

Piotr Szkudlarek

Email: kontakt@piotrszkudlarek.com

LinkedIn: <https://www.linkedin.com/in/szkudlarekpiotr/>

GitHub: <https://github.com/szkudlarekPiotr/>

Professional Summary

Since April 2026 I've been working as a SOC Analyst L1: I analyze SIEM and EDR alerts, configure a SIEM built on Elastic/OpenSearch and automate my team's work in Python with my own Mini-SOAR engine and user account analyzer. Before that I worked as an IT/OT Systems Implementation Specialist, where I handled incidents and monitored SCADA systems.

Professional Experience

SOC Analyst L1 - Komputronik Biznes

on-site | April 2026 - present

- Triaging and analyzing SIEM and EDR alerts: Windows/AD, Cloudflare WAF, VPN, Office 365, network traffic
- Complex DQL, Query DSL and Lucene queries combining multiple conditions and data sources
- SIEM configuration and development (Elastic/OpenSearch): adding log sources, indices, scripted fields, alert rules based on MITRE ATT&CK and interactive dashboards
- Incident handling: analysis, EDR actions (CrowdStrike, ESET Protect & Inspect) including host isolation, escalation and reporting
- Python automation for the whole team: my own Mini-SOAR engine with the user account analyzer, VirusTotal enrichment and an automated shift report
- Co-creating a ticketing system in Alloy - alert handling logic and workflow for multiple clients

IT/OT Systems Implementation Specialist - Mikronika

hybrid | May 2025 - March 2026

- Handling incidents with SCADA systems: verification, root cause analysis and escalation with a recommendation
- System monitoring (Grafana, PRTG), alert configuration, system and application log analysis
- Validating operational data with SQL and Excel, working in Linux
- An Excel/VBA tool fed by Python, tracking nearly 1,000 Jira Helpdesk tickets: statuses, SLA and KPIs

Junior Data Analyst - Santander Digital Services

remote | July 2024 - April 2025

- Analyzing operational and user data in an AML/CTF-regulated environment
- Data quality validation, detecting anomalies and inconsistencies
- Excel reporting, collaboration with technical and analytical teams

Education

Master's degree in Data Analysis and Processing - Adam Mickiewicz University, Poznań | 2022-2024

- Thesis: "Applying artificial intelligence and machine learning methods to gesture annotation"

- Thesis: "Comparison of automatic and manual gesture annotation"

Projects

Mini-SOAR and user account analyzer - alert enrichment and threat hunting in Python

- Enriches new alerts by adding risk level, recommended steps, the reasoning behind security findings, mapping to MITRE ATT&CK
- Hourly threat hunting across all Windows/AD logs: detects password spraying, Kerberoasting, DCSync and other attack techniques
- Handles all Windows alerts within about 2 minutes of the event (median), calibrated to the environment's logs so it doesn't add noise
- User account analyzer: an account activity report from correlated logs, with security breach hypotheses and their justification - a concise security verdict, risk score and recommendation
- Hypotheses with evidence straight from the SIEM, MITRE ATT&CK links and an L1 checklist
- Comparison with the same account's baseline of previous days, VPN session correlation, a timeline of all events
- Skills: Python, OpenSearch, Sigma (pySigma), MITRE ATT&CK, Active Directory, PowerShell, systemd, SQLite

VirusTotal enrichment and automated shift report - Python automation for the whole SOC team

- VirusTotal enrichment: a Python script gathers public information (OSINT) from VirusTotal about IP addresses in Cloudflare alerts and writes it back to the SIEM
- Each alert is checked once, and only public addresses go to VirusTotal
- Shift report: automatically detects the current shift's time range and pulls its data from the SIEM
- Groups alerts by rule and lists their most important details
- Fills in a standardized report template, including text boxes, headers and footers
- Skills: Python, Query DSL, VirusTotal API v3, cron, python-docx

Skills & Languages

- **SIEM & detection:** Elastic/OpenSearch, DQL, Query DSL, Lucene, rules and dashboards, Sigma (pySigma), MITRE ATT&CK; Splunk - basics
- **Analysis & response:** alert triage, threat hunting, incident handling, EDR (CrowdStrike, ESET Protect & Inspect)
- **Systems & logs:** Windows / Active Directory, Linux (terminal, cron, systemd), VPN, Office 365, IT/OT and SCADA, Grafana, PRTG
- **Automation & data:** Python, SQL/NoSQL, Excel/VBA, VirusTotal API, Jira/Atlassian
- **Soft skills:** analytical thinking, working with ambiguous data, attention to data quality, teamwork
- **Languages:** Polish - native, English - C1 (Cambridge English), German and Spanish - basic