

安全运营中心 快速入门



腾讯云

【 版权声明 】

©2013–2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

快速入门

最近更新时间：2024-11-20 16:45:42

步骤1：日志源接入

1. SOC 首先需要接入日志，进入[系统管理](#) > [数据接入](#) > [日志接入](#)。
2. 在日志接入页面，根据实际需求，选择日志类型。
3. 单击**新建**，填写日志源名称、IP、接入方式、端口、解析策略组、编码方式、高级提取等配置。
4. 单击**保存完成新建**，完成内部各个日志源的接入和解析。

步骤2：查看告警

接入的日志会进行下一步的关联分析，与已有的告警策略匹配，命中的会产生告警，进入[安全检测](#) > [告警列表](#)，查看已产生的告警。

步骤3：检索数据

1. 对系统接入和产生的数据做检索，进入[调查中心](#) > [智能检索](#)。
2. 在智能检索页面，单击**搜索**，查看所有的日志或告警，或输入框输入搜索查询语句如 `logsource_subtype:腾讯御界`，单击 **Enter 键** > **搜索**查看检索后的日志。

步骤4：安全态势

在[安全可视](#) > [安全态势](#)页面，可以查看企业在全网范围内的日志、告警、安全事件的数量、趋势和 TOP 详情、安全运营趋势图，ATT&CK 告警态势概览等。