

# Cybersecurity Summer Bootcamp

LEÓN - 2024

Du 8 au 18 juillet 2024

**León, Espagne**

#CyberSBC2024

Organisé par:



En collaboration avec: **Canada**



# Informations Générales

## Objectifs:

1. former aux dernières techniques en matière de lutte contre la cybercriminalité, à la gestion des incidents de cybersécurité et aux aspects législatifs à prendre en compte à cet égard.
2. Améliorer la coordination dans la gestion des incidents et de la cybercriminalité.

## Format pratique

## Langues:

- Espagnol : tous les parcours
- Anglais : CSIRT ou CERT (niveau élémentaire et avancé)
- Français : PM/Cyberdiplomatie

## Pour les parcours FFCCS et CSIRT ou CERT, deux niveaux de difficulté sont proposés : élémentaire et avancé

## Événement international et gratuit

## Formation exclusive et de pointe de la plus haute qualité

## Thèmes novateurs et dernières tendances en matière de détection de la cybercriminalité

## Ateliers pratiques animés par les meilleurs professionnels

## Possibilité de faire du networking de haut niveau avec les participants

## Public cible:

- **Forces armées et de sécurité de l'État (FFCCS):** membres des forces armées et de sécurité travaillant dans des unités opérationnelles en lien avec la cybersécurité.
- **CSIRT ou CERT:** personnel technique travaillant dans des centres d'intervention en cas d'urgence informatique.
- **Fiscal:** personnel du parquet travaillant sur des affaires de cybercriminalité ou cybersécurité.
- **Juges et magistrats:** membres de la profession judiciaire, magistrats et avocats de l'État travaillant sur des affaires de cybercriminalité ou cybersécurité.
- **PM/Cyberdiplomatie:** *policy makers*, acteurs politiques, régulateurs ou législateurs : personnel travaillant dans des domaines liés aux aspects juridiques et réglementaires de la cybersécurité, décideurs en matière de cybersécurité et diplomatie.

Plus d'informations sur: <https://www.incibe.es/en/events/summer-bootcamp/>



# Caractéristiques de l'événement

Programme international de formation spécialisée en cybersécurité.



**5 parcours différents** | **182 heures de formation**

- Programme de **39,5 heures** à l'intention des **membres des forces armées et de sécurité** travaillant dans des unités opérationnelles en lien avec la cybersécurité (FCS).
- Programme de **37 heures** en espagnol à l'intention des **personnels techniques travaillant dans des centres d'intervention en cas d'urgence informatique (CSIRT)**.
- Programme de **37 heures** en anglais à l'intention des **personnels techniques travaillant dans des centres d'intervention en cas d'urgence informatique (CSIRT)**.
- Programme de **15 heures** à l'intention des **membres de la profession judiciaire en activité**.
- Programme de **17,5 heures** à l'intention des **personnels du parquet en activité**.
- Programme de **37 heures** à l'intention du **personnel des organismes régulateurs ou législateurs travaillant dans des domaines liés aux aspects juridiques et réglementaires de la cybersécurité (Policy Makers) et à la cyberdiplomatie**.

\* Les heures sont données à titre indicatif et peuvent être modifiées.

- Ateliers animés par des **experts de premier rang** sur des questions pertinentes et actuelles pour chacun des 5 parcours de spécialisation.

## Programmes de Formation\*



### Enquête de police (FFCCS):

Le parcours de cybersécurité pour les forces armées et de sécurité couvre différents domaines clés pour lutter contre la cybercriminalité. Inclut des thèmes tels que l'OSINT dans le cadre des enquêtes policières, l'utilisation de l'IA par les cybercriminels et d'autres sujets d'actualité. Cette formation permettra aux professionnels de développer les compétences nécessaires pour aborder les menaces numériques actuelles et protéger la société.



### Opérations CSIRT:

Notre parcours spécialisé en cybersécurité pour les équipes de CSIRT/CERT porte sur des thèmes fondamentaux tels que les techniques de cyberpatrouille, l'intervention en cas d'incident, la détection et la surveillance des menaces et un vaste programme de formation pour relever les défis de la cybercriminalité en appliquant les meilleures pratiques et en utilisant les meilleurs outils du secteur.



## Programme pour les juges:

Un parcours de cybersécurité conçu exclusivement pour les juges, une initiative pionnière qui fournit une compréhension profonde des complexités de la cybercriminalité et forme les professionnels du droit pour qu'ils soient capables d'aborder ces enjeux dans le système judiciaire. À partir d'une approche pratique et actualisée, ce cours aborde des sujets clés permettant aux juges d'acquérir les connaissances nécessaires pour lutter contre la cybercriminalité de manière efficace.



## Programme pour les procureurs:

Le programme de cybersécurité conçu pour les procureurs est une chance unique de renforcer sa capacité de lutter contre la cybercriminalité dans le système judiciaire. Ce parcours propose une approche intégrale qui développe les connaissances nécessaires pour aborder efficacement les enjeux du monde numérique.

## Programme pour policy makers et cyber-diplomates:

Ce programme fournit aux participants les outils et les connaissances nécessaires pour développer des politiques et des stratégies de cybersécurité efficaces ainsi que pour promouvoir la coopération internationale et la création de capacités dans ce domaine clé pour la sécurité nationale et mondiale.



## Autres Activités

- ♦ Activités pour favoriser le **networking** entre les participants et répondre aux besoins de collaboration entre eux.
  - ♦ **Role Play**: cas pratiques et collaboratifs avec la participation de profils des différentes spécialités donnant leur point de vue pour la résolution d'un incident.
  - ♦ **Ateliers pratiques** : ces ateliers offrent des simulations réalistes de crises de cybersécurité, où les participants doivent prendre des décisions rapides et efficaces pour gérer la situation. Cela inclut la coordination avec d'autres agences gouvernementales, la communication avec le public et la prise de décisions stratégiques en temps réel
  - ♦ **Activités de loisir** : visites guidées de la ville de León et visite des monuments les plus emblématiques. Les participants sont encouragés à partager ces activités sur les réseaux sociaux.
- ♦ **Conférences données par des experts** sur différents sujets d'actualité, recherches en cours et nouveaux outils en lien avec la cybersécurité et d'autres domaines.



# Résultats de l'édition 2023

- 🟡 Format présentiel avec plus de **260** participants de **25** pays.
- 🟡 **4** heures of **keynotes** et **séances magistrales**.
- 🟡 **Formation spécifique:**
  - 🔹 Enquête de police: **35 heures** de formation
  - 🔹 Opérations CSIRT: **37,5 heures** de formation
  - 🔹 Personnel du parquet: **17 heures** de formation
  - 🔹 Juges et magistrats: **17 heures** de formation
  - 🔹 Acteurs politiques, régulateurs ou législateurs et cyber-diplomates: **22 heures** de formation
- 🟡 **80** intervenants et **8** **keynotes internationaux**.

## Feedback des apprenants:

- 🟡 **100%** recommande le programme de formation
- 🟡 **100%** de satisfaction
- 🟡 **90%** des contenus jugés de grand intérêt et utilité



# Cybersecurity Summer Bootcamp

LEÓN - 2024

[www.incibe.es/en/events/summer-bootcamp/](http://www.incibe.es/en/events/summer-bootcamp/)

Organisé par:



En collaboration avec: **Canada**

