

Les métiers de la Cybersécurité

Analyste SOC, pentester, RSSI, investigateur numérique... Découvrez les fiches de poste, la rémunération et l'employabilité des métiers de la cybersécurité en France.

+12 000

Offres ouvertes en France

+15 000

Postes non pourvus (ANSSI)

48-95K€

Fourchette de rémunération

01 Analyste SOC / Threat Hunter

02 Pentester / Auditeur SI

03 Analyste CTI (Cyber Threat Intelligence)

04 Investigateur numérique (DFIR)

05 Analyste malware / Reverse engineer

06 RSSI (Responsable Sécurité des SI)

Le secteur en chiffres

La cybersécurité est aujourd'hui l'un des secteurs les plus en tension du marché de l'emploi en France. Les entreprises, ESN, cabinets de conseil, administrations et OIV (opérateurs d'importance vitale) peinent à recruter des profils qualifiés, ce qui tire les rémunérations vers le haut et sécurise l'employabilité des jeunes diplômés dès la sortie de formation.

+12 000

Offres d'emploi ouvertes en cybersécurité en France

SOURCE : OCDE, 2024

4,8M

Déficit mondial de professionnels de la cybersécurité

SOURCE : ISC2, 2024

+15 000

Postes non pourvus en France faute de candidats

SOURCE : ANSSI, 2026

Employabilité

Le déficit structurel de compétences (4,8 millions de professionnels manquants dans le monde selon l'ISC2) place les profils cybersécurité parmi les plus recherchés du marché IT. En France, l'ANSSI recense plus de 15 000 postes non pourvus : un diplômé formé aux méthodologies opérationnelles (SOC, forensics, CTI, gouvernance) trouve généralement un poste en moins de 6 mois, souvent avant la fin de sa formation en alternance.

Pourquoi se former à ces métiers avec KaiSchool

- Approche par la menace : les étudiants apprennent à « penser comme l'adversaire »
- Labs en cyber ranges, challenges CTF et incidents simulés en conditions réelles
- Modules co-construits avec des professionnels du secteur (SOC, RSSI, forces de l'ordre)
- Alternance valorisée avec suivi pédagogique dédié et jury sectoriel

Analyste SOC / Threat Hunter

OPÉRATIONNEL

Surveiller en continu les systèmes d'information pour détecter, qualifier et traiter les incidents de sécurité avant qu'ils ne causent des dommages.

ACTIVITÉS PRINCIPALES

- Superviser les flux et alertes remontées par le SIEM (Splunk, ELK)
- Qualifier les incidents et déclencher les procédures de remédiation
- Traquer proactivement les menaces avancées (threat hunting)
- Rédiger les rapports d'incident et les indicateurs de compromission

COMPÉTENCES CLÉS

- SIEM & corrélation de logs
- Frameworks MITRE ATT&CK
- Analyse réseau (Wireshark)
- Réactivité et rigueur

RÉMUNÉRATION

35-50K€

TENSION MARCHÉ

Très forte

ACCÈS

Débutant / Bac+5

Débouchés / évolution : Analyste SOC N1 → N2/N3 → Threat Hunter → Responsable SOC ou Analyste CTI.

Pentester / Auditeur SI

OFFENSIF

Simuler des attaques réelles sur les systèmes, applications et réseaux d'une organisation afin d'en identifier les vulnérabilités avant qu'un attaquant ne les exploite.

ACTIVITÉS PRINCIPALES

- Réaliser des tests d'intrusion internes, externes et applicatifs
- Exploiter des vulnérabilités en conditions contrôlées
- Rédiger des rapports d'audit techniques et des plans de remédiation
- Restituer les résultats auprès des équipes techniques et de la direction

COMPÉTENCES CLÉS

- Méthodologies OWASP / OSSTMM
- Scripting (Python, Bash)
- Ingénierie réseau et systèmes
- Pédagogie et synthèse écrite

RÉMUNÉRATION

40-65K€

TENSION MARCHÉ

Forte

ACCÈS

Bac+5 / 1-3 ans

Débouchés / évolution : Pentester junior → Pentester senior / Red teamer → Lead Offensive Security.

Analyste CTI (Cyber Threat Intelligence)

RENSEIGNEMENT

Collecter, analyser et diffuser du renseignement sur les menaces (acteurs, techniques, campagnes) pour permettre à l'organisation d'anticiper les attaques.

ACTIVITÉS PRINCIPALES

- Surveiller les sources ouvertes, forums et le darkweb (OSINT)
- Exploiter des plateformes de threat intelligence (MISP, OpenCTI)
- Produire des rapports de renseignement stratégique et opérationnel
- Alimenter les équipes SOC et direction en indicateurs actionnables

COMPÉTENCES CLÉS

- OSINT et recherche darkweb
- Plateformes MISP / OpenCTI
- Analyse géopolitique et sectorielle
- Rédaction de rapports de renseignement

RÉMUNÉRATION

40-60K€

TENSION MARCHÉ

Forte

ACCÈS

Bac+5

Débouchés / évolution : Analyste CTI → CTI Lead → Responsable Threat Intelligence.

Investigateur numérique (DFIR)

INVESTIGATION

Intervenir après un incident pour reconstituer la chronologie de l'attaque, préserver les preuves numériques et documenter la chaîne de preuve en vue d'une procédure judiciaire.

ACTIVITÉS PRINCIPALES

- Collecter et préserver des preuves numériques (disques, mémoire, logs)
- Analyser des supports avec des outils forensics (Autopsy, Volatility)
- Reconstituer le mode opératoire de l'attaquant
- Rédiger des rapports opposables et coordonner avec les autorités

COMPÉTENCES CLÉS

- Forensic disque et mémoire
- Chaîne de preuve et aspects judiciaires
- Rigueur méthodologique
- Coordination avec les autorités

RÉMUNÉRATION

42-65K€

TENSION MARCHÉ

Forte

ACCÈS

Bac+5

Débouchés / évolution : Investigateur DFIR → Expert forensics judiciaire → Responsable investigation.

Analyste malware / Reverse engineer

TECHNIQUE

Décortiquer le fonctionnement de codes malveillants pour comprendre leurs capacités, leur origine et produire des signatures de détection.

ACTIVITÉS PRINCIPALES

- Analyser des malwares en environnement isolé (sandbox, VM dédiées)
- Effectuer de la rétro-ingénierie de binaires (Ghidra)
- Documenter les techniques, tactiques et procédures observées
- Produire des signatures de détection pour les équipes SOC

COMPÉTENCES CLÉS

- Reverse engineering (Ghidra)
- Assembleur et architectures bas niveau
- Sandboxing et environnements isolés
- Curiosité technique

RÉMUNÉRATION
45-70K€

TENSION MARCHÉ
Modérée à forte

ACCÈS
Bac+5 / spécialisation

Débouchés / évolution : Analyste malware → Reverse engineer senior → Chercheur en sécurité.

RSSI (Responsable Sécurité des Systèmes d'Information)

PILOTAGE

Définir et piloter la stratégie de sécurité de l'organisation, arbitrer les risques et garantir la conformité réglementaire (RGPD, NIS2).

ACTIVITÉS PRINCIPALES

- Élaborer la politique de sécurité et la feuille de route SSI
- Piloter la gestion des risques (méthode EBIOS) et les audits
- Coordonner la réponse à incident et la gestion de crise
- Reporter au COMEX et sensibiliser les collaborateurs

COMPÉTENCES CLÉS

- Gouvernance et normes ISO 27001
- Méthode EBIOS RM
- Leadership et communication COMEX
- Gestion de crise

RÉMUNÉRATION
65-95K€

TENSION MARCHÉ
Forte (poste senior)

ACCÈS
5-10 ans d'expérience

Débouchés / évolution : RSSI → RSSI groupe / CISO → Directeur cybersécurité.

Se former à ces métiers

Le Mastère Cybersécurité de KaiSchool prépare en 24 mois (ou 6-12 mois selon profil) aux six familles de métiers présentées dans ce document, à travers 850 heures de formation en présentiel, hybride ou alternance.

Mastère Cybersécurité — Expert Renseignement & Investigation (Bac+5, RNCP niveau 7)

Un parcours en 6 blocs de compétences (cadre stratégique, analyse des menaces, détection et investigation, renseignement CTI, gouvernance, gestion de crise), avec labs en cyber ranges, challenges CTF et projet fil rouge. Certification RNCP niveau 7 (Bac+5), éligible CPF. Site de Paris (Fontenay-sous-Bois) ou à distance.

Processus d'admission

Candidature en ligne, analyse du dossier, entretien de motivation et test technique de positionnement. Réponse sous 48h ouvrables. Diplôme Bac+4 ou 2 ans d'expérience IT requis (accès dérogatoire possible pour reconversion).

Prêt(e) à vous lancer ?

EMAIL

contact@kaischool.fr

TÉLÉPHONE

+33 (0)7 55 50 66 56

WEB

kaischool.fr/mastere-cybersecurite-kaischool



Chiffres de marché : OCDE (2024), ISC2 (2024), ANSSI (2026). Fourchettes de rémunération : estimations marché France 2025-2026 à titre indicatif, à affiner selon expérience, secteur et localisation.