1. **名字**

软件活动监控（Software Activity Monitor）

1. **问题**

这是我在实际使用Windows以及Linux的过程中遇到的一些比较实际的问题：

1. 总所周知，在Windows以及Linux系统中，某些软件会偷偷的开启一些不必要的后台占用你宝贵的系统资源；

2. 某些软件会在运行时创建大量文件、修改你的注册表等等，然而在你将软件卸载后，这些文件以及注册表并不会被删除，这就导致你的系统变得越来越臃肿，甚至出现卡顿。即使你想要自己整理，面对大量的文件以及条目与五花八门的命名，你也很难入手；

3. 此外，某些软件在安装时，会偷偷捆绑安装其它软件，例如挖矿软件等。通过软件活动监控，可以及时发现这些行为，并进行阻止。

1. **方法**

1. 开发一个低资源占用的后台服务，实时记录软件启动、运行和退出时间

2. 利用文件系统监控API，建立文件操作钩子（hook），捕获所有文件创建和删除事件并记录相关元数据

3. 建立集中式日志管理系统，将收集的数据进行存储和索引

4. 提供可视化界面，允许用户查询和分析软件行为模式

5. 设计报警机制，当检测到异常活动时自动通知系统管理员

1. **举例**

某企业的IT部门部署该软件来监控公司网络内的计算机。在一次监控中，系统检测到一个普通办公应用程序在非工作时间突然启动，并开始快速创建和删除大量文件。系统立即向IT管理员发送警报，管理员发现这是一个勒索软件的早期活动迹象。由于及时干预，管理员能够隔离受影响的计算机，防止勒索软件加密企业关键数据和扩散到网络中的其他设备，避免了潜在的重大损失。

1. **功能**

1. 软件运行时间跟踪：记录软件启动时间、总运行时长、频率统计

2. 文件活动监控：捕获并记录文件创建、删除、修改事件及相关元数据

3. 实时告警：当检测到异常模式时发送通知

4. 历史数据查询：按照应用程序、时间段、活动类型等条件搜索历史记录

5. 数据可视化：通过图表和时间线展示软件行为模式

6. 报告生成：自动生成定期或按需的活动摘要报告

7. 规则配置：允许自定义监控规则和阈值

1. **设备**

该软件需要与以下设备和系统集成：

1. 各类操作系统（Windows、macOS、Linux）上运行的计算机和服务器

2. 移动设备（用于远程监控和告警接收）