https://www.emagine.org/fr/nos-offres/details/analyste_cybersecurite/paris/cr073754.html

https://www.emagine.org/fr/home.html#sites6

Notre client, acteur majeur des médias, a engagé une démarche de renforcement global de la **sécurité** de son système d'information via plusieurs projets visant à mettre en œuvre des moyens de **cyber** défense pour la gestion des vulnérabilités, la détection et la réponse aux incidents de **sécurité** IT, et ce, dans un environnement audiovisuel. Dans ce contexte, il recherche un(e) **Analyste** Cybersécurité pour renforcer l'équipe CSIRT interne rattachée au Responsable de la **Sécurité** Opérationnelle, et pilotée par un team leader.

L'activité principale consiste en :
- L'analyse et la qualification d'évènements et incidents de **sécurité** via un SIEM interne et un SOC externalisé ;

- **La qualification est une recommandation de produits et services de cybersécurité éprouvés et approuvés par ANSSI. Pour les produits, l'évaluation de la robustesse consiste à éprouver leur capacité à résister à des attaques informatiques selon un contexte d'emploi et un niveau de menace définis. Pour les services, l'évaluation de la compétence d'un prestataire de services permet de démontrer son aptitude à identifier et maitriser les menaces et risques pour satisfaire les exigences inscrites dans des référentiels métiers. Pour les produits, l'évaluation de la confiance signifie confidentialité / protection des données / correction des failles et vulnérabilités,etc. Pour les services, l'évaluation de la confiance signifie Maintien des compétences,etc.**

- **Expérience SIEM (Splunk / RSA NetWitness / IBM Qradar / LogRythm / NextGen SIEM / Exabeam / McAfee Enterprise Security Manager / Securonix). Il dispose d'une capacité de traitements et de stockage des données très importante (les réseaux / les points d'accès / les malwares / les vulnérabilités du système). Il permet notamment de faire le lien entre différents évènements, alerter en temps-réel en cas d'intrusion la personne chargée du SIEM mais aussi de générer des rapports sur tous types de problèmes de sécurité.**

- **SOC: Security Operations Center, C'est divisé par SOC interne et SOC externalisé. Sa promesse est opérationnelle à tout moment à 24/7. Pour SOC interne, les avantages sont Toutes les données sont stockées et traitées en interne / une communication et une corrélation plus facile d'événements entre chaque département. Pour SOC externalisé, les avantages sont Évolutivité et flexibilité / Mise à disposition d'experts / Pas de conflit avec les autres départements (simplement conseil extern et reporting)**

- **Je faisais la surveillance des évènements de sécurité / Qualification des évènements, levée de doute et élimentation des faux positifs / et aussi paramétrage, affinage des règles du splunk. Concernant Couche 1&2&3, j'ai mis en place la politique de remédiation efficace et piloté des intervenants pour la résolution de l'incident. Parfois, j'ai utilisé des outils de rétro-ingénierie comme désassembleur,décompilateur pour le débogage.**

- **Couche 2 Risques: ARP Spoofing**
- **Couche 3 Risquse: Smurf Attack /DDOS / Ping Flood/**
- **Couche 4 Risques: Idle scanner / Port Scanner**
- **Couche 7 Risques: DNS Spoofing /DHCP Snooping / SQL Injection / Keylogger / Screen / Malware / XSS/ Phishing**
- **Par example, face à l'attaque login, générer une alerte concernant 3 ou +3 échec login pendant une minute du meme hote.**
- **Par example, face à l'attaque pare-feu, générer une alerte concernant 15 ou +15 dénier / rejeter évènement pendant une minutes du meme hote.**

- La qualification implique le suivi et la gestion des incidents, les échanges avec les différents acteurs internes et externes, ainsi que les recommandations à l'IT (remédiation) et la capitalisation (RETEX, base d'incidents etc...), l'analyse forensic.

- **RETEX: Fiche Retour d'expérience des cyberattaques pour assurer la continuité d'activité et la gestion de crise,face aux cybermenaces. Il existe les autres méthodes : Fiche par catégorie de cyberatttaque et Tableau de synthèse des actions à mettre en place pour type de cyberattaque.**

- L'activité comprend également la veille (technologique, vulnérabilités, menaces), le maintien en condition opérationnelle et l'amélioration continue des outils de **sécurité** internes à l'équipe CSIRT et des process liés, l'animation d'ateliers récurrents avec les équipes IT, la sensibilisation, la communication de bulletin d'alerte et la participation active en cas de crise.

- **CSIRT: Computer Security Incident Response Team, C'est un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises et aux administrations. Les taches prioritaires sont:**
  I. **Centralisation des demandes d'assistance à la suite des attaques: réception des demandes / analyse des symptomes et éventuelle corrélation des incidents.**
  II. **Traitement des alertes et réaction aux attaques informatiques.**
  III. **Établissement et maintenance d'une base de données des vulnérabilités.**
  IV. **Prévention par diffusion d'informations pour minimiser les risques d'incidents.**

- Livrables: qualification, CR d'incidents, tableaux de bord... saisis dans un outil de gestion d'incidents, ou fichiers bureautiques.

- **CR d'incidents: Compte-Rendu d'incidents**

Compétences attendues :
- Expérience en **Sécurité** des SI / Systèmes, réseaux et stockages

- Connaissance des techniques et solutions de **sécurité** / Sondes réseaux et analyse protocolaire / Shell, scripts, langage de programmation