KIT MÉDIA CANDIDATS

GUIDE ENTRETIEN D'EMBAUCHE

Réussir son entretien d'embauche en Cybersécurité

Analyste SOC, pentester, RSSI... Préparez-vous efficacement aux entretiens techniques et comportementaux des métiers de la cybersécurité.

3-4	48-95K€	STAR
Entretiens en moyenne avant une offre	Fourchette de rémunération à négocier	La méthode à maîtriser

Une question ?
contact@kaischool.fr
+33 (0)7 55 50 66 56

Kit média candidats KaiSchool
Mastère Cybersécurité — Expert Renseignement & Investigation

Avant l'entretien

Un entretien en cybersécurité évalue autant votre rigueur méthodologique que vos connaissances techniques. Recruteurs SOC, RSSI et responsables sécurité cherchent des profils capables d'expliquer clairement un raisonnement, pas seulement de réciter des définitions.

Préparer sa recherche

- Étudiez la surface d'exposition publique de l'entreprise (CERT-FR, avis de sécurité, présence sur les réseaux)
- Identifiez le SOC/SIEM ou les outils mentionnés dans l'offre (Splunk, QRadar, Sentinel, etc.)
- Repérez si l'entreprise a un programme de bug bounty ou une politique de divulgation
- Préparez 2-3 questions sur l'organisation de l'équipe sécurité et son périmètre (SOC interne vs MSSP)

La méthode STAR pour structurer ses réponses

Pour chaque expérience (stage, projet, CTF, alternance), structurez votre réponse en 4 temps : le contexte, votre mission, les actions menées, et le résultat obtenu ou l'incident résolu.

Situation **Tâche** **Action** **Résultat**

Questions comportementales fréquentes

- Racontez un incident de sécurité que vous avez traité ou analysé — comment avez-vous priorisé ?
- Comment restez-vous à jour sur les nouvelles menaces et vulnérabilités (CVE, threat intel) ?
- Décrivez une situation où vous avez dû expliquer un risque technique à un public non technique
- Comment gérez-vous la pression lors d'un incident critique en production ?

Questions techniques à anticiper

Exemples de questions

- Expliquez la différence entre une analyse SOC de niveau 1, 2 et 3
- Comment détecteriez-vous un mouvement latéral sur un réseau d'entreprise ?
- Quelles sont les étapes d'une réponse à incident (NIST / SANS) ?
- Différence entre un test d'intrusion boîte noire, grise et blanche
- Comment analyseriez-vous un binaire suspect sans l'exécuter (analyse statique) ?
- Qu'est-ce que le framework MITRE ATT&CK et comment l'utilisez-vous ?
- Comment sécuriseriez-vous une architecture cloud multi-comptes (AWS/Azure) ?
- Expliquez un cas d'usage concret de la corrélation de logs en SIEM

Négocier sa rémunération

En cybersécurité, la tension sur les profils qualifiés (ANSSI : +15 000 postes non pourvus en France) joue en votre faveur. Basez votre négociation sur des certifications (CEH, OSCP, GCIH), votre expérience en gestion d'incidents réels et le niveau d'astreinte demandé.

Repère marché : 48-95K€ selon poste et séniorité

Après l'entretien

- Envoyez un email de remerciement sous 24h, en rebondissant sur un point technique discuté
- Si un test technique ou un CTF vous a été proposé, soignez la clarté de votre rapport écrit
- Relancez poliment après 7-10 jours sans réponse, sans excès de pression
- Demandez un retour constructif même en cas de refus — utile pour progresser

« En cybersécurité, on ne recrute pas seulement un niveau technique, mais une capacité à documenter et communiquer sous pression. » — retour recruteur, secteur SOC/MSSP.

Repères de marché : ANSSI 2026, ISC2 2024, retours d'expérience KaiSchool. À affiner selon l'entreprise, le poste et la localisation.