安全云脑

产品介绍

文档版本 07

发布日期 2025-02-24

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 什么是安全云脑

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。

为什么选择安全云脑

- 一键安全合规：一键生成遵从报告，华为积累的全球安全合规经验服务化，帮助用户快速实现云上业务安全/隐私保护遵从。
- 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：结合华为云积累的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。

更多安全云脑产品优势请参见**产品优势**。

2 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，利用华为云安全运营团队多年沉淀经验，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。

3 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。

4 产品功能

安全云脑基于云原生安全，提供全面的日志采集、安全治理、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。

同时，为满足不同场景下的安全需求，安全云脑提供了基础版、标准版和专业版供您选择，不同版本的功能存在差异，您可以根据业务需求选择合适的版本。

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 4-1 总览功能介绍

功能模块	功能描述	基础版	标准版	专业版
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、企业项目和Region，可支撑不同场景下的工作空间运营模式。

表 4-2 工作空间功能说明

功能模块	功能描述	基础版	标准版	专业版
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。 • 空间托管：跨账号安全运营，可实现工作空间委托集中安全运营查看统一资产风险、告警和事件等。	√	√	√

安全治理

安全治理为您提供安全治理模板与合规策略扫描服务，将安全遵从包内的法规标准条款转化成检查项。

表 4-3 安全治理功能说明

功能模块	功能描述	基础版	标准版	专业版
安全治理	• 提供安全遵从包 华为开放的安全治理模板，包含法规标准条款原文、扫描策略、自评估检查项以及华为专家的改进建议，覆盖PCI DSS、ISO27701、ISO27001、隐私等法规标准。用户可以订阅、取消订阅安全遵从包，查看合规评估与治理结果。 • 合规策略扫描 Policy as Code，将安全遵从包内的法规标准条款代码化，周期性、自动化扫描云上资产的合规情况，可视化看板呈现风险，提供华为专家改进建议。 • 自评估检查项 将安全遵从包内的法规标准条款转化成检查项，租户可根据检查项完成自身业务的合规评估，查看历史评估结果，进行证据上传和下载，根据华为专家改进建议进行治理。 • 合规结果可视 可视化呈现合规评估结果与安全治理情况，包括租户订阅的法规、标准条款遵从概况，各安全遵从包状态，各策略扫描概况。 **说明** 使用安全治理功能前，需先**提交工单**申请开通使用权限。	×	×	√

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 4-4 已购资源功能说明

功能模块	功能描述	基础版	标准版	专业版
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 4-5 安全态势功能介绍

功能模块	功能描述	基础版	标准版	专业版
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** 安全大屏功能需要在标准版/专业版基础上单独购买。	×	√	√
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 4-6 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。	√	√	√

风险预防

风险预防提供基线检查、漏洞管理、策略管理功能，帮助您的云安全配置达到等保、ISO、PCI等各类权威安全标准和华为云安全最佳实践标准；知晓全局的漏洞分布，并一键修复漏洞。

表 4-7 风险预防功能介绍

功能模块	功能描述	基础版	标准版	专业版
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	通过自动同步华为云主机安全服务（Host Security Service，HSS）的漏洞扫描数据，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。	×	×	√
应急漏洞公告	针对业界披露的热点安全漏洞，支持每5分钟抓取一次安全漏洞讯息，获取最新应急漏洞公告详情。	√	√	√
策略管理	支持统一管理防线策略和应急策略。	×	√	√

威胁管理

威胁管理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 4-8 威胁管理功能介绍

功能模块	功能描述	基础版	标准版	专业版
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	通过集成云服务告警，包含HSS、WAF、DDoS等，集中呈现并管理告警信息。	×	√	√
情报管理	支持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。	×	√	√
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华为云产品中，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** 需额外购买增值包中的安全分析功能。其中，安全分析、内置剧本、安全编排含有赠送配额，具体说明请参见**赠送规格说明**。	×	√	√

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 4-9 安全编排功能介绍

功能模块	功能描述	基础版	标准版	专业版
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。 **说明** 需额外购买增值包中的安全编排功能。其中，安全分析、内置剧本、安全编排含有赠送配额，具体说明请参见**赠送规格说明**。	×	√	√
页面布局	提供安全可视化低代码开发平台，基于此平台可自定义安全分析报告、告警管理、事件管理、漏洞管理、基线管理、威胁情报指标库管理等页面布局。	×	√	√
插件管理	支持将安全编排流程中使用的插件进行统一管理。	×	×	√

数据采集

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 4-10 数据采集功能说明

功能模块	功能描述	基础版	标准版	专业版
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 4-11 数据集成功能说明

功能模块	功能描述	基础版	标准版	专业版
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。	×	√（仅支持集成云服务告警）	√

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 4-12 目录定制功能说明

功能模块	功能描述	基础版	标准版	专业版
目录定制	支持查看已有目录及更换布局等操作。	×	√	√

赠送规格说明

安全云脑增值包中的安全分析、安全编排功能在不同的版本有不同的赠送配额，具体说明如下：

表 4-13 赠送规格说明

功能		标准版	专业版
安全分析	安全数据采集	120 MB/天/配额	120 MB/天/配额
	安全数据保留	120 MB/天/配额	120 MB/天/配额
	安全数据导出	120 MB/天/配额	120 MB/天/配额
	平台安全数据	40 MB/天/配额	40 MB/天/配额
	安全建模分析	×	120 MB/天/配额
威胁管理	预制威胁模型	×	计算模型数据120 MB/天/配额；预置模型200个
	预制响应剧本	×	预置剧本30个
安全编排	安全编排	×	操作7000次

5 个人数据保护机制

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

收集范围

安全云脑收集及产生的个人数据如表5-1所示。

表 5-1 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
邮箱	采用邮箱方式启用通知类剧本时，安全云脑获取对应消息通知服务主题订阅的邮箱。 或者开启安全分析报告定时发送功能时，安全云脑获取用户在界面输入的接收邮箱地址（需要经过拥有接收邮箱地址的用户授权同意接收安全分析报告邮件）。	是	是
请求源IP	安全云脑上开启WAF防护场景，有攻击防护域名时，被WAF拦截或者记录的攻击者IP。	否	是
URL	安全云脑上开启WAF防护场景，有攻击的防护域名的URL，被WAF拦截或者记录的防护域名的URL。	否	是
HTTP/HTTPS Header信息（包括Cookie）	安全云脑上开启WAF防护场景，且有攻击命中用户配置的CC攻击、精准访问防护规则时，在攻击告警中可能携带用户在配置界面输入的Cookie值和Header值。	否	否 如果配置的Cookie和Header信息不含有用户的个人信息，则安全云脑也不会收集及产生用户的个人数据。

类型	收集方式	是否可以修改	是否必须
请求参数（Get、Post）	安全云脑上开启WAF防护场景，在WAF防护日志里，WAF记录的请求详情。	否	否 如果请求参数里不含有用户的个人信息，则WAF记录的相关请求中不会收集及产生用户的个人数据。
登录位置信息	安全云脑上开启HSS主机防护场景，服务器开启防护后，登录云服务器时，HSS记录的用户登录位置信息。	否	是

存储方式

安全云脑（SecMaster）通过加密算法对用户个人敏感数据加密后进行存储。

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

访问权限控制

用户个人数据通过加密后存储在安全云脑数据库中，数据库的访问需要通过白名单的认证与授权。

用户只能查看自己业务的相关日志。

6 经验包

6.1 内置剧本

安全编排根据需求内置了剧本，可以根据需要直接进行使用。

内置剧本

默认已启用以下剧本：

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

表 6-1 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

安全防线	剧本名	描述	数据类
	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
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

安全防线	剧本名	描述	数据类
	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
	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
	同步CFW黑IP到情报	将CFW的黑IP同步到云脑的情报管理中	CommonContext
	同步WAF黑IP到情报	将WAF的黑IP同步到云脑的情报管理中	CommonContext

6.2 内置类型

本章节介绍安全云脑支持的内置告警类型、内置事件类型、内置威胁情报类型、内置漏洞类型。

内置告警类型

表 6-2 内置告警类型列表

类型名称	子类型/子类型标识	内置	描述
DDoS攻击	DNS协议攻击 Tcp Dns	是	DNS协议攻击
	异常端口通信 Unusual Network Port	是	异常端口通信
	异常协议攻击 Unusual Protocol	是	异常协议攻击
	ACK Flood ACK Flood	是	ACK Flood
	BGP Flood攻击 BGP Flood Attack	是	BGP Flood攻击
	DNS IP TTL DNS IP TTL Check Fail	是	DNS IP TTL
	DNS Reply Flood 攻击 DNS Reply Flood	是	DNS Reply Flood 攻击
	DNS查询攻击 DNS Query Flood	是	DNS查询攻击
	DNS大小异常 DNS Size Abnormal	是	DNS大小异常
	DNS反射 DNS Reflection	是	DNS反射
	DNS返回域名流异常 DNS Reply Domain Flow Abnormal	是	DNS返回域名流异常
	DNS格式错误 DNS Format Error	是	DNS格式错误
	DNS缓存匹配 DNS Cache Match	是	DNS缓存匹配

类型名称	子类型/子类型标识	内置	描述
	DNS缓存投毒 DNS Cache Poisoning	是	DNS缓存投毒
	DNS请求域名流异常 DNS Request Domain Flow Abnormal	是	DNS请求域名流异常
	DNS无效域名 DNS No Such Name	是	DNS无效域名
	FIN/RST Flood FIN/RST Flood	是	FIN/RST Flood
	HTTPS Flood HTTPS Flood	是	HTTPS Flood
	HTTP慢速攻击 HTTP Slow Attack	是	HTTP慢速攻击
	ICMP协议封禁 ICMP Protocol Block	是	ICMP协议封禁
	IP信誉 IP Reputation	是	IP信誉
	SIP Flood SIP Flood	是	SIP Flood
	SIP源速率异常 SIP Source Rate Abnormity	是	SIP源速率异常
	SYN Flood SYN Flood	是	SYN Flood
	SYN-ACK Flood SYN-ACK Flood	是	SYN-ACK Flood
	TCP带宽溢出 TCP Bandwidth Overflow	是	TCP带宽溢出
	TCP多连接攻击 TCP Connection Flood	是	TCP多连接攻击

类型名称	子类型/子类型标识	内置	描述
	TCP分片带宽溢出 TCP Fragment Bandwidth Overflow	是	TCP分片带宽溢出
	TCP分片攻击 TCP Fragment Flood	是	TCP分片攻击
	TCP畸形报文 TCP Malformed	是	TCP畸形报文
	TCP认证UDP攻击 TCP-authenticated UDP Attack	是	TCP认证UDP攻击
	TCP协议封禁 TCP Protocol Block	是	TCP协议封禁
	UDP带宽溢出 UDP Bandwidth Overflow	是	UDP带宽溢出
	UDP分片 UDP Fragment Flood	是	UDP分片
	UDP分片带宽溢出 UDP Fragment Bandwidth Overflow	是	UDP分片带宽溢出
	UDP畸形报文 UDP Malformed	是	UDP畸形报文
	UPD协议封禁 UDP Protocol Block	是	UPD协议封禁
	URI监控 URI Monitor	是	URI监控
	暗网IP Dark IP	是	暗网IP
	单IP带宽溢出 Single IP Bandwidth Overflow	是	单IP带宽溢出

类型名称	子类型/子类型标识	内置	描述
	当前连接耗尽攻击 Concurrent Connections Flood	是	当前连接耗尽攻击
	端口扫描攻击 Port Scanning Attack	是	端口扫描攻击
	恶意域名攻击 Malicious Domains Attack	是	恶意域名攻击
	反恶意软件 Anti-Malware	是	反恶意软件
	分布式拒绝服务攻击 DDOS	是	分布式拒绝服务攻击
	分区带宽溢出 Zone Bandwidth Overflow	是	分区带宽溢出
	过滤器攻击 Filter Attack	是	过滤器攻击
	黑名单 Blacklist	是	黑名单
	僵尸网络/特洛伊木马/蠕虫 Botnets/Trojan horses/Worms Attack	是	僵尸网络/特洛伊木马/蠕虫
	目的IP新会话限速 Destination IP new session rate limiting	是	目的IP新会话限速
	其他Flood攻击 Other Flood	是	其他Flood攻击
	其他带宽溢出 Other Bandwidth Overflow	是	其他带宽溢出
	其他全局异常 Global Other Abnormal	是	其他全局异常

类型名称	子类型/子类型标识	内置	描述
	其他协议封禁 Other Protocol Block	是	其他协议封禁
	全局ICMP异常 Global ICMP Abnormal	是	全局ICMP异常
	全局TCP分片异常 Global TCP Fragment Abnormal	是	全局TCP分片异常
	全局TCP异常 Global TCP Abnormal	是	全局TCP异常
	全局UDP分片异常 Global UDP Fragment Abnormal	是	全局UDP分片异常
	全局UDP异常 Global UDP Abnormal	是	全局UDP异常
	网页攻击 Web Attack	是	网页攻击
	位置攻击 Location Attack	是	位置攻击
	新连接耗尽攻击 New Connections Flood	是	新连接耗尽攻击
	域名劫持 Domain Hijacking	是	域名劫持
	源DNS返回流异常 Source DNS Reply Flow Abnormal	是	源DNS返回流异常
	源DNS请求流异常 Source DNS Request Flow Abnormal	是	源DNS请求流异常

类型名称	子类型/子类型标识	内置	描述
	主机流量溢出 Host Traffic Over Flow	是	主机流量溢出
	HTTP Flood HTTP Flood	是	HTTP Flood
	ICMP Flood ICMP Flood	是	ICMP Flood
	SSL Flood SSL Flood	是	SSL Flood
	TCP Flood TCP Flood	是	TCP Flood
	UDP Flood UDP Flood	是	UDP Flood
	XML Flood XML Flood	是	XML Flood
	放大攻击 Amplification	是	放大攻击
Web恶意代码	网页暗链 Web Page Dark Link	是	网页暗链
	网页挂马 Web Page Trojan	是	网页挂马
Web攻击	Webshell Webshell	是	Webshell
	WAF机器人 WAF Robot	是	WAF机器人
	白名单IP White IP	是	白名单IP
	攻击惩罚 Known Attack Source	是	攻击惩罚
	黑名单IP Black IP	是	黑名单IP

类型名称	子类型/子类型标识	内置	描述
	漏洞攻击 Vulnerability Attack	是	漏洞攻击
	命中隐私泄露规则 Leakage	是	命中隐私泄露规则
	默认 Default	是	默认
	扫描/爬虫 Scanner & Crawler	是	扫描/爬虫
	CC攻击 Challenge Collapsar	是	CC攻击
	IP信誉库 IP Repuation	是	IP信誉库
	SQL注入 SQL Injection	是	SQL注入
	XSS Cross-Site Scripting	是	XSS
	本地文件包含 Local Code Inclusion	是	本地文件包含
	地理访问控制拦截 Geo IP	是	地理访问控制拦截
	恶意爬虫 Malicious Web Crawlers	是	恶意爬虫
	反爬虫 Anticrawler	是	反爬虫
	防篡改 AntiTamper	是	防篡改
	非法请求 Illegal Access	是	非法请求
	黑白名单拦截 White or Black IP	是	黑白名单拦截

类型名称	子类型/子类型标识	内置	描述
	精准防护 Custom Rule	是	精准防护
	命令注入 Command Injection	是	命令注入
	目录遍历 Path Traversal	是	目录遍历
	网站木马 Website Trojan	是	网站木马
	网站信息防泄漏 Information Leakage	是	网站信息防泄漏
	网站信息泄露 Web Service Exfiltration	是	网站信息泄露
	远程代码执行 Remote Code Execute	是	远程代码执行
	远程文件包含 Remote Code Inclusion	是	远程文件包含
恶意软件	加密货币挖矿 Cryptomining	是	加密货币挖矿
	Docker恶意程序 Docker Malware	是	Docker恶意程序
	钓鱼 Phishing	是	钓鱼
	恶意广告软件 Adware	是	恶意广告软件
	恶意软件 Malicious Software	是	恶意软件
	黑客工具 Hacktool	是	黑客工具
	灰色软件 Grayware	是	灰色软件

类型名称	子类型/子类型标识	内置	描述
	间谍软件 Spyware	是	间谍软件
	垃圾邮件 Spam	是	垃圾邮件
	Rootkit Rootkit	是	Rootkit
	Webshell Webshell	是	Webshell
	病毒、蠕虫 Virus and Worm	是	病毒、蠕虫
	恶意文件 Malicous File	是	恶意文件
	反弹shell Reverse Shell	是	反弹shell
	后门木马 Backdoor Trojan	是	后门木马
	僵尸网络程序 Botnet Program	是	僵尸网络程序
	勒索软件 Ransomware	是	勒索软件
	挖矿程序 Bitcoin Miner	是	挖矿程序
	挖矿软件 Mining Software	是	挖矿软件
风险审计	Webcms漏洞 Webcms Vulnerability	是	Webcms漏洞
	Windows OS 漏洞 Windows Vulnerability	是	Windows OS 漏洞
	本地访问漏洞 Local Access Vulnerability	是	本地访问漏洞

类型名称	子类型/子类型标识	内置	描述
	错误配置策略 Mis-Configured Policy	是	错误配置策略
	其它OS漏洞 Other OS Vulnerability	是	其它OS漏洞
	其它漏洞 Other Vulnerability	是	其它漏洞
	应用程序漏洞 Application Vulnerability	是	应用程序漏洞
	远程访问漏洞 Remote Access Vulnerability	是	远程访问漏洞
风险审计	弱口令 Weak Password	是	弱口令
	系统风险配置 System Risk Configuration	是	系统风险配置
攻击探测	钓鱼 Phishing	是	钓鱼
	网络拓扑构建 Map Network Topology	是	网络拓扑构建
	账户、组信息收集 Identify Groups/ Roles	是	账户、组信息收集
	指纹扫描 Fingerprinting	是	指纹扫描
	主机发现 Determine IP Address	是	主机发现

类型名称	子类型/子类型标识	内置	描述
漏洞利用	ActiveX漏洞利用 ActiveX Exploit	是	ActiveX漏洞利用
	CGI攻击 CGI Attack	是	CGI攻击
	DNS漏洞利用 DNS Exploit	是	DNS漏洞利用
	FTP漏洞利用 FTP Exploit	是	FTP漏洞利用
	Hadoop漏洞利用 Hadoop Vulnerability Exploit	是	Hadoop漏洞利用
	Hypervisor漏洞利用 Hypervisor Exploit	是	Hypervisor漏洞利用
	LDAP注入攻击 LDAP Injection Attack	是	LDAP注入攻击
	MacOS漏洞利用 MacOS Exploit	是	MacOS漏洞利用
	MySQL漏洞利用 MySQL Vulnerability Exploit	是	MySQL漏洞利用
	Office软件漏洞利用 Office Exploit	是	Office软件漏洞利用
	Redis漏洞利用 Redis Vulnerability Exploit	是	Redis漏洞利用
	RPC漏洞利用 RPC Exploit	是	RPC漏洞利用
	SQL注入 SQL Injection	是	SQL注入
	SSH漏洞利用 SSH Exploit	是	SSH漏洞利用

类型名称	子类型/子类型标识	内置	描述
	SSI注入攻击 SSI Injection Attack	是	SSI注入攻击
	Struts2 OGNL注入 Struts2 OGNL Injection	是	Struts2 OGNL注入
	Telnet漏洞利用 TELNET Exploit	是	Telnet漏洞利用
	Unix漏洞利用 Unix Exploit	是	Unix漏洞利用
	Web漏洞利用 Web Exploit	是	Web漏洞利用
	XSS攻击 Cross-Site Scripting	是	XSS攻击
	本地文件包含 Local File Inclusion	是	本地文件包含
	恶意文件投递 Malicious File Delivery	是	恶意文件投递
	恶意文件执行 Malicious File Execution	是	恶意文件执行
	缓冲区溢出攻击 Buffer Overflow	是	缓冲区溢出攻击
	会话劫持 Session Hijack	是	会话劫持
	口令猜测 Password Cracking	是	口令猜测
	浏览器漏洞利用 Browser Exploit	是	浏览器漏洞利用
	弱口令访问 Weak Password Access	是	弱口令访问
	数据库漏洞利用 Database Exploit	是	数据库漏洞利用

类型名称	子类型/子类型标识	内置	描述
	未知漏洞利用 Unknown Exploit	是	未知漏洞利用
	隐藏链接访问 Hide Link Access	是	隐藏链接访问
	邮件漏洞利用 Mail Exploit	是	邮件漏洞利用
	远程代码执行 Remote Code Execution	是	远程代码执行
	远程访问漏洞利用 Remote Access Exploit	是	远程访问漏洞利用
	远程文件包含攻击 Remote File Inclusion	是	远程文件包含攻击
	远程文件注入 Remote File Injection	是	远程文件注入
	组合漏洞利用 Misc Exploit	是	组合漏洞利用
	CMS漏洞 CMS Exploit	是	CMS漏洞
	CSRF攻击 CSRF Attack	是	CSRF攻击
	JNDI注入攻击 JNDI Injection Attack	是	JNDI注入攻击
	Linux漏洞 Linux Exploit	是	Linux漏洞
	SMB漏洞 SMB Exploit	是	SMB漏洞
	Windows漏洞 Windows Exploit	是	Windows漏洞
	XML注入 XML Injection	是	XML注入

类型名称	子类型/子类型标识	内置	描述
	代码注入 Code Injection	是	代码注入
	漏洞逃逸攻击 Vulnerability Escape Attack	是	漏洞逃逸攻击
	命令执行 Command Execution	是	命令执行
	命令注入 Command Injection	是	命令注入
	文件逃逸攻击 File Escape Attack	是	文件逃逸攻击
	虚拟机逃逸攻击 VM Escape Attack	是	虚拟机逃逸攻击
	一般漏洞利用 General Exploit	是	一般漏洞利用
命令与控制	ECS存在当前IP被用于向高危网络发送消息 Command Control Activity	是	ECS存在当前IP被用于向高危网络发送消息
	可疑的域名、IP地址、端口动态生成访问 Dynamic Resolution	是	可疑的域名、IP地址、端口动态生成访问
	其他可疑连接 Abnormal Connection	是	其他可疑连接
	其他可疑行为 Abnormal Behaviour	是	其他可疑行为
	外连恶意DNS Malicious Domain Query	是	外连恶意DNS

类型名称	子类型/子类型标识	内置	描述
	外连恶意IP地址 Malicious Ip Address Query	是	外连恶意IP地址
	隐蔽隧道 Protocol Tunneling	是	隐蔽隧道
	与矿池地址通信 Mining Pool Communication	是	与矿池地址通信
其他	公共舆情 Public_Opinion	是	公共舆情
	云防火墙攻击 CFW_RISK	是	云防火墙攻击
数据泄露	数据窃取 Steal Data	是	数据窃取
	违规外传 Transfer Data Abnormal	是	违规外传
网络异常行为	IP访问频率异常 IP Access Frequency Abnormal	是	IP访问频率异常
	IP切换异常 IP Switch Abnormal	是	IP切换异常
	IP首次访问 IP First Access	是	IP首次访问
	Sinkhole攻击IP访问 Sink Hole	是	Sinkhole攻击IP访问
	代理IP访问 Proxy	是	代理IP访问
	恶意资源访问 Resource Permissions	是	恶意资源访问
	欺诈付款网站IP/域名访问 Payment	是	欺诈付款网站IP/域名访问

类型名称	子类型/子类型标识	内置	描述
	洋葱网络IP访问 Tor	是	洋葱网络IP访问
	C&C异常通信 C&C Abnormal Communication	是	C&C异常通信
	IP黑名单访问 IP Blacklist Access	是	IP黑名单访问
	URL黑名单访问 URL Blacklist Access	是	URL黑名单访问
	恶意URL访问 Malicious URL Access	是	恶意URL访问
	恶意域名访问 Malicious Domain Name Access	是	恶意域名访问
	非授权访问企图 Unauthorized Access Attemp	是	非授权访问企图
	可疑的网络流量 Suspicious Network Traffic	是	可疑的网络流量
	容器网络外联 Container Network Connect	是	容器网络外联
	未知网络访问 Unknown Abnormal Network Access	是	未知网络访问
	文件MD5黑名单访问 File MD5 Blacklist Access	是	文件MD5黑名单访问
	异常外联行为 Abnormal External Behavior	是	异常外联行为

类型名称	子类型/子类型标识	内置	描述
	域名黑名单访问 Domain Name Blacklist Access	是	域名黑名单访问
	周期外联通信 Periodic Outreach	是	周期外联通信
	可疑的端口转发 Suspicious Port Forward	是	可疑的端口转发
无文件攻击	VDSO劫持 VDSO Hijacking	是	VDSO劫持
	动态库注入进程 Dynamic Library Inject Process	是	动态库注入进程
	关键配置变更 Critical File Change	是	关键配置变更
	环境变量变更 Environment Change	是	环境变量变更
	进程注入 Process Inject	是	进程注入
	内存文件进程 Memfd Process	是	内存文件进程
	文件操纵 File Manipulation	是	文件操纵
系统行为异常	Crontab可疑任务 Crontab Suspicious Task	是	Crontab可疑任务
	Socket连接异常 Abnormal Socket Connection	是	Socket连接异常
	备份删除 Backup Deletion	是	备份删除
	非法数据库访问 Unauthorized Database Access	是	非法数据库访问

类型名称	子类型/子类型标识	内置	描述
	权限异常访问 Privilege Abnormal Access	是	权限异常访问
	日志异常变化 Unexpected Log Change	是	日志异常变化
	容器进程退出 Container Process Exist	是	容器进程退出
	未知主机异常行为 Unknown Host Abnormal Activity	是	未知主机异常行为
	文件黑名单访问 File blocklist access	是	文件黑名单访问
	文件权限异常改变 Unexpected File Permission Change	是	文件权限异常改变
	系统安全防护被禁用 System Security Protection disabled	是	系统安全防护被禁用
	系统账号变更 System Account Change	是	系统账号变更
	异常注册表操作 Abnormal Registry Operation	是	异常注册表操作
	Crontab脚本提权 Crontab Script Privilege Escalation	是	Crontab脚本提权
	Crontab脚本修改 Crontab Script Change	是	Crontab脚本修改
	高危命令执行 High-risk Command Execution	是	高危命令执行

类型名称	子类型/子类型标识	内置	描述
	高危系统调用 High-Risk Syscall	是	高危系统调用
	关键文件/目录变更 File/Directory Change	是	关键文件/目录变更
	关键文件变更 Key File Change	是	关键文件变更
	进程提权 Process Privilege Escalation	是	进程提权
	进程异常行为 Process Abnormal Activity	是	进程异常行为
	敏感文件访问 Sensitive File Access	是	敏感文件访问
	容器进程异常 Container Abnormal Process	是	容器进程异常
	容器异常启动 Container Abnormal Start	是	容器异常启动
	数据库连接异常 Abnormal Database Connection	是	数据库连接异常
	网卡混杂模式 Network Adapter Promiscuous Mode	是	网卡混杂模式
	文件提权 File Privilege Escalation	是	文件提权
	文件异常删除 File Abnormal Delete	是	文件异常删除
	系统启动脚本改变 System Start Script Change	是	系统启动脚本改变

类型名称	子类型/子类型标识	内置	描述
	异常shell Abnormal Shell	是	异常shell
	异常命令执行 Abnormal Command Execution	是	异常命令执行
信息破坏	信息篡改 Information Tampering	是	信息篡改
	信息丢失 Information Loss	是	信息丢失
	信息假冒 Information Masquerading	是	信息假冒
	信息窃取 Information Interception	是	信息窃取
	信息泄漏 Information Disclosure	是	信息泄漏
	Linux网页篡改 Linux Web Page Tampering	是	Linux网页篡改
	Windows网页篡改 Windows Web Page Tampering	是	Windows网页篡改
	目录遍历 Directory Traversal	是	目录遍历
用户行为异常	Token恶意利用 Token Leakage	是	Token恶意利用
	Token恶意利用成功 Token Leakage Success	是	Token恶意利用成功
	异常用户首次访问 User First Cross Domain Access	是	异常用户首次访问

类型名称	子类型/子类型标识	内置	描述
	用户访问频率异常 User Access Frequency Abnormal	是	用户访问频率异常
	用户访问时段异常 User Hour Level Access Abnormal	是	用户访问时段异常
	用户使用特定IP下载行为异常 User IP Download Abnormal	是	用户使用特定IP下载行为异常
	用户首次访问桶对象 Client First Access	是	用户首次访问桶对象
	用户下载行为异常 User Download Abnormal	是	用户下载行为异常
	暴力破解 Brute Force Cracking	是	暴力破解
	违规登录 Illegal Login	是	违规登录
	未知用户异常行为 Unknown User Abnormal Activity	是	未知用户异常行为
	异常登录 Abnormal Login	是	异常登录
	用户登录尝试 User Login Attempt	是	用户登录尝试
	用户密码窃取 User Password Theft	是	用户密码窃取
	用户权限提升成功 User Privilege Escalation Succeeded	是	用户权限提升成功

类型名称	子类型/子类型标识	内置	描述
	用户权限提升失败 User Privilege Escalation Failed	是	用户权限提升失败
	用户首次登录 User First login	是	用户首次登录
	用户账号删除 User Account Removed	是	用户账号删除
	用户账号添加 User Account Added	是	用户账号添加
	用户组变更 User Group Changed	是	用户组变更
	用户组删除 User Group Removed	是	用户组删除
	用户组添加 User Group Added	是	用户组添加
	账号伪冒 Account Forgery	是	账号伪冒
	ECS可疑账号创建 Suspicious Ecs User Create	是	ECS可疑账号创建
	ECS账号权限修改 ECS User Escalate Privilege	是	ECS账号权限修改
	IAM可疑账号创建 Suspicious IAM Account Create	是	IAM可疑账号创建
	IAM账号权限修改 IAM Permissons Escalation	是	IAM账号权限修改
	暴力破解登录ECS ECS BruteForce Login	是	暴力破解登录ECS

类型名称	子类型/子类型标识	内置	描述
	暴力破解登录IAM IAM BruteForce Login	是	暴力破解登录IAM
	非法系统账号 Invalid System Account	是	非法系统账号
	风险账号 Risky Account	是	风险账号
	可疑IP登录ECS Suspicious IP Address Login	是	可疑IP登录ECS
	可疑IP登录IAM Suspicious IP Address Login	是	可疑IP登录IAM
	异常登录IAM IAM Abnormal Login	是	异常登录IAM
	异地登录ECS Instance Credential Exfiltration	是	异地登录ECS
	用户登录成功 User Login Success	是	用户登录成功
	用户登录拒绝 User Login Denied	是	用户登录拒绝
	用户账号变更 User Account Changed	是	用户账号变更
资源操控	恶意逻辑插入 Malicious Logic Insertion	是	恶意逻辑插入
	基础设施操纵 Infrastructure Manipulation	是	基础设施操纵
	配置/环境操纵 Configuration/ Environment Manipulation	是	配置/环境操纵

类型名称	子类型/子类型标识	内置	描述
	容器逃逸 Container Escape	是	容器逃逸
	容器资源操纵 Container Resource Manipulation	是	容器资源操纵
	软件完整性 Software Integrity Attack	是	软件完整性
资源侦查	端口探测数量异常 Port Detection	是	端口探测数量异常
	ARP 扫描 ARP Scan	是	ARP 扫描
	DNS探测 DNS Recon	是	DNS探测
	Hypervisor探测 Hypervisor Recon	是	Hypervisor探测
	ICMP探测 ICMP Recon	是	ICMP探测
	Linux探测 Linux Recon	是	Linux探测
	MacOS探测 MacOS Recon	是	MacOS探测
	NMAP扫描 NMAP Scan	是	NMAP扫描
	RPC请求探测 RPC Recon	是	RPC请求探测
	SNMP扫描 SNMP Recon	是	SNMP扫描
	TCP扫描 TCP Recon	是	TCP扫描
	UDP扫描 UDP Recon	是	UDP扫描
	Unix探测 Unix Recon	是	Unix探测

类型名称	子类型/子类型标识	内置	描述
	WEB探测 Web Recon	是	WEB探测
	Windows探测 Windows Recon	是	Windows探测
	加密渗透扫描 Encrypted Penetration Scan	是	加密渗透扫描
	普通扫描事件 General Scanner	是	普通扫描事件
	数据库探测 Database Recon	是	数据库探测
	邮件探测 Mail Recon	是	邮件探测
	主机扫描 Host Scan	是	主机扫描
	组合探测 Misc Recon	是	组合探测
	端口扫描 Port Scan	是	端口扫描

内置事件类型

表 6-3 内置事件类型列表

类型名称	子类型/子类型标识	内置	描述
DDoS攻击	DNS协议攻击 Tcp Dns	是	DNS协议攻击
	异常端口通信 Unusual Network Port	是	异常端口通信
	异常协议攻击 Unusual Protocol	是	异常协议攻击
	ACK Flood ACK Flood	是	ACK Flood
	BGP Flood攻击 BGP Flood Attack	是	BGP Flood攻击
	DNS IP TTL DNS IP TTL Check Fail	是	DNS IP TTL
	DNS Reply Flood攻击 DNS Reply Flood	是	DNS Reply Flood 攻击
	DNS查询攻击 DNS Query Flood	是	DNS查询攻击
	DNS大小异常 DNS Size Abnormal	是	DNS大小异常
	DNS反射 DNS Reflection	是	DNS反射
	DNS返回域名流异常 DNS Reply Domain Flow Abnormal	是	DNS返回域名流异常
	DNS格式错误 DNS Format Error	是	DNS格式错误
	DNS缓存匹配 DNS Cache Match	是	DNS缓存匹配

类型名称	子类型/子类型标识	内置	描述
	DNS缓存投毒 DNS Cache Poisoning	是	DNS缓存投毒
	DNS请求域名流异常 DNS Request Domain Flow Abnormal	是	DNS请求域名流异常
	DNS无效域名 DNS No Such Name	是	DNS无效域名
	FIN/RST Flood FIN/RST Flood	是	FIN/RST Flood
	HTTPS Flood HTTPS Flood	是	HTTPS Flood
	HTTP慢速攻击 HTTP Slow Attack	是	HTTP慢速攻击
	ICMP协议封禁 ICMP Protocol Block	是	ICMP协议封禁
	IP信誉 IP Reputation	是	IP信誉
	SIP Flood SIP Flood	是	SIP Flood
	SIP源速率异常 SIP Source Rate Abnormity	是	SIP源速率异常
	SYN Flood SYN Flood	是	SYN Flood
	SYN-ACK Flood SYN-ACK Flood	是	SYN-ACK Flood
	TCP带宽溢出 TCP Bandwidth Overflow	是	TCP带宽溢出
	TCP多连接攻击 TCP Connection Flood	是	TCP多连接攻击

类型名称	子类型/子类型标识	内置	描述
	TCP分片带宽溢出 TCP Fragment Bandwidth Overflow	是	TCP分片带宽溢出
	TCP分片攻击 TCP Fragment Flood	是	TCP分片攻击
	TCP畸形报文 TCP Malformed	是	TCP畸形报文
	TCP认证UDP攻击 TCP-authenticated UDP Attack	是	TCP认证UDP攻击
	TCP协议封禁 TCP Protocol Block	是	TCP协议封禁
	UDP带宽溢出 UDP Bandwidth Overflow	是	UDP带宽溢出
	UDP分片 UDP Fragment Flood	是	UDP分片
	UDP分片带宽溢出 UDP Fragment Bandwidth Overflow	是	UDP分片带宽溢出
	UDP畸形报文 UDP Malformed	是	UDP畸形报文
	UPD协议封禁 UDP Protocol Block	是	UPD协议封禁
	URI监控 URI Monitor	是	URI监控
	暗网IP Dark IP	是	暗网IP
	单IP带宽溢出 Single IP Bandwidth Overflow	是	单IP带宽溢出

类型名称	子类型/子类型标识	内置	描述
	当前连接耗尽攻击 Concurrent Connections Flood	是	当前连接耗尽攻击
	端口扫描攻击 Port Scanning Attack	是	端口扫描攻击
	恶意域名攻击 Malicious Domains Attack	是	恶意域名攻击
	反恶意软件 Anti-Malware	是	反恶意软件
	分布式拒绝服务攻击 DDOS	是	分布式拒绝服务攻击
	分区带宽溢出 Zone Bandwidth Overflow	是	分区带宽溢出
	过滤器攻击 Filter Attack	是	过滤器攻击
	黑名单 Blacklist	是	黑名单
	僵尸网络/特洛伊木马/蠕虫 Botnets/Trojan horses/Worms Attack	是	僵尸网络/特洛伊木马/蠕虫
	目的IP新会话限速 Destination IP new session rate limiting	是	目的IP新会话限速
	其他Flood攻击 Other Flood	是	其他Flood攻击
	其他带宽溢出 Other Bandwidth Overflow	是	其他带宽溢出
	其他全局异常 Global Other Abnormal	是	其他全局异常

类型名称	子类型/子类型标识	内置	描述
	其他协议封禁 Other Protocol Block	是	其他协议封禁
	全局ICMP异常 Global ICMP Abnormal	是	全局ICMP异常
	全局TCP分片异常 Global TCP Fragment Abnormal	是	全局TCP分片异常
	全局TCP异常 Global TCP Abnormal	是	全局TCP异常
	全局UDP分片异常 Global UDP Fragment Abnormal	是	全局UDP分片异常
	全局UDP异常 Global UDP Abnormal	是	全局UDP异常
	网页攻击 Web Attack	是	网页攻击
	位置攻击 Location Attack	是	位置攻击
	新连接耗尽攻击 New Connections Flood	是	新连接耗尽攻击
	域名劫持 Domain Hijacking	是	域名劫持
	源DNS返回流异常 Source DNS Reply Flow Abnormal	是	源DNS返回流异常
	源DNS请求流异常 Source DNS Request Flow Abnormal	是	源DNS请求流异常

类型名称	子类型/子类型标识	内置	描述
	主机流量溢出 Host Traffic Over Flow	是	主机流量溢出
	HTTP Flood HTTP Flood	是	HTTP Flood
	ICMP Flood ICMP Flood	是	ICMP Flood
	SSL Flood SSL Flood	是	SSL Flood
	TCP Flood TCP Flood	是	TCP Flood
	UDP Flood UDP Flood	是	UDP Flood
	XML Flood XML Flood	是	XML Flood
	放大攻击 Amplification	是	放大攻击
Web恶意代码	网页暗链 Web Page Dark Link	是	网页暗链
	网页挂马 Web Page Trojan	是	网页挂马
Web攻击	Webshell Webshell	是	Webshell
	WAF机器人 WAF Robot	是	WAF机器人
	白名单IP White IP	是	白名单IP
	攻击惩罚 Known Attack Source	是	攻击惩罚
	黑名单IP Black IP	是	黑名单IP

类型名称	子类型/子类型标识	内置	描述
	漏洞攻击 Vulnerability Attack	是	漏洞攻击
	命中隐私泄露规则 Leakage	是	命中隐私泄露规则
	默认 Default	是	默认
	扫描/爬虫 Scanner & Crawler	是	扫描/爬虫
	CC攻击 Challenge Collapsar	是	CC攻击
	IP信誉库 IP Repuation	是	IP信誉库
	SQL注入 SQL Injection	是	SQL注入
	XSS Cross-Site Scripting	是	XSS
	本地文件包含 Local Code Inclusion	是	本地文件包含
	地理访问控制拦截 Geo IP	是	地理访问控制拦截
	恶意爬虫 Malicious Web Crawlers	是	恶意爬虫
	反爬虫 Anticrawler	是	反爬虫
	防篡改 AntiTamper	是	防篡改
	非法请求 Illegal Access	是	非法请求
	黑白名单拦截 White or Black IP	是	黑白名单拦截

类型名称	子类型/子类型标识	内置	描述
	精准防护 Custom Rule	是	精准防护
	命令注入 Command Injection	是	命令注入
	目录遍历 Path Traversal	是	目录遍历
	网站木马 Website Trojan	是	网站木马
	网站信息防泄漏 Information Leakage	是	网站信息防泄漏
	网站信息泄露 Web Service Exfiltration	是	网站信息泄露
	远程代码执行 Remote Code Execute	是	远程代码执行
	远程文件包含 Remote Code Inclusion	是	远程文件包含
恶意软件	加密货币挖矿 Cryptomining	是	加密货币挖矿
	Docker恶意程序 Docker Malware	是	Docker恶意程序
	钓鱼 Phishing	是	钓鱼
	恶意广告软件 Adware	是	恶意广告软件
	恶意软件 Malicious Software	是	恶意软件
	黑客工具 Hacktool	是	黑客工具
	灰色软件 Grayware	是	灰色软件

类型名称	子类型/子类型标识	内置	描述
	间谍软件 Spyware	是	间谍软件
	垃圾邮件 Spam	是	垃圾邮件
	Rootkit Rootkit	是	Rootkit
	Webshell Webshell	是	Webshell
	病毒、蠕虫 Virus and Worm	是	病毒、蠕虫
	恶意文件 Malicous File	是	恶意文件
	反弹shell Reverse Shell	是	反弹shell
	后门木马 Backdoor Trojan	是	后门木马
	僵尸网络程序 Botnet Program	是	僵尸网络程序
	勒索软件 Ransomware	是	勒索软件
	挖矿程序 Bitcoin Miner	是	挖矿程序
	挖矿软件 Mining Software	是	挖矿软件
风险审计	Webcms漏洞 Webcms Vulnerability	是	Webcms漏洞
	Windows OS 漏洞 Windows Vulnerability	是	Windows OS 漏洞
	本地访问漏洞 Local Access Vulnerability	是	本地访问漏洞

类型名称	子类型/子类型标识	内置	描述
	错误配置策略 Mis-Configured Policy	是	错误配置策略
	其它OS漏洞 Other OS Vulnerability	是	其它OS漏洞
	其它漏洞 Other Vulnerability	是	其它漏洞
	应用程序漏洞 Application Vulnerability	是	应用程序漏洞
	远程访问漏洞 Remote Access Vulnerability	是	远程访问漏洞
风险审计	弱口令 Weak Password	是	弱口令
	系统风险配置 System Risk Configuration	是	系统风险配置
攻击探测	钓鱼 Phishing	是	钓鱼
	网络拓扑构建 Map Network Topology	是	网络拓扑构建
	账户、组信息收集 Identify Groups/ Roles	是	账户、组信息收集
	指纹扫描 Fingerprinting	是	指纹扫描
	主机发现 Determine IP Address	是	主机发现

类型名称	子类型/子类型标识	内置	描述
漏洞利用	ActiveX漏洞利用 ActiveX Exploit	是	ActiveX漏洞利用
	CGI攻击 CGI Attack	是	CGI攻击
	DNS漏洞利用 DNS Exploit	是	DNS漏洞利用
	FTP漏洞利用 FTP Exploit	是	FTP漏洞利用
	Hadoop漏洞利用 Hadoop Vulnerability Exploit	是	Hadoop漏洞利用
	Hypervisor漏洞利用 Hypervisor Exploit	是	Hypervisor漏洞利用
	LDAP注入攻击 LDAP Injection Attack	是	LDAP注入攻击
	MacOS漏洞利用 MacOS Exploit	是	MacOS漏洞利用
	MySQL漏洞利用 MySQL Vulnerability Exploit	是	MySQL漏洞利用
	Office软件漏洞利用 Office Exploit	是	Office软件漏洞利用
	Redis漏洞利用 Redis Vulnerability Exploit	是	Redis漏洞利用
	RPC漏洞利用 RPC Exploit	是	RPC漏洞利用
	SQL注入 SQL Injection	是	SQL注入
	SSH漏洞利用 SSH Exploit	是	SSH漏洞利用

类型名称	子类型/子类型标识	内置	描述
	SSI注入攻击 SSI Injection Attack	是	SSI注入攻击
	Struts2 OGNL注入 Struts2 OGNL Injection	是	Struts2 OGNL注入
	Telnet漏洞利用 TELNET Exploit	是	Telnet漏洞利用
	Unix漏洞利用 Unix Exploit	是	Unix漏洞利用
	Web漏洞利用 Web Exploit	是	Web漏洞利用
	XSS攻击 Cross-Site Scripting	是	XSS攻击
	本地文件包含 Local File Inclusion	是	本地文件包含
	恶意文件投递 Malicious File Delivery	是	恶意文件投递
	恶意文件执行 Malicious File Execution	是	恶意文件执行
	缓冲区溢出攻击 Buffer Overflow	是	缓冲区溢出攻击
	会话劫持 Session Hijack	是	会话劫持
	口令猜测 Password Cracking	是	口令猜测
	浏览器漏洞利用 Browser Exploit	是	浏览器漏洞利用
	弱口令访问 Weak Password Access	是	弱口令访问
	数据库漏洞利用 Database Exploit	是	数据库漏洞利用

类型名称	子类型/子类型标识	内置	描述
	未知漏洞利用 Unknown Exploit	是	未知漏洞利用
	隐藏链接访问 Hide Link Access	是	隐藏链接访问
	邮件漏洞利用 Mail Exploit	是	邮件漏洞利用
	远程代码执行 Remote Code Execution	是	远程代码执行
	远程访问漏洞利用 Remote Access Exploit	是	远程访问漏洞利用
	远程文件包含攻击 Remote File Inclusion	是	远程文件包含攻击
	远程文件注入 Remote File Injection	是	远程文件注入
	组合漏洞利用 Misc Exploit	是	组合漏洞利用
	CMS漏洞 CMS Exploit	是	CMS漏洞
	CSRF攻击 CSRF Attack	是	CSRF攻击
	JNDI注入攻击 JNDI Injection Attack	是	JNDI注入攻击
	Linux漏洞 Linux Exploit	是	Linux漏洞
	SMB漏洞 SMB Exploit	是	SMB漏洞
	Windows漏洞 Windows Exploit	是	Windows漏洞
	XML注入 XML Injection	是	XML注入

类型名称	子类型/子类型标识	内置	描述
	代码注入 Code Injection	是	代码注入
	漏洞逃逸攻击 Vulnerability Escape Attack	是	漏洞逃逸攻击
	命令执行 Command Execution	是	命令执行
	命令注入 Command Injection	是	命令注入
	文件逃逸攻击 File Escape Attack	是	文件逃逸攻击
	虚拟机逃逸攻击 VM Escape Attack	是	虚拟机逃逸攻击
	一般漏洞利用 General Exploit	是	一般漏洞利用
命令与控制	ECS存在当前IP被用于向高危网络发送消息 Command Control Activity	是	ECS存在当前IP被用于向高危网络发送消息
	可疑的域名、IP地址、端口动态生成访问 Dynamic Resolution	是	可疑的域名、IP地址、端口动态生成访问
	其他可疑连接 Abnormal Connection	是	其他可疑连接
	其他可疑行为 Abnormal Behaviour	是	其他可疑行为
	外连恶意DNS Malicious Domain Query	是	外连恶意DNS

类型名称	子类型/子类型标识	内置	描述
	外连恶意IP地址 Malicious Ip Address Query	是	外连恶意IP地址
	隐蔽隧道 Protocol Tunneling	是	隐蔽隧道
	与矿池地址通信 Mining Pool Communication	是	与矿池地址通信
其他	公共舆情 Public_Opinion	是	公共舆情
	云防火墙攻击 CFW_RISK	是	云防火墙攻击
数据泄露	数据窃取 Steal Data	是	数据窃取
	违规外传 Transfer Data Abnormal	是	违规外传
网络异常行为	IP访问频率异常 IP Access Frequency Abnormal	是	IP访问频率异常
	IP切换异常 IP Switch Abnormal	是	IP切换异常
	IP首次访问 IP First Access	是	IP首次访问
	Sinkhole攻击IP访问 Sink Hole	是	Sinkhole攻击IP访问
	代理IP访问 Proxy	是	代理IP访问
	恶意资源访问 Resource Permissions	是	恶意资源访问
	欺诈付款网站IP/域名访问 Payment	是	欺诈付款网站IP/域名访问

类型名称	子类型/子类型标识	内置	描述
	洋葱网络IP访问 Tor	是	洋葱网络IP访问
	C&C异常通信 C&C Abnormal Communication	是	C&C异常通信
	IP黑名单访问 IP Blacklist Access	是	IP黑名单访问
	URL黑名单访问 URL Blacklist Access	是	URL黑名单访问
	恶意URL访问 Malicious URL Access	是	恶意URL访问
	恶意域名访问 Malicious Domain Name Access	是	恶意域名访问
	非授权访问企图 Unauthorized Access Attemp	是	非授权访问企图
	可疑的网络流量 Suspicious Network Traffic	是	可疑的网络流量
	容器网络外联 Container Network Connect	是	容器网络外联
	未知网络访问 Unknown Abnormal Network Access	是	未知网络访问
	文件MD5黑名单访问 File MD5 Blacklist Access	是	文件MD5黑名单访问
	异常外联行为 Abnormal External Behavior	是	异常外联行为

类型名称	子类型/子类型标识	内置	描述
	域名黑名单访问 Domain Name Blacklist Access	是	域名黑名单访问
	周期外联通信 Periodic Outreach	是	周期外联通信
	可疑的端口转发 Suspicious Port Forward	是	可疑的端口转发
无文件攻击	VDSO劫持 VDSO Hijacking	是	VDSO劫持
	动态库注入进程 Dynamic Library Inject Process	是	动态库注入进程
	关键配置变更 Critical File Change	是	关键配置变更
	环境变量变更 Environment Change	是	环境变量变更
	进程注入 Process Inject	是	进程注入
	内存文件进程 Memfd Process	是	内存文件进程
	文件操纵 File Manipulation	是	文件操纵
系统行为异常	Crontab可疑任务 Crontab Suspicious Task	是	Crontab可疑任务
	Socket连接异常 Abnormal Socket Connection	是	Socket连接异常
	备份删除 Backup Deletion	是	备份删除
	非法数据库访问 Unauthorized Database Access	是	非法数据库访问

类型名称	子类型/子类型标识	内置	描述
	权限异常访问 Privilege Abnormal Access	是	权限异常访问
	日志异常变化 Unexpected Log Change	是	日志异常变化
	容器进程退出 Container Process Exist	是	容器进程退出
	未知主机异常行为 Unknown Host Abnormal Activity	是	未知主机异常行为
	文件黑名单访问 File blocklist access	是	文件黑名单访问
	文件权限异常改变 Unexpected File Permission Change	是	文件权限异常改变
	系统安全防护被禁用 System Security Protection disabled	是	系统安全防护被禁用
	系统账号变更 System Account Change	是	系统账号变更
	异常注册表操作 Abnormal Registry Operation	是	异常注册表操作
	Crontab脚本提权 Crontab Script Privilege Escalation	是	Crontab脚本提权
	Crontab脚本修改 Crontab Script Change	是	Crontab脚本修改
	高危命令执行 High-risk Command Execution	是	高危命令执行

类型名称	子类型/子类型标识	内置	描述
	高危系统调用 High-Risk Syscall	是	高危系统调用
	关键文件/目录变更 File/Directory Change	是	关键文件/目录变更
	关键文件变更 Key File Change	是	关键文件变更
	进程提权 Process Privilege Escalation	是	进程提权
	进程异常行为 Process Abnormal Activity	是	进程异常行为
	敏感文件访问 Sensitive File Access	是	敏感文件访问
	容器进程异常 Container Abnormal Process	是	容器进程异常
	容器异常启动 Container Abnormal Start	是	容器异常启动
	数据库连接异常 Abnormal Database Connection	是	数据库连接异常
	网卡混杂模式 Network Adapter Promiscuous Mode	是	网卡混杂模式
	文件提权 File Privilege Escalation	是	文件提权
	文件异常删除 File Abnormal Delete	是	文件异常删除
	系统启动脚本改变 System Start Script Change	是	系统启动脚本改变

类型名称	子类型/子类型标识	内置	描述
	异常shell Abnormal Shell	是	异常shell
	异常命令执行 Abnormal Command Execution	是	异常命令执行
信息破坏	信息篡改 Information Tampering	是	信息篡改
	信息丢失 Information Loss	是	信息丢失
	信息假冒 Information Masquerading	是	信息假冒
	信息窃取 Information Interception	是	信息窃取
	信息泄漏 Information Disclosure	是	信息泄漏
	Linux网页篡改 Linux Web Page Tampering	是	Linux网页篡改
	Windows网页篡改 Windows Web Page Tampering	是	Windows网页篡改
	目录遍历 Directory Traversal	是	目录遍历
用户行为异常	Token恶意利用 Token Leakage	是	Token恶意利用
	Token恶意利用成功 Token Leakage Success	是	Token恶意利用成功
	异常用户首次访问 User First Cross Domain Access	是	异常用户首次访问

类型名称	子类型/子类型标识	内置	描述
	用户访问频率异常 User Access Frequency Abnormal	是	用户访问频率异常
	用户访问时段异常 User Hour Level Access Abnormal	是	用户访问时段异常
	用户使用特定IP下载行为异常 User IP Download Abnormal	是	用户使用特定IP下载行为异常
	用户首次访问桶对象 Client First Access	是	用户首次访问桶对象
	用户下载行为异常 User Download Abnormal	是	用户下载行为异常
	暴力破解 Brute Force Cracking	是	暴力破解
	违规登录 Illegal Login	是	违规登录
	未知用户异常行为 Unknown User Abnormal Activity	是	未知用户异常行为
	异常登录 Abnormal Login	是	异常登录
	用户登录尝试 User Login Attempt	是	用户登录尝试
	用户密码窃取 User Password Theft	是	用户密码窃取
	用户权限提升成功 User Privilege Escalation Succeeded	是	用户权限提升成功

类型名称	子类型/子类型标识	内置	描述
	用户权限提升失败 User Privilege Escalation Failed	是	用户权限提升失败
	用户首次登录 User First login	是	用户首次登录
	用户账号删除 User Account Removed	是	用户账号删除
	用户账号添加 User Account Added	是	用户账号添加
	用户组变更 User Group Changed	是	用户组变更
	用户组删除 User Group Removed	是	用户组删除
	用户组添加 User Group Added	是	用户组添加
	账号伪冒 Account Forgery	是	账号伪冒
	ECS可疑账号创建 Suspicious Ecs User Create	是	ECS可疑账号创建
	ECS账号权限修改 ECS User Escalate Privilege	是	ECS账号权限修改
	IAM可疑账号创建 Suspicious IAM Account Create	是	IAM可疑账号创建
	IAM账号权限修改 IAM Permissons Escalation	是	IAM账号权限修改
	暴力破解登录ECS ECS BruteForce Login	是	暴力破解登录ECS

类型名称	子类型/子类型标识	内置	描述
	暴力破解登录IAM IAM BruteForce Login	是	暴力破解登录IAM
	非法系统账号 Invalid System Account	是	非法系统账号
	风险账号 Risky Account	是	风险账号
	可疑IP登录ECS Suspicious IP Address Login	是	可疑IP登录ECS
	可疑IP登录IAM Suspicious IP Address Login	是	可疑IP登录IAM
	异常登录IAM IAM Abnormal Login	是	异常登录IAM
	异地登录ECS Instance Credential Exfiltration	是	异地登录ECS
	用户登录成功 User Login Success	是	用户登录成功
	用户登录拒绝 User Login Denied	是	用户登录拒绝
	用户账号变更 User Account Changed	是	用户账号变更
资源操控	恶意逻辑插入 Malicious Logic Insertion	是	恶意逻辑插入
	基础设施操纵 Infrastructure Manipulation	是	基础设施操纵
	配置/环境操纵 Configuration/ Environment Manipulation	是	配置/环境操纵

类型名称	子类型/子类型标识	内置	描述
	容器逃逸 Container Escape	是	容器逃逸
	容器资源操纵 Container Resource Manipulation	是	容器资源操纵
	软件完整性 Software Integrity Attack	是	软件完整性
资源侦查	端口探测数量异常 Port Detection	是	端口探测数量异常
	ARP 扫描 ARP Scan	是	ARP 扫描
	DNS探测 DNS Recon	是	DNS探测
	Hypervisor探测 Hypervisor Recon	是	Hypervisor探测
	ICMP探测 ICMP Recon	是	ICMP探测
	Linux探测 Linux Recon	是	Linux探测
	MacOS探测 MacOS Recon	是	MacOS探测
	NMAP扫描 NMAP Scan	是	NMAP扫描
	RPC请求探测 RPC Recon	是	RPC请求探测
	SNMP扫描 SNMP Recon	是	SNMP扫描
	TCP扫描 TCP Recon	是	TCP扫描
	UDP扫描 UDP Recon	是	UDP扫描
	Unix探测 Unix Recon	是	Unix探测

类型名称	子类型/子类型标识	内置	描述
	WEB探测 Web Recon	是	WEB探测
	Windows探测 Windows Recon	是	Windows探测
	加密渗透扫描 Encrypted Penetration Scan	是	加密渗透扫描
	普通扫描事件 General Scanner	是	普通扫描事件
	数据库探测 Database Recon	是	数据库探测
	邮件探测 Mail Recon	是	邮件探测
	主机扫描 Host Scan	是	主机扫描
	组合探测 Misc Recon	是	组合探测
	端口扫描 Port Scan	是	端口扫描

内置威胁情报类型

表 6-4 内置威胁情报类型列表

类型名称/类型标识	内置	描述
IPv4 IPv4	是	IPv4
IPv6 IPv6	是	IPv6
邮件 Email	是	邮件
域名 domain	是	域名
URL URL	是	URL

类型名称/类型标识	内置	描述
其他 Unclassified	是	其他

内置漏洞类型

表 6-5 内置漏洞类型列表

类型名称/类型标识	内置	描述
网站漏洞 Website Vulnerabilities	是	网站漏洞
Linux软件漏洞 Linux Vulnerabilities	是	Linux软件漏洞
Web-CMS漏洞 Web-CMS Vulnerabilities	是	Web-CMS漏洞
Windows系统漏洞 Windows Vulnerabilities	是	Windows系统漏洞
应用漏洞 Application Vulnerabilities	是	应用漏洞

7 约束与限制

本文介绍安全云脑 SecMaster在使用过程中的约束和限制。

购买

表 7-1 购买

模块	约束与限制
配额数	• 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。 • 配额数最大限制为10000台。
增值包	• 基础版不支持购买增值包，如需使用增值包功能，请升级为标准版或专业版。 • 增值包不支持单独使用。 – 如果需要购买增值包，请先购买标准版或专业版。 – 如果退订了按需计费的专业版，系统将自动一并退订增值包。 – 如果退订了包周期计费的标准版或专业版，需手动一并退订增值包。
标签	最多支持为安全云脑添加10个标签。

工作空间

表 7-2 工作空间

模块	约束与限制
工作空间（Workspace）	• 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。 • 暂不支持在同一个浏览器的多个窗口进入不同的工作空间进行操作。
纳管环境	• 不支持纳管边缘环境：IEC、DEC、IES等边缘站点。 • 仅支持纳管Default项目，不支持纳管子项目。 • 不支持按EPS粒度纳管资源。
空间托管	• 单账号单Region内最多创建1个空间托管视图。 • 一个托管视图可以跨Region管理不同账号下的最多150个工作空间。 • 单账号最多创建10个账号委托。

安全报告

表 7-3 安全报告

模块	约束与限制
安全报告	单账号单workspace内，最多可创建10个安全报告（包含日报、周报和月报）。

告警模型

表 7-4 告警模型

模块	约束与限制
告警模型	• 单账号单Region单workspace最多创建100个告警模型。 • 一个告警模型的运行时间间隔须 ≥ 5分钟，查询数据的时间范围 ≤ 14天。

安全分析

表 7-5 安全分析

模块	约束与限制
查询与分析	● 单次查询分析最多支持返回500条结果。 ● 一个数据管道内最多创建50个快速查询，即最多可以将50个查询分析条件保存为快速查询。 ● 单次查询结果大于50000条时，准确率可能会下降。请通过缩短查询的时间范围、添加查询限制条件等方法减少查询结果的数量。 ● 使用聚合查询（例如group by语句）聚合多个字段时，第二个字段默认分桶数量为10，如果超出会有数据丢失的情况，将导致查询结果不准确。 ● 查询与分析结果保存为指标卡片时，单账号单Workspace最多保存100个。
数据空间	单账号单Region单Workspace最多创建5个数据空间。
数据管道	单账号单Region单数据空间最多创建20个数据管道。

事件、告警、情报、漏洞

表 7-6 安全报告

模块	约束与限制
漏洞	单账号单Workspace内，每天最多新增100个漏洞。
告警	● 单账号单Workspace内，每天最多新增100个告警。 ● 单账号单Workspace内，每天最多可以告警转事件100个。
事件	单账号单Workspace内，每天最多新增100个事件。
情报	单账号单Workspace内，每天最多新增100个情报。

安全编排

表 7-7 安全编排

模块	约束与限制
剧本	单账号单workspace内，单剧本调度频率时间 ≥ 5分钟。

模块	约束与限制
剧本和流程实例	单账号单workspace内一天内的重试次数限制如下： ● 手动重试：流程实例最大重试次数100次。重试之后，等剧本执行完毕之后才允许再次重试。 ● API接口重试：流程实例最大重试次数100次。重试之后，等剧本执行完毕之后才允许再次重试。
分类&映射	● 单账号单workspace内，分类&映射模板 ≤ 50个。 ● 单账号单workspace内，分类和映射的映射关系规格为1:100。 ● 单账号单workspace内，最多可新增分类&映射100个。

8 安全

8.1 责任共担

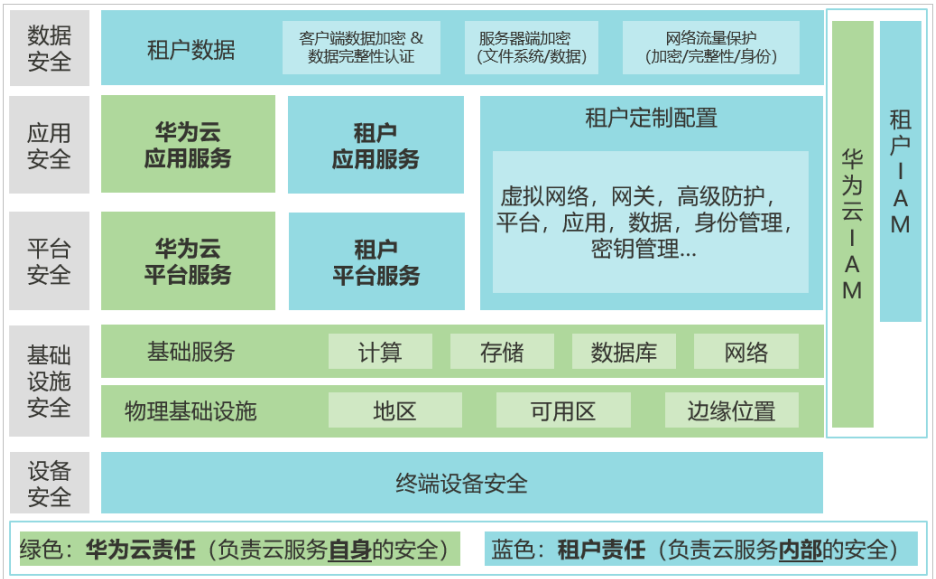
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图8-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 8-1 华为云安全责任共担模型



8.2 身份认证与访问控制

SecMaster对接了统一身份认证服务（Identity and Access Management，IAM）服务。SecMaster租户身份认证与访问控制通过IAM权限控制。

统一身份认证（Identity and Access Management，简称IAM）是华为云提供权限管理的基础服务，可以帮助SecMaster服务安全地控制访问权限。

通过IAM，可以将用户加入到一个用户组中，并用策略来控制他们对SecMasterr资源的访问范围。SecMaster权限可以通过细粒度定义允许和拒绝的访问操作，以此实现SecMaster资源的权限访问控制。

8.3 数据保护技术

SecMaster通过多种数据保护手段和特性，保证通过SecMaster的数据安全可靠。

表 8-1 SecMaster 的数据保护手段和特性

数据保护手段	简要说明
静态数据保护	SecMaster通过敏感数据加密保证用户流量中敏感数据的安全性。
传输中的数据保护	微服务间数据传输进行加密，防止数据在传输过程中泄露或被篡改。用户的配置数据传输采用安全协议HTTPS，防止数据被窃取。
数据完整性校验	1. SecMaster接入云服务告警、漏洞和基线等时，有数据完整性校验。 2. SecMaster核心数据面进程启动时，配置数据执行可靠事件模式确保数据完整性（网络抖动、延迟、配置数据重发&重试等场景）。

数据保护手段	简要说明
数据隔离机制	租户区与管理面隔离，租户的所有操作权限隔离，不同租户间的策略、日志等数据隔离。
数据销毁机制	考虑到残留数据导致的信息泄露问题，华为云根据客户等级设定了不同的保留期时长，保留期到期仍未续订或充值，存储在云服务中的数据将被删除，云服务资源将被释放。SecMaster对云服务自动感知并在保留期到期后释放资源。

同时，SecMaster服务充分尊重用户隐私，遵循法律法规，不会采集和存储任何用户隐私数据。更多隐私数据使用和保护问题，请参考**隐私政策声明**。

8.4 审计与日志

- 审计

  云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

  用户开通云审计服务并创建和配置追踪器后，CTS可记录SecMaster的管理事件和数据事件用于审计。

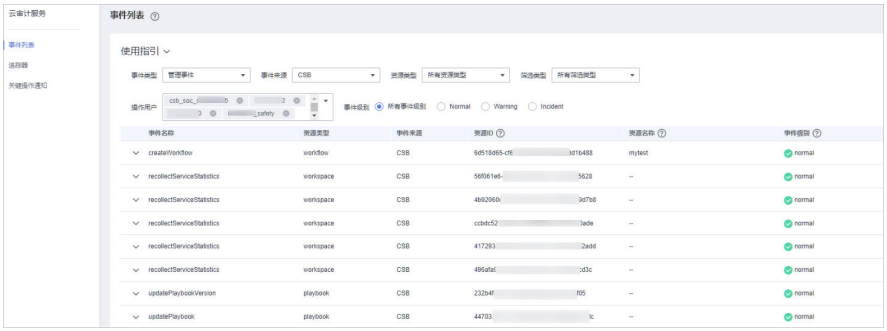
  CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

- 日志
  - 查询

    出于分析或审计等目的，用户开启了云审计服务后，系统开始记录SecMaster资源的操作。云审计服务管理控制台保存最近7天的操作记录。

    关于SecMaster云审计日志的查看，如**图8-2**所示。

    图 8-2 查询日志

8.5 服务韧性

华为云SecMaster当前主要部署在国内，已部署数据中心都处于正常运营状态，无一闲置。数据中心互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。为了减少由硬件故障、自然灾害或其他灾难带来的服务中断，华为云SecMaster提供灾难恢复计划。

当发生故障时，SecMaster的五级可靠性架构支持不同层级的可靠性，因此具有更高的可用性、容错性和可扩展性。

华为云SecMaster当前主要部署在国内，并在多个分区部署，同时SecMaster的所有管理面、引擎等组件均采用主备或集群方式部署。

8.6 监控安全风险

SecMaster已对接云监控服务（Cloud Eye，CES），可以通过管理控制台，查看SecMaster的相关运行指标，及时了解SecMaster运行状况。CES服务是华为云为用户提供一个针对各种云上资源的立体化监控平台，用户通过云监控服务可以全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

SecMaster自身作为云上安全运营作战平台，可以接入其他云服务的安全告警，按照告警类型和等级统一维度呈现，可以准确实时监控云上威胁攻击、检测您资产中的安全告警事件；定义威胁告警通知，设置每日定时告警通知和实时告警通知，通过接收消息通知及时了解威胁风险。定义监控的威胁名单、告警类型、告警级别等，选择性呈现关注的威胁告警。帮助用户及时了解安全状况，从而起到预警作用。

CES的详细介绍和开通配置方法，请参见**CES快速入门**。

表 8-2 监控

事件来源	事件名称	事件级别	事件说明	处理建议	事件影响
SYS.SecMaster	独享引擎创建失败	重要	一般是由于底层资源不足等原因导致。	提交工单让运维在后台协调资源再重试。	无法创建独享引擎
SYS.SecMaster	独享引擎运行异常	紧急	一般是由于流量过大或者恶意流程，插件导致。	1. 排查流程，插件执行是否占用资源过多。 2. 查看实例监控，短期内是否实例数量暴增。	无法执行实例
SYS.SecMaster	剧本实例执行失败	一般	一般是由于剧本，流程配置出错导致。	通过实例监控查看失败原因，修改剧本，流程配置。	无
SYS.SecMaster	剧本实例突增	一般	一般是由于剧本，流程配置出错导致。	通过实例监控查看突增原因，修改剧本，流程配置。	无
SYS.SecMaster	日志消息突增	重要	上游服务产生大量日志，导致消息快速增加。	需要排查上游服务业务是否正常。	无
SYS.SecMaster	日志消息突减	重要	上游服务产生日志突然变小。	需要排查上游业务是否正常	无

告警监控相关内容详细操作请参见：

- **漏洞管理**
- **基线检查**
- **安全报告**

8.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 8-3 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 8-4 资源中心

8.8 安全编排

SecMaster的安全编排功能可以针对云上安全事件提供安全编排剧本，实现安全事件的高效、自动化响应处置。其主要功能如下：

- 剧本管理：内置自动响应的剧本，支持按需定义扩展。

  编写剧本的过程就是将安全运营流程和规程转换为剧本，并在剧本中将各种应用编排到一起的过程，也是将人读安全运营流程转换为机读工作流的过程。
- 流程管理：绘制流程图响应剧本触发。
- 资产管理：支持对关键资产、安全资产等进行统一管理呈现。
- 实例管理：支持对运行的实例进行监控管理及记录查看。
- 安全事件自动化响应：对需要处理的安全事件（incidence）以及可疑事件，通过安全编排实现自动化处置及事件调查。

安全编排设置方法请参见**安全编排**。

9 SecMaster 权限管理

如果您需要对华为云上购买的安全云脑（SecMaster）资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并使用策略来控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有安全云脑（SecMaster）的使用权限，但是不希望他们拥有删除SecMaster等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用SecMaster，但是不允许删除SecMaster的权限策略，控制他们对SecMaster资源的使用范围。

如果账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用SecMaster的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账户中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

SecMaster 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

SecMaster部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问SecMaster时，需要先切换至授权区域。

权限根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对SecMaster服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

如表9-1所示，包括了SecMaster的所有系统权限。

表 9-1 SecMaster 系统权限

系统角色/策略名称	描述	类别
SecMaster FullAccess	安全云脑的所有权限。	系统策略
SecMaster ReadOnlyAccess	安全云脑只读权限，拥有该权限的用户仅能查看安全云脑数据，不具备安全云脑配置权限。	系统策略

SecMaster 控制台功能依赖的角色或策略

IAM主账号给IAM子账号授予**区域级**SecMaster FullAccess权限后，在安全云脑控制台使用服务委托授权操作时，还需要给子账号授予IAM创建委托权限、委托授权策略权限，具体说明如下：

表 9-2 SecMaster 控制台依赖服务的角色或策略

控制台功能	依赖服务	需配置角色/策略
服务委托授权	统一身份认证服务 IAM	IAM子账号设置了**区域级**SecMaster FullAccess权限后，需要增加IAM创建委托权限、委托授权策略权限，具体操作请参见**IAM子账号补充授权操作**。

相关介绍

- **IAM产品介绍**
- **创建用户组、用户并授予SecMaster权限**
- **SecMaster自定义策略**
- **SecMaster权限及授权项**

SecMaster FullAccess 策略内容

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "secmaster:*:*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:vpcs:list",
                "vpc:subnets:get",
                "vpcep:endpoints:*"
            ],
            "Effect": "Allow"
        },
        {
```



```
            "Action": [
                "obs:bucket:ListBucketVersions"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:permissions:checkRoleForAgencyOnDomain",
                "iam:permissions:checkRoleForAgencyOnProject",
                "iam:permissions:checkRoleForAgency",
                "iam:permissions:grantRoleToAgency",
                "iam:permissions:grantRoleToAgencyOnDomain",
                "iam:permissions:grantRoleToAgencyOnProject",
                "iam:policies:*",
                "iam:agencies:*",
                "iam:roles:*",
                "iam:users:listUsers",
                "iam:tokens:assume"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "organizations:organizations:get",
                "organizations:delegatedAdministrators:list",
                "organizations:roots:list",
                "organizations:ous:list",
                "organizations:accounts:list"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ecs:cloudServers:list"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "sts:agencies:assume"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "lts:log*:list*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

SecMaster ReadOnlyAccess 策略内容

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "secmaster:*:get*",
                "secmaster:*:list*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:vpcs:list",
                "vpc:subnets:get",
                "vpcep:endpoints:get",
```

```
            "vpcep:endpoints:list"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "obs:bucket:ListBucketVersions"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "iam:permissions:checkRoleForAgencyOnDomain",
            "iam:permissions:checkRoleForAgencyOnProject",
            "iam:permissions:checkRoleForAgency",
            "iam:policies:get*",
            "iam:policies:list*",
            "iam:agencies:get*",
            "iam:agencies:list*",
            "iam:roles:get*",
            "iam:roles:list*",
            "iam:users:listUsers"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "organizations:organizations:get",
            "organizations:delegatedAdministrators:list",
            "organizations:roots:list",
            "organizations:ous:list",
            "organizations:accounts:list"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "ecs:cloudServers:list"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "lts:log*:list*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

IAM 子账号补充授权操作

SecMaster部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效。

当给IAM子账号进行区域级项目授权SecMaster FullAccess授权后，由于安全云脑对其他云服务资源有依赖，因此，还需要给IAM子账号进行全局级Action操作授权。具体添加权限如下：

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "iam:roles:listRoles",
```



```
            "iam:agencies:listAgencies",
            "iam:permissions:checkRoleForAgencyOnDomain",
            "iam:permissions:checkRoleForAgencyOnProject",
            "iam:permissions:checkRoleForAgency",
            "iam:agencies:createAgency",
            "iam:permissions:grantRoleToAgencyOnDomain",
            "iam:permissions:grantRoleToAgencyOnProject",
            "iam:permissions:grantRoleToAgency"
        ]
    }
  ]
}
```

其中，“iam:permissions:grantRoleToAgencyOnDomain”、“iam:permissions:grantRoleToAgency”、“iam:permissions:grantRoleToAgencyOnProject”、“iam:agencies:createAgency”为使用安全云脑时的**服务委托授权**操作权限，非IAM子账号必选权限，请根据需要进行配置，授权情况说明如下：

- 未授权：仅IAM主账号可进行服务委托授权操作，且IAM子账号进行服务委托授权操作时会出现报错提示。
- 授权：IAM主账号及已授权的IAM子账号均可以进行服务委托授权操作。

10 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**主机安全**（Host Security Service，HSS）、**Web应用防火墙**（Web Application Firewall，WAF）、**Anti-DDoS流量清洗**（Anti-DDoS）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。更多说明请参见**安全云脑与其他安全服务之间的关系与区别**。

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。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS），为SecMaster提供云服务资源的操作记录，记录内容包括从访问管理控制台发起的云服务资源操作请求以及每次请求的结果，供您查询、审计和回溯使用。

CTS记录SecMaster相关操作事件，方便用户日后的查询、审计和回溯。

与云监控服务的关系

云监控（Cloud Eye）为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。用户可以通过事件及时了解安全云脑的状况，并及时收到异常报警做出反应，保证业务顺畅运行。具体请参见《云监控服务用户指南》。

与标签管理服务的关系

标签管理服务（Tag Management Service，简称TMS）是一种快速便捷将标签集中管理的可视化服务，方便用户通过标签标识管理工作空间实例。

表 10-1 标签管理服务支持的 SecMaster 操作列表

操作名称	资源类型	事件名称
查询资源实例列表	Workspace	listResourceInstance
查询资源实例数量	Workspace	countResourceInstance
批量查询资源标签	Tag	batchTagResources
批量删除资源标签	Tag	batchUntagResources
查询项目标签	Tag	listProjectTag
更新标签值	Tag	updateTagValue
查询资源标签	Tag	listResourceTag

与企业管理的关系

企业中有多个项目，多个项目的资源需要分开结算，且分属不同人员进行管理。同时项目可以单独启动或停止，对其他项目没有影响。**企业管理**可以针对企业中的每个项目，分别建立企业项目，管理各自的资源，并且针对不同的企业项目，设置不同的人员进行管理。

安全云脑支持企业管理，您可以将安全云脑上的资源按照企业项目进行管理，并设置每个企业项目的用户权限。

11 基本概念

11.1 安全运营中心

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

SOC 的功能

SOC团队承担以下职能来帮助防止、响应攻击并在遭到攻击后恢复。

- **资产和工具清单**

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

- **减少攻击面**

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

11.2 总览和态势总览

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。总览页面实时呈现安全云脑所有工作空间的整体安全评估结果，查看方法请参见**查看总览**。

态势总览

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

安全风险

安全风险是对资产安全状况的综合评估，反映了一段时间内资产遭受的安全风险。安全风险通常体现为一个量化的数值，便于用户理解目前资产的安全状况，数值大小并不代表资产的安全或危险，仅作为资产遭受攻击严重程度的参考。

安全评分

安全云脑实时呈现您云上资产的整体安全评估状况，并根据不同版本的威胁检测能力，评估整体资产安全健康得分。

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

如下将介绍在安全评分中，不同分值的含义以及扣分项的详细情况。

- 安全分值

  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 11-1 安全分值表

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

- 安全评分扣分项

  安全评分扣分项及其分值情况如下所示：

表 11-2 安全评分扣分项

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

11.3 工作空间

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。

11.4 告警管理

威胁告警

广义的威胁告警是指由于自然因素、人为因素或软硬件本身的原因，对信息系统造成危害的事件，或对社会造成负面影响的威胁。对于安全云脑来讲，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。

事件

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

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

告警

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

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

告警的目的是及时通知相关人员，以便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。

11.5 安全编排

分类和映射

分类和映射是指对云服务告警进行类型匹配和字段映射。

安全编排

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

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

剧本

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

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

流程

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

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

剧本和流程的关系

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

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

插件管理

- 插件：是包含函数、连接器、公共库的聚合。插件有自定义插件和商业插件两种类型，其中，自定义的插件可以在集市中显示，也可以在剧本中使用。
- 插件集：是具有相同业务场景的插件集合。
- 函数：是可以在剧本中选用的执行函数，在剧本中执行特定的行为。
- 连接器：是用于连接数据源，将告警、事件等安全数据接入安全云脑，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。

资产连接

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。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。

实例监控

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

11.6 安全分析

生产者

是用来构建并传输数据到服务端的逻辑概念，负责把数据放入消息队列。

订阅器

用于订阅安全云脑管道消息，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。