SODIK TURSUNBOEV

JUNIOR SOC ANALYST | SECURITY OPERATIONS & INCIDENT INVESTIGATION

Warsaw, Poland · hello@sodik.eu
sodik.eu · LinkedIn · GitHub · TryHackMe

PROFESSIONAL PROFILE

CEH v13-certified cybersecurity analyst with hands-on SOC lab experience in alert triage, endpoint telemetry, phishing analysis and incident documentation. Familiar with Splunk, Elastic, Microsoft Sentinel, EDR and SOAR workflows. Built a custom SIEM with **35 detection rules** and tested detections against controlled attacks.

CORE SKILLS

SOC OPERATIONS Alert triage, incident escalation, phishing/email header analysis, IOC investigation, case documentation

SIEM & ENDPOINT Splunk, Elastic (ELK), Microsoft Sentinel, Microsoft Defender for Endpoint, Wazuh, SOAR workflows

DETECTION Windows Event Logs, Sysmon, MITRE ATT&CK, Sigma, log correlation, detection validation

SYSTEMS Windows, Linux, Active Directory, PowerShell, Python

PRACTICAL SOC EXPERIENCE

Independent SOC & Security Labs | Nov 2023 – Present

- Investigated simulated **suspicious logons, process execution and endpoint activity** using Windows Security and Sysmon logs; documented investigation findings and detection gaps.
- Practiced **phishing triage, IOC analysis and security-event correlation** in controlled exercises; used MITRE ATT&CK to describe attacker behavior and defensive response.

SELECTED SECURITY PROJECTS

Custom SIEM + Breach & Attack Simulation (BAS) | 2026 · GitHub

- Developed Windows/Linux log ingestion, **35 detection rules**, alert correlation, case management and analyst-approved response workflows.
- Validated 10 Atomic Red Team tests: **7 detected, 3 missed**. Investigated a missed Kerberoasting alert and traced the gap to a missing **TicketEncryptionType** parser field.

Active Directory Purple Team Lab | 2026 · GitHub

- Simulated credential abuse, lateral movement, DCSync and Golden Ticket techniques in an isolated AD environment; correlated Windows/Sysmon events and documented mitigations.

CERTIFICATIONS, EDUCATION & LANGUAGES

Certified Ethical Hacker (CEH v13) · EC-Council · Oct 2025

TryHackMe · Top 1% globally · SOC Level 1 path · 240+ rooms

Blue Team Labs Online · Top 1% globally · #6 in Poland

Vistula University · Full-time bachelor's studies (Cybersecurity) · Oct 2026 – Present

English · Full professional working proficiency

I consent to the processing of my personal data included in this application for recruitment purposes in accordance with Regulation (EU) 2016/679 (GDPR).