Corrigé Activité P1C5

Voici une proposition de grille d'évaluation basée sur des mises en situation concrètes pour le poste d'Analyste SOC chez Téraveo :

Grille d'évaluation : Analyste SOC (Profil Reconversion)

Scénario 1 : L'investigation initiale (Hard Skills / Raisonnement)

- *Question posée au candidat :* « Un collaborateur du service comptabilité vous signale par téléphone un e-mail suspect. Il avoue, paniqué, avoir cliqué sur une pièce jointe nommée "Facture_Urgente.pdf". Quelles sont vos toutes premières actions ? »
- *Comportements attendus (Ce qu'on veut entendre) :* Le candidat rassure l'utilisateur (Soft Skill). Il demande la déconnexion immédiate du poste du réseau (Isolement). Il récupère l'adresse IP ou le nom de la machine. Il indique qu'il va ensuite analyser les journaux (logs) du pare-feu et de l'antivirus pour voir si la pièce jointe a exécuté une charge malveillante.
- *Red flag (Ce qu'on ne veut pas entendre) :* "Je formate immédiatement le PC", sans chercher à qualifier l'incident ou à préserver les preuves.

Scénario 2 : La communication sous pression (Soft Skills / Gestion de crise)

- *Question posée au candidat :* « Il est 17h45. En analysant une alerte de votre SIEM, vous suspectez une compromission active et grave sur le serveur contenant les données de nos clients industriels. Comment communiquez-vous la situation à votre responsable et à la direction ? »
- *Comportements attendus (Ce qu'on veut entendre) :* Le candidat explique qu'il hiérarchise l'information. Il alerte immédiatement le RSSI avec des faits qualifiés (Quoi, Qui, Quel système), sans céder à la panique. Il adapte son vocabulaire pour que la direction comprenne l'urgence (risque métier) sans se noyer dans le jargon technique.
- *Red flag (Ce qu'on ne veut pas entendre) :* Le candidat panique, agit seul sans escalader, ou envoie un e-mail incompréhensible rempli d'acronymes à toute l'entreprise.

Scénario 3 : La gestion de l'incertitude (Humilité / Adaptabilité)

- *Question posée au candidat :* « Comment utiliseriez-vous une règle YARA pour chasser un malware *fileless* (sans fichier) injecté directement dans la mémoire vive ? » *(Note : C'est une question très avancée, hors de portée d'un profil junior).*
- *Comportements attendus (Ce qu'on veut entendre) :* Le candidat admet avec honnêteté qu'il ne maîtrise pas ce concept avancé. Il explique cependant comment il s'y prendrait pour apprendre : "Je ne sais pas le faire de tête, mais je consulterais la documentation officielle, je demanderais conseil à un membre senior de l'équipe, et je testerais ma règle dans un environnement bac à sable (sandbox) avant de la déployer."
- *Red flag (Ce qu'on ne veut pas entendre) :* Le candidat invente une réponse technique farfelue pour masquer son ignorance.

Feedback post-entretien :

- *Axe de progression à partager au candidat en cas de second tour :* (Exemple) "Excellente gestion du stress sur le scénario 2. Pour notre prochain échange, j'aimerais que vous vous documentiez sur notre secteur industriel pour mieux comprendre quels types de données nos attaquants pourraient cibler en priorité."