

Didier MORANDI

21 rue des Rosiers
Lains
39320 Montlainsia
France
GSM : +336 7983 6418

didier.morandi@gmail.com
retraité



Expert en sécurité générale et informatique

Expérience

Novembre 2013 – février 2014 : Airbus (STERIA), Toulouse

- Conception de documents fonctionnels sur la sécurité des documentations en anglais

Octobre 2012 – février 2013 : iTrust France, Toulouse

- Étude sur la création de la filiale suisse de **iTrust France** à Genève
- Support 2^e niveau sur l'analyseur de vulnérabilités iKare Monitoring
- *Pen Testing* (RSA et Metasploit) et *Source Code Analysis*
- Divers audits en sécurité
- Formation des Clients

Juillet – octobre 2012 : CNES, Toulouse

Coordonnateur SSI auprès de la Direction de l'exploitation informatique du **CNES**. Pilotage des activités d'exploitation de la SSI :

- reporting
- tableaux de bord
- correspondant CNES auprès du sous-traitant chargé en infogérance de l'exploitation du SI du CNES
- assistance deuxième niveau auprès des utilisateurs
- membre du Comité de coordination SSI

Contrôle des prestations SSI de l'infogérant

- mesures de réactivité
- évaluation du respect des engagements contractuels
- contrôles techniques de conformité
- enquêtes techniques sur les moyens (antivirus, firewalls, filtrages, sondes réseau etc.)
- appréciation des méthodes et procédures d'exploitation et d'administration

Expertise SSI

- force de proposition pour améliorer la sécurité informatique du CNES (hors lanceurs)
- optimisation des performances
- automatisation des contrôles (étude de la mise en place d'un SIEM)
- identification en temps réel des dysfonctionnements
- validation des solutions proposées par l'infogérant
- responsable de l'infrastructure de gestion des clés
- gérant des plans de reprise et de continuité de service
- interface avec le partenaire chargé du laboratoire d'expertise antivirus (Devoteam)
- contrôle des prestations du partenaire

Outils gérés

- Antivirus McAfee EPo, Sophos, Bit-Defender, Kaspersky
- Proxy Web
- sondes réseau (physiques et virtuelles)
- TripWire
- SecureBox

Solutions SIEM étudiées pour le projet "Alarmes Temps réel"

- Alcatel-Lucent - OA_SafeGuard
- Araknos - Akab2
- BlackStratus - Netforensics
- Cisco - Cisco Security Manager
- Correlog - Correlog Solution Suite
- CS - Prelude/Vigilo
- eIQ Networks - SecureView
- EMC2 - RSA
- HP - ArcSight
- LogLogic - Enterprise Virtual Appliance
- LogRhythm - SIEM 2.0 security intelligence
- NetIQ - Security Manager
- NitroSecurity - McAfee Enterprise Security Manager
- Novell - Sentinel
- Q1 - Qradar
- Sensage - Advanced SIEM and Log Management
- Splunk - Splunk
- Symantec - Security Information Manager
- Tripwire - Log Center
- Trustwave Intellitactics - Security Manager for SIEM

1986 – 2012 : DTL Conseil, Sophia-Antipolis

Créateur et gérant d'une SSII spécialisée dans la sécurité informatique (**DTL Conseil**), puis installation comme consultant indépendant. Conception de logiciels spécifiques. Rédaction de procédures d'exploitation. Formation. Audits physiques et informatiques (MEHARI et EBIOS). Dossiers ISO 27000. Analyse de vulnérabilités de codes sources et de sites WEB. Plans de reprise en cas de sinistre (Binomial PlanBuilder). Définition de politiques de sécurité. Enquêtes d'intrusion. Prestations préventives, palliatives ou curatives. Gestion de projets (MS Project).

Missions concernant plus spécialement la sécurité générale et informatique :

- Banque NSM, Paris (OPC du déménagement de l'informatique et des réseaux)
- Banque UBS, Zurich (analyste informatique pour une migration DEC - IBM)
- Banque UEB, Genève (création de la fonction *auditeur en sécurité informatique*)
- Centrale des Titres du Crédit Agricole, Mer (audit sécurité MARION)
- CNES, Toulouse (correspondant sécurité informatique à la Direction de l'Exploitation)
- Crédit Agricole, Paris (OPC du déménagement de l'informatique et des réseaux)
- Crédit Lyonnais, Paris (étude du plan de secours de la salle des marchés)
- Digital Equipment, Paris (plan de continuité de services)
- DTL Conseil, Sophia-Antipolis (logiciel de gestion de sécurité pour VAX/VMS)
- Édipresse Publications SA, Lausanne (audit sécurité MARION)
- Édipresse Publications SA, Lausanne (étude sur la confidentialité)
- Interohm, Paris (rapatriement d'alarmes bancaires par X25)
- MATIF, Paris (déménagement du site de secours)
- Ordipat Gestion de Brevets, Paris (audit sécurité MARION)
- Partenaire Sécurité Informatique, Paris (responsable du département Logiciels)
- Sapeurs-Pompiers, Nice (étude informatique opérationnelle tactique)
- SEMVAT, Toulouse (audit sécurité du poste de commandement du métro VAL)
- SIGEMS, Villeneuve-sur-Lot (audit EBIOS)

- Société Générale, Marne la Vallée (étude préalable d'un site de secours)
- URSSAF de Lyon (audit sécurité MARION)
- URSSAF de Melun (audit sécurité MARION)
- URSSAF de Nantes (audit sécurité MARION)
- URSSAF de Quimper (audit sécurité MARION)
- URSSAF de St Etienne (audit sécurité MARION)

1983 – 1986 : Digital Equipment France, Paris

Créateur et responsable de la fonction "sécurité informatique interne" (RSSI) chez **Digital France**.

Dans cette fonction, j'ai réalisé notamment les tâches suivantes :

- Surveillance des systèmes (pénétration de l'extérieur, tentatives d'accès non autorisés aux ressources protégées de l'intérieur, contrôles de validité des procédures de sécurité, etc.)
- Conception du plan de reprise en cas de sinistre
- Conception du guide de la sécurité informatique interne
- Audits en sécurité (Méthode MARION)
- Formations pour les Clients, conférences, correspondant DECUS.

Divers

Disponibilité : Immédiate (à la retraite depuis le 1^{er} décembre 2015).
Mobilité : Tous pays francophones et anglophones.
Langues : Anglais courant.
Divers : Membre fondateur du CLUSIF, le Club de la Sécurité Informatique Français (1985). Ancien Country Manager de BINOMIAL France (2012).

Formation

- Conservatoire National des Arts et Métiers, Paris, cours du soir (1978-1983).
Cycle d'informatique et de gestion financière des entreprises.
- Université Technologique de Compiègne, IMI (1994).
Troisième cycle de gestion des systèmes d'information.
- Diplômes : Baccalauréat série C
Diplôme du Conservatoire national des Arts et métiers (Économie et gestion)
- Certification SAP ASAP (Bureau Van Dick).
- Préparation à la certification CISSP (Certified Information Systems Security Professional)

Publications

Gestion d'erreurs et Scripts Windows : <http://www.didiermorandi.com/VBScript>

Padirac : Une méthode de déménagement de l'informatique et des réseaux.