

Sławomir Babicz

SENIOR SECURITY ENGINEER

CONTACT

Volketswil, Switzerland
+41 79 927 56 34
slawomirbabicz@gmail.com
slawomirbabicz.com
linkedin.com/in/slawomirbabicz
github.com/sbabicz

SKILLS

SECURITY ENGINEERING

Incident Response · Detection Engineering · SIEM (Elastic, Splunk) · EDR (CrowdStrike) · Threat Intelligence · Threat Hunting · Phishing Defense

CLOUD & INFRASTRUCTURE

AWS · GCP · IAM / Okta · Kubernetes · Terraform · Linux · CI/CD Security · Elasticsearch

AUTOMATION & AI

Python · AI Agents · LLM Alert Triage

PROFILE

Senior Security Engineer with 10+ years across incident response, detection engineering, and cloud security. Handles incidents end-to-end – from forensics to postmortems and stakeholder presentations. Builds SIEM platforms and detection tooling, most recently AI agents for phishing classification and alert triage. Track record securing AWS/GCP environments and blockchain infrastructure for Swiss banking and Web3 organisations.

EXPERIENCE

Senior Infrastructure Security Engineer

08/2022 – 06/2026

DFINITY Foundation · Zürich, Switzerland

- Responded to security incidents, handling investigations end-to-end including forensic analysis, postmortems, and stakeholder presentations
- Designed and built a technically deep Elastic SIEM platform with custom detection rules covering a wide range of applications and threat vectors; migrated audit logging off Splunk to cut licensing costs
- Developed detection tooling for identifying attacks, abuse, and data leaks, including phishing and malware targeting the blockchain platform
- Deployed AI agents for phishing classification and for SIEM alert throttling and triage
- Operated and continuously improved the CrowdStrike EDR platform as part of daily operations
- Maintained IAM permissions and access control for AWS infrastructure, implemented Okta (SAML) integrations, and built internal tool chains across AWS and GCP
- Contributed to hardening of release pipelines to strengthen the security of the software delivery process
- Conducted internal security design and implementation reviews, and contributed to security governance including compliance and benchmark-based assessments

Security Engineer

2021 – 2022

Credit Suisse (contractor via iET SA) · Zürich, Switzerland

- Designed and implemented end-to-end technical solutions for security and business use cases utilizing Splunk and UEBA commercial tools
- Built monitoring of privileged user accounts (PAMO) for the bank
- Implemented UEBA use cases with Exabeam, building automations, enrichments, and telemetry ingestion pipelines from UEBA tooling
- Built parsers, models, rules, Splunk searches and dashboards
- Wrote technical documentation and concepts, developed integrations between various tools

Professional Threat Responder

2018 – 2021

ISPIN AG · Bassersdorf, Zürich Area, Switzerland

- Built a threat intelligence platform, gathering, processing and correlating TI data for distributing into SIEM/EDR solutions
- Onboarded customers to SIEM platform, performed onsite hardware installations
- Built, deployed and optimized SIEM to track, log and keep historical records of all incidents
- Built and maintained high-throughput Elasticsearch clusters (40+ nodes, 50TB+ bare metal)
- Developed phishing framework and ran high-profile phishing campaigns for major financial organizations in Switzerland
- Built the Cyber Defense Center from scratch, recruiting team members and providing mentorship

LANGUAGES

Polish – Native | English – Fluent | German – Good

INTERESTS

- Cybersecurity Research
- Protocol Reverse Engineering
- Infrastructure Automation

Senior SOC Specialist
2015 – 2018

Akamai Technologies · Cracow, Poland

- Led DDoS mitigation and served as escalation point for the global Security Operations Center (SOC)
- Provided premium technical support for high-profile and high-visibility clients
- Detected DDoS attack vectors by performing deep packet analysis
- Developed mitigation policies for constantly emerging threats and performed in-depth attack forensics
- Built the Cracow SOC from scratch, recruiting team members, producing training and technical documentation
- Performed onsite advanced training related to TCP/IP, BGP, OSPF, DNS, HTTP, HTTPS, DDoS detection

CMS Network Engineer
2015

Cisco Systems · Cracow, Poland

- Configured and administered Cisco equipment in mission-critical infrastructures; managed incidents according to ITIL/ISO procedures

3rd Line Network Engineer
2013 – 2015

Atos IT Solutions and Services · Bydgoszcz, Poland

- Provided 3rd line network support: LAN/WLAN infrastructure, BGP, OSPF, HSRP, VRRP, ACLs and EtherChannels

Field Engineer
2011 – 2013

SpeedNet · Ropczyce, Poland

- Wireless point-to-point deployments (802.11a/b/g) and Cisco configuration in the field

EDUCATION

Bachelor's degree, Technical Information and Education
2009 – 2013

University of Rzeszow · Rzeszów

- Received scientific scholarships
- Erasmus exchange at University of Matej Bel, Banska Bystrica, Slovakia
- MOST exchange at University of Kazimierz Wielki, Bydgoszcz, Poland

PROJECTS

- **German Learning Platform** (2026) – Interactive German grammar platform with exercises, user accounts, and an iOS companion app – built end-to-end with AI-assisted engineering. *Astro*, *Cloudflare Workers*, *D1*, *iOS*
- **slawomirbabicz.com** (2026) – Personal site with experience, projects, and blog in three languages. *HTML/CSS*, *Cloudflare*
- **Client & portfolio sites** (2026) – Designed, built, and deployed alexandra-eyer.ch (client work) and a bilingual photography portfolio. *HTML/CSS*, *Cloudflare Workers*
- **tcpdump-bpf-cheatsheet** (2019) – Open-source graphical TCP/IP stack model for writing BPF filters. *BPF*, *tcpdump*