

Sławomir Babicz

SENIOR SECURITY ENGINEER

KONTAKT

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

KENNTNISSE

SECURITY ENGINEERING

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

CLOUD & INFRASTRUKTUR

AWS
GCP
IAM / Okta
Kubernetes
Terraform
Linux
CI/CD-Sicherheit
Elasticsearch

AUTOMATISIERUNG & KI

Python
KI-Agenten
LLM-Alert-Triage

PROFIL

Senior Security Engineer mit über 10 Jahren Erfahrung in Incident Response, Detection Engineering und Cloud-Sicherheit. Verantwortet Vorfälle End-to-End – von der Forensik über Postmortems bis zu Stakeholder-Präsentationen. Baut SIEM-Plattformen und Detection-Tooling, zuletzt KI-Agenten für Phishing-Klassifizierung und Alert-Triage. Nachweisliche Erfolge bei der Absicherung von AWS-/GCP-Umgebungen und Blockchain-Infrastruktur für Schweizer Banken und Web3-Organisationen.

BERUFSERFAHRUNG

Senior Infrastructure Security Engineer

08/2022 – 06/2026

DFINITY Foundation · Zürich, Schweiz

- Bearbeitung von Sicherheitsvorfällen mit End-to-End-Verantwortung für Untersuchungen, inklusive forensischer Analysen, Postmortems und Stakeholder-Präsentationen
- Konzeption und Aufbau einer technisch tiefgehenden Elastic-SIEM-Plattform mit massgeschneiderten Erkennungsregeln; Migration des Audit-Loggings von Splunk zur Senkung der Lizenzkosten
- Entwicklung von Detection-Tooling zur Erkennung von Angriffen, Missbrauch und Datenabflüssen, einschliesslich Phishing und Malware mit Ziel auf die Blockchain-Plattform
- Einsatz von KI-Agenten für Phishing-Klassifizierung sowie für Drosselung und Triage von SIEM-Alerts
- Betrieb und kontinuierliche Verbesserung der CrowdStrike-EDR-Plattform im täglichen operativen Einsatz
- Pflege von IAM-Berechtigungen und Zugriffskontrollen für die AWS-Infrastruktur, Umsetzung von Okta-Integrationen (SAML) sowie Aufbau interner Toolchains in AWS und GCP
- Härtung der Release-Pipelines zur Absicherung des Software-Delivery-Prozesses
- Durchführung interner Security-Design- und Implementierungs-Reviews sowie Beiträge zur Security Governance, einschliesslich Compliance- und Benchmark-basierter Assessments

Security Engineer

2021 – 2022

Credit Suisse (Contractor via iET SA) · Zürich, Schweiz

- Konzeption und Umsetzung von End-to-End-Lösungen für Security- und Business-Use-Cases mit Splunk und kommerziellen UEBA-Tools
- Aufbau des Monitorings privilegierter Benutzerkonten (PAMO) für die Bank
- Umsetzung von UEBA-Use-Cases mit Exabeam, inklusive Automatisierungen, Anreicherungen und Telemetrie-Pipelines aus UEBA-Tools
- Entwicklung von Parsern, Datenmodellen, Korrelationsregeln, Splunk-Suchen und Dashboards
- Technische Dokumentationen und Konzepte; Integrationen zwischen verschiedenen Tools

SPRACHEN

Polnisch – Muttersprache
Englisch – Fliessend
Deutsch – Gut

INTERESSEN

- Cybersecurity-Forschung
- Protokoll-Reverse-Engineering
- Infrastruktur-Automatisierung

Professional Threat Responder
2018 – 2021

ISPIN AG · Bassersdorf, Region Zürich, Schweiz

- Aufbau einer Threat-Intelligence-Plattform zur Sammlung, Verarbeitung und Korrelation von TI-Daten für die Verteilung in SIEM-/EDR-Lösungen
- Onboarding von Kunden auf die SIEM-Plattform; Hardware-Installationen vor Ort
- Aufbau, Deployment und Optimierung des SIEM zur Protokollierung und Historisierung aller Incidents
- Aufbau und Betrieb von Elasticsearch-Clustern mit hohem Durchsatz (40+ Nodes, 50TB+ Bare Metal)
- Entwicklung eines Phishing-Frameworks und Durchführung von Phishing-Kampagnen für führende Schweizer Finanzinstitute
- Aufbau des Cyber Defense Center von Grund auf, inklusive Rekrutierung und Mentoring

Senior SOC Specialist
2015 – 2018

Akamai Technologies · Krakau, Polen

- Führender DDoS-Mitigation-Experte und Eskalationsstelle für das globale Security Operations Center (SOC)
- Premium-Support für hochkarätige Kunden mit hoher Sichtbarkeit
- Erkennung von DDoS-Angriffsvektoren durch tiefgehende Paketanalysen
- Entwicklung von Mitigationsrichtlinien für neue Bedrohungen; detaillierte Angriffsforensik
- Aufbau des Krakauer SOC: Rekrutierung, Schulungen und technische Dokumentation
- Durchführung von Schulungen vor Ort zu TCP/IP, BGP, OSPF, DNS, HTTP/HTTPS und DDoS-Erkennung

CMS Network Engineer
2015

Cisco Systems · Krakau, Polen

- Konfiguration und Administration von Cisco-Equipment in unternehmenskritischen Infrastrukturen; Incident-Management gemäss ITIL/ISO

3rd Line Network Engineer
2013 – 2015

Atos IT Solutions and Services · Bydgoszcz, Polen

- 3rd-Level-Netzwerksupport: LAN-/WLAN-Infrastruktur, BGP, OSPF, HSRP, VRRP, ACLs und EtherChannels

Field Engineer
2011 – 2013

SpeedNet · Ropczyce, Polen

- Funkinstallationen und Punkt-zu-Punkt-Verbindungen (802.11a/b/g) sowie Cisco-Konfiguration im Aussendienst

AUSBILDUNG

Bachelor, Technische und Informatische Bildung
2009 – 2013

Universität Rzeszów · Rzeszów, Polen

- Wissenschaftliche Stipendien für Studienleistungen
- Erasmus-Austausch an der Matej-Bel-Universität, Banská Bystrica, Slowakei
- MOST-Austausch an der Kazimierz-Wielki-Universität, Bydgoszcz, Polen

PROJEKTE

- **Deutsch-Lernplattform** (2026) – Interaktive Grammatik-Plattform mit Übungen, Benutzerkonten und iOS-App – End-to-End mit KI-gestütztem Engineering. *Astro, Cloudflare Workers, D1, iOS*
- **slawomirbabicz.com** (2026) – Persönliche Website mit Projekten und Blog. *HTML/CSS, Cloudflare*
- **Kunden- & Portfolio-Websites** (2026) – Design und Deployment von alexandra-eyer.ch und einem Fotografie-Portfolio. *HTML/CSS, Cloudflare Workers*
- **tcpdump-bpf-cheatsheet** (2019) – Grafisches TCP/IP-Modell als Open-Source-Cheatsheet für BPF-Filter. *BPF, tcpdump*