

Vishal DESAI

Cybersecurity Engineer

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

French Nationality

LinkedIn: vishaldesai-cybersecurity | GitHub: VD17 | vishal-desai.fr



PROFESSIONAL EXPERIENCE

Cybersecurity Consultant

SAYCURIT, Paris 13

Sep 2022 - Present

- **Palo Alto (NGFW, Panorama, GlobalProtect)**: Firewall management, rule creation, migrations & implementations, monthly audits.
- **CATO Networks (SASE/SD-WAN)**: Implementation of CATO sockets, deployment of secure network infrastructure.
- **Lead & Responsible for Rapid7 (InsightVM, AppSec, IDR)**: Integration, client training, vulnerability analysis, remediation tracking, SOC monitoring.
- **SentinelOne**: EDR deployment, alert analysis, incident response.
- **Okta (IAM)**: SSO, MFA, SCIM provisioning, automation via Workflows, Zero Trust posture.
- **Digital Guardian (DLP)**: Policy creation, data leak incident analysis.
- **Netwrix Privilege Secure**: Privilege Manager policy design including use case analysis, delegation models, and semi-automated elevations.
- **Netwrix Auditor**: Advanced security audit on Active Directory, access log analysis, anomaly detection after security incidents (post-mortem).
- **Mimecast**: Quarantine management, user awareness, incident operations and remediation.

Freelance Trainer

VD Formations – Paris & PACA Region

Sep 2021 - Present

- **Training for BTS, TAI & early years**: Linux (Bash, hardening, iptables), Windows Server (Active Directory, GPO), Networks (TCP/IP, VLAN, VPN).
- **Cybersecurity modules**: Penetration testing, SIEM, XDR, IAM, operational SOC.

EDUCATION

ESGI, Paris

2023 – 2025

Master's Degree in Computer Science, Cybersecurity

PERSONAL PROJECTS

Panther ASOC (Automated SOC)

Wazuh, Suricata, TheHive, pfSense orchestrated by Ansible (Incident Response deployment).

Harmony

Modular HTTP load balancer with traffic distribution, health checks, rate limiting, and logging. Inspired by Stanford's CS110L project.

Proxmox Infrastructure

Complete HomeLab with virtualization, high availability, IoT, and site-to-site VPN.

SKILLS, LANGUAGES & INTERESTS

Technical Skills: SIEM, EDR/XDR, IAM, SSO/MFA (SAML, OIDC, SCIM), DLP, NGFW, IPSec/SSL VPN, 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.

Languages: English (C1 - 890), Hindi (C1), French (Native), Spanish (A1)

Interests: Reading, Golf, Weight training, Motorsports