



Simon Rouault - Plup

IT Security Engineer / DevOps

<http://rouault.me>

Experience

IT Security Engineer / DevOps

Freelance

since September
2015
moving around the
world

Security auditor missions:

- Hardening Linux servers
- Audit infrastructures and applications
- Recover hacked systems
- Ensure deployment security inside containers

Linux - Docker - Metasploit - Continuous Pentesting - Reverse Engineering - Malware eradication - Python

DevOps missions:

- Design and install automated deployment architectures with Ansible
- Design and develop a Docker orchestrator with Salt and Python
- Install and exploit services for Linux architectures : SMTP, DNS, log collectors and monitoring
- Install continuous delivery infrastructures with Gitlab CI and Ansible

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

Web developer missions:

- Develop websites with Django
- Develop websites with Wordpress
- Develop e-commerce websites with Prestashop

Python - Django - PHP - Wordpress - Prestashop - Git

IT Security expert in research and development

French Ministry of Defense

May 2013 -
September 2015
(2,5 years)
Paris - France

Design and implement secured communication devices:

- Design technical architectures in response to the tender specifications
- Realize security products for massive use
- Develop new softwares in various technologies (C, C++, Java, PHP, Python...)
- Integrate and sustain the new security products in the information system
- Develop and maintain the Public Key Infrastructure

- Ensure technology watch

Architecture - C/C++ - Java - Python - IGC - Digital nomad - Smartphone - Cipher equipment - Audit

Project manager

French Ministry of Defense Organize and manage multiple projects from conception to completion:

*November 2012 - April 2013 (6 months)
Paris - France*

- Define the scope and objectives of the project
- Design the architecture according to specifications
- Lead and coordonnate work teams
- Negotiate with international technical partners
- Train users

Project - Budget - Specification - Qualification - Production

Lecturer on the Information Security Management System

Ecole des Mines d'Albi-Carmaux Teaching risk analysis and the security management processes to engineers:

*2011 - 2015 (5 hours / year)
Albi - France*

- Writing conference materials
- Amphitheater presentation

ISSP - EBIOS - Education

Head of Operational Security

French Ministries of Economy and SI: Ensuring the security of economic intelligence information hosted on the

Budget

*October 2009 - October 2012 (3 years)
Paris - France*

- Design and build architectures dedicated to mobile workstations, IP phones, Internet browsing and Web access
- Secure the interconnections between networks of ministries
- Organize a Disaster Recovery Plan
- Manage DNS servers, firewalls and filtering proxies
- Lead a team of 5 experts
- Manage security incidents

Management - Architecture - High availability - DRP - Audit - Project - VPN - BYOD

Deputy IS Security Officer

French Ministry of Defense Approve the interconnection network and simulation platform for scientific computing:

*February 2009 - September 2009 (8 months)
Paris - France*

- Analyze security risks by EBIOS method
- Write a registration dossier for each system
- Audit the technical elements

EBIOS - Audit - Project

Methodology and management

- Agile *SCRUM, Xtreme programming*
- Information security management system *ISO 27001*
- Risks assessments *ISO 27005, EBIOS*
- Asset management *ITIL v3*

Deployment and optimisation

- Version control *Git*
- Configuration management *Ansible, Salt*
- Testing *XUnit, Selenium*
- Packaging *Docker*
- Orchestration *Compose, Kubernetes, OpenShift*
- Continuous integration *Jenkins, Gitlab CI*

Data storage

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

Application languages and frameworks

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

Web languages and frameworks

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

Security audit

- Vulnerability research *Metasploit, Peach fuzzer*
- SQL injection *SQLMap*
- Web Analyse *Burp suite, SSL stripping*
- Network Analyse *Nmap, Scapy, MITM*
- Shellcodes *Metasploit, ROP*
- Reverse engineering *gdb, IDA Pro*

Cryptography

- Public Key Infrastructure *EJBCA*
- Encryption *RSA, AES, Shamir's secret*
- Signature *RSA, ECDSA*
- Authentication *Kerberos, 802.1x, OAuth2*
- Smartcard *PKCS#11, PKCS#15*

System

- Virtualization *Virtualbox, Vagrant, Docker*
- Supervision *Sensu, Grafana*
- Log management *Elastic search, Logstash, Kibana*
- Web servers *Nginx*
- App servers *NodeJS*
- Linux *Debian*
- Windows Active Directory *2008, 2012*

Network

- High Availability *VRRP, Load balancing, Redondancy, Simulation*
- LAN *STP, OSPF, VRF, DHCP*
- DNS *Bind*
- SMTP *Postfix*
- Virtual Private Network *IPSec, VPN SSL*
- Filtering architecture *DMZ, Proxy, WAF*
- Firewalls *Netfilter, Arkoon, NetAsq, CheckPoint*
- Intrusion Detection Systems *Snort, Suricata*
- OSI model *802.11n, Ethernet, IP, TCP, NetBIOS, ASN.1, HTTP,...*

Education

Professional training

Private organizations

- Certification Ethical Hacker from EC council
- Certification Administrator Web Gateway from McAfee
- Certification Firewall Security Administrator from Arkoon
- Certification Firewall Security Administrator from Checkpoint

University cursus

Engineer degree

- General engineer degree specialty Information Systems from École des Mines d'Albi-Carmaux (2009)

Bachelor degree

- Scientific Bachelor degree specialty Mathematics (2004)

Languages

- French - native

State agencies

- Training "Internet and security" from ANSSI
- Training "Pratice of IS Security" from ANSSI
- English - Full professional proficiency
- Spanish - Professional proficiency
- Arabic - Survival concepts