**Honeypot: Esse tipo de detecção funciona usando um servidor como "isca", que tem os mesmos aplicativos e programas de um servidor comum da empresa, mas sem dados (ou dados falsos). Suas vantagens são que ele funciona como um observatório para visualizar os ataques (já que é possível deixar o atacante "brincar" ali), além de servir para distrair-los, e ainda servem para atrasar os atacantes, pois a invasão terá sido em vão.**

**Suas desvantagens são que um servidor é propositalmente inutilizado (custo financeiro, energetico, etc), e seu funcionamento não deve ser confiado, já que seus dados não são reais.**

**Anomalia: Como comentado na questão anterior, um IDS pode ter ciência de um ataque acontecendo observando o tráfego na rede: enquanto esse tráfego estiver estável e num valor normal para o sistema, sabemos que está tudo bem. Quando há um pico de tráfego, é possível detectar uma tentativa de intrusão na rede (ou uma intrusão com sucesso). Suas vantagens são de que esse tipo de detecção é simples, pois usa apenas o monitorador, e confiável (dadas as corretas configurações).**

**PS: para configurar um sistema desse, deve ser descrito tudo que não é um ataque para que quando haja algo fora desse escopo, seja possível detectar.**

**Com a informação acima, temos outras vantagens: a política de detecção é personalizada, e é feita a detecção para quaisquer ataques.**

**Desvantagens: como é um sistema de detecção generalizada (detecta o ataque, mas não qual), não é possivel tratar casos específicos. E a configuração deste também não é das mais fáceis, visto que devem ser descritos todos os cenários normais.**