CENTRALE MARSEILLE

Mastère Spécialisé :
Cybersécurité des Systèmes Complexes pour l'Industrie et la Défense

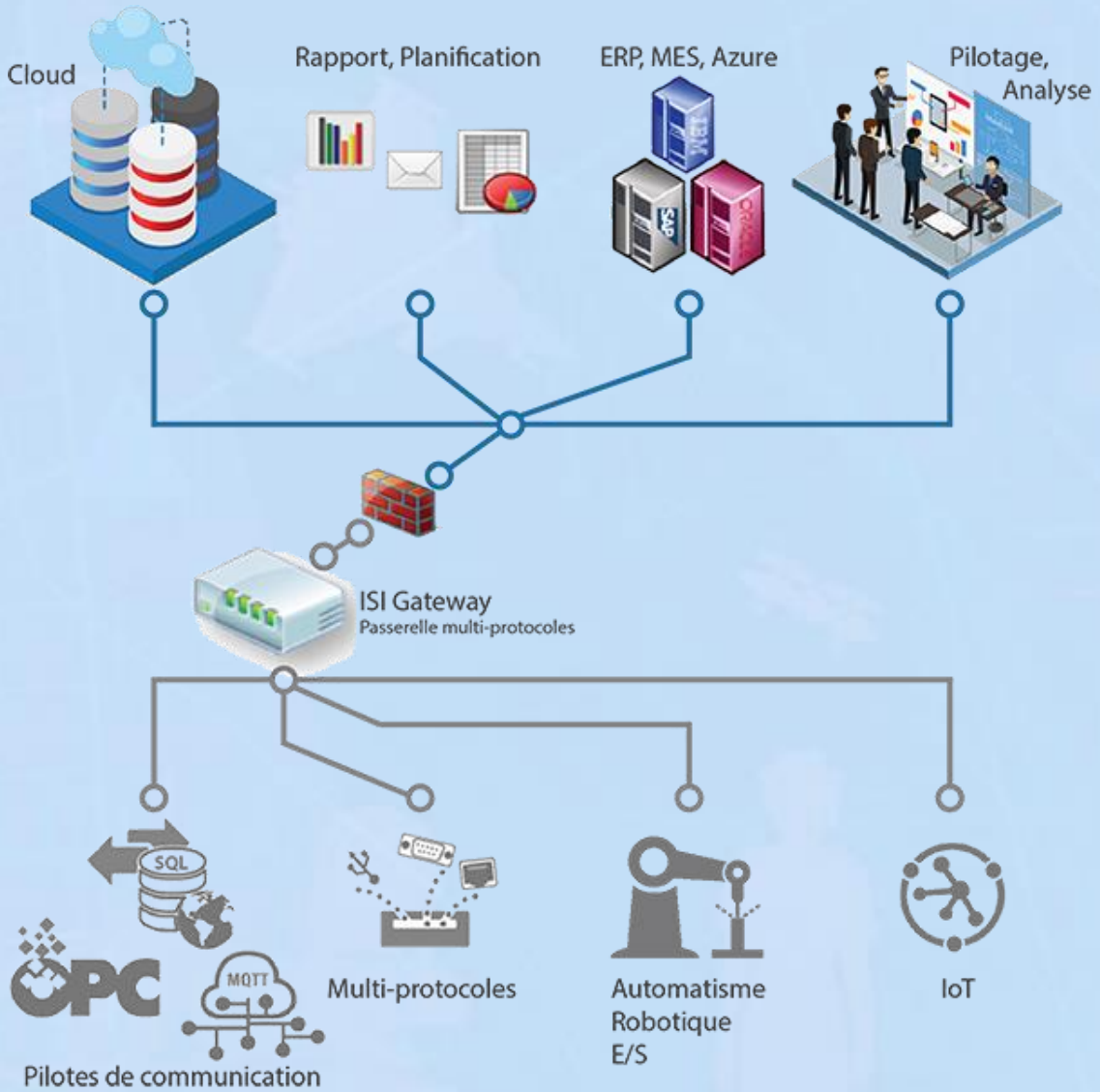
CyberSCID

MS® Cyber SCID

2 avril 2021

- Les **systèmes de contrôle industriel ICS**, ou encore les **SCADA** (Supervisory Control And Data Acquisition) , contrôlent les **infrastructures critiques** de la société depuis les réseaux électriques au traitement de l'eau, de l'industrie chimique aux transports et en passant par la santé et la défense.

- Ils sont **présents partout**.



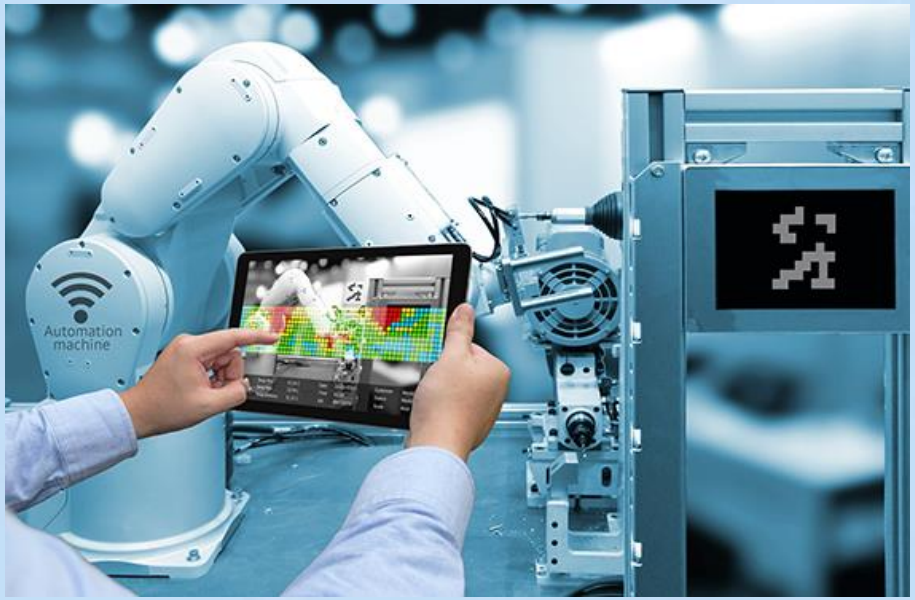
- Les entreprises et institutions aux infrastructures critiques disposent de départements dédiés pour protéger les deux infrastructures clés classiques : le data center (serveurs) et le réseau local (postes de travail).

- Il existe également **un "3e réseau"** : le réseau de contrôle des processus, **qui nécessite le même niveau d'attention.**

➢ les réseaux SCADA sont souvent les moins protégés :

- Ces réseaux sont souvent construits pour durer.
- Ces réseaux sont pas prévus pour subir des modifications
- Un empilement technologique peut niveler le niveau de sécurité par le bas
- Ils sont souvent considérés comme intrinsèquement sûrs car historiquement isolés
- Le réseau SCADA est souvent "invisible" . Vu comme un outil de production il ne bénéficie pas de suffisamment d'attention et d'investissement, comparé aux autres réseaux.
- Les objectifs de production ou de sureté de fonctionnement s'opposent à l'urgence cyber
- Souvent une équipe différente gère le réseau de contrôle des processus alors que le service informatique gère les autres réseaux.

Les **systèmes industriels et de défense** sont aujourd'hui fortement informatisés et interconnectés avec les systèmes d'information classiques, et Internet.



À ce titre, ils sont exposés aux **mêmes menaces**, avec des **conséquences potentiellement plus graves.**

- **Les approches habituelles de la SSI ne peuvent s'appliquer telles quelles sur les systèmes de contrôle industriel**

- Il faut comprendre le métier et les problématiques, savoir dialoguer avec les automaticiens, et connaître et comprendre les normes propres au monde industriel.

- **Quel que soit l'apport des solutions techniques elles ne constituent pas à elles seules une réponse suffisante aux besoins de cybersécurité.**

- Elles nécessitent d'être implémentées, maintenues et surveillées par des personnes ayant les compétences et expertises adéquates

- **La formation est un élément central**

- 2017-18 identification des besoins
  - projet de formation
- 2018-19 : orientation vers un MS
- **2019-20 : accréditation**
- 2020-21 : Rentrée de la **première promo 5/11/20**

- Une formation avec pour objectifs:
  - comprendre les enjeux spécifiques liés à la cybersécurité des systèmes complexes dans les domaines de l'industrie et de la Défense,
  - savoir identifier les vulnérabilités de ces systèmes, d'acquérir une méthodologie et des techniques appropriées de renforcement du niveau de cybersécurité des systèmes existants,
  - comprendre et savoir mettre en place des méthodes et outils pour détecter une attaque et y répondre en appliquant un plan de remédiation,
  - comprendre et identifier les points clés à examiner lors de la conception de systèmes complexes intégrant de la cybersécurité de bout en bout.

➢ FORMATION

Mastère Spécialisé (bac +6)

360 h	80 h	4 à 6 mois
d'enseignements (36 ECTS)	de projet (9 ECTS)	de mission professionnelle (30 ECTS)

National Institute of Standards and Technology

➢ Module 1 : Remise à niveau

6 ECTS / 60 heures

- Remise à niveau **EEA & automatisme**

- Remise à niveau **Informatique & réseaux**

- Passage du CCNA

Cisco Certified Network Associate

(optionnel : *3 ECTS / 60 heures*)

➢Module 2 : Fondamentaux de cybersécurité

6 ECTS / 60 heures

- Catégorisation des menaces
- Droit et réglementation cyber
- Relations Internationales et cybersécurité
- Intelligence Cyber /veille

- Travaux Pratiques d'illustration

- Certification CCNA Cybersecurity Operations (*facultatif – 4 ECTS)*

➢Module 3 : Cartographie des systèmes, identification de la menace

4 ECTS / 40 heures

- Cartographie des systèmes
- Analyse de risque
- Menace cyber et mode opératoire

➢Module 4 : Méthodes et mécanismes de protection des systèmes

6 ECTS / 60 heures

- Mise en place d'une architecture sécurisée
- Cryptographie et sécurité de l'information
- Sécurité des logiciels et des systèmes d'exploitation

➢Module 5 : Méthodes et outils de détection *4 ECTS / 40 heures*

- IA et Data mining pour la cyber
- Mécanismes et outils de détection

➢Module 6 : Méthodes de réponse à une attaque, remédiation

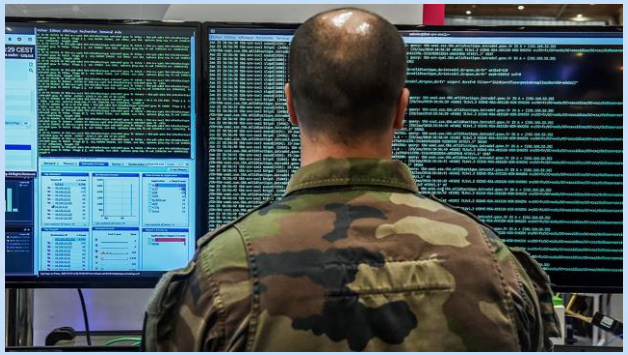
3 ECTS / 30 heures

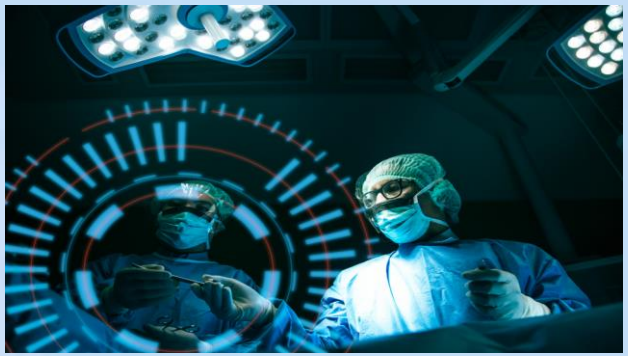
- Déroulement d'une cyber attaque et réactions d'urgence
- Rôle du SOC (Security Operations Center) et du CERT (Computer Emergency Response Team)
- Remédiation

➢Modules électifs (1/4 au choix)

6 ECTS / 60 heures

- Défense *(habilitation Confidentiel Défense requise)*
- Énergie
- Santé
- Transports





➢Projet

9 ECTS / 80 heures

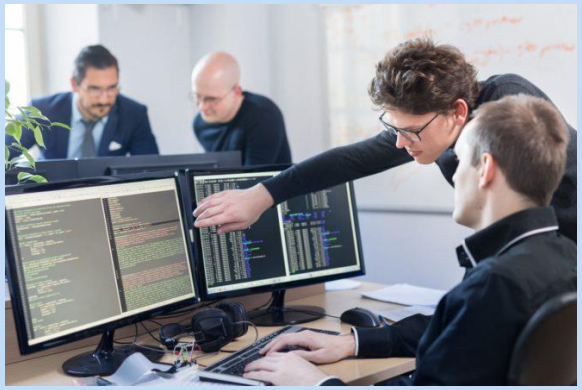
➢Mettre en œuvre par équipes (en utilisant la plateforme Hynesim de l'École de l'air) les différentes étapes du NIST :

- mettre en œuvre le système d'information type d'une organisation (réseaux, ordinateurs, logiciels, SCADA) en faisant sa cartographie et en identifiant les menaces qui lui sont propres
- sécuriser le système mis en œuvre
- attaquer le système d'un autre groupe
- analyser le système mis en œuvre au premier point, investigation
- rétablir le système, proposer des évolutions

➢Thèse professionnelle

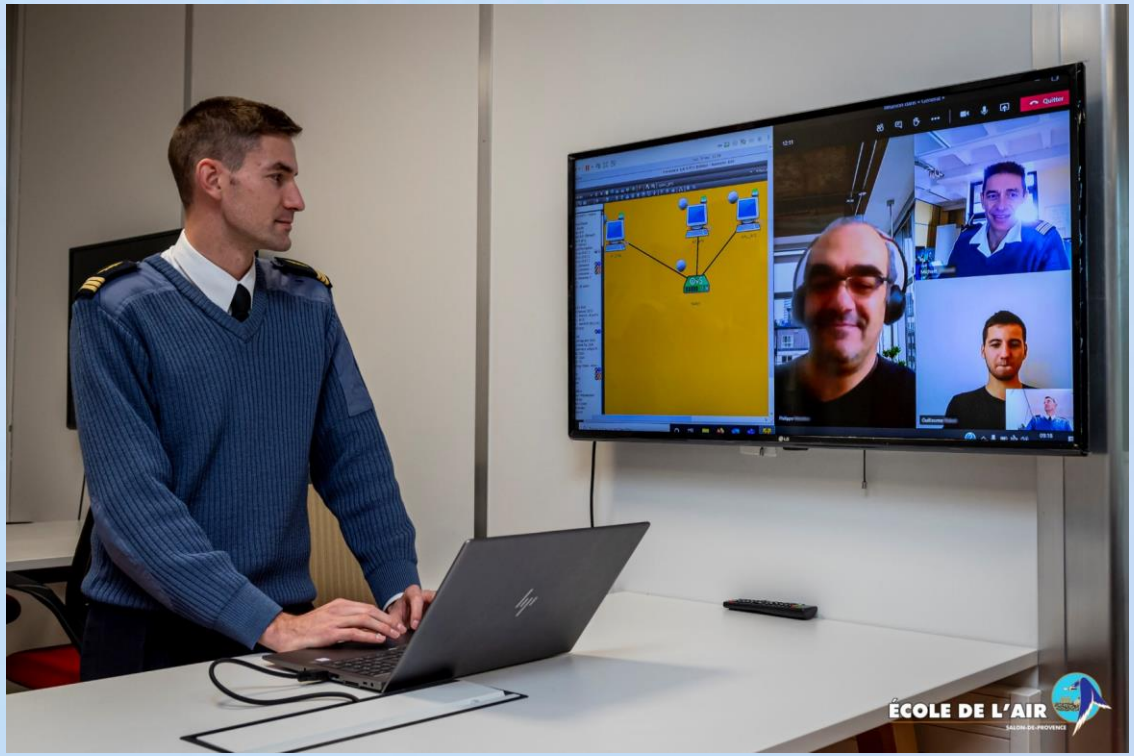
30 ECTS / 4 à 6 mois

- Formation pratique de 4 à 6 mois en entreprise,
- Validée par un rapport et une soutenance
- Réalisation d’ un travail d’analyse, de conception et d’implémentation visant à prouver les capacités de l’ étudiant à répondre à un problème de cybersécurité relevant du secteur industriel ou militaire.



➢ PROMO « 1.0 »

- 8 étudiants
- Rentrée le 5/11/20
- 2 électifs ouverts :
  - Défense
  - Transports
- Départ en stage 1/05/21



➢ RECRUTEMENT

- Le recrutement est ouvert aux titulaires :
  - d'un diplôme de niveau bac + 5 (ingénieur, master ou équivalent)
  - d'un diplôme de niveau M1 dans les mêmes domaines + 3 années d'expérience professionnelle
  - d'un diplôme étranger équivalent aux diplômes français mentionnés ci-dessus

- Retrait des dossiers de candidature : admission-ms@centrale-marseille.fr
  admission-ms@ecole-air.fr

- Jury de recrutement (dossier et entretien) : fin Mai / début Juillet
- Rentrée : Septembre 2021

LCL Michaël SIMOND
Michael.simond@ecole-air.fr

Pr. Caroline FOSSATI
Caroline.fossati@centrale-marseille.fr