入侵检测系统框架(Common intrusion detection framework, CIDF)

四个组件：

1. 事件产生器：收集时间，转换成GIDO格式
2. 事件分析器：分析从其他组件收到的GIDO，产生分析结果，并传送给其他组件
3. 响应单元：接收处理到的GIDO，根据分析结果做出反应
4. 事件数据库：用来存储GIDO，以备系统需要的时候查询和使用