

## FICHE DE POSTE

(à diffuser au format PDF)

### IDENTIFICATION DU POSTE

**INTITULE DU POSTE :** RESPONSABLE DU CENTRE OPERATIONNEL DE SECURITE DES SYSTEMES D'INFORMATION MINISTERIEL (COSSIM)

<b>DIRECTION OU SERVICE :</b> DNE	
<b>CATEGORIE :</b> A / A+	<b>POINTS NBI :</b> <input type="text"/>
<b>FAMILLE(S) PROFESSIONNELLE(S) REME</b> SYSTEMES ET RESEAUX D'INFORMATION ET DE COMMUNICATION	<b>DOMAINE FONCTIONNEL RIME</b> Numérique et systèmes d'information et de communication
<b>INTITULE DE L'EMPLOI TYPE REME</b> Responsable sécurité des systèmes et réseaux d'information et de communication	<b>EMPLOI REFERENCE RIME</b> Chargé de cyberdéfense
<b>CONTEXTE DU RECRUTEMENT</b> (activer les cases souhaitées dans le menu « propriétés »)	
<input type="checkbox"/> Poste vacant <input type="checkbox"/> Poste susceptible d'être vacant <input checked="" type="checkbox"/> Création	
Date souhaitable de prise de fonction : 02/05/2018	
<input type="checkbox"/> Suppléance	
Durée de la suppléance : du <input type="text"/> au <input type="text"/>	
<b>LOCALISATION ADMINISTRATIVE ET GEOGRAPHIQUE</b>	
<b>Direction ou service :</b>	DIRECTION DU NUMERIQUE POUR L'ÉDUCATION, SERVICE DES TECHNOLOGIES ET DES SYSTEMES D'INFORMATION
<b>Sous-direction :</b>	SOUS-DIRECTION DES INFRASTRUCTURES TECHNIQUES ET DE L'EXPLOITATION
<b>Bureau et secteur :</b>	CENTRE OPERATIONNEL DE SECURITE DES SYSTEMES D'INFORMATION MINISTERIEL
<b>Sigle :</b>	COSSIM
<b>Adresse :</b>	61-65 RUE DUTOT 75015 PARIS

### LE POSTE ET SON ENVIRONNEMENT

<b>FONCTION :</b> RESPONSABLE DU CENTRE OPERATIONNEL DE SECURITE DES SYSTEMES D'INFORMATION MINISTERIEL
<b>NOMBRE D'AGENTS A ENCADRER :</b> 2 (2 A, 0 B, 0 C)
<b>CONDITIONS PARTICULIERES D'EXERCICE :</b>
Description de la structure (missions, organisation) :

La direction du numérique pour l'éducation est une direction commune au secrétariat général et à la direction générale de l'enseignement scolaire.

Elle comprend, outre la cellule d'expertise et relations partenariales, le secrétariat des instances stratégiques, le bureau du budget et du contrôle de gestion, la mission communication :

- le service du développement du numérique éducatif ;
- le service des technologies et des systèmes d'information.

Les chefs de service ont qualité d'adjoint au directeur pour les questions relevant de leurs compétences.

Le **Service des Technologies et des Systèmes d'Information (DNE B - STSI)** contribue à l'élaboration des grandes orientations en matière de systèmes d'information pour l'ensemble des ministères en charge de l'éducation nationale, de l'enseignement supérieur, de la recherche et de l'innovation et de leurs établissements.

Il conduit la mise en œuvre opérationnelle du schéma stratégique des systèmes d'information et des télécommunications.

Il assure la maîtrise d'œuvre des projets et services informatiques et en assure l'industrialisation.

Il assure l'urbanisation, la mise à niveau, la sécurité et la qualité des systèmes d'information et de communication.

Il anime et coordonne l'action des services déconcentrés et d'administration centrale dans les domaines relevant de sa compétence.

Le service des technologies et des systèmes d'information comprend :

- la sous-direction des infrastructures techniques et de l'exploitation ;
- la sous-direction des systèmes d'information.

La **Sous-Direction des Infrastructures Techniques et de l'Exploitation (DNE B1 - SDITE)** veille à la cohérence des choix techniques et définit le schéma directeur des infrastructures.

Elle assure la programmation financière des plans d'équipement techniques.

Elle anime et coordonne l'action des services déconcentrés dans les domaines relevant de sa compétence.

Elle contribue au pilotage et à l'animation du réseau des directions des systèmes d'information académiques, des pôles de compétences, des centres de ressources techniques et des centres d'exploitation et de services.

Elle assure également le rôle de centre de services en informatique et télécommunications pour l'administration centrale en mettant à disposition des utilisateurs les équipements et les services associés.

La sous-direction des infrastructures techniques et de l'exploitation est constituée :

- du bureau des expertises techniques, des projets d'infrastructures et de la sécurité des systèmes d'information ;
- du bureau du pilotage de l'exploitation des systèmes d'information ;
- du bureau des infrastructures techniques et des prestations de service informatique pour l'administration centrale.

**EFFECTIFS DE LA STRUCTURE : 3 A 0 B 0 C**

**DESCRIPTION DU POSTE (responsabilités, missions, attributions et activités) :**

Le titulaire du poste sera le responsable du futur centre opérationnel de sécurité des systèmes d'information ministériel (COSSIM). Le COSSIM sera rattaché hiérarchiquement au sous-directeur des infrastructures techniques et de l'exploitation, et s'inscrit dans l'organisation générale de la sécurité des systèmes d'information du ministère.

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.

Le 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 (MEN et MESRI), y compris les tutelles.

Ses missions sont :

1. Expertise : maintenir un bon niveau d'expertise opérationnelle dans le domaine de la SSI
2. Détection : mettre en place une détection opérationnelle des attaques sur le périmètre de l'administration centrale (automatisation de processus de collecte, maîtrise de la journalisation, outils de détection et règles de corrélation d'événements) et participer à la mise en place de systèmes de détection sur les autres périmètres du ministère (Réseau d'interconnexion Education Nationale, académies, centres d'hébergements mutualisés, Renater, ...)
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.
4. Analyse et investigation : coordonner, orienter et contrôler les activités techniques d'analyse, procéder à l'analyse des incidents les plus significatifs touchant les systèmes des ministères
5. Communication : communiquer vers les autorités du ministère et vers les acteurs de la SSI (état de la menace, situation de crise, retours d'expériences).

Le COSSIM est à constituer et installer, aussi le responsable s'attachera à organiser son équipe, formaliser les processus, définir et mettre (ou faire mettre) en place les outils nécessaires, mettre en œuvre la chaîne d'alerte. La formalisation de tableaux de bord et de ses indicateurs associés à un reporting régulier sera à mettre en œuvre. Selon le calendrier, il sera amené à participer au recrutement des 2 autres membres du périmètre initial.

Il est requis du responsable 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.

#### RESPONSABILITES PARTICULIERES :

Sans contrainte particulière

#### PRINCIPAUX INTERLOCUTEURS :

- |   |   |  |
|---|---|--|
| <input checked="" type="checkbox"/> les autres services de la direction | <input checked="" type="checkbox"/> les services déconcentrés | <input checked="" type="checkbox"/> d'autres ministères      |
| <input type="checkbox"/> les agents du ministère                        | <input checked="" type="checkbox"/> les cabinets ministériels | <input checked="" type="checkbox"/> d'autres acteurs publics |
| <input checked="" type="checkbox"/> les autres directions               | <input checked="" type="checkbox"/> le secteur privé          | <input type="checkbox"/> des organismes étrangers            |

#### EXPERIENCE PROFESSIONNELLE SOUHAITEE :

- Ce poste est ouvert aux agents sans expérience professionnelle
- Ce poste est ouvert aux agents ayant une expérience professionnelle initiale
- Ce poste est ouvert aux agents ayant une expérience professionnelle confirmée

### LES CONNAISSANCES ET COMPETENCES MISES EN ŒUVRE :

#### CONNAISSANCES :

- Applications et techniques de surveillance
- Méthodologies d'identification et de gestion des risques et des aléas, méthode d'analyse des risques et contrôle interne
- Normes de sécurité informatique
- Techniques de cyber attaques et contre-mesures pour les prévenir
- Fonctionnement de sondes de détections d'intrusions et d'outils de corrélation de journaux d'événements
- Protocoles et architectures réseaux, pratique de l'analyse des traces réseau et de journaux
- Notions de cryptographie et d'algorithmique
- Expertise en systèmes d'exploitation, en particulier Linux ainsi que les protocoles courants pour le fonctionnement des services
- Connaissance des architectures web et des systèmes de gestion de bases de données (conception de schéma de bases de données et mise en œuvre)
- Maîtrise de l'anglais technique
- Connaissance des aspects juridiques liés aux systèmes d'information et au numérique

#### COMPETENCES OPERATIONNELLES :

- Détecter et analyser un risque
- Alerter et gérer une situation à risque
- Diagnostiquer
- Gérer une situation de crise, d'urgence ou dangereuse
- Rédiger une lettre, un document, une note, un rapport, une communication
- Capacité de dialogue et de vulgarisation avec l'encadrement supérieur des ministères
- Capacité à transmettre la connaissance ou à organiser un retour d'expérience
- Connaissance des principes de fonctionnement des solutions de supervision des informations et des événements de sécurité (SIEM)
- Capacité à définir, à mettre ou faire mettre en œuvre, l'outillage requis pour le fonctionnement du COSSIM

## COMPETENCES COMPORTEMENTALES

- Rigueur, organisation du travail
- Discrétion
- Réactivité
- Capacité d'adaptation à des contextes très différents
- Esprit d'initiative, d'analyse et de synthèse
- Autonomie, capacité à travailler seul et en équipe
- Capacité d'organisation et d'animation d'équipe
- Capacité d'impulsion dans les actions
- Capacité d'écoute et de dialogue avec les collaborateurs, les partenaires internes et externes
- Capacité d'analyse des points de vue des différents acteurs
- Maîtrise des techniques de communication orales et écrites

## VOS CONTACTS RH *(nom, prénom, fonction, téléphone, adresse électronique)*

M. Laurent LE PRIEUR – Sous-directeur des infrastructures techniques et de l'exploitation

✉ [laurent.le-prieur@education.gouv.fr](mailto:laurent.le-prieur@education.gouv.fr) - ☎ 01 55 55 25 86

M. François GILLES – Adjoint au sous-directeur des infrastructures techniques et de l'exploitation

✉ [francois.gilles@education.gouv.fr](mailto:francois.gilles@education.gouv.fr) - ☎ 01 55 55 77 80