OVHcloud

Les cloud providers et les cyber-menaces

clement.boin@ovhcloud.com

définition d’un cloud provider

Définition du cloud

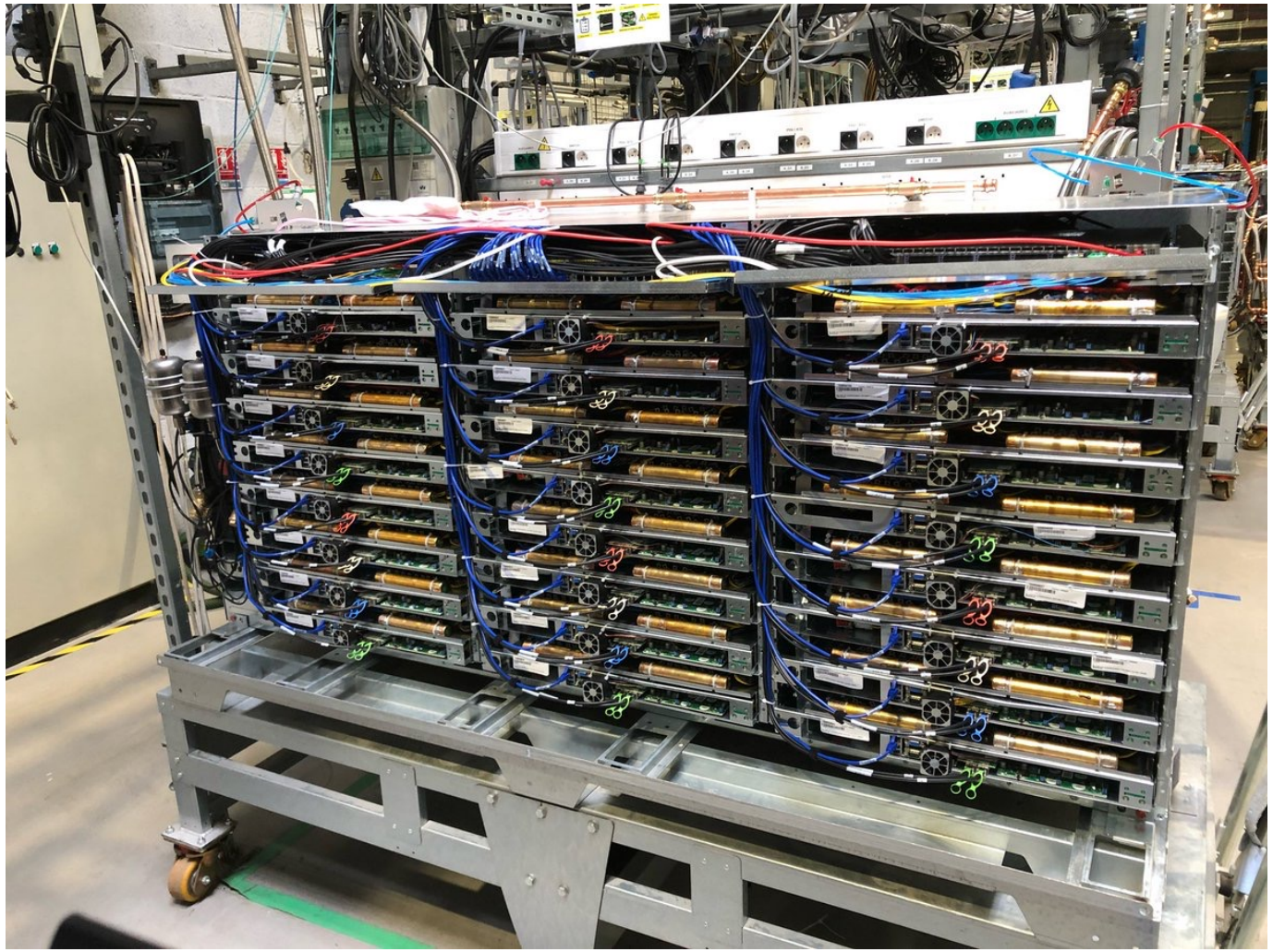
- Le cloud c’est :
  - La **mise à disposition de ressources** informatiques **à la demande**
  - **Sans gestion d’active et directe** par les utilisateurs
- Les avantages sont :
  - **Scalabilité** : propriété d'un système de traiter une quantité **croissante/décroissante** de travail en **ajoutant/supprimant** des ressources au système ;
  - **Flexibilité** : capacité à s'adapter pour répondre aux **exigences uniques** des utilisateurs ;
  - **Economie d’échelle** : **réduction des coûts d’opération** de l’infrastructure, en réduisant les coûts d'achat, de maintenance et de personnel, et en permettant une utilisation plus efficace des ressources.

Source: P. P. Ray, "An Introduction to Dew Computing: Definition, Concept and Implications," in IEEE Access, vol. 6, pp. 723-737, 2018, doi: 10.1109/ACCESS.2017.2775042.

L’infrastructure informatique d’un cloud provider (CP)

- Un CP c’est des ressources de **stockage**, de **calcul** et **réseau**
- Un CP possède beaucoup de ressources, **elle sont distribuées géographiquement**
- Par exemple, OVHcloud c’est :
  - 33 datacenters sur 4 continents,
  - Plus de 600 000 serveurs,
  - Plusieurs dizaise d’Exabytes de stockage,
  - Une capacitée réseau de plus de 50 Tbps.

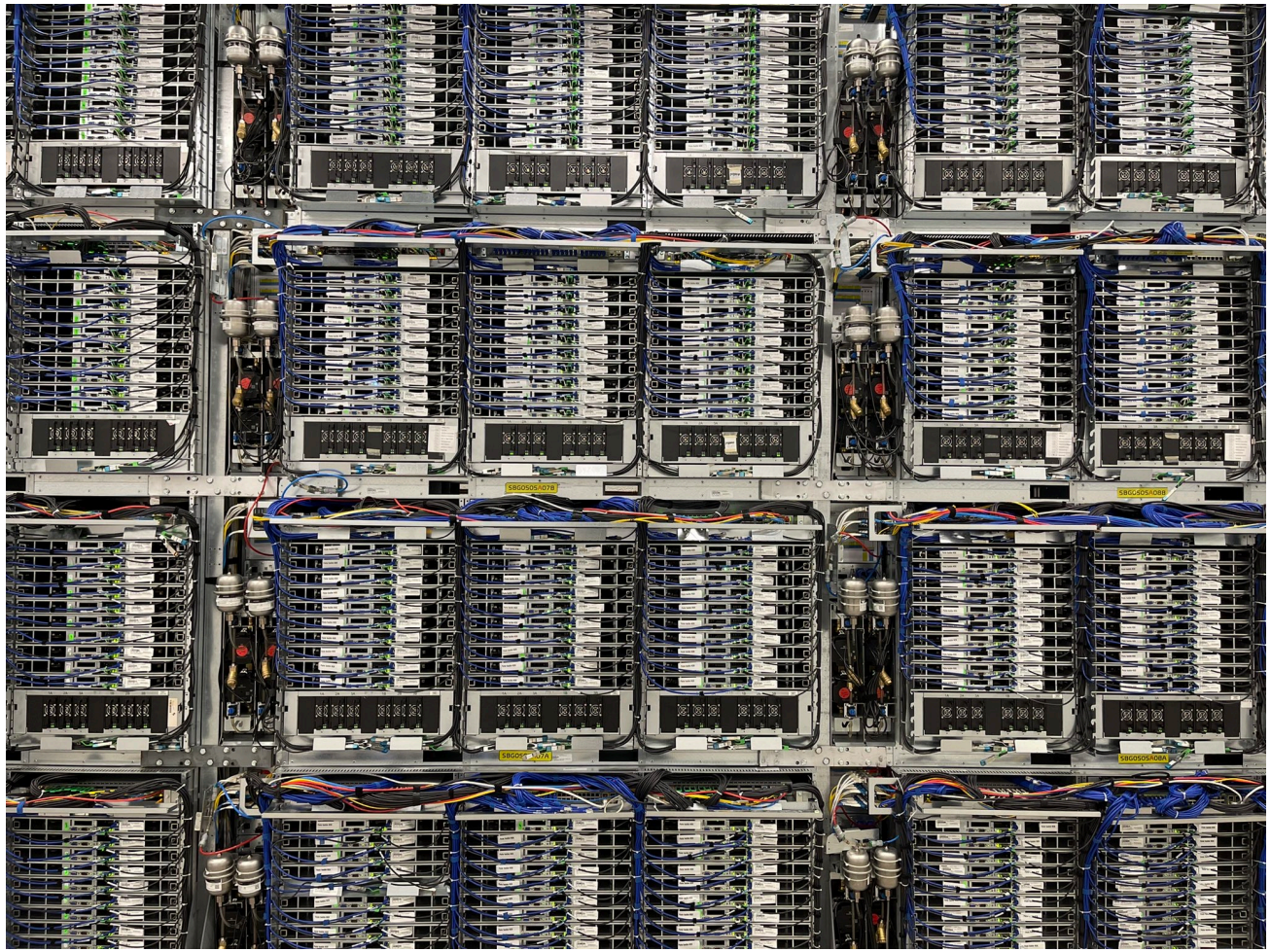
Example d’une baie de 24 serveurs chez OVHcloud



8 GPU par serveur.

Source : https://twitter.com/olesovhcom/status/1546866142748332038

Mur de baies chez OVHcloud

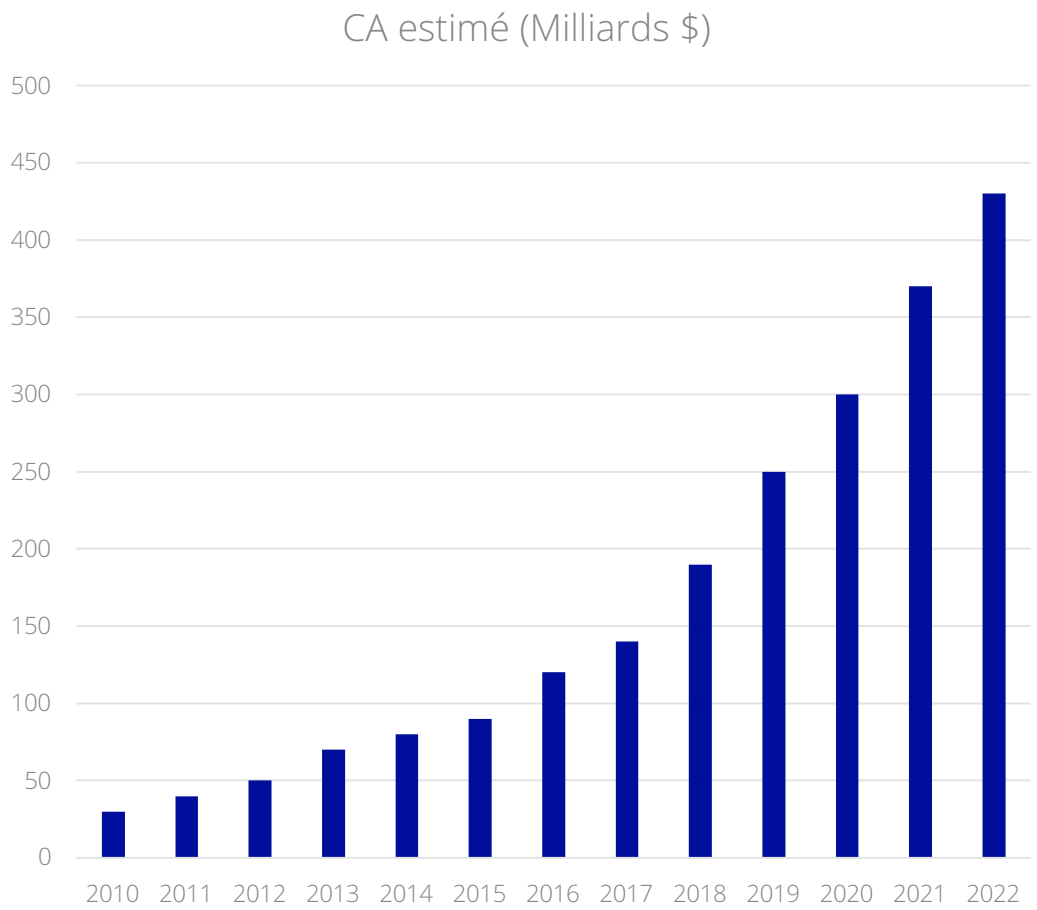


Shadow France

Source : https://twitter.com/olesovhcom/status/1569311645251371011?s=20

Importance des cyber-menaces pour les CP

- L'utilisation **croissante** du cloud, rends ce secteurs vulnérables aux attaques des cybercriminels pour plusieurs raisons.
- Risques pour les entreprises et les utilisateurs :
  - cyber-attaques,
  - perte de données,
  - violation de la vie privée.
- Impact sur les activités :
  - Dégradation de la réputation,
  - Dégradation de la productivité,
  - Pertes financières.



Source: Forrester

Les ressources de cloud providers

Ressources de stockage

- **Le stockage à chaud** représente ce qui se trouve sur un disque dur ou une mémoire flash connectée. Il permet **d'accéder rapidement** aux données et est souvent utilisé pour les **applications critiques en temps réel**.
- **Le stockage à froid** n'est pas toujours connecté à un système informatique. Il est utilisé pour stocker des données peu utilisées qui nécessitent une **mise à disposition rapide en cas de besoin**.
- **L'archivage** est destiné à conserver les données pendant **une longue période de temps**, souvent plusieurs années. Il est moins coûteux, mais les données y sont plus **difficiles à accéder**.

Example de baie de stockage chez OVHcloud

How does 45PB look like? 13PB already open, 32PB will be tomorrow.

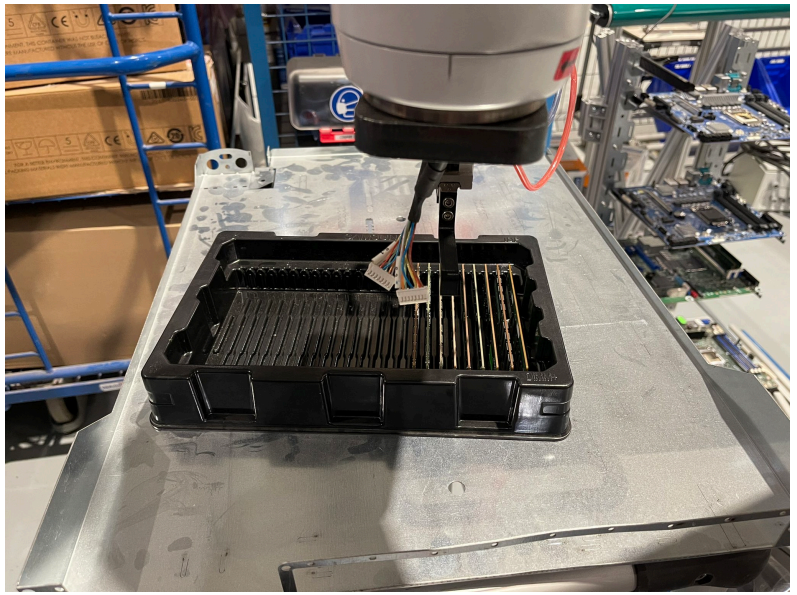
Source : https://twitter.com/olesovhcom/status/1468218400430243845?s=20

Puissance de calcul chez un cloud provider

- La puissance de calcul désigne **la capacité d'exécution des tâches** informatiques telles que le traitement de données, la modélisation, la simulation, l'analyse, etc.
- Elle se mesure généralement en termes :
  - de nombre de cœurs de processeur,
  - de mémoire vive (RAM)
  - puissance de traitement graphique (GPU).

Exemple de puissance de calcul chez OVHcloud

Serveur avec 16 GPU

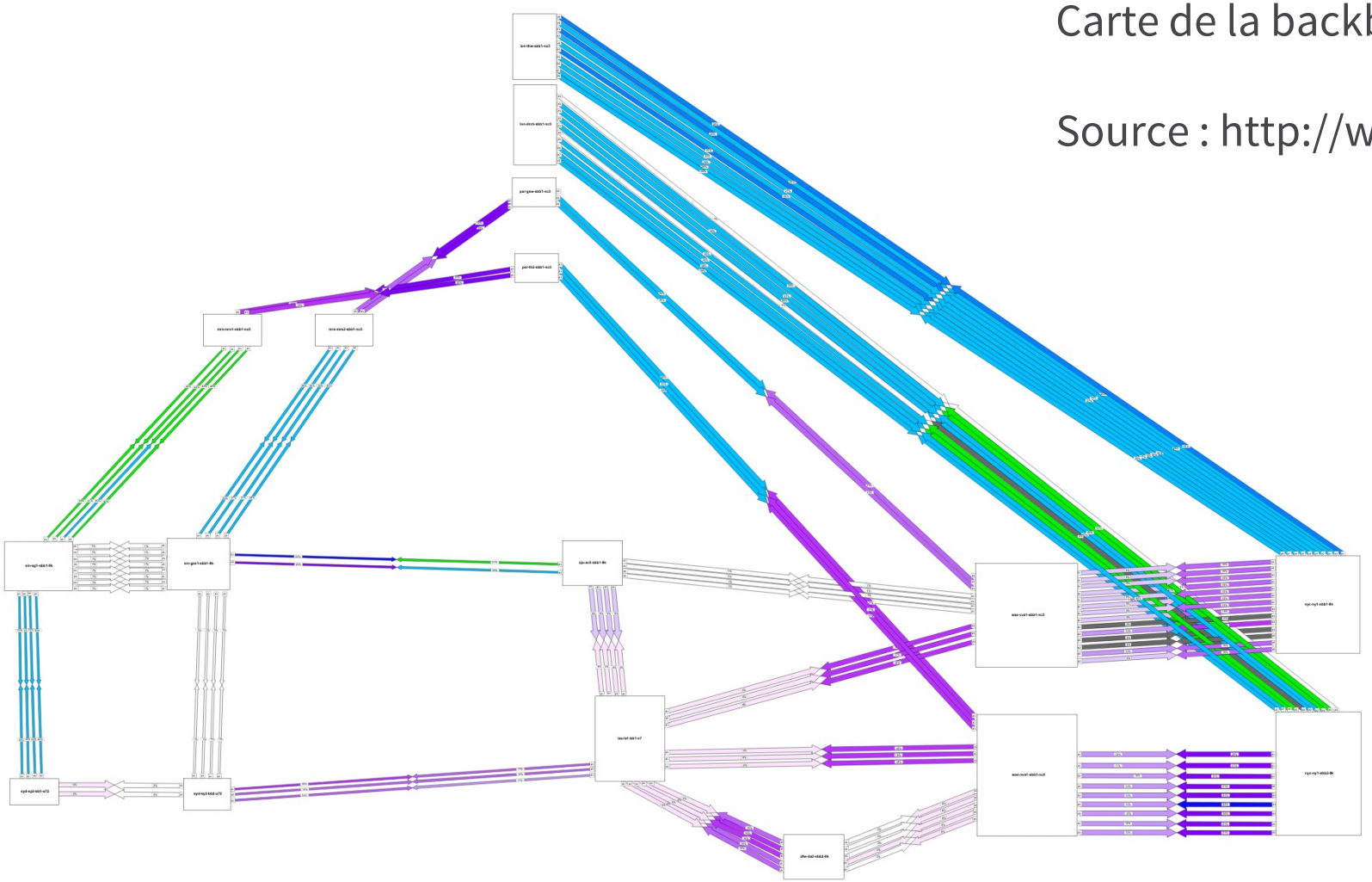


Bras robot pour mettre des barrettes de RAM

Capacité réseau d’un cloud provider

- La capacité de réseau désigne **la quantité de bande passante** et de **débits** disponibles pour les utilisateurs.
- Cela comprend :
  - les capacités de **transmission** de données entrantes et sortantes,
  - la **qualité de service** (QoS) pour les applications sensibles aux délais.
- Les utilisateurs peuvent éviter les **coûts** liés à la **mise en place** et à la **maintenance** d'infrastructures réseaux coûteuses.
- De plus, les fournisseurs de cloud peuvent offrir une connectivité de haute qualité **avec d'autres services cloud** ce qui peut **améliorer** la performance et la disponibilité des applications pour les **utilisateurs finaux**.

Exemple de capacité réseau avec OVHcloud



Carte de la backbone mondiale d’OVHcloud

Source : http://weathermap.ovh.net/#world

Qui sont les cyber-criminels et pourquoi visent-ils les cloud providers

Qui sont les cybercriminels et leurs motivations ?

- Les cybercriminels peuvent être :
  - des groupes organisés,
  - des individus isolés,
  - des nation-états.
- Les motivations des cybercriminels :
  - la collecte d'informations confidentielles,
  - la demande de rançon,
  - la perturbation de services,
  - la reconnaissance de marque.

Pourquoi viser les cloud providers ?

- Les cloud providers sont particulièrement vulnérables aux attaques en raison :
  - De la **quantité** et de la **variété** des données qu'ils stockent,
  - Des **ressources informatiques** dont ils disposent.

Cas pratique : Construction d’un botnet pour DDoS

- Un attaquant peut cibler un fournisseur de cloud dans le but de construire un **botnet** pour lancer des **attaques DDoS** (Distributed Denial of Service).
- **Botnet** : est un réseau de dispositifs (bots) **infectés** par un logiciel malveillant. Les bots peuvent être **contrôlés à distance** en utilisant un canal de **commande et de contrôle** (C&C) pour leur donner des instructions.
- **Attaques DDoS** : est une forme d'attaque qui vise à **rendre un service inaccessible** pour les utilisateurs légitimes en **inondant** la cible avec une **quantité massive** de trafic malveillant.

Cas pratique : Construction d’un botnet pour DDoS

1. **Recherche de vulnérabilité** : L'attaquant recherche des **vulnérabilités** dans les systèmes du fournisseur, en utilisant des **outils automatisés** pour scanner les ports et les applications.
2. **Compromission de l'infrastructure** : Une fois une vulnérabilité identifiée, l'attaquant peut accéder à l'infrastructure du fournisseur de cloud en **exploitant** cette vulnérabilité.
3. **Création du botnet** : L'attaquant peut alors **utiliser** les ordinateurs infectés pour **former** un botnet, qui peut être contrôlé à distance pour lancer des attaques DDoS.
4. **Lancement de l'attaque** : L'attaquant peut lancer une attaque DDoS sur une application cible, en **envoyant** une quantité massive de **trafic malveillant** provenant du botnet.

Comment les cloud providers se protègent des cybermenaces

Normes et bonne pratiques

- Les cloud providers peuvent se protéger des cybermenaces en utilisant :
  - **Normes de sécurité** : adhérer à des normes de sécurité **strictes** telles que le SecNumCloud en France, la norme ISO 27001, et le NIST Cybersecurity Framework aux États-Unis.
  - **Équipes de sécurité dédiées** : avoir des équipes de sécurité **dédiées** qui surveillent en **permanence** les systèmes pour **détecter** les menaces potentielles et y répondre.
  - **Mises à jour régulières et patchs** : **maintenir** des systèmes à jour en installant **régulièrement** les mises à jour et les patchs de sécurité.
  - **Séparation de données** : séparer les données des **différents** clients pour **minimiser** les risques de fuite de données.
  - **Contrôles d'accès** : utiliser des contrôles d'accès pour **gérer les accès** aux données et aux applications dans le cloud.
  - **Documentation complète et transparence** : documenter les **processus de sécurité**, les **politiques de sécurité** et **les contrôles de sécurité** pour garantir la **transparence et la confiance** des clients.

OVHcloud

Merci, des questions ?