Opérateur analyste SOC (Security Operation Center)

Il a pour mission la surveillance du système d'information afin de détecter toutes les activités suspectes ou malveillantes, il intervient aussi en amont pour faire de la prévention, il assurer le niveau 1 et le niveau 2 du SOC , il relève les alertes et fait un premier diagnostic et il réalise l'analyse détaillée des alertes , communique vers les équipes concernées , accompagne le traitement des incidents de sécurité et dans certains cas , il peut mettre en place des remédiations

Il interprète et traite les alertes et tickets de sécurité émises par le centre des opérations de sécurité **(**SOC**)** qui est une plateforme de surveillance, d'évaluation et de défense des systèmes d'information

L'analyste SOC joue également un rôle de prévention auprès des utilisateurs. Il veille au respect des bonnes pratiques et apporte ses conseils sur toutes les questions relatives à la sécurité.

L'activité de l'**analyste SOC** comporte une grande part de veille sur les menaces et les vulnérabilités ainsi que du reporting.

Détection des menaces:

- Identifier les événements de sécurité en temps réel, les analyser et les qualifier
- Évaluer la gravité des incidents de sécurité
- Notifier les incidents de sécurité, escalader le cas échéant **Réaction face aux menaces :**
- Transmettre les plans d'action aux entités en charge du traitement et apporter un support concernant les correctifs à mettre en œuvre
- Faire des recommandations sur les mesures immédiates
- Accompagner le traitement des incidents par les équipes d'investigation **Mise en place des usages et des outils :**
- Contribuer à la mise en place du service de détection (SIEM, etc.)
- Contribuer à la définition de la stratégie de collecte des journaux d'évènements
- Participer au développement et au maintien des règles de corrélation d'événements **Veille et amélioration :**
- Collaborer à l'amélioration continue des procédures ; construire les procédures pour les nouveaux types d'incidents
- Contribuer à la veille permanente sur les menaces, les vulnérabilités et les méthodes d'attaques afin d'enrichir les règles de corrélation d'événements **Reporting et documentation :**
- Renseigner les tableaux de bord rendant compte sur l'état de la sécurité du SI
- Maintenir à jour la documentation
- Activités de recherche de compromissions (threat hunting)

L'opérateur analyste SOC travaille de concert avec Le SOC externe chez le prestataire, , il sera très souvent en interaction directe avec les équipes DSI, les prestataires, les partenaires qui ont une connexion avec le SI UBCI

Formation / expérience professionnelle

- Formation : Bac +3, pécialisation en cybersécurité, ingénieur en Sécurité

Compétences coeur de métier

- Sécurité des systèmes d'exploitation
- Sécurité de l'AD
- Sécurité des réseaux et protocoles
- Cyberdéfense : pratique de l'analyse de journaux (systèmes ou applicatifs)
- Cyberdéfense : pratique de l'analyse de flux réseaux
- Cyberdéfense : connaissance d'outils et de méthodes de corrélation de journaux d'évènements (SIEM)
- Cyberdéfense : connaissances des solutions de supervision sécurité
- Cyberdéfense : connaissance des techniques d'attaques et d'intrusions
- Cyberdéfense : connaissances des vulnérabilités des environnements **Compétences comportementales**
- Capacité à travailler en équipe
- Capacité à communiquer
- Capacité à définir des procédures