Tomasz **Samel**

Junior SOC Analyst (SIEM / Blue Team)

+48 515087250 | tomaszrudnik@op.pl | tomaszrudnik/soc-home-lab

Summary

Junior SOC Analyst focused on Blue Team activities and SIEM operations. Hands-on experience gained through a personal SOC Home Lab based on Splunk, Windows Security Logs, and Sysmon. Skilled in log analysis, alert triage, and first-line incident response (SOC Tier 1). Experience includes attack simulation, detection engineering fundamentals, and mapping techniques to the MITRE ATT&CK framework. Background in software testing (manual and automated) supporting a structured, analytical, and process-driven approach. Highly motivated to start a Junior SOC role and continue professional growth within a security operations team. Available immediately.

Professional Experience

SOC Home Lab – Splunk SIEM

Remote

Personal Project

2024 – Present

- Built and maintained a personal SOC lab focused on SIEM operations and detection engineering.
- Collected, ingested, and analyzed logs using Splunk, Windows Security Logs, and Sysmon.
- Performed alert triage and first-line incident response activities (SOC Tier 1).
- Developed detection logic in SPL and mapped detection use cases to the MITRE ATT&CK framework.
- Tested and validated detections through simulated adversary techniques.

Manufacturing and Logistics Company (Regional Operations)

Rzeszów, Poland

Operations Supervisor

November 2005 – Present

- Incident handling and operational response in time-critical environments.
- Worked with procedures, security policies, and compliance requirements.
- Task prioritization, escalation, and resolution across multiple parallel incidents.
- Coordinated teams and external vendors during operational disruptions.
- Ensured continuity of operations and risk mitigation.

Skills

SIEM / SOC	Splunk, log analysis, alert triage (Tier 1), basic incident response
Windows Security	Event logs, Event ID 4688, Sysmon, fundamentals of threat detection
MITRE ATT&CK	Technique mapping, detection logic
Operating Systems	Windows, Linux (basic administration)
Testing / Automation	Manual testing, basics of Selenium WebDriver
Languages	Polish – native, English – B2

Education

ISC2 Candidate (Certified in Cybersecurity path)

ISC2 - International Information System Security Certification Consortium

2026 – Present

Remote

- Currently pursuing the Certified in Cybersecurity (CC) certification to formalize foundational security knowledge.
- Focus: Security Operations, Incident Response, and Global Security Standards.

Cybersecurity (SOC & SIEM) – Certificate

University of Warsaw / HackerU

2022 – 2023

Warsaw, Poland

- Specialized training in SOC operations, SIEM (Splunk) management, and alert triage (Tier 1).
- Practical application of MITRE ATT&CK mapping and Windows security log analysis.

Postgraduate Studies – Software Testing

University of Information Technology and Management (WSIiZ)

2023 – 2024

Rzeszów, Poland

- Developed a structured, process-driven approach to data analysis and system validation.