**CORRECTION DU TD1**

1. L‘agent chargé de vérifier cette alerte est : **l’opérateur de sécurité de niveau 1**

Il dégrossi les menaces, les tickets et préqualifie les alertes.

1. Le ticket d’incident doit être dégénéré à **un expert en sécurité** en vu d’un examen plus approfondi
2. Les deux services fournis par le centre opérationnel de sécurité sont :

**-La gestion des solutions complète de lutte contre les menaces**

**-Le contrôle des menaces de la sécurité**

1. La mesure utilisée pour évaluer les temps moyens nécessaire pour identifier les incidents est :

**Le temps moyen de détection** (Mean Time To Detect). Le temps moyen de détection est un indicateur de performance clé qui est important dans le domaine de la gestion des incidents de l’informatique. Le MTTD peut se définir comme le temps écoulé entre le début d’un incident informatique et la découverte de l’incident par votre équipe de sécurité. MTTD= la somme totale de détection / le nombre total d’incident

1. La mesure d'indicateur de performance clé SOAR utilisé 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 est :

**Le temps d’immobilisation.** Le SOAR (Security Orchestration Automation and Reponse) décrit les technologies qui permet de protéger les systèmes informatiques contre les menaces

1. Le rôle du SIEM est :

Il prend en compte toutes les données générées par le$ pare-feu et les systèmes de détection et autre

1. La caractéristique de la plateforme de sécurité SOAR est d’inclure des Play boot prédéfinis qui permettent une réponse automatique a des menaces spécifiques.
2. La fonction généralement attribuée à un nouvel employé est : **Analyste de sécurité**
3. Le nombre de minute de disponibilité toléré par an est : **52,56 secondes**
4. L’organisme qui propose la certification CSA+ indépendante du fournisseur est **le ComPTIA+**
5. Le système fréquemment utilisé pour permettre à un analyste de sélectionner des alertes dans un pool en vue de faire des recherches est : **le système de gestion des incidents**
6. Pour aider le personnel à lutter contre les menaces contre la sécurité il faut **collecter les données et les filtrer**
7. 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 sont**:**

**- La surveillance de la sécurité**

**- Le suivit des vulnérabilités**

**- Les informations sur les menaces**

Correction du TD 2

Quel plan de gestion

Kismac est une application qui passe la carte wifi en mode moniteur

C’est un outils de reseau sans fils