DATA SHEET

SERVICES DE SÉCURITÉ MANAGÉS

Public Cloud Native

De quoi est fait le cloud ?

Aujourd'hui, le cloud est devenu monnaie courante. Chaque jour, des entreprises se tournent vers des solutions cloud pour répondre à des besoins opérationnels les plus divers : stockage de données, développement d'applications, problématiques complexes de sécurité réseau, etc. Toutefois, comme c'est souvent le cas avec les technologies émergentes adoptées à marche forcée, beaucoup de choses restent à découvrir sur le cloud, tant en termes de pièges à éviter que de potentiel à exploiter.

Si le cloud a bien des avantages, il apporte aussi son lot de risques. Or, beaucoup d'entreprises choisissent de ne retenir que les avantages et de déléguer toute la partie risque aux fournisseurs de services cloud publics (CSP, *Cloud Service Provider*). Grave erreur, car les responsabilités doivent en fait être comprises et partagées par les deux parties. La gouvernance et la sécurité des systèmes cloud sont des questions majeures. D'où l'importance pour les organisations d'exploiter tous les moyens à leur disposition pour optimiser leurs systèmes tout en protégeant leurs données dans le cloud.

Exploitez tout le potentiel du cloud

Le service Public Cloud Native (PCN) de NTT vous permet de gérer toutes ces problématiques de front. PCN vous aide à vous adapter à ce nouvel environnement agile au moyen de mécanismes sécurisés pour le développement et le déploiement d'applications, ainsi que des outils et formations qui vous aideront à mieux exploiter les fonctionnalités offertes par votre fournisseur.

Les prestations Public Cloud Native :

- Visibilité intégrale sur les contrôles de service implémentés par votre CSP pour une meilleure compréhension de votre environnement cloud
- Surveillance et détection des risques de sécurité en lien avec les questions de conformité, de politiques et de bonnes pratiques
- Suivi des contrôles et du plan de gestion natifs, en partant du principe qu'aucun autre contrôle tiers n'est appliqué

Avantages de Public Cloud Native :

- **Contrôle absolu**
  Visibilité intégrale sur les contrôles de service implémentés par le fournisseur pour une meilleure compréhension de l'environnement cloud
- **Équilibre risques/bénéfices**
  Comprendre les fonctionnalités de votre cloud vous permet de mieux maîtriser cet environnement fluide et changeant, en toute sérénité et en toute sécurité
- **Support multi-cloud**
  Support de nombreuses offres de service cloud, sans aucun agent ni équipement à ajouter
- **Assistance 24h/7j**
  Support H24 assuré par nos centres opérationnels de sécurité (*SOC, Security Operation Centers*)
- **Analyse personnalisée (formule « Enhanced »)**
  Analyse 100 % personnalisable des incidents avec assistance d'experts 24h/7j
- **Amélioration continue**
  PCN-E met à votre disposition Shield X, une solution de micro-services qui s'intègre à votre cycle de développement pour vous offrir des mises à jour continues qui renforcent votre sécurité

Schéma 1 : Les quatre piliers de Public Cloud Native

PCN se décline en deux formules :

Standard

Public Cloud Native Standard (PCN-S) s'adresse aux entreprises qui n'envisagent pas une refonte complète de leur structure, et dont les équipements de sécurité obéissent à des politiques et des obligations réglementaires standard. Le service PCN-S se base sur des règles et un profil de conformité standard pour identifier les anomalies et signaler les incidents de sécurité dans les environnements cloud suivants :

- Amazon Web Services (AWS) – CloudTrail
- Microsoft Azure – Azure Monitor

Quelques exemples de détections :

Bonnes pratiques de sécurité – incidents de sécurité symptomatiques d'un manquement aux bonnes pratiques et recommandations : erreur d'authentification, modification des politiques, appels API non autorisés...

Conformité aux politiques internes – incidents de sécurité indiquant une infraction aux politiques internes prédéfinies sur la base des exigences de conformité standard de NTT.

Analyse comparative – contrôle du respect des cadres règlementaires sectoriels.

Enhanced

Le service Enhanced (PCN-E) est spécialement conçu pour les entreprises qui souhaitent explorer pleinement toutes les opportunités du cloud. À l'aide de règles personnalisées, PCN-E effectue des missions d'identification et de reporting dans les environnements CSP cités ci-contre, avec à la clé une visibilité et une protection renforcées par rapport aux méthodes traditionnelles de type pare-feu classiques.

En outre, PCN-E propose **SHIELD X**, une solution de micro-services qui s'intègre en toute transparence à votre cycle de développement pour vous offrir des mises à jours continues. Sans impact pour vos systèmes, Shield X améliore continuellement notre offre PCN-E.

A propos de NTT

NTT est un leader mondial des services technologiques. Convaincus qu'ensemble nous accomplissons de grandes choses, nous avons conjugué les capacités de 28 entreprises remarquables afin de créer un leader des services technologiques. En partenariat avec vous, nous mettons notre gamme complète de capacités hors pair au service de vos collaborateurs, stratégies, opérations et technologies. Ensemble nous préparons le futur connecté.

Vous souhaitez en savoir plus sur nos services de sécurité managés ?

Rendez-vous sur **hello.global.ntt**

