Titre de la prestation

Sécurité Cloud Public CSRO AWS

Cadre, contexte, objectifs de la prestation:

Le département Risques opérationnels et Sécurité (RESG/XXX/XXX), dirigé par le Responsable Sécurité des Systèmes d'Information (RSSI) de RESG/XXX, pilote les initiatives et le suivi de la sécurité et des risques opérationnels à travers RESG/XXX sous la supervision fonctionnelle du RSSI et de l'ORM SI du Groupe.
RESG: Direction des Ressources du Group, qui regroupe les Systèmes d'information, les infrastructures techniques, les achats et l'immobilier d'exploitation.
ORM: Object/Relational Mapping

Le service RESG/XXX/XXX/XXX a en charge de la sécurité des environnements Cloud (public/privé) ainsi que celle de la plate-forme ; à ce titre il :
• Prend en charge le volet sécurité du Programme Cloud (à travers de multiples projets de mise en oeuvre)
• Spécifie les principes et directives de sécurité applicables à la plate-forme
• Gère la définition des modalités d'intégration de la sécurité en mode Agile
• Assiste les entités dans la prise en compte de la sécurité au sein de leurs projets et initiatives liés au Cloud ou à l'automation.

A ce titre, le Bénéficiaire souhaite bénéficier de l'expertise du Prestataire en termes d'Expertise technique et/ou fonctionnelle.

Dans ce cadre la Prestation consiste à contribuer à/au(x):

L'entité Cloud Center Of Excellence du service Go To Cloud, qui est en charge de la mise à disposition des composants d'infrastructure Cloud Public, la mission consiste en la fourniture d'une expertises sécurité sur le périmètre AWS. (Expertise complémentaire AZURE et/ou GOOGLE).
- Assistance d'entité de développements (Python, PowerShell...) en mode Agile/DevOps (Chaines CI/CD, Ansible, JIRA, GIT...)
PowerShell: Microsoft framework for task automation and configuration management, consisting of a command-line shell and scripting langage.
DevOps: C'est une pratique technique visant à l'unification du développement logiciel et de l'administration des infrastructure informatiques. Les principes soutiennent des cycles de développement plus courts, une augmentation de la fréquence des déploiements et des livraisons continues, pour une une meilleure atteinte des objectifs économiques de l'entreprise. Le développement, l'intégration, les tests, la livraison, le déploiement, l'exploitation de la maintenance des infrastructures.
CI/CD: Continuous integration et Continous delivery, pour le génie logiciel.

Les livrables sont :
• Assistance sécurité à l'implémentation des applications au sein des environnements Cloud Public AZURE / AWS :
- Livrables documentaires sécurité (dossiers de sécurité, blueprint, Dossiers d'analyse des risques et d'identification des mitigations/contre-mesures associées...)
- Dossiers de consolidation des exigences et spécifications sécurité en déclinaisons des User-Stories

- Revue sécurité des codes des composants développés
- Chapitre sécurité des livrables documentaires propres aux composants d'infrastructures développés (DAT, DAH, LLD, HLD...)
- Supports de communication des moyens à des fins de restitution (management, projet...)
- Spécification des contrôles de supervision au sein des environnements techniques des CSP (AWS, AZURE...) en vue de leur automatisation au sein des frameworks de contrôle
• Préparation/conduite/remédiation des audits et pentests sur les environnements Cloud Public déployés
• Assistance ponctuelle à la remédiation des incidents de sécurité sur les environnements opérés
• échange d'expertises / lean formation sécurité
• Planning des actions nécessaires aux projets dans le respect des objectifs et délais annoncés
• Reporting périodique sur les activités conduites.

LLD: Low-level Design
HLD: High-level Design
DAA: Dossiers d'Architecture Applicative
DAH: Dossiers d'Architecture Hébergement
DAT: Dossiers d'Architecture Technique
CSP: Cloud Service Provider

Autres informations:
- Expertises techniques requises sur les domaines liés aux environnements Cloud AWS (AZURE et/ou GOOGLE)
- concepts liés à la sécurité de l'information et aux analyses des risques, des expertises/certifications sur les normes ISO (27001, 27002, 27005, 27018), EBiOS et SOC (1-2-3)
- Environnement anglophone.

Compétences techniques attendues:
- Environnement Cloud Public AWS
- Idéalement : environnement Cloud Public AZURE / GOOGLE
- **Solutions CWPP (CloudCustodian, Prowler...)**
- Python / BOTO 3
- JIRA
- SOAP, REST
- Git
- Ansible

BOTO3: AWS SDK (software development kit) for python
JIRA: Système de suivi de bugs / Système de gestion d'incidents
SOAP: Simple Object Access Protocol, a messaging protocol between webservice requester and webservice provider.
REST: Representational State Transfer, a software architectural style that defines a set of constraints for creating webservices.
Ansible : a plateforme libre pour la configuration et la gestion des ordinateurs.

Ce qu'il faut retenir:

On recherche des consultants sécurité Cloud Public AWS, la double compétences est nécessaire! Sécurité + Cloud.

Mission longue d’accompagnement des features teams de la SG.

Anglais: impératif

Que du temps complet, pas de temps partiel.