Executive Summary – Alternance chez Onet Sécurité

El kbabty Mouad

Introduction

Dans le cadre de ma formation en Master 2 MIAGE, j'ai effectué une alternance de deux ans chez Onet Sécurité, filiale du groupe Onet spécialisée dans les solutions de sécurité et de sûreté électronique. Forte de son expertise dans la gestion des systèmes d'alarme, de vidéosurveillance et de contrôle d'accès, l'entreprise accompagne de nombreux clients dans la sécurisation de leurs sites sensibles.

Intégré au sein de l'équipe R&D en tant que développeur fullstack, j'ai pu participer activement à des projets structurants pour l'entreprise. Mon rôle a notamment porté sur la refonte de l'authentification de nos serveurs et l'amélioration de la communication avec nos équipements, deux chantiers majeurs à fort impact client.

Problématique et contexte métier

L'un des problèmes rencontrés par Onet Sécurité concernait la connexion instable et peu flexible entre notre serveur central et les systèmes d'information de nos clients. Plus précisément, la solution d'authentification utilisée jusque-là — basée sur Tomcat Realm — montrait ses limites en matière de compatibilité avec les environnements clients modernes, notamment en contexte d'intégration avec des systèmes de type Active Directory, ou SSO d'entreprise.

Cette difficulté représentait un frein à l'intégration de notre plateforme dans les SI clients, ralentissait les déploiements, et générait des coûts de maintenance supplémentaires. Il devenait donc impératif de moderniser et sécuriser notre système de gestion des connexions tout en répondant aux normes attendues (SAML, LDAP…).

En parallèle, un second axe stratégique portait sur la migration de la communication entre notre serveur applicatif et nos périphériques terrain (concentrateurs, capteurs, lecteurs d'accès…). L'usage des WebSocket n'était plus adapté à l'échelle et à la robustesse attendue. Il a donc été décidé de basculer vers une architecture orientée message avec NATS, pour améliorer la scalabilité et la résilience du système.

Missions réalisées et valeur ajoutée

1. Refonte du système d'authentification : de Tomcat Realm à Spring Security avec SAML & LDAP

Ma première mission a consisté à concevoir et implémenter une nouvelle architecture d'authentification, plus modulaire, sécurisée et interopérable. J'ai :

- Migré l'ancienne solution d'authentification (Tomcat Realm) vers Spring Security, en mode full Java backend.
- Intégré une gestion SAML pour permettre la fédération d'identité avec les annuaires d'entreprise des clients (SSO).
- Couplé la solution avec un service LDAP pour la gestion fine des rôles et utilisateurs.
- Développé des fonctionnalités d'import/export d'utilisateurs pour faciliter les déploiements et les synchronisations.
- Défendu ma conception technique lors de réunions avec l'équipe architecture et sécurité.
- Participé aux phases de test avec l'équipe QA, notamment via le framework RobotFramework.

Cette solution est déployée en production chez un client depuis janvier 2025. Les retours ont été très positifs, et le client a salué la simplicité d'intégration ainsi que la robustesse du mécanisme d'authentification.

2. Migration de la communication serveur ↔ concentrateurs : de WebSocket à NATS

J'ai également travaillé sur un projet technique d'envergure visant à remplacer le canal WebSocket utilisé pour piloter nos périphériques terrain. Après une phase d'étude, nous avons opté pour NATS, une solution de messagerie légère, rapide et résiliente.

Ma contribution a couvert :

- L'analyse comparative des solutions existantes (MQTT, Kafka, NATS).
- La participation à la migration de l'infrastructure réseau, avec adaptation des messages émis par nos concentrateurs.
- La modification de la couche de communication du serveur, pour qu'il publie et consomme via NATS.

- La mise en place d'un monitoring simple pour les flux de messages.

Cette évolution permet une meilleure gestion de la charge, une résilience accrue en cas de coupure réseau, et pose les bases d'un système plus distribué pour l'avenir.

Résultats et bilan personnel

Au terme de ces deux années, les projets menés ont permis de :

- Moderniser le cœur d'un produit critique pour l'entreprise.
- Accélérer les intégrations clients, réduisant les délais de mise en service.
- Renforcer la sécurité et la conformité des échanges d'authentification.
- Améliorer la communication avec le matériel terrain, avec un gain de stabilité notable.

J'ai également acquis de solides compétences techniques : Spring Security, SAML, LDAP, RobotFramework, messagerie NATS, mais aussi des compétences transverses : travail en équipe, expression orale en contexte technique, documentation, support client.

Cette alternance m'a permis de prendre en charge des missions à forte responsabilité, tout en étant encadré et challengé. Elle constitue pour moi un tremplin vers une future carrière en développement logiciel dans un contexte exigeant.

Conclusion

Mon alternance chez Onet Sécurité a été marquée par des projets concrets, à fort impact, dans un domaine sensible où la qualité et la fiabilité sont des impératifs. En me confiant des responsabilités techniques dès les premiers mois, l'entreprise m'a permis de monter en compétence rapidement et d'évoluer dans un environnement stimulant.

À travers ces missions, j'ai su démontrer ma valeur ajoutée en apportant des solutions robustes, évolutives et adaptées aux attentes des clients finaux. L'ensemble de ces expériences me prépare aujourd'hui à intégrer le marché du travail avec des bases solides en architecture logicielle, sécurité des systèmes et travail collaboratif.