Identity & Security Architect

Active Directory/Microsoft Entra ID (ex. Azure AD)

DOMAINE DE COMPÉTENCES

- Architecture**,** Conception, réalisation et mises en service d'infrastructure Active Directory 2012 à 2022
- Analyser et comprendre les besoins du client
- Migration Active Directory 2008 R2 → 2016/2019/2022 ; Migration Active Directory 2012 → 2019/2022
- Rationalisation de 2 forêts Active Directory ; Rationalisation 3 forêts Legacy en One AD, Move AD to Microsoft Entra ID (ex Azure ADà
- Suivre le projet de la réalisation jusqu'à la livraison (coordonner les intervenants, animer une équipe) en respectant les contraintes (budget, qualité, délais)
- Accompagner l'équipe N3 dans les changements techniques (réunions, supports de formation).
- Amélioration SI respect des niveaux de service (ITIL) / Méthodologie AGILE SCRUM /KanBan
- Élaboration et rédaction des procédures d'exploitation, DAT, DIT, DEX & FEX, HLD, LLD
- Réalisation des Projets ET MCO Infrastructure Systèmes N3-4
- Gestion des projets via la méthodologie AGILE : SCRUM MASTER
- Active Directory 2003 → 2022 CORE (+55 Forêts)
- Cloud Microsoft (Azure) ; Microsoft 365 Defender (Microsoft Defender for Identity (MDI, anciennement Azure ATP), Microsoft Defender for Cloud Apps (Anciennement Microsoft Cloud App Security), Microsoft Defender for Endpoint, Microsoft Defender for Office 365)
- AD FS 3.0/4.0 (Active Directory Federation Services) & +6 AD FS farms
- AD CS (Active Directory Certificate Services, Microsoft PKI)
- Architecture Windows Server de 2003 → 2022 Desktop & Core version
- Architecture Active Directory on-permise & Azure AD (**Microsoft Entra ID**)
- Azure ARC, Azure Monitoring Agent, On-Demand Assessment
- Architecture des plateformes Cloud : Office 365 & Azure & Cloud VPN Service & Azure vNet, NSG (Network Security Groups), Subscription, Role RBAC, Conditional Access policies, PIM (Privileged Identity Manager), MFA
- Scripting (Powershell 2.0 → 5.1, Batch)
- Identification & résolution des incidents complexe : Troubleshooting avancées
- Gestion de parcs Informatique (plus que 20000 serveurs)
- Migration des serveurs au Cloud AWS/AZURE
- Administration des plateformes de Virtualisation Hyper-V R2, VMware 4.0 → 6.5
- Architecture & Implémentation & Administration de SPLUNK/SENTINEL/ELK Security/Wazuh/Tenable.AD (ex Alsid)
- Security Audit, Remediation & Hardening : PingCaslte, PupleKnight, Forest Druid AD, Bloodhound, Rapid7
- Tiering Model (Tier 1, Tier 2, Tier 3), Zero Trust Appoach, MS Security Baseline, PAW

COMPÉTENCES TECHNIQUES

- **Microsoft:** Windows Server 2003/2008/2012 R2/2016/2019/2022 CORE, AD, Replication inter-DC, DNS, DHCP, DFS, PowerShell, WDS, ADMT 3.2; Office 365, Azure AD, Azure AD Connect, Azure, AD FS 3.0 / 4.0 ; SAML 2.0, WS-Federation & OAuth 2.0 ; MFA (Multi-factor Authentication) ; AD FS Rapid Restore
- **Messagerie :** Exchange 2010/2013/2016/2019 & Exchange Online
- **Base de données :** SQL Server 2008/2012/2014/2016/2019
- **Sécurité :** Firewall Fortigate, Symantec Endpoint Security v12, Trend Micro 10.6, MS Intune Endpoint Protection, SPLUNK, Evidian, PKI (Active Directory Certificate Services)
- **Virtualisation :** VMware 4/5/5.5/6.5, Hyper-v 2016/2019/2022

- **Scripting :** Batch, Powershell 3/4/5, Azure Cloud Shell
- **Cloud :** Azure, Microsoft 365 Defender (Microsoft Defender for Identity (MDI, anciennement Azure ATP), Microsoft Defender for Cloud Apps (Anciennement Microsoft Cloud App Security), Microsoft Defender for Endpoint, Microsoft Defender for Office 365)
- **Patch Management :** Microsoft Intune, WSUS
- **Scripting : PowerShell v5**
- **SIEM :** SENTINEL, SPLUNK, ELK Security, WAZUH

CERTICICATIONS

- **M**icrosoft **C**ertified **T**echnology **S**pecialist (**MCTS**): **Administering and Deploying System Center 2012 Configuration Manager R2 SP1**
- **M**icrosoft **C**ertified **S**olutions **A**ssociate (**MCSA**) : **Office 365**
- **M**icrosoft **C**ertified **S**pecialist (**MCS**) : **Implementing Microsoft Azure Infrastructure Solutions**
- **M**icrosoft **C**ertified **P**rofessional **(MCP): Cloud Services**
- **M**icrosoft **C**ertified **S**pecialist (**MCS**): **Server Virtualization with Hyper-V and System Center 2012 R2**
- **M**icrosoft **C**ertified **P**rofessional **(MCP): Virtualization Hyper-V & System Center**
- **FCNSA** – **F**ortinet **C**ertified **N**etwork **S**ecurity **A**dministrator
- **FCNSP**– **F**ortinet **C**ertified **N**etwork **S**ecurity **P**rofessional
- **VSP5**- **V**Mware **S**ales **P**rofessional ET **VTSP5**- **V**Mware **T**echnical **S**ales **P**rofessional)
- **VMSP**- **V**eea**M** **S**ales **P**rofessional ET **VMTSP**- **V**eea**M** **T**echnical **S**ales **P**rofessional)
- Formation professionnel Microsoft : **Course 10136A** - **C**onfiguration, **G**estion et **M**aintenance des **S**erveurs **W**indows **S**erver **2008**
- Formation Agile : Les fondamentaux de la méthode **Agile SCRUM**
- **Formation Gestion de projet sur Udemy**
- **Formation Windows PowerShell 5.1 avancée sur Udemy**
- **Formation Hacking Ethique – Cyber Sécurité sur Udemy**
- **Microsoft Certified : Microsoft Azure Fundamentals (AZ-900)**
- **Microsoft Certified : Microsoft Azure Security Technologies (AZ-500)**

FORMATIONS

- **Juin-2011 :** Diplôme d'**Ingénieur en TELECOMMUNICATIONS ENIT** (**E**cole **N**ationale d'**I**ngénieurs de **T**unis)
  Option **Systèmes / Sécurité / Réseaux**
  Projet de fin d'études réussi avec mention **Très bien**
- **Juin-2008 :** Diplôme des Etudes Universitaires Premier Cycle (**Cycle Préparatoire** Math-Physique)
  IPEIM (Institut **P**réparatoire aux **E**tudes d'**I**ngénieurs de **M**onastir - Tunisie**)**
- **Juin-2006 :** Baccalauréat **Mathématiques** (Mention **Bien**) – Lycée Raccada Kairouan – Tunisie.

LANGUES

- **Français :** Courant
- **Anglais :** Courant
- **Arabe :** Maternelle

EXPÉRIENCE PROFESSIONNELLE

Novembre 2021 jusqu'à Aujourd'hui :

Architecte Identité et Sécurité _ L'Oréal

- **Mission :** Conception des d'architectures techniques, rédaction des documents technique (HLD, LLD, Procédure, RunBook, etc…), élaborer et suivre des roadmaps techniques, réaliser des impacts techniques et des analyse de risque, des POC (Preuve de Concept), Assurer une veille technologique et de proposer des solutions innovantes porteuses de valeur aux métiers, conseiller et d'assurer le support de niveau 4 sur les architectures techniques et accompagner le niveau 3 en INDE chez Accenture, la mise en place de processus, la gestion de projets techniques, l'analyse des besoins, Automatisation : développer des scripts PowerShell (Backup Reporting, Backup Encryption and Export, GPO Import, Fix-Bad-Owners sur les Objets AD, Create gMSA automatically, Check needed TCP ports, Active Directory Health Check, DNS Backup/Restore, GPO Base line deploiment…etc)
- **Réalisation :** Projet de Conception et Implémentation de Ms Defender for Identity (HLD/Runbook…etc) et déploiement et Analyse des alertes ; Projet de migration Active Directory 2012 to 2019 ; Projet de sécurisation Active Directory (Tiering Model, audit et remédiation des vulnérabilité selon les points de contrôles ANSSI, Delegation Model, Raise Functional Level),
- **Technologies** : Active Directory 2012 > Active Directory 2019 Desktop ;Azure; Azure AD , ADFS 4.0; WAP; Intune, AIP; Azure ATP (Microsoft Defender For Identity) ; WSUS ; GPO ; Sentinel, Logs analytics, Alsid; PingCastle ;Trimark, Tenable.ad, Tenable.sc ;
- **Références :** L'Oréal

Novembre 2019 jusqu'à Novembre 2021 (2 ans) :

Architecte Active Directory et Azure / Chef de projet Technique _ EDF

- **Mission :** Conception des d'architectures techniques, produire et présenter les dossiers d'architecture technique dans les instances de gouvernance interne (CATE), réaliser des analyses de risque, réaliser de l'enregistrement RGPD, élaborer et suivre des roadmaps techniques, réaliser des impacts techniques, des POC (Preuve de Concept), Assurer une veille technologique et de proposer des solutions innovantes porteuses de valeur aux métiers, conseiller et d'assurer le support de niveau 4 sur les architectures techniques et accompagner le niveau 3, la mise en place de processus, la gestion de projets techniques, l'analyse des besoins, développer des scripts PowerShell (Backup Reporting, Backup Encryption and Export, GPO Import, Fix-Bad-Owners sur les Objets AD…etc)
- **Réalisation :** Projet de Conception et Implémentation d'une infrastructure Active Directory d'authentification et d'habilitation dédié au Bastion (CyberArk) dans le cadre de projet GAP (Gestion de accès à privilèges) ; Projet de refonte et évolution technique de l'infrastructure Active Directory Bureautique et Applicatif ainsi que l'infrastructure ADFS 4.0 ; Projet d'étude et d'implémentation de la solution Cloud-Based Microsoft Defender For Identity ; Projet de durcissement de la forêt bureautique
- **Technologies** : Active Directory 2012 > Active Directory 2019 CORE ;Azure; Azure AD , ADFS 4.0; WAP; Intune, AIP; Azure ATP (Microsoft Defender For Identity) ; RedForest ; WSUS ; GPO ; GateWay SCOM; Alsid; PingCastle ;Trimark ;
- **Références :** EDF

Juin 2018 jusqu'à Novembre 2019 (1 an & 6 mois) :

Ingénieur Expert Identity Management & AGILE SCRUM MASTER – SOCIETE GENERALE

- **Mission :** Support d'Expertise N3, gestion d'incidents et demandes complexe, Réalisation des Changes (Changement), administration (Windows Servers 2008/2012 R2/Windows 2016, 55 forêts, Etude, implémentation des projets (migration AD, Windows Backup, etc…), réalisation des procédures technique, DAT, DIT, DEX, FEX ; Optimisation de l'Infrastructure Microsoft via des scripts PowerShell, Maintien en condition opérationnel de l'infrastructure Active Directory, ADFS, Office365, PKI…etc.
- **Technologies** : Active Directory de 2008 à 2016 et protocoles d'authentification (Kerberos, NTLM, ...);Active Directory Federation Services (ADFS 3.0); Protocole SAML 2.0, WS-Federation & OAuth 2.0 ; Windows Server de 2008 à 2016 ; Scripting Powershell v 5.1; Microsoft Office365, Azure AD Connect; Microsoft PKI (Public Key Infrastructure); Evidian Entreprise SSO; Microsoft SQL, SCOM; Active Directory Lightweight Directory Services; Quest GPO ADMIN; Quest ChangeAuditor; Analyse/compréhension des logs sécurité sur les technologies du périmètre; Gestion des priorités, autonomie dans le troubleshooting; Connaissance des principes de détection/intrusion, sensibilisation aux risques/menaces; Veille technologique sur la sécurité; Méthodologie Agile SCRUM; Change Manager BACKUP; Scrum Master Identity Management & Data Management
- **Références :** Société Générale

Septembre 2016 jusqu'à MAI 2018 (1 an & 9 mois) :

Ingénieur Consultant Infrastructure – ENEDIS (ex ERDF)

- **Mission :** Support d'Expertise N3, gestion d'incidents et demandes complexe, Réalisation des MEP (Mise En Production et Changement), administration (Windows Servers 2012 R2, 3 forêts avec 15 DC/forêt, 40 Clusters vSphere Server v6 Update 2), Etude, implémentation des projets (migration AD, WSUS, AUDIT Sécurité ANSSI), réalisation des procédures technique, DAT, DIT, DEX, FEX ; Optimisation de l'Infrastructure Microsoft via des scripts PowerShell, Maintien en condition opérationnel de l'infrastructure
- **Technologies** : les systèmes d'exploitation 2003/2008 R2/2012 R2 (Active directory, services réseau, GPO, DHCP, DNS, DFS-N, DFS-R, ADMT 3.2…), les technologies de déploiement, gestion et automatisation HPE Server Automation (HPESA), le Scripting (PowerShell, batch), Virtualisation VMware 6 update 2 (plus que 7000 VM), WSUS, Antivirus Symantec Endpoint Protection, Cluster Windows, Linux (Redhat release 5/6/7), AIX 6/7
- **Projets** : Migration AD Windows 2008 R2 Server ➔ Windows 2012 R2 Server (Changement de nom DNS inclus)
- **Références :** ENEDIS (ex ERDF)

Aout 2014 jusqu'à Août 2016 (2 ans) :

Ingénieur Systèmes & Réseaux – Les Cinémas Gaumont Pathé, Secours-Catholique, LFB, Dirickx Group, XPO Logistics Europe

- **Mission :** Support d'Expertise N2-3, gestion d'incidents complexe, administration (Windows Servers 2012 R2, 4 DC, Cluster Hyper-V 2012 R2, Supervision PRTG Network & Nagios, Sauvegarde Acronis, Sauvegarde sur Cloud Amazon AWS S3 via SynCovery Pro, Azure AD Connect, Yammer Sync, OFFICE 365, plateforme Azure, ADFS, WAP, Azure VPN, Azure VNet, gestion du par via SCCM, Microsoft Intune, 70 NAS QNAP des cinémas), Etude, implémentation des projets, réalisation des procédures technique, DAT, DIT, DEX ;Optimisation de l'Infrastructure Microsoft via des scripts PowerShell, Météo, administration (Landesk 9.6 SP2, Symantec Endpoint Security v12.1)
- **Technologies** : les systèmes d'exploitation Windows XP/Vista/Seven/Eight/2003/2008/2012 (Active directory, services réseau, GPO, DHCP, DNS, …), les technologies de déploiement (SMS, SCCM, Landesk), le Scripting (PowerShell, batch), Virtualisation (VMware 5.0 & Hyper-V 2012 R2), Sauvegarde (HP Data Protector, Acronis, Syncovery Pro), supervision (Nagios, Whats'up Gold, PRTG Network), WSUS, Microsoft Intune, Antivirus (Trend Micro, Symantec Endpoint Protection), Firewall (Fortigate 100d), Office365, Cloud Microsoft Azure, Stockage (NAS (Synology, QNAP), SAN (HP 3Par), HP LTO 3), Cluster Windows
- **Références :** Les Cinémas Gaumont Pathé, Secours-Catholique, LFB, Dirickx Group, XPO Logistics Europe

Aout 2012 jusqu'à Aout 2014 (2 ans) :

Ingénieur Support (CA Technologies) – Help-Line Tunisia

- En charge du support technique pour tout le marché francophone d'un des grands éditeurs de logiciels américains (CA Technologies) autour de la sauvegarde et de la réplication des infrastructures réseaux. J'interviens en tant qu'expert technique auprès d'Ingénieurs systèmes & réseaux, responsables informatiques, chefs de projet, consultants, ...

Janvier jusqu'à Juin 2013 (Projet en Freelance : 6 mois) :

IT Consultant Freelance – Just WebDesign - Italie

- Intervenir dans les projets IT associés à WebDesign en Italie : Etude du projet, Analyse des besoins, mise en place (via des sessions à distance TeamViewer/VPN) des projets IT, documentation suite à chaque mission accompli, Résolution des problèmes d'IT chez les clients, Conseils concernant la stratégie IT d'une entreprise, Intégration de systèmes.

Août 2011 jusqu'à Aout 2012 (1 an):

Ingénieur Réseaux et Systèmes – Gérance Informatique

- Installation et administration des serveurs physiques et des serveurs (contrôleur de domaine, fichiers, applications, DHCP, DNS, Hyper-V, VMware (ESX, View, vSphere, vCenter), proxy, vpn, Veeam, Splunk, Exchange server 2003/2007/2010, ESET NOD32, SolarWinds, SQL Server)
- Mise en place de la sécurité des réseaux (Firewall, ISA Server 2004, GFI WebMonitor, Cryptages, chiffrement…)
- Installation ET administration Windows server (2000, 2003, 2008, 2008 R2), Small Business Server 2003 Windows (XP/Vista/Seven), Linux (Ubuntu, Debian, Mandriva, Fedora)
- Sauvegarde et archivage (NAS, SAN, DAS), ShadowProtect
- Mise en place et suivi des back-ups
- Monitoring et Audit Réseaux (GFI LanGuard, Nmap, Nessus, SolarWinds)

- Rédaction de nombreuses documentations techniques et procédures et rapports du travail, présentation des produits chez nos clients.

Janvier 2011 jusqu'à Aout 2011 (7 mois):

Ingénieur Systèmes, Réseaux et Sécurité – Sagemcom

- Administrer et exploiter des plate-formes Cloud en production
- Configurer des serveurs, des firewalls, des switches/des routeurs
- Diagnostiquer et résoudre des incidents de niveau 3 (tickets)
- Superviser et sécuriser des infrastructures
- Analyser des performances systèmes et réseaux