europass

Simone Pio Tosatto

Date of birth: 29/12/2001 | **Nationality:** Italian | **Gender:** Male | **Phone number:** (+39) 3473681025 (Mobile) | **Email address:** tosatto.simonepio@gmail.com | **Website:** https://simo56.github.io/MyPortfolio/ | **LinkedIn:** https://www.linkedin.com/in/simonepiotosatto/ | **GitHub:** https://github.com/Simo56 |

Address: Senftlstraße 1A, 81541, Munich, Bavaria, Germany (Home)

ABOUT ME

I am a determined student with a passion for cybersecurity, a fervent curiosity for blockchain technology, and a keen interest in digital forensics. I have developed my skills through self-guided learning, exploring topics such as Solidity programming and continuously pursuing opportunities to deepen my knowledge in the field.
In addition to my dedication to technology, I have an athletic side that has allowed me to represent Italy in multiple European beach volleyball championships. My experience in winning the Austrian national beach volleyball championship U21 has contributed to shaping my mindset, teaching me the importance of teamwork, discipline, and adaptability.
I believe that the combination of technical skills and qualities acquired through sports has prepared me for professional challenges. I am excited to further explore opportunities in the realm of cybersecurity and blockchain, contributing to the development of innovative and secure solutions for the digital challenges of the future.

WORK EXPERIENCE

06/2016 – 09/2023 Caorle, Italy
DEVELOPER AND OFFICE EMPLOYEE TOSATTOFRUIT S.R.L.

- Managed network infrastructure
- Managed the security posture
- Designed the platform for customer order management.

10/2021 – 02/2022 Montebelluna, Italy
HIGH SCHOOL TEACHER IIS EINAUDI SCARPA

- Taught Systems and Networks to high school juniors
- Taught Computer Science classes with first, second and fourth-year students.

05/2018 – 08/2019 Asolo, Italy
DEVELOPER AND DIGITAL FORENSICS ANALYST SECURCUBE

- Designed and developed BTS Tracker as part of a team (an application for the analysis of cell towers and mobile data extraction)
- Conducted Forensic Analyses using Kali Linux, Paladin OS and other tools.

06/2024 – CURRENT München, Germany
VOLLEYBALL COACH TSV MÜNCHEN-OST

- Planned, organized, and conducted team training sessions to improve technical, tactical, and physical skills.
- Developed game strategies and provided in-game coaching during matchdays.
- Motivated and mentored players to foster teamwork, discipline, and continuous improvement.

EDUCATION AND TRAINING

10/2023 – CURRENT Munich, Bavaria, Germany

MASTER OF SCIENCE, CYBERSECURITY Hochschule der Bayerischen Wirtschaft (HDBW) gGmbH

Website https://www.hdbw-hochschule.de/

09/2020 – 10/2023 Milan, Italy

BACHELOR'S DEGREE, SYSTEM AND NETWORK SECURITY Università degli Studi di Milano

Website https://www.unimi.it

09/2015 – 07/2020 Montebelluna, Italy

DIPLOMA ISTITUTO TECNICO E PROFESSIONALE, INFORMATICA E TELECOMUNICAZIONI IIS Einaudi-Scarpa

Website https://www.iiseinaudiscarpa.edu.it/ | **Field of study** Information and Communication Technologies |

Final grade 100/100

LANGUAGE SKILLS

Mother tongue(s): **ITALIAN**

Other language(s):

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken production	Spoken interaction	
ENGLISH	C2	C2	C2	C2	C2
SPANISH	B1	B1	B1	B1	B1
GERMAN	A1	A1	A1	A1	A1

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

VOLUNTEERING

02/2024 – 05/2024 Munich, Bavaria

Volunteer - ReDI School of Digital Integration

During the Spring 2024 semester, I volunteered as a teacher at the ReDI School of Digital Integration in Munich, contributing to the Introduction to Coding, Data, and Design Course. My role required teaching, planning, and coordinating various tasks.

In this course, I taught students the basics of programming, emphasizing independent learning through online resources. The curriculum covered writing simple algorithms, understanding data structures and types in Python, running commands in the command line, and creating small web apps using HTML and CSS.
This course aims to empower high-need adult students—particularly women—through a journey in digital education.

PROJECTS

10/2024 – 11/2024

NAIR (NeuralAgent for Intelligence Reconnaissance)

NeuralAgent for Intelligence Reconnaissance is a project that detects Wildfires using Artificial Intelligence employed on Copernicus Sentinel 2 satellite images. After getting the precise coordinates, we can feed them to deploy a swarm of AI-powered smart drones that can provide real-time quality data.

Link https://github.com/ksanda5/NAIR

01/2024 – 02/2024

AST-iPyNB

This repository contains code for a malware detector using a feedforward neural network implemented with scikit-learn. The detector is designed to classify PE Files as either benign or containing malware.

Link https://github.com/Simo56/AST-iPyNB

10/2023 – 12/2023

APT-TS

This repository hosts an automated set of tools for penetration testing developed using Typescript and Node.js with Express. The suite is designed to automate various penetration testing tasks, simplifying the security assessment of systems and applications.

Link https://github.com/Simo56/APT-TS

CryptoNovusRacing

I created this Ethereum Smart Contract, CryptoNovusRacing, using Solidity 0.8.0. This innovative smart contract generates unique NFT cars with random parts and rarities, providing users with an exciting and unique collectible experience. The project includes dynamic creation, adjustable costs, transparent ownership tracking, and integration with IPFS for metadata storage. As the project founder, I implemented features for contract configurability and secure fund withdrawal. The DApp that I've developed with Web3.js, allows users to smoothly mint and display their unique NFT cars on the Ethereum blockchain.

Link https://github.com/Simo56/CryptoNovusRacing_Public

LadonCloudAgent [My Bachelor's Thesis]

In the context of the growing significance of privacy, digital identity, and cybersecurity, I have developed "Ladon," an innovative agent for self-sovereign identity (SSI). This decentralized model of digital identity management leverages Hyperledger Aries and blockchain technology, incorporating distributed ledgers, asymmetric encryption, Zero-Knowledge Proofs (ZKPs), and Decentralized Identifiers (DIDs).

The project is implemented in TypeScript and is based on a Node.js web server with Express and npm. The approach focuses on the practical application of Hyperledger Aries technologies and their integration into the ecosystem. Throughout development, I adhered to best practices in digital identity management, decentralization, cybersecurity, and user control over their digital identity.

The thesis covers the fundamentals of digital identities, major innovations, comparisons with current methodologies, and an exploration of blockchain technology and Hyperledger Aries. Ladon's architecture, features, and its role in the blockchain-based self-sovereign identity space are examined.

This implementation contributes to understanding the potential of blockchain-based SSI, providing a practical example of technology application. It promotes user autonomy and control over their digital identity, emphasizing the key role of Hyperledger Aries in providing a robust and scalable framework for digital identity management in an increasingly decentralized era. This opens new possibilities for secure and private digital interactions based on blockchain technology.

Link https://github.com/Simo56/LadonCloudAgent

"From Anti-Cheat to Spying Software? An In-Depth Malware Analysis of Vanguard's Kernel-Level Operations" [My Master's Thesis]

Kernel-level software, which operates with the highest privileges in a system, poses significant risks if misused, as it can access and control virtually every aspect of a user's computer.
Video games are among the most widely used software applications, and developers must find ways to combat in-game cheating. To address this, Riot Games developed Vanguard, a kernel-level anti-cheat software that has attracted attention and controversy due to its deep integration into users' systems, raising concerns about potential privacy violations and data security risks. As explored in this thesis, Vanguard is installed as a kernel-mode driver and runs as an on-boot application, leading to complaints from users and gamers. Understanding the implications of such software is essential in an era where digital privacy is increasingly under threat.
The central research question of this thesis is: ***To what extent does Vanguard pose a threat to user privacy and security, and how can malware analysis techniques be used to uncover these risks?***
This question has been addressed through a combination of static, dynamic, and policy analysis methods, utilizing tools such as IDA, WinDbg, Ghidra, peTree, and Process Monitor to thoroughly investigate the software's operations. It also explored bypasses and exploits to better understand the context in which Vanguard operates.

This research strived to maintain objectivity, avoiding bias toward either Riot Games or user perspectives, to ensure the most accurate and insightful results. It aimed to present facts and raise important security-related questions, encouraging informed and critical consideration of kernel-level software and privacy concerns.