SAMUEL ANYA KALU

Security Analyst II – SOC

Prague, Czech Republic | +420 774 310 087 | samuel.kalu@samietech.eu

LinkedIn Profile | Credly Portfolio

PROFESSIONAL SUMMARY

High-caliber Security Analyst with over 4 years of hands-on experience in 24/7 Security Operations Centers. Specialized in delivering high-quality investigations and proactive monitoring within large-scale corporate environments. Expert in identifying, analyzing, and containing threats across hybrid and cloud infrastructures. Proven capability in advanced querying (**KQL/SPL**) to uncover patterns and drive improvements in detection and response logic.

TECHNICAL PROFICIENCIES

- **SIEM/XDR Platforms: Splunk (SPL)**, **Microsoft Sentinel (KQL)**, Exabeam, Wazuh, Elastic SIEM.
- **Security Tools: CrowdStrike Falcon**, FireEye HX, Darktrace, Cortex XDR, **M365 Defender**.
- **Cloud & Networking: Azure**, AWS, TCP/IP, DNS, HTTP/S, Active Directory.
- **Frameworks: MITRE ATT&CK**, **NIST Incident Response**, Cyber Kill Chain.
- **Core Skills:** Advanced Investigation, **Proactive Threat Hunting**, Detection Engineering, Root Cause Analysis.

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst (SOC) | SecureOps s.r.o, Prague *March 2022 – Present*

- **Incident Investigation & Response:** Deliver accurate and timely investigative analysis, acting as a key responder during active incidents to diagnose root causes and mitigate impact.
- **Advanced Threat Hunting:** Conduct proactive threat hunting to uncover unknown threats and strengthen early detection capabilities using advanced SIEM queries (KQL/SPL).
- **Detection Optimization:** Optimized SOC playbooks and automated use cases, resulting in a **35% improvement in true-positive rates**.
- **Adversary Mapping:** Map attacker techniques to the **MITRE ATT&CK** framework to maintain situational awareness of emerging trends and vulnerabilities.

- **Collaborative Response:** Partner with Incident Managers and Threat Intelligence teams for unified containment and remediation of sophisticated security events.
- **Technical Reporting:** Produce clear, technical post-incident reviews and actionable recommendations to strengthen security posture.

CERTIFICATIONS

- **CompTIA CySA+** (Cybersecurity Analyst)
- **Microsoft SC-200** (Security Operations Analyst Associate)
- **Microsoft SC-900** (Security, Compliance, and Identity Fundamentals)
- **Fortinet Certified Fundamentals** – Cybersecurity & Threat Landscape 2.0
- **ISO/IEC 27001** Information Security Associate

EDUCATION

- **MBA in Business Analytics** | EDU Effective Business School
- **Diploma in Computer Science** | Bellab Computer College

LANGUAGES

- **English:** Fluent (Full Professional Proficiency)