INSIDER.

TAKE-AWAY

Formation des analystes Cloud

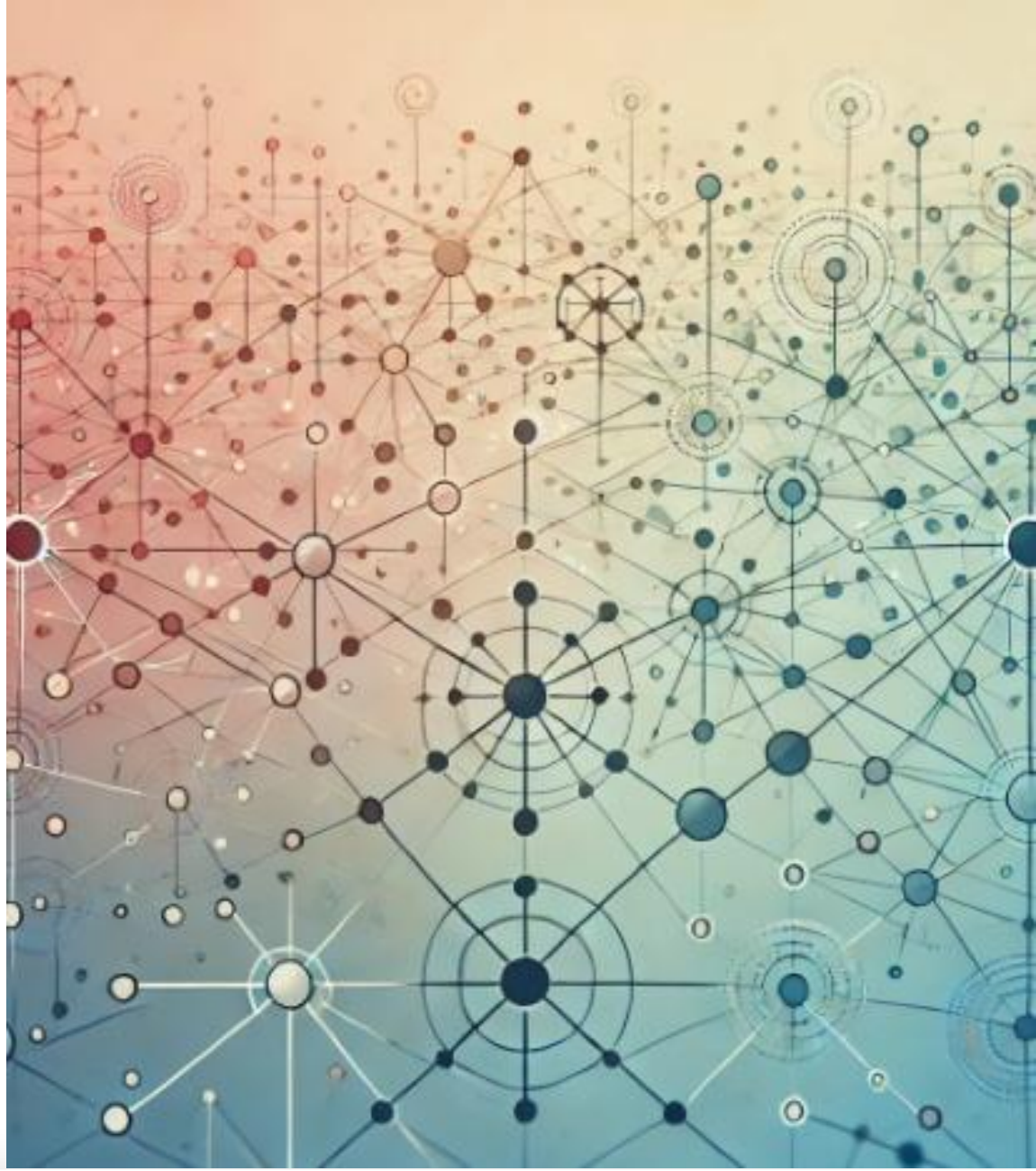
Juillet 2025

LA THÉMATIQUE.

Alors que les environnements de détection SOC (Security Operations Centers) évoluent (professionnalisation, automatisation…) et que les technologies Cloud deviennent de plus en plus spécifiques, on constate que les acteurs de la détection sont (très) rarement formés aux infrastructure Cloud.

Le GT « Formation des analystes Cloud » s'est penché sur la problématique des **compétences nécessaires à la détection des menaces dans le Cloud.**

Trois livrables ont été produits entre avril et novembre 2024. Disponibles sur le Wiki du Studio des communs, ils s'adressent particulièrement aux responsables de SOC et/ou aux organismes de formation qui souhaiteraient faire évoluer leurs programmes.



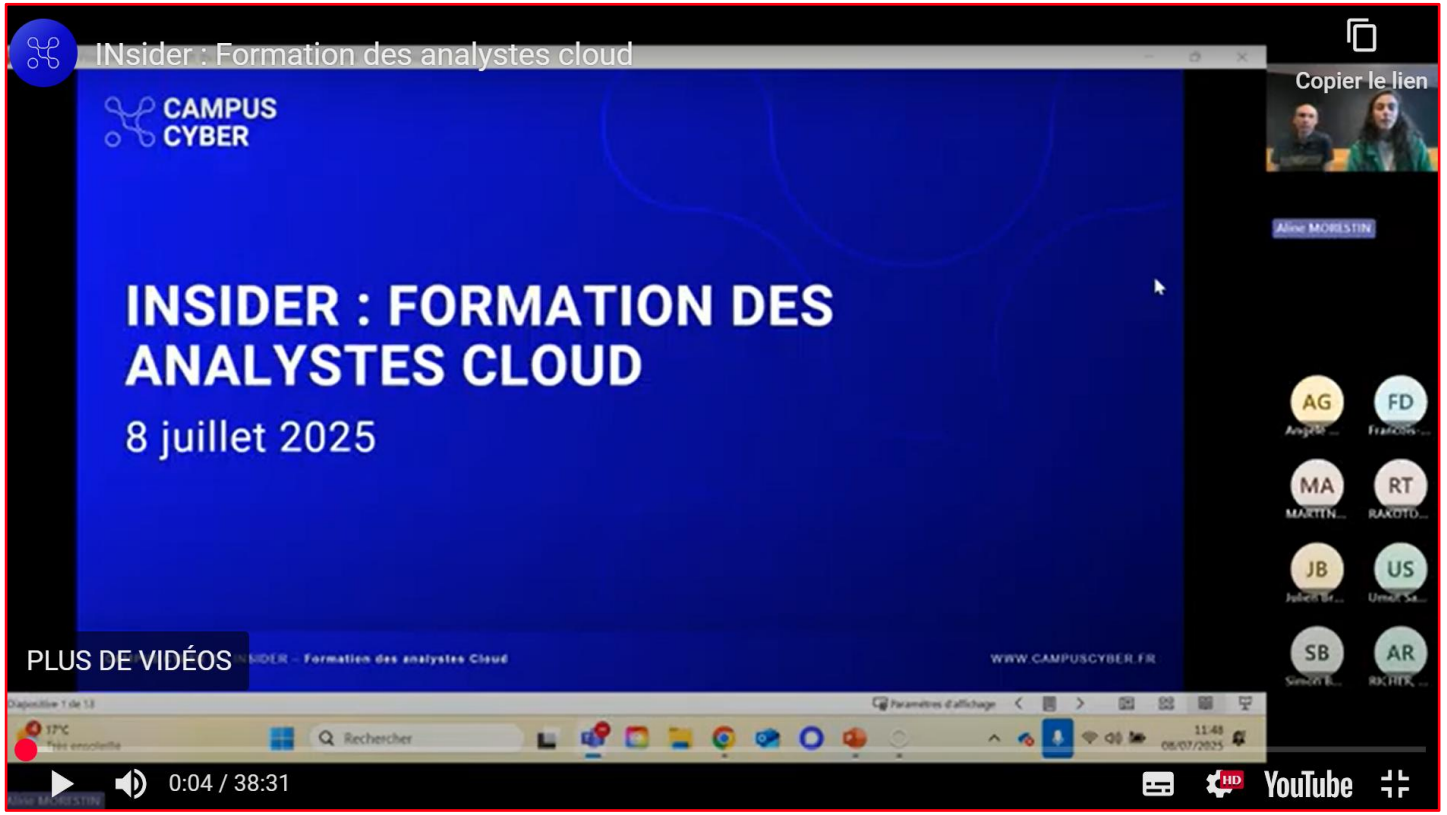
L'INTERVENANT.

PIERRE PARREND

ENSEIGNANT-CHERCHEUR À L'EPITA

Pierre enseigne la cybersécurité et l'Intelligence Artificielle à EPITA Strasbourg. Il est également responsable de l'équipe « Sécurité et Systèmes » du Laboratoire de Recherche de l'EPITA. Ses recherches portent principalement sur la détection des anomalies dans la protection des infrastructures critiques.

LE REPLAY.



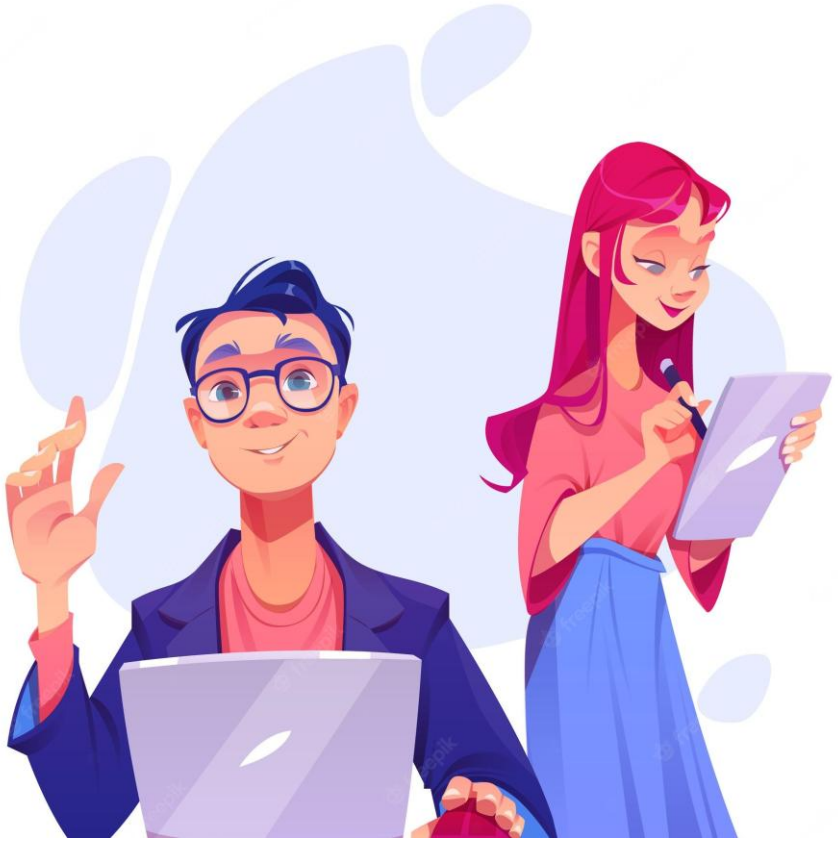
Le replay est disponible sur le Wiki du Studio des communs.

LES 3 POINTS À RETENIR.

+ Les « fiches métiers » produites par le GT apportent une vision précise des compétences nécessaires aux analystes SOC, en fonction de leur niveau d'expertise et de leur expérience (Analyste SOC pour le Cloud N1, Analyste SOC pour le Cloud N2, Analyste SOC pour le Cloud N3, Responsable de SOC, Administrateur technique du SOC). Ce découpage est justifié par le fait que les environnements Cloud sont communs, mais que les infrastructures et les outils de détection restent spécifiques.

+ Les exercices de cadrage listent les pratiques encadrées recommandées pour la formation des professionnels œuvrant en SOC pour les environnements Cloud. Le document présente également une manière d'entrainer / de tester ces professionnels avec un exercice transversal d'intrusion. Il s'agit, pour chaque métier, d'identifier des situations pratiques auxquelles s'entrainer et de mettre en œuvre un exercice d'intrusion Red Team/Blue Team grandeur nature.

+ Le référentiel de certification propose une liste exhaustive des compétences nécessaires aux analystes Cloud, en fonction de leur expertise et de leur expérience (Analyste SOC pour le Cloud N1, Analyste SOC pour le Cloud N2, Analyste SOC pour le Cloud N3). Ces 3 niveaux sont progressifs, et sont atteints en acquérant des compétences 'Cœur de métier' et 'Comportementales et transverses'.



ANNEXE – RECAP' STUDIO.

TOUTE L'ACTUALITÉ DU STUDIO DES COMMUNS DU MOIS DE JUIN, ACCESSIBLE EN DETAILS SUR LE WIKI.

- **Lancement de la CI « Cybersécurité et Supply Chain ».** Deux premiers ateliers de travail ont lieu pour définir le périmètre et les enjeux de la CI.
- **Lancement de la CI « Prospective ».** Les GT élaborent des questionnaires et guides d'interview qui seront déployés auprès des publics cible afin d'établir un rapport de prospective à 3 ans sur le futur marché de la cybersécurité en termes de besoins en équipement, investissements et compétences.

CONSULTEZ LE RECAP' COMPLET

CONTACTS.

Pour contacter le Studio des Communs :
communautes@campuscyber.fr

CAMPUS CYBER