

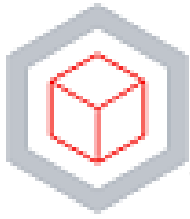
## MSO

### EXPERT SECURITE & ARCHITECTURE (SI, CLOUD AZURE & GOUVERNANCE) (15 ANS XP)

#### DOMAINES DE COMPETENCES

Architectures :	<ul style="list-style-type: none"><li>• Cloud Azure (IAAS, PAAS)</li><li>• CORBA</li></ul>	<ul style="list-style-type: none"><li>• DOCKER</li><li>• Distributed systems</li></ul>
Sécurité :	<ul style="list-style-type: none"><li>• CSPM</li><li>• CASB</li><li>• Pentesting</li><li>• Hardening</li><li>• Scapy</li><li>• Burp Suite</li><li>• IRMA</li><li>• Whireshark</li><li>• JTR</li><li>• THC Hydra</li><li>• Kismet</li></ul>	<ul style="list-style-type: none"><li>• Metasploit</li><li>• Backtrack</li><li>• Kali Linux</li><li>• Nmap</li><li>• Aircrack-ng</li><li>• Paros</li><li>• Nessus</li><li>• Snort</li><li>• Netcat</li><li>• Colasoft</li></ul>
Supervision :	<ul style="list-style-type: none"><li>• Zabbix</li><li>• Nagios</li><li>• Hyperic</li><li>• BigBen</li><li>• Centreon</li><li>• HP-OV</li></ul>	<ul style="list-style-type: none"><li>• HP Network Node Manager</li><li>• TCM</li><li>• Kibana</li><li>• Grafana</li><li>• Prometheus</li><li>• Asemon</li></ul>
Big Data :	<ul style="list-style-type: none"><li>• Hadoop clustering</li><li>• Mesos-Marathon</li><li>• Hbase</li><li>• Elasticsearch</li></ul>	<ul style="list-style-type: none"><li>• Apache Spark</li><li>• Infinispan</li><li>• Teiid</li><li>• Datamining</li><li>• Drill</li></ul>
Cloud :	<ul style="list-style-type: none"><li>• Microsoft Azure</li><li>• Azure AD</li></ul>	<ul style="list-style-type: none"><li>• Azure Sentinel</li><li>• Cloud Control</li></ul>

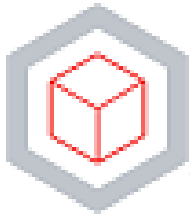




# TEASERPUB

	<ul style="list-style-type: none"> <li>• PIM</li> <li>• Azure Access</li> </ul>	<ul style="list-style-type: none"> <li>• IAAS PAAS Hardening</li> <li>• Azure Security</li> </ul>
Devops :	<ul style="list-style-type: none"> <li>• Chef</li> <li>• Consul</li> <li>• Jenkins</li> <li>• Confluence</li> </ul>	<ul style="list-style-type: none"> <li>• Gerrit</li> <li>• Git</li> <li>• XLDeploy</li> <li>• Jira</li> <li>• Logstash</li> </ul>
OS :	<ul style="list-style-type: none"> <li>• Unix (Solaris)</li> <li>• Linux (KALI, CentOS, RedHat, Debian)</li> </ul>	<ul style="list-style-type: none"> <li>• Windows</li> </ul>
Langages :	<ul style="list-style-type: none"> <li>• Script Shell</li> <li>• Power Shell</li> <li>• Javascript</li> </ul>	<ul style="list-style-type: none"> <li>• C</li> <li>• C++</li> <li>• DotNet</li> </ul>
Middleware	<ul style="list-style-type: none"> <li>• Apache</li> <li>• LDAP</li> </ul>	<ul style="list-style-type: none"> <li>• JBOSS</li> </ul>
Base de données	<ul style="list-style-type: none"> <li>• Oracle (8,9,10,11)</li> <li>• MySQL</li> <li>• MongoDB (NoSQL)</li> </ul>	<ul style="list-style-type: none"> <li>• Sybase (12,15)</li> <li>• SQLServer 2005</li> <li>• SQLite</li> </ul>
Ordonnanceurs	<ul style="list-style-type: none"> <li>• ControlM (V6, V7, V8)</li> </ul>	<ul style="list-style-type: none"> <li>• Autosys</li> </ul>
Flux	<ul style="list-style-type: none"> <li>• RabbitMQ</li> </ul>	<ul style="list-style-type: none"> <li>• CFT</li> </ul>
Outillages	<ul style="list-style-type: none"> <li>• ITOP</li> <li>• ITSM</li> <li>• Syslog</li> </ul>	<ul style="list-style-type: none"> <li>• BSD Jail</li> <li>• Consul</li> <li>• Silva</li> <li>• Confluence</li> </ul>
Appli.Bancaires	<ul style="list-style-type: none"> <li>• Summit</li> <li>• Infinity</li> <li>• KONDOR</li> <li>• Decalog</li> <li>• GP3</li> <li>• EAI STP</li> </ul>	<ul style="list-style-type: none"> <li>• ESPM</li> <li>• EFIRA STP</li> <li>• QlikView</li> <li>• BLOFI</li> <li>• LIQUID</li> </ul>
Normes	<ul style="list-style-type: none"> <li>• RGPD</li> <li>• ISO 27K</li> </ul>	<ul style="list-style-type: none"> <li>• PCI DSS V3</li> </ul>
Méthodes	<ul style="list-style-type: none"> <li>• ITIL V2 ET V3</li> </ul>	<ul style="list-style-type: none"> <li>• Agile et Lean Management</li> </ul>
Langues :	<ul style="list-style-type: none"> <li>• Français : Courant</li> </ul>	<ul style="list-style-type: none"> <li>• Anglais : Courant</li> </ul>





## ETUDES ET DIPLOMES

---

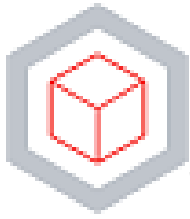
- **2020/En cours** : **CISSP** (Certified Information Systems Security Professional), **CCSP** (Certified Cloud Security Professional)
- **2018/2020** : **AZ-300 Architect, AZ-400 DevOps, AZ-500 Azure Security Technologies**
- **2016** : **Formation CEH** (Certified Ethical Hacker)
- **2015** : **Formation Lean Management**
- **2012** : **Formation Hyperic**
- **2011** : **Formation TCM** (Tivoli Control Manager)
- **2010** : **Formations ITIL V3 ControlM, Oracle 10g**
- **2009** : **Formation Solaris**
- **2008** : **Formation ITIL V2**
- **2004/2007** : **Diplôme d'ingénieur grande école en Informatique** (Spécialité : Génie Informatique : Mention Bien sur les 3 ans, Mention très bien en PFE)
- **2004** : **Licence en Math/Physique** (Moyenne générale en cycle préparatoire aux études de grandes écoles octroyant directement la Licence en Math/physique)
- **2004** : **Licence en Psychologie**

## COMPETENCES FONCTIONNELLES

---

- **Industrie** : Saint Gobain, Hewlett Packard, Sun Microsystem, Oracle, SAGEM Safran
- **Assurances** : AXA Assurance
- **Finance de marché** : CA-CIB, Natixis
- **Asset Management** : Covéa Finances
- **Web** : Criteo
- **Vente en ligne / téléphone** : (Confidentiel)
- **Moyens de paiement** : Transactis,
- **Télécoms** : SFR, British TelecomTélécom



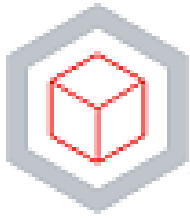


## DOMAINES D'INTERVENTIONS

---

- **Direction de projets techniques** : Direction de programmes de mise en conformité réglementaire, migrations, standardisation, uniformisation, planification, gestion de budget, de ressources, reporting management, garant des livrables.
- **Sécurisation des SI** : Audits, hardening, remédiation, mise en conformité (RGPD, PCI DSS, ISO 27k)
- **Architecture** : Production applicative et des infrastructures, optimisation de solutions, gestion PCA/PRA/DRP
- **Services & Processus** : Normes de production et de sécurité, élaboration de SLA et KPI, RACI d'exploitation, Processus ITIL
- **Documentation** : Dossiers d'architecture DAT, d'exploitation DEX, conventions de services, reporting, capacity planning, planification budgétaire
- **Optimisation de performances** : Industrialisation, automatisation de reporting et de supervision, amélioration continue et revue des standards
- **Support N3** : Gestion des incidents, investigations de résolutions, MEP correctives, suivi et gestion des changements
- **Mise en conformité** : Normes BDF, AMF et industrie Asset Management, Banque d'investissement, Moyens de paiement, industrie sensible et vitale





## EXPERIENCE PROFESSIONNELLE

---

### EXPERT EN SECURITE CLOUD, AXA ASSURANCE

➔ De novembre 2020 à ce jour

**Contexte :** Sécurisation & mise sous contrôle du Public Cloud AXA

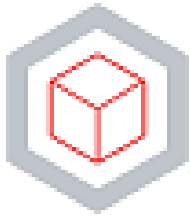
- Etablissement du modèle GRC (Gouvernance Risk Compliance) du Public Cloud AXA
- Réponse aux problématiques de sécurité remontée par l'internal audit
- Etablissement du Framework de Security Assurance Plan du Public Cloud
- Evaluation des procédures, mécanismes et outils de sécurité Azure
- Rédaction des politiques de sécurité Cloud (Policies/Controls) et des moyens de prévention, check et remédiation
- Identification des points faibles du cloud Azure chez AXA
- Conseil et orientation sur les moyens, process et technologies de sécurisation du cloud Azure
- Etablissement des plans de remédiation
- Management et suivi des résultats de remédiation
- Intégration de la sécurité dans le process de développement et de migration dans le cloud (Security By Design, Minimum Security Rules, Audit, Hardening, DevSecOps Process, SDLC Principles)
- Mise en place du plan de Service Enablement
- Optimisation de la base de risques et vulnérabilités du Public Cloud
- Définition des plans de backup, isolation et de fast recovery avec les équipes de résilience
- Définition des méthodologies et des solutions de sécurisation
- Benchmark et reporting des solutions de sécurisations (Palo Alto, McAfee, Scout-Suite from NCC Group...)
- Animation de Workshops Techniques
- Analyses de risques (STRIDE, NIST, EBIOS et 27005) + principes CSA (Cloud Security Alliance) + respect des normes DICT pour la classification des données (RGPD compliance) + OWASP
- Rédaction et revue de Documents d'architectures Techniques et d'Exploitation

### Environnement technique :

**Cloud Azure :** AzureAD, Sentinel, Powershell, Solutions O365, Solutions SAAS, PAAS, IAAS, Managed IAAS

**Network :** VPN/VPC, Firewalling, Routage, peering Cloud, matrices de flux





# TEASERPUB

**Sécurité** : CSPM, CASB, Cyberark, Cryptage, Chiffrement, Gestion des accès, Cloisonnement environnemental, KeyVault, OAuth2, SAML, Double authentification, clés RSA, Microsoft Authenticator, HSM, filtrage IP + toutes les solutions de sécurisation Azure (Security Center, Sentinel, MFA, PIM, Access Review, Threat Protection, Network Monitoring ...)

**Reporting** : PowerBI, Datalake,

**Systemes** : Windows

## EXPERT EN SECURITE CLOUD, SAINT GOBAIN

➡ De mars 2019 à aout 2020

**Contexte** : Sécurisation du projet de migration vers le Cloud Azure de l'ensemble des applications Saint Gobain internes et partenaires

- Définition de l'orientation du projet de sécurisation
- Définition des axes d'interventions
- Création des process de migration et des conditions d'acceptabilité
- Animation de workshops avec les intégrateurs Cloud de Saint Gobain (linkbynet, Claranet)
- Présentation et planification avec le Business de l'approche de sécurisation
- Intégration de la sécurité dans le process de migration (Security By Design, Minimum Security Rules, Audit, Hardening, DevSecOps Process)
- Revue et sécurisation des architectures d'accueil et applicatives Cloud
- Définition des méthodologies et des solutions de sécurisation
- Benchmark et reporting des solutions de sécurisations
- Animation de Workshops Techniques
- Analyses de risques (STRIDE, NIST, EBIOS et 27005) + principes CSA (Cloud Security Alliance) + respect des normes DICT pour la classification des données (RGPD compliance) + OWASP
- Rédaction et revue de Documents d'architectures Techniques et d'Exploitation
- Préparation et rédaction des PSAT
- Reporting Managérial au RSSI et DSI Saint Gobain

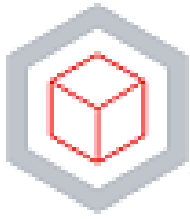
### Environnement technique :

**Cloud Azure** : AzureAD, Sentinel, Powershell, Solutions O365, Solutions SAAS, PAAS, IAAS

**Network** : VPN, Firewalling, routage, peering Cloud, matrices de flux

**Sécurité** : Cryptage, Chiffrement, Gestion des accès, Cloisonnement environnemental, KeyVault, OAuth2, SAML, Double authentification, clés RSA, Microsoft Authenticator, HSM, hardening de postes de travail, filtrage IP + toutes les solutions de sécurisation Azure. **Systemes** : Windows





**EXPERT EN SECURITE ET GOUVERNANCE PCI-DSS, TRANSACTIS**

➔ **De décembre 2018 à décembre 2019**

**Contexte :** Pilotage du projet de préparation du SI à la certification PCI-DSS et assistance au RSSI sur les préconisations du contrôle interne

- Analyses de risques sur les plateformes de moyens de paiement
- Animation de workshops techniques et fonctionnels sur l'intégration de la sécurité aux projets
- Audit des plateformes existantes
- Rédaction et contrôle des préconisations sécurité (avec l'assistance de l'auditeur Verizon)
- Reporting Managérial
- Analyse et mise à jour des process et de la politique de sécurité
- Analyse de sécurité sur les solutions et applications Cloud
- Rédaction de document d'architecture technique pour les besoins du contrôle interne
- Mise à jour des référentiels de sécurité (process et outillage)
- Rédaction de documents de réponse (Audit et preuves) aux contrôle interne
- Certification PA-DSS des applications
- Certification du Datacenter front office en PCI-DSS obtenue
- Optimisation des process internes de gestion des utilisateurs avec scripting et reporting
- Interventions sur les failles de sécurité en urgence (approche technique, implémentation déléguée)

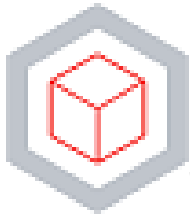
**Environnement technique :**

**Cloud Azure :** AzureAD, Solutions O365

**Sécurité :** Vérification et audit des règles PCI-DSS sur les plateformes moyens de paiement

**Systèmes :** Windows





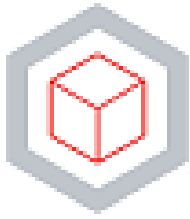
## EXPERT EN SECURITE ET GOUVERNANCE PCI-DSS, CLIENTS CONFIDENTIELS

### ➔ D'octobre 2015 à novembre 2018

- Assistance RSSI : Mise en place d'architecture et sécurisation de plateformes CLOUD pour la Finance de marché (Obligation de respect des normes réglementaires en vigueur)
- Auditeur au sein de l'inspection générale et du contrôle continu
- Analyse de sécurité sur la fraude (Moyens de paiement : Cartes bancaires, GAB/DAB ...)
- Pilotage des projets de certifications sécurité ISO27K, P2PE
- Audit et activation des protocoles de traitement sécurisés
- Rédaction des recommandations, accompagnement technique à la mise en place et aide directe à la revue des architectures en place
- Optimisation budgétaire avec analyse des différentes solutions de cloud hybride suivant les besoins
- Sécurisation des différentes plateformes et applications d'entreprises critiques, réglementaires et non réglementaires (Point de référence : BCE, BDF, AMF), des accès, des flux et des interfaces de communication
- Présentation du RGPD au Barreau de Paris en 2016 (Plus de 300 interlocuteurs et avocats experts en protection des données personnelles)
- Pilotage technique des projets de sécurisation RGPD:
  - Analyse de la méthodologie projet RGPD
  - Réflexion et rédaction de la méthodologie d'Audit technique
  - Collaboration à la revue technique du bouquin (Réussir votre mise en conformité GDPR : Guide pratique)
  - Mise en place des tests techniques et entretiens avec les consultants experts
  - Conseil des Directeurs de projets et Architectes auditeurs chez les clients
  - Rédaction des templates projet et techniques (DAT, DEX, Reporting)
  - Suivi des comités de direction et de livraison
  - Aide à l'audit et au suivi de la méthodologie RGPD
  - Encadrement vis-à-vis des différents clients (7 clients RGPD tous confidentiels)
- Responsable du pôle Formation d'Anyon Consulting
  - Création du pôle Formation chez Anyon
  - Préparation du contenu de formation DEVOPS
  - Préparation du contenu de formation Auditeur Sécurité
  - Préparation du contenu de formation Sécurité technique pour le RGPD







## ESCALATION MANAGER N3, CRITEO

➔ D'aout 2016 à mars 2018

**Contexte :** Escalation Manager au sein de l'équipe Escalation (Support de Production Niveau 3)

- Analyse et gestion des changements applicatifs  
Préparation aux déploiements applicatifs (Applications Web haute performance)  
Organisation et priorisation des changements  
Optimisation du process devops (revue du kanban, restructuration du process de livraison sur Jenkins/Groovy, schématisation du projet de Timeline et de CMDB)  
Participation à la définition d'OKR
- Gestion des incidents d'expertise niveau 3
- Evaluation des incidents applicatifs et métier (Criticité haute, impact technique, impact métier et financier, impact indirect)
- Identification et résolution des incidents (Worldwide)
- Préparation et mise en place des plans de remédiation
- Rédaction des post mortems et suivi de la mise en place des correctifs suggérés

### Environnement technique :

*BigData, Machine Learning, Cloud computing, Web*

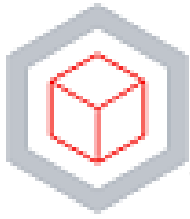
## AUDITEUR SECURITE, COVEA FINANCES

➔ De février 2016 à mars 2016

**Contexte :** Auditer et Analyser les risques du projet de migration de Datacenter Covéa développé par CAPGEMINI

- Analyse du projet de migration du SI de Covéa Finance  
Etude de l'architecture existant de Covéa Finance  
Etude de l'architecture cible
- Audit du projet de migration élaboré  
Analyse du projet Capgemini élaboré en vue de la migration  
Identification des correspondances et des décalages entre l'architecture souhaitée et le plan de migration  
Identification des phases critiques et mise en place des plans de sécurisation adaptés





- Retours sur Audit  
Elaboration de plans de mitigation pour les phases déjà entamées  
Mise en place des plans de continuité de service durant et après

## AUDIT ET CONSULTING PCI-DSS, CLIENT MOYENS DE PAIEMENT (CONFIDENTIEL)

➔ De novembre 2015 à janvier 2016

**Contexte** : PREPARATION DU DOSSIER DE MISE EN CONFORMITE PCI-DSS (Certification Obtenue par le client)

- Audit Sécurité pour obtention de l'agrément « Organisme de Moyens de Paiement » :  
Audit de la sécurité de l'architecture technique et des processus sécurité  
Elaboration d'un rapport de Sécurité à l'attention de la Banque de France
- Pilotage du projet de mise en conformité PCI DSS (sécurité des données bancaires)  
Audit et Planification : identification et réduction du périmètre PCI DSS, gap analysis, planning et un budget de mise à niveau  
Définition de l'architecture PCI DSS, des politiques et procédures, des rôles et responsabilités (RACI, SOD), des plans de tests,  
Implémentation des solutions techniques, des contrôles et mesures compensatoires et rédaction des politiques et procédures PCI DSS  
Evaluation avant audit du QSA : évaluation des processus d'amélioration, performance des pratiques PCI DSS

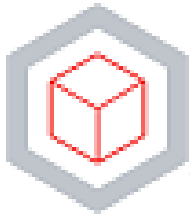
## RESPONSABLE PROJET SECURITE, COVEA FINANCES

➔ De mars 2015 à octobre 2015

**Contexte** : Auditer et Planifier la sécurisation du SI Covéa

- Responsable du projet de sécurisation et de normalisation du SI  
Phase 1 : Audit du SI et de la logique de gestion d'incidents de Covéa  
Phase 2 : Mise en oeuvre des chantiers logiques et techniques et suivi des processus de sécurisation et de normalisation  
Gestion de la communication inter-équipes et inter-entités pour la mise en place du process de gestion d'incidents
- Sécurisation et normalisation du SI :





# TEASERPUB

Audit : étude de l'existant en termes d'architecture technique et logique, documentation, processus et bonnes pratiques  
Identification des points d'améliorations  
Définition du plan d'urbanisation permettant la sécurisation et la normalisation du SI  
Chiffrage, planification et priorisation des chantiers  
Choix des outils et solutions techniques nécessaires  
Mise en place des normes et des règles de bon fonctionnement  
Rationalisation de l'architecture technique,  
Automatisation et industrialisation en vue de réduction du risque opérationnel et des délais de traitement  
Délégation et gestion des actions entre les équipes concernées pour une meilleure implication de ces dernières sur le long terme

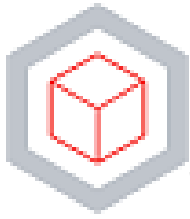
## RESPONSABLE PROJET SECURITE, NATIXIS

➡ De novembre 2014 à mars 2015

**Contexte** : Responsable du projet d'urbanisation du SI et mise en conformité technique et processus suite aux directives de l'Audit Interne.

- Gestion du projet de mise en conformité  
Élaboration et suivi du planning projet, garant de la tenue des délais,  
Communication et coordination Inter-Équipes (Métier, Etudes, Prod, Infra),  
Reporting au management, remontée des alertes, gestion des changements  
Garant de la qualité des livrables remis, implémentation des actions techniques.
- Mise en oeuvre technique  
Définition du plan d'urbanisation et des améliorations à apporter,  
Mise en place du monitoring et de la logique de gestion d'incidents (Zabbix, Hypervision)  
Migration de l'exploitation applicative de la MOE vers une production structurée (ControlM, XLDeploy)  
Remplacement des couches techniques obsolètes  
Migration sur le NAS de la plateforme NFS et FS Locaux  
Migration sur Datasynapse des calculs de Grid DR
- Redéfinition ou élaboration puis déploiement des processus et normes  
Élaboration des SLA et calibrage des KPI,  
Redéfinition du RACI et des processus d'exploitation,  
Application des normes ITIL  
Définition et mise en place des normes de sécurité (infra, utilisateurs, cloisonnement technique et applicatif),





# TEASERPUB

Déploiement des normes de sauvegardes réglementaires

## **Environnement technique :**

*Solaris, Linux (Redhat, Centos), Windows, TSM, Datasynapse, Zabbix, XLDeploy, ControlM, Shell, CFT, LDAP, NAS, NFS*

## **ARCHITECTE DE SI, CREDIT AGRICOLE CORPORATE & INVESTMENT BANK**

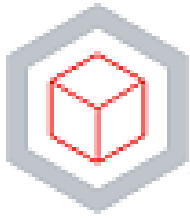
➡ **De novembre 2011 à novembre 2014**

**Contexte :** Architecte de SI & Ingénieur de production N3

- Architecture Projet Sécurisation et Normalisation (métiers, applications et infrastructures) :  
Travail en étroite collaboration avec la Direction Générale et le Contrôle Continu (projet confidentiel)  
Architecte du scope Front Office pour le projet sécurisation et industrialisation du SI  
Audit sécurité des droits, accès et privilèges utilisateurs métiers et applications (maison et éditeurs)  
Mise en oeuvre de la normalisation et sécurisation des accès utilisateurs et applications  
Mise en place d'outils et processus de monitoring d'activités en vue de tracabilité des actions
- Architecte référent technique de l'équipe de production applicative Front-Office :  
Architecte de production sur les projets d'amélioration continue  
Répartition des tâches et suivi d'avancement, Formations des nouveaux arrivants  
Reporting auprès du management Health Check, suivi incidents, avancement des projets...  
Responsable du portefeuille applicatif sur les applications de Trading  
Développement d'outils spécifiques aux Health Check Applicatifs à des fins de reporting  
Gestion de l'infrastructure de production (Supervision, PSI, ControlM, Flux) sous Unix et Windows.  
Gestion de projets pour la mise en place d'applications réglementaires (Desk CVA, DTCC)  
Ingénierie de support Niveau 3 sur des applications FO critiques  
Gestion de la relation avec équipes support Niveaux 1 et 2 à Singapour.  
Documentations DAT, DEX en anglais

**Environnement technique :** *Solaris, Linux, Shell, Nagios, Hyperic, ControlM, CFT, LDAP, NIS, NFS, Networker, PHP, Javascript, JQuery, Highcharts, SUMMIT, KONDOR, Infinity, EAI STP, ESPM, EFIRA STP, QlikView, BLOFI, LIQUID*





## EXPERT DE PRODUCTION & INFRASTRUCTURE, ORACLE & SUN MICROSYSTEMS

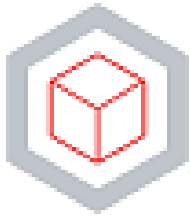
➔ De mars 2009 à novembre 2011

**Contexte :** EXPERT DE PRODUCTION & Infrastructure

- Manager d'équipe d'infogérance (équipe de 3 personnes)  
Management d'équipe d'ingénierie de Production N3  
Reporting projets de l'équipe auprès de la direction  
Pilotage de projets d'industrialisation, répartition des tâches, suivi d'avancement
- Création et déploiement des outils de mesure des engagements de SUN vis-à-vis du Client EDF infogéré :  
Identification des points de contention sur le système de remontée et de traitement d'alertes afin de respecter les engagements.  
Création et mise en place de l'outillage de reporting et de supervision sur l'environnement de production  
Création et mise en place de l'outillage applicatif pour la gestion des incidents.  
Création des outils pour la gestion interne (des incidents, des rapports de supervision).
- Infogérance technique du projet IBEX du Client EDF :  
Administration de la plateforme (réseau + web) de la plateforme interne de Sun.  
Création de nouvelles fonctionnalités pour la plateforme Sun.  
Correction des bugs et des incidents (connexions utilisateurs, rapports de reporting ...)  
Création et administration en production des utilitaires de système d'information.  
Gestion des certificats SSH (mise en place de l'outillage + administration en production).  
Création et déploiement des systèmes de supervision et de reporting sur l'outil Tivoli Manager (Rapports de sauvegardes de bases de données et système sur l'environnement de Production EDF, Création de l'architecture de modification de mots de passes et de gestion des modifications sur l'environnement de Production EDF...)  
Amélioration des reporting ControlM sur le référentiel client.  
Responsable TCM et gestion de l'infrastructure client via Tivoli Manager (gestion de packaging, chantiers d'infrastructure, sécurité, reporting, authentification...)

**Environnement technique :** *Solaris, Aix, Linux, Shell, ORACLE 9/10, TCM, LDAP, SQL, PL/SQL, PHP, VBS, VB.net*





## INGENIEUR DE PRODUCTION ET ARCHITECTURE DE SUPERVISION, BRITISH TELECOM

➡ D'octobre 2008 à janvier 2009

**Contexte** : Mise en place de l'infrastructure de Reporting Réseau des équipements British Telecom

- Ingénieur Consultant en Supervision (Réseau + Base de données + Système Linux)  
Étude de l'architecture de supervision réseau en open source  
Installation et paramétrage de Nagios  
Mise en place de l'environnement de développement  
Paramétrage de la supervision via Nagios  
Création de scripts pour la supervision Nagios (Équipements Cisco, Ciena ...)  
Formation des équipes BT à l'administration et à l'utilisation de Nagios

**Environnement technique** : *Debian, Python, SQLite, Mibs SNMP (Cisco, Ciena ...), Routage IP, DNS, NAT/PAT*

## INFOGERANCE DE PRODUCTION ET CONSULTING EN SUPERVISION / MONITORING, HEWLETT PACKARD

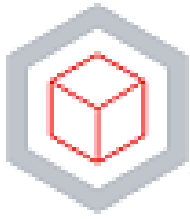
➡ De juillet 2007 à aout 2008

**Contexte** : Support en environnement de production des plateformes de services SFR et Pre-Sales HPOVO

- Projet HP OpenView OV (OVO, LGTO, OVIS, OVPI):  
Consulting Client  
Étude de faisabilité d'un outil de monitoring d'applications OVO  
Développements de plugins OVO (Shell + OVO Templates), V.A.B.F, Mise en production,  
Formation et support technique
- Mise en place d'environnements de développement sous Solaris  
Installation et administration système  
Mise en place et administration des bases de données Oracle 10g  
Administration des serveurs de la plateforme
- Développement d'applications d'industrialisation
- Administration de la base de connaissances de l'équipe HP C&I (Plateforme Zope et programmation Python)

**Environnement technique** : *HP OVO, Solaris, Oracle, Shell, VB.net, C++, Python, Zope, Perl, Java*





# TEASERPUB

**DEVELOPPEUR C++, SAGEM SOFTWARE & TECHNOLOGIES (PFE)**

➔ **De février 2007 à juin 2007**

**Contexte** : Conception et développement d'un émulateur de périphériques multifonction

- Conception et implémentation d'un méta-serveur incluant 4 serveurs incorporés et interconnectés
- Étude de faisabilité de la modification du système d'authentification de Windows Vista et création d'une DLL permettant de modifier les caractéristiques graphiques de l'affichage de l'écran de Logon de Vista et la récupération du mot de passe à l'aide des Credentials Providers.

**Environnement technique** : *Visual C++ 2005 a, Dot Net 3.5, Vista SDK, Visual C++ 6.0, MFC*

