Thibault Normand

33 yo, French, Married • Toulouse - France • +33 668 666 396 thibault.normand@gmail.com

Cyber Security Data Engineer

Presentation

Passionated technical architect and security engineer, I like to treat projects combining these two skills. My experience in security and develoment allows me to have a different approach, especially be aware of security issues, in development lifecycle. I'm in permanent technologic exploration, always looking for the "best tool", and better skills to exploit.

Jobs expected : Technical Architect; Full Stack Developer; Technical Expertise; Consulting;
Domains expected : Cyber Security; Big Data; Machine Learning; BlockChain; IoT;

Professional Experience

N/C [Security Research and Development] **Toulouse - France**
Cyber Security Engineer / Data Engineer / Full Stack Developer / DevOps *October 2013 -*

- CERT / SOC Tools development
- Customer services portal. (Go, RethinkDB, VueJS)
- Realtime Wallboards for customer services metrics (Elixir, Phoenix, Sass, VueJS)
- Design and develop a malware analysis workflow for IoC extraction. (Go, RethinkDB, RabbitMQ, Docker, Cuckoo, VirusTotal, Yara, AngularJS 2)
- "Cyber Threat Analytics" for data graph clustering research. (R, Neo4j, ElasticSearch, Machine learning, Clustering)
- "Technical Threat Intelligence" platform for IoC feeds aggregation. (Go, RabbitMQ, ElasticSearch, Neo4j, AngularJS)
- Malware submission portal service. (Go, RabbitMQ, MongoDB)
- Security advisories portal service. (Go, RabbitMQ, MongoDB, AngularJS)
- Malware decontamination autonomous service. (Go, AngularJS, Qt, ZMQ, Docker)
- Risk coverage oriented SIEM rules exchange platform. (Go, MongoDB, AngularJS)
- Microservice platform : email(compose, send, sign), authorization / authentication, token generation, licensing (Go, gRPC, Consul, Vault, Docker, Rancher)
- Dashboards and software metrics monitoring (Go, Prometheus, InfluxDB, ElasticSearch, Grafana)
- Security Code Review (Java / J2EE)
- Intern mentoring.

INFOTEL [Software Research and Development] **Toulouse - France**
Lead Developer / ScrumMaster *January 2010 - October 2013*

- High available, legally valuable and secure file deposit platform (RabbitMQ, Protobuf, Scala/AKKA, Java, Spring, ElasticSearch, AngularJS)
- OAUTH 2.0 based SSO services. (Java, Spring, JWT, PKI, PKCS#11, HOTP)
- Javascript application development. (jQuery, Backbone.JS, CoffeeScript)
- Continuous integration. (Git, Jenkins, Sonar)
- Doc as code worflow. (Git, Jenkins, Maven, Docbook5, XSLT, FOP)
- Process management Web interfaces for DB2 / Z/OS. (Java, Portlets)
- Quality and Security Code Review (Java, J2EE)
- Product maintenance. (ClearCase, Java, Struts2, Eclipse RCP)
- Intern mentoring.

SCASSI Conseil [IT Security] **Toulouse - France**
Application Security Engineer *July 2008 - December 2009*

- EBIOS risk analysis based software design. (SOA, J2EE, .Net)
- Risk analysis method generalization (UML)
- Security code review (Java/J2EE, C/C++, PHP)
- Reverse engineering, malware analysis
- SOC Analyst for a local account.
- Teacher for technical courses. (Virtualisation / Firewall and Access Controls)

Intern - Developer *October 2007 - June 2008*

- Design et develop an EBIOS related risk analysis tool. (Ruby, RoR)
- Network and System administrator for small enterprise environment.
- Web Application PenTest (from a developer side view).

Opencube Technologies [Numerical Media] — **Toulouse - France**
Intern - Developer — *March 2007 - September 2007*
- DFXP subtitle format decoding and visualisation API. (Qt, C++)
- Digital Signal Processing for TeleText data extraction. (Linux, C++)

MEDES / IMPS [Health / Space] — **Toulouse - France**
Intern - Développeur — *March 2006 - August 2006*
- Geographical Information System (GIS) visualisation component. (Java, Eclipse, RCP)
- OpenSource GIS server enumeration report. (PostGIS, GRASS)
- Network architecture, setted up a 'free' domain controller. (OpenLDAP, Samba, Kerberos, DHCP, DNS, NTP)
- Virtualisation servers (Gentoo, Xen, VMWare)

Karobas [Video Games] — **Sophia Antipolis - France**
Intern - System and Network Administrator — *March 2005 - September 2005*
- Network infrastructure desgin for game servers.
- High Availability and Security.
- Exchange 2003 Domain and Mail Services.
- Database system migration, and software impacts.
- Interactive 3D world designs (Virtools)

Nice-Antiques.com [Art / Antique] — **Nice - France**
Intern - WebMaster — *March 2004 - July 2004*
- Design and develop a dynamic website. (PHP / MYSQL)
- Commercial referencing campaign optimization.

Education

IUP ISI — **Toulouse - France**
M2 ISI - Métamodélisation et Temps réel critique — 2007 - 2008
- Métamodélisation UML, J2EE, Programmation temps réel (ADA, C, SCADE), Droit

M1 Ingénierie des Systèmes Informatiques (ISI) — 2006 - 2007
- UML, Programmation distribuée (Java / J2EE, C), Base de données (avancé), XML, Mathématiques, Gestion

L3 Ingénierie des Systèmes Informatiques (ISI) — 2005 - 2006
- UML, Programmation (Java, C++), Base de données, Mathématiques, Gestion

IUT Informatique — **Nice - France**
Licence Professionelle, Administration des systèmes et des réseaux (ASR) — 2004 - 2005
- Réseau, Administration système (Unix, Windows) / base de données (Oracle), Mathématiques, Gestion, Droit

DUT Informatique, Génie Logiciel — 2002 - 2004
- Réseau, Base de données, C, Java/C++, Programmation système, Mathématiques, Gestion

Lycée A. Camus — **Fréjus - France**
Bac S Sience de l'ingénieur, Spécialité Mathématiques — - 2002
- Mathématiques, Electronique, Mécanique, Informatique

Certifications

- MCP MS72-215 - Microsoft Windows 2000 Server

Languages

- Français: Langue maternelle
- Anglais: Lu, Ecrit & Parlé

Skills

Functionnal
Project Management / ScrumMaster; Meeting management; Pedagogy / Popularizaion; Scienfitic publication writeup; Public talks; Technology Watch;

Languages
Go; JavaScript; Java; C/C++; Ruby; Python; ASM (x86, ARM7); Scala; Elixir;

Databases
MongoDB; RethinkDB; Redis; Neo4j; MySQL / MariaDB; PostgreSQL; Hadoop / HBase; Oracle; SQL Server;

Operating Systems
Linux (Daily usage : ArchLinux); MacOS X; Windows;

Web Framework

Node.js / Express; MeteorJS; Ruby on Rails; Django; Play! Framework; Microformats; Phoenix;

Frontend / UX
ES6 / ES7 / TypeScript; AngularJS 1 / 2; React / Flux; VueJS; Grunt / Gulp / WebPack; HTML5; CSS3 / SASS / LESS; Elm;

DevOps
LXC / Docker; Chef / Puppet / Ansible / SaltStack; Logstash / Fluentd / Graylog; Sentry; Jenkins / TravisCI / DroneIO / GitlabCI; Kubernetes / Deis; CoreOS / Rancher; Prometheus / Gafana;

Data Engineering
Machine Learning (SVM, PNN, RF, GBM); H2o; SciKit Learn; Protégé; R; Python / Jupyter / Pandas; Qlikview; Maltego; ElasticSearch / LogStash / Kibana (ELK);

Security
Cuckoo Sandbox / VMCloak; Suricata / Bro / OSSEC-HIDS; Honeypots (Cowerie / Kippo); DNS / SMTP Sinkhole;

BlockChain
Ethereum;

Java
J2EE; Spring (Core, MVC, Security, Data); Apache Storm; Apache Spark; Apache Kafka; Zookeeper;

Other activities

- Practice drum since September 2013;
- Practice saxophon;
- Continuous improvement with technologic watch, experimentation and personnal projects (Security, Softwares, Management);
- Writer (blog);
- Technology explorer;