

## CONTACT

☎ : 06-27-40-58-65  
✉ : ndrianaras@gmail.com  
🏠 : 78 Dpt des Yvelines

# CHRISTOPHER RASOANAIVO

INGÉNIEUR/ADMINISTRATEUR

#INFRA #SYSTÈME #RÉSEAU #CYBERSÉCURITÉ #RSSI #AUDIT #GRC #SOC

in www.linkedin.com/in/christopher-ar-189490206



## PROFIL

Après avoir validé la partie "technique" (projets et examens)" du Master 2 Responsable en Sécurité des SI / RSSI - Cybersécurité, je suis actuellement à la recherche d'un poste orienté **Ingénieur-Administrateur Infrastructure (Systèmes, Réseaux et Sécurité)**, **Assistant RSSI** ou **Consultant Cybersécurité** ne demandant pas d'habilitation.

A la recherche d'une entreprise audacieuse, flexible, innovante et humaine... :) )

## COMPÉTENCES TECHNIQUES

### Infrastructure Systèmes Réseaux

Client-SRV W10, Server 2016/2019 (AD, Azure AD)  
Client-SRV Linux (Debian/Ubuntu/Kali, CentOS)

• **Réseaux** switch/routeur CISCO,

• **Virtualisation** VMware, Virtualbox, GNS3 (VM)

• **Sécurité réseau** PfSense, iptables, nftables, Kaspersky, Check Point

• **Serveur Web** Apache/MySQL/PHP

• **Pentest réseau et applications Web** Kali, Wireshark, Nmap, Hydra, DVWA, Burp Suite, Metasploit,

• **Analyse/scan vulnérabilité** Kali, Wireshark, Nessus, SIFT, Volatility, Oledump, MFT, Autopsy, FTK imager, Mandiant IOCe, MITRE ATT&CK

• **Cryptographie** ECB/CBC/CTR/GCM/CBC -MAC/HMAC, Argon2, Bcrypt, PBKDF, VeraCrypt, GPG, OpenPGP, OpenSSL, Let's Encrypt, IPsec, PKI, RSA, AES

• **Exigences/tests** OWASP

• **Monitoring/Surveillance** Nagios-EON, Sysmon, Rsyslog, SIEM Splunk/ElasticSearch

• **Normes** ISO 9001/18045/19011/27001/27002/27005

• **Protection des données** RGPD

• **Bonnes pratiques** ANSSI, CNIL, ITIL, Agile, Scrum

## PARCOURS PROFESSIONNELS

OpenClassrooms / Université de Technologie de Troyes - Paris | 07.2021 - NIVEAU MASTER 2 SSI /OPTION RSSI - CYBERSÉCURITÉ (EN COURS)

• Validation de projets sous forme de Portfolio :

§ Contexte de la Cybersécurité et RSSI : Compétences attendues, rôle dans le SI

§ Sécurité des infrastructures SI : Sécurité architectures SI, déploiement/ administration/sécurisation systèmes et réseaux (OS Serveurs Microsoft/Linux (AD/Contrôleurs de Domaine/Web), CISCO, Firewalling (Pare-feu), virtualisation et sauvegarde

§ Sécurité des applications du SI : Sécurité d'architecture applications Web, tests/rapports d'intrusion et préconisations, données sensibles/BDD/authentifications/contrôles d'accès/requêtes/sessions/paramètres de configuration, WAF (Web Application Firewall)

§ Audit de la sécurité SI : Charte d'audit (limites/modalités intervention, responsabilités, contextes, périmètres/objectifs sécurité SI), préparation (démarches ISO 18045-19011, moyens, outils métriques/standards/référentiels/normes, cartographies/topologie processus/droits d'accès/SI/disponibilité et confidentialité données), audit organisationnel (PSSI, gestion, organisation sécurité information/RH/actifs/accès/cryptographie/exploitation/ communication/cycles/fournisseurs/gestion incidents/PCA), audit physique/environnemental, audit technique (systèmes et réseau/architectures/configurations/vulnérabilités/sécurités/ codes sources), tests d'intrusion (externes/internes, boîtes noire/grise/blanche), audit réglementaire (conformité), évaluation risques, plans d'audit, PDCA/SMSI (ISO 9001/18045/19011/27001/27002), RGD, rapports de synthèse, clôture et recommandations)

§ Monitoring/Surveillance de la sécurité SI : Architectures de surveillance sécurité SI, journalisation éléments SI (AD Contrôleur de domaine, Serveurs/Clients, pare-feu, IDS/IPS/EDR, switches/routeurs), analyse/parsing logs (Windows Event Forwarder Server/Sysmon Windows, Rsyslog Linux), déploiement outils SIEM (installation/configuration/centralisation logs, stockage/indexation, création règles de détection/d'alertes, installation/exploitation modules), scénarios corrélation/attaques, automatisation outils remédiation

§ Analyse forensics/incidents de sécurité : Déploiement outils d'analyse, collecte informations/ données, analyse dump mémoire/copies disques durs/fichiers malveillants des machines infectées, identification/traitement vecteurs d'infection/incidents, reporting indicateurs de compromission, rapports d'investigation forensic, MITRE ATT&CK

§ PSSI, gouvernance des risques du SI et PCA : Enjeux/objectifs/documents/implémentation durable PSSI avec plan d'actions/livrables, mise en place PCA/PRA, démarches/outils d'amélioration continue PDCA, déploiement SMSI (ISO 27001-27002-27005), analyse risques SI (méthode EBIOS-RM), inventaire/évaluation/choix/plan de traitement risques, risques résiduels, communication, PACS

§ Veille et solution sur les menaces en Cybersécurité : Mise en place/industrialisation d'un processus de veille /chasse aux vulnérabilités, sensibilisation

>Environnement technique : Windows Server Active Directory Contrôleur de Domaine (2016/2019), Windows Client (7/10), NetBIOS, DNS, DHCP, GPO, WDS, MDT, GPO, RPCSS, EVENTSYSTEM, NTFRS, SYSVOL, NETLOGON, NTDS, DFSR, Linux Debian/Ubuntu/CentOS/Tiny Core/Kali/SIFT), ACL, Setfacl, pare-feu iptables/nftables/PfSense/Kaspersky, CISCO (Vlan/routeurs/dns/dhcp/haute disponibilité), ICMP, ARP, TCP-IP, UDP, TLS/SSL, SSH, OSPF, HRSP, VmWare WorkStation pro 15/16), VirtualBox, GNS3, GNS3 VM, SSH, AES, Bcrypt, PBKDF, VeraCrypt, GPG, OpenPGP, OpenSSL, Let's Encrypt, Apache2, MySQL, PHP, Wireshark, Nmap, Hydra, DVWA, Burp Suite, Metasploit2, CyberChef, JavaScript Beautifier, Nessus, SIFT, Volatility, Oledump, MFT, Autopsy, FTK Imager, PDF Parser, Mandiant IOCe, SandBoxie, Avira, Nagios, Sysmon, Rsyslog, Splunk, Elasticsearch, Bash, Powershell, Python, C++, EBIOS-RM, PDCA, ANSSI, CNIL, CERT, ISO 18045/19011/27001/27002/27005, RGD

**CHEF DE PROJET/ADMINISTRATEUR SYSTÈMES, RÉSEaux ET SÉCURITÉ ESN (pour Vivendi, Kaufman & Broad, Hipay, ICON) - Boulogne-Billancourt |**

**aug 2017- jun 2021**

• **Exécution de missions d'Administrateur systèmes et réseaux (Exploitation/prod) :**

\* Déploiement/administration serveurs Windows (AD)/Linux (Web Apache2/PHP/MySQL)/de fichiers (WDS/FTP)/d'applications métiers/SIEM Splunk), PMAD infrastructures serveurs,

\* MCO-MCS/maintien en conditions opérationnelles/de sécurité serveurs (utilisation ressources, droits d'accès (comptes utilisateurs/administrateurs, domaines, forêts), relations d'approbation, ports/flux réseaux, patch correctifs de maj/de sécurité, fonctionnement des API)

• **Support & administration** Office 365 Administration, Google Workspace Admin

• **Canal sécurisé** VPN SSL, Wifi WPA2

• **Protocoles** DNS, DHCP, GPO, WDS, MDT, SCCM, CSM, RDS, WinRM, LDAP, ICMP, ARP, TCP-IP, UDP, SSH, TLS/SSL, ACL, OSPF, HSRP

• **Base de données** Access, DBaseIII+

• **Scripting** Python, C++, Bash, Powershell

## SOFT SKILLS

• Capacité d'analyse et de synthèse  
• Travail d'équipe et management de projet  
• Démarche d'amélioration continue (PDCA)  
• Permis B

## LANGUE

Anglais conversationnel  
Allemand notions

## CENTRES D'INTÉRÊT

• Objets connectés (IoT, BYOD)  
• Photographie voyages-découvertes  
• Jogging, foot, tennis, guitare  
• Arts martiaux et philosophie Zen

• Déploiement PKI Client-Serveur, VPN SSL Client-Serveur, cryptographie des fichiers  
• Déploiement/maj sécurité/d'applications bureautiques/métiers par stratégie de groupe (GPO)  
• Mise en place PCA/PRA avec serveurs virtualisés (sous VMware)  
• Déploiement/administration équipements réseaux Cisco (Vlan Switchs, routeurs, wifi)  
• Analyse des alertes de sécurité/logs, installation/maj modules/signatures, ouverture flux FW  
• Migration Windows server 2012 --> 2016 et postes utilisateurs Win7 --> 10  
• Traitement demandes du support technique N2-N3 et escalade incidents au Dir Infrastructure  
• Audit SI (revue des droits/accès, services desk), rédaction rapports d'audit (synthèse, plan d'amélioration continue)  
• Co-pilotage/Delivery Management (Réunions/supervision QoS/SLA Qualité de service Client)  
• Intégration/recouvrement/gouvernance équipe IT

> Environnement humain: Utilisateurs classiques, VIP et ultra-VIP

> Environnement technique : Infrastructure Client-Serveur; architecture 3-tiers (Serveurs locaux et distants) Windows AD, Azure AD, SCCM, CSM, Office 365 Administration, Google Workspace Admin, Linux Debian/Ubuntu/CentOS, serveurs Web Apache PHP MySQL/applicatifs/métiers, VMware Workstation, postes de travail W10/Linux Ubuntu/Mac OS, Citrix, VLAN Switching Routage Cisco, VoIP/ToIP, PKI, VPN SSL Serveur-Client, Bcrypt, ServiceNow, Kaspersky, Check Point, PfSense, EDR, Splunk, Linux Bash, PowerShell, Agile, Scrum), PDCA, ISO 9001/18045/19011/27002/27005, RGPD

## IT ADMINISTRATEUR

### Dentsu-Aegis Media Network France - La Défense | jan-aug 2017

• Déploiement/Administration/gestion AD Windows Server/SCCM/MacOS (master/création/compte profil utilisateurs : office 365, messageries, habilitation/droits d'accès aux ressources)  
• Configuration équipements réseaux (Switch VLAN Cisco)  
• Analyse logs/alertes sur équipements de sécurité (pare-feu Kaspersky/Check Point)  
• Supervision/monitoring infrastructure  
• Assistance informatique/traitement incidents de proximité/à distance, escalade incidents au N3 (Admin en Irlande, Inde)  
• Préparation/installation/maintenance postes utilisateurs, périphériques, téléphonies (VoIP ToIP)  
• Gestion parc et inventaire actifs sur site

> Environnement humain et technique : Utilisateurs classique, VIP et ultra-VIP, Windows AD, SCCM, CSM, Mac OS, Exchange Server, Outlook, serveurs Linux Debian fichiers/applicatifs/métiers, Google Workspace Admin, VLAN Switch Cisco, Zendesk, Skype Business, Altiris, PABX, Jabra, Plantronics, VPN Client, Kaspersky/Check Point, GLPI, FusiInventory, Nagios, ISO 9001

## CONTRÔLEUR QUALITÉ DISTRIBUTION

### Mediapost S.A. (Groupe La Poste) - La Courneuve | jul 2012-jan 2017

• Contrôle distribution, vérification conformité, sécurité et qualité (process, tournées), amélioration continue (env. : PDCA, ISO 9001/19011, Suite Office...)

## ASSISTANT D'ENSEIGNEMENT

### Université de Versailles (UVSQ) - Ville de Versailles CCAS | sep 2009-jul 2012

• Préparation cours, encadrement travaux dirigés L3-M1 (statistiques, microéconomie, innov.)

## CONSULTANT EN ORGANISATION & QUALITÉ

### B.E.S.D.I (Banque Européenne de Sauvegarde de Données Informatique) - Paris | jan 2008-aug 2009

• Audit qualité/conseil opérationnel Direction Marketing (env. : PDCA, ISO 9001/19011, Suite Office...)

## FORMATIONS & DIPLOMES

### UTT TROYES / OPENCLASSROOMS - PARIS | 2021 - 2022

Master 2 Sécurité des Systèmes d'Information / RSSI - Cybersécurité (en cours)

### UDEMY - PARIS | 2022

Certification Cybersecurity EBIOS-Risk Manager (EBIOS-RM)

### OPENCLASSROOMS | 2022

Certifications Administration systèmes Linux, Tests d'intrusion, PSSI et Audit de la sécurité, Analyse Forensic, PSSI et gouvernance des risques du SI, Monitoring/Surveillance de la sécurité SI SIEM, Méthodologie DevOps,

### OPENCLASSROOMS | 2021

Certifications Programmation Python, Sécurité des Infrastructures du SI, Sécurité des Applications du SI,

### UTT TROYES - TROYES | 2021

Master 1 Sécurité des SI via Validation des Acquis Professionnels (VAP)  
Accès au Master 2 SSI - Cybersécurité

### INSTITUT SUPÉRIEUR TECHNIQUE PRIVÉ IFOP - PARIS | 2017

BTS Informatique - Solutions d'Infrastructure, Systèmes et Réseaux SISR

### ISM-HEC - PARIS-SACLAY | 2007

Master 2 Management : Evolutions Technologiques, Organisationnelles et Stratégiques

### GEORGETOWN UNIVERSITY - WASHINGTON DC | 2006

Certificate in Management and International Experience Program

