

MONDI XHARDA

RECHERCHE ALTERNANCE CYBERSÉCURITÉ — SOC / DÉTECTION · 2026-2028

RYTHME 3 SEM. ENTREPRISE / 1 SEM. ÉCOLE · DISPONIBLE IMMÉDIATEMENT

+33 7 67 05 84 56 · mondi.xharda@supdevinci-edu.fr · Bordeaux

21 ans / 2005 · Permis B

PROFIL

Étudiant en Mastère Cybersécurité (Sup de Vinci), certifié PJPT. En alternance chez Dolist, j'ai déployé seul un SIEM Graylog en production sur un parc d'environ 400 VM et automatisé sa collecte avec Ansible. Pratique offensive régulière (Active Directory, top 7 % TryHackMe) mise au service de la détection. Je recherche une alternance SOC / détection sur 2 ans.

CERTIFICATIONS

- PJPT — TCM Security · août 2026
- LPIC-1 · en préparation
- SAL 1 — TryHackMe · objectif 2027

EXPÉRIENCE

ALTERNANT SÉCURITÉ OPÉRATIONNELLE & SUPPORT IT

DOLIST · ÉDITEUR SAAS EMAILING/SMS (ISO 27001) · MÉRIGNAC
MARS – SEPT. 2026 · ALTERNANCE DE 3E ANNÉE

- Déploiement d'un SIEM Graylog en production (Docker, Graylog/MongoDB + OpenSearch) sur un parc d'environ 400 VM : 6 tableaux de bord, 106 widgets, alertes temps réel vers Teams.
- Filtrage à la source mesuré et vérifié sur trafic réel : 98,2 % du bruit pare-feu écarté (327 000 → 6 000 messages par jour). 12 mois de rétention tenus en consommant 4 fois moins que le budget disque.
- Industrialisation de la collecte en rôles Ansible (Winlogbeat/Filebeat) : raccordement d'un lot de serveurs ramené de 1 jour à moins d'1 minute.
- Audit des clés SSH sur 405 hôtes en 49 s : 115 clés privées non protégées, en réalité 50 clés recopiées sur 93 serveurs. Risque documenté et remonté.
- Gestion des vulnérabilités (SecPod Saner) : priorisation par criticité et suivi de la remédiation.
- Migration du datacenter : cartographie réseau pour une bascule tracée, sans interruption de service.
- Documentation de reconstruction de 27 pages.

FORMATIONS

MASTÈRE INFORMATIQUE — SPÉCIALITÉ CYBERSÉCURITÉ
SUP DE VINCI · 2026 – 2028

BACHELOR COORDINATEUR DE PROJETS INFORMATIQUES (EN ALTERNANCE)
SUP DE VINCI · 2023 – 2026

BACCALAURÉAT GÉNÉRAL — OPTION NSI / SES
LYCÉE FERNAND DAGUIN · 2020 – 2023

LANGUES

- Français : courant (bilingue)
- Albanais : langue maternelle
- Anglais : professionnel

RÉSEAUX

Portfolio : https://mondi-xharda.fr
TryHackMe : mdx13
Root-Me : D - N o t e X
LinkedIn : Mondi Xharda
Github : github.com/mond1-d3v

COMPÉTENCES

DÉTECTION & SOC :
SIEM GRAYLOG · WINLOGBEAT/FILEBEAT · FILTRAGE ET QUALIFICATION DES LOGS · ALERTING · MITRE ATT&CK · IDS SURICATA · GRAFANA, PROMETHEUS

OFFENSIF / RED TEAM :
ACTIVE DIRECTORY (BLOODHOUND, ÉLÉVATION DE PRIVILÈGES, COMPROMISSION DE DOMAINE) · POST-EXPLOITATION · CTF

VULNÉRABILITÉS & THREAT INTEL :
CVE, CVSS, EPSS, CISA KEV · SECPOD SANER · CERT-FR / ANSSI · PRIORISATION PAR EXPLOITABILITÉ

SYSTÈMES, RÉSEAUX :
WINDOWS SERVER, ACTIVE DIRECTORY, LINUX · PROXMOX, DOCKER · PFSENSE, STORMSHIELD, VLAN, VPN IPSEC

AUTOMATISATION & DEVSECOPS :
ANSIBLE · N8N · RAG / LLM LOCAL

RÉFÉRENTIELS & CONFORMITÉ :
ISO 27001 · RGPD

PROJETS

SENTINELIA — VEILLE ET PRIORISATION DES VULNÉRABILITÉS:

- Pipeline n8n croisant CISA KEV et EPSS pour ne remonter que les failles réellement exploitées, avec assistant RAG local (Ollama, pgvector) générant les synthèses d'analyste.

LABO ACTIVE DIRECTORY — OFFENSIF :

- Cartographie des chemins d'attaque avec BloodHound, élévation de privilèges jusqu'à la compromission complète du domaine, puis rédaction des contre-mesures.

CTF & BUG BOUNTY :

- StarHack x Yogosha : 27e / 373 (top 7 %) · Participation au programme Yogosha 2025 · TryHackMe top 7 %.

ARCHITECTURE SÉCURISÉE — PROJET ALTHEA SYSTEMS:

- Segmentation VLAN, Stormshield, VPN IPsec, IDS Suricata et SIEM Wazuh sur environnement virtualisé.

CENTRES D'INTÉRÊT

- HackTheBox, TryHackMe, Root-Me
- Veille CERT-FR / ANSSI
- Salle de Sport
- Jeux vidéo (CS2, Call of Duty)