

Rachid SADIK

Ingénieur Cybersécurité, Systèmes & Poste de Travail

Mastère Cybersécurité RNCP 7 · 2 ans env. bancaire critique · SCCM · Tanium · SOC · Vulnérabilités · PowerShell

Île-de-France

+33 7 68 88 74 51

Rachid.Sadik.Pro@outlook.com

[LinkedIn](#)

Ingénieur cybersécurité et systèmes diplômé **Mastère Cybersécurité RNCP 7**, fort de 2 ans d'expérience en environnement bancaire critique (Ayvens - Société Générale, 2 000+ endpoints). Initiateur de la collaboration production/SSI sur la gestion des vulnérabilités (0% Very High atteint), chef de projet du renouvellement de 50 postes suite à faille RCE critique, et expert du cycle complet poste de travail Windows (SCCM, MDT, PXE, GPO, PowerShell). Compétences SOC consolidées via des projets personnels sérieux (Wazuh, TheHive, Suricata, MISP, forensique). Disponible immédiatement - ouvert aux postes Ingénieur Cybersécurité, Poste de Travail, SOC ou Gestion des Vulnérabilités.

Expériences Professionnelles

Ingénieur Systèmes, Poste de Travail & Sécurité

Sept. 2023 - Sept. 2025

Ayvens - Filiale Société Générale

Nanterre | Environnement bancaire critique | 2 000+ endpoints | SCCM, MDT, Tanium, Active Directory, PowerShell, O365

- ▶ **Initiative & gestion des vulnérabilités (Tanium / SCCM):** à l'origine de la collaboration avec l'équipe SSI - framework NIST adapté au contexte bancaire SG, qualification CVE avec scores CVSS/EPSS, priorisation par impact métier, remédiation multi-méthodes (collections SCCM, PowerShell silencieux, registre à distance) - objectifs atteints : 0% Very High, <10% High
- ▶ **Projet renouvellement de parc - faille RCE critique (chef de projet & admin):** pilotage de bout en bout du remplacement de 50 postes sur 6 sites - master Windows 11 durci (TPM 2.0, Secure Boot, BitLocker, EDR, GPO), déploiement MDT/PXE avec injection pilotes %Model%, sauvegarde/restauration OneDrive, checklist post-migration, PV utilisateurs signés - 100% du périmètre traité dans les délais
- ▶ **Ingénierie poste de travail (SCCM / MDT):** masters Windows 10/11 Entreprise, Task Sequences multi-fabricants (Dell, HP, Lenovo), injection pilotes dynamique %Model%, déploiement applicatif Required/Available par vagues - 2 000 postes migrés PDFSam (remédiation CVE critiques)
- ▶ **Remédiation PowerShell avancée:** connexion distante silencieuse, extraction GUID MSI via registre (HKLM Uninstall), msixexec /qn /norestart, reconfiguration agents Tanium mal configurés (ServerName/LastGoodServer HKLM WOW6432Node), scripts automatisés et documentés
- ▶ **Analyse des événements & surveillance:** Event Viewer, Sysmon (EventID 4688/4624/4625/7045), détection de comportements suspects, surveillance IAM Active Directory (écarts de droits, abus de privilèges), remontée structurée aux équipes SSI
- ▶ **Administration O365 & IAM:** Exchange Online, Teams, SharePoint, Entra ID, Active Directory - licences, droits, MFA, Conditional Access, cycle de vie des identités en environnement bancaire réglementé
- ▶ **Recensement Java - conformité & vulnérabilités:** inventaire Tanium Interact + SCCM, croisement usages métier, désinstallation sur 38% du parc - réduction surface d'attaque CVE et conformité licences Oracle
- ▶ **Reporting & pilotage sécurité:** KPI (taux de remédiation, conformité, exposition), tableaux de bord hebdomadaires, comités SSI et management - matrice RACI sur projets transverses multi-sites
- ▶ **Veille CVE/CERT:** suivi NVD, CISA KEV, MITRE ATT&CK - intégration continue pour réduire la surface d'attaque

Technicien Support Informatique N2

Sept. 2022 - Sept. 2023

Imerys

Paris | Siège EMEA | Environnement international (Europe, Moyen-Orient, Afrique)

- ▶ **Support N2 (ServiceNow):** diagnostic et résolution des incidents, SLA, support remote et on-site en environnement EMEA
- ▶ **Administration systèmes:** supervision serveurs virtualisés Windows/Linux, monitoring, performances
- ▶ **IAM (Active Directory):** comptes, groupes de sécurité, droits d'accès, cycle de vie des identités
- ▶ **Réseau Cisco:** switches, VLAN, TCP/IP, dépannage connectivité multi-sites
- ▶ **Documentation:** procédures techniques et sensibilisation cybersécurité utilisateurs

Projets Techniques

SOC Cloud Hybride	Déploiement SOC complet : SIEM Wazuh (10+ sources, règles de corrélation), SOAR TheHive (playbooks de réponse), IDS Suricata, CTI MISP enrichi Cortex/VirusTotal/AbuseIPDB - Docker, Bash, Python
Renouvellement parc Win11	56 postes / 11 sites suite à faille RCE - master MDT/PXE sécurisé (TPM 2.0, Secure Boot, BitLocker, EDR, GPO), injection pilotes %Model%, 100% du périmètre traité dans les délais
Analyse Forensique	Investigation système compromis : analyse RAM (Volatility - processus, artefacts), disque (Autopsy, FTK Imager), persistance (clés Run, services, tâches planifiées), reconstruction kill chain MITRE ATT&CK
Architecture AWS 3-Tiers	Infrastructure sécurisée AWS : Security Groups, vulnerability scanning, audit conformité IAM - rapport de conformité cloud

Compétences Techniques

Déploiement / MDT / SCCM	Collections WQL, Task Sequences, images master Windows, PXE, injection pilotes %Model%, déploiement applicatif par vagues, Monitoring > Deployments
Vulnérabilités / Sécurité	Tanium (Comply, Interact, Asset, Patch), CVE/CVSS/EPSS, CISA KEV, remédiation, hardening GPO, BitLocker, TPM 2.0, EDR/XDR, NIST SP 800-40
Systèmes Windows	Windows 10/11, Windows Server, registre, Event Viewer, Sysmon, GPO, troubleshooting avancé
SOC / SIEM / CTI	Wazuh, Splunk, ELK, TheHive (SOAR), MISP (CTI), Suricata, Cortex - détection, corrélation, incidents, playbooks
Scripting	PowerShell (remédiation, administration, registre à distance), Python, Bash - automatisation et industrialisation
Microsoft 365 / IAM	Entra ID, Exchange Online, Teams, SharePoint, Active Directory, OKTA, MFA, Conditional Access
Virtualisation / Cloud	VMware ESXi, Hyper-V, Proxmox, AWS, Azure - administration et sécurité
Réseau	TCP/IP, OSI, Cisco (VLAN, switches), Wireshark, Palo Alto IDS/IPS, PFSense
Forensique	Volatility, Autopsy, FTK Imager - analyse RAM/disque, persistance, timeline
Référentiels	MITRE ATT&CK, ISO 27001, NIST, NIS 2, RGPD, OWASP

Formation

Mastère Cybersécurité - RNCP Niveau 7 <i>Expert en systèmes d'information, spécialisation Cybersécurité</i> Sup de Vinci - La Défense	2023 - 2025
Bachelor AIS - RNCP Niveau 6 <i>Administrateur d'Infrastructures Sécurisées</i> Webitech - Paris	2022 - 2023
BTS Systèmes Numériques Lycée Jules Ferry - Versailles	2020 - 2022

Certifications & Divers

CTF Tanium 2024 CompTIA Security+ - En cours de préparation Pratique régulière TryHackMe / HackTheBox	Langues : Français (natif) Anglais (B2) Hindi (natif) Veille : CVE/CERT, MITRE ATT&CK, actualité cyber & IA - Reddit netsec, HackTheBox writeups
---	--