



COMMENT SECURISER LES ECHANGES MICROSERVICES AU SEIN DU SI ?

L'évolution des systèmes d'information, d'un modèle Legacy type SOA à une architecture type Microservices, ainsi que les nouvelles cinématiques liées au Cloud et à la conteneurisation, imposent de revoir les outils et méthodes mis en place pour sécuriser les échanges.

Les services ont un cycle de vie plus court, leurs IP ne sont plus fixes, et leur nombre croît exponentiellement. Les anciennes méthodes de sécurisation telles le filtrage IP ne suffisent plus. Le modèle en « zones de confiance » est abandonné au profit d'une approche *Zero Trust*, déportant au niveau applicatif les contrôles anciennement au niveau réseau.

Il est alors essentiel de savoir comment s'adapter, pour garder une maîtrise sur la sécurisation des échanges au sein du SI. Il faut déplacer la sécurité au plus près de chaque service, privilégier la fédération au proxy, le contrôle d'accès au filtrage, etc.

Objectif du stage :

Dans le cadre de ce stage, vous serez amené à déterminer les solutions et bonnes pratiques les plus pertinentes pour répondre aux challenges mis en perspective ci-avant par les nouvelles pratiques Microservices dans un contexte Cloud et conteneurisé. Vos objectifs de stages seront de :

- Etudier les impacts des nouvelles pratiques orientées cloud sur la sécurisation des échanges Microservices.
- Se construire une expertise sur les challenges liés à la sécurisation des échanges entre Microservices, et les outils permettant d'y répondre.
 - Exemples de solutions :
 - Explorateur de services (type HashiCorp Consul)
 - Service Mesh (type ISTIO)
 - Micro Gateways d'API Management
 - ...
- Faire aboutir ces recherches par une expérimentation (POC) permettant de mettre en pratique et démontrer la plus-value apportée par les solutions identifiées.

Travaux à réaliser

Intégré pour la durée de votre stage au sein d'une tribu sur la sécurité des systèmes d'information, vous serez amené, sous la supervision d'un consultant expérimenté, à réaliser les travaux suivants :

- Cadrage :
 - Rédiger une note de cadrage du sujet de stage, comprenant :
 - Votre compréhension du stage
 - Le planning et les jalons clés
 - La liste des livrables à réaliser

- Etude :
 - Comprendre et expliquer les problématiques de sécurisation des échanges Microservices au sein d'un SI dans le contexte actuel.
 - Dresser un état des lieux des solutions permettant de répondre à ces problématiques, et en déterminer les cas d'usage.
 - Effectuer un comparatif détaillé (fonctionnel et technique) de deux à trois solutions par catégorie, afin de connaître les spécificités de chacune et de se forger une conviction.

- Mise en pratique :
 - Identifier une solution susceptible d'être intéressantes à mettre en place dans le cadre d'un POC.
 - Mettre en œuvre la solution identifiée au travers d'un démonstrateur.
 - Le but est de démontrer l'intérêt des solutions choisies pour sécuriser les échanges entre Microservices de façon à répondre aux problématiques actuelles.
 - Ce démonstrateur pourra être réutilisé dans un séminaire Nexworld.

- Pour aller plus loin :
 - Participer au développement de la tribu en apportant les connaissances acquises durant le stage.
 - Participer à la mise à jour des documentations Nexworld sur le sujet : séminaires, articles, livres blancs, retours d'expérience, etc.
 - Participer à la définition d'une conviction Nexworld sur les bonnes pratiques de sécurisation des Microservices dans un contexte Cloud.

En parallèle, vous participerez à des missions de conseil, en intégrant une équipe de consultants Nexworld placée sous la responsabilité d'un directeur de mission.