europass Curriculum vitae

PERSONAL INFORMATION

Muntea Andrei-Marius

munteaandrei17@gmail.com

https://github.com/AndreiMuntea

Gender Male | Date of birth | Nationality Romanian

WORK EXPERIENCE

2023 – Present — Senior Software Engineer, Bitdefender

I'm currently working as part of Bitdefender's Active Threat Control team, where we're developing the behavioral analysis module. My responsibilities range from developing new features in our Windows Kernel driver component, or BSODs and Crashes analysis using WinDbg, to reverse engineering malware.

2021 – 2023 — Software Engineer, CrowdStrike

I was part of CrowdStrike's Data Security team, Insider Risk project. We built the module responsible for detecting insider threats. My biggest achievement was to reduce the scan duration with almost 15 percent and come up with solutions for file sharing and access issues. I was also responsible for leading an initiative that added source code classification functionality in Windows agent. I was also involved in architecture discussions regarding the project and helping with the interviewing process.

2017 – 2021 — Software Engineer, Bitdefender

I worked at Bitdefender in Active Threat Control team where we were developing the behavioral analysis module. My responsibilities ranged from developing new features in our Windows Kernel driver component, or BSODs and Crashes analysis using WinDbg, to reverse engineering malware. My biggest achievement was helping the team transition from C to C++, implementing multiple STL structures and adapting them to work in both user mode and kernel mode, thus making the testing process easier. I also gave multiple presentations regarding various topics to my team, and often got involved in internship trainings.

2016 — Software Engineer Intern, Neusoft EDC

As part of my internship project, I helped develop a C++ application for a vending machine.

EDUCATION AND TRAINING

2023 – Present — PhD – Thesis Title: "Malware Detection and Analysis in Distributed Ecosystems: Exploring Multi-Entity Threats", Technical University of Cluj-Napoca

Currently, I am pursuing a 4-year PhD program at Technical University of Cluj-Napoca, specialized in Computer and Information Systems Security.

2018 – 2020 — Master's Degree in Computer and Information Systems Security, Technical University of Cluj-Napoca

For my Master's degree, my thesis was a threat model for Windows inter-process communication through ALPC ports. I reverse engineered the ALPC framework as it is completely undocumented, and managed to write an antivirus-evasive application which simulates ransomware behavior using standard ALPC ports.

2015 – 2018

Bachelor's Degree at Faculty of Mathematics and Computer Science, Babeș-Bolyai University

For my Bachelor's degree, I implemented a real time behavioral analysis module to monitor running applications. It included a kernel mode driver and a user mode component to log the actions received, and also an experimental Hidden Markov Model classifier to alert the user of suspicious behavior.

PERSONAL SKILLS

Mother tongue: Romanian

Other languages

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	B2	B2	B2	B2	B2

Levels: A1 and A2: Basic user – B1 and B2: Independent user – C1 and C2: Proficient user
Common European Framework of Reference for Languages

Digital competences

SELF-ASSESSMENT				
Information Processing	Communication	Content creation	Safety	Problem solving
Proficient user	Proficient user	Proficient user	Proficient user	Proficient user

Digital competences - Self-assessment grid

Hobbies: I run a YouTube channel dedicated to teaching the fundamentals of programming, with all the content presented in Romanian – https://www.youtube.com/@InfoCuAndrei

Driving licence: B

ADDITIONAL INFORMATION

Publications: *Monitoring of RPC Messages with ALPC-Level API Hooking*, AQTR Cluj-Napoca (2024), DOI: 10.1109/AQTR61889.2024.10554183