Simon Rouault - Plup

Ingénieur sécurité / DevOps

http://rouault.me

Expérience

Ingénieur Sécurité / DevOps

Freelance

depuis sept. 2015

international

Missions d'Auditeur en SSI :

- Durcir des serveurs Linux
- Auditer des architectures et des applications
- Récupérer des systèmes compromis
- Assurer la sécurité de déploiements en containers

Linux - Docker - Metasploit - Pentest continu - Retro Ingénierie - Eradication de malwares - Python

Missions de Développeur Opérationnel :

- Concevoir et mettre en oeuvre des architectures de déploiments automatisés avec Ansible
- Concevoir et développer un orchestrateur Docker avec Salt et Python
- Installer et exploiter des services d'architectures sur des serveurs Linux : SMTP, DNS, collecteurs de logs et supervision
- Installer des infrastructures de déploiement continu avec Gilab CI et Ansible

Linux - Ansible - Salt - Docker - Gitlab CI - Python

Missions de Développeur Web :

- Développer des sites web avec Django
- Développer des sites web avec Wordpress
- Développer des sites E-commerce avec Prestashop

Python - Django - PHP - Wordpress - Prestashop - Git

Expert Sécurité des SI en recherche et développement

Ministère de la Défense

mai 2013 - sept. 2015 (2,5 ans)

Paris - France

Concevoir et réaliser des moyens de communications sécurisés :

- Concevoir les architectures techniques en réponse aux cahiers de charges
- Réaliser des solutions de sécurité réinstanciables
- Développer de nouveaux logiciels dans des technologies variées (C, C++, Java, PHP, Python,...)

- Assurer l'intégration et la pérennité des solutions dans le SI
- Développer et maintenir l'Infrastructure de Gestion des Clefs
- Assurer la veille technologique

Architecture - C/C++ - Java - Python - IGC - Nomadisme - Smartphone - Chiffreur - Audit

Chef de projet maîtrise d'oeuvre

Ministère de la Défense
nov. 2012 - avr. 2013 (6 mois)
Paris - France

Organiser et piloter plusieurs projets de leur conception à leur achèvement :

- Définir le périmètre et les objectifs d'un projet
- Concevoir l'architecture en respectant le cahier des charges
- Piloter et coordonner les équipes de réalisation
- Négocier avec des partenaires techniques internationaux
- Former les utilisateurs

Projet - Budget - Cahier des charges - Spécification - Qualification - Production

Conférencier sur la Sécurité des Systèmes d'Information

Ecole des Mines d'Albi-Carmaux
2011 - 2015
(5 heures / an)
Albi - France

Enseigner l'analyse de risques et les processus de gestion de la sécurité aux ingénieurs :

- Rédaction des supports de conférence
- Présentation en amphithéâtre

PSSI - EBIOS - Enseignement

Responsable Sécurité Opérationnelle

Ministères de l'Economie et du Budget
oct. 2009 - oct. 2012 (3 ans)
Paris - France

Assurer la sécurité des informations d'intelligence économique hébergées sur le SI :

- Concevoir et bâtir les architectures dédiées aux postes nomades, aux téléphones IP, à la navigation internet et aux accès Web
- Sécuriser les interconnexions entre réseaux des ministères
- Organiser un PCA informatique
- Gérer les serveurs DNS, les pare-feux et les proxies filtrants
- Animer une équipe de 5 experts
- Gérer les incidents de sécurité

Management - Architecture - Haute disponibilité - Audit - Projet - VPN - BYOD

Adjoint Officier de Sécurité des SI

Ministère de la Défense
févr. 2009 - sept. 2009 (8 mois)
Istres - France

Homologuer le réseau d'interconnexion et les plates-formes de simulation de l'Informatique Scientifique :

- Analyser les risques de sécurité par la méthode EBIOS
- Rédiger un dossier d'homologation pour chaque système
- Auditer les éléments techniques

EBIOS - Audit - Projet

Aptitudes

Méthodologie et gestion

- Agile *SCRUM, Xtreme programming*
- Système de management de la SSI *ISO 27001*
- Analyse de risques *ISO 27005, EBIOS*
- Gestion des incidents *ITIL v3*

Déploiement et optimisation

- Contrôle de version *Git*
- Gestion de configuration *Ansible, Salt*
- Testing *XUnit, Selenium*
- Packaging *Docker*
- Orchestration *Compose, Kubernetes, OpenShift*
- Intégration continue *Jenkins, Gitlab CI*

Stockage de données

- SQL *PostgreSQL, MariaDB*
- NoSQL *MongoDB, Cassandra, Redis*
- Cloud computing *Openstack swift*
- Columns oriented *Hbase*

Langages et frameworks applicatifs

- Shell scripting *Bash, Python*
- C / C++ *LGMP*
- ASM *NASM*
- Debugging *gdb, strace, IDA Pro*

Langages et frameworks web

- Web sémantique *HTML5, CSS3*
- Responsive web design *Bootstrap*
- Python *Django*
- PHP *Symfony*
- Javascript *NodeJS, AngularJS*
- Protocoles *AJAX, WebSocket*
- CMS *Wordpress, Prestashop*

Audit de sécurité

- Recherche de vulnérabilités *Metasploit, Peach fuzzer*
- SQL injection *SQLMap*
- Analyse Web *Burp suite, SSL striping*
- Analyse réseau *Nmap, Scapy, MITM*
- Shellcodes *Metasploit, ROP*
- Rétro-ingénierie *gdb, IDA Pro*

Cryptographie

- Infrastructure de Gestion des Clefs *EJBCA*
- Chiffrement *RSA, AES, Shamir's secret*
- Signature *RSA, ECDSA*
- Authentification *Kerberos, 802.1x, OAuth2*
- Cartes à puce *PKCS#11, PKCS#15*

Système

- Virtualisation *Virtualbox, Vagrant, Docker*
- Supervision *Sensu, Grafana*
- Gestion des logs *Elastic search, Logstash, Kibana*
- Serveurs Web *Nginx*
- Serveurs Applicatifs *NodeJS*
- Linux *Debian*
- Windows Active Directory *2008, 2012*

Réseau

- Haute Disponibilité *VRRP, Balance de charge, Redondance, Simulation*
- LAN *STP, OSPF, VRF, DHCP*
- DNS *Bind*
- SMTP *Postfix*
- Virtual Private Network *IPSec, VPN SSL*
- Architecture de filtrage *DMZ, Proxy, WAF*
- Pare-feux *Netfilter, Arkoon, NetAsq, CheckPoint*
- Système de Détection d'Intrusion *Snort, Suricata*
- Modèle OSI *802.11n, Ethernet, IP, TCP, NetBIOS, ASN.1, HTTP,...*

Formation

Formations professionnelles

Organismes privés

- Certification Ethical Hacker de l'EC council
- Formation Administrateur Web Gateway de McAfee
- Certification Administrateur de parefeux Arkoon

Cursus scolaire

Ingénieur

- Diplôme d'ingénieur généraliste spécialisé en Génie des Systèmes d'Information de l'École des Mines d'Albi-Carmaux (2009)

Baccalauréat

- Diplôme du Baccalauréat Scientifique

- Certification Administrateur de parefeux Checkpoint

Organismes étatiques

- Formation "Internet et sécurité" de l'ANSSI
- Formation "Pratique de la SSI" de l'ANSSI

spécialité Mathématiques (2004)

Langues

- Français - langue native
- Anglais - complète compétence professionnelle
- Espagnol - compétence professionnelle acceptable
- Arabe - notions de survie