

Piotr Szkudlarek

Email: kontakt@piotrszkudlarek.com

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

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

Profil zawodowy

Od kwietnia 2026 pracuję jako SOC Analyst L1: analizuję alerty z SIEM i EDR, konfiguruje SIEM oparty na Elastic/OpenSearch i automatyzuję pracę zespołu w Pythonie, m.in. autorskim silnikiem Mini-SOAR i analizatorem użytkowników. Wcześniej pracowałem jako specjalista ds. wdrożeń systemów IT/OT, gdzie obsługiwałem incydenty i monitorowałem systemy SCADA.

Doświadczenie zawodowe

SOC Analyst L1 - Komputronik Biznes

stacjonarnie | kwiecień 2026 - obecnie

- Triage i analiza alertów z SIEM i EDR: Windows/AD, Cloudflare WAF, VPN, Office 365, ruch sieciowy
- Złożone zapytania w DQL, Query DSL i Lucene łączące wiele warunków i źródeł danych
- Konfiguracja i rozwój SIEM (Elastic/OpenSearch): dodawanie źródeł logów, indeksy, scripted fields, reguły alertów oparte na MITRE ATT&CK, interaktywne dashboardy
- Obsługa incydentów: analiza, działania w EDR (CrowdStrike, ESET Protect & Inspect), m.in. izolacja hosta, eskalacja i raportowanie
- Automatyzacje w Pythonie dla całego zespołu: autorski silnik Mini-SOAR z analizatorem użytkowników, enrichment VirusTotal i automatyczny raport zmianowy
- Współtworzenie systemu ticketowego w Alloy - logika i workflow obsługi alertów dla wielu klientów

Specjalista ds. wdrożeń systemów IT/OT - Mikronika

hybrydowo | maj 2025 - marzec 2026

- Obsługa incydentów zakłócających działanie systemów SCADA: weryfikacja, analiza przyczyn i eskalacja z rekomendacją
- Monitorowanie systemów (Grafana, PRTG), konfiguracja alertów, analiza logów systemowych i aplikacyjnych
- Walidacja danych operacyjnych w SQL i Excelu, praca w Linuksie
- Narzędzie Excel/VBA zasilane Pythonem, monitorujące blisko 1000 zgłoszeń Jira Helpdesk: statusy, SLA i KPI

Młodszy Analityk Danych - Santander Digital Services

zdalnie | lipiec 2024 - kwiecień 2025

- Analiza danych operacyjnych i użytkowników w środowisku regulowanym AML/CTF
- Walidacja jakości danych, wykrywanie anomalii i niespójności
- Raporty w Excelu, współpraca z zespołami technicznymi i analitycznymi

Wykształcenie

Studia magisterskie: Analiza i przetwarzanie danych - Uniwersytet im. Adama Mickiewicza w Poznaniu | 2022-2024

- Praca magisterska: „Zastosowanie sztucznej inteligencji i metod nauczania maszynowego w anotacji gestów”

Studia licencjackie: Lingwistyka komputerowa - Uniwersytet im. Adama Mickiewicza w Poznaniu | 2019-2022

- Praca licencjacka: „Porównanie automatycznej i manualnej anotacji gestów”

Projekty

Mini-SOAR i analizator użytkowników - wzbogacanie alertów i threat hunting w Pythonie

- Wzbogacanie nowych alertów na bieżąco - skala ryzyka, zalecane kroki, uzasadnienie wykryć bezpieczeństwa, mapowanie do MITRE ATT&CK
- Threat hunting obejmujący całe logi Windows/AD, uruchamiany raz na godzinę: wykrywa password spraying, Kerberoasting, DCSync i inne techniki ataków
- Obsługuje wszystkie alerty Windows w ciągu ok. 2 minut od zdarzenia (mediana), skalibrowany pod logi środowiska, aby nie wprowadzał szumu
- Analizator użytkowników: raport aktywności konta ze skorelowanych logów z hipotezami naruszeń bezpieczeństwa i ich uzasadnieniami - zwięzły werdykt bezpieczeństwa, ocena ryzyka i rekomendacja
- Hipotezy z dowodami bezpośrednio z SIEM, odnośnikami do MITRE ATT&CK i checklistą dla L1
- Porównanie aktywności z normą tego samego konta w poprzednich dniach, korelacja sesji VPN, oś czasu wszystkich zdarzeń
- Umiejętności: Python, OpenSearch, Sigma (pySigma), MITRE ATT&CK, Active Directory, PowerShell, systemd, SQLite

Enrichment VirusTotal i automatyczny raport zmianowy - automatyzacje w Pythonie dla całego zespołu SOC

- Enrichment VirusTotal: skrypt w Pythonie zbiera z VirusTotal publiczne informacje (OSINT) o adresach IP z alertów Cloudflare i dopisuje je do alertu w SIEM
- Każdy alert jest sprawdzany raz, a do VirusTotal trafiają tylko adresy publiczne
- Raport zmianowy: automatycznie rozpoznaje zakres bieżącej zmiany i pobiera dla niej dane z SIEM
- Grupuje alerty według reguł, a także wypisuje ich najważniejsze szczegóły
- Wypełnia ustandaryzowany szablon raportu, w tym pola tekstowe, nagłówki i stopki
- Umiejętności: Python, Query DSL, VirusTotal API v3, cron, python-docx

Umiejętności i języki

- **SIEM i detekcja:** Elastic/OpenSearch, DQL, Query DSL, Lucene, reguły i dashboardy, Sigma (pySigma), MITRE ATT&CK; Splunk - podstawy
- **Analiza i reagowanie:** triage alertów, threat hunting, obsługa incydentów, EDR (CrowdStrike, ESET Protect & Inspect)
- **Systemy i logi:** Windows / Active Directory, Linux (terminal, cron, systemd), VPN, Office 365, IT/OT i SCADA, Grafana, PRTG
- **Automatyzacja i dane:** Python, SQL/NoSQL, Excel/VBA, VirusTotal API, Jira/Atlassian
- **Kompetencje miękkie:** myślenie analityczne, praca z niejednoznacznymi danymi, dbałość o jakość danych, praca zespołowa
- **Języki:** polski - ojczysty, angielski - C1 (Cambridge English), niemiecki i hiszpański - podstawowy