

MB

REFERENT VULNERABILITES

FORMATIONS & CERTIFICATIONS

2008 : Diplôme National d'Ingénieur - Institut National des Sciences Appliqués de Tunis

COMPÉTENCES

- Elaboration de processus de gestion des vulnérabilités
- Suivi de remédiation
- Coordination avec les équipes
- Reporting mensuel sur les vulnérabilités

COMPETENCES TECHNIQUES :

- Cyber : Tenable, Qualys, Rapid7, VULCAN, Haquity, AD Audit, ScoreCards, CERT-IST
- Serveur : Debian/Ubuntu, Microsoft Windows Server R2, Centos , Redhat ,Unix
- CRM/ERP : MS DYNAMICS, ERP IOT/Indus4.0, HPSM, CustomerCare, Support CRM,
- Base de données : MS SQL , PostgreSQL, MySql, Oracle
- Middle : Microsoft IIS , Apache, NGINX, Tomcat
- Workflow/Groupware: Microsoft Sharepoint Services 3.0, TeamLab, TRAC, ALFRESCO
- Réseaux : VIP(F5), VPN, DNS, TelcoBridges, SMPP,Diameter, SS7,VOIP
- Web : Web services (WSDL, SOAP, and SOA)
- SMS : Kannel, JasminSMS
- Deploiement : Docker, Ansible, shell
- Supervision : Zabbix, Cetreon, Nagios
- Telco : ZigBee, Xbee
- VOIP: CosmoCom, Asterisk

LANGUES

Anglais : courant

CONTACT

Pierre Muchart
Tilencia
06 89 47 83 80
pierre@tilencia.com

EXPÉRIENCES

Société :

AMERSPORTS

04/2024 à ce jour

Poste :

Responsable du programme gestion de vulnérabilités

Environnement technique :

OPEN VAS, QUALYS, QUALYS AGENT, ACUNETIX, BITSIGHT, IPM, NESSUS, CLOUD ALI, EDR, EPSS, POWER BI

Missions réalisées

Projets :

- Étude et déploiement d'un scanner de vulnérabilités pour les environnements Cloud et On-Premise, garantissant une couverture complète des surfaces d'attaque.
- Élaboration d'un processus global et transverse de gestion des vulnérabilités, optimisant la détection et le suivi de la remédiation.
- Déploiement de l'agent Rapid7, assurant une surveillance continue et automatisée des vulnérabilités.
- Implémentation des tags d'assets (Marque, Exposition, Criticité métier), facilitant une priorisation intelligente des risques et l'identification des porteurs des actions.
- Développement de rapports et KPI pour un suivi détaillé des risques et de la mesure de la capacité à faire.
- Intégration de Defect Dojo à l'écosystème et à la stack de sécurité du groupe, améliorant la gestion des vulnérabilités et des correctifs.

Tâches:

- Mise place du process de gestion de vulnérabilité transverse
- Élaborer un plan d'action pour optimiser les activités LOA/BAU.
- Rédaction des rapports mensuels sur les vulnérabilités : analyse des tendances, des performances de remédiation, et priorisation des risques pour chaque marque du groupe.
- Animation des comités de suivi de la remédiation, en coordonnant les équipes techniques et métiers des différentes marques pour assurer le respect des SLAs.
- Collaborer avec l'équipe projet et les autres parties prenantes nécessitant les capacités de l'équipe de gestion des vulnérabilités.
- Accompagnement et support des équipes de sécurité des marques dans la gestion des vulnérabilités.
- Définition des rôles et responsabilités du poste "Vulnerability Champion", et gestion du processus de candidature pour chaque marque et nomination des référents.
- Suivi et monitoring des performances de remédiation des différentes marques, avec des revues régulières des progrès et des indicateurs de performance.
- Restitution des rapports et KPIs aux instances de direction, lors des comités de suivi, avec des recommandations pour renforcer la posture.
- Agir en tant que conseiller lors de prises de décisions techniques.
- Piloter la phase technique et les opérations de tests.

Société :

Poste :

Environnement technique

Missions réalisées

- Conduite du POC (Proof of Concept) des alertes et veille sécurité avec VOC FORMIND, afin de valider l'efficacité du dispositif d'alerte et d'ajuster les processus de réponse.
- Analyser et améliorer les processus ITSM.
- Suivi de l'ingestion et de l'agrégation des sources de vulnérabilités dans un Data Lake, garantissant la centralisation des données pour une meilleure analyse et gestion des risques.
- Intégration des inventaires INFRA et cloud au scanner OPEN VAS, améliorant ainsi la couverture des analyses de sécurité et réduisant les angles morts dans l'infrastructure.
- Documentation opérationnelle pour la mise en production.
- Livraison du backlog produit associé.
- Communication de l'avancement aux équipes Cyberdéfense.
- Reporting auprès du Product Manager avant les comités de pilotage (SteerCo).
- Rapports avec suivi des SLA renforcés pour l'ITSM.
- Documentation des plans d'amélioration

SAINT-GOBAIN

09/2023 à 03/2024

Responsable du programme de gestion de vulnérabilité

VULCAN, QUALYS, KNIME, Security Score Card, CrowdStrike, CERT-IST, EPSS, CISA , POWER BI, Haquity, Vulcan, CISCO KENNA, EPSS, Pentest, Projets

- Déploiement d'un agrégateur de différentes sources de vulnérabilités
- Process Global et auxiliaire (Exceptions, Faux positifs, Task Force) de la Gestion des vulnérabilités.
- Déploiement de l'agent Qualys.
- Implémentation des scans WAS (QUALYS WEB) de surface et authentifiés.
- Définition et généralisation des Tags de contexte sur Qualys.
- Ingestion des vulnérabilités (DATA LAKE) et leur corrélation avec les données de la CMDB.
- Security Tower : Interface web de visualisation et pilotage de la vulnérabilité à l'échelle du groupe.
- Reporting & Indicateurs relatifs à la mesure de la remédiation.
- Risk Score Calculation (Process, Prérequis, développement et POC)

Tâches:

- Rédaction des documents des process de gestion des vulnérabilités.
- Animation du COPIL mensuel.
- Conduite du process de gestion des Faux positifs et leur status sur le scanner.
- Suivi et monitoring des performances de remédiation des différentes entités techniques.

- Arbitrage au sujet des exceptions et le suivis de leurs délais d'expiration.
- Rédaction des spécification fonctionnelles et techniques d'un outil web de pilotage de la vulnérabilité.
- Gestion des scans des vulnérabilité (Planification, surface, output).
- Homogénéisation des sources des vulnérabilités et leur ingestion dans un Data Lake.
- Administration des scanners de vulnérabilités et leur optimisation.
- Etablissement d'un comparatif des consoles de gestions de vulnérabilités du marché.
- Définition et récupération des informations de contexte des assets INFRA et applications WEB.
- Restitution de KPIs et indicateurs aux équipes SOC, CISO et INFRA.
- Etablissement des mécanismes d'attribution des vulnérabilités et leur distribution.
- Intégration des outils ITSM au process de gestion de la remédiation.
- Suivi des backlogs des différentes entités et l'avancement des travaux de remédiation

Société :

VINCI AUTOROUTES

12/2022 à 08/2023

Poste :

Référent sécurité

Environnement technique :

OPEN VAS, QUALYS, QUALYS AGENT, ACUNETIX, BITSIGHT, IPM, NESSUS, CLOUD ALI, EDR, EPSS, POWER BI

Missions réalisées

Projets :

- Projet Console Transverse de Gestion des vulnérabilités Traverse VA (VULCAN).
- Initialisation de la Veille des vulnérabilités sur la base de la note du CERT-IST.
- Etablissement du process de la gestion de la vulnérabilité pour les différentes entités VA.
- Build de la stack Gestion de la vulnérabilité pour les différentes entités VA (COF/ESC/ASF)
- Mise en place et Suivi des MCC PCI DSS.
- Suivi et Build de la stack MCS.

Tâches :

- Accompagnement en tant que spécialiste SSI sur les projets groupe.
- Évaluation de la conformité des projets par rapport aux exigences de sécurité identifiées.
- Définir et suivre l'avancement des plans projets pour les travaux de mise en conformité et l'application des éventuelles mesures correctives.

- RUN de Veille de la gestion de vulnérabilité en transverse.
- Rédaction des processus de remédiation des vulnérabilités dans le cadre de la gouvernance SSI.
- Pilotage des atelier de remédiation sur les périmètres sensibles (LPM, PCI DSS)
- Accompagnement à la remédiation des différentes vulnérabilités
- Mise en place et pilotage des scanners de vulnérabilités.
- Etude et construction de la stack de gestion des vulnérabilités :
Scanners (Rapid7, Qualys, Nexxus)
Sondes.
CMDB (GLPI, NETBOX,...)
Puits de données.
- Étude et réduction de risque sur les environnements à contraintes obsoletes, absence de patch,..)
- Conduite de comités de sécurité opérationnelle.
- Contrôle de conformité des INFRAs assujétis aux audits de sécurité

Société :

CREDIT AGRICOLE

08/2021 à 12/2022

Poste :

Chef de projet transverse

Environnement technique :

TENABLE, SATELLITE, SCCM, POWER BI (Offre GOZEN), INFRA SoCloud (CAGIP), ORACLE, SQL, MYSQL, ZABIX, SOPHOS, DEFENDER, REDHAT, AIX, VMWARE

Missions réalisées

Projets

- VULCAIN 1&2 Suivi est remédiation des vulnérabilités des INFRAs du SOCLE OPEN.
- Automatisation des Indicateurs de Sécurité Opérationnelle.
- Migrations des consoles Antivirus (Sophos, Semantec, Defender).
- Migrations des Consoles d'administration SATELLITE & SCCM.

Tâches :

- Planification et Animation des différents comités de sécurité opérationnelle au sein de CAGIP :
- Elaboration / Restitution des KPI de sécurité : Patch management (Win, UNIX, LIN, AIX, CITRIX, VMWare, BDD, MWR, etc). Lutte Antivirale. Hardening (Win, LNX).
- Vulnérabilités (INFRA, Réseau, MiddleWare, BDD, SOCLE, etc).
- Mise en place et amélioration des processus de remédiation des vulnérabilités.
- Expertise sur le contrôle de conformité des INFRAs CAGIP (Patch management, Lutte Antivirale, Hardening, Vulnérabilités, Incidents SOC, Audits, Contrôles permanents)
- Planification des scans des vulnérabilités dans le parc.
- Définition des plugins et périmètre des scans des vulnérabilités.
- Expertise sur les moyens de remédiation des vulnérabilités.
 - Implémentation de dashboard et d'interfaces de reporting / management de la sécurité.

- Limitation des risques sur les vulnérabilités à plan de remédiation dérogées
- Pilotage des cellules de crises des vulnérabilités à haut risques / urgentes.
- Interprétation et qualification des résultats d'audits de sécurité.
- Coordination et Suivi de la planification du patch management.

Société :

GRDF

11/2019 à 08/2021

Poste :

Référent technique

Environnement technique :

F5, NAS Hitashi/NetApp, Linux RHL, Windows Server, Java, VmWare, F5, Apache, MySQL, VIP, SuperCluster Oracle, Tomcat. APN Mobile, Transmission Radio, Chaîne Communicante, ELK, Compteur connecté.

Missions réalisées

Projet

Extension des infras du projet du compteur connecté GazPar

- Migration des shares NAS Hitashi vers NeTApp
- Généralisation l'Espace de travail Saturne (Windows).
- Patching SuperCluster Oracle.
- Patching Windows Server suivant les préconisations du RSSI.
- Sécurisation des VIP (internes et externes).
- Upgrade des Serveurs RedHat.
- Chaîne communicante et des relevés de comptage.
- Dashboard ELK.

Tâches :

- La coordination transverse entre les différentes parties prenantes et intervenants du projet "GasPar".
- L'appréhension des concepts techniques infra, réseaux et applications.
- Relecture / Validation des EB infra (VIP, DNS, NAS, VM, Backup, Supervision)
- Suivi et vérification de l'application des changements émis aux exploitants.
- La native réflexion de challenger les fournisseurs et intervenants sur leurs livrables.
- Participer aux comités du comité de changements transverses.
- Assurer un bon niveau de communication et de relationnel avec les différentes vis à vis.
- Participer à faire évoluer le projet dans la durée.
- Pilotage du traitement des non-conformités.
- Définition de la stratégie de traitement des écarts ainsi que les priorités de traitement.
- Encadrement technique des collaborateurs au sein de l'équipe.
- Validation des données d'entrée permettant le traitement des évolutions et des demandes de changement.
- Vérification et approbation des avis techniques rédigés par les architectes SI.

Société :

Poste :

Environnement technique :
Missions réalisées

- Assurer l'interface entre le client, les ingénieries et les architectes.
- Participer aux réunions d'avancement, workshops, PRA.
- Suivi de la disponibilité des environnements.
- Supervision de la télé relève.

BNP PARIBAS

11/2019 à 08/2021

Chef de projet technique

Linux, Oracle, Java, VmWare, HA, F5, Apache, MySQL, TAGETIK, Jira
Projets

- Création d'espaces privés sur TAGETIK, permettant de refondre aux besoins des métiers bancaires IRB et LS en matière de consolidation des flux des données budgétaires de façon intégrée et l'harmonisation des concepts et principes budgétaires sur les espaces privés et avec le Groupe.
- Mise en conformité des EPs Groupe et FORTIS sur le plan architectural afin de les aligner aux mises à jour des normes de sécurité et architecture.

Tâches :

- Élaboration du plan de déploiement conjointement avec la MOA et le programme.
- Préparation des comités et étude des phases du projet : Initialisation, Validation, Construction, Transition.
- Rédaction des documents projet : DUP, fiche navette, dossier économique, Expression du besoin, Macro planning.
- Étude et expression de risques.
- Transition des plans d'action en cas de risque et gérer son acceptation par les parties prenantes.
- Initiation et suivi des trains au sein de la direction des projets ITG finance en fonction du processus établi par le programme.
- Étude de l'architecture en collaboration avec les différents intervenants.
- Organisation et animation des ateliers fonctionnels.
- Spécification des flux et modèles de données avec la MOA et les BA impliqués.
- Création et suivi des demandes de création d'infra et flux réseaux.
- Construction des environnements bac à sable, développement, recette, prod et pre prod.
- Validation et recette des environnements
- Planifier et animer les séances de recette, acceptation
- Cadrement des tests de charge et suivi des séances de tests.
- Suivi et gestion des incidents en mode projet

Société :

MARABOUT TECHNOLOGY

12/2017 à 06/2019

Poste :

Chef de projet technique

Environnement technique :

Ms Project, MindManager, Bitrix, Slack, Appear.in, JIRA, Linux, Aix, Ubuntu, Ansible, Tomcat, QT, Node JS, Angular JS, Altium, Eagle, MS DYNAMICS CRM, Jira, java, python

Missions réalisées

Projets

- Déploiement et intégration d'une solution de suivi de production I4.0
- Conception d'un WorkFlow de suivi de productivité industrielle par agent/machine/chaîne/produit
- Mise en place de POCs et Demo sur les sites clients (industrie textile: Hugo Boss, Busche, EfQa)
- Application Mobile d'Audit industriel : GUEMBA WALK
- Design et Coodination de developpement d'ERP industriel à base de technologies WEB.

Missions

- Coordonner les travaux de travaux de recherche en électronique et IT.
- Recevoir et qualifier l'expression des besoins clients .
- L'étude et l'analyse de la faisabilité du projet .
- Suivi des déploiements .
- Encadrer et manager des équipes .
- Assurer la relation avec les clients pour définir les données d'entrée.
- Suivre et piloter les tâches de la phase de conception à la phase de déploiement.
- Piloter et suivre des différentes parties prenantes.
- Rédiger les différents livrables du projet.
- Communiquer avec les différentes parties prenantes des projets.
- Assurer le suivi et le pilotage des différentes actions du projet.
- Veille technologique des plateformes en cours d'exploitation.
- Vérification de la qualité de l'ensemble des livrables

Société :

ORANGE TUNISIE

12/2017 à 06/2019

Poste :

Chef de projet technique

Environnement technique :

CCU 6/7, MS DYNAMICS CRM, MS Windows 2008R2, MS SQL Server 2008, ORACLE, MS Active directory 2003, F5: Big IP, Fax: ZetaFax, VMWare :Esxi, Supervision /CR Management : HPSM, Protocoles SIP/IMS, RTP, TCP/IP, SNMP, systèmes Linux, Windows, Solaris, Ms Project, MindManager, CosmoComWebadmin, CosmoDesigner, Jira

Missions réalisées

Projet

- Upgrade/ Migration /Gestion de Changements CRM MS DYNAMICS
- Exploitation/ Support de la Plateforme Call Center Cosmocom
- Exploitation / Monitoring / Support/ Upgrade Cisco Call Manager
- Maintenance évolutive et continue Gateways IPNX
- HPSM Monitoring et supervision

- **Deploiement / Exploitation / Support Fax2Mail ZetaFax**

Missions

- **Coordonner les travaux**
- **Conception et chiffrage des besoins Métier**
- **Développement du projet CRM**
- **Tests d'intégration**
- **Livraison en environnements Intégration, UAT**
- **Assistance à la recette MOE et Métier**
- **Assistance mise en pré-production et production**
- **Accompagnement et échanges avec différents départements de l'entreprise.**
- **Etudes / Recueils de besoins avec les métiers**
- **Estimation de charges et planification des ressources**
- **Rédaction de spécifications techniques et fonctionnelle**
- **Encadrement des équipes de développements internes et externes (pilotage fournisseur) sur la maintenance évolutive / corrective**
- **Planification, Suivi budget / qualité**
- **Suivi de l'avancement des projets de migration**
- **Gestion des changements**
- **Rédaction des modes opératoires et des procédures d'exploitation**

Société :

STREAMWIDE

05/2012 à 06/2015

Poste :

Chef de projet technique

Environnement technique :

Linux RedHat, Debian, VMWare, VPN : Cisco, Ramses, IN Huawei, IN Ericsson, SCAP V1, 3gpp, diameter, SMS Huawei, VMS, VVM, VVG, MCA/RA Streamwide, Environment Mobile RIM/iOS/Android, F5: Big IP, Huawei Blades
infra, Switchs Cisco Catalyst Dell PowerEdge, Firewall : Sophos, PfSense, Supervision : Nagios, Centreon, Backup: BackupPC, HA : Corosync, Drbd, HA cluster, SMS : Kannel, JasminSMS, Protocoles SIP/IMS, RTP, TCP/IP, SNMP, SMPP, Asana, Slack, MS Project, WebtoProject

Missions réalisées

Projets :

- **Déploiement et intégration des plateformes VAS**
- **Gestion Développement Applications Mobiles Android, iOS et BlackBerry**
- **Gestion de Développement des Interfaces web de la VMS**
- **Messagerie vocale : Tunisie Telecom, AL MADAR, Orange TN, La Réunion, Mayotte**
- **Gateway Messagerie Visuelle et clients VVM Android, iOS et RIM : Tunisie Telecom, La Réunion, Mayotte**
- **Alerte de joignabilité et d'appels manqués : AL MADAR, Orange TN**
- **Filtrage et restriction d'appels : AL MADAR**
- **Mises à jour et extension des back ends opérateurs**

- Intégration avec CORE Mobile : SIP, SMPP, SCAP/3GPP, SNMP, SS7

Missions

- Superviser la conception de la solution la plus adaptée à la demande du client (CR)
- Suivi de l'avancement des projets et évaluation des risques et des enjeux
- Planification et suivi de l'avancement de l'intégration
- Animer, coordonner les réunions d'avancement (internes, comités projet), et en rendre compte
- Vérification de la qualité de l'ensemble des livrables
- Coordination des experts techniques, des partenaires et sous-traitants concourant à la solution
- Suivi de consommation des charges