

**M1846****INGÉNIEUR / INGÉNIEURE CYBERSÉCURITÉ DATACENTER**Emploi  
cadreTransition  
numérique

## Définition

Passionné(e) par la protection des infrastructures critiques et la sécurisation des données sensibles, l'Ingénieur(e) Cybersécurité Datacenter joue 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

Cet emploi 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. Les formations de niveau Bac+5 sont privilégiées.

### 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
- S'assurer du respect des règles de cybersécurité
- Anticiper les risques de cybersécurité
- Gérer les risques de cybersécurité

Transition numérique

Transition numérique

Transition numérique

Transition numérique

## Communication, Création, Innovation, Nouvelles technologies

- Gérer la sécurité informatique
- Savoir reconnaître les données sensibles pour la cybersécurité
- Piloter les fonctionnalités des équipements et systèmes de sécurité informatique
- Déployer des modes de fonctionnement dégradés (solution d'attente) d'un équipement informatique ou bureautique

Transition numérique

Transition numérique

Transition numérique

Transition numérique

## Management, Social, Soins

- Conseiller en matière de prévention, de sécurité et de facteurs de risque liés à l'informatique

Transition numérique

## Savoir-faire secondaires

### Production, Construction, Qualité, Logistique

- Respecter la 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
- Mener un processus de test en cybersécurité
- Piloter un audit interne de sécurité réalisé par un prestataire externe
- Former et informer les salariés pour les sensibiliser à la prévention des risques
- Garantir le bon fonctionnement, la disponibilité et la performance d'une solution logicielle

Transition numérique

Transition numérique

Transition numérique

## Communication, Création, Innovation, Nouvelles technologies

- Concevoir des architectures de sécurité robustes
- Paramétrer un logiciel, un outil, un système numérique
- Déterminer des axes d'évolution technologiques
- Surveiller les évolutions technologiques des systèmes d'information et de télécommunications et proposer des solutions techniques

Transition numérique

Transition numérique

Transition numérique

Transition numérique

## Coopération, Organisation et Développement de ses compétences

- Suivre les évolutions réglementaires
- Respecter des 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

# Savoir-être professionnels

---

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

## Savoirs

---

### Domaines d'expertise

- Sécurité physique des datacenters
- Firewalls et systèmes de détection d'intrusions
- Systèmes de gestion de base de données
- Modèle informatique client-serveur
- Technologies de l'accessibilité numérique
- Informations chiffrées ou codées
- Cryptologie
- Génie logiciel
- Intelligence artificielle

Transition numérique

Transition numérique

Transition numérique

Transition numérique

Transition numérique

Transition numérique

Transition numérique

### Normes et procédés

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

Transition numérique

Transition numérique

Transition numérique

Transition numérique

### Produits, outils et matières

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

Transition numérique

Transition numérique

Transition numérique

## 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