

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

PERSONAL PROJECT

Remote

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)

OPERATIONS SUPERVISOR

Rzeszów, Poland

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

Cybersecurity (SOC & SIEM) – Certificate

2022 – 2023

University of Warsaw / HackerU

Warsaw, Poland

- SOC operations, SIEM (Splunk), log analysis, incident response (SOC Tier 1).
- Windows security logs, Sysmon, MITRE ATT&CK techniques mapping.
- Hands-on SOC & SIEM laboratories and final defensive project.

Postgraduate Studies – Software Testing

2023 – 2024

University of Information
Technology and Management
(WSIiZ)

Rzeszów, Poland

- Fundamentals of manual and automated software testing.
- Selenium WebDriver, test cases, and test scenarios.