# Consultant Cybersécurité

**Formation labellisée SECNUMEDU-FC par l'ANSSI**

**Nombre de places disponibles par session** : 20

**Rémunération moyenne en sortie de formation** : 35 à 50 K€/an* selon profil et expérience

**Durée et lieu de la formation** : 50 jours à Nanterre (92) – ou à distance le temps de la crise sanitaire

* moyenne constatée des recruteurs participant avec une variation possible selon expérience et compétences

**Prochaines dates de formation**

*Consulter notre site web*

https://www.devenez.fr/espace-candidats/les-offres-en-cours/consultant-en-cybersecurite/

## PROFIL RECHERCHE

- **Bac+2 à 5**, diplômé de l'enseignement supérieur en informatique ou d'écoles d'ingénieur orientée NTIC, (Bac+2 acceptés si expérience en réseau, système ou programmation).

Compétences techniques :

- Curiosité et le goût pour l'expertise technique et pour les **nouvelles technologies**.
- Bonnes bases en système et en **réseau**.
- Connaissances de base en programmation (idéalement sur le langage Python) seraient un plus.

Savoir être :

- **Autonomie** et organisation.
- Bon niveau de communication et forte capacité à fournir un suivi de votre activité.
- Bonne capacité d'**analyse** et de **synthèse**.
- **Rigueur et** méthode.
- Capacité à travailler **en équipe** et à respecter des procédures.

## DESCRIPTIF MÉTIER

Le consultant cyber appréhende le fonctionnement des attaques informatiques, identifie les **menaces** et les **enjeux** de la Cybersécurité.

Cette formation vise à former au concept de sécurité à partir de **méthodes**, **techniques**, **bonnes pratiques** et **outils** destinés à protéger les ressources afin d'assurer la disponibilité des services, la confidentialité des informations et l'intégrité des systèmes.

Ce parcours de formation s'articule autour d'un compromis entre la **gouvernance** et la **technique** sur une infrastructure traditionnelle tout en initiant à la sécurité **cloud** et **mobile**.

En tant que Consultant Cybersécurité, vous serez en charge :

- D'analyser, de préconiser et de valider des solutions techniques en matière de sécurité des SI,

# Consultant Cybersécurité

**Formation labellisée SECNUMEDU-FC par l'ANSSI**

- D'administrer les solutions déployées dans ce domaine,
- D'intervenir dans les études de cartographie des risques des systèmes d'information,
- De réaliser des audits de configuration et de résistance des systèmes aux risques cyber (analyses de vulnérabilités, tests d'intrusions, RedTeam),
- D'opérer la mise en conformité réglementaire des organisations dans lesquelles vous interviendrez (ex. norme PCI-DSS, règlement GDPR, directive européenne NIS).

## CERTIFICATION

- **Certificat de Compétences Professionnelles « Implémenter la cybersécurité en entreprise »**

## APPROCHE PÉDAGOGIQUE ET MODALITÉS D'ÉVALUATION

### FORMATEUR ET PÉDAGOGIE

Cette formation à 4 objectifs :

- Analyser, de préconiser et de valider des solutions techniques en matière de sécurité des SI.
- Administrer les solutions déployées dans ce domaine.
- Intervenir dans les études de cartographie des risques des systèmes d'information.
- Réaliser des audits de configuration et de résistance des systèmes aux risques cyber (analyses de vulnérabilités, tests d'intrusions).

Cette formation est composée de quatre volets :

- Un volet **gouvernance**
- Un volet **technique**
- Un volet de **compétences transverses** (savoir-être et méthode)
- Un volet de mise en situation pratique

Chaque formateur à une double casquette celle d'**expert** et de **pédagogue**. C'est cette double compétence qui garantit une acquisition de compétences optimum pour chaque stagiaire.

L'organisation pédagogique privilégie les **aspects pratiques** (70% du temps de la formation) : démonstrations, travaux pratiques, simulation, travaux dirigés et rapportés.

### QUALITÉ DES CONDITIONS TECHNIQUES

Un formateur anime le cours sur un **groupe Teams**, partage sa **vidéo** et son **écran**, diffuse ses **supports**, met une **base documentaire** à disposition, **interagit** avec les stagiaires, lance les TP sur des outils et plateformes cloud, peut **prendre la main** sur les postes.

### MODALITÉS D'ÉVALUATION - VALIDATION DE LA MISE EN OEUVRE DE LA COMPÉTENCE

Les cursus complets sont validés par la **réalisation d'un projet de 5 jours** et par une **soutenance en ligne face un jury** de professionnels du métier.

Toute notre approche pédagogique est basée sur le respect des critères de la norme ISO 9001.

# Consultant Cybersécurité

**Formation labellisée SECNUMEDU-FC par l'ANSSI**

## PROGRAMME DE FORMATION

| Catégorie | Modules | Durée en Jours |
|---|---|---|
| Savoir-Faire Métier - Compétences transverses | **Introduction à la cybersécurité** | 1 |
| | • Aborder les **termes** et **définitions** de la sécurité des systèmes d'information.<br>• Découvrir les **métiers** de la cybersécurité.<br>• Termes et définitions | |
| | **La continuité d'activité & les normes et référentiels de SMSI** | 4 |
| | • Découvrir les normes ISO **27001**, Management de la sécurité de l'information et ISO **22301**, référence internationale en continuité d'activité.<br>• Intégrer l'**amélioration continue.**<br>• Garantir une haute disponibilité avec un **PCA** et **PRA** pour le SOC.<br>• Introduction à l'ISO 19011 : référence internationale en matière d'audit.<br>• Introduction à l'ISO 22301 : référence internationale en Continuité d'activité.<br>• Réaliser un atelier de mise en œuvre d'un plan de continuité d'activité conforme à l'ISO 27001 et ISO 22301. | |
| | **Protection des données personnelles** | 2 |
| | • Définir les **aspects juridiques** du RGPD.<br>• Comprendre l'importance des obligations du RGPD.<br>• S'assurer de la **licéité du traitement**.<br>• Réaliser une **analyse d'impact** relative à **la protection des données**.<br>• Tenir le **registre des activités** du traitement.<br>• Parcourir la taxonomie des données.<br>• Évaluation du **risque** associé au RGPD. | |
| | **ITIL v4 : l'essentiel** | 1 |
| | • Comprendre la **terminologie** et les **concepts** d'ITIL.<br>• Identifier les **principes directeurs** d'ITIL 4 pouvant aider une organisation à adapter le management des services.<br>• Acquérir les 4 dimensions de la **gestion des services.**<br>• Comprendre la **valeur ajoutée** d'ITIL. | |
| Savoir-être | **Préparer et animer une présentation** | 2 |
| | • **Concevoir** et **animer** une présentation.<br>• Mettre en scène l'information pour la rendre plus **attractive**. | |
| | **Adopter la posture attendue en milieu professionnel** | 1 |
| | • Être capable de **se présenter** dans un temps limité et savoir **se vendre en entretien**.<br>• Être capable de répondre à une question dans un temps limité.<br>• Apprendre à présenter le résultat d'un travail, par **écrit** et à l'**oral**.<br>• Apprendre à **gérer les conflits** et **travailler en équipe** et à **respecter des procédures.** | |
| Compétences techniques | **Réseaux et sécurisation des réseaux** | 3 |
| | • Parcourir les **bases réseaux** nécessaires à la bonne interprétation des outils de la cyber.<br>• Comprendre les protocoles réseaux aussi que leurs **failles** & **remédiations** associées.<br>• Mettre des mesures de protection et durcissement avec des **VLAN**s.<br>• Aborder les différences et points communs entre l'**IPV4** et l'**IPV6.**<br>• Explorer les **vulnérabilités WI-FI.**<br>• Découvrir les **vulnérabilités** spécifiques de l'**ARP** et l'**ICMP.**<br>• Analyser le **routage forcé** de paquets IP (source routing).<br>• Étudier le fonctionnement : | |

# Consultant Cybersécurité

**Formation labellisée SECNUMEDU-FC par l'ANSSI**

| Catégorie | Modules | Durée en Jours |
|---|---|---|
| | ○ De la **fragmentation IP** et les règles de réassemblage.<br>○ Des attaques par déni de service.<br>○ De la prédiction des **numéros de séquence TCP**.<br>○ Du vol de session TCP : hijacking (Hunt, Juggernaut).<br>○ De l'attaque par **TCP Spoofing** (Mitnick).<br>○ De l'attaque DNS **Dan Kaminsky**.<br>○ De l'attaque **sslstrip** et **sslsnif**. | |
| | **Administration et durcissement Linux** | **3** |
| | • Gérer des **droits** - Sécurité des programmes avec **AppArmor**.<br>• Partitionnement et systèmes de fichiers - LVM - GRUB & Secure-Boot.<br>• **Durcir** Debian 11 - **Signaux** et **processus**<br>• Gérer des **paquets** - Service/**systemctl** - Gestion des logs – **Nftables**<br>• Décryptage de la **journalisation** locale.<br>• Découvrir **Kali** Linux | |
| | **Concepts et règles d'architectures sécurisées** | **2** |
| | • Découvrir les **méthodes de conception** d'une architecture sécurisée.<br>• Apprendre à se protéger « by design » :<br>• Étudier la conception d'architecture de sécurité défensive par le **cloisonnement cinématique des flux** et la **rupture protocolaire**.<br>• Générer une **matrice de flux**.<br>• Configurer une **DMZ**.<br>• Comprendre le principe des « **pots de miel** » (Honeypots).<br>• Réaliser une étude de cas. | |
| | **Sécurité des systèmes mobiles** | **2** |
| | • Découvrir les fondamentaux de la sécurisation des systèmes mobiles avec **Android** : architecture, sandboxing, permission, rooting, composantes d'une application.<br>• Réaliser une attaque « **Man-in-the-middle** » sur Android.<br>• Mettre en place de l'environnement de test virtualisé.<br>• Élever ses privilèges. | |
| | **Administration et durcissement Windows** | **3** |
| | • Comprendre le **durcissement** de Windows.<br>• Décryptage de la **journalisation** locale.<br>• Installer **Windows Serveur 2022**.<br>• Activation et **configuration du domaine.**<br>• Activation et configuration du service **Active Directory.**<br>• Détecter une **intrusion administrateur** dans l'Active Directory (l'agent WinlogBeat). | |
| | **Web intelligence, google hacking, deep web, Ingénierie sociale, prise d'empreintes** | **2** |
| | • Découvrir la **cyber Kill Chain**, à l'**OSINT**, aux techniques de **prise d'empreinte**.<br>• Identifier les mécanismes cryptographiques employés par les **ransomwares**.<br>• S'exercer avec les outils de **Google Hacking** et l'exploration du **Deep Web**.<br>• S'initier à l'**intelligence gathering**.<br>• Étudier les TTP dans un framework MITRE ATT&CK ? | |

# Consultant Cybersécurité

**Formation labellisée SECNUMEDU-FC par l'ANSSI**

| Catégorie | Modules | Durée en Jours |
|---|---|---|
| | **Cryptographie PKI et monnaies virtuelles** | **2** |
| | • Introduction sur les **services** et **concepts** cryptographiques.<br>• S'inciter à l'algorithme **Diffie-Hellman**.<br>• Comprendre de fonctionnement du chiffrements **symétrique** et **asymétrique**.<br>• Étudier l'infrastructure de gestion des clés (IGC/**PKI**).<br>• Utiliser les fonctions de **hachage**.<br>• Connaitre les principes et algorithmes cryptographiques (DES, 3DES, AES, RC4, RSA, DSA, ECC).<br>• Gérer les **certifications** des clés publiques, **révocation**, **renouvellement** et **archivage** des clés.<br>• Découvrir le fonctionnement des **monnaies virtuelles**. | |
| | **Configurer les outils de la sécurité périmétrique (firewall – proxy – IPS - VPN)** | **6** |
| | • Généralités sur les **UTM**.<br>• Découvrir le fonctionnement d'un firewall de **nouvelle génération**.<br>• Identifier les types de **filtrages** et de **firewalls**.<br>• Configurer le **routage** d'un réseau, la **translation d'adresses** dynamique et statique et par port, l'ordre d'application des **règles de NAT**, du **Proxy HTTPS**, de l'analyse **antivirale** de l'**IPS** et du **filtrage** de contenu.<br>• Configurer un **portail d'authentification**.<br>• Mettre en place un tunnel **VPN Ipsec** et **SSL**.<br>• Associer l'**authentification transparente** et la liaison à un **annuaire**.<br>• Exporter les données vers un **SIEM**.<br>• Réaliser un lab complet reprenant tous les éléments ci-dessus avec **Stormshield.** | |
| | **Gérer l'information liée aux incidents, événements et les logs** | **2** |
| | **Gérer l'information liée aux incidents, événements et les logs :**<br>• Comprendre le fonctionnement d'un SIEM au sein d'un SOC.<br>• Apprendre à gérer une variété d'**incidents**.<br>• Configurer l'analyse de **vulnérabilité.**<br>• Comprendre l'analyse des **logs.**<br>• **Collecter** l'information provenant des pare-feu, serveurs et postes de travail.<br>• **Agréger** les logs<br>• **Normaliser** les traces brutes pour obtenir des valeurs probantes.<br>• **Corréler** en appliquant des règles pour permettre d'identifier un événement qui a causé la génération des logs<br>• Créer un **reporting** pour générer des tableaux de bord et des rapports<br>• **Archiver** pour garantir l'intégrité des traces pour des raisons juridiques et réglementaires.<br>• **Rejouer les événements** pour mener des enquêtes post-incidents. | |
| | **Cyber labs - Tests d'intrusion - Détection et remédiation** | **5** |
| | **Méthodologie de l'audit :**<br>• Connaitre les **différents types** de Pentest.<br>• Intégrer le test d'intrusion dans un **processus de sécurité général**.<br>• Apprendre à définir une **politique** de management de la sécurité et d'un Pentest itératif.<br>• **Organiser** et **planifier** l'intervention et préparer le **référentiel** ?<br>• Préparer un **audit**.<br>• Définir les **habilitations**.<br>• Étudier les bonnes pratiques de Penetration Testing Exécution Standard (PTES) | |

79-105 avenue François ARAGO 92000 NANTERRE - Tél. : 01 55 70 80 90 - Fax : 01 47 89 16 08 - E-mail : info@fitec.fr
S.A au Capital de 450 000 euros - n° SIRET 349 640 003 00100 - n° d'identification intracommunautaire FR 45349640003
Code APE 8559A - n° de déclaration d'existence : 11921557492

# Consultant Cybersécurité

**Formation labellisée SECNUMEDU-FC par l'ANSSI**

| Catégorie | Modules | Durée en Jours |
|---|---|---|
| | **Les outils de Pentest :**<br>• Faire inventaire des principaux outils destinés :<br>• Faire inventaire des principaux frameworks d'exploitation.<br><br>**Vulnérabilités réseau :**<br>• Comprendre le fonctionnement **scanner de port**.<br>• Effectuer des scans de réseaux simples ou en mode "**stealth**".<br><br>**Vulnérabilités système :**<br>• Exploiter les vulnérabilités système avec **Metasploit**.<br><br>**Sécurité des applications Web :**<br>• Connaitre le contenu des champs de l'**en-tête**, codes de status 1xx à 5xx.<br>• Étudier le TOP 10 des vulnérabilités de l'**OWASP**.<br>• Cartographier un site et rechercher des failles avec **VEGA**.<br>• Auditer une application WEB avec **W3af**.<br>• Scanner la sécurité des serveurs web avec **Nikto**.<br><br>**Sécurité WI-FI :**<br>• Exploiter les **vulnérabilités Wi-Fi** WEP et WPA avec **Aircrack** et remédiations associées.<br>• Mettre en pratique la technique de l'**Evil TWIN.** | |
| | **Sécurisation des environnements Cloud** | **2** |
| | • Connaitre les différents **modèles** de cloud computing.<br>• Discerner la **responsabilité** de sécurité « **du** » et « **dans** » le cloud.<br>• Découvrir l'architecture des r**égions** et **zones de disponibilités** du cloud.<br>• Découvrir les fondamentaux de la sécurité cloud avec le « **Cloud Security Knowledge** ». | |
| **Certifications** | **Mise en situation professionnelle - Préparation à la certification professionnelle** | **7** |
| | Mettre en place à travers un cahier des charges l'ensemble des méthodes et technologies vues lors de l'ensemble de la formation. Formalisation et présentation des résultats de l'étude.<br>• Soutenance individuelle devant jury. | |
| | **Durée totale en jours** | **50** |

Note : Ce document n'est pas contractuel et peut faire l'objet de modifications afin de répondre à des impératifs d'ordre pédagogique

# Consultant Cybersécurité

**Formation labellisée SECNUMEDU-FC par l'ANSSI**

## TARIFS ET FINANCEMENTS (possibilité de prise en charge partielle ou intégrale)

Tarif public des formations de 50 jours : 7500 € HT / stagiaire (tarif indicatif)

**Votre formation peut être prise en charge par un organisme de financement. Dans le cadre d'un FNE, POE, AIF, CSP, n'hésitez pas à nous contacter à recrutement@devenez.fr**

En fonction de votre statut au moment de l'entrée en formation (salarié ou demandeur d'emploi), cette prise en charge pourra être **partielle ou intégrale**.
Plus d'informations sur les financements : https://www.devenez.fr/financements/

## MODALITES D'INSCRIPTION ET DELAIS D'ACCES

Délai d'inscription variable selon le mode de financement.

**INSCRIPTION SUR NOTRE SITE INTERNET :**
https://www.devenez.fr/espace-candidats/les-offres-en-cours/consultant-en-cybersecurite/

## ACCESSIBILITÉ :

Public en situation de handicap, contactez notre Référent : M. Olivier BENANOU – o_benanou@devenez.fr

## POUR TOUTE DEMANDE DE RENSEIGNEMENT :

*Nous fabriquons les compétences Cybersécurité*
Kalis Consulting est une société du Groupe FITEC

Communication@kalis-consulting.fr

101-103 avenue Arago - 92000 Nanterre
Bureau : +33 (0)1 42 67 28 48

Site web : www.kalis-consulting.fr

*Version mise à jour le 11/01/2022*