Alternant Ingénieur Cybersécurité / Systèmes & Réseaux - ESIEA Laval

Honoré Sèwanoudé MITCHOZOUNNOU

honoresewanoude@gmail.com 0616845806 Poissy 22 ans

Profil

Admis en cycle ingénieur cybersécurité à l'ESIEA Laval, je recherche une alternance de 36 mois à partir de septembre 2026. Intéressé par la sécurité des systèmes d'information et les infrastructures IT, j'ai développé des compétences en **administration systèmes et réseaux, virtualisation, supervision, détection d'incidents et analyse de logs, au sein d'environnements Windows/Linux**. Motivé par les enjeux de continuité de service, de sécurité et de fiabilité des systèmes, je souhaite intégrer votre entreprise afin de contribuer à la sécurisation des infrastructures informatiques

Formation

09/2024 – Present
Tarbes

BTS Cybersécurité, Informatique et réseaux, Électronique (CIEL)
Lycée Saint Pierre
- **Cisco Certified Network Associate (CCNA) en cours**

09/2022 – 07/2024
Cotonou, Bénin

Licence 1 et 2 Informatique Réseaux Télécommunication
ESGIS

07/2022
Bénin

Baccalauréat (sciences mathématiques)
CEG Ikpinlè

Compétences / Projets Personnels réalisés

Déploiement d'un SIEM Wazuh
- Installation du manager, ajout d'agents Windows/Linux
- Mise en place d'un IDS Hôte (HIDS) via Wazuh (analyse Sysmon, brute force, Kerberos, événements Windows/Linux)
- Analyse des Faux positifs / vrais positifs

Environnement Active Directory complet
- Installation Windows Server, DNS, DHCP
- Création d'OU, GPO, gestion permissions
- Simulation d'attaques (failed logon, bruteforce RDP) + analyse des logs

Virtualisation d'un réseau complet (VMware)-Sécurité avancée (NDR)
- Mise en place d'un réseau multi-VLAN avec trunking, routage inter-VLAN et firewalling
- Déploiement d'un IDS/IPS réseau (Suricata) et d'un moteur d'analyse NDR (Zeek) pour la détection d'anomalies L2/L3
- Détection de scans Nmap, ARP spoofing, DHCP rogue, brute force SSH et comportements suspects
- Intégration avec Wazuh (SIEM) pour la corrélation des événements et l'investigation
- Construction d'un mini environnement attaque/défense (Kali-Windows Server) pour valider les alertes

Expérience Professionnelle

ANTHEA INFORMATIQUE
Stage Technicien Informatique
Environnement technique: Cisco (IOS), Windows Server 2019, Active Directory, Linux Ubuntu, Wireshark, Nmap, VMware
- Configuration et sécurisation des switchs Cisco : VLAN, trunking 802.1Q, DHCP Snooping, Dynamic ARP Inspection
- Mise en place d'un domaine Active Directory: installation, intégration de 24 postes dans le domaine, gestion des utilisateurs, permissions et premières GPO
- Analyse, capture et diagnostic du trafic réseau avec Wireshark et Nmap
- Participation au durcissement du réseau et à la surveillance des événements critiques (logs Windows/Linux)

Soft Skills

- Rigoureux
- Esprit analytique
- Capacité à travailler en équipe

Langues

Français
Courant

Anglais
Technique