

Technicien(ne) systèmes et réseaux Orienté Cybersécurité

PRÉSENTATION

Nous vivons dans un monde où des menaces existent. Ces menaces prennent une forme explicite, de la simple malveillance au terrorisme et au crime organisé, ou une forme implicite, comme les défaillances matérielles, les erreurs humaines ou les caprices de la nature.

Les systèmes d'information prennent une place de plus en plus importante dans l'activité des entreprises ainsi que dans la vie privée. On observe dorénavant un développement de la virtualisation, l'arrivée à maturité de la mobilité, et l'explosion du Cloud Computing.

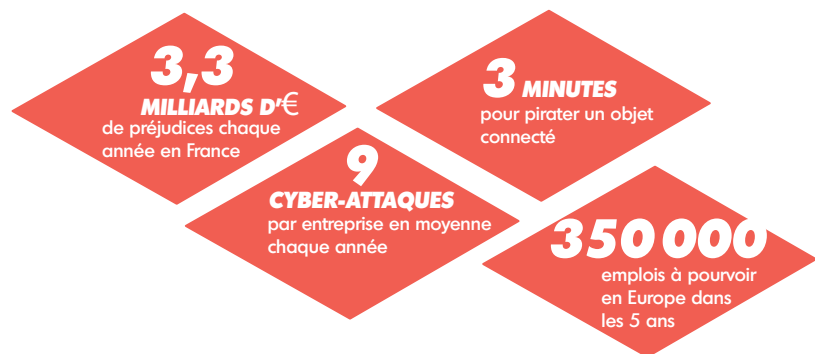
Ce dernier ouvre toujours plus les systèmes d'information vers l'extérieur, et ne fera que renforcer la criticité de la sécurité (site internet, ordinateur portable, smartphone, réseaux sociaux tels que twitter ou Facebook, ainsi que les objets connectés comme les véhicules, les réfrigérateurs, ...).

Le facteur de vulnérabilité augmente donc vis-à-vis de cette modification de notre mode de vie. Plus de 80% des entreprises françaises ont déjà été victimes de vols d'information. En 2015, le préjudice des cyberattaques était de 3,3 Milliards d'euros en France. La firme McAfee avait estimé entre 300 et 1000 milliards de dollars les pertes mondiales engendrées par les cybercriminels.

La sécurité des réseaux d'information est aussi critique pour la souveraineté nationale :

- Espionnage industriel et militaire, altération des services clés (énergie, réseaux, finance, etc.)
- Cyber terrorisme
- Cyber criminalité, cyber défense
- Vol d'ordinateurs dans des chambres d'hôtels
- Pénétration d'agents à l'occasion d'une visite, piratage de technologie...

Dans ce contexte, la place du Technicien(ne) systèmes et réseaux» orienté Cyber Sécurité devient primordiale.



La formation au métier de Technicien(ne) systèmes et réseaux» orienté Cyber Sécurité permet d'acquérir les compétences pour devenir un véritable acteur de la sécurisation des données.



OBJECTIFS

À l'issue de la formation, les stagiaires sont capables de :

- **Cerner les besoins de sécurité** des entreprises afin de pouvoir y répondre efficacement ;
- **Savoir identifier les vulnérabilités** d'un système d'information et être force de proposition dans une logique d'amélioration ;
- **Savoir rédiger un dossier d'architecture** sécurité pour un système d'information ;
- **Savoir développer une application** en prenant en compte les bonnes pratiques de sécurisation de code ;
- **Acquérir un savoir-faire opérationnel** pour communiquer et promouvoir efficacement sa solution de sécurisation de système d'information.

Nous contacter



0805 62 23 45

Numéro vert



/Webforce3

Pour vous inscrire aux

prochaines réunions d'information,
inscrivez-vous sur notre site
Internet: webforce3.fr

Webforce3 - 18 rue Geoffroy l'Asnier - 75004 PARIS - info@wf3.fr



PROGRAMME

La formation est dispensée autour de **6 blocs de compétences** principaux :

1. Acquérir les bases de l'architecture réseau d'un système d'information ;
2. Acquérir les bases de l'architecture système d'un système d'information ;
3. Comprendre et mettre en place des architectures réseau sécurisées ;
4. Comprendre et mettre en place des architectures système sécurisées ;
5. Développer, produire des sites et applications web sécurisés ;
6. Savoir communiquer de manière professionnelle sur ses solutions techniques.



MOYENS PÉDAGOGIQUES, TECHNIQUES ET D'ENCADREMENT

Méthodes pédagogiques

- 30% de théorie
- 70% de pratique

Moyens et supports utilisés

- Ressources numériques (LMS) : plateforme d'apprentissage en ligne avec fiches de révision, QCM, exercices et vidéos.
- Diaporamas

Encadrement

Par des professionnels en activité (experts système, réseaux, cyber sécurité, développeurs, etc.).



CONDITIONS D'ACCÈS

Public concerné

- Tout public

Prérequis

- Niveau IV (Baccalauréat ou niveau Bac) ou autodidacte
- Utilisation courante de l'ordinateur
- Bon niveau de culture générale
- Projet professionnel motivé



MODALITÉS DE SÉLECTIONS

- **Tests** de logique, de culture générale web et informatique
- **Entretiens individuel**
- **Parcours de formation individualisé** en fonction des prérequis et du projet professionnel des candidats.



ÉVALUATIONS ET VALIDATION

Pendant la formation

Evaluations théoriques et pratiques.

À l'issue de la formation

Présentation devant un jury RNCP pour l'obtention du **Titre professionnel TSSR (niv. III) : «Technicien Supérieur Systèmes et Réseaux».**

Code RNCP 31115 / Code NSF : 326 Informatique, traitement de l'information, réseaux de transmission..



DURÉE

Formations intensives :

3 mois (399 h) à 4,5 mois (602 h) en centre de formation + Stage en entreprise (environ 2 mois)

Formations en alternance :

1 an, dont 420 heures en centre de formation, complétées par un stage en entreprise.



DATES ET LIEU

Dates : nous consulter

Lieu : nous consulter

Nous contacter

 **0805 62 23 45**

Numéro vert



/Webforce3

Pour vous inscrire aux

prochaines réunions d'information,

inscrivez-vous sur notre site

Internet: webforce3.fr

Webforce3 - 18 rue Geoffroy l'Asnier - 75004 PARIS - info@wf3.fr