MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES
Liberté
Égalité
Fraternité

Fonction principale : Auditeur sécurité des systèmes d?information

ANALYSTE CYBERSECURITE – REPONSE AUX INCIDENTS DE SECURITE

Emploi-type principal :	**CHARGÉ OU CHARGÉE DE CYBERDÉFENSE**
Domaine d'activité :	NUMÉRIQUE ET SYSTÈMES D'INFORMATION ET DE COMMUNICATION
Code Emploi-type NOMADE :	NSIC-06
Emploi-référence interministériel :	FP2SIC20 CHARGEE /CHARGE DE CYBERDEFENSE
Domaine fonctionnel interministériel :	NUMERIQUE ET SYSTEMES D'INFORMATION ET DE COMMUNICATION

Affectation :	DNUM - Mission Infrastructure, Exploitation et Sécurité - Bureau COSAE
Lieu de travail :	DNUM - Mission Infrastructure, Exploitation et Sécurité - Bureau COSAE - Secteur COS Site Quai d'Orsay, 37 Quai d'Orsay, Paris 7e
Numéro du poste de travail :	0003007561

Emploi(s)-type de rattachement	Domaine(s) d'activité	Pourcentage
Chargé ou chargée de cyberdéfense	Numérique et systèmes d'information et de communication	100

Description synthétique du poste

Au sein du secteur Conduite des Opérations de Sécurité (COS) du COSAE, l'analyste réponse aux incidents de sécurité intervient en cas de soupçons sur une activité malveillante ou d'attaque au sein du système d'information, Il analyse les symptômes et réalise les analyses techniques sur le système d'information. Il identifie le mode opératoire de l'attaquant et qualifie l'étendue de la compromission. Il fournit des recommandations de remédiation pour assurer l'assainissement et le durcissement des systèmes attaqués.

Composition de l'équipe de travail

Equipe constituée de 5 personnes

Activités principales

Sous l'autorité du chef de secteur, vous aurez pour missions principales :

Anticipation :
• Réaliser une veille sur les nouvelles vulnérabilités, sur les nouvelles technologies et sur les méthodes des attaques relatives aux différents composants du système d'information
• Alimenter les bases de renseignement sur les menaces (threat intelligence)
• Maintenir et développer des outils d'investigation

Analyse des incidents :
• Collecter les informations techniques d'un large ensemble de systèmes d'information, réaliser la recherche d'indicateurs de compromission
• Analyser les relevés techniques réalisés afin d'identifier le mode opératoire et l'objectif de l'attaquant et de qualifier l'étendue de la compromission
• Rédiger des rapports d'investigation

Conseil :
• Préconiser des mesures de contournement et de remédiation de l'incident (assainissement et durcissement)
• Préconiser des mesures d'amélioration des capacités d'analyse (extraction des indicateurs de compromission)
• Préparer des rapports

Environnement professionnel

Travail en espace sécurisé
Soumis à habilitation

Liaisons fonctionnelles

Conditions particulières d'exercice

Non adapté à un temps partiel
Formation possible

Durée d'affectation attendue

Détachement sur contrat ou contrat à durée déterminée jusqu'au 31 août 2025, renouvelable.

Profil statutaire du poste

- A

Agent titulaire de la fonction publique de catégorie A ou agent contractuel.

Rémunération : selon expérience et qualifications, dans une fourchette allant de 44 220 à 66 000 euros annuels bruts.

Groupe de prime
Groupe 4 - Catégorie A

Contacts
Courriel : emplois.rh-3@diplomatie.gouv.fr (uniquement pour rapporter une difficulté technique). Seules les candidatures reçues à travers l'application Transparence seront prises en considération par la DRH. Aucune candidature reçue par courriel ne pourra être traitée. Les candidats sont priés de remplir intégralement et précisément le formulaire de candidature (en particulier « DIPLÔMES » et « EXPÉRIENCE PROFESSIONNELLE » qui détermineront le niveau de rémunération qui pourra être proposé).

Compétences

Légende :

Facultatif	Débutant	Pratique	Maîtrise	Expert
☐☐☐☐	■☐☐☐	■■☐☐	■■■☐	■■■■

Connaissance		*Requise*
Applications et techniques de surveillance	■■■☐	
Méthodologies d'identification et de gestion des risques et des aléas	■■■☐	
Normes de sécurité informatique	■■☐☐	
Techniques de cyber-attaques et contre-mesures pour les prévenir	■■■☐	
Savoir-faire		*Requise*
Alerter sur une situation à risque	■■■☐	
Analyser un risque	■■■☐	
Diagnostiquer	■■■☐	
Gérer une situation de crise, d'urgence ou dangereuse	■■☐☐	
Rédiger	■■☐☐	
Savoir-être		*Requise*
Esprit d'initiative	■■■☐	
Etre rigoureux	■■■☐	
Faire preuve de discrétion	■■■☐	
Réactivité	■■■☐	
Compétence outil		*Requise*
LAMP (Linux/Apache/MySQL/PHP)	■■■☐	

Compétences		
Outils de supervision, de contrôle et d'audit	■■■□	
Compétence linguistique		*Requise*
Anglais technique	B1 Seuil	

Diplômes ou expérience professionnelle recommandée pour exercer les fonctions
Bac +3 à Bac+5 - Spécialisation en cybersécurité serait un plus