Diego **Zamboni**

SENIOR ENGINEERING MANAGER · COMPUTER SECURITY EXPERT · IT SECURITY ARCHITECT

✉ diego@zzamboni.org · 🏠 zzamboni.org · 🦋 zzamboni · 🐙 zzamboni · 🖥 zzamboni · 💼 zzamboni · 🐦 zzamboni

I am a Senior Engineering Manager and IT Architect with 29 years of experience building systems and leading teams in startups as well as big companies. I have experience working with and leading remote teams. I possess a strong combination of leadership, conceptual and technical skills. I have excellent communication abilities, with ample writing, teaching and public speaking experience. I specialize in the areas of Computer Security, Cloud Computing and Configuration Management.

Key skills

Leadership	Team and project leadership, systems and software architecture, agile methodologies.
Computer Security	Secure software development, security architecture, risk management and compliance, virtualization and cloud computing security, intrusion detection and prevention, operating system and network security.
Communications	Excellent written and spoken communication skills, with more than 30 years of written and spoken communication and teaching experience.
Systems and Development	Unix/Linux systems engineering and administration, system health management and monitoring, cloud platforms (Amazon EC2, Cloud Foundry), software development experience (Ruby, Python, C, Perl, LISP, etc.).
Configuration management	CFEngine, Ansible, Puppet.
Languages	Spanish (native), English (100%), German (60% - B1 level).

Experience

Swisscom   *2014 – Present*   *Switzerland/U.S.A.*

ENTERPRISE ARCHITECT AND IT CLOUDS SOLUTION SECURITY ARCHITECT   *Apr 2019 – Present*

- Member of the *Swisscom IT Clouds* leadership team, which defines and manages Swisscom's cloud offerings.
- Member of the *Swisscom Enterprise Architecture* team, which defines future Swisscom products and solutions.
- Maintain cloud platform and service compliance with internal, contractual and regulatory standards (ISO27001, ISAE3402/3000, FINMA, GDPR).
- Established *Security Champions* initiative to promote and improve a culture of security responsibility.
- Established organization-wide processes for risk management, threat modeling, audits and penetration testing.

ENGINEERING TEAM LEAD FOR MONITORING, HEALTH AND STATE MANAGEMENT   *Aug 2014 – Apr 2019*

- Established and managed a team of up to 16 engineers that designed, implemented and operated monitoring and logging capabilities for Swisscom's IaaS and PaaS cloud platforms
- Unified diverse platform and service monitoring components into one cohesive pipeline, reducing costs and increasing efficiency.
- Defined architecture and oversaw implementation of customer-facing monitoring and logging services.
- Designed the architecture and implemented the initial version of the *Orchard* monitoring platform for Swisscom's *Application Cloud*.
- Managed business relationship and technical implementation of OpsGenie for alert management in IT Clouds.
- Defined and implemented integrations between Jira and OpsGenie for alerting of user-reported incidents.

CFEngine AS   *2011 – 2014*   *Norway/U.S.A. (remote)*

SENIOR SECURITY ADVISOR AND PRODUCT MANAGER   *Oct 2011 – Jun 2014*

- Established and led the CFEngine Design Center project.
- Participated in the development of the CFEngine language roadmap and security strategy.
- Overall CFEngine Advocate, with a special focus on security.
- Gave talks, wrote articles and blog posts, taught classes, and in general spread the word about CFEngine.

HP Enterprise Services   *2009 – 2011*   *Mexico*

ACCOUNT SECURITY OFFICER AND SERVICE DELIVERY CONSULTANT   *Nov 2009 – Oct 2011*

- First point of contact for security-related issues for HP enterprise customers in Mexico, some of them with international presence.
- Initiated, advised and managed security-related projects.
- Handled communication and coordination between technical teams involved in security initiatives.
- Oversaw all security-related aspects of the design, implementation and delivery of IT Outsourcing projects.
- Performed analysis, design and implementation of solutions in multiple areas of expertise, including system automation, configuration management, system administration, system design, virtualization, performance and security.

IBM Zurich Research Lab   *2001 – 2009*   *Switzerland*

RESEARCH STAFF MEMBER   *Oct 2001 – Oct 2009*

- I worked in multiple intrusion detection, malware detection and containment, and virtualization security research projects, including:
    - *Project Phantom*: Security for VMware virtual environments using virtual machine introspection.
    - *Billy Goat*: An active worm-detection and capture system, deployed in the IBM internal and external networks.
    - *Router-based Billy Goat*: An active worm-capture device deployed at the network boundary and coupled with a border router to effectively and automatically spoof every unused IP address outside the local network.
    - *Exorcist*: Host-based, behavior-based intrusion detection using sequences of system calls.

National Autonomous University of Mexico (UNAM)   *1991 – 1996*   *Mexico*

HEAD OF COMPUTER SECURITY AREA   *Aug 1995 – Aug 1996*

- Established UNAM's first Intrusion Response Team, which has since evolved into a much larger organization.
- Supervised up to nine people working on different projects related to computer security.
- Supervised and participated in the direct monitoring of the security of a Cray supercomputer and 22 Unix workstations.
- Provided security services to the whole University, including incident response, security information, auditing and teaching.
- Established the celebration of the *International Computer Security Day* (sponsored by the Association for Computing Machinery) at UNAM. Acted as the main organizer of the event for two years (1994 and 1995). This event has grown and divided into the *Computer Security Day* (a one-day event) and the *Seguridad en Cómputo* (Computer Security) conference (a multi-day event).
- Designed and headed development of an audit-analysis tool for Unix systems (SAINT).

SYSTEM ADMINISTRATOR   *Nov 1991 – Aug 1995*

- Part of the system administration team at the University's Supercomputing Center, managing UNAM's Cray Y-MP Supercomputer and related systems.
- Responded to security incidents affecting the Cray supercomputer and related workstations.

Education

Ph.D. in Computer Science   *West Lafayette, IN, U.S.A.*

PURDUE UNIVERSITY   *Aug 1996 – Aug 2001*

Using Internal Sensors for Computer Intrusion Detection, Advisor: Eugene H. Spafford.

Certifications

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)   *April 2019*

SAFe® 4 CERTIFIED PRODUCT OWNER/PRODUCT MANAGER   *July 2017*

Published books

LITERATE CONFIGURATION   *Self-published, 2019*

LEARNING HAMMERSPOON   *Self-published, 2018*

LEARNING CFENGINE   *O'Reilly Media 2012, self-published 2017*

Research, Publications, and References

Available upon request.

Full Curriculum Vitæ available at https://zzamboni.org/vita/.