

安全云脑

# 快速入门

文档版本 06  
发布日期 2025-01-22



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI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 购买和使用安全云脑基础版.....	1
2 购买和使用安全云脑标准版.....	6
3 购买和使用安全云脑专业版.....	12
4 入门实践.....	25

# 1 购买和使用安全云脑基础版

## 操作场景

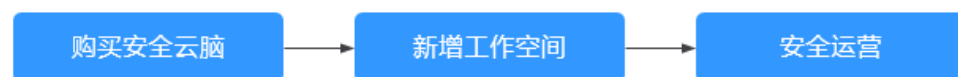
安全云脑（SecMaster）是华为云原生的新一代安全运营中心，旨在为用户提供一站式的云上安全管理解决方案。通过安全云脑，用户可以实现对云上资产、安全态势、安全信息和事件的集中管理，从而提升安全运营效率和响应速度。

本文档将以首次在亚太-曼谷区域购买如下配置的安全云脑，并使用首个工作空间的默认配置进行安全运营的场景为例进行介绍：

- 计费模式：包周期
- 版本：基础版
- 主机配额：50

此场景的操作流程如下所示：

图 1-1 操作流程



## 操作流程

操作步骤	说明
<b>准备工作</b>	注册华为账号、开通华为云，赋予SecMaster权限。
<b>步骤一：购买安全云脑基础版</b>	购买安全云脑，选择版本（本文以基础版为例）、配额数等信息。
<b>步骤二：新增工作空间</b>	新增首个用于安全运营的工作空间。
<b>步骤三：安全运营</b>	首个工作空间新增完成后，安全云脑将自动进行空间初始化操作。初始化完成后，将可以进行体验安全云脑功能。

## 准备工作

1. 在购买SecMaster之前，请先注册华为账号并开通华为云。具体操作详见[注册华为账号并开通华为云](#)。  
如果您已开通华为云，请忽略此步骤。
2. 请确保已为账号赋予“SecMaster FullAccess”权限。具体操作请参见[创建用户并授权使用SecMaster](#)。  
购买安全云脑时，还需要为账号授予“BSS Administrator”权限。

## 步骤一：购买安全云脑基础版

安全云脑提供了“基础版”、“标准版”、“专业版”供您使用，包括态势感知、基线检查、查询与分析以及安全编排等功能。

本步骤以购买基础版为例进行参数设置及介绍，更多购买安全云脑详细配置请参见[购买安全云脑](#)。

1. [登录华为云管理控制台](#)。
2. 在页面上方选择区域后，在服务列表中选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑控制台。
3. 在总览页面中，单击“购买安全云脑”后，在弹出的访问授权页面中，勾选同意授权并单击“确认”。
4. 在购买安全云脑页面，配置购买参数。  
本示例中仅解释必要参数，其他参数请根据实际情况进行选择。

表 1-1 购买安全云脑参数配置说明

参数	示例	说明
计费模式	包周期	选择安全云脑的“包周期”计费模式。
区域	亚太-曼谷	根据已有云上资源所在的区域选择安全云脑的区域。
版本	基础版	安全云脑提供有基础版、标准版、专业版供您选择，请根据您的需求进行选择，各版本的功能差异请参见 <a href="#">产品功能</a> 。
配额数	1	配额数是指支持防护的最大ECS主机资产数量。请根据当前账户下所有ECS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。 <ul style="list-style-type: none"><li>• 配额数最大限制为10000台。</li><li>• 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。</li></ul>
购买时长	1个月	根据需求选择购买时长。

5. 确认参数配置无误后，在页面右下角单击“立即购买”。

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”。
7. 在支付页面，选择付款方式完成付款，完成购买操作。
8. 单击“返回安全云脑控制台”，返回安全云脑控制台页面。

## 步骤二：新增工作空间

工作空间（Workspace）属于安全云脑顶层工作台，使用安全云脑功能前，需要先新增工作空间。

1. 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 1-2 工作空间管理页面



2. 在弹出的授权页面中，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”。

由于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。

3. 在工作空间管理页面中，单击“新增”，并配置工作空间参数。  
本示例中仅解释必要参数，其他参数请根据实际情况进行选择。

表 1-2 新增工作空间参数配置说明

参数	示例	说明
区域	亚太-曼谷	根据待查看的云上资源所在的区域选择创建工作空间的区域。
项目类型	普通项目	选择工作空间所属的项目。
工作空间名称	SecMaster	安全运营工作空间的名称。

4. 单击“确定”。

## 步骤三：安全运营

首个工作空间新增完成后，安全云脑将自动进行空间初始化操作。初始化完成后，可以进行体验安全云脑功能。

1. 管理资产与风险

安全运营的本质指安全风险管理的本质，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，还可以将云外资产导入到安全云脑中，并标记其所属的环境。汇聚后，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）等，方便查看资产的安全状态。

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[安全治理](#)、[基线检查](#)。

- 使用总览仪表盘展示当前工作空间中资源的安全评分，快速了解当前的安全状况。

更多详细介绍及操作请参见[态势总览](#)。

## 相关信息

体验安全云脑基础版后，如果需要运用安全云脑进行高效运营，并灵活融合业务需求，可以选购标准版或专业版，进一步接入多样化的数据源，激活全方位的模型与剧本功能，以实现更深层次、更全面的分析与运营策略制定：

- 接入日志数据**：接入华为云云服务日志数据，以统一管理日志信息，以及检索并分析所有收集到的日志，可以实时监控系统和网络的安全状态，及时发现异常行为和潜在威胁。
- 采集数据**：接入非华为云日志数据，整合和分析来自不同来源的信息，从而提供更全面的安全视角，可以更深入、全面地分析，方便快速定位系统故障的原因，加速问题解决过程。
- 漏洞管理**：在修复配置类风险之后，安全云脑还可以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、网站漏洞，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，帮助您实时了解漏洞情况。
- 查看告警信息**：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。安全运营人员需要对告警做出分析判定。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。
- 查看事件信息**：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，分析后对事件发起应急响应。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。
- 新建告警模型**：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。
- 安全分析**：提供了日志数据检索功能，帮助筛选威胁。

- **启用剧本**：通过剧本实现安全事件的高效、自动化响应处置，降低安全事件的平均响应时间（MTTR），提高整体的安全防护能力。
- **配置防线策略**：通过配置防线策略，联动其他安全服务，以便构建一个多层次、全方位的安全防护体系。
- **新增应急策略**：通过配置应急策略，可以迅速有效地应对网络安全威胁，限制或阻止来自特定IP地址的访问，从而保护网络资源和用户数据的安全。
- **创建安全报告**：可以自动发送安全态势报告，展示安全评分、基线检查结果、安全漏洞、策略覆盖等信息，方便及时掌握资产的安全状况数据。
- **安全大屏**：查看资源的实时态势并处理攻击事件等，可以帮助安全运营团队实时监控和分析各种安全威胁和事件，从而做出快速响应。



# 2 购买和使用安全云脑标准版

## 操作场景

安全云脑实现了开箱即用，即默认在每个区域（Region）的首个工作空间中自动加载当前区域的所有资产，以及接入推荐的云服务日志数据，并启用精选预置模型和剧本。无需进行繁琐的手动配置，简化了使用流程并提升了效率。后续新增的用于自定义运营的工作空间，不会自动加载数据与资产，需要用户自定义处理。

购买安全云脑并新增首个工作空间完成后，您将可以在安全云脑中执行查看资源安全态势、统一管理资产、全面分析日志数据和自动化安全编排处理事件等操作，帮助您为您的资产构建一个全面的安全防御体系，实现自动化的安全运营和管理工作，满足您的安全需求。

本文档将以首次在亚太-曼谷区域购买如下配置的安全云脑，并使用首个工作空间的默认配置进行安全运营的场景为例进行介绍：

- 计费模式：包周期
- 版本：标准版
- 主机配额：50

此场景的操作流程如下所示：

图 2-1 操作流程



## 操作流程

操作步骤	说明
准备工作	注册华为账号、开通华为云，赋予SecMaster权限。
步骤一：购买安全云脑标准版	购买安全云脑，选择版本（本文以标准版为例）、主机配额等信息。
步骤二：新增工作空间	新增首个用于安全运营的工作空间。

操作步骤	说明
<b>步骤三：安全运营</b>	<p>每个区域的首个工作空间新增完成后，安全云脑将自动进行空间初始化操作。初始化完成后，将可以进行管理资产、检查与寻找威胁、调查告警、响应威胁等安全运营操作，同时，还可以使用仪表盘、大屏等查看安全态势。</p> <p>初始化操作包括接入云上当前区域当前账号中的所有资产、接入推荐的云服务日志数据（例如，WAF攻击日志）、并启用精选预置模型（例如，主机异常网络连接）和剧本（例如，高危漏洞自动通知）。</p>

## 准备工作

1. 在购买SecMaster之前，请先注册华为账号并开通华为云。具体操作详见[注册华为账号并开通华为云](#)。  
如果您已开通华为云，请忽略此步骤。
2. 请确保已为账号赋予“SecMaster FullAccess”权限。具体操作请参见[创建用户并授权使用SecMaster](#)。  
购买安全云脑时，还需要为账号授予“BSS Administrator”权限。

## 步骤一：购买安全云脑标准版

安全云脑提供了“基础版”、“标准版”、“专业版”供您使用，包括态势感知、基线检查、查询与分析以及安全编排等功能。

本步骤以购买标准版为例进行参数设置及介绍，更多购买安全云脑详细配置请参见[购买安全云脑](#)。

1. [登录华为云管理控制台](#)。
2. 在页面上方选择区域后，在服务列表中选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑控制台。
3. 在总览页面中，单击“购买安全云脑”后，在弹出的访问授权页面中，勾选同意授权并单击“确认”。
4. 在购买安全云脑页面，配置购买参数。

表 2-1 购买安全云脑参数配置说明

参数	示例	说明
计费模式	包周期	选择安全云脑的“包周期”计费模式。
区域	亚太-曼谷	根据已有云上资源所在的区域选择安全云脑的区域。
版本	标准版	安全云脑提供有基础版、标准版、专业版供您选择，请根据您的需求进行选择，各版本的功能差异请参见 <a href="#">产品功能</a> 。

参数	示例	说明
配额数	50	配额数是指支持防护的最大ECS主机资产数量。请根据当前账户下所有ECS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。 <ul style="list-style-type: none"><li>配额数最大限制为10000台。</li><li>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。</li></ul>
安全大屏	关闭	确认是否需要使用安全云脑提供的“安全大屏”功能，是否需要增配“日志审计”、“安全分析”或“安全编排”功能。如果需要购买，请根据您的需要设置对应的购买量。 增值包说明、配置推荐详细介绍请参见 <a href="#">增值包说明</a> 。
日志审计	暂不购买	
安全分析	暂不购买	
安全编排	暂不购买	
标签	<ul style="list-style-type: none"><li>标签键：<b>test</b></li><li>标签值：<b>01</b></li></ul>	为安全云脑绑定标签，用来标识资源。标签更多详细介绍请参见 <a href="#">增值包说明</a> <a href="#">标签管理服务</a> 。
购买时长	1个月	根据需求选择购买时长，“按需”模式无需配置。 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。

5. 确认参数配置无误后，在页面右下角单击“立即购买”。
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”。
7. 在支付页面，选择付款方式完成付款，完成购买操作。
8. 单击“返回安全云脑控制台”，返回安全云脑控制台页面。

## 步骤二：新增工作空间

工作空间（Workspace）属于安全云脑顶层工作台，使用安全云脑功能前，需要先新增工作空间。

1. 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 2-2 工作空间管理页面



- 在弹出的授权页面中，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”。

由于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。

- 在工作空间管理页面中，单击“新增”，并配置工作空间参数。  
本示例中仅解释必要参数，其他参数请根据实际情况进行选择。

表 2-2 新增工作空间参数配置说明

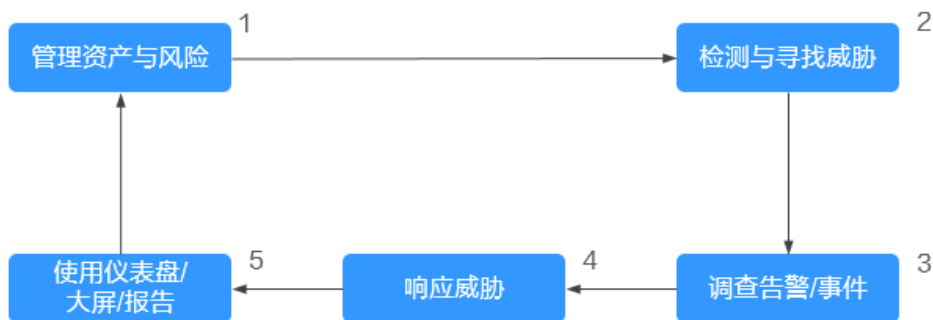
参数	示例	说明
区域	亚太-曼谷	根据待查看的云上资源所在的区域选择创建工作空间的区域。
项目类型	普通项目	选择工作空间所属的项目。
工作空间名称	SecMaster	安全运营工作空间的名称。

- 单击“确定”。

### 步骤三：安全运营

首个工作空间新增完成后，安全云脑将自动进行空间初始化操作。初始化完成后，将可以进行管理资产、检查与寻找威胁、调查告警、响应威胁等安全运营操作，同时，还可以使用仪表盘、大屏等查看安全态势。

图 2-3 安全运营



- 管理资产与风险

安全运营的本质指安全风险的管理，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，还可以将云外资产导入到安全云脑中，并标记其所属的环境。汇聚后，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)等,方便查看资产的安全状态。

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[安全治理](#)、[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、网站漏洞,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,帮助您实时了解漏洞情况。

更多详细介绍及操作请参见[漏洞管理](#)。

### 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型,使您能够执行某些对应操作时收到此类威胁的通知。启用这些模型后,它们将自动在整个环境中搜索可疑活动。同时,可以根据您的需要自定义模型,以搜索或筛选出威胁。

同时,提供了日志数据检索功能,帮助您筛选威胁。

更多详细介绍及操作请参见[模型模板](#)、[安全分析](#)。

### 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。安全运营人员需要对告警做出分析判定。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,分析后对事件发起应急响应。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](#)。

### 4. 响应威胁

当您在告警、事件进行响应时,可以使用剧本来做自动化处置,提高效率。

更多详细介绍及操作请参见[安全编排](#)。

### 5. 使用总览仪表盘、大屏、报告

- **总览仪表盘**  
展示当前工作空间中资源的安全评分，快速了解当前的安全状况。
  - **安全大屏**  
查看资源的实时态势并处理攻击事件等，可以帮助安全运营团队实时监控和分析各种安全威胁和事件，从而做出快速响应。
  - **安全报告**  
可以自动发送安全态势报告，展示安全评分、基线检查结果、安全漏洞、策略覆盖等信息，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](#)。

## 相关信息

在运用安全云脑进行高效运营的基础上，您还能灵活融合业务需求，进一步接入多样化的数据源，激活全方位的模型与剧本功能，以实现更深层次、更全面的分析与运营策略制定：

- **接入日志数据**：接入华为云云服务日志数据，以统一管理日志信息，以及检索并分析所有收集到的日志，可以实时监控系统和网络的安全状态，及时发现异常行为和潜在威胁。

### 说明

建议将安全云脑管理的资产以及资产的告警、基线检查结果、漏洞数据、日志数据接入同一个工作空间，便于统一运营，进行安全分析关联。

- **采集数据**：接入非华为云日志数据，整合和分析来自不同来源的信息，从而提供更全面的安全视角，可以更深入、全面地分析，方便快速定位系统故障的原因，加速问题解决过程。
- **新建告警模型**：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。
- **启用剧本**：通过剧本实现安全事件的高效、自动化响应处置，降低安全事件的平均响应时间（MTTR），提高整体的安全防护能力。
- **执行基线检查**：通过执行基线检查可以帮助您评估当前系统、软件、数据库等的安全状态、识别安全风险、防范潜在威胁以及满足合规性要求等。
- **配置防线策略**：通过配置防线策略，联动其他安全服务，以便构建一个多层次、全方位的安全防护体系。
- **新增应急策略**：通过配置应急策略，可以迅速有效地应对网络安全威胁，限制或阻止来自特定IP地址的访问，从而保护网络资源和用户数据的安全。
- **创建安全报告**：可以自动发送安全态势报告，展示安全评分、基线检查结果、安全漏洞、策略覆盖等信息，方便及时掌握资产的安全状况数据。

# 3 购买和使用安全云脑专业版

## 操作场景

安全云脑（SecMaster）是华为云原生的新一代安全运营中心，旨在为用户提供一站式的云上安全管理解决方案。通过安全云脑，用户可以实现对云上资产、安全态势、安全信息和事件的集中管理，从而提升安全运营效率和响应速度。

本文档将以首次在亚太-曼谷区域购买如下配置的安全云脑，并使用首个工作空间进行安全运营的场景为例进行介绍：

- 计费模式：包周期
- 版本：专业版
- 主机配额：50
- 增值包：安全大屏、日志审计、安全分析、安全编排

此场景的操作流程如下所示：

图 3-1 操作流程



## 操作流程

操作步骤	说明
准备工作	注册华为账号、开通华为云，赋予SecMaster权限。
步骤一：购买安全云脑专业版	购买安全云脑，选择版本（本文以专业版为例）、主机配额等信息。
步骤二：新增工作空间	新增首个用于安全运营的工作空间。

操作步骤	说明
<b>步骤三：接入数据</b>	接入数据信息，便于安全云脑对资源进行全面管理。 <ul style="list-style-type: none"><li>• 订阅资产数据：订阅当前账号当前region中所有资产信息，方便统一管理资产信息。</li><li>• 接入日志数据：接入其他服务日志数据，便于统一管理和分析。<ul style="list-style-type: none"><li>- 接入华为云服务日志数据</li><li>- （可选）接入非华为云日志数据</li></ul></li></ul>
<b>步骤四：配置和启用相关检查</b>	启用告警模型、剧本，执行基线检查，并配置策略管理，全面检查资源。 <ul style="list-style-type: none"><li>• 启用内置模型：可以利用模型对日志数据进行监控，如果检测到满足触发条件的内容时，将产生告警提示。</li><li>• 启用剧本：可以实现安全事件的高效、自动化响应处置。</li><li>• 执行基线检查：可以了解最新的云服务基线配置状态，获取云服务基线的风险配置。</li><li>• （可选）配置防线策略和应急策略：通过配置防线策略，实现全流程安全防护；通过配置应急策略进行风险控制。</li></ul>
<b>步骤五：创建报告</b>	设置报告信息，实现安全运营报告自动发送。
<b>步骤六：安全运营</b>	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。

## 准备工作

1. 在购买SecMaster之前，请先注册华为账号并开通华为云。具体操作详见[注册华为账号并开通华为云](#)。  
如果您已开通华为云，请忽略此步骤。
2. 请确保已为账号赋予“SecMaster FullAccess”权限。具体操作请参见[创建用户并授权使用SecMaster](#)。  
购买安全云脑时，还需要为账号授予“BSS Administrator”权限。

## 步骤一：购买安全云脑专业版

安全云脑提供了“基础版”、“标准版”、“专业版”供您使用，包括态势感知、基线检查、查询与分析以及安全编排等功能。

本步骤以购买专业版为例进行参数设置及介绍，更多购买安全云脑详细配置请参见[购买安全云脑](#)。

1. [登录华为云管理控制台](#)。
2. 在页面上方选择区域后，在服务列表中选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑控制台。



3. 在总览页面中，单击“购买安全云脑”后，在弹出的访问授权页面中，勾选同意授权并单击“确认”。
4. 在购买安全云脑页面，配置购买参数。

表 3-1 购买安全云脑参数配置说明

参数	示例	说明
计费模式	包周期	选择安全云脑的计费模式。 <ul style="list-style-type: none"><li>● 包周期：一种预付费模式，即先付费再使用，按照订单的购买周期进行结算。购买周期越长，享受的折扣越大。</li><li>● 按需：一种后付费模式，即先使用再付费，按照实际使用时长计费，秒级计费，按小时结算。按需计费模式允许您根据实际业务需求灵活地调整资源使用，无需提前预置资源，从而降低预置过多或不足的风险。</li></ul>
区域	亚太-曼谷	根据已有云上资源所在的区域选择安全云脑的区域。
版本	专业版	安全云脑提供有基础版、标准版、专业版供您选择，请根据您的需求进行选择，各版本的功能差异请参见 <a href="#">产品功能</a> 。
配额数	50	配额数是指支持防护的最大ECS主机资产数量。请根据当前账户下所有ECS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。 <ul style="list-style-type: none"><li>● 配额数最大限制为10000台。</li><li>● 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。</li></ul>
安全大屏	开启	确认是否需要使用安全云脑提供的“安全大屏”功能，是否需要增配“日志审计”、“安全分析”或“安全编排”功能。如果需要购买，请根据您的需要设置对应的购买量。 增值包说明、配置推荐详细介绍请参见 <a href="#">增值包说明</a> 。
日志审计	现在购买并根据每日新增日志量设置规格。	
安全分析	现在购买并根据需要设置每日每台服务器的配额数量。	
安全编排	现在购买并设置每日数据采集量和数据存储总量。	

参数	示例	说明
标签	<ul style="list-style-type: none"> <li>• 标签键：<b>test</b></li> <li>• 标签值：<b>01</b></li> </ul>	为安全云脑绑定标签，用来标识资源。标签更多详细介绍请参见值包说明 <a href="#">标签管理服务</a> 。
购买时长	<b>1个月</b>	<p>根据需求选择购买时长，“按需”模式无需配置。</p> <p>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。</p>

5. 确认参数配置无误后，在页面右下角单击“立即购买”。
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”。
7. 在支付页面，选择付款方式完成付款，完成购买操作。
8. 单击“返回安全云脑控制台”，返回安全云脑控制台页面。

## 步骤二：新增工作空间

工作空间（Workspace）属于安全云脑顶层工作台，使用安全云脑功能前，需要先新增工作空间。

1. 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 3-2 工作空间管理页面



2. 在弹出的授权页面中，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”。

由于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。

3. 在工作空间管理页面中，单击“新增”，并配置工作空间参数。  
本示例中仅解释必要参数，其他参数请根据实际情况进行选择。

表 3-2 新增工作空间参数配置说明

参数	示例	说明
区域	<b>亚太-曼谷</b>	根据待查看的云上资源所在的区域选择创建工作空间的区域。

参数	示例	说明
项目类型	普通项目	选择工作空间所属的项目。
工作空间名称	SecMaster	安全运营工作空间的名称。

- 单击“确定”。

### 步骤三：接入数据

由于安全云脑中的数据来源于其他云服务，因此，工作空间创建完成后，需要接入数据信息，便于安全云脑对资源进行全面管理。

- 接入资产**

安全云脑纳管了网站、弹性云服务器、数据库、IP、VPC等资产，并关联对应的安全服务，护网、重保期间立志于从网络层、应用层、主机层、数据层等多方面构建整体网络防护架构，全面保障用户业务系统的安全稳定。

**每个Region的首个工作空间可自动加载当前Region所有资产。后续新增的用于自定义运营的工作空间，不会自动加载资产，需要用户自定义接入。**

本部分介绍如何手动接入资产数据信息。

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

图 3-3 进入目标工作空间管理页面



- 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 3-4 资产管理



- 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。
- 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。
- 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。后续，将每天晚上自动同步资产信息。

- 接入云服务日志数据**

日志作为安全运营提供重要数据支撑，安全云脑支持一键接入WAF、HSS等多种华为云产品的日志数据。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。

每个Region的首个工作空间可自动加载当前Region推荐接入的云服务日志数据（未全部接入）。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。

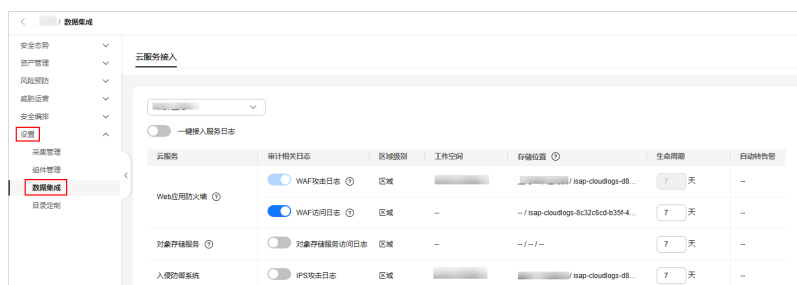
### 📖 说明


建议将安全云脑管理的资产以及资产的告警、基线检查结果、漏洞数据、日志数据接入同一个工作空间，便于统一运营，进行安全分析关联。


本部分介绍如何接入所需要的且未自动接入的云服务日志数据。

- 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。


图 3-5 数据集成页面



- 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。

- 设置生命周期，建议保持默认即可。
- 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。

- 单击“保存”。

接入完成后，将创建默认数据空间和管道。

- **（可选）接入非华为云日志数据**

安全云脑的日志采集功能支持将第三方（非华为云）安全日志接入安全云脑，详细操作请参见[采集数据](#)。

## 步骤四：配置和启用相关检查

- **新建并启用告警模型**

安全云脑内置了基于应用、网络、主机多维度的安全分析模型，自动化的完成数据汇聚、分析和报警。

通过模型汇聚分析筛选告警，降低误报率，提升值班人员分析处理效率。同时，也可以结合用户场景编辑模型进行模型调整，适配不同用户场景，降噪告警。

每个Region的首个工作空间可自动启用推荐使用的内置的告警模型（未全部启用），后续新增的用于自定义运营的工作空间，不会自动启用预置模型，需要用户自定义创建并启用。

如果有需要使用的且未自动启用的模型，请参照以下步骤使用已有模板创建模型：

- a. 在左侧导航栏选择“威胁管理 > 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 3-6 模型模板页面



- b. 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”，并在右侧弹出模板详情页面右下角单击“创建模型”。
- c. 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 3-7 获取管道名称



- 其他参数建议保持默认值即可。
- d. 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。
  - e. 设置模型逻辑，建议保持默认即可。
  - f. 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。
  - g. 预览确认无误后，单击页面右下角“确定”。
  - h. 重复b-g为其他模板创建告警模型。
- 启用剧本

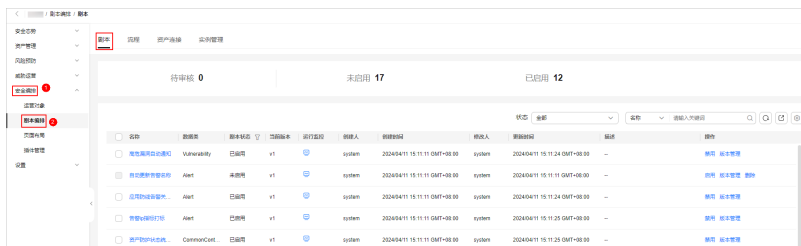
数据接入后，针对云上安全事件提供了安全编排剧本，实现安全事件的高效、自动化响应处置。

每个Region的首个工作空间可自动启用内置的流程，无需再进行手动启用。同时，内置的剧本中推荐使用的高频剧本默认已启用（未全部启用）。后续新增的用于自定义运营的工作空间，不会自动启用剧本，需要用户自定义启用。

若还需开启未默认启用的剧本，请参考下述操作步骤进行启用：

- a. 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 3-8 进入剧本管理页面



- b. 在剧本页面中，单击目标剧本所在行“操作”列的“启用”。
- c. 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”。

● 执行基线检查

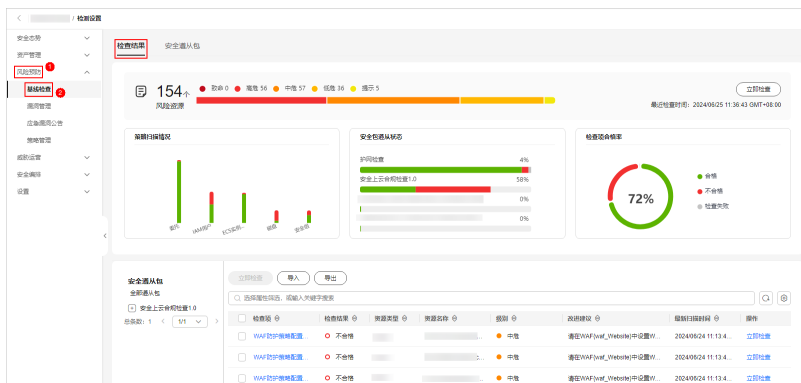
接入数据后，需要执行基线检查，以便检查云上资产的关键配置项。通过执行扫描任务，检查云服务基线配置风险状态，分类呈现云服务配置检测结果，告警提示存在安全隐患的配置，并提供相应配置加固建议和帮助指导。基线检查功能支持定期自动检查和立即检查：

- 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。

本步骤以立即检查已有的遵从包中所有检查项的遵从情况为例进行介绍。

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

图 3-9 进入基线检查结果页面



- b. 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”，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。

● （可选）配置防线策略和应急策略

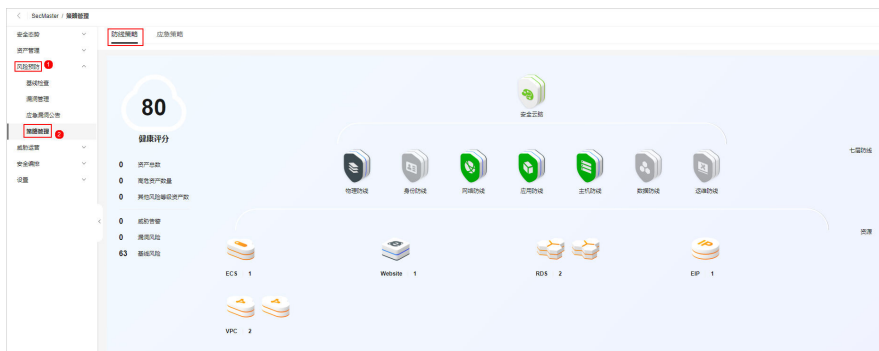
通过策略配置可以开通、配置和使用七层安全防线，实现全流程安全防护。同时，支持通过应急策略功能进行风险控制。

a. 配置防线策略。

本部分以配置应用防线的WAF防护策略为例进行介绍。

- i. 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 3-10 进入防线策略管理页面

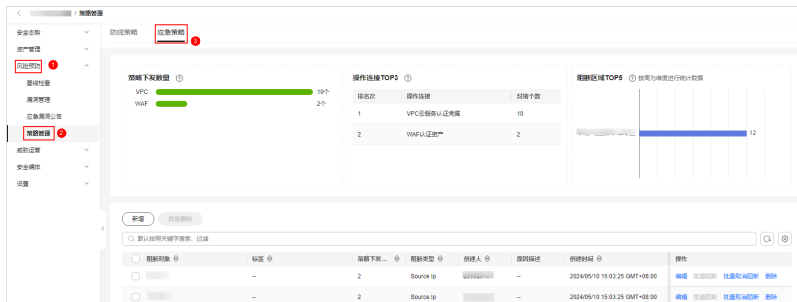


- ii. 单击应用防线名称，右侧滑出应用防线对应的云产品信息。
- iii. 在WAF页签中，单击“防护策略”，进入WAF防护策略配置页面。  
如果还未购买WAF，请在产品介绍描述信息中单击产品名称“Web应用防火墙”，进入WAF控制台页面后，单击“购买WAF实例”，进入购买WAF页面，参见[购买WAF](#)开通WAF产品。
- iv. 在WAF防护策略配置，选择“策略管理”页签，进入策略管理页面后，单击列表的左上角的“添加防护策略”。
- v. 在弹出的对话框中，输入策略名称，单击“确认”，添加的策略会展示在策略列表中。
- vi. 在目标策略所在行，单击策略名称，进入防护规则配置页面，参见[配置防护规则](#)为策略添加防护规则。

b. 配置应急策略。

- i. 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后，选择“应急策略”页签，进入应急策略管理页面。

图 3-11 进入应急策略管理页面



- ii. 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。
- iii. 在新增策略页面中，配置策略信息。

表 3-3 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或IAM。
阻断对象	<ul style="list-style-type: none"><li>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。</li><li>当阻断对象类型为IAM时，请填写IAM用户名称。</li><li>单次下发应急策略阻断对象说明如下：<ul style="list-style-type: none"><li>当需要下发策略至CFW时，单用户单次最多可新增50个IP作为阻断对象。</li><li>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。</li><li>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。</li><li>当需要下发策略至IAM时，单用户单次最多可新增50个IAM用户作为阻断对象。</li></ul></li></ul>
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。
阻断老化	确认是否老化该条阻断。 <ul style="list-style-type: none"><li>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地址段或IAM用户。</li><li>如果选择否，则该策略将一直有效，阻断设置的IP地址或IP地址段或IAM用户。</li></ul>
策略描述	自定义该策略的描述信息。

iv. 单击“确定”。

## 步骤五：创建报告

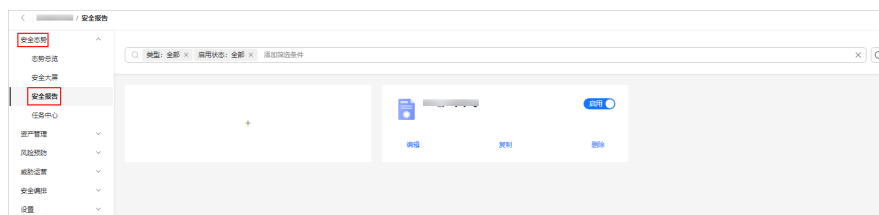
安全云脑可以自动发送安全态势报告，展示安全评分、基线检查结果、安全漏洞、策略覆盖等信息，方便及时掌握资产的安全状况数据。

本步骤以创建安全运营日报为例进行介绍。

1. 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 3-12 进入安全报告页面



2. 在安全报告页面中单击 **+** 按钮，进入配置报告基本信息页面后，配置报告基本信息。

表 3-4 报告基本信息参数说明

参数	示例	说明
报告名称	安全态势报告-日报	自定义报告名称。
报告类型	日报	选择安全态势报告的类型。
统计周期	--	根据您选择的“报告类型”显示安全报告统计周期，无需单独配置。
报告发送时间	--	设置安全态势报告的发送时间点。 当报告类型为日报时，默认发送前一天 00:00:00~23:59:59的安全信息报告。
邮件标题	安全云脑安全态势日报	设置报告发送邮件的标题信息。
报告接收人邮箱	test01@example.com	添加接收人邮箱地址。 <ul style="list-style-type: none"> <li>最多可添加100个邮箱地址。</li> <li>有多个邮箱地址，请使用英文分号隔开。例如： test01@example.com;test02@example.com</li> </ul>
(可选)抄送	test03@example.com	添加抄送人邮箱地址。 <ul style="list-style-type: none"> <li>最多可添加100个邮箱地址。</li> <li>有多个邮箱地址，请使用英文分号隔开。例如： test03@example.com;test04@example.com</li> </ul>
(可选)备注	--	自定义安全报告的备注信息。

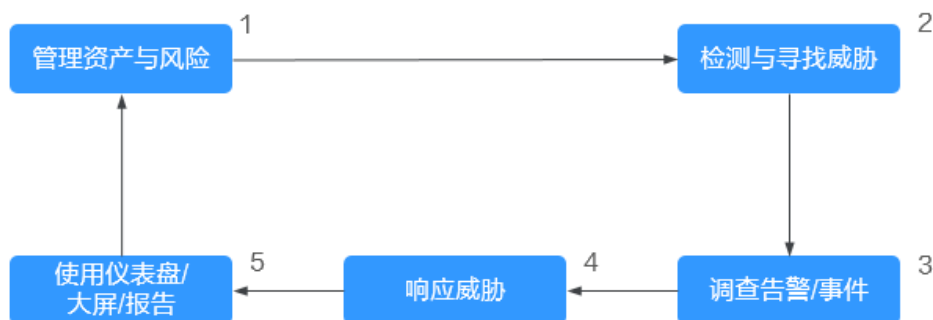
3. 报告基本信息配置完成后，单击右下角“下一步：报告选择”，进入报告选择页面。
4. 在“报告选择”页面的左侧已有报告布局中，选择已有报告布局。选择完成后，可以在右侧页面中预览报告样式。  
此处示例选择“日报”。

- 单击右下角“完成”，返回安全报告管理页面，即可查看创建的安全报告。

## 步骤六：安全运营

首个工作空间新增完成后，安全云脑将自动进行空间初始化操作。初始化完成后，可以进行管理资产、检查与寻找威胁、调查告警、响应威胁等安全运营操作，同时，还可以使用仪表盘、大屏等查看安全态势。

图 3-13 安全运营



### 1. 管理资产与风险

安全运营的本质指安全风险管理的本质，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，还可以将云外资产导入到安全云脑中，并标记其所属的环境。汇聚后，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）等，方便查看资产的安全状态。

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[安全治理](#)、[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、网站漏洞，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，帮助您实时了解漏洞情况。

更多详细介绍及操作请参见[漏洞管理](#)。

### 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型，使您能够执行某些对应操作时收到此类威胁的通知。启用这些模型后，它们将自动在整个环境中搜索可疑活动。同时，可以根据您的需要自定义模型，以搜索或筛选出威胁。

同时，提供了日志数据检索功能，帮助您筛选威胁。

更多详细介绍及操作请参见[模型模板](#)、[安全分析](#)。

### 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。安全运营人员需要对告警做出分析判定。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，分析后对事件发起应急响应。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](#)。

### 4. 响应威胁

当您在告警、事件进行响应时，可以使用剧本来做自动化处置，提高效率。

更多详细介绍及操作请参见[安全编排](#)。

### 5. 使用总览仪表盘、大屏、报告

#### - 总览仪表盘

展示当前工作空间中资源的安全评分，快速了解当前的安全状况。

#### - 安全大屏

查看资源的实时态势并处理攻击事件等，可以帮助安全运营团队实时监控和分析各种安全威胁和事件，从而做出快速响应。

#### - 安全报告

可以自动发送安全态势报告，展示安全评分、基线检查结果、安全漏洞、策略覆盖等信息，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](#)。

# 4 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 4-1 常用实践

实践	描述
<a href="#">安全看板</a>	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。
<a href="#">资产管理</a>	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。
<a href="#">安全分析</a>	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。
<a href="#">自动化处理安全事件</a>	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。
<a href="#">将非华为云日志数据接入安全云脑或将安全云脑日志转出至第三方系统/产品</a>	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。