# **TAREFAS PARA SRC:**

1. Cálculo de **estatísticas** relevantes (endereços de IP de origem, endereços de IP destino, portos mais comuns, protocolos mais comuns, estatísticas do número de pacotes/bytes de upload e de download)
2. Deteção de **exfiltracao** de dados (taxas anormais de upload/download usando os protocolos HTTP/HTTPS, portos 80 e 443, e DNS porta 53). Verificar se os IP de destino pertencem a serviços “Cloud”.
3. **Comunicações não habituais** (IPS de origem de países estranhos, previamente identificados e colocados numa “lisa negra”)
4. **Deteção de botnets** (comunicações entre máquinas internas em número diferente do habitual).
5. **Command and Control** (troca não habitual, em número e tamanho dos pacotes, de mensagens DNS porto de destino 53)
6. **Distinção dos clientes externos** que se comportam de forma estranha nos “nossos” servidores (analisando por exemplo intervalos pequenos/periódicos entre fluxos)
7. Protocolos mais comuns: