

# Alejandro Andreu

SECURITY ANALYST · DEVOPS ENGINEER

Carrer del Treball, Barcelona, Spain

☎ (+34) 685 807 002 | ✉ contact@alejandroandr.eu | 🏠 alejandroandr.eu | 📱 alejandroandreu | 🌐 andreuisabal

*"Be the change that you want to see in the world."*

## Education

### Universitat Pompeu Fabra

B.S. IN TELEMATICS ENGINEERING

Barcelona, Spain

Sep. 2009 - Jul. 2013

## Experience

### Proficio

SOC ANALYST

Barcelona, Spain

Jul. 2017 - PRESENT

- Dealt with a number of events that were initially generated by a wide array of different devices: Palo Alto, Cisco Asa, Darktrace, Bluecoat, Snort, etc.
- Timely and concisely worked on security incidents that affected the customers' infrastructure.
- Worked with two main SIEM products: HP ArcSight and Splunk.
- Performed incident response when critical situations arised (worm outbreaks, DDoS attacks, spam campaigns).
- Effectively communicated information surrounding certain events to the customers.

### Midokura

DEVOPS ENGINEER

Barcelona, Spain

Jun. 2016 - Jul. 2017

- Streamlined the process of integrating Midokura's award winning MEM software into Red Hat OpenStack Platform (RHOSP), reducing complexity to operators in the process of deploying, maintaining and upgrading clouds.
- Set up a robust, highly available monitoring system using Prometheus. Tailored precise alerts to be bothered only when the situation really requires it.
- Acquired extensive experience with OpenStack and its core components along numerous releases (from Kilo to Pike).
- Made significant contributions to upstream open source projects.
- Implemented Puppet modules to install and configure Midokura's software in different versions of Ubuntu and RHEL derivatives.

### Netcentric

SYSTEM ENGINEER

Barcelona, Spain

Oct. 2015 - May. 2016

- Administered and maintained a customer's AEM production environment in Amazon Web Services (AWS) with on-call rotation outside of business hours.
- Released, packaged and deployed project code on heterogeneous systems.
- Set up several Adobe AEM environments (from staging to production) for a client from scratch, whilst administering the MongoDB clusters that acted as the application database.
- Designed and implemented caching strategies for improved overall performance on client infrastructure.
- Enhanced security of public-facing Apache web servers.
- Automated many of the Operations team periodic tasks by developing an extensive set of Bash scripts.
- Broadened my knowledge on continuous integration systems, especially with Jenkins.

### Netcentric

JUNIOR SYSTEM ENGINEER

Barcelona, Spain

Oct. 2013 - Oct. 2015

- Administered numerous UNIX/Linux servers in a wide variety of flavors as well as the internal network.
- Shrunk downtime or malfunctioning of Netcentric's internal infrastructure by implementing a reliable monitoring system with Zabbix.
- Provided IT support for several customers' production environments in a timely and decisive manner. Travelled on-site regularly to give education to end users of the web application.
- Performed configuration management of Netcentric's internal infrastructure with Puppet.
- Reduced the complexity and effort of deploying new staging environments by setting up Foreman, a lifecycle management tool.
- Worked side by side with customer to migrate its Solaris already-running infrastructure to Linux.

### Code for Europe

SOFTWARE DEVELOPER

Barcelona, Spain

Sep. 2012 - Jul. 2013

- Designed and implemented a fault-tolerant sensor network using only open technologies (Raspberry Pi, Arduino, XBee) which leveraged the power of already existing open data portals to store and display the data.
- Gained experience in C and Python programming languages.
- Cooperated with other similar initiatives being deployed along the continent.

## Projects

---

### SOC Helper

Software

[HTTPS://GITHUB.COM/ALEJANDROANDREU/SOC-HELPER](https://github.com/ALEJANDROANDREU/SOC-HELPER)

SOC Helper is a configurable utility that saves intelligence-gathering analyst time by querying certain websites with the user input. Currently it supports IP addresses, URLs, domains and file hashes.

### alejandroandr.eu

Website

[HTTPS://ALEJANDROANDR.EU](https://alejandroandr.eu)

Personal blog where I share short articles as I get started in the information security field.

## Certifications

---

### SUSE Certified Linux Professional

SUSE

APR. 2015 - PRESENT

License 10272802

### LPIC-1

Linux Professional Institute

MAR. 2015 - MAR. 2020

License LPI000321778

### ITILF

EXIN

MAR. 2015 - PRESENT

License 5322396.20383935

## Presentation

---

### Wireless Battle Mesh v6

Aalborg, Denmark

PRESENTER FOR <COMMONS FOR EUROPE>

Apr. 2013

- Introduced wireless sensor mesh network that I designed and implemented and how to take advantage of it in different scenarios.