧管理	~	* 类型	○ 日报 ○ 周报 ● 月报 ○ 季报 ○ 年报	· 培制八团浓石砂 · · · · · · · · · · · · · · · · · · ·
的运营	~	*报表生成时间	15 ~ - ©00:00	端口扫描情况
斤中心	^			请选择 选择
日志查询		* 内容	段落 > 默认字体 > 小四 > 三 石 兰	100 80 9
原始告誓查询	<		⊞ × <i>I</i> < < < < < < < < < < < < < < < < < < <	60 40
吉蓉查询			$B I \underline{U} \underbrace{S} X_2 X^2 \underline{\mathscr{I}} \lor \underline{A} \lor$	
专题分析			≡ ≡ ≡ ≢≡ × IAI × © ×	100.89.2.190
响应	~		A	L
中心	~			
报表任务			120	云等保级别分布情况
服表模板			120	请选择 选择
阿资源			90	150 120

4.6. 编排响应

4.6.1. 剧本管理

为了提高告警处置的自动化程度及效率,提高告警解决方案的复用性。可以使用剧本将某些处置操作模板化, 程序化。在类似告警发生时,可以自动规则匹配或人工选择相关剧本进行自动化的处置。其中的剧本匹配规则, 则用于告警发生后,自动匹配并调用剧本进行操作。剧本管理模块则用于对这些剧本和剧本匹配规则进行统一 管理。剧本管理的的剧本列表,可以查看、新建、编辑、导入导出相关的剧本。



新建剧本

打开剧本管理的剧本列表界面,点击"新建",创建一个只有一个开始节点的新剧本。剧本新增页面右侧可对

剧本属性进行编辑。

	剧本管理		
1@t			
()		节点属性	剧本属性
20		制本名称	流程1721898196181 15/128
811		E	日常运营制本
0	\bigcirc .	FÆ	日常管理 × · · ·
	та	EY	process1721808100181
	,	支持场景	日常运营
		^غ [0/2048
		李問荃	=告誓剧本= ~ ~

说明:

- 一个剧本有且只有一个开始节点和结束节点。
- 每个用户在新增的剧本编辑界面停留过长时,会最多保留一份新增草稿,在用户下次新增时会提示是否进入草稿。
- 在对已存在剧本进行修改时,若在修改页面停留时间过长,会自动为改剧本保留一份草稿,在下次重新对 剧本进行编辑时提示是否进入草稿。
- 剧本保存时会对剧本进行校验,若该剧本存在不能到达或不能结束的孤立节点,需用户完善后才能保存。
 后续版本将会升级启停功能,非正常剧本允许保存,不允许启用。

新建完成后,可以在列表中看到新建的剧本。

标查	请选择		~	剧本名称 请输入			剧本类型 请选择							
状态	请选择		×	启停状态 请 选择		~							查询	1
æ ∼	◎ 删除	Pat Refer	副太米刑	花囊空欲	443公司/表计(集)公)	ಎಡಡಿಡಿಗಣ	查 acc时间	钟志	4 1	5/5				
	01租户副本	公有云版本	834	日常运营,HW 行动,安全运营	1/1	2024-05-31 09:31:59:526	2024-05-31 00:32:03.411	正本/未引用	c	Ľ	0	Ð		
	流程1718984531284	公有云版本	本場	日常运营,HW 行动,安全运营	5/5	2024-05-29 15:13:57.863	2024-05-29 15:14:01.441	正本/未引用	с	1	0	Ð		

新增剧本节点

选择节点后,点下如下按钮,新增剧本节点。

剧本管理			
2)保存开发布 +新建 つ C Q Q	节点属性	剧本属性	
	节点类型	bpmn:StartEvent	
0 % 2	节点ID	StartEvent_01ydzqe	
	节点名称	开始	2/32

新增的节点默认为用户节点。选取节点后,右侧可对节点属性进行编辑。



剧本管理			
習 保存井发布 → 新建 つ C Q Q	节点属性	剧本属性	
	节点类型	bpmn:User1	ask
	节点D	UserTask_1	Dgnvb5
O & 物 首 2	* 节点名称	用户节点	4/32
	备注		0/2048
7714	单位名称	=单位名称=	~
	角色名称	=角色名称=	~
	处理人员		
	人员列表	ē 0/0	已选择 0/0
	无数据		无数据
	处理时限	天	时分
	是否允许终止	◉ 允许	○ 不允许

● 是否允许终止

终止功能,剧本编辑界面如图所示。

本查看				
R 7.777788	节点属性	剧本属	±	
	角色名称 处理人员	=角色名称:	1	×
	人民利养 无数据	010	C Bizif	0/1 in
	处理时限	1 天	时	分
	是否允许终止	① 允许	〇 不 允许	
	是否允许回過	 	○ 不允许	
	拉验工具	=检验工具:		×
	采集数据	+		

有"终止"权限的人工节点(在剧本编辑中设置),可以"终止"当前告警工单的剧本执行。



1.117.106.197对172.17.0.2触	发告警,攻击类型为XSS攻击			责任人修改
玉阶段: 【侦查】	发生时间:2024-05-29 17:50:34	外部成胎尸	影响资产:	
或时间表: 2024-05-31 23:28:28	处置建议:			
工单处量				
用户节点 处量意见			G	当前剩余:1天0小时0分钟)

• 处理时限

人工节点处理时限,剧本编辑中,人工节点编辑界面,可以设置该节点处理时限设置。剧本编辑,设置人工节点处理超时时限,如下图所示。

剧本查看				
25 分布法本 Q、 Q、 (0)	节点属性	剧本属性		
0 4 4 11 2	管注			0/2048
	角色名称	sec22030001 =角色名称=	@ IOS.COM	-
	处理人员			
	□ 人员列表	0.0		0/1
	无数据		chenwer	
	处理时限	1 天	时	分
	是百允许终止	允许 () 不允许	
	是否允许回還	• 允许 () 不允许	

设置后,在告警管理列表和告警处置中会显示是否超时。

脑入事件名或资产中					~ 最近7天		推行 重百 共	H MiR
) 处置中 处置完 -	成 自动处量 勿离处量							
◆ 教授 重発	28	油粉研習 ↓						
副本 ‡	发生时间 🗘	环节名 ≑	完成时限 ≑	制余时间 🗅	当前状态 ‡	完成时限 💠	制余时间 🗘	19
副本 ≑ 01祖户副本	发生时间 ↓ 2024-05-29 17:50:34	鮮物名 ≑ 川)≏問』芯(chenwen)	完成时限 ‡ 2024-06-01 11:26:29	剩余时间 ‡ 0天21小时	当前状态 ‡ (秋道中	完成时限 ‡ 2024-05-31 23:26:28	對余时间 ≑ D天9小81	19
副本 ‡ 01祖户副本	¥生田3(明) 수 2024-05-29 17:50:34 2024-05-24 10:01:36	時時名 \$ 川户哲成(chenwen)	完成时限 章 2024-08-01 11:25:29	制余时间 \$ 0天21小时	当前状态:	完成时禄 ↓ 2024-05-31 23:26:28	剩余时间 \$ 0天9小时	39
副本 ‡ 01祖戸副木	数生的间 ↓ 2024-05-29 17:50.34 2024-05-24 10:01.35 2024-05-21 17:17:35	時物名 ‡ 川(戸哲xǐt(chenwēn)	現成时期 0 2024-08-01 11:25 29	制绘图500 ≑ 0天21小时	当前状态 \$ <u> 秋田</u> 中 将秋田 将秋田	現成的操 章 2024-05-31 23:26:28	新会的问 ≑ 0天9-)0j	19
副本 수 011山으리木	牧生町同	時物名 0 川(戸町)式(chenwen)	完成时期 ↓ 2024-08-01 11:25 29	制会(19月1日) ¢ 0天21小(19月	当時状态 \$	完成的第 ↓ 2024-05-31 23:28:28	新会封网 ↓ 0天9小时	55

新增脚本任务节点



点击默认新增的用户节点,在节点上方显示节点工具,选择脚本任务。

剧本管理		
四 保存并发布 +新建 つ C	Q Q	
	◎ 剧本任务 5 脚本任务	

切换为脚本任务后,系统默认从左侧弹出插件选取栏,可通过插件选取栏搜索相关插件或直接选取。

说明:

依据定时任务配置,当系统在配置的间隔时间内触发了告警时,每间隔一段时间发送产生的告警数量

,紧急告警数量的短信通知用户。

充插件				
2有云Soar短信邁知插件 v1.0.0	~ Q		节点题	性 副本属性
95년信 天版本soar短信插件发送短信	25年		节点类型	bpmr:ScriptTask
	1		15,000	UserTask_01g83up
	点击		*节点名称	脚本带点 4/32
			IMAR	5
	O 🌡 🍫	₫ ⁸ 4	量于模板	-迅排溢示模板- ~
				<u>SélHan</u>

也可通过右侧的节点属性中的查看工具/插件按钮弹出插件选取栏。



剧本管理		
D D C Q Q	节点属性	剧本属性
	节点类型	bpmn:SotpfTask
	节点ID	UserTask_01g83up
	*节点名称	脚本节点 4/32
	工具/油作名	公有云Soartellia道印度作。发送短信
O & % iii 2	* 9 租户ID	/ 0
	◎ 爭机号	0
	1 🔒 通知类型	0
开始	1 😝 通知消息	0
	调用服务	01角色
	显示模板	-选择型示模板- · ·
		查看工具储件
	/	
	击点	

选取完插件后,设置插件的入参。

剧本管理					
日 保存并没布 +新建 つ	C Q Q			节点属性	剧本属性
				节点类型	bpmn:ScriptTask
				节点回	UserTask_G1g83up
				- 节点名称	脚本节点 4/32
				工具编作名	公布云Soarie信道知题件,发送短信
		0 % % 🛍 😫		- <mark>9</mark> 祖中ID	0
				◎ 手机号	/ 0
)	\bigcirc			○ 通知共型	0
	开始	(. <u></u>		- 😦 道河消息	0
				VE PELIER PE	01角色
				显示模板	-选择显示模板- ~
					查看工具/抽件

剧本线条设置

点击线条,可以在线条上增加线条说明,以及在线条上添加判断条件,以控制流程走向。

剧本管理			
图 保存并没有	2 (14+	节点属住	剧本属性
		节点失型	bpmit:SequenceFlow
		节点ID	SequenceFlow_Gayzfx4
		节点名称	0/32
			li li
			选择为新行条件
c		_	

点击"选择判断条件",增加或修改线条判断条件。



¥存井波布 + 新姓 つ C Q Q			节点属住	剧本属住
			节点类型	bpmn:SequenceFlow
			节点10	SequenceFlow_Dayztx4
			节点名称	0/32
				选择归新条件
				古丰
				加加
开始	結束			
到明室住设罢				
				×
				×
				×
	· 清洁择 · · · · · · · · · · · · · · · · · · ·	2.	0/32	×
★当時に下を上上	清近洋 〜 清明	iλ	0/32	×
a选择字段 ✓	清近祥 〜 清裕	λ	0/32	×
AND 添加条件	请选择 ~ 请谢	ίλ	0/32	X D
新法律字段 × AND × 添加条件 添加组 創除组	- 演送择 → 演討	λ	0/32	X
新造様字段 × AND × 添加条件 添加組 創除组	· 清送择 ~ 清闲	iλ	0/32	x

复制剧本

1. 选择已经创建好的剧本。

2. 点击复制按钮。

标签	请选择	~	剧本名称	请输入		剧本类型	请选择		
\$状态	请选择	×	启停状态	请选择	Ŷ				前
新建 ~	回 删除								
	剧本名称	剧本标签	剧本类型	场景名称	触发次数(累计/最近)	模板类型	创建时间	操作	
	云等保专区_下一代防火墙_境外IP 攻击封堵_模板	日常管理	剧本	日常运营	1	预置模板	2024-09-03	•]
	外部扫描攻击处置	外部扫描	剧本	日常运营	4	预置模板	2024-08-28	•	
	测试获取租户ID服务剧本4	日常管理	剧本	日常运营	25	预置模板	2024-09-03	•	
	atest	日常管理	剧本	日常运营		预置模板	2024-08-16	•	

3. 编辑剧本信息,确保剧本名称不重复。



く 剧本管理



4. 点击保存并发布,完成剧本复制。

4.6.2. 插件管理

插件管理支持管理所有的一类插件工具,这类插件工具拥有相同的接口调用。

通过插件管理,一类插件可以新建多个不同的连接服务,方便在剧本调用时灵活切换调用。

新增服务

- 1. 登录云安全中心控制台。
- 2. 在左侧导航栏选择"编排响应 > 插件管理",进入插件管理页面。

件管理	1				
	版本号	工具名	语言类型	12109	操作
>	1.0.0	公有云Web应用防火墙(原生版)插件	java	公有云Web应用防火墙(原生版)插件	Đ
>	1.0.0	公有云Soar短信通知插件	java	公有云通知插件	Œ

3. 单击操作列的新增图标,弹出新增服务对话框。

名称 test	*服务名称
备注	备注

测试连接

确定

4. 填写服务名称和备注信息后,单击"确定"。服务新增完成后如下所示。

	版本号	工具名	语言类型	说明	ê	腱人		操作	
	1.0.0	公有云Soar短信通知插件	java	公有云通知插件	题	級管理员	8	1	í
BR	時名称		状态	说明	创建人	操作			
ter	est		off		chenwen	a	0	m	

5. 服务状态默认为关闭,单击操作列的"启用"图标,启用服务。

4.6.3. 规则配置

规则配置模块可以进行规则的新建、查找、启动、暂停、查看与删除。

新建规则

- 1. 登录云安全中心控制台。
- 2. 在左侧导航栏选择"编排响应 > 规则配置",进入规则配置页面。
- 3. 点击"新建",新建剧本触发规则。填写规则名称,以及剧本触发条件,再勾选相关剧本即可。

٢	3天费云 拉制中心		剧本触发规则设置	×	费用 工样 發変	支持 合作	 ग	0
=	云安全中心	規则配置						
8	2420		- 现时名称	0/128				
G	WEDO -	規则名称 清临入规则做本名					會闲	EE
68	(2104-FB		* 触发条件					
FO	page -	+ 新建 + 白用 ③ 停用 1	- 音響名称	ũ				
()	9版中心 *	10169-9	AND ··· Iātuskit		Citetile	10.0	0.0	
	编组编成				2024 00 24 40 25	****		
20	····································		就没倒本		2024-09-24 18:35	340(212)	0 2 9	
~	浙体管理			-				
	規則配置		■本語編 音編入名称 ■本校整 音法科 ~	RX.				
101	报表中心 *		剧本名称 场限名称					
-	已购资源	2	多用户节点 日常运算					
3	设置 -		⑦ 预制告罄培復_1725904972470 日常运营					
0								
#								
-								
9								
9				_				
			* SLA(处置时限) 12小时	1997				
			83					
				0/2048/				
			Ria	R #				

启动规则

规则新建完成后,默认为"未启动",单击操作列的启动图标,启动规则。

规则配置									
规则名称	请输入规则/剧本名							查询	重置
+ 新建	▶ 启用 ◎ 停用	創 删除							
	规则名称	处置剧本/工具	处置时限	备注	创建时间	状态	操作		
	test	(剧本) 预制告警短信_172590497	12小时		2024-09-24 18:35	未启动	0	/ 8	Ū

4.7. 报表中心

报表中心是用户生成报表的功能模块。该功能模块主要由两部分组成,分别是报表任务和报表模版。通过报表 任务,用户能够定时的生成报表内容。通过报表模版,用户能指定报表的格式以及排版。

4.7.1. 报表任务

报表任务功能,实现管理和维护报表任务,用户可以自定义报表的生成周期,每个用户需要自行管理自己的报 表任务。

可以实现:新建即时报表任务、新建周期报表任务、查看报表任务、删除报表任务以及生成报表等功能。

说明:

周期报表任务执行时发送报表短信到用户在系统配置的手机号。

前提条件

已创建报表模板。

新建报表任务

- 1. 登录云安全中心控制台。
- 2. 在左侧导航栏选择"报表中心 > 报表任务"。

云安全中心		报表任务					
安全态势	•	状态 请遗择		→ 名称 请输入			青海
资产中心	•						
风险管理	*						
威胁运营		十新建					
分析中心	•	名称	状态	开始时间	结束时间	报表	操作
工单管理							
编排响应	•	4			无数据		
报表中心 报表任务	•					共0 条 20条/页 ~ 〈	1 > 前往 1 页
报表模板							
已购资源							
设置	•						

9. 单击"新建", 弹出新建报表任务对话框。填写报表名称、选择报表模板、选择报表类型(支持即时报表任务、周期报表任务)。

* 报表名	Z称		
1000	-13.		
* 报表核	莫板 请选择	~	
报表学	きを見ていた 日期		
报表学	料		



4. 配置完成后,单击"保存"。

管理报表任务

启动周期性任务

在周期性报表任务的操作列,单击"立即启动"图标。(周期性报表任务最多启动10个任务)

十新建					
名称	状态	开始时间	结束时间	报表	操作
日报3	创建	2024-06-27 17:53:08	2024-06-27 18:23:08	Ē	ΖūΟ

编辑报表任务

在周期性报表任务的操作列,单击"编辑"图标。报表名称不支持修改,其余参数均可修改。

十新建					
名称	状态	开始时间	结束时间	报表	操作
日报3	创建	2024-06-27 17:53:08	2024-06-27 18:23:08	Ē	2 0

查看报表

单击如下图标,查看已生成的报表列表。并支持下载报表到本地。

十新建					
名称	状态	开始时间	结束时间	报表	操作
日报3	创建	2024-06-27 17:53:08	2024-06-27 18:23:08	Ē	2 1 0

4.7.2. 报表模板

报表模板,维护和定义报表模板,用户可以自定义报表的模版,每个用户需要自行管理自己的报表模版。 支持自定义指标、自定义图表以及报表预览等功能。

新建模板

- 1. 登录云安全中心控制台。
- 2. 在左侧导航栏选择"报表中心 > 报表模板"。
- 3. 单击"新建",进入新建模板页面。

报表模板	
报表模板 新建模板 ×	
* 名称 * 类型 ④ 日报 周报 月报 季报 年报	常用 自定义指标 自定义图表
**时间范围 **内容 段落 ~ 默认字体 ~ 小四 ~ 徑 徑 徑 筐	∃ ~ <i>I</i> ×
	♥ ♥ ▼

4. 配置模板名称、类型、时间范围和报表内容。

其中类型指定的时间为报表自定义指标的默认数据周期时间(当自定义指标中指定了绝对时间后,会覆盖 默认数据周期时间)。

5. 单击"保存",保存模板。

云安全中心		报表模板									
安全概念		报表模板									
资产中心											
风险管理		+ 新建 0 200						请输入名称			С
威胁运营	-	D ID	名称	类型	状态	创建时间	更新能	涧	操作	F	
分析中心	~	21	周报	周报	可用	2024-04-22 10:57:56	2024-04-22	10:57:56	0 /	Û	
工单管理		20	日报	日报	使用中	2024-04-22 10:50:01	2024-04-22	10:52:42	0 /	ū	
编排响应	- 4										
报表中心	•					共2条	20条/页	< 1	> 1	前往 1	页
报表任务											
报察模板											
已购资源											
	*										

4.8. 设置

4.8.1. 集成配置

开通云安全中心实例后,系统默认会接入部分日志数据并对用户进行初始化配置。您可以根据自己的业务特性 修改初始化配置。

打开云安全中心的"设置 > 集成配置",在集成配置中选择需要接入的日志类型。部分日志支持直接转告警, 可以直接打开转告警开关,云安全中心会根据内置转告警规则进行转告警配置。



前提条件

需确保要接入日志的数据源监控处于启用状态。具体操作请参见数据源监控。

操作步骤

- 1. 登录云安全中心控制台。
- 2. 选择"设置 > 集成配置",打开数据集成配置页面。
- 3. 选择需要接入的日志,并打开日志接入开关。



云安全中心		集成配置				
安全概范	27					
统产中心	э.	安全服务	日志美型	状态	日志接入	自动转告答
风险管理			1	已線入		
或動运営	×		1000 A	已接入		
分析中心	÷		2000	已接入		
工单管理		locati (1	*	已接入		
扁桃响应	ेर			已接入		
設ま中心	9			已接入		
200		4	Harden	已接入		
集成配置		-		未授入		
数据源监控						

4. 选择需要转告警的日志,并打开自动转告警的开关。

云安全中心		集成配置				
全概范						
萨中心		安全服务	日志笑型	秋态	日志掖入	自动转告答
心管理				已援入		
动运营				已接入		
忻中心			المراجعيني ا	已接入		
半世現				已接入		
唯明应			107	已接入		
表中心	-		8	已接入		
ii.	•	•		已接入		
THE PACE		and the second s		未把入		
数据琼蓝控						

说明:

- 系统默认会接入部分日志,用户如有需要,可以自行关闭。
- 需要先在数据源监控页面启用开关后,才可以在集成配置页面中开启日志和告警配置。
- 选择需要接入的日志时,只能针对您已经购买的云产品。
- 选择需要转告警的日志,只能针对已经选择接入的日志进行。
- 自动转告警打开,对应的日志类型才能产生告警。

4.8.2. 数据源监控

在数据源监控中可以查看到已经接入到系统的数据源。可以直接通过开关对数据源进行开启或关闭,云安全中 心会根据您的操作对数据源数据进行收取或拒绝收取。

1. 点击"设置 > 数据源监控",打开数据源监控页面。



云安全中心		数据源监控							
安全态势	÷								
资产中心	•	数据源IP: 请输入数	效据源IP	重海 重量					
风险管理	•								
威胁运营	-	Kafka日志	Syslog日志						
分析中心	-								
工单管理		数据源IP	资产名称	设备厂商	设备类型	端口	状态	收到最近一条日志时间	操作
编排响应	- 1	192.168.1.101	服务器安全卫士 (原生版)	天翼云	主机	9092	启用中		00
报表中心	•	127.0.0.1	Web应用防火墙 (原生版)	天翼云	防火増	9092	启用中		00
已购资源						共2条	10条/页	× < 1 >	前往 1 页
设置	•								
集成配置									
数据源监控									

2. 选择需要接入的数据源,并启用数据源。

Kafka日志	Syslog日志						
数据源IP	资产名称	设备厂商	设备类型	端口	状态	收到最近一条日志时间	操作
192.168. <mark>1</mark> .101	服务器安全卫士 (原生版)	天翼云	主机	9092	启用中		00
127.0.0.1	Web应用防火墙 (原生版)	天翼云	防火墙	9092	启用中		00

说明:

- 选择需要接入的数据源时,只能针对您已经购买的云产品。
- 停止数据源,对应的"集成配置"将不允许操作。

4.8.3. 规则标签配置

云安全中心的规则标签功能,提供白名单及自定义的规则标签,用户可设置需要打标签的日志筛选范围,并赋 予其白名单或自定义的标签。

- 白名单标签:当日志解析出的内容匹配到了白名单标签规则,日志则会被标记为白名单,对应日志将不会
 产生告警。
- 自定义标签:当日志解析出的内容匹配到了自定义标签规则,日志则会被标记为自定义标签,仍然会产生告警。

新增标签规则

- 1. 登录云安全中心控制台。
- 2. 在左侧导航栏选择"设置 > 规则标签配置",单击"新建"。

↔ 天翼云

规则标签	配置					
Q请	输入内容					查询
状态:	· 開 ∨ ^{杨签} 点击	多选项		~		
十新建						
	有效期	标签	内容	命中次数 🜲	创建时间 🗢	
	永久有效	白名单	源IP地址 = 192.168.0.9 and 目的IP地址 = 100.89.2.190 an d 威胁类型 = EDR and 日志未 源 = 云等保专区	0	2024-11-08 09:51:40	z ū 💽

- 3. 在弹出的新增窗口中,配置标签、匹配条件、有效期、备注信息。
 - 标签:支持选择一个或多个标签。
 - 标签设置为白名单时,当日志解析出的内容匹配到了标签规则,日志则会被标记为白名单,对应 日志将不会生成告警。
 - 标签设置为自定义标签时,当日志解析出的内容匹配到了标签规则,日志则会被标记为自定义标签,不影响告警产生。
 - 标签同时设置了白名单标签和自定义标签时,当日志解析出的内容匹配到了标签规则,日志则会 被标记为白名单+自定义标签,对应日志将不会生成告警。
 - 匹配条件:配置日志内容需要匹配的条件。
 - 有效期:标签规则仅在有效期内生效。若不配置,则永久有效。

	~			~`			
* 标签 * 匹配条件	自名单源IPt	跑过标名	<u>+</u> × <u>+</u>	J			
有效期		2024-11-08	至	2024-11-16	0		
* 备注	test						

4. 参数配置完成后,单击"保存",回到规则标签配置页面。



启用/停止标签规则

● 启用标签规则,规则生效,日志匹配标签规则。

十新建	首删除					
	有效期	标签	内容	命中次数 💠	创建时间 💠	启用状态
	永久有效	白名单	源IP地址 = 192.168.0.9 and 目的IP地址 = 100.89.2.190 an d 威胁类型 = EDR and 日志来 源 = 云等保专区	0	2024-11-08 09:51:40	× •

● 停用标签规则,规则失效,日志不匹配标签规则。

十新建	首删除					
	有效期	标签	内容	命中次数 🜲	创建时间 💠	停用状态
	永久有效	白名单	源IP地址 = 192.168.0.9 and 目的IP地址 = 100.89.2.190 an d 威胁类型 = EDR and 日志来 源 = 云等保专区	0	2024-11-08 09:51:40	Z 🛛 💽

从日志添加标签规则

- 1. 登录云安全中心控制台。
- 2. 在左侧导航栏选择"设置 > 规则标签配置"。
- 3. 在日志查询列表找到需要添加标签的日志,点击日志。

日志查询 图表分	计析 TOP分析				
告警名称 🜲	源IP地址 🗢	目的IP地址 ≑	威胁类型 ≑	日志级别 🌩	日志发生时间 🗢
数据窃取攻击	192.168.0.9	100.89.2.190	EDR	警告	2024-11-07 20:26:16
漏洞扫描	192.168.0.9	100.89.2.190	EDR	整告	2024-11-07 19:34:16
漏洞扫描	192.168.0.9	100.89.2.190	EDR	警告	2024-11-07 19:34:16
数据下载异 ^常	192.168.0.9	100.89.2.190	EDR	蓉告	2024-11-07 19:33:16
数据下载异常	192.168.0.9	100.89.2.190	EDR	整告	2024-11-07 19:33:16
可疑域名访问	192.168.0.9	100.89.2.190	EDR	警告	2024-11-07 19:33:16
可疑域名访问	192.168.0.9	100.89.2.190	EDR	蓉告	2024-11-07 19:33:16

4. 在日志详情页,单击白名单按钮。

查看详情				点击白名单按钮 ×
基本信息	威胁详情	原始信息		e.
日志来源	ତ ତ	云等保专区	进程路径	123
厂商		云等保	安全服务编号 ① 〇	platform-c
产品		主机安全	登录账号	cm9vdA==
公有云租户ID	ର ପ	1ff24e947bfb4af9a66a48f66591b5a6		
协议		ТСР	动作	已拦截
日志级别	ତ ତ	警告	事件类型名称	全局事件
告警名称	ତ ତ	数据窃取攻击	日志发生时间	2024-11-07 20:26:16
服务ID	0 Q	2183	威胁类型 ④ 〇	EDR
五元组				
源IP地址		192.168.0.9		
源端口	ତ ପ	58164		
目的IP地址		100.89.2.190 共享地址/共享地址/ (/)		

5. 在弹出的新增窗口中,配置标签、匹配条件、有效期、备注信息。参数配置完成后,单击"保存"。

塇			7)74/77/7	<u>v</u>			
*标签	白名单		in an	+			
*匹配条件	源IP地	助上 = 192.168.0	.9 and 目(的IP地址 = 100.89.2	.190 and 威胁类型 = E	DR and 日志来源 = 云等保专区	¢
有效期		开始日期	至	结束日期	0		
* 备注	test					点击保存	
						取消	保存

查看日志的标签

- 1. 登录云安全中心控制台。
- 2. 在左侧导航栏选择"设置 > 规则标签配置"。
- 3. 在日志查询列表的"规则标签"列,可以查看日志的标签。

日志	查询 图表分析	TOP分析					
	渡IP地址 ≑	目的IP地址 💠	威胁类型 ≑	日志级别 💠	日志发生时间 ≑	厂商 ≑	规则标签 💠
窨	139.200.108.9	47.109.21.183	ALARM	歡命	2024-11-04 15:15:30		["测试标签"]
	139.200.108.9	47.109.21.183	ALARM	致命	2024-11-04 15:14:30		["测试标签"]
警	139.200.108.9	47.109.21.183	ALARM	致命	2024-11-04 15:13:30		
譇	139.200.108.9	47.109.21.183	ALARM	致命	2024-11-04 09:31:30		["测试标签"]

4. 在日志查询列表找目标日志,点击日志。

↔ 天翼云

5. 在日志详情页的基本信息中,可以看到"规则标签"。

查看详情						×	
基本信息	威胁详情	原始信息					
规则标签	Q (Q	[测试标签]	日志来源	0 D	Web应用防火墙 (原生版)		
安全服务编号	ତ୍ର ତ୍ର	waf					
公有云租户ID	€ ⊝	1ff24e947bfb4af9a66a48f66591b5a6					
攻击类型		22	动作		拦截		
日志级别	\odot	致命	事件类型名称		全局类型(内置)		
告警名称	ଭ ଭ	Web应用防火墙(原生版)告警					
注入规则ID	\odot	-6b139e43c9ca456a9b9be04bc4c9694c					
日志发生时间		2024-11-04 15:15:30	威胁类型	0 Q	ALARM		
五元组							
源IP地址		139.200.108.9 中国/四川/宜宾 (104.16293/28.	64369) (电信)				
目的IP地址		47.109.21.183 中国/四川/成都 (104.06151/30.	17.109.21.183 中国/四川/成都 (104.06151/30.67387) (阿里云/电信/联通修动教育网)				
目的端口	⊚ ⊝	8090					



5. 最佳实践

5.1. 如何进行剧本管理

为了提高告警处置的自动化程度及效率,提高告警解决方案的复用性。可以使用剧本将某些处置操作模板化, 程序化。在类似告警发生时,可以自动规则匹配或人工选择相关剧本进行自动化的处置。其中的剧本匹配规则, 则用于告警发生后,自动匹配并调用剧本进行操作。剧本管理模块则用于对这些剧本和剧本匹配规则进行统一 管理。剧本管理的的剧本列表,可以查看、新建、编辑、导入导出相关的剧本。

		剧本标签	请选择		× .	剧本名称	輸入		剧本类型 请选择							
*																
		剧本状态	清法择		~	启停状态 谱	造操	×.							畫面	-
•		新建 ~	 ● 删除 ● 删除 	日春出												
			剧本名称	剧本标签	剧本类型	场景名称	餘发次数(累计)最近)	创建时间	更新时间	状态	6 1	操作				
	4		01程户剧本	公有 <mark>云版本</mark>	副本	日常运营.H 行动.安全运	V 1/1	2024-05-31 09:31:59.526	2024-05-31 09:32:03.411	正本/未引用	с	1	0	đ		
					P.+	日常运营用	V 5/5	2024-05-29 15 13:57 863	2024-05-29 15:14:01:441	正本/未引用	c.	42	0	-		

1、打开剧本管理的剧本列表界面,点击新建,创建一个只有一个开始节点的新剧本。剧本新增页面右侧可对

剧本属性进行编辑。

云安全中心		剧本管理		
安全板院	-	□ 保行共気布 + 新建 つ C Q Q	节点属性	剧本属性
资产中心	÷		* 副本名称	流程1717123123405 15/128
风险管理	*			<u>1</u> 00000
成勘运营				▼ 安服制本
分析中心	-	\bigcirc	*标签	遺法择 ×
工業管理		开始		+ 请告评切签
编排响应	-		KEY	process1717123123405
报表中心		•	* 支持场景	□ 日常运营 □ HW行助
12 1	-			· 安全遗营
			警注	0.0040
				012040/
			事件剧本	=審佛殿本= ~ ~

说明:

一个剧本有且只有一个开始节点和结束节点。

每个用户在新增的剧本编辑界面停留过长时,会最多保留一份新增草稿,在用户下次新增时会提示是否进入草 稿。

在对已存在剧本进行修改时,若在修改页面停留时间过长,会自动为改剧本保留一份草稿,在下次重新对剧本 进行编辑时提示是否进入草稿。

剧本保存时会对剧本进行校验,若改剧本存在不能到达或不能结束的孤立节点,需用户完善后才能保存。后续 版本将会升级启停功能,非正常剧本允许保存,不允许启用。

2、剧本新增节点,默认为用户节点。选取节点后,右侧可对节点属性进行编辑。

云安全中心		剧本管理			
安全概范	•	₽ 8 8 3 2 C Q Q Q	节点属性	剧本属性	
资产中心	*	点击	节点微型	bpmn:StartEvent	
风险管理	•		ちょつ	StartFuent 01vdzne	
威胁运营	•				
分析中心	•		节点名称	开始 2/32	
工業管理		北京			
编排响应	•				
报表中心	•	•			
19 1	•				
云安全山心		P/+MTB			
AXITO		助本管理			
安全抵抗		D 保防井波布 →家舗 つ C Q Q	节点属性	剧本属性	
资产中心	*		节点类型	bpmn:UserTask	1
风险管理	•	0 \$ 4 11 2	₩,ēID	UserTask_01g83up	Ш
■ 2000年 日本100日			*节点名称	用户节点 4/32	Ш
工業管理		π	警注	0/2048/2	Ш
编排响应	•		单位名称	=当片友致=	Ш
报表中心	•	4		an WPM.	Ш
12 1	•		角色名称	=角色名称= ~ ~	Ш
			处理人员		Ш
			□ 人员列表	0/0 日选择 0/0	Ш
			无数据	无数据	
			(+)理B168	→ B4 分	

3、终止功能,有"终止"权限的人工节点(在剧本编辑中设置),可以"终止"当前告警工单的剧本执行。 剧本编辑界面如图所示。


云安全中心		剧本查看				
安全概题		2) 月行为高法本 Q Q ○	节点属性	剧本属	±	
资产中心	-					
风险管理	*		角色名称	=角色名称		~
成助运营	*		处理人员			
分析中心	•		- Leve	0.0	- Dave	0/1
工業管理		开始	/_32954A	0.0		
编排响应			无数据		chenwer	C
报表中心		•				
2	•					
			处理时限	1 天	时	分
			是百允许终止	● 光祥	○ 不允许	
			是否允许回過	 允许 	〇 不允许	2
			检验工具	-拉脸工具		~
			采集数据	+		

開始		111.117.106.197对172.17.0.2触发告	警,攻击类型为X\$\$攻击			责任人修改
6	-	攻击阶段: 【侦查】	发生时间:2024-05-29 17:50:34	外省区或能的中于	影响资产:	
1		完成时候: 2024-05-31 23:28:28	处 置 建议:			
		工单处置				
		用户节点			G	当前剩余:1天0小时0分钟)
		处置意见				
						0/255
55						

4、人工节点处理时限,剧本编辑中,人工节点编辑界面,可以设置该节点处理时限设置。设置后,在告警管 理列表和告警处置中会显示是否超时。剧本编辑,设置人工节点处理超时时限,如下图所示。

安全中心		剧本查看
全概約	-	8 分行为新商本 9 , 9 , 9 , ○ 市点開性 副体開性
产中心	÷	
	•	9/4 0.2240/
22 22	π.	변화 <u>acc200001(g103.com</u> ~)
中心	•	Abáň ****
管理		////
响应		
Φŵ	×.	· Asym 00 284 01
	•	元規領 日 therwes 日 元規領 日 日
		社理部項 1 天 时 分 展開分所確止 ® 元年 ○ 不允年 最預允所回述 ● 允年 ○ 不允年



ŵ	工单管理									
		输入事件名或资产P					─ 最近7天		主法 学	出商级。
			成 自动处量 勿喜处量							
			N24-04/00 A		当朝环节 \$		umum a	drukterin a	ALCONTRA -	100
	•	800 ·	ocardini *	环节名 \$	完成时限 💲	制余时间 🗘		APREADER *	ADDRONG +	INT
		01租户副本	2024-05-29 17:50:34	用户带动(cherwer)	2024-06-01 11:26:29	0天21小时	处诞中	2024-05-31 23:26:28	0天9小时	
t	• •		2024-05-24 10:01:36				得处置			
			2024 05 24 12 12 25				特处面			
			20200002117.17.05							
			2024-05-21 16:50:34				特性面			
			2024-05-21 16:50:34 2024-05-21 16:36:34				特性面			

5、脚本任务节点新增,点击默认新增的用户节点,在节点上方显示节点工具,选择脚本任务

云安全中心		剧本管理			
安全概题		<u>8 497936 +az</u> 9 C Q Q	节点属性	副本属性	
沉严中心			节点类型	bpmn:UserTask	
风险管理	•		节点ID	UserTask_01g83up	
分析中心			* 节点名称	用户带点	4/32
工单管理		F+	審注.		0/2048
编排响应			单位名称	sec22050001@163.com	, v
报表中心		Bi+rcz Bi+rcz	角色名称	-角色名称-	~
设置	•		处理人员		
		Т щ		04 E	us 00
			C chenwer		51035
			ALTERIAL	天 时	8
			是否允许终止	 允许 ⑦ 不允许 	
			是否允许问道	 允许 不允许 	

6、切换为脚本任务后,系统默认从左侧弹出插件选取栏,也可通过右侧的节点属性中的查看工具/插件按钮弹



云安全中心		剧本管理		
安全规范		9 9 9 0 0 0 0 0 0	节点属性	剧本属住
资产中心	•		节点类型	bpmn:ScriptTask
风险管理	*		节点口	UserTask 01g83up
威胁运营	2		- #,520	W+#.5 472
分析中心	•		12302210	Judy 17/m with
工单管理			工具/抽件名	公布云Soarle信道知時作波说短信
SERVICE	20	0 % % 🖬 😫	· 0 租户ID	/ 0
2015			● 手机号	0
(Call			* 🧿 通知类型	0
		开始	* 😖 通知消息	0
			调用服务	01角色
			显示模板	-选择显示模板- ~
				查看工具/油件
			/	
			点击	

7、可通过插件选取栏搜索相关插件或直接选取



調給入名称			Q Ch-	14 14 35 3H	1917 S.	m ⊟	0
系统插件	~						
公有云Soar短信遥知插件 v1.0.0	Q				节点属性	副本属性	
发送短信 公有云版本soar短信播件发送短信	法 律				节点类型	bpmn:ScriptTask	
					物面ロ	UserTack_01g83up	
	点击				- 节点名称	重本带点	4/32
					工具结核名		
	0	2 🔹 🛍 🖧			墨示模板	*选择显示模板*	
	······································	脚本节点				BETRISH	

8、选取完插件后,设置插件的入参

云安全中心		刷本管理		
安全规范		Q Q C Q Q	节点属性	剧本属性
资产中心			节点类型	bpmn:ScripfTaek
风险管理	100		节点口	UserTask 01g83up
威胁运营			• 若点常故	B+E.5 (22)
分析中心			12 MACHINE	30-0-123/8 • • 32
T#CH			IR/B/18	公有云Scar拒信道知错件。发送担信
辦納应		O & % 🖬 😫	. ⁶ Abb	0
CPPR 2			● 手机号	0
			1 😑 道如美型	
		开始	1 😦 道知消息	0
			调用服务	01角色
			宣示模板	-选择显示模板- ~
				查看工具/结件

9、剧本线条设置,点击线条,可以在线条上增加线条说明,以及在线条上添加判断条件,以控制流程走向。

云安全中心		顧本管理		
安全规范	~	0.977 C Q Q Q	点耳性	影本庸性
资产中心	*	形成	토	bpmn:SequenceFlow
风险管理	÷	5 AD		SequenceFlow Davztra
威胁运营	<u>.</u>			and and and and and
分析中心	*	Bala Bala Bala Bala Bala Bala Bala Bala	S.	0/32
工业管理				
编排响应	3			14 SIX MING AL AT
感家中心	*			A2347 201 0417
设置	•	4. m		
		→ ● 用户节点 ● 二 二 ● 发送短信 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●		

10、点击选择判断条件,增加或修改线条判断条件



云安全中心		剧本管理		
安全概范		Q 92#### D C Q Q	节点属性	剧本属性
流产中心	2		节点类型	bpmt: SequenceFlow
风险管理				
威胁运营			节点ID	SequenceFlow_Dayzbul
分析中心			节点名称	0/32
工单管理				
编制明应				
授表中心	2			选择归新条件
1022				点击

2X±TU		期本管理		
安全账题		D 677826 +bit 9 C Q Q	牧点属性	剧本属性
资产中心		判断条件设置	节点类型	bpmr:SequenceFlow
风险管理			11.61D	
威胁运营		演送単分祝 ✓ 現法用 ✓ 開造品 032 自	Dieto	
分析中心	352	AND V MINISTER STORE FEILER	节点名称	0/32
工業管理				
编排响应				选择判断条件
設ま中心				
82 	•			

5.2. 如何进行漏洞管理

1、进入风险管理-漏洞管理页面,为租户提供漏洞查询及处置功能。

云安全中心		漏洞管理								
安全概览	•	漏洞名称	请输入		漏洞等级 请	选择	✓ CVE编号 Ⅱ	青榆入	\odot	查询 重置
风脸管理		dareft.	An Annala - The Annale							
漏洞管理 弱口令管理			「お豆中」」「「お豆」」	CVHAI CVE编号	漏洞等级	处置状态	服务器	最后发现时间	更新时间	操作
威胁运营	*		10211	1000000.0	高店	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68-	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
分析中心			1000	C100 1000 2	高危	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68-	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
工单管理			-	100.000.0	高危	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68-	2024-03-05 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
编排响应	•		- : ·	(IIII.) (III.) (I	中危	 待修复 	ecm-ceshif825d35f-17fe-3162-0e68-	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 查看
报表中心	*		100		低危	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68-	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已加固 責看
已购资源			100		高危	 待修复 	ecm-ceshif825d35f-17fe-3162-0e68-	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 查看
设置	*		Marco -	100,000	商品	• 忽略	ecm-ceshif825d35f-17fe-3162-0e68-	2024-02-20 11:15:27	2024-03-11 11:15:17	修复中 已修复 已加固 查看
			1000	100.000.0	藏危	 待修复 	ecm-ceshif825d35f-17fe-3162-0e68-	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 查看
			80)	distant a	低危	•修复中	ecm-ceshif825d35f-17fe-3162-0e68-	2024-01-09 11:15:27	2024-03-11 11:15:17	忽略 已修复 已加固 查看
			10.7	and allow	中庭	 待修复 	ecm-ceshif825d35f-17fe-3162-0e68-	2024-03-01 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 查看

2、支持条件查询,用户输入或选择相关条件内容



	漏洞管理				/	输入或选择相关条件内容		去点	
÷	漏洞名称	请输入		漏洞等级 高危		~ CVE编号 请输入	n	\odot	tin Bi
	服务器	请输入		处 置状 态	ž	~ 最后发现时间 📄	开始日期 - 結束日期		
	206	修复中 已修复	已加商						
		漏洞名称	CVE编号	漏洞等级	处置状态	服务器	最后发现时间	更新时间	操作
		100.0		高危	 已加固 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-06-21 15:22:49	忽略 修复中 已修复 直看
	1	10.1		商危	• 忽略	主机名称_5f825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-06-21 14:58:03	修复中 已修复 已加固 責看
		10.1	C al	高冠	• 已加固	主机名称_5f825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-06-21 14:53:48	忽略 修复中 已修复 直看
		100.0	till inset.	商危	• 忽略	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:47	修复中 已修复 已加固 查看
•		100.0	UL inse	高危	• 已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
		100.0	100.000	商范	• 已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 直看
		100,0	100,000,000	商意	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
		1000	100,000,0	高意	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-05 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
		100.0	100,000,000	高度	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
		1000.00	1008.0000.00	高危	 待修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 査

3、提供处置能力,可直接或批量修改漏洞处置状态。状态枚举值:修复中、已修复、忽略、已加固等。

		漏洞名称	请输入		漏洞等级高危		 V CVE编号 请输 	λ	\odot	重向
		服务器	请输入		处置状态 请选择		◇ 最后发现时间 🗐	开始日期 - 结束日期		
E			批量久	置						
理		忽略	修复中 已修复	已加固						单个处置
	÷	•	漏洞名称	CVE编号	漏洞等级	处置状态	服务器	最后发现时间	更新时间	100 /Jr- 200 / Jr
			100.0	(=	高危	• 已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-06-21 15:22:49	忽略 修复中 已修复 直接
		1	10.1		高茂	 忽略 	主机名称_5f825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-06-21 14:58:03	修算中 已修复 已加固 查
			10.1	THE PARTY.	高危	• 已加固	主机名称_5f825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-06-21 14:53:48	忽略 修复中 已修复 直接
			10.1	10.001	高危	 忽略 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:47	修复中 已修复 已加固 击
	÷		10.1	UR Albert	高范	•已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查得
			100.0	C = 1	高危	• 已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 直接
			100.0	100.0000	高茂	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 直接
			100.0	10,000	高危	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-05 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查報
			100,0	100,00011	高危	• 已修复	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查報
			100.0	AND DESCRIPTION	高范	• 待修复	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固

修改处置状态可填写状态变更原因。

4、进行处置,在漏洞详情中可以历史所有的状态变更记录的信息:处置人、处置状态、处置说明等。

🕝 天翼云

云安全中心		漏洞管理								
安全概览		調測 标记:	6修复由						×	直询 重置
资产中心	*	10,407	J 20 20 1						~	
风险管理			确认要把该漏洞标证	己为修复中吗?						
混詞管理		n	363	同名称	c	/E编号	No	响服务器		
弱口令管理		C	18	Repti -	5m)	i i peng	ecm-ceshif825d35f-17fe-3	3162-0e68-d10676d09b781.1.	1.5	操作
威胁运营		E bhar	8-00 最多可输入	255个字符					49	忽略 修复中 已修复 查香
分析中心	*	NCM.	2043						03	修复中 已修复 已加固 查看
工单管理		4 C							48	忽略 修复中 已修复 查香
编排响应		1							33	忽略 修复中 已修复 直看
报表中心	*	E				取制	保存		20	忽略 修复中 已修复 已加固 查看
已购资源		à	名称_5	CVE_2024_5	31 10	• 忽略	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:47	修复中 已修复 已加固 查看
设置	*		名称_4	CVE_2024_4	4/6	• 修复中	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:43	忽略 已修复 已加固 直看
			名称_5	CVE_2024_5	素商	• EMB	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
			名称_5	CVE_2024_5	低位	 已加固 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
			名称_5	CVE_2024_5	-	• 已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看

査询 重置
2.2
击点
操作
忽略 修复中 已修复 查看
修复中 已修复 已加固 查看
忽略 修复中 已修复 查看
修复中 已修复 已加區 查看
忽略 修复中 已修复 查看
忽略 修复中 已修复 查看
忽略 修复中 已加固 查看
忽略 修复中 已加固 直看
忽略 修复中 已加固 查看
忽略 修复中 已修复 已加固 直看

ර	る天闘云		♀ 埠东1		
 10	云安全中心		漏洞管理		
0	安全概范		32 30 Greb	1476.5	
G	资产中心	*	8589 CH44	房照 人	
G	风险管理				
E II	漏洞管理		216	修复中 已修复	
8	卵口令管理			漏洞名称	CVE编号
G	威胁运营			100.2	600 June
۲	分析中心			100.0	
930	工单管理			100.5	
(H)	輸非响应			118.2	24_
æ	报表中心	*		108.4	(U.H. 1994.
	已购资源			100.0	C\ (4_
20	设置	•		100.0	CV 24_
0				100.0	VE
()				100,0	in/E, inner
۲				100.0	Cuil and
G					
B					

漏洞详情

漏洞名称: 名称_2 CVE编号: CVE_2024_1

漏洞级别: 高危 服务器:名称_2f825d35f-17fe-3162-0e68-d10676d09b781.1.1.2

处置历史:

处置人	处置状态	处置说明	处置时间
超级管理员	 已修复 	22222	2024-03-12 18:25:45
超级管理员	•修复中	11111	2024-03-12 18:25:36
超级管理员	 已修复 	批量测试修复中	2024-03-12 17:29:17
超级管理员	 已修复 	批量测试修复中	2024-03-12 17:28:07
超级管理员	• 修复中	批量处置修复中	2024-03-12 17:27:42
超级管理员	 您略 		2024-03-12 17:26:25

×



已购资源 设置

5、每条漏洞能够关联资产信息,可快速查看关联的资产详情。

安全中心	漏洞管理								
全概范 ▼ ≃中心 ▼	漏洞名称	请输入		混 词等级 高危		- CVE编号 请偷入		©	địn đã
2管理 •	忽略	修复中 已修复	已加固				点击		
旧令管理		漏洞名称	CVE编号	漏洞等级	处置状态	服务器	最后发现时间	更新时间	操作
运营 👻		100.0	10,000	高臣	•已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-06-21 15:22:49	忽略 修复中 已修复 直看
中心 👻		100.0	10.000	<i>818</i>	• 忽略	主机名称_5f825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-06-21 14:58:03	修复中 已修复 已加固 直看
管理	• •	100.0	100.000.0	商店	• 已加固	主机名称_5f825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-06-21 14:53:48	忽略 修复中 已修复 吉香
响应 -		100.0	10.000	南段	 您略 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:47	修复中 已修复 已加固 查看
中心 👻		100.0	100.000.0	高度	• 已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
资源		100.0	C = 1	高能	• 已加固	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
		100.1	νπ. 2 π.	商商	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
		100.1	~ ~	激励	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-05 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查着
		100.1	10.007	商商	 已修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
		486.4	the state of	商位	 待修复 	ecm-ceshif825d35f-17fe-3162-0e68	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 查看
安全中心	资产详情	1					٢	1 2 > 共12条	10条/页 > 前往 1
全観光 マ	资产	信息 脆弱性信息							
-+-U +	基础	信息	() 基本信息						
(自注 平	基本	信息	7-10-24%, new stabl			主机D: ab9fbafe-76d2-4eeb-b021-b753aad	dedfe6	资产状态:运行中	
()));());());());());());());());());()			TOWN CON-CESIN						
)运营 👻			进行系统: linux			操作系统版本:		虚拟私有云名称: vpc-osm-oeshi	
)运营 ・ (中心 ・			- 10-244. BUH-Deshi 操作系统: linux 云资源创建时间: 2024-0	06-18 01:04:30		操作系统版本: 云资源限期时间:2024-07-18 01:05:37		虚拟私有云名称:vpc-osm-ceshi 地域:	
か运营 ・ F中心 ・ P管理			王句记AN, BCHILDESHI 操作系统: linux 云资源创建时间: 2024-0 可用区: default	06-18 01:04:30		操作系统版本: 云资源到期时间:2024-07-18 01:05:37		虚拟私有云名称:vpc-osm-ceshi 地域:	

5.3. 如何对资产进行查看管理

1、进入资产中心-资产管理页面,为租户提供资产及资产属性的查询功能。

云安全中心		资产管理							
安全概览	•						曲 全部		nia mm
资产中心	*	 ④ ④ 添加条件 							
资产概范	- I								
风险管理	×	一云资源创建时间	云资源到期时间	是否安装安全卫士	资产状态	主机名称	安全卫士agent是否在线	资产重要性	操作
威胁运营	÷	2024-06-12 16:09:22	2024-07-12 16:09:34		运行中	ctcss-stab-j9R			直看
分析中心	•	2024-06-12 16:10:31	2024-07-12 16:10:46		运行中	ctcss-stab-x44			查看
工单管理		2024-06-12 16:11:40	2024-07-12 16:11:51		运行中	ctcss-stab-7g4			直看
编排响应	•	2024-04-18 14:43:35	2024-07-18 14:43:50		运行中	ctcss-lab-centos7-a618			直看
报表中心	•	2024-04-18 14:47:14	2024-07-18 14:47:26		运行中	ctcss-lab-ubuntu18-4e70			直看
已购资源		2024-06-12 16:16:21	2024-07-12 16:16:32		运行中	ctcss-stab-rpv			直看
设置	-	2024-06-12 16:12:49	2024-07-12 16:12:59		运行中	ctcss-stab-W5s			責看
		2024-06-12 16:15:06	2024-07-12 16:15:19		运行中	ctcss-stab-9sJ			查看

110



2、选择常用搜索项查询。

女主中心		资产	管理				1.点击搜索框			
全概览	•							☐ 全部	U	查询 重置
中心	*		常用搜索项:							
产管理			主机名称 资产状态	是否安装安全卫士	安全卫士agent是否在线	资产重要性				
管理	*	»	ム灾得切地可可	ム交線主要加加回	定白又农又主ビ上	RT-WO	工机包括	マエエエagent是否在线	资产重要性	操作
运营	•		2024-06-18 01:07:41	2024-07-18 01:07:51		运行中	ecm-ceshi			查看
中心	•		2024-06-18 01:13:16	2024-07-18 01:13:27		运行中	ecm-osm-ceshi			查看
曾理		4	2024-06-18 17:50:44	2024-07-18 17:50:58		运行中	VM-b989b4b1			查看
响应	*		2024-06-18 17:50:44	2024-07-18 17:50:57		运行中	VM-1321844f			直看
中心	•		2024-06-18 17:49:08	2024-08-18 17:49:21		运行中	VM-3bd4041a			直看
资源			2024-06-18 17:49:08	2024-08-18 17:49:20		运行中	VM-f85523ac			直看
	-		2024-06-20 20:08:57			运行中	proxy			直看
			2024-06-20 19:02:02			运行中	tcpserver			直看
			2024-06-20 19:53:05			运行中	client			直看
			2024-06-12 14:39:18			运行中	ctcss-test-mq			直看
			2024-06-02 17:13:09	2024-07-02 17:13:41		运行中	ycdi-5			查看
			2024-05-14 15:41:17			运行中	ctcss-test-KxZ3			查看

			3.输入相	送搜索内容					
既览	-	主机名称 = v *ecm-ces	shi * ×				× 曲 全部	9	查询 正
₽心 ≃概范	-	 ④ 添加条件 							r
管理								点击【查询】按	钮
都理	• »	云资源创建时间	云资源到期时间	是否安装安全卫士	资产状态	主机名称	安全卫士agent是否在线	资产重要性	操作
运营	-	2024-06-18 01:07:41	2024-07-18 01:07:51		运行中	ecm-ceshi			直看
中心		2024-06-18 01:13:16	2024-07-18 01:13:27		运行中	ecm-osm-ceshi			查看
書理	4	2024-06-18 17:50:44	2024-07-18 17:50:58		运行中	VM-b989b4b1			查看
龟应		2024-06-18 17:50:44	2024-07-18 17:50:57		运行中	VM-1321844f			查看
中心		2024-06-18 17:49:08	2024-08-18 17:49:21		运行中	VM-3bd4041a			直看
资源		2024-06-18 17:49:08	2024-08-18 17:49:20		运行中	VM-f85523ac			查看
	-	2024-06-20 20:08:57			运行中	proxy			查看
		2024-06-20 19:02:02			运行中	tcpserver			直看
		2024-06-20 19:53:05			运行中	client			查看
		2024-06-12 14:39:18			运行中	ctcss-test-mq			直看
		2024-06-02 17:13:09	2024-07-02 17:13:41		运行中	ycdl-5			直看
		2024-05-14 15:41:17			运行中	ctcss-test-KxZ3			直看
							共82条 < 1 2	3 4 5 >	20条/页

3、选择常用时间查询。



全中心		资	产管理				点击"	'日历" 图	标				
戰范	٠									全部		P	查询 표
心	•		 ④ ③ 添加条件 						常用时间	ŋ			
管理						j	选择"时间"		今天		最近7天	最近30天	全部
會理	*	>	云资源创建时间	云资源到期时间	是否安装安全卫士	资产状态	主机名称	安全卫:	从	•	开始日期	至	结束日期
营	•		2024-06-18 01:07:41	2024-07-18 01:07:51		运行中	ecm-ceshi						
зò	*		2024-06-18 01:13:16	2024-07-18 01:13:27		运行中	ecm-osm-ceshi						查看
管理			2024-06-18 17:50:44	2024-07-18 17:50:58		运行中	VM-b989b4b1						直看
和应	•		2024-06-18 17:50:44	2024-07-18 17:50:57		运行中	VM-1321844f						查看
ŧύ	*		2024-06-18 17:49:08	2024-08-18 17:49:21		运行中	VM-3bd4041a						查看
现进			2024-06-18 17:49:08	2024-08-18 17:49:20		运行中	VM-f85523ac						查看
	*		2024-06-20 20:08:57			运行中	proxy						查看
			2024-06-20 19:02:02			运行中	tcpserver						直看
			2024-06-20 19:53:05			运行中	client						直看
			2024-06-12 14:39:18			运行中	ctcss-test-mq						直看
			2024-06-02 17:13:09	2024-07-02 17:13:41		运行中	ycdl-5						查看
			2024-05-14 15:41:17			运行中	ctcss-test-KxZ3						直看
								共 82 祭	ξ <	1	2 3 4	5 >	20条/页

4、选择时间段查询。

安全中心		资产管	锂																	
F全概览	*													全部			۳	査) III	重賞
资产概范		0	④ 添加条件					J	点击	_			常用助	间	最近7天		最近30	Ŧ	全部	
风险管理	. »		云资源创建时间	云资源到期时间	是否安装安全卫士	资产状态		3	E机名称		5	安全卫	Ж	G	开始E	期	至	结束E	明	
成防运营	-		2024-06-18 01:07:41	2024-07-18 01:07:51		运行中	2024-0	6-21			00:00:00			> 20	4-07-31			00:00:00		
分析中心			2024-06-18 01:13:16	2024-07-18 01:13:27		运行中	« «		202	24年	6月					20	24年	7月		> 3
□单管理	4		2024-06-18 17:50:44	2024-07-18 17:50:58		运行中	в		=	Ξ	四	五	六	E	-	=	Ξ	29	五	六
朝期响应			2024-06-18 17:50:44	2024-07-18 17:50:57		运行中	26	27	28	29	30	31	1	3	1	2	3	4	5	6
被表中心	-		2024-06-18 17:49:08	2024-08-18 17:49:21		运行中	2	3	4	5	6	7	8	7	8	9	10	11	12	13
则为资源			2024-06-18 17:49:08	2024-08-18 17:49:20		运行中	9	10	11	12	13	14	15	1.	15	16	17	18	19	20
2置	÷		2024-06-20 20:08:57			运行中	16	17	18	10	20		22	2	22	23	24	25	26	27
			2024-06-20 19:02:02			运行中	10		10			•							20	~
			2024-06-20 19:53:05			运行中	23	24	25	26	27	28	29	2	29	30	31	1	2	3
			2024-06-12 14:39:18			运行中	30	1	2	3	4	5	6	4	5	6	7	8	9	10
			2024-06-02 17:13:09	2024-07-02 17:13:41		运行中													清空	iitii
			2024-05-14 15:41:17			运行中		ctcss	s-test-Kx2	23									血有	-

5、查询条件组:保存查询条件,方便用户快速查询。



2024-05-14 15:41:17

云安全中心		tet.	管产管理						
安全概览 资产中心 资产概览	•		主肌名称 = ∨ "ecm-ces	ni * ×			×		2024-06-21 00:00:00-2024-07-31 00:00:00
资产管理 风险管理	•	*	云资源创建时间	云资源到期时间	是否安装安全卫士	资产状态	主机名称	您可	以新增查询条件组,以便下次快速查询
威胁运营	-		2024-06-18 01:07:41	2024-07-18 01:07:51		运行中	ecm-ceshi		
分析中心	•		2024-06-18 01:13:16	2024-07-18 01:13:27		运行中	ecm-osm-ceshi		
工单管理		4	2024-06-18 17:50:44	2024-07-18 17:50:58		运行中	VM-b989b4b1		
编排响应	*		2024-06-18 17:50:44	2024-07-18 17:50:57		运行中	VM-1321844f		
报表中心	-		2024-06-18 17:49:08	2024-08-18 17:49:21		运行中	VM-3bd4041a		
已购资源			2024-06-18 17:49:08	2024-08-18 17:49:20		运行中	VM-f85523ac		
设置	•		2024-06-20 20:08:57			运行中	proxy		
			2024-06-20 19:02:02			运行中	tcpserver		
			2024-06-20 19:53:05			运行中	client		
			2024-06-12 14:39:18			运行中	ctcss-test-mq		
			2024-06-02 17:13:09	2024-07-02 17:13:41		运行中	ycdl-5		

点击

操作

查看

查看

查看

查看

查看

直看

查看
 查看
 查看
 查看
 查看

查看

新招

共75条 く 1 2 3 4 > 20条页 ~

云安全中心		资	产管理						
安全概览 资产中心 资产概览	•		主机名称 = · · · *ecm-cesh ④ ④ 添加条件	(* ×			×	 2024-06-21 00:00:00-2024-07-31 00:00:00 已保存查询条件组: 	董道 重重
资产管理								您可以新增查询条件组,以便下次快捷查询 新牌	1
风险管理	*	*	云资源创建时间	云资源到期时间	是否安装安全卫士	资产状态	主机名称		操作
威胁运营			2024-06-18 01:07:41	2024-07-18 01:07:51		运行中	ecm-ceshi		查看
分析中心	*		2024-06-18 01:13:16	2024-07-18 01:13:27		运行中	ecm-osm-ceshi	点击	宣誓
工单管理		4	2024-06-18 17:50:44	2024-07-18 17:50:58		运行中	VM-b989b4b1		直看
编排响应	*		2024-06-18 17:50:44	2024-07-18 17:50:57		运行中	VM-1321844f		直看
报表中心	*		2024-06-18 17:49:08	2024-08-18 17:49:21		运行中	VM-3bd4041a		查看
已购资源			2024-06-18 17:49:08	2024-08-18 17:49:20		运行中	VM-f85523ac		查看
设置	•		2024-06-20 20:08:57			运行中	proxy		查看
			2024-06-20 19:02:02			运行中	tcpserver		查看
			2024-06-20 19:53:05			运行中	client		查看
			2024-06-12 14:39:18			运行中	ctcss-test-mq		直看
			2024-06-02 17:13:09	2024-07-02 17:13:41		运行中	ycdl-5		查看
			2024-05-14 15:41:17			运行中	ctcss-test-KxZ3		查看
								共75条 < 1 2 3 4	> 20条/页 ~

运行中

ctcss-test-KxZ3

云安全中心		资产管理							
安全概范 资产中心 资产概流	* *	主机名称 =	shi * ×	保存查询条件组		×	2024-06-21 00:00:00~2024-07-31	00:00:00	<u>主</u> 狗 王王
资产管理				* 查询条件组名称:					
风险管理	-	》云资源创建时间	云资源到期日	test			安全卫士agent是否在线	资产重要性	操作
威胁运营		2024-06-18 01:07:41	2024-07-18 01	描述					查看
分析中心		2024-06-18 01:13:16	2024-07-18 01			shi			拉斯
工单管理		4 2024-06-18 17:50:44	2024-07-18 17			// b1			直着
编排响应		2024-06-18 17:50:44	2024-07-18 17	是否保存查询条件:		.4f			查看
报表中心	*	2024-06-18 17:49:08	2024-08-18 17	是否保存查询时间:		ta			直看
已购资源		2024-06-18 17:49:08	2024-08-18 17	输入和选择对应条件		ac	古未		查看
QM		2024-06-20 20:08:57			取消	Rtr			直看
		2024-06-20 19:02:02			运行中	tcpserver			直看
		2024-06-20 19:53:05			运行中	client			近着
		2024-06-12 14:39:18			运行中	ctcss-test-mq			直看
		2024-06-02 17:13:09	2024-07-02 17:1	3:41	运行中	yodi-5			查看
		2024-05-14 15:41:17			运行中	ctcss-test-KxZ3			直動
							共75条 < 1	2 3 4 >	20条/页 \vee

6、添加条件查询。

云安全中心		3	资产管理							
安全概范 印 ⁹ 中心	•		0	点击				曲 最近7天		前
资产概览 资产管理				• 城 操作						
险管理	*	>>	i	資产状态 / = / -	安全卫士	资产状态	主机名称	安全卫士agent是否在线	资产重要性	操作
协运营	-		202			运行中	ecm-ceshi			童看
所中心	*		202	億选择对应的操作输入或者选择相应的值		运行中	ecm-osm-ceshi			查看
自管理		4	202	运行中 🗸		运行中	VM-b989b4b1			直看
响应			202	_		运行中	VM-1321844f			查看
中心	•		202	取消 輸定		运行中	VM-3bd4041a			查看
的资源			2024-	4-06-18 17:49:08 2024-08-18 17:49:20		运行中	VM-f85523ac			查看
t	•		2024-	4-06-20 20:08:57		运行中	proxy			查看
			2024-	4-06-20 19:02:02		运行中	tcpserver			查看
			2024-	4-06-20 19:53:05		运行中	client			查看
			2024-	4-06-12 14:39:18		运行中	ctcss-test-mq			查看
			2024-	4-06-02 17:13:09 2024-07-02 17:13:41		运行中	ycdl-5			直看
								共82条 〈 1 2	3 4 5 >	20象页 ~

5.4. 如何进行威胁建模

1、进入云安全中心-威胁监测-威胁建模页面

可以通过关键字、快捷方式、规则类型和标签查询关联分析规则。



Action Action<	の認識「夢	剧中心	♥ 内蕨8 👻				Q IER	费用	工单 备案	支持合作	s*******m	9 0	99+ 09+
¹ CRUCCRUCACAN SINGNO S	云安全中心		关联分析										
Ref Ref Abitation - Abitat	安全概范		○规则ID/规则名称·事件名称										0
	资产中心	•	标签:										
All	风险管理												
• • • • • • • • • • • • • • • • • • •	成制运营 告警概范	•	080 08± +		98 [197 C	自检规则							
 本時地部 - 本部語 - 本部語 - 本部語 	告誓堂理		规则名称	规则类型 相关	事件	euzenim 🗘	开始时间	持续时间	时间窗口	告誓数量(累计/ 最近) 💲	10	fF	
1 1 1 <	威胁拉剑												
自名単語 ・ 対象音道 ・ ジドや・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	或設建構								7030438				
対策電 対策で シンドキン 工業電源 総映地位 2 総共中心 2 役工 2	白名单管理												
分析中へ ・ 工業課題 期期中へ ・ 役置 ・	对象管理												
工業2222 総称称 - 総称 - 変置 -	分析中心												
編8444	工学管理												
2. (現象・) - (現象・) - (見象・) - ((見象・) - ((見象・) - ((見象・) - ((Dask + (Dask + (编排响应												
2 2 -	报表中心												
	17 1												

2、点击"新建规则"按钮

ć		制中心	♥ 内蔵8 ▼				Q ET	费用	If Sr	支持 合作	s*************************************	a @ 🥮
III .8.	云安全中心		关联分析									
(<u>@</u>)	安全概范		○规则□/规则名称/事件名称									o
20	资产中心		标签:	点	击							
E II	风险管理	•										
0	成物运营		080 06± +	873 8 (1988)	Car Cay	の自检照則						
	 合整管理 		规则名称	规则类型	相关事件	创建时间 👙	开始时间	持续时间	时间窗口	告誓敬重(累计/ 最近) 👙	操作	
	威胁拉剑								7 85-1			
	成助建模		٠						70(94)			
	日名单管理											
	对象管理											
	分析中心	-										
	工業管理											
	编排响应											
	报表中心	-										
	12 1	•										
										12	trend to the second sec	

3、填写基本信息填写,带有*的为必填项

合語	5	控制中心	9 P	h薪8 、							费用 工单	新玄 支持	合作	s*************************************		0 🤔
云安全	中心		×	联分析规则配置												
). 安全概3	đ															
3774	Ċ.	-		■ 基本信息												_
	æ	*		1规则名称	test										◎ 名称可用	4/64
x80/22	Ŧ			规则描述	清治入											
9 9 19 19 19 19 19 19 19 19 19 19 19 19	ò															0/500
) INTR	æ				Sharts -											
编排响。	应	•		NUNDER	Endlander											
报表中(Ċ.			* 规则横板	普通模板	~										
18 1				3	规则模板描述:普通模板,用于	基于单个属性的事件名称转换	æ,									
				标签	请法择类型	~ 553	815									
				◎ 原始告警護												
				*事件名称A	网络暴力破解	> 过滤条件	无							1		
				■ 輸出結果												
				* 輸出層性	A.日志ID		< 聚合类型	: 6 2	· 重命名为:	告警关联日志口		~				
				* 1911 唐件	A日志労牛时间		∨ 取合类型	MIN	√ 田会名为・	· · · · · · · · · · · · · · · · · · ·		v 💼				
												_				
	8840 - U	1000000 - 110	-						Sector Sector		-	10.000 - 10.000	100000			99+1
いた	5	控制中心	₽ P	1歳8 🔻							费用 工单	發展 支持	合作	s*************************************		0 💭

		*事件各称A	网络暴力蔽解	> 过渡条件 无							1	
安全概范	÷											
资产中心		25										
な設管理	-	論出結果										
或師运営	-	* 輸出属性	A.日志ID	8	聚合类型:	但會	✓ 重命	S为: 告誓关联日志に)			
分析中心		*输出属性	A.日志发生时间	Ŷ	聚合类型:	MIN	~ 重命	名为: 告誓开始时间		~ 0		
I#22		* 輸出属性	A.日志发生时间	~	聚合类型:	MAX	~ 重命	白为: 告警结束时间		~ 0		
廣排响应	-		A MERCHANNELS		BOTEL.	101	Ŧa	train a secondaria				
限表中心	- 4	制正用注	AL 27 IF ADAL	~	BAD SALE -	TATIEN.	✓ 里=p			× •		
2 2		* 输出属性	A.透明口	8	聚合类型:	MIN	~ 重命	当为: 源湖口		~ 8		
		1 輸出属性	A.目的IP地址	×	聚合类型:	MIN	~ 重命	名为: 目的IP地址		× 🖬		
		11 输出属性	A目的端口	~	聚合类型:	MIN	~ 重命	笃为: 目的端口		· 0		
		*輸出属性	A资产ID	~	聚合类型:	MIN	~ 重命	名为: 资产D		- 1		
		ĺ	禄加输出属性									
		▲ 告答配置										
		· 6###	0 TR#									

3	天費云	控制中心	♀ 内蔵8	-]	Q 定 新用 I单 参索 支持 台作 新用 」 [] ③ [] ④ [] ●
	云安全中心			* 輸出属性	A 決声D V 要合型2: MIN V 重合型3: 扱声D V
(@) ¹	安全概范	•			
& : 1	20 〒0 风险管理	-	-	5	
0	成初运营	•	1	告替配置 (旧并模式)	0 78#
	977年0 工業管理				
	續排响应	-		分组条件	清武将和卫 🗸
-	报表中心 注言	•	1	其它输出学段	· 通过标件社 · · ·
				*原始告警阶段	(焼車) マー
				*原始告警级别	
				*原始告誓内考	165] 4/128,/
				她建议	濟地人
					0/128
					- 1019 (R.9-)

٢		控制中心	٢	内蔵8	•		0 #	谱规则成功		费用	If Sq	支持合作	5*************************************	4	0	
111 181	云安全中心		-	关联分析			• 19	则自检成功								
()	安全板统			ONE	IID/1000(名称/高仲名称											
20	资产中心	•		标签:												
B II	风险管理	*														
0	成物运营			0=3	056	+ 253 (1980)		C自检规则								
æ	告警抵范															
	- See See See See See See See See See Se				规则名称	规则类型	相关事件	创建时间:	开始时间	持续时间	时间窗口	告誓敗重(累计/ 最近) 💲		操作		
	威胁检测	-			test	数据窃取	网络暴力破解	2024-05-30 10:52:19			5分钟	0/0	0 /	0	ŵ	
	成的建模		٠													
	白名单管理	E .														
	对象管理															
	分析中心	*														
	工業管理															
	编排响应															
	报表中心	-														
	17 11	*														
													(1) (1) (1)			

5.5. 等级保护测评解读

云安全中心产品符合等级保护 2.0 标准体系主要标准。根据《网络安全等级保护基本要求》(GB/T 22239-2019), 云安全中心满足第三级及以下安全要求:

等保标准章节	等保标准序号	云安全中心对应功能	功能解读
安全区域边		插件管理、威胁运	云安全中心通过获取 WAF、防火墙以及安全卫士
界-边界防护	8.1.3.1	营、编排响应	等日志数据,保证跨越边界的访问和数据流通过
			边界设备提供的受控接口进行通信。同时能够对



等保标准章节	等保标准序号	云安全中心对应功能	功能解读
			非授权设备私自联到内部网络的行为进行检查,
			通过处置功能实现对相关访问进行限制
			云安全中心通过获取 WAF、防火墙以及安全卫士
安全区域边			等日志数据,保证跨越边界的访问和数据流通过
又王匹城起	8.1.3.2	一一百年、风加运	边界设备提供的受控接口进行通信。同时能够对
75-011月王中1			非授权设备私自联到内部网络的行为进行检查,
			通过处置功能实现对相关访问进行限制
			云安全中心通过获取 WAF、防火墙以及安全卫士
安全区域边	0122	插件管理、威胁运	等日志数据,可在关键网络节点处检测、防止或
界-入侵防范	0.1.3.3	营、编排响应	限制从外部/内部发起的网络攻击行为,并对这些
			攻击行为进行分析、记录以及提供报警
安全区域边			云安全中心通过获取 WAF、防火墙以及安全卫士
界-恶意代码	8121	插件管理、威胁运	等日志数据,可在关键网络节点处对恶意代码进
和垃圾邮件	0.1.3.4	营、编排响应	行检测、分析,并通过处置功能实现对相关机器
防范			访问进行限制
			云安全中心通过获取 WAF、防火墙以及安全卫士
			等日志数据,可以在网络边界以及重要网络节点
安全区域边	Q 1 2 5	插件管理、威胁运	进行安全审计,记录包括相关告警的日期和时间
界-安全审计	0.1.3.5	营	、用户、告警类型、告警是否成功及其他与审计
			相关的信息,通过威胁运营,能将单独用户行为
			审计和数据分析。
安全计管环		插件管理 威胁运	云安全中心通过获取 WAF、防火墙以及安全卫士
	8.1.4.3		等日志数据,可以在网络边界以及重要网络节点
│		A	进行安全审计,记录包括相关告警的日期和时间



等保标准章节	等保标准序号	云安全中心对应功能	功能解读
			、用户、告警类型、告警是否成功及其他与审计
			相关的信息。云安全中心日志通过多副本实时存
			储多分,保障用户日志在其存储周期内不丢失、
			可恢复
			云安全中心通过获取 WAF、防火墙以及安全卫士
空合计算环		专业管理 成功运	等日志数据,能发现可能存在的已知漏洞,并在经
女王11 昇环	8.1.4.4	油什官理、威胁运 	过充分测试评估后,及时修补漏洞,同时应能够检
項-入侵防氾		'宫、 狮 排啊 <u>心</u>	测到对重要节点进行入侵的行为,并在发生严重入
			侵时提供报警
中人计算环			云安全中心通过获取 WAF、防火墙以及安全卫士
女王订昇 小	0.1.4.5	插件管理、威胁运	等日志数据,能够及时采用免受恶意代码攻击的
- □- 志思 □- ☆ ☆ ☆ ☆	8.1.4.5	营、编排响应	技术措施或主动免疫可信验证机制及时识别入侵
防范			和病毒行为。通过处置功能将其有效阻断。
			云安全中心通过获取 WAF、防火墙以及安全卫士
			等日志数据,以及不同安全设备的处置集成,实
			现对分布在网络中的安全设备或安全组件进行管
			控;
			通过内网建立一条安全的信息传输路径,对网络中
安全区域边	8.1.5.4	插件管理、威胁运	的安全设备或安全组件进行管理;
界-集中管控		营、编排响应	形成对网络链路、安全设备、网络设备和服务器
			等的运行状况进行集中监测;
			通过实时的日志采集,对分散在各个设备上的审
			计数据进行收集汇总和集中分析,并保证审计记录
			的留存时间符合法律法规要求;
安全区域边 界-集中管控	8.1.5.4	插件管理、威胁运 营、编排响应	现对分布在网络中的安全设备或安全组件进行管 控; 通过内网建立一条安全的信息传输路径,对网络中 的安全设备或安全组件进行管理; 形成对网络链路、安全设备、网络设备和服务器 等的运行状况进行集中监测; 通过实时的日志采集,对分散在各个设备上的审 计数据进行收集汇总和集中分析,并保证审计记录 的留存时间符合法律法规要求;



等保标准章节	等保标准序号	云安全中心对应功能	功能解读
			同时在应对安全策略、恶意代码、补丁升级等安
			全相关事项进行集中管理;
			通过编排响应能对网络中发生的各类安全告警进
			行识别、报警和分析;

5.6. 如何接入产品日志、告警

打开云安全中心的设置>集成配置,在集成配置中选择需要接入的日志类型。部分日志支持直接转告警,可以 直接打开转告警开关,云安全中心会根据内置转告警规则进行转告警配置。

接入流程如下:



- 1. 选择"设置 > 数据源监控",打开数据源监控页面。
- 2. 在操作列点击"启用",确保数据源监控处于启用状态。

数据源盖控				
教集集中: 清洁入的活动中 93 0 重	=			
Kafka日志 Syslog日志				
数据题P 资产名称	经施厂商	设备问题	80	秋志 收到最近一条日本时间 操作
10.4.1.6 Web应用防火墙(原生版)	天興五	際の海	9092	28日中 00
			#1#	1046页 -> (1 > 前性 1 页



- 3. 选择"设置 > 集成配置",打开数据集成配置页面。
- 4. 选择需要接入的日志,并打开日志接入开关。

뽑		
全服务	日志典型	状态 日志被入 自动转出
	X	
	(B)	己穂人
	2mm	
9);	*	
	THE CONTRACT OF A DESCRIPTION OF A DESCR	已線入 💽 💽
	and the second	
la		未短人 🚺 🕥

5. 选择需要转告警的日志,并打开自动转告警的开关。

或配置			
安全服务	日志英型	状态 日志扱入	自动转告警
		己親入	
	H	已接入	
		日接入	
	1002	已接入	
	t k	已經入	
		已經入	
	1000 B	未授入	

说明:

- 系统默认会接入部分日志,用户如有需要,可以自行关闭。
- 需要先在数据源监控页面启用开关后,才可以在集成配置页面中开启日志和告警配置。
- 选择需要接入的日志时,只能针对您已经购买的云产品。
- 选择需要转告警的日志,只能针对已经选择接入的日志进行。



6. 常见问题

6.1. 产品咨询类

Q: 云安全中心是否只是对其他云安全产品日志进行采集分析?

A: 云安全中心产品除了采集其他安全产品的日志进行统一管理外,还提供编排响应以及处置的能力,能够对 告警形成自己的处置流程,并进行自动化处置。云安全中心打通了云上的各类安全产品形成联动响应处置,帮 助用户提升威胁响应处置效率。

Q: 云安全中心如何帮助客户满足等保合规要求?

A: 云安全中心提供的插件管理、威胁运营、编排响应等功能,可以满足等保的"边界防护"、"访问控制"、
 "入侵防范"、"恶意代码和垃圾邮件防范"、"安全审计"、"恶意代码防范"、"集中管控"等要求。具体可参见等级保护测评解读。

Q: 云安全中心支持采集云上哪些安全日志?

A: 云安全中心目前支持采集云上安全产品的安全告警日志, 包括服务器安全卫士、WAF 以及防火墙等产品。

Q:短信使用余量是否进行提醒?

A: 云安全中心会在剩余 500 条和全部使用完短信时提醒用户的短信剩余量。

6.2. 计费购买类

Q:同一个账号可以购买多个云安全中心实例吗?

A: 同一个账号在同一个区域只能购买一个云安全中心实例,对应一个主资源版本。购买云安全中心实例后, 您可以购买扩展资源。

Q:云安全中心实例到期后,数据还会保留吗?

A:购买的云安全中心实例到期后如未按时续费,公有云平台会提供一定的保留期。

- 保留期内,平台会冻结云安全中心的服务,用户配置的各类数据会继续生效,但用户无法访问云安全
 中心。
- 保留期满,用户若仍未续费,平台会清除实例资源,用户原有的配置信息将会被删除,同时云安全中 心将不再获取第三方日志、用户云上资产等信息。

Q: 云安全中心实例可以降低规格吗?

A: 云安全中心实例不支持降级,同时已绑定的扩展资源也不支持单独退订。如您需要降低当前规格,你可以 先退订当前的云安全中心实例,再重新购买云安全中心实例。

Q: 云安全中心是否支持自动续订?

A: 支持。您可以在购买套餐的同时勾选自动续订,同时也支持在使用过程中,在订单中心中设置自动续订。

Q: 云安全中心存在规格差异吗?

A:当前云安全中心只有一个标准版,标准版版本附带的服务如下所示。

版本	即时通知服务	日志分析量
标准版	10000条/月	50G/月

Q: 云安全中心有哪些扩展服务可以购买?

A: 云安全中心支持 2 种类型的扩展资源,用户可支持根据实际使用需求购买日志分析量扩展资源和态势大屏 扩展资源。其中,态势大屏扩展资源只可购买一次,日志分析量扩展资源的购买资源最小单位为 50G,即扩展 资源需要购买 50G 的整数倍。

Q:续费时是否可同时变更云安全中心版本或规格?

↔ 天翼云

A:续费时您只能为当前的云安全中心实例版本规格进行续费,增加使用时长。续费时不能同时变更云安全中心的规格。您可以在续费完成后,对云安全中心实例版本进行升级。

Q:扩展资源购买上限是什么?

A:当前云安全中心提供态势大屏扩展资源及日志分析量拓展包。态势大屏扩展资源订购上限为1个,日志分析量拓展包订购暂无订购上限。请您根据业务需要按需订购。

Q: 云安全中心是否支持按需计费?

A: 当前云安全中心不支持按需计费。

Q: 云安全中心有促销折扣吗?

A:当前云安全中心暂无优惠折扣。

Q:在使用期间购买了扩展资源,资源到期时间是何时?

A: 扩展资源购买后与主资源绑定,资源到期时间与主资源一致。

Q:购买的扩展资源,支持单独退订吗?

A: 不支持。扩展资源购买后与主资源绑定,不支持单独退订。

Q: 退订重购后, 原实例的配置数据可以保留吗?

A: 用户退订后在 15 天内重新购买实例时,可恢复原有配置。当重新购买时距离退订已超过 15 天,原资源已 释放且配置数据已删除,则无法恢复。

Q:如何选择日志分析量扩展资源?

A:购买日志分析量扩展资源时,您需要测算接入云安全中心的所有日志数据总量,确保您选购的日志分析量 能覆盖每月的日志数据总量。

Q: 日志分析量扩展资源会过期吗?

A:每月优先使用主资源赠送的日志分析量,当赠送部分使用完毕后再消耗日志分析量扩展资源。未用完的日 志分析量扩展资源会一直累积(赠送部分每月清零不进行累积)。

Q: 如何查看当前购买产品的产品规格

A:购买、续订、升级扩容后可以通过产品信息页面查看所购买产品的规格,同时个人消息中心以及用户绑定的手机也能够收到相关的购买成功提示短信。

查看购买后的云安全中心规格方式如下:

- 1. 登录天翼云控制中心。
- 2. 在控制台列表页,选择"安全>云安全中心"。
- 3. 进入产品服务页面,选择"已购资源"。

云安全中心		产品信息	
安全态势	÷	云安全中心(标准版) 🕯 回周期 付表方式	
资产中心	•	到期时间: 2024-09-06 00:35:48 (距离到期还有22天)	
风险管理	*		
威胁运营	•	مُعْلَمُ الله مُعْلَمُ مُعْلَمُ مُعْلَمُ الله مُعْلَمُ مُعْ	
分析中心	*	头扔、可视化的晶花和分析网络安全态势,提供全面的安全就能信息和烦害,如刀用尸块遮碍加机和宣言音。 云安至平心先感为您提供每月 50G 的日志分析额度,如果您需要额外的额度,确另外物头。	
编排响应	•	土 印5.37 印 三 本林士 安 已使用(GB) 剩余量(GB)	
报表中心	- 1	木内矢 0 100 駒実日志分析量	
已购资源		100%	
设置	•		

注意:

购买成功后需要等待一段时间相关规格才能刷新,预计等到 1-2 分钟左右。

6.3. 配置类

6.3.1. 数据接入相关

Q:为什么要进行数据接入?

A:云安全中心 (CT-CSC, Cloud Security Center,简称 CSC)作为用户侧的安全中心,其核心数据来源是 用户的各种安全设备。

↔ 天翼云

Q: 云安全中心数据接入要如何配置?

A: 打开云安全中心的设置>集成配置, 在集成配置中选择需要接入的日志类型即可。

Q: 云安全中心告警需要如何配置?

A: 打开云安全中心的设置>集成配置, 在集成配置中选择需要接入的日志类型。部分日志支持直接转告警, 可以直接打开转告警开关, 云安全中心会根据内置转告警规则进行转告警配置。同时云安全中心还支持自定义 转告警配置, 即通过云安全中心的"威胁运营 > 威胁检测 > 威胁建模"功能实现自定义告警配置。

6.3.2. 告警通知相关

Q: 如何获取钉钉机器人的 token 和 secret?

1. 进入钉钉选择组织团队



2. 发起群聊



3. 创建群聊

发起群聊

Q搜索				已选择(1/1000)	
00	&	Ûõ	ම		
按好友选	按架构选	按群 <mark>聊</mark> 选	批量导入		
				群名称: 取个群名称方便后续搜	厥
				群场景:内部群 内部 用于企业/团队内部沟通,所 于同一个团队。创建后仅支持	切換 有群成员均来自 导邀请本企业/团
				队内部成员入群 群归属:	>

 \times

4. 点击群设置

	Q 搜索 (Ctrl+Shift+F)	89				Zai	C	+		ð	×
) IRO					Þ	\leq	4	—	2	ĒQ	¢
		3分钟前								1	
	发起了群聊。本開 本群是内部群,企业管理	成员来自同一组织, 里员已设置本群的聊玥 ",企业数据	为内部群,请放心 E文件保存至组织 安全可控)安全沟通。 *			点击	群设	置		
		4审批 🖸 着闲竹			牆应用						
7			•••								ر ا

5. 下拉点击机器人



6. 点击添加机器人



7. 选择自定义机器人



8. 点击添加

简介:使用钉	钉机器人API,可以将任何你需要的服务消息推送到钉钉	
消息预览:	VIP监控报酬 []]]]	
	消息发送失败率高于5%,模块202, 网络类型4G。@易楠 紧急处理	
	- 移动端首页tab个数显示降级 - 操作人:须莫	
信息来源网站:	: https://www.dingtalk.com/	



9. 勾选加签(产生的密码对应云安全中心中钉钉通知联系组的 secret)

安全设置②	自定义关键词		
2043×14	☑ 加签 勾选加签		
	SECa387469edd930eaaef10d948f13b8	重置	复制
	密钥如上,签名方法请参考 说明文档		
	IP地址 (段)		
	IPABAL (FX)		

10.完成后点击机器人





11. 点击机器人设置





12.复制 Webhook

机器人名字:	test	
接收群组:		
消息推送:	开启	
Webhook :	https://oapi.dingtalk.com/robot/send?ac 复制 重置	٦
	* 请保管好此 Webhook 地址,不要公布在外部网站上,泄露有安全风险 使用 Webhook 地址,向钉钉群推送消息 查看文档	

13.获取 Webhook 后

https://oapi.dingtalk.com/robot/send?access_token=39c0d034b99e9818aaa56e07c907f91b54ec8cd

d5dfddd78ff73e8bc99e955d4

token=后的部分为云安全中心联系组钉钉需要的 token

Q:如何获取企业微信机器人的 key?

注: 微信群必须是内部群 外部群添加不了群机器人

1.添加群机器人





11:33 <i>120</i> %	\$ © 101 🖬 Sul (37)		
← 聊天信息(3)			
	Ż	(+)	
查看全部群成员			3人 >
群聊名称		Ŧ	长命名 >
群二维码			
群公告		3	未设置 >
备注			>
查找聊天记录			×
□ □ □ 文件 图片/视频	 ④ 链接 	〇 群工具	② 小程序
群管理			>
群机器人 ⊙		5	⊧添加 >
消息免打扰			0

2. 获取到机器人的 key 值



添加机器人	完成
已添加 test 配置Webhook后可推送消息到	则群
配置说明	>
Webhook地址 https://qyapi.weixin.qq.com/cgi	复制

https://qyapi.weixin.qq.com/cgi-bin/webhook/send?key=0317a550-1837-46ea-bf69-4a04dcd876c0

Key=后面的值为云安全中心联系组中的 KEY