KAN

CONSULTANT RESEAU ET SECURITE N3

DOMAINES DE COMPÉTENCES

Savoir-faire	•
Sécurité	• Firewalling (Checkpoint, Fortigate, Sophos, Pfsense, Mikrotik) • Gestion de parc informatique (GLPI, ManageEngine Central, Maas360) • Gestion d'accès et identité (Active directory, ZTNA, Maas360, Delinea) • Gestion de vulnerabilité (OpenVas, Immuniweb, Owasp 10, Nessus,) • Gestion des logs (Seceon, Wazuh, AllienVault, Qradar community) • Gestion des solutions d'EDR (Checkpoint, Kaspersky, SentinelOne, Sophos intercept X) • Connaissance du Mitre attack Framework • Protection d'acces distant (Checkpoint ZTNA, VPN SSL, IPSEC) • Maitrise des technologies (HA, Cluster, Loadbalancing) • Parfaite maitrise de la solution Tufin
Réseau	• Interconnexion logique (SDWAN, VPN IPsec, VPN ssl, L2tp,) • Conception infrastructure réseau 3 tiers (Cisco Switching & routing) • Bonne connaissance des protocoles de réseau de niveau 3 (OSPF, RIP, EIGRP, Statique, VRR) • Bonne connaissance des protocoles de niveau 2 (HSRP, Vlan, STP, Etherchannel, VTP, Port security)

DIPLÔMES

- **2018 :** Licence en réseaux informatiques et télécommunication.
- **2012 :** Brevet de technicien supérieur (BTS) en réseaux informatiques et télécom

CERTIFICATIONS

- **En cours**: Palo Alto Certified Network Expert
- **2024** : Palo Alto PCNSA/ PSE
- **2024 :** Tufin Aurora TCSE 6 Delivery path/ Fortinet Certified Professional Network Security
- **2023 :** Checkpoint CCSE**,** CCSA**,** CCPA
- **2023 :** Fortinet Certified Associate in Cybersecurity
- **2022 :** Certified In Cybersecurity (CC) – ISC2/ Certified IBM MDM/UEM Maas 360 architect
- **2021 :** Certified Sophos XG firewall Engineer
- **2022 :** Cisco Certified Network Associate

LANGUES

- **Anglais :** Courant

EXPÉRIENCES PROFESSIONNELLES

Consultant Réseau et Sécurité Build & Run & Référent Tufin - Forfait

Multi Clients : A*PRIA, STET, CANAL+, RATP, SAFRAN*

Depuis janvier 2024

Projet : Gestion centralisée de la sécurité des réseaux et des politiques de pare-feu / Optimisation et automatisation des politiques de sécurité

Tâches principales :

Préparation et planification

- **Analyse des besoins et des exigences** : Évaluer les besoins en sécurité réseau et les exigences de conformité spécifiques à l'organisation pour orienter le déploiement.
- **Inventaire de l'infrastructure :** Lister les dispositifs de sécurité réseau (pares-feux, routeurs, etc.) et les environnements (on-premise, cloud, hybride) qui seront intégrés à Tufin
- **Définition des objectifs du projet** : Formuler les objectifs spécifiques pour la gestion centralisée, l'optimisation et l'automatisation des politiques de sécurité.
- **Planification des ressources** : Identifier les ressources nécessaires (personnel, serveurs, licences) pour le déploiement et déterminer un calendrier des étapes du projet.

Installation et configuration de tufin

- **Installation des composants Tufin** : Déployer les serveurs nécessaires pour Tufin SecureTrack, SecureChange, SecureApp, etc., en fonction des besoins de l'entreprise.
- **Configuration réseau :** Configurer les connexions réseau pour que Tufin puisse interagir avec les pare-feux, routeurs et autres équipements.
- **Paramétrage des comptes et des rôles utilisateurs :** Configurer les accès en fonction des rôles pour respecter la gouvernance et la séparation des tâches

Intégration des Dispositifs de Sécurité

- **Connexion des pare-feux et équipements de sécurité** : Intégrer les pare-feux et dispositifs réseau au sein de Tufin pour permettre une gestion centralisée.
- **Collecte des politiques existantes** : Importer les politiques de sécurité en cours et les configurations pour établir une vue d'ensemble.
- **Cartographie des réseaux** : Utiliser les outils de Tufin pour créer une cartographie des flux et des relations d'interdépendance entre applications et réseaux.

Définition et Optimisation des Politiques de Sécurité

- **Analyse et nettoyage des politiques** : Identifier les règles obsolètes, redondantes ou risquées et définir des règles optimisées.
- **Mise en place de règles de segmentation** : Définir des politiques de segmentation pour protéger les segments critiques du réseau.
- **Automatisation des politiques de sécurité** : Configurer les workflows d'automatisation pour appliquer et maintenir les règles de sécurité à l'aide de Tufin SecureChange.

Mise en Place de l'Orchestration des Changements

- **Configuration des workflows de changement** : Configurer les workflows de modification des politiques pour les demandes de changement, les validations et les approbations automatisées.
- **Tests et validation des modifications automatisées** : Effectuer des tests pour valider que les changements automatisés sont appliqués de manière conforme et sécurisée.

- **Documentation des processus de modification** : Documenter les workflows et les processus pour garantir la traçabilité et la conformité.

Assurance Conformité et Gestion des Risques

- **Rapports et audits** : Configurer et automatiser la génération de rapports pour les audits de sécurité et la conformité.
- **Gestion proactive des risques** : Utiliser les fonctionnalités de Tufin pour surveiller les risques liés aux modifications de politiques et anticiper les vulnérabilités.

Formation et livrables

- **Formation des équipes** : Former les équipes sur l'utilisation de Tufin, l'interprétation des rapports, et la gestion des changements et des incidents.
- **Livrable de la solution** : HLD, LLD, DEX

Validation et Mise en Production

- **Tests de validation** : Exécuter des tests finaux pour vérifier que Tufin fonctionne comme prévu dans l'environnement de production.
- **Mise en production** : Migrer vers l'environnement de production une fois les tests validés.
- **Suivi post-déploiement** : Surveiller les performances et l'efficacité des politiques automatisées, et ajuster si nécessaire.

Environnement technique : Tufin, Palo Alto, Fortinet, Forcepoint, Cisco, Forti-Manager, Panorama

Consultant Réseau BUILD I Radio Télévisé Ivoirien - Forfait

D'aout 2023 à novembre 2023 (3 mois)

Projet : Optimisation du réseau informatique

Tâches principales :

- Conception et mise en place d'une architecture réseau
- Déploiement de 2 pares-feux checkpoint serie 1800 en cluster actif-actif
- Configuration des règles de routages internes et externes, NAT, DNAT, Firewalling, IPS…
- Migration des réseaux du WAN vers la nouvelle DMZ
- Configuration du serveur de Management cloud des pares-feux
- Intégration des pares-feux au serveur de management smart-1 cloud

Environnement technique : Checkpoint, smartcloud, Cisco Catalyst

Consultant Réseau BUILD I Confidentiel Santé, Côté d'Ivoire - Forfait

De janvier 2023 à avril 2023 (4 mois)

Projet : Mise en place d'un SIEM

Tâches principales :

- Déploiement de la solution de gestion des évènements de sécurité (SECEON aiSIEM) sur VM
- Identification des sources de logs critiques (Fortinet, Active directory, Messagerie office 365 et applications web)
- Intégration des sources de données de chaque actif critique
- Collection des logs des différents actifs criques via le Protocol Syslog et agents
- Test des fonctionnalités (collecte de données, analyse des données, Corrélation des données, rapport et visualisation)

Environnement technique : SIEM SECEON, Fortinet, Office365, AD

Consultant Réseau BUILD I Banque National Ivoirienne

D'Aout 2022 à décembre 2022 (5 mois)

Projet : Renfort référent Sécurité Réseau

Tâches principales :

- Evaluation du niveau de sécurité SI basé sur le CIS control
- Accompagnement lors de test d'intrusion sur l'infrastructure réseau
- Recommandations des mesures de sécurité

Environnement technique/fonctionnel : Cis Control, Kali linux, Nessus, Owasp 10

Consultant Réseau BUILD I Petro Ivoire - Forfait

Mars 2022 à avril 2022 (2 mois)

Projet : Mise en place d'une solution de protection d'accès à distance

Tâches principales :

- Déploiement et configuration de la plateforme ZTNA harmony Connect de checkpoint
- Création des groupes utilisateurs selon leurs niveaux d'habilitation
- Création des règles et des politiques de contrôle d'accès aux applications appliquées à chaque groupe utilisateur
- Publications des applications dans le portail ZTNA des utilisateurs
- Formation et prise en main des administrateurs

Environnement technique : Checkpoint ZTNA Harmony Connect

Consultant Réseau BUILD I Confidentiel Santé - Forfait

Février 2022 à Mars 2022 (1 mois)

Projet : Migration du serveur Management local checkpoint vers le Cloud

Taches principales :

- Upgrade du serveur de management local à la version R81
- Exportation de la BD du serveur de management local vers la nouvelle plateforme de management cloud
- Reconnexion automatique des agents endpoints vers la nouvelle plateforme via un script de Checkpoint
- Formation des administrateurs à la plateforme cloud

Environnement technique : Checkpoint SMS R81, Infinity Portal

Consultant Réseau BUILD I ALC, Côté d'Ivoire - Forfait

Novembre 2021 à janvier 2022 (3 mois)

Projet : Mise en place d'une infrastructure réseau 3 tier

Taches principales :

- Mise en place d'une architecture 3 tier avec des équipements cisco
- Segmentation du réseau LAN en plusieurs Vlans en fonction des services au niveau des switchs d'acces

- Configuration de la redondance des passerelles vlan via le protocol HSRP au niveau des switchs d'accès
- Configuration du protocole trunk entre les switchs d'accès et de distribution
- Configuration du protocole EtherChannel LACP entre le switch de distribution et d'accès
- Configuration du protocole OSPF au niveau des switchs de distriburion et switchs coeurs
- Mise en place des ACLs et la sécurité des ports.

Environnement technique : CISCO Catalyst L2 & L3

Référent Sécurité et Réseau I La Poste, Côté d'Ivoire

Février 2021 – Juin 2022

Contexte : Au sein du département de sécurité, où je faisais partie d'une équipe de 2 ingénieurs en sécurité, ma mission consistait à mettre en place des bonnes pratiques et des technologies réseau et sécurité pour assurer la protection des systèmes et des données de l'organisation.

Taches principales :

- Référent privilège avec le responsable au centre de sécurité du système d'information pour toute question relative à la sécurité.
- Effectuer les tâches de contrôle continu et de contrôle récurrent des mesures de sécurité (contrôle contre les codes malveillants, contrôle contre les intrusions dans le réseau, revues périodiques des droits);
- Veiller à ce que la sécurité du SI soit systématiquement prise en compte dans les projets (ISP)
- Collaborer avec le le chef du Centre de sécurité du système d'information et le DSI dans la mise en œuvre du plan de traitement des risques ;
- S'assurer que les directions appliquent les mesures de traitement de risques applicatives à leur périmètre de responsabilité et acceptent ces mesures ;
- S'assurer que les utilisateurs utilisent systématiquement les moyens informatiques mis à leur disposition conformément aux procédures en vigueur ;
- Contrôler et évaluer les sauvegardes et des plans de reprise et de continuité d'activité.

Environnement technique : Mikrotik, Cisco, Active directory, SDWAN, Sophos, AlienVault, Sophos XDR, GLPI

Administrateur Réseau RUN I La Poste, Côté d'Ivoire

Janvier 2019 – Février 2021

Contexte : Au sein du département réseau, constitué d'une équipe de 6 personnes, ma principale mission consistait à garantir le bon fonctionnement de l'infrastructure réseau et à assurer sa capacité d'évolution.

Taches principales :

- Optimisation de l'infrastructure réseau
- Gestion du routage interne et externe
- Gestion des Vlans
- Gestion des ouvertures et des fermetures de flux réseaux au niveau des pare-feu
- Gestion des accès VPNs et des liens SDWANs
- Analyse de la performance du réseau et résolution de problèmes potentiels
- Gestion des comptes Active Directory des utilisateurs internes et externes
- Gestion du réseau sans fil (WLAN)

Projet : Interconnexion des bureaux de poste avec la technologie SDWAN sophos – Durée 1 mois

Taches principales :

- Installation des boitiers SDWANs sur chaque site distant
- Onbording et configuration intiale des boitiers via la plateforme de management
- Configuration des routes vers le site principal et des policies appliqués aux differents boitiers depuis la plateforme de Controle
- VSR

Environnement technique : Mikrotik, Cisco, Active directory, SDWAN, Sophos, AP Mikrotik, Zabbix.