高级威胁追溯系统

词汇表

产品文档

腾讯云

【版权声明】

【商标声明】

【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。

词汇表

最近更新时间：2022-12-29 15:34:42

威胁情报

威胁情报（ TI，Threat intelligence ）是基于证据的知识，包括背景、机制、指标、影响和可采取行动的建议，涉及对资产现有或新出现的威胁或危害，可用于为有关主体应对措施的决定提供这种威胁或危险的信息。

高级持续性威胁

高级持续性威胁（ APT，Advanced Persistent Threat ）指拥有专业知识和重要资源的攻击者，通过多种攻击向量，针对特定对象，长期、有计划性和组织性地发动的攻击。

沙箱

沙箱是一个虚拟系统程序，允许用户在沙盘环境中运行浏览器或其他程序，因此运行所产生的变化可以随后删除。它创造了一个类似沙盒的独立作业环境，在其内部运行的程序并不能对硬盘产生永久性的影响。

WHOIS

WHOIS 用来查询互联网中域名的 IP 以及所有者等信息的传输协议。早期的 WHOIS 查询多以命令行接口（ Command Line ）存在，但是现在出现了一些基于网页接口的简化在线查询工具，甚至可以一次向不同的数据库查询。网页接口的查询工具仍然依赖 WHOIS 协议向服务器发送查询请求，命令行接口的工具仍然被系统管理员广泛使用。

ATT&CK

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) 是用于描述攻击者在企业内网可能采取行动的一个模型与框架。ATT&CK 对于 post－access 是一个持续进步的共同参考，其可以在网络入侵中意识到什么行动最可能发生。