

LA RA&D ET LA FORMATION CONTINUE, DEUX PILIERS DE L'ILCE AU SERVICE DE LA FORMATION POLICIÈRE

Novembre 2021

Sébastien Jaquier



Certifié ISO 9001

Au menu

Formation

- Lien avec la SNPC
- Stratégie de formation policière en matière de numérique
- Formation de base et
- Formations spécialisées

Projets de recherche

- Illustration
- Points de concordance et perspectives

Stratégie nationale de protection de la Suisse contre les cyberrisques 2018 - 2022

- 10 champs d'action, 29 mesures
- Champ d'action : **poursuite pénale**
 - 18. Tableau de la situation en matière de cybercriminalité
 - 19. Réseau de soutien aux enquêtes relatives à la cybercriminalité
 - 20. Formation à la lutte contre la cybercriminalité
 - 21. Office central de lutte contre la cybercriminalité



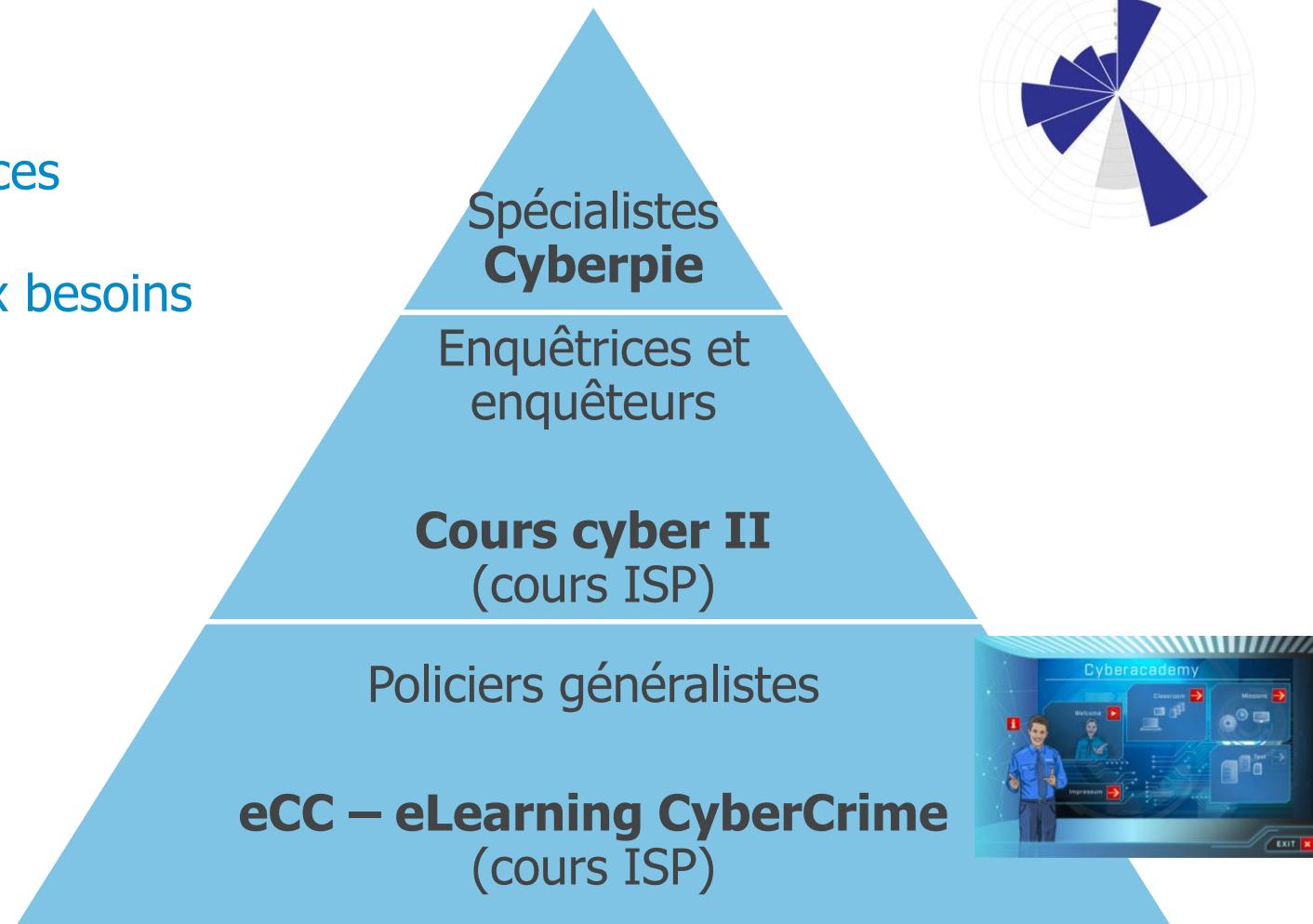
➤ **Concept de formation policière en matière cyber avec :**

- E-CC
- Formation enquêtrices et enquêteurs
- Grille d'évaluation des formations pour spécialistes

Stratégie de formation policière en matière numérique

Principes

- Hiérarchie des compétences
- Ajustements continus aux besoins du terrain
- Modularisation
- Ciblage des formations





NATIONALE BILDUNGSPLATTFORM POLIZEI **NBPP**
PLATEFORME NATIONALE DE FORMATION POLICIERE **PNFP**
PIATTAFORMA NAZIONALE DELLA FORMAZIONE DI POLIZIA **PNFP**
NATIONAL POLICE EDUCATION PLATFORM **NPEP**

COURS EXAMENS **E-FORMATION** MANUELS BIBLIOTHEQUE MES DONNEES SUPPORT INFO



HOME / E-FORMATION / MES E-LEARNINGS

MES E-LEARNINGS



E-learning Cybercrime (e-CC)

L'e-learning *Cybercrime* a été conçu par l'ISP sur mandat de la CCPCS. Il vous permettra d'acquérir les fondamentaux afin de mener une lutte efficace contre la cybercriminalité, que ce soit dans la prévention ou la répression. Il comporte deux modules et s'adresse à tous les membres des corps de police suisses. Bienvenue à la « Cyberacademy » !

ATTENTION

Veuillez s'il vous plaît utiliser une des deux dernières versions des navigateurs Internet suivants : Google Chrome, Mozilla Firefox, Internet Explorer 11, Microsoft Edge, Safari.

Lorsque vous interrompez (même pour quelques minutes) votre progression dans le e-CC, IL EST IMPÉRATIF de cliquer sur le bouton EXIT afin de sauvegarder ce que vous avez fait.

Merci de votre compréhension

e-learning Cybercrime_d – Modul 1	Ouvert
e-learning Cybercrime_d – Modul 2	Ouvert
e-learning Cybercrime_f – Module 1	Réussi
e-learning Cybercrime_f – Module 2	Ouvert
e-learning Cybercrime_i – Modulo 1	Ouvert
e-learning Cybercrime_i – Modulo 2	Ouvert

Le **Test**: ne peut être réalisé qu'après avoir réussi toutes les missions. 80% de réponses correctes doivent avoir été trouvées pour le réussir.

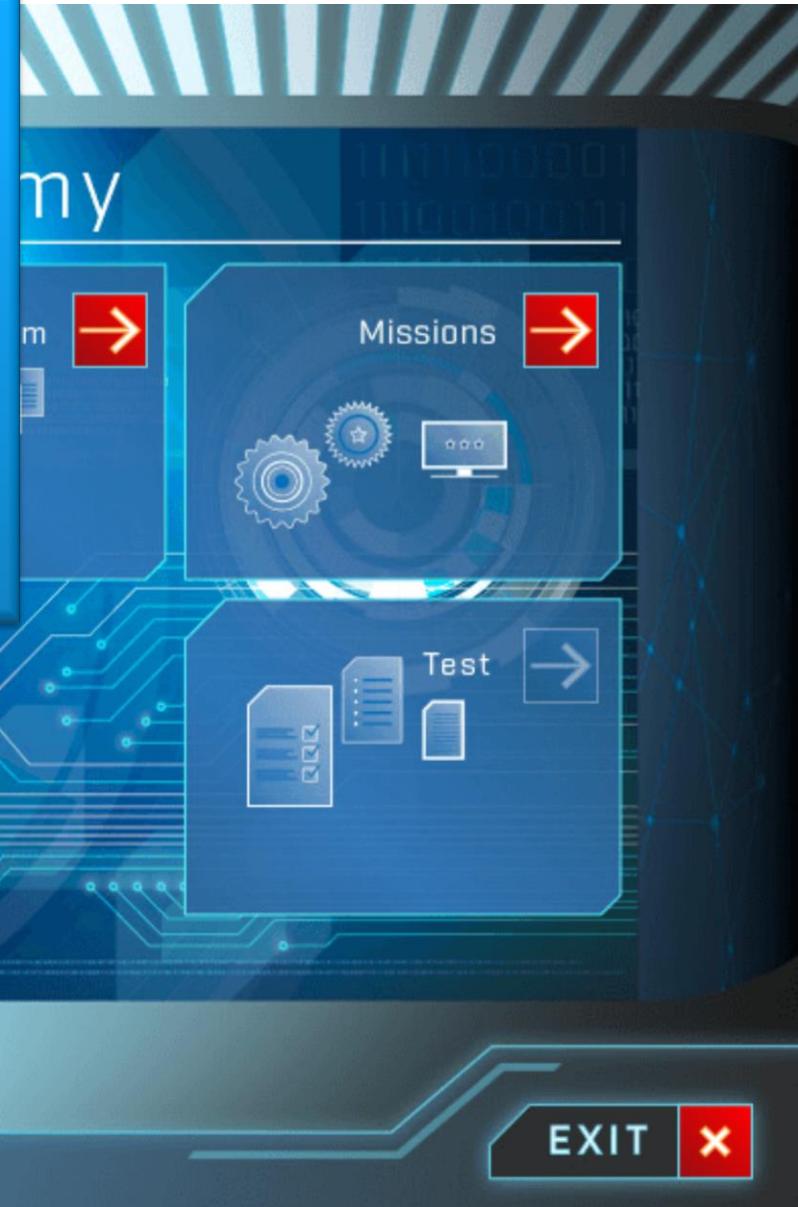
Chaque module se termine par un test.

Ce test n'est pas sommatif et il peut être répété tant qu'il n'a pas été réussi.

- Données EXIF et GPS
- Extraction de données (démarche)
- Communication sur Internet

la policière,
s ont été
uations)
le école...)
es tags)
mobile

re



Formation pour enquêtrices et enquêteurs

Cyberpie – le principe

Conçu à partir de la matrice de compétences qui regroupe 13 domaines

- Analyse forensique de la téléphonie mobile
- Analyse forensique des ordinateurs et supports de données
- Introduction au domaine spécialisé
- Analyse forensique de réseaux
- Surveillance des télécommunications
- Recherches sur internet et les bases de données publiques (« recherches open source »)
- Domaines spécialisés
- Analyse
- Sécurité informatique (interne)
- Droit applicable
- Bénéficiaire des prestations / partenaires
- Sécurité informatique / protection des données / prévention (externe)
- Engagement lié à un incident cybernétique

Il permet de qualifier le niveau de compétences à acquérir dans chaque domaine pour 5 profils de compétences dont 3 de spécialistes:

- IT-Enquête
- IT-Forensique
- Analyse Cybercrime

Cyberpie – les objectifs

- *Responsables de formation et commandement* : base d'orientation et de décision claire
- *Personnel à former* : Vue synthétique pertinente de l'offre de formations
- *Personnel formé* : Qualification de la formation suivie
- *Instituts et écoles* : Plateforme permettant de mettre en valeur leur offre

Cyberpie – La réalisation

CYBERPIE
Formations pour les polices

Rechercher 10 IT-Enquête Trier par pertinence Graph participant-e-s

Fachkurs Cybercrime
Jours de cours : 2
Jours de pratique : 1

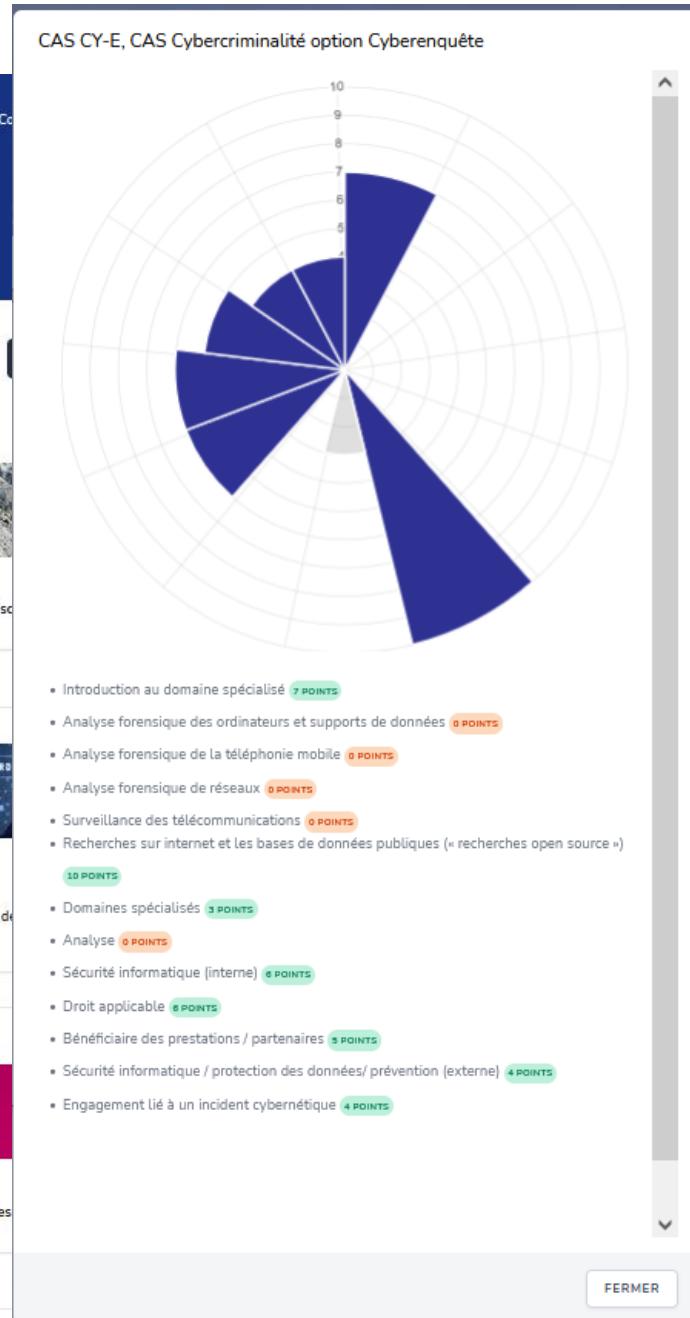
Hacking, Cracking und Malware im Cybercrime-Umfeld

CAS CY-E, CAS Cybercriminalité option Cyberenquête
Jours de cours : 20
Jours de pratique : 5

Le CAS Cybercriminalité option cyberenquête (CAS CY-E) vise à former les spécialistes des autorités de poursuite pénale (enquêteurs, analystes, procureurs) en matière de lutte contre la criminalité informatique en leur fournissant les outils pertinents pour des enquêtes ayant une composante cyber.

Investigation et veille sur Internet
Jours de cours : 5
Jours de pratique : 3

Comprendre la nature, le potentiel et les limitations des traces internétiques, saisir les enjeux liés à la qualité des données collectées en ligne, ainsi qu'adopter une démarche forensique pour collecter des données en ligne et assurer la continuité de la preuve numérique



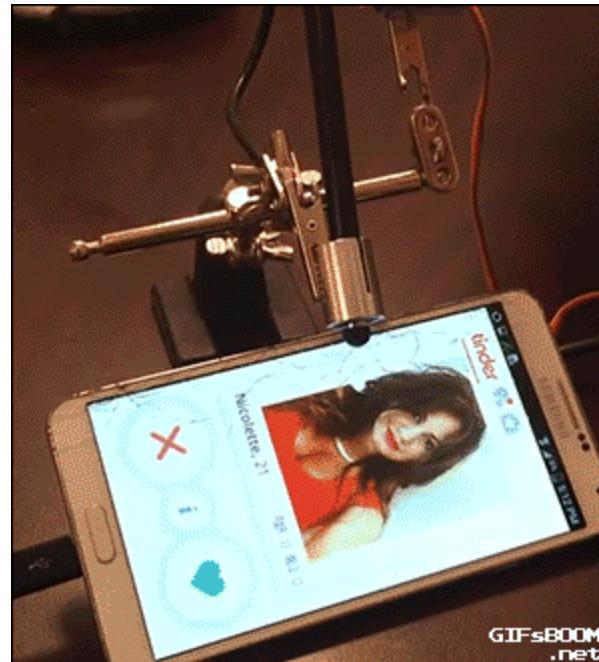
Projet «Lovid-19»: *Scambaiting* en pandémie

Etudier le phénomène de près pour :

- Mieux comprendre les victimes
- Analyser les stratagèmes des fraudeurs
- Identifier des pistes de prévention novatrices
- Confirmer ou infirmer les constats de la littérature scientifique



Projet «Lovid-19»: *Scambaiting* en pandémie



Sarah



Sandra



Christine



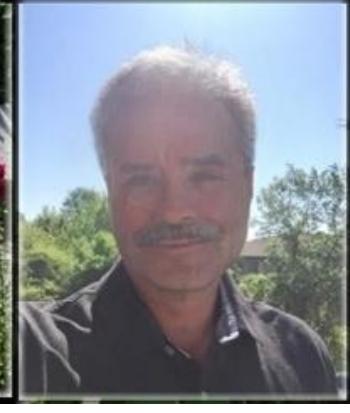
David



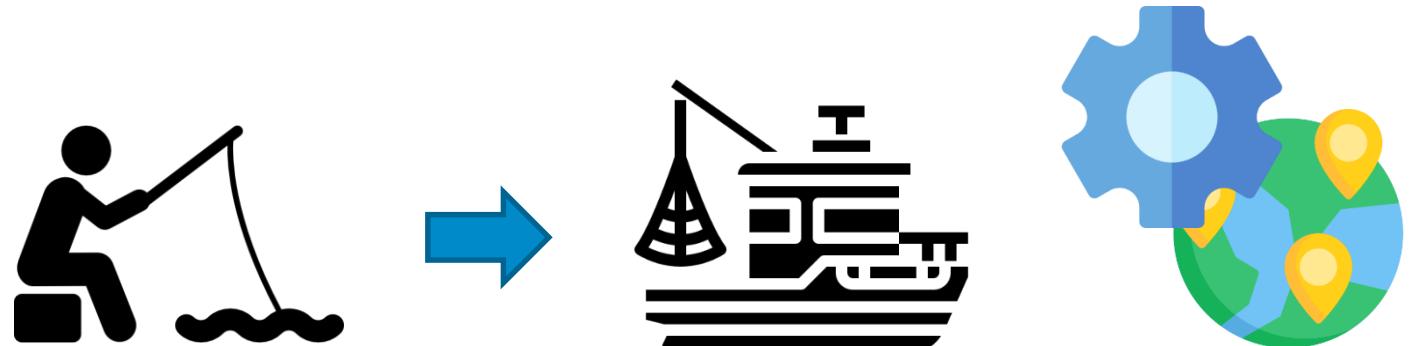
Daniel



Martin



Projet Interscam: La suite



- Explorer l'intérêt du scambaiting et les possibilités de perturbation qui y sont liées
- Etudier les limites éthiques et juridiques du scambaiting dans une perspective policière
- Réfléchir aux bases d'une IA



A votre disposition

Sébastien Jaquier
Doyen de l'ILCE
Tél. direct: +41 79 380 222 7
E-mail: sebastien.jaquier@he-arc.ch

