Diego **Zamboni**

Senior Engineering Leader · Computer Security Expert · IT Security Architect

diego@zzamboni.org · zzamboni.org · zzamboni · zzamboni · zzamboni · zzamboni · zzamboni

I am a Senior Engineering Manager, IT Architect and Researcher 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 with excellent communication abilities. I specialize in the areas of Computer Security, Cloud Computing and Configuration Management.

Key skills

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

Experience

Swisscom

2014 – Present *Switzerland/U.S.A.*

Enterprise Architect and IT Clouds Solution Security Architect — *Apr 2019 – Present*

- As a Solution Security Architect for IT Clouds:
  - I define and manage the security features and characteristics of Swisscom's cloud offerings, as a member of the *Swisscom IT Clouds* leadership team.
  - I work with product managers, engineering teams and the corporate security group to maintain cloud platform and service compliance with internal, contractual and regulatory standards (e.g. ISO27001, ISAE3402/3000, FINMA and GDPR).
  - I established and manage the *Security Champions* initiative to promote and improve a culture of security responsibility.
  - I established organization-wide processes for risk management, threat modeling, audits and penetration testing.
  - I am the point of contact for CISO-level interactions with Swisscom's cloud customers.
- As an Enterprise Architect, I define future Swisscom products and solutions as part of the *Swisscom Enterprise Architecture* team.

Architect and Engineering Leader for Monitoring, Health and State Management — *Aug 2014 – Apr 2019*

- Starting as a project lead and architect, I founded and led a team of up to 16 people that designed, implemented and operated the monitoring and logging capabilities for Swisscom's IaaS and PaaS cloud offerings.
  - Unified diverse monitoring components into a cohesive framework, reducing costs and increasing efficiency by 20%.
  - Defined architecture and implementated customer-facing monitoring and logging services.
  - Designed and implemented the *Orchard* monitoring platform for Swisscom's *Application Cloud*.
  - Defined and implemented integrations between Jira and OpsGenie for alerting of user-reported incidents.
  - Managed business relationship and implementated Swisscom-wide use of OpsGenie for alert management.
  - Managed engineering relationship with VMware for integration of their products in Swisscom's monitoring systems.

CFEngine AS

2011 – 2014 *Norway/U.S.A. (remote)*

Senior Security Advisor and Product Manager — *Oct 2011 – Jun 2014*

- Developed the CFEngine language roadmap and security strategy.
- Acted as 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.
- Published the book Learning CFEngine (O'Reilly Media), which was used for promotion and education.
- Established and led the *CFEngine Design Center* project through its initial implementation phase.

HP Enterprise Services — 2009 – 2011 — Mexico

Account Security Officer and Service Delivery Consultant — Nov 2009 – Oct 2011

- Managed security-related topics for HP enterprise customers in Mexico.
- Initiated, advised and managed security-related projects.
- Coordinated communication among technical teams involved in security initiatives.
- Managed all security-related aspects of the design, implementation and delivery of IT Outsourcing projects.
- Analyzed, designed and implementated solutions in the areas of 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

- Established and participated in research projects in intrusion detection, malware containment, and virtualization security, 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.
- Managed security services for the whole University, including incident response, security information, auditing and teaching.
- Established 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, Purdue University — *West Lafayette, IN, U.S.A.* — *1996–2001*

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, Teaching and References

Available upon request.

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