



SPÉCIALISTES DU NUMÉRIQUE

DIPLÔME D'ÉTABLISSEMENT (DE) SÉCURITÉ NUMÉRIQUE EN SANTÉ (SECNUM SANTÉ)

 1 an


 2024-2025





La cybersécurité constitue un enjeu majeur pour les établissements de Santé, qui sont la cible de nombreuses attaques de leurs Systèmes d'Information (SI).

Dans un contexte de données sensibles, de plus en plus partagées au sein de l'écosystème de la Santé, des besoins spécifiques en experts qualifiés et possédant une culture en santé se fait cruellement sentir.

Fort de ce constat, l'ESNbyUM s'associe à Polytech Montpellier pour proposer dès la rentrée 2024 un **nouveau parcours orienté Sécurité en Santé Numérique**.


 **Composante de rattachement :**
Polytech Montpellier


 **Type de diplôme :** Diplôme d'Établissement
Nom du Parcours : Sécurité Numérique en Santé

 **Modalités de formations :** formation continue, contrats de professionnalisation

CONTACT

Responsable du DE SECNUM
Pascal Benoit

 **SECNUM Santé :**
Responsable : Pr Emmanuel Le Clézio
emmanuel.le-clezio@umontpellier.fr
Création Pédagogique
Sabine Mousseau-Tinland
sabine.mousseau-tinland@umontpellier.fr

 **SECNUM Industrie :**
Responsable : Pascal Benoit
polytech-secnum@umontpellier.fr

PUBLIC CIBLE

- Titulaires d'un Bac +5, diplôme ingénieur ou master, dans les domaines de l'électronique, microélectronique et informatique industrielle, informatique.

PARCOURS

DE SECNUM

SECNUM SANTÉ

SECNUM INDUSTRIE

OBJECTIFS

Polytech Montpellier propose une formation de niveau Bac+6, s'adressant à des ingénieurs ou titulaires d'un Master, déjà diplômés de filières telles que l'électronique, l'informatique, les systèmes embarqués (liste non exhaustive) et qui souhaitent acquérir une expertise en cybersécurité.

Cette offre de formation est complétée, dans le cadre de l'ESNbyUM, par un Diplôme d'Établissement en Sécurité Numérique en Santé.

L'objectif du DE SECNUM Santé vise à accroître le nombre d'acteurs économiques ayant des compétences conjointes en cybersécurité et en Santé Numérique, et pouvant déployer et sécuriser des systèmes d'information hébergeant et traitant des données de santé.

COMPÉTENCES

spécifiques apportées par le parcours

- Identifier les acteurs du Numérique en Santé et les grands programmes de transformation numérique
- Identifier le marché de la Santé Numérique
- Maîtriser le cycle de vie de la donnée de santé
- Identifier, analyser et réagir aux différents types d'actions malveillantes
- Respecter et mettre en application le cadre légal et réglementaire d'hébergement et de traitement des données de santé
- Déployer des outils de surveillance et de sécurisation des systèmes d'information en Santé

MODALITÉS PÉDAGOGIQUES

En plus des 335 heures d'enseignements en tronc commun proposées par Polytech Montpellier, l'ESNbyUM propose 55 heures de nouveaux contenus dédiés à la Santé Numérique :

30h en Sécurité des données et systèmes de santé
25h en Aspects réglementaires et juridiques en Santé Numérique

À ces nouveaux enseignements, dispensés par des enseignants de l'Université de Montpellier mais aussi des professionnels du secteur de la Santé (hospitalier, institutionnel), s'ajoutera une orientation santé :

du projet tutoré (100 h),
du stage (560 h)

ALTERNANCE

Que ce soit dans le cadre de la formation continue ou d'un contrat de professionnalisation, la formation est répartie en 3 périodes de 4 semaines chacune, séparées par des périodes en entreprise.

Modalités d'admission : L'admission définitive ne sera prononcée que lorsqu'une entreprise d'accueil se sera engagée dans la signature d'un contrat de formation continue (contrat de professionnalisation ou convention de formation continue).

DIPLÔME D'ÉTABLISSEMENT (DE) SÉCURITÉ NUMÉRIQUE EN SANTÉ (SECNUM SANTÉ)

CONTENU DU PARCOURS

Diplôme d'Établissement Sécurité Numérique en Santé

UE0 : Mise à niveau (18h)

UE1 : Fondamentaux de la cryptologie (63h)

UE2 : Sécurisation des applications embarquées (81h)

- Systèmes embarqués (21h)
- Vulnérabilité et preuve formelle (9h)
- Sécurité des données et systèmes de santé (30h)
- Expérimentation sur plateformes d'analyses (6h)
- Injection de fautes (15h)

UE3 : Sécurisation des réseaux, protocoles et infrastructures (54h)

UE4 : Aspects réglementaires, juridiques et experts de la sécurité numérique (74h)

- Aspects réglementaires et juridiques (17h)
- Gestion de projets (8h)
- Forensic (21h)
- Aspects réglementaires et juridiques en Santé Numérique (25h)

UE5 : Projet ESNbyUM (100h)

UE6 : Module professionnel ESNbyUM (560h)

Diplôme d'Établissement Sécurité Numérique Industrie

UE0 : Mise à niveau (18h)

UE1 : Fondamentaux de la cryptologie (63h)

UE2 : Sécurisation des applications embarquées (81h)

- Systèmes embarqués (21h)
- Vulnérabilité et preuve formelle (9h)
- Conception, techniques d'attaques et contremesures associées (30h)
- Expérimentation sur plateformes d'analyses (6h)
- Injection de fautes (15h)

UE3 : Sécurisation des réseaux, protocoles et infrastructures (54h)

UE4 : Aspects réglementaires, juridiques et experts de la sécurité numérique (74h)

- Aspects réglementaires et juridiques (17h)
- Gestion de projets (8h)
- Forensic (21h)
- Aspects experts (25h)

UE5 : Projet (100h)

UE6 : Module professionnel (560h)

Légende

 École de Santé Numérique

DÉBOUCHÉS PROFESSIONNELS



Domaine du numérique

- Évaluateur Cybersécurité en Santé
- Architecte de sécurité en Santé
- Ingénieur Cybersécurité en Santé
- Ingénieur Systèmes en Santé
- Consultant Cybersécurité en Santé
- Pentesters auprès des établissements et industriels en Santé
- Expert Sécurité des systèmes d'information en Santé

- Auditeur Sécurité des Établissements de Santé
- Développeur Sécurité en Santé
- Analyste Security Operation Center (SOC) en Établissement de Santé
- Responsable Sécurité de l'information en Santé
- Responsable de la sécurité des systèmes d'information en Santé
- Manager de la sécurité et des risques de l'information en Santé