Kawtar TARMIDI
INGENIEURE CYBERSECURITE
8 ans d'expérience
Kawtar.tarmidi@gmail.com

1. PROFIL

COMPETENCES METIERS

- Tourisme, Energie, Import/Export, RH, Formation Professionnelle, Réseaux Sociaux d'Entreprise, GED, Gouvernance (SMSI).

COMPETENCES TECHNIQUES

- Vérification de la conformité des SI aux dispositions de sécurité (patchs, mises à jour).
- Assurer la veille technologique, et le suivi des vulnérabilités et indicateurs de sécurité.
- Administration et amélioration des dispositifs de sécurité (firewall, Endpoint, PAM OneIdentity Wallix)
- Gestion des incidents de sécurité et analyse des demandes d'ouverture de flux, règles du pare-feu/WAF ou l'ajout d'exceptions. (Netscaler, Fortigate, Forcepoint, Sophos, Opensense)
- Réponse aux incidents de sécurité et infection potentielle dans un soucis de continuité d'activité.
- Test régulier du bon fonctionnement des dispositifs de sécurité (techniques et fonctionnels).
- Supervision et Reporting : Documentation et optimisation des tableaux de bord.
- Administration des antivirus/EDR/antimalware: (Harfanglab, Bitdefender, Sophos, Trendmicro)
- Gestion des vulnérabilités et patching (TENABLE, ACUNETIX, GREENBONE)

COMPETENCES ORGANISATIONNELLES

- Force de propositions techniques et organisationnelles.
- Bonnes capacités de communication à travailler en équipe.
- Encadrement d'équipe de 5 à 10 personnes : planification, organisation et exécution des tâches
- Gestion de projet : suivi de l'observance des livrables (JIRA), coordinations des équipes, gestion des prestataires, POC, lancement (comités cyber, Coproj, atelier kickoff, COPIL, démos…)
- Mise en place du SOC hybride
- Capacité d'adaptation aux environnements multiculturels.

COMPETENCES FONCTIONNELLES :

- Définition d'architectures réseaux et sécurité.
- Intégration, déploiement et support N2/N3.
- Gestion et animation de la relation avec des AMOA / clients et des MOE internes ou externes (opérateurs, intégrateurs).

- **DIPLOMES / CERTIFICATIONS**

2024	**CISSP en cours**
2022	**Certification Fortinet NSE4**
2020	**Scrum Foundation Professional Certificate**
2018	**Certification Sophos Engineer**
2016	**Première année Doctorat Télécommunications INPT (Institut National des postes et télécommunications)**
2015	**Diplôme d'Ingénieur d'état Réseaux & Télécommunications – ENSA**

2. COMPETENCES TECHNIQUES

RESEAUX ET TELECOM	**RÉSEAU:** LAN / DATACENTER / FO, VSAT **PROTOCOLES:** SNMP, DHCP, NAT, VPN IPSEC/SSL
SECURITE ET AUDIT	**ANTIVIRUS:** BITDEFENDER SOPHOS, KASPERSKY, TRENDMICRO, ESET, SYMANTEC **EDR:** HARFANGLAB **FIREWALL:** SOPHOS, FORTINET, FORCE POINT, PFSENSE. **WAF :** Citrix Netscaler Ubika SaaS **PAM:** One identity (Balabit) WALLIX **VPN:** FORCE POINT, CITRIX GATEWAY **AUDIT:** ANALYSE DE VULNERABILITE (TENABLE, ACUNETIX, GREENBONE)
SYSTEMES	**MICROSOFT:** GPO, ACTIVE DIRECTORY , WINDOWS 7/8/8.1/10 Windows Server 2016/2019 **VIRTUALISATION:** HYPERV, VSPHERE, NUTANIX AHV
LOAD BALANCING	NETSCALER
MESSAGERIE	GSUITE
MONITORING	SOLARWINDS, ZABBIX
STOCKAGE	VERITAS, COMMVAULT, NAS
BASE DE DONNEES	Oracle DB, MYSQL, POSTGRES, SQL SERVER
Tools	JIRA CONFLUENCE
NORMALISATION	ISO 27001

3. PROJETS & EXPERIENCES

PROJET	**INGENIEURE CYBERSECURITE**
PERIODE	**Mai 2023 À AUJOURD'HUI**
SECTEUR/ CLIENT	**Archivage digital et physique / XELIANS**
ROLE	**Ingénieure cybersécurité**
CONTEXTE	Renforcement de la sécurité des systèmes d'archivage numérique
ACTIVITES	Mise en place et administration d'une solution EDR Harfanglab on premise • **Conception et Planification** : ▪ Évaluation des besoins spécifiques de sécurité de l'entreprise pour une intégration efficace de la solution EDR Harfanglab. ▪ Planification détaillée de l'architecture de la solution, en accord avec l'infrastructure IT existante. • **Déploiement et Configuration** : ▪ Installation et configuration précise du système EDR Harfanglab sur l'ensemble des terminaux et serveurs. ▪ Établissement de politiques de détection robustes et de règles de corrélation d'événements pour une surveillance efficace. • **Surveillance et Détection des Menaces** : ▪ Surveillance continue des terminaux à l'aide de techniques avancées et d'intelligence artificielle pour identifier les comportements suspects. ▪ Analyse et triage des alertes de sécurité pour distinguer les menaces légitimes des faux positifs. ▪ Personnalisation des règles de détection, notamment l'utilisation des règles YARA pour cibler des patterns spécifiques de malwares et les règles Sigma pour une détection normalisée. • **Réponse aux Incidents et Remédiation** : ▪ Réponse rapide aux menaces identifiées, incluant l'isolement des terminaux affectés et la neutralisation des menaces. ▪ Analyse post-incident pour déterminer la source et la méthode d'attaque, et prévenir de futures intrusions. • **Maintenance et Mise à jour** : ▪ Mises à jour régulières du logiciel EDR pour s'adapter aux nouvelles menaces et vulnérabilités. ▪ Révision continue des politiques de sécurité et des configurations pour maintenir une protection optimale. • **Rapports et Conformité** : ▪ Génération de rapports détaillés sur les incidents de sécurité et les tendances observées pour des améliorations continues. ▪ Assurance de la conformité des pratiques de sécurité avec les normes et réglementations en vigueur. Mise en place et administration d'une solution antivirus/antimalware Bitdefender on premise • **Installation et Configuration Simplifiée :** ▪ Déploiement du logiciel Bitdefender sur les terminaux et serveurs. ▪ Réglage fin des paramètres pour une protection efficace tout en préservant les performances système. ▪ **Gestion des Politiques de Sécurité et des Exclusions** :

	▪ Établissement de politiques de sécurité adaptées, incluant des listes d'exclusions pour les applications sensibles et minimiser les faux positifs. • **Surveillance Active et Intervention Rapide :** ▪ Monitoring continu pour une détection proactive des menaces. ▪ Réaction immédiate aux alertes pour contenir et neutraliser les infections. • **Maintenance et Mises à Jour Continues** : ▪ Mises à jour régulières pour une défense contre les nouvelles menaces. ▪ Entretien constant du système pour une efficacité maximale. • **Rapports et Analyse des Tendances de Sécurité** : ▪ Production de rapports détaillés pour un suivi précis des menaces et des incidents. <u>Mise en place et administration d'une solution de scan de vulnérabilités TENABLE dans le cloud</u> • **Déploiement et Configuration dans le Cloud** : ▪ Mise en œuvre de la solution TENABLE dans l'environnement cloud pour un scan complet des vulnérabilités. ▪ Configuration adaptée pour cibler efficacement les actifs et zones sensibles de l'infrastructure. • **Scans Réguliers et Évaluation des Vulnérabilités** : ▪ Planification et exécution de scans réguliers pour détecter proactivement les vulnérabilités. ▪ Analyse précise des résultats pour évaluer les risques et prioriser la remédiation. • **Gestion des Correctifs et Processus de Remédiation** : ▪ Coordination des efforts de remédiation, y compris la sélection et l'application des correctifs. ▪ Suivi rigoureux des actions correctives pour garantir la résolution efficace des vulnérabilités. • **Reporting et Conformité** : ▪ Génération de rapports détaillés pour documenter l'état des vulnérabilités et le suivi de la remédiation. ▪ Veiller à la conformité avec les normes de sécurité et les réglementations. ▪ **Collaboration et Amélioration Continue** : ▪ Collaboration étroite avec les équipes IT et de sécurité pour une gestion des vulnérabilités intégrée et efficace. <u>Mise en place d'un SOC managé</u> • **Planification et Conception du SOC** : • Définition de la structure et des capacités requises pour le SOC, en s'assurant de l'intégration optimale du SIEM dans l'environnement existant. • Élaboration des processus de collecte de données et de surveillance de la sécurité pour maximiser l'efficacité du SOC.
ENVIRONNEMENT	HARFANGLAB, BITDEFENDER, TENABLE, IOC, IRM, SOC

PROJET	INGENIEURE SECURITE-CYBERSECURITE
PERIODE	**DECEMBRE 2019 A JANVIER 2023**
SECTEUR/ CLIENT	**COMMERCE EXTERIEUR / PORTNET**
ROLE	**Ingénieure Réseau et Sécurité**
CONTEXTE	Sécuriser les plateformes d'échanges de l'écosystème du guichet unique PORTNET
ACTIVITES	Préparation du projet SOC Hybride IBM QRADAR ▪ Analyse des différentes actions réseaux à entreprendre pour l'intégration des équipements ▪ Collecter l'ensemble des logs à partir des différentes sources ▪ Définition des use cases et des segments critiques ▪ Traiter les faux positifs, tunning des règles du SIEM Administration WAF/ LB CITRIX ADC ▪ Publication des nouvelles applications ▪ Ouverture des flux nécessaires dans les firewalls ▪ Intégration des services dans le LB ▪ Optimiser les règles du WAF pour éviter les blocages ▪ Gestion du VPN utilisateurs et partenaires Sécuriser les accès des collaborateurs/partenaires/prestataires aux plateformes ▪ Gestion de la matrice des flux via les firewalls internes (Forcepoint) et frontaux (Fortigate) ▪ Gestion des accès des utilisateurs aux serveurs en combinant LDAP et PAM Application des correctifs de vulnérabilités émis par le Centre de Veille de Détection et de Réaction aux Attaques Informatiques ▪ Gestion des upgrades et des patching pour les différents systèmes de sécurité ▪ Faire le suivi des vulnérabilités avec des outils de gestion de vulnérabilités (GREENBONE), et DAST (ACUNETIX) IPAM (INFOBLOX) ▪ Gestion des DNS et du DHCP ▪ Déploiement des plans IP des nouveaux sites Gestion de la sauvegarde et de la restauration des environnements de l'entreprise ▪ Backups & Restauration des Bases de données, des fichiers NFS, des VMs et des clusters Kubernetes Elaboration des procédures du PRA de l'entreprise ▪ Test du basculement des services publiés entre le DC1 et le DC2 ▪ MCO des équipements réseau Mise en conformité avec le nouveau SMSI ▪ Préparation de la cartographie des risques et des plans d'actions associés ▪ Animer les comités du CPSI / COSI / CTSSI ▪ Elaborer les plannings du PCA ▪ Animer les campagnes de sensibilisation aux risques cyber
ENVIRONNEMENT	FORTIGATE 500D, FORCEPOINT NGFW 1401, IPAM (ONE IDENTITY), NETSCALER, QRADAR, GREENBONE, ACUNETIX, NETBACKUP, COMMVAULT, SOLARWINDS, TRENDMICRO, NNT CHANGE TRACKER, CERTIFICATION ISO27001

PROJET	**INGENIEURE RESEAU ET SECURITE**
PERIODE	**JANVIER 2017-NOVEMBRE 2019**
SECTEUR/ CLIENT	**GROUPE PETROLIER/ MICROFINANCE/ CLUBMED FUTURELINK**
ROLE	**Ingénieure Sécurité, Réseaux et Systèmes**
CONTEXTE	Mettre en place des architectures réseaux d'entreprise, partagées entre les réseaux filaires (Ethernet), les réseaux sans fil (WLAN WiFi), les réseaux longue distance (VPN SSL, liens privés), et les télécom' (téléphonie sur IP). Identifier et répondre aux besoins des utilisateurs, prendre en compte les applications du système d'information existantes, et gérer tous les aspects de sécurité liés à ces dernières.
ACTIVITES	▪ Etude de l'existant et spécification du besoin ▪ POC de la solution SOPHOS / OPNsens/ Riverbed SteelConnect SDWAN ▪ Participation à la rédaction des spécifications techniques pour l'acquisition des solutions (SOPHOS, SYNOLOGY). ▪ Elaboration de l'architecture réseau cible pour les sites distants et le siège. ▪ Installation et mise en service : ○ SOPHOS XG/OPENsense : ▪ Mise en rack et raccordement du boitier. ▪ Configurations initiales (Adressage, routage, …) ▪ Définition des profils de sécurité pour les fonctionnalités IPS, AV, Contrôle Applicatif, Filtrage URL… ▪ Configurations des règles de sécurité selon la politique de sécurité ▪ Paramétrage des tunnels VPN. ○ SOPHOS ENDPOINT ▪ Intégration de la solution sur l'ensemble des postes de travail ▪ Configuration des politiques et stratégies de sécurité à appliquer ○ CUCM CISCO / ASTERISK ▪ Etablissement du plan de numérotation ▪ Paramétrage des restrictions ▪ Paramétrage du standard d'accueil ▪ Paramétrage de la collecte des logs. ▪ Paramétrage des rapports.
ENVIRONNEMENT	SOPHOS, OPENSENSE, WINDOWS SERVER, AD, DNS, WINDOWS 8, WINDOWS 10, GESTION DE PROJET ET DOCUMENTATION, ESET, KASPERSKY, RIVERBED