J. Jair C. Santanna

PROFESSIONAL SUMMARY

- Cybersecurity expert with an in-depth knowledge of cybercriminal phenomena and emerging cyber threats.
- Specialised in leveraging advanced data analysis techniques (including ML, AI, S/LLM) to address complex cybersecurity challenges.
- Proven successful experience collaborating with Law Enforcement, including two phases of Operation PowerOff.
- Creator of successful National and Europe-wide initiatives to combat DDoS attacks.
- Results-oriented professional with strong communication skills and a can-do mentality.

CONTACT

✉ jairsantanna@gmail.com
🌐 www.linkedin.com/in/jjcsantanna
📱 +31 682508224

EDUCATION

PhD - Computer Science
University of Twente
2013 - 2017 (Netherlands)

MSc - Computer Science
Federal University of Rio Grande do Sul
2007-2010 (Brazil)

BSc - Computer Engineering
Federal University of Pará
2001-2007 (Brazil)

LANGUAGES

- Portuguese (Native)
- English (Proficient)
- Dutch (Basic)

SKILLS

- In-depth Cybersecurity expertise
- Advanced Data Analytics
- Programming & Automation
- Analytical & Investigative Thinking
- Leadership & Project Management
- Communication & Collaboration
- Adaptability
- Creativity & Innovation

ACCOMPLISHMENTS

- **2018, 2023:** My PhD thesis and scripts were used in the successful international *'Operation PowerOff'*.
- **2018:** Won as the *'Best Science Communicator of the Netherlands'* by FameLab competition.
- **2018:** Selected among the *'Top Young Talented Engineers of the Netherlands'* by Het Koninklijk Instituut Van Ingenieurs
- **2020:** The DDoS Clearing House pilot was deployed in several European countries, including the Netherlands with the name of *Anti-DDoS-Coalitie (nomoreddos.org)*.
- **2021:** The DDoS Clearing House Pilot got selected as *'key innovation' by the European Commission.*
- **2024:** Northwave won by Microsoft the *'Partner of the year in Security'* title under my leadership of the Cloud proposition.

WORK EXPERIENCE

Principal Researcher & Innovator

Northwave Cyber Security *Jan 2024 - Current*

Drive innovation in cybersecurity by preparing strategic plans, developing cutting-edge prototypes, and leading multidisciplinary teams to transform how organizations detect, prevent, and respond to cyber threats using data mining, machine learning, and AI.
Public projects include:
• Automation of phishing email analysis and escalation (including LLMs)
• Adaptive anomaly detection for identity-related attacks (using ML)
• Automation of leaked dataset analysis from cybercriminals (including LLMs & RAG)

Cloud Security Lead

Northwave Cyber Security *Dec 2019 - Dec 2023*

Develop and implement strategic Cloud Security innovations using the latest technologies to drive business transformation at scale. Deploy a cloud-based SIEM for a Security Operations Center. Design customized automated solutions to enhance client operations and deliver projects with advanced automation for efficiency and scalability. Collaborate with teams (including Security Operations and Incident Response) to create pioneering security solutions that build resilience and generate social impact, while engaging with senior stakeholders, clients, and technology partners to align solutions with strategic goals.

Assistant Professor

University of Twente *Dec 2019 - Current ('Guest')*
Dec 2017 - Dec 2019

Research: Initially focused on the investigation and mitigation of DDoS attacks; broadened to Cloud Security; currently focused on the use of AI to automate cyber-related processes.
Teaching: Dozens courses, hundreds of lectures, and thousands of students. Currently, I offer two highly practical, data-driven courses: "Digital Forensics for Cybercrime" and "Secure Cloud Computing."
Project Management: Led two national projects on DDoSDB and DDoS fingerprints with multiple team members; managing a pilot in a European project on DDoS Clearing House with 42 members.
Supervision: 1 PhD, 12 MSc, and 16 BSc students. Two students are now Digital Experts at the Dutch Team High Tech Crime Unit.

Digital Forensic Technical Support (Voluntary)

Politie Midden Nederland *Jan 2020, Oct-Nov 2020, Aug-Dec 2022*
Team High Tech Crime politie unit *Dec 2017 - Dec 2019*

Provide scripts and large datasets that I collected, classified, and analyzed to create actionable threat intelligence related to DDoS-as-a-service providers (Booters). I developed and implemented fast methodologies to facilitate the analysis and attribution of DDoS attacks. All my contributions were used in multiple PowerOff operations (2018 and 2023).

Visiting Researcher

University of Southern California, USA *Nov 2016*
Cambridge CyberCrime Center, UK *Jul 2018*

Actively collaborate with the cybersecurity research community on DDoS attack detection, mitigation, and attribution.

(Invited) Guest Lecturer

I have demonstrated thought leadership and passion for science communication. I have delivered over a hundred guest lectures in academic, law enforcement, and industry organizations over the last decade. The main topics included DDoS attacks, ransomware, cloud security, and AI in/for cybersecurity.