https://buroservicesmadagascar.fr/poste/expert-cybersecurite-microsoft-365-siem-sentinelone/

EXPERT CYBERSÉCURITÉ MICROSOFT 365 / SIEM / SENTINELONE

Organisme employeur
Buroservices Madagascar

Type de poste
Temps plein

Durée du contrat
CDI

Lieu du poste
Antananarivo, 101, Antananarivo, Analamanga, Madagascar

Date de publication
27 juillet 2026

Valide jusqu'au
30.09.2026

Description

Dans le cadre du développement des activités de l'un de nos clients, nous recrutons un **Expert Cybersécurité** afin de renforcer la sécurité de son système d'information. Vous interviendrez sur la protection des environnements Microsoft 365, le déploiement et l'administration des solutions SIEM, ainsi que la prévention, la détection et la gestion des incidents de sécurité.

Responsabilités

Au quotidien, vous serez amené(e) à :

- Administrer, configurer et faire évoluer la solution SentinelOne ainsi que la plateforme SIEM (Microsoft Sentinel ou solution équivalente)
- Assurer la supervision des événements de sécurité, qualifier les alertes et piloter les actions de réponse aux incidents
- Évaluer la sécurité des environnements Microsoft 365, identifier les risques et proposer des actions correctives pour renforcer la protection des identités et des accès
- Participer au déploiement, au paramétrage et au suivi opérationnel d'une solution MDR (Managed Detection & Response)
- Élaborer les procédures de sécurité, maintenir la documentation technique et promouvoir les bonnes pratiques auprès des équipes
- Travailler en étroite collaboration avec les équipes Infrastructure, Réseau et Support tout en assurant une veille permanente sur les nouvelles menaces et les technologies de cybersécurité

Qualifications

Nous recherchons un(e) professionnel(le) autonome, méthodique et passionné(e) par la cybersécurité, capable d'évoluer dans un environnement exigeant.

- Diplôme Bac+3 à Bac+5 en informatique, cybersécurité ou équivalent
- Minimum 3 ans d'expérience sur un poste similaire
- Excellente maîtrise des solutions Microsoft Security (Microsoft Defender, Entra ID, Intune) ainsi que des outils SIEM, EDR et MDR, notamment Microsoft Sentinel et SentinelOne
- Bonne connaissance des mécanismes de détection des menaces, de l'analyse de journaux, de la gestion des incidents et du renforcement de la sécurité des systèmes
- Esprit d'analyse, sens de l'organisation, autonomie et aptitude à résoudre des problématiques complexes
- Discrétion, sens des responsabilités et bonnes qualités relationnelles pour travailler en équipe
- Les certifications Microsoft (AZ-500, SC-200, SC-300, SC-900) et/ou **CompTIA Security+** seront fortement appréciées.