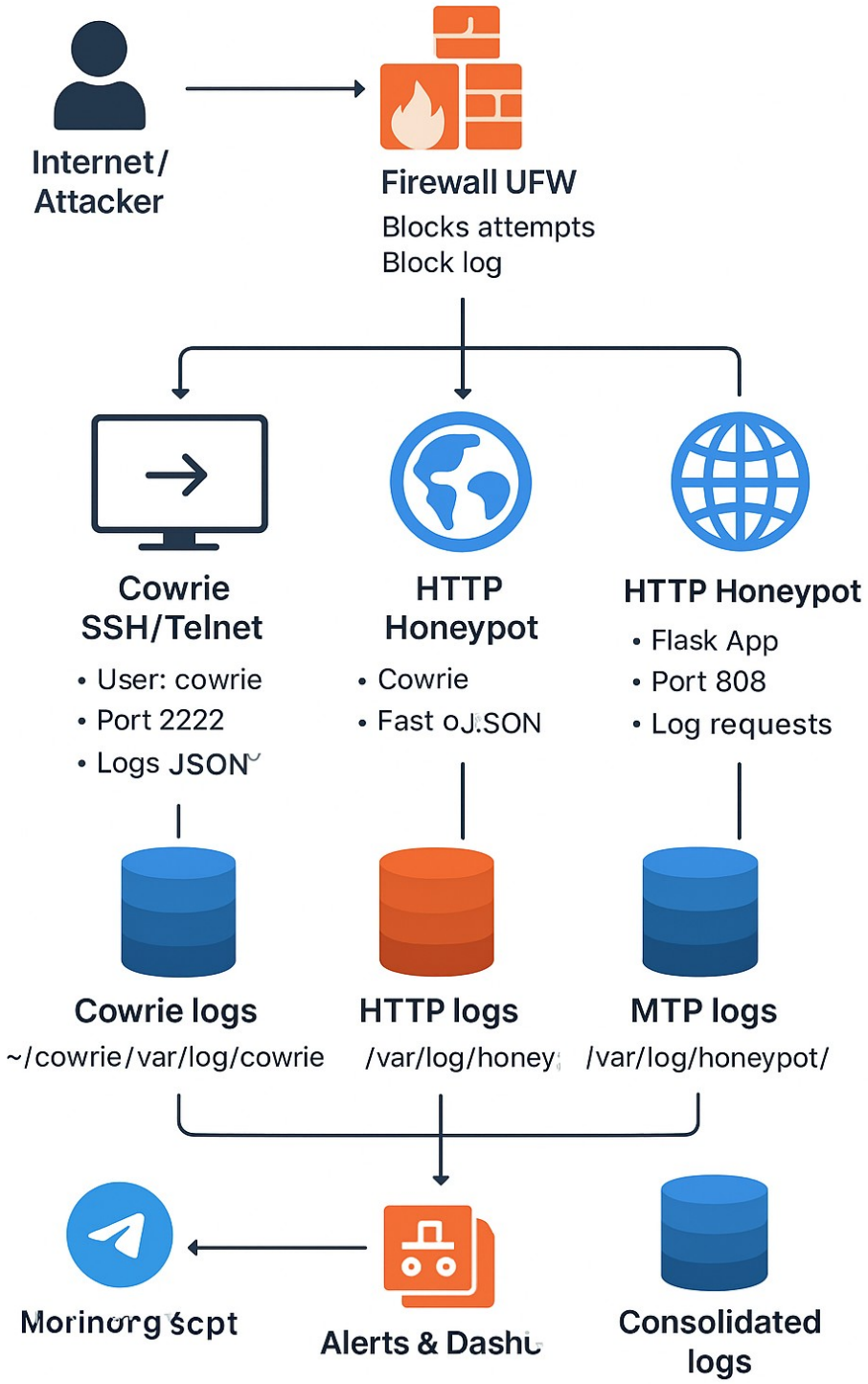
🐝 Projeto “Potinho-de-Mel” – ADR (Arq. Alam Izaguirre)



1. Ideia inicial

- Criar **um mecanismo de segurança que funciona como "honeypot"**.
- O objetivo é **convidar invasores** a entrar em uma VM simulando ambiente produtivo, para:
    - rastrear ações;
    - catalogar tentativas de fraude;
    - gerar evidências jurídicas para possíveis ações contra o invasor.
- Diferencial: foco em **monitoramento, documentação e coleta de evidências**, não bloqueio preventivo tradicional.

---

2. Funcionalidades planejadas

- **VM com portas abertas** simulando produção.
- **"Potinho de mel" digital**: recursos que parecem vulneráveis para atrair invasores.
- **Registro detalhado**: logs de origem e ações do invasor.
- **Possibilidade de automação inteligente**:
    - detectar tipo de ataque;
    - coletar dados para análise futura;
    - integração com sistemas de alerta.
- **Objetivo judicial**: criar provas válidas juridicamente com rastreamento completo.

---

3. Etapas de implementação discutidas

- **Dia 1**: Criar VM/ambiente honeypot.
- **Dia 2**: Configurar portas e serviços simulados vulneráveis.
- **Dia 3**: Log e monitoramento detalhado de atividades.
- **Dia 4**: Automatizar alertas ou captura de evidências.
- **Dia 5**: Teste de segurança e simulação de ataques.

---

4. Recursos e tecnologias citadas

- **VMs e ambientes isolados** (possivelmente Docker ou virtualização tradicional).
- **Captura de rede e logs detalhados** (tcpdump, Wireshark, ou agentes custom).

- **Integração futura**:
    - análise automática por LLM ou IA generativa;
    - classificação de ataques;
    - geração de relatórios prontos para uso jurídico.
- Links/ideias mencionadas: GitHub – Potinho de Mel (não publicado ainda).

---

5. Ideias adicionais e extensões

- **“Super DDoS” simulado** para testar respostas sem impactar produção real.
- **Porta aberta como convite** com monitoramento em tempo real.
- Possível **integração com dashboards** para visualização de comportamento dos atacantes.
- Consideração ética/jurídica: manter ambiente seguro e evidências válidas, sem expor dados reais.

Tipo de Hack	Resposta Potinho-de-Mel
- Reconhecimento - Port scanning - Fingerprinting - Enumeração de serviços	Registra IP, horários e padrões de varredura
- Exploração - SQL Injection - Brute Force - Exploits conhecidos	Captura payloads, usuários/IPs e comportamento
- Malware / Scripts - Upload de arquivos maliciosos - Execução remota simulada Tentativas de Troja - Bot	Registra scripts enviados e payloads
- DDoS / Ataques de Rede - Flood TCP/UDP - Ping/SYN floods	Registra origem e padrões sem afetar produção
- Engenharia Social / APIs - Tentativas de enviar comandos - Exploração de credenciais	Registra ações e padrões de tentativa
- Técnicas Avançadas / Persistência - Tentativa de apagar logs - Escalonamento de privilégios - Movimentação lateral simulada	Coleta evidências e comportamento do atacante

Ações previstas em um ataque cibernético em segui as reações.

Por se tratar de um ambiente em uma VM para que os ofensores baixem a guarda, não será feita nenhuma intervenção militar até que estejam distantes da cidade;