UNIVERSITÉ DE LA RÉUNION

FICHE DE POSTE

Fonctions : INGENIEUR EN CYBERSECURITE OPERATIONNELLE

Métier ou emploi type : Administrateur-trice des systèmes d'information (E2A41)
*REME, REFERENS, BIBLIOFIL

Fiche descriptive du poste

Catégorie : IGE

Affectation

Administrative : **Université de La Réunion – 15 avenue René Cassin – 97744 SAINT DENIS**

Géographique : **CAMPUS DU MOUFIA**

Direction : **Direction des Systèmes d'Information et du Numérique**

Missions

INGENIEUR EN CYBERSECURITE OPERATIONNELLE

Intégré au sein de la Direction des Systèmes d'Information et du Numérique (DSIN), l'ingénieur en cybersécurité opérationnelle a pour mission principale de piloter le durcissement des systèmes, la remédiation des vulnérabilités et le suivi des indicateurs de sécurité. Au cœur des équipes techniques, en lien fonctionnel avec le RSSI, son périmètre englobe l'exploitation des mécanismes de défense de l'établissement et la mise en conformité de l'Université de La Réunion à travers sa participation active aux projets informatiques transversaux.

ACTIVITÉS PRINCIPALES:

1. Supervision opérationnelle et gestion des mécanismes de défense (SecOps)

- **Exploitation de la sécurité au quotidien :** Administrer et suivre au premier niveau les alertes issues des solutions de détection et de réponse de l'établissement (ex : EDR).
- **Réponse aux incidents :** Coordonner et apporter une expertise technique de niveau 2/3 aux équipes de la DSIN lors de la levée de doutes ou de la remédiation d'incidents de sécurité.
- **Suivi de la performance :** Concevoir, renseigner et suivre les indicateurs clés de performance (KPI) et de pilotage de la sécurité opérationnelle
- **Supervision de la sécurité des identités :** Surveiller, analyser et traiter de manière unifiée les événements et alertes de sécurité critiques liés à l'annuaire central Active Directory, Microsoft Entra ID et 365, afin de détecter et de remédier aux menaces
- **Gestion de la centralisation des logs (SIEM) :** Piloter le cycle de vie de la solution de gestion des événements de sécurité de l'établissement, depuis son intégration technique par le raccordement des sources de données de la DSIN jusqu'à son exploitation opérationnelle

2. Maintien en Condition de Sécurité (MCS) et gestion des vulnérabilités

- **Gestion du Patch Management :** Coordonner avec les administrateurs systèmes et réseaux, le suivi du patching des serveurs et des postes de travail
- **Audits techniques et réduction de la surface d'attaque :** Planifier et réaliser des scans de vulnérabilités réguliers sur les actifs du SI, analyser l'empreinte numérique exposée (OSINT) et documenter les plans d'action correctifs
- **Hygiène informatique :** Veiller au respect des bonnes pratiques d'administration,

notamment la gestion des comptes à privilèges, l'activation du MFA et les revues régulières des droits d'accès

- **Durcissement de l'environnement Windows et Active Directory :** Piloter la mise en œuvre des recommandations de sécurité de l'ANSSI concernant l'annuaire, notamment la mise en place d'un modèle d'administration en couches ou Tiering, la restriction des protocoles obsolètes et la sécurisation des relations de confiance.

3. Gouvernance technique et conformité (relai PSSI / NIS 2)

- **Homogénéisation des règles :** Collaborer avec les responsables de site et les ingénieurs centraux pour harmoniser et durcir les règles de filtrage réseau (firewalls d'interconnexion, pare-feu de sortie de site) et veiller au bon cloisonnement des VLANs de bout en bout.
- **Déclinaison de la PSSI :** Traduire les orientations stratégiques et la politique de sécurité des systèmes d'information définies par le RSSI en fiches réflexes, procédures techniques et standards de configuration applicables par les équipes de la DSIN pour l'ensemble des environnements sur site et Cloud.
- **Contrôle de conformité :** Vérifier de manière continue l'alignement des pratiques de la DSIN avec les exigences réglementaires nationales et européennes (Directive NIS 2, ANSSI, RGPD, RGS).
- **Audits réguliers de l'AD :** Réaliser des audits de sécurité récurrents de l'annuaire à l'aide d'outils spécialisés (ex: PingCastle, BloodHound) afin d'identifier et de remédier aux chemins d'attaque, comptes dormants, mots de passe faibles ou GPOs mal configurées.
- **Interface et remontée des besoins du terrain :** Agir comme un relai d'information au cœur de la DSIN en identifiant, en centralisant et en remontant de manière proactive au RSSI les besoins opérationnels, les contraintes techniques et les réalités concrètes constatées par les équipes informatiques.

4. Cyber Threat Intelligence (CTI) et amélioration continue

- **Veille et gestion des alertes externes :** Assurer une veille active sur les menaces émergentes, suivre les bulletins des centres d'alerte nationaux (CERT-FR, ANSSI) et identifier de manière proactive les actifs de l'Université concernés par ces failles.
- **Amélioration continue :** Proposer des évolutions d'architecture ou des durcissements de configuration pour adapter continuellement les barrières de défense de l'Université face à l'évolution des modes opératoires d'attaque.
- **Promotion de la culture cyber :** Assurer la diffusion et la promotion des fiches de cyberculture du site institutionnel cyber.univ-reunion.fr afin de valoriser les bonnes pratiques de sécurité auprès des équipes informatiques et des agents de l'établissement.

Conditions particulières d'exercice :

Niveau d'étude : BAC + 5 avec spécialisation cybersécurité
Contrainte d'horaires décalés en cas de gestion de crise / nécessité de service
Permis de conduire B (VL) indispensable
Certifications professionnelles en cybersécurité souhaitées (ex : Tryhackme, Hackthebox)

Encadrement : Non ~~- Oui~~

Conduite de projet : ~~Non~~ – Oui

Compétences*

Connaissances et savoirs thématiques :

- Architecture, environnement technique et sécurité approfondie du système d'information
- Méthodologie de conduite de projet informatique et transverse
- Normes, référentiels et réglementations en cybersécurité, notamment la Directive NIS 2, le RGPD, les recommandations de l'ANSSI et l'ISO 27001
- Technologies des environnements Windows Server, Active Directory ainsi que les architectures hybrides Microsoft Entra ID et Office 365
- Protocoles réseaux, architectures de filtrage et fonctionnement des mécanismes de détection de type EDR et SIEM
- Langages de programmation et de scripting pour l'automatisation (ex : Python, Bash, PowerShell)
- Anglais technique de niveau général pour la lecture des documentations et des bulletins d'alerte

Savoir-faire opérationnels :

- Utiliser les outils de diagnostic, de cartographie et d'audit de sécurité (ex : PingCastle, BloodHound ou OpenVAS)
- Appliquer rigoureusement les règles de sécurité informatique, les standards de durcissement et les normes de conformité de l'établissement
- Analyser des fichiers de logs et corréler des événements de sécurité pour identifier les signaux faibles
- Documenter de manière claire les vulnérabilités identifiées et formaliser des plans d'action correctifs ou de remédiation
- Coordonner et suivre le déploiement des correctifs de sécurité sur les serveurs et les postes de travail en lien avec les équipes techniques

Savoir être:

- Autonomie, rigueur et fort sens de la confidentialité dans la manipulation des données de sécurité.
- Esprit d'analyse, de synthèse et pragmatisme face aux contraintes de production des équipes informatiques.
- Pédagogie, diplomatie et sens du collectif pour assurer un rôle de facilitateur auprès des administrateurs et des techniciens du terrain.
- Réactivité, maîtrise de soi et sang-froid lors de la gestion des alertes critiques ou des situations d'incident cyber.

Outils/Connaissances spécifiques:

- Outils d'audit de sécurité (ex : OpenVAS, Pingcastle)
- Outils de tests d'intrusion (ex : Metasploit)
- Systèmes d'exploitation (Windows, Linux, Mac OS)
- Réseaux et protocoles de sécurité