网络威胁是**指任何情况或事件，有可能对组织运作（包括任务、职能、形象或声誉）、组织资产、个人、其他组织或国家产生负面影响，通过未经授权的访问、销毁、披露或修改信息和/或拒绝服务。**

威胁信息是**任何与威胁相关的信息，这些信息可能帮助组织保护自己不受威胁或发现演员的活动。**主要类型的威胁信息包括以下内容：

**指标**：是技术产物或观察结果，表明攻击即将发生或正在进行中，或者可能已经发生了妥协。指标可用于检测和防范潜在威胁。指标的例子包括一个可疑的命令和控制服务器的因特网协议（IP）地址，一个可疑的域名系统（DNS）域名，一个统一的资源定位器（URL），它引用了恶意的内容，一个恶意的可执行文件的文件散列，或者一个恶意电子邮件消息的主题行文本。

**TTPs（策略、技巧和程序，**Tactics, techniques, and procedures**）**：描述一个参与者的行为。策略是对行为的高级描述，技术是在策略的上下文中对行为的详细描述，而过程是更低级的，在技术的上下文中非常详细的描述。TTPs可以描述一个参与者使用特定的恶意软件变体、操作顺序、攻击工具、交付机制（例如，网络钓鱼或水坑攻击）或利用的倾向。

**安全警报**：也称为警告、公告和漏洞注释，是关于当前漏洞、漏洞和其他安全问题的简短的、通常是人类可读的技术通知。安全警报来自美国计算机应急准备小组（US-CERT）、信息共享和分析中心（ISACs）、国家漏洞数据库（NVD）、产品安全事件响应小组（PSIRTs）、商业安全服务提供商和安全研究人员等来源。

**威胁情报报告**：通常是描述TTPs、参与者、系统类型和信息的目标的散文文档，以及其他与威胁相关的信息，这些信息为组织提供了更大的态势感知。威胁情报是一种威胁信息，它已经被聚合、转换、分析、解释或丰富，为决策过程提供了必要的上下文。

**工具配置**：是建立和使用支持自动收集、交换、处理、分析和使用威胁信息的工具（机制）的建议。例如，工具配置信息可以包含关于如何安装和使用rootkit检测和删除实用程序的说明，或者如何创建和定制入侵检测签名、路由器访问控制列表（acl）、防火墙规则或web过滤器配置文件。

**关于威胁信息格式**：网上没有明确的定义，但有一个相关的标准：《信息安全技术 网络安全威胁信息格式规范》，这个标准还没发布，网上也没有可下载的版本。

个人认为应该是规范，准确，全面地用于描述威胁信息表示的规范要求。

**威胁信息交换和共享**：目前也没有相关的定义。

个人认为：面对日益严重的安全威胁，单个企业无法进行全面，坚固的防御，可以通过交换企业之间的威胁情报来提高各自的防御能力，进而推进整体的网络安全，同时能够更有效的管理与网络相关的风险。

另外，查到了两个相关的条目： **结构化威胁信息表示**（STIX™），一种用于**交换网络威胁情报（CTI）**的语言和序列化格式。STIX使组织能够以一致且机器可读的方式彼此共享CTI，从而使安全社区能够更好地了解他们最有可能看到的基于计算机的攻击，并更快，更有效地预测和/或响应这些攻击。

还有 **可信的自动智能信息交换**（TAXII™），一种应用层协议，用于以简单且可扩展的方式传递网络威胁信息。通过HTTPS交换网络威胁情报（CTI）的协议。TAXII通过定义与常见共享模型一致的API，使组织能够共享CTI。**TAXII专门用于支持STIX中代表的CTI的交换。**