安全云脑

快速入门

文档版本 04

发布日期 2024-02-29

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 入门指引

安全云脑（SecMaster）是华为云原生的新一代安全运营中心，集华为云多年安全经验，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。

本文档介绍使用专业版安全云脑的流程，具体流程如下所示：

表 1-1 使用流程

序号	操作项		说明
1	**购买安全云脑**		介绍如何购买专业版安全云脑和增值包功能（安全大屏、智能分析和安全编排）。
2	**配置服务授权**		购买安全云脑后，需要进行授权，才能正常使用安全云脑。
3	**新增工作空间**		创建安全云脑顶层工作台——工作空间。
4	接入数据	**接入资产**	在工作空间内开启资产订阅，同步当前账号资产相关信息至目标工作空间。
		接入日志数据	接入WAF、HSS、OBS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，实现集中运维。
5	配置/启用相关功能	**配置策略**	通过策略配置可以开通、配置和使用七层安全防线，实现全流程安全防护。
		启用模型	开启智能建模后会通过模型实现告警、事件、情报等信息的自动提取。
		启用剧本	通过剧本实现告警、事件、威胁情报的自动化闭环。
		执行基线检查	检查云上资产的关键配置项，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。

序号	操作项	说明
6	**报告管理**	设置报告信息，实现安全报告自动发送。
7	**安全运营**	配置完成后，便可以针对集成的数据执行资产管理、检测威胁、调查告警等操作。

2 购买安全云脑

本章节介绍如何通过**包周期**方式购买**专业版**安全云脑和**增值包**功能。

版本信息说明

安全云脑提供有基础版、标准版、专业版供您选择，各版本的功能差异请参见**服务版本差异**，计费相关差异请参见**计费说明**。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 在总览页面中，单击右上角“购买安全云脑”，进入购买安全云脑页面。

步骤4 在购买安全云脑页面，配置购买参数。

图 2-1 包周期购买专业版

表 2-1 包周期购买专业版参数说明

参数名称	说明
计费模式	此处选择“包周期”，按配置周期计费。
区域	选择您所在的区域。
版本	选择“专业版”。
主机配额	主机配额是指主机资产支持防护的最大主机数量。 请根据当前账户下所有主机资产总数设置配额数，可设置最大主机配额需等于或大于当前账户下主机总数量，且不支持减少。 **说明** • 主机配额最大限制为10000台。 • 为避免主机资产在防护份额外，不能及时感知攻击威胁，而造成数据泄露等安全风险。当主机资产数量增加后，请及时增加配额数。
增值包	开通/购买“安全大屏”、“智能分析配额”功能“安全编排”功能。
标签	如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签，也可以直接在购买安全云脑时创建标签。

参数名称	说明
购买时长	选择“购买时长”。单击时间轴的点，选择购买时长，可以选择1个月～3年的时长。 **说明** 勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤5 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤6 确认订单详情无误后，阅读并勾选《安全云脑服务(SecMaster)免责声明》，单击“去支付”。

步骤7 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

3 配置服务授权

当您**首次**使用安全云脑时，需要先进行授权，才能正常访问，如果已经授权，请跳过该步骤。

前提条件

已完成IAM账号授权操作，详细操作请参见**IAM账号授权**。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 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”，进入工作空间管理页面。

图 3-1 工作空间管理页面

步骤4 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。

图 3-2 服务委托授权

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

----结束

4 新增工作空间

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。

在安全云脑前，需要创建工作空间，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。

约束与限制

- 付费版本安全云脑：单账号单Region内最多创建5个工作空间。
- 免费版本安全云脑：单账号单Region内最多创建1个工作空间。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 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”，进入工作空间管理页面。

图 4-1 工作空间管理页面

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。
项目类型	选择待新增工作空间所属的项目类型。 当选择为“企业项目”时，需要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。 如需使用该功能，请**开通企业管理功能**。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 **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

5 接入数据

5.1 接入资产

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，资产信息将在一分钟内同步展示。

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 在页面左上角单击 ☰，选择“安全与合规 > 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。

图 5-1 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。

图 5-2 资产管理

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

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，资产信息将在一分钟内同步展示。

----结束

5.2 接入日志数据

安全云脑支持集成WAF、HSS、OBS等多种华为云云产品的日志数据。集成后，可以检索并分析所有收集到的日志。

接入服务日志

步骤1 登录管理控制台。

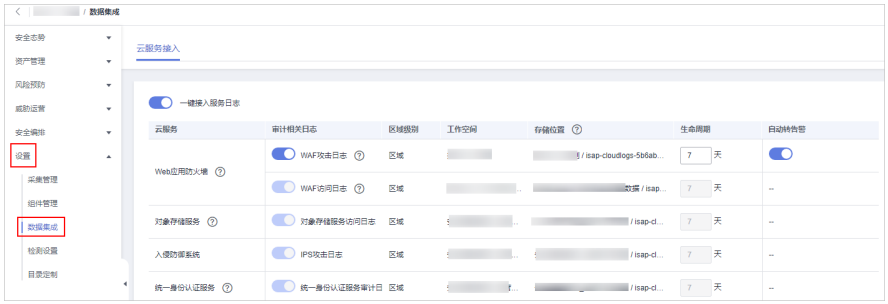
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

图 5-3 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。

图 5-4 数据集成页面



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。

建议直接单击“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，建议保持默认即可。

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。

步骤8 单击“保存”。

接入完成后，将创建默认数据空间和管道。

----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”。

6 配置/启用相关检查

6.1 配置策略

通过策略配置可以开通、配置和使用七层安全防线，实现全流程安全防护。

本章节以配置**应用防线**的**WAF**防护策略为例进行介绍。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 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。

图 6-1 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”，默认进入防线策略管理页面。

图 6-2 进入防线策略管理页面

步骤5 单击应用防线名称，右侧滑出应用防线对应的云产品信息。

步骤6 在WAF页签中，单击“防护策略”，进入WAF防护策略配置页面。

如果还未购买WAF，请在产品介绍描述信息中单击产品名称“Web应用防火墙”，进入WAF控制台页面后，单击“购买WAF实例”，进入购买WAF页面，参见**购买WAF**开通WAF产品。

步骤7 在WAF防护策略配置，选择“策略管理”页签，进入策略管理页面后，单击列表的左上角的“添加防护策略”。

步骤8 在弹出的对话框中，输入策略名称，单击“确认”，添加的策略会展示在策略列表中。

步骤9 在目标策略所在行，单击策略名称，进入防护规则配置页面，参见**配置防护规则**为策略添加防护规则。

----结束

6.2 启用告警模型

数据接入后，可以利用模型对数据进行扫描，如果在模型设置范围内容，将产生告警提示。

需要使用以下内置的模板创建告警模型并启用模型：

应用-WAF关键攻击告警、主机-虚拟机横向连接、网络-高危端口对外暴露、网络-登录爆破告警、主机-疑似外联、网络-源ip对多个目标进行攻击、网络-命令注入告警、网络-恶意外联、主机-反弹shell、主机-恶意程序、应用-分布式url遍历攻击、应用-源ip进行url遍历、主机-高危命令检测、应用-源ip对域名进行爆破攻击、主机-暴力破解成功、主机-异常shell、主机-弱口令、主机-异地登录、主机-rootkit事件。

创建告警模型

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 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。

图 6-3 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。

图 6-4 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。

图 6-5 模型模板详情

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。

- 管道名称：选择该告警模型的执行管道。依赖的执行管道名称可根据描述中的“使用约束”选择。

图 6-6 获取管道名称

- 其他参数建议保持默认值即可。

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，建议保持默认即可。

如需进行配置，详细操作请参见**新建告警模型**。

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”。

步骤12 重复**步骤5**-**步骤11**为其他模板创建告警模型。

----结束

启用告警模型

步骤1 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。

图 6-7 可用模型页面

步骤2 在模型列表中，勾选所有需要启动的模型，然后单击列表左上角的“启用”。

步骤3 当模型状态更新为启用，则表示启动模型成功。

----结束

6.3 启用剧本

接入数据后，针对云上安全事件提供了安全编排剧本，实现安全事件的高效、自动化响应处置。

- 流程：内置流程默认已启用，无需手动操作。
- 剧本：部分高频剧本默认启用，具体如下：

  主机告警状态同步、高危漏洞自动通知、主机防线告警关联历史处置信息、云脑WAF地址组关联策略、应用防线告警关联历史处置信息、网络防线告警关联历史处置信息、重复告警自动关闭、告警ip指标打标、资产防护状态统计通知、未关闭告警自动统计通知、高危告警自动通知

  若还需开启未默认启用的剧本，可参考下述操作步骤进行处理。

操作步骤

步骤1 登录管理控制台。

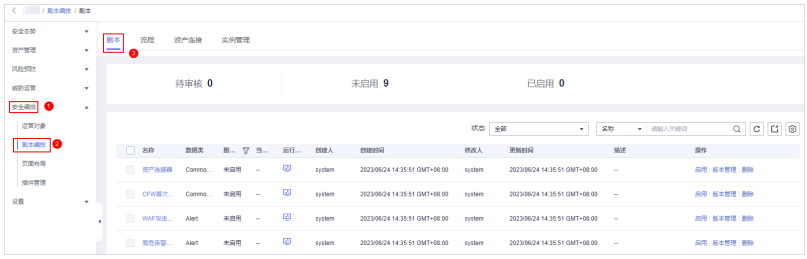
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

图 6-8 进入目标工作空间管理页面

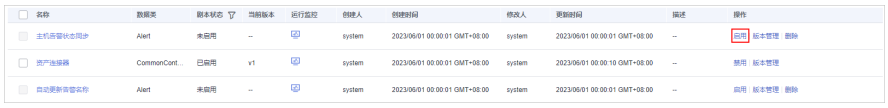
步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 6-9 进入剧本管理页面



步骤5 在剧本页面中，单击目标剧本所在行“操作”列的“启用”。

图 6-10 启用剧本



步骤6 在弹出启用确认信息框中，选择启用的剧本版本v1，并单击“确认”。

----结束

6.4 执行基线检查

接入数据后，需要执行基线检查，以便检查云上资产的关键配置项。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。

建议启用以下检查规范：**安全上云合规检查1.0**

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 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。

图 6-11 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”，并在基线检查页面右上角单击“立即检查”，立即执行扫描任务。

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。

图 6-12 立即检查

----结束

7 创建报告

设置报告信息，实现安全报告自动发送。

创建安全报告

步骤1 登录管理控制台。

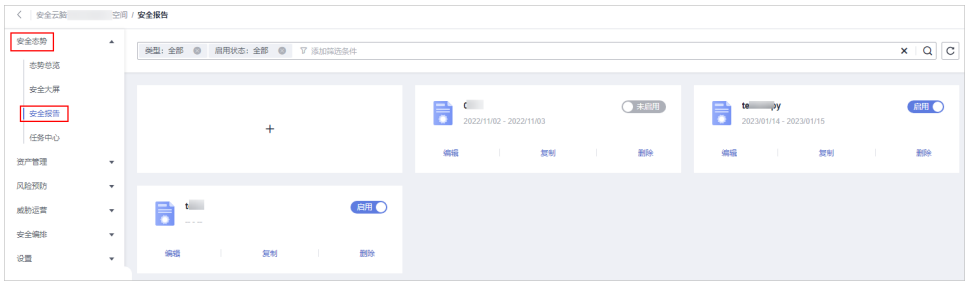
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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。

图 7-1 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 7-2 进入安全报告页面



步骤5 在安全报告页面中单击 + 按钮，进入配置报告基本信息页面。

步骤6 配置报告基本信息。

表 7-1 报告基本信息参数说明

参数名称	参数说明
报告名称	自定义报告名称。
报告类型	选择报告类型。 ● 日报：默认统计前一天00:00~24:00的安全信息。 ● 周报：默认统计上一周安全信息，上周一00:00到上周日24:00。 ● 月报：默认统计上一月安全信息，上月第一天00:00到上月最后一天24:00。 ● 自定义：自定义选择时间范围。
统计周期	根据您选择的“报告类型”显示安全报告统计周期。 当“报告类型”选择“日报”、“周报”或“月报”时，系统会根据您选择的“报告类型”显示安全报告统计周期。
报告发送时间	当“报告类型”选择为“日报”、“周报”或“月报”时，需要设置报告发送时间。 ● 日报：设置为每天报告的发送时间点，默认发送前一天00:00:00~23:59:59的安全信息报告。 ● 周报：设置为每周报告的发送时间点，默认发送上周一00:00到上周日24:00的安全信息报告。 ● 月报：设置为每月报告的发送时间点，默认发送前一个月整月的安全信息报告。
报告发送频次	当“报告类型”选择“自定义”时，需要选择安全报告的发送频次。
发送规则	当“报告类型”选择“自定义”时，需要设置报告的发送时间以及统计范围。 最多可添加5个发送规则。
邮件标题	设置报告发送邮件的标题信息。
报告接收人邮箱	添加接收人邮箱地址。 ● 最多可添加100个邮箱地址。 ● 有多个邮箱地址，请使用英文逗号隔开。例如：test01@example.com,test02@example.com
（可选）抄送	添加抄送人邮箱地址。 ● 最多可添加100个邮箱地址。 ● 有多个邮箱地址，请使用英文逗号隔开。例如：test03@example.com,test04@example.com
（可选）备注	自定义安全报告的备注信息。

步骤7 单击右上角“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，选择已有报告布局。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

  a. 单击右侧预览页面左上角的  。
  b. 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。

- 全屏查看报告：单击右侧预览页面左上角的  ，可以全屏查看安全报告。

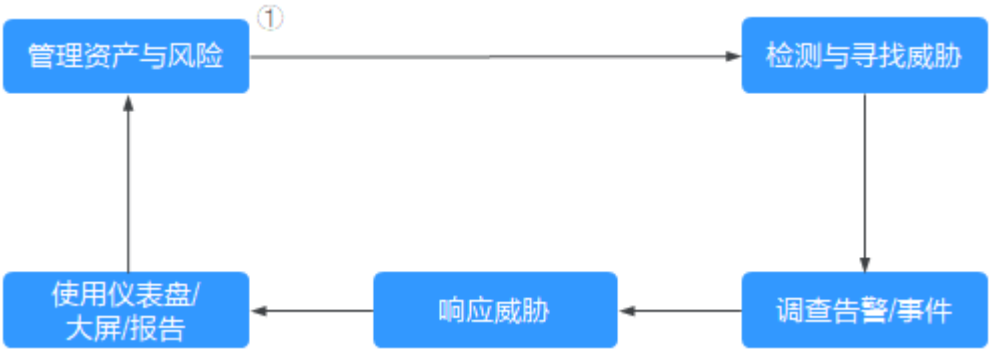
步骤9 单击右下角“完成”，返回安全报告管理页面，即可查看创建的安全报告。

----结束

8 安全运营

配置完成后，便可以针对集成的数据执行资产管理、检测威胁、调查告警等操作。

图 8-1 安全运营



步骤 1：管理资产与风险

安全运营的本质指安全风险管理，根据ISO的定义，其三要素包括“资产”，“脆弱性”和“威胁”。因此，梳理您要防护的资产，是安全运营的业务流起点。

- **资产管理**

  安全云脑可以帮助您：

  - 将云上资产从不同租户、不同Region汇集到一个视图中。
  - 将云外资产导入到安全云脑中，并标记其所属的环境。
  - 将资产的风险情况标识出来，例如：是否有不安全的配置、是否有OS或者应用漏洞、是否存在疑似入侵的告警、是否覆盖了对应的防护云服务（例如：ECS上应该安装HSS的Agent、域名应纳入到WAF的防护策略中）。

  更多详细介绍及操作请参见**资产管理**。

- **检查并清理不安全的配置**

  在安全运营过程中，最常见的“脆弱性”是不安全的配置。安全云脑基于安全合规经验，形成自动化检查的基线，按照业界通用的规范标准，提供基线检查包。

  - 云服务中的配置可以自动检查。如：IAM是否按角色进行授权分数、VPC的安全组中是否存在完全放通的策略、WAF的防护策略是否开启等。您可以根据“详情”中建议的方法，对配置进行加固。

  更多详细介绍及操作请参见**基线检查**。

- **发现并修复漏洞**

  在修复配置类风险之后，安全云脑还可以帮助您，发现并修复安全漏洞。支持检测Linux软件漏洞、Windows系统漏洞、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。

  更多详细介绍及操作请参见**漏洞管理**。

步骤 2：检测与寻找威胁

数据源连接到安全云脑后，我们已经清点了要保护的资产，并查找及修复了不安全的配置和漏洞，接下来就是识别可疑活动和威胁。

安全云脑可提供多种内置的由安全专家和分析团队根据已知威胁、常见攻击媒介和可疑活动上报链设计的模板，使你能够执行某些对应操作时收到此类威胁的通知。启用这些模板后，它们将自动在整个环境中搜索可疑活动。同时，可以根据你的需要自定义模板，以搜索或筛选出活动。

同时，还支持云服务安全日志数据检索、分析功能，提供专业级的安全分析能力，实现对云负载、各类应用及数据的安全保护。

更多详细介绍及操作请参见**模型模板**、**安全分析**。

步骤 3：调查告警与事件

- **调查告警**

  威胁检测模型分析大量的安全云服务日志，找到疑似入侵的行为，即告警。安全云脑中的告警包含如下字段：名称、等级、发起可疑行为的资产/威胁、遭受可疑行为的资产。安全值班人员，需要在较短的时间内对告警做出判定。如果风险较低，则关闭告警（如：重复告警、运维操作）；如果风险较高，需要单击“转事件”，将告警转为事件。

  更多详细介绍及操作请参见**查看告警信息**、**告警转事件**。

- **调查事件**

  告警转成事件后，就可以在事件管理中查看到生成的事件，事件生成后可以进行调查分析。您可以在事件上关联与可疑行为相关的实体：资产（如：VM）、情报（如：攻击源IP）、账号（如：泄露的账号）、进程（如：木马）等；也可以关联历史上相似的其他告警或事件。

  更多详细介绍及操作请参见**查看事件信息**、**编辑事件**。

步骤 4：响应威胁

利用实时自动化，您可以通过对重复类型的告警实现常规响应自动化来减少告警研判工作量。同时，也可以利用自动化的剧本，完成自动化止血操作。

更多详细介绍及操作请参见**安全编排**。

步骤 5：使用总览仪表盘、大屏、报告

- **总览仪表盘**

  实时呈现当前工作空间中资源整体安全评估状况，实现云上安全态势一览和风险统一管控。

- **安全大屏**
  - 综合态势感知：可以还原攻击历史，感知攻击现状，预测攻击态势，呈现安全运营的全局指标情况。
  - 值班响应大屏：可以查看未处理告警、事件、漏洞、基线等需要处理的安全风险事项。
  - 资产大屏：可以查看资产总数、受攻击资产数、未防护资产数等需要处理的资产以及资产视角的风险情况。
  - 威胁态势大屏：可以查看DDoS攻击次数、网络攻击次数、应用拦截次数、主机层拦截次数等威胁攻击趋势及其防御、检测情况。
  - 脆弱性大屏：可以查看脆弱性资产、漏洞、基线、未防护资产等脆弱性配置或资产的趋势及分布。
- **安全报告**

  展示安全评分、基线检查结果、安全漏洞、策略覆盖等信息，您可以通过创建安全报告，及时掌握资产的安全状况数据。

更多详细介绍及操作请参见**态势总览**、**安全大屏**、**安全报告**。

9 入门实践

当您完成了新增工作空间、采集数据、配置并启用了相关检查等基本操作后，可以根据业务需求使用安全云脑提供一系列实践。

表 9-1 常用实践

实践	描述
安全看板	安全看板可以联动其他云安全服务，实时呈现云上资产整体安全评估状况，集中展示云上安全。
资产管理	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。
安全分析	介绍如何同时管理多个云产品的安全告警和日志，并对告警及日志进行聚合分析，获取攻击信息、主动搜寻威胁。
自动化处理安全事件	介绍如何通过安全编排功能对安全事件进行自动化响应处置，实现安全运维的自动化编排和快速响应。
数据转入转出操作指导	介绍如何采用多种方式采集各类日志数据，以及如何对采集的日志数据进行解析、转出、可视化查询、威胁建模等操作。

A 修订记录

发布日期	修改记录
2024-02-29	第四次正式发布。 更新**启用告警模型**、**启用剧本**章节内容，优化描述信息。
2023-10-30	第三次正式发布。 ● 新增**配置策略**、**创建报告**章节内容。 ● 更新**入门指引**章节内容，优化描述信息。 ● 优化章节结构。
2023-07-15	第二次正式发布。 新增**入门实践**章节。
2023-06-20	第一次正式发布。