ilce - institut de lutte contre
la criminalité économique
heg - haute école de gestion

CYBERCRIMINALITÉ – LA RA&D COMME INGRÉDIENT ESSENTIEL AU DÉVELOPPEMENT DES FORMATIONS POLICIÈRES

Février 2024

Renaud Zbinden
Sébastien Jaquier

Hes·so

ilce - institut de lutte contre
la criminalité économique
heg - haute école de gestion

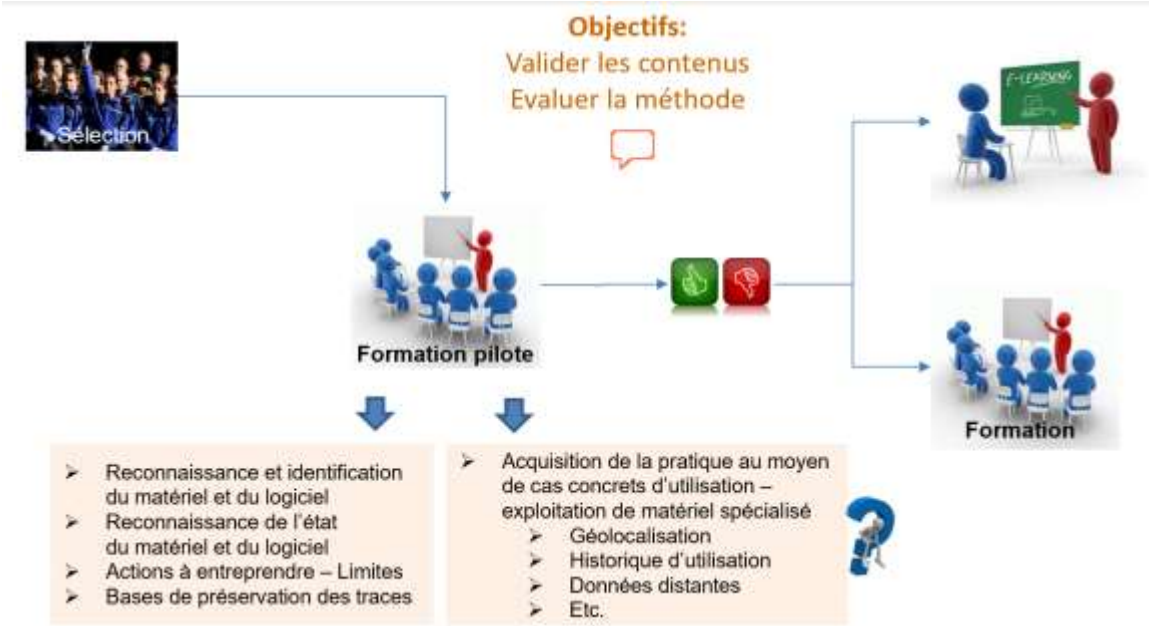
Cyber: L'émergence d'un besoin pour la police

Développement d'une formation nationale en ligne

Hes·so

Cyber: L'émergence d'un besoin pour la police

- Emergence du cyber dans le quotidien du policier
- 2014 – Idée de formation de base en préservation des traces numériques



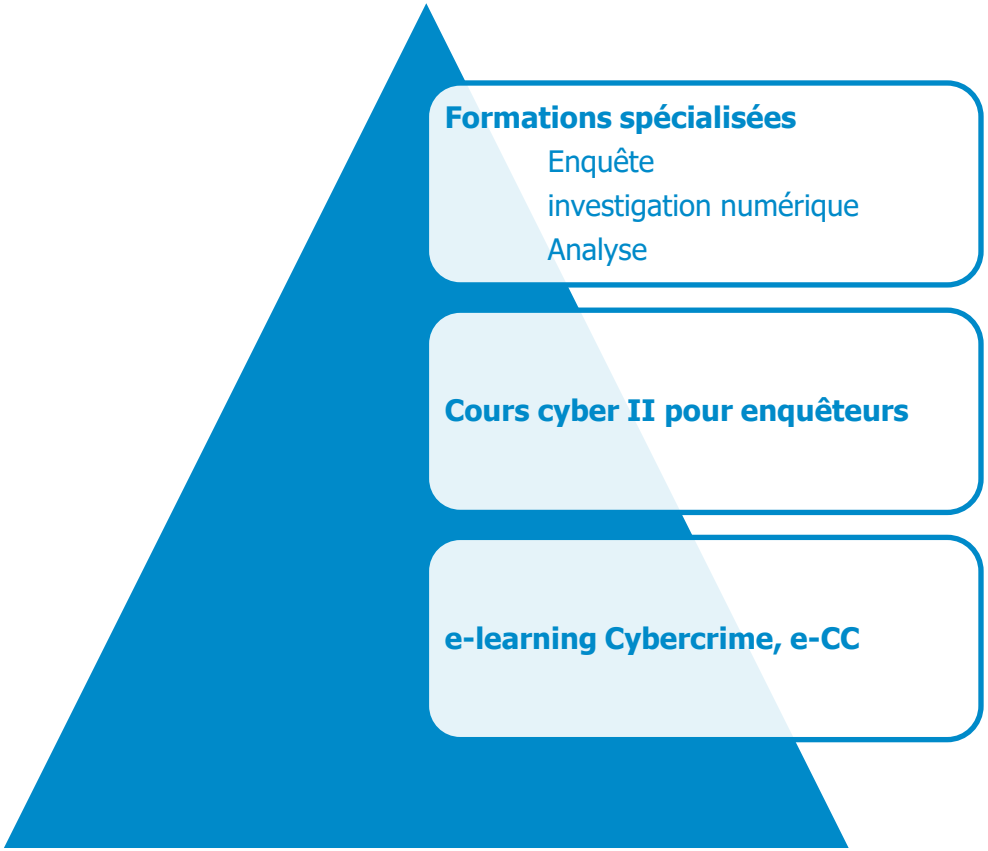
ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Concept de formation policière en matière Cyber

Spécialistes

Enquêteurs

Tous les policiers



Hes·so

Evolution des besoins

L'enquête devient Cyber.

Constats:

- Le Cyber fait désormais partie de l'enquête
- Tous les enquêteurs ne sont pas informaticiens
- Les ressources spécialisées en informatiques sont limitées
- Emergence de l'enquête IT en tant que discipline

Exemple de projet de recherche

Darknet Monitoring (DarkMon)

Question de recherche :

Comment les fraudeurs présents sur le Darknet interagissent-ils dans les salles de discussions privées ?

Terrain d'observation :

Forums destinés à la vente de logiciels malveillants (malware)

Projet : Darknet Monitoring

- ✓ Projet effectué de mai 2020 à novembre 2021
- ✓ Partenariat avec une entreprise canadienne spécialisée dans la surveillance du Darkweb
- ✓ Quasi-totalité des recherches précédentes portées sur les salles de discussions publiques uniquement

Projet : Darknet Monitoring

Objectif :

Décrire et comprendre les impacts que peut avoir la nature privée des forums de discussion sur les activités de leurs participants

Comprendre si les réseaux de fraudeurs actifs dans les salles privées sont les mêmes qui opèrent dans les salles publiques et si les informations qu'ils échangent sont de nature différente de celles qui le sont dans les salles publiques.

Projet : Darknet Monitoring

Langel, S., Décary-Hétu, D., Beaudet-Labrecque, O., Brunoni, L., & Zbinden, R. (2022). Private clubs For hackers: how private forums shape the malware market. *The Journal on Cybercrime & Digital Investigations.*

Private Clubs For Hackers: How Private Forums Shape The Malware Market

Sandra Langel[1], David Décary-Hétu[2], Olivier Beaudet-Labrecque[1], Luca Brunoni[1], Renaud Zbinden[1]

[1]Institut de lutte contre la criminalité économique, HEG Arc // HES-SO, [2]Université de Montréal

This paper was presented at Botconf 2022, Nantes, 26-29 April 2022, www.botconf.eu
This paper is published in the Journal on Cybercrime & Digital Investigations by CECyF, https://journal.cecyf.fr

Abstract

Offenders seek online private discussion forums where participants are screened before gaining access to connect with sophisticated peers and evade detection. Past research finds that most public discussion forum participants have a low level of technical skill and rely on more established participants for the tools and techniques they need to commit their offences. To date, research has mostly focused on public discussion forums of online offenders as gaining access to private forums comes with many challenges. The aim of this research is to describe and understand the impacts of the private nature of discussion forums on their participants' activities. Our driving hypothesis is that private discussion forums are host to more sophisticated participants that will, in turn, offer and have access to more sophisticated tools. To understand the impacts of the private nature of discussion forums, we selected two discussion forums available on the internet whose focus is the sale of malware; one of them is private, while the other is public. Our analysis suggests that while there are differences between private and public discussion forums, there are few significant differences between both inters of the products they advertise.

Keywords: malware, discussion forum, hacking.

1 Introduction

Discussion forums are the descendants of bulletin board systems (BBS) which were used in the pre-internet days. BBS were used to post public messages, exchange private messages as well as files [26]. Their main limit came from their access method which limited the speed at which participants could communicate, as well as their geographical reach. Using phone lines to connect to BBS meant that participants had to pay international fees when connecting to a distant BBS, unless they could somehow bypass the phone companies' billing systems. BBS were often associated with illicit activities as they facilitated the pirating of software and enabled the sharing of hacking tactics and methods [3].

Discussion forums did not inherit the bad reputation of BBS but provide many of the services that BBS did in the 1970s, 1980s and early 1990s. Discussion forums quickly replaced BBS as they could be reached by any internet users at no additional costs to their basic internet connection. At their core, discussion forums are asynchronous communication channels hosted on internet websites [20]. Discussion forums are divided into subforums, which contain multiple discussion threads. Each threat usually discusses a very specific topic (ex. how to hack a Windows password) within a more general subforum (ex. hacking techniques).

Discussion forum participants are divided into multiple groups [21, 28]. The first, the administrators, manage the forum and enforce the social rules [21]. They publish the rules under which everyone else must abide by, and hand out the punishments to those that abuse the rules. Administrators can be elected in some cases but are most often those that create a discussion forum or receive or purchase the

Projet : Darknet Monitoring

Intérêt pour la formation :

- ✓ Observation des comportements criminels
  = «Traque des cybercriminels»
- ✓ Potentiel de perturbation
- ✓ Enquête / Poursuite

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Formation des spécialistes: Cyberpie

Objectifs visés:

- *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

Hes·so

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Formation des spécialistes:

Cyberpie

S'appuie sur la matrice de compétence des profils police dans le domaine cyber

Méthodologie:

Détermination de 5 profiles concernés par le cyber:

- Policier de terrain
- Enquêteur
- IT-Enquête
- IT-Forensique
- Analyse Cybercrime

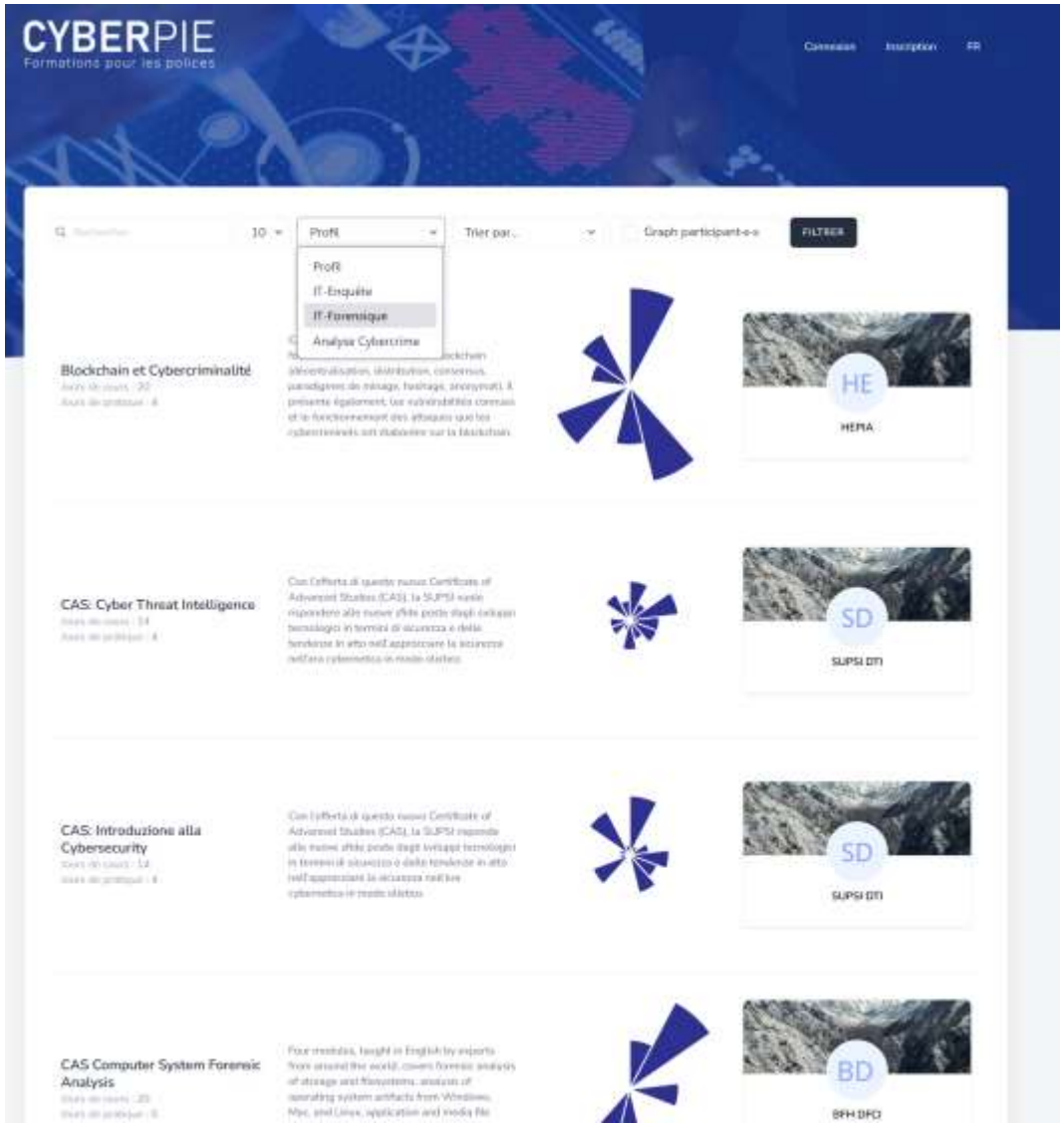
Elaboration d'une matrice de compétence listant 13 domaines

Avec pour chaque domaine différents niveau de connaissance - compétence

Hes·so

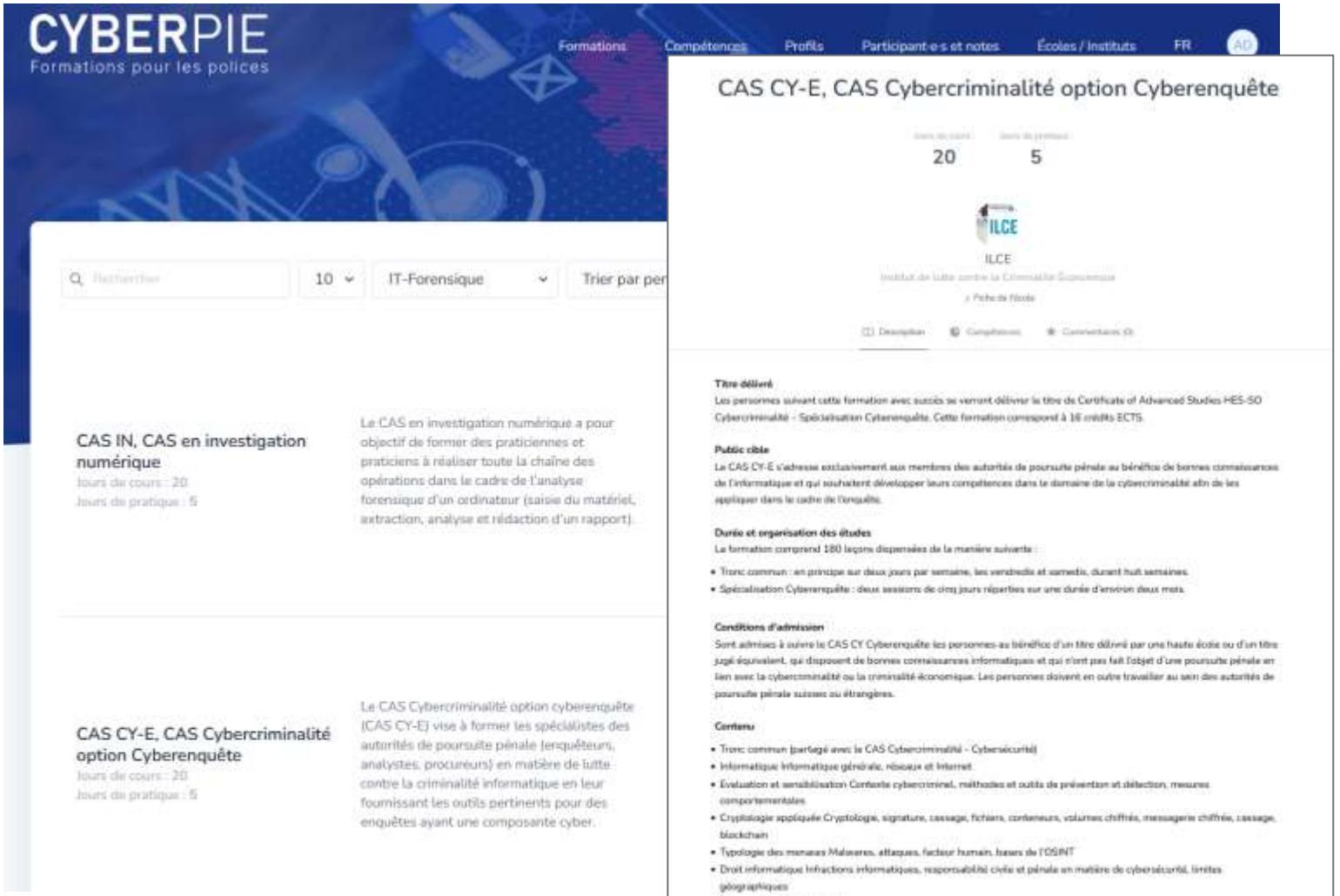
Cyberpie

Illustrations



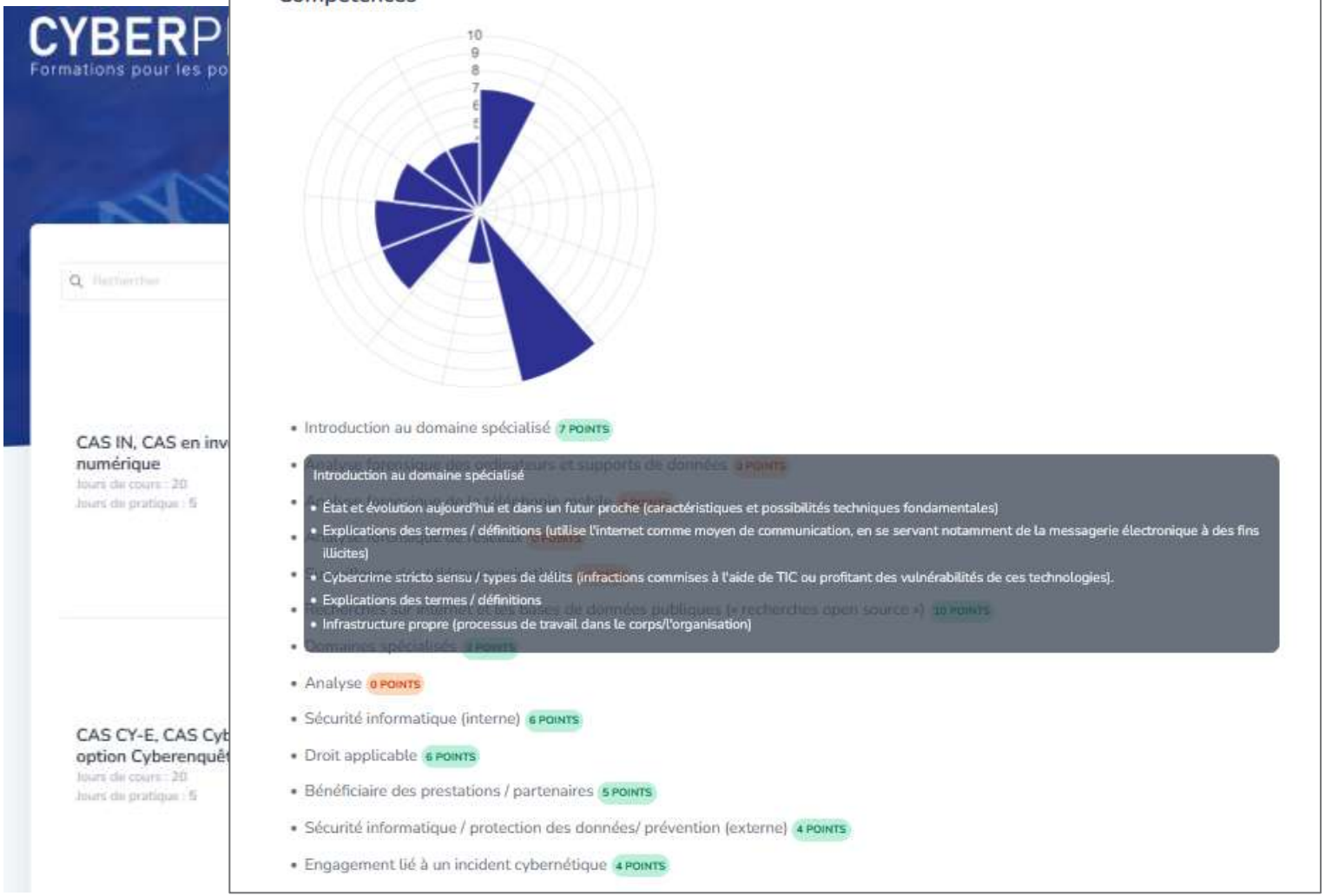
Cyberpie – Aspects fonctionnels

Illustrations



Cyberpie – Aspects fonctionnels

Illustrations



ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

A votre disposition

Sébastien Jaquier
Doyen de l'ILCE
E-mail : sebastien.jaquier@he-arc.ch

Renaud Zbinden
Collaborateur scientifique
Tél. direct : +41 32 930 23 56
Email : renaud.zbinden@he-arc.ch

Hes·so

ilce - institut de lutte contre
la criminalité économique
heg - haute école de gestion

Questions / Informations complémentaires

ILCE / ERMP / CINC

HEG Haute école de gestion Arc
21, Espace de l'Europe
CH - 2000 Neuchâtel
Tél +41 32 930 20 15

www.ilce.ch

Hes·so

Merci !