安全云脑

用户指南

文档版本 03

发布日期 2024-10-30

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 产品介绍

1.1 什么是安全云脑

安全云脑（SecMaster）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。

为什么选择安全云脑

- 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。
- 一云全局分析：结合每日数亿威胁情报定位威胁，多维关联分析，消除无效告警、识别潜在高级威胁。
- 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 什么是安全运营中心

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，这有助于他们领先于最新威胁。

- **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，他们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。他们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，他们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。他们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，他们负责在出现违规后收集情报来确定其根本原因。他们会搜寻系统漏洞、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，如果他们没有威胁调查员，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、政府和其他组织领先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。他们会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，他们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，他们会隐藏起来、窃取大量数据，并在任何人注意到之前提升他们的权限。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。首先是要找到最优秀的人才，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。他们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会在卓越安全工具上投入，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。与终结点检测和响应 (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/组织的终结点、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。

说明

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。安全云脑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。他们还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。

1.3 产品优势

见微知著的指标脉络与态势呈现

您可以通过安全态势即时查看大屏、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、MSSP（Managed Security Service Provider）托管等。

1.4 应用场景

云安全的理念是“三分建设，七分运营”，安全云脑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。

1.5 产品功能

安全云脑基于云原生安全，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。

本文介绍安全云脑支持使用的功能及各版本的功能差异。

总览

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。

表 1-1 总览功能介绍

功能模块	功能描述
总览	● 安全评分：根据安全云脑的威胁检测能力，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。 评估得分越低，即风险值越大，则整体资产安全隐患越大。 ● 安全监控：集中呈现未处理的威胁告警、漏洞和合规检查的风险数目，支持快速查看威胁告警、漏洞和合规风险详情。 ● 安全趋势：呈现最近7天整体资产安全健康得分的趋势图。

工作空间管理

工作空间属于安全云脑顶层工作台，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。

表 1-2 工作空间功能说明

功能模块	功能描述
工作空间	● 空间管理： 安全云脑顶层工作台，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。

已购资源

已购资源集中呈现当前账号已经购买的资源，方便统一管理已购资源。

表 1-3 已购资源功能说明

功能模块	功能描述
已购资源	在安全云脑的已购资源中可统一呈现当前账号已经购买的资源，方便统一管理已购资源。

安全态势

支持通过安全态势即时查看大屏、定期订阅安全运营报告，了解安全运营核心关注指标。

表 1-4 安全态势功能介绍

功能模块	功能描述
态势总览	• 安全评分：根据安全云脑的分析检测能力，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。评估得分越低，即风险值越大，则整体资产安全隐患越大。 • 安全监控：集中呈现未处理的威胁告警、漏洞和合规检查的风险数目，支持快速查看威胁告警、漏洞和合规风险详情。 • 安全趋势：呈现最近7天整体资产安全健康得分的趋势图。
安全大屏	利用AI技术将海量云安全数据的分析并分类，通过安全大屏将数据可视化展示，集中呈现云上实时动态，云上关键风险一目了然，掌握云上安全态势更简单，更直观，更高效。 **说明** 安全大屏功能需要单独申请。
安全报告	通过创建分析报告，定时以邮件形式向指定的收件人发送安全报告，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。

资产管理

资产管理支持持对云上资产全面盘点，也可灵活纳管云外各种资产，点清所有资产，并呈现资产实时安全状态。

表 1-5 资产管理功能说明

功能模块	功能描述	基础版	标准版	专业版
资产管理	同步所有资源的安全状态统计信息，支持查看资源的名称、所属服务、安全状况等，帮助您快速定位安全风险问题。	×	√	√

表 1-6 资产管理功能说明

功能模块	功能描述
资产管理	同步所有资源的安全状态统计信息，支持查看资源的名称、所属服务、安全状况等，帮助您快速定位安全风险问题。

风险预防

风险预防提供基线检查和漏洞管理功能，帮助您的云安全配置达到各类权威安全标准；知晓全局的漏洞分布。

表 1-7 风险预防功能介绍

功能模块	功能描述
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	通过自动同步企业主机安全（Host Security Service，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	支持统一管理应急策略。

威胁运营

威胁运营提供丰富的威胁检测模型，帮助您从海量的安全日志中，发现威胁、生成告警；同时，提供丰富的安全响应剧本，帮助您对告警进行自动研判、处置，并对安全防线和安全配置自动加固。

表 1-8 威胁运营功能介绍

功能模块	功能描述
事件管理	集中呈现事件详情，支持人工转事件、自动化转事件。
告警管理	提供统一的数据类管理（安全运营对象），内置告警标准。通过集成各云服务告警，包含HSS、WAF、DDoS等，集中呈现告警信息。
情报管理	提供统一的数据类管理（安全运营对象），内置威胁情报指标库标准。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。
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。

功能模块	功能描述
安全分析	● 查询与分析 – 检索分析：支持数据的快捷检索分析，支持安全调查场景安全数据的快速筛留、筛除等操作，快速定位关键数据。 – 筛选统计：支持数据字段快速分析统计，并基于分析结果进行数据的快速筛选；时序数据支持默认时间分区统计，快速识别数据量的变化趋势，支持基于时间分区的快速筛选；支持分析、统计、排序等丰富统计分析函数，支撑快速构建安全分析模型。 – 可视化：支持数据可视化分析，直观反映业务结构性和趋势性特征，并基于此构建自定义分析报告和分析指标。 ● 数据投递：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。 ● 数据监控：支持数据流量端到端的监控管理。 ● 数据消费：提供数据消费和生产的流式通信接口，提供数据管道集成SDK，支持租户利用SDK进行系统集成，支持客户自定义数据的生产和消费。提供Logstash开源采集软件插件，支持利用开源生态进行数据消费和生产。 **说明** 需额外申请增值包中的安全分析功能。

安全编排

安全编排支持剧本管理、流程管理、数据类管理（安全实体对象）和资产连接管理等。同时，可以自定义剧本和流程等。

通过安全编排可以对安全响应剧本进行拖拽式的灵活编排，动态适配您的业务需求。也可以对安全运营的对象、交互的页面进行灵活扩展和定义。

表 1-9 安全编排功能介绍

功能模块	功能描述
运营对象	集中对数据类、数据类类型、分类映射等运营对象进行管理。
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。 **说明** 需额外申请增值包中的安全编排功能。
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。

数据采集

通过多种方式采集各类日志数据。采集后，可以快速实现历史数据分析比对、数据关联分析、以及未知威胁发现等相关分析。

表 1-10 数据采集功能说明

功能模块	功能描述
数据采集（采集管理和组件管理）	使用Logstash通过多种方式采集各类日志数据。采集后，可以快速实现历史数据分析比对、数据关联分析、以及未知威胁发现等相关分析。

数据集成

通过集成云原生安全产品，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。

表 1-11 数据集成功能说明

功能模块	功能描述
数据集成	云内置采集系统，支持一键集成存储、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。

目录定制

支持自定义目录，可以根据需要对目录进行定制。

表 1-12 目录定制功能说明

功能模块	功能描述
目录定制	支持查看已有目录及更换布局等操作。

1.6 与其他云服务的关系

本章节主要介绍安全云脑与其他云服务之间的关系。

与安全服务的关系

安全云脑从企业主机安全（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

安全云脑为弹性云服务器（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。

1.7 基本概念

本节介绍安全云脑相关概念。

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。

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。对于安全云脑来讲，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。

工作空间

工作空间（Workspace）属于安全云脑顶层工作台，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。

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。

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

用于订阅安全云脑管道消息，一个管道可由多个订阅器进行订阅，安全云脑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，负责通过订阅器把安全云脑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 服务委托授权

操作场景

安全云脑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安全云脑，让安全云脑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**使用安全云脑时，需要先进行委托授权操作，才能正常访问和使用安全云脑。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“工作空间 > 空间管理”，进入安全云脑工作空间页面。

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

3 安全总览

3.1 总览

安全云脑“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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“总览”，进入安全云脑总览页面。

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 3-1 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，具体评分详细信息请参见**安全评分**。

参数名称	统计周期	更新频率	说明
威胁告警	近7天	每5分钟	本账号安全云脑下全部工作空间告警管理中的告警总和。
漏洞	近7天	每5分钟	本账号安全云脑下全部工作空间漏洞管理中的漏洞总和。
合规检查	实时	每5分钟	本账号安全云脑下全部工作空间基线检查中的问题总和。
安全趋势	近7天	每5分钟	近7天的安全评分数据。

----结束

安全评分

“安全评分”板块根据安全云脑的威胁检测能力，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。

  说明

  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 3-2 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。
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。 – 仅当主机中Agent版本为2.0时，才会在“漏洞类型Top5”中显示对应数据。如未显示数据或需要查看TOP5漏洞类型，请将主机将Agent1.0升级至Agent2.0。 ● 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。

参数名称	参数说明
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。

3.2 安全评分

操作场景

安全云脑实时呈现您云上资产的整体安全评估状况，并根据安全云脑的威胁检测能力，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。

本章节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

SecMaster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。

  说明

  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 3-3 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表3-4所示。

表 3-4 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	-	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，自动刷新评分。	20
	存在未处理的高危不合规项	5		
	存在未处理的中危不合规项	2		
	存在未处理的低危不合规项	0.1		

分类	扣分项	单项扣分值	处理建议	最高扣分上限
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		

4 工作空间

4.1 工作空间概述

本章节将介绍工作空间的定义、类型和基本操作等内容。

什么是工作空间?

工作空间（Workspace）属于安全云脑顶层工作台。

- 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。

什么是数据空间?

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载均衡策略。

什么是数据管道?

数据传输消息主题和存储索引组合为数据管道。

4.2 新增工作空间

操作场景

工作空间（Workspace）属于安全云脑顶层工作台，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。

在使用安全云脑的基线检查、告警管理、安全分析、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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“工作空间 > 空间管理”，进入安全云脑工作空间页面。

步骤4 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5 配置新建工作空间参数，参数说明如下表所示：

表 4-1 新增工作空间

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6 单击“确定”，完成工作空间的新增。

----结束

4.3 空间管理

4.3.1 查看工作空间详情

操作场景

本章节将介绍用户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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“工作空间 > 空间管理”，进入安全云脑工作空间页面。

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 4-1 工作空间详情

表 4-2 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。
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，可查看工作空间详细信息。
事件	该工作空间中的事件数量。
漏洞	该工作空间中的漏洞数量。
告警	该工作空间中的告警数量。
情报	该工作空间中的情报数量。
资产	该工作空间中已有资产的数量。
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。

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。

在工作空间的“基本信息”页签中，可以查看工作空间的名称、所属项目、ID等信息；在“标签管理”页签中，可以管理标签，管理标签详细操作请参见**管理工作空间标签**。

----结束

4.3.2 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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“工作空间 > 空间管理”，进入安全云脑工作空间页面。

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 4-2 工作空间详情页面入口

步骤5 在工作空间的“基本信息”页签中，单击“编辑”。

步骤6 编辑工作空间名称或描述后，单击“保存”。

----结束

4.3.3 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。

如您的组织已经设定安全云脑服务的相关标签策略，则需按照标签策略规则为工作空间添加标签。标签如果不符合标签策略的规则，则可能会导致工作空间创建失败，请联系组织管理员了解标签策略详情。

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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“工作空间 > 空间管理”，进入安全云脑工作空间页面。

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 4-3 工作空间详情页面入口

步骤5 在工作空间的详情页面中选择“标签管理”页签中，进入标签管理页面。

步骤6 在标签管理页面中，对标签进行管理。

表 4-3 管理标签

参数名称	参数说明
添加标签	1. 在标签管理页面中，单击“添加标签”。 2. 在弹出的添加标签页面中，配置标签键和值。 3. 配置完成后，单击“确定”。
编辑标签	1. 在标签管理页面中，单击标签所在行“操作”列的“编辑”。 2. 在弹出的编辑页面中，修改标签值。 3. 修改完成后，单击“确定”。
删除标签	在标签管理页面中，单击标签所在行“操作”列的“删除”，并在弹出的确认框中单击“是”。

----结束

4.3.4 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，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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“工作空间 > 空间管理”，进入安全云脑工作空间页面。

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 4-4 工作空间详情页面入口

步骤5 在工作空间的“基本信息”页签中，单击“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”中输入工作空间名称，并单击“删除”。

注意

- 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。

----结束

5 查看已购资源

操作场景

在安全云脑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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 5-1 查看已购资源信息

参数名称	参数说明
已开通区域/总区域	当前账号已开通安全云脑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申请版本中，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，已申请的总配额数量。
已购资源列表	各区域具体申请安全云脑资源的详细情况。 如果版本或区域较多，可以使用搜索功能，查看指定资源申请信息。

----结束

6 安全态势

6.1 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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“安全态势 > 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 6-1 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，具体评分详细信息请参见**安全分值和扣分项说明**。

参数名称	统计周期	更新频率	说明
威胁告警	近7天	每5分钟	当前工作空间内，“威胁运营 > 告警管理”中的告警总和。
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。
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。
安全趋势	近7天	每5分钟	近7天的安全评分数据。

----结束

安全评分

“安全评分”板块根据安全云脑的威胁检测能力，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**安全分值和扣分项说明**。
- 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。

  说明

  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。

安全分值和扣分项说明

安全云脑实时呈现您资产的整体安全评估状况，并根据安全云脑的威胁检测能力，评估整体资产安全健康得分。

此处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

  根据安全云脑的威胁检测能力，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。

    说明

    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 6-2 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表6-3所示。

表 6-3 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	-	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，自动刷新评分。	20
	存在未处理的高危不合规项	5		
	存在未处理的中危不合规项	2		
	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		

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 6-4 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。

参数名称	参数说明
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。 – 仅当主机中Agent版本为2.0时，才会在“漏洞类型Top5”中显示对应数据。如未显示数据或需要查看TOP5漏洞类型，请将主机将Agent1.0升级至Agent2.0。 ● 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。 ● 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。

6.2 安全大屏

6.2.1 综合态势感知大屏

操作场景

在现场讲解汇报、实时监控等场景下，为了获得更好的演示效果，通常需要将安全云脑服务的分析结果展示在大型屏幕上。如果只是单纯将控制台界面放大显示，视觉效果并不是很理想。此时可以利用**安全大屏**，展示专为大型屏幕设计的服务界面，获得更清晰的态势信息和更好的视觉效果。

安全云脑默认提供一个**综合态势感知大屏**，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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“安全态势 > 安全大屏”，进入安全大屏页面。

步骤5 单击综合安全态势大屏右下角的“播放”，进入综合态势感知大屏信息页面。

页面中各个模块的功能介绍、数据信息等详见下述内容。

----结束

安全评分

展示当前资产安全健康得分。

表 6-5 安全评分

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 • 随当前工作空间“态势总览”中的“安全评分”手动更新而更新，约有5分钟延迟	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，加权计算得来。 • 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”。

告警统计情况

展示已接入服务的告警统计情况。

告警数据统计情况来源于当前工作空间的“威胁运营 > 告警管理”，如需查看对应详细信息，可以前往该页面进行查看。

表 6-6 告警统计情况

参数名称	统计周期	更新频率	说明
新增告警	今天	5分钟	当天新增的告警数量。
威胁告警	近7天	5分钟	近7天新增的告警数量。
待解决告警	近7天	5分钟	近7天“状态”不是“关闭”的告警数量。
已解决告警	近7天	5分钟	近7天“状态”为“关闭”的告警数量。

资产防护率

展示近7天内主机和网站的防护情况，包含已防护和未防护资产的比例。将鼠标悬停在对应模块上，可以查看已防护/未防护资产数量。

表 6-7 资产防护率

参数名称	统计周期	更新频率	说明
资产防护率	近7天	5分钟	近7天内主机和网站的防护情况，包含已防护和未防护资产的比例。 ● 主机防护情况：已开启和未开启企业主机安全 HSS的ECS数量统计。 ● 网站防护情况：已开启和未开启Web应用防火墙 WAF防护网站数据统计。

基线合规

展示当前资产基线配置和漏洞修复情况、基线扫描后的风险资源分布情况和近7天内漏洞修复的趋势。

- 基线数据统计情况来源于当前工作空间的“风险预防 > 基线检查”，如需查看对应详细信息，可以前往该页面进行查看。
- 漏洞数据统计情况来源于当前工作空间的“风险预防 > 漏洞管理”，如需查看对应详细信息，可以前往该页面进行查看。

表 6-8 基线合规

参数名称	统计周期	更新频率	说明
配置基线	实时	5分钟	最近一次执行基线检查后，基线配置的统计情况，即基线配置通过和不通过的配置项目数量。
漏洞处理	近7天	5分钟	近7天的漏洞处理情况，包括已修复、未修复漏洞的数量。
风险资源分布	实时	5分钟	最近一次执行基线检查的风险资产分布情况以及风险资产的数量。风险等级分为：致命、高危、中危、低危、提示几个级别。
漏洞趋势	近7天	5分钟	近7天的每日新增的漏洞数据及其分布趋势。

威胁态势

展示**近7天内**每日受到威胁的资产的数量和**近7天内**每日上报的安全日志日志量大小。

威胁态势的横坐标表示时间，左侧纵坐标表示受威胁资产的数量，右侧纵坐标表示受威胁访问的日志量。将鼠标箭头置于某个日期上，可以看到该日受威胁的资产总数和日志量大小。

表 6-9 威胁态势

参数名称	统计周期	更新频率	说明
总攻击趋势	近7天	5分钟	近7天每日告警数量。 告警数据统计情况来源于当前工作空间的“威胁运营 > 告警管理”，如需查看对应详细信息，可以前往该页面进行查看。
日志量趋势	近7天	5分钟	近7天每日上报的安全日志日志量大小。

待办工单

实时展示当前工作空间内的待办事项。

表 6-10 待办工单

参数名称	统计周期	更新频率	说明
待办工单	实时	5分钟	当前工作空间内的“安全态势 > 任务中心”中待办的任务。

响应闭环

展示告警处置情况、近7天内SLA（计划关闭时间）和MTTR（平均恢复时间）达成率和近7天内事件自动处置统计情况。

告警数据统计情况来源于当前工作空间的“威胁运营 > 告警管理”，如需查看对应详细信息，可以前往该页面进行查看。

表 6-11 响应闭环

参数名称		统计周期	更新频率	说明
告警统计	告警总数	近7天	5分钟	近7天新增的告警数量。
	处置数			近7天“状态”为“关闭”的告警数量。
	及时处置数			近7天“状态”为“关闭”且满足计划关闭时间的告警数量。 满足计划关闭时间是指关闭时间早于或等于计划关闭时间。

参数名称		统计周期	更新频率	说明
	自动处置数			近7天“状态”为“关闭”且为安全云脑剧本等自动关闭的告警数量。 告警关闭方式查看方法：在告警详情中查看“close_comment”字段中的数值是否为“ClosedByCSB”或“ClosedBySecMaster”，如果是，则为自动关闭，如果不是则为手动关闭。
7天SLA和MTTR	SLA统计分析	近7天	5分钟	近7天告警处理的时效满足情况。计算方法如下： 已设置了SLA（计划关闭时间）字段的告警，当告警关闭时间-告警产生时间≤设置的SLA时间时，则表示满足，反之则表示不满足。 ● 满足：告警关闭时间早于或等于告警计划关闭时间； ● 不满足：告警关闭时间晚于告警计划关闭时间。
	MTTR平均响应时间			近7天平均告警关闭时间。计算方法如下： MTTR（平均恢复时间）=每个告警的处理时间总和/告警总数，其中，每个告警的处理时间=关闭时间-创建时间。
7天告警自动处置统计		近7天	5分钟	近7天告警被手动处理和自动处理了的统计总数。 ● 手动处置：告警管理中手动关闭的告警数量； ● 自动处置：由安全云脑剧本等方式自动关闭的告警数量。 告警关闭方式查看方法：在告警详情中查看“close_comment”字段中的数值是否为“ClosedByCSB”或“ClosedBySecMaster”，如果是，则为自动关闭，如果不是则为手动关闭。

6.2.2 值班响应大屏

操作场景

在现场讲解汇报、实时监控等场景下，为了获得更好的演示效果，通常需要将安全云脑服务的分析结果展示在大型屏幕上。如果只是单纯将控制台界面放大显示，视觉效果并不是很理想。此时可以利用**安全大屏**，展示专为大型屏幕设计的服务界面，获得更清晰的态势信息和更好的视觉效果。

安全云脑默认提供一个**值班响应大屏**，可以查看未处理告警、事件、漏洞、基线的总览情况，实现一屏全面感知。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“安全态势 > 安全大屏”，进入安全大屏页面。

步骤5 单击安全响应大屏右下角的“播放”，进入值班响应大屏信息页面。

页面中各个模块的功能介绍、数据信息等详见下述内容。

----结束

值班响应大屏总览

展示未处理告警、事件、漏洞、基线的总数。

表 6-12 值班响应大屏总览

参数名称	统计周期	更新频率	说明
未处理告警	近7天	5分钟	近7天“状态”为“打开”的告警数量。 告警数据统计情况来源于当前工作空间的“威胁运营 > 告警管理”，如需查看对应详细信息，可以前往该页面进行查看。
未处理事件	近7天	5分钟	近7天“状态”为“打开”或“阻塞”的事件数量。 事件数据统计情况来源于当前工作空间的“威胁运营 > 事件管理”，如需查看对应详细信息，可以前往该页面进行查看。
未处理漏洞	实时	5分钟	未处理漏洞统计数据。 漏洞数据统计情况来源于当前工作空间的“风险预防 > 漏洞管理”，如需查看对应详细信息，可以前往该页面进行查看。
未处理基线	实时	5分钟	基线检查中检查不通过的统计数据。 基线数据统计情况来源于当前工作空间的“风险预防 > 基线检查”，如需查看对应详细信息，可以前往该页面进行查看。

未处理告警

呈现TOP5的未处理威胁告警事件的信息，包括告警发现时间、威胁告警描述信息、告警等级、告警所属的类型。

TOP5是根据创建时间降序来排序的，即最新的时间排在最前，以此往下进行排序。

表 6-13 未处理告警

参数名称	统计周期	更新频率	说明
未处理告警	近7天	5分钟	近7天“状态”为“打开”的告警数量。 告警数据统计情况来源于当前工作空间的“威胁运营 > 告警管理”，如需查看对应详细信息，可以前往该页面进行查看。

未处理事件

呈现TOP5的未处理事件的信息，包括事件发现时间、事件描述、事件等级、事件所属类型。

TOP5是根据创建时间降序来排序的，即最新的时间排在最前，以此往下进行排序。

表 6-14 未处理事件

参数名称	统计周期	更新频率	说明
未处理事件	近7天	5分钟	近7天“状态”为“打开”或“阻塞”的事件数量。 事件数据统计情况来源于当前工作空间的“威胁运营 > 事件管理”，如需查看对应详细信息，可以前往该页面进行查看。

未处理漏洞

呈现TOP5的未处理漏洞的信息，包括漏洞发现时间、漏洞描述、漏洞类别、漏洞等级、受影响资产数。

TOP5是根据创建时间降序来排序的，即最新的时间排在最前，以此往下进行排序。

表 6-15 未处理漏洞

参数名称	统计周期	更新频率	说明
未处理漏洞	近7天	5分钟	未处理漏洞统计数据。 漏洞数据统计情况来源于当前工作空间的“风险预防 > 漏洞管理”，如需查看对应详细信息，可以前往该页面进行查看。

未处理基线

呈现TOP5的未处理基线的信息，包括基线发现时间、基线描述、基线检查项目的检查方式、受影响的资源总数。

TOP5是根据创建时间降序来排序的，即最新的时间排在最前，以此往下进行排序。

表 6-16 未处理基线

参数名称	统计周期	更新频率	说明
未处理基线	近7天	5分钟	基线检查中检查不通过的统计数据。 基线数据统计情况来源于当前工作空间的“风险预防 > 基线检查”，如需查看对应详细信息，可以前往该页面进行查看。

6.2.3 资产大屏

操作场景

在现场讲解汇报、实时监控等场景下，为了获得更好的演示效果，通常需要将安全云脑服务的分析结果展示在大型屏幕上。如果只是单纯将控制台界面放大显示，视觉效果并不是很理想。此时可以利用**安全大屏**，展示专为大型屏幕设计的服务界面，获得更清晰的态势信息和更好的视觉效果。

安全云脑默认提供一个**资产大屏**，可以查看资产总数、受攻击资产数、未防护资产数等总览情况，实现一屏全面感知。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“安全态势 > 安全大屏”，进入安全大屏页面。

步骤5 单击资产安全态势大屏右下角的“播放”，进入资产大屏信息页面。

页面中各个模块的功能介绍、数据信息等详见下述内容。

----结束

资产大屏总览

展示当前工作空间内资产、受攻击资产、未防护资产、漏洞和弱配置资产的总数。

表 6-17 资产大屏总览

参数名称	统计周期	更新频率	说明
资产总数	实时	每小时	“资产管理”中的全部资产数量。
受攻击资产数	近7天	每小时	“威胁运营 > 告警管理”中，受告警影响的资产去重后的数量。
未防护资产数	实时	每小时	未开启安全防护的资产数量，例如，没有开启企业主机安全的ECS，没有开启DDoS的弹性公网IP等。此处展示了“资产管理”的“防护状态”为“未防护”的资产数量。 资产管理中，资产防护状态说明如下： ● 已防护：表示已购买对应安全防护产品，且已开启防护。 ● 未防护：表示未购买对应安全防护产品，且未开启防护。如果需要防护目标资产，请购买对应安全防护产品并开启防护，例如，需要防护ECS，则请购买HSS，并在HSS中开启防护。 ● --：表示对应的安全防护产品在该region不支持使用。
漏洞和弱配置资产数	实时	每小时	受漏洞影响资产和基线检查中检查资源存在风险项的资产去重后的数据。 漏洞数据来源于“风险预防 > 漏洞管理”，基线检查数据来源于“风险预防 > 基线检查”中“检查资源”页签，如需查看对应详细信息，可以前往该页面进行查看。

资产分布情况

呈现资产类型的分布情况、资产防护率统计情况、资产变化趋势和TOP5受攻击资产所在区域分布情况。

表 6-18 资产分布情况

参数名称	统计周期	更新频率	说明
资产类型分布	实时	每小时	“资产管理”中的全部资产的不同类型资产的数量。
资产防护率统计	实时	每小时	不同类型资产开启安全防护的比例。 某一类型资产的开启安全防护的比例 = “防护状态”为“已防护”的资产 / 该类型资产总数。
资产变化趋势	近7天	每小时	近7天资产总数和存在漏洞、弱配置的资产数统计。
TOP5 受攻击资产	近7天	每小时	近7天受到攻击的前五名资产及其被攻击次数。 该数据来源于“威胁运营 > 告警管理”页面中，近7天告警数据中受影响资产统计情况，如需查看对应详细信息，可以前往该页面进行查看。

TOP5 漏洞数最多资产和 TOP5 资产防护率

呈现当前时间TOP5漏洞数量最多的资产和TOP5部门名下的资产防护率。

表 6-19 TOP5 漏洞数最多资产和 TOP5 资产防护率

参数名称	统计周期	更新频率	说明
Top5 漏洞数最多资产	实时	每小时	不同部门存在漏洞最多的资产前五名。 资产统计信息为“风险预防 > 漏洞管理”页面中受漏洞影响资产（该资产须在“资产管理”页面中的部门信息不为空的资产），按照部门进行统计后取前五名的资产。
Top5 资产防护率	实时	每小时	不同部门资产开启防护的比例，由高到低前五名。 “资产管理”中部门信息不为空的资产，按照部门进行统计后取前五名的信息。

6.2.4 威胁态势大屏

操作场景

在现场讲解汇报、实时监控等场景下，为了获得更好的演示效果，通常需要将安全云脑服务的分析结果展示在大型屏幕上。如果只是单纯将控制台界面放大显示，视觉效

果并不是很理想。此时可以利用**安全大屏**，展示专为大型屏幕设计的服务界面，获得更清晰的态势信息和更好的视觉效果。

安全云脑默认提供一个**威胁态势大屏**，可以查看网络攻击次数、应用拦截次数、主机层拦截次数等总览情况，实现一屏全面感知。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 单击威胁态势大屏右下角的“播放”，进入威胁态势大屏信息页面。

页面中各个模块的功能介绍、数据信息等详见下述内容。

----结束

威胁态势大屏总览

展示当前账号内资产的网络日志攻击次数、应用日志攻击次数和主机日志攻击次数。

表 6-20 威胁态势大屏总览

参数名称		统计周期	更新频率	说明
网络日志攻击	次数	近7天	每小时	近7天弹性公网IP被攻击的次数。
	较上周			近7天弹性公网IP被攻击次数，与近7-14天弹性公网IP被攻击次数的差值。
应用日志攻击	次数	近7天	每小时	近7天网站被攻击次数。
	较上周			近7天网站被攻击次数，与近7-14天网站被攻击次数的差值。
主机日志攻击	次数	近7天	每小时	近7天ECS被攻击次数。
	较上周			近7天ECS被攻击次数，与近7-14天ECS被攻击次数的差值。

攻击来源分布情况

呈现TOP5的网络攻击和应用攻击来源的分布情况，包括被攻击的资产IP、所属部门以及个数。

表 6-21 攻击来源分布情况

参数名称	统计周期	更新频率	说明
Top5 网络日志攻击来源分布	近7天	每小时	近7天弹性公网IP被攻击的情况，按照攻击的源IP进行聚合统计，按照聚合后的统计次数由多到少取前五名。
Top5 应用告警攻击来源分布	近7天	每小时	近7天网站被攻击的情况，按照攻击的源IP进行聚合统计，按照聚合后的统计次数由多到少取前五名。

攻击类型分布

呈现TOP5的网络攻击类型、TOP5的应用攻击类型、主机类型分布情况。

表 6-22 攻击类型分布

参数名称	统计周期	更新频率	说明
Top5 网络告警攻击类型	近7天	每小时	近7天弹性公网IP被攻击的类型统计，按照不同类型的攻击从多到少取前5名。 如果不存在网络攻击或没有对应数据表，则会展示五项全为0的默认类型。
Top5 应用告警攻击类型	近7天	每小时	近7天网站被攻击的类型统计，按照不同类型的攻击从多到少取前5名。 如果不存在应用攻击或没有对应数据表，则会展示五项全为0的默认类型。
Top5 主机告警攻击类型	近7天	每小时	近7天ECS被攻击的类型统计，按照不同类型的攻击从多到少取前5名。 如果不存在ECS攻击或没有对应数据表，则会展示五项全为0的默认类型。 资产统计信息来源于安全云脑的“威胁运营 > 告警管理”页面。

威胁态势统计

当前账号内资产的告警统计情况、日志分析总量及分布情况、模型检测总量及分布情况。

表 6-23 威胁态势统计

参数名称		统计周期	更新频率	说明
告警统计	日志条数	近7天	每小时	近7天网络、应用、主机被访问产生的日志条数总和。

参数名称		统计周期	更新频率	说明
	威胁攻击数			近7天网络、应用、主机识别为被攻击产生的日志条数总和。
	告警数			近7天“威胁运营 > 告警管理”中依据攻击日志产生的告警数量。
	事件数			近7天“威胁运营 > 事件管理”依据告警，转为的事件数量。
日志分析	总日志量	近7天	每小时	近7天网络、应用、主机被访问产生的日志大小总和，单位为MB。
	环比			近7天网络、应用、主机被访问产生的日志大小总和，与近7-14天用户网络、应用、主机被访问产生的日志大小总和的对比。 计算方法：（本期数 - 上期数）/ 上期数 × 100%。
	统计趋势图			近7天每天网络、应用、主机被访问产生的日志大小总和，单位为MB。
模型监测统计	模型总数	实时	每小时	“威胁运营 > 智能建模”中已有模型的数量。
	统计表格	近7天	每小时	每种类型的威胁检测模型，检测出的威胁次数。 如果没有威胁检测模型，则会默认展示四种类型，其值全部为0。

6.2.5 脆弱性大屏

操作场景

在现场讲解汇报、实时监控等场景下，为了获得更好的演示效果，通常需要将安全云脑服务的分析结果展示在大型屏幕上。如果只是单纯将控制台界面放大显示，视觉效果并不是很理想。此时可以利用**安全大屏**，展示专为大型屏幕设计的服务界面，获得更清晰的态势信息和更好的视觉效果。

安全云脑默认提供一个**脆弱性大屏**，可以查看脆弱性资产、漏洞、基线、未防护资产等总览情况，实现一屏全面感知。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“安全态势 > 安全大屏”，进入安全大屏页面。

步骤5 单击脆弱性大屏右下角的“播放”，进入脆弱性大屏信息页面。

页面中各个模块的功能介绍、数据信息等详见下述内容。

----结束

脆弱性大屏总览

展示脆弱性资产、漏洞、不合格基线、未防护资产的总数。

脆弱性资产表示当前时间存在未处理的漏洞、不合格的基线或未防护的资产。

表 6-24 脆弱性大屏总览

参数名称	统计周期	更新频率	说明
脆弱性资产总数	实时	每小时	存在漏洞、基线检查问题的资产数量统计
漏洞	实时	每小时	漏洞管理中的漏洞统计数据
不合格基线数	实时	每小时	安全云脑基线检查中的数据
未防护资产	实时	每小时	用户没有开启安全防护的资产数量，例如没有开启企业主机安全的ECS，没有开启DDoS的弹性公网IP等。

TOP5 部门脆弱性统计

呈现脆弱性统计TOP5的部门，包括部门名称，该部门的脆弱性风险资产数量、未修复漏洞数和未防护资产数。

表 6-25 部门脆弱性统计

参数名称	统计周期	更新频率	说明
Top5 部门脆弱性统计	实时	每小时	不同部门存在脆弱性资产、受漏洞影响资产、未防护的资产总和，从多到少排列的前五名资产。 脆弱性资产包括“风险预防 > 漏洞管理”中受漏洞影响的资产、“风险预防 > 基线检查”中包含检查不通过项的资产、“资产管理”中未开启防护的资产相加的总数，按照部门进行统计后取的前五名。其中，资产须在“资产管理”页面中的部门信息不为空的资产。

TOP5 部门未防护统计

呈现TOP5的部门未覆盖防护策略情况，包括部门的名称、未覆盖策略数、DBSS、WAF、DDoS、HSS、CFW。

TOP5是从部门索引取值，按未防护资产数降序排序。

表 6-26 部门未防护统计

参数名称	统计周期	更新频率	说明
Top5 部门未防护统计	实时	每小时	不同部门未开启安全防护的资产，将其未开启的安全服务进行统计计数。将总数按从多到少排列，取前5名。

漏洞修复率

展示漏洞修复率、TOP5 漏洞类型分布情况和漏洞趋势变化情况。

表 6-27 漏洞修复率

参数名称	统计周期	更新频率	说明
漏洞修复率	实时	每小时	漏洞修复率 =（已修复漏洞数 / 漏洞总数）* 100%。 如果不存在漏洞，则全部显示为100%。
漏洞类型分布	实时	每小时	漏洞按照漏洞的类型进行统计。
漏洞趋势变化	近7天	每小时	近7天的漏洞按照严重程度进行分类计数。

基线检查通过率

呈现基线检查通过率、基线自动检查不通过资源统计情况、基线检查不通过类型及其数量、基线检查总数等。

表 6-28 基线检查通过率

参数名称	统计周期	更新频率	说明
基线检查通过率	实时	每小时	基线检查通过率 =（基线检查合格项 / 总检查项）* 100%。
基线自动检查不通过资源统计	实时	每小时	基线检查不合格项，按照严重程度统计其影响的资源数。
基线检查	实时	每小时	基线检查合格、不合格、失败数量统计。

6.3 安全报告

6.3.1 创建/复制安全报告

操作场景

安全云脑提供安全报告功能。您可以通过创建安全报告，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

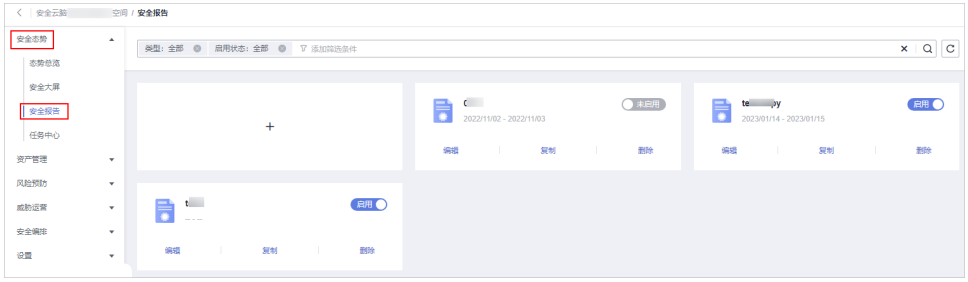
步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“安全态势 > 安全报告”，进入安全报告页面。

图 6-1 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 6-29 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。

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。
报告周期	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：报告选择”，进入报告选择页面。

步骤8 在“报告选择”页面的左侧已有报告布局中，根据报告类型选择报告布局。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；如果选择的是“周报”，此处请选择周报布局；如果选择的是“月报”，此处请选择月报布局。

- 下载报告：单击报告预览页面左上角的  ，并在弹出的对话框中，选择报告格式，单击“确定”。

  系统将自动下载对应格式的报告到本地。

- 全屏查看报告：单击报告预览页面左上角的  ，可以全屏查看安全报告。

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。

----结束

复制安全报告

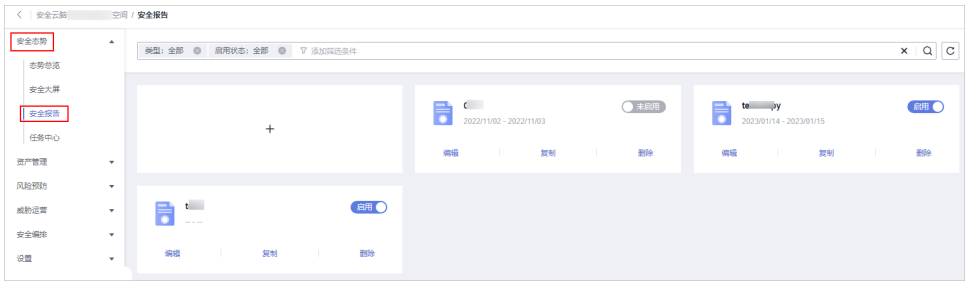
步骤1 登录管理控制台。

步骤2 单击页面左上方的  ，选择“安全 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“安全态势 > 安全报告”，进入安全报告页面。

图 6-2 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 单击右上角“下一步：报告选择”，进入报告选择配置页面，修改报告内容。

- 下载报告：单击报告预览页面左上角的，并在弹出的对话框中，选择报告格式，单击“确定”。
  系统将自动下载对应格式的报告到本地。
- 全屏查看报告：单击报告预览页面左上角的，可以全屏查看安全报告。

步骤8 单击右上角“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

6.3.2 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。

操作步骤

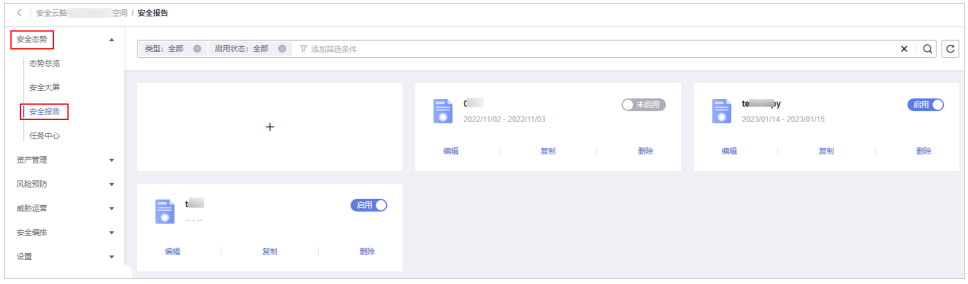
步骤1 登录管理控制台。

步骤2 单击页面左上方的，选择“安全 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“安全态势 > 安全报告”，进入安全报告页面。

图 6-3 进入安全报告页面



步骤5 选择目标报告，单击报告图标，跳转到报告详情页面。

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 6-30 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。
安全评分	根据您的安全云脑的威胁检测能力，评估前一天00:00:00~23:59:59整体资产安全健康得分，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： ● 当前基线检查项目总数量 ● 最近一次基线检查不合规检查项目数量
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
策略覆盖	展示当前安全产品覆盖情况，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） ● 主机安全覆盖率（=受保护ECS数量/全部ECS数量） ● 当前受保护云主机数量 ● 当前受保护网站数量
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
安全响应（总览）	展示**前一天**安全响应情况，包含以下信息： ● 前一天处置的安全告警数量 ● 前一天确认的入侵事件数量 ● 前一天运行的自动化响应剧本数量 ● 前一天自动化剧本闭环率 ● 前一天的MTTR平均时间 ● 前一天确认高风险入侵事件数量

参数模块	参数说明
资产风险	展示**前一天**资产安全状况，包含以下信息： ● 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巡检情况 ● 前一天网络主机攻击变化趋势 ● 前一天WAF巡检情况 ● 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 ● 前一天主机安全巡检情况
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**的日志变化趋势 ● 截至昨天为止的**近7天**的TOP5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： ● 前一天已处理告警数量 ● 前一天已处理事件数量 ● 前一天已处理漏洞数量 ● 前一天已处理基线数量 ● 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应急响应统计情况 ● 前一天TOP20威胁告警处理情况
外部安全热点	展示**前一天**外部安全热点的情况。

模板周报展示内容

表 6-31 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。
安全评分	根据您的安全云脑的威胁检测能力，评估上周最后一天最新的整体资产安全健康得分，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： ● 当前基线检查项目总数量 ● 最后一次基线检查不合规检查项数量
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
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： ● 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） ● 主机安全覆盖率（=受保护ECS数量/全部ECS数量） ● 当前受保护云主机数量 ● 当前受保护网站数量

参数模块	参数说明
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： ● 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
安全响应（总览）	展示上周一整周安全响应情况，包含以下信息： ● 上周一整周已处置的安全告警数量 ● 上周一整周确认的入侵事件数量 ● 运行的自动化响应剧本数量 ● 自动化剧本闭环率 ● MTTR平均时间 ● 确认高风险入侵事件数量
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 ● 资产防护率
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巡检情况 ● 网络攻击变化趋势 ● 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 ● TOP主机告警分布情况 ● TOP5网络攻击源分布情况 ● 主机安全巡检情况

参数模块	参数说明
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 ● TOP5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： ● 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
外部安全热点	展示外部安全热点的情况。

模板月报展示内容

表 6-32 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。
安全评分	根据您的安全云脑的威胁检测能力，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： ● 当前基线检查项目总数量 ● 最后一次基线检查不合规检查项数量
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： ● 漏洞总数量 ● 未修复漏洞数量

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） ● 主机安全覆盖率（=受保护ECS数量/全部ECS数量） ● 当前受保护云主机数量 ● 当前受保护网站数量
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
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： ● 上一个月整月已处置的安全告警数量 ● 上一个月整月确认的入侵事件数量 ● 运行的自动化响应剧本数量 ● 自动化剧本闭环率 ● MTTR平均时间 ● 确认高风险入侵事件数量
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 ● 资产防护率

参数模块	参数说明
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巡检情况 ● 网络攻击变化趋势 ● 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 ● TOP主机告警分布情况 ● TOP5网络攻击源分布情况 ● 主机安全巡检情况
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 ● TOP5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
外部安全热点	展示外部安全热点的情况。

6.3.3 下载安全报告

操作场景

安全云脑创建并生成报告后，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。

操作步骤

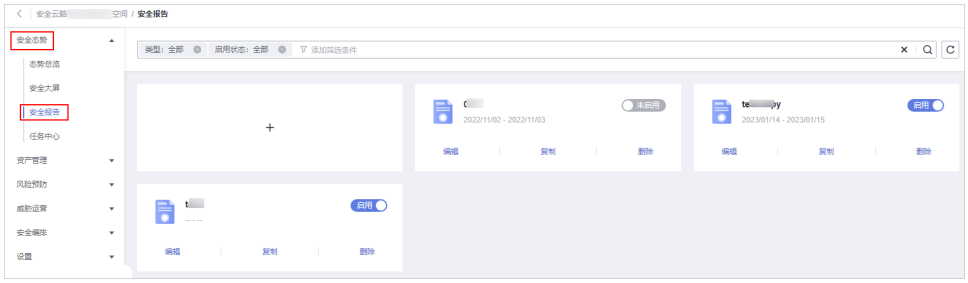
步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“安全态势 > 安全报告”，进入安全报告页面。

图 6-4 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“编辑”，进入报告基本信息配置页面。

创建/复制安全报告时，也可以下载报告，具体操作请参见**创建/复制安全报告**。

步骤6 单击右上角“下一步：报告选择”，进入报告选择配置页面。

步骤7 在报告选择页面，单击右侧预览页面左上角的  。

如需修改报告数据周期，可以在右侧预览页面右上角进行编辑。

步骤8 在弹出的下载对话框中，选择报告格式，并单击“确定”。

系统将自动下载对应格式的报告到本地。

----结束

6.3.4 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。

操作步骤

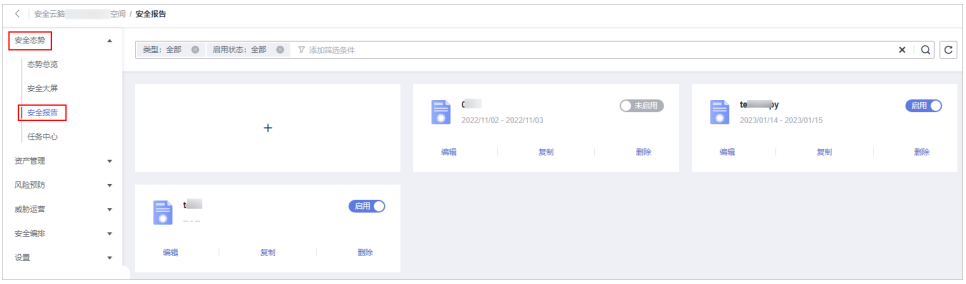
步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“安全态势 > 安全报告”，进入安全报告页面。

图 6-5 进入安全报告页面



步骤5 管理安全报告。

表 6-33 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，单击目标报告模块中的“编辑”，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”，返回安全报告管理页面。
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”，返回安全报告管理页面。

----结束

6.4 任务中心

6.4.1 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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“安全态势 > 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 6-34 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。
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

6.4.2 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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“安全态势 > 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”。

----结束

6.4.3 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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“安全态势 > 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。

当已处理任务较多时，可以通过搜索功能，选择搜索条件并在搜索框中输入关键词后按“Enter”，即可快速查询指定任务。

表 6-35 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。
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 资产管理

7.1 资产管理概述

安全云脑支持对云上资产全面自动盘点，也可灵活纳管云外各种资产，点清所有资产，并呈现资产实时安全状态。

在资产管理中，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，包括资源的名称、所属服务、安全状况等，帮助您快速定位安全风险问题并提供解决方案。

7.2 设置资产订阅

操作场景

安全云脑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进行更新。

本章节介绍如何订阅资产。

说明

- 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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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进行更新。

----结束

7.3 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。

前提条件

- 已完成资产订阅，详细操作请参见**设置资产订阅**。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

安全云脑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进行更新。

说明

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。
- 当资产较多时，可以通过搜索功能，可快速查询指定资产。

  如果需要查看某个企业项目对应的资产信息，选择企业项目名称进行筛选，查询指定资产信息。

- 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

相关操作

在资产管理页面可以对资产的部门、业务系统、责任人进行编辑。操作步骤如下：

1. 勾选需要编辑的资产，并单击资产列表左上角“批量编辑”。
2. 在弹出的资产编辑框中，编辑资产信息。
3. 单击“确认”。

7.4 导入/导出资产

操作场景

安全云脑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。

本章节介绍如何导入/导出资产。

约束与限制

- 仅支持导入.xlsx格式的文件，且单次导入文件大小不超过5MB。
- 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。例如，需要导入主机资产，则选择“主机资产”页签。

步骤6 在资产列表左上方，单击“导入”，弹出导入资产对话框。

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。

步骤8 待导入资产文件信息填写完成后，在导入资产对话框中，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。

----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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

步骤7 在导出资产对话框中，配置参数。

表 7-1 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

7.5 编辑/删除资产

操作场景

在资产管理页面可以对资产的部门、业务系统、责任人进行编辑。另外，如果不再需要在安全云脑资产管理页面展示某个/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/删除资产。

约束与限制

仅支持删除云下导入的资产。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 7-2 编辑或删除资产

操作	执行步骤
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，对资产的部门、业务系统、责任人进行编辑。 3. 编辑完成后，单击“确认”。
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，勾选您需要删除的资产，并单击列表上方的“批量删除”。 系统将删除已勾选资产。

----结束

8 风险预防

8.1 基线检查

8.1.1 基线检查概述

安全云脑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

  SecMaster默认每隔3天检查一次，每次在00:00~06:00对您账号下当前region所有资产按照“安全上云合规检查1.0”遵从包进行检查。

  同时，您还可以自定义自动检测周期及时间，详细操作请参见**新增自定义检查计划**。

- 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。

使用流程

表 8-1 使用流程

序号	操作项	说明
1	（可选）**新增自定义检查计划**	安全云脑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所有资产进行检查。 • 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。

序号	操作项	说明
2	（可选）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。

8.1.2 新增自定义检查计划

操作场景

安全云脑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所有资产按照“安全上云合规检查1.0”遵从包自动执行基线检查。另外，您还可以自定义自动检测周期及时间。

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”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。
- 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 8-2 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。
	检查时间	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		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，安全云脑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。

- 查看已有检查计划
  a. 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。
  b. 在检查计划页面中，查看已有的基线检查计划。
- 编辑自定义检查计划

  仅支持修改用户自定义创建的检查计划。
  a. 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。
  b. 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。
  c. 编辑需要修改的计划参数后，单击“确定”。
- 删除自定义检查计划

  仅支持删除用户自定义创建的检查计划。
  a. 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。
  b. 在目标计划所在框的右上角单击“删除”。
  c. 在弹出的对话框中，单击“确定”。
- 关闭或开启检查计划

a. 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。
b. 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。

8.1.3 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：根据安全云脑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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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”，默认进入检查结果管理页面。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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”，默认进入检查结果管理页面。

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

8.1.4 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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 数据集成”，进入数据集成页面后，在**安全云脑**所在行“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”，默认进入检查结果管理页面。

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8-3**所示。

表 8-3 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的后，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。
检查项合格率	最近一次执行基线检查的基线合格率。 整体合格率=合格检查项数量/检查项总数。合格率的统计范围为全部规范的全部检查项目。 检查项结果分为合格、不合格、检查失败几种。
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。 ● 当检查项较多时，可以通过搜索功能，选择搜索类型并按“Enter”，即可快速查询指定检查项。 ● 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

8.1.5 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：

- **修复风险项**：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。
- **忽略检查项**：如果您对某个检查项有其他检查要求（例如，“会话超时策略检查”检查项中检查会话时限是否设置为15分钟，而您的需求为会话时限是否设置为20分钟）或不需要对某检查项进行检查，可以执行忽略操作。
- **导入检查结果**：将线上检查结果导出至本地。
- **导出检查结果**：将线下检查结果数据信息导入至安全云脑基线检查中。

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。

前提条件

- 已扫描云服务基线。

修复风险项

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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”，默认进入检查结果管理页面。

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，并根据检查资源的“加固建议”进行修复。

修复所有存在风险的配置后，可单击“立即检查”，确认风险项是否已修复。

----结束

反馈检查结果

安全云脑的基线检查项中的**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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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”，默认进入检查结果管理页面。

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”。

说明

反馈结果有效期为7天，7天后请重新手动检查。

----结束

忽略检查项

如果您对某个检查项有其他检查要求（例如，SecMaster的“会话超时策略检查”检查项中检查会话时限是否设置为15分钟，而您的需求为会话时限是否设置为20分钟）或不需要对某检查项进行检查，可以执行忽略操作。

忽略后，再次检查时，将不再对已忽略检查项进行检查，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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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”的“忽略”。

步骤7 在弹出的确认框中，单击“确定”。

说明

- 忽略后，再次执行检查时，将不再对已忽略检查项进行检查，且“检查项合格率”中，也将不再纳入计算中。
- 忽略后，如需再次检查该检查项目，在待取消忽略检查项的“操作”列单击“取消忽略”，并在弹出的确认框单击“确定”。

----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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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”，默认进入检查结果管理页面。

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。

说明

- 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”。

----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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“确定”。

----结束

8.1.6 查看已有遵从包

本章节介绍如何查看已有的安全遵从包。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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8-4所示。

表 8-4 查看已有遵从包

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。遵从包状态包含启用和未启用两种。
内置遵从包数量	安全云脑内置的遵从包数量。
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。 • 当遵从包较多时，可以通过搜索功能，选择搜索类型并按“Enter”，即可快速查询指定遵从包。 • 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

8.1.7 添加自定义遵从包

本章节介绍如何自定义添加安全遵从包。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 8-5 配置基础信息

参数名称	参数说明
遵从包名称	自定义遵从包名称。

参数名称		参数说明
描述		自定义遵从包描述信息。
（可选）高级配置	版本	设置遵从包版本。
	分类	填写遵从包所属分类。
	领域	填写遵从包所属领域。
	责任人	设置遵从包责任人。
	适用区域	填写遵从包使用区域。

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，并单击添加按钮，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”。

----结束

相关操作

- 停用遵从包
  a. 在待停用遵从包所在行“操作”列，单击“停用”。
  b. 在弹出的确认框中单击“确定”。
- 启用遵从包
  a. 在待启用遵从包所在行“操作”列，单击“启用”。
  b. 在弹出的确认框中单击“确定”。
- 编辑检查项
  a. 在待编辑遵从包名称进入遵从包详情页面。
  b. 在遵从包内容栏中“编辑”。
  c. 编辑节点信息或绑定的检查项后，单击“确认”。
- 删除遵从包
  a. 在待删除遵从包所在行“操作”列，单击“删除”。
  b. 在弹出确认框中输入“DELETE”后，单击“确定”。

8.1.8 导入/导出遵从包

操作场景

本章节介绍如何导入、导出遵从包。

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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

说明

- 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”。

----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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

8.1.9 查看已有检查项

本章节介绍如何查看已有检查项。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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8-6所示。

表 8-6 查看已有检查项

参数名称	参数说明
检查项总数	当前工作空间内容，检查项的总数量。
内置检查项数量	安全云脑内置的检查项数量。
自定义检查项数量	用户自定义新增的检查项数量
检查项及其详细信息	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。 • 当检查项较多时，可以通过搜索功能，选择搜索类型并按“Enter”，即可快速查询指定检查项。 • 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、遵从包引用情况等信息。

----结束

8.1.10 创建自定义检查项

章节介绍如何自定义创建检查项。

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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 8-7 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。
描述	自定义检查项描述信息。
等级	选择此检查项的等级。
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。 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。

步骤7 单击“确定”。

说明

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。

----结束

相关操作

- 编辑检查项
  a. 在待编辑检查项所在行“操作”列，单击“编辑”。
  b. 在编辑检查项页面中，修改检查项参数后，单击“确定”。
- 删除检查项
  a. 在待删除检查项所在行“操作”列，单击“删除”。
  b. 在弹出确认框中输入“DELETE”后，单击“确定”。

8.1.11 导入/导出检查项

操作场景

本章节介绍如何导入、导出检查项。

约束与限制

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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

说明

- 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”。

----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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

8.2 漏洞管理

8.2.1 漏洞管理概述

背景介绍

安全云脑通过集成企业主机安全（Host Security Service，HSS）漏洞扫描数据，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。

主机漏洞

安全云脑支持接入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。

主机漏洞共支持以下漏洞项的检测：

表 8-8 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）是否存在的漏洞，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，并推送微软官方补丁，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。
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，安全云脑中漏洞的等级和HSS中修复优先级的说明如下：

- HSS：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。

- SecMaster：显示漏洞的等级，等级是根据漏洞最高CVSS分值得出的，反应漏洞的严重程度。

  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。

8.2.2 查看漏洞详情

操作场景

本章节介绍如何查看漏洞的详细信息。

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**数据集成**。如果数据集成操作时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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 在安全云脑管理页面选择“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。

表 8-9 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。
漏洞TOP5排行	• TOP5是根据受漏洞影响的资产数量的多少来进行排序，影响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TOP5的风险资产。

参数名称	参数说明
漏洞列表	• 在下方漏洞列表中，选择“Linux漏洞”、“Windows漏洞”、“Web-CMS漏洞”、“应用漏洞”任意一个页签，进入对应漏洞列表管理页面，漏洞列表参数信息说明请参见表8-10。 • 当漏洞较多时，可以通过搜索功能，可快速查询指定漏洞。 • 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 8-10 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。
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	该漏洞是否已处理。

----结束

8.2.3 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，您可以在企业主机安全控制台一键自动修复漏洞，对于Web-CMS漏洞、应用漏洞、应急漏洞，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》。

- 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”。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 在安全云脑管理页面选择“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，选择“受影响资产”页签，并在资产列表中，单击待处理资产所在行“操作”列的“修复”，系统提示修复操作触发成功。

如需批量修复，可以勾选所有需要修复的资产，然后在列表左上角，单击“批量修复”。

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”。

说明

“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8-11**。

说明

- “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 8-11 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*
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。

  说明

  - 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 8-12 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*
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。

8.2.4 导入/导出漏洞

操作场景

本章节介绍如何导入、导出漏洞。

- 导入漏洞
- 导出漏洞

约束与限制

- 仅支持导入.xlsx格式的文件，且文件大小不超过5MB。
- 安全云脑最多支持导出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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 在安全云脑管理页面选择“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。

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“确认”，完成导入。

----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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 在安全云脑管理页面选择“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。

步骤7 在导出漏洞对话框中，配置漏洞参数。

表 8-13 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

8.2.5 忽略/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，安全云脑也将同步漏洞信息。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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 在安全云脑管理页面选择“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，选择“受影响资产”页签，并在资产列表中，单击待处理资产所在行“操作”列的“更多 > 忽略”。

- 取消忽略

  a. 在漏洞信息页面中，选择“受影响资产”页签，并在资产列表中，单击待处理资产所在行“操作”列的“更多 > 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

8.3 策略管理

8.3.1 策略管理概述

安全云脑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。

约束与限制

- 应急策略目前仅支持VPC安全组/WAF的黑名单策略。
- 单用户单工作空间内容最多新增300条支持阻断老化的应急策略，全量最多新增1300条应急策略。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WAF时，单用户单次最多可新增50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20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，VPC/WAF将不会做任何检测，直接拦截。

8.3.2 新增/编辑应急策略

操作场景

应急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/编辑应急策略。

约束与限制

- 单用户单工作空间内容最多新增300条支持阻断老化的应急策略，全量最多新增1300条应急策略。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WAF时，单用户单次最多可新增50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20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，VPC/WAF将不会做任何检测，直接拦截。
- 应急策略新增成功后，**不支持**修改阻断对象（即新增时设置的IP地址或IP地址段）。

新增应急策略

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，进入应急策略管理页面。

步骤5 在应急策略管理页面中，单击“新增”，右侧弹出新增应急策略页面。

步骤6 在新增策略页面中，配置策略信息。

表 8-14 新增应急策略

参数名称	参数说明
阻断对象类型	选择阻断对象的类型，可选择IP。
阻断对象	• 当阻断对象类型选择IP时，输入需要阻断的单个（或多个）IP地址或IP地址段，如有多个IP地址或地址段，请使用英文逗号隔开。 • 单次下发应急策略阻断对象说明如下： – 当需要下发策略至WAF时，单用户单次最多可新增50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20个IP作为阻断对象。
标签	自定义应急策略的标签。
操作连接	操作七层防线中安全服务的阻断流程所绑定的资产连接。 选择该策略的操作连接。

参数名称	参数说明
阻断老化	确认是否老化该条阻断。 • 如果选择是，请设置策略老化时间，如设置为180天，即该策略在设置后的180天内有效，180天后将不再继续阻断设置的IP地址或IP地址段。 • 如果选择否，则该策略将一直有效，阻断设置的IP地址或IP地址段。
策略描述	自定义该策略的描述信息。

步骤7 单击“确定”。

----结束

编辑应急策略

说明

应急策略新增成功后，**不支持**修改阻断对象（即新增时设置的IP地址或IP地址段）。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，进入应急策略管理页面。

步骤5 在应急策略管理页面中，单击待修改策略所在行“操作”列的“编辑”，右侧弹出编辑应急策略页面。

步骤6 在编辑策略页面中，修改策略信息。

表 8-15 编辑应急策略

参数名称	参数说明
阻断对象类型	应急策略新增成功后，**不支持修改**。
阻断对象	应急策略新增成功后，**不支持修改**。
标签	自定义应急策略的标签。
操作连接	选择该策略的操作连接。

参数名称	参数说明
阻断老化	确认是否老化该条阻断。 ● 如果选择是，请设置策略老化时间，如设置为180天，即该策略在设置后的180天内有效，180天后将不再继续阻断设置的IP地址或IP地址段。 ● 如果选择否，则该策略将一直有效，阻断设置的IP地址或IP地址段。
策略描述	自定义该策略的描述信息。

步骤7 单击“确定”。

----结束

8.3.3 查看应急策略

操作场景

本章节介绍如何查看已有应急策略。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，进入应急策略管理页面。

步骤5 在应急策略管理页面上方中，查看应急策略统计情况。

- 策略下发数量：策略下发到各个云产品的数量统计情况。
- 操作连接TOP3：策略封堵的操作链接TOP3统计情况及其封堵个数。
- 阻断区域TOP5：策略封堵对象所在的区域TOP5统计及其分布情况。

步骤6 在策略列表中，查看应急策略的相关信息，参数说明下所示：

表 8-16 查看应急策略

参数名称	参数说明
阻断对象	阻断的单个（或多个）IP地址或IP地址段。
标签	策略的标签信息。
策略下发数量	策略在产品中下发的数量。
阻断类型	策略所属的阻断类型。

参数名称	参数说明
创建人	策略的创建人信息。
原因描述	策略的描述信息。
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。

步骤7 如需查看某个应急策略的详细信息，可以选中需查看的策略，并单击页面下方“已选择：xxx”，将显示目标策略的详细信息。

在详细信息页面中，可以对策略进行阻断、取消阻断、删除操作，还可以查看策略的历史记录。

----结束

8.3.4 删除应急策略

操作场景

本章节介绍删除/批量删除应急策略。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，进入应急策略管理页面。

步骤5 在应急策略管理页面中，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”。

----结束

8.3.5 批量阻断/批量取消阻断

操作场景

新增阻断时将设置某个IP地址或IP地址段，如果该阻断也适用于其他操作连接，可以进行批量阻断操作。同时，配置阻断时将设置某个IP地址或IP地址段，如果该阻断已不适用，可以进行批量取消阻断操作。

本章节介绍如何执行批量阻断、批量取消阻断操作。

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，VPC将不会做任何检测，直接拦截。

批量阻断

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，进入应急策略管理页面。

步骤5 在应急策略管理页面中，单击待阻断策略所在行“操作”列的“批量阻断”。

步骤6 在弹出的批量阻断对话框中，输入阻断原因，并单击“确定”。

----结束

批量取消阻断

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，进入应急策略管理页面。

步骤5 在应急策略管理页面中，单击待取消阻断策略所在行“操作”列的“批量取消阻断”。

步骤6 在弹出的取消阻断对话框中，输入取消阻断原因，并单击“确定”。

----结束

9 威胁运营

9.1 事件管理

9.1.1 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。

在安全云脑的事件管理页面，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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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。

图 9-1 查看事件信息

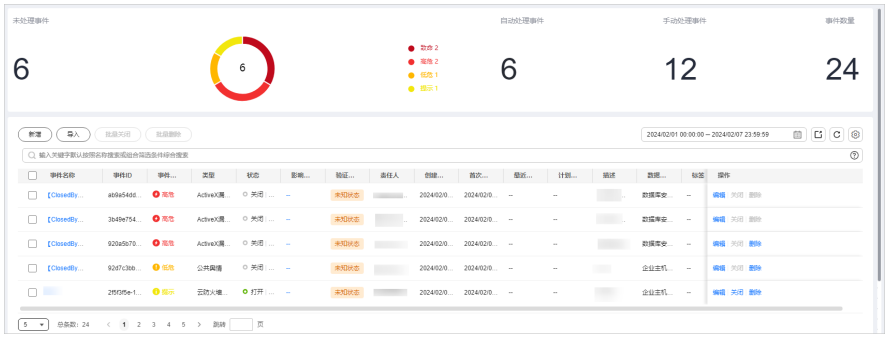


表 9-1 查看事件信息

参数名称	参数说明
未处理事件	当前工作空间在设定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	当前工作空间在设定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	当前工作空间在设定的时间范围内手动处理的事件数量。
事件数量	当前工作空间在设定的时间范围内的事件总数量。
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。 ● 在事件概览页面可以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/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

9.1.2 新增/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

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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9-2所示。

表 9-2 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255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。
	状态	选择事件状态。
	（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	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。

参数名称		参数说明
	（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。 ● 事件后活动：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。
	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1024个字符。

步骤6 单击“确认”，完成事件创建。

----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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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 9-3 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255个字符。
	事件类型	选择事件类型。

参数名称		参数说明
	（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。
	状态	选择事件状态。
	（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。
	（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。 ● 事件后活动：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，**不支持修改**。
	（可选）标签	填写事件的标签。
	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1024个字符。

步骤7 单击“确认”，完成事件编辑。

----结束

9.1.3 导入/导出事件

操作场景

本章节主要介绍如何导入、导出事件。

约束与限制

- 仅支持导入.xlsx格式的文件，且文件大小不超过5MB。

- 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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”。

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。

----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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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。

步骤6 在导出事件对话框中，配置参数。

表 9-4 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

9.1.4 关闭/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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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 9-5 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”。
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”。 **说明** 事件删除后将无法恢复，请谨慎操作。

----结束

9.2 告警管理

9.2.1 查看告警信息

操作场景

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，以便他们能够迅速响应并采取措施解决问题。

当安全云脑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安全云脑告警管理界面中。

在安全云脑的告警管理页面，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。

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“数据集成”页面中开启“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**接入数据**。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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 9-6 查看告警信息

参数名称	参数说明
设置告警的显示时间范围	右上角可设置展示告警的周期，默认展示本周内告警信息。
未处理告警	当前工作空间在设定的时间范围内未处理告警的数量及其所属等级分布情况。
自动处理告警	当前工作空间在设定的时间范围内通过剧本自动处理的告警数量。
手动处理告警	当前工作空间在设定的时间范围内手动处理的告警数量。
告警总数	当前工作空间在设定的时间范围内告警总数量。

参数名称	参数说明
告警列表	展示告警的详细信息。 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、摘要、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。 ● 在告警详情页面中，可以对该条告警进行评论、一键解封、一键阻断、转事件、关闭、删除、刷新操作。 ● 在告警详情页面可以查看告警的总览、上下文、关系图和评论信息。 – 总览：展示该条告警的摘要、处理建议、基础信息、请求详情等信息。 – 上下文：通过JSON和表格两种方式展示该条告警的上下文关键信息和全文信息。 – 关系图：展示该条告警的关联信息，例如关联的告警、事件、情报和受影响的资产信息。 – 评论：展示该条告警的历史评论信息，还可以新增评论。

----结束

9.2.2 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 9-7 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，以便他们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 9-8 告警转事件或关联事件的原因

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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，单击页面右上角的“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“事件类型”。

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”。

----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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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“关系图 > 关联事件**”页签，查看关联信息。**

----结束

9.2.3 新增/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

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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**表9-9**所示。

表 9-9 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255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。
	状态	选择告警状态，可选择以下状态：打开、阻塞、关闭。
	（可选）责任人	选择告警的主要责任人。
	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。
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）确认状态	选择告警的确认状态，标识告警的准确性。可选择以下状态：未知状态、攻击成功、关闭攻击。
	（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。 ● 事件后活动：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1024个字符。

步骤6 单击“确认”。

----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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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 > 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，参数说明如表9-10所示。

表 9-10 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255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。
	状态	选择告警状态，可选择以下状态：打开、阻塞、关闭。
	（可选）责任人	选择告警的主要责任人。
	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。
其他	标签	填写告警的标签。

参数名称		参数说明
	调试数据	选择是否开启模拟调试功能，**不支持修改**。
	确认状态	选择告警的确认状态，标识告警的准确性。可选择以下状态：未知状态、攻击成功、关闭攻击。
	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。 ● 事件后活动：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1024个字符。

步骤7 单击“确认”。

----结束

9.2.4 导入/导出告警

操作场景

本章节主要介绍如何导入、导出告警。

约束与限制

- 仅支持导入.xlsx格式的文件，且文件大小不超过5MB。
- 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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”。

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。

----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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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。

步骤6 在导出告警对话框中，配置参数。

表 9-11 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

9.2.5 关闭/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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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 9-12 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”。
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”。 **说明** 告警删除后将无法恢复，请谨慎操作。

----结束

9.2.6 一键阻断/解封

操作场景

应急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。

本章节介绍如何执行一键阻断和一键解封操作。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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，单击页面右上角的“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 9-13 一键阻断

参数名称	参数说明
阻断对象	• 当阻断对象类型选择IP时，输入需要阻断的单个（或多个）IP地址或IP地址段，如有多个IP地址或地址段，请使用英文逗号隔开。 • 单次下发应急策略阻断对象说明如下： – 当需要下发策略至WAF时，单用户单次最多可新增50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20个IP作为阻断对象。
标签	自定义阻断策略的标签。
操作连接	选择该阻断策略的操作连接。
阻断老化	确认是否老化该条阻断策略。 • 如果选择是，请设置策略老化时间，如设置为180天，即该策略在设置后的180天内有效，180天后将不再继续阻断设置的IP地址或IP地址段。 • 如果选择否，则该策略将一直有效，阻断设置的IP地址或IP地址段。
策略描述	自定义该阻断策略的描述信息。

步骤7 确认配置无误后，单击“确定”，并在弹出的提示框中，单击“确认”。

----结束

一键解封

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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

9.3 情报管理

9.3.1 新增/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

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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 9-14 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。
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。
状态	选择指标状态，可选择以下状态：打开、关闭、作废。
（可选）置信度	填选指标的可信度，范围为80~100。
（可选）责任人	选择该条指标的主要责任人。
（可选）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。

参数	说明
（可选）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，可选择以下粒度：首次发现、自产数据、需购买、外网直接查询。
其他参数	根据选择的不同类型，还需要配置对应的参数信息，请根据界面显示进行填写。 例如，当“类型”选择“ipv6”时，还需要配置IP地址、邮箱账户、地区等信息。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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 9-15 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**。

参数	说明
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。
最近发现时间	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，可选择以下粒度：首次发现、自产数据、需购买、外网直接查询。
其他参数	根据选择的不同类型，还需要配置对应的参数信息，请根据界面显示进行填写。 例如，当“类型”选择“ipv6”时，还需要配置IP地址、邮箱账户、地区等信息。

步骤7 单击“确认”。

----结束

9.3.2 关闭/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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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 9-16 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”。
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

9.3.3 导入/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。

约束与限制

- 仅支持导入.xlsx格式的文件，且文件大小不超过5MB。
- 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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”。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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。

步骤6 在导出指标对话框中，配置参数。

表 9-17 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

9.3.4 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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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 9-18 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。
威胁度	呈现不同威胁程度对应的情报指标数量。
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

9.4 智能建模

9.4.1 查看已有模板

操作场景

安全云脑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，需利用已有模板创建模型。

本章节介绍如何查看已有模型模板。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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 9-19 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。
严重程度	显示当前已有模板的严重程度统计情况，包含致命、高危、中危、低危、提示级别。
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

9.4.2 新建/编辑模型

操作场景

安全云脑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。

本章节将介绍如何创建并编辑告警模型。

- 使用已有模板创建告警模型
- 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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9-20**所示。

表 9-20 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。
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。
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9-21**所示。

表 9-21 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-SQL语法**。 **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。

参数名称	参数说明
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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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9-22所示。

表 9-22 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。
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。
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9-23所示。

表 9-23 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。 语法参考请参见查询与分析语法-SQL语法。
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。

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，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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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9-24所示。

表 9-24 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。

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	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9-25所示。

表 9-25 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-SQL语法**。 **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

9.4.3 查看已有模型

操作场景

本章节将介绍如何查看已新增的模型。

前提条件

已新增模型，详细操作请参见**新建/编辑模型**。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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 9-26 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

9.4.4 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、删除模型等操作。

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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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 9-27 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。

操作	操作说明
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

9.5 安全分析

9.5.1 安全分析概述

安全云脑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

安全云脑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**支持接入的日志**。

9.5.2 使用流程

安全分析功能使用具体流程如**表9-28**所示。

表 9-28 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。
数据集成	配置需要接入的数据源。 安全云脑支持集成存储、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。

子流程	说明
（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。
图表统计查询分析结果	当您执行了查询分析语句后，安全云脑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。

9.5.3 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 9-29 通用字段

字段名	字段类型	字段含义
__time	Date	日志产生的时间

字段名	字段类型	字段含义
__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
[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

字段名	字段类型	字段含义
[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 9-30 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。
attack_stream_id	String	与group_id相关，是日志组下用户的access_stream的ID。

字段		类型	字段含义
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9-31所示。

表 9-31 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。
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。

字段	类型	字段含义
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 9-32 sec-obs-access

字段	类型	字段含义
srcip	String	访问obs的源ip。

字段	类型	字段含义
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。
http_version	String	http版本。
host	String	服务obs域名。
port	String	端口。

字段	类型	字段含义
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
access_key	String	ak。

sec-nip-attack

IPS攻击日志字段含义如下所示：

表 9-33 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。
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。

字段	类型	字段含义
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 9-34 sec-iam-audit

字段	类型	字段含义
uid	String	用户id。
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。

字段	类型	字段含义
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 9-35 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。
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	受影响租户ID。
enterpriseProjectId		String	受影响企业租户ID。
appendInfo		Object	漏洞详情。
appendInfo	vulId	String	漏洞官方ID。

字段		类型	字段含义
	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。
	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。

字段		类型	字段含义
	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 9-36 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。
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	受影响租户ID。
enterpriseProjectId		String	受影响企业租户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。

字段			类型	字段含义
	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。
	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。

字段			类型	字段含义
		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。
		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。

字段			类型	字段含义
		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。
		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。

字段			类型	字段含义
		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。
		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。

字段			类型	字段含义
		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。
		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。

字段			类型	字段含义
		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。
		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。

字段			类型	字段含义
		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。
		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。

字段			类型	字段含义
		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 9-37 sec-hss-log

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。

字段		类型	字段含义
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	受影响租户ID。
enterpriseProjectId		String	受影响企业租户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。

字段			类型	字段含义
	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。
		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。

字段			类型	字段含义
		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。
		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。

字段			类型	字段含义
		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。
		parent_process_cmdline	String	父进程文件命令行。

字段			类型	字段含义
		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_last time	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。

字段			类型	字段含义
	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。
		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。

字段			类型	字段含义
	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。
		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。

字段			类型	字段含义
		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-ddos-attack

DDoS攻击日志字段含义如下所示：

表 9-38 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。

字段	类型	字段含义
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。
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。

字段	类型	字段含义
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。
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 9-39 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。

字段	类型	字段含义
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。
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 9-40 sec-cfw-risk

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 9-41 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。
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 9-42 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 9-43 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。
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。

字段	类型	字段含义
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 9-44 dbss-alarm

字段	类型	字段含义
domain_id	String	账号ID。
project_id	String	项目ID。
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。

字段		类型	字段含义
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 9-45 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。
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。

字段	类型	字段含义
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 9-46 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。
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 9-47 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。
keyword	String	匹配敏感数据规则关键字。

9.5.4 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

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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9-48**所示。

表 9-48 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。
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

9.5.5 查询与分析

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：

- **输入查询条件进行查询分析**
- **使用已有字段进行查询分析**
- **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**数据集成**。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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-SQL语法**。

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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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。

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。

- 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 。
- 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 。

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

操作查询分析结果

安全云脑通过**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。

- **原始日志**

  在“原始日志”页签将展示当前查询结果。

  - 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。
    - 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。
    - 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。
      - 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。

- 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。

- 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。

  图表统计是安全云脑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**图表统计概述**。

- **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**快速查询**。

9.5.6 下载日志

操作场景

安全云脑支持将原始日志或查询分析日志下载到本地。

前提条件

已完成数据接入，详细操作请参见**数据集成**。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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。

- 下载原始日志：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

9.5.7 查询与分析语法-SQL 语法

9.5.7.1 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 9-49 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。

9.5.7.2 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。

9.5.7.3 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 9-50 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 9-51 普通查询示例

查询需求	查询语句
查询所有日志	*
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

查询需求	查询语句
查询请求时间为60秒的日志。	request_time = 60

9.5.7.4 分析语句-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 9-52 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
18	Dale	M	Orick	4180	null	MD	Adams	32

查询指定字段

```
SELECT firstname, lastname
```

表 9-53 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 9-54 使用 AS 给字段定义别名

num
1
16
13
18

使用 DISTINCT 去重

```
SELECT DISTINCT age
```

表 9-55 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 9-56 使用 SQL 函数

len	firstname
4	Amber
6	Hattie
7	Nanette
4	Dale

9.5.7.5 分析语句-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 9-57 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 9-58 按字段别名分组

num
1
16
13
18

按多个字段分组

```
SELECT account_number AS num, age GROUP BY num, age
```

表 9-59 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 9-60 使用 SQL 函数

len	count
4	2
5	2

9.5.7.6 分析语句-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 9-61 HAVING

age	MAX(balance)
28	32838
32	39225

9.5.7.7 分析语句-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 9-62 使用字段值排序

age
28
32
32
36

9.5.7.8 分析语句-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 9-63 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 9-64 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

9.5.7.9 分析语句-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 9-65 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
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

函数	作用	定义	示例
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
/	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 9-66 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

函数	作用	定义	示例
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 9-67 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
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

函数	作用	定义	示例
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 9-68 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
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

函数	作用	定义	示例
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 9-69 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

9.5.7.10 分析语句-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 9-70 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

函数	作用	定义	示例
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

9.5.8 快速查询

操作场景

快速查询为安全云脑提供的用于保存查询分析操作的功能。您可以将某个常用的查询分析语句另存为快速查询，以便后续直接使用，快速执行查询分析操作。

本章节将介绍如何创建快速查询。

前提条件

已配置索引，详细操作请参见**配置索引**。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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**查询与分析**。

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 9-71 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

9.5.9 快速添加日志告警模型

操作场景

安全云脑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**数据集成**。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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**。

步骤7 单击页面右上角“添加告警”，进入新建告警模型页面。

步骤8 配置告警基础信息，参数说明如**表9-72**所示。

表 9-72 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。
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。

参数名称	参数说明
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9-73所示。

表 9-73 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-SQL语法**。 **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。

参数名称	参数说明
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

9.5.10 图表统计

9.5.10.1 图表统计概述

当您执行了查询和分析语句后，安全云脑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。

安全云脑可以通过以下图表类型展示查询和分析结果：

- **表格**
- **折线图**
- **柱状图**
- **饼图**

9.5.10.2 表格

查询分析结果可以通过表格形式进行展示。

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。在安全云脑中，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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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 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 。

步骤8 配置表格参数。

表 9-74 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。

----结束

相关操作

- 下载日志：配置后，如需导出当前查询分析数据，可单击表格右上角“下载日志”，系统将下载当前查询分析日志数据至本地。
- 收起配置：图表配置完成后，在“预览图表”右侧单击“收起配置”，页面将不显示图表配置参数。
- 展开配置：图标配置收起后，如需再次配置，可在“预览图表”右侧单击“展开配置”。

9.5.10.3 折线图

查询分析结果可以通过折线图形式进行展示。

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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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 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  。

步骤8 配置折线图参数。

表 9-75 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。
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。

----结束

相关操作

- 下载日志：配置后，如需导出当前查询分析数据，可单击表格右上角“下载日志”，系统将下载当前查询分析日志数据至本地。
- 收起配置：图表配置完成后，在“预览图表”右侧单击“收起配置”，页面将不显示图表配置参数。
- 展开配置：图标配置收起后，如需再次配置，可在“预览图表”右侧单击“展开配置”。

9.5.10.4 柱状图

查询分析结果可以通过柱状图形式进行展示。

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。安全云脑中，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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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 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。

步骤8 配置柱状图参数。

表 9-76 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。

----结束

相关操作

- 下载日志：配置后，如需导出当前查询分析数据，可单击表格右上角“下载日志”，系统将下载当前查询分析日志数据至本地。
- 收起配置：图表配置完成后，在“预览图表”右侧单击“收起配置”，页面将不显示图表配置参数。
- 展开配置：图标配置收起后，如需再次配置，可在“预览图表”右侧单击“展开配置”。

9.5.10.5 饼图

查询分析结果可以通过饼图形式进行展示。

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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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 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。

步骤8 配置饼图参数。

表 9-77 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

相关操作

- 下载日志：配置后，如需导出当前查询分析数据，可单击表格右上角“下载日志”，系统将下载当前查询分析日志数据至本地。
- 收起配置：图表配置完成后，在“预览图表”右侧单击“收起配置”，页面将不显示图表配置参数。

- 展开配置：图标配置收起后，如需再次配置，可在“预览图表”右侧单击“展开配置”。

9.5.11 管理数据空间

9.5.11.1 新增数据空间

操作场景

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载均衡策略。

当您需要使用安全云脑提供的**安全分析**、**数据分析**、**智能建模**等功能时，需要新增数据空间。

本章节介绍如何创建数据空间。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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。

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9-78所示。

表 9-78 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

9.5.11.2 查看数据空间详情

操作场景

该任务指导用户通过管理控制台查看数据空间的信息，包括名称、类型和创建时间等。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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9-79所示。

表 9-79 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。
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。

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9-80所示。

表 9-80 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。

参数名称	参数说明
描述	数据空间的描述信息。

----结束

9.5.11.3 编辑数据空间

操作场景

数据空间新增成功后，如果需要对其**描述信息**进行修改，可参见本章节进行处理。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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

9.5.11.4 删除数据空间

操作场景

如果不再需要某个数据空间，可以参照本章节进行删除。

约束与限制

- 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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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。

⚠ 注意

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

9.5.12 管理管道

9.5.12.1 创建管道

操作场景

数据传输消息主题和存储索引组合为数据管道。

当您需要使用安全云脑提供的**安全分析**、**数据分析**、**智能建模**功能时，需要创建管道。

本章节介绍如何创建管道。

前提条件

- 已新建工作空间，具体操作请参见**新增工作空间**。
- 已新增数据空间，具体操作请参见**新增数据空间**。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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。

步骤6 在创建管道页面中，配置管道参数，参数说明如**表9-81**所示。

表 9-81 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5-63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。 ● 名称须为数据空间中的唯一，不能与数据空间中其他管道名称相同。
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7 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

9.5.12.2 查看管道详情

操作场景

该任务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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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。

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 9-82 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

9.5.12.3 编辑管道

操作场景

管道创建成功后，可对管道**Shard数**、**描述**、**生命周期**进行修改。

本章节介绍如何修改管道参数信息。

约束与限制

系统创建的数据管道**不支持**编辑操作。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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。

步骤6 单击管道名称后的“更多 > 编辑”。

步骤7 从编辑管道页面中，配置管道参数，参数说明如**表9-83**所示。

表 9-83 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

9.5.12.4 删除管道

操作场景

本章节介绍如何删除管道。

数据将会被同步删除，且不可恢复，请谨慎操作。

约束与限制

系统创建的数据管道**不支持**删除操作。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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。

步骤6 单击管道名称后的“更多 > 删除”。

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

9.5.13 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。

安全云脑提供数据消费功能，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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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。

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9-84所示。

表 9-84 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。

9.5.14 数据监控

安全云脑数据监控功能支持监控安全云脑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：用于订阅安全云脑管道消息，一个管道可由多个订阅器进行订阅，安全云脑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，负责通过订阅器把安全云脑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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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。

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

9.6 数据投递

9.6.1 新增数据投递

操作场景

安全云脑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，安全云脑将定时将采集到的数据投递至其他管道或对应的云产品。

目前支持投递到以下云产品中：对象存储服务（Object Storage Service，OBS）、云日志服务（Log Tank Service，LTS）。

本章节介绍如何新增数据投递。

前提条件

- 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。

新增数据投递

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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。

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 9-85 基本信息

参数名称	参数说明
投递名称	自定义投递规则的名称。
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 9-86 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。
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9-87所示。

       表 9-87 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9-88所示。

       表 9-88 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。
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所在管道的ID，查询方法请参见步骤6。
写入身份	默认生成，无需配置。

   - LTS：将当前管道数据投递到LTS服务，参数配置说明如表9-89所示。
     投递到LTS中，需要已有可用的日志组和日志流。

表 9-89 配置数据目的-LTS

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LTS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LTS。
日志组	选择目的LTS日志组。
日志流	选择目的LTS日志流
写入身份	默认生成，无需配置。

- OBS：将当前管道数据投递到OBS服务，参数配置说明如**表9-90**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 9-90 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

后续处理

数据投递新增后，需进行投递权限授予操作，接受授权后，投递才会生效，详细操作请参见**数据投递授权**。

9.6.2 数据投递授权

操作场景

数据投递新增后，需进行投递权限授予操作，接受授权后，投递才会生效。

本章节介绍如何执行数据投递授权。

前提条件

已新增数据投递。

约束与限制

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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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“跨租投递权限授予”页签，进入跨租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，详细操作请参见**查看数据投递情况**。

----结束

相关操作

在跨租投递权限授权页面可以的投递权限进行**拒绝**和**取消**授权操作：

表 9-91 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”。

9.6.3 查看数据投递情况

操作场景

数据投递成功后，可以到投递目的地查看数据投递情况。请根据您的投递目的地选择对应操作：

- **投递到其他数据管道**
- **投递到OBS桶**
- **投递到LTS**

前提条件

已完成数据投递操作，具体操作请参见**新增数据投递**。

投递到其他数据管道

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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

投递到 OBS 桶

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

投递到 LTS

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

9.6.4 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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 9-92 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管道。
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。
投递目的信息	数据投递目的地相关信息。

操作	操作说明
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。
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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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

9.6.5 投递日志数据至 LTS

操作场景

安全云脑支持集成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**数据集成**。

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。

前提条件

- 已完成需投递日志的数据集成至安全云脑操作，详细操作请参见**数据集成**。
- 投递到LTS中，需要已有可用的日志组和日志流。

操作步骤

新增数据投递

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 安全分析”，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。

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”。

数据投递授权

步骤9 在数据投递管理页面，选择“跨租投递权限授予”页签，进入跨租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。

查看数据投递情况

步骤10 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11 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12 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13 在日志流详情页面，查看投递的日志信息。

----结束

10 安全编排

10.1 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。

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。**剧本和流程的含义、关系说明如下**：

- 含义：
  - 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（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。
- 联系与区别
  - 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。

10.2 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 10-1 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
	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，则通知客户并生成代办，如果人工审核通过则加入安全云脑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

安全防线	剧本名	描述	数据类
应用安全	云脑WAF地址组关联策略	将安全云脑指定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加入安全云脑WAF阻断策略中	Alert
运维安全	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
	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

安全防线	剧本名	描述	数据类
	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

10.3 安全编排使用流程

安全编排的使用流程如下：

图 10-1 安全编排使用流程

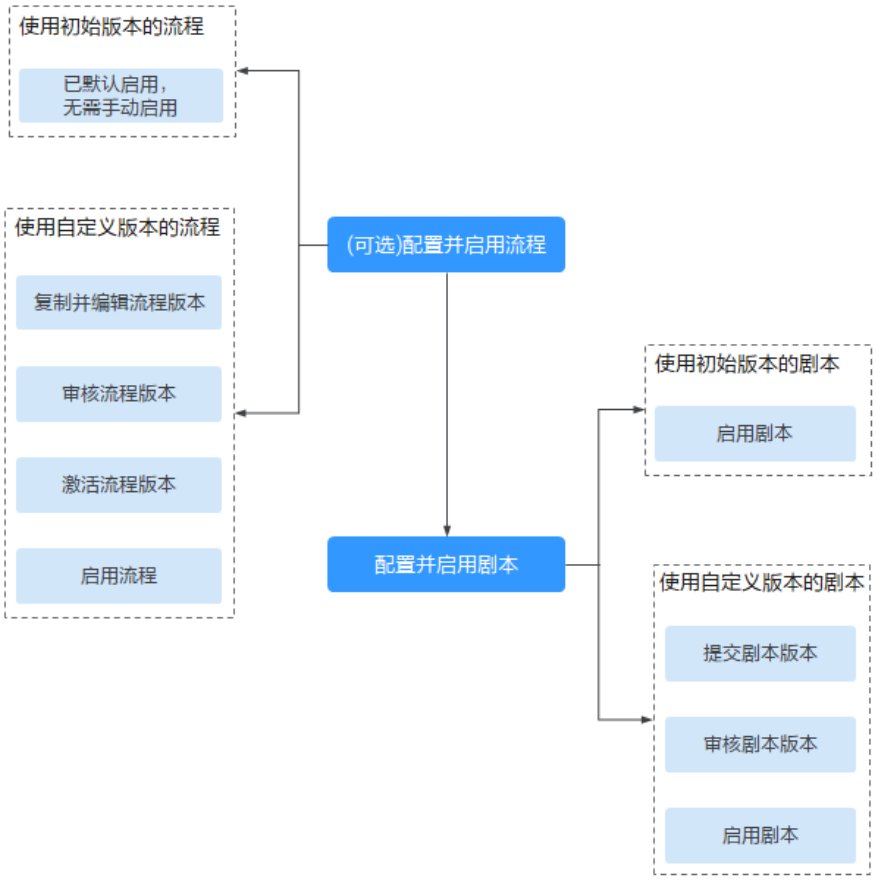


表 10-2 使用流程

序号	操作项	说明
1	（可选）配置并启用流程	启用需要的安全云脑内置的流程。 安全云脑默认提供了“WAF一键解封”、“主机告警状态同步”、“告警指标提取”等流程，且流程的初始版本（V1）也已启用，无需手动启用。 同时，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。
2	（可选）配置并启用剧本	启用需要的安全云脑内置的剧本。 安全云脑默认提供了“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。

10.4 （可选）配置并启用流程

操作场景

安全云脑默认提供了“WAF一键解封”、“主机告警状态同步”、“告警指标提取”等流程，且流程的初始版本（V1）也已启用，无需手动启用。

同时，还支持对已有流程进行自定义编辑，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。

启用自定义版本的流程

进入流程管理页面

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

复制流程版本

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。

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”。

编辑并提交流程版本

步骤8 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9 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 10-3 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10-4**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 10-4 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。

参数名称	参数说明
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。
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。
处理人	设置此流程的审核处理人为当前账号中的用户。设置后如有流程需审批，仅设置的责任人可在**任务中心**页面进行处理，非责任人仅支持查看。 **说明** 首次使用，需要授权。具体操作如下： 1. 单击“现在授权”，右侧弹出访问授权页面。 2. 在访问授权页面中，勾选“同意授权”，并单击“确认”。

步骤10 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。

审核流程版本

步骤11 编辑并提交流程版本后，页面返回流程管理页面。在**流程管理**页面中，单击目标流程“操作”列“版本管理”，右侧弹出流程版本管理页面。

步骤12 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13 在审核确认框中，选择“审核意见”为“通过”，并单击“确定”。

激活流程版本

步骤14 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”。

步骤15 在弹出确认框中，单击“确定”。

启用流程

默认已启用流程无需再手动启用。如果为未启用流程，请执行如下启用操作：

步骤16 在**流程管理**页面中，单击目标流程所在行的“操作”列的“启用”，页面弹出启用确认框。

步骤17 在弹出的确认框中，选择启用的流程版本后，单击“确定”。

----结束

10.5 配置并启用剧本

安全云脑默认提供了“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。

- 启用初始版本的剧本
- 启用自定义版本的剧本

启用初始版本的剧本

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

启用自定义版本的剧本

进入剧本管理页面

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 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。

复制剧本版本

步骤4 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5 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6 在弹出复制版本信息框中，单击“确定”。

编辑并提交剧本版本

步骤7 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8 在剧本版本编辑页面，编辑版本信息。

步骤9 单击“确定”。

提交剧本版本

步骤10 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“提交”。

步骤11 单击“确定”。

审核剧本版本

步骤12 在**剧本**版本管理页面中，单击目标剧本版本所在行的“操作”列的“审核”。

步骤13 在审核确认页面中，选择“审核意见”为“通过”，并单击“确定”。

激活剧本版本

步骤14 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“激活”。

启用剧本

默认已启用剧本无需再手动启用。如果为未启用剧本，请执行如下启用操作：

步骤15 在**剧本管理**页面中，单击目标剧本所在行的“操作”列的“启用”。

步骤16 在弹出的确认框中，选择启用的剧本版本后，单击“确定”。

----结束

10.6 运营对象管理

10.6.1 数据类

10.6.1.1 查看已有数据类

操作场景

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。

本章节介绍如何查看已有数据类。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

10.6.2 类型管理

10.6.2.1 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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10-5**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 10-5 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-6 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。
SLA	设置告警的SLA处理时间。

参数名称	参数说明
描述	自定义告警类型描述信息。

说明

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

说明

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

说明

- 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-7 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

说明

- 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 10-8 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

10.6.2.2 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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10-9所示。

表 10-9 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-10 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。

说明

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

说明

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

说明

- 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-11 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。
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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

说明

- 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 10-12 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。
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

10.6.2.3 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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10-13所示。

表 10-13 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-14 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。
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。

说明

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

说明

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

说明

- 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-15 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

说明

- 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 10-16 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

10.6.2.4 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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10-17**所示。

表 10-17 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-18 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。

说明

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

说明

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

说明

- 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-19 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

说明

- 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 10-20 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

10.6.2.5 管理自定义类型

操作场景

本章节介绍如何管理自定义类型。

- 添加自定义类型：介绍如何自定义新增类型。

- **新增自定义类型的子类型**：介绍如何自定义新增子类型。
- **自定义类型/子类型关联布局**：介绍如何将自定义新增的类型/子类型关联已有布局。
- **编辑自定义类型/子类型**：介绍如何编辑自定义新增的类型/子类型。
- **启用/禁用自定义子类型**：介绍如何启用/禁用新增的类型/子类型。
- **查看已有的自定义类型/子类型**：介绍查看自定义新增的类型/子类型。
- **删除自定义类型/子类型**：介绍删除自定义新增的类型/子类型。

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”。

添加自定义类型

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，并在自定义类型管理页面中单击“添加类型”，右侧弹出添加类型页面。

图 10-2 添加类型

步骤6 在添加类型页面中，配置类型参数。

表 10-21 自定义类型参数说明

参数名称	参数说明
数据类	选择已有数据类。
类型名称	自定义新增类型的名称。

参数名称	参数说明
类型标识	填写类型标识。标识关键字需遵循大驼峰命名规范，例如TypeTag。
启动状态	设置类型的启动状态。
描述	自定义类型的描述信息。

说明

自定义类型新增成功后，**不支持**修改“数据类”、“类型名称”和“类型标识”。

步骤7 在页面右下角单击“确认”。

新增完成后，可以在自定义类型页面的“类型列表”中查看已新增的类型。

----结束

新增自定义类型的子类型

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，在左侧“类型列表”中，单击需要新增子类型的自定义类型名称，右侧将展示自定义类型的详细信息。

步骤6 在右侧自定义类型管理页面中，单击“新增”，右侧弹出添加子类型页面。

图 10-3 新增子类型

步骤7 在新增子类型页面中，配置子类型参数。

表 10-22 子类型参数说明

参数名称	参数说明
数据类	当前数据类名称。
类型名称	当前数据类类型的名称。
类型标识	当前数据类类型标识。
子类型	自定义子类型关键字。
子类型标识	自定义子类型标识。标识关键字需遵循大驼峰命名规范，例如SubTypeTag。
启动状态	设置子类型的启动状态。
SLA	设置子类型的SLA处理时间。
描述	子类型的描述信息。

步骤8 单击“确认”。

----结束

自定义类型/子类型关联布局

说明

系统内置的类型和子类型默认已关联布局，**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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，并在自定义类型管理页面中根据类型选择对应操作。

- 类型
  a. 在自定义类型管理页面左侧的“类型列表”中，选择需要关联布局的类型。
  b. 在右侧展示该类型的详细信息中单击目标类型页面的“关联布局”，页面弹出绑定布局编辑框。
  c. 在绑定布局编辑框中，选择需要关联的布局，并单击“确认”。
- 子类型
  a. 在自定义类型管理页面左侧的“类型列表”中，选择需要关联布局的类型。
  b. 在右侧展示该类型的子类型列表中，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。

c. 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

编辑自定义类型/子类型

说明

- 系统内置的类型和子类型**不支持**编辑。
- 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”、“子类型标识”。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，并在自定义类型管理页面中请根据类型选择对应操作。

- 类型
  a. 在自定义类型管理页面左侧的“类型列表”中，选择需要编辑的类型。
  b. 在右侧展示该类型的详细信息中单击目标类型页面的“编辑”，页面右侧弹出编辑类型页面。
  c. 在编辑类型页面中，编辑类型的参数信息。

  表 10-23 类型参数说明

参数名称	参数说明
数据类	类型所属的数据类，**不支持修改**。
类型名称	自定义类型的名称，**不支持修改**。
类型标识	漏洞类型标识，**不支持修改**。
启动状态	设置类型的启动状态。
描述	自定义类型的描述信息。

  d. 在页面右下角单击“确认”。
- 子类型
  a. 在自定义类型管理页面左侧的“类型列表”中，选择需要编辑的类型。
  b. 在右侧展示该类型的子类型列表中，单击目标类型所在行“操作”列的“编辑”，页面右侧弹出编辑子类型页面。
  c. 在编辑子类型页面中，编辑子类型的参数信息。

表 10-24 子类型参数说明

参数名称	参数说明
数据类	类型所属的数据类，**不支持修改**。
类型名称	自定义类型的名称，**不支持修改**。
类型标识	类型标识，**不支持修改**。
子类型名称	子类型的名称，**不支持修改**。
子类型标识	子类型标识，**不支持修改**。
启动状态	设置子类型的启动状态。
SLA	设置子类型的SLA处理时间。
描述	自定义子类型的描述信息。

d. 在页面右下角单击“确认”。

----结束

启用/禁用自定义子类型

说明

系统内置的子类型默认已启用，**不支持**禁用。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，并在自定义类型管理页面左侧的“类型列表”中，单击目标类型名称。

步骤6 在右侧展示该类型的子类型列表中，在目标子类型的“启用状态”列中进行启用（或禁用）设置。

选择需要批量启用（或禁用）子类型，可以选勾选多个子类型后，单击类型列表左上角“批量启用”（或“批量禁用”）。

步骤7 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”（或启用）时，则表示禁用（或启用）成功。

----结束

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

删除自定义类型/子类型

说明

系统内置的类型和子类型**不支持**删除。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，并在自定义类型管理页面中根据类型选择对应操作。

- 类型
  a. 在自定义类型管理页面左侧的“类型列表”中，选择需要目标
  b. 在右侧展示该类型的详细信息中单击目标类型页面的“删除”，弹出删除确认框。
  c. 在弹出的确认框中，单击“确认”。
- 子类型
  a. 在自定义类型管理页面左侧的“类型列表”中，选择需要目标类型。
  b. 在右侧展示该类型的子类型列表中，单击目标类型所在行“操作”列的“删除”，弹出删除确认框。

c. 在弹出的确认框中，单击“确认”。

----结束

10.6.3 分类&映射

10.6.3.1 查看已有分类映射

操作场景

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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

10.6.3.2 创建/复制/编辑分类映射

操作场景

分类和映射是对云服务告警进行类型匹配和字段映射。

本章节介绍如何创建、编辑、复制分类映射。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

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10-25所示。

   表 10-25 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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10-25所示。

   表 10-26 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

10.6.3.3 管理分类映射

操作场景

本章节介绍如何管理分类映射，如启用、禁用、删除操作。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

说明

- 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 10-27 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

10.7 剧本编排管理

10.7.1 剧本

10.7.1.1 提交剧本版本

操作场景

本章节主要介绍如何提交剧本版本。

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**。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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7 在确认框中，单击“确定”，提交剧本版本。

说明

- 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

后续处理

剧本版本提交后，需要进行审核，详细操作请参见**审核剧本版本**。

10.7.1.2 审核剧本版本

操作场景

本章节主要介绍如何审核剧本版本。

前提条件

已提交剧本，具体操作请参见**提交剧本版本**。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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10-28**所示。

表 10-28 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）。

说明

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

后续处理

剧本版本审核后，需要启用剧本，详细操作请参见**启用剧本**。

10.7.1.3 启用剧本

操作场景

完成剧本版本审核后可启用剧本，本章节主要介绍如何启用剧本。

前提条件

已激活剧本版本，具体操作请参见**激活/失活剧本版本**。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

10.7.1.4 管理剧本

操作场景

本章节将介绍如何执行**查看已有剧本**、**导出剧本信息**、**禁用剧本**、**删除剧本**等操作。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

- 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 10-29 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。

参数名称	参数说明
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

导出剧本信息

说明

安全云脑支持导出“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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

说明

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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”。

说明

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

10.7.1.5 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

说明

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

说明

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

说明

- 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

说明

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

说明

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

说明

剧本版本删除后，不可找回，请谨慎操作。

----结束

10.7.2 流程

10.7.2.1 审核流程版本

操作场景

本章节主要介绍如何审核流程版本。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

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10-30**所示。

表 10-30 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。
驳回原因	输入审核意见（当审核意见勾选驳回时必填）。

说明

- 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

后续处理

流程版本审核后，需要启用流程，详细操作请参见**启用流程**。

10.7.2.2 启用流程

操作场景

本章节主要介绍如何启用流程。

前提条件

已激活流程版本，具体操作请参见**管理流程版本**。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

10.7.2.3 管理流程

操作场景

本章节将介绍如何**查看流程**、**导出流程**、**删除流程**、**禁用流程**。

查看流程

步骤1 登录管理控制台。

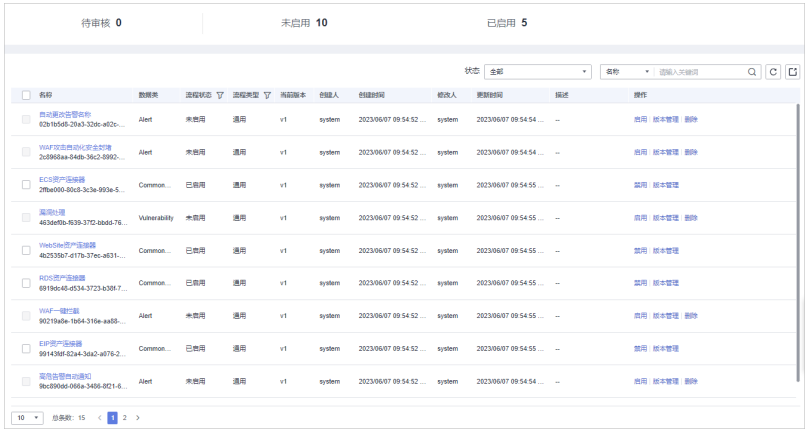
步骤2 单击页面左上方的 ☰，选择“安全 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-4 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 10-31 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。

参数名称	参数说明
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。
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

导出流程

说明

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

说明

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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”。

说明

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

10.7.2.4 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

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

说明

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

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 10-32 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10-33**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。

参数名称			参数说明
	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 10-33 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。
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。
处理人	设置此流程的审核处理人为当前账号中的用户。设置后如有流程需审批，仅设置的责任人可在任务中心页面进行处理，非责任人仅支持查看。 **说明** 首次使用，需要授权。具体操作如下： 1. 单击“现在授权”，右侧弹出访问授权页面。 2. 在访问授权页面中，勾选“同意授权”，并单击“确认”。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

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。

步骤7 在确认框中，单击“确定”，提交流程版本。

说明

- 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

说明

- 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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

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”。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

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”。

说明

流程版本删除后，不可找回，请谨慎操作。

----结束

10.7.3 资产连接

10.7.3.1 新增资产连接

操作场景

- **含义**：资产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。
- **资产连接与插件的关系**：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）。资产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资产连接，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新建资产连接。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“资产连接”页签，进入资产连接管理页面。

步骤5 在资产连接管理页面中，单击“新增”，右侧弹出新增资产连接面板。

步骤6 在新增资产连接面板中，配置资产连接参数，参数说明如表10-34所示。

表 10-34 资产连接参数说明

参数名称	说明
连接名称	输入资产连接名称。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。
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。
插件	选择资产连接所需的插件。插件详细信息请参见查看插件详情。
连接类型	选择资产连接的类型。 • 云服务委托：使用云服务类型的插件时，建议优先使用云服务委托。 该类型不需要手动输入域名和用户名/密码等鉴权参数，自动根据插件名称获取对应云服务的域名（Endpoint），采用云服务委托的方式进行鉴权。 • AK&SK：需要用户手动输入域名（Endpoint），采用AK&SK的方式进行鉴权。 • 用户名及密码：需要用户手动输入域名（Endpoint），采用用户名/密码的方式进行鉴权。 • 其他：部分插件有除了上述鉴权参数在内的其他鉴权参数，请根据插件登录凭证参数指导进行填写。
凭证信息	根据选择的连接类型填写凭证信息，例如Endpoint、AK、SK等。

步骤7 单击“确认”，返回资产列表，即可查询已经创建的资产连接信息。

----结束

10.7.3.2 管理资产连接

操作场景

本章节主要介绍如何查看资产连接、编辑资产连接、删除资产连接。

查看资产连接

步骤1 登录管理控制台。

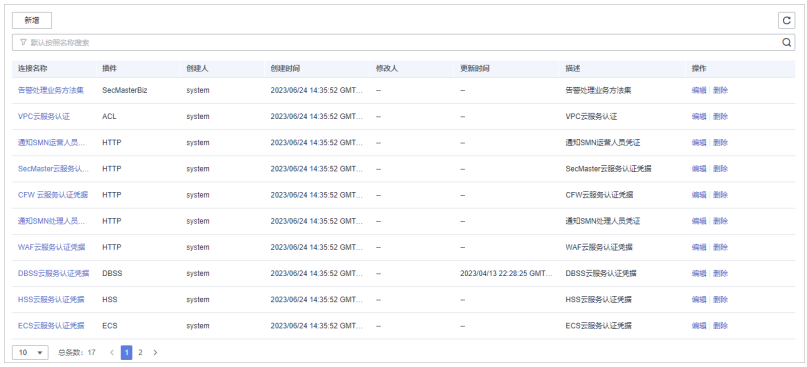
步骤2 单击页面左上方的，选择“安全 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“资产连接”页签，进入资产连接管理页面。

步骤5 在资产连接管理页面，查看资产连接信息。

图 10-5 查看资产连接信息



- 在资产连接列表中，可以查看资产连接的名称、插件、创建人等信息。
- 当资产连接较多时，可以通过搜索功能快速查询指定资产连接。
- 如需查看某个资产连接的详细信息，可单击待查看资产连接的名称，进入资产连接详情页面进行查看。

----结束

编辑资产连接

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“资产连接”页签，进入资产连接管理页面。

步骤5 在目标资产连接所在行“操作”列，单击“编辑”，弹出编辑资产连接页面。

步骤6 在资产连接编辑页面中，编辑资产连接参数，参数说明如**表10-35**所示。

表 10-35 资产连接参数说明

参数名称	说明
连接名称	输入资产连接名称。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。
描述	可选参数，输入资产连接描述，描述信息长度不能超过64个字符。
插件	选择资产连接所需的插件。插件相关介绍请参见**查看插件详情**。
创建人	资产连接的创建人，该参数**不支持修改**。
创建时间	资产连接的创建时间，该参数**不支持修改**。
修改人	资产连接的最近一次修改的用户，该参数**不支持修改**。
连接类型	选择资产连接的类型。
凭证信息	根据选择的连接类型填写凭证信息，例如AK、SK等。

步骤7 单击“确认”，完成资产连接的编辑。

----结束

删除资产连接

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“资产连接”页签，进入资产连接管理页面。

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”，完成资产连接删除。

说明

资产连接删除后，不可找回，请谨慎操作。

----结束

10.7.4 实例管理

10.7.4.1 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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，选择“剧本实例”或“流程实例”页签，可查看实例信息，参数说明如表10-36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 10-36 实例列表参数

参数名称	参数说明
实例名称	系统生成的实例的名称。
剧本/实例名称	实例对应的剧本/实例名称。
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

参数名称	参数说明
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。

10.8 页面布局管理

10.8.1 查看已有布局模板

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已有布局模板。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 > 布局管理”，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

10.8.2 管理已有布局

操作场景

本章节将介绍如何查看已有布局、删除布局。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

删除布局

支持删除自定义新增的页面布局。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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，将鼠标放在目标布局上，并单击布局右上角，弹出删除确认框。

步骤6 单击“确认”，删除布局。

----结束

10.9 插件管理

10.9.1 插件管理概述

安全云脑支持将安全编排流程中使用的插件进行统一管理。

名词解释

- **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安全云脑，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。

10.9.2 查看插件详情

操作场景

本章节介绍如何查看安全云脑内置插件及详细信息。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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

11 设置

11.1 数据采集

11.1.1 数据采集概述

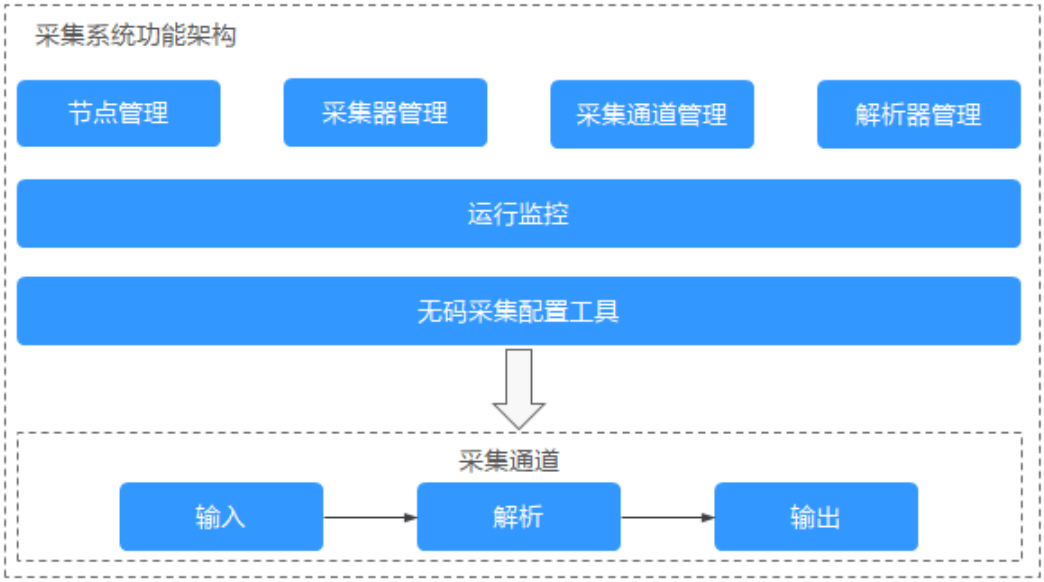
安全云脑的数据采集功能，提供了将第三方日志数据接入安全云脑的能力。它使用Logstash通过多种方式采集各类日志数据，采集后，可以快速实现历史数据分析比对、数据关联分析、以及未知威胁发现等相关分析。

图 11-1 数据采集

数据采集原理

数据采集的基本原理是安全云脑提供组件控制器（isap-agent），安装在租户云服务器上，通过组件控制器来管理采集组件Logstash，通过Logstash完成租户自身、租户与安全云脑数据的收发工作。

图 11-2 采集系统功能架构



含义

- 采集器：定制化的Logstash。采集器节点则是定制化的Logstash+组件控制器（isap-agent）。
- 节点：安装了组件控制器（isap-agent），并被安全云脑纳管的云服务器叫做节点。节点纳管成功后，即可在组件管理中下发采集引擎Logstash。
- 组件：为了很好地完成业务而定制的软件，目前提供汇聚式收集引擎Logstash用于租户日志收发安全云脑业务。
- 连接器：Logstash配置的基础概念，主要包括input、output两部分，分别对应源连接器、目的连接器，用于定义采集器Logstash接受数据方式和规范。其中，安全云脑管道pipe连接器可以对接安全云脑，实现租户数据上报安全云脑，安全云脑数据转储到租户的能力。
- 解析器：Logstash配置的基础概念，主要为Logstash的filter部分，安全云脑解析器是对其filter部分的无码化封装和定制，用户只需在页面上配置解析器规则即可生成原生的filter配置脚本，从而轻松实现将原始日志转化为目标格式。
- 采集通道：采集通道等价于Logstash的pipeline，在Logstash可以配置多个pipeline，每个pipeline包括input、filter、output部分，每个pipeline为单独的作业，互不影响。在安全云脑租户采集上，可将相同的pipeline部署在多个节点上，并且配置相同的pipeline视为一个采集通道。

约束与限制

- 目前，数据采集的组件控制器支持运行在Linux系统x86_64和arm64架构的ECS主机上。

采集器规格

采集管理中，选作为节点的云服务器规格说明如下表所示：

表 11-1 采集器规格

CPU内核数	内存大小	系统盘	数据盘	参考处理能力
4U	8G	50G	100G	2000 EPS @ 1KB 4000 EPS @ 500B
8U	16G	50G	100G	5000 EPS @ 1KB 10000 EPS @ 500B
16U	32G	50G	100G	10000 EPS @ 1KB 20000 EPS @ 500B
32U	64G	50G	100G	20000 EPS @ 1KB 40000 EPS @ 500B
64U	128G	50G	100G	40000 EPS @ 1KB 80000 EPS @ 500B

说明

云服务器规格最少为2U4G，目录磁盘至少挂载100G磁盘。

日志量应当与机器规格成比例放大，总体来说，建议按表中规格比例进行放大。如果机器压力较大，建议部署多台采集器，通过采集通道来统一管理，分摊单机日志中转压力。

安装组件控制器前，建议先挂载磁盘，然后使用分盘脚本对磁盘进行分配，确保目录磁盘下有超过100G的剩余空间，保证采集器Logstash的正常安装和运行。

日志源的数量

采集器支持的日志源数量不受限制，可随云资源配置变化而动态扩展。

数据采集流程

图 11-3 数据采集流程

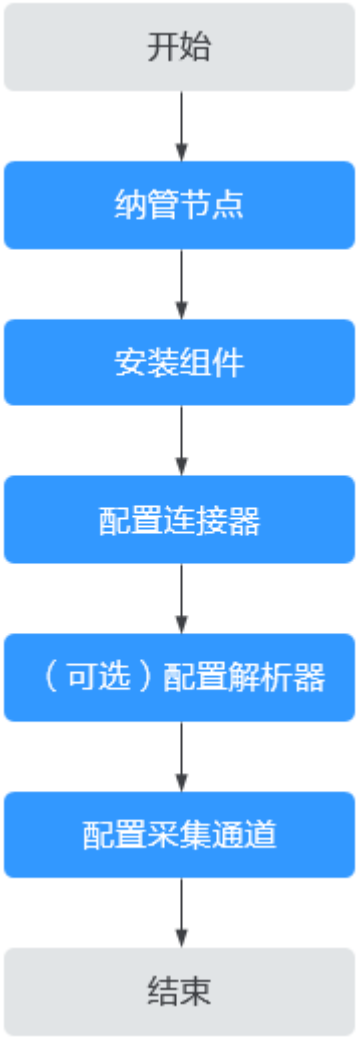


表 11-2 数据采集流程说明

序号	步骤	说明
1	**纳管节点**	选择或购买云服务器，在云服务器上安装组件控制器，完成节点纳管。
2	**安装组件**	节点纳管完成之后可以通过管理下发安装引擎Logstash，完成组件安装。
3	**配置连接器**	配置源和目的连接器，根据需要选择连接器并完成参数配置。
4	（可选）**配置解析器**	根据需要在页面上进行无码化解析器配置。
5	**配置采集通道**	配置连接通道，并与节点进行关联，下发Logstash的pipeline配置，完成整个数据采集的配置。

序号	步骤	说明
6	采集结果验证	配置完成采集通道之后，验证数据是否采集。 如果是日志接入到安全云脑管道，可以在安全云脑“安全分析”页面查询结果。

数据采集移除流程

图 11-4 数据采集移除流程

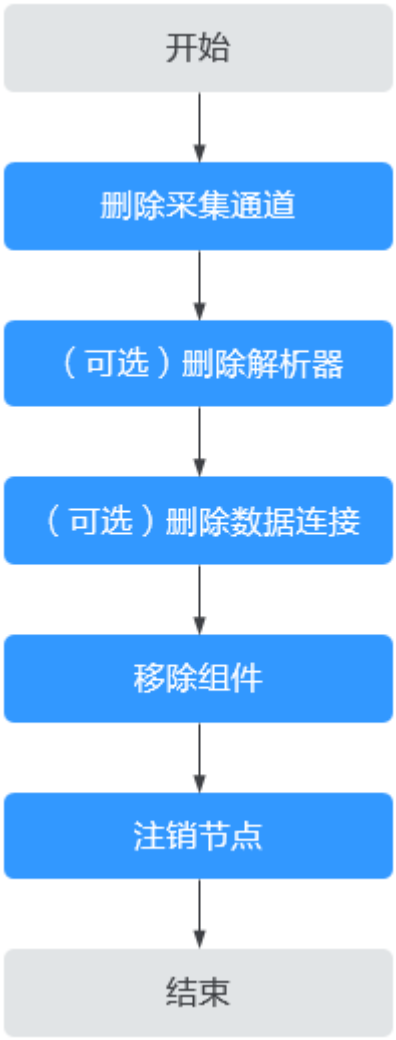


表 11-3 数据采集移除流程说明

序号	步骤	说明
1	删除采集通道	请在采集通道管理页面中，停止并删除Logstash的pipeline配置。 注：相关节点上的所有采集通道都需要进行停止并删除，才可以完整移除组件、注销节点。

序号	步骤	说明
2	（可选）删除解析器	如果配置了解析器，请在解析器管理页面中，删除配置的无码化解析器。
3	（可选）删除数据连接	如果新增了数据连接，请在连接管理页面中，删除源和目的连接器。
4	移除组件	删除节点上安装的采集引擎Logstash，移除组件。
5	注销节点	移除组件控制器，完成节点注销。 注：注销节点不会删除ECS和endpointinterface资源，后续如果不再使用数据采集功能，需要手动释放。

11.1.2 组件管理

11.1.2.1 新增/编辑节点

操作场景

本章节将介绍如何新增/编辑节点。

⚠ 注意

安装路径建议为“/opt/cloud”，本章节也以此路径为例进行介绍。如需安装在其他自定义路径中，请根据路径修改，例如，如果安装路径为“/tmp”，则将该章节操作步骤中的安装路径改为“/tmp”。

新增节点前准备

- **检查磁盘大小**

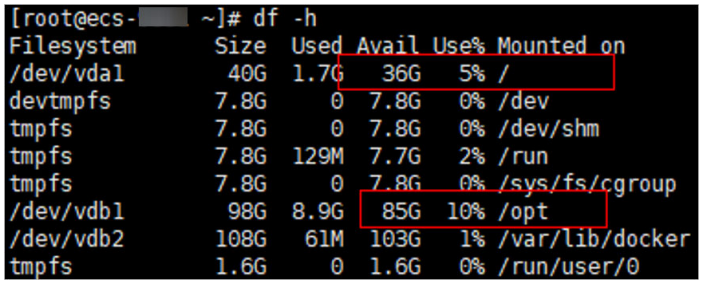
  新增节点前需要先检查待安装组件控制器的ECS主机的磁盘的/opt目录下是否预留100G以上的磁盘空间。

  a. 远程登录待安装组件控制器的ECS。

     - 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机。
     - 如果您的主机已经绑定了弹性IP，您也可以使用远程管理工具（例如：Xftp、SecureFX、WinSCP、PuTTY、Xshell等）登录主机，并使用root账号在主机中安装组件控制器。

  b. 执行**df -h**命令，检查磁盘/opt目录下是否预留100G以上的磁盘空间，CPU核数需要2核以上，内存需要4G以上。

图 11-5 检查磁盘



如果内存不足，请关闭一些高内存占用的应用程序或扩充内存容量后再进行安装。

为了磁盘/opt目录下有超过100G的剩余磁盘空间，可以采用分盘脚本对磁盘进行分配，磁盘分区具体操作请参见**磁盘分区**。

新增节点

步骤1 完成**新增节点前准备**操作后，登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 组件管理”，默认进入节点管理页面。

步骤5 在节点管理页面中，单击“新增”，页面右侧弹出新增节点页面。

步骤6 在新增节点页面中，配置通道。

1. 在网络通道配置栏中，选择待安装ECS所属的虚拟私有云和子网。
2. 在网络通道列表中，单击**所有通道**操作列的“配置”，并在弹出的确认框中，单击“确定”。

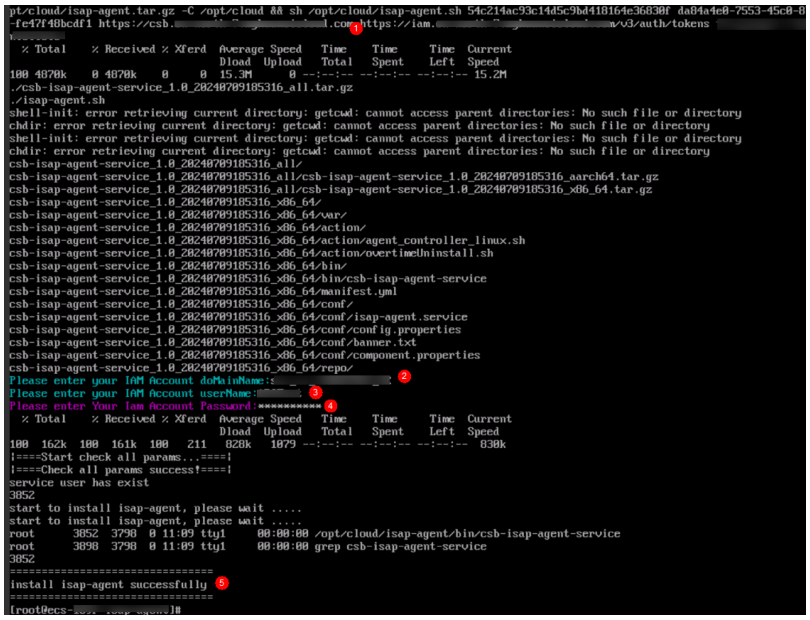
步骤7 单击页面右下角“下一步”，进入“脚本安装验证”页面。

步骤8 选择云服务器系统，根据安装步骤，并单击 复制安装组件控制器的命令。

步骤9 安装组件控制器。

1. 远程登录待安装组件控制器的ECS。
   - 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机。
   - 如果您的主机已经绑定了弹性IP，您也可以使用远程管理工具（例如：Xftp、SecureFX、WinSCP、PuTTY、Xshell等）登录主机，并使用root账号在主机中安装组件控制器。
2. 粘贴**步骤8**复制的安装命令，并以root权限执行，在ECS中安装组件控制器。
3. 根据界面提示，输入账号和密码。
4. 如果界面回显“install isap-agent successfully”信息时，则表示组件控制器安装成功。

图 11-6 安装成功



安装过程中，如果安装失败请参考**组件控制器安装失败**进行排查处理；如果提示内存不足，请参见**磁盘分区**进行处理。

步骤10 确认已安装后，返回安全云脑新增节点页面，单击页面右下角“确认”。

安装完成后，可以在节点页面查看已新增的节点。

----结束

编辑节点

节点新增成功后，仅支持修改节点补充信息。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 组件管理”，默认进入节点管理页面。

步骤5 在节点管理页面中，单击目标节点所在行“操作”列的“编辑”，页面右侧弹出编辑节点页面。

步骤6 在编辑节点页面中，编辑节点补充信息。

表 11-4 节点补充信息

参数名称	参数说明
数据中心	自定义数据中心名称。
网络平面	选择节点网络平面。

参数名称	参数说明
标签	设置节点标签。
描述	自定义节点描述信息。
维护人	选择节点维护人。

步骤7 单击页面右下角“确认”。

----结束

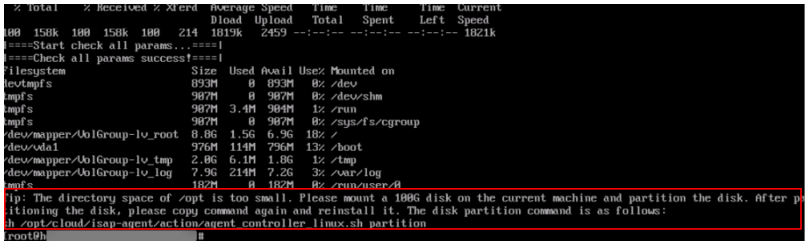
11.1.2.2 磁盘分区

目前，租户采集主要用于数据中转业务，为保证采集器的正常运行，有如下约束与限制条件：

- 组件控制器（isap-agent）安装仅支持非管理员账户的账户。
- 安装组件控制器（isap-agent）并使用采集器用于数据转入转出业务时，请保证“/opt/cloud”空间下有至少100G磁盘空间。

因此，当您在/opt目录下安装isap-agent时，如果出现如图11-7所示的提示信息时，则表示当前ECS的/opt目录磁盘空间不够。

图 11-7 磁盘空间不够



由于安装组件控制器（isap-agent）的ECS目录磁盘至少挂载100G，因此需要先执行提示中的命令执行进行分区，确保目录磁盘大小充足。

此时，需要对租户采集磁盘进行分区操作，具体操作步骤如下：

步骤1 申请并挂载磁盘。

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 在页面左上角单击 ，选择“计算 > 弹性云服务器”，并在弹性云服务器列表中，单击当前安装isap-agent的ECS名称，进入ECS详情页面。
4. 选择“云硬盘”页签，进入云硬盘页面后，单击“新增磁盘”。
5. 在申请云硬盘页面，申请一个“磁盘规格”容量为“100GB”的磁盘。

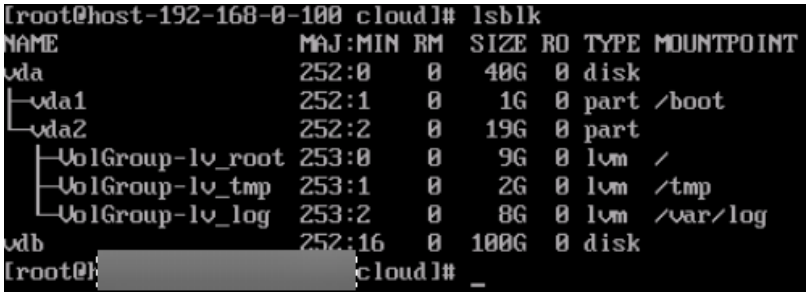
   云硬盘的申请参数信息配置请参考《云硬盘用户指南》。
6. 磁盘挂载成功后，可以在ECS的云硬盘页面查看已挂载的磁盘。

   云硬盘挂载至云服务器后，需要登录云服务器初始化云硬盘，即格式化云硬盘，之后云硬盘才可以正常使用。

步骤2 进行磁盘分区操作。

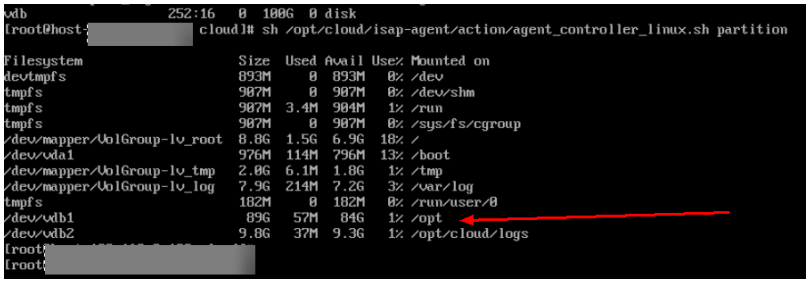
1. 登录到当前安装isap-agent节点，执行如下命令，查看当前节点的磁盘情况：
   lsblk

   图 11-8 查看节点磁盘大小情况



2. 执行如下命令，进行磁盘分区：
   sh /opt/cloud/isap-agent/action/agent_controller_linux.sh partition
   当提示信息如下图所示时，则表示磁盘分区成功。

   图 11-9 磁盘分区



步骤3 重新安装组件控制器（isap-agent），详细操作请参见**纳管节点**。

----结束

11.1.2.3 管理节点

操作场景

本章节将介绍如何执行**查看节点管理信息**、**注销节点**操作。

查看节点管理信息

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 组件管理”，默认进入节点管理页面。

步骤5 在节点管理页面中，查看节点的详细信息。

当节点较多时，可以通过搜索功能快速查询指定节点。

表 11-5 节点参数说明

参数名称	参数说明
节点名称/ID	节点的名称/ID。
健康状态	节点的健康状态。
区域	节点所在区域。
IP地址	节点的IP地址。
CPU使用率	节点的CPU使用率。
内存使用率	节点的内存使用率。
磁盘使用率	节点的磁盘使用率。
网络速率	节点的网络速率。
标签	节点的标签信息。
心跳过期失联标识	节点是否心跳过期失联。 15分钟内没有心跳则节点将标记为“失联”。

步骤6 如需查看某个节点的详细信息，可单击节点名称，在右侧弹出的详情页面进行查看。

----结束

注销节点

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 组件管理”，默认进入节点管理页面。

步骤5 在节点管理页面中，单击目标节点所在行“操作”列的“注销”。

步骤6 在弹出的确认框中，单击“确定”。

说明

仅注销节点，不会删除ECS和endpointinterface资源。后续如果不再使用数据采集功能，需要手动释放。

----结束

11.1.2.4 配置组件

操作场景

本章节将介绍如何配置组件信息。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 组件管理”，进入节点管理页面后，选择“组件管理”页签，进入组件管理页面。

步骤5 在组件管理页面中，单击待查看组件右上角“编辑配置”，右侧将弹出该组件的配置管理页面。

步骤6 在节点配置栏中，单击节点列表左上角“添加”，并在弹出的“添加节点”框中选择节点后，单击“确认”。

步骤7 单击页面右下角“保存并应用”。

等待一段时间，当组件状态为“应用完成”时，表示在当前节点上采集器Logstash已经安装完成。

----结束

11.1.2.5 Logtash 组件配置项说明

租户采集Logstash采集器是安全云脑经过定制化处理的。其在不同传输场景可进行不同程度的优化配置，此处主要提供日志配置log4j2.properties、jvm.options运行内存优化配置。

jvm 运行内存配置

表 11-6 jvm 运行内存配置

配置项	配置类型	默认值	配置说明
-Djava.awt.headless	boolean	true	服务端配置，在缺少设备（键盘或鼠标等）下可运行，用于数据类服务
-XX:+UseConcMarkSweepGC	boolean	false	是否使用CMS垃圾回收器回收采集器运行时堆内存生成的对象

配置项	配置类型	默认值	配置说明
-Xmn	string	1024M	采集器堆内存中年轻代占用的大小，如果采集压较大力时，可适当调整，年轻代空间越大，内存回收次数越少，采集效率越高。Xmn必须小于等于Xmx
-Xmx	string	2048M	采集器堆空间的最大值，合理设置这个参数可以避免JVM过度消耗系统资源，从而提高应用程序的稳定性和性能。此值设置过低会导致采集器频繁进行内存回收，影响正常采集能力
-Djruby.jit.threshold	number	0	表示方法调用的次数，当达到这个次数时，JRuby 的 JIT 编译器会尝试编译该方法的本地代码。设置这个值可以帮助平衡启动时间（编译成本）和执行时性能
-XX:CMSInitiatingOccupancyFraction	number	75	CMS垃圾收集器，当老年代达到75%时，触发CMS垃圾回收
-Xms	string	20248M	用于设置Java堆内存的初始大小。在JVM启动时，它将尝试分配指定数量的内存给堆。合理设置这个参数可以避免在应用程序运行过程中频繁地调整堆大小，从而提高性能。

log4j2 日志配置

表 11-7 log4j2 日志配置

配置项	配置类型	默认值	配置说明
appender.json_console_slowlog.layout.compact	boolean	true	是否开启json慢日志输出
appender.json_console_slowlog.layout.type	string	JSONLayout	追加json慢日志布局类型，采用默认值即可
appender.json_console_slowlog.type	string	Console	追加json慢日志类型，默认值Console，表示直接打印在控制台
appender.json_console_slowlog.layout.eventEol	boolean	true	是否开启json慢日志输出自动换行

配置项	配置类型	默认值	配置说明
appender.json_console_slowlog.name	string	json_console_slowlog	json慢日志输出的名称，采用默认值即可

11.1.2.6 查看组件详情

操作场景

本章节将介绍如何查看组件详细信息。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 组件管理”，进入节点管理页面后，选择“组件管理”页签，进入组件管理页面。

步骤5 在组件管理页面中，查看组件的详细信息。

- **运行节点**：
  单击待运行组件右上角“运行节点”，右侧将弹出该组件的运行节点信息。
- **查看配置**：
  单击待查看组件右上角“查看配置”，右侧将弹出该组件的详细配置信息。
- **编辑配置**：
  a. 单击待查看组件右上角“编辑配置”，右侧将弹出该组件的配置管理页面。
  b. 在节点配置栏中，编辑节点配置信息。
     - 添加节点：单击节点列表左上角“添加”，并在弹出的“添加节点”框中，选择节点后，单击“确认”。
     - 编辑已添加节点参数信息：单击节点名称前的 ⌄，展开节点配置信息后，编辑节点参数信息。
     - 运行参数：单击目标节点所在行“操作”列的“运行参数”。
     - 移除节点：单击目标节点所在行“操作”列的“移除”。
     - 批量删除：选中待移除节点后，单击列表左上角“批量移除”。
     - 查看历史版本：单击页面右下角“历史版本”。
  c. 单击页面右下角“保存并应用”。

----结束

11.1.3 采集管理

11.1.3.1 新增/编辑连接

操作场景

本章节主要介绍如何新增/编辑连接。

约束与限制

- 数据连接新增成功后，仅支持对已选择的数据源类型的参数信息进行修改，不支持变更数据源类型。

新增连接

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，默认进入连接管理页面。

步骤5 新增数据连接来源。

1. 在“连接管理”页面中，单击“新增”，默认进入选择数据连接来源页面。
2. 配置数据连接来源参数。
   - 连接方式：选择“来源”。
   - 连接类型：选择数据源的类型。
   - 其他参数配置：根据选择的连接类型进行参数配置，详细参数说明请参见**源连接器**。
3. 设置完成后，单击页面右下角“确认”。

步骤6 新增数据连接目的。

1. 在“连接管理”页面中，单击“新增”，进入选择数据连接页面。
2. 配置数据连接目的参数。
   - 连接方式：选择“目的”。
   - 连接类型：选择数据连接目的的类型。
   - 其他参数配置：根据选择的连接类型进行参数配置，详细参数说明请参见**目的连接器**。
3. 设置完成后，单击页面右下角“确认”。

----结束

编辑数据连接

说明

数据连接新增成功后，仅支持对已选择的数据源类型的参数信息进行修改，不支持变更数据源类型。

例如，新增数据连接时选择的数据源类型为“文件（File）”，仅支持对文件类型中的参数进行修改，不支持变更“文件（File）”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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，默认进入连接管理页面。

步骤5 在连接管理页面中，单击目标连接所在行“操作”列的“编辑”。

步骤6 在编辑数据连接页面中，编辑数据源类型信息参数信息。

步骤7 设置完成后，单击页面右下角“确认”。

----结束

11.1.3.2 连接器规则说明

源连接器

安全云脑租户采集连接器，目前支持的源连接器类型如下表所示：

表 11-8 源连接器类型

连接器名称	对应的logstash插件	描述
传输控制协议 TCP	tcp	用于接收TCP协议日志，配置规则请参见表11-9。
用户数据协议 UDP	udp	用于接收UDP协议日志，配置规则请参见表11-10。
对象存储 OBS	obs	用于读取对象存储OBS桶的日志数据，配置规则请参见表11-11。
消息队列 KAFKA	kafka	用于读取Kafka网络日志数据，配置规则请参见表11-12。
云脑管道 PIPE	pipe	用于将安全云脑数据外发到租户侧，配置规则请参见表11-13。
Elasticsearch CSS	elasticsearch	用于读取ES集群的数据，配置规则请参见表11-14。

表 11-9 tcp 连接器配置规则

规则	对应logstash配置项	类型	默认值	是否必填	描述
端口	port	number	1025	是	采集节点端口号
解码类型	codec	string	plain	是	编码格式 • plain：读取原始内容 • json：处理json格式内容
报文标签	type	string	tcp	是	用于对日志标签
是否SSL	ssl_enable	boolean	false	否	是否开启ssl认证
ssl证书	ssl_cert	file	null	否	cert证书
ssl-key文件	ssl_key	file	--	否	ssl-key文件
ssl秘钥	ssl_key_passphrase	string	--	否	ssl证书密钥

表 11-10 udp 连接器配置规则

规则	对应logstash配置项	类型	默认值	是否必填	描述
端口	port	number	1025	是	采集节点端口好
解码类型	codec	string	plain	是	解码类型 • plain：读取原始内容 • json：处理json格式内容
报文标签	type	string	udp	否	报文标签，有于后续处理的标记
队列大小	queue_size	number	20000	否	队列大小
接收缓冲区字节数	receive_buffer_bytes	number	20000	否	接收缓冲区字节数
缓冲区大小	buffer_size	number	10000	否	缓冲区大小

规则	对应logstash配置项	类型	默认值	是否必填	描述
工作线程	workers	number	1	否	工作线程数

表 11-11 obs 连接器配置规则

规则	对应logstash配置项	类型	默认值	是否必填	描述
region	region	string	--	是	region
桶	bucket	string	demo-obs-sec-mrd-datas	是	对象桶名
endpoint	endpoint	string	--	是	endpoint地址，注意要添加https
AK	ak	string	--	否	AK
SK	sk	string	--	否	SK
前缀	prefix	string	/test	否	日志读的文件夹前缀
缓存文件夹	temporary_directory	string	/temp	否	日志读取时，缓存的文件夹
报文标签	type	string	--	否	报文标签
记忆路径	sincedb_path	string	/opt/cloud/logstash/pipeline/file_name	否	用于设置读取的位置信息，防止重启导致的全文遍历

表 11-12 kafka 连接器配置规则

规则	对应logstash配置项	类型	默认值	是否必填	描述
服务地址	bootstrap_servers	string	--	是	服务地址
主题	topics	array	logstash	是	主题，可同时消费多个主题
消费线程	consumer_threads	number	1	是	消费线程

规则	对应logstash配置项	类型	默认值	是否必填	描述
偏移复位	auto_offset_reset	string	latest	否	偏移复位 • earliest：读取最早的消息 • latest：读取最新的消息
SSL证书	ssl_truststore_location	file	--	否	SSL证书 当选择SSL相关协议时需要填写该参数
SSL秘钥	ssl_truststore_password	string	--	否	SSL秘钥 当选择SSL相关协议时需要填写该参数
安全协议	security_protocol	string	SASL_SSL	否	安全协议
sasl连接配置	sasl_jaas_config	string	--	否	sasl连接配置
是否加密	is_pw_encrypted	string	false	否	是否加密
sasl机制	sasl_mechanism	string	PLAIN	否	sasl_mechanism
分组Id	group_id	string	--	否	group_id
其中，“sasl连接配置”需要根据kafka规格进行填写。示例如下： • 明文连接配置 org.apache.kafka.common.security.plain.PlainLoginModule required username='*kafka用户* password='*kafka密码*'; • 密文连接配置 org.apache.kafka.common.security.scram.ScramLoginModule required username='*kafka用户名* password='*kafka密码*';					

表 11-13 pipe 连接器配置规则

规则	对应logstash配置项	类型	默认值	是否必填	描述
类型	type	string	租户	是	类型
管道	pipeId	string	--	是	管道id

规则	对应logstash配置项	类型	默认值	是否必填	描述
域账户	domain_name	string	domain_name	是	账户domaionName
用户名	user_name	string	user_name	是	账户user_name
密码	user_password	string	--	是	账户user_password
订阅类型	subscription_type	string	true	否	订阅类型 • Shared：共享模式 • Exclusive：独占模式 • Failover：灾备模式
订阅初始位置	subscription_initial_position	string	true	否	订阅初始位置

表 11-14 elasticsearch 连接器配置规则

规则	对应logstash配置项	类型	默认值	是否必填	描述
主机地址	hosts	array	--	是	主机地址
索引	index	string	--	是	索引
检索语句	query	string	--	是	检索语句
用户名	user	string	--	是	用户名
密码	user_password	string	--	是	密码
查询数量	size	number	20	是	查询数量
卷	scroll	string	5m	是	卷
文档信息	docinfo	boolean	true	是	文档信息
是否配置加密	is_pw_encrypted	boolean	true	是	是否配置加密
是否SSL	ssl	boolean	true	否	是否SSL
证书文件	ca_file	file	--	否	证书文件

规则	对应logstash配置项	类型	默认值	是否必填	描述
是否SSL证书校验	ssl_certificate_verification	boolean	true	否	是否SSL校验

目的连接器

安全云脑租户采集连接器，目前支持的目的连接器类型如下表所示：

表 11-15 目的连接器类型

连接器名称	对应的logstash插件	描述
传输控制协议 TCP	tcp	用于发送TCP协议日志，配置规则请参见**表11-16**。
用户数据协议 UDP	udp	用于发送UDP协议日志，配置规则请参见**表11-17**。
消息队列 KAFKA	kafka	用于将日志写入Kafka消息队列，配置规则请参见**表11-18**。
对象存储 OBS	obs	用于写日志到对象存储OBS桶中，配置规则请参见**表11-19**。
云脑管道 PIPE	pipe	用于将日志写入安全云脑管道中，配置规则请参见**表11-20**。

表 11-16 tcp 连接器配置规则

规则	对应logstash配置项	类型	默认值	是否必填	描述
端口	port	number	1025	是	端口
解码类型	codec	string	plain	是	解码类型，json_lines或者plain • plain：读取原始内容 • json_lines：处理json格式内容
主机地址	host	string	192.168.0.66	是	host地址 注：与节点网络互通

规则	对应logstash配置项	类型	默认值	是否必填	描述
ssl证书	ssl_cert	file	--	否	ssl_cert证书
是否SSL	ssl_enable	boolean	false	否	是否开启ssl
ssl-key文件	ssl_key	file	--	否	ssl_key文件
ssl秘钥	ssl_key_passphrase	string	--	否	ssl_key_passphrase密钥

表 11-17 udp 连接器配置规则

规则	对应logstash配置项	类型	默认值	是否必填	描述
主机地址	host	string	--	是	主机地址 注：与节点网络互通
端口	port	number	1025	是	端口
解码类型	codec	string	json_lines	是	解码类型，json_lines或者plain • plain：读取原始内容 • json_lines：处理json格式内容
重试次数	retry_count	number	3	否	重试次数
重试延迟毫秒数	retry_backoff_ms	number	200	否	重试延迟毫秒数

表 11-18 kafka 连接器配置规则

规则	对应logstash配置项	类型	默认值	是否必填	描述
服务地址	bootstrap_servers	string	--	是	服务地址 eg:192.168.21.21:9092,192.168.21.24:9999
主题	topic_id	string	logstash	是	主题

规则	对应logstash配置项	类型	默认值	是否必填	描述
解码类型	codec	string	plain	是	解码类型，json或者plain
请求体最大长度	max_request_size	number	10485760	是	请求体最大长度
SSL证书	ssl_truststore_location	file	--	否	SSL证书 当选择SSL相关协议时需要填写该参数
SSL秘钥	ssl_truststore_password	string	--	否	SSL秘钥 当选择SSL相关协议时需要填写该参数
安全协议	security_protocol	string	PLAINTEXT	否	安全协议
sasl连接配置	sasl_jaas_config	string	--	否	sasl连接配置
是否加密	is_pw_encrypted	string	true	否	是否加密
sasl机制	sasl_mechanism	string	PLAIN	否	sasl_mechanism
其中，“sasl连接配置”需要根据kafka规格进行填写。示例如下： ● 明文连接配置 org.apache.kafka.common.security.plain.PlainLoginModule required username='*kafka用户* password='*kafka密码*'; ● 密文连接配置 org.apache.kafka.common.security.scram.ScramLoginModule required username='*kafka用户名* password='*kafka密码*';					

表 11-19 obs 连接器配置规则

规则	对应logstash配置项	类型	默认值	是否必填	描述
region	region	string	--	是	region
桶	bucket	string	demo-obs-sec-mrd-datas	是	桶名
endpoint	endpoint	string	--	是	endpoint

规则	对应logstash配置项	类型	默认值	是否必填	描述
缓存文件夹	temporary_directory	string	/temp/logstash/	是	缓存路径
编码类型	codec	string	plain	否	编码格式plain或者json
AK	ak	string	--	否	AK
SK	sk	string	--	否	SK
前缀	prefix	string	test	否	路径前缀
编码格式	encoding	string	gzip	否	编码格式gzip或者纯文件
记忆路径	sincedb_path	string	/opt/cloud/logstash/pipeline/file_name	否	用于设置读取的位置信息，防止重启导致的全文遍历

表 11-20 pipe 连接器配置规则

规则	对应logstash配置项	类型	默认值	是否必填	描述
类型	type	string	租户	是	类型
管道	pipeId	string	--	是	管道
AK	ak	string	--	是	AK 选择平台类型需填写该参数
SK	sk	string	--	是	SK 选择平台类型需填写该参数
域账户	domain_name	string	domain_name	是	账户domain_name 选择租户类型需填写该参数
用户名	user_name	string	user_name	是	账户user_name 选择租户类型需填写该参数

规则	对应logstash配置项	类型	默认值	是否必填	描述
密码	user_password	string	--	是	账户user_password 选择租户类型需填写该参数
压缩类型	compression_type	string	NONE	否	报文压缩类型
队列满阻止	block_if_queue_full	boolean	true	否	队列满阻止进入
启用批处理	enable_batching	boolean	true	否	是否开启批处理

11.1.3.3 管理连接

操作场景

本章节主要介绍如何执行查看连接管理信息、删除数据连接操作。

查看连接管理信息

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，默认进入连接管理页面。

步骤5 在连接管理页面中，查看连接管理的详细信息。

表 11-21 连接管理参数说明

参数名称	参数说明
连接名称	连接的名称。
连接类型	连接的类型
连接信息	连接相关信息。
引用通道	连接被引用的通道数量。
描述	连接相关描述。
操作	支持对连接进行编辑、删除操作。

----结束

删除数据连接

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，默认进入连接管理页面。

步骤5 在连接管理页面中，单击目标连接所在行“操作”列的“删除”。

步骤6 在弹出的确认框中单击“确定”。

----结束

11.1.3.4 创建/编辑解析器

操作场景

安全云脑默认内置快速接入解析器，可根据需要进行选择：

表 11-22 解析器场景说明

类型	场景
快速接入	无需对源数据进行处理直接传输。
模板	需要对数据源进行清理、字段加工处理等操作的时候，可以根据用户需要的使用场景进行模板选择，创建对应的解析器。
自定义	需要对数据源进行清理、字段加工处理等操作的时候，模板中不包含用户需要的使用场景的时候，可以自定义用户的解析器，配置对应的处理规则。

本章节主要介绍创建/编辑解析器。

创建解析器

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

步骤5 支持**•自定义新增**和**•由模板创建**，请根据您的需要进行选择。

- **自定义新增**
  a. 在解析器列表管理页面中，单击“新增”，进入新增解析器页面。
  b. 在新增解析器页面中，进行参数配置。

表 11-23 新增解析器

参数名称		参数说明
基本信息	名称	设置解析器名称。
	描述	输入解析器描述信息。
规则列表		设置解析器解析规则。操作步骤如下： 1. 单击“添加”，并选择规则类型。 ○ 解析规则：选择解析器的解析规则，详细参数说明请参见**解析器规则说明**。 ○ 条件控制：选择解析器的条件控制原则，支持选择“if条件”、“else条件”、“else if条件”。 2. 根据选择的规则配置对应的参数信息。

  c. 设置完成后，单击页面右下角“确定”。

- **由模板创建**
  a. 在解析器管理页面中，选择“模板列表”页签。
  b. 在模板列表页面中，单击目标模板所在行“操作”列的“由模板创建”。
  c. 在新增解析器页面中，进行参数配置。

表 11-24 新增解析器

参数名称		参数说明
基本信息	名称	解析器名称，系统已根据模板自动生成，可进行修改。
	描述	解析器描述信息，系统已根据模板自动生成，可进行修改。

参数名称	参数说明
规则列表	解析器解析规则，系统已根据模板自动生成，可进行修改。 如需添加规则，可以单击“添加”，选择规则类型，并根据选择的规则配置对应的参数信息。 ■ 解析规则：选择解析器的解析规则，详细参数说明请参见**解析器规则说明**。 ■ 条件控制：选择解析器的条件控制原则，支持选择“if条件”、“else条件”、“else if条件”。

d. 设置完成后，单击页面右下角“确定”。

----结束

编辑解析器

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

步骤5 在解析器列表管理页面中，单击目标解析器所在行“操作”列的“编辑”。

步骤6 在编辑解析器页面中，编辑解析器信息。

表 11-25 编辑解析器

参数名称		参数说明
基本信息	名称	设置解析器名称。
	描述	输入解析器描述信息。
规则列表		设置解析器解析规则。操作步骤如下： 单击“添加”，并选择规则类型。 ● 解析规则：选择解析器的解析规则，详细参数说明请参见**解析器规则说明**。 ● 条件控制：选择解析器的条件控制原则。

步骤7 设置完成后，单击页面右下角“确定”。

----结束

11.1.3.5 解析器规则说明

租户采集功能主要使用定制化logstash用于数据中转业务，解析器是对logstash中filter部分的无码化封装。目前，支持如下类型的logstash插件：

表 11-26 支持的类型

解析器	对应logstash中的插件	说明
kv解析	kv	键值对解析，解析规则请参见**表11-27**。
mutate解析	mutate	mutate解析，解析规则请参见**表11-28**。
grok解析	grok	正则解析，解析规则请参见**表11-29**。
date解析	date	时间解析，解析规则请参见**表11-30**。
drop解析	drop	报文删除。无具体规则，选择该规则，即可删除当前传入的日志记录。
prune解析	prune	黑白名单解析，解析规则请参见**表11-31**。
csv解析	csv	csv格式解析，解析规则请参见**表11-32**。
函数解析	ruby	云脑自封装ruby解析，解析规则请参见**表11-33**。
json解析	json	json处理转化，解析规则请参见**表11-34**。
Split解析	split	切割解析，解析规则请参见**表11-35**。
Clone解析	clone	克隆解析，解析规则请参见**表11-36**。
uuid解析	uuid	uuid解析，解析规则请参见**表11-37**。

表 11-27 kv 解析

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
源字段	source	string	source	是	要翻译的字段
目标字段	target	string	message	否	目标字段
字段切割	field_split	string	,	否	字段切割
值切割	value_split	string	=	否	字段切割
去除字段空格	trim_key	string	--	否	去除key中的空格

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
去除值空格	trim_value	string	--	否	去除value中的空格
允许重复	allow_duplicate_values	boolean	true	否	允许重复
默认字段	default_keys	array	--	否	添加key
排除字段	exclude_keys	array	--	否	排除key
包含字段	include_keys	array	--	否	包含key
前缀匹配	prefix	string	--	否	前缀匹配
递归解析	recursive	boolean	true	否	递归解析
字段转化	transform_key	string	--	否	key的转换
添加字段	add_field	hash	--	否	添加字段
添加Tag	add_tag	array	--	否	添加tag
移除字段	remove_field	array	--	否	移除字段
移除Tag	remove_tag	array	--	否	移除tag
id标记	id	string	--	否	id标记
空白策略	whitespace	string	strict/lenient	否	空白策略
字段修剪	remove_char_key	string	<>[](),	否	字段修剪

表 11-28 mutate 解析

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
类型转化	convert	hash	--	否	类型转化
数组联合	join	hash	--	否	数组联合
转为小写	lowercase	array	--	否	转化为小写
默认字段	coerce	hash	--	否	默认字段
字段改名	rename	hash	--	否	字段改名
字段改值	replace	hash	--	否	字段改值
字段分割	split	hash	--	否	字段分割

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
去除空格	strip	array	--	否	去除空格
更新字段	update	hash	--	否	更新字段
转化大写	uppercase	array	--	否	转化为大写
添加字段	add_field	hash	--	否	添加字段
添加Tag	add_tag	array	--	否	添加tag
移除字段	remove_field	array	--	否	移除字段
移除Tag	remove_tag	array	--	否	移除tag
ID标记	id	string	--	否	id标记
字段复制	copy	hash	--	否	字段复制
gsub值替换	gsub	array	--	否	gsub值替换

表 11-29 grok 解析

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
正则匹配	match	hash	--	是	正则匹配
第一匹配	break_on_match	boolean	true	否	正则匹配跳出
覆盖字段	overwrite	array	message	否	覆盖字段
添加字段	add_field	hash	--	否	添加字段
添加Tag	add_tag	array	--	否	添加tag
移除字段	remove_field	array	--	否	移除字段
移除Tag	remove_tag	array	--	否	移除tag
ID标记	id	string	--	否	id标记

表 11-30 date 解析

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
正则匹配	match	array	--	是	正则

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
目标字段	target	string	timestamp	是	目标字段
添加字段	add_field	hash	--	否	添加字段
添加Tag	add_tag	array	--	否	添加tag
移除字段	remove_field	array	--	否	移除字段
移除Tag	remove_tag	array	--	否	移除tag
ID标记	id	string	test	否	id标记
locale	locale	string	--	否	locale
时区	timezone	string	+8:00	否	timezone

表 11-31 prune 解析

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
黑名单字段	blacklist_names	array	--	否	黑名单字段
黑名单值	blacklist_values	array	--	否	黑名单值
白名单字段	whitelist_names	array	--	否	白名单字段
白名单值	whitelist_values	array	--	否	白名单值

表 11-32 csv 解析

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
解析字段	source	string	message	否	解析字段
列字段	columns	array	--	否	列字段
切割符	separator	string	,	否	切割符
跳过空列	skip_empty_columns	boolean	true	否	跳过空列

表 11-33 函数解析

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
长度过滤	filter_length	number	10	否	长度过滤
设置时间	set_time	ruby_time	123	否	设置时间

表 11-34 json 解析

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
解析字段	source	string	message	是	解析源
跳过异常	skip_on_invalid_json	boolean	true	否	跳过异常json解析
添加字段	add_field	hash	null	否	添加字段
添加Tag	add_tag	array	null	否	添加tag
移除字段	remove_field	array	null	否	移除字段
移除Tag	remove_tag	array	null	否	移除tag
目标字段	target	string	message	否	目标字段

表 11-35 split 解析器解析规则

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
字段	field	string	message	是	需要切割的字段

表 11-36 clone 解析器解析规则

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
克隆	clones	array	--	是	需要克隆的字段列表

表 11-37 uuid 解析器解析规则

解析规则	对应的logstash配置项	类型	默认值	是否必填	描述
目标字段	target	string	uuid	是	目标字段
是否覆盖	overwrite	boolean	true	是	是否覆盖

11.1.3.6 管理解析器

操作场景

本章节主要介绍如何执行**查看解析器管理信息**、**导入解析器**、**导出解析器**、**删除解析器**操作。

查看解析器管理信息

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

步骤5 在解析器管理页面中，查看解析器的详细信息。

表 11-38 解析器管理参数说明

参数名称	参数说明
名称	解析器的名称。
引用通道	解析器被引用的通道数量。
描述	解析器相关描述。
操作	支持对解析器进行编辑、删除等操作。

步骤6 在解析器管理页面中，选择“模板列表”页签，进入模板列表页面。

步骤7 在模板列表页面中，查看解析器模板信息。

表 11-39 模板参数说明

参数名称	参数说明
名称	解析器模板名称。
描述	解析器模板相关描述。
操作	支持对解析器模板进行创建解析器操作。

----结束

导入解析器

说明

- 仅支持导入json格式的文件，且文件大小不超过1MB。
- 一次最多支持导入5个解析器文件，且每个解析器文件最多支持包含100个解析器。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

步骤5 在解析器列表管理页面中，单击解析器列表左上角的“导入”，弹出导入文件对话框。

步骤6 在弹出的导入文件对话框中，单击“添加文件”，选择需要导入的json文件。

注意

- 仅支持导入json格式的文件，且文件大小不超过1MB。
- 一次最多支持导入5个解析器文件，且每个解析器文件最多支持包含100个解析器。

步骤7 选择完成后，单击“确认”，完成导入。

导入成功后，可以在解析器列表中查看导入的解析器信息。

----结束

导出解析器

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

步骤5 在解析器列表管理页面中，勾选需要导出的解析器，并单击列表上方的“导出”。

系统将自动下载.json格式的解析器文件到本地。

----结束

删除解析器

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

步骤5 在解析器管理页面中，单击目标解析器所在行“操作”列的“删除”。

步骤6 在弹出的确认框中单击“确定”。

----结束

11.1.3.7 新增/编辑采集通道

操作场景

本章节主要介绍如何新增/编辑采集通道。

新增分组

新增采集通道前，需先新增分组。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

步骤5 新增分组。

1. 在采集通道管理页面中，单击“分组列表”右侧的。
2. 输入分组名称，并单击，完成新增。

分组新增完成后，如需编辑/删除，可以将鼠标悬停在分组名称后，单击编辑/删除按钮，进行编辑/删除操作。

----结束

新增采集通道

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

步骤5 在采集通道管理页面的分组列表右侧，单击“新增”，进入新增采集通道页面。

步骤6 在“基础配置”页面中，配置基础信息。

表 11-40 基础配置参数说明

参数名称		参数说明
基础信息	名称	自定义采集通道名称。
	通道分组	选择采集通道所属分组。
	（可选）描述	输入采集通道描述信息。
来源配置	源名称	选择采集通道来源名称。 选择后系统将自动生成已选择来源的相关信息。
目的配置	目的名称	选择采集通道目的名称。 选择后系统将自动生成已选择目的相关信息。

步骤7 基础配置完成后，单击页面右下角“下一步”，进入“解析器配置”页面。

步骤8 在“解析器配置”页面中，选择解析器，选择后，系统将显示已选择解析器的相关信息。

如果无可选解析器或需新增解析器，可以单击“新建”，新建解析器。新增解析器详细操作请参见**创建/编辑解析器**。

步骤9 解析器配置完成后，单击页面右下角“下一步”，进入“运行节点选择”页面。

步骤10 在“运行节点选择”页面中，单击“新增”，并在弹出的添加节点框中选择节点后，单击“确认”。

- 运行参数：节点添加后，如果需要在已添加节点中配置运行参数，请参照以下步骤进行处理：

a. 在节点列表中，单击目标节点所在行“操作”列的“运行参数”按钮。

b. 单击“添加配置”，设置运行键和运行值。

如果用户需要对采集通道的运行参数做优化，此处提供了pipeline.batch.size、pipeline.workers、pipeline.batch.delay三个可选优化参数，用户可以根据自身业务情况进行优化。如果无需优化，直接删除相关的配置即可。

表 11-41 参数配置说明

参数	类型	说明
pipeline.batch.size	int	配置每个worker线程每次收集event的数量，配置越大越有效率，但同理，内存开销也会增大，可以在jvm.options中配置增加堆空间。
pipeline.workers	int	pipeline中的worker线程数配置，默认是CPU的核数。
pipeline.batch.delay	int	设置当前pipe提交延迟时间，设置此时间可以提升消息提交次数，提升系统消耗。

- 移除节点：节点添加后，如需移除，请在节点列表中，单击目标节点所在行“操作”列的“移除”按钮，已添加节点将被移除。

步骤11 运行节点选择完成后，单击页面右下角“下一步”，进入“通道详情预览”页面。

步骤12 在“通道详情预览”页面确认配置无误后，单击“保存并执行”。

当采集通道状态为“正常”，表示当前采集通道下发已经全部成功。采集通道状态代表的含义如下表所示：

表 11-42 采集通道状态

监控状态	说明
健康	采集通道下发成功。
异常	采集通道下发部分成功，部分异常。
故障	采集通道下发尚未成功。此状态为心跳上报状态，存在一定延迟，一般下发成功后，30秒之后会恢复监控状态。

----结束

编辑采集通道

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

步骤5 在采集通道管理列表中，单击目标通道所在行“操作”列的“更多 > 编辑”，进入编辑采集通道页面。

步骤6 在“基础配置”页面中，配置基础信息。

表 11-43 基础配置参数说明

参数名称		参数说明
基础信息	名称	自定义采集通道名称。
	通道分组	选择采集通道所属分组。
	（可选）描述	输入采集通道描述信息。
来源配置	源名称	选择采集通道来源名称。 选择后系统将自动生成已选择来源的相关信息。
	目的名称	选择采集通道目的名称。 选择后系统将自动生成已选择目的的相关信息。

步骤7 基础配置完成后，单击页面右下角“下一步”，进入“解析器配置”页面。

步骤8 在“解析器配置”页面中，选择解析器，选择后，系统将显示已选择解析器的相关信息。

如果无可选解析器或需新增解析器，可以单击“新建”，新建解析器。新增解析器详细操作请参见**创建/编辑解析器**。

步骤9 解析器配置完成后，单击页面右下角“下一步”，进入“运行节点选择”页面。

步骤10 在“运行节点选择”页面中，单击“新增”，并在弹出的添加节点框中选择节点后，单击“确认”。

- 运行参数：节点添加后，如在已添加节点中运行参数，请参照以下步骤进行处理：
  a. 在节点列表中，单击目标节点所在行“操作”列的“运行参数”按钮。
  b. 单击“添加配置”，设置运行键和运行值。
- 移除节点：节点添加后，如需移除，请在节点列表中，单击目标节点所在行“操作”列的“移除”按钮，已添加节点将被移除。

步骤11 运行节点选择完成后，单击页面右下角“下一步”，进入“通道详情预览”页面。

步骤12 在“通道详情预览”页面确认配置无误后，单击“保存并执行”。

----结束

11.1.3.8 管理采集通道

操作场景

本章节主要介绍如何执行**查看采集通道**、**删除采集通道**、**启用/停止/重启采集通道**操作。

查看采集通道

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

步骤5 在采集通道管理页面中，查看采集通道的详细信息。

表 11-44 采集通道参数说明

参数名称	参数说明
分组列表	采集通道分组列表及各分组名称。
名称	采集通道的名称。
连接信息	采集通道连接信息。
创建人	采集通道的创建人。
健康状态	采集通道的状态。
接收速率	采集通道的接收速率。
发送速率	采集通道的发送速率。
配置状态	采集通道的配置状态。
通道实例	采集通道数量。
运行状态	采集通道的运行状态。
操作	支持对采集通道进行编辑、停止等操作。

----结束

删除采集通道

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

步骤5 在采集通道管理列表中，单击目标通道所在行“操作”列的“更多 > 删除”。

说明

只有当采集通道处于停止状态，才能执行删除操作。

步骤6 在弹出的确认框中单击“确定”。

----结束

启用/停止/重启采集通道

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

步骤5 在采集通道管理列表中，单击目标通道所在行“操作”列的启用/停止/重启。

步骤6 在弹出的确认框中单击“确定”。

----结束

11.1.3.9 查看采集节点信息

操作场景

本章节主要介绍如何查看采集节点信息。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 采集管理”，进入采集管理页面后，选择“采集节点管理”页签，进入采集节点管理页面。

步骤5 在采集节点管理页面中，查看采集节点的详细信息。

当节点较多时，可以通过搜索功能快速查询指定节点。

如需查看某个节点的详细信息，可单击节点名称，在右侧弹出的详情页面进行查看。

表 11-45 节点参数说明

参数名称	参数说明
节点名称/ID	节点的名称/ID。
健康状态	节点的健康状态。
区域	节点所在区域。
IP地址	节点的IP地址。
CPU使用率	节点的CPU使用率。
内存使用率	节点的内存使用率。
磁盘使用率	节点的磁盘使用率。
网络速率	节点的网络速率。
标签	节点的标签信息。
心跳过期失联标识	节点是否心跳过期失联。 15分钟内没有心跳则节点将标记为“失联”。

----结束

11.1.4 升级组件控制器

操作场景

租户采集原组件控制器采用salt方案，考虑到业务的发展，在设计上采用了agent的方式，需要将原有agent进行升级操作，即将租户采集salt-minion升级到isap-agent。

说明

升级不影响数据面。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 注销节点。

1. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面后，单击目标节点所在行“操作”列的“注销”。
2. 在弹出的确认框中，单击“确定”。

节点注销成功，且“健康状态”显示为“失联”。

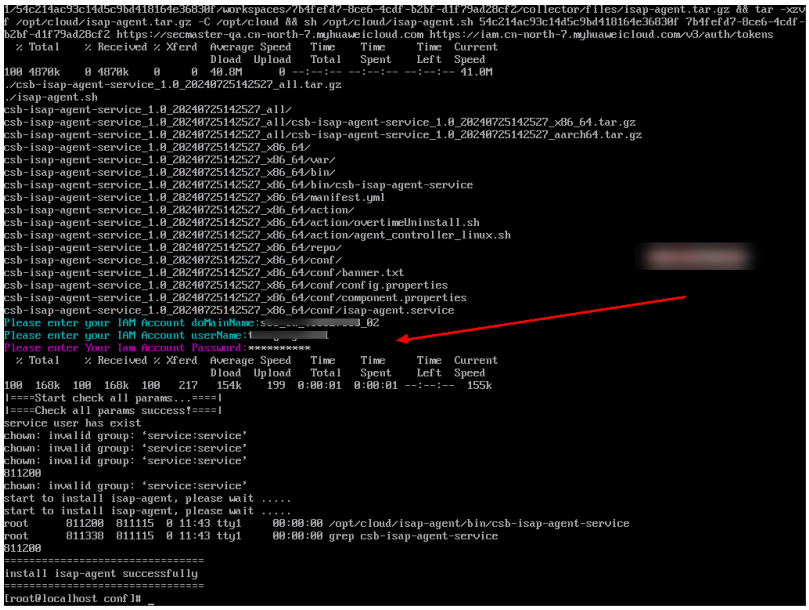
步骤5 复制脚本。

1. 在节点管理页面中，单击“新增”。
2. 在新增节点页面中，单击“下一步”，并在脚本验证页面中，复制脚本。

步骤6 安装组件控制器。

1. 使用远程管理工具（例如：Xftp、SecureFX、WinSCP、PuTTY、Xshell等）登录失联ECS节点。
2. 粘贴复制的**步骤5.2**复制的安装命令，以root权限执行，在ECS中安装Agent。

图 11-10 安装 agent



3. 根据界面提示，输入账号信息及密码。
4. 如果界面回显类似如下信息时，则表示Agent安装成功。
   ```
   install isap-agent successfully
   ```
5. 安装成功后，在安全云脑控制台的节点管理页面中，查看节点的状态。

步骤7 删除旧的管理通道。

1. 在“设置 > 组件管理 > 节点管理”页面中，单击“新增”，并在新增节点页面中，分别单击两个**管理通道**所在行操作列的“删除”。
2. 在弹出的确认框中，单击“确定”。

----结束

11.2 数据集成

11.2.1 支持接入的日志

安全云脑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 11-46 支持接入的日志

安全分类	服务	服务类型	日志	日志描述
主机安全	企业主机安全（HSS）	租户侧云服务	hss-alarm	主机安全告警
			hss-vul	主机漏洞扫描结果
			hss-log	主机安全日志
应用安全	Web应用防火墙（WAF）	租户侧云服务	waf-attack	WAF攻击日志
			waf-access	WAF访问日志
	云审计服务（CTS）	租户侧云服务	cts-audit	云审计服务日志
运维安全	云堡垒机（CBH）	租户侧云服务	cbh-audit	堡垒机审计日志

11.2.2 接入数据

操作场景

安全云脑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。

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

数据集成操作成功后，日志数据订阅预计在十分钟内生效。

接入服务日志

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 数据集成”，进入云服务日志接入页面。

步骤5 在待接入云产品的“审计相关日志”列，单击 ，开启接入的云服务日志。

如需接入当前region所有支持的云产品的日志，可直接单击“一键接入服务日志”前的 按钮，一键接入当前region所有云服务日志。

步骤6 设置生命周期。

系统默认存储数据7天，您可以根据需要进行设置。

步骤7 设置是否自动转告警。

在待设置云产品的“自动转告警”列，单击，开启接入的云服务日志满足告警条件时，自动转为告警，并且在“告警管理”页面中进行展示。

说明

- 如果此处未开启自动转告警，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。
- 在安全云脑的“漏洞管理”页面可以接入主机漏洞扫描结果，如果数据集成操作时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”将不会展示主机相关的漏洞扫描情况。

步骤8 单击“保存”，并在弹出的配置保存框中，单击“确定”。

说明

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

查看日志数据的存储位置

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 数据集成”，进入数据集成页面后，在云产品接入表格的“存储位置”列查看日志数据存储位置。

查看后，可以前往目标工作空间的对应管道查看接入的日志数据。

----结束

相关操作

- 取消数据接入
  a. 在待取消接入云产品的“审计相关日志”列，单击，关闭接入的云服务日志。
  b. 单击“保存”。
- 编辑数据接入生命周期
  a. 在待编辑云产品的“生命周期”列，输入生命周期时间。
  b. 单击“保存”。
- 取消自动转告警
  a. 在待取消云产品的“自动转告警”列，单击，关闭告警映射。
  b. 单击“保存”。

11.3 目录定制

操作场景

安全云脑支持自定义目录，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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 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 11-47 目录参数说明

参数名称	参数说明
一级目录	目录所属的一级目录名称。
二级目录	目录所属的二级目录名称。
目录状态	目录所属的类型。
目录地址	目录所在地址。
布局	目录关联的布局。
发布者	目录的发布者。
操作	可对目录进行更换布局等操作。

----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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“设置 > 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

12 常见问题

12.1 产品咨询

12.1.1 为什么没有看到攻击数据或者看到的攻击数据很少?

安全云脑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，安全云脑可能会显示您的系统当前遭受的攻击程度较低。

12.1.2 安全云脑的数据来源是什么?

安全云脑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。

安全云脑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。

12.1.3 安全云脑与其他安全服务之间的关系与区别?

SecMaster与其他安全防护服务（WAF、HSS、Anti-DDoS、DBSS）的关系与区别如下：

- 关联：

  SecMaster：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SecMaster中，呈现全局安全威胁攻击态势。

- 区别：

  SecMaster：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。

SecMaster与其他安全防护服务区别，详细内容如表12-1。

表 12-1 SecMaster 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
安全云脑（SecMaster）	安全管理	SecMaster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SecMaster。	保障企业业务稳定性。
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SecMaster。	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SecMaster，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SecMaster。	保障云上数据库安全和资产安全。

12.1.4 SecMaster 与 HSS 服务的区别?

服务含义区别

- 安全云脑（SecMaster）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，SecMaster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

- SecMaster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 12-2 SecMaster 与 HSS 主要功能区别

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。	• SecMaster：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	-	• SecMaster：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。	• SecMaster：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	-	• SecMaster：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	-	• SecMaster：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。

12.1.5 如何更新安全评分?

安全云脑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。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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“安全态势 > 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。

说明

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

12.1.6 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。

安全云脑联动企业主机安全（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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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“威胁运营 > 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

12.1.7 数据同步或数据一致性相关问题

为什么 WAF、HSS 中的数据和 SecMaster 中的数据不一致?

由于SecMaster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SecMaster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，安全云脑将在**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。

12.2 数据采集故障排查

12.2.1 组件控制器安装失败

数据采集时，需要在ECS上安装组件控制器（isap-agent），当出现安装失败等问题时，请参照本章节进行排查处理：

排查过程中，常用命令请参见**组件控制器常用命令**。

可能原因

组件控制器（isap-agent）安装失败的可能原因如下：

- 待安装组件控制器（isap-agent）的ECS服务器与存储Agent的OBS桶之间网络不通
- ECS服务器的磁盘空间不足
- workspaceId校验失败
- 组件控制器（isap-agent）已经安装，系统仍将重复安装

原因排查及解决方法

- **待安装组件控制器（isap-agent）的ECS服务器与存储Agent的OBS桶之间网络不通**

  图 12-1 主机与 OBS 网络不通

  解决方法：
  - （可选）方法一：将ECS主机与OBS的网络连通。
  - （可选）方法二：手动将安装脚本以及安装包下载到本地后，再将安装包上传到主机的“/opt/cloud”路径下。
    i. 登录OBS管理控制台。
    ii. 在左侧导航栏选择“桶列表”，并单击目标桶名称，进入桶对象管理页面。
    iii. 单击目标桶对象名称，进入桶对象详情页面后，下载安装脚本和安装包。
    iv. 通过远程管理工具（如：SecureFX、WinSCP）远程登录目标云服务器。
    v. 将安装包上传到主机的“/opt/cloud”路径下。
- **ECS主机的磁盘空间不足**

  图 12-2 磁盘空间不足

  解决方法：

  清理磁盘，预留足够空间。
- **workspaceId校验失败**

- **问题现象**

  当日志出现如下图所示信息时，则表示Workspace ID校验失败。

  图 12-3 workspaceId 校验失败

  ```
  start to install isap-agent, please wait.....
  start to install isap-agent, please wait.....
  start to install isap-agent, please wait.....
  start to install isap-agent, please wait.....
  start to install isap-agent, please wait.....
  workspaceId error, install isap-agent fail
  ```

- **解决方法**

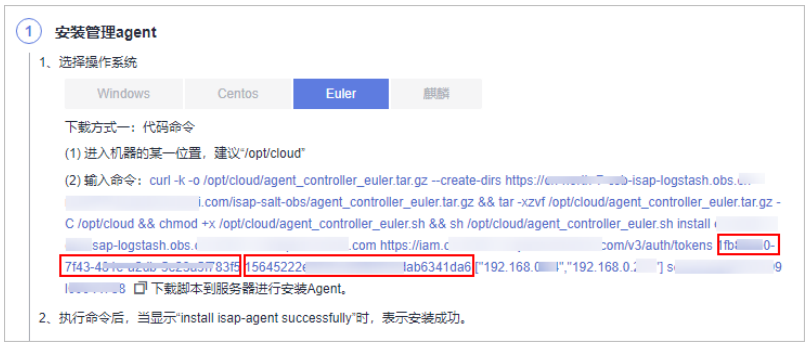
  i. 登录安全云脑管理控制台。

  ii. 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。

  iii. 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，单击目标节点名称。

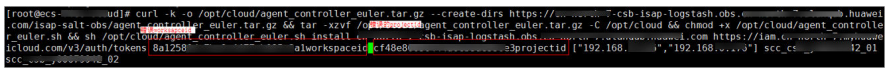
  iv. 查看执行命令中的workspaceId和projectId。

  图 12-4 控制台中的参数信息

  v. 查看实际运行命令中的workspaceId和projectId，是否与**iv**中的一致。

  图 12-5 命令中的参数信息

  vi. 修改实际执行命令中的workspaceId和projectId。

- **组件控制器（isap-agent）已经安装，系统仍将重复安装**

  - **问题现象**

    当日志出现如下图所示信息时，则表示Agent已经安装。

    图 12-6 Agent 重复安装

    ```
    warning: group servicegroup does not exist - using root
    warning: user service does not exist - using root
    warning: group servicegroup does not exist - using root
    warning: user service does not exist - using root
    warning: group servicegroup does not exist - using root
    The ISAP-salt-minion-euler has been installed. Do not install the ISAP-salt-minion-euler again.
    [root@ecs          i]#
    ```

  - **解决方法**

    i. （可选）方法一：通过管理控制台注销该节点。

1) 登录安全云脑管理控制台。
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。
3) 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，单击目标节点所在行“操作”列的“注销”。
4) 在弹出的确认框中，单击“确认”。

ii. （可选）方法二：通过脚本命令卸载组件控制器（isap-agent）。

1) 通过远程管理工具（如：SecureFX、WinSCP）远程登录目标云服务器。
2) 执行**sh /opt/cloud/agent_controller_euler.sh uninstall**命令，卸载组件控制器。

iii. 检查是否已完成卸载。

1) 通过远程管理工具（如：SecureFX、WinSCP）远程登录目标云服务器。
2) （可选）方法一：执行**ls -a /opt/cloud/**查看“/opt/cloud”目录下的文件，当提示如下图所示信息（只有脚本文件）时，则表示已完成卸载。

图 12-7 脚本文件

3) （可选）方法二：执行**salt-minion --version**命令，当提示如下图所示信息时，则表示已卸载完成。

图 12-8 检查 isap-agent 信息

注意

节点注销需要一定的时间，不建议执行完注销立刻安装。

12.2.2 采集节点或采集通道故障

问题现象

采集节点状态和采集通道健康状态采用isap-agent定时上报机制，虽然存在一定的延迟（预计一分钟），但是在采集通道下发3分钟后，采集节点和采集通道的“健康状态”依然显示为“故障”，并且该服务器的CPU使用率或内存使用率即将达到100%。

图 12-9 采集节点故障

图 12-10 采集通道故障

可能原因

用户配置的连接器或解析器在语法或者语义上存在错误，导致采集器无法正常运行，不断重启导致CPU、内存被占满。

问题定位

1. 远程登录采集节点所在的ECS。
   - 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机。
   - 如果您的主机已经绑定了弹性IP，您也可以使用远程管理工具（例如：Xftp、SecureFX、WinSCP、PuTTY、Xshell等）登录主机，并使用root账号在主机中安装组件控制器。
2. 执行如下命令，命令查看当前系统的运行状态：

   top

   当显示如下图所示时，则表示ECS中Java进程占用了大量CPU资源。

   图 12-11 运行状态

```
top - 19:21:09 up 8 days, 29 min,  2 users,  load average: 1.04, 0.29, 0.13
Tasks:  84 total,   1 running,  83 sleeping,   0 stopped,   0 zombie
%Cpu(s): 95.8 us,  3.7 sy,  0.0 ni,  0.5 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  3879596 total,   532820 free,  1234536 used,  2112240 buff/cache
KiB Swap:        0 total,        0 free,        0 used.  2295348 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
29442 root      20   0 4731800   1.0g  15528 S 190.3 27.9   0:44.63 java
29245 root      20   0  353640  30420  16508 S   0.7  0.8   0:00.23 dockerd
29425 root      20   0   11780   5464   2740 S   0.7  0.1   0:00.02 containerd-shim
    9 root      20   0       0      0      0 S   0.3  0.0   1:41.10 rcu_sched
23490 root      20   0  830056   9704   4360 S   0.3  0.3   0:02.47 csb-isap-agent-
```

3. 执行如下命令，查看采集器运行日志：

   docker logs isap-logstash -f

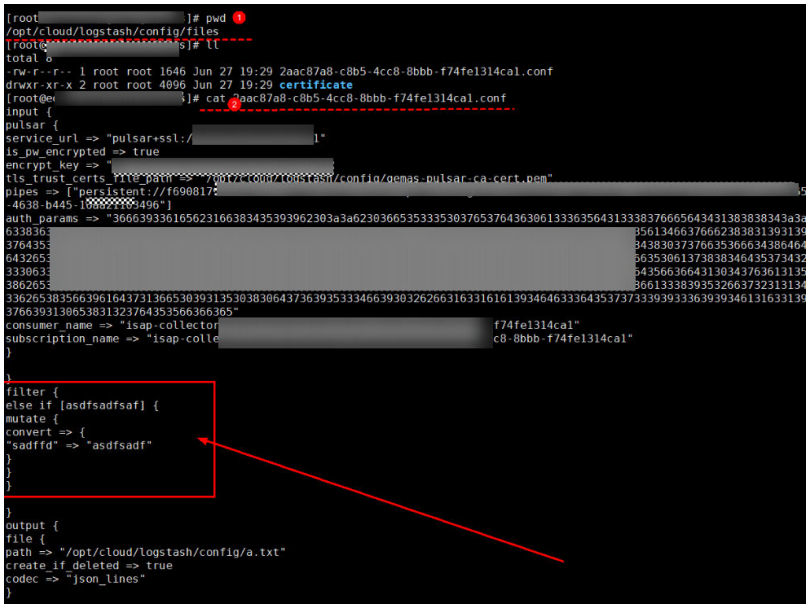
   通过查看日志，定位到当前采集通道filter部分（解析器）配置有误，如下图所示：

   图 12-12 采集器运行日志

```
=75, -XX:+UseConcMarkSweepGC, -Xmn1024M, -Djava.awt.headless=true, -Djruby.jit.threshold=0]
19:29:52.441 [main] INFO  logstash.settings - Creating directory {:setting=>"path.queue", :path=>"/opt/cloud/logstash/data/queue"}
19:29:52.452 [main] INFO  logstash.settings - Creating directory {:setting=>"path.dead_letter_queue", :path=>"/opt/cloud/logstash/data/dead_letter_queue"}
19:29:53.071 [LogStash::Runner] INFO  logstash.agent - No persistent UUID file found. Generating new UUID {:uuid=>"496252c6-e46b-4e48-82b3-1b3d27664db2", :path=>"/opt/cloud/logstash/data/uuid"}
19:29:54.574 [Api Webserver] INFO  logstash.agent - Successfully started Logstash API endpoint {:port=>9600, :ssl_enabled=>false}
19:29:56.063 [Converge PipelineAction::Create<2aac87a8-c8b5-4cc8-8bbb-f74fe1314ca1>] ERROR logstash.agent - Failed to execute action {:action=>LogStash::PipelineAction::Create/pipeline_id:2aac87a8-c8b5-4cc8-8bbb-f74fe1314ca1, :exception=>"LogStash::ConfigurationError", :message=>"Expected one of [ \\t\\r\\n], \"#\", \"{\" at line 15, column 6 (byte 1463) after filter {\nelse ", :backtrace=>["/opt/cloud/logstash/logstash-core/lib/logstash/compiler.rb:32:in `compile_imperative'", "org/logstash/execution/AbstractPipelineExt.java:189:in `initialize'", "org/logstash/execution/JavaBasePipelineExt.java:72:in `initialize'", "/opt/cloud/logstash/logstash-core/lib/logstash/java_pipeline.rb:48:in `initialize'", "/opt/cloud/logstash/logstash-core/lib/logstash/pipeline_action/create.rb:52:in `execute'", "/opt/cloud/logstash/logstash-core/lib/logstash/agent.rb:388:in `block in converge_state'"]}
19:29:56.151 [LogStash::Runner] INFO  logstash.runner - Logstash shut down.
19:29:56.160 [LogStash::Runner] FATAL org.logstash.Logstash - Logstash stopped processing because of an error: (SystemExit) exit
org.jruby.exceptions.SystemExit: (SystemExit) exit
        at org.jruby.RubyKernel.exit(org/jruby/RubyKernel.java:747) ~[jruby-complete-9.2.20.1.jar:?]
        at org.jruby.RubyKernel.exit(org/jruby/RubyKernel.java:710) ~[jruby-complete-9.2.20.1.jar:?]
        at opt.cloud.logstash.lib.bootstrap.environment.<main>(/opt/cloud/logstash/lib/bootstrap/environment.rb:94) ~[?:?]
Using bundled JDK: /opt/cloud/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
WARNING: Could not find logstash.yml which is typically located in $LS_HOME/config or /etc/logstash. You can specify the path using --path.settings. Continuing using the defaults
```

4. 执行以下命令，进入采集通道配置文件所在路径。
   cd /opt/cloud/logstash/config/files
5. 执行以下命令，查看filter部分是否存在异常。
   cat *配置文件名*
   当出现如下图所示内容时，则表示当前filter部分存在异常：

图 12-13 filter 部分存在异常



处理步骤

步骤1 登录安全云脑管理控制台，并进入目标工作空间。

步骤2 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

步骤3 单击目标解析器所在行操作列的“编辑”，并在编辑页面中，删除错误配置信息，修改为正确的配置信息。

图 12-14 问题解析器配置

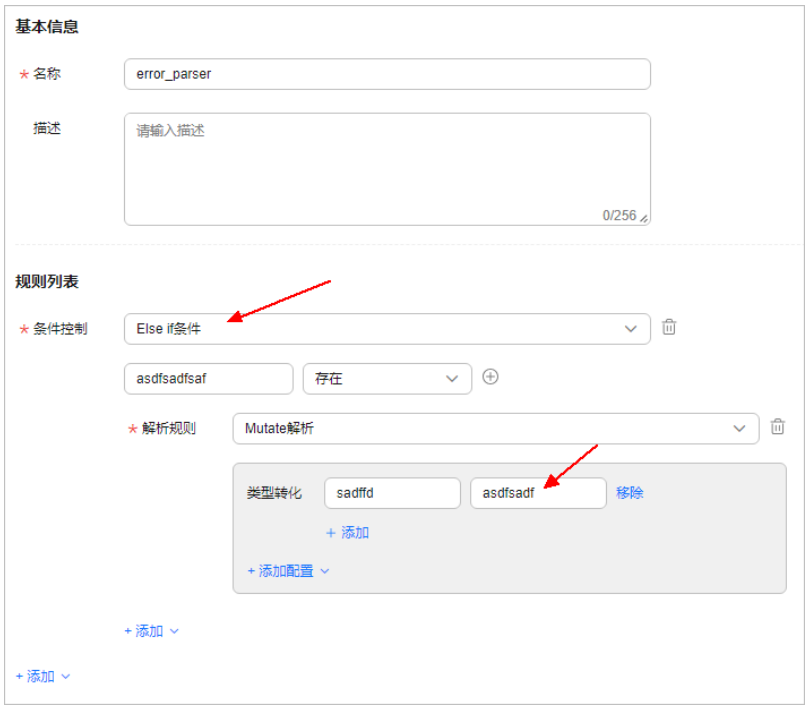
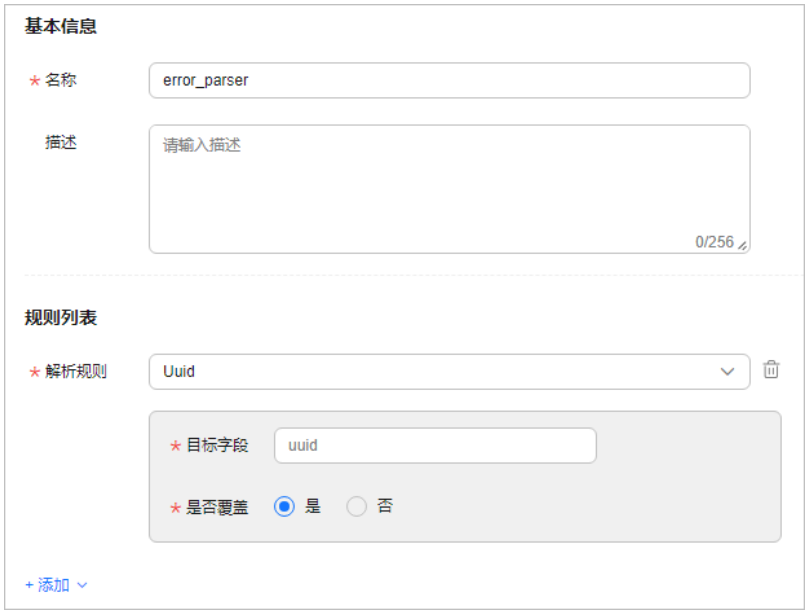


图 12-15 修改解析器配置



步骤4 单击“确定”。

步骤5 编辑完成后，在上方选择“采集通道管理”页签，并单击目标采集通道操作列的“重启”，重启采集通道。

步骤6 检查采集通道和采集节点状态。

- 重启完成后，在“采集通道管理”页面中，检查目标采集通道的健康状态。
- 在上方选择“采集节点管理”页签，页面，检查目标采集节点的健康状态。

当采集通道和采集节点的“健康状态”均显示为“正常”时，则表示问题处理成功。

----结束

12.2.3 组件控制器常用命令

如果组件控制器（isap-agent）安装失败，在故障排查过程中，可能需要使用命令进行处理，其中，常用命令如下：

- 重启

  sh /opt/cloud/isap-agent/action/agent_controller_linux.sh restart

  说明：使用此命令将先停止isap-agent进程，并重新启动该进程。此命令用于isap-agent启动失败，或者节点因为机器故障导致的进程不存在情况。

- 启动

  sh /opt/cloud/isap-agent/action/agent_controller_linux.sh start

  说明：当isap-agent因为机器宕机，容灾自拉起时间未到，用户可使用此命令启动isap-agent。

- 停止

  sh /opt/cloud/isap-agent/action/agent_controller_linux.sh stop

  说明：此命令用于停止isap-agent，使用此命令将自动清理定时自拉起检测，使得isap-agent进程停止。

- 查看进程

  ps -ef|grep isap-agent

  说明：此命令用于查看当前机器上isap-agent是否存在。

- 查看日志

  tail -100f /opt/cloud/isap-agent/log/run.log

  说明：用于查看isap-agent服务，最近100行日志，用于通过日志定位agent异常问题。

- 磁盘分区

  sh /opt/cloud/isap-agent/action/agent_controller_linux.sh partition

  说明：用于在节点安装采集器，手动挂载磁盘，并进行磁盘分区的场景。

A 修订记录

发布日期	修改记录
2024-10-30	第三次正式发布。 ● 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“新增/编辑应急策略”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“资产大屏”章节内容，更新指标含义说明。 ● 更新“新增资产连接”章节内容，补充资产连接含义、作用等描述信息。 ● 优化数据采集资料内容，补充操作步骤说明。

发布日期	修改记录
2024-06-30	第二次正式发布。 ● 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“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。 ● 新增“策略管理”章节，支持统一管理应急策略。 ● 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。 ● 新增支持标签功能，新增“管理工作空间标签”章节内容。 ● 新增“一键阻断/解封”章节内容。 ● 更新“安全编排概述”章节内容，更新剧本和流程描述信息。
2024-02-23	第一次正式发布。