**TD PRINCIPES FONDAMENTAUX DE LA CYBERSECURITE**

**EXERCICE 01 :**

1- Quel agent au sein d'un centre opérationnel de sécurité est chargé de vérifier si une alerte déclenchée par un logiciel de surveillance correspond réellement à un incident ?

2- Après la confirmation d'un incident au sein d'un centre opérationnel de sécurité, un gestionnaire des incidents l'examine, mais ne parvient pas à en identifier la source, ni à établir une procédure de traitement des menaces efficace. À qui le ticket d'incident doit-il être dégénéré?

3- Quels sont les deux services fournis par les centres opérationnels de sécurité ? Citez-en deux.

4- Quelle mesure est utilisée dans les SOC pour évaluer le temps moyen nécessaire pour identifier les incidents de sécurité valides sur le réseau?

5- Quelle mesure d'indicateur de performance clé SOAR utilise-t-elle pour mesurer la durée pendant laquelle les acteurs de menace ont accès à un réseau avant qu'ils ne soient détectés et que l'accès des acteurs de menace soit arrêté?

6- Quel est le rôle du SIEM?

7- Quelle est la caractéristique de la plateforme de sécurité SOAR?

8- Un professionnel de la sécurité du réseau a posé sa candidature à un poste de niveau 2 au sein d'un centre opérationnel de la sécurité. Quelle fonction est généralement attribuée à un nouvel employé ?

9- Si un centre opérationnel de sécurité a un objectif de disponibilité de 99.99%, combien de minutes d'indisponibilité par an sont tolérées?

10- Quel organisme propose la certification CSA+ indépendante du fournisseur ?

11- Dans le cadre de l'exploitation d'un centre opérationnel de sécurité, quel système est fréquemment utilisé pour permettre à un analyste de sélectionner des alertes dans un pool en vue de faire des recherches ?

12- Comment un système de gestion des événements et des informations liés à la sécurité peut-il être utilisé au sein d'un centre opérationnel de sécurité pour aider le personnel à lutter contre les menaces pour la sécurité ?

13- Quelles sont les trois technologies que devrait intégrer le système de gestion des événements et des informations liés à la sécurité d'un centre opérationnel de sécurité ? Citez-en trois.