

# 高级威胁追溯系统

## 产品简介

## 产品文档



腾讯云

**【版权声明】**

©2013-2019 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

**【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。

**【服务声明】**

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。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模式的承诺或保证。

## 文档目录

### 产品简介

产品概述

产品优势

应用场景

# 产品简介

## 产品概述

最近更新时间：2018-12-14 17:37:14

## 什么是高级威胁追溯系统？

腾讯安图高级威胁追溯系统（以下简称安图），是腾讯构建的高级威胁追溯平台，旨在帮助用户通过该平台进行线索研判，攻击定性和关联分析，追溯威胁源头，预测威胁的发生并及时预警。

## 产品功能

- 线索研判  
全面展示威胁情报信息、威胁情报事件、访问该域名的样本信息、该域名上的可疑 URL、该域名上的可疑样本信息、包含该域名的样本信息。
- 攻击定性  
收集到的线索信息通过人工智能算法进行攻击定性。
- 关联分析  
通过人工智能算法，分析安图所收集到的不同信息之间的关联。

## 产品优势

最近更新时间：2019-05-20 15:51:41

### 多维度情报数据

安图汇集了全球不同来源的威胁情报及网络基础设施数据，包括失陷检测 IoC、IP 信誉、域名信誉、文件信誉、文件动静态分析数据、事件、家族、黑客团伙等。扩展信息包括地理信息、WHIOS 信息、关联样本、关联 APT 事件、历史活跃信息以及全面的开源威胁情报。

### 智能可视化分析

安图能进行智能的可视化关联分析，对线索的安全要素进行深度挖掘，自动输出关联分析后的溯源路径，降低安全分析门槛，提高安全分析效率。

### 态势分析

安图对安全要素的态势分析包括 IP、域名、文件、事件、家族的传播趋势和地域分布，用户可以通过分析结果直观的了解安全要素的影响情况。

# 应用场景

最近更新时间：2019-05-20 15:51:30

## 提升安全运营效率

- 通过安图追溯安全设备大量报警原因，帮助用户及时进行处理。
- 通过安图查询报警信誉度，高效判定线索威胁等级，提升安全运营效率。

## 研判黑客行为

- 有可疑黑客行为，可疑文件、IP、域名访问记录时，通过安图进行入侵确认与入侵目的研判。
- 通过安图对线索进行研判、关联分析，对攻击定性，实现追溯攻击来源的功能。