

Corrigé Activité P2C1



Voici comment vous pouvez structurer et séquencer les deux premières semaines de votre nouvel Analyste SOC pour maximiser son intégration technique et humaine :

Semaine 1 : Découverte, Culture et Environnement

- **Lundi matin (Objectif : Accueil institutionnel)** : Accueil par le manager (vous) et les RH. Remise du matériel, présentation du programme des 90 jours, déjeuner informel avec toute l'équipe sécurité.
- **Mardi (Objectif : Comprendre le terrain)** : "Vis ma vie" d'une demi-journée avec un administrateur réseau de la DSI de Téraveo. *Pourquoi ? Pour comprendre concrètement l'architecture qu'il devra défendre et nouer un premier contact humain.*
- **Mercredi (Objectif : Découverte des outils)** : Session en binôme avec son mentor. Découverte de l'interface du SIEM en mode "lecture seule". L'objectif n'est pas d'agir, mais de regarder le mentor travailler et de comprendre comment remonte une alerte.
- **Jeudi (Objectif : Cadre documentaire)** : Lecture autonome mais guidée des principales fiches réflexes (réaction face à un phishing, isolement d'un poste).
- **Vendredi après-midi (Objectif : Feedback)** : Point de fin de semaine avec vous (le manager). Recueil de ses premières impressions. Le cadre psychologique sécurisant est posé.

Semaine 2 : Pratique guidée et Mise en situation

- **Lundi et Mardi (Objectif : Pratique accompagnée)** : *Shadowing* inversé. Le collaborateur prend la souris sur le SIEM pour faire ses premiers tris d'alertes de niveau 1, mais le mentor est assis à côté de lui en permanence pour le guider et valider ses choix d'investigation.
- **Mercredi (Objectif : Acculturation métier)** : Rencontre de 30 minutes avec un interlocuteur clé (ex: le directeur de la production industrielle) pour comprendre quelles sont les machines critiques qui ne doivent *jamais* être coupées sans préavis, même en cas de virus.
- **Jeudi (Objectif : Autonomie encadrée)** : Traitement de tickets simples de manière autonome. Le mentor ne fait que valider la clôture du ticket à la fin de l'analyse.
- **Vendredi (Objectif : Validation et Confiance)** : Résolution d'un faux incident (un CTF interne ou un exercice sur table préparé par l'équipe). Le collaborateur doit appliquer une fiche réflexe de A à Z. Clôture de la semaine par un point de suivi RH et manager pour lancer le mois suivant.