NDR 网络威胁检测系统

词汇表

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。

词汇表

最近更新时间：2025-04-14 10:35:47

样本

样本（Sample）是需要经过分析来确定其是否会对计算机系统安全造成损害的文件。

木马病毒

木马病毒（Malware）是可以危害计算机系统安全的软件或程序。

高级持续性威胁

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

威胁情报

威胁情报（TI，Threat Intelligence）是基于证据的知识，包括针对攻击者的背景、机制、指标、影响力的描述，和可采取的防护措施的建议。它可以是描述已存在的或者是刚出现的能对资产产生威胁或危害的相关信息。 相关主体可参考这些信息，做出具体应对举措。

沙箱

沙箱（Sandbox）是一个虚拟系统程序，它创造了一个的独立运行环境，在其内部运行的程序并不会对硬盘产生实际影响。因此，沙箱通常用来运行样本。

入侵检测系统

入侵检测系统（IDS，Intrusion Detection System）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。