Informatique / Réseaux et télécommunications

Titre de niveau 5 (ex III) | Contrat d'apprentissage |
RNCP 38290

# Titre Opérateur en CyberSécurité (TE_OCS)

## PRÉSENTATION

### Présentation de la formation

La formation d'Opérateur Cybersécurité prépare à la fonction de Technicien Systèmes et Réseaux dominante cybersécurité.

Objectifs :
- Garantir le bon fonctionnement des réseaux informatiques,
- Superviser les applications logicielles,
- Administrer et gérer la maintenance des parcs informatiques.

La sécurité étant incluse dans toutes les matières et 20% des cours traitant spécifiquement de cyber sécurité, ils sont capables d'appliquer les mesures nécessaires à la protection des réseaux d'une organisation.

Par cette formation, l'EECS forme des collaborateurs de niveau N1 voire N2 des ingénieurs.
Les diplômés qui le souhaitent peuvent naturellement poursuivre au-delà de Bac + 2.

### Métiers visés

Environnement : grandes entreprises (informatique, énergie, télécom...), SOC, entreprises des services du numérique, administration publique (Ministère de la Défense, Intérieur...), collectivité locales, hôpitaux, PME...
- Technicien/Administrateur système et réseau dominante cybersécurité.
- Gestionnaire de la sécurité des données, des réseaux et des systèmes.
- Technicien support.
- Technicien maintenance.
- Analyste SOC (Security Operationnal Centre)/détection d'incident.

## Rythme d'alternance

Année 1 :
- Phase 1 : remise à niveau intensive 175 premières heures soit 5 semaines. La formation s'effectue à temps plein au sein de l'école.
- Phase 2 : trois jours en entreprise et deux jours en école des semaines 6 à 18 incluses. A partir de la semaine 19 à la fin de l'année universitaire, l'alternant est 100% en entreprise.

Année 2 :
- Phase 3 : semaines 1 à 24 incluse : 2j en école + 3 j en entreprise.
- Phase 4 : A partir de la semaine 25 jusqu'à la fin de l'année universitaire, l'alternant est 100% en entreprise

## Dates de la formation et volume horaire

1 ère année : 13/09/2023 > 12/09/2025 (504 heures)
2 ème année : 14/09/2023 > 13/09/2024 (504 heures)
Durée : 2 ans
Nombre d'heures : 1008h

# UNIVERSITE/ECOLE

## Adresse administrative Composante

Ecole Européenne de Cyber Sécurité

7 Rue des Réservoirs

78000 - VERSAILLES

Journées Portes ouvertes

Le 22/11/2023

## Siège Établissement

Ecole européenne d'intelligence économique

7 Rue des Réservoirs

78000 - VERSAILLES

# ADMISSION

## Conditions d'admission

### Pré-requis :

- Forte appétence pour les réseaux informatiques et le code, curiosité, autonomie, éthique.
- Niveau BAC, spécialisation informatique souhaitable
- La sélection est faite grâce à un Q.C.M. et un entretien de motivation.
- Le programme est ouvert aux jeunes en continuité de formation post-terminale, aux personnes en reconversion professionnelle ou en congés de formation.

### Année 1 :

Remplir les pré-requis.
Avoir signé un contrat d'alternance (apprentissage ou contrat pro) d'au moins 24 mois avec une entreprise.

### Année 2 :

Idem A1

## Modalités de candidature

1° Inscription des candidats en ligne
Dossier d'inscription gratuit (aucun frais de dossier, etc.) par Internet, avec des questions sur le parcours du candidat et examen du CV.

2° Test de sélection
Afin que les candidats puissent évoluer dans les meilleures conditions, un test de sélection permet de définir si le postulant a le niveau requis pour intégrer la formation. Ce test, non éliminatoire, aide l'encadrement à orienter l'élève vers une formation courte de remise à niveau avant d'intégrer la formation d'Opérateur.trice en cybersécurité.

3° Entretien avec le candidat
Pour chaque candidature, un entretien individuel est obligatoire.
Cet entretien structuré en plusieurs parties vise à :
- Valider le parcours du candidat
- Mesurer ses compétences
- Vérifier sa motivation
- Évaluer son projet professionnel

L'entretien permet de s'assurer que le candidat sera en adéquation avec la formation proposée.

4° Réunion du conseil pédagogique pour constituer une promotion.

# CONTACTS

## Vos référents FORMASUP PARIS IDF

**Héloïse AVERLAN**

contact@formasup-paris.com

**Soumia EL MALLOULI**

Pour les publics en situation de handicap (RQTH ou non) : consultez notre page Alternance et Handicap

## Vos contacts « École/Université »

**Contact**

contact@eecs.fr

# PROGRAMME

## Code RNCP 28290

## Direction et équipe pédagogique

La formation apporte les compétences et connaissances nécessaires au bon déroulement de la mission quotidienne d'un technicien système et réseaux informatiques en entreprise, et d'opérateur au sein d'un SOC.

La formation s'appuie sur 6 piliers :
1. Maîtriser les principes de la programmation
2. Connaître le fonctionnement des différents systèmes d'exploitation
3. Comprendre le fonctionnement des bases de données relationnelles et savoir les administrer
4. Maîtriser le fonctionnement des réseaux
5. Superviser et sécuriser les réseaux et les échanges
6. Maîtriser les bases du hacking

## Programme détaillé de la formation

| | Volume horaire session 2024 - 2025 année 1 | Volume horaire session 2024 - 2025 année 2 |
|---|---|---|
| Scripting | 100h | |
| Réseaux | 200h | |
| Systèmes d'exploitation | 80h | |
| Base de données relationnelles | 40h | |
| Maîtriser les bases du hacking | 44h | 136h |
| Sécurisation des réseaux et échanges | | 120h |
| Supervision réseaux | | 100h |
| Comprendre son environnement professionnel | | 28h |
| TOEIC | 20h | 60h |
| Certifications | 20h | 60h |

## Modalités pédagogiques

- remise à niveau en ligne avant le début de la scolarité
- cours à l'EECS
- travaux pratiques au sein de l'EECS et dans des lieux publics
- visite d'entreprises
- travaux personnels

- alternance en entreprise avec le soutien d'un tuteur ou maître d'apprentissage
- coordination entre le tuteur et l'EECS
- témoignages
- retour d'expérience à l'issue des phases majeures en entreprise

## Contrôle des connaissances

Le contrôle des connaissances est réalisé essentiellement lors de mises en situations professionnelles. Il est complété par un contrôle plus théorique le plus souvent à base de QCM, d'épreuves écrites individuelles, par la présentation d'une étude de cas soumise par une entreprise et par un compte-rendu effectué sur les périodes réalisées au sein des entreprises.

### Année 1 :

Scripting : automatisation de tâches répétitives, lecture de scripts d'exécution contenant des vulnérabilités.
Gestion d'un parc : mise en place d'un serveur windows avec un cahier des charges, idem sur linux, idem sur serveurs virtualisés et les interconnecter.
Administration d'une base de données : installation et administration d'une base de données.
Configuration et administration d'un réseau : mise en place d'un réseau avec Cisco Packet Tracer + QCM sur le choix des composants physiques nécessaires. Parametrage d'un routeur et utilisation d'un commutateur. Mise en place d'une connexion sécurisée. Configuration de réseaux locaux
Surveillance des réseaux : utilisation d'un système de visualisation et d'interprétation des logs.

### Année 2 :

Protection des SI : application des règles de gestion d'accès en utilisant un IAM. Durcissement de postes linux et windows. Chiffrement d'une communication en deux utilisateurs en utilisant un chiffrement asymétrique. Application de règles de parefeu.
Sécurisation des réseaux sans fil : attaque d'un réseau sans fil WLAN.
Sécurisation d'un réseau d'entreprise : attaque d'une réseau LAN d'entreprise.
Sécurisation des applications web : attaque d'un site web pour prendre le contrôle d'un serveur.

## Diplôme délivré

Tite de niveau 5 Opérateur en cybersécurité. Diplôme d'Etat délivré par l'Ecole Européenne de Cybersécurité, faisant partie de l'Ecole Européenne d'Intelligence Economique.

# COMPÉTENCES

Le diplômé est apte à tenir un poste de technicien systèmes et réseaux, opérateur cybersécurité dans un SOC et en entreprise. A savoir :

- Installation et administration courante de systèmes et réseaux
- Analyse et interprétation des différentes remontées des alertes issues du centre de supervision

- Anticipation des nouveaux modes opératoires des cyber criminels
- Reporting et documentation

## Activités

- rédaction de scripts
- analyse de programmes informatiques, détection de vulnérabilités
- gestion d'un parc, administration d'un système, appréhension des risques
- application de standards et de correctifs
- configuration de serveurs et sécurisation de leurs accès
- administration de bases de données, mise en oeuvre de requêtes
- paramétrage
- détection
- configuration de VPN
- veille technologique
- virtualisation de serveurs
- gestion d'identités et d'accès

### Année 1 :

- rédaction de scripts
- analyse de programmes informatiques, détection de vulnérabilités
- gestion d'un parc, administration d'un système, appréhension des risques
- application de standards et de correctifs
- configuration de serveurs et sécurisation de leurs accès
- administration de bases de données, mise en oeuvre de requêtes
- paramétrage
- détection
- configuration de VPN
- veille technologique
- virtualisation de serveurs
- gestion d'identités et d'accès

### Année 2 :

- supervision de réseaux d'entreprise
- paramétrage d'outils d'analyse
- analyse de la menace
- chiffrement
- mise en place de parefeu
- cartographie de la vulnérabilité d'un réseau
- attaques variées de réseaux sans fil

- attaque de routeur
- exploitation de différentes vulnérabilités

## Réaliser des tâches de programmation

- - Développer des scripts d'automatistion des tâches
- Analyser un programme informatique
- - Déceler des menaces potentielles

## Configurer et administrer un réseau d'entreprise

- - Administrer un réseau d'entreprise
- Configurer un NAT et un DNS
- Calculer, gérer les adressages
- - Paramétrer les applications
- Déployer et gérer les réseaux à accès
- Choisir les supports de transmission
- - Paramétrer les réseaux domiciles
- Choisir les solutions cellulaires
- Installer un réseau
- Configurer les VPN
- Configurer les réseaux sans fil
- Choisir le type de réseau sans fil

## Configurer et administrer systèmes et applications dans un environnement virtualisé

- - Gérér un parc
- Assurer le fonctionnement d'un système d'exploitation
- Administrer un système
- - Appliquer les correctifs
- Déployer des applications

## Superviser et sécuriser les réseaux et échanges

- - Utiliser les outils de manipulation des fichiers de logs
- Paramétrer les outils d'analyse
- Administrer, détecter
- - Analyser le niveau de menace, la classerselon le niveau de criticité
- Sécuriser les réseaux et échanges
- - Durcir les postes linux et windows
- Appliquer les principes de cryptographie, mettre en place une politique de chiffrement
- Mettre en place des règles de filtrage

## Installer et gérer des bases de données relationnelles

- - Administrer des bases de données de type relationnel
- - S'appuyer sur la méthode MERISE
- Effectuer des requêtes
- Gérer la conception des bases de données
- - Appliquer les règles de sécurité sur une base de données relationnelles

## Tester la sécurité d'un réseau informatique avec les méthodes de hacking

- - Attaquer un réseau sans fil par les vulnérabilités de chiffrement WLAN et en visant l'infrastructure
- - Attaquer un réseau sans fil WPA-E et Radius
- Attaquer un réseau sans fil type WPS et Probe
- - Utiliser les vulnérabilités d'un réseau dans le cadre de l'attaque d'un routeur, de la post exploitation, de postes clients, d'attaques avancées, de phases de reconnaissance et d'exploitation...