le cnam
Auvergne – Rhône-Alpes

# IAML : IA et du ML pour la cybersécurité

**IAML : IA et du ML pour la cybersécurité**

**SEC201**

## Planning

| Période | Modalité |
|---|---|
| Information Indisponible - Information Indisponible | Formation ouverte et à distance (FOAD) |

## CONDITIONS D'ACCES / PRÉREQUIS

**Avec le niveau Bac+ 4 informatique IMPERATIVEMENT dans la spécialité et être agréé par l'enseignant**

**Avoir validé, suivi et obtenu RCP101 ou RCP105 IMPERATIVEMENT au moment de l'inscription et ne pas suivre ces UE en même temps**

**Les fondamentaux suivants sont demandés : "Représentation vectorielle et matricielle des données", "transformations linéaires", "calcul différentiel et intégral", "calculs statistiques et probabilistes", base de "logique propositionnelle", théorie des graphes, conception de reqûetes de type SQL, etc.**

**Connaitre le langage de programmation python**

**Ne suivre qu'une UE sur ce semestre (pas d'UAMM*, d'ENG*,…)**

**1 ECTS appelle environ entre 20:00 à 30:00 d'effort élève au total.**

## OBJECTIFS PÉDAGOGIQUES

L’objectif pédagogique du cours sera d'apprendre à modéliser et concevoir des moteurs d'apprentissage artificiel simples (ML), supervisés et non supervisés susceptibles d'être utilisés dans un centre de sécurité opérationnel (SOC) en complément d'outils de gestion des informations de sécurité (SIEM). Il permettra de mettre en place une gestion des connaissances cyber (KM), à partir d'ontologies ou de graphes de connaissances. Il vous permettra également d'explorer des techniques intéressantes pour la cybersécurité comme le "process mining" (PM) ou encore la détection d'anomalies (DA).

Enfin, dans un contexte où les hautes technologies évoluent rapidement, il est difficile de faire des choix structurants face à une problématique de traitement de données massives. On ne peut pas tout connaitre ! les outils évoluent vite. Le cours est là pour vous "apprendre à apprendre"  à partir du module de recherche bibliographique, à maitriser les "deep tech", avoir une démarche scientifique pour connaitre et évaluer l'état de l'art des différentes techniques et méthodes d'IA associées à la cybersécurité.

## COMPÉTENCES VISÉES

Le cours vise l’acquisition de compétences élevées sur 3 domaines de l'Intelligence Artificielle afin de mener des activités d'extraction, d'analyses et de présentation des données massives, ces activités sont par exemple présentes dans les centres de sécurité opérationnelle (SOC), particulièrement utilisés dans l'outillage de cyberdéfense, d'investigation (forensic) ou d’anticipation de la menace (CTI-Hunting).

Le cours permet d'acquérir les fondamentaux suivants :

- Appliquer des prétraitements sur les donnés collectées, structurées ou non (par exemple que l'on trouve dans un centre de sécurité opérationnelle comme les journaux d'évènements, les configurations des systèmes, les base de connaissances TTP, CVE, ...),
- Prétraiter et analyser des données structurées pour répondre à un problème métier,
- Prétraiter et analyser des données non structurées (texte, images) pour obtenir un jeu de données exploitable
- Développer des algorithmes basés sur des méthodes de machine learning ou de modélisation des connaissances, en sachant rédiger une spécification des besoins,

Entraîner un modèle d’apprentissage :

- supervisé pour réaliser une analyse prédictive, (par exemple que l'on trouve sur les moteurs de détection comportementale).
- non supervisé pour la segmentation réduction de données (par exemple que l'on trouve dans les journaux d'évent collectés dans un centre  de sécurité opérationnelle).

Déployer un modèle d’apprentissage automatique à l’échelle technologies du Big data (appliqué aux journaux d'évènements)

- Présenter et déployer un  modèle d’apprentissage automatique auprès d’utilisateurs finaux.

Les exemples de compétences “cybersécurité” listés ci-dessous sont issus d'offres d'emplois, ces compétences sont attendues par les entreprises, elles sont demandées à un ingénieur informatique du parcours cybersécurité pour concevoir par exemple un prototype d'intelligence artificielle ou encore analyser ou développer un algorithme d'IA. Ces compétences reposent directement sur celles du machine learning (ML), de la gestion des connaissances (knowledge management (KM)) ou de la détection d'anomalies(DA).

- la compétence “Participer à la veille sur les nouveaux mécanismes de détection ainsi qu'aux nouvelles méthodes d'investigation”,
- la compétence "Effectuer, à partir des scénarios d'agressions redoutés, les activités de mise sous surveillance, la traduction en règle de corrélation, la construction de la collecte des données nécessaires, la définition des réponses à incident, le pilotage de la mise en oeuvre et la recette,
- la compétence “mettre en place des outillages d'ingénierie de la connaissance cyber visant à structurer et automatiser les phases de collecte des données puis d'extraction, de modélisation et d'enrichissement de la connaissance d'intérêt cyber à des fins de capitalisation.”
- la compétence “Implémenter les pipelines automatisées pour le déploiement et la surveillance des modèles (gestion des alertes)”,
- la compétence “Configurer / Déployer / Automatiser / Industrialiser le déploiement de modèles ML”,
- la compétence “Développer, entraîner et optimiser des modèles d’intelligence artificielle destinés aux outils numériques de l'organisation”.

## Contenu de la formation

Le déploiement des enseignements s'effectue à raison d'un volume de 12 unités temps (UT).

**Temps 1 : IAML pour la cyber**

(IA/ML 1 UT*)

Histoire, enjeux et champ disciplinaire de l'intelligence artificielle.

Techniques de l'intelligence artificielle au service de la cybersécurité.

Fondamentaux de la détection d’anomalie à partir des données.

Typologie des données de sécurité traitées pour l'apprentissage  (hétérogénité, structures, ..).

Modèle général du traitement automatique des logs.

**Temps 2 : KM**

(KM : 4 UT*)

Fondamentaux pour la gestion des connaissances

Langages semi-formels : ontologies et web sémantique

**Temps 3 : ML**

(ML : 4 UT*)

Classifications statistiques : supervisées, semi-supervisées, non supervisées

Fondamentaux pour l'apprentissage artificiel

Techniques du machine learning (Réseaux de neurone, Deep learning).

**Temps 4 : PM ou AD**

(PM : 1 UT*)

Généralités sur le Process Mining ou sur la Détection d'Anomalies (AD)

**Temps 5 : RB : IA/ML pour la cyber**

RB: 4 UT*)

Lien avec les applications actuelles en cybersécurité au travers d'une étude bibliographique tutorée par un enseignant chercheur,

Outils de cybersécurité à base de machine learning, knowledge management et IA.

**Remarques**

*Par semaine, 1 UT comprend deux heures de cours, deux heures de travaux pratiques, attend quatre heures à minima de travail personnel. Chaque UT est donc espacée d'une semaine, ce rythme doit être pris en compte dans la planification des enseignements

## Modalités de validation et d’évaluation

**Contrôle continu:** Contrôle de connaissances et de savoirs qui se déroule tout le long du temps de l'enseignement

**Projet(s):** Projet(s) à réaliser amenant la livraison d'un livrable

**Mémoire:** Ecrit portant sur un sujet validé par l'enseignant

## Accompagnement et suivi:

Prise en charge des auditeurs inscrits à une unité d’enseignement, depuis l’inscription jusqu’au déroulement effectif de la formation.

## Parcours

## Cette UE est constitutive des diplômes suivants:

[{"code":"CYC9106A","code_suivi":1031,"date_debut_validite":"2024-09-01","date_fin_validite":"2025-08-31","date_limite_utilisation":"2025-08-31","affichable":true}]

## ECTS: 6

| Volume Horaire indicatif | Financement individuel hors tiers financeur et CPF | Tarif de référence (Employeur) |
|---|---|---|
| 45 heures | 450.00 | 900.00 |

## Infos Pratiques

| Durée indicative | Modalité | Période | Date de début des cours | Date de fin des cours |
|---|---|---|---|---|
| 45 heures | Formation ouverte et à distance (FOAD) | Second semestre | Information Indisponible | Information Indisponible |

Dernière mise à jour: 02/07/2025 10:20:08