ADEXTAN
BIFORA DATA CONSULTING
CONFIRM IT
ENGINOV
EXTEAM
FASTOR INGENIERIE
HEXAGONE DIGITALE
IGM
INSTILIA
IZENCIA
MARTE
OMICRONE
PARTENAIRE GC
SAPIENS CONSULTING
SYMOLIA
TIBCO
TILENCIA
YZZY

ADE

Expert AppSec / DevSecOps / Gestion des Vulnérabilités

Expert AppSec / DevSecOps avec plus de 10 ans d'expérience en cybersécurité, ayant piloté la gestion et la remédiation de plus de 1 000 vulnérabilités dans des environnements critiques et réglementés.
Solide expérience de la sécurité applicative, de l'industrialisation des contrôles SAST/SCA et de l'accompagnement des équipes de développement
Il est intervenu dans des contextes bancaires majeurs (Société Générale) et cloud souverain (NumSpot), avec une forte capacité à coordonner les plans d'actions, produire des indicateurs de suivi et accélérer la réduction du risque sécurité.

FORMATIONS & CERTIFICATIONS

2026 : Google Cloud – Cybersecurity, DevSecOps et Security Engineer

2026 : Linux Foundation – Secure Software Development track (LFD121, LFS180, LFS184, LFD125, LFEL1010, SKF100)

Certification : CEH (EC-Council)

Master IT Security – ESGI Paris

Bachelor IS Quality & Security – IUT Blois

BTS Systèmes & Réseaux

COMPETENCES FONCTIONNELLES & TECHNIQUES

Compétences principales :

- **Expert AppSec / DevSecOps**
- **Gestion de plus de 1 000 vulnérabilités**
- **Mise en œuvre et pilotage SAST / DAST / SCA**
- **Accompagnement de plus de 200 développeurs**
- **Expérience Banque (Société Générale)**
- **Expérience Cloud souverain SecNumCloud (NumSpot)**
- **Maîtrise Checkmarx, Fortify, Qualys, Semgrep, Trivy**
- **DevSecOps & AppSec**

Gestion des vulnérabilités

- **SAST / DAST / SCA**
- **Secure SDLC**
- **Remédiation sécurité**
- **Accompagnement des développeurs**
- **Audits de code**

Compétences fonctionnelles : DevSecOps, sécurité cloud-native, pentest Web/API/Mobile, Red Team, gestion des vulnérabilités, détection & réponse, audit SecNumCloud / PASSI / HDS / ISO 27001, accompagnement des équipes de développement.

Cloud & sécurité : Kubernetes, RBAC, NetworkPolicy, Pod Security Standards, admission controllers, Falco, Trivy, Aqua Security, Grype, Renovate, AWS, Azure, GCP, SecNumCloud, Docker, VMware.
SAST / DAST / SCA / Supply Chain : Checkmarx, Fortify, Snyk, Bandit, Semgrep, NodeJsScan, ESLint-security, Gitleaks, Trufflehog, OSV-Scanner, Dependabot, gosec, govulncheck, CycloneDX, SPDX, Cosign, Sigstore, SLSA, Syft.

IaC & CI/CD : Terraform, OpenTofu, Ansible, Puppet, GitHub Actions, GitLab CI/CD, Renovate, Checkov, tfsec, Terrascan, KICS.
Pentest & Red Team : BurpSuite Pro, SQLMap, Metasploit, Nessus, OpenVAS, Nmap, Nikto, WPScan, MobSF, OSINT, intrusion physique, Wi-Fi, caméras IP, contrôle d'accès.
IAM, SIEM & réponse : HashiCorp Vault, AWS Secrets Manager, Azure Key Vault, Keycloak, OAuth2/OIDC/SAML, JWT, Splunk, Wazuh, Elastic/ELK, Sentinel, HarfangLab EDR, Suricata, ModSecurity, Sysdig, Cyberwatch, Qualys, Rapid7, Grafana, Prometheus.
Langages & conformité : Go, Python, Bash, JavaScript/TypeScript, PHP, Perl, SQL, iptables, SELinux, AppArmor, Grsecurity, OSSEC, Auditd, GDPR, NIS2, DORA, OWASP Top 10 / API / LLM, MITRE ATT&CK, STRIDE, PASTA.

Langues : Anglais

EXPERIENCES PROFESSIONNELLES

NUMSPOT, 2024 / 2026
Senior DevSecOps / Lead Pentester

Contexte du projet :
- Intervention au sein d'un cloud souverain SecNumCloud, dans un environnement réglementé, avec un périmètre de 180 services et plus de 150 dépôts applicatifs.

Missions réalisées :
- Mise en œuvre des contrôles ANSSI SecNumCloud, analyses d'écarts et préparation des audits avec les équipes ingénierie, opérations et conformité.
- Consolidation des scanners Semgrep, Gitleaks, Trivy, Cyberwatch, Gemnasium et Renovate dans une chaîne DevSecOps unifiée SAST, SCA, secrets et conteneurs.
- Qualification et suivi de plus de 1000 vulnérabilités, avec remédiation directe des vulnérabilités critiques et coordination des corrections avec les équipes de développement.
- Durcissement des environnements Kubernetes de production avec Falco, Trivy en CI et gestion des mises à jour de dépendances via Renovate.
- Exploitation quotidienne de Splunk, Wazuh, Elastic et HarfangLab EDR : traitement d'incidents de phishing, tuning des règles de corrélation et construction de tableaux de bord SIEM.
- Développement d'une plateforme CTF interne en Go pour l'acculturation sécurité des équipes et benchmark d'outils CSPM / CWPP.

Impact : réduction du risque applicatif, standardisation des contrôles DevSecOps et amélioration de la préparation aux audits réglementaires.

Environnement technique :
SecNumCloud, Kubernetes, Falco, Trivy, Semgrep, Gitleaks, Cyberwatch, Gemnasium, Renovate, Splunk, Wazuh, Elastic, HarfangLab, Sysdig, Qualys, Nessus, Rapid7, Go, GitLab CI/CD, PASSI, HDS, ISO 27001.

Consultant pour divers clients, 2022 / 2024
Pentester / DevSecOps

Contexte du projet :
- Missions de sécurité auprès de clients des secteurs hôtellerie, retail et transport, couvrant des périmètres Red Team, pentest et durcissement cloud.

Missions réalisées :
- Pilotage de plus de 30 missions de Red Team et de pentest : intrusion physique, Wi-Fi, caméras IP, contrôle d'accès et durcissement poste de travail.
- Sécurisation d'environnements multi-cloud AWS, Azure, GCP et VMware par Terraform, Ansible et Puppet.
- Intégration des contrôles IaC Checkov et tfsec dans les chaînes GitLab et GitHub CI.
- Restitution des constats, priorisation des risques et accompagnement des équipes dans la remédiation.

Impact : amélioration de la résilience des environnements clients et accélération du traitement des risques techniques identifiés.

Environnement technique :
AWS, Azure, GCP, VMware, Terraform, Ansible, Puppet, GitLab CI/CD, GitHub Actions, Checkov, tfsec, BurpSuite Pro, Nmap, Metasploit, Nessus, OSINT, Wi-Fi.

SOCIETE GENERALE, 2019 / 2022
DevSecOps / Lead Pentester

Contexte du projet :
- Accompagnement DevSecOps et pilotage de la sécurité applicative dans un contexte bancaire, avec un périmètre de plus de 150 applications et 200 ingénieurs.

Missions réalisées :
- Industrialisation d'une chaîne SAST / DAST intégrant Bandit, Qualys WAS, NodeJsScan, ESLint-security, Trufflehog, Checkmarx et Fortify.
- Pilotage de plus de 150 missions de pentest externes : cadrage, gestion des prestataires, revue des livrables et suivi de remédiation.
- Réalisation de contre-audits internes sur les constats critiques et coordination avec le SOC sur les incidents applicatifs.
- Animation d'un programme d'acculturation sécurité pour plus de 200 ingénieurs : ateliers, guides de durcissement et fiches secure-by-default.
- Encadrement de l'équipe pentest SG India sur des périmètres Web et API.

Impact : renforcement de la sécurité applicative, homogénéisation des pratiques de remédiation et transfert de compétences aux équipes de développement.

Environnement technique :
Bandit, Qualys WAS, NodeJsScan, ESLint-security, Trufflehog, Checkmarx, Fortify, CI/CD, Web, API, SOC, Python, SAST, DAST.

GENERALI, 2018 / 2019
Security Expert / Pentester

Contexte du projet :
- Intervention au sein d'équipes agiles pour intégrer les activités de pentest dans les cycles de développement applicatif.

Missions réalisées :
- Réalisation de plus de 30 missions de pentest Web, mobile et OSINT dans les sprints projet.
- Cadrage des tests, débriefing des résultats avec les développeurs et suivi des corrections.
- Formalisation des constats et priorisation des vulnérabilités selon leur exposition et leur criticité métier.

Impact : intégration plus fluide de la sécurité dans les cycles agiles et réduction des risques avant mise en production.

Environnement technique :
Web, Mobile, OSINT, BurpSuite Pro, OWASP Top 10, tests statiques et dynamiques, méthodes agiles.

NES CONSEIL, 2017 / 2018
Security Expert / Pentester

Contexte du projet :
- Réalisation d'audits techniques sur des plateformes Web, API et mobiles, notamment des CMS hébergés sur AWS et des architectures SOAP / REST / JSON.

Missions réalisées :
- Conduite de plus de 50 pentests Web, API et Mobile sur environnements AWS, CMS, Android et services exposés.
- Recherche et exploitation contrôlée de vulnérabilités XSS, SQLi, XXE, injections XPath / LDAP, désérialisation, NoSQL, CSRF et contournements CORS.
- Analyse statique et dynamique d'applications mobiles avec MobSF et restitution des scénarios d'exploitation.

Impact : fiabilisation des applications auditées et amélioration de la priorisation des correctifs de sécurité.

Environnement technique :
AWS, CMS, SOAP, REST, JSON, Android, MobSF, BurpSuite Pro, SQLMap, Nmap, Nikto, WPScan, OWASP Top 10.

ADE

ORANGE, 2014 / 2016

Unix Security Engineer

Contexte du projet :

- Audit et durcissement de plateformes Linux / Unix selon des référentiels de sécurité et des standards de conformité.

Missions réalisées :

- Réalisation d'audits de sécurité Linux / Unix selon NIST, CIS Benchmark, ANSSI et NSA.
- Durcissement des infrastructures avec iptables, SELinux, Grsecurity, AppArmor, OSSEC et Auditd.
- Réalisation des contrôles et remédiations par scripts Shell, Python, Perl et SQL.
- Analyse des écarts, documentation des actions correctives et accompagnement des équipes d'exploitation.

Impact : renforcement du niveau de durcissement système et standardisation des contrôles de conformité techniques.

Environnement technique :

Linux, Unix, RedHat, Debian, iptables, SELinux, Grsecurity, AppArmor, OSSEC, Auditd, Shell, Python, Perl, SQL, NIST, CIS Benchmark, ANSSI, NSA.