

Vishal DESAI

Ingénieur Cybersécurité

vishal_desai@hotmail.fr | +33 7 82 28 27 36 | Paris, France

Nationalité Française

Linkedin : vishal-desai-cybersecurity | GitHub : VD17 | vishal-desai.fr



EXPÉRIENCE PROFESSIONNELLE

Consultant Cybersécurité

SAYCURIT, Paris 13

Sep 2022 - Aujourd'hui

- **Palo Alto (NGFW, Panorama, GlobalProtect)** : Gestion des Firewalls, création de règles, migrations & implémentations, audits mensuels.
- **CATO Networks (SASE/SD-WAN)** : Implémentation de sockets CATO, déploiement d'infrastructure réseau sécurisée.
- **Référent & responsable Rapid7 (InsightVM, AppSec, IDR)** : Intégration, formation client, analyse de vulnérabilités, suivi de remédiation, monitoring SOC .
- **SentinelOne** : Déploiement EDR, analyse d'alertes et réponse à incidents.
- **Okta (IAM)** : Mise en place SSO, MFA, provisioning SCIM, automatisation via Workflows, posture Zero Trust.
- **Digital Guardian (DLP)** : Création de politiques, analyse incidents de fuite de données.
- **Netwrix Privilege Secure** Conception de politiques Privilege Manager incluant analyse des cas d'usage, modèles de délégation et élévations semi-automatisées
- **Netwrix Auditor** : Audit de sécurité avancé sur Active Directory, analyse des logs d'accès et détections d'anomalies suite à des incidents de sécurité (post-mortem investigations).
- **Mimecast** : gestion des quarantaines et sensibilisation utilisateurs, run et remédiations d'incidents.

Formateur Freelance

VD Formations – Paris & Région PACA

Sep 2021 - Aujourd'hui

- **Formation de BTS, TAI & premières années** : Linux (Bash, hardening, iptables), Windows Server (AD, GPO), réseaux (TCP/IP, VLAN, VPN).
- **Modules en cybersécurité** : Pentest, SIEM, XDR, IAM, SOC opérationnel.

FORMATION

ESGI, Paris

2023 – 2025

Master Informatique, Cybersécurité

PROJETS PERSONNELS

Panther ASOC (SOC Automatisé)

Stack Wazuh, Suricata, TheHive, pfsense orchestrée par Ansible (Déploiement à la réponse aux incidents).

Harmony

Load balancer HTTP modulaire avec répartition du trafic, vérification d'état, limitation de débit et journalisation. Inspiré du projet CS110L de Stanford

Infrastructure Proxmox

HomeLab complet avec virtualisation, HA, IoT, VPN site-to-site.

COMPÉTENCES, LANGUES & CENTRES D'INTÉRÊT

Compétences techniques : SIEM, EDR/XDR, IAM, SSO/MFA (SAML, OIDC, SCIM), DLP, NGFW, VPN IPSec/SSL, SASE, SD-WAN, ADDS, Zero Trust, RBAC, Python, PowerShell, Bash, Ansible, Cloud (IaaS, SaaS, Azure), SOC, Incident Response.

Certifications : MOOC ANSSI, SentinelOne IR Engineer – SIREN, Palo Alto System Engineer (PSE), CATO Certified Associate, Netwrix Privilege Secure – Professional Service Engineer, Cisco CCNA, EBIOS Club MOOC.

Langues : Anglais (C1 - 890), Hindi (C1), Français (Natale), Espagnol (A1)

Centres d'intérêt : Lecture, Golf, Musculation, Sport automobile