



La sécurité des systèmes d'information m'enthousiasme dans son rapport avec l'ingénierie : la résolution de problématiques de technique et d'efficacité avec de la *rigueur* et de l'*originalité*. J'aime considérer ses enjeux comme un tout, de la gestion du SMSI fonctionnel aux tests d'intrusions techniques. *Créatif et déterminé*, j'impulse l'énergie du changement dans les organisations, en apportant une vision *transversale*.

EXPÉRIENCE

Dep. 2018

Formind : Consultant Sécurité des SI. 

- Groupe SUEZ, assistance RSSI opérationnel groupe, expertise sécurité et support niveau 3 aux incidents de sécurité (création d'un CSIRT);
- SNCF Réseau, coach SSI auprès des équipes métiers, direction clients et services;
- Compétences de sensibilisation, de création et implémentation de processus, coordination internationale, réponse à incident, suivi d'audits

2016 – 2018

Thales : Ingénieur Cybersécurité mégadonnées (Big-Data). 

- Analyse et mise en place des cas d'utilisations relatifs à la cybersécurité;
- Mise en place de la normalisation, classification, gestion de l'évènement et indicateurs selon des normes existantes;
- Formation aux bonnes pratiques de développement : AGILE, cycles de vie.

2013 – 2016

Thales : Référent technique de la plateforme d'infogérance cybersécurité.

- Conception, dimensionnement d'architectures de sécurité, choix techniques et réalisation en temps restreint;
- Architecture à haute disponibilité, haute sécurité, à très haut débit redimensionnable;
- Gestion d'une équipe de 5 personnes (orientée AGILE);
- Déploiement de SOC à l'international sur le modèle conçu (Hollande, Hong Kong);
- Référentiel PDIS de l'ANSSI, ISO 27001;
- Représentant du SOC à l'extérieur : conférencier dans les Grandes Écoles d'ingénieur, communication externe.

Avr-sep 2013

Thales Services, Élancourt : Projet de supervision de sécurité au sein d'un SOC

- Audit de sécurité de l'architecture en place;
- Compétences en détection d'intrusions, de corrélation avec SIEM, de log management.

Jun-Sep 2012

IBM, La Gaude : Projet Extreme Blue 

- Compétition mondiale sur des innovations technologiques sur le thème des villes intelligentes; Projets : optimisation de livraisons avec GrandLyon; parking intelligent avec Streetline, déploiement d'IBM IOC à Rio.

2010 – 12

Secrétaire et responsable technique de Supélec Rézo (FAI des résidents de Supélec) 

- Gestion de projets : Organisation de conférences (Journées FedeRez), très bonnes connaissances en architecture réseau, 6 personnes à manager, projet de sécurisation d'une architecture.

FORMATION

2016

Formé ISO 27001:2013 Certification Lead Auditor par LSTI; 

2010 – 13

Élève ingénieur à SUPÉLEC, option Sécurité des Systèmes d'Information. 

- Aujourd'hui CentraleSupélec, Gif-sur-Yvette : majeure à dominante de cryptographie, détection d'intrusions, management de SI.

2008 – 10

Classes préparatoires PC* au Lycée La Martinière Monplaisir, Lyon 7.

COMPÉTENCES


Informatique

- Maîtrise GNU/Linux, théorie des réseaux, virtualisation; avec spécialisation mégadonnées pour la sécurité;
- Compétences en outils de sécurité : CERTs, SIEMs, sondes...

Langues

- Anglais : C1 – IELTS 7.5/9 (28 Avril 2012) : Good user;
- Allemand : B2 – Séjour de 6 mois cumulé en Allemagne et Autriche;
- Espagnol : A2 (Séjour Espagne et Costa Rica).

Intérêts et loisirs

- Littérature et langue française (8^e sur 260 à la dictée ECE),
- Contributeur GNU sur GitHub et Wikipédia (traduction, relecture), 
- Menuiserie et recyclage de matériaux
- Domotique et Raspberry Pi hacking,
- Techniques de communication et de PNL.

Ingénieur sécurité SI & Big Data
ISO 27001, expert GNU/Linux

Geoffrey Montel

📍 78, France

☎ +33(0) 6 98 67 44 25

@ geoffrey.montel (AT) jserv.fr

🌐 geoffreymontel 🐑 moutonjr



APTITUDES TECHNIQUES

Mégadonnées et traitement distribué :

<i>Storm</i>	●●●●●	<i>Kafka</i>	●●●●●	<i>Spark</i>	●●○○○	<i>Metron</i>	●●○○○
<i>Elasticsearch</i>	●●●●●	<i>Kibana</i>	●●●●●	<i>Logstash</i>	●●●○○	<i>Zookeeper</i>	●●●●○
<i>Spot</i>	●●○○○	<i>Hadoop</i>	●●○○○	<i>CEPH</i>	●●●○○	<i>Picviz</i>	●●○○○

Applicatifs de la sécurité :

<i>BlackStratus</i>	●●●●●	<i>IBM QRadar</i>	●●○○○	<i>Maltego CE</i>	●●○○○	<i>Qualys</i>	●●○○○
<i>Checkmarx</i>	●●○○○	<i>The Hive</i>	●●○○○	<i>Metasploit</i>	●●○○○		

Infrastructure et Cloud :

<i>Linux KVM</i>	●●●●●	<i>Docker+Mesos</i>	●●●○○	<i>LXC</i>	●●●●●	<i>Openstack</i>	●●●○○
<i>Ansible</i>	●●●●●	<i>Chef</i>	●●○○○	<i>Puppet</i>	●●●●○	<i>Saltstack</i>	●○○○○
<i>Linux</i>	●●●●●	<i>Windows</i>	●●●○○	<i>BSD</i>	●●●○○	<i>Saltstack</i>	●●○○○
<i>BIND9</i>	●●●●●	<i>OpenLDAP</i>	●●●●●	<i>Postfix</i>	●●●●●	<i>NetFilter</i>	●●●●●
<i>HTTPD</i>	●●●●●	<i>HAProxy</i>	●●●●●	<i>Nagios</i>	●●●●●	<i>Pacemaker</i>	●●●●●

Réseaux et équipements :

<i>Juniper</i>	●●●●●	<i>ForcePoint</i>	●●●●○	<i>Cisco (Switch)</i>	●●●○○	<i>StormShield</i>	●●●●○
<i>SourceFire</i>	●●●○○	<i>DenyAll</i>	●●○○○	<i>Infoblox</i>	●●○○○		

Développement et script :

<i>Bash</i>	●●●●●	<i>Python</i>	●●○○○	<i>Java</i>	●●●●●	<i>LaTeX</i>	●●●●●
<i>Python</i>	●●○○○						

NB : ● installé ; ●● testé ; ●●● utilisé en production ; ●●●● utilisé & exploration des fonctionnalités ●●●●● maîtrise