



DÉPARTEMENT
Finistère
Penn-ar-Bed

Technicien Sécurité du Système d'Information

Direction des Systèmes d'Information et des Relations Humaines

Service : Système, Réseau et Téléphonie

Fiche de poste n° 535

Caractéristiques du poste :

Conditions d'accès	
Métier : technicien poste de travail support et sécurité	Diplôme ou équivalence : Bac +2
Filière(s) concernée(s) : Technique	Cadre d'emploi : B
Emploi repère : Technicien du système d'information	Grade : Technicien, Technicien principal
Encadrement : <input type="checkbox"/> oui <input checked="" type="checkbox"/> non Nombre de personnes à encadrer :	Encadrant de direction <input type="checkbox"/> Encadrant de service <input type="checkbox"/> Encadrant de proximité <input type="checkbox"/>
NBI : <input type="checkbox"/> oui <input checked="" type="checkbox"/> non (nombre points + rubrique)	Nombre de point :
Localisation administrative et géographique	
Adresse de la direction : 10 rue le Déan	
Lieu d'affectation de l'agent : Quimper	Résidence administrative du poste : Quimper

Descriptif du poste :

Sous l'autorité du Responsable de l'unité Sécurité, le poste de Technicien Sécurité du Système d'Information assure l'administration quotidienne et l'évolution de la sécurité du système d'information dans le respect des plannings et de la qualité attendue.

Il fait partie de l'équipe technique qui a en charge le volet SecOps, afin de surveiller le paysage numérique de l'Organisation à la recherche de signes d'activité malveillante de rechercher de manière proactive les événements anormaux sur les réseaux, les points de terminaison, les applications, tout en se préparant si possible à atténuer les cybermenaces potentielles ou évidentes.

Dans un contexte de forte évolution des technologies IT, de montée en croissance du cloud et de l'enjeu de sécurité informatique, le technicien est un technicien informatique confirmé qui a une solide expérience sur les technologies de sécurité et ayant une appétence pour le domaine de la sécurité informatique. Le technicien travaille au sein d'un binôme technicien du domaine d'expertise de la sécurité du SI en lien avec un ingénieur gérant en complément les projets.

Le technicien assure l'administration courante, l'évolution et le maintien en condition opérationnelle des infrastructures de sécurité, incluant les environnements de pare-feu, de reverse-proxy et de passerelles diverses (sécurité de la messagerie, maintien en condition de sécurité des serveurs, ...).

Il participe à la définition des politiques de sécurité et assure l'administration avancée des technologies qui lui sont confiées.

Il assure la prise en charge et le traitement jusqu'à la clôture des tickets d'assistance et de demandes de niveau 2 dans le domaine des infrastructures de sécurité, en apportant son expertise technique pour le diagnostic et la résolution des dysfonctionnements.

Missions :	Activités :
Administration avancée de la sécurité du SI interne	<ul style="list-style-type: none"> - Participer à la définition de la politique de sécurité - Relever et alerter des manquements à la politique de sécurité - Mettre en œuvre les décisions prises dans l'équipes ou par la hiérarchie - Administrer et exploiter quotidiennement les solutions impactant la sécurité telles que Pare-feu, Proxy, WAF, SOC, ou autres ... - Participer aux évolutions des infrastructures de sécurité et les maintenir au maximum à jour - Participer à la définition des politiques de sécurisation des environnements serveurs de type Windows et Linux et contrôler leurs applications - Assurer la traçabilité de toutes les actions entreprises - Suivre les évolutions technologiques et proposer des évolutions - S'intégrer au maximum à la vie du pôle technique informatique en respectant les règles et procédures existantes au sein de l'équipe
Administration avancée de la sécurité du SI externe (Cloud, MS365)	<ul style="list-style-type: none"> - Définir et appliquer la politique de sécurité sur MS365 - Administrer et exploiter quotidiennement la sécurité sur l'environnement MS365 - Être contributeur pour la gestion globale de l'environnement MS365
Réalisation du volet SecOps de l'organisation	<ul style="list-style-type: none"> - Surveiller les systèmes via les outils de sécurité disponibles (consoles d'administration, supervision, messagerie, ...) - Détecter et qualifier les alertes de sécurité - Intervenir en première analyse sur les incidents (analyse de logs, remontée d'alertes) - Participer activement à la gestion de tout incident de sécurité et contribuer au mieux à la fourniture d'information au sein de l'équipe en vue de l'alimentation vers la cellule de crise - Escalader et documenter les incidents vers les équipes de niveau supérieur ou le RSSI - Participer à l'élaboration des retours d'expérience (REX) après incident
Participation aux projets d'évolution du SI	<ul style="list-style-type: none"> - Apporter une expertise sécurité dans les projets d'infrastructure (réseau, cloud, applications) - Contribuer aux phases de tests et validation sécurité avant mise en production - Documenter les procédures de déploiement et d'exploitation sécurisée - Suivre et appliquer les recommandations des audits externes ou internes
Support niveau 2 des infrastructures de sécurité	<ul style="list-style-type: none"> - Respecter les règles définies au sein du Pôle technique pour le bon fonctionnement du centre de services - Prendre son tour au Quart sécurité et prendre en compte les tickets dirigés vers l'unité Sécurité - Prendre en charge les tickets et leur cycle de vie jusqu'à leur clôture en s'appuyant fortement sur l'outil de ticketing GLPI - Participer activement au groupe de résolution de l'unité Sécurité et suivre les décisions du groupe
Sensibilisation et accompagnement des utilisateurs	<ul style="list-style-type: none"> - Participer à la sensibilisation des utilisateurs aux bonnes pratiques de cybersécurité - Diffuser des guides ou supports pédagogiques (phishing, mots de passe, mobilité) - Accompagner les équipes métiers dans l'adoption sécurisée des outils numériques - Participer aux campagnes internes de tests de sécurité (simulations phishing)
Administration courante	<ul style="list-style-type: none"> - Assurer une veille technologique - Assurer une veille régulière des vulnérabilités - Rédiger et maintenir de la documentation technique
Gestion des datacenters	<ul style="list-style-type: none"> - Suivre les remontées d'alarmes et les prendre en compte en cas de risques pour le SI - Respecter les règles définies au sein du pôle technique

Santé sécurité au travail

Chaque agent doit prendre soin de sa santé et veiller à sa sécurité et celle des autres personnes présentes sur le lieu de travail. Il doit respecter les instructions et consignes fixées par son responsable.

Compétences :

Niveau requis à la prise de poste*	Niveau attendu*
------------------------------------	-----------------

Savoir faire (compétences métier)		Niveau :	Niveau :
	• Connaissances des réseaux TCP/IP	Niveau : 2	Niveau : 3
	• Connaissances des procédures, normes et standards de sécurité	Niveau : 3	Niveau : 4
	• Avoir pleine conscience de l'importance de la sécurisation du SI	Niveau : 3	Niveau : 4
	• Bonne sensibilisation des règles et aspects légaux qui s'appliquent au SI (Charte informatique, CNIL)	Niveau : 2	Niveau : 3
	• Maîtriser les outils de sécurité de type Firewall, Proxy, SOC, WAF, ...	Niveau : 3	Niveau : 4
	• Connaissances des infrastructures de type AD, DHCP, DNS, DFS, EXCHANGE, ...	Niveau : 2	Niveau : 3
	• Connaissances du fonctionnement des différents matériels (serveurs et terminaux) et la façon dont ils sont intégrés dans le SI de la collectivité	Niveau : 2	Niveau : 4
	• Connaissances de l'environnement MS365	Niveau : 2	Niveau : 3
	• Connaissances du système d'exploitation Windows	Niveau : 3	Niveau : 3
	• Connaissances du système d'exploitation Linux	Niveau : 3	Niveau : 4
	• Connaissances des scripting (Powershell, batch)	Niveau : 3	Niveau : 3
	• Savoir élaborer des documentations techniques et des supports utilisateurs	Niveau : 2	Niveau : 3
	• Savoir prendre en compte les priorités du service	Niveau : 3	Niveau : 3
	• Savoir anticiper les risques et proposer des plans d'actions	Niveau : 3	Niveau : 4
	• Savoir assurer la traçabilité de ses actions	Niveau : 3	Niveau : 4
	• Connaître le fonctionnement de la collectivité et de ses services pour les accompagner	Niveau : 2	Niveau : 2
	• Connaître les politiques d'équipement en vigueur dans la collectivité	Niveau : 2	Niveau : 2
• Anglais technique	Niveau : 2	Niveau : 3	

Savoir être (compétences comportementales)	• <i>Etre soucieux de la satisfaction de l'utilisateur</i>	Niveau : 2	Niveau : 4
	• <i>Respecter les consignes et les procédures établies</i>	Niveau : 2	Niveau : 4
	• <i>Respecter les plannings et la qualité attendue</i>	Niveau : 2	Niveau : 4
	• <i>Savoir travailler en équipe</i>	Niveau : 2	Niveau : 4
	• <i>Savoir faire preuve d'écoute et de pédagogie</i>	Niveau : 2	Niveau : 4
	• <i>Savoir gérer des situations d'urgence, les situations de stress et la tension mentale</i>	Niveau : 3	Niveau : 4
	• <i>Savoir rendre compte, partager des informations, faire un rapport des incidents</i>	Niveau : 2	Niveau : 3
	• <i>Faire preuve de qualités relationnelles et savoir s'adapter au niveau de son interlocuteur</i>	Niveau : 3	Niveau : 4
	• <i>Etre réactif et disponible</i>	Niveau : 1	Niveau : 3
	• <i>Posséder des qualités rédactionnelles</i>	Niveau : 2	Niveau : 3
	• <i>Savoir s'adapter aux technologies nouvelles</i>	Niveau : 2	Niveau : 4
	• <i>Etre force de proposition dans l'évolution des pratiques et outils de son domaine de compétence</i>	Niveau : 2	Niveau : 3
	• <i>Etre rigoureux et méthodique</i>	Niveau : 2	Niveau : 3
	• <i>Savoir être polyvalent</i>	Niveau : 2	Niveau : 3
	• <i>Faire preuve d'initiative</i>	Niveau : 2	Niveau : 3
• <i>Etre autonome</i>	Niveau : 2	Niveau : 3	

Niveau 1 Notions/Débutant	Niveau 2 Travail en semi autonomie/Qualifié	Niveau 3 Maîtrise	Niveau 4 Expertise
-------------------------------------	--	-----------------------------	------------------------------

Conditions d'exercice :

Moyens mis à disposition : (préciser les spécificités liées au poste)	Ordinateur, imprimante, photocopieur, téléphone Dotation EPI / VT : <input type="checkbox"/> oui <input checked="" type="checkbox"/> non
Exigences du poste :	Déplacements locaux, régionaux et nationaux
Environnement lié au poste de travail	Bureau partagé. Le poste est assujéti à des interventions en heures non ouvrées, à titre exceptionnel
Télétravail	<input checked="" type="checkbox"/> oui selon les nécessités de service <input type="checkbox"/> non

Pour rappel :

- *La fiche de poste est susceptible d'évoluer*
- *Tout agent est soumis à des droits et obligations (sens du service public, esprit d'équipe, professionnalisme, capacité d'adaptation, devoir de réserve)*