

Ingénieur IMT Mine Alès / INSA Lyon

Cybersécurité / Gestion des vulnérabilités

Expert Hackuity, Qualys VMDR et accompagnement à la remédiation.

RRI est un expert cybersécurité senior, spécialisé en gestion des vulnérabilités, AppSec et sécurité offensive.

Avec plus de 10 ans d'expérience, il allie expertise technique, culture du développement et forte capacité d'exécution de manière autonome.

Son passage chez Hackuity est un véritable atout : il connaît la plateforme de l'intérieur, ses workflows, ses intégrations comme Qualys VMDR, ainsi que les enjeux de remédiation et d'AppSec.

Agile et rapidement opérationnel, il intervient avec crédibilité sur des environnements sensibles, du paramétrage à l'analyse des vulnérabilités jusqu'au suivi des remédiations. Son expertise en pentest lui permet en outre de monter en compétence en deux jours sur des sujets non maîtrisés. Enfin, les contraintes ne posent pas de difficulté.

En bref : un profil senior, légitime, agile et créateur de valeur immédiate.

COMPETENCE CLES

Domaines de compétences techniques :

- *Hackuity : administration fonctionnelle, paramétrage de workflows, onboarding de sources, reporting, base de connaissance, accompagnement des usages*
- *Gestion des vulnérabilités : qualification, scoring CVSS, priorisation, analyse d'exposition, pilotage des remédiations*
- *Application Security : intégration et évaluation d'outils SAST / DAST / SCA, revue de code, support sécurité aux équipes de développement*
- *Outillage sécurité : Qualys, Qualys VMDR, Qualys Policy Compliance, Rapid7, Splunk, Checkmarx, Nessus, Burp Suite, etc.*
- *Conformité & audits : participation aux audits, recommandations de remise en conformité, rédaction de standards et guides*
- *Développement : Python, JavaScript, TypeScript, PHP, Bash, C / C++*
- *Systèmes & réseaux : GNU/Linux, Windows Server, Active Directory, TCP / UDP, HTTP, DNS, DHCP, VLAN, IPv4 / IPv6*
- *Déploiement & exploitation : Git, GitHub, GitLab, CI / CD, Ansible, Docker, LXC, QEMU, Proxmox, Hyper-V*
- *Communication : restitution à des équipes techniques, RSSI, directions et clients internationaux*

Domaines de compétences fonctionnelles :

- Méthodique, rigoureux et autonome, capable de passer de l'analyse technique à la recommandation actionnable
- Coordination transverse avec développeurs, ingénierie, exploitation, clients et métiers
- Pilotage de remédiation, formalisation des actions, suivi des écarts et communication d'avancement
- Rédaction de rapports, synthèses exécutives, guides, standards et contenus de connaissance
- Participation aux audits, à la mise en conformité et à l'amélioration continue
- Anglais professionnel écrit et oral, opérationnel avec équipes et clients internationaux

METHODOLOGIES ET OUTILS

- **Gestion des vulnérabilités**
Hackuity, workflows de suivi, paramétrage, onboarding de sources, priorisation et remédiation
- **Application Security**
Intégration SAST / DAST / SCA, revue de code, support ingénierie et recherche IA appliquée à la sécurité
- **Outillage de sécurité**
Qualys VMDB, Qualys Policy Compliance, Rapid7, Checkmarx, Nessus, Burp Suite, Splunk
- **RUN / MCO sécurité**
MCO, analyse d'incidents, stabilisation de plateformes et pilotage des remédiations
- **Développement**
Python, JavaScript, TypeScript, PHP, Bash, C / C++, Django, FastAPI / Pydantic, React, Vue
- **Systèmes OS**
GNU / Linux, Windows, Windows Server
- **Network & Infrastructures**
Active Directory, protocoles L1-L7, TCP / UDP, HTTP, DNS, DHCP, IPv4, IPv6, 802.1Q (VLAN)
- **Outillage & supervision**
CI / CD, Grafana, Splunk, Ansible, Docker / LXC, QEMU, Proxmox et Hyper-V
- **Conformité & Gouvernance**
ISO 27001, EBIOS, PCI DSS, NIS2, GDPR, DORA, audits, standards et cadre juridique
- **Communication**
Rapports techniques, restitutions RSSI / direction, standards et recommandations

EXPERIENCE PROFESSIONNELLE

Experts cybersécurité (depuis 10/2023)

Contexte : Accompagnement de clients variés sur des sujets de gestion des vulnérabilités, d'AppSec, de sécurité offensive et de conseil technique.

▼ Gestion des vulnérabilités & sécurité offensive

- ✓ Analyse et qualification de vulnérabilités issues d'audits ou d'outils, priorisation des actions et recommandations de remédiation exploitables.
- ✓ Accompagnement des équipes techniques dans la transformation des constats sécurité en plans d'action concrets.
- ✓ Interventions avec forte autonomie dans des contextes clients sensibles ou fortement contraints, avec exigence de rigueur et de traçabilité.

▼ Conseil produit & expertise sécurité

- ✓ Échanges avec des DSI, des RSSI/CISO et des équipes techniques autour de l'outillage sécurité, de la remédiation et de la gouvernance.
- ✓ Conseil technique auprès d'une startup cybersécurité autour d'une plateforme de pentest assistée par IA, avec validation d'architecture et retours d'usage.
- ✓ Contribution à la stratégie produit, à la priorisation de sujets à forte valeur et à l'amélioration de l'efficacité opérationnelle.

Expertise sur la mission : Posture de consultant senior, autonomie, remédiation, coordination transverse, communication claire avec équipes techniques et décideurs.

HACKUITY : Ingénieur R&D et Lead Pentester - Application Security (2019 - 2023 : 4 ans)

Contexte : Éditeur d'une plateforme SaaS / OnPrem, de gestion des vulnérabilités et d'orchestration AppSec ; rôle partagé entre développement produit, paramétrage fonctionnel et pilotage d'activité pentest.

▼ Plateforme de gestion des vulnérabilités / Application Security

- ✓ Contribution à la conception et à l'évolution de fonctionnalités de plateforme liées à la gestion des vulnérabilités, aux workflows de traitement et au reporting.
- ✓ Intégration et évaluation d'une quarantaine d'outils de sécurité, dont Qualys VMDR, Rapid7, Checkmarx et d'autres solutions SAST / DAST / SCA.
- ✓ Participation au paramétrage fonctionnel, à la structuration des usages et à l'accompagnement opérationnel des équipes sur la plateforme.
- ✓ Création et maintenance d'une base de connaissance de vulnérabilités avec classification standardisée et recommandations de remédiation actionnables.
- ✓ Support expert aux équipes d'ingénierie sur les sujets sécurité, revue de composants sensibles et contribution à la fiabilisation du dispositif.
- ✓ Contribution à des sujets de recherche IA appliquée à la sécurité et à l'industrialisation de pratiques AppSec.

▼ Pentest & accompagnement client

- ✓ Pilotage de l'équipe pentest et encadrement de l'activité.
- ✓ Réalisation d'audits web, mobile et infrastructures internes pour des secteurs sensibles : pharmaceutique, finance, assurance et tourisme.
- ✓ Restitution des résultats à des RSSI, équipes techniques et interlocuteurs exécutifs, avec accompagnement des remédiations.
- ✓ Production de livrables techniques et de synthèse : rapports, recommandations, documentation, standards et contenus de connaissance.

Expertise sur la mission : Hackuity, paramétrage, workflows de vulnérabilités, Qualys VMDR, remédiation, reporting, coordination transverse, communication RSSI / direction

SMILE : Ingénieur logiciel puis Lead Developer (2016 - 2018 : 2 ans)

Contexte : Projet de maintenance puis de refonte des sites rsi.fr et secu-independants.fr dans un environnement open source.

▼ Développement & pilotage technique

- ✓ Conception et développement en PHP / TYPO3 sur un projet critique de maintenance et de reconstruction.
- ✓ Prise de rôle de lead developer pendant 8 mois au sein d'une équipe de 5 personnes.
- ✓ Gestion technique du run puis du build lors de la refonte

Expertise sur la mission : Culture développement forte, compréhension des enjeux de build / run et de MCO applicatif, capacité à dialoguer efficacement avec les équipes de réalisation.

ORANGE BUSINESS SERVICES : Ingénieur développement sécurité réseau (2015 - 2016 : 1 an)

Contexte : Conception, développement et pilotage d'une plateforme métier web et mobile à destination d'équipes cybersécurité.

▼ Plateforme sécurité

- ✓ Conception et développement (build) d'une plateforme supportant les activités d'équipes cybersécurité.
- ✓ Interface entre besoins métier, contraintes opérationnelles et réalisation technique.

Expertise sur la mission : Compréhension concrète des besoins des équipes de sécurité opérationnelle, des plateformes outillées et du maintien en conditions opérationnelles.

ENSEIGNEMENT : Intervenant & membre de jury de mémoire / thèse (depuis 2020)

Contexte : Interventions ponctuelles dans plusieurs établissements (IUT Béziers, Ynov, MyDigitalSchool, etc.).

▼ Transmission & pédagogie

- ✓ Animation de cours et interventions autour de la cybersécurité.
- ✓ Participation à des jurys de mémoire / thèse.

Expertise sur la mission : Capacité à structurer un discours, transmettre, vulgariser et accompagner des interlocuteurs de niveaux variés.

DIPLOMES

- 2019 – INSA Lyon Mastère Spécialisé Cybersécurité
 - Spécialisation post-ingénieur couvrant la gouvernance, la conformité (contrôle et audit ISO 27001, EBIOS, gestion de projet) et l'expertise technique.
- 2018 – IMT Mines Alès
 - Diplôme d'ingénieur (MSc)
 - Filière Informatique et Réseaux (INFRES) en apprentissage, avec spécialisation développement logiciel.

FORMATION

- Montée en compétences continue sur la gestion des vulnérabilités, Hackuity, Qualys VMDR, les pratiques AppSec, la recherche de vulnérabilités et les outils de pentest.
- Veille et échanges réguliers avec d'autres professionnels (RSSI/CISO, équipes SOC, métiers de l'audit et du contrôle...) sur les sujets de GRC, de normes et de législation (NIS2, ISO 27001, DORA, RGPD, etc.).
- Product owner sur des sujets de recherche IA appliquée à la cybersécurité chez Hackuity.
- Interventions pédagogiques depuis 2020 en écoles et jurys, contribuant à l'actualisation régulière des connaissances et des pratiques.

LANGUES

- Anglais : courant