CYBER'OCC
LE CENTRE CYBERSÉCURITÉ EN OCCITANIE

Offre d'emploi Analyste CSIRT*

Computer Security Incident Response Team

1- A propos de notre organisation

Cyber'Occ est le centre régional dédié à la Cybersécurité, fondé par la Région Occitanie, l'agence AD'OCC et Ekitia. Hub régional de la Cybersécurité, Cyber'Occ offre aux entreprises, collectivités et toute autre organisation d'Occitanie, les moyens d'une véritable sécurité numérique éthique et durable, de la sensibilisation à la lutte contre la cybercriminalité, à la pointe de l'innovation en partenariat à l'échelle nationale et européenne.

Cyber'Occ a pour ambition, d'une part d'apporter des solutions aux acteurs économiques locaux en cas d'attaque et pour se prémunir au mieux des risques de sécurité sur leurs systèmes d'information et les produits qu'ils développent et d'autre part, d'animer et répondre aux besoins de la filière Cybersécurité en Occitanie et participer à la représentation de ce savoir-faire régional auprès des diverses instances nationales et européennes.

Cyber'Occ déploie le service de CSIRT régional qui est un service gratuit d'assistance en cas de cyber-incident, aux TPE, PME, ETI, collectivités et associations d'Occitanie pour contribuer à la sécurité de l'infrastructure en aidant à prévenir, détecter, atténuer et répondre aux cyberattaques.

Contexte et enjeux

Pour faire face à l'accroissement de la cybermenace, le plan France Relance prévoit l'émergence, dans chaque région, d'une équipe de réponse aux incidents de sécurité informatique (Computer Security Incident Response Team – CSIRT) ayant pour mission d'accompagner les acteurs implantés sur le territoire régional à répondre aux incidents survenant sur leurs systèmes d'information.

Ces CSIRT régionaux viennent renforcer un écosystème existant où opèrent des prestataires de réponse à incident. Véritables partenaires de ces prestataires, les équipes CSIRT régionales s'adressent à un public principalement constitué d'acteurs locaux de taille moyenne (PME, ETI, associations, institutions, collectivités territoriales, etc.), auprès desquels ils constituent un point de contact opérationnel de référence en cas d'incident de sécurité informatique.

Leurs missions auprès de leurs bénéficiaires consistent à :

- Répondre aux alertes de cybersécurité de premier niveau (triage et qualification des alertes) ;
- Rediriger vers des prestataires externes de réponse à incident pour la réponse de second niveau (investigation forensique, remédiation, reconstruction, pilotage, etc.) ;
- Être présent tout au long de l'incident via un suivi du déroulement ;
- Transmettre les informations et conseils relatifs aux poursuites juridictionnelles.

Les CSIRT régionaux ont aussi vocation à s'intégrer dans l'écosystème global de la réponse à incident en assurant un rôle de relai entre les différents acteurs de la réponse à incident (CERT-FR, Cybermalveillance.gouv.fr, les autres CSIRT : régionaux, sectoriels, etc… , l'InterCERT France) et les prestataires de réponse à incident locaux tout en contribuant à la consolidation de l'incidentologie régionale.

Le service CSIRT régional d'Occitanie est un service du centre cybersécurité régionale Cyber'Occ.

2- Description de la mission

Placé sous la responsabilité du responsable du CSIRT de Cyber'Occ :

En tant qu'analyste CSIRT, vous serez le **premier point de contact** pour les bénéficiaires lors de la réponse aux incidents de sécurité.

Les **principales missions** qui vous seront confiées sont les suivantes :

- **Communiquer** avec le bénéficiaire dans des conditions de crise de cybersécurité ;
- **Collecter, trier et analyser les informations techniques** apportées par le bénéficiaire lors du premier contact (ex. population impactée, services impactés, informations nécessaires à l'investigation, etc.) ;
- **Qualifier les incidents de cybersécurité** ;
- Transmettre les premières **mesures réflexes** au bénéficiaire (ex. bonnes pratiques) ;
- Conseiller les bénéficiaires sur les **démarches immédiates** à effectuer et les **procédures légales** à suivre (ex. préservation des preuves, dépôt de plainte) ;
- **Identifier, à l'aide d'une matrice d'engagement, les acteurs locaux de la réponse à incident** les plus à même d'assurer une réponse face à la menace rencontrée (ex. disponibilité, technologie engagée, localisation géographique, services proposés, etc.) ;
- **Suivre le dossier** du bénéficiaire tout au long de l'incident ;
- Assurer une veille de cybersécurité proactive ;
- *Identifier des possibilités **d'améliorer les processus de réponse à incident** ou les activités pouvant être outillées, voire automatisées ;*
- ***Proposer** des axes **d'amélioration continue des processus** en introduisant de nouveaux outils, de nouvelles technologies et de nouvelles pratiques pour aider l'équipe à se développer et à renforcer ses activités ;*
- Contribuer aux actions de **partage** au sein de la communauté de la réponse à incident.

En tant qu'analyste CSIRT, vous ferez partie d'une équipe chargée de **qualifier et transférer les incidents** aux prestataires experts de la réponse afin de répondre aux menaces qui pèsent sur toute la région. En rejoignant l'équipe à un moment clé, vous jouerez un **rôle essentiel** en aidant à développer et à façonner leur sécurité opérationnelle.

Vous rejoindrez une équipe à taille humaine et serez amenés à participer aussi à d'autres sujets pour venir en appui au reste de l'équipe Cyber'Occ. Vous serez amené par exemple à participer à des projets numériques, aux actions de sécurisation du SI interne, ainsi qu'aux prestations externes telles que les accompagnements d'entreprises, les audits et sensibilisations.

3- Profil recherché

Formation : BAC +3 ou techniciens supérieurs avec une expérience dans la réponse aux incidents de sécurité.

3.1 - Compétences

Savoir

- Réelle **appétence** pour les sujets techniques liés à la **cybersécurité** et/ou à la **réponse aux incidents**
- Compréhension du **fonctionnement**, de la **sécurisation** et des **vulnérabilités** des principaux **systèmes d'exploitation**
- Compétences d'**analyse** de système d'information (SI) et d'architecture du SI
- **Connaissance d'outils d'analyse** (ex. journaux de Pare-feu, Proxy, EVTX, etc.) et des procédures légales
- **Connaissance** des sujets de **renseignement sur la menace** (ex. Cyber Threat Intelligence, veille de vulnérabilité)
- **Connaissance de vulnérabilités** connues et de **techniques**, **tactiques** et **procédures** entreprises par des attaquants
- Bonne maîtrise de l'anglais

Savoir-faire

- **Capacité de restitution et de vulgarisation**
- Capacité à suivre des procédures et des processus
- Capacité à gérer les priorités dans un environnement au rythme rapide
- Respect de la confidentialité et sécurisation de l'information
- Aptitude à tenir le rôle de conseil auprès de la direction et du conseil d'administration

Savoir-être

- Curiosité, esprit critique, analytique et rigoureux
- Esprit d'amélioration continue, être positif et constructif
- Sens prononcé du service
- Capacité d'organisation et d'aide à la décision
- Sens du relationnel et du travail en équipe
- **Excellentes aptitudes à la communication et aux relations interpersonnelles**
- Disponibilité, réactivité, respect des délais, capacité à rendre compte et alerter

- Écoute, empathie, pédagogie

3.2- Expériences

- 2 ans d’expérience minimum dans le domaine de la cybersécurité / SSI

4- Informations supplémentaires

- Rémunération selon expérience
- Horaires de travail : 9h-12h30 / 13h30-17h
- Télétravail possible, 2 jours par semaine
- Travail au sein d'une équipe à taille humaine

Pour candidater, envoyez votre candidature (CV + lettre de motivation)
à administratif@cyberocc.fr