M1883
ANALYSTE SOC (SECURITY OPERATIONS CENTER)

Emploi cadre

Transition numérique

Définition

L'Analyste SOC surveille et protège les systèmes informatiques des organisations contre les cyberattaques.

- Surveille les réseaux et les systèmes pour détecter les anomalies et les signes d'intrusion
- Analyse les alertes pour identifier les incidents et menaces de sécurité informatique
- Gère les incidents de sécurité en coordonnant les réponses appropriées
- Met à jour les règles de sécurité et les configurations pour prévenir les futures attaques
- Réalise des audits de sécurité réguliers pour identifier les vulnérabilités
- Collabore avec d'autres équipes techniques pour améliorer la sécurité des systèmes informatiques

Accès à l'emploi

Ce métier est accessible avec un Bac + 5 Master ou un Diplôme d'ingénieur en informatique, sécurité des systèmes, cybersécurité. Les certifications en sécurité telles que CISSP (professionnel certifié en sécurité des systèmes d'information) ou GIAC (certificat global en infosécurité) sont couramment requises.

Certifications et diplômes :

- Certificat de compétence analyste en cybersécurité
- Ingénieur diplômé de l'école nationale supérieure d'informatique pour l'industrie et l'entreprise spécialité informatique

Compétences

Savoir-faire

Savoir-faire principaux

Production, Construction, Qualité, Logistique

- Evaluer, prévenir, et gérer les risques et la sécurité
- Respecter une politique de sécurité de l'information
- Mettre en place des procédures de sécurité pour la protection des données — Transition numérique

Communication, Création, Innovation, Nouvelles technologies

- Mener des simulations d'attaque pour tester la sécurité — Transition numérique
- Piloter les fonctionnalités des équipements et systèmes de sécurité informatique — Transition numérique

Coopération, Organisation et Développement de ses compétences

- Agir rapidement en cas de détection d'intrusion
- Respecter les politiques de confidentialité des données Transition numérique

Pilotage, Gestion, Cadre réglementaire

- Rédiger des rapports de sécurité

Savoir-faire secondaires

Production, Construction, Qualité, Logistique

- Analyser les besoins de sécurité informatique Transition numérique
- Identifier les besoins en logiciel de sécurité Transition numérique
- Analyser les alertes de sécurité informatique Transition numérique
- Gérer les incidents de sécurité et les réponses aux incidents
- Analyser les risques de sécurité informatique Transition numérique
- Concevoir et maintenir un système de cybersécurité Transition numérique
- Mener un processus de test en cybersécurité Transition numérique
- Implémenter des solutions de cybersécurité adaptées Transition numérique
- Maintenir les systèmes de surveillance

Communication, Création, Innovation, Nouvelles technologies

- Réaliser des veilles technologiques en sécurité Transition numérique
- Maintenir les registres de sécurité à jour
- Analyser les tendances de menaces informatiques Transition numérique
- Gérer la sécurité informatique Transition numérique

Coopération, Organisation et Développement de ses compétences

- Gérer les situations d'urgence et appliquer les procédures adéquates
- Respecter les normes de sécurité informatique Transition numérique
- Documenter les procédures de sécurité, ainsi que les incidents
- Rapporter les incidents et anomalies rencontrés
- Participer à des réunions de sécurité

Pilotage, Gestion, Cadre réglementaire

- Assurer la conformité réglementaire en matière de sécurité

Développement économique

- Développer des tableaux de bord de sécurité

© Copyright octobre 2026 France Travail - Reproduction et diffusion interdites sans l'accord de France Travail

Management, Social, Soin

- Coordonner les activités avec d'autres équipes techniques
- Former les utilisateurs aux bonnes pratiques de sécurité informatique Transition numérique

Savoir-être professionnels

- Faire preuve de rigueur et de précision
- Etre force de proposition
- Avoir l'esprit d'équipe

Savoirs

Domaines d'expertise

- Analyse forensique numérique Transition numérique
- **Audit de sécurité informatique** Transition numérique
- Evaluation des risques de sécurité Transition numérique
- Gestion des menaces persistantes avancées (APT) Transition numérique
- Veille technologique en sécurité informatique Transition numérique
- Optimisation des processus de sécurité informatique Transition numérique
- Conseil en sécurité informatique Transition numérique

Produits, outils et matières

- Mise en place de solutions de sécurité informatique Transition numérique

Normes et procédés

- Gestion des menaces et des vulnérabilités Transition numérique

Contextes de travail

Conditions de travail et risques professionnels

- En bureau d'études

Horaires et durée du travail

- Travail en astreinte
- Travail en horaires décalés
- Travail selon un rythme irrégulier et des pics d'activité

© Copyright octobre 2026 France Travail - Reproduction et diffusion interdites sans l'accord de France Travail

Publics spécifiques

- Clientèle d'entreprises

Statut d'emploi

- Salarié secteur privé (CDI, CDD)
- Salarié secteur public

Types de structures

- Entreprises et milieux professionnels
- Organisme public

Secteurs d'activité

- Informatique et télécommunication

© Copyright octobre 2026 France Travail - Reproduction et diffusion interdites sans l'accord de France Travail