态势感知（专业版）

用户使用指南

天翼云科技有限公司

目 录

1 产品介绍

1.1 什么是态势感知（专业版）

态势感知（专业版）是云原生的新一代安全运营中心，基于云原生安全，提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，可以鸟瞰整个云上安全，精简云安全配置、云防护策略的设置与维护，提前预防风险，同时，可以让威胁检测和响应更智能、更快速，帮助您实现一体化、自动化安全运营管理，满足您的安全需求。

为什么选择态势感知（专业版）

- 一屏全面感知：采集各类安全服务的告警事件，并进行大数据关联、检索、排序，全面评估安全运营态势，支持大屏展示安全运营动态。
- 一体全程处置：服务内置多种处理剧本，实现 99%以上的安全事件分钟级自动化响应。

1.2 产品优势

见微知著的指标脉络与态势呈现

您可以通过态势感知即时查看大屏、定期订阅安全运营报告，了解安全运营核心关注指标。

云原生的资产盘点与风险预防

云上资产自动盘点，云安全配置自动检查，支持定位到资产，指导并辅助自动加固，帮助您告别黑资产、错配置的焦虑。同时避免传统的外挂式安全方案引入的隐式通道或安全设备漏洞。

智能高效的威胁检测与响应处置

专注于快速找到真正的威胁。通过每天对数十亿安全日志进行分析，利用多年沉淀经验，内置模型和研判剧本来降低合法事件的干扰。通过威胁及资产画像，与威胁告警

环环关联，还原整个攻击链，配置自动化处置剧本进行响应，简化操作、提升安全性，提升了处理告警和事件的效率。

灵活的环境集成与作战协同

可通过配置连接到所有安全服务，进行数据对接或者联动操作；也可以定义您自己的模型、研判/处置剧本，以最佳适配您的安全需求。通过工作空间，还可以实现大型组织协同作战。

1.3 应用场景

云安全的理念是“三分建设，七分运营”，态势感知（专业版）的应用场景即是占了七分的安全运营。主要有以下几个应用场景：

日常安全运营

日常过程中，基于安全运营中关注的要素，对各个安全目标，执行各安全运营流程剧本，从而发现并消减风险，并对流程进行持续改进，避免风险再次发生。

重大保障

重大节日、假日、活动、会议期间，进行高强度 7*24 的安全保障，侧重于防攻击，保障业务可用性不因安全攻击受影响。

防护演练

国家机关单位、地方政府、企业组织的攻防演练中，进行高强度的安全防守保障，侧重于防入侵，保障不因入侵失分被问责（通报、批评等）。

安全评估

重大保障及防护演练前，信息全面的脆弱性盘点，包括白盒方式的基线评估、黑盒方式的攻击面、攻击路径探测。

1.4 产品功能

态势感知（专业版）基于云原生安全，提供全面的日志采集、智能分析、态势感知、编排响应等快速闭环的安全信息和事件管理能力，助您守护云上安全。

产品功能

表 1-1 产品功能

服务功能	功能模块	功能概述

服务功能	功能模块	功能概述
总览		呈现云上整体安全评估状况，并联动其他云安全服务，集中展示云上安全。
工作空间	空间管理	态势感知（专业版）顶层工作台，单个工作空间可绑定项目和Region，可支撑不同场景下的工作空间运营模式。
	空间托管	跨账号安全运营，可实现工作空间委托集中安全运营查看统一资产风险、告警和事件等。
已购资源		在态势感知（专业版）的已购资源中可统一呈现当前账号已经申请的资源，方便统一管理已申请资源。
安全态势	态势总览	• 安全评分：集中呈现资产安全风险评分和风险等级分布，同时展示当前风险防御能力。 • 安全监控：实时展示安全监控统计数据。 • 安全趋势：展示近 7 天内您的整体资产安全健康得分的趋势。
	安全报告	通过创建分析报告，及时掌握资产的安全状况数据。
	任务中心	集中呈现当前需要进行处理的任务。
	AI 风险概览	AI 风险概览实时为您呈现大模型合规态势，支持大模型的数据语料风险运营、推理业务风险运营和环境安全风险运营，实时呈现大模型的风险概览，助您识别大模型风险和潜在威胁。通过控制台“AI 风险概览”为您呈现**推理安全**、**语料安全**、**环境安全**的风险态势。
资产管理		同步资源信息，集中呈现资源整体安全状况。
风险预防	基线检查	通过执行云服务基线扫描，检查基线配置风险状态，告警提示存在安全隐患的配置，并提供基线加固建议。
	漏洞管理	通过自动同步 HSS 漏洞扫描数据，分类呈现漏洞扫描详情，支持查看漏洞详情，并提供相应漏洞修复建议。
	策略管理	支持统一管理策略。
威胁管理	事件管理	集中呈现安全威胁事件。
	告警管理	提供统一的安全告警管理。通过集成各云服务告警，集中呈现告警信息。
	情报管理	提供统一的安全威胁情报指标管理。支持接入各云服务情报，同时也可以基于告警和事件自定义规则提取指标。

服务功能	功能模块	功能概述
	智能建模	支持利用模型对管道中的日志数据进行扫描，如果检测到有满足模型中设置触发条件的内容时，系统将产生告警提示。
	安全分析	支持对数据进行查询分析、消费、监控、投递。
安全编排	运营对象	集中对数据类、数据类类型、分类映射等进行管理。
	剧本编排	支持对剧本、流程、资产连接、实例的全生命周期管理。
	页面布局	提供安全可视化低代码开发平台，基于此平台可自定义安全分析报告、告警管理、事件管理、漏洞管理、基线管理、威胁情报指标库管理等页面布局。
	插件管理	支持将安全编排流程中使用的插件进行统一管理。
数据集成		通过集成生态安全产品，进行联动操作或数据对接。集成后，可以检索并分析所有收集到的日志。
目录定制		支持查看已有目录及更换布局等操作。

1.5 个人数据保护机制

为了确保您的个人数据（例如用户名、密码、邮箱等）不被未经过认证、授权的实体或者个人获取，态势感知（专业版）通过加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

态势感知（专业版）收集及产生的个人数据如表 1-2 所示。

表 1-2 个人数据范围列表

类型	收集方式	是否可以修改	是否必须

类型	收集方式	是否可以修改	是否必须
邮箱	采用邮箱方式启用通知类剧本时，态势感知（专业版）获取对应消息通知服务主题订阅的邮箱。 或者开启安全分析报告定时发送功能时，态势感知（专业版）获取用户在界面输入的接收邮箱地址（需要经过拥有接收邮箱地址的用户授权同意接收安全分析报告邮件）。	是	是
请求源IP	态势感知（专业版）上开启 WAF 防护场景，有攻击防护域名时，被 WAF 拦截或者记录的攻击者 IP。	否	是
URL	态势感知（专业版）上开启 WAF 防护场景，有攻击的防护域名的 URL，被 WAF 拦截或者记录的防护域名的 URL。	否	是
HTTP/HTTPS Header 信息（包括 Cookie）	态势感知（专业版）上开启 WAF 防护场景，且有攻击命中用户配置的 CC 攻击、精准访问防护规则时，在攻击告警中可能携带用户在配置界面输入的 Cookie 值和 Header 值。	否	否 如果配置的 Cookie 和 Header 信息不含有用户的个人信息，则态势感知（专业版）也不会收集及产生用户的个人数据。
请求参数（Get、Post）	态势感知（专业版）上开启 WAF 防护场景，在 WAF 防护日志里，WAF 记录的请求详情。	否	否 如果请求参数里不含有用户的个人信息，则 WAF 记录的相关请求中不会收集及产生用户的个人数据。
登录位置信息	态势感知（专业版）上开启 HSS 主机防护场景，服务器开启防护后，登录云服务器时，HSS 记录的用户登录位置信息。	否	是

存储方式

态势感知（专业版）通过加密算法对用户个人敏感数据加密后进行存储。

- 邮箱：加密存储。

- 登录位置信息：不属于敏感数据，明文存储。
- 请求源 IP、URL、HTTP/HTTPS Header 信息（包括 Cookie）、请求参数（Get、Post）：对敏感字段提供了脱敏配置，其他字段在日志中明文保存。

访问权限控制

用户个人数据通过加密后存储在态势感知（专业版）数据库中，数据库的访问需要通过白名单的认证与授权。

用户只能查看自己业务的相关日志。

1.6 经验包

1.6.1 内置剧本

安全编排根据需求内置了剧本，可以根据需要直接进行使用。

内置剧本

表 1-3 内置剧本

安全防线	剧本名	描述	数据类
主机安全	主机告警状态同步	自动同步主机告警状态	Alert
	高危漏洞自动通知	对威胁等级为 High 的漏洞进行邮件或者短信通知	Vulnerability
	攻击链路分析告警通知	针对攻击链路进行分析，如果主机产生告警，就会查看关联主机所属的网站，如果有对应网站信息且有告警，就进行告警通知	Alert
	主机资产风险统计通知	查询资产管理中绑定 EIP 的主机资产，将其漏洞信息统计通知给客户	CommonContext
	HSS 文件隔离查杀	自动隔离查杀恶意软件	Alert
	挖矿主机隔离	当主机告警类型是挖矿程序/挖矿软件，对当前主机进行隔离，添加安全组，对入方向和出方向全部阻断	Alert
	勒索主机隔离	当主机告警类型是勒索软件，对当前主机进行隔离，添加安全组，对入方向和出方向全部阻断	Alert
	主机防线告警关联历史处置信息	针对主机类告警，关联 HSS 告警历史处置信息，并添加至该告警评论中	Alert

安全防线	剧本名	描述	数据类
	新增主机资产防护状态通知	新增主机资产为未防护状态，通知客户及时防护	Resource
	HSS 高危告警拦截通知	主机高危告警，如果源 IP 未加入安全组阻断，则通知客户并生成待办，如果人工审核通过则加入态势感知（专业版）VPC 策略阻断	Alert
	主机 Rootkit 事件攻击自动化处置	当主机告警类型为 Rootkit，对当前主机进行隔离，添加安全组，对入方向和出方向全部阻断，同时关闭告警	Alert
	主机反弹 Shell 攻击自动化处置	当主机告警类型为反弹 shell，对当前主机进行隔离，添加安全组，对入方向和出方向全部阻断，同时关闭告警	Alert
应用安全	云脑 WAF 地址组关联策略	将态势感知（专业版）指定 WAF 地址组(黑 IP 地址组)绑定 WAF 所有企业项目全部策略的黑白名单	CommonContext
	WAF 删除空防护策略	每周一 9 点查询 WAF 防护策略，对空防护策略进行删除	CommonContext
	应用防线告警关联历史处置信息	针对 WAF 告警，关联 WAF 告警历史处置信息，并添加至该告警评论中	Alert
	Web 登录爆破拦截	对登录爆破成功的 IP 进行情报验证，如果不在白名单，则进行拦截通知，生成拦截代办，代办人工审核通过后会将该 IP 加入态势感知（专业版）WAF 阻断策略中	Alert
	关键运维操作实时通知	针对模型产生的运维告警，进行实时通知。目前支持挂载网卡、peering 对等连接、资源绑定 EIP 三种关键运维操作进行 smn 通知	Alert
身份安全	身份防线告警关联历史处置信息	针对 IAM 告警，关联 IAM 告警历史处置信息，并添加至该告警评论中	Alert
网络安全	网络防线告警关联历史处置信息	针对 CFW 告警，关联 CFW 告警历史处置信息，并添加至该告警评论中	Alert
其他/通用	高危告警自动通知	对威胁级别为 High 或者 Fatal 的告警进行邮件或者短信通知	Alert
	告警指标提取	将告警中 IP 信息抽取，通过情报系统进行验证，如果为恶意 IP，可以将 IP 信息设置成指标，并与源告警相互关联	Alert

安全防线	剧本名	描述	数据类
	重复告警自动关闭	将近 7 日内第二次及第二次以上出现的告警状态置为关闭，并关联 7 日内同名告警	Alert
	自动更新告警名称	根据客户需要，筛选关键字段信息，拼接告警名称	Alert
	告警 ip 指标打标	告警添加告警关联攻击源 IP 及目标 IP 的标签信息	Alert
	关联内外部 IP 画像情报	告警关联云脑情报、微步情报（优先关联内部情报）	Alert
	资产防护状态统计通知	每周统计客户资产防护状态，同时发送邮件/短信通知给客户	CommonContext
	未关闭告警自动统计通知	每天晚上 7 点，统计未关闭的告警，并发送邮件/短信通知给客户	Alert
	高危告警自动化安全封堵	针对高危和致命告警，源 IP 地址攻击次数达到阈值(次数>3)且命中微步在线的恶意标签，根据告警来源将该 ip 对应策略阻断(WAF、VPC、CFW、IAM)	Alert
	低危告警自动关闭	对于低危和提示的告警，进行自动化关闭	Alert

1.7 与其他云服务的关系

本章节主要介绍态势感知（专业版）与其他云服务之间的关系。

与安全服务的关系

态势感知（专业版）从企业主机安全（Host Security Service，HSS）、Web 应用防火墙（Web Application Firewall，WAF）等安全防护服务中获取必要的安全事件记录，进行大数据挖掘和机器学习，智能 AI 分析并识别出攻击和入侵，帮助用户了解攻击和入侵过程，并提供相关的防护措施建议。

与弹性云服务器的关系

态势感知（专业版）为弹性云服务器（Elastic Cloud Server，ECS）提供资产安全管理服务，结合 HSS 主机防护状态，全方位呈现当前 ECS 安全风险态势，并提供相应防护建议。

1.8 基本概念

1.8.1 安全运营中心

安全运营中心（Security Operations Center，SOC）一个集中式功能或团队，负责全天候检测端点、服务器、数据库、网络应用程序、网站和其他系统的所有活动，以实时发现潜在的威胁；对网络安全事件进行预防、分析和响应，以改进企业的网络安全态势。SOC 还使用最新的威胁情报来掌握威胁组和基础结构的最新信息，并在攻击者利用系统或流程漏洞之前识别和处理这些漏洞，从而主动开展安全工作。大多数 SOC 每周 7 天全天候运行，跨多个国家/地区的大型企业/组织可能还依赖于全球安全运营中心（GSOC）来掌控全球安全威胁，并协调多个本地 SOC 之间的检测和响应。

SOC 的功能

SOC 团队承担以下职能来帮助防止、响应攻击并在遭到攻击后恢复。

- **资产和工具清单**

  为了消除覆盖范围中的盲点和缺口，SOC 需要了解它保护的资产，并深入了解它用于保护企业/组织的工具。这意味着考虑到本地和多个云中的所有数据库、云服务、标识、应用程序和客户端。该团队还跟踪企业/组织中使用的所有安全解决方案，例如防火墙、反恶意软件、反勒索软件和监视软件。

- **减少攻击面**

  SOC 的主要责任是减少企业/组织的攻击面。为此，SOC 会维护包含所有工作负载和资产的清单、将安全修补程序应用于软件和防火墙、识别错误配置，并新资产联机时添加这些资产。团队成员还负责研究新出现的威胁并分析风险。

- **持续监视**

  SOC 团队使用安全分析解决方案全天候监视整个环境 - 本地、云、应用程序、网络和设备，来发现异常或可疑行为；其中这些解决方案包括安全信息企业管理（SIEM）解决方案、安全编排、自动化和响应（SOAR）解决方案和扩展检测和响应（XDR）解决方案。这些工具会收集遥测数据、聚合数据，并在某些情况下自动进行事件响应。

- **威胁情报**

  SOC 还使用数据分析、外部源和产品威胁报告来深入了解攻击者行为、基础结构和动机。这种情报提供了有关 Internet 上正在发生的情况的全局视图，并帮助团队了解威胁组是如何运作的。借助此信息，SOC 可快速发现威胁，并加强企业/组织对新出现的风险的应对。

- **威胁检测**

  SOC 团队使用 SIEM 和 XDR 解决方案生成的数据来识别威胁。这首先会从实际问题中筛选掉误报。然后，按严重性和对业务的潜在影响确定威胁的优先级。

- **日志管理**

  SOC 还负责收集、维护和分析每个客户端、操作系统、虚拟机、本地应用和网络事件生成的日志数据。分析有助于建立正常活动的基线，并揭示可能指示恶意软件、勒索软件或病毒的异常。

- **事件响应**

识别到网络攻击后，SOC 会快速采取措施，在尽可能减少业务中断的情况下限制对企业/组织的损害。措施可能包括关闭或隔离受影响的客户端和应用程序、暂停被入侵的账户、移除遭到感染的文件，以及运行防病毒和反恶意软件。

- **发现和修正**

  在攻击之后，SOC 负责将公司恢复到其原始状态。团队将擦除并重新连接磁盘、标识、电子邮件和客户端，重启应用程序，直接转换到备份系统，并恢复数据。

- **根本原因调查**

  为了防止类似的攻击再次发生，SOC 进行了彻底的调查，来确定漏洞、效果不佳的安全流程和其他导致事件的教训。

- **安全性优化**

  SOC 使用事件期间收集的任何情报来解决漏洞、改进流程和策略，并更新安全路线图。

- **合规性管理**

  SOC 职责的一个关键部分是确保应用程序、安全工具和流程符合隐私法规，例如，《PCI DSS 安全遵从包》、《ISO 27701 安全遵从包》和《ISO 27001 安全遵从包》等。团队定期审核系统来确保合规性，并确保在数据泄露后通知监管机构、执法人员和客户。

SOC 中的关键角色

根据企业/组织的规模，典型的 SOC 包括以下角色：

- **事件响应总监**

  此角色通常只出现在非常大型的企业/组织中，负责协调安全事件期间的检测、分析、遏制和恢复。还管理与相应利益干系人的沟通。

- **SOC 管理者**

  SOC 监督员是管理者，通常向首席信息安全官（CISO）报告。职责包括监督人员、运行业务、培训新员工和管理财务。

- **安全工程师**

  安全工程师负责企业/组织安全系统的启动和运行。这包括设计安全体系结构以及研究、实施和维护安全解决方案。

- **安全分析师**

  安全分析师是安全事件中的第一响应人，负责识别威胁、确定威胁的优先级，然后采取行动来遏制损害。在遭到网络攻击期间，安全分析师可能需要隔离已遭到感染的主机、客户端或用户。在一些企业/组织中，会根据安全分析师负责解决的威胁的安全程度来对这些分析师进行分级。

- **威胁搜寻者**

  在一些企业/组织中，经验最丰富的安全分析师被称为威胁搜寻者。威胁搜寻者识别和响应自动工具未检测到的高级威胁。该角色主动行动，旨在加深企业/组织对已知威胁的了解，并在攻击发生之前揭示未知的威胁。

- **取证分析师**

  大型企业/组织可能还会聘用取证分析师，取证分析师负责在出现违规后收集情报来确定其根本原因。会搜寻系统漏洞、违反安全策略的行为和网络攻击模式，这些有可能帮助防止将来发生类似的入侵。

SOC 的类型

企业/组织有几种不同的方式来设置其 SOC。一些企业/组织选择构建具有全职员工的专用 SOC。这种类型的 SOC 可以是内部的，具有物理的本地位置，也可以是虚拟的，员工使用数字工具远程协调工作。许多虚拟 SOC 既有合同工，也有全职员工。外包 SOC 也可称为“托管 SOC”或“安全运营中心即服务”，它由托管安全服务提供商运行，该提供商负责防止、检测、调查和响应威胁。此外，它可以既有内部员工，也有托管安全服务提供商。这种版本被称为托管或混合 SOC。企业/组织使用这种方法来增加自身员工的影响力。例如，如果没有威胁调查员，那么聘用第三方可能与在内部配备这些人员更加容易。

SOC 团队的重要性

强大的 SOC 可帮助企业、政府和其他组织适应于不断变化的网络威胁环境。这不是一件容易的事。攻击者和防御社区都经常开发新的技术和战略，而管理所有的变化需要时间和精力。SOC 利用其对更广泛的网络安全环境的了解以及对内部薄弱点和业务优先级的理解，帮助企业/组织制定符合业务长期需求的安全路线图。SOC 还可限制发生攻击时对业务的影响。持续监视网络并分析警报数据，因此与分散在其他几个优先事项的团队相比，更有可能更早地发现威胁。通过定期培训和记录良好的流程，SOC 可以快速处理当前事件，即使在压力极大的情况下也能做到。对于没有全天候关注安全运营的团队来说，这可能很困难。

SOC 的优势

通过将用于保护企业/组织免受威胁影响的人员、工具和流程进行统一，SOC 可帮助企业/组织更有效、更高效地防御攻击和泄露。

- **强大的安全状况**

  提高企业/组织的安全性是一项永无止境的工作。它需要持续监视、分析和规划，以发现漏洞并掌握不断变化的技术。当有待处理事项的优先级不相上下时，很容易会忽视安全性，而关注感觉更紧迫的任务。

  集中式 SOC 有助于确保持续改进流程和技术，从而减低成功攻击带来的风险。

- **遵守隐私法规**

  行业、国家和地区在治理数据收集、存储和使用方面的法规各有不同。许多法规要求企业/组织在使用者请求时报告数据泄露并检测个人数据。制定适当的流程和程序与拥有适当的技术同样重要。SOC 的成员帮助企业/组织承担保持技术和数据流程最新的责任来遵守这些法规。

- **快速响应事件**

  发现和阻止网络攻击的速度有多快至关重要。借助适当的工具、人员和情报，可以在漏洞造成任何损害之前遏止这些漏洞。但是，恶意操作者也很聪明，会隐藏起来、窃取大量数据，并在任何人注意到之前提升权限。安全事件也是一个让人非常有压力的事情，尤其是对于在事件响应方面缺乏经验的人来说。

  借助统一的威胁情报和记录良好的程序，SOC 团队能够快速检测、响应攻击，并在遭到攻击后快速恢复。

- **降低入侵成本**

  对于企业/组织来说，一次成功的入侵可能会付出非常昂贵的代价。恢复通常需要停机很长时间，很多企业在事件发生后不久会失去客户或难以赢得新客户。通过

先于攻击者行动并快速响应，SOC 可帮助企业/组织在重回正常运营时节省时间和金钱。

SOC 团队的最佳做法

要负责的事情太多，SOC 必须有效地企业/组织和管理才能取得结果。拥有强大 SOC 的企业/组织会实施以下安全做法：

- **策略与业务看齐**

  即使资金最充裕的 SOC 也必须决定将时间和金钱集中在哪些方面。企业/组织通常会先进行风险评估，来识别最容易出现风险的方面和最大的业务机会。这有助于确定需要保护哪些内容。SOC 还需要了解资产所在的环境。很多企业的环境很复杂，一些数据和应用程序在本地，一些跨多个云分布。策略有助于确定安全专业人员是否需要每天任何时间都可联系，以及是在内部配置 SOC 还是使用专业服务更好。

- **员工具备能力、经过良好培训**

  有效 SOC 的关键在于高技能且不断进步的员工。首先是要找到人才，但由于安全人员市场竞争非常激烈，因此这可能很棘手。为了避免技能差距，许多企业/组织试着寻找拥有各种专业知识的人员，这些知识包括系统和情报监视、警报管理、事件检测和分析、威胁搜寻、道德黑客、网络取证和逆向工程。还会部署可自动执行任务的技术，让较小型的团队更加高效，并提高初级分析员的产出。在定期培训方面投入有助于企业/组织留住关键员工、弥补技能差距和发展员工的职业生涯。

- **端到端可见性**

  攻击可能从单个客户端开始，因此 SOC 了解企业/组织的整个环境至关重要，这包括由第三方管理的任何内容。

- **适当的工具**

  安全事件是如此的多，团队很容易不知所措。有效 SOC 会在安全工具上投入，这些工具可很好地协同工作，并使用 AI 和自动化来上报重大风险。互操作性是避免覆盖范围出现缺口的关键。

SOC 工具与技术

- **安全信息和事件管理（SIEM）**

  SOC 中最重要的工具之一是基于云的 SIEM 解决方案，它将来自多个安全解决方案和日志文件的数据聚合在一起。借助威胁情报和 AI，这些工具帮助 SOC 检测不断演化的威胁、加快事件响应速度并先于攻击者行动。

- **安全编排、自动化和响应（Security Orchestration, Automation and Response，SOAR）**

  SOAR 可自动执行定期和可预测的扩充、响应和修正任务，从而空出时间和资源来进行更深入的调查和搜寻。

- **扩展检测和响应（Extended Detection and Response，XDR）**

  XDR 是一种服务型软件工具，它通过将安全产品和数据集成到简化的解决方案中来提供全面、更优的安全性。企业/组织使用这些解决方案在多云混合环境中主动有效地应对不断演化的威胁环境和复杂的安全挑战。与终端节点检测和响应 (EDR) 等系统相比，XDR 扩大了安全范围，从而跨更广泛的产品集成了保护，包

括企业/组织的终端节点、服务器、云应用程序和电子邮件等。在此基础中，XDR 将预防、检测、调查和响应相结合，提供可见性、分析、相关事件警报和自动化响应来增强数据安全并对抗威胁。

- **防火墙**

  防火墙会监视进出网络的流量，根据 SOC 定义的安全规则允许或阻止流量。

- **日志管理**

  日志管理解决方案通常是 SIEM 的一部分，它会记录来自企业/组织中运行的每个软件、硬件和客户端的所有警报。这些日志提供了网络活动的相关信息。

- **漏洞管理**

  漏洞管理工具会扫描网络来帮助识别攻击者可能利用的任何薄弱点。

- **用户和实体行为分析（User and Entity Behavior Analytics，UEBA）**

  用户和实体行为分析构建在许多新式安全工具之中，它使用 AI 来分析从各种设备收集的数据，来为每个用户和实体建立正常活动的基线。当事件偏离基线时，会标记该事件供进一步分析。

SOC 和 SIEM

如果没有 SIEM，SOC 将很难完成其任务。新式 SIEM 提供：

- 日志聚合：SIEM 会收集日志数据并关联警报，分析人员可使用这些信息来检测和搜寻威胁。
- 上下文：SIEM 跨组织中的所有技术收集数据，所以它帮助将单个事件之间的点连接起来，识别复杂的攻击。
- 减少警报数：SIEM 使用分析和 AI 来关联警报并识别最严重的事件，从而减少用户需要审查和分析的事件数。
- 自动响应：内置规则使 SIEM 能够识别和阻止可能的威胁，无需人员交互。

另请务必注意，单靠 SIEM 不足以保护组织。用户需要将 SIEM 与其他系统集成，为基于规则的检测定义参数，并评估警报。正因为如此，定义 SOC 策略和聘用适当的员工至关重要。

SOC 解决方案

有多种解决方案可用来帮助 SOC 保护组织。最佳解决方案协同工作，跨本地和多个云提供完整覆盖范围。云安全提供全面的解决方案，来帮助 SOC 消除覆盖范围方面的差距，并获得其环境的 360 度视图。态势感知（专业版）检测和响应解决方案集成，为分析师和威胁搜寻者提供查找和遏止网络攻击所需的数据。

常见问题

1. 安全运营中心团队要做什么？

   SOC 团队监视服务器、设备、数据库、网络应用程序、网站和其他系统，以实时发现潜在威胁。及时了解最新威胁并在攻击者利用系统或进程漏洞之前发现和解决这些漏洞，以执行主动安全工作。如果企业/组织已然遭受到攻击，SOC 团队负责根据需要去除威胁以及还原系统和备份。

2. 安全运营中心的关键组件是什么？

SOC 由有助于保护组织免受网络攻击的人员、工具和流程组成。为了实现其目标，它执行以下功能：清点所有资产和技术、日常维护和准备、持续监视、威胁检测、威胁情报、日志管理、事件响应、恢复和修正、根本原因调查、安全优化和合规性管理。

3. 为什么企业/组织需要强大的 SOC？

   强大的 SOC 通过统一防御、威胁检测工具和安全流程来帮助企业/组织更高效和有效地管理安全性。与没有 SOC 的公司相比，具有 SOC 的企业/组织能够改进其安全流程、更快地应对威胁以及更好地管理合规性。

4. SIEM 和 SOC 有什么区别？

   SOC 是负责保护企业/组织免受网络攻击的人员、流程和工具。SIEM 是 SOC 用于保持可见性和响应攻击的众多工具之一。SIEM 汇总日志文件，并使用分析和自动化向决定响应方式的 SOC 成员揭示可信威胁。

1.8.2 总览和态势总览

总览

态势感知（专业版）“总览”页面实时呈现云上整体安全评估状况，并联动其他云安全服务，集中展示云上安全，包括资产的安全评估结果、安全监控和安全趋势等信息，可以全面了解资产的安全情况。总览页面实时呈现态势感知（专业版）所有工作空间的整体安全评估结果，查看方法请参见查看总览。

态势总览

“态势总览”页面实时呈现当前工作空间中资源的整体安全评估状况，包括资产的安全评估结果、安全监控和安全趋势等信息，可以全面了解资产的安全情况。目标工作空间的“态势感知 > 态势总览”页面呈现当前单个工作空间的安全评估结果，查看方法请参见查看态势总览。

安全风险

安全风险是对资产安全状况的综合评估，反映了一段时间内资产遭受的安全风险。安全风险通常体现为一个量化的数值，便于用户理解目前资产的安全状况，数值大小并不代表资产的安全或危险，仅作为资产遭受攻击严重程度的参考。安全大屏中的可以还原攻击历史，感知攻击现状，预测攻击态势，为用户提供强大的事前、事中、事后安全管理能力，实现一屏全面感知。

安全评分

态势感知（专业版）实时呈现您云上资产的整体安全评估状况，并根据态势感知（专业版）的威胁检测能力，评估整体资产安全健康得分。

安全评分每天凌晨 2:00 自动更新，也支持通过在页面中单击“重新检测”来进行实时更新。

如下将介绍在安全评分中，不同分值的含义以及扣分项的详细情况。

- 安全分值

  态势感知（专业版）根据威胁检测能力，评估整体资产安全健康得分。

- 风险等级包括“无风险”、“提示”、“低危”、“中危”、“高危”和“致命”。
- 分值范围为 0～100，分值越大表示风险越小，资产更安全。
- 分值从 0 开始，每隔 20 取值范围对应不同的风险等级，例如分值范围 40~60 对应风险等级为“中危”。
- 分值环形图不同色块表示不同威胁等级，例如黄色对应“中危”。
- 资产风险修复，并手动刷新告警事件状态后，安全评分可以通过手动单击“重新检测”进行更新。

资产安全风险修复后，为降低安全评分的风险等级，需手动忽略或处理告警事件，刷新告警列表中告警事件状态。

表 1-4 安全分值表

风险等级	安全分值	分值说明
无风险	100 分	恭喜您，您的资产当前安全状况良好。
提示	80≤分值<100	您的资产存在少量的安全隐患，建议您及时加固安全防护体系。
低危	60≤分值<80	您的资产存在较多的安全隐患，建议您及时加固安全防护体系。
中危	40≤分值<60	您的资产防御黑客入侵的能力较弱，建议您立即加固安全防护体系。
高危	20≤分值<40	您的资产存在较高的黑客入侵和病毒感染的风险，建议您立即处理。
致命	0≤分值<20	您的资产很可能遭受到黑客入侵和病毒感染的威胁，建议您立即处理。

- 安全评分扣分项

  安全评分扣分项及其分值情况如下所示：

表 1-5 安全评分扣分项

分类	扣分项	单项扣分值	处理建议	最高扣分上限
安全服务启用	未开启安全相关服务	不扣分	开启安全相关服务	30
合规检查	存在未处理的致命不合规项	10	按照合规修复建议指导进行合规问题修复，修复后重新触发扫描任务，自	20
	存在未处理的高危不合规项	5		

分类	扣分项	单项扣分值	处理建议	最高扣分上限
	存在未处理的中危不合规项	2	动刷新评分。	
	存在未处理的低危不合规项	0.1		
漏洞	存在未处理的致命漏洞	10	按照漏洞修复建议指导进行漏洞修复，修复后重新触发漏洞扫描任务，自动刷新评分。	20
	存在未处理的高危漏洞	5		
	存在未处理的中危漏洞	2		
	存在未处理的低危漏洞	0.1		
威胁告警	存在未处理的致命告警事件	10	按照威胁事件处置指导建议进行修复，修复后自动刷新评分。	30
	存在未处理的高危告警事件	5		
	存在未处理的中危告警事件	2		
	存在未处理的低危告警事件	0.1		

1.8.3 工作空间

工作空间

工作空间（Workspace）属于态势感知（专业版）顶层工作台，单个工作空间可绑定普通项目、企业项目和 Region，可支撑不同场景下的工作空间运营模式。

数据空间

数据空间是进行数据分组、负载、流控单元。同一数据空间的数据共享同一负载均衡策略。

数据管道

数据传输消息主题和存储索引组合为数据管道。

1.8.4 告警管理

威胁告警

广义的威胁告警是指由于自然因素、人为因素或软硬件本身的原因，对信息系统造成危害的事件，或对社会造成负面影响的威胁。对于态势感知（专业版）来讲，威胁告警泛指根据大数据分析检测出的，对用户资产产生威胁的安全事件。

事件

事件是一个广泛的概念，可以包括告警，但不限于此，它可以是系统正常操作的一部分，也可以是异常或错误。在运维和安全领域，事件通常指的是已经发生并需要被关注、调查和处理的问题或故障。事件可能由一条或多条告警触发，也可能由其他因素（如用户操作、系统日志等）引发。

事件的目的是为了记录、分析、报告或审计，通常用于记录和报告系统的历史行为，以便于分析和审计。

告警

告警是运维中的一种异常信号的通知，通常是由监控系统或安全设备在检测到系统或网络中的异常情况时自动生成的。例如，当服务器的 CPU 使用率超过 90%时，系统可能会发出告警。这些异常情况可能包括系统故障、安全威胁或性能瓶颈等。

告警通常有明确的指示性，能够明确指出异常发生的位置、类型和影响。同时，告警可以按照严重程度来进行分类，如紧急、重要、一般等，以便运维人员根据告警的严重程度来决定哪些需要优先处理。

告警的目的是及时通知相关人员，以便能够迅速响应并采取措施解决问题。

当态势感知（专业版）检测到的云资源中存在的异常情况（例如，某个恶意 IP 对资产攻击、资产已被入侵等）时，将以告警的形式将威胁信息展示在态势感知（专业版）告警管理界面中。

告警和事件关系说明

本部分介绍告警和事件的含义、区别，告警转事件的原因和告警关联事件的原因。

- **告警和事件的含义与区别**

表 1-6 告警和事件的含义与区别

类别	描述

类别	描述
定义	• 告警： 告警是运维中的一种异常信号的通知，通常是由监控系统或安全设备在检测到系统或网络中的异常情况时自动生成的。例如，当服务器的 CPU 使用率超过 90%时，系统可能会发出告警。这些异常情况可能包括系统故障、安全威胁或性能瓶颈等。 告警通常有明确的指示性，能够明确指出异常发生的位置、类型和影响。同时，告警可以按照严重程度来进行分类，如紧急、重要、一般等，以便运维人员根据告警的严重程度来决定哪些需要优先处理。 告警的目的是及时通知相关人员，以便能够迅速响应并采取措施解决问题。 • 事件： 事件是一个更广泛的概念，可以包括告警，但不限于此。事件可以是系统正常操作的一部分，也可以是异常或错误。在运维和安全领域，事件通常指的是已经发生并需要被关注、调查和处理的问题或故障。事件可能由一条或多条告警触发，也可能由其他因素（如用户操作、系统日志等）引发。 事件的目的更广泛，可以是为了记录、分析、报告或审计，通常用于记录和报告系统的历史行为，以便于分析和审计。
处理流程	• 告警： 告警的处理流程通常包括接收、确认、分析、响应和关闭等步骤。当监控系统发出告警时，运维人员首先需要确认告警的真实性，然后分析告警的原因和影响范围，最后采取相应的措施来解决问题，并关闭告警。 • 事件： 事件的处理流程则更加复杂和全面。除了包含告警处理流程中的各个环节外，事件处理还需要进行事件调查、影响评估、风险分析、制定应急计划、执行应急响应、事后总结等步骤。事件处理的目标是彻底解决问题，防止类似事件再次发生，并减少事件对业务的影响。

类别	描述
重要性与紧急程度	• 告警： 告警一般需要立即评估和响应。 每条告警的紧急程度和重要性各不相同，取决于告警的类型、级别和影响的范围。一些告警可能只是简单的提醒或预警，而另一些告警则可能表示系统已经遭受严重攻击或面临重大故障风险。 • 事件： 事件可能需要记录、分析或在某些情况下采取行动，但不一定需要立即响应。 事件通常比告警具有更高的重要性和紧急程度。因为事件已经发生并产生了实际的影响，需要立即采取措施来应对和解决问题。如果事件得不到及时处理，可能会给组织带来重大的经济损失或声誉损害。

- **告警转事件或关联事件的原因**

  告警通常是在系统或服务出现异常或潜在故障时产生的通知。这些异常可能会直接影响业务的正常运行，因此告警需要被及时处理，以防止业务异常。告警通常需要采取相应的措施来清除故障，否则可能会因为这些异常或故障引起业务的异常。

  事件则是在系统或服务在正常运行状态下产生的通知，它可能涉及到一些重要的状态变化，但不一定会引起业务异常。因此，事件一般不需要进行处理，主要用于帮助分析、定位问题。

表 1-7 告警转事件或关联事件的原因

类别	说明

类别	说明
告警转事件原因	当告警的严重性达到一定程度，或者持续出现，或者其影响范围广泛时，它可能不再仅仅是一个需要关注的信号，也可能表明系统或网络中存在一个持续性的问题，此时，它已经演变成了一个需要立即处理的事件，这种情况下，可以将告警转化为事件来处理，以便深入调查问题的根源，并采取相应的措施来彻底解决。通常告警转事件的原因有以下几个方面： • 信息聚合与分类 告警通常是对某个特定条件或阈值被违反的即时响应。随着时间的推移，大量的告警可能会被触发，如果直接处理这些独立的告警，可能会变得非常混乱和低效。将这些告警聚合成事件，可以帮助相关人员根据告警的类型、来源、影响等维度进行分类，从而更有效地处理它们。 • 简化工作流程 告警到事件的转换过程，通常伴随着对告警的过滤、去重、聚合等处理。这些处理使得原本可能触发多个相似告警的情况，被整合为一个更具代表性的事件。这样不仅减少了处理单个告警的工作量，也使得处理过程更加条理清晰，便于跟踪和记录。 • 提升问题解决效率 将告警转换为事件后，由于事件通常提供了比单个告警更全面的上下文信息，因此相关人员可以更容易地识别出问题的根本原因，有助于更快地定位问题，并采取有效的解决措施。 • 便于历史回顾与趋势分析 事件记录了问题的发生、发展、解决的全过程，这为后续的问题预防、系统优化等提供了宝贵的历史数据。通过对事件进行趋势分析，可以发现系统中潜在的薄弱环节，提前采取措施进行改进。 • 增强跨部门协作 在大型组织中，不同的部门可能需要共同参与问题的处理。将告警转换为事件后，可以更容易地在不同部门之间共享相关信息，促进跨部门协作，提高问题解决的效率。 总而言之，将告警转换为事件助于简化工作流程、提升问题解决效率、便于历史回顾与趋势分析。

类别	说明
告警关联事件原因	告警关联事件是监控和故障管理中的一个重要环节，它涉及到将多个独立但可能相互关联的事件或告警组合起来，以便更好地理解问题的根源和范围，从而更有效地进行故障排查和响应。通常告警关联事件的原因有以下几个方面： • 依赖关系 在复杂的系统中，各个组件之间往往存在复杂的依赖关系。当一个组件出现故障时，可能会影响依赖它的其他组件的正常工作，进而引发一系列告警。例如，在微服务架构中，一个服务的崩溃可能导致调用该服务的其他服务也出现问题。 • 资源共享 当多个系统或服务共享同一资源（如服务器、数据库、网络设备等）时，该资源的问题可能导致多个系统或服务同时发出告警。例如，共享数据库服务器的性能下降可能会触发多个依赖该数据库的应用程序的性能告警。 • 连锁反应 某些情况下，一个初始的故障可能触发一系列连锁反应，导致更多的组件或系统受到影响。这种连锁反应可能由于系统设计不当、错误处理机制不完善或资源限制（如内存泄漏导致的性能下降）等原因引起。 • 配置错误 配置错误或不一致的配置可能导致系统行为异常，进而触发多个看似不相关的告警。例如，错误的路由配置可能导致流量被错误地路由到不稳定的服务器，从而引发多个与性能相关的告警。 • 软件缺陷 软件中的缺陷（如 bug）可能导致程序在特定条件下表现异常，并触发告警。如果这些缺陷影响了多个组件或系统，则可能引发多个关联告警。 • 外部因素 外部因素如自然灾害（如地震、洪水）、网络攻击、基础设施故障（如电力中断、网络中断）等也可能导致多个系统或组件同时出现问题，并触发大量告警。

1.8.5 安全编排

分类和映射

分类和映射是指对云服务告警进行类型匹配和字段映射。

安全编排

安全编排（Security Orchestration）是将企业和组织在安全运营过程中涉及的不同系统或者一个系统内部不同组件的安全功能通过可编程接口（API）封装后形成的安全能力（即应用）和人工检查点按照一定的逻辑关系组合到一起，以完成某个特定的安全运营过程和规程。

安全编排是将安全运营相关的工具/技术、流程和人员等各种能力整合到一起的一种协同工作方式。

剧本

剧本（Playbook）是安全运营流程在安全编排系统中的形式化表述，它是将安全运营流程和规程转换为机读工作流的过程。

剧本体现了安全防护的逻辑，指示如何调度安全能力。剧本具有灵活性和可扩展性，可以根据实际需求进行修改和扩展，以适应不断变化的安全威胁和业务需求。

流程

流程（Workflow）是将安全运营相关的工具、技术、流程和人员等各种能力整合到一起，形成一种协同工作方式。它由多个相连接的组件构成，流程定义完成后可被外部触发，例如，当新工单产生时自动触发自动审核工单流程。您可以通过可视化流程编辑画布，定义每个节点的组件动作。

流程是剧本触发时响应的方式，它负责将剧本中的指令和规程转化为具体的操作和执行步骤。

剧本和流程的关系

- 联系：剧本提供了安全运营的指导和规则，而流程则负责将这些规则转化为具体的执行步骤和操作。剧本和流程相互依赖，剧本指导流程的执行，而流程则实现了剧本的意图和要求。
- 区别：剧本和流程之间也存在一定的区别。首先，剧本更侧重于定义和描述安全运营的流程和规程，它关注的是整体的框架和策略；而流程则更侧重于具体的操作和执行步骤，它关注的是如何将剧本中的要求转化为实际的行动。其次，剧本具有较大的灵活性和可扩展性，可以根据需要进行修改和扩展；而流程则相对固定，一旦设计完成，就需要按照规定的步骤执行。

示例：以一个具体的网络安全事件响应案例为例，当组织遭受到一次网络攻击时，安全编排系统会首先根据预设的剧本识别出攻击的类型和严重程度。然后，系统会根据剧本中定义的流程，自动触发相应的安全措施，如隔离被攻击的系统、收集攻击数据、通知安全团队等。在这个过程中，剧本和流程紧密配合，确保安全响应的准确性和及时性。

插件管理

- 插件：是包含函数、连接器、公共库的聚合。插件有自定义插件和商业插件两种类型，其中，自定义的插件可以在集市中显示，也可以在剧本中使用。
- 插件集：是具有相同业务场景的插件集合。
- 函数：是可以在剧本中选用的执行函数，在剧本中执行特定的行为。

- 连接器：是用于连接数据源，将告警、事件等安全数据接入态势感知（专业版），包括事件触发和定时触发两种连接器类型。
- 公共库：是一个公共模块，包含在其他组件中会使用到的 API 调用和公共函数。

操作连接

操作连接是安全编排流程中，每个插件节点需要使用到的连接域名和鉴权参数。用于在安全编排的流程执行过程中，每个插件节点运行时，传入需要连接的域名信息，以及在访问该域名时，需要使用到的用户鉴权信息，如用户名/密码、账号 AK/SK 等。

操作连接与插件的关系

每个插件在运行过程中，需要通过域名调用的方式访问其他云服务或者三方服务，调用过程中需要鉴权，因此，在插件的登录凭证参数中会定义需要的域名参数（Endpoint）和认证参数（用户名/密码、账号 AK/SK 等）。操作连接则是配置插件登录凭证的参数值，流程中每个插件节点绑定不同的操作连接，支持相同插件的不同节点访问不同的服务。

实例监控

当剧本/流程执行完成后，实例管理列表中会生成剧本/流程实例，即实例监控。实例监控列表每条记录是一个实例，可呈现实例的历史实例任务列表，以及历史实例任务的运行情况。

1.8.6 安全分析

生产者

是用来构建并传输数据到服务端的逻辑概念，负责把数据放入消息队列。

订阅器

用于订阅态势感知（专业版）管道消息，一个管道可由多个订阅器进行订阅，态势感知（专业版）通过订阅器进行消息分发。

消费者

是用来接收并处理数据的运行实体，负责通过订阅器把态势感知（专业版）管道中的消息进行消费并处理。

消息队列

是数据存储和传输的实际容器。

威胁检测模型

是一种被训练的 AI 智能识别算法模型。能针对特定威胁，自动化的完成数据汇聚、分析和报警，这种检测模式具备较好的泛化能力，防躲避能力强，可在不同业务系统中发挥同等效果，应对复杂的新型攻击。

2 购买态势感知（专业版）

2.1 购买态势感知（专业版）

操作场景

态势感知（专业版）专业版支持包周期和按需方式进行购买，您可以根据业务需求购买态势感知（专业版）。

购买态势感知（专业版）

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在总览页面中，单击右上角“购买态势感知（专业版）”，进入购买态势感知（专业版）页面。

步骤 4 （可选）购买访问授权。

首次购买需要进行访问授权，获取账号中的 ECS 主机资产信息。在弹出的访问授权页面中，勾选同意授权并单击“确认”。

步骤 5 在购买态势感知（专业版）页面，配置购买参数，参数说明如下所示：

表 2-1 购买态势感知（专业版）参数说明

参数名称	说明
计费模式	请根据您的需求选择“包周期”或“按需”计费模式。 • 包周期：一种预付费模式，即先付费再使用，按照订单的购买周期进行结算。购买周期越长，享受的折扣越大。 • 按需：一种后付费模式，即先使用再付费，按照实际使用时长计费，秒级计费，按小时结算。按需计费模式允许您根据实际业务需求灵活地调整资源使用，无需提前预置资源，从而降低预置过多或不足的风险。

参数名称	说明
区域	根据已有云上资源所在的区域选择态势感知（专业版）的区域。
版本	选择“专业版”。
配额数	配额数是指主机资产支持防护的最大主机数量。 请根据当前账户下所有主机资产总数设置配额数，可设置最大主机配额需等于或大于当前账户下主机总数量，且不支持减少。 **说明** • 配额数最大限制为 10000 台。 • 为避免主机资产在防护份额外，不能及时感知攻击威胁，而造成数据泄露等安全风险。当主机资产数量增加后，请及时增加配额数。
购买时长	选择“购买时长”。 其中，选择按 1 个月进行收费时，到期将自动续费。

步骤 6 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤 7 确认订单详情无误后，阅读并同意相关协议，单击“去支付”。

步骤 8 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

生效条件

付款成功后，您可以在管理控制台“已购资源”页面查看当前购买的态势感知（专业版）版本。

2.2 增加配额

操作场景

购买态势感知（专业版）资产配额完成后，当用户资产数量增加，或需对不同资产有不同使用时长需求，可参考本章节增加配额扩充“配额数”，并配置使用时长。

约束与限制

- 配额数是授权检测主机的数量。配额数最大限制为 10000 台。
- 在购买态势感知（专业版）时，选择的最大配额需等于或大于当前账户下主机总数量，且不支持减少。如果购买的最大配额小于主机数量，可能会造成未授权检测的主机被攻击后，不能及时感知威胁，造成数据泄露等风险。

增加配额

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版） ”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“已购资源”，进入已购资源页面后，在待购买态势感知（专业版）专业版所在 region 栏中，单击“增加配额”。

步骤 4 在购买态势感知（专业版）页面，配置购买参数。

表 2-2 增加配额参数说明

参数名称	说明
当前配置	显示已选择 region 态势感知（专业版）版本信息，**无需配置**。
升级方式	选择“增加配额”。
配额数	配额数是指主机资产支持防护的最大主机数量。 请根据当前账户下所有主机资产总数设置配额数，可设置最大主机配额需等于或大于当前账户下主机总数量，且不支持减少。 说明 ● 配额数最大限制为 10000 台。 ● 为避免主机资产在防护份额外，不能及时感知攻击威胁，而造成数据泄露等安全风险。当主机资产数量增加后，请及时增加配额数。
标签	如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在 TMS 中创建预定义标签，也可以直接在此处创建标签。

步骤 5 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤 6 确认订单详情无误后，阅读并勾选《态势感知（专业版）服务免责声明》，单击“去支付”。

步骤 7 在支付页面，选择付款方式完成付款，完成增加配额购买操作。

----结束

2.3 续费

操作场景

态势感知（专业版）续费是在原已购买的版本规格的基础上，延长使用时间。续费操作不可变更版本规格，即不能改变“配额数”。

续费操作仅针对**包周期**版本规格。

- 包周期（包年/包月）模式为预付费方式。当购买的包周期版本到期时，用户需通过续费延长使用期。

- 按需计费为按小时计费，即开即用。在账户余额充足前提下，不涉及过期情况，即无需续费操作。

手动续费

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“已购资源”，进入已购资源页面后，在待续费态势感知（专业版）版本所在 region 栏中，单击“续费”，系统跳转至费用中心“续费管理”页面。

步骤 4 在态势感知（专业版）实例所在行，单击“续费”，跳转至“续费”页面。

步骤 5 配置“续费时长”，如选择“一年”。

步骤 6 （可选）设置并勾选“统一到期时间”。默认将统一到期时间设置为每月 1 号 23:59:59 GMT+08:00。

步骤 7 单击“去支付”，跳转至支付页面，完成付款。

步骤 8 返回续费管理页面，可查看态势感知（专业版）已续费成功。

----结束

开通自动续费

在账户余额充足前提下，已配置“自动续费”后，包周期版本的资产配额、增值包、安全编排将自动续费，延长使用周期。

步骤 1 登录管理控制台。

步骤 2 单击“费用与成本 > 续费管理”，跳转至费用中心“续费管理”页面。

步骤 3 在“手动续费项”页签，选择态势感知（专业版）专业版实例，单击“设为自动续费”，跳转至自动续费配置页面。

步骤 4 选择配置“自动续费周期”和勾选“预设自动续费次数”。

步骤 5 单击“开通”，完成自动续费配置。

步骤 6 返回续费管理页面，在“自动续费项”页签，可查看态势感知（专业版）已开通自动续费。

后续将根据配置，自动续费延长使用期。

----结束

2.4 退订

操作场景

如果用户不再使用态势感知（专业版）防护功能或增值包，可执行退订或一键取消操作。

- 包周期（包年/包月）计费模式：预付费方式。新购 5 天内的资源，支持每年 10 次 5 天无理由“退订”；使用超过 5 天的资源，“退订”需要收取手续费。

退订包周期计费

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在“总览”页面中，单击右上角“专业版”，显示版本管理窗口。

步骤 4 针对包周期购买的资产配额，单击“退订”，进入云服务退订页面。

步骤 5 在需要退订的实例所在行，单击“操作”列中的“退订资源”，进入退订资源页面。

步骤 6 确认待退订资源信息，选择退订原因，并勾选退订确认。

步骤 7 单击“退订”，在退订管理页面确认退订。

退订成功后，返回版本管理窗口，包年/包月计费的资产配额已取消。

----结束

3 服务委托授权

操作场景

态势感知（专业版）功能对其他云服务资源有依赖，需要您将相关云服务的操作权限委托给态势感知（专业版），让态势感知（专业版）以您的身份使用这些云服务，代替您进行一些任务调度、资源运维等工作。

当您**首次**使用态势感知（专业版）时，需要先进行委托授权操作，才能正常访问和使用态势感知（专业版）。

前提条件

已购买态势感知（专业版）。

服务委托授权

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，进入态势感知（专业版）工作空间页面。

步骤 4 （可选）在空间管理页面上方单击“服务委托授权-当前租户”，右侧弹出授权页面。

首次进入无需进行单击操作，页面将自动弹出服务委托授权页面。

步骤 5 在授权页面中，默认已勾选所需全部权限，请勾选权限下方的“同意授权”，并单击“确认”。

----结束

4 查看总览

态势感知（专业版）“总览”页面实时呈现云上整体安全评估状况，并联动其他云安全服务，集中展示云上安全，包括资产的安全评估结果、安全监控和安全趋势等信息，可以全面了解资产的安全情况。

态势感知（专业版）支持查看所有工作空间的整体安全评估结果，以及单个工作空间的安全评估结果，其中：

- 总览：总览页面实时呈现态势感知（专业版）所有工作空间的整体安全评估结果，具体查看方法请参见本章节操作步骤。
- 态势总览：目标工作空间的“态势感知 > 态势总览”页面呈现单个工作空间的安全评估结果，具体查看方法请参见查看态势总览。

查看总览

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“总览”，进入态势感知（专业版）总览页面。

步骤 4 在总览页面查看您的资产安全总览情况，并进行相关操作。“总览”分为以下几个板块：

- 安全评分
- 安全监控
- 安全趋势

各个板块数据统计周期及更新频率如下表所示：

表 4-1 总览

参数名称	统计周期	更新频率	说明

参数名称	统计周期	更新频率	说明
安全评分	实时	• 每天 2:00 自动更新 • 随手动单击“重新检测”更新而更新	根据是否开启各安全服务防护、未处理的配置问题等级及个数、未处理的漏洞等级及个数、未处理的威胁事件等级及个数等计算而来。 详细评分信息请参见安全评分。
威胁告警	近 7 天	每 5 分钟	本账号态势感知（专业版）下全部工作空间告警管理中的告警总和。 详细信息请参见表 4-2 中“威胁告警”的说明。
漏洞	近 7 天	每 5 分钟	本账号态势感知（专业版）下全部工作空间漏洞管理中的漏洞总和。 详细信息请参见表 4-2 中“漏洞”的说明。
合规检查	实时	每 5 分钟	本账号态势感知（专业版）下全部工作空间基线检查中的问题总和。 详细信息请参见表 4-2 中“合规检查”的说明。
安全趋势	近 7 天	每 5 分钟	展示**近 7 天内**整体资产安全健康得分的趋势图。

----结束

安全评分

“安全评分”板块根据态势感知（专业版）的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况。

- 安全评分每天凌晨 2:00 自动更新，也支持通过单击“重新检测”来进行实时更新。
- 分值范围为 0～100，分值越大表示风险越小，资产更安全，安全分值详细说明请参见安全评分。
- 分值环形图不同颜色表示不同威胁等级。例如，黄色对应“中危”。
- 资产风险修复，并手动刷新告警事件状态后，安全评分实时更新。资产安全风险修复后，也可以直接单击“重新检测”，重新检测资产并进行评分。

  资产安全风险修复后，为降低安全评分的风险等级，需手动忽略或处理告警事件，刷新告警列表中告警事件状态。
- 安全评分显示为历史扫描结果，**非实时**数据，如需获取最新数据及评分，可单击“重新检测”，获取最近的数据。

安全监控

“安全监控”板块展示待处理**威胁告警**、待修复**漏洞**、**合规检查**问题的安全监控统计数据。

表 4-2 安全监控参数说明

参数名称	参数说明
威胁告警	呈现**近 7 天内**本账号所有工作空间内未处理威胁告警，可快速了解资产遭受的威胁告警类型和数量，呈现威胁告警的统计结果。统计信息更新频率为每 5 分钟更新一次。 • 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了入侵事件，建议您立即查看告警事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看告警事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该告警事件的详情。 • 单击威胁告警模块，系统将列表实时呈现**近 7 天内** TOP5 的威胁告警事件，可快速查看威胁告警详情，监控威胁告警状况。 – 呈现近 7 天 TOP5 的威胁告警事件的信息，包括威胁告警名称、告警等级、资产名称、告警发现时间。 – 如果列表显示内容为空，表示近 7 天无威胁告警事件。

参数名称	参数说明
漏洞	展示您本账号所有工作空间内资产中 TOP5 漏洞类型，以及**近 7 天内**还未修复的漏洞总数和不同漏洞风险等级对应的数量。统计信息更新频率为每 5 分钟更新一次。 • 此处严重等级含义如下： – 高危：即高危风险，表示资产中检测到了漏洞事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 中危：即中危风险，表示资产中检测到了可疑的异常事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 其他：即其他类型（低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该漏洞的详情。 • 单击漏洞模块中的“漏洞类型 Top5”栏，系统将呈现 TOP5（根据某个漏洞影响的主机数量进行排序）的漏洞类型。 – 此处的 TOP 等级是根据某个漏洞影响的主机数量进行排序，受影响主机数量越多排名越靠前。 – 要求 **Linux** 系统主机中 Agent 版本为 3.2.9.30 及以上，**Windows** 系统主机中 Agent 版本为 4.0.19.30 及以上。更多信息请参见主机 Agent 版本说明和升级主机 Agent。 • 单击漏洞模块中的“实时监控最新漏洞风险事件 Top5”栏，系统将列表实时呈现**近 7 天内** TOP5 的漏洞事件，可快速查看漏洞详情。 – 呈现当日最新 TOP5 漏洞事件详情，包括漏洞名称、漏洞等级、资产名称、漏洞发现时间。 – 如果列表显示内容为空，表示当日无漏洞事件。
合规检查	展示您本账号所有工作空间内资产中存在的合规风险总数量和不同危险等级的合规检查风险对应的数量。统计信息更新频率为每 5 分钟更新一次。 • 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了不合规配置，建议您立即查看合规异常事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常配置，建议您立即查看合规检查事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常配置，建议您及时查看该合规检查项目的详情。 • 单击合规检查异常模块，系统将列表实时呈现 TOP5 的合规检查异常事件，可快速查看合规检查详情。 – 呈现最近一次合规检查中 TOP 的合规异常事件详情，包括合规检查项目名称、等级、受影响资产数量、发现时间。 – 如果列表显示内容为空，表示无合规异常事件。

安全趋势

“安全趋势”板块展示**近 7 天内**您的整体资产安全健康得分的趋势图。更新频率为每 5 分钟更新一次。

5 工作空间

5.1 工作空间概述

本章节将介绍工作空间相关的如下内容：

- 什么是工作空间？

此外，工作空间支持如下操作：

- 新增工作空间：工作空间（Workspace）属于态势感知（专业版）顶层工作台，单个工作空间可绑定普通项目、企业项目，可支撑不同场景下的工作空间运营模式。在使用态势感知（专业版）的基线检查、告警管理、日志审计、安全编排等功能前，需要先创建工作空间，它可以将资源划分为各个不同的工作场景，避免资源冗余查找不便，影响日常使用。
- 查看工作空间：用户通过管理控制台查看已有工作空间的信息，包括名称、类型和创建时间等。
- 编辑工作空间：工作空间新增成功后，可以对工作空间的基本信息（**名称**、**描述**）进行修改。
- 删除工作空间：如果不再需要某个工作空间，可以删除工作空间。工作空间删除后，相关的资产会存在风险，且会影响资产的风险预防和处理，安全性能降低，删除后不可恢复，请谨慎操作。
- 管理工作空间标签：工作空间新增成功后，可以对工作空间的标签进行添加、编辑和删除操作。标签以键值对的形式表示，用于标识工作空间，便于对工作空间进行分类。此处的标签仅用于工作空间的管理。
- 创建空间托管：空间托管是指跨账号安全运营，可实现 Workspace 委托集中安全运营查看统一资产风险、告警和事件等。态势感知（专业版）支持将项目中的工作空间托管给其他用户，托管后，可实现 Workspace 委托集中安全运营查看统一资产风险、告警和事件等。
- 管理托管：空间托管页面中，可以管理托管视图、我纳管的和纳管我的。
  - 托管视图：查看已创建的托管视图及其详细信息，支持查看、编辑、修改、删除或批量删除托管视图。
  - 我纳管的：呈现有哪些工作空间托管在我创建的托管视图中，支持查看我纳管的任务以及任务参数，管理我纳管的任务（包括接收、拒绝、解除、删除）。

- 纳管我的：呈现我的工作空间被哪些托管视图纳管着，支持查看纳管我的托管视图相关参数，支持修改已接收的托管任务、撤回已接收的托管任务、重申托管关系、解除托管关系、删除托管任务。

什么是工作空间？

工作空间（Workspace）属于态势感知（专业版）顶层工作台。

- 空间管理：

  单个工作空间可绑定普通项目，可支撑不同场景下的工作空间运营模式。

- 空间托管：

  跨账号安全运营，可实现工作空间委托集中安全运营查看统一资产风险、告警和事件等。

5.2 新增工作空间

操作场景

工作空间（Workspace）属于态势感知（专业版）顶层工作台，单个工作空间可绑定普通项目、企业项目，可支撑不同场景下的工作空间运营模式。

在使用态势感知（专业版）的基线检查、告警管理、日志审计、安全编排等功能前，需要先创建工作空间，它可以将资源划分为各个不同的工作场景，避免资源冗余查找不便，影响日常使用。

本章节介绍如何新增工作空间。

新增工作空间

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，进入态势感知（专业版）工作空间页面。

步骤 4 （可选）首次进入空间管理页面时，需要进行授权操作。

1. 在空间管理页面上方单击“服务委托授权-当前租户”，右侧弹出授权页面。
2. 在授权页面中，默认已勾选所需的全部权限，请勾选权限下方的“同意授权”，并单击“确认”。

步骤 5 在工作空间管理页面中，单击“新增”，系统从右侧弹出新增工作空间页面。

步骤 6 配置新建工作空间参数，参数说明如下表所示：

表 5-1 新增工作空间

参数名称	参数说明

参数名称	参数说明
区域	选择待新增工作空间所在区域。
企业项目	可选参数，在下拉列表中选择您所在的企业项目。 企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。 **说明** “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。
工作空间名称	自定义工作空间的名称。命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_()）。 • 长度不能超过 64 个字符。
标签	可选参数，添加该工作空间的标签，用于标识工作空间，方便您对工作空间进行分类和跟踪。
描述	可选参数，设置该工作空间的备注信息。

步骤 7 单击“确定”，完成工作空间的新增。

步骤 8 工作空间配置完成后，在左侧导航栏选择“工作空间 > 空间管理”，进入态势感知（专业版）工作空间管理页面，可查看已新增的工作空间。

----结束

5.3 空间管理

5.3.1 查看工作空间

操作场景

本章节介绍用户如何通过管理控制台查看工作空间的信息，包括名称、类型和创建时间等。

约束与限制

新创建的工作空间需要初始化，工作空间创建完成后需要等待约 10 分钟后刷新查看。

查看工作空间

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，进入态势感知（专业版）工作空间页面。

步骤 4 在工作空间界面，查看已有工作空间的信息。

当工作空间较多时，可以通过搜索功能快速查询指定工作空间。

图 5-2 工作空间详情

表 5-2 工作空间参数说明

参数名称	参数说明
名称	工作空间的名称。
类型	工作空间的类型。 工作空间分为普通工作空间和托管视图。 • 普通工作空间 – 未托管：未被托管视图纳管的工作空间，工作空间名称后不携带标签。 – 已托管：已经被托管视图纳管的工作空间，工作空间名称后会有“已托管”标签。 • 托管视图 – 托管视图：可用于纳管其他工作空间，实现多个工作空间集中管理，实现跨账号安全运营。托管视图更多信息请参见创建空间托管。
ID	工作空间的 ID。
区域	工作空间所属区域。
项目	工作空间所属的项目。
更多	将鼠标悬停在“更多”上，可查看工作空间 ID、区域、项目、企业项目、创建时间等信息。
托管状态	工作空间是否托管。
事件	该工作空间中的事件数量。事件更多信息请参见查看事件信息。
漏洞	该工作空间中的漏洞数量。漏洞更多信息请参见漏洞管理概述。
告警	该工作空间中的告警数量。告警更多信息请参见告警概述。
情报	该工作空间中的情报数量。情报更多信息请参见查看情报指标。

参数名称	参数说明
资产	该工作空间中已有资产的数量。资产管理更多信息请参见资产管理概述。
安全分析	该工作空间中已有数据空间数量。
实例	该工作空间中已有实例的数量。
剧本	该工作空间中已有剧本的数量。剧本更多信息请参见安全编排概述。

步骤 5 如需查看某个工作空间的详细信息，可单击待查看工作空间右侧的，进入工作空间基本信息页面查看详细信息。

- 在工作空间详情页面，可查看工作空间的名称、创建时间、所属项目等信息。另外，还支持修改工作空间名称和描述信息。
- 在“标签”页签中，支持“编辑标签”，标签的详细操作请参考管理工作空间标签。
- 在“导航设置”页签，可以设置当前工作空间的目录，导航设置页签的参数含义如下：

表 5-3 目录参数说明

参数名称	参数说明
面包屑导航显示开关	按钮默认开启。该开关用于控制是否允许用户返回外层导航目录。 • 开关打开：用户可返回外层空间管理导航目录。 • 开关关闭：用户无法返回外层空间管理导航目录。
工作空间导航设置	• 新增：用户自定义新增目录。 • 批量编辑：支持批量编辑，设置“落地页”，设置“是否显示”按钮。落地页即单击工作空间名称后进入空间详情的默认页面。 • 批量删除：支持批量删除目录，仅用户自定义的目录支持删除，系统内置目录不支持删除。
导航名称	导航目录所属的一级目录名称。单击一级目录名称前方的按钮可展开该一级目录下的二级目录名称。
目录状态	目录所属的类型。
发布者	目录的发布者。
布局	目录关联的布局。
目录地址	目录所在地址。系统自动生成的访问目录页面的地址。
中文别名	目录的中文名称。

参数名称	参数说明
英文别名	目录的英文名称。
落地页	设置单击工作空间名称后进入空间详情的默认页面。 • 一个工作空间必须有一个落地页。 • 只能设置允许显示的目录中的一个作为落地页。 • 一级目录不支持设置为落地页。
是否显示	控制该目录是否在导航栏显示。
操作	可对目录进行编辑、更换布局等操作。 编辑：支持编辑目录的“中文别名”、“英文别名”、“落地页”、“是否显示”。 更换布局：用户自定义的目录，或系统内置的关联了布局的目录支持更换布局。**仅支持更换相同布局类型的其他布局。**

----结束

5.3.2 编辑工作空间

操作场景

工作空间新增成功后，您可以对工作空间的基本信息（**名称**、**描述**）进行修改。

该任务指导您如何编辑工作空间。

编辑工作空间

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，进入态势感知（专业版）工作空间页面。

步骤 4 单击目标工作空间所在栏右上角的（设置按钮），进入工作空间详情页面。

图 5-3 工作空间详情页面入口

步骤 5 在工作空间详情页面，单击“工作空间名称”或“描述”后的（编辑按钮）。

表 5-4 编辑工作空间参数说明

参数名称	参数说明
名称	编辑工作空间的名称。配置约束如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_()）。 • 长度不能超过 64 个字符。
描述	编辑工作空间描述。不超过 512 个字符长度。

步骤 6 编辑工作空间名称或描述后，单击“确定”。并单击工作空间详情页面右下角的“关闭”按钮。

步骤 7 在左侧导航栏选择“工作空间 > 空间管理”，进入态势感知（专业版）工作空间页面。单击待查看工作空间右侧的，进入工作空间基本信息页面查看详细信息。

----结束

5.3.3 删除工作空间

操作场景

如果不再需要某个工作空间，可以参照本章节进行删除。

工作空间删除后，相关的资产会存在风险，且会影响资产的风险预防和处理，安全性能降低，**且删除后不可恢复，请谨慎操作**。

约束与限制

- 删除时，工作空间内运行的剧本、流程、引擎等将立即停止。
- 选择永久删除，工作空间内的所有内容将永久删除无法恢复。
- 工作空间创建时系统会执行工作空间初始化，待工作空间初始化完成后才可执行删除工作空间操作。

删除工作空间

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，进入态势感知（专业版）工作空间页面。

步骤 4 单击目标工作空间所在栏右上角的（设置按钮），进入工作空间详情页面。

图 5-4 工作空间详情页面入口

步骤 5 在工作空间详情页面，单击右下角“删除”。

步骤 6 在弹出的删除工作空间框中，确认无误后，勾选“永久删除工作空间”，并在确认删除提示框中输入“DELETE”后，单击“确定”。

步骤 7 完成工作空间删除后，在左侧导航栏选择“工作空间 > 空间管理”，在该页面无已删除工作空间的信息则表示工作空间删除执行成功。

- 删除时，工作空间内运行的剧本、流程、引擎等将立即停止。
- 选择永久删除，工作空间内的所有内容将永久删除无法恢复。
- 工作空间创建时系统会执行工作空间初始化，待工作空间初始化完成后才可执行删除工作空间操作。

----结束

5.3.4 管理工作空间标签

操作场景

工作空间新增成功后，您可以对工作空间的标签进行添加、编辑和删除操作。标签以键值对的形式表示，用于标识工作空间，便于对工作空间进行分类。此处的标签仅用于工作空间的管理。

该章节指导您如何管理标签。

约束与限制

一个工作空间最多添加 20 个标签。

管理工作空间标签

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，进入态势感知（专业版）工作空间页面。

步骤 4 单击目标工作空间所在栏右上角的（设置按钮），进入工作空间详情页面。

图 5-5 工作空间详情页面入口

步骤 5 在工作空间详情页面中单击“编辑标签”，进入编辑标签页面。

步骤 6 在编辑标签页面中，支持对标签做如下操作。

表 5-5 管理标签

参数名称	参数说明
添加新标签	1. 在编辑标签页面中，单击“添加新标签”。 2. 配置标签键和值。 • 键的长度最大 36 字符，由英文字母、数字、下划线、中划线、中文字符组成。 • 值的长度最大 43 字符，由英文字母、数字、下划线、点、中划线、中文字符组成。 3. 配置完成后，单击“确定”。
删除标签	1. 在编辑标签页面中，单击标签所在行的“删除”。 2. 配置完成后，单击“确定”。

----结束

5.4 空间托管

5.4.1 创建空间托管

空间托管概述

空间托管旨在协助企业解决安全运营人员不足、提高安全运营效率，通过空间托管实现:

- 多个工作空间集中管理。
- 统一查看资产风险、告警、事件等。
- 实现跨账号安全运营。

空间托管支持的功能参见表 5-6。

表 5-6 空间托管支持的统一管理功能说明

功能	子功能	说明

功能	子功能	说明
统一安全运营	态势总览	汇总托管视图纳管的多个工作空间的安全评估结果。 查看态势总览请参见查看态势总览。
	安全报告	呈现托管视图纳管的多个工作空间的所有安全报告，根据安全报告名称后的报告归属的工作空间名称根据需要选择查看。 查看安全报告请参见查看安全报告。
统一资产管理	资产管理	呈现托管视图纳管的多个工作空间的所有资产，资产统一管理，根据资产列表中资产对应的“工作空间名称”区分资产所属的工作空间。 更多信息请参见资产管理概述。
统一风险预防	基线检查	可汇聚托管视图纳管的多个工作空间的基线检查结果，支持查看检查结果、立即执行基线检查、反馈检查结果。根据检查结果列表中每个检查项对应的“工作空间名称”区分该项检查结果所属的工作空间。
	漏洞管理	可汇聚托管视图纳管的多个工作空间的漏洞信息，仅支持查看漏洞信息。关于漏洞的更多信息请参见漏洞管理概述。根据漏洞列表中每个漏洞对应的“工作空间名称”区分漏洞所属的工作空间。
	策略管理	可汇聚托管视图纳管的多个工作空间的策略，支持统一管理，支持新增策略、管理策略。在托管视图工作空间“风险预防 > 策略管理”界面策略列表中策略对应的“工作空间名称”区分策略所属的工作空间。
统一威胁运营	事件管理	可汇聚托管视图纳管的多个工作空间的事件，支持统一管理，支持查看事件信息、新增或编辑事件、关闭或删除事件。在托管视图工作空间“威胁管理 > 事件管理”页面，根据事件列表中事件对应的“工作空间名称”区分事件所属的工作空间。
	告警管理	可汇聚托管视图纳管的多个工作空间的告警，支持统一管理，支持查看告警信息、告警转事件或关联事件、关闭或删除告警、新增或编辑告警、一键阻断或解封。在托管视图工作空间“威胁管理 > 告警管理”页面，根据告警列表中告警对应的“工作空间名称”区分告警所属的工作空间。

功能	子功能	说明
	情报管理	可汇聚托管视图纳管的多个工作空间的情报信息，支持统一管理，支持查看情报指标、新增或编辑情报指标。在托管视图工作空间“威胁管理 > 情报管理”页面，根据情报指标列表中指标对应的“工作空间名称”区分指标所属的工作空间。
	智能建模	支持按照工作空间维度呈现，方便用户查看和管理。 支持 12.1.2 查看模型模板、12.1.3 新建或编辑模型、12.1.4 查看模型、12.1.5 管理模型。
	安全分析	支持按照工作空间维度呈现数据空间，方便用户查看和管理。 安全分析更多信息请参见 11.2.1 安全分析概述。
安全编排	剧本编排	支持按照工作空间维度呈现，方便用户查看和管理。 更多信息请参见安全编排概述。
	页面布局	支持按照工作空间维度呈现，方便用户查看和管理。 更多信息请参见查看布局、查看布局模板。
	插件管理	支持按照工作空间维度呈现，方便用户查看和管理。 更多信息请参见查看插件详情。
云服务接入	云服务接入	支持按照工作空间维度呈现，方便用户查看和管理。 更多信息请参见 11.5.1 支持接入的云服务日志、11.5.2 接入日志数据。

空间托管流程

空间托管的流程说明如下：

表 5-7 空间托管流程

操作步骤	说明
步骤一：创建托管视图	创建托管视图管理托管任务。

操作步骤	说明
步骤二：创建托管	态势感知（专业版）支持将项目中的工作空间托管给其他用户，托管后，可实现 Workspace 委托集中安全运营查看统一资产风险、告警和事件等。
步骤三：托管授权	由于托管是将本项目中的工作空间托管给其他用户，因此，需要双重授权。 1. 创建委托后，需要先在已有账号中，接收授权，同意将工作空间托管给其他用户。 2. 然后在目标账号的“工作空间 > 空间托管 > 我纳管的”菜单下进行托管授权，统一接收托管。 授权后，被托管空间将挂载到托管账号下的空间中，进行统一管理。

约束与限制

- 空间托管视图以及工作空间个数的规格如下:
  - 托管视图规格约束：单账号单 Region 内最多创建 1 个空间托管视图。
  - 纳管的规格约束：
    - 单 Region 场景：1 个空间托管视图可以纳管的工作空间总数≤ 100 个。
    - 跨 Region 场景：1 个空间托管视图可以纳管的工作空间总数 ≤ 10 个。
    - 如果托管视图纳管的工作空间个数超出以上规格，需要提交工单申请扩容。
  - 被纳管的规格约束：单账号创建空间委托总数 ≤ 10 个。

步骤一：创建托管视图

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间托管”，进入空间托管管理页面。

步骤 4 在“托管视图”页签中，单击“创建托管视图”，右侧弹出创建托管视图页面。

步骤 5 配置托管视图参数。

表 5-8 创建托管视图参数说明

参数名称	参数说明
托管视图名称	设置托管视图名称。配置约束如下: • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_()）。 • 长度不能超过 64 个字符。

参数名称	参数说明
绑定空间名称	下拉选择需要绑定的工作空间。此处绑定的空间即为主空间。
（可选）描述	自定义托管视图描述信息。长度不超过 512 个字符。

步骤 6 单击“确定”。

创建成功后，可以在“空间管理”或“空间托管”页面中查看已创建的托管视图。

----结束

步骤二：创建托管

步骤 1 在空间托管页面中，单击页面右上角“创建托管”，右侧弹出创建托管页面。

步骤 2 配置托管参数。

表 5-9 创建托管参数说明

参数名称		参数说明
发起方式		选择空间托管的发起方式。
托管方	托管空间	下拉选择托管工作空间。
受托管方	租户	输入受托管方用户的账号名称。可单击“使用当前租户信息”获取账号名称，或参考如下方式获取： 1. 已登录管理控制台。并将鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”，默认进入 API 凭证页面。 2. 在 API 凭证页面中，获取“账号名”。
	托管视图	选择已有的托管视图。
托管信息	托管名称	设置托管名称。配置约束如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_()）。 • 长度不能超过 64 个字符。
	托管时长	选择托管时长。
	托管策略	选择托管策略。
	描述	自定义托管描述信息。长度不超过 512 个字符。

步骤 3 单击“确认”。

----结束

步骤三：托管授权

步骤 1 在托管页面中，选择“我纳管的”页签，并在目标托管任务所在行“操作”列，单击“接收”。

如果接收托管时，界面提示未授权，请先参考服务委托授权进行授权后，再进行托管接收操作。

步骤 2 在弹出的确认框中，单击“确认”。

----结束

后续处理

授权后，可以在“工作空间 > 空间管理”页面中查看已创建的托管视图，单击视图名称，进入后，可以查看被托管空间的详细信息。

相关操作

- 编辑托管视图
  a. 在待编辑托管视图所在行“操作”列，单击“编辑”。
  b. 在弹出的编辑托管视图中，修改托管视图参数后，单击“确定”。
- 删除托管视图
  当确认需要删除托管空间及托管信息，可执行删除托管视图操作。
  a. 在待删除视图所在行“操作”列，单击“删除”。
  b. 在弹出确认框中，单击“确认”。

5.4.2 管理托管

操作场景

空间托管页面中，可以管理托管视图、我纳管的和纳管我的。

- **托管视图**：查看已创建的托管视图及其详细信息，支持查看、编辑、修改、删除或批量删除托管视图。
- **我纳管的**：呈现有哪些工作空间托管在我创建的托管视图中，支持查看我纳管的任务以及任务参数，管理我纳管的任务（包括接收、拒绝、解除、删除）。
- **纳管我的**：呈现我的工作空间被哪些托管视图纳管着，支持查看纳管我的托管视图相关参数，支持修改已接收的托管任务、撤回已接收的托管任务、重申托管关系、解除托管关系、删除托管任务。

托管视图

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间托管”，进入空间托管管理页面。

步骤 4 在托管页面中，选择“托管视图”页签，进入托管视图页面。

步骤 5 在托管视图页面中，可以查看和管理托管视图。

- 查看托管视图

表 5-10 查看托管视图

参数名称	参数说明
托管视图名称	托管视图的名称。
区域	托管视图所在的区域。
绑定空间名称/ID	托管视图绑定的工作空间的名称和 ID 信息。
纳管空间数量	托管视图中绑定的工作空间数量。
创建时间	托管视图的创建时间。
描述	托管视图的描述信息。
操作	可以对托管视图进行编辑、删除操作。

- 编辑托管视图
  a. 在待编辑托管视图所在行“操作”列，单击“编辑”。
  b. 在弹出的编辑托管视图中，修改托管视图参数后，单击“确定”。
- 删除托管视图
  a. 在待删除视图所在行“操作”列，单击“删除”。
     如果需要删除多个视图，可以在列表中勾选需要删除的视图，并单击列表上方“批量删除”。
  b. 在弹出确认框中，单击“确认”。

----结束

我纳管的

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间托管”，进入空间托管管理页面。

步骤 4 在托管页面中，选择“我纳管的”页签，进入我纳管的页面。

步骤 5 在我纳管的页面中，可以查看和管理我纳管的任务。

- 查看我纳管的

表 5-11 查看我纳管的

参数名称	参数说明
托管名称	托管的名称。
名称/ID	被我的托管视图纳管的工作空间的名称和 ID。
托管视图名称	托管视图的名称。
发起方式	托管任务的发起方式。 • 当前租户：使用租户账号登录态势感知（专业版），选择租户账号进行托管的场景。 • 组织：使用组织管理员账号或者委托管理员账号登录态势感知（专业版），选择组织下的账号进行托管场景。
托管状态	托管任务的托管状态。 • 已接收 • 待接收 • 已拒绝 • 已解除 • 已撤回
选中状态	托管任务的选中状态。
托管时长	托管任务的时长。
托管时间	托管任务的开始时间。
托管策略	托管任务使用的策略。
操作	可以对我纳管的任务进行接收、删除操作。

- 管理我纳管的

表 5-12 管理我纳管的

操作	说明
接收托管	1. 在待接收托管所在行“操作”列，单击“接收”。 如果需要接收多个托管关系，可以在列表中勾选需要接收的托管关系，并单击列表上方“批量接收”。 2. 在弹出确认框中，单击“确认”。 **托管状态为已接收、已解除和已撤回的托管任务，不支持接收托管操作。**

操作	说明
拒绝托管关系	1. 在待拒绝托管所在行“操作”列，单击“拒绝”。 如果需要拒绝多个托管关系，可以在列表中勾选需要拒绝的托管关系，并单击列表上方“批量拒绝”。 2. 在弹出确认框中，单击“确认”。 **托管状态为已接收、已拒绝、已解除和已撤回的托管任务，不支持拒绝托管关系操作。**
解除托管关系	1. 在待解除托管所在行“操作”列，单击“更多 > 解除”。 如果需要解除多个托管关系，可以在列表中勾选需要解除的托管关系，并单击列表上方“批量解除”。 2. 在弹出确认框中，单击“确认”。
删除托管任务	1. 在待删除托管所在行“操作”列，单击“更多 > 删除”。 如果需要删除多个托管，可以在列表中勾选需要删除的托管，并单击列表上方“批量删除”。 2. 在弹出确认框中，单击“确认”。 **托管状态为已接收的托管任务，不支持删除托管任务操作。**

----结束

纳管我的

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间托管”，进入空间托管管理页面。

步骤 4 在托管页面中，选择“纳管我的”页签，进入纳管我的页面。

步骤 5 在纳管我的页面中，可以查看和管理纳管我的。

- 查看纳管我的

表 5-13 查看纳管我的

参数名称	参数说明
托管名称	托管视图的名称。
名称/ID	我方工作空间的名称和 ID 信息。
受托管方	工作空间的受托管方信息。
发起方式	托管任务的发起方式。
托管视图名称	托管任务所属的托管视图的名称。

参数名称	参数说明
托管时长	托管任务的时长。
托管状态	托管任务的托管状态。
托管时间	托管任务的开始时间。
托管策略	托管任务的策略。
操作	可以对托管关系进行修改、删除等操作。

- 管理纳管我的

表 5-14 管理纳管我的

操作	说明
修改托管任务	1. 在待修改托管所在行“操作”列，单击“修改”。 2. 在弹出编辑页面中修改托管信息。 3. 单击“确认”。 **托管状态为已接收和已解除的托管任务，不支持修改操作。**
撤回已接收的托管任务	1. 在待撤回托管所在行“操作”列，单击“撤回”。 如果需要撤回多个解除关系，可以在列表中勾选需要撤回的托管关系，并单击列表上方“批量撤回”。 2. 在弹出确认框中，单击“确认”。 **托管状态为已拒绝、已解除和已撤回的托管任务，不支持撤回操作。**
重申托管关系	如果受纳管方拒绝了托管，可发起再次申请操作。 1. 在待重申托管所在行“操作”列，单击“更多 > 重申”。 2. 在弹出确认框中，单击“确认”。 **托管状态为已接收、待接收和已撤回的托管任务，不支持重申操作。**
解除托管关系	1. 在待解除托管所在行“操作”列，单击“更多 > 解除”。 如果需要解除多个托管关系，可以在列表中勾选需要解除的托管关系，并单击列表上方“批量解除”。 2. 在弹出确认框中，单击“确认”。
删除托管任务	1. 在待删除托管所在行“操作”列，单击“更多 > 删除”。 如果需要删除多个托管，可以在列表中勾选需要删除的托管，并单击列表上方“批量删除”。 2. 在弹出确认框中，单击“确认”。 **托管状态为已接收的托管任务，不支持删除操作。**

----结束

6 查看已购资源

操作场景

在态势感知（专业版）的已购资源中可统一呈现当前账号已经申请的资源，方便统一管理已购资源。

查看已购资源

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“已购资源”，进入已购资源管理页面。

步骤 4 在已购资源页面查看详细信息。

表 6-1 查看已购资源信息

参数名称	参数说明
已开通区域/总区域	当前账号已开通态势感知（专业版）的区域以及总区域数量。
可升级	当前账号所有区域的所有已购版本中，可以升级的资源数量。
将到期版本	当前账号所有区域的所有已购的版本和增值包中，即将到期的规格及增值包数量。
总配额	当前账号所有区域中，已购买的总配额数量。
已购资源列表	各区域具体购买态势感知（专业版）资源的详细情况。 如果版本或区域较多，可以使用搜索功能，通过区域、版本或订单号进行搜索，查看指定资源购买信息。

----结束

7 态势感知

7.1 查看态势总览

“态势总览”页面实时呈现当前工作空间中资源的整体安全评估状况，包括资产的安全评估结果、安全监控和安全趋势等信息，可以全面了解资产的安全情况。

态势感知（专业版）支持查看所有工作空间的整体安全评估结果，以及单个工作空间的安全评估结果，其中：

- 总览：总览页面实时呈现态势感知（专业版）所有工作空间的整体安全评估结果，查看方法请参见查看总览。
- 态势总览：目标工作空间的“态势感知 > 态势总览”页面呈现当前单个工作空间的安全评估结果，查看方法请参见本章节操作步骤。

查看态势总览

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“态势感知 > 态势总览”，进入态势总览页面。

步骤 5 在态势总览页面查看您的资产安全总览情况，并进行相关操作。“态势总览”分为以下几个板块：

- 安全评分
- 安全监控
- 安全趋势

各个板块数据统计周期及更新频率如下表所示：

表 7-1 态势总览

参数名称	统计周期	更新频率	说明
安全评分	实时	• 每天 2:00 自动更新 • 随手动单击“重新检测”更新而更新	根据是否开启各安全服务防护、未处理的配置问题等级及个数、未处理的漏洞等级及个数、未处理的威胁事件等级及个数等计算而来。 详细评分信息请参见安全评分。
威胁告警	近 7 天	每 5 分钟	当前工作空间内，“威胁管理 > 告警管理”中的告警总和。 详细信息请参见表 7-2 中“威胁告警”的说明。
漏洞	近 7 天	每 5 分钟	当前工作空间内，“风险预防 > 漏洞管理”中的漏洞总和。 详细信息请参见表 7-2 中“漏洞”的说明。
合规检查	实时	每 5 分钟	当前工作空间内，“风险预防 > 基线检查”中的问题总和。 详细信息请参见表 7-2 中“合规检查”的说明。
安全趋势	近 7 天	每 5 分钟	“安全趋势”板块展示**近 7 天**内您的整体资产安全健康得分的趋势图。

----结束

安全评分

“安全评分”板块根据不同版本的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况。

- 安全评分每天凌晨 2:00 自动更新，也支持通过单击“重新检测”来进行实时更新。
- 分值范围为 0～100，分值越大表示风险越小，资产更安全，安全分值详细说明请参见安全评分。
- 分值环形图不同颜色表示不同威胁等级。例如，黄色对应“中危”。
- 单击“立即处理”，系统右侧弹出“安全风险处理”页面，您可根据该页面的提示，参考对应的帮助文档或直接对风险进行处理。
  - 安全风险处理页面中包含所有需要您尽快处理的安全风险和威胁，分为“威胁告警”、“漏洞”、“合规检查”三大类别。
  - “安全风险处理”页面中显示的数据为最近/最新检测后的数据结果，“告警管理”、“漏洞管理”、“基线检查”页面（单击“前往处理”，进入该页面）显示

的是所有检测时间的各类数据详情，因此，安全风险处理页面的数据总数≤告警管理或漏洞管理页面的数据总数。

- **处理安全风险：**
  i. 在“安全评分”栏中，单击“立即处理”，系统右侧弹出“安全风险处理”页面。
  ii. 在“安全风险处理”页面中，单击“前往处理”，进入“告警管理”、“漏洞管理”或“基线检查”页面。
  iii. 对风险告警、漏洞或基线检查项目进行处理。

- 资产风险修复，并手动刷新告警事件状态后，安全评分实时更新。资产安全风险修复后，也可以直接单击“重新检测”，重新检测资产并进行评分。

资产安全风险修复后，为降低安全评分的风险等级，需手动忽略或处理告警事件，刷新告警列表中告警事件状态。

- 安全评分显示为历史扫描结果，**非实时**数据，如需获取最新数据及评分，可单击“重新检测”，获取最近的数据。

安全监控

“安全监控”板块展示待处理**威胁告警**、待修复**漏洞**、**合规检查**问题的安全监控统计数据。

表 7-2 安全监控参数说明

参数名称	参数说明
威胁告警	呈现最**近 7 天内**当前工作空间中未处理威胁告警，可快速了解资产遭受的威胁告警类型和数量，呈现威胁告警的统计结果。统计信息更新频率为每 5 分钟更新一次。 • 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了入侵事件，建议您立即查看告警事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看告警事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该告警事件的详情。 • 单击威胁告警模块，系统将列表实时呈现**近 7 天内** TOP5 的威胁告警事件，可快速查看威胁告警详情，监控威胁告警状况。 – 呈现近 7 天 TOP5 的威胁告警事件的信息，包括威胁告警名称、告警等级、资产名称、告警发现时间。 – 如果列表显示内容为空，表示近 7 天无威胁告警事件。 – 单击“查看更多”，可跳转到“告警管理”页面，查看更多的威胁告警信息，并可自定义过滤条件查询告警信息。
漏洞	展示当前工作空间中您资产中 TOP5 漏洞类型，以及**近 7 天内**还未修复的漏洞总数和不同漏洞风险等级对应的数量。统计信息更

参数名称	参数说明
	新频率为每 5 分钟更新一次。 • 此处严重等级含义如下： – 高危：即高危风险，表示资产中检测到了漏洞事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 中危：即中危风险，表示资产中检测到了可疑的异常事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 其他：即其他类型（低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该漏洞的详情。 • 单击漏洞模块中的“漏洞类型 Top5”栏，系统将呈现 TOP5（根据某个漏洞影响的主机数量进行排序）的漏洞类型。 – 此处的 TOP 等级是根据某个漏洞影响的主机数量进行排序，受影响主机数量越多排名越靠前。 – 要求 **Linux** 系统主机中 Agent 版本为 3.2.9.30 及以上，**Windows** 系统主机中 Agent 版本为 4.0.19.30 及以上。更多信息请参见主机 Agent 版本说明和升级主机 Agent。 • 单击漏洞模块中的“实时监控最新漏洞风险事件 Top5”栏，系统将列表实时呈现**近 7 天内** TOP5 的漏洞事件，可快速查看漏洞详情。 – 呈现当日最新 TOP5 漏洞事件详情，包括漏洞名称、漏洞等级、资产名称、漏洞发现时间。 – 如果列表显示内容为空，表示当日无漏洞事件。 – 单击“查看更多”，可跳转到“漏洞管理”页面，查看更多的漏洞信息，并可自定义过滤条件查询漏洞信息。
合规检查	展示当前工作空间中您资产中存在的合规风险总数量和不同危险等级的合规检查风险对应的数量。统计信息更新频率为每 5 分钟更新一次。仅统计近 30 天的合规检查结果。 • 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了入侵事件，建议您立即查看合规异常事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看合规检查事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该合规检查项目的详情。 • 单击合规检查异常模块，系统将列表实时呈现 TOP5 的合规检查异常事件，可快速查看合规检查详情。 – 呈现最近一次合规检查中 TOP 的合规异常事件详情，包括合规检查项目名称、等级、受影响资产数量、发现时间。 – 如果列表显示内容为空，表示无合规异常事件。 – 单击“查看更多”，可跳转到“基线检查”页面，查看更多的合规异常信息，并可自定义过滤条件查询合规检查信息。

安全趋势

“安全趋势”板块展示**近 7 天**内您的整体资产安全健康得分的趋势图。更新频率为每 5 分钟更新一次。

7.2 安全报告

7.2.1 创建或复制安全报告

操作场景

态势感知（专业版）提供安全报告功能。您可以通过安全报告，及时掌握资产的安全状况数据。

本章节主要介绍如何新建安全报告，以及如何通过复制已创建的报告快速创建报告。

创建安全报告

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“态势感知 > 安全报告”，进入安全报告页面。

步骤 5 在安全报告页面中单击按钮，进入配置报告基本信息页面。

步骤 6 配置报告基本信息。

表 7-3 报告基本信息参数说明

参数名称	参数说明
报告名称	自定义报告名称。 • 报告名称由字母、数字、汉字、下划线和连接符组成。 • 长度为 1~30 个字符。

参数名称	参数说明
报告类型	选择报告类型。 • 日报：默认统计前一天 00:00:00~23:59:59 的安全信息。 • 周报：默认统计上一周安全信息，上周一 00:00:00 到上周日 23:59:59。 • 月报：默认统计上一月安全信息，上月第一天 00:00:00 到上月最后一天 23:59:59。 • 自定义：自定义选择时间范围。
统计周期	如果报告类型选择为日报、周报、月报时，将根据选择的报告类型自动生成报告的周期。 如果报告类型选择为自定义，则可以设置根据需要设置安全报告统计周期。

步骤 7 报告基本信息配置完成后，单击右下角“下一步:报告模板选择”，进入报告模板选择页面。

步骤 8 在“报告模板选择”页面的左侧已有报告布局中，根据报告类型选择报告模板。选择完成后，可以在右侧页面中预览报告样式。

如果前一步基本信息配置中选择的“报告类型”为“日报”时，此处请选择日报布局；

如果前一步基本信息配置中选择的“报告类型”为“周报”，此处请选择周报布局；

如果前一步基本信息配置中选择的“报告类型”为“月报”，此处请选择月报布局。

步骤 9 单击右下角“完成”，返回安全报告管理页面，即可查看创建的安全报告。

步骤 10 此外，在安全报告管理页面，可以下载、分享、编辑、复制、删除安全报告。

- 下载报告：在安全报告管理页面，单击待下载报告右下角“更多”按钮，在功能下拉菜单中单击“下载”，弹出报告预览页面，单击预览页面上方的“下载”按钮，并在弹出的对话框中，选择报告格式后，单击“确定”。系统将自动下载对应格式的报告到本地。
- 分享报告：在安全报告管理页面，单击待分享报告右下角“更多”按钮，在功能下拉菜单中单击“分享”，并在弹出的对话框中，单击复制按钮，进行分享。

  分享完成后，可以单击“确定”，关闭对话框。
- 编辑报告：在安全报告管理页面，单击待编辑报告下方的“编辑”按钮，更多详细操作指导请参见管理安全报告。
- 复制报告：在安全报告管理页面，单击待复制报告下方的“复制”按钮，更多详细操作指导请参见复制安全报告。
- 删除报告：在安全报告管理页面，单击待删除报告下方的“删除”按钮，更多详细操作指导请参见管理安全报告。

----结束

复制安全报告

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“态势感知 > 安全报告”，进入安全报告页面。

步骤 5 在已创建的目标安全报告模块，单击“复制”，跳转到报告基本信息配置页面。

步骤 6 修改报告基本信息。

步骤 7 单击右下角“下一步：报告模板选择”，进入报告模板选择配置页面，修改报告内容。

步骤 8 单击右下角“完成”，返回安全报告管理页面，即可查看复制的安全报告。

----结束

相关操作

- 查看安全报告
- 下载安全报告
- 管理安全报告：支持启用、停用、编辑、删除安全报告操作。

7.2.2 查看安全报告

操作场景

本章节介绍如何查看已创建的安全报告及其展示的信息。

查看安全报告

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“态势感知 > 安全报告”，进入安全报告页面。

步骤 5 单击目标报告所在模块，进入报告详情页面。

在报告详情页面，可以预览当前安全报告的详细信息。

----结束

模板**日报**展示内容

表 7-4 模板日报展示内容

参数模块	参数说明
统计周期	日报默认统计周期为前一天 00:00:00~23:59:59。
统计类型	报告类型。
生成时间	报告生成的时间。
安全评分	根据您的态势感知（专业版）的威胁检测能力，评估前一天 00:00:00~23:59:59 整体资产安全、基线配置、威胁告警、安全漏洞四个维度综合的健康得分，可以快速了解资产的整体安全状况。
基线检查	展示**最近一次**基线检查的统计情况，包含以下信息： • 总检查项：最近一次基线检查项目总数量 • 不合规项：最近一次基线检查不合规检查项目数量 • 未修复项：最近一次基线检查未修复的项目数量
安全漏洞	展示接入云服务**前一天**的漏洞统计情况，包含以下信息： • 漏洞总数量 • 未修复漏洞数量
安全响应	展示**前一天**安全响应情况，包含以下信息： • 告警总数 • 未处理告警 • 闭环率：自动化闭环率，闭环率=前一天由态势感知（专业版）自动化响应剧本关闭的告警数/前一天关闭的告警总数。
资产安全	展示当前资产安全情况，包含以下信息： • 当前资产总数量 • 当前存在风险的资产数量
安全分析	展示**前一天**安全分析统计情况，包含以下信息： • 前一天安全日志总流量 • 安全日志模型数量
策略覆盖	展示当前安全产品策略覆盖情况，包含以下信息： • 覆盖实例：受安全产品保护的实例数量（=受保护 ECS 数量+受保护 WAF 实例数量） • 覆盖率：主机安全覆盖率（=受保护 ECS 数量/全部 ECS 数量）
资产风险	展示**前一天**资产安全状况，包含以下信息：

参数模块	参数说明
	• 前一天受攻击资产数量 • 前一天未防护资产数 • 前一天脆弱性资产数 • 截止昨天为止的**近 7 天**的资产变化趋势 • 前一天资产类型防护率
威胁态势	展示**前一天**资产的威胁态势情况，包含以下信息： • 前一天 DDoS 攻击次数 • 前一天网络攻击次数 • 前一天应用攻击次数 • 前一天主机攻击次数 • 前一天 DDoS 攻击次数变化趋势 • 前一天网络/主机攻击次数趋势变化 • 前一天 WAF 巡检情况（WAF 请求总量、WAF 告警量、WAF 拦截次数）变化趋势 • 前一天 TOP5 网络攻击类型统计情况 • 前一天 TOP5 应用攻击类型统计情况 • 前一天 TOP5 主机攻击类型统计情况 • 前一天 TOP5 应用攻击源分布情况 • 前一天 TOP5 应用攻击目的分布情况 • 前一天 TOP5 主机告警分布情况 • 前一天 TOP5 网络攻击源分布情况
日志分析	展示**前一天**日志分析的情况，包含以下信息： • 前一天日志源数量 • 前一天日志索引数量 • 前一天日志接收总数 • 前一天日志存储总量 • 截至昨天为止的**近 7 天**的日志存储量变化趋势 • 截至昨天为止的**近 7 天**的 TOP3 日志源接入流量统计情况 • 前一天 TOP10 模型检测告警统计数量

参数模块	参数说明
安全响应（详细信息）	展示**前一天**安全响应的情况，包含以下信息： • 前一天未处理告警数量 • 前一天未处理事件数量 • 前一天未处理漏洞数量 • 前一天未处理基线数量 • 前一天威胁告警分布情况及数量 • 前一天 TOP5 入侵事件分布情况及数量 • 前一天 TOP5 应急响应事件统计 • 前一天 TOP20 威胁告警处置列表

模板**周报**展示内容

表 7-5 模板周报展示内容

参数模块	参数说明
统计周期	周报默认统计周期为上周一 00:00:00 到上周日 23:59:59。
统计类型	报告的类型
生成时间	生成报告的时间
安全评分	根据您的态势感知（专业版）的威胁检测能力，评估上周最后一天最新的整体资产安全、基线配置、威胁告警、安全漏洞四个维度综合的健康得分，可以快速了解资产的整体安全状况。
基线检查	展示上周最后一次基线检查的统计情况，包含以下信息： • 总检查项：最近一次基线检查项目总数量 • 不合规项：最近一次基线检查不合规检查项目数量 • 未修复项：最近一次基线检查未修复的项目数量
安全漏洞	展示接入云服务上周日最新的漏洞统计情况，包含以下信息： • 漏洞总数量 • 未修复漏洞数量

参数模块	参数说明
安全响应	展示上周一整周安全响应情况，包含以下信息： • 告警总数 • 未处理告警 • 闭环率：自动化闭环率，闭环率=前一天由态势感知（专业版）自动化响应剧本关闭的告警数/前一天关闭的告警总数。
资产安全	展示上周最后一天最新的资产安全情况，包含以下信息： • 当前资产总数量 • 当前存在风险的资产数量
安全分析	展示安全分析统计情况，包含以下信息： • 上周一整周安全日志总流量 • 上周最后一天的安全日志模型数量
策略覆盖	展示上周最后一天最新的安全产品覆盖情况，包含以下信息： • 覆盖实例：受安全产品保护的实例数量（=受保护 ECS 数量+受保护 WAF 实例数量） • 覆盖率：主机安全覆盖率（=受保护 ECS 数量/全部 ECS 数量）
资产风险	展示上周最后一天最新的资产安全状况，包含以下信息： • 受攻击资产数量以及较月报统计月的上周的变化 • 未防护资产数以及较月报统计月的上周的变化 • 脆弱性资产数以及较月报统计月的上周的变化 • 上周的资产变化趋势 • 资产类型防护率

参数模块	参数说明
威胁态势	展示上周最后一天最新的资产的威胁态势情况，包含以下信息： • DDoS 攻击次数 • 网络攻击次数 • 应用攻击次数 • 主机攻击次数 • DDoS 攻击次数的变化趋势 • 网络/主机攻击次数趋势变化 • WAF 巡检情况 • TOP5 网络攻击类型统计情况 • TOP5 应用攻击类型统计情况 • TOP5 主机攻击类型统计情况 • TOP5 应用攻击源分布情况 • TOP5 应用攻击目的分布情况 • TOP5 主机告警分布情况 • TOP5 网络攻击源分布情况
日志分析	展示上周一整周日志分析的情况，包含以下信息： • 日志源数量 • 日志索引数量 • 日志接收总数 • 日志存储总量 • 日志存储量变化趋势 • TOP3 日志源接入量统计情况 • TOP10 模型检测告警统计数量
安全响应（详细信息）	展示上周一整周安全响应的情况，包含以下信息： • 未处理告警数量 • 未处理事件数量 • 未处理漏洞数量 • 未处理基线数量 • 威胁告警分布情况及数量 • TOP5 入侵事件分布情况及数量 • TOP5 应急响应事件统计情况 • TOP20 威胁告警处置列表

模板月报展示内容

表 7-6 模板月报展示内容

参数模块	参数说明
统计周期	月报默认统计周期为上一个月整月。
统计类型	报告的类型
生成时间	生成报告的时间
安全评分	根据您的态势感知（专业版）的威胁检测能力，评估上一个月最后一天最新的整体资产安全、基线配置、威胁告警、安全漏洞四个维度综合的健康得分，可以快速了解资产的整体安全状况。
基线检查	展示上一个月最后一次基线检查的统计情况，包含以下信息： • 总检查项：最近一次基线检查项目总数量 • 不合规项：最近一次基线检查不合规检查项目数量 • 未修复项：最近一次基线检查未修复的项目数量
安全漏洞	展示接入云服务上一个月最后一天最新的漏洞统计情况，包含以下信息： • 总漏洞数量 • 未修复漏洞数量
安全响应（总览）	展示上一个月整月安全响应情况，包含以下信息： • 告警总数 • 未处理告警数 • 闭环率：自动化闭环率，闭环率=前一天由态势感知（专业版）自动化响应剧本关闭的告警数/前一天关闭的告警总数。
资产安全	展示上一个月最后一天最新的资产安全情况，包含以下信息： • 资产总数量 • 存在风险的资产数量
安全分析	展示安全分析统计情况，包含以下信息： • 上一个月整月安全日志总流量 • 上一个月最后一天的安全日志模型数量

参数模块	参数说明
策略覆盖	展示上一个月最后一天最新的安全产品覆盖情况，包含以下信息： • 受安全产品保护的实例数量（=受保护 ECS 数量+受保护 WAF 实例数量） • 覆盖率（=受保护 ECS 数量/全部 ECS 数量）
资产风险	展示上一个月最后一天最新的资产安全状况，包含以下信息： • 受攻击资产数量以及较月报统计月的上一月的变化 • 未防护资产数以及较月报统计月的上一月的变化 • 脆弱性资产数以及较月报统计月的上一月的变化 • 上一个月的资产变化趋势 • 资产类型防护率
威胁态势	展示上一个月最后一天最新的资产的威胁态势情况，包含以下信息： • DDoS 攻击次数 • 网络攻击次数 • 应用攻击次数 • 主机攻击次数 • DDoS 攻击次数的变化趋势 • 网络/主机攻击次数趋势变化 • WAF 巡检情况 • TOP5 网络攻击类型统计情况 • TOP5 应用攻击类型统计情况 • TOP5 主机攻击类型统计情况 • TOP5 应用攻击源分布情况 • TOP5 应用攻击目的分布情况 • TOP5 主机告警分布情况 • TOP5 网络攻击源分布情况
日志分析	展示上一个月整月日志分析的情况，包含以下信息： • 日志源数量 • 日志索引数量 • 日志接收总数 • 日志存储总量 • 日志存储量变化趋势 • TOP3 日志源接入量统计情况 • TOP10 模型检测告警统计数量

参数模块	参数说明
安全响应（详细信息）	展示上一个月整月安全响应的情况，包含以下信息： • 已处理告警数量 • 已处理事件数量 • 已处理漏洞数量 • 已处理基线数量 • 威胁告警分布情况及数量 • TOP5 入侵事件分布情况及数量 • TOP5 应急响应统计情况 • TOP20 威胁告警处理情况 • 未处理告警数量 • 未处理事件数量 • 未处理漏洞数量 • 未处理基线数量 • 威胁告警分布情况及数量 • TOP5 入侵事件分布情况及数量 • TOP5 应急响应事件统计情况 • TOP20 威胁告警处理情况

相关操作

- 下载安全报告
- 管理安全报告：支持启用、停用、编辑、删除安全报告操作。

7.2.3 下载安全报告

操作场景

态势感知（专业版）创建并生成报告后，可以将报告下载至本地。

本章节将介绍如何下载报告至本地。

下载安全报告

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“态势感知 > 安全报告”，进入安全报告页面。

步骤 5 在安全报告管理页面，单击待下载报告右下角“更多”按钮，在功能下拉菜单中单击“下载”。

步骤 6 弹出报告预览页面，单击预览页面上方的“下载”按钮，并在弹出的对话框中，选择报告格式后，单击“确定”。系统将自动下载对应格式的报告到本地。

----结束

7.2.4 管理安全报告

操作场景

本章节介绍如何管理安全报告，包括启用、停用、编辑、删除操作。

管理安全报告

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“态势感知 > 安全报告”，进入安全报告页面。

步骤 5 管理安全报告。

表 7-7 管理安全报告

操作名称	执行步骤
启用/停用安全报告	在安全报告页面中，单击目标报告模块中的未启用或启用按钮。 • 安全报告状态更新为启用，则表示启用成功。 • 安全报告状态更新为未启用，则表示停用成功。
编辑安全报告	1. 在安全报告页面中，单击目标报告中的“编辑”按钮，跳转到报告基本信息配置页面。 2.（可选）编辑报告基本信息。 3. 单击“下一步：报告选择”，跳转到报告选择页面。 4.（可选）勾选报告布局。 5. 单击右上角“完成”。
删除安全报告	1. 在安全报告页面中，单击目标报告中的“删除”，弹出删除报告确认窗口。 2. 单击“确定”。

操作名称	执行步骤
下载安全报告	1. 在安全报告管理页面，单击待下载报告右下角“更多”按钮，在功能下拉菜单中单击“下载”，弹出报告预览页面。 2. 单击预览页面上方的“下载”按钮，并在弹出的对话框中，选择报告格式后，单击“确定”。系统将自动下载对应格式的报告到本地。
分享安全报告	1. 在安全报告管理页面，单击待分享报告右下角“更多”按钮，在功能下拉菜单中单击“分享”。 2. 在弹出的对话框中，单击复制按钮，进行分享。 3. 分享完成后，可以单击“确定”，关闭对话框。

----结束

7.3 任务中心

7.3.1 查看待办任务

操作场景

待办列表呈现当前需要您进行处理的任务，本章节主要介绍如何查看待办任务列表。

查看待办任务

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“态势感知 > 任务中心”，默认进入我的待办页面。

步骤 5 在待办任务列表中查看待办任务详情。

表 7-8 待办任务参数说明

参数名称	参数说明
任务名称	该条任务的名称。

参数名称	参数说明
业务类型	任务属于的类型。 • 流程发布 • 剧本发布 • 剧本-节点审核
关联对象	对应的剧本/流程名称。
创建人	创建任务的用户。
审核人	该剧本/流程的审核人员。
备注	任务的备注信息。
创建时间	该剧本/流程的创建时间。
更新时间	该剧本/流程的最近一次更新时间。
到期时间	该条任务的到期时间。
操作	对待办任务进行审批操作。

----结束

7.3.2 处理待办任务

操作场景

当剧本/流程任务执行到某一节点时，任务暂停需人工处理，剧本/流程任务才能继续执行。

本章节主要介绍如何处理待办任务。

前提条件

已触发剧本/流程任务，且任务流程需人工处理。

处理待办任务

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“态势感知 > 任务中心”，默认进入我的待办页面。

步骤 5 在目标待办任务所在行“操作”列，单击“审批”。

不同业务类型，审批方式不同：

- 剧本发布：右侧弹出“剧本发布”界面，填写“审核意见”，并根据页面提示进行审批。
- 流程发布：右侧弹出“流程发布”界面，填写“审核意见”，并根据页面提示进行审批。
- 剧本-节点审核：右侧弹出“剧本-节点审核”界面，可选择“继续执行”或“终止”。

步骤 6 审批完成后，在左侧导航栏选择“态势感知 > 任务中心”，选择“已处理”页签，进入已处理任务页面，查看已处理任务。

----结束

7.3.3 查看已处理任务

操作场景

已处理列表呈现当前您已处理的任务，本章节主要介绍如何已处理的任务列表。

查看已处理任务

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“态势感知 > 任务中心”，进入任务中心后，选择“已处理”页签，进入已处理任务页面。

步骤 5 在已处理任务列表中查看已处理任务详情。

表 7-9 已处理任务参数说明

参数名称	参数说明
任务名称	该条任务的名称。
业务类型	任务属于的类型。 • 流程发布 • 剧本发布 • 剧本-节点审核
关联对象	对应的剧本/流程名称。
创建人	创建任务的用户。
备注	该条任务的备注信息。

参数名称	参数说明
审核人	该剧本/流程的审核人员。
审核意见	该条任务的审核意见。
描述	该条任务的描述信息。
创建时间	该剧本/流程的创建时间。
更新时间	该剧本/流程的最近一次更新时间。
到期时间	该条任务的到期时间。

----结束

7.4 AI 风险概览

操作场景

AI 风险概览实时为您呈现大模型合规态势，支持大模型的数据语料风险运营、推理业务风险运营和环境安全风险运营，实时呈现大模型的风险概览，助您识别大模型风险和潜在威胁。通过控制台“AI 风险概览”为您呈现**推理安全**、**语料安全**、**环境安全**的风险态势。

- 推理安全：基于 WAF 攻击日志和访问日志，分析呈现大模型接口的调用请求次数、调用请求命中防护策略数、以及命中防护策略数排名前 5 的推理模型域名和数量、提示词注入的攻击分布、推理模型攻击类型分布等。
- 语料安全：基于 DSC 告警日志，分析呈现大模型中的语料风险类别和数量、TOP5 语料风险资产分布等。
- 环境安全：基于态势感知（专业版）基线检查、漏洞管理、告警管理功能，分析呈现当前工作空间的 TOP5 合规检查风险、TOP5 漏洞风险、TOP5 告警和最近攻击列表。

前提条件

- **推理安全**依赖 Web 应用防火墙 WAF 服务，在使用 AI 风险概览的推理安全功能模块前需要确保 Web 应用防火墙 WAF 服务在有效使用期内，且**仅 WAF 云模式支持**。
- **语料安全**依赖数据安全中心 DSC 服务，在使用 AI 风险概览的语料安全功能模块前需要确保大模型数据安全防护在有效使用期内。
- 已经在态势感知（专业版）控制台接入“WAF 攻击日志”，“WAF 访问日志”和“DSC 告警日志”。接入云服务日志请参见接入日志数据。
- 仅态势感知（专业版）专业版支持。

查看 AI 风险概览

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版） ”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“态势感知 >AI 风险概览”，进入 AI 风险概览页面。

步骤 5 在 AI 风险概览页面，可查看以下信息：

表 7-10 AI 风险概览界面参数说明

模块	参数名称	参数说明
统计时间	统计时间	支持用户选择或自定义查看的概览的时间，支持选择范围如下： • 近 24 小时 • 近 3 天 • 近 7 天 • 近 30 天 • 自定义：用户自定义起止时间范围。
推理安全	推理安全风险汇总	推理安全模块呈现所设置的统计时间周期内大模型推理业务风险运营的结果： • 请求总数：WAF 请求日志中大模型接口调用的请求次数总和。 • 命中防护策略数：WAF 攻击日志中告警类型为提示词注入攻击、提示词内容合规、响应内容合规数量总和。 • 提示词注入攻击次数：WAF 攻击日志中提示词攻击数量总和。 • 提示词内容合规次数：WAF 攻击日志中提示词内容合规数量总和 • 响应内容合规次数：WAF 攻击日志中响应内容合规次数总和。
	请求趋势	请求趋势呈现“总请求数”和“命中防护策略数”指标随时间的变化趋势，实时更新。其中 • 总请求数：WAF 请求日志中大模型接口调用的请求数量。 • 命中防护策略数：WAF 攻击日志中告警类型为提示词注入攻击、提示词内容合规、响应内容合规数量总和。

模块	参数名称	参数说明
	TOP5 资产风险分布	WAF 攻击日志中，根据推理模型域名分组求和，展示命中防护策略数中排名前 5 的推理模型域名及数量。
	提示词注入攻击分布	WAF 攻击日志中提示词注入攻击类型为越狱攻击、提示词泄露、角色扮演、不安全的指令话题、不安全的观点、反向诱导、政治敏感、合规敏感、个人隐私数据的分类数量统计。
	大模型攻击类型分布	WAF 攻击日志中告警类型为提示词注入、提示词内容合规、响应内容合规三种类型的告警分类数量统计。
语料安全	TOP5 语料资产风险分布	DSC 攻击日志中根据上报告警的 OBS 桶 ID 分组求和，展示前 5 的桶名及数量。
	文本风险类别	DSC 攻击日志中文本风险类型为个人隐私敏感、内容合规敏感类型、来源或版权不合规三种类型的分类数量统计。
环境安全	TOP5 合规检查	按照合规检查受影响资产数量排序，呈现 TOP5 影响资产数最多的 5 个不合规风险项。
	TOP5 漏洞风险	按照漏洞的风险等级排序展示用户设定的 AI 风险概览“统计时间”内的 TOP5 漏洞，若漏洞的风险等级相同则按照漏洞名称排序。
	TOP5 告警	按照告警的发现时间展示最近发生的 5 个告警。
	最近攻击清单	基于用户设定的 AI 风险概览“统计时间”展示攻击列表。

----结束

8 资产管理

8.1 资产管理概述

态势感知（专业版）支持管理云上资产和云外资产，可以查看当前工作空间所在region中所有资源的安全状态统计信息，帮助您快速定位安全风险问题并提供解决方案。

- **云上资产**：云上资产，如弹性云服务器（Elastic Cloud Server，ECS）、Web应用防火墙（Web Application Firewall，WAF）、虚拟私有云（Virtual Private Cloud，VPC）。
- **云外资产**：非云上资产，如本地服务器、IDC服务器或第三方云厂商的服务器等。

管理云上资产

- 设置资产订阅：同步资产信息，资产订阅仅支持订阅和同步云上资产。
- 查看资产信息：支持查看所有资产信息，可以查看资产的名称、类型、防护状态等信息。
- 导入或导出资产：支持导入或导出资产的信息。
- 编辑或删除资产：支持对资产的部门、业务系统、责任人进行编辑；**云上资产仅支持编辑，不支持删除**。

管理云外资产

- 查看资产信息：支持查看所有资产信息，可以查看资产的名称、类型、防护状态等信息。
- 导入或导出资产：支持导入或导出资产的信息。
- 编辑或删除资产：支持对资产的部门、业务系统、责任人进行编辑；若不再需要态势感知（专业版）资产管理页面展示某个或某些云下导入的资产信息时可以删除资产。**仅支持云外资产删除**。

管理云上资产和云外资产的区别

- 云上资产支持资产订阅，而云外资产不支持资产订阅且只能通过导入资产的方式接入态势感知（专业版）。
- 云上资产信息不支持删除，而云外资产支持删除资产。

8.2 设置资产订阅

操作场景

态势感知（专业版）只有在开启资产订阅设置的工作空间才能同步资产相关信息。订阅后，资产信息将在每天晚上自动进行更新。

本章节介绍如何订阅资产。

- 仅支持订阅和同步云上资产。同时，不建议同一个区域的资产订阅至多个工作空间。

约束与限制

资产订阅仅支持订阅和同步云上资产。

设置资产订阅

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

步骤 5 在资产管理页面中，单击页面右上角“资产订阅设置”，右侧弹出资产订阅设置页面。

步骤 6 在订阅资产设置页面中，在需要订阅资产所在的 region 所在行“是否开通”列开启订阅。

步骤 7 单击页面右下角的“确认”。

订阅后，资产信息将在每天晚上自动进行更新。

----结束

8.3 查看资产信息

操作场景

在资产管理页面，可以查看资产的名称、类型、防护状态等信息，支持查看云上资产和云外资产。

前提条件

- 已完成资产订阅，详细操作请参见设置资产订阅。

查看资产信息

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

步骤 5 （可选）首次查看需要设置资产订阅，如果已订阅，请跳过该步骤。

态势感知（专业版）只有在开启资产订阅设置的工作空间才能同步资产相关信息。订阅后，资产信息将在每天自动晚上进行更新。

仅支持订阅和同步云上资产。同时，不建议同一个区域的资产订阅至多个工作空间。

1. 在资产管理页面中，单击页面右上角“资产订阅设置”，右侧弹出订阅资产设置页面。
2. 在订阅资产设置页面中，在需要订阅资产所在的 region 所在行“是否开通”列开启订阅。
3. 单击页面右下角的“确认”。

   订阅后，资产信息将在每天晚上自动进行更新。

步骤 6 在资产管理页面查看资产的详细信息。

- 如需查看指定类型资产信息，如主机资产，请选择“主机资产”页签进行查看。当前支持分类查看的资产类别有“主机资产”、“网站”、“数据库”、“VPC”、“EIP”、“设备”。“全部资产”页签查看所有资产。
- 部门及业务系统：该页签汇聚了资产所对应的“部门”及“业务系统”信息。
- 在资产列表中下方可以查看资产总条数。其中，使用翻页查看时最多可查看 10000 条资产信息，如果需要查看超过 10000 条以外数据，请优化过滤条件筛选数据。
- 如果需要查看某个资产的更多详细信息，可以先选择待查看资产所属类型，然后再在对应资产类型页面中单击资产名称，进入资产详情页面进行查看。

  例如，需要查看某个主机资产的详细信息，请选择“主机资产”页签，再在主机资产页面中，单击目标主机资产名称，进入目标主机资产详情页面。
  - 在资产详情页面，可以查看资产相关的环境信息、资产信息和网络信息等信息。
  - 在资产详情页面，可以对资产的责任人、业务系统和部门信息进行编辑，还可以绑定或解绑资产。

----结束

8.4 导入或导出资产

操作场景

态势感知（专业版）支持导入云外各种资产，导入后，可以呈现资产的安全状态。同时，还可以将资产信息导出，支持导出云上资产和云外资产的信息。

本章节介绍如何导入或导出资产。

约束与限制

- 仅支持导入.xlsx 格式的文件，单次导入文件大小不超过 5MB，且单次导入数据不超过 100 条。
- 最多支持导出 9999 条资产信息。

导入资产

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

步骤 5 在资产管理页面中，选择对应资产页签，如主机资产、网站、数据库等。

例如，需要导入主机资产，则选择“主机资产”页签。

需要导入部门或业务系统，则选择“部门及业务系统”页签。

步骤 6 导入资产，在资产列表左上方，单击“导入”，弹出导入资产对话框。

导入部门，单击“部门”下方的导入按钮，弹出导入部门对话框。

导入业务系统，单击“业务系统”下方的“导入”按钮，弹出导入业务系统对话框。

步骤 7 在导入资产对话框中，单击“下载模板”，并根据模板填写要求填写待导入资产信息。

在导入部门对话框中，单击“下载模板”，并根据模板填写要求填写待导入部门信息。

在导入业务系统对话框中，单击“下载模板”，并根据模板填写要求填写待导入业务系统信息。

步骤 8 待导入文件信息填写完成后，在导入对话框中，单击“添加文件”，并选择需要导入的 Excel 文件。

步骤 9 选择完成后，单击“确定”，完成导入。

步骤 10 导入完成后，在左侧导航栏选择“资产管理 > 资产管理”，在资产管理页面选择导入资产对应的资产页签，即可在资产列表中查看已导入的资产。

----结束

导出资产

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

步骤 5 在资产管理页面中，选择对应资产页签，进入对应资产页面。例如，需要导出主机资产，则选择“主机资产”页签。

步骤 6 在对应资产页面，勾选您需要导出的资产，并单击列表右上角的，弹出导出对话框。

若需要导出部门，则选择“部门及业务系统”页签，单击待导出部门后的导出按钮，弹出导出对话框。

若需要导出业务系统，则选择“部门及业务系统”页签，勾选您需要导出的业务系统，并单击列表上方的“导出”按钮，弹出导出对话框。

步骤 7 在导出资产对话框中，配置参数。

表 8-1 导出资产

参数名称	参数说明
导出格式	默认导出 excel 格式的资产列表。
自定义导出列	选择导出表格中，需要导出的参数。

步骤 8 单击“确定”。

系统将自动下载资产 excel 表格到本地。

----结束

8.5 编辑或删除资产

操作场景

在资产管理页面可以对资产的业务系统进行编辑。另外，如果不再需要在态势感知（专业版）资产管理页面展示某个或某些云下导入的资产的信息，可以删除资产。

本章节介绍如何编辑或删除资产。

- **云上和云外资产都支持编辑。**
- **仅自定义导入的云外资产支持删除，云上资产不支持删除。**

约束与限制

- 仅自定义导入的云外资产支持删除，云上资产不支持删除。

编辑或删除资产

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

步骤 5 编辑或删除资产。

表 8-2 编辑或删除资产

操作	执行步骤
编辑资产	**编辑资产** 1. 在资产管理页面中，勾选需要编辑的资产，并单击资产列表左上角“批量编辑”。 如果需要编辑某个类型的资产，可以选择对应资产页签，进入对应资产页面。例如，需要编辑主机资产，则选择“主机资产”页签。 2. 在弹出的资产编辑框中，对资产的业务系统进行编辑。 3. 编辑完成后，单击“确认”。 4. 在资产管理页面选择对应资产页签，可在资产列表查看资产信息。 **编辑部门** 1. 在资产管理页面中，选择“部门及业务系统”页签，单击“部门”后的编辑按钮。 2. 在弹出的“编辑部门”框中，编辑“部门名称”。 3. 编辑完成后，单击“确认”。 4. 在资产管理页面，选择“部门及业务系统”页签，可查看修改后的部门名称。 **编辑业务系统** 1. 在资产管理页面中，选择“部门及业务系统”页签，单击“业务系统”列表对应业务系统操作列的“编辑”按钮。 2. 在弹出的“编辑”对话框中，编辑“业务系统”，选择业务系统所在的“部门”，编辑“责任人”，设置“业务系统”关联的资产。 3. 编辑完成后，单击“确认”。 1. 在资产管理页面，选择“部门及业务系统”页签，可查看修改后的业务系统信息。

操作	执行步骤
删除资产	**删除资产** 1. 在资产管理页面中，选择对应资产页签，进入对应资产页面。例如，需要删除主机资产，则选择“主机资产”页签。 2. 在对应资产页面，勾选您自定义导入的需要删除的资产，并单击列表上方的“批量删除”。 3. 系统将删除已勾选资产。 **删除部门** 1. 在资产管理页面中，选择“部门及业务系统”页签。 2. 单击待删除“部门”后的删除按钮。 3. 在弹出的“删除部门”对话框中，确认信息无误后，单击“一键输入”DELETE，单击“确定”。 **删除业务系统** 1. 在资产管理页面中，选择“部门及业务系统”页签。 2. 选中待删除的“业务系统”，单击操作列的“删除”按钮或列表上方的“删除”按钮。 3. 在弹出的“删除业务系统”对话框中，确认信息无误后，单击“一键输入”DELETE，单击“确定”。

----结束

9 风险预防

9.1 基线检查

9.1.1 基线检查概述

态势感知（专业版）的基线检查功能支持检测云服务关键配置项，通过执行扫描任务，检查云服务基线配置风险状态，分类呈现云服务配置检测结果，告警提示存在安全隐患的配置，并提供相应配置加固建议和帮助指导。

基线检查方式

- **自动执行基线检查**

  态势感知（专业版）默认每隔 3 天检查一次，每次在 00:00~06:00 对您账号下当前区域的“安全上云合规检查 1.0”遵从包所涉及的资产进行检查。

  默认检查计划仅支持变更开启或关闭自动执行基线检查的操作。

- **自定义定时执行基线检查**

  根据需要支持自定义自动检查周期、检查时间和检查范围，详细操作请参见定时执行基线检查。

- **立即执行基线检查**
  - 立即检查所有遵从包：检查已有的，且已启用的遵从包中所有自动检查项的遵从情况。
  - 立即执行某个检查计划：检查已选择的检查计划中设置的遵从包中的检查项目的遵从情况。
  - 立即检查某个或某些检查项目：检查选中的检查项。

- **手动执行基线检查**

  基线检查的一些检查项目为手动检查项，需要您在线下执行检查后，再在控制台上反馈检查结果，以便计算检查项合格率。另外，自动检查的检查项目也可以进行手动检查。

  手动检查详细操作请参见手动执行基线检查。

使用流程

基线检查使用流程说明如下：

表 9-1 使用流程

序号	操作项	说明
0	（可选）接入“企业主机安全 HSS”的“主机安全基线”日志到态势感知（专业版）	仅态势感知（专业版）专业版且启用了“操作系统配置基线”、“经典弱口令检测”、“口令复杂度策略检测”遵从包场景需要执行该操作，启用遵从包请参见编辑、启用、停用或删除遵从包。 在目标工作空间左侧导航栏选择“日志审计 > 云服务接入”，进入云服务日志接入页面，打开“企业主机安全 HSS”服务的“主机安全基线”前的按钮以及“自动转告警”列对应的按钮，单击“保存”，并在弹出的配置保存框中，单击“确定”。更多信息请参见接入日志数据。
1	定时执行基线检查	态势感知（专业版）将使用默认检查计划对所有资产进行检查。 • 默认检查计划：默认每隔 3 天检查一次，每次在 00:00~06:00 对您账号下当前区域的“安全上云合规检查 1.0”遵从包所涉及的资产进行检查。 • 自定义基线检查计划：根据您的需求自定义遵从包和检查时间。
2	立即执行基线检查	基线检查功能支持定期自动检查和立即检查。 • 定期自动检查：根据系统默认基线检查计划或您自定义的基线检查计划，定时自动执行基线检查。 • 立即检查：如果您新增或修改了自定义的基线检查计划，您可以在基线检查页面选择该基线检查计划，立即执行基线检查，实时查看服务器中是否存在对应的基线风险。
3	查看检查结果	自动/手动基线检查完成后，可以查看基线检查结果，了解基线检查项影响的资产、基线项目详情等信息。
4	处理基线检查结果	基线检查完后，可以根据修复建议对风险项目进行处理。 • 查看风险项的改进建议：根据检测结果修复风险检查项。 • 反馈检查结果：检查项中的手动检查项，您在线下执行检查后，需要在控制台上反馈检查结果，以便计算检查项合格率。 • 导入检查结果：将线下检查结果数据信息导入至态势感知（专业版）基线检查中。 • 导出检查结果：将线上检查结果导出至本地。

9.1.2 立即执行基线检查

操作场景

为了解最新的云服务基线配置状态，您需要执行扫描任务，扫描结束后才能获取云服务基线的风险配置。基线检查功能支持定期自动检查和立即检查：

- 定期自动检查：根据态势感知（专业版）提供的默认基线检查计划或您自定义的基线检查计划，定时自动执行基线检查。
- 立即检查：支持立即检查所有检查规范或某个检查计划，实时查看是否存在基线风险。

本章节介绍如何**立即**执行基线检查，包含以下几种类型：

- 立即检查所有遵从包：检查已有的，且已启用的遵从包中所有自动检查项的遵从情况。
- 立即执行某个检查计划：检查已选择的检查计划中设置的遵从包中的检查项目的遵从情况。
- 立即检查某个或某些检查项目：检查选中的检查项。

约束与限制

- “立即检查”任务在 10 分钟内仅能执行一次。
- 手动立即执行“定期自动检查任务”在 10 分钟内仅能执行一次。

立即检查所有遵从包

本部分将介绍如何立即检查操作，检查已有的、且已启用的遵从包中的自动检查项的遵从情况。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入检查结果页面。

步骤 5 在“检查结果”页面中，单击“立即检查”，并在弹出的确认框中，单击“确认”。

刷新页面，查看“最近检查时间”，即可确认是否为最新的扫描结果。

----结束

立即执行某个检查计划

本部分将介绍如何立即执行某个检查计划，配置后，系统将立即执行已选择的检查计划，开始检查遵从包中的检查项目。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，并在安全遵从包页面中，选择“检查计划”页签，进入检查计划管理页面。

步骤 5 在待执行立即手动检查的检查计划所在栏的上方单击“立即检查”。

系统将立即执行已选择的基线检查计划。

----结束

立即检查某个或某些检查项目

本部分介绍如何立即检查某个或某些检查项。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入检查结果页面。

步骤 5 立即检查某个或某些检查项目。

- 某个检查项目
  a. 在检查结果页面下方检查项目列表中，单击目标自动检查项所在行操作列的“立即检查”。
  b. 在弹出的确认框中，单击“确认”。
     刷新页面，查看“最新扫描时间”，即可确认是否为最新的扫描结果。
- 某些检查项目
  a. 在检查结果页面下方检查项目列表中，勾选多个待检查的自动检查项目，并单击列表左上方的“立即检查”。
  b. 在弹出的确认框中，单击在弹出的确认框中，单击“确认”。
     刷新页面，查看“最新扫描时间”，即可确认是否为最新的扫描结果。

----结束

9.1.3 定时执行基线检查

操作场景

态势感知（专业版）支持根据基线检查计划检查您的资产是否存在风险，默认每隔 3 天，每次在 00:00~06:00 对您账号下当前 region 相关资产按照“安全上云合规检查 1.0”遵从包自动执行基线检查，无需用户执行额外操作，系统默认开启。

另外，还可以自定义自动检测周期、时间以及检查范围。

本文档将介绍如何新增自定义基线检查计划。

约束与限制

- 同一个检查遵从包只能属于一个检查计划。
- 由于“等保 2.0 三级要求”、“GDPR”、“PCI-DSS”、“NIST SP 800-53”遵从包中的检查项为手动检查项目，因此不支持创建包含该遵从包的检查计划。
- “操作系统配置基线”、“经典弱口令检测”、“口令复杂度策略检测”遵从包不支持在态势感知（专业版）侧执行基线检查，态势感知（专业版）仅支持查看 HSS 的基线检查结果。
- 支持检查“安全上云合规检查 1.0”、“护网检查”、“云安全配置基线”遵从包中支持自动化项的检查项。
- 默认检查计划不支持变更包含的遵从包以及检查时间，仅支持执行开启或关闭操作。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，并在安全遵从包页面中，选择“检查计划”页签，进入检查计划管理页面。

步骤 5 在检查计划页面中，单击“创建计划”，系统右侧弹出新建检查计划页面。

步骤 6 配置检查计划。

表 9-2 新建检查计划

参数名称		参数说明
基本信息	计划名称	自定义检查计划的名称。命名规则如下： • 计划名称由中文、字母、数字、下划线和连接符组成。 • 长度为 1~255 个字符。
	检查时间	下拉选择检测周期和检查触发时间。 • 检测周期：每隔 1 天、3 天、7 天、15 天、30 天检查一次 • 检查触发时间：00:00~06:00、06:00~12:00、12:00~18:00、18:00~24:00
选择遵从包		勾选选择需要检测的遵从包。

步骤 7 单击“确定”。

检查计划创建完成后，态势感知（专业版）会在指定的时间执行云服务基线扫描，扫描结果可以在“风险预防 > 基线检查”中查看。

----结束

相关操作

基线检查计划创建后，您可以查看检查计划、对检查计划进行编辑、删除、关闭、开启操作，详细操作请参见管理检查计划。

9.1.4 手动执行基线检查

操作场景

基线检查的一些检查项目为手动检查项，需要您在线下执行检查后，再在控制台上反馈检查结果，以便计算检查项合格率。

本章节介绍手动检查项目执行检查的操作。

约束与限制

- “操作系统配置基线”、“经典弱口令检测”、“口令复杂度策略检测”遵从包不支持在态势感知（专业版）侧执行基线检查，态势感知（专业版）仅支持查看 HSS 的基线检查结果。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入检查结果页面。

步骤 5 单击待反馈结果检查项目所在行“操作”列的“反馈结果”。

步骤 6 在弹出提示框中，选择反馈结果，并单击“确定”。反馈结果完成后，在“风险预防 > 基线检查”检查结果页面，查看检查项列表各个检查项的检查状态等信息。

反馈结果有效期为 7 天，7 天后请重新手动检查。

----结束

9.1.5 查看检查结果

操作场景

检查计划设置完成后，如果需尽快查看检查结果，可以在基线检查页面，执行立即检查。执行完成后，约 10 分钟后将可以在检查结果页面进行查看，立即检查相关操作请参见立即执行基线检查。

如果未执行立即检查，系统将按照已设置的检查计划，在指定时间内执行检查，例如，默认每隔 3 天检查一次，每次在 00:00~06:00 执行。检查完成后，将可以在检查结果页面中进行查看。

本章节介绍如何查看基线检查结果。

前提条件

- 已进行云服务基线扫描。
- 仅态势感知（专业版）专业版支持“操作系统配置基线”、“经典弱口令检测”、“口令复杂度策略检测”遵从包，需要提前在态势感知（专业版）接入企业主机安全 HSS 的“主机安全基线”日志且打开“主机安全基线”日志对应的“自动转告警”按钮。接入日志数据详细操作请参见 11.5.2 接入日志数据。

查看检查结果

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 （可选）在左侧导航栏选择“日志审计 > 云服务接入”，进入云服务日志接入成页面后，在**态势感知（专业版）**所在行的“审计相关日志”列，开启合规基线日志设置。

每个 Region 的首个工作空间可自动加载当前 Region 所有数据，无需手动处理。后续新增的用于自定义运营的工作空间，不会自动加载数据，需要用户自定义接入。

本步骤介绍手动接入操作指导。

设置完成后，如果需尽快查看检查结果，可以在基线检查页面，执行立即检查。执行完成后，约 10 分钟后将可以在检查结果页面进行查看，立即检查相关操作请参见立即执行基线检查。

如果未执行立即检查，系统将按照已设置的检查计划，在指定时间内执行检查，例如，默认每隔 3 天检查一次，每次在 00:00~06:00 执行。检查完成后，将可以在检查结果页面中进行查看。

步骤 5 在左侧导航栏选择“风险预防 > 基线检查”，默认进入检查结果页面。

步骤 6 在检查结果页面中，查看检查项的检查结果，参数说明如表 9-3 所示。

表 9-3 查看检查结果

参数名称	参数说明
风险资源及风险等级	最近一次支持基线检查的检查结果中，风险资源总数、不同风险等级的不合格检查项目数据和对应的风险资源的数量。 风险等级分为：致命、高危、中危、低危、提示几个级别。
策略扫描情况	对各个云服务的资产扫描后，合格、不合格以及检查失败数据信息。
安全包遵从状态	最近一次执行基线检查后，各个安全遵从包中合格、不合格以及检查失败数据和不合格检查项目所占比例。
检查结果合格率	最近一次执行基线检查的基线合格率。 检查结果合格率 = 基线检查合格项 / (合格项 + 不合格项 + 检查失败项) * 100%，不涉及的检查项将不会计算在内。
安全遵从包及检查结果列表	展示所有遵从包以及检查结果列表。 • 如果需要查看某个遵从包的检查结果，可以在左侧选择需要查看的检查规范，右侧列表中将会展示该遵从包中的检查项的检查结果详情。 • 单击检查结果列表右上角的设置按钮，可以对列表展示（例如，是否换行、是否固定操作列等）进行设置。 • 如需查看某个基线检查项详情，可以单击待查看检查项名称，进入检查项目详情页面。 在检查项目详情页面，查看检查项目的详细描述、检查过程、检查结果和对应的检查资源等详细信息。

----结束

9.1.6 处理检查结果

本章节介绍如何处理检查结果，请根据您的需要进行选择：

- 查看风险项的改进建议：根据检测结果修复风险检查项。
- 反馈检查结果：检查项中的手动检查项，您在线下执行检查后，需要在控制台上反馈检查结果，以便计算检查项合格率。
- 导入检查结果：将线下检查结果数据信息导入至态势感知（专业版）基线检查中。
- 导出检查结果：将线上检查结果导出至本地。

约束与限制

导入检查结果数据时，有以下限制条件：

- 支持导入.xlsx 格式的文件。
- 一次仅支持导入一个文件，文件大小不超过 500KB，且单次导入数据条不超过 500 条。
- 重复数据信息系统将进行去重处理，不会重复导入。

“操作系统配置基线”、“经典弱口令检测”、“口令复杂度策略检测”遵从包下的检查项仅支持针对检查项“加白名单”和“导出检查结果”，不支持在态势感知（专业版）侧修复，不支持导入检查结果。

前提条件

已扫描云服务基线。

查看风险项的改进建议

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入检查结果页面。

步骤 5 在检查结果页面下方的检查结果列表中，单击“检查状态”为“不合格”检查项名称，进入检查项详情页面。

步骤 6 查看检查项描述信息，查看“改进建议”。由用户根据风险项的改进建议手动修复风险配置，用户修复完成后可在检查项详情页面单击“立即检查”。

步骤 7 检查完成后，可参考查看检查结果确认风险项是否已修复。

----结束

反馈检查结果

态势感知（专业版）的基线检查项中的**手动**检查项，您在线下执行检查后，需要在控制台上反馈检查结果，以便计算检查项合格率。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入检查结果页面。

步骤 5 在检查结果页面下方的检查结果列表中，单击目标手动检查项所在行“操作”列的“反馈结果”。

步骤 6 在弹出提示框中，选择反馈结果，并单击“确定”。反馈结果完成后，在“风险预防 > 基线检查”检查结果页面，查看检查项列表各个检查项的检查状态等信息。

反馈结果有效期为 7 天，7 天后请重新手动检查。

----结束

导入检查结果

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入检查结果页面。

步骤 5 在下方检查结果列表左上角，单击的“导入”。

步骤 6 在弹出的对话框中单击“下载模板”，根据模板填写检查项目信息。

步骤 7 填写完成后，在弹出的对话框中单击“添加文件”，上传已填写的信息表格。

- 支持导入.xlsx 格式的文件。
- 一次仅支持导入一个文件，文件大小不超过 500KB，且单次导入数据条不超过 500 条。
- 重复数据信息系统将进行去重处理，不会重复导入。

步骤 8 上传完成后，单击“导入”。

步骤 9 导入完成后，在“风险预防 > 基线检查”检查结果页面，查看检查项列表各个检查项的检查结果信息。

----结束

导出检查结果

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入检查结果页面。

步骤 5 在下方检查结果列表中勾选需要导出的基线检查项目，并单击检查结果列表左上角的“导出”。

步骤 6 在弹出的对话框中，选择导出格式并自定义勾选需要导出的列。

步骤 7 单击“确定”。

----结束

9.1.7 管理遵从包

本章节介绍如何管理遵从包，包括：查看遵从包、添加自定义遵从包、导入遵从包、导出遵从包、编辑、启用、停用或删除遵从包。

- 查看遵从包：系统内置的遵从包和自定义遵从包都支持。
- 添加自定义遵从包：仅自定义遵从包支持。
- 导入遵从包：仅自定义遵从包支持。
- 导出遵从包：系统内置的遵从包和自定义遵从包都支持。
- 编辑遵从包：仅自定义遵从包支持，**系统内置遵从包不支持编辑操作**。
- 启用、停用遵从包：系统内置的遵从包和自定义遵从包都支持。
- 删除遵从包：仅自定义遵从包支持，**系统内置遵从包不支持删除操作**。

约束与限制

- 导入遵从包数据时，有以下限制条件：
  - 支持导入.xlsx 格式的文件。
  - 一次仅支持导入一个文件，且单次导入数据条不超过 100 条。
- 系统内置的遵从包不支持编辑、删除操作。
- 在空间托管场景，托管视图的“风险预防 > 基线检查”页面呈现的遵从包与主空间配置一致，其中主空间是用户在创建托管视图时绑定的工作空间。
- “操作系统配置基线”、“经典弱口令检测”、“口令复杂度策略检测”遵从包仅支持查看、启用、停用、导出遵从包，不支持导入、编辑和删除操作。

查看遵从包

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，默认进入遵从包页面。

步骤 5 在遵从包页面查看已有遵从包信息，参数说明如表 9-4 所示。

表 9-4 查看已有遵从包

参数名称	参数说明

参数名称	参数说明
遵从包总数及状态	已有遵从包总数及不同状态遵从包数量。 • 遵从包总数 • 启用的遵从包个数 • 未启用的遵从包个数
内置遵从包数量	态势感知（专业版）内置的遵从包数量。
自定义遵从包数量	用户自定义新增的遵从包数量。
遵从包及其详细信息	展示所有遵从包及其基本信息。 • 在遵从包列表中，可以查看遵从包的类型、状态、包含的检查项目数量等信息，还可以对遵从包进行启用、停用、删除（自定义新增的遵从包）操作。 • 单击遵从包列表右上角的设置按钮，可以对列表展示（例如，是否换行、是否固定操作列等）进行设置。 • 如果需要查看某个遵从包的详细信息，可以单击待查看遵从包名称，进入遵从包详情页面。 在遵从包详情页面，可以查看遵从包的版本、描述信息，以及包含的检查项等信息。

----结束

添加自定义遵从包

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，默认进入遵从包页面。

步骤 5 单击遵从包列表左上角的“添加遵从包”，进入创建遵从包页面。

步骤 6 在创建遵从包页面中，配置遵从包基础信息。

表 9-5 配置基础信息

参数名称	参数说明

参数名称		参数说明
遵从包名称		自定义遵从包名称。命名规则如下： • 遵从包名称由中文、字母、数字、下划线、小数点、连接符组成。 • 长度为 1~256 个字符。
描述		自定义遵从包描述信息。长度不超过 4096 个字符。
（可选）高级配置	版本	设置遵从包版本。版本配置示例：v1.0。 配置规范要求如下： • 由中文、字母、数字、下划线、小数点、连接符组成。 • 长度为 1~64 个字符。
	分类	填写遵从包所属分类。 遵从包分类配置示例如：国际标准、法律法规、行业标准、金融标准等。 填写规范要求如下： • 由中文、字母、数字、下划线、小数点、连接符组成。 • 长度为 1~64 个字符。
	领域	填写遵从包所属领域。领域配置示例：信息安全，隐私保护，网络安全，数据安全等。 填写规范要求如下： • 由中文、字母、数字、下划线、小数点、连接符组成。 • 长度为 1~64 个字符。
	责任人	设置遵从包责任人。 填写规范要求如下： • 由中文、字母、数字、下划线、小数点、连接符组成。 • 长度为 1~64 个字符。
	适用区域	填写遵从包使用区域。适用区域配置示例：全球、亚太等。 填写规范要求如下： • 由中文、字母、数字、下划线、小数点、连接符组成。 • 长度为 1~64 个字符。

步骤 7 单击“下一步”，进入配置遵从包页面。

步骤 8 在配置遵从包页面中，配置遵从包参数信息。

1. 在左侧导航栏中，单击，并在弹出的添加框中，输入节点名称后单击“确认”。
   - 添加子节点：如果还需要再添加二级或三级节点，可以将鼠标悬停在节点名称上，并单击新增按钮，并在弹出的添加框中，输入节点名称后按“Enter”。
   - 编辑或删除节点：如果需要对节点进行编辑或删除操作，可以将鼠标悬停在节点名称上，并单击编辑或删除按钮，对节点进行编辑或删除处理。
2. 选中已添加节点名称（最小级别，如增加了三级节点，则选中三级节点名称），并在右侧所有检查项中，选择需要关联的检查项。

步骤 9 单击“下一步”，进入确认配置页面。

步骤 10 确认配置信息无误后，单击“确定”。

步骤 11 添加成功后，在遵从包页面可查看已添加的遵从包信息，可以对遵从包进行启用、停用、编辑、删除操作。

----结束

导入遵从包

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，默认进入遵从包页面。

步骤 5 在下方遵从包列表左上角，单击“导入”。

步骤 6 在弹出的对话框中单击“下载模板”，根据模板填写遵从包信息。

步骤 7 填写完成后，在弹出的对话框中单击“添加文件”，上传已填写的信息表格。

- 导入遵从包数据时，有以下限制条件：
- 支持导入.xlsx 格式的文件。
- 一次仅支持导入一个文件，且单次导入数据条不超过 100 条。
- 系统内置的遵从包不支持编辑、删除操作。
- 在空间托管场景，托管视图的“风险预防 > 基线检查”页面呈现的遵从包与主空间配置一致，其中主空间是用户在创建托管视图时绑定的工作空间。
- “操作系统配置基线”、“经典弱口令检测”、“口令复杂度策略检测”遵从包仅支持查看、启用、停用、导出遵从包，不支持导入、编辑和删除操作。

步骤 8 上传完成后，单击“导入”。

步骤 9 导入完成后，在遵从包页面可查看已导入的遵从包信息，可以对遵从包进行启用、停用、编辑、删除操作。

----结束

导出遵从包

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，默认进入遵从包页面。

步骤 5 在下方遵从包列表中勾选需要导出的遵从包，并单击遵从包列表左上角的“导出”。

步骤 6 在弹出的对话框中，选择导出格式并自定义勾选需要导出的列。

步骤 7 单击“导出”。

----结束

编辑、启用、停用或删除遵从包

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，默认进入遵从包页面。

步骤 5 在遵从包列表中，对遵从包进行编辑、启用、停用或删除操作。

表 9-6 启用、停用或删除遵从包

操作名称	操作说明
编辑自定义新增的遵从包	1. 单击目标自定义新增的遵从包名称。 2. 编辑基本信息：在目标遵从包详情页面中，可以单击遵从包名称、描述等信息后的，编辑后，单击，保存修改。 3. 编辑遵从包内容：在遵从包内容所在栏中单击“编辑”，编辑遵从包节点或选择需要关联的检查项，编辑完成后单击“确认”。

操作名称	操作说明
停用遵从包	1. 单击目标遵从包所在行操作列的“停用”。 2. 在弹出的确认框中，单击“确定”。 3. 停用后，在遵从包页面可查看对应遵从包的状态变更为“未启用”。
启用遵从包	1. 单击目标遵从包所在行操作列的“启用”。 2. 在弹出的确认框中，单击“确定”。 3. 启用后，在遵从包页面可查看对应遵从包的状态变更为“启用”。
删除自定义新增的遵从包	仅自定义遵从包的且“状态”为“未启用”的遵从包支持删除。 1. 单击目标自定义新增的遵从包所在行操作列的“删除”。 2. 在弹出的对话框中，确认删除并输入“DELETE”，单击“确定”。

----结束

9.1.8 管理检查项

本章节介绍管理检查项，检查项支持如下操作：

表 9-7 管理检查项操作说明

操作类型	管理操作	说明
查看检查项	查看检查项	系统内置的遵从包检查项和自定义遵从包检查项都支持。
创建自定义检查项	创建自定义检查项	仅支持自定义遵从包的检查项。
对检查项加白名单	方式 1：在检查结果页面对某检查项加白名单	如果您不需要对某检查项进行检查，或者不需要对某检查项下的部分服务资源实例进行检查，可以执行加白名单操作。 在检查结果页面仅支持加白名单操作，不支持取消加白。 若希望再次检查该检查项，即取消加白，则需要通过遵从包详情页对检查项进行取消加白，或者通过“策略设置”删除检查项白名单策略。

操作类型	管理操作	说明
	方式 2：在遵从包详情页对某检查项加白名单	如果您不需要对某检查项进行检查，可以执行“加白名单”操作。 若希望再次检查该检查项，可以“取消加白”。 通过遵从包详情页对检查项进行加白操作仅支持对整个检查项加白，不支持对检查项下的部分资源实例加白。
	方式 3：通过策略设置对某检查项进行加白名单策略设置	如果您不需要对某检查项进行检查，或者不需要对某检查项下的部分服务资源实例进行检查，可以执行加白名单操作。 支持加白名单策略设置，支持删除或批量删除白名单策略。
导入	导入检查项	仅支持自定义遵从包的检查项。
导出	导出检查项	系统内置的遵从包检查项和自定义遵从包检查项都支持。
编辑或删除	编辑或删除检查项	仅支持自定义遵从包里的检查项，**系统内置的遵从包的检查项不支持编辑或删除操作**。

约束与限制

- 自定义检查项创建成功后，暂不支持对新增的单个检查项进行检查，需要执行立即检查或检查该检查项绑定的遵从包，才可以查看自定义检查项的检查结果。
- 导入检查项数据时，有以下限制条件：
  - 支持导入.xlsx 格式的文件。
  - 一次仅支持导入一个文件，且单次导入数据条不超过 100 条。
- 系统内置的遵从包检查项仅支持查看和导出检查项，不支持编辑或删除操作。

查看检查项

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，并在安全遵从包页面中，选择“检查项”页签，进入检查项管理页面。

步骤 5 在检查项页面中查看已有检查项信息，参数说明如表 9-8 所示。

表 9-8 查看已有检查项

参数名称	参数说明
检查项总数	当前工作空间内，检查项的总数量。
内置检查项数量	态势感知（专业版）内置的检查项数量。
自定义检查项数量	用户自定义新增的检查项数量。
检查项列表	展示所有检查项及其基本信息。 • 在检查项列表中，可以查看检查项的描述、类型、遵从包引用数量等信息，还可以对自定义检查项进行编辑、删除操作。 • 单击检查项列表右上角的设置按钮，可以对列表展示（例如，是否换行、是否固定操作列等）进行设置。 • 如果需要查看某个检查项的详细信息，可以单击待查看检查项名称，右侧弹出检查项详情页面。 在遵检查项详情页面，可以查看检查项的描述信息、基础信息、遵从包引用情况等信息。

----结束

创建自定义检查项

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，并在安全遵从包页面中，选择“检查项”页签，进入检查项管理页面。

步骤 5 单击检查项列表左上角的“创建检查项”，进入创建检查项页面。

步骤 6 在创建检查项页面中，配置检查项参数信息。

表 9-9 创建检查项

参数名称	参数说明
检查项名称	自定义检查项名称。 命名规则如下： • 由中文、字母、数字、下划线、小数点、连接符组成。 • 长度为 1~256 个字符。

参数名称	参数说明
描述	自定义检查项描述信息。长度不超过 4096 个字符。
等级	选择此检查项的等级。 • 致命 • 高危 • 中危 • 低危 • 提示
执行动作	选择此检查项的执行动作。 • 通过流程执行：此检查项通过流程自动进行检测，并反馈检测结果。 • 手动检测：此检查项目需要用户线下进行检查。
选择流程	当“执行动作”选择“通过流程执行”时，需要选择此检查项的执行流程，仅“流程类型”为“基线检查”的流程可选择使用。 如果没有合适的流程，可以单击“新建流程”，在流程页面中进行新建。
手动检测配置项	当“执行动作”选择“手动检测”时，系统默认设置了手动检测时，需要配置的检查结果选项。
云服务	填写此检查项关联的云服务信息。输入长度范围为 0~36 个字符。

步骤 7 单击“确定”。创建检查项完成后，在检查项页面，可通过已创建的检查项名称筛选检查项，查看检查项基本信息。

自定义检查项创建成功后，暂不支持对新增的单个检查项进行检查，需要执行立即检查或检查该检查项绑定的遵从包，才可以查看自定义检查项的检查结果。

添加成功后，可以根据需要对自定义检查项进行编辑或删除操作。

----结束

在检查结果页面对某检查项加白名单

如果您不需要对某检查项进行检查，或者不需要对某检查项下的部分服务资源实例进行检查，可以执行加白名单操作。

加白名单后，再次检查时，将不再对已加白检查项进行检查，且“检查项合格率”中，也将不再纳入计算中。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入检查结果页面。

步骤 5 在检查结果列表中，单击对应检查项所在行操作列的“加白名单”。

步骤 6 在弹出的确认框中，单击“确定”。加白名单后，检查结果列表中将不展示该检查项的信息。加白名单后，再次执行检查时，将不再对已加白检查项进行检查，且“检查项合格率”中，也将不再纳入计算中。

----结束

在遵从包详情页对某检查项加白名单

如果您不需要对某检查项进行检查，可以执行加白名单操作。

加白名单后，再次检查时，将不再对已加白的检查项进行检查，且“检查项合格率”中，也将不再纳入计算中。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，默认进入遵从包页面。

步骤 5 单击目标遵从包名称，进入遵从包详情页面。

步骤 6 在遵从包列表中搜索目标检查项，搜索到指定检查项后，单击待忽略检查项“操作”列的“加白名单”。

步骤 7 在弹出的确认框中，单击“确定”。加白名单后，检查结果列表中将不展示该检查项的信息。加白名单后，再次执行检查时，将不再对已加白检查项进行检查，且“检查项合格率”中，也将不再纳入计算中。

----结束

通过“策略设置”对某检查项进行加白名单策略设置

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入检查结果页面。

步骤 5 单击页面右上角“策略设置”，弹出“策略设置”配置页面。

步骤 6 在“白名单策略”栏下单击“新增加白策略”，弹出“新增加白策略”配置页面，配置对应参数。

表 9-10 新增加白策略参数说明

参数名称	参数说明
环境	选择待加白检查项所属的云环境。 仅支持下拉选择，不支持输入。
云服务	选择“环境”后，进一步选择待加白检查项所属的云服务。 仅支持下拉选择，不支持输入。 “云服务”的可选取值范围来自云环境中所有检查项关联的云服务合集。
检查项	选择“环境”和“云服务”后，选择待加白名单的检查项。 仅支持下拉选择，不支持输入。 “检查项”的可选取值范围是已选择的云环境对应的“云服务”下的所有关联检查项。
策略应用范围	设置检查项加白名单策略的应用范围。可选取值： • “全部实例”：当一个检查项关联了多个资源实例，配置“全部实例”则对整个检查项加白名单，检查项下的所有资源实例都生效加白名单策略。 • “部分实例”：当一个检查项关联了多个资源实例，配置“部分实例”可只对该检查项下的部分资源实例生效加白名单策略。 • 当一个检查项仅关联了一个资源实例，则配置为“全部实例”与配置为“部分实例”效果相同。
备注（可选）	添加对应的备注说明信息。 长度不能超过 1000 个字符。

步骤 7 参数配置完成后，单击“确认”。可在“策略设置”页面查看已新增的检查项加白名单策略。

----结束

取消加白或删除白名单策略

加白名单后，再次执行检查时，将不再对已加白的检查项进行检查，且“检查项合格率”中，也将不再纳入计算中。如需再次检查该检查项目，可以执行取消加白或删除白名单策略。检查项加白名单有三种方式，三种不同加白方式下取消加白或删除白名单策略的方法如下：

- 当通过在检查结果页面对某检查项加白名单，可通过如下两种方式进行取消加白操作：
  - 方式 1：参考在遵从包详情页对某检查项加白名单指导，在待取消加白检查项的“操作”列单击“取消加白”，并在弹出的确认框单击“确定”。
  - 方式 2：参考通过策略设置对某检查项进行加白名单策略设置指导，删除待取消加白检查项对应的白名单策略。
- 当通过在遵从包详情页对某检查项加白名单
  - 参考在遵从包详情页对某检查项加白名单指导，在待取消加白检查项的“操作”列单击“取消加白”，并在弹出的确认框单击“确定”。
- 当通过通过策略设置对某检查项进行加白名单策略设置，可以在“策略设置”页面删除对应的检查项加白策略。
  - 删除：在待取消加白的检查项加白策略所在行操作列的“删除”。在弹出的“删除”页面确认信息后单击“确定”。
  - 批量删除：勾选待取消加白的检查项加白策略，支持同时勾选多个加白策略，单击“批量删除”。在弹出的“删除”页面确认信息后单击“确定”。

导入检查项

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，并在安全遵从包页面中，选择“检查项”页签，进入检查项管理页面。

步骤 5 在下方检查项列表左上角，单击的“导入”。

步骤 6 在弹出的对话框中单击“下载模板”，根据模板填写检查项信息。

步骤 7 填写完成后，在弹出的对话框中单击“添加文件”，上传已填写的信息表格。

- 支持导入.xlsx 格式的文件。
- 一次仅支持导入一个文件，且单次导入数据条不超过 100 条。

步骤 8 上传完成后，单击“导入”。

步骤 9 导入完成后，在检查项页面可查看已导入的检查项信息，可通过检查项名称过滤筛选。

----结束

导出检查项

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，并在安全遵从包页面中，选择“检查项”页签，进入检查项管理页面。

步骤 5 在检查项列表中勾选需要导出的检查项，并单击检查项列表左上角的“导出”。

步骤 6 在弹出的对话框中，选择导出格式并自定义勾选需要导出的列。

步骤 7 单击“导出”。

----结束

编辑或删除检查项

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，并在安全遵从包页面中，选择“检查项”页签，进入检查项管理页面。

步骤 5 在检查项列表中，对检查项进行编辑或删除操作。

表 9-11 编辑或删除检查项

操作名称	操作说明
编辑自定义检查项	1. 单击目标自定义新增的检查项所在行操作列的“编辑”。 2. 编辑需要修改的参数后，单击“确定”。 3. 编辑完成后，在检查项页面，根据检查项名称过滤筛选检查项，查看检查项信息。 **系统内置的遵从包里的检查项不支持编辑操作，仅自定义检查项支持编辑。**
删除自定义检查项	1. 单击目标自定义新增的检查项所在行操作列的“删除”。 2. 在弹出的对话框中，确认删除并输入“DELETE”，单击“确定”。 **系统内置的遵从包里的检查项不支持删除操作，仅自定义检查项支持删除。**

----结束

9.1.9 管理检查计划

操作场景

本章节介绍如何管理检查计划。

约束与限制

- 默认检查计划不支持变更包含的遵从包以及检查时间，仅支持执行开启或关闭操作。
- **仅支持对自定义新增的检查计划进行编辑和删除操作。**

管理检查计划

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，并在安全遵从包页面中，选择“检查计划”页签，进入检查计划管理页面。

步骤 5 在检查计划页面中，对检查计划进行管理。

表 9-12 管理检查计划

操作名称	操作说明
查看已有检查计划	在检查计划页面中，查看已有的基线检查计划的名称、执行时间、绑定的遵从包。
编辑自定义检查计划	1. 在目标计划所在框的右上角单击“编辑”，系统右侧弹出编辑检查计划页面。 2. 编辑需要修改的计划参数后，单击“确定”。
关闭或开启检查计划	在目标计划所在框中的关闭（或开启）按钮，开启（或关闭）检查计划。
删除自定义检查计划	1. 在目标计划所在框的右上角单击“删除”。 2. 在弹出的对话框中，单击“确定”。

----结束

9.2 漏洞管理

9.2.1 漏洞管理概述

背景介绍

漏洞是指在操作系统实现、安全策略、软件等方面存在的缺陷或弱点，这些缺陷或弱点可能被攻击者利用，从而导致系统被破坏、数据泄露、服务中断或其他安全问题。态势感知（专业版）通过**集成企业主机安全（Host Security Service，HSS）漏洞扫描数据以及手动导入漏洞数据**，集中呈现云上资产漏洞风险，帮助用户及时发现资产安全短板，修复危险漏洞。

- 查看漏洞详情：介绍如何查看漏洞的详细信息。
- 修复漏洞：当扫描到服务器存在漏洞时，您需要及时根据漏洞的危害程度结合实际业务情况处理漏洞，避免漏洞被入侵者利用入侵您的服务器。如果漏洞对您的业务可能产生危害，建议您尽快修复漏洞。对于 Linux 漏洞、Windows 漏洞，您可以在企业主机安全控制台一键自动修复，对于 Web-CMS 漏洞、应用漏洞、应急漏洞和网站漏洞，暂不支持自动修复，您可以参考漏洞详情界面提供的修复建议手动修复。
- 忽略或取消忽略漏洞：某些漏洞只在特定条件下存在风险，比如某漏洞必须通过开放端口进行入侵，如果主机系统并未开放该端口，则该漏洞不存在危害。如果评估后确认某些漏洞无害，可以忽略该漏洞，无需修复。忽略后，下次 HSS 漏洞扫描后仍然会对该漏洞进行告警，态势感知（专业版）也将同步漏洞信息。**如果已忽略的漏洞需要再次关注，可以取消之前的忽略操作。**
- 导入或导出漏洞：介绍如何导入或导出漏洞。

主机漏洞

主机漏洞指的是态势感知（专业版）接入的 HSS 的漏洞扫描结果数据，实时呈现主机漏洞扫描检测信息，支持查看漏洞详情，并提供相应漏洞修复建议。

主机漏洞支持以下漏洞项的检测：

表 9-13 主机漏洞检测项说明

检测项	说明
Linux 软件漏洞检测	通过与漏洞库进行比对，检测出系统和软件（例如：SSH、OpenSSL、Apache、Mysql 等）是否存在漏洞，将存在风险的结果上报至管理控制台，并为您提供漏洞告警。
Windows 系统漏洞检测	通过订阅微软官方更新，判断服务器上的补丁是否已经更新，及时推送微软官方补丁，将存在风险的结果上报至管理控制台，并为您提供漏洞告警。
Web-CMS 漏洞检测	通过对 Web 目录和文件进行检测，识别出 Web-CMS 漏洞，将存在风险的结果上报至管理控制台，并为您提供漏洞告警。

检测项	说明
应用漏洞	通过检测服务器上运行的软件及依赖包发现是否存在漏洞，将存在风险的漏洞上报至控制台，并为您提供漏洞告警。

集成后，态势感知（专业版）中漏洞的等级和企业主机安全中修复优先级的说明如下：

- 企业主机安全：显示漏洞的修复优先级，它是由漏洞最高 CVSS 分值、漏洞发布时间和漏洞影响的资产重要性进行加权计算得出，反映了漏洞修复的紧急程度。

  漏洞修复优先级主要分为紧急、高、中、低四个等级，您可以参考修复优先级优先修复对您的服务器影响较大的漏洞。
- 态势感知（专业版）：显示漏洞的等级，等级是根据漏洞最高 CVSS 分值得出的，反映漏洞的严重程度。

  漏洞等级主要分为高危、中危、低危、提示四个等级，您可以根据漏洞的严重程度（由高到低）进行修复。

网站漏洞

网站漏洞指的是 WEB 网站存在的漏洞，当前仅支持手动导入漏洞数据。且网站漏洞不支持自动修复，您可以参考漏洞详情界面提供的修复建议手动修复漏洞。

9.2.2 查看漏洞详情

操作场景

当您需要查看漏洞类型分布，漏洞列表，受漏洞影响的 TOP 资产，以及漏洞的详情参数等信息，可参考本章节查看漏洞详情。

前提条件

- 已在 HSS 中完成 Agent 安装操作，详细操作请参见《企业主机安全用户指南》。
- **已接入 HSS 产品日志并已开启自动转告警设置**，详细操作请参见 11.5 云服务接入。如果接入了主机漏洞扫描结果，但是未开启自动转告警，则在“漏洞管理”将不会展示相关的漏洞扫描情况。

查看漏洞详情

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在态势感知（专业版）管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

步骤 5 在漏洞管理页面，查看漏洞信息。在漏洞列表上方的搜索框内，支持通过输入关键字进行模糊匹配过滤筛选漏洞信息。

表 9-14 查看漏洞信息

参数名称	参数说明
漏洞类型分布	呈现漏洞整体数量，及各类型漏洞分布情况。 系统默认呈现 5 种类型漏洞的分布情况，分别是 Linux 漏洞、Windows 漏洞、Web-CMS 漏洞、应用漏洞、网站漏洞。更多漏洞说明请参考漏洞管理概述章节内容。
漏洞 TOP5 排行	漏洞 TOP5 排行是根据受漏洞影响的资产数量的多少来进行排序，影响的资产越多排序越靠前。 • “漏洞编号”页签中，显示 TOP5 的漏洞的编号及受影响资产数量。 • “漏洞类型”页签中，显示 TOP5 的漏洞的名称、漏洞危险等级及受影响资产。
风险资产 TOP5 排行	呈现受漏洞影响的 TOP5 的风险资产。以条形图呈现每个风险资产中的不同等级的漏洞数量占比。
漏洞列表	• 在下方漏洞列表中，选择漏洞类型页签（例如，选择“Linux 漏洞”页签），进入对应漏洞类型的漏洞列表管理页面，漏洞列表参数信息说明请参见表 9-15。 • 如需查看某个漏洞的详细信息，可单击漏洞名称，在右侧弹出的详情页面进行查看。 • 在漏洞列表中下方可以查看漏洞总条数。其中，使用翻页查看时最多可查看 10000 条漏洞信息，如果需要查看超过 10000 条以外数据，请优化过滤条件筛选数据。

表 9-15 漏洞参数说明

参数名称	参数说明
漏洞名称	扫描出的漏洞名称。 单击漏洞名称，可查看该漏洞的简介、相关漏洞库信息。
等级	漏洞的危险程度。当前可分为 4 个等级：高危、中危、低危、提示。
漏洞 ID	漏洞的 ID 信息。
影响资产	受某个漏洞影响的资产总数。
漏洞编号	漏洞对应的编号。
最近扫描时间	最近一次扫描的时间。
是否处理	该漏洞的处理状态：“已处理”或“待处理”

----结束

9.2.3 修复漏洞

操作场景

当扫描到服务器存在漏洞时，您需要及时根据漏洞的危害程度结合实际业务情况处理漏洞，避免漏洞被入侵者利用入侵您的服务器。

如果漏洞对您的业务可能产生危害，建议您尽快修复漏洞。

- 对于 **Linux 漏洞、Windows 漏洞**，您可以**通过控制台修复漏洞**。
- 对于 **Web-CMS 漏洞、应用漏洞、应急漏洞和网站漏洞**，暂**不支持自动修复**，您可以参考漏洞详情界面提供的修复建议手动修复系统软件漏洞。

约束限制

- 企业主机安全各版本支持的漏洞处理操作请参见《企业主机安全用户指南》。
- 表 9-16 所示操作系统官方已停止维护，HSS 不再支持自动修复漏洞，建议您使用正在维护的操作系统。

表 9-16 官方已停止维护的操作系统

操作系统	说明
CentOS 8	官方已停止维护，HSS 使用 Red Hat 的补丁公告替代扫描，由于官方不出补丁所以无法修复，建议使用正在维护的操作系统。
Ubuntu 16.04、18.04、22.04	官方已停止维护，目前已不支持免费补丁更新，需要订阅 Ubuntu Pro 后才能安装升级包，未配置 Ubuntu Pro 会导致漏洞修复失败。
Debian 9、10	官方已停止维护，由于官方不出补丁所以无法修复，建议使用正在维护的操作系统。
Windows 2012 R2	官方已停止维护，由于官方不出补丁所以无法修复，建议使用正在维护的操作系统。

- CCE、MRS、BMS 的主机不能修复内核漏洞，贸然修复可能导致功能不可用。
- 处理漏洞时需保证目标服务器的“服务器状态”为“运行中”、“Agent 状态”为“在线”、“防护状态”为“防护中”。
- 手动导入的漏洞不支持修复。

操作风险

- 执行主机漏洞修复可能存在漏洞修复失败导致业务中断，或者中间件及上层应用出现不兼容等风险，并且无法进行回滚。为了防止出现不可预料的严重后果，建议您通过云备份（CBR）为 ECS 创建备份。然后，使用空闲主机搭建环境充分测试，确认不影响业务正常运行后，再对主机执行漏洞修复。

- 在线修复主机漏洞时，需要连接 Internet，通过外部镜像源提供漏洞修复服务。

通过控制台修复漏洞

仅 Linux 软件漏洞和 Windows 系统漏洞支持使用控制台的漏洞修复功能。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在态势感知（专业版）管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

步骤 5 在漏洞管理界面，选择“Linux 漏洞”、“Windows 漏洞”任意一个页签，进入对应漏洞管理页面。

步骤 6 在漏洞列表中，单击目标漏洞名称，右侧弹出漏洞信息页面。

步骤 7 在漏洞信息页面中的“受影响资产”所在栏中，单击资产列表中待处理资产所在行“操作”列的“修复”，系统提示修复操作触发成功。

步骤 8 漏洞修复完成后，如果修复成功，修复状态将变更为“修复成功”。如果修复失败，修复状态将变更为“修复失败”。

“Linux 系统 Kernel 类的漏洞”修复完成后需要手动重启，否则系统仍可能为您推送漏洞消息。

----结束

手动修复系统软件漏洞

对于 Web-CMS 漏洞、应用漏洞，不支持一键自动修复，您可以参考漏洞详情页面的修复建议，登录服务器手动修复。

- **漏洞修复命令**

  进入到漏洞的基本信息页，可根据修复建议修复已经被识别出的漏洞，漏洞修复命令可参见表 9-17。

  - “Windows 系统漏洞”和“Linux 系统 Kernel 类的漏洞”修复完成后需要手动重启，否则系统仍可能为您推送漏洞消息。
  - 不同的漏洞请根据修复建议依次进行修复。
  - 如果同一主机上的多个软件包存在同一漏洞，您只需修复一次即可。

表 9-17 漏洞修复命令

操作系统	修复命令
CentOS/Fedora /Euler/Redhat/Oracle	**yum update** *软件名称*

操作系统	修复命令
Debian/Ubuntu	**apt-get update && apt-get install** *软件名称* *--only-upgrade*
Gentoo	请参见漏洞修复建议。

- **漏洞修复方案**

  漏洞修复有可能影响业务的稳定性，为了防止在修复漏洞过程影响当前业务，建议参考以下两种方案，选择其中一种执行漏洞修复：

  - **方案一：创建新的虚拟机执行漏洞修复**
    i. 为需要修复漏洞的 ECS 主机创建镜像。
    ii. 使用该镜像创建新的 ECS 主机。
    iii. 在新启动的主机上执行漏洞修复并验证修复结果。
    iv. 确认修复完成之后将业务切换到新主机。
    v. 确定切换完成并且业务运行稳定无故障后，可以释放旧的主机。如果业务切换后出现问题且无法修复，可以将业务立即切换回原来的主机以恢复功能。
  - **方案二：在当前主机执行修复**
    i. 为需要修复漏洞的 ECS 主机创建备份。
    ii. 在当前主机上直接进行漏洞修复。
    iii. 如果漏洞修复后出现业务功能问题且无法及时修复，立即使用备份恢复功能将主机恢复到修复前的状态。

- 方案一适用于第一次对主机漏洞执行修复，且不确定漏洞修复的影响。
- 方案二适用于已经有同类主机执行过修复，漏洞修复方案已经比较成熟可靠的场景。

修复验证

漏洞修复后，建议您立即进行验证。

表 9-18 修复验证

验证方式	操作方法
手动验证	• 通过漏洞详情页面的“验证”，进行一键验证。 • 执行以下命令查看软件升级结果，确保软件已升级为最新版本。 – CentOS/Fedora /Euler/Redhat/Oracle 操作系统：**rpm -qa | grep** *软件名称* – Debian/Ubuntu 操作系统：**dpkg -l | grep** *软件名称* – Gentoo 操作系统：**emerge --search** *软件名称*

验证方式	操作方法
自动验证	如果您未进行手动验证，HSS 每日凌晨进行全量检测，您修复后需要等到次日凌晨检测后才能查看修复效果。

9.2.4 忽略或取消忽略漏洞

操作场景

某些漏洞只在特定条件下存在风险，比如某漏洞必须通过开放端口进行入侵，如果主机系统并未开放该端口，则该漏洞不存在危害。如果评估后确认某些漏洞无害，可以忽略该漏洞，无需修复。忽略后，下次 HSS 漏洞扫描后仍然会对该漏洞进行告警，态势感知（专业版）也将同步漏洞信息。同时，如果某个漏洞仍然需要关注，可以执行取消忽略操作。

本章节介绍如何忽略和取消忽略某个漏洞。

忽略或取消忽略漏洞

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在态势感知（专业版）管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

步骤 5 在漏洞管理界面，选择漏洞类型的任意一个页签，进入对应漏洞管理页面，并在漏洞列表中，单击目标漏洞名称，右侧弹出漏洞信息页面。

例如，需要对目标 Linux 漏洞进行处理，则此处选择“Linux 漏洞”页签，然后单击目标漏洞名称，右侧弹出漏洞信息页面。

步骤 6 对目标漏洞进行忽略或取消忽略操作。

- 忽略

  在漏洞信息页面中的“受影响资产”所在栏中，单击资产列表中待处理资产所在行“操作”列的“忽略”。

- 取消忽略

  a. 在漏洞信息页面中的“受影响资产”所在栏中，单击资产列表中待处理资产所在行“操作”列的“取消忽略”，弹出取消忽略确认框。

  b. 在确认框中，确认无误后，单击“确认”。

----结束

9.2.5 导入或导出漏洞

操作场景

态势感知（专业版）通过集成企业主机安全（Host Security Service，HSS）漏洞扫描数据以及手动导入漏洞数据，集中呈现云上资产漏洞风险，帮助用户及时发现资产安全短板，修复危险漏洞。

导入漏洞：针对态势感知（专业版）无法自动同步的云服务或资产的漏洞信息，支持用户手动导入漏洞数据，导入漏洞数据后，可在态势感知（专业版）统一查看跟踪。

导出漏洞：当您需要查看全量的漏洞信息时，态势感知（专业版）支持导出漏洞列表，支持用户自定义导出漏洞的参数信息。

本章节介绍如何导入、导出漏洞。

约束与限制

- 仅支持导入.xlsx 格式的文件，单次导入文件大小不超过 5MB，且单次导入数据不超过 100 条。
- 态势感知（专业版）最多支持导出 9999 条漏洞信息。

导入漏洞

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在态势感知（专业版）管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

步骤 5 在漏洞管理界面，选择漏洞类型的任意一个页签，进入对应漏洞管理页面。

例如，导入 Linux 漏洞，则此处选择“Linux 漏洞”页签。

步骤 6 在漏洞管理页面中，单击漏洞管理列表上方的“导入”，弹出导入对话框。

仅支持导入.xlsx 格式的文件，单次导入文件大小不超过 5MB，且单次导入数据不超过 100 条。

步骤 7 在导入漏洞对话框中，单击“下载模板”，并根据模板填写要求填写待导入漏洞信息。

步骤 8 待导入漏洞文件填写完成后，在导入漏洞对话框中，单击“添加文件”，并选择需要导入的 Excel 文件。

步骤 9 选择完成后，单击“确定”，完成导入。

步骤 10 导入完成后，可选择“风险预防 > 漏洞管理”，进入漏洞管理页面查看漏洞信息，可通过漏洞名称或漏洞 ID 过滤筛选。

----结束

导出漏洞

最多支持导出 9999 条漏洞信息。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在态势感知（专业版）管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

步骤 5 在漏洞管理界面，选择待导出漏洞所属分类的页签，进入对应漏洞管理页面。

例如，需要导出 Linux 漏洞，则选择“Linux 漏洞”页签，进入 Linux 漏洞管理页面。

步骤 6 在漏洞管理页面中，单击漏洞管理列表右上方的，弹出导出漏洞对话框。

最多支持导出 9999 条漏洞信息。

步骤 7 在导出漏洞对话框中，配置漏洞参数。

表 9-19 导出漏洞

参数名称	参数说明
导出格式	默认导出 excel 格式的漏洞列表。
自定义导出列	选择导出表格中，需要导出的参数。

步骤 8 单击“确定”。

系统将自动下载漏洞 excel 表格到本地。

----结束

9.3 策略管理

9.3.1 策略管理概述

态势感知（专业版）的策略管理功能可以简化您在多个账户和资源上的管理和维护任务，支持统一展示所有策略信息、查看人工/自动化拦截记录等操作。

- 新增策略：策略作为告警一键阻断的止血手段，可根据告警来源选择相应的类型对攻击者进行阻断。
- 管理策略：介绍如何查看策略、编辑策略、删除策略。

约束与限制

- 策略目前仅支持 CFW/WAF/VPC 安全组的黑名单策略。
- 单用户单工作空间内容最多新增 300 条支持阻断老化的，全量最多新增 2500 条。同时，单次下发策略阻断对象数量限制如下：
  - 当需要下发策略至 CFW 时，单用户单次最多可新增 500 个 IP 或域名作为阻断对象。
  - 当需要下发策略至 WAF 时，单用户单次最多可新增 500 个 IP 作为阻断对象。
  - 当需要下发策略至 VPC 时，单用户单次 1 分钟内最多可新增 500 个 IP 作为阻断对象。
- 将 IP 或 IP 地址段配置为黑名单后，来自该 IP 或 IP 地址段的访问，CFW/WAF/VPC 将不会做任何检测，直接拦截。
- 为确保系统稳定性，同时执行的任务数量必须小于等于 5 个，若检测到已有 5 个任务正在执行，系统将禁止继续新增、重试或编辑操作。

基本概念

- 操作连接：应急策略的流程所绑定的资产连接，资产连接是流程中插件节点使用到的连接域名和鉴权参数，通过域名调用的方式可以访问其他云服务或者三方服务。更多资产连接的信息请参见管理操作连接。

9.3.2 新增策略

操作场景

策略作为告警一键阻断的止血手段，可根据告警来源选择相应的类型对攻击者进行阻断。

本章节介绍如何新增策略。

约束与限制

- 将 IP 或 IP 地址段配置为黑名单后，来自该 IP 或 IP 地址段的访问，CFW/WAF/VPC 将不会做任何检测，直接拦截。
- 为确保系统稳定性，同时执行的任务数量必须小于等于 5 个，若检测到已有 5 个任务正在执行，系统将禁止继续新增、重试或编辑操作。
- 策略新增成功后，**不支持**修改阻断对象（即新增时设置的 IP 地址或 IP 地址段）。
- 新增成功后，**不支持**修改策略对象、策略类型、对象类型、和已经勾选的操作连接。

新增策略

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后选择“策略视图”页签，进入应急策略策略管理页面。

步骤 5 在策略管理页面中，单击“新增策略”，右侧弹出新增策略页面。

步骤 6 在新增策略页面中，配置策略信息。

表 9-20 新增策略

参数名称	参数说明
策略类型	根据需要选择策略类型：“阻断”或“加白名单”。 • 当选择“阻断”：阻断的策略对象将被禁止访问。 • 当选择“加白名单”：加入白名单的策略对象访问请求将被放行。
对象类型	当“策略类型”选择“阻断”时，对象类型可选范围有“IP”、“账号”、“域名”。 当“策略类型”选择“加白名单”时，对象类型可选范围有“IP”、“域名”。 请根据需要选择对象类型。 • 当选择“IP”：策略的操作对象是 IP 地址或 IP 地址段。 • 当选择“域名”：策略的操作对象是域名。 • 当选择“账号”：策略的操作对象是云服务账号（IAM 用户名）。
策略对象	请输入策略对象。 • 当“对象类型”选择“IP”时：策略对象请输入 IP 地址或 IP 地址段。请输入单个或多个 IP 地址或 IP 地址段，如有多个 IP 地址或 IP 地址段，请用英文逗号隔开。 填写示例：IPV4：192.168.0.0 或 192.168.0.0/12，IPV6：0:0:0:0:0:0:0:0 或 0:0:0:0:0:0:0:0/128。 • 当“对象类型”选择“域名”时：策略对象请输入域名。请输入单个或多个域名，如有多个域名，请用英文逗号隔开。域名只能由字母、数字、-、_和.组成，单段不能超过 63 个字符长度。 • 当“策略类型”选择“阻断”且“对象类型”选择“账号”时：策略对象请输入云服务账号（IAM 用户名）。请输入单个或多个云服务账号（IAM 用户名），如有多个云服务账号（IAM 用户名），请用英文逗号隔开。
策略生效范围	请根据需求选择“当前区域和企业项目”或“所有区域和企业项目”。

参数名称	参数说明
操作连接	应急策略的流程所绑定的操作连接。请根据需要选择该策略的操作连接。 • 当“策略类型”选择“阻断”且“对象类型”选择“IP”时：可选择防线类型为 CFW、VPC、WAF 对应的操作连接。 • 当“策略类型”选择“阻断”且“对象类型”选择“域名”时：可选择防线类型为 CFW 对应的操作连接。 • 当“策略类型”选择“加白名单”且“对象类型”选择“IP”时：可选择防线类型为 WAF 对应的操作连接。 • 当“策略类型”选择“加白名单”且“对象类型”选择“域名”时：可选择防线类型为 CFW 对应的操作连接。 • 当“策略类型”选择“阻断”且“对象类型”选择“IP”时：可选择防线类型为 VPC、WAF 对应的操作连接。 • 当“策略类型”选择“加白名单”且“对象类型”选择“IP”时：可选择防线类型为 WAF 对应的操作连接。
自动过期	确认新增的应急策略是否自动过期。 • 如果选择是，请设置策略过期时间。 • 如果选择否，则该策略将一直有效。
标签（可选）	自定义应急策略的标签。
策略描述（可选）	自定义该策略的描述信息。

步骤 7 配置完成后，单击“确定”。

步骤 8 新增策略配置完成后，返回策略管理页面，可查看新增的策略信息。

----结束

9.3.3 管理策略

操作场景

本章节介绍如何查看策略、编辑策略、删除策略。

查看策略

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后选择“策略视图”页签，进入应急策略策略管理页面。

步骤 5 应急策略管理页面默认进入“策略视图”页面，查看任务下发成功的应急策略统计情况：

- 策略过期分布：以饼图形式呈现“自动过期”策略占比，并统计“有自动过期”和“无自动过期”的策略数量。
- 策略分布：以柱状图形式呈现各个防线类型的“阻断”和“加白”策略类型的策略数量。应急策略支持的防线类型请参考约束与限制说明。
- 阻断区域 Top5：以条形图呈现策略对象所在的区域，仅统计 Top5 区域的应急策略数量分布情况。
- 应急策略列表：以列表形式呈现应急策略基本信息。策略列表参数说明如下：

表 9-21 查看应急策略策略列表参数说明

参数名称	参数说明
策略对象	策略对象，一个策略对象单独呈现一行。 • 当“对象类型”是“IP”时：此处呈现 IP 地址。 • 当“对象类型”是“域名”时：此处呈现单个域名。 • 当“对象类型”是“账号”时：此处呈现云服务账号（IAM 用户名）。
策略类型	策略类型：“阻断”或“白名单”。 • “阻断”：阻断的策略对象将被禁止访问。 • “白名单”：加入白名单的策略对象访问请求将被放行。
对象类型	策略的对象类型。 当“策略类型”是“阻断”时，对象类型可选范围有“IP”、“账号”、“域名”。 当“策略类型”是“白名单”时，对象类型可选范围有“IP”、“域名”。
防线类型	策略的防线类型。 • 应急策略支持的防线类型有 CFW/WAF/VPC。
区域	策略中的操作连接对应的区域。
标签	策略的标签信息。
创建人	策略的创建人信息。
自动过期	显示策略自动过期时间与当前时间的间隔。
过期时间	策略的自动过期时间点。

参数名称	参数说明
描述	策略的描述信息，该参数默认隐藏。单击应急策略列表上方搜索框最右侧的设置按钮，支持对应急策略列表进行如下设置： • “基础设置”： “表格内容折行”：启用此能力可让表格内容自动折行，禁用此功能可截断文本。 “操作列”：启用此能力可让操作列固定在最后一列永久可见。 • “自定义显示列”：自定义应急策略列表参数显示列，勾选参数前的则该参数会在列表中显示，去勾选参数前的则对应参数不在列表中显示。
创建时间	策略的创建时间。
操作	对策略进行编辑、删除等操作。详细操作指导参考编辑策略、删除策略。

单击某个策略对象前的，可展开该策略对象所有相关的操作连接列表，单击操作连接列表所在操作列的“历史记录”可查看该操作连接的历史记录信息。

步骤 6 单击管理页面的“任务视图”页面，可以查看应急策略的任务的统计情况，其中应急策略的新增、删除操作会生成任务。

“任务视图”页面包含如下信息：

- 策略下发：以柱状图形式呈现各个防线类型的应急策略任务下发的成功次数和失败次数。应急策略支持的防线类型请参考约束与限制说明。
- 区域策略下发：以柱状图形式呈现各个区域应急策略任务下发的成功次数和失败次数。
- 企业项目下发：以柱状图形式呈现各企业项目应急策略任务下发的成功次数和失败次数。
- 任务列表：以列表形式呈现应急策略任务的基本信息。任务列表参数说明如下：

表 9-22 应急策略任务列表参数说明

参数名称	参数说明
任务名称	显示任务名称信息，生成任务时由系统自动生成。
任务 ID	显示任务 ID 信息，生成任务时由系统自动生成。
策略类型	显示应急策略任务的策略类型信息：“阻断”或“白名单”。 • “阻断”：阻断的策略对象将被禁止访问。 • “白名单”：加入白名单的策略对象访问请求将被放行。
对象类型	应急策略任务的对象类型：“IP”、“账号”、“域名”。

参数名称	参数说明
创建人	任务的创建人信息。
状态	显示任务的状态信息： • “任务执行中”：显示任务执行的进度。 • “成功”：任务中执行成功的策略对象个数。 • “失败”：任务中执行失败的策略对象个数。
创建时间	应急策略任务的创建时间。
操作	对应急策略任务进行重试操作，当应急策略任务存在部分或全部策略对象任务下发失败的场景可执行该操作。 针对下发失败的任务，单击任务所在行“操作”列的“重试”。 如果需要对批量任务进行重试操作，可以在任务列表中勾选需要重试的任务，并单击列表上方“批量重试”。

----结束

编辑策略

策略新增成功后，**不支持**修改策略对象、策略类型、对象类型、和已经勾选的操作连接。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后选择“策略视图”页签，进入应急策略策略管理页面。

步骤 5 在策略管理页面“策略视图”中，单击待修改策略所在行“操作”列的“编辑”，右侧弹出编辑策略页面。

步骤 6 在编辑策略页面中，支持修改应急策略的标签和策略描述，支持修改自动过期策略，支持增加操作连接。

表 9-23 编辑应急策略

参数名称	参数说明
策略对象	策略对象。**该参数不支持修改。**
策略类型	策略类型。**该参数不支持修改。**
对象类型	策略的对象类型。**该参数不支持修改。**

参数名称	参数说明
策略生效范围	策略的生效范围。**支持修改。**
操作连接	策略的操作连接。已勾选的操作连接不支持取消，**未勾选的操作连接支持继续勾选**。
自动过期	确认新增的应急策略是否自动过期。**支持修改。** • 如果选择是，请设置策略过期时间。 • 如果选择否，则该策略将一直有效。
标签（可选）	应急策略的标签，**支持修改**。
策略描述（可选）	应急策略的描述信息，**支持修改**。

若需要删除策略对象的操作连接，可单击“策略视图”页面应急策略列表中对应策略对象所在行前的按钮，展开该策略对象所有相关的操作连接，并单击**待删除**操作连接所在行操作列的“删除”，在弹出的删除信息确认页面确认信息无误后单击“确定”即可。

步骤 7 单击“确定”。编辑完成后，可参考查看策略查看修改后的策略信息。

----结束

删除策略

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后选择“策略视图”页签，进入应急策略策略管理页面。

步骤 5 在应急策略管理页面的“策略视图”界面，单击待删除策略所在行“操作”列的“删除”。

如果需要删除多条策略，可以在策略列表中勾选需要删除的策略，并单击列表上方“批量删除”。

步骤 6 在弹出的删除确认框中，确认无误后单击“确定”。操作完成后，参考查看策略，界面无已经删除的策略信息则表示删除策略执行成功。

----结束

10 威胁管理

10.1 事件管理

10.1.1 查看事件信息

操作场景

事件是一个广泛的概念，可以包括告警，但不限于此，它可以是系统正常操作的一部分，也可以是异常或错误。在运维和安全领域，事件通常指的是已经发生并需要被关注、调查和处理的问题或故障。事件可能由一条或多条告警触发，也可能由其他因素（如用户操作、系统日志等）引发。

事件的目的是为了记录、分析、报告或审计，通常用于记录和报告系统的历史行为，以便于分析和审计。当前事件的主要生成方式如下：

- 新增事件：用户在事件管理页面新增事件。当用户识别到有攻击成功，或有需要被关注、处理的问题故障等，可以新增事件进行跟踪处理，需要逐条事件新增，若需要批量新增事件建议通过导入事件方式实现。
- 导入事件：用户在事件管理页面导入事件列表。支持通过列表的方式批量创建事件。
- 告警转事件或关联事件：通过告警转事件或关联事件方式生成。当收到告警信息且经过分析后，如果发现有攻击成功或有其他较为严重影响的，则需要进行单独处理，可以将它转为事件或关联事件。

在态势感知（专业版）的事件管理页面，可以通过查看事件列表了解近 360 天的事件的统计信息列表。列表内容包括事件的名称、类型、等级和发生时间等。并可通过自定义过滤条件，如事件名称、事件等级和发生时间等，快速查询到相应事件的统计信息。

本章节主要介绍如何查看事件信息。

告警和事件关系说明

本部分介绍告警和事件的含义、区别。

- **告警和事件的含义与区别**

表 10-1 告警和事件的含义与区别

类别	描述
定义	• 告警： 告警是运维中的一种异常信号的通知，通常是由监控系统或安全设备在检测到系统或网络中的异常情况时自动生成的。例如，当服务器的 CPU 使用率超过 90%时，系统可能会发出告警。这些异常情况可能包括系统故障、安全威胁或性能瓶颈等。 告警通常有明确的指示性，能够明确指出异常发生的位置、类型和影响。同时，告警可以按照严重程度来进行分类，如紧急、重要、一般等，以便运维人员根据告警的严重程度来决定哪些需要优先处理。 告警的目的是及时通知相关人员，以便能够迅速响应并采取措施解决问题。 • 事件： 事件是一个更广泛的概念，可以包括告警，但不限于此。事件可以是系统正常操作的一部分，也可以是异常或错误。在运维和安全领域，事件通常指的是已经发生并需要被关注、调查和处理的问题或故障。事件可能由一条或多条告警触发，也可能由其他因素（如用户操作、系统日志等）引发。 事件的目的更广泛，可以是为了记录、分析、报告或审计，通常用于记录和报告系统的历史行为，以便于分析和审计。
处理流程	• 告警： 告警的处理流程通常包括接收、确认、分析、响应和关闭等步骤。当监控系统发出告警时，运维人员首先需要确认告警的真实性，然后分析告警的原因和影响范围，最后采取相应的措施来解决问题，并关闭告警。 • 事件： 事件的处理流程则更加复杂和全面。除了包含告警处理流程中的各个环节外，事件处理还需要进行事件调查、影响评估、风险分析、制定应急计划、执行应急响应、事后总结等步骤。事件处理的目标是彻底解决问题，防止类似事件再次发生，并减少事件对业务的影响。

类别	描述
重要性与紧急程度	• 告警： 告警一般需要立即评估和响应。 每条告警的紧急程度和重要性各不相同，取决于告警的类型、级别和影响的范围。一些告警可能只是简单的提醒或预警，而另一些告警则可能表示系统已经遭受严重攻击或面临重大故障风险。 • 事件： 事件可能需要记录、分析或在某些情况下采取行动，但不一定需要立即响应。 事件通常比告警具有更高的重要性和紧急程度。因为事件已经发生并产生了实际的影响，需要立即采取措施来应对和解决问题。如果事件得不到及时处理，可能会给组织带来重大的经济损失或声誉损害。

查看事件信息

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 事件管理”，进入事件管理页面。

步骤 5 在事件管理页面查看事件信息。

表 10-2 查看事件信息

参数名称	参数说明
未处理事件	当前工作空间在筛选的时间范围内未处理事件的数量及其所属等级分布情况。
自动处理事件	当前工作空间在筛选的时间范围内通过剧本自动处理的事件数量。
手动处理事件	当前工作空间在筛选的时间范围内手动处理的事件数量。
事件数量	当前工作空间在筛选的时间范围内的事件总数量。

参数名称	参数说明
事件列表	展示事件的详细信息。 在事件列表中下方可以查看事件总条数。其中，使用翻页查看时最多可查看 10000 条事件信息，如果需要查看超过 10000 条以外数据，请优化过滤条件筛选数据。 事件列表中，可以查看事件的名称、等级、来源、状态等信息。 如需**查看某个事件概览**，可单击事件名称，页面右侧将展示事件的概览信息。 • 在事件概览页可查看事件等级、状态、责任人信息。在事件等级和状态的下拉箭头中修改事件等级、状态。 • 在事件概览页面可查看事件的处置建议、基本信息和关联信息（包括关联的威胁指标、告警、事件、攻击信息等）。 • 如果需要查看事件详情，可以在事件概览页面右下角单击“事件详情”，进入事件详情页面。 在详情页面除了可以查看概览页面的信息外，还可以查看事件的时间线和攻击信息。例如：事件首次发生时间、检测时间、攻击进程 ID 等。 • 在事件概览/详情页面可以关联或取消关联告警、事件、情报，还可以查看受影响资产相关信息。

----结束

相关操作

- 新增或编辑事件
- 导入或导出事件
- 关闭或删除事件

10.1.2 新增或编辑事件

操作场景

本章节主要介绍如何新增事件，以及如何对已有的事件进行编辑。

- 新增事件：当用户识别到有攻击成功，或有需要被关注、处理的问题故障等，可以新增事件进行跟踪处理。
- 编辑事件：当事件的状态、等级、责任人等信息发生变化时，可通过编辑事件修改信息。

新增事件

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 事件管理”，进入事件管理页面。

步骤 5 在事件管理页面单击“新增”，并在右侧弹出的新增事件管理页面中配置参数，参数说明如表 10-3 所示。

表 10-3 新增事件参数说明

参数名称		参数说明
基础信息	事件名称	自定义事件名称，命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。 • 长度不能超过 2550 个字符。
	事件类型	下拉选择事件类型。
	（可选）业务 ID	填写事件对应的业务 ID。
	事件等级	选择事件严重等级。 可选的等级有：致命、高危、中危、低危、提示。
	状态	选择事件状态。 可选事件状态有：打开、阻塞、关闭。 • 打开：确认事件未处理或故障仍然存在，可选择打开。 • 阻塞：确认事件因为特定原因无法进一步处理或解决，可选择阻塞。 • 关闭：确认事件已处理完成，问题已解决或故障已消失，可选择关闭事件。
	（可选）责任人	选择事件的主要责任人。
	数据源产品名称	选择数据源产品的名称。
	数据源类型	选择数据源所属类型。例如，来源为云服务，则选择云服务。
时间线	首次发生时间	配置事件首次发生时间。
	（可选）最近发生时间	配置事件最近一次发生的具体时间。
	（可选）计划关闭时间	选择事件计划关闭时间。

参数名称		参数说明
其他	（可选）验证状态	选择事件的验证状态，标识事件的准确性。 • 未知：无法确认事件是否带来实质的攻击。 • 攻击成功：确认该事件已经攻击成功。 • 攻击失败：确认该事件已经攻击失败。
	（可选）阶段	选择您的事件阶段。 • 准备：准备资源处理事件。 • 检测与分析：检测与分析事件发生原因。 • 控制、清除、恢复：进行事件问题处理。 • 告警后活动：事件处理完成后的后续活动。
	（可选）调试数据	选择是否开启模拟调试功能。
	（可选）标签	填写事件的标签。如“矿池”，“外联”等，多个标签用逗号隔开。
	描述	事件描述信息，输入规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。 • 长度不能超过 10240 个字符。

步骤 6 单击“确认”，完成事件创建。新增事件配置完成后，在左侧导航栏选择“威胁管理 > 事件管理”，进入事件管理页面，在事件管理页面可查看已新增的事件信息，详细操作指导和事件参数解释请参见查看事件信息。

----结束

编辑事件

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 事件管理”，进入事件管理页面。

步骤 5 在事件管理列表中，单击目标事件所在行“操作”列的“编辑”，右侧弹出编辑事件页面。

步骤 6 在弹出的“编辑”页面中，编辑事件参数。

表 10-4 编辑事件参数说明

参数名称		参数说明
基础信息	事件名称	自定义事件名称，命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。 • 长度不能超过 2550 个字符。
	事件类型	选择事件类型。
	（可选）业务 ID	填写事件对应的业务 ID。
	事件等级	选择严重等级。可选的等级有：致命、高危、中危、低危、提示。
	状态	选择事件状态。 可选事件状态有：打开、阻塞、关闭。 • 打开：确认事件未处理或故障仍然存在，可选择打开。 • 阻塞：确认事件因为特定原因无法进一步处理或解决，可选择阻塞。 • 关闭：确认事件已处理完成，问题已解决或故障已消失，可选择关闭事件。
	（可选）责任人	选择事件的主要责任人。
	数据源产品名称	选择数据源产品的名称，**不支持修改**。
	数据源类型	选择数据源所属类型，**不支持修改**。
时间线	首次发生时间	该事件首次发生时间。
	（可选）最近发生时间	该事件最近一次发生的具体时间。
	（可选）计划关闭时间	选择事件计划关闭时间。
其他	（可选）验证状态	选择事件的验证状态，标识事件的准确性。 • 未知：无法确认事件是否带来实质的攻击。 • 攻击成功：确认该事件已经攻击成功。 • 攻击失败：确认该事件已经攻击失败。
	（可选）阶段	选择您的事件阶段。 • 准备：准备资源处理事件。 • 检测与分析：检测与分析事件发生原因。 • 控制、清除、恢复：进行事件问题处理。 • 告警后活动：事件处理完成后的后续活动。

参数名称		参数说明
	（可选）调试数据	选择是否开启模拟调试功能，**不支持修改**。
	（可选）标签	填写事件的标签。如“矿池”，“外联”等，多个标签用逗号隔开。
	描述	事件描述信息，输入规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。 • 长度不能超过 10240 个字符。

步骤 7 单击“确认”，完成事件编辑。编辑事件配置完成后，在左侧导航栏选择“威胁管理 > 事件管理”，进入事件管理页面，在事件管理页面可查看事件信息，详细操作指导和事件参数解释请参见查看事件信息。

----结束

相关操作

- 查看事件信息：在态势感知（专业版）的事件管理页面，可以通过查看事件列表了解近 360 天的事件的统计信息列表。列表内容包括事件的名称、类型、等级和发生时间等。并可通过自定义过滤条件，如事件名称、事件等级和发生时间等，快速查询到相应事件的统计信息。
- 导入或导出事件：您可以将事件详情导出到本地，便于跨部门协作处理事件，提高内部信息共享效率。最多支持导出 9999 条事件记录。
- 关闭或删除事件：介绍如何关闭事件，删除事件信息。
- 告警转事件或关联事件：当收到告警信息且经过分析后，如果发现有攻击成功或有其他较为严重影响的，则需要进行单独处理，可以将它转为事件或关联事件。告警与事件的区别和联系请参见告警和事件关系说明。

10.1.3 导入或导出事件

操作场景

本章节主要介绍如何导入、导出事件。

- 导入事件：通过列表的方式批量创建事件。
- 导出事件：通过导出事件列表到本地，在本地查看事件信息，或者在团队内共享事件信息时可执行该操作。

约束与限制

- 仅支持导入.xlsx 格式的文件，单次导入文件大小不超过 5MB，且单次导入数据不超过 100 条。
- 最多支持导出 9999 条事件信息。

导入事件

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 事件管理”，进入事件管理页面。

步骤 5 在事件管理页面中，单击事件表格左上角的“导入”。

仅支持导入.xlsx 格式的文件，单次导入文件大小不超过 5MB，且单次导入数据不超过 100 条。

步骤 6 在弹出的“导入”对话框中，单击“下载模板”，并根据模板填写要求填写待导入事件信息。

步骤 7 待导入事件文件填写完成后，在导入事件对话框中，单击“添加文件”，选择需要导入的 Excel 文件。

步骤 8 选择完成后，单击“确定”，完成导入。导入完成后，在左侧导航栏选择“威胁管理 > 事件管理”，进入事件管理页面，在事件管理页面可以查看事件信息。

----结束

导出事件

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 事件管理”，进入事件管理页面。

步骤 5 在事件管理页面，勾选您需要导出的事件，并单击列表右上角的，弹出导出对话框。

最多支持导出 9999 条事件信息。

步骤 6 在导出事件对话框中，配置参数。

表 10-5 导出事件

参数名称	参数说明
导出格式	默认导出 excel 格式的事件列表。
自定义导出列	选择导出表格中，需要导出的参数。

步骤 7 单击“确定”。

系统将自动下载事件 excel 表格到本地。

----结束

10.1.4 关闭或删除事件

操作场景

本章节主要介绍如何执行关闭/删除事件操作。

- 关闭事件：确认事件已处理完成，问题已解决或故障已消失，可选择关闭事件。
- 删除事件：当满足如下场景，用户可选择删除事件。**事件删除后将无法恢复。**
  - 当用户确认该条事件是无效或无关事件；
  - 确认是重复冗余事件；
  - 确认是过期或历史事件，且无需保留事件数据或记录，无需后续处理动作。

关闭或删除事件

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 事件管理”，进入事件管理页面。

步骤 5 在事件管理页面中，对事件进行关闭或删除操作。

表 10-6 管理事件

操作	操作说明
关闭事件	1. 单击目标事件所在行“操作”列的“关闭”，弹出关闭事件确认框。 如果需要关闭多条事件，可以在事件列表中勾选需要关闭的事件，并单击列表上方“批量关闭”。 2. 在关闭确认框中，选择“关闭原因”并填写“关闭评论”后，单击“确认”。 3. 事件关闭后，在左侧导航栏选择“威胁管理 > 事件管理”，进入事件管理页面，对应关闭的事件“状态”为“关闭”则表示关闭事件执行成功。

操作	操作说明
删除事件	1. 在事件管理页面，单击目标事件所在行“操作”列的“删除”，弹出删除事件确认框。 如果需要删除多条事件，可以在事件列表中勾选需要删除的事件，并单击列表上方“批量删除”。 2. 确认无误后，在弹出的确认框中，单击“确认”。 3. 事件删除后，在左侧导航栏选择“威胁管理 > 事件管理”，进入事件管理页面，在事件管理页面无已删除的事件信息则表示删除事件执行成功。 **说明** 事件删除后将无法恢复，请谨慎操作。

----结束

10.2 告警管理

10.2.1 告警概述

告警是运维中的一种异常信号的通知，通常是由监控系统或安全设备在检测到系统或网络中的异常情况时自动生成的。例如，当服务器的 CPU 使用率超过 90%时，系统可能会发出告警。这些异常情况可能包括系统故障、安全威胁或性能瓶颈等。

告警通常有明确的指示性，能够明确指出异常发生的位置、类型和影响。同时，告警可以按照严重程度来进行分类，如紧急、重要、一般等，以便运维人员根据告警的严重程度来决定哪些需要优先处理。

告警的目的是及时通知相关人员，以便能够迅速响应并采取措施解决问题。

当态势感知（专业版）检测到的云资源中存在的异常情况（例如，某个恶意 IP 对资产攻击、资产已被入侵等）时，将以告警的形式将威胁信息展示在态势感知（专业版）告警管理界面中。

告警管理

在态势感知（专业版）的告警管理页面可以执行以下操作：

- 查看告警信息：可以通过查看告警列表了解近 360 天的告警威胁的统计信息列表，列表内容包括告警事件的名称、类型、等级和发生时间等。并可通过自定义过滤条件，如告警名称、告警等级和发生时间等，快速查询到相应告警事件的统计信息。
- 告警转事件或关联事件：当收到告警信息且经过分析后，如果发现有攻击成功或有其他较为严重影响的，则需要进行单独处理，可以将它转为事件或关联事件。
- 一键阻断或解封：策略作为告警一键阻断的止血手段，可根据告警来源选择相应的类型对攻击者进行阻断，拦截该恶意 IP 的访问。
- 关闭或删除告警：支持关闭或删除告警，告警删除后将无法恢复，请谨慎操作。

- 新增或编辑告警：支持新增告警，或者编辑告警参数。
- 导入或导出告警：支持导入或导出告警。

告警和攻击的区别

安全告警区分告警和攻击：

- 告警：告警则是基于态势感知（专业版）的威胁检测模型生成的模型告警，也可以是用户自定义或导入的告警。
- 攻击：攻击是原始的防线告警。

攻击是原始的防线告警。二者的区别如下：

表 10-7 告警和攻击的区别

名称	数据来源	支持的管理操作

名称	数据来源	支持的管理操作
告警	• 态势感知（专业版）威胁检测模型生成的告警。 • 用户自定义新增的告警。 • 用户导入的告警。	• 查看告警信息：可以通过查看告警列表了解近 360 天的告警威胁的统计信息列表，列表内容包括告警事件的名称、类型、等级和发生时间等。并可通过自定义过滤条件，如告警名称、告警等级和发生时间等，快速查询到相应告警事件的统计信息。 • 告警转事件或关联事件：当收到告警信息且经过分析后，如果发现有攻击成功或有其他较为严重影响的，则需要进行单独处理，可以将它转为事件或关联事件。 • 一键阻断或解封：策略作为告警一键阻断的止血手段，可根据告警来源选择相应的类型对攻击者进行阻断，拦截该恶意 IP 的访问。 • 关闭或删除告警：确认告警已处理完成，问题已解决，可选择关闭告警。当确认是无效告警或冗余告警或过期告警，用户可选择删除告警。告警删除后将无法恢复，请谨慎操作。 • 新增或编辑告警：态势感知（专业版）支持管理云上资产和云外资产，资产管理更多信息请参见资产管理概述。其中，云上资产的告警可以通过接入日志数据自动同步到态势感知（专业版），云外资产的告警数据需要用户在态势感知（专业版）通过新增告警或导入告警将告警数据接入态势感知（专业版）。当告警的状态和基础信息发生变化需要修改时，可通过编辑告警修改告警参数。 • 导入告警：云外资产的告警信息需要通过新增告警或导入告警的方式接入态势感知（专业版）。导入告警支持通过告警列表方式批量创建告警。 • 导出告警：通过导出告警列表到本地，在本地查看告警信息，或者在团队内共享告警信息时可执行该操作。
攻击	原始的防线告警。	• 查看攻击信息 • 导出攻击 • 处置攻击

告警的风险等级分类

表 10-8 告警的风险等级分类说明

风险等级	描述
致命	致命级别的告警表示系统已经受到严重的攻击，可能导致数据丢失、系统崩溃或者长时间的服务中断。例如，发现勒索加密行为或恶意程序感染。建议您立即处理，避免对系统造成更严重的损害。
高危	高危级别的告警表示系统可能正在受到攻击，但尚未造成严重的损害。例如，检测到未授权的登录尝试或执行了危险命令（如删除关键系统文件或修改系统设置的命令）。建议您及时调查并采取措施，以防止攻击蔓延。
中危	中危级别的告警表示系统存在潜在的安全威胁，但目前没有明显遭受攻击的迹象。例如，检测到文件或目录的异常修改，表明系统可能存在潜在的攻击路径或配置错误。建议您进一步分析并采取适当的防范措施，以确保系统的安全。
低危	低危级别的告警表示系统存在轻微的安全威胁，不会对系统的正常运行产生显著影响。例如，检测到一些端口扫描行为，这些行为通常是攻击者尝试寻找系统漏洞的前奏。这类告警可以在合适的时间进行处理，不需要立即采取紧急措施。如果您的资产安全等级要求较高，可以关注该等级的安全告警。
提示	对应资源存在潜在的错误可能影响到业务。如果您对您的资产的安全等级要求较高，可以关注该等级的安全告警。

告警的处置方式说明

告警常见的处置方式有一键阻断或解封、关闭告警、删除告警、告警转事件或关联事件、新增告警、编辑告警、导入导出告警。

表 10-9 告警的处置方式说明

处置方式	使用场景说明
一键阻断或解封	一键阻断：通过一键阻断配置阻断策略，拦截恶意 IP 或非法 IAM 用户的访问。 一键解封：解除对一键阻断策略中配置的 IP 或 IAM 用户的访问拦截，**仅针对下发过“一键阻断”操作且执行成功的告警才可以执行“一键解封”操作。**
关闭告警	确认告警已处理完成，问题已解决，可选择关闭告警。

处置方式	使用场景说明
删除告警	• 当满足如下场景，用户可选择删除告警。**仅用户自定义新增的告警或导入的告警支持删除操作，且告警删除后将无法恢复。** – 当用户确认该条告警是无效或无关告警； – 确认是重复冗余告警； – 确认是过期或历史告警，且无需保留告警数据，无需后续处理动作的告警。
告警转事件或关联事件	当收到告警信息且经过分析后，如果发现有攻击成功或有其他较为严重影响的，则需要进行单独处理，可以将它转为事件或关联事件。
新增告警	态势感知（专业版）支持管理云上资产和云外资产，资产管理更多信息请参见资产管理概述。其中，云上资产的告警可以通过接入日志数据自动同步到态势感知（专业版），云外资产的告警数据需要用户在态势感知（专业版）通过新增告警或导入告警将告警数据接入态势感知（专业版）。
编辑告警	当告警的状态和基础信息发生变化需要修改时，可通过编辑告警修改告警参数。
导入导出告警	导入告警：云外资产的告警信息需要通过新增告警或导入告警的方式接入态势感知（专业版）。 导出告警：通过导出告警列表到本地，在本地查看告警信息，或者在团队内共享告警信息时可执行该操作。

攻击处置方式说明

攻击是原始告警，支持在态势感知（专业版）侧进行处置，关闭或忽略本次攻击告警，更多详细信息请参见处置攻击。

- 关闭告警：如果告警已手动处理完毕，可以选择关闭本次告警。
- 忽略告警：如果告警风险可控，可以选择忽略本次告警。当相同告警事件再次触发时，将再次告警。

约束与限制

- 删除告警：仅用户自定义新增的告警或导入的告警支持删除操作。
- 导入告警：仅支持导入.xlsx 格式的文件，单次导入文件大小不超过 5MB，且单次导入数据不超过 100 条。
- 导出告警：最多支持导出 9999 条告警信息。
- 一键阻断或解封：约束与限制请参见约束与限制。

10.2.2 查看告警信息

操作场景

在态势感知（专业版）的告警管理页面，可以通过查看告警列表了解近 360 天的告警威胁的统计信息列表，列表内容包括告警事件的名称、类型、等级和发生时间等。并可通过自定义过滤条件，如告警名称、告警等级和发生时间等，快速查询到相应告警事件的统计信息。

告警管理页面分别呈现“告警”和“攻击”，二者的区别如下：

表 10-10 告警和攻击的区别

名称	数据来源
告警	• 态势感知（专业版）威胁检测模型生成的告警。 • 用户自定义新增的告警。 • 用户导入的告警。
攻击	原始的告警。

本章节主要介绍如何查看告警信息。

前提条件

如果需要查看已接入云服务的告警信息，需要在云服务接入时开启“自动转告警”设置。如果未开启，在对应日志满足告警条件时，将不会转为告警，也不会在“告警管理”页面中进行展示。详细操作请参见 11.5.2 接入日志数据。

查看告警信息

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面。

步骤 5 在告警管理页面查看告警信息。

表 10-11 查看告警信息

参数名称	参数说明

参数名称	参数说明
设置告警的显示时间范围	左上角可设置展示告警的周期，默认展示最近一周内的告警信息。用户可下拉选择或自定义展示告警的周期： • 最近 24 小时 • 最近一周 • 最近一个月 • 自定义：用户自定义设置起止时间。
信息统计	从 3 个维度统计状态为“打开”或“阻塞”的告警信息： • 来源分布：以柱状图形式统计各数据源的告警数。 • 类型 Top5：以告警数维度降序排序统计前 Top5 类型的告警。 • 资产风险 Top5:展示告警数多的 Top5 风险资产。
急需处理告警	当前工作空间中状态为“打开”或“阻塞”且风险等级为“高危”或“致命”的告警数量。
待处理告警	当前工作空间中状态为“打开”或“阻塞”，在筛选的时间范围内未处理告警的数量。
告警总数	当前工作空间在筛选的时间范围内告警总数量。
自动处理告警	当前工作空间在筛选的时间范围内通过剧本自动关闭的告警数量。
手动处理告警	当前工作空间在筛选的时间范围内手动关闭的告警数量。

参数名称	参数说明
告警列表	在告警列表中下方可以查看告警总条数。其中，使用翻页查看时最多可查看 10000 条告警信息，如果需要查看超过 10000 条以外数据，请优化过滤条件筛选数据。 告警列表中，可以查看告警的类型、等级、来源、处理状态等信息。如需查看某个告警概览信息详情，可单击目标告警分类，页面将展示该条告警的详情信息。 也可单击某条告警，进入告警详情页面，在告警详情页面中，可以对该条告警进行编辑、评论、一键解封、一键阻断、处置、转事件、打开、阻塞、关闭、刷新操作。告警详情页的“基础信息”、“告警说明”、“处置建议”、“攻击技战术”**最终呈现的告警参数信息取决于告警模型的字段配置，新建或编辑模型请参考新建或编辑模型。** 告警详情页面分别呈现如下告警信息： • 概览 – 基础信息：呈现告警的基本信息，如告警 ID、发生时间、数据来源等。 – 告警说明：呈现告警模型中配置的除基础信息外的其他告警信息，比如告警描述、置信度、关键性、攻击信息等。 – 处置建议：告警的处置建议。 – 分析链接：告警分析名称即产生告警的模型名称。 – 攻击技战术：攻击技术，攻击战术。 – 评论：展示该条告警以及运行的剧本的历史评论信息，还可以新增评论。 • 攻击 • 关联已有事件：该告警关联的事件。 • 关联情报：该告警关联的情报。 • 关联资产：该告警关联的资产信息。

----结束

查看攻击信息

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面。

步骤 5 在告警管理页面，选择“攻击”页签，查看攻击信息。

表 10-12 查看攻击信息

参数名称	参数说明
设置告警的显示时间范围	左上角可设置展示告警的周期，默认展示最近一周内的告警信息。用户可下拉选择或自定义展示告警的周期： • 最近 24 小时 • 最近一周 • 最近一个月 • 自定义：用户自定义设置起止时间。
信息统计	从 3 个维度统计状态为“打开”或“阻塞”的告警信息： • 来源分布：以柱状图形式统计各数据源的告警数。 • 类型 Top5:以告警数维度降序排序统计前 Top5 类型的告警。 • 资产风险 Top5:展示告警数多的 Top5 风险资产。
急需处理告警	当前工作空间中状态为“打开”或“阻塞”且风险等级为“高危”或“致命”的告警数量。
待处理告警	当前工作空间中状态为“打开”或“阻塞”，在筛选的时间范围内未处理告警的数量。
告警总数	当前工作空间在筛选的时间范围内告警总数量。
自动处理告警	当前工作空间在筛选的时间范围内通过剧本自动关闭的告警数量。
手动处理告警	当前工作空间在筛选的时间范围内手动关闭的告警数量。

参数名称	参数说明
告警列表	在告警列表中下方可以查看告警总条数。其中，使用翻页查看时最多可查看 10000 条告警信息，如果需要查看超过 10000 条以外数据，请优化过滤条件筛选数据。 告警列表中，可以查看告警名称、等级、类型、受影响资产、防御状态、状态、防线、数据来源、最近发生时间信息。 如需查看某个告警信息详情，可单击目标告警，进入告警详情页面： • 概览：告警详情页的基础信息模块，呈现告警 ID、防线/来源、攻击阶段、责任人、告警类型、首次发生时间。 • 受影响资产：呈现该告警影响的资产信息，包括资产名称、区域、资产归属账号名称/ID、企业项目名称/ID。 • 处置建议：告警的处置建议。 • 更多信息：告警的基础信息、受影响资产、进程信息等详细信息。 • 相似告警：呈现相似告警的告警列表。

----结束

10.2.3 告警转事件或关联事件

操作场景

当收到告警信息且经过分析后，如果发现有攻击成功或有其他较为严重影响的，则需要进行单独处理，可以将它转为事件或关联事件。

本章节主要介绍如何将告警转为事件，以及告警如何关联事件。

告警和事件关系说明

本部分介绍告警和事件的含义、区别，告警转事件的原因和告警关联事件的原因。

- **告警和事件的含义与区别**

表 10-13 告警和事件的含义与区别

类别	描述

类别	描述
定义	• 告警： 告警是运维中的一种异常信号的通知，通常是由监控系统或安全设备在检测到系统或网络中的异常情况时自动生成的。例如，当服务器的 CPU 使用率超过 90%时，系统可能会发出告警。这些异常情况可能包括系统故障、安全威胁或性能瓶颈等。 告警通常有明确的指示性，能够明确指出异常发生的位置、类型和影响。同时，告警可以按照严重程度来进行分类，如紧急、重要、一般等，以便运维人员根据告警的严重程度来决定哪些需要优先处理。 告警的目的是及时通知相关人员，以便能够迅速响应并采取措施解决问题。 • 事件： 事件是一个更广泛的概念，可以包括告警，但不限于此。事件可以是系统正常操作的一部分，也可以是异常或错误。在运维和安全领域，事件通常指的是已经发生并需要被关注、调查和处理的问题或故障。事件可能由一条或多条告警触发，也可能由其他因素（如用户操作、系统日志等）引发。 事件的目的更广泛，可以是为了记录、分析、报告或审计，通常用于记录和报告系统的历史行为，以便于分析和审计。
处理流程	• 告警： 告警的处理流程通常包括接收、确认、分析、响应和关闭等步骤。当监控系统发出告警时，运维人员首先需要确认告警的真实性，然后分析告警的原因和影响范围，最后采取相应的措施来解决问题，并关闭告警。 • 事件： 事件的处理流程则更加复杂和全面。除了包含告警处理流程中的各个环节外，事件处理还需要进行事件调查、影响评估、风险分析、制定应急计划、执行应急响应、事后总结等步骤。事件处理的目标是彻底解决问题，防止类似事件再次发生，并减少事件对业务的影响。

类别	描述
重要性与紧急程度	• 告警： 告警一般需要立即评估和响应。 每条告警的紧急程度和重要性各不相同，取决于告警的类型、级别和影响的范围。一些告警可能只是简单的提醒或预警，而另一些告警则可能表示系统已经遭受严重攻击或面临重大故障风险。 • 事件： 事件可能需要记录、分析或在某些情况下采取行动，但不一定需要立即响应。 事件通常比告警具有更高的重要性和紧急程度。因为事件已经发生并产生了实际的影响，需要立即采取措施来应对和解决问题。如果事件得不到及时处理，可能会给组织带来重大的经济损失或声誉损害。

- **告警转事件或关联事件的原因**

  告警通常是在系统或服务出现异常或潜在故障时产生的通知。这些异常可能会直接影响业务的正常运行，因此告警需要被及时处理，以防止业务异常。告警通常需要采取相应的措施来清除故障，否则可能会因为这些异常或故障引起业务的异常。

  事件则是在系统或服务在正常运行状态下产生的通知，它可能涉及到一些重要的状态变化，但不一定会引起业务异常。因此，事件一般不需要进行处理，主要用于帮助分析、定位问题。

表 10-14 告警转事件或关联事件的原因

类别	说明

类别	说明
告警转事件原因	当告警的严重性达到一定程度，或者持续出现，或者其影响范围广泛时，它可能不再仅仅是一个需要关注的信号，也可能表明系统或网络中存在一个持续性的问题，此时，它已经演变成了一个需要立即处理的事件，这种情况下，可以将告警转化为事件来处理，以便深入调查问题的根源，并采取相应的措施来彻底解决。通常告警转事件的原因有以下几个方面： • 信息聚合与分类 告警通常是对某个特定条件或阈值被违反的即时响应。随着时间的推移，大量的告警可能会被触发，如果直接处理这些独立的告警，可能会变得非常混乱和低效。将这些告警聚合成事件，可以帮助相关人员根据告警的类型、来源、影响等维度进行分类，从而更有效地处理它们。 • 简化工作流程 告警到事件的转换过程，通常伴随着对告警的过滤、去重、聚合等处理。这些处理使得原本可能触发多个相似告警的情况，被整合为一个更具代表性的事件。这样不仅减少了处理单个告警的工作量，也使得处理过程更加条理清晰，便于跟踪和记录。 • 提升问题解决效率 将告警转换为事件后，由于事件通常提供了比单个告警更全面的上下文信息，因此相关人员可以更容易地识别出问题的根本原因，有助于更快地定位问题，并采取有效的解决措施。 • 便于历史回顾与趋势分析 事件记录了问题的发生、发展、解决的全过程，这为后续的问题预防、系统优化等提供了宝贵的历史数据。通过对事件进行趋势分析，可以发现系统中潜在的薄弱环节，提前采取措施进行改进。 • 增强跨部门协作 在大型组织中，不同的部门可能需要共同参与问题的处理。将告警转换为事件后，可以更容易地在不同部门之间共享相关信息，促进跨部门协作，提高问题解决的效率。 总而言之，将告警转换为事件助于简化工作流程、提升问题解决效率、便于历史回顾与趋势分析。

类别	说明
告警关联事件原因	告警关联事件是监控和故障管理中的一个重要环节，它涉及到将多个独立但可能相互关联的事件或告警组合起来，以便更好地理解问题的根源和范围，从而更有效地进行故障排查和响应。通常告警关联事件的原因有以下几个方面： • 依赖关系 在复杂的系统中，各个组件之间往往存在复杂的依赖关系。当一个组件出现故障时，可能会影响依赖它的其他组件的正常工作，进而引发一系列告警。例如，在微服务架构中，一个服务的崩溃可能导致调用该服务的其他服务也出现问题。 • 资源共享 当多个系统或服务共享同一资源（如服务器、数据库、网络设备等）时，该资源的问题可能导致多个系统或服务同时发出告警。例如，共享数据库服务器的性能下降可能会触发多个依赖该数据库的应用程序的性能告警。 • 连锁反应 某些情况下，一个初始的故障可能触发一系列连锁反应，导致更多的组件或系统受到影响。这种连锁反应可能由于系统设计不当、错误处理机制不完善或资源限制（如内存泄漏导致的性能下降）等原因引起。 • 配置错误 配置错误或不一致的配置可能导致系统行为异常，进而触发多个看似不相关的告警。例如，错误的路由配置可能导致流量被错误地路由到不稳定的服务器，从而引发多个与性能相关的告警。 • 软件缺陷 软件中的缺陷（如 bug）可能导致程序在特定条件下表现异常，并触发告警。如果这些缺陷影响了多个组件或系统，则可能引发多个关联告警。 • 外部因素 外部因素如自然灾害（如地震、洪水）、网络攻击、基础设施故障（如电力中断、网络中断）等也可能导致多个系统或组件同时出现问题，并触发大量告警。

告警转事件

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面。

步骤 5 在告警管理列表中，单击目标告警所在行“操作”列的“转事件”，右侧弹出转事件配置页面。

同时，还可以在某条告警详情页面，单击页面上方的“告警转事件”。

步骤 6 在转事件配置页面中，填写“事件名称”并选择“类型”。

事件名称将自动填入当前告警的名称，可以根据需要进行修改。

步骤 7 设置完成后，单击“确认”。

步骤 8 在左侧导航栏选择“威胁管理 > 事件管理”，进入事件管理页面查看事件信息，详细操作指导和事件参数解释请参见查看事件信息。

----结束

告警关联事件

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面。

步骤 5 在告警管理列表中，勾选需要关联事件的告警，并单击列表上方的“关联事件”，弹出绑定事件对话框。

步骤 6 在绑定事件对话框中，勾选需要绑定的事件，并单击“确认”。

关联完成后，在告警列表中单击目标告警类型，进入告警详情页面后，选择“关联已有事件”页签，查看关联信息。

----结束

10.2.4 一键阻断或解封

操作场景

一键阻断：通过一键阻断配置阻断策略，拦截恶意 IP 或非法 IAM 用户的访问。

一键解封：解除对一键阻断策略中配置的 IP 或 IAM 用户的访问拦截，**仅针对下发过“一键阻断”操作且执行成功的告警才可以执行“一键解封”操作。**

策略作为告警一键阻断的止血手段，可根据告警来源选择相应的类型对攻击者进行阻断，拦截该恶意 IP 的访问。

本章节介绍如何执行一键阻断和一键解封操作。

约束与限制

- 将 IP 或 IP 地址段配置为黑名单后，来自该 IP 或 IP 地址段的访问，CFW/WAF/VPC 将不会做任何检测，直接拦截。
- 为确保系统稳定性，同时执行的任务数量必须小于等于 5 个，若检测到已有 5 个任务正在执行，系统将禁止继续新增、重试或编辑操作。
- 策略新增成功后，**不支持**修改阻断对象（即新增时设置的 IP 地址或 IP 地址段）。
- 新增成功后，**不支持**修改策略对象、策略类型、对象类型、和已经勾选的操作连接。
- 当同一个 IP 被同一个云服务同时配置在黑名单和白名单中，实际生效以黑名单为准。

一键阻断

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面。

步骤 5 在告警管理列表中，单击目标告警所在行“操作”列的“更多 > 一键阻断”，右侧弹出一键阻断配置页面。

同时，还可以在某条告警详情页面，单击页面上方的“一键阻断”。

步骤 6 在一键阻断配置页面中，配置阻断策略信息。

表 10-15 一键阻断新增策略

参数名称	参数说明
策略类型	根据需要选择策略类型：“阻断”或“加白名单”。 • 当选择“阻断”：阻断的策略对象将被禁止访问。 • 当选择“加白名单”：加入白名单的策略对象访问请求将被放行。

参数名称	参数说明
对象类型	当“策略类型”选择“阻断”时，对象类型可选范围有“IP”、“账号”、“域名”。 当“策略类型”选择“加白名单”时，对象类型可选范围有“IP”、“域名”。 请根据需要选择对象类型。 • 当选择“IP”：策略的操作对象是 IP 地址或 IP 地址段。 • 当选择“域名”：策略的操作对象是域名。 • 当选择“账号”：策略的操作对象是云服务账号（IAM 用户名）。
策略对象	请输入策略对象。 • 当“对象类型”选择“IP”时：策略对象请输入 IP 地址或 IP 地址段。请输入单个或多个 IP 地址或 IP 地址段，如有多个 IP 地址或 IP 地址段，请用英文逗号隔开。 填写示例：IPV4：192.168.0.0 或 192.168.0.0/12，IPV6：0:0:0:0:0:0:0:0 或 0:0:0:0:0:0:0:0/128。 • 当“对象类型”选择“域名”时：策略对象请输入域名。请输入单个或多个域名，如有多个域名，请用英文逗号隔开。域名只能由字母、数字、-、_和.组成，单段不能超过 63 个字符长度。 • 当“策略类型”选择“阻断”且“对象类型”选择“账号”时：策略对象请输入云服务账号（IAM 用户名）。请输入单个或多个云服务账号（IAM 用户名），如有多个云服务账号（IAM 用户名），请用英文逗号隔开。
策略生效范围	请根据需求选择“当前区域和企业项目”或“所有区域和企业项目”。
操作连接	应急策略的流程所绑定的操作连接。请根据需要选择该策略的操作连接。 • 当“策略类型”选择“阻断”且“对象类型”选择“IP”时：可选择防线类型为 CFW、VPC、WAF 对应的操作连接。 • 当“策略类型”选择“阻断”且“对象类型”选择“域名”时：可选择防线类型为 CFW 对应的操作连接。 • 当“策略类型”选择“加白名单”且“对象类型”选择“IP”时：可选择防线类型为 WAF 对应的操作连接。 • 当“策略类型”选择“加白名单”且“对象类型”选择“域名”时：可选择防线类型为 CFW 对应的操作连接。
自动过期	确认新增的应急策略是否自动过期。 • 如果选择是，请设置策略过期时间。 • 如果选择否，则该策略将一直有效。

参数名称	参数说明
标签（可选）	自定义应急策略的标签。
策略描述（可选）	自定义该策略的描述信息。

步骤 7 配置完成后，单击“确定”。

----结束

一键解封

仅针对下发过“一键阻断”操作且执行成功的告警才可以执行“一键解封”操作。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面。

步骤 5 在告警管理列表中，单击目标告警所在行“操作”列的“更多 > 一键解封”。

同时，还可以在某条告警详情页面，单击页面右上角的“一键解封”。

步骤 6 在弹出的一键解封确认框中，输入解封原因，并单击“确定”。

----结束

10.2.5 关闭或删除告警

操作场景

本章节主要介绍如何执行关闭/删除告警操作。

- 关闭告警：确认告警已处理完成，问题已解决，可选择关闭告警。关闭告警后，在告警管理页面的告警列表中，对应告警的“状态”变为“关闭”，则表示关闭告警操作执行成功。
- 删除告警：当满足如下场景，用户可选择删除告警。**仅用户自定义新增的告警或导入的告警支持删除操作，且告警删除后将无法恢复。**
  - 当用户确认该条告警是无效或无关告警。
  - 确认是重复冗余告警。
  - 确认是过期或历史告警，且无需保留告警数据，无需后续处理动作的告警。

约束与限制

- 仅用户**自定义新增的告警**、**导入的告警**、在态势感知（专业版）接入云服务日志**自动转告警生成的告警**支持删除操作。

关闭或删除告警

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面。

步骤 5 在告警管理页面中，对告警进行关闭或删除操作。

表 10-16 管理告警

操作	操作说明
关闭告警	1. 单击目标告警所在行“操作”列的“关闭”，弹出关闭告警确认框。 如果需要关闭多条告警，可以在告警列表中勾选需要关闭的告警，并单击列表上方“批量关闭”。 2. 在关闭确认框中，选择“关闭原因”并填写“关闭评论”后，单击“确认”。 3. 告警管理页面的告警列表中，对应告警的“状态”变为“关闭”，则表示关闭告警操作执行成功。
删除告警	1. 单击目标告警所在行“操作”列的“更多 > 删除”，弹出删除告警确认框。 如果需要删除多条告警，可以在告警列表中勾选需要删除的告警，并单击列表上方“更多 > 批量删除”。 2. 在弹出的确认框中，单击“确认”。 3. 告警删除后，告警管理页面的告警列表中将不再显示被删除的告警信息。 **说明** 告警删除后将无法恢复，请谨慎操作。

----结束

10.2.6 新增或编辑告警

操作场景

本章节主要介绍如何新增告警，以及如何对已有的告警进行编辑。

新增告警：态势感知（专业版）支持管理云上资产和云外资产，资产管理更多信息请参见资产管理概述。其中，云上资产的告警可以通过 11.5.2 接入日志数据自动同步到态势感知（专业版），云外资产的告警数据需要用户在态势感知（专业版）通过新增告警或导入告警将告警数据接入态势感知（专业版）。

编辑告警：当告警的状态和基础信息发生变化需要修改时，可通过编辑告警修改告警参数。

新增告警

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面。

步骤 5 在告警管理页面单击“新增”，并在右侧弹出的新增告警管理页面中配置参数，参数配置说明如下表所示。

表 10-17 告警参数说明

参数名称		参数说明
基础信息	告警名称	自定义告警名称，命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。 • 长度不能超过 2550 个字符。
	告警类型	选择告警类型。
	告警等级	选择告警严重等级，可选择以下等级：提示、低危、中危、高危、致命。告警等级的说明请参见告警的风险等级分类。

参数名称		参数说明
	状态	选择告警状态，告警状态用于标识告警跟踪的状态。可选择以下状态：打开、阻塞、关闭。 • 打开：未处理且需要继续跟踪关注的告警，建议配置为“打开”状态。 • 阻塞：跟踪的告警因某些原因暂时无法处置需要挂起的建议配置为“阻塞”状态。 • 关闭：已经处置完毕且不需要继续跟踪的告警建议配置为“关闭”状态。
	（可选）责任人	选择告警跟踪或处置的主要责任人。
	数据源产品名称	选择数据源产品的名称。
	数据源类型	选择数据源所属类型，可选择以下类型：云服务、第三方产品、租户私有产品。 • 云服务：接入态势感知（专业版）的云服务日志的告警，支持接入的云服务日志请参见 11.5.1 支持接入的云服务日志。 • 第三方产品：第三方的产品产生的告警数据。 • 租户私有产品：租户自己的私有产品产生的告警数据。
时间线	首次发生时间	该条告警首次发生时间。
	（可选）最近发生时间	该条告警最近一次发生的具体时间。
	（可选）计划关闭时间	选择告警计划关闭时间。
其他	（可选）验证状态	选择告警的确认状态，标识告警攻击的状态，确认是否造成实际的负面影响。可选择以下状态：未知、攻击成功、攻击失败。 • 未知：无法确认告警是否带来实质的攻击。 • 攻击成功：确认该告警已经攻击成功。 • 攻击失败：确认该告警已经攻击失败。 • 可疑：该告警存在可疑的攻击行为，如攻击尝试。 • 白名单：确认无攻击行为的主机告警。 • 非攻击信息：非恶意攻击，如系统脆弱性告警，风险账号、弱口令等。

参数名称		参数说明
	（可选）阶段	选择您的告警阶段。 • 准备：准备资源处理告警。 • 检测与分析：检测与分析告警发生原因。 • 控制、清除、恢复：进行告警问题处理。 • 告警后活动：告警处理完成后的后续活动。
	（可选）调试数据	选择是否开启模拟调试功能。
	（可选）标签	填写告警的标签。
	描述	填写告警描述信息，填写规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。 • 长度不能超过 10240 个字符。

步骤 6 单击“确认”。新增告警配置完成后，在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面查看告警信息。

----结束

编辑告警

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面。

步骤 5 在告警管理列表中，单击目标告警所在行“操作”列的“编辑”，右侧弹出编辑告警页面。

步骤 6 在弹出的编辑告警页面中，编辑告警参数，参数说明如下表所示。

表 10-18 告警参数说明

参数名称		参数说明
基础信息	告警名称	自定义告警名称，命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。 • 长度不能超过 2550 个字符。

参数名称		参数说明
	告警类型	选择告警类型。
	告警等级	选择告警严重等级，可选择以下等级：提示、低危、中危、高危、致命。 告警等级的说明请参见告警的风险等级分类。
	状态	选择告警状态，告警状态用于标识告警跟踪的状态。可选择以下状态：打开、阻塞、关闭。 • 打开：未处理且需要继续跟踪关注的告警，建议配置为“打开”状态。 • 阻塞：跟踪的告警因某些原因暂时无法处置需要挂起的建议配置为“阻塞”状态。 • 关闭：已经处置完毕且不需要继续跟踪的告警建议配置为“关闭”状态。
	（可选）责任人	选择告警跟踪或处置的主要责任人。
	数据源产品名称	选择数据源产品的名称，**不支持修改**。
	数据源类型	选择数据源所属类型，**不支持修改**。
时间线	首次发生时间	该条告警首次发生时间。
	最近发生时间	该条告警最近一次发生的具体时间。
	计划关闭时间	选择告警计划关闭时间。
处置建议	推荐处理方法	告警的推荐处置方法描述。
其他	标签	填写告警的标签。
	调试数据	选择是否开启模拟调试功能，**不支持修改**。

参数名称		参数说明
	（可选）验证状态	选择告警的确认状态，标识告警攻击的状态，确认是否造成实际的负面影响。可选择以下状态：未知、攻击成功、攻击失败。 • 未知：无法确认告警是否带来实质的攻击。 • 攻击成功：确认该告警已经攻击成功。 • 攻击失败：确认该告警已经攻击失败。 • 可疑：该告警存在可疑的攻击行为，如攻击尝试。 • 白名单：确认无攻击行为的主机告警。 • 非攻击信息：非恶意攻击，如系统脆弱性告警，风险账号、弱口令等。
	阶段	选择您的告警阶段。 • 准备：准备资源处理告警。 • 检测与分析：检测与分析告警发生原因。 • 控制、清除、恢复：进行告警问题处理。 • 告警后活动：告警处理完成后的后续活动。
	描述	填写告警描述信息，填写规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_()）。 • 长度不能超过 10240 个字符。

步骤 7 单击“确认”。配置完成后，在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面查看告警信息。

----结束

10.2.7 导入或导出告警

操作场景

本章节主要介绍如何导入、导出告警。

- 导入告警：云外资产的告警信息需要通过新增告警或导入告警的方式接入态势感知（专业版）。导入告警支持通过告警列表方式批量创建告警。
- 导出告警：通过导出告警列表到本地，在本地查看告警信息，或者在团队内共享告警信息时可执行该操作。

约束与限制

- 仅支持导入.xlsx 格式的文件，单次导入文件大小不超过 5MB，且单次导入数据不超过 100 条。

- 最多支持导出 9999 条告警信息。

导入告警

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面。

步骤 5 在告警管理页面中，单击告警列表左上角的“更多 > 导入”。

仅支持导入.xlsx 格式的文件，单次导入文件大小不超过 5MB，且单次导入数据不超过 100 条。

步骤 6 在弹出的“导入”对话框中，单击“下载模板”，并根据模板填写要求填写待导入告警信息。

步骤 7 待导入告警文件填写完成后，在导入告警对话框中，单击“添加文件”，选择需要导入的 Excel 文件。

步骤 8 选择完成后，单击“确定”，完成导入。

步骤 9 导入完成后，在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面查看告警信息。

----结束

导出告警

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面。

步骤 5 单击告警列表左上角的“更多 > 导出”，弹出导出对话框，系统默认导出当前告警列表中的全量告警，最多支持导出 9999 条告警信息。同时也支持在告警管理列表中，勾选您需要导出的告警，并单击告警列表左上角的“更多 > 导出”，弹出导出对话框，该场景下仅导出用户勾选的告警。

最多支持导出 9999 条告警信息。

步骤 6 在导出告警对话框中，配置参数。

表 10-19 导出告警

参数名称	参数说明
导出格式	默认导出 excel 格式的告警列表。
自定义导出列	选择导出表格中，需要导出的参数。

步骤 7 单击“确定”。

系统将自动下载告警 excel 表格到本地。

----结束

导出攻击

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面。

步骤 5 在告警管理页面，选择“攻击”页签，进入攻击告警管理页面。

步骤 6 在告警列表中，勾选您需要导出的告警，并单击告警列表左上角的“导出”，弹出导出对话框。

最多支持导出 9999 条告警信息。

步骤 7 在导出告警对话框中，配置参数。

表 10-20 导出告警

参数名称	参数说明
导出格式	默认导出 excel 格式的告警列表。
自定义导出列	选择导出表格中，需要导出的参数。

步骤 8 单击“确定”。

系统将自动下载告警 excel 表格到本地。

----结束

10.2.8 处置攻击

操作场景

本章节介绍如何处置攻击。攻击是原始的告警，支持在态势感知（专业版）侧进行处置，关闭或忽略本次攻击告警。

- 关闭告警：如果告警已手动处理完毕，可以选择关闭本次告警。
- 忽略告警：如果告警风险可控，可以选择忽略本次告警。当相同告警事件再次触发时，将再次告警。

处置攻击

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警管理页面。

步骤 5 在告警管理页面，选择“攻击”页签，进入攻击告警管理页面。

步骤 6 在告警管理列表中，单击目标告警所在行“操作”列的“处置”，右侧弹出攻击处置配置页面。

同时，还可以在某条告警详情页面，单击页面右上角的“处置”。

步骤 7 在处置配置页面，配置攻击处置参数。

表 10-21 处置参数

参数	参数含义
处理方式	• 我已手动处理：如果告警已手动处理完毕，可以选择关闭本次告警。 • 忽略：如果告警风险可控，可以选择忽略本次告警。当相同告警事件再次触发时，将再次告警。
批量处理	同时处理重复告警：如果您希望将不同时间发生的同类告警进行归并，进行批量处理时，可以勾选此按钮。
备注描述	根据需要输入攻击告警处置的备注描述信息。

步骤 8 配置完成后，单击“确定”，界面弹出“告警处置成功”提示信息。

步骤 9 在弹出的攻击处置信息界面，单击“确定”。

----结束

相关操作

- 查看攻击请参见查看攻击信息。
- 导出攻击请参见导出攻击。
- 告警和攻击的区别请参见告警概述。

10.3 情报管理

10.3.1 情报管理概述

威胁情报是描述对系统和用户的现有或潜在威胁的信息，使用威胁情报为异常活动提供必要的上下文，以便安全负责人可以快速采取措施来保护其人员、信息和资产。

威胁情报的形式是情报指标，情报指标是将 URL 或 IP 地址等观察项目与网络钓鱼或恶意软件等已知威胁活动关联起来的数据。它会大规模地应用于安全产品和自动化服务，以检测组织面临的潜在威胁并进行防范。通过情报指标的创建和管理，加快威胁检测和修正。态势感知（专业版）仅支持人工新增情报指标或导入情报指标，创建情报指标后可以通过自定义剧本实现威胁管理分析处理等操作。

情报指标支持如下管理操作：

- 新增情报指标：当发现对系统和用户潜在的威胁信息时，可通过新增情报指标记录威胁信息，以便安全负责人可以快速采取措施来保护其人员、信息和资产，加快威胁检测和修正。
- 编辑情报指标：当情报指标的威胁度、状态、责任人等参数信息发生变化时，支持编辑情报指标，修改情报指标信息。
- 关闭或删除情报指标：当确认情报指标对应的威胁已消除，可关闭情报指标。当确认情报指标信息有误或情报指标所描述的威胁场景不存在，可删除情报指标，**情报指标删除后不可找回，请谨慎操作。**
- 导入指标：支持通过情报指标列表方式批量创建情报指标，提高效率。
- 导出指标：通过导出情报指标列表到本地，在本地查看情报指标信息，或者在团队内共享情报指标信息时可执行该操作。
- 查看情报指标：可以查看情报指标的威胁度、发现时间、状态等信息。支持翻页查看或自定义过滤条件筛选情报指标。

情报指标的来源

- **用户新增情报指标**，具体操作请参见新增情报指标。
- **用户导入情报指标**，具体操作请参见导入指标。

情报指标类型

态势感知（专业版）支持的情报指标类型有 IPv6、URL、邮件、域名、IPv4、其他（文件、漏洞、弱口令等）。新增情报指标时可配置“类型”。

10.3.2 新增或编辑情报指标

操作场景

情报指标库呈现当前您的所有指标信息。

本章节主要介绍如何新建或编辑情报指标。

- 新增情报指标：当发现对系统和用户潜在的威胁信息时，可通过新增情报指标记录威胁信息，以便安全负责人可以快速采取措施来保护其人员、信息和资产，加快威胁检测和修正。
- 编辑情报指标：当情报指标的威胁度、状态、责任人等参数信息发生变化时，支持编辑情报指标，修改情报指标信息。

新增情报指标

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 情报管理”，进入情报管理页面。

步骤 5 在情报管理页面单击“新增”，并在右侧弹出的新增情报管理页面中配置参数。

表 10-22 指标参数说明

参数	说明
指标名称	自定义威胁情报指标名称，命名规则如下： 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。
类型	选择指标类型。可选范围：IPv6、URL、其他、邮件、域名、IPv4。
威胁度	选择威胁度等级。 • 黑：表示危险 • 灰：表示一般 • 白：表示安全
数据源产品名称	选择数据源产品的名称。
数据源类型	选择数据源所属类型，可选择以下类型：云服务、第三方产品、租户私有产品。

参数	说明
状态	选择指标状态，可选择以下状态：打开、关闭、作废。 • 打开 • 关闭：当确认情报指标对应的威胁已消除，可关闭情报指标。 • 作废：当确认情报指标信息有误或情报指标所描述的威胁场景不存在，可作废或删除情报指标，**情报指标删除后不可找回，请谨慎操作。**
置信度	填选指标的可信度，范围为 80~100。
责任人	选择该条指标的主要责任人。
标签	自定义指标的标签。
首次发生时间	选择该条指标首次发生时间。
最近发生时间	选择该条指标最近一次发生的具体时间。
失效时间	选择该指标的失效时间。
是否失效	选择是否失效该条指标。默认为“否”。
粒度	选择该指标的粒度。
显示名称	当“类型”选择“邮件”时，可以自定义配置邮件的显示名称。
家族	当“类型”选择“域名”时，可以自定义配置域名所属家族。
邮箱账户	当“类型”选择“IPv6”、“IPv4”、“邮件”或“域名”时，可以自定义配置邮箱账户信息。
地区	当“类型”选择“IPv6”或“IPv4”时，可以自定义配置 IP 地址所属地区。
URL	当“类型”选择“URL”时，可以自定义配置 URL 信息。
DNS 类别	当“类型”选择“域名”时，可以自定义配置域名的 DNS 类别。
描述	自定义配置指标的描述信息。
值	填写指标的值，如 IP、URL、Domain 等。

步骤 6 单击“确认”。

----结束

编辑情报指标

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 情报管理”，进入情报管理页面。

步骤 5 在情报管理页面中，单击目标情报所在行“操作”列的“编辑”，右侧弹出编辑情报页面。

步骤 6 在弹出的编辑情报指标页面中，编辑指标参数。

表 10-23 指标参数说明

参数	说明
指标名称	自定义威胁情报指标名称，命名规则如下： 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。
类型	选择指标类型。
威胁度	选择威胁度等级。 • 黑：表示危险 • 灰：表示一般 • 白：表示安全
数据源产品名称	选择数据源产品的名称，**不支持修改**。
数据源类型	选择数据源所属类型，**不支持修改**。
状态	选择指标状态，可选择以下状态：打开、关闭、作废。
置信度	填选指标的可信度，范围为 80~100。
责任人	选择该条指标的主要责任人。
标签	自定义指标的标签。
首次发生时间	选择该条指标首次发生时间。
最近发生时间	选择该条指标最近一次发生的具体时间。
失效时间	选择该指标的失效时间。
是否失效	选择是否失效该条指标。默认为“否”。
粒度	选择该指标的粒度。
MD5	自定义填写情报指标的 MD5 值。
SHA1	自定义填写情报指标的 SHA1 值。
SHA256	自定义填写情报指标的 SHA256 值。

参数	说明
文件类型	自定义填写情报指标的文件类型。
编译时间	自定义填写情报指标的编译时间。
文件名	自定义填写情报指标的文件名。
文件 mime 类型	自定义填写情报指标的文件 mime 类型。
家族	自定义填写情报指标的所属家族信息。
类别	自定义填写情报指标的类别。

步骤 7 单击“确认”。

----结束

10.3.3 关闭或删除情报指标

操作场景

本章节主要介绍如何关闭和删除情报指标。

- 关闭情报指标：当确认情报指标对应的威胁已消除，可关闭情报指标。
- 删除情报指标：当确认情报指标信息有误或情报指标所描述的威胁场景不存在，可删除情报指标，**情报指标删除后不可找回，请谨慎操作。**

关闭或删除情报指标

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 情报管理”，进入情报管理页面。

步骤 5 在情报管理页面中，对情报进行关闭或删除操作。

表 10-24 管理情报

操作	操作说明
关闭情报	1. 在情报管理页面，单击目标情报所在行“操作”列的“关闭”，弹出关闭情报确认框。 2. 在弹出的关闭情报确认框中，选择“关闭原因”，并填写评论信息。 3. 单击“确认”。

操作	操作说明
删除情报	1. 在情报管理页面中，单击目标情报所在行“操作”列的“删除”，弹出删除确认框。 2. 确认无误后，在弹出的确认框中，单击“确认”。 说明 指标删除后，不可找回，请谨慎操作。

----结束

10.3.4 导入或导出情报指标

操作场景

本章节主要介绍如何导入、导出情报指标。

- 导入指标：支持通过情报指标列表方式批量创建情报指标，提高效率。
- 导出指标：通过导出情报指标列表到本地，在本地查看情报指标信息，或者在团队内共享情报指标信息时可执行该操作。

约束与限制

- 仅支持导入.xlsx 格式的文件，单次导入文件大小不超过 5MB，且单次导入数据不超过 100 条。
- 最多支持导出 9999 条情报指标信息。

导入指标

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 情报管理”，进入情报管理页面。

步骤 5 在情报管理页面中，单击指标列表左上角的“导入”。

仅支持导入.xlsx 格式的文件，单次导入文件大小不超过 5MB，且单次导入数据不超过 100 条。

步骤 6 在弹出的“导入”对话框中，单击“下载模板”，并根据模板填写要求填写待导入情报指标信息。

步骤 7 待导入情报指标文件填写完成后，在导入情报指标对话框中，单击“添加文件”，选择需要导入的 Excel 文件。

步骤 8 选择完成后，单击“确定”，完成导入。

----结束

导出指标

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 情报管理”，进入情报管理页面。

步骤 5 在情报管理页面中，勾选您需要导出的指标，并单击列表右上角的，弹出导出对话框。

最多支持导出 9999 条情报指标信息。

步骤 6 在导出指标对话框中，配置参数。

表 10-25 导出指标

参数名称	参数说明
导出格式	默认导出 excel 格式的指标列表。
自定义导出列	选择导出表格中，需要导出的参数。

步骤 7 单击“确定”。

系统将自动下载指标 excel 表格到本地。

----结束

10.3.5 查看情报指标

操作场景

本章节主要介绍如何查看已有情报指标信息。

- 查看情报指标：可以查看情报指标的威胁度、发现时间、状态等信息。支持翻页查看或自定义过滤条件筛选情报指标。

查看情报指标

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 情报管理”，进入情报管理页面。

步骤 5 在情报管理页面查看情报指标信息。

表 10-26 查看情报指标信息

参数名称	参数说明
情报类型	呈现所有类型情报指标总数及对应类型下情报指标数量。
超期情报	呈现已超过威胁情报指标设置的失效时间，且还未关闭的威胁情报指标总数。
情报状态	呈现不同状态的情报指标总数及对应状态下情报指标数量。 • 关闭：已经关闭的情报指标数量。 • 作废：已经作废的情报指标数量。 • 打开：处于打开状态的情报指标数量。
威胁度	呈现不同威胁程度对应的情报指标数量。 • 黑：表示危险，威胁程度为黑的情报指标数量。 • 灰：表示一般，威胁程度为灰的情报指标数量。 • 白：表示安全，威胁程度为白的情报指标数量。
情报管理列表	展示情报的详细信息。 在情报指标列表中下方可以查看情报指标总条数。其中，使用翻页查看时最多可查看 10000 条情报指标信息，如果需要查看超过 10000 条以外数据，请优化过滤条件筛选数据。 情报指标列表中，可以查看情报的威胁度、发现时间、状态等信息。如需查看某个指标详细信息，可单击指标名称，页面右侧将展示指标的详细信息。 • 在情报概览页面可以查看情报的基本信息和关联信息（包括关联的威胁指标、告警、事件）。 • 在**关联信息**中，可以将情报指标和其他情报指标、告警和事件进行绑定或解绑操作。

----结束

11 日志审计

11.1 日审总览

11.1.1 查看日审总览

“日审总览”页面呈现统计周期内当前工作空间中整体日志审计状况。

查看日审总览

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 日审总览”，进入日审总览页面。

步骤 5 在日审总览页面查看整体日志审计状况，具体展示信息如下：

表 11-1 日志审计总览展示内容说明

参数模块	参数说明
统计周期	日志审计的统计周期，可以在右上角设置显示周期。可以选择周期范围： • 昨天 • 上一周 • 上一月 • 自定义：自定义日志审计报告的开始日期和结束日期。

参数模块	参数说明
日志存储	展示统计周期内日志总览和日志流速情况，包含以下信息： • 总览 – 日志源数及其较上期变化 – 当前日志存储量及其较上期变化 – 日志记录总条数及其较上期变化 • 日志流速 – 日志平均每秒流入速率 – 日志平均每秒流入吞吐 – 日志平均日记录数 – 日志平均日存储量 – 日志记录数变化趋势 – 日志源接入流量 TOP5 – 日志源接入数量分布 TOP5
主机安全审计	统计周期内，HSS 的安全日志和告警日志审计情况，包含以下信息： • 活跃主机数及其较上期变化 • 主机登录源 IP 数及其较上期变化 • 主机告警次数及其较上期变化 • 活跃主机 Top5 • 主机登录源 IP 分布 Top5 • 主机告警源 IP 分布 Top5 • 主机告警类型 Top5 分布 • 主机稀有告警类型 Top5 分布

参数模块	参数说明
公网网络审计	统计周期内，NDR 的攻击日志和流量日志、DDoS 的攻击日志审计情况，包含以下信息： • NDR 审计 – 公网来访流量（源 IP） Top5 – 访问公网流量（源 IP） Top5 – 公网来访范围（源 IP） Top5 – 访问公网范围（源 IP） Top5 – 网络攻击类型 Top5 • DDoS 审计 – DDoS 攻击次数及其较上期变化 – DDoS 攻击源 IP 数及其较上期变化 – DDoS 攻击次数变化趋势 – DDOS 攻击来源 IP Top5
应用访问审计	统计周期内，WAF 的攻击日志和访问日志审计情况（核心审计对象为：应用、网络和域名），包含以下信息： • 活跃域名数量及其较上期变化 • WAF 访问源 IP 数及其较上期变化 • WAF 攻击次数及其较上期变化 • WAF 拦截次数及其较上期变化 • WAF 访问源 IP Top5 • WAF 攻击源 IP Top5 • WAF 拦截源 IP Top5 • WAF 攻击类型 Top5 • 活跃域名访问频次 Top5
数据库访问审计	统计周期内，DBSS 的告警日志审计情况（核心审计对象为：用户、数据库和操作），包含以下信息： • 活跃数据库数及其较上期变化 • 数据库活跃用户数及其较上期变化 • 数据库告警源 IP 数及其较上期变化 • SQL 执行种类数及其较上期变化 • 活跃数据库 IP Top5 • 数据库活跃用户 Top5 • SQL 执行类型 Top5 • 数据库用户源 IP 数 Top5

----结束

11.2 安全分析

11.2.1 安全分析概述

态势感知（专业版）的安全分析功能是一种云原生安全信息和事件管理（SIEM）解决方案，支持采集多产品的安全日志及告警，并基于预定义和自定义的安全检测规则对多来源的告警及日志进行聚合分析，旨在帮助企业快速发现和响应安全事件，实现对云负载、各类应用及数据的安全保护。

支持接入的云产品和日志

态势感知（专业版）支持集成多种云产品的日志数据。集成后，可以检索并分析所有收集到的日志。

具体支持接入的云服务日志请参见支持接入的云服务日志。

使用流程

表 11-2 使用流程

子流程	说明
新增工作空间	新增工作空间，用于资源隔离和控制。
云服务接入	配置需要接入的数据源。 态势感知（专业版）支持集成存储、管理与监管、安全等多种云产品的日志数据。集成后，可以检索并分析所有收集到的日志。
（可选）新增数据空间	创建用于存储收集日志数据的数据空间。 通过控制台接入的数据，系统将创建默认数据空间，无需再进行创建。
（可选）创建管道	创建用于日志数据的采集、存储和查询的数据管道。 通过控制台接入的数据，系统将创建默认数据管道，无需再进行创建。
配置索引	配置索引条件，缩小查询范围。
查询与分析	对接入的数据进行查询、分析。
下载日志	支持将原始日志或查询分析后的日志下载到本地。
查看图表统计结果	当您执行了查询分析语句后，态势感知（专业版）支持通过图表统计的形式对查询和分析的结果进行可视化展示。 目前支持表格、折线图、柱状图和饼图方式进行展示。

11.2.2 配置索引

安全分析中的索引是一种存储结构，用于对日志数据中的一列或多列进行排序。不同的索引配置，将会产生不同的查询和分析结果，请根据您的需求合理配置索引。

如果您需要使用分析功能，必须配置字段索引。配置字段索引后，您可以指定字段名称和字段值（Key:Value）进行查询，缩小查询范围。例如查询语句 level:error，表示查询 level 字段值包含 error 的日志。

约束与限制

- 仅自定义新增的管道支持自定义配置索引，新增管道详细操作请参见创建管道。
- 配置字段索引不支持删除操作。

配置字段索引

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

步骤 6 在数据管道检索页面，单击右上角“索引配置”，页面右侧展示索引配置页面。

步骤 7 在索引配置页面中，配置索引参数。

1. 开启索引状态。

   索引状态默认开启，索引状态关闭时，将无法索引和查询采集到的日志。

2. 配置索引参数，参数配置说明如表 11-3 所示。

表 11-3 索引配置参数说明

参数名称	参数说明
字段名称	日志字段名称（key）。
字段类型	日志字段值（value）的数据类型，可选值为 text、keyword、long、integer、double、float、date 和 json。

参数名称	参数说明
包含中文	查询时是否区分中英文。当字段类型选择“text”时，需要设置该参数。 • 开启开关后，如果日志中包含中文，则按照中文语法拆分中文内容，按照分词符配置拆分英文内容。 • 关闭开关后，按照分词符配置拆分所有内容。 示例：日志内容为：**user:WAF 日志用户张三**。 • 关闭“包含中文”开关后，按照分词符半角冒号（:）进行拆分，日志会被拆分为 user、WAF 日志用户张三，您可以通过 user 或 WAF 日志用户张先生查找该日志。 • 开启“包含中文”开关后，日志服务后台分词器将日志拆分为 user、WAF、日志、用户和张三，您通过日志或张先生等词都可以查找到该日志。

步骤 8 单击“确定”。

----结束

11.2.3 查询与分析日志

操作场景

数据收集成功后，您可以在查询分析页面对收集到的日志数据进行实时查询分析。

本章节将介绍如何对日志数据进行查询分析，请根据您的需要选择查询分析方式：

- 方式一：输入查询条件进行查询分析
- 方式二：使用已有字段进行查询分析
- 方式三：创建快速查询
- 操作查询分析结果

前提条件

已完成数据接入，详细操作请参见云服务接入。

输入查询条件进行查询分析

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

步骤 6 在管道数据检索页面，输入查询分析语句。

查询分析语句由查询语句和分析语句构成，格式为**查询语句|分析语句**，查询分析语句语法详细内容请参见查询与分析语法概述。

如果筛留字段为 text 类型时，默认会使用 MATCH_QUERY 进行分词查询。

步骤 7 单击“15 分钟（相对）”，设置查询时间范围。

您可以选择相对时间（15 分钟、1 小时、24 小时），或自定义查询时间。

步骤 8 单击“查询/分析”，查看查询分析结果。

----结束

使用已有字段进行查询分析

本部分将介绍如何使用已有字段对接入日志进行查询分析。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击默认数据空间名称，展开数据管道列后，单击管道名称，右侧将显示管道数据的检索页面。

步骤 6 设置查询条件。

如果筛留字段为 text 类型时，默认会使用 MATCH_QUERY 进行分词查询。

- 在原始日志中，单击左侧可选字段前的，并单击待筛选字段名称后的（筛选某字段值），查询框中将按照已筛选的字段进行查询。如果需要排除某字段值，可以单击该字段名称前的。

图 11-2 筛选某字段值（一）

- 如果您已展开某时间点的具体日志数据，需要筛选某些字段，可以单击该字段名称前的（筛选某字段值），查询框中将按照已筛选的字段进行查询。如果需要排除某字段值，可以单击该字段名称前的。

图 11-3 筛选某字段值（二）

步骤 7 默认查询并显示最近 15 分钟内数据。如果需要查询其他时间段日志数据，则需要设置查询时间，并单击“查询/分析”。

----结束

创建快速查询

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

步骤 6 输入查询分析语句，设置时间范围，并单击“查询/分析”。

更多查询分析详细操作请参见输入查询条件进行查询分析。

步骤 7 单击页面右上角“保存为快速查询”，在右侧页面中配置查询参数。

表 11-4 快速查询参数配置

参数名称	参数说明
查询名称	设置快速查询的名称。
查询语句	系统自动生成步骤 6 中输入的查询语句。

步骤 8 单击“确定”。

创建快速查询后，您可以在管道数据的查询分析页面中，单击快速查询搜索框中的，并选择目标快速查询名称，即可使用快速查询。

----结束

操作查询分析结果

态势感知（专业版）通过**原始日志**、**日志分布直方图**、**图表统计**形式展示查询分析结果。

- **日志分布直方图**

此处将展示查询到的日志在时间上的分布情况，同时，将鼠标放在柱状图上，可查看该数据块代表的时间和日志命中次数。

图 11-4 日志分布直方图

- **原始日志**

  在“原始日志”页签将展示当前查询结果。

  图 11-5 原始日志

  - 设置显示日志数据信息：
    - 页面中默认展示最近 15 分钟内的日志数据，如果需要展示其他时间数据，可以在右上角选择展示的时间。

      图 11-6 选择显示时间

    - 如需查看某时间所有字段中的数据，可单击表格中对应时间前方的展开所有数据，默认展示以表格形式展示数据。

      如需查看 JSON 格式数据，可以选择“JSON”页签，页面将展示 JSON 格式的数据。

      图 11-7 展开显示数据

    - 如需在列表中展示/筛选某些字段信息，可在右侧可选字段中选择需展示的字段，并单击字段名称后的，该字段将显示在右侧日志数据列表中。

      图 11-8 选中显示字段

      - 字段选中后，如需**调整显示先后顺序**，可在右侧日志数据列表的表头列单击该字段名称后的（向左移一列）、（向右移一列）按钮来进行调整。

图 11-9 调整顺序

□ 字段选中后，如需**取消**，可在右侧日志数据列表的表头列单击该字段名称后的按钮来进行取消，或左侧在“选定字段”单击该字段名称后的按钮来取消显示。

图 11-10 取消选择

- 导出日志：在原始日志页签，在页面右上方单击图标，系统将自动下载当前原始日志表格到本地。

- **图表统计**

  查询语句查询后，在“图表统计”页签可以查看可视化的查询分析结果。

  图表统计是态势感知（专业版）根据查询分析语句渲染出的结果，提供有表格、线图、柱状图、饼图等多种图表类型，详细信息请参见查看图表统计结果。

- **告警**

  在查询分析页面右上角单击“添加告警”，可以将查询分析结果设置告警，详细信息请参见快速添加日志告警模型。

- **快速查询**

  在查询分析页面右上角单击“保存为快速查询”，可以将某一查询分析条件保存为快速查询，详细信息请参见创建快速查询。

11.2.4 日志字段含义

本章节将介绍各字段的含义。

- 通用字段：通用字段含义。
- sec-waf-attack：WAF 攻击日志字段含义。
- sec-waf-access：WAF 访问日志字段含义。
- sec-obs-access：OBS 访问日志字段含义。
- sec-nip-attack：IPS 攻击日志字段含义。
- sec-iam-audit：IAM 审计日志字段含义。
- sec-hss-vul：HSS 主机漏洞扫描结果字段含义。
- sec-hss-alarm：HSS 主机安全告警字段含义。
- sec-hss-log：HSS 主机安全日志字段含义。
- sec-ddos-attack：DDoS 攻击日志字段含义。
- sec-cts-audit：CTS 日志字段含义。
- sec-cfw-risk：CFW 攻击事件日志字段含义。
- sec-cfw-flow：CFW 流量日志字段含义。

- sec-cfw-block：CFW 访问控制日志字段含义。
- sec-apig-access：API 网关的访问日志字段含义。
- sec-dbss-alarm：DBSS 告警日志字段含义。
- sec-dsc-alarm：DSC 告警日志字段含义。

通用字段

表 11-5 通用字段

字段名	字段类型	字段含义
__time	Date	日志产生的时间
__raw	String	原始日志
ops.source	String	数据源名称
ops.rgn	String	所属局点
ops.csvc	String	数据源(云服务)
ops.ver	String	数仓版本号
ops.hash	String	extend hash value of original 数据完整性验证
[src_/dest_]asset.domain.id	String	租户 id
[src_/dest_]asset.domain.name	String	租户名
[src_/dest_]asset.id	String	资产 id
[src_/dest_]asset.name	String	资产名称
[src_/dest_]asset.type	String	资产类型
[src./dest.]asset.region	String	资产局点
[src_/dest_]geo.ip	String	ip 地址
[src_/dest_]geo.country	String	国家(中文)
[src_/dest_]geo.prov	String	省份（中文）
[src_/dest_]geo.city	String	城市名称（中文）
[src_/dest_]geo.org	String	注册 IP 的组织
[src_/dest_]geo.isp	String	运营商
[src_/dest_]geo.loc.lat	Float	纬度
[src_/dest_]geo.loc.lon	Float	经度

字段名	字段类型	字段含义
[src_/dest_]geo.tz	Integer	时区
[src_/dest_]geo.utc_off	Integer	时区
[src_/dest_]geo.cac	String	时区
[src_/dest_]geo.iddc	String	国际电话前缀码
[src_/dest_]geo.cc	String	国家编码 ISO
[src_/dest_]geo.contc	String	大洲编码 ISO
[src_/dest_]geo.idc	String	数据中心，机房
[src_/dest_]geo.bs	String	移动基站
[src_/dest_]geo.cc3	String	国家代码 3 位
[src_/dest_]geo.euro	String	欧盟成员国

sec-waf-attack

WAF 攻击日志字段含义如下所示：

表 11-6 sec-waf-attack

字段	类型	字段含义
category	String	分类，此处值为“attack”。
time	Date	标识日志时间。
time_iso8601	Date	标识日志的 ISO 8601 格式时间。
policy_id	String	标识防护策略 ID。
level	Integer	标识防护策略层级（1 为宽松，2 为中等，3 为严格）。

字段	类型	字段含义
attack	String	标识攻击类型。攻击类型的解释为： • default：默认 • xss：跨站脚本攻击 • sqli：SQL 注入攻击 • cmdi：命令注入攻击 • lfi：本地文件包含 • rfi：远程文件包含 • webshell：WebShell 攻击 • robot：爬虫攻击（根据 UA 黑名单拦截） • vuln：漏洞攻击 • cc：命中 CC 规则 • custom_custom：命中精准防护规则 • custom_whiteip：命中白名单规则 • custom_geoip：命中地理位置规则 • illegal：非法请求 • anticrawler：命中反爬虫规则（JS 挑战） • antitamper：命中防篡改规则 • leakage：命中隐私泄露规则 • followed_action：攻击惩罚 • trojan：网站木马
action	String	标识处理动作。处理动作的解释为： • block：拦截 • log：仅记录 • captcha：人机验证
rule	String	标识触发的规则 ID 或者自定义的策略类型描述。

字段	类型	字段含义
sub_type	String	当 attack 为 robot 时，该字段不为空。标识爬虫的子类型。 • script_tool：脚本工具 • search_engine：搜索引擎 • scaner：扫描工具 • uncategorized：其他爬虫
location	String	标识触发的 payload 的位置。
resp_headers	String	标识响应头。
resp_body	String	标识响应体。
hit_data	String	标识触发的 payload 字符串。
status	String	标识请求的响应状态码。
reqid	String	随机 ID 标识。
id	String	攻击 ID。
method	String	标识请求方法。
sip	String	标识客户端请求 IP。
sport	String	标识客户端请求端口。
host	String	标识请求的服务器域名。
http_host	String	标识请求的服务器端口。
uri	String	标识请求 URL。
header	String	标识请求 header 信息。
mutipart	String	标识请求 multipart header（文件上传场景）。
cookie	String	标识请求 cookie 信息。
params	String	标识请求 URI 后的参数信息。
body_bytes_sent	String	标识发送给客户端的响应体字节数。
upstream_response_time	String	标识后端服务器响应时间。
process_time	String	标识引擎的检测用时。
engine_id	String	标识引擎的唯一标识。
group_id	String	用于对接 LTS 服务的日志组 ID。

字段		类型	字段含义
attack_stream_id		String	与 group_id 相关，是日志组下用户的 access_stream 的 ID。
hostid		String	标识防护域名 ID。
tenantid		String	标识防护域名的租户 ID。
projectid		String	标识防护域名的项目 ID。
backend		Object	标识请求转发的后端服务器地址。
backend	type	String	标识当前后端 Host 类型（IP 或域名）。
	alive	String	标识当前后端状态。
	host	String	标识当前后端 Host 值。
	protocol	String	标识当前后端协议。
	port	Integer	标识当前后端端口。

sec-waf-access

WAF 访问日志字段含义如表 11-7 所示。

表 11-7 sec-waf-access

字段	类型	字段含义
requestid	String	随机 ID 标识。
time	Date	标识日志时间。
eng_ip	String	标识引擎 IP。
hostid	String	标识防护域名 ID。
tenantid	String	标识防护域名的租户 ID。
projectid	String	标识防护域名的项目 ID。
remote_ip	String	标识请求的客户端 IP。
scheme	String	标识请求协议类型。
response_code	String	标识请求响应码。
method	String	标识请求方法。
http_host	String	标识请求的服务器域名。

字段	类型	字段含义
url	String	标识请求 URL。
request_length	String	标识请求长度。
bytes_send	String	标识发送给客户端的总字节数。
body_bytes_sent	String	标识发送给客户端的响应体字节数。
upstream_addr	String	标识选择的后端服务器地址。
request_time	String	标识请求处理时间，从读取客户端的第一个字节开始计时。
upstream_response_time	String	标识后端服务器响应时间。
upstream_status	String	标识后端服务器的响应码。
upstream_connect_time	String	标识后端服务器连接用时。
upstream_header_time	String	标识后端服务器接收到第一个响应头字节的用时。
bind_ip	String	标识引擎回源 IP。
engine_id	String	标识引擎的唯一标识。
time_iso8601	Date	标识日志的 ISO 8601 格式时间。
sni	String	标识通过 SNI 请求的域名。
tls_version	String	标识建立 SSL 连接的协议版本。
ssl_curves	String	标识客户端支持的曲线列表。
ssl_session_reused	String	标识 SSL 会话是否被重用。 • 重用：r • 未重用：.
process_time	String	标识引擎的检测用时。
x_forwarded_for	String	标识请求头中 X-Forwarded-For 的内容。
cdn_src_ip	String	标识请求头中 Cdn-Src-Ip 的内容。
x_real_ip	String	标识请求头中 X-Real-Ip 的内容。

sec-obs-access

对象存储服务访问日志字段含义如下所示：

表 11-8 sec-obs-access

字段	类型	字段含义
srcip	String	访问 obs 的源 ip。
srcport	String	访问 obs 的源端口。
logtime	Date	日志记录时间。
ces_log_version	String	内部请求为 V0，V0 不记录 CES 审计日志，V1 记录 CES 审计日志。
request_start_time	String	请求开始时间。
ctx_request_id	String	请求 ID，请求跟踪的唯一标识。
request_method	String	请求方法（get/post）。
remote_ip	String	客户端 IP:端口。
operation	String	操作类型，如 GET.OBJECT。
bucket_name	String	桶名。
object_name	String	对象名（文件名）。
query_string	String	请求 query。
http_status	String	http 请求状态码，如 200。
content_length	String	请求内容长度。
user_agent	String	客户端 agent。
storage_class	String	对象存储类型。
user_name	String	请求者用户名称。
user_id	String	请求者用户 ID。
domain_name	String	请求者账号名称。
domain_id	String	请求者账号 ID。
project_id	String	请求者项目 ID。
owner_domain_name	String	桶 owner 租户名称。
owner_domain_id	String	桶 owner 租户 ID。
owner_project_id	String	桶 owner 项目 ID。
transmission_type	String	网络类型： • 1：内网 • 2：公网
scheme	String	网络协议。

字段	类型	字段含义
http_version	String	http 版本。
host	String	服务 obs 域名。
port	String	端口。
auth_v2_v4	String	鉴权方式。
host_type	String	访问方式。
x_forwarded_for	String	代理客户端 IP。
pub_bkt	String	是否为匿名访问桶。
pub_obj	String	是否为匿名访问对象。
website_req	String	是否为 website 请求。
crr_req	String	是否为 crr 请求。
batch_delete_success_count	String	批删成功个数。
ctc_log_urn	String	委托。
requester	String	委托账号。
is_over_write	String	是否为覆盖写。
error_code	String	错误原因。
detail_error_code	String	详细错误原因。
request_content_type	String	请求对象类型。
request_content_md5	String	请求对象 md5。
total_bytes_received	String	接收到内容总数。
response_content_type	String	响应对象类型。
total_bytes_sent	String	发送内容总数响应头+响应 BODY 体。
referrer	String	引用页。
index_read_count	String	查询元数据表时延。
persistence_read_count	String	读数据的次数。
vpc_id	String	标识请求客户端所属的 VPCID。
access_with_security_token	String	使用 sts token。
copy_size	String	copy_size。
vpcep_traffic	String	走 EP

字段	类型	字段含义
access_key	String	ak。

sec-nip-attack

IPS 攻击日志字段含义如下所示：

表 11-9 sec-nip-attack

字段	类型	字段含义
SyslogId	String	日志序号。
Vsys	String	虚拟系统名称。
Policy	String	安全策略名称。
SrcIp	String	报文的源 IP 地址
DstIp	String	报文的目的 IP 地址
SrcPort	String	报文的源端口（对于 ICMP 报文，该字段为 0）。
DstPort	String	报文的目的端口（对于 ICMP 报文，该字段为 0）。
SrcZone	String	报文的源安全域。
DstZone	String	报文的目的安全域。
User	String	用户名。
Protocol	String	签名检测到的报文所属协议。
Application	String	签名检测到的报文所属应用。
Profile	String	配置文件的名称。
SignName	String	签名的名称。
SignId	String	签名的 ID。
EventNum	String	日志归并引入字段，是否归并需根据归并频率及日志归并条件来确定，不发生归并则为 1。

字段	类型	字段含义
Target	String	签名所检测的报文所攻击的对象。具体情况如下： • server：攻击对象为服务端。 • client：攻击对象为客户端。 • both：攻击对象为服务端和客户端。
Severity	String	签名所检测的报文所造成攻击的严重性。具体情况如下： • information：表示严重性为提示。 • low：表示严重性为低。 • medium：表示严重性为中。 • high：表示严重性为高。
Os	String	签名所检测的报文所攻击的操作系统。具体情况如下： • all：所有系统。 • android：安卓系统。 • ios：苹果系统。 • unix-like：Unix 系统。 • windows：Windows 系统。 • other：其他系统。
Category	String	签名检测到的报文攻击特征所属的威胁分类。
Action	String	签名动作。 • alert：签名动作为告警。 • block：签名动作为阻断。
Reference	String	签名的参考信息。
Extend	String	增强模式下的取证字段。

sec-iam-audit

统一身份认证审计日志字段含义如下所示：

表 11-10 sec-iam-audit

字段	类型	字段含义
uid	String	用户 id。

字段	类型	字段含义
un	String	用户名。
did	String	租户 id。
dn	String	租户名。
src	String	请求域名。
opl	String	操作级别。
op	String	操作类型。
res	String	IAM 服务调用结果。
ter	String	源 ip。
dtl	String	iam 认证详情。
tn	Date	发生时间。
ts	Long	iam 服务调用的发生时间戳。
tid	String	traceid。
evnt	String	事件。
tobj	String	操作服务。

sec-hss-vul

主机漏洞扫描结果字段含义如下所示：

表 11-11 sec-hss-vul

字段	类型	字段含义
agentUuid	String	agent 的 UUID。
alarmCsn	String	告警 UUID，master 生成告警时随机生成。
alarmKey	String	告警关键字。对于告警，当前透传 agent 上报的信息 msg_id；对于漏洞，由 master 生成。
alarmVersion	String	agent 版本号。
occurTime	Int64	漏洞检测时间（ms）。
severity	Int32	HSS 定义的漏洞等级。
hostUuid	String	受影响主机 UUID。

字段		类型	字段含义
hostName		String	受影响主机名。
hostIp		String	受影响主机通信 IP。
ipList		String	受影响主机 IP 列表。
cloudId		String	cloudagent sn。
region		String	受影响主机所在区域。
projectId		String	项目 ID。
enterpriseProjectId		String	企业项目 ID。
appendInfo		Object	漏洞详情。
appendInfo	vulId	String	漏洞官方 ID。
	type	Int32	漏洞类型。 • 0：linux • 1：windows • 2：webcms
	repairNecessity	Int32	漏洞修复必要性级别。 • 1：低危 • 2&3：中危 • 4：高危
	status	Int32	保留字段。
	cve_ids	String	CVE ID 列表，通过英文逗号连接。
	url	String	漏洞详情官网链接。
	vulNameEn	String	漏洞英文名。
	vulNameCn	String	漏洞中文名。
	severityLevel	String	漏洞危害级别，分为如下等级： • Critical：严重 • High：高 • Medium：中 • Low：低
	descriptionEn	String	漏洞英文描述。
	descriptionCn	String	漏洞中文描述。
	solutionEn	String	解决方案英文描述。

字段		类型	字段含义
	solutionCn	String	解决方案中文描述。
	repairCmd	String	修复命令。
	needBoot	Int32	是否需要重启；当前默认 1，暂时不用。
	errorInfo	String	修复失败原因。
	appName	String	存在漏洞的软件名（linux 漏洞特有）。
	version	String	存在漏洞的软件版本（linux 漏洞特有）。
	createTime	Int64	首次检测时间（ms）。
	updateTime	Int64	漏洞修复时间（ms）；初始值同 createTime。
	agentId	String	关联主机 agent 的 UUID。
	projectId	String	受影响租户 ID。

sec-hss-alarm

主机安全告警日志字段含义如下所示：

表 11-12 sec-hss-alarm

字段	类型	字段含义
agentUuid	String	agent 的 UUID。
alarmCsn	String	告警 UUID。
alarmKey	String	告警关键字。对于告警，当前透传 agent 上报的信息 msg_id；对于漏洞，由 master 生成。
alarmVersion	String	agent 版本号。
occurTime	Long	事件发生时间（ms）。
severity	Long	风险等级。
hostUuid	String	受影响主机 UUID。
hostName	String	受影响主机名。
hostIp	String	受影响主机通信 IP。

字段		类型	字段含义
ipList		String	受影响主机 IP 列表。
cloudId		String	cloudagent sn。
region		String	受影响主机所在区域。
projectId		String	项目 ID。
enterpriseProjectId		String	企业项目 ID。
appendInfo		Object	告警详情。
appendInfo	agent_id	String	AGENT ID。
	version	String	事件版本。
	container_name	String	容器 ID（容器安全场景）。
	image_name	String	镜像名称（容器安全场景）。
	event_id	String	事件 ID，GUID。
	event_name	String	事件名称。
	event_classid	String	事件唯一标识。
	occur_time	Long	发生时间（秒）。
	recent_time	Long	最近一次发生时间（秒）。
	event_category	Integer	事件大类。
	event_type	Integer	事件类型。
	event_count	Integer	事件次数。
	severity	Integer	严重级别。
	attack_phase	Integer	攻击阶段。
	attack_tag	Integer	攻击标识。
	confidence	Integer	置信度。
	action	Integer	动作类型。
	detect_module	String	检测模块。
	report_source	String	上报源。
	related_events	String	相关事件 ID。
	resource_info	Object	资源信息。
	network_info	Object	网络信息。
	app_info	Object	应用信息。

字段			类型	字段含义
	system_info		Object	系统信息。
	process_info		list	进程信息。
	user_info		list	用户信息。
	file_info		list	文件信息。
	geo_info		Object	地理信息。
	malware_info		Object	恶意软件信息。
	forensic_info		String	取证字段。
	recommendation		String	处置建议。
	extend_info		String	事件扩展信息。
	resource_info	project_id	String	项目 ID。
		region_name	String	Region 名称。
		vpc_id	String	VPC ID。
		host_name	String	主机名称。
		host_ip	String	主机 IP。
		host_id	String	主机 ID（ECS 对应 ID）。
		cloud_id	String	CloudAgent SN。
		vm_name	String	虚拟机名称。
		vm_uuid	String	虚拟机 UUID。
		container_id	String	容器 id。
		image_id	String	镜像 id。
		sys_arch	String	系统 CPU 架构。
		os_bit	String	操作系统位数。
		os_type	String	操作系统类型。
		os_name	String	操作系统名称。
		os_version	String	操作系统版本。
	network_info	local_address	String	本地地址。
		local_port	Integer	本地端口。

字段			类型	字段含义
		remote_address	String	远程地址。
		remote_port	Integer	远程端口。
		src_ip	String	源 IP。
		src_port	Integer	源端口。
		src_domain	String	源域。
		dest_ip	String	目的 IP。
		dest_port	Integer	目的端口。
		dest_domain	String	目的域。
		protocol	String	协议。
		app_protocol	String	应用层协议。
		flow_direction	String	流量方向。
	app_info	sql	String	执行的 sql 语句。
		domain_name	String	DNS 域名。
		url_path	String	URL 路径。
		url_method	String	URL 方法。
		req_refer	String	URL 请求 refer 信息。
		email_subject	String	邮件主题。
		email_sender	String	邮件发送者。
		email_receiver	String	邮件接收者。
		email_keyword	String	邮件关键字。
	process_info	process_name	String	进程名称。
		process_path	String	进程文件路径。

字段			类型	字段含义
		process_pid	Integer	进程 id。
		process_uid	Integer	进程用户 id。
		process_username	String	运行进程的用户名。
		process_cmdline	String	进程文件命令行。
		process_filename	String	进程文件名。
		process_start_time	Long	进程启动时间。
		process_gid	Integer	进程组 ID。
		process_egid	Integer	进程有效组 ID。
		process_euid	Integer	进程有效用户 ID。
		parent_process_name	String	父进程名称。
		parent_process_path	String	父进程文件路径。
		parent_process_pid	Integer	父进程 id。
		parent_process_uid	Integer	父进程用户 id。
		parent_process_cmdline	String	父进程文件命令行。
		parent_process_filename	String	父进程文件名。
		parent_process_start_time	Long	父进程启动时间。
		parent_process_gid	Integer	父进程组 ID。
		parent_process_egid	Integer	父进程有效组 ID。

字段			类型	字段含义
		parent_process_euid	Integer	父进程有效用户 ID。
		child_process_name	String	子进程名称。
		child_process_path	String	子进程文件路径。
		child_process_pid	Integer	子进程 id。
		child_process_uid	Integer	子进程用户 id。
		child_process_cmdline	String	子进程文件命令行。
		child_process_filename	String	子进程文件名。
		child_process_start_time	Long	子进程启动时间。
		child_process_gid	Integer	子进程组 ID。
		child_process_egid	Integer	子进程有效组 ID。
		child_process_euid	Integer	子进程有效用户 ID。
		virt_cmd	String	虚拟化命令。
		virt_process_name	String	虚拟化进程名称。
		escape mode	String	逃逸方式。
		escape cmd	String	逃逸后执行的命令。
	user_info	user_id	Integer	用户 uid。
		user_gid	Integer	用户 gid。
		user_name	String	用户名称。
		user_group_name	String	用户组名称。
		user_home_dir	String	用户 home 目录。

字段			类型	字段含义
		login_ip	String	用户登录 ip。
		service_type	String	登录的服务类型。
		service_port	Integer	登录服务端口。
		login_mode	String	登录方式。
		login_lasttime	Long	用户最后一次登录时间。
		login_fail_count	Integer	用户登录失败次数。
		pwd_hash	String	口令 hash。
		pwd_with_fuzzing	String	匿名化处理后的口令。
		pwd_used_days	Integer	密码使用的天数。
		pwd_min_days	Integer	口令的最短有效期限。
		pwd_max_days	Integer	口令的最长有效期限。
		pwd_warn_left_days	Integer	口令无效时提前告警天数。
	file_info	file_path	String	文件路径/名称。
		file_alias	String	文件别名。
		file_size	Integer	文件大小。
		file_mtime	Long	文件最后一次修改时间。
		file_atime	Long	文件最后一次访问时间。
		file_ctime	Long	文件最后一次状态改变时间。
		file_hash	String	文件 hash。
		file_md5	String	文件 md5。
		file_sha256	String	文件 sha256。
		file_type	String	文件类型。
		file_content	String	文件内容。

字段			类型	字段含义
		file_attr	String	文件属性。
		file_operation	String	文件操作类型。
		file_change_attr	String	变更前后的属性。
		file_new_path	String	新文件路径。
		file_desc	String	文件描述。
		file_key_word	String	文件关键字。
		is_dir	Boolean	是否目录。
		fd_info	String	文件句柄信息。
		fd_count	Integer	文件句柄数量。
	forensic_info	monitor_process	String	监控进程。
		escape_mode	String	逃逸方式。
		abnormal_port	String	异常端口。
	geo_info	src_country	String	源国家。
		src_city	String	源城市。
		src_latitude	Long	源纬度。
		src_longitude	Long	源经度。
		dest_country	String	目的国家。
		dest_city	String	目的城市。
		dest_latitude	Long	目的纬度。
		dest_longitude	Long	目的经度。
	malware_info	malware_family	String	恶意家族。

字段			类型	字段含义
		malware_class	String	恶意软件分类。
	system_info	pwd_valid	Boolean	口令结果是否有效。
		pwd_min_len	Integer	口令长度。
		pwd_digit_credit	Integer	口令中数字要求。
		pwd_uppercase_letter	Integer	口令中大写字母。
		pwd_lowercase_letter	Integer	口令中小写字母。
		pwd_special_characters	Integer	口令中特殊字符。
	extend_info	hit_rule	String	特征规则。
		rule_name	String	规则名称。
		rulesetname	String	规则集名称。
		report_type	String	上报数据类型。
	ti_info	ti_source	String	情报来源。
		ti_class	String	情报分类。
		ti_threat_type	String	情报威胁类型。
		ti_first_time	Long	第一次发现时间。
		ti_last_time	Long	最近一次发现时间。

sec-hss-log

主机安全日志字段含义如下所示：

表 11-13 sec-hss-log

字段	类型	字段含义
agentUuid	String	agent 的 UUID。

字段		类型	字段含义
alarmCsn		String	告警 UUID。
alarmKey		String	告警关键字。对于告警，当前透传 agent 上报的信息 msg_id；对于漏洞，由 master 生成。
alarmVersion		String	agent 版本号。
occurTime		Long	事件发生时间（ms）。
severity		Long	风险等级。
hostUuid		String	受影响主机 UUID。
hostName		String	受影响主机名。
hostIp		String	受影响主机通信 IP。
ipList		String	受影响主机 IP 列表。
cloudId		String	cloudagent sn。
region		String	受影响主机所在区域。
projectId		String	项目 ID。
enterpriseProjectId		String	企业项目 ID。
appendInfo		Object	告警详情。
appendInfo	agent_id	String	AGENT ID。
	version	String	事件版本。
	container_name	String	容器 ID（容器安全场景）。
	image_name	String	镜像名称（容器安全场景）。
	event_id	String	事件 ID，GUID。
	event_name	String	事件名称。
	event_classid	String	事件唯一标识。
	occur_time	Long	发生时间（秒）。
	recent_time	Long	最近一次发生时间（秒）。
	event_category	Integer	事件大类。
	event_type	Integer	事件类型。
	event_count	Integer	事件次数。
	severity	Integer	严重级别。

字段			类型	字段含义
	attack_phase		Integer	攻击阶段。
	attack_tag		Integer	攻击标识。
	confidence		Integer	置信度。
	action		Integer	动作类型。
	detect_module		String	检测模块。
	report_source		String	上报源。
	related_events		String	相关事件 ID。
	resource_info		Object	资源信息。
	network_info		Object	网络信息。
	app_info		Object	应用信息。
	system_info		Object	系统信息。
	process_info		list	进程信息。
	user_info		list	用户信息。
	file_info		list	文件信息。
	geo_info		Object	地理信息。
	malware_info		Object	恶意软件信息。
	forensic_info		String	取证字段。
	recommendation		String	处置建议。
	extend_info		String	事件扩展信息。
	resource_info	project_id	String	项目 ID。
		region_name	String	Region 名称。
		vpc_id	String	VPC ID。
		host_name	String	主机名称。
		host_ip	String	主机 IP。
		host_id	String	主机 ID（ECS 对应 ID）。
		cloud_id	String	CloudAgent SN。
		vm_name	String	虚拟机名称。
		vm_uuid	String	虚拟机 UUID。

字段			类型	字段含义
		container_id	String	容器 id。
		image_id	String	镜像 id。
		sys_arch	String	系统 CPU 架构。
		os_bit	String	操作系统位数。
		os_type	String	操作系统类型。
		os_name	String	操作系统名称。
		os_version	String	操作系统版本。
	network_info	local_address	String	本地地址。
		local_port	Integer	本地端口。
		remote_address	String	远程地址。
		remote_port	Integer	远程端口。
		src_ip	String	源 IP。
		src_port	Integer	源端口。
		src_domain	String	源域。
		dest_ip	String	目的 IP。
		dest_port	Integer	目的端口。
		dest_domain	String	目的域。
		protocol	String	协议。
		app_protocol	String	应用层协议。
		flow_direction	String	流量方向。
	app_info	sql	String	执行的 sql 语句。
		domain_name	String	DNS 域名。
		url_path	String	URL 路径。
		url_method	String	URL 方法。

字段			类型	字段含义
		req_refer	String	URL 请求 refer 信息。
		email_subject	String	邮件主题。
		email_sender	String	邮件发送者。
		email_receiver	String	邮件接收者。
		email_keyword	String	邮件关键字。
	process_info	process_name	String	进程名称。
		process_path	String	进程文件路径。
		process_pid	Integer	进程 id。
		process_uid	Integer	进程用户 id。
		process_username	String	运行进程的用户名。
		process_cmdline	String	进程文件命令行。
		process_filename	String	进程文件名。
		process_start_time	Long	进程启动时间。
		process_gid	Integer	进程组 ID。
		process_egid	Integer	进程有效组 ID。
		process_euid	Integer	进程有效用户 ID。
		parent_process_name	String	父进程名称。
		parent_process_path	String	父进程文件路径。
		parent_process_pid	Integer	父进程 id。
		parent_process_uid	Integer	父进程用户 id。

字段			类型	字段含义
		parent_process_cmdline	String	父进程文件命令行。
		parent_process_filename	String	父进程文件名。
		parent_process_start_time	Long	父进程启动时间。
		parent_process_gid	Integer	父进程组 ID。
		parent_process_egid	Integer	父进程有效组 ID。
		parent_process_euid	Integer	父进程有效用户 ID。
		child_process_name	String	子进程名称。
		child_process_path	String	子进程文件路径。
		child_process_pid	Integer	子进程 id。
		child_process_uid	Integer	子进程用户 id。
		child_process_cmdline	String	子进程文件命令行。
		child_process_filename	String	子进程文件名。
		child_process_start_time	Long	子进程启动时间。
		child_process_gid	Integer	子进程组 ID。
		child_process_egid	Integer	子进程有效组 ID。
		child_process_euid	Integer	子进程有效用户 ID。
		virt_cmd	String	虚拟化命令。

字段			类型	字段含义
		virt_process_name	String	虚拟化进程名称。
		escape mode	String	逃逸方式。
		escape cmd	String	逃逸后执行的命令。
	user_info	user_id	Integer	用户 uid。
		user_gid	Integer	用户 gid。
		user_name	String	用户名称。
		user_group_name	String	用户组名称。
		user_home_dir	String	用户 home 目录。
		login_ip	String	用户登录 ip。
		service_type	String	登录的服务类型。
		service_port	Integer	登录服务端口。
		login_mode	String	登录方式。
		login_lasttime	Long	用户最后一次登录时间。
		login_fail_count	Integer	用户登录失败次数。
		pwd_hash	String	口令 hash。
		pwd_with_fuzzing	String	匿名化处理后的口令。
		pwd_used_days	Integer	密码使用的天数。
		pwd_min_days	Integer	口令的最短有效期限。
		pwd_max_days	Integer	口令的最长有效期限。
		pwd_warn_left_days	Integer	口令无效时提前告警天数。
	file_info	file_path	String	文件路径/名称。
		file_alias	String	文件别名。

字段			类型	字段含义
		file_size	Integer	文件大小。
		file_mtime	Long	文件最后一次修改时间。
		file_atime	Long	文件最后一次访问时间。
		file_ctime	Long	文件最后一次状态改变时间。
		file_hash	String	文件 hash。
		file_md5	String	文件 md5。
		file_sha256	String	文件 sha256。
		file_type	String	文件类型。
		file_content	String	文件内容。
		file_attr	String	文件属性。
		file_operation	String	文件操作类型。
		file_change_attr	String	变更前后的属性。
		file_new_path	String	新文件路径。
		file_desc	String	文件描述。
		file_key_word	String	文件关键字。
		is_dir	Boolean	是否目录。
		fd_info	String	文件句柄信息。
		fd_count	Integer	文件句柄数量。
	forensic_info	monitor_process	String	监控进程。
		escape_mode	String	逃逸方式。
		abnormal_port	String	异常端口。
	geo_info	src_country	String	源国家。
		src_city	String	源城市。

字段			类型	字段含义
		src_latitude	Long	源纬度。
		src_longitude	Long	源经度。
		dest_country	String	目的国家。
		dest_city	String	目的城市。
		dest_latitude	Long	目的纬度。
		dest_longitude	Long	目的经度。
	malware_info	malware_family	String	恶意家族。
		malware_class	String	恶意软件分类。
	system_info	pwd_valid	Boolean	口令结果是否有效。
		pwd_min_len	Integer	口令长度。
		pwd_digit_credit	Integer	口令中数字要求。
		pwd_uppercase_letter	Integer	口令中大写字母。
		pwd_lowercase_letter	Integer	口令中小写字母。
		pwd_special_characters	Integer	口令中特殊字符。
	extend_info	hit_rule	String	特征规则。
		rule_name	String	规则名称。
		rulesetname	String	规则集名称。
		report_type	String	上报数据类型。
	ti_info	ti_source	String	情报来源。
		ti_class	String	情报分类。
		ti_threat_type	String	情报威胁类型。

字段			类型	字段含义
		ti_first_time	Long	第一次发现时间。
		ti_last_time	Long	最近一次发现时间。

sec-ddos-attack

DDoS 攻击日志字段含义如下所示：

表 11-14 sec-ddos-attack

字段	类型	字段含义
log_type	String	日志类型。
time	Date	本地时间。
device_ip	String	设备 IP。
device_type	String	设备类型（清洗：CLEAN；检测：DETECT）。
direction	String	日志方向（inbound，outbound）。
zone_id	String	防护对象 ID。
zone_name	String	防护对象名称。
zone_ip	String	IP。
biz_id	String	业务 ID。
is_deszone	String	是否网段流量（是：true；否：false）。
is_ipLocation	String	是否地址位置流量（是：true，否：false）。
ipLocation_id	String	地理位置 ID。
total_pps	String	总 pps。
total_kbps	String	总 Kbps。
tcp_pps	String	到目标的 TCP 总包速率 pps。
tcp_kbps	String	到目标的 TCP 总流量 Kbps。
tcpfrag_pps	String	到目标的 TCP 碎片包速率 pps。
tcpfrag_kbps	String	到目标的 TCP 碎片流量 Kbps。
udp_pps	String	到目标的 UDP 总包速率 pps。

字段	类型	字段含义
udp_kbps	String	到目标的 UDP 总流量 Kbps。
udpfrag_pps	String	到目标的 UDP 碎片包速率 pps。
udpfrag_kbps	String	到目标的 UDP 碎片流量 Kbps。
icmp_pps	String	到目标的 ICMP 总包速率 pps。
icmp_kbps	String	到目标的 ICMP 总流量 Kbps。
other_pps	String	到目标的 Other 总包速率 pps。
other_kbps	String	到目标的 Other 总流量 Kbps。
syn_pps	String	到目标的 SYN 报文数。
synack_pps	String	到目标的 SYN/ACK 报文数 pps。
ack_pps	String	到目标的 ACK 报文数 pps。
finrst_pps	String	到目标的 FIN/Rst 报文数 pps。
http_pps	String	到目标的 HTTP 总包速率 pps。
http_kbps	String	到目标的 HTTP 总流量 Kbps。
http_get_pps	String	到目标的 HTTP 请求总包速率 pps。
https_pps	String	到目标的 HTTPS 总包速率 pps。
https_kbps	String	到目标的 HTTPS 总流量 Kbps。
dns_request_pps	String	到目标业务 DNS Query 包速率 pps。
dns_request_kbps	String	到目标业务 DNS Query 总流量 Kbps。
dns_reply_pps	String	到目标业务 DNS Reply 包速率 pps。
dns_reply_kbps	String	到目标业务 DNS Reply 总流量 Kbps。
sip_invite_pps	String	到目标业务 SIP 包速率 pps。
sip_invite_kbps	String	到目标业务 SIP 总流量 Kbps。
tcp_increase_con	String	到目标的 tcp 每秒新建连接数统计。
udp_increase_con	String	到目标的 udp 每秒新建连接数统计。
icmp_increase_con	String	到目标的 icmp 每秒新建连接数统计。
other_increase_con	String	到目标的 other 协议每秒新建连接数统计。
tcp_concur_con	String	到目标的 tcp 并发连接数统计。
udp_concur_con	String	到目标的 udp 并发连接数统计。

字段	类型	字段含义
icmp_concur_con	String	到目标的 icmp 并发连接数统计。
other_concur_con	String	到目标的 other 协议并发连接数统计。
total_average_pps	String	到目标的所有流量的平均 pps。
total_average_kbps	String	到目标的所有流量的平均 Kbps。

sec-cts-audit

云审计服务日志字段含义如下所示：

表 11-15 sec-cts-audit

字段	类型	字段含义
time	Date	事件发生时间。以当地标准时间（采用格林威治时间加当地时区形式）进行展示，例如：2022/11/08 11:24:04 GMT+08:00。
user	Object	发起操作的云账户信息。
request	Object	操作的请求内容。
response	Object	操作的响应内容。
service_type	String	操作来源。
resource_type	String	资源类型。
resource_name	String	资源名称。
resource_id	String	资源的唯一标识。
source_ip	String	发起本次操作的用户的 IP，如果为系统内调用，则为空。
trace_name	String	操作名称。
trace_rating	String	操作事件等级，分为以下等级： • normal：代表本次操作成功。 • warning：代表本次操作失败。 • incident：代表本次操作引起了比失败更严重的后果，比如会造成节点故障或用户业务故障等情况。

字段	类型	字段含义
trace_type	String	操作类型，分为以下几种： • ConsoleAction：表示通过管理控制台执行的操作。 • SystemAction：表示系统内部触发的操作。 • ApiCall：表示调用 ApiGateway 触发的操作。 • ObsSDK：表示通过调用 OBS 提供的 SDK 触发的关于 OBS 桶相关操作。 • Others：表示除去通过“ObsSDK”触发的关于 OBS 桶相关的操作。
api_version	String	作为操作来源的云服务的 API 版本号。
message	Object	备注信息。
record_time	Long	记录操作的时间，表示方式为时间戳。
trace_id	String	操作的唯一标识。
code	Integer	事件 http 返回码，例如 200，400。
request_id	String	记录本次请求的 request id。
location_info	String	记录本次请求出错后，问题定位所需要的辅助信息。
endpoint	String	该操作涉及云资源的详情页面的 endpoint。
resource_url	String	该操作涉及云资源的详情页面的访问链接（不含 endpoint）。
user_agent	String	OBS 桶相关操作中非 ObsSDK 方式调用时的操作类型。
content_length	Long	OBS 桶相关操作中请求消息体的长度。
total_time	Long	OBS 桶相关操作中请求的响应时间。

sec-cfw-risk

云防火墙攻击事件日志字段含义如下所示：

表 11-16 sec-cfw-risk

字段	类型	字段含义

字段	类型	字段含义
event_time	Date	检测到的攻击时间。
action	String	云防火墙当前的响应动作。 • permit：放行 • deny：阻断
app	String	应用类型。
attack_rule	String	检测到攻击的防御规则。
attack_rule_id	String	检测到攻击的防御规则 ID 号。
attack_type	String	发生攻击的类型： • Vulnerability Exploit Attack：漏洞攻击 • Vulnerability Scan：漏洞扫描 • Trojan：木马病毒 • Worm：蠕虫病毒 • Phishing：网络钓鱼攻击 • Web Attack：Web 攻击 • Application DDoS：DDoS 攻击 • Buffer Overflow：缓冲区溢出攻击 • Password Attack：密码攻击 • Mail：邮件相关类型的攻击行为 • Access Control：访问控制行为 • Hacking Tool：黑客工具 • Hijacking：劫持行为 • Protocol Exception：存在异常协议 • Spam：存在垃圾邮件 • Spyware：存在间谍软件 • DDoS Flood：DDoS 泛洪攻击 • Suspicious DNS Activity：可疑 DNS 活动 • Other Suspicious Behavior：其他可疑行为
dst_ip	String	目的 IP 地址。
dst_port	String	目的端口号。
packet	String	攻击日志的原始数据包。
protocol	String	协议类型。

字段	类型	字段含义
level	String	表示检测到威胁的等级： • CRITICAL：严重 • HIGH：高 • MIDDLE：中 • LOW：低
source	String	检测到攻击的防御模式： • 0：基础防御 • 1：虚拟补丁
src_ip	String	源 IP 地址。
src_port	String	源端口号。
direction	String	流量方向： • out2in：入方向 • in2out：出方向

sec-cfw-flow

云防火墙流量日志字段含义如下所示：

表 11-17 sec-cfw-flow

字段	类型	字段含义
app	String	应用类型。
dst_ip	String	目的 IP 地址。
dst_port	String	目的端口号。
end_time	Date	流结束时间。
protocol	String	协议类型。
to_c_bytes	String	服务端向客户端发送的字节数。
to_c_pkts	String	服务端向客户端发送的报文数。
to_s_bytes	String	客户端向服务端发送的字节数。
to_s_pkts	String	服务端向客户端发送的报文数。
src_ip	String	源 IP 地址。
src_port	String	源端口号。

字段	类型	字段含义
start_time	Date	流开始时间。

sec-cfw-block

云防火墙访问控制日志字段含义如下所示：

表 11-18 sec-cfw-block

字段	类型	字段含义
hit_time	Date	访问发生的时间。
action	String	云防火墙当前的响应动作： • permit：放行 • deny：阻断
app	String	应用类型。
dst_ip	String	目的 IP 地址。
dst_port	String	目的端口号。
protocol	String	协议类型。
rule_id	String	触发规则的 ID。
src_ip	String	源 IP 地址。
src_port	String	源端口号。

sec-apig-access

API 网关访问日志字段含义如下所示：

表 11-19 sec-apig-access

字段	类型	字段含义
region_id	String	局点。
api_id	String	API ID。
body_bytes_sent	String	返回 Body 大小。
bytes_sent	String	整个返回大小。
domain	String	公网域名。

字段	类型	字段含义
errorType	String	是否被流控（1：被流控）。
http_user_agent	String	用户代理标识。
http_x_forwarded_for	String	X-Forwarded-For 头。
opsuba_api_url	String	请求的 URI。
out_times	String	网关内部与周边组件交互耗时。
remote_addr	String	远端 ip。
request_id	String	请求 id。
request_length	String	整个请求大小。
request_method	String	HTTP 请求方法。
request_time	String	访问耗时。
scheme	String	协议。
server_protocol	String	请求协议。
status	String	状态。
time_local	Date	时间。
upstream_addr	String	远端 ip。
upstream_connect_time	String	远端连接耗时。
upstream_header_time	String	远端头耗时。
upstream_response_time	String	远端返回耗时。
upstream_status	String	远端状态。
upstream_uri	String	请求后端的 URI。
user_name	String	用户 projectid 或 appid。

sec-dbss-alarm

DBSS 告警日志字段含义如下所示：

表 11-20 dbss-alarm

字段	类型	字段含义
domain_id	String	账号 ID。
project_id	String	项目 ID。

字段		类型	字段含义
region		String	region
tenant_vpc_id		String	租户的 VPC ID。
tenant_subnet_id		String	租户的子网 ID。
instance_id		String	实例 ID。
instance_name		String	实例名。
alarm		Object	告警对象。
source_type		String	dbss。
alarm	alarm_risk	String	告警等级。
	client_ip	String	连接 IP。
	database_ip	String	数据库访问 IP。
	count	Long	告警次数。
	user_name	String	数据库用户名。
	schema	String	oracle schema。
	rule_name	String	规则名称。
	rule_id	String	规则 ID。
	sql_type	String	SQL 执行类型。
	sql_result	String	SQL 执行结果。
	db_type	String	数据库类型。

sec-dsc-alarm

DSC 告警日志的保留字段根据日志类型有所不同，具体如下：

表 11-21 AK SK 泄露（aksk_leakage）

字段	类型	字段含义
log_type	String	告警类型。
region_id	String	region。
domain_id	String	账号 ID。
project_id	String	项目 id。
leakage_ak	String	AK。

字段	类型	字段含义
source	String	泄漏源。
find_time	String	发现时间。
account	String	账号名。
file_name	String	文件名。
file_suffix	String	文件后缀。
leakage_user_id	String	泄露子用户 ID。
leakage_user_name	String	泄露子用户名。
leakage_domain_id	String	泄露主账号 ID。
leakage_domain_name	String	泄露主账号名。
url	String	泄露网址。

表 11-22 风险 OBS 桶文件（obs_risk）

字段	类型	字段含义
log_type	String	告警类型。
region_id	String	region。
domain_id	String	账号 ID。
project_id	String	项目 id。
bucket_policy	String	公开桶/私有桶。
bucket_domain_id	String	桶所属账号 ID。
bucket_project_id	String	桶所属项目 ID。
bucket_name	String	桶名称。
file_name	String	文件名称。
file_path	String	文件路径。
risk_level	Integer	敏感风险等级。
sensitive_data_type	String[]	敏感数据类型。
privacy_detail	String	个人隐私数据明细。
file_type	String	文件类型。
mimetypes	String	文件类型。

字段	类型	字段含义
rule_list	List<Map<String,String>>	匹配规则列表。
keyword	String	匹配敏感数据规则关键字。
available_zone	String	可用区。
encrypted	String	是否加密。

表 11-23 数据敏感字段信息（db_risk）

字段	类型	字段含义
log_type	String	告警类型。
region_id	String	region。
domain_id	String	账号 ID。
project_id	String	项目 id。
vpc_id	String	VPC ID。
db_instance_type	String	RDS PUB。
db_instance_id	String	数据库实例 ID。
db_instance_type	String	数据库实例类型。
db_instance_ip	String	数据库实例 IP。
db_instance_domain_id	String	数据库实例所属账号 ID。
db_instance_project_id	String	数据库实例所属项目 ID。
db_instance_name	String	数据库实例名称。
db_name	String	数据库名称。
table_name	String	表名称。
field_name	String	字段名称。
data_type	String	字段数据类型。
risk_level	Integer	敏感风险等级。
sensitive_data_type	String[]	敏感数据类型。
privacy_detail	String	个人隐私数据明细。
rule_list	List<Map<String,String>>	匹配规则列表。

字段	类型	字段含义
keyword	String	匹配敏感数据规则关键字。

11.2.5 快速添加日志告警模型

操作场景

态势感知（专业版）支持将查询分析结果设置告警模型，并在满足条件时触发告警。

本章节将接入如何快速为日志设置告警模型。

前提条件

已完成数据接入，详细操作请参见云服务接入。

快速添加日志告警模型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

步骤 6 输入查询分析语句，设置时间范围，并单击“查询/分析”，显示查询分析结果。

更多查询分析详细操作请参见查询与分析日志。

步骤 7 单击页面右上角“添加告警”，进入新建告警模型页面。

图 11-11 添加告警

步骤 8 配置告警基础信息，参数说明如表 11-24 所示。

表 11-24 告警模型基础配置

参数名称	参数说明
管道名称	该告警模型的执行管道，系统默认生成。
模型名称	自定义该条告警模型的名称。

参数名称	参数说明
严重程度	设置该告警模型的严重程度。可以设置致命、高危、中危、低危、提示级别。
告警类型	选择该条告警模型触发后，提示的告警类型。
模型类型	默认为规则模型。
描述	填写该告警模型的描述信息。
启用状态	设置该告警模型的启用状态。 此处设置的状态，可在整个告警模型设置成功后进行更改。

步骤 9 设置完成后，单击页面右下角“下一步”，进入设置模型逻辑页面。

步骤 10 设置模型逻辑，参数说明如表 11-25 所示。

表 11-25 设置模型逻辑

参数名称	参数说明
查询规则	设置告警的查询规则，设置完成后可以单击“运行”，查看当前运行结果。 查询分析语句由查询语句和分析语句构成，格式为**查询语句|分析语句**，查询分析语句语法详细内容请参见查询与分析语法概述。 **说明** 如果筛留字段为 text 类型时，默认会使用 MATCH_QUERY 进行分词查询。
查询计划	设置告警查询计划。 • 运行查询间隔：xx 分钟/小时/天。 当运行查询间隔为分钟时，可设置为 5-59 分钟；当运行查询为小时时，可设置为 1-23 小时；当运行查询为天时，可设置为 1-14 天。 • 时间窗口：xx 分钟/小时/天。 当时间窗口为分钟时，可设置为 5-59 分钟；当时间窗口为小时时，可设置为 1-23 小时；当时间窗口为天时，可设置为 1-14 天。 • 延迟执行时间：xx 分钟，可以设置为 0-5 分钟。
告警扩充	• 自定义信息：自定义告警扩充信息。 单击“添加”，并设置 key+value 信息，完成新增。 • 告警详细信息：自定义填写告警名称、描述和处置建议。

参数名称	参数说明
触发条件	设置告警触发条件。可设置为：大于/等于/不等于/小于 xx 时，触发告警。 如有多条触发条件，可以单击“添加”按钮进行添加，最多可添加 5 个触发条件。 当设置了多个触发条件时，在日志数据扫描检测中，系统将按照从上到下的校验逻辑，如果有满足此处设置的触发条件被检测到时，系统都将展示不同类型的告警。
告警分组	配置将规则查询结果分组到告警的方式。可选择以下方式： • 将所有查询结果分组到一个告警中 • 将每条查询结果独立触发告警
调试模式	设置是否生成调试类告警。
抑制	设置生产告警后是否停止运行查询。 • 如果设置为抑制，即生成告警后**停止**运行查询。 • 如果设置为不抑制，即生成告警后**不停止**运行查询。

步骤 11 设置完成后，单击页面右下角“下一步”，进入模型详情预览页面。

步骤 12 预览确认无误后，单击页面右下角“确定”。

----结束

11.2.6 查看图表统计结果

当您执行了查询和分析语句后，态势感知（专业版）支持通过图表统计的形式对查询和分析的结果进行可视化展示，您可以根据分析需求选择合适的统计图表类型展示查询和分析结果。

态势感知（专业版）可以通过以下图表类型展示查询和分析结果：

- 表格形式展示查询与分析结果
- 折线图形式展示查询和分析结果
- 柱状图形式展示查询和分析结果
- 饼图形式展示查询和分析结果

前提条件

已经执行了查询和分析语句。安全分析说明请参见安全分析概述，查询与分析日志请参见查询与分析日志。

查看图表统计结果操作步骤

查询分析结果可以通过表格、折线图、柱状图、饼图形式进行展示。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

步骤 6 输入查询分析语句，设置时间范围，并单击“查询/分析”。

步骤 7 根据需要选择合适的统计图表类型展示查询和分析结果。

- 表格形式展示查询与分析结果

  表格为最常见的数据展示类型，通过对数据的整理，可以快速对数据进行分析。在态势感知（专业版）中，通过查询分析语句得到的数据结果在图表统计中，默认以表格形式进行展示。

  在下方选择“图表统计”页签，并在图表统计页面右侧的“图表类型”中单击。

  配置表格参数。

表 11-26 表格参数配置

参数类别	参数名称	参数说明
基本配置	标题	自定义表格标题名称。
图表配置	隐藏字段	选择目标字段，将该字段在表格中隐藏。

  图表设置完成后，左侧可预览配置后的数据分析情况。

- 折线图形式展示查询和分析结果

  折线图一般用于展示一组数据在某一周期内的某一个有序数据类别上的变化情况，属于趋势类的分析图表，可以清晰直观地分析数据变化的趋势。

  在下方选择“图表统计”页签，并在图表统计页面右侧的“图表类型”中选择。

  配置折线图参数。

表 11-27 折线图参数配置

参数类别	参数名称	参数说明
基本配置	标题	自定义线图标题名称。

参数类别	参数名称	参数说明
图表配置	X 轴标题	自定义 X 轴标题名称。
	Y 轴标题	自定义 Y 轴标题名称。
	X 轴字段	选择 X 轴显示字段。
	Y 轴字段	选择 Y 轴显示字段。
图例配置	显示图例	确认是否显示图例。
	图例位置	开启显示图例时须配置。 图例在图表中的位置，可以配置为上、下、左和右。

图表设置完成后，左侧可预览配置后的数据分析情况。

- 柱状图形式展示查询和分析结果

  柱状图是一种由矩形表示类别的数据显示方法，可以在多个数据和趋势分析之间进行清晰比较。态势感知（专业版）中，柱状图默认采用垂直柱子（即矩形块的宽度一定，高度代表数值大小）来展示数据。

  在下方选择“图表统计”页签，并在图表统计页面右侧的“图表类型”中选择。

  配置柱状图参数。

表 11-28 柱状图参数配置

参数类别	参数名称	参数说明
基本配置	标题	自定义线图标题名称。
图表配置	X 轴标题	自定义 X 轴标题名称。
	Y 轴标题	自定义 Y 轴标题名称。
	X 轴字段	选择 X 轴显示字段。
	Y 轴字段	选择 Y 轴显示字段。
图例配置	显示图例	确认是否显示图例。
	图例位置	开启显示图例时须配置。 图例在图表中的位置，可以配置为上、下、左和右。

图表设置完成后，左侧可预览配置后的数据分析情况。

- 饼图形式展示查询和分析结果

  饼图用于表示不同分类的占比情况，通过弧度大小来对比各种分类。

  在下方选择“图表统计”页签，并在图表统计页面右侧的“图表类型”中选择。

配置饼图参数。

表 11-29 饼图参数配置

参数类别	参数名称	参数说明
基本配置	标题	自定义线图标题名称。
图表配置	分类	数据分类。
	数列值	分类数据对应的数值。
图例配置	显示图例	确认是否显示图例。
	图例位置	开启显示图例时须配置。 图例在图表中的位置，可以配置为上、下、左和右。

图表设置完成后，左侧可预览配置后的数据分析情况。

----结束

11.2.7 下载或导出日志

操作场景

态势感知（专业版）支持将原始日志或查询分析日志下载或导出到本地，方便通过日志分析和定位问题。本章节介绍如何下载或导出日志。

- 导出原始日志：在“原始日志”页签中，单击，系统将下载日志到本地。
- 下载图表日志：在“图表统计”页签中，单击“下载日志”，系统将下载日志到本地。

前提条件

已完成数据接入，详细操作请参见云服务接入。

下载或导出日志

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

步骤 6 （可选）在管道数据检索页面，输入查询条件，选择时间下拉菜单中选择查询时间，并单击“查询/分析”。

步骤 7 下载日志。

- 导出原始日志：在“原始日志”页签中，单击，系统将下载日志到本地。
- 下载图表日志：在“图表统计”页签中，单击“下载日志”，系统将下载日志到本地。

----结束

11.2.8 管理数据空间

数据空间是进行数据分组、负载、流控单元。同一数据空间的数据共享同一负载均衡策略。

本章节介绍管理数据空间的相关操作：

- 新增数据空间：如果需要使用态势感知（专业版）提供的**安全分析**、**数据分析**、**智能建模**等功能时，需要新增数据空间。
- 查看数据空间详情：通过管理控制台查看数据空间信息，包括名称、类型和创建时间等。
- 编辑数据空间：数据空间新增成功后，如果需要对其**描述信息**进行修改。
- 删除数据空间：如果不再需要某个数据空间，可以删除数据空间。

约束与限制

- 删除数据空间场景
  - 系统创建默认数据空间**不支持**删除操作。
  - 如果待删除数据空间中，存在数据管道，则该数据空间不能直接删除。您需要先删除数据管道，再删除数据空间。

新增数据空间

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在数据空间列表左上角，单击“新增”，系统从右侧弹出新增数据空间界面。

图 11-12 新增数据空间

步骤 6 在新增数据空间页面中，配置新建数据空间参数，参数说明如表 11-30 所示。

表 11-30 新增数据空间

参数名称	参数说明
数据空间	输入数据空间名称。命名规则如下： • 名称长度取值范围为 5-63 个字符。 • 可包含英文字母、数字和-。其中，-不能出现在开头和结尾，且不能连续出现。 • 名称须为全局唯一，不能与其他数据空间名称相同。
描述	可选参数，设置该数据空间的备注信息。

步骤 7 单击“确定”，完成数据空间的新增。

新增完成后，可以在数据空间列表中查看已新增的数据空间。

----结束

查看数据空间详情

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在数据空间管理页面中，查看全部数据空间信息，相关参数说明如表 11-31 所示。

表 11-31 数据空间

参数名称	参数说明
数据空间	数据空间名称。
类型	数据空间中的数据所属类型，包含以下两种类型： • system-defined：数据接入时，系统默认创建的数据空间。 • user-defined：用户自行创建的数据空间。
当前管道数	数据空间中目前已有管道的数量。
创建时间	数据空间的创建时间。
描述	数据空间的描述信息。

参数名称	参数说明
操作	用户可以在操作栏中，执行编辑、删除等操作。

步骤 6 在左侧数据空间栏中，单击某个数据空间名称后的，右侧弹出当前数据空间的详情。

图 11-13 进入数据空间详情页面

步骤 7 在数据空间详情中，可以查看某个数据空间的详细信息，参数说明如表 11-32 所示。

表 11-32 数据空间详情

参数名称	参数说明
数据空间	数据空间名称。
当前管道数	该数据空间中目前已有管道的数量。
创建时间	数据空间的创建时间。
描述	数据空间的描述信息。

----结束

编辑数据空间

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在待编辑数据空间所在行“操作”列，单击“编辑”。

步骤 6 在弹出编辑数据空间界面，修改数据空间描述信息。

步骤 7 单击“确定”。

----结束

删除数据空间

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在需要删除的数据空间所在行的“操作”列，单击“删除”。

步骤 6 在弹出的对话框中单击“确定”，完成删除数据空间的操作。

如果待删除数据空间中，存在数据管道，则该数据空间不能直接删除。您需要先删除数据管道，再删除数据空间。

----结束

11.2.9 管理管道

数据传输消息主题和存储索引组合为数据管道。本章节介绍管理数据管道的相关操作：

- 创建管道：如果需要使用态势感知（专业版）提供的**安全分析**、**数据分析**、**智能建模**功能时，需要创建管道。
- 查看管道详情：指导用户通过管理控制台查看管道的信息，包括名称、所属数据空间和创建时间等。
- 编辑管道：管道创建成功后，可对管道 **Shard 数**、**描述**、**生命周期**等管道参数进行修改。
- 删除管道：删除管道后数据将会被同步删除，且不可恢复，请谨慎操作。

创建管道

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 （可选）已新增数据空间，具体操作请参见新增数据空间。

步骤 6 在左侧数据空间导航栏中，单击数据空间名称右侧的，并在下拉选项中选择的“创建管道”，系统从右侧弹出创建管道页面。

图 11-14 创建管道

步骤 7 在创建管道页面中，配置管道参数，参数说明如表 11-33 所示。

表 11-33 创建管道

参数名称	参数说明
数据空间	该管道所属的数据空间，系统默认生成。
管道名称	自定义管道的名称。 命名规则如下： • 名称长度取值范围为 5-64 个字符。 • 名称须为工作空间内唯一，不能与工作空间内的其他管道名称相同。 • 必须以小写英文字母开头，且只能包含小写英文字母、数字和'_'，且'_'不能在结尾，也不能连续出现。 • 不能以系统预留的前缀 isap_、csb_、secmaster_、sec_、s_sec_、i_sec_、l_sec_、security_开头。
Shard 数	该管道的 Shard 数量。取值范围为：1-64。 索引可以存储数据量超过 1 个节点硬件限制的数据。为满足这样的需求，Elasticsearch 提供了一个能力，将一个索引拆分为多个，称为 Shard。当您创建一个索引时，您可以根据实际情况指定 Shard 的数量。每个 Shard 托管在集群中的任意一个节点中，且每个 Shard 本身是一个独立的、全功能的“索引”。
生命周期	该管道内数据的生命周期。取值范围为：7-180。
描述	可选参数，设置该管道的备注信息。

步骤 8 单击“确定”。

创建成功后，可单击数据空间名称或数据空间栏后的，展开查看已创建的管道。

----结束

查看管道详情

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开已创建的管道。

图 11-15 查看管道

步骤 6 单击待查看管道名称后的，右侧将显示管道的详细信息。

表 11-34 管道参数说明

参数名称	参数说明
工作空间名称	当前管道所属工作空间的名称。
工作空间 ID	当前管道所属工作空间的 ID。
数据空间名称	当前管道所属数据空间的名称。
数据空间 ID	当前管道所属数据空间的 ID。
管道名称	当前管道的名称。
管道 ID	当前管道的 ID。
Shard 数	管道的 Shard 数。
生命周期	管道内数据保存周期。
创建时间	管道的创建时间。
描述	管道的描述信息。

----结束

编辑管道

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开已创建的管道。

图 11-16 查看管道

步骤 6 单击管道名称后的“更多 > 编辑”。

图 11-17 编辑管道入口

步骤 7 从编辑管道页面中，配置管道参数，参数说明如表 11-35 所示。

表 11-35 编辑管道

参数名称	参数说明
数据空间	该管道所属的数据空间。系统默认，**不支持**修改。
管道名称	您创建管道时设置的名称，创建后**不支持**修改。
Shard 数	该管道的 Shard 数量。取值范围为：1-64。
生命周期	该管道内数据的生命周期。取值范围：7-180。
描述	可选参数，设置该管道的备注信息。

步骤 8 单击“确定”。

----结束

删除管道

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开已创建的管道。

图 11-18 查看管道

步骤 6 单击管道名称后的“更多 > 删除”。

图 11-19 删除管道

步骤 7 在弹出的删除确认框中，单击“确定”，完成删除管道的操作。

----结束

11.2.10 开启数据消费

数据消费是指第三方软件、云产品等通过客户端实时消费日志服务的数据，是对全量数据的顺序读写。

态势感知（专业版）提供数据消费功能，支持通过客户端实时消费数据。

开启数据消费

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，单击目标管道名称后的“更多 > 数据消费”，进入数据消费页面。

图 11-20 进入数据消费页面

步骤 6 在数据消费页面中，单击当前状态后的，开启数据消费。

开启后，将显示消费配置信息，具体说明如表 11-36 所示。

表 11-36 数据消费参数说明

参数名称	参数说明
当前状态	当前管道中数据消费配置状态。
管道名称	当前数据管道的名称。
订阅器	系统预置的订阅模式，决定数据如何传递给消费者。
访问节点	当前数据的访问节点。

----结束

相关操作

数据消费开启后，如需关闭，则可在数据消费页面，单击“当前状态”后的，关闭数据消费。

11.2.11 开启数据监控

态势感知（专业版）数据监控功能支持监控态势感知（专业版）管道上下游的生产速率、生产量、消费总速率等指标，您可以根据监控判断业务运行状态。

相关概念

- 生产者：是用来构建并传输数据到服务端的逻辑概念，负责把数据放入消息队列。
- 订阅器：用于订阅态势感知（专业版）管道消息，一个管道可由多个订阅器进行订阅，态势感知（专业版）通过订阅器进行消息分发。
- 消费者：是用来接收并处理数据的运行实体，负责通过订阅器把态势感知（专业版）管道中的消息进行消费并处理。
- 消息队列：是数据存储和传输的实际容器。

查看监控指标

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，单击目标管道名称后的“更多 > 监控”，进入管道监控页面。

图 11-21 进入数据监控页面

步骤 6 在数据管道的监控页面，查看监控指标。

- 总览：显示当前管道中生产者、管道、订阅器、消费者之间生产速率等信息。
- 生产者：显示生产者的“当前生产 TPS”、“当前生产速率”、“当前生产数量”、“当前消息存储大小”等相关指标信息。
- 管道：显示当前管道指定时间（近 2/6/12/24 小时、近 7 天或自定义）内的“管道存储的消息大小(MB)”、“生产到管道的消息大小(MB)”、“生产到管道的消息数量(条)”、“从管道消费的消息大小(MB)”、“从管道消费的消息数量(条)”、“未确认的

消息大小(B)”、“管道的生产速率(条/秒)”、“管道的消费速率(条/秒)”、“每条消息大小平均值(B)”、“未卸载的消息大小(B)”等相关指标信息。

- 订阅器：显示当前订阅器指定时间（近 2/6/12/24 小时、近 7 天或自定义）内的“订阅器消费总速率(条/秒)”、“订阅器消费的数据大小(B)”、“订阅器消费的数据数量(条)”、和“活跃消费者”等相关指标信息。

----结束

11.3 查询与分析语法

11.3.1 查询与分析语法概述

本部分介绍安全分析使用的查询与分析语法，态势感知（专业版）支持检索 SQL 语法。在态势感知（专业版）控制台上，具体输出查询与分析语法位置如下所示：

基本语法

SQL 由查询语句和分析语句组成，以竖线 | 分隔。查询语句可单独使用，分析语句必须与查询语句一起使用。

```
查询语句 | 分析语句
```

表 11-37 基本语法

语句类型	说明
查询语句	查询语句用于指定日志查询时的筛选条件，返回符合条件的日志。通过设置筛选条件，可以帮助您快速、有效地查询到所需日志。
分析语句	分析语句用于对查询结果进行计算和统计。

约束与限制

- 查询语句不支持数学运算，比如：(age + 100) ≤ 1000。
- 聚合函数只支持字段，不支持表达式，比如 avg(log(age))。
- 不支持多表关联。
- 不支持子查询。
- 页面查询只支持返回 500 条。
- GROUP BY 分组上限为 10000 组。

11.3.2 查询语句

查询语句用于指定日志查询时的筛选条件，返回符合条件的日志。通过设置筛选条件，可以帮助您快速、有效地查询到所需日志。

本章节将介绍查询语句以及使用示例。

语法

查询语句有两种形式：

- 仅为*，表示不进行筛选，返回全量数据。
- 由一个或多个查询子句组成，子句间通过“NOT”、“AND”、“OR”连接，并支持使用“()”提高括号内查询条件的优先级。

查询子句基本结构如下所示：

```
字段名称 操作符 字段值
```

其中，可使用的操作符如操作符所示。

操作符

表 11-38 操作符说明

操作符	说明
=	查询某字段值**等于**某数值的日志。
<>	查询某字段值**不等于**某数值的日志。
>	查询某字段值**大于**某数值的日志。
<	查询某字段值**小于**某数值的日志。
>=	查询某字段值**大于或等于**某数值的日志。
<=	查询某字段值**小于或等于**某数值的日志。
IN	查询某字段值**处于某数值范围内**的日志。
BETWEEN	查询某字段值**处于指定的范围内**的日志。
LIKE	全文搜索某字段值的日志。
IS NULL	查询某字段值为 NULL 的日志。
IS NOT NULL	查询某字段值为 NOT NULL 的日志。

示例

表 11-39 普通查询示例

查询需求	查询语句
查询所有日志	*

查询需求	查询语句
查询 GET 请求成功（状态码为 200~299）的日志。	request_method = 'GET' AND status BETWEEN 200 AND 299
查询 GET 请求或 POST 请求的日志。	request_method = 'GET' OR request_method = 'POST'
查询非 GET 请求的日志。	NOT request_method = 'GET'
查询 GET 请求或 POST 请求，且请求成功的日志。	(request_method = 'GET' OR request_method = 'POST') AND status BETWEEN 200 AND 299
查询 GET 请求或 POST 请求，且请求失败的日志。	(request_method = 'GET' OR request_method = 'POST') NOT status BETWEEN 200 AND 299
查询 GET 请求成功（状态码为 200~299）且请求时间大于等于 60 秒的日志。	request_method = 'GET' AND status BETWEEN 200 AND 299 AND request_time >= 60
查询请求时间为 60 秒的日志。	request_time = 60

11.3.3 分析语句

11.3.3.1 SELECT

完整的分析语句语法如下：

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

其中，SELECT 表示指定查询的字段。本章节内容将介绍 SELECT 语法参数说明及示例。

使用*查询所有字段

```
SELECT *
```

表 11-40 使用*查询所有字段

account_number	firstname	gender	city	balance	employer	state	lastname	age
1	Amber	M	Brogan	39225	Pyrami	IL	Duke	32
16	Hattie	M	Dante	5686	Netagy	TN	Bond	36
13	Nanette	F	Nogal	32838	Quility	VA	Bates	28

account_number	firstname	gender	city	balance	employer	state	lastname	age
18	Dale	M	Orick	4180	null	MD	Adams	32

查询指定字段

```
SELECT firstname, lastname
```

表 11-41 查询指定字段

firstname	lastname
Amber	Duke
Hattie	Bond
Nanette	Bates
Dale	Adams

使用 AS 给字段定义别名

```
SELECT account_number AS num
```

表 11-42 使用 AS 给字段定义别名

num
1
16
13
18

使用 DISTINCT 去重

```
SELECT DISTINCT age
```

表 11-43 使用 DISTINCT 去重

age
32
36
28

使用 SQL 函数

函数相关内容请参见函数。

```
SELECT LENGTH(firstname) as len, firstname
```

表 11-44 使用 SQL 函数

len	firstname
4	Amber
6	Hattie
7	Nanette
4	Dale

11.3.3.2 GROUP BY

完整的分析语句语法如下：

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

其中，GROUP BY 表示按值分组。本章节内容将介绍 GROUP BY 语法参数说明及示例。

按字段的值分组

```
SELECT age GROUP BY age
```

表 11-45 按字段的值分组

age
28
32
36

按字段别名分组

```
SELECT account_number AS num GROUP BY num
```

表 11-46 按字段别名分组

num

num
1
16
13
18

按多个字段分组

```
SELECT account_number AS num, age GROUP BY num, age
```

表 11-47 按多个字段分组

num	age
1	32
16	36
13	28
18	32

使用 SQL 函数

函数相关内容请参见函数。

```
SELECT LENGTH(lastname) AS len, COUNT(*) AS count GROUP BY LENGTH(lastname)
```

表 11-48 使用 SQL 函数

len	count
4	2
5	2

11.3.3.3 HAVING

完整的分析语句语法如下：

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

其中，HAVING 子句用于指定过滤分组结果（GROUP BY）或聚合计算结果的条件。本章节内容将介绍 HAVING 语法参数说明及示例。

在分组的基础上，结合聚合函数来筛选数据。

```
SELECT age, MAX(balance) GROUP BY age HAVING MIN(balance) > 10000
```

表 11-49 HAVING

age	MAX(balance)
28	32838
32	39225

11.3.3.4 ORDER BY

完整的分析语句语法如下：

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

其中，ORDER BY 表示按字段值排序。本章节内容将介绍 ORDER BY 语法参数说明及示例。

使用字段值排序

```
SELECT age ORDER BY age DESC
```

表 11-50 使用字段值排序

age
28
32
32
36

11.3.3.5 LIMIT

完整的分析语句语法如下：

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

其中，LIMIT 表示指定返回数据的条数。本章节内容将介绍 LIMIT 语法参数说明及示例。

指定返回的条数

```
SELECT * LIMIT 1
```

表 11-51 指定返回的条数

account_number	firstname	gender	city	balance	employer	state	lastname	age
1	Amber	M	Brogan	39225	Pyrami	IL	Duke	32

指定返回的条数和偏移量

```
SELECT * LIMIT 1 OFFSET 1
```

表 11-52 指定返回的条数和偏移量

account_number	firstname	gender	city	balance	employer	state	lastname	age
16	Hattie	M	Dante	5686	Netagy	TN	Bond	36

11.3.3.6 函数

完整的分析语句语法如下：

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

本章节介绍函数。

数学类

表 11-53 数学类

函数	作用	定义	示例
abs	绝对值	abs(number T) -> T	SELECT abs(0.5) LIMIT 1
add	加法	add(number T, number) -> T	SELECT add(1, 5) LIMIT 1
cbrt	立方根	cbrt(number T) -> T	SELECT cbrt(0.5) LIMIT 1
ceil	向上取整	ceil(number T) -> T	SELECT ceil(0.5) LIMIT 1

函数	作用	定义	示例
divide	除法	divide(number T, number) -> T	SELECT divide(1, 0.5) LIMIT 1
e	自然底数 e	e() -> double	SELECT e() LIMIT 1
exp	自然底数 e 的次幂	exp(number T) -> T	SELECT exp(0.5) LIMIT 1
expm1	自然底数 e 的次幂减一	expm1(number T) -> T	SELECT expm1(0.5) LIMIT 1
floor	向下取整	floor(number T) -> T	SELECT floor(0.5) AS Rounded_Down LIMIT 1
ln	自然对数	ln(number T) -> double	SELECT ln(10) LIMIT 1
log	以 T 为底数的对数	log(number T, number) -> double	SELECT log(10) LIMIT 1
log2	以 2 为底数的对数	log2(number T) -> double	SELECT log2(10) LIMIT 1
log10	以 10 为底数的对数	log10(number T) -> double	SELECT log10(10) LIMIT 1
mod	取余	mod(number T, number) -> T	SELECT modulus(2, 3) LIMIT 1
multiply	乘法	multiply(number T, number) -> number	SELECT multiply(2, 3) LIMIT 1
pi	π	pi() -> double	SELECT pi() LIMIT 1
pow	T 的次幂	pow(number T, number) -> T	SELECT pow(2, 3) LIMIT 1
power	T 的次幂	power(number T) -> T, power(number T, number) -> T	SELECT power(2, 3) LIMIT 1
rand	随机数	rand() -> number, rand(number T) -> T	SELECT rand(5) LIMIT 1
rint	舍弃小数	rint(number T) -> T	SELECT rint(1.5) LIMIT 1
round	四舍五入	round(number T) -> T	SELECT round(1.5) LIMIT 1
sign	符号	sign(number T) -> T	SELECT sign(1.5) LIMIT 1
signum	符号	signum(number T) -> T	SELECT signum(0.5) LIMIT 1
sqrt	平方根	sqrt(number T) -> T	SELECT sqrt(0.5) LIMIT 1
subtract	减法	subtract(number T, number) -> T	SELECT subtract(3, 2) LIMIT 1

函数	作用	定义	示例
/	除法	number / number -> number	SELECT 1 / 100 LIMIT 1
%	取余	number % number -> number	SELECT 1 % 100 LIMIT 1

三角函数

表 11-54 三角函数

函数	作用	定义	示例
acos	反余弦	acos(number T) -> double	SELECT acos(0.5) LIMIT 1
asin	反正弦	asin(number T) -> double	SELECT asin(0.5) LIMIT 1
atan	反正切	atan(number T) -> double	SELECT atan(0.5) LIMIT 1
atan2	T 和 U 相除的结果的反正切	atan2(number T, number U) -> double	SELECT atan2(1, 0.5) LIMIT 1
cos	余弦	cos(number T) -> double	SELECT cos(0.5) LIMIT 1
cosh	双曲余弦	cosh(number T) -> double	SELECT cosh(0.5) LIMIT 1
cot	余切	cot(number T) -> double	SELECT cot(0.5) LIMIT 1
degrees	弧度转换为度	degrees(number T) -> double	SELECT degrees(0.5) LIMIT 1
radians	度转换为弧度	radians(number T) -> double	SELECT radians(0.5) LIMIT 1
sin	正弦	sin(number T) -> double	SELECT sin(0.5) LIMIT 1
sinh	双曲正弦	sinh(number T) -> double	SELECT sinh(0.5) LIMIT 1
tan	正切	tan(number T) -> double	SELECT tan(0.5) LIMIT 1

时间函数

表 11-55 时间函数

函数	作用	定义	示例
curdate	当前日期	curdate() -> date	SELECT curdate() LIMIT 1
date	日期	date(date) -> date	SELECT date() LIMIT 1

函数	作用	定义	示例
date_format	根据格式获取对应日期值	date_format(date, string) -> string	SELECT date_format(date, 'Y') LIMIT 1
day_of_month	月份	day_of_month(date) -> integer	SELECT day_of_month(date) LIMIT 1
day_of_week	周几	day_of_week(date) -> integer	SELECT day_of_week(date) LIMIT 1
day_of_year	当年天数	day_of_year(date) -> integer	SELECT day_of_year(date) LIMIT 1
hour_of_day	当天小时数	hour_of_day(date) -> integer	SELECT hour_of_day(date) LIMIT 1
maketime	生成日期	maketime(integer, integer, integer) -> time	SELECT maketime(11, 30, 00) LIMIT 1
minute_of_hour	当前小时分钟数	minute_of_hour(date) -> integer	SELECT minute_of_hour(date) LIMIT 1
minute_of_day	当天分钟数	minute_of_day(date) -> integer	SELECT minute_of_day(date) LIMIT 1
monthname	月份名称	monthname(date) -> string	SELECT monthname(date) LIMIT 1
now	当前时间	now() -> time	SELECT now() LIMIT 1
second_of_minute	秒数	minute_of_day(date) -> integer	SELECT minute_of_day(date) LIMIT 1
timestamp	日期	timestamp(date) -> date	SELECT timestamp(date) LIMIT 1
year	年份	year(date) -> integer	SELECT year(date) LIMIT 1

文本函数

表 11-56 文本函数

函数	作用	定义	示例
ascii	第一个字符的ASCII 值	ascii(string T) -> integer	SELECT ascii('t') LIMIT 1
concat_ws	连接字符串	concat_ws(separator, string, string) -> string	SELECT concat_ws('-', 'Tutorial', 'is', 'fun!') LIMIT 1
left	从左往右取字符串	left(string T, integer) -> T	SELECT left('hello', 2) LIMIT 1

函数	作用	定义	示例
length	长度	length(string) -> integer	SELECT length('hello') LIMIT 1
locate	查找字符串	locate(string, string) -> integer	SELECT locate('o', 'hello') LIMIT 1
replace	替换字符串	replace(string T, string, string) -> T	SELECT replace('hello', 'l', 'x') LIMIT 1
right	从右往左取字符串	right(string T, integer) -> T	SELECT right('hello', 1) LIMIT 1
rtrim	去除右侧空字符串	rtrim(string T) -> T	SELECT rtrim('hello ') LIMIT 1
substring	取子字符串	substring(string T, integer, integer) -> T	SELECT substring('hello', 2,5) LIMIT 1
trim	去除两侧空字符串	trim(string T) -> T	SELECT trim(' hello ') LIMIT 1
upper	全部转为大写	upper(string T) -> T	SELECT upper('helloworld') LIMIT 1

其他

表 11-57 其他

函数	作用	定义	示例
if	if 判断	if(boolean, object, object) -> object	SELECT if(false, 0, 1) LIMIT 1 , SELECT if(true, 0, 1) LIMIT 1
ifnull	字段为 null 时，填充默认值	ifnull(object, object) -> object	SELECT ifnull('hello', 1) LIMIT 1 , SELECT ifnull(null, 1) LIMIT 1
isnull	字段是否为 null，是返回 1，否返回 0	isnull(object) -> integer	SELECT isnull(null) LIMIT 1 , SELECT isnull(1) LIMIT 1

11.3.3.7 聚合函数

完整的分析语句语法如下：

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

本章节介绍聚合函数。

表 11-58 聚合函数

函数	作用	定义	示例
avg	求平均	avg(number T) -> T	SELECT avg(age) LIMIT 1
sum	求和	sum(number T) -> T	SELECT sum(age) LIMIT 1
min	最小值	min(number T) -> T	SELECT min(age) LIMIT 1
max	最大值	max(number T) -> T	SELECT max(age) LIMIT 1
count	次数	count(field) -> integer , count(*) -> integer , count(1) -> integer	SELECT count(age) LIMIT 1 , SELECT count(*) LIMIT 1 , SELECT count(1) LIMIT 1

11.4 数据投递

11.4.1 数据投递概述

操作场景

态势感知（专业版）支持将数据实时投递至其他管道或其他云产品中，便于您存储数据或联合其它系统消费数据。配置数据投递后，态势感知（专业版）将定时将采集到的数据投递至其他管道或对应的云产品。

表 11-59 数据投递场景说明

分类	投递场景	场景说明
数据投递场景	投递日志数据至其他数据管道	投递日志数据到其他数据管道。
	投递日志数据至OBS 桶	投递日志数据到对象存储服务（Object Storage Service，OBS）。
	投递日志数据至LTS	投递日志数据到云日志服务（Log Tank Service，LTS）。

分类	投递场景	场景说明
管理数据投递任务	管理数据投递任务	包括查看数据投递任务、挂起投递任务、启动投递任务、删除投递任务。 • 查看数据投递任务：查看数据投递任务相关信息。 • 挂起投递任务：数据投递成功后，如需停止投递，可挂起目标投递任务。 • 启动投递任务：数据投递任务停止投递后，如需重启投递，可启动目标投递任务。 • 删除投递任务：如果不再需要某个投递任务，可删除投递任务。

功能优势

- 操作简单：只需要在控制台中完成简单的配置，即可将态势感知（专业版）的数据投递至 OBS 等云产品。
- 数据集中：态势感知（专业版）已完成不同服务中的数据集中化，只需要将采集到的数据投递到 OBS 等云产品中，即可完成数据集中管理。
- 分类管理：态势感知（专业版）的采集数据时，对数据进行了分类管理。可以利用此功能，将不同项目、不同类型的数据投递到不同的云产品中。

前提条件

- 仅态势感知（专业版）标准版或专业版支持，态势感知（专业版）基础版不支持该功能。
- 云服务日志已接入态势感知（专业版），态势感知（专业版）的数据管道中已有数据。如需接入云服务日志请参见接入日志数据。
- 如需投递到 OBS 中，需要已有一个桶策略为私有、公共读或公共读写的可用的桶（暂不支持并行文件桶）。
- 如需投递到 LTS 中，需要已有可用的日志组和日志流。

约束与限制

- 跨账号投递仅支持投递到其他账号管道中，不支持投递到其他云服务。
- 如果新增的数据投递为跨账号投递，则需要登录目的账号进行授权操作。

11.4.2 投递日志数据至其他数据管道

操作场景

本章节介绍如何投递日志数据至其他数据管道。主要步骤如下：

- 步骤一：创建数据投递任务
- 步骤二：数据投递授权

- 步骤三：在数据投递的目的数据管道查看数据投递

约束与限制

- 跨账号投递仅支持投递到其他账号管道中，不支持投递到其他云服务。
- 如果新增的数据投递为跨账号投递，则需要登录目的账号进行授权操作。

步骤一：创建数据投递任务

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道后，单击目标管道名称后的“更多 > 投递”，右侧弹出现在数据投递设置页面。

图 11-22 进入投递设置页面

步骤 6 （可选）在弹出的授权提示中，确认无误后，单击“确定”，完成授权。

首次投递到目的投递类型需要进行授权，如果已经授权，则无需执行此步骤。

步骤 7 在新增投递配置页面中，配置数据投递相关参数。

1. 配置基本信息。

表 11-60 基本信息

参数名称	参数说明
投递名称	自定义投递名称。
投递资源消耗	默认生成，**无需配置**。

2. 配置数据源。

   数据源配置中，显示当前管道数据的详细信息，**无需配置**。

表 11-61 数据源参数说明

参数名称	参数说明
投递类型	数据投递类型，默认显示为 PIPE，即默认从态势感知（专业版）管道投递。

参数名称	参数说明
区域	当前管道所在区域。
工作空间	当前管道所属的工作空间。
数据空间	当前管道所属的数据空间。
管道	管道的名称。
数据位置策略	当前管道中数据位置的策略。
读取身份	数据源读取身份信息说明。

3. 配置数据目的，请根据投递目的进行配置。
   - PIPE：将当前管道数据投递到本账号其他管道或其他账号的管道中，请根据您的需要进行选择配置。
     - 本账号投递：将当前管道数据投递到本账号的其他管道中，参数配置说明如表 11-62 所示。

表 11-62 配置数据目的-本账号 PIPE

参数名称	参数说明
账号类型	选择数据投递目的地的账号类型，**此处选择“本账号”**。
投递类型	选择投递类型，**此处选择 PIPE**。
工作空间	选择目的 PIPE 所在工作空间。
数据空间	选择目的 PIPE 所在数据空间。
管道	选择目的 PIPE 所在管道。
写入身份	默认生成，**无需配置**。

     - 跨账号投递：将当前管道数据投递到其他账号的管道中，参数配置说明如表 11-63 所示。

表 11-63 配置数据目的-跨账号 PIPE

参数名称	参数说明
账号类型	选择数据投递目的地的账号类型，**此处选择“跨账号”**。
投递类型	选择投递类型，**此处选择 PIPE**。
账号 ID	输入目的 PIPE 所在账号的 ID。
工作空间 ID	输入目的 PIPE 所在工作空间的 ID，查询方法请参见步骤 6。

参数名称	参数说明
数据空间 ID	输入目的 PIPE 所在数据空间的 ID，查询方法请参见步骤 6。
管道 ID	输入目的 PIPE 的 ID，查询方法请参见步骤 6。
写入身份	默认生成，**无需配置**。

4. 在“访问授权”中，查看步骤 6 中授予的权限。

   投递请求需要获取访问您云资源的读写权限，授权后，投递任务才能拥有对您云资源相应的访问权限。

步骤 8 单击“确定”。

----结束

步骤二：数据投递授权

步骤 1 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 2 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 3 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面后，选择“数据投递管理”页签，进入数据投递管理页面。

步骤 4 在数据投递管理页面，选择“投递权限授予”页签，进入投递权限授权页面后，单击目标投递任务所在行“操作”列的“接受”。

如需批量接受授权，可以勾选所有需要授权的任务，然后单击列表左上角的“接受”。

授权授予后，目标投递任务授权状态更新为“已授权”，更新后，可前往投递目的地查看投递情况。

----结束

步骤三：在数据投递的目的数据管道中查看数据投递

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

步骤 6 在目标管道中，查看投递的日志信息。

----结束

数据投递授权相关操作

在跨租投递权限授权页面可以对投递权限进行**拒绝**和**取消**授权操作：

表 11-64 跨租投递权限管理

操作	具体操作方法
拒绝	在目标投递任务所在行“操作”列，单击“拒绝”。 如需批量拒绝授权，可以勾选所有需要拒绝的任务，然后单击列表左上角的“拒绝”。
取消	1. 在目标投递任务所在行“操作”列，单击“取消”。 如需批量取消授权，可以勾选所有需要取消的任务，然后单击列表左上角的“取消”。 2. 在弹出的确认框中，单击“确定”。

11.4.3 投递日志数据至 OBS 桶

操作场景

本章节介绍如何投递日志数据至 OBS 桶。主要步骤如下：

步骤一：创建数据投递任务

步骤二：数据投递授权

步骤三：在 OBS 中查看数据投递

约束与限制

- 跨账号投递仅支持投递到其他账号管道中，不支持投递到其他云服务。
- 如果新增的数据投递为跨账号投递，则需要登录目的账号进行授权操作。

步骤一：创建数据投递任务

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道后，单击目标管道名称后的“更多 > 投递”，右侧弹出现在数据投递设置页面。

图 11-23 进入投递设置页面

步骤 6 （可选）在弹出的授权提示中，确认无误后，单击“确定”，完成授权。

首次投递到目的投递类型需要进行授权，如果已经授权，则无需执行此步骤。

步骤 7 在新增投递配置页面中，配置数据投递相关参数。

1. 配置基本信息。

表 11-65 基本信息

参数名称	参数说明
投递名称	自定义投递名称。
投递资源消耗	默认生成，**无需配置**。

2. 配置数据源。

数据源配置中，显示当前管道数据的详细信息，**无需配置**。

表 11-66 数据源参数说明

参数名称	参数说明
投递类型	数据投递类型，默认显示为 PIPE，即默认从态势感知（专业版）管道投递数据。
区域	当前管道所在区域。
工作空间	当前管道所属的工作空间。
数据空间	当前管道所属的数据空间。
管道	管道的名称。
数据位置策略	当前管道中数据位置的策略。
读取身份	数据源读取身份信息说明。

3. 配置数据目的，请根据投递目的进行配置。

- OBS：将当前管道数据投递到 OBS 服务，参数配置说明如表 11-67 所示。

  投递到 OBS 中，需要已有一个桶策略为私有、公共读或公共读写的可用的桶（暂不支持并行文件桶）。

表 11-67 配置数据目的-OBS

参数名称	参数说明
账号类型	选择数据投递目的地的账号类型。**投递到 OBS 服务仅支持选择“本账号”类型。**
投递类型	选择投递类型，**此处选择 OBS。**
桶名称	选择目的 OBS 桶名称。
写入身份	默认生成，**无需配置**。

4. 在“访问授权”中，查看步骤 6 中授予的权限。

   投递请求需要获取访问您云资源的读写权限，授权后，投递任务才能拥有对您云资源相应的访问权限。

步骤 8 单击“确定”。

----结束

步骤二：数据投递授权

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面后，选择“数据投递管理”页签，进入数据投递管理页面。

步骤 5 在数据投递管理页面，选择“投递权限授予”页签，进入投递权限授权页面后，单击目标投递任务所在行“操作”列的“接受”。

如需批量接受授权，可以勾选所有需要授权的任务，然后单击列表左上角的“接受”。

授权授予后，目标投递任务授权状态更新为“已授权”，更新后，可前往投递目的地查看投递情况。

----结束

步骤三：在 OBS 中查看数据投递

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“存储 > 对象存储服务”，默认进入桶列表管理页面。

步骤 3 在桶列表页面中，单击新增数据投递时选择的 OBS 桶的名称，进入目标 OBS 桶详情页面。

步骤 4 在 OBS 桶详情页面，查看投递的日志信息。

----结束

数据投递授权相关操作

在跨租投递权限授权页面可以对投递权限进行**拒绝**和**取消**授权操作：

表 11-68 跨租投递权限管理

操作	具体操作方法
拒绝	在目标投递任务所在行“操作”列，单击“拒绝”。 如需批量拒绝授权，可以勾选所有需要拒绝的任务，然后单击列表左上角的“拒绝”。
取消	1. 在目标投递任务所在行“操作”列，单击“取消”。 如需批量取消授权，可以勾选所有需要取消的任务，然后单击列表左上角的“取消”。 2. 在弹出的确认框中，单击“确定”。

11.4.4 投递日志数据至 LTS

操作场景

态势感知（专业版）支持集成 WAF、HSS、CFW 等其他云产品日志，具体集成操作及支持集成的云服务请参见云服务接入。

集成后的日志还支持投递至云日志服务（Log Tank Service，简称 LTS），方便用户快速高效地进行实时决策分析、设备运维管理、用户业务趋势分析等。

本章节将介绍如何将集成的日志数据投递至 LTS。操作步骤如下：

- 步骤一：创建数据投递任务
- 步骤二：数据投递授权
- 步骤三：在 LTS 中查看投递数据

前提条件

- 已完成需投递日志的接入态势感知（专业版）操作，详细操作请参见云服务接入。
- 投递到 LTS 中，需要已有可用的日志组和日志流。

步骤一：创建数据投递任务

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道后，单击目标管道名称后的“更多 > 投递”，右侧弹出现在数据投递设置页面。

图 11-24 进入投递设置页面

步骤 6 （可选）首次投递到目的投递类型需要进行授权，如果已经授权，请跳过该步骤。

在弹出的授权提示中，确认无误后，单击“确定”，完成授权。

步骤 7 在新增投递配置页面中，配置数据投递相关参数。

- 投递名称：自定义数据投递名称。
- 账号类型：此处请选择“本账号”。投递到 LTS 服务仅支持投递本账号内的日志数据。
- 投递类型：此处请选择“LTS”。
- 日志组：选择 LTS 日志组。
- 日志流：选择目的 LTS 日志流。

其他配置参数，系统默认生成，无需配置。

步骤 8 单击“确定”。

----结束

步骤二：数据投递授权

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面后，选择“数据投递管理”页签，进入数据投递管理页面。

步骤 5 在数据投递管理页面，选择“投递权限授予”页签，进入投递权限授权页面后，单击目标投递任务所在行“操作”列的“接受”。

如需批量接受授权，可以勾选所有需要授权的任务，然后单击列表左上角的“接受”。

授权授予后，目标投递任务授权状态更新为“已授权”，更新后，可前往投递目的地查看投递情况。

----结束

步骤三：在 LTS 中查看投递数据

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“管理与监管 > 云日志服务”，进入日志管理页面。

步骤 3 在日志管理页面的“日志组列表”栏中，找到新增数据投递时填写的日志组，并单击日志组名称前的按钮。

步骤 4 展开后，单击新增数据投递时选择的日志流的名称，进入日志流详情页面。

步骤 5 在日志流详情页面，查看投递的日志信息。

----结束

数据投递授权相关操作

在跨租投递权限授权页面可以对投递权限进行**拒绝**和**取消**授权操作：

表 11-69 跨租投递权限管理

操作	具体操作方法
拒绝	在目标投递任务所在行“操作”列，单击“拒绝”。 如需批量拒绝授权，可以勾选所有需要拒绝的任务，然后单击列表左上角的“拒绝”。
取消	1. 在目标投递任务所在行“操作”列，单击“取消”。 如需批量取消授权，可以勾选所有需要取消的任务，然后单击列表左上角的“取消”。 2. 在弹出的确认框中，单击“确定”。

11.4.5 管理数据投递任务

操作场景

本章节介绍管理投递任务，请根据您的需要选择对应操作：

- 查看数据投递任务：查看数据投递任务相关信息。
- 挂起投递任务：数据投递成功后，如需停止投递，可挂起目标投递任务。
- 启动投递任务：数据投递任务停止投递后，如需重启投递，可启动目标投递任务。
- 删除投递任务：如果不在需要某个投递任务，可删除投递任务。

前提条件

已新增数据投递。

查看数据投递任务

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面后，选择“数据投递管理”页签，进入数据投递管理页面。

步骤 5 在投递任务列表页面中，查看已有投递任务。

表 11-70 投递任务

操作	操作说明
名称/ID	投递任务名称/ID。
数据源	投递任务的数据源所在的管道路径。
消费策略	投递任务的消费策略。
目的类型	数据投递目的地所属的类型。如 OBS、LTS 等。
投递目的信息	数据投递目的地相关信息。
监控	数据投递监控情况。可单击监控图标，查看数据消费情况。
状态	投递任务的状态。 • 投递中：已创建数据投递任务且已完成数据投递授权，数据投递中。 • 挂起 • 待授权：已创建数据投递任务，但是未执行数据投递授权。 • 授权失败：已创建数据投递任务，且拒绝了数据投递授权。 • 投递取消：取消了数据投递任务。
创建时间	投递任务创建时间。
操作	可对数据投递任务进行挂起、删除等操作。

----结束

挂起投递任务

数据投递新增并授权成功后，投递任务状态自动更新为投递中，如需停止投递，可挂起目标投递任务。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面后，选择“数据投递管理”页签，进入数据投递管理页面。

步骤 5 在数据投递管理页面，单击目标投递任务所在行“操作”列的“挂起”。

挂起后，投递任务状态更新为“挂起”，则表示挂起投递任务成功。

----结束

启动投递任务

数据投递任务停止投递后，如需重启投递，可启动目标投递任务。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面后，选择“数据投递管理”页签，进入数据投递管理页面。

步骤 5 在数据投递管理页面，单击目标投递任务所在行“操作”列的“启动”。

挂起后，投递任务状态更新为“投递中”，则表示启动投递任务成功。

----结束

删除投递任务

如果不再需要某个数据投递任务，可执行删除操作。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面后，选择“数据投递管理”页签，进入数据投递管理页面。

步骤 5 在数据投递管理页面，单击目标投递任务所在行“操作”列的“删除”，并在弹出的确认框中单击“确定”。

----结束

11.5 云服务接入

11.5.1 支持接入的云服务日志

态势感知（专业版）支持集成多种云产品的日志数据。集成后，可以检索并分析所有收集到的日志。

表 11-71 支持接入的日志

云服务	日志描述	日志	日志生命周期范围
Web 应用防火墙（Web Application Firewall，WAF）	攻击日志	waf-attack	7~30 天
	访问日志	waf-access	7~30 天
态势感知（专业版）	合规基线日志	secmaster-baseline	7~10 天
对象存储服务（Object Storage Service，OBS）	访问日志	obs-access	7~15 天
入侵防御系统（Intrusion Prevention System，IPS）	攻击日志	nip-attack	7~180 天
统一身份认证（Identity and Access Management，IAM）	审计日志	iam-audit	7~180 天
企业主机安全（Host Security Service，HSS）	主机安全告警	hss-alarm	7~180 天
	主机漏洞扫描结果	hss-vul	7 天
	主机安全日志	hss-log	7~15 天
数据安全中心（Data Security Center，DSC）	告警日志	dsc-alarm	7~180 天
Anti-DDoS 流量清洗（Anti-DDoS）	攻击日志	ddos-attack	7~180 天
数据库安全服务（Database Security Service，DBSS）	告警日志	dbss-alarm	7~180 天

云服务	日志描述	日志	日志生命周期范围
云审计服务（Cloud Trace Service，CTS）	云审计服务日志	cts-audit	7~180 天
云防火墙（Cloud Firewall，CFW）	访问控制日志	cfw-block	7~30 天
	流量日志	cfw-flow	7~15 天
	攻击事件日志	cfw-risk	7~180 天
API 网关（API Gateway）	访问日志	apig-access	7~180 天

11.5.2 接入日志数据

操作场景

态势感知（专业版）支持一键接入多种云产品的日志数据。接入后，可以统一管理日志信息，以及检索并分析所有收集到的日志。

建议将态势感知（专业版）管理的资产以及资产的告警、基线检查结果、漏洞数据、日志数据接入同一个工作空间，便于统一运营，进行安全分析关联。

本章节介绍如何接入数据并查看日志存储位置。

约束与限制

- 日志接入操作成功后，日志数据订阅预计在十分钟内生效。
- 态势感知（专业版）支持一键接入 CFW 日志数据，若接入的是**新购买的** CFW 的日志数据，由于日志上报存在一定的延迟，如果您当天在态势感知（专业版）执行了接入 CFW 日志操作，则将会隔天才能在态势感知（专业版）中查看到上报的 CFW 日志数据。

接入云服务日志

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“日志审计 > 云服务接入”，进入云服务日志接入页面。

步骤 5 在云服务日志接入页面，配置日志接入。**请根据当前 region 已开通云服务按需进行接入。**

一键接入多个云服务产品的日志，在云服务日志接入页面，单击“一键接入”按钮，右侧弹出“一键接入”配置页面。在一键接入配置页面，下拉选择**数据源区域**，下拉勾选需要接入的云服务日志。配置完成后，单击右下角“确定”，完成设置。

步骤 6 **云服务日志接入也支持设置单个云产品的日志接入。**在云服务接入管理页面，单击云服务产品所在行操作列的“设置”，右侧弹出日志接入设置配置页面。

在设置页面，根据需要配置接入开关。

表 11-72 云服务日志接入设置页面参数说明

参数名称	参数说明
日志类型	日志的类型。
日志接入	设置日志接入开关。按钮打开表示日志接入态势感知（专业版）。
自动转告警	在“自动转告警”列，单击，开启后，当接入的云服务日志满足告警触发条件时，自动转为告警，并且在“告警管理”页面中进行展示。
生命周期	日志接入后的存储时长。
日志状态	日志接入的状态。 • 已接入：日志已接入且执行成功。 • 未接入：日志未接入。 • 接入失败：日志接入且执行失败。
最近活跃时间	最近日志接入时间，即活跃时间。
操作	单击“编辑”，可设置该日志类型的生命周期，单位天。生命周期指的是日志接入后的存储时长。

步骤 7 云服务日志接入配置完成后，在“日志审计 > 云服务接入”页面可查看云服务产品的日志接入状态。

操作成功后，日志数据订阅预计在十分钟内生效。接入完成后，将创建默认数据空间和管道。

----结束

查看日志数据及其存储位置

日志数据接入完成后，请前往安全分析的安全数据表页面查看接入的日志数据：

1. 在左侧导航栏选择“日志审计 > 安全数据”，进入安全分析页面。
2. 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

   在管道数据检索页面即可查看接入的日志数据。

相关操作

- 取消数据接入
  a. 在云服务接入管理页面，单击待取消接入云服务产品所在行操作列的“设置”，右侧弹出日志接入设置配置页面。
  b. 在设置页面，单击“日志接入”列的，关闭接入的云服务日志。
- 编辑数据接入生命周期
  a. 在云服务接入管理页面，单击对应云服务产品所在行操作列的“设置”，右侧弹出日志接入设置配置页面。
  b. 在设置页面，单击日志所在行操作列的“编辑”按钮。
  c. 在弹出的编辑页面，修改“生命周期”配置，输入生命周期时间。
  d. 修改完成后，单击“确定”。
- 取消自动转告警
  a. 在云服务接入管理页面，单击对应云服务产品所在行操作列的“设置”，右侧弹出日志接入设置配置页面。
  b. 在设置页面，单击“自动转告警”列的，关闭告警映射。

12 建模分析

12.1 智能建模

12.1.1 智能建模概述

基本概念

- 模板：态势感知（专业版）内置了多种分析规则模板（包括场景说明、模型原理、处置建议、使用约束等信息），用户可利用内置的模板快速创建模型。
- 模型：模型是基于模板创建的，态势感知（专业版）支持利用模型对管道中的日志数据进行扫描，如果检测到有满足模型中设置触发条件的内容时，系统将产生告警提示。

操作场景

本文介绍模型模板的管理操作。

- 查看模型模板：态势感知（专业版）根据常用场景内置了多种模型模板（包括场景说明、模型原理、处置建议、使用约束等信息），支持查看模板的详情信息。
- 新建或编辑模型：态势感知（专业版）支持利用模型对管道中的日志数据进行监控，如果检测到有满足模型中设置触发条件的内容时，将产生告警提示。新建模型可以使用使用已有模型模板创建告警模型，也支持自定义新建告警模型。当模型的信息发生变化需要更新时可编辑模型。
- 查看模型：可查看模型的严重程度和模型列表信息。模型列表中，可查看当前已有模型的严重程度、名称/ID、管道名称、模型类型、更新时间和创建时间等信息。
- 管理模型：介绍如何启用、停用、删除模型。

12.1.2 查看模型模板

操作场景

态势感知（专业版）支持利用模型对管道中的日志数据进行扫描，如果检测到有满足模型中设置触发条件的内容时，系统将产生告警提示。模型是基于模板而创建的，因此，需利用已有模型模板创建模型。

态势感知（专业版）根据常用场景内置了多种模型模板（包括场景说明、模型原理、处置建议、使用约束等信息），请在参考本章节进行查看。

查看模型模板

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“建模分析 > 智能建模”，进入智能建模页面后，选择“模型模板”页签，进入模型模板页面。

步骤 5 在模型模板页面，查看已有模型模板。

表 12-1 查看模板信息

参数名称	参数说明
模型模板统计	显示**可用模板**和**活跃模板**数量。 • 可用模板：可用的模板总数。 • 活跃模板：指已经被用来创建模型的模板，会被统计为活跃模板。使用模板创建模型请参见新建或编辑模型。

参数名称	参数说明
严重程度	显示当前已有模板的严重程度统计情况，与模板关联的告警的严重程度一致，包含致命、高危、中危、低危、提示级别。 • 致命：致命级别的告警表示系统已经受到严重的攻击，可能导致数据丢失、系统崩溃或者长时间的服务中断。例如，发现勒索加密行为或恶意程序感染。建议您立即处理，避免对系统造成更严重的损害。 • 高危：高危级别的告警表示系统可能正在受到攻击，但尚未造成严重的损害。例如，检测到未授权的登录尝试或执行了危险命令（如删除关键系统文件或修改系统设置的命令）。建议您及时调查并采取措施，以防止攻击蔓延。 • 中危：中危级别的告警表示系统存在潜在的安全威胁，但目前没有明显遭受攻击的迹象。例如，检测到文件或目录的异常修改，表明系统可能存在潜在的攻击路径或配置错误。建议您进一步分析并采取适当的防范措施，以确保系统的安全。 • 低危：低危级别的告警表示系统存在轻微的安全威胁，不会对系统的正常运行产生显著影响。例如，检测到一些端口扫描行为，这些行为通常是攻击者尝试寻找系统漏洞的前奏。这类告警可以在合适的时间进行处理，不需要立即采取紧急措施。如果您的资产安全等级要求较高，可以关注该等级的安全告警。 • 提示：对应资源存在潜在的错误可能影响到业务。如果您对您的资产的安全等级要求较高，可以关注该等级的安全告警。
模板列表	• 模板列表中，显示当前已有模板的严重程度、名称、模型类型、更新时间和创建时间等信息。 • 如需查看某个模型模板的详细信息，可单击模板所在行“操作”列的“详情”，右侧弹出当前模板详情页面。 在详情页面中可以查看当前模型模板的描述信息、查询规则、触发条件、查询计划等信息。

----结束

12.1.3 新建或编辑模型

操作场景

态势感知（专业版）支持利用模型对管道中的日志数据进行监控，如果检测到有满足模型中设置触发条件的内容时，将产生告警提示。

新建模型可以使用已有内置模型模板进行创建模型，同时，也支持自定义新建告警模型：

- 使用已有模型模板创建告警模型
- 自定义新建告警模型
- 编辑模型

使用已有模型模板创建告警模型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“建模分析 > 智能建模”，进入智能建模页面后，选择“模型模板”页签，进入模型模板页面。

步骤 5 在模型模板列表中，单击目标模型模板所在行“操作”列的“详情”，右侧弹出模板详情页面。

步骤 6 在模型模板详情页面，单击右下角“创建模型”，进入新建告警模型页面。

步骤 7 在新增告警模型页面中，配置告警模型基础信息，参数说明如表 12-2 所示。

表 12-2 告警模型基础配置

参数名称	参数说明
管道名称	请根据此页面的“描述”中的“使用约束”中描述的管道来选择该告警模型的执行管道。
模型名称	自定义该条告警模型的名称。

参数名称	参数说明
严重程度	设置该告警模型的严重程度。 可以设置致命、高危、中危、低危、提示级别。 • 致命：致命级别的告警表示系统已经受到严重的攻击，可能导致数据丢失、系统崩溃或者长时间的服务中断。例如，发现勒索加密行为或恶意程序感染。建议您立即处理，避免对系统造成更严重的损害。 • 高危：高危级别的告警表示系统可能正在受到攻击，但尚未造成严重的损害。例如，检测到未授权的登录尝试或执行了危险命令（如删除关键系统文件或修改系统设置的命令）。建议您及时调查并采取措施，以防止攻击蔓延。 • 中危：中危级别的告警表示系统存在潜在的安全威胁，但目前没有明显遭受攻击的迹象。例如，检测到文件或目录的异常修改，表明系统可能存在潜在的攻击路径或配置错误。建议您进一步分析并采取适当的防范措施，以确保系统的安全。 • 低危：低危级别的告警表示系统存在轻微的安全威胁，不会对系统的正常运行产生显著影响。例如，检测到一些端口扫描行为，这些行为通常是攻击者尝试寻找系统漏洞的前奏。这类告警可以在合适的时间进行处理，不需要立即采取紧急措施。如果您的资产安全等级要求较高，可以关注该等级的安全告警。 • 提示：对应资源存在潜在的错误可能影响到业务。如果您对您的资产的安全等级要求较高，可以关注该等级的安全告警。
告警类型	选择该条告警模型触发后，提示的告警类型。
模型类型	默认为规则模型。
描述	该告警模型的描述信息。
启用状态	设置该告警模型的启用状态。 此处设置的状态，可在整个告警模型设置成功后进行更改。

步骤 8 设置完成后，单击页面右下角“下一步”，进入设置模型逻辑页面。

步骤 9 设置模型逻辑，参数说明如表 12-3 所示。

表 12-3 设置模型逻辑

参数名称	参数说明

参数名称	参数说明
查询规则	设置告警的查询规则，设置完成后可以单击“运行”，查看当前运行结果。 查询分析语句由查询语句和分析语句构成，格式为**查询语句|分析语句**，查询分析语句语法详细内容请参见查询与分析语法概述。 **说明** 如果筛留字段为 text 类型时，默认会使用 MATCH_QUERY 进行分词查询。
查询计划	设置告警查询计划。 • 运行查询间隔：xx 分钟/小时/天。 当运行查询间隔为分钟时，可设置为 5-59 分钟；当运行查询为小时时，可设置为 1-23 小时；当运行查询为天时，可设置为 1-14 天。 • 时间窗口：xx 分钟/小时/天。 当时间窗口为分钟时，可设置为 5-59 分钟；当时间窗口为小时时，可设置为 1-23 小时；当时间窗口为天时，可设置为 1-14 天。 • 延迟执行时间：xx 分钟，可以设置为 0-5 分钟。
告警扩充	• 自定义信息：自定义告警扩充信息。 单击“添加”，并设置 key+value 信息，完成新增。 • 告警详细信息：自定义填写告警名称、描述和处置建议。
触发条件	设置告警触发条件。可设置为：大于/等于/不等于/小于 xx 时，触发告警。 如有多条触发条件，可以单击“添加”按钮进行添加，最多可添加 5 个触发条件。 当设置了多个触发条件时，在日志数据扫描检测中，系统将按照从上到下的校验逻辑，如果有满足此处设置的触发条件被检测到时，系统都将展示不同类型的告警。
告警分组	配置将规则查询结果分组到告警的方式。可选择以下方式： • 将所有查询结果分组到一个告警中 • 将每条查询结果独立触发告警
调试模式	设置是否生成调试类告警。
抑制	设置生产告警后是否停止运行查询。 • 如果设置为抑制，即生成告警后**停止**运行查询。 • 如果设置为不抑制，即生成告警后**不停止**运行查询。

步骤 10 设置完成后，单击页面右下角“下一步”，进入模型详情预览页面。

步骤 11 预览确认无误后，单击页面右下角“确定”。

----结束

自定义新建告警模型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“建模分析 > 智能建模”，进入智能建模的可用模型页面。

步骤 5 在可用模型列表左上角单击“新建模型”，进入新建告警模型页面。

步骤 6 在新增告警模型页面中，配置告警模型基础信息，参数说明如表 12-4 所示。

表 12-4 告警模型基础配置

参数名称	参数说明
管道名称	选择该告警模型的执行管道。
模型名称	自定义该条告警模型的名称。

参数名称	参数说明
严重程度	设置该告警模型的严重程度。可以设置致命、高危、中危、低危、提示级别。 • 致命：致命级别的告警表示系统已经受到严重的攻击，可能导致数据丢失、系统崩溃或者长时间的服务中断。例如，发现勒索加密行为或恶意程序感染。建议您立即处理，避免对系统造成更严重的损害。 • 高危：高危级别的告警表示系统可能正在受到攻击，但尚未造成严重的损害。例如，检测到未授权的登录尝试或执行了危险命令（如删除关键系统文件或修改系统设置的命令）。建议您及时调查并采取措施，以防止攻击蔓延。 • 中危：中危级别的告警表示系统存在潜在的安全威胁，但目前没有明显遭受攻击的迹象。例如，检测到文件或目录的异常修改，表明系统可能存在潜在的攻击路径或配置错误。建议您进一步分析并采取适当的防范措施，以确保系统的安全。 • 低危：低危级别的告警表示系统存在轻微的安全威胁，不会对系统的正常运行产生显著影响。例如，检测到一些端口扫描行为，这些行为通常是攻击者尝试寻找系统漏洞的前奏。这类告警可以在合适的时间进行处理，不需要立即采取紧急措施。如果您的资产安全等级要求较高，可以关注该等级的安全告警。 • 提示：对应资源存在潜在的错误可能影响到业务。如果您对您的资产的安全等级要求较高，可以关注该等级的安全告警。
告警类型	选择该条告警模型触发后，提示的告警类型。
模型类型	默认为规则模型。
描述	该告警模型的描述信息。
启用状态	设置该告警模型的启用状态。 此处设置的状态，可在整个告警模型设置成功后进行更改。

步骤 7 设置完成后，单击页面右下角“下一步”，进入设置模型逻辑页面。

步骤 8 设置模型逻辑，参数说明如表 12-5 所示。

表 12-5 设置模型逻辑

参数名称	参数说明

参数名称	参数说明
查询规则	设置告警的查询规则，设置完成后可以单击“运行”，查看当前运行结果。 语法参考请参见查询与分析语法概述。
查询计划	设置告警查询计划。 • 运行查询间隔：xx 分钟/小时/天。 当运行查询间隔为分钟时，可设置为 5-59 分钟；当运行查询为小时时，可设置为 1-23 小时；当运行查询为天时，可设置为 1-14 天。 • 时间窗口：xx 分钟/小时/天。 当时间窗口为分钟时，可设置为 5-59 分钟；当时间窗口为小时时，可设置为 1-23 小时；当时间窗口为天时，可设置为 1-14 天。 • 延迟执行时间：xx 分钟，可以设置为 0-5 分钟。
告警扩充	• 自定义告警扩充信息。 单击“添加”，并设置 key+value 信息，完成新增。 • 告警详细信息：自定义填写告警名称、描述和处置建议。
触发条件	设置告警触发条件。可设置为：大于/等于/不等于/小于 xx 时，触发告警。 如有多条触发条件，可以单击“添加”按钮进行添加，最多可添加 5 个触发条件。 当设置了多个触发条件时，在日志数据扫描检测中，如果有满足此处设置的不同的触发条件被检测到时，系统都将展示不同类型的告警。
告警分组	配置将规则查询结果分组到告警的方式。可选择以下方式： • 将所有查询结果分组到一个告警中 • 将每条查询结果独立触发告警
调试模式	设置是否生成调试类告警。
抑制	设置生产告警后是否停止运行查询。 • 如果开启，则表示抑制，即生成告警后**停止**运行查询。 • 如果关闭，表示不抑制，即生成告警后**不停止**运行查询。

步骤 9 设置完成后，单击页面右下角“下一步”，进入模型详情预览页面。

步骤 10 预览确认无误后，单击页面右下角“确定”。

----结束

编辑模型

仅支持编辑自定义创建的模型。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“建模分析 > 智能建模”，进入智能建模的可用模型页面。

步骤 5 在可用模型列表中，单击目标模型所在行“操作”列的“编辑”，右侧弹出编辑告警模型页面。

步骤 6 在编辑告警模型页面中，配置告警模型基础信息，参数说明如表 12-6 所示。

表 12-6 告警模型基础配置

参数名称	参数说明
管道名称	选择该告警模型的执行管道。**暂不支持编辑**。
模型名称	自定义该条告警模型的名称。
严重程度	设置该告警模型的严重程度。可以设置致命、高危、中危、低危、提示级别。
告警类型	选择该条告警模型触发后，提示的告警类型。
模型类型	默认为规则模型。
描述	该告警模型的描述信息。

步骤 7 设置完成后，单击页面右下角“下一步”，进入设置模型逻辑页面。

步骤 8 设置模型逻辑，参数说明如表 12-7 所示。

表 12-7 设置模型逻辑

参数名称	参数说明
查询规则	设置告警的查询规则，设置完成后可以单击“运行”，查看当前运行结果。 查询分析语句由查询语句和分析语句构成，格式为**查询语句|分析语句**，查询分析语句语法详细内容请参见查询与分析语法概述。 **说明** 如果筛留字段为 text 类型时，默认会使用 MATCH_QUERY 进行分词查询。

参数名称	参数说明
查询计划	设置告警查询计划。 • 运行查询间隔：xx 分钟/小时/天。 当运行查询间隔为分钟时，可设置为 5-59 分钟；当运行查询为小时时，可设置为 1-23 小时；当运行查询为天时，可设置为 1-14 天。 • 时间窗口：xx 分钟/小时/天。 当时间窗口为分钟时，可设置为 5-59 分钟；当时间窗口为小时时，可设置为 1-23 小时；当时间窗口为天时，可设置为 1-14 天。 • 延迟执行时间：xx 分钟，可以设置为 0-5 分钟。
告警扩充	• 自定义信息：自定义告警扩充信息。 单击“添加”，并设置 key+value 信息，完成新增。 • 告警详细信息：自定义填写告警名称、描述和处置建议。
触发条件	设置告警触发条件。可设置为：大于/等于/不等于/小于 xx 时，触发告警。 如有多条触发条件，可以单击“添加”按钮进行添加，最多可添加 5 个触发条件。 当设置了多个触发条件时，在日志数据扫描检测中，系统将按照从上到下的校验逻辑，如果有满足此处设置的触发条件被检测到时，系统都将展示不同类型的告警。
告警分组	配置将规则查询结果分组到告警的方式。可选择以下方式： • 将所有查询结果分组到一个告警中 • 将每条查询结果独立触发告警
调试模式	设置是否生成调试类告警。
抑制	设置生产告警后是否停止运行查询。 • 如果设置为抑制，即生成告警后**停止**运行查询。 • 如果设置为不抑制，即生成告警后**不停止**运行查询。

步骤 9 设置完成后，单击页面右下角“下一步”，进入模型详情预览页面。

步骤 10 预览确认无误后，单击页面右下角“确定”。

----结束

12.1.4 查看模型

操作场景

本章节将介绍如何查看模型。模型列表中，可查看当前已有模型的严重程度、名称/ID、管道名称、模型类型、更新时间和创建时间等信息。

前提条件

已新增模型，详细操作请参见新建或编辑模型。

查看模型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“建模分析 > 智能建模”，进入智能建模的可用模型页面。

步骤 5 在可用模型页面，查看已有模型。

表 12-8 查看已有模型信息

参数名称	参数说明
模型统计	显示**可用模型**和**活跃模型**数量。
严重程度	显示当前已有模型的严重程度统计情况，包含致命、高危、中危、低危、提示级别。
模型列表	模型列表中，显示当前已有模型的严重程度、名称/ID、管道名称、模型类型、更新时间和创建时间等信息。

----结束

12.1.5 管理模型

操作场景

本章节将介绍如何管理模型，如启用、停用、删除自定义创建的模型等操作。

- 启用模型：态势感知（专业版）支持利用模型对管道中的日志数据进行监控，如果检测到有满足模型中设置触发条件的内容时，将产生告警提示。当用户完成模型新建后，需要使用模型来生成告警，则需要启用模型。
- 停用模型：当用户不再需要模型生成告警提示，则可以停用模型。

- 删除模型：当模型规则不再适用且确认未来也不会使用时，用户可选择删除模型。

约束与限制

仅支持对自定义创建的模型进行启用、停用、删除操作。

管理模型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“建模分析 > 智能建模”，进入智能建模的可用模型页面。

步骤 5 在可用模型页面中，管理模型。

表 12-9 管理模型

操作	操作说明
启用模型	在模型列表中，单击目标模型所在行“操作”列的“启用”。 **说明** 如需批量启动模型，可以勾选所有需要启动的模型，然后单击列表左上角的“启用”。 当模型状态更新为启用，则表示启动模型成功。
停用模型	在模型列表中，单击目标模型所在行“操作”列的“停用”。 **说明** 如需批量暂停模型，可以勾选所有需要暂停的模型，然后单击列表左上角的“停用”。 当告警模型状态更新为“停用”，表示停用成功。
删除模型	1. 在模型列表中，单击目标模型所在行“操作”列的“删除”。 **说明** 如需批量删除模型，可以勾选所有需要删除的模型，然后单击列表左上角的“删除”。 2. 在弹出的确认框中，单击“确定”。

----结束

13 安全编排

13.1 安全编排概述

安全编排（Security Orchestration）是将企业和组织在安全运营过程中涉及的不同系统或者一个系统内部不同组件的安全功能按照一定的逻辑关系组合到一起，以完成某个特定的安全运营过程和规程。旨在帮助企业和组织的安全团队快速并高效地响应网络威胁，实现安全事件的高效、自动化响应处置。

基本概念说明

在安全编排中，剧本和流程是两个核心元素，它们相互关联、依赖，并协同工作以确保安全运营的有效性和高效性。

- **剧本**

  剧本（Playbook）：是安全运营流程在安全编排系统中的形式化表述，它是将安全运营流程和规程转换为机读工作流的过程，剧本是一个预定义的、结构化的响应计划，用于处理特定类型的事件或威胁。剧本详细列出了在某些触发条件（如检测到特定安全事件）下应采取的步骤和操作。

  剧本体现了安全防护的逻辑，指示如何调度安全能力。剧本具有灵活性和可扩展性，可以根据实际需求进行修改和扩展，以适应不断变化的安全威胁和业务需求。

  一个剧本中有且仅有一个流程。

- **流程**

  流程（Workflow）：是将安全运营相关的工具、技术、流程和人员等各种能力整合到一起，形成一种协同工作方式。它由多个相连接的组件构成，流程定义完成后可被外部触发，例如，当新工单产生时自动触发自动审核工单流程。您可以通过可视化流程编辑画布，定义每个节点的组件动作。

  流程是剧本触发时响应的方式，它负责将剧本中的指令和规程转化为具体的操作和执行步骤。

- **剧本与流程的联系**

  剧本提供了安全运营的指导和规则，而流程则负责将这些规则转化为具体的执行步骤和操作。剧本和流程相互依赖，剧本指导流程的执行，而流程则实现了剧本的意图和要求。

- **剧本与流程的区别**

剧本和流程之间也存在一定的区别。首先，剧本更侧重于定义和描述安全运营的流程和规程，它关注的是整体的框架和策略；而流程则更侧重于具体的操作和执行步骤，它关注的是如何将剧本中的要求转化为实际的行动。其次，剧本具有较大的灵活性和可扩展性，可以根据需要进行修改和扩展；而流程则相对固定，一旦设计完成，就需要按照规定的步骤执行。

- **示例**

  以一个具体的网络安全事件响应案例为例，当组织遭受到一次网络攻击时，安全编排系统会首先根据预设的剧本识别出攻击的类型和严重程度。然后，系统会根据剧本中定义的流程，自动触发相应的安全措施，如隔离被攻击的系统、收集攻击数据、通知安全团队等。在这个过程中，剧本和流程紧密配合，确保安全响应的准确性和及时性。

安全编排使用流程

安全编排的使用流程如下：

图 13-1 安全编排使用流程

表 13-1 使用流程

序号	操作项	说明
1	启用流程	流程是剧本触发时响应的方式，态势感知（专业版）默认提供了“WAF 一键解封”、“主机告警状态同步”、“告警指标提取”等流程。 启用流程分为以下场景： • 场景一：使用初始版本的流程 流程的初始版本（V1）自动启用，无需手动启用。 • 场景二：使用自定义版本的流程 如果需要对某个流程进行编辑，可以复制初始版本进行处理，启用自定义流程版本的流程操作步骤如下： 1. 复制流程版本 2. 编辑并提交流程版本 3. 审核流程版本 4. 启用流程 • 场景三：使用新增的流程 1. 复制流程 2. 编辑并提交流程版本 3. 审核流程版本 4. 启用流程

序号	操作项	说明
2	启用剧本	剧本是处理一类安全问题的方法描述，是态势感知（专业版）在安全编排系统中的形式化表述。 态势感知（专业版）默认提供了“告警指标提取”、“主机告警状态同步”、“重复告警自动关闭”等剧本，且剧本的初始版本（V1）也已激活，只需要启用就可以进行使用。 同时，如果需要对某个剧本进行编辑，可以复制初始版本进行处理。 启用剧本分为以下场景： • 场景一：使用初始版本的剧本 系统默认激活剧本的初始版本（V1），仅开启剧本启用即可，参考启用剧本。 • 场景二：使用自定义版本的剧本 如果需要使用某个未启用剧本，支持对剧本版本进行修改后再启用，启用自定义剧本版本操作步骤如下： 1. 复制剧本版本 2. 编辑并提交剧本版本 3. 审核剧本版本 4. 启用剧本

13.2 剧本编排管理

13.2.1 启用流程

流程是剧本触发时响应的方式，态势感知（专业版）默认提供了“WAF 一键解封”、“主机告警状态同步”、“告警指标提取”等流程。流程的初始版本（V1）系统默认启用，无需手动启用。同时，还支持对已有流程版本进行自定义编辑，使用自定义流程。

本章节将介绍如何配置并启用自定义版本的流程：

- 复制流程版本
- 编辑并提交流程版本
- 审核流程版本
- 启用流程

此外，用户可通过复制流程实现快速新增流程，复制流程并启用该流程的步骤如下：

- 复制流程
- 编辑并提交流程版本
- 审核流程版本

- 启用流程

前提条件

在启用流程前需要确保**已激活流程版本**，具体操作请参见管理流程版本。

复制流程版本

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 13-2 进入流程版本管理页面

步骤 6 在**流程**版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“复制”，弹出确认框。

步骤 7 在弹出的确认框中，单击“确定”。

----结束

复制流程

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在目标流程“操作”列，单击“复制流程”，弹出“复制流程”配置页面。

步骤 6 在“复制流程”配置页面，配置如下参数：

表 13-2 复制流程配置参数

参数名称	参数含义

参数名称	参数含义
基于版本	选择需要复制的版本，点击"确定"，将生成一条新的流程。 复制流程是需要基于已有流程的某个版本进行复制的。 仅支持下拉选择，不支持输入。
流程名称	自定义新的流程名称。 • 流程名称不能与已有流程名称重复。 • 流程名称不能为空。 • 长度 1~64 字符，由中文字符、大小写英文字母、数字、点、中划线、下划线、空格组成。

步骤 7 配置完成后，单击“确定”。可以在“流程”页签查看新生成的流程信息。复制流程完成后，若需要启用流程，需要编辑并提交流程版本、审核流程版本、启用流程。

----结束

编辑并提交流程版本

支持对“版本状态”为“待提交”或“审核驳回”的流程版本进行编辑。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 13-3 进入流程版本管理页面

步骤 6 在**流程**版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“编辑”，进入流程图绘制界面。

步骤 7 在流程图绘制页面中，从左侧资源库（提供基础节点、流程节点、插件节点）拖拽节点到右边画布，进行设计。

表 13-3 资源库参数详情

参数名称			参数说明
基础	基础节点	开始节点	一个流程的开始。每个流程仅允许一个开始节点，整个流程从开始节点启动执行。
		结束节点	一个流程的结束。每个流程存在多个结束节点，但是流程必须以结束节点收尾，即结束节点不允许出现在其他节点执行之前。
		人工审核	流程执行到该节点会暂停，此时在任务中心页面产生一条待办任务。 用户在我的待办页面处理完成后，继续执行后续节点。 人工审核节点参数说明如表 13-4 所示。
		子流程	另起一个流程，主要用于执行循环操作。相当于流程中的循环体。
	系统插件	排他网关	线路分流时，根据条件表达式选择多条线路中的一条执行。 线路汇聚时，多条线路只要有一条线路到达则继续后面的节点执行。
		并行网关	线路分流时，所有线路都会执行。 线路汇聚时，多条线路全部到达，才会继续后续节点的执行(如果有一条失败，则整个流程都会失败)
		包容网关	线路分流时，根据条件表达式选择符合条件的所有表达式执行。 线路汇聚时，所有分流时被执行的线路都到达包容网关时，才会继续后续节点执行(如果有一条失败，则整个流程都会失败)
流程节点			可以选择当前工作空间中已经发布的所有流程。
插件节点			可以选择当前工作空间中所有插件。

表 13-4 人工审核节点参数说明

参数名称	参数说明
主键 ID	系统自动生成主键 ID，可根据需要进行修改。
名称	自定义人工审核节点名称。
到期时间	人工审核节点到期时间。
到期后任务处理方式	选择到期后，任务的处理方式。

参数名称	参数说明
描述	自定义人工审核节点的描述信息。
查看参数	单击，并在弹出的选择上下文页面中，选择已有的参数名称。如需新增，可单击“新增参数”进行添加。
人工处理参数	输入参数 Key。如需新增，可单击“新增参数”进行添加。

步骤 8 设计完成后，单击右上角“保存并提交”，并在弹出的流程自动校验框中，单击“确定”。

如果流程校验失败，请根据失败提示进行检查。

----结束

审核流程版本

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 13-4 进入流程版本管理页面

步骤 6 在流程版本管理页面中，单击目标流程所在行的“操作”列的“审核”，弹出审核确认框。

步骤 7 在审核确认框中，选择“审核意见”，参数说明如表 13-5 所示。

表 13-5 审核流程参数说明

参数	说明
审核意见	勾选审核结论。 • 通过，通过后流程版本状态更新为已激活。 • 驳回，驳回后流程版本状态更新为审核驳回，可再次编辑后提交。

参数	说明
驳回原因	输入审核意见（当审核意见勾选驳回时必填）。

- 审核驳回后的流程版本可进行编辑，具体操作请参见管理流程版本。
- 流程版本状态变化：

  当前流程仅有一个流程版本时，审核通过后的流程“版本状态”默认为“已激活”。

步骤 8 单击“确定”，完成审核流程版本。

----结束

启用流程

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在目标流程所在行的“操作”列，单击“启用”，页面弹出启用确认框。

步骤 6 在弹出的确认框中，选择启用的流程版本后，单击“确定”，完成流程启用。

----结束

13.2.2 启用剧本

剧本是处理一类安全问题的方法描述，是态势感知（专业版）在安全编排系统中的形式化表述。

态势感知（专业版）默认提供了“告警指标提取”、“主机告警状态同步”、“重复告警自动关闭”等剧本，且剧本的初始版本（V1）也已激活，只需要启用就可以进行使用。

同时，如果需要对某个剧本进行编辑，可以复制初始版本进行处理。

本章节主要介绍配置并启用剧本。

- 场景一：系统默认激活剧本的初始版本（V1），仅开启剧本启用即可，参考启用剧本。
- 场景二：如果需要使用某个未启用剧本，支持对剧本版本进行修改后再启用，启用自定义剧本版本操作步骤如下：
  - 复制剧本版本
  - 编辑并提交剧本版本

- 审核剧本版本
- 启用剧本

前提条件

- **已启用剧本绑定的流程**，具体操作请参见启用流程。
- 在启用剧本前需要确保**已激活剧本版本**，具体操作请参见激活/失活剧本版本。

复制剧本版本

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

步骤 6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“复制”。

步骤 7 在弹出复制版本信息框中，单击“确定”。

----结束

编辑并提交剧本版本

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

步骤 6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“编辑”。

步骤 7 在剧本版本编辑页面，编辑版本信息。

步骤 8 单击“确定”。

步骤 9 在剧本版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“提交”，弹出提交审核确认框。

步骤 10 在确认框中，单击“确定”，提交剧本版本。

- 剧本版本提交后“版本状态”变为待审核。

- 剧本版本提交后不可以再编辑，如果需要编辑可以新建版本，或者在审核中驳回提交。

----结束

审核剧本版本

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

步骤 6 在版本管理页面中，单击“审核”，弹出审核剧本版本页面。

步骤 7 在审核剧本版本页面，填写审核信息，审核剧本版本参数说明如表 13-6 所示。

表 13-6 审核剧本版本参数说明

参数	说明
审核意见	勾选审核结论。 • 通过，通过后剧本版本状态更新为已激活。 • 驳回，驳回后剧本版本状态更新为审核驳回，可再次编辑后提交。
驳回原因	当“审核意见”为“驳回”时，需要填写该参数。 输入审核意见（当审核意见勾选驳回时必填）。

当前剧本仅有一个剧本版本时，审核通过后的剧本“版本状态”默认为“已激活”。

步骤 8 单击“确定”，完成审核剧本版本。

----结束

启用剧本

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 在待启用剧本所在行“操作”列，单击“启用”，弹出启用确认信息框。

步骤 6 选择启用的剧本版本后，单击“确认”。

----结束

13.2.3 管理流程

操作场景

本章节将介绍如何查看流程、导入流程、导出流程、删除流程、禁用流程、复制流程。

查看流程

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在流程管理页面中，查看已有流程的信息。

图 13-5 查看流程信息

- 流程列表上方，呈现当前**待审核**、**未启用**、**已启用**流程的总数。
- 在流程列表中查看已有流程的信息。
  当流程较多时，可以通过搜索功能快速查询指定流程。

表 13-7 流程参数说明

参数名称	参数说明
名称	流程名称。
数据类	流程对应的数据类。
流程状态	流程当前状态。当前分为已启用和未启用两种状态。
流程类型	流程当前的类型。
当前版本	流程当前的版本。
创建人	创建该流程的用户。
创建时间	流程的创建时间。

参数名称	参数说明
修改人	最近一次修改该流程的用户。
更新时间	流程最近一次更新的时间。
描述	流程的描述信息。
操作	用户可以在操作栏中，执行启用、版本管理等操作。

- 如需查看某个流程的详细信息，可单击待查看流程的名称，进入流程详情页面查看流程的详细信息。

----结束

导入流程

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在流程管理列表右上角单击“导入”，弹出导入流程窗口。

步骤 6 单击“添加文件”，并选择待导入文件。

步骤 7 单击“上传”。

----结束

导出流程

支持导出“流程状态”为“已启用”的流程。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在流程管理页面中，勾选需导出的流程，并单击列表右上角的，弹出导出流程确认框。

步骤 6 在弹出的确认框中，单击“确认”，系统将导出流程信息到本地。

----结束

删除流程

删除流程需要**全部满足**下列条件：

- “流程状态”为“未启用”。
- 当前流程中不存在激活的流程版本。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在流程管理页面中，单击目标流程所在行“操作”列的“删除”，弹出删除流程确认框。

步骤 6 在弹出的确认框中，单击“确认”。

删除时，默认删除当前流程中的所有历史版本，删除后不可恢复，请谨慎操作。

----结束

禁用流程

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在目标流程所在行的“操作”列，单击“禁用”，页面弹出禁用确认框。

步骤 6 在弹出的确认框中，单击“确定”，完成流程禁用。

----结束

复制流程

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在目标流程“操作”列，单击“复制流程”，弹出“复制流程”配置页面。

步骤 6 在“复制流程”配置页面，配置如下参数：

表 13-8 复制流程配置参数

参数名称	参数含义
基于版本	选择需要复制的版本，点击"确定"，将生成一条新的流程。 复制流程是需要基于已有流程的某个版本进行复制的。 仅支持下拉选择，不支持输入。
流程名称	自定义新的流程名称。 • 流程名称不能与已有流程名称重复。 • 流程名称不能为空。 • 长度 1~64 字符，由中文字符、大小写英文字母、数字、点、中划线、下划线、空格组成。

步骤 7 配置完成后，单击“确定”。可以在“流程”页签查看新生成的流程信息。复制流程完成后，若需要启用流程，需要编辑并提交流程版本、审核流程版本、启用流程。

----结束

13.2.4 管理流程版本

操作场景

本章节将介绍如何复制流程版本、编辑流程版本、提交流程版本、激活/失活流程版本、删除流程版本。

复制流程版本

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 13-6 进入流程版本管理页面

步骤 6 在流程版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“复制”，弹出确认框。

步骤 7 在弹出的确认框中，单击“确定”，完成复制流程版本。

----结束

编辑流程版本

支持对“版本状态”为“待提交”或“审核驳回”的流程版本进行编辑。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 13-7 进入流程版本管理页面

步骤 6 在流程版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“编辑”，进入流程图绘制界面。

步骤 7 在流程图绘制页面中，从左侧资源库（提供基础节点、流程节点、插件节点）拖拽节点到右边画布，进行设计。

表 13-9 资源库参数详情

参数名称			参数说明
基础	基础节点	开始节点	一个流程的开始。每个流程仅允许一个开始节点，整个流程从开始节点启动执行。

参数名称			参数说明
		结束节点	一个流程的结束。每个流程存在多个结束节点，但是流程必须以结束节点收尾，即结束节点不允许出现在其他节点执行之前。
		人工审核	流程执行到该节点会暂停，此时在任务中心页面产生一条待办任务。 用户在我的待办页面处理完成后，继续执行后续节点。 人工审核节点参数说明如表 13-10 所示。
		子流程	另起一个流程，主要用于执行循环操作。相当于流程中的循环体。
	系统插件	排他网关	线路分流时，根据条件表达式选择多条线路中的一条执行。 线路汇聚时，多条线路只要有一条线路到达则继续后面的节点执行。
		并行网关	线路分流时，所有线路都会执行。 线路汇聚时，多条线路全部到达，才会继续后续节点的执行(如果有一条失败，则整个流程都会失败)
		包容网关	线路分流时，根据条件表达式选择符合条件的所有表达式执行。 线路汇聚时，所有分流时被执行的线路都到达包容网关时，才会继续后续节点执行(如果有一条失败，则整个流程都会失败)
流程节点			可以选择当前工作空间中已经发布的所有流程。
插件节点			可以选择当前工作空间中所有插件。

表 13-10 人工审核节点参数说明

参数名称	参数说明
主键 ID	系统自动生成主键 ID，可根据需要进行修改。
名称	自定义人工审核节点名称。
到期时间	人工审核节点到期时间。
描述	自定义人工审核节点的描述信息。
查看参数	单击，并在弹出的选择上下文页面中，选择已有的参数名称。如需新增，可单击“新增参数”进行添加。

参数名称	参数说明
人工处理参数	输入参数 Key。如需新增，可单击“新增参数”进行添加。

步骤 8 设计完成后，单击右上角“保存并提交”，并在弹出的流程自动校验框中，单击“确定”。

如果流程校验失败，请根据失败提示进行检查。

----结束

提交流程版本

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 13-8 进入流程版本管理页面

步骤 6 在流程版本管理页面中，单击“版本信息”栏中目标流程所在行的“操作”列的“提交”，弹出提交确认框。

图 13-9 提交流程版本

步骤 7 在确认框中，单击“确定”，提交流程版本。

- 流程版本提交后“版本状态”更新为待审核。
- 流程版本提交后不可以再编辑，如果需要编辑可以新建版本，或者在审核中驳回提交。

----结束

激活/失活流程版本

- 只有版本状态为未激活的流程版本才能激活。
- 每个流程只允许存在一个激活版本。
- 激活当前版本后，之前激活的版本将会失活。例如，此次激活 V2 版本，则处于已激活状态的 V1 版本将被取消激活，更新为未激活状态。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 13-10 进入流程版本管理页面

步骤 6 在流程版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“激活”或者“取消激活”。

图 13-11 取消激活示例

步骤 7 在弹出确认框中，单击“确定”，完成激活/失活操作。

----结束

删除流程版本

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 13-12 进入流程版本管理页面

步骤 6 在流程版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“删除”。

步骤 7 在弹出的确认框中，单击“确定”。

流程版本删除后，不可找回，请谨慎操作。

----结束

13.2.5 管理剧本

操作场景

本章节将介绍如何执行查看已有剧本、导入剧本信息、导出剧本信息、禁用剧本、删除剧本等操作。

约束与限制

- 导入剧本时，上传文件格式为.zip，剧本个数不超过 10 个，且文件总量不超过 100M。

查看已有剧本

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 在剧本管理页面，查看剧本的信息。

图 13-13 查看剧本信息

- 剧本列表上方，呈现当前**待审核**、**未启用**、**已启用**剧本的总数。
- 在剧本列表中查看已有剧本的信息。

  当剧本较多时，可以通过搜索功能快速查询指定剧本。

  如需查看某个剧本的详细信息，可单击待查看剧本的名称，进入剧本详情页面。

表 13-11 剧本参数说明

参数名称	参数说明
名称	创建的剧本的名称。
数据类	剧本对应的数据类。
剧本状态	剧本当前状态。当前分为已启用和未启用两种状态。
当前版本	剧本当前版本。
运行监控	单击，查看剧本运行监控。 • 选择时间：选择查看的监控时间。支持最近 24 小时、最近 3 天、最近 30 天和最近 90 天的查询。 • 版本：选择查看的监控版本。支持全部、当前有效和已删除类型的查询。 • 运行次数：提供查看剧本的运行总次数、定时触发次数和事件触发次数。 • 平均运行时长：提供查看平均运行时长、最长运行时长和最短运行时长。其中，平均运行时长=实例运行总时长/实例总个数。 • 实例状态统计：提供查看实例运行总个数、运行成功个数、运行中的实例个数、运行失败个数和终止个数。
创建人	创建该剧本的用户。
创建时间	剧本的创建时间。
修改人	最近一次修改该剧本的用户。
更新时间	剧本最近一次更新的时间。
描述	剧本的描述信息。

----结束

导入剧本信息

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 在剧本管理列表右上角单击“导入”，并在弹出导入剧本窗口中单击“添加文件”，选择待导入文件。

步骤 6 单击“上传”。

----结束

导出剧本信息

态势感知（专业版）支持导出“剧本状态”为“已启用”的剧本。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 勾选需导出的剧本，单击列表右上角的，弹出导出剧本确认信息框。

步骤 6 在弹出的确认框中，单击“确认”，导出剧本信息到本地。

----结束

禁用剧本

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 在目标剧本所在行“操作”列，单击“禁用”，弹出确认信息框。

步骤 6 在弹出确认框中，单击“确定”。

----结束

删除剧本

删除剧本需要**全部满足**以下条件：

- “剧本状态”为“未启用”。
- 当前剧本中不存在激活的剧本版本。
- 不存在正在运行的剧本实例。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 在待删除的剧本“操作”列，单击“删除”，弹出删除剧本确认信息框。

步骤 6 在弹出的确认框中，单击“确认”。

删除剧本默认删除当前剧本中的所有剧本版本，删除操作不可恢复，请谨慎操作。

----结束

13.2.6 管理剧本版本

操作场景

本章节将介绍如何执行预览剧本版本、编辑剧本版本、激活/失活剧本版本、复制剧本版本、删除剧本版本等操作。

预览剧本版本

草稿版本暂不支持预览。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

步骤 6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“预览”，弹出预览版本页面。

步骤 7 在剧本版本预览页面，查看目标剧本版本的详情，包括“基本信息”、“版本信息”、“匹配流程”等。

----结束

编辑剧本版本

仅支持对版本状态为“未提交”的剧本版本进行编辑。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

步骤 6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“编辑”，弹出编辑版本页面。

步骤 7 在剧本版本编辑页面，编辑版本信息。

步骤 8 单击“确定”，完成剧本的编辑。

----结束

激活/失活剧本版本

- 只有版本状态为未激活的剧本版本才能激活。
- 每个剧本只允许存在一个激活版本。
- 激活当前版本后，之前激活的版本将会失活。例如，此次激活 V2 版本，则处于已激活状态的 V1 版本将被取消激活，更新为未激活状态。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

步骤 6 在版本管理页面中，单击“版本信息”栏中目标剧本版本所在行“操作”列的“激活”（或“取消激活”），完成激活（或失活）操作。

----结束

复制剧本版本

仅支持复制“已激活”、“未激活”的剧本版本。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

步骤 6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“复制”，弹出复制版本页面。

步骤 7 在弹出复制版本信息框中，单击“确定”，完成复制剧本版本。

----结束

删除剧本版本

删除剧本版本需要**全部满足**以下条件：

- 剧本版本处于失活状态。
- 不存在正在运行的剧本版本实例。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

步骤 6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“删除”，完成删除剧本版本。

剧本版本删除后，不可找回，请谨慎操作。

----结束

13.2.7 管理操作连接

操作场景

- **含义**：操作连接是安全编排流程中，每个插件节点需要使用到的连接域名和鉴权参数。
- **作用**：用于在安全编排的流程执行过程中，每个插件节点运行时，传入需要连接的域名信息，以及在访问该域名时，需要使用到的用户鉴权信息，如用户名/密码、账号 AK/SK 等。
- **操作连接与插件的关系**：每个插件在运行过程中，需要通过域名调用的方式访问其他云服务或者三方服务，调用过程中需要鉴权，因此，在插件的登录凭证参数中会定义需要的域名参数（Endpoint）和认证参数（用户名/密码、账号 AK/SK 等）。操作连接则是配置插件登录凭证的参数值，流程中每个插件节点绑定不同的操作连接，支持相同插件的不同节点访问不同的服务。

本章节主要介绍如何管理操作连接，包括：新增操作连接、查看操作连接、编辑操作连接、删除操作连接。

新增操作连接

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“操作连接”页签，进入连接管理页面。

步骤 5 在操作连接管理页面中，单击“新增”，右侧弹出新增操作连接面板。

步骤 6 在新增操作连接面板中，配置连接参数，参数说明如表 13-12 所示。

表 13-12 操作连接参数说明

参数名称	说明
连接名称	输入操作连接名称。名称规则如下： • 可输入英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（_）。 • 长度不能超过 64 个字符。
插件	选择操作连接所需的插件。插件详细信息请参见查看插件详情。
描述	可选参数，输入资产描述，描述信息长度不能超过 64 个字符。

步骤 7 单击“确认”，返回列表，即可查询已经创建的操作连接信息。

----结束

查看操作连接

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“操作连接”页签，进入连接管理页面。

步骤 5 在操作连接管理页面，查看操作连接信息。

- 在操作连接列表中，可以查看连接的名称、插件、创建人等信息。

- 当操作连接较多时，可以通过搜索功能快速查询指定操作连接。
- 如需查看某个操作连接的详细信息，可单击待查看操作连接的名称，进入操作连接详情页面进行查看。

----结束

编辑操作连接

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“操作连接”页签，进入连接管理页面。

步骤 5 在目标操作连接所在行“操作”列，单击“编辑”，弹出编辑操作连接页面。

步骤 6 在操作连接编辑页面中，编辑操作连接参数，参数说明如表 13-13 所示。

表 13-13 操作连接参数说明

参数名称	说明
连接名称	输入操作连接名称。名称规则如下： • 可输入英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（_）。 • 长度不能超过 64 个字符。
插件	选择操作连接所需的插件。插件相关介绍请参见查看插件详情。
创建人	操作连接的创建人，该参数**不支持修改**。
创建时间	操作连接的创建时间，该参数**不支持修改**。
修改人	操作连接的最近一次修改的用户，该参数**不支持修改**。
描述	可选参数，输入操作连接描述，描述信息长度不能超过 64 个字符。

步骤 7 单击“确认”，完成操作连接的编辑。

----结束

删除操作连接

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“操作连接”页签，进入连接管理页面。

步骤 5 在目标连接所在行“操作”列，单击“删除”，弹出删除确认框。

步骤 6 在弹出的确认框中，单击“确认”，完成操作连接删除。

操作连接删除后，不可找回，请谨慎操作。

----结束

13.2.8 查看实例监控

操作场景

当剧本/流程执行完成后，实例管理列表中会生成剧本/流程实例，即实例监控。实例监控列表每条记录是一个实例，可呈现实例的历史实例任务列表，以及历史实例任务的运行情况。

本章节主要介绍如何查看实例监控信息。

查看实例监控

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“实例管理”页签，进入实例管理页面。

步骤 5 在实例管理页面中，可查看实例信息，参数说明如表 13-14 所示。

- 在实例列表中下方可以查看实例总条数。其中，使用翻页查看时最多可查看 10000 条实例信息，如果需要查看超过 10000 条以外数据，请优化过滤条件筛选数据。
- 实例的保存时长最长为 180 天。
- 如需查看某个实例的详细信息，可以单击任一实例名称，进入实例图页面，可查看实例流程图、流程节点、运行开始时间、结束时间等信息。

表 13-14 实例列表参数

参数名称	参数说明

参数名称	参数说明
实例名称	系统生成的实例的名称。
剧本名称	实例对应的剧本名称。
数据类	剧本的运营对象，即数据类。
触发方式	实例的触发方式。 • 定时触发 • 事件触发
状态	实例的状态。 • 成功：剧本实例成功执行。 • 失败：剧本实例执行失败，单击操作列的重试可重新执行剧本。 • 运行中：剧本实例处于运行状态，单击操作列的终止可终止剧本。 • 重试中：剧本实例正在重试中。 • 终止中：剧本实例正在终止。 • 已终止：剧本实例已经成功终止。
上下文	实例的上下文信息。
实例创建时间	实例创建的具体时间。
实例结束时间	实例结束的具体时间。
操作	用户可执行终止、重试操作。

----结束

相关操作

- 如果实例正在运行中，可以单击目标实例所在行操作列的“终止”，终止实例的运行。实例终止完成后，将不支持任何操作。
- 如果实例运行失败，可以单击目标实例所在行操作列的“重试”，实例将重新进行运行。

  单账号单 workspace 内一天内，手动重试流程实例的最大重试次数 100 次。重试之后，等剧本执行完毕之后才允许再次重试。

13.3 运营对象管理

13.3.1 运营对象管理概述

- **数据类**：安全编排与响应中的剧本和流程的运行都需要绑定数据类，由数据对象（数据类的实例）触发剧本。常见的数据类包括告警、事件、威胁情报、漏洞等。查看数据类请参考查看数据类。
- **告警**：告警是运维中的一种异常信号的通知，通常是由监控系统或安全设备在检测到系统或网络中的异常情况时自动生成的。例如，当服务器的 CPU 使用率超过90%时，系统可能会发出告警。这些异常情况可能包括系统故障、安全威胁或性能瓶颈等。告警通常有明确的指示性，能够明确指出异常发生的位置、类型和影响。同时，告警可以按照严重程度来进行分类，如紧急、重要、一般等，以便运维人员根据告警的严重程度来决定哪些需要优先处理。告警的目的是及时通知相关人员，以便能够迅速响应并采取措施解决问题。常见的告警类型有网页防篡改、进程异常行为、异常网络连接等。管理告警类型请参考管理告警类型。
- **事件**：事件是一个广泛的概念，可以包括告警，但不限于此，它可以是系统正常操作的一部分，也可以是异常或错误。在运维和安全领域，事件通常指的是已经发生并需要被关注、调查和处理的问题或故障。事件可能由一条或多条告警触发，也可能由其他因素（如用户操作、系统日志等）引发。事件的目的是为了记录、分析、报告或审计，通常用于记录和报告系统的历史行为，以便于分析和审计。管理事件类型请参考管理事件类型。
- **威胁情报**：管理威胁情报请参考管理威胁情报。
- **漏洞**：常见的漏洞类型有 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞等。管理漏洞类型请参考管理漏洞类型。
- **自定义类型**：针对已有的数据类，可新增自定义类型，详细操作请参考查看自定义类型。
- 管理**分类&映射**：分类&映射指的是数据源与数据对象（数据类的实例）的映射关系。管理分类&映射请参考管理分类&映射。

13.3.2 查看数据类

安全编排与响应中的剧本和流程的运行都需要绑定数据类，由数据对象（数据类的实例）触发剧本。数据类支持如下操作：

- 查看数据类

查看数据类

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，默认进入运营对象的数据类管理页面。

步骤 5 在数据类列表中，查看已有数据类信息。

- 当数据类较多时，可以通过搜索功能，可快速查询指定数据类。
- 在数据类列表中，可以查看数据类的名称、业务编码、是否为内置数据类等信息。
- 如需查看某个数据类的详细信息，可单击目标数据类的名称，右侧将弹出目标数据类的详情页面。

  在数据类详情页面中，可以查看数据类的基本信息和字段信息。

----结束

13.3.3 管理告警类型

操作场景

本章节介绍如何管理告警类型，详细操作如下：

- 查看已有告警类型：**查看**已有的告警类型及其详细信息。
- 新增告警类型：介绍如何自定义**新增**告警类型。
- 告警类型关联布局：介绍如何将自定义新增的告警类型**关联已有布局**。
- 编辑已有告警类型：介绍如何**编辑**自定义新增的告警类型。
- 管理已有告警类型：介绍如何**启用**、**禁用**、**删除**自定义新增的告警类型。

约束与限制

- 系统内置告警类型已默认关联已有布局，暂**不支持**自定义关联布局。
- 系统内置告警类型默认处于启用状态，且暂**不支持**进行编辑、禁用、删除操作。
- 自定义告警类型新增成功后，**不支持**修改“类型名称”、“类型标识”、“子类型标识”参数信息。

查看已有告警类型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“告警类型”页签，进入告警类型管理页面。

步骤 6 在告警类型管理页面中，左侧“类型名称”中，可查看所有的告警类型。

如需查看某个告警类型中子类型的详细信息，可在左侧“类型名称”中单击目标类型名称，右侧将展示所有子类型详细信息，参数说明如表 13-15 所示。

如果子类型较多，可通过选择“子类型”、“关联布局”，并输入对应关键字进行搜索。

表 13-15 查看告警类型参数说明

参数名称	参数说明
子类型/子类型标识	告警子类型的名称和标识。
关联布局	告警类型已关联的布局。
启用状态	告警类型的启用状态。 • 启用：当前类型已启用。 • 禁用：当前类型已被禁用。
SLA	告警类型的 SLA 处理时间。
描述	告警类型的描述信息。
操作	可以对告警类型进行编辑、删除等操作。

----结束

新增告警类型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“告警类型”页签，进入告警类型管理页面。

步骤 6 在告警类型管理页面中单击“新增”，右侧弹出新增告警类型页面。在新增告警类型页面中，配置告警类型参数。

表 13-16 新增告警类型参数说明

参数名称	参数说明
类型名称	自定义新增告警类型的名称。
类型标识	填写告警类型标识。标识关键字需遵循大驼峰命名规范，例如 TypeTag。
子类型	填写告警类型的子类型。
子类型标识	填写告警子类型标识。标识关键字需遵循大驼峰命名规范，例如 SubTypeName。
启动状态	设置告警类型的启动状态。

参数名称	参数说明
SLA	设置告警的 SLA 处理时间。
描述	自定义告警类型描述信息。

自定义告警类型新增成功后，**不支持**修改“类型名称”、“类型标识”、“子类型标识”参数信息。

步骤 7 在页面右下角单击“确认”，完成新增操作。

新增完成后，可以在告警类型页面的“类型名称”中查看已新增的告警类型。

----结束

告警类型关联布局

系统内置告警类型已默认关联已有布局，暂不支持自定义关联布局。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“告警类型”页签，进入告警类型管理页面。

步骤 6 在告警类型管理页面中，选择需要关联布局的类型，并单击目标类型所在行“操作”列的“关联布局”，页面弹出绑定布局编辑框。

步骤 7 在绑定布局编辑框中，选择需要关联的布局，并单击“确认”。

----结束

编辑已有告警类型

- 暂不支持编辑系统内置告警类型。
- 自定义告警类型新增成功后，不支持修改“类型名称”、“类型标识”、“子类型标识”参数信息。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“告警类型”页签，进入告警类型管理页面。

步骤 6 在告警类型管理页面的“类型名称”中，单击需要编辑的自定义告警类型名称，右侧将展示自定义告警类型的详细信息。

步骤 7 在右侧告警列表页面中，单击目标类型所在行“操作”列的“编辑”，右侧弹出编辑页面。

步骤 8 在编辑告警类型页面中，修改告警类型的参数信息。

表 13-17 编辑告警类型参数说明

参数名称	参数说明
类型名称	告警类型的名称，**不支持修改**。
类型标识	告警类型标识，**不支持修改**。
子类型	填写告警类型的子类型。
子类型标识	告警子类型标识，**不支持修改**。
启动状态	设置告警类型的启动状态。
SLA	设置告警的 SLA 处理时间。
描述	自定义告警类型描述信息。

步骤 9 在页面右下角单击“确认”。

----结束

管理已有告警类型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“告警类型”页签，进入告警类型管理页面。

步骤 6 在告警类型管理页面中，对告警类型进行管理。

- 系统内置告警类型默认处于启用状态，无需手动启用。

- 暂不支持禁用或删除系统内置告警类型。
- 暂不支持删除系统内置告警类型。

表 13-18 管理已有告警类型

操作	操作说明
启用	1. 在告警类型管理页面中，选择需要启用的告警类型，并单击类型列表左上角“批量启用”。 也可以直接单击需要启用的告警类型所在行“启用状态”所在列的禁用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“启用”时，则表示启用成功。
禁用	1. 在告警类型管理页面中，选择需要禁用的告警类型，并单击类型列表左上角“批量禁用”。 也可以直接单击需要禁用的告警类型所在行“启用状态”所在列的启用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“禁用”时，则表示禁用成功。
删除	1. 在告警类型管理页面中，选择需要删除的告警类型，并单击目标类型所在行“操作”列的“删除”，右侧弹出删除确认界面。 2. 在弹出的确认框中，单击“确认”。

----结束

13.3.4 管理事件类型

操作场景

本章节介绍如何管理事件类型，详细操作如下：

- 查看已有事件类型：**查看**已有的事件类型及其详细信息。
- 新增事件类型：介绍如何自定义**新增**事件类型。
- 事件类型关联布局：介绍如何将自定义新增的事件类型**关联已有布局**。
- 编辑已有事件类型：介绍如何**编辑**自定义新增的事件类型。
- 管理已有事件类型：介绍如何**启用**、**禁用**、**删除**自定义新增的事件类型。

约束与限制

- 系统内置事件类型已默认关联已有布局，暂**不支持**自定义关联布局。

- 系统内置事件类型默认处于启用状态，暂**不支持**进行编辑、启用、禁用、删除操作。
- 自定义事件类型新增成功后，**不支持**修改“类型名称”、“类型标识”、“子类型标识”参数信息。

查看已有事件类型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“事件类型”页签，进入事件类型管理页面。

步骤 6 在事件类型管理页面中，查看已有事件类型的详细信息，参数说明如表 13-19 所示。

表 13-19 事件类型参数说明

参数名称	参数说明
类型名称	事件类型的名称。
子类型/子类型标识	事件子类型的名称和标识。
关联布局	事件类型已关联的布局。
启用状态	事件类型的启用状态。 • 启用：当前类型已启用。 • 禁用：当前类型已被禁用。
SLA	事件类型的 SLA 处理时间。
描述	事件类型的描述信息。
操作	可以对事件类型进行编辑、删除等操作。

----结束

新增事件类型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“事件类型”页签，进入事件类型管理页面。

步骤 6 在事件类型管理页面中单击“新增”，右侧弹出新增事件类型页面。在新增事件类型页面中，配置事件类型参数。

表 13-20 事件类型参数说明

参数名称	参数说明
类型名称	自定义新增事件类型的名称。
类型标识	填写事件类型标识。标识关键字需遵循大驼峰命名规范，例如 TypeTag。
子类型	填写事件类型的子类型。
子类型标识	填写事件子类型标识。标识关键字需遵循大驼峰命名规范，例如 SubTypeName。
启动状态	设置事件类型的启动状态。
SLA	设置事件的 SLA 处理时间。
描述	自定义事件类型描述信息。

自定义事件类型新增成功后，**不支持**修改“类型名称”、“类型标识”、“子类型标识”参数信息。

步骤 7 在页面右下角单击“确认”，完成新增操作。

新增完成后，可以在事件类型页面的“类型名称”中查看已新增的类型。

----结束

事件类型关联布局

系统内置事件类型已默认关联已有布局，暂不支持自定义关联布局。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“事件类型”页签，进入事件类型管理页面。

步骤 6 在事件类型管理页面中，选择需要关联布局的类型，并单击目标类型所在行“操作”列的“关联布局”，页面弹出绑定布局编辑框。

步骤 7 在绑定布局编辑框中，选择需要关联的布局，并单击“确认”。

----结束

编辑已有事件类型

- 暂不支持编辑系统内置事件类型。
- 自定义事件类型新增成功后，不支持修改“类型名称”、“类型标识”、“子类型标识”参数信息。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“事件类型”页签，进入事件类型管理页面。

步骤 6 在事件类型管理页面的“类型名称”中，单击需要编辑的自定义事件类型名称，右侧将展示自定义事件类型的详细信息。

步骤 7 在右侧事件类型页面，单击目标类型所在行“操作”列的“编辑”，右侧弹出编辑页面。

步骤 8 在编辑事件类型页面中，编辑参数信息。

表 13-21 事件类型参数说明

参数名称	参数说明
类型名称	事件类型的名称，**不支持修改**。
类型标识	事件类型标识，**不支持修改**。
子类型	填写事件类型的子类型。
子类型标识	事件子类型标识，**不支持修改**。
启动状态	设置事件类型的启动状态。
SLA	设置事件的 SLA 处理时间。

参数名称	参数说明
描述	自定义事件类型描述信息。

步骤 9 在页面右下角单击“确认”。

----结束

管理已有事件类型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“事件类型”页签，进入事件类型管理页面。

步骤 6 在事件类型管理页面中，对事件类型进行管理。

- 系统内置事件类型默认处于启用状态，无需手动启用。
- 暂不支持禁用或删除系统内置事件类型。

表 13-22 管理已有事件类型

操作	操作说明
启用	1. 在事件类型管理页面中，选择需要启用的类型，并单击类型列表左上角“批量启用”。 也可以直接单击需要启用的事件类型所在行“启用状态”所在列的禁用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“启用”时，则表示启用成功。
禁用	1. 在事件类型管理页面中，选择需要禁用的类型，并单击类型列表左上角“批量禁用”。 也可以直接单击需要禁用的事件类型所在行“启用状态”所在列的启用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“禁用”时，则表示禁用成功。

操作	操作说明
删除	1. 在事件类型管理页面中，选择需要删除的类型，并单击目标类型所在行“操作”列的“删除”，右侧弹出删除确认界面。 2. 在弹出的确认框中，单击“确认”。

----结束

13.3.5 管理威胁情报

操作场景

本章节介绍如何管理威胁情报类型。

- 查看已有威胁情报类型：**查看**已有的威胁情报类型及其详细信息。
- 新增威胁情报类型：介绍如何自定义**新增**威胁情报类型。
- 威胁情报类型关联布局：介绍如何将自定义新增的威胁情报类型**关联已有布局**。
- 编辑已有威胁情报类型：介绍如何**编辑**自定义新增的威胁情报类型。
- 管理已有威胁情报类型：介绍如何**启用**、**禁用**、**删除**自定义新增的威胁情报类型。

约束与限制

- 系统内置威胁情报类型已默认关联已有布局，暂**不支持**自定义关联布局。
- 系统内置威胁情报类型默认处于启用状态，暂**不支持**进行编辑、启用、禁用、删除操作。
- 自定义威胁情报类型新增成功后，**不支持**修改类型标识。

查看已有威胁情报类型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“威胁情报”页签，进入威胁情报类型管理页面。

步骤 6 在威胁情报类型管理页面中，查看已有威胁情报的详细信息，参数说明如表 13-23 所示。

表 13-23 威胁情报参数说明

参数名称	参数说明
类型名称/类型标识	威胁情报的名称和标识。
关联布局	威胁情报已关联的布局。
启用状态	威胁情报的启用状态。 • 启用：当前类型已启用。 • 禁用：当前类型已被禁用。
失效时间	威胁情报的失效时间。
内置	是否为系统内置的威胁情报。
描述	威胁情报的描述信息。
操作	可以对威胁情报进行编辑、删除等操作。

----结束

新增威胁情报类型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“威胁情报”页签，进入威胁情报类型管理页面。

步骤 6 在威胁情报类型管理页面中单击“新增”，右侧弹出新增类型页面。在新增类型页面中，配置类型参数。

表 13-24 威胁情报参数说明

参数名称	参数说明
类型名称	自定义新增威胁情报的名称。
类型标识	填写威胁情报标识。标识关键字需遵循大驼峰命名规范，例如 TypeTag。
启动状态	设置威胁情报的启动状态。

参数名称	参数说明
失效时间	设置威胁情报的失效时间。 • 永不失效：表示当前情报类型永不失效。 • 时间间隔：设置情报失效的间隔时间。
描述	自定义威胁情报的描述信息。

自定义威胁情报类型新增成功后，**不支持**修改类型标识。

步骤 7 在页面右下角单击“确认”，完成新增操作。

新增完成后，可以在威胁情报类型页面的表格中查看已新增的类型。

----结束

威胁情报类型关联布局

系统内置威胁情报类型已默认关联已有布局，暂不支持自定义关联布局。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“威胁情报”页签，进入威胁情报类型管理页面。

步骤 6 在威胁情报类型管理页面中，选择需要关联布局的类型，并单击目标类型所在行“操作”列的“关联布局”，页面弹出绑定布局编辑框。

步骤 7 在绑定布局编辑框中，选择需要关联的布局，并单击“确认”。

----结束

编辑已有威胁情报类型

- 暂不支持编辑系统内置威胁情报类型。
- 自定义威胁情报类型新增成功后，不支持修改类型标识。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“威胁情报”页签，进入威胁情报类型管理页面。

步骤 6 在威胁情报类型管理页面中，选择需要编辑的类型，并单击目标类型所在行“操作”列的“编辑”，右侧弹出编辑页面。

步骤 7 在编辑页面中，编辑对应类型的参数信息。

表 13-25 威胁情报参数说明

参数名称	参数说明
类型名称	自定义威胁情报的名称。
类型标识	威胁情报标识，**不支持修改**。
启动状态	设置威胁情报的启动状态。
失效时间	设置威胁情报的失效时间。 • 永不失效：表示当前情报类型永不失效。 • 时间间隔：设置情报失效的间隔时间。
描述	自定义威胁情报的描述信息。

步骤 8 在页面右下角单击“确认”。

----结束

管理已有威胁情报类型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“威胁情报”页签，进入威胁情报类型管理页面。

步骤 6 在威胁情报类型管理页面中，对威胁情报类型进行管理。

- 系统内置威胁情报类型默认处于启用状态，无需手动启用。
- 暂不支持禁用或删除系统内置威胁情报类型。

表 13-26 管理已有威胁情报类型

操作	操作说明
启用	1. 在威胁情报类型管理页面中，选择需要启用的类型，并单击类型列表左上角“批量启用”。 也可以直接单击需要启用的情报类型所在行“启用状态”所在列的禁用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“启用”时，则表示启用成功。
禁用	1. 在威胁情报类型管理页面中，选择需要禁用的类型，并单击类型列表左上角“批量禁用”。 也可以直接单击需要禁用的情报类型所在行“启用状态”所在列的启用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“禁用”时，则表示禁用成功。
删除	1. 在威胁情报类型管理页面中，选择需要删除的类型，并单击目标类型所在行“操作”列的“删除”，右侧弹出删除确认界面。 2. 在弹出的确认框中，单击“确认”。

----结束

13.3.6 管理漏洞类型

操作场景

本章节介绍如何管理漏洞类型，详细操作如下：

- 查看已有漏洞类型：**查看**已有的漏洞类型及其详细信息。
- 新增漏洞类型：介绍如何自定义**新增**漏洞类型。
- 漏洞类型关联布局：介绍如何将自定义新增的漏洞类型**关联已有布局**。
- 编辑已有漏洞类型：介绍如何**编辑**自定义新增的漏洞类型。
- 管理已有漏洞类型：介绍如何**启用**、**禁用**、**删除**自定义新增的漏洞类型。

约束与限制

- 系统内置漏洞类型暂**不支持**自定义关联布局。
- 系统内置漏洞类型默认处于启用状态，暂**不支持**进行编辑、启用、禁用、删除操作。
- 自定义漏洞类型新增成功后，**不支持**修改类型标识。

查看已有漏洞类型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“漏洞类型”页签，进入漏洞类型管理页面。

步骤 6 在漏洞类型管理页面中，查看已有漏洞类型的详细信息，参数说明如表 13-27 所示。

表 13-27 漏洞类型参数说明

参数名称	参数说明
类型名称/类型标识	漏洞类型的名称和标识。
关联布局	漏洞类型已关联的布局。
启用状态	漏洞类型的启用状态。 • 启用：当前类型已启用。 • 禁用：当前类型已被禁用。
内置	是否为系统内置的漏洞类型。
描述	漏洞类型的描述信息。
操作	可以对漏洞类型进行编辑、删除等操作。

----结束

新增漏洞类型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“漏洞类型”页签，进入漏洞类型管理页面。

步骤 6 在漏洞类型管理页面中单击“新增”，右侧弹出新增类型页面。在新增类型页面中，配置类型参数。

表 13-28 漏洞类型参数说明

参数名称	参数说明
类型名称	自定义新增漏洞类型的名称。
类型标识	填写漏洞类型标识。标识关键字需遵循大驼峰命名规范，例如 TypeTag。
启动状态	设置漏洞类型的启动状态。
描述	自定义漏洞的描述信息。

自定义漏洞类型新增成功后，**不支持**修改“类型标识”。

步骤 7 在页面右下角单击“确认”，完成新增操作。

新增完成后，可以在漏洞类型页面的表格中查看已新增的类型。

----结束

漏洞类型关联布局

系统内置漏洞类型暂不支持自定义关联布局。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“漏洞类型”页签，进入漏洞类型管理页面。

步骤 6 在漏洞类型管理页面中，选择需要关联布局的类型，并单击目标类型所在行“操作”列的“关联布局”，页面弹出绑定布局编辑框。

步骤 7 在绑定布局编辑框中，选择需要关联的布局，并单击“确认”。

----结束

编辑已有漏洞类型

- 暂不支持编辑系统内置漏洞类型。

- 自定义漏洞类型新增成功后，不支持修改类型标识。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“漏洞类型”页签，进入漏洞类型管理页面。

步骤 6 在漏洞类型管理页面中，选择需要编辑的类型，并单击目标类型所在行“操作”列的“编辑”，右侧弹出编辑页面。

步骤 7 在编辑页面中，编辑对应类型的参数信息。

表 13-29 漏洞类型参数说明

参数名称	参数说明
类型名称	自定义漏洞类型的名称。
类型标识	漏洞类型标识，**不支持修改**。
启动状态	设置漏洞类型的启动状态。
描述	自定义漏洞的描述信息。

步骤 8 在页面右下角单击“确认”。

----结束

管理已有漏洞类型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“漏洞类型”页签，进入漏洞类型管理页面。

步骤 6 在漏洞类型管理页面中，对漏洞类型进行管理。

- 系统内置漏洞类型默认处于启用状态，无需手动启用。

- 暂不支持禁用或删除系统内置漏洞类型。

表 13-30 管理已有漏洞类型

操作	操作说明
启用	1. 在漏洞类型管理页面中，选择需要启用的类型，并单击类型列表左上角“批量启用”。 也可以直接单击需要启用的漏洞类型所在行“启用状态”所在列的禁用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“启用”时，则表示启用成功。
禁用	1. 在漏洞类型管理页面中，选择需要禁用的类型，并单击类型列表左上角“批量禁用”。 也可以直接单击需要禁用的漏洞类型所在行“启用状态”所在列的启用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“禁用”时，则表示禁用成功。
删除	1. 在漏洞类型管理页面中，选择需要删除的类型，并单击目标类型所在行“操作”列的“删除”，右侧弹出删除确认界面。 2. 在弹出的确认框中，单击“确认”。

----结束

13.3.7 查看自定义类型

操作场景

本章节介绍如何查看自定义类型。

约束与限制

- 系统内置的类型和子类型**不支持**关联布局、编辑、删除、启用和禁用。
- 自定义类型新增成功后，**不支持**修改“数据类”、“类型名称”、“类型标识”。
- 子类型新增成功后，**不支持**修改“数据类”、“类型名称”、“类型标识”、“子类型标识”。

查看已有的自定义类型/子类型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

步骤 5 在类型管理页面，选择“自定义类型”页签，进入自定义类型管理页面后，查看已有自定义类型/子类型的详细信息。

- 左侧显示类型列表，展示已有的类型。
- 如需查看某个类型的详细信息，请单击左侧类型列表中类型的名称，右侧将展示类型的详细信息。具体信息如下：
  - 目标类型的基本信息：名称、创建人、创建时间、关联布局。
  - 子类型列表：已有子类型、子类型名称、子类型关联的布局等信息。

----结束

13.3.8 管理分类&映射

分类和映射是对云服务告警进行类型匹配和字段映射。

本章节介绍如何查看已有分类映射、创建分类映射、复制已有的分类映射、编辑分类映射、启用、禁用或删除分类映射。

查看已有分类映射

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“分类&映射”页签，进入分类映射管理页面。

步骤 5 在分类映射管理页面中，查看已创建分类映射的详细信息。

- 在分类映射列表中，查看分类映射的名称、数据类、关联插件实例数等信息。
- 如果分类映射较多时，可以通过搜索功能，输入关键字进行搜索，即可快速查询指定分类映射。
- 如果需要对分类映射进行编辑，可以单击目标分类映射的名称，进入编辑页面进行编辑。

  在编辑页面，可以编辑分类映射的信息。
- 在分类映射列表中，还可以启用、禁用或复制、删除已有分类映射。

----结束

创建分类映射

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“分类&映射”页签，进入分类映射管理页面。

步骤 5 在分类映射管理页面中，单击“创建”，进入创建分类映射页面。

步骤 6 在创建分类映射页面中，配置分类映射参数信息。

图 13-14 创建分类映射

1. 在左侧“基本信息配置”栏中，配置分类映射的基本信息，参数说明如表 13-31 所示。

表 13-31 配置基本信息

参数名称	参数说明
名称	自定义分类映射名称。
数据类	选择对应的数据类。
描述	自定义分类映射描述信息。

2. 选择左侧“数据源”栏中，选择分类映射的数据源。

   当“数据源”选择“上传 JSON 文件”时，需要单击“上传 JSON 文件”，并上传 JSON 文件。

3. 在右侧“分类”页签中，选择分类方式，并配置对应参数。
4. 完成分类配置后，单击页面右上角，保存配置。
5. 在右侧“映射”页签中，选择映射方式，并配置对应参数。
6. 完成分类映射后，单击页面右上角，保存配置。
7. 在右侧“预处理”页签中，设置预处理映射参数。
8. 完成预处理配置后，单击页面右上角，保存配置。

----结束

复制已有的分类映射

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“分类&映射”页签，进入分类映射管理页面。

步骤 5 在分类映射管理页面中，单击目标分类映射所在行“操作”列的“复制”。

步骤 6 在弹出的确认框中，编辑复制项名称，并单击“确认”。

----结束

编辑分类映射

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“分类&映射”页签，进入分类映射管理页面。

步骤 5 在分类映射管理页面中，单击目标分类映射名称，进入编辑页面。

步骤 6 在编辑分类映射页面，编辑分类映射参数信息。

1. 在左侧“基本信息配置”栏中，配置分类映射的基本信息，参数说明如表 13-32 所示。

表 13-32 配置基本信息

参数名称	参数说明
名称	自定义分类映射名称。
数据类	选择对应的数据类，暂不支持编辑
描述	自定义分类映射描述信息。

2. 选择左侧“数据源”栏中，选择分类映射的数据源。

   当“数据源”选择“上传 JSON 文件”时，需要单击“上传 JSON 文件”，并上传 JSON 文件。

3. 在右侧“分类”页签中，选择分类方式，并配置对应参数。

4. 完成分类配置后，单击页面右上角，保存配置。
5. 在右侧“映射”页签中，选择映射方式，并配置对应参数。
6. 完成分类映射后，单击页面右上角，保存配置。
7. 在右侧“预处理”页签中，设置预处理映射参数。
8. 完成预处理配置后，单击页面右上角，保存配置。

----结束

启用、禁用或删除分类映射

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“分类&映射”页签，进入分类映射管理页面。

步骤 5 在分类映射管理页面中，对分类映射进行管理。

- 自定义新增的分类映射暂不支持启用、禁用操作。
- 暂不支持删除系统内置分类映射。

表 13-33 管理分类映射

操作	操作说明
启用	在分类映射管理页面中，单击目标分类映射所在行“启用状态”列的禁用按钮。 当“启用状态”更新为“启用”时，表示启用成功。
禁用	在分类映射管理页面中，单击目标分类映射所在行“启用状态”列的启用按钮。 当“启用状态”更新为“禁用”时，表示禁用成功。
删除	1. 在分类映射管理页面中，单击目标分类映射所在行“操作”列的“删除”。 2. 在弹出的删除映射确认框中，确认无误后，单击“删除”。 **说明** ● 删除分类映射时，与待删除分类映射关联的插件、连接等都将立即停止。 ● 分类映射删除后，无法恢复，请谨慎操作。

----结束

13.4 自定义页面布局

13.4.1 查看布局

操作场景

布局中已有多个页面布局，例如告警列表、情报详情、漏洞详情等。

本章节主要介绍如何查看布局。

查看已有布局

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 页面布局”，默认进入页面布局管理页面。

步骤 5 在布局管理页面，查看已有布局。

将鼠标悬停在目标布局上，并单击布局右上角，可以进入布局配置详情页面进行查看。

----结束

13.4.2 查看布局模板

操作场景

布局中已有多个页面布局的管理页和详情页面模板，例如告警管理、事件管理、漏洞管理等。

本章节主要介绍如何查看布局模板。

查看布局模板

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 页面布局”，进入布局管理页面后，选择“模板”页签，进入布局模板页面。

步骤 5 在布局模板页面，查看模板信息。

可以通过“布局类型”、“页面类型”，并输入关键字来搜索指定布局模板。

- 可以查看当前已有模板的名称、页面类型、创建时间等信息。
- 可以对已有模板的名称、模板内的布局进行编辑。

----结束

13.5 查看插件详情

操作场景

本章节介绍如何查看态势感知（专业版）内置插件及详细信息。

查看插件详情

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 插件管理”，进入插件管理页面。

步骤 5 在插件管理页面中，查看插件详细信息。

- 左侧显示内置所有插件集、插件、函数信息。
- 如需查看某个插件的详细信息，可以单击插件名称，右侧将展示插件的详细信息。
- 如果查看某个函数的详细信息，可以展开插件后，单击需要查看的函数名称，右侧将展示函数的详细信息。

----结束

13.6 目录定制

操作场景

态势感知（专业版）支持自定义目录，您可以根据需要对目录进行定制。本章节将介绍以下操作：

- 查看已有目录
- 更换布局

约束与限制

- 系统内置的目录**不支持**编辑、删除操作。

查看已有目录

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 目录定制”，进入目录定制页面。

步骤 5 在目录定制列表中，查看目录的详细信息。

表 13-34 目录参数说明

参数名称	参数说明
面包屑导航显示开关	按钮默认开启。该开关用于控制是否允许用户返回外层导航目录。 • 开关打开：用户可返回外层空间管理导航目录。 • 开关关闭：用户无法返回外层空间管理导航目录。
工作空间导航设置	• 新增：用户自定义新增目录。 • 批量编辑：支持批量编辑，设置“落地页”，设置“是否显示”按钮。落地页即单击工作空间名称后进入空间详情的默认页面。 • 批量删除：支持批量删除目录，仅用户自定义的目录支持删除，系统内置目录不支持删除。
导航名称	导航目录所属的一级目录名称。单击一级目录名称前方的按钮可展开该一级目录下的二级目录名称。
目录状态	目录所属的类型。
发布者	目录的发布者。
布局	目录关联的布局。
目录地址	目录所在地址。系统自动生成的访问目录页面的地址。
中文别名	目录的中文名称。
英文别名	目录的英文名称。
落地页	设置单击工作空间名称后进入空间详情的默认页面。 • 一个工作空间必须有一个落地页。 • 只能设置允许显示的目录中的一个作为落地页。 • 一级目录不支持设置为落地页。
是否显示	控制该目录是否在导航栏显示。

参数名称	参数说明
操作	可对目录进行编辑、更换布局等操作。 编辑：支持编辑目录的“中文别名”、“英文别名”、“落地页”、“是否显示”。 更换布局：用户自定义的目录，或系统内置的关联了布局的目录支持更换布局。**仅支持更换相同布局类型的其他布局。**

----结束

更换布局

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“安全编排 > 目录定制”，进入目录定制页面。

步骤 5 单击目标目录所在行“操作”列的“更换布局”，弹出更换布局页面。

步骤 6 在更换布局页面中，选择需要替换的布局。

步骤 7 单击“确定”。

----结束

14 云审计服务支持的关键操作

14.1 云审计服务支持的态势感知（专业版）操作列表

云审计服务（Cloud Trace Service，CTS）记录了态势感知（专业版）相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《云审计服务用户指南》。

云审计服务支持的态势感知（专业版）操作列表如表 14-1 所示。

表 14-1 云审计服务支持的态势感知（专业版）操作列表

操作名称	资源类型	事件名称
剧本审核	playbook	approvePlaybook
创建剧本动作	playbook	createPlaybookAction
修改剧本动作	playbook	updatePlaybookAction
删除剧本动作	playbook	deletePlaybookAction
创建剧本	playbook	createPlaybook
修改剧本	playbook	updatePlaybook
删除剧本	playbook	deletePlaybook
操作剧本实例	playbook	operatePlaybookInstance
导出剧本实例	playbook	exportPlaybookInstance
导出剧本	playbook	exportPlaybook
导入剧本	playbook	importPlaybook
新增剧本触发规则	playbook	createPlaybookRule
更新剧本触发规则	playbook	updatePlaybookRule
删除剧本触发规则	playbook	deletePlaybookRule
创建剧本版本	playbook	createPlaybookVersion

操作名称	资源类型	事件名称
更新剧本版本	playbook	updatePlaybookVersion
删除剧本版本	playbook	deletePlaybookVersion
克隆剧本版本	playbook	clonePlaybookVersion
创建流程	workflow	createWorkflow
修改流程	workflow	updateWorkflow
删除流程	workflow	deleteWorkflow
创建流程版本	workflow	createWorkflowVersion
修改流程版本	workflow	updateWorkflowVersion
审核流程版本	workflow	approveWorkflowVersion
删除流程版本	workflow	deleteWorkflowVersion
导出流程	workflow	exportWorkflow
导入流程	workflow	importWorkflow
创建资产连接	asset	createAsset
创建资产连接	asset	updateAsset
删除资产连接	asset	deleteAsset
上传附件	component	uploadAttachement
创建插件模板	component	createComponentTemplate
更新插件模板	component	updateComponentTemplate
删除插件模板	component	deleteComponentTemplate
添加评论	task	commentTask
提交待办	task	commitTask
创建工作空间	workspace	createWorkspace
删除工作空间	workspace	deleteWorkspace
更新工作空间	workspace	updateWorkspace
重新收集子服务统计数据	workspace	recollectServiceStatistics

14.2 在 CTS 事件列表查看云审计事件

场景描述

云审计服务能够为您提供云服务资源的操作记录，记录的信息包括发起操作的用户身份、IP 地址、具体的操作内容的信息，以及操作返回的响应信息。根据这些操作记录，您可以很方便地实现安全审计、问题跟踪、资源定位，帮助您更好地规划和利用已有资源、甄别违规或高危操作。

什么是事件

事件即云审计服务追踪并保存的云服务资源的操作日志，操作包括用户对云服务资源新增、修改、删除等操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。

约束与限制

- 用户通过云审计控制台只能查询最近 7 天的操作记录，过期自动删除，不支持人工删除。如果需要查询超过 7 天的操作记录，您必须配置转储到对象存储服务（OBS）或云日志服务（LTS），才可在 OBS 桶或 LTS 日志组里面查看历史事件信息。否则，您将无法追溯 7 天以前的操作记录。
- 用户对云服务资源做出创建、修改、删除等操作后，1 分钟内可以通过云审计控制台查询管理类事件操作记录，5 分钟后才可通过云审计控制台查询数据类事件操作记录。

在 CTS 新版事件列表查看审计事件

步骤 1 登录控制台，单击左上角，选择“管理与部署 > 云审计服务 CTS”，进入云审计服务页面。

步骤 2 单击左侧导航栏的“事件列表”，进入事件列表信息页面。

步骤 3 在列表上方，可以通过筛选时间范围，查询最近 1 小时、最近 1 天、最近 1 周的操作事件，也可以自定义最近 7 天内任意时间段的操作事件。

步骤 4 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件。

表 14-2 事件筛选参数说明

参数名称	说明
事件名称	操作事件的名称。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 各个云服务支持审计的操作事件的名称请参见《云审计服务用户指南》的“支持审计的服务及操作列表”章节。 示例：updateAlarm

参数名称	说明
云服务	云服务的名称缩写。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 示例：IAM
资源名称	操作事件涉及的云资源名称。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 当该事件所涉及的云资源无资源名称或对应的 API 接口操作不涉及资源名称参数时，该字段为空。 示例：ecs-name
资源 ID	操作事件涉及的云资源 ID。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 当该资源类型无资源 ID 或资源创建失败时，该字段为空。 示例：*{虚拟机 ID}*
事件 ID	操作事件日志上报到 CTS 后，查看事件中的 trace_id 参数值。 输入的值需全字符匹配，不支持模糊匹配模式。 示例：01d18a1b-56ee-11f0-ac81-******1e229
资源类型	操作事件涉及的资源类型。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 各个云服务的资源类型请参见《云审计服务用户指南》的“支持审计的服务及操作列表”章节。 示例：user
操作用户	触发事件的操作用户。 下拉选项中选择一个或多个操作用户。 查看事件中的 trace_type 的值为“SystemAction”时，表示本次操作由服务内部触发，该条事件对应的操作用户可能为空。
事件级别	下拉选项包含“normal”、“warning”、“incident”，只可选择其中一项。 • normal 代表操作成功。 • warning 代表操作失败。 • incident 代表比操作失败更严重的情况，如引起其他故障等。

步骤 5 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。

- 在搜索框中输入任意关键字，按下 Enter 键，可以在事件列表搜索符合条件的数据。
- 单击“导出”按钮，云审计服务会将查询结果以.xlsx 格式的表格文件导出，该.xlsx 文件包含了本次查询结果的所有事件，且最多导出 5000 条信息。
- 单击按钮，可以获取到事件操作记录的最新信息。

- 单击按钮，可以自定义事件列表的展示信息。启用表格内容折行开关，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。

步骤 6 （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

----结束

在 CTS 旧版事件列表查看审计事件

步骤 1 登录控制台，单击左上角，选择“管理与部署 > 云审计服务 CTS”，进入云审计服务页面。

步骤 2 单击左侧导航栏的“事件列表”，进入事件列表信息页面。

步骤 3 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。

步骤 4 在页面右上方，可以通过筛选时间范围，查询最近 1 小时、最近 1 天、最近 1 周的操作事件，也可以自定义最近 7 天内任意时间段的操作事件。

步骤 5 事件列表支持通过筛选来查询对应的操作事件。

表 14-3 事件筛选参数说明

参数名称	说明
事件类型	事件类型分为“管理事件”和“数据事件”。 • 管理类事件，即用户对云服务资源新建、修改、删除等操作事件。 • 数据类事件，即 OBS 服务上报的 OBS 桶中的数据的操作事件，例如上传数据、下载数据等。
云服务	在下拉选项中，选择触发操作事件的云服务名称。
资源类型	在下来选项中，选择操作事件涉及的资源类型。 各个云服务的资源类型请参见《云审计服务用户指南》的“支持审计的服务及操作列表”章节。
筛选类型	筛选类型分为“资源 ID”、“事件名称”和“资源名称”。 • 资源 ID：操作事件涉及的云资源 ID。 当该资源类型无资源 ID，或资源创建失败时，该字段为空。 • 事件名称：操作事件的名称。 各个云服务支持审计的操作事件的名称请参见《云审计服务用户指南》的“支持审计的服务及操作列表”章节。 • 资源名称：操作事件涉及的云资源名称。 当事件所涉及的云资源无资源名称，或对应的 API 接口操作不涉及资源名称参数时，该字段为空。

参数名称	说明
操作用户	触发事件的操作用户。 下拉选项中选择一个或多个操作用户。 查看事件中的 trace_type 的值为“SystemAction”时，表示本次操作由服务内部触发，该条事件对应的操作用户可能为空。
事件级别	可选项包含“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。 • Normal 代表操作成功。 • Warning 代表操作失败。 • Incident 代表比操作失败更严重的情况，如引起其他故障等。

步骤 6 选择完查询条件后，单击“查询”。

步骤 7 在事件列表页面，您还可以导出操作记录文件和刷新列表。

- 单击“导出”按钮，云审计服务会将查询结果以 CSV 格式的表格文件导出，该 CSV 文件包含了本次查询结果的所有事件，且最多导出 5000 条信息。
- 单击按钮，可以获取到事件操作记录的最新信息。

步骤 8 在事件的“是否篡改”列中，您可以查看该事件是否被篡改：

- 上报的审计日志没有被篡改，显示“否”；
- 上报的审计日志被篡改，显示“是”。

步骤 9 在需要查看的事件左侧，单击展开该记录的详细信息。

步骤 10 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。

步骤 11 （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

----结束

相关文档

- 关于事件结构的关键字段详解，请参见“《云审计服务用户指南》 > 事件参考 > 事件结构”章节和“《云审计服务用户指南》 > 事件参考 > 事件样例”章节。

15 常见问题

15.1 产品咨询

15.1.1 态势感知（专业版）与其他安全服务之间的关系与区别？

态势感知（专业版）与其他安全防护服务（WAF、HSS、Anti-DDoS、DBSS）的关系与区别如下：

- 关联：

  态势感知（专业版）：作为安全管理服务，依赖于其他安全服务提供威胁检测数据，进行安全威胁风险分析，呈现全局安全威胁态势，并提供防护建议。

  其他安全服务：威胁检测数据可以统一汇聚在态势感知（专业版）中，呈现全局安全威胁攻击态势。

- 区别：

  态势感知（专业版）：仅为可视化威胁检测和分析的平台，不实施具体安全防护动作，需与其他安全服务搭配使用。

  其他安全服务：仅展示对应服务的检测分析数据，并实施具体安全防护动作，不会呈现全局的威胁攻击态势。

态势感知（专业版）与其他安全防护服务区别，详细内容如表 15-1。

表 15-1 态势感知（专业版）与其他服务的区别

服务名称	服务类别	关联与区别	防护对象
态势感知（专业版）	安全管理	态势感知（专业版）着重呈现全局安全威胁攻击态势，统筹分析多服务威胁数据和云上安全威胁，并提供防护建议。	呈现全局安全威胁攻击态势。
Anti-DDoS 流量清洗（Anti-DDoS）	网络安全	Anti-DDoS 集中于异常 DDoS 攻击流量的检测和防御，相关攻击日志、防护等数据同步给态势感知（专业版）。	保障企业业务稳定性。

服务名称	服务类别	关联与区别	防护对象
企业主机安全（HSS）	主机安全	HSS 着手于保障主机整体安全性，检测主机安全风险，执行防护策略，相关告警、防护等数据同步给态势感知（专业版）。	保障主机整体安全性。
Web 应用防火墙（WAF）	应用安全	WAF 服务对网站业务流量进行多维度检测和防护，防御常见攻击，阻断恶意流量攻击，防止对网站造成威胁。相关入侵日志、告警数据等同步给态势感知（专业版），呈现全网 Web 风险态势。	保障 Web 应用程序的可用性、安全性。
数据库安全服务（DBSS）	数据安全	DBSS 着力于数据库访问行为的防护和审计，相关审计日志、告警数据等同步给态势感知（专业版）。	保障云上数据库安全和资产安全。

15.1.2 态势感知（专业版）与 HSS 服务的区别？

服务含义区别

- 态势感知（专业版）是云原生的新一代安全运营中心，基于云原生安全，提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，可以鸟瞰整个云上安全，精简云安全配置、云防护策略的设置与维护，提前预防风险，同时，可以让威胁检测和响应更智能、更快速，帮助您实现一体化、自动化安全运营管理，满足您的安全需求。
- 企业主机安全（Host Security Service，HSS）是以工作负载为中心的安全产品，集成了**主机**安全、**容器**安全和**网页防篡改**，旨在解决混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。

简而言之，态势感知（专业版）是呈现**全局**安全态势的服务，HSS 是提升**主机**和**容器**安全性的服务。

服务功能区别

- 态势感知（专业版）通过采集**全网安全数据**（包括 HSS、WAF、AntiDDoS 等安全服务检测数据），提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，帮助您实现一体化、自动化安全运营管理，满足您的安全需求。
- HSS 通过在**主机**中安装 Agent，使用 AI、机器学习和深度算法等技术分析主机中风险，并从 HSS 云端防护中心下发检测和防护任务，全方位保障主机安全。同时可从可视化控制台，管理主机 Agent 上报的安全信息。

表 15-2 态势感知（专业版）与 HSS 主要功能区别

功能项	共同点	不同点

功能项		共同点	不同点
资产安全	主机资产	呈现主机资产的整体安全状态。	• 态势感知（专业版）：仅支持同步 HSS 主机资产风险信息，呈现各主机资产的整体安全状况。 • HSS：不仅支持呈现主机的安全状况，还支持深度扫描主机中的账号、端口、进程、Web 目录、软件信息和自启动任务。
	网站资产	-	• 态势感知（专业版）：支持检查和扫描网站安全状态，呈现各网站资产的整体安全状况。 • HSS：不支持该功能。
漏洞管理	主机漏洞	呈现主机漏洞扫描结果，管理主机漏洞。	• 态势感知（专业版）：仅支持同步 HSS 主机漏洞扫描结果，管理主机漏洞。 • HSS：支持检测 Linux 漏洞、Windows 漏洞、Web-CMS 漏洞、应用漏洞，提供漏洞概览，包括主机漏洞检测详情、漏洞统计、漏洞类型分布、漏洞 TOP5 和风险服务器 TOP5，帮助您实时了解主机漏洞情况。
基线检查	云服务基线	-	• 态势感知（专业版）：针对云服务关键配置项，从多种风险类别，了解云服务风险配置的所在范围和风险配置数目。 • HSS：不支持该功能。
	主机基线	-	• 态势感知（专业版）：不支持该功能。 • HSS：针对主机，提供基线检查功能，包括检测复杂策略、弱口令及配置详情，包括对主机配置基线通过率、主机配置风险 TOP5、主机弱口令检测、主机弱口令风险 TOP5 的统计。

15.1.3 态势感知（专业版）的数据来源是什么？

态势感知（专业版）基于云上威胁数据和云服务采集的威胁数据，通过大数据挖掘和机器学习，分析并呈现威胁态势，并提供防护建议。

- 一方面采集全网流量数据，以及安全防护设备日志等信息，通过大数据智能 AI 分析采集的信息，呈现资产的安全状况，并生成相应的威胁告警。
- 另一方面汇聚企业主机安全（Host Security Service，HSS）、Web 应用防火墙（Web Application Firewall，WAF）等安全防护服务上报的告警数据，从中获取必要的安全事件记录，进行大数据挖掘和机器学习，智能 AI 分析并识别出攻击和入侵，帮助用户了解攻击和入侵过程，并提供相关的防护措施建议。

态势感知（专业版）通过对多方面的安全数据的分析，为安全事件的处置决策提供依据，实时呈现完整的全网攻击态势。

15.2 购买和变更规格

15.2.1 态势感知（专业版）如何收费？

态势感知（专业版）服务提供包年/包月和按需计费的计费模式。

- 包年/包月

  购买时长越久越便宜，包周期计费按照订单的购买周期来进行结算。

- 按需计费

  按小时计费，根据实际使用时长（小时）计费。先使用后付费，使用方式灵活，可以即开即停。

15.2.2 态势感知（专业版）支持退订吗？

如果用户不再使用态势感知（专业版）防护功能或增值包，可执行退订或一键取消操作。

- 包周期（包年/包月）计费模式：预付费方式。新购 5 天内的资源，支持每年 10 次 5 天无理由“退订”；使用超过 5 天的资源，“退订”需要收取手续费。
- 按需计费模式：按小时计费方式。资源即开即停，支持一键“取消”释放资源。

在使用态势感知（专业版）的数据采集功能时，需要购买 ECS 节点（用于采集数据）、新增并配置 VPC 终端节点（用于连通和管理采集节点）。如果退订了态势感知（专业版），需要手动释放创建的 ECS 资源和 VPC 终端节点资源，避免继续计费。

退订包周期计费

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在“总览”页面中，单击右上角“专业版”，显示版本管理窗口。

步骤 4 针对包周期购买的资产配额，单击“退订”，进入云服务退订页面。

步骤 5 在需要退订的实例所在行，单击“操作”列中的“退订资源”，进入退订资源页面。

步骤 6 确认待退订资源信息，选择退订原因，并勾选退订确认。

步骤 7 单击“退订”，在退订管理页面确认退订。

退订成功后，返回版本管理窗口，包年/包月计费的资产配额已取消。

----结束

15.2.3 态势感知（专业版）即将到期，如何续费？

态势感知（专业版）续费是在原已购买的版本规格的基础上，延长使用时间。续费操作不能变更版本规格，即不能改变“主机配额”。

续费操作仅针对包周期版本。

- 包周期（包年/包月）模式为预付费方式。当购买的包周期版本到期时，用户需通过续费延长使用期。
- 按需计费为按小时计费，即开即用。在账户余额充足前提下，不涉及过期情况，即无需续费操作。

手动续费

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“已购资源”，进入已购资源页面后，在待续费态势感知（专业版）版本所在 region 栏中，单击“续费”，系统跳转至费用中心“续费管理”页面。

步骤 4 在态势感知（专业版）实例所在行，单击“续费”，跳转至“续费”页面。

步骤 5 配置“续费时长”，如选择“一年”。

步骤 6 （可选）设置并勾选“统一到期时间”。默认将统一到期时间设置为每月 1 号 23:59:59 GMT+08:00。

步骤 7 单击“去支付”，跳转至支付页面，完成付款。

步骤 8 返回续费管理页面，可查看态势感知（专业版）已续费成功。

----结束

开通自动续费

在账户余额充足前提下，已配置“自动续费”后，包周期版本的资产配额、增值包、安全编排将自动续费，延长使用周期。

步骤 1 登录管理控制台。

步骤 2 单击“费用与成本 > 续费管理”，跳转至费用中心“续费管理”页面。

步骤 3 在“手动续费项”页签，选择态势感知（专业版）专业版实例，单击“设为自动续费”，跳转至自动续费配置页面。

步骤 4 选择配置“自动续费周期”和勾选“预设自动续费次数”。

步骤 5 单击“开通”，完成自动续费配置。

步骤 6 返回续费管理页面，在“自动续费项”页签，可查看态势感知（专业版）已开通自动续费。

后续将根据配置，自动续费延长使用期。

----结束

15.2.4 态势感知（专业版）到期后，会继续收费吗？

态势感知（专业版）到期后，不会继续收费。若到期后，未及时续费，会依次进入宽限期、保留期。

- 到期时间：针对包周期购买的态势感知（专业版）和资源，用户可以在态势感知（专业版）控制台“已购资源”页面查看到期时间。而按需资源自动扣费导致欠费后，将进入宽限期。
- 宽限期：指客户的包年/包月资源到期未续订或按需资源欠费时，**宽限期内该资源可以正常使用**。
- 保留期：指宽限期到期后客户的包年/包月资源仍未续订或按需资源仍未缴清欠款，将进入保留期。**保留期内该资源不能正常使用，但对客户存储在该资源中的数据仍予以保留。**

  保留期到期后，包年/包月资源仍未续订或按需资源仍未充值缴清欠款，存储在该资源中的数据将被删除，包年/包月资源将被释放，按需资源将被删除。

15.2.5 如何修改或取消态势感知（专业版）自动续费？

态势感知（专业版）开通自动续费后，如果需要取消或修改，可参照本章节进行处理。

取消态势感知（专业版）自动续费

态势感知（专业版）开通自动续费后，支持取消自动续费操作。关闭自动续费后，版本到期将恢复为手动续费。

修改态势感知（专业版）自动续费

态势感知（专业版）开通自动续费后，支持修改续费配置，包括修改续费设定、修改自动续费周期、重置自动续费次数等。

15.2.6 态势感知（专业版）可以免费使用吗？

可以。

态势感知（专业版）提供基础版和专业版两个服务版本。

- 用户可长期免费使用基础版。
- 专业版支持包周期或按需计费购买。

15.3 安全态势

15.3.1 如何更新安全评分？

态势感知（专业版）支持实时检测整体资产的安全状态，评估整体资产安全健康得分。通过查看安全评分，可快速了解未处理风险对资产的整体威胁状况。

资产安全风险修复后，为降低安全评分的风险等级，目前需手动忽略或处理告警事件，刷新告警列表中告警事件状态。告警事件状态刷新并启动重新检测后，安全评分将更新。

更新安全评分

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面，对不合格的基线检查项目进行处理。

步骤 5 在左侧导航栏选择“风险预防 > 漏洞管理”，进入漏洞管理页面，对漏洞进行处理。

步骤 6 在左侧导航栏选择“威胁管理 > 告警管理”，进入全部告警管理页面，对告警事件进行处理。

步骤 7 相应基线、漏洞、告警处理后，返回“态势感知 > 态势总览”页面，单击“重新检测”，检测后可查看更新的安全评分。

由于检测需要一定的时间，请您在单击“重新检测”按钮**5分钟**后，再刷新页面，查看最新检测的安全评分。

----结束

15.3.2 为什么没有看到攻击数据或者看到的攻击数据很少？

态势感知（专业版）支持检测云上资产遭受的各类攻击，并进行客观的呈现。

但是，如果您的云上资产在互联网上的暴露面非常少（所谓“暴露面”是指资产可被攻击或利用的风险点，例如，端口暴露和弱口令都可能成为风险点），那么遭受到攻击的可能性也将大大降低，所以，态势感知（专业版）可能会显示您的系统当前遭受的攻击程度较低。

如果您认为态势感知（专业版）未能真实反映系统遭受攻击的状况，欢迎您向技术人员反馈问题。

15.3.3 为什么总览页面中数据不一致或未展示数据？

为什么 WAF、HSS 中的数据和态势感知（专业版）中的数据不一致？

由于态势感知（专业版）中汇聚了 WAF、HSS 上报的所有历史告警数据，而 WAF 和 HSS 中展示的是实时告警数据，导致存在态势感知（专业版）与 WAF、HSS 中数据不一致的情况。

因此，建议您前往对应服务（WAF 或 HSS）进行查看并处理。

为什么总览页面中没有显示资产总数？

问题现象：

工作空间新增完成后，在工作空间内的“资产管理”页面中同步并已显示资产信息，但是“总览”页面中的资产总数仍然显示为 0。

问题原因：

工作空间创建成功，且资产等数据信息接入完成后，态势感知（专业版）将在**整点**进行数据同步，请耐心等待同步后再进行查看。

解决方法：

请您耐心等待，同步会系统将更新资产等相关数据信息。

15.4 威胁管理

15.4.1 如何处理暴力破解告警事件？

暴力破解是一种常见的入侵攻击行为，攻击者通常使用暴力破解的方式猜测远程登录的用户名和密码，一旦破解成功，即可实施攻击和控制，严重危害资产的安全。

态势感知（专业版）联动企业主机安全（HSS），接收 HSS 检测到的暴力破解行为，集中呈现和管理告警事件，提升运维效率。

处理告警事件

HSS 通过暴力破解检测算法和全网 IP 黑名单，如果发现暴力破解主机的行为，对发起攻击的源 IP 进行拦截，并上报告警事件。

当接收到来源于 HSS 的告警事件时，请登录 HSS 管理控制台确认并处理告警事件。

- 如果您的主机被爆破成功，检测到入侵者成功登录主机，账户下所有云服务器可能已被植入恶意程序，建议参考如下措施，立即处理告警事件，避免进一步危害主机的风险。
  a. 请立即确认登录主机的源 IP 的可信情况。
  b. 请立即修改被暴力破解的系统账户口令。
  c. 请立即执行检测入侵风险账户，排查可疑账户并处理。
  d. 请及时执行恶意程序云查杀，排查系统恶意程序。
- 如果您的主机被暴力破解，攻击源 IP 被 HSS 拦截，请参考如下措施，加固主机安全。
  a. 请及时确认登录主机的源 IP 的可信情况。
  b. 请及时登录主机系统，全面排查系统风险。
  c. 请根据实际需求升级 HSS 防护能力。
  d. 请根据实际情况加固主机安全组、防火墙配置。

标记告警事件

告警事件处理完成后，您可以根据处理情况，标记已识别的告警事件，加强对告警事件的管理。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

步骤 4 在左侧导航栏选择“威胁管理 > 告警管理”，进入告警列表管理页面。

步骤 5 选择“暴力破解”类型，刷新告警列表。

步骤 6 选择目标告警，根据实际情况删除无威胁告警事件。

----结束

15.4.2 如何查看所有日志已占用的存储空间大小？

态势感知（专业版）支持在“安全报告”中查看所有日志占用的存储空间大小。在安全报告中可以查看日志分析的以下信息：

- 安全报告的**日报**中的“日志分析”参数可展示前一天的日志存储总量；
- 安全报告的**周报**中的“日志分析”参数展示上周一整周日志分析的情况，包含日志存储总量；
- 安全报告的**月报**中的“日志分析”参数展示上一个月整月日志分析的情况，包含日志存储总量。

安全报告查看方法请参见查看安全报告。

16 修订记录

发布日期	修改记录
2025-09-08	第六次正式发布。 • 更新产品介绍中的“产品功能”章节内容，补充“AI 风险概览”相关功能说明。 • 更新基本概念章节下的“安全编排”章节内容，“资产连接”变更为“操作连接”。 • 更新“查看总览”章节内容，场景说明中“态势总览”的目录从“安全态势”变更到“态势感知”下。 • 更新“查看工作空间”章节内容，工作空间详情页新增了“导航设置”页签，增加相关说明。 • 更新“查看态势总览”章节内容，态势总览目录界面词变化，从“安全态势 > 态势总览”变更到“态势感知 > 态势总览”。 • 更新“创建或复制安全报告”章节内容，适配控制台界面变更。 • 更新“查看安全报告”章节内容，适配控制台安全报告的目录变更，以及安全报告模板展示内容的变更。 • 更新“下载安全报告”章节内容，适配控制台安全报告的界面变更。 • 更新“管理安全报告”章节内容，适配控制台安全报告的界面变更，安全报告支持下载和分享。 • 更新“任务中心”章节内容，任务中心目录界面词变化，从“安全态势 > 任务中心”变更到“态势感知 > 任务中心”。 • 新增“AI 风险概览”章节内容。 • 更新“查看资产信息”，“导入或导出资产”，“编辑或删除资产”章节内容，资产管理界面新增“部门及业务系统”相关内容。 • 更新“基线检查概述”章节内容，补充使用流程说明。 • 更新“定时执行基线检查”、“手动执行基线检查”章节

发布日期	修改记录
	的“约束与限制”内容。 • 更新“查看检查结果”章节的前提条件内容。 • 更新“处理检查结果”章节的约束与限制内容。 • 更新“管理遵从包”章节的约束与限制内容。 • 更新“管理检查项”章节内容，支持对检查项加白名单。 • 更新“漏洞管理概述”章节内容，补充网站漏洞相关说明。 • 更新“策略管理概述”章节约束与限制内容，单次下发策略阻断对象数规格变更。 • 更新“新增策略”章节的约束与限制，以及操作步骤。 • 更新“管理策略”章节内容操作步骤。 • 删除“批量阻断或批量取消阻断”章节。 • 更新“告警概述”章节内容，告警区分告警和攻击。 • 更新“查看告警信息”章节内容，告警区分告警和攻击，适配控制台变化。 • 更新“告警转事件或关联事件”章节内容操作步骤。 • 更新“一键阻断或解封”章节约束与限制，操作步骤。 • 更新“新增或编辑告警”章节内容，更新告警参数说明。 • 更新“导入或导出告警”章节内容，新增“导出攻击”相关操作步骤。 • 新增“处置攻击”章节。 • 更新“智能建模”章节内容，智能建模所在目录从“威胁管理”变更到“建模分析”下。 • 更新“安全分析”章节内容，适配控制台安全分析导航目录变化。 • 更新“数据投递”章节内容，适配控制台导航目录变化。 • 更新“安全编排概述”。“启用流程”、“管理流程”章节内容，补充复制流程相关内容。 • 更新管理资产连接章节内容，“资产连接”变更为“操作连接”。 • 更新“接入日志数据”章节内容，适配控制台日志接入界面和导航目录变更。 • 更新“目录定制”章节内容，适配控制台导航目录变更。 • 用户指南手册目录结构调整，适配控制台工作空间的导航目录变更。
2025-07-24	第五次正式发布。 • 新增 CTS 相关“云审计服务支持的关键操作”章节内容。
2025-03-30	第四次正式发布。

发布日期	修改记录
	• 更新“基线检查”章节内容，基线检查功能全量升级，支持自定义新增检查项和遵从包。 • 更新描述信息：“威胁运营”更名为“威胁管理”。 • 更新“新增/编辑策略”章节内容，更新操作权限、策略约束与限制说明。 • 更新“安全编排概述”章节内容，更新剧本和流程描述信息。 • 更新“产品功能”章节内容，更新页面呈现方式。 • 新增“经验包”章节，承载产品内置能力，比如内置检查项，内置剧本。 • 更新“约束与限制”章节，优化章节结构。 • 更新“基本概念”章节，优化章节结构，补充了基本概念内容。
2024-11-30	第三次正式发布。 • 更新“购买态势感知（专业版）”章节内容，更新参数描述信息。 • 删除数据采集相关内容。
2024-05-15	第二次正式发布。 • 更新“查看待办任务”、“查看已处理任务”章节内容，新增任务到期时间描述信息。 • 更新“查看资产信息”、“编辑/删除资产”章节内容，新增批量编辑资料描述信息；章节内容优化。 • 更新“查看基线检查结果”章节内容，新增检查结果页面描述。 • 更新“处理基线检查结果”章节内容，新增导入、导出检查结果操作指导。 • 更新“创建/复制安全报告”、“查看安全报告”章节内容，新增周报、月报展示内容说明信息。 • 更新“查看资产信息”、“查看漏洞详情”、“查看事件信息”、“查看告警信息”、“新增/编辑情报指标”章节内容，更新页面布局截图。 • 更新“内置剧本和流程”章节内容，新增并更新内置剧本和流程信息。
2023-11-30	第一次正式发布。