# M1846
# INGÉNIEUR / INGÉNIEURE CYBERSÉCURITÉ DATACENTER

Emploi cadre

Transition numérique

## Définition

L' Ingénieur Cybersécurité Datacenter est passionné par la protection des infrastructures critiques et la sécurisation des données sensibles, jouant un rôle essentiel en garantissant la résilience et la sécurité des datacenters face aux cybermenaces les plus sophistiquées.

- Assure la sécurité physique et environnementale des datacenters ainsi que de leurs réseaux
- Décide, met en place et surveille les mesures de sécurité et de protection des données stockées dans le Datacenter
- Gère les accès et les identités
- Veille à l'amélioration continue des systèmes de sécurité informatique en surveillant les points faibles du systèmes de protection et en évaluant les facteurs de risque
- Gère les incidents de sécurité et mène des analyses forensiques

## Accès à l'emploi

Ce métier est accessible avec une formation de niveau Bac + 3 à Bac + 5 en informatique ou cybersécurité.
Une certification professionnelle en sécurité des systèmes d'information peut être un atout.

**Certifications et diplômes :**

- Titre professionnel administrateur d'infrastructures sécurisées
- Mastère spécialisé cybersécurité et cyberdéfense
- Mastère spécialisé manager de la sécurité des systèmes d'information
- Mastère spécialisé cybersécurité du numérique

## Compétences

### Savoir-faire

#### Savoir-faire principaux

##### Production, Construction, Qualité, Logistique

- Concevoir et maintenir un système de cybersécurité — Transition numérique
- S'assurer du respect des règles de cybersécurité — Transition numérique
- Anticiper les risques de cybersécurité — Transition numérique
- Gérer les risques de cybersécurité — Transition numérique
- Savoir reconnaître les données sensibles pour la cybersécurité — Transition numérique

### Communication, Création, Innovation, Nouvelles technologies

- Gérer la sécurité informatique — Transition numérique
- Piloter les fonctionnalités des équipements et systèmes de sécurité informatique — Transition numérique
- Déployer des modes de fonctionnement dégradés (solution d'attente) d'un équipement informatique ou bureautique — Transition numérique

### Management, Social, Soin

- Conseiller en matière de prévention, de sécurité et de facteurs de risque

## Savoir-faire secondaires

### Production, Construction, Qualité, Logistique

- Respecter une politique de sécurité de l'information
- Mettre en place des mesures de sécurité
- Réaliser ou participer à la réalisation d'études de risques (identification, recensement, évaluation, ...)
- Définir des mesures de prévention des risques
- Assister la mise en place d'actions de prévention des risques
- Identifier les besoins en logiciel de sécurité — Transition numérique
- Mener un processus de test en cybersécurité — Transition numérique
- Former et informer les salariés pour les sensibiliser à la prévention des risques
- Piloter un audit interne de sécurité réalisé par un prestataire externe
- Garantir le bon fonctionnement, la disponibilité et la performance d'une solution logicielle — Transition numérique

### Communication, Création, Innovation, Nouvelles technologies

- Concevoir des architectures de sécurité — Transition numérique
- Paramétrer un logiciel, un outil, un système numérique — Transition numérique
- Faciliter l'accès aux technologies numériques — Transition numérique
- Déterminer des axes d'évolution technologiques — Transition numérique
- Surveiller les évolutions technologiques des systèmes d'information et de télécommunications et proposer des solutions techniques — Transition numérique

### Coopération, Organisation et Développement de ses compétences

- Suivre les évolutions réglementaires
- Respecter les règles de sécurité
- Garder son sang-froid dans une gestion de crise

### Pilotage, Gestion, Cadre réglementaire

- Rédiger des rapports de sécurité
- Intégrer les normes réglementaires et standards internationaux

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

# Savoir-être professionnels

- Faire preuve d'autonomie
- Etre force de proposition
- Avoir l'esprit d'équipe

# Savoirs

## Domaines d'expertise

- Firewalls et systèmes de détection d'intrusions — Transition numérique
- Systèmes de gestion de base de données
- Modèle informatique client-serveur — Transition numérique
- Informations chiffrées ou codées — Transition numérique
- Cryptologie
- Génie logiciel — Transition numérique
- Intelligence artificielle — Transition numérique

## Normes et procédés

- Procédures qualité et sécurité des systèmes d'information et de télécoms
- Protection des données numériques — Transition numérique
- Règlement Général européen sur la Protection des Données (RGPD) — Transition numérique
- Gestion des risques (Risk Management)
- Test de pénétration et évaluation de la sécurité — Transition numérique
- Méthodes d'analyse (systémique, fonctionnelle, de risques, ...)
- Norme ISO/IEC 27001
- Droit du numérique — Transition numérique
- Sécurité physique des datacenters — Transition numérique

## Produits, outils et matières

- Logiciels anti-virus et anti-malware — Transition numérique
- Analyseur de protocole de télécommunication — Transition numérique
- EDR, NDR, XDR, scanner de vulnérabilité — Transition numérique

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

# Contextes de travail

## Conditions de travail et risques professionnels

- Déplacements professionnels
- En bureau d'études
- Possibilité de télétravail
- Travail en mode projet

## Horaires et durée du travail

- Travail en astreinte
- Travail les week-ends et jours fériés
- Travail selon un rythme irrégulier et des pics d'activité

## Statut d'emploi

- Profession libérale
- Salarié secteur privé (CDI, CDD)

# Secteurs d'activité

- Informatique et télécommunication

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