Miron Gabriel GHEORGHE

108, 13 September Street – Bucharest, Romania
miron.gheorghe@purple8-solutions.com
miron_gheorghe@yahoo.com

WORK EXPERIENCE

Sep 2022 – present

Cybersecurity Consultant

Eau de Web, Bucharest, www.eaudeweb.ro
Main activities and responsibilities:

- Providing IT consultancy for IoT and Cybersecurity services,
- Perform penetration testing, vulnerability assessment, source code analysis and forensic analysis services
- Perform quality assurance

Aug 2022 – present

Cybersecurity Consultant

Î.C.S Reliable Solutions Distributor S.R.L. Chisinau, Republic of Moldova www.rsd.md
Main activities and responsibilities:

- Providing IT consultancy for IoT and Cybersecurity services,
- Perform penetration testing, vulnerability assessment, source code analysis and forensic analysis services
- IBM solutions implementation consultant
- Perform quality assurance

Oct 2019 – present

Owner and CEO

Purple8 Solutions, Bucharest
Main activities and responsibilities:

- Act as Project Manager/ QA and security trainer
- Providing IT consultancy for IoT and Cybersecurity services,
- Perform penetration testing, vulnerability assessment, source code analysis and forensic analysis services

Projects:

[2022] ***Cybersecurity consulting services*** *for Bynet Consulting SRL*

- *Perform vulnerability services and penetration services for web and mobile app*
- *Perform vulnerability services and penetration Services for network and WiFI infrastructure*
- *Perform source code analysis for internal app*.

Tools: Kali Linux, Appscan, Fortify, Nexpose, Acunetix, Burp, Aircrack-ng

[2022] ***Penetration testing services*** *for MIXT ENERGY SRL*

- *Perform vulnerability services and penetration services for web and mobile app*
- *Perform vulnerability services and penetration Services for IoT infrastructure*

Tools: Kali Linux, Appscan, Fortify, Nexpose, Acunetix, Burp, Spike

[2022] ***Digital forensic services*** *for Banca Romaneasca*

- *Digital forensic analysis to support an internal investigation for the legal department*

[2020 – 2022] ***IBM Qradar SIEM tuning consulting services for*** *Banca Romaneasca*

- *Perform Architectural Review and implement design best practices, and design steps to increase Qradar efficiency*
- *Research, analyze, and implement relevant log sources utilized for the purpose of security monitoring, particularly security and networking devices (such as firewalls, routers, anti-virus products, vulnerability scanners, proxies, and operating systems)*
- *Eliminating false-positive offenses and tuning the improperly working correlation rules*
- *Create and develops correlation and detection rules on events of interest to detect potential security incidents*
- *Improve security detection posture by mapping the MITRE ATT&CK framework to rules and building blocks*
- *Create and develops dashboards and customize reports based on regulatory and compliance requirements (PCI DSS, Basel II, EU Data Protection Directive, ISO 27001)*
- *Perform cyber security incident response process improvements by running pre-planned purple team exercises launching specific cyber-attacks, emulating multiple Tactics, Techniques, and Procedures (TTPs) and waiting for the internal team to indicate detection and response of a particular attack, identifying any weaknesses or gaps in detection and response, and immediately supporting remediation of the issue*

[2021 - 2022] ***IoT and cybersecurity consulting services*** *for TrustChain*

- *Define and document the technical architecture and security requirements for IoT solution*
- *Perform source code analysis for web and mobile app*
- *Perform vulnerability services and penetration services for cloud infrastructure*

- *Define and implement technical controls and management framework for ISO 27001 and GDPR standards*
- *Perform vulnerability services and penetration Services for IoT infrastructure*

Tools: Kali Linux, Appscan, Fortify, Nexpose, Acunetix, Burp, Spike

*[2022] Perform **IBM Guardium training session***

*[2020 – 2022] Perform **IBM Qradar training session***

*[2019] **i2 Training session** for SELEC - Southeast European Law Enforcement Center (2 iBase and i2 Analyst`s Notebook training sessions including I2 suite is the most trusted intelligence analysis platform)*

Jan 2005 – Oct 2019

Chief Security Officer

TRANSFOND SA, Bucharest, Romania

Main activities and responsibilities:

- Perform solution architecture, business analysis, consultancy, and support services
- Perform security and audit services
- Lead security awareness and training initiatives
- Lead organization`s security policy efforts and policy-related activities for risk management
- Perform phishing exercises and threat assessments an o regular cadence
- Perform risk assessment support, supported routine and ad-hoc audits
- Perform regular dynamic and static analysis of web applications and analyse systems for potential vulnerabilities (vulnerabilities assessment) that may result from improper system configuration, hardware or software flows
- Review policies and act like a subject matter expert on best practices; also review security documentation and make recommendations;
- Perform analytical support of security incidents across the enterprise
- Design alerting, communications, workflow, and training of other IT users
- Perform IT infrastructure hardening procedures
- Troubleshoot and researched security incidents using IBM Qradar Security Intelligence Platform, PaloAlto EDR, Checkpoint NGFW, etc
- Investigating logs and payloads for server crashes/core dump, DDoS attacks, SQL/XSS, SPAM, etc
- Lead security team and perform quality assurance

Mar 2003 – Jan 2005

IT Expert

Ministry of Justice, Romania

Main activities and responsibilities:

- Perform solution architecture, business analysis, consultancy, and support services
- Perform security and audit services
- Contribute security best practices to operations strategy planning, design, implementation, and maintenance activities
- Provides expert-level analysis of policy activities including policy impacts on IT systems, procedural integration, and alignment to policy; policy rollout or implementations plans
- Perform risk analysis and evaluation of security controls in order to prepare external audit missions;
- Implementation and management of the security program within the IT department
- Development of policies, standards, and controls in compliance with ISO 27001;

Sep 2002 - Mar 2003

Network designer

Raiffeisen Bank, Bucharest, Romania

Main activities and responsibilities:

- Involved in complete LAN, and WAN development;
- Provided Tier 2 support for network issues
- Used Layer 3 protocols like EIGRP, and BGP to configure routers in the network
- Used network monitoring tools to ensure network connectivity and protocol analysis tools to asses and pinpoint networking issues causing service disruptions

Sep 1998 – Sep 2002

System Engineer/ Team leader

Romanian Saving BANK, Bucharest, Romania

Main activities and responsibilities:

- Perform solution architecture, business analysis, consultancy, and support services
- Perform security and audit services
- Develop and implement IT goals, plans, and objectives
- Assist in budget management, project prioritization, and recommendation og new systems/software products and services
- Coordinate and direct the day-to-day activities of systems administration, storage administration, backup, and restore the administration
- Establish and maintain documentation for IT systems and processes
- Developing automation scripts
- Perform administration of the IT infrastructure;

- Perform the annual technical training sessions

Sep 1995 - Oct 1998

System Engineer

Silvan Computers, Bucharest, Romania

Main activities and responsibilities:

- Perform software install and management
- Design and implement network structured cabling
- Perform administering servers and network equipment

EDUCATION

1991–1995

BS Degree in Electronics

University POLITEHNICA of BUCHAREST (Romania), Faculty of Electronics and Telecommunication

TRAININGs

1996 - 2022

- Trainings and certifications awarded
- Mile2 - Threat Intelligence Analyst;
- Mile2 - Secure Web Application Engineers;
- Mile2 - Penetration Testing Consultant;
- Mile2 - Digital Forensics Examiner;
- Pentester Academy – Embedded/Iot Linux for RedBlue Teams
- Pentester Academy – Certified Red Team Professional
- Pentester Academy – Certified Red Team Expert
- Pentester Academy - Windows Process Injection for Red-Blue Teams
- INE - Web Application Penetration Testing eXtreme
- INE – Exploit Development
- INE- Mobile Application Penetration Testing Professional
- INE- Incident Handling&Response:SOC 3.0 Operations & Analytics
- Microfocus – Fortify SCA;
- SkyBox;
- IBM Qradar (IBM Training);
- IBM Guardiun (IBM Training);
- IBM Guardiun (IBM Training);
- IBM Endpoint Manager;
- Qualys Vulnerability Management;
- Rapid7 Nexpose, Metasploit (Rapid7 Training);
- Mandiant - Windows Enterprise Incident Response
- PCIDSS (IBR Training);
- SUSE Linux Enterprise Server Administration (SUSE Training);
- Symantec DLP (Symantec Training);
- ISMS Implementer/Lead Implementer ISO 27001:2005 (Veridion 2010);
- ITIL Foundation, ITIL RCV, ITIL PPO;
- ECSA/LPT;
- SANS Hacker Techniques, Exploits & Incident Handling;
- SANS Web App Penetration Testing and Ethical Hacking;
- SANS Network Penetration Testing and Ethical Hacking;
- SANS Advanced Computer Forensic Analysis and Incident Response;
- SANS Secure Coding in Java/JEE: Developing Defensible Application;
- SANS Intrusion Detection In-Depth;
- SANS Auditing Networks, Perimeters, and Systems;
- SANS Cutting-Edge Hacking Techniques;
- Audit for an Information Security Management System as for BS 7799-2/2002 and BS ISO/IEC 17799:2000 Standards and European Accreditation Norms (Instructions, Directives, Guidelines);
- Business Continuity - Disaster Recover Planning;
- Oracle DBA Fundamentals I;
- AIX 5L System Administration;
- Configuring and Troubleshooting Enterprise Networks;
-

CERTIFICATIONS

2010 - Certified Information Systems Auditor (CISA) –ISACA;
2010-2014 - Web App Penetration Testing and Ethical Hacking (GWAPT)- SANS,
2007-2015 - GIAC Certified Incident Handler (GCIH) - SANS,
2005 - TUV- Information Security Internal Auditor
2018 - Project Management PRINCE2 Practitioner;
2017 - ITIL Practitioner;
2017 - COBIT Foundation;

2017	▪ ISO 27001 Lead Implementer;
2018-2020	▪ EC-Counsil ECSA;
2015	▪ IBM Certified Analyst i2 Analyst Notebook,
2015	▪ IBM Certified i2 iBase Support Professional,
2022	▪ IBM Qradar
2015	▪ Rapid7 Nexpose Cerified Administrator,
2021	▪ Acunetix Profesional,
2022	▪ Fortify Administrator,
2022	▪ Microfocus -Fortify SCA

PERSONAL SKILLS

Mother tongue(s): Romanian

Other language(s)

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C1	C1	C1	C1	C1
Italian	C1	C1	C1	C1	C1

Digital skills

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

Communication skills

- Excellent communication skills, team and people leader, trainer and speaker. Open minded, assertive, with good non-verbal communication, able to read the audience and to adjust the speech in the proper manner. Very good writing skills, being structured, precise and with keen attention to every nuance of a word

Organisational/ managerial skills

- Major leadership experience; Experience in project/ contract management and team management; interpersonal relationship skills. Ability to initiate and develop partnerships; ability of collaboration and cooperation with individuals with same interests, motivations, attitudes, behaviours, values.
- More than 17 years in performing security services

Job-related skills

- Expert in. cybersecurity, incident response process, penetration testing, , vulnerability assessment, source code analysis and forensic analysis services
- Solid knowledge of the entire solution architecture, planning, analysis, testing, deployment, documentation, training and support using various technology, tools and methodologies..
- More than 20 years banking experience

Technologies

Programming languages:
- Python, C++, C, Javascript, Powershell, Ruby

Testing:
- Selenium, Nightwatch, pytest, LoadRunner, UFTOne

Project management
- Agile, SCRUM, TDD, BDD, Prince2

Tools:
- Version management: Git, SVN
- Monitoring: Sentry, Zabbix, PRTG, NAGIOS,
- Issue tracking: Github, Redmine, Trac, Bugzilla, Jira
- Virtualization: VMware Vsphere, IBM PowerVM, Nutanix Ahv
- OS: Linux, Android, IOS, AIX
- Networking: Cisco, Fortinet, PaloAlto, Checkpoint, Extreme Networks
- Pentest Tools: Kali Linux, Cobalt Strike, Spike, John the Ripper, Wireshark, Aircrack-ng, Hydra, IDA Pro, Burp Suite, Rapid7 Metasploit, Rapid7 Nexpose, OWASP-ZAP Nmap, Nessus, Acunetix, Netsparker, Checkmarx, AppScan, Fortify, SonarQube