RÉSUMÉ DE 1ère PÉRIODE EN ENTREPRISE

Sécurité des services et applications cloud

Dates de la période : 11//2024 – 08//2025

Entreprise / Département : Cloud Temple / Cloud Provider

Maître / Tuteur d'apprentissage : Paul LEPETIT

Tuteur pédagogique : Kamel MOULAOUI

Résumé

Durant mon alternance chez *Cloud Temple*, acteur majeur du cloud de confiance en France, j'ai occupé le poste de **Cloud Security Engineer Junior**.

Certifiée **SecNumCloud, ISO 27001** et **HDS**, l'entreprise accompagne des clients sensibles dans des secteurs critiques tels que la santé, l'industrie et la finance, en alliant sécurité, conformité et innovation dans ses services cloud.

Mon expérience s'est inscrite donc dans ce contexte hautement exigeant en matière de sécurité et de disponibilité, cela m'a permis de contribuer à des projets directement liés à la cybersécurité et à la fiabilité des infrastructures cloud.

Ma mission principale consistait à renforcer **la sécurité des services** et **des processus internes**. Les enjeux pour *Cloud Temple* étaient multiples :

- **Assurer la conformité réglementaire** essentielle pour conserver la confiance de ses clients issus de secteurs critiques.
- **Renforcer la posture de sécurité** de l'entreprise face à la montée des cybermenaces, les attaques ciblant les environnements cloud et les chaînes CI/CD.
- **Garantir la souveraineté numérique**, les choix technologiques doivent rester compatibles avec l'indépendance et la sécurité des données sensibles.
- **Optimiser l'efficacité opérationnelle**, en intégrant la sécurité directement dans les processus DevOps afin d'éviter des interventions correctives coûteuses en production.

1. Projets réalisés lors de mon alternance

1.1. Sécurisation des pipelines CI/CD

J'ai intégré **OWASP ZAP** dans les pipelines GitLab CI afin d'automatiser les tests de sécurité des applications internes. Cette intégration a permis de détecter des vulnérabilités dès les phases de développement, grâce à des rapports transmis aux équipes de sécurité et CSP ce qui leur a permis d'y remédier rapidement.

1.2. Sécurité des images Docker

Le second projet consistait à sécuriser les images Docker, en déployant **Trivy** pour le scan de vulnérabilités et **Cosign** pour la signature et la vérification des images, cela réduit les risques liés aux dépendances et d'assurer la traçabilité des images, ce qui a permis de détecter et corriger les vulnérabilités avant le déploiement.

1.3. Études comparatives de solutions de sécurité

Dans notre contexte, j'ai réalisé 2 **analyses comparatives**: l'une pour sélectionner un WAF et l'autre pour identifier une solution sécurisée de partage de secrets, elles ont été présentées sous forme de tableaux et d'exposés oraux auprès de l'équipe décisionnelle, mes analyses ont été validées par mon tuteur et retenues par l'équipe décisionnelle pour orienter certains choix techniques.

1.4. Gestion sécurisée du partage de secrets

Enfin, j'ai étudié et testé des solutions telles que **Yopass** et **Cryptgeon**, destinées à sécuriser le partage secret dans le but d'éliminer les échanges en clair via des canaux non sécurisés (messageries teams, emails) et à proposer une solution interne adaptée aux besoins des équipes et des clients.

2. Compétences mises en œuvre

Ces projets m'ont permis de mobiliser un ensemble de compétences variées :

- **Techniques** : GitLab CI/CD, Python, Docker, outils de sécurité (ZAP, Trivy, Cosign) et pratiques DevSecOps.
- **Méthodologiques** : conduite d'études comparatives, rédaction de rapports techniques, synthèse des résultats sous forme de présentations.
- **Professionnelles** : travail collaboratif, communication avec des équipes pluridisciplinaires, restitution de résultats à des décideurs techniques.

En conclusion, cette alternance a constitué une expérience formatrice et enrichissante. Elle m'a permis de contribuer à l'amélioration de la sécurité des services de l'entreprise, de développer des compétences techniques solides et de renforcer ma posture professionnelle dans un environnement exigeant. Cette première année m'a donné une

vision claire des enjeux de la sécurité cloud et m'a préparé à aborder ma deuxième année de Master avec des bases opérationnelles robustes.

Abstract

During my work-study program at *Cloud Temple*, a leading trusted cloud provider in France, I held the position of **Junior Cloud Security Engineer**.
Certified **SecNumCloud**, **ISO 27001**, and **HDS**, the company supports sensitive clients in critical sectors such as healthcare, industry, and finance, combining security, compliance, and innovation in its cloud services.

My experience took place in this highly demanding context in terms of security and availability, allowing me to contribute to projects directly related to cybersecurity and the reliability of cloud infrastructures.

My main mission was to strengthen the **security of internal services** and **processes**. The challenges for *Cloud Temple* were multiple:

- Ensure regulatory compliance, essential to maintain the trust of clients from critical sectors.
- Strengthen the company's security posture against the rise of cyber threats, particularly attacks targeting cloud environments and CI/CD pipelines.
- Guarantee digital sovereignty, ensuring technological choices remain compatible with the independence and security of sensitive data.
- Optimize operational efficiency by integrating security directly into DevOps processes to avoid costly corrective actions in production.

1. Projects carried out during my work-study

1.1. Securing CI/CD pipelines

I integrated OWASP ZAP into GitLab CI pipelines to automate security testing of internal applications. This integration allowed vulnerabilities to be detected early in the development phases, with reports shared with the security and CSP teams, enabling prompt remediation.

1.2. Docker image security

The second project focused on securing Docker images by deploying Trivy for vulnerability scanning and Cosign for signing and verifying images. This reduced risks associated with dependencies and ensured image traceability, allowing vulnerabilities to be detected and corrected before deployment.

1.3. Comparative studies of security solutions

In this context, I conducted two comparative analyses: one to select a WAF and the other to identify a secure secret-sharing solution. These analyses were presented to the decision-making team in the form of tables and oral presentations, validated by my tutor, and retained by the team to guide certain technical decisions.

1.4. Secure secret-sharing management

Finally, I studied and tested solutions such as Yopass and Cryptgeon to secure secret sharing, eliminating plaintext exchanges via insecure channels (Teams, emails) and proposing an internal solution adapted to the needs of both teams and clients.

2. Skills applied

These projects allowed me to apply a range of skills:

- **Technical:** GitLab CI/CD, Python, Docker, security tools (ZAP, Trivy, Cosign), and DevSecOps practices.
- **Methodological:** conducting comparative studies, writing technical reports, and summarizing results in presentations.
- **Professional:** collaborative work, communication with multidisciplinary teams, and presenting results to technical decision-makers.

In conclusion, this apprenticeship has been both a formative and rewarding experience. It allowed me to contribute to strengthening the security of the company's services, to develop solid technical skills, and to enhance my professional maturity within a demanding environment. This first year has provided me with a clear understanding of the challenges of cloud security and has prepared me to approach my second year of the Master's program with strong operational foundations.