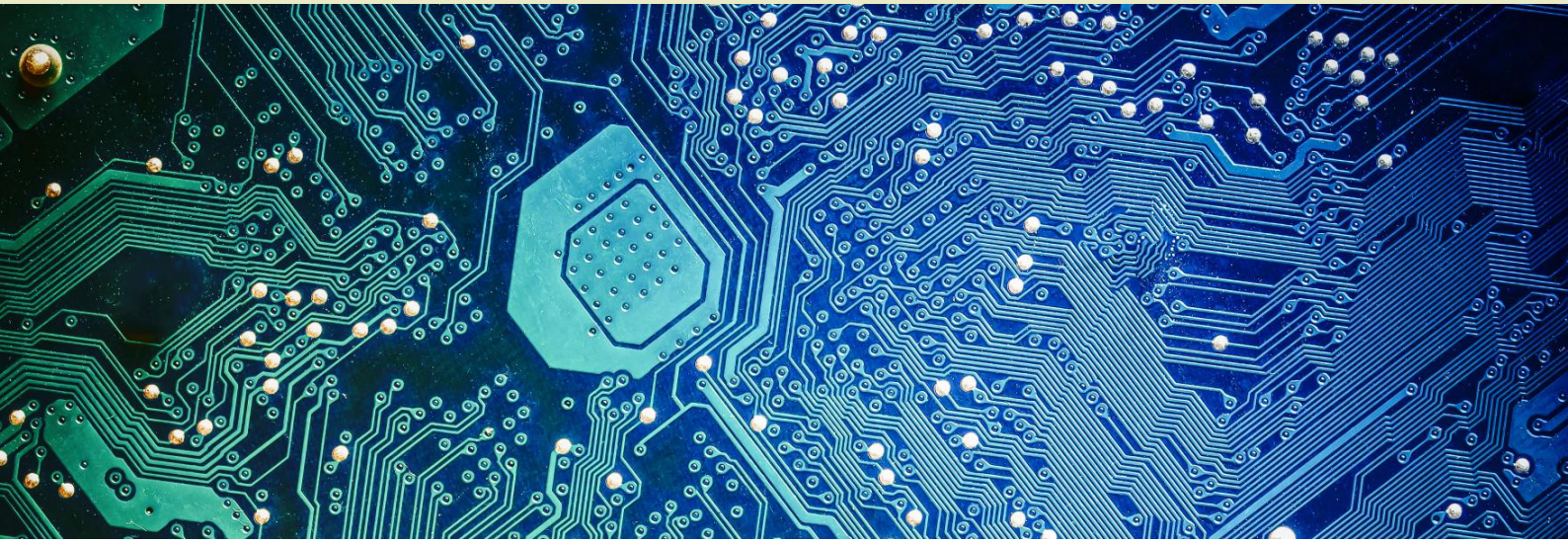
DIPLÔME

Licence professionnelle Sciences, technologies, santé mention Métiers de l'informatique : administration et sécurité des systèmes et des réseaux parcours Cybersécurité et réponse à incident pour les systèmes d'information, indust. et urbains (CRISIS)

Code : LP15401A



Niveau d'entrée : Bac + 2
Niveau de sortie : Bac + 3, Bac + 4
ECTS : 60

Déployabilité
Apprentissage : Fomation pouvant se suivre en apprentissage
Package : Formation pouvant se suivre en s'inscrivant à un "package" (groupe d'enseignements indissociables)
Contrat de professionnalisation : Formation pouvant se suivre en contrat de professionnalisation

Objectifs pédagogiques

L'objectif de la formation est de former des spécialistes en cyber sécurité en mesure de comprendre et d'intervenir sur les infrastructures IT/OT/IoT/IIoT d'opérateurs d'importance vitale (OIV).
Ces infrastructures sont complexes, elles concernent tout aussi bien les capteurs (Cyber Physiqical Systems) en lien direct avec les entités physiques (vannes, ...), les automates (PLC,...) pour réaliser des opérations techniques, et enfin, plus global, le shysteme de contrôle et d'acquisition des données (SCADA)destiné au controle de tous ces équipements et des processus métier. Les SCADA collectent également les données relevées par les netités physiques, en temps réel, même auprès de sites distants.
Ces infrastructures sont sujettes à de nombreuses vulnérabilités, il n'est pas toujours possible de réaliser des mises à jour sur les installations en production continue ou encore en dehors des fenetres de maintenance dont le cycle est parfois de deux ans ! Par ailleurs, la cybersécurité n'a pas été pensée dès la conception, d'autant que les pièces informatiques ont été intégrées plus tard. Pendant longtemps, la cybersécurité de ces ensembles informatiques et physiques ont concerné les grands

groupes industriels, avec la transformation numérique, ce sont les petites et moyennes entreprises du secteur de l'industrie qui deviennent exposées aux cyberattaques.
Selon l'ANSSI, le maintien des conditions de sécurité des systèmes industriels et urbains est une condition majeure du maintien de la sécurité globale, de notre pays mais également au niveau mondial, ces systèmes industriels sont actuellement la cible de nombreuses attaques informatiques.

Compétences et débouchés

La déployabilité du cursus est soumise à validation avec la présence et l'agrément d'un enseignant chercheur dans la responsabilité opérationnelle.
BLOC 1 : Maintien des conditions opérationnelles de sécurité (MCS) et gestion des incidents de sécurité des infrastructures IT OT IoT IIoT
(installer, configurer, superviser, développer)

- Participer à la supervision du MCS de moyens techniques en lien avec le RSSI, le CERT et le SOC
- Participer au traitement des incidents de sécurité en lien avec le SOC et le CERT
- Assurer la mise en place des techniques de sécurité (ségrégation réseau, mot de passe, patch management, droits d'accès physiques et logiques, ...) dans les systèmes informatiques virtualisés ou non (réseaux, postes de travail, serveurs, Active Directory,...) ou dans lesinfratsructures OT (operational technology) d'une entreprise (Automates industriels, Machines de maintenance, supervision SCADA, protocoles industriels, etc.).
- Assurer une veille technologique sur les menaces et techniques d'attaques (CERT, TTP,...) et spéicfiques aux systèmes industriels (CISA, ANSSI,...)
- Intervenir sur la sécurité des systèmes d'information de production ou de maintenance (GMAO/MES/ ERP)
- Installer, intégrer, paramétrer des dispositifs de de collecte et de détection (sondes IDS, SIEM, EDR de type SentinelOne,...) dans les centres de sécurité opérationnelle (SOC) ou de supervision des OT
- Appliquer les bonnes pratiques selon les référentiels informatiques (ISO27002, RGS,...) ou industriels (CEI 61508, IEC 61508, ISO 26262,...)
- Réaliser des scripts d'automatisation sur les dispositifs de sécurité ou sécurisés
- Reprogrammer des automates (PLC,...) en respectant les critères de cybersécurité.

BLOC 2 : Analyse et audit de sécurité des infrastructures IT OT IoT IIoT
(Vérifier, corriger)

- Analyser les vulnérabilités des systemes informatiques à l'aide d'outils de gestion de vulnérabilités (Nessus Tenable,...)
- Analyser les codes malveillants
- Analyser les alertes cybersécurité, investiguer et effectuer le diagnostic technique de ces alertes
- Veiller à l'application
- Assurer une veille technologique sur les solutions de « sécurité »
- Participer à l'évaluation de conformité des systemes d'informatiques ou des projets de développemens (applications, réseaux, systèmes et données)au regard de normes globales en vigueur (NIST, ANSSI,...)
- Participer à l'élaboration des recommandations suite à un audit de sécurité (Mise en place de Firewall, VLAN)

BLOC 3 : Management de projet et conception d'architecture de sécurité de base de la sécurité des infrastructures IT OT IoT IIoT
(Planifier, diffuser, travailler en équipe, rédiger)

- Participer à la conception de projet en prenant en compte les exigences de sécurité spécifique (politique interne, classification des données, etc)
- Préparer et suivre les travaux de sécurisation

- Rédiger, analyser puis suivre les marchés liés aux missions de sécurité informatique des systèmes industriels,
- Participer à toutes les démarches visant à améliorer la sécurité des infrastructure IT ou OT.
- Participer à la définition des procédures qualité et documents internes (RGPD, charte informatique) et de sécurité en lien avec les IT/OT/IoT/IIoT.
- Recenser les besoins de sécurité des utilisateurs, assurer le suivi et proposer des arbitrages (via ticketing, plateforme de pilotage),
- S'impliquer dans les projets en lien avec l'architecture du système d'information et la sécurité,
- Former les collaborateurs du service technique sur les matériels et logiciels choisis
- Aider dans le choix des solutions de sécurité matérielles et logicielles

Méthodes pédagogiques

Les enseignements théoriques, couplés à des mises en application en travaux dirigés et travaux pratiques sur matériels et logiciels métiers permettront une professionnalisation rapide. L'espace numérique de formation du Cnam (Moodle) permet à chaque enseignant de rendre accessible des ressources spécifiques à ses enseignements. Des modalités plus détaillées seront communiquées au début de chaque cours.

Modalités de validation

Devoir final avec jury, contrôle continu par matière avec examen sur table, projet, mise en situation simulée, évaluation individuelle écrite et orale.
Travaux pratiques notés.
Mise en situation simulée d'une cyberattaque sur une ligne de production fonctionnelle equipée de composants industriels (PLC, IoT,....).

Prérequis et conditions d'accès

- Être titulaire d'un diplôme de niveau 5 en informatique : BTS SN, SIO, FED ;
- DUT 2ième année ou BUT informatique, GEII ;
- DPCT informatique ; diplôme analyste programmeur du Cnam ;
- certains titres Afpa homologués au niveau 5.
- Être titulaire d'un diplôme qui dispense des niveaux L1 et L2.

MENTIONS OFFICIELLES

Code RNCP
40102

Date d'enregistrement au RNCP
30/05/2025

Date de l'échéance de l'enregistrement au RNCP
31/08/2030

Mots-clés

Cybersécurité

Informations complémentaires

Type de diplôme
Licence professionnelle

Code NSF
326n - Analyse informatique, conception d'architecture de réseaux

Codes ROME
Analyste en cybersécurité[M1805]

Formacode
Sécurité informatique [31006]

Code du parcours
LP15401

Modules d'enseignement

- → Analyse de la menace, des attaques et des vulnérabilités des CPS et SCADA
- → Analyse des enjeux principes, doctrines de sécurité : description de la menace, attaques, vulnérabilités
- → Anglais et SHS en anglais/français : compréhension écrite, géopolitique, droit et criminologie, éthiques
- → Architectures SCADA et CPS
- → Base de données et structures de données des SI, ERP, des systèmes industriels, SCADA et MES
- → Développement, algorithmie, langages et programmation d'automate, systèmes embarqués
- → Développement, algorithmie, langages et programmation Java, Web
- → Dispositifs de sécurité : DMZ, Pare-feu, IDS, principes généraux et configuration du SI
- → Dispositifs de sécurité appliqués au systèmes industriels et embarqués
- → Mathématiques générales et appliquées à l'algorithmie et la cryptographie
- → Modélisation et Ingénierie des systèmes : besoin, exigences, conception et architecture
- → Projet et mémoire
- → Réseaux et protocoles, réseaux industriels
- → Système d'exploitation : principes, virtualisation, introduction aux automates et systèmes embarqués

Blocs de compétences

Un bloc de compétences est constitué d'un ensemble d'Unités qui répond aux besoins en formation de l'intitulé du bloc.
Les unités ci-dessus sont réparties dans les Blocs de compétences ci-dessous.
Chaque bloc de compétences peut être validé séparément.

Usage numérique
LP154B11

Exploitation de données à des fins d'analyse
LP154B21

Expression et communication écrites et orales
LP154B31

Positionnement vis à vis d'un champ professionnel
LP154B41

Action en responsabilité au sein d'une organisation professionnelle
LP154B51

Développement et mise en œuvre d'outils de conception et d'analyse
LP154B61