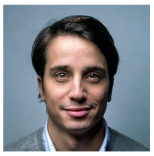
Dawid Kamiński

Młodszy Specjalista Cyberbezpieczeństwa



PROFIL

Absolwent cyberbezpieczeństwa na Wojskowej Akademii Technicznej z certyfikatem CompTIA Security+. Podczas stażu w zespole SOC banku monitorowałem i analizowałem alerty bezpieczeństwa generowane przez infrastrukturę obsługującą 3,2 mln klientów. Doświadczenie w triażu incydentów, analizie logów SIEM i hardening systemów.

WYKSZTAŁCENIE

Stopień i kierunek
Wojskowa Akademia Techniczna, Warszawa
Paź 2022 – Lut 2026

UMIEJĘTNOŚCI

- Splunk (SIEM)
- Nessus / OpenVAS
- Wireshark / tcpdump
- Linux (Kali, Ubuntu)
- Firewall (pfSense, iptables)
- MITRE ATT&CK Framework
- Python (skrypty bezpieczeństwa)
- Active Directory (hardening)
- Burp Suite (podstawy)
- OWASP Top 10

JĘZYKI

- Polski (ojczysty)
- Angielski (B2)

KONTAKT

Warszawa, Polska
dawid.kaminski.sec@gmail.com
+48 515 682 439
linkedin.com/in/dawid-kaminski-cybersec
github.com/dkaminski-sec

DOŚWIADCZENIE

Stażysta SOC Analyst, PKO Bank Polski, Warszawa *Lip 2025 – Sty 2026*
Staż w Security Operations Center jednego z największych banków w Europie Środkowej.

- Triaż średnio **1.400 alertów SIEM** miesięcznie w platformie Splunk z 96% wskaźnikiem prawidłowej klasyfikacji
- Eskalacja **28 incydentów** bezpieczeństwa do analityków L2, w tym 4 o priorytecie krytycznym
- Przygotowanie **12 procedur** reagowania na incydenty (playbooks) dla typowych wektorów ataku
- Monitoring infrastruktury obsługującej **3,2 mln klientów** bankowości elektronicznej

Praktykant ds. Bezpieczeństwa IT, Orange Polska, Warszawa *Sty 2025 – Maj 2025*
Praktyki w dziale bezpieczeństwa teleinformatycznego.

- Wsparcie w **skanowaniu podatności** (Nessus) dla 800 hostów w sieci korporacyjnej
- Przygotowanie raportów z **audytu konfiguracji** firewalli dla 3 lokalizacji

CERTYFIKATY

CompTIA Security+ (SY0-701), CompTIA *Maj 2025*

PROJEKTY

HackYeah 2025 CTF *Paź 2025 – Paź 2025*
Udział w największym hackathonie w Europie Środkowej.

- Miejsce w **top 10** (z 180 zespołów) w kategorii cybersecurity
- Rozwiązanie **14 z 18 zadań** z zakresu web exploitation, kryptografii i reverse engineering