TEAM PARTNERS
smart data for smart business.

Contact commercial

vfaysse@team-partners.ch

022 710 27 40 / 079 770 06 22

www.team-partners.ch

L. S.

Consultante cybersécurité

DOMAINE DE COMPETENCES

Cybersécurité — Débutant — Expert

Sécurité réseau — Débutant — Expert

DIPLÔMES & FORMATIONS

2016 **Diplôme d'ingénieur en Qualité et sécurité des Réseaux** (BAC+5) à l'ESIREM de Dijon

2013 **Diplôme d'Ingénieur de travaux informatiques** (Bac +3) option Systèmes et Réseaux à l'IAI - Cameroun.

CONNAISSANCES TECHNIQUES

Réseau

- Certification Cisco : CCNA1 (notions de bases sur les réseaux), CCNA2 (routage et commutation), CCNA3 (commutation de réseau local et réseau local sans fil)
- Administration et gestion des réseaux : DNS, DHCP, TCP/IP, OSI, RSVP, serveur web (Apache), SNMP, Active Directory, Centreon
- Simulation et analyse du trafic réseau : NS-2, Cisco packet tracer, Wireshark, GNS-3

Systèmes d'exploitation : Ubuntu, Debian,CentoS, Windows Server 2008
Sécurité Réseau : RSA, Fortinet, ESI, SECOPS,
Gestion de projet : Certification Prince2 fondamental
SIEM : RSA, logstash, Arcsight
Monitoring des bases de données : Guardium Data Protection
Formation : Préparation à la certification BPM Foundation OMG-OCEB

LANGUES

- Français ◉◉◉◉◉
- Anglais ◉◉◉◉◉

EXPERIENCES PROFESSIONNELLES

Consultante cybersécurité
Banque X (Confidentiel) (Genève) 06/2020 – 09/2021

Projet de migration de Arcsight vers Logstash + Deploiement Guardium Data Protection

- Installation de la solution logstash
- Ouverture de flux
- Création des VIPs
- Mise en place des services logstash
- Mise en place du monitoring sur les services et les serveurs logstash
- Test et validation de la collecte des logs dans un environnement de recette
- Déploiement dans l'environnement de production
- Vérification du format de logs et des Use cases
- Rédaction de la documentation d'onboarding des différentes technologies
- Mise en place du coverage
- Projet Guardium :
    - Mise en place de l'architecture de recette et de production
    - Création des VIPs
    - Ouverture des flux
    - Ouverture des flux applications et serveurs
    - Installation et configuration de la solution guardium
    - Installation des agents sur les serveurs de base de données
    - Mise en place et test des Use Case

Technologies : SIEM Arcsight, Logstash, Guardium Data Protection

Consultante cybersécurité
BNP PARIBAS Leasing Solutions (France) 06/2019 – 11/2019

Projet de Migration Acsight vers une nouvelle version

- Installation de la solution arcsight
- Installation et configuration des collecteurs
- Mise en place de la collecte des logs
- Proposition des Use Case de surveillance pour la surveillance de l'infrastructure

Technologies : SIEM Arcsight

Chef de projet SOC
CREDIT AGRICOLE (France) 04/2019 – 06/2019

- Identification des applications qui utilisent les protocoles obsolètes LDAP et NTLMv1
- Remonter la liste à chaque entité
- Réunion de suivi de correction de l'obsolescence
- Proposition des planning de correction

EXPERIENCES PROFESSIONNELLES

Projet SOC Build & MCO SOC
Linky ENEDIS (France) 04/2018

- Assurer l'administration et l'exploitation technique des différents outils utilisés
- Maintenir à jour les bases documentaires (dossiers d'architecture et d'exploitation, livrables)
- Assister l'équipe d'analyse et identifier des mesures ou solutions permettant d'améliorer le travail de détection ou de supervision
- Fournir les indicateurs de fonctionnement de la plateforme
- Planifier et organiser les éventuelles montées de version
- Corriger dans les délais les plus brefs tout incident lié à la plateforme de supervision
- Identifier des idées d'industrialisation ou d'amélioration des procédures et techniques d'administration et d'exploitation
- Vérifier la collecte et fiabiliser la collecte des logs
- Faire une amélioration continue en termes de parsing des logs.
- Rédiger des PV de collecte de logs.
- Modifier, créer les feeds et les apprules
- Créer et indexer les metas
- Installer les agents NXLOG sur les serveurs Windows afin de collecter les logs.

Technologies : SIEM RSA Netwitness for Logs and Packets, gestion de vulnérabilités.

Consultante
Silca (Crédit Agricole) (France) 04/2017 – 03/2018

Analyste N2 SOC 01/2018 – 03/2018

- Analyse et traitement des incidents sur les Antivirus Symantec et Sophos
- Analyse et traitement des incidents sur le périmètre Airwatch pour la gestion de la mobilité.
- Analyse des rapports des flux de données, la fuite de données web mail
- Analyse des rapports d'IOC et ajout dans les feeds
- Rédaction du bulletin hebdomadaire
- Envoie des rapports d'EPS (Evènements Par Seconde)

Technologies : SIEM RSA Netwitness, SECOPS, Linux

Build SOC 04/2017 – 12/2017

- Collecte et vérification de la collecte des logs
- Création et amélioration des parsers pour les logs des équipements : Ciscorouter, Fortinet, Ciscoasa, Ciscopix,Windows, Rhlinux, Symantec, Trendmicro
- Création des rapports de contrôle de collecte
- Vérification et mise à jour du référentiel de collecte SILCA
- Création et indexation des métadonnées
- Configuration du POC ODBC pour la collecte des logs de base de données SQL et Oracle.
- Création et mise en place des uses cases (Alertes et Rapports) pour générer les incidents de sécurité
- Rédaction des PV de collecte
- Rédaction des fiches reflexes

Technologies : SIEM RSA netwitness, ESI, Linux, Windows

EXPERIENCES PROFESSIONNELLES

Audit de configuration des SI
Sogeti (France) 09/2016 – 03/2017

- Audit de serveurs Linux & Windows
- Audit des bases de données PostgreSQL, Sybase
- Audit serveur web Apache, serveur d'application Tomcat
- Audit Serveur Exchange 2013 & Microsoft Outlook 2010
- Revue des règles de firewall

Stagiaire
Savoye (France) 02/2016 – 07/2016

- Audit des réseaux CAN, WIFI, ETHERNET, PROFIBUS, RS485.
- Proposition de solutions pour pallier aux différents problèmes rencontrés dans ces réseaux.
- Etude et mise en place d'une solution de monitoring
- Rédaction du cahier des charges
- Tests des outils
- Choix de l'outil ou des outils
- Déploiement de l'outil

Stagiaire
My Media (France) 06/2015 – 08/2015

- Développement et benchmark de diverses solutions de tracking
- Administration et audit réseau

Stagiaire Administration réseau avec Active Directory
Thelligence International (Cameroun) 05/2013 – 08/2013

- Installation et administration des services DNS, DHCP, Active Directory.
- Gestion du partage des fichiers, des imprimantes, des sessions utilisateur et du profil

Stagiaire
CAMPOST (Cameroun) 06/2012 – 09/2013

- Mise en place d'un serveur Proxy
- Maintenance matérielle et logicielle du parc informatique