1.Honeypot

Um *honeypot* **é um recurso de segurança projetado para ser alvo de ataques, desviando a atenção de sistemas reais**. Existem dois tipos principais: honeypots de baixa interação, que emulam serviços sem expor vulnerabilidades reais, e honeypots de alta interação, que simulam sistemas operacionais completos e serviços reais. Ao atrair atacantes para um ambiente falso, os honeypots permitem que as organizações estudem táticas, técnicas e procedimentos (TTPs) de potenciais adversários. Isso facilita a detecção precoce e a resposta a ameaças reais.

2.Honeynet

Uma *honeynet* **é uma rede de honeypots interconectados**. Essa abordagem amplia as capacidades do honeypot, permitindo a observação de atividades coordenadas em uma escala maior. Honeynets proporcionam uma visão mais abrangente das estratégias de ataque, pois simulam uma rede real. Elas são particularmente eficazes para a detecção de ataques coordenados e campanhas maliciosas mais amplas.

3.Honeyfile

Um *honeyfile* **é um arquivo fictício projetado para atrair atividades maliciosas**. Pode ser usado para detectar tentativas de acesso não autorizado a informações específicas. Ao monitorar e analisar atividades em torno do honeyfile, as organizações podem identificar tentativas de acesso não autorizado ou exfiltração de dados.

4.Honeytoken

Utilizado para adicionar dados rastreáveis a sua *honeynet*. Se estes dados são roubados, é possível saber de onde eles vieram. Uma maneira de criar *honeytoken* são com credenciais de APIs, porém, os dados contidos nestes *tokens* são falsos, garantindo nenhum acesso a rede interna. Quando forem usados, será emitido um alerta de tentativa de acesso. Exemplos de dados podem ser também endereços de e-mail, registros de banco de dados, cookies de *browsers* e muitos outros