UNIL | Université de Lausanne

CAHIER DES CHARGES

1. Actualisation :			
Etabli le : 23.01.2024	Par :	Roberto Fabbretti	Remplace la version du :
Motif d'actualisation : Nouveau poste			

2. Identification du poste			
Direction / Faculté	Direction	Département/Service/ Institut/Section	Centre informatique/DCSR/Pôle infrastructure de recherche
N° de poste		Intitulé du poste dans l'entité	Ingénieur opérationnel en sécurité de l'information
N° de validation SRH	0224059	Libellé emploi type – n°	Administrateur-trice d'outils / de systèmes / réseaux – télécoms - 106
Chaîne	314	Niveau	11

3. Descriptif et missions générales du poste

3.1 But du poste

Sous la responsabilité du responsable de la DCSR, le poste vient renforcer les activités du security operation center (SOC) du Centre informatique (CI). Il a pour but de garantir la sécurité des données collectées par différents groupes de recherche.

3.2 Missions générales

1.	Assurer un degré de support sécurité IT conforme aux SLA de l'UNIL
2.	Assurer l'Administration, l'Exploitation et les Maintenances adaptées à la sécurité IT de l'UNIL
3.	Participer au traitement des incidents de sécurité.
4.	Mettre en œuvre les normes de sécurité en termes de sécurité IT
5.	Participer aux formations à propos de la sensibilisation à la sécurité

4. Conduite : ETP directement subordonné-s : ☐ Cf. Organigramme

☒ Non
☐ Oui :

5. Mode de remplacement prévu, en cas d'absence du titulaire :

☒ Non
☐ Oui :

UNIL | Université de Lausanne

6. Mission et activités :	Temps moyen en %
1. Assurer un degré de support sécurité IT conforme aux SLA de l'UNIL	20
○ Mettre en place des outils de surveillance pour détecter les activités suspectes ou les violations de sécurité.	
○ Analyser les journaux d'événements et les alertes de sécurité pour identifier les menaces potentielles.	
○ Effectuer des audits réguliers des systèmes et des activités liées à la sécurité.	
○ Mettre en œuvre des mécanismes de contrôle d'accès pour restreindre l'accès aux ressources sensibles.	
2. Assurer l'Administration, l'Exploitation et les Maintenances adaptées à la sécurité IT de l'UNIL	30
○ S'assurer que tous les systèmes, logiciels et applications sont régulièrement mis à jour avec les derniers correctifs de sécurité.	
○ Planifier et effectuer des mises à jour de manière régulière tout en respectant les SLA.	
○ Effectuer des analyses de vulnérabilités pour identifier les faiblesses potentielles du système.	
○ Mettre en œuvre des mesures correctives pour remédier aux vulnérabilités détectées.	
3. Participer au traitement des incidents de sécurité.	20
○ Analyser et investiguer les événements de sécurité. Effectuer des analyses informatiques pour identifier les vecteurs d'entrée et la portée de l'attaque. Récupérer les indicateurs de compromission (IOC) qui seront utilisés pour la détection de toute activité malveillante.	
○ Effectuer l'analyse OSINT et placer le contexte afin d'établir le profil de menace et de risque.	
○ Rédiger des rapports techniques d'analyse et d'investigation.	
4. Mettre en œuvre les normes de sécurité en termes de sécurité IT	10
○ Participer à la configuration, à la surveillance et à la maintenance des dispositifs de sécurité tels que les pare-feu, les systèmes de détection d'intrusion, Web Application Firewall, etc.	
○ Participer à la mise en conformité des dispositifs de sécurité aux normes et politiques établies.	
5. Participer aux formations à propos de la sensibilisation à la sécurité	20
○ Participer à l'organisation des sessions de formation et de sensibilisation à la sécurité pour le personnel et les utilisateurs.	
○ Diffuser des informations sur les meilleures pratiques en matière de sécurité informatique.	

7. Eventuelles responsabilités particulières attribuées au titulaire :

UNIL | Université de Lausanne

8. Exigences requises :

8.1 Formation de base

Titre	
Master en informatique ou en systèmes de communication, niveau EPF ou HES ou titre jugé équivalent	☒ Exigé ☐ Souhaité

8.2 Formation complémentaire

Titre	

8.3 Expériences professionnelles

Domaine	Nombre d'années
Ingénierie dans les domaines de la sécurité opérationnelle de l'information	0 à 2

8.4 Connaissances et capacités particulières

Domaine	
Linux Redhat et/ou Debian. Renforcement de la sécurité de l'OS, Python et/ou POwershell, Ansible	☒ Exigé ☐ Souhaité
Bonnes connaissances des couches réseau	☒ Exigé ☐ Souhaité
Anglais B2 ou plus écrit et oral	☒ Exigé ☐ Souhaité
Notions de gestion VMWare ESX, Vpshere et Kubernetes	☐ Exigé ☒ Souhaité
Sécurisation des services Web (NGINX / Apache mod_security)s	☐ Exigé ☒ Souhaité
Gestion des pare-feux Palo Alto / Fortinet	☐ Exigé ☒ Souhaité

9. Astreintes particulières *(travail de nuit, service de piquet, etc...)* :

Peut être amené à intervenir hors des heures de bureau lors de déploiements ou de pannes.

10. Signatures :

UNIL | Université de Lausanne

Le/la titulaire atteste avoir pris connaissance du présent cahier des charges.		
Date :	Nom et prénom :	Signature :
Le/la supérieur/e hiérarchique.		
Date :	Nom et prénom :	Signature :
Le/la représentant/e de l'autorité d'engagement. (décanat, chef-fe de service ou direction).		
Date :	Nom et prénom :	Signature :