目录

安全总览

安全总览页实时展示了您账号下资产的威胁概览信息、实时安全评分及安全事件趋势，包括网络入侵、DDoS攻击情况、Web攻击、漏洞数、主机问题等安全统计信息。

安全评分

安全评分根据您资产近期的被攻击情况及资产安全现状等安全问题进行综合评估计算得到安全评分值，实时展现当前整体的安全状态。

当日安全情况总览

当日安全情况总览统计当日账号下资产的受攻击情况和资产存在的问题情况，您可以点击统计数据进入问题详情页，安全统计数据包括：

网络入侵

基于网络入口旁路流量深度分析进行入侵威胁检测，统计当日网络入侵整体情况。

DDoS攻击

当前只展示高防IP的DDoS攻击事件统计。

Web攻击

当日Web应用攻击统计，数据来源为WAF。

主机问题

展现账号下资产存在的安全问题。

DDoS攻击情况

DDoS攻击情况为您展示公有云弹性IP的基础防护情况和高防IP的DDoS攻击统计信息，您可以查看今天、近一周、近一月的DDoS攻击情况。

防护阈值

默认的防护阈值。

封禁阈值

即黑洞值，攻击超过封禁阈值将执行黑洞。

当前状态

封禁状态下状态将显示为“已封禁”。

攻击流量

查询时间段内的DDoS攻击总流量。

攻击峰值

查询时间段内的DDoS攻击峰值。

攻击次数

查询时间段内的DDoS攻击次数。

受攻击URL TOP排名

受攻击URL排名数据来源于WAF，展示您账号下web资产的受攻击URL排名情况，支持查询当日、近一周、近一月的URL受攻击情况

入侵威胁

入侵威胁通过在网络入口分光进行流量数据包深度检测和DNS安全分析，对出入向流量进行入侵威胁发现及告警，可以检测以下威胁问题：

- 网络病毒：包括僵尸、蠕虫、木马、勒索、挖矿等恶意软件
- 主机失陷：发现失陷的对外连接主机
- 恶意流量：发现具备威胁特征的恶意网络流量
- ATP攻击发现：通过对威胁事件进行时间行为关联与大数据分析进行APT攻击发现
- 其他未知威胁：基于机器学习及威胁模型发现未知威胁

威胁事件列表

进入入侵威胁页面，默认展示当天的入侵威胁列表，提供当日、近一周、近一月的入侵威胁事件查询。

威胁详情

威胁事件点击查看详情进入查看威胁事件详情，详情页可查看威胁概览，影响主机列表和处置建议。

查看威胁影响主机

您可在详情页面点击**影响主机**查看该次入侵威胁受影响的所有主机资产，也可在威胁事件列表中点击影响资产数量进入详情页查看。

弱点发现

弱点发现联动服务器安全Agent，对资产进行实时安全检测，可发现服务器系统漏洞、Web通用漏洞及第三方应用漏洞；同时对服务器进行异地登录、后门、暴力破解、网站威胁等安全检测并预警，帮助您及时发现服务器安全弱点。

服务器安全问题

进入弱点发现页面，点击**服务器安全问题**菜单进入服务器安全问题列表页。

- 服务器安全问题页展示账号下主机安全检测情况，包括登录权限问题、后门程序问题、系统补丁问题、暴力破解问题、网站安全问题
- 服务器安全问题详情当前需前往服务器安全产品控制台进行管理

攻击分析

攻击分析展示当日、近一周、近一月您账号下资产所受到的DDoS攻击和Web应用攻击的攻击事件列表，并进行可视化统计分析。

DDoS攻击分析

进入攻击分析页面，在**DDoS攻击**菜单下，查看DDoS攻击事件列表。

DDoS攻击可视化

DDoS攻击统计提供DDoS攻击次数、DDoS攻击峰值、被攻击资产TOP、攻击来源TOP、攻击类型分布的可视化分析。可查询当日、近一周、近一月的统计数据。

DDoS攻击事件列表

DDoS攻击事件列表展示您账号下高防IP资产的DDoS攻击事件列表，包括攻击开始时间和结束时间、被攻击IP、攻击类型、攻击源统计、攻击峰值、攻击状态。可查询当日、近一周、近一月的DDoS攻击事件列表，您可移动到列名右边的下拉按钮进行筛选或排序。

查看DDoS攻击源统计

您可点击查看攻击事件列表中的攻击源攻击，可查看攻击事件的攻击来源具体IP

Web攻击分析

进入攻击分析页面，点击**Web攻击**菜单进入Web攻击事件列表页。

Web攻击可视化

Web攻击统计提供Web攻击次数、被攻击域名TOP、攻击来源TOP、攻击类型分布的可视化分析。可查询当日、近一周、近一月的统计数据

Web攻击事件列表

Web攻击事件列表数据来源为WAF产品。可查询当日、近一周、近一月的DDoS攻击事件列表，您可移动到列名右边的下拉按钮进行筛选或排序。

实时大屏

云安全管理中心实时大屏为您提供多块实时态势大屏，从网络层、主机层、业务层全面感知各类网络安全风险，通过可视化大屏实时展现账号下资产、漏洞、攻击等安全攻防情况及安全运营数据，帮助您实现云上安全统一管理，提升整体安全威胁感知能力。

前提条件

实时大屏为增值服务，使用实时大屏前您需开通实时大屏。

查看大屏

登录云安全管理中心控制台，左侧菜单栏选择**实时大屏**，进入实时大屏页面，点击指定大屏可直接进入大屏页面。每块大屏分辨率为1080P。

编辑大屏标题

您可点击大屏标题右边的编辑功能修改大屏标题，修改后进入重新大屏即可生效。

Demo大屏

实时大屏提供全网安全态势大屏Demo页面，Demo页面提供多种DDoS攻击地图展示效果，点击第一块大屏标题右侧Demo入口即可进入Demo大屏。

安全态势总览

安全态势总览大屏展示用户资产的整体网络安全态势，包括以下部分

- **安全评分：** 安全评分根据您资产近期的被攻击情况及资产安全现状等安全问题进行综合评估计算得到安全评分值，实时展现当前整体的安全状态
- **七天受攻击总数：** 账号下所有资产过去七天内的DDoS攻击和Web入侵攻击总次数
- **资产分析：** 账号下所有EIP资产的region分布情况
- **24小时流量：** 账号下所有EIP过去24小时的请求总流量
- **24小时请求数：** 账号下所有EIP资产过去24小时的请求次数
- **24小时告警次数：** 账号下所有EIP资产过去24小时的告警总数，包含DDoS攻击、Web攻击、网络入侵攻击和服务器安全问题告警
- **DDoS网络攻击轨迹：** 展示最近一次DDoS攻击事件轨迹，国外攻击来源粒度为国家的，国内攻击目标精确到城市

- **实时带宽：** 账号下EIP资产过去1小时的实时入向和出向带宽
- **攻击来源地域TOP5：** DDoS攻击和Web攻击来源IP的地域排名TOP5
- **攻击目标地域TOP5：** DDoS攻击目标IP的地域排名TOP5

主机安全态势

主机安全态势以主机维度视角实时展示主机资产信息和安全告警情况，主机安全态势大屏包含以下功能：

- **主机情况**：展示整体的主机情况，包括主机总数、主机安全状态、主机告警情况及主机安全问题总览
- **告警列表**：实时滚动展示账号下主机资产的安全告警问题包括登录权限、后门程序、系统补丁、暴力破解问题
- **主机漏洞扫描情况**：展示账号下EIP资产的漏洞扫描情况
- **告警类型分布**：统计主机资产的安全告警问题类型TOP5分布情况
- **主机漏洞分布**：统计主机资产的漏洞TOP5类型分布情况
- **一周告警趋势**：展示主机资产一周的告警趋势，包括告警数量和告警主机数

业务安全态势

业务安全态势以Web业务为第一视角实时展示业务的受攻击情况，数据来源为WAF系统，业务安全态势大屏包含以下功能：

- **攻击来源IP TOP5**：对近一周对Web进行攻击的来源IP TOP5统计
- **攻击类型TOP5**：对进一周的Web攻击类型按照攻击次数进行TOP5排名
- **被攻击页面**：对近一周Web被攻击的URL和攻击类型进行滚动展示
- **风险页面扫描**：展示Web业务的风险页面扫描情况
- **一周攻击趋势**：展示近一周的Web受攻击趋势，包括受攻击次数和CC攻击次数