

# Diego Zamboni



✉ diego@zzamboni.org | 🏠 zzamboni.org | 📍 Zurich, CH | 🌐 zzamboni |  
📖 zzamboni | 📱 zzamboni | 🦋 zzamboni.org

CISO • Organizational Leader • Security Expert • Computer Scientist

Senior computer scientist, security expert and organizational leader with 30 years of experience across security governance, cloud security architecture, research and engineering. I combine strategic leadership, technical depth and clear communication to help organizations design secure systems, scale teams and deliver measurable outcomes.

## Professional Highlights

### Management and leadership, IT security, cloud computing

- Chief Information Security Officer for Governance at Avaloq, defining and managing Avaloq's global ISO27001-certified Information Security Management System
- Managed security architecture at the Stellantis *Virtual Engineering Workbench* project. Worked with Stellantis CISO and business stakeholders to define governance, establish security best practices and drive risk analysis, threat modeling and mitigation.
- Established scalable and durable mechanisms to enable partners to work securely in the Volkswagen Digital Production Platform (DPP) program.
- Managed security architecture, risk management, data governance and compliance (ISO27001, ISAE3402/3000, etc.) for Swisscom's Cloud platforms.
- Established and led the Swisscom IT Clouds security community of practice.
- Established and led the *Health and State Management* team at Swisscom to design, implement and operate a framework for scalable monitoring, logging and alerting for Swisscom's Cloud platforms.
- Established and led the first computer security organization at UNAM, which has grown into the university's Information Security Coordination (UNAM-CERT).
- Managed IT security customer relationships at HP Enterprise Services, including overseeing the activities of operational and engineering teams, risk and compliance management, requirements discussion and reporting.

### Research, architecture and design

- Designed the *Orchard* monitoring framework for Swisscom's *Application Cloud* platform, and led the team that implemented it and brought it into production.
- Designed and implemented the *Billy Goat* malware capture and analysis system at IBM.

## Experience



Switzerland  
Jan 2024 - Present

Lead Avaloq's global CISO Governance team and define and monitor the company's Information Security Management System.

- Own security policy and governance direction.
- Provide second-line oversight of first-line security functions.
- Drive compliance monitoring and control effectiveness in a regulated fintech environment.



Switzerland  
Sep 2021 - Dec 2023

Worked with global AWS customers and internal teams to improve security posture, define secure architecture patterns and scale security awareness.

- Led security architecture in the Stellantis Virtual Engineering Workbench program.
- Established security workstreams, metrics and reporting for business and technical stakeholders.
- Helped launch and scale Security Champions and Security Guardians initiatives.
- Supported secure collaboration mechanisms for the Volkswagen Digital Production Platform.



Switzerland  
Apr 2019 - Sep 2021

Led security architecture, risk and compliance activities for Swisscom cloud platforms across multiple services.

- Directed compliance and governance activities including ISO27001, ISAE3402/3000 and GDPR requirements.
- Built and led a Security Champions community across IT Clouds teams.
- Coordinated threat modeling, audits, penetration testing and vulnerability management.

TEAM LEAD & PRODUCT OWNER FOR HEALTH & STATE MANAGEMENT

Aug 2014 - Apr 2019

Built and led the Health and State Management team for Swisscom cloud platforms.

- Owned roadmap and prioritization with product managers and stakeholders.
- Defined and delivered platform-wide monitoring, logging and alerting capabilities.
- Led the *Orchard* project through its implementation, production release and further improvements and development.



**CFEngine AS**  
PRODUCT MANAGER

Norway/U.S.A. (remote)  
Oct 2011 - Jun 2014

- CFEngine Advocate, with a special focus on security.
- Managed the CFEngine language roadmap.
- Created and led the CFEngine Design Center project, which was the foundation for the current CFEngine Build service.
- Coordinated the work on CFEngine third-party integration (e.g. AWS EC2, VMware, Docker and OpenStack).
- Wrote the book *Learning CFEngine 3*, published by O'Reilly Media, which became the de facto introductory text to CFEngine.



**IBM Zurich Research Lab**  
RESEARCH STAFF MEMBER

Switzerland

Oct 2001 - Oct 2009

Member of IBM Zurich's Global Security Analysis Laboratory, working on intrusion detection, malware containment and virtualization security research.



**National Autonomous University of Mexico (UNAM)**  
FOUNDER AND LEAD OF COMPUTER SECURITY AREA

Mexico

Aug 1995 - Aug 1996

- Established UNAM's *Computer Security Area*, the University's first team dedicated to computer security, which has evolved into the *Information Security Organization (UNAM-CERT)*.
- Managed up to nine people working on different projects related to computer security.
- Provided security services to the whole University, including incident response, security information, auditing and teaching.

## Education



**Purdue University**  
PH.D. IN COMPUTER SCIENCE

West Lafayette, IN, U.S.A.

Aug 1996 - Aug 2001

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



**Purdue University**  
M.S. IN COMPUTER SCIENCE

West Lafayette, IN, U.S.A.

Aug 1996 - May 1998

- Advisor: Eugene H. Spafford



**National Autonomous University of Mexico (UNAM)**  
BACHELOR'S DEGREE IN COMPUTER ENGINEERING

Mexico City, Mexico

Aug 1989 - Jul 1995

- Thesis: UNAM/Cray Project for Security in the Unix Operating System (in Spanish, original title: *Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix*)

## Certifications

See full list on Credly ([www.credly.com/users/zzamboni](http://www.credly.com/users/zzamboni))



**Certified Information Systems Security Professional (CISSP)**  
ISC2

Apr 2019

## Selected Research

See the *online publications list* ([zzamboni.org/vita/publications](http://zzamboni.org/vita/publications)) for publication details.

### Billy Goat: Active worm detection and capture

2002 - 2008

IBM RESEARCH

- Pioneered active worm-capture technology that became the foundation for modern honeypots and honeynets
- Designed system to simulate thousands of vulnerable hosts to attract and capture propagating worms
- Implemented automated analysis to extract signatures and update intrusion detection/prevention systems
- Publications: [18], [25]

### Ph.D. Thesis: Using internal sensors and embedded detectors for intrusion detection

1996 - 2001

PURDUE UNIVERSITY

- Investigated novel approaches to data collection for intrusion detection systems
- Implemented and evaluated internal sensors and embedded detectors as data collection mechanisms
- Analyzed trade-offs and effectiveness of different sensor placement strategies in IDS architectures
- Publications: [11], [19], [20], [27], [26], [32]

## Software

### Open-source software projects

- GitHub: [github.com/zzamboni](https://github.com/zzamboni)

## Honors & Awards

---

- May 2020 **IEEE Security & Privacy Test of Time Award (IEEE S&P page, CERIAS blog post)**, IEEE
- 2010 **CFEngine Champion**, CFEngine AS
- May 1996 **Fulbright Scholarship (for pursuing Ph.D. studies at Purdue University)**, Fulbright Program and CONACYT

## Selected publications

---

Full list online ([zzamboni.org/vita/publications](https://zzamboni.org/vita/publications))

### Books

- [1] Diego Zamboni. *Publishing with Emacs, Org-mode and Leanpub*. Leanpub, June 2020.
- [2] Diego Zamboni. *Learning CFEngine*. O'Reilly Media, Inc. 2012–2017, afterwards self-published, 2012.

### Editorial Activities

- [3] Diego Zamboni and Christopher Kruegel, editors. *Proceedings of the Recent Advances in Intrusion Detection (RAID): 9th International Symposium*. Lecture Notes in Computer Science. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2006.

### Theses

- [4] Diego Zamboni. "Using Internal Sensors for Computer Intrusion Detection". CERIAS TR 2001-42. PhD thesis, West Lafayette, IN: Purdue University, August 2001.

### Refereed Papers

- [5] James Riordan, Diego Zamboni, and Yann Duponchel. "Building and deploying Billy Goat, a worm-detection system". In: *Proceedings of the 18th Annual FIRST Conference*. June 2006.
- [6] Florian Kerschbaum, Eugene H. Spafford, and Diego Zamboni. "Using internal sensors and embedded detectors for intrusion detection". In: *Journal of Computer Security* 10.1,2 (2002), pages 23–70.
- [7] Christoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford, Aurobindo Sundaram, and Diego Zamboni. "Analysis of a Denial of Service Attack on TCP". In: *Proceedings of the 1997 IEEE Symposium on Security and Privacy*. Awarded the 2020 IEEE Security & Privacy Test of Time Award. IEEE Computer Society, IEEE Computer Society Press, May 1997. pages 208–223.

## Skills

---

**Leadership** 32 years of multidisciplinary team and project leadership experience · IT Enterprise Architecture · Scaled Agile Framework (SAFe)

**Information and Cyber Security** Enterprise security governance · Enterprise security architecture · Virtualization and cloud computing security · Risk management and compliance · Intrusion detection and prevention · Software security and secure software development · ISO27001

**Technology** Broad and deep IT expertise · Cloud computing · Computer security · Operating systems · Networking · Configuration management · Software & services development · Programming languages

**Research** Ph.D. in Computer Science · 9 years of experience at IBM Research

**Communication** Excellent written and spoken communication skills · Extensive public speaking experience · Professional writing and teaching experience

## Languages

---

**Spanish** Native  
**English** Full proficiency  
**German** Intermediate proficiency (B2 level)

## References

---

Available by request