



<https://latribunelibre.com/emploi/consultante-iam-f-h>

Consultant(e) IAM F/H

Description

Rejoignez l'équipe de Maguen Cyber

Maguen Cyber est né de la volonté d'un accompagnement innovant et adapté en cybersécurité en fonction des besoins de nos clients. Maguen Cyber se positionne en tant que pure-Player cybersécurité avec une couverture internationale et nous avons l'ambition de s'imposer comme une référence du secteur, avec vous à nos côtés.

Nous recherchons un(e) Consultant(e) IAM pour une opportunité de mission de longue durée à pourvoir chez l'un de nos clients situés en Ile-de-France.

Contexte de la mission:

Notre client recherche des experts en solutions Broadcom SiteMinder et gestion d'annuaires LDAP. L'équipe, dédiée à la gestion des identités et des accès, soutient l'authentification et l'autorisation pour les clients internes et externes. En utilisant des cadres standardisés, elle gère les politiques d'accès et déploie des technologies pour garantir un accès approprié aux ressources. Le poste implique de travailler au sein d'une équipe pluridisciplinaire répartie sur 3 régions et 6 sites, avec pour missions :

- Architecture
- Livraison de projets
- Support et maintenance des plateformes SSO et gestion des identités
- Gestion des incidents, problèmes et changements.

Détail de la mission:

Architecture :

- Fournir une expertise pour favoriser l'amélioration des technologies et des processus.
- Contribuer au développement des roadmaps pour SSO et LDAP.
- Collaborer aux revues architecturales avec les équipes d'architecture.

Organisme employeur

AMD Blue

Type de poste

Temps plein

Secteur

CONSEIL EN SYSTÈMES ET LOGICIELS INFORMATIQUES

Lieu du poste

75112, PARIS 12, PARIS, France

Date de publication

24 septembre 2024 à 11:02

Valide jusqu'au

24.10.2024

- Suivre les nouvelles technologies et tendances.
- Automatiser les processus pour accélérer les délais de livraison.

Livraison de projets :

- Assurer la livraison de projets clés autour du SSO et LDAP.
- Collaborer avec les chefs de projet pour concevoir et implémenter de nouvelles fonctionnalités. • Travailler avec les développeurs pour diagnostiquer les problèmes récurrents.
- Apporter une expertise SSO et gestion des identités aux équipes de développement.
- Promouvoir l'amélioration des processus et technologies pour les services d'authentification.

Support et maintenance de la plateforme :

- Surveiller et améliorer la performance des environnements de production.
- Gérer proactivement la capacité des applications en production.

Gestion des incidents et des problèmes :

- Analyser les incidents critiques avec les équipes partenaires.
- Proposer des améliorations pour réduire les incidents récurrents sur SSO et LDAP.

Gestion des changements :

- S'assurer que les changements en production sont planifiés et contrôlés.
- Garantir la qualité technique et la planification des changements sur les environnements SSO et gestion des identités.
- Participer activement aux réunions de gestion des changements et des problèmes.

Étant donné qu'il s'agit d'un rôle de support en production, axé sur une gamme de technologies différentes et souvent innovantes, les candidats doivent avoir l'aptitude et le désir d'apprendre. De plus, la capacité d'être d'astreinte et de fournir du support en dehors des heures normales est essentielle.

Qualifications

- Diplômé(e) d'une école d'ingénieur ou titulaire d'un master en sécurité.
- Expérience d'au moins 11 ans en cybersécurité.
- Bon niveau d'anglais.

Compétences techniques essentielles :

- Expertise en administration, support, définition et documentation.
- Maîtrise de Python.
- Connaissance approfondie des middleware comme Microsoft IIS, Apache Tomcat, et Apache HTTP Server.
- Expertise en sécurité avec CA SiteMinder.
- Maîtrise de la gestion de processus selon ITIL.
- Compétence en réseaux et protocoles, notamment LDAP et API REST.

Compétences non techniques : • Solides capacités analytiques et grande attention aux détails.

- Approche structurée et méthodique, capable de travailler sous une direction IT exigeante.
- Attitude proactive, voyant les changements comme des opportunités d'amélioration.
- Esprit d'équipe et excellentes compétences interpersonnelles et de communication.