La Ruelle 3
1268 Begnins, Suisse
+41 79 554 78 76
pierre.rouveyrol@protonmail.com
Nationality : Swiss, French

Pierre Rouveyrol

Sysadmin, Infosec, Devops, Open Source, 7 years experience

Skills

System Administration
OS : 10 years experience in managing **GNU/Linux** and **BSD** systems, both personally and professionally, using multiple distributions. Some professional experience using and managing Microsoft **Windows**, AD, GPOs.
Monitoring : Mostly **Zabbix, ELK, Grafana, Splunk, Prometheus**, some experience using **Nagios**.
Orchestration : Experience using **Ansible, Puppet**, along with **Foreman, Rundeck**. I have deployed **Kubernetes** clusters and managed their utilization by dev teams.

Virtualization
Most of my experience is with **KVM** based solutions, along with **QEMU** in some instances. I also had the chance to work with **Xen** and **VMWare** products.
Recently, most of my work had to do with **Docker/Podman**. I have written numerous Dockerfiles to containerize some web applications, using either **Docker Compose** or **Kubernetes**.

Security
Most of my previous missions were at least related to security. I have driven adoption of **SIEM** solutions such as **Rapid7 InsightVM and InsightIDR**. I have managed **ESET** security solutions in an international company context. I have been in charge of monitoring and responding to incidents with **Azure Sentinel** worldwide.
I have experience in malware development and **pentesting** as well as **applider cryptograpahy** both in an academic and industry context.

Network
I have been working with **PFSense** and **Fortinet**. I can manage most **DHCP, DNS** solutions and I have been in charge of managing **VPN** using **IPSec, OpenVPN and Wireguard**.
I can manage **Nginx, Apache, and HAProxy**.

Cloud
I have worked with **Openstack and Kubernetes**, and I have some experience using **Azure and AWS** services, notably **S3 and Swift** for which I did some development.
I have deployed and maintained **CEPH** clusters. Bare metal, and in K8s using **Rook**.

DevOps
I have been using **Git** for the last 10 years, and written **CI/CD** pipelines with **Gitlab and Jenkins** for building, testing, auditing and deploying applications.

Development
While not a developper, I have some experience using **C++, Python, Bash, Java, ADA and Go**. These were mostly in the context of system administration or debugging. I can do some very basic web development, using **Flask and Hugo**. I have however written numerous scripts making use of **REST** APIs.

Soft skills
I have been driving adoption of security products and uniformization of best practices within an IT context. I have also been managing L1 and L2 support teams, and occasionally had to recruit them. I have been giving some training regarding security best practices, cryptography and version control using Git.

Experience

05.2021-03.2022 **Systems and Automation Engineer**, INFOMANIAK, Geneva, Switzerland.
Part of the team in charge of infrastructure maintenance and improvement.
L4 Incident response, MCO, automation using Rundeck and Puppet.
Backup automation and validation with Rundeck.
SSL Certificate issuance and renewing automation, using Letsencrypt, cfssl.
CI/CD pipelines development in Gitlab.
Monitoring using Zabbix, Grafana, Prometheus and ELK.
K8s administration, containerisation of web services for use in K8s.
HA Proxy administration, load balancing, filtering, K8s ingresses.
S3 administration on CEPH RADOS, Provisioning and administration of Ceph, development and maintenance of helper scripts in Python and Bash.
Migration of legacy services from Xen to Open Stack or K8s.
0 downtime operations on Icecast radio clusters.
Improvement of IPAM solution, with API based DHCP.
Night and weekend shifts

03.2020-04.2021 **IT Security Specialist**, MSC, Geneva, Switzerland.

Second in charge of EMEA security.
Migration of most of the infrastructure to Azure.
Architecturing of Azure services to improve security.
Deployment and management of worldwide web allow listing policy. Python development of services to streamline requests related to allowlistting policy.
Monitoring and incident response using Splunk, Azure Sentinel.
Company wide software upgrades through GPO.
Designing physical security architecture to protect videosurveillance and identification systems.
Worldwide level 3 support on security related matters.
Management of L2 teams in Greece, Brazil and Italy

01.2017-02.2020 **IT Security Specialist**, Viseo Group, Grenoble, France.

In charge of company wide security improvement, maintenance and incident response, as well as IT operations.
International level 3 IT support for Linux systems, networks and cloud infrastructure.
Management of L2 teams in Morocco, Philippines and France.
Introduction of Ansible to manage security controls on all servers of the company.
Automation of server provisioning inside OVH's Openstack services, migration of all on prem servers to OpenStack.
Automation of SSH access management using Vault for key storage and Ansible for deployment.
Upgrading of all legacy web services, contributions to GLPI, Fusion Inventory.
Introduction, installation and maintenance of Rapid7 InsightVM SIEM solution to manage security on servers and user terminals.
Introduction and deployment of Microsoft Intune for user terminal management.
Maintenance of network services using PFSense, installation and upgrade of physical and virtual instances.
Setup and maintenance of IPSEC VPN links with customers using PFSense.

2015-2016 **Cybersecurity Engineer**, Thales, Montbonnot, France.

Security consulting on an undisclosed SCADA project.
Applying EBIOS methodology of a critical infrastructure project.
Automation of SSH based access control.
Pentesting monitoring, distributed and web services and Scada systems.
Improvement of architecture for security.
Design and implementation of security controls using Jenkins

2014-2015 **Research Engineer**, Inria : Privatics, Montbonnot, France.

Research and development of a password guessing algorithm for targeted attacks based on Markov chains.
Solving performance and memory constraints related to operations on huge datasets.
Several talks given about the project and its targets and implications.
more details : https://team.inria.fr/privatics/omen-leveraging-personal-information-for-password-cracking/

03.2014-09.2014 **Research Intern**, Inria : Privatics, Montbonnot, France.

Feasibility assessment of consumer grade Wi-Fi APs exploitation as a geotracking botnet.
Reverse engineering of consumer grade internet set top boxes to evaluate the feasibility of deploying large scale, privacy threatening malware.
More details : https://hal.inria.fr/hal-01151446/document

Languages

French	**Native**	
English	**Fluent**	*Numerous travels abroad (Irland, UK, US, Canada...) and all work in English*
German	**Basic**	*3 years in school*

Education

Academic

2015-2016 **Master 2 cybersecurity**, *SAFE : Sécurité, Audit, inFormatique légalE*, Université Joseph Fourier.

2013-2014 **Master 1 computer science**, *International program, MoSIG*, Université Joseph Fourier.

2012-2013 **Bachelor computer science**, *Video games conception*, Université du Québec à Chicoutimi.

2010-2012 **DUT Informatique (French 2 year diploma)**, *IUT 2 de Grenoble*, Université Pierre Mendès-France, *Rank : 10/84*.

2007-2010 **Baccalauréat S-SI (Engineering)**, *Lycée Ferdinand Buisson*.

MOOC

07.2013-09.2013 **Computer Networks**, *https://www.coursera.org/*, Washington university's networks course, *Grade : 96/100*.

10.2011-12.2011 **AI-Class**, *https://www.ai-class.com/*, Stanford's introductory Artificial Intelligence course, *Grade : 98/100*.