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

AF&E UND WEITERBILDUNG

ZWEI WICHTIGE PFEILER DES ILCE IM DIENST DER POLIZEIAUSBILDUNG

November 2021

Sébastien Jaquier

Hes·so

Inhalt

Ausbildung

- Verbindung zur NCS
- Digitale Ausbildungsstrategie der Polizei
- Grundausbildung und
- Ausbildungen für Spezialisten/-innen

Forschungsprojekte

- Grafiken
- Übereinstimmungspunkte und Perspektiven

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022

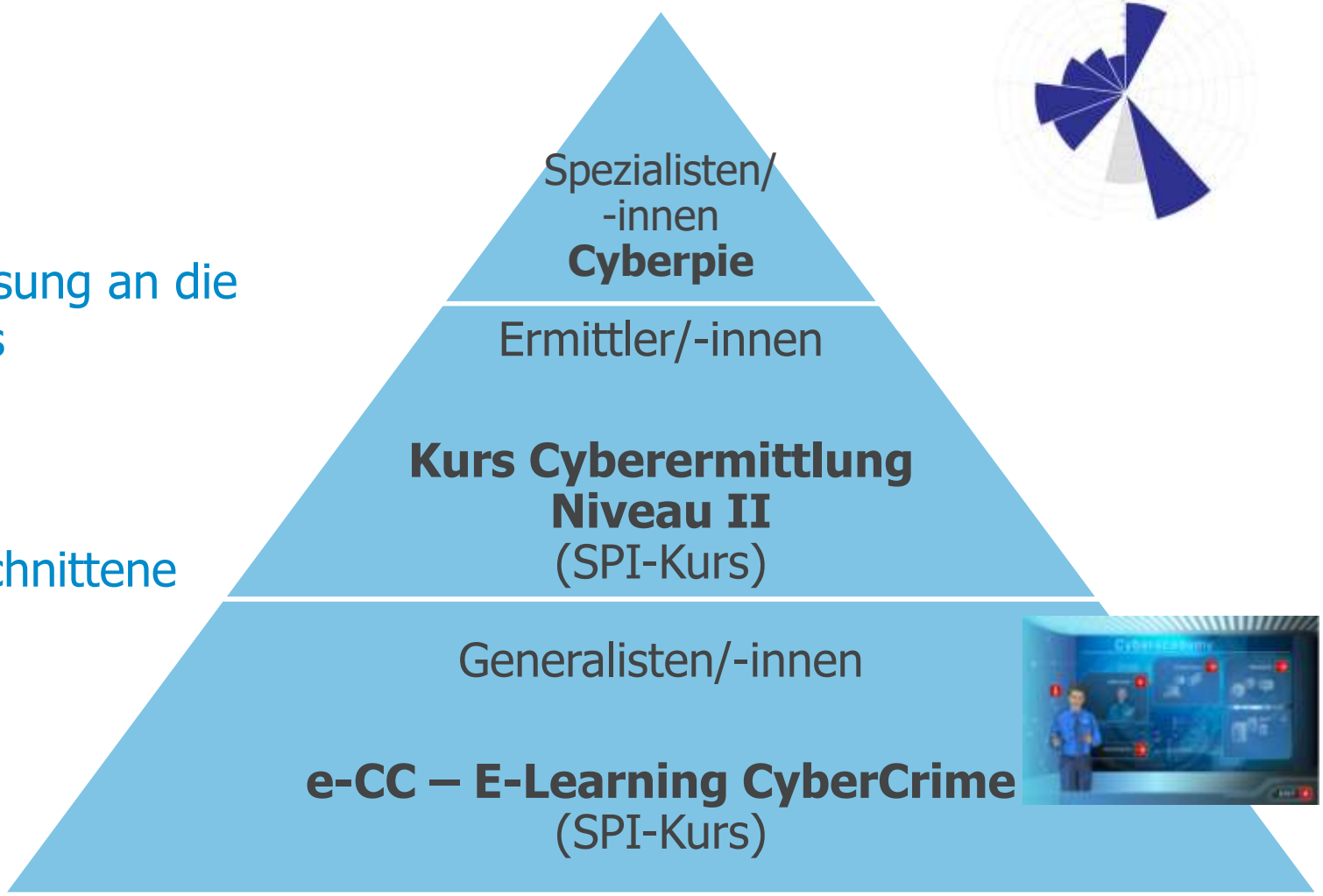
- 10 Handlungsfelder, 29 Massnahmen
- Handlungsfeld: **Strafverfolgung**
  - 18. Cyberkriminalität – eine Bestandsaufnahme
  - 19. Netzwerk zur Unterstützung von Untersuchungen im Bereich Cyberkriminalität
  - 20. Ausbildung in der Bekämpfung von Cyberkriminalität
  - 21. Zentralstelle zur Bekämpfung von Cyberkriminalität

➢ **Ausbildungskonzept der Polizei im Bereich «Cyber» mit :**
- e-CC
- Ausbildung für Ermittlerinnen und Ermittler
- Bewertungsraster der Ausbildungen für Spezialisten/-innen

Digitale Ausbildungsstrategie der Polizei

Grundsätze

- Kompetenzhierarchie
- Kontinuierliche Anpassung an die Bedürfnisse der Praxis
- Modularisierung
- Auf Zielgruppe zugeschnittene Ausbildung



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 » !

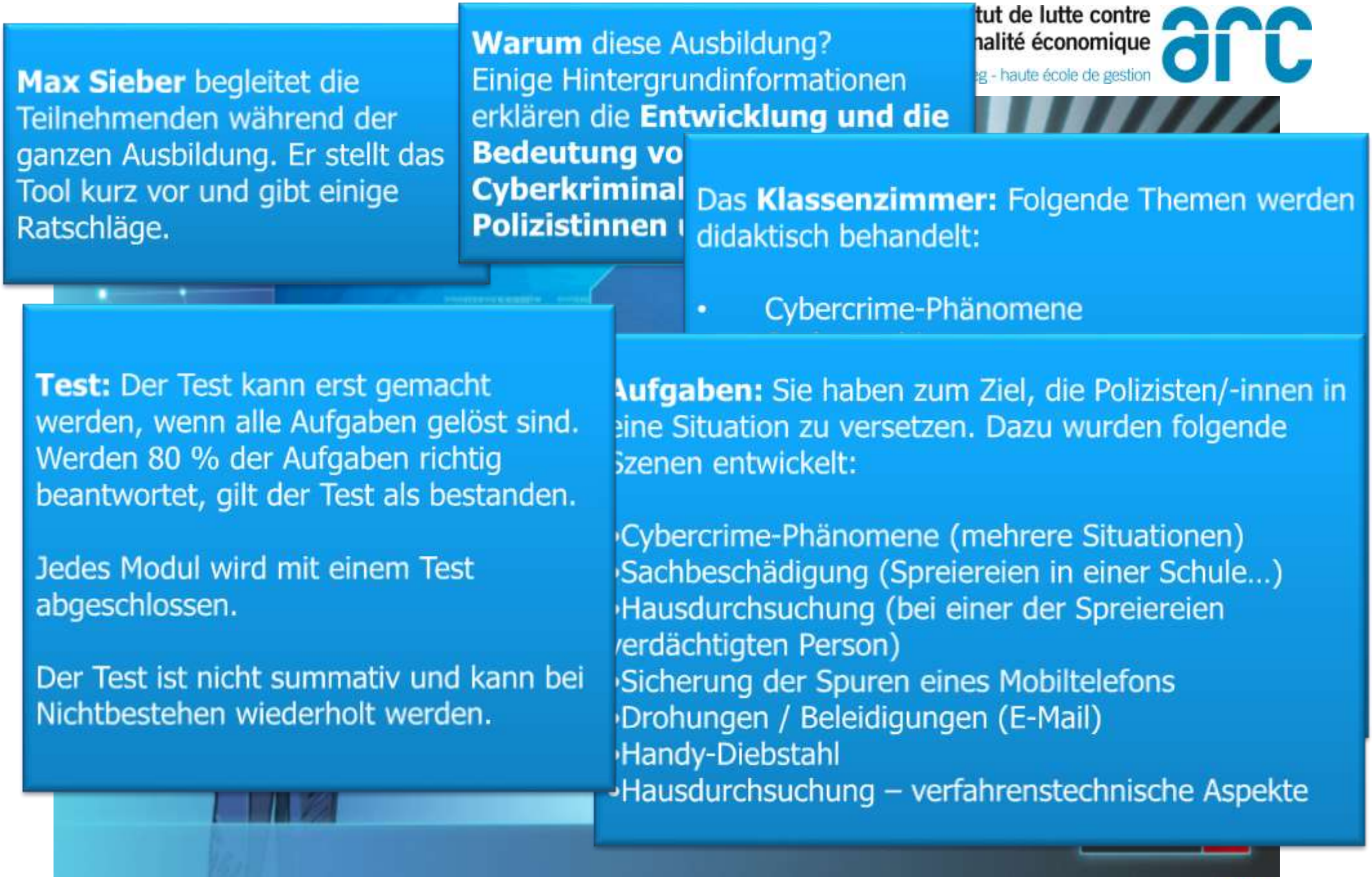
ATTENTION

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


Max Sieber begleitet die Teilnehmenden während der ganzen Ausbildung. Er stellt das Tool kurz vor und gibt einige Ratschläge.
Warum diese Ausbildung? Einige Hintergrundinformationen erklären die **Entwicklung und die Bedeutung vo Cyberkriminal Polizistinnen**
tut de lutte contre nalité économique
g - haute école de gestion
arc
Das **Klassenzimmer:** Folgende Themen werden didaktisch behandelt:
• Cybercrime-Phänomene
Test: Der Test kann erst gemacht werden, wenn alle Aufgaben gelöst sind. Werden 80 % der Aufgaben richtig beantwortet, gilt der Test als bestanden.
Jedes Modul wird mit einem Test abgeschlossen.
Der Test ist nicht summativ und kann bei Nichtbestehen wiederholt werden.
Aufgaben: Sie haben zum Ziel, die Polizisten/-innen in eine Situation zu versetzen. Dazu wurden folgende Szenen entwickelt:
•Cybercrime-Phänomene (mehrere Situationen)
•Sachbeschädigung (Spreiereien in einer Schule…)
•Hausdurchsuchung (bei einer der Spreiereien verdächtigten Person)
•Sicherung der Spuren eines Mobiltelefons
•Drohungen / Beleidigungen (E-Mail)
•Handy-Diebstahl
•Hausdurchsuchung – verfahrenstechnische Aspekte
Hes·so

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

Ausbildung für Ermittlerinnen und Ermittler

1re journée		2e journée		3e journée	
30′	**Accueil et introduction**	60′	**La sécurité sur internet** BE	180′	**Traces numériques** Sur la base de : Exploitation des données informatiques (FJR)
15′	**Travailler avec les moyens didactiques électroniques** VD + ILCE	60′	**Exercice mobilité IP, e-mails frauduleux, NAT/PAT** fedpol		
60′	**Systèmes d'exploitation et réseaux informatiques**				
60′	**Phénomènes Cyber**				
	Pause de midi				
3 x 60′	**3 blocs d'apprentissage pratique :** (s'appuyant sur l'e-CC) - **Perquisition IT** - **OSINF** Introduction à la recherche en ligne (réseau = données non structurées, les résultants varient selon le lieu d'où se fait la recherche etc.) - **Phénomènes Cyber** BE JU VD	90′	**Demande de préservation et collaboration avec les fournisseurs d'accès internet** fedpol	90′ 60′	**Les cryptomonnaies et leur Saisie** GE **Étude de cas** GE

4e journée		5e journée	
15′	**Accueil / introduction**	30′	**Droit de procédure pénale : Investigation secrète et recherches secrètes** (y.c. délimitation par rapport au droit policier) VD
105′	**Étude de cas (type « RentoPlus »)**		
		150′	**OSINF** EXT
	Pause de midi		
180′	**Forensique téléphonie mobile** Sur la base de : Exploitation des données d'appareils mobiles (FJR) GE	60′ 105′	**Darknet** EXT **Étude de cas sur l'ensemble de la matière** NE VD
		15′	**Clôture du cours** VD + ILCE

Kurs wird hauptsächlich von Polizisten/-innen geleitet

Kontinuierliche Anpassungen

Koordination auf nationaler Ebene

Hes·so

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

Cyberpie – Grundsatz

Baut auf der Kompetenzmatrix auf, welche 13 Bereiche abdeckt

- Mobilfunkforensik
- Computer- und Datenträgerforensik
- Einführung in das Fachgebiet
- Netzwerkforensik
- Fernmeldeüberwachung
- Abklärungen im Internet und in öffentlichen Datenbanken («Open-Source-Recherchen»)
- Fachgebiete
- Analyse
- Informationssicherheit (intern)
- Anwendbares Recht
- Leistungsempfänger/-innen / Partner/-innen
- Informationssicherheit / Datenschutz / Prävention (extern)
- Einsatz Cybereregnis

In jedem Bereich werden in fünf Profilen – davon in drei Spezialprofilen –, die zu erwerbenden Kometenzen erlangt.

- IT-Ermittlung
- IT-Forensik
- Cybercrime-Analyse

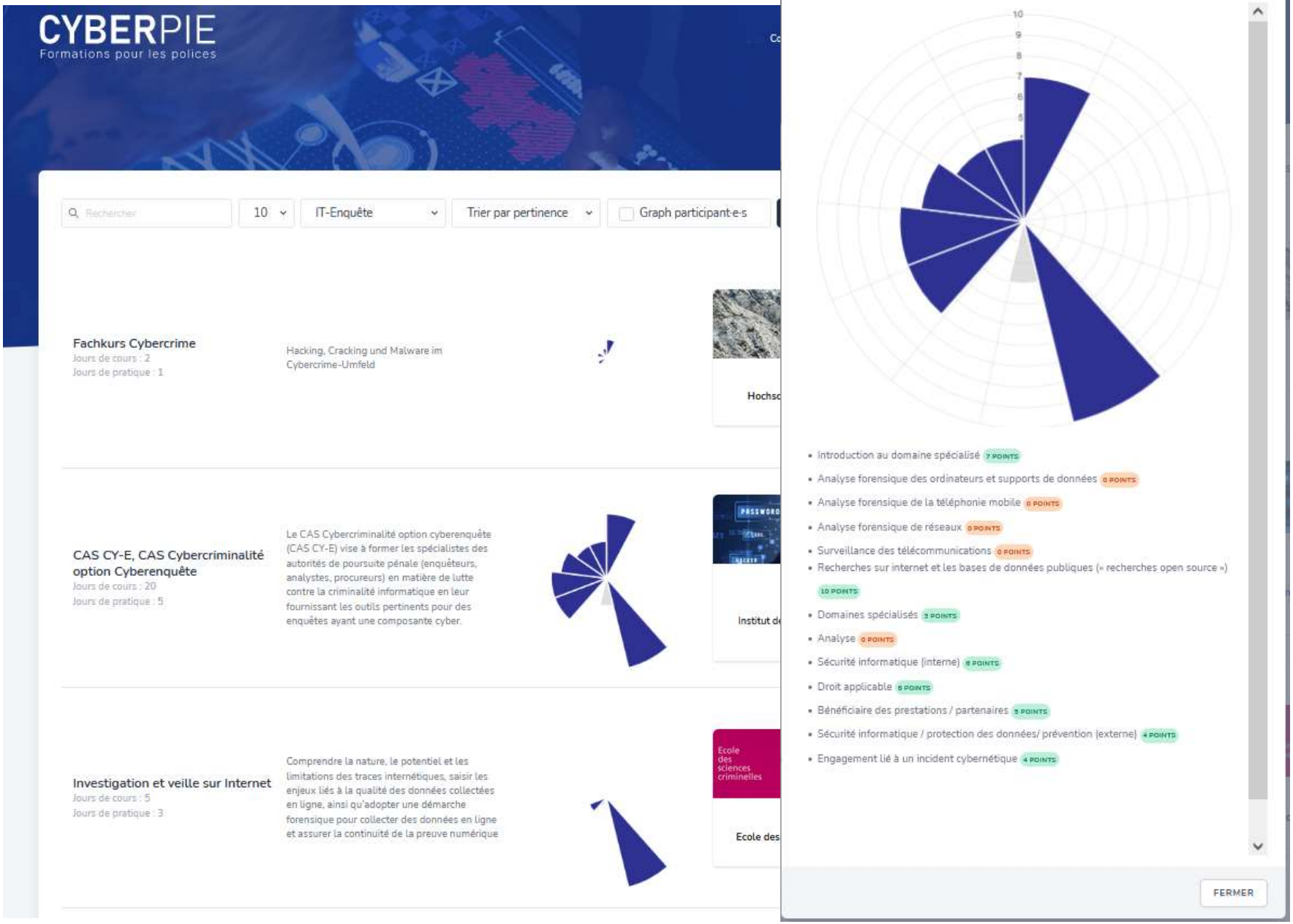
Hes·so

Cyberpie – Ziele

- *Ausbildungsverantwortliche und Führung: klare Orientierungs- und Entscheidungsbasis*
- *Auszubildendes Personal: Schlüssige Gesamtübersicht über das Ausbildungsangebot*
- *Ausgebildetes Personal: Qualifikation aus der abgeschlossenen Ausbildung*
- *Institute und Schulen: Plattform, um ihr Angebot zu präsentieren*

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

Cyberpie – Umsetzung



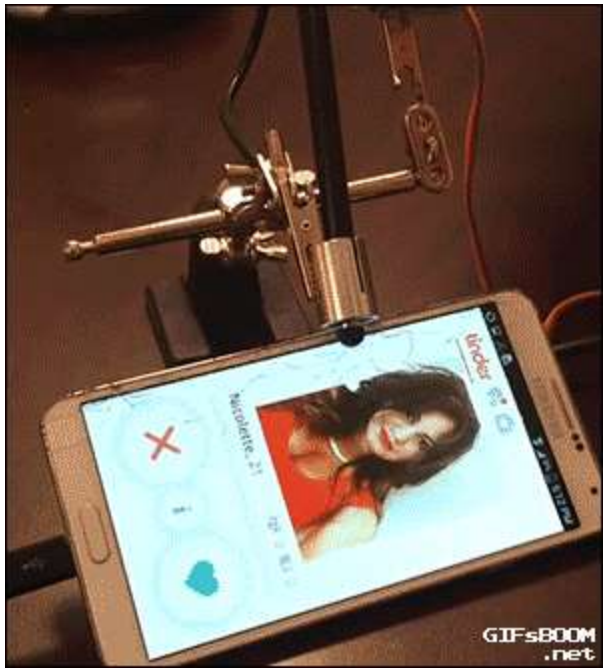
Hes·so

Projekt «Lovid-19»: *Scambaiting* in der Pandemie

Das Phänomen genau untersuchen, um:

- die Opfer besser zu verstehen,
- das Vorgehen der Betrüger/-innen zu analysieren,
- neuartige Präventionsmöglichkeiten zu identifizieren,
- Erkenntnisse aus Fachliteratur zu bestätigen oder zu widerlegen.

Projekt «Lovid-19»: *Scambaiting* in der Pandemie



Sarah | Sandra | Christine

David | Daniel | Martin

Projekt «Interscam»: Fortsetzung

- Anreiz für *Scambaiting* untersuchen und damit verbunden Wege, um das Phänomen zu unterbinden
- Ethische und juristische Grenzen des *Scambaiting* aus polizeilicher Perspektive untersuchen
- Über die Grundlagen einer IA nachdenken

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

Bei Fragen:

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

Hes·so