

# Diego Zamboni

SENIOR SECURITY ARCHITECT · ORGANIZATIONAL LEADER · COMPUTER SCIENTIST

[diego@zzamboni.org](mailto:diego@zzamboni.org) · [zzamboni.org](https://www.zzamboni.org) · [zzamboni](#) · [zzamboni](#) · [zzamboni](#)

I am a Senior Enterprise Security Architect, Organizational Leader and Computer Scientist with 32 years of experience building systems and leading teams and projects. I specialize in the areas of Computer Security, Cloud Computing and Configuration Management. I have experience working with and leading remote teams. I possess a strong combination of leadership, conceptual and technical skills with excellent communication abilities.

## Key skills

<b>Leadership</b>	32 years of team and project leadership experience; IT Enterprise Architecture.
<b>Computer Security</b>	Enterprise security architecture; virtualization and cloud computing security; risk management and compliance; intrusion detection and prevention; software security and secure software development.
<b>Cloud Computing</b>	AWS architecture, infrastructure, development and security.
<b>Communications and Research</b>	Excellent written and spoken communication skills; research and teaching experience.
<b>Research</b>	Ph.D. in Computer Science, 9 years of experience at IBM Research.
<b>Languages</b>	Spanish (native), English (100%), German (B1 level).

## Experience

### Amazon Web Services

2021 – Present

Switzerland

SENIOR GLOBAL SECURITY ARCHITECT

Oct 2021 – Present

- I work with customers and within AWS to increase security awareness, design and build secure solutions, mentor and develop colleagues and customers in security best practices.
- As Lead Security Architect at the [Stellantis Virtual Engineering Workbench](#) (VEW) project, I have:
  - Established the VEW security workstream, define and promote security best practices and drive activities related to risk analysis, threat modeling and mitigation.
  - Established measurement mechanisms for status and metrics for security activities, which provide visibility to both technical and business stakeholders.
  - Established a *Security Champions* program to promote and transfer security knowledge.
  - Define and track security features to fulfill customer business requirements and AWS best practices.

GLOBAL SECURITY ARCHITECT

Sep 2021 – Sep 2022

- Worked with AWS global customers to improve security posture and promote secure design and implementation practices.
- In the [Volkswagen Digital Production Platform \(DPP\)](#) program, I established scalable and durable mechanisms to enable DPP partners to work securely in the DPP program. I also created and promoted security learning materials tailored for various roles within the project, and increased security awareness and knowledge by promoting a *Security Guardians* initiative across the organization.

### Swisscom

2014 – 2021

Switzerland/U.S.A.

ENTERPRISE ARCHITECT AND IT CLOUDS SOLUTION SECURITY ARCHITECT

Apr 2019 – Sep 2019

- As a Solution Security Architect for IT Clouds, I was a member of the *Swisscom IT Clouds* leadership team:
  - I defined and manage yearly KPIs and the security features and characteristics of [Swisscom's cloud offerings](#).
  - I ensured 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 was the point of contact for CISO-level interactions with Swisscom's cloud customers.
- As an Enterprise Architect, I defined future Swisscom products and solutions as part of the *Swisscom Enterprise Architecture* team.

- 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 evolving cloud offerings:
  - Unified diverse monitoring components into a cohesive framework, reducing costs and increasing efficiency by 20%.
  - Defined architecture and implemented 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 implemented 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.
- 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 and abroad.
- Managed all security-related aspects of the design, implementation and delivery of IT Outsourcing projects.
- Analyzed, designed and implemented 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 developed 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.

**National Autonomous University of Mexico (UNAM)**

1991 – 1996

Mexico

HEAD OF [COMPUTER SECURITY AREA](#) AND SYSTEM ADMINISTRATOR

Nov 1991 – Aug 1996

- Established UNAM's first [Intrusion Response Team](#), which has since evolved into a much larger organization.
- Managed security services for the supercomputing organization and for the whole University, including incident response, security information, auditing and teaching.
- Established the [International Computer Security Day](#), which 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).
- System Administrator at UNAM's Supercomputing Center, managing UNAM's [Cray Y-MP Supercomputer](#) and related systems.

## 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



## Research, Publications, Teaching and References

Books: [Learning CFEngine](#) (2012), [Learning Hammerspoon](#) (2018), [Literate Configuration](#) (2019), [Publishing with Emacs, Org-mode and Leanpub](#) (2021).

References available upon request. Full Curriculum Vitæ available at <https://zzamboni.org/vita/>.