EARNED CERTIFICATIONS

CM)CTA | CySA+, C)CSA & C3SA | CCDA | HTB CDSA | C|SA | PSAP | PSAA | CSOA | CBTeamerX | CBTeamer | CBTP | CM)CFI | GCFE | GCFA | GNFA | CCDFA | C)NFE | C)DFE | eCDFP | CDFEH | ISO/IEC 27037 LI | WCNA | GCED | C|ND | CCD | C)ISSO | CPTA | HTB CPTS | C)PTC | C)PTE | C)PEH | C)VA | RvBCWP | CM)IPS | eCTHP | CRTS | CRTA | CRTeamer | CCMA | C)TIA | CIoTSP | OOSE | CNSP | CNSE | CCC | CCE | CCSE | CCSS

ISSUED BY

GIAC (associated with SANS Institute), Mile2 Cybersecurity Institute, EC-Council, CompTIA, HTB Academy, INE Security, TCM Security, CyberWarFare Labs, CyberDefenders, Cyber5W, The SecOps Group, CertNexus, Hackviser, OPSWAT Academy, Protocol Analysis Institute (WCNA Certification Program), United States Cybersecurity Institute, Pacific Certifications, Blockchain Council and Global Tech Council.

ANAB ACCREDITED PERSONNEL CERTIFICATION BODY

DoD 8140 APPROVED

Michał Sołtysik

✆ +48 796 *** ***
✉ me@michalsoltysik.com
https://michalsoltysik.com/

Cybersecurity Consultant

Cybersecurity Consulting | Blue Teaming | Purple Teaming | Red Teaming | Forensics Examiner | SOC Trainer | Cyber Warfare Organizer | SOC Operational Capability and Maturity Development | Adversary Emulation

Cybersecurity Consultant and **Blue Team**, **Purple Team**, and **Red Team** Analyst with broad and in-depth expertise across multiple cybersecurity domains.

Digital and Network Forensics Examiner, **Cyber Warfare Organizer**, and **SOC Trainer**, specializing in **SOC Operational capability and maturity development**, **network edge traffic profiling**, and **adversary emulation in EDR testing**.

EXPERIENCE

Cybersecurity Consultant | Warsaw | Remote

Security Operations Centre (SOC) Consulting. **Tier 1, Tier 2, and Tier 3 Technical Guidance and Mentoring**. SIEM Engineering and Administration (Splunk, Elastic SIEM, IBM QRadar). Security Solution Integration and Optimization (SOAR, SIEM, IDS/IPS, WAF, EDR, NAC, APT, NTA, NIDS, UTM). Blue Team vs. Red Team Exercise and Cyber Warfare Simulation Organization. Cybersecurity Exercise Coordination (including Cyber Europe 2024). SOC Recruitment and Technical Candidate Assessment. SOC and Cybersecurity Training Delivery. Malware Reverse Engineering (Windows and Linux). SOC Lab Creation, Administration, and Management. Digital and Network Forensics. Controlled Adversary Simulation and Malware Analysis. Penetration Testing and Security Assessment. Security Infrastructure Hardening Recommendations. EDR, Application, and Anti-DDoS Solution Testing and Validation. Incident Response and Threat Analysis. Digital Evidence Handling and Forensic Incident Response (DEFR/DES).

Government digital transformation and cybersecurity sector. Public administration and national online service platforms. State cybersecurity, telecommunications, and research organizations. Nationwide educational network and digital infrastructure providers. Internal security, intelligence, and counterintelligence agencies. Anti-corruption and public integrity enforcement institutions. Public funding and financial administration institutions. Judicial and court administration institutions. National healthcare and medical research institutions. Energy, gas storage, and critical infrastructure operators. Maritime port authorities and logistics operators. Municipal heating and utility service providers. Industrial manufacturing and chemical production companies. Interior design and architectural solution companies. Construction and infrastructure development corporations. Furniture manufacturing and furnishing companies. IT infrastructure and technology service providers. Higher education and academic institutions. Automotive and industrial component manufacturers. Pharmaceutical and healthcare product manufacturers. Municipal and local government administration institutions.

An official reference letter from a SOC Manager, based on 5 years of work as a SOC Consultant, Analyst, and Trainer

https://michalsoltysik.com/references/

MORE INFORMATION

Certifications:
https://michalsoltysik.com/certifications/

Services:
https://michalsoltysik.com/services/

Training:
https://michalsoltysik.com/training/

Skills:
https://michalsoltysik.com/skills/

References:
https://michalsoltysik.com/references/

Cybersecurity content:
https://michalsoltysik.com/cybersecurity-content/

Own tools:
https://michalsoltysik.com/own-tools/

Events:
https://michalsoltysik.com/events/

Contact:
https://michalsoltysik.com/contact/

SOC Analyst Level 3 | Warsaw | On-site

Security Operations Centre (**SOC**) **Level 3 Operations**. Security Operations Centre Development, Implementation, and Team Design. Security Solution Deployment and Integration. Security Process, Procedure, and Documentation Development. Tier 1 and Tier 2 Analyst Mentoring and Technical Guidance. IBM QRadar SIEM Administration, Flow and Event Rule Creation, and Tuning.

Public and commercial sector. State cybersecurity, telecommunications, and research organizations. Nationwide educational network and digital infrastructure providers. Critical infrastructure operators.

SOC Analyst Level 2 | Warsaw | On-site

Security Operations Centre (**SOC**) **Level 2 Operations**. Security Operations Centre Development and Implementation. Security Solution Integration and Optimization. Security Process, Procedure, and Documentation Development. Tier 1 Analyst Mentoring and Technical Guidance. IBM QRadar SIEM Administration, Rule Creation, and Tuning. Digital and Network Forensics.

Government online services, portals, websites, and digital applications. Government digital transformation and cybersecurity sector. Public sector IT infrastructure and informatics service providers.

SOC Analyst | Warsaw | On-site

Security Operations Centre (**SOC**) **Level 1 and Level 2 Security Operations**.

International insurance, financial services, and corporate enterprise environments worldwide.

Network Specialist | Warsaw | On-site

Network Operations Centre (**NOC**) **Level 2 Technical Support**.

CORP IT Specialist | Warsaw | On-site

Service Desk Support.

IT Operations associate | Warsaw | On-site

Global Service Desk Support.

Helpdesk Agent with English | Warsaw | On-site

IT Helpdesk Support.

Founder, Owner & Manager - Sick Slaughterhouse

Founded and managed an EDM record label specializing in electronic music production, artist management, music distribution, marketing, promotion, and international business collaboration.

Music Producer, Composer & Audio Engineer - MikeWave

Created original music releases distributed across international digital streaming and music distribution platforms.

For access to the extended version of the CV containing detailed information, please contact me directly.