| Expert(e) en cyberdéfense | |
|---|---|
| **Corps :** | Ingénieur de recherche de 1ère classe |
| **Nature du concours :** | Externe |
| **Branche d'activité professionnelle (BAP) :** | « E » Informatique, Statistiques et Calcul Scientifique |
| **Famille d'activité professionnelle :** | Ingénierie des systèmes d'information |
| **Famille d'activité professionnelle REME :** | Systèmes et réseaux d'information et de communication |
| **Emploi type :** | Chef-fe de projet ou expert-e en ingénierie des systèmes d'information |
| **Emploi type de rattachement (REME) :** | Responsable sécurité des systèmes et réseaux d'information et communication |
| **Nombre de postes offerts :** | 1 |
| **Localisation du poste :** | MENESR – Administration centrale - PARIS |
| **Descriptif du poste offert au concours** | |
| **Activités essentielles** | |
| **Fonction :** | Expert en cyberdéfense |
| **Description :** | **DESCRIPTION DU POSTE (responsabilités, missions, attributions et activités) :**<br><br>Le titulaire du poste exercera au sein du centre opérationnel de sécurité des systèmes d'information ministériels (COSSIM). Le COSSIM est rattaché au bureau de la sécurité numérique et du Centre opérationnel de sécurité des systèmes d'information ministériels (bureau DNE SOCLE 4).<br><br>Les missions et objectifs du COSSIM, sont définis par un comité de pilotage composé du Haut-Fonctionnaire de Défense et de Sécurité (HFDS), de la DNE. Une feuille de route est définie annuellement et fait l'objet d'un suivi mensuel.<br><br>L'équipe est constituée du responsable du COSSIM, de quatre experts en analyse et traitements d'incidents (Forensic) et en analyse de flux afin de mettre en place une détection des attaques.<br><br>Les activités d'analyse et de traitements des incidents consistent à analyser les incidents de sécurité et le fonctionnement des attaques que subissent les systèmes d'information afin d'en définir leur état de compromission et de proposer les contre-mesures nécessaires.<br><br>Les activités de détection d'intrusion consistent à :<br>• Analyser les attaques observées sur le système d'information,<br>• Définir l'état de compromission du système,<br>• Proposer des mesures adaptées et guider les victimes dans leur mise en œuvre.<br><br>L'expert(e) sera par ailleurs chargé(e) de participer au développement et au maintien d'outils d'investigation numérique, de mécanismes et de règles de corrélation d'événements, de journalisation et de surveillance. Il(elle) sera également chargé(e) d'effectuer de la veille technologique sur les techniques d'attaques et d'investigation numérique et pourra être impliqué(e) dans des actions de formation. |

| Compétences requises | |
|---|---|
| **Domaine :** | Cybersécurité |
| **Qualités requises :** | **COMPETENCES OPERATIONNELLES :**<br>- Détecter et analyser un risque<br>- Alerter et gérer une situation à risque<br>- Diagnostiquer<br>- Gérer une situation de crise, d'urgence ou dangereuse<br>- Rédiger une lettre, un document, une note, un rapport, une communication<br>- Capacité de dialogue et de vulgarisation avec l'encadrement supérieur des ministères<br>- Capacité à transmettre la connaissance ou à organiser un retour d'expérience<br><br>**COMPETENCES COMPORTEMENTALES :**<br>- Rigueur, organisation du travail<br>- Discrétion<br>- Réactivité<br>- Capacité d'adaptation à des contextes très différents<br>- Esprit d'initiative, d'analyse et de synthèse<br>- Autonomie, capacité à travailler seul et en équipe<br>- Capacité d'écoute et de dialogue avec les collaborateurs, les partenaires internes et externes<br>- Capacité d'analyse des points de vue des différents acteurs<br>- Maîtrise des techniques de communication orales et écrites |

| Environnement et contexte de travail | |
|---|---|
| **Descriptif du service :** | **<u>Direction du numérique pour l'éducation</u>**.<br>Le numérique est un enjeu sociétal et en particulier pour l'éducation nationale, mêlant projets territoriaux, nationaux et internationaux. Née en 2014, la direction du numérique pour l'éducation a pour mission l'impulsion et l'accompagnement de la transformation numérique du système éducatif au bénéfice de l'ensemble de la communauté éducative (personnels des établissements, élèves, parents, collectivités…) ainsi que des agents.<br>C'est une direction jeune, à forte valeur ajoutée. Elle définit la politique de développement du numérique éducatif, en assure le déploiement et la valorisation. Elle prépare aussi les orientations stratégiques et les éléments de programmation en matière de numérique pour l'éducation. La direction coordonne le volet numérique de l'activité des opérateurs de l'enseignement scolaire (CNED, CANOPE, ONISEP…) et conduit la politique partenariale avec les acteurs publics et privés de la filière numérique.<br>La direction du numérique pour l'éducation c'est aussi l'animation de réseaux en territoire (délégations académiques au numérique éducatif, direction des systèmes d'information…), la gestion, la production et le support de projets à enjeux nationaux (examens, concours, Ressources Humaines, bourses…). Ces enjeux et projets, aussi riches que variés, impactent en priorité, 1 162 850 personnels et 12 858 550 élèves.<br><br>Au sein de la sous-direction du socle numérique, et du **bureau de la sécurité numérique** (DNE Socle 4)**,** le **centre opérationnel de la sécurité des systèmes d'information ministériels** (COSSIM) intervient sur des missions dites synchrones (détection et réaction immédiate) et asynchrones (analyse, qualification, mesures techniques et retour d'expérience). Son périmètre d'action couvre l'ensemble des entités des deux ministères (MENJS et MESRI), y compris les tutelles. Ses missions sont les suivantes :<br>1. Expertise : maintenir un bon niveau d'expertise opérationnelle dans le domaine de la SSI.<br>2. Détection : mettre en place une détection opérationnelle des attaques sur le périmètre de l'administration centrale (maitrise de la journalisation et outils de détection) et participer à la mise en place de systèmes de détection sur les autres périmètres du ministère (Réseau d'interconnexion Education Nationale, Académies, Renater, …). Contribuer aux spécifications, développement et à la mise en œuvre des outils nécessaires à l'analyse et à la capitalisation des informations sur les attaques et les modes opératoires suivis.<br>3. Gestion : réceptionner et recenser les déclarations des incidents les plus significatifs en collaboration avec les organisations existantes (EN : Pôle SSI, ESRI : CERT Renater) et les RSSI des différentes entités.<br>4. Analyse : procéder à l'analyse des incidents les plus significatifs touchant les systèmes des ministères. Analyser les tactiques et techniques d'attaques et réaliser les corrélations techniques entre les attaques et les modes opératoires connus.<br>5. Retour d'expérience : fournir l'organisation de pilotage des retours d'expériences, des informations et les indicateurs de sécurité nécessaires à l'analyse de la menace et au suivi de la stratégie. Orienter les équipes de veille et les investigations menées. |
| **Contraintes particulières :** | Il est requis, des membres du COSSIM, une disponibilité et une réactivité en cas d'incidents de sécurité concernant les systèmes d'information. Des possibilités d'astreintes ou d'horaires décalés adaptés aux nécessités du service sont à prévoir. |