Junior GBOKOSSOU

1. INTRODUCTION

Dans un écosystème numérique où les périmètres de sécurité traditionnels s'effritent, la question n'est plus de savoir *si* une intrusion aura lieu, mais *quand*. Face à cette situation, les stratégies purement bloquantes (Firewall, AV) montrent leurs limites.
Ce rapport de veille se concentre sur une réponse proactive à ce problème : les **Honeypots (Pots de Miel)** et la **Déception Technologique**. L'objectif est de passer d'une défense passive à une défense active, capable de piéger l'attaquant et d'analyser son comportement en temps réel.

2. DÉFINITION ET FONCTIONNEMENT

2.1. Qu'est-ce qu'un Honeypot ?

Un Honeypot est un système d'information leurre (serveur, base de données, fichier, clé API) volontairement rendu vulnérable et exposé. Il n'a aucune fonction de production légitime.

> **Le principe clé :** "Toute interaction avec un honeypot est, par définition, une anomalie suspecte et potentiellement malveillante."

2.2. Mécanisme de défense

Le fonctionnement repose sur l'exploitation des phases de reconnaissance de l'attaquant (Kill Chain) :

1. **Leurre :** Le honeypot imite une cible de haute valeur (ex: serveur "Compta_2024").
2. **Attraction :** L'attaquant scanne le réseau et mord à l'hameçon.
3. **Surveillance :** Contrairement à un serveur réel, le honeypot enregistre chaque frappe de clavier, chaque commande et chaque fichier téléchargé sans bruit de fond.
4. **Alerte :** Une notification précise est envoyée aux équipes de sécurité (SOC) pour une réaction immédiate.

2.3. Typologie

- **Faible Interaction (Low-Interaction) :** Simule uniquement des services (ports ouverts, bannières). Peu risqué, facile à déployer.
- **Haute Interaction (High-Interaction) :** Vrai système d'exploitation instrumenté. Très réaliste, permet d'observer les outils de l'attaquant, mais demande plus de surveillance.

3. TENDANCES ACTUELLES (2024-2025)

L'évolution des menaces pousse les technologies de leurre à se transformer. Voici les trois tendances majeures identifiées lors de cette veille :

A. L'Honeypot "Full-Stack" (Deception Everywhere)

On ne déploie plus un simple serveur isolé. La tendance est à la dissémination de **Honeytokens** (miettes de pain) partout : fausses clés AWS dans le code, faux fichiers "mots de passe" sur les postes utilisateurs.

- *Objectif :* Détecter les mouvements latéraux instantanément, même dans le Cloud ou les conteneurs Kubernetes.

B. Intégration SOAR et Automatisation

Le honeypot devient le détonateur de la réponse à incident.

- *Scénario actuel :* Une intrusion est détectée sur le leurre -> Le système SOAR (Security Orchestration) isole automatiquement le VLAN concerné et bloque l'IP attaquante en moins de 30 secondes, sans intervention humaine.

C. Réalisme comportemental

Pour contrer les pirates qui vérifient s'ils sont dans un piège (Anti-VM), les honeypots modernes simulent une activité humaine : mouvements de souris aléatoires, faux historiques de navigation, cycles de redémarrage cohérents.

4. CONCLUSION & VISION : L'IMPACT DE L'IA

L'avenir des Honeypots se joue désormais sur le terrain de l'**Intelligence Artificielle (IA)**. C'est la prochaine frontière de ma veille.

Jusqu'à récemment, un expert pouvait reconnaître un honeypot à cause de ses réponses statiques. L'IA générative (LLM) change la donne :

1. **Honeypots Conversationnels :** Des leurres pilotés par l'IA peuvent désormais tenir une "conversation" technique avec l'attaquant