INSIDER.

TAKE-AWAY

Panorama des outils d’aide à la détection dans le Cloud

Septembre 2025

LA THÉMATIQUE.

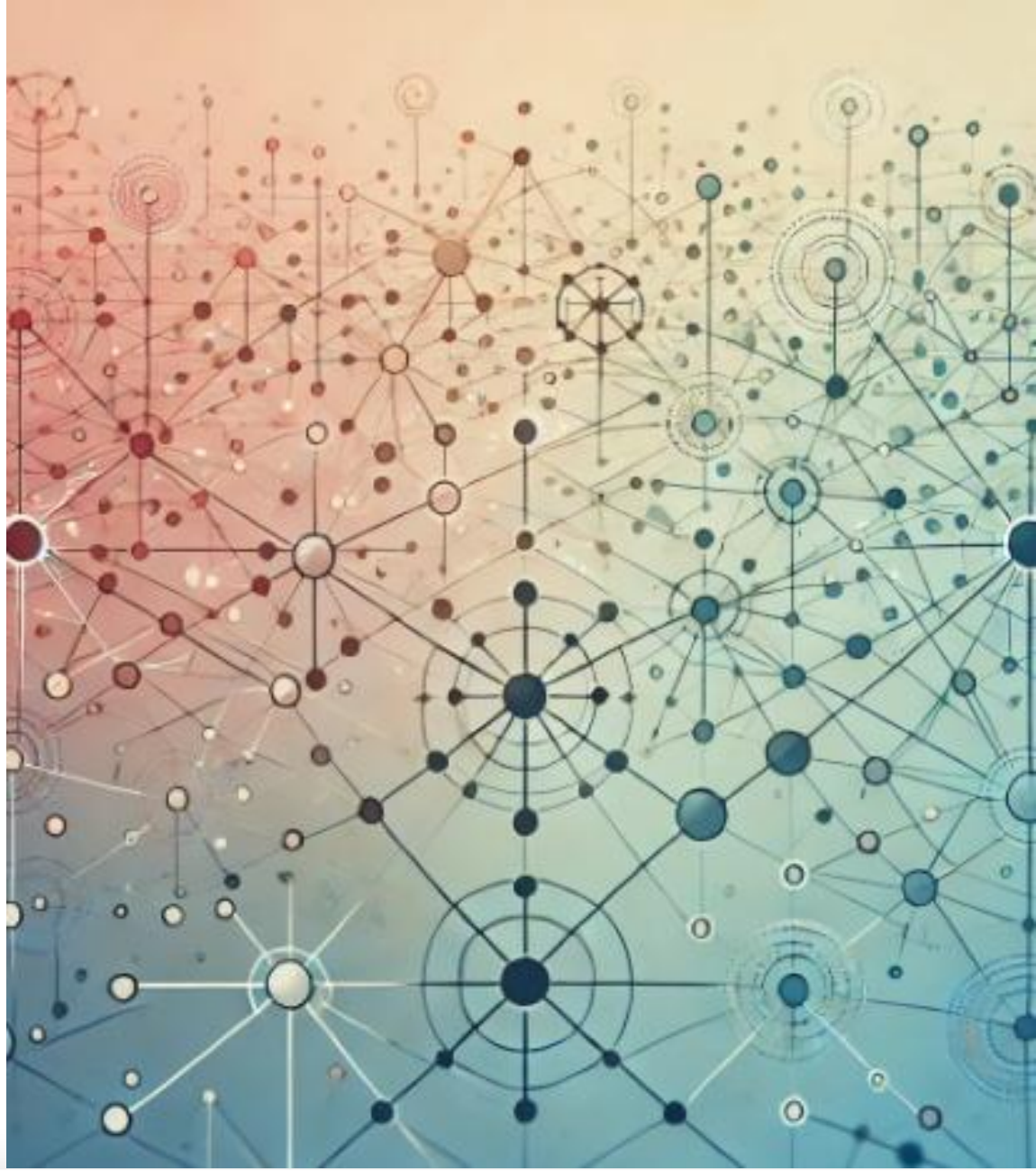
Le Cloud est aujourd'hui présent dans la plupart des organisations, quelles que soient leurs activités et leur volume d'affaire. D'après le rapport de CISCO 2022, 92 % des entreprises questionnées utilisent plusieurs Clouds publics pour en exploiter tout le potentiel et améliorer l'agilité opérationnelle, la sécurité, la performance des applications et la résilience de leurs opérations.

L'utilisation de ce type de solution génère cependant de **nouvelles problématiques de sécurité liées à l'évolution de la surface d'attaque du système d'information** (exposition sur Internet, mauvaises configurations, etc.).

Plusieurs options de sécurité s'offrent alors aux organisations :

1) Utiliser les outils traditionnels, qui peuvent néanmoins être limités sur le Cloud
2) Utiliser un outil spécialisé de type CNAPP (Cloud Native Applications Protection Platform)
3) Hybrider des outils traditionnels avec un CNAPP

Ce livret a pour ambition de vous présenter de façon synthétique **un panorama de ces solutions et un guide de choix en fonction de vos contraintes.**



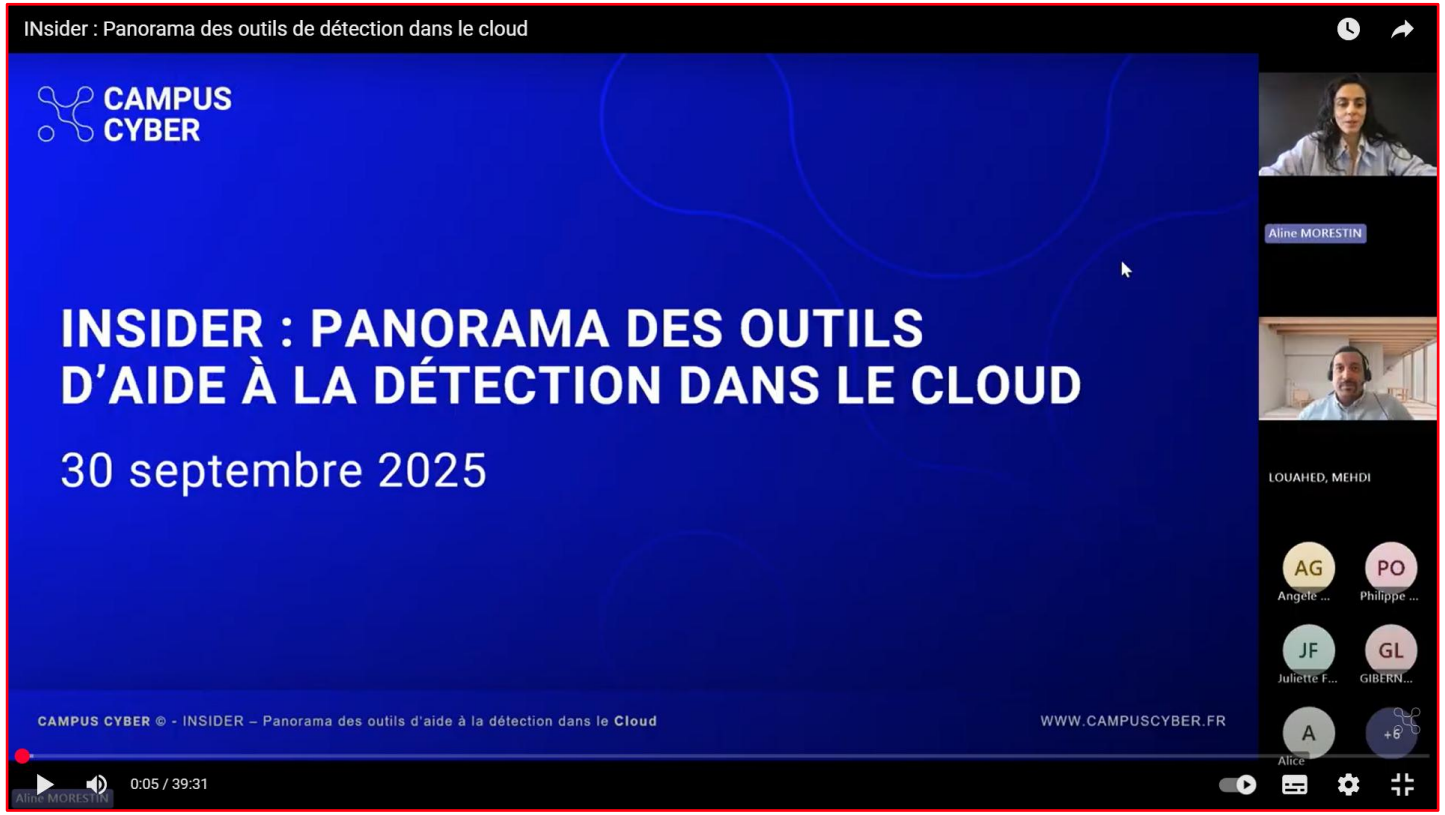
L'INTERVENANT.

MEHDI LOUAHED

MANAGER ARCHITECTURE CYBERSÉCURITÉ CHEZ BOUYGUES TELECOM

Fort de plus de 10 ans d'expérience dans l'architecture cloud, Medhi a participé activement à l'élaboration du panorama des outils d'aide à la détection dans le Cloud. Il a notamment travaillé pour Thalès et EDF, avant de rejoindre les équipes de Bouygues Télécom.

LE REPLAY.



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

LES 3 POINTS À RETENIR.

+ En utilisant le Cloud public, les entreprises font face à de nouvelles menaces :
  - Elargissement de la surface d'attaque ;
  - Dilution des responsabilités entre les clients et les fournisseurs ;
  - Lacune de gouvernance / perte de visibilité dans le déploiement confiés à des équipes pluridisciplinaires.

+ De nouveaux outils peuvent aider à répondre efficacement à ces menaces, **à l'image du CNAPP**. Il permet de :
  - Regagner en visibilité sur les ressources déployées et les niveaux de conformité ;
  - Mettre en évidence les risques et prioriser les remédiations ;
  - Détecter et réagir aux menaces en temps réel ;
  - Gagner en maturité et contrôler en amont.

LES 3 POINTS À RETENIR.

+ Recourir à un CNAPP est un choix qui dépend de la taille et de la maturité de l'entreprise.

  Si un CNAPP est adopté, cela entraine nécessairement une redéfinition de la gouvernance :

  - Une redéfinition des rôles, des responsabilités et des processus ;
  - L'adoption d'une approche basée sur les risques ;
  - Une redéfinition de la transparence envers les équipes, en faisant entrer les métiers dans l'outillage sur un scope correspond à leur responsabilité.

Stratégie	#1 - Outil CSP uniquement	#2 – 100% CNAPP	#3 – Mode hybride CNAPP et outils existants
Pourquoi ?	- Intégration simple - Environnement mono-cloud	- Peu ou pas d'outils existants - Environnement multi-cloud et /ou hybride	- Rationalisation - Capitaliser sur l'existant - Environnement multi-cloud et /ou hybride
Complexité d'implémentation	Moyenne - Activation des outils natifs simples - Nouvelle expertise requise	Complexe - Définition d'une nouvelle gouvernance - Nouvelle expertise requise	Complexe - Définition d'une nouvelle gouvernance - Nouvelle expertise requise - Beaucoup d'équipes à solliciter
Pourrait convenir à...	- Petite entreprise (e.g., start up) < 50 employés - Pas ou peu d'historique - Team IT restreinte	- Peu ou pas d'outils existants - Environnement multi-cloud et /ou hybride	Grande entreprise (e.g., CAC 40) > 1000 employees - Fort historique - Outillage existant pour la majorité des risques

CONTACTS.

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

CAMPUS CYBER