## 一、APT攻击的典型步骤

构建APT流量检测平台的主体思路，是要功能和模块化的。即一个模块监控APT攻击的一个环节。在开始设计之前需要了解一下APT攻击具有哪些典型步骤。



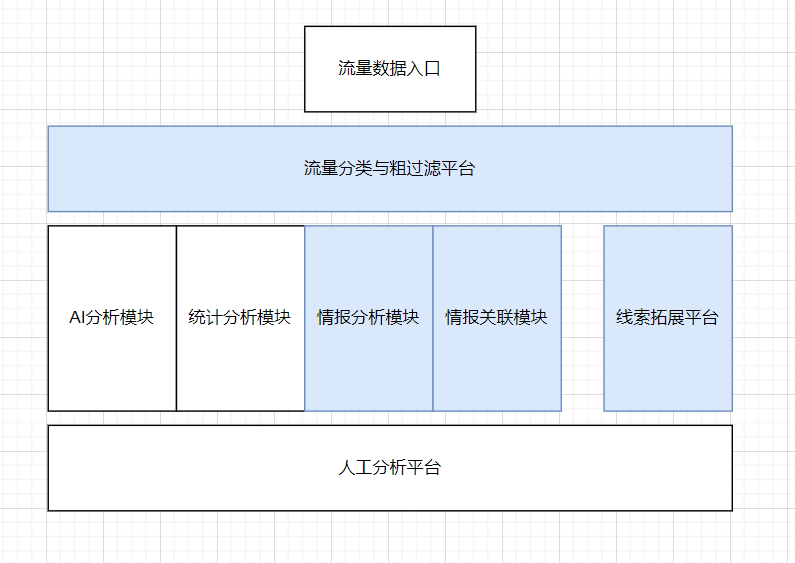
除上图之外，在标准ATT&CK里，还有侦察这一项。在这些攻击步骤中，可使用流量分析进行监控的环节有：

|  |  |
| --- | --- |
| 战术名称 | 可以通过流量监控的黑客技术手段 |
| 侦察阶段 | 主动扫描、收集受害者主机信息、收集受害者身份信息、收集受害者网络信息、收集受害者组织信息、网络钓鱼获取信息、搜索闭源、搜索开放技术数据库、搜索开放网站/域、搜索受害者拥有的网站 |
| 初始入侵阶段 | 偷梁换柱钓鱼、利用面向公众的服务、外部暴露服务、网络钓鱼、第三方信任关系、有效账户。 |
| 凭据访问阶段 | 基于网络的暴力破解、中间者攻击、利用盗取的凭据访问、强制身份验证、伪造网络凭据、基于网络的输入捕获，修改身份验证过程、网络嗅探、Kerberos 票证类攻击、窃取cookie，搜索不安全凭据。 |
| 信息发现阶段 | 账户发现、云基础架构发现、云服务仪表板、云服务发现、云存储对象发现、域信任发现、网络服务发现、网络共享发现、网络嗅探、远程系统发现、软件发现、系统位置发现、系统网络配置发现、系统网络连接发现、 |
| 横向移动阶段 | 利用远程服务、内部鱼叉式网络钓鱼、工具横向转移、远程服务会话劫持、远程服务、利用目标本地第三方工具、污染共享内容、使用备用身份验证材料。 |
| 信息收集阶段 | 中间者攻击、电子邮件收集、来自云存储的数据、来自信息库的数据。 |
| 命令与控制阶段 | 应用层协议、数据编码、数据混淆、动态分辨率、加密通道、利用目标本地第三方工具、多级通道、非应用层协议、非标端口、协议隧道、代理、远程访问软件、流量信令、网络服务。 |
| 数据泄露阶段 | 流量复制、数据分割传输、通过C2替代协议渗出、通过 C2 信道进行数据外渗、通过合法服务渗出、计划传输、将数据传输到云账户。 |

## 基于攻击步骤的流量监控平台

运营商的特点是流量大，流量大意味着信息全，意味着可以把许多弱线索，串联成线索连条，变成强线索，从而定义APT攻击。这也是本平台设计的优势。

总体设计如下：



图中蓝色部分为核心差异化的体现模块。同时设计中省区了存储、展示等等这些细节，以功能为核心进行设计。

流量经过分类与粗过滤平台，进行分类，然后根据分类，分配差异化的策略，进而差异化的执行后续流程。

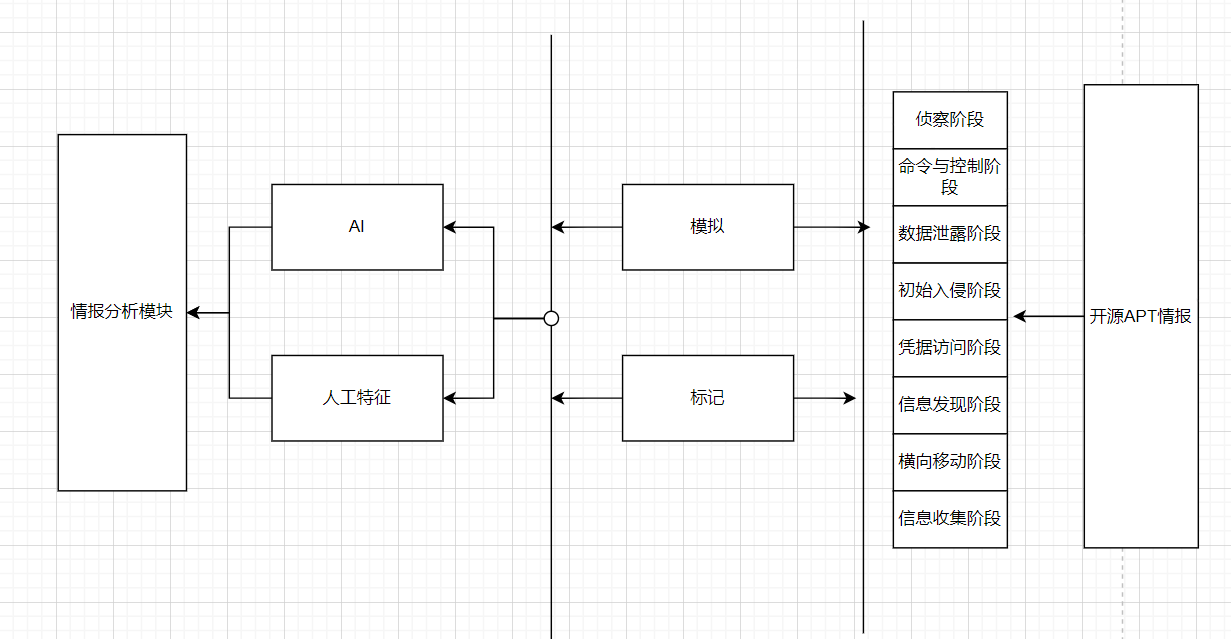
后续，流程会进入到AI分析模块和统计分析模块，通过一些常规或者现有的规则去进行网络威胁研判。

同时，流程会分布式的进入情报分析模块，根据APT攻击的各个阶段，进行流量识别。理论上结合病毒分析或者开源情报，可补全攻击的所有环节，这也是项目落地的一个方向。

接着，情报关联模块，会根据四元组信息，智能而又动态的，去情报库中进行线索拓展，进行综合分析，研判此流量的威胁程度。

考虑到落地场景，我们需要根据甲方提供的线索，进行线索拓展，进行APT溯源、攻击还原。所以需要一个专业的模块来查询这些信息。线索拓展平台就是以此为目的设计的。

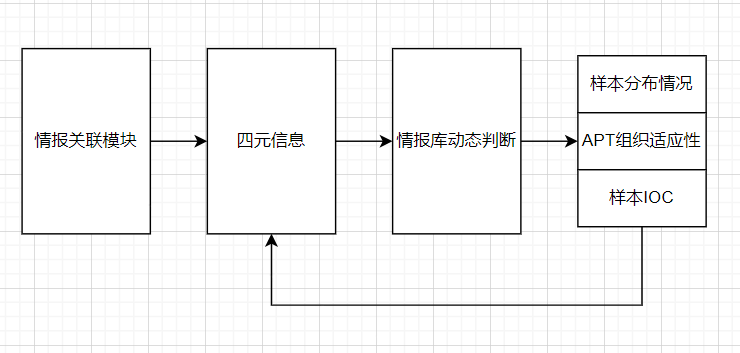
### 情报分析模块



情报分析人员，从各种开源渠道或者闭源渠道，获取样本、环境、文章、常见入侵手法。进行研判，进行标记，并从中提取特征，用于AI鉴别，用于特征匹配。

做到：数据经过情报分析模块，可以产生此数据是侦察阶段的概率，命令控制阶段的概率是多少。当数据量又全又大的时候，整个攻击链条就能还原。

### 情报关联模块



这是一个不停嵌套运行，发散查询线索的模块，APT分析不知能只靠着流量来分析，落地的场景也不可能只关注流量，需要去各个情报库发散线索，来确定这个IP这个流量是属于哪个组织，是不是恶意的。