Corrigé Activité P1C2

Voici comment vous pouvez structurer le diagnostic en vous inspirant du profil *Cyber Incident Responder* de l'ECSF :

Diagnostic de création de poste : Analyste SOC (Cyber Incident Responder)

Tâches ECSF (Missions réelles)	Maturité interne actuelle
Qualification et tri des alertes de sécurité de niveau 1.	Processus moyennement mature. Procédures et fiches réflexes existantes. Idéal pour un profil junior.
Analyse des logs systèmes et réseaux pour qualifier l'incident.	Processus à consolider avec le nouvel outil SIEM. Potentiel d'apprentissage technique requis.
Coopération avec la DSI pour l'isolement des machines compromises.	Processus nécessitant beaucoup de tact humain.

Compétences (Skills) et Connaissances (Knowledge) recherchées :

- **Compétences (Techniques et Comportementales) :**
  - Capacité à collecter, gérer et analyser des fichiers journaux (logs).
  - Gestion du stress et capacité à travailler sous pression lors d'un incident.
  - Excellente communication interpersonnelle pour collaborer avec tous types d'interlocuteurs et sans conflit.
- **Connaissances (Prérequis) :**
  - Compréhension des réseaux informatiques (TCP/IP) et des systèmes d'exploitation.
  - Connaissance générale des cybermenaces et des vecteurs d'attaque.