

Analyste de Menaces Cyber

Missions et activités

- Superviser et administrer les solutions du Security Operating Center (SOC)
- Détecter, analyser et qualifier les incidents et les menaces
- Identifier leurs sources et bloquer leur accès aux solutions existantes
- Orienter les équipes techniques quant aux correctifs ou palliatifs à mettre en œuvre
- Veiller à leur application et à leur exploitabilité
- Assurer une veille permanente sur les menaces ainsi que les vulnérabilités logicielles et hardware
- Documenter les bases de connaissances et procédures de traitement
- Suivre constamment la vulnérabilité software et hardware
- Analyser les malwares

Compétences métier

Il faut de bonnes connaissances sur l'environnement IT :

- En réseaux
- En sécurité informatique (cryptographie, systèmes de codage)
- En systèmes des logiciels d'infrastructure (Systèmes d'exploitation, bases de données)
- Maitrise des systèmes Microsoft, Linux, Unix
- Maitrise des réseaux Firewall, Vlan, Routage
- Maitrise de malwares
- Connaissance du RGPD

Compétences transversales

Maîtrise de l'anglais technique (niveau B2)

Qualité rédactionnelle pour les rapports à écrire

Disponibilité et réactivité en toutes situations L'Analyste de Menaces Cyber est rattaché à la Direction des Systèmes d'Information ou directement au Directeur de la Sécurité des SI.

Compétence indispensable acquise et à acquérir :

Acquise :

Anglais technique

Qualité rédactionnelle

A acquérir :

Savoir programmer en HTML, python...

Avoir de bonnes connaissances en réseaux, en sécurité informatique et en système d'exploitation

Le BTS SIO m'apportera les connaissances nécessaires pour faire ce métier. Cependant, au vu de l'évolution de l'informatique des études supérieures, sont conseillés.

Accès au métier :

À partir d'un Bac+5 dans une école d'ingénieurs qui propose un diplôme d'ingénieur en sécurité informatique ou en systèmes et réseaux.

Perspectives d'évolution

Le domaine de l'informatique est très recherché. Les entreprises se numérisent de plus en plus et deviennent en même temps des cibles pour les menaces extérieures.

De ce fait, l'Analyste de Menaces en Cyber peut travailler pour n'importe quelle entreprise. Il a pour mission de détecter les menaces en temps réel, de les analyser, de les décortiquer et d'en anticiper les futures évolutions. Avec un bac+5 une évolution de carrière rapide est envisageable.

Pourquoi faire ce métier ?

Je souhaite travailler pour l'Armée. De ce fait ce métier me semble être un bon compromis entre l'armée et l'informatique. Notamment parce que les guerres sont maintenant informatiques et on a besoin de se protéger contre les menaces extérieures.

Alice Delachat