天翼云·态势感知（专业版）

用户使用指南

天翼云科技有限公司

目 录

1 产品介绍

1.1 什么是态势感知？

态势感知（Situation Awareness，SA）是可视化威胁检测和分析的平台。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为用户呈现出全局安全攻击态势。

工作原理

态势感知通过采集全网流量数据和安全防护设备日志信息，并利用大数据安全分析平台进行处理和分析，态势感知检测出威胁告警，实时为用户呈现完整的全网攻击态势，进而为安全事件的处置决策提供依据。

1.2 功能特性

态势感知提供全局安全态势集中管理，包括安全概览、资产管理、威胁告警、基线检查、检查结果、日志管理、产品集成等功能。

安全概览

安全概览呈现云上整体安全评估状况，并联动其他云安全服务，集中展示云上安全。

表1-1 安全概览功能介绍

功能模块	功能详情
安全评分	根据分析检测能力，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。

资源管理

态势感知支持呈现云上资产实时安全状态。

表1-2 资源管理功能说明

功能模块	功能详情
资源管理	同步当前帐号中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并提供解决方案。

威胁告警

“实时监控”云上威胁攻击，提供告警通知和监控，记录近 180 天告警事件详情，分析威胁攻击情况，并针对典型威胁事件预置策略实施防御手段。

目前，支持检测和呈现威胁告警事件，包括 DDoS、暴力破解、Web 攻击、后门木马、僵尸主机、异常行为、漏洞攻击和命令与控制。

表1-3 威胁告警功能说明

功能模块	功能详情
告警列表	列表呈现威胁告警事件统计信息，支持查看告警事件和受威胁资产详情，并支持导出全部告警事件。
威胁分析	支持从“攻击源”或“被攻击资产”查询威胁攻击，统计威胁攻击次数或资产被攻击次数。
告警监控	自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。
通知告警	自定义威胁告警通知，支持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。

威胁告警事件

默认“实时监控”并上报威胁告警事件，支持检测和呈现威胁告警事件，包括 DDoS、暴力破解、Web 攻击、后门木马、僵尸主机、异常行为、漏洞攻击和命令与控制。

表1-4 威胁告警事件说明

告警名称	威胁告警说明
DDoS	“实时检测”互联网主机的 DDoS 攻击。

告警名称	威胁告警说明
	共支持检测 100+种子类型 DDoS 威胁。 • 网络层攻击 NTP Flood 攻击、CC 攻击等。 • 传输层攻击 SYN Flood 攻击、ACK Flood 攻击等。 • 会话层攻击 SSL 连接攻击等。 • 应用层攻击 HTTP Get Flood 攻击、HTTP Post Flood 攻击等。
暴力破解	“实时检测”入侵资产的行为和主机资产内部的风险，检测 SSH、RDP、FTP、SQL Server、MySQL 等账户是否遭受的口令破解攻击，以及检测资产账户是否被破解异常登录。 共支持检测 22 种子类型的暴力破解威胁。 • 支持检测的暴力破解威胁 包括 SSH 暴力破解（2 种）、RDP 暴力破解、MSSQL 暴力破解、MySQL 暴力破解、FTP 暴力破解、SMB 暴力破解（3 种）、HTTP 暴力破解（4 种）、Telnet 暴力破解。 • 接入的 HSS 服务上报的告警事件 包括 SSH 暴力破解、RDP 暴力破解、FTP 暴力破解、MySQL 暴力破解、IRC 暴力破解、Webmin 暴力破解、其他端口被暴力破解、系统被成功爆破事件。
Web 攻击	“实时检测”Web 恶意扫描器、IP、网马等威胁。 共支持检测 38 种子类型的 Web 攻击威胁。 • 支持检测的 Web 攻击威胁 包括 Webshell 攻击（3 种）、跨站脚本攻击、代码注入攻击（7 种）、SQL 注入攻击（9 种）、命令注入攻击。 • 接入的 HSS 服务上报的告警事件 包括 Webshell 攻击、Linux 网页篡改、Windows 网页篡改。 • 接入的 WAF 服务上报的告警事件 包括跨站脚本攻击、命令注入攻击、SQL 注入攻击、目录遍历攻击、本地文件包含、远程文件包含、远程代码执行、网站后门、网站信息泄露、漏洞攻击、IP 信誉库、恶意爬虫、网页防篡改、网页防爬虫。
后门木马	“实时检测”资产系统是否存在后门木马风险，以及被后门木马程序入侵后的恶意请求行为。 共支持检测 5 种子类型的后门木马威胁。 • 检测主机资产上 Web 目录中的 PHP、JSP 等后门木马文件类型。 • 检测资产被植入木马特性

告警名称	威胁告警说明
	检测内容包括资产系统存在 win32/ramnit checkin 木马、被入侵后执行 wannacry 勒索病毒相关的 DNS 解析请求、被入侵后尝试下载木马程序，被入侵后访问 HFS 下载服务器等。
僵尸主机	“实时检测”资产被入侵后对外发起攻击的威胁。 共支持检测 7 种子类型的僵尸主机威胁。 • 对外发起 SSH 暴力破解 • 对外发起 RDP 暴力破解 • 对外发起 Web 暴力破解 • 对外发起 MySQL 暴力破解 • 对外发起 SQLServer 暴力破解 • 对外发起 DDoS 攻击 • 被入侵后安装挖矿程序
异常行为	“实时检测”资产系统异常变更和操作行为。 共支持检测 21 种子类型的异常行为威胁。 • 支持检测的异常行为威胁 包括文件系统被扫描、CMS V1.0 漏洞、敏感文件被访问。 • 接入的 HSS 服务上报的告警事件 包括系统成功登录审计事件、文件目录变更监测事件、混杂模式网卡、异常权限用户、反弹 Shell、异常 Shell、高危命令执行、异常自启动、文件提权、进程提权、Rootkit 程序。 • 接入的 WAF 服务上报的告警事件 包括自定义规则、白名单、黑名单、地理访问控制、扫描器爬虫、IP 黑白名单、非法访问。
漏洞攻击	“实时检测”资产被尝试使用漏洞进行攻击。 共支持检测 2 种子类型的漏洞攻击威胁。 • WebCMS 漏洞攻击
命令控制	“实时检测”资产可能被命令与控制服务器（C&C，Command and Control Server）远程控制，访问与恶意软件或建立与恶意软件之间的链接。 共支持检测 3 种子类型的命令控制威胁。 • 监控主机存在访问 DGA 域名行为 • 监控主机存在访问恶意 C&C 域名行为 • 监控主机存在恶意 C&C 通道行为

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。

表1-5 基线检查功能说明

功能模块	功能详情
云服务基线	通过一键扫描或设置定级扫描，分类呈现云服务配置检测结果，提示不合格检测项，并提供相应配置加固建议和帮助指导。

检测结果

通过集成安全防护产品，接入安全产品检测数据，管理全部检测结果。

表1-6 全部结果功能说明

功能模块	功能详情
检测结果	通过呈现多种结果类型，支持标记、导出检测结果，并支持自定义结果列表。 • 结果类型 威胁告警、漏洞、风险、合规检查、违法违规、舆情、安全公告。

日志管理

通过授权对象存储（原生版）II 型服务（Object Storage Service，OBS）存储态势感知日志，帮助用户轻松应对安全日志存储、导出场景，满足日志存储 180 天及集中审计的要求。

表1-7 日志管理功能说明

功能模块	功能详情
日志管理	通过 OBS 存储日志，满足 SA 日志审计和容灾需求。

产品集成

通过集成安全防护产品，接入安全产品检测数据，管理检测结果的数据来源。

表1-8 产品集成功能说明

功能模块	功能详情

功能模块	功能详情
安全产品集成	通过集成安全防护产品，接入安全产品检测数据，管理检测结果的数据来源，支持查看传输数据量，管理数据上报健康状态。

1.3 应用场景

资产风险管理

云上业务众多，云上资产日益庞大，以及云资产的变化频繁，大大增加了云上安全风险。

态势感知集中呈现云上所有资产安全状况，实时监控云上业务整体安全，让服务器中的漏洞、威胁和攻击情况一目了然，保障所有资产的安全，帮助企业轻松应对资产安全风险。

威胁事件告警

面对云上各类安全威胁，以及不断涌出的新型威胁类型，态势感知通过汇集全网流量数据和安全防护设备日志信息，能够实时检测和监控云上安全风险，实时呈现告警事件的统计信息，并可对各种威胁事件进行汇聚统计。

此外，针对常见的暴力破解、Web 攻击、僵尸主机威胁事件，可预制的安全防护策略有效防御威胁风险，提升运维效率。

风险配置管理

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

1.4 服务版本差异

目前态势感知提供基础版和专业版两个版本，不同版本有不同功能使用范围，详细功能介绍请参见功能特性。

版本功能差异

说明

不同版本支持功能差别，标识符号说明如下：

- ×：代表不支持该功能。
- √：代表支持该功能。

表1-9 不同版本功能差异

服务功能	功能模块	功能概述	基础版	专业版
安全概览	安全评分	集中呈现资产安全风险评分和风险等级分布，同时展示当前风险防御能力。	√	√
	安全监控	实时呈现展示待处理威胁告警、待修复漏洞、基线异常问题的安全监控统计数据。	√	√
	安全趋势	展示近 7 天内您的整体资产安全健康得分的趋势。	√	√
资源管理	资源安全状况	同步资源信息，集中呈现资源整体安全状况。	×	√
威胁告警	告警列表	集中呈现威胁告警事件统计信息，导出告警事件。	√	√
		通过将告警忽略、标记为线下处理，标识告警事件。	×	√
	威胁分析	根据“攻击源”的 IP 查询被攻击的资产信息，亦可根据“被攻击的资产”的 IP 查询威胁攻击来源信息。	×	√
基线检查	云服务基线	通过一键扫描云服务基线，分类呈现云服务配置项检测结果信息。	×	√
		通过一键扫描云服务基线，分类呈现云服务配置项检测结果信息。支持查看检测结果详情，并提供相应修复建议。	×	√
检测结果	全部结果	集中呈现安全产品的检测结果，可导出结果、标识结果等。	√	√
日志管理	日志管理	通过授权 OBS 存储 SA 日志，满足日志审计和容灾需求。	×	√
产品集成	安全产品集成	通过集成安全产品，接入安全产品检测结果，管理检测结果的数据来源。	√	√

1.5 计费说明

计费项

态势感知**基础版**免费体验，**专业版**按选购的资产配额数计费。

表1-10 计费项说明

版本	计费项	计费说明
基础版	无	免费体验，不计费。
专业版	资产配额	按购买的资产配额数计费，包括主机资产配额数和网站资产配额数。
	按包周期购买计费	提供包月和包年的购买模式。
	按需购买计费	即开即停，按小时结算。

计费模式

态势感知的计费模式为包周期和按需计费。

- 包周期（包年/包月）
- 按需计费：按小时结算，根据实际使用时长（小时）计费。先使用后付费，使用方式灵活，可以即开即停。

变更配置

- 变更资产配额

  当您的资产数量增加，可在当前计费模式内增加资产配额数，不支持减少配额数。
- 退订

  若购买态势感知后，需停止使用，请执行退订操作。

须知

- **基础版不支持退订。**
- **不支持部分配额购买专业版。**

续费

- 包周期购买的版本到期后，您可以单击右上角“续费”，跳转至续费管理页面完成续费，延长使用期。

  为避免版本到期未及时续费，导致安全风险，建议开通自动续费。开通自动续费后，系统将根据配置自动续费，无需手动操作。
- 按需计费是按小时计费，请确保账户余额充足，及时为账户充值。在账户余额充足的前提下，将持续为您提供防护服务，不影响使用。

到期与欠费

- 到期

  若包周期版本到期后，未及时续费，会根据“客户等级”和“订购方式”定义不同的保留期时长，保留期内专业版服务可继续使用。若保留期到期后，仍未及时续费，专业版会变为基础版。

- 欠费

  当您的账户欠费后，可查看欠费详情，此时账户将进入欠费状态，需要在约定时间内支付欠款。为避免相关服务不被停止，请及时为账户充值。

1.6 基本概念

本节介绍态势感知相关概念。

安全风险

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

威胁告警

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

云服务基线

云服务基线是应用在云场景下，帮助用户检测云产品上存在的风险配置项，并提供修复建议。

攻击类型

- 暴力破解

  暴力破解法是一种密码分析方法，基本原理是在一定条件范围内对所有可能结果进行逐一验证，直到找出符合条件的结果为止。攻击者通常使用暴力破解的方式猜测远程登录的用户名和密码，一旦破解成功，即可实施攻击和控制。

- Web 攻击

  Web 攻击是针对用户上网行为或网站服务器等设备进行攻击的行为。常见的 Web 攻击方式包括 SQL 注入攻击、跨站脚本攻击、跨站请求伪造攻击等。

- 僵尸主机

  僵尸主机亦称傀儡机，是由攻击者通过木马蠕虫感染的主机，大量僵尸主机可以组成僵尸网络（Botnet）。攻击者通过控制信道向僵尸网络内的大量僵尸主机下达指令，令其发送伪造包或垃圾数据包，使攻击目标瘫痪并“拒绝服务”，这就是常见的 DDoS 攻击。此外，随着虚拟货币（如比特币）价值的持续增长，以及挖矿成本的逐渐增高，攻击者也开始利用僵尸主机进行挖矿和牟利。

- 异常行为

  异常行为主要指在主机中发生了一些不应当出现的事件。例如，某用户在非正常时间成功登录了系统，一些文件目录发生了计划外的变更，进程出现了非正常的行为等。这些异常的行为事件很多是有恶意程序在背后作乱。所以在发生这类异常行为时，应当引起重视。态势感知中的异常行为数据主要来源于主机安全服务。

- 漏洞攻击

  漏洞是指计算机系统安全方面的缺陷，可导致系统或应用数据遭受保密性、完整性、可用性等方面的威胁。攻击者利用漏洞获取计算机权限、盗取敏感数据、破坏软硬件系统等行为均可称为漏洞攻击。

1.7 用户权限

系统默认提供两种权限策略：系统策略和自定义策略。系统策略是 IAM 预置的策略，用户只能使用不能修改。若系统策略不满足授权要求，用户可以创建自定义策略，自由搭配需要授予的权限集。

用户组配置权限策略后，将用户加入用户组中，可以使该用户获得权限策略中定义的操作权限。

1.8 与其他云服务的关系

本小节主要介绍态势感知与其他云服务之间的关系。

与安全服务的关系

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

与 ECS 的关系

态势感知为弹性云主机（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 OBS 的关系

通过对象存储（原生版）II 型服务（Object Storage Service，OBS），您可以将 SA 日志存储至 OBS 桶中，确保日志不丢失，实现数据持久化。

2 升级版本

态势感知提供基础版、专业版供您选择。

- **基础版**仅提供检测部分威胁风险，呈现一定云上资产安全态势。
- 为及时和深入了解资产安全状况，确保云上资产安全，建议您升级为**专业版**。
  - **专业版**提供更多种类的威胁检测和分析服务，包含威胁分析、告警设置、基线检查等功能。
  - 更多基础版、专业版功能差异，请参见服务版本差异。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击管理控制台左上角的，选择区域或项目。

步骤 3 在页面左上角单击，选择“安全 > 态势感知”，默认进入态势感知安全概览管理页面。

步骤 4 单击右上角“升级”，进入购买专业版页面。

步骤 5 选择使用角色。

默认可选 IT 运维人员、安全运维人员、合规审计人员、CSO/CIO/CISO 四类角色，不同角色推荐配置不同。

步骤 6 选择“计费模式”，可以选择包周期或按需。

步骤 7 选择“态势感知版本”，此处默认选择专业版。

步骤 8 配置“主机配额”。

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。

主机配额最大限制如下：

- 当前账户下主机总数量≤10 台：主机配额最大限制为 100 台。
- 当前账户下主机总数量>10 台：主机配额最大限制=当前账户下主机总数量 x10 台
  示例：当前账户下主机总数量为 20 台，则主机配额最大限制为 20x10=200 台。

说明

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。

步骤 9 当“计费模式”选择“包周期”时，需要选择“购买时长”。

步骤 10 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤 11 确认订单详情无误后，单击“去支付”，完成购买操作。

步骤 12 进入“付款”页面，选择付款方式进行付款。

----结束

后续管理

若不再使用态势感知专业版功能，可单击“取消”，可继续使用基础版功能。

3 版本管理

3.1 选择计费模式

3.1.1 包周期计费

包年/包月的计费模式也称为包周期计费模式，是一种预付费方式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。

适用于包周期的资源

SA 资产配额，主要为主机配额。

若您需购买包年/包月的态势感知服务，可同时购买资产配额，配置费用包括两种资源的费用之和。

3.1.2 按需计费

按需计费是按小时付费，是一种后付费方式，可以随时开通/取消。系统会根据资源的实际使用情况（按 SA 服务的实际使用时长计费）每小时出账单，并从账户余额里扣款。

适用于按需的资源

SA 资产配额，主要为主机配额。

3.2 购买专业版

背景信息

态势感知提供基础版、专业版供您选择。

- 用户注册天翼云帐号后，可免费体验**基础版**。
  基础版仅提供检测部分威胁风险，呈现一定云上资产安全态势。
- 为及时和深入了解资产安全状况，确保云上资产安全，建议您升级为**专业版**。

- **专业版**提供更多种类的威胁检测和分析服务，您需根据全局资产数购买配额，一个资产配额支持全方位防护一台资产。

须知

- 基础版不支持退订。
- 不支持部分配额购买专业版。

前提条件

- 已获取管理控制台的登录帐号与密码。

包周期方式

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 > 态势感知”，进入态势感知管理控制台。

步骤 3 在页面右上角单击“升级”。

步骤 4 （可选）选择使用角色。

默认可选 IT 运维人员、安全运维人员、合规审计人员、CSO/CIO/CISO 四类角色，不同角色推荐配置不同。

步骤 5 选择计费模式，“计费模式”选择“包周期”，按配置周期计费。

步骤 6 选择态势感知版本。

当前默认选择“专业版”，由基础版功能升级为专业版功能。

步骤 7 配置资产配额，相关参数如表 1 配置参数说明。

表3-1 配置参数说明

参数	说明
主机配额	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。 主机配额最大限制如下： • 当前账户下主机总数量≤10 台：主机配额最大限制为 100 台。 • 当前账户下主机总数量>10 台：主机配额最大限制=当前账户下主机总数量 x10 台 示例：当前账户下主机总数量为 20 台，则主机配额最大限制为 20x10=200 台。 说明 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

参数	说明
	全风险。当主机资产数量增加后，请及时增加配额数。

步骤 8 选择态势感知使用时长。

- 配置资产配额的使用时长。

  计费模式选择“包周期”后，必须配置“购买时长”。

  - 可按月（选择 1/2/3/4/5/6/7/8/9 个月）或按年（选择 1/2/3 年）购买。
- 勾选“自动续费”。在账户余额充足前提下，当购买的版本即将到期时，自动续费，不影响使用。

步骤 9 配置完成后，单击“立即购买”。

步骤 10 进入“订单详情”页面，确认订单无误后，单击“去支付”。

步骤 11 在支付页面，选择付款方式完成付款。

步骤 12 成功付款后，返回态势感知控制台页面，确认已生效和到期时间。

----结束

按需方式

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 > 态势感知”，进入态势感知管理控制台。

步骤 3 在页面右上角单击“升级”。

步骤 4 （可选）选择使用角色。

默认可选 IT 运维人员、安全运维人员、合规审计人员、CSO/CIO/CISO 四类角色，不同角色推荐配置不同。

步骤 5 选择计费模式，“计费模式”选择“按需”，按小时计费。

从开通开始到取消结束，按实际防护时长（小时）计费。

步骤 6 选择态势感知版本。

当前默认选择“专业版”，由基础版功能升级为专业版功能。

步骤 7 配置资产配额，相关参数如表 1 配置参数说明。

表3-2 配置参数说明

参数	说明
主机配额	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。

参数	说明
	主机配额最大限制如下： • 当前账户下主机总数量≤10 台：主机配额最大限制为 100 台。 • 当前账户下主机总数量>10 台：主机配额最大限制=当前账户下主机总数量 x10 台 示例：当前账户下主机总数量为 20 台，则主机配额最大限制为 20x10=200 台。 说明 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。

步骤 8 配置完成后，单击“立即购买”。

步骤 9 进入“订单详情”页面，确认订单无误，单击“确认开通”。

步骤 10 返回态势感知控制台页面，确认按需版本已生效。

----结束

后续管理

- 若需变更资产配额，可单击“增加配额”，添加资产配额购买，详细说明请参见增加资产配额。
- 若购买的包周期版本即将到期或已经到期，可单击“续费”，延长当前包周期资源的使用期限，详细说明请参见续费。
- 若不再使用资产配额功能，可单击“退订”或“取消”，退订相应态势感知服务，详细说明请参见退订。

3.3 增加资产配额

购买态势感知资产配额完成后，当用户资产数量增加，或需对不同资产有不同使用时长需求，可参考本小节扩充“主机配额”，并配置使用时长。

约束限制

- 主机配额是授权检测主机的数量。主机配额最大限制如下：

表3-3 主机配额最大限制

当前账户下主机总数量/台	主机最大配额/台
当前账户下主机总数量≤10	100
当前账户下主机总数量>10	当前账户下主机总数量 x10 示例：已有 20 台主机，则主机最大配额为

当前账户下主机总数量/台	主机最大配额/台
	20x10=200。

- 在购买态势感知时，选择的最大配额需等于或大于当前账户下主机总数量，且不支持减少。若购买的最大配额小于主机数量，可能会造成如下影响：

  未授权检测的主机被攻击后，不能及时感知威胁，造成数据泄露等风险。

按需方式

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 > 态势感知”，进入态势感知管理控制台。

步骤 3 单击“增加配额”，跳转到态势感知购买页面。

步骤 4 查看当前配置。

步骤 5 选择计费模式，“计费模式”选择“按需”，按小时计费。

从开通开始到取消结束，按实际防护时长（小时）计费。

步骤 6 配置“主机配额”，在原有配额数基础上，增加的资产配额数。

步骤 7 配置完成后，单击“立即购买”。

步骤 8 进入“订单确认”页面，确认订单无误后，单击“去支付”。

步骤 9 返回态势感知控制台页面，即可对相应配额数的主机进行安全防护。

----结束

3.4 续费

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

续费操作仅针对包周期版本规格。

- 包周期（包年/包月）模式为预付费方式。当购买的包周期版本到期时，用户需通过“续费”延长使用期。
- 按需计费为按小时计费，即开即用。在账户余额充足前提下，不涉及过期情况，即无需续费操作。

手动续费

步骤 1 登录管理控制台。

步骤 2 在页面左上角单击 ☰，选择“安全 > 态势感知”，进入态势感知管理控制台。

步骤 3 单击右上角“专业版”，显示版本管理窗口。

步骤 4 单击“续费”，系统跳转至费用中心“续费管理”页面。

步骤 5 在态势感知专业版实例所在行，单击“续费”，跳转至“续费”页面。

步骤 6 配置“选择续费时长”，如选择“一年”。

步骤 7 单击“去支付”，跳转至支付页面，完成付款。

步骤 8 返回续费管理页面，可查看态势感知已续费成功。

----结束

开通自动续费

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

步骤 1 登录管理控制台。

步骤 2 单击“费用 > 续费管理”，跳转至费用中心“续费管理”页面。

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

步骤 4 选择配置“自动续费周期”和勾选“预设自动续费次数”。

步骤 5 单击“开通”，完成自动续费配置。

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

后续将根据配置，自动续费延长使用期。

----结束

3.5 退订

若用户不再使用态势感知防护功能，可执行退订或一键取消操作。

- 包周期（包年/包月）计费模式：预付费方式。新购 5 天内的资源，支持每年 10 次 5 天无理由“退订”；使用超过 5 天的资源，“退订”需要收取手续费。
- 按需计费模式：按小时计费方式。资源即开即停，支持一键“取消”释放资源。

退订包周期计费

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 > 态势感知”，进入态势感知管理控制台。

步骤 3 单击右上角“专业版”，显示版本管理窗口。

步骤 4 针对包周期购买的资产配额，单击“退订”，进入“退订管理”列表页面。

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

步骤 6 确认待退订资源信息，选择退订原因，并勾选退订确认。

步骤 7 单击“退订”，在退订管理页面确认退订。

退订成功后，返回版本管理窗口，包年/包月计费的资产配额已取消。

----结束

取消按需计费

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 > 态势感知”，进入态势感知管理控制台。

步骤 3 单击右上角“专业版”，显示版本管理窗口。

步骤 4 针对按需购买的版本，单击“取消”，一键释放按需计费的资产配额。

返回版本管理窗口，按需计费的资产配额资源已取消。

----结束

4 安全概览

4.1 总览

SA 的“安全概览”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。在“安全概览”查看安全概览信息和相关一键操作，实现云上安全态势一览和风险统一管控。

您可以在“安全概览”页面查看您的资产安全总览情况，并进行相关操作。“安全概览”分为以下几个板块：

- 安全评分
- 安全监控
- 安全趋势

安全评分

“安全评分”板块根据不同版本的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况，如图 4-1。

图4-1 安全评分

- 分值范围为 0～100，分值越大表示风险越小，资产更安全，安全分值详细说明请参见安全评分。
- 分值环形图不同颜色表示不同威胁等级。例如，黄色对应“中危”。
- 单击“立即处理”，系统右侧弹出“安全风险处理”页面，您可根据该页面的提示，参考对应的帮助文档或直接对风险进行处理。

- 安全风险处理页面中包含所有需要您尽快处理的安全风险和威胁，分为“威胁告警”、“漏洞”、“合规检查”三大类别。
- “安全风险处理”页面中显示的数据为最近/最新检测后的数据结果，“检测结果”页面（单击“前往处理”，进入该页面）显示的是所有检测时间的各类数据详情，因此，安全风险处理页面的数据总数≤检测结果页面的数据总数。
- **处理安全风险：**
  i. 在“安全评分”栏中，单击“立即处理”，系统右侧弹出“安全风险处理”页面。
  ii. 在“安全风险处理”页面中，单击“前往处理”，进入检测结果页面。
  iii. 选择一个或多个“未处理”状态的结果，单击“忽略”或“标记为线下处理”，对不同检测结果批量执行相应的处理操作。
    - 忽略：如果确认该检测结果不会造成危害，在“忽略风险项”窗口记录“处理人”、“忽略理由”，可标记为“已忽略”状态。
    - 标记为线下处理：如果该检测结果已在线下处理，在“标记为线下处理”窗口记录“处理人”、“处理时间”和“处理结果”，可标记为“已线下处理”状态。

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

说明

- 由于检测需要一定的时间，请您在单击“重新检测”按钮 **5 分钟**后，再刷新页面，查看最新检测的安全评分。
- 资产安全风险修复后，为降低安全评分的风险等级，需手动忽略或处理告警事件，刷新告警列表中告警事件状态。

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

安全监控

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

图4-2 安全监控

表4-1 安全监控参数说明

参数名称	参数说明
威胁告警	呈现最**近 7 天内**未处理威胁告警，可快速了解资产遭受的威胁告

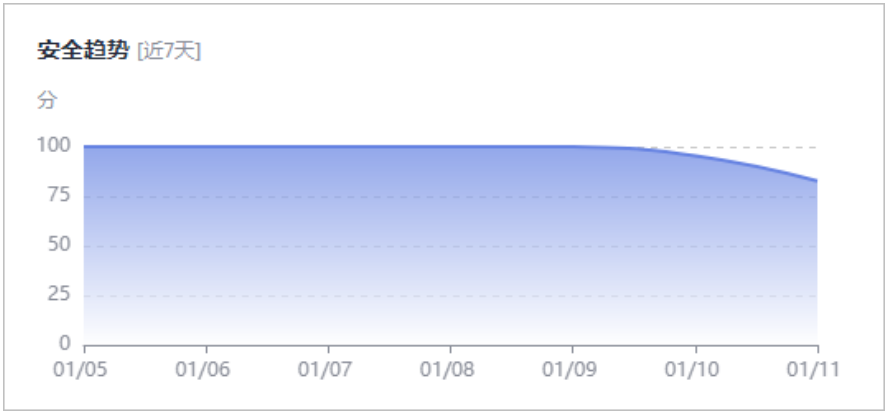
参数名称	参数说明
	警类型和数量，呈现威胁告警的统计结果。 • 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了入侵事件，建议您立即查看告警事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看告警事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该告警事件的详情。 • 单击威胁告警模块，系统将列表实时呈现**近 7 天内** TOP5 的威胁告警事件，可快速查看威胁告警详情，监控威胁告警状况。 – 列表呈现近 7 天 TOP5 的威胁告警事件的信息，包括威胁告警名称、告警等级、资产名称、告警发现时间。 – 若列表显示内容为空，表示近 7 天无威胁告警事件。 – 单击“查看更多”，可跳转到“检测结果”页面，查看更多的威胁告警信息，并可自定义过滤条件查询告警信息。
漏洞	展示您资产中 TOP5 漏洞类型，以及**近 24 小时内**还未修复的漏洞总数和不同漏洞风险等级对应的数量。 • 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了漏洞事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该漏洞的详情。 • 单击漏洞模块中的“实时监控最新漏洞风险事件 Top5”栏，系统将列表实时呈现**近 24 小时内** TOP5 的漏洞事件，可快速查看漏洞详情。 – 列表呈现当日最新 TOP5 漏洞事件详情，包括漏洞名称、漏洞等级、资产名称、漏洞发现时间。 – 若列表显示内容为空，表示当日无漏洞事件。 – 单击“查看更多”，可跳转到“检查结果”页面，查看更多的漏洞信息，并可自定义过滤条件查询漏洞信息。
合规检查	展示您资产中**近 30 天内**存在的合规风险总数量和不同危险等级的合规检查风险对应的数量。 • 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了不合规的配置，建议您立即查看合规异常事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常配置，

参数名称	参数说明
	建议您立即查看合规异常事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常配置，建议您及时查看该合规检查项目的详情。 • 单击合规检查异常模块，系统将列表实时呈现**近 30 天内** TOP5 的合规检查异常事件，可快速查看合规检查详情。 – 列表呈现最近一次合规检查中 TOP 的合规异常事件详情，包括合规检查项目名称、等级、资产名称、发现时间。 – 若列表显示内容为空，表示近 30 天无合规异常事件。 – 单击“查看更多”，可跳转到“检查结果”页面，查看更多的合规异常信息，并可自定义过滤条件查询合规检查信息。

安全趋势

“安全趋势”板块展示近 7 天内您的整体资产安全健康得分的趋势图。

图4-3 安全趋势



4.2 安全评分

态势感知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。

本章节将介绍在安全评分中，不同分值的含义以及扣分项的详细情况。

安全分值

SA 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。

- 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，安全评分实时更新。

说明

- 由于检测需要一定的时间，请您在单击“重新检测”按钮 **5 分钟**后，再刷新页面，查看最新检测的安全评分。
- 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4-2 安全分值表

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

安全评分扣分项

安全评分扣分项及其分值情况如表 4-3 所示。

表4-3 安全评分扣分项

分类	扣分项	单项扣分项	处理建议	最高扣分上限
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	2		

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

5 资源管理

态势感知提供资源管理功能。在“资源管理”页面，您可以查看当前帐号中所有资源的安全状态统计信息，包括资源的名称、所属服务、安全状况等，帮助您快速定位安全风险问题并提供解决方案。

操作步骤

步骤 1 登录管理控制台。

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

步骤 3 在左侧导航栏选择“资源管理”，进入资源管理页面。

步骤 4 查看全部资源安全状态，相关说明如表 5-1 所示。

表5-1 资源安全状态参数说明

参数名称	参数说明
名称	呈现资源的名称。
服务	呈现资源所属的服务。
资源类型	呈现资源所属的类型。例如：云服务器、磁盘、实例等。
安全状况	呈现资源的安全风险等级。 • 风险等级包括“致命”、“高危”、“中危”、“低危”、“提示”和“无风险”。 • 呈现当前资源风险的最高等级。例如，ECS 中有高危、低危和提示级别的风险，则此处取最高值，显示为高危。 • 单击，可按风险等级排序资源列表。
IP 地址	呈现资源的 IP 地址。
防护状态	呈现资源是否开启安全防护。如果未开启防护，可单击“去开启”进行设置。

参数名称	参数说明
威胁	呈现资源**近 7 天内**存在的威胁告警总数。 单击告警数量可跳转“检测结果”页面，查看更多的威胁告警信息，并可自定义过滤条件查询告警信息。
漏洞	呈现资源**近 24 小时内**未修复的漏洞总数。 • 单击漏洞数量可跳转“检测结果”页面，查看更多的漏洞信息，并可自定义过滤条件查询漏洞信息。 • “资源管理”页面中显示的数据为最近/最新检测后的数据结果，“检测结果”页面显示的是所有检测时间的各类数据详情，因此，资源管理页面的数据总数≤检测结果页面的数据总数。
基线	呈现资源**近 30 天内**存在的基线风险总数。 • 单击基线检查异常数量可跳转“检测结果”页面，查看更多的基线异常信息，并可自定义过滤条件查询基线检查信息。 • “资源管理”页面中显示的数据为最近/最新检测后的数据结果，“检测结果”页面显示的是所有检测时间的各类数据详情，因此，资源管理页面的数据总数≤检测结果页面的数据总数。
企业项目	呈现资源所属的企业项目。
标签	呈现资源已有的标签。 如果资源当天添加了标签，则在 SA 资源管理中第二天才会同步显示。

步骤 5 根据资源信息，筛选查看相关资源安全状态。

单击“服务”、“区域”或“安全状况”后的选项，将呈现符合过滤条件的资源列表。

- **服务**：筛选资源所属的服务。选择服务后，还可以根据“资源类型”来查看选择指定资源类型的安全状态。
- **区域**：筛选资源所在的区域。
- **安全状况**：筛选资源的安全风险等级。

  可选择风险等级包括“致命”、“高危”、“中危”、“低危”、“提示”或“无风险”。

步骤 6 当资源列表较多时，可以通过搜索功能，快速查询指定资源。

在搜索框中输入资源的“弹性公网 IP”、“名称”或“私有 IP”，单击  ，即可查看目标资源的安全状态。

----结束

6 威胁告警

6.1 威胁告警简介

背景信息

态势感知威胁告警功能汇集了多个安全服务的告警能力，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。

同时，通过威胁分析，从攻击源和受攻击资产两个维度，帮助您及时发现资产中的安全威胁、实时掌握您资产的安全态势。

态势感知威胁告警支持以下功能项：

- 告警列表

  通过“实时监控”云上威胁告警事件，并接入 HSS、WAF 等服务上报的告警事件，提供告警通知和监控，记录近 180 天告警事件详情。
- 威胁分析

  从“攻击源”或“被攻击资产”查询威胁攻击，统计威胁攻击次数或资产被攻击次数。

告警类型

目前 SA 支持检测 8 类威胁告警事件，共包括 200+种子告警类型。

DDoS 事件

“实时检测”互联网主机的 DDoS 攻击。

共支持检测 100+种子类型的 DDoS 威胁。

- 网络层攻击

  NTP Flood 攻击、CC 攻击等。
- 传输层攻击

  SYN Flood 攻击、ACK Flood 攻击等。
- 会话层攻击

SSL 连接攻击等。

- 应用层攻击

  HTTP Get Flood 攻击、HTTP Post Flood 攻击等。

暴力破解事件

“实时检测”入侵资产的行为和主机资产内部的风险，检测 SSH、RDP、FTP、SQL Server、MySQL 等账户是否遭受的口令破解攻击，以及检测资产账户是否被破解异常登录。

共支持检测 22 种子类型的暴力破解威胁。

- 支持检测的暴力破解威胁

  包括 SSH 暴力破解（2 种）、RDP 暴力破解、MSSQL 暴力破解、MySQL 暴力破解、FTP 暴力破解、SMB 暴力破解（3 种）、HTTP 暴力破解（4 种）、Telnet 暴力破解。

- 接入的 HSS 服务上报的告警事件

  包括 SSH 暴力破解、RDP 暴力破解、FTP 暴力破解、MySQL 暴力破解、IRC 暴力破解、Webmin 暴力破解、其他端口被暴力破解、系统被成功爆破事件。

Web 攻击事件

“实时检测”Web 恶意扫描器、IP、网马等威胁。

共支持检测 38 种子类型的 Web 攻击威胁。

- 支持检测的 Web 攻击威胁

  包括 Webshell 攻击（3 种）、跨站脚本攻击、代码注入攻击（7 种）、SQL 注入攻击（9 种）、命令注入攻击。

- 接入的 HSS 服务上报的告警事件

  包括 Webshell 攻击、Linux 网页篡改、Windows 网页篡改。

- 接入的 WAF 服务上报的告警事件

  包括跨站脚本攻击、命令注入攻击、SQL 注入攻击、目录遍历攻击、本地文件包含、远程文件包含、远程代码执行、网站后门、网站信息泄露、漏洞攻击、IP 信誉库、恶意爬虫、网页防篡改、网页防爬虫。

后门木马事件

“实时检测”资产系统是否存在后门木马风险，以及被后门木马程序入侵后的恶意请求行为。

共支持检测 5 种子类型的后门木马威胁。

- 检测主机资产上 Web 目录中的 PHP、JSP 等后门木马文件类型。
- 检测资产被植入木马特性

  检测内容包括资产系统存在 win32/ramnit checkin 木马、被入侵后执行 wannacry 勒索病毒相关的 DNS 解析请求、被入侵后尝试下载木马程序，被入侵后访问 HFS 下载服务器等。

僵尸主机事件

“实时检测”资产被入侵后对外发起攻击的威胁。共支持检测 7 种子类型的僵尸主机威胁。

- 对外发起 SSH 暴力破解
- 对外发起 RDP 暴力破解
- 对外发起 Web 暴力破解
- 对外发起 MySQL 暴力破解
- 对外发起 SQLServer 暴力破解
- 对外发起 DDoS 攻击
- 被入侵后安装挖矿程序

异常行为事件

“实时检测”资产系统异常变更和操作行为。共支持检测 21 种子类型的异常行为威胁。

共支持检测 21 种子类型的异常行为威胁。

- 支持检测的异常行为威胁

  包括文件系统被扫描、CMS V1.0 漏洞、敏感文件被访问。
- 接入的 HSS 服务上报的告警事件

  包括系统成功登录审计事件、文件目录变更监测事件、混杂模式网卡、异常权限用户、反弹 Shell、异常 Shell、高危命令执行、异常自启动、文件提权、进程提权、Rootkit 程序。
- 接入的 WAF 服务上报的告警事件

  包括自定义规则、白名单、黑名单、地理访问控制、扫描器爬虫、IP 黑白名单、非法访问。

漏洞攻击事件

“实时检测”资产被尝试使用漏洞进行攻击。共支持检测 2 种子类型的漏洞攻击威胁。

- WebCMS 漏洞攻击

命令控制事件

“实时检测”资产可能被命令与控制服务器（C&C，Command and Control Server）远程控制，访问与恶意软件或建立与恶意软件之间的链接。

共支持检测 3 种子类型的命令控制威胁。

- 监控主机存在访问 DGA 域名行为
- 监控主机存在访问恶意 C&C 域名行为
- 监控主机存在恶意 C&C 通道行为

6.2 查看告警列表

通过查看“告警列表”，您可以了解近 180 天的告警威胁的统计信息列表，列表内容包括告警事件的名称、类型、等级和发生时间等。并可通过自定义过滤条件，如告警名称、告警等级和发生时间等，快速查询到相应告警事件的统计信息。

此外，您还可以通过及时处理告警事件，标记告警事件处理状态，并支持一键导出近 180 天的告警事件。

约束限制

- 仅专业版支持忽略和标记告警事件，基础版不支持。
- 仅支持导出近 180 天的全部告警事件，暂不支持筛选导出告警事件信息。
- 按过滤场景筛选告警，最多可呈现 10000 条告警。

查看告警详情

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“威胁告警”，默认进入态势感知告警列表管理页面。

步骤 4 筛选“告警名称”、“告警等级”、“发生时间”和“处理状态”条件选项，在列表栏查看显示符合过滤条件的告警事件列表。

- 告警名称：告警事件所属的分类。
- 告警等级：告警事件对应的等级，包括“致命”、“高危”、“中危”、“低危”、“提示”。
- 处理状态：用户对告警事件的处理标记，可选择“未处理”、“已忽略”、“已线下处理”。
- 发生时间：告警事件发生的时间范围，可选择“今天”、“昨天”、“近 3 天”、“近 7 天”、“近 30 天”和“近半年”。

步骤 5 当过滤后的告警事件较多时，可以利用搜索功能快速找到指定告警事件。

在下拉框中选择“资产 IP”、“来源 IP”、“主机 ID”，在搜索框中输入相应 IP 或 ID，单击 ，即可查看到指定资产相关的告警信息。

步骤 6 查看告警事件详情。

单击列表中告警的“告警名称”，右侧滑出告警详情窗口，可查看与该告警相关的“基本信息”、“数据来源”、“攻击信息”、受影响的用户等信息，以及该告警的处理状态。

----结束

标记告警事件

当 SA 检测出告警事件后，您可手动标记已处理的告警事件。

步骤 1 在“告警列表”页面，标记告警事件的处理状态。

- 忽略：如果确认该告警事件不会造成危害，可标记为“已忽略”状态。
- 标记为线下处理：如果该告警事件已在线下处理，在“标记为线下处理”窗口记录“处理人”、“处理时间”和“处理结果”，可标记为“已线下处理”状态。

步骤 2 批量标记告警事件。

选择一个或多个“未处理”状态的告警，单击“忽略”或“标记为线下处理”，对不同告警事件批量执行相应的处理操作。

步骤 3 单个标记告警事件。

在告警列表对应“操作”列，单击“忽略”或“标记为线下处理”，对单个告警事件执行相应处理操作。

步骤 4 取消告警事件标记。

告警处理状态标记后，可在告警事件对应“操作”列，单击“取消忽略”或“取消标记”，恢复告警“未处理”状态，再修改告警状态。

----结束

导出告警事件

在“告警列表”页面，单击“导出全部告警”，一键导出列表中全部告警事件，并以 excel 文件形式保存在本地。导出完成后，即可离线查看告警事件列表。

导出的 excel 文件中包含“事件标识”、“受影响资源”、“严重等级”和“发现时间”等信息。

说明

目前仅支持导出近 180 天的全部告警事件。

6.3 威胁分析

当告警列表中积累了较多威胁告警信息时，您可以使用“威胁分析”功能，从“攻击源”或“被攻击资产”的维度分析网络攻击情况。

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 > 态势感知 > 威胁告警 > 威胁分析”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“威胁告警”，进入威胁告警页面后，选择“威胁分析”页签，进入威胁分析管理页面。

步骤 4 在下拉框中选择条件“攻击源”或“被攻击资产”、“发生时间”，并输入待查询的 IP 地址，单击“开始分析”。

说明

发生时间可选择“今天”、“昨天”、“近 3 天”、“近 7 天”、“近 30 天”、“近半年”。

步骤 5 在列表栏查看符合过滤条件的威胁信息，可以直观看到该攻击源对哪些资产发起了何种类型的攻击，或被攻击资产遭到了哪些攻击。

----结束

7 基线检查

7.1 云服务基线简介

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

约束与限制

SA **基础版**暂不支持使用云服务基线检查功能。为及时了解云服务配置状态，以及确保云服务的配置的合理性，建议您使用专业版。

7.2 设置基线检查计划

态势感知支持根据基线检查计划检查您的服务器基线配置是否存在风险。

本文档介绍了如何新增、编辑、删除基线检查计划。

背景信息

开通基线检查服务后，态势感知将使用默认检查计划对所有资产进行检查。默认检查计划的自动检查时间、检查对象如下：

- 自动检查时间：每隔 3 天检查一次，每次在 00:00~06:00 进行检查。
- 检查对象：您帐号下当前区域的所有资产。

约束限制

创建检查计划是同一个检查规范只能属于一个检查计划。

创建检查计划

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 > 态势感知”，进入态势感知管理页面。

步骤 3 进入基线检查计划配置页面。

- 方法一：
  a. 在左侧导航栏选择“基线检查”，进入基线检查页面。
  b. 单击页面右上角的“设置检查计划”，进入检测设置页面。

图7-1 进入基线检查计划配置页面

- 方法二：
  在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。

步骤 4 在检测设置页面中，选择待创建计划所在的区域，并单击“创建计划”，系统右侧弹出新建检查计划页面。

步骤 5 配置检查计划。

1. 填写基本信息，具体参数配置如表 7-1 所示。

表7-1 检查计划基本信息

参数名称	参数说明
计划名称	自定义检查计划的名称。
检查时间	选择检测周期和检查触发时间。 • 检测周期：每隔 1 天、3 天、7 天、15 天、30 天检查一次 • 检查触发时间：00:00~06:00、06:00~12:00、12:00~18:00、18:00~24:00

2. 选择检查规范。
   选择需要检测的基线检查项目。更多关于基线检查项目详细描述请参见云服务基线简介。
3. 单击“确定”。
   检查计划创建完成。
   SA 会在指定的时间执行云服务基线扫描，扫描结果可以在“基线检查”中查看。

----结束

相关操作

基线检查计划创建后，您可以查看检查计划、对检查计划进行编辑或删除。

- 查看已有检查计划
  a. 登录管理控制台。
  b. 在页面左上角单击 ☰，选择“安全 > 态势感知”，进入态势感知管理页面。
  c. 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。
  d. 在检测设置页面中，查看已有的基线检查计划。
- 编辑检查计划
  a. 在目标计划所在框的右上角单击“编辑”，系统右侧弹出编辑检查计划页面。
  b. 编辑需要修改的计划参数。
  c. 单击“确定”。
- 删除检查计划
  a. 在目标计划所在框的右上角单击“删除”。
  b. 在弹出的对话框中，单击“是”。

7.3 执行基线检查计划

基线检查项目分为“自动检查”和“手动检查”项目两种，本章节介绍自动检查项目执行检查的操作。

为了解最新的云服务基线配置状态，您需要执行扫描任务，扫描结束后才能获取云服务基线的风险配置。

基线检查功能支持定期自动检查和立即检查。

- 定期自动检查：根据 SA 为您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。默认检查计划每隔 3 天在 0 点的时候自动执行基线检查。
- 立即检查：如果您新增或修改了自定义的基线检查计划，您可以在基线检查页面选择该基线检查计划，立即执行基线检查，实时查看服务器中是否存在对应的基线风险。

约束限制

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

前提条件

已配置自定义的基线检查计划。

立即检查所有检查规范

SA 可根据您设置的检查规范，立即执行已配置的检查规范。

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“基线检查”，并在基线检查页面右上角单击“设置检查规范”，系统弹出选择检查规范窗口。

图7-2 基线检查页面

步骤 4 在弹出的选择规范窗口中，选择检查规范，并单击“确定”。

步骤 5 在页面右上角单击“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。

系统将立即执行已配置的检查规范。

----结束

立即执行某个检查计划

本部分将介绍如何立即执行某个检查计划，配置后，系统将立即执行已选择的基线检查计划。

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。

步骤 4 在检测设置页面，选择检查计划所在的区域。

步骤 5 在待执行立即手动检查的检查计划所在栏的上方单击“立即检查”。

图7-3 执行某个检查计划

系统将立即执行已选择的基线检查计划。

----结束

7.4 查看基线检查结果

本章节介绍如何查看基线检查详情、结果，您可以了解基线检查项影响的资产、基线项目详情等信息。

前提条件

- 已购买态势感知**专业版**，且在有效使用期内。
- 已扫描云服务基线。

查看检查结果总数据

查看某区域中所有检查项的检查结果。

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤 4 选择待查看检查结果所在的区域，系统将展示当前区域的所有检查结果相关数据。

步骤 5 查看当前区域检测到的基线检查结果汇总数据。

- 检查规范数：最近一次执行基线检查的检查规范数/检查规范总数。
- 检查项：最近一次执行基线检查中所有的检查项数目。
- 检查项合格率：最近一次执行基线检查的基线合格率。

  整体合格率=合格检查项数量/检查项总数。合格率的统计范围为全部规范的全部检查项目。

  检查项结果分为合格、不合格、检查失败和待检查几种。
- 风险资源分布：最近一次执行基线检查的风险资源分布情况以及风险资源的数量。

  风险等级分为：致命、高危、中危、低危、提示几个级别。

----结束

查看基线检查规范列表

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤 4 选择待查看检查结果的区域，并选择“检查规范”页签。

步骤 5 在基线检查规范中，选择“全部规范”，系统将显示当前区域所有检查规范及其详细信息。

基线检查规范页面会展示所有基线检查规范的列表，包括检查项、检查状态、检查分类、风险资源、描述，以及最近检查时间等信息。

说明

您也可在基线检查规范列表中，选择某个基线检查规范，查看该规范对应的基线检查项目列表。

----结束

查看某个基线检查项目详情

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤 4 选择待查看检查项目的区域，并选择“检查规范”页签。

步骤 5 在基线检查规范列表中，在待查看检查项目所在行的“操作”列，单击“查看详情”，系统进入检查项目详情页面。

步骤 6 在检查项目详情页面，查看检查项目的详细信息。

查看该风险检查项的详细描述、检查提示和检查结果等。

----结束

查看检查资源列表

资料列表只展示已检查的资源。

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤 4 选择待查看检查结果的区域。

步骤 5 选择“检查资源”页签，系统将显示当前区域所有检查资源以及其详细信息。

检查资源页面会展示所有检查资源的列表，包括资源名称、资源类型、检查项，以及风险项等信息。

----结束

查看某个资源的检查详情

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤 4 选择待查看检查项目的区域，并选择“检查资源”页签。

步骤 5 在检查资源列表中，在待查看资源所在行的“操作”列，单击“查看详情”，系统进入资源详情页面。

步骤 6 在资源详情页面，查看资源的详细信息。

查看该资源的检查项、检查状态、检查方式、最近检查时间等。

----结束

查看检查结果列表

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤 4 选择待查看检查结果的区域。

步骤 5 选择“检查结果”页签，系统将显示当前区域所有检查结果以及其详细信息。

检查结果页面会展示所有检查结果的列表，包括检查项、检查结果、资源类型、资源名称，以及最近检查时间等信息。

----结束

8 检测结果

8.1 查看全部检测结果

您可以在“全部结果”页面，获取安全状态的全视图，助您及时确定检测结果的优先级，统筹分析安全趋势。

“全部结果”支持以下特性：

- 支持呈现威胁告警、漏洞、风险、合规检查、违法违规、时讯舆情等领域信息。
- 支持实时接收安全产品检测数据，实时更新结果列表。
- 支持按时间范围、过滤场景等筛选结果。默认呈现近 7 天内检测结果。
- 支持查看检测结果详情，以及 JSON 格式的结果详情。
- 支持自定义结果列表呈现的属性。
- 支持标识检测结果的处理状态。

约束限制

- 按过滤场景筛选检测结果，最多可呈现 10000 条结果。
- 仅可呈现近 180 天的检测结果。

前提条件

- 已接收到安全产品的检测结果。

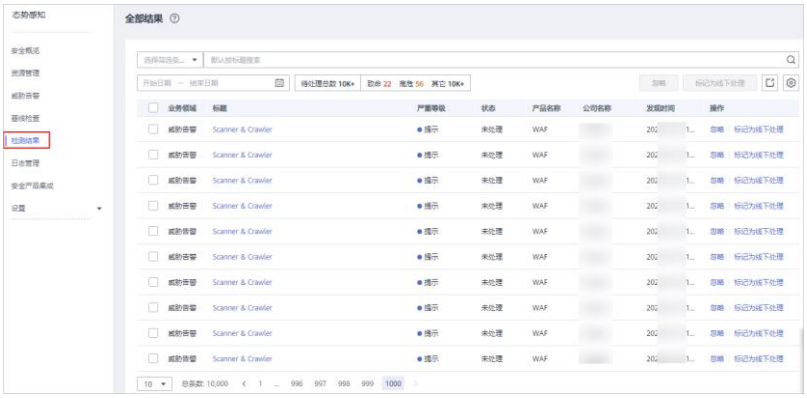
操作步骤

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“检查结果”，进入全部结果管理页面。

图8-1 查看全部检测结果



步骤 4 筛选查看检测结果。

- 在场景列框选择过滤场景，单击，即可查看到目标场景下检测结果。
- 当过滤后的结果仍较多时，可补充过滤条件和选择时间范围，快速查找结果。
  - 在筛选框补充过滤条件，添加一项或多项过滤条件，并配置相应条件属性，单击，快速查找指定条件属性的结果。
  - 在时间过滤框中，选择检测结果发现的时间范围，单击“确认”，快速查找指定时间范围内的结果。

步骤 5 查看检测结果列表。

筛选后的列表，可查看满足条件的检测结果列表，以及结果统计信息。

步骤 6 查看检测结果详情。

1. 单击列表中结果的“标题”，右侧滑出结果详情窗口。
2. 查看与该结果相关的“基本信息”、“描述”、“资源信息”、“攻击信息”、受影响的用户等信息，更多参数说明请参考。

表8-1 检测结果详情参数说明

参数	参数说明
基本信息	检测结果的基本信息，包括标题、严重等级、状态、发现时间、业务领域、公司名称、产品名称、类型等信息。
描述	检测结果的简要介绍。
资源信息	受影响的资源信息，包括资源名称、资源 ID、资源类型、资源区域等信息。
环境信息	受影响的用户信息，包括租户 ID、项目 ID、用户所在区域等信息。
攻击信息	攻击来源信息，包括攻击源 IP、攻击目标 IP、攻击源端口、攻击目标端口等信息。
相关检测结	相关联检测结果的信息，包括相关联资源名称、结果来源等信息。

参数	参数说明
果	
漏洞信息	漏洞结果信息，包括漏洞 ID、CVSS 分数、CVSS 版本、提供方等信息。
漏洞影响范围	漏洞影响范围信息，包括影响版本、安全版本等信息。
合规检查信息	合规检查基本信息，包括检查项、检查结果等信息。
涉及 CVE	漏洞结果 CVE 编号。
参考链接/链接	结果相关参考链接。
修复建议/处置建议	结果修复或处置建议说明。

3. 单击“查看 JSON”，查看 JSON 格式检测结果详情。

----结束

8.2 处理检测结果

当接收到检测结果后，您可标记结果处理状态。

- 忽略：如果确认该检测结果不会造成危害，在“忽略风险项”窗口记录“处理人”、“忽略理由”，可标记为“已忽略”状态。
- 标记为线下处理：如果该检测结果已在线下处理，在“标记为线下处理”窗口记录“处理人”、“处理时间”和“处理结果”，可标记为“已线下处理”状态。

说明

由于 SA 中的检测结果汇聚了企业主机安全（Host Security Service，HSS）、Web 应用防火墙（Web Application Firewall，WAF）等安全防护服务上报的告警数据，因此，处理检测结果时须注意以下顺序:

1. 需先在 SA 检测结果详情页面查看来源。
2. 前往来源服务进行优先处理。
3. 处理后再到 SA 中来标记结果处理状态。

例如，告警显示来源产品名称为 HSS，则需在 HSS 控制台上进行处理后，再在 SA 中进行标记处理。

前提条件

已接收到安全产品的检测结果。

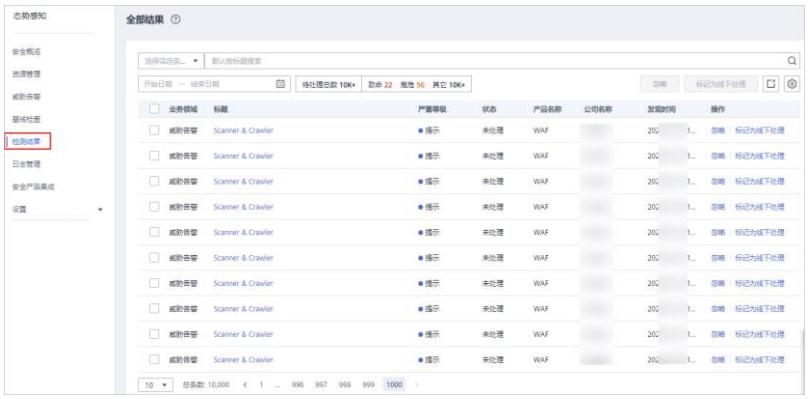
操作步骤

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“检测结果”，进入全部结果管理页面。

图8-2 查看全部检测结果



步骤 4 筛选检测结果。

步骤 5 批量标记检测结果。

选择一个或多个“未处理”状态的结果，单击“忽略”或“标记为线下处理”，对不同检测结果批量执行相应的处理操作。

步骤 6 单个标记检测结果。

- 在结果列表对应“操作”列，单击“忽略”或“标记为线下处理”，对单个检测结果执行相应处理操作。
- 在结果详情窗口，右下角单击“忽略”或“标记为线下处理”，对单个检测结果执行相应处理操作。

----结束

8.3 导出检测结果

态势感知支持一键导出检测结果。

导出的 excel 文件中包含“产品名称”、“公司名称”、“受影响资源”、“业务领域”、“标题”、“发生时间”、“发生次数”、“置信度”、“重要性”和“状态”等信息。

约束限制

- 按过滤场景筛选检测结果，最多可导出 10000 条结果。
- 仅可导出近 180 天的检测结果。

前提条件

- 已接收到安全产品的检测结果。

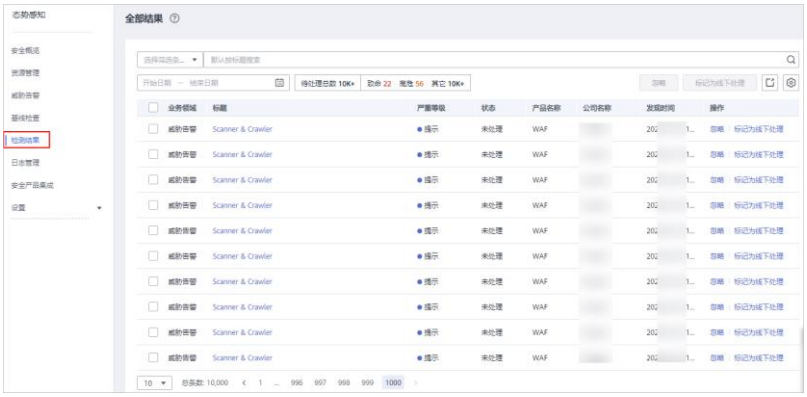
操作步骤

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“检测结果”，进入全部结果管理页面。

图8-3 查看全部检测结果



步骤 4 筛选检测结果。

步骤 5 单击 ，一键导出筛选的检测结果列表，并以.csv 格式文件保存在本地。

导出完成后，即可离线查看结果。

----结束

8.4 自定义结果列表

态势感知支持自定义检测结果列表。

前提条件

- 已接收到安全产品的检测结果。

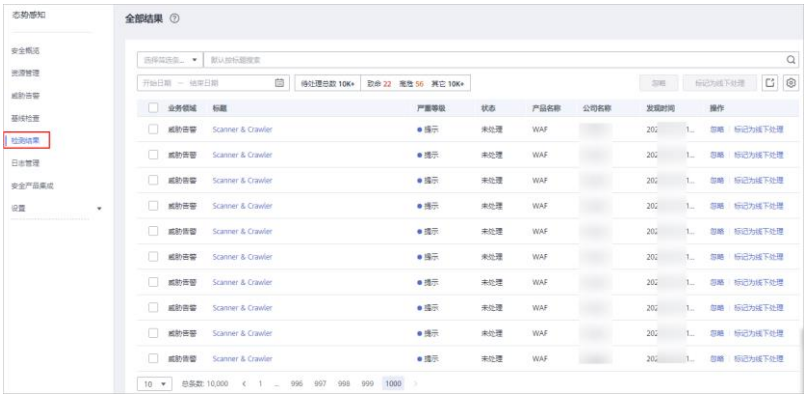
操作步骤

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“检测结果”，进入全部结果管理页面。

图8-4 查看全部检测结果



步骤 4 单击，展开结果列表属性框。

步骤 5 勾选结果属性。

步骤 6 刷新结果列表，即可在列表查看目标属性。

----结束

8.5 管理筛选条件

筛选条件用于筛选符合场景中过滤条件的结果，呈现匹配的结果列表。例如筛选条件添加产品名称和资源类型两个条件，属性分别为“企业主机安全”和“云服务器”，则匹配的结果必须同时符合这两个条件属性。

目前可添加的条件及属性如下：

- 标题：检测结果的标题内容，可输入关键字。默认按标题搜索。
- 严重等级：检测结果的风险等级，包括“致命”、“高危”、“中危”、“低危”、“提示”。
- 业务领域：检测结果所属业务领域，包括“威胁告警”、“漏洞”、“合规检查”、“违法违规”、“风险”、“舆情”、“安全公告”。
- 状态：用户对检测结果的处理状态，包括“未处理”、“已忽略”、“已线下处理”。
- 资源名称：检测结果来源资源的名称，需输入资源名称。
- 资源类型：检测结果来源资源的类型，包括“云服务器”、“虚拟私有云”、“安全组”、“弹性公网 IP”、“磁盘”、“其他”。
- 公司名称：检测结果来源产品所属公司，需输入公司名全称。
- 产品名称：检测结果来源安全产品，需输入产品名全称。

约束限制

- 一个筛选条件仅能包含一组“标题”关键字。
- 一个筛选条件仅能包含一个“资源名称”。

- 一个筛选条件仅能包含一个“公司名称”。
- 一个筛选条件仅能包含一个“产品名称”。

创建筛选条件

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“检测结果”，进入全部结果管理页面。

步骤 4 添加筛选条件。

- 在筛选框添加过滤条件，添加一项或多项过滤条件，并配置相应条件属性。
- 在时间筛选框中，选择时间范围。

步骤 5 单击筛选框后“保存”，弹出筛选条件保存窗口。

图8-5 保存筛选条件

步骤 6 配置筛选条件信息。

- 设置“场景名称”，自定义筛选条件名称。
- （可选）勾选“设为默认筛选条件”。

步骤 7 单击“确定”，返回全部结果列表页面，即可在场景列框查看新建的筛选条件。

----结束

修改筛选条件

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“检查结果”，进入全部结果管理页面。

步骤 4 在筛选条件列框，选择筛选条件。

步骤 5 在筛选框后单击“编辑”，弹出编辑窗口。

图8-6 编辑筛选条件

步骤 6 修改筛选条件名称。

步骤 7 单击“确认”，返回全部结果列表页面，即可查看已修改的筛选条件。

----结束

删除筛选条件

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 > 态势感知”，进入态势感知管理页面。

步骤 3 在左侧导航栏选择“检查结果”，进入全部结果管理页面。

步骤 4 在筛选条件列框，选择筛选条件。

步骤 5 在筛选框后单击“编辑”，弹出编辑窗口。

图8-7 删除筛选条件

步骤 6 单击“删除”，返回全部结果列表页面，即完成筛选条件的删除。

----结束

9 日志管理

通过授权对象存储（原生版）II 型服务（Object Storage Service，OBS）存储态势感知日志，帮助用户轻松应对安全日志存储、导出场景，以及满足日志存储 180 天及集中审计的要求。

背景信息

日志管理通过授权 OBS 存储 SA 日志，可实现日志存储、导出场景。日志存储后，支持长久存储和本地下载日志数据。

前提条件

已购买专业版态势感知，且在有效使用期内。

创建日志存储至 OBS 桶

为满足安全审计日志存储 180 天要求，可将日志存储至 OBS 桶。OBS 支持长久存储日志数据，并支持在 OBS 控制台下载日志文件。

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 > 态势感知 > 日志管理”，进入日志管理页面。

步骤 3 在“存储至 OBS 桶”栏中，单击  ，开启存储。

图9-1 存储至 OBS 桶

步骤 4 配置存储日志相关参数，具体参数说明如表 9-1 所示。

表9-1 配置存储日志参数说明

参数名称	参数说明
桶名称	选择已创建的 OBS 桶。 如果没有可选择的 OBS 桶，单击“您没有可用的 OBS 桶，请前往创建”，进入对象存储（原生版）II 型服务管理控制台，创建 OBS 桶。 说明 • 目前仅支持选择当前帐号所在的区域中已有的 OBS 桶。 • 目前仅支持存储类别为“标准存储”和“低频访问存储”的 OBS 桶。
对象名称	自定义对象名称。
存储路径	根据桶名称和对象名称生成的存储路径。

步骤 5 单击“确定”，完成配置。

配置成功后，日志将在大约 10 分钟后存储至 OBS 桶。

----结束

其他操作

若不再需要将日志存储至 OBS，可在“存储至 OBS 桶”栏中，单击  ，关闭日志存储至 OBS 桶。取消后，已上传存储到 OBS 桶的日志数据不会被删除。

10 产品集成

10.1 管理产品集成

态势感知通过集成安全防护产品，接入各安全产品检测数据，集中管理风险检测结果。

说明

若需启用其他产品集成，请在“安全产品集成”页面，单击右上角“我要推荐”，反馈相关产品信息。

本小节主要介绍如何管理安全产品集成，包括启用和取消产品集成。

启用产品集成

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 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

步骤 3 查询目标产品。

选择“未集成”筛选条件，查找符合条件的产品。更多查询方式请参见查看产品集成列表。

步骤 4 开启接收检测结果。

在目标产品列框，单击“开启集成”，开启接收来自该产品的检测数据。

启用产品集成后，约 5 分钟后即可接收到产品上报的数据。

说明

为确保产品检测数据的正常接收，请确保已开启各产品相应防护功能。

----结束

取消产品集成

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 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

步骤 3 查询目标产品。

选择“已集成”筛选条件，查找符合条件的产品。更多查询方式请参见查看产品集成列表。

步骤 4 取消接收检测结果。

在目标产品列框，单击“关闭集成”，取消接收来自该产品的检测数据。

----结束

10.2 查看产品集成

启用产品集成，并接入安全产品数据后，您可以管理集成列表，并可查看从产品接收的统计结果数量。

查看产品集成列表

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 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

步骤 3 选择“集成类型”和“探测状态”。

集成类型分为“检测结果类产品集成”、“调查分析类产品集成”。

探测状态分为“探测正常”、“探测异常”、“从未探测”、“停止探测”。

步骤 4 选择“产品名称”、“产品类型”或“公司名称”筛选条件。

步骤 5 在搜索框输入关键字，单击🔍，即可查看到满足条件的产品。

----结束

查看产品集成结果

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 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

步骤 3 查询目标产品。

选择“已集成”、集成类型和探测状态，查找符合条件的产品。更多查询方式请参见查看产品集成列表。

步骤 4 查看接收结果数量。

- 在目标产品列框，可查看从该产品的接收的全部和近一小时接收的结果数量。
- 单击“查看”，可跳转到“全部结果”管理页面，呈现该产品的检测结果列表。更多检测结果说明，请参见查看全部检测结果。

----结束

10.3 查看探测状态

“探测状态”是指安全产品数据上报到 SA 的状态。通过查看探测状态，您可以判断是否正常上报当前产品数据。

表10-1 探测状态说明

状态	说明
探测正常	表示一个小时内，数据接口被调用次数大于等于 8 次，接口连通性正常，“探测状态”检测正常，正常上报当前产品数据。 启用产品集成后一个小时内，默认探测状态为正常。
探测异常	表示一个小时内，数据接口被调用次数大于 0 次小于 8 次，接口连通性异常，“探测状态”检测异常，不能正常上报当前产品数据。
停止探测	表示已停止上报当前产品数据。
从未探测	表示从未上报当前产品数据。

说明

探测正常状态判断原则：启用产品集成上报数据后，产品可每 5 分钟调用一次探测接口确认连通性。通过记录产品调用数据接口次数，判断探测健康状态。

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 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

步骤 3 在探测状态中，选择目标状态，即可呈现该状态的全部产品。

步骤 4 在产品介绍栏，即可查看从该产品接收的数据量，以及该产品探测状态。

----结束

11 设置

11.1 检测设置

使用云服务基线相关功能时，需要先参考本章节设置检查计划。

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 > 态势感知”，进入态势感知页面。

步骤 3 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。

步骤 4 在检测设置页面中，选择待创建计划所在的区域，并单击“创建计划”，系统右侧弹出新建检查计划页面。

步骤 5 配置检查计划。

1. 填写基本信息，具体参数配置如表 11-1 所示。

表11-1 检查计划基本信息

参数名称	参数说明
计划名称	自定义检查计划的名称。
检查时间	选择检测周期和检查触发时间。 • 检测周期：每隔 1 天、3 天、7 天、15 天、30 天检查一次 • 检查触发时间：00:00~06:00、06:00~12:00、12:00~18:00、18:00~24:00

2. 选择检查规范。

   选择需要检测的基线检查项目。更多关于基线检查项目详细描述请参见云服务基线简介。

3. 单击“确定”。

步骤 6 检查计划创建完成。

SA 会在指定的时间执行云服务基线扫描，扫描结果可以在“安全 > 态势感知 > 基线检查”中查看。

----结束

12 常见问题

12.1 产品咨询

12.1.1 态势感知可以为我提供什么服务？

态势感知（Situation Awareness，SA）是可视化威胁检测和分析的平台。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为用户呈现出全局安全攻击态势。

12.1.2 为什么没有看到攻击数据或者看到的攻击数据很少？

态势感知支持检测云上资产遭受的各类攻击，并进行客观的呈现。但是，如果您的云上资产在互联网上的暴露面非常少（所谓“暴露面”是指资产可被攻击或利用的风险点，例如端口暴露和弱口令都可能成为风险点），那么遭受到攻击的可能性也将大大降低，所以态势感知可能会显示您的系统当前遭受的攻击程度较低。

12.1.3 态势感知的数据来源是什么？

态势感知基于云上威胁数据和云服务采集的威胁数据，通过大数据挖掘和机器学习，分析并呈现威胁态势，并提供防护建议。

- 一方面采集全网流量数据，以及安全防护设备日志等信息，通过大数据智能 AI 分析采集的信息，呈现资产的安全状况，并生成相应的威胁告警。
- 另一方面汇聚企业主机安全（Host Security Service，HSS）等安全防护服务上报的告警数据，从中获取必要的安全事件记录，进行大数据挖掘和机器学习，智能 AI 分析并识别出攻击和入侵，帮助用户了解攻击和入侵过程，并提供相关的防护措施建议。

态势感知通过对多方面的安全数据的分析，为安全事件的处置决策提供依据，实时呈现完整的全网攻击态势。

12.1.4 如何获取风险程度最高的资产信息？

通过查看资产风险排名，可以获取风险程度最高的资产信息，并可进一步了解该资产遭受的威胁告警统计信息。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面的上方的 ☰，选择“安全 > 态势感知 > 资源管理”，进入态势感知服务资源管理页面。

单击“安全状况”、“威胁”、“漏洞”、或“基线”列排序按钮，排序当前资产风险排名。

----结束

12.1.5 态势感知与其他安全服务之间的关系与区别？

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

- 关联：

  SA：作为安全管理服务，依赖于其他安全服务提供威胁检测数据，进行安全威胁风险分析，呈现全局安全威胁态势，并提供防护建议。

  其他安全服务：威胁检测数据可以统一汇聚在 SA 中，呈现全局安全威胁攻击态势。

- 区别：

  SA：仅为可视化威胁检测和分析的平台，不实施具体安全防护动作，需与其他安全服务搭配使用。

  其他安全服务：仅展示对应服务的检测分析数据，并实施具体安全防护动作，不会呈现全局的威胁攻击态势。

SA 与其他安全防护服务含义、关联与区别如表 12-1 所示。

表12-1 SA 与其他服务的区别

服务名称	服务类别	关联与区别	防护对象
态势感知（SA）	安全管理	SA 着重呈现全局安全威胁攻击态势，统筹分析多服务威胁数据和云上安全威胁，并提供防护建议。	呈现全局安全威胁攻击态势。
Anti-DDoS 流量清洗（Anti-DDoS）	网络安全	Anti-DDoS 集中于异常 DDoS 攻击流量的检测和防御。 同步相关攻击日志、防护等数据给 SA。	保障企业业务稳定性。
企业主机安全（HSS）	主机安全	HSS 着手于保障主机整体安全性，检测主机安全风险，执行防护策略。 同步相关告警、防护等数据给 SA。	保障主机整体安全性。
Web 应用防火墙（WAF）	应用安全	WAF 服务对网站业务流量进行多维度检测和防护，防御常见攻击，阻断攻击进一步威胁。	保障 Web 应用程序的可用性、安全性。

服务名称	服务类别	关联与区别	防护对象
		同步相关入侵日志、告警数据等给 SA，呈现全网 Web 风险态势。	

12.1.6 SA 与 HSS 服务的区别？

服务含义区别

- 态势感知（Situation Awareness，SA）是可视化威胁检测和分析的**安全管理平台**。着重呈现**全局**安全威胁攻击态势，统筹分析多服务威胁数据和云上安全威胁，帮助企业构建全局安全体系，呈现全局安全攻击态势。
- 主机安全服务（Host Security Service，HSS）是以工作负载为中心的安全产品，集成了**主机**安全、**容器**安全和**网页防篡改**，旨在解决混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。

简而言之，SA 是呈现**全局**安全态势的服务，HSS 是提升**主机**和**容器**安全性的服务。

服务功能区别

- SA 通过采集**全网安全数据**（包括 HSS、WAF、AntiDDoS 等安全服务检测数据），使用大数据 AI、机器学习等分析技术，从资产安全、威胁告警、基线检查维度，分类呈现资产安全状况。
- HSS 通过在**主机**中安装 Agent，使用 AI、机器学习和深度算法等技术分析主机中风险，并从 HSS 云端防护中心下发检测和防护任务，全方位保障主机安全。同时可从可视化控制台，管理主机 Agent 上报的安全信息。

表12-2 SA 与 HSS 主要功能区别

功能项		共同点	不同点
资产安全	主机资产	呈现主机资产的整体安全状态。	• SA：仅支持同步 HSS 主机资产风险信息，列表呈现各主机资产的整体安全状况。 • HSS：不仅支持呈现主机的安全状况，还支持深度扫描主机中的帐号、端口、进程、Web 目录、软件信息和自启动任务。
	网站资产	-	• SA：支持检查和扫描网站安全状态，列表呈现各网站资产的整体安全状况。 • HSS：不支持该功能。
基线检查	云服务基线	-	• SA：针对云服务关键配置项，从“安全上云合规检查 1.0”、“护网检查”风险类别，了解云服务风险配置的所在范围和风险配置数目。 • HSS：不支持该功能。
	主机基	-	• SA：不支持该功能。

功能项		共同点	不同点
	线		• HSS：针对主机，提供基线检查功能，包括检测复杂策略、弱口令及配置详情，包括对主机配置基线通过率、主机配置风险TOP5、主机弱口令检测、主机弱口令风险TOP5 的统计。

12.1.7 为什么主机最大配额不能小于主机数量？

主机最大配额是授权检测主机的最大数量。在购买态势感知时，选择的最大配额需等于或大于当前账户下主机总数量，且不支持减少。若购买的最大配额小于主机数量，可能会造成如下影响：

- 未授权检测的主机被攻击后，不能及时感知威胁，造成数据泄露等风险。

操作步骤

登录态势感知控制台，单击“升级”。根据规划或现有主机数量，配置主机最大配额。

图12-1 配置最大配额

12.1.8 如何更新安全评分？

态势感知支持实时检测整体资产的安全状态，评估整体资产安全健康得分。通过查看安全评分，可快速了解未处理风险对资产的整体威胁状况。

资产安全风险修复后，为降低安全评分的风险等级，目前需手动忽略或处理告警事件，刷新告警列表中告警事件状态。告警事件状态刷新并启动重新检测后，安全评分将更新。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在页面左上角单击，选择“安全 > 态势感知 > 检测结果”，进入全部检测结果页面。

步骤 3 忽略告警事件。

在相应告警事件“操作”列，单击“忽略”，告警事件状态更新为“已忽略”。

步骤 4 标记为线下处理。

1. 在相应告警事件“操作”列，单击“标记为线下处理”，弹出告警事件处理窗口。
2. 记录“处理人”、“处理时间”和“处理结果”。
3. 单击“确认”，返回告警列表页面，告警事件状态更新为“已线下处理”。

步骤 5 相应告警事件已标记后，返回“安全概览”页面，单击“重新检测”，检测后可查看更新的安全评分。

说明

由于检测需要一定的时间，请您在单击“重新检测”按钮 **5 分钟**后，再刷新页面，查看最新检测的安全评分。

----结束

12.1.9 如何处理暴力破解告警事件？

暴力破解是一种常见的入侵攻击行为，攻击者通常使用暴力破解的方式猜测远程登录的用户名和密码，一旦破解成功，即可实施攻击和控制，严重危害资产的安全。

态势感知联动企业主机安全服务（HSS），接收 HSS 检测到的暴力破解行为，集中呈现和管理告警事件，提升运维效率。

处理告警事件

HSS 通过暴力破解检测算法和全网 IP 黑名单，若发现暴力破解主机的行为，对发起攻击的源 IP 进行拦截，并上报告警事件。

当接收到来源于 HSS 的告警事件时，请登录 HSS 管理控制台确认并处理告警事件。

- 若您的主机被爆破成功，检测到入侵者成功登录主机，账户下所有云服务器可能已被植入恶意程序，建议参考如下措施，立即处理告警事件，避免进一步危害主机的风险。
  a. 请立即确认登录主机的源 IP 的可信情况。
  b. 请立即修改被暴力破解的系统账户口令。
  c. 请立即执行检测入侵风险账户，排查可疑账户并处理。
  d. 请及时执行恶意程序云查杀，排查系统恶意程序。
- 若您的主机被暴力破解，攻击源 IP 被 HSS 拦截，请参考如下措施，加固主机安全。
  a. 请及时确认登录主机的源 IP 的可信情况。
  b. 请及时登录主机系统，全面排查系统风险。
  c. 请根据实际需求升级 HSS 防护能力。
  d. 请根据实际情况加固主机安全组、防火墙配置。

标记告警事件

告警事件处理完成后，您可以根据处理情况，标记已识别的告警事件，加强对告警事件的管理。

步骤 1 登录管理控制台。

步骤 2 在页面左上角单击，选择“安全 > 态势感知 > 威胁告警”，进入告警列表管理页面。

步骤 3 选择“暴力破解”事件类型，刷新告警列表。

步骤 4 选择目标事件，根据实际情况忽略无威胁告警事件，标记已处理的告警事件。

----结束

12.1.10 为什么 WAF、HSS 中的数据和 SA 中的数据不一致？

由于 SA 中汇聚 WAF 和 HSS 上报的所有历史告警数据，而 WAF 和 HSS 中展示的是实时告警数据，导致存在 SA 与 WAF、HSS 中数据不一致的情况。

因此，建议您前往对应服务（WAF 或 HSS）进行查看并处理。

12.2 购买咨询

12.2.1 态势感知如何收费？

态势感知服务提供包年/包月和按需计费的计费模式。

- 包年/包月
- 按需计费：按小时计费，根据实际使用时长（小时）计费。先使用后付费，使用方式灵活，可以即开即停。

12.2.2 态势感知支持退订吗？

若用户不再使用态势感知防护功能，可执行退订或一键取消操作。

- 包周期（包年/包月）计费模式：预付费方式。新购 5 天内的资源，支持每年 10 次 5 天无理由“退订”；使用超过 5 天的资源，“退订”需要收取手续费。
- 按需计费模式：按小时计费方式。资源即开即停，支持一键“取消”释放资源。

退订包周期专业版

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 > 态势感知”，进入态势感知管理控制台。

步骤 3 单击右上角“专业版”，显示版本管理窗口。

步骤 4 针对包周期购买的资产配额，单击“退订”，进入“退订管理”列表页面。

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

步骤 6 确认待退订资源信息，选择退订原因，并勾选退订确认。

步骤 7 单击“退订”，在退订管理页面确认退订。

退订成功后，返回版本管理窗口，包年/包月计费的资产配额已取消。

----结束

退订按需专业版

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 > 态势感知”，进入态势感知管理控制台。

步骤 3 单击右上角“专业版”，显示版本管理窗口。

步骤 4 针对按需购买的版本，单击“取消”，一键释放按需计费的资产配额。

返回版本管理窗口，按需计费的资产配额资源已取消。

----结束

12.2.3 态势感知即将到期，如何续费？

态势感知续费是在原已购买的版本规格的基础上，延长使用时间。续费操作不能变更版本规格，即不能改变“主机配额”选择。

续费操作仅针对包周期版本。

- 包周期（包年/包月）模式为预付费方式。当购买的包周期资产配额到期时，用户需通过“续费”延长使用期。
- 按需计费为按小时计费，即开即用。在账户余额充足前提下，不涉及过期情况，即无需续费操作。

手动续费

步骤 1 登录管理控制台。

步骤 2 在页面左上角单击 ☰，选择“安全 > 态势感知”，进入态势感知管理控制台。

步骤 3 单击右上角“专业版”，显示版本管理窗口。

步骤 4 单击“续费”，系统跳转至费用中心“续费管理”页面。

步骤 5 在态势感知专业版实例所在行，单击“续费”，跳转至“续费”页面。

步骤 6 配置“选择续费时长”，如选择“一年”。

步骤 7 单击“去支付”，跳转至支付页面，完成付款。

步骤 8 返回续费管理页面，可查看态势感知已续费成功。

----结束

开通自动续费

在账户余额充足前提下，已配置“自动续费”后，包周期版本将自动续费，延长使用周期。

步骤 1 登录管理控制台。

步骤 2 单击“费用 > 续费管理”，跳转至费用中心“续费管理”页面。

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

步骤 4 选择配置“自动续费周期”和勾选“预设自动续费次数”。

步骤 5 单击“开通”，完成自动续费配置。

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

后续将根据配置，自动续费延长使用期。

----结束

12.2.4 态势感知到期后，会继续收费吗？

态势感知到期后，不会继续收费。

若到期后，未及时续费，会根据“客户等级”和“订购方式”定义不同的保留期时长，保留期内服务可继续使用，不收取费用。若保留期到期后，仍未及时续费，专业版会变为基础版。

12.2.5 如何修改或取消态势感知自动续费？

态势感知开通自动续费后，如果需要取消或修改，可参照本章节进行处理。

取消态势感知自动续费

态势感知开通自动续费后，支持取消自动续费操作。关闭自动续费后，版本到期将恢复为手动续费。

修改态势感知自动续费

态势感知开通自动续费后，支持修改续费配置，包括修改续费设定、修改自动续费周期、重置自动续费次数等。

12.2.6 态势感知可以免费使用吗？

可以。

态势感知提供基础版、专业版两个服务版本。

- 用户可长期免费使用基础版；
- 专业版支持包周期或按需计费购买。

A 修订记录

发布日期	修改记录
2023-03-20	第一次正式发布。