# 缩写

|  |  |  |
| --- | --- | --- |
| 缩写 | 全称 | 描述 |
| APT | Advanced Persistent Threat | 高级持久性威胁 |
| ATT&CK | Adversarial Tactics, Techniques, and Common Knowledge | 对抗性的战术、技术和常识 |
| C&C | Command and Control |  |
| CTI | Cyber threat intelligence | 网络威胁情报 |
| CVSS | Common Vulnerability Scoring System | 常见的漏洞评分系统 |
| DARPA | Defense Advanced Research Projects Agency | 国防高等研究计划署 |
| ETW | Event Tracing for Windows | 窗口的事件跟踪 |
| GPM | Graph Pattern Matching | 图形模式匹配 |
| HSG | High-level Scenario Graphs | 高级方案图 |
| IDS | Intrusion Detection System | 入侵检测系统 |
| IOC | Indicator of compromise | 折衷指标 |
| IPS | Intrusion Prevention System | 入侵预防系统 |
| LoC | Lines of Code | 代码行数 |
| PLC | Programmable Logic Controller | 可编程序逻辑控制器 |
| RAT | Remote Administration Tool | 远程管理工具 |
| SIEM | Security Information and Event Management | 安全信息和事件管理 |
| TC | Transparent Computing Project (by DARPA) | 透明计算项目(由DARPA提供) |
| TTP | Tactics, Techniques, and Procedures | 战术、技术和程序 |

P15