安全运营中心

快速入门

腾讯云

【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。