

Said SAADI

Security Officer · Sécurité opérationnelle & gestion des vulnérabilités

Montreuil (93) | +33 7 69 75 98 10 | said9313362@gmail.com | linkedin.com/in/said-saadi-CYB | https://saiDSAADI.pages.dev/
CDI · disponible en août 2027 · Mobilité : Paris / Île-de-France

PROFIL

Plus de 3 ans d'expérience IT, dont plus d'un an en cybersécurité chez Capgemini : maintien en condition de sécurité (MCS) d'un parc mondial d'environ 5 400 serveurs et 2 100 bases de données pour un grand groupe du luxe. Spécialisé en gestion des vulnérabilités par le risque (Qualys VMDR, CrowdStrike Spotlight, mémoire sur le CTEM) et en sécurité des identités techniques (PAM, clés SSH, comptes de service). Projet phare : revue d'environ 7 400 clés SSH menée jusqu'à la remédiation en production. Maîtrise de l'IA générative : usage quotidien en entreprise et conception d'agents de sécurité autonomes. Anglais professionnel C1. Recherche un CDI de Security Officer ou d'ingénieur sécurité opérationnelle à partir d'août 2027.

COMPÉTENCES

Sécurité opérationnelle : gestion des vulnérabilités par le risque, patch management Windows et Linux, durcissement CIS, obsolescence, conformité EDR, cycle de vie des certificats
Identités et accès : revues d'accès, JML, comptes à privilèges et de service, clés SSH, sudoers, Service Principals, Entra ID, AD
Outils sécurité : Qualys VMDR, CrowdStrike Falcon (EDR, Spotlight), Pentera, Delinea (PAM)
Automatisation et pilotage : Python, PowerShell, AWX/Ansible, ServiceNow (incidents, changements, CMDB), Power BI, VBA
IA appliquée : IA générative, prompt engineering, agents autonomes (Claude Agent SDK), RAG, sécurité des outils IA (MCP, MLflow)
Systèmes : Windows Server, Linux, AIX, VMware ESXi, Nutanix, Azure, Cisco
Référentiels : ISO/IEC 27001:2022, SOC 1 Type II, K-ISMS, plan d'assurance sécurité · notions de NIS2, DORA et PCI DSS
Langues : français (langue maternelle) · anglais C1, usage professionnel quotidien · arabe B2 · allemand A2

EXPÉRIENCE PROFESSIONNELLE

Account Security Officer (alternance) — Capgemini sept. 2025 – août 2027

Client confidentiel : grand groupe international du luxe, infogérance mondiale · sécurité opérationnelle (MCS)
Rattaché au responsable sécurité du compte ; préparation du comité sécurité mensuel et des KPI ; coordination en anglais avec l'Inde.

- Vulnérabilités et correctifs** : 121 vulnérabilités critiques priorisées par le risque et plans de remédiation suivis avec l'exploitation ; pilotage des campagnes de scan Qualys VMDR, de la conformité des correctifs et des dérogations.
- Identités techniques** : projet clés SSH mené de bout en bout, de la revue d'environ 7 400 clés sur 920 serveurs Unix jusqu'à la remédiation en production via la gestion des changements ; secrets des Service Principals Azure et comptes de service.
- Contrôles MCS mensuels** : maintien du niveau de sécurité d'environ 5 400 serveurs et 2 100 bases (correctifs, durcissement, comptes et mots de passe à privilèges, EDR) ; suivi automatisé en VBA, plus rapide et plus fiable.
- EDR et certificats** : reporting hebdomadaire de conformité CrowdStrike Falcon pour résorber les écarts (agents obsolètes, actifs non équipés, cas éditeur) ; cycle de vie des certificats, des expirations anticipées aux renouvellements.
- Obsolescence** : suivi de la fin de vie d'ESXi 7 jusqu'à la migration vers ESXi 8 ; inventaire Java pour cibler les versions obsolètes.
- Droits d'accès** : revues d'accès mensuelles ; cadrage de la recertification des accès à une vingtaine d'outils de sécurité.
- Sécurité des changements** : revue sécurité d'une automatisation AWX/Ansible avant sa mise en production ; audit de sécurité des serveurs d'administration et bastions ; remédiation des constats Pentera.
- Conformité et audits** : audit du plan d'assurance sécurité (128 constats) ; mise en place d'un portail de 35 procédures d'exploitation sécurité ; contribution aux audits ISO 27001, SOC 1 Type II et K-ISMS.

Technicien support IT N2/N3 et réseau (CDD) — Nestlé France sept. 2023 – août 2025

Siège d'Issy-les-Moulineaux · plus de 3 000 utilisateurs

- Support N2/N3** : résolution des incidents et des escalades poste de travail et réseau, supervision du LAN Cisco.
- Migration Windows 11** : parc migré avec Autopilot et Intune.
- Active Directory et automatisation** : arrivées et départs, automatisation des tâches récurrentes en PowerShell et Python.

FORMATION

Master Cybersécurité, Réseaux & Cloud — EFREI Paris · bac+5, en alternance 2025 – 2027
GRC, audit, IAM, gestion des incidents · mémoire : gestion des vulnérabilités par le risque (CTEM)

Licence Informatique — Université Paris-Est Créteil (UPEC) 2020 – 2023

CERTIFICATIONS

Obtenues : CompTIA Security+ (SY0-701) – 2026 · Cisco CCNA – 2024 · Microsoft Azure Administrator (AZ-104)
En cours : ISO/IEC 27001 Lead Implementer (PECB) – examen prévu en 2027

PROJETS ET ENGAGEMENTS

Agents IA de sécurité : agent de recherche de vulnérabilités sur Claude Agent SDK, isolé en bac à sable et adossé à une base RAG de 641 attaques réelles ; agents de pentest autonomes sur Hack The Box (40 machines compromises)
Lab Active Directory : audit BloodHound et PingCastle d'une forêt à deux domaines, score de risque ramené de 57 à 30 après durcissement ; Windows Server 2022 durci selon le CIS (12 points sur 13 prouvés)
Lab AppSec : tests OWASP Top 10 (A01 contrôle d'accès, A09 journalisation), avec détection Loki/Grafana et blocage fail2ban
IHEDN : session « défense et sécurité nationale » au Campus Cyber (avril 2026)