SECURISATION DES SECRETS DANS UN CONTEXTE CLOUD

L'arrivée des technologies Cloud, IaaS et PaaS, Public ou On Premise, change profondément l'architecture des applications ainsi que les méthodes de travail des équipes MOE. La gestion des secrets techniques ainsi que les outils associés doivent évoluer pour garantir leur confidentialité face à l'autonomie grandissante des équipes de développement et à la granularité des architectures type Microservices.
La manipulation des secrets par les différents acteurs du SI doit être limitée au maximum. Également, la confidentialité des secrets doit être garantie au sein des systèmes applicatifs et des chaines de déploiement.

Pour se faire, les solutions de coffre-fort numérique et autres outils cryptographiques doivent offrir une approche self-service, industrialisable, intégrée aux pipelines de déploiement des applications et compatible avec les technologies d'hébergement type Cloud.

Objectifs du stage

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

- Acquérir une solide base de connaissances théoriques et techniques sur les mécanismes cryptographiques associés à la gestion des secrets (coffre-fort numérique, cérémonie des clés, autorité de certification, chiffrement, facteur d'authentification, échanges de clés, etc…)
- Etudier les impacts des nouvelles pratiques orientées Cloud sur la sécurisation des secrets d'infrastructures (mots de passe de base de données, certificats, clés de chiffrement...)
- Identifier des outils et pratiques permettant de sécuriser ces secrets durant tout le cycle de vie d'un projet informatique (réalisation, déploiement, maintenance, évolution, test, etc…)
- Implémenter et tester plusieurs solutions afin de réaliser un comparatif prenant en compte les enjeux de sécurité, d'exploitation, d'agilité et de coût.
- Une des solutions testées doit s'appuyer sur le produit Vault Hashicorp, considéré comme à l'état de l'art pour répondre à cette problématique.

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 :

- 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.
- Expliciter et mettre en évidence les problématiques de protection des secrets dans un contexte Cloud.
- Monter en compétence sur le produit Vault Hashicorp comme première solution à l'état de l'art de cette problématique.

- Réaliser un POC sur le produit Vault Hashicorp comprenant les points suivants :
    - Déploiement et utilisation du produit
    - Intégration dans un hébergement type PaaS et IaaS
    - Intégration dans une chaine CI/CD
- Identifier des solutions et implémentations alternatives permettant de réaliser à minima un second POC.
- Réaliser un comparatif fonctionnel et technique de ces outils prenant en compte les enjeux de sécurité, d'exploitation, d'agilité et de coût.
- Participer à la mise à jour des documentations Nexworld concernant ce sujet : séminaires, articles, livres blancs, retours d'expérience, etc…
- Participer à la définition d'une conviction Nexworld sur les bonnes pratiques de protection des secrets sur un hébergement 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.