Sefa Gemade

Cybersecurity Engineer and Analyst

London, UK • U.S. citizen – no sponsorship required • Eligible for UK Graduate Visa

+44 7907 288 596
Email: thesefaway@gmail.com
LinkedIn: https://www.linkedin.com/in/sefa-gemade
GitHub: github.com/sefagemade
Website: sefagemade.com
YouTube: youtube.com/@PDFreakAI
Project site: PDFreak AI (demo available on YouTube)

Professional Summary

Cybersecurity Engineer & Analyst with 3 years of hands-on experience automating threat detection and response for 500 + endpoints in heavily regulated environments (HIPAA, ISO 27001, SOC 2). Skilled in **Python, KQL, Logic Apps, and MITRE-aligned threat hunting**, backed by a **First-Class Computer Science degree**. Experienced in AI-driven security analysis and DevSecOps integrations.

Experience

Indivior Plc / Cybersecurity Engineer and Operations Analyst

JUL 2023 - PRESENT, SLOUGH, UK

- Developed **Logic Apps workflows** for automated IP and URL analysis within Microsoft Sentinel to streamline incident response.
- Created **Python scripts** to extract and analyze endpoint logs, integrating with VirusTotal Enterprise for enriched threat intelligence.
- Implemented **phishing simulations** and awareness training using **PhishER** to enhance user security posture.
- Investigated and resolved daily alerts using **Microsoft 365 Defender and Sentinel**, ensuring timely incident response.
- Authored internal **knowledge base articles** to support new interns in SOC operations and Sentinel investigations.
- Utilized **Kusto Query Language (KQL)** for advanced threat hunting, identifying abnormal behaviors and potential compromises.
- Automated **remote device isolation** for suspicious activities using Logic Apps and Defender API integrations.
- Integrated **AI Foundry** to ingest and summarize security logs, supporting proactive threat detection and analysis.
-

AIENAI / Website Vulnerability Analyst & Interaction Designer

MAY 2022 - JUL 2023, LONDON

- Led end-to-end web-app penetration tests for 5 SaaS products, uncovering 120 + critical & high-severity issues (OWASP Top 10) and driving a 40 % reduction in average vulnerability age before remediation.
- Developed a Python-based vulnerability scanning pipeline combining Nuclei, Nikto, and custom regex-based detectors.
- Collaborated with DevOps to embed DevSecOps security stages (SCA, SAST) into CI/CD workflows using GitHub Actions.
- Created interactive risk dashboards (Figma → React prototype) that made CVSS scores and mitigation status clear to non-technical stakeholders, accelerating sign-off cycles by 1 week on average.

Skills

- **Cloud & Tooling:** Microsoft 365 Defender, Microsoft Sentinel, Logic Apps, Power Automate, VirusTotal Enterprise
- **Programming & Scripting:** Python, PowerShell, JavaScript (React), Kusto Query Language (KQL)
- **Frameworks & Methodologies:** DevSecOps, MITRE ATT&CK, Agile, HIPAA, ISO 27001, SOC 2

- **AI / ML:** Azure Machine Learning, TensorFlow, LLMs, RAG pipelines
- **Soft Skills:** Technical writing, training & mentorship, cross-team collaboration, UX-driven reporting
-

Projects

PDFreak AI: Explainable AI Framework for PDF Analysis / Brunel University

SEP 2024 - APR 2025, LONDON

- Engineered a **self-hosted, privacy-focused PDF analysis platform** for small SOC teams, leveraging explainable AI to detect threats within budget constraints.
- Integrated a **large language model (LLM)** with **PDFiD** (static analysis) and **Ghidra** (dynamic analysis), identifying malicious scripts and exploits in 50+ PDFs daily with **20% improved detection accuracy.**
- Dissertation achieved an **83.1% model accuracy** using a **Random Forest** binary classifier with **SHAP/LIME** explainability.
- Presented and demonstrated the tool on YouTube, driving community engagement within cybersecurity forums.
- Developed a user-friendly drag-and-drop Azure deployment pipeline to simplify analysis for non-technical users.

Education

Brunel University London / Bachelor of Science in Computer Science

1st Class Honors with Placement

SEP 2021 - JUL 2025, LONDON

PDFreak AI: Static/dynamic PDF analysis (PDFiD, peepdf, PDF-parser, Ghidra) → binary classifier 83.1%, + self-hosted RAG for category/MITRE ATT&CK mapping; web UI with plain-language reports; SHAP/LIME explanations.

Selected modules: Algorithms, Networks & OS, Usability, Software Dev & Mgmt, Logic & Computation.

Certifications & Training

- CompTIA Cybersecurity Analyst (CySA+), In Progress, Expected Completion: November 2025
- Microsoft Build 2025: Deploying Secure AI Applications, Microsoft, May 2025
- Microsoft Defender Fundamentals, Microsoft Learn, 2024
- TryHackMe Cybersecurity Challenges, Completed 10+ Rooms, 2024