Sécurité des services et applications cloud

RAPPORT DE 1ère PÉRIODE EN ENTREPRISE

Prénom NOM: Massinissa BRAHIMI

Formation: Master MSI – Parcours Sécurité des Systèmes Informatiques en apprentissage

Promo : 14

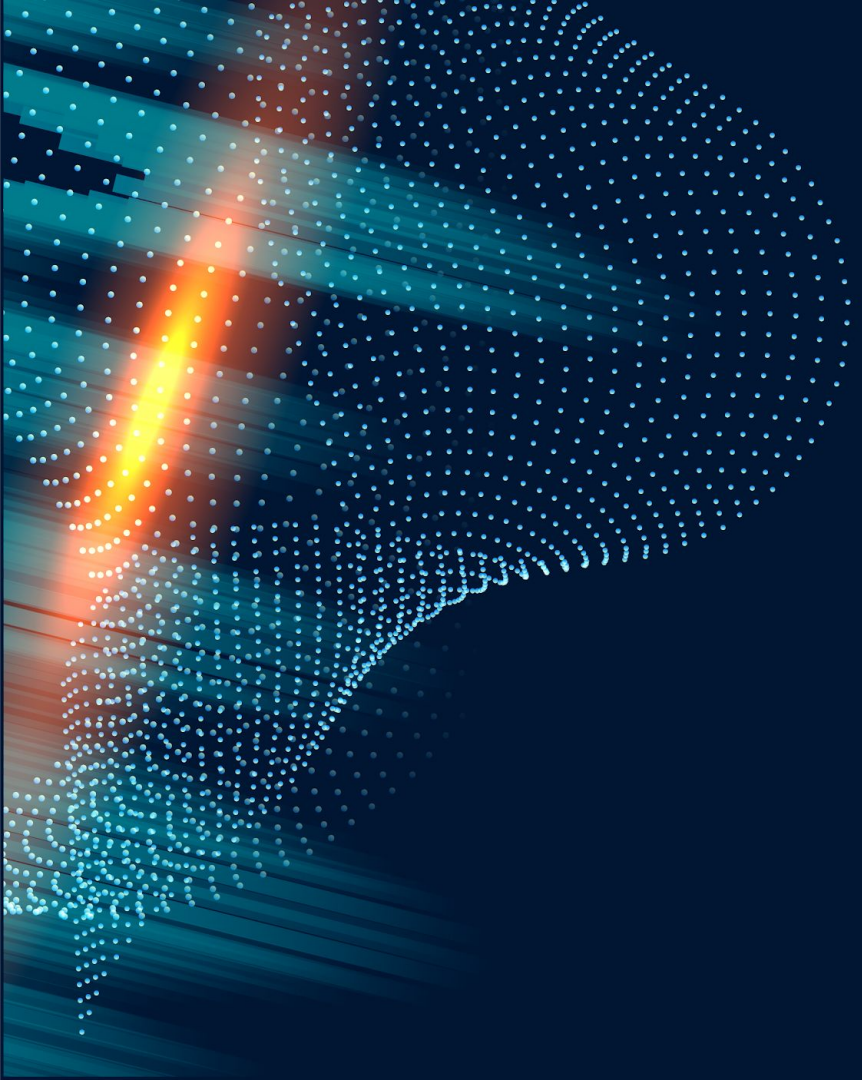
Dates de la période : 11//2024 – 08//2025

Entreprise / Département : Cloud Temple / Cloud Provider

Poste: Alternant – Cloud Security Engineer Junior

Maître / Tuteur d'apprentissage : Paul LEPETIT

Tuteur pédagogique : Kamel MOULAOUI



Cloud Security Mission Overview

- Joined Cloud Temple as a Junior Cloud Security Engineer during a work-study internship
- Integrating security testing (OWASP ZAP) into CI/CD pipelines
- Worked on automating vulnerability detection for cloud applications
- Gained experience in cloud & application security and DevSecOps practices

Plan général

01
INTRODUCTION

- Entreprise & Equipe
- Contexte
- Enjeux & Objectifs

02
ETAT DE L'ART

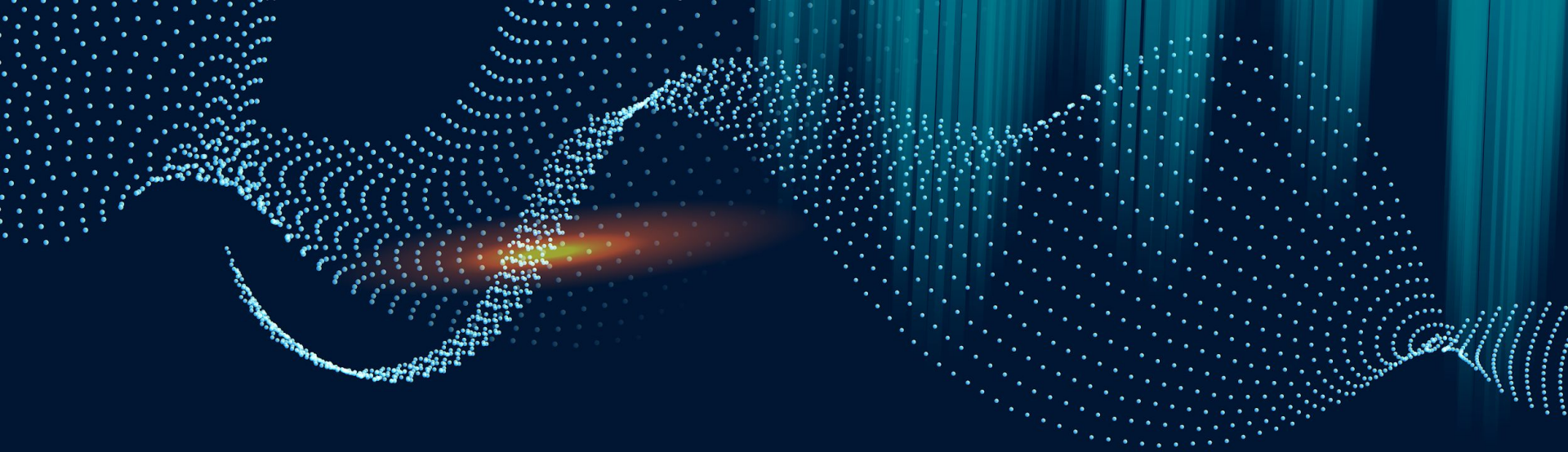
- Sécurité des systèmes d'information
- DevOps
- DevSecOps
- Automatisation

03
MISSION

- Démarche
- Architecture
- Exemple d'éxecution
- Résultats

04
CONCLUSION

- Objectifs atteints ?
- Perspectives & évolutions
- Bibliographie



01 INTRODUCTION

Présentation de l’entreprise

Qui est Cloud Temple ?

- Acteur majeur du cloud de confiance en France
- Certifié SecNumCloud, HDS et ISO 27001
- Plus de 230 collaborateurs

CLOUD TEMPLE
Innovative by design

Équipe

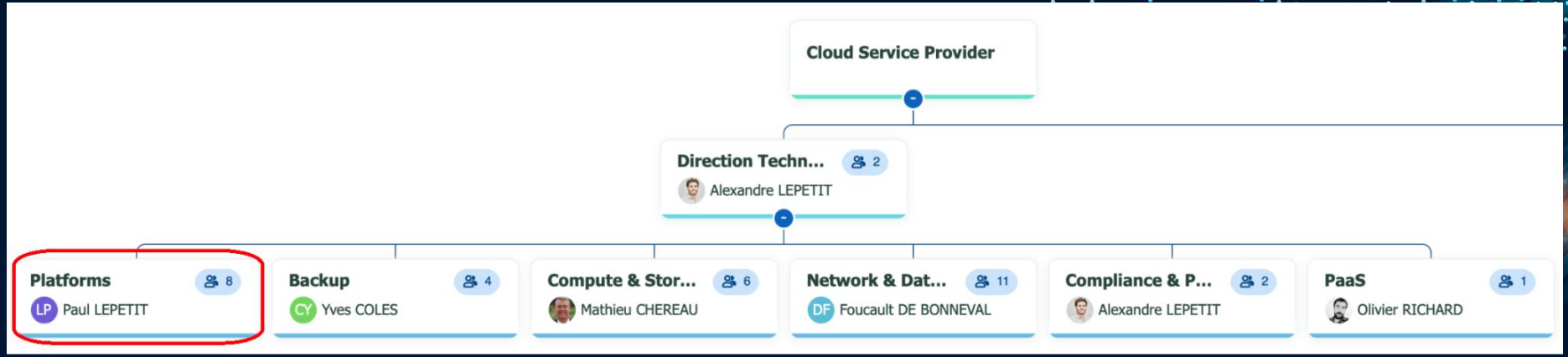


Figure 01 : Organigramme

Platforms

- Mise en place et sécurisation des infrastructures
- Automatisation des déploiements et processus
- Pilotage de projets structurants

Mon rôle

- Intégration d'outils de sécurité dans les pipelines CI/CD
- Contribution à la sécurisation des environnements cloud
- Analyses comparatives pour choix stratégiques

Technologies

Contexte

La sécurité des systèmes d'information est devenue un enjeu majeur face à la multiplication des menaces (phishing, ransomware, DDoS...).

L'essor du cloud et des architectures modernes (microservices, conteneurs) complexifie encore la protection des environnements.

Dans ce contexte, les entreprises doivent concilier rapidité de livraison et sécurité renforcée.

Entre 2020 et 2024

93%

Niveau d’infiltration

140%

Volume d’incident

40%

PME vs cyberattaque

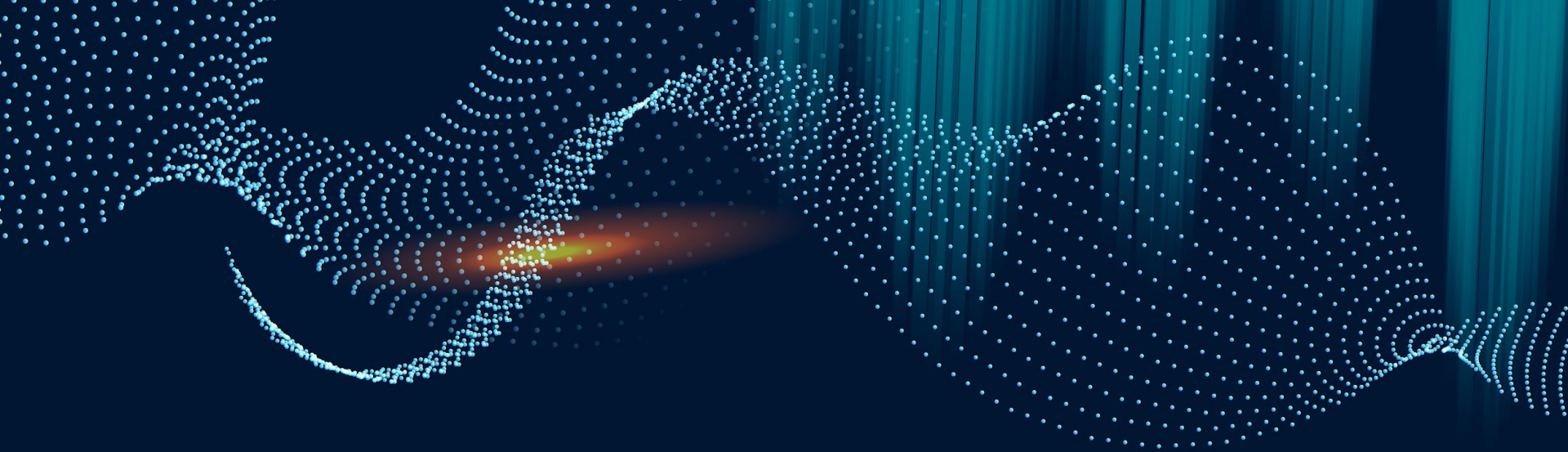
Enjeux & Objectifs

Enjeux

- Comment intégrer la sécurité sans ralentir les cycles DevOps ?
- Quels outils et approches permettent d'automatiser les contrôles de sécurité ?
- Comment garantir un haut niveau de conformité et de protection dans un environnement cloud agile ?

Objectifs de l'étude

- Mettre en œuvre des tests de sécurité automatisés dans un environnement CI/CD
- Concevoir une architecture sécurisée
- L'évaluer dans un contexte réel



02 | Etat de l’art

Sécurité des systèmes d’information

La sécurité des systèmes d'information regroupe l'ensemble des mesures techniques, organisationnelles et humaines visant à protéger les ressources numériques contre les menaces, les vulnérabilités et les risques.

Réglementation et conformité

- RGPD : protection des données personnelles.
- ISO 27001 : management de la sécurité.
- ANSSI / SecNumCloud : cadre français et européen.

Figure 02 : Triade CIA

DevOps – approche orientée vitesse et agilité

DevOps est une approche qui vise à unifier les équipes développement (Dev) et opérations (Ops)

Avantages

- Livraison rapide et continue
- Automatisation des processus (CI/CD)
- Collaboration accrue Dev + Ops
- Amélioration de la qualité logicielle

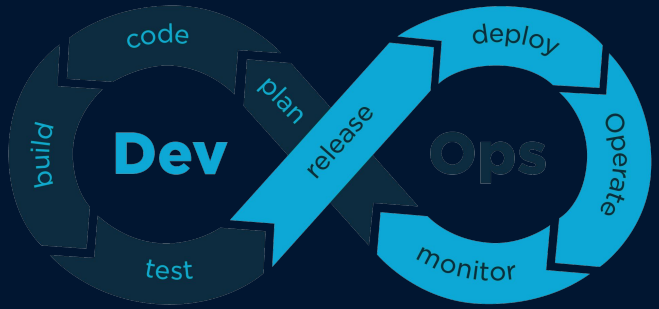


Figure 03 : Chaine DevOps

Limites

- Sécurité souvent intégrée trop tard
- Manque de contrôle face aux menaces modernes

L’approche DevSecOps : vers un DevOps sécurisé

DevSecOps est une évolution de DevOps qui intègre la sécurité dès le début du cycle de développement et de déploiement

Principes clés

- Sécurité intégrée by design
- Automatisation des contrôles de sécurité dans CI/CD
- Détection et correction précoces des vulnérabilités
- Collaboration Dev + Sec + Ops

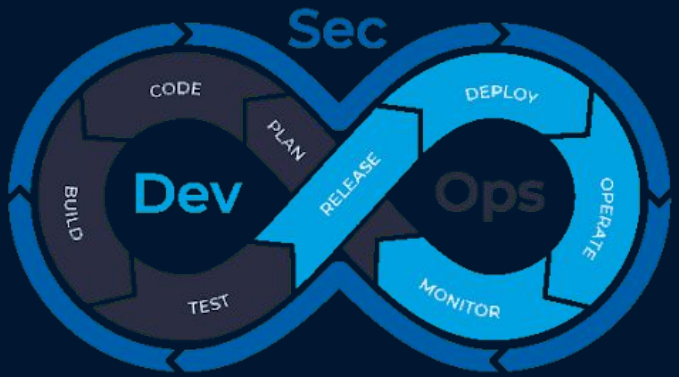


Figure 03 : Chaine DevSecOps

Bénéfices

- Réduction des coûts de correction
- Respect des normes (RGPD, ISO 27001, SecNumCloud…)
- Plus grande résilience face aux menaces
- Maintien de la rapidité des livraisons

Automatisation des tests de sécurité

Dans un environnement DevSecOps, les tests de sécurité peuvent être automatisés pour détecter les vulnérabilités à chaque étape du cycle de développement

SAST

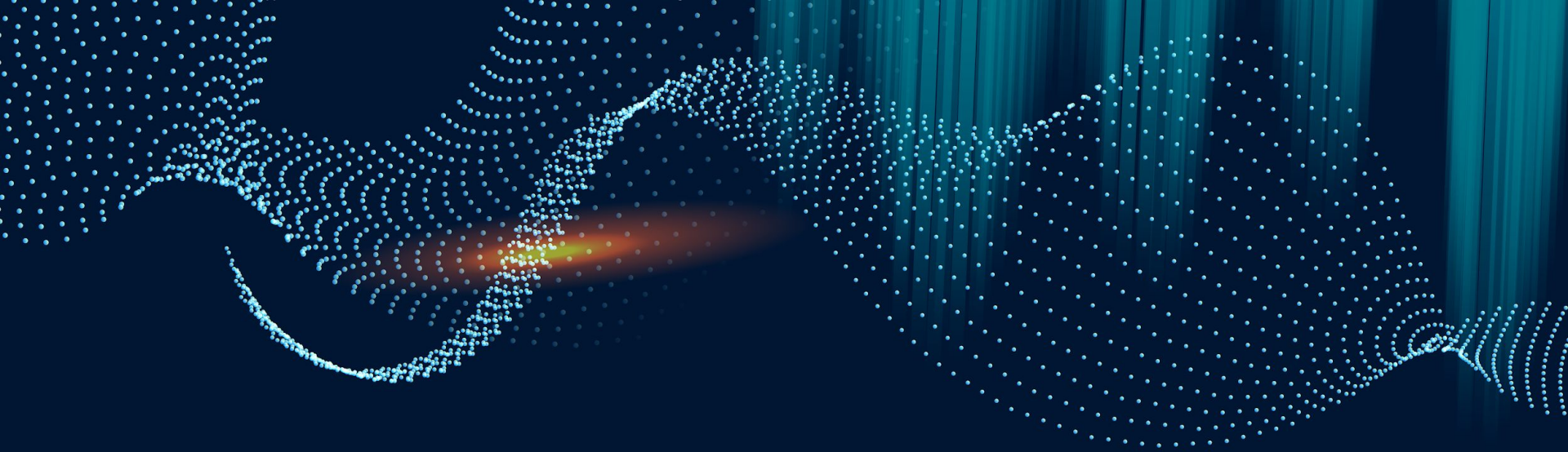
analyse du code source pour détecter les vulnérabilités avant compilation.

SCA

analyse des composants et librairies tierces pour identifier les vulnérabilités connues.

DAST

tests dynamiques sur l'application en fonctionnement pour identifier les failles exploitables.



03 | MISSION

Automatisation d’un scan Dast ...

Le test DAST permet d’identifier les vulnérabilités de sécurité applicative à l’exécution, en simulant des attaques réelles sur l'application en cours de fonctionnement.

- ✅ Détection avancée des vulnérabilités complexes.
- ✅ Documentation officiels robustes
- ⚠️ Version Pro coûteuse, Community limitée en fonctionnalités
- ⚠️ Intégration CI/CD moins flexible que ZAP

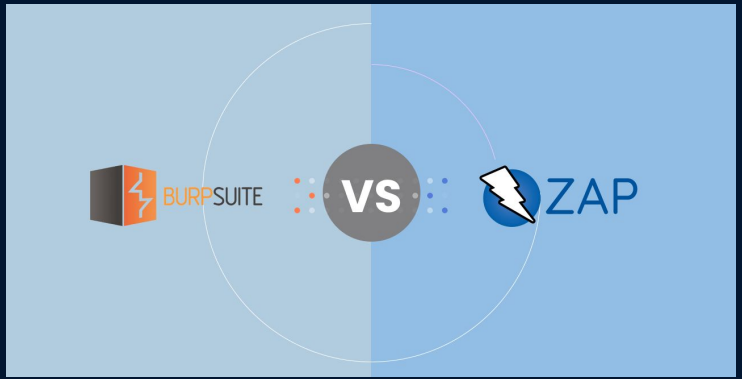


Figure 04 : BurpSuite VS ZAProxy

- ✅ Gratuit et open source
- ✅ Intégrable dans CI/CD via API REST et CLI.
- ⚠️ Moins précis que Burp Suite sur certaines vulnérabilités complexes
- ⚠️ Support officiel moins centralisé

... Avec ZAproxy

Atouts d'OWASP ZAP

- **Open source et gratuit** → adoption facile, pas de coût de licence
- **Intégration DevSecOps** → API REST, CLI, Docker, CI/CD (GitLab, Jenkins, GitHub Actions)
- **Personnalisable** → règles ajustables (zap-config.cfg)
- **Large spectre de détection** → SQLi, XSS, failles d'authentification, mauvaises configurations...
- **Interopérable** → connexion avec SIEM, Splunk, Wazuh
- **Communauté active & mature** → mises à jour régulières, documentation riche

Figure 05 : ZAProxy

Architecture de la solution

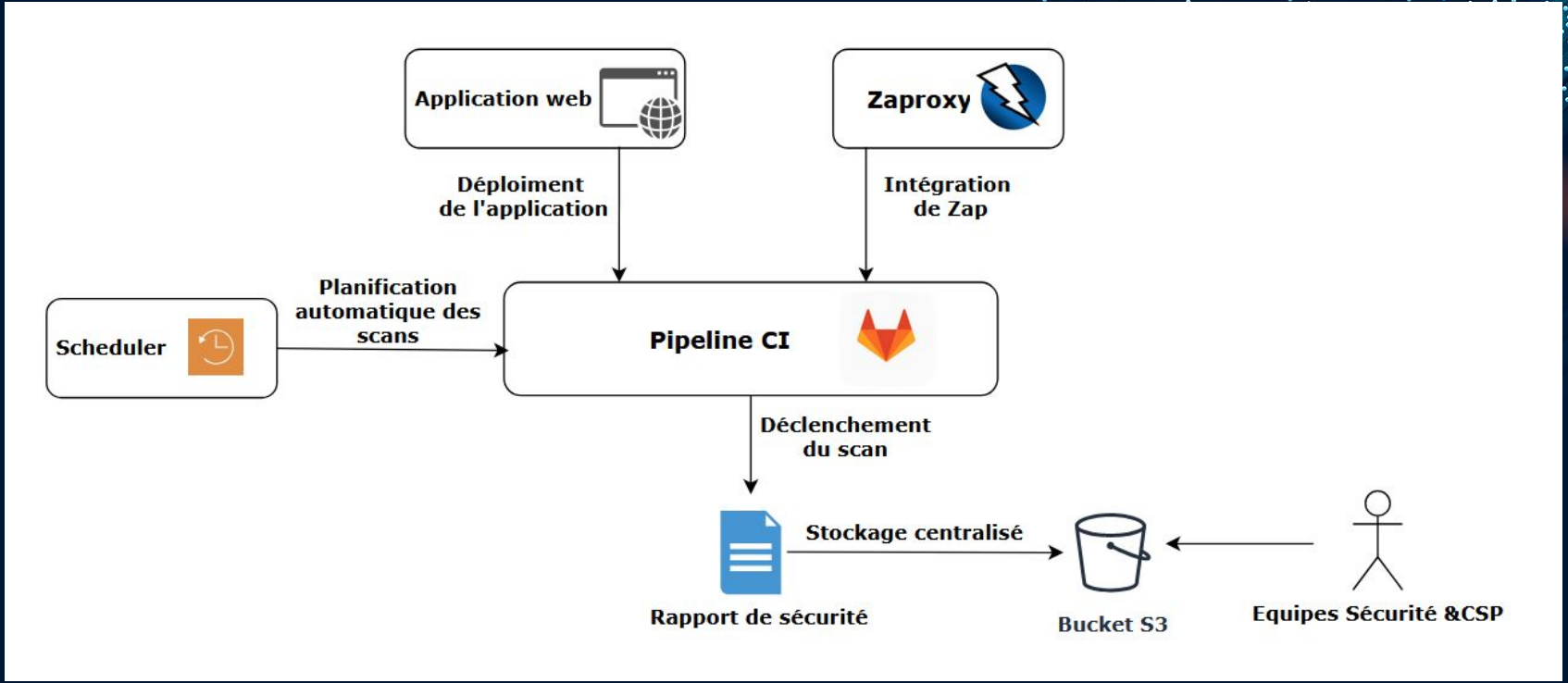


Figure 06: Architecture de la solution

Exemple d'exécution d’un scan ZAP via GitLab CI/CD

- Description
- Cron
- Targets
- Activation

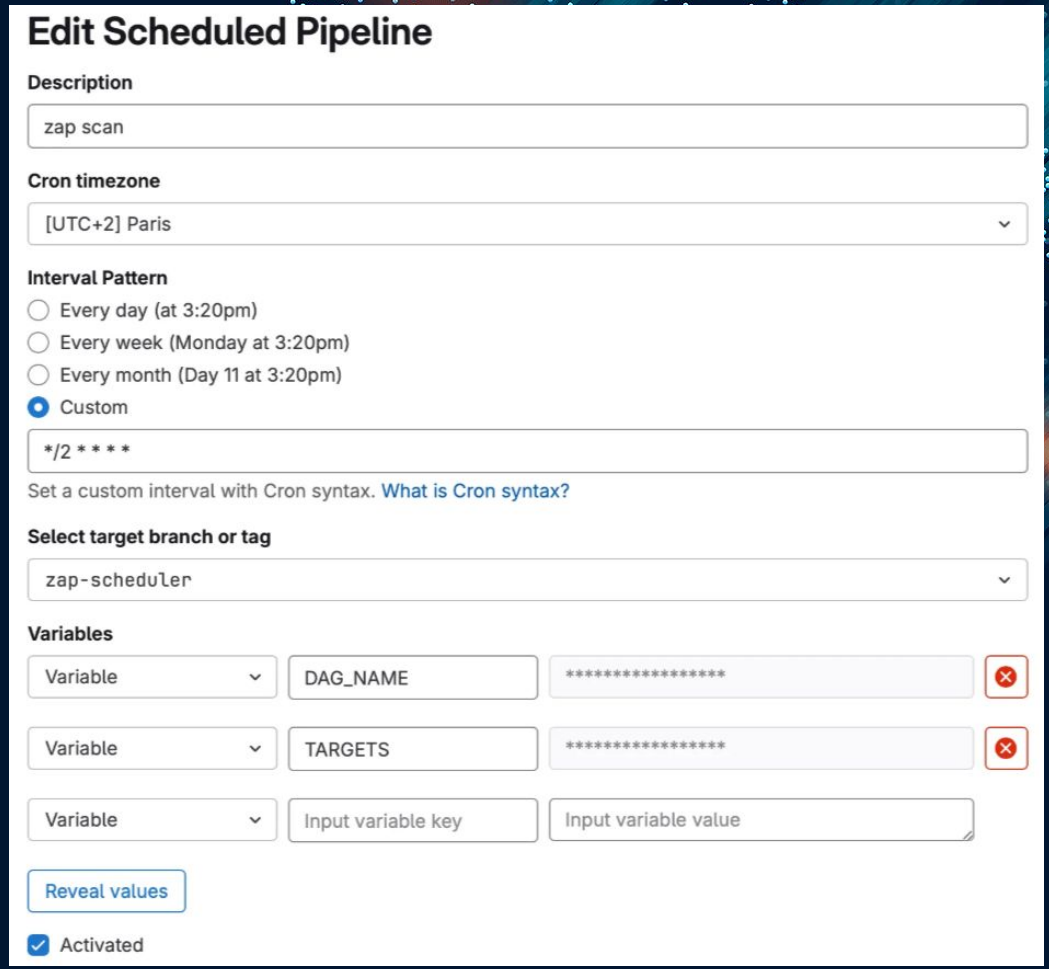


Figure 07: Exemple d’une planification

Suivi du scan

- Lancement manuel et / ou automatique
- Accès aux pipelines pour progression
- Consultation des logs en temps réel

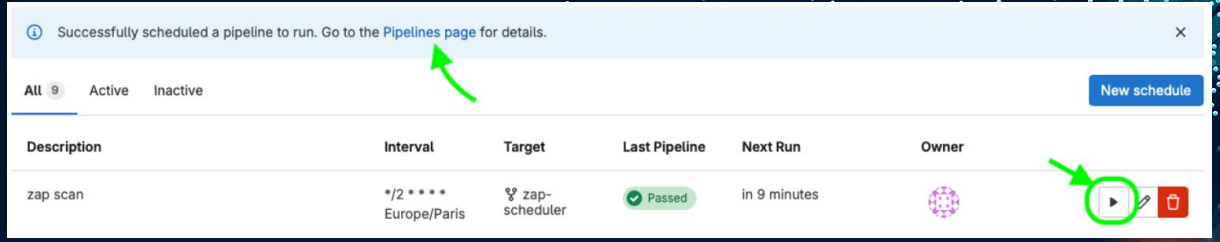


Figure 08: Exécution d'un scan

```
183 [*] Scanning: https://api.shiva.rec.lan/
184 Using the Automation Framework
185 Total of 4 URLs
186 PASS: Vulnerable JS Library (Powered by Retire.js) [10003]
187 PASS: Cookie No HttpOnly Flag [10010]
188 PASS: Cookie Without Secure Flag [10011]
189 PASS: Re-examine Cache-control Directives [10015]
190 PASS: Cross-Domain JavaScript Source File Inclusion [10017]
191 PASS: Content-Type Header Missing [10019]
192 PASS: Anti-clickjacking Header [10020]
193 PASS: X-Content-Type-Options Header Missing [10021]
194 PASS: Information Disclosure - Debug Error Messages [10023]
```

Figure 09: Suivi et logs du scan

Résultats

- Succès du job confirmé dans CI/CD pipeline
- Rapport généré après chaque scan
- Transfert automatique vers MinIO / S3 bucket
- Rapport disponible pour exploitation ultérieure

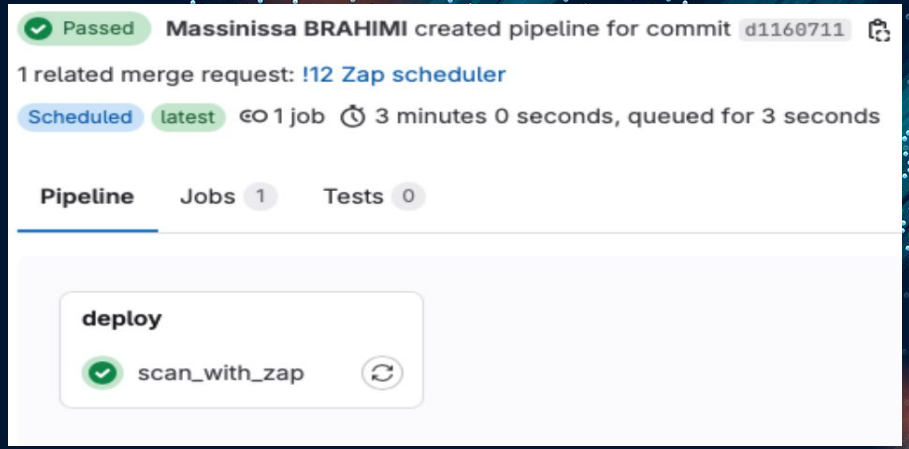
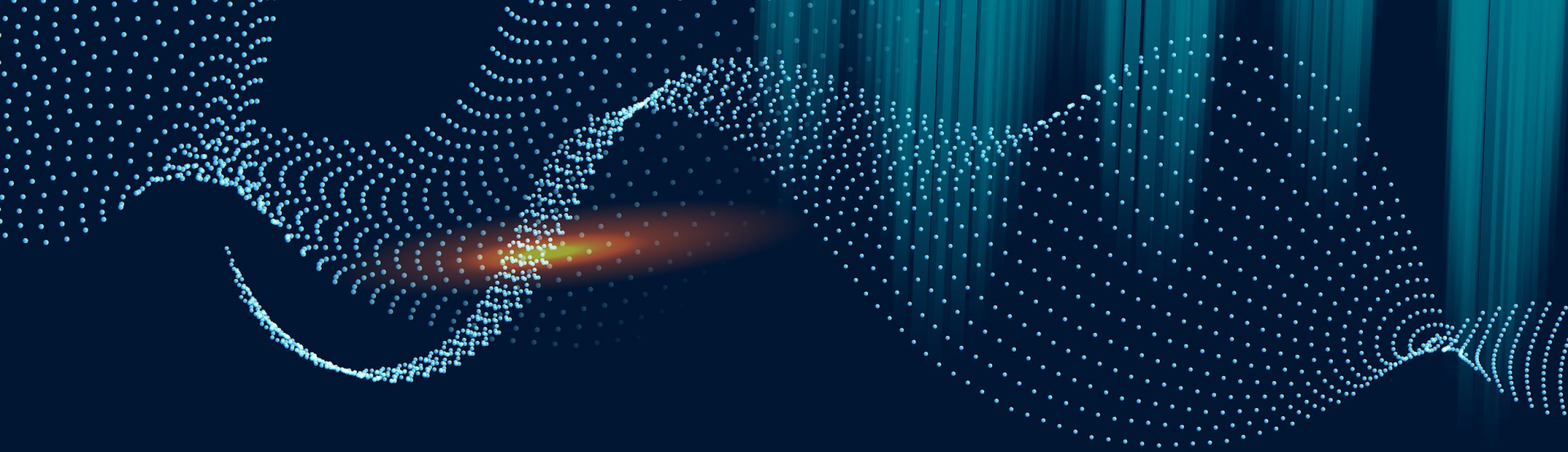


Figure 10: Jobs exécuté avec succès

```
249 [+] Scan completed for https://api.shiva.rec.lan/
250 [*] Transferring the report zap_scan_api_shiva_rec_lan.html for https://api.shiva.rec.lan/
251 `/zap/wrk/zap_scan_api_shiva_rec_lan.html` -> `vidhar/scan-dast/zap_scan_api_shiva_rec_lan.html
    `
252
253 | Total     | Transferred | Duration | Speed       |
254 | 20.67 KiB | 20.67 KiB   | 00m00s   | 431.44 KiB/s |
255
256 $ echo "[+] All scans and reports have been completed"
257 [+] All scans and reports have been completed
258 Cleaning up project directory and file based variables                    00:03
259 Updating CA certificates...
260 WARNING: ca-cert-ca.pem does not contain exactly one certificate or CRL: skipping
261 Job succeeded
```

Figure 11: Logs du job



04 | CONCLUSION

Objectifs atteints ?

- **Mise en place d'une architecture sécurisée** : sélection d'OWASP ZAP comme outil DAST adapté aux besoins du projet, intégration dans un pipeline CI/CD réel.
- **Automatisation des tests** : détection continue et fiable des vulnérabilités, permettant de gagner en efficacité et de réduire les risques opérationnels.
- **Perspectives techniques immédiates** : possibilité d'enrichir le dispositif avec un SIEM ou une gestion plus fine des faux positifs.
- **Enjeux atteints** : sécurisation des environnements, expérimentation dans un contexte réel, maîtrise des processus DevSecOps.
- **Limites :** seul le test DAST a été implémenté, certaines configurations peuvent encore être optimisées pour réduire les faux positifs.

Perspectives & évolutions

Développement personnel : amélioration de la communication, du travail en équipe et de la capacité à présenter et défendre des choix techniques devant un public professionnel.

Acquisition de compétences clés : compréhension globale des environnements cloud sécurisés, DevSecOps et pipelines CI/CD, expérimentation concrète en conditions réelles.

Motivation et apprentissage continu : bases solides en sécurité cloud et applicative, avec une volonté claire d'approfondir pour atteindre un niveau d'expertise.

Vision professionnelle : préparation à un rôle avancé en sécurité offensive (Red Team), avec maîtrise des infrastructures modernes.

La sécurité n’est pas un produit, mais un processus

— Bruce Schneier

Bibliographie

1. Références de l'étude : https://www.ninjaone.com/fr/blog/7-statistiques-sur-la-cybersecurite-que-chaque-pme-et-msp-doit-connaitre/

2. **OWASP ZAP** – https://www.zaproxy.org

3. **Burp Suite** – https://portswigger.net/burp

4. **GitLab CI/CD** – https://docs.gitlab.com/ee/ci/

5. **MinIO** – https://min.io

6. **ISO/IEC 27001:2013** – Norme internationale sur la sécurité de l'information.

7. **SecNumCloud** – https://www.ssi.gouv.fr/guide/secnumncloud

8. **HDS** (Hébergeur de Données de Santé) – https://www.sante.gouv.fr

Merci!

Prêt pour répondre à vos questions !!


END OF PRESENTATION
ANY QUESTIONS?
CLARIFICATIONS?