Europass CURRICULUM VITAE

Personal information

Name	Marius-Ştefăniţă PREDA
Address	Bucharest, Sector 1, Romania
Telephone	+40-785-257-440
E-mail	marius.preda@mta.ro
Nationality	Romanian
Date of birth	17th July 1989

Work experience

Dates	December 2012 -
Occupation or position held	Cyber Security Engineer
Main activities and responsibilities	Incident Response, Security monitoring, Digital Investigations
Name and address of employer	Ministry of Defence 9-11 Izvor Street, Sector 5, Bucharest www.mapn.ro
Type of business or sector	Network Security

Dates	May 2013 -
Occupation or position held	Digital Investigations Expert
Main activities and responsibilities	Incident Response, Penetration Testing, Malware Analysis, Digital Investigations
Name and address of employer	National Cyber Security Directorate - DNSC 22nd Italian Street, 2nd Sector, Bucharest, Romania www.dnsc.ro
Type of business or sector	Cyber Security

Education and training

Dates	2016 -
Title of qualification awarded	Doctoral Degree
Principal subjects/occupational skills covered	Computer Science and Information Technology *Internet of Things Security and Privacy*

Name and type of organisation providing education and training	Military Technical Academy Bucharest, Romania
Dates	2018 - 2019
Title of qualification awarded	Cyber Security Fundamentals and Cyber Security Defense Certifications
Principal subjects/occupational skills covered	Computer Security, Network Security, Secure management of Systems, Network Traffic Analysis, Computer Forensics, Cyber Security Incident Response and Recovery
Name and type of organisation providing education and training	Naval Postgraduate School Monterey, CA, USA
Dates	2013 – 2015
Title of qualification awarded	Master's Degree
Principal subjects/occupational skills covered	Electronics applied in robotics and automation *Remote Command & Control with PLCs*
Name and type of organisation providing education and training	Military Technical Academy Bucharest, Romania
Dates	2008 - 2012
Title of qualification awarded	Bachelor's Degree
Principal subjects/occupational skills covered	Electronics and Telecommunications Engineering *Remote Command & Control with microcontrollers*
Name and type of organisation providing education and training	Military Technical Academy Bucharest, Romania

Personal skills and competences

Mother language	Romanian									
Other languages										
Self-assessment	Understanding				Speaking				Writing	
European level	Listening		Reading		Spoken interaction		Spoken production			
English	C1	Proficient user	C1	Proficient user	C1	Proficient user	C1	Proficient user	C1	Proficient user
French	B2	Independent user	B2	Independent user	B2	Independent user	B2	Independent user	B2	Independent user

Social skills and competences	Team spirit Ability to adapt to changes in work environment Good communications skills

Organisational skills and competences

Leadership
Sense of organisation
Good experience in project or team management

Technical skills and competences

Good experience in **Incident Response**

- Respond to cyber security incidents while capturing essential details and artefacts
- Handle cyber security incidents, including performing lead investigator duties, from detection through to completion including post-mortem root cause analysis
- Utilise sensor data and correlated logs containing IDS/IPS, AV, web application firewalls, Operating System events, web proxy, and similar data to establish context and scope
- Working with Request Trackers systems, incident handling and malware analysis tools
- Working knowledge of the information security threat landscape (attack vectors and tools, best practices for securing systems and networks)

Good experience in **Network and Web Applications Penetration Testing**

- Planning, executing and reporting penetration tests
- Following penetration test methodology and using the tools associated for each case (network pentest, web application pentest, wireless pentest etc.)
- Working with automated tools or scanners like nmap, netcat, Burp suite, Scapy, Acunetix, Nessus, Core Impact, Metasploit, meterpreter etc.
- Working with tools for each phase of the test from reconnaissance to post exploitation
- Using scripting languages like Python for task automation and increase test efficiency (fuzzing, packet crafting, etc.)
- Manual testing for particular cases and vulnerability validation

Good experience in **Digital Forensics, Investigations and Malware Analysis**

- Performing digital forensics/investigation, including analysing system artefacts (file system, memory, running processes, network connections) for indicators of infection/compromise
- Performing Live Incident Response (OoV), digital evidence collection, processing and analysis using tools like EnCase, open source tools and operating system specific features.

Embedded Systems Programming (MCU, DSPIC, PLC, SCADA)

Computer and network training	Cyber Diplomacy (UN) Integrating Cyber Considerations into Operational Planning (CCD CoE) Counter Terrorism Attacking the Network (DAT CoE) FOR578: Cyber Threat Intelligence (SANS) Cyber Security Fundamentals and Defense (NPS) SEC660: Advanced Penetration Testing, Exploit Writing and Ethical Hacking (SANS) SEC560: Network Penetration Testing and Ethical Hacking (SANS) Advanced Malware Analysis (MANDIANT) Digital Forensic Training (ViewTheNet) Certified Ethical Hacking (EC-COUNCIL) Certified Hacking Forensics Investigator (EC-COUNCIL) Introduction to Intelligence-Driven Defence (Lockheed Martin) Advanced Intelligence-Driven Defence (Lockheed Martin) CoreImpact Certified Professional (CORE SECURITY) Cisco Network Fundamentals APT (ENISA training) Honeypots (ENISA training) Botnets fundaments (ENISA training) Participation at ENISA Cyber Europe Exercise (2014, 2016, 2018) Participation at NATO Cyber Defence Exercise Cyber Coalition (2014, 2015, 2016)
Computer skills and competences	Working with Incident Response, Penetration Testing and Malware Analysis plans, methodologies, tools and techniques, reports, etc. Security Information and Event Management user skills (ArcSight) Good skills of using VMware virtualization solutions (WorkStation, ESXi, vCenter, vSphere, Horizon) Overall understanding of multiple programming and scripting languages like C/C++, PHP, HTML, Java, Python, Perl, ASM, etc. Good skills of using Windows OS, Linux/Unix – basic shell scripting Good knowledge of Computer Networks (CCNA1) Microsoft Office Suite (Word, Excel, Outlook, Access, Power Point)
Other skills and competences	**Publications** Author of „IoT botnet anomaly detection using unsupervised deep learning”, Electronics, vol. 10, no. 16, MDPI, 2021 Author of “Internet of Things Traffic Characterization using flow and packet analysis”, 12th International Conference Electronic, Computers and Artificial Intelligence Conference (ECAI), 2020; Author of "Simulating RPL Attacks in 6lowpan for Detection Purposes," 2020 13th International Conference on Communications (COMM), Bucharest, Romania, 2020, pp. 239-245, doi: 10.1109/COMM48946.2020.9142026. Author of “Digital Forensics of Internet of Things - Smart Heating System Investigation”, Journal of Military Technology, Vol. 3, No. 1, Jun. 2020. Author of “National Security Implications of 5G”, INFOSFERA, 2020.
Driving licence	B Category