# RIFAT ERDEM SAHIN

## SOC ANALYST | SECURITY OPERATIONS & THREAT ANALYSIS SPECIALIST


📍 **Location:** London, United Kingdom
🇬🇧 **Citizenship:** British
✉️ **Email:** contact@rifaterdemsahin.com
📞 **Phone:** +44 7848 024173
🔗 **LinkedIn:** linkedin.com/in/rifaterdemsahin
💻 **GitHub:** github.com/rifaterdemsahin
🌐 **Portfolio:** https://rifaterdemsahin.com
📅 **Schedule a Call:** https://calendly.com/rifaterdem/schedule


## PROFESSIONAL SUMMARY


Senior SOC Analyst specializing in **security monitoring, incident triage, and threat hunting**. Deep expertise in SIEM technologies (Splunk, Microsoft Sentinel) and EDR tools. Proven track record in reducing mean time to detect (MTTD) and respond (MTTR) by refining correlation rules and automating investigation workflows.


## CORE COMPETENCIES

🛡️ **Security Operations** - Log Analysis & Correlation (Splunk SPL, KQL) - Incident Triage & Investigation - Threat Intelligence (TIP) Integration - Phishing Analysis & Malware Sandbox

⚙️ **Tools & Automation** - SIEM (Splunk, Sentinel, ELK) - SOAR (Tines, Palo Alto XSOAR) - EDR using (CrowdStrike, SentinelOne) - Network Traffic Analysis (Wireshark, Zeek)

## KEY ACCOMPLISHMENTS

### 2024 | Global MSP | London

**SOC Maturity Improvement** - **Challenge:** High volume of false positives causing alert fatigue for analysts. - **Solution:** Tuned SIEM correlation rules and implemented SOAR playbooks for initial triage. - **Impact:** - Reduced false positives by 60%. - Improved analyst efficiency, allowing 2x investigation volume. - Reduced MTTR for critical incidents to <30 minutes.

### 2023 | Financial Services | London

**Insider Threat Detection** - **Challenge:** Detect anomalous data exfiltration attempts by employees. - **Solution:** Created UEBA (User and Entity Behavior Analytics) rules based on login patterns and data transfer volumes. - **Impact:** - Detected and stopped a reliable data leak incident. - Established a baseline of normal user behavior. - integrated alerts with HR systems for context.

---

## PROFESSIONAL EXPERIENCE HIGHLIGHTS

**Senior SOC Analyst / AI Solutions Architect** | January 2025 - Present *IBM* | *London, UK*

- Architecting hybrid cloud transformation using IBM Cloud and Red Hat OpenShift for Fortune 500 enterprises
- Implementing watsonx AI solutions for intelligent automation, reducing operational overhead by 35%
- Leading DevSecOps transformation with Ansible Automation Platform and Terraform IaC across multi-cloud environments
- Delivering zero-downtime Kubernetes cluster migrations for mission-critical financial and government workloads
- Building enterprise CI/CD pipelines with GitHub Actions and Jenkins serving 500+ developers globally

**Senior SOC Analyst / Technical Lead** | 2020 - 2025 *Goldman Sachs, Ypsomed, Cushman & Wakefield*

- Led soc analyst initiatives across finance, healthcare, and real estate sectors
- Designed and implemented solutions supporting millions of daily transactions
- Established best practices and automated frameworks

- Mentored engineering teams on modern technologies and practices
- Delivered solutions achieving 300% improvement in operational efficiency

**SOC Analyst** | 2016 - 2020 *Microsoft, Emerson, Various Fortune 500*

- Built enterprise solutions for digital transformation initiatives
- Led cross-functional teams designing scalable applications
- Established frameworks and implementation strategies
- Evangelized modern technologies through technical leadership

---

## EDUCATION

🎓 **Bachelor of Science**
Southern New Hampshire University, USA 🇺🇸 | 2013

---

## CERTIFICATIONS & CONTINUOUS LEARNING

📜 **Microsoft Certified Solutions Architect Expert**
📜 **AWS Certified Solutions Architect Professional**
📜 **Azure Solutions Architect Expert**
📜 **Certified Kubernetes Administrator (CKA)**

**Continuous Learning:**
- Active contributor to open-source projects - Regular participant in technical communities - Following latest developments in technology - Experimenting with emerging tools and practices

---

## SECURITY CLEARANCES

🔒 **UK SC (Security Check)** - Valid until 2028
🔒 **NATO Clearance** - Valid until 2029
✓ **Background Checks:** Watchdog (2024), Sterling (2019)

---

## AVAILABILITY & CONTACT

**Immediate Availability** for soc analyst roles

📅 **Schedule a Discussion:** https://calendly.com/rifaterdem/schedule
📧 **Email:** contact@rifaterdemsahin.com
📞 **Phone:** +44 7848 024173

---

## SUPPORTING DOCUMENTS

📊 **Technical Portfolio & Presentations:**
https://rifaterdemsahin.com/wp-content/uploads/2025/02/rifaterdemsahinprofilepresentation.v2025.2.pdf

---

*References and detailed project portfolios available upon request*